DO NOT REPRINT
© FORTINET
Passdumps.com



FortiSIEM

Study Guide

for FortiSIEM 6.3

Vouchers & Dumps are Available | Passdump

FORTINET NSE Training Institute

DO NOT REPRINT
© FORTINET
Brave-dumps.com

Fortinet Training

https://training.fortinet.com

Fortinet Document Library

https://docs.fortinet.com

Fortinet Knowledge Base

https://kb.fortinet.com

Fortinet Fuse User Community

https://fusecommunity.fortinet.com/home

Fortinet Forums

https://forum.fortinet.com

Fortinet Support

https://support.fortinet.com

FortiGuard Labs

https://www.fortiguard.com

Fortinet Network Security Expert Program (NSE)

https://training.fortinet.com/local/staticpage/view.php?page=certifications

Fortinet | Pearson VUE

https://home.pearsonvue.com/fortinet

Feedback

Email: askcourseware@fortinet.com

FORTINET

12/20/2021

Vouchers & Dumps are Available | WhatsApp +201224560923

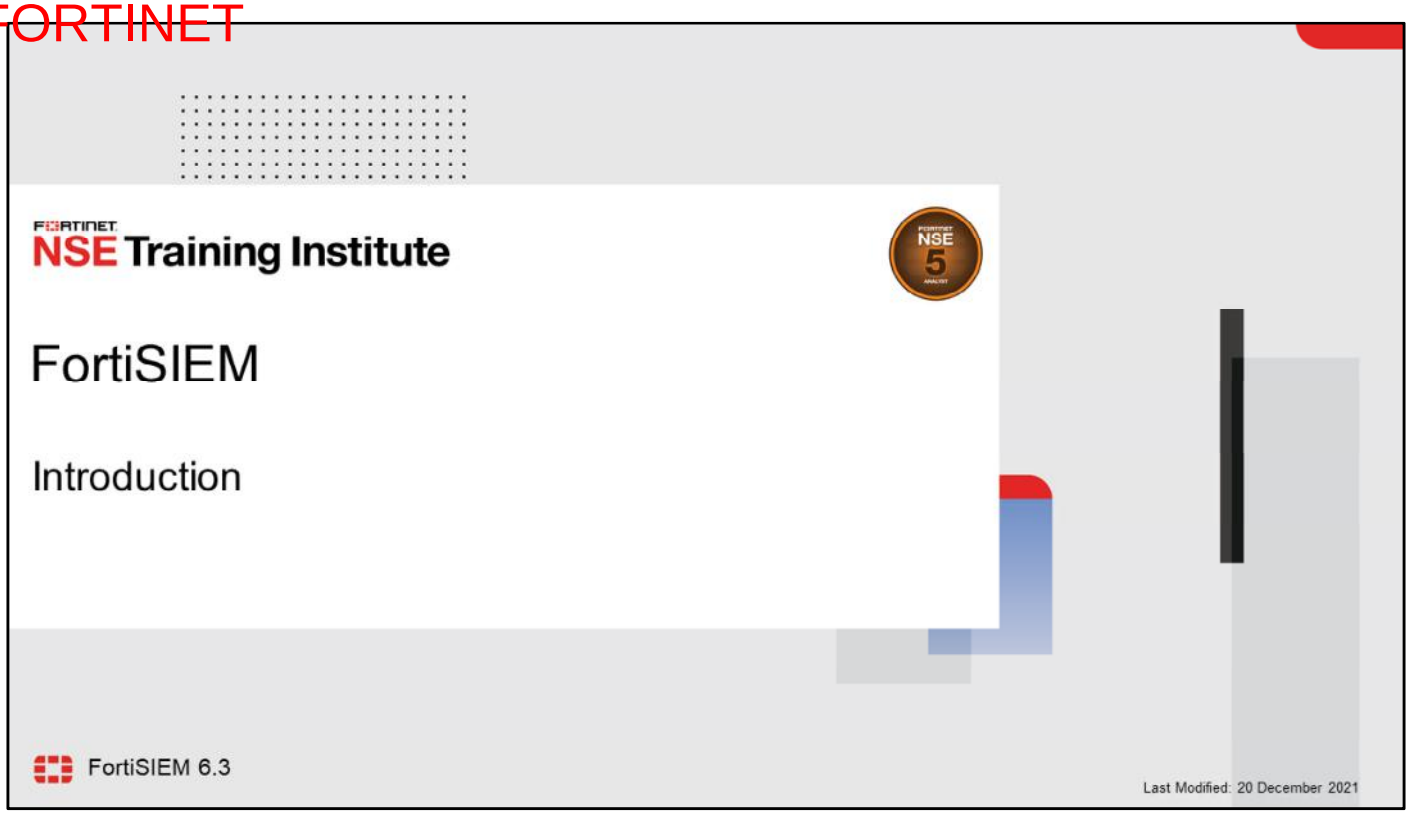
DO NOT REPRINT
© FORTINET
Brave-dumps.com

TABLE OF CONTENTS

01 Introduction 4
02 SIEM and PAM Concepts 63
03 Discovery and FortiSIEM Agents 109
04 FortiSIEM Analytics 169
05 CMDB Lookups and Filters 206
06 Group By and Data Aggregation 234
07 Rules and MITRE ATT&CK 252
08 Incidents and Notification Policies 314
09 Reports and Dashboards 376
10 Maintaining and Tuning 450
11 Troubleshooting 500

Vouchers & Dumps are Available | WhatsApp +201224560923

DO NOT REPRINT
© FORTINET
Brave-dumps.com

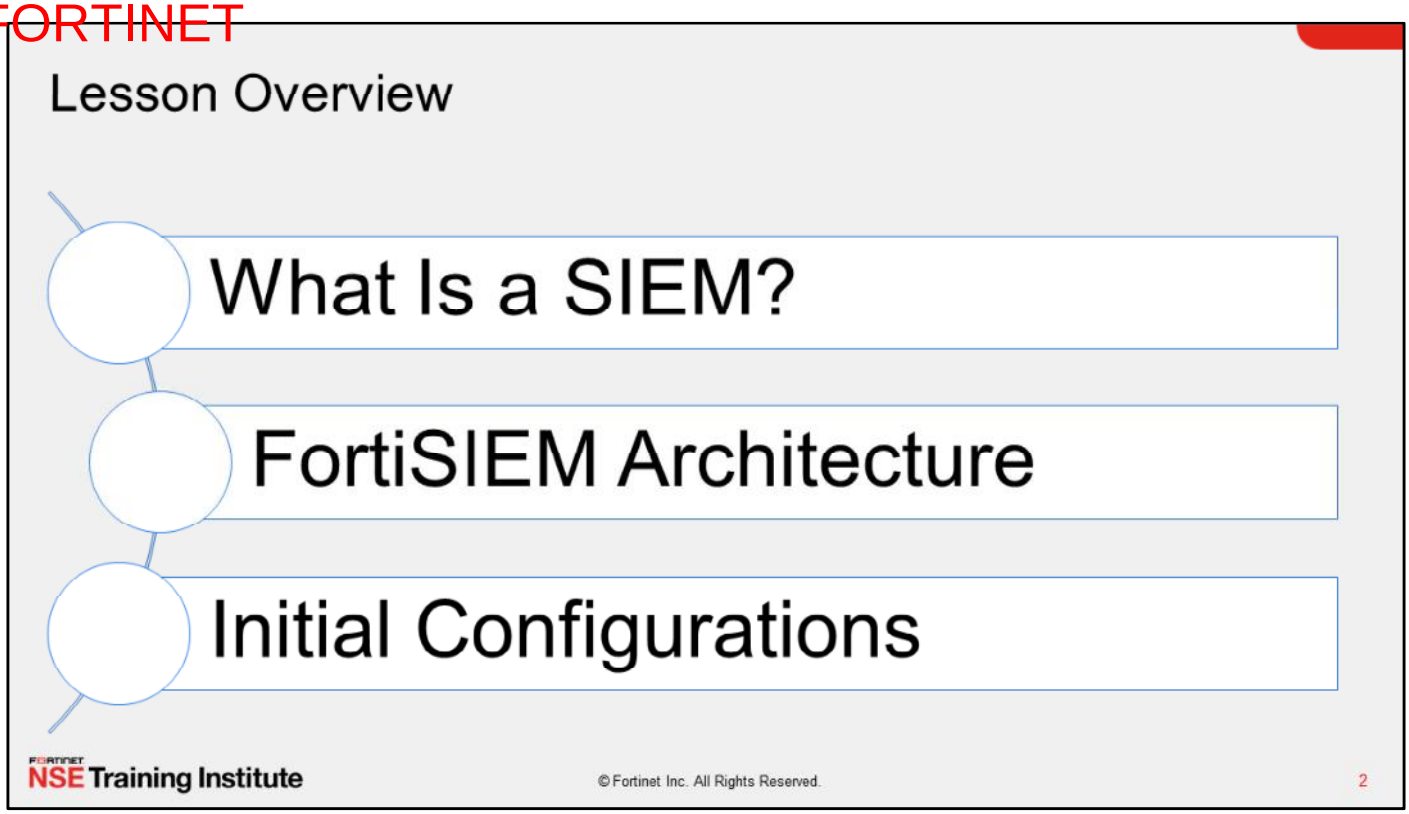


In this lesson, you will learn what a security information and event management (SIEM) is, and how FortiSIEM is different from other SIEMs.

You will also learn about the FortiSIEM architecture and some initial configuration.

Vouchers & Dumps are Available | WhatsApp +201224560923

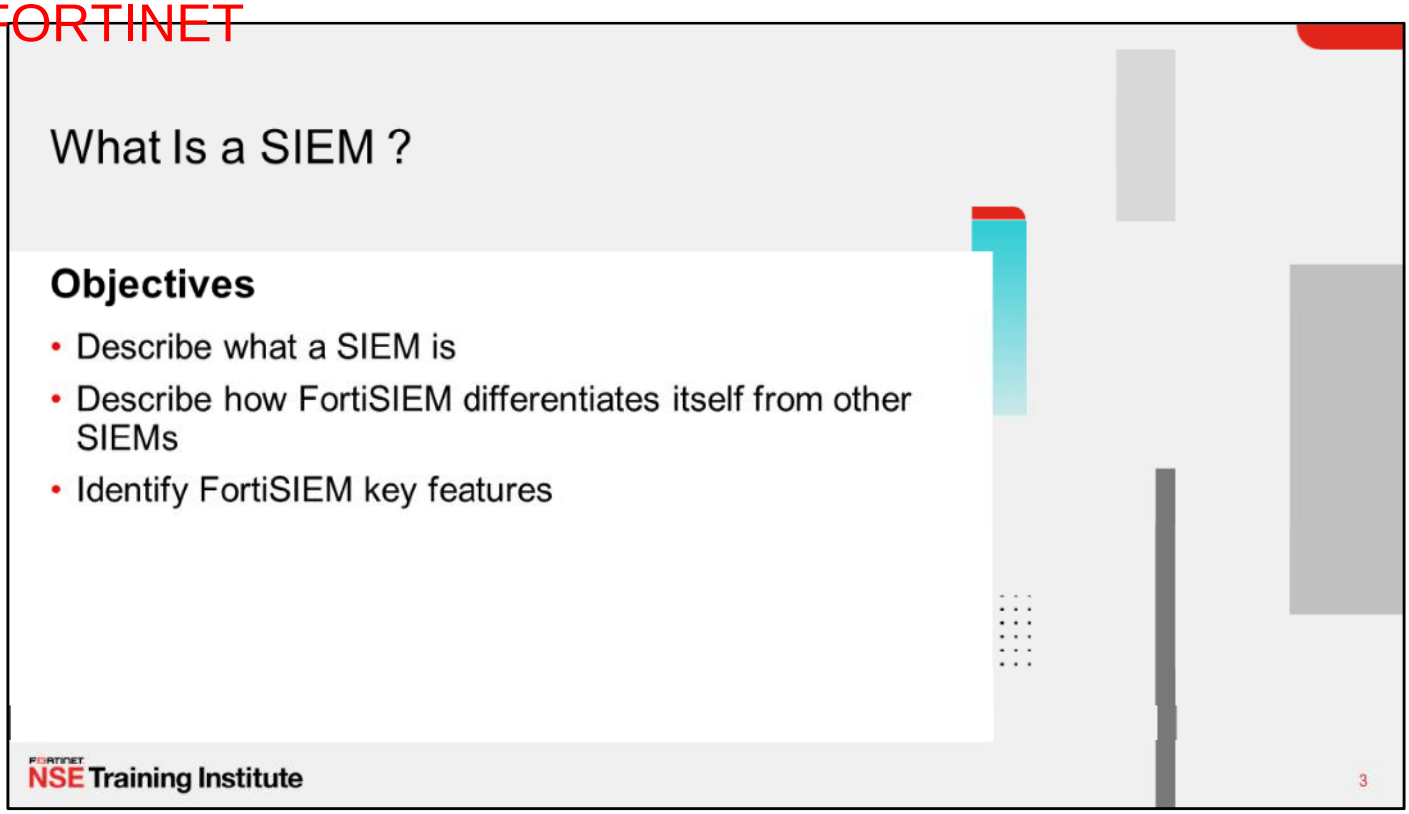
DO NOT REPRINT
© FORTINET
Brave-dumps.com



In this lesson, you will explore the topics shown on this slide.

Vouchers & Dumps are Available | WhatsApp +201224560923

DO NOT REPRINT
© FORTINET
Brave-dumps.com

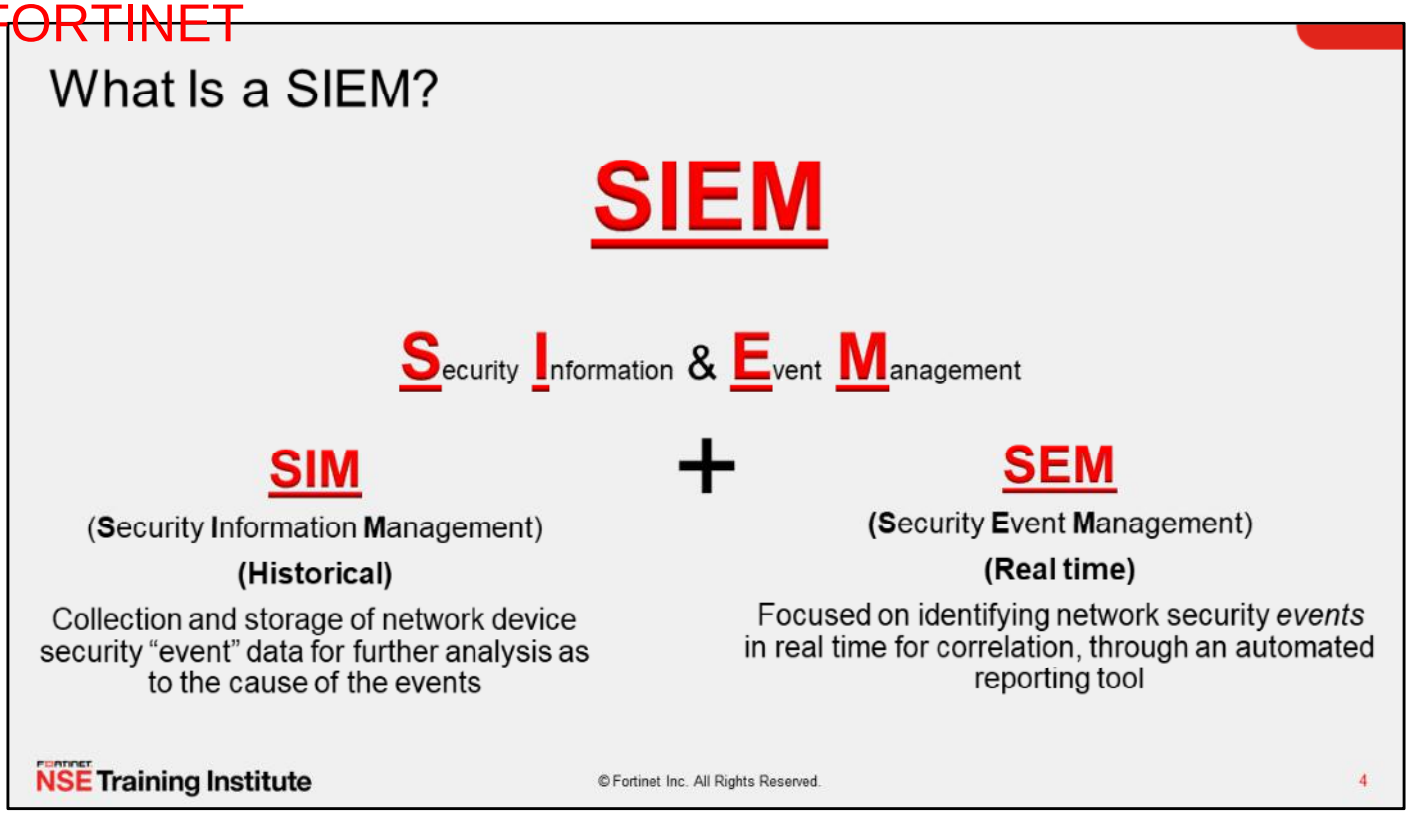


After completing this section, you should be able to achieve the objectives shown on this slide.

By demonstrating competence in understanding SIEMs and how FortiSIEM is different from other SIEMs, you will be able to effectively use the strength of FortiSIEM.

Vouchers & Dumps are Available | WhatsApp +201224560923

DO NOT REPRINT
© FORTINET
Brave-dumps.com



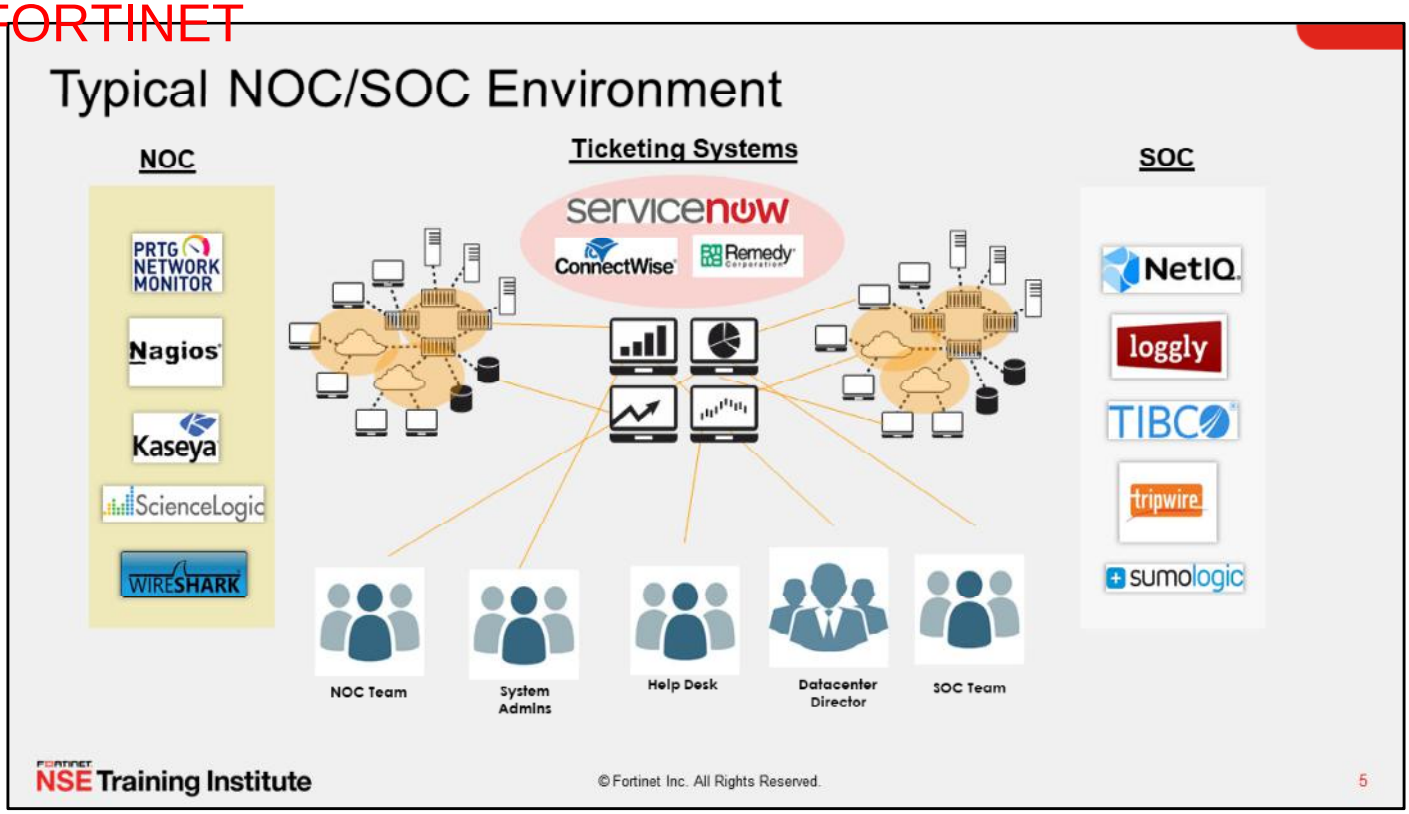
SIEM is an acronym coined by Mark Nicolett from Gartner. Essentially, SIEM combines what were previously two methods of analyzing log data from network elements.

SIM, or security information management, collects data in a central repository for trend analysis and provides automated reporting for compliance and centralized reporting. SEM, or security event management, centralizes the storage and interpretation of logs and allows near real-time analysis, which enables security personnel to take defensive action more quickly. This is also known as incident response (IR).

By bringing SIM and SEM together, SIEM systems focus on providing faster identification, analysis, isolation, and recovery of security threats and events. A key, overarching function of SIEMs is to help compliance managers monitor and validate network conformance with regulatory and compliance requirements.

Vouchers & Dumps are Available | WhatsApp +201224560923

DO NOT REPRINT
© FORTINET
Brave-dumps.com



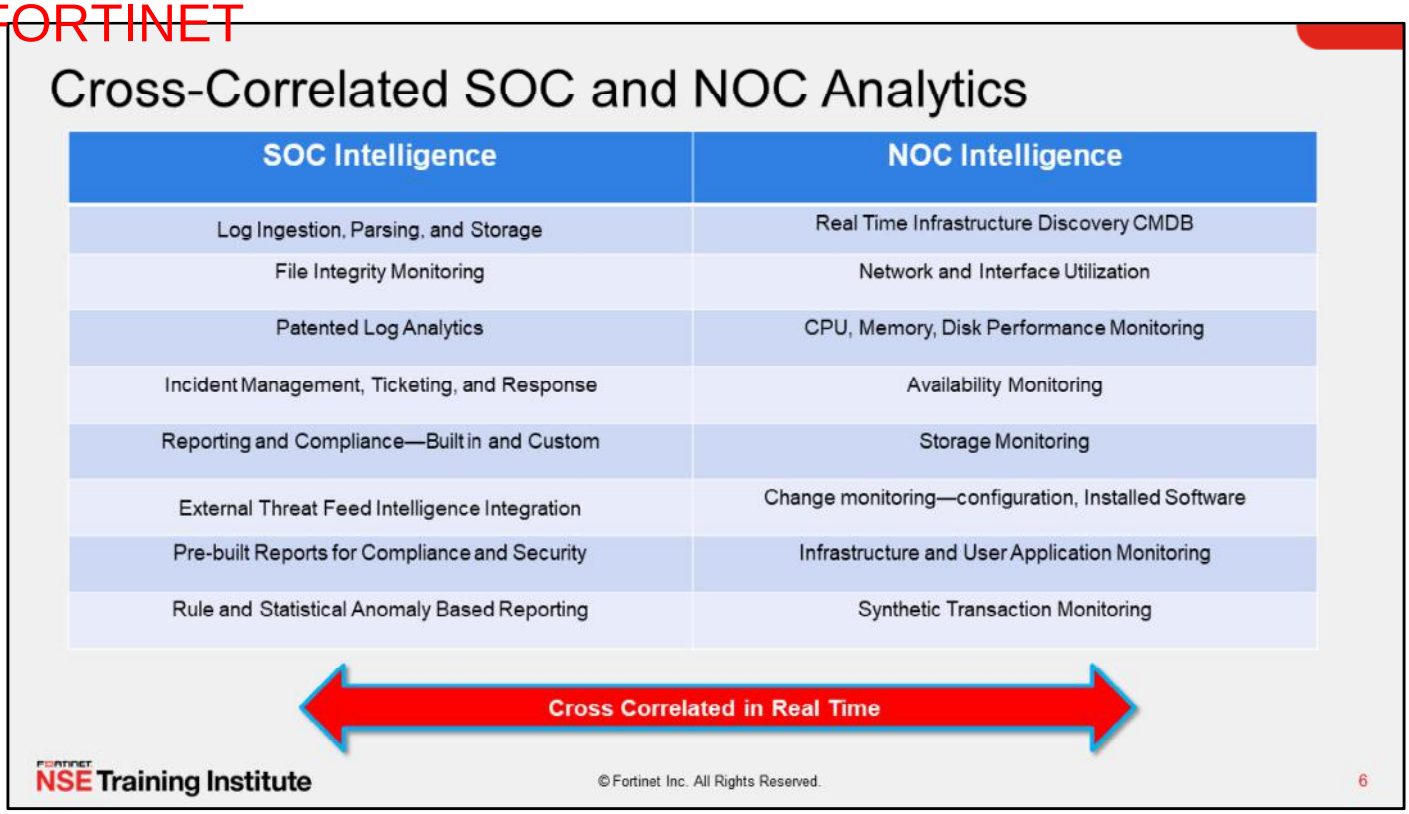
As you know, the likelihood of a breach is now becoming very real for many organizations. This is due, in part, to the inefficient, siloed approach that commonly exists in many IT organizations. The network operations center (or NOC) is primarily focused on network performance, availability, and up time. The security operations center (or SOC) is primarily focused on network security and compliance efforts.

Each department generally employs a wide variety of systems and tools, which are rarely integrated or correlated into a cohesive, and comprehensive view of the organization's overall network. All these factors add up to a complex monitoring and reporting environment, which increases the likelihood that threats and breaches can go undetected for some time. As well, the risks of a breach continue to increase due to an ever growing list of sources and types of threats, such as the internet of things (IoT). When a breach does occur, it poses a daunting challenge to many organizations because the structure of their environment is designed in such a way that the methods used to deal with breaches is often reactive, rather than proactive.

Obtaining the forensics needed to identify the root cause of a breach, requires that all IT hands be on deck and bring data from the disparate systems they manage. Also, because there is no single source of analytics, they need to streamline their efforts. In order to perform these duties, IT representatives must be pulled away from their normal day-to-day operations, and productivity is impacted as they go about the tedious manual correlation of data from each department's systems.

Vouchers & Dumps are Available | WhatsApp +201224560923

DO NOT REPRINT
© FORTINET
Brave-dumps.com

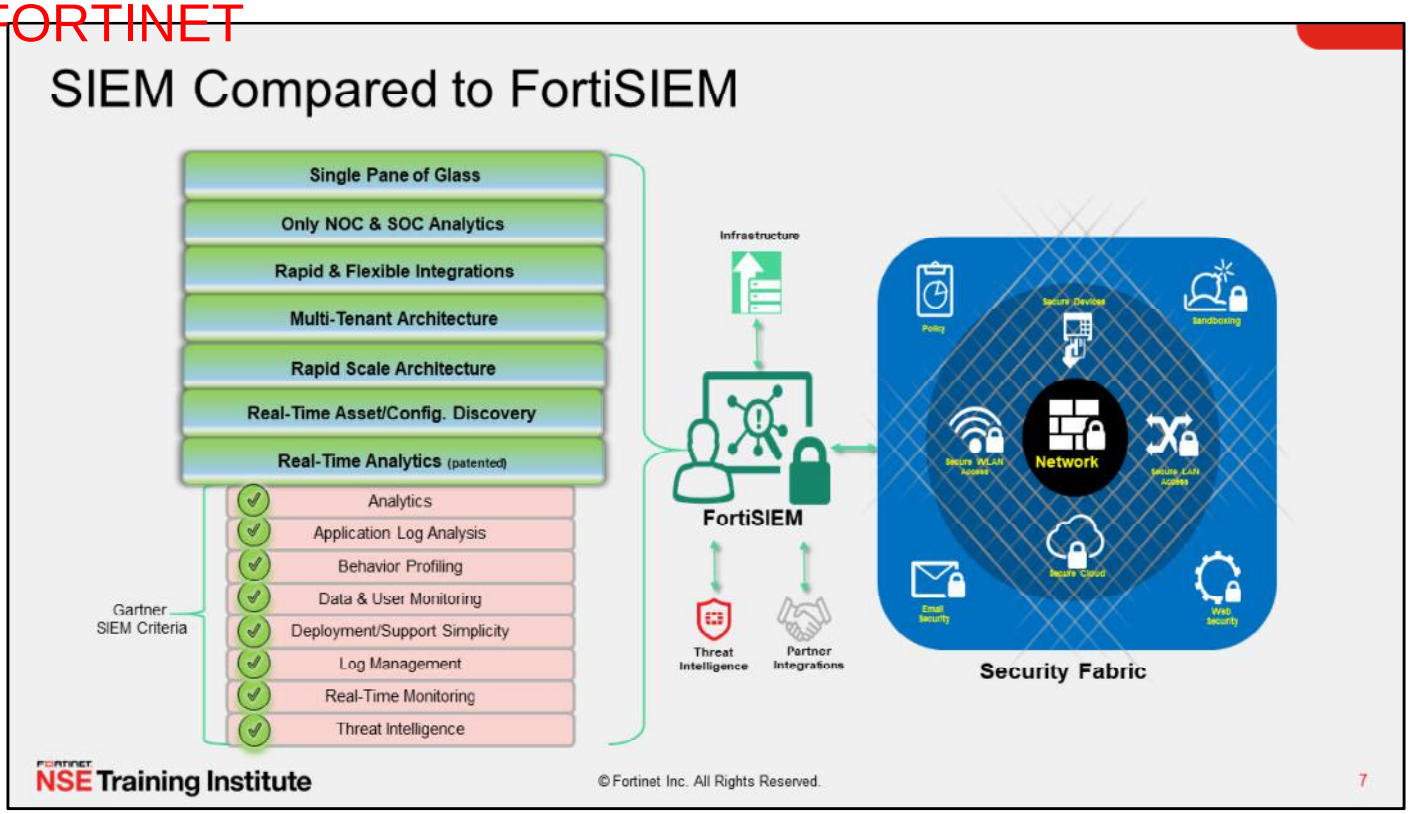


FortiSIEM patented analytics can cross-correlate data that comes from the NOC with data that comes from the SOC.

The FortiSIEM ability to unify data points that are traditionally dispersed across a wide range of NOC and SOC tools and sources, enables organizations and users to monitor, cross-correlate, and analyze, in real time, numerous sources and types of event information. In this deeper context, organizations are more likely and better able to identify threats and their root causes for faster remediation. These rich sources of data also provide the foundation for more comprehensive dashboards and reports.

Vouchers & Dumps are Available | WhatsApp +201224560923

DO NOT REPRINT Brave-dumps.com
© FORTINET



FortiSIEM exceeds basic SIEM functions with its unique, patented, competitive differentiators. FortiSIEM provides organizations with actionable analytics, derived and correlated from dynamic sources of data. The primary goals of FortiSIEM are to:

- Enable organizations to detect threats and breaches sooner
- Provide deep context for root causes
- Supply the information needed to remedy and prevent future threats

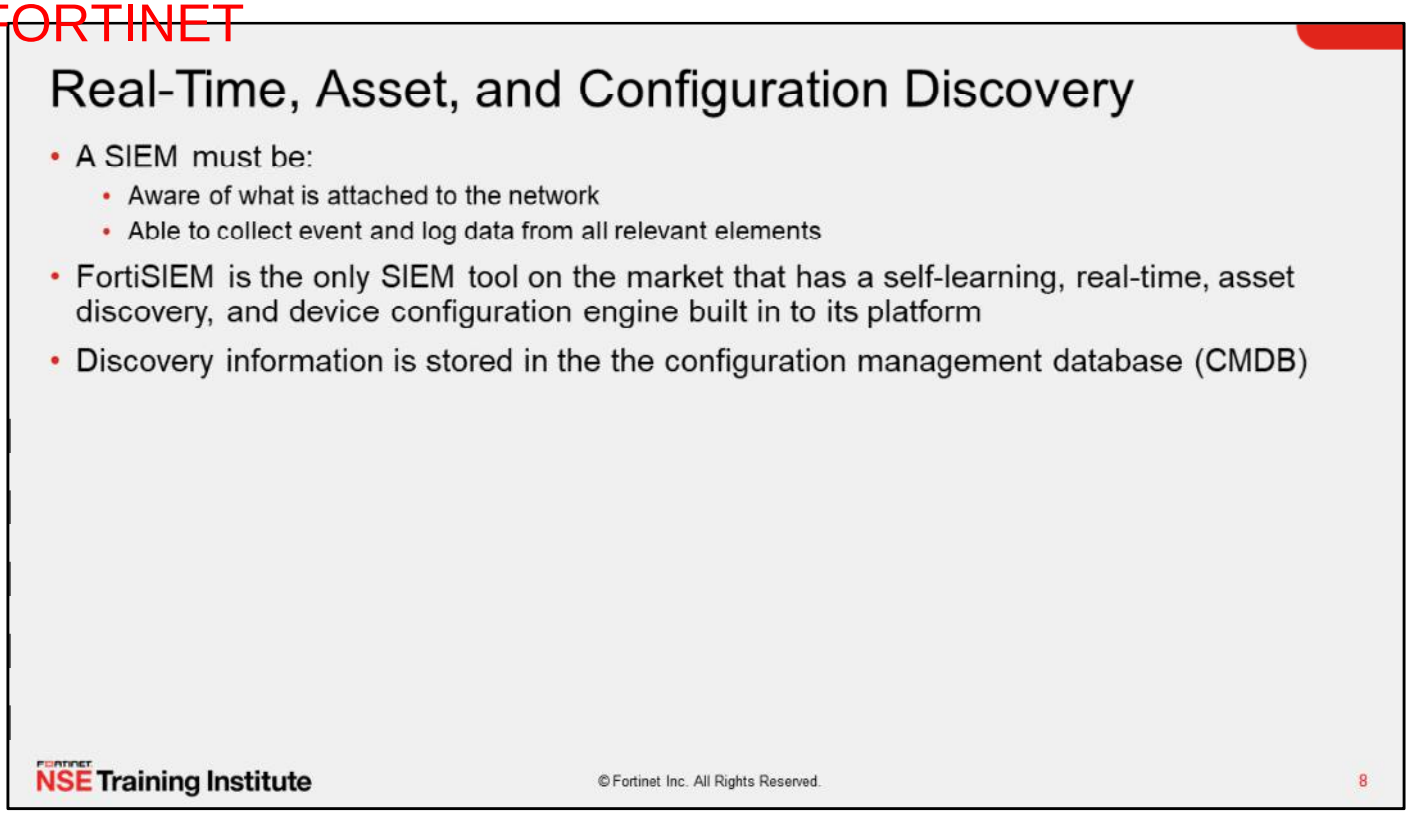
The characteristics that make FortiSIEM unique are:

- Patented real-time analytics
- Real-time asset and configuration discovery
- Purpose-built support for rapid scalability
- A multi-tenant architecture
- Fast and flexible third-party technology integrations
- Analytics delivery through a single pane of glass
- A seamless platform that performs automated network and security operations, and can cross-correlate security event data with network and infrastructure performance data to provide SOC and NOC analytics in real time. FortiSIEM is the only SIEM on the market that provides this capability.

FortiSIEM provides visibility into an organization's entire infrastructure. It supplies information about the infrastructure's real-time performance matched to security event data. To supply this information and increase visibility into the Fortinet Security Fabric, FortiSIEM uses APIs that gather additional information from external threat intelligence sources, and integrates with hundreds of technology partners throughout the stack.

Vouchers & Dumps are Available | WhatsApp +201224560923

DO NOT REPRINT
© FORTINET
Brave-dumps.com



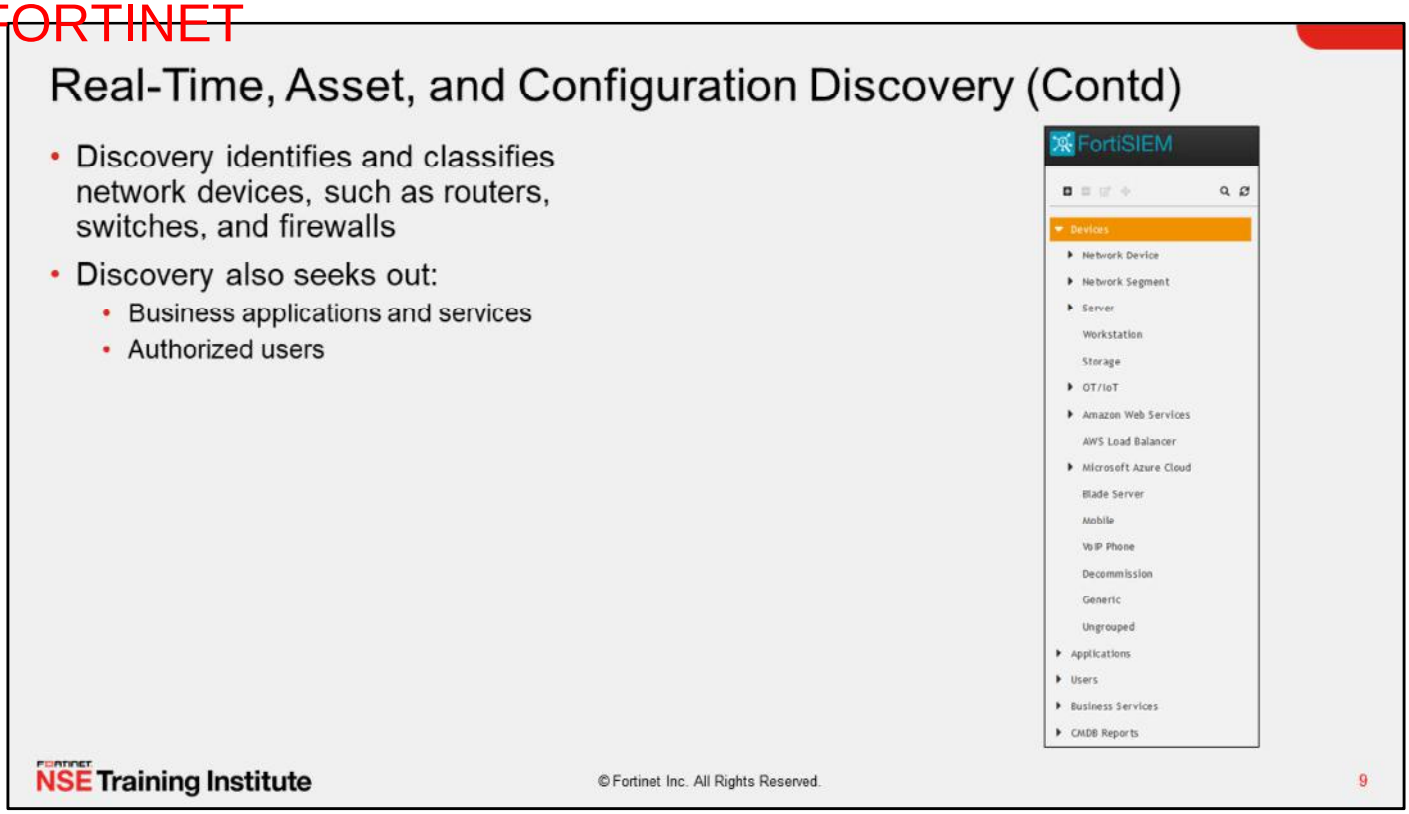
In order for any SIEM tool to be effective, it must be aware of what is attached to the network and be able to collect event and log data from all relevant elements. Any element attached to the network that is unknown to the SIEM can expose an organization breaches. This is especially a concern with rogue elements, such as those associated with IoT.

ForitiSIEM is the only SIEM tool on the market that has a self-learning, real-time, asset discovery, and device configuration engine built into its platform. Many competing SIEM solutions require this data to be entered manually, which introduces the potential for human error, and also increases the likelihood that the information is out of date as soon as it is entered. This process helps organizations establish baselines for their networks and identify normal behavior, which then help form the criteria for abnormal conditions that will generate alerts and alarms.

Discovery information is stored in the CMDB. After you enter the device administrator's credentials, as well as the range of IP addresses that exists on the network, the CMDB has the unique ability to discover all physical and virtual network infrastructure elements.

Vouchers & Dumps are Available | WhatsApp +201224560923

DO NOT REPRINT
© FORTINET
Brave-dumps.com

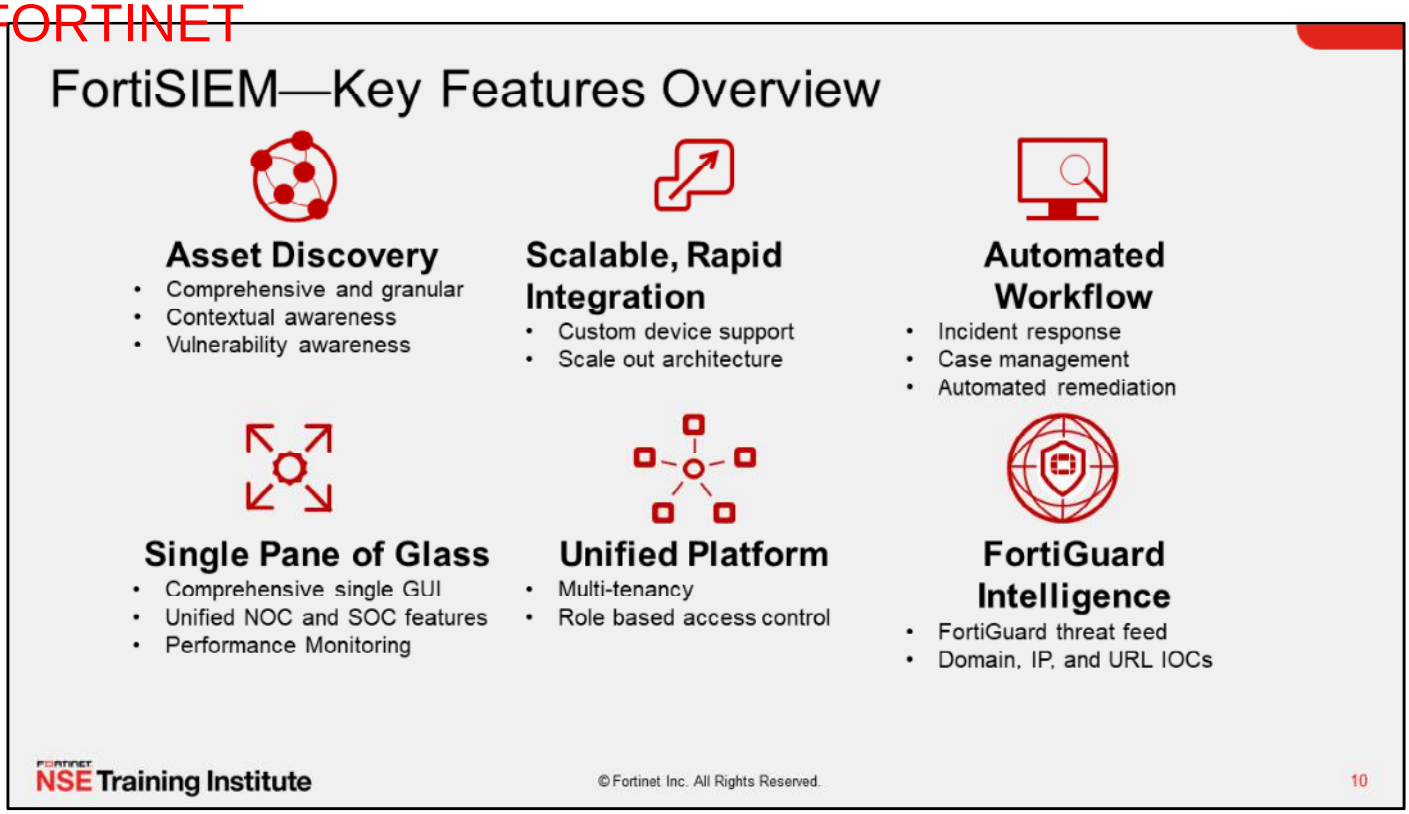


Discovery identifies and classifies network devices, such as routers, switches, and firewalls, as well as cloud and virtual environments on the network. But it doesn't stop there. It also seeks out business applications and services running on the network, as well as authorized users and their roles.

Once FortiSIEM CMDB baseline details are established, the organization can then identify alert and alarm criteria that, when met, trigger automatic notifications when changes occur against the established thresholds.

Vouchers & Dumps are Available | WhatsApp +201224560923

DO NOT REPRINT
© FORTINET
Brave-dumps.com



Review key features that differentiate FortiSIEM from standard SIEM platforms.
Active asset discovery and performance monitoring: FortiSIEM can perform active asset discovery. It has an integrated CMDB to assist with asset management. FortiSIEM performs performance and availability monitoring, such as CPU, memory, storage and configuration change monitoring. This extends the functionality of the platform, and provides the user with additional contextual data.

Scale out architecture: The virtual machine (VM) architecture of FortiSIEM allows rapid scalability, easily increase performance and log processing capacity by adding virtual appliances and there is no charge for virtual machines.

Single-pane-of-glass: Most FortiSIEM features, including dashboards, analytics, incidents, CMDB, and administration, are accessed using an intuitive, web-based, GUI. Customizable role-based access control (RBAC) allows organizations to control what each user can access.

Multi-tennant MSSP features: FortiSIEM supports MSSP deployments with a scalable multi-tenant feature set, including a customizable, multi-tenant capable GUI, multi-tenant-capable database, and scalable, multi-tenant capable architecture.

FortiGuard integration: The FortiSIEM IOC subscription provides access to the FortiGuard Indicators of Compromise threat feed. You can correlate this high value threat feed with logs to help identify malicious traffic.

Of course, FortiSIEM also performs traditional SIEM functions, such as, central log management, automated analysis and alerting, log analytics and reporting, and dashboards.

Vouchers & Dumps are Available | WhatsApp +201224560923

DO NOT REPRINT
© FORTINET
Brave-dumps.com

Knowledge Check

1. FortiSIEM can cross-correlate data that comes from the SOC with data that comes from the_____.
   - ✓ A. NOC
   - B. POC

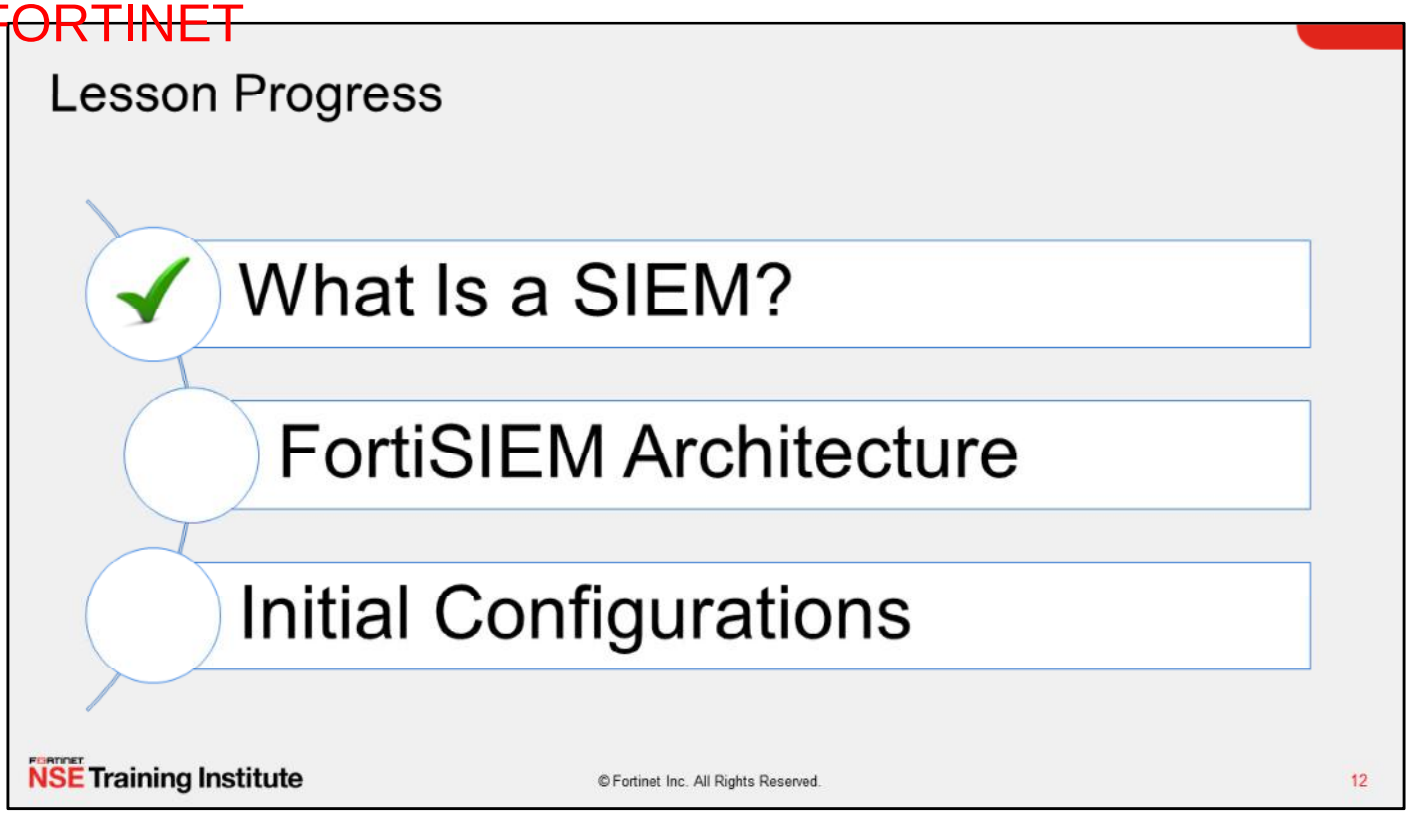
NSE Training Institute

© Fortinet Inc. All Rights Reserved.

11

Vouchers & Dumps are Available | WhatsApp +201224560923

DO NOT REPRINT
© FORTINET
Brave-dumps.com

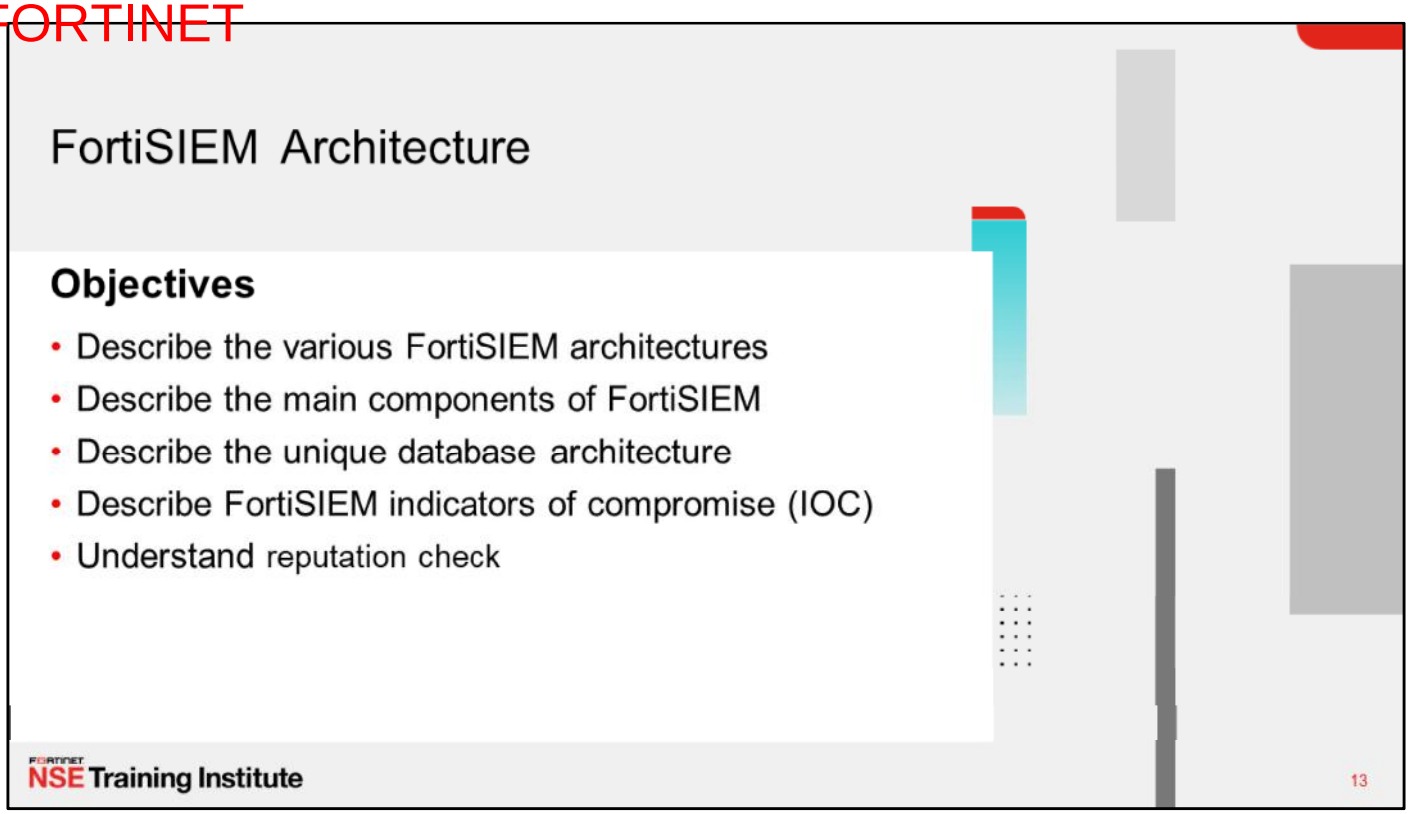


Good job! You now understand what a SIEM is and how FortiSIEM is unique in the market.

Now, you'll learn about FortiSIEM architecture.

Vouchers & Dumps are Available | WhatsApp +201224560923

DO NOT REPRINT
© FORTINET
Brave-dumps.com

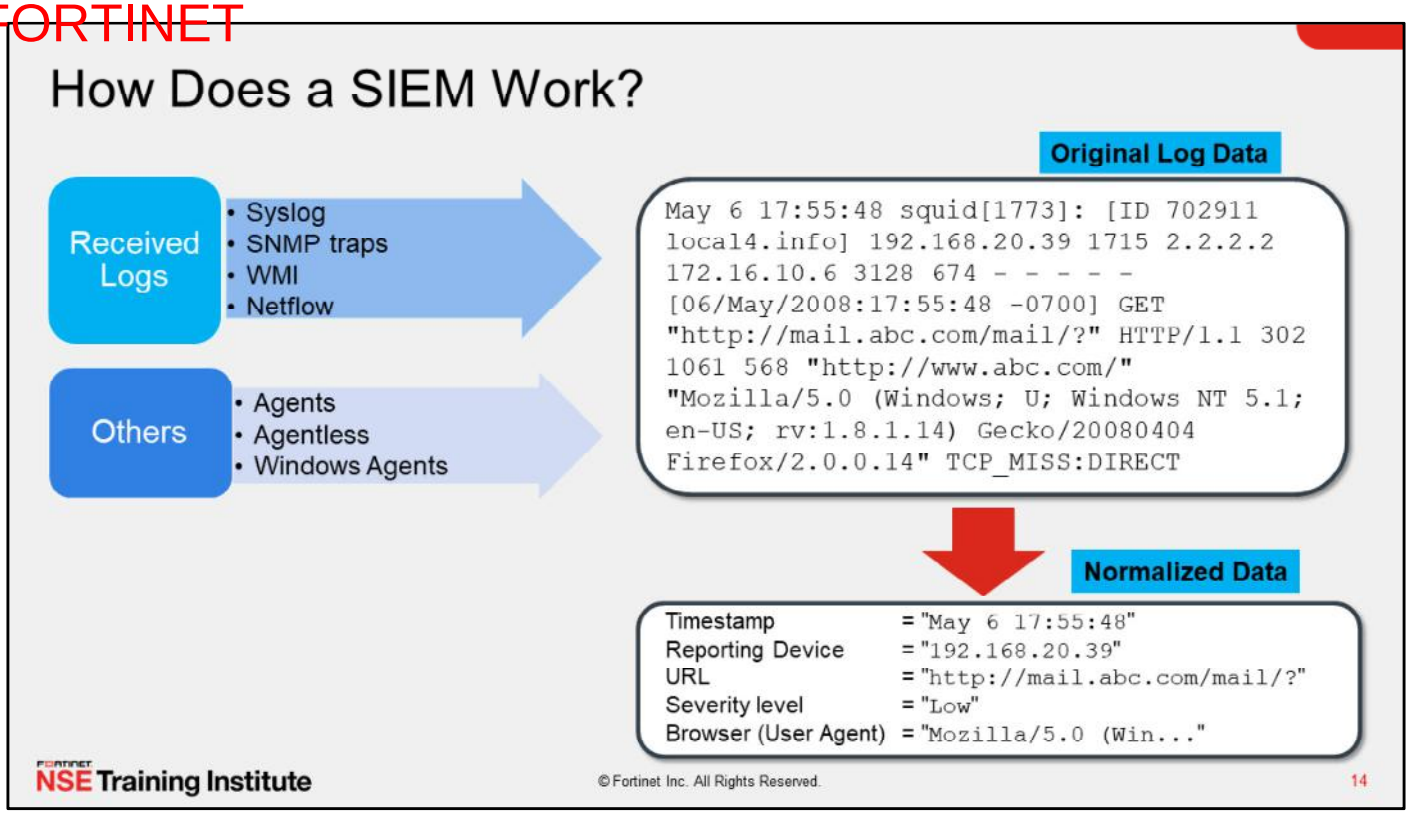


After completing this section, you should be able to achieve the objectives shown on this slide.

By demonstrating competence in understanding FortiSIEM architecture, you will be able to describe the main components of FortiSIEM and its unique database architecture.

Vouchers & Dumps are Available | WhatsApp +201224560923

DO NOT REPRINT Brave-dumps.com
© FORTINET



FortiSIEM receives logs from various sources, such as syslog and others. After receiving logs, FortiSIEM parses and normalizes data.

There are five primary data analysis tasks:

- Indexing the data and storing it in an event database
- Searching the data
- Correlating the data in streaming mode to trigger rules (behavioral anomalies)
- Creating a user identity and location database for adding context to data
- Creating baselines for anomaly detection

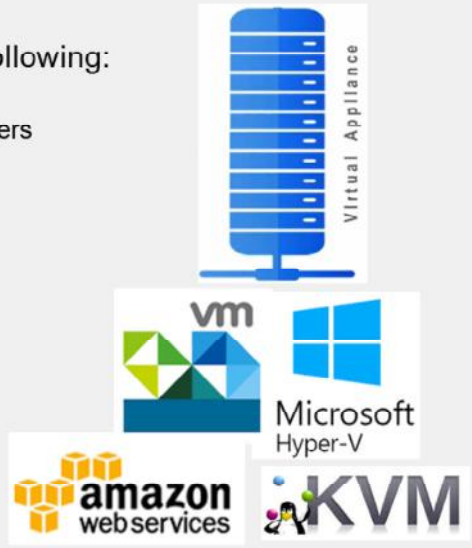
In this lesson, you will learn how FortiSIEM achieves all of the tasks listed above.

Vouchers & Dumps are Available | WhatsApp +201224560923

DO NOT REPRINT
© FORTINET
Brave-dumps.com

FortiSIEM Architecture

- FortiSIEM is a prebuilt 64-bit virtual machine (VM), that runs on VMware ESX or ESXi, Hyper-V, Amazon EC2, KVM
- VA event and performance data are stored on one of the following:
  - Virtual disk up to 2 TB of data
  - NFS storage used when >2 TB of data or when using super + workers
  - Elasticsearch
- Hardware appliances are also available:
  - 2000F (15K EPS)
  - 3500F (30K EPS)
  - 500F Collectors (5K EPS)



NSE Training Institute

© Fortinet Inc. All Rights Reserved.

15

A key element of the FortiSIEM architecture is its form factor. FortiSIEM is available as a virtual appliance and also a physical appliance. FortiSIEM is available as a hardware device. It is also available as a 64-bit, hardened, CentOS virtual machine that is preconfigured and preinstalled with FortiSIEM for your hypervisor environment.

FortiSIEM supports VMware, Windows Hyper-V, Amazon's AWS and Red Hat KVM.

Vouchers & Dumps are Available | WhatsApp +201224560923

DO NOT REPRINT
© FORTINET
Brave-dumps.com

FortiSIEM Hardware Devices

- Three models:
  - Collector – FSM-500F
  - Mid-range all-in-one device – FSM-2000F
  - High-end all-in-one device – FSM-3500F



Model	Hardware	Performance
Collector FSM-500F	4 core, 16 GB	5K EPS, 500 SNMP, 200 WMI
FSM-2000F	6 core, 32 GB, 36 TB	15K EPS (all features turned on)
FSM-3500F	20 core, 64 GB, 72 TB	30K EPS (all features turned on)

NSE Training Institute

© Fortinet Inc. All Rights Reserved.

16

Currently three models are available for FortiSIEM hardware devices:

- Collector – FSM-500F
- Mid-range all-in-one device – FSM-2000F
- High-end all-in-one device – FSM-3500F
- Refer to the quick start guide for each hardware model for further information.

Vouchers & Dumps are Available | WhatsApp +201224560923

DO NOT REPRINT
© FORTINET
Brave-dumps.com

Resource Requirements for FortiSIEM Virtual Machines

- Minimum hardware requirements for FortiSIEM virtual machine nodes are as follows

Node	vCPU	RAM	Local Disks
Supervisor (all in one)	Minimum – 16 Recommended - 32	Minimum •without UEBA – 24 GB •with UEBA – 64 GB Recommended •without UEBA – 32 GB •with UEBA – 64 GB	OS – 25 GB OPT – 100 GB CMDB – 60 GB SVN – 60 GB Local Event database – based on need
Workers	Minimum – 8 Recommended - 8	Minimum – 16 GB Recommended – 24 GB	OS – 25 GB OPT – 100 GB
Collector	Minimum – 4 Recommended – 8 (based on load)	Minimum – 4 GB Recommended – 8 GB	OS – 25 GB OPT – 100 GB

Note that these are only the minimum requirements. Performance may improve if you increase vCPUs and RAM in certain situations. External storage depends on your EPS mix and the number of days of log storage needs

NSE Training Institute

© Fortinet Inc. All Rights Reserved.

17

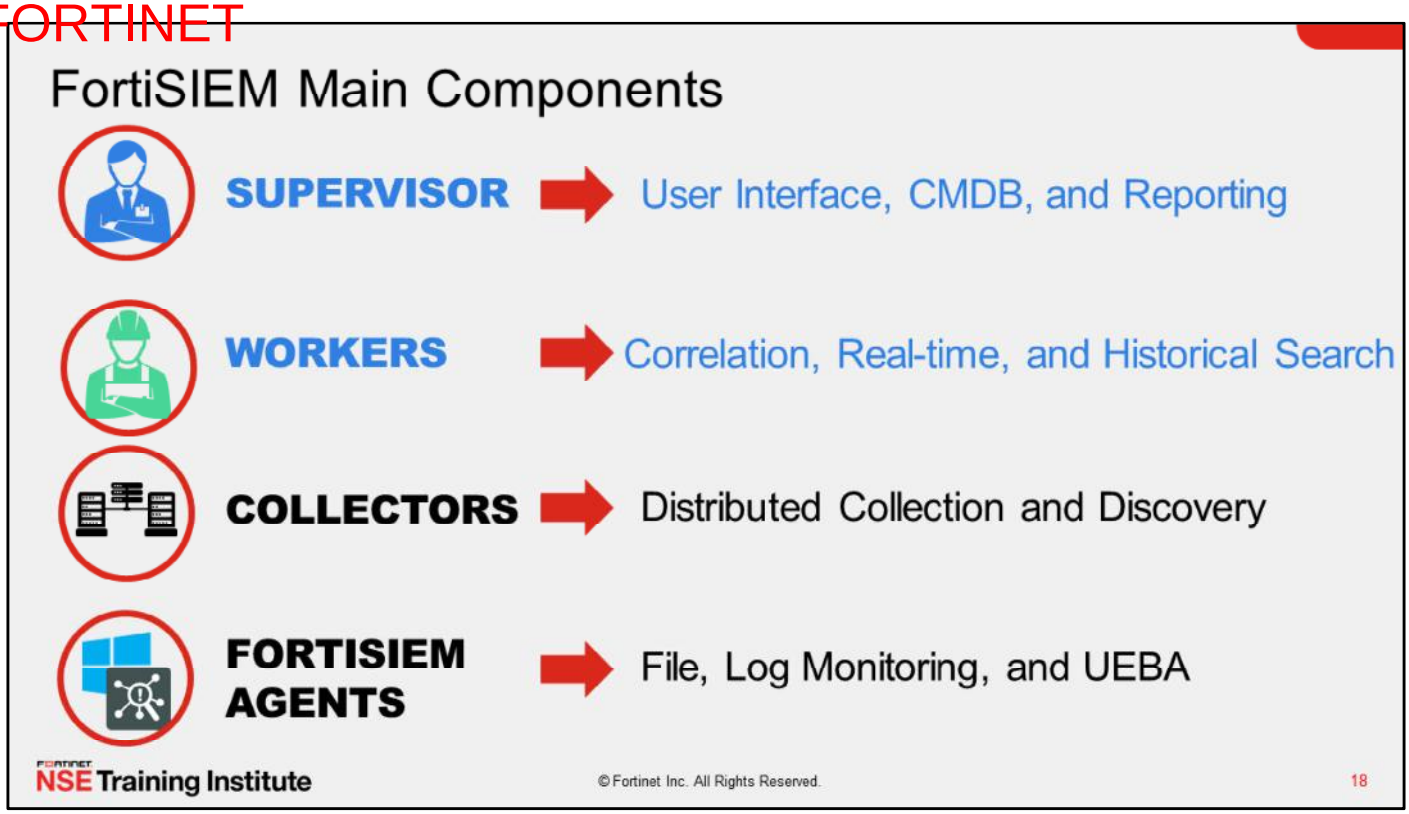
A big benefit of the FortiSIEM form factor is scalability. If your company grows, and you start sending more data to FortiSIEM than what it was initially configured to handle, you can upgrade the VM and add more resources. It's easy to add CPUs, memory, and even storage to VMs. There are no charges or fees from Fortinet, unlike some vendors that charge by the number of CPUs used. You can also add additional VMs—collectors and workers–at no extra charge. The minimum hardware requirements for a supervisor are, 16 vCPU, 32 GB of RAM, and additional storage for the events database (500 EPS ~= 1TB/year).

There are no size limits for the events database, and no charges or fees for storing months' or years' worth of data. That is important to note when considering compliance reporting, and PCI or HIPPA requires that you store a year's worth of data in order to provide appropriate audit reports. It's very easy to determine how much storage you'll need. If your network is sending 500 events per second to FortiSIEM, it requires approximately 1 TB of storage space for a year's worth of data. And that equation is very linear. A 1,000 EPS would require 2 TB, and a 1,500 EPS requires 3 TB of storage.

You can use a similar linear equation when calculating storage requirements for performance data. Storing performance and availability monitoring metrics for 500 devices takes about 100 GB of disk space a year. So, metrics from 1,000 devices requires 200 GB, and 1,500 devices require 300 GB of storage for a year's worth of data. Refer to the *FortiSIEM User Guide* for the hardware requirements for the supervisor, worker, and collector based on the licensed EPS.

Vouchers & Dumps are Available | WhatsApp +201224560923

DO NOT REPRINT
© FORTINET
Brave-dumps.com



FortiSIEM scales seamlessly from small enterprises to large and geographically distributed enterprises and service providers.

- For smaller deployments, you can deploy FortiSIEM as a single all-in-one hardware or virtual machine that contains the full functionality of the product.
- For larger environments that need greater event handling throughput, you can deploy FortiSIEM in a cluster of supervisor and worker virtual machines.

There are three types of FortiSIEM nodes :

- Supervisor
- Worker
- Collector

Supervisor and worker nodes reside inside the data center and perform data analysis functions using distributed cooperative algorithms.
Collectors are used to scale data collection from various geographically separated network environments that reside potentially behind firewalls. Collectors communicate to the devices, collect, parse, and compress the data, and then send the data to the supervisor/worker nodes over a secure HTTP(S) channel in a load balanced manner.
You will review various deployment scenarios using these three nodes later in this lesson.

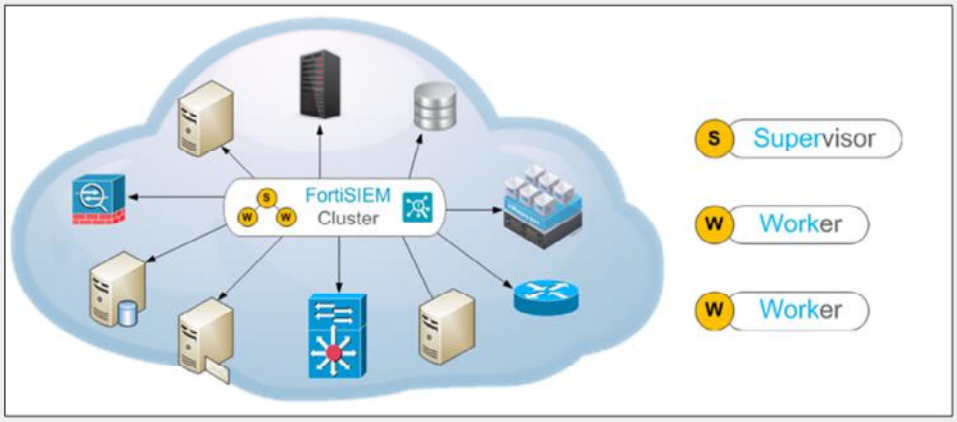
Network devices, such as routers, switches, and firewalls typically have syslog capabilities. That is to say, they have the ability to push out audit logs to a syslog collector. Server devices like Linux servers, for example, typically run a syslog daemon, which again enables the devices to send the logs to FortiSIEM. Other server devices, such as Windows servers, don't have the ability to send syslog messages natively. For those devices, you can install a syslog agent, such as a FortiSIEM Windows agent, to perform that function.

Vouchers & Dumps are Available | WhatsApp +201224560923

DO NOT REPRINT
© FORTINET
Brave-dumps.com

FortiSIEM Components—Supervisor and Workers

- FortiSIEM cluster consists of supervisor and one or more workers sharing the same NFS mount for data storage



NSE Training Institute

© Fortinet Inc. All Rights Reserved.

19

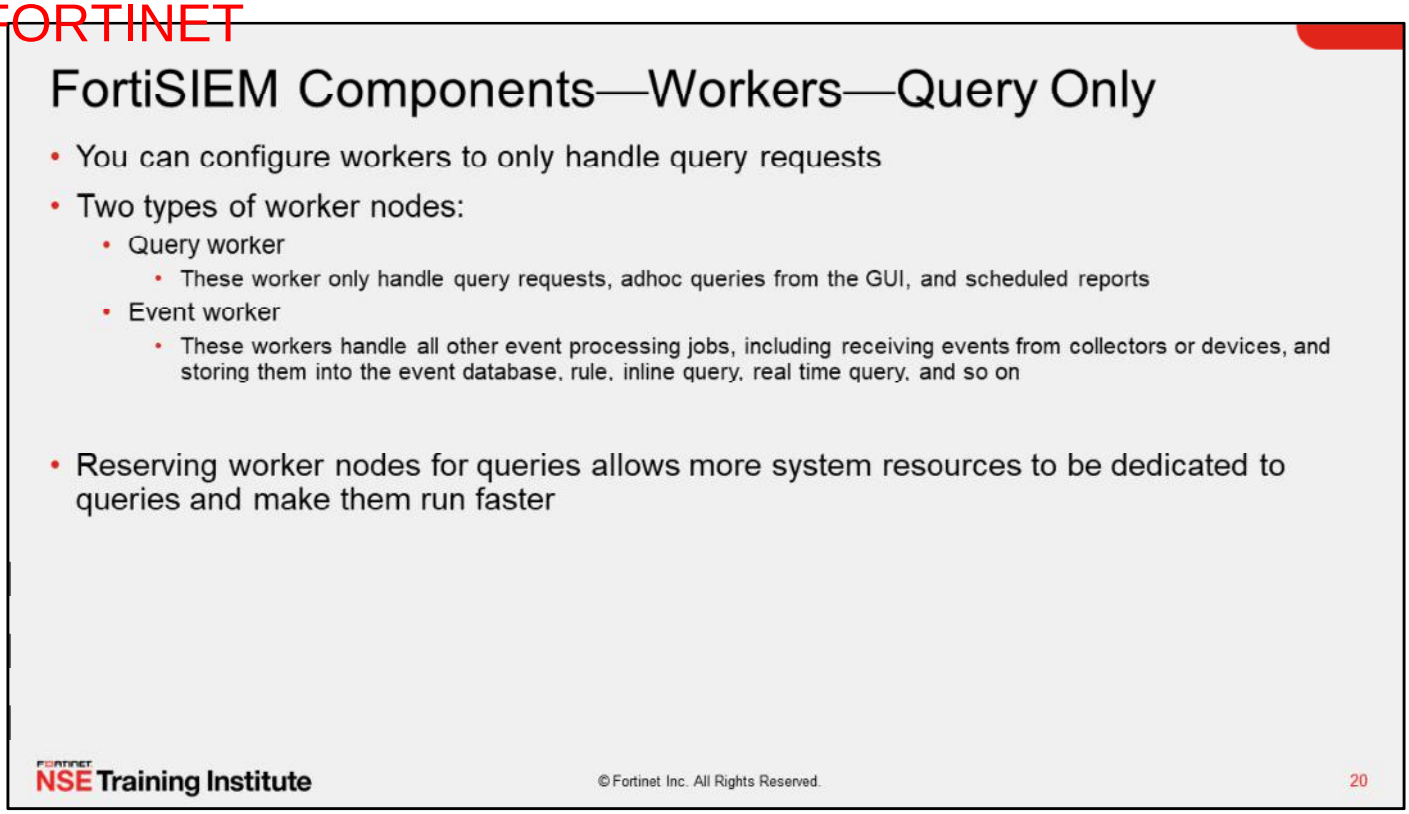
A FortiSIEM cluster consists of a supervisor and one or more workers sharing the same NFS mount or Elasticsearch for data storage.

There are five primary data analysis tasks:
- Indexing the data and storing it in an event database
- Searching the data
- Correlating the data in a streaming mode to trigger rules (behavioral anomalies)
- Creating a user identity and location database for adding context to data
- Creating baselines for anomaly detection

For scalability, each of these tasks is divided into a heavyweight worker component executed by the worker nodes and a lightweight master component executed by the supervisor node. The supervisor node also functions as the GUI using a self-contained three-tier model—GUI, application server containing the business logic, and a relational database for holding the FortiSIEM application state.

Vouchers & Dumps are Available | WhatsApp +201224560923

DO NOT REPRINT
© FORTINET
Brave-dumps.com



You can configure workers to only handle query requests. There are now two types of worker nodes:

- Query Worker - these worker only handle query requests, adhoc queries from the GUI, and scheduled reports.
- Event Worker - these workers handle all other event processing jobs, including receiving events from collectors or devices, and storing them into the event database, rule, inline query, real time query, and so on.

Reserving worker nodes for queries allows more system resources to be dedicated to queries and make them run faster.

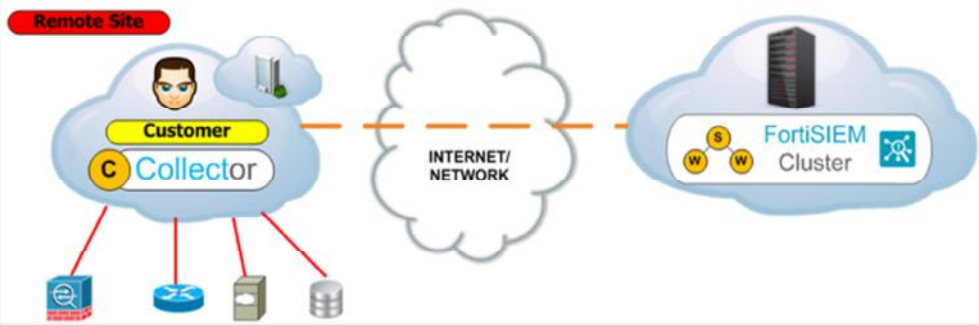
For more information on configuring an event worker or a query worker, refer to the *FortiSIEM User Guide* .

Vouchers & Dumps are Available | WhatsApp +201224560923

DO NOT REPRINT
© FORTINET
Brave-dumps.com

FortiSIEM Components—Collectors

- You can use collectors in both the enterprise and service provider editions
- A collector serves the purposes of monitoring and collecting logs from remote devices before shipping the data back to the central installation



- Under normal operation, the collector does not store data

NSE Training Institute
© Fortinet Inc. All Rights Reserved.
21

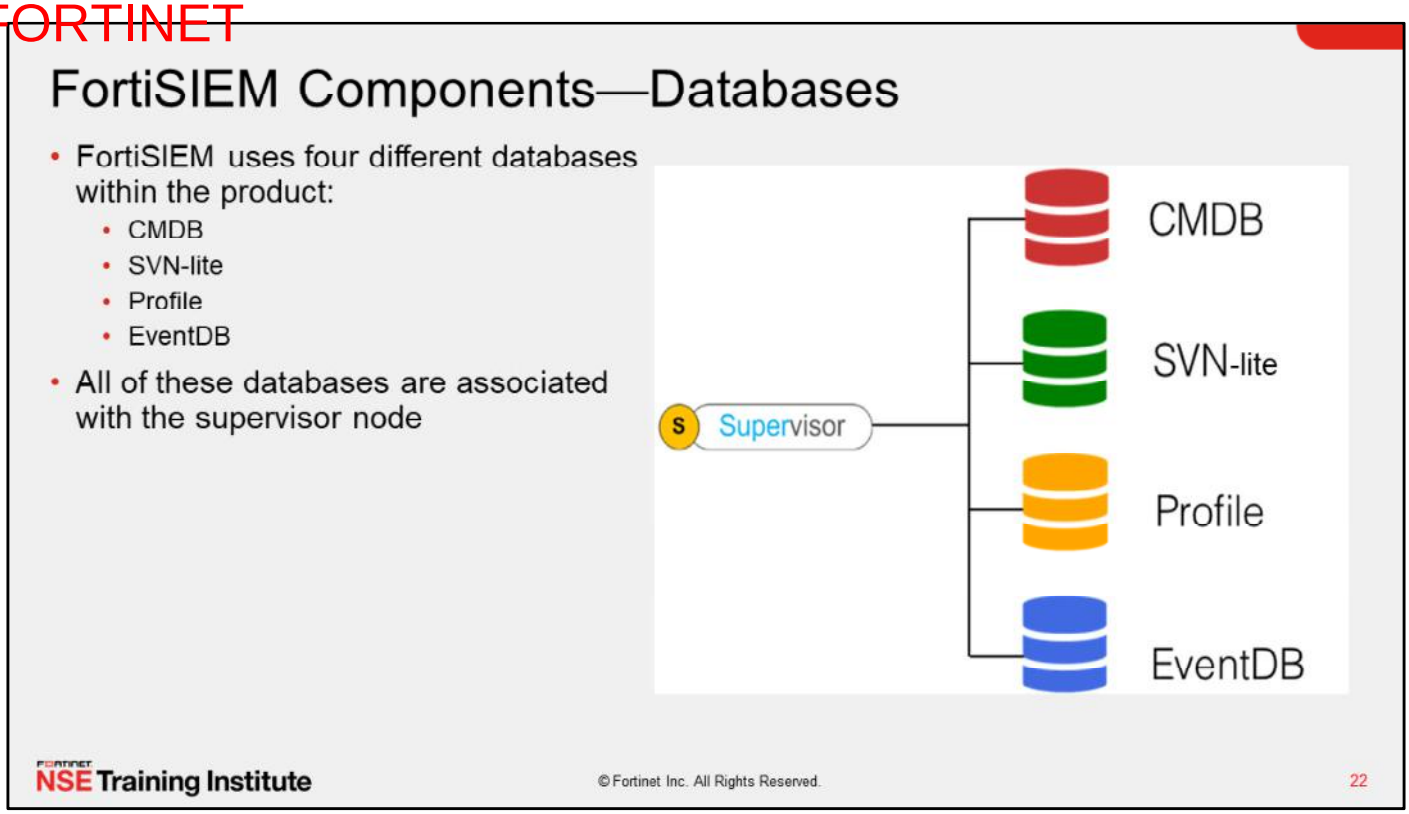
You can use collectors in both the enterprise and service provider editions.

Collector servers monitor and also collect logs from remote devices before shipping the data back to the central installation.

Under normal operation, the collector does not store data.

Vouchers & Dumps are Available | WhatsApp +201224560923

DO NOT REPRINT
© FORTINET
Brave-dumps.com



FortiSIEM uses four different databases within the product:

- CMDB
- SVN-lite
- Profile
- EventDB

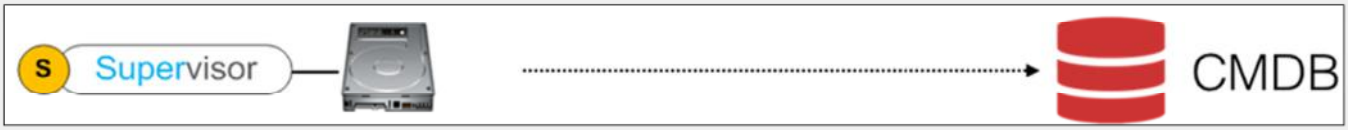
All of these databases are associated with a supervisor node.

Vouchers & Dumps are Available | WhatsApp +201224560923

DO NOT REPRINT
© FORTINET
Brave-dumps.com

FortiSIEM Components—CMDB

- The CMDB resides on the supervisor node



- Uses a postgres database to store FortiSIEM configuration items, such as device information, credentials, discovery information, rules, reports, and so on
- By default, the CMDB also resides on the worker nodes, but is not used

NSE Training Institute

© Fortinet Inc. All Rights Reserved.

23

The CMDB resides on the supervisor node.

The CMDB uses a postgres database to store FortiSIEM configuration items, such as device information, credentials, discovery information, rules, reports, and so on.

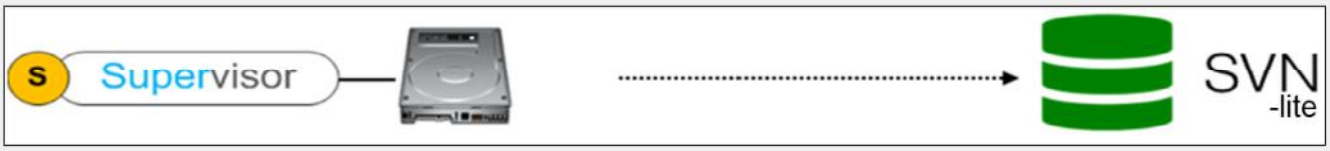
By default, the CMDB also resides on the worker nodes, but is not used.

Vouchers & Dumps are Available | WhatsApp +201224560923

DO NOT REPRINT
© FORTINET
Brave-dumps.com

FortiSIEM Components—SVN-Lite Database

- A lightweight version of subversion(SVN-lite database) resides on the supervisor node



- The SVN-lite database is used for storing current and historical device CLI-based configurations for supported items, such as firewall, router, switch start-up and running configurations, and installed software on servers
- By default, the SVN-lite database also resides on worker nodes, but is not used

NSE Training Institute
© Fortinet Inc. All Rights Reserved.

A lightweight version of subversion (SVN-lite database) resides on the supervisor node.

The SVN-lite database is used for storing current and historical device CLI-based configurations for supported items, such as firewall, router, switch start-up and running configurations, and installed software on servers.

By default, the SVN-lite database also resides on worker nodes, but is not used.

Vouchers & Dumps are Available | WhatsApp +201224560923

DO NOT REPRINT
© FORTINET
Brave-dumps.com

FortiSIEM Components—SQLite Database (Profiling)

- Profile database is not installed on its own disk but is installed on the operating system disk, usually disk 1 on supervisor node



- Small SQLite database is used for profile database
- Profile database is used for storing anomaly baseline data calculated for many parameters, such as traffic and device resource usage profiles, running averages, and standard deviation values

NSE Training Institute

© Fortinet Inc. All Rights Reserved.

25

The profiling database is not on its own disk. Instead, it is installed on the operating system disk, usually disk one on the supervisor node.

A small SQLite database is used as a profile database.

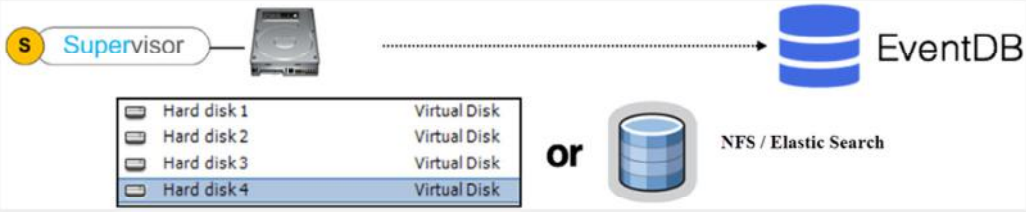
The profile database is used to store anomaly baseline data calculated for many parameters, such as traffic and device resources usage profiles, running averages, and standard deviation values.

Vouchers & Dumps are Available | WhatsApp +201224560923

DO NOT REPRINT
© FORTINET
Brave-dumps.com

FortiSIEM Components—EventDB

- The event database is installed either on a local disk attached to the supervisor node or remote storage, such as NFS mount/Elasticsearch reachable from supervisors and all worker appliances. It is referred to as */data disk*



- The event database is a proprietary no SQL flat file-type database, if NFS or local disk used
- Used to store raw logs and parsed metadata
- Customer defines the size depending on use and length of time for data retention for online searches and analysis

NSE Training Institute

© Fortinet Inc. All Rights Reserved.

26

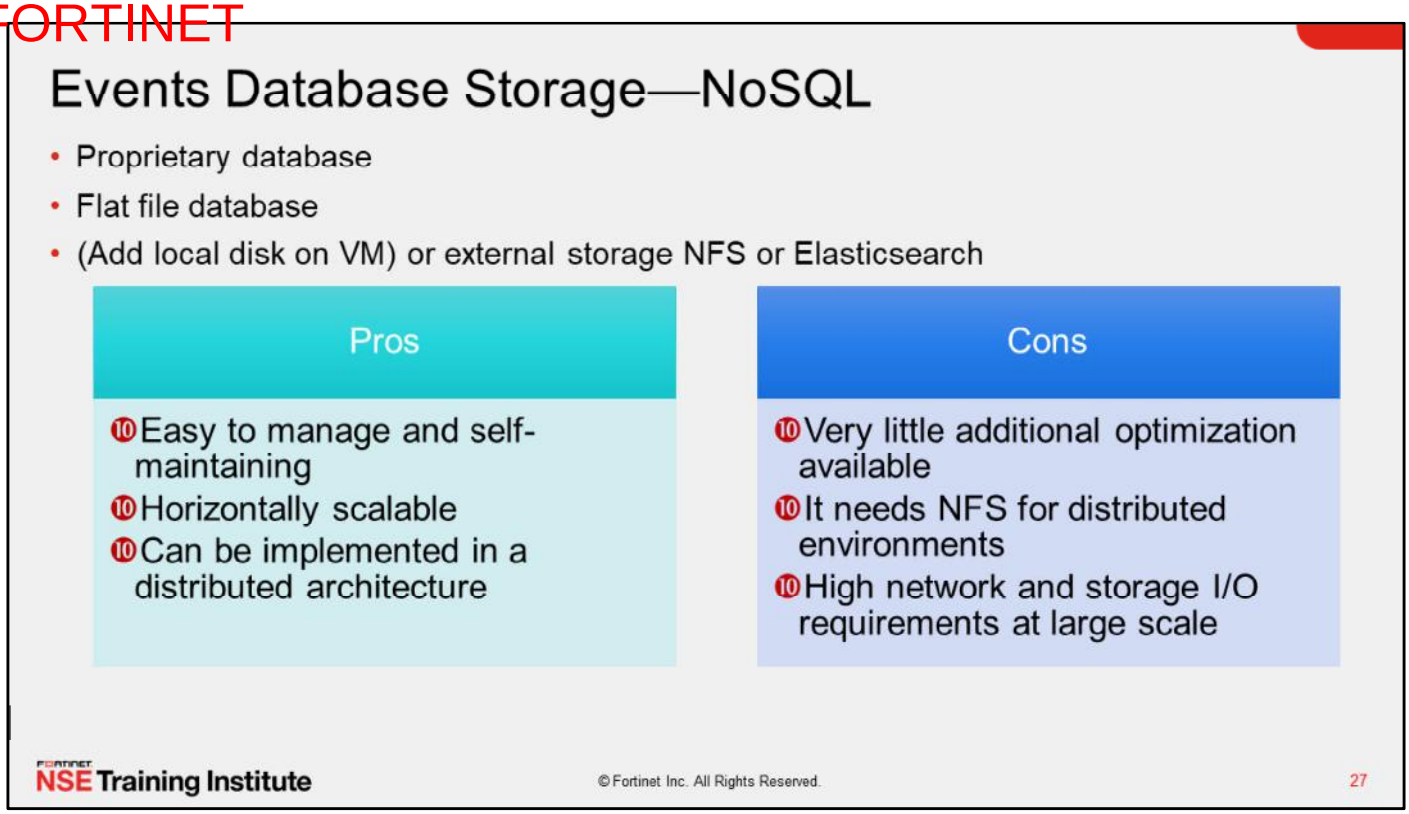
The event database is installed either on a local disk attached to the supervisor node or remote storage, such as NFS mount or Elasticsearch reachable from supervisors and all worker appliances. It is referred to as the */data disk*.

The event database is a proprietary no SQL flat file type database. It is used to store raw logs and parsed metadata. The customer defines the size of the event database. The size depends on usage and the length of time required for data retention for online searches and analysis.

Note that Elasticsearch is not a proprietary database. For more information, refer to the *FortiSIEM - Elasticsearch Storage Guide.*

Vouchers & Dumps are Available | WhatsApp +201224560923

DO NOT REPRINT
© FORTINET
Brave-dumps.com



For scalable event database storage, FortiSIEM provides three options:

- Local disk
- FortiSIEM NoSQL event database with data residing on an NFS server
- Elasticsearch distributed database

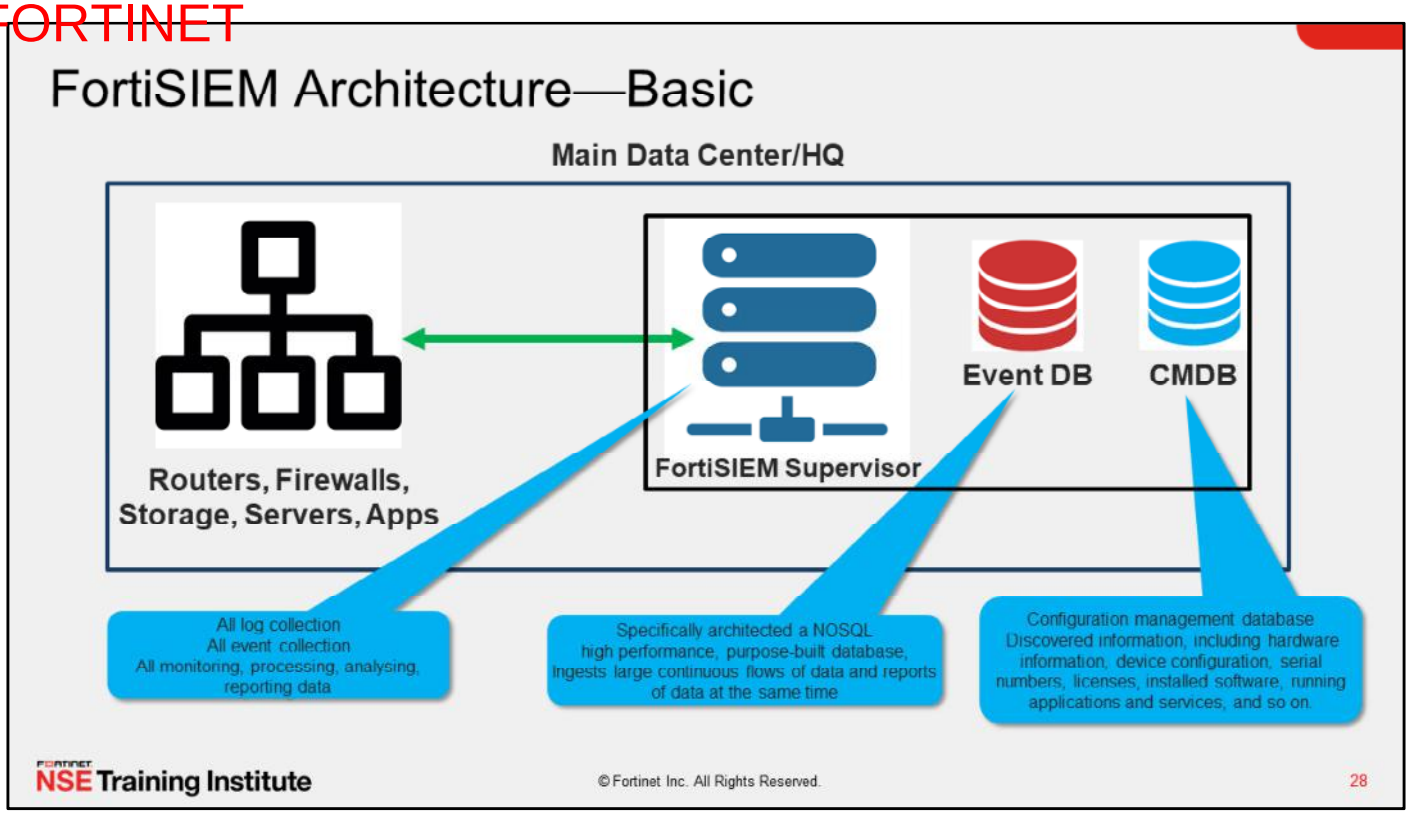
Hardware appliance and all-in-one virtual machine solutions use the Local disk option while a FortiSIEM cluster of supervisors and workers can exploit the No SQL option..
The NoSQL event database option is a purpose-built FortiSIEM proprietary solution. The supervisor and worker nodes create and maintain the database indices.

To scale event insertion and search performance in this mode requires:

- A fast communication network between the supervisor and worker nodes and the NFS server
- High NFS input/output operations per second (IOPS) that can be achieved using fast RAID disk or tiered SSD and magnetic disks

Vouchers & Dumps are Available | WhatsApp +201224560923

DO NOT REPRINT
© FORTINET
Brave-dumps.com



Now you will take a high-level look at a few FortiSIEM architectures, starting with the basic implementation.

The basic implementation of FortiSIEM consists of a single FortiSIEM device—the supervisor—that does all of the log collection, correlation of the events, and monitoring, processing, analyzing, and reporting the data.

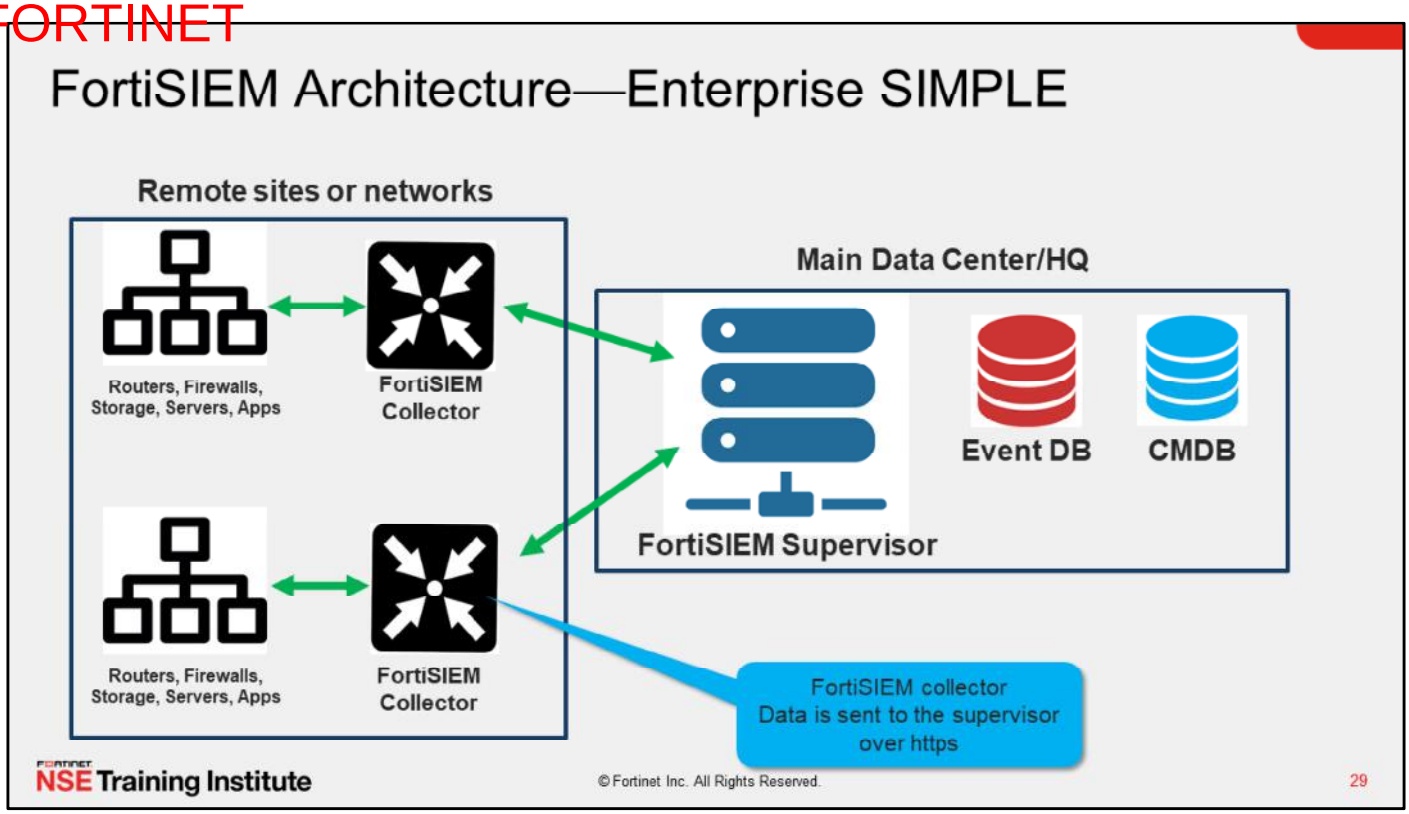
The supervisor contains an event database that is designed specifically as a NoSQL, high-performance database. Its purpose is to ingest large, continuous flows of data while generating reports from the data at the same time. A SQL database can't provide those two things simultaneously.

The supervisor also contains a CMDB as well as a versioning database (SVN-lite) the same type of database that coders use when they check in their code at the end of the programming day. FortiSIEM uses the versioning database to track changes in devices.

The basic architecture is the simplest deployment option for FortiSIEM. It's sufficient for small-to-medium size companies but it is not suitable for larger, enterprise companies.

Vouchers & Dumps are Available | WhatsApp +201224560923

DO NOT REPRINT
© FORTINET
Brave-dumps.com



The basic architecture consists of a single, all-in-one supervisor, which is sufficient for a small local network. However, if you have remote networks, or a segmented network, how do you collect those events? To answer that, take a look at the simple architecture.

For larger deployments, or deployments that have segmented networks, you can scale up FortiSIEM by adding VMs called collectors. Collectors have a lower hardware requirement (CPU and memory) than supervisors or workers. Collectors gather events from the remote or segmented network, including syslog and netflow feeds, and perform push and poll methods for collecting information, such as SNMP or WMI polling. Collectors also perform discoveries of the remote environments themselves.

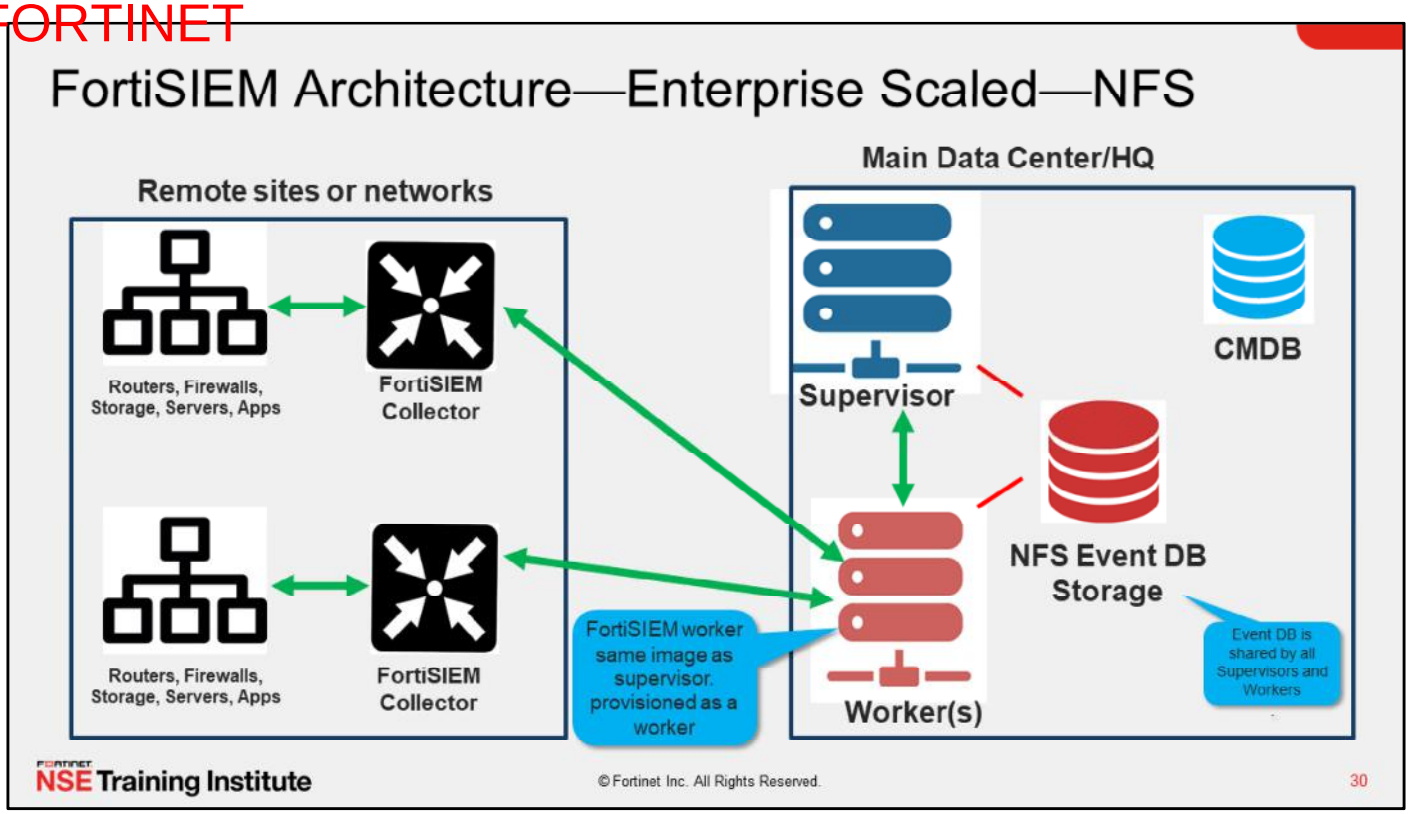
After collecting the data, the collector parses and normalizes the data locally. You will learn about parsing and normalization later in this course. Then, the collector compresses the data and forwards it over an encrypted channel (HTTPS) to the supervisor. This process allows you to deploy a collector in a remote office, and then send the data over the internet to the supervisor at the main office without needing a dedicated line.

Another benefit of using collectors is scalability, because the discovery process and event parsing is offloaded from the supervisor to the collectors. Adding collectors to a single supervisor is referred to as *horizontal scaling*.

Note that when you scale up, depending on the number of events per second and how long you need to keep the events in the events database, you might reach the 2 GB size limit of a virtual disk. If you reach this limit, you must use an NFS system.

Vouchers & Dumps are Available | WhatsApp +201224560923

DO NOT REPRINT
© FORTINET
Brave-dumps.com



As you can see in the scaled architecture shown on this slide, FortiSIEM also allows you to scale up vertically by making copies of the supervisor. The supervisor copies become a cluster, and act as one unit.

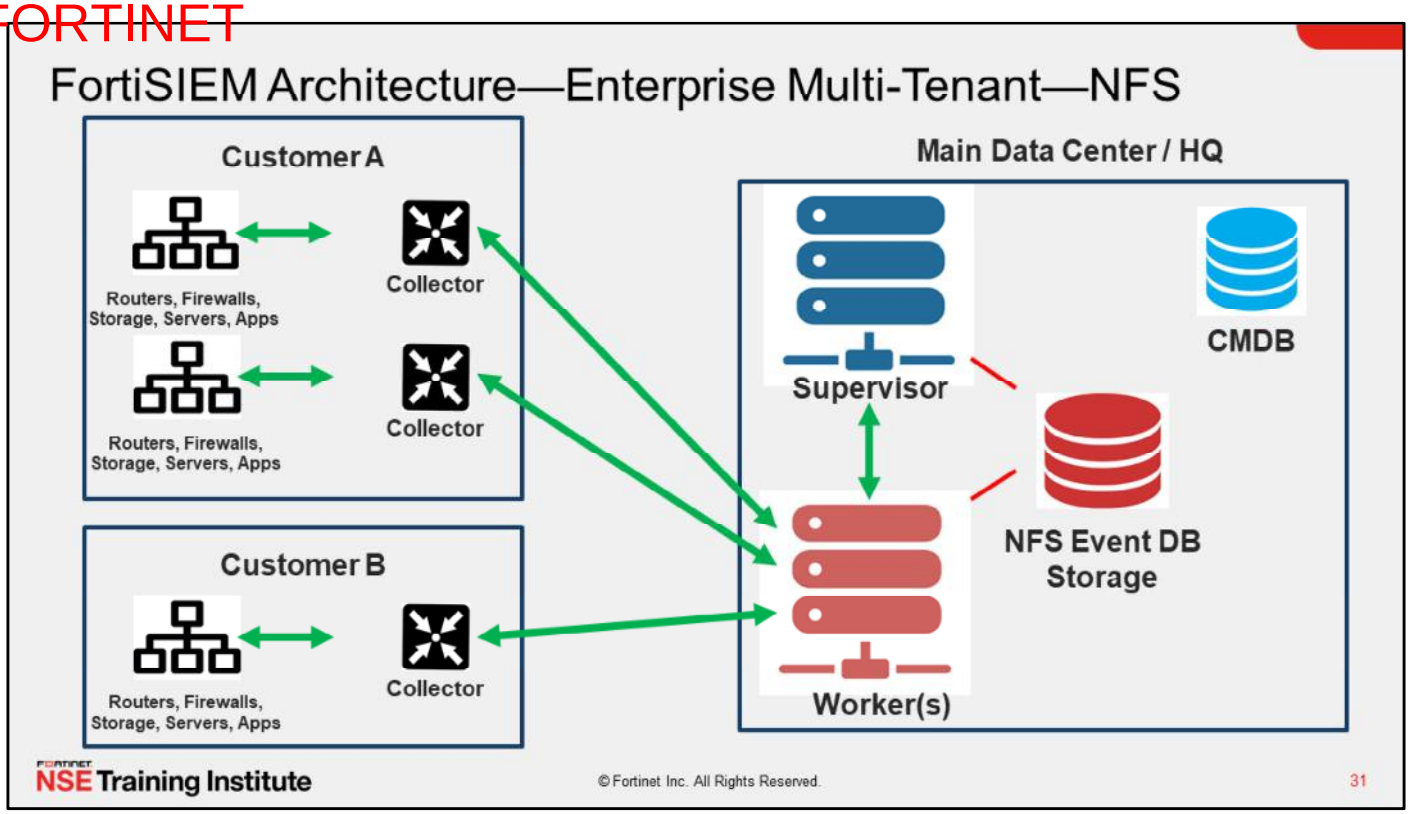
In the scaled model, the event database that previously might have been a virtual disk on the virtual machine, must use NFS storage because all of the machines need to share the database. All of the appliances run a hardened version of CentOS, so NFS storage is a natural way for them to share data.

The worker is a scaled-down version of the supervisor. It's the same virtual appliance image; however, during installation, if a supervisor already exists, the supervisor provisions itself as a worker.

Adding worker nodes increases performance; that is, the speed at which an analytic search returns a report. Performance increases because FortiSIEM distributes the search among the supervisor and all of the workers. When a collector uploads the events to a worker, it doesn't matter from a FortiSIEM architecture point of view, which of the workers receives the events. The rule correlation happens across the entire cluster.

Vouchers & Dumps are Available | WhatsApp +201224560923

DO NOT REPRINT
© FORTINET
Brave-dumps.com



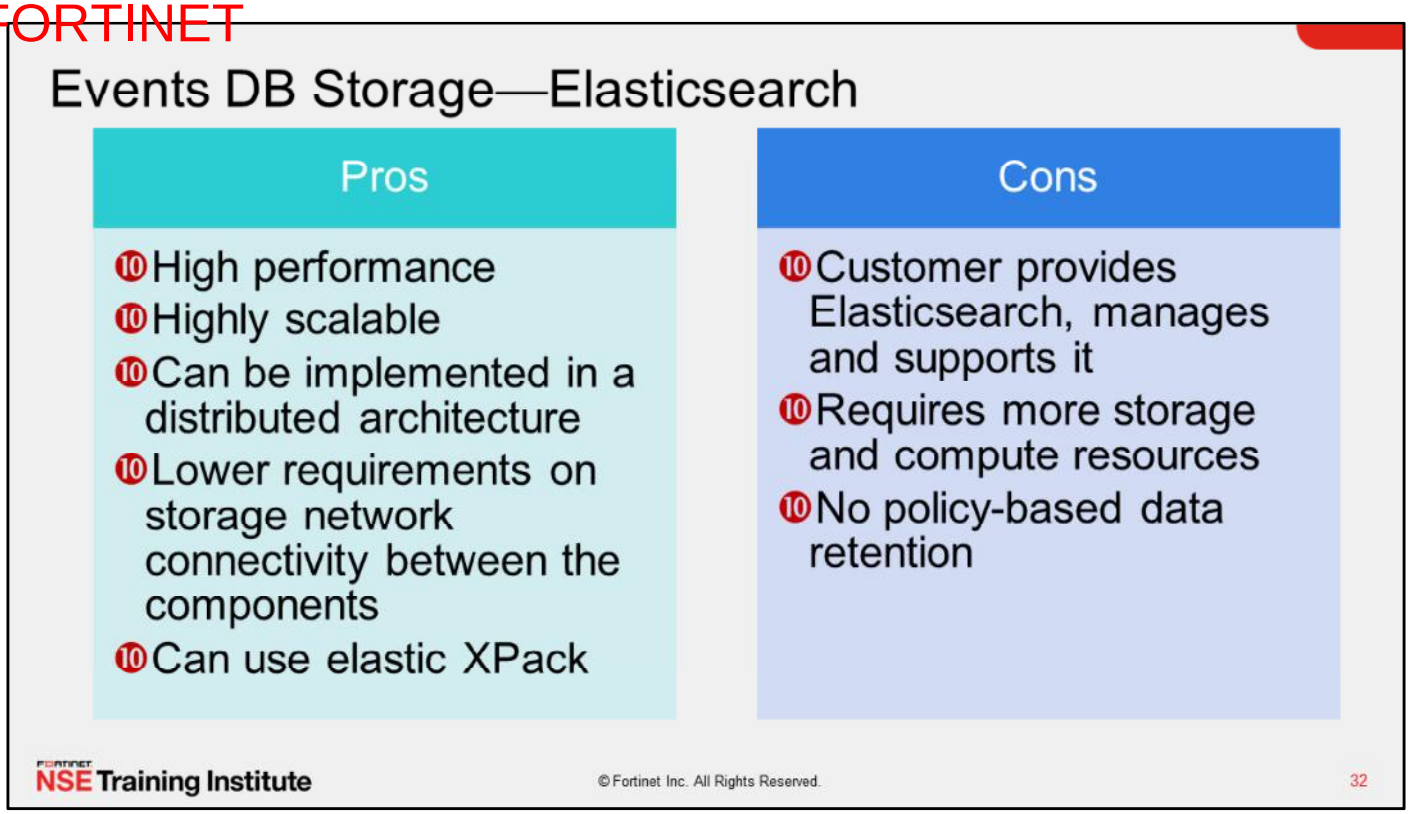
Service providers can use FortiSIEM in a multi-tenant deployment. The architecture is essentially the same as the scaled architecture, but the collectors are deployed in different customer sites. Multi-tenancy allows you to create multiple distinct management environments using a single FortiSIEM installation.

All of the data collected by all of the collectors is stored in one central database, but it's all segmented. The database isolates the settings, policies, and events for each tenant. It's completely secure and meets audit and compliance requirements. You can give tenants access to the FortiSIEM GUI to manage their own assets, such as users, devices, reports, and rules, independently of other tenants. No tenant's events or devices are visible to any other tenant. Each tenant is independent and isolated from every other tenant.

So, as you can see, a FortiSIEM architecture of workers, collectors, and supervisor offers many deployment options for enterprises on any scale, as well as deployment options for managed service providers who need multi-tenant solutions.

Vouchers & Dumps are Available | WhatsApp +201224560923

DO NOT REPRINT
© FORTINET
Brave-dumps.com



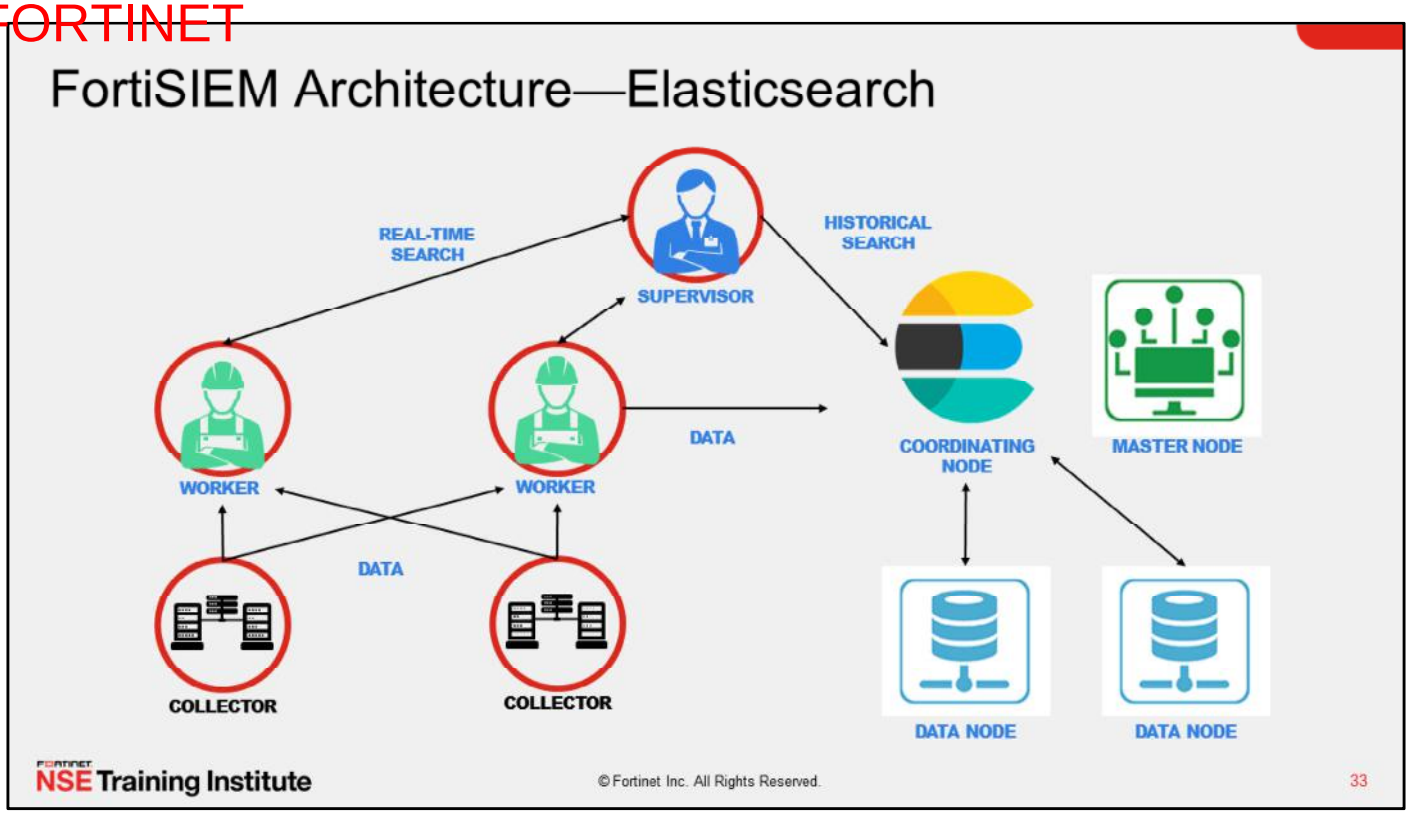
FortiSIEM provides the Elasticsearch database option for storing events.

Elasticsearch provides a true distributed, redundant columnar database option for scale-out database performance at the expense of higher storage needs. In this option, FortiSIEM worker nodes push the data in real time to the Elasticsearch cluster, which maintains the event database. FortiSIEM has developed an intermediate adaptation layer, so that the same GUI can run seamlessly on both Elasticsearch and the FortiSIEM NoSQL event database.

Elasticsearch is a distributed database that provides linearly scalable event insertion speed and query response time improvement.

Vouchers & Dumps are Available | WhatsApp +201224560923

DO NOT REPRINT
© FORTINET
Brave-dumps.com



This slide shows a full cluster deployment architecture with Elasticsearch.

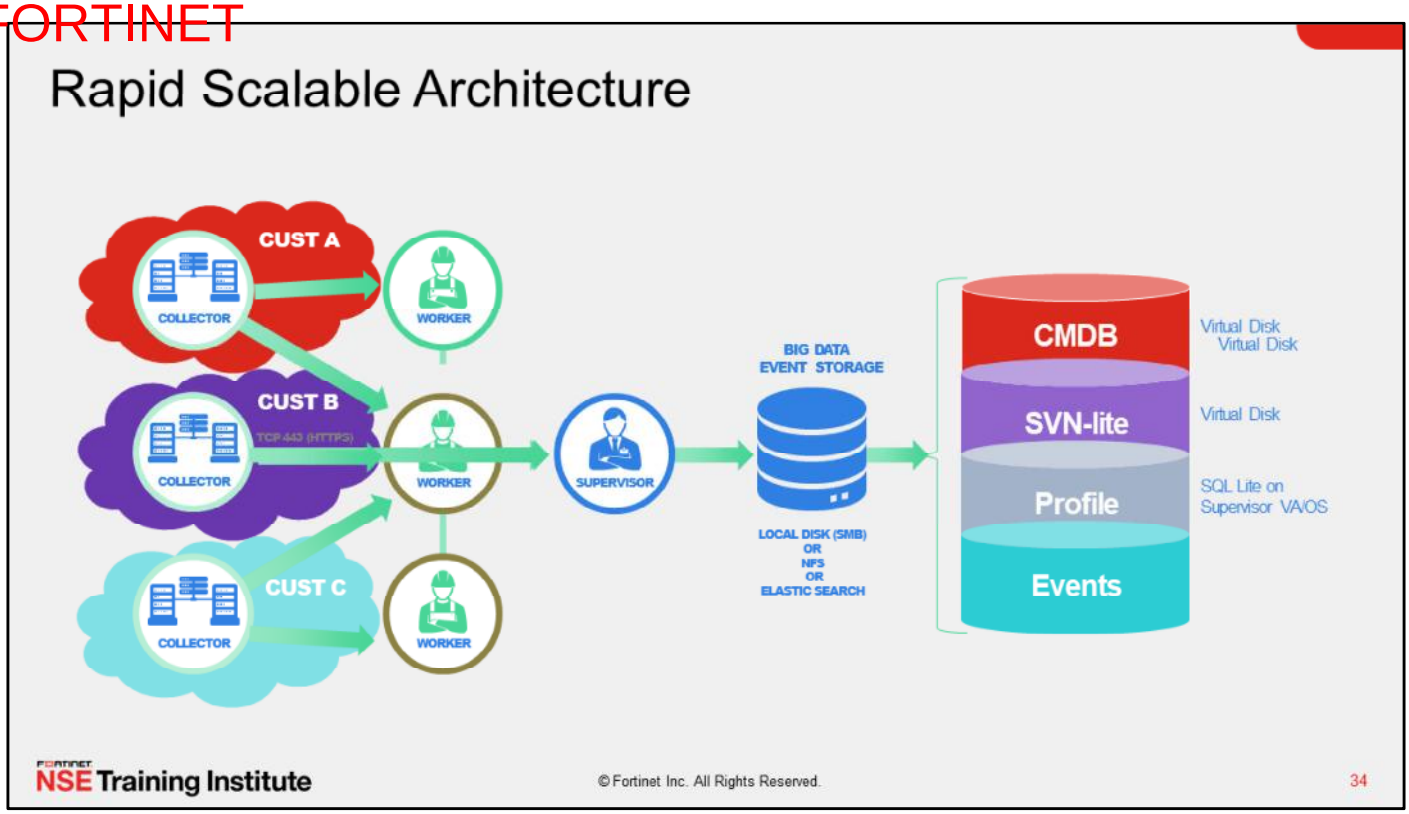
Elasticsearch is a distributed database. You can deploy it as an all-in-one node, but more commonly you deploy it in a cluster setup consisting of a master node, coordinating node, and data nodes.

FortiSIEM can work with both Elasticsearch configurations:
- All-in-one node
- Cluster

In a full cluster deployment architecture, the supervisor and worker nodes perform the real-time operations (collection, rules and inline reports) while the data is indexed and stored in Elasticsearch. Historical search queries are sent from the supervisor node to the coordinating node, which communicates with the data nodes to produce search results.

Vouchers & Dumps are Available | WhatsApp +201224560923

DO NOT REPRINT
© FORTINET
Brave-dumps.com



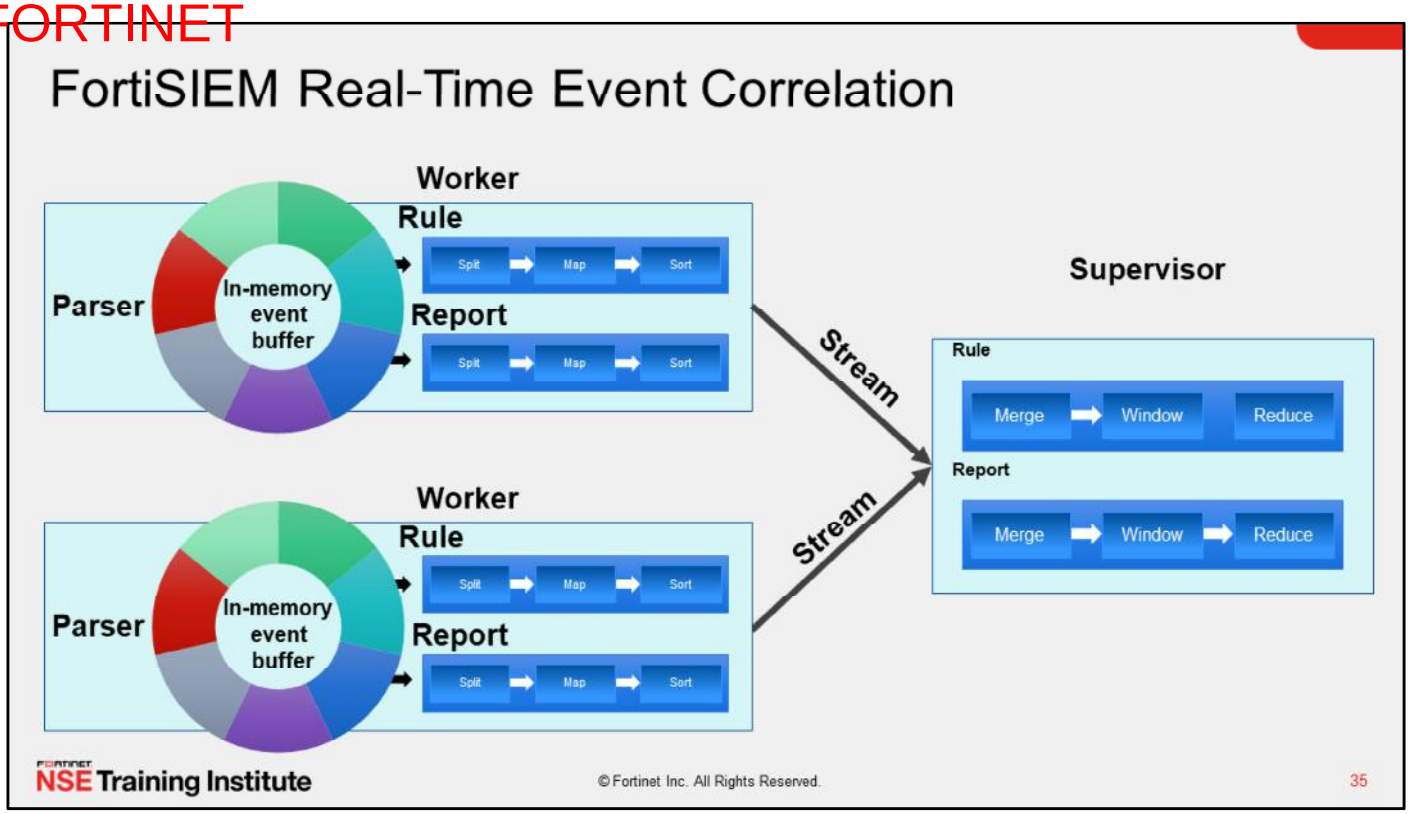
FortiSIEM has a highly-scalable architecture.

Collectors are typically deployed close to the log sources, and then they forward logs to workers.

The number of workers required is proportional to the networks events per second (EPS) rate.

Vouchers & Dumps are Available | WhatsApp +201224560923

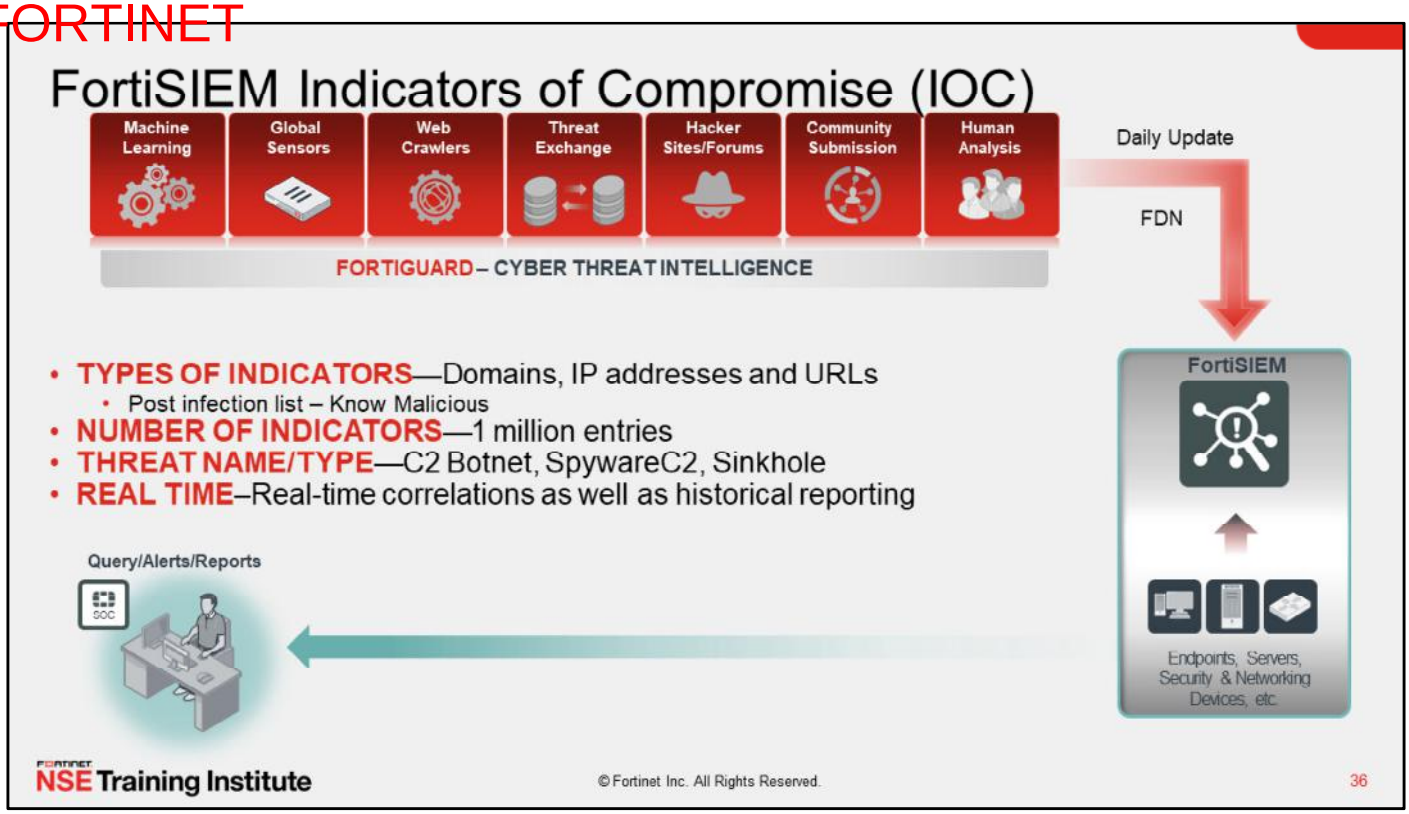
DO NOT REPRINT
© FORTINET
Brave-dumps.com



FortiSIEM is the only vendor that has a distributed real-time, event correlation engine. This means that as events come in, the worker that received the event runs it through its correlation engine. However, an individual worker may not have all of the information to trigger a rule, especially if the rule is complex. Instead, the worker looks for partial rule matches. When the worker finds a partial match, it sends the information to the supervisor. The supervisor then combines the partial matches from all the workers and ultimately generates an incident. This process occurs in memory, in streaming mode, without ever touching a disk, which greatly increases speed and efficiency.

Vouchers & Dumps are Available | WhatsApp +201224560923

DO NOT REPRINT
© FORTINET
Brave-dumps.com

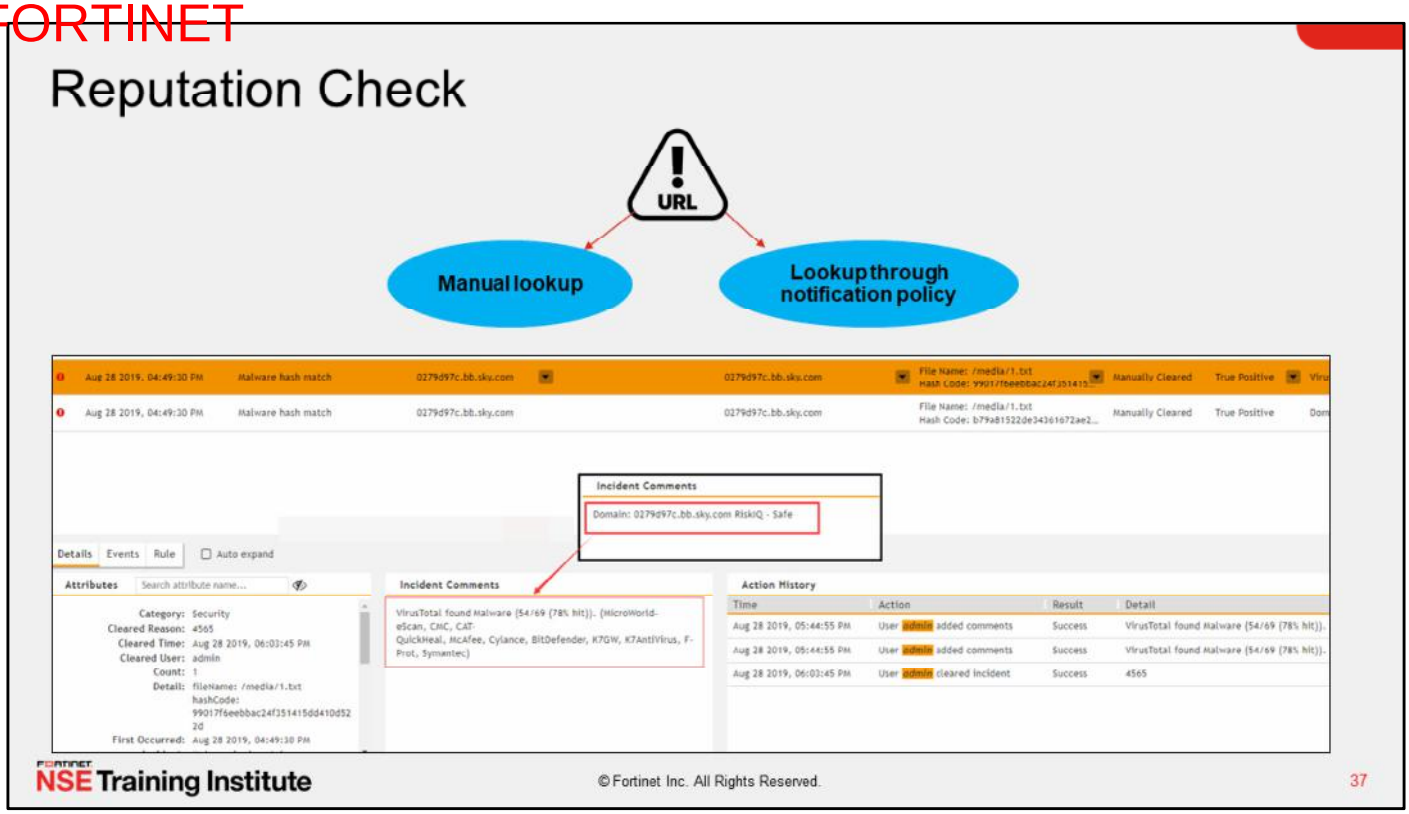


FortiGuard Labs has been around for more than 16 years and is the main force that drives Fortinet's threat intelligence. FortiGuard Labs collects threat information in a variety of ways, including:

- Machine learning: It uses machine learning techniques, to capture IOCs, such as bad IP addresses, domains and URLs.
- Global sensors: There are three million sensors deployed around the world, consisting of customer devices and honeypots. These sensors provide an early warning to what is happening in cyber space globally.
- Web crawlers: Proprietary web crawlers with the use of artificial intelligence will crawl the internet looking for malicious sites.
- Threat exchange: There are more than 200 threat sharing agreements with governments, certification authorities, and strategic vendors around the globe.
- Hacker sites/forums: It trolls the underground to uncover new threat events.
- Community submissions: Customer submission of new threats to analyze either manually or through the Fortinet cloud sandbox technology. Fortinet also executes approximately 500,000 malware samples daily to extract IOCs.
- Human analysis: FortiGuard Labs likes to rely on automation as much as possible; however, you also need expert human analysis. More than 200 analysts are trying to solve various threat problems around the world.
- FortiSIEM IOC service: A set of indicators that FortiGuard Labs packages daily, and deliver through the FDN network to the FortiSIEM technology. Rules on the FortiSIEM are configured to alert and flag in the watch lists indicators that show up in the logs your devices produce. An alert usually means that a device in your network contains a threat, and should be investigated.
- FortiSIEM IOC package: Each day, the existing package is removed from FortiSIEM and a new one, containing an updated list of indicators (bad domains, IP addresses, and URLs), is added.

Vouchers & Dumps are Available | WhatsApp +201224560923

DO NOT REPRINT
© FORTINET
Brave-dumps.com



FortiGuard IOC provides reputation checks for different malware like IP, domain, URL, and hash. Reputation checks can be invoked in two ways:

- When an incident triggers, users can manually do a lookup through FortiGuard IOC, virus total, or RiskIQ. Any external website can also be looked up, but the results of FortiGuard IOC, VirusTotal or RiskIQ are parsed and the user is provided with a simplified verdict (safe, unsure, or malicious based on thresholds).
- Users can automate reputation checks by including it in their incident notification policies. When included, the reputation check will automatically be done when an incident triggers. Incident comments are updated with the results.

Every licensed FortiSIEM can do FortiGuard IOC lookup. No special configuration is required.

Vouchers & Dumps are Available | WhatsApp +201224560923

DO NOT REPRINT
© FORTINET
Brave-dumps.com

Knowledge Check

1. A FortiSIEM supervisor at headquarters is struggling to keep up with an increase of EPS being reported across the enterprise. Which component should an administrator consider deploying to assist the supervisor with processing data?
   - A. Supervisor
   - ✓ B. Worker

2. Which database stores the running configuration for devices?
   - A. CMDB
   - ✓ B. SVN-lite DB

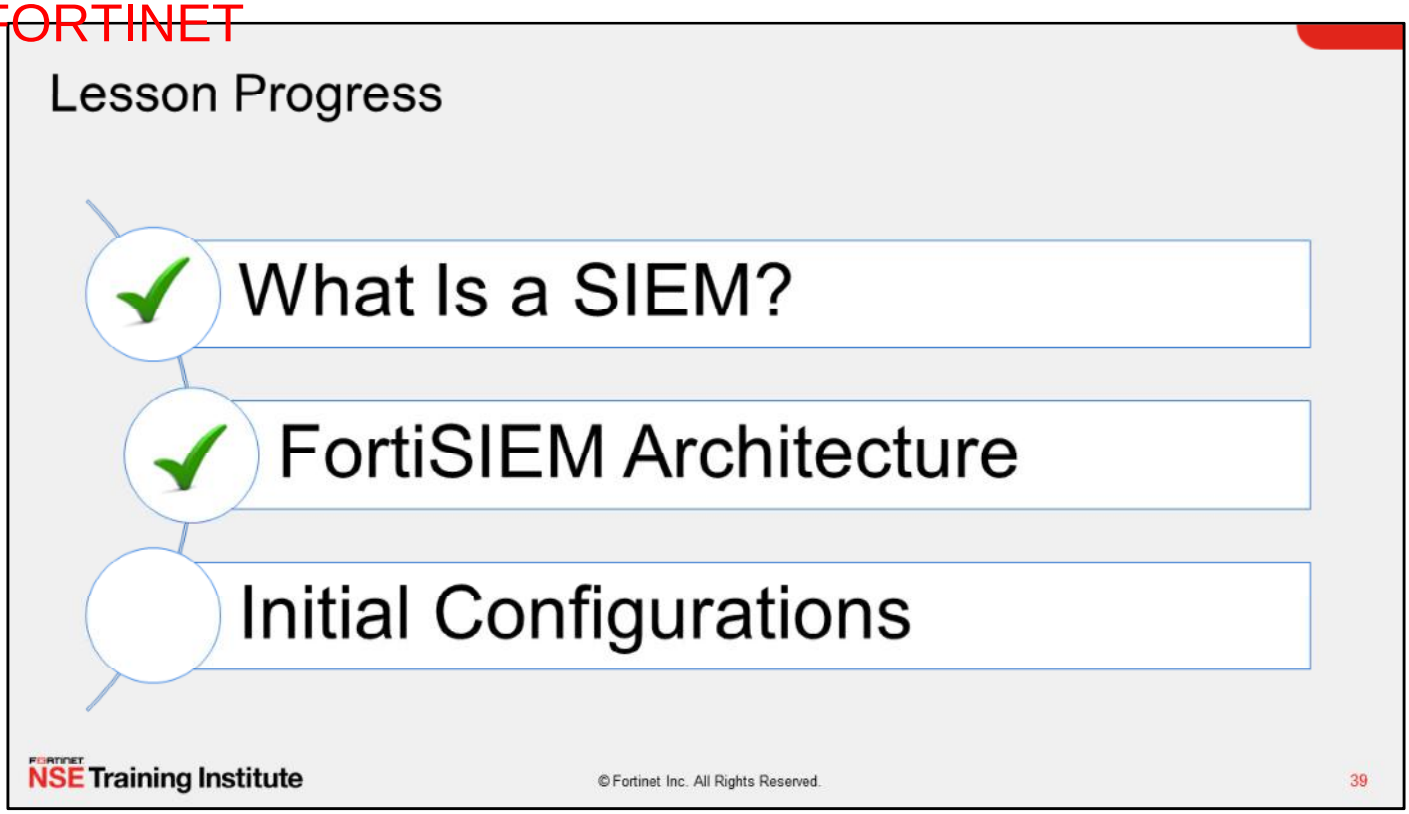
NSE Training Institute

© Fortinet Inc. All Rights Reserved.

38

Vouchers & Dumps are Available | WhatsApp +201224560923

DO NOT REPRINT
© FORTINET
Brave-dumps.com

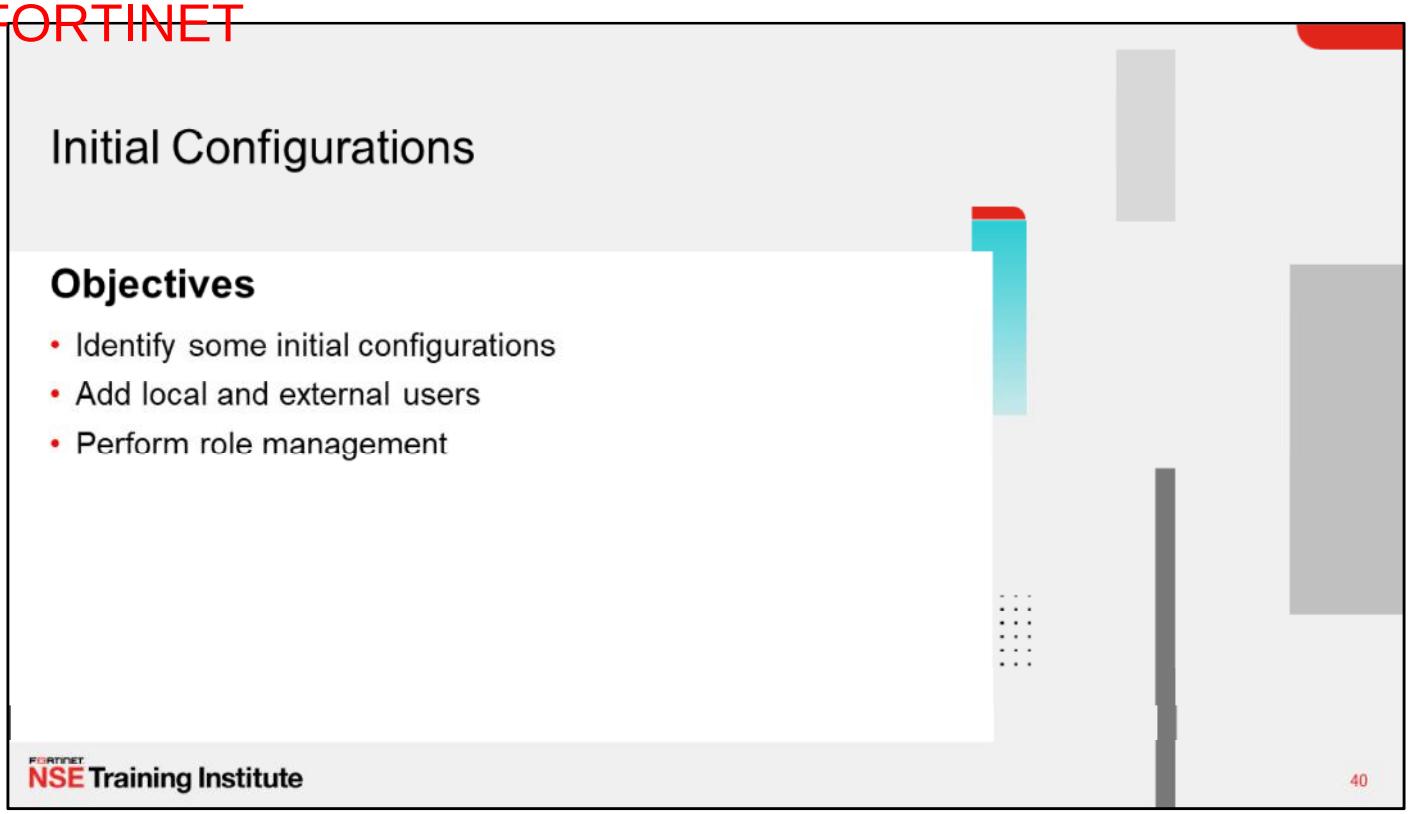


Good job! You now understand the FortiSIEM architecture.

Now, you'll learn about FortiSIEM initial configurations.

Vouchers & Dumps are Available | WhatsApp +201224560923

DO NOT REPRINT
© FORTINET
Brave-dumps.com



After completing this section, you should be able achieve the objectives shown on this slide.

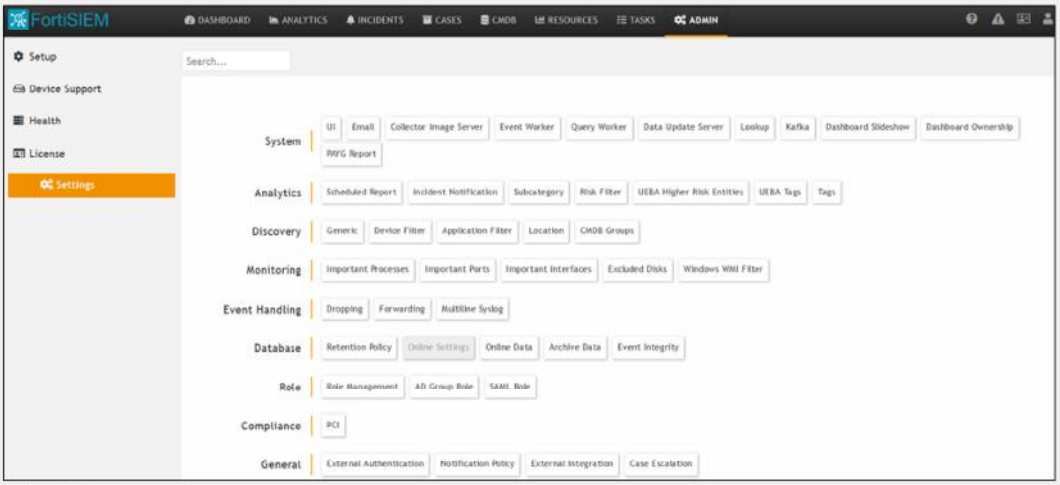
By demonstrating competence understanding and performing initial configurations, you will be prepared to install and configure a FortiSIEM in your network.

Vouchers & Dumps are Available | WhatsApp +201224560923

DO NOT REPRINT
© FORTINET
Brave-dumps.com

Initial System Configuration

- Email gateway
- Custom roles
- Administrators
- Optional
  - SNMP traps for incident notifications
  - Integration configuration for external ticketing systems



NSE Training Institute

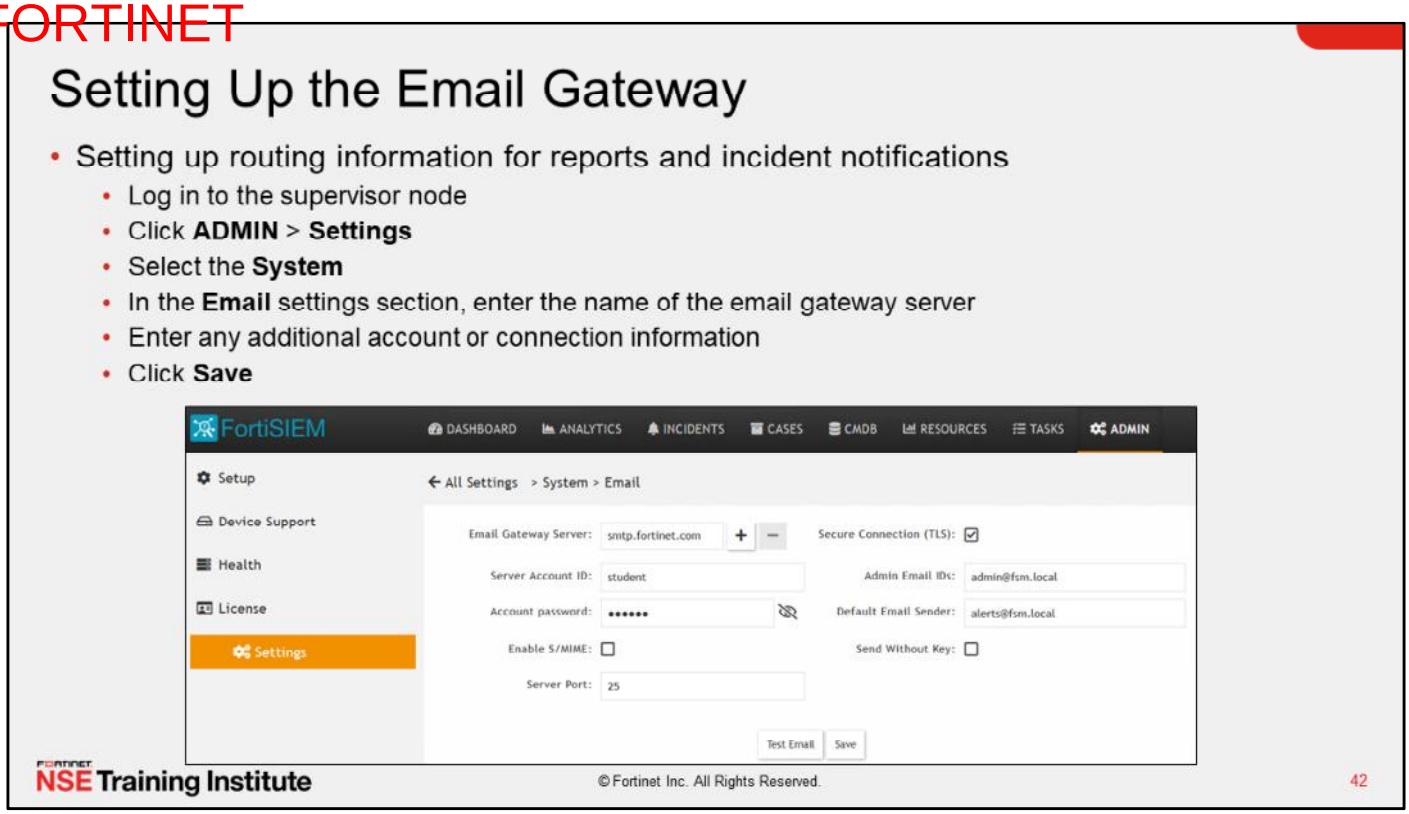
© Fortinet Inc. All Rights Reserved.

41

After you install FortiSIEM, you must configure some system settings. The list of system settings discussed in this lesson is not complete. You can configure these system settings at any time.

Vouchers & Dumps are Available | WhatsApp +201224560923

DO NOT REPRINT
© FORTINET
Brave-dumps.com



FortiSIEM can send out notifications by email when it runs a scheduled report or it meets a predefined set of conditions. FortiSIEM can also automate the sending of tickets to a remedy system, when an incident occurs.

Before you can set up notifications, you must set up the email gateway that your system uses for all notifications.

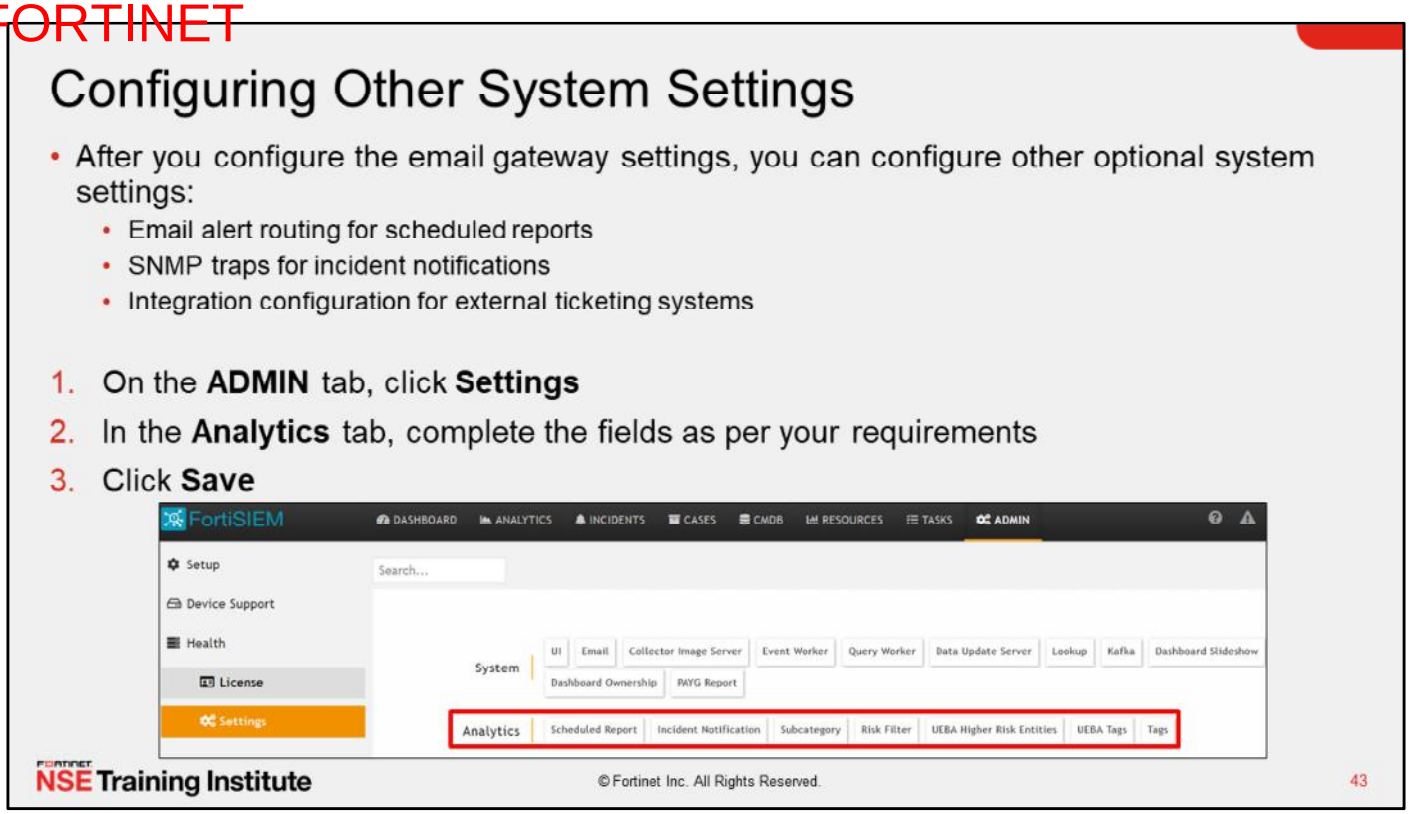
To set up an email gateway for notifications

1. Log in to the supervisor node.
2. Click **ADMIN** > **Settings**.
3. Click the **System** tab.
4. In the **Email Gateway Server field**, section, enter the name of the email gateway server.
5. Enter any additional account or connection information.
6. Click **Save**.

After you configure the email gateway settings, you can configure the other items that use the email gateway.

Vouchers & Dumps are Available | WhatsApp +201224560923

DO NOT REPRINT
© FORTINET
Brave-dumps.com



After you configure the email gateway settings, you can configure email alert routing for scheduled reports.

You can configure FortiSIEM to send a standard email notification to specific people when it runs scheduled reports.

To configure email alert routing for scheduled reports

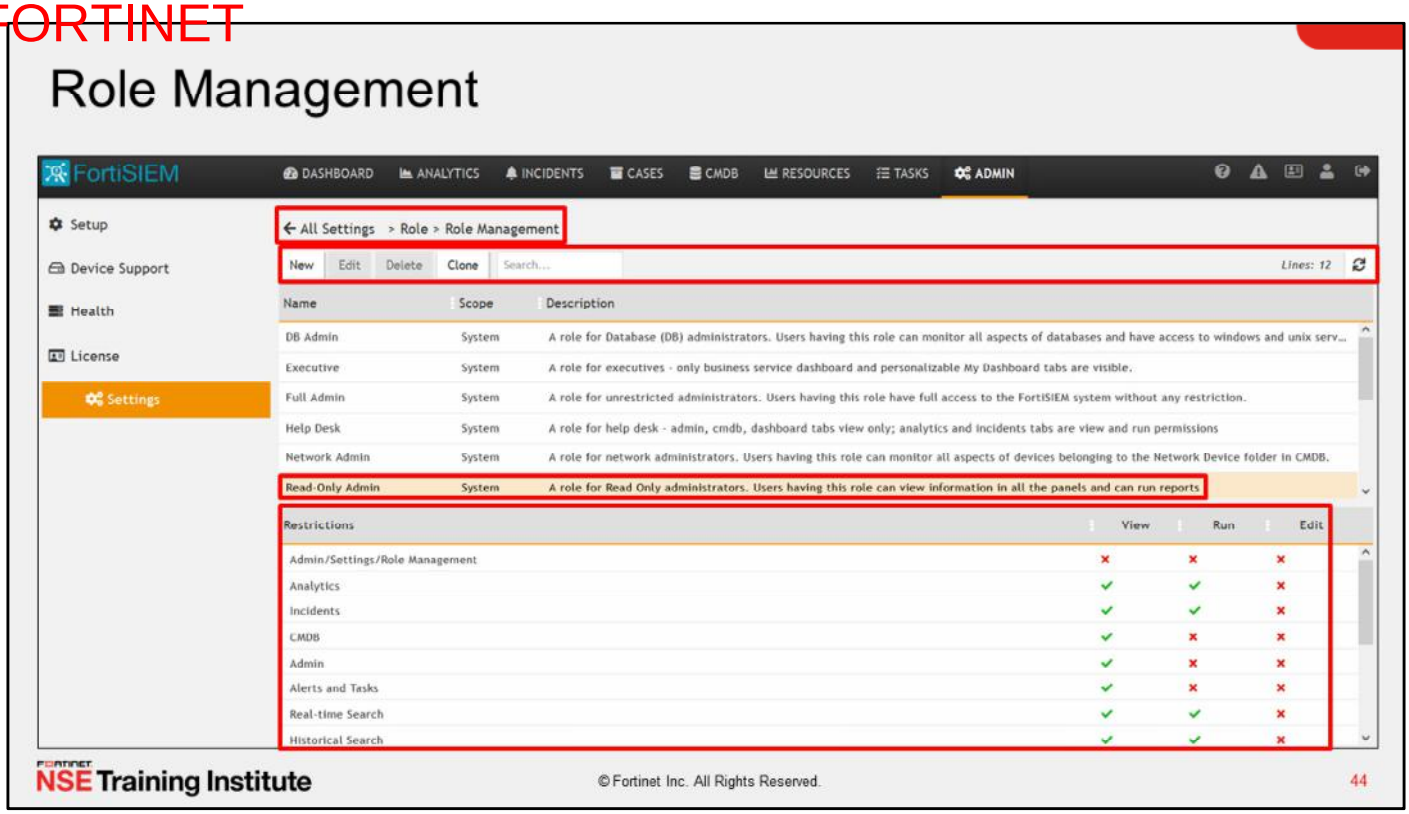
1. On the **ADMIN** tab, click **Settings**.
2. Click the **Analytics** tab.
3. Complete the fields according to your requirements.
4. Click **Save**.

On the **Analytics** tab, you can also set up the following:

- **SNMP traps for incident notifications**: Define SNMP traps that are notified when an event triggers an incident.
- **XML message routing for incident notifications**: Configure FortiSIEM to send an XML message using HTTPS when an incident is triggered by a rule.
- **Routing for Remedy tickets:** Set up remedy routing to accept notifications from FortiSIEM and generate tickets from those notifications, as described in the *FortiSIEM User Guide*. These instructions explain how to set up routing to your remedy server.

Vouchers & Dumps are Available | WhatsApp +201224560923

DO NOT REPRINT
© FORTINET
Brave-dumps.com



FortiSIEM provides a comprehensive role-based management feature. This feature allows you to control what data a user can access on the GUI, and what options on the GUI tabs a user can view.

- What if you want to give an auditor access to logs from a particular server?
- What if a user needs access to only specific parts of the GUI, such as reports?

Role-based management allows you to:

- Give an auditor access to logs from a specific server or group of servers in your FortiSIEM system
- Give a user access to only specific parts of the GUI
- Remove the **ADMIN** tab from specific users to prevent them from making changes on the tab
- Make the GUI read-only for other types of users

By default, FortiSIEM comes with 12 roles. You can also create as many custom roles as you need. To create a new role, click **New**, and then select the access rights and conditions for the role. Alternatively, you can edit an existing role.

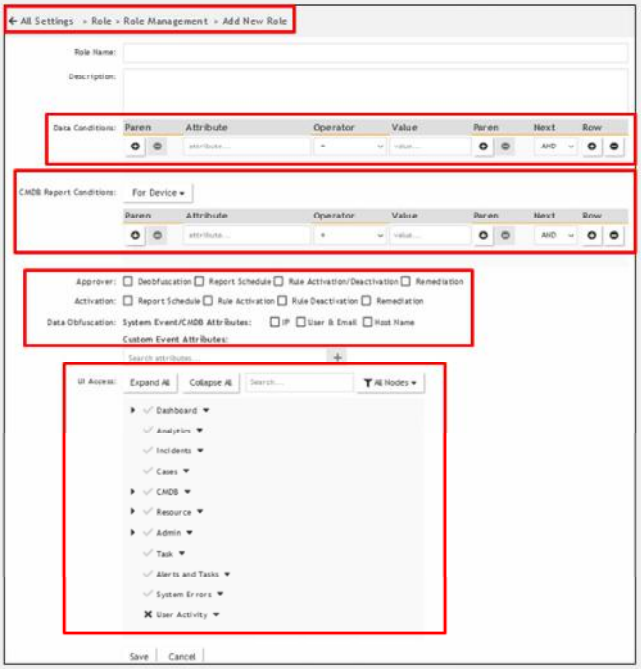
If you need several roles that have similar rights and conditions, create the first role, clone it, and then edit the cloned role. That way, you won't have to start from scratch to create each successive role.

Vouchers & Dumps are Available | WhatsApp +201224560923

DO NOT REPRINT
© FORTINET
Brave-dumps.com

Role Management Options

- You can restrict FortiSIEM roles based on:
  - Data conditions
  - CMDB report conditions
  - GDPR data obfuscation
  - GUI access restrictions



NSE Training Institute

© Fortinet Inc. All Rights Reserved.

45

You can restrict FortiSIEM roles based on four criteria:

- Data conditions
- CMDB report conditions
- GDPR data obfuscation
- GUI access restrictions

Vouchers & Dumps are Available | WhatsApp +201224560923

DO NOT REPRINT
© FORTINET
Brave-dumps.com

Roles—Data Conditions

- Data conditions and CMDB reporting apply to real-time and historical searches, as well as report and dashboard output



- You can base conditions on IP or device selection from the CMDB



NSE Training Institute

© Fortinet Inc. All Rights Reserved.

46

You can use data conditions and CMDB reporting to allow a role to retrieve only specific data from the database and display it to the user.

For example, you can allow users with this role to see data from only a particular device, from a category of devices, or from devices on a particular network segment.

The data conditions apply to real-time and historical searches as well as report and dashboard output. You can base the conditions on IP or device selection from the CMDB.

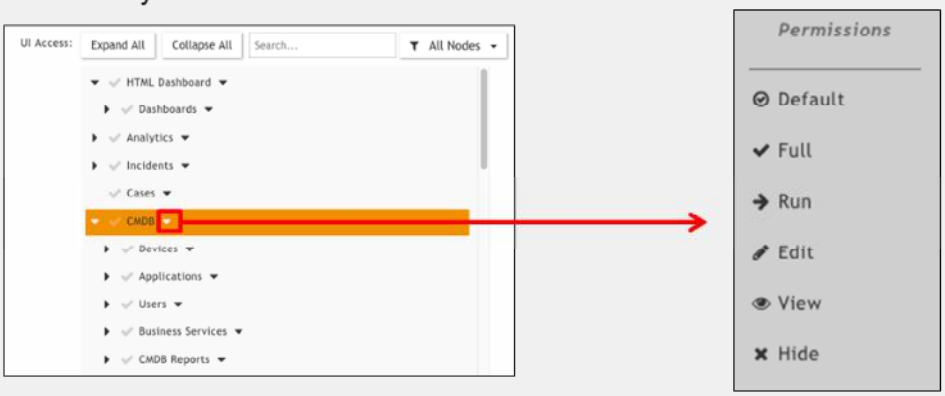
So, if two different users, each having a different role, ran the same report, they would each see different sets of incidents from the other user.

Vouchers & Dumps are Available | WhatsApp +201224560923

DO NOT REPRINT
© FORTINET
Brave-dumps.com

Roles—GUI Access

- Specifies which GUI features are available to a particular user, and which are hidden, viewable, or read-only



- Possible to specify at the device level. For example:
  - Server administrators see only servers in the CMDB
  - Only network administrators see device configurations

NSE Training Institute
© Fortinet Inc. All Rights Reserved.
47

The GUI access option allows you to:
- Hide certain parts of the GUI from users who have a specific role
- Specify which GUI features are available to a particular user and which are hidden, viewable, or read-only

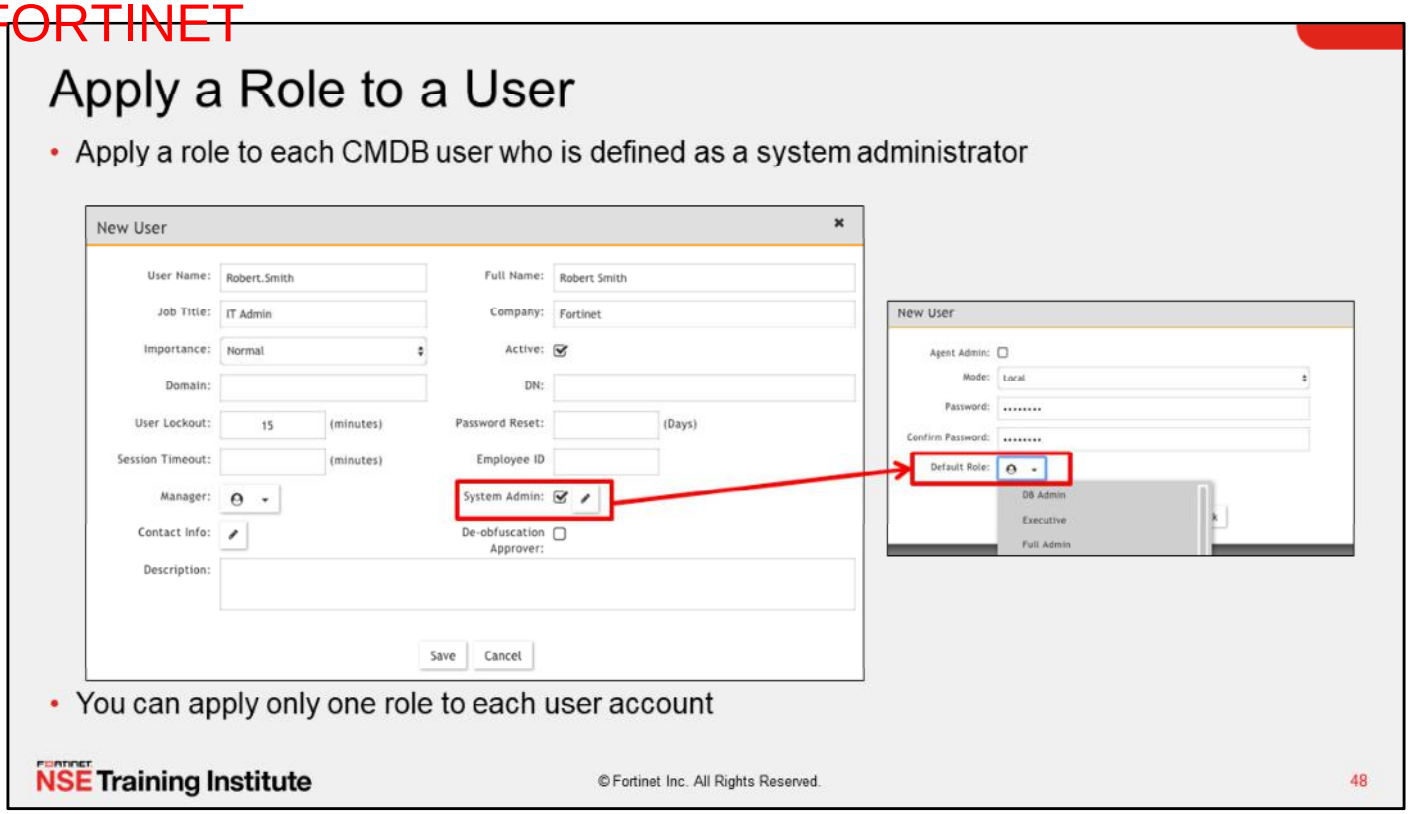
For example, you can set the **Dashboard** tab, **Analytics** tab, **Incident** tab, or **Admin** tab to be read-only for a user or be completely hidden from a user.

You can configure access at the level of individual devices in the CMDB. For example, you can specify that a server administrator can see only servers in the CMDB. That user wouldn't be able to see any network devices, such as firewalls or switches.

Additionally, if you've discovered configurations on your network devices, you can configure a role that would allow only network administrators to see those device configurations while hiding them from all other users.

Vouchers & Dumps are Available | WhatsApp +201224560923

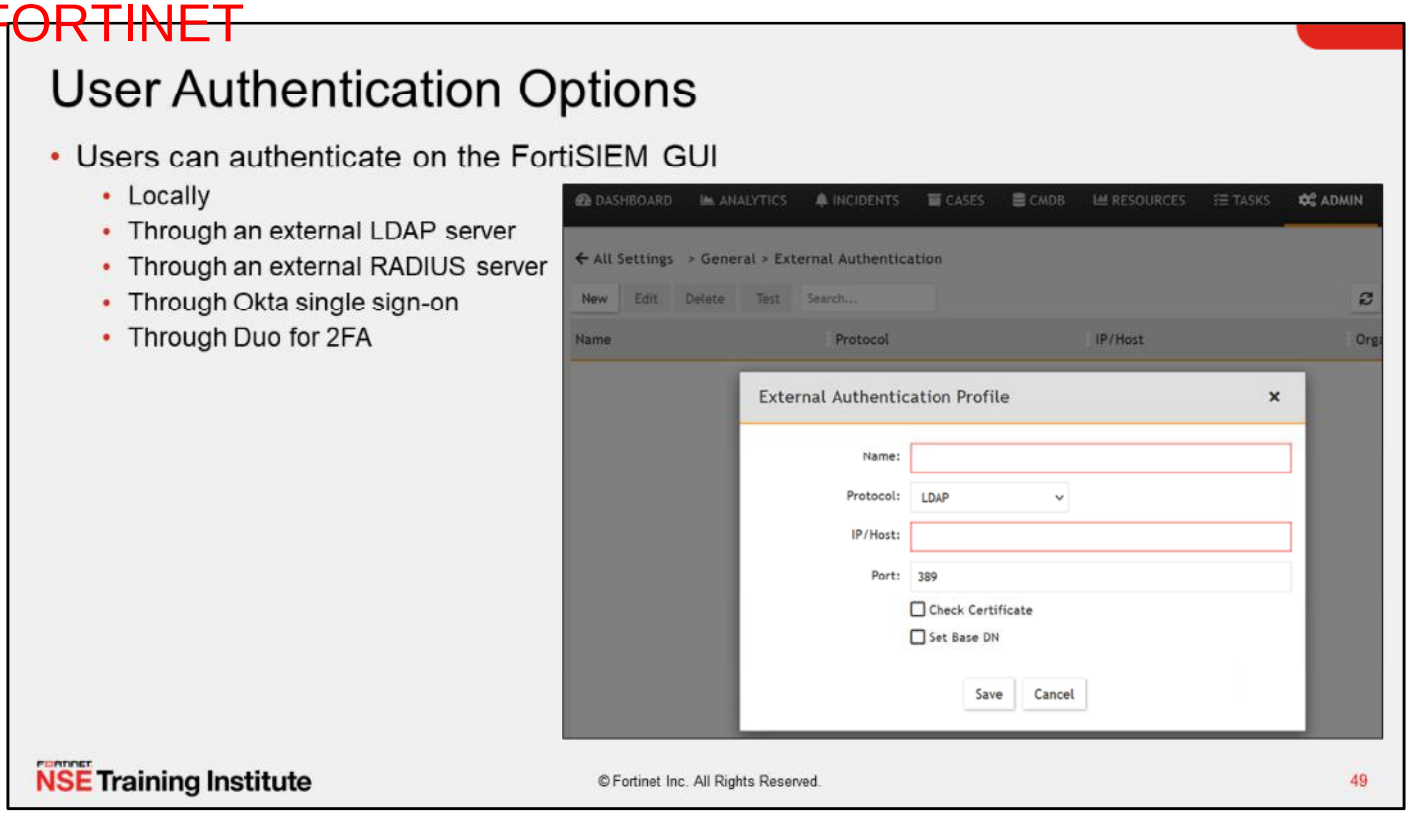
DO NOT REPRINT
© FORTINET
Brave-dumps.com



You must assign a role to any user who is defined as being a system administrator. You can apply only one role to each user.

Vouchers & Dumps are Available | WhatsApp +201224560923

DO NOT REPRINT
© FORTINET
Brave-dumps.com



A user can use two different types of accounts to authenticate on the FortiSIEM GUI: a local user account or an external user account.

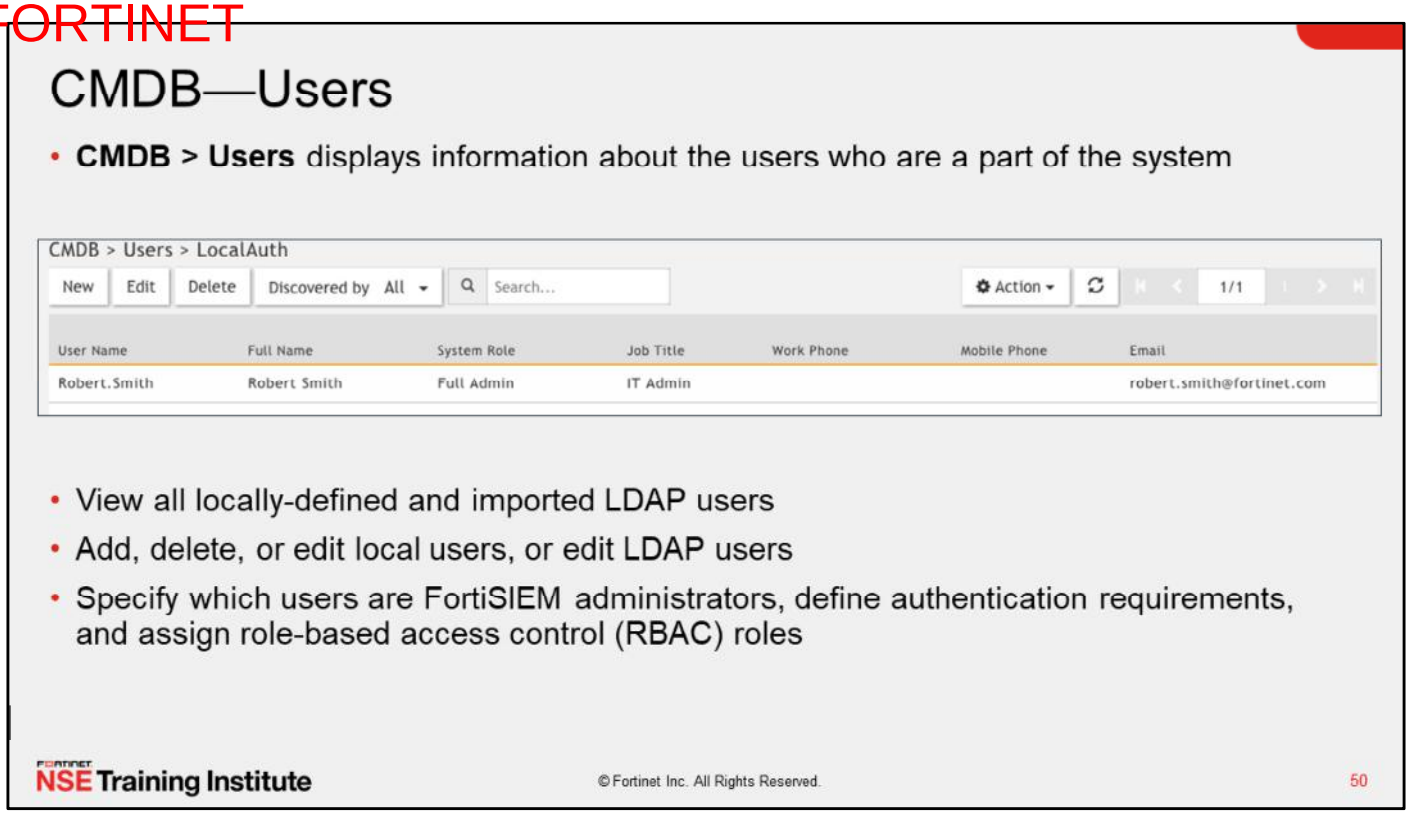
You can create a local user account using the FortiSIEM GUI. In which case, the user's login credentials, including password, are stored in the local CMDB database.

In the case of external user accounts, the user's login credentials come from an external source. The source can be an LDAP server (such as Active Directory) or a RADIUS server.

FortiSIEM also supports Okta single sign-on, and duo for two-factor authentication.

Vouchers & Dumps are Available | WhatsApp +201224560923

DO NOT REPRINT
© FORTINET
Brave-dumps.com

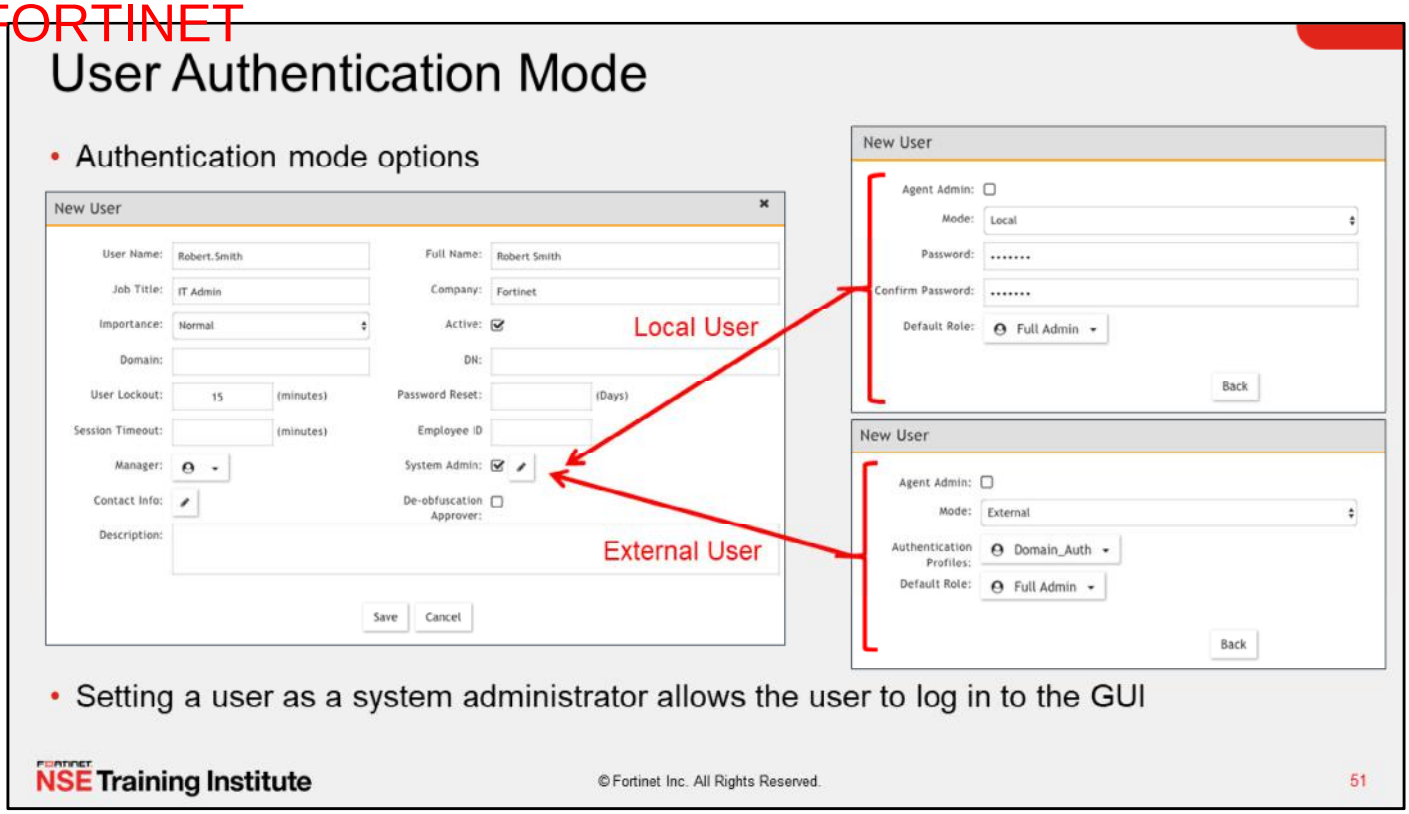


To view users who are known to FortiSIEM (local or external), select the **CMDB** tab, and then, in the left pane, select **Users**.

On the **Users** screen, you can:
- View all locally-defined users, and any users you imported from an external source, such as an LDAP server
- Add, delete, or edit local users, or edit LDAP users
- Specify which users are FortiSIEM administrators, define their authentication requirements, and assign RBAC roles to them

Vouchers & Dumps are Available | WhatsApp +201224560923

DO NOT REPRINT
© FORTINET
Brave-dumps.com



Setting a user as a system administrator allows the user to log in to the FortiSIEM GUI.

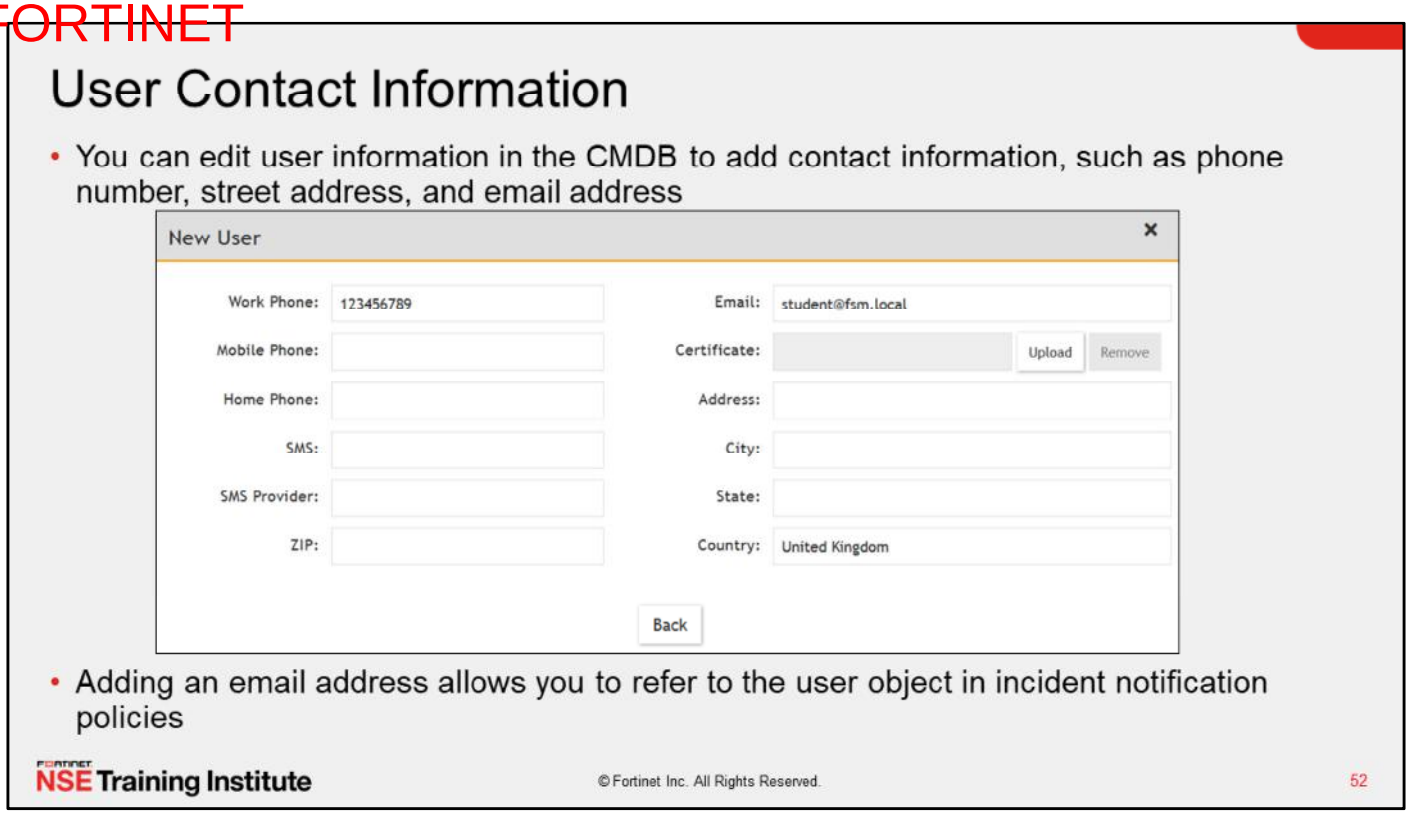
When you set a user as a system administrator by selecting the **System Admin** option, the authentication mode options dialog opens.

For local users, you must enter and confirm a password, as well as assign the user a role.

For external users, in the **Authentication Profiles** drop-down list, select the external device where the user's profile is stored. As well, you must assign the external user a role.

Vouchers & Dumps are Available | WhatsApp +201224560923

DO NOT REPRINT
© FORTINET
Brave-dumps.com

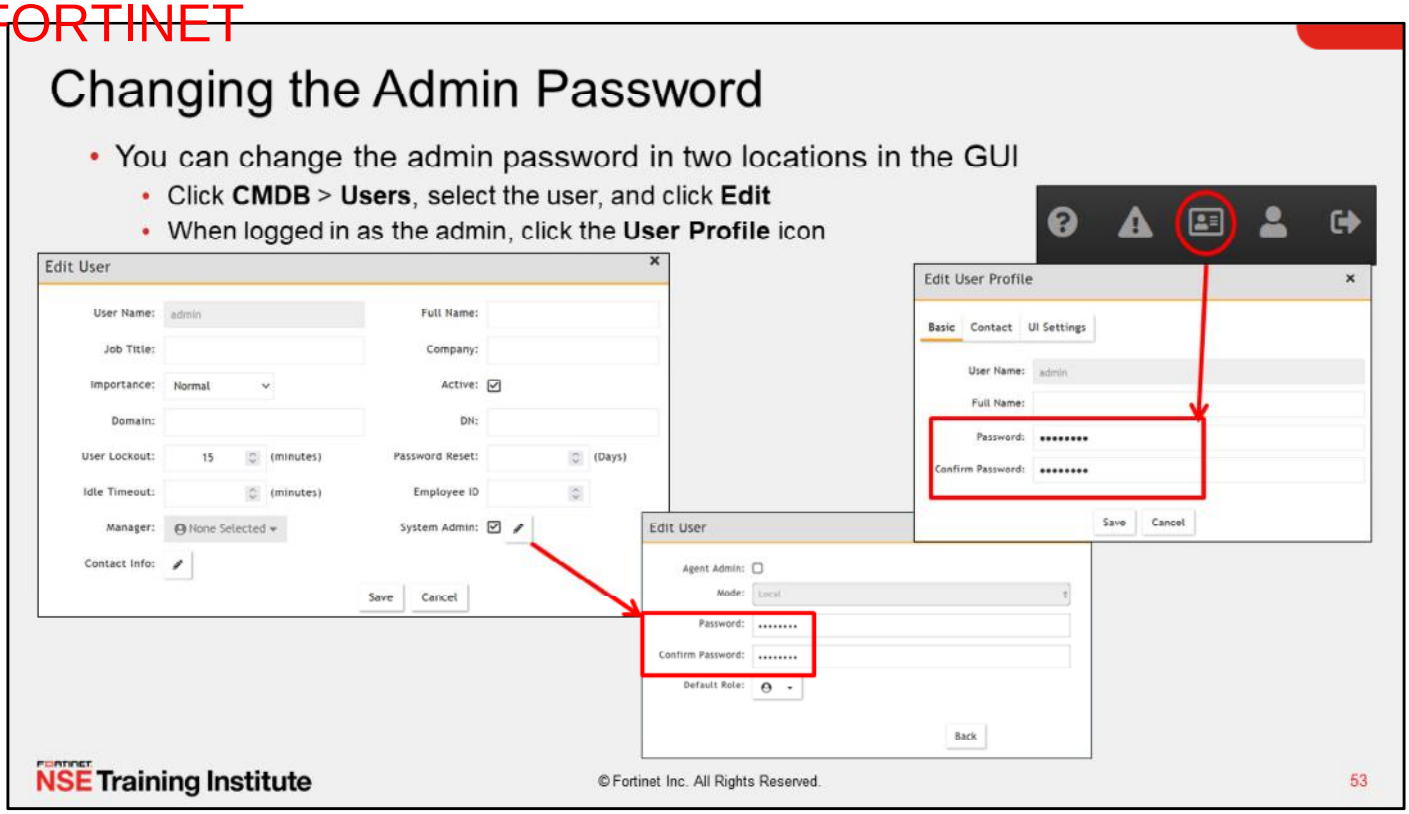


In the CMDB, you can edit the information for internal and external users to add contact information, such as phone number, street address, country, or email address.

It is important to note that you can refer to a user in the incident notification policies only if you add the user's email address to the CMDB.

Vouchers & Dumps are Available | WhatsApp +201224560923

DO NOT REPRINT
© FORTINET
Brave-dumps.com



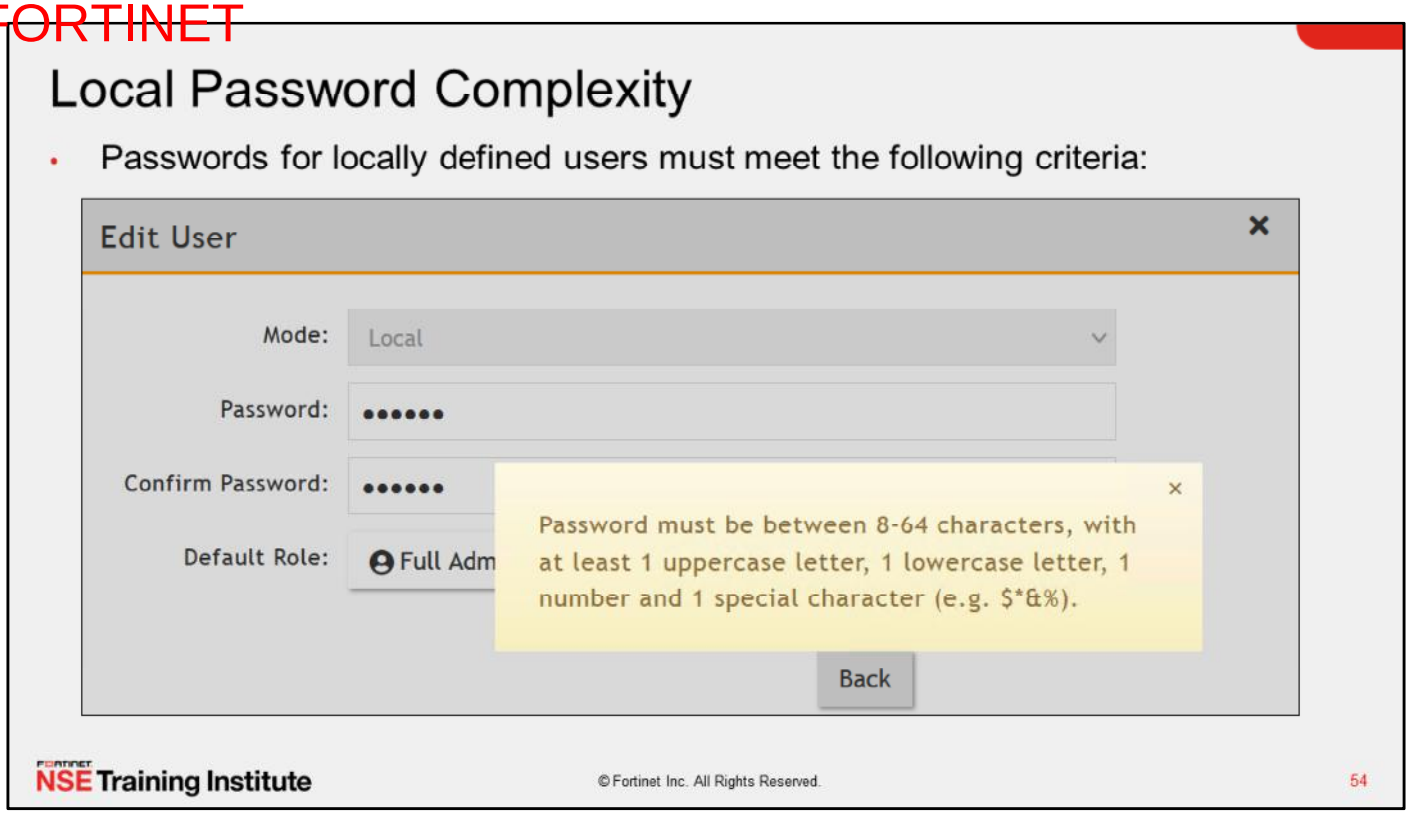
You can change the password in two locations on the GUI.

On the **CMDB** tab, click **Users**, and then edit the admin user's properties. You can change the password for a locally-defined user on this screen as well.

Alternatively, any local defined user logged in to the FortiSIEM GUI can click the user icon in the upper-right corner of the GUI, and then, in the **Edit User Profile** window, change the password.

Vouchers & Dumps are Available | WhatsApp +201224560923

DO NOT REPRINT
© FORTINET
Brave-dumps.com



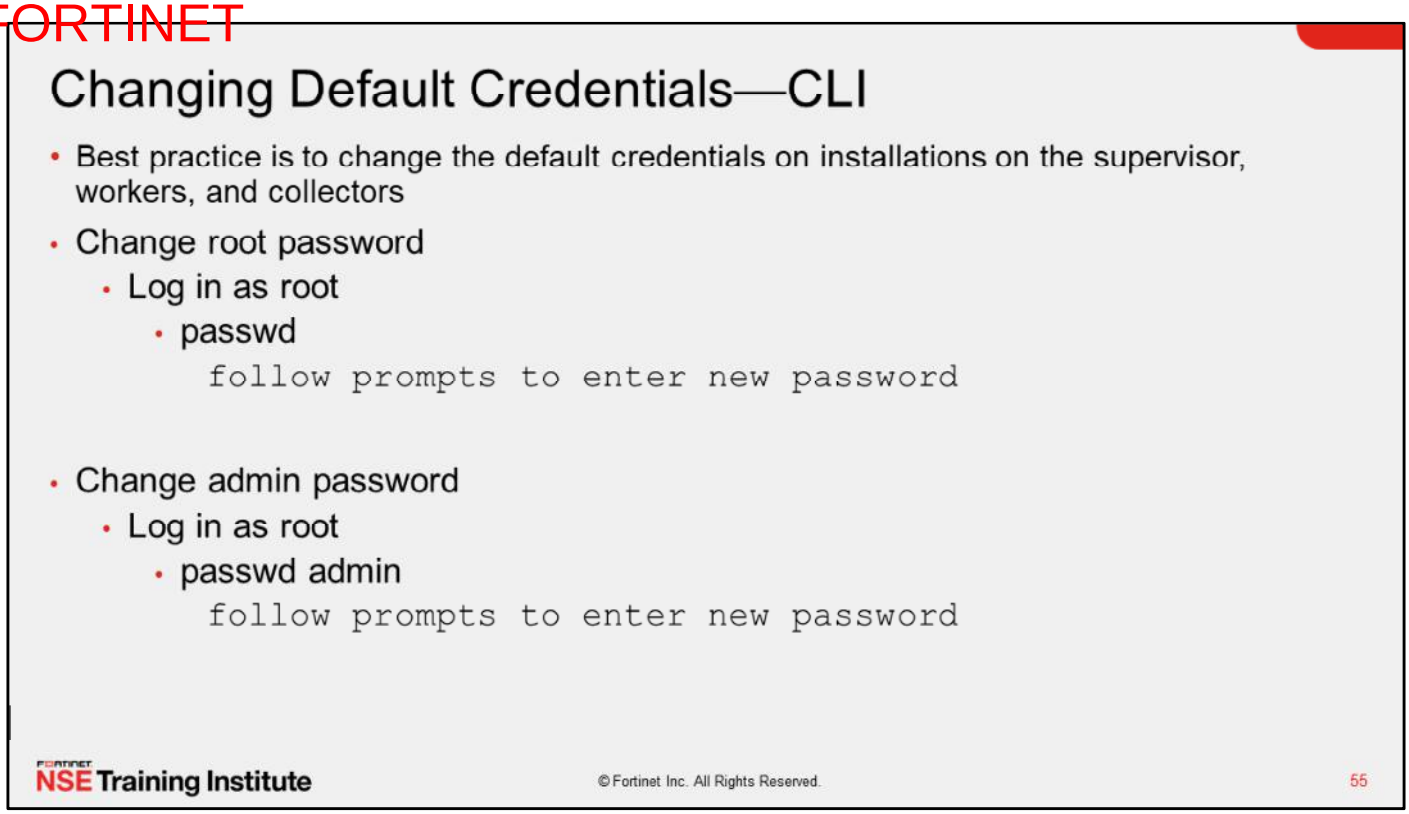
FortiSIEM has no control over the password rules that are applied to external user accounts because those passwords are managed by another device.

However, FortiSIEM applies password rules to locally defined user accounts.

The password must contain 8 to 64 characters, and must contain at least one uppercase letter, at least one lowercase letter, at least one number, and one special character.

Vouchers & Dumps are Available | WhatsApp +201224560923

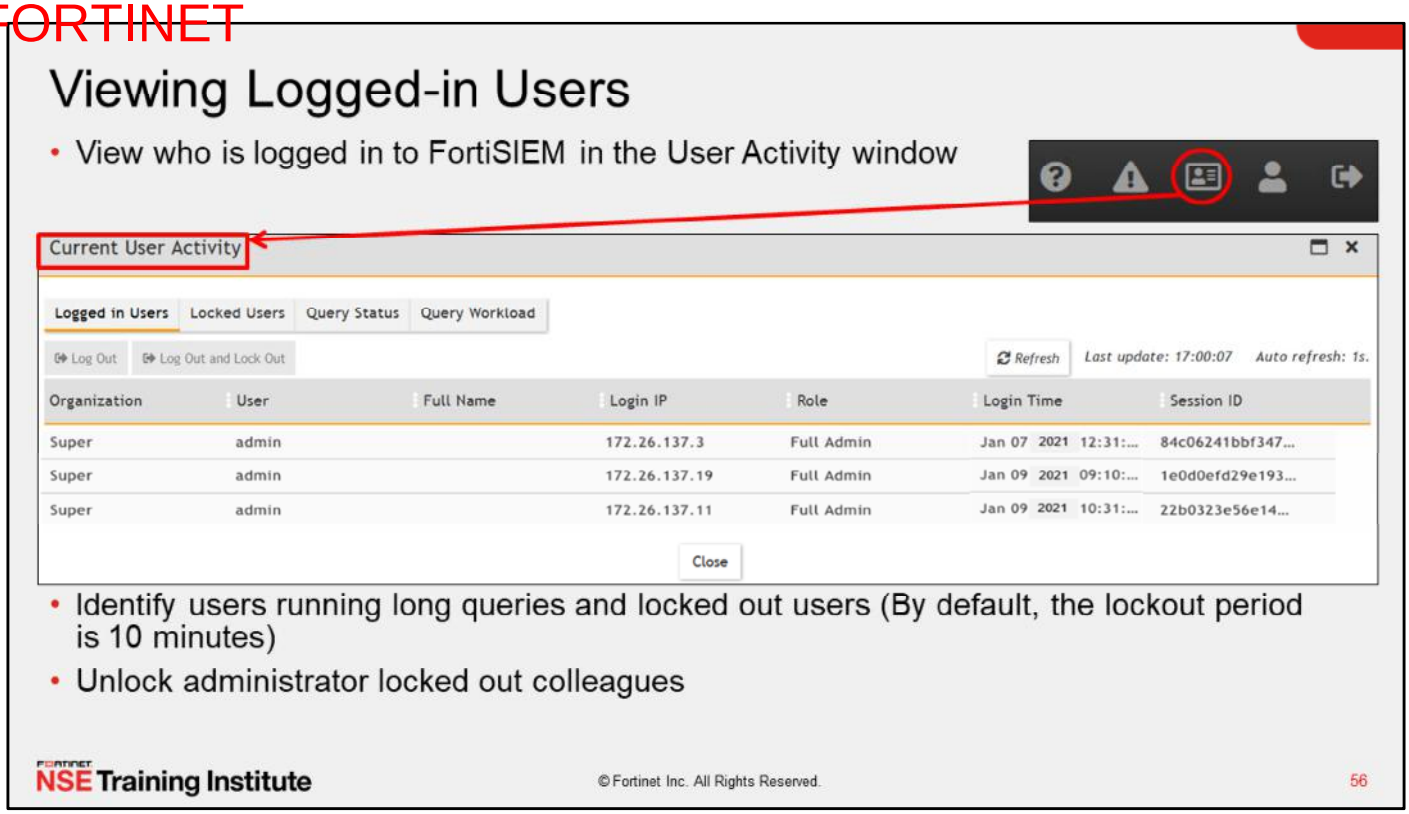
DO NOT REPRINT
© FORTINET
Brave-dumps.com



This slide shows how to change passwords for the *root* and *admin* accounts using the CLI. The best practice is to change the default credentials on installations on the supervisor, workers, and collectors.

Vouchers & Dumps are Available | WhatsApp +201224560923

DO NOT REPRINT
© FORTINET
Brave-dumps.com



The **User Activity** icon is located in the upper-right corner of the FortiSIEM GUI. Administrators can click the **User Activity** icon to open the **Current User Activity** pop-up window and view *who* is logged in to FortiSIEM. The **Current User Activity** pop-up window doesn't show you as yourself, but it shows you any other user who is logged in.

On the **Current User Activity** window, you can select the **Query Workload** tab to identify users who are running long queries.

To view users who have been locked out of FortiSIEM, on the **Current User Activity** window, select the **Locked Users** tab. The default lockout period is 10 minutes. Administrators can unlock locally defined users on the **Locked Users** tab.

Vouchers & Dumps are Available | WhatsApp +201224560923

DO NOT REPRINT
© FORTINET
Brave-dumps.com

Knowledge Check

1. A FortiSIEM administrator wants to restrict a network administrator to running searches for firewall devices only. Under role management, which option does the FortiSIEM administrator need to configure to achieve this scenario?

A. CMDB report conditions
✓ B. Data conditions
C. UI access

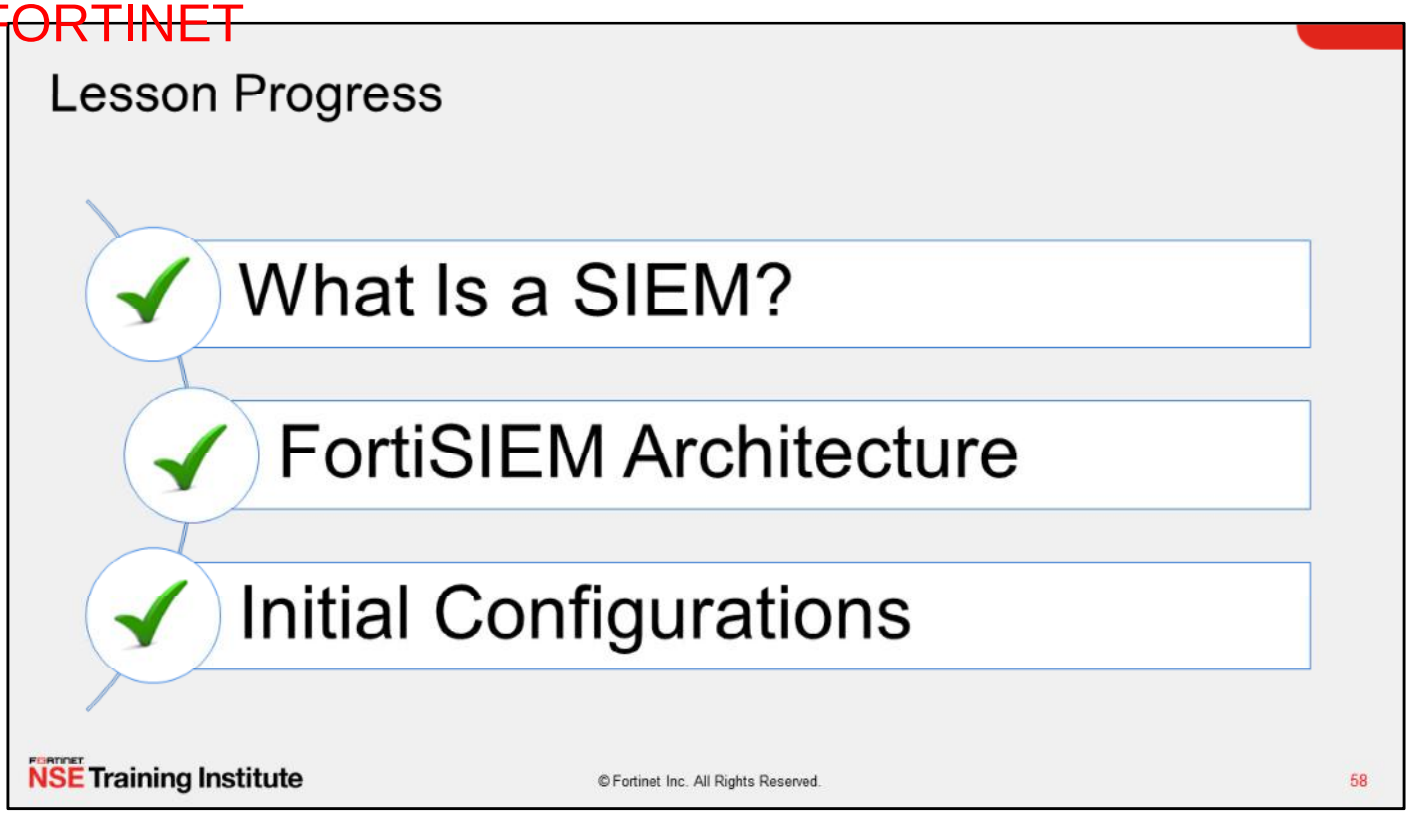
NSE Training Institute

© Fortinet Inc. All Rights Reserved.

57

Vouchers & Dumps are Available | WhatsApp +201224560923

DO NOT REPRINT
© FORTINET
Brave-dumps.com

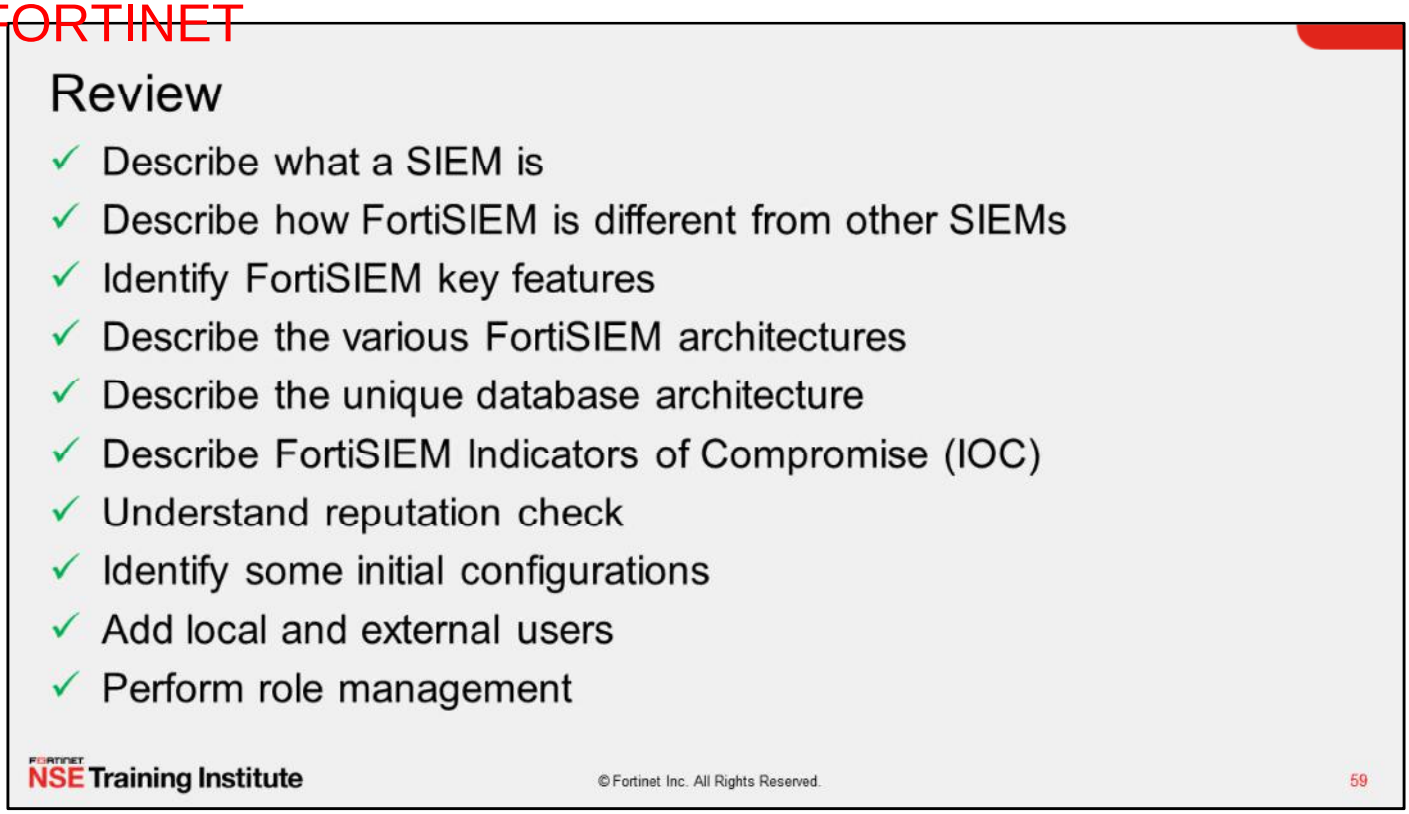


Congratulations! You have completed this lesson.

Now, you will review the objectives that you covered in the lesson.

Vouchers & Dumps are Available | WhatsApp +201224560923

DO NOT REPRINT
© FORTINET
Brave-dumps.com

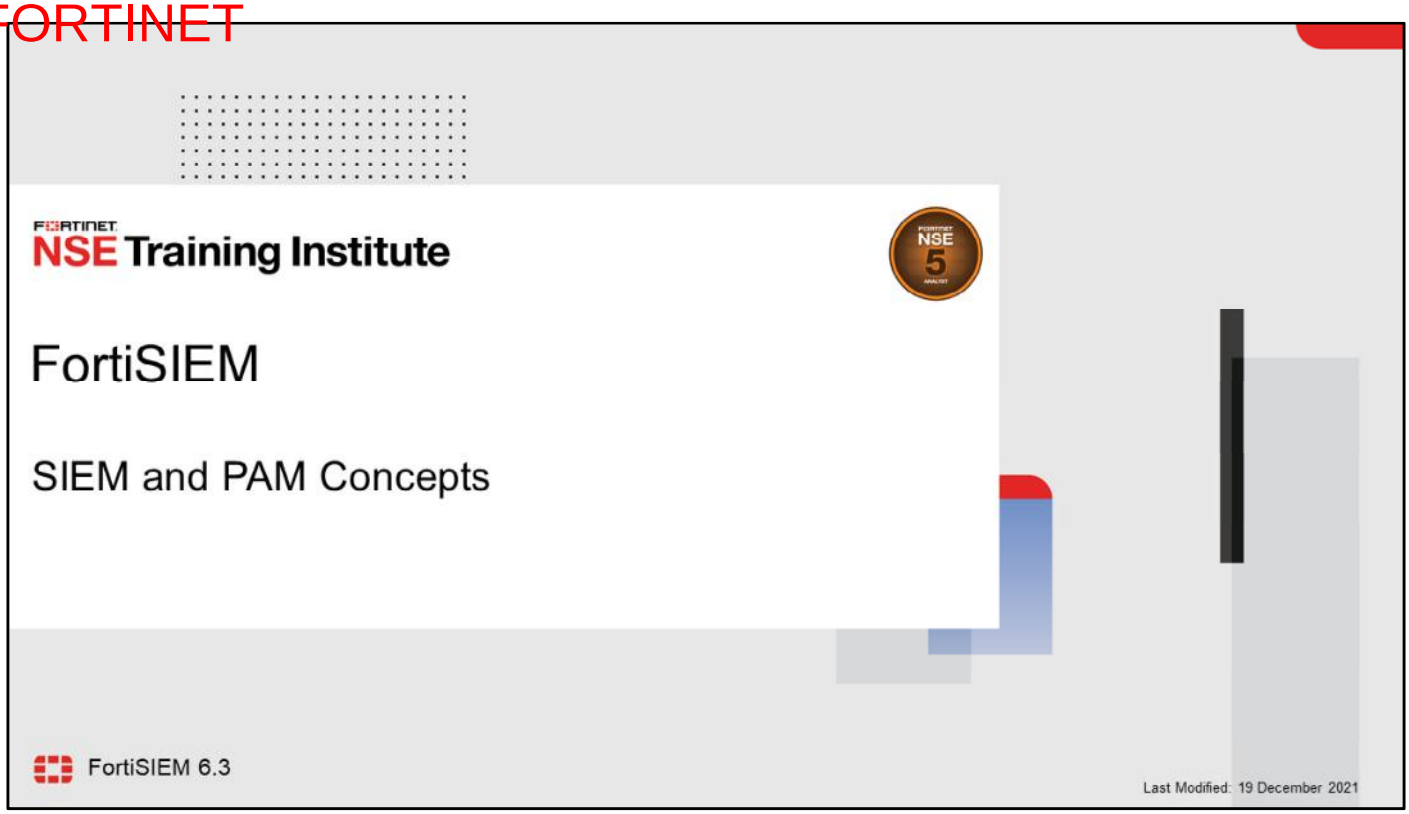


This slide shows the objectives covered in this lesson.

By mastering the objectives covered in this lesson, you learned how to differentiate FortiSIEM from other SIEMs, identify the strengths of FortiSIEM, understand FortiSIEM architecture, install FortiSIEM, and perform the initial configuration.

Vouchers & Dumps are Available | WhatsApp +201224560923

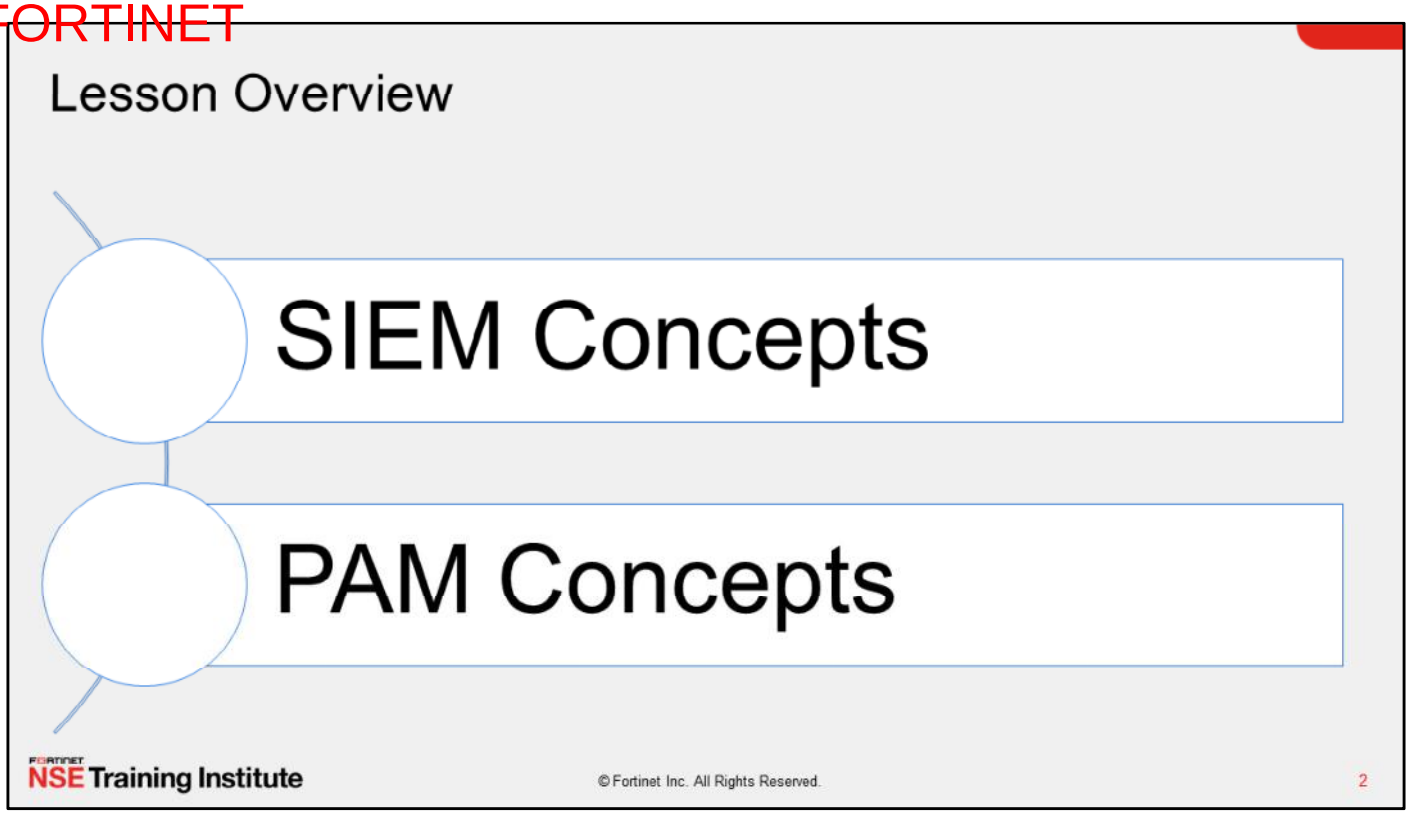
DO NOT REPRINT
© FORTINET
Brave-dumps.com



In this lesson, you will learn how FortiSIEM receives, collects, and normalizes logs. You will also learn how PAM data is collected and processed.

Vouchers & Dumps are Available | WhatsApp +201224560923

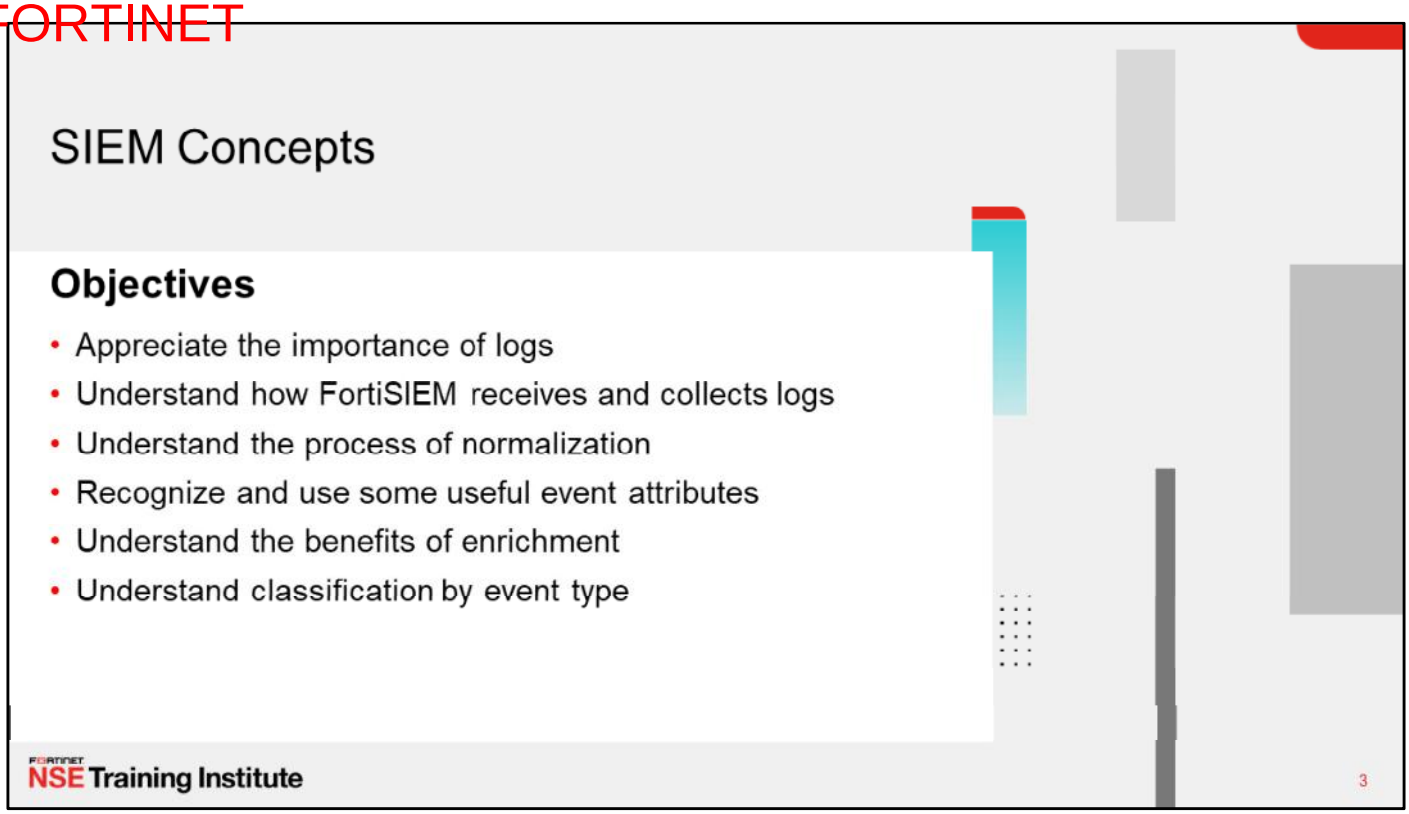
DO NOT REPRINT
© FORTINET
Brave-dumps.com



In this lesson, you will learn about the topics shown on this slide.

Vouchers & Dumps are Available | WhatsApp +201224560923

DO NOT REPRINT
© FORTINET
Brave-dumps.com



After completing this section, you should be able to achieve the objectives shown on this slide.
By demonstrating competence in understanding how FortiSIEM receives, collects, and normalizes logs, you will have the practical skills and knowledge required to understand how FortiSIEM works with logs.

Vouchers & Dumps are Available | WhatsApp +201224560923

DO NOT REPRINT
© FORTINET
Brave-dumps.com



Log collection is at the heart of what a FortiSIEM does. All FortiSIEM devices collect and process logs, but which of these logs are the most useful?

- Audit logs
- User activity logs
  - These include, a user logging in to a system, failing to log in to a system, or modifying a particular account in a network.
- Transaction logs
- Intrusion logs, such as from your intrusion detection or intrusion prevention systems
- Connection logs
  - These come from devices like firewalls or switches. An example would be something like, “this source went to that destination through that port”.
- Application logs
  - These come from a DNS server, DHCP server, or, perhaps, an SQL server.
- SNMP traps
- Other types of messages within your environment

The more logs FortiSIEM can collect, the more information you’ll have, and the easier it will be to establish a baseline and spot anomalies.

Vouchers & Dumps are Available | WhatsApp +201224560923

DO NOT REPRINT
© FORTINET
Brave-dumps.com

Logs From What Components?

- Firewalls
- IDS or IPS devices
- Routers or switches
- Servers or virtualization
- Business applications
- Databases
- Antivirus or end point
- Web proxies and VPNs
- Devices can be on premise or in the cloud



NSE Training Institute

© Fortinet Inc. All Rights Reserved.

5

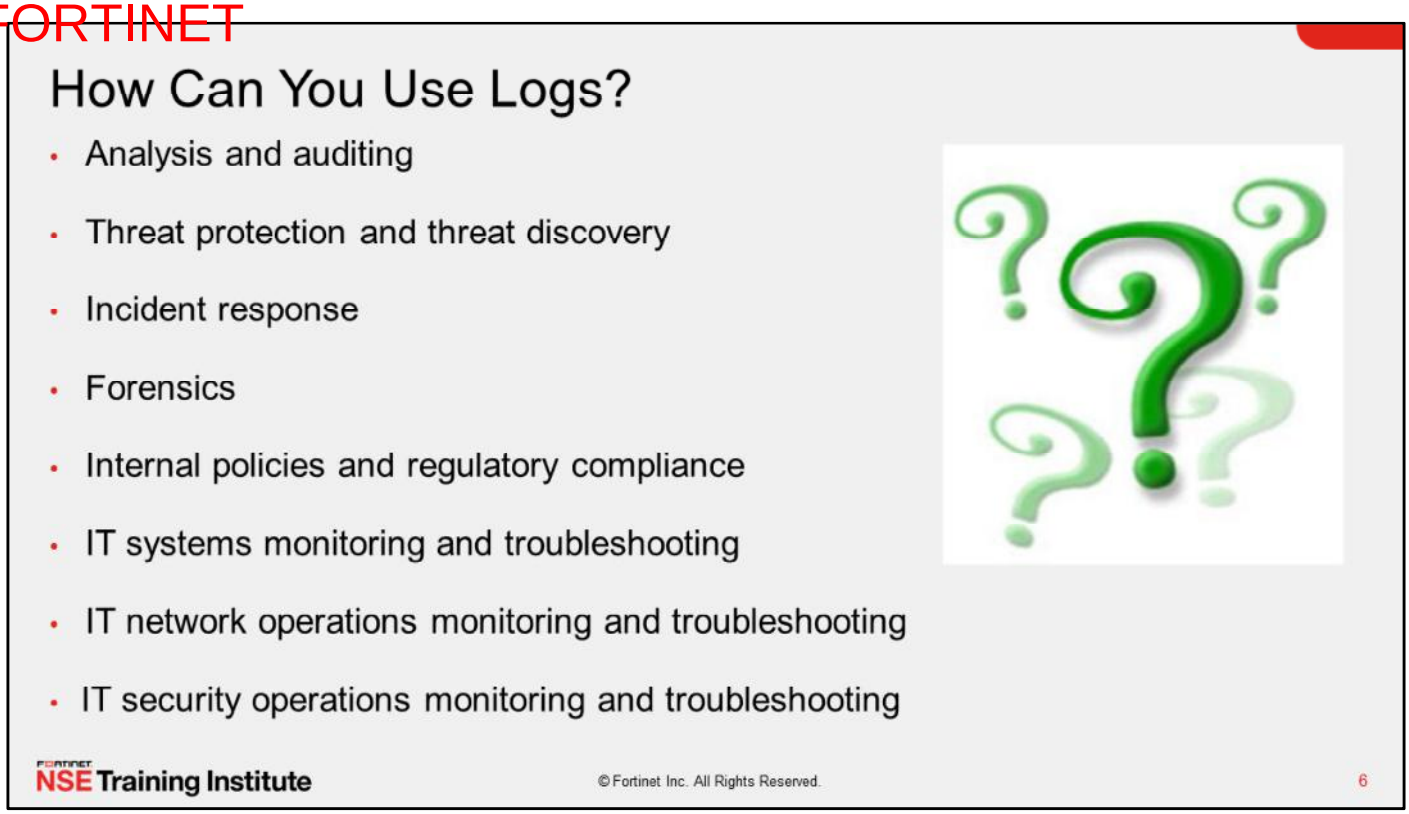
You'll want to collect the logs that come from the critical components of your network and business.

The greatest sources of information are: your firewalls, switches, and routers; your key servers, both physical and virtual; and your active directory and database servers, as well as others.

Think about the parts of your infrastructure that are crucial to running your business. The logs that these components generate are the keys to keeping your network up, and your business running. Whether these components are located on premises, or in the cloud, it's useful for FortiSIEM to collect this kind of information.

Vouchers & Dumps are Available | WhatsApp +201224560923

DO NOT REPRINT
© FORTINET
Brave-dumps.com



How can you use the logs that FortiSIEM collects? You can use the information in these logs for the following purposes:

- Analysis and auditing
- Threat protection and threat discovery
- Forensics

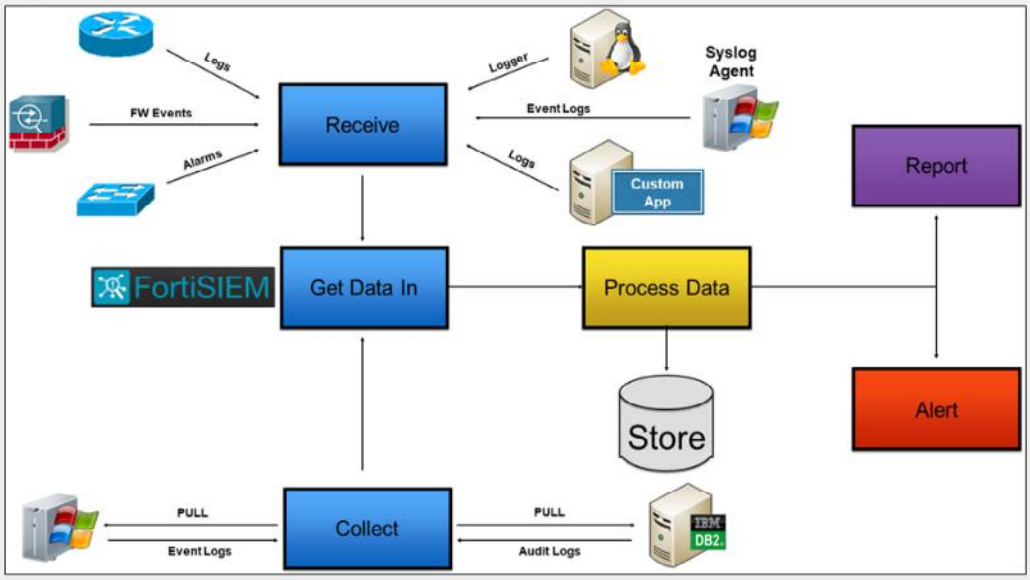
You may need logs for regulatory compliance. You can also use logs to monitor and troubleshoot your IT systems, network, or security operations.
Logs are securely stored and checksums created to detect tampering.

Vouchers & Dumps are Available | WhatsApp +201224560923

DO NOT REPRINT Brave-dumps.com
© FORTINET

FortiSIEM Functionality

- This is a high-level view of how a traditional FortiSIEM functions



NSE Training Institute

© Fortinet Inc. All Rights Reserved.

7

The primary job of FortiSIEM is to process logs. But, how do we get all of these logs into the FortiSIEM in the first place?

FortiSIEM either *receives* data from devices and applications, or it *collects* data from devices and applications.

Network devices, such as routers, switches, and firewalls, typically have *syslog capability*. That is, these devices have the ability to push out traffic and audit logs to a syslog collector. In a FortiSIEM network, the syslog collector is a supervisor, a worker, or a collector node.

Servers typically run a syslog daemon. This means that servers, like routers, have syslog capability. However, some servers, such as Windows servers, don't have the ability to send syslogs. You can install a syslog *agent* on these servers to give them syslog capability. The agent that you install can be a FortiSIEM agent, or a third-party agent. However, there are some types of information that you can collect without an agent. You can use the WMI protocol to pull events from Windows servers, and you can pull audit logs from databases using JDBC.

After FortiSIEM has received or collected data from the network, it processes and stores the data. At that point, you can generate reports and alerts, based on the data that FortiSEIM has collected.

Vouchers & Dumps are Available | WhatsApp +201224560923

DO NOT REPRINT Brave-dumps.com
© FORTINET

Receiving Logs and Flow Data

- FortiSIEM can receive the following types of data from applications or devices:
- Message formats:
  - SYSLOG - UDP/514, TCP/1470,514, SSL/443
  - SNMP Trap - UDP/162
- Flow data formats:
  - NetFlow (versions 5 and 9 being sent on port UDP/2055)
  - sFlow (UDP/6343)
  - Cisco ASA Netflow (UDP/2055)
  - **Note:** If you intend to send both syslog and SNMP traffic, make sure that FortiSIEM supports both of those protocols from that specific device



NSE Training Institute

© Fortinet Inc. All Rights Reserved.

8

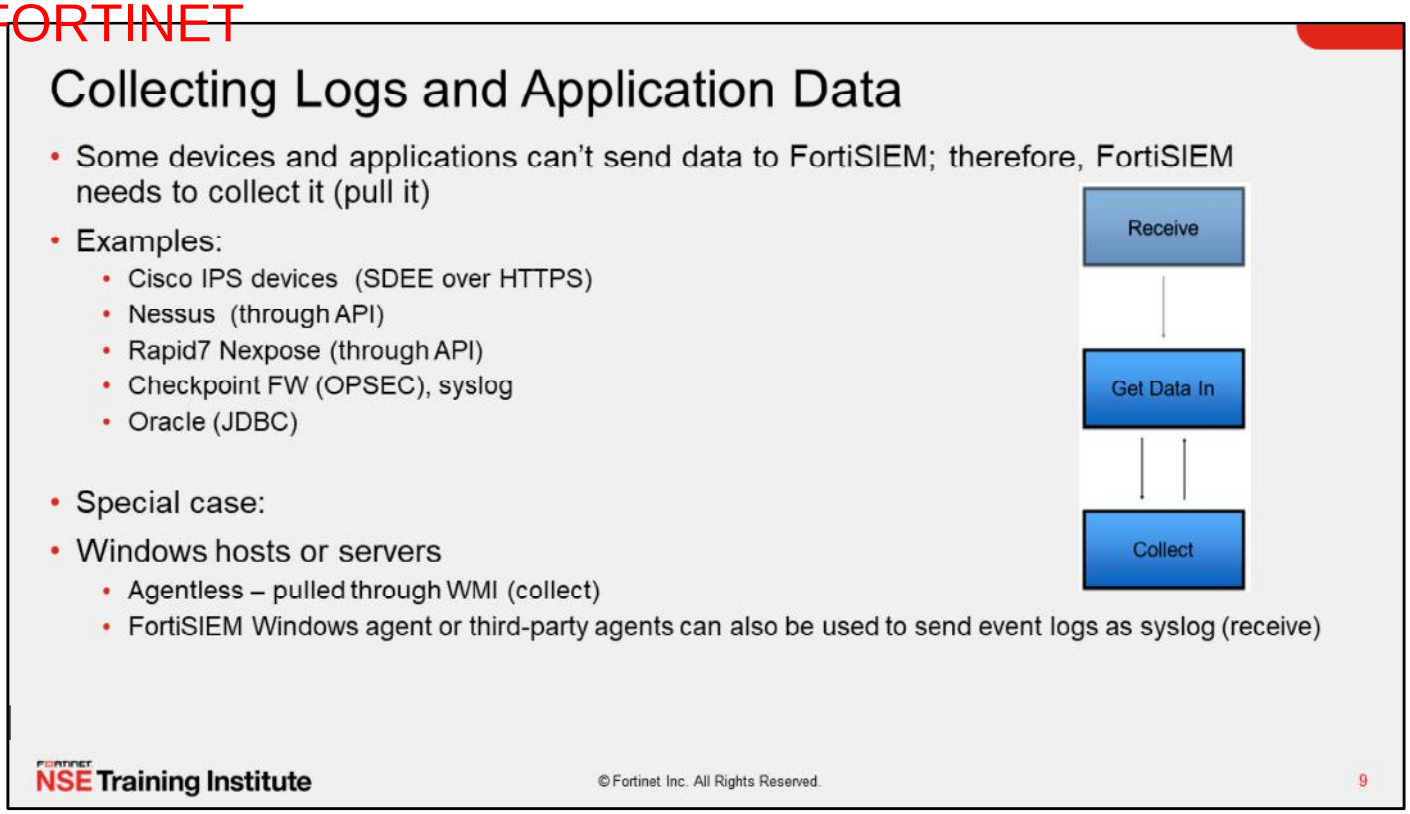
When devices send their data to FortiSIEM, FortiSIEM expects the data to come in specific formats. FortiSIEM can receive data in many formats:

- Syslog
  - Default ports are 514 for UDP, 1470/514 for TCP, and 443 for SSL
- SNMP traps
  - UDP on port 162
- Netflow version 5 and 9
  - Default UDP port 2055
- sFlow
  - Default UDP port of 6343
- Cisco ASA Netflow
  - Uses UDP port 2055

You should send SNMP traffic to a device only if FortiSIEM supports reading SNMP traps from that device. A common mistake is to assume that FortiSIEM supports SNMP traffic from a device because it supports syslog traffic from that device. This is not always the case. If you intend to send both syslog and SNMP traffic, make sure that FortiSIEM supports both of those protocols from that specific device.

Vouchers & Dumps are Available | WhatsApp +201224560923

DO NOT REPRINT
© FORTINET
Brave-dumps.com



Some devices and applications don't have the ability to send data to FortiSIEM; therefore, FortiSIEM needs to collect or *pull* that data from the device or application.

Examples of devices and applications that can't send data are:
- **Cisco IPS devices:** Uses a protocol known as SDEE that works over https
- **Nessus:** Has an API that you can use to pull the requested data
- **Rapid7:** Has an API that you can use to pull the requested data
- **Checkpoint firewall:** You can use OPSEC protocol to pull information
- **Databases:** You can use JDBC protocol to pull information

Windows servers are a special case. You have a couple of options that you can use to collect data from these devices: you can use WMI to pull data from them, or you can install an agent on them. Installing an agent is the recommended option for busy Windows servers, such as domain controllers.

The FortiSIEM agent provides the following functions:
- Event collection
- File integrity monitoring
- Registry monitoring
- The ability to run PowerShell scripts
- Additional functions

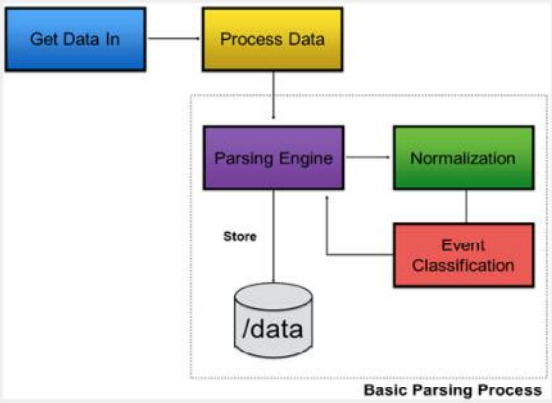
You can also use third-party agents. The third-party agents supported by FortiSIEM read the windows event logs and send that data to FortiSIEM as syslog.

Vouchers & Dumps are Available | WhatsApp +201224560923

DO NOT REPRINT Brave-dumps.com
© FORTINET

FortiSIEM Process Flow

1. Data is collected from devices
2. Data is processed by the parsing engine
3. The parsing engine performs normalization on the data
4. The parsing engine performs event classification on the data
5. The structured data is stored



NSE Training Institute

© Fortinet Inc. All Rights Reserved.

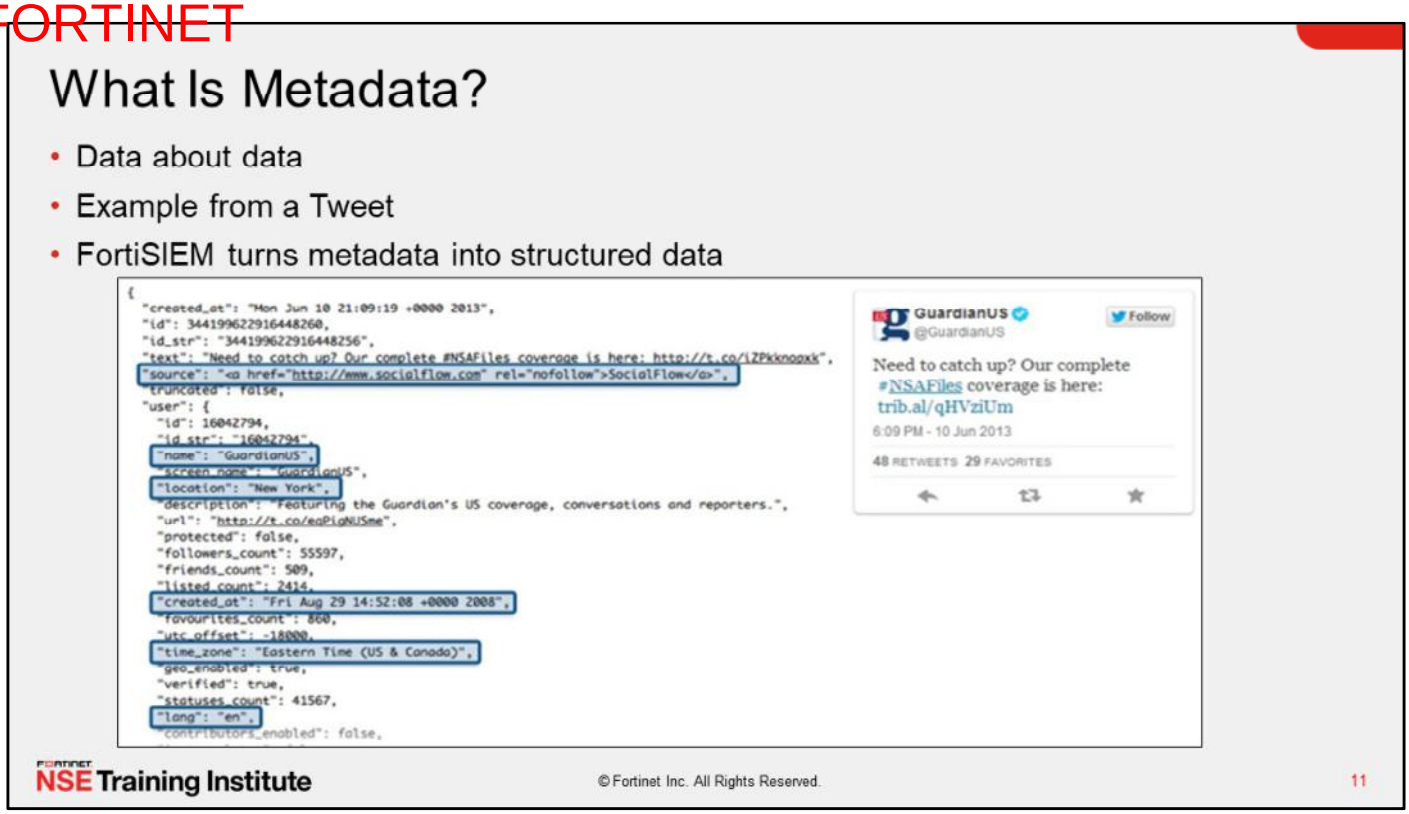
10

Let's take a look at FortiSIEM's process flow.

1. Data is collected from the devices and processes running in the network.
2. The collected data is processed by the parsing engine, or parser.
   - The parser provides the intelligence required to understand the data.
   - FortiSIEM supports more than 170 types of devices and applications. The FortiSIEM parser can parse logs at more than 10,000 events per second, for each node.
3. The parser performs normalization on the data.
   - *Normalization* is the process of taking raw input events from all devices or applications, extracting individual fields, and mapping those fields to a common schema.
4. The parser performs event classification on the data.
   - *Event classification* is the process of assigning an event identifier or event type to each message based on a unique attribute.
5. The structured data is stored by FortiSIEM.
   - *Structured data* is the data that has been parsed or processed by the FortiSIEM parser. Other vendors refer to this data as *parsed data* or *metadata*.

Vouchers & Dumps are Available | WhatsApp +201224560923

DO NOT REPRINT
© FORTINET
Brave-dumps.com



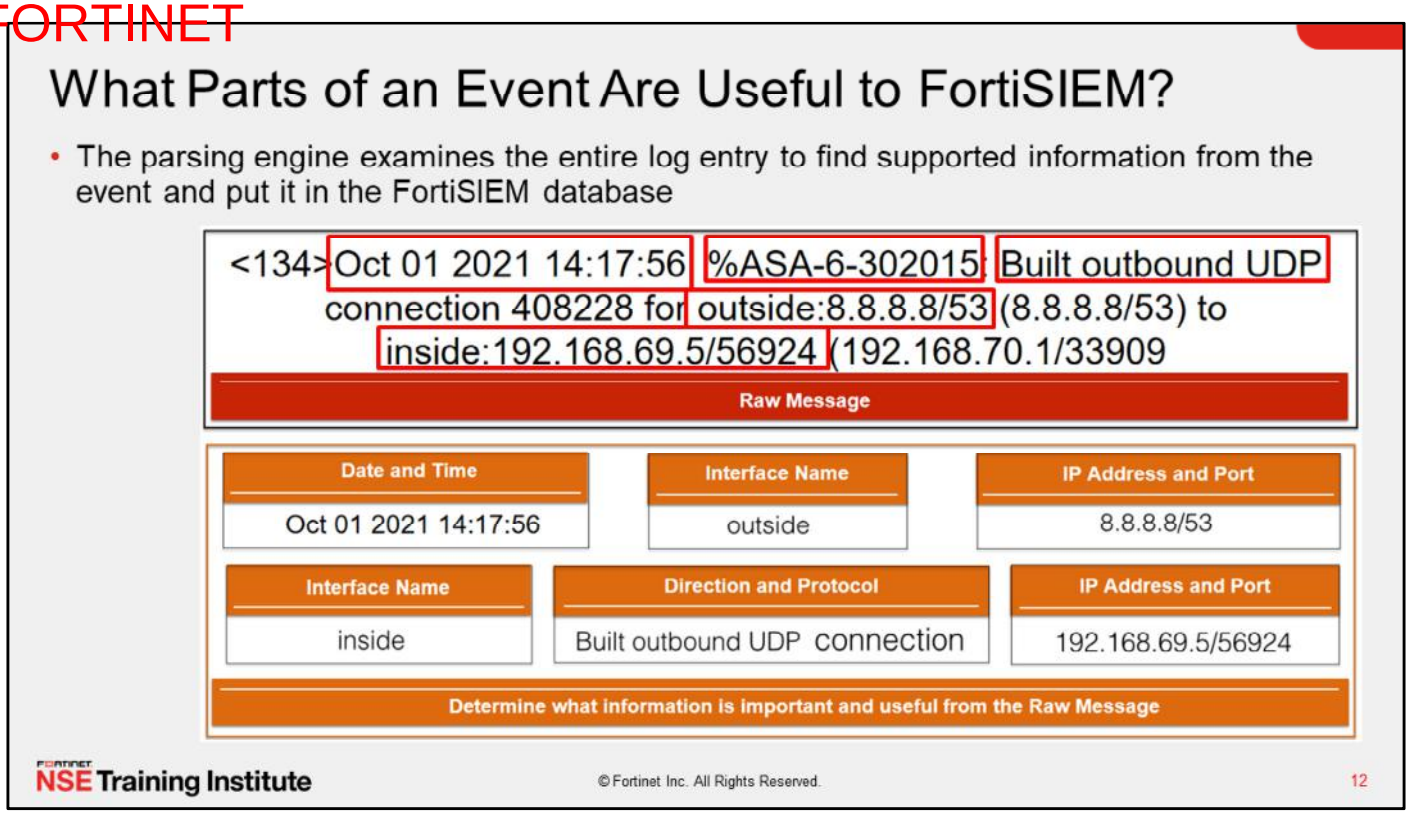
What is metadata? Simply put, metadata is data about data.

Let’s use a tweet in Twitter as an example. The message itself is actually very small. But, if you looked at the data behind the message, you would see that many different fields have been created, such as the source, the name, the location, the time stamp, languages, and so on. The amount of metadata that is produced by the message may actually be larger than the message itself.

FortiSIEM turns this metadata into structured data.

Vouchers & Dumps are Available | WhatsApp +201224560923

DO NOT REPRINT
© FORTINET
Brave-dumps.com

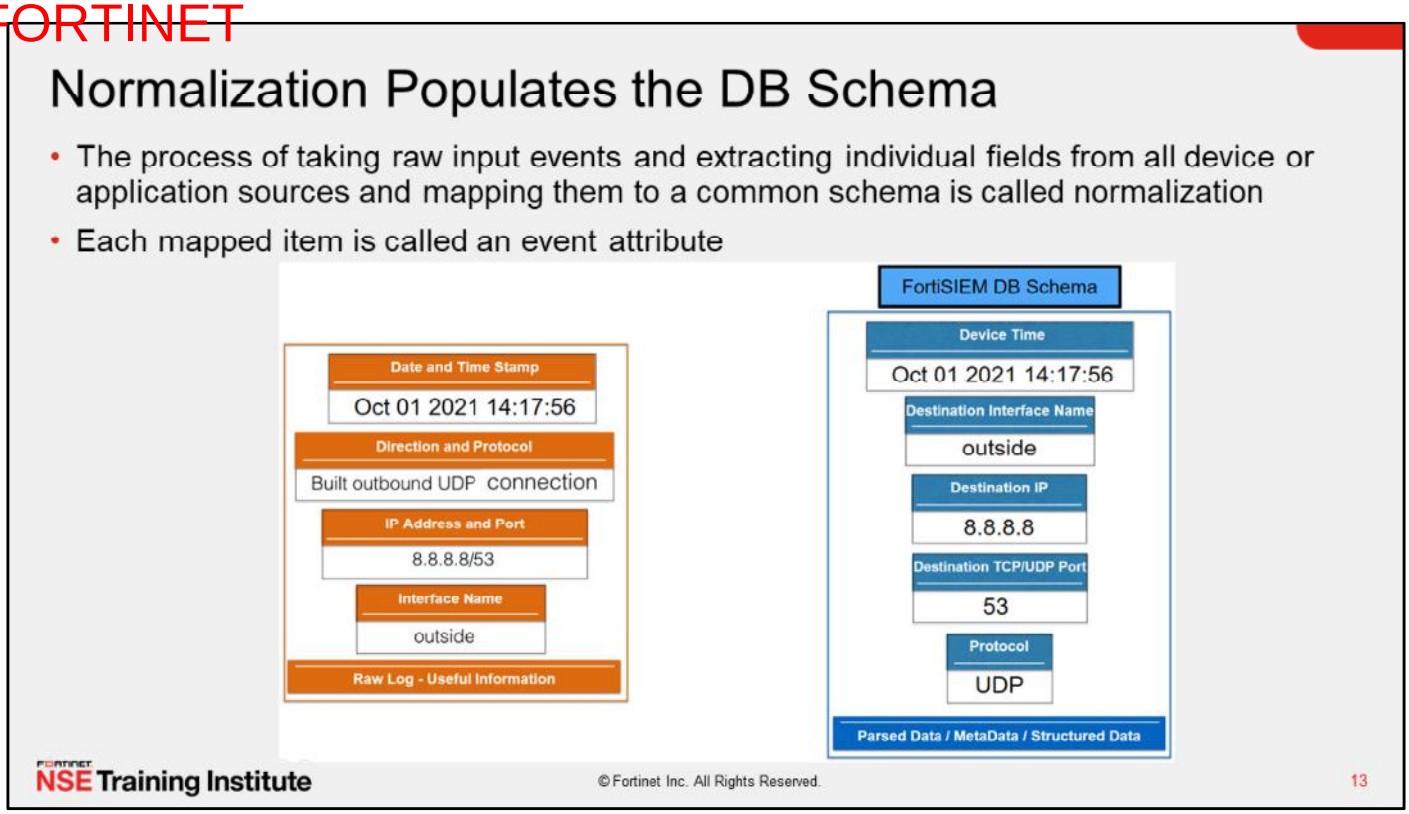


One of the main functions of the parsing engine is to separate the entire log file into its essential elements. The parsing engine then examines each of these elements to determine which ones hold important or useful information. It then puts all this information from the event into the FortiSIEM database.

Consider the simplified sample of a firewall message shown on this slide. You can see that this message comes from a Cisco ASA. You can also see that there's a date, a time stamp, an interface name, and a couple of IP addresses and ports. You know the direction of the traffic was outbound, and the protocol was UDP. You could have pulled even more information from the full raw message than what was discussed in this example.

Vouchers & Dumps are Available | WhatsApp +201224560923

DO NOT REPRINT
© FORTINET
Brave-dumps.com



Devices and applications from different vendors have their own ways of representing information in their log events; for example, there are several formats that can be used to represent a date and time. Not only will log events from different devices and applications hold different information, and they hold common information in different order.

The process of taking raw input events, extracting individual fields, and mapping those fields to a common schema, is called *normalization*. FortiSIEM is able to work with the logs from many different sources.

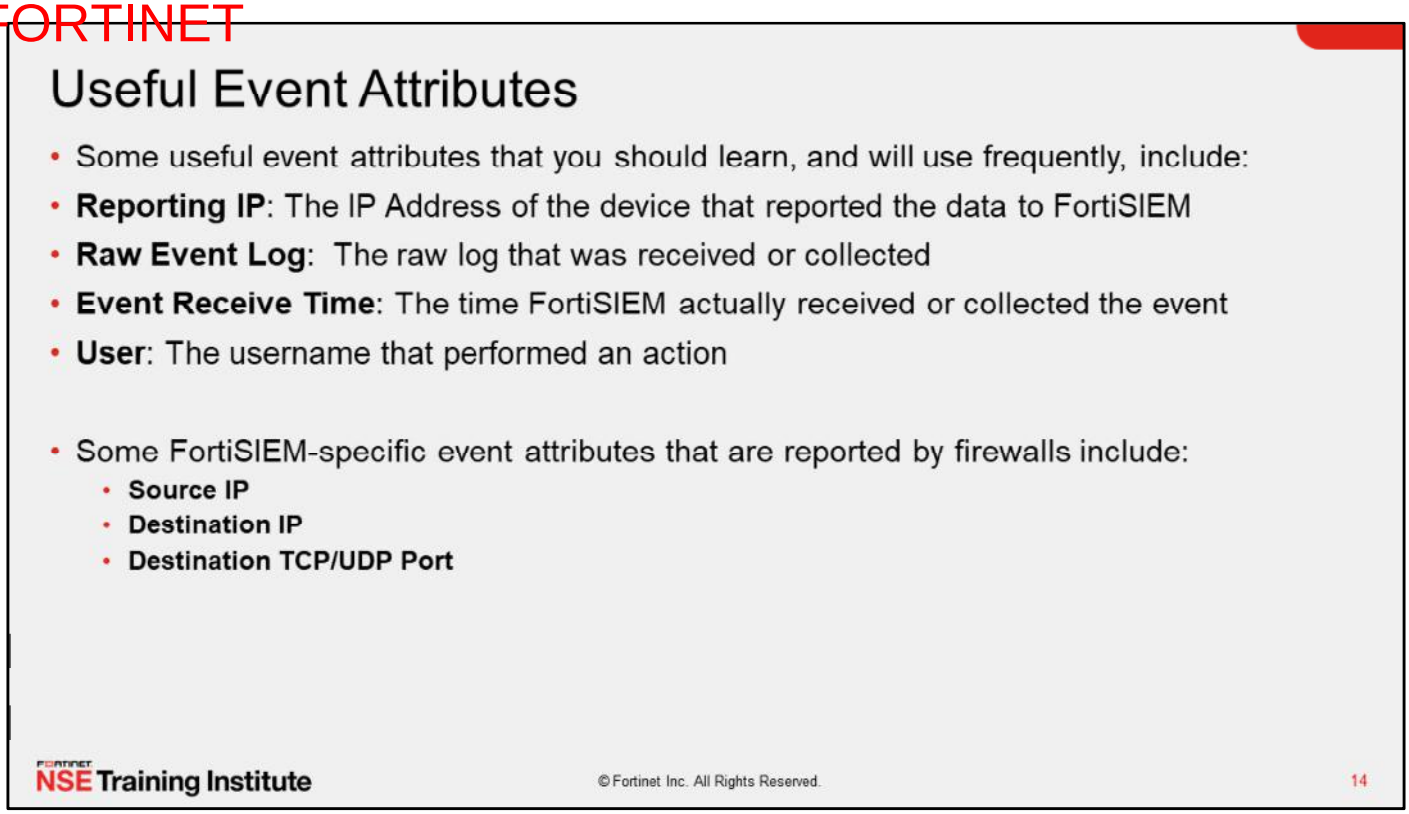
In this example, you can see that the parser mapped the following fields to the following FortiSIEM database attributes:

- The **Date and Time Stamp** field was mapped to the **Device Time** database attribute.
- The **IP Address and Port** field was mapped to the **Destination Address** and **Destination Port** attributes.
- The **Direction and Protocol** field was mapped to the **Protocol** and **Destination Interface** attributes.

Each of the fields that is mapped to an attribute in the ForiSIEM database is called an *event attribute*.

Vouchers & Dumps are Available | WhatsApp +201224560923

DO NOT REPRINT
© FORTINET
Brave-dumps.com



Some useful event attributes that you should learn, and will use frequently, include:

- **Reporting IP**: This is the IP address from the device that reported the data to FortiSIEM.
- **Raw Event Log**: This is the raw log that was received or collected from a particular device. It is important to note that, although the log was normalized and mapped to the FortiSIEM schema, a copy of the original log is saved as well.
- **Event Received Time**: This is a timestamp that FortiSIEM puts in the message that records the time that it received or collected the event.
- **User**: If there is a username populated within an event, it will be populated in an attribute called User.

Some SIEM-specific event attributes that are reported by firewalls, include:

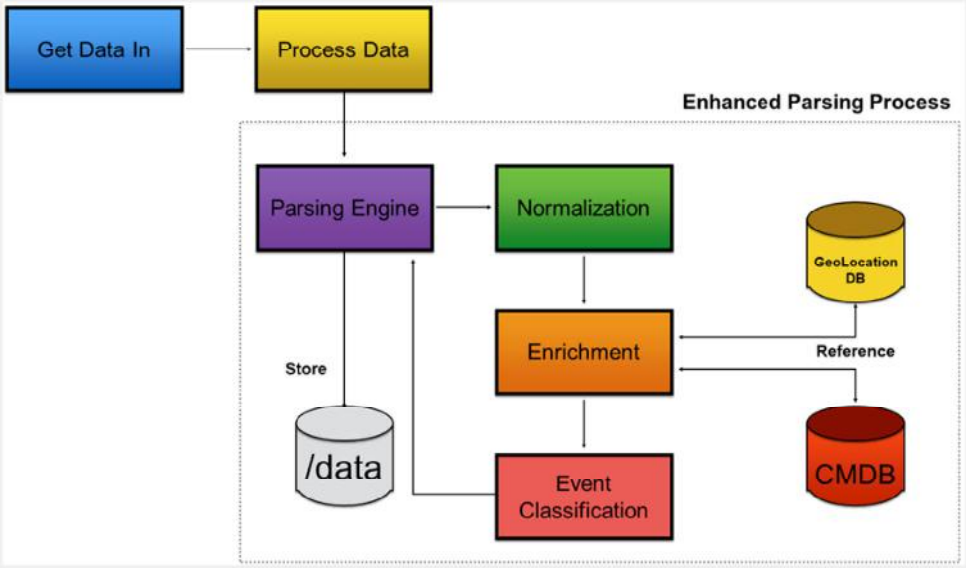
- Source IP
- Destination IP
- Destination TCP/UDP port

Vouchers & Dumps are Available | WhatsApp +201224560923

DO NOT REPRINT
© FORTINET
Brave-dumps.com

Adding Enrichment

- The parsing engine will also enrich the structured data that it produces



NSE Training Institute

© Fortinet Inc. All Rights Reserved.

15

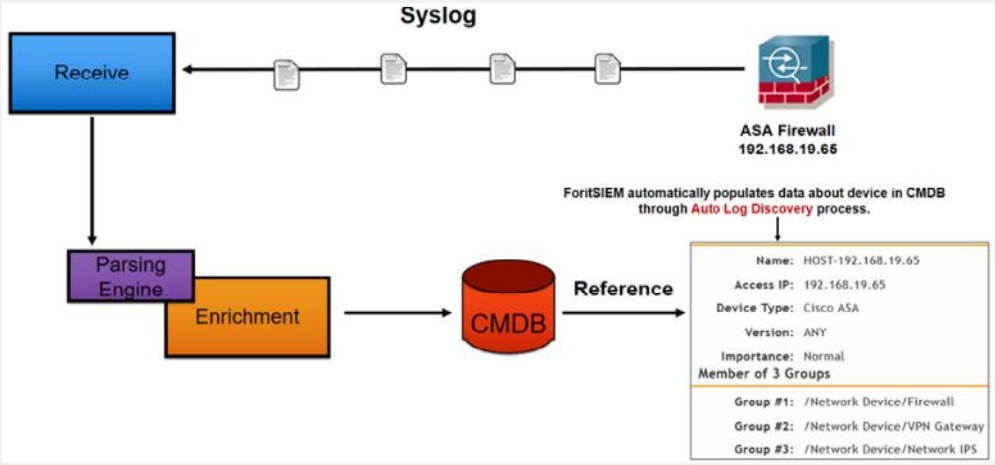
After the parsing engine completes the process of *normalizing* a raw event log, FortiSIEM can also *enrich* the structured data fields that have been produced. The process of enrichment involves adding additional information to an event, based on information that FortiSIEM already knows about that device or IP address.

Vouchers & Dumps are Available | WhatsApp +201224560923

DO NOT REPRINT
© FORTINET
Brave-dumps.com

Reporting IP and Model

- An example of enrichment: the addition of reporting IP, model, and vendor information
- The enrichment activity shown on this slide allows you to search for data by the reporting IP address of the device



- **Note**: Logs alone won't provide enough information for the device in the CMDB

NSE Training Institute © Fortinet Inc. All Rights Reserved. 16

An example of enrichment is the addition of the reporting IP of the device, along with the model.

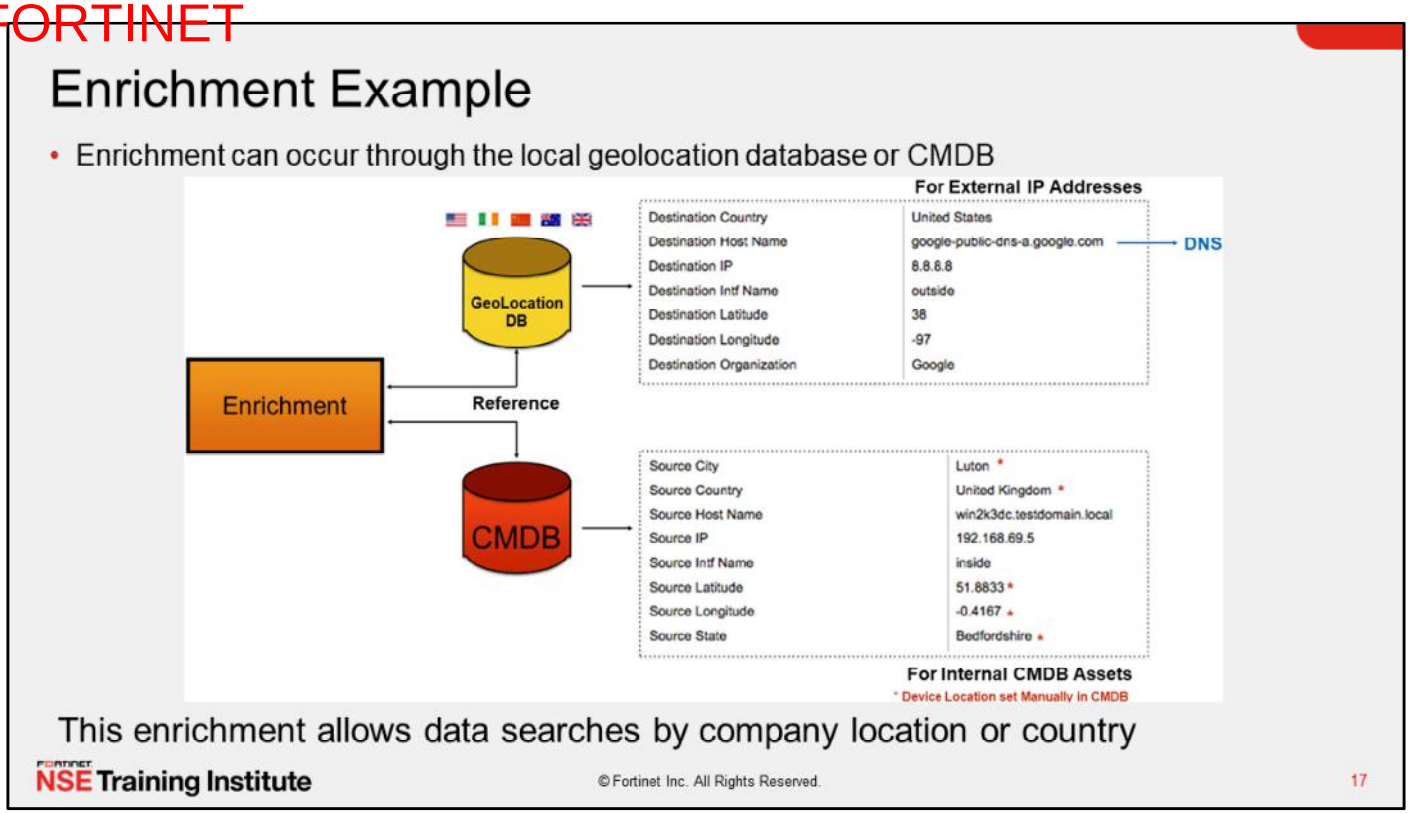
In the example shown on this slide, an ASA firewall is sending syslogs to FortiSIEM. The model and the IP address of the firewall may not be in the syslog, but FortiSIEM knows the IP address of the device that sent the message. FortiSIEM can look in the configuration management database (CMDB) to determine which device is associated with that IP address, and use some of that information to enrich the event log.

If the name of the device is not determined, then FortiSIEM will display device name as Host-(IP x.x.x.x).

Because FortiSIEM performs enrichment by adding extra fields to the structured data, it allows you to search and filter based on those enriched fields. This might be useful when generating reports, for example.

Vouchers & Dumps are Available | WhatsApp +201224560923

DO NOT REPRINT
© FORTINET
Brave-dumps.com



Another example of FortiSIEM enrichment is the addition of geolocation data to events. Geolocation data can come from a geolocation database provided by Maxmind, or from the CMDB.

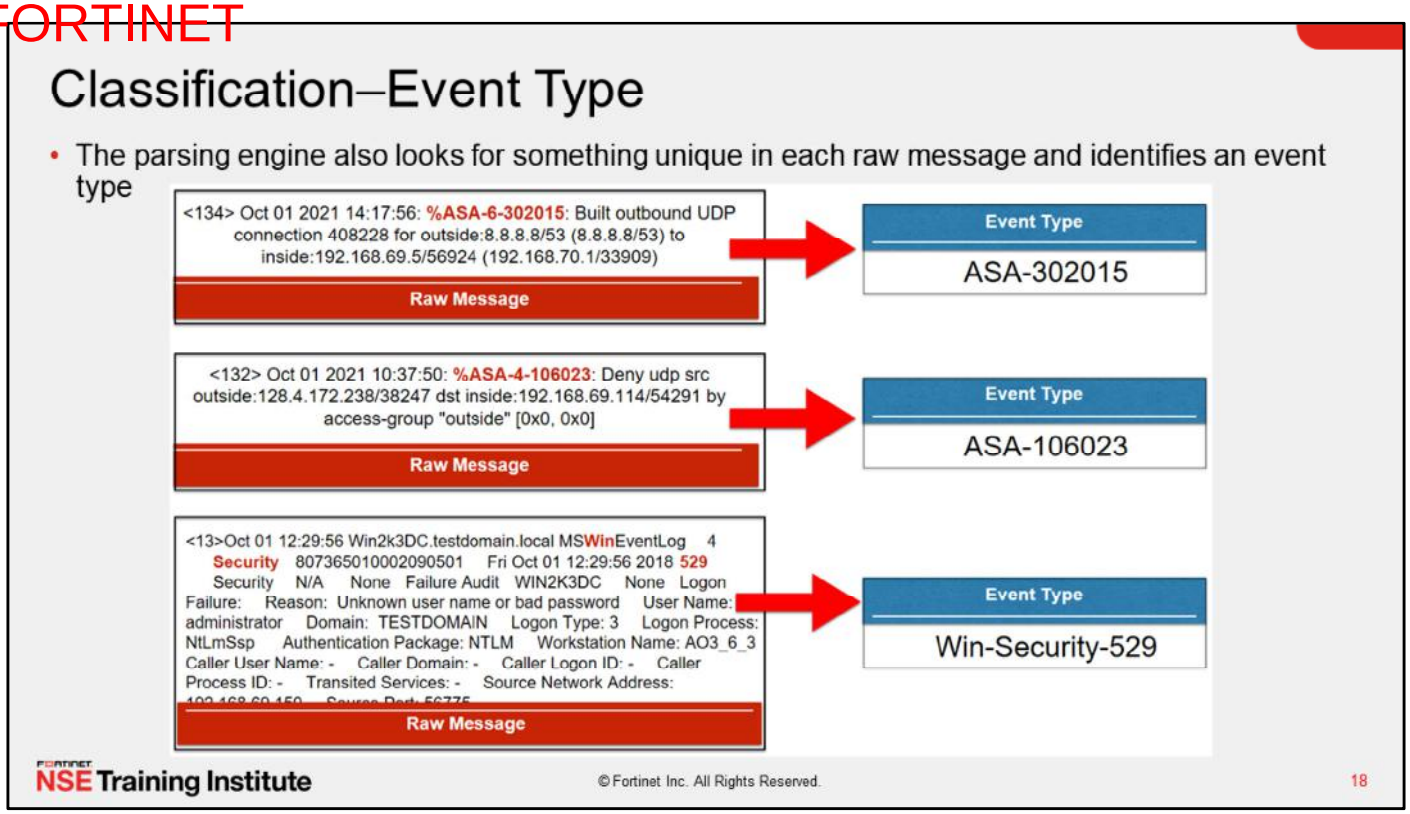
When FortiSIEM sees an external IP address referenced in a log, it looks up that IP address in the geolocation database. If there's information available, such as the destination country, destination city, destination organization, or any latitude and longitude coordinates, FortiSIEM adds that information, using the appropriate enrichment fields, to the structured data.

If the IP address referred to in the log is from a device within your organization, then it is an on-premise IP address. Obviously, this IP address will not be found in any external geolocation database. Administrators can set a location manually for each device in the CMDB. Location attributes include city, state, country, latitude, and longitude, to name a few. These fields would also be enriched in the structured data.

When structured data is enriched, it allows you to do very granular reporting, based on company location or country.

Vouchers & Dumps are Available | WhatsApp +201224560923

DO NOT REPRINT
© FORTINET
Brave-dumps.com

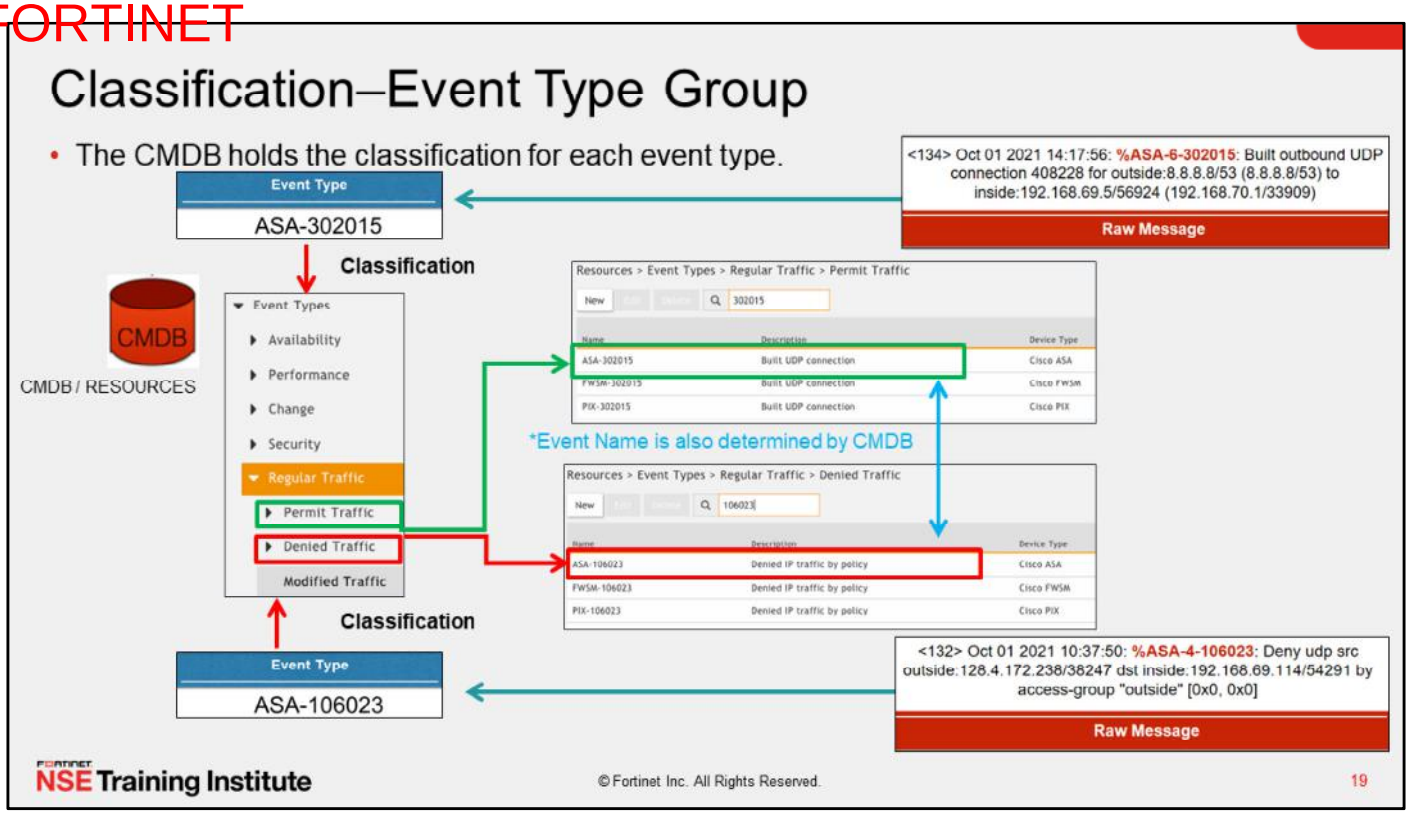


Another job of the parser is to give every message an event type. The parser looks for something unique in each message and assigns it an event identifier.

In the example shown on this slide, there are two different ASA messages: one of them is an outbound UDP connection message, the other is a deny UDP connection message. The parser looks for unique key words in the message to identify what kind of message it is. Cisco uses unique identifying numbers in their messages, so, in this example, the parser can use those numbers to identify the event types. Windows also uses unique IDs in their event logs, which the parser can use to assign an event identifier.

Vouchers & Dumps are Available | WhatsApp +201224560923

DO NOT REPRINT
© FORTINET
Brave-dumps.com



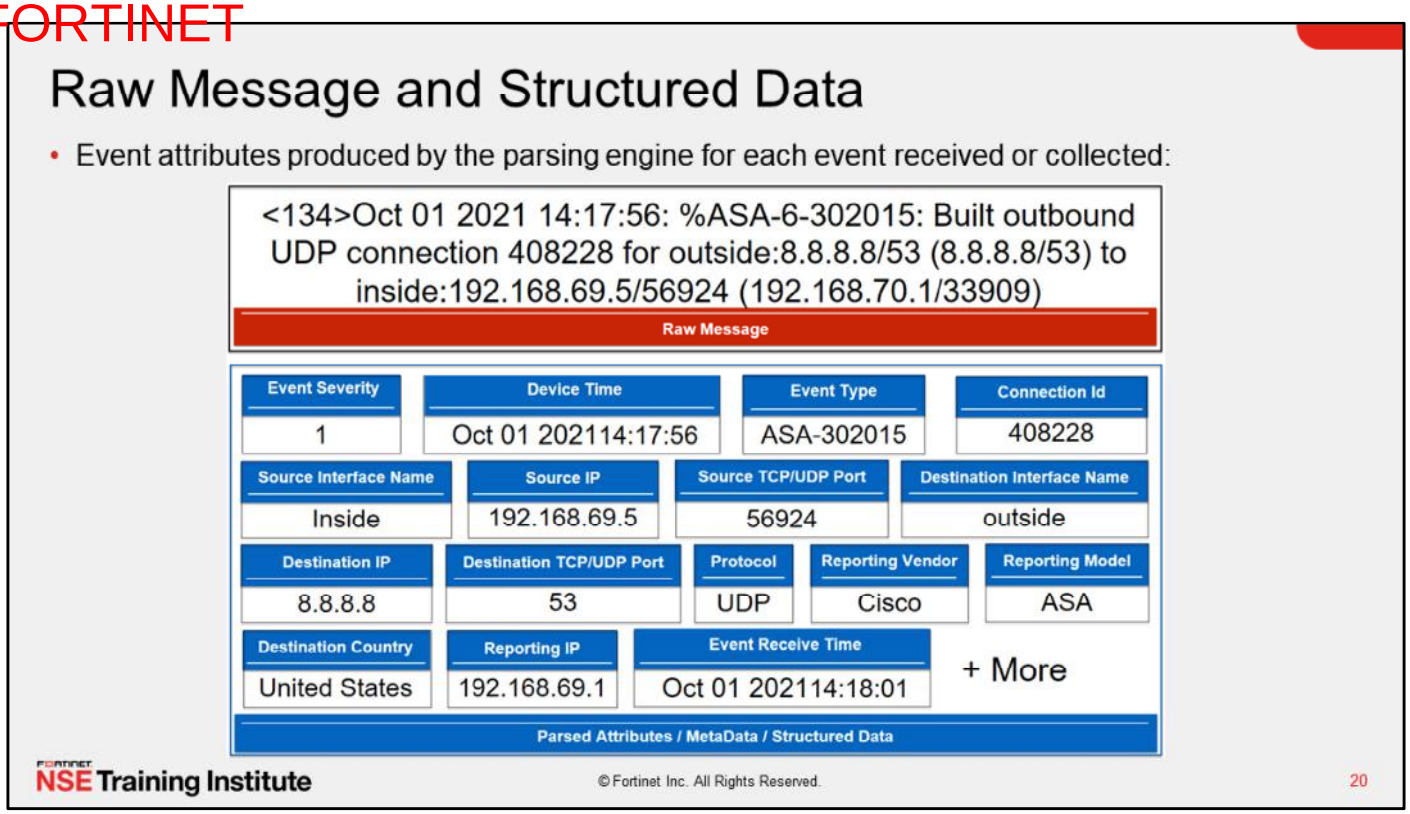
There are many different vendors that report messages to FortiSIEM. FortiSIEM understands over 100,000 different events reported by different applications, network devices, server devices, and so on. Many of these messages mean the same thing. If you consider regular traffic at a high level, it is either permitted traffic or denied traffic.

The CMDB holds the classification for each event type, and also groups them by event type.

Let’s return to the regular traffic example shown on this slide. You can see that the events are stored in their respective groups. These event type groups can be referenced later, in a search. For example, if you search for permitted traffic reported by a firewall, the system looks at all the different event types under that group in the CMDB, and reports on only those event types.

Vouchers & Dumps are Available | WhatsApp +201224560923

DO NOT REPRINT
© FORTINET
Brave-dumps.com



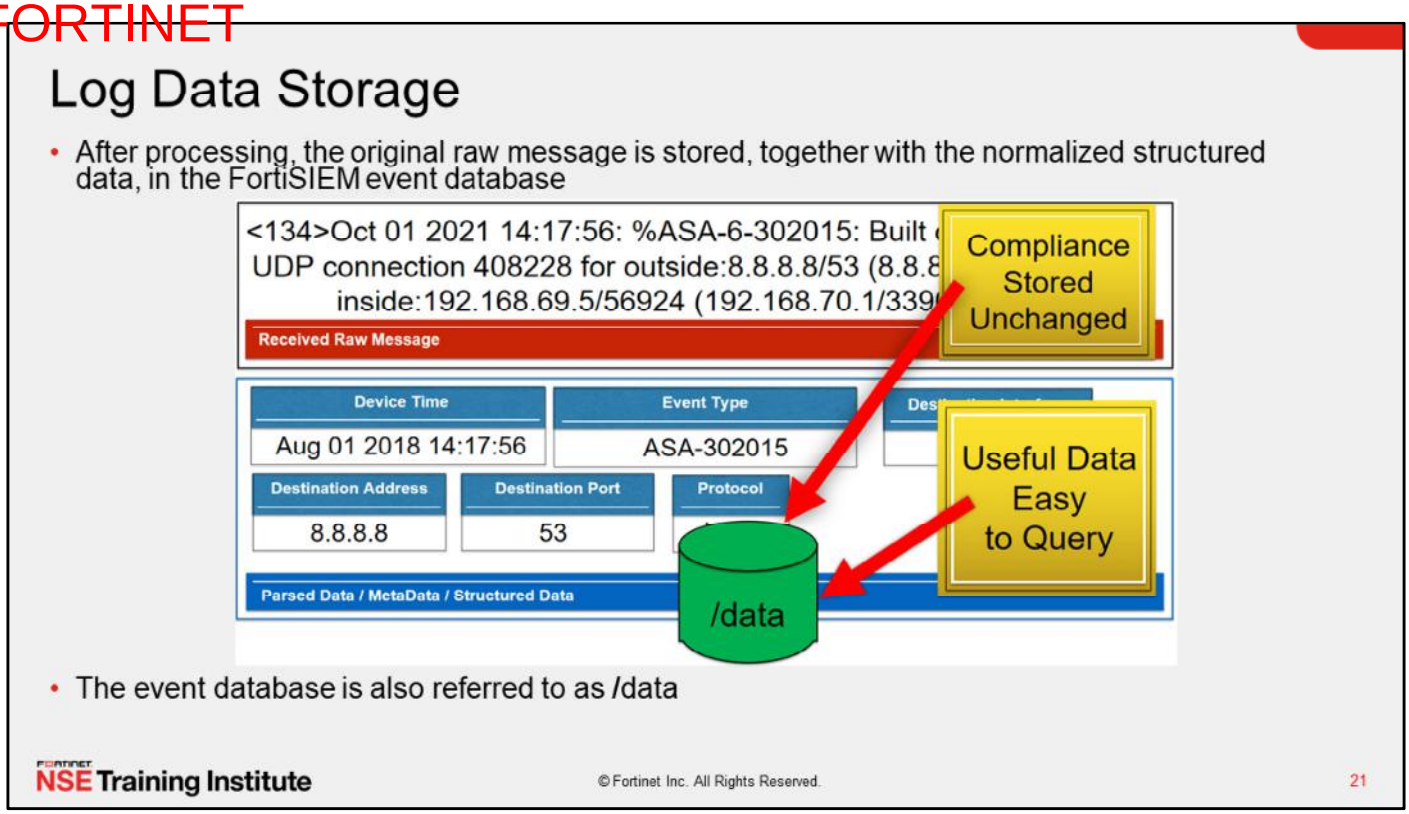
For each event, whether it was received or collected, the parsing engine takes the raw message, extracts everything it can from it, and creates a normalized, structured data event from it.

Some of the attributes in the final event come from the raw message itself, such as the time the event took place on the device, the source IP address, the destination IP address, and ports. Some attributes are added by the parsing engine, such as the timestamp indicating when the event was received, and the event type. Still more attributes are added through enrichment from the CMDB database or the geolocation database, such as the destination country.

In the end, the final event is enriched with far more data than was originally sent. All of this additional data makes searching, filtering, and reporting more granular than would be possible otherwise.

Vouchers & Dumps are Available | WhatsApp +201224560923

DO NOT REPRINT
© FORTINET
Brave-dumps.com



For compliance reasons, FortiSIEM can't change the original raw message. For that reason, the original raw message is stored, together with the normalized structured data, in the FortiSIEM event database. There are strict controls around the storage of that data. Checksums are performed on the data, and you can validate any changes to the data in the FortiSIEM GUI. The event database is also referred to as the /data partition in your FortiSIEM installation.

Vouchers & Dumps are Available | WhatsApp +201224560923

DO NOT REPRINT
© FORTINET
Brave-dumps.com

Knowledge Check

1. Which statement about raw logs is correct?
   - A. Raw logs can be altered after they have been received by FortiSIEM
   - ✓ B. Raw logs cannot be altered after they have been received by FortiSIEM

2. By default, on which port Syslogs can be sent to FortiSIEM?
   - A. UDP port 541
   - ✓ B. TCP port 514

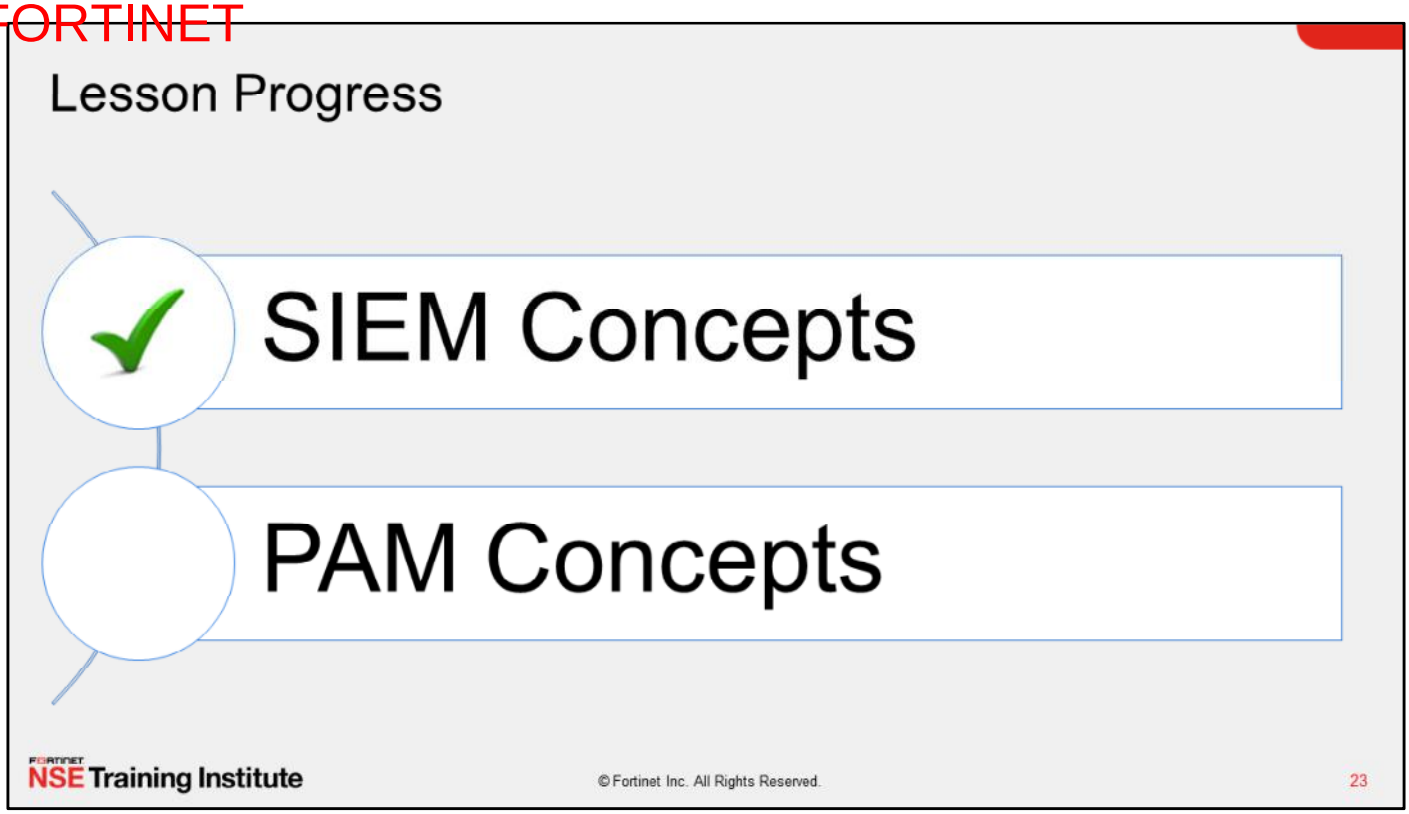
NSE Training Institute

© Fortinet Inc. All Rights Reserved.

22

Vouchers & Dumps are Available | WhatsApp +201224560923

DO NOT REPRINT
© FORTINET
Brave-dumps.com

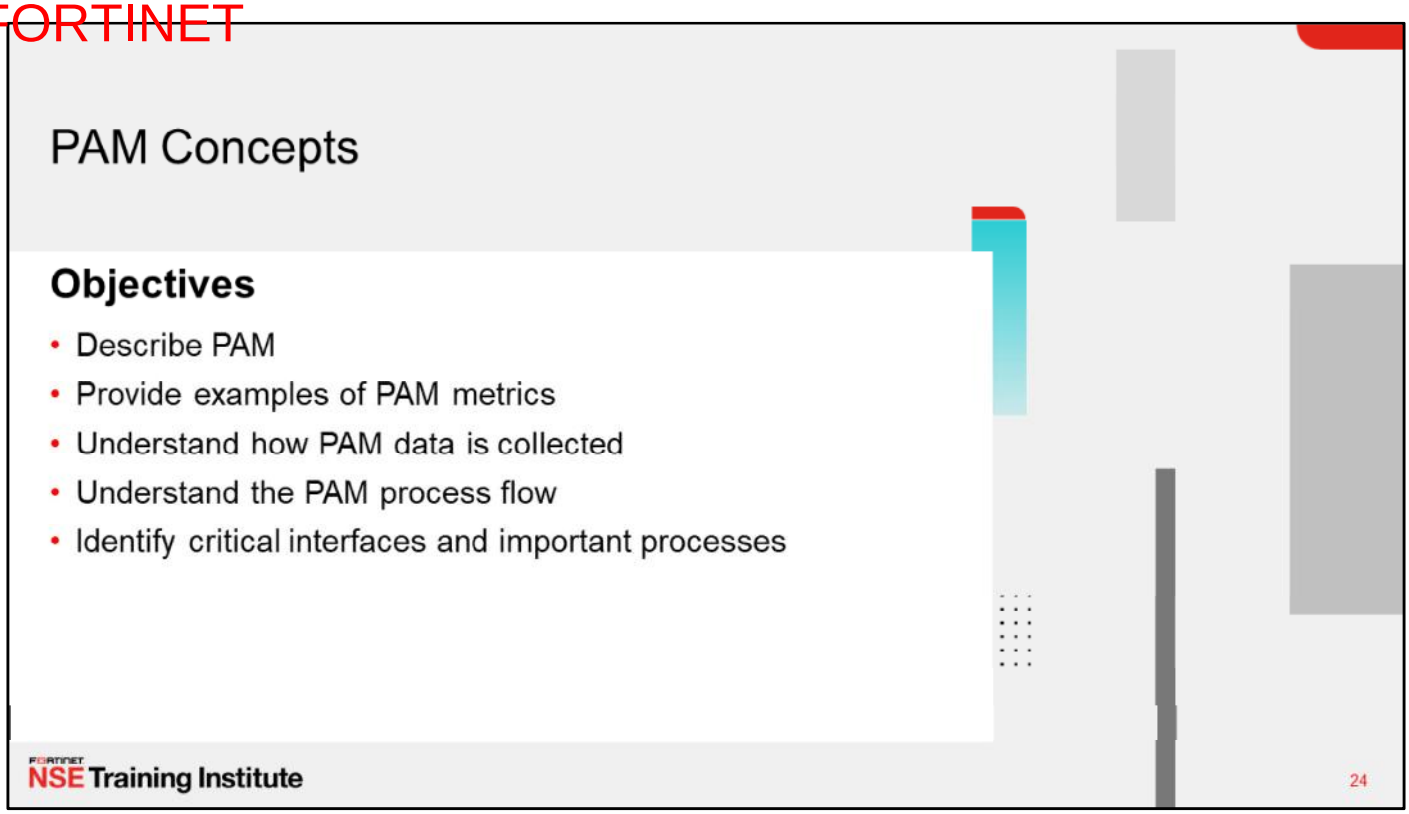


Good job! You now understand SIEM concepts.

Now, you'll learn about PAM concepts.

Vouchers & Dumps are Available | WhatsApp +201224560923

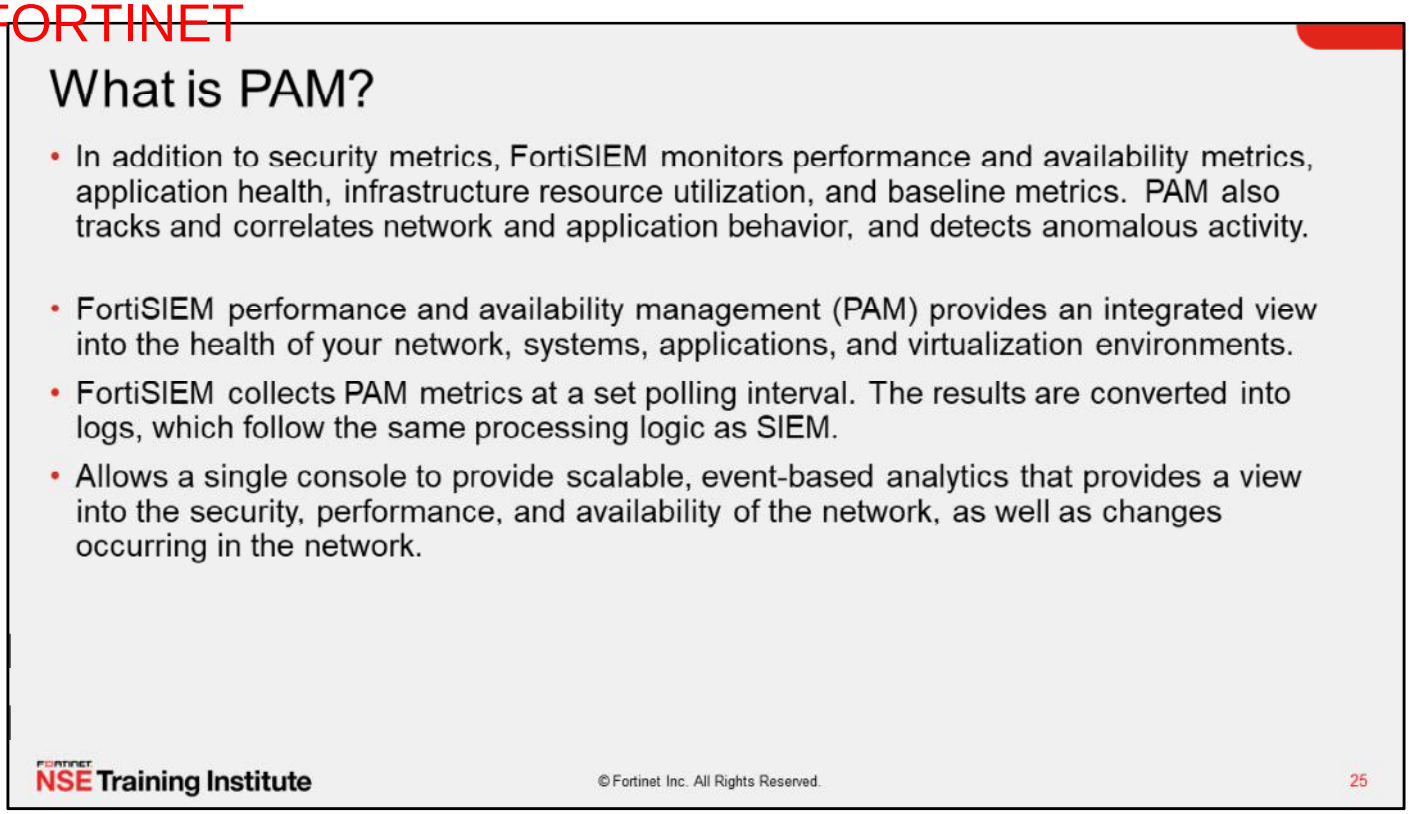
DO NOT REPRINT
© FORTINET
Brave-dumps.com



After completing this section, you should be able to achieve the objectives shown on this slide.
By understanding how the PAM process work and how PAM data is collected, you will be able to better understand the role that PAM processes play in your network.

Vouchers & Dumps are Available | WhatsApp +201224560923

DO NOT REPRINT
© FORTINET
Brave-dumps.com



FortiSIEM doesn't just collect security metrics, it also collects performance and availability information, from devices and applications.

FortiSIEM performance and availability management (PAM), provides an integrated view into the health of your network, systems, applications, and the virtualization environment.

Using all of this information, FortiSIEM builds a baseline of the network and application behaviors. Then, by continuously comparing what is currently happening in the network against the baseline, FortiSIEM can detect anomalous activity.

FortiSIEM collects the performance metrics at a set polling interval, and converts the metrics into logs following the same processing logic that is used for SIEM data.

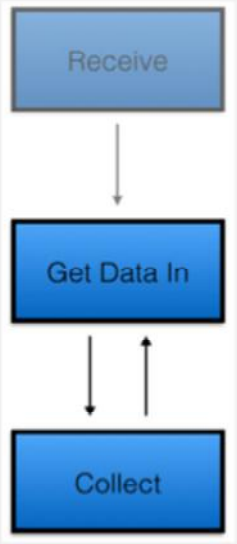
This process allows a single console to provide scalable, event-based analytics that provide a view into the security, performance, and availability of the network, as well as changes occurring in the network.

Vouchers & Dumps are Available | WhatsApp +201224560923

DO NOT REPRINT
© FORTINET
Brave-dumps.com

Collecting PAM Data

- FortiSIEM collects PAM data from devices and applications using various industry-standard protocols
- Examples:
  - ICMP
  - SNMP
  - WMI
  - Telnet/SSH
  - JDBC
  - JMX
- And vendor-specific APIs from VMware, NetApp, and so on



NSE Training Institute

© Fortinet Inc. All Rights Reserved.

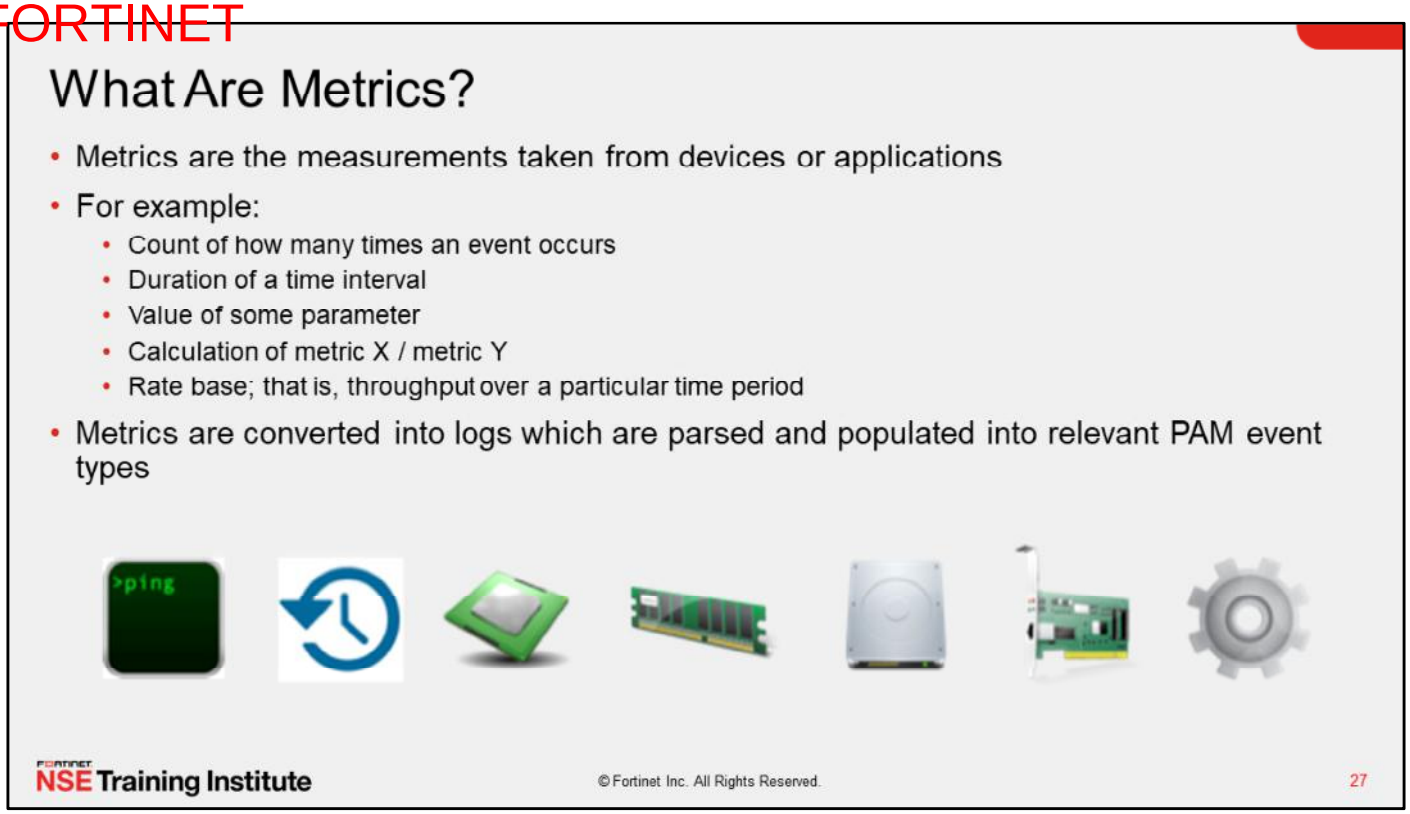
26

FortiSIEM collects PAM data from devices and applications using various industry-standard protocols.

For example:
- ICMP: Allows FortiSIEM to establish availability
- SNMP, WMI, Telnet, and SSH: Allow FortiSIEM to log into a device and run commands or pull network configurations
- JDBC and JMX
- Other vendor-specific APIs from VMware, NetApp, and so on

Vouchers & Dumps are Available | WhatsApp +201224560923

DO NOT REPRINT
© FORTINET
Brave-dumps.com



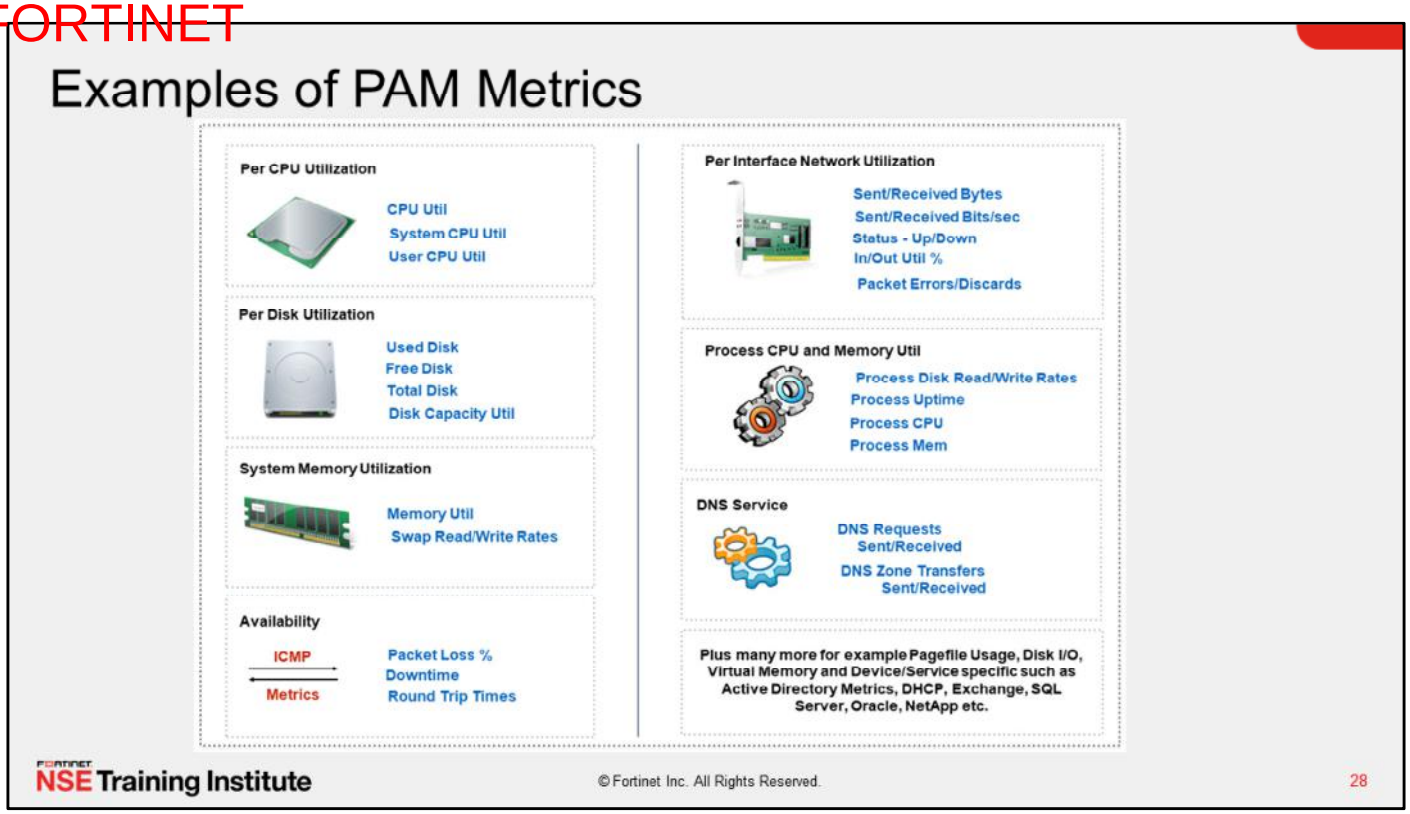
Metrics are measurements taken from devices or applications.
For example:

- Count of how many times an event occurs
- Duration of a time interval
- Value of some parameter
- Calculation of metric X / metric Y
- Rate base; that is, throughput over a particular time period

Metrics are converted into logs, which are parsed and populated into relevant PAM event types.

Vouchers & Dumps are Available | WhatsApp +201224560923

DO NOT REPRINT Brave-dumps.com
© FORTINET



Take a look at some examples of PAM metrics.

You poll devices to discover count, duration, value, and rate of things like the CPU, disks, memory, applications, and network interfaces.

For disks, for example, you might collect disk utilization metrics, such as total disk space, free disk space, used disk space, and read-write rates. Using these values, you can calculate a disk capacity utilization value. There is a set of each of these metrics for every disk on the device.

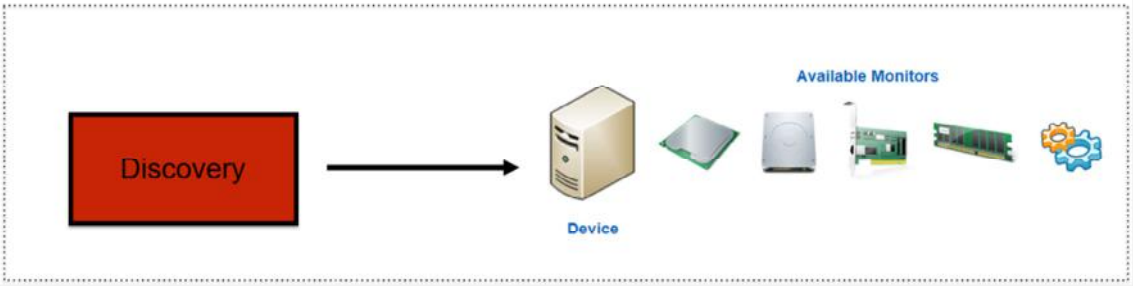
Similarly, for each network interface card on the device, you could collect sent and received bytes over a particular interval, the up and down status of each interface, and the packet errors and discards. If you find applications, such as a DNS services, running on any of those devices, you can poll application-based metrics, such as the number of sent and received DNS requests, or zone transfers. There are many more things you can poll metrics for, such as page file utilization, disc I/O, virtual memory, active directory metrics, DHCP, exchange, SQL, Oracle, and so on.

Vouchers & Dumps are Available | WhatsApp +201224560923

DO NOT REPRINT
© FORTINET
Brave-dumps.com

What PAM Metrics Are Collected for Each Device?

- The FortiSIEM discovery process determines the PAM metrics to be collected by the Performance Monitor



- Discovery uses information from various sources (such as SNMP, WMI, SSH, LDAP, VM SDK, and so on) and at various levels (such as physical, virtual, network, storage, user, application) and combines it to populate a CMDB that depicts an accurate picture of the infrastructure–not just of individual systems, but also of inter-relationships

NSE Training Institute
© Fortinet Inc. All Rights Reserved.
29

So, what metrics are collected for each device in your environment?

The FortiSIEM discovery process determines the PAM metrics to be collected by the Performance Monitor.

The discovery process uses credentials and various protocols such as SNMP, WMI, SSH, and at various levels, such as the physical, virtual, network, or storage level. The discovery process looks at the device and identifies what FortiSIEM can monitor on the device. It combines information from various sources and levels and uses that information to populate a CMDB that provides an accurate picture of the infrastructure, and not just individual systems, as well as the applications running on those systems, and the inter-relationships among devices.

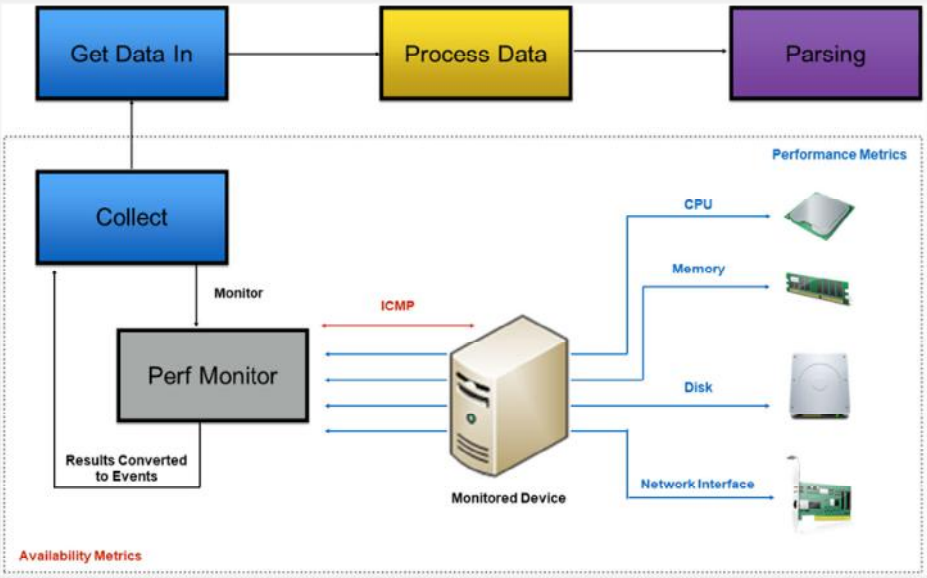
Most of the information in the CMDB is populated by this discovery process.

Vouchers & Dumps are Available | WhatsApp +201224560923

DO NOT REPRINT
© FORTINET
Brave-dumps.com

Availability and Performance Monitoring

- After discovery, the Performance Monitor module collects PAM metrics



NSE Training Institute

© Fortinet Inc. All Rights Reserved.

30

After the discovery process is completed, FortiSIEM knows which availability and performance metrics the Performance Monitor module can collect on each device.

This slide shows an example of a monitored device that FortiSIEM knows how to monitor.

The Performance Monitor can use ICMP for availability purposes. It also knows what metrics it can retrieve from things like the CPU, memory, hard drives, and network interface cords.

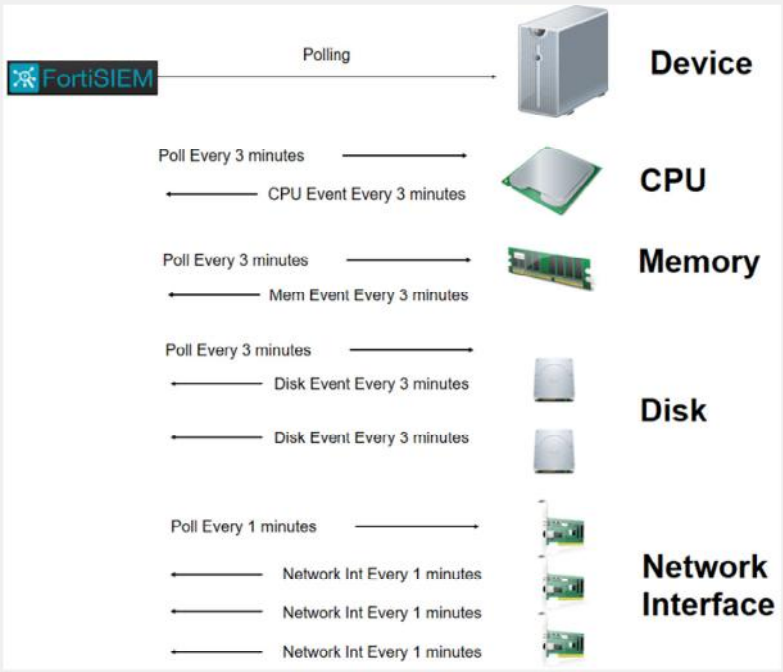
When the Performance Monitor polls these devices for those values, it converts the results into logs. The logs then go back in to the system and get converted into events in the same way a syslog message would.

Vouchers & Dumps are Available | WhatsApp +201224560923

DO NOT REPRINT Brave-dumps.com
© FORTINET

PAM Event Rates

- As discussed earlier, PAM metrics are collected on a polling interval, so the volume of data is a lot less than SIEM
- Some polls produce one event and others produce an event for each device object



NSE Training Institute

© Fortinet Inc. All Rights Reserved.

31

Now, you'll learn about performance and availability event rates.

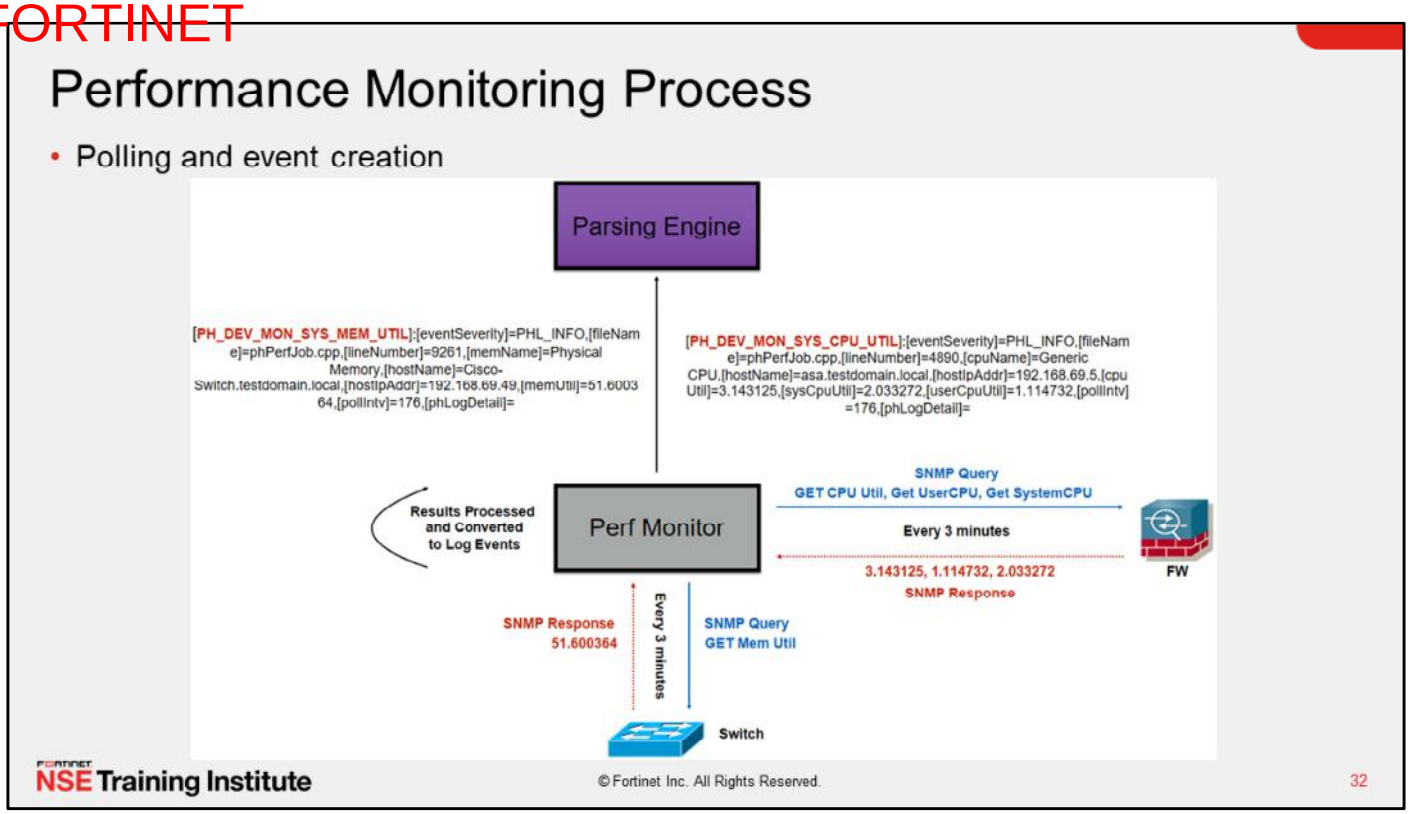
Performance data is collected at a set polling interval, so the volume of data received is a lot less than for SIEM events. Consider a firewall, for example. Traffic flows continuously across its interfaces, producing events that are then sent back to FortiSIEM. However, because PAM collection is performed at a set polling interval, every two or five minutes for example, the quantity of data that the Performance Monitor sends to FortiSIEM is a lot less.

It’s important to note that sometimes, when you poll a device for a specific metric, it may produce more than one event. For example, if you monitor a server that has a single disk, you’ll get a single disk event back every three minutes. However, if the server has ten disks, you’ll get ten events back when you poll the disk utilization on it because you’ll get an event back for every disk on the server.

The same thing applies to network devices. If you poll a router or a switch for its network interface utilization, and the router or switch has 14 interface cards, you’ll get back 14 events—one event for each interface.

Vouchers & Dumps are Available | WhatsApp +201224560923

DO NOT REPRINT
© FORTINET
Brave-dumps.com



Now, you will learn a little bit more about the performance monitoring process.

The role of the Performance Monitor is to collect various metrics from devices.

In the example shown on this slide, the Performance Monitor is configured to poll the firewall for CPU utilization. It sends an SNMP query to the firewall requesting the total CPU utilization, the system CPU utilization, and the user CPU utilization, and gets the three values back. Then, the Performance Monitor converts this information into a log and sends the log to the parsing engine. The parsing engine processes the log into an event.

In the example shown on this slide, the Performance Monitor created the log `PH_DEV_MON_SYS_CPU_UTIL` and populated it with the information the parser needs to create an event—the name and IP address of the device, the CPU name, and the CPU values returned by the poll.

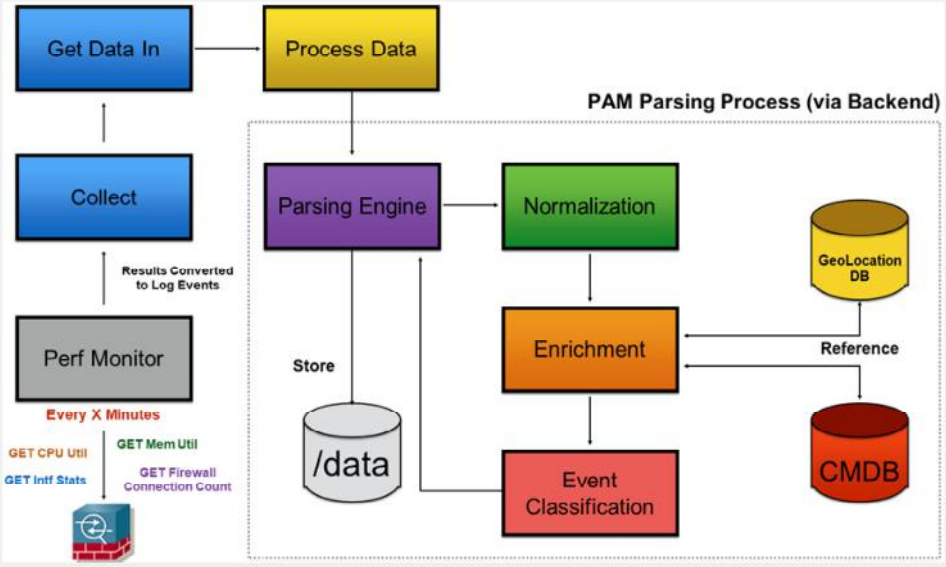
Similarly, for the switch shown on this slide, the Performance Monitor performed an SNMP query for the switch's memory utilization and received the values. The Performance Monitor converted the information into a log, `PH_DEV_MON_SYS_MEM_UTIL`, which will also be processed into an event by the parsing engine.

Vouchers & Dumps are Available | WhatsApp +201224560923

DO NOT REPRINT
© FORTINET
Brave-dumps.com

PAM Process Flow

- After data collection, the events are parsed, just like SIEM



NSE Training Institute

© Fortinet Inc. All Rights Reserved.

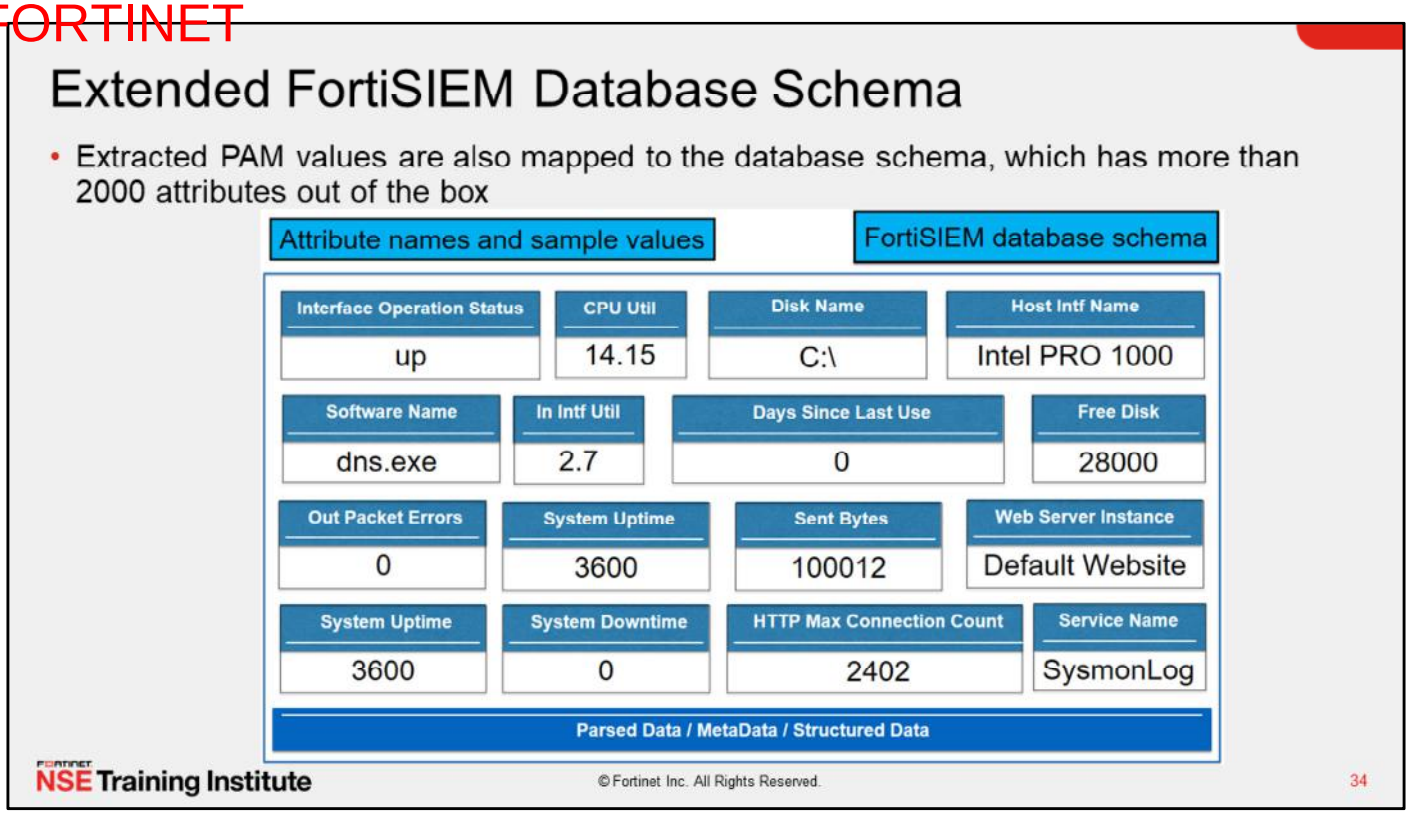
33

Now, you will look at the PAM process flow as a whole.

In the lower-left corner of the example shown on this slide, the Performance Monitor is polling a device periodically. The Performance Monitor collects the returned information and processes it into a log. From this point on, the log that the Performance Monitor created is treated just like any other SIEM message. The parsing engine takes the raw log, normalize it into an event, adds any enrichments that it can, classifies the event, and, finally, stores the event in the event database.

Vouchers & Dumps are Available | WhatsApp +201224560923

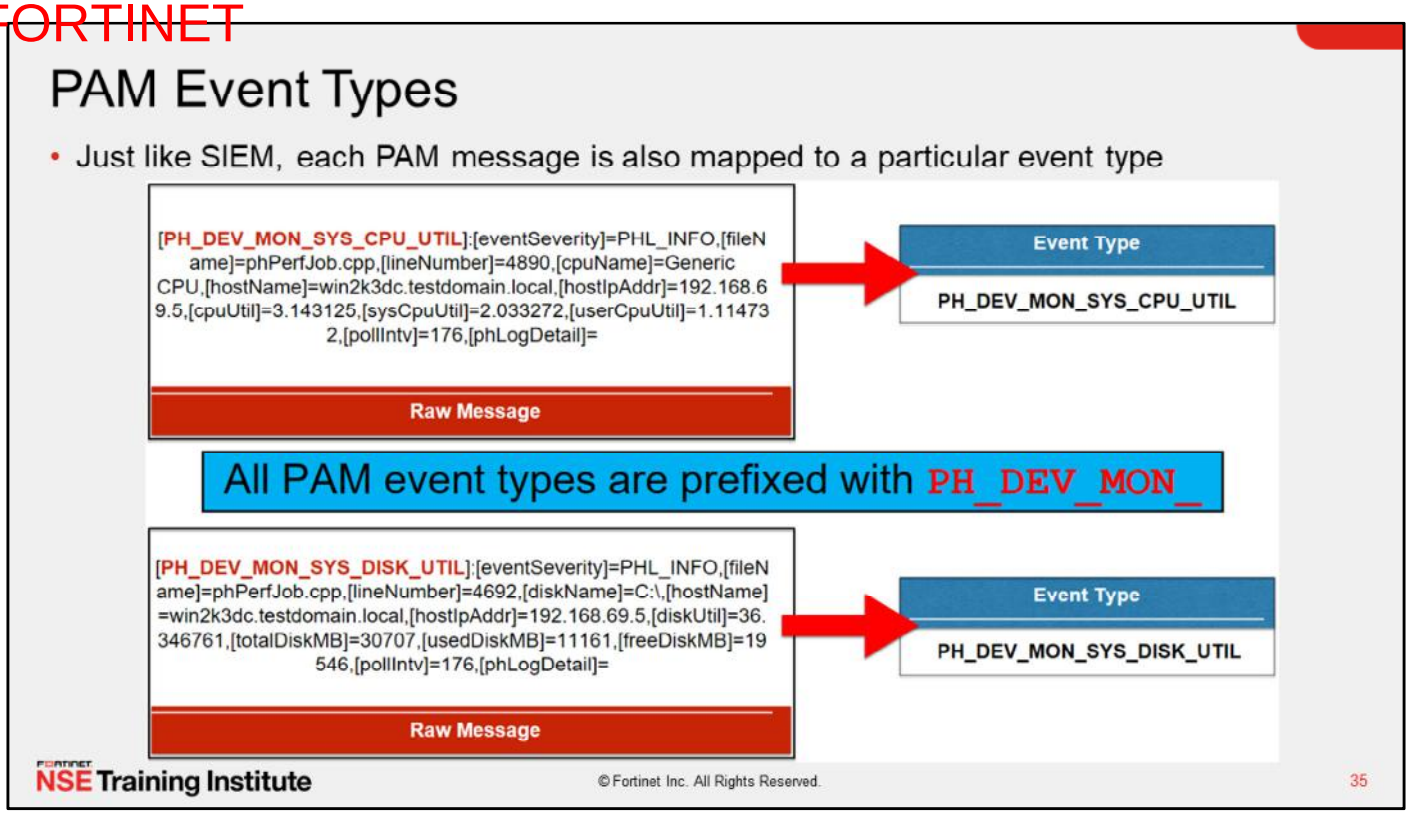
DO NOT REPRINT
© FORTINET
Brave-dumps.com



In the last step on the previous slide, the parsing engine extracted the PAM values and mapped them to the FortiSIEM database schema. There are more than 2000 attributes that you can use to map this data. If an appropriate field is not available, it is very easy to extend the database schema and add additional fields.

Vouchers & Dumps are Available | WhatsApp +201224560923

DO NOT REPRINT
© FORTINET
Brave-dumps.com



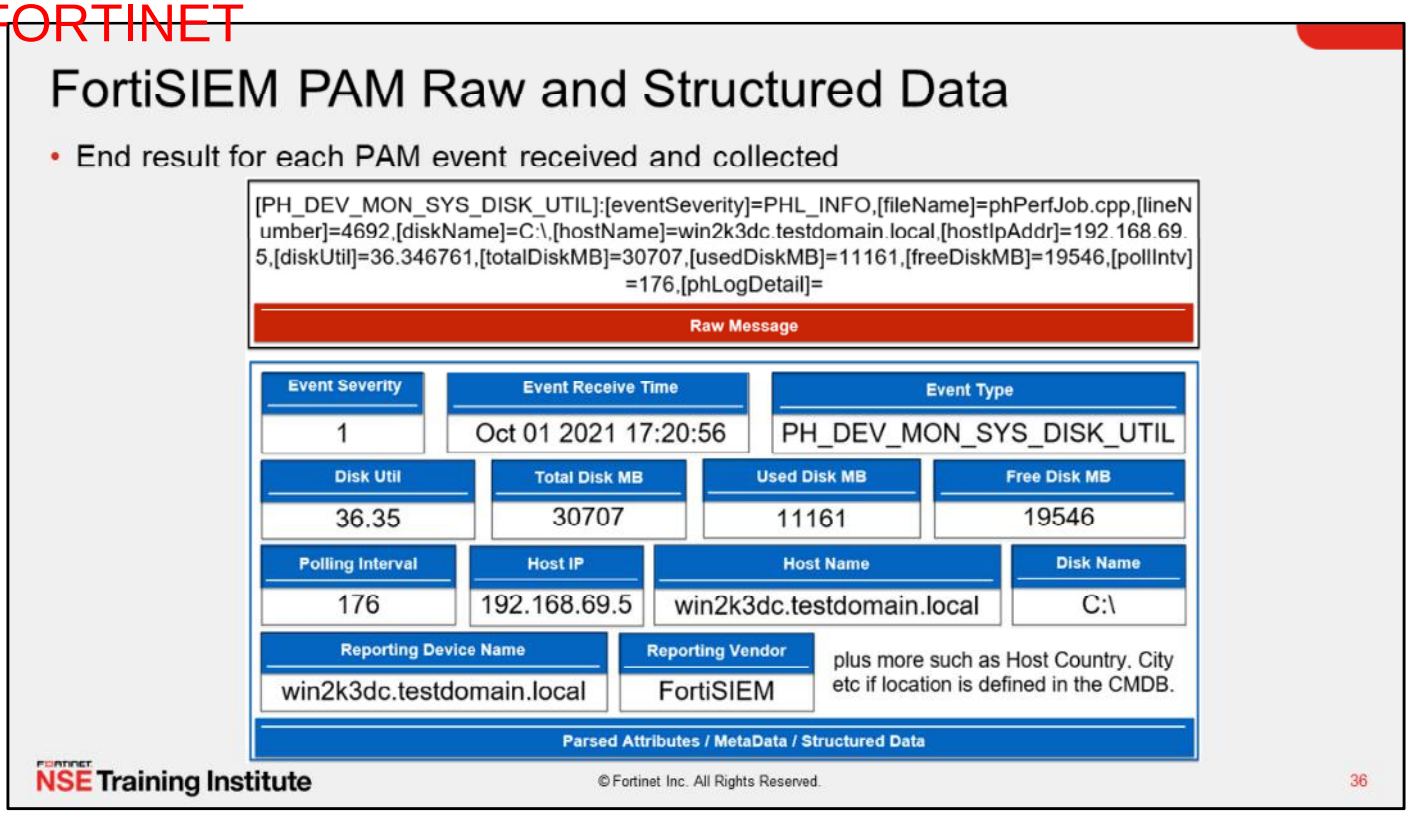
Just like SIEM, each performance and availability message is also mapped to a particular event type.

The example shown on this slide shows a system CPU utilization event that is mapped to the event type `PH_DEV_MON_SYS_CPU_UTIL`, and a disk utilization event that is mapped to the event type `PH_DEV_MON_SYS_DISK_UTIL`.

All performance events have the prefix of `PH_DEV_MON`, which means a device monitoring event, or, put another way, an event derived from a Performance Monitoring poll.

Vouchers & Dumps are Available | WhatsApp +201224560923

DO NOT REPRINT
© FORTINET
Brave-dumps.com



In the example shown on this slide, a Windows server was polled for its disk utilization. The Performance Monitor then converted that information into a log and sent it to the parsing engine.

The result of a PAM log is the same as any log message that is sent to the parsing engine: the parsing engine normalizes and extracts the relevant information, and maps it to the appropriate attributes in the events database, along with a copy of the original raw message.

It is important to note that the original raw message is always saved for compliance and forensic reasons.

Vouchers & Dumps are Available | WhatsApp +201224560923

DO NOT REPRINT
© FORTINET
Brave-dumps.com

Sample Disk Utilization Event

- Event Type = PH_DEV_MON_SYS_DISK_UTIL
- Description: Event contains disk utilization metrics



Useful Attributes	Description
Host IP	Access IP of the device whose Disk utilization is being reported
Host Name	Host name of the device
Event Receive Time	Time at which FortiSIEM generated this event
Disk Name	The Disk Name
Free Disk (MB)	Size of free disk available in Megabytes
Used Disk (MB)	Size of used disk in Megabytes
Total Disk (MB)	Size of total disk in Megabytes
Disk Capacity Util	Disk utilization for a specific disk name (between 0-100).

NSE Training Institute

© Fortinet Inc. All Rights Reserved.

37

The example shown on this slide is a disk utilization event.

The event type is PH_DEV_MON_SYS_DISK_UTIL, and it contains disk utilization metrics.

Some of the useful attributes for this event type are: the name of the disk, free disk space, used disk space, and total disk size. Each of these values is expressed in megabytes. Using these metrics, FortiSIEM calculates a disk capacity utilization value for each disk in the system, which is an example of the enrichment capabilities of FortiSIEM.

This event is produced for every disk on a system.

Vouchers & Dumps are Available | WhatsApp +201224560923

DO NOT REPRINT
© FORTINET
Brave-dumps.com

Sample CPU Utilization Event



- Event Type = `PH_DEV_MON_SYS_CPU_UTIL`
- Description: Event contains CPU utilization metrics

Useful Attributes	Description
Host IP	Access IP of the device whose CPU utilization is being reported
Host Name	Host name of the device
Event Receive Time	Time at which FortiSIEM generated this event
CPU Util	Overall CPU utilization (between 0-100). The number is an average over all CPUs in a multi-cpu system.
System CPU Util	System CPU utilization (between 0-100). The number is an average over all CPUs in a multi-cpu system.
User CPU Util	User CPU utilization (between 0-100). The number is an average over all CPUs in a multi-cpu system.

- **Note**: There is also a `PH_DEV_MON_SYS_PER_CPU_UTIL` event for each CPU in the device

NSE Training Institute

© Fortinet Inc. All Rights Reserved.

38

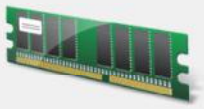
The example shown on this slide is a CPU utilization event.

The event type is `PH_DEV_MON_SYS_CPU_UTIL`, and it contains CPU utilization metrics.

Vouchers & Dumps are Available | WhatsApp +201224560923

DO NOT REPRINT
© FORTINET
Brave-dumps.com

Sample Memory Utilization Event



- Event Type = `PH_DEV_MON_SYS_MEM_UTIL`
- Description: Event containing system memory utilization metrics

```
[PH_DEV_MON_SYS_MEM_UTIL]:[eventSeverity]=PHL_INFO,[fileName]=phPerfJob.cpp,[lineNumber]=5152,[m
emName]=PhysicalMemory,[hostName]=WIN2K8DC,[hostIpAddr]=192.168.69.6,[memUtil]=29.084249,[swapIn
Rate]=59.021473,[swapOutRate]=0.005670,[swapRate]=59.027144,[pollIntv]=176,[phLogDetail]=
```

Useful Attributes	Description
Host IP	Access IP of the device whose Mem utilization is being reported
Host Name	Host name of the device
Event Receive Time	Time at which FortiSIEM generated this event
Memory Util	Overall system physical memory utilization (between 0-100).
Swap Read Rate (Pages/sec)	Rate at which pages are swapped in.
Swap Write Rate (Pages/sec)	Rate at which pages are swapped out.
Total Swap Rate (Pages/sec)	Total of the Swap Rates

NSE Training Institute

© Fortinet Inc. All Rights Reserved.

39

The example shown on this slide is a memory utilization event.

The event type is `PH_DEV_MON_SYS_MEM_UTIL`, and it contains memory utilization metrics.

Vouchers & Dumps are Available | WhatsApp +201224560923

DO NOT REPRINT
© FORTINET
Brave-dumps.com

Sample Ping Stat Event

- Event Type = PH_DEV_MON_PING_STAT
- Description: event containing ping stat metrics




```
[PH_DEV_MON_PING_STAT]:[eventSeverity]=PHL_INFO,[fileName]=phPerfMonitor.cpp,[lineNumber]=2743,[ho
stName]=ASA.testdomain.local,[hostIpAddr]=192.168.69.1,[avgDurationMSec]=0,[minDurationMSec]=0,[ma
xDurationMSec]=0,[pktLossPct]=0.000000,[sysDownTime]=0,[sysDegradedTime]=0,[pollIntv]=120,[phLogDe
tail]=
```

Useful Attributes	Description
Host IP	Access IP of the device whose Packet Loss is being reported
Host Name	Host name of the device
Event Receive Time	Time at wFortiSIEMOps generated this event
Packet Loss Pct	Packet loss percentage from the ping tests done during this interval
Min Round Trip Time	Min Round trip time from the ping tests done during this interval
Max Round Trip Time	Max Round trip time from the ping tests done during this interval
System Down Time	Amount of time during this polling interval that there was 100% ping loss
System Degraded Time	Amount of time during this polling interval that there was 50%+ ping loss

NSE Training Institute

© Fortinet Inc. All Rights Reserved.

40

The example shown on this slide is a ping stat event.

The event type is PH_DEV_MON_PING_STAT, and it contains ping stat metrics.

Vouchers & Dumps are Available | WhatsApp +201224560923

DO NOT REPRINT
© FORTINET
Brave-dumps.com

Sample Network Interface Utilization Event



- Event Type = PH_DEV_MON_NET_INTF_UTIL
- Description: Event containing network interface utilization metrics

```
[PH_DEV_MON_NET_INTF_UTIL]:[eventSeverity]=PHL_INFO,[fileName]=phPerfJob.cpp,[lineNumber]=6646,[int
fName]=Intel[R] PRO_1000 MT Network
Connection,[intfAlias]=,[hostName]=WIN2K8DC,[hostIpAddr]=192.168.69.6,[pollIntv]=56,[recvBytes64]=4
4273,[recvBitsPerSec]=6324.714286,[inIntfUtil]=0.000632,[sentBytes64]=82014,[sentBitsPerSec]=11716.
285714,[outIntfUtil]=0.001172,[recvPkts64]=449,[sentPkts64]=255,[inIntfPktErr]=0,[inIntfPktErrPct]=
0.000000,[outIntfPktErr]=0,[outIntfPktErrPct]=0.000000,[inIntfPktDiscarded]=0,[inIntfPktDiscardedPc
t]=
```

Useful Attributes	Description
Host IP	Access IP of the device whose Interface utilization is being reported
Host Name	Host name of the device
Event Receive Time	Time at which FortiSIEM generated this event
Host Intf Name	The name of the network interface for which this statistics applies
Interface Operational Status	Running state of the interface

NSE Training Institute

© Fortinet Inc. All Rights Reserved.

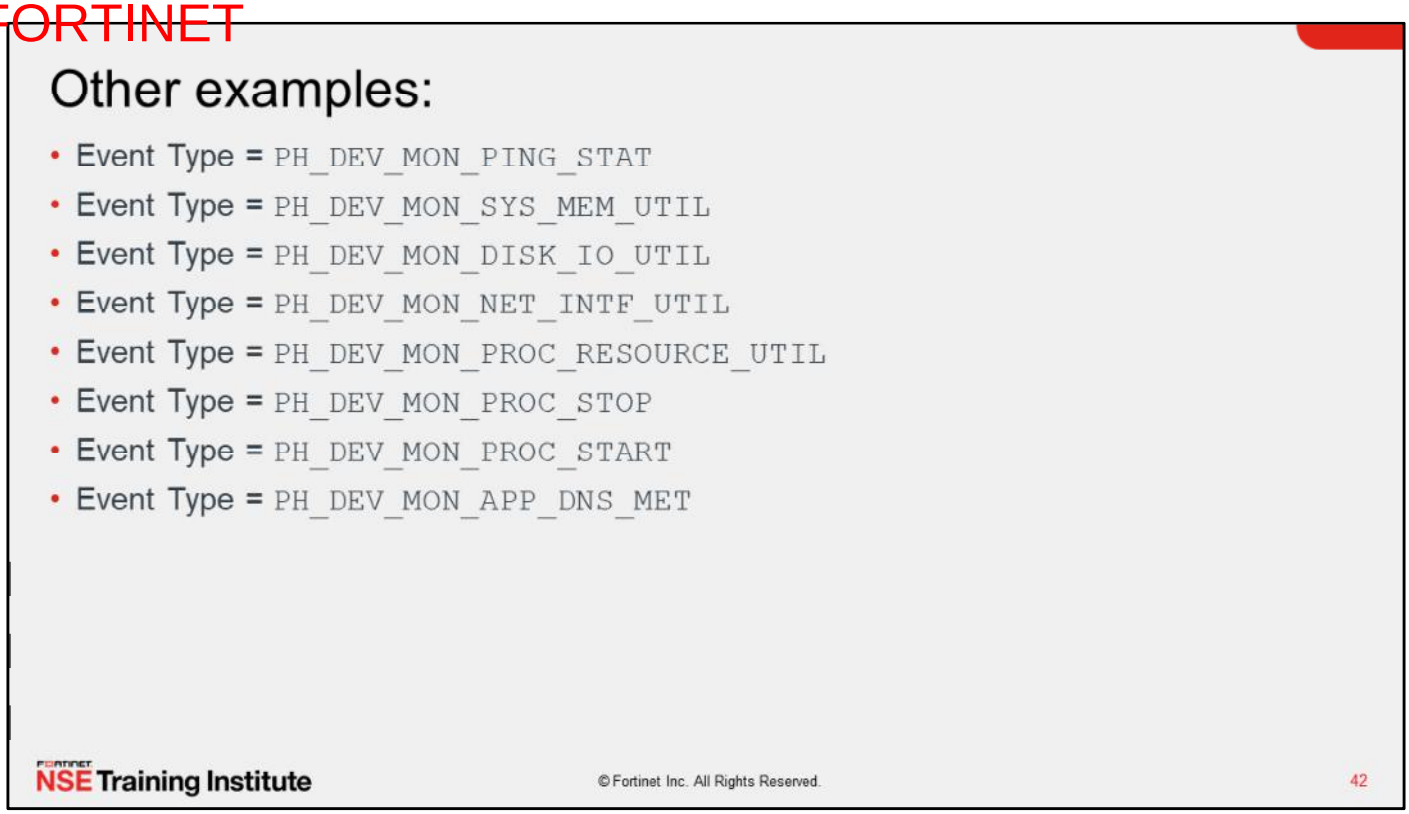
41

The example shown on this slide is a network interface utilization event.

The event type is PH_DEV_MON_NET_INTF_UTIL, and it contains network interface utilization metrics.

Vouchers & Dumps are Available | WhatsApp +201224560923

DO NOT REPRINT
© FORTINET
Brave-dumps.com



There are many more event types.

The ping stat even type is used to identify if a device is up or down. There are also event types for hardware components, such as CPU, disk, and network interface cards.

There are some event types that get metrics on processes, and can tell you if a specific process was started or stopped.

There are even event types for applications, such as DNS, DHCP, IIS, and SQL.

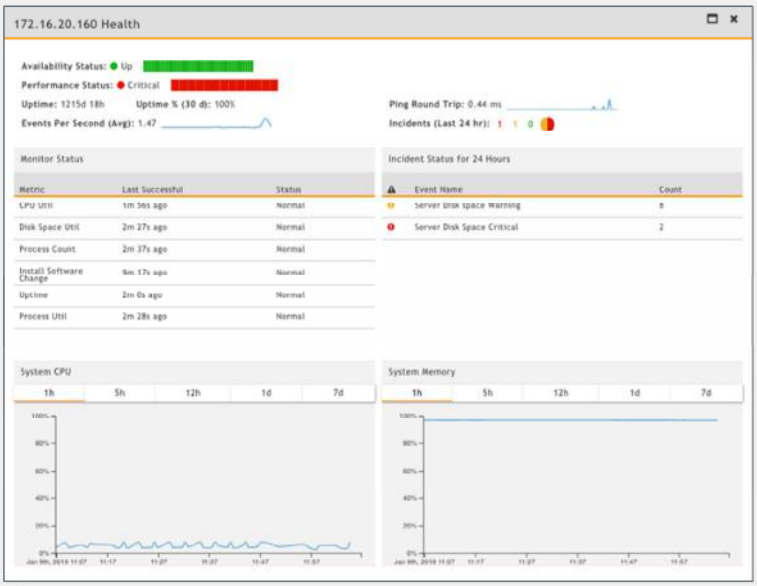
There is an event type for almost any metric you want to collect, and each event type has unique attributes for its particular function.

Vouchers & Dumps are Available | WhatsApp +201224560923

DO NOT REPRINT
© FORTINET
Brave-dumps.com

PAM Data Visualized on the GUI

- In the CMDB and dashboards



NSE Training Institute

© Fortinet Inc. All Rights Reserved.

43

You can view all of the PAM metrics collected by the Performance Monitor using widgets on the dashboard. You can also use the metrics as search criteria, and in your reports.

Vouchers & Dumps are Available | WhatsApp +201224560923

DO NOT REPRINT
© FORTINET
Brave-dumps.com

Knowledge Check

1. What kind of PAM event is this?

```
[PH_DEV_MON_HW_TEMP]:[eventSeverity]=PHL_INFO,[fileName]=deviceCiscoIOS.cpp,[lineNumber]=2318,[hostName]=CiscoSwitch.testdomain.local.testdomain.local,[hostIpAddr]=192.168.69.49,[hwComponentName]=chassis,[envTempDegC]=0,[envTempHighThreshDegC]=0,[envTempOffHighDegC]=0,[envTempDegF]=26,[envTempHighThreshDegF]=26,[envTempOffHighDegF]=0,[phLogDetail]=
```

✓A. Device hardware temperature
B. Device disk utilization

2. What kind of PAM event is this?

```
[PH_DEV_MON_DATASTORE_UTIL]:[eventSeverity]=PHL_INFO,[datacenter]=hadatacenter,[datastore]=datastore1,[datastoreType]=VMFS,[diskUtil]=77.76,[totalDiskMB]=147456.0,[freeDiskMB]=32795.0,[usedDiskMB]=114661.0,[hostIpAddr]=192.168.69.3,[relayDevIpAddr]=192.168.69.3
```

A. Hyper V datastore utilization
B. Device disk utilization
✓C. VMware datastore utilization

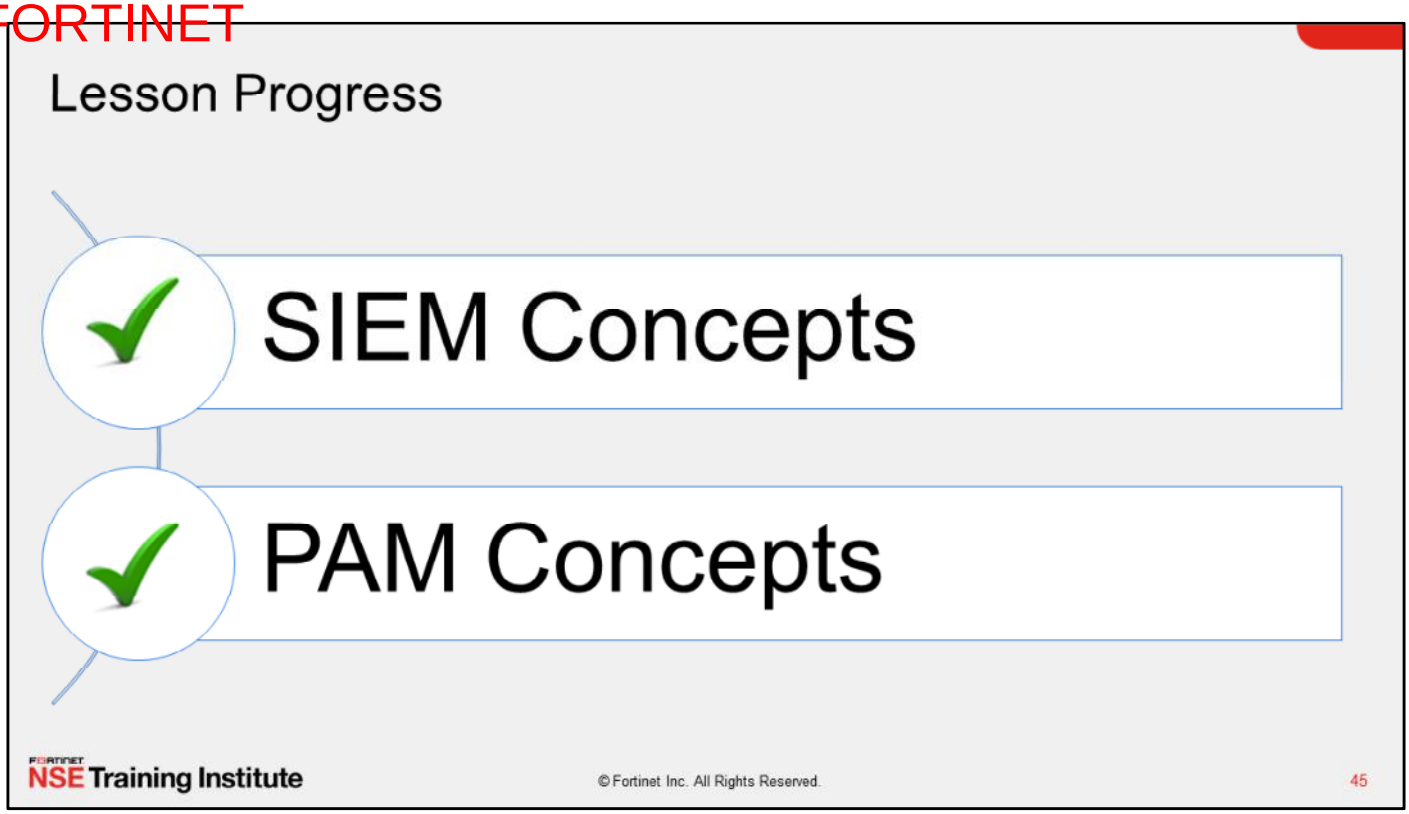
NSE Training Institute

© Fortinet Inc. All Rights Reserved.

44

Vouchers & Dumps are Available | WhatsApp +201224560923

DO NOT REPRINT
© FORTINET
Brave-dumps.com

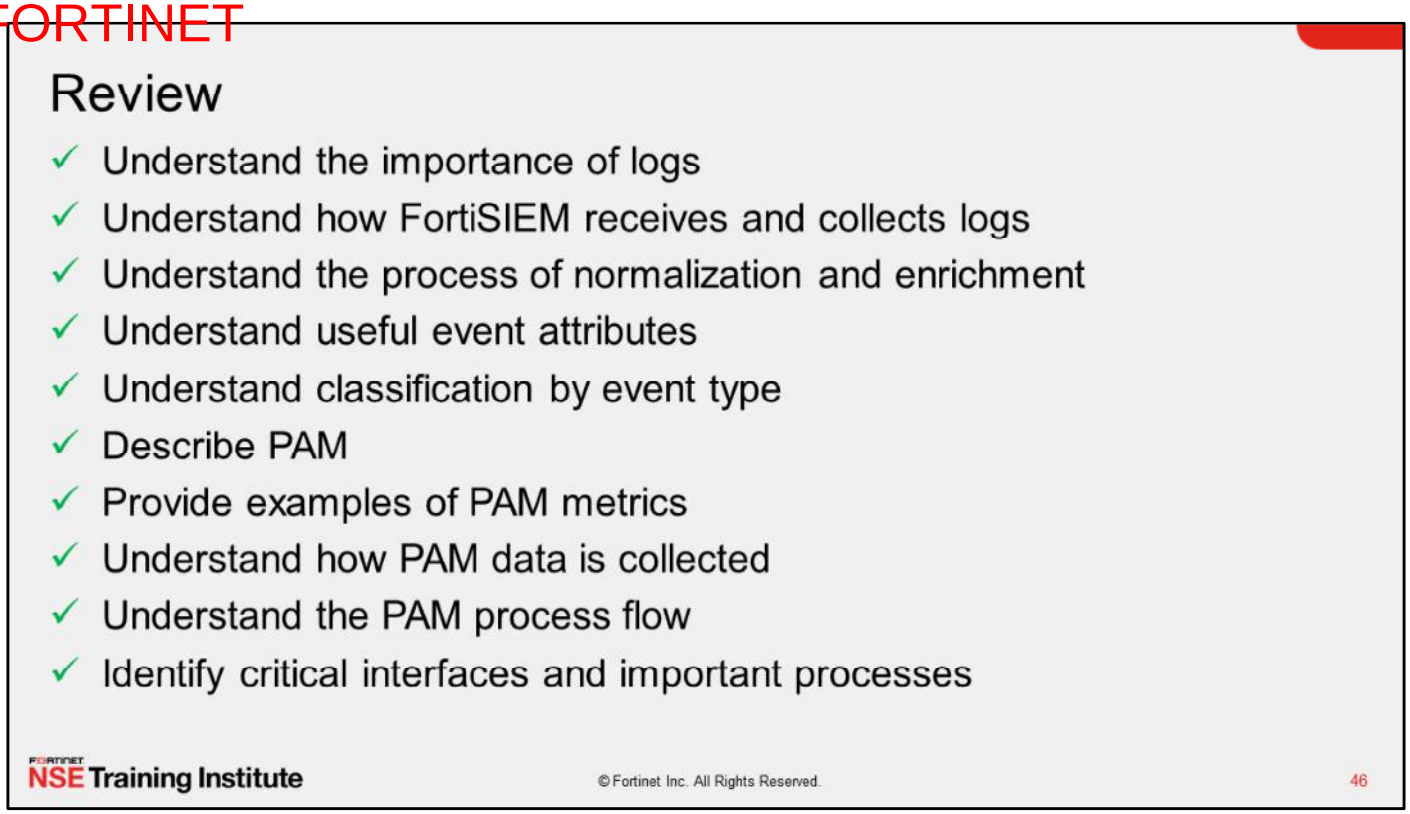


Congratulations! You have completed this lesson.

Now, you will review the objectives that you covered in this lesson.

Vouchers & Dumps are Available | WhatsApp +201224560923

DO NOT REPRINT
© FORTINET
Brave-dumps.com

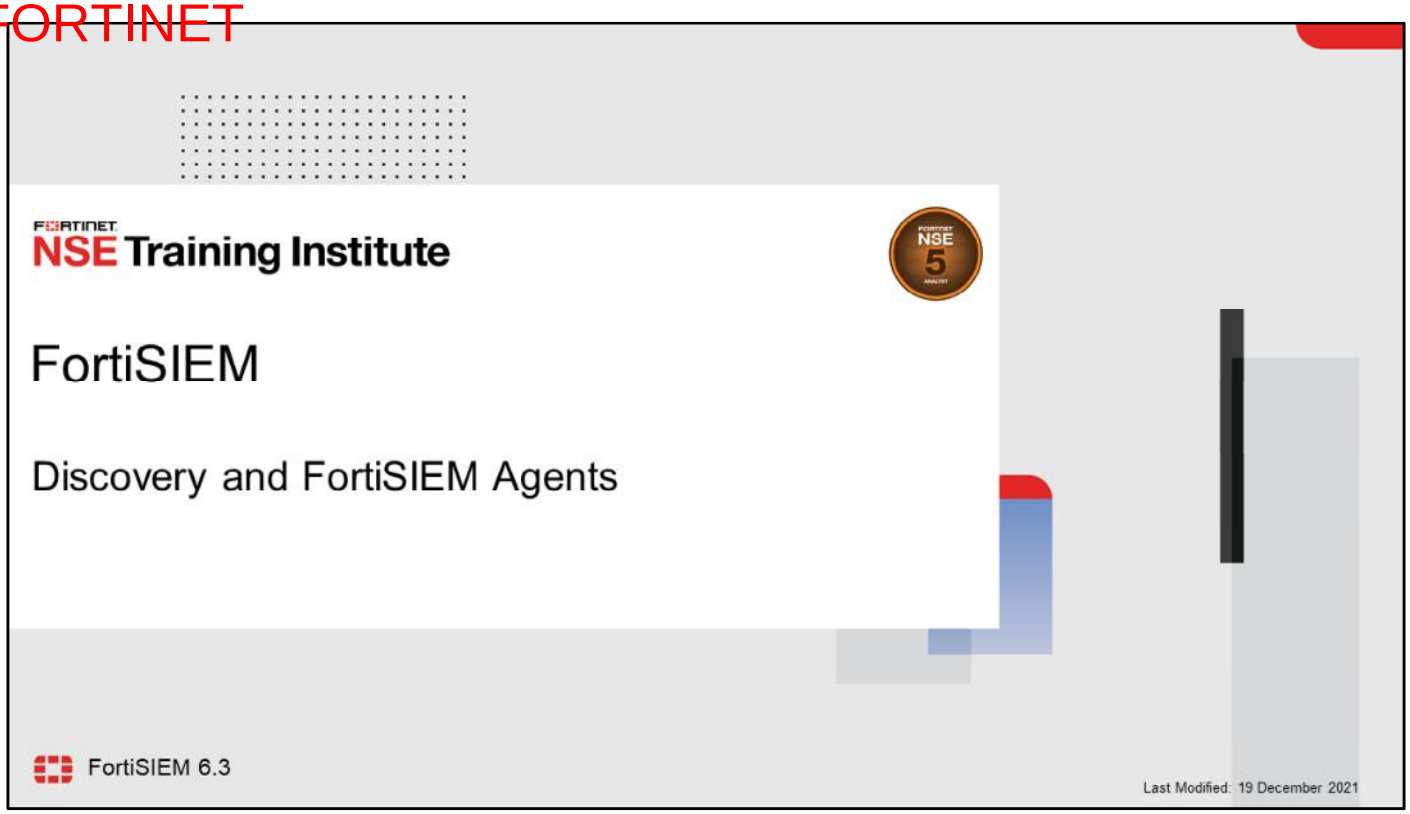


This slide shows the objectives that you covered in this lesson.

By mastering the objectives covered in this lesson, you learned how FortiSIEM receives, collects, and normalized logs, and how PAM data is collected and processed.

Vouchers & Dumps are Available | WhatsApp +201224560923

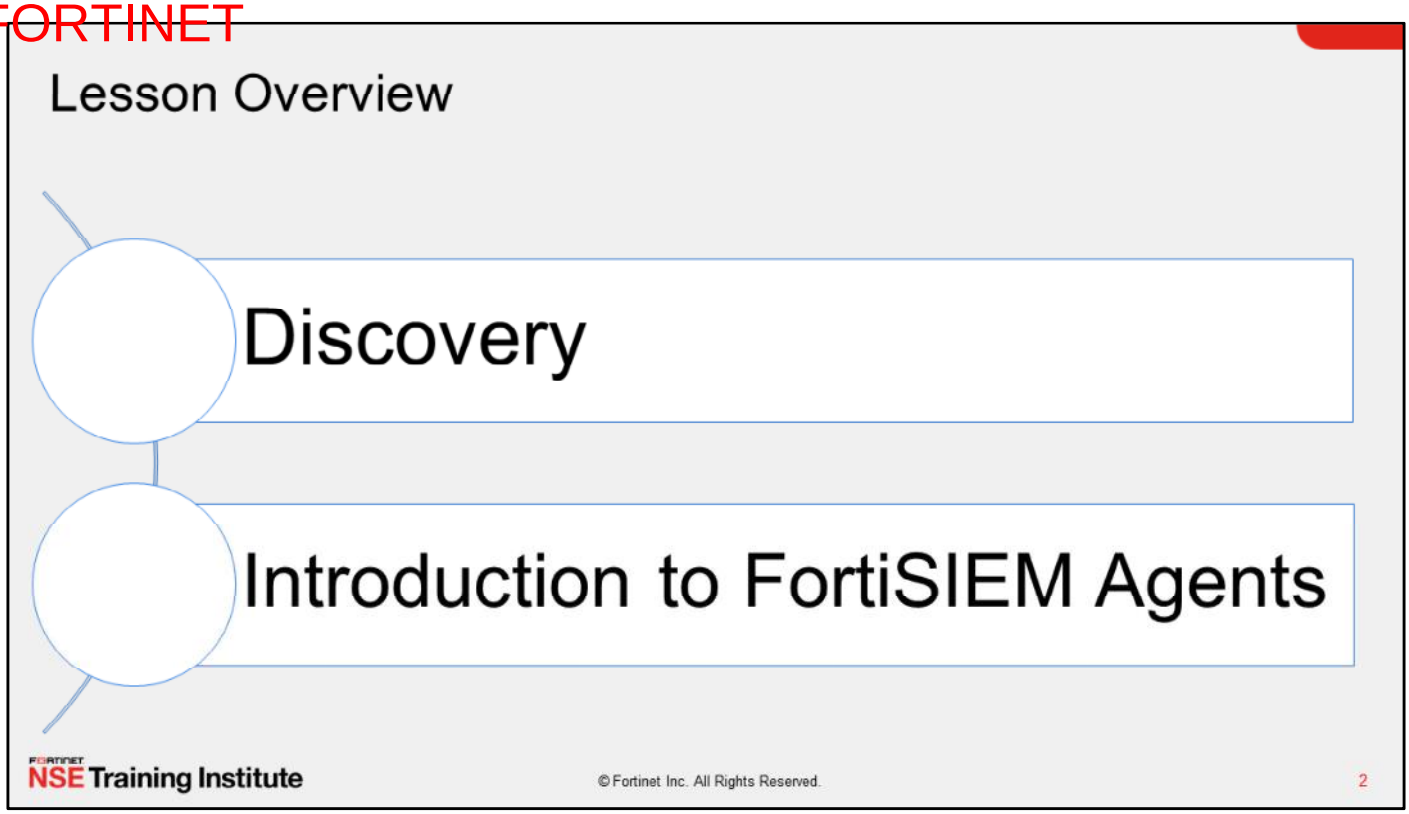
DO NOT REPRINT
© FORTINET
Brave-dumps.com



In this lesson, you will learn about the two types of discovery used by FortiSIEM, and the differences between them. You will take a close look at the GUI discovery process and the steps used to perform a discovery.

Vouchers & Dumps are Available | WhatsApp +201224560923

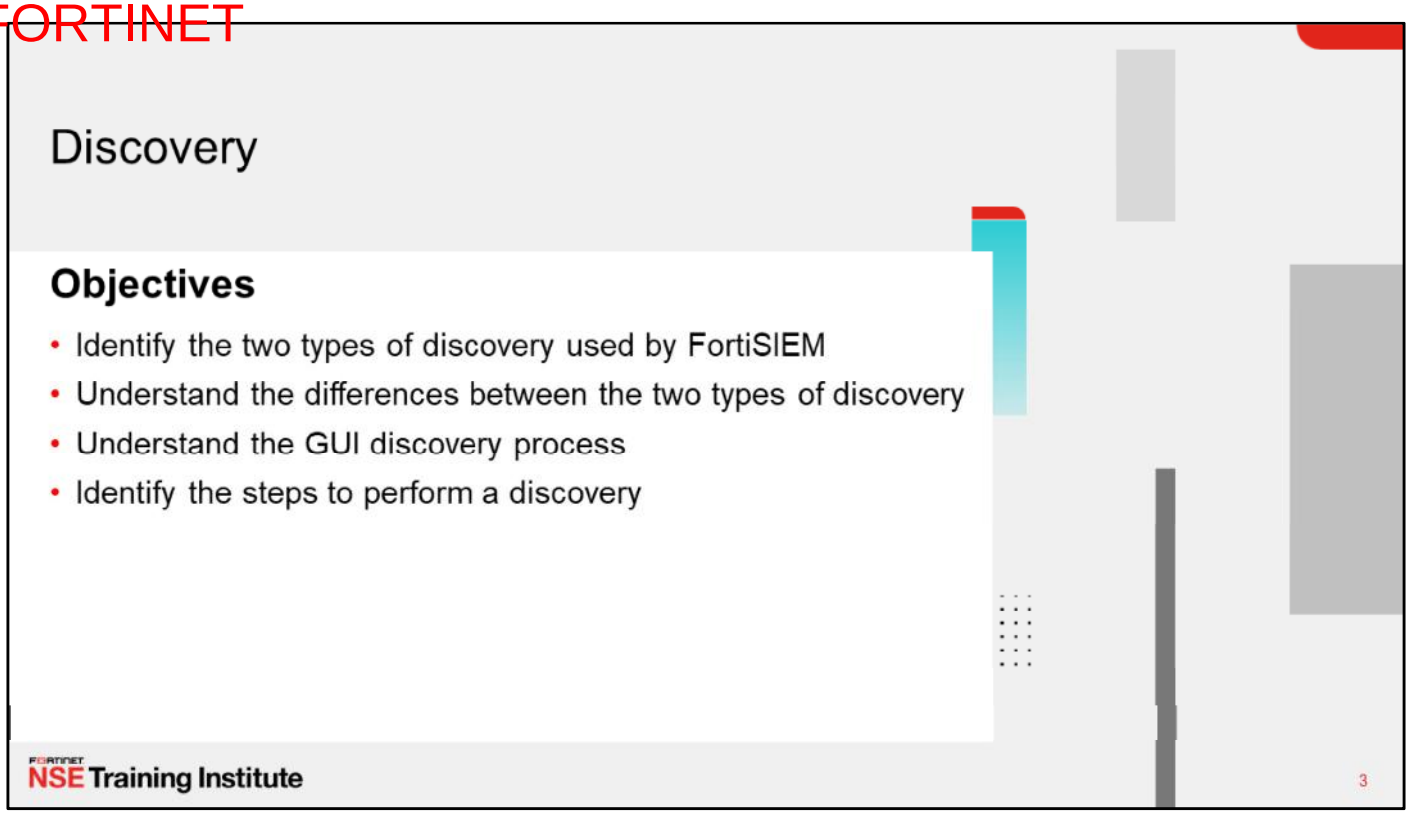
DO NOT REPRINT
© FORTINET
Brave-dumps.com



In this lesson, you will learn about the topics shown on this slide.

Vouchers & Dumps are Available | WhatsApp +201224560923

DO NOT REPRINT
© FORTINET
Brave-dumps.com

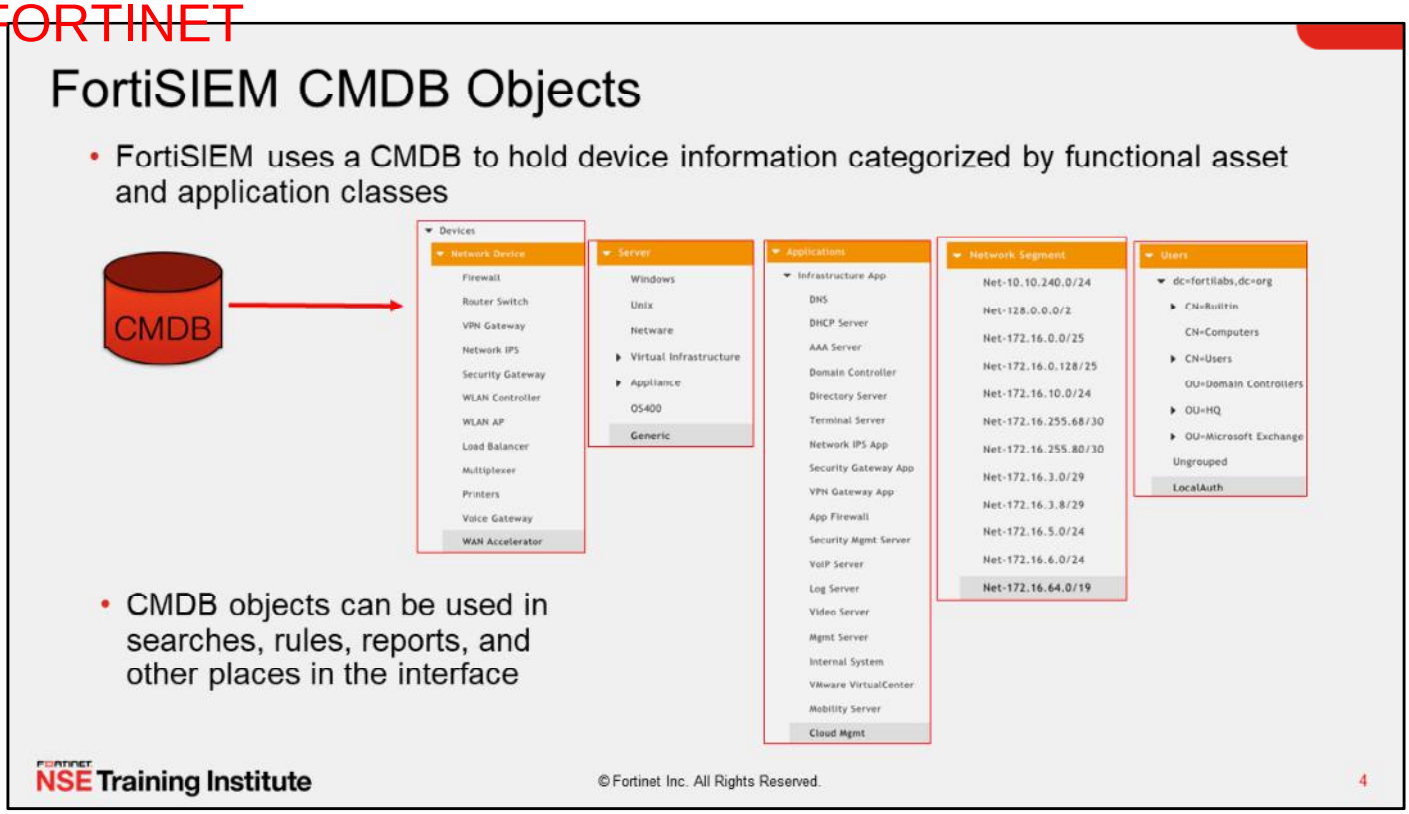


After completing this lesson, you should be able to achieve the objectives shown on this slide.

By demonstrating competence in identifying and understanding the discovery processes, you will be able to understand how discovery works in your network.

Vouchers & Dumps are Available | WhatsApp +201224560923

DO NOT REPRINT
© FORTINET
Brave-dumps.com



FortiSIEM uses a configuration management database (CMDB) to hold device information categorized by functional asset and application classes.

For example, if FortiSIEM discovers a firewall, it puts that firewall in the firewall group. If FortiSIEM discovers a Windows server, FortiSIEM puts it in a windows server group. If that Windows server is running DNS, FortiSIEM will put that Windows server in the DNS application group as well.

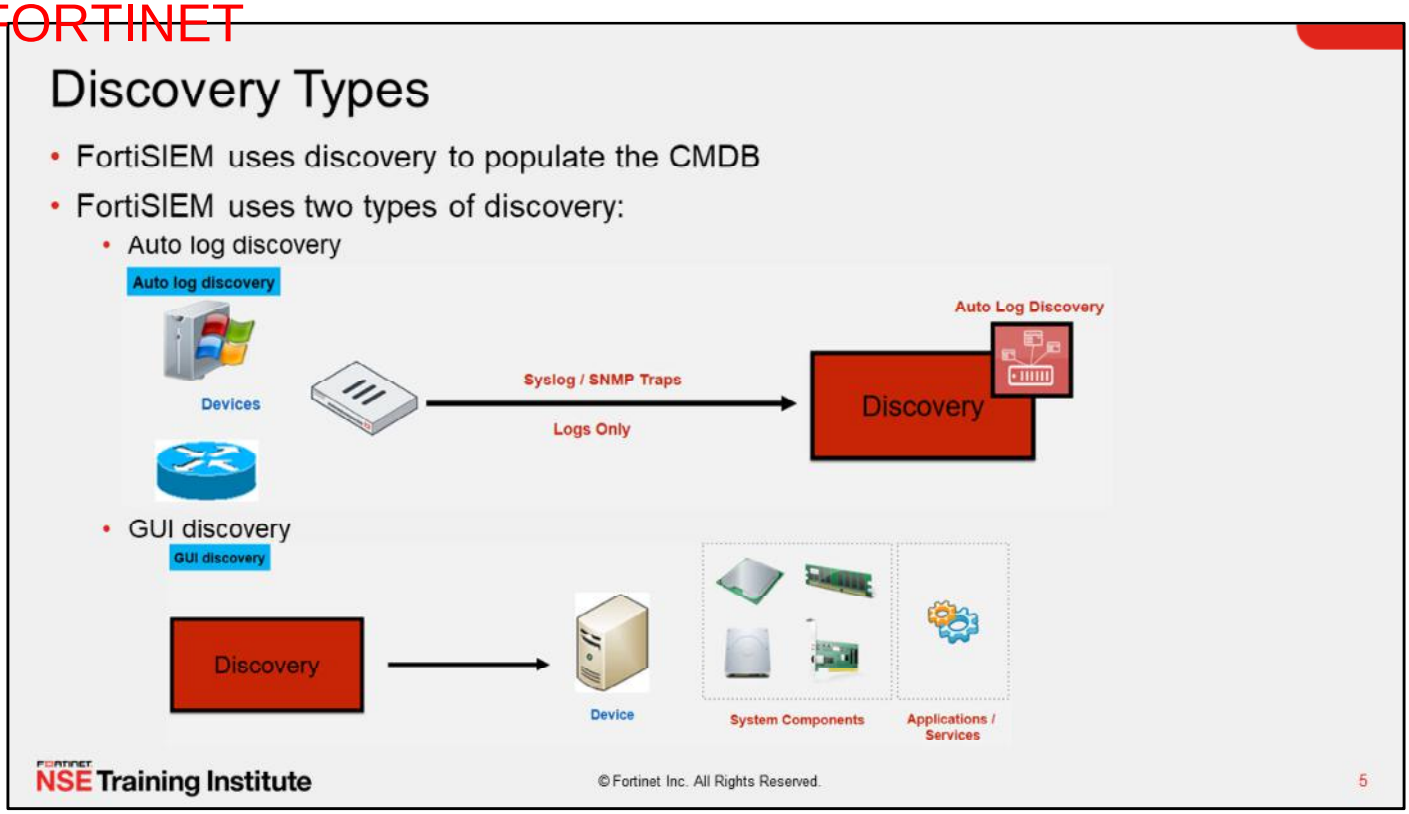
The CMDB allows you to easily look at what devices are in your environment:
- Select a particular device group, and you will get a list of all of the devices that are in that group.
- Select a an application group, and you will get a list of the devices that are running that application.
- Select a network segment, and you will get a list of all the devices that are on that segment.

If you've imported user information, that information is also available in the CMDB.

After objects are populated in the CMDB, you can use them in searches, rules, reports, notifications, and other places in the interface.

Vouchers & Dumps are Available | WhatsApp +201224560923

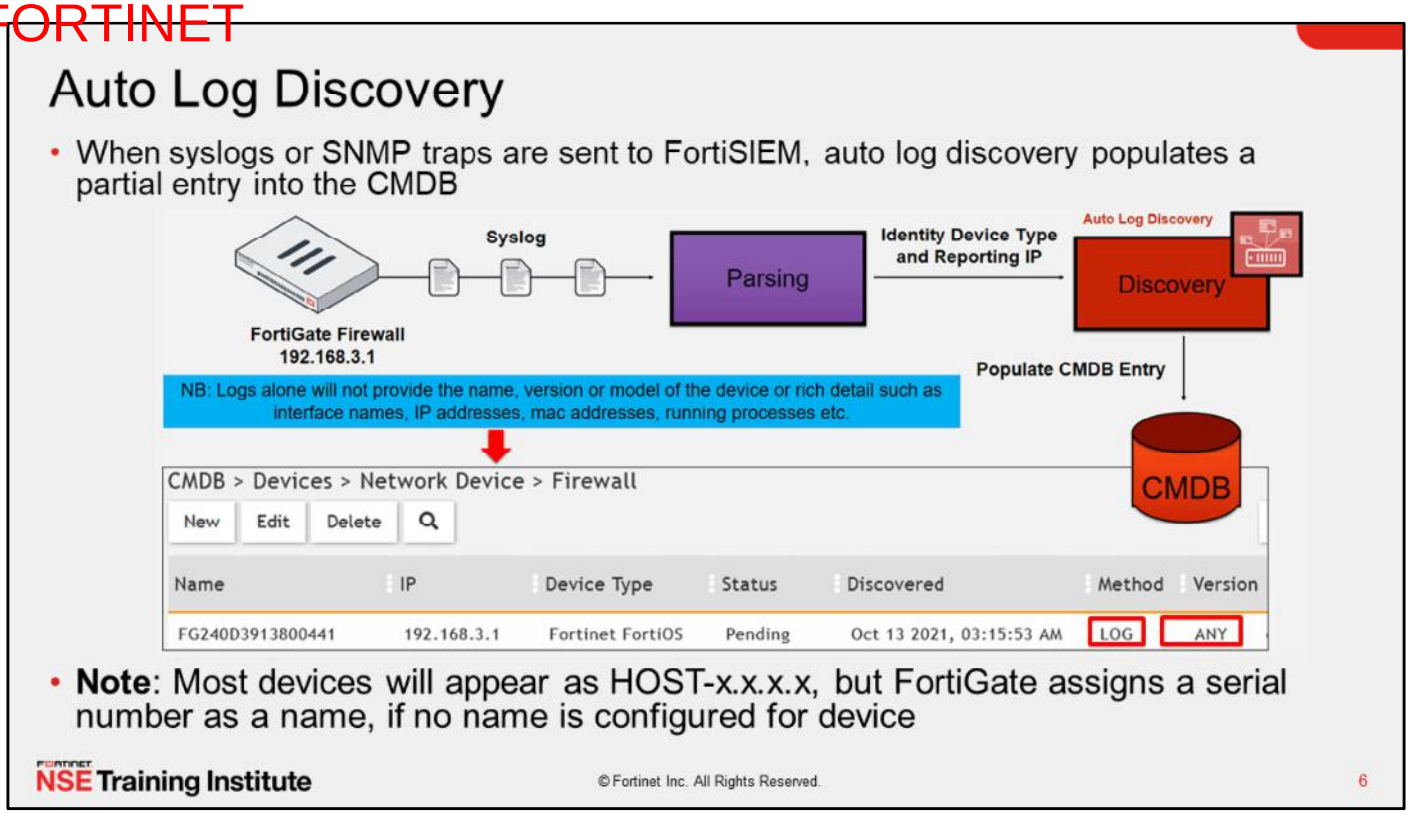
DO NOT REPRINT
© FORTINET
Brave-dumps.com



FortiSIEM uses discovery to populate the CMDB. FortiSIEM uses two discovery methods:
- Auto log discovery
- GUI discovery

Vouchers & Dumps are Available | WhatsApp +201224560923

DO NOT REPRINT Brave-dumps.com
© FORTINET



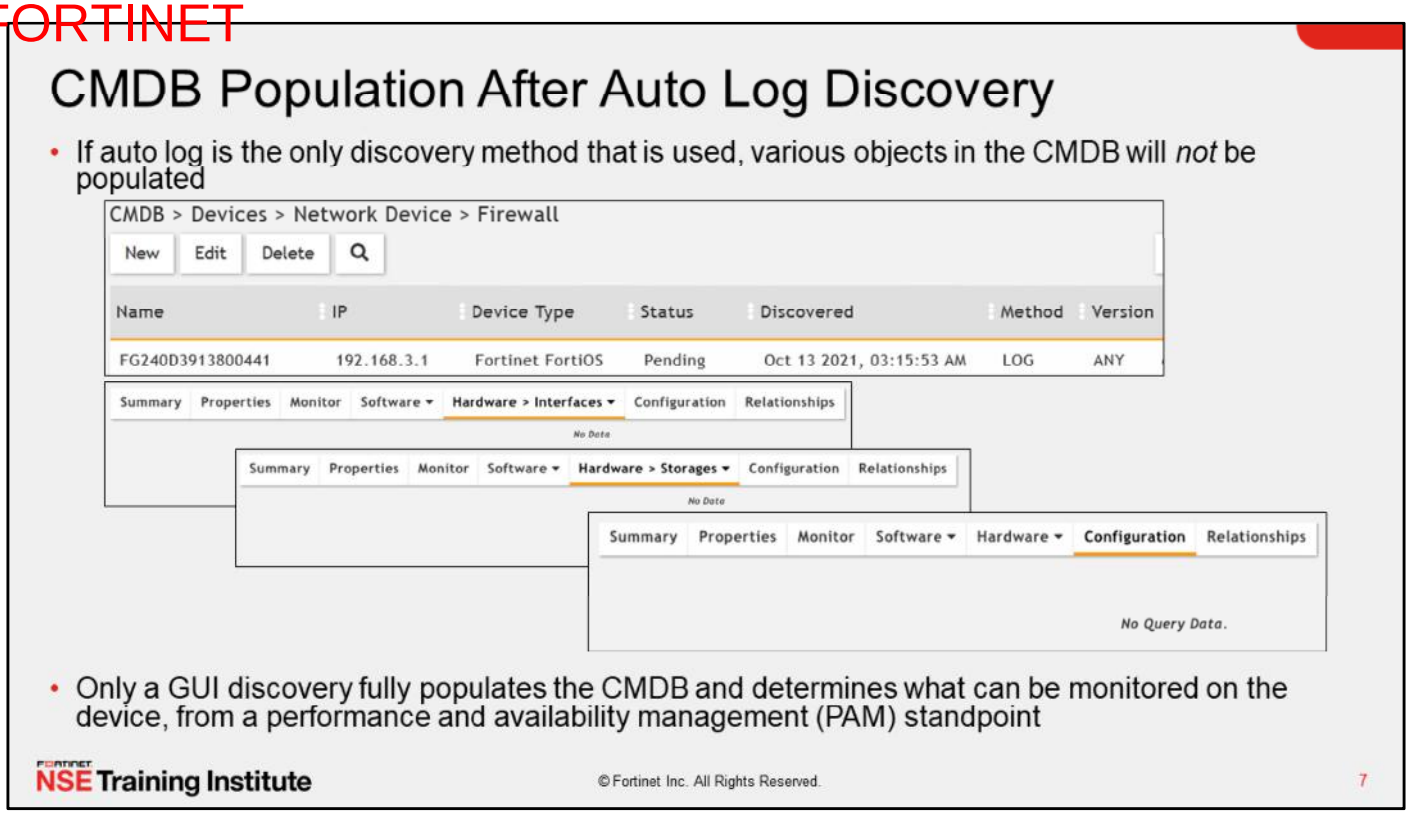
When it is using auto log discovery, you can think of the FortiSIEM as being in *passive* mode. It simply waits for devices, such as a firewall or router, to send it syslog messages or SNMP traps. When they do, FortiSIEM uses the auto discovery process to create a partial entry in the CMDB.

The entry is referred to as a *partial entry*, because the messages that were used to create it do not contain all of the information that FortiSIEM would like to have about the device that sent the message.

In the example shown on this slide, a FortiGate is the device that sends the message. FortiSIEM categorizes the device as a firewall, and creates a partial entry in the firewall group. FortiSIEM knows the IP address of the device that is sending the firewall events, but it does not know the name of the device, the type of Fortinet device, or what firmware version the device is running. Logs alone will not provide that information. If you want this additional information about the device added to the CMDB, you can manually edit the entries to change the name or add other information. However, there is a better way of getting this information, which you will learn about in this lesson.

Vouchers & Dumps are Available | WhatsApp +201224560923

DO NOT REPRINT
© FORTINET
Brave-dumps.com

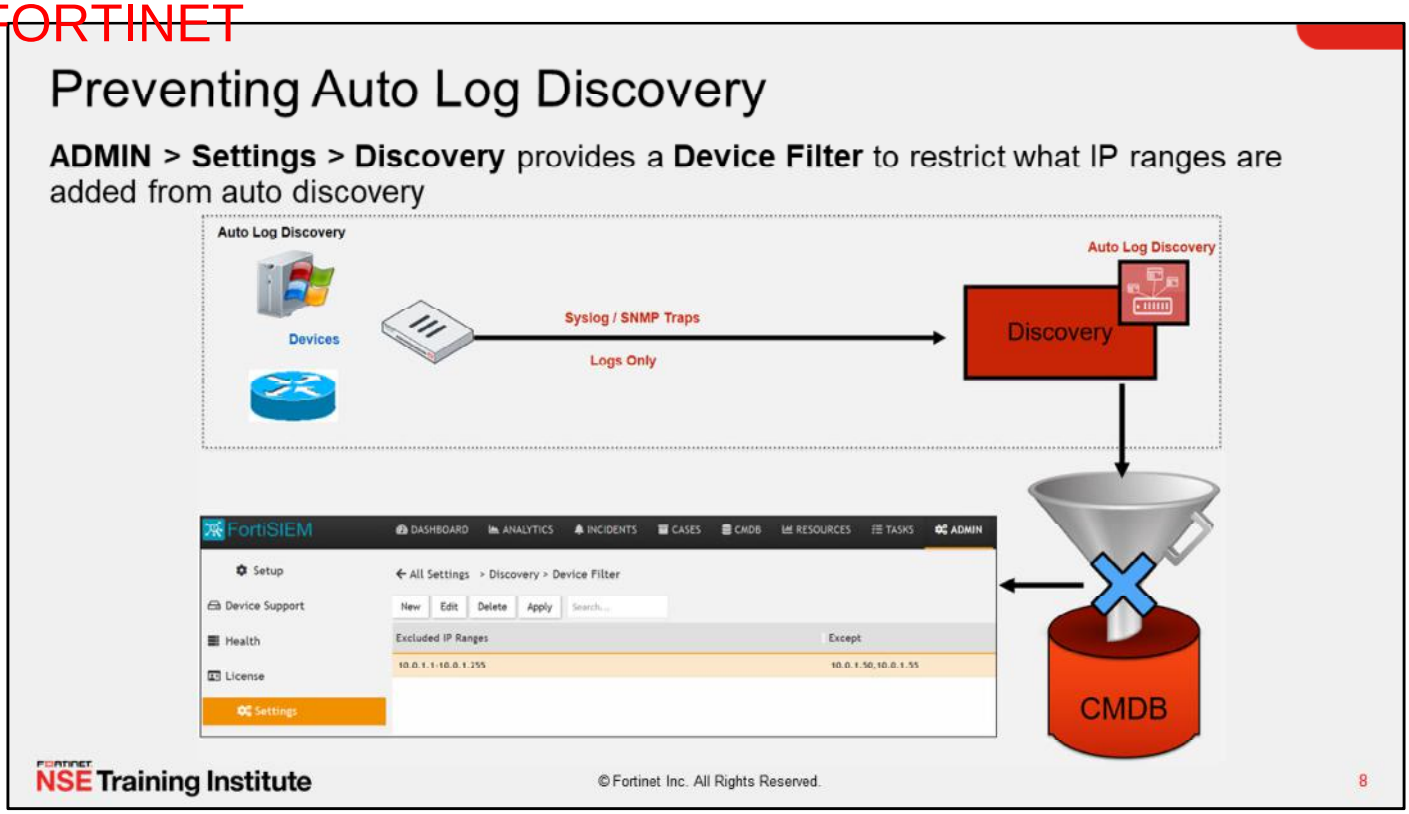


This slide shows another example of a partial entry. If FortiSIEM uses only the auto log discovery method, various objects in the CMDB will *not* be populated.

If you look at the **Interfaces** tab in this example, you can see that it is blank. The logs that were sent contain no information about the device's interface. What about other components? Again, If FortiSIEM only receives logs from a device, it won't get any information about any of the components of that device. The **Configuration** tab is also blank. FortiSIEM has the ability to collect and keep track of system configurations, but, as you can see in this example, FortiSIEM cannot collect any of that information by receiving logs only through auto log discovery. Only GUI discovery can fully populate the CMDB and determine what can be monitored on this device from a PAM standpoint.

Vouchers & Dumps are Available | WhatsApp +201224560923

DO NOT REPRINT
© FORTINET
Brave-dumps.com

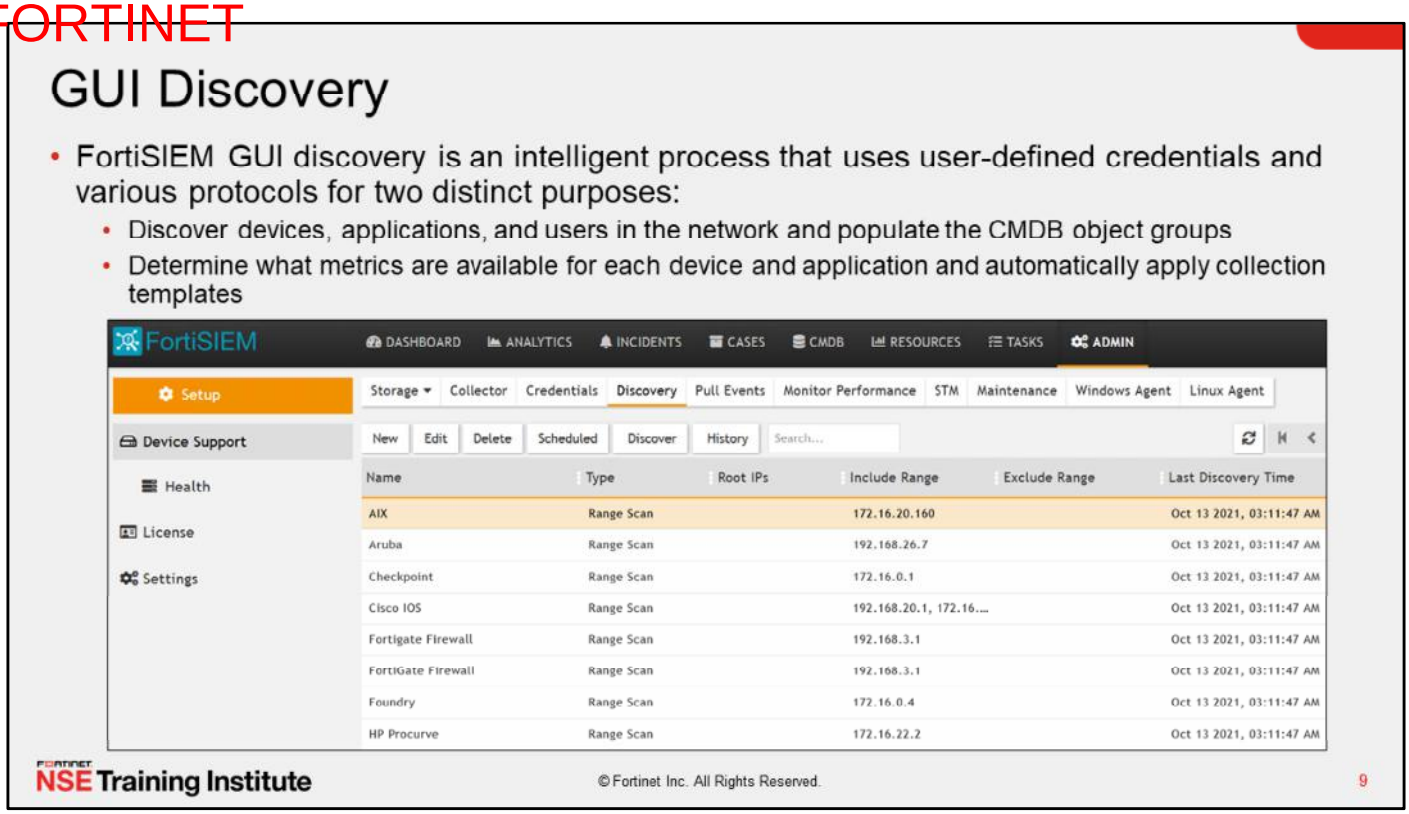


In some cases, you may want to restrict what devices can be added to the system through auto log discovery. To accommodate this use case, FortiSIEM can prevent auto log discovery from occurring for a particular IP address range.

If you click **ADMIN** > **Settings** > **Discovery** you can use the **Device Filter** tab to specify IP addresses that will be excluded from auto log discovery. You can specify individual IP addresses, or a range of IP addresses. If you specify a range, you can enter exceptions within that range. The IP addresses in the exception column are included in the auto log discovery.

Vouchers & Dumps are Available | WhatsApp +201224560923

DO NOT REPRINT
© FORTINET
Brave-dumps.com



The second type of discovery used by FortiSIEM is GUI discovery.

Unlike the auto log discovery method, in which FortiSIEM passively collects syslog and SNMP traps that are sent to it, when FortiSIEM uses GUI discovery, it actively collects data from the devices in the network.

GUI discovery is an intelligent process that uses user-defined credentials and various protocols for two distinct purposes:

- To discover the devices, applications, and users in the network and populate the CMDB object groups
- To determine what metrics are available for each device and application, identify which of those metrics it understands how to collect, and automatically apply the associated collection templates to these devices or applications

Collection templates allow FortiSIEM to retrieve information, such as CPU, memory, disk space, and network interface statistics, or or application-related metrics such as DNS services, DHCP services, active directory, and so on.

Vouchers & Dumps are Available | WhatsApp +201224560923

DO NOT REPRINT
© FORTINET
Brave-dumps.com

GUI Discovery–Data Collection Jobs

- For security event (SIEM) log collection, GUI discovery applies log collection templates known as pull events



NSE Training Institute

© Fortinet Inc. All Rights Reserved.

10

When a device sends syslog events, it's the device itself that is sending data to FortiSIEM. But, not all devices are designed to send syslog events. A Windows server, for example, does not send syslog events. The GUI discovery method supports a collection template called **Pull Events**, that is designed to pull security or SIEM-type events from these devices.

Two examples of when the Pull Events collection template would be used to pull SIEM-type events (also called SIEM-specific jobs) are: when using WMI to collect Windows event logs at regular intervals from a Windows 2008 server, and when collecting VMware audit logs, where FortiSIEM collects the events.

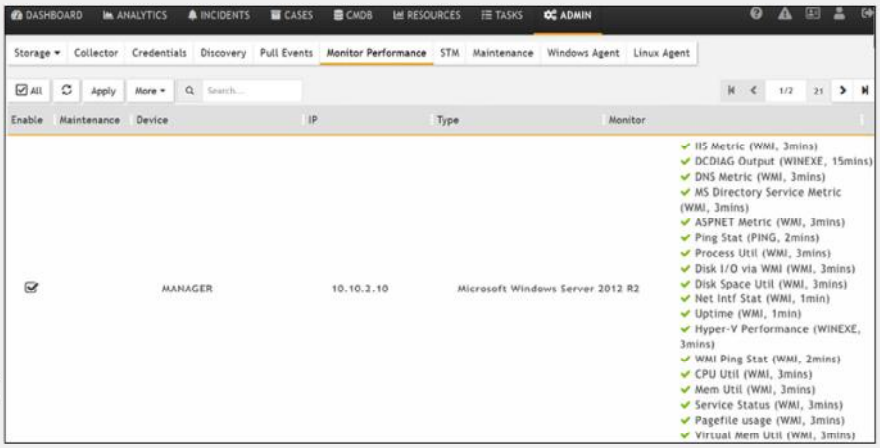
In **ADMIN** > **Setup**, on the **Pull Events** tab, you can view the SIEM collection jobs that FortiSIEM has applied through GUI discovery.

Vouchers & Dumps are Available | WhatsApp +201224560923

DO NOT REPRINT
© FORTINET
Brave-dumps.com

GUI Discovery–Data Collection Jobs

- The collection templates used for PAM event collection are System Monitor and Application Monitor
- System monitor jobs collect data on device resources, such as CPU, memory, network interfaces, disk, page file usage, and so on
- Application monitor jobs collect the metrics of business critical applications, such as Exchange, SQL Server, Oracle, IIS, DHCP, and many more



NSE Training Institute

© Fortinet Inc. All Rights Reserved.

11

There are also data collection templates for performance data or PAM. These templates are called System Monitor and Application Monitor.

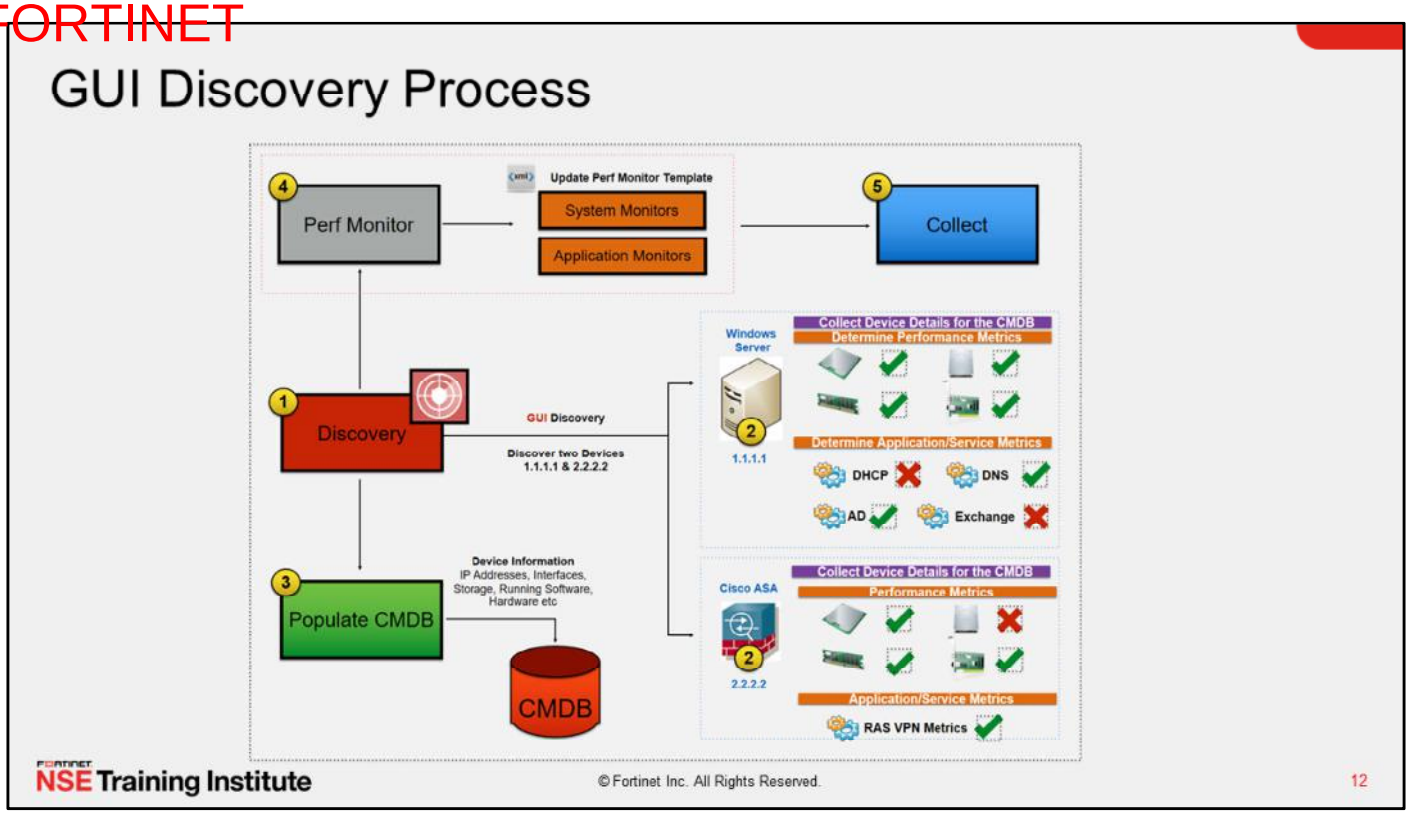
Under the **Monitor Performance** tab in the **ADMIN** > **Setup**, you can see the system monitor and application monitor jobs that have been deployed.

A system monitor job collects device resources, such as CPU, memory, network interfaces, disk page file usage, and so on.

An application monitor job to collect metrics of application-related data, such as Exchange, SQL Server, IIS, DHCP, and many more.

Vouchers & Dumps are Available | WhatsApp +201224560923

DO NOT REPRINT
© FORTINET
Brave-dumps.com



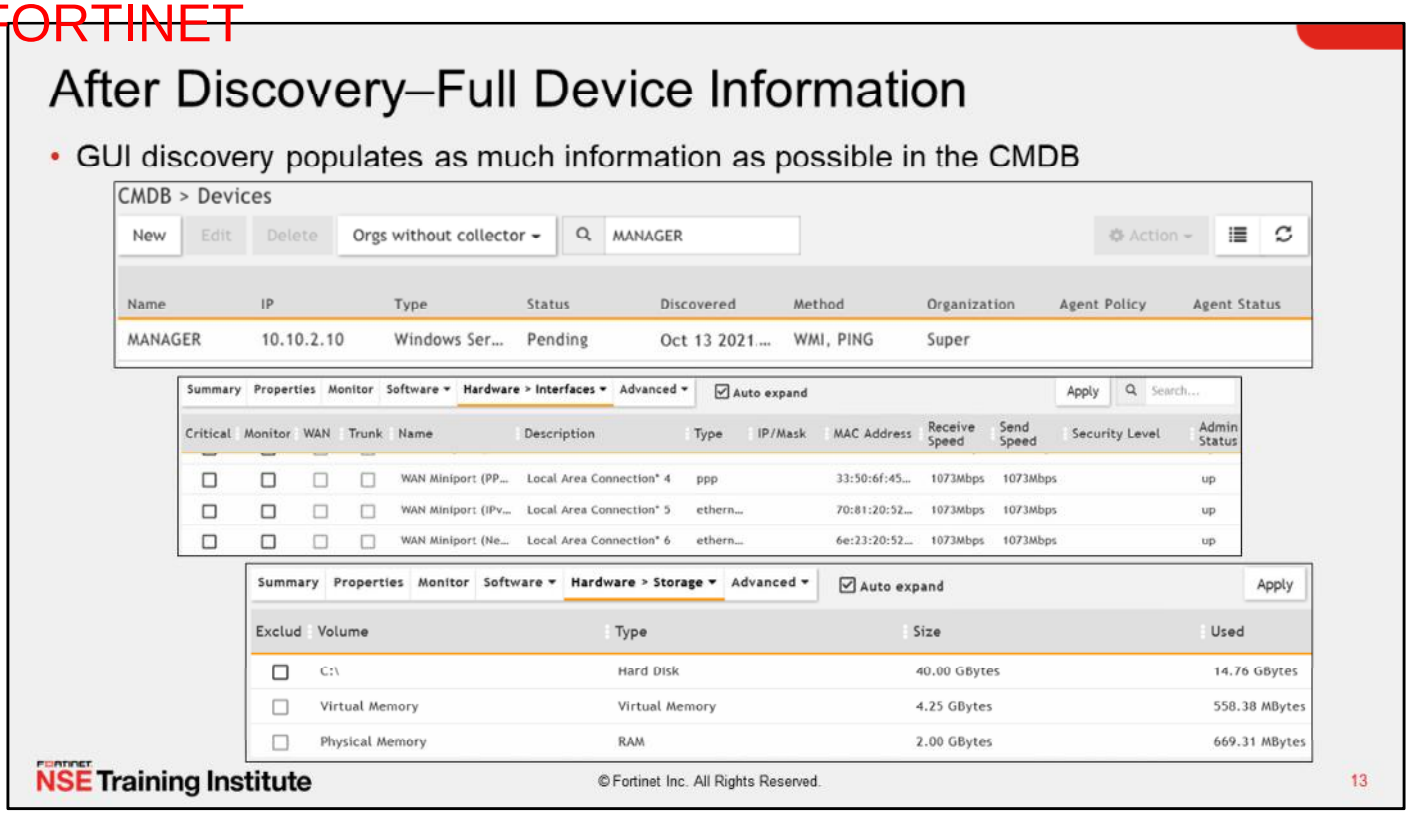
This slide shows a high-level view of the GUI discovery process.

1. An administrator has provided the appropriate credentials and associated them with IP addresses. Then, the administrator defines two IP addresses to discover: one is a Windows server and the other is a Cisco ASA firewall.
2. FortiSIEM reaches out to these devices and determines what kind of components they have: Network interfaces, CPU, memory, storage, and so on. FortiSIEM also looks to see what applications are running on these devices. In this example, FortiSIEM knows that it's looking at a Windows server, so it will look for applications, such as DHCP, DNS, Active Directory, Exchange, and so on. FortiSIEM will reach out to the Cisco ASA firewall to collect the same types of data, but It will only look for the applications expected to be running on a Cisco ASA, such as RAS VPN.
3. FortiSIEM populates the CMDB with the data that it collects from these devices.
4. The Performance Monitor then applies the relevant System Monitor and Application Monitor templates to the devices. The templates determine what kind of metrics can be collected from the components. For example, when determining what System Monitoring templates to apply to these devices, the Performance Monitor's process might go something like the following:
   - This device has a CPU; therefore, system CPU usage and user CPU usage metrics can be collected.
   - Total disk space, free disk space, used disk space, and disk I/O rates can be collected from the hard disk.
   - There is no disk on the ASA. Therefore a disk metric will not be applied for this device

   The Performance Monitor will make similar decisions about application metrics using the Application Monitor templates.
5. After the templates have been updated and assigned to each device, collection jobs will automatically be created and the metrics collected. All of this new information will then be saved in the device's entries in the CMDB.

Vouchers & Dumps are Available | WhatsApp +201224560923

DO NOT REPRINT
© FORTINET
Brave-dumps.com

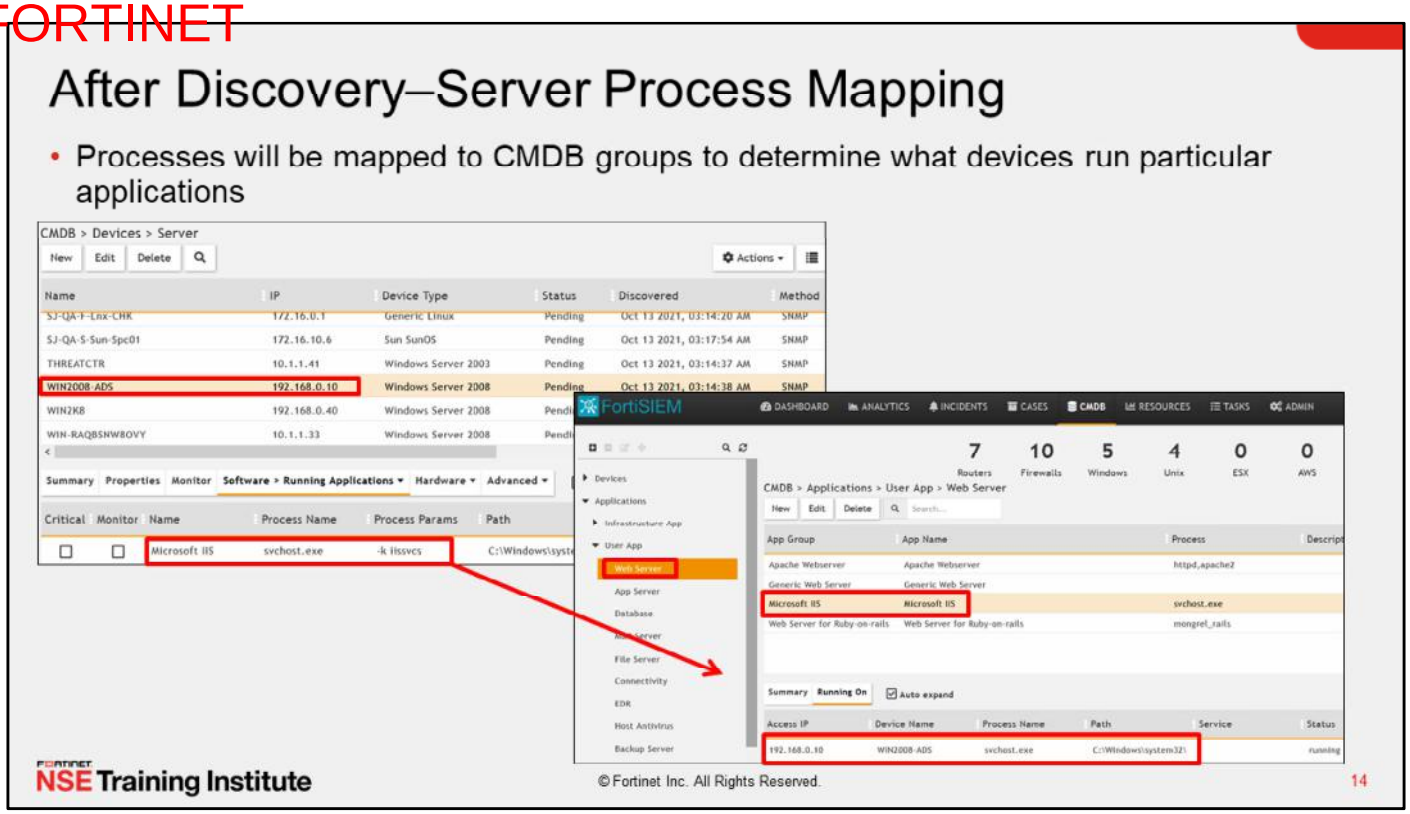


GUI discovery populates as much information as possible in the CMDB.

Let's take another look at the device we looked at in the auto log discovery example. In the auto discovery example, you will remember that the **Interfaces** and **Hardware** tabs were blank because this information is not in event logs. But, in the example of GUI discovery shown in this slide, these tabs are populated with information. The ASA now has a name and we know that it is a Cisco ASA , specifically the ASA5510 model. We also know what version of code is currently running on the device. The **Interface** tab shows the IP address, MAC address, speed, and status. The **Components** tab shows the serial number.

Vouchers & Dumps are Available | WhatsApp +201224560923

DO NOT REPRINT
© FORTINET
Brave-dumps.com



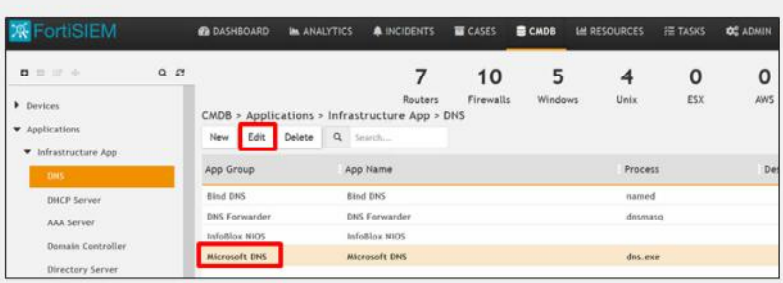
After GUI discovery, processes are mapped to CMDB groups to determine which devices run particular applications. In this example, the running applications list for this device shows that FortiSIEM knows that the name Microsoft IIS is associated with the process name `svchost.exe`, which also has a parameter of IIS services. FortiSIEM looks for these mappings so that it knows what kind of application is running on a device. It also populates mappings in the application groupings.

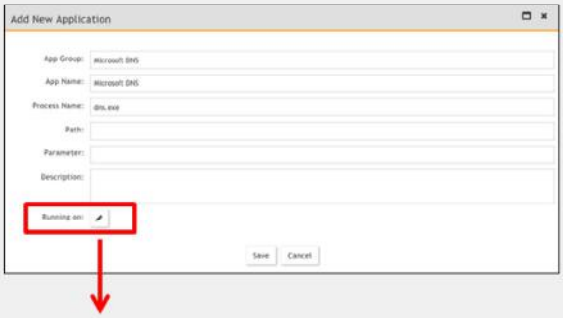
Vouchers & Dumps are Available | WhatsApp +201224560923

DO NOT REPRINT
© FORTINET
Brave-dumps.com

Manually Populating Application Groups

- Some customers struggle to provide credentials for devices in environments and hence the discovery process cannot auto populate the CMDB application groups





- These groups can be edited with IP Address Only associations added so existing correlation rules function as normal



NSE Training Institute

© Fortinet Inc. All Rights Reserved.

15

FortiSIEM provides the ability to manually populate application groups.

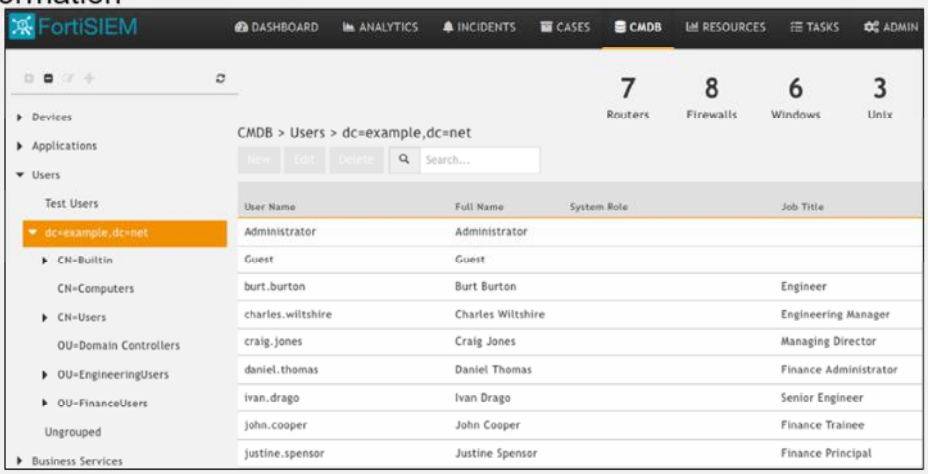
If you can't provide credentials for the devices in your network, the discovery process can't populate the CMDB application groups. In these cases, you can go to the CMDB, select the application categories, select an individual application, and edit and define these devices using only the IP address. After you do this, any existing correlation rules will function as normal.

Vouchers & Dumps are Available | WhatsApp +201224560923

DO NOT REPRINT
© FORTINET
Brave-dumps.com

After Discovery–LDAP Discovery

- When LDAP credentials are provided, user information is populated for correlation with identity information



- This user information can also be used for GUI LDAP authentication

NSE Training Institute

© Fortinet Inc. All Rights Reserved.

16

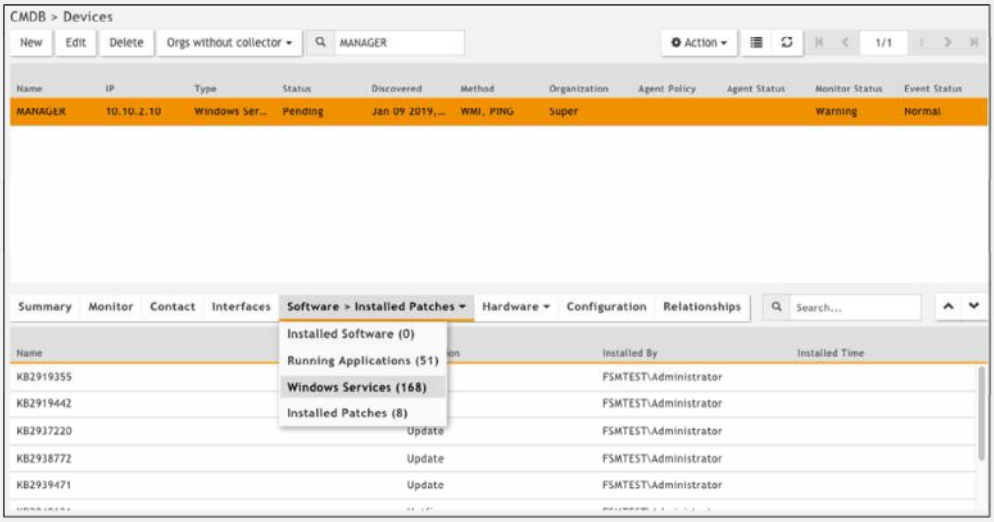
If LDAP credentials are provided, user information is populated for correlation with the identity and location feature. In the CMDB, all the users are grouped in lists. This information can also be used for LDAP authentication to the FortiSIEM GUI.

Vouchers & Dumps are Available | WhatsApp +201224560923

DO NOT REPRINT Brave-dumps.com
© FORTINET

After Discovery—Windows Services / Patches

- Windows service and patch information.



NSE Training Institute

© Fortinet Inc. All Rights Reserved.

17

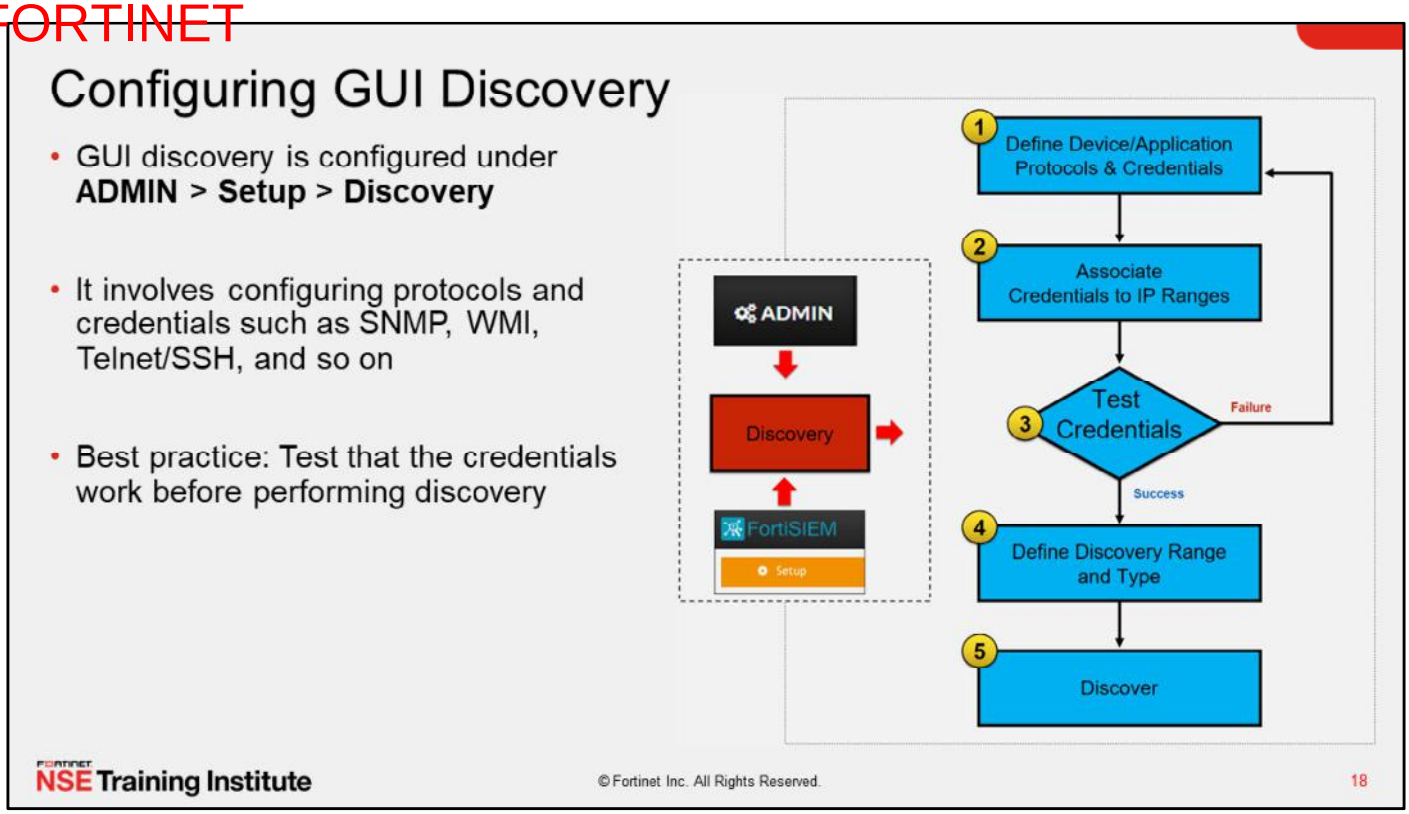
Here is another example of the type of information that is populated in the CMDB after a GUI discovery.

The example on this slide shows Windows services and patch information. When FortiSIEM discovers a Windows device, it looks at what services are running on that device and lists them in the CMDB. It also records the current state and start-up mode of the service. If a service on a Windows device has a start-up mode of auto, and that service suddenly stops, FortiSIEM can produce an alert notifying administrators that the service has stopped. This is useful for services such as antivirus.

The **Installed Patches** tab lists the name of the patch that was installed, who installed it, and when. Note that the service and patch information is only as good as the last discovery. For this reason, FortiSIEM can be configured to discover servers on a scheduled basis.

Vouchers & Dumps are Available | WhatsApp +201224560923

DO NOT REPRINT
© FORTINET
Brave-dumps.com

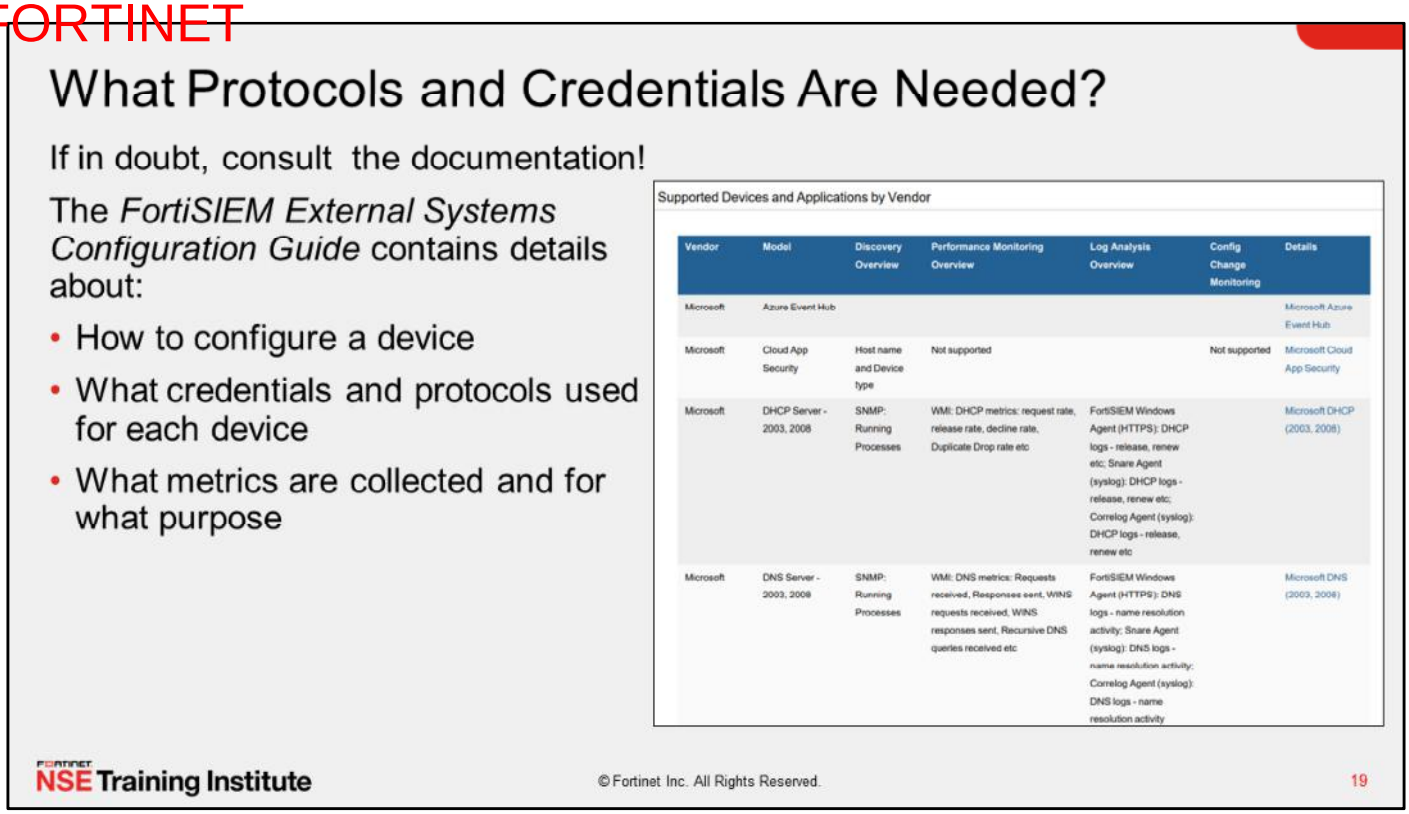


You configure GUI discovery under **ADMIN** > **Setup**.

1. Configure device and application protocols and credentials, such as SNMP , WMI, Telnet or SSH, and so on.
2. Associate these credentials with IP addresses in the network.
3. Test these credentials. It is a best practice to make sure the credentials work before a discovery is performed. If you've entered improper credentials, the discovery fails.
4. Define a discovery range and scan type.
5. Choose whether you want to perform the discovery now or in the future, and perform the discovery.

Vouchers & Dumps are Available | WhatsApp +201224560923

DO NOT REPRINT
© FORTINET
Brave-dumps.com



How do you know what protocols and credentials are needed? If in doubt, consult the documentation. The *FortiSIEM External Systems Configuration Guide* contains details about:

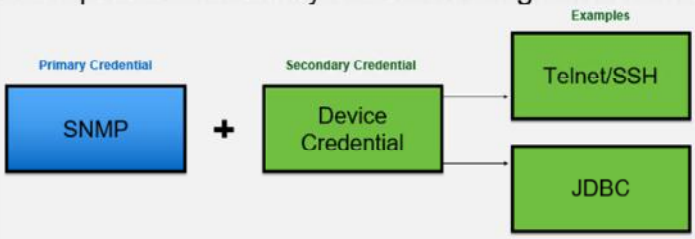
- How to configure every device
- What credentials and protocols are used for each device
- What metrics are collected for what purpose

Vouchers & Dumps are Available | WhatsApp +201224560923

DO NOT REPRINT
© FORTINET
Brave-dumps.com

GUI Discovery Credentials

- Credentials are used for the collection of SIEM data and PAM
- Almost every device requires a read-only SNMP credential.
  - This is a primary credential and FortiSIEM supports versions 1, 2c, and 3.
- Some devices also require a secondary credential to get more information



- If the documentation states that SNMP is required, but it is not enabled on the device, no other access methods are attempted and discovery fails

NSE Training Institute
© Fortinet Inc. All Rights Reserved.
20

You can't collect information from a device without proper authentication. In order for FortiSIEM to perform GUI discovery collection jobs, either SIEM or PAM, it requires proper credentials. FortiSIEM uses primary and secondary credentials.

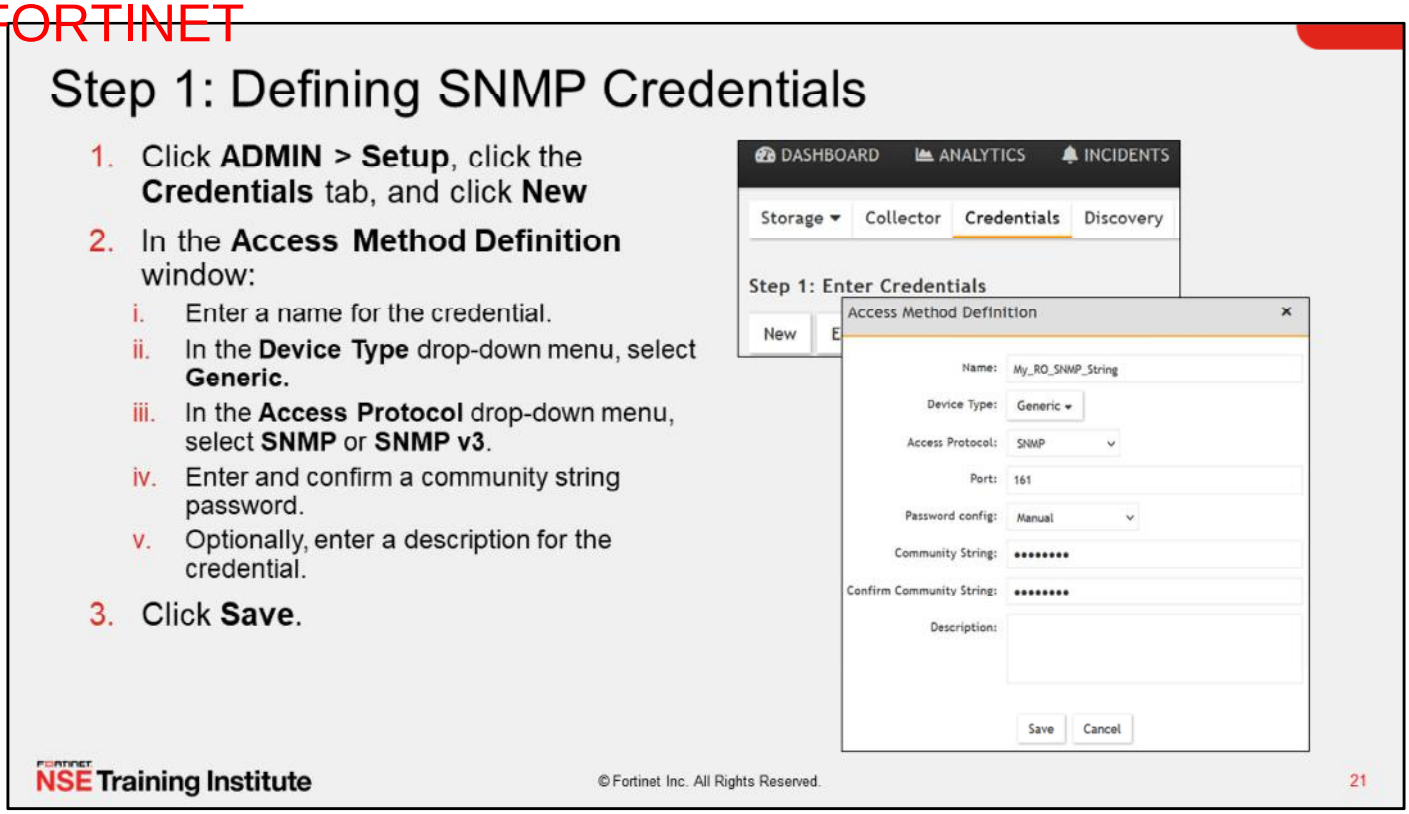
Almost every device requires a read-only SNMP credential. This is the primary credential for a device. FortiSIEM supports versions 1, 2c, and 3 of SNMP. There are some exceptions. For example, Windows devices require only a WMI credential; SNMP is optional. Checkpoint is another example of a device that does not require an SNMP credential. The user guide provides details about which devices require SNMP for a GUI discovery.

Some devices also require a secondary credential to allow information collection. An example of this is a Cisco ASA, or a Cisco switch. If you want to collect the running configuration of that device, you need to add a secondary credential, such as telnet or SSH. SNMP alone will not allow you to collect the configuration data.

If the documentation states that SNMP is required, but it is not enabled on the device, no other access methods are attempted and the discovery fails.

Vouchers & Dumps are Available | WhatsApp +201224560923

DO NOT REPRINT
© FORTINET
Brave-dumps.com

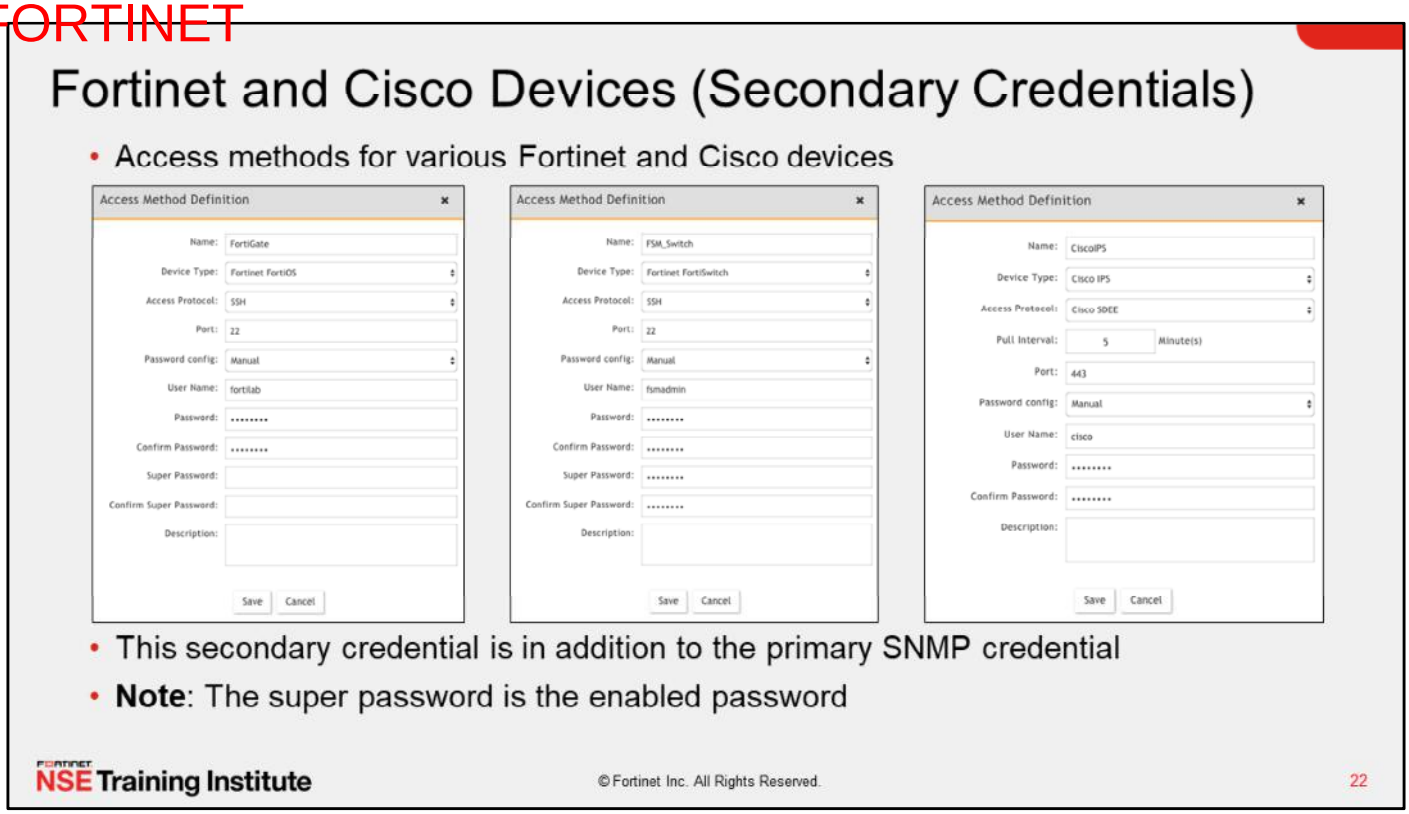


Let's take a look at the steps to define SNMP credentials.

1. Click **Admin** > **Setup** click the **Credentials** tab, and click **New**.
2. In the **Access Definition** window:
    i. Enter a name for the credential. It should be something appropriate to where it will be used.
    ii. In the **Device Type** drop-down menu, select **Generic**. This is because SNMP can be use across multiple devices.
    iii. In the **Access Protocol** drop-down menu, select **SNMP** and select the version number, if you are using version 3.
    iv. Enter and confirm the community string password.
    v. Optionally, enter a description for the credential.
3. Click **Save**.

Vouchers & Dumps are Available | WhatsApp +201224560923

DO NOT REPRINT
© FORTINET
Brave-dumps.com



This slide shows how to define a secondary credential for Fortinet and Cisco devices:

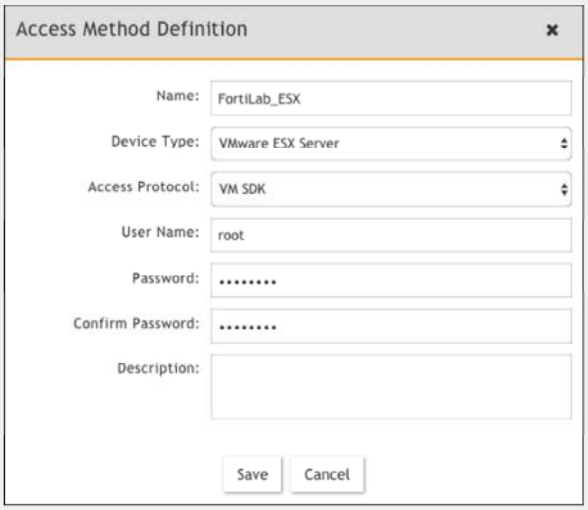
1. When you select one of these devices in the **Device Type** drop-down menu, select the appropriate access protocol: SSH for Fortinet FortiOS, SSH for the Fortinet FortiSwitch and Cisco's proprietary protocol, SDEE, for the IPS device.
2. The system will set the port to the default port for the selected protocol. You can change this if the device is configured to use a non-standard port. You can also change the different available access protocols for devices like HTTPS, SSH, Telnet etc.
3. You need to enter a user name and password, and may also need to enter a root password or super password, depending on the device.

Vouchers & Dumps are Available | WhatsApp +201224560923

DO NOT REPRINT
© FORTINET
Brave-dumps.com

VMware Access Credentials

- FortiSIEM can communicate with a vCenter server, or with individual VMware ESX or ESXi server that you want to monitor
- FortiSIEM applies a Pull Event job to collect audit logs and a System Monitor job to collect VM performance metrics
- **Note**: VMware monitoring does not require SNMP, because FortiSIEM uses the VMware API



NSE Training Institute

© Fortinet Inc. All Rights Reserved.

23

FortiSIEM can communicate with a vCenter server or with each individual VMware ESX or ESXi server that you want to monitor in your network.

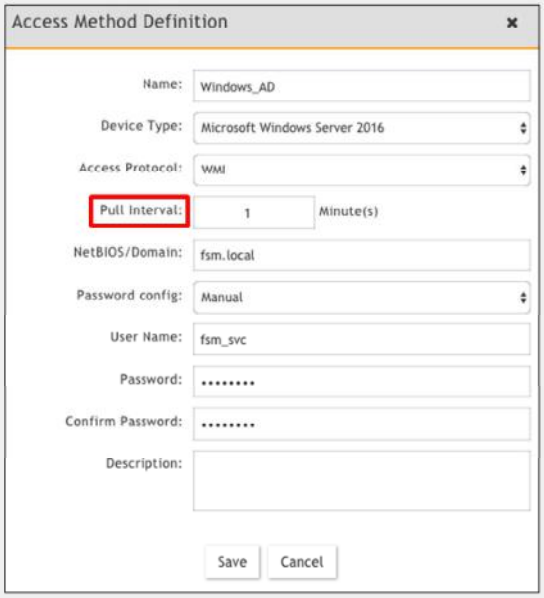
VMware monitoring does not require SNMP. FortiSIEM uses the VMware API authentication to collect the data. When it discovers a VMware device, FortiSIEM applies two collection jobs: a Pull Event job, to collect SIEM-type information, such as audit logs, and a system monitor job, to collect VM performance metrics (PAM).

Vouchers & Dumps are Available | WhatsApp +201224560923

DO NOT REPRINT
© FORTINET
Brave-dumps.com

Windows Devices

- Windows device credentials can use the WMI access protocol
- A single credential is used for collecting SIEM (event) and PAM (performance) data
- **Pull Interval**: This setting specifies how often to pull the security, application, and system event logs (SIEM collection only)
- Alternatively, the FortiSIEM agent or third-party agents, such as Snare, can be used to push and filter Windows event logs, in real time, to FortiSIEM



NSE Training Institute

© Fortinet Inc. All Rights Reserved.

24

Most customers use a WMI credential to collect data from Windows devices. This single WMI credential is used for both SIEM event collection and the collection of performance and availability metrics.

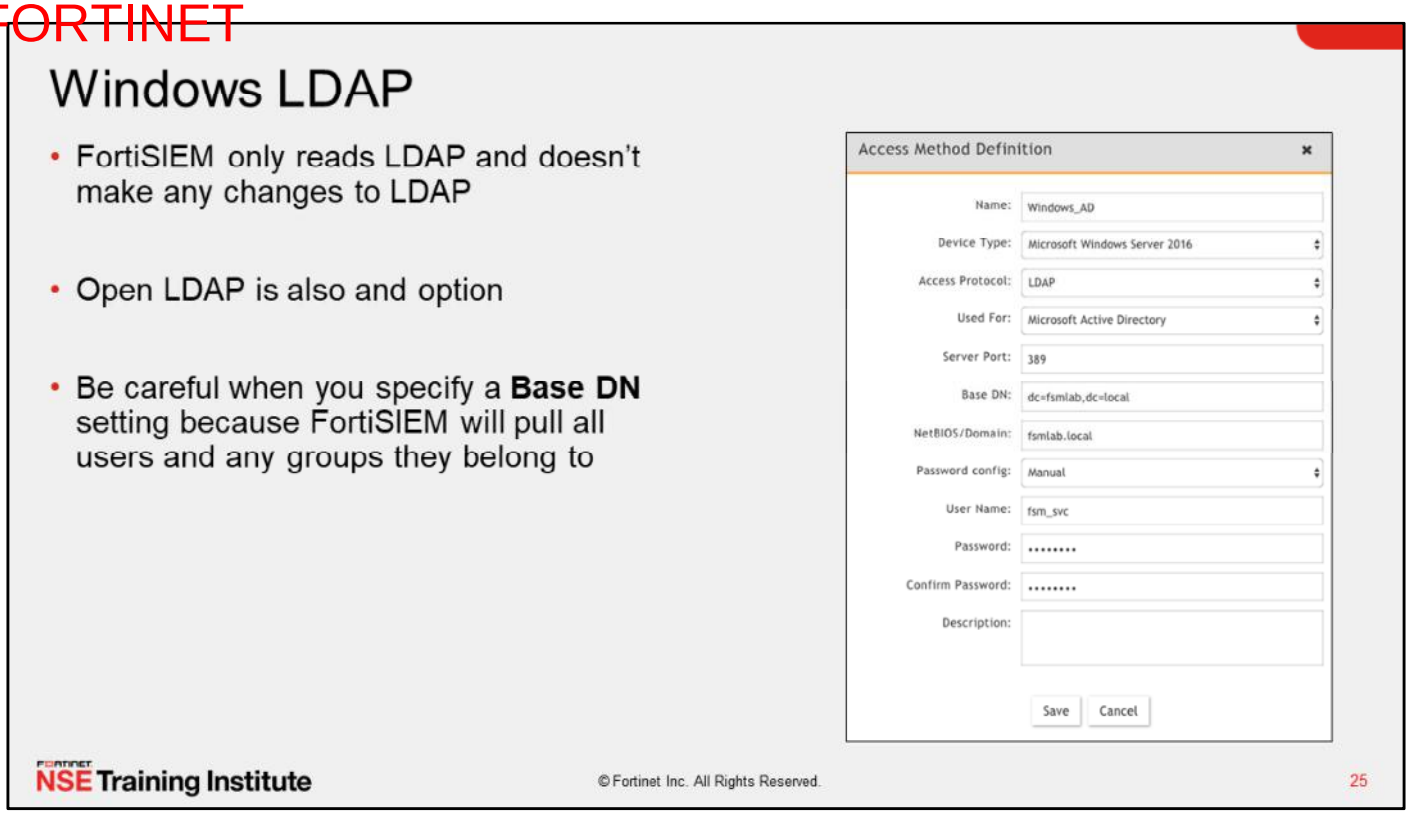
Take note that the pull interval set in this example applies only to the collection Windows security, application, and system events logs (SIEM). Collection is done in an agentless fashion at every interval.

Alternatively, you could install an agent on the Windows device. FortiSIEM has its own agent that can be used for that purpose. Third-party agents, such as Snare and Corelog, are also supported for this purpose.

An agent essentially gives a Windows device the capability to send Windows event logs, in a real time, as though they were syslog. If you use a WMI collection job, at each interval, you are collecting chunks of events, which could have a performance impact, depending on how busy the Windows devices are.

Vouchers & Dumps are Available | WhatsApp +201224560923

DO NOT REPRINT
© FORTINET
Brave-dumps.com



To create a Windows LDAP credential, specify Microsoft Windows as the device type as and select LDAP as the access protocol.

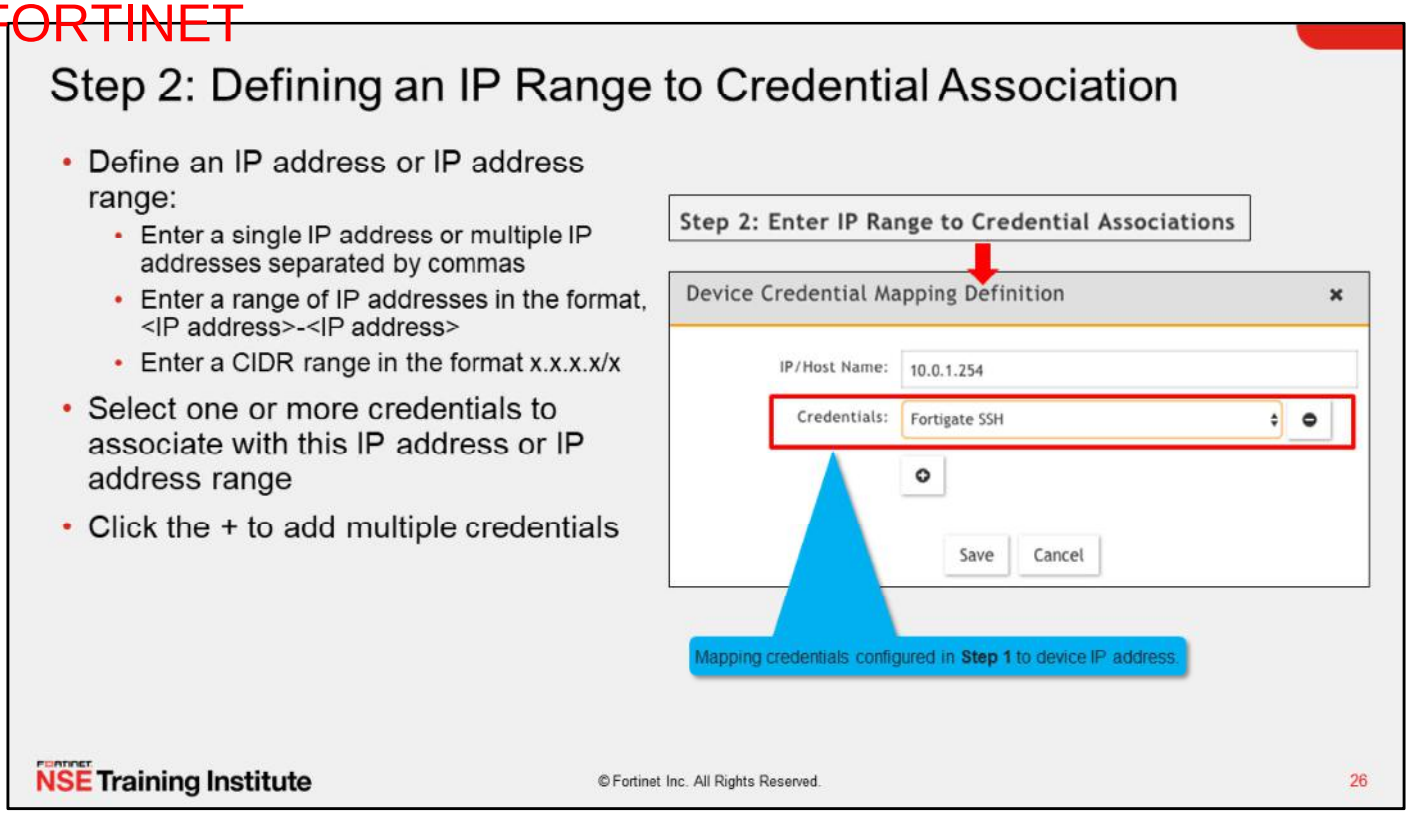
FortiSIEM only *reads* from the LDAP server. It doesn't try to make any changes to it. Therefore, the account that you specify needs only *read* access to the LDAP tree.

Note that **Open LDAP** is also available as an option from the **Device Type** drop-down menu..

You should be careful when specifying the **Base DN** setting. FortiSIEM uses this setting as an entry point, and it will pull all of the users and groups below this point. Depending on the tree structure, you could be needlessly searching areas of the tree that do not have user information, or collecting user information from branches you did not intend to collect from.

Vouchers & Dumps are Available | WhatsApp +201224560923

DO NOT REPRINT
© FORTINET
Brave-dumps.com



Once you've defined all of the credentials for the devices in your network, you will associate those credentials with IP addresses. You specify either a single IP address, multiple IP addresses (separated by commas), or a range of IP addresses. When you specify an IP address range, use the format <IP address> – <IP address> . When you specify a CIDR range, use the format x.x.x.x/x.
Use the plus sign (+) to associate more than one credential with an IP address or IP range.

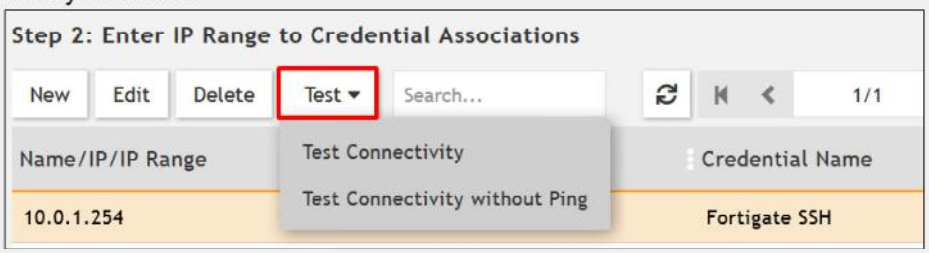
You should try to be specific when defining these credentials. For example, if you know the Windows server range, apply Windows server credentials to only that particular group, or range, of IP addresses.

Vouchers & Dumps are Available | WhatsApp +201224560923

DO NOT REPRINT
© FORTINET
Brave-dumps.com

Testing Credentials

- After you define and associate the credentials, test them using the FortiSIEM test connectivity function



- Two options are available from the **Test** drop-down list.:
  - Test Connectivity
  - Test Connectivity without Ping
- The testing determines if the defined credentials will succeed
- If the connectivity test is not successful, discovery will fail

NSE Training Institute
© Fortinet Inc. All Rights Reserved.
27

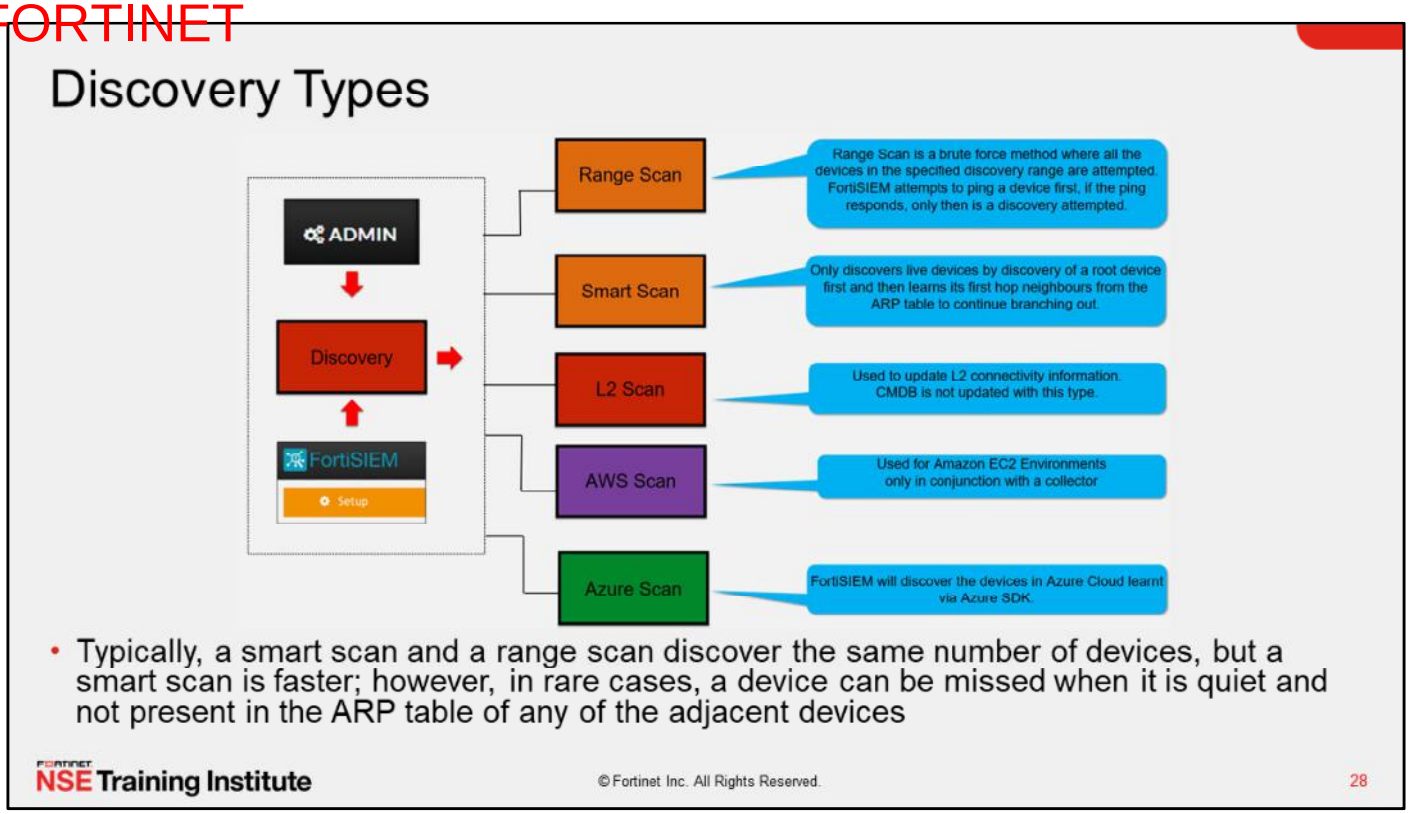
After you define and associate your credentials, you can test them using the test connectivity function provided in FortiSIEM. There are two options available for testing: test connectivity and also test connectivity without ping.

By default, when you select the **Test Connectivity** option, FortiSIEM pings the device to see if that device is alive before it tests the credentials. But, if a device has a firewall that doesn't respond to ping, the **Test Connectivity** option won't work. In this case, you would use the option **Test Connectivity Without Ping**. When you select this option, FortiSIEM *does not* do the ping before it tests the credentials.

If the test fails, your discovery will fail. Take note of the responses you get from the connectivity test. If the test is unsuccessful, the message it returns will give you some idea of what went wrong. Correct the issue, and test again. Make sure that the connectivity test is successful, before moving on to discovery.

Vouchers & Dumps are Available | WhatsApp +201224560923

DO NOT REPRINT
© FORTINET
Brave-dumps.com



FortiSIEM includes these discovery options: a range scan, a smart scan, an L2 scan, an AWS scan, and an Azure scan. The most commonly used options are the range scan and smart scan.

When you use the range scan discovery method, FortiSIEM pings every IP address in the given range (ICMP echo request). If the ping succeeds, FortiSIEM then attempts a full discovery using the credentials provided. During the discovery phase, the capabilities of the device, along with key information such as hostname, type of device, and so on, will be discovered.

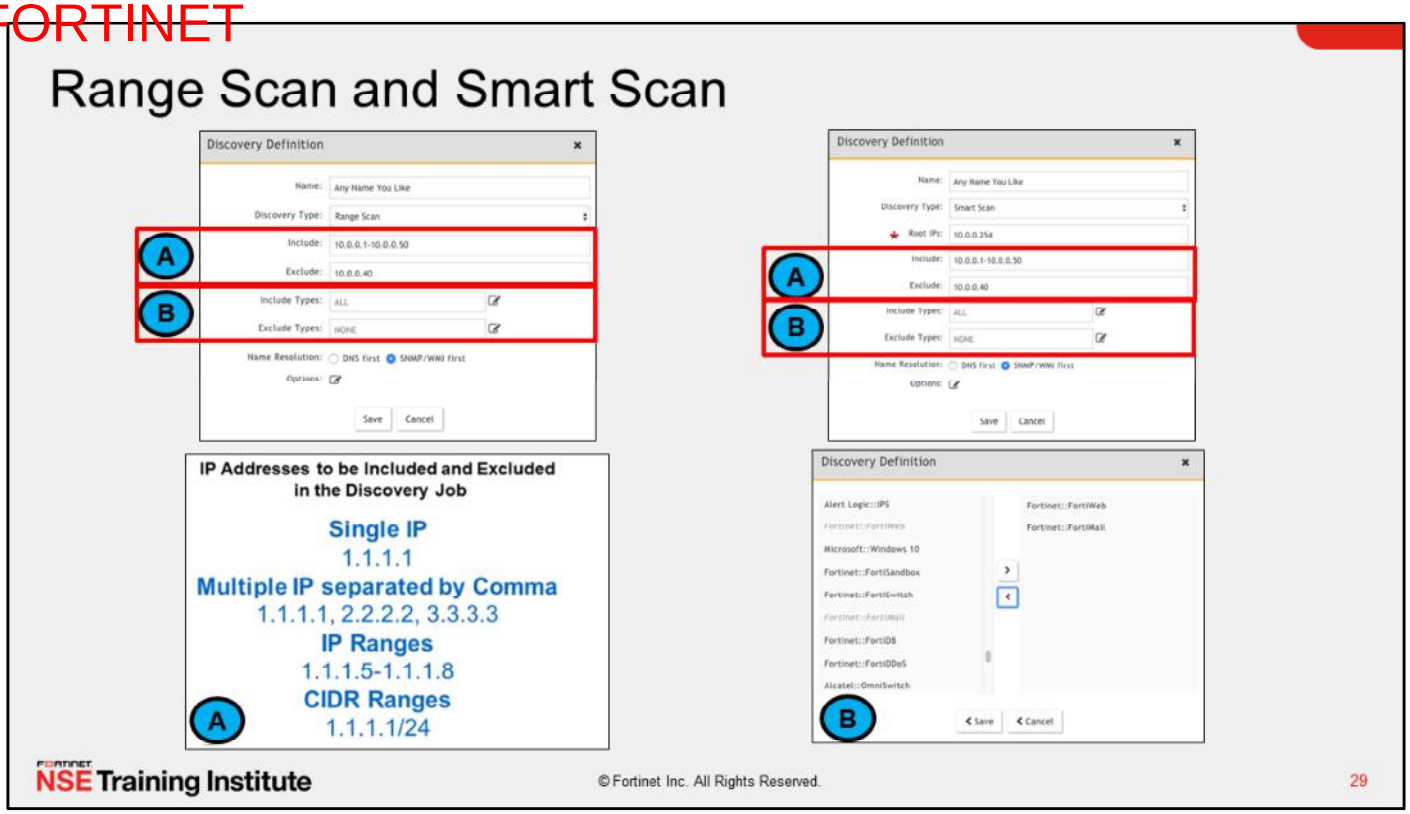
The smart scan discovery method is based on FortiSIEM iteratively learning about only the live devices in the network. In addition to an address range, a smart scan requires that root devices be provided. First, the root devices are discovered and then, from their routing table (provided by SNMP), all of their live one-hop neighboring IP addresses are learned. Then, each neighbor is discovered, using the provided credentials, and their one-hop neighbors are discovered. The process continues until there are no more new devices to be learned. Since only the live hosts are traversed, smart scan can be significantly faster than range scan.

A reasonably topologically connected layer 3 router/switch/firewall typically suffices as a root device. If a network device, such as a firewall, can block SNMP, then root devices on both sides of the firewall may need to be provided for discovering devices on both sides of the blocking device. Typically, the smart scan is faster than the range scan method. However, in rare scenarios, a device can be missed when it's quiet and not present in the ARP table of any of the adjacent devices.

The L2 scan is purely for updating the content addressable memory (CAM) table of switch-type devices. It is a smaller discovery that is not going to grab all of the performance metrics, such as CPU and memory. Because it is going to look at only the CAM table, it can be run quite frequently. The AWS scan and Azure scan methods, as the name suggests, are used to scan their respective environments.

Vouchers & Dumps are Available | WhatsApp +201224560923

DO NOT REPRINT
© FORTINET
Brave-dumps.com



The most common discovery types are range scan and smart scan.

The definitions of these discovery jobs are very similar, but the smart scan also requires the root IP of a layer 3 network device.

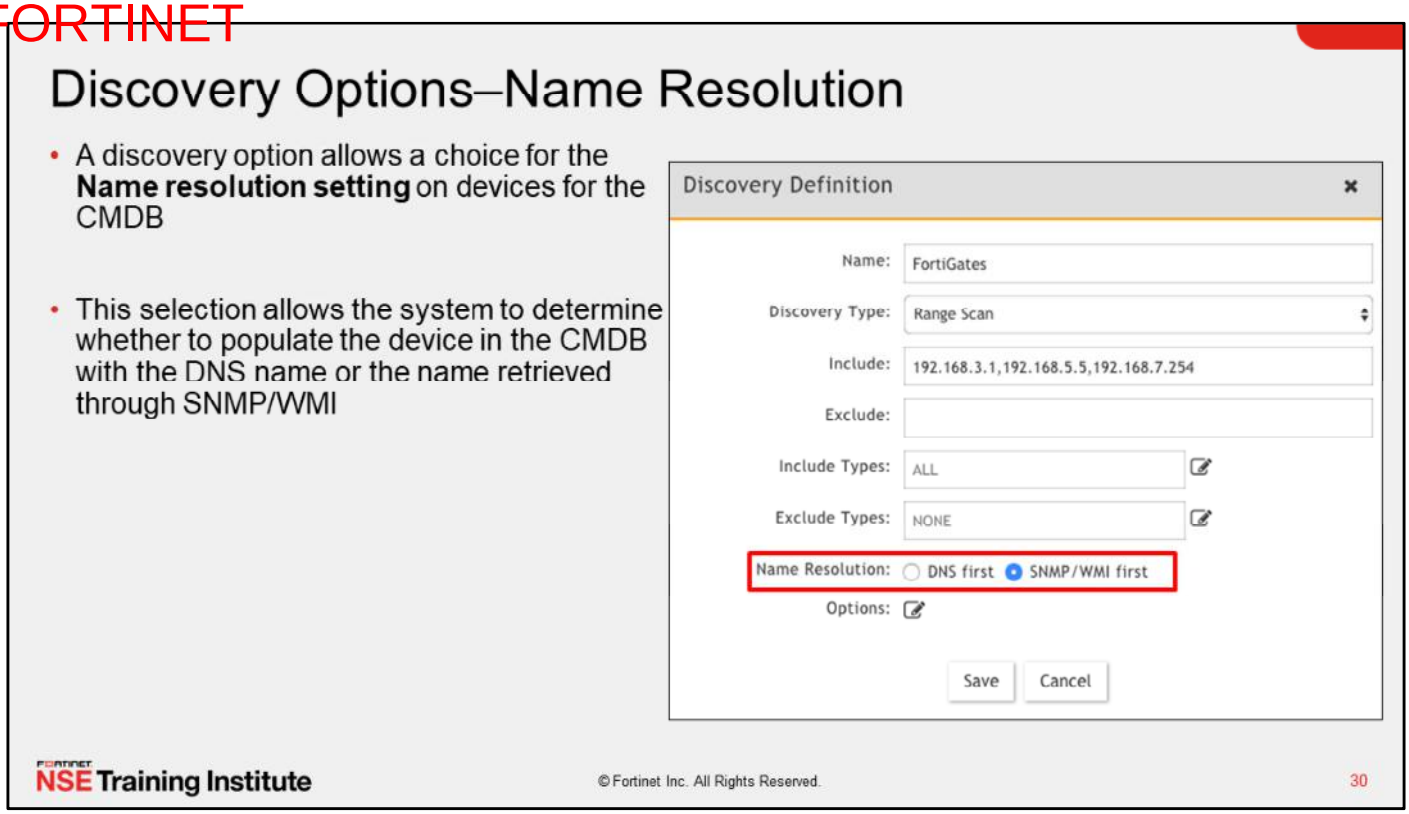
When you run either discovery job, you must:

1. Specify a name for the discovery job.
2. Specify an IP address range to be discovered:
   - You can specify a single IP address, multiple IP addresses, IP ranges, or CIDR ranges
   - You can exclude IP addresses from the range
3. Include or exclude specific device types from the discovery job. For example, you might want to scan only for Windows server, or you want to exclude Cisco or Juniper devices.

Between the inclusion and exclusion of IP addresses, and the inclusion and exclusion of device types, you have very granular control over what is discovered by the discovery jobs.

Vouchers & Dumps are Available | WhatsApp +201224560923

DO NOT REPRINT
© FORTINET
Brave-dumps.com



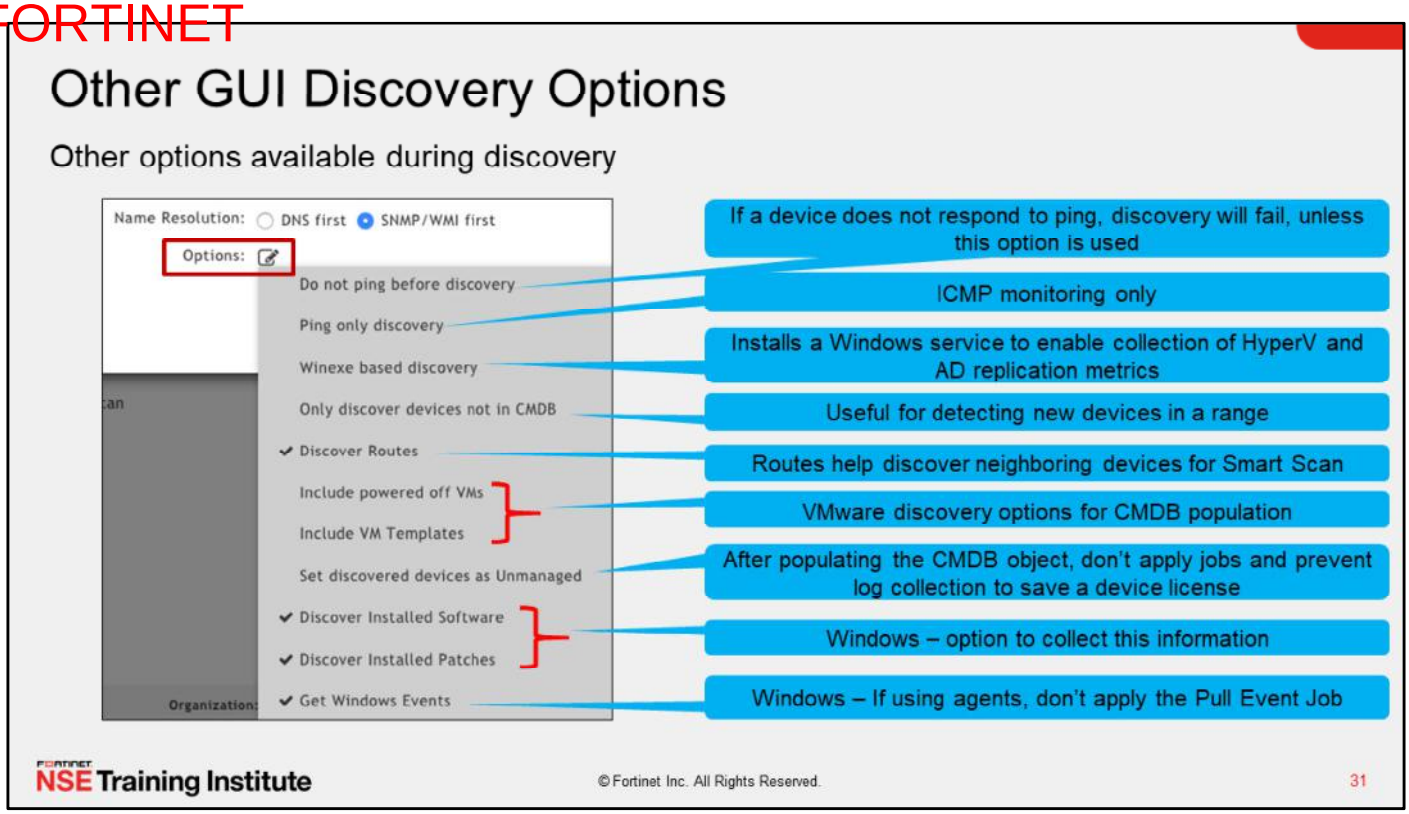
A discovery option allows a choice for Name Resolution on devices for the CMDB.

This selection allows the system to determine whether to populate the device in the CMDB with the DNS name or the name retrieved through SNMP/WMI first.

Host names can learn from DNS look up or SNMP/WMI. If these do not match, then choose a discovery method with a higher priority. For example, if DNS is chosen, then FortiSIEM will get host names from DNS. If DNS lookup fails for an IP, the host names will be obtained from SNMP/WMI.

Vouchers & Dumps are Available | WhatsApp +201224560923

DO NOT REPRINT
© FORTINET
Brave-dumps.com

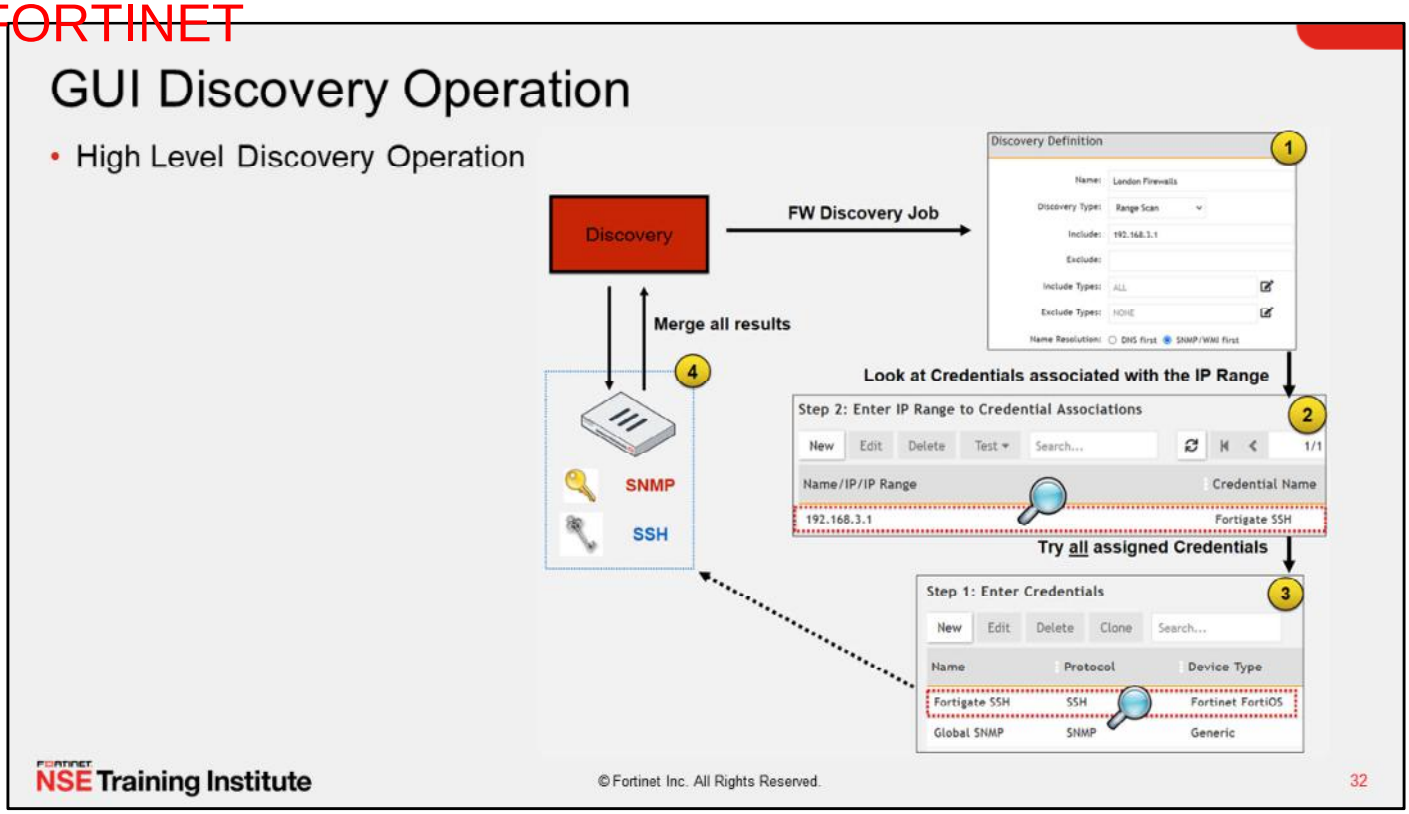


There are other options that you can select when you define a smart scan or range scan discovery:

- **Do not ping before discovery:** By default, FortiSIEM tries to ping a device, before discovery, to see if it's alive. If the ping fails, then FortiSIEM won't attempt to discover that device. If you are trying to discover a device that is running a firewall, or if there is a firewall between FortiSIEM and that device, the ping may fail. When you select the **Do not ping before discovery** option, FortiSIEM doesn't attempt to ping the device, and goes directly to the discovery. However, because FortiSIEM uses ICMP to determine availability metrics, or the ping stat job, if you select this option, FortiSIEM will not be able to apply a ping stat metric to that device.
- **Ping only discovery option**: If you have a device in your network that doesn't support SNMP, or if you have a device that FortiSIEM doesn't support at all, you might want to simply ping that device, to see if it's up and running. When you select the **Ping only on discovery** option, FortiSIEM will apply a ping state metric every one or two minutes, or it will constantly ping that device, and you can be notified if that device stops responding.
- **Only discover devices not in the CMDB**: This options is useful when you have already discovered your network, but you want to run scans periodically, to detect any devices that have recently been added to your network. When you select this option, the discovery ignores all of the devices that are already present in the CMDB.
- **Include powered off VMs** and **Include VM Templates**: These two options apply only to VMware monitoring. By default, when you discover VMware servers, FortiSIEM doesn't include powered off VMs or VMware templates. If you want to include those devices or templates in FortiSIEM, then select these options, as required.
- **Discover Routes**: This options is performed during a smart scan as it is hopping from router to router discovering devices.

Vouchers & Dumps are Available | WhatsApp +201224560923

DO NOT REPRINT
© FORTINET
Brave-dumps.com



Take a high-level look at the GUI discovery operation.

To set up a discovery job, you:
1. Defined your credentials
2. Associated those credentials against a particular IP address range in your network
3. Created a discovery job

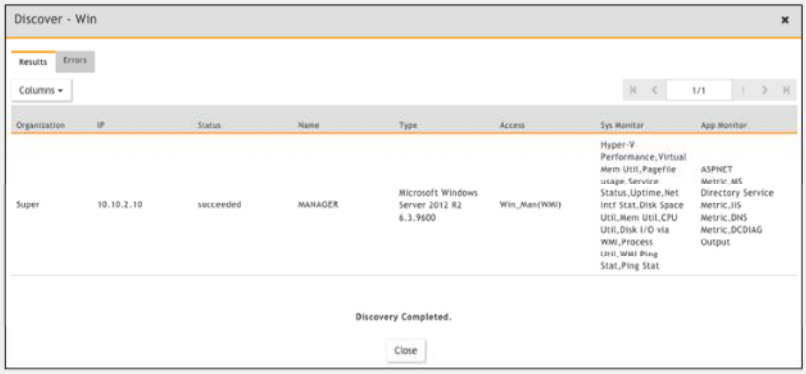
When you run the discovery job, FortiSIEM essentially takes those steps in reverse order. It:
1. Takes the IP addresses or range that were entered in the discovery job
2. Looks at what credentials have been assigned to each IP address
3. Uses the assigned credentials to collect various metrics from the devices
4. Merges the collected results and stores them in the CMDB

Vouchers & Dumps are Available | WhatsApp +201224560923

DO NOT REPRINT
© FORTINET
Brave-dumps.com

Viewing Live Discovery Results

- Once discovery is in progress a discovery Results pane appears.



- Results include the device IP address, name, access methods used, and any system and application monitors discovered
- The size of the IP range being discovered impacts how long the discovery will take

NSE Training Institute

© Fortinet Inc. All Rights Reserved.

33

Once you run a discovery, a discovery results pane appears with live data. The discovery results pane shows you every IP address that was discovered; regardless of whether it succeeded or failed. It also shows some information about the discovered devices.

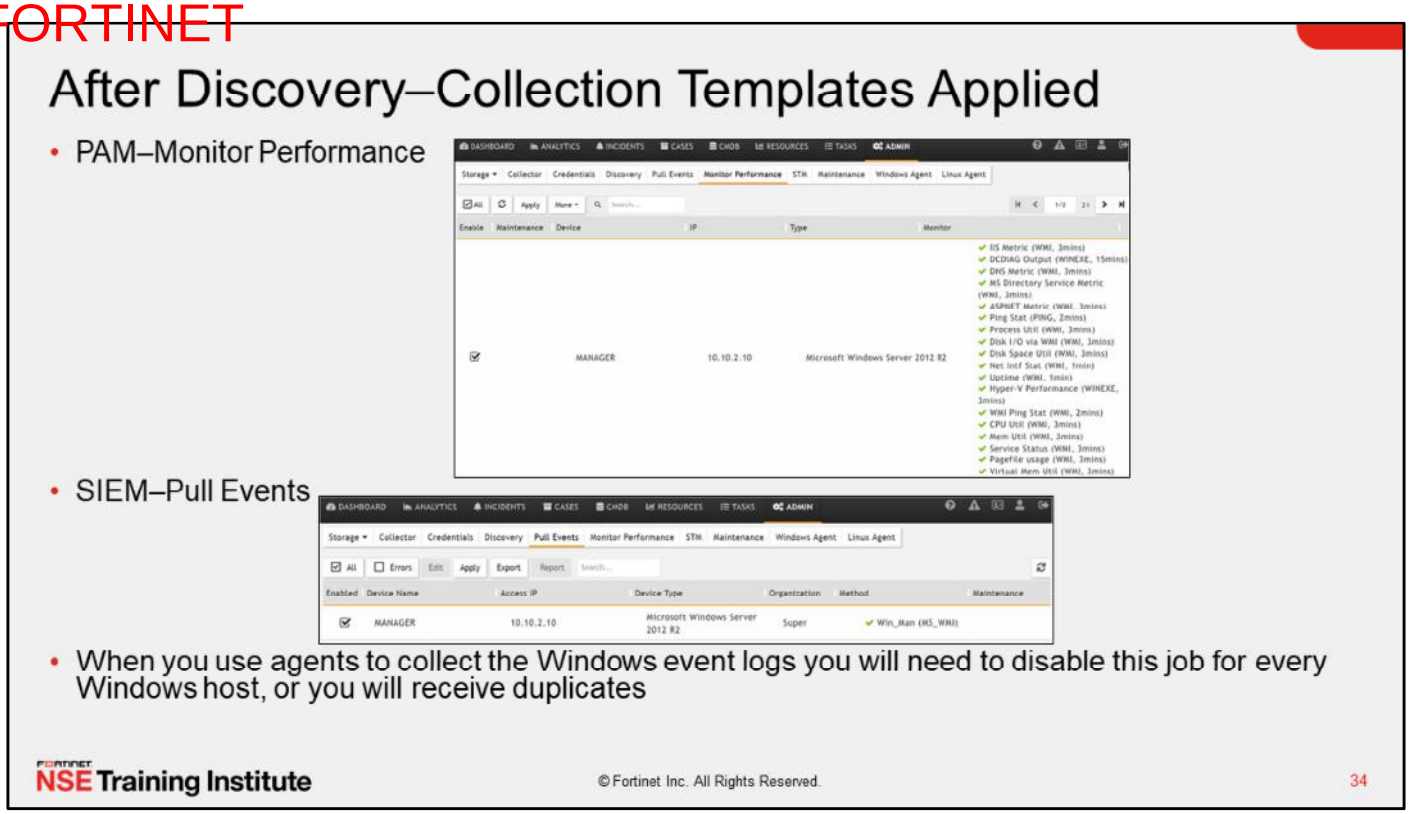
The discovery results pane includes a couple of options, located at the bottom of the screen, that allow you to stop the discovery, or run the discovery in background mode.

If you need to do a large discovery, selecting the **Run in Background** option allows you to carry out other tasks in the FortiSIEM interface, while the discovery is running.

The amount of time the discovery will take is dependent upon how many IP addresses are being discovered, and how many credentials were associated with those IP addresses.

Vouchers & Dumps are Available | WhatsApp +201224560923

DO NOT REPRINT
© FORTINET
Brave-dumps.com



After completing discovery, FortiSIEM does two things:

- It enters the discovered devices in the CMDB
- It applies the collection jobs for the discovered devices

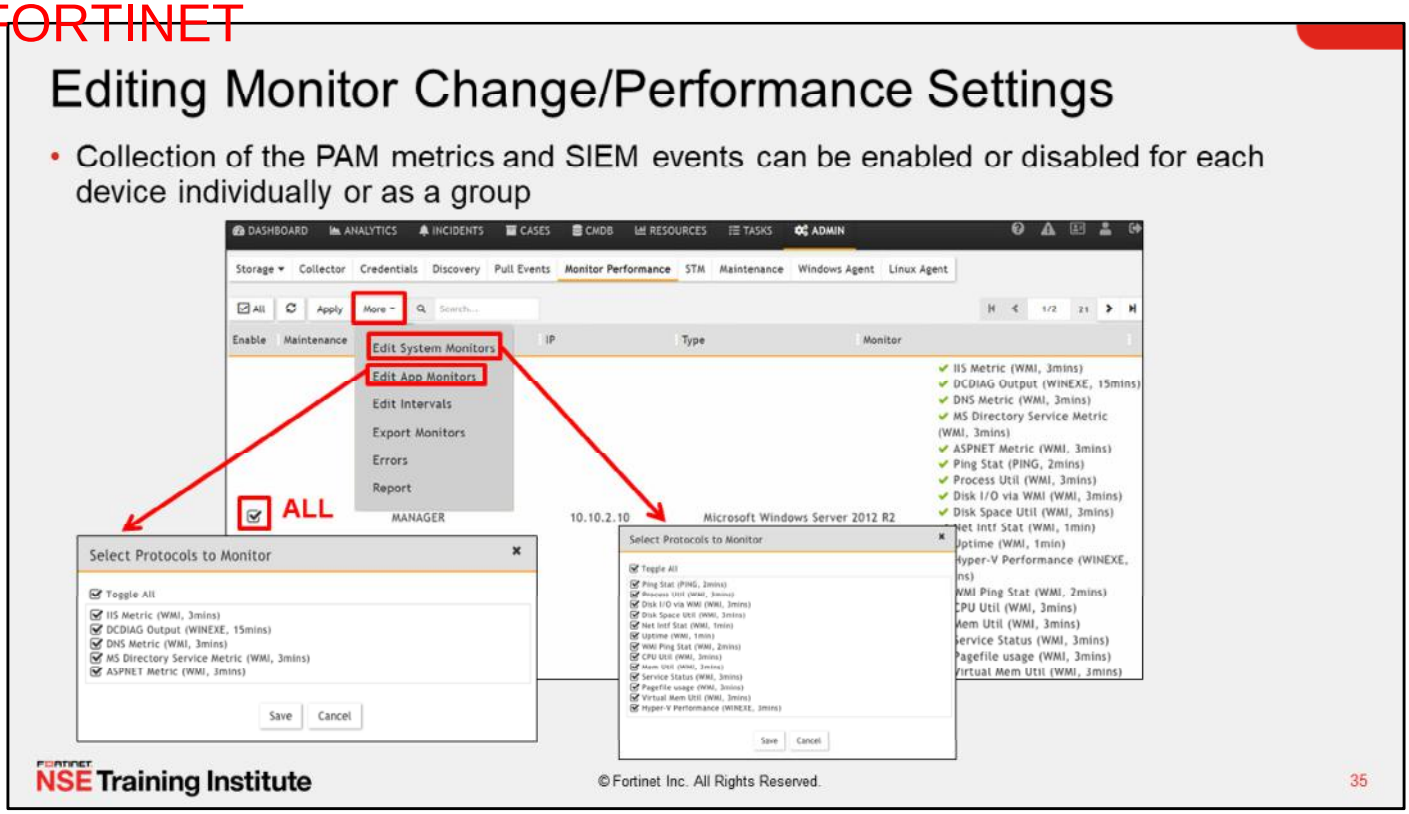
If you look at the **Monitor Performance** tab and the **Pull Events** tab, you will see the different collection jobs that FortiSIEM has applied. You will also see the metric that has been collected, such as the disk space utilization, the protocol that's been used to collect that data, and how often data is collected.

Discovery of any Windows server by FortiSIEM adds a **Pull Events** job by default for WMI. This **Pull Events** job is an agentless collection of system, security, and application event logs.

The system adds these jobs automatically. When you use agents to collect the same Windows event logs you will need to disable this job for every Windows host, or you will receive duplicates.

Vouchers & Dumps are Available | WhatsApp +201224560923

DO NOT REPRINT
© FORTINET
Brave-dumps.com



FortiSIEM is very customizable. You can edit various parameters on the **Monitor Change Performance** tab and the **Pull Events** tab.

There may be times when you don't want to collect a particular metric from a particular device. For example, you may want to turn off the ping stat metric, or the service status metric for a Windows server. If you click on **More** drop down list will appear select the **System Monitor** or the **Application Monitor** column, a window opens listing all of the metrics that are being collected. You can enable or disable the collection of any of those metrics. You can do the same in the **Pull Events** tab.

The **Enable** column holds an option that allows you to globally enable or disable the collection of all metrics. For example, if you are installing an application on this server and you don't want the collection process to run during the installation, you can turn off the collection of all metrics by disabling the check box in the **Enable** column. Collections for that device will be suspended. Once the installation is complete, you can come back here and re-enable the collection of PAM metrics.

Vouchers & Dumps are Available | WhatsApp +201224560923

DO NOT REPRINT
© FORTINET
Brave-dumps.com

Knowledge Check

1. If ping is disabled on a device, will FortiSIEM still collect availability metrics?
   - A. Yes
   - ✓ B. No

2. If an administrator sends syslogs from the FortiGate firewall, but does not perform a GUI discovery, will the device still appear in the CMDB?
   - ✓ A. Yes
   - B. No

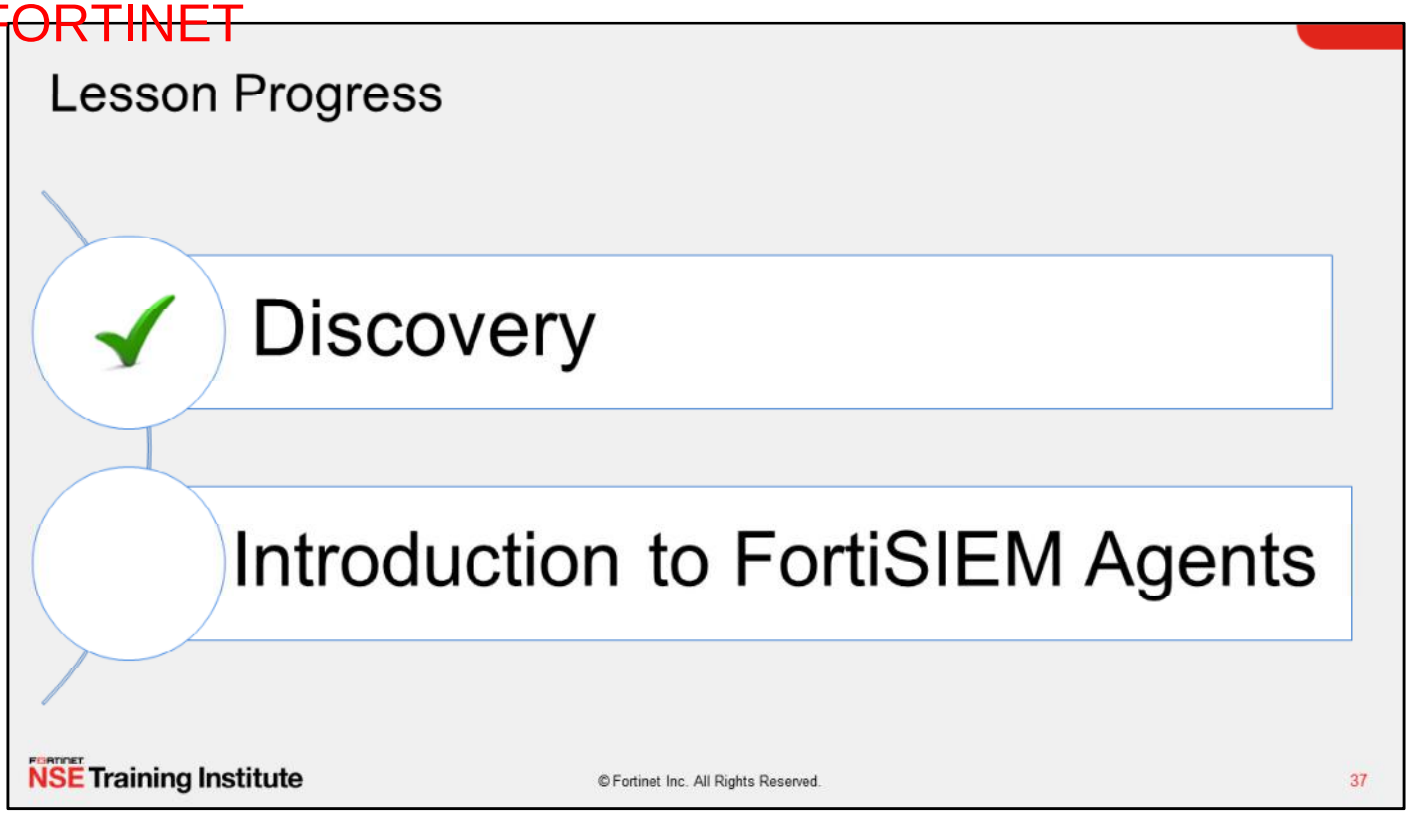
NSE Training Institute

© Fortinet Inc. All Rights Reserved.

36

Vouchers & Dumps are Available | WhatsApp +201224560923

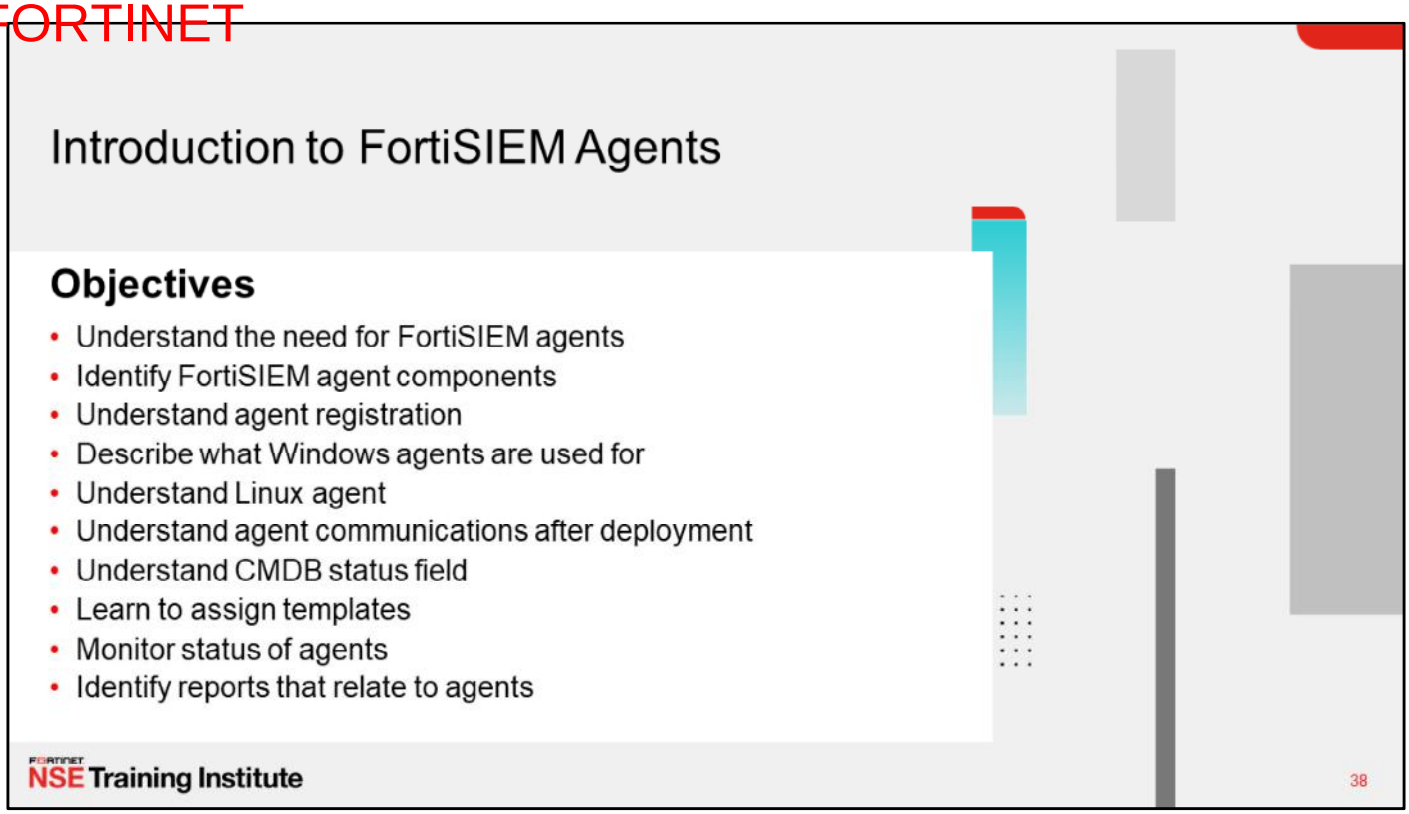
DO NOT REPRINT
© FORTINET
Brave-dumps.com



Good job! You now understand discovery. Now, you'll learn about FortiSIEM agents.

Vouchers & Dumps are Available | WhatsApp +201224560923

DO NOT REPRINT
© FORTINET
Brave-dumps.com

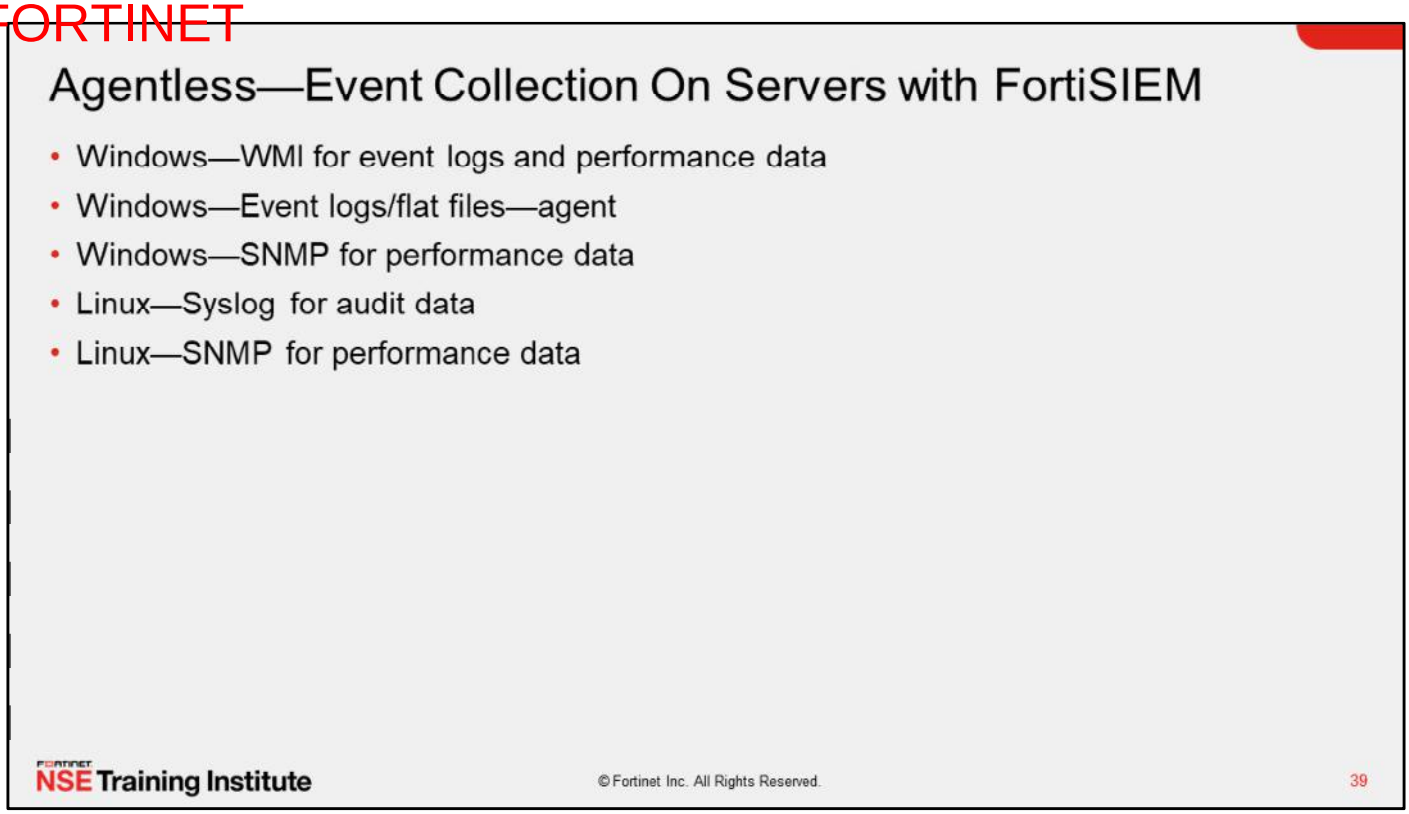


After completing this section, you should be able to achieve the objectives shown on this slide.

By demonstrating a competent understanding of FortiSIEM agents, you will be able to understand and deploy FortiSIEM agents in your network.

Vouchers & Dumps are Available | WhatsApp +201224560923

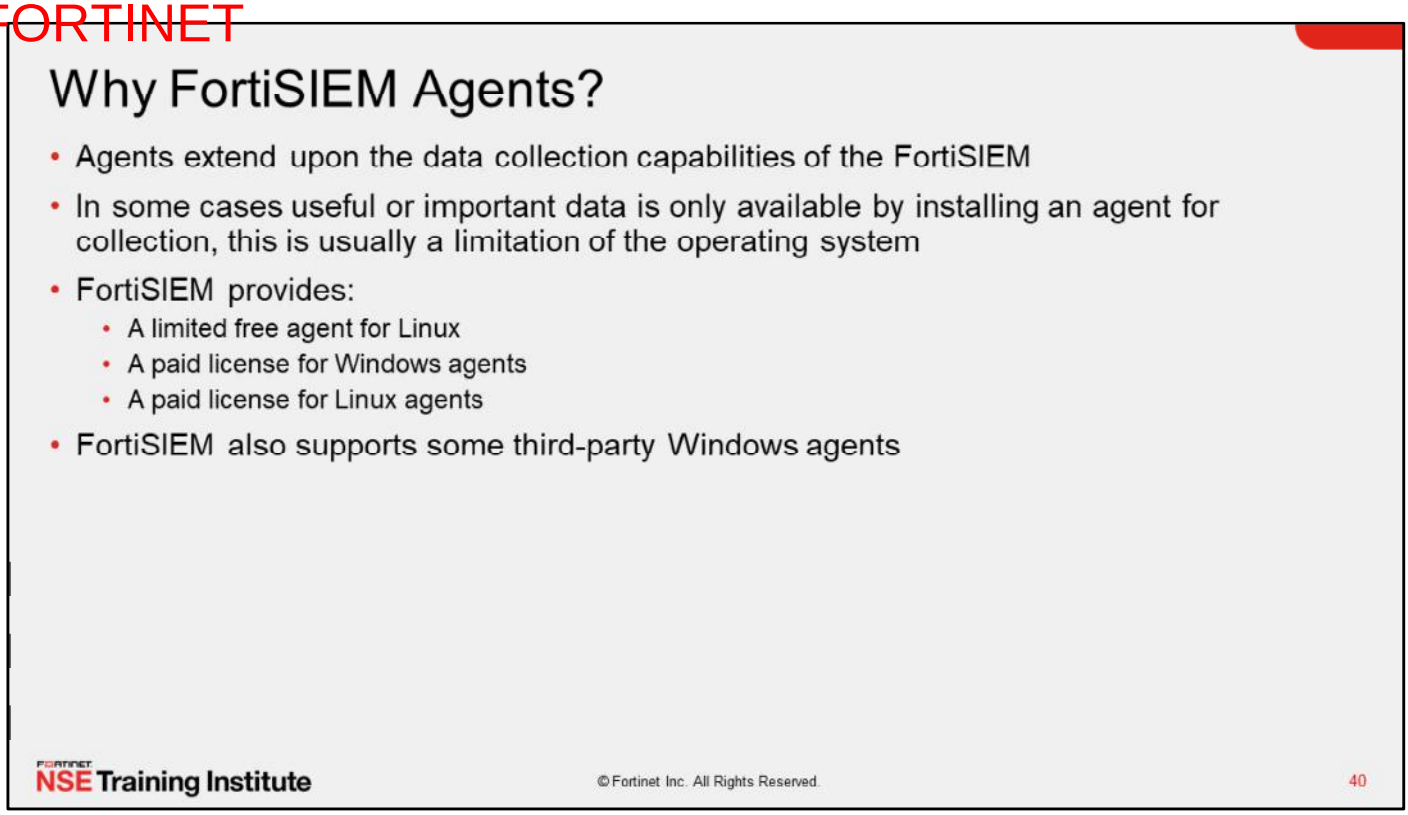
DO NOT REPRINT
© FORTINET
Brave-dumps.com



Some logs and performance metrics can be collected remotely from Windows servers through WMI, and SNMP, and by running Winexe commands. Some key performance metrics and file monitoring on Linux servers can be done through SSH, SNMP, and syslog.

Vouchers & Dumps are Available | WhatsApp +201224560923

DO NOT REPRINT
© FORTINET
Brave-dumps.com



There are few limitations when you rely completely on FortiSIEM to collect all types of logs from Windows and Linux servers. Some of those limitations are as follows:

- Not all metrics can be collected from a FortiSIEM Linux platform through WMI.
- Remotely running some programs, such `Winexe`, starts services on the servers, which may trigger security alerts in certain environments,
- WMI service often creates CPU load on the servers when a large number of logs are pulled through WMI,
- Collecting logs through polling from thousands of servers is not efficient. If a server is slow or unresponsive, you have to wait for the connection to time out. This this wastes resources.
- Linux servers send logs through syslog. However, if you want to collect file integrity monitoring data, then some configuration must be done remotely.

Agents provide a clean and efficient way to collect exactly the data that is needed. FortiSIEM agents are very lightweight and do not consume more than 5% of system CPU and memory. Logging data is collected and delivered over a secured channel to the collector.

Vouchers & Dumps are Available | WhatsApp +201224560923

DO NOT REPRINT
© FORTINET
Brave-dumps.com

FortiSIEM Agent Components

- In all deployments, there is one supervisor node and, optionally, worker and/or collector nodes, depending on the chosen architecture





- The supervisor node now has an integrated agent manager component which manages FortiSIEM Windows and Linux agents
- Collectors can be multi-tenant for special cases

NSE Training Institute

© Fortinet Inc. All Rights Reserved.

41

In all types of deployments, there is always one supervisor node. You can also add worker or collector nodes, depending on the chosen type of architecture.

The supervisor node has an integrated agent manager component that can manage FortiSIEM Windows and Linux agents. Windows Agents (version 3.1 and onwards), can be configured and managed from the FortiSIEM GUI. Windows agent manager is not required. As long as a license is available, you can install Windows agents and register on the FortiSIEM supervisor node.

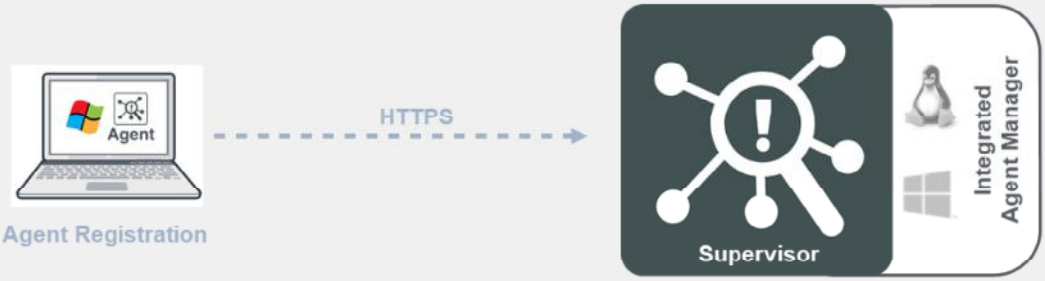
Linux agent require a license. You can install a Linux agent and register on the FortiSIEM supervisor node. You can configure and manage Linux agents from the FortiSIEM GUI.

Vouchers & Dumps are Available | WhatsApp +201224560923

DO NOT REPRINT
© FORTINET
Brave-dumps.com

Agent Registration

- Agents register with the supervisor node



- Agents automatically belong to the organization detailed in the `InstallSettings.xml` (win) file or Linux command line and an entry appears in the CMDB
- Ensure that any firewall located between the agents and the supervisor permit HTTPS traffic on port 443

NSE Training Institute

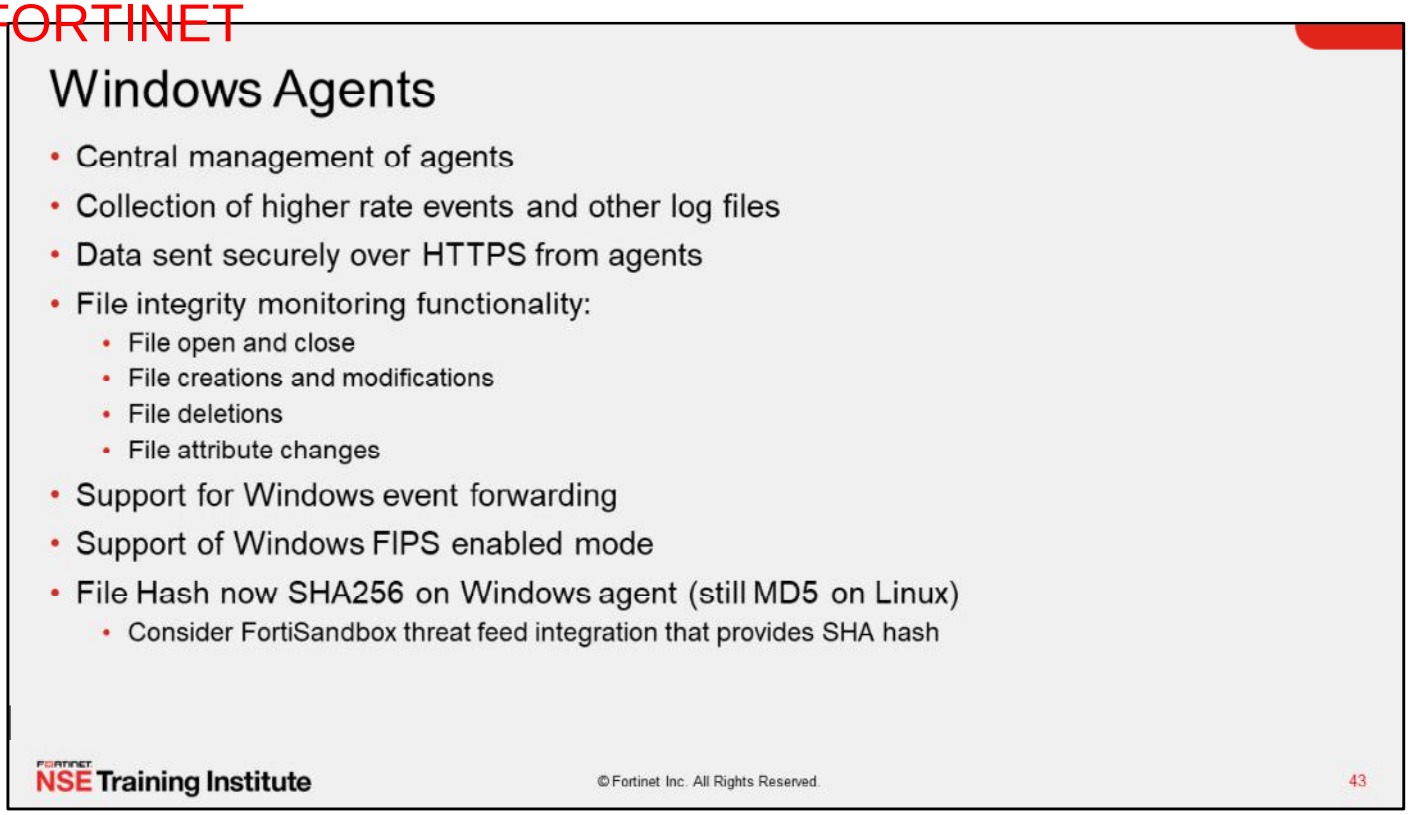
© Fortinet Inc. All Rights Reserved.

42

Agents register with the supervisor node using HTTPS protocol. Ensure that any firewall between the agents and supervisor node permits HTTPS traffic on port 443. Agents automatically belong to the organization detailed in the `InstallSettings.xml` file for Windows, and the Linux command line for Linux agents. Every registered agent appears as an entry in the CMDB.

Vouchers & Dumps are Available | WhatsApp +201224560923

DO NOT REPRINT
© FORTINET
Brave-dumps.com

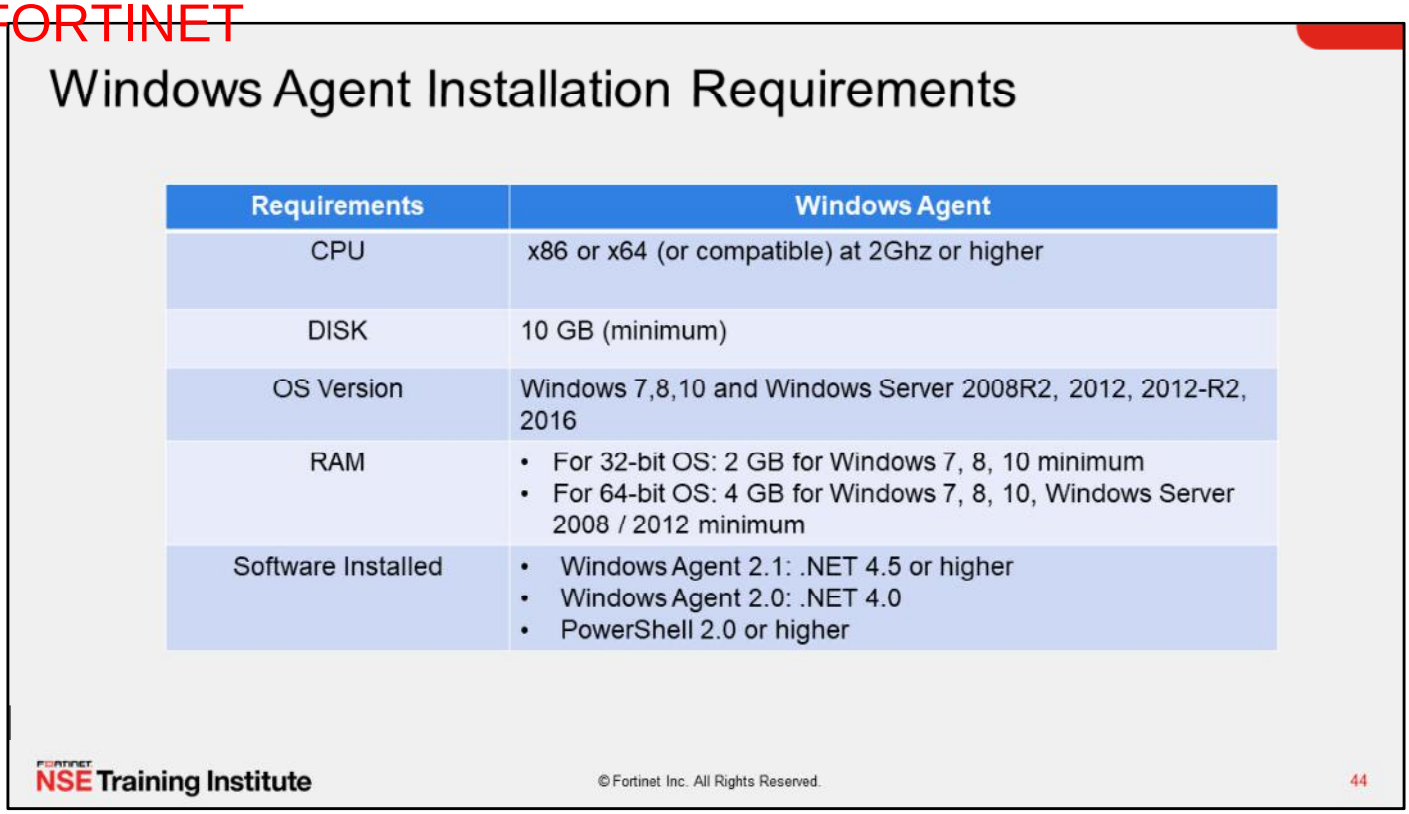


FortiSIEM Windows agents have the following functionality:

- They can be managed centrally from FortiSIEM supervisor node
- They collect all Windows event logs, including security, application, and performance event logs; DHCP/DNS logs; Sysmon logs, and so on. Agents can collect logs and forward them to the FortiSIEM supervisor or collector at a very high rate.
- They send all the data and logs that they collect to FortiSIEM securely over HTTPS.
- Agents that perform file integrity monitoring:
    - Collect custom log files
    - Detect registry changes
    - Detect file read, write, and edits (FIM) with added user context
- They support Windows event forwarding. When Windows even forwarding is installed on a central server, it can collect all events from various Windows servers and send them to the FortiSIEM node.
- They support Windows in FIPS enabled mode.
- Note that on Windows agents, the file hash is now SHA256. (On Linux agents, the file hash is still MD5.) Consider using FortiSandbox threat feed integration, which provides SHA hash capabilities.

Vouchers & Dumps are Available | WhatsApp +201224560923

DO NOT REPRINT
© FORTINET
Brave-dumps.com



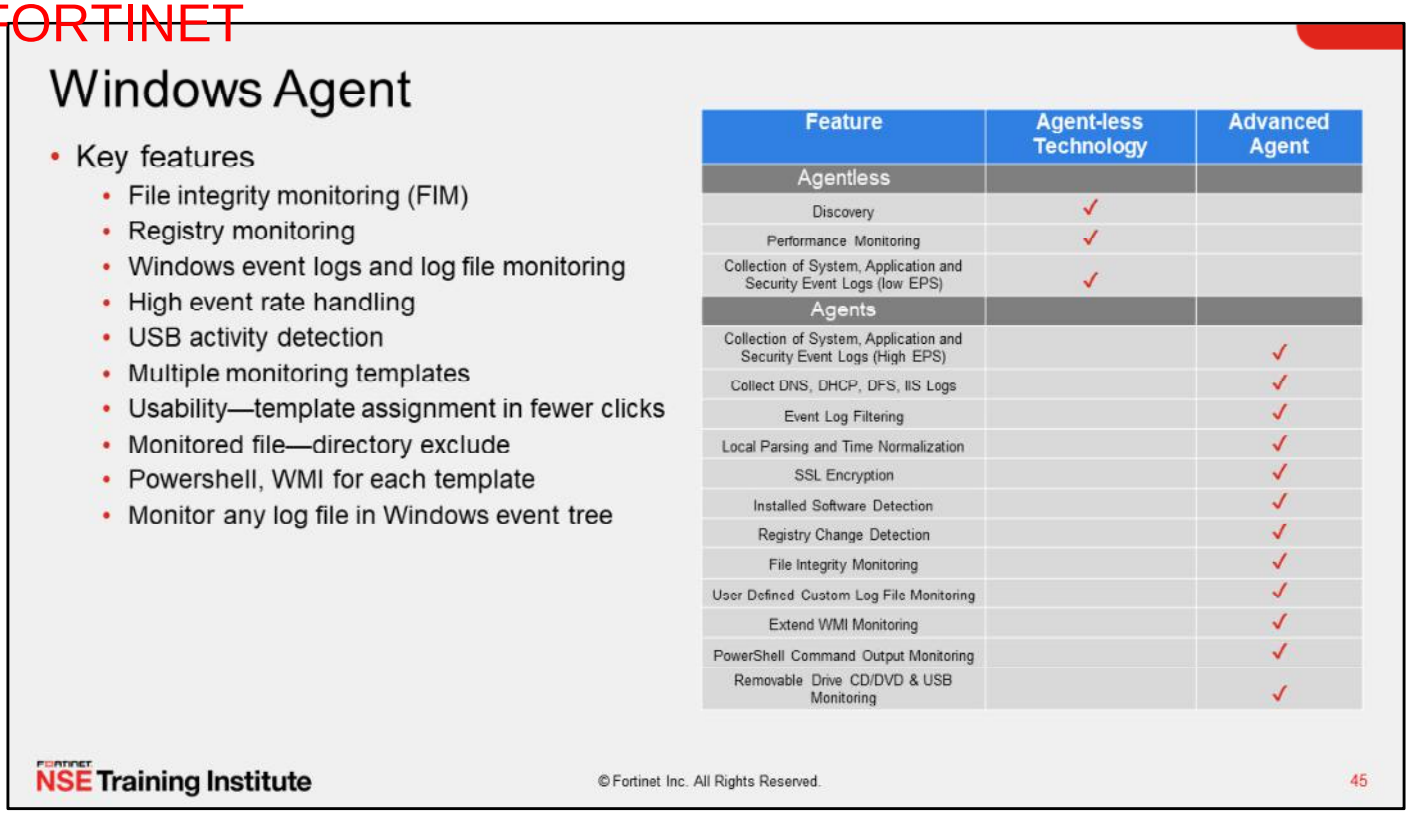
FortiSIEM Windows Agent 3.0 runs on the following operating systems:

- Windows 7 Enterprise/Professional
- Windows 8
- Windows 10
- Windows Server 2008 R2
- Windows Server 2012
- Windows Server 2012 R2
- Windows Server 2016

You need a minimum of 10 GB disk space, a 2-GHz or higher CPU, 2 GB or 4 GB of RAM, depending on the OS, and .NET framework software must be installed.

Vouchers & Dumps are Available | WhatsApp +201224560923

DO NOT REPRINT Brave-dumps.com
© FORTINET



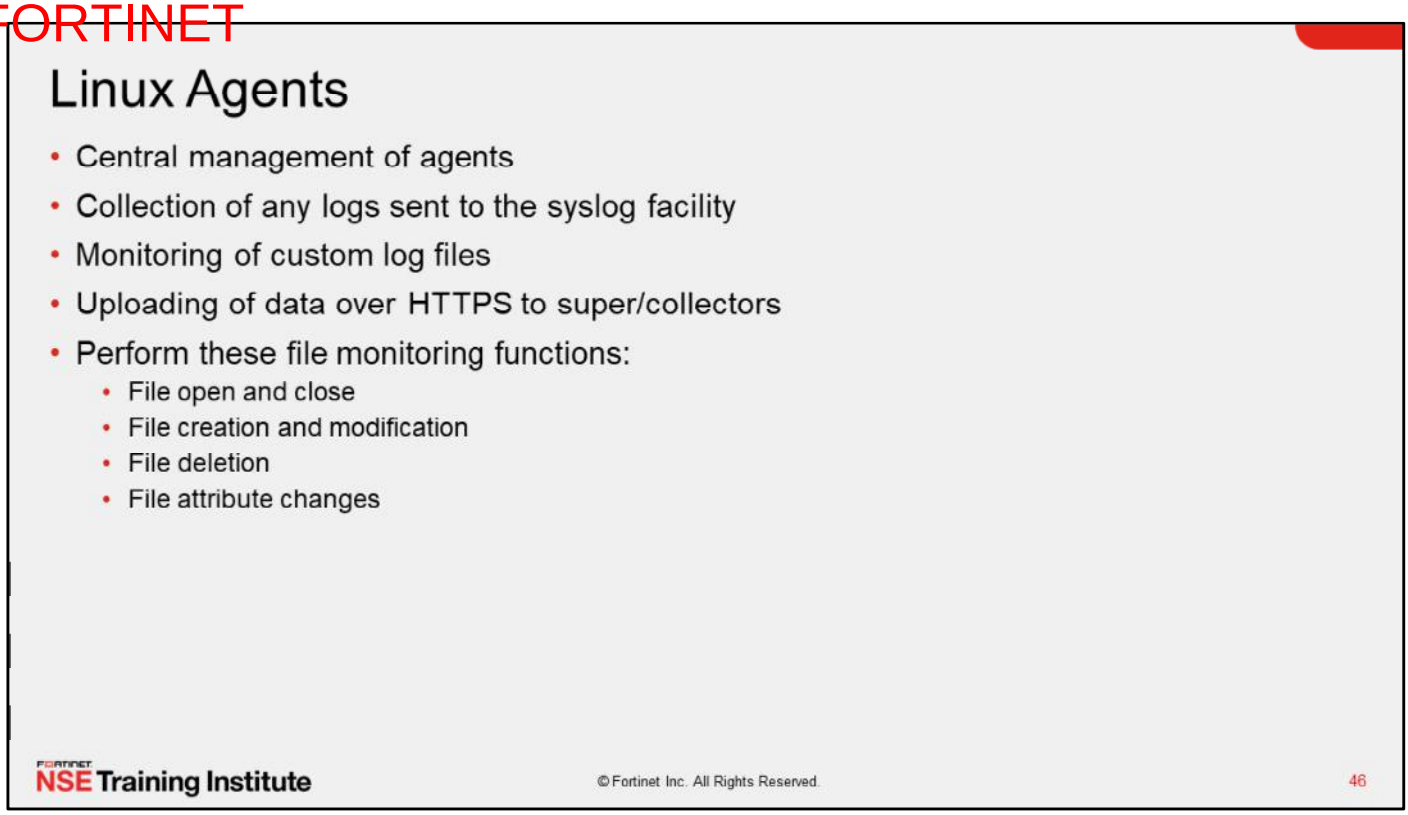
Windows agents provide a clean and efficient way to collect exactly the data that you need. FortiSIEM agents are lightweight and do not consume more than 5% of system CPU and memory. FortiSIEM Windows agents have the following functionality:

- Collect any Windows event log including security, application and performance event logs, DHCP/DNS logs, Sysmon logs, and so on.
- Collect custom log files.
- Detect registry changes.
- Detect file read, write, and edits (FIM) with added user context.
- Run any powershell command and send the output as logs, which allows users to capture data at periodic intervals and send to FortiSIEM.
- Detect removable media insertion, deletion, read, and write.

The FortiSIEM agent manager can manage a large number of FortiSIEM Windows agents using configuration templates. You need to create a template and associate it with the servers. You can configure Windows agents to send logs to FortiSIEM collectors.

Vouchers & Dumps are Available | WhatsApp +201224560923

DO NOT REPRINT
© FORTINET
Brave-dumps.com



FortiSIEM Linux agents, which is a paid version, provides a scalable way to collect logs and other telemetry from Linux systems in a secure and optimized manner. Linux servers send logs through Syslog.
However, if you want to collect file integrity monitoring data, then you must perform specific configuration remotely.
For that purpose, you can use the Linux agent, which can do the following:

- Central management of agents
- Collect any logs sent to the syslog facility
- Monitor custom log files
- Upload data over HTTPS to super/collectors
- Perform these file monitoring functions:
    - File open and close
    - File creation and modification
    - File deletion
    - File attribute changes

Vouchers & Dumps are Available | WhatsApp +201224560923

DO NOT REPRINT
© FORTINET
Brave-dumps.com

Linux Agent – Linux Agent Installation Requirements

- The FortiSIEM Linux Agent runs on the following operating systems:
- CentOS 6.x and 7.x
- Redhat Enterprise Linux 6.x and 7.x
- Ubuntu 14.04, 16.04, 18.04, 20.04 LTS
- Amazon Linux 1 and Amazon Linux 2

Requirements	Windows Agent
CPU	1 x vCPU x64 at 1.5Ghz or higher
DISK	1 GB (minimum), agent used ~ 300MB
OS Version	CentOS 6.x and 7.x Redhat Enterprise Linux 6.x and 7.x Ubuntu 14, 16, 18 Amazon Linux 1 and Amazon Linux 2
Memory	• 512MB or higher, agent uses <100MB

NSE Training Institute

© Fortinet Inc. All Rights Reserved.

47

FortiSIEM Linux Agent has been tested to run on the following Linux operating systems:

- CentOS 6.9 and later
- CentOS 7.4 and later
- Red Hat Enterprise Linux 6.9 and later
- Ubuntu 14.04, 16.04, 18.04, 20.04 LTS
- Amazon Linux 1 and Amazon Linux 2

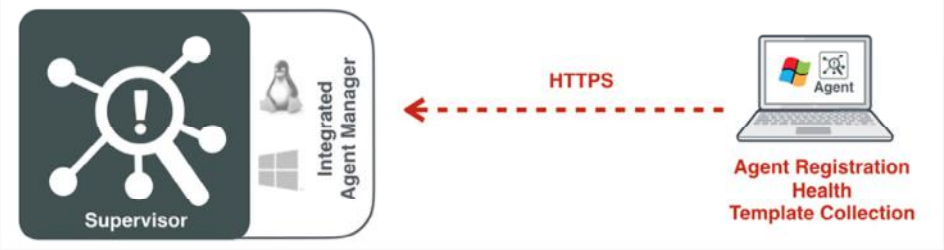
You need a minimum of 1GB disk space, a 1.5Ghz or higher CPU, and 512 MB or higher of RAM.

Vouchers & Dumps are Available | WhatsApp +201224560923

DO NOT REPRINT
© FORTINET
Brave-dumps.com

Agent Communications After Installation

- Agents maintain communication with the supervisor after initial installation



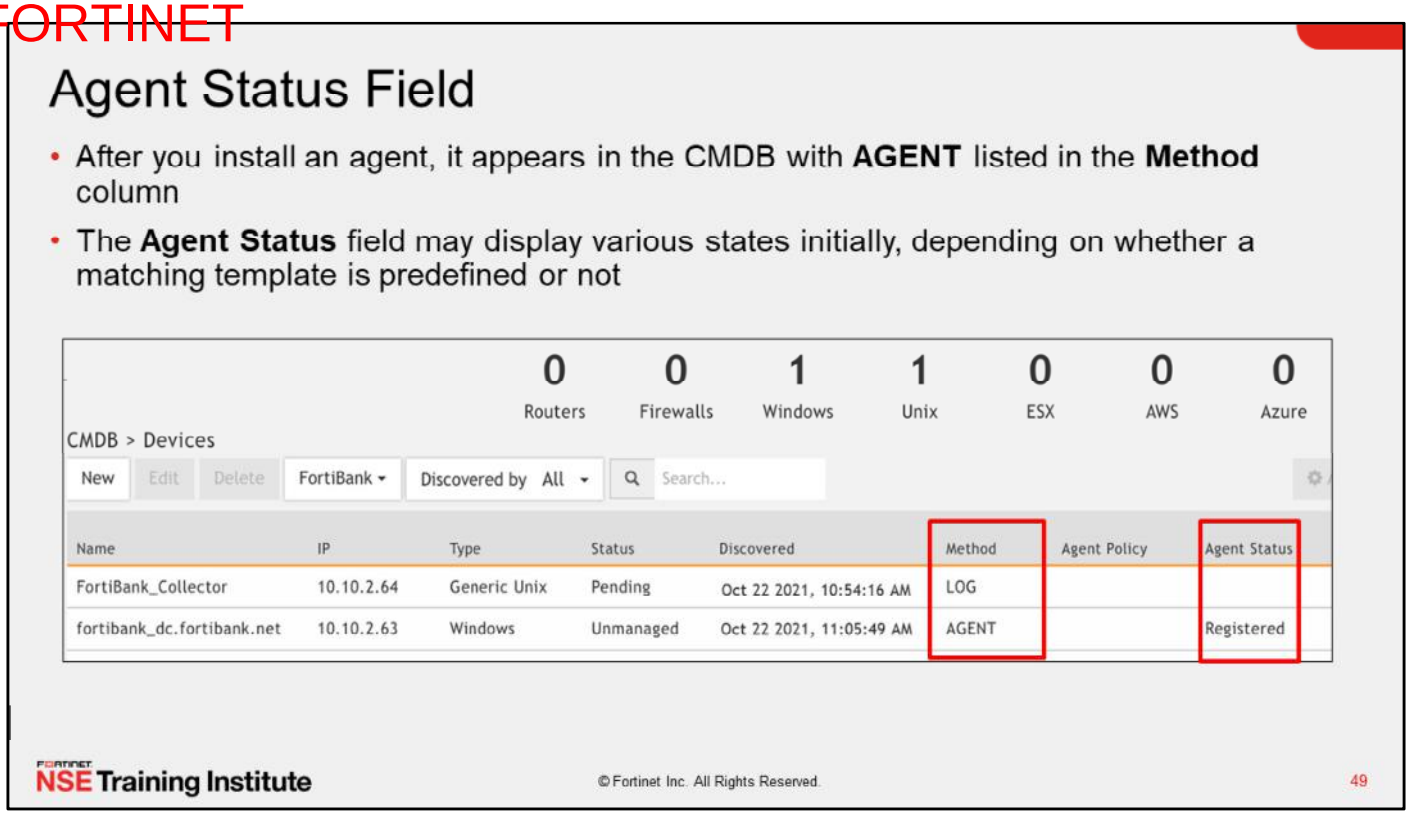
- This serves two purposes:
  - Report agent status and health
  - Poll and collect any new agent templates
- Each agent will poll the supervisor every one minute, by default

NSE Training Institute
© Fortinet Inc. All Rights Reserved.
48

The agents continue to communicate with the supervisor node after initial installation. There are two reasons for that: one is to report agent status and health and the other is to poll and collect any new agent templates. By default, every agent polls the supervisor every one minute.

Vouchers & Dumps are Available | WhatsApp +201224560923

DO NOT REPRINT
© FORTINET
Brave-dumps.com

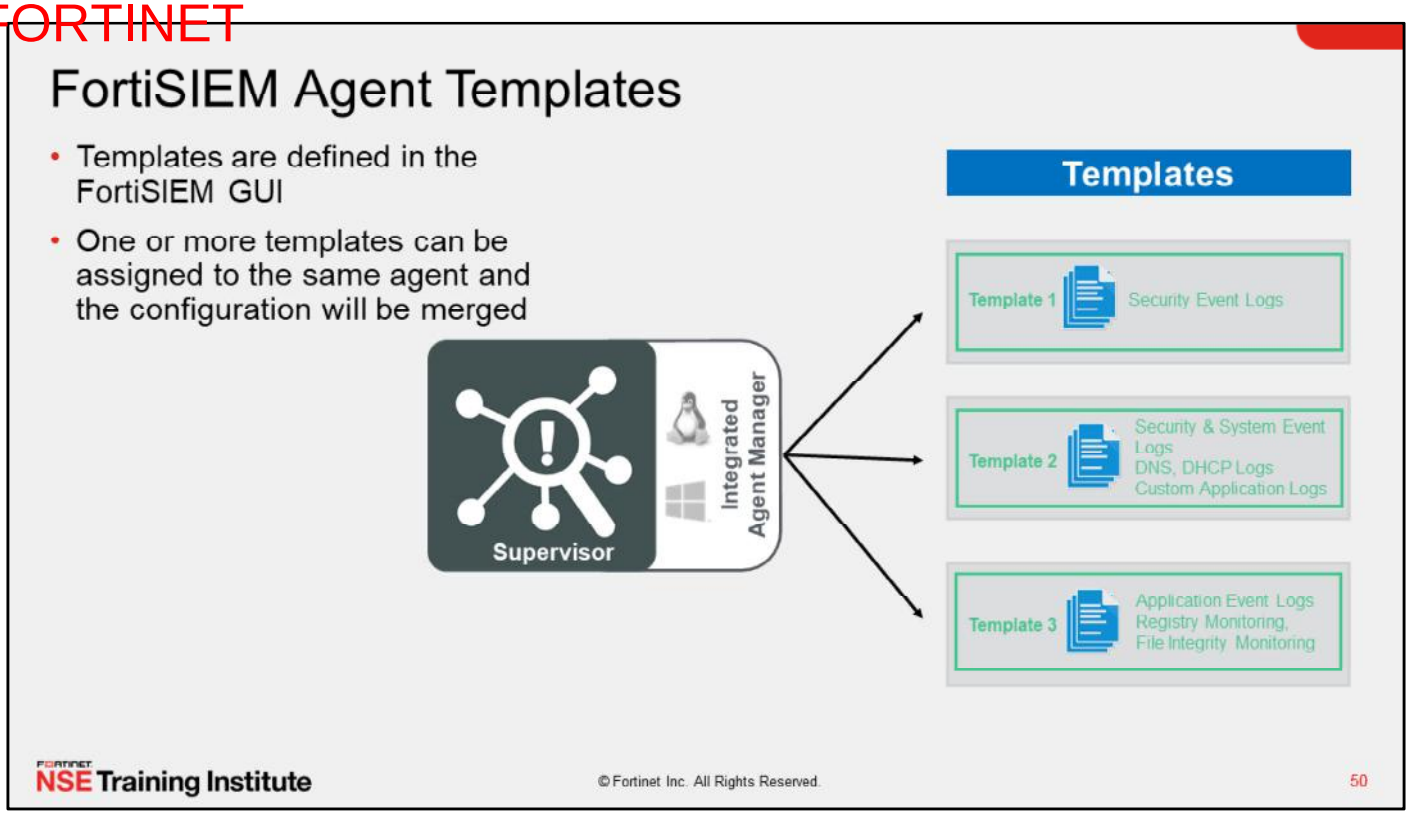


After you install an agent, it appears in the CMDB with **AGENT** listed under the **Method** column**.** The **Agent Status** field may display various states initially depending upon whether a matching template is predefined or not.

The following agent status values are possible:
Registered: The agent has completed registration but has not received the monitoring template.
Running Active: The agent has received a monitoring template and it is performing properly.
Running Inactive: The agent is running, but does not have a monitoring template. The reasons could be that there is no license, or there is an incomplete definition; that is, no collector or template is defined for that host.
Stopped: The agent is stopped on the Linux server.
Disconnected: The supervisor did not receive any status from the agent for the last 10 minutes.

Vouchers & Dumps are Available | WhatsApp +201224560923

DO NOT REPRINT
© FORTINET
Brave-dumps.com



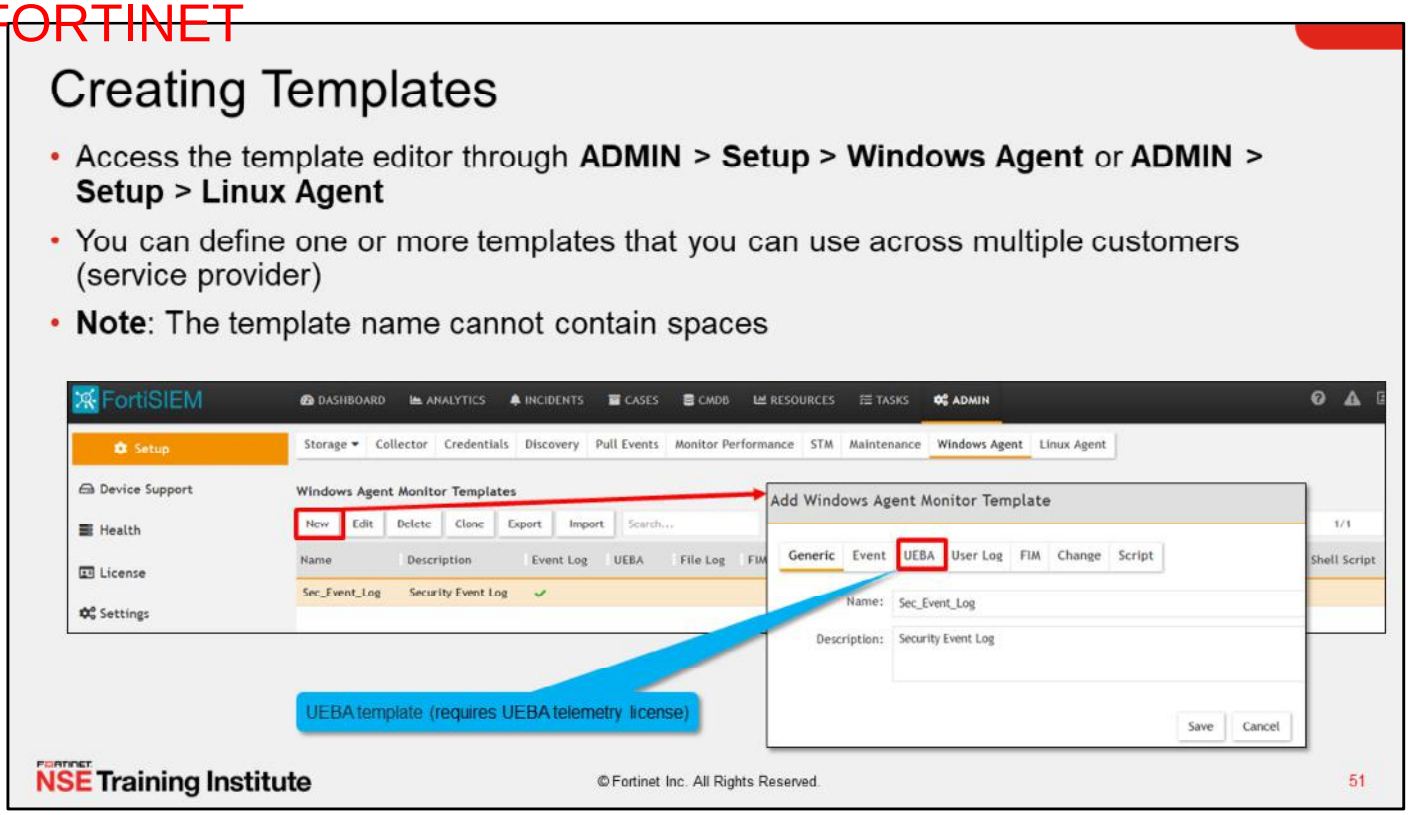
Templates are defined in the FortiSIEM GUI. You can assign one or more templates to the same agent and the configuration will be merged.

Templates define security event logs, system event logs, DNS logs, DHCP logs, custom application logs, file integrity monitoring logs, and so on.

For example, you might use template 1 to collect Windows event logs, template 2 to collect Windows event logs or application logs from DNS and DHCP, and so on.

Vouchers & Dumps are Available | WhatsApp +201224560923

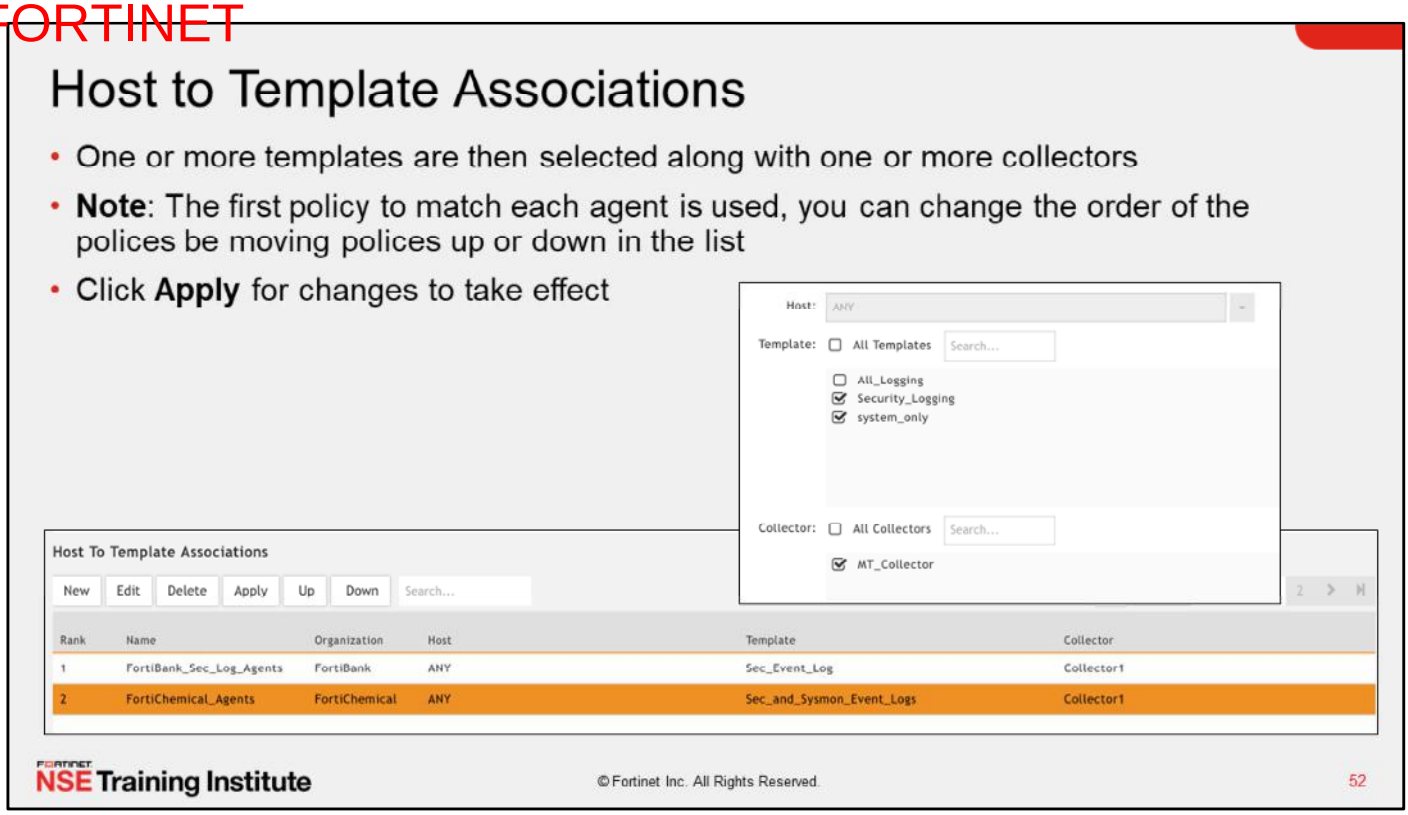
DO NOT REPRINT
© FORTINET
Brave-dumps.com



You can create, edit, or delete a template from **ADMIN** > **Setup** > **Windows** or **ADMIN> Setup > Linux Agent**. You can use the templates across multiple customers or service providers. Remember that the template name cannot contain spaces.

Vouchers & Dumps are Available | WhatsApp +201224560923

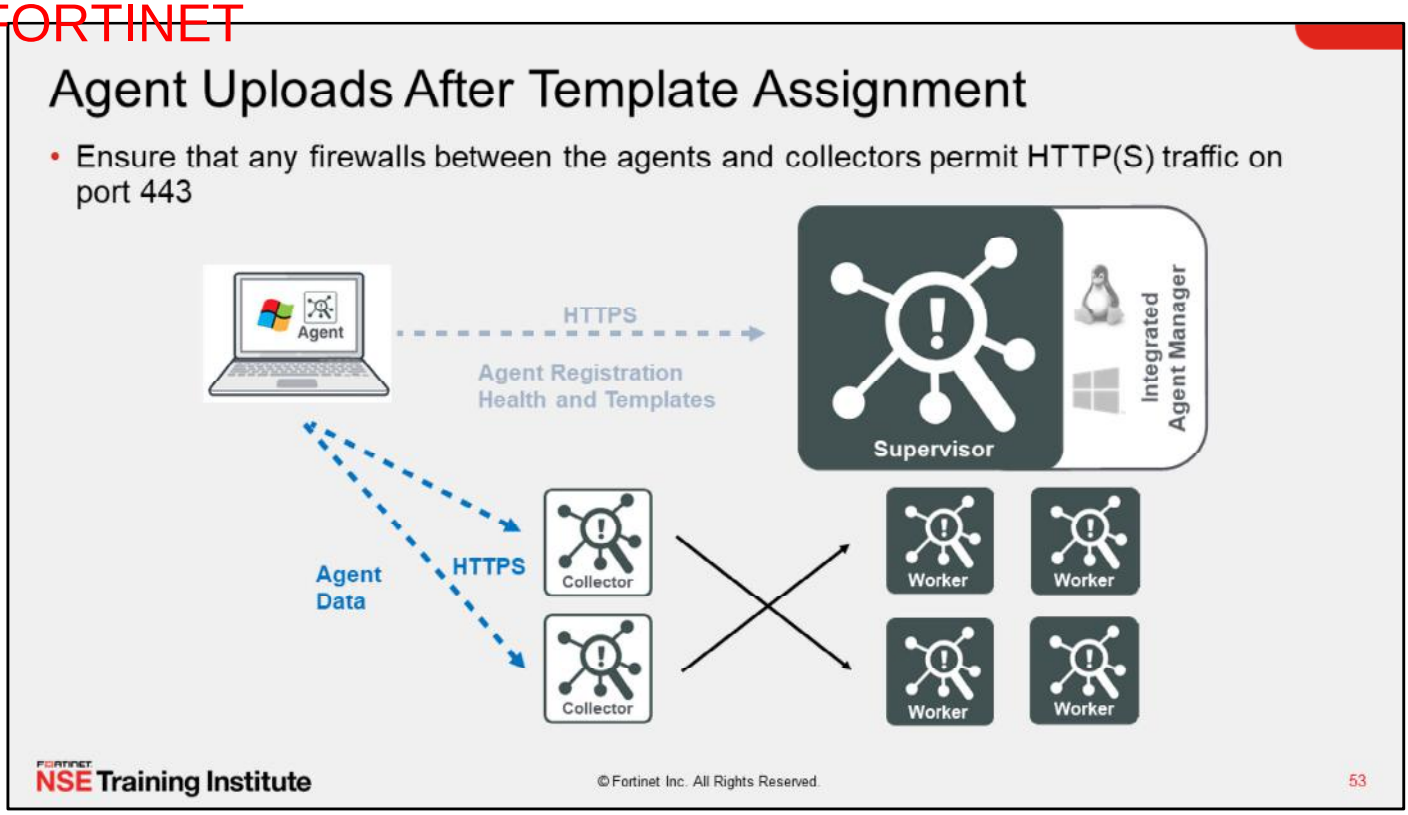
DO NOT REPRINT
© FORTINET
Brave-dumps.com



After defining the templates, you need to associate hosts with templates. One or more templates are then selected along with one or more collectors. To scale to many hosts, use policies. A policy is a mapping from organization and host, to templates and collectors. Policies are evaluated in order (lower order or rank is given higher priority) and the policy that matches first, is selected. Therefore, define the exceptions first followed by broad policies. Hosts are defined in terms of CMDB device groups or business services. Multiple templates can be used in one policy and if there are conflicts, the system detects them.

Vouchers & Dumps are Available | WhatsApp +201224560923

DO NOT REPRINT
© FORTINET
Brave-dumps.com

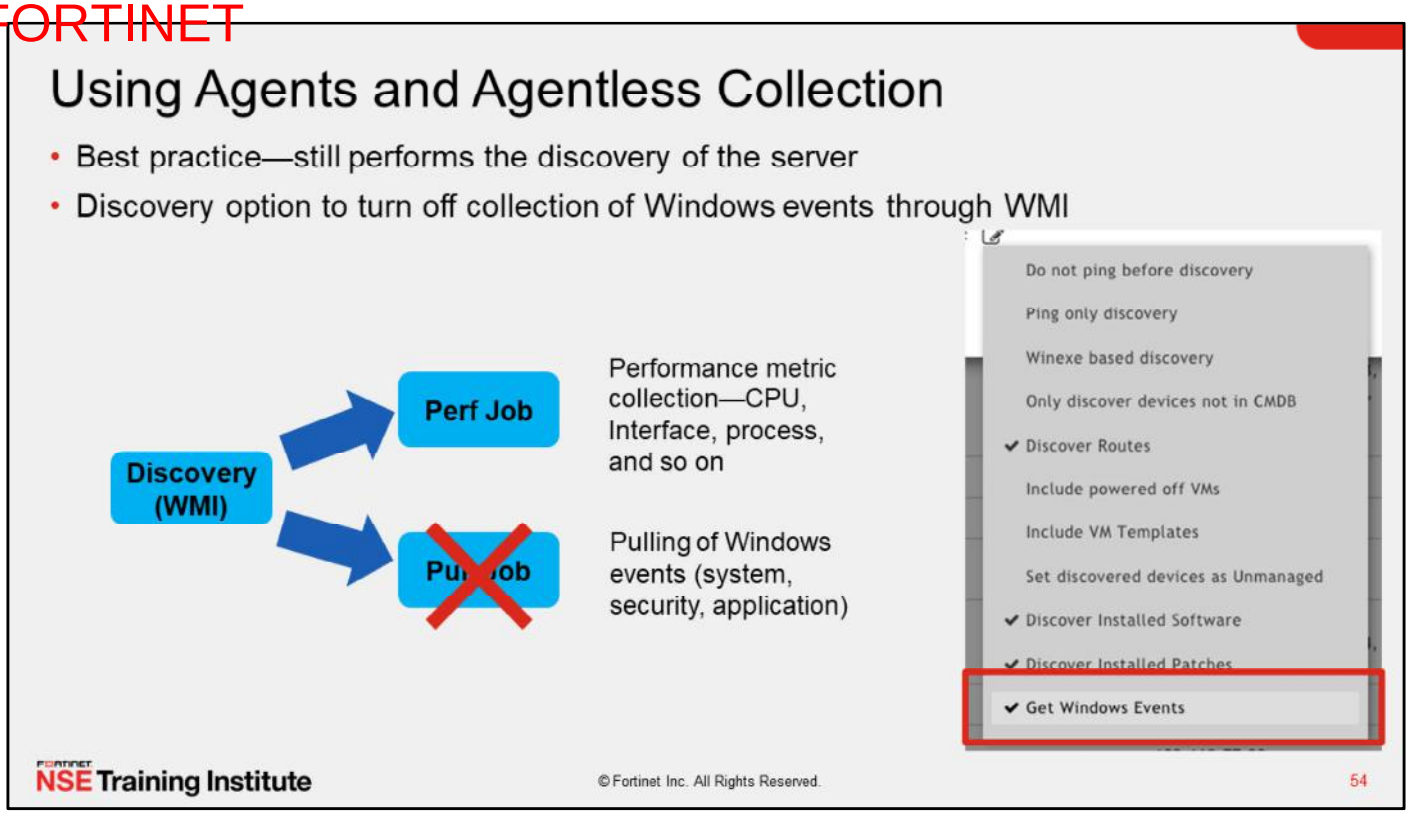


The agents collect the data from Windows computers, as defined in the assigned template, and send the data to the collector using HTTPS.

A collector is always required for agents to upload data. Agents cannot upload data directly to the supervisor node.

Vouchers & Dumps are Available | WhatsApp +201224560923

DO NOT REPRINT
© FORTINET
Brave-dumps.com



The discovery of any Windows server by FortiSIEM adds a **Pull Events** job by default for WMI. This **Pull Events** job is an agentless collection of system, security, and application event logs.
The system adds these jobs automatically. When you use agents to collect the same Windows event logs, you will need to disable this job for every Windows host, or you will receive duplicates.

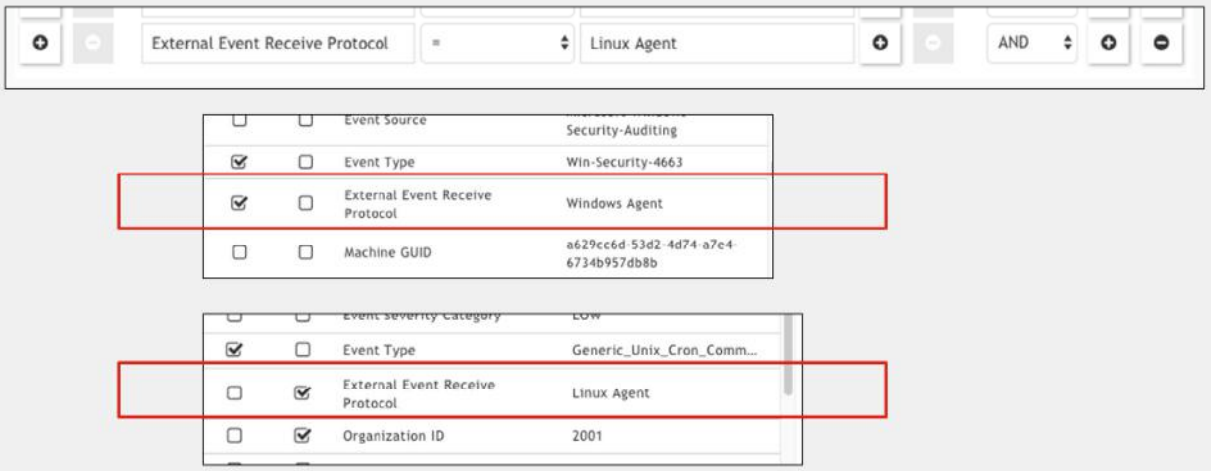
It's a best practice to use agents for Windows event log collection, especially for critical, high-volume machines, such as domain controllers. If performance data is also required (CPU, memory, disk and so on), you can use agentless collection through WMI. To avoid getting duplicate Windows security, application, and system events, you clear **Get Windows Events**, which is associated with event log collection only.

Vouchers & Dumps are Available | WhatsApp +201224560923

DO NOT REPRINT
© FORTINET
Brave-dumps.com

Finding Events From Linux or Windows Agents

- External Event Receive Protocol = **Linux Agent**
- External Event Receive Protocol = **Windows Agent**



NSE Training Institute

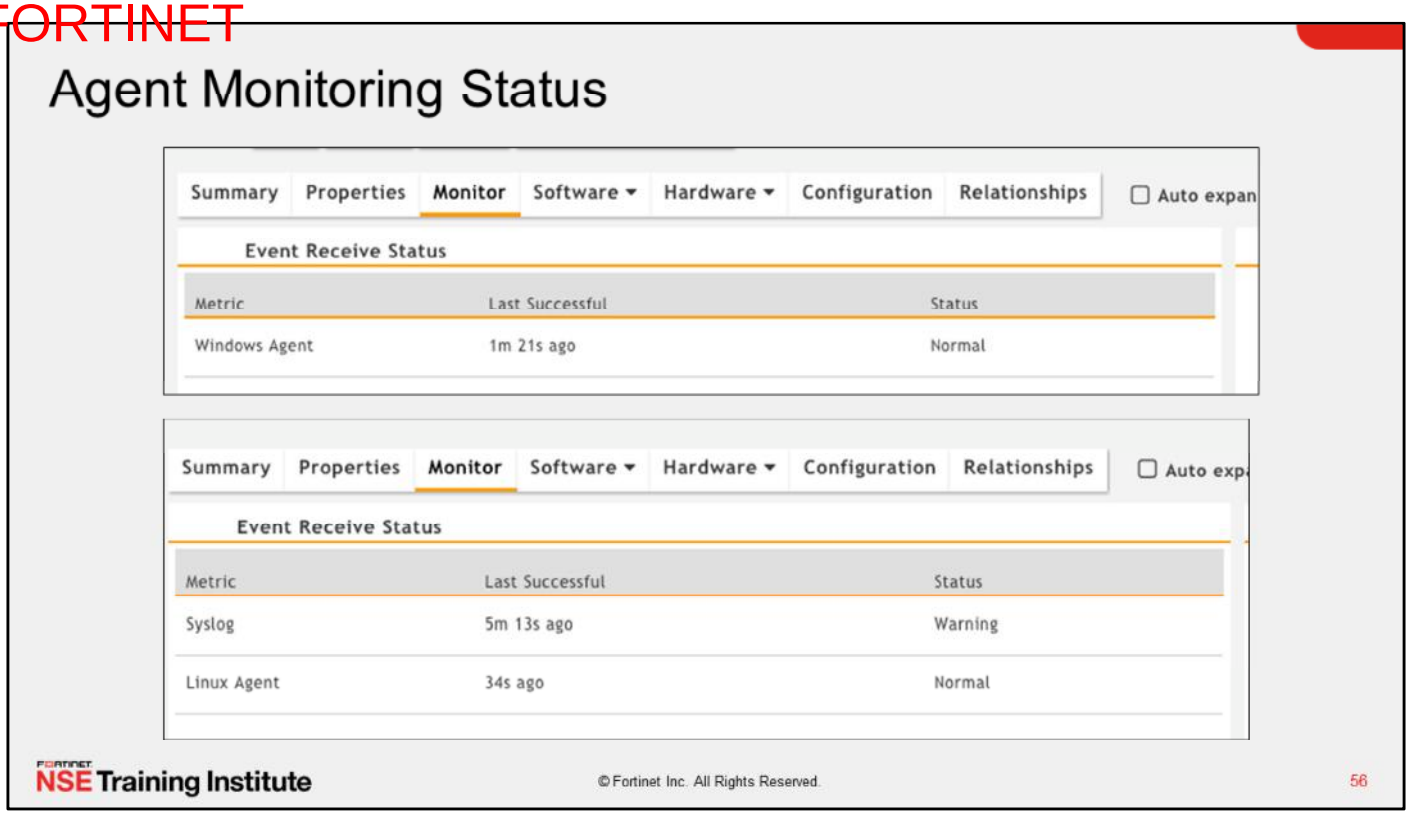
© Fortinet Inc. All Rights Reserved.

55

To search for events that are uploaded by a Linux or Windows agent, you can search by **External Event Receive Protocol** for **Linux Agent** or **Windows Agent**.

Vouchers & Dumps are Available | WhatsApp +201224560923

DO NOT REPRINT
© FORTINET
Brave-dumps.com



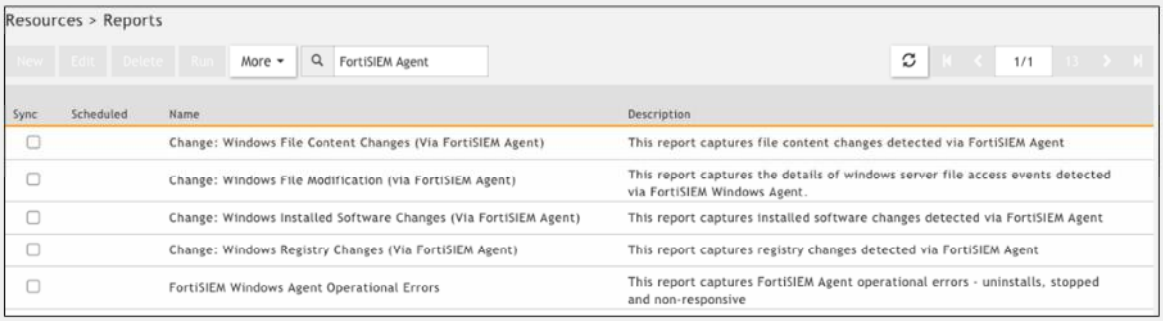
Windows and Linux agents have their own **Event Receive Status** metric, which reports the last time events were received from each agent.

Vouchers & Dumps are Available | WhatsApp +201224560923

DO NOT REPRINT
© FORTINET
Brave-dumps.com

Reports

- All pre-existing Windows auditing reports work with events reported by the Windows agent
- There are some agent-specific reports available that allow reporting on:
  - Installed software changes
  - Registry changes
  - File modifications
  - File content changes



NSE Training Institute

© Fortinet Inc. All Rights Reserved.

57

All pre-existing Windows auditing reports work with events reported by the Windows agent.

There are some agent-specific reports available that allow reporting on some of the specific features of the agent, such as installed software changes, registry changes, file modifications, and file content changes.

Click **RESOURCES** > **Reports**. In the search field, type `agent` to get a list of the agent-specific reports.

Vouchers & Dumps are Available | WhatsApp +201224560923

DO NOT REPRINT
© FORTINET
Brave-dumps.com

Knowledge Check

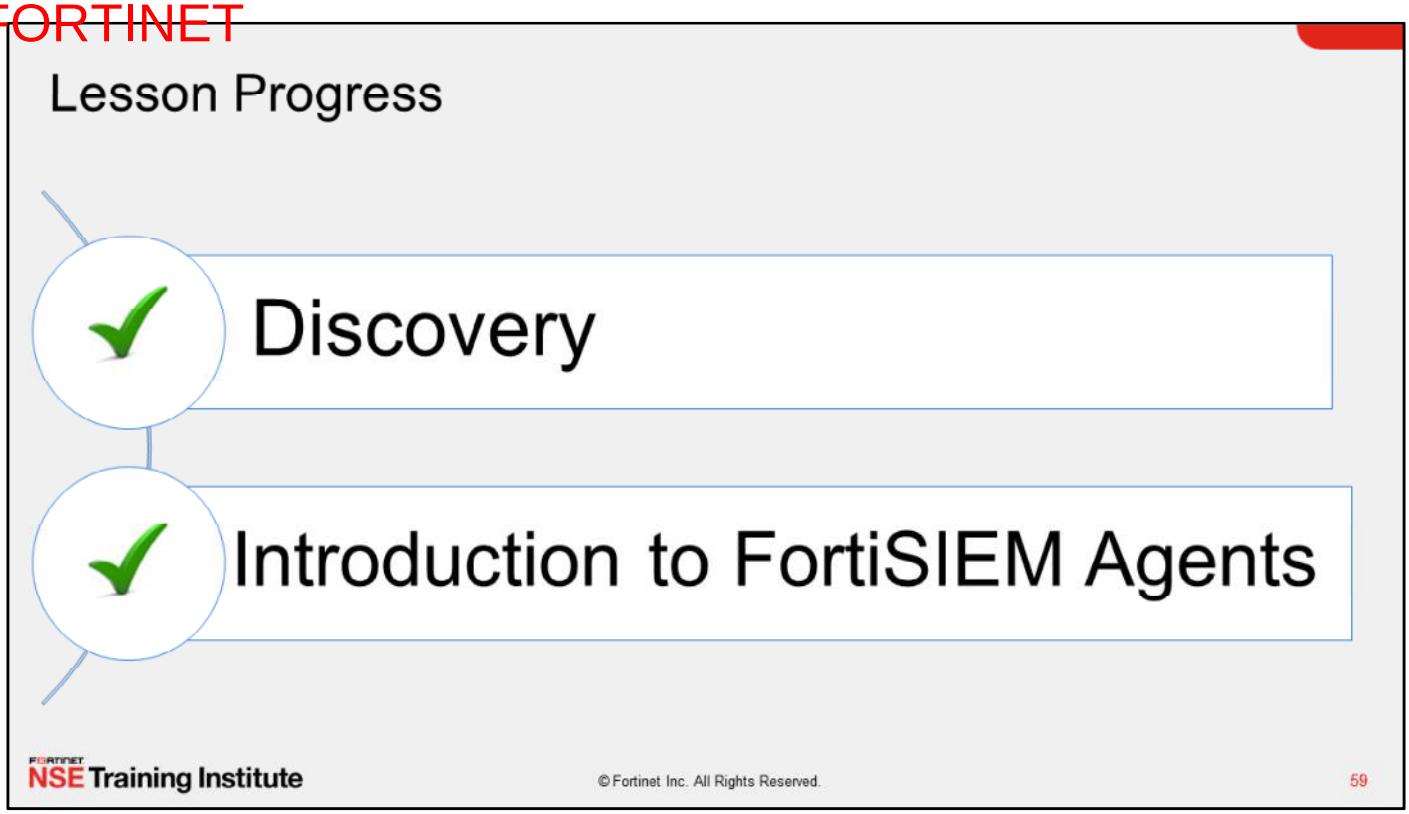
1. Which two Linux OS types support Linux Agent? (Choose two.)
   - ✓ A. Centos 6.x
   - ✓ B. Amazon Linux 2
   - C. Tiny Core Linux
   - D. Kali Linux

2. What protocol is used for communication between an agent and a supervisor?
   - A. FTP
   - B. SSH
   - C. HTTP
   - ✓ D. HTTPS

NSE Training Institute
© Fortinet Inc. All Rights Reserved.
58

Vouchers & Dumps are Available | WhatsApp +201224560923

DO NOT REPRINT
© FORTINET
Brave-dumps.com

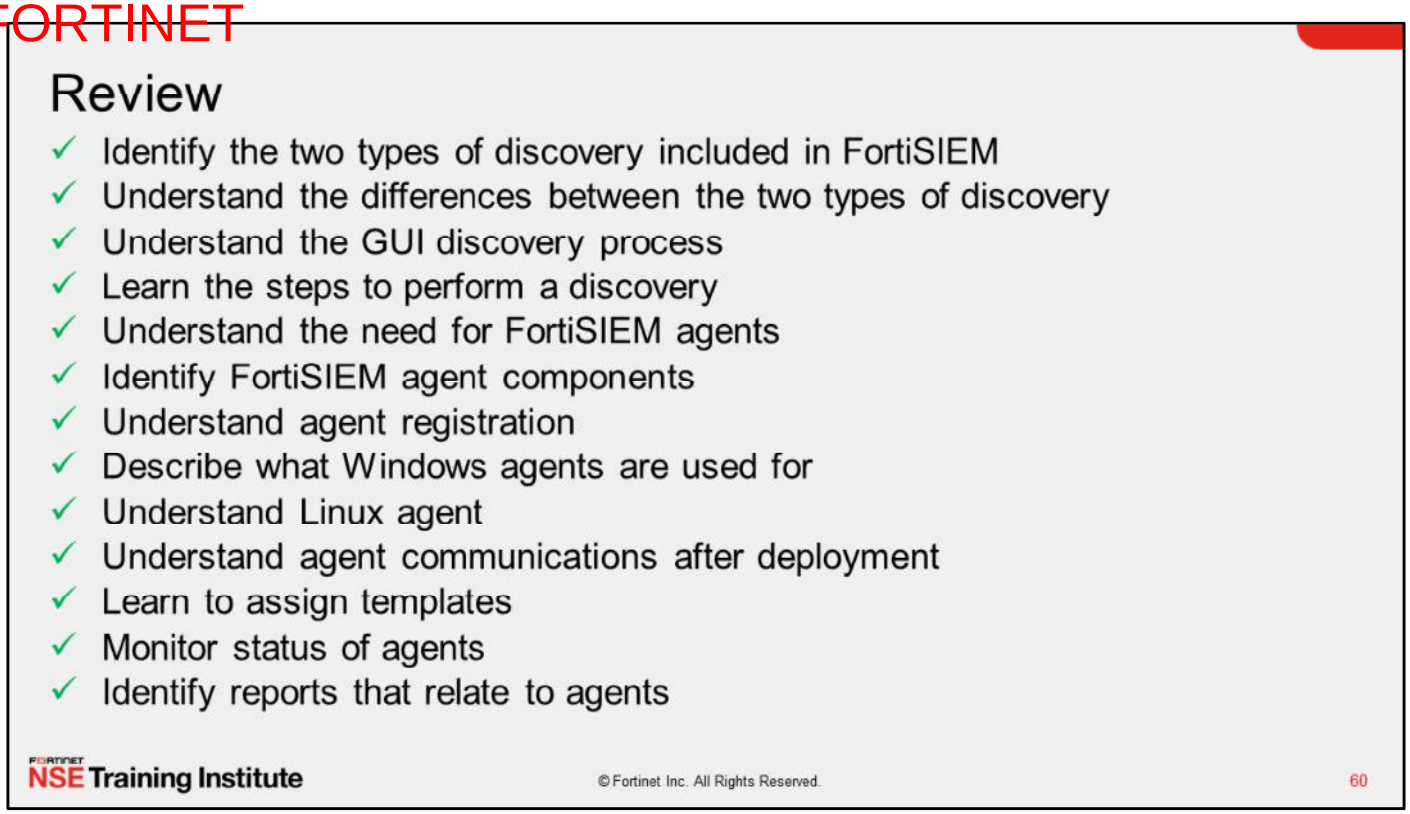


Good job! You have completed this lesson.

Now, you will review the objectives that you covered in this lesson.

Vouchers & Dumps are Available | WhatsApp +201224560923

DO NOT REPRINT
© FORTINET
Brave-dumps.com

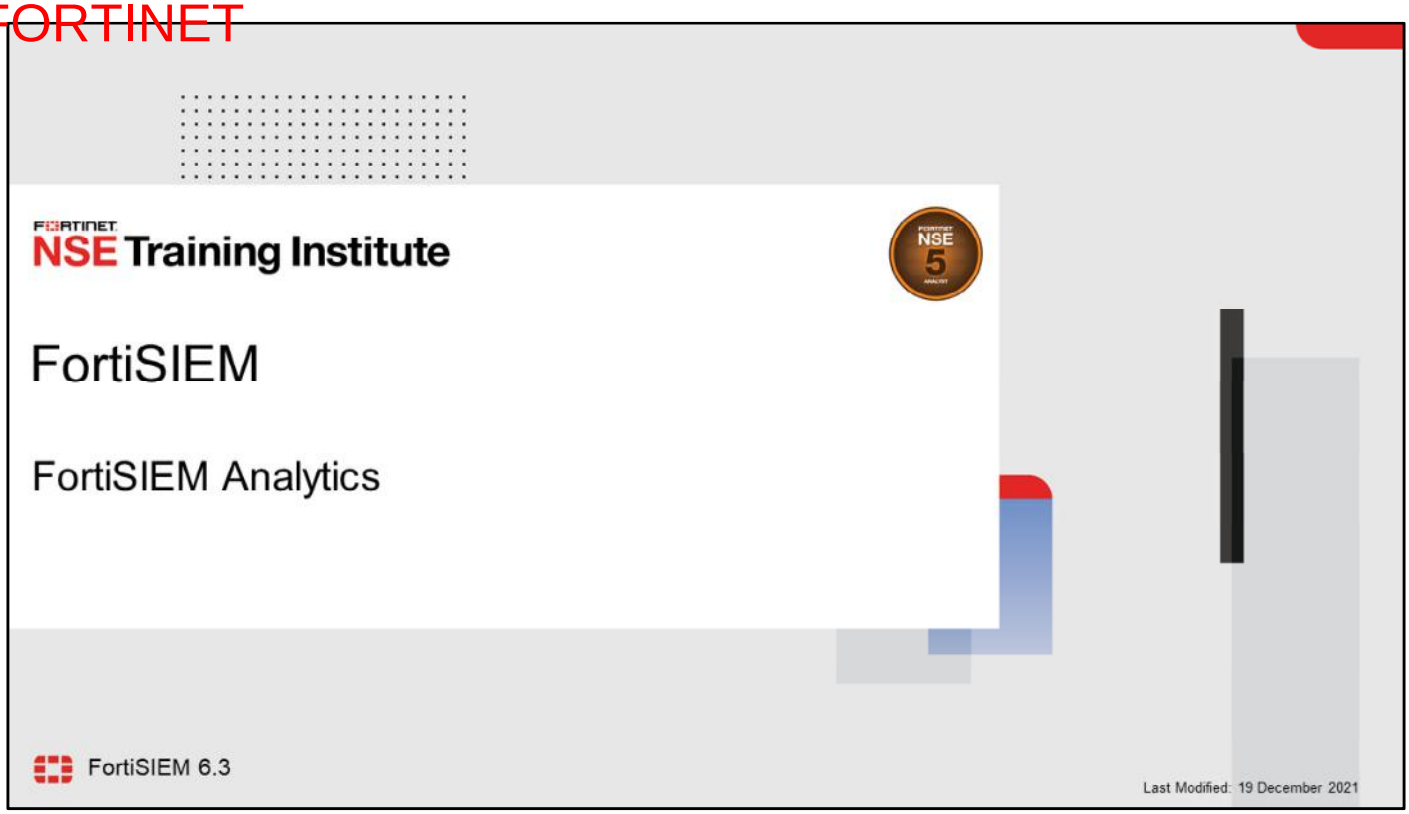


This slide shows the objectives that you covered in this lesson.

By mastering the objectives that you covered in this lesson, you learned how to understand and identify discovery methods, and how to deploy Windows and Linux agents with FortiSIEM.

Vouchers & Dumps are Available | WhatsApp +201224560923

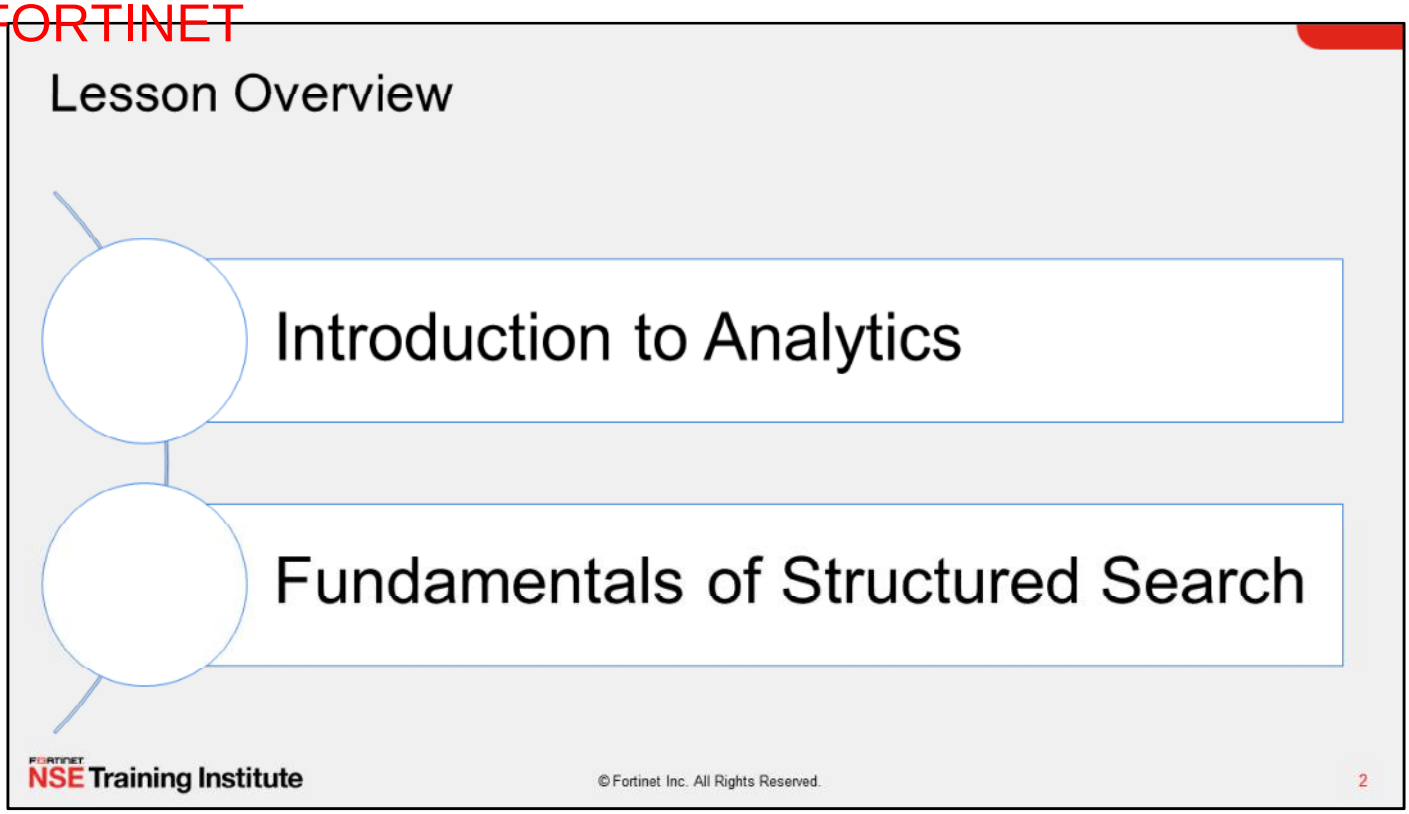
DO NOT REPRINT
© FORTINET
Brave-dumps.com



In this lesson, you will learn about FortiSIEM analytics by looking at structured raw message searches and structured searches using various operators.

Vouchers & Dumps are Available | WhatsApp +201224560923

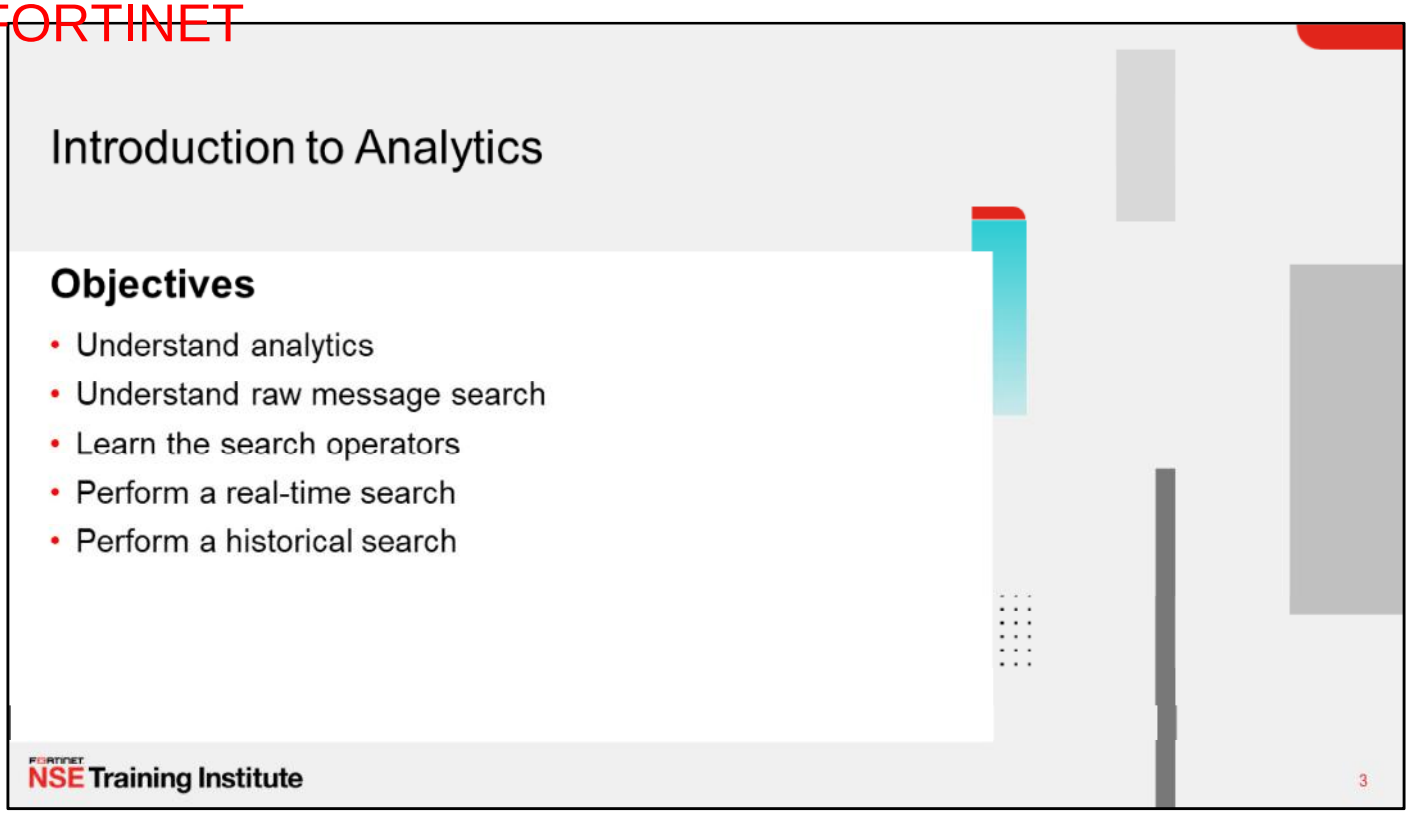
DO NOT REPRINT
© FORTINET
Brave-dumps.com



In this lesson, you will learn about the topics shown on this slide.

Vouchers & Dumps are Available | WhatsApp +201224560923

DO NOT REPRINT
© FORTINET
Brave-dumps.com

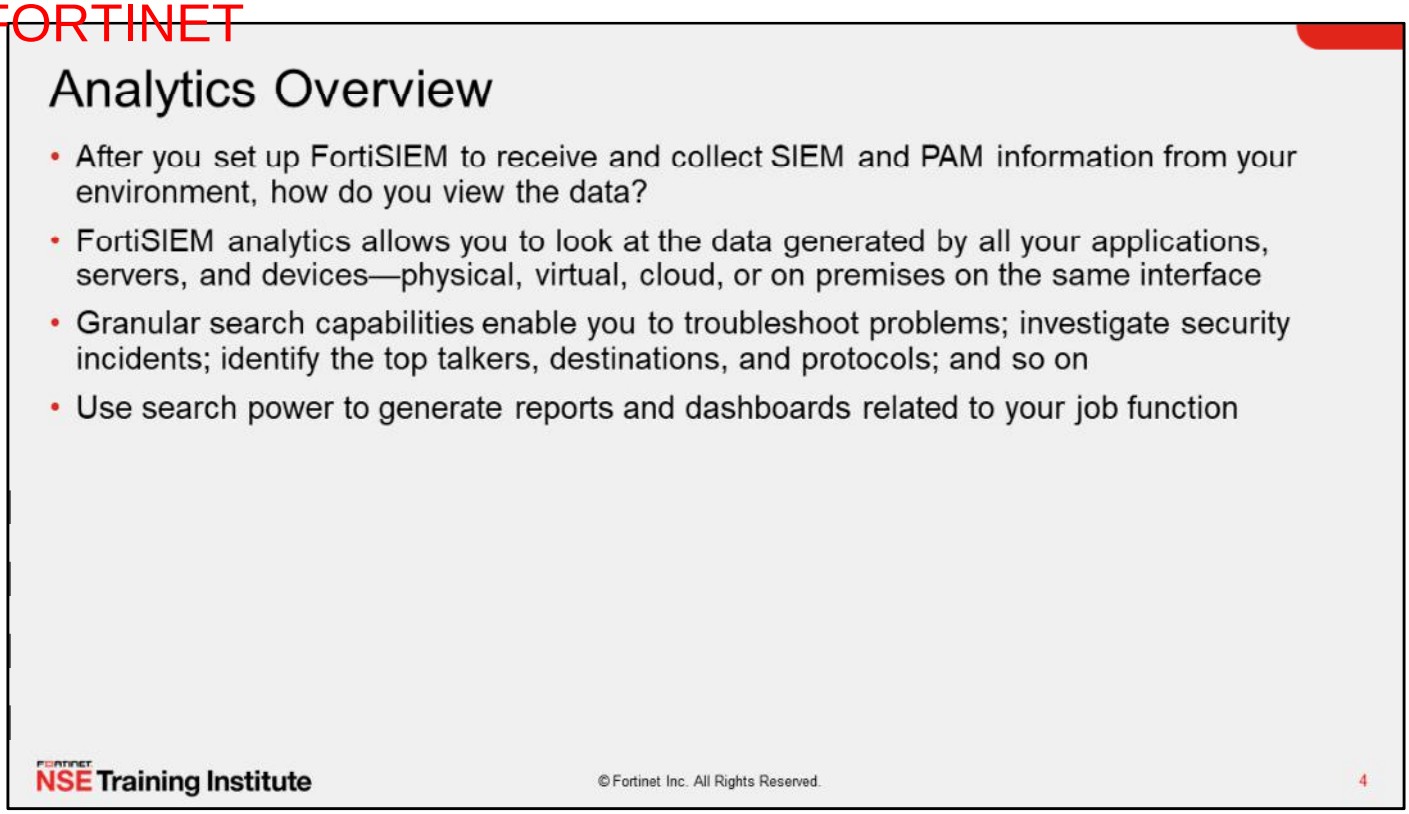


After completing this section, you should be able to achieve the objectives shown on this slide.

By demonstrating competence in understanding analytics, you will be able to use them to search analytics.

Vouchers & Dumps are Available | WhatsApp +201224560923

DO NOT REPRINT
© FORTINET
Brave-dumps.com



After you set up FortiSIEM to receive and collect SIEM and PAM information from your environment, how do you view the data?

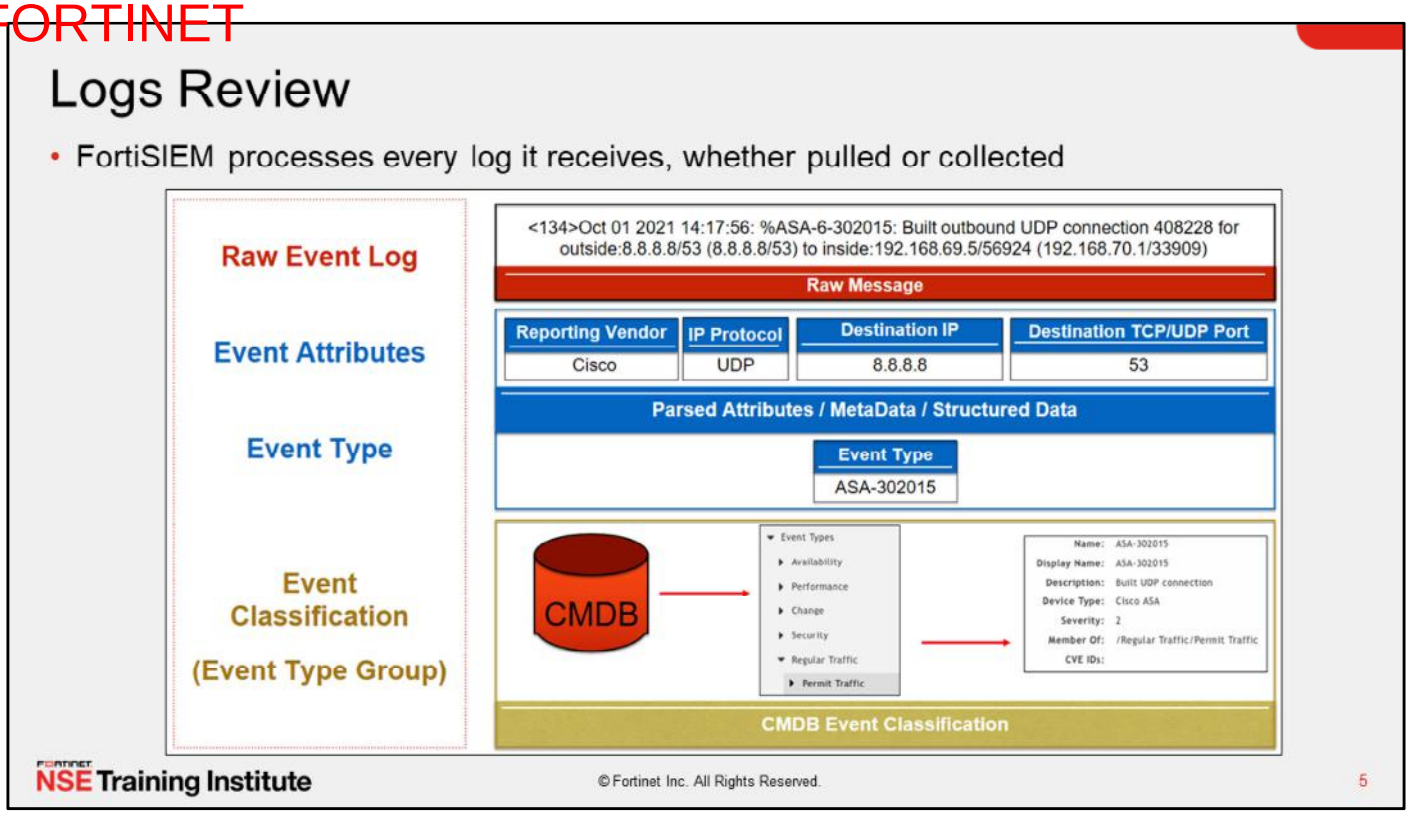
FortiSIEM analytics allows you to look at the data generated by all your applications, servers, and devices, whether they are physical, virtual, in the cloud, or on premises on the same interface.

FortiSIEM analytics also provides granular search capabilities that enable you to troubleshoot problems; investigate security, performance, and network incidents; identify the top talkers, destinations, and protocols; and so on, reported by all of your devices.

You can then use this search power to generate reports and dashboards related to your job function.

Vouchers & Dumps are Available | WhatsApp +201224560923

DO NOT REPRINT
© FORTINET
Brave-dumps.com



FortiSIEM processes every log it receives, whether it is pulled or collected, whether it is security information or performance information.

FortiSIEM log processing includes parsing the data, populating event attributes, and enriching other attributes. Then, FortiSIEM maps the log to an event type, and stores all of that information in the CMDB. FortiSIEM also stores the original message in the raw event log.

FortiSIEM gives most events a classification within the CMDB that describe the kind of message it is. For example, was it a security event? Or was it a permitted or denied traffic event? Or was it a logon failure?

Vouchers & Dumps are Available | WhatsApp +201224560923

DO NOT REPRINT
© FORTINET
Brave-dumps.com

Time-Related Search Types

- FortiSIEM provides two different time-related search types:
  - Real-time: data currently entering the system
  - Historical: data that was received previously
    - Relative
    - Absolute
- How far back in time you can go depends on your storage

ANALYTICS

Time Range
Real-time Relative Last 10 Minutes
Absolute

- **Note**: Real-time searches retrieve data from memory and historical searches retrieve data from disk

NSE Training Institute
© Fortinet Inc. All Rights Reserved.
6

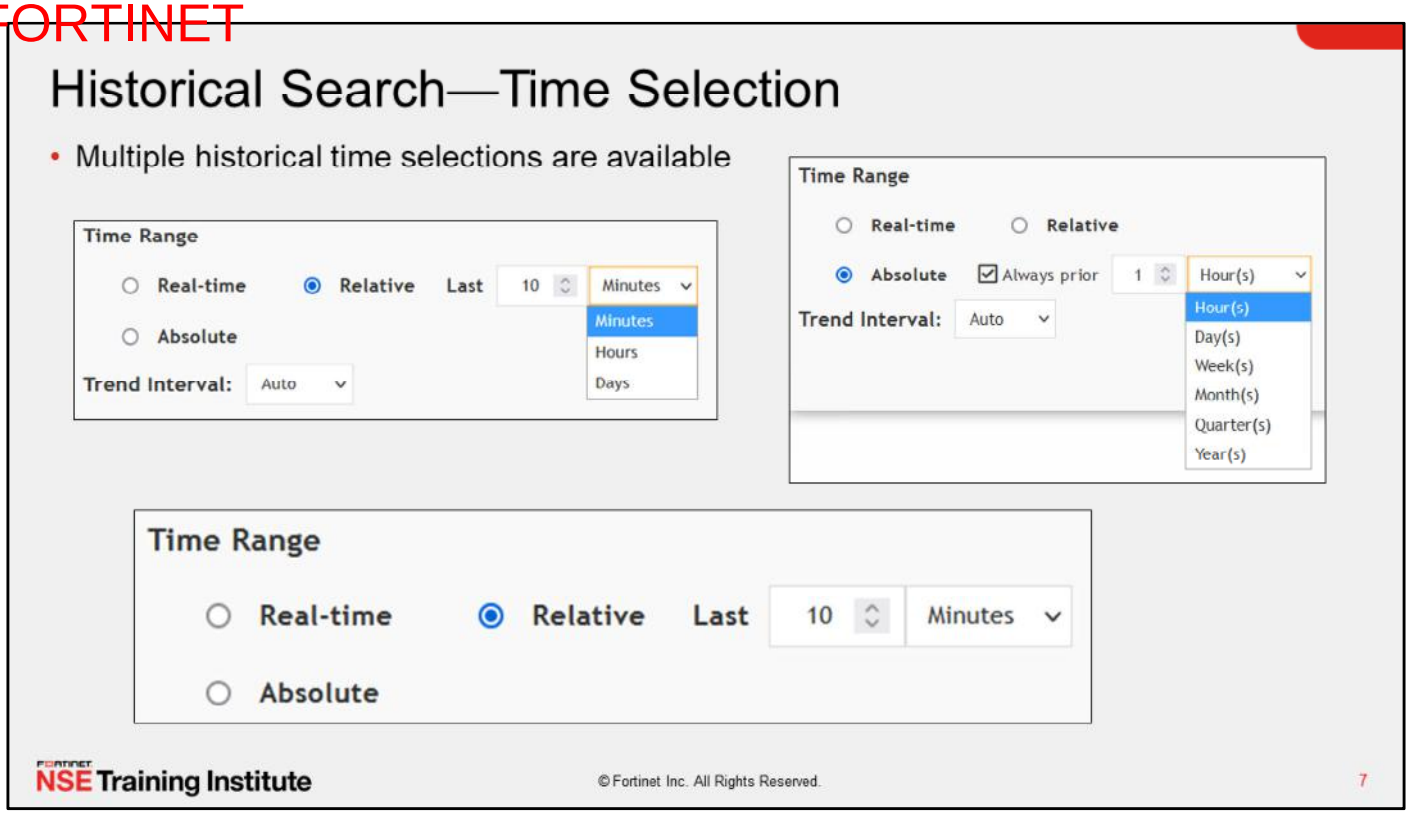
FortiSIEM provides two different time-related search types. The first search type is called a real-time search, which looks at the data as it comes into the system, whether the data is sent by a device or pulled by FortiSIEM.

A historical search looks at data that was previously received and stored. How far back in time you can go depends on how much storage is allocated to the system, and the number of events per second the environment generates. For example, if your network is sending 500 events per second to FortiSIEM, it would require approximately 1 TB of storage space for a years' worth of data.

Note that real-time searches retrieve data from memory before the data is stored, and historical searches retrieve data from disk.

Vouchers & Dumps are Available | WhatsApp +201224560923

DO NOT REPRINT
© FORTINET
Brave-dumps.com



If you choose to perform a historical search, you can choose from multiple time selections.

One option is relative time, which allows you to go back a certain number of minutes, hours, or days, relative to the time you start the search.

There is also the absolute time option, which allows you to look at a specific date and time, such as last Thursday between 1:00 and 1:30 in the afternoon.

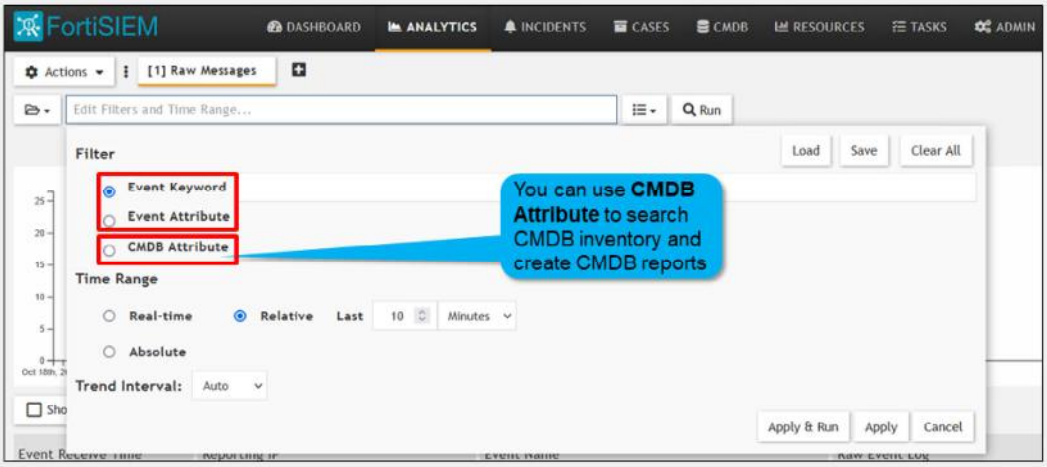
The **Always prior** option allows you to specify the previous day, the previous week, or the previous month, quarter, or year.

Vouchers & Dumps are Available | WhatsApp +201224560923

DO NOT REPRINT
© FORTINET
Brave-dumps.com

Search—Filter Criteria Types

- FortiSIEM provides three options for searching data: **Event Keyword**, **Event Attribute**, and **CMDB Attribute**



- You can use either filter in a real-time or relative (historical) search
- You can use **CMDB Attribute** to search CMDB inventory

NSE Training Institute

© Fortinet Inc. All Rights Reserved.

8

FortiSIEM uses operators to build search conditions to filter data in a structured way.

You can use query filters to perform a real-time search or a historical search.

You can also run the search without any condition for both real-time or historical search.

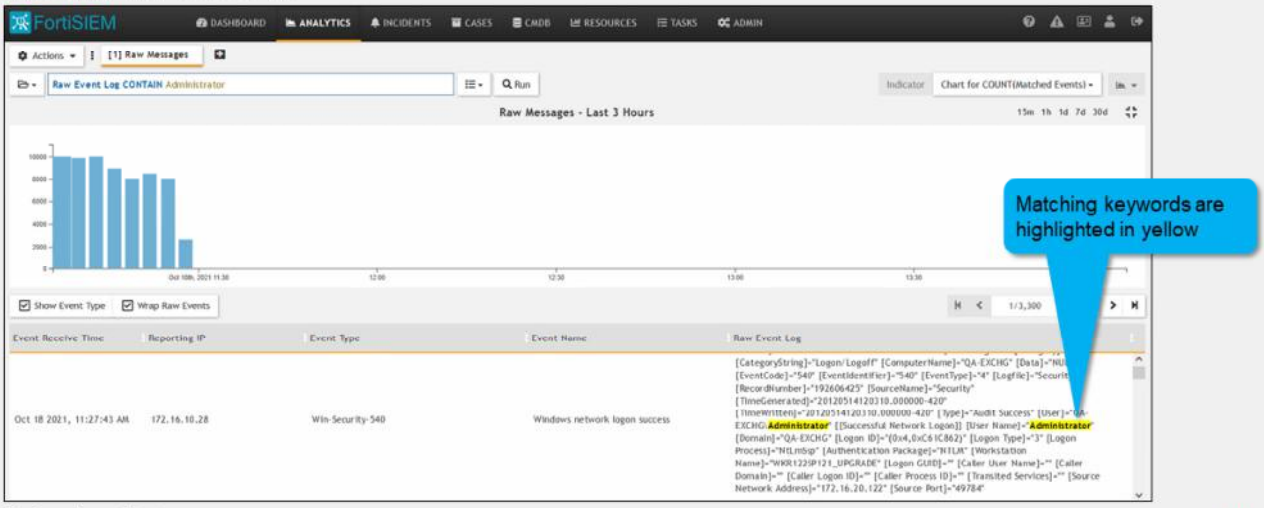
You can use **CMDB Attribute** to search CMDB inventory.

Vouchers & Dumps are Available | WhatsApp +201224560923

DO NOT REPRINT Brave-dumps.com
© FORTINET

Analytics—Keyword Search

- Keyword search queries the stored raw message for keywords
- You can use a keyword search to query any raw message, even if the message is *unknown* to FortiSIEM



NSE Training Institute

© Fortinet Inc. All Rights Reserved.

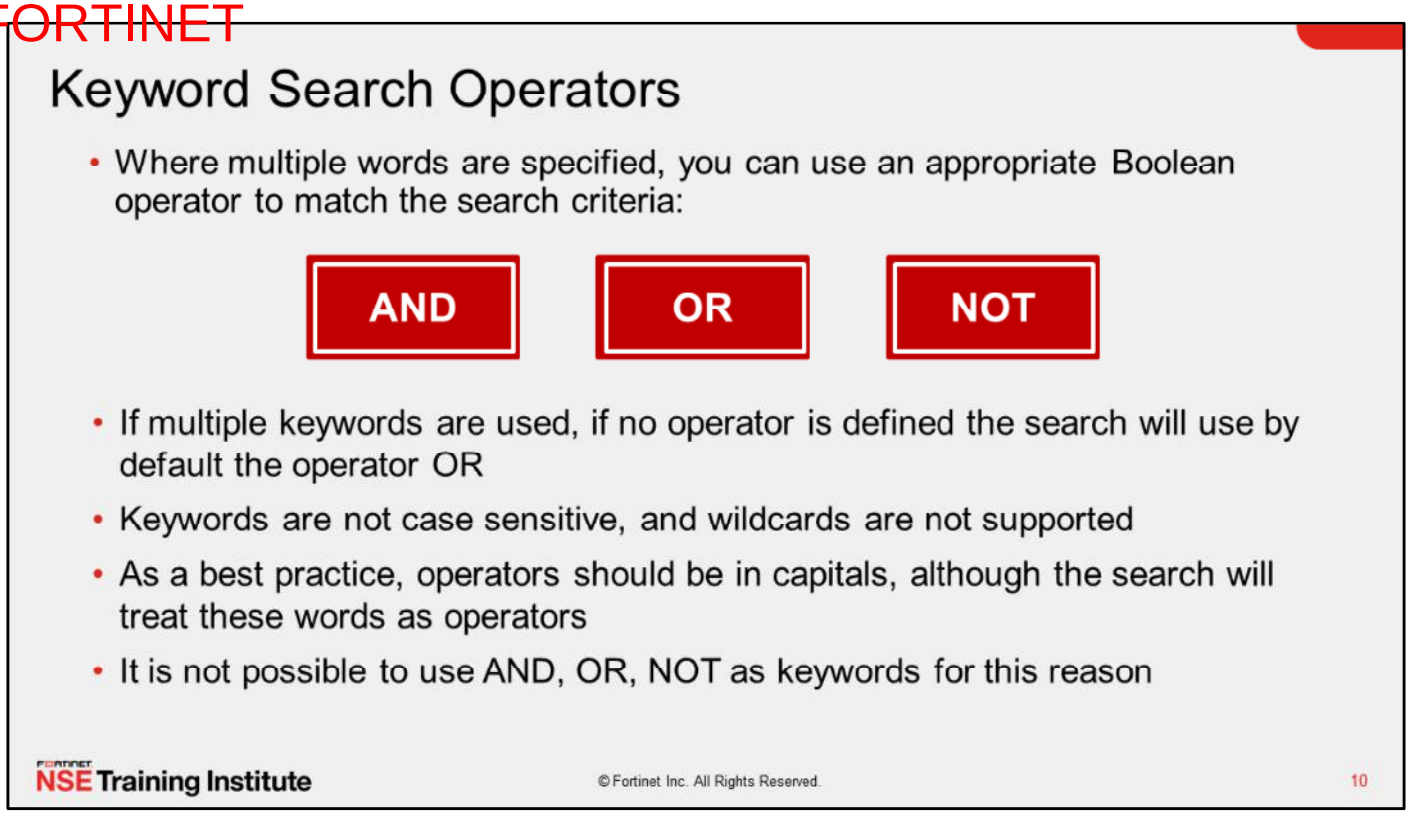
9

One of the benefits of storing the raw message is that you can use a raw message search to examine the raw message for keywords.

You can query any raw message, even messages that are unknown to FortiSIEM. An unknown message is a message that FortiSIEM received for which it didn't have an appropriate parser to correctly parse the message and give it an event type.

Vouchers & Dumps are Available | WhatsApp +201224560923

DO NOT REPRINT
© FORTINET
Brave-dumps.com



Raw messages can be searched by building a search query with the **Raw Event Log** attribute. This allows to search keywords in log messages with structured queries.

The supported Boolean operators are AND, OR, and NOT.

Use the CONTAIN or NOT CONTAIN operator in structured search condition.

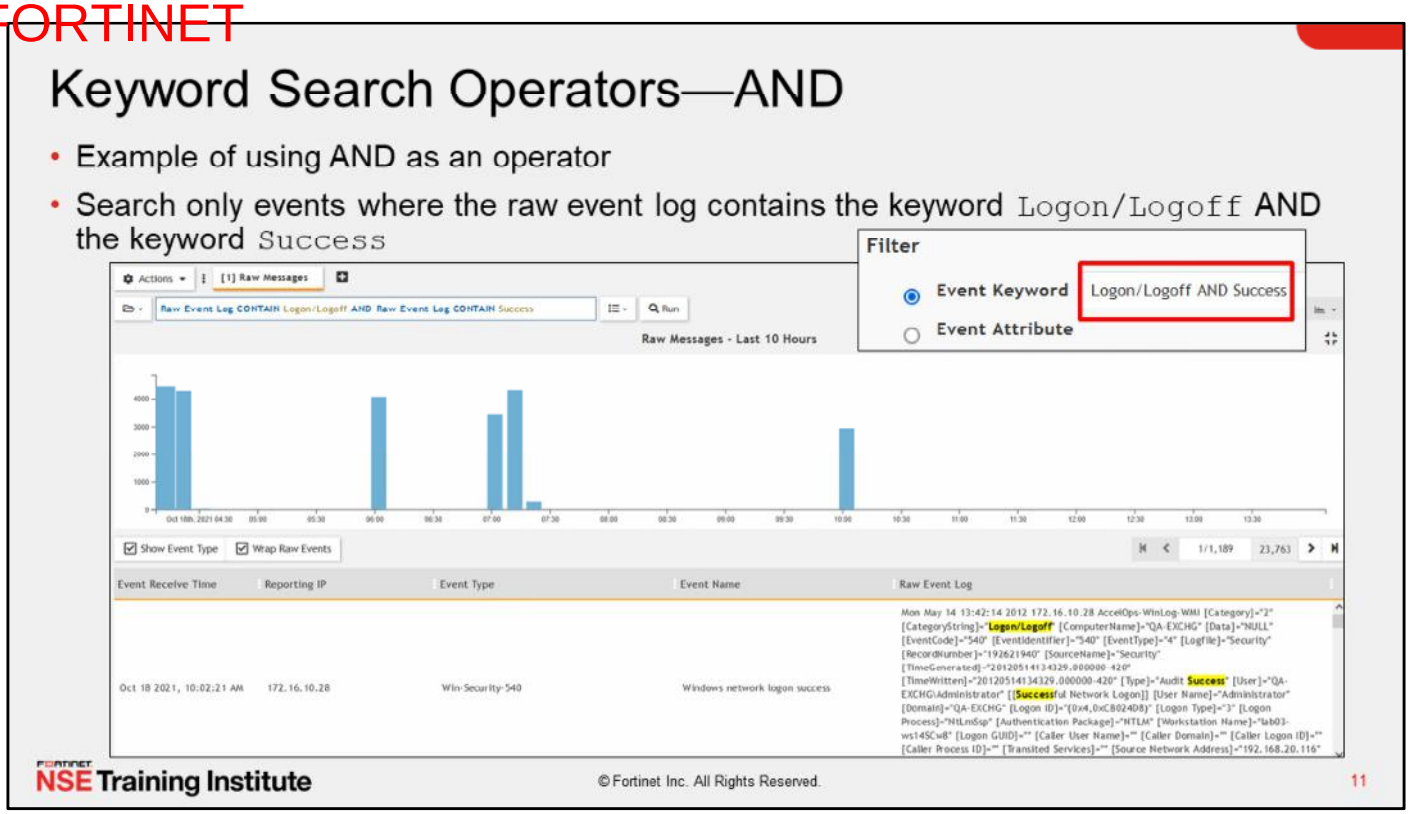
Keywords are not case sensitive, and wildcards are not supported.

So, if you search for the word in lowercase, the search returns results that contain words in uppercase as well.

The CONTAIN operator will be discussed later in the lesson.

Vouchers & Dumps are Available | WhatsApp +201224560923

DO NOT REPRINT
© FORTINET
Brave-dumps.com



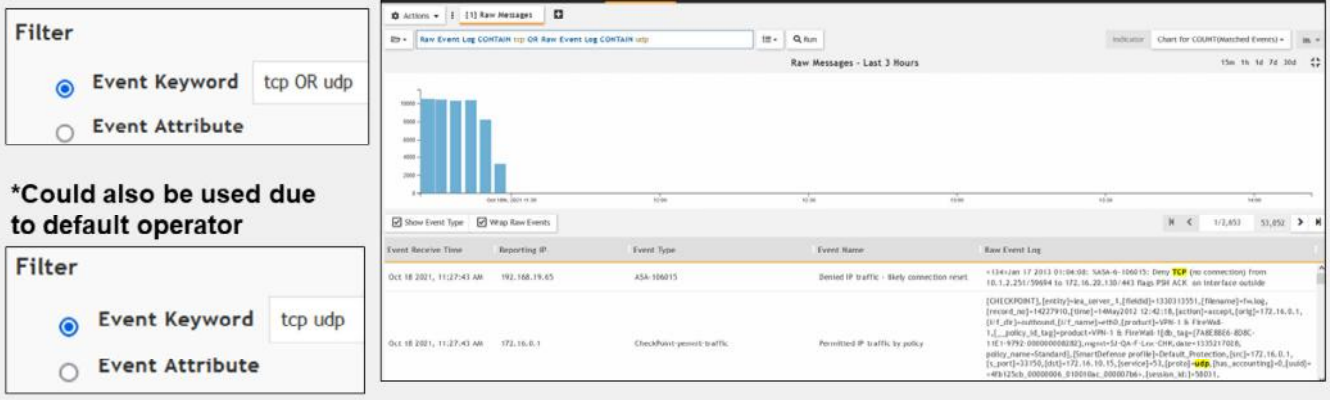
This is an example of an AND operator where you are searching for logon/logoff events that had been successful. So you would use an AND operator to build your search criteria. This searches for events where the raw event log contains the keyword `Logon/Logoff` AND the keyword `Success`.

Vouchers & Dumps are Available | WhatsApp +201224560923

DO NOT REPRINT
© FORTINET
Brave-dumps.com

Keyword Search Operators—OR

- Example of using OR as an operator
- Search only events where the raw event log contains the keyword tcp OR the keyword udp



NSE Training Institute

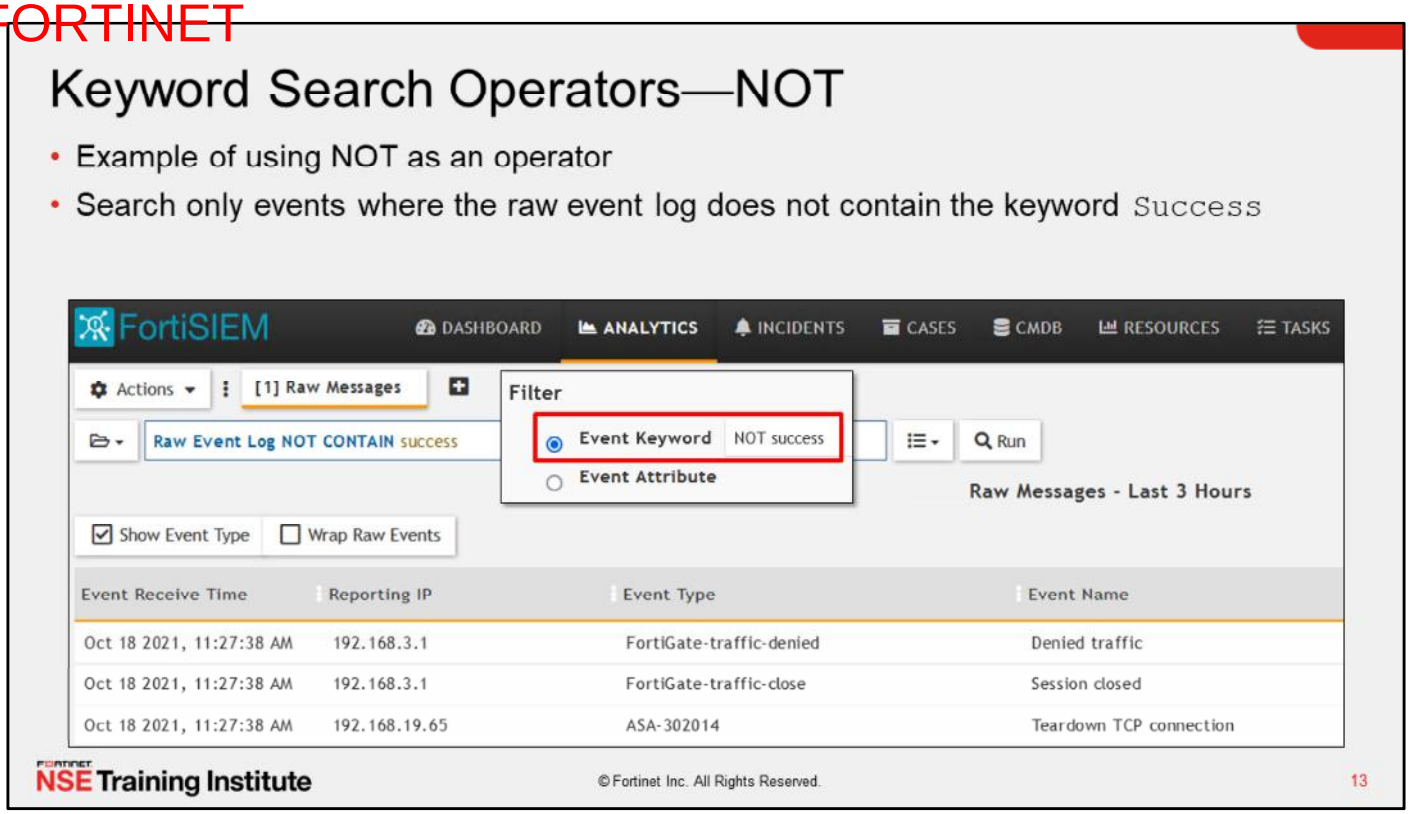
© Fortinet Inc. All Rights Reserved.

12

This slide shows an example of an OR operator where you are searching for TCP or UDP events. So, you would use an OR operator to build your search criteria. This would search for only events where the raw event log contains the keyword `tcp OR udp`.

Vouchers & Dumps are Available | WhatsApp +201224560923

DO NOT REPRINT
© FORTINET
Brave-dumps.com



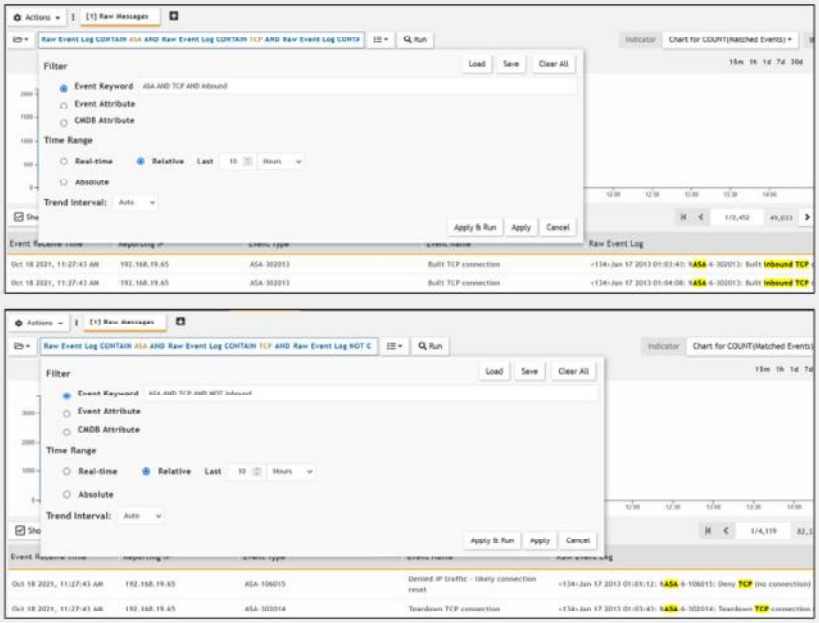
This is an example of a NOT operator where you are searching for Logon/Logoff events that had been unsuccessful. So, you would use the NOT operator to build your search criteria. This would only search for events where the raw event log does not contain the keyword `Success`.

Vouchers & Dumps are Available | WhatsApp +201224560923

DO NOT REPRINT Brave-dumps.com
© FORTINET

Keyword Search Multi-Operators

- Example of using AND and NOT as operators
- First search looks for a specific firewall event that is `TCP` and includes the keyword `inbound`
- The second search looks for the same firewall event that is `TCP` but does not include the keyword `inbound`, and so returns outbound connections only



NSE Training Institute

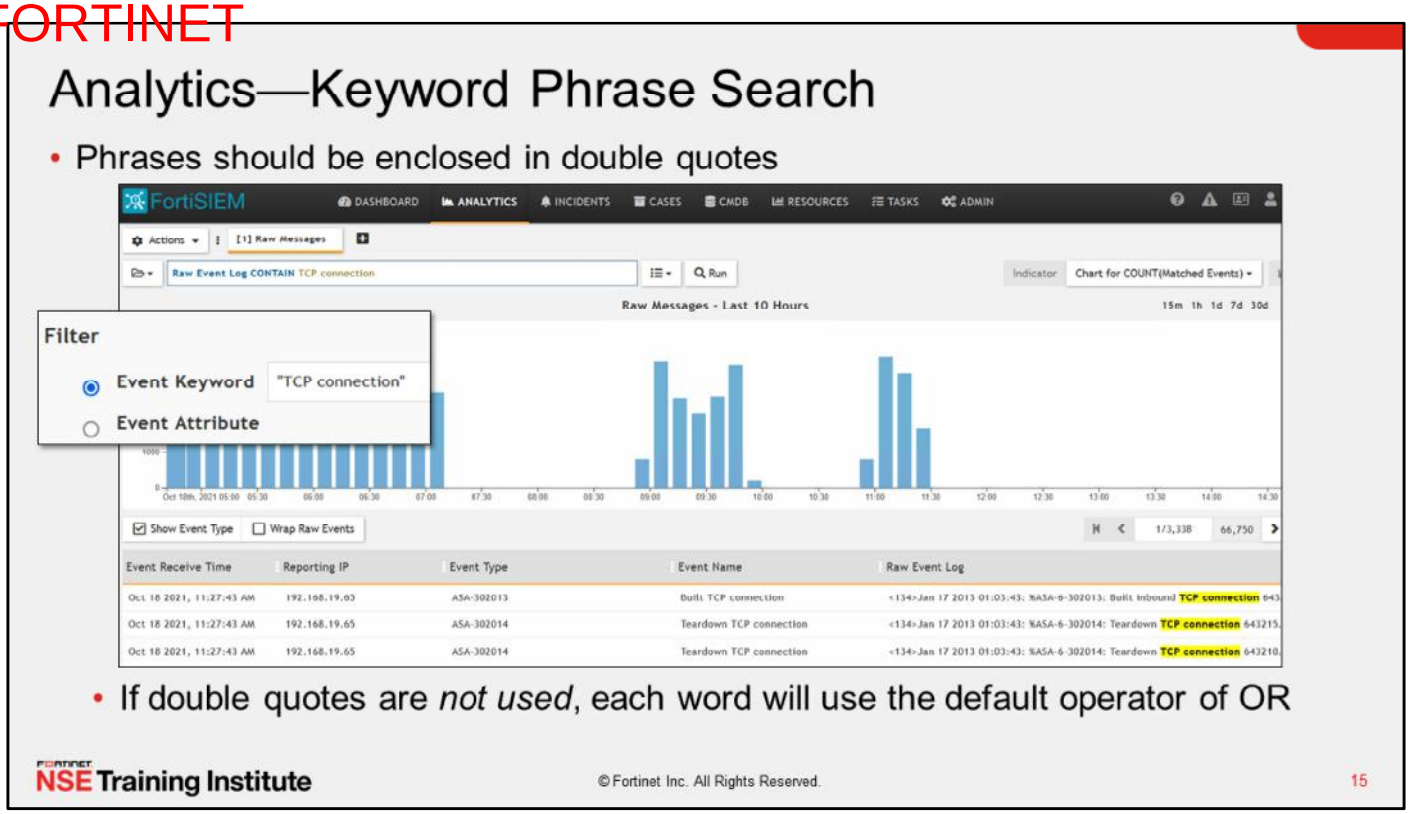
© Fortinet Inc. All Rights Reserved.

14

This is an example of keyword search using AND and NOT as operators. The first search looks for a specific firewall event that is `TCP` and includes the keyword `inbound`. The second search looks for the same firewall event that is `TCP` but does not include the keyword `inbound`, and so returns outbound connections only.

Vouchers & Dumps are Available | WhatsApp +201224560923

DO NOT REPRINT Brave-dumps.com
© FORTINET



One of the benefits of storing the raw message is that you can use a raw message search to examine the raw message for keywords.

You can query any raw message, even messages that are unknown to FortiSIEM. An unknown message is a message that FortiSIEM receives, but does not have the appropriate parser to correctly parse and assign an event type to.

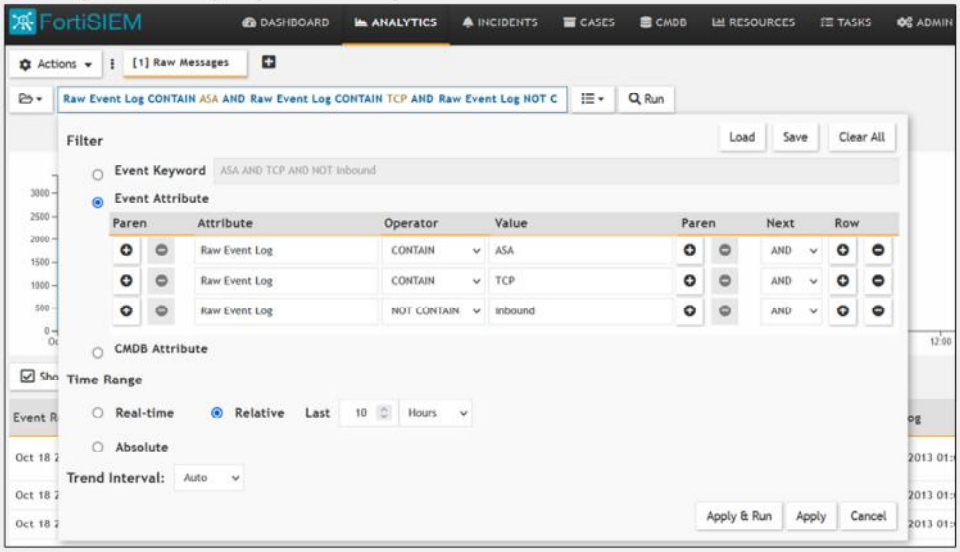
In this example, you are performing a keyword search `"TCP connection"`. If you do not use double quotes, then each word will use the default operator of OR.

Vouchers & Dumps are Available | WhatsApp +201224560923

DO NOT REPRINT
© FORTINET
Brave-dumps.com

Changing From a Keyword Search to an Attribute Search

- After running and obtaining results from any keyword search, selecting the attribute search option displays the equivalent search criteria for further refinement



NSE Training Institute

© Fortinet Inc. All Rights Reserved.

16

After running and obtaining results from any keyword search, selecting the attribute search option displays the equivalent search criteria for further refinement.

One of the benefits of storing the raw message is that you can use a raw message search to examine the raw message for keywords.

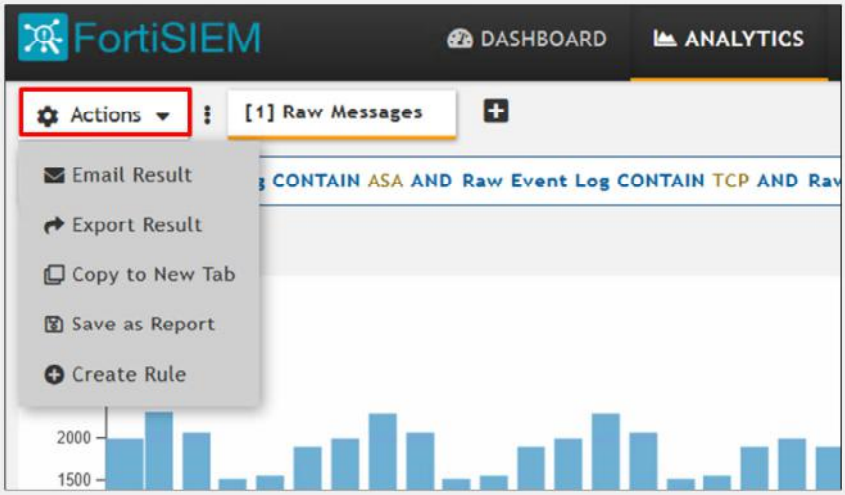
You can query any raw message, even messages that are unknown to FortiSIEM. An unknown message is a message that FortiSIEM received for which it didn't have an appropriate parser to correctly parse the message and give it an event type.

Vouchers & Dumps are Available | WhatsApp +201224560923

DO NOT REPRINT
© FORTINET
Brave-dumps.com

Perform Actions on Search Results

- FortiSIEM provides the following options to perform an action on analytics results:
  - **Email Result**
  - **Export Result**
  - **Copy To New Tab**
  - **Save as Report**
  - **Create Rule**



NSE Training Institute

© Fortinet Inc. All Rights Reserved.

17

To perform actions on results, click the **Actions** drop-down and choose one of the following options:

- **Email Result**
- **Export Result**
- **Copy To New Tab**
- **Save Report**
- **Create Rule**

Vouchers & Dumps are Available | WhatsApp +201224560923

DO NOT REPRINT
© FORTINET
Brave-dumps.com

Knowledge Check

1. If FortiSIEM administrator searched for the word `ADMIN` using the **Raw Event Log** attribute, would administrator also receive events for the word `admin`?
   - ✓A. Yes
   - B. No

2. If an administrator sends custom billing application event logs for an unsupported device to FortiSIEM as syslog, could the administrator search for data for that device?
   - ✓A. Yes
   - B. No

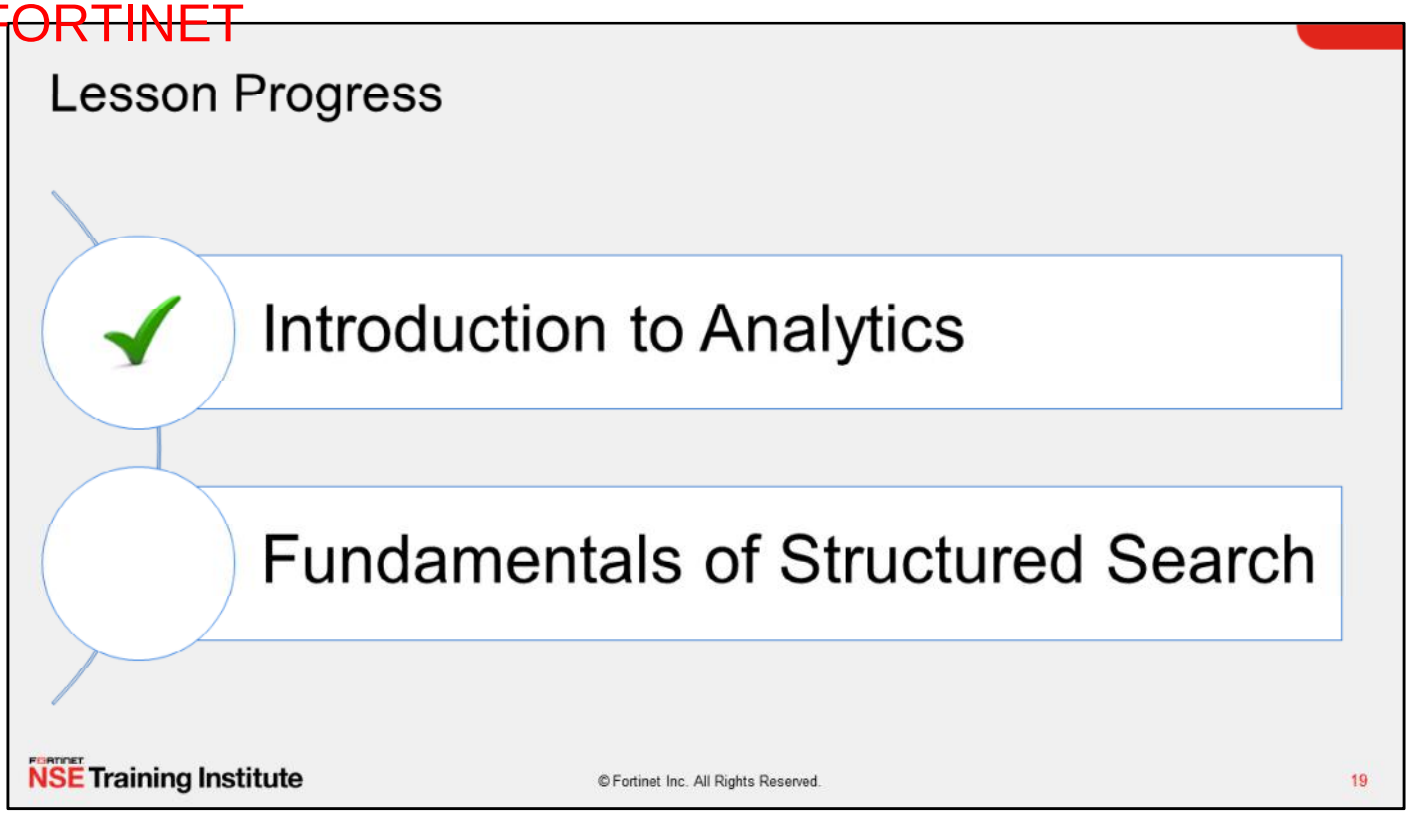
NSE Training Institute

© Fortinet Inc. All Rights Reserved.

18

Vouchers & Dumps are Available | WhatsApp +201224560923

DO NOT REPRINT
© FORTINET
Brave-dumps.com

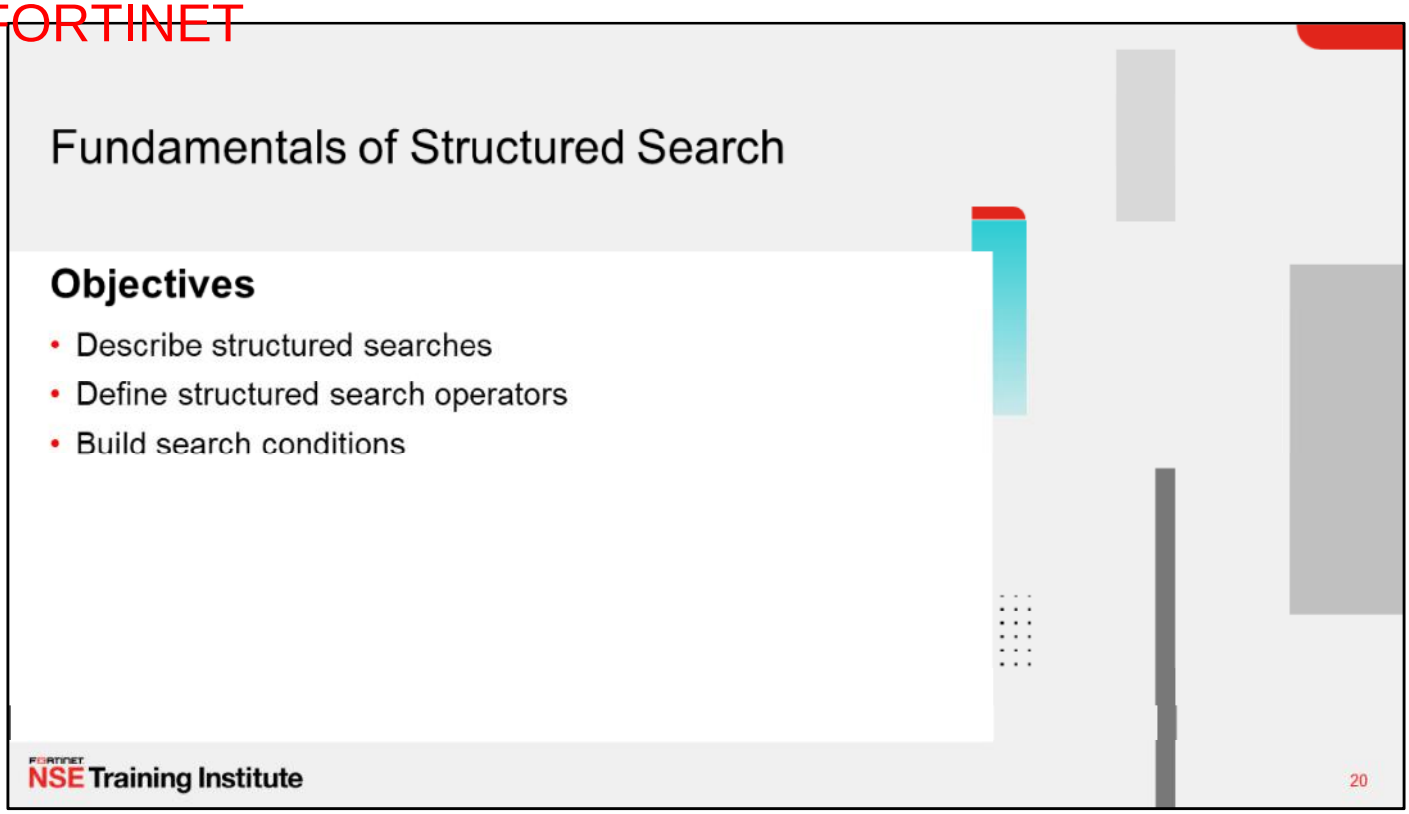


Good job! You now understand analytics.

Now, you'll learn about the fundamentals of structured searches.

Vouchers & Dumps are Available | WhatsApp +201224560923

DO NOT REPRINT
© FORTINET
Brave-dumps.com

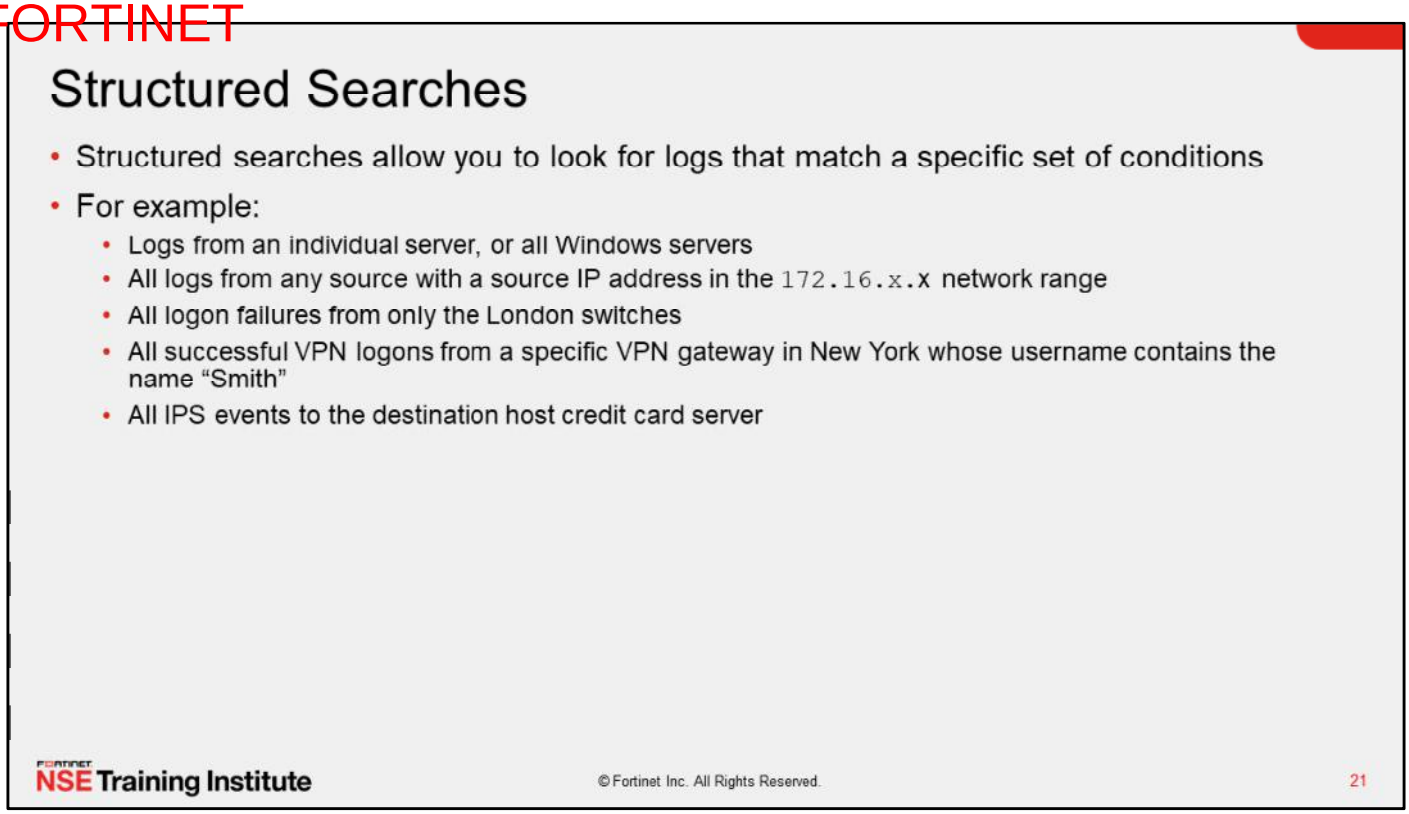


After completing this section, you should be able to achieve the objectives shown on this slide.

By demonstrating a competent understanding of structured search conditions and operators, you will be able to use structured search operations to build search conditions.

Vouchers & Dumps are Available | WhatsApp +201224560923

DO NOT REPRINT
© FORTINET
Brave-dumps.com

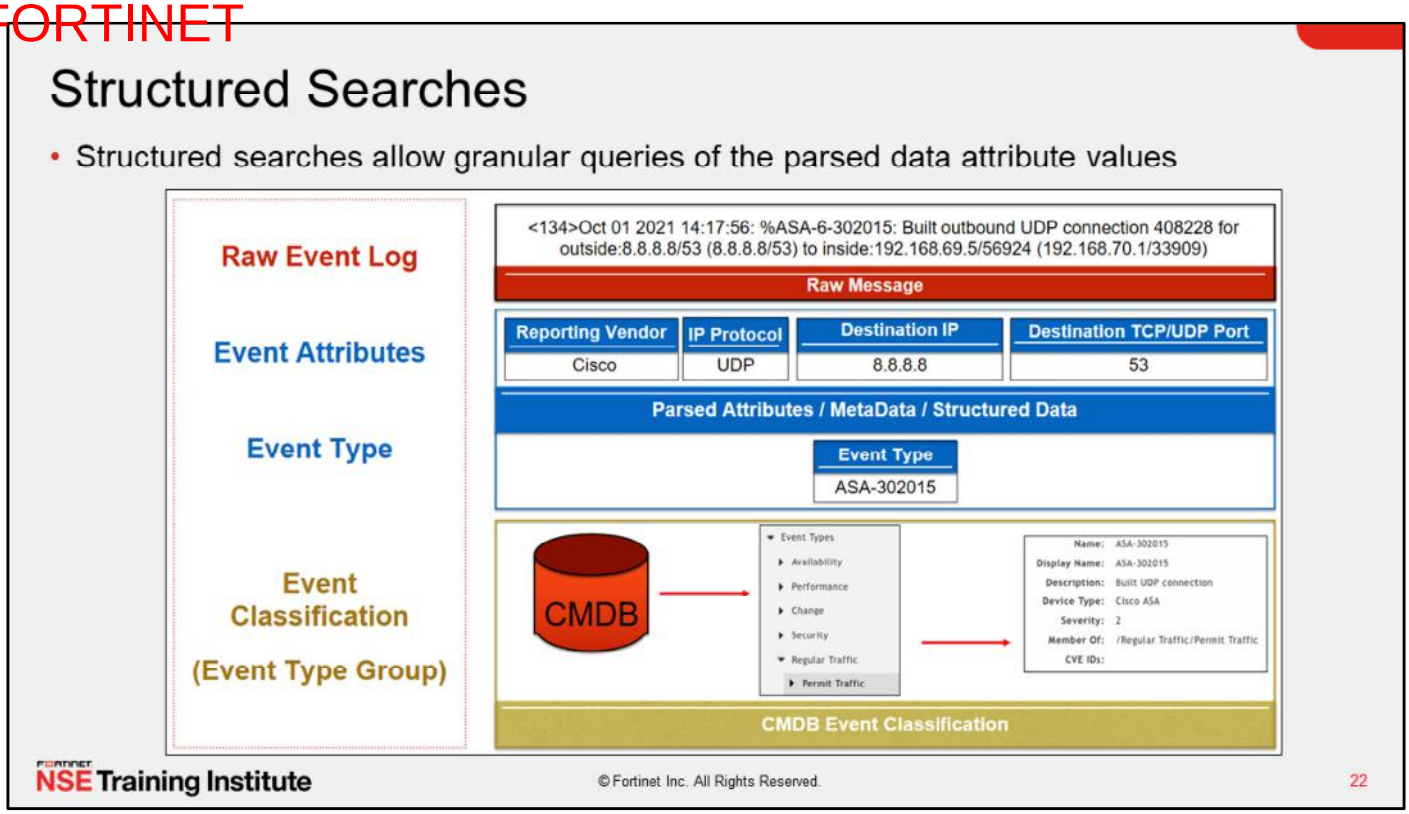


Structured searches allow you to look for logs that match a specific set of conditions. For example:

- Logs from an individual server, or all Windows servers
- All logs from any source that has a source IP address in a specific network range
- Logon failures from only the London switches
- All successful VPN logons from a specific VPN gateway in New York whose username contains the name "Smith"
- All IPS events to a specific destination host credit card server in your network

Vouchers & Dumps are Available | WhatsApp +201224560923

DO NOT REPRINT
© FORTINET
Brave-dumps.com



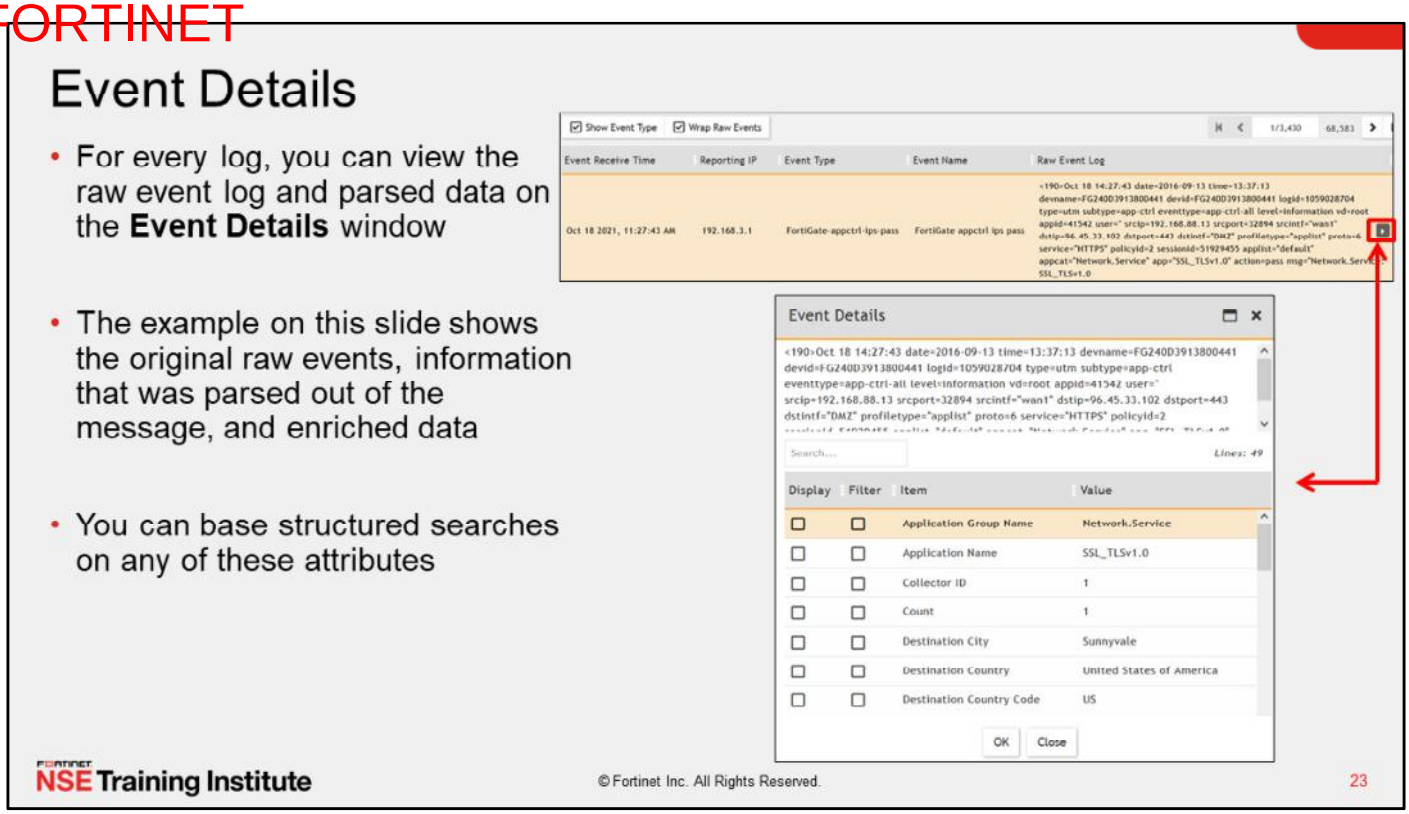
FortiSIEM processes every log it receives, whether pulled or collected, whether it is security information or performance information.

FortiSIEM log processing includes parsing the data, populating event attributes, and enriching other attributes. Then, FortiSIEM maps the log to an event type, and stores all of that information in the CMDB. FortiSIEM also stores the original message in the raw event log.

FortiSIEM gives most events a classification within the CMDB that describes the kind of message it is. For example, was it a security event? Or was it a permitted or denied traffic event? Or was it a logon failure?

Vouchers & Dumps are Available | WhatsApp +201224560923

DO NOT REPRINT Brave-dumps.com
© FORTINET



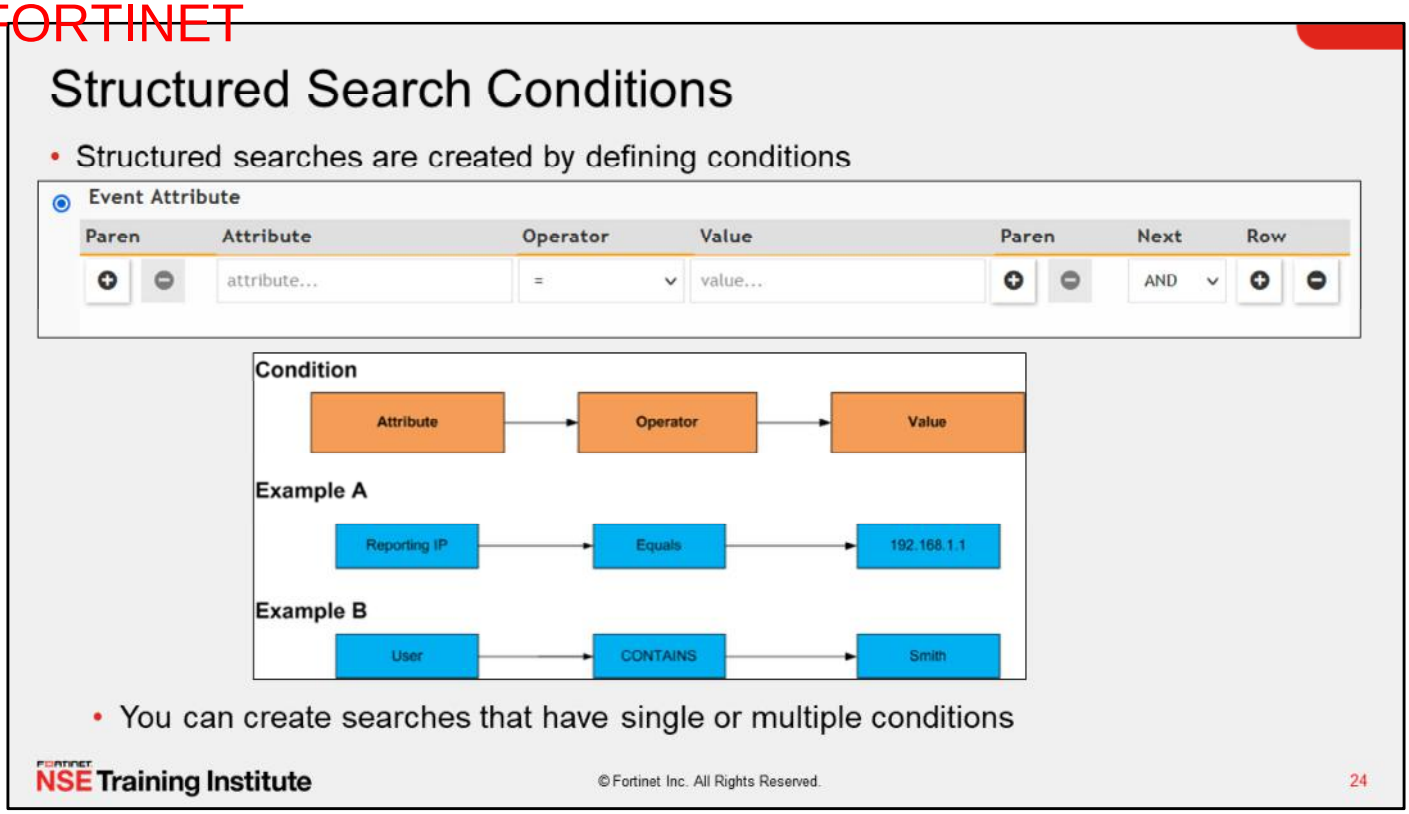
To view **Event Details**, select any raw log message under **Raw Event Log** column. When you select the raw event log, a right arrow icon appears in the **Raw Event Log** column. If you click the arrow icon, you will see the **Event Details** associated with that event.

For every log, you can view the raw event log and parsed data in the event details.

The example on this slide shows the original raw message, information that was parsed out of the message, as well as enriched data. You can base structured searches on these attributes.

Vouchers & Dumps are Available | WhatsApp +201224560923

DO NOT REPRINT
© FORTINET
Brave-dumps.com



You can create structured searches by defining conditions that have the following structure: an attribute, an operator, and a value.

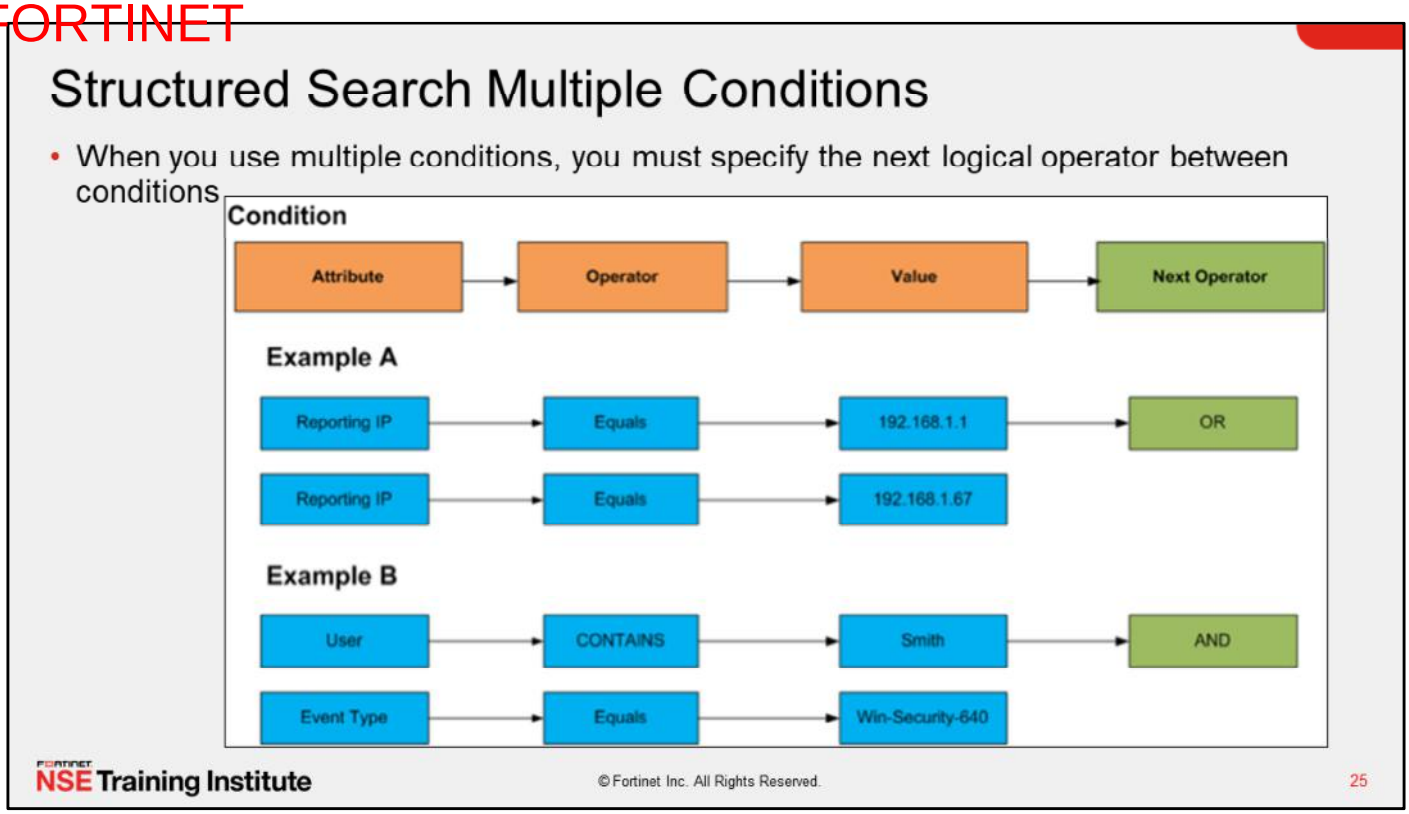
For an example, the **Reporting IP** attribute, which is the IP address of the device that is reporting data, equals a specific value, such as `192.168.1.1`.

Or, the **User** attribute contains the word `Smith`.

You can create structured searches that have single or multiple conditions.

Vouchers & Dumps are Available | WhatsApp +201224560923

DO NOT REPRINT
© FORTINET
Brave-dumps.com



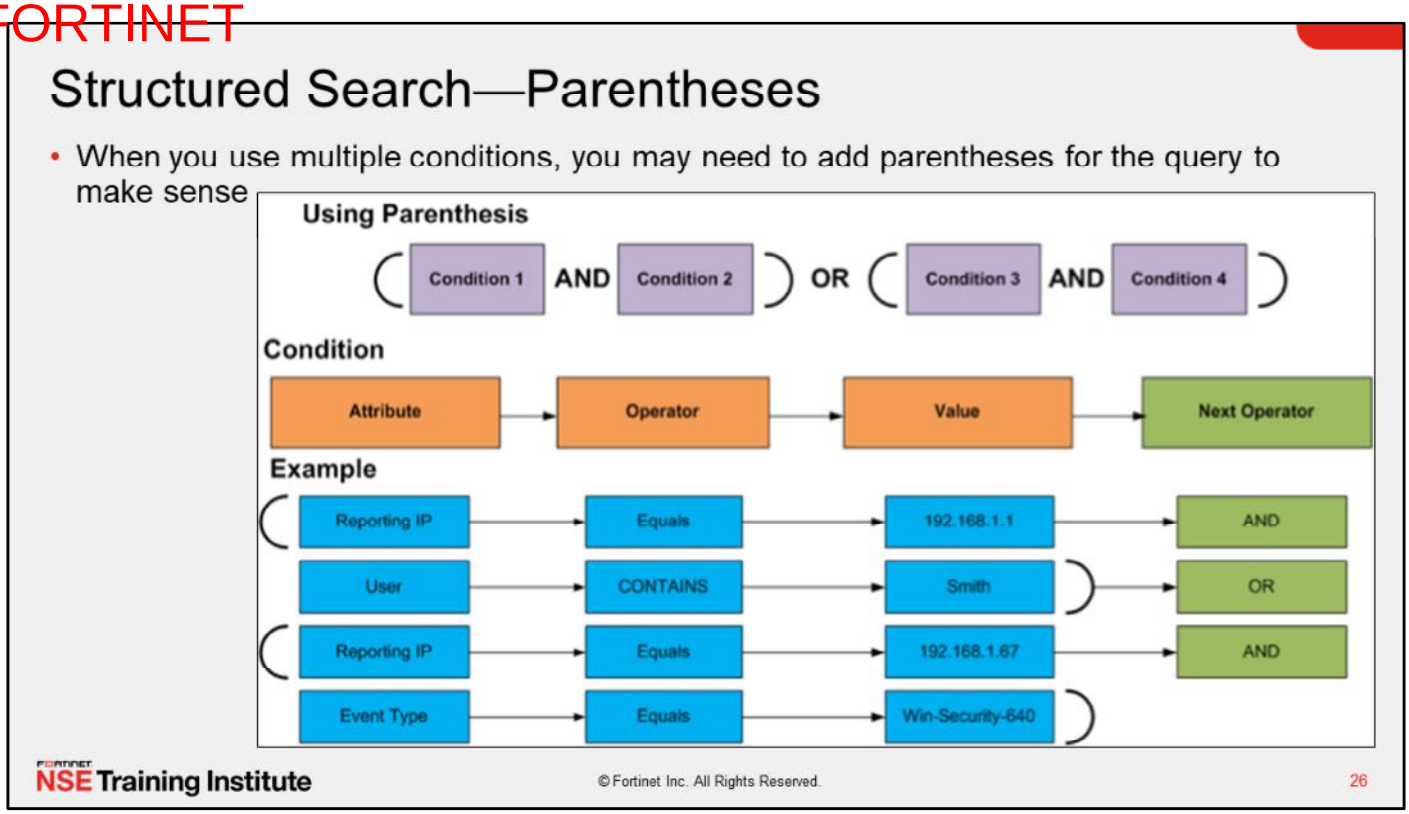
When you use multiple conditions in a structured search, you must specify the *next logical operator* between conditions.

On this slide, example A shows a search for events that came from two specific devices:
- The first condition specifies that the reporting IP equals `192.168.1.1`.
- The second condition specifies that the reporting IP equals `192.168.1.67`.
- The next logical operator between the two conditions is an OR operator, because the search is for events from condition 1 OR condition 2.

On this slide, example B shows a search for a specific event type, but only when the user attribute has a particular value:
- The first condition specifies that the user contains the word `smith`
- The second condition specifies that the event type equals `Win-Security-640`.
- Because you are looking for events in which both of these conditions are met, you must use the AND operator as the next logical operator

Vouchers & Dumps are Available | WhatsApp +201224560923

DO NOT REPRINT
© FORTINET
Brave-dumps.com



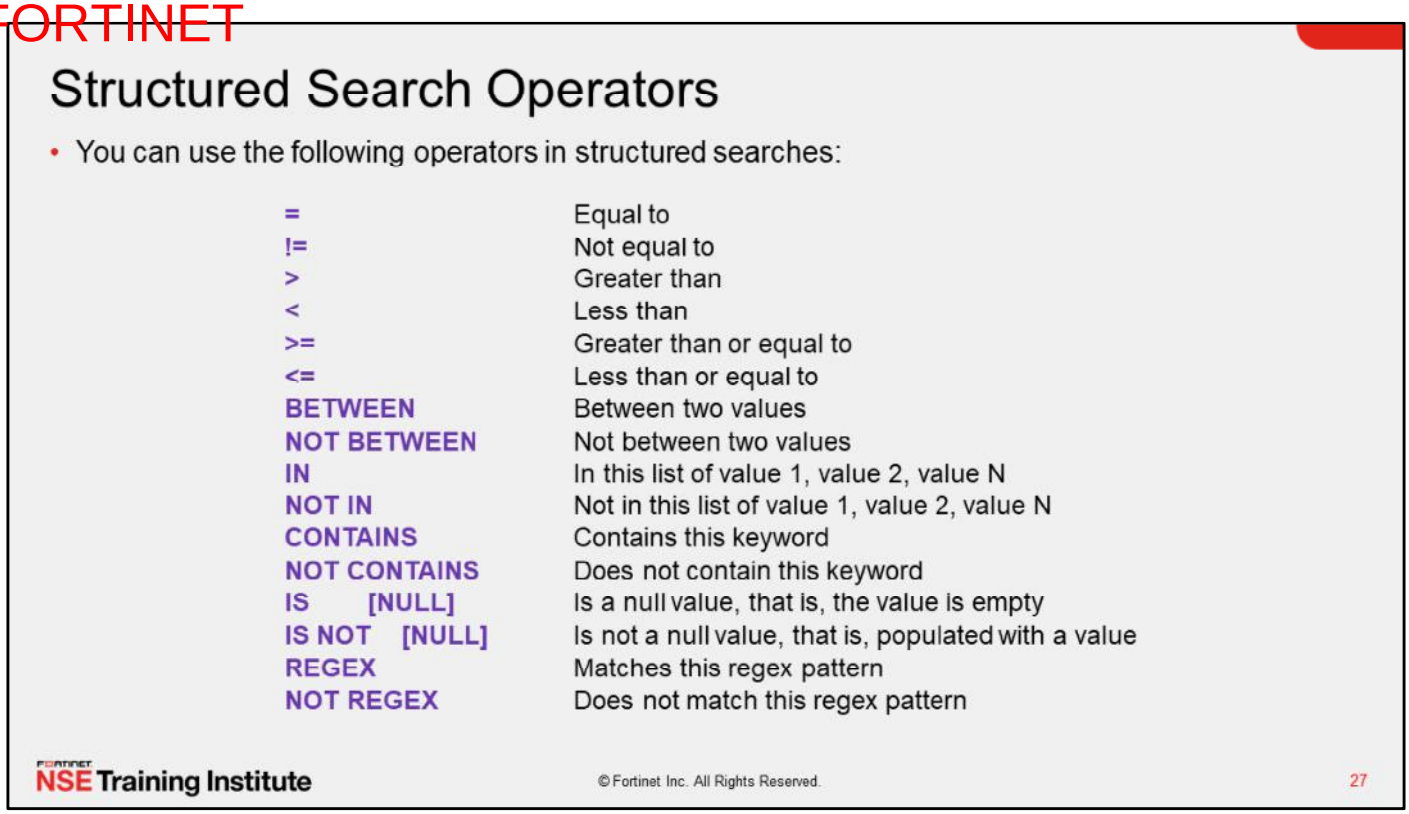
Sometimes, when you are performing a search that has multiple and complex conditions, you may need to use parentheses for the query to make sense. This is a search in which you might specify condition 1 AND condition 2 OR condition 3 AND condition 4.

The interface allows you to put parentheses around specific search conditions, so that the search makes sense.

This slide shows an example of a search for events in which the reporting IP address equals a specific value, AND the user attribute contains a particular word, OR events in which the reporting IP address equals a specific value, AND the event type contains a specific event type.

Vouchers & Dumps are Available | WhatsApp +201224560923

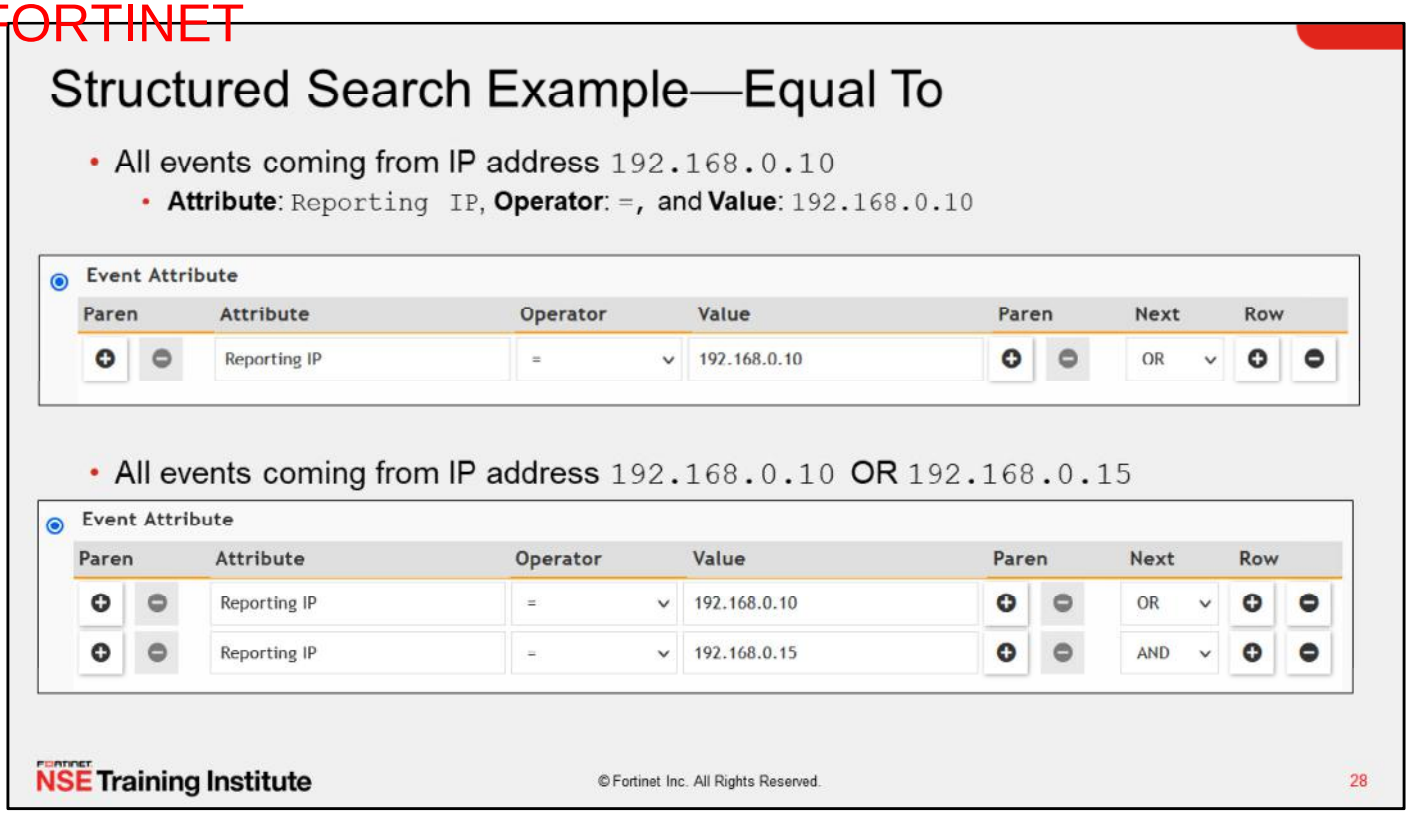
DO NOT REPRINT
© FORTINET
Brave-dumps.com



You can use many different operators in a structured search to filter events and extract the events you are searching for.

Vouchers & Dumps are Available | WhatsApp +201224560923

DO NOT REPRINT
© FORTINET
Brave-dumps.com

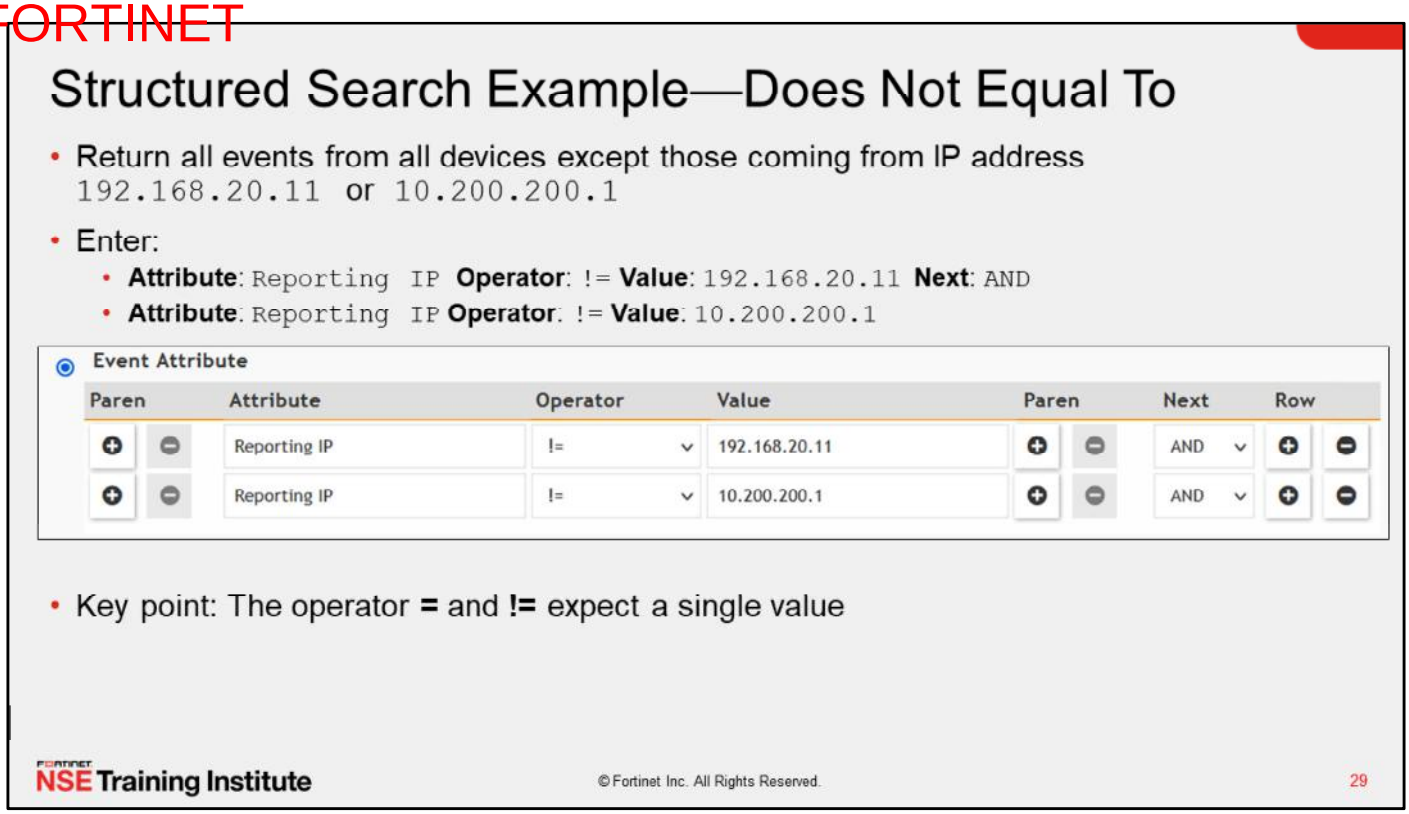


A commonly used operator is the equal to (=) operator, which you have seen in previous examples. To review, if you want to look for all events coming from the IP address `192.168.0.10`, you can create a condition in which the attribute is set to `Reporting IP`, the operator is `=`, and the value is that of the IP address in question.

Similarly, to look at all events coming from two different IP addresses, you can create two conditions like the example shown on the slide. Each condition specifies one of the IP addresses for the value, with the next operator of OR between them.

Vouchers & Dumps are Available | WhatsApp +201224560923

DO NOT REPRINT
© FORTINET
Brave-dumps.com



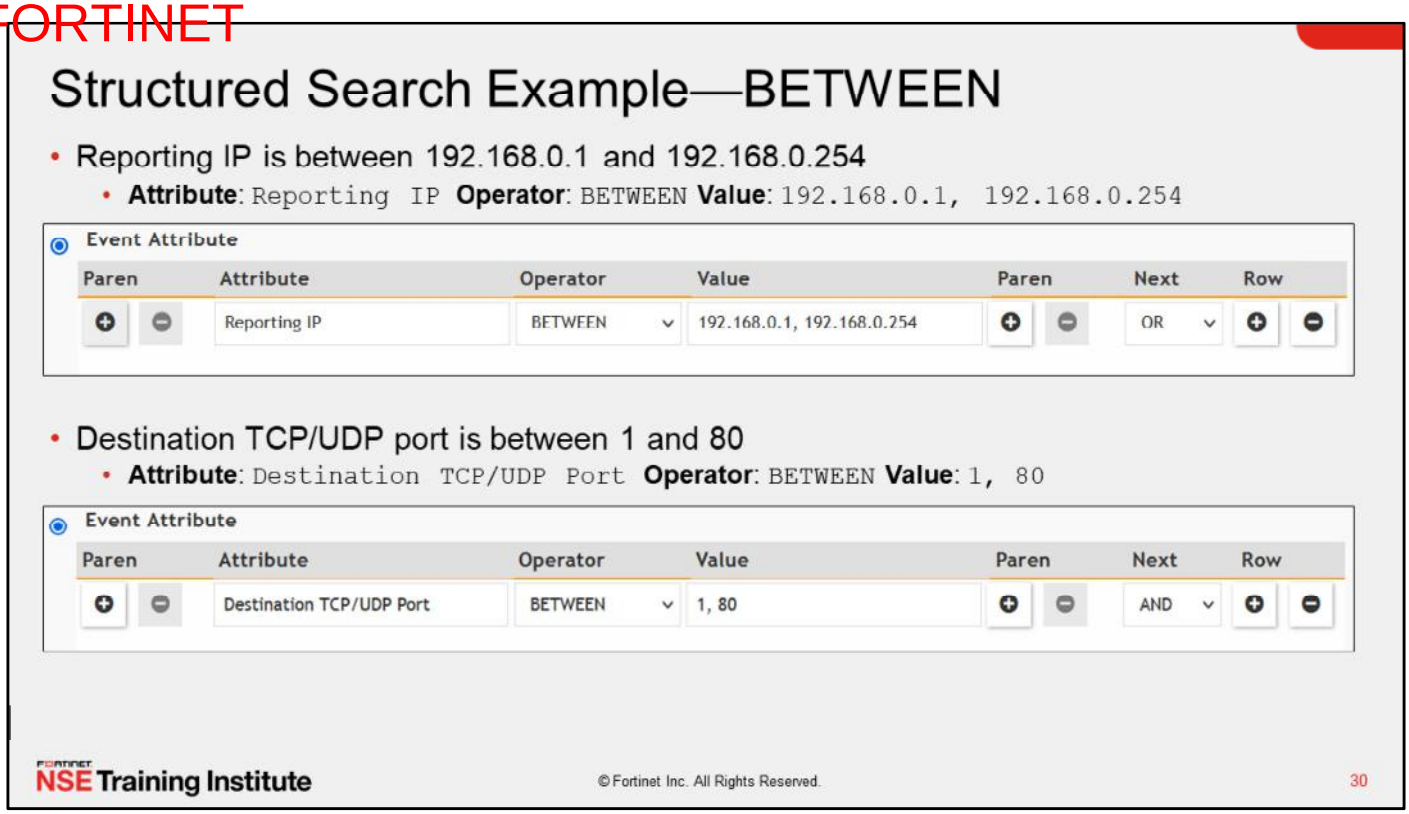
The not equal to (!=) operator performs the opposite function from the equal to (=) operator. In the example shown on this slide, the != operator returns events from all devices, except those coming from IP addresses `192.168.20.11` and `10.200.200.1`.

To achieve this result, create a condition where the reporting IP does not equal to the first IP address, specify the next operator of AND, and then create a second condition where the reporting IP address does not equal to the second IP address.

The key point to remember is that the equal to and the does not equal to operators, expect a single value.

Vouchers & Dumps are Available | WhatsApp +201224560923

DO NOT REPRINT
© FORTINET
Brave-dumps.com



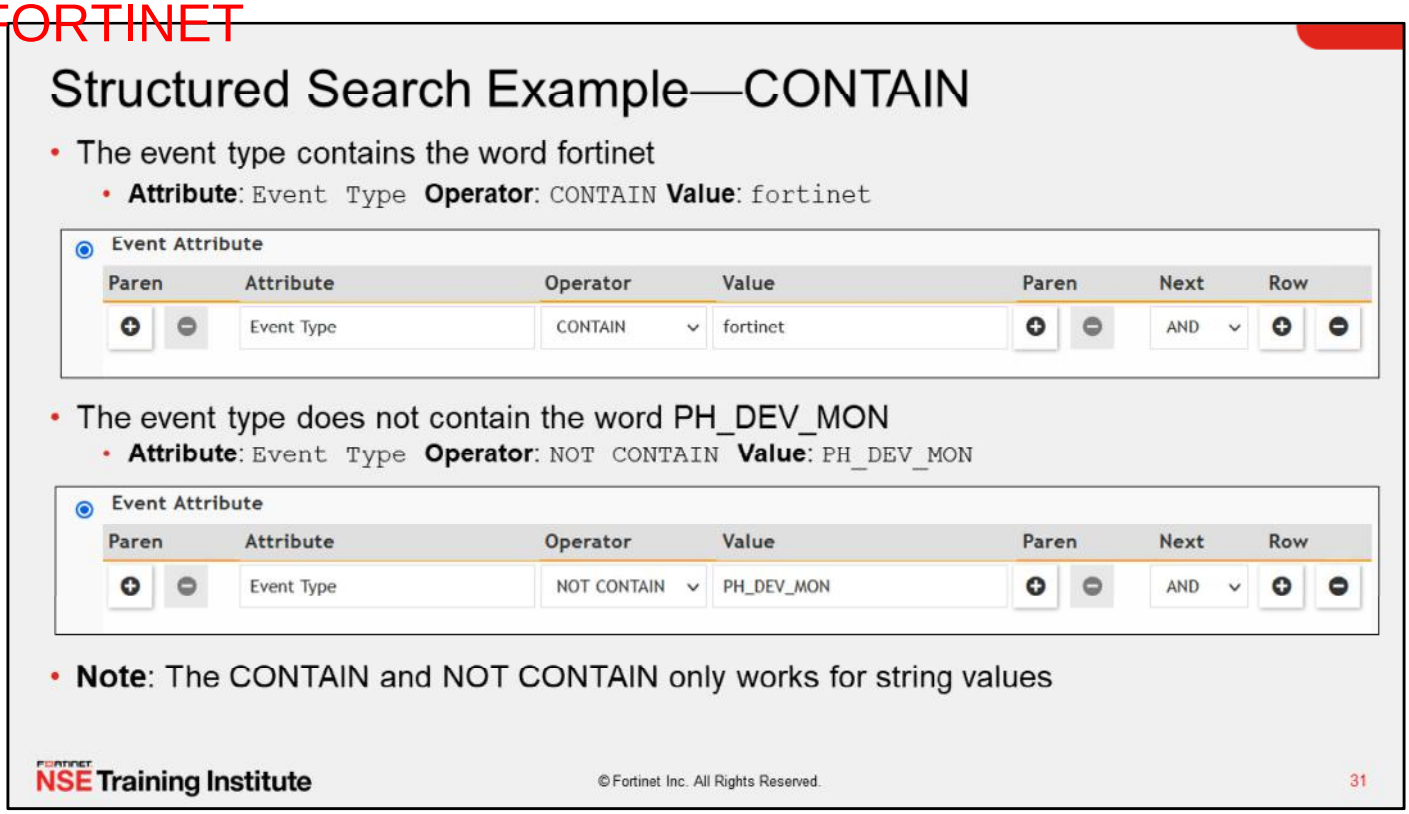
The BETWEEN operator allows you to search for data between two values.

This first example on this slide shows a search for events where the reporting IP address is between `192.168.0.1` and `192.168.0.254`.

You can also use the BETWEEN operator to search for elements such as ports. The second example on this slide shows a search for events containing the destination TCP/UDP port, the operator BETWEEN, and a value between `1` and `80`.

Vouchers & Dumps are Available | WhatsApp +201224560923

DO NOT REPRINT
© FORTINET
Brave-dumps.com



You can use the CONTAINS operator to search for attribute values that contain a specific keyword.

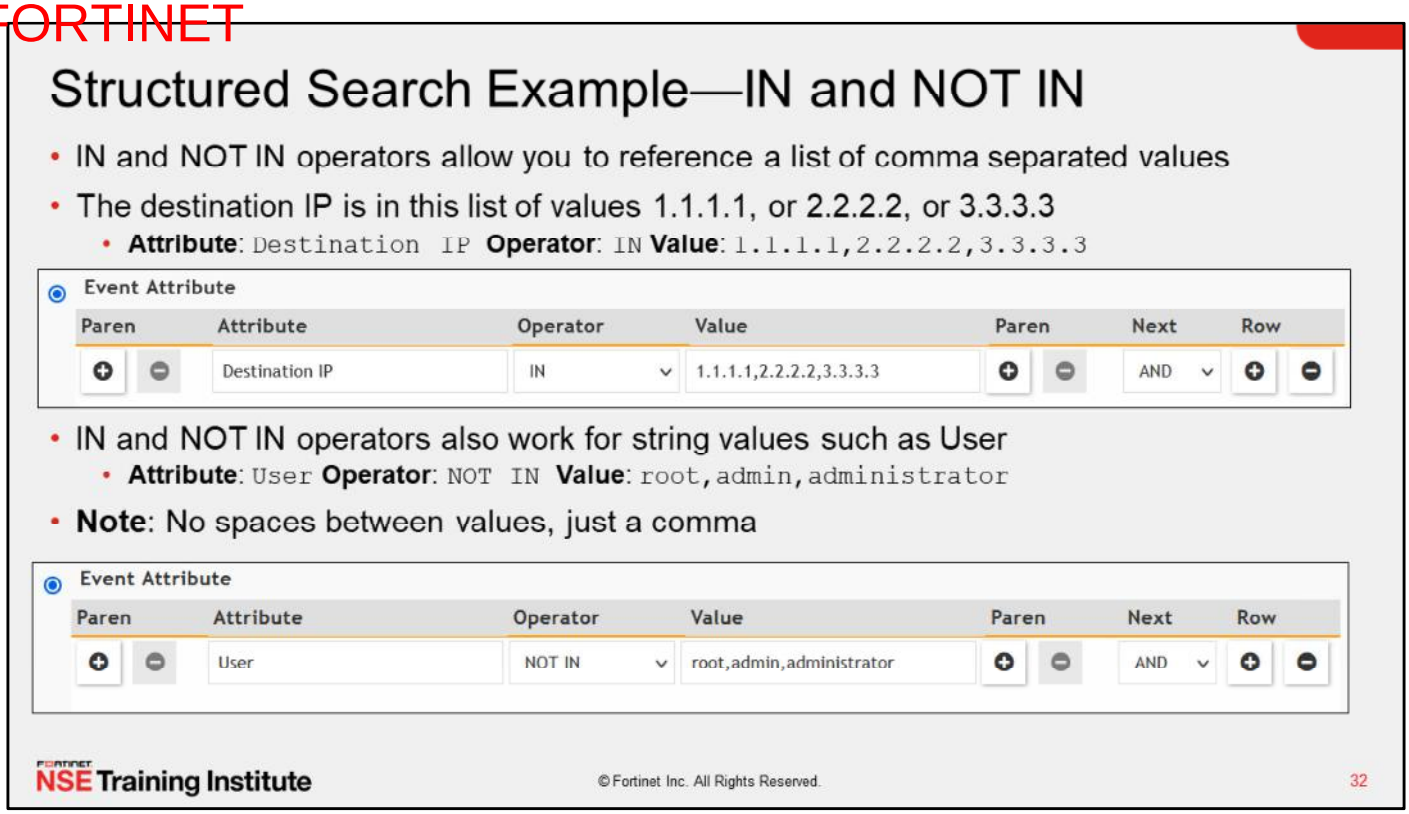
The first example on this slide shows a search for all event types that contain the word `fortinet`.

Alternatively, you can search for all event types that do *not* contain a specific value by using the NOT CONTAIN operator.

Note that the CONTAINS and NOT CONTAINS operators work only with string values. So, if you enter a numerical value, the search treats the numerical value as a string.

Vouchers & Dumps are Available | WhatsApp +201224560923

DO NOT REPRINT
© FORTINET
Brave-dumps.com

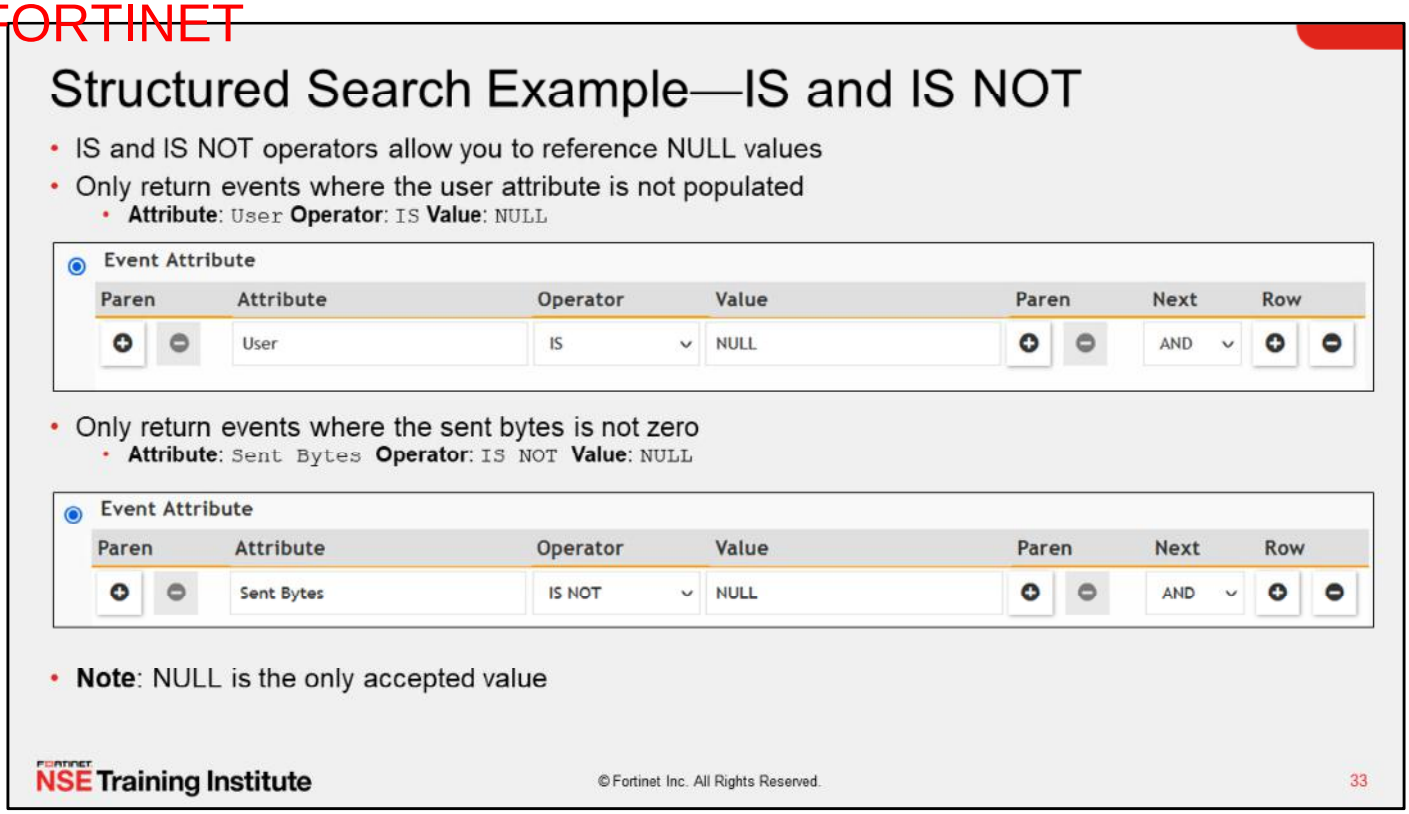


The IN and NOT IN operators allow you to reference a list of comma separated values. This slide shows an example where the reporting IP address is in the comma separated list of `1.1.1.1`, `2.2.2.2`, `3.3.3.3`.

The IN and NOT IN operator also works for string values such as User. So, you can create a condition to search for all events where the user is not root, admin, or administrator.

Vouchers & Dumps are Available | WhatsApp +201224560923

DO NOT REPRINT
© FORTINET
Brave-dumps.com



The IS and IS NOT operators allow you to reference NULL values. That is, attributes that have not been populated with a value.

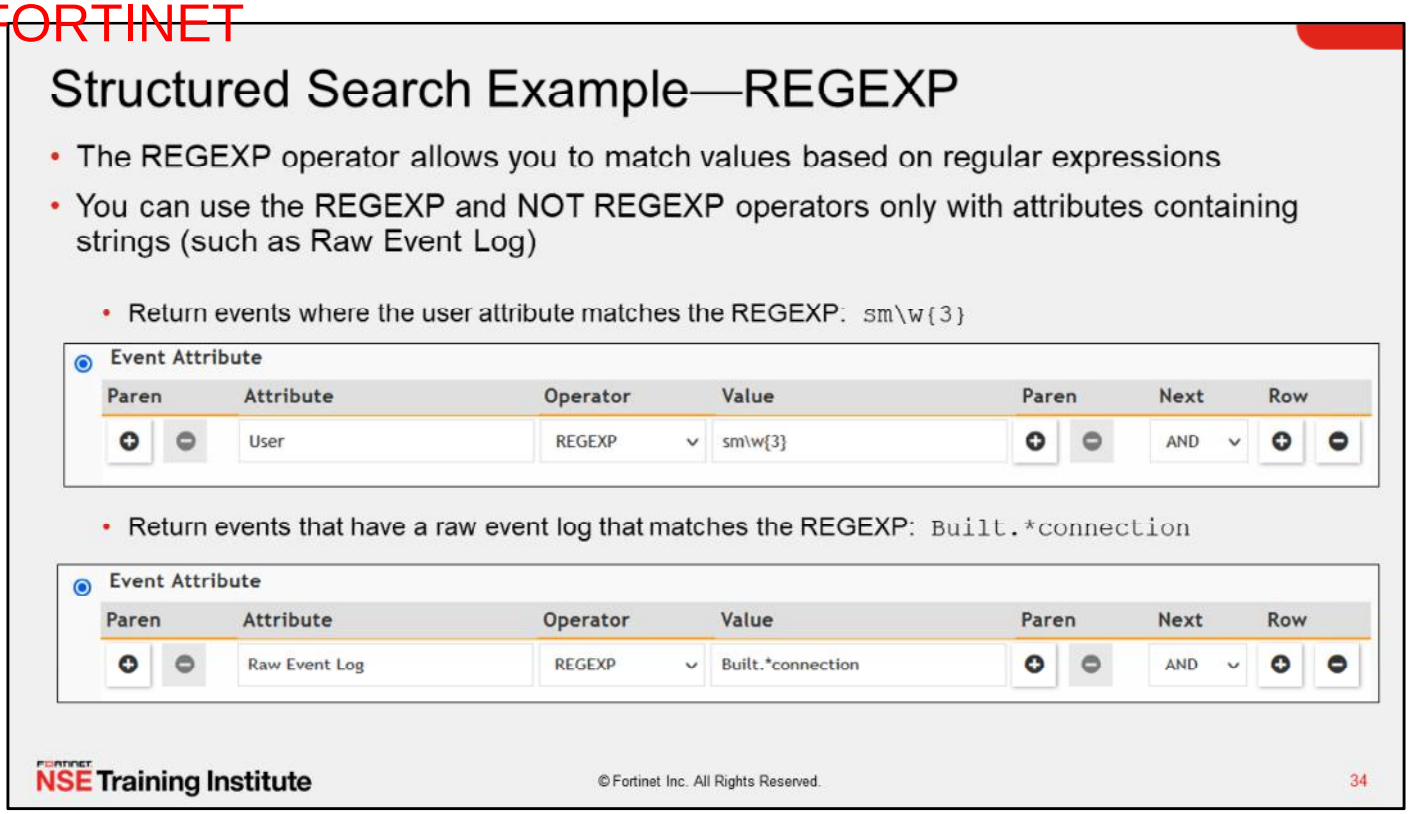
The first example on this slide shows a search for all events where the user attribute is not populated. In this condition, the attribute is set to `User`, the operator is set to `IS`, and the value is `NULL`.

The second example on this slide shows a search for events that have a value populated in the `Sent Bytes` attribute using the IS NOT operator.

Note that the word NULL is the only accepted value for the IS and IS NOT operator. You must type the word `NULL` because it doesn't appear in the **Value** drop-down list.

Vouchers & Dumps are Available | WhatsApp +201224560923

DO NOT REPRINT Brave-dumps.com
© FORTINET



A regular expression, or REGEXP, is a sequence of characters that define a search pattern. This pattern is then used by string searching algorithms to match the pattern in a string. The REGEXP operator allows you to match values based on regular expression patterns applied against the event attribute.

You can use the REGEXP and NOT REGEXP operators only with attributes containing strings.

The example on this slide shows a search for events where the user attribute matches the REGEXP pattern `sm\w{3}`. This REGEXP pattern looks for any string that starts with `sm` followed by three letters. The results match any five-letter word that starts with `sm`, such as the words smith, small, smile, and so on.

You can also apply regex to the raw event log by selecting raw event log as the attribute. The example on this slide shows a search for events containing the REGEXP value of `Built.*connection`. This search returns events where the Raw Event Log attribute contains the word `Built`, with a greedy match for anything up to the word `connection`.

The NOT REGEXP operator return events that did *not* match the REGEXP string in the attribute value.

Vouchers & Dumps are Available | WhatsApp +201224560923

DO NOT REPRINT
© FORTINET
Brave-dumps.com

Knowledge Check

1. Why would this search return no events?

   Attribute: `Reporting IP` **Operator:** `=` **Value:** `1.1.1.1` **Next :** `AND`
   Attribute: `Reporting IP` **Operator:** `=` **Value:** `2.2.2.2`

   ✓ A. Wrong boolean operator
   B. Invalid IP subnet

2. Review the search syntax below. Is the syntax valid?

   Attribute: `User` **Operator:** `IS` **Value:** `Administrator`

   A. Yes
   ✓ B. No

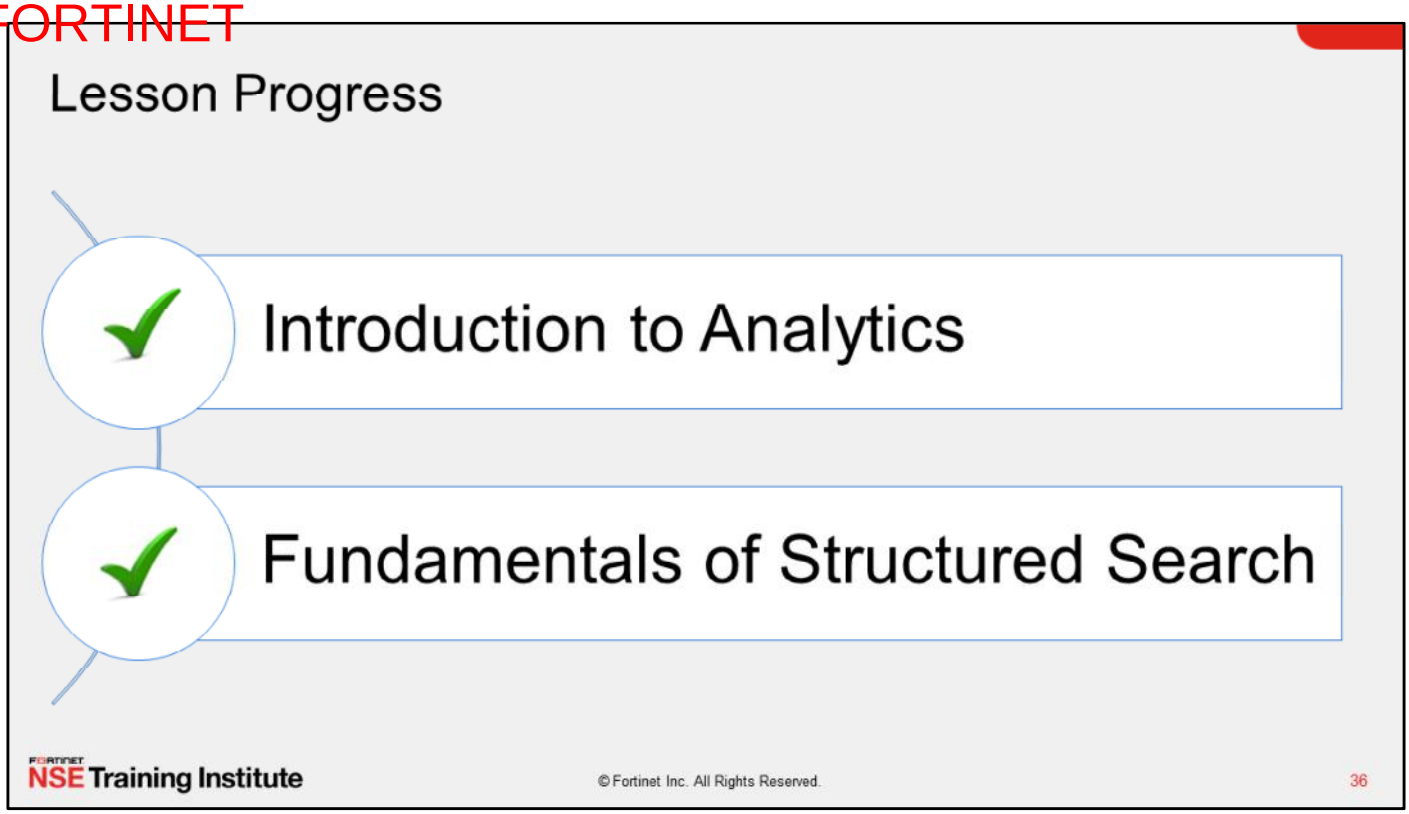
NSE Training Institute

© Fortinet Inc. All Rights Reserved.

35

Vouchers & Dumps are Available | WhatsApp +201224560923

DO NOT REPRINT
© FORTINET
Brave-dumps.com

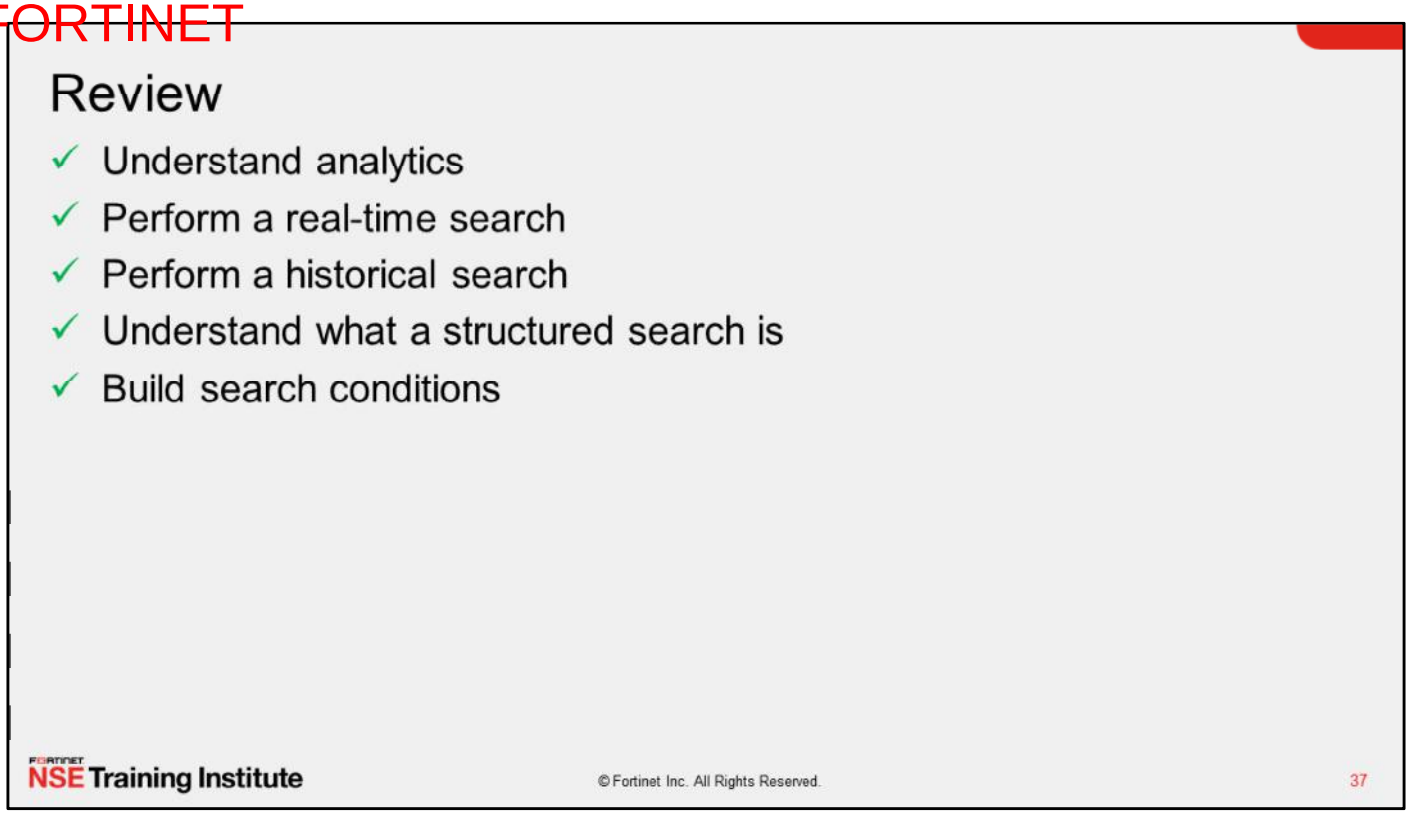


Congratulations! You have completed this lesson.

Now, you will review the objectives that you covered in this lesson.

Vouchers & Dumps are Available | WhatsApp +201224560923

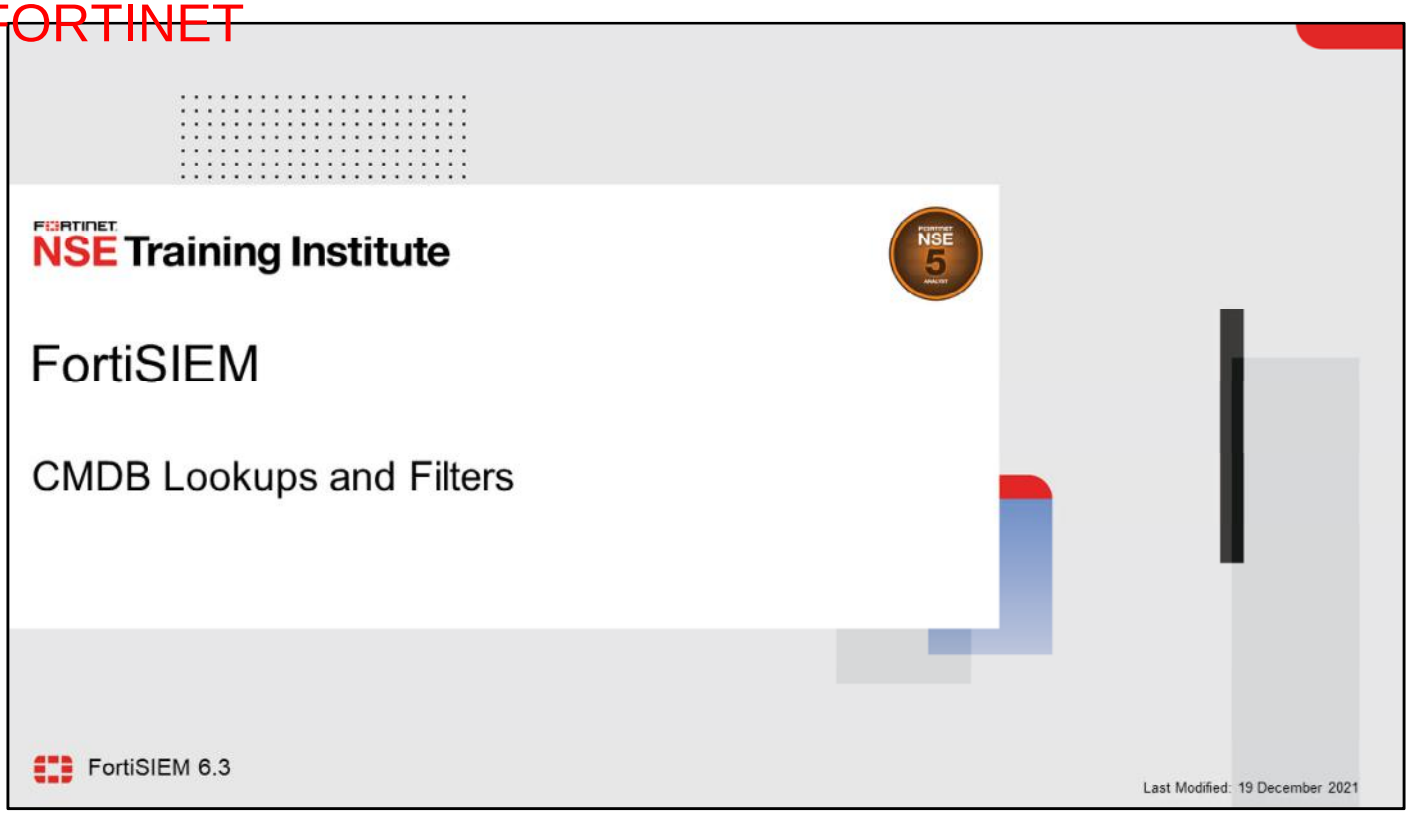
DO NOT REPRINT
© FORTINET
Brave-dumps.com



This slide shows the objectives that you covered in this lesson.
By mastering the objectives you covered in this lesson, you learned how to understand and use analytics and structured searches.

Vouchers & Dumps are Available | WhatsApp +201224560923

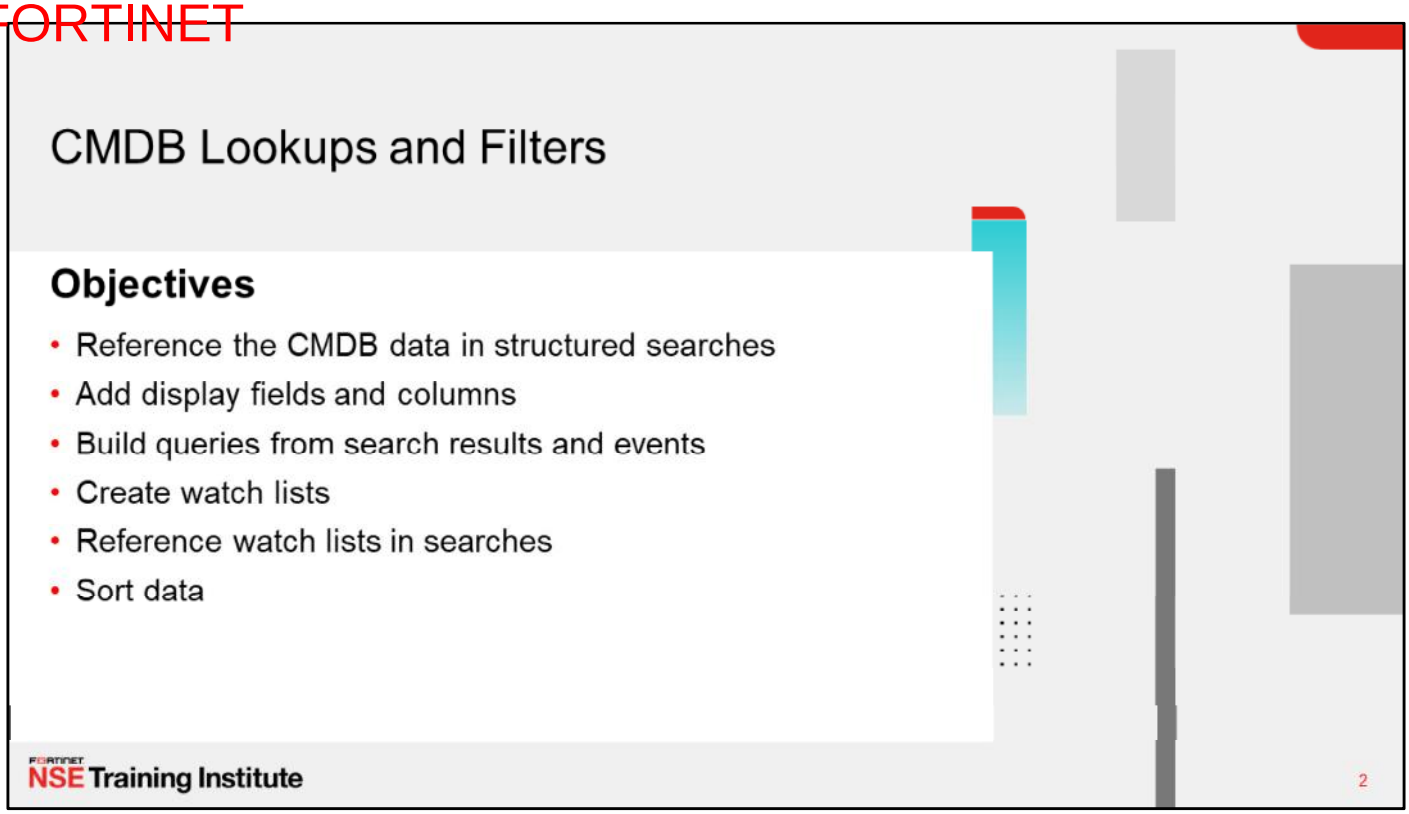
DO NOT REPRINT
© FORTINET
Brave-dumps.com



In this lesson, you will learn about ways to reference the CMDB in search queries, as well as ways to filter and sort the results.

Vouchers & Dumps are Available | WhatsApp +201224560923

DO NOT REPRINT
© FORTINET
Brave-dumps.com

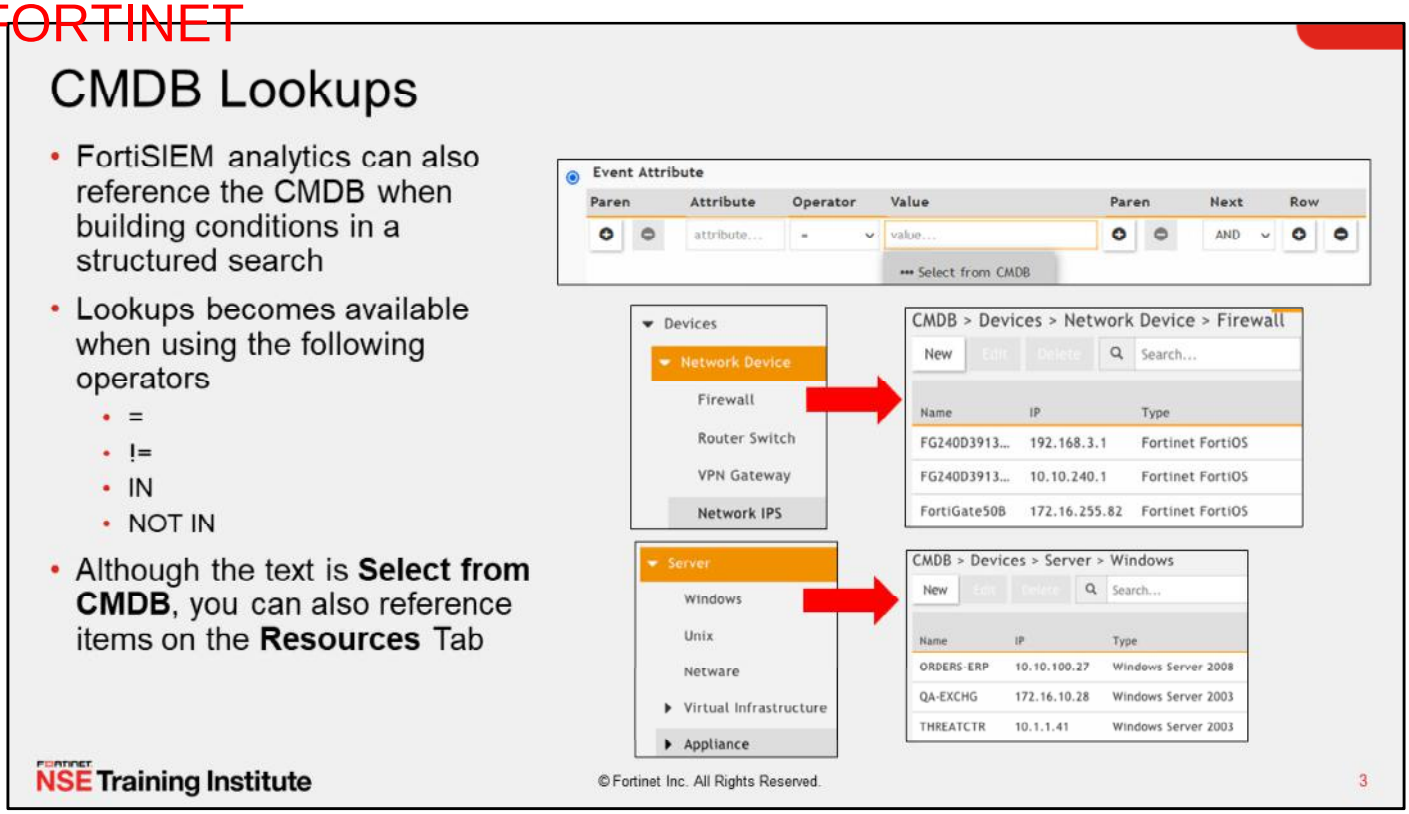


After completing this lesson, you should be able to achieve the objectives shown on this slide.

By demonstrating competence in CMDB lookups and filters, you will be able to reference the CMDB data in structured searches, build and display search results, create watch lists, and reference watch lists.

Vouchers & Dumps are Available | WhatsApp +201224560923

DO NOT REPRINT
© FORTINET
Brave-dumps.com



What if you want to list the events that come from all of your organization's firewalls? It's not uncommon for an organization to use firewall devices from different vendors. So, you could create a search that has conditions for each type of firewall in your network.

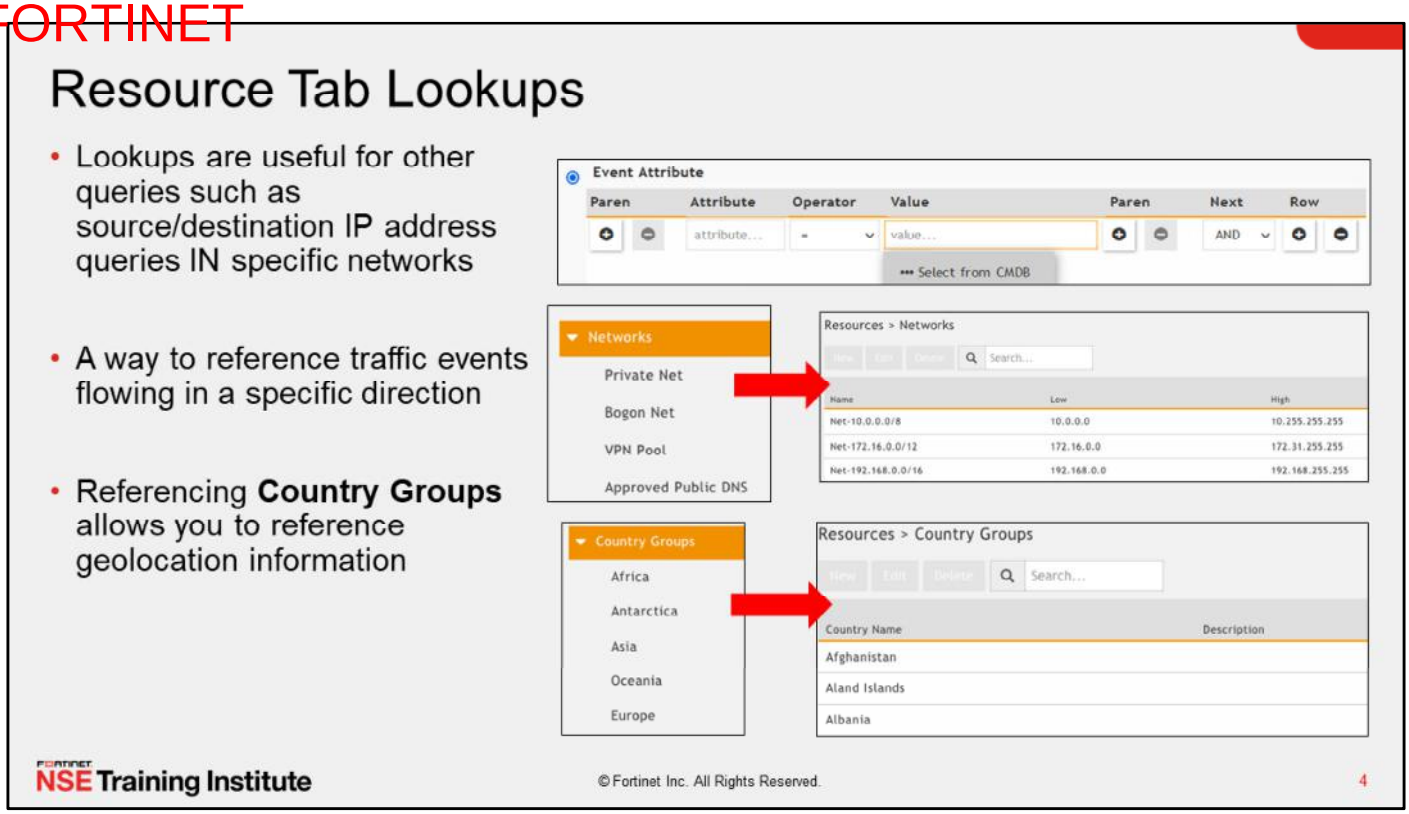
CMDB groups your devices into different categories and FortiSIEM analytics allows you to reference the CMDB when building conditions in a structured search. So, you need to create only one condition that references the firewall group in the CMDB to search all of your organization's firewalls.

The condition would read something like the following: the **Reporting IP** address is **IN** the **Firewall** CMDB group, or: the **Reporting IP** is **IN** the server CMDB group.

The CMDB lookup option becomes available only when you are using the equal to, not equal to, in, and not in operators.

Vouchers & Dumps are Available | WhatsApp +201224560923

DO NOT REPRINT
© FORTINET
Brave-dumps.com



The CMDB lookups are useful for other types of queries, such as source/destination IP address queries in a specific network segment.

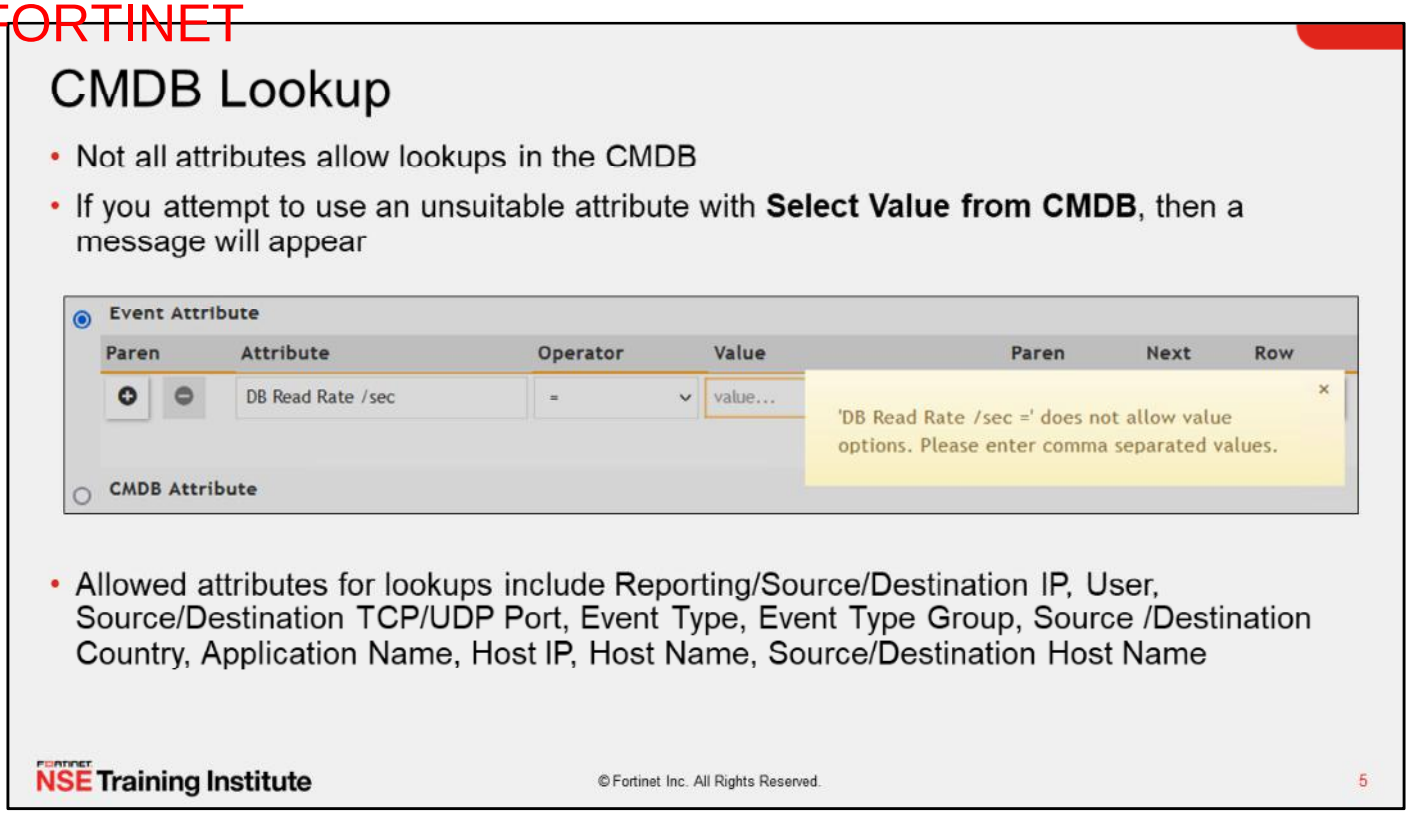
When you perform a device discovery, FortiSIEM looks at the IP address and subnet mask on the network interfaces, and can then populate the various network segments. This is one way to reference traffic events in a particular direction, or to a particular network.

For example, your search condition might have **Source IP** for the attribute and **IN** as the operator. Then, you can browse the CMDB and select the appropriate network segment. Or, you could say that the device in question is **NOT IN** a specific network segment.

You can also reference specific application groups to search for events only from devices running specific apps.

Vouchers & Dumps are Available | WhatsApp +201224560923

DO NOT REPRINT
© FORTINET
Brave-dumps.com



Not all FortiSIEM attributes allow lookups in the CMDB.

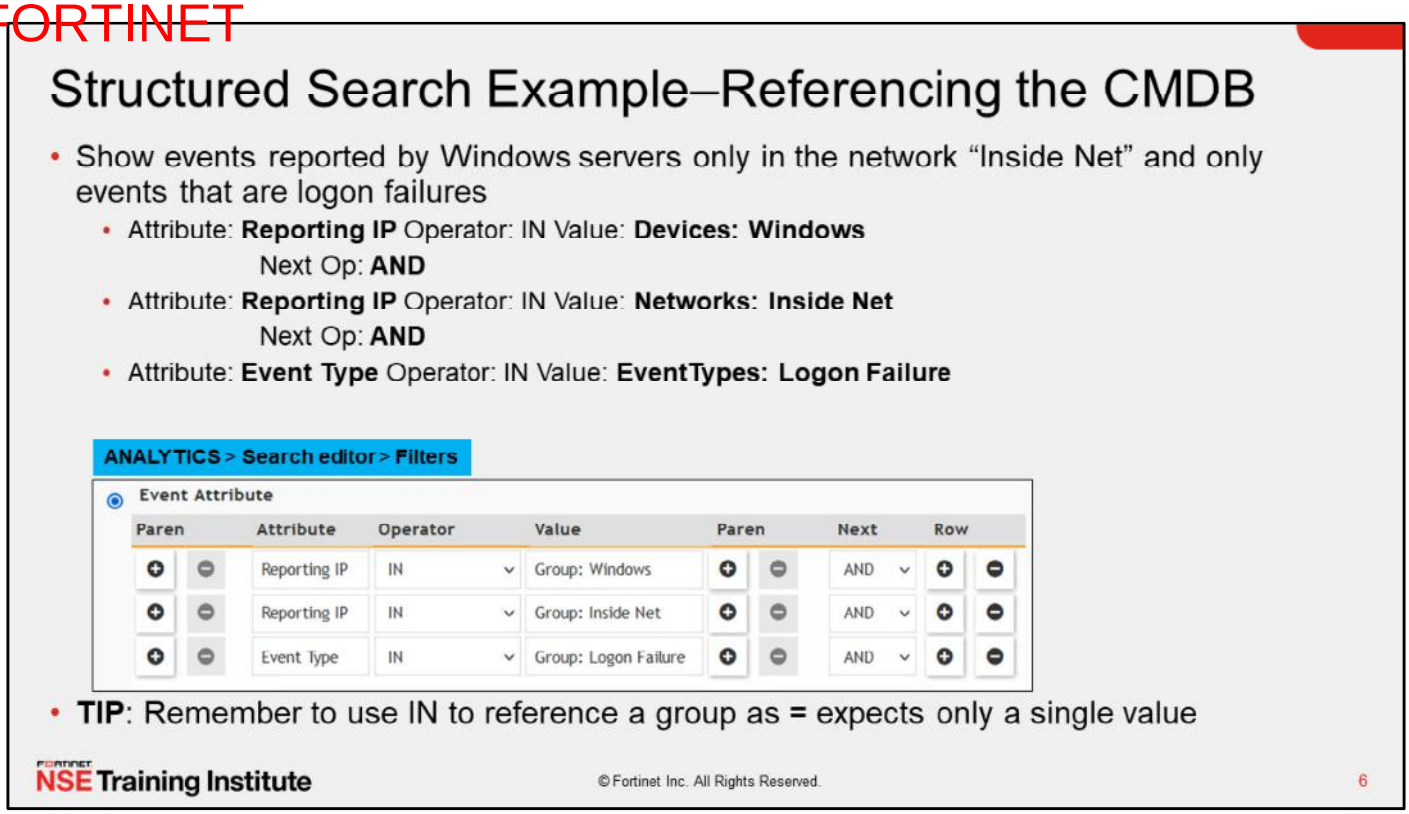
If you look up an unavailable attribute in **Select Value from CMDB**, then a prompt message will appear notifying you that the option isn't available for the selected attribute type.

The first example shown on this slide shows the **DB Read Rate (/sec)** attribute. There is nothing to reference in the CMDB for this attribute, so clicking **Select Value from CMDB** will prompt a message to appear stating that the selected attributes does not allow value option**.**

Allowed attributes for lookup include, Reporting IP, Source IP, Destination IP, User, Source or Destination TCP/UDP Port, Event Type, Event Type Group, Source or Destination Country, Application Name, Host IP, Host Name, Source or Destination Host Name, and so on.

Vouchers & Dumps are Available | WhatsApp +201224560923

DO NOT REPRINT
© FORTINET
Brave-dumps.com



The example on this slide shows a structured search that references the CMDB.

Say you wanted to show events reported by Windows servers within your network, but only Windows servers that are located in a specific network segment, and only events that are logon failures. In the structured search, you can set the first condition's attribute as **Reporting IP** and the operator to **IN**. Then, you can browse the CMDB and select the **Windows** device group, and then set the next operator to **AND**.

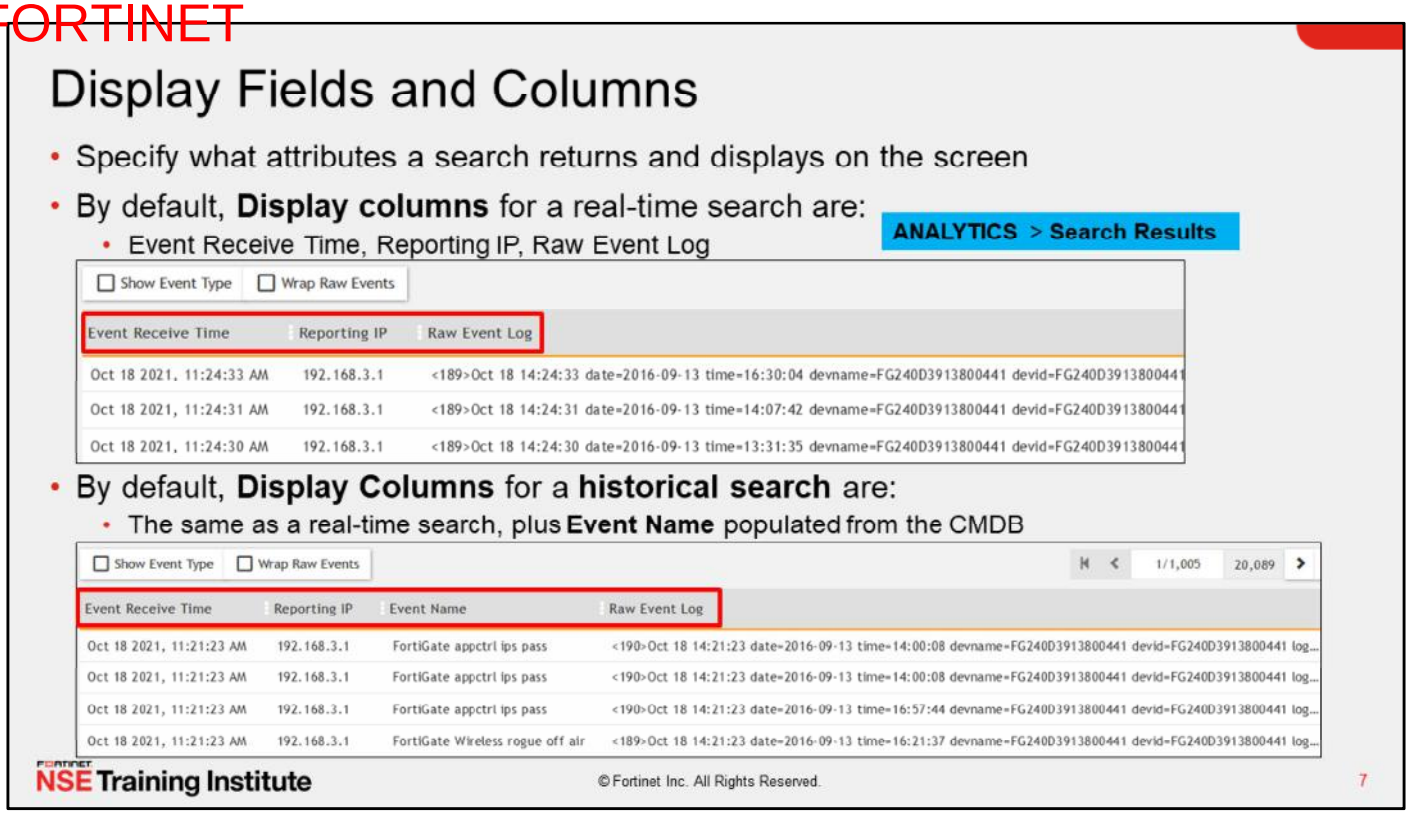
Then, you can set the second condition's attribute as **Reporting IP** and the operator to **IN**, and then browse the CMDB. This time, select the **Networks: Inside Net** value, and then set the Next Operator to **AND**.

The third condition's attribute is **Event Type**, the operator is **IN**. Then, in the CMDB, browse the event types values, and then select **Event Types: Logon Failure**.

Remember to use **IN** to reference a group because **=** allows you to select only a single value. Therefore, if you use =, you can select only individual devices in the CMDB; however, if you use IN, you can select multiple devices or classifications of devices, such as firewall groups, server groups, and so on.

Vouchers & Dumps are Available | WhatsApp +201224560923

DO NOT REPRINT
© FORTINET
Brave-dumps.com



Display fields and columns specify what attributes display on the screen when you perform a search.

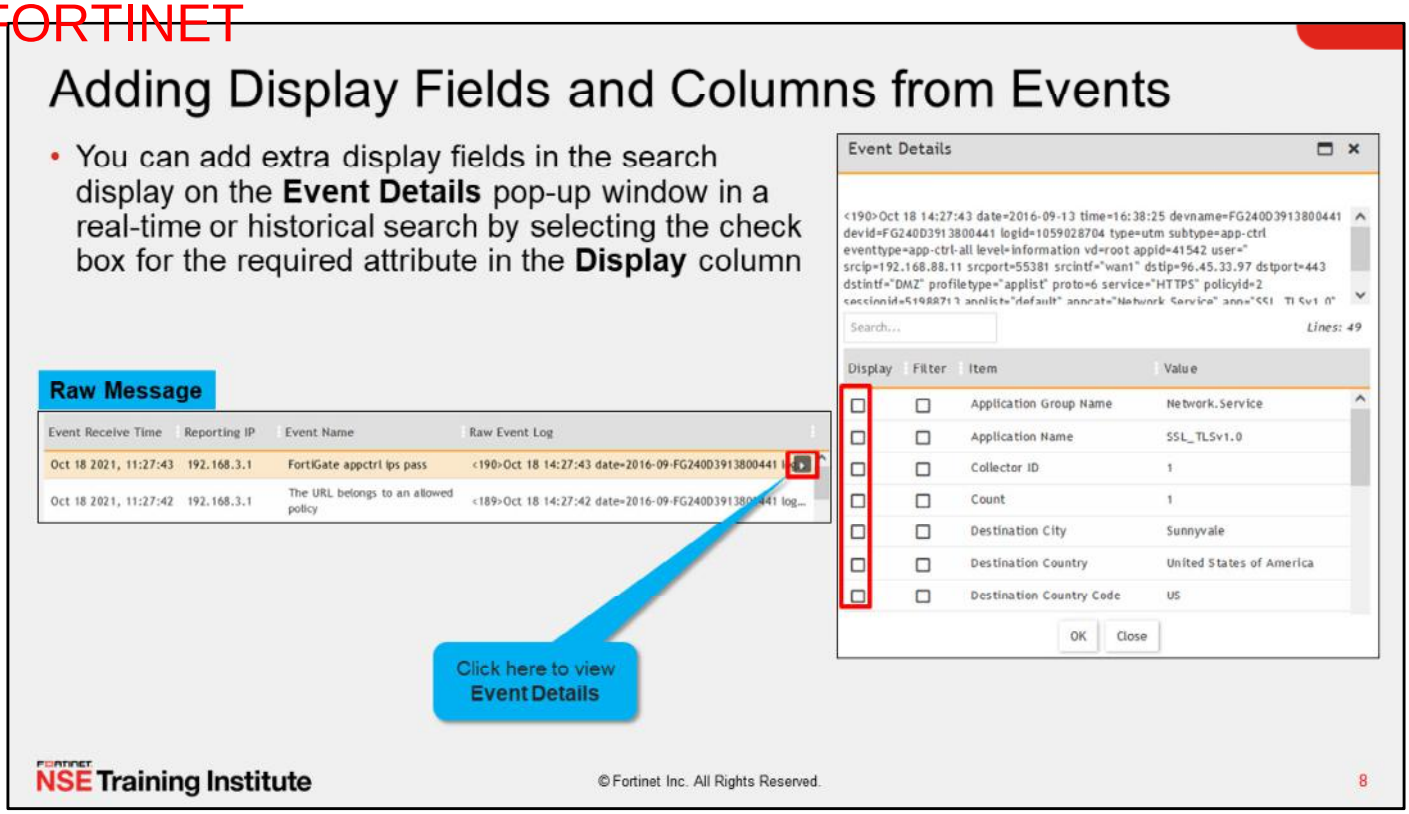
By default, the display columns for a real-time search are:
- **Event Receive Time**
- **Reporting IP**
- **Raw Event Log**

You can include **Event Type** by selecting the **Show Detail** option.

By default, the display columns for a historical search are the same as a real-time search, plus the **Event Name** column. The event name comes from the CMDB, and so is not available in a real-time search.

Vouchers & Dumps are Available | WhatsApp +201224560923

DO NOT REPRINT
© FORTINET
Brave-dumps.com



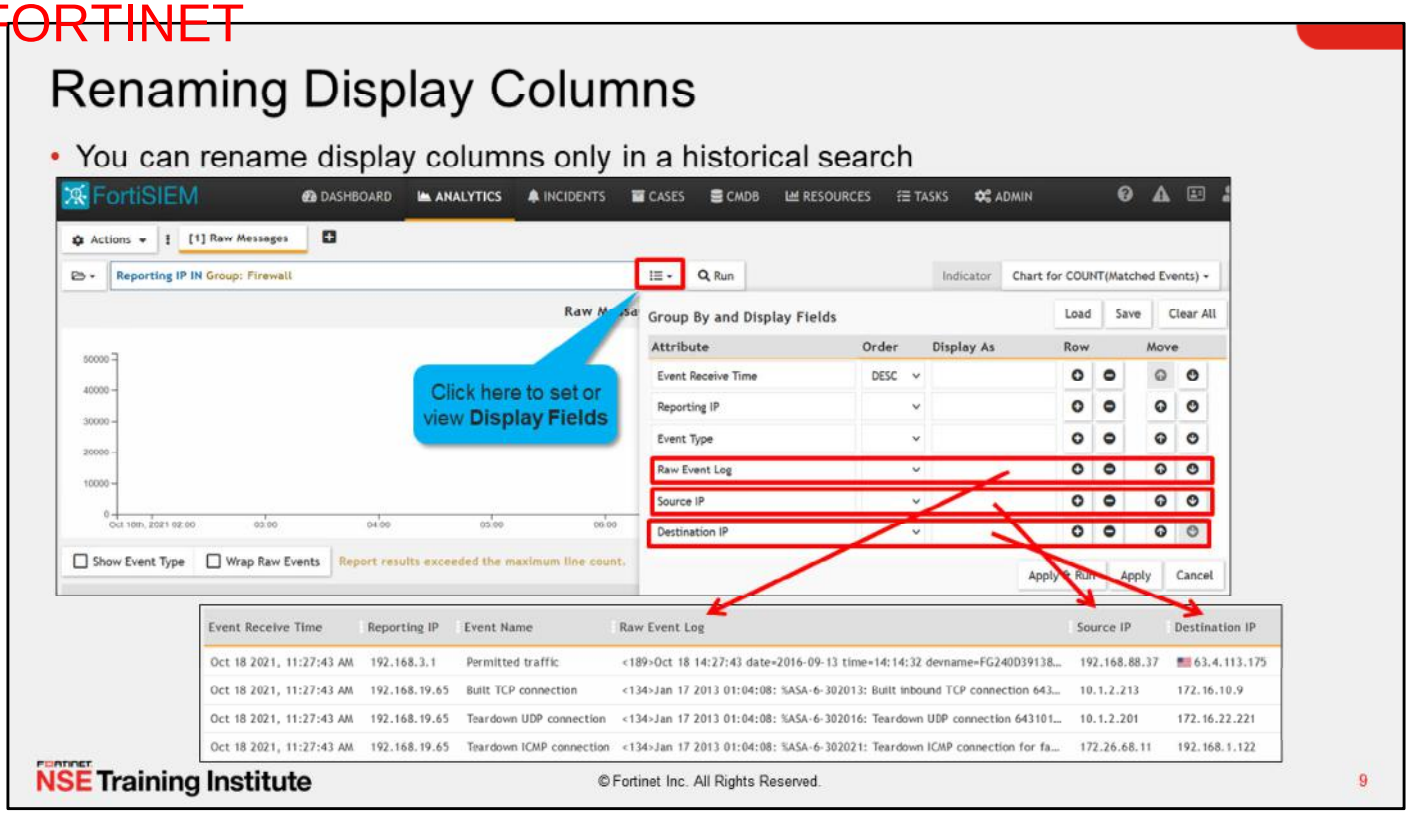
The default display fields and columns might not meet all your requirements. Sometimes, you must add additional fields and columns to the display. You can do this using the **Event Details** pop-up window.

The example on this slide shows that adding display fields and columns works for both real-time searches and historical searches. The first column is the **Display** column. If you select any of the check boxes in the **Display** column and then run the search again, the selected columns will display on the screen.

To view the **Event Details** window, select any raw log message**.** Once the message is selected, a right arrow icon will appear under **Raw Event Log** column. Clicking the icon will provide you the **Event Details** associated with that event.

Vouchers & Dumps are Available | WhatsApp +201224560923

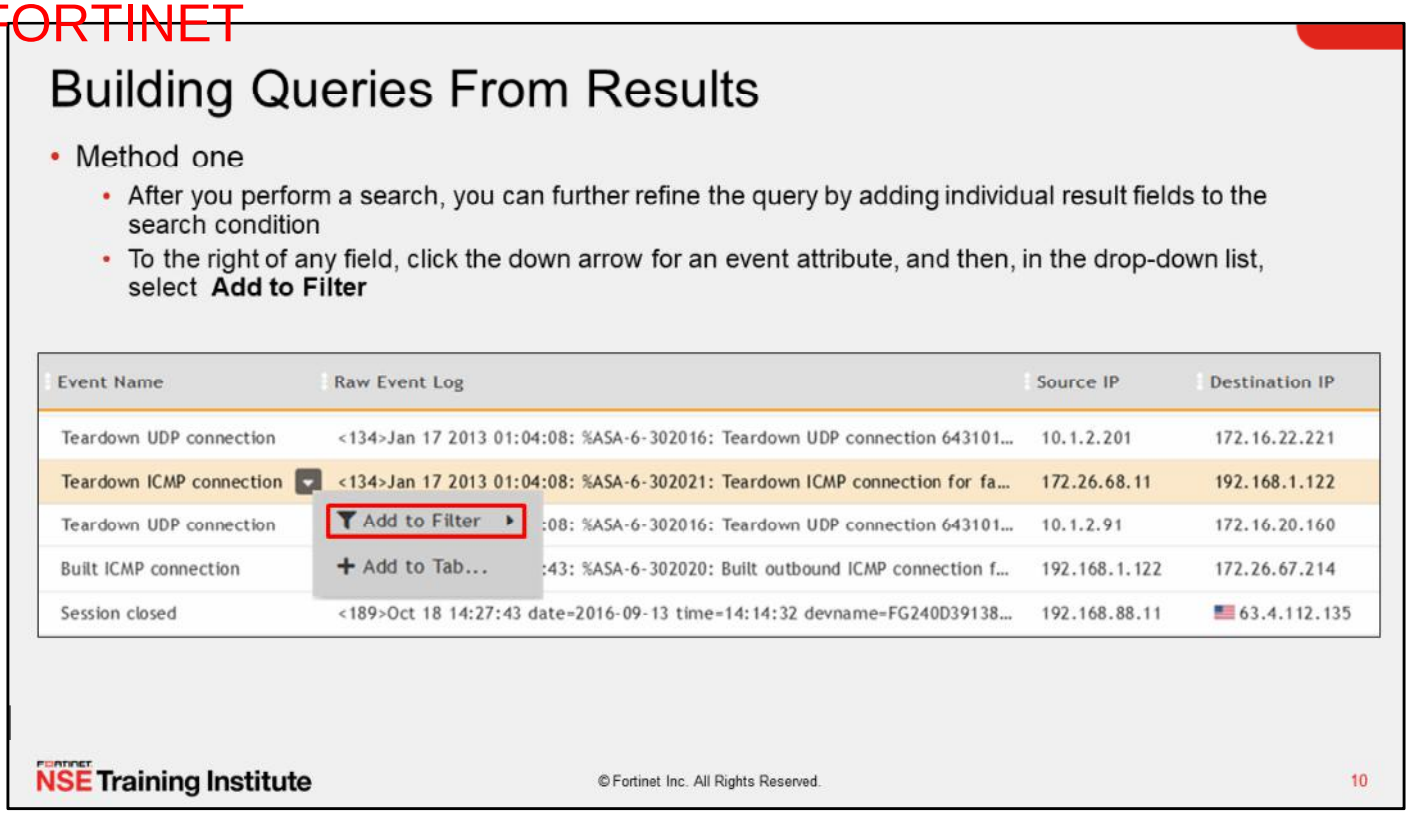
DO NOT REPRINT
© FORTINET
Brave-dumps.com



You can rename display columns, but only in a historical search. If you click in the display column, a list all of the attributes that will display on the screen will appear. The **Display As** column allows you to change the display name of a specific column, which is useful for reporting.

Vouchers & Dumps are Available | WhatsApp +201224560923

DO NOT REPRINT
© FORTINET
Brave-dumps.com

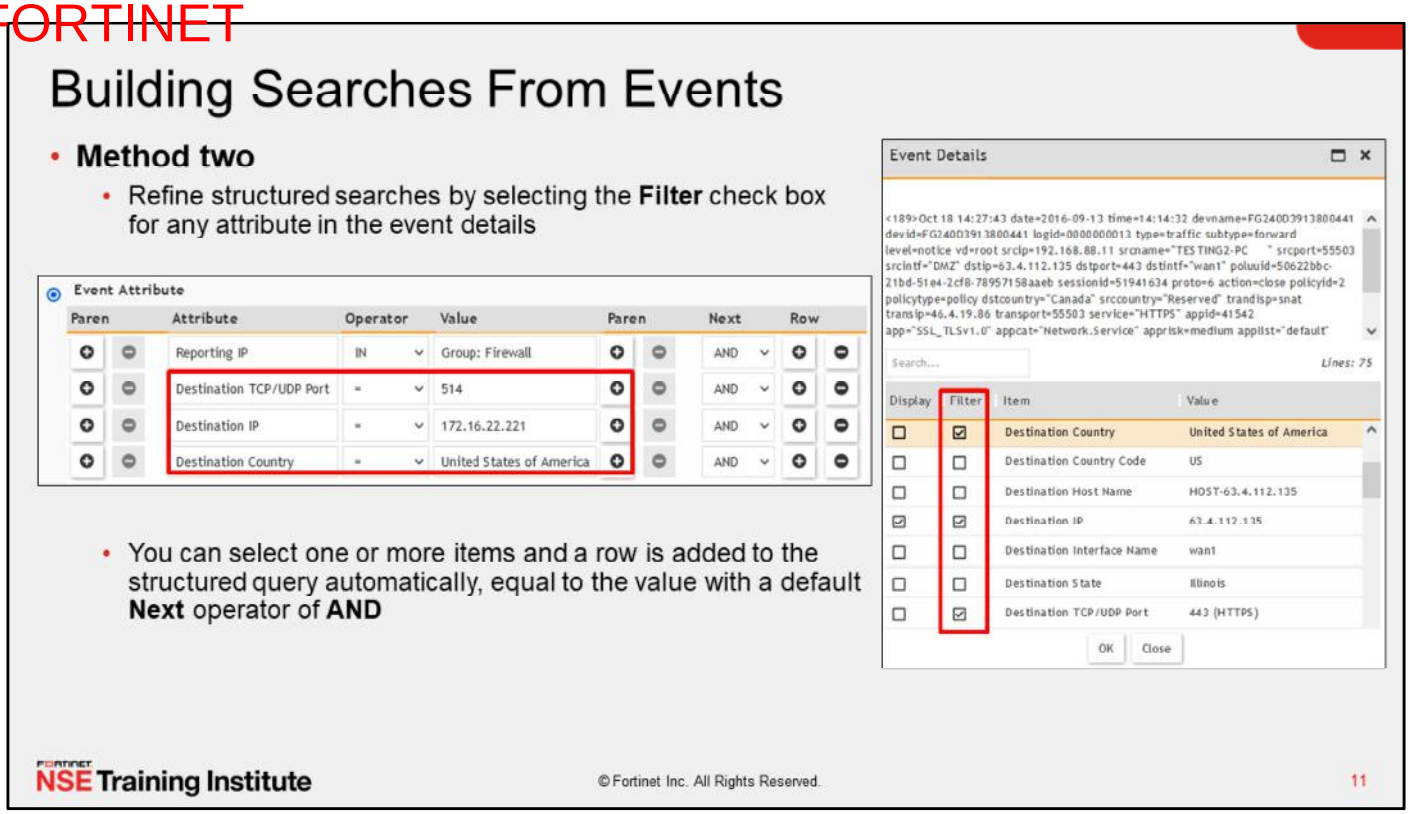


If you perform a search, and you want to drill deeper into something you saw in the results, there are a couple of ways to refine the search results.

Using method one, highlight a value in any display column, and then click the white down arrow that appears. In the drop-down list, select **Add to Filter**, to add the value to the search condition. Run the search again to apply the new attribute.

Vouchers & Dumps are Available | WhatsApp +201224560923

DO NOT REPRINT
© FORTINET
Brave-dumps.com



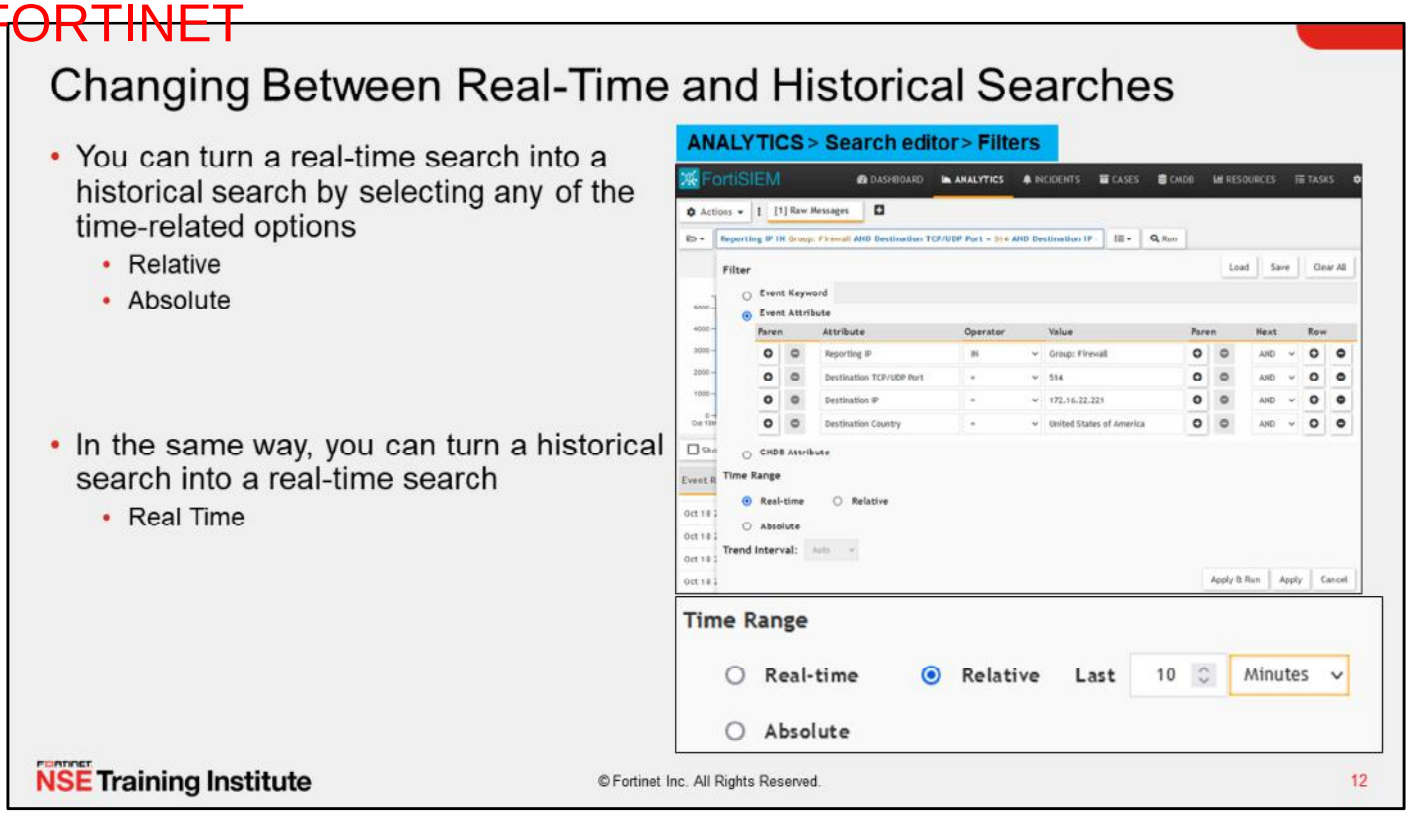
The second method of refining your search uses the **Event Details** screen.

On the **Event Details** screen, the column located to the right of the **Display** column is the **Filter** column. You can select one or more items for any event to add the items automatically to the search condition.

By default, the added search conditions have a **Next** operator of **AND**, but you can go back to the search and change the **Next** operator to other available option according to the logic of your condition.

Vouchers & Dumps are Available | WhatsApp +201224560923

DO NOT REPRINT
© FORTINET
Brave-dumps.com



Search can be performed in two modes:
- Real-time mode: from current time onwards.
- Historical mode: for previous time periods.

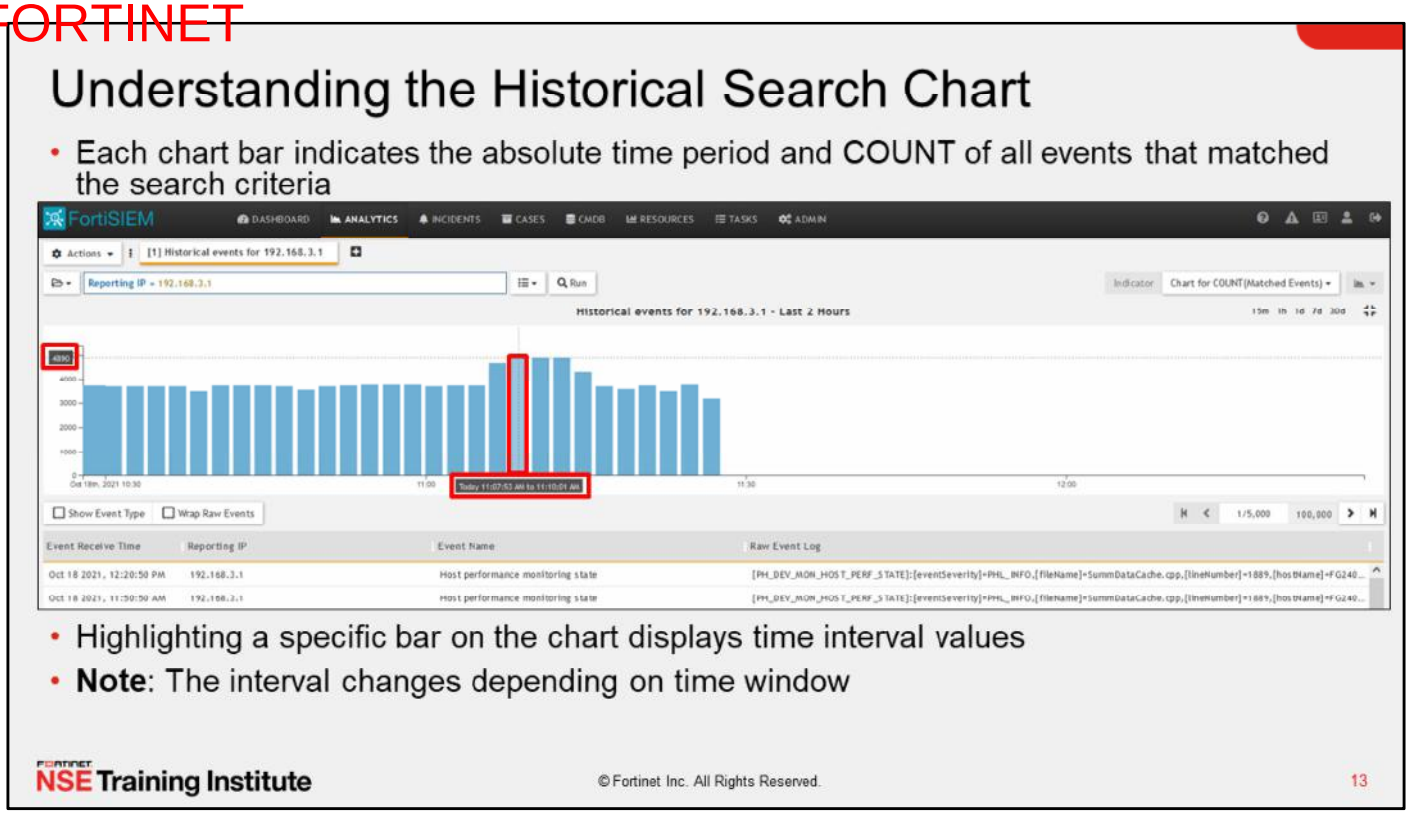
You can turn a real-time search into a historical search by selecting any of the time-related options.
- Relative: The query will run for a duration in the past, starting from the current time. Select the value and time scale in (**Minutes**/**Hours**/**Days**).
- Absolute: The query will run for a specific time window in the past.

Similarly, you can turn a historical search into a real-time search by selecting **Real Time** in **Filters**.

This populates either the historical or real-time search results with a same search criteria and display columns that you selected for the original search, and automatically runs a new search.

Vouchers & Dumps are Available | WhatsApp +201224560923

DO NOT REPRINT
© FORTINET
Brave-dumps.com



Each chart bar indicates the absolute time period and COUNT of all events matched the search criteria.

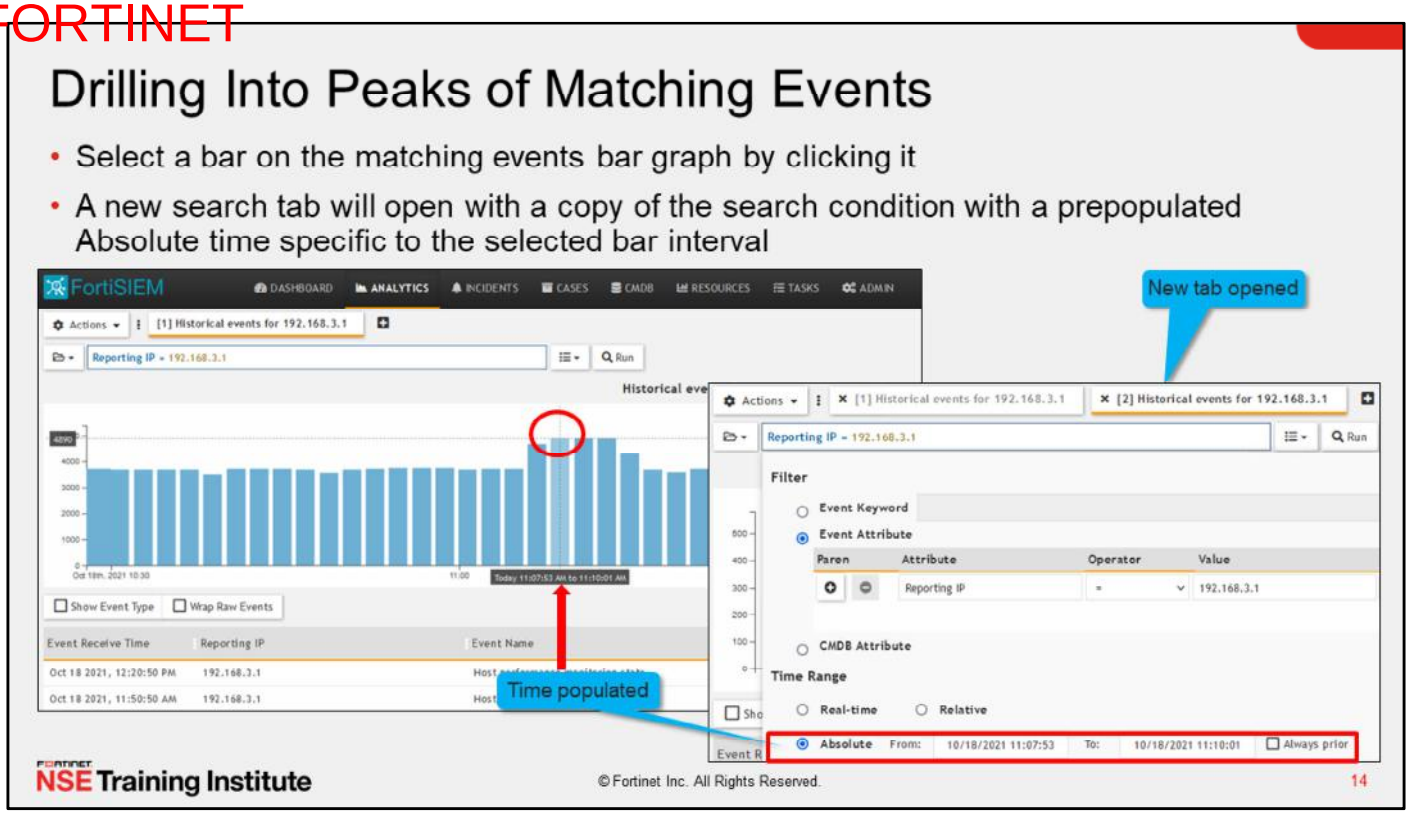
Because we can only plot so many points on the graph, the interval for which each point (or count) is calculated changes depending on the time scale you select. In the example shown on this slide, the graph is set to display the events that have occurred in the last two hours. For this time scale, the graph is divided into three minutes intervals. Each peak in the graph represents the count of events that occurred during a three minutes period.

If you highlight any bar on the chart, you'll see the absolute time range for that time interval.

If you search for a day or a week, the interval changes to accommodate the new time scale.

Vouchers & Dumps are Available | WhatsApp +201224560923

DO NOT REPRINT
© FORTINET
Brave-dumps.com



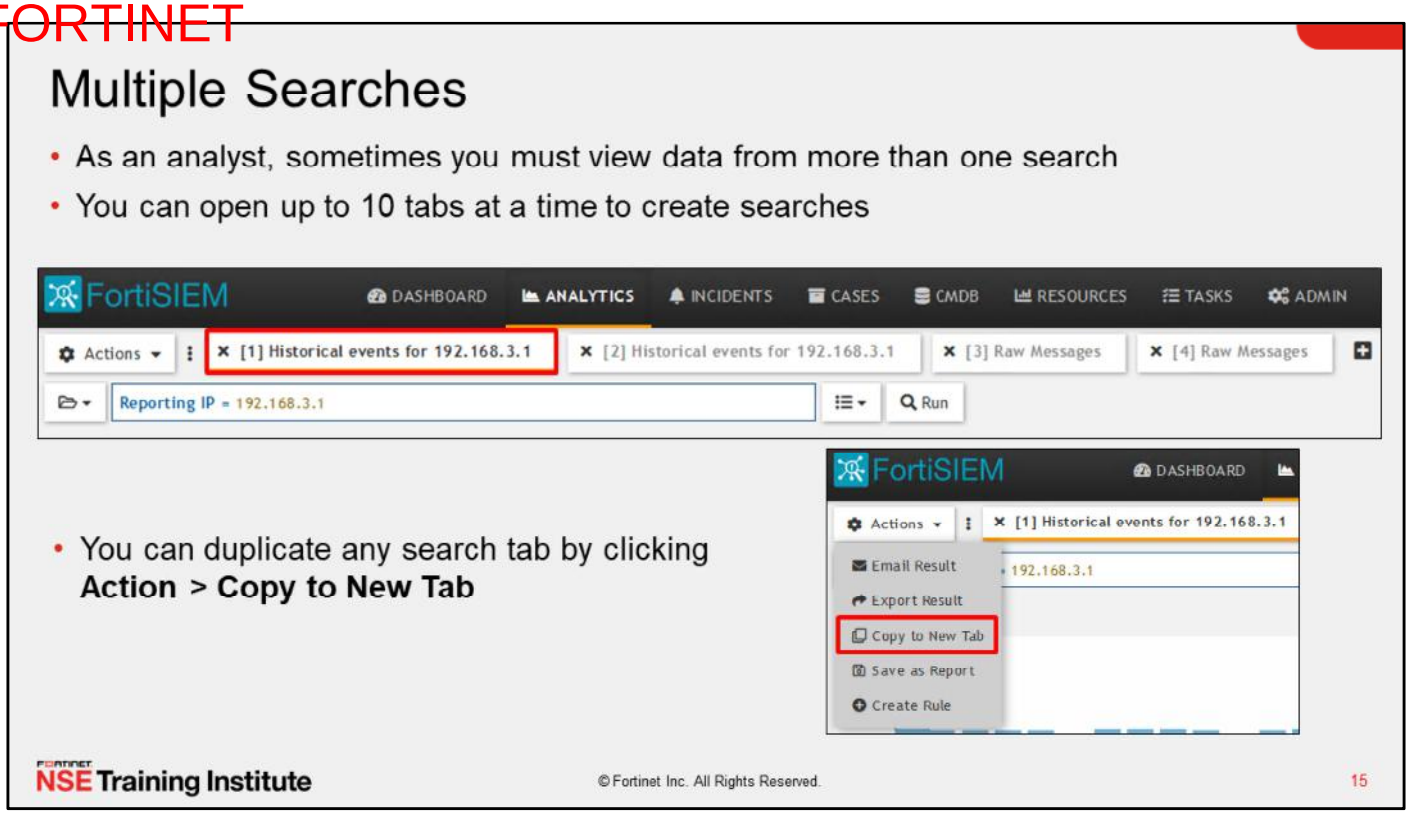
Let's say you want to drill into a specific event spike for a specific time period. If you select a peaked chart bar by clicking it, a new search tab will open automatically with the search time range changed to the absolute time range for the chart bar you selected.

This allows you to drill into only the events that formed that peak.

A count of events for the selected time period will be shown as well.

Vouchers & Dumps are Available | WhatsApp +201224560923

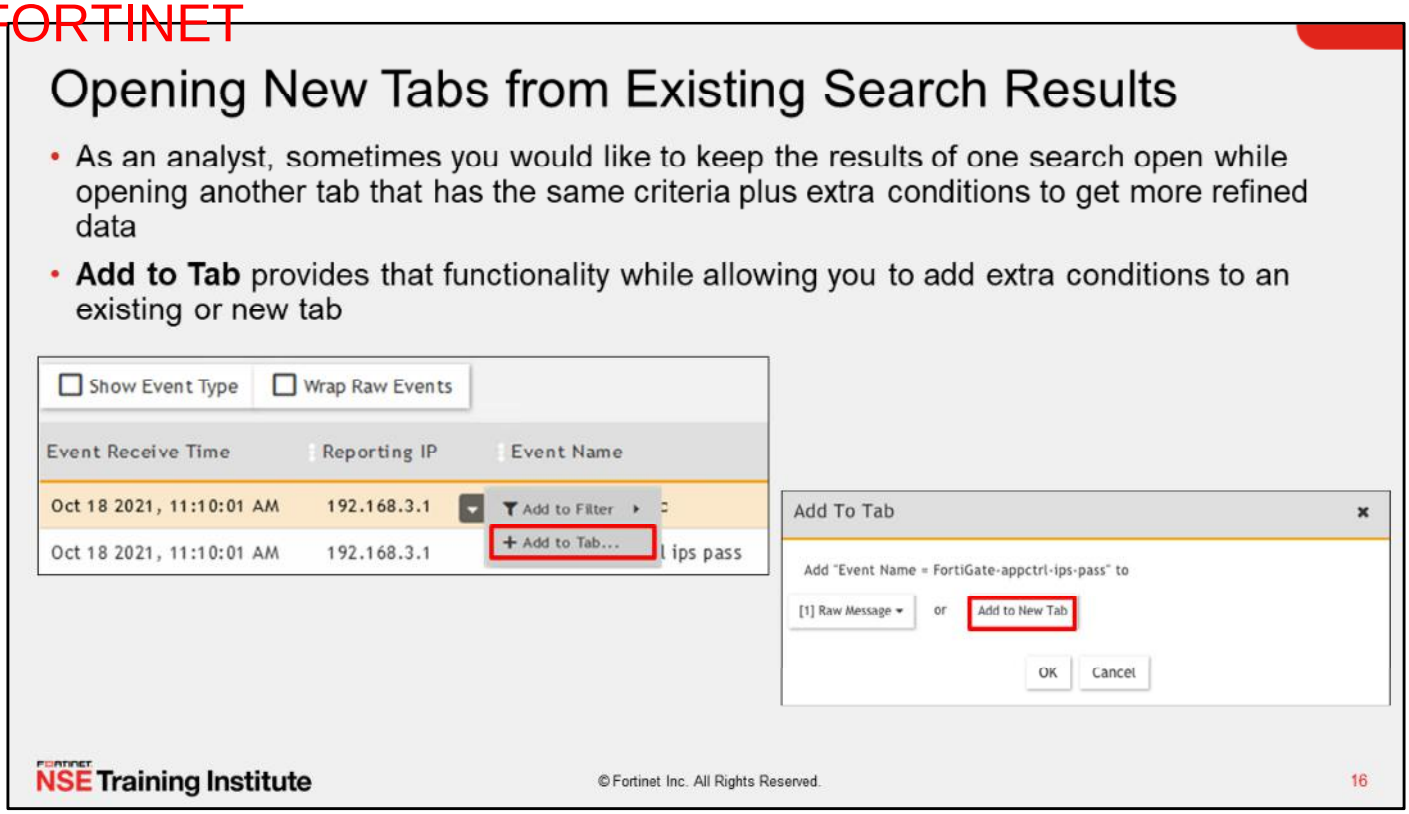
DO NOT REPRINT
© FORTINET
Brave-dumps.com



As an analyst, sometimes you must view data from more than one search. You can open up to 10 tabs at a time to create different searches. You can close any tab as needed, except the first tab.
You can duplicate search results on another tab by clicking **Copy to New Tab**.

Vouchers & Dumps are Available | WhatsApp +201224560923

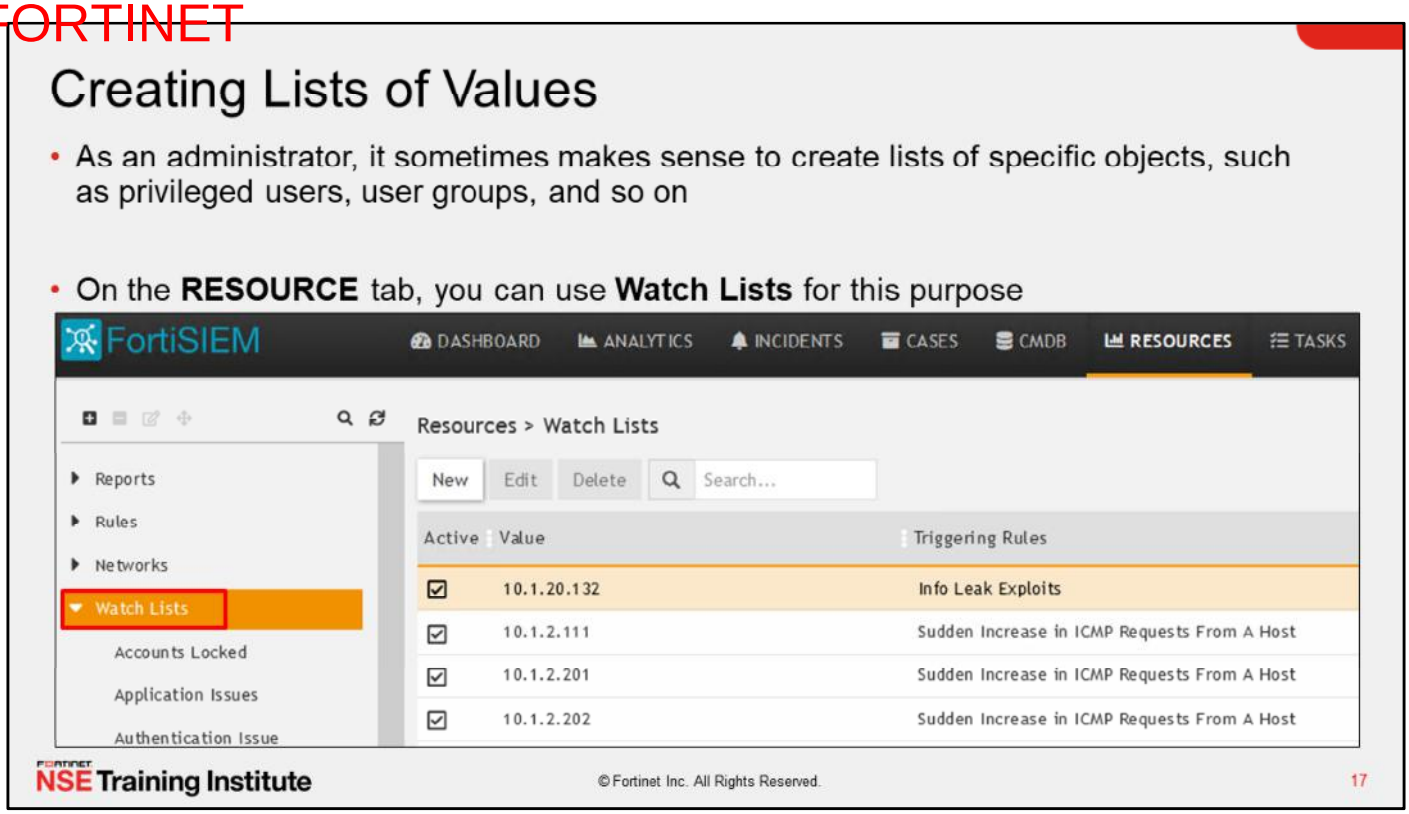
DO NOT REPRINT
© FORTINET
Brave-dumps.com



As an analyst, sometimes you want to keep the results of one search open while opening another tab that has the same criteria plus extra conditions to get more refined data. The **Add to Tab** feature provides that functionality, allowing you to add extra conditions to an existing or new tab.

Vouchers & Dumps are Available | WhatsApp +201224560923

DO NOT REPRINT
© FORTINET
Brave-dumps.com

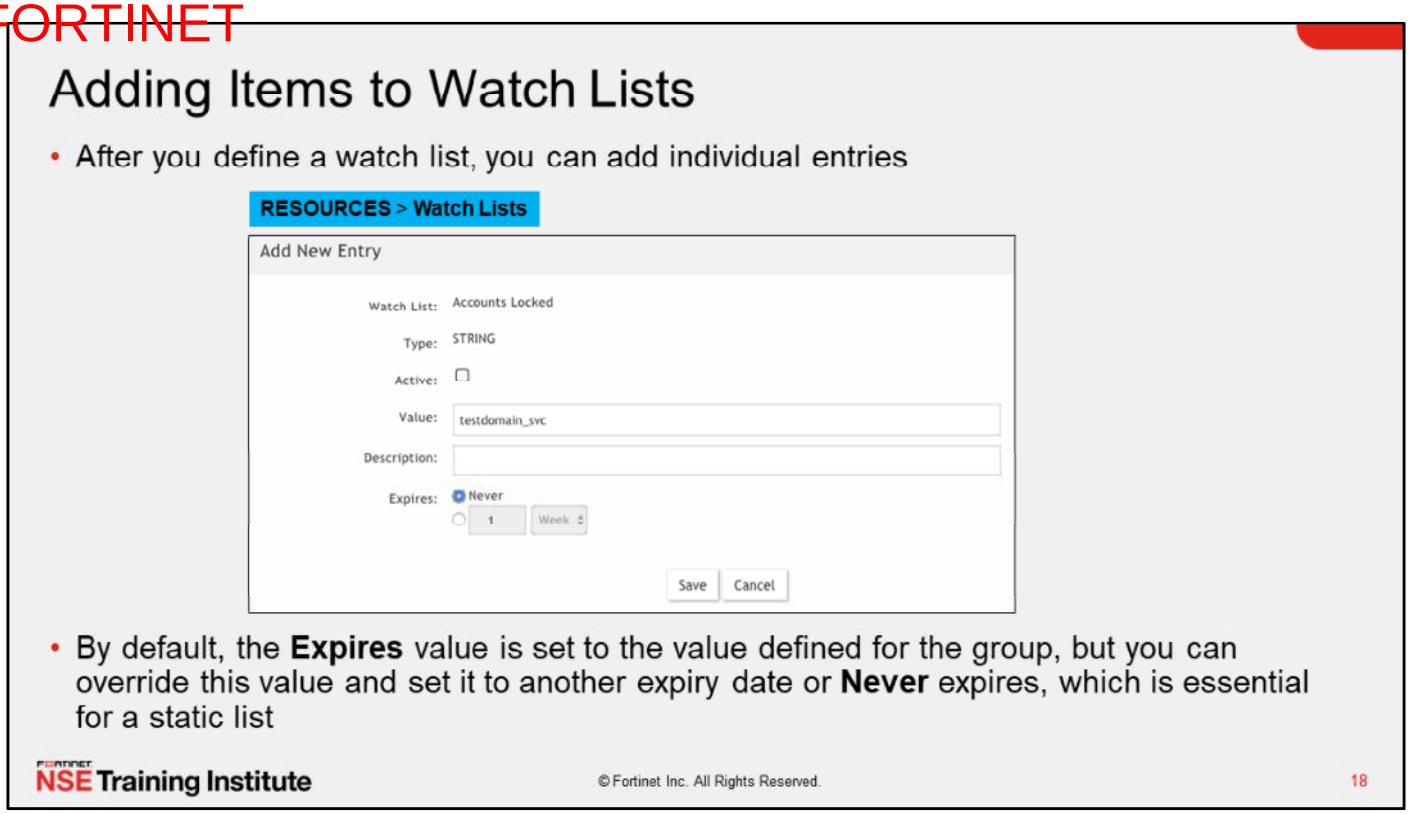


As an administrator, it sometimes makes sense to create lists of specific objects such as privileged users, user groups, denied ports, and so on. The CMDB has a watch list feature that you can use for this purpose.

When you create a new watch list, you must enter an expiry value. However, individual entries in the group take precedence over this value, and so can override it.

Vouchers & Dumps are Available | WhatsApp +201224560923

DO NOT REPRINT
© FORTINET
Brave-dumps.com

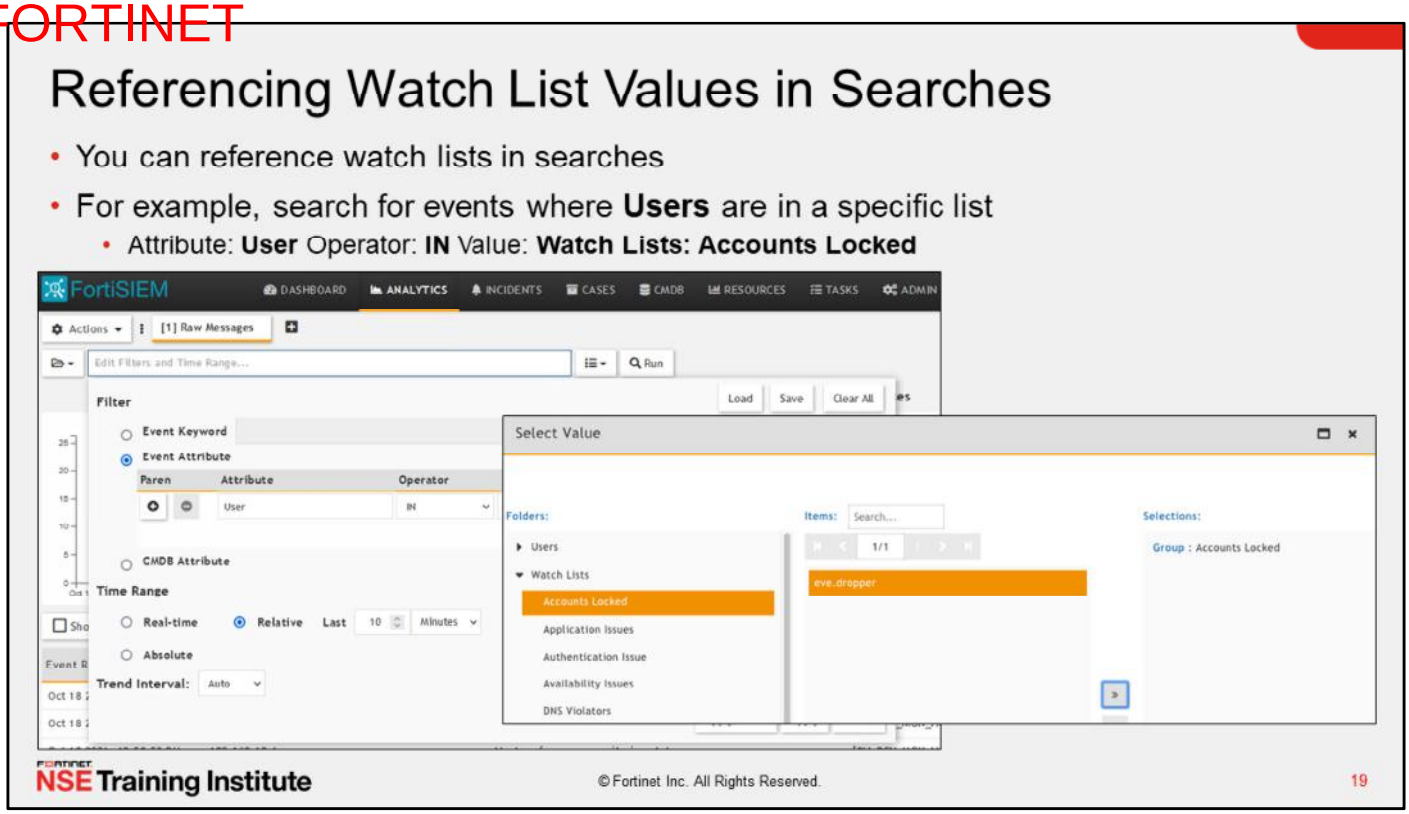


After you create a watch list, you can add individual items to it.

By default, the newly added item inherits its expiry date from the value defined in the group. But as was just mentioned, you can override the default value and set it to another expiry date, or even to **Never** expires, which is essential for static lists.

Vouchers & Dumps are Available | WhatsApp +201224560923

DO NOT REPRINT
© FORTINET
Brave-dumps.com



In searches, you can reference the watch lists you created. For example, if you created a watch list for **Accounts Locked** for service accounts, you can reference that watch list in a search.

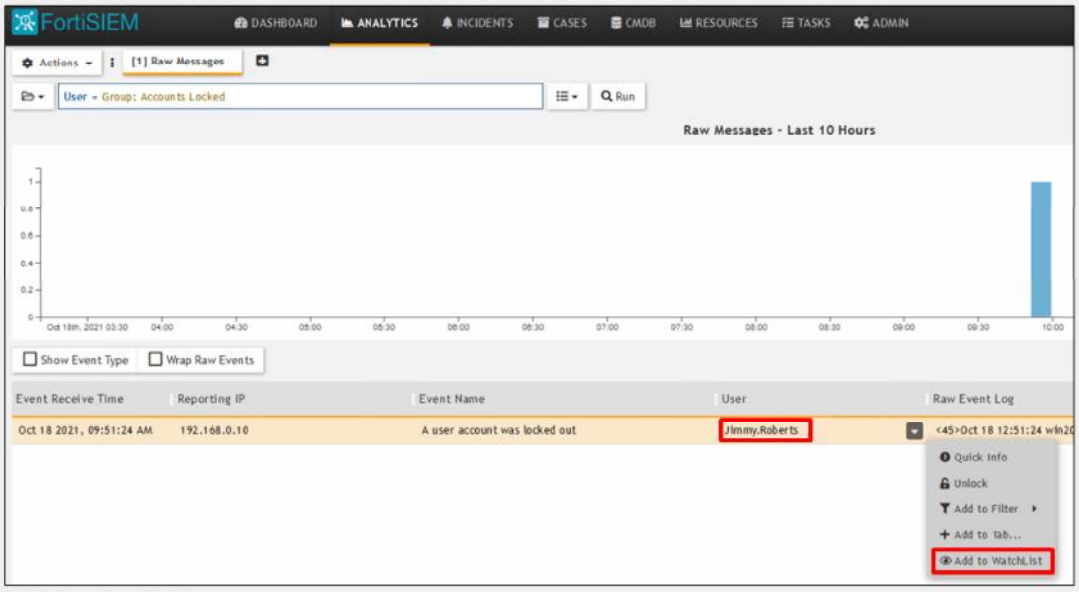
In a search condition, set the attribute to **User**, and use the operator **IN**. Then, in the CMDB, browse the watch lists, and then select the **Accounts Locked** group.

Vouchers & Dumps are Available | WhatsApp +201224560923

DO NOT REPRINT
© FORTINET
Brave-dumps.com

Adding to a Watch List from a Search

- From a search result field select **Add to WatchList**



NSE Training Institute

© Fortinet Inc. All Rights Reserved.

20

You can also add an attribute type to a watchlist from a search result. Select the attribute, then select **Add to WatchList** to add the object to the watchlist group.

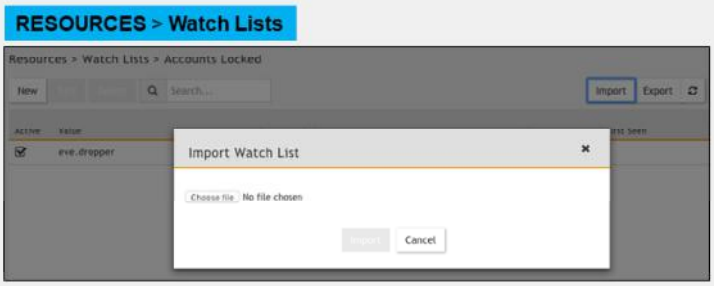
Vouchers & Dumps are Available | WhatsApp +201224560923

DO NOT REPRINT
© FORTINET
Brave-dumps.com

Importing Watch List Values

- You can import watch lists from a CSV file
- Create a CSV file and format your entries with the following three comma-separated fields:

```
#Watch List Group,Organization,Value
Service Accounts,Super,aosvc
Service Accounts,Super,uksvc
Service Accounts,Super,retailsvc
Service Accounts,Super,hqsvc
```



- In the enterprise version of FortiSIEM, the organization value is always **Super**
- Before you import, select the group you want to import into

NSE Training Institute

© Fortinet Inc. All Rights Reserved.

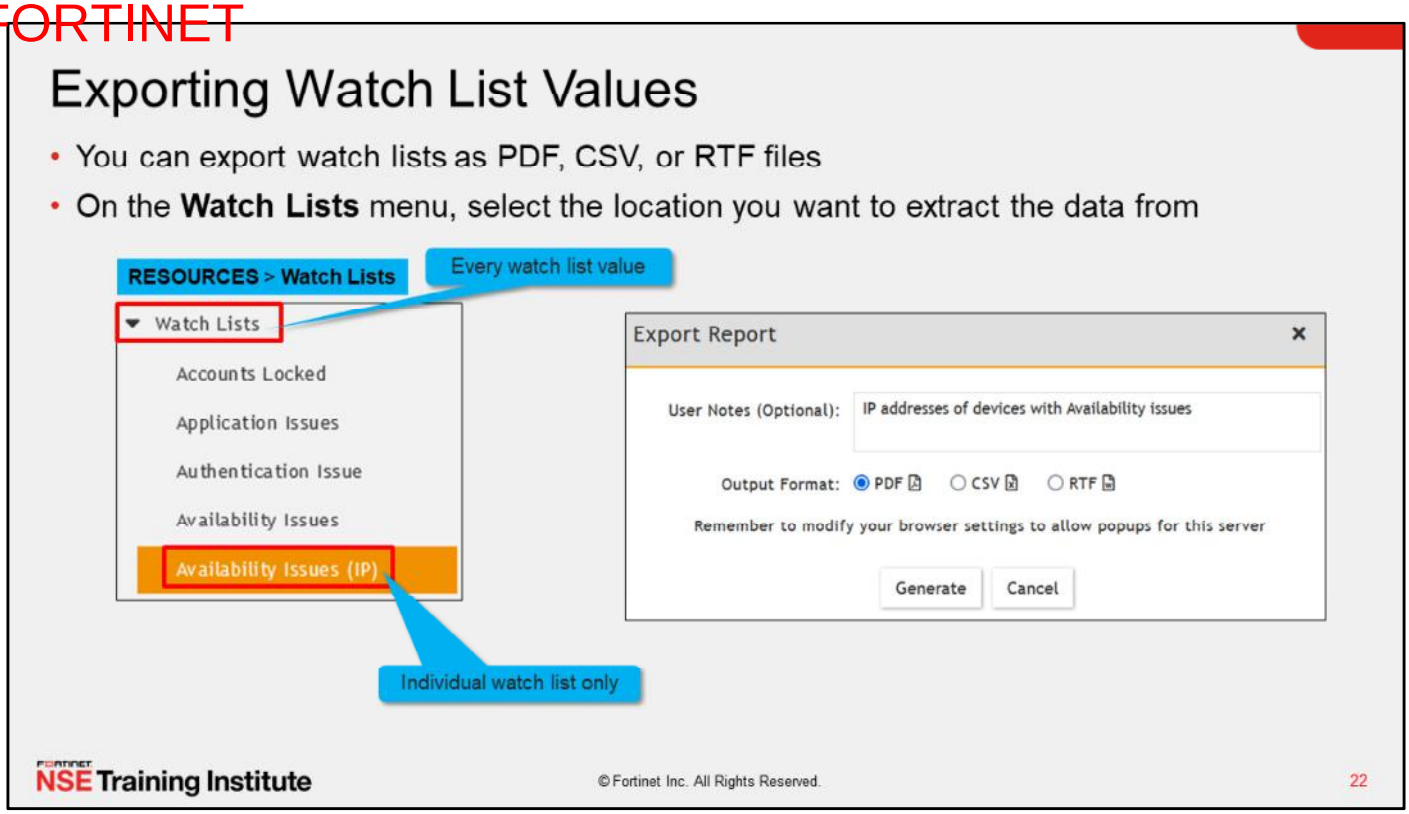
21

You can import watch lists from a CSV file. The CSV file must have the following format: watch list group, organization, and value, each separate by a comma.

Note that in the enterprise version of FortiSIEM, the organization value is always **Super**.

Vouchers & Dumps are Available | WhatsApp +201224560923

DO NOT REPRINT
© FORTINET
Brave-dumps.com

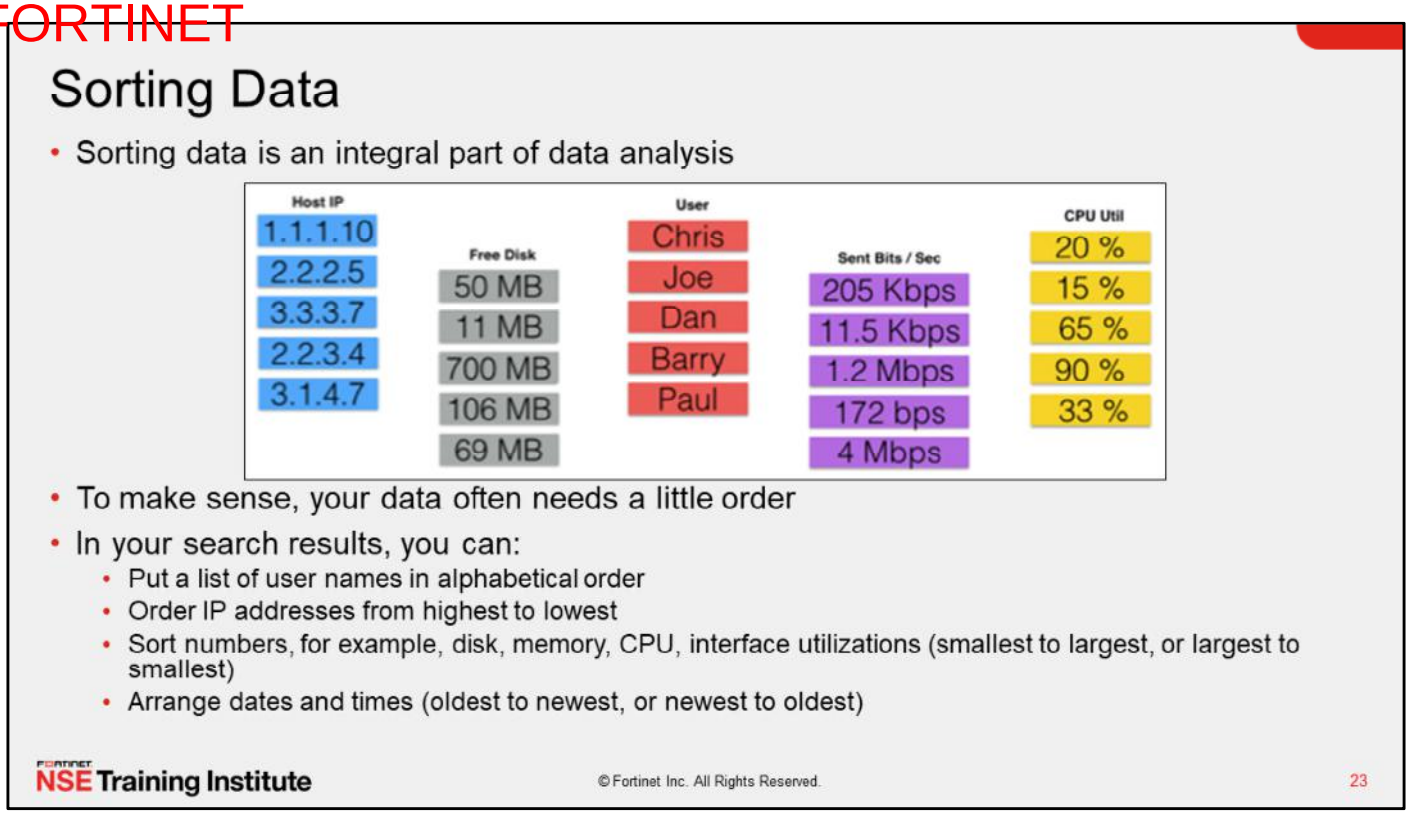


You can export watch lists as PDF, CSV, or RTF files.

The quantity of information that is exported depends on the location you select in the watch list tree. If you select the root of the watch list, you'll extract every value in every list, but if you select a specific watch list, you'll extract the values from only that watch list.

Vouchers & Dumps are Available | WhatsApp +201224560923

DO NOT REPRINT
© FORTINET
Brave-dumps.com



Sorting data is an integral part of data analysis.

Often, when you get a lot of results in your search, to make sense of it, you need to order your data.

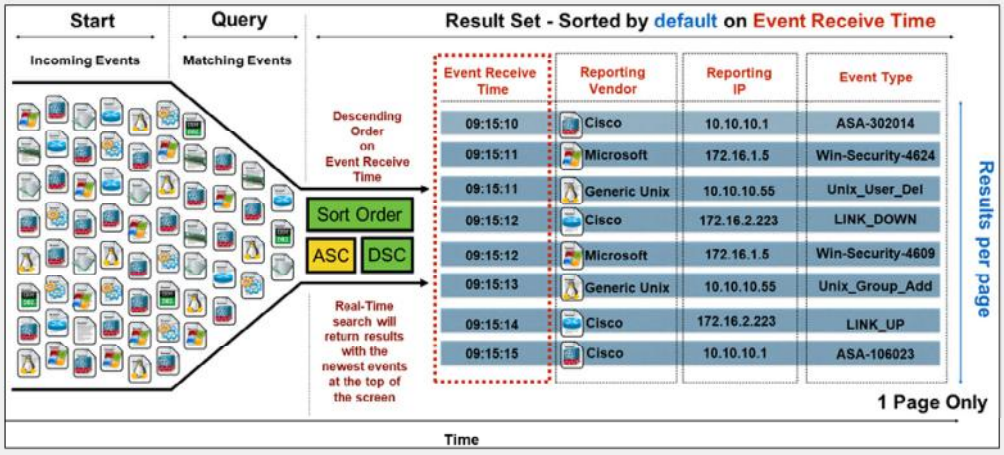
For example, you might want to:
- Put a list of user names in alphabetical order
- Order IP addresses from highest to lowest
- Sort numbers, for example, disk, memory, CPU, interface utilizations (smallest to largest, or largest to smallest)
- Arrange dates and times (oldest to newest, or newest to oldest)

Vouchers & Dumps are Available | WhatsApp +201224560923

DO NOT REPRINT
© FORTINET
Brave-dumps.com

Sorting in Real-Time Search

- Real-time default sorting order is descending



NSE Training Institute

© Fortinet Inc. All Rights Reserved.

24

When you do a real-time search, you may not realize that there are some default sorting orders.

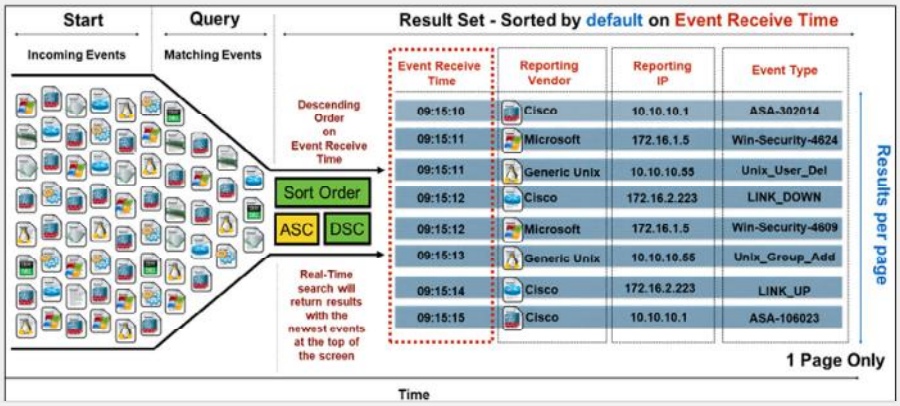
A real-time search displays the results on the screen, which is continually scrolling. This list is sorted by the event-received time. So, real-time searches return results with the newest events at the top of the screen.

Vouchers & Dumps are Available | WhatsApp +201224560923

DO NOT REPRINT
© FORTINET
Brave-dumps.com

Sorting in Historical Search

- Historical search default sorting order is ascending



- Historical search displays results on a page, and paginates the results

NSE Training Institute

© Fortinet Inc. All Rights Reserved.

25

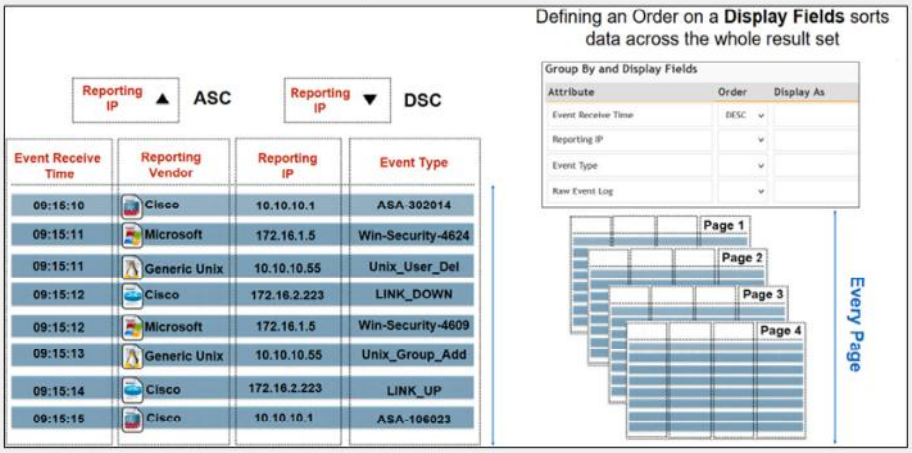
A historical search also has a default sorting order, and it displays results on a page. For longer results, a historical search paginates the results across many pages.

Vouchers & Dumps are Available | WhatsApp +201224560923

DO NOT REPRINT
© FORTINET
Brave-dumps.com

Display Column Sort Order

- Applies to historical searches only



- Order specified in display columns sorts the whole results set
- You can order results by one or more columns

NSE Training Institute

© Fortinet Inc. All Rights Reserved.

26

As was previously mentioned, by default, a historical search paginates the results across many pages. It is possible however, to sort the results for a particular column across the whole results set, that is, across all the pages. In the upper-right corner of the GUI, click the icon for **GroupBy and Display Fields** to open the display columns editor. In the **Order** option column, set the order for the column to ascending or descending. Run the search again to sort the whole result set.

Vouchers & Dumps are Available | WhatsApp +201224560923

DO NOT REPRINT
© FORTINET
Brave-dumps.com

Knowledge Check

1. Which type of search returns results with the newest events at the top of the screen?
   - ✓ A. Real-time search
   - B. Historical search

2. A FortiSIEM administrator wants to sort the results for a particular column across the whole results set; that is, across all the pages in ascending order. Under which option will they find the settings to set the order for columns across all pages?
   - A. Event Details
   - ✓ B. GroupBy and Display Fields

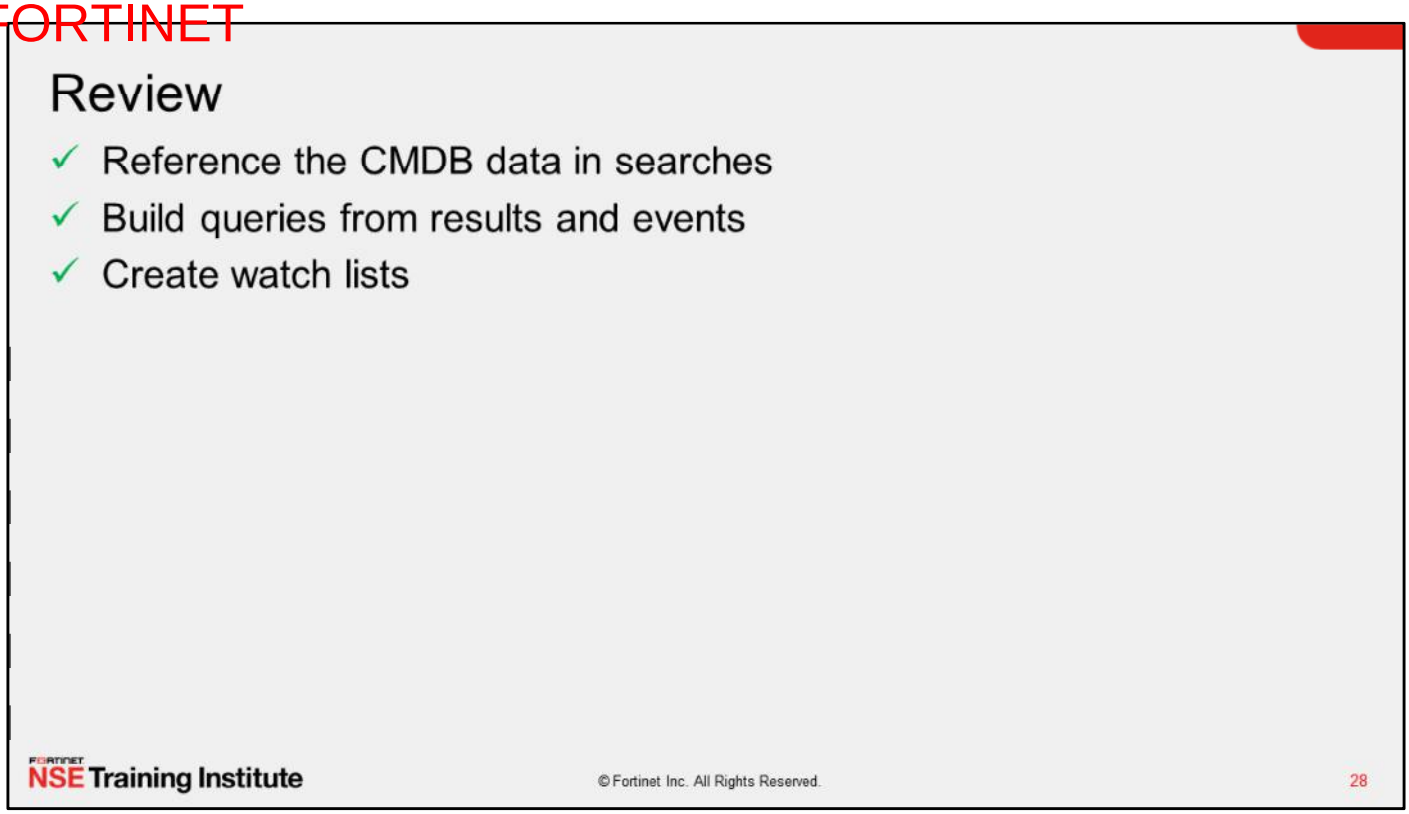
NSE Training Institute

© Fortinet Inc. All Rights Reserved.

27

Vouchers & Dumps are Available | WhatsApp +201224560923

DO NOT REPRINT
© FORTINET
Brave-dumps.com

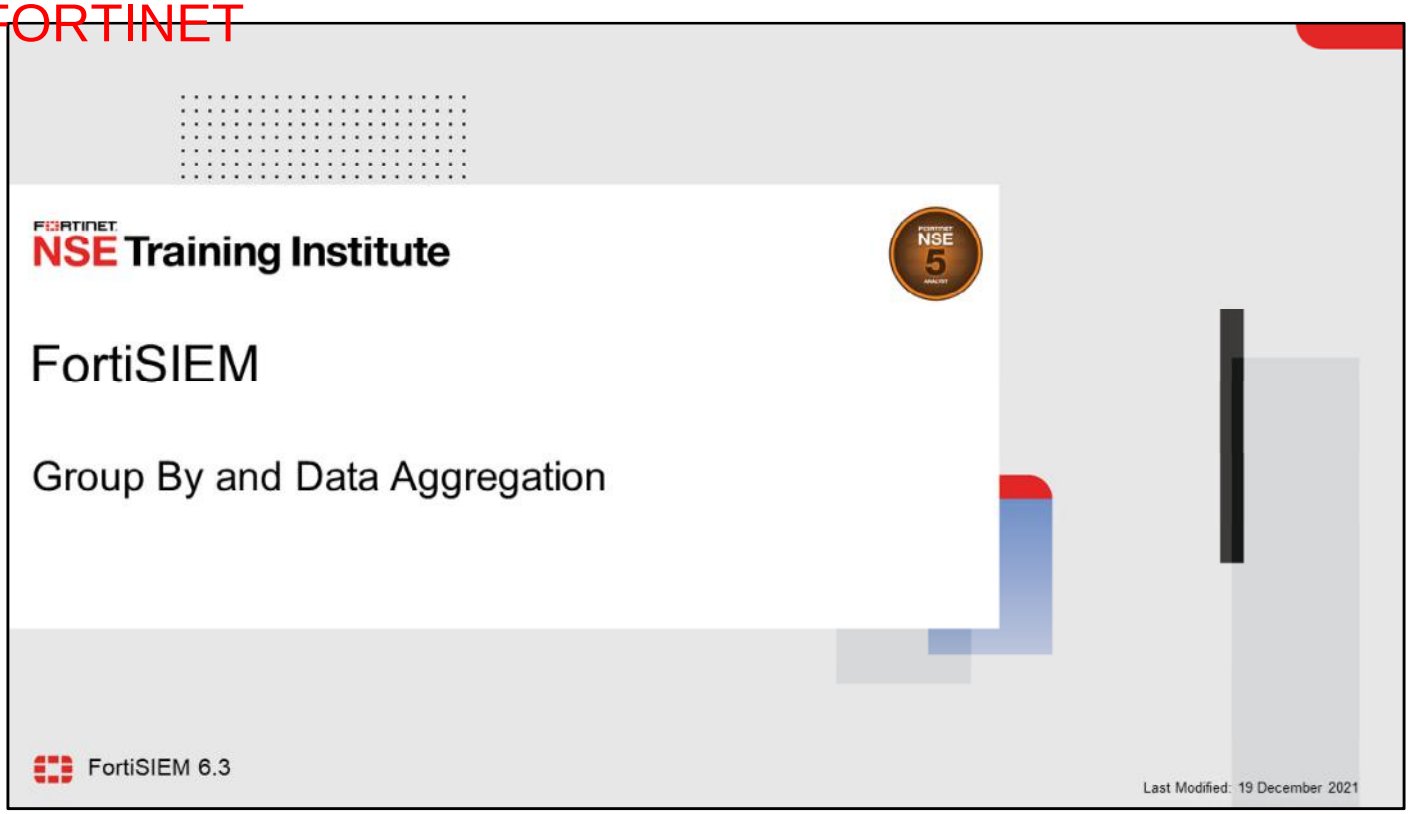


This slide shows the objectives that you covered in this lesson.

By mastering the objectives covered in this lesson, you learned how to reference the CMDB in search queries, as well as filter and sort the results.

Vouchers & Dumps are Available | WhatsApp +201224560923

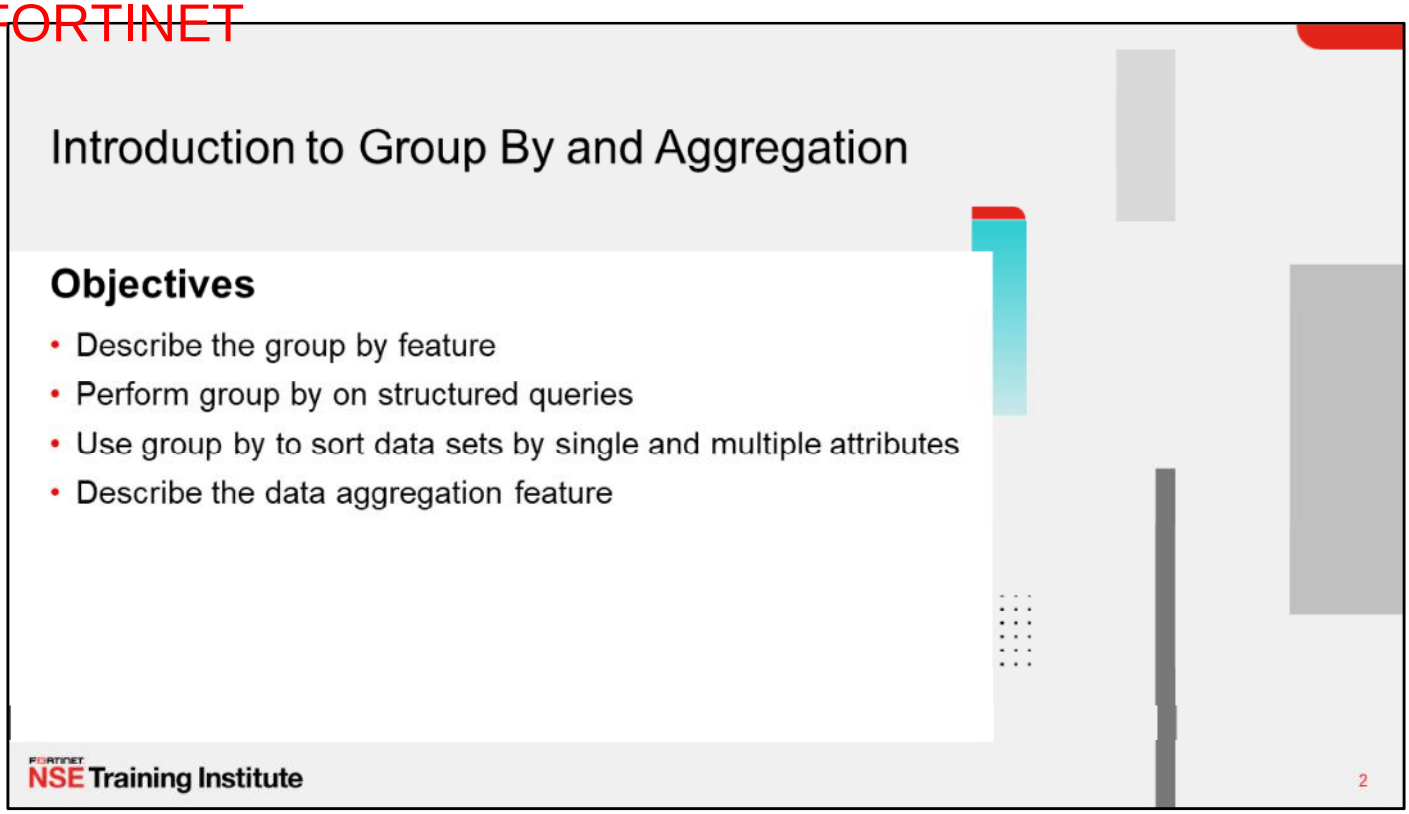
DO NOT REPRINT
© FORTINET
Brave-dumps.com



In this lesson, you will learn about the group by and data aggregation features of FortiSIEM.

Vouchers & Dumps are Available | WhatsApp +201224560923

DO NOT REPRINT
© FORTINET
Brave-dumps.com

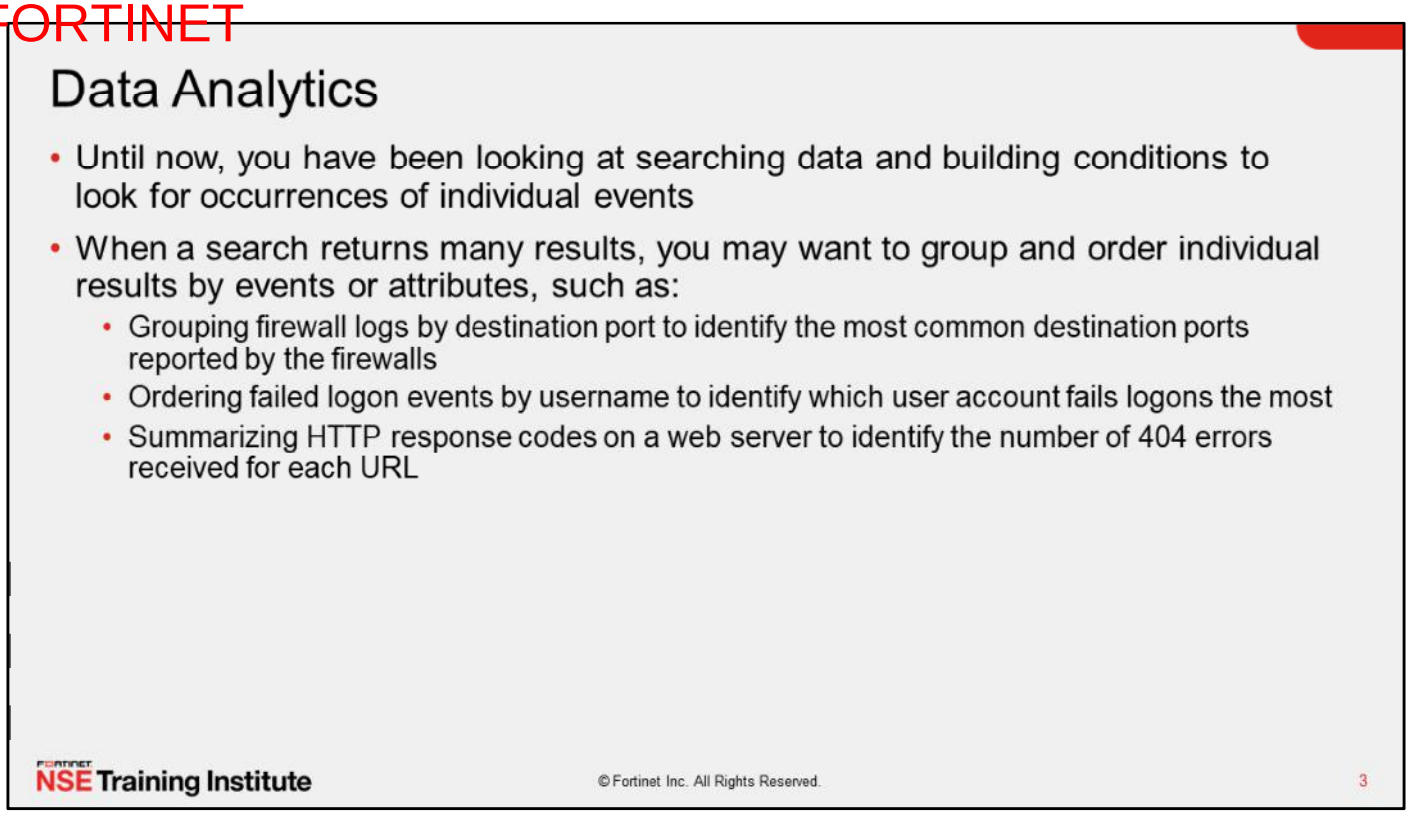


After completing this lesson, you should be able to achieve the objectives shown on this slide.

By demonstrating a competent understanding of the group by and aggregation features of FortiSIEM, you will be able to use them to sort and analyze data.

Vouchers & Dumps are Available | WhatsApp +201224560923

DO NOT REPRINT
© FORTINET
Brave-dumps.com



Until now, you have been looking at searching data and building conditions to look for occurrences of individual events.

When a search returns many results, you may want to group and order individual results, either by event or by attributes, such as

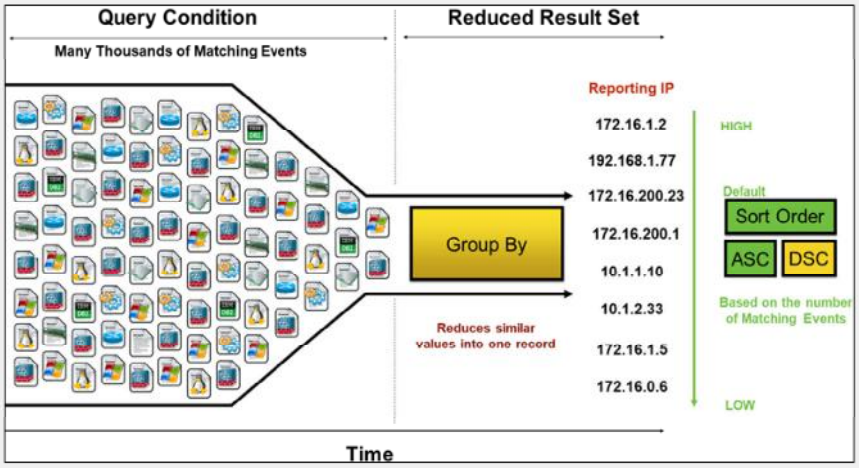
- Grouping firewall logs by destination port to identify the most common destination ports reported by the firewalls
- Ordering failed logon events by username to identify which user account fails logons the most
- Summarizing HTTP response codes on a web server to identify the number of 404 errors received for each URL

Vouchers & Dumps are Available | WhatsApp +201224560923

DO NOT REPRINT
© FORTINET
Brave-dumps.com

Introducing Group By

- Like SQL, the group by feature reduces similar values into one record



- You can group results can by one or more attributes

NSE Training Institute

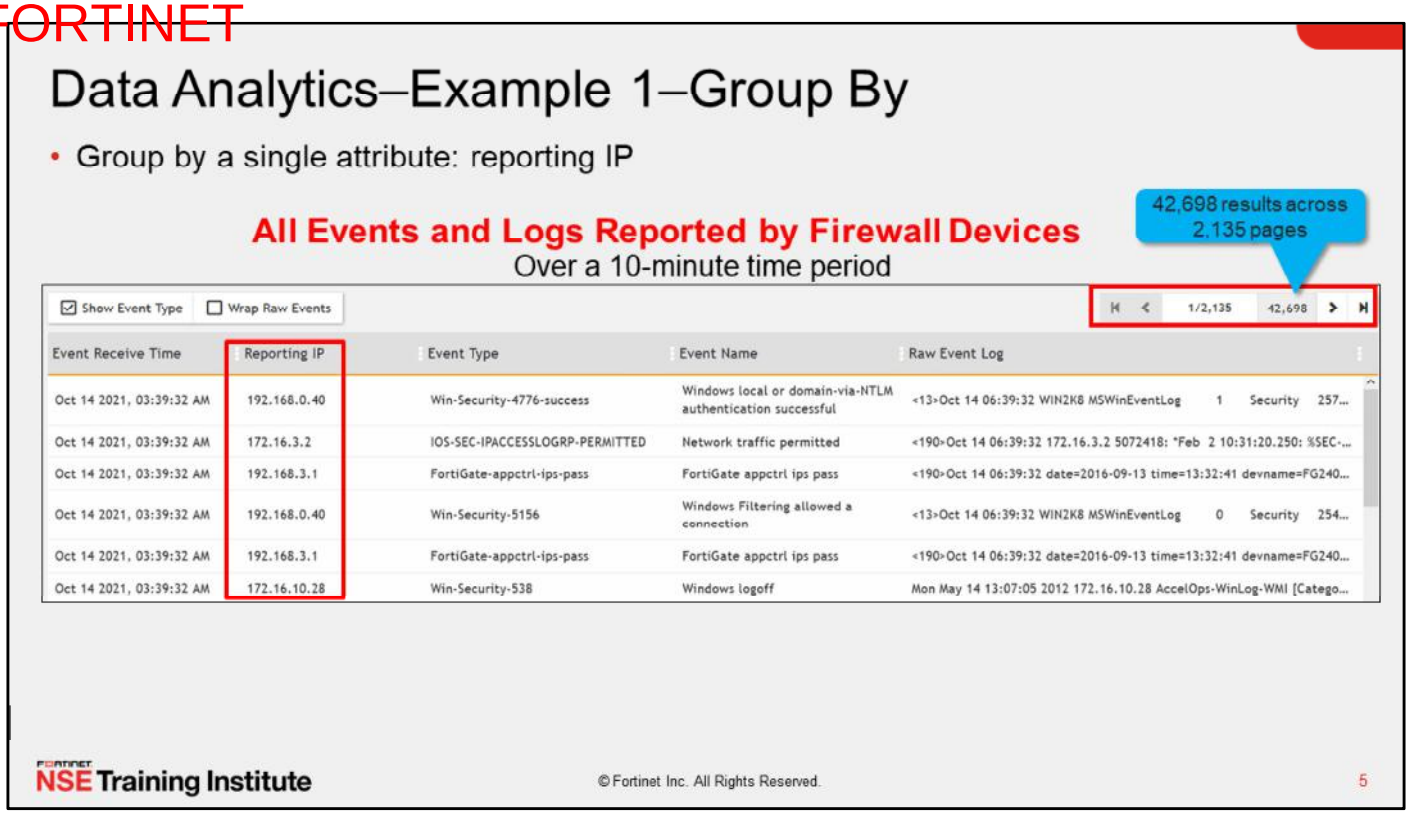
© Fortinet Inc. All Rights Reserved.

4

Like SQL, the group by feature reduces similar values into a single record. You can group the results by one or more attributes.

Vouchers & Dumps are Available | WhatsApp +201224560923

DO NOT REPRINT
© FORTINET
Brave-dumps.com



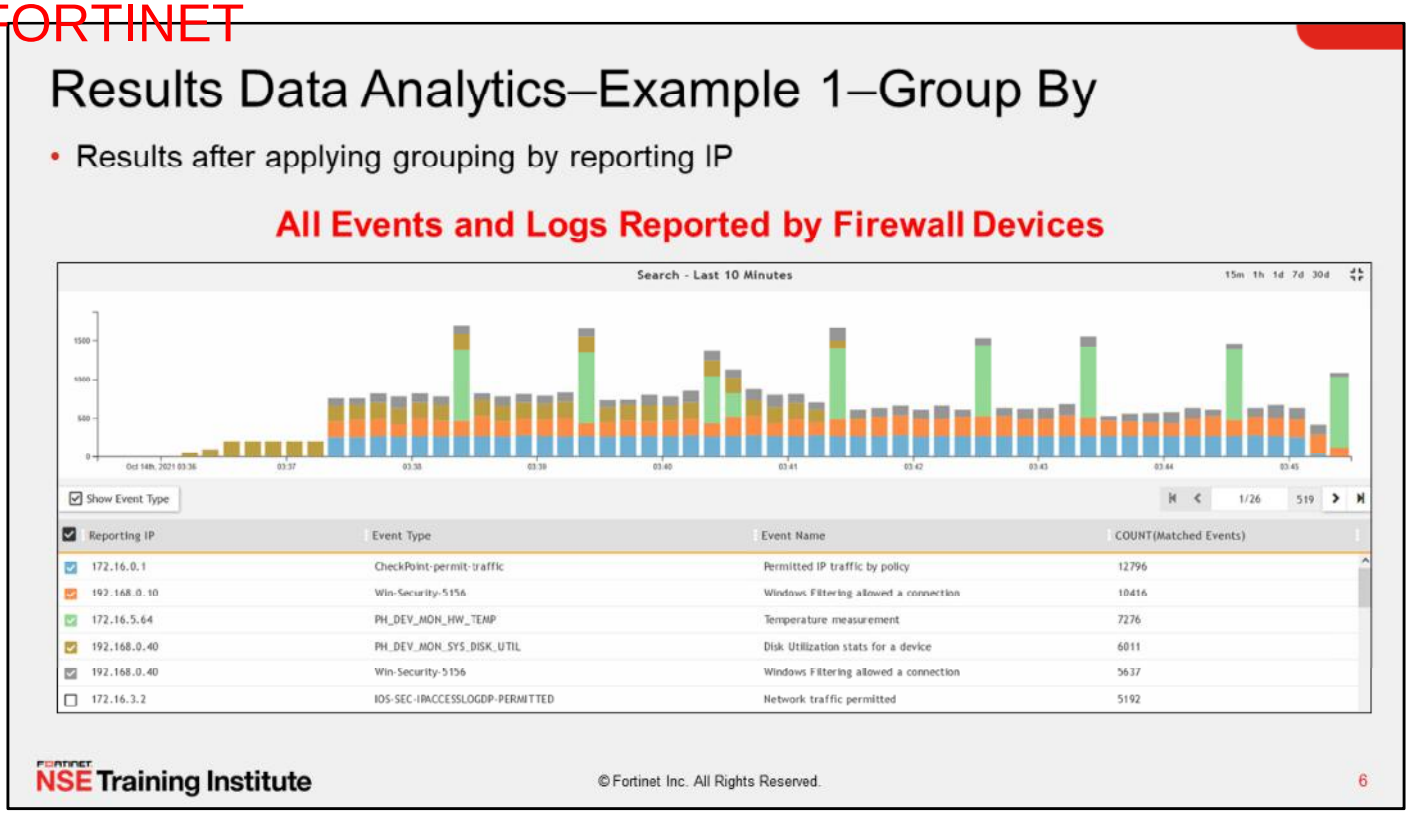
Now, you will look at a few examples.

Imagine that you've run a search and received hundreds of results spread across multiple pages. You may want to know which device reported the most events. The example shown on this slide has 42,698 results across 2,135 pages.

You could group the results by reporting IP and list them in ascending sort order. You would then get a single column of results where the reporting IP at the top of the list is the device that reported the most events, and the reporting IP at the bottom reported the least.

Vouchers & Dumps are Available | WhatsApp +201224560923

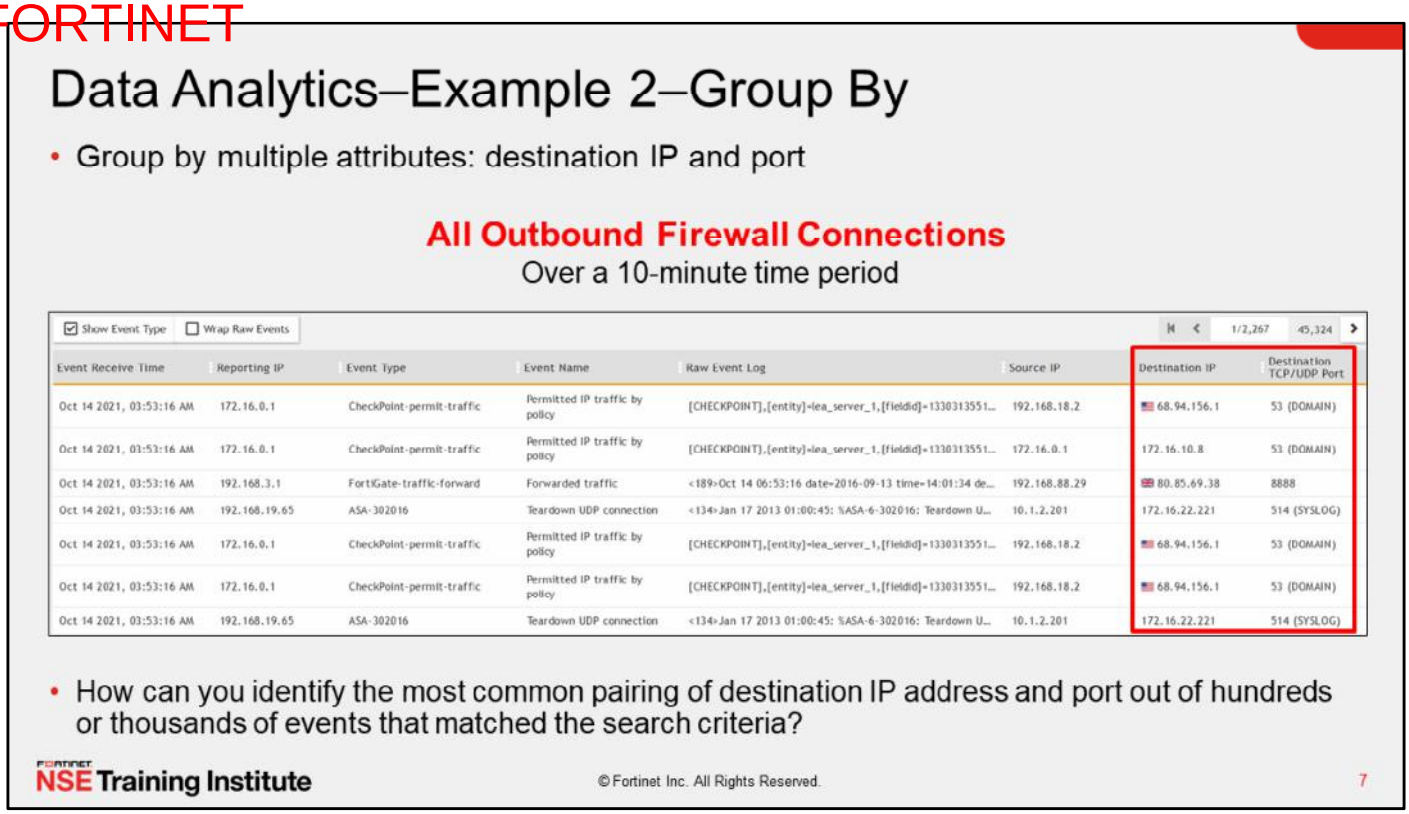
DO NOT REPRINT
© FORTINET
Brave-dumps.com



You can view the results after grouping them by a single attribute: reporting IP for all firewall devices. The reporting IP of the firewall with the most events is at the top of the list.

Vouchers & Dumps are Available | WhatsApp +201224560923

DO NOT REPRINT
© FORTINET
Brave-dumps.com

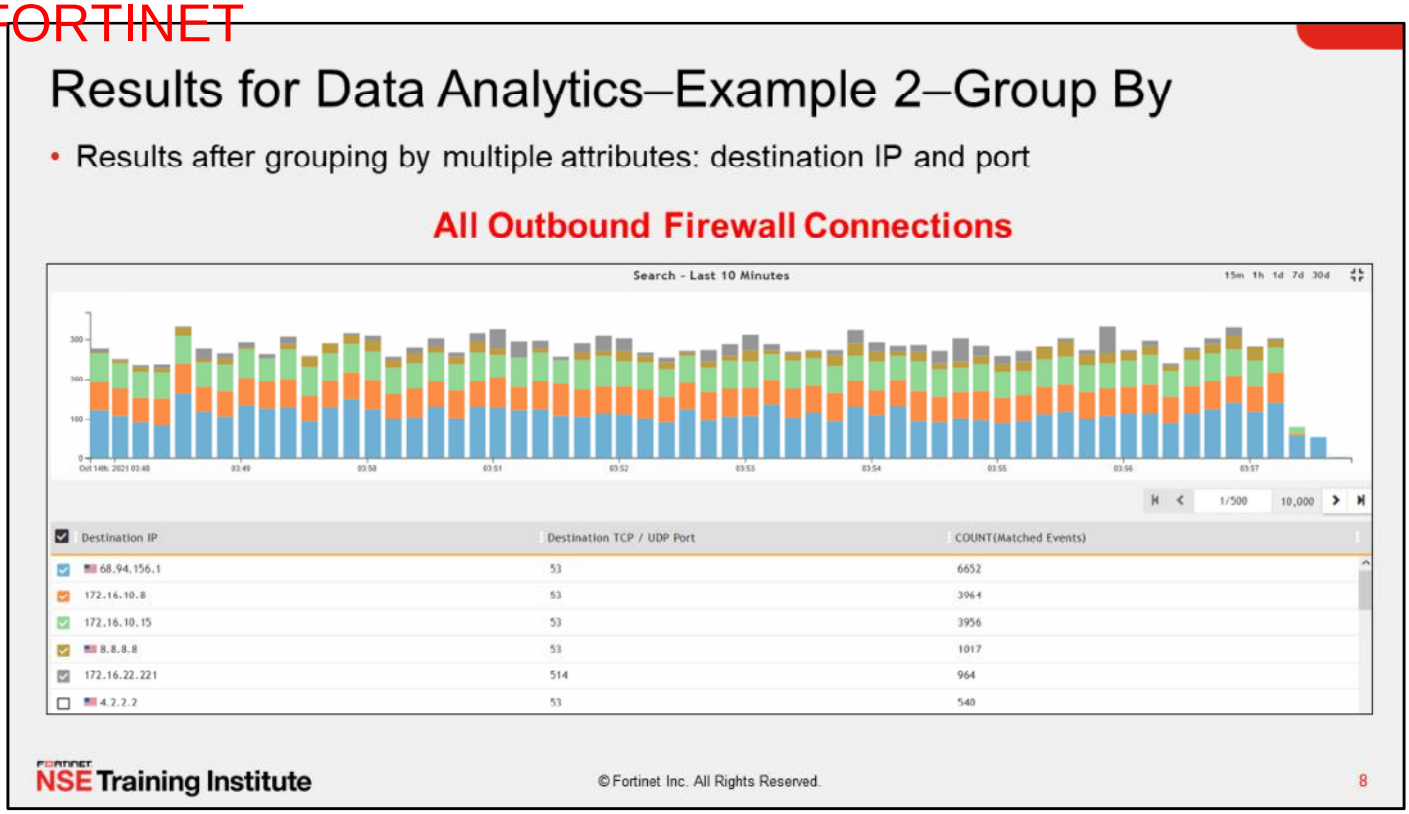


The example on this slide shows list of all firewall outbound connections over a 10-minute time period. There are hundreds of results over multiple pages. How do you identify the most common pairing of destination IP address and destination TCP/UDP port in these matching events?

To get the answer, you must group the results by multiple attributes, in this case, the destination IP address and the destination TCP/UDP port. You will get a single result, ordered from the highest reported pairing of destination IP address and port to the lowest reported pairing.

Vouchers & Dumps are Available | WhatsApp +201224560923

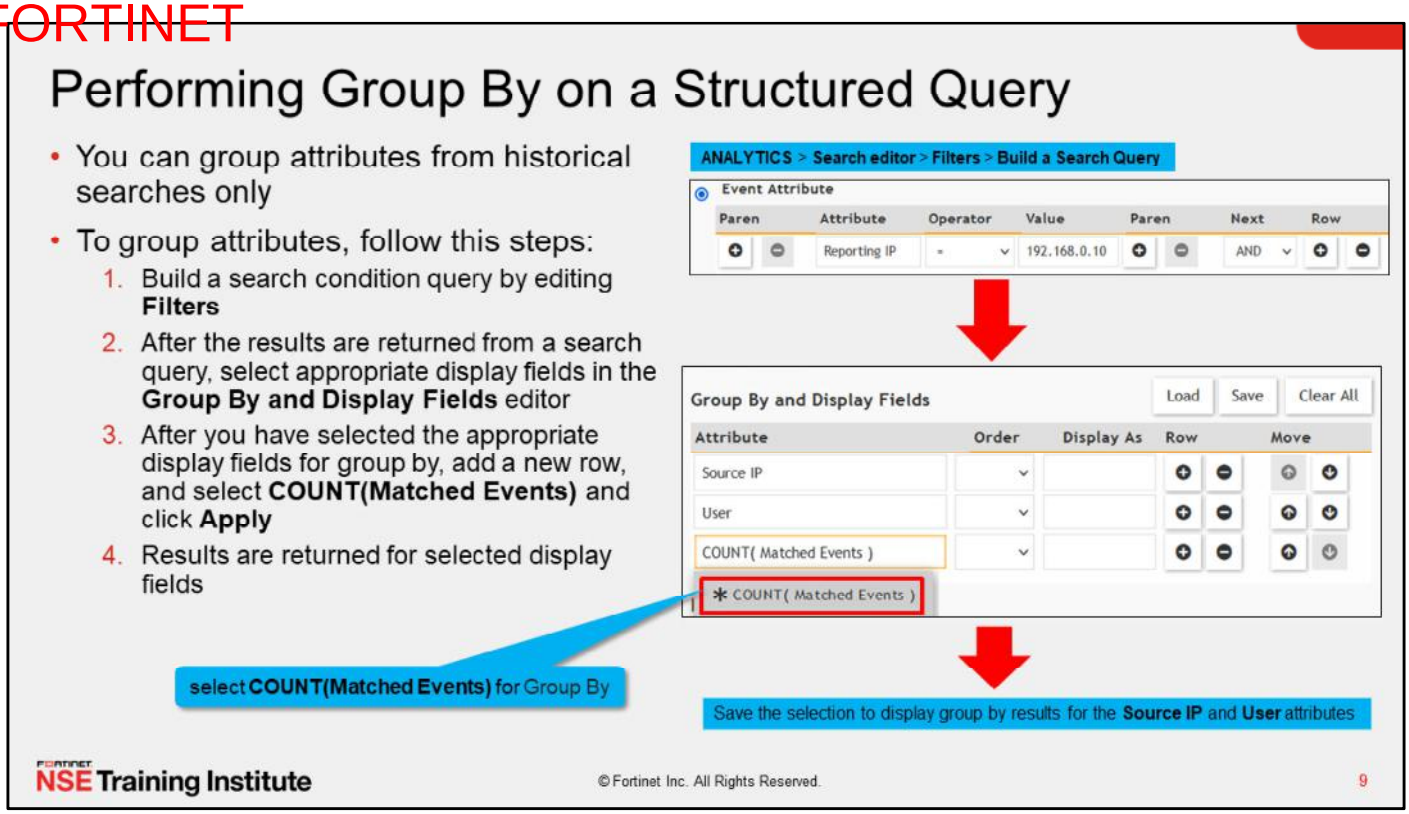
DO NOT REPRINT
© FORTINET
Brave-dumps.com



To get the answer, you must group the results by multiple attributes, in this case, the destination IP address and the destination TCP/UDP port. You will get a single result, ordered from the highest reported pairing of destination IP address and port to the lowest reported pairing.

Vouchers & Dumps are Available | WhatsApp +201224560923

DO NOT REPRINT Brave-dumps.com
© FORTINET

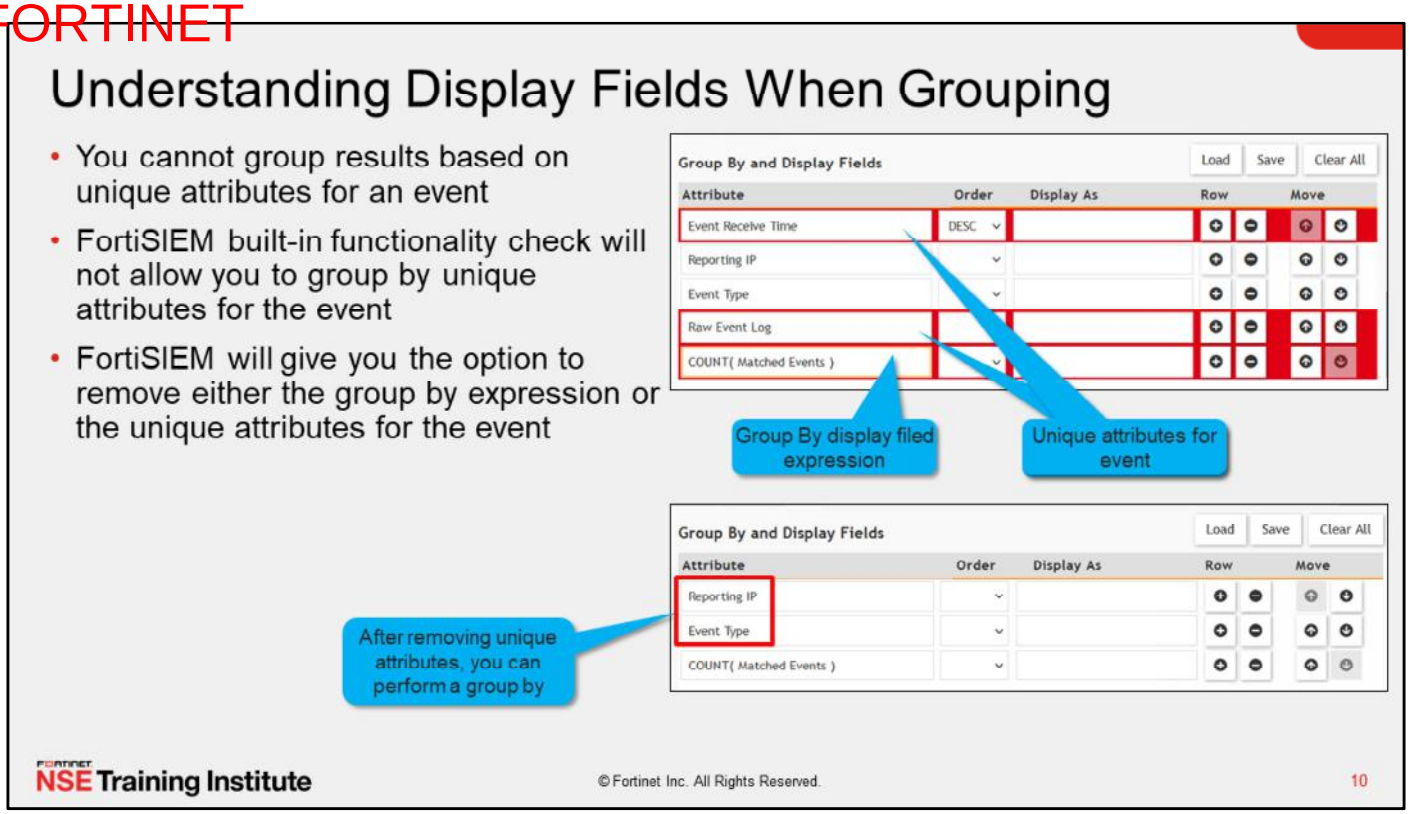


You can apply Group By to historical searches only.
Use the following steps to group attributes:

1. Build a search condition query by editing **Filters**.
2. After the results are returned from a search query, select appropriate display fields in the **Group By and Display Fields** editor.
3. After you have selected the appropriate display fields for group by, add a new row, and select **COUNT(Matched Events)** and click **Apply**.
4. Results are returned for selected display fields.

Vouchers & Dumps are Available | WhatsApp +201224560923

DO NOT REPRINT
© FORTINET
Brave-dumps.com



You cannot group unique attributes for an event.

The FortiSIEM built-in functionality check will not allow you to group by unique attributes for the event. In the example shown on the slide, the user tried to group by the default **Group By and Display Fields** attributes which includes **Event Receive Time**, **Reporting IP**, **Event Type**, and **Raw Event Log**.

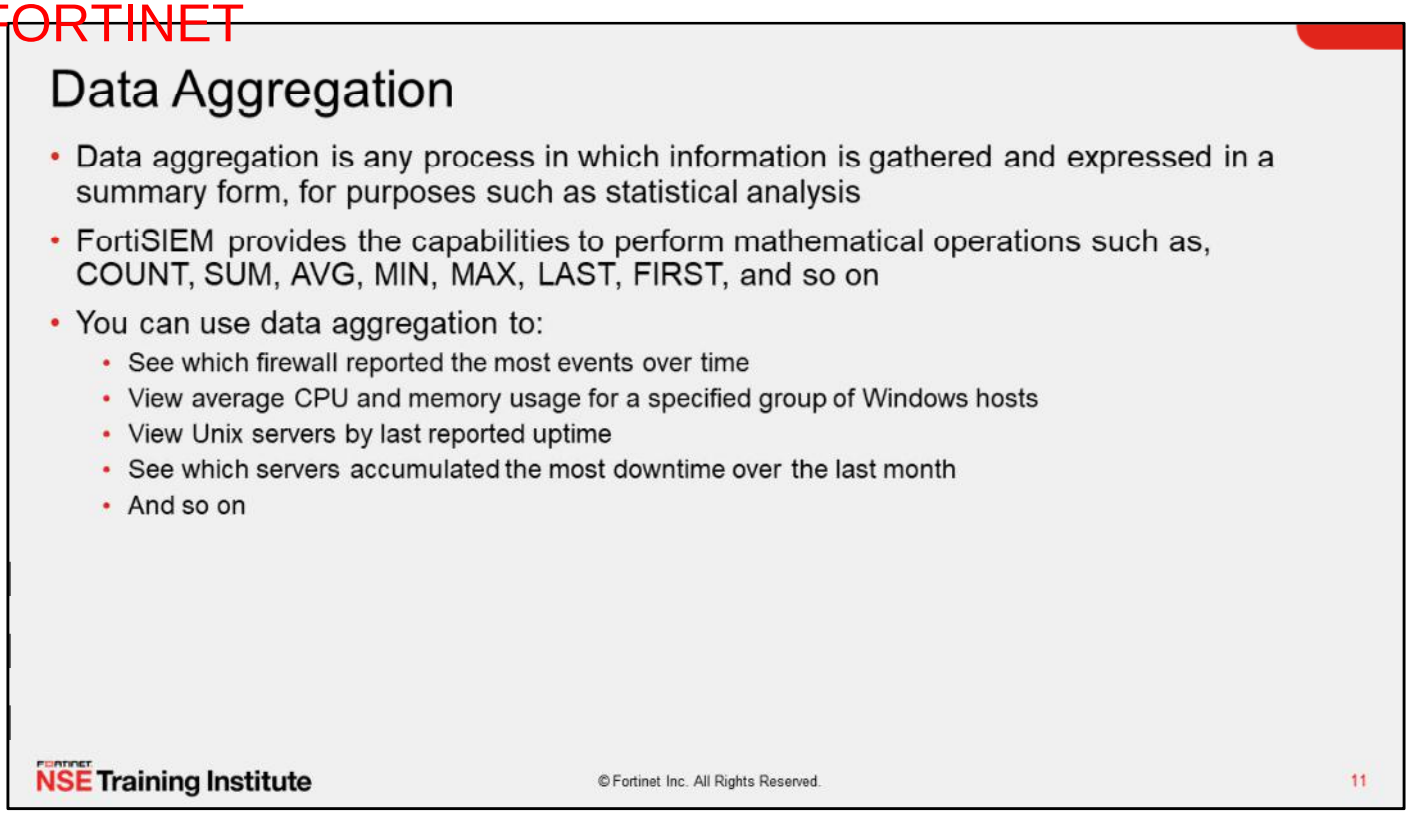
In the example shown on this slide, **Event Receive Time** and **Raw Event Log** are unique values of an event, which means every event will have a different time. This means that is not possible to group events by the **Event Receive Time** attribute. FortiSIEM detects this anomaly and highlights those attributes in red.

FortiSIEM will give you the option to either remove the **COUNT** expression for group by or remove unique attributes for the event, in this case, **Event Receive Time** and **Raw Event Log**.

After removing the rows for the unique attributes **Event Receive Time** and **Raw Event Log**, FortiSIEM allows you to group by attributes **Reporting IP** and **Event Type** by using a **COUNT** expression.

Vouchers & Dumps are Available | WhatsApp +201224560923

DO NOT REPRINT
© FORTINET
Brave-dumps.com



Data aggregation is any process in which information is gathered and expressed in a summary form, for purposes such as statistical analysis.

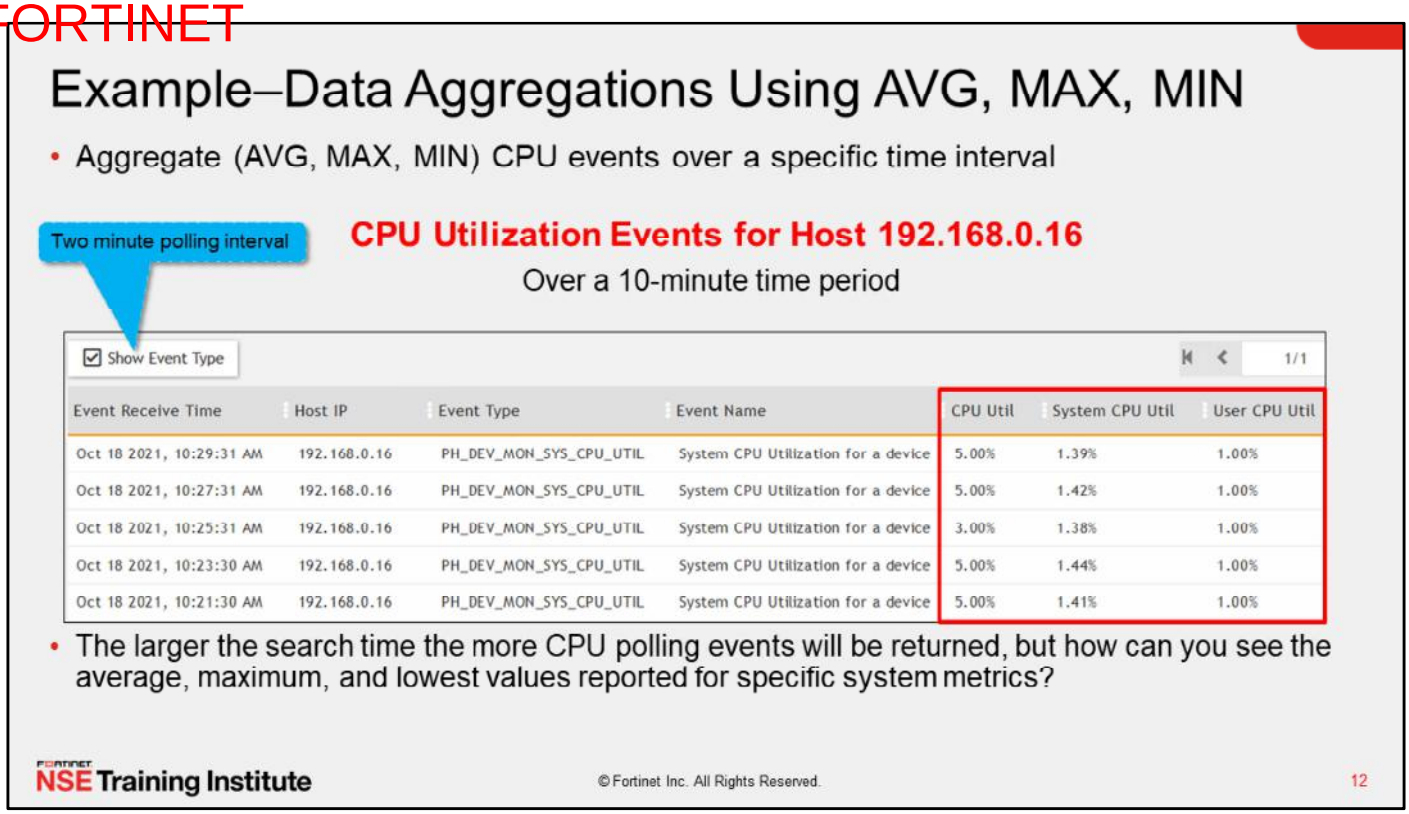
FortiSIEM provides the capabilities to perform mathematical operations such as COUNT, SUM, AVG, MIN, MAX, LAST, FIRST, and so on.

You can use data aggregation to:

- See which firewall reported the most events over time
- View average CPU and memory usage for a specified group of Windows hosts
- View Unix servers by last reported uptime
- See which servers accumulated the most downtime over the last month
- And so on

Vouchers & Dumps are Available | WhatsApp +201224560923

DO NOT REPRINT
© FORTINET
Brave-dumps.com

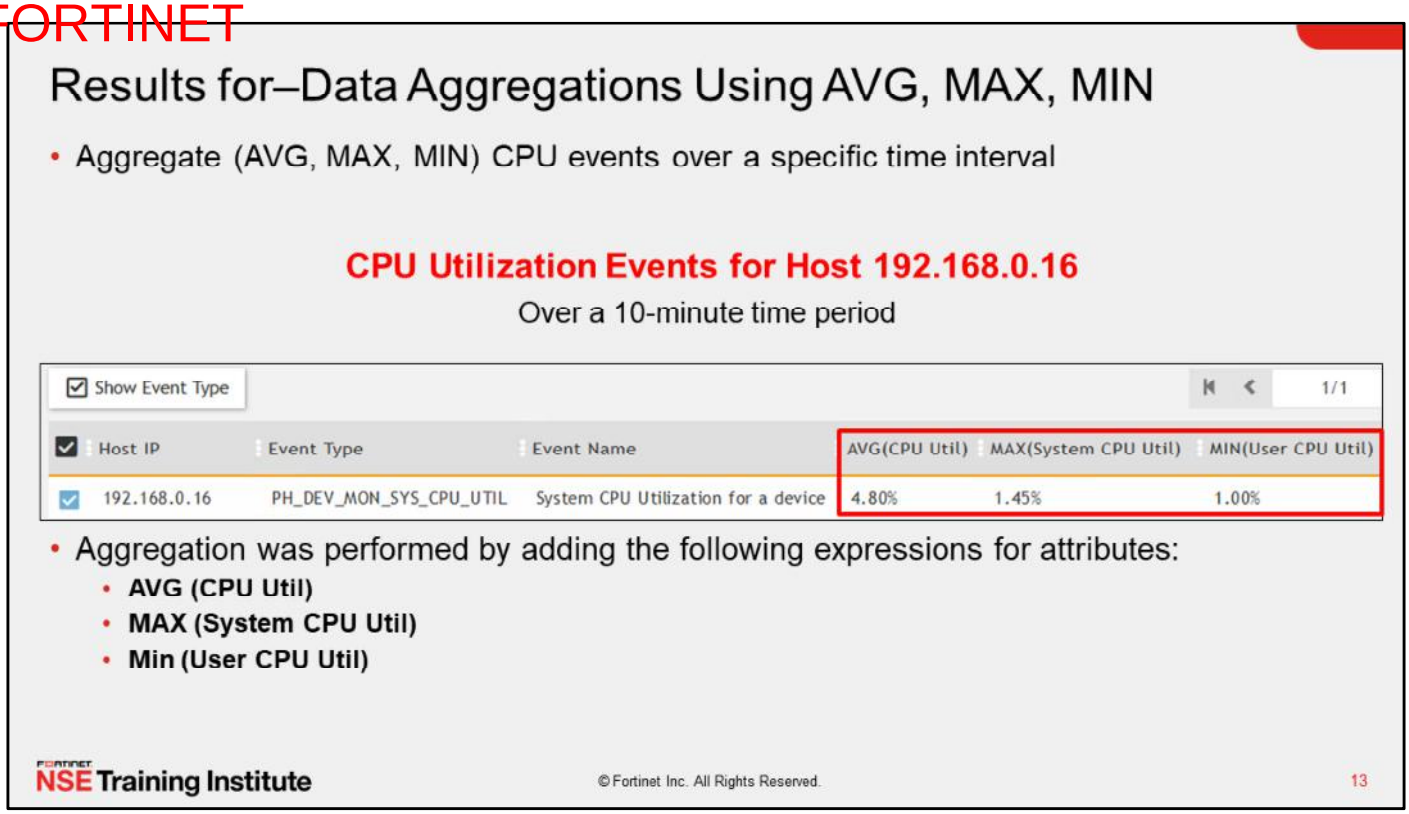


Now, you will look at an example that involves determining average, maximum, and minimum values for specific system metrics. In the example shown on this slide, you have a series of events with performance metrics. The events are being polled every three minutes, and the values for each event were taken when the event was polled. This information, as it is, is not very useful. So how can you see the average, maximum, and lowest values reported for specific system metrics?

Set up a structured query for the host IP over a 10-minute period, and then, in the **Group By and Display Fields** section, select the attribute **Host IP** and add aggregation function expressions **AVG**, **MAX**, and **MIN** for **CPU**-related attributes.

Vouchers & Dumps are Available | WhatsApp +201224560923

DO NOT REPRINT
© FORTINET
Brave-dumps.com

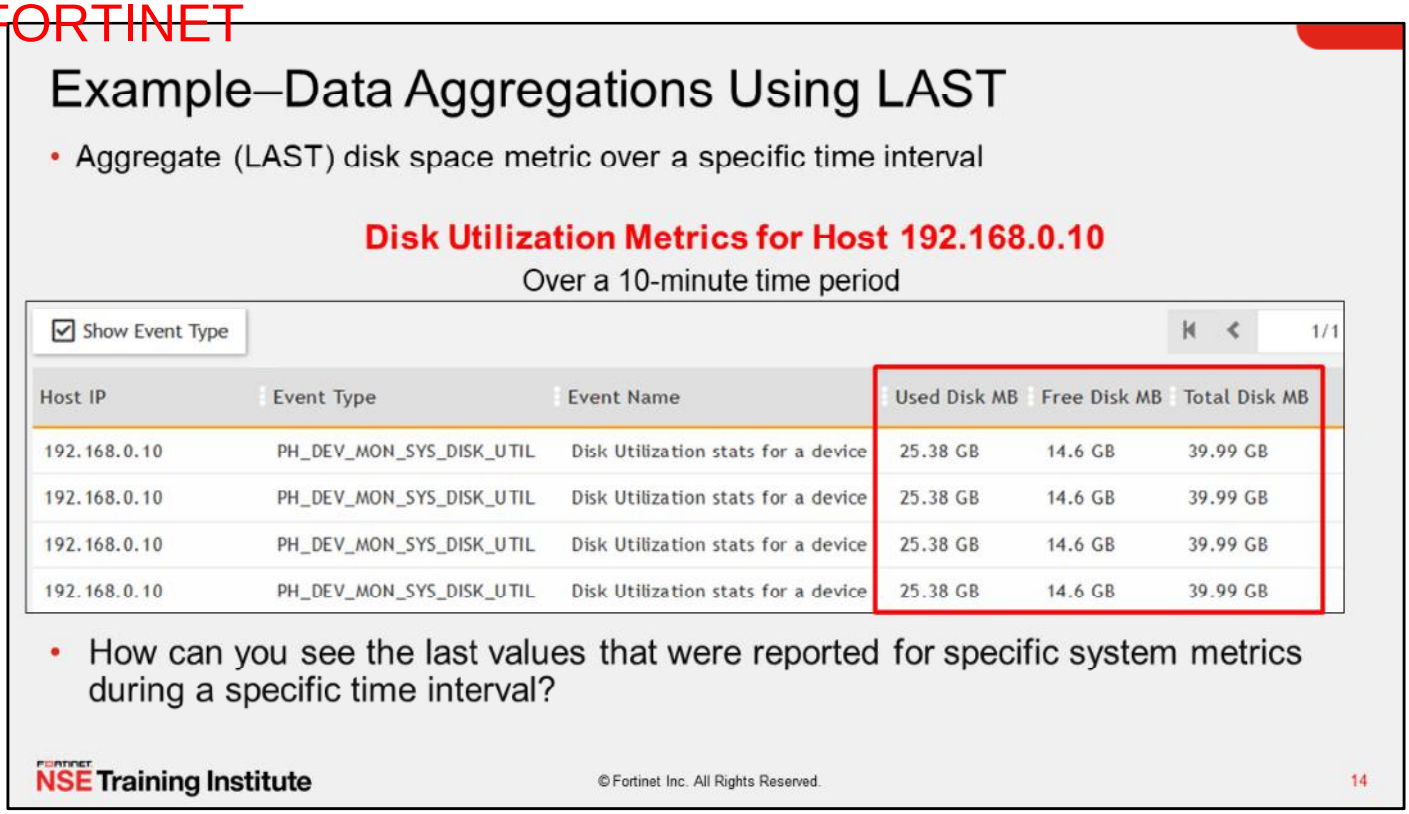


To achieve results for the scenario discussed in last slide, aggregation expressions were added for the following attributes:

- **AVG (CPU Util)**
- **MAX System (CPU Util)**
- **Min User (CPU Util)**

Vouchers & Dumps are Available | WhatsApp +201224560923

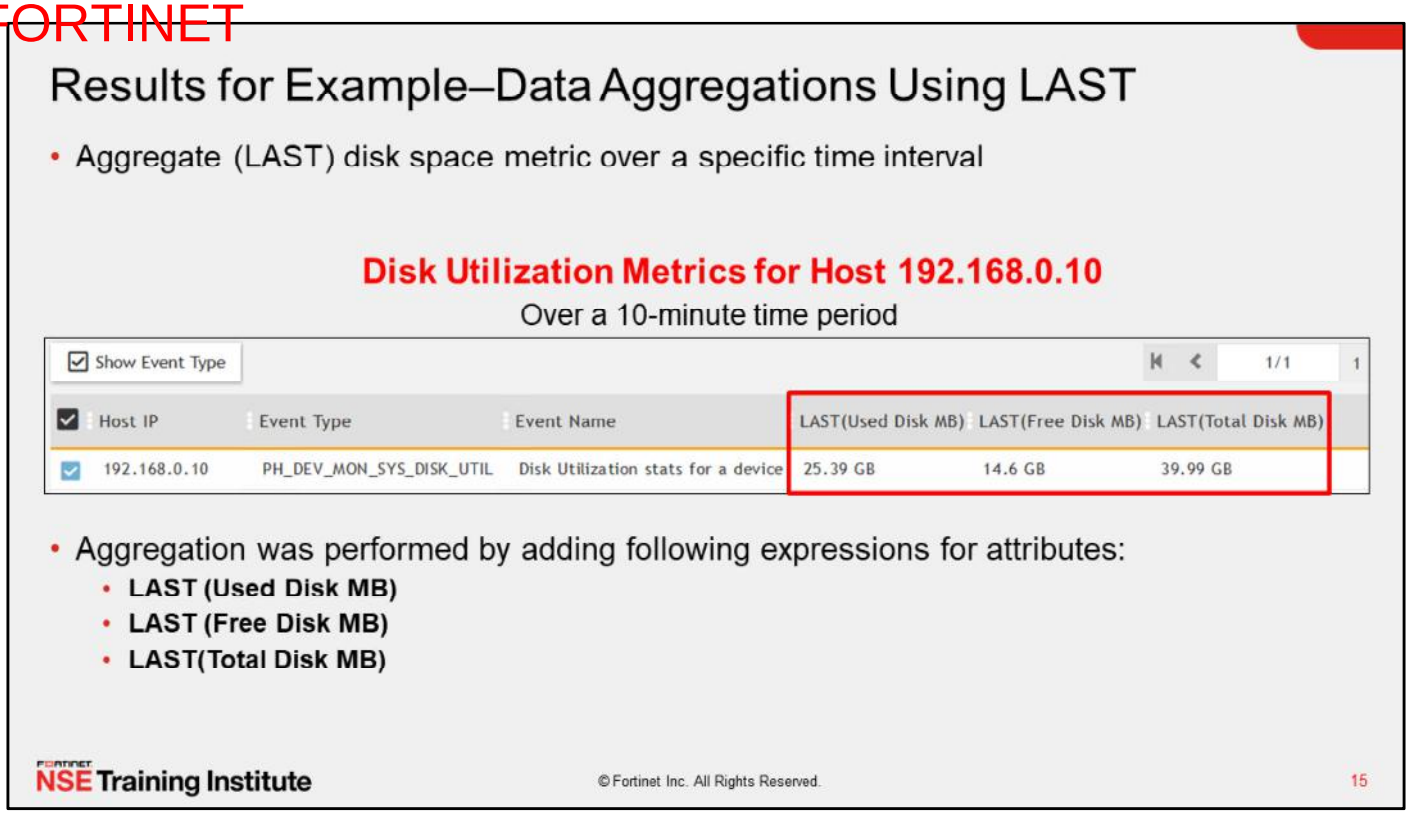
DO NOT REPRINT
© FORTINET
Brave-dumps.com



The example shown on this slide is similar to the previous one, only this time the metric you are working with is disk space, and you want to know the last values that were reported for specific system metrics. To do this, you need to add two attributes to the **Group By and Display Fields** section: **Host IP** and **Disk Name**. Then, the aggregation expressions for the **LAST** used **Disk**, **Total Disk**, and **Free Disk** in display fields.

Vouchers & Dumps are Available | WhatsApp +201224560923

DO NOT REPRINT
© FORTINET
Brave-dumps.com

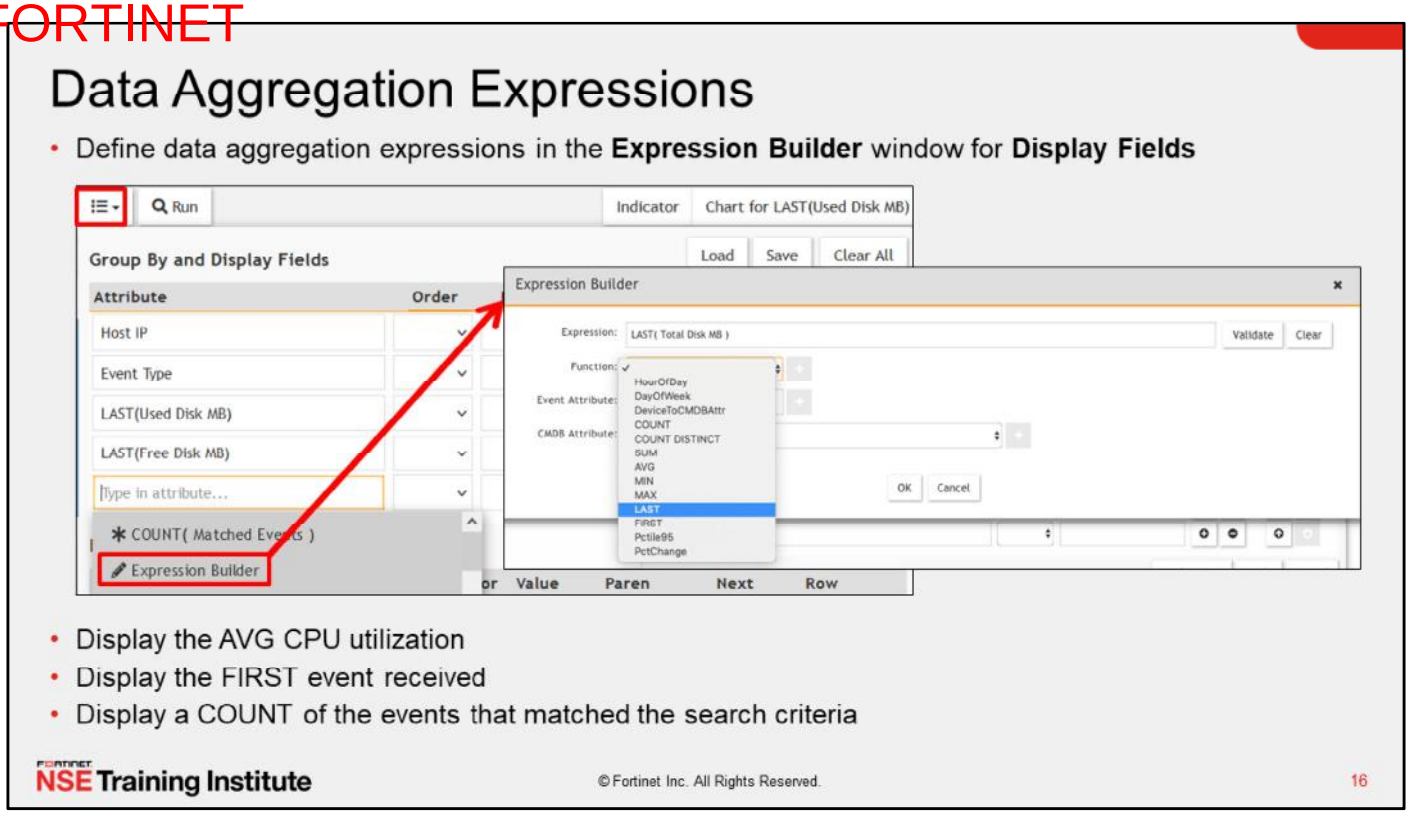


To achieve results for the scenario discussed on the previous slide, aggregation expressions were added for the following attributes :

- **LAST (Used Disk MB)**
- **LAST (Free Disk MB)**
- **LAST (Total Disk MB)**

Vouchers & Dumps are Available | WhatsApp +201224560923

DO NOT REPRINT
© FORTINET
Brave-dumps.com



Define data aggregation expressions using the **Expression Builder** window. You can open it by clicking on the **Expression Builder** in the **Attribute** column drop-down list.

The **Expression Builder** window contains the settings that you use to create an aggregation expression, such as the following:

- Display the **AVG** CPU utilization
- Display the **FIRST** event received
- Display a **COUNT** of the events that matched the search criteria

Vouchers & Dumps are Available | WhatsApp +201224560923

DO NOT REPRINT
© FORTINET
Brave-dumps.com

Knowledge Check

1. Examine the following table. If grouped by the **Reporting IP**, how many results would be displayed?

Reporting IP	User	Destination IP	Sent Bytes
6.6.6.6	Fred	1.1.1.1	100
6.6.6.6	Ken	2.2.2.2	200
6.6.6.6	Bill	3.3.3.3	300
6.6.6.6	Fred	2.2.2.2	400
6.6.6.6	Ken	4.4.4.4	500

✓ A. 1
B. 2
C. 5
D. 3

2. Examine the table in Question 1 again. If grouped by **Reporting IP** and **User**, how many results would be displayed?

A. 1
B. 2
C. 5
✓ D. 3

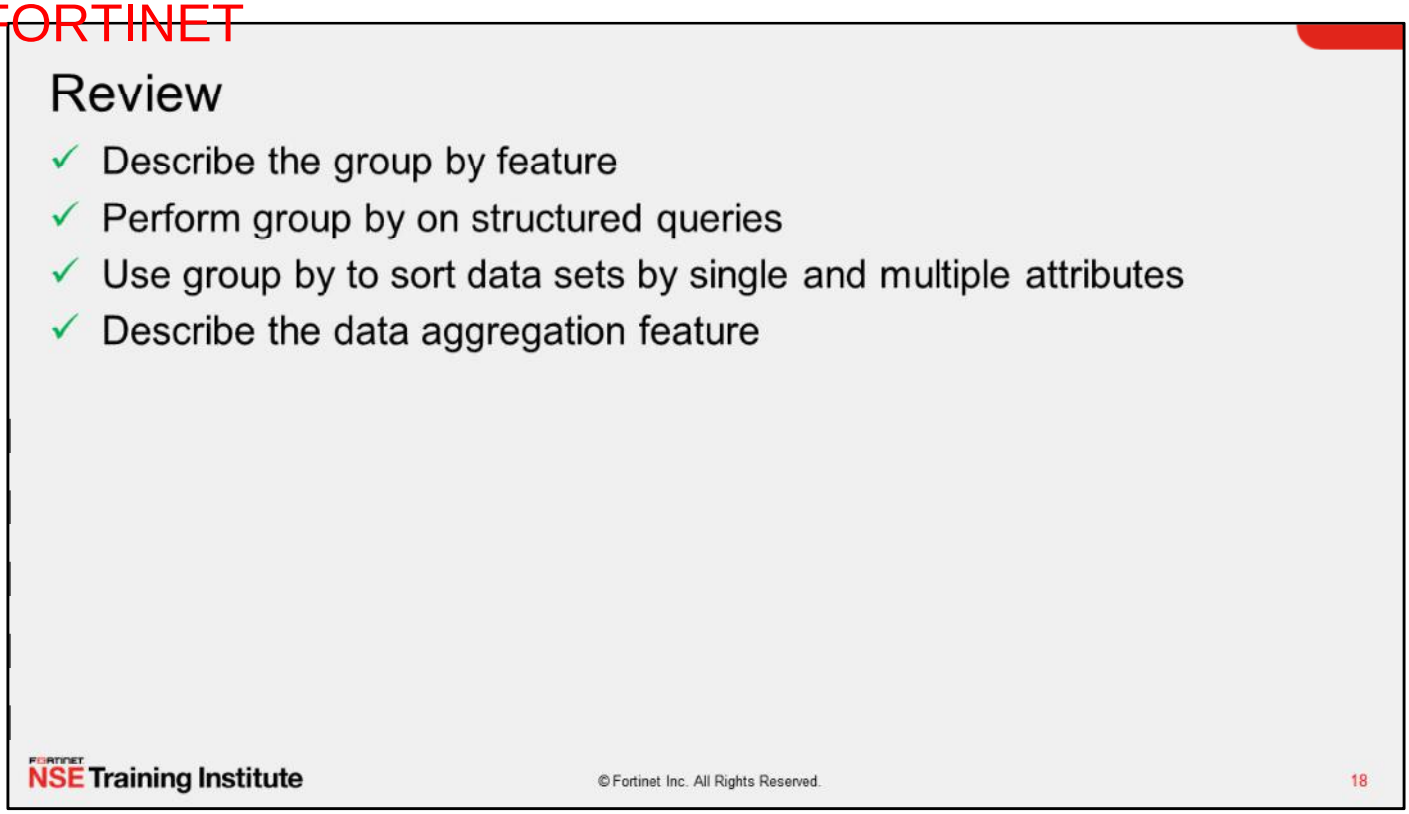
NSE Training Institute

© Fortinet Inc. All Rights Reserved.

17

Vouchers & Dumps are Available | WhatsApp +201224560923

DO NOT REPRINT
© FORTINET
Brave-dumps.com

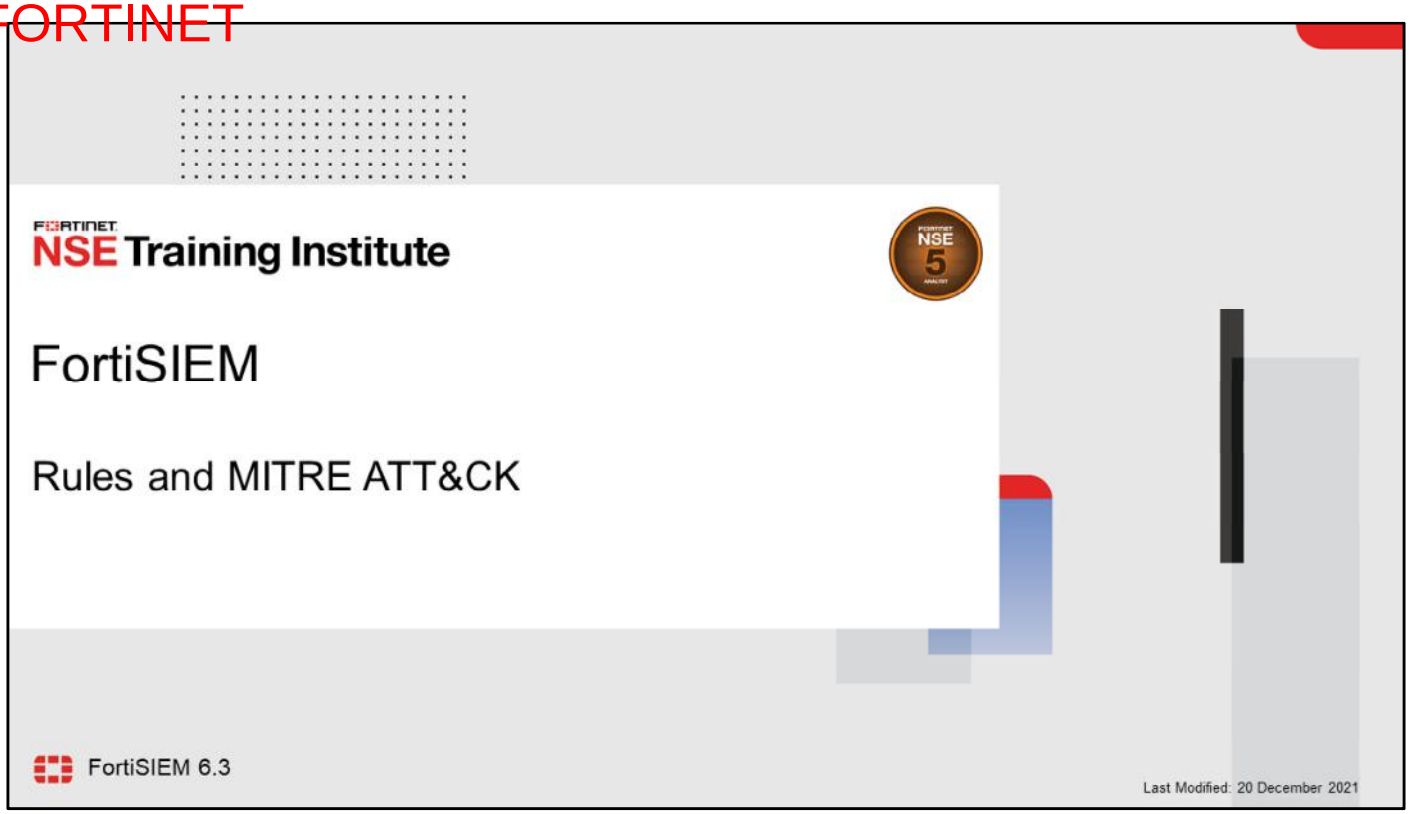


This slide shows the objectives that you covered in this lesson.

By mastering the objectives covered in this lesson, you learned how to use the group by and data aggregation features of FortiSIEM.

Vouchers & Dumps are Available | WhatsApp +201224560923

DO NOT REPRINT
© FORTINET
Brave-dumps.com



In this lesson, you will learn about rules.

Vouchers & Dumps are Available | WhatsApp +201224560923

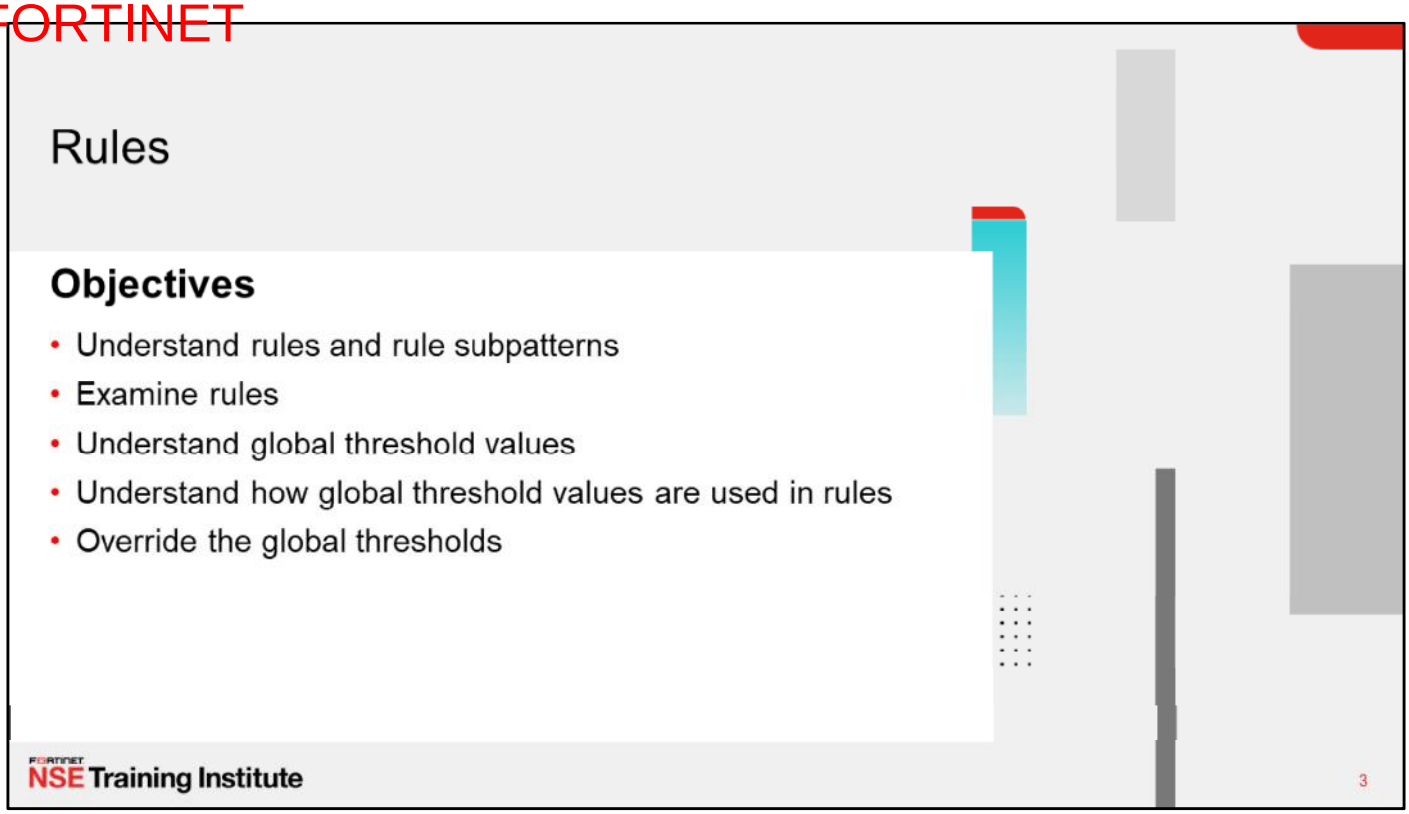
DO NOT REPRINT
© FORTINET
Brave-dumps.com



In this lesson, you will explore the topics shown on this slide.

Vouchers & Dumps are Available | WhatsApp +201224560923

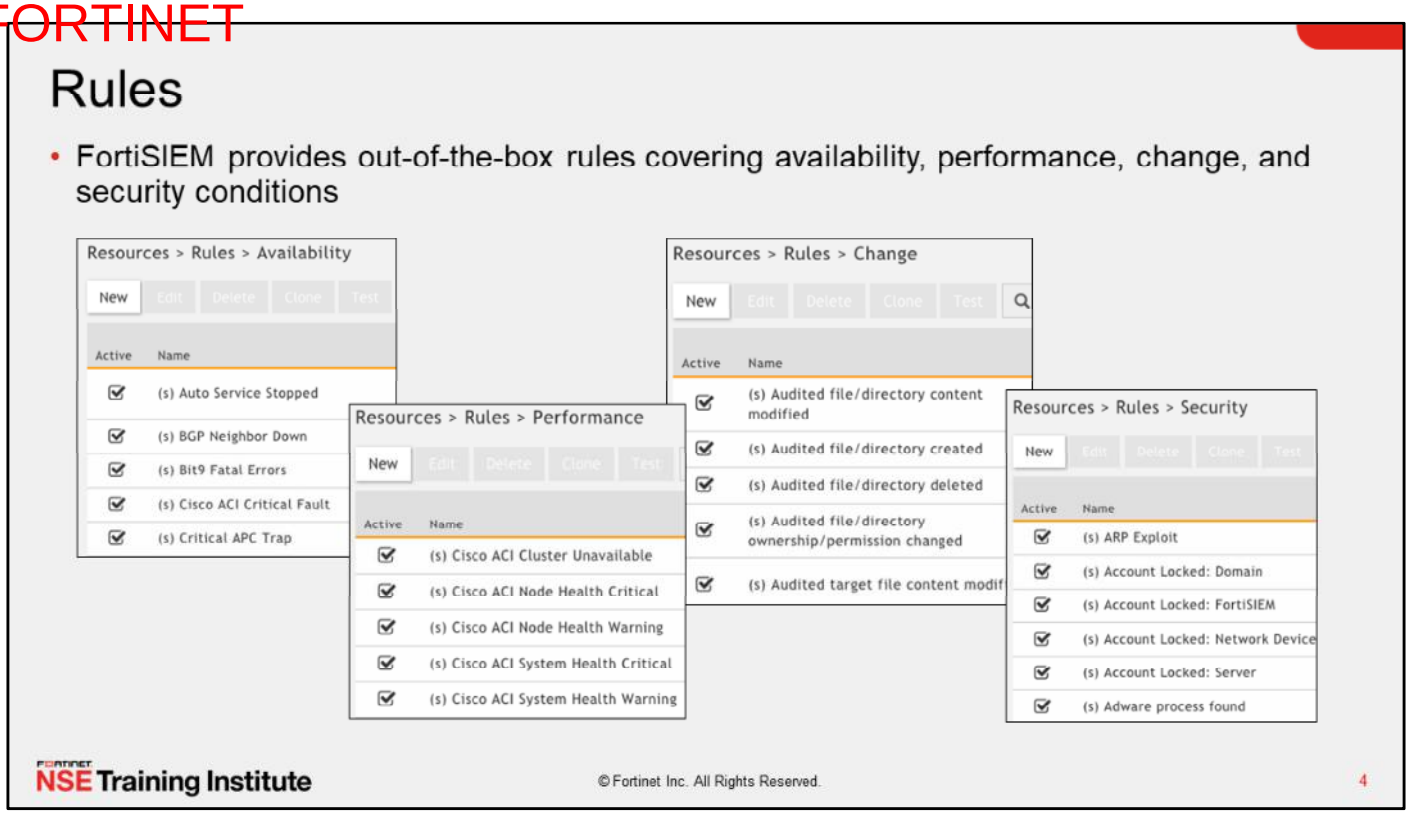
DO NOT REPRINT
© FORTINET
Brave-dumps.com



After completing this section, you should be able to achieve the objectives shown on this slide.

Vouchers & Dumps are Available | WhatsApp +201224560923

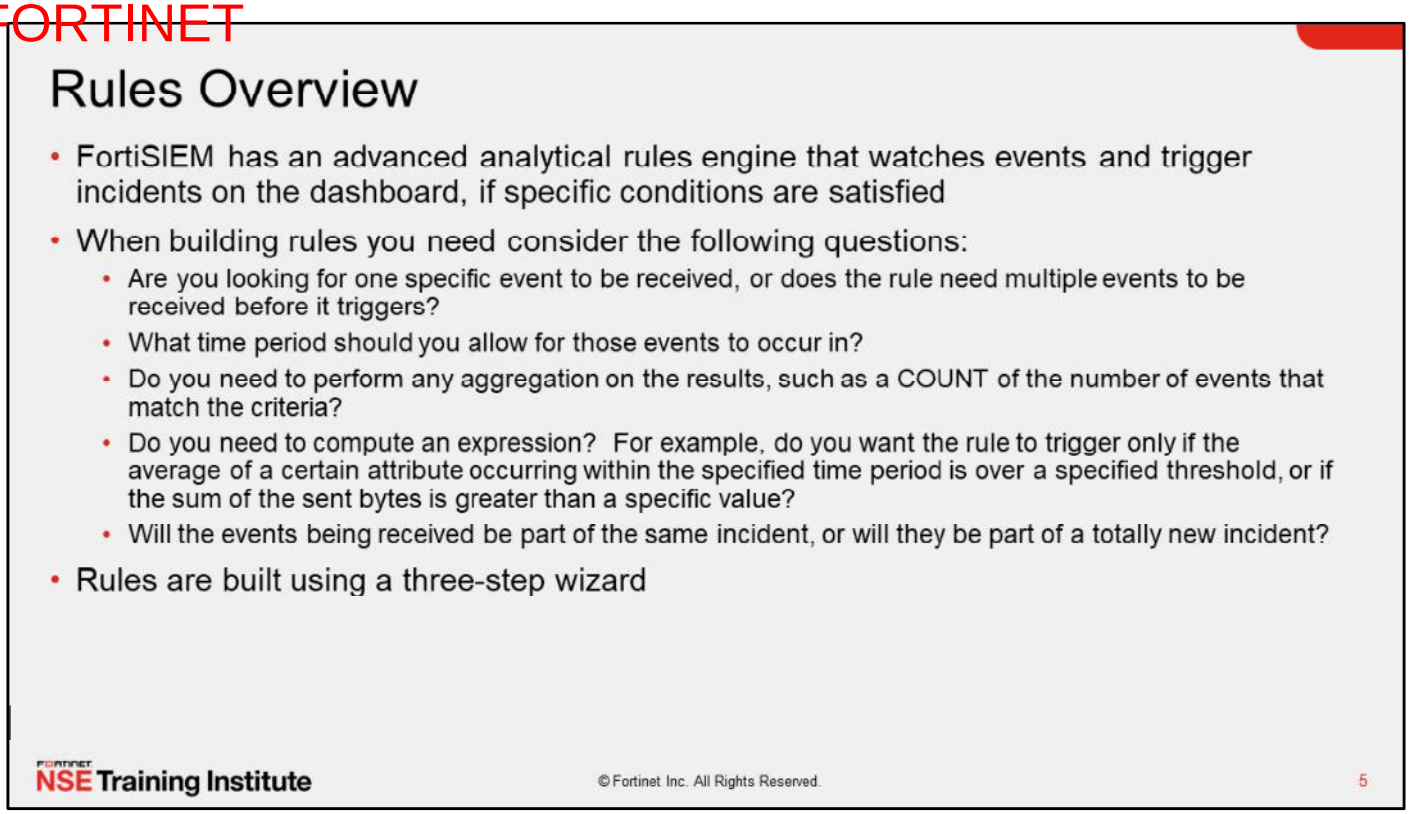
DO NOT REPRINT
© FORTINET
Brave-dumps.com



FortiSIEM provides hundreds of out-of-the-box rules covering availability, performance, change, and security conditions. You can edit these rules, clone them, or build new ones from scratch.

Vouchers & Dumps are Available | WhatsApp +201224560923

DO NOT REPRINT
© FORTINET
Brave-dumps.com



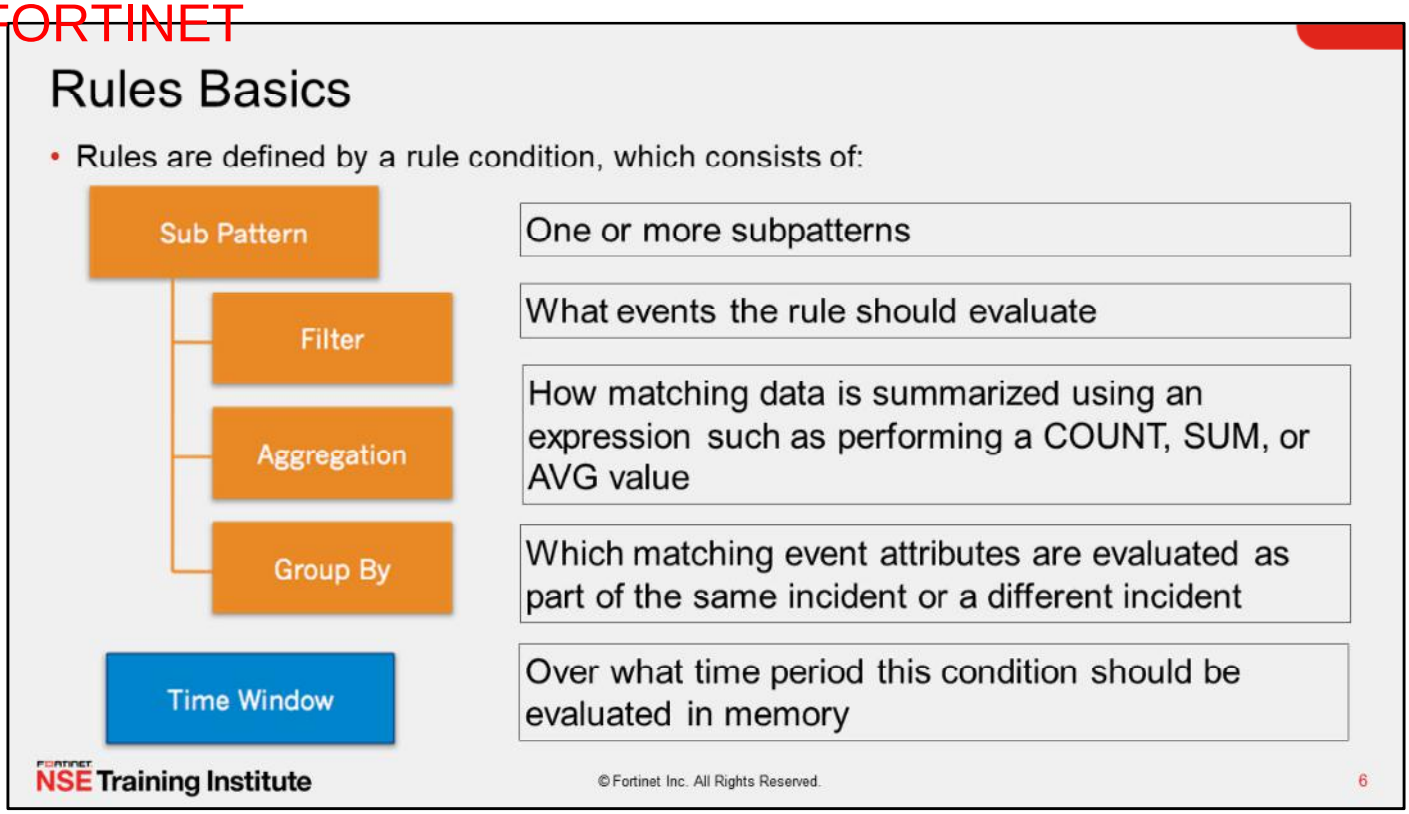
FortiSIEM has an advanced analytical rules engine that watches events and trigger incidents on the dashboard, if specific conditions are satisfied.

When building rules you must consider the following questions:

- Are you looking for one specific event to be received, or does the rule need multiple events to be received before it triggers?
- What time period should you allow for those events to occur in?
- Do you need to perform any aggregation on the results, such as a COUNT of the number of events that match the criteria?
- Do you need to compute an expression? For example, do you want the rule to trigger only if the average of a certain attribute occurring within the specified time period is over a specified threshold, or if the sum of the sent bytes is greater than a specific value?
- Will the events being received be part of the same incident, or will they be part of a totally new incident?

Vouchers & Dumps are Available | WhatsApp +201224560923

DO NOT REPRINT
© FORTINET
Brave-dumps.com



Rules are defined by a rule condition, which consists of one or more subpatterns.

A subpattern is defined by a filter, aggregation, and group by definitions. The filter is like a search condition. It specifies what event the rule should evaluate. For example, the rule might be looking for a particular reporting IP address, or an event type that is a login failure.

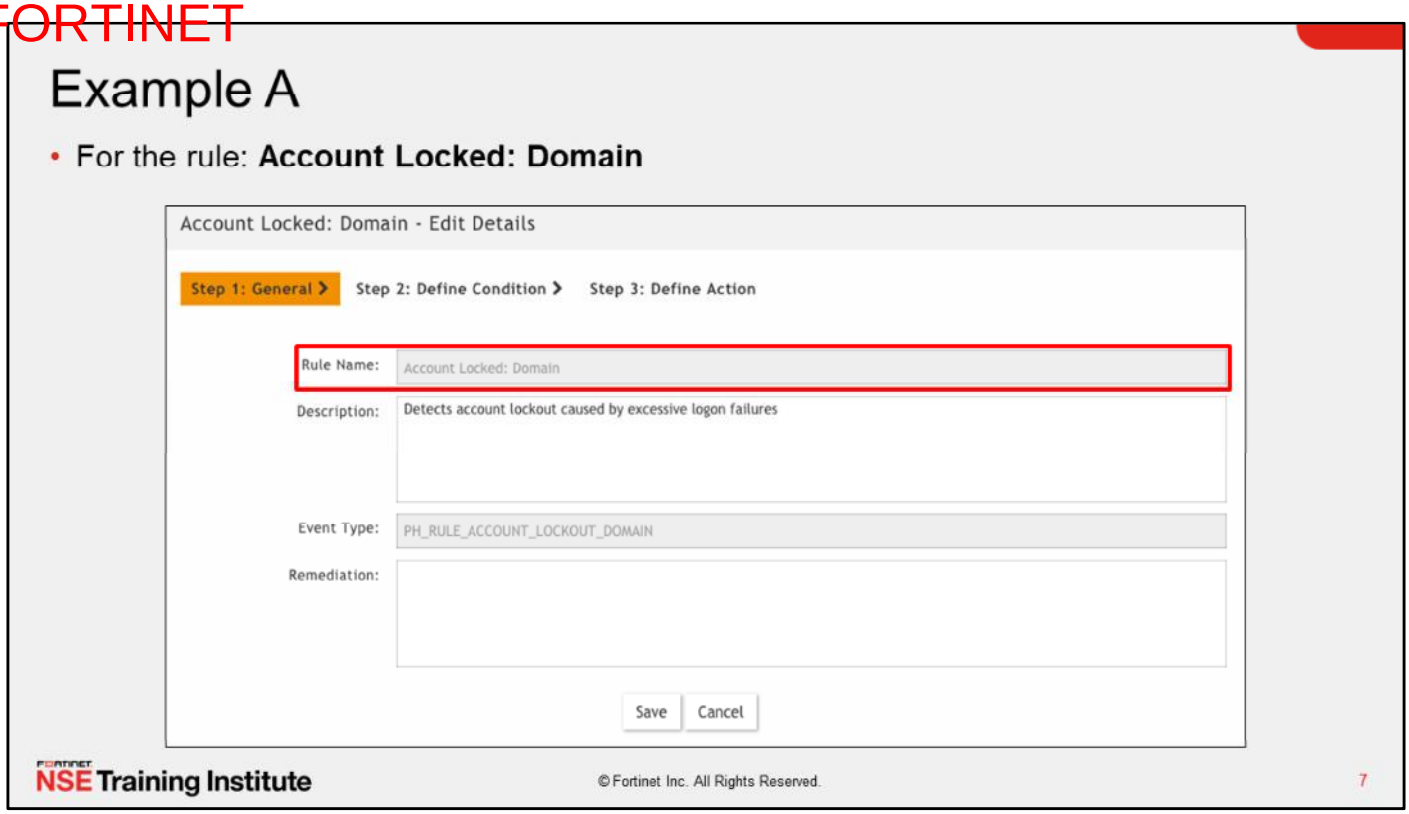
The aggregation condition tells the rules engine how to summarize the matching data, for example, by counting the number of times a specific event occurred, adding up the values within a number of events, or calculating the average of the values.

The group by condition allows the rules engine to identify which matching event attributes are evaluated as part of the same incident, or as part of a totally different incident.

The time window tells the rules engine the time period over which it should evaluate this condition.. For example, the engine could look for one or more login failures over a five-minute time period.

Vouchers & Dumps are Available | WhatsApp +201224560923

DO NOT REPRINT
© FORTINET
Brave-dumps.com

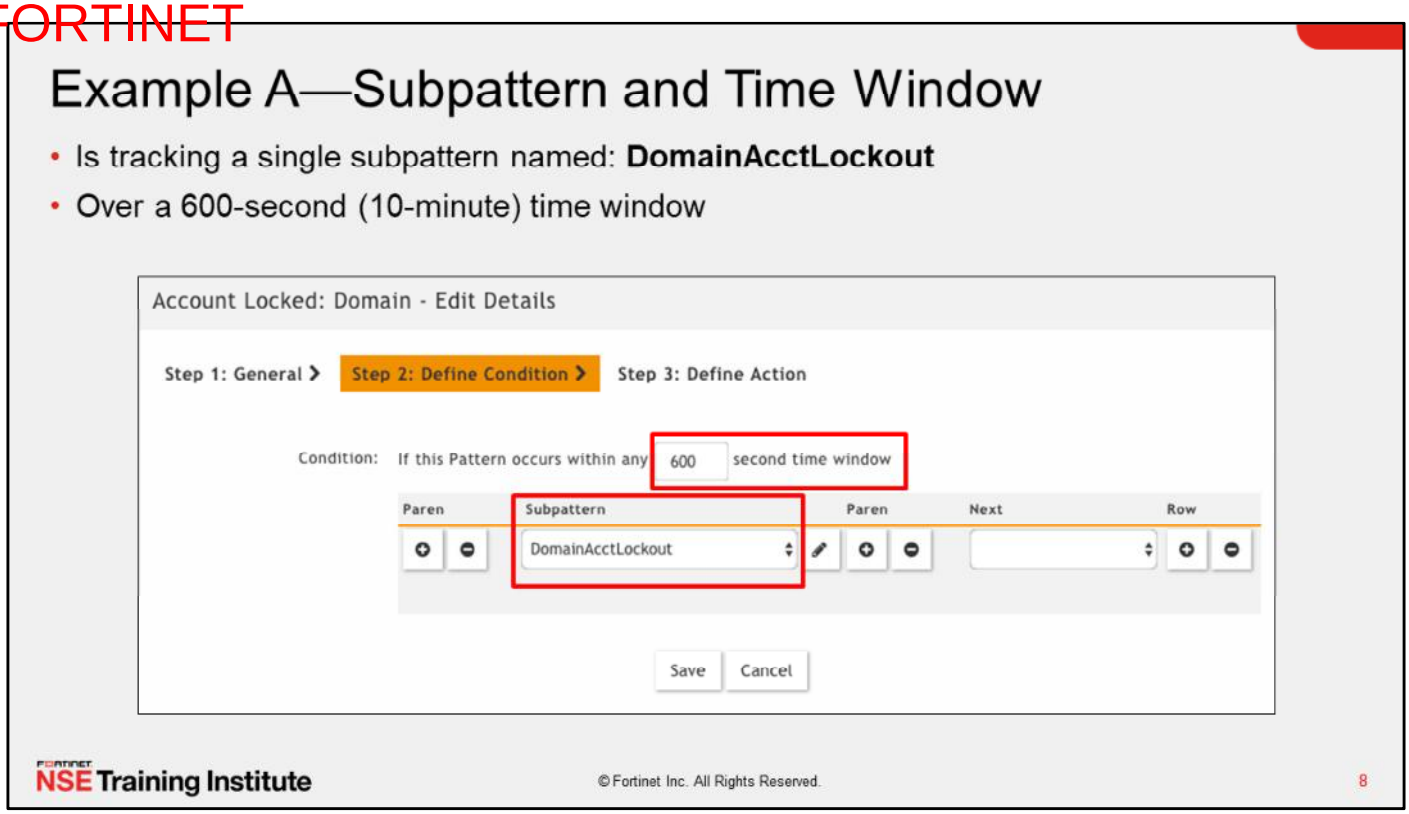


This slide shows an example rule. The name of the rule is **Account Locked: Domain**, which you can edit on the **RESOURCES** tab. The purpose of the rule is to detect account lockouts caused by excessive login failures. If it is a new rule then you must enter a rule name. The name you enter in the **Rule Type** is replicated in the **Event Type** field.

For the **Remediation** field, make sure that the remediation script for your scenario is defined. Check the existing remediation scripts by clicking **ADMIN** > **Settings** > **Notification**, and then looking in the **Action** column. If your device is not on the list, add the needed remediation script.

Vouchers & Dumps are Available | WhatsApp +201224560923

DO NOT REPRINT
© FORTINET
Brave-dumps.com



In the second step, you define the rule conditions. Rule conditions define the event attributes and thresholds that trigger an incident. Rule conditions are built from subpatterns of event attribute filters and aggregation functions. You can specify more than one subpattern and the relationships and constraints among them.

A subpattern defines the characteristics of events that will cause a rule to trigger an incident. A subpattern involves defining event attributes that are monitored, and then defining the threshold values for aggregations of event attributes that trigger an incident.

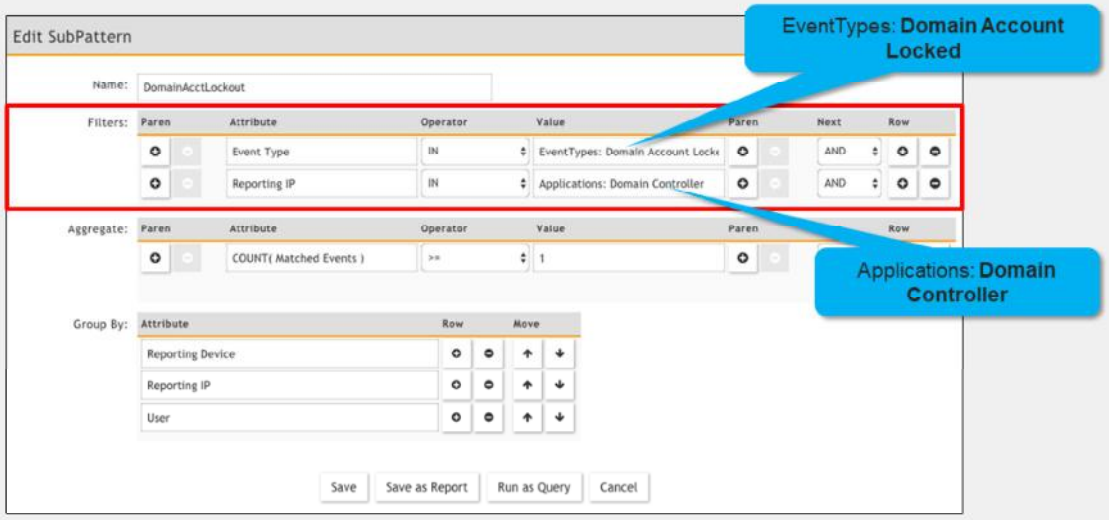
You can specify the time window during which the rule is triggered if it matches the condition.

Vouchers & Dumps are Available | WhatsApp +201224560923

DO NOT REPRINT
© FORTINET
Brave-dumps.com

Example A—Subpattern Filter

- The filter is defined to look for events that are categorized as **Domain Account Locked** and only those reported by **Domain Controllers**



NSE Training Institute

© Fortinet Inc. All Rights Reserved.

9

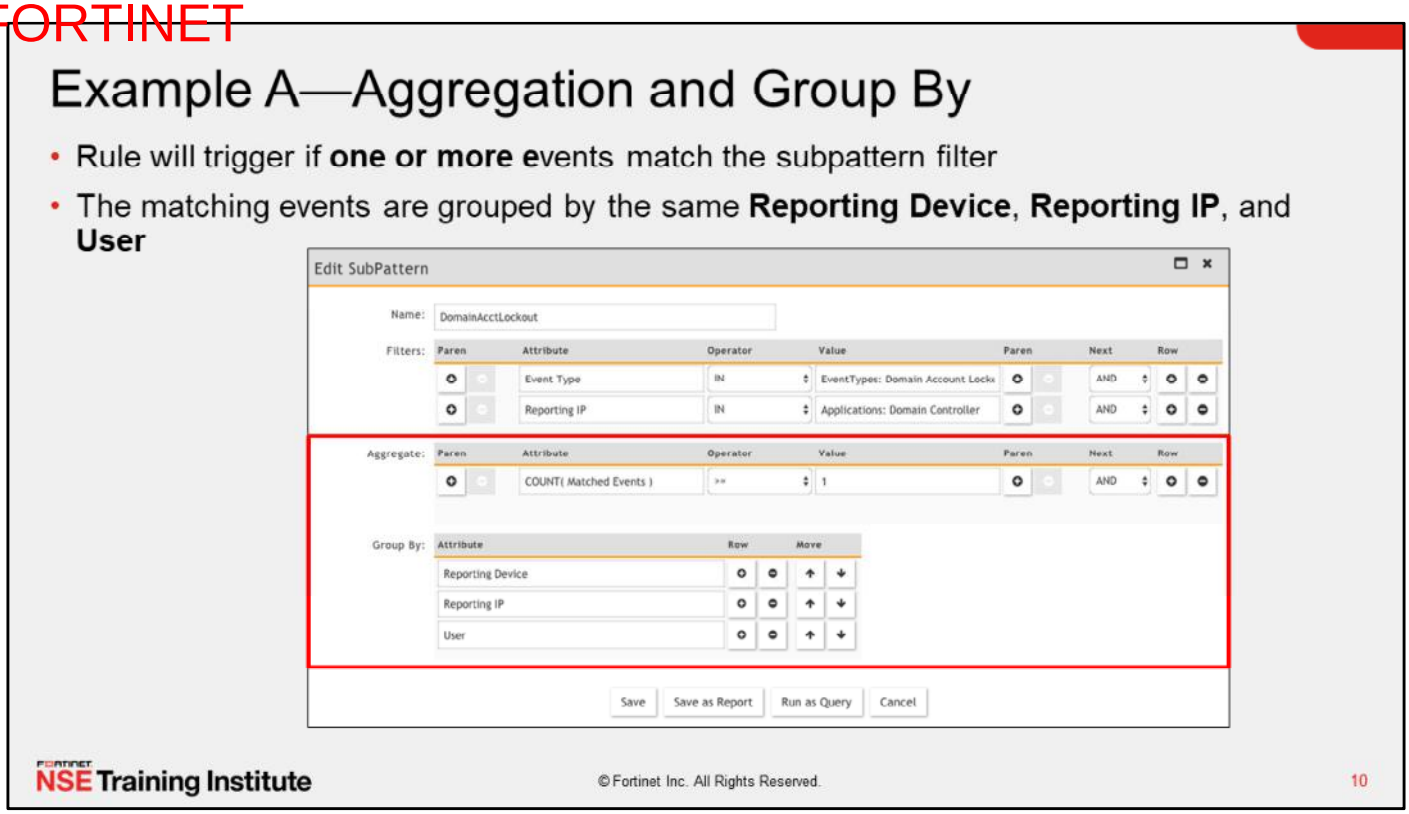
You can edit the subpattern and specify **Filters**, **Aggregate**, and **Group By** attributes.

In the example shown on this slide, the rule has a subpattern filter, which is defined by two conditions:

- In the first condition, the selected attribute is **Event Type,** the selected operator is **IN**, and the selected value is **Event Types: Domain Account Locked**. So, this condition is looking for any event types in the configuration management database (CMDB) that are in the **Domain Account Locked** category. This condition also includes the next logical operator, **AND**.
- In the second condition, the selected attribute is **Reporting IP**, the selected operator is **IN**, and the selected value is **Applications: Domain Controllers**. So, this condition is looking for reporting IP addresses in the CMDB that come from a domain controller.

Vouchers & Dumps are Available | WhatsApp +201224560923

DO NOT REPRINT
© FORTINET
Brave-dumps.com



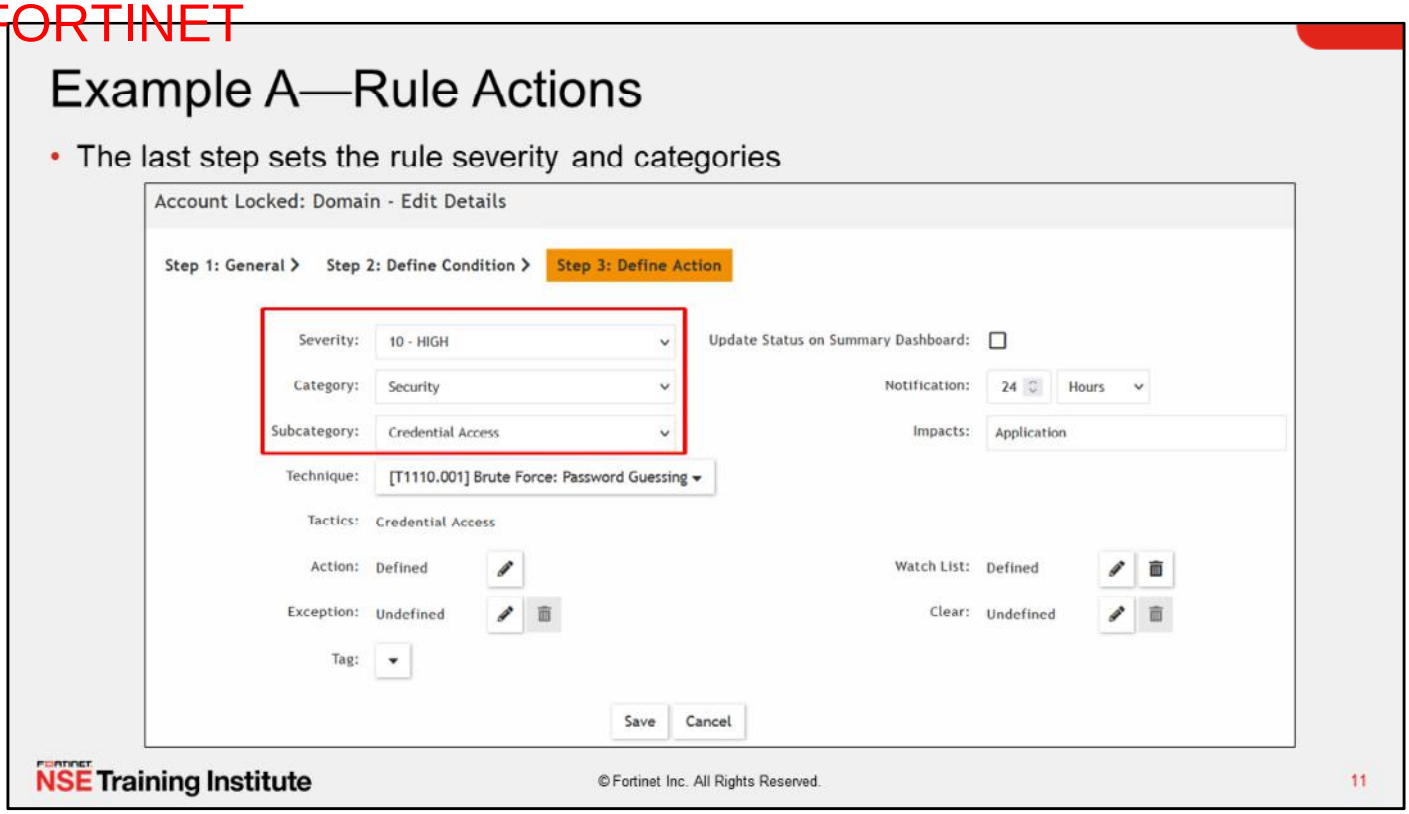
This rule has an aggregate condition that specifies that the rule looks for one or more events that match the filter criteria over a time period defined as 600 seconds (or 10 minutes). It does this by using a **COUNT (Matched Events)** attribute, where the operator is equal to or greater than **1**.

The results should be grouped by the reporting IP address and user. It is the **Group By** operation that tells the rules engine which matching event attributes to evaluate as part of the same incident, or as part of a different incident.

In the example shown on this slide, because the count is one or more, if you received five events that match the domain account lockout, AND were from a reporting IP of a domain controller, then you would need to make sure that you are referring to the same reporting IP address and the same user in each incident.

Vouchers & Dumps are Available | WhatsApp +201224560923

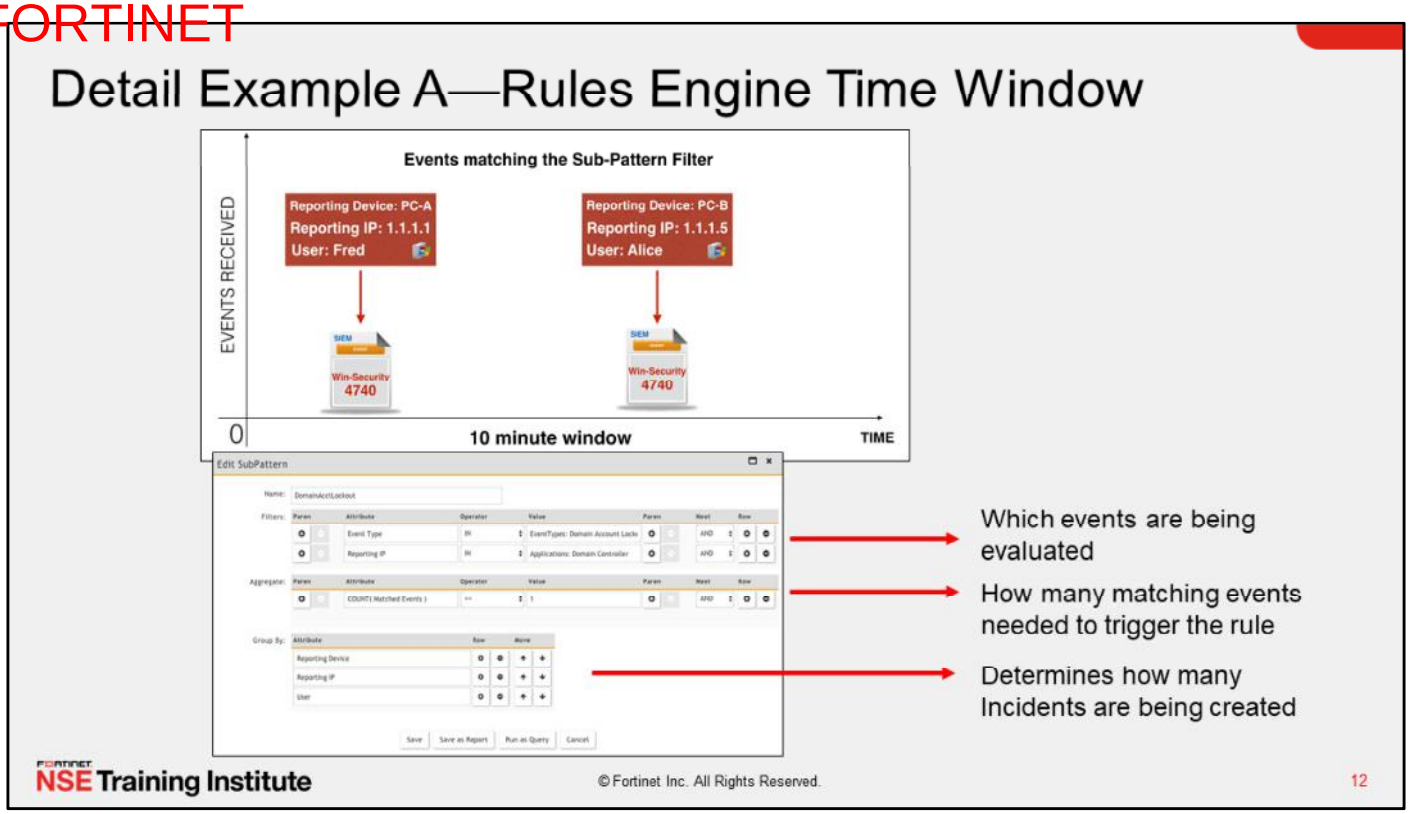
DO NOT REPRINT
© FORTINET
Brave-dumps.com



The third step sets the action criteria for the rule. You can select **Severity** to associate with the incident triggered by the rule. You should select the **Category** of incidents to be triggered by the rule and the **Subcategory** from the available list, based on the selected incident **Category**.

Vouchers & Dumps are Available | WhatsApp +201224560923

DO NOT REPRINT
© FORTINET
Brave-dumps.com



Now, you will examine this rule in more detail.

Rules are evaluated over a specified time interval. In the 10-minute window shown in the example on this slide, two events were received that matched the search filter. The first event was from the reporting IP address 1.1.1.1 and user Fred, and the second event was from the reporting IP of 1.1.1.5 and user Alice.

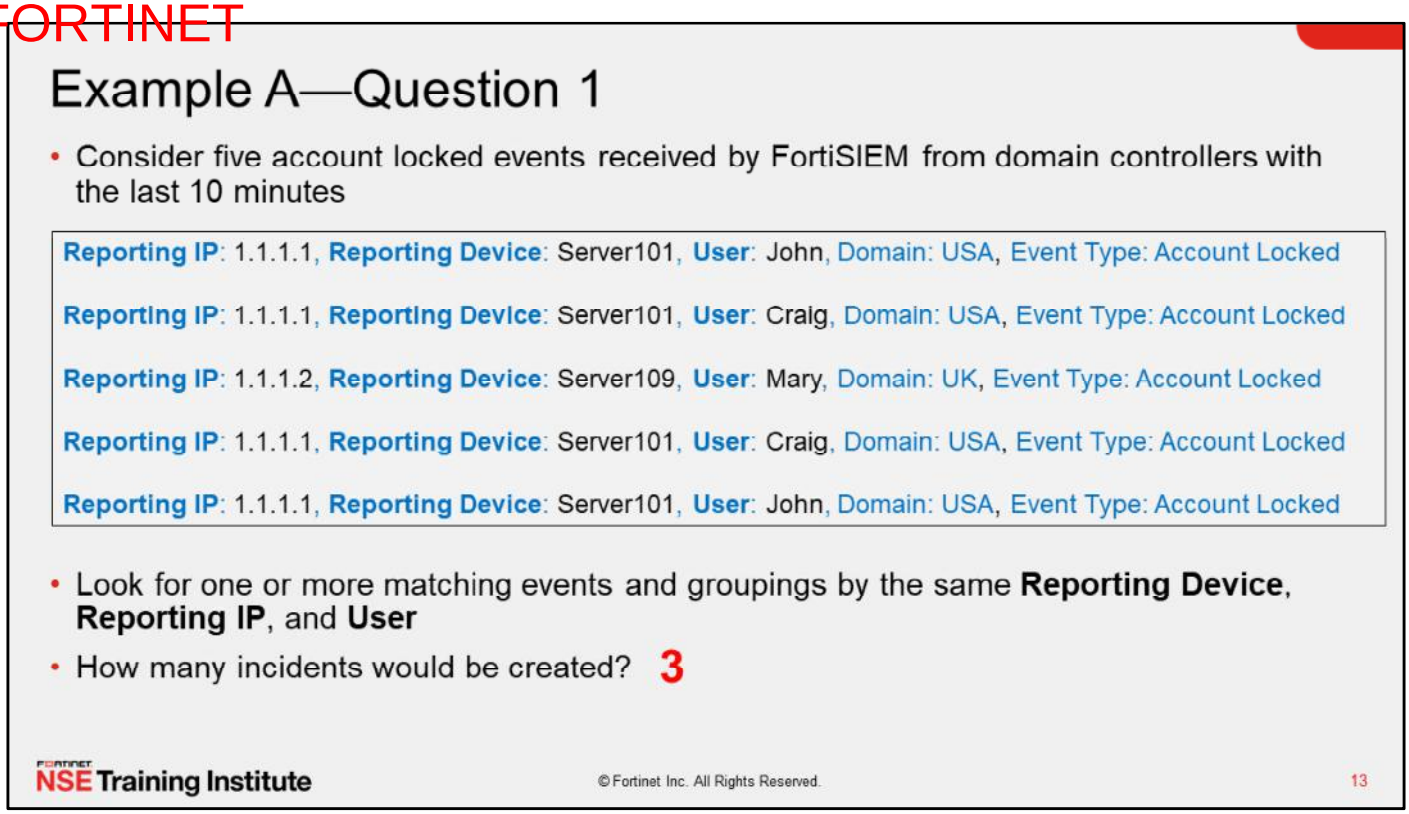
The aggregate condition tells us how many matching events are required to trigger the rule. The grouping will identifies which of the attributes in the matching events will be considered as part of the same incident and when to generate a totally separate incident.

In the example shown on this slide, two events meet the aggregation condition and are grouped by the same reporting IP address and user. So, in this example, two totally separate incidents are generated: the first for reporting IP address 1.1.1.1 and user Fred, and the second for reporting IP address 1.1.1.5 and user Alice.

Consider a scenario where these two events were the same; that is, they were both from the reporting IP address 1.1.1.1 and user Fred. In that case, because the count of matching events is one or more, the two events would be part of the same incident.

Vouchers & Dumps are Available | WhatsApp +201224560923

DO NOT REPRINT
© FORTINET
Brave-dumps.com



The question shown on this slide is based on the example shown on the previous slide.

Consider the following five account locked events received by FortiSIEM from domain controllers within the last 10 minutes:

1. Reporting IP 1.1.1.1, user Fred, USA Domain
2. Reporting IP 1.1.1.1, user Craig, USA Domain
3. Reporting IP 1.1.1.2, user Mary, UK Domain
4. Reporting IP 1.1.1.1, user Craig, USA Domain
5. Reporting IP 1.1.1.1, user Fred, USA Domain

If you are looking for one or more matching events and groupings by the same reporting IP address and user, how many incidents would be created?

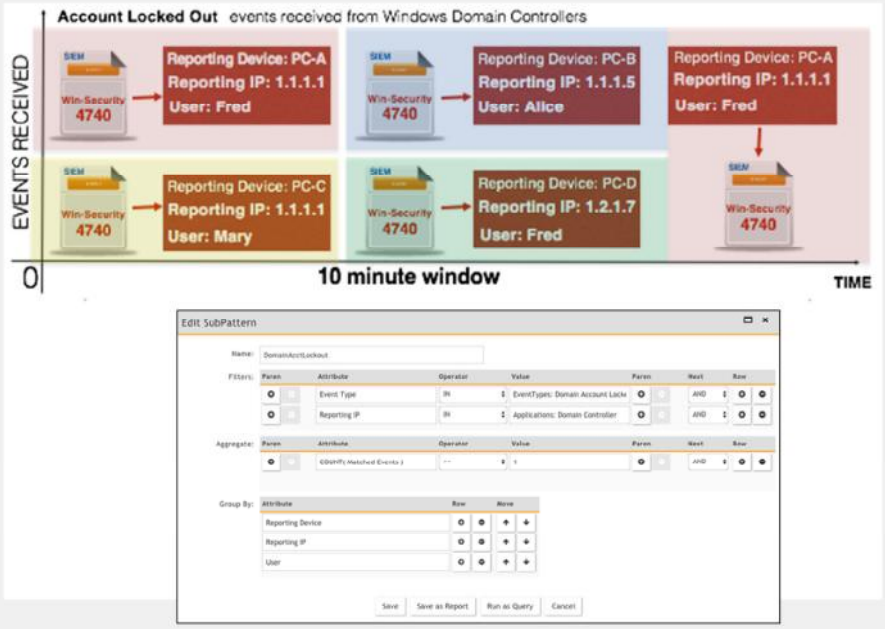
The answer is three. In this list of events, the reporting IP address 1.1.1.1 and the user Fred is reported twice: in the first event and the fifth event. The second and the fourth event also have the same reporting IP address and the same user (Craig). The third event is unique, but, because we are looking for one or more matching events, it satisfies the criteria. Therefore, in this example, three incidents are created.

Vouchers & Dumps are Available | WhatsApp +201224560923

DO NOT REPRINT
© FORTINET
Brave-dumps.com

Example A—Question 2

- How about now?



- Answer: 4

NSE Training Institute

© Fortinet Inc. All Rights Reserved.

14

In the example shown on this slide, you are still using the same rule, but you receive five matching events during the specified 10-minute time window. Again, all these events are account lockout events received from a Windows domain controller. The following are the five events that were received:

1. Reporting IP 1.1.1.1, user Fred
2. Reporting IP 1.1.1.5, user Alice
3. Reporting IP 1.1.1.1, user Fred
4. Reporting IP 1.1.1.1, user Mary
5. Reporting IP 1.2.1.7, user Fred

Based on the aggregate condition and grouping in this rule, how many incidents are generated?

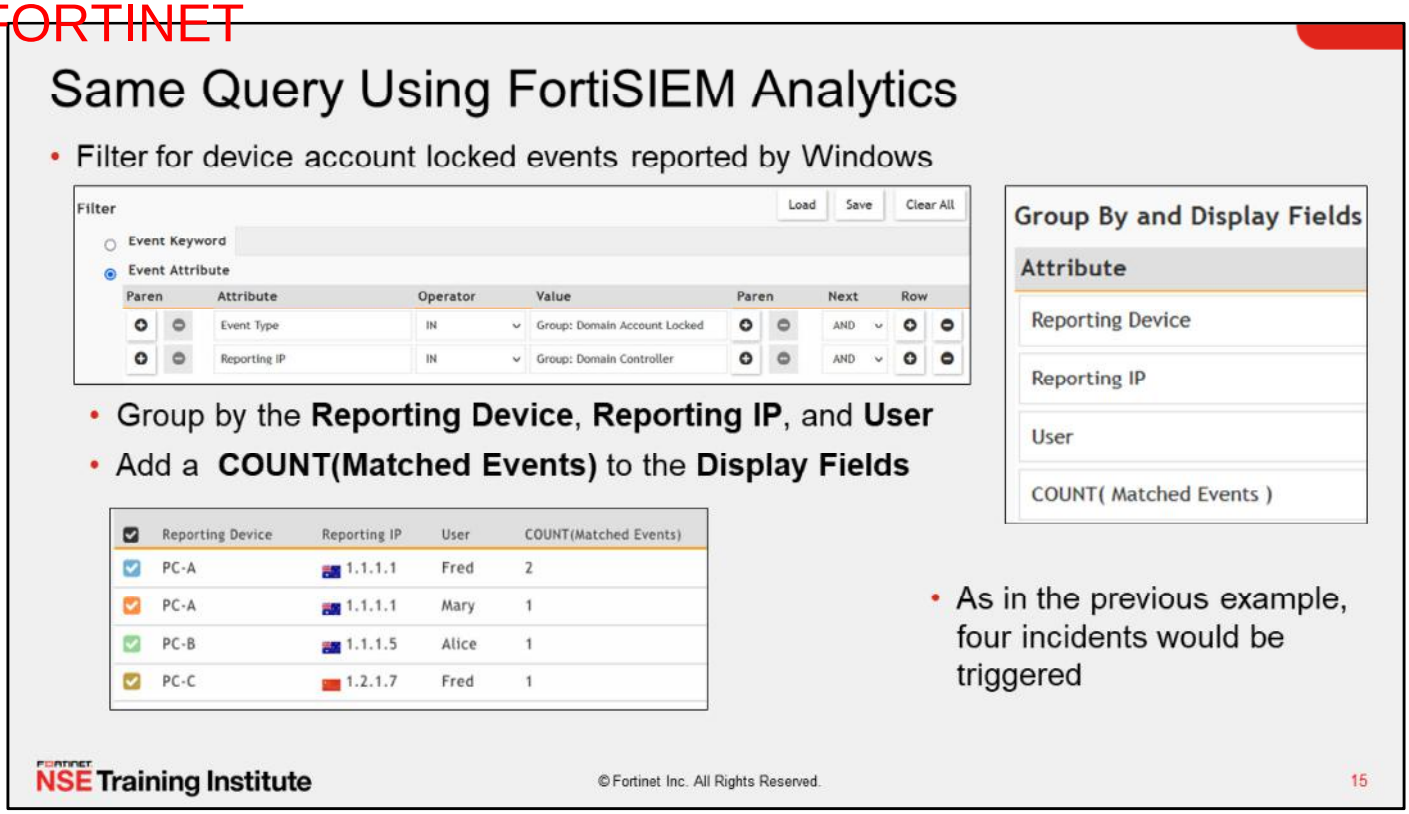
Events one, three, and four all have the same reporting IP of 1.1.1.1, but only events one and three also have the same user, Fred. Therefore, events one and three are grouped as a single incident.

Event two has no matching reporting IP and user combinations, so it is reported as a single incident. As previously discussed, event three is grouped with event one as one incident. That puts our current incident count at two. Event four has the same reporting IP as events one and three, but has a different user, Mary, so it is reported as a single incident.

Finally, the user in event five has been used in previous events, Fred, but it has a unique reporting IP, so it is counted as a separate incident. Therefore, the incident count for this example, and the answer to the question, is four.

Vouchers & Dumps are Available | WhatsApp +201224560923

DO NOT REPRINT
© FORTINET
Brave-dumps.com



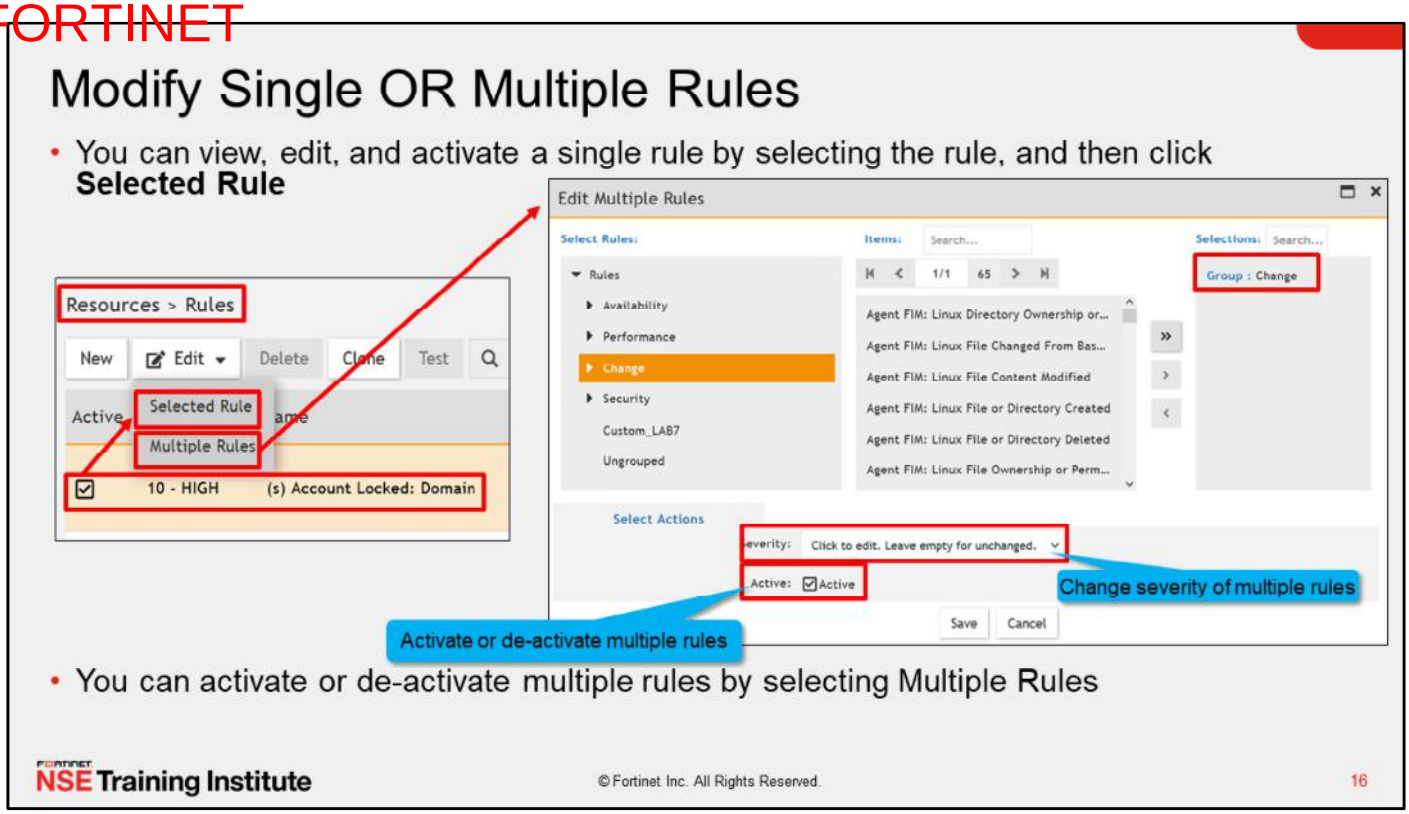
To help put rules into context, examine what would happen if you made the same query using FortiSIEM analytics.

The example on this slide shows a search condition to look for lockout events reported by a Windows domain controller. The resulting events are grouped by the reporting IP address and user. The example also shows the addition of a count of the matching events to the display columns.

As you can see, you get exactly the same four entries in the results. The top entry indicates that two events match the same reporting IP address and user, and the rest are single entries.

Vouchers & Dumps are Available | WhatsApp +201224560923

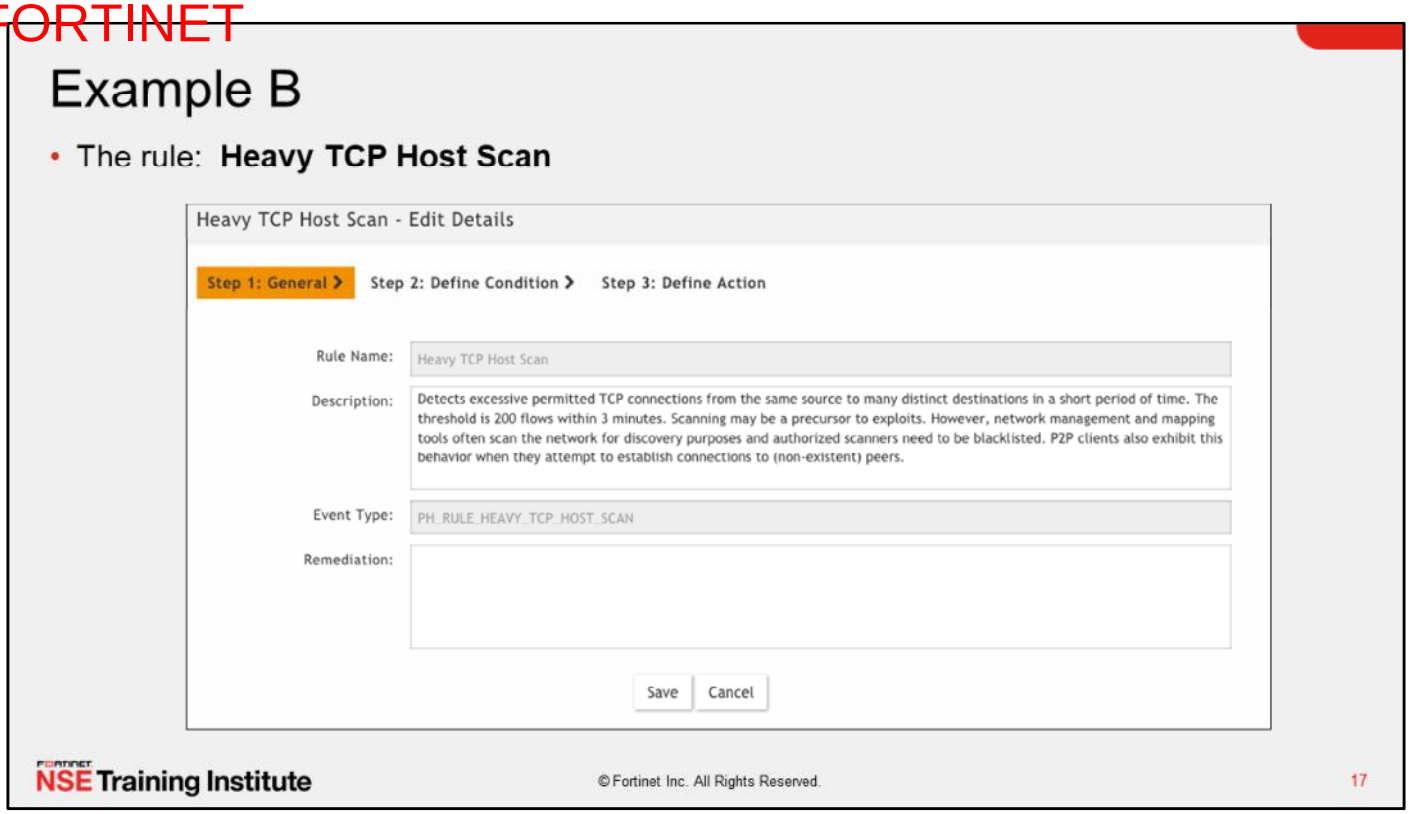
DO NOT REPRINT
© FORTINET
Brave-dumps.com



You can view, edit, and activate a single rule by selecting and then clicking **Selected Rule.** You can also change severity of multiple rules, and activate or de-activate multiple rules by selecting **Multiple Rules.**

Vouchers & Dumps are Available | WhatsApp +201224560923

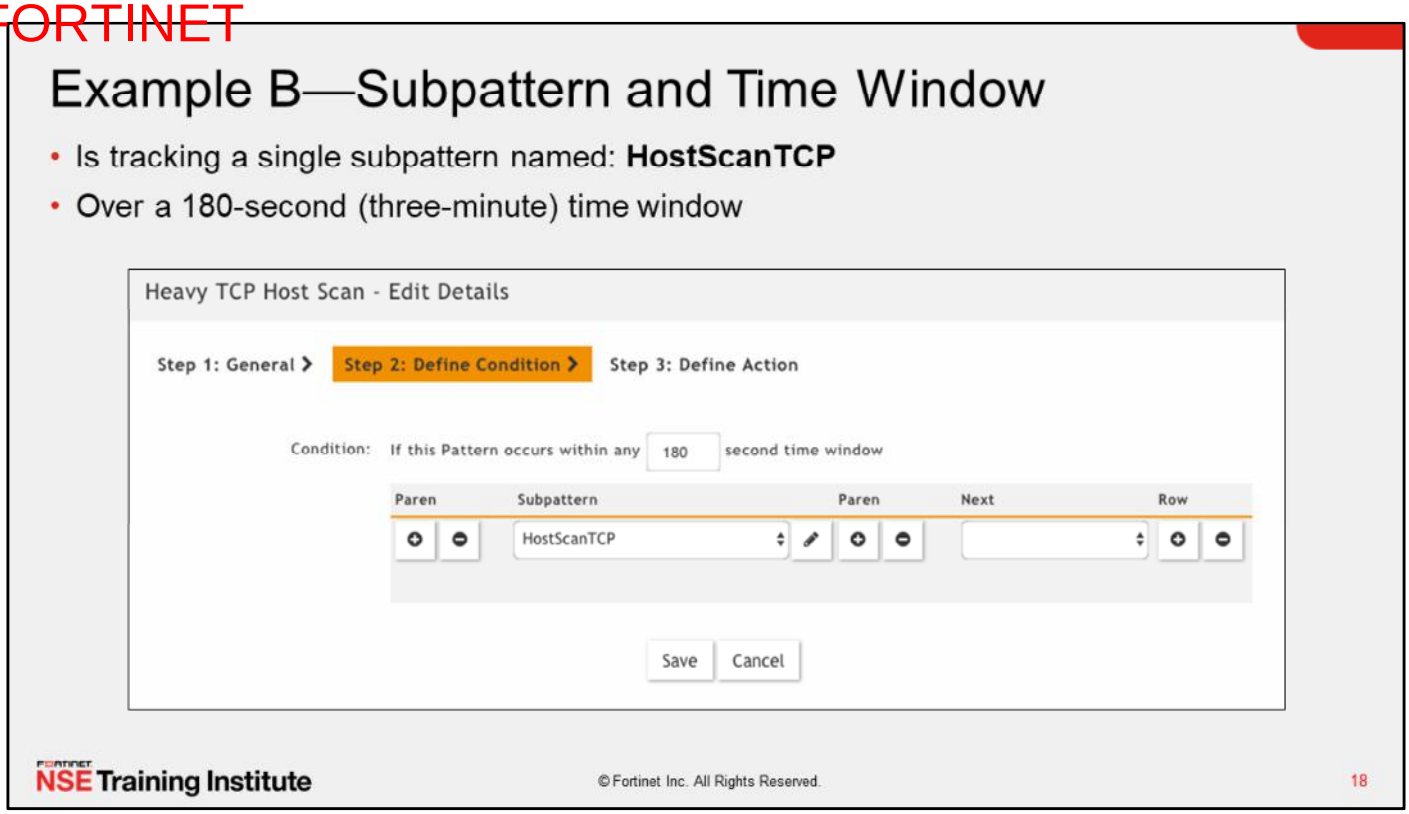
DO NOT REPRINT
© FORTINET
Brave-dumps.com



The second example rule that you will look at is a heavy TCP host scan. This rule detects an excessive number of permitted TCP connections from the same source, going to many different destinations, within a short period of time.

Vouchers & Dumps are Available | WhatsApp +201224560923

DO NOT REPRINT
© FORTINET
Brave-dumps.com



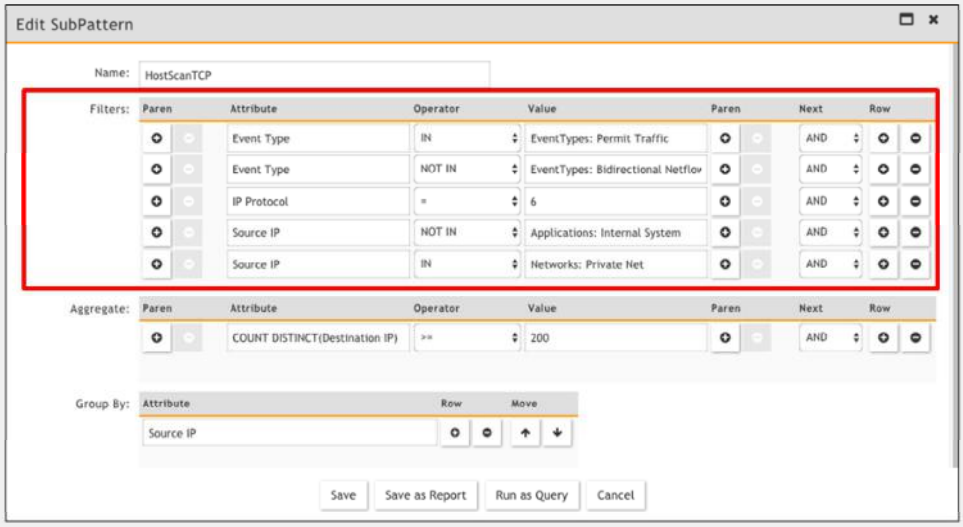
In the second step, you will define the **Subpattern**, which in this example is **HostScanTCP**. The rule is triggered if the pattern occurs within a 180-second (three-minute) window.

Vouchers & Dumps are Available | WhatsApp +201224560923

DO NOT REPRINT
© FORTINET
Brave-dumps.com

Example B—Subpattern Filter

- The filter is defined to look for events that are permitted traffic and TCP, but not from flow traffic, where the source IP is internal but not from FortiSIEM itself



NSE Training Institute

© Fortinet Inc. All Rights Reserved.

19

When you edit the **HostScanTCP** subpattern, you will have the option to modify the **Filters**, **Aggregate**, and **Group By** attributes.

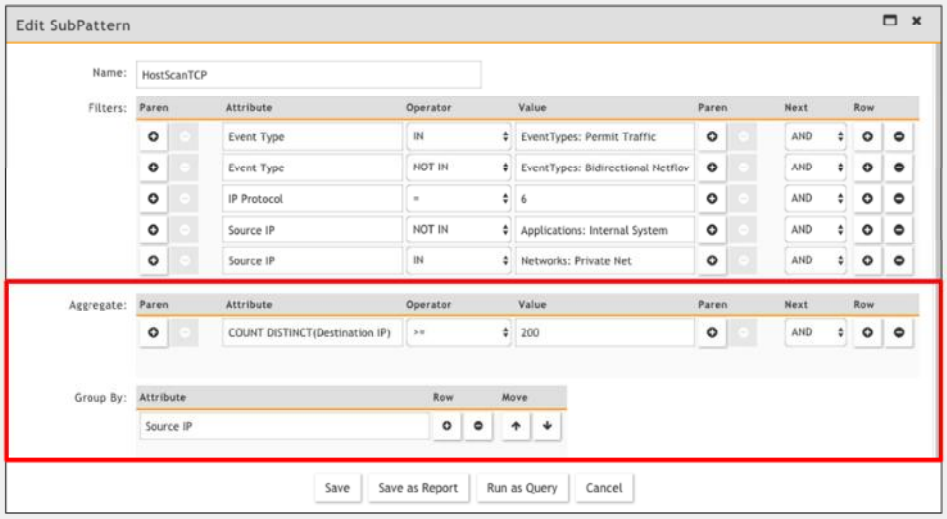
The filter is defined to look for events that are permitted traffic and TCP, but not from flow traffic, where the source IP is internal but not from FortiSIEM itself.

Vouchers & Dumps are Available | WhatsApp +201224560923

DO NOT REPRINT
© FORTINET
Brave-dumps.com

Example B—Aggregation and Group By

- Rule triggers if 200 or more *distinct destination IPs* recorded for the same **Source IP**



NSE Training Institute

© Fortinet Inc. All Rights Reserved.

20

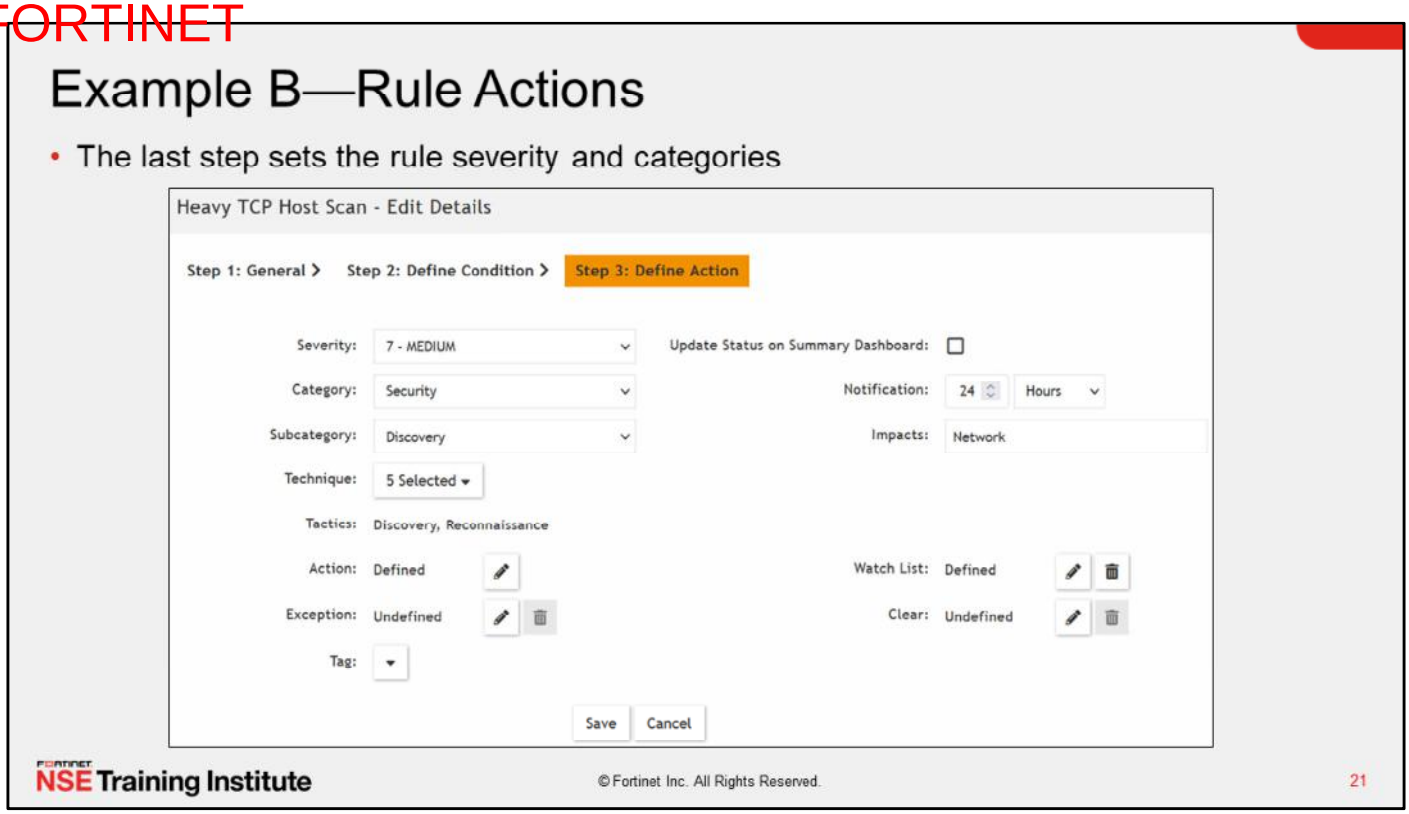
The aggregate condition in this rule is looking for 200 or more different destination IP addresses.

The aggregate condition is defined as **COUNT DISTINCT (Destination IP)** that is greater than or equal to 200, over the time period of 180-seconds (three minutes).

These results are going to be grouped by the same source IP. If the same device goes to 200 or more different destination IP addresses within 180 seconds, it triggers this rule.

Vouchers & Dumps are Available | WhatsApp +201224560923

DO NOT REPRINT
© FORTINET
Brave-dumps.com



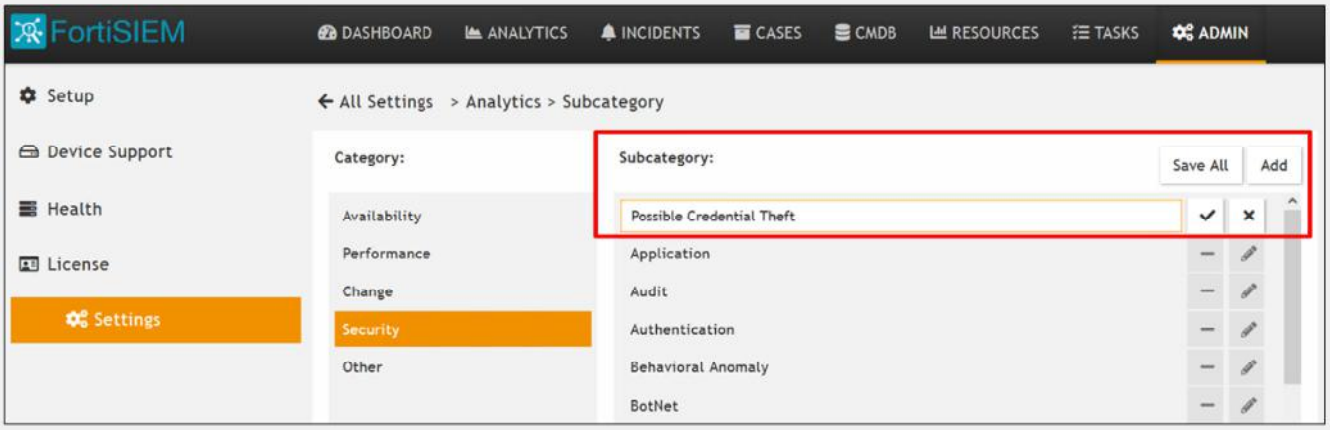
The third step sets the action criteria for the rule. You can select **Severity** to associate with the incident triggered by the rule. You should select the **Category** of incidents to be triggered by the rule and the **Subcategory** from the available list based on the selected incident **Category**.

Vouchers & Dumps are Available | WhatsApp +201224560923

DO NOT REPRINT
© FORTINET
Brave-dumps.com

Rule Categories and Subcategories

- You can define custom subcategories under **ADMIN > Settings > Analytics > Subcategory**



NSE Training Institute © Fortinet Inc. All Rights Reserved. 22

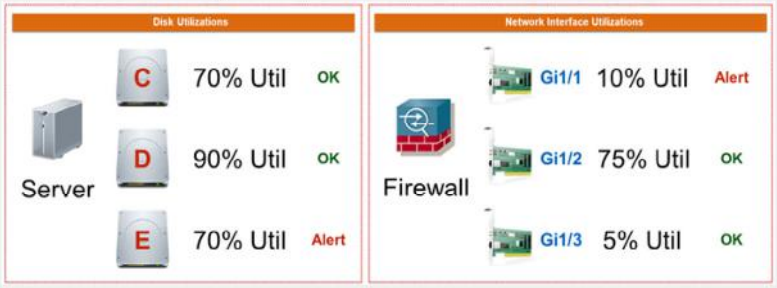
FortiSIEM groups incidents into different categories—**Availability**, **Change**, **Performance**, **Security**, and **Other**. The system assigns a category to every rule and you can search any incident using these categories. The system defines a subcategory for every system-defined rule. You can add a subcategory for custom rules and also create new subcategories. You can search incidents using both categories and subcategories.

Vouchers & Dumps are Available | WhatsApp +201224560923

DO NOT REPRINT
© FORTINET
Brave-dumps.com

Introducing Threshold-Based Rules

- In your network, there are differences in the loads and utilizations of hardware and software components across devices
- What if you want to be alerted to different utilization values for each interface on a router, or to different utilization values for each disk on a database server, rather than using the same thresholds across all objects?



- FortiSIEM includes global thresholds and per-device-object thresholds for specific PAM metrics

NSE Training Institute

© Fortinet Inc. All Rights Reserved.

23

In your network, there are differences in the loads and utilizations of hardware and software components across many different devices.

What if you want to be alerted to different utilization values for each interface on a router, or to different utilization values for each disk on a database server, rather than using the same thresholds across all device components?

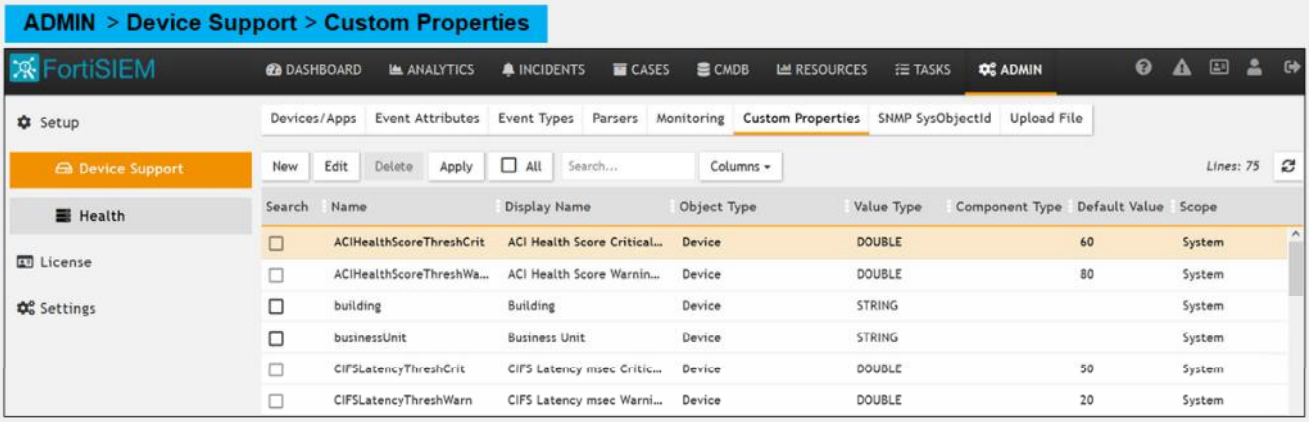
It's for exactly these types of requirements that FortiSIEM includes global thresholds and per-device-object thresholds, for specific PAM metrics.

Vouchers & Dumps are Available | WhatsApp +201224560923

DO NOT REPRINT Brave-dumps.com
© FORTINET

Global Threshold Values

- Globally applied metric thresholds that the rules engine references by default
- Typically two values: **warning** and **critical**
- Separate thresholds for servers, network devices, storage devices, and so on

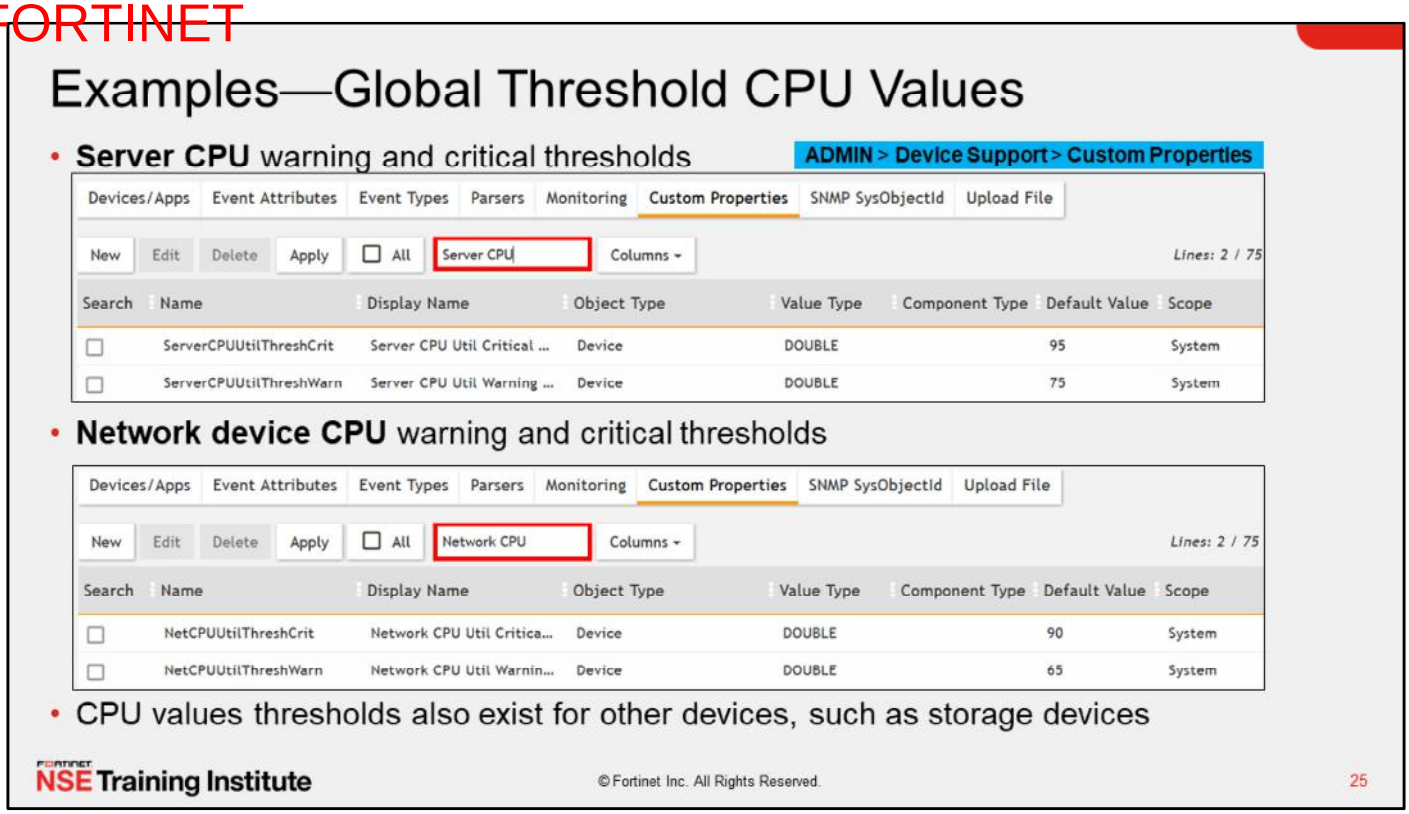


NSE Training Institute
© Fortinet Inc. All Rights Reserved.

You can find the global thresholds on the **Custom Properties** tab, under **ADMIN** > **Device Support**. As the name implies, global thresholds are globally applied metric thresholds**.** The rules engine references these values by default. Typically, you will see two values for these thresholds: a global threshold for warning, and a global threshold for critical. There are separate warning and critical thresholds for servers, network devices, storage devices, and so on.

Vouchers & Dumps are Available | WhatsApp +201224560923

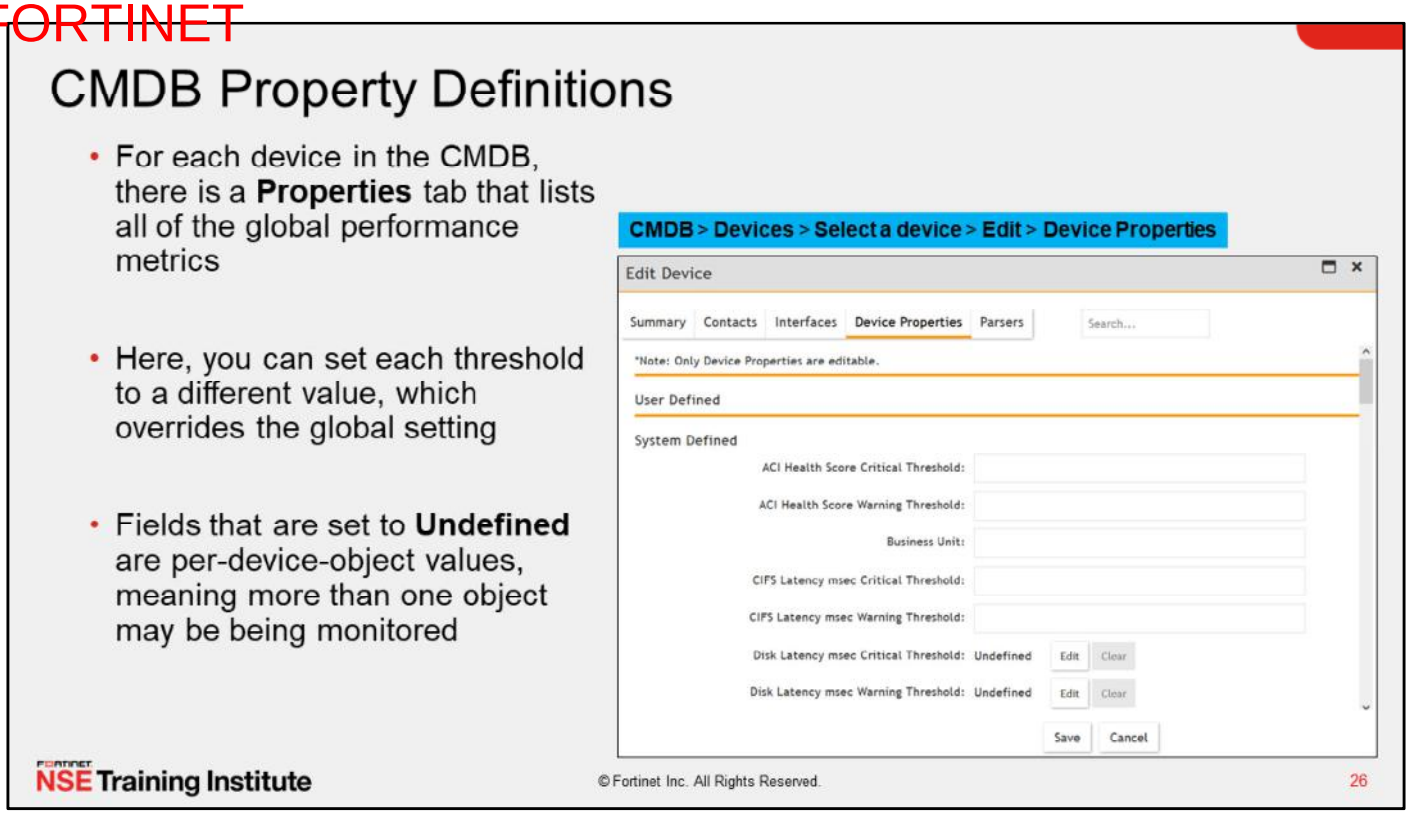
DO NOT REPRINT
© FORTINET
Brave-dumps.com



If you search for the word `server CPU`, you see the warning and critical threshold default values related to the server CPU, which the rules engine references. Alternatively, if you searched for `NetCPU`, you see the network-related warning and critical network CPU default values. The system also includes CPU values for other devices.

Vouchers & Dumps are Available | WhatsApp +201224560923

DO NOT REPRINT
© FORTINET
Brave-dumps.com

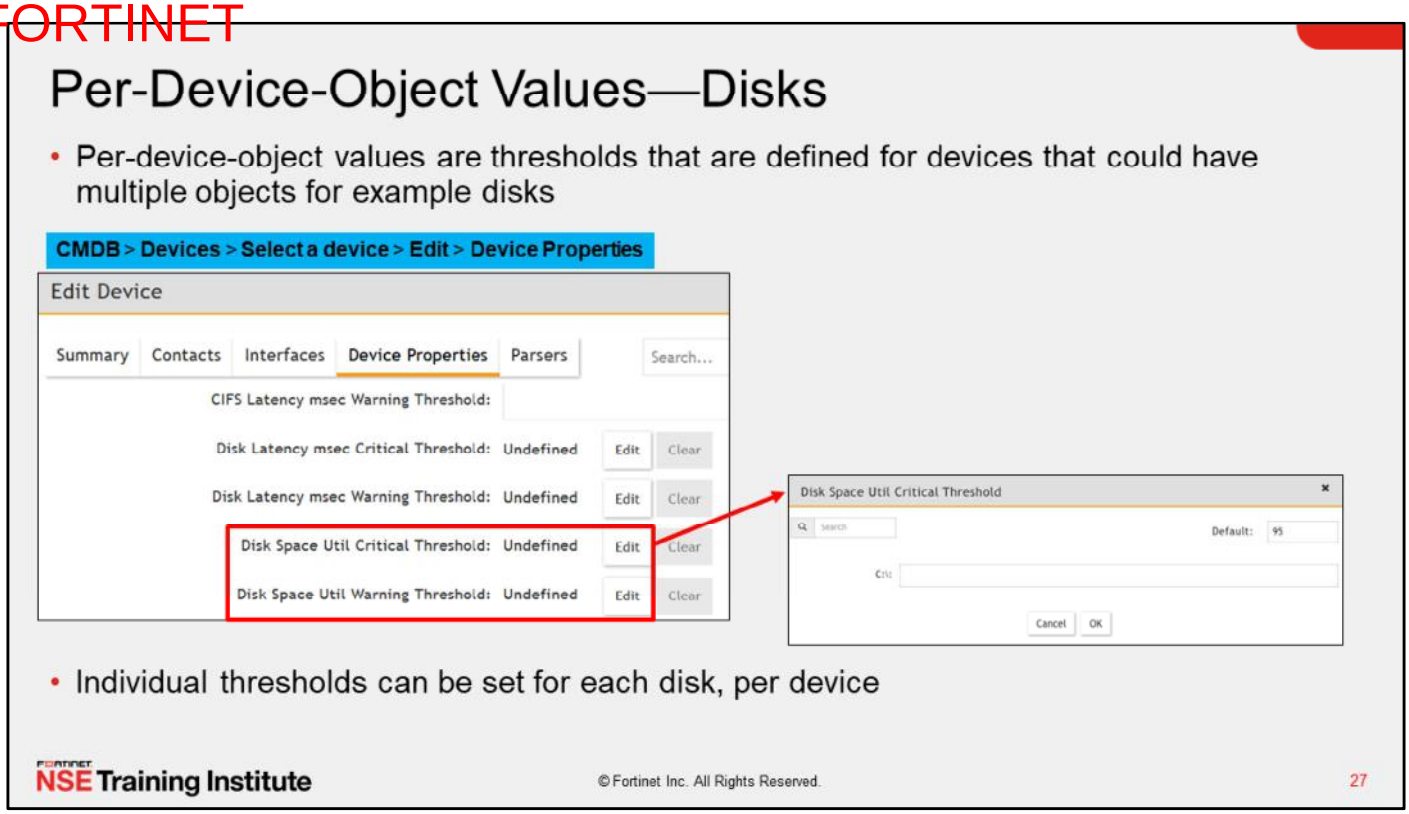


For each device in the CMDB, there is a **Properties** tab that lists all of the global performance metrics-related thresholds. On this tab, you can set each threshold to a different value. These settings override the global settings. Click **CMDB** > **Select a device** > **Edit** > **Properties**.

Fields that are set to **Undefined** are known as per-device-object values. This means that there may be more than one object being monitored, such as multiple discs on a server, or multiple interfaces on a router or switch.

Vouchers & Dumps are Available | WhatsApp +201224560923

DO NOT REPRINT
© FORTINET
Brave-dumps.com

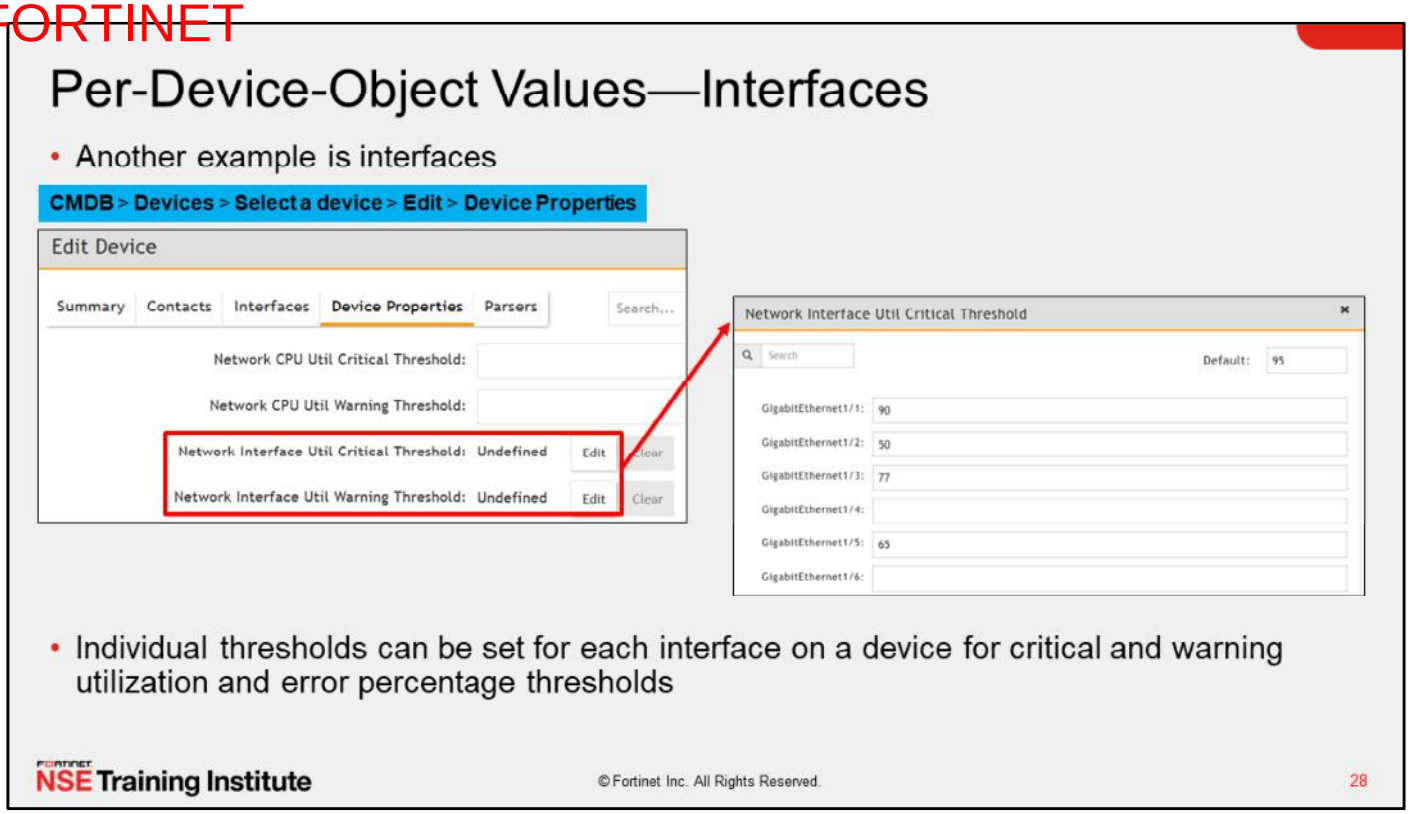


As previously stated, per-device-object values are thresholds that are defined for devices that have multiple objects, such as interfaces or disks.

If you've performed a discovery on these devices, then this detail is in the CMDB. If you select **Edit** on one of these per-device thresholds, you see a list of all of the components that use that threshold on this device, which you can then set individual threshold values for.

Vouchers & Dumps are Available | WhatsApp +201224560923

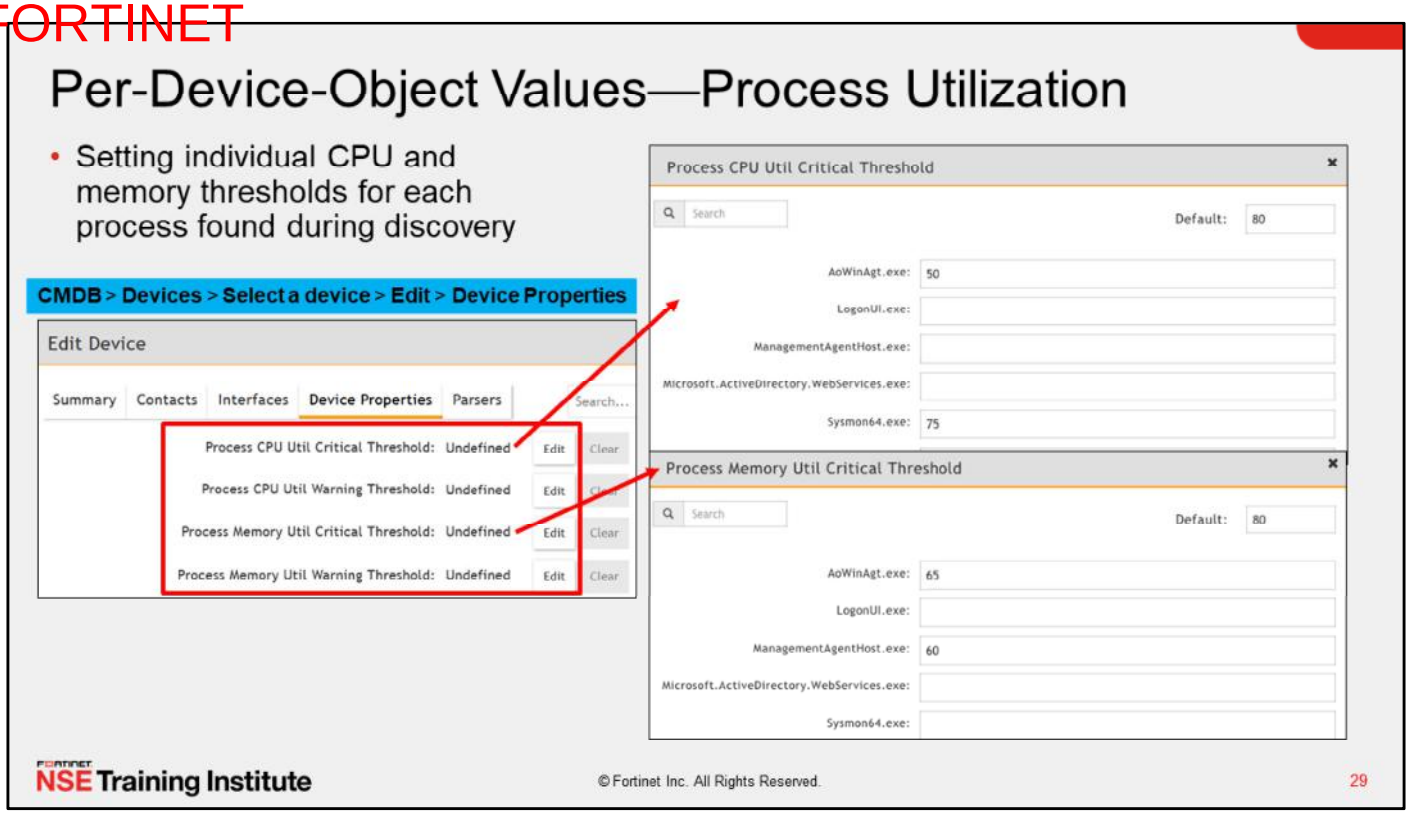
DO NOT REPRINT
© FORTINET
Brave-dumps.com



Setting the network interface threshold value is another example of per-device-object values. You can set individual thresholds for each interface on a device for critical and warning utilization and error percentage thresholds. You can configure rules to trigger based on those threshold values.

Vouchers & Dumps are Available | WhatsApp +201224560923

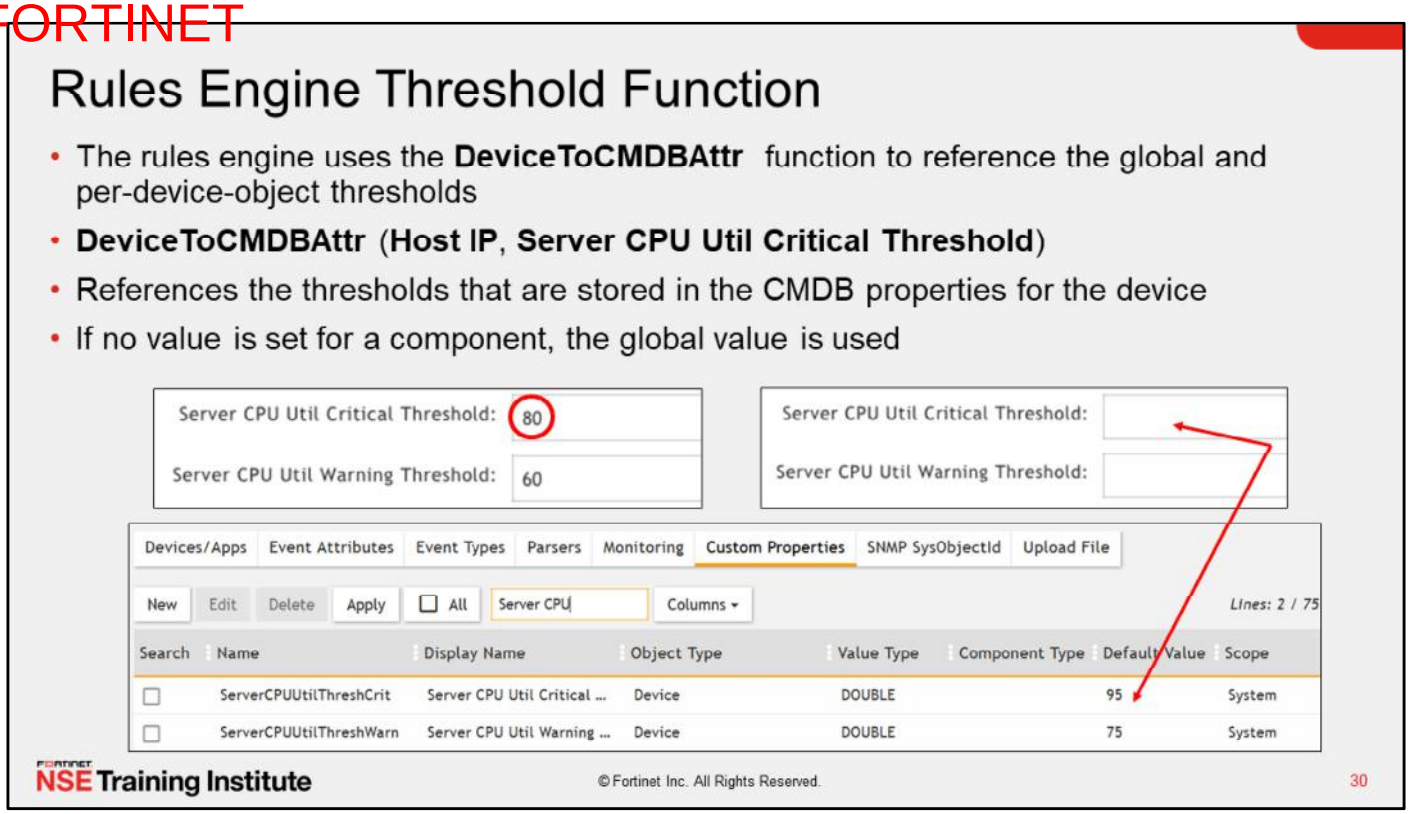
DO NOT REPRINT Brave-dumps.com
© FORTINET



Process utilization is another commonly used per-device-object value. You can set process utilization threshold values for CPU and memory for devices, and monitor those thresholds by configuring rules. FortiSIEM can generate an alert if resource utilization exceeds those threshold values.

Vouchers & Dumps are Available | WhatsApp +201224560923

DO NOT REPRINT
© FORTINET
Brave-dumps.com



The rules engine uses a function to reference the global and per-device-object values. The function is called **DeviceToCMDBAttr**.

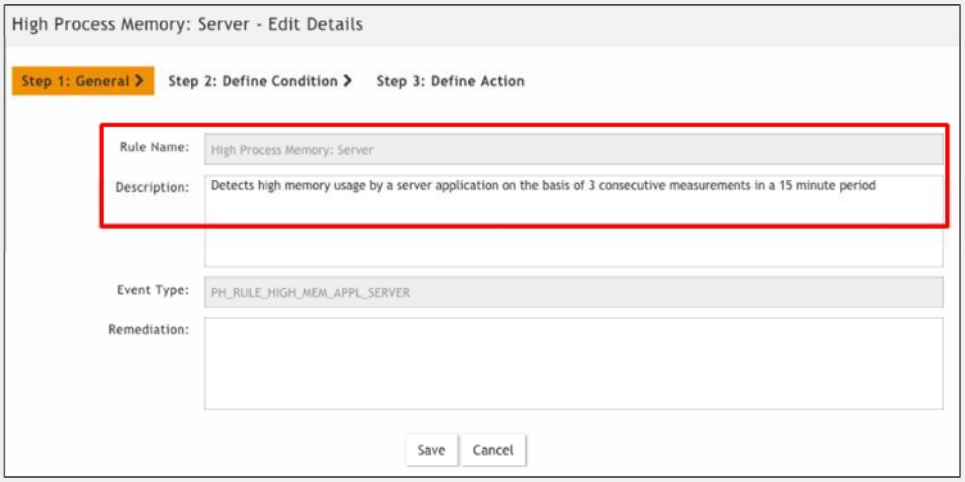
When the rules engine calls this function, it passes along a couple of parameters: the host IP and the attribute to look up. In the example shown on this slide, the attribute is **Server CPU Util Critical Threshold**. The function looks up that attribute in the CMDB for that device. If a value is set, then the function uses that value; otherwise, if a value is not set, the function references the global value for that component.

Vouchers & Dumps are Available | WhatsApp +201224560923

DO NOT REPRINT
© FORTINET
Brave-dumps.com

Example C

- For the rule: **High Process Memory: Server**



NSE Training Institute

© Fortinet Inc. All Rights Reserved.

31

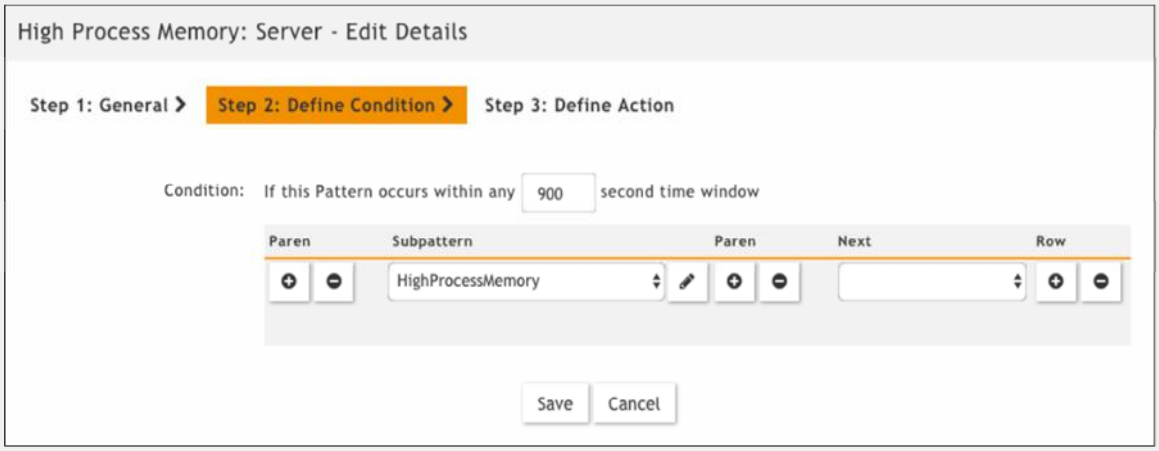
This slide shows an example of the **High Process Memory: Server** rule, which detects high memory usage by a server application on the basis of three consecutive measurements in a 15-minute period.

Vouchers & Dumps are Available | WhatsApp +201224560923

DO NOT REPRINT
© FORTINET
Brave-dumps.com

Example C—Subpattern and Time Window

- Is tracking a single subpattern named: **HighProcessMemory**
- Over a 900-second (15-minute) time window



NSE Training Institute

© Fortinet Inc. All Rights Reserved.

32

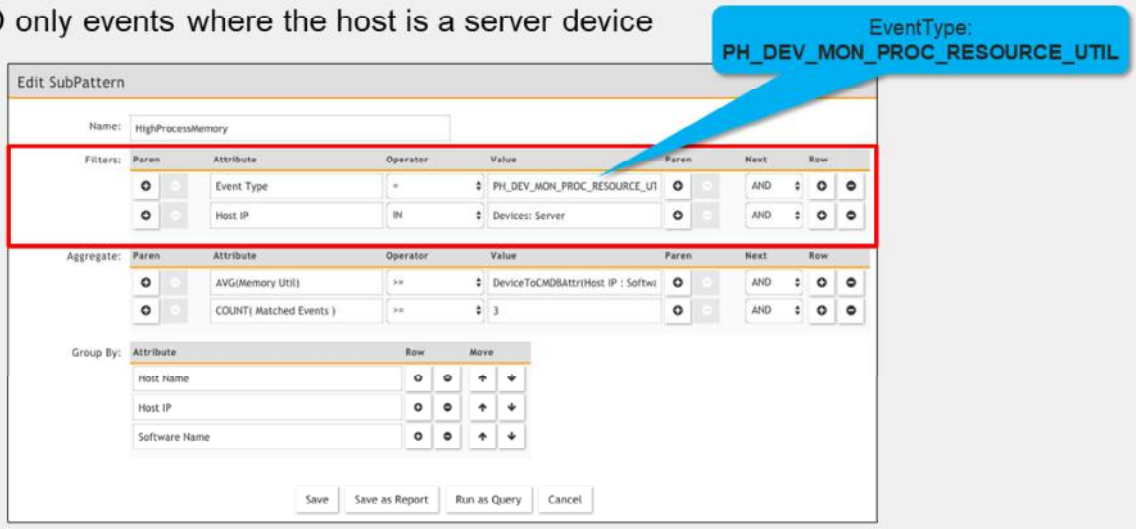
The **Subpattern** for this rule is **HighProcessMemory** which tracks high memory usage over a 15-minute time window.

Vouchers & Dumps are Available | WhatsApp +201224560923

DO NOT REPRINT
© FORTINET
Brave-dumps.com

Example C—Subpattern Filter

- The filter is defined to look for events that are device monitoring process resource utilization events (CPU and memory usage reported for every process)
- AND only events where the host is a server device



© Fortinet Inc. All Rights Reserved.

The example on this slide shows a performance and availability-related rule that that references global values. This rule is for high-memory usage on a server. It is looking at events that are device monitoring, process resource utilization events.

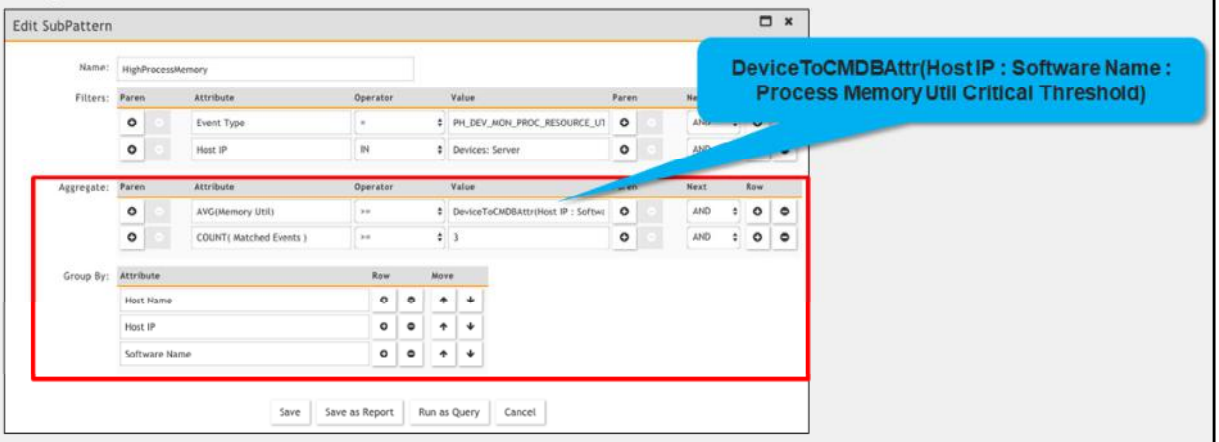
This event collects CPU and memory usage reported for every process on a server device, where the host IP is in the server device category in the CMDB.

Vouchers & Dumps are Available | WhatsApp +201224560923

DO NOT REPRINT
© FORTINET
Brave-dumps.com

Example C—Aggregation and Group By

- Rule will trigger if based on at least three or more matching events, the **AVG(Memory Utilization)** is greater than either the global threshold or individual process (software name) object override
- **Grouped By** the same **Host Name**, **Host IP**, and **Software Name**



NSE Training Institute

© Fortinet Inc. All Rights Reserved.

34

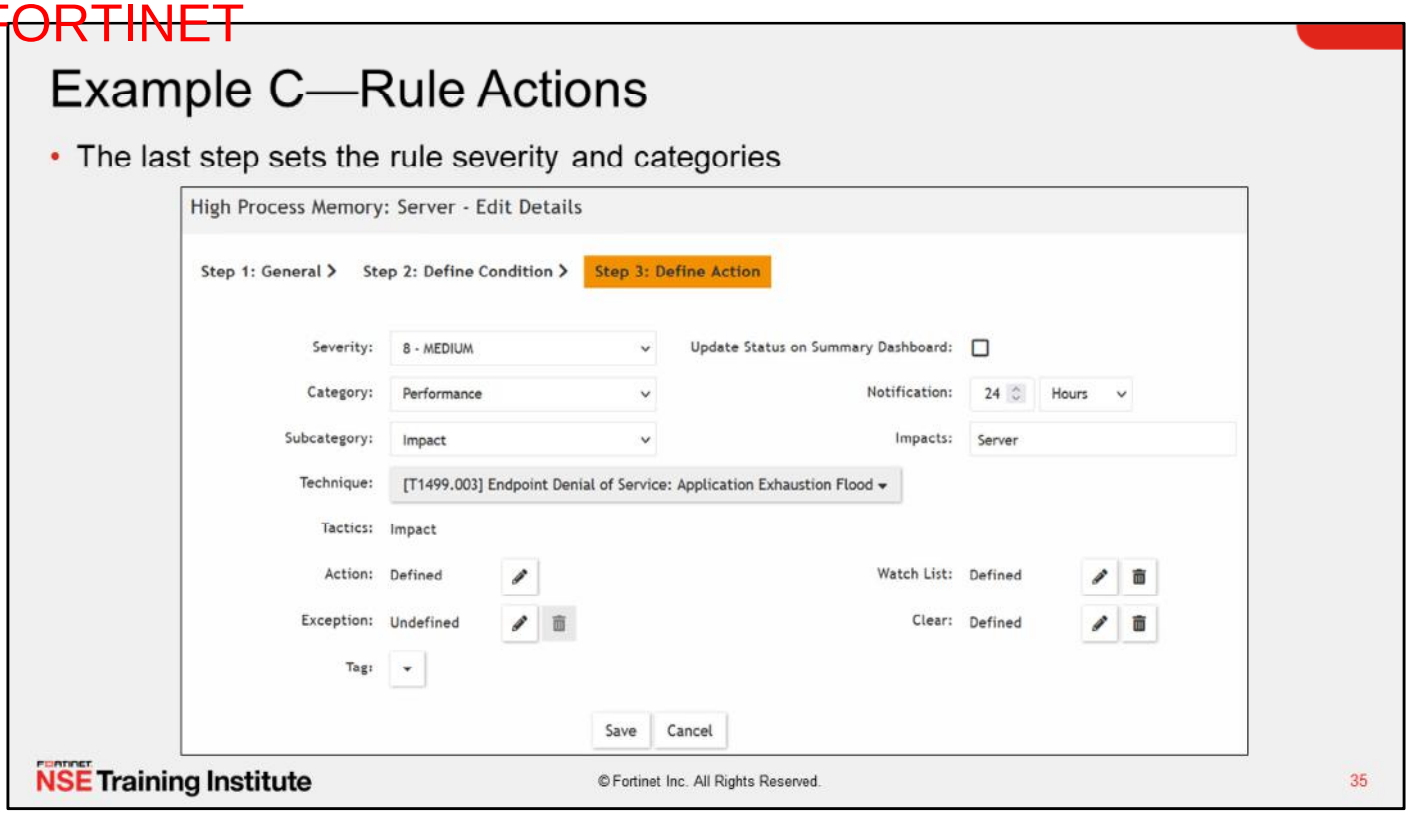
Rule triggers if based on at least three or more matching events, the **AVG(Memory Utilization)** is greater than either the global threshold or individual process (software name) object override.

The **Group By** condition for this rule is to group matching events by the same host name, host IP, and application name.

If you think about it, you could be monitoring hundreds or even thousands of server devices in your network, all sending these events. So, the grouping operation helps to ensure that you are looking at events coming from the same host and the same application.

Vouchers & Dumps are Available | WhatsApp +201224560923

DO NOT REPRINT Brave-dumps.com
© FORTINET

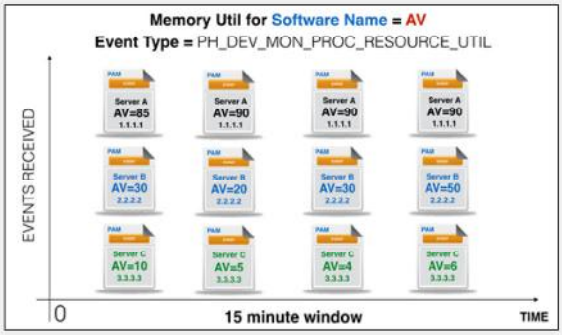


The third step sets the action criteria for the rule. You can select **Severity** to associate with the incident triggered by the rule. You should select the **Category** of incidents to be triggered by the rule and the **Subcategory** from the available list based on the selected incident **Category**.

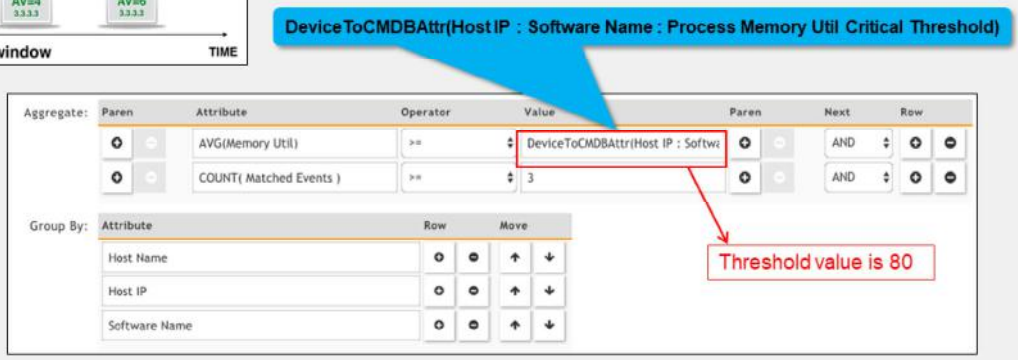
Vouchers & Dumps are Available | WhatsApp +201224560923

DO NOT REPRINT
© FORTINET
Brave-dumps.com

Example C—How Many Incidents?



- In this example, over a 15-minute time period, FortiSIEM collects four process resource utilization events for three servers, and all three servers are running the same antivirus application, named *AV*



NSE Training Institute

© Fortinet Inc. All Rights Reserved.

36

Still using the rule from the previous example, consider a 15-minute time period during which FortiSIEM collects four process resource utilization events from three different servers. Call them server A , server B, and server C. All three servers are running an antivirus application that you will call *AV*.

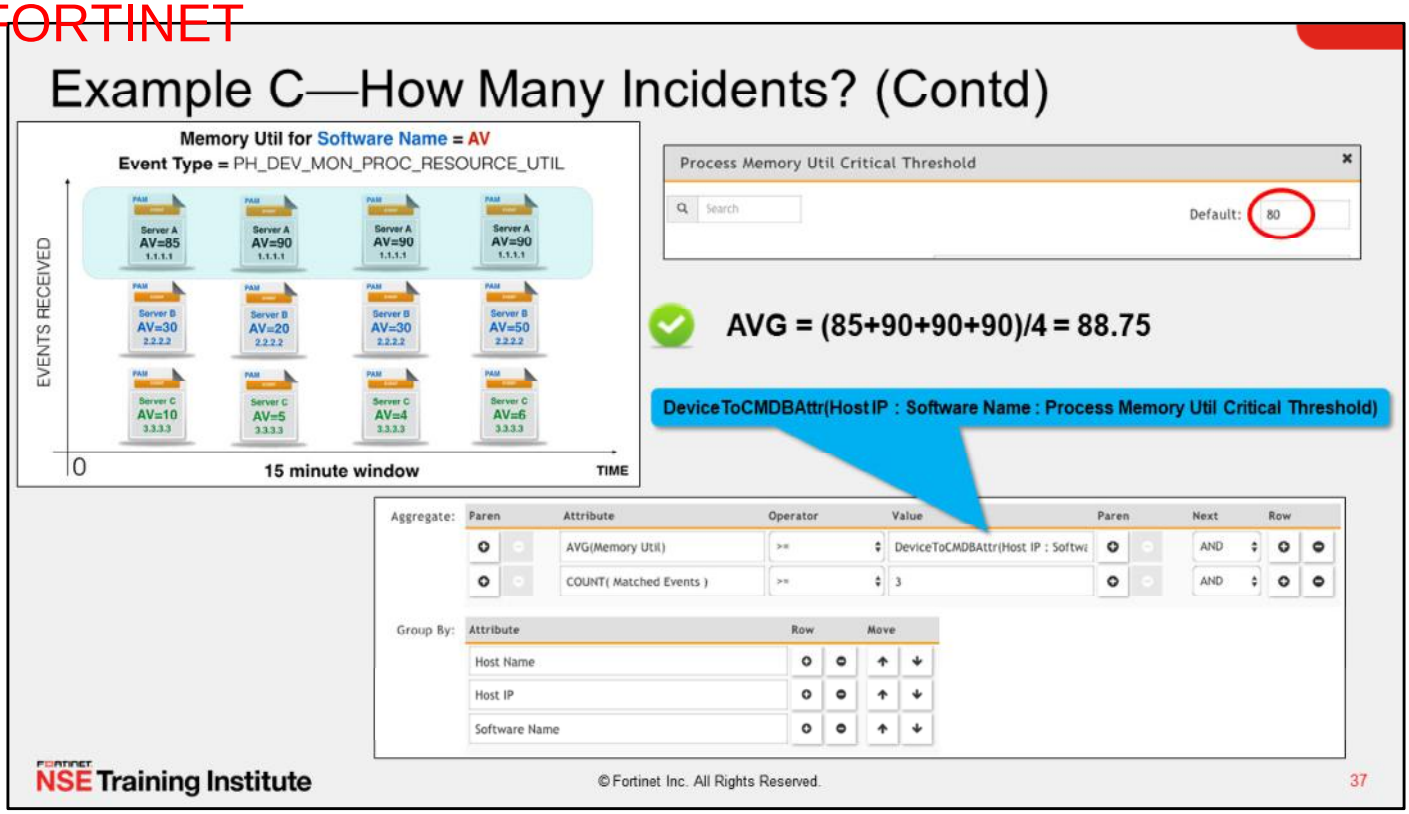
If you look at the aggregate condition, you want the average memory utilization to be equal to or greater than 80, and get at least three or more matching events within the 15-minute time period to trigger this rule.

The results are grouped by the host name, host IP, and application name.

How many incidents are generated in this example?

Vouchers & Dumps are Available | WhatsApp +201224560923

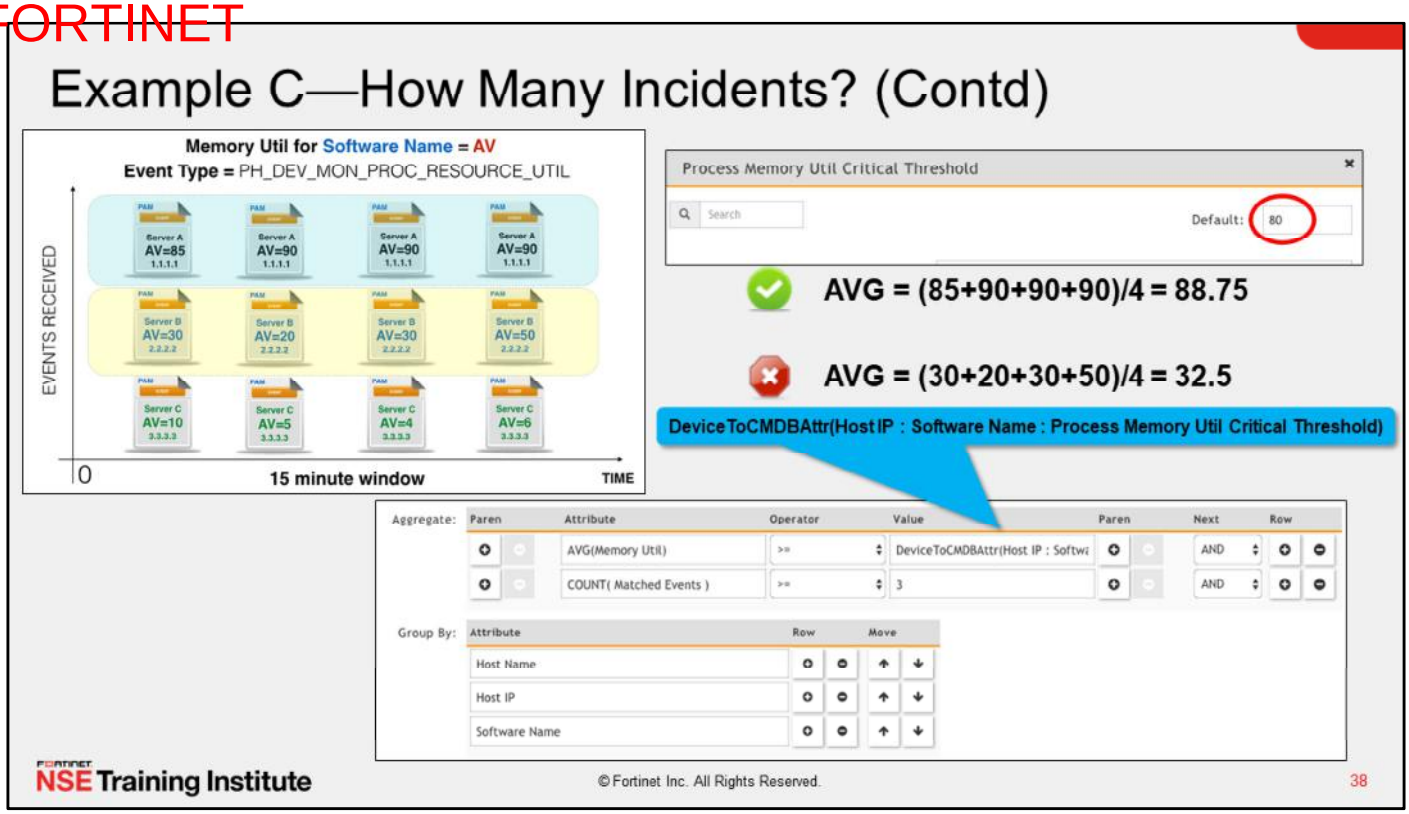
DO NOT REPRINT Brave-dumps.com
© FORTINET



If you look at server A, there are four events that match the filter criteria. The average of those four events is, 85+90+90+90, divided by the number of events, which is four. That gives you a value of 88.75. Is this value greater than 80? Yes it is, so this is an incident that triggers the rule for server A, for the AV application.

Vouchers & Dumps are Available | WhatsApp +201224560923

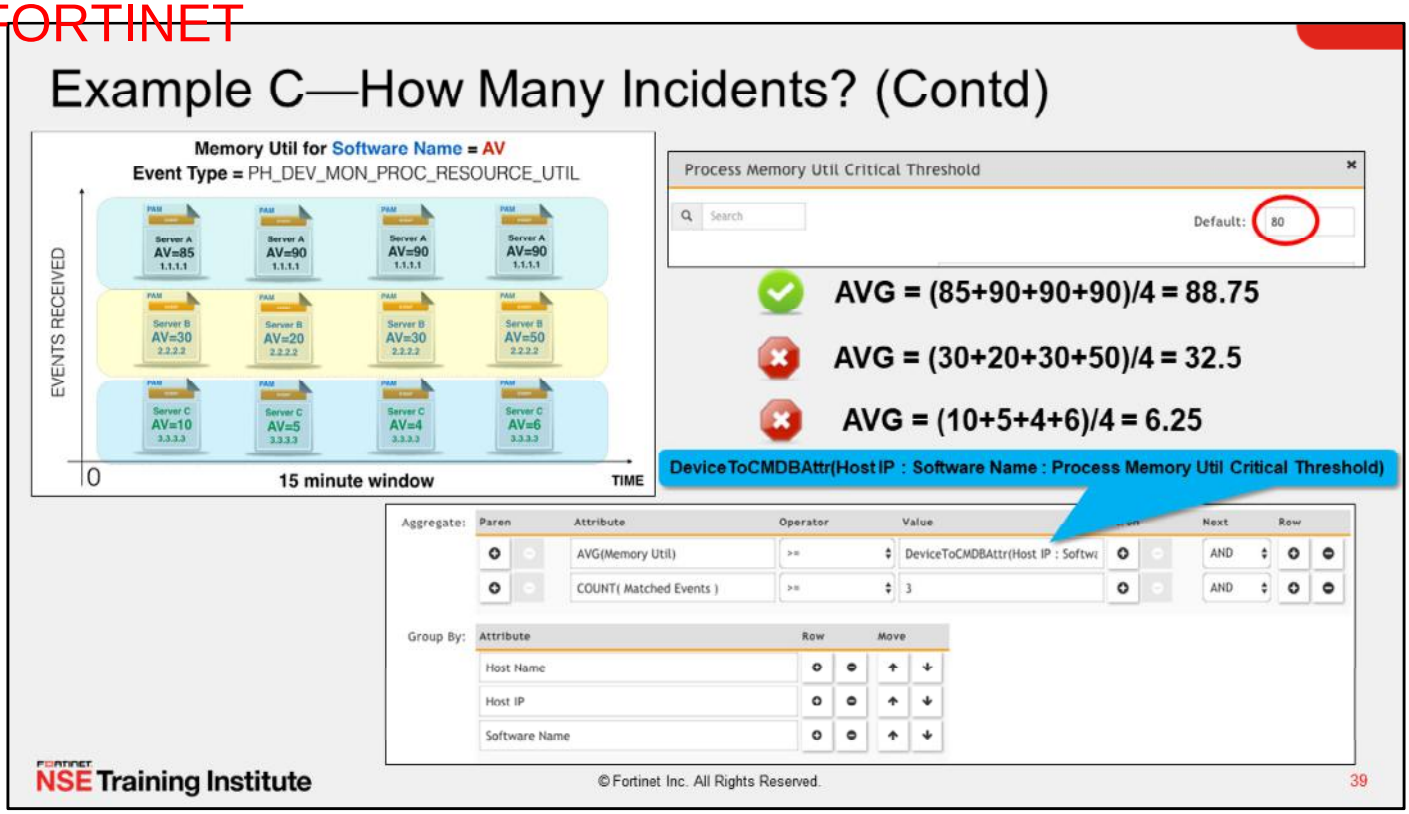
DO NOT REPRINT
© FORTINET
Brave-dumps.com



When you look at server B, you can see that there are also four events that match the filter criteria. The average of those four events is 32.5. This isn't equal to or greater than 80, so this does not trigger the rule and therefore does not generate an incident for server B.

Vouchers & Dumps are Available | WhatsApp +201224560923

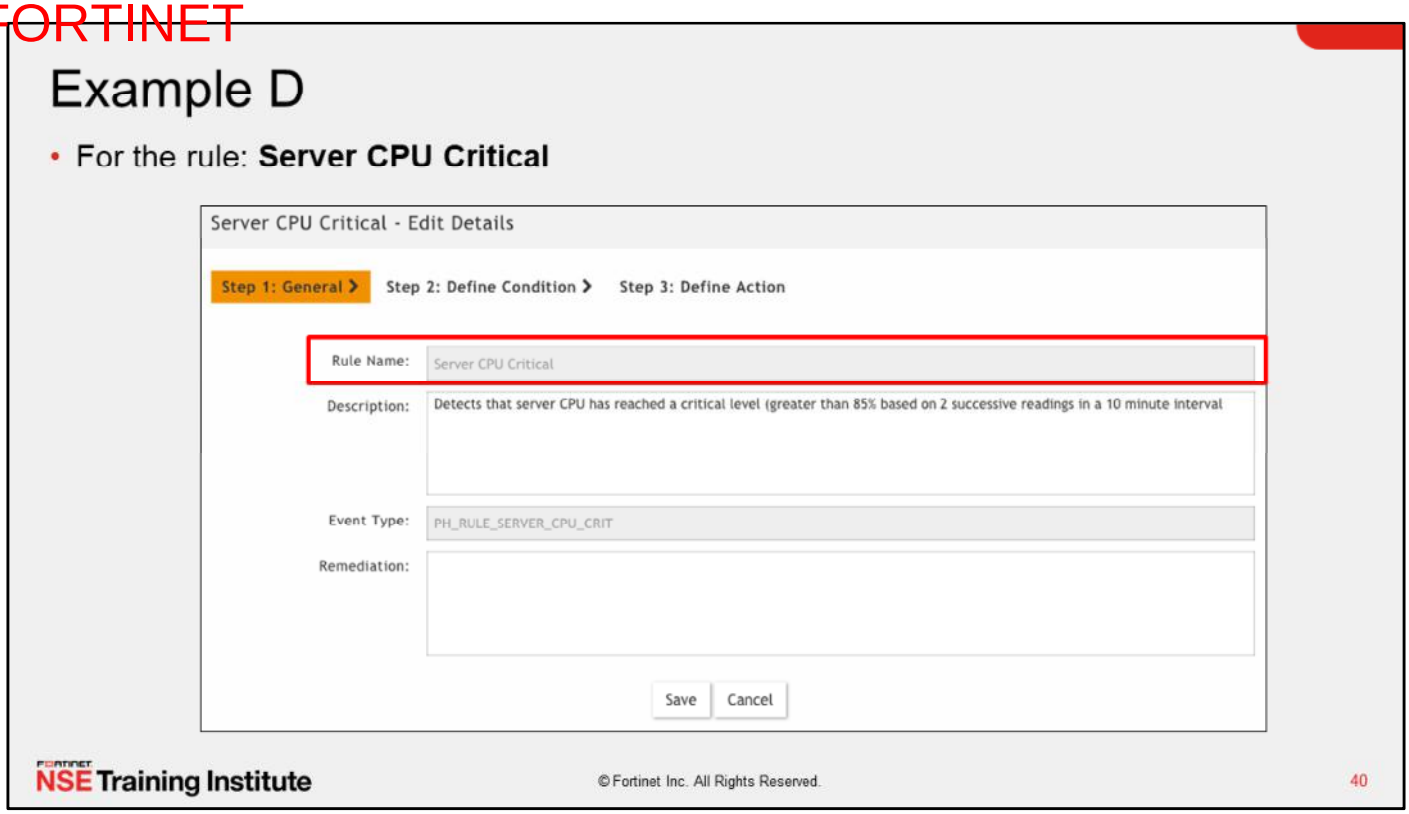
DO NOT REPRINT
© FORTINET
Brave-dumps.com



The same is true for server C. There are four events, and the average of those four events is to only 6.25. Again, this is less than the required condition, so there is no incident for server C.

Vouchers & Dumps are Available | WhatsApp +201224560923

DO NOT REPRINT
© FORTINET
Brave-dumps.com



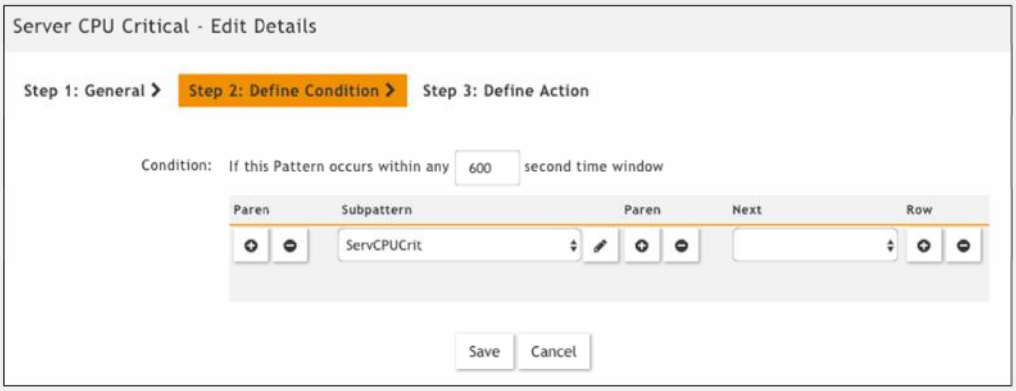
This is an example of the **Server CPU Critical** rule which detects that server CPU has reached a critical level (greater than 85% based on two successive readings in a 10-minute interval).

Vouchers & Dumps are Available | WhatsApp +201224560923

DO NOT REPRINT
© FORTINET
Brave-dumps.com

Example D—Subpattern and Time Window

- Is tracking a single subpattern named: **ServCPUCrit**
- Over a 600-second (10-minute) time window



NSE Training Institute

© Fortinet Inc. All Rights Reserved.

41

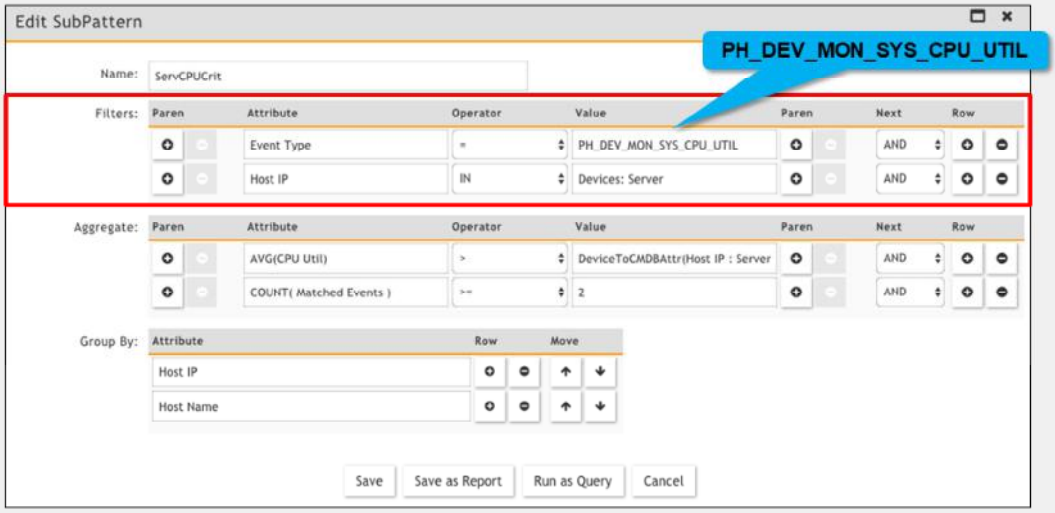
The rule is tracking a single subpattern **ServCPUCrit** over a 600-second (10-minute) time window.

Vouchers & Dumps are Available | WhatsApp +201224560923

DO NOT REPRINT
© FORTINET
Brave-dumps.com

Example D—Subpattern Filter

- The filter is defined to look for events that are device monitoring CPU utilization events AND only from hosts that are server devices



NSE Training Institute
© Fortinet Inc. All Rights Reserved.
42

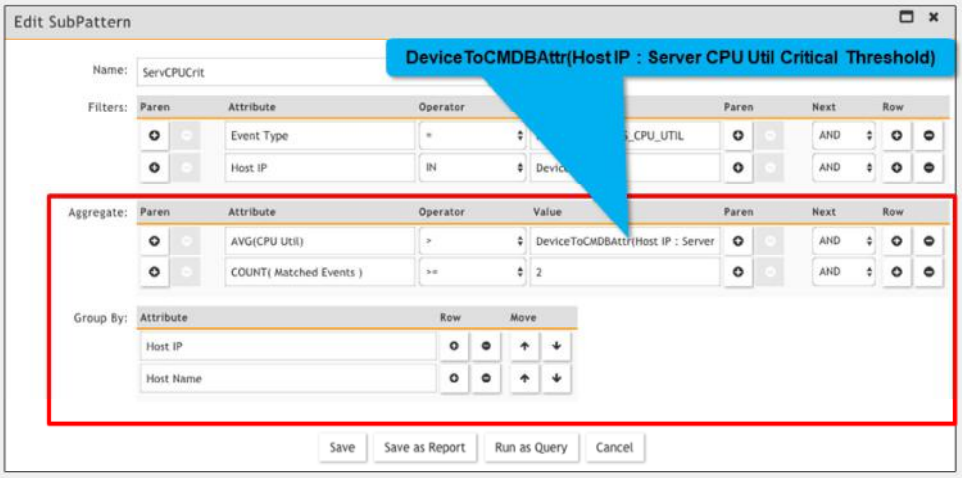
The subpattern is looking for a particular event type, PH_DEV_MON_SYS_CPU_UTIL, coming only from server devices.

Vouchers & Dumps are Available | WhatsApp +201224560923

DO NOT REPRINT
© FORTINET
Brave-dumps.com

Example D—Aggregation and Group By

- Rule triggers if based on at least two or more matching events if the **AVG(CPU Utilization)** is greater than either the global threshold or device object override
- **Grouped By** the same **Host Name**, **Host IP**



NSE Training Institute

© Fortinet Inc. All Rights Reserved.

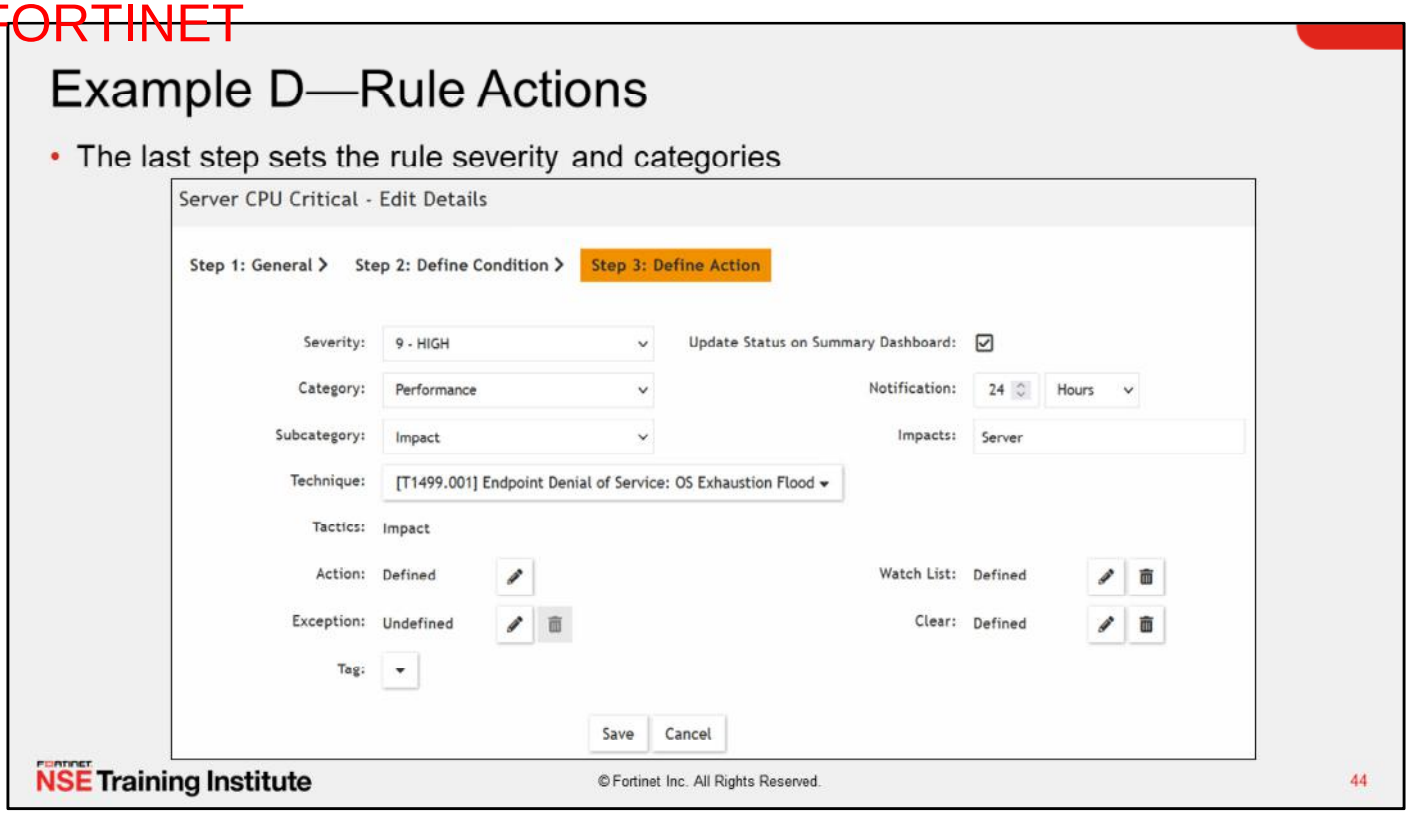
43

The aggregate condition for this rule looks for two or more events that match the filter criteria and, for those matching events, calculates the average CPU utilization. Once it has calculated the average, identify if it is greater than either the global threshold or device object override, over a specified time period. For this rule, the time period is 600 seconds.

The results are grouped by the same host IP and host name. Make sure you calculate the average for the same device.

Vouchers & Dumps are Available | WhatsApp +201224560923

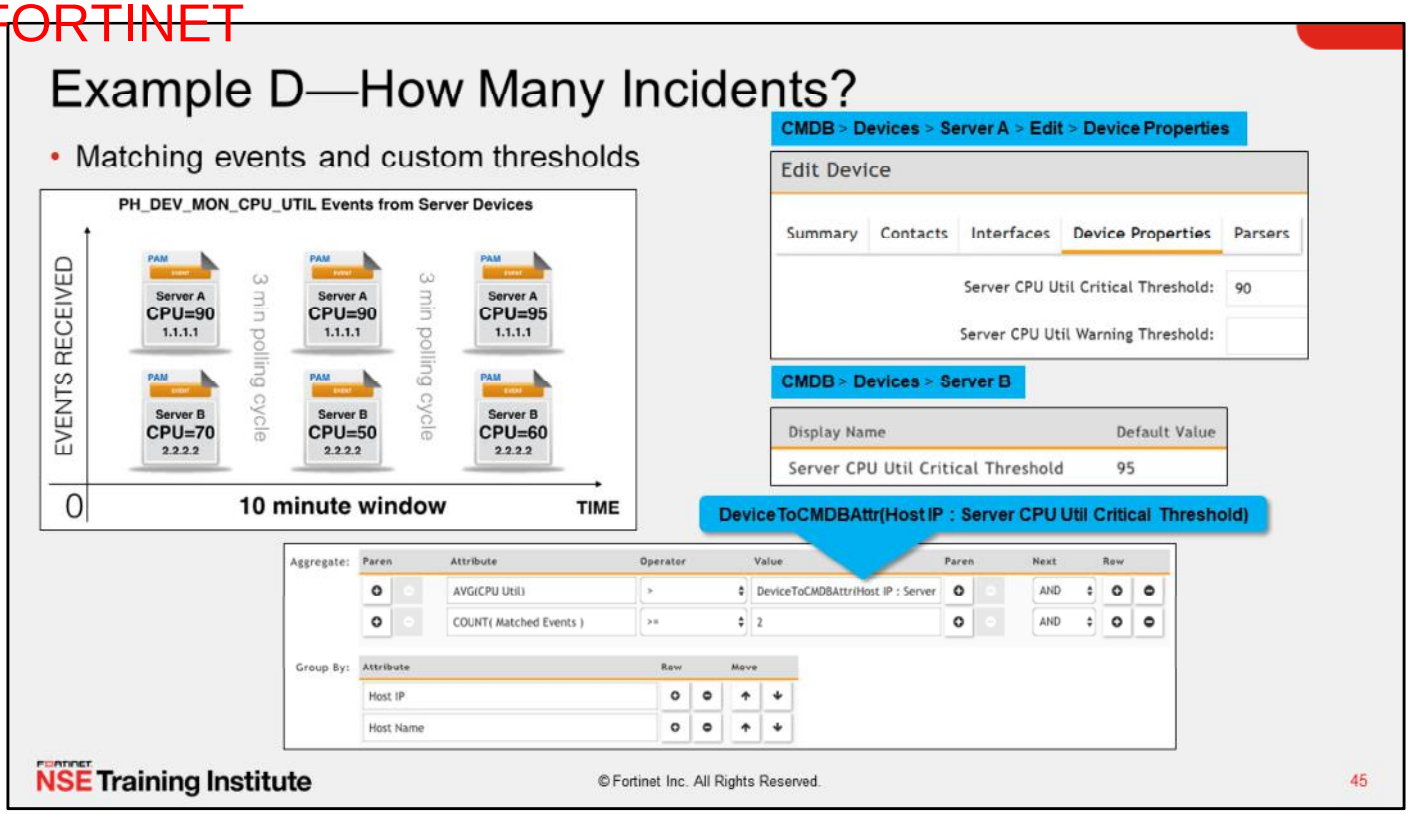
DO NOT REPRINT
© FORTINET
Brave-dumps.com



The third step sets the action criteria for the rule. You can select **Severity** to associate with the incident triggered by the rule. You should select the **Category** of incidents to be triggered by the rule and the **Subcategory** from the available list based on the selected incident **Category**.

Vouchers & Dumps are Available | WhatsApp +201224560923

DO NOT REPRINT
© FORTINET
Brave-dumps.com

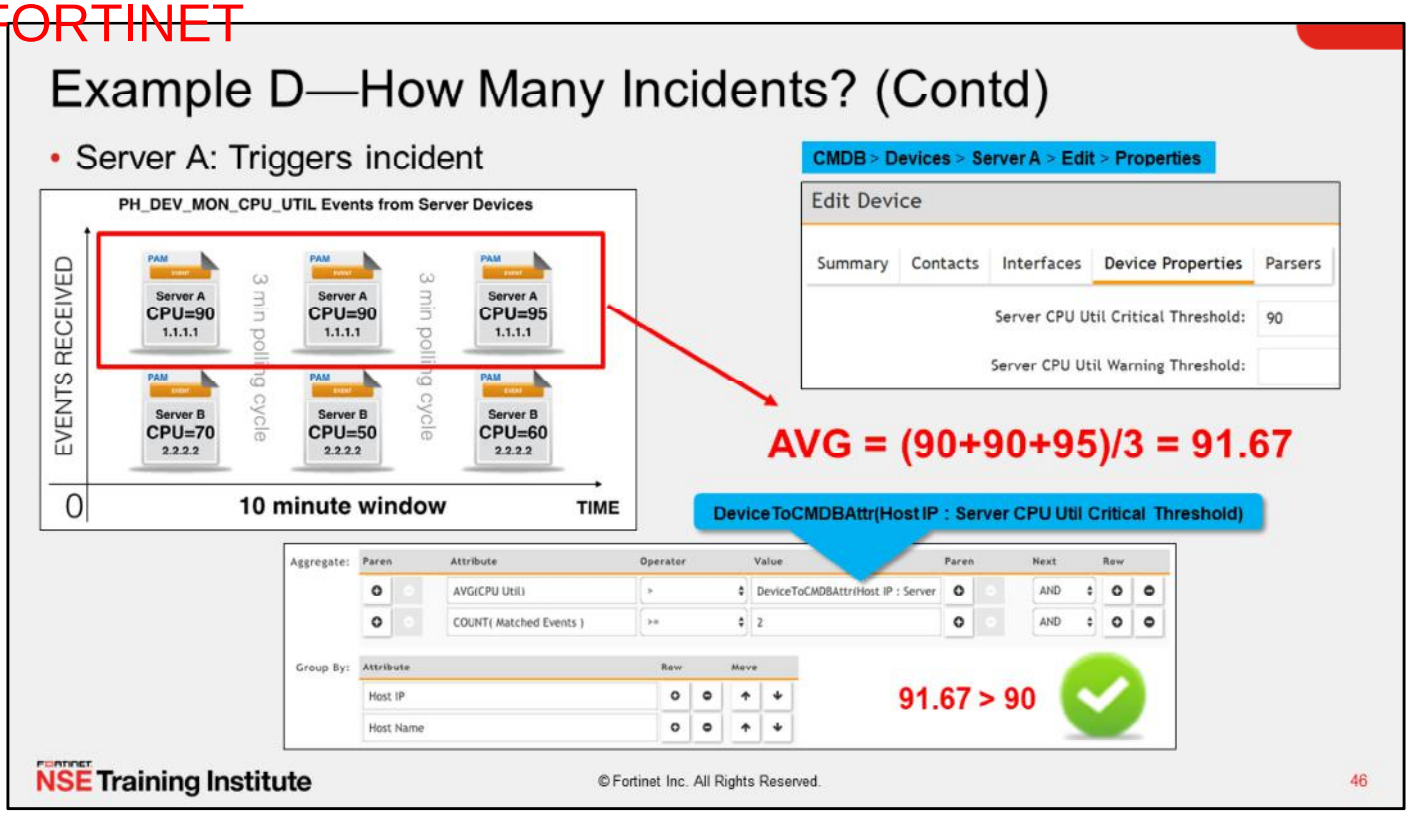


In the example shown on this slide, there are three events for two server devices, server A and server B, collected over a 10-minute time window. In the CMDB, you override the default values for the server CPU utilization critical threshold. The threshold value for server A is set to 90 and set to 95 for server B.

How many incidents do you think will be generated?

Vouchers & Dumps are Available | WhatsApp +201224560923

DO NOT REPRINT
© FORTINET
Brave-dumps.com

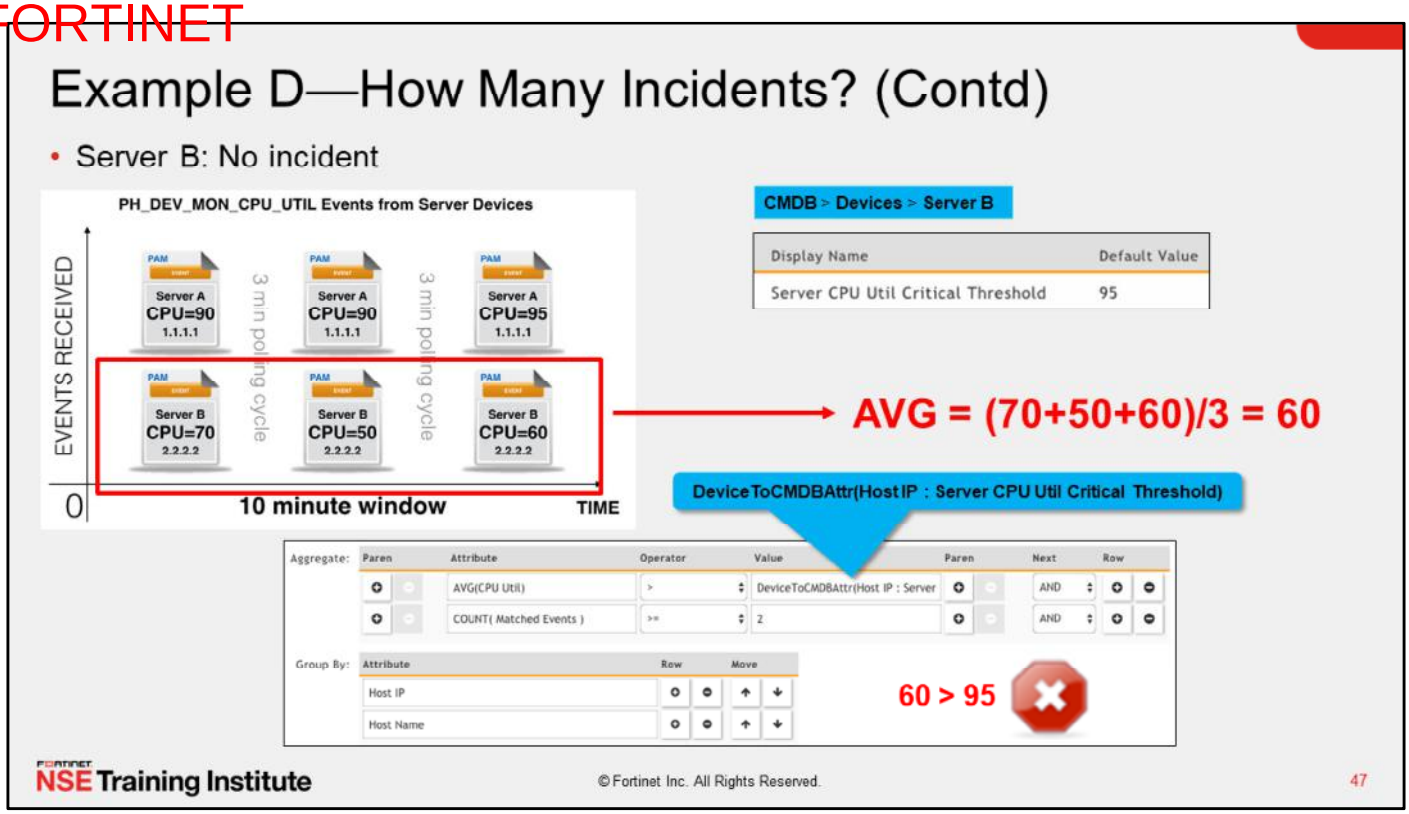


In the example shown on this slide, there are three events for two server devices, server A and server B, collected over a 10-minute time window. In the CMDB, you override the default values for the server CPU utilization critical threshold. The threshold value for server A is set to 90 and set to 95 for server B.

How many incidents do you think will be generated for server A?
One incident will be created, because the average value is 91.67, which is greater than the threshold value of 90.

Vouchers & Dumps are Available | WhatsApp +201224560923

DO NOT REPRINT
© FORTINET
Brave-dumps.com



In the example shown on this slide, there are three events for two server devices, server A and server B, collected over a 10-minute time window. In the CMDB, you override the default values for the server CPU utilization critical threshold. The threshold value for server A is set to 90 and set to 95 for server B.

How many incidents do you think will be generated server B?
No incidents will be created, because the average value is 60, which is not greater than the threshold value of 95.

Vouchers & Dumps are Available | WhatsApp +201224560923

DO NOT REPRINT
© FORTINET
Brave-dumps.com

Knowledge Check

1. A subpattern for a rule is defined by_____.
   - ✓ A. Filters, aggregation, group by definitions
   - B. Filters, aggregation, time window definitions
   - C. Filters, threshold, time window definitions

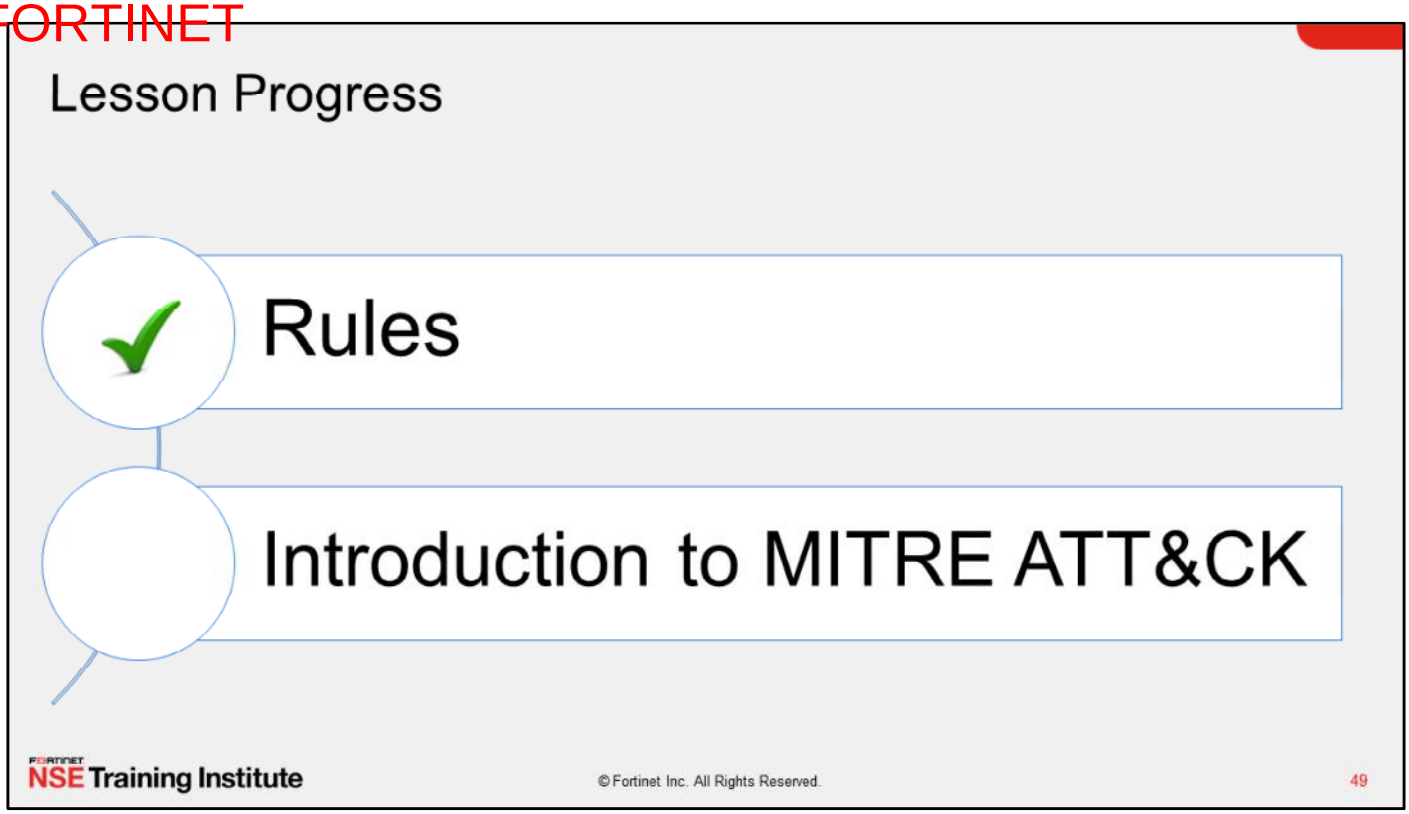
NSE Training Institute

© Fortinet Inc. All Rights Reserved.

48

Vouchers & Dumps are Available | WhatsApp +201224560923

DO NOT REPRINT
© FORTINET
Brave-dumps.com

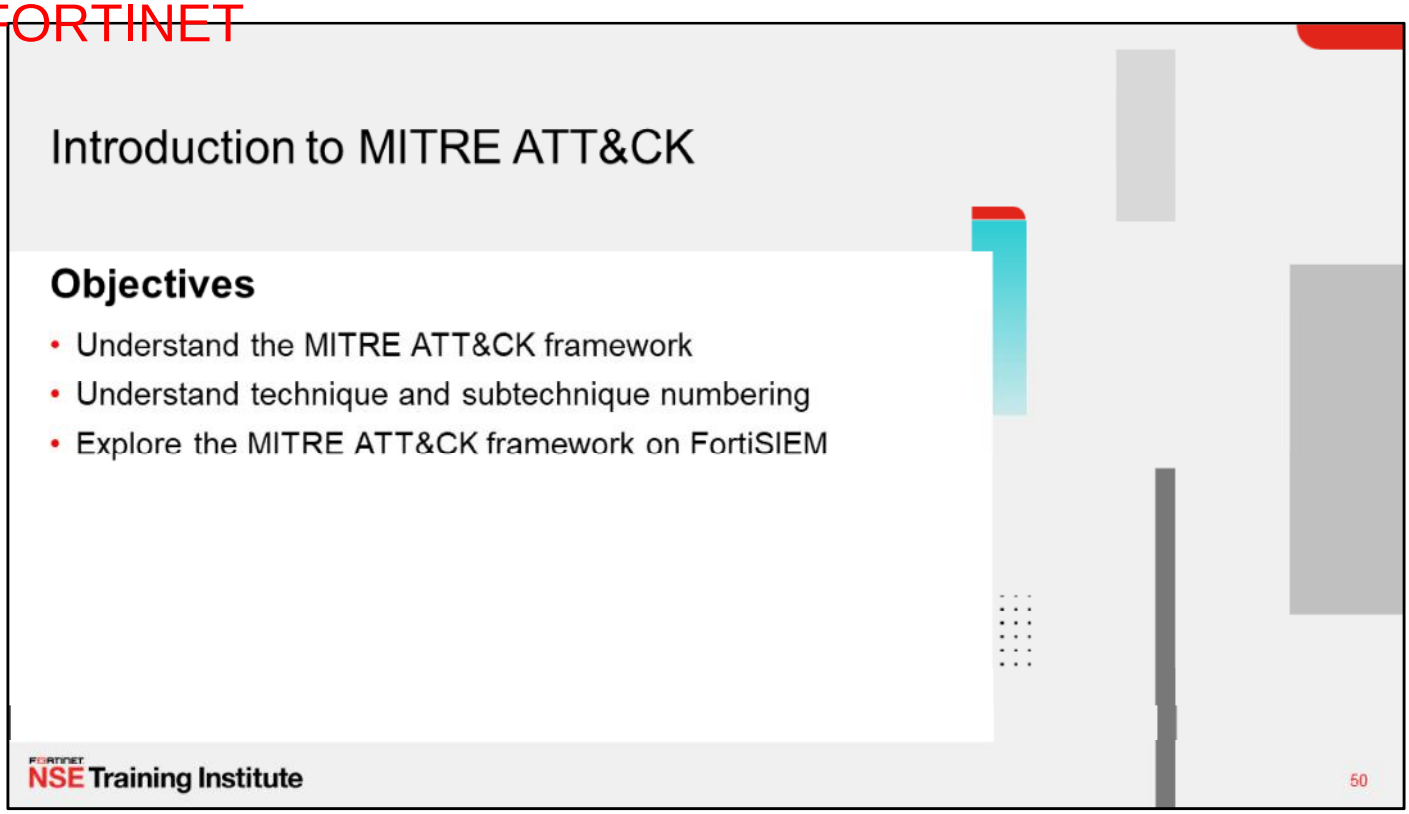


Good job! You now understand rules.

Now, you'll learn about the MITRE ATT&CK framework and various tactics and techniques.

Vouchers & Dumps are Available | WhatsApp +201224560923

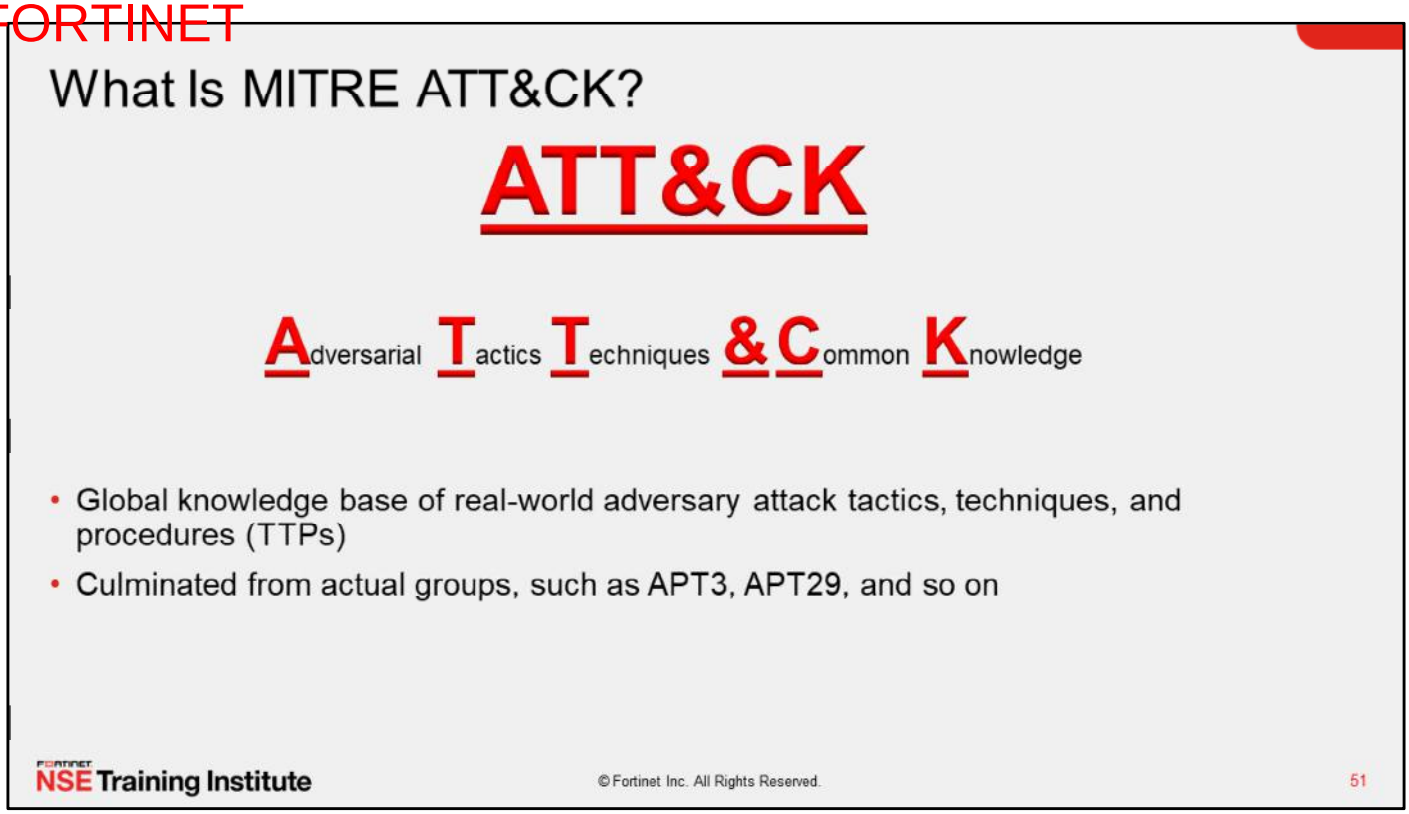
DO NOT REPRINT
© FORTINET
Brave-dumps.com



After completing this section, you should be able to achieve the objectives shown on this slide.

Vouchers & Dumps are Available | WhatsApp +201224560923

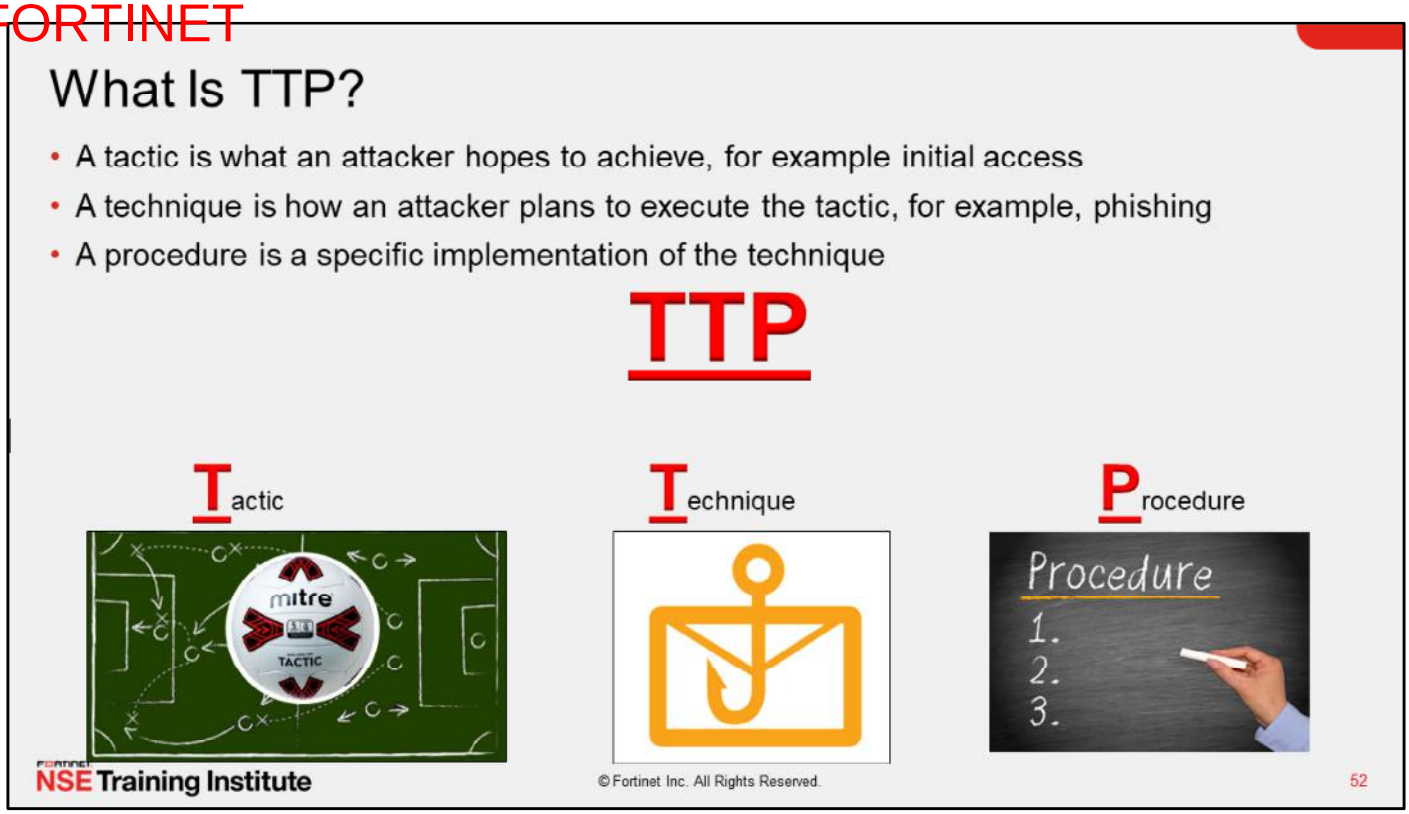
DO NOT REPRINT
© FORTINET
Brave-dumps.com



MITRE ATT&CK is a global knowledge base of real-world adversary attack TTPs. The knowledge base is populated with popular attacks and techniques used by various attack groups over the years, such as APT3, APT29, and so on. ATT&CK maps various techniques to tactics so that it becomes easy to identify similar attacks.

Vouchers & Dumps are Available | WhatsApp +201224560923

DO NOT REPRINT
© FORTINET
Brave-dumps.com



Very often SOC teams use the term TTP, which stands for tactics, technique, and procedure.

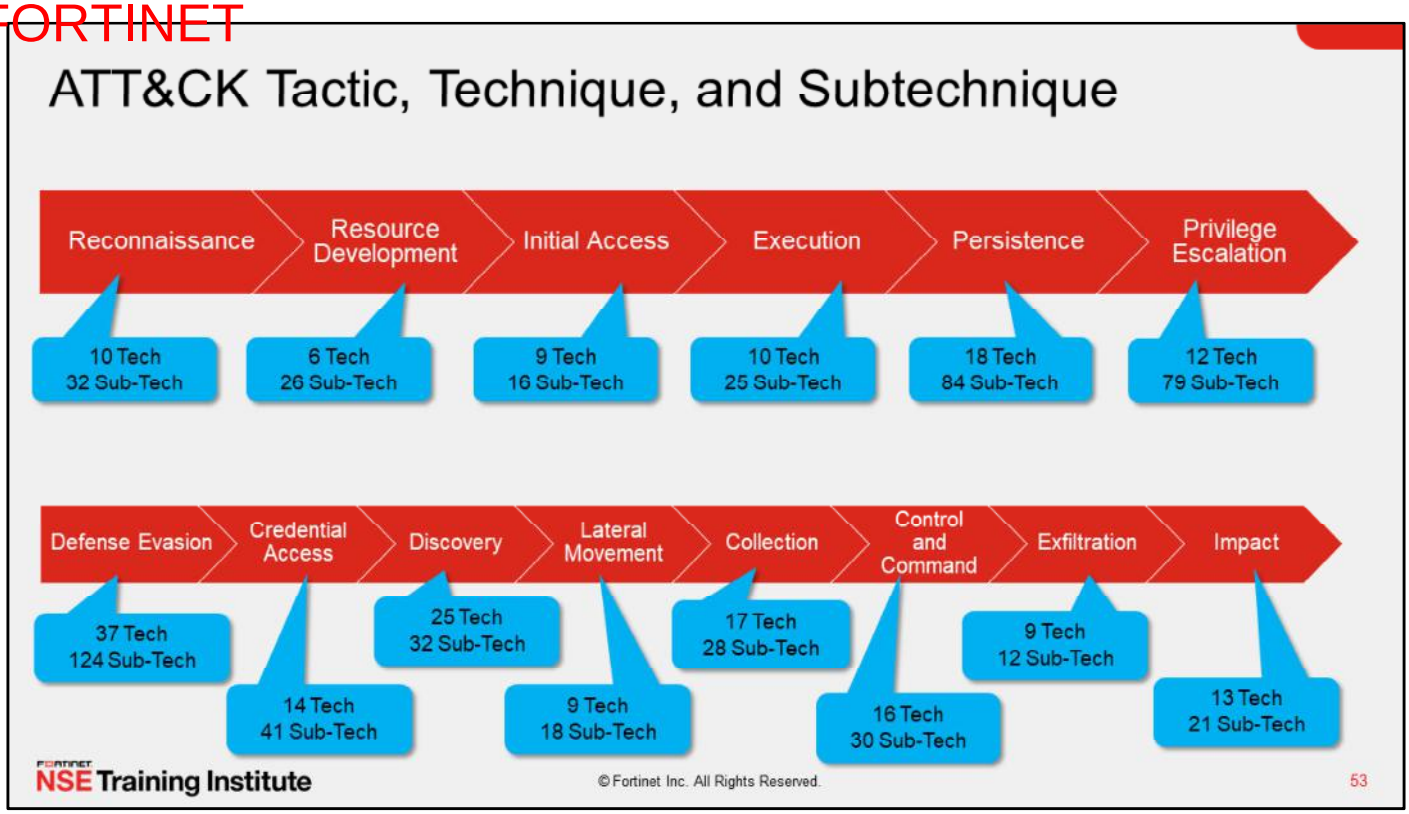
Tactics describe the immediate technical objectives the attackers are trying to achieve, such as gaining initial access, maintaining persistence, or establishing command and control. Invariably, attackers must use multiple tactics to successfully complete an attack.

Techniques describe the methods attackers use to achieve a tactic. All tactics in each matrix have multiple techniques. The enterprise matrix breaks some techniques down further into subtechniques. An example of this is the phishing technique attackers use to gain initial access. The three subtechniques associated with the phishing technique are spearphishing attachment, spearphishing link, and spearphishing through service.

Procedures describe the specific implementations of techniques and sub-techniques APTs have used (sometimes in clever or novel ways), or it can refer to specific malware or other tools attackers have used.

Vouchers & Dumps are Available | WhatsApp +201224560923

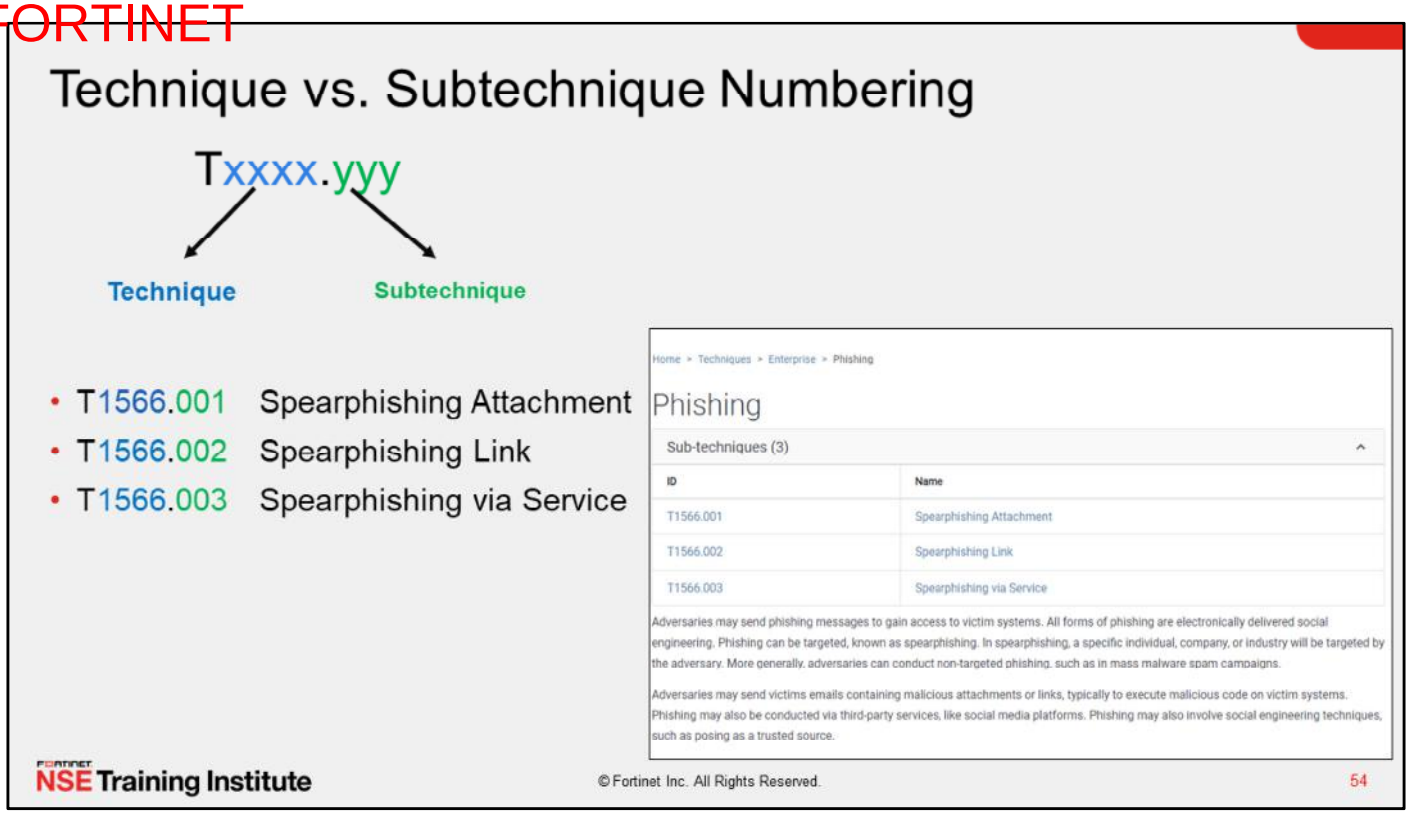
DO NOT REPRINT
© FORTINET
Brave-dumps.com



There are 14 different tactics. Each tactic has multiple techniques, and every technique may have several subtechniques.

Vouchers & Dumps are Available | WhatsApp +201224560923

DO NOT REPRINT
© FORTINET
Brave-dumps.com

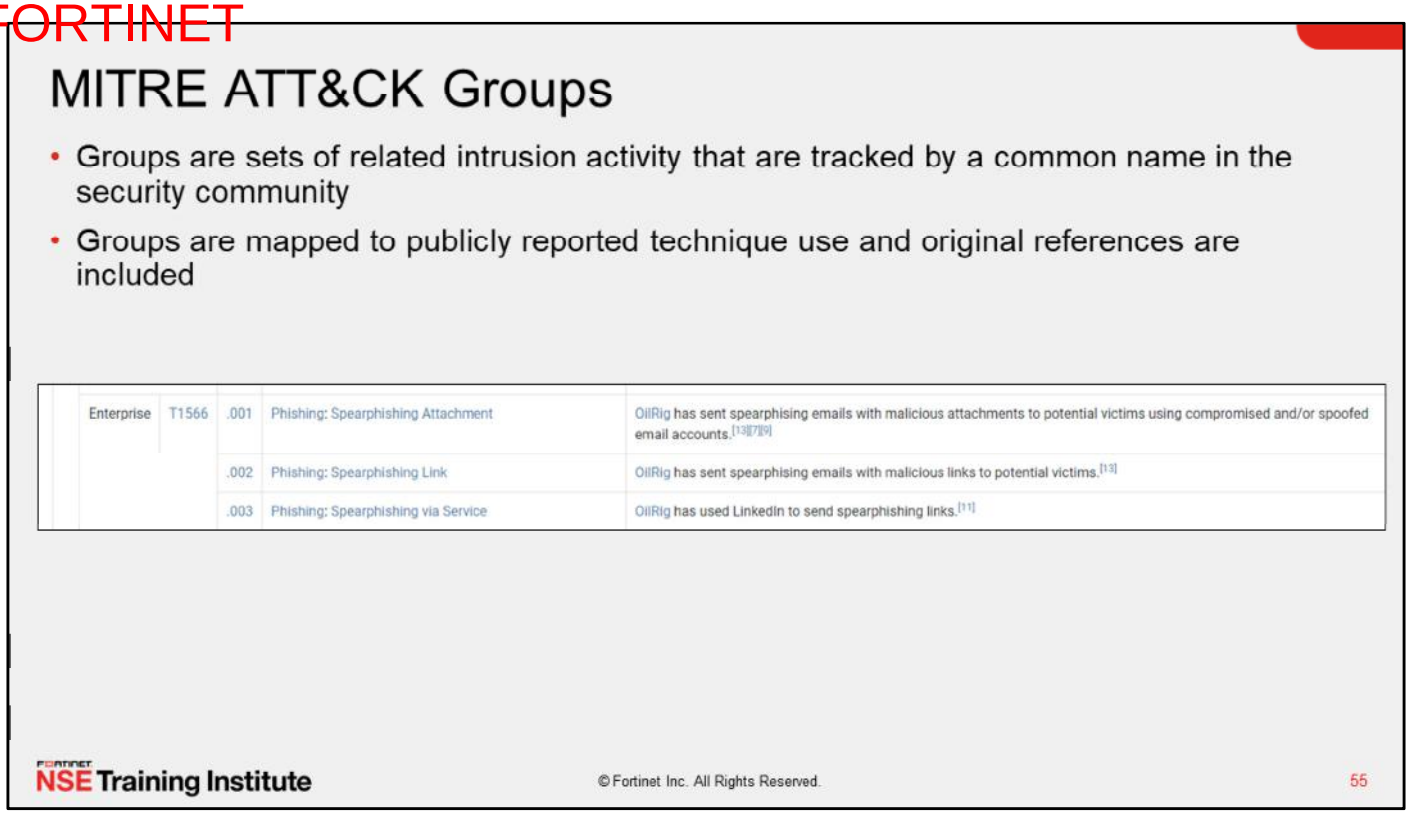


The technique numbering starts with the letter T followed by a four digit technique numbers. After the decimal there is a three-digit subtechnique number if there is a subtechnique associated with that technique.

For example, the phishing technique is T1566 and it has three different subtechniques called spearphishing attachment, spearphishing link, and spearphishing through service.

Vouchers & Dumps are Available | WhatsApp +201224560923

DO NOT REPRINT
© FORTINET
Brave-dumps.com

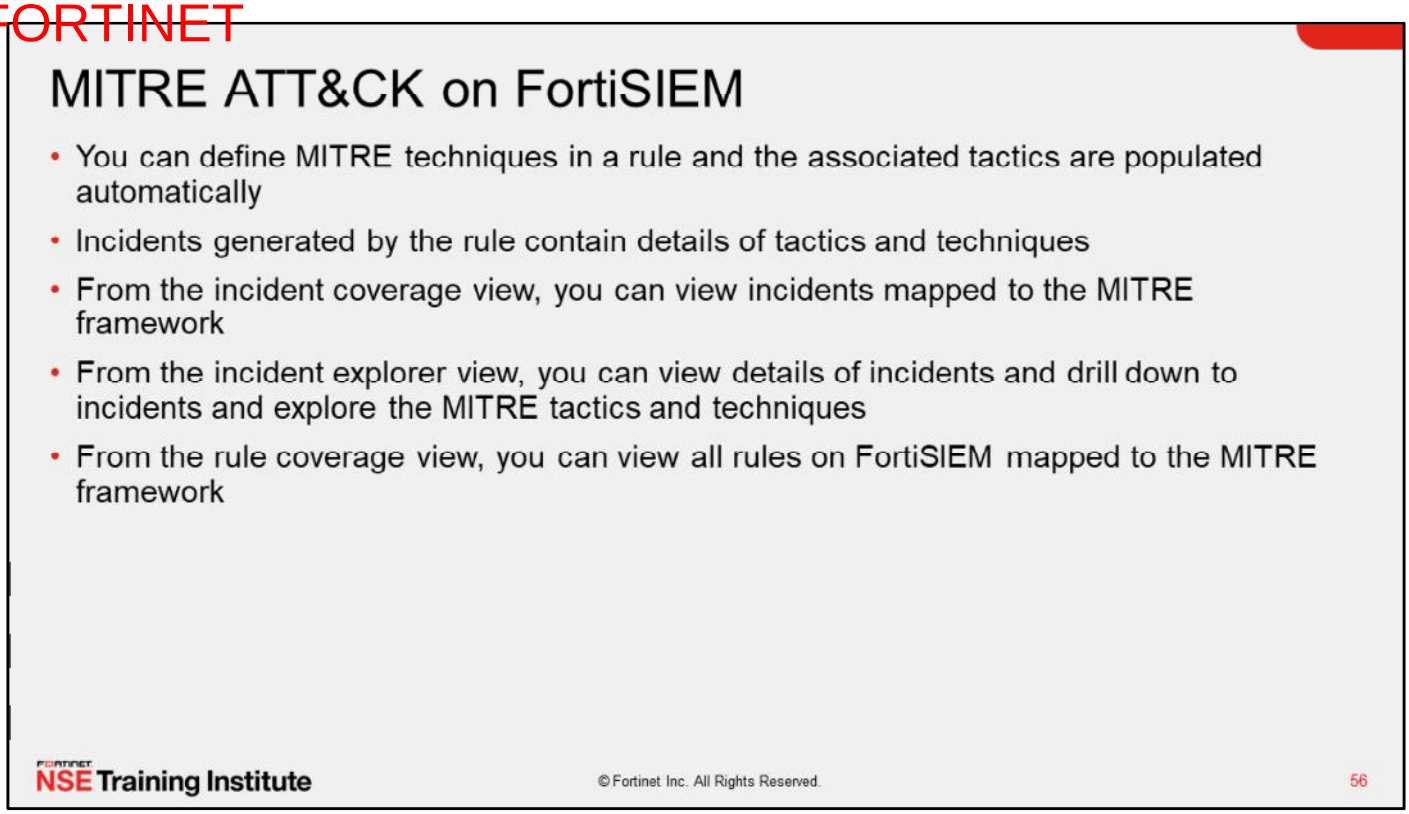


Groups are sets of related intrusion activity that are tracked by a common name in the security community. Analysts track clusters of activities using various analytic methodologies and terms such as threat groups, activity groups, threat actors, intrusion sets, and campaigns. Some groups have multiple names associated with similar activities because of various organizations tracking similar activities by different names. The group definitions of the organizations may partially overlap with groups designated by other organizations and may disagree on specific activity.

OilRig is an example of a group that used several tactics and techniques. It is a suspected threat group that has targeted Middle Eastern and international victims since at least 2014. The group has targeted a variety of industries, including financial, government, energy, chemical, and telecommunications, and has largely focused its operations within the Middle East. It appears the group carries out supply chain attacks, leveraging the trust relationship between organizations to attack their primary targets.

Vouchers & Dumps are Available | WhatsApp +201224560923

DO NOT REPRINT
© FORTINET
Brave-dumps.com



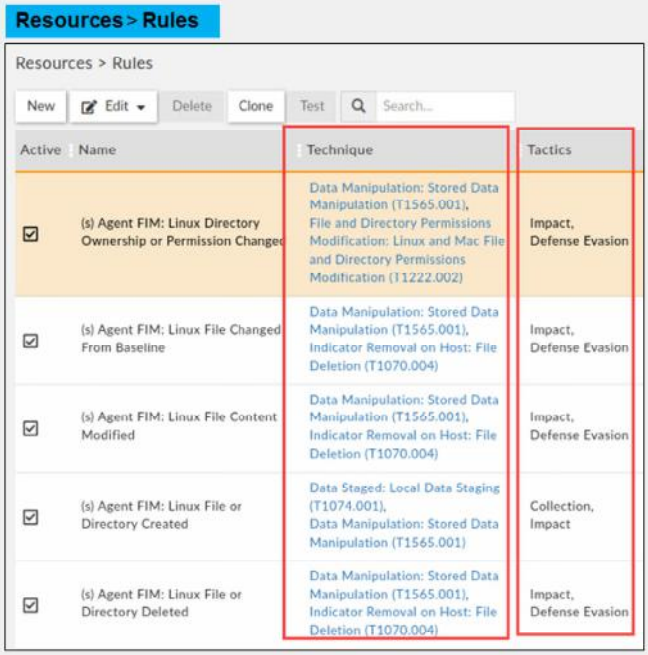
You can define MITRE techniques in a rule and the associated tactics are populated automatically. Incidents generated by the rule contain details of tactics and techniques. From the incident coverage view, you can view incidents mapped to the MITRE framework. From the incident explorer view, you can view details of incidents and drill down to incidents and explore the MITRE tactics and techniques. From the rule coverage view you can view all rules on FortiSIEM mapped to the MITRE framework.

Vouchers & Dumps are Available | WhatsApp +201224560923

DO NOT REPRINT
© FORTINET
Brave-dumps.com

ATT&CK Rule Association

- Associate FortiSIEM rules with MITRE ATT&CK techniques
- One-to-many mapping
- Works for system and custom rules
- More than 900 built-in MITRE ATT&CK mapped rules



NSE Training Institute

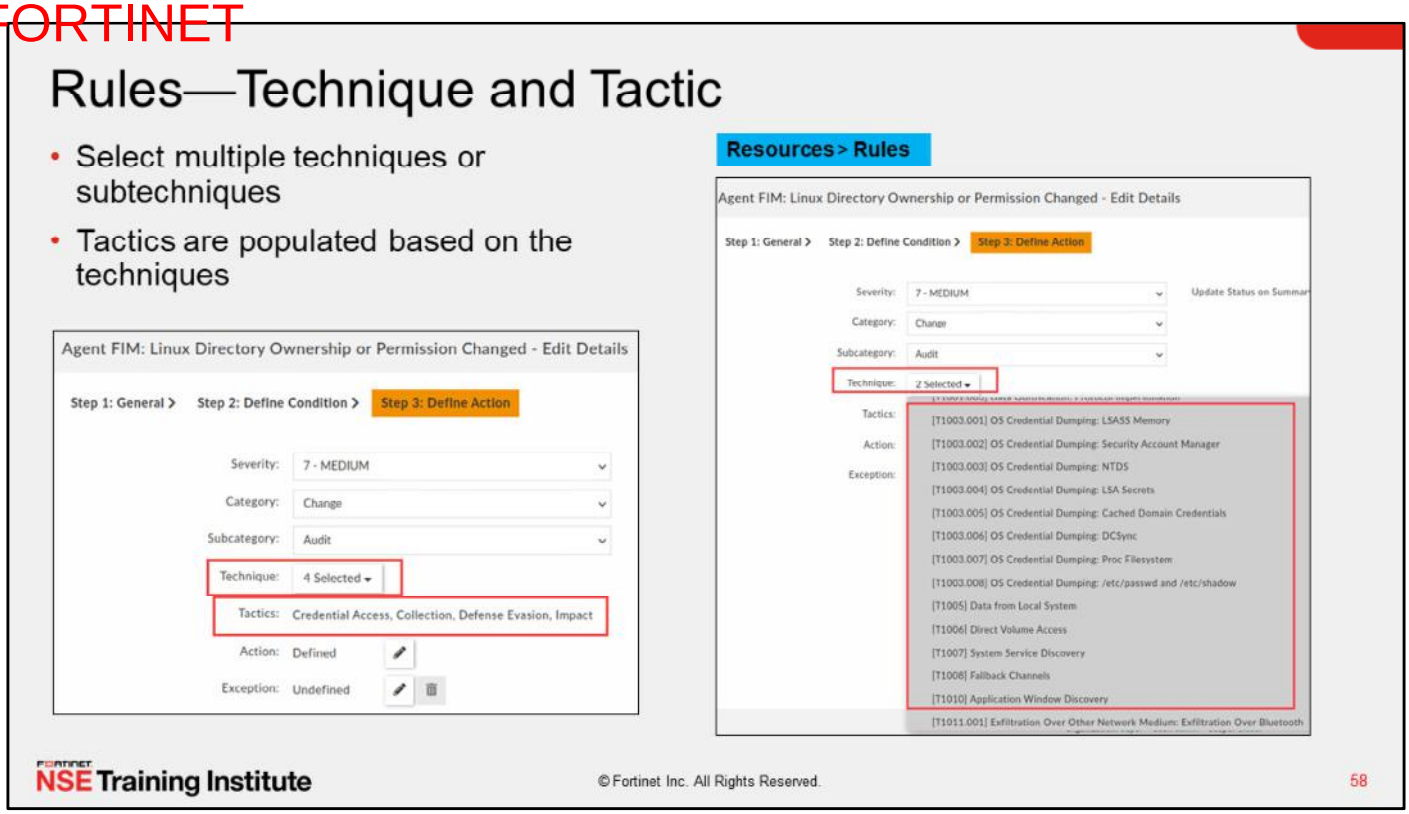
© Fortinet Inc. All Rights Reserved.

57

More than 900 built-in rules on FortiSIEM are associated with MITRE ATT&CK techniques. You can apply the technique and tactic to system rules or custom rules.

Vouchers & Dumps are Available | WhatsApp +201224560923

DO NOT REPRINT
© FORTINET
Brave-dumps.com



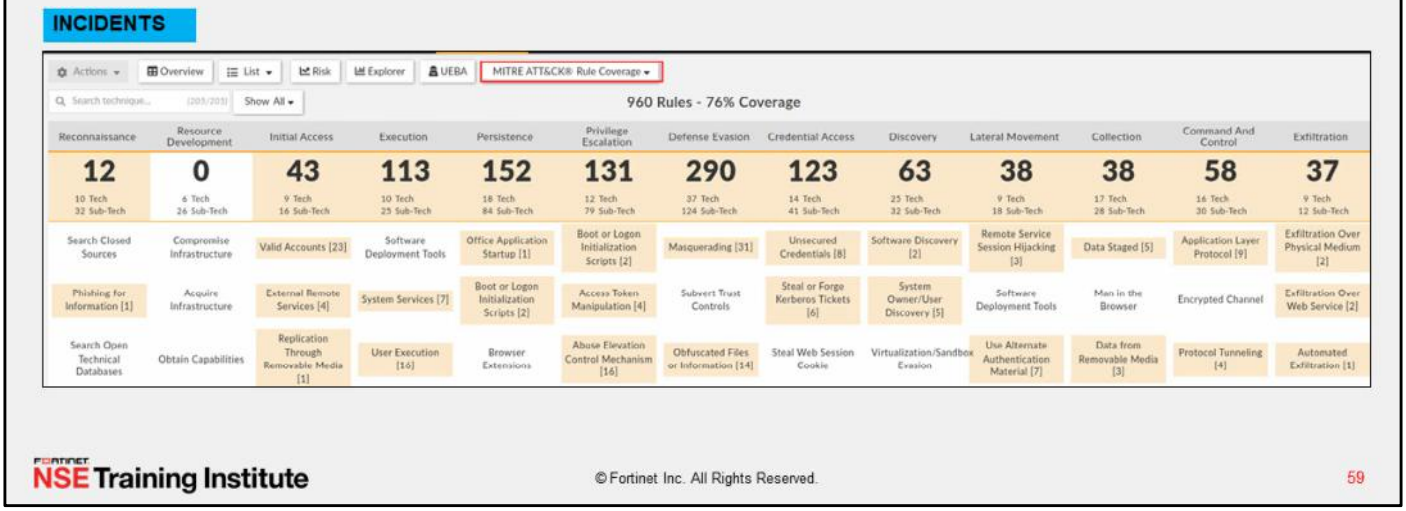
All existing rules are mapped to MITRE ATT&CK tactics and techniques where applicable. You can add techniques to your own custom rule or you can edit the techniques of the built-in rules. You can select multiple techniques or subtechniques in a rule. The tactics are populated based on the techniques that you select.

Vouchers & Dumps are Available | WhatsApp +201224560923

DO NOT REPRINT Brave-dumps.com
© FORTINET

ATT&CK Dashboards—Rule Coverage

- Rule coverage dashboard shows MITRE ATT&CK coverage for rules
- Top row displays the number of rules and the percentage of MITRE techniques that FortiSIEM covers



NSE Training Institute
© Fortinet Inc. All Rights Reserved.

The rule coverage view provides an overview of the tactics and techniques that FortiSIEM covers as defined by MITRE Corporation. The top row displays the number of rules and the percentage of MITRE techniques that FortiSIEM covers. In the main row header, the bolded number that appears under each tactic indicates the number of rules that are covered under it. Clicking a tactic here shows all the rules that belong to it. Each tactic cell also lists the number of major techniques (Tech) and subtechniques (Sub-Tech) related to the involved tactic. All major techniques related to a tactic are listed underneath their respective tactic column. Tactics and techniques covered by FortiSIEM rules are indicated by a light yellow background.
You can hover your cursor over any major technique to view the following information:

- Total number of rules covered by the technique (security category)
- The number of rules covered by each subtechnique (if applicable)

Vouchers & Dumps are Available | WhatsApp +201224560923

DO NOT REPRINT
© FORTINET
Brave-dumps.com

Knowledge Check

1. What does TTP stand for?
   - ✓ A. Tactics, Techniques, and Procedures
   - B. Target, Tools, and Procedures

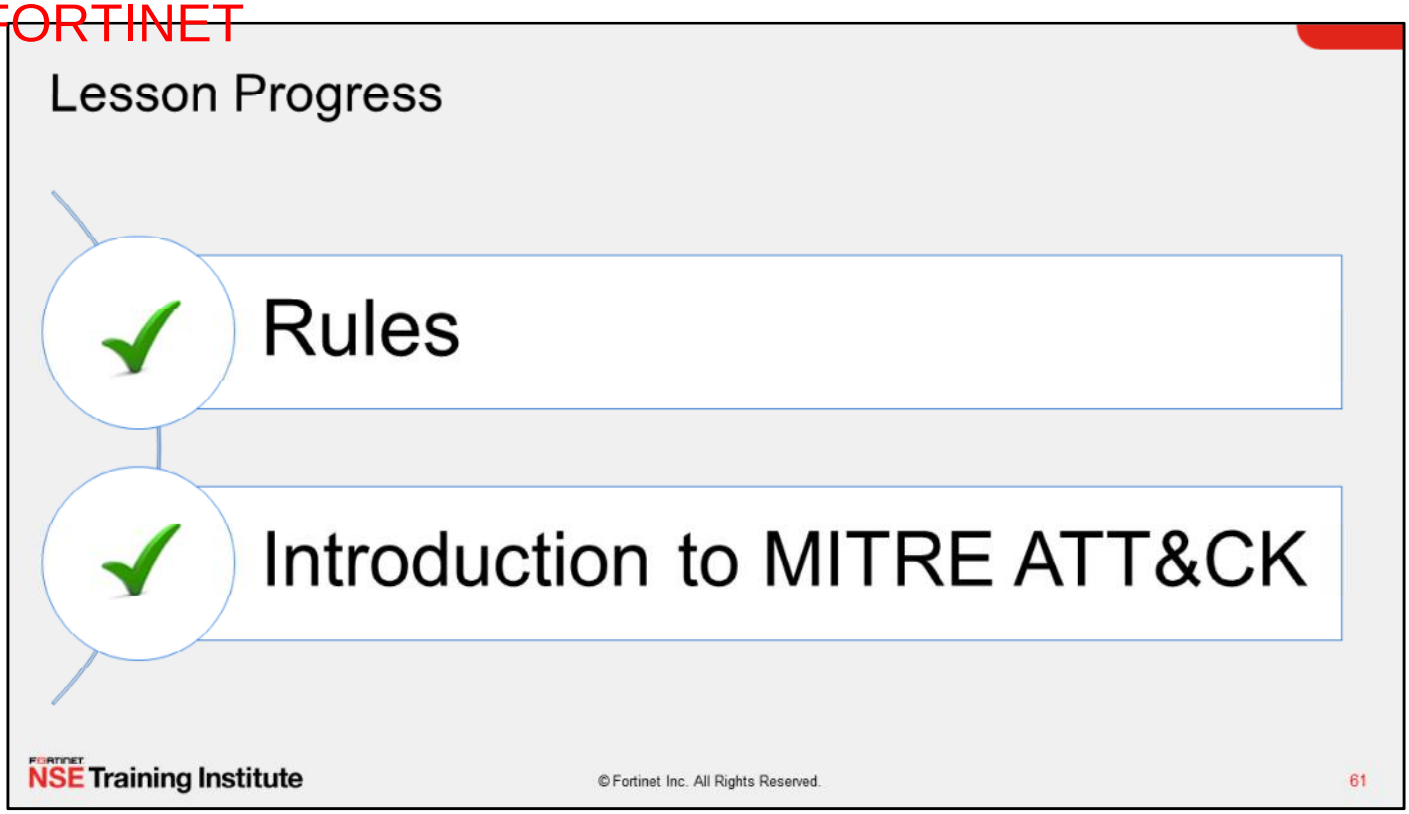
NSE Training Institute

© Fortinet Inc. All Rights Reserved.

60

Vouchers & Dumps are Available | WhatsApp +201224560923

DO NOT REPRINT
© FORTINET
Brave-dumps.com

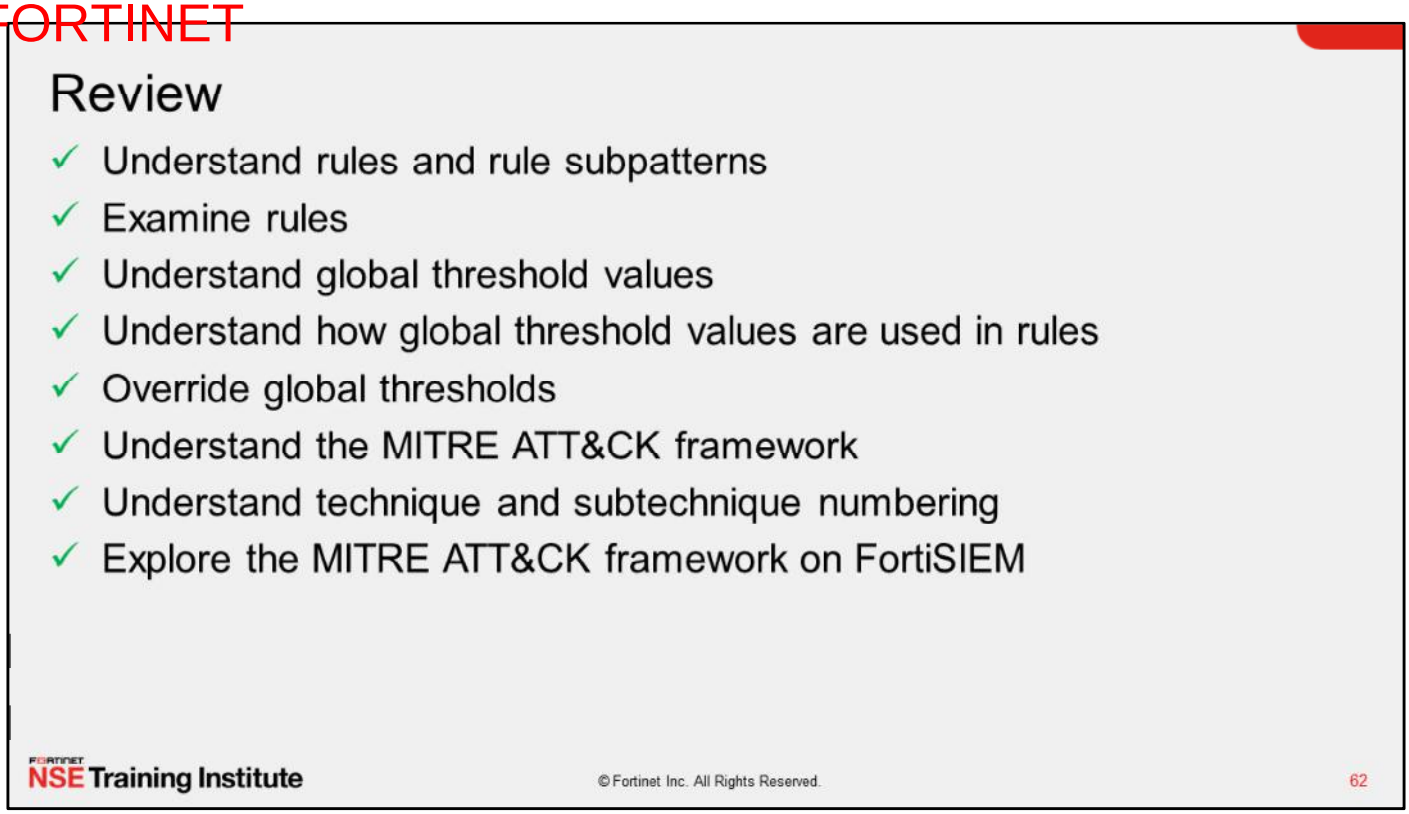


Congratulations! You have completed this lesson.

Now, you will review the objectives that you covered in this lesson.

Vouchers & Dumps are Available | WhatsApp +201224560923

DO NOT REPRINT
© FORTINET
Brave-dumps.com

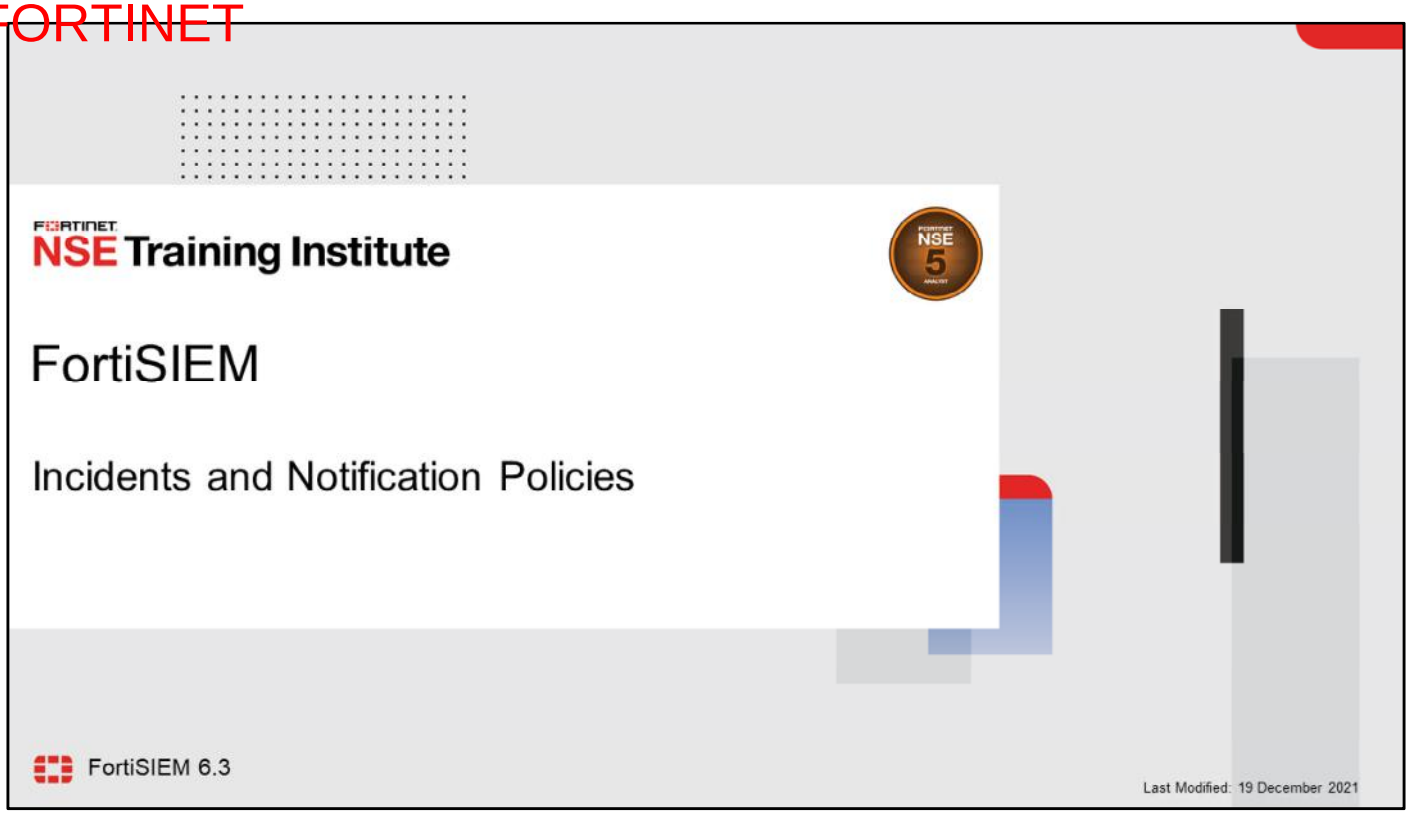


This slide shows the objectives that you covered in this lesson.

By mastering the objectives covered in this lesson, you learned how to use rules and the MITRE ATT&CK framework .

Vouchers & Dumps are Available | WhatsApp +201224560923

DO NOT REPRINT
© FORTINET
Brave-dumps.com



In this lesson, you will learn what incidents are and how to define a notification policy.

Vouchers & Dumps are Available | WhatsApp +201224560923

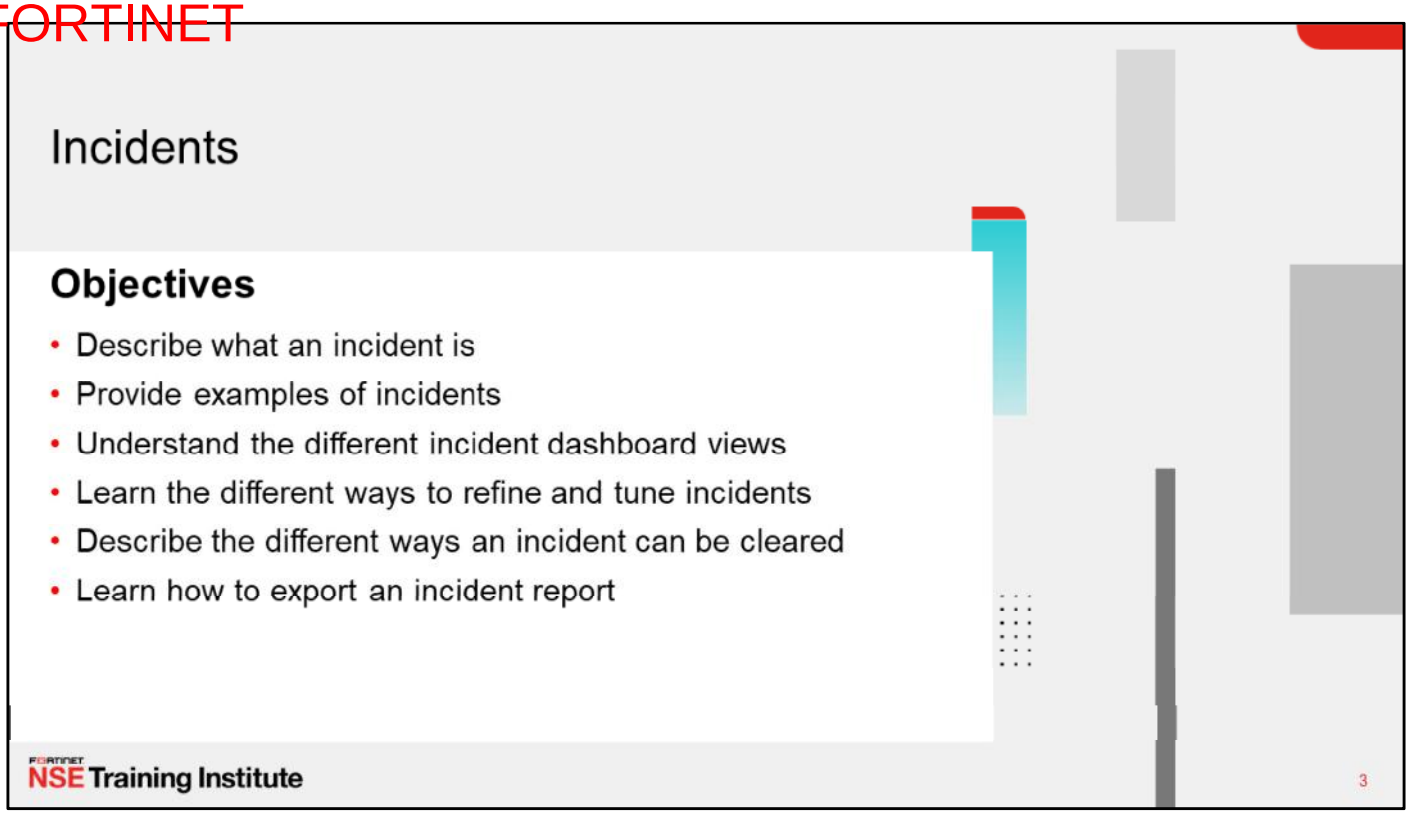
DO NOT REPRINT
© FORTINET
Brave-dumps.com



In this lesson, you will explore the topics shown on this slide.

Vouchers & Dumps are Available | WhatsApp +201224560923

DO NOT REPRINT
© FORTINET
Brave-dumps.com

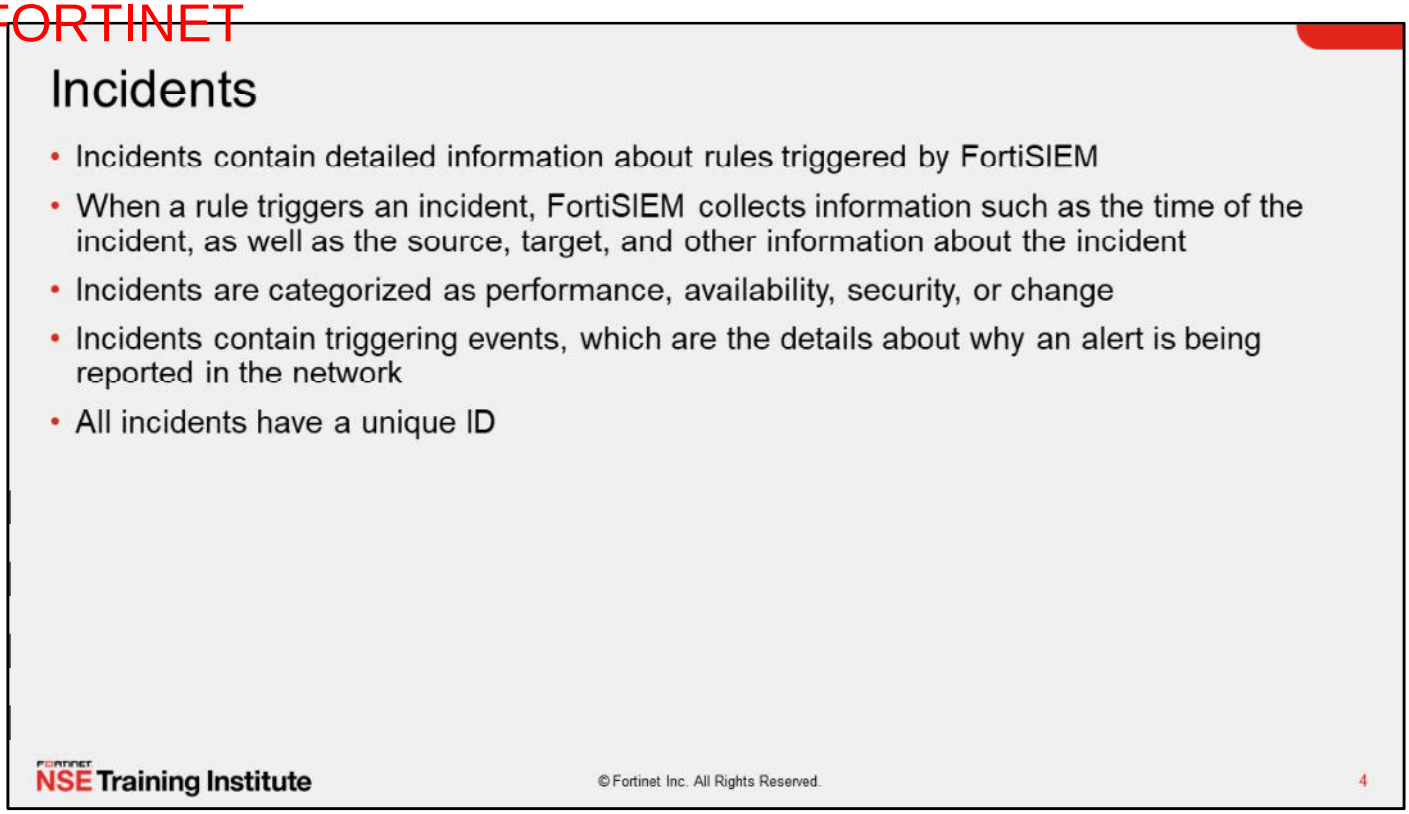


After completing this section, you should be able to achieve the objectives shown on this slide.

By demonstrating competence in identifying and managing incidents, you will be able to manage your network better using FortiSIEM.

Vouchers & Dumps are Available | WhatsApp +201224560923

DO NOT REPRINT
© FORTINET
Brave-dumps.com



Incidents contain detailed information about rules that have been triggered by FortiSIEM.

When FortiSIEM triggers a rule, it collects information such as the time of the incident, source, target, and other information.

The incident is then categorized as an incident related to performance, availability, security, or change.

Incidents also contain the triggering events, which are the details about why an alert is being reported in the network.

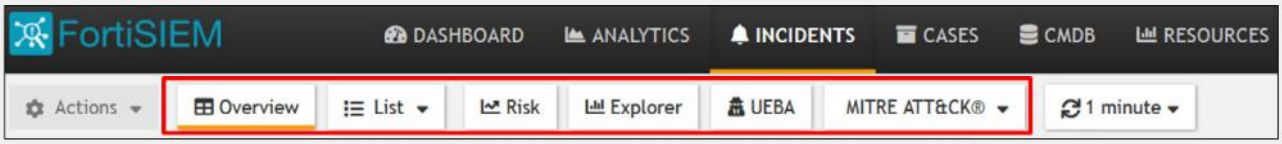
All incidents have a unique ID.

Vouchers & Dumps are Available | WhatsApp +201224560923

DO NOT REPRINT
© FORTINET
Brave-dumps.com

Viewing Incident Information

- The **INCIDENTS** tab provides *six* views of incident data:
  - Overview
  - List
  - Risk
  - Explorer
  - UEBA
  - MITRE ATT&CK



NSE Training Institute

© Fortinet Inc. All Rights Reserved.

5

The **INCIDENT tab** provides *six* views of incident data:

- **Overview**: Provides a top-down view of the various types of incidents and impacted hosts
- **List**: Enables the user to search incidents and take actions
- **Risk**: Organizes impacted entities (hosts, users) by risk based on the triggered incidents
- **Explorer**: Helps users to correlate actors (IP, Host, User) across multiple incidents, without creating multiple reports in separate tabs
- **UEBA**: Monitors the AI alerts obtained from FortiInsight
- **MITRE ATT&CK**: Classifies security events detected by FortiSIEM into MITRE ATT&CK categories

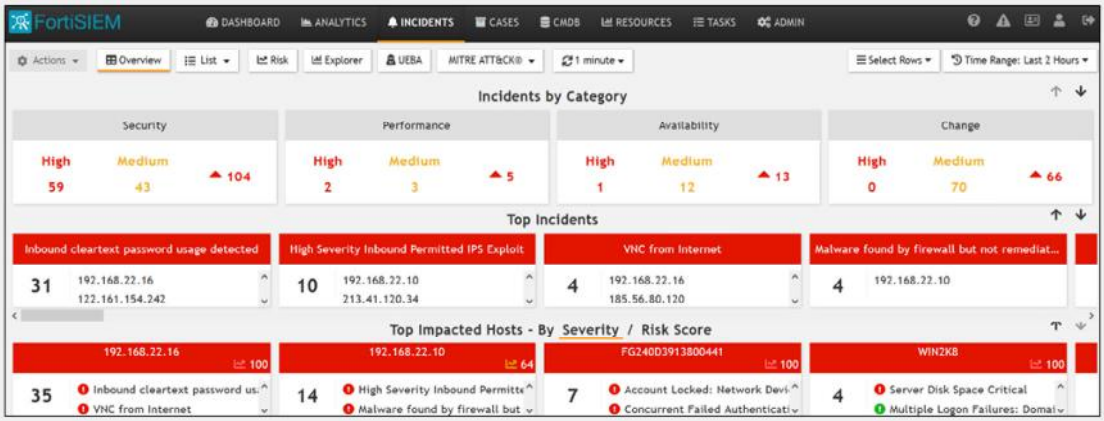
Now, you will examine views in greater detail.

Vouchers & Dumps are Available | WhatsApp +201224560923

DO NOT REPRINT Brave-dumps.com
© FORTINET

INCIDENTS Tab—Overview

- A top-down view of various types of incidents and impacted hosts
- The panel is divided into three sections:
  - **Incident By Category**
  - **Top Incidents**
  - **Top Impacted Hosts By Severity / Risk Score**



NSE Training Institute © Fortinet Inc. All Rights Reserved. 6

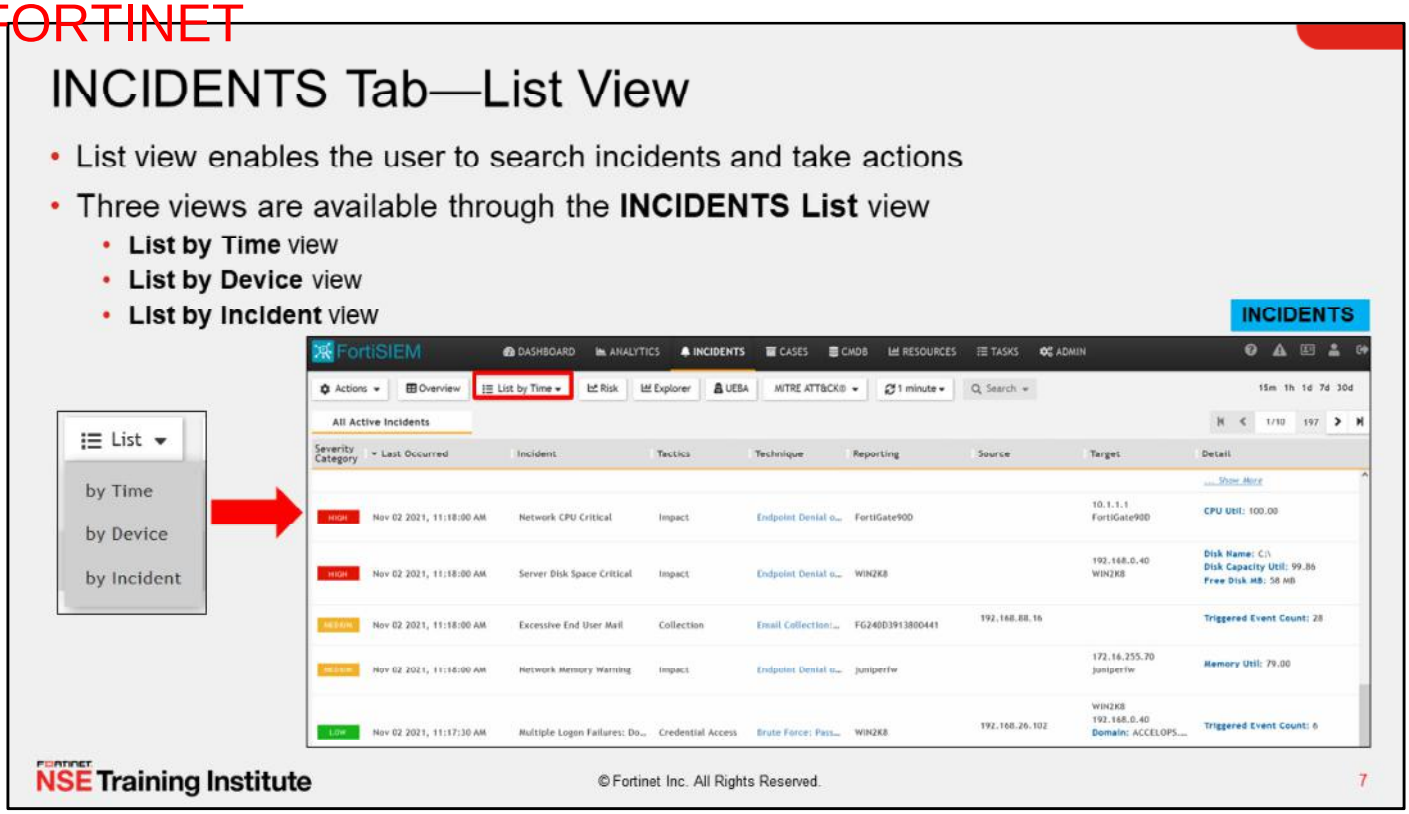
By default, the Overview provides a top-down view of various types of incidents and impacted hosts that occurred during the previous two hours.

The panel is divided into three sections:
- **Incidents By Category**: Displays incident counts by function and severity.
- **Top Incidents**: Displays the top incidents sorted first by severity and then count.
- **Top Impacted Hosts By Severity / Risk Score**: Displays the most affected hosts by severity and risk score.

To drill into a specific category, click the number that represents the risk score. The matching incidents are displayed in a separate incident **List** view. To return to the main view, click the **<** button.

Vouchers & Dumps are Available | WhatsApp +201224560923

DO NOT REPRINT Brave-dumps.com
© FORTINET



In this view, the user can search incidents and take action.

Three views are available through the **INCIDENTS List** view:

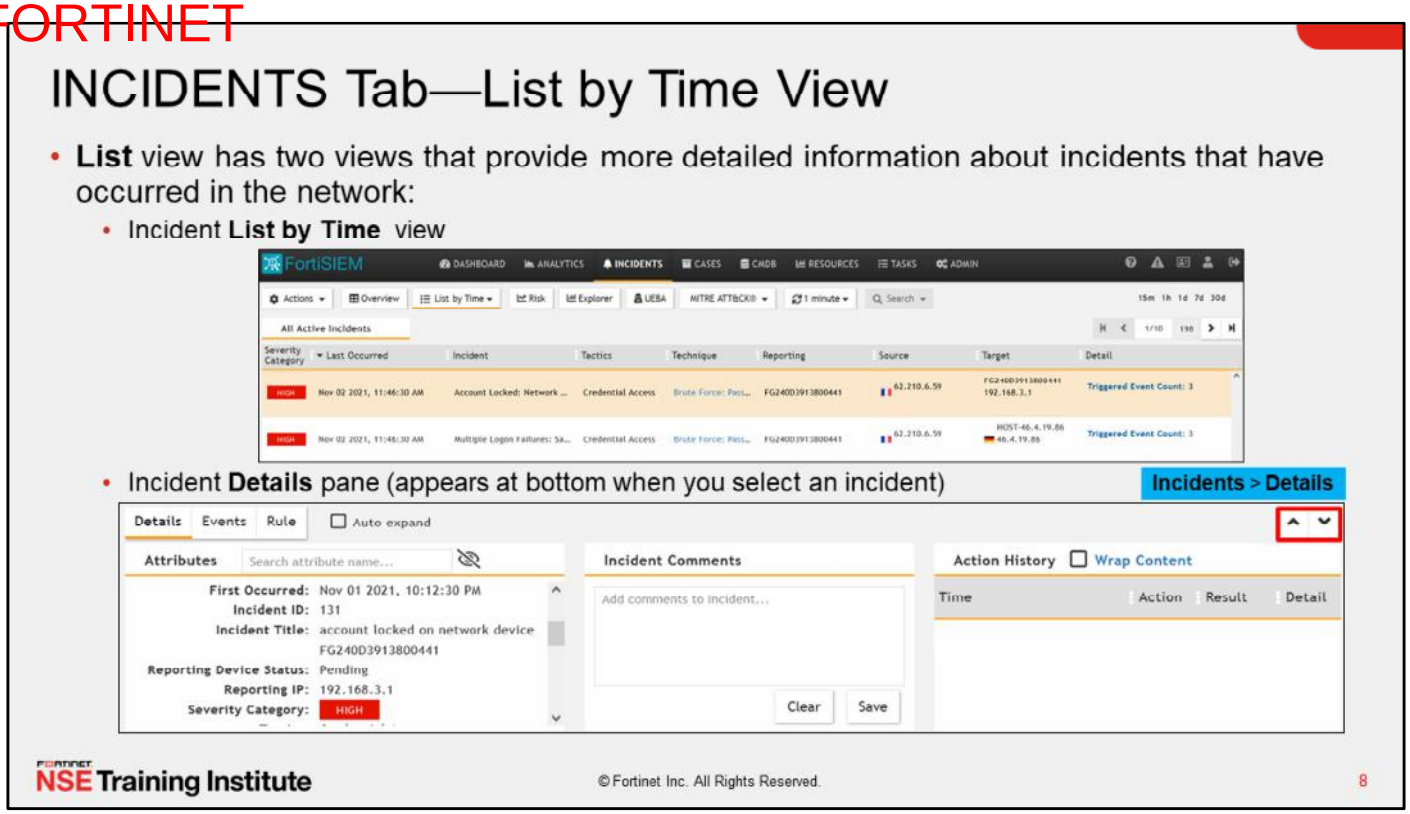
- **List by Time**: By default, this view refreshes every minute. The refresh menu on the top bar allows you to disable the automatic refresh or choose a different refresh interval, by default, the active incidents in the last two hours. The latest incident sorted by **Last Occurred** time is shown first.
- **List by Device**: The upper pane of the view lists the devices that are experiencing incidents. In the list, the device can be identified by either an IP or a host name.
- **List by Incident**: The upper pane of the **List by Incident** view lists the incidents detected by FortiSIEM. The name of the incident is followed by the number of incidents in parentheses. Click the incident name to see the incidents associated with the device. The lower portion of the view contains the same features and functionality as the **List by Time** view.

Acting on incidents:

- The **Action** menu provides a list of actions that you can take on incidents

Vouchers & Dumps are Available | WhatsApp +201224560923

DO NOT REPRINT
© FORTINET
Brave-dumps.com



The Incidents **List by Time** view has two views that provide more detailed information about incidents that have occurred in the network.

The incident table view displays tabular columns that show the following incident attributes for each incident:

- **Severity** (icon): HIGH (red), MEDIUM (yellow) or LOW (green)
- **Last Occurred**: The last time this incident occurred
- **Incident**: The name of the incident
- **Tactics**: The name of the tactic involved with the incident
- **Technique**: The name of the technique involved with the incident
- **Reporting**: set of devices that are reporting the incident
- **Source**: The source of the incident (host name or IP address)
- **Target**: The target of the incident (host name or IP address or user)
- **Detail**: Other incident details, for example, counts, average CPU utilization, file name and so on
- **Status**: **Active**, **Cleared**, **System Cleared**, or **External Cleared**
- **Resolution**: **Open** (not defined or not known whether the incident is True Positive or False Positive), **True Positive**, and **False Positive**

The incident **Details** pane displays the reasons the incident was triggered:

- **Events**: shows the set of events that triggered the incident
- **Rule**: select the rule to see the events belonging to each sub-pattern

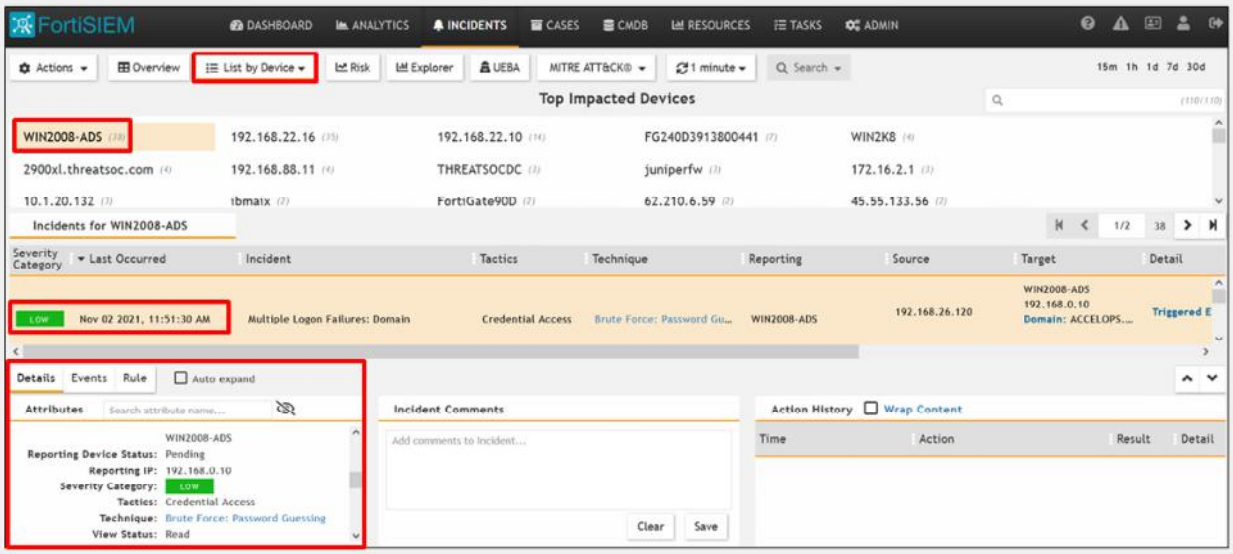
To close the incident **Details** pane, click the highlighted incident

Vouchers & Dumps are Available | WhatsApp +201224560923

DO NOT REPRINT Brave-dumps.com
© FORTINET

INCIDENTS Tab—List by Device View

- Upper pane of the **List by Device** view lists the devices that are experiencing incidents

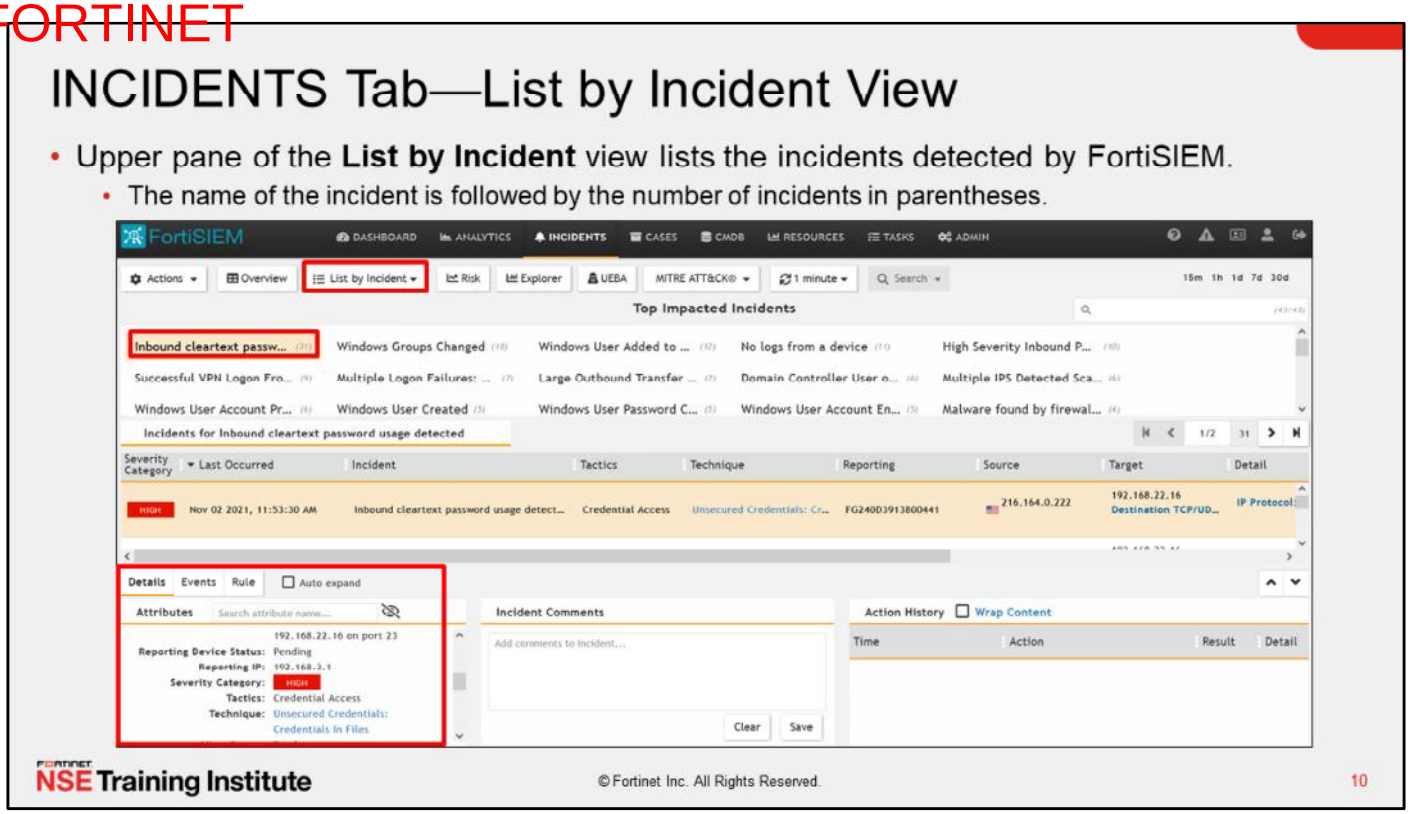


NSE Training Institute
© Fortinet Inc. All Rights Reserved.

The upper pane of the **List by Device** view lists the devices that are experiencing incidents. In the list, the device can be identified by either an IP address or a host name. The name of the device is followed by the number of incidents in parentheses. Click the device name to see the incidents associated with the device. The lower portion of the view contains the same features and functionality as the **List by Time** view.

Vouchers & Dumps are Available | WhatsApp +201224560923

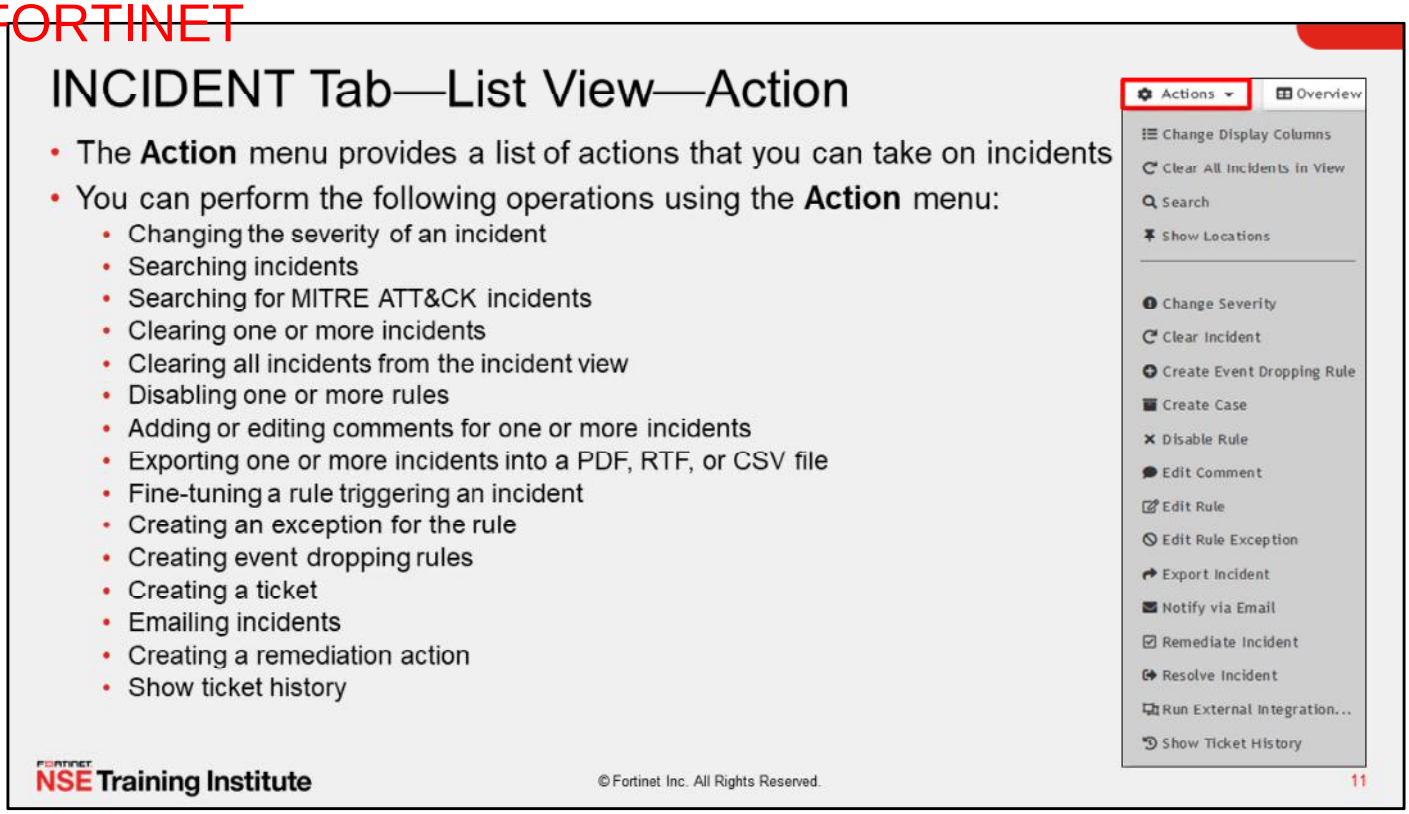
DO NOT REPRINT Brave-dumps.com
© FORTINET



The upper pane of the **List by Incident** view lists the incidents detected by FortiSIEM. The name of the incident is followed by the number of incidents in parentheses. Click the incident name to see the incidents associated with the device. The lower portion of the view contains the same features and functionality as the **List by Time** view.

Vouchers & Dumps are Available | WhatsApp +201224560923

DO NOT REPRINT
© FORTINET
Brave-dumps.com

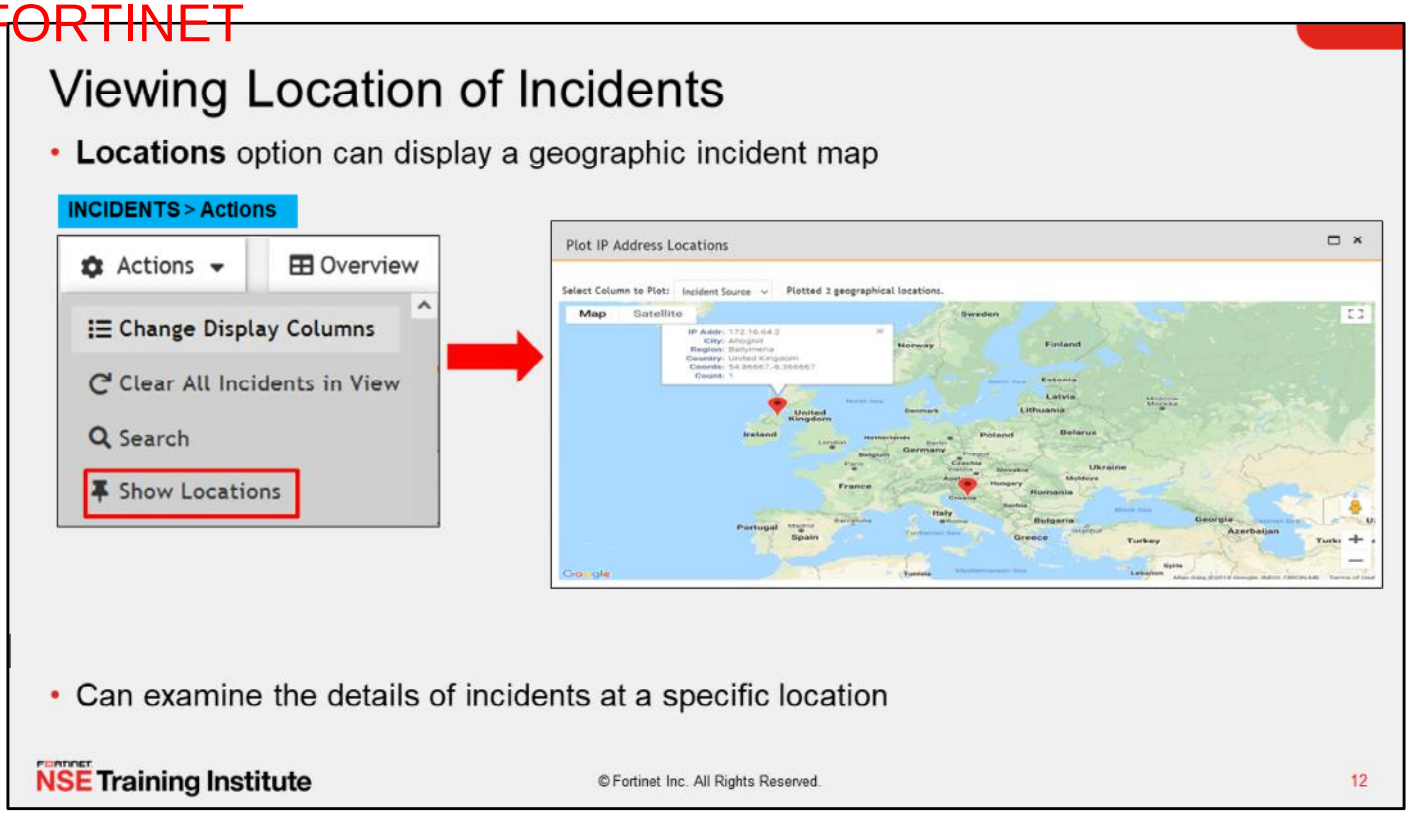


The **Actions** menu provides a list of actions that you can take on incidents.

You can perform the following operations using the **Actions** menu:
- Changing the severity of an incident
- Searching incidents
- Searching for MITRE ATT&CK incidents
- Clearing one or more incidents
- Clearing all incidents from the incident view
- Disabling one or more rules
- Adding or editing comments for one or more incidents
- Exporting one or more incidents into a PDF, RTF, or CSV file
- Fine tuning a rule triggering an incident
- Creating an exception for the rule
- Creating event dropping rules
- Creating a ticket
- Emailing incidents
- Creating a remediation action
- Show ticket history

Vouchers & Dumps are Available | WhatsApp +201224560923

DO NOT REPRINT
© FORTINET
Brave-dumps.com



The **Locations** option enables you to display a geographic incident map, and allows you to examine incidents that occur at a specific location.

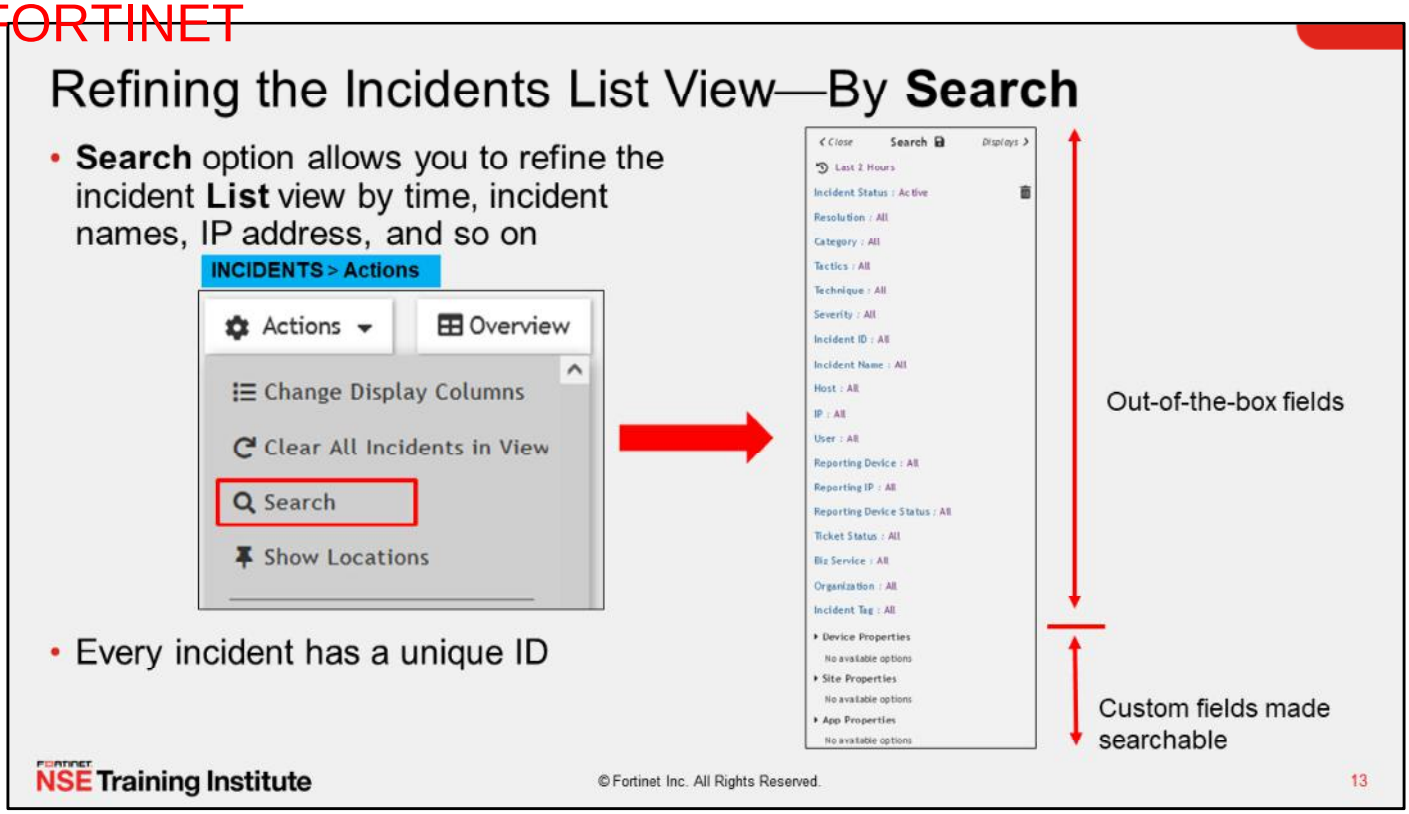
To see a location view of the incidents, select **Locations** from the **Actions** menu. FortiSIEM has a built-in database on locations of public IP addresses.

You can define private IP address locations on **ADMIN** > **Settings** > **Discovery** > **Location**.

To view the location of specific incidents, press and hold the **Shift** key and select incidents by clicking the left mouse key. The selected incidents are highlighted, and then select **Locations** from the **Actions** menu.

Vouchers & Dumps are Available | WhatsApp +201224560923

DO NOT REPRINT
© FORTINET
Brave-dumps.com



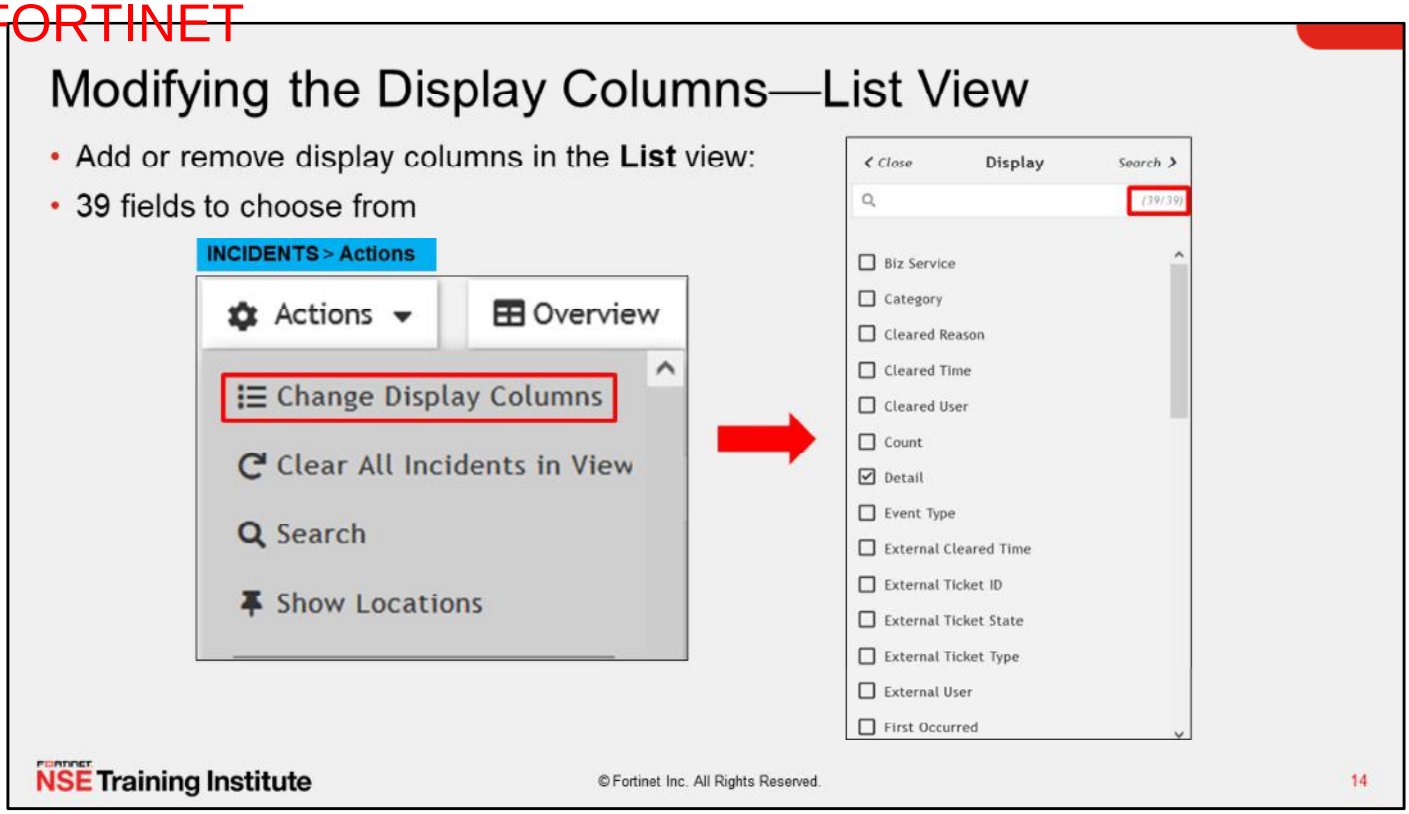
You can refine the incident **List** view by incident names, IP address, and so on by using the **Search** option.

To search incidents:

1. In the **Action** menu, select **Search**.
2. On the left pane, click on an incident attribute (for example, **Category**).
   All possible values of the selected attribute with a count next to it are shown (for example, **Security**, **Availability** and **Performance** for **Category**).
3. Select any value (for example, **Performance**).
   The right pane updates with the relevant incidents.
4. Click and select other incident attributes to refine the search or click **< Search** to cancel the selection.

Vouchers & Dumps are Available | WhatsApp +201224560923

DO NOT REPRINT Brave-dumps.com
© FORTINET



You can add or remove incident attributes from the **Change Display Columns** in the **List** view.

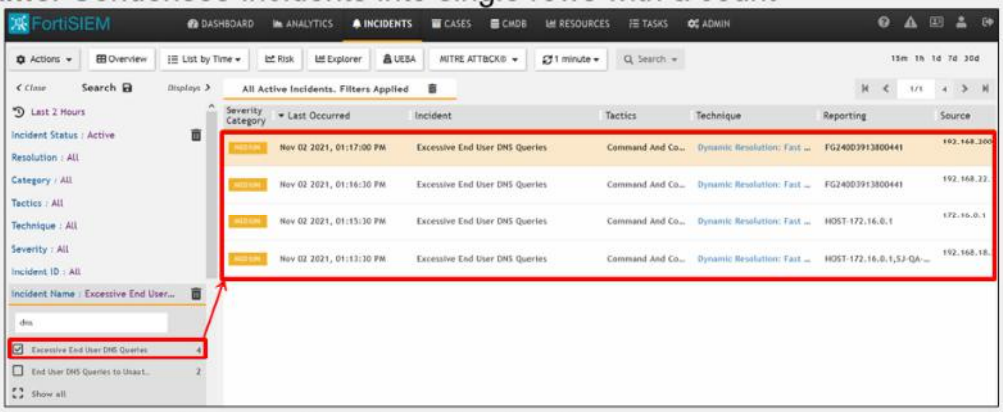
To change the incident attribute display columns in the **List** view, select **Change Display Columns** from the **Actions** menu, and then select the attributes you want to display.

Vouchers & Dumps are Available | WhatsApp +201224560923

DO NOT REPRINT
© FORTINET
Brave-dumps.com

Refining the Incidents in List by Time View—Incident Name

- **Incident Name**: Condenses incidents into single rows with a count



- Allows instant consolidation over time to understand:
  - Which incidents are triggered most often
  - Which sources or targets have the most incidents
- Extremely useful when tuning the system to reduce noise

NSE Training Institute

© Fortinet Inc. All Rights Reserved.

15

You can refine the incident using the **Incident Name** option in the **Search** list. **Incident Name** groups incidents by name with a count, similar to the way you use group by with a COUNT function for FortiSIEM analytics.

This feature is very useful when tuning your system to reduce noise. For example, if you filter by incident name, you can see which incidents are triggered most often. If you tune out the noisiest incidents, the incident table will make more sense to you in the future.

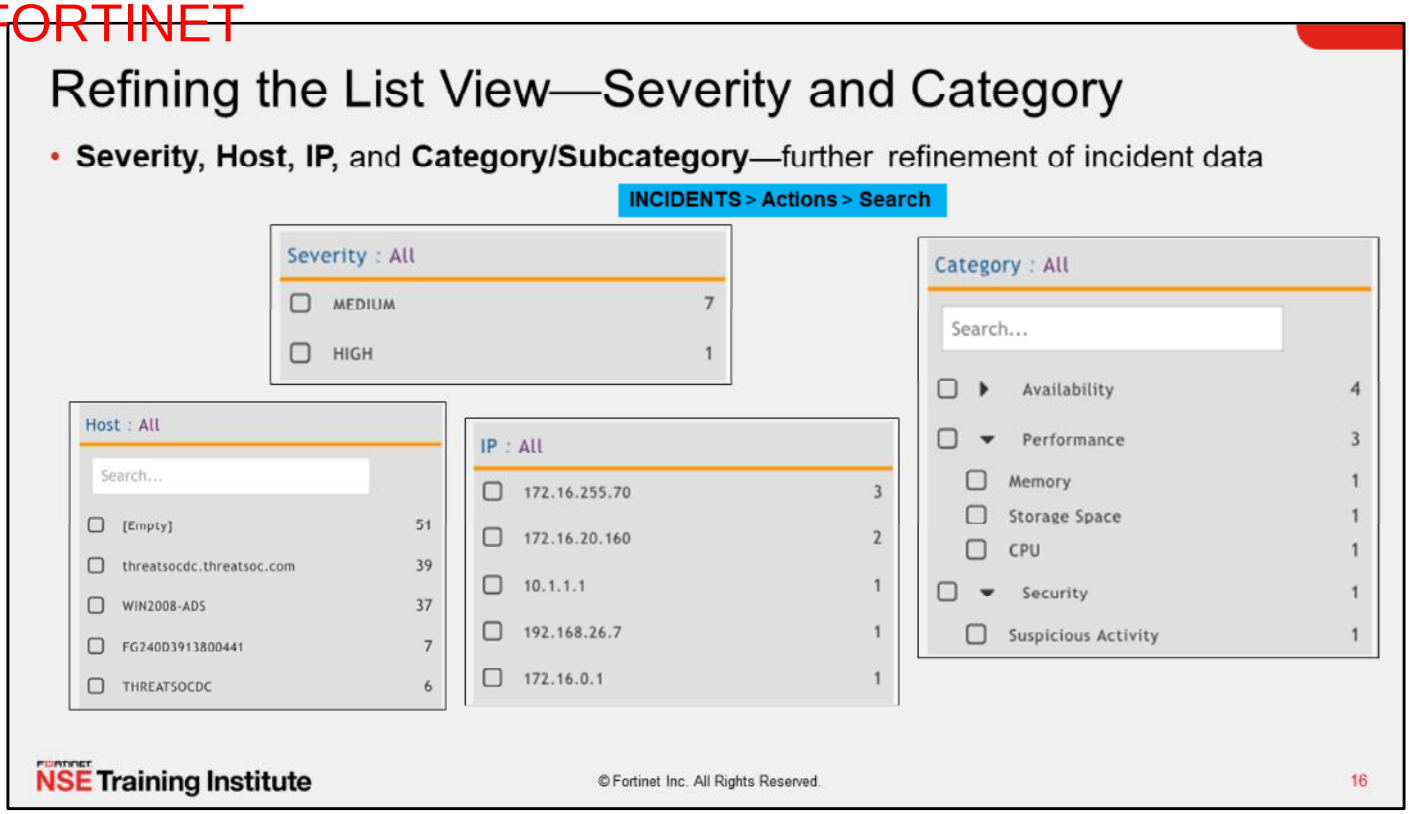
In the example shown on this slide, incident name **Excessive End User DNS Queries** is selected. The count indicates there are two incidents for the selected name of incident.

Once you have made your selections, the right pane displays incidents based on your selections.

After you finish selecting names, you can close the left **Search** pane by clicking **< Search** on the upper-left corner of the page.

Vouchers & Dumps are Available | WhatsApp +201224560923

DO NOT REPRINT Brave-dumps.com
© FORTINET



You can also refine the **List** view using the **Search** option by **Severity, Host, IP,** and **Category/Subcategory**. This allows you to drill into incidents of a specific severity or a specific type.

The **Severity** list allows you to examine incidents of specific severity: **HIGH, MEDIUM, LOW, OR HIGH + MEDIUM**. The severity of an incident is set in the rule that triggered it.

The **Category** list allows you to examine incidents of a particular type: **Security**, **Performance**, **Availability**, **Change**, or any of the subcategories.

The **Host** list allows you to examine various hosts on your network and security incidents associated with those hosts.

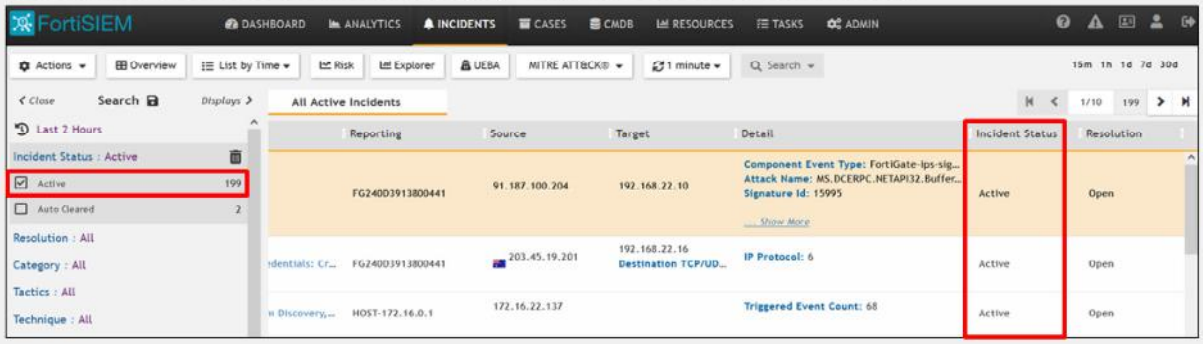
The **IP** list allows you to examine various IP addresses on your network.

Vouchers & Dumps are Available | WhatsApp +201224560923

DO NOT REPRINT Brave-dumps.com
© FORTINET

Refining the Incident List View—Incident Status

- **Incident Status**: Allows filtering by current status of an incident



- When an incident is first triggered, its status is **Active**
- By default, the Incident view focuses on active incidents
- When an incident is cleared, it is filtered in the view, but not deleted, to allow you to focus on issues currently active in the network

NSE Training Institute

© Fortinet Inc. All Rights Reserved.

17

You can also filter by incident **Status**. By default, the view shows **Active** incidents that occurred during a two-hour time period.

When an incident is first triggered, it has a status of **Active**. When an incident is **Cleared**, whether manually or by a clear condition in the rule, the status of the incident is updated, but the incident is not deleted.

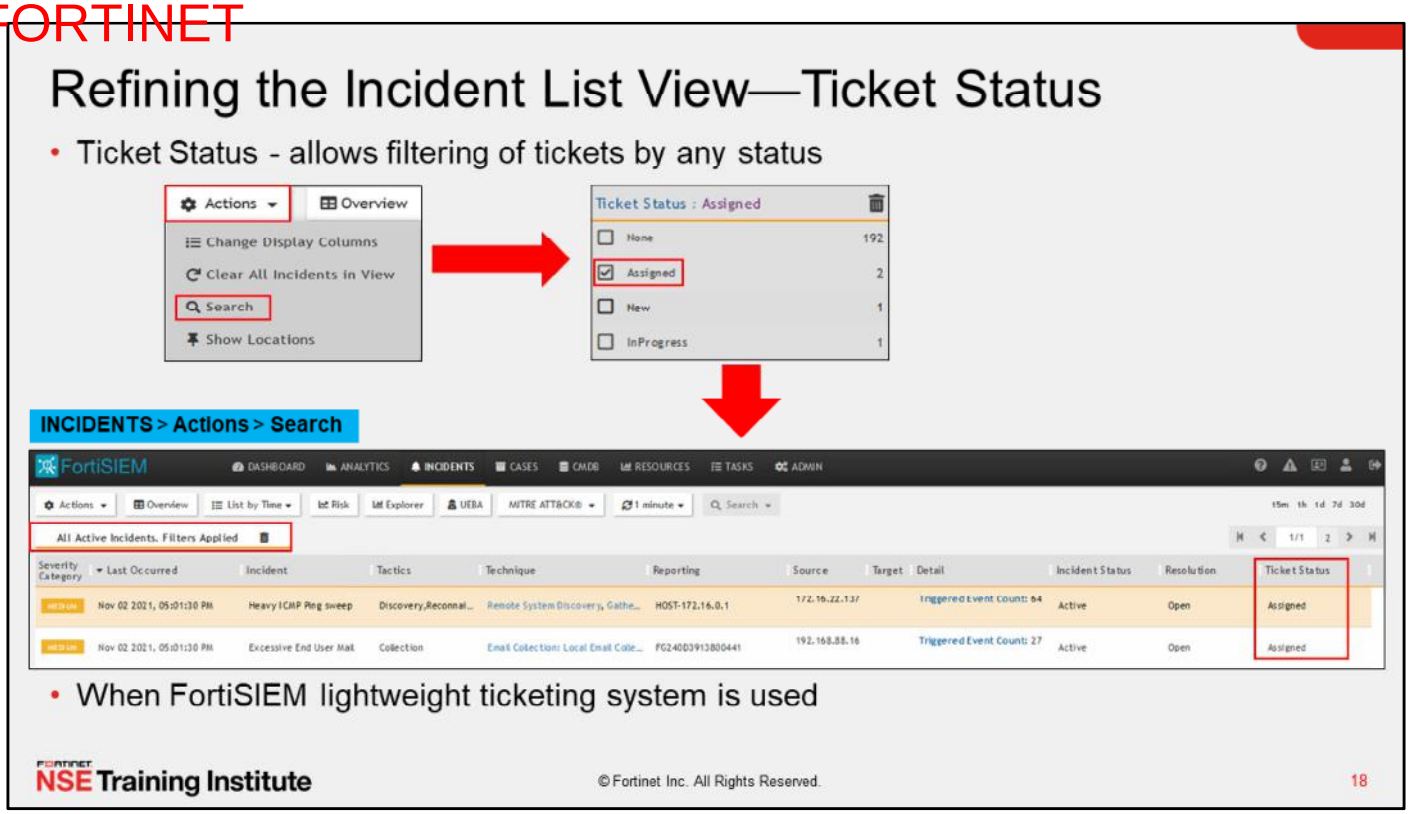
You can still view all of the non-active incidents in this view.

The availability of the **Incident Status** depends on the time range you select. For example, if you select a time of the last two hours, and if in the last two hours there is no incident with **Cleared** status, then the **Cleared** status option is not be available for selection. You need to change the time range, for example, to last four hours to see the **Cleared** status option.

This applies to all other incident attributes as well. Whether they are available for selection or not depends on the time range.

Vouchers & Dumps are Available | WhatsApp +201224560923

DO NOT REPRINT Brave-dumps.com
© FORTINET



You can also filter the **List** view by **Ticket Status**.

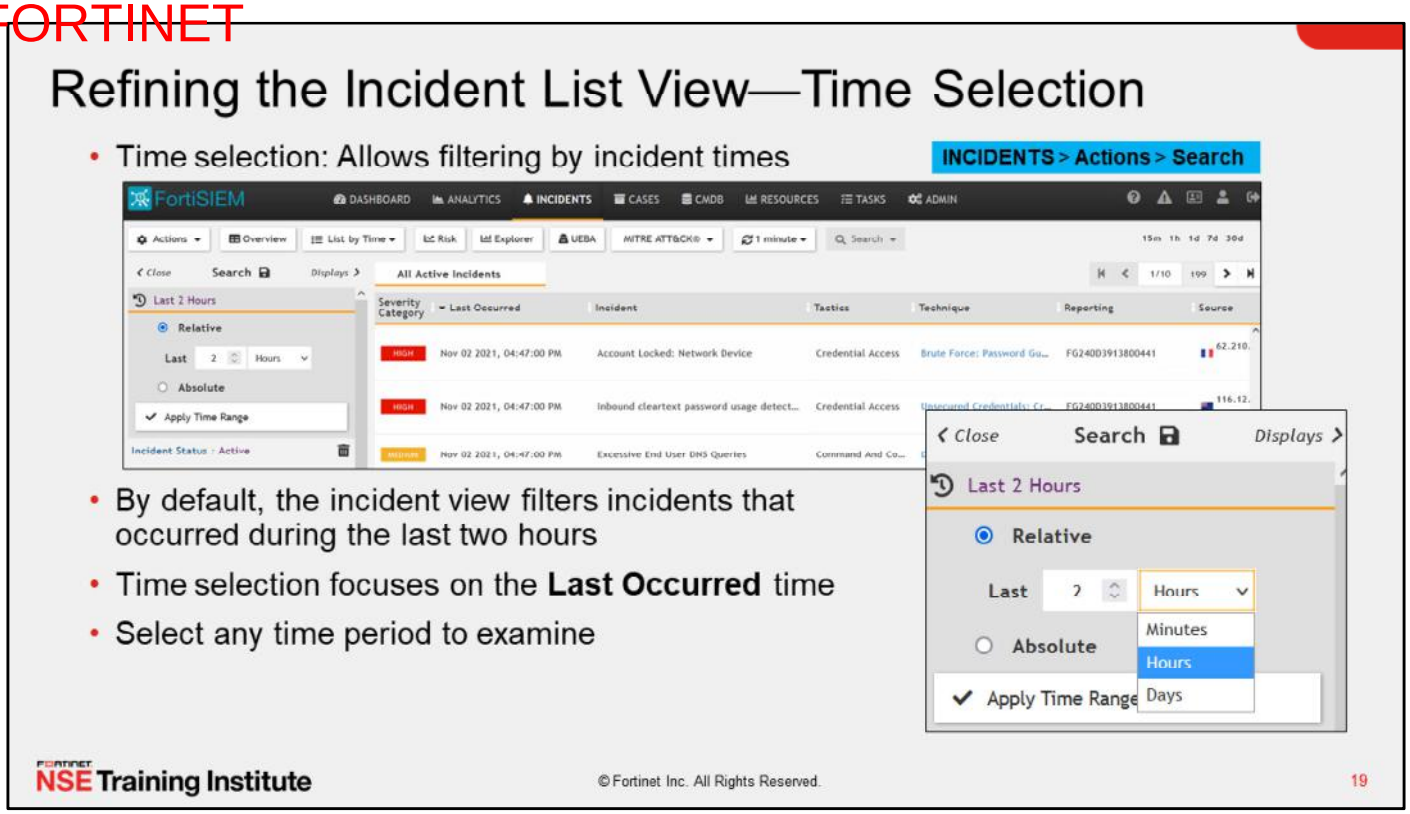
FortiSIEM has its own lightweight ticketing system in which you can view **New**, **Assigned**, **Closed, InProgress**, and **None** tickets.

The **Run External Integration** option allows you to reference the third-party ticketing systems integrated with FortiSIEM, such as Salesforce, ServiceNow, or ConnectWise.

The **Ticket Status** column does not appear in the incident **List** view by default. You can add it by selecting it in the **Change Display Columns** option.

Vouchers & Dumps are Available | WhatsApp +201224560923

DO NOT REPRINT Brave-dumps.com
© FORTINET



You can also filter by the time at which an incident occurred.

By default, FortiSIEM displays the incident table for active incidents that occurred during the previous two hours.

Time Selection focuses on the **Last Occurred** time in minutes, hours, or days.

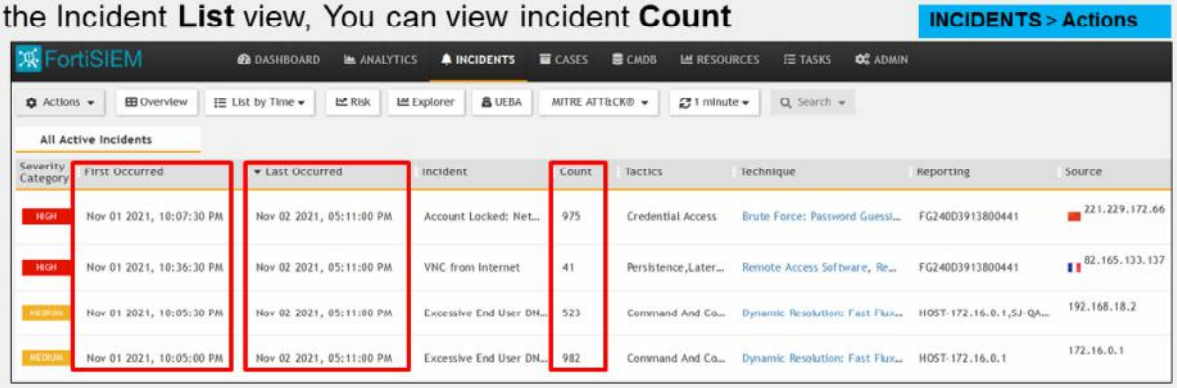
You can select the time period you want to examine, whether it's a relative time period such as a number of minutes, hours, or days, or an absolute time period.

Vouchers & Dumps are Available | WhatsApp +201224560923

DO NOT REPRINT Brave-dumps.com
© FORTINET

Incident List View—Count

- In the Incident **List** view, You can view incident **Count**



- Rules are based on time periods, for example, every X minutes. If the same rule with the same incident conditions is triggered repeatedly, FortiSIEM increases the count, rather than creating a separate incident in the table
- The **First Occurred** and **Last Occurred** time columns will be updated, while triggered **Events** shows the latest data

NSE Training Institute

© Fortinet Inc. All Rights Reserved.

20

In the Incident **List** view, you can view the incident **Count.**

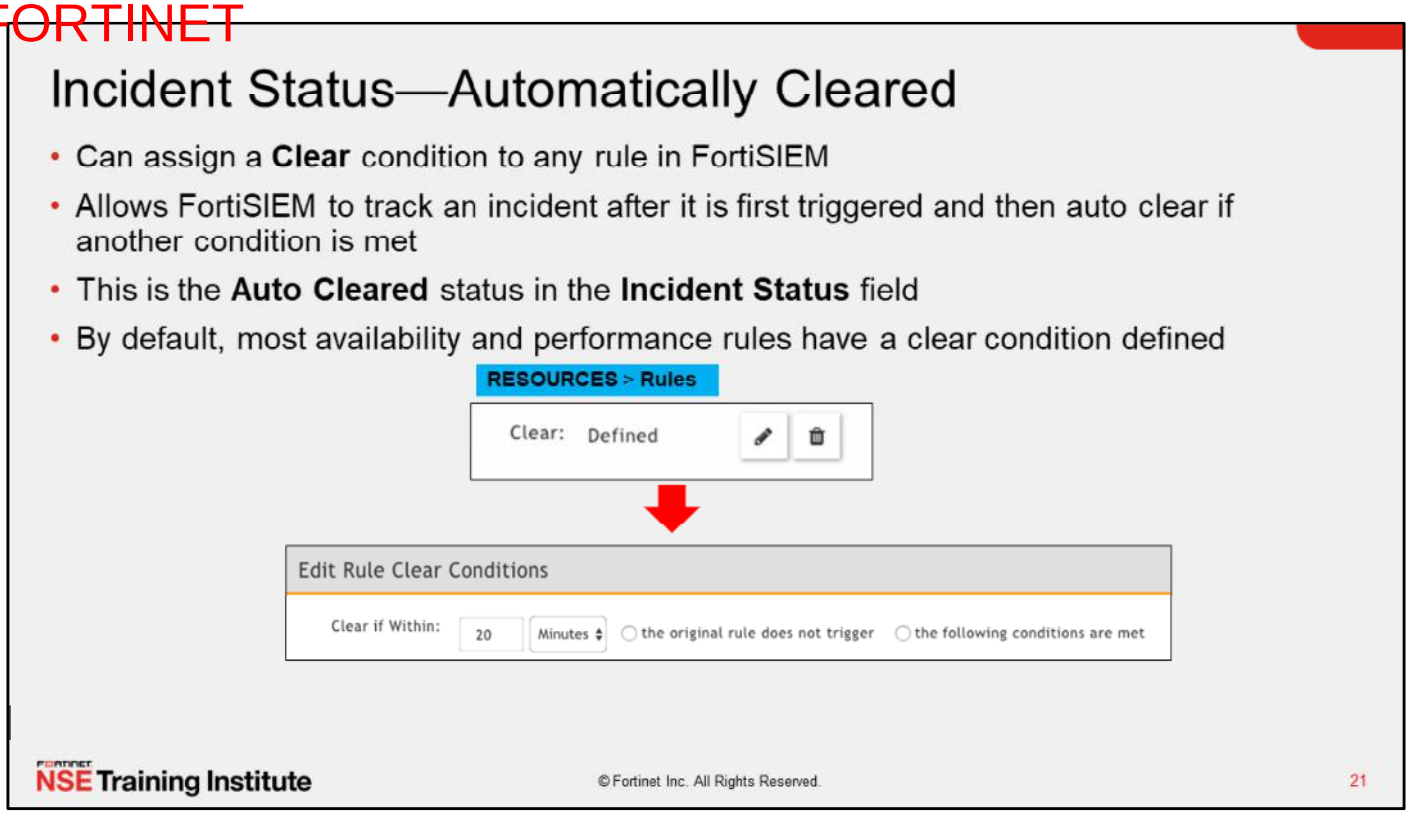
Rules are based on time periods–for example, every 10 minutes–if the same rule with the same incident conditions is triggered repeatedly, FortiSIEM will increase the count rather than create a separate incident in the table.

When an incident is triggered for the first time, FortiSIEM sets the **First Occurred** and the **Last Occurred** to the same value. When the incident is triggered again within the rule's time period, FortiSIEM increases the count and update the **Last Occurred** in the Incident **List** view, while the triggered **Events** view displays the latest data.

The **First Occurred** and **Count** columns do not appear in the incident **List** view by default. You can add them by selecting them in **Change Display Columns** option.

Vouchers & Dumps are Available | WhatsApp +201224560923

DO NOT REPRINT
© FORTINET
Brave-dumps.com



You can assign a **Clear** condition to any rule in FortiSIEM. A **Clear** condition allows FortiSIEM to track an incident after it is first triggered, and then automatically clear the incident if another condition is met.

When a rule first triggers an incident, the incident's status is set to active. If the rule that triggered the incident has a **Clear** condition, and if the **Clear** condition is met, then the **Incident Status** changes to **Auto Cleared** in the incident **Status** field.

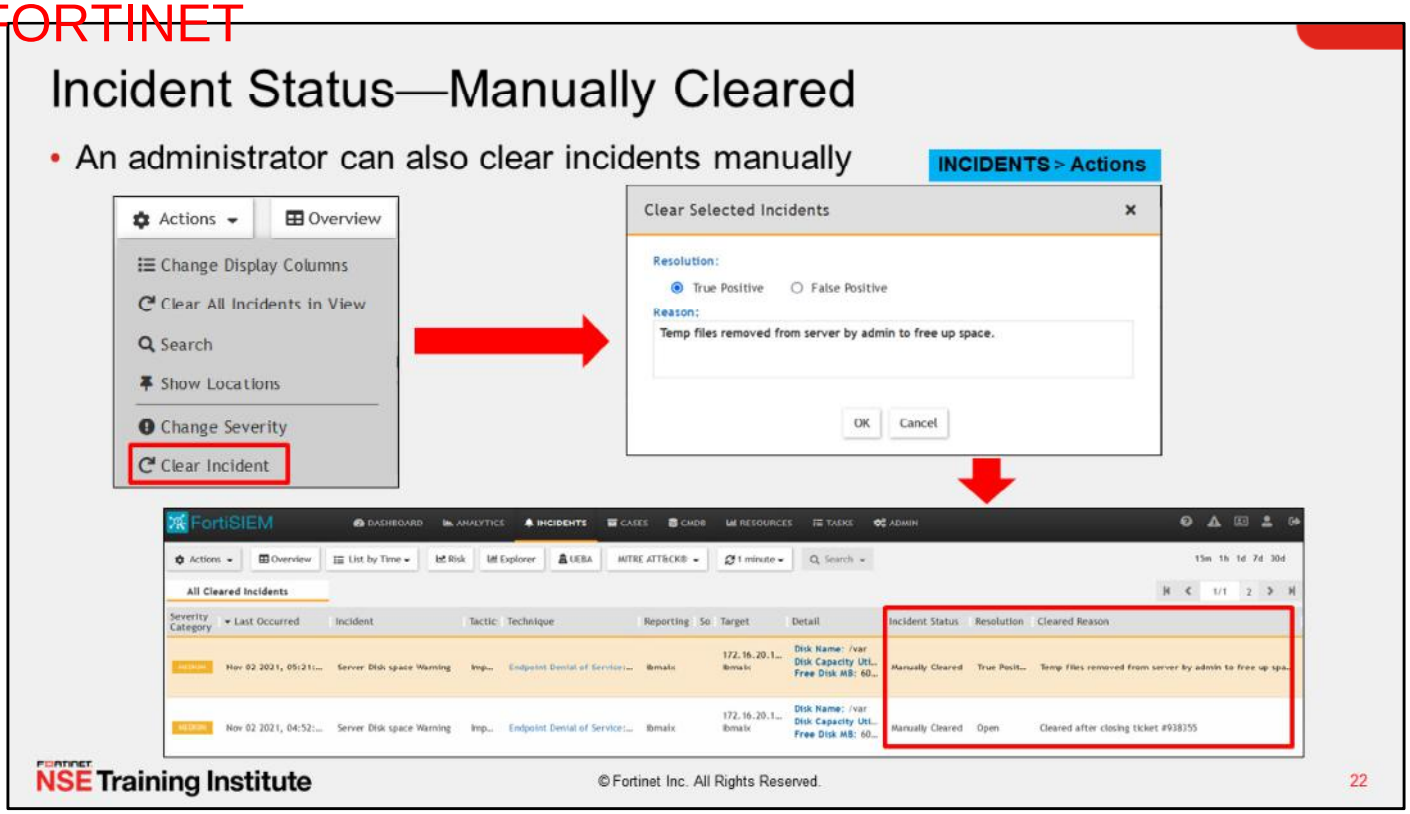
You can set the rule to clear automatically, if one or both of the following conditions are met within a specific period of time:

- **the original rule does not trigger** the incident again
- **the following conditions are met**

By default, most availability and performance rules have a **Clear** condition defined.

Vouchers & Dumps are Available | WhatsApp +201224560923

DO NOT REPRINT
© FORTINET
Brave-dumps.com



You can also clear incidents manually.

To clear one or more incidents manually, select an incident and click the **Clear** incident option from the **Actions** drop-down list. When you do, there is an option to provide a **Reason** for manually clearing the incident. The **Cleared Reason** is stored with the incident and can be reported on using FortiSIEM analytics.

The **External Cleared**, status appears only when the incident is cleared in the external ticketing system.

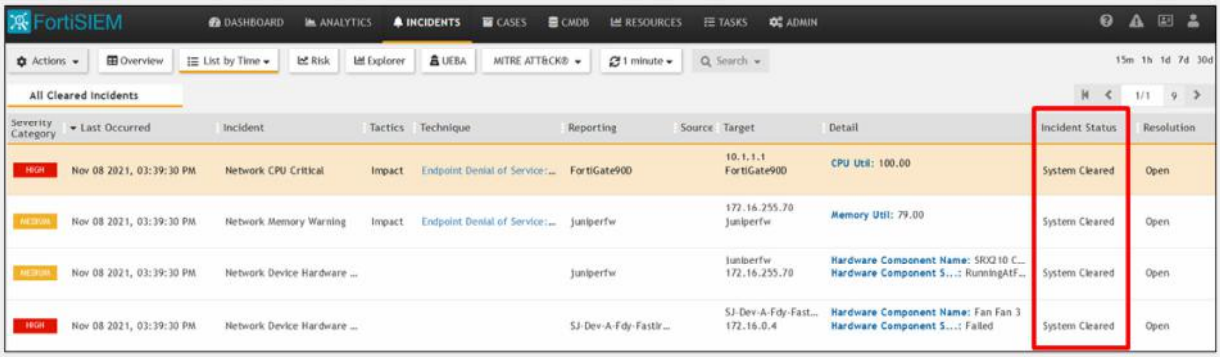
By default, the **Cleared Reason** column does not appear in the incident **List** view. You can add it by selecting it in the **Change Display Columns** option.

Vouchers & Dumps are Available | WhatsApp +201224560923

DO NOT REPRINT
© FORTINET
Brave-dumps.com

Incident Status—System Cleared

- The last incident status is called **System Cleared**
- To conserve system memory, if an unusual condition occurs where an incident (performance and availability only) is not triggered again within 24 hours, then the system considers the issue to be resolved or removed, and changes the status to **System Cleared**



- You can extend the 24-hour period using a back-end configuration file

NSE Training Institute

© Fortinet Inc. All Rights Reserved.

23

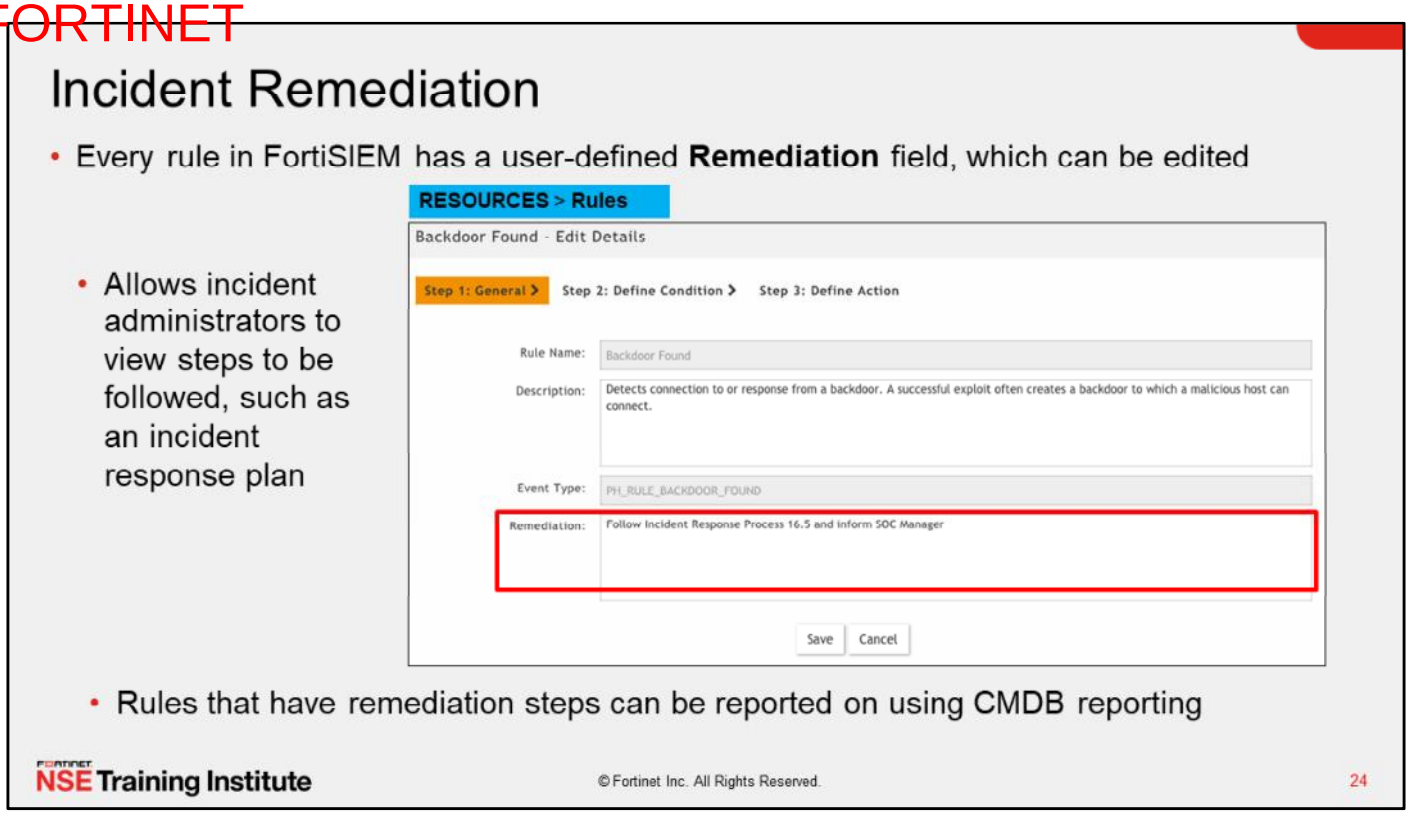
The last incident status is called **System Cleared**.

To conserve system memory, if an unusual condition occurs where an incident is not triggered again within 24 hours, then the system considers the issue to be resolved or removed, and changes the **Status Flag** to **System Cleared**. This relates only to performance and availability incidents.

You can extend the 24-hour period using a back-end configuration file.

Vouchers & Dumps are Available | WhatsApp +201224560923

DO NOT REPRINT
© FORTINET
Brave-dumps.com

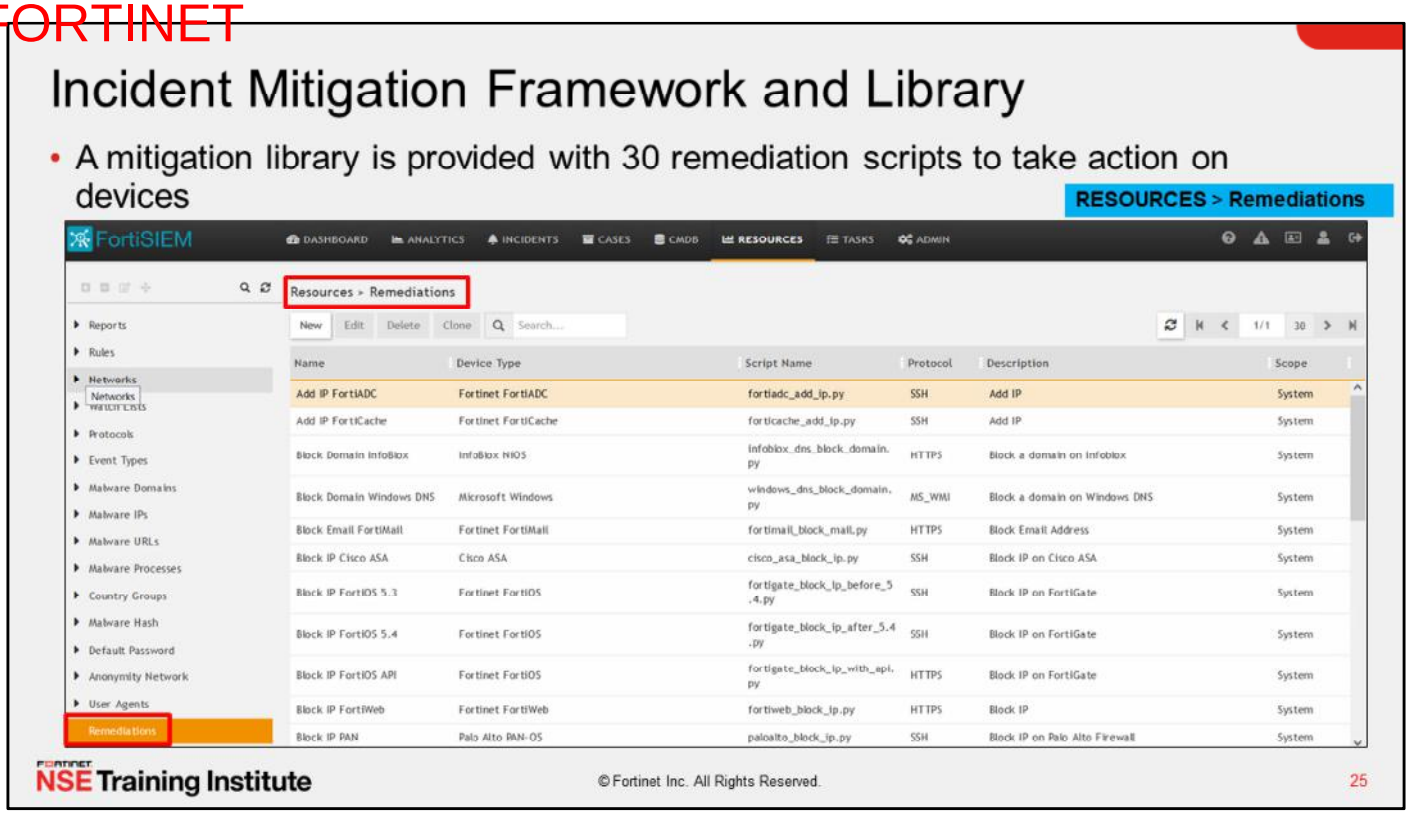


Each rule in FortiSIEM also has a user-defined **Remediation** field. To view the field, in the incidents **List** view, select an incident, then in the **Actions** drop-down list, select an **Edit Rule** option. The **Remediation** field allows you to view steps to be followed, such as an incident response plan.

You can report on rules that have remediation steps using the CMDB reporting feature.

Vouchers & Dumps are Available | WhatsApp +201224560923

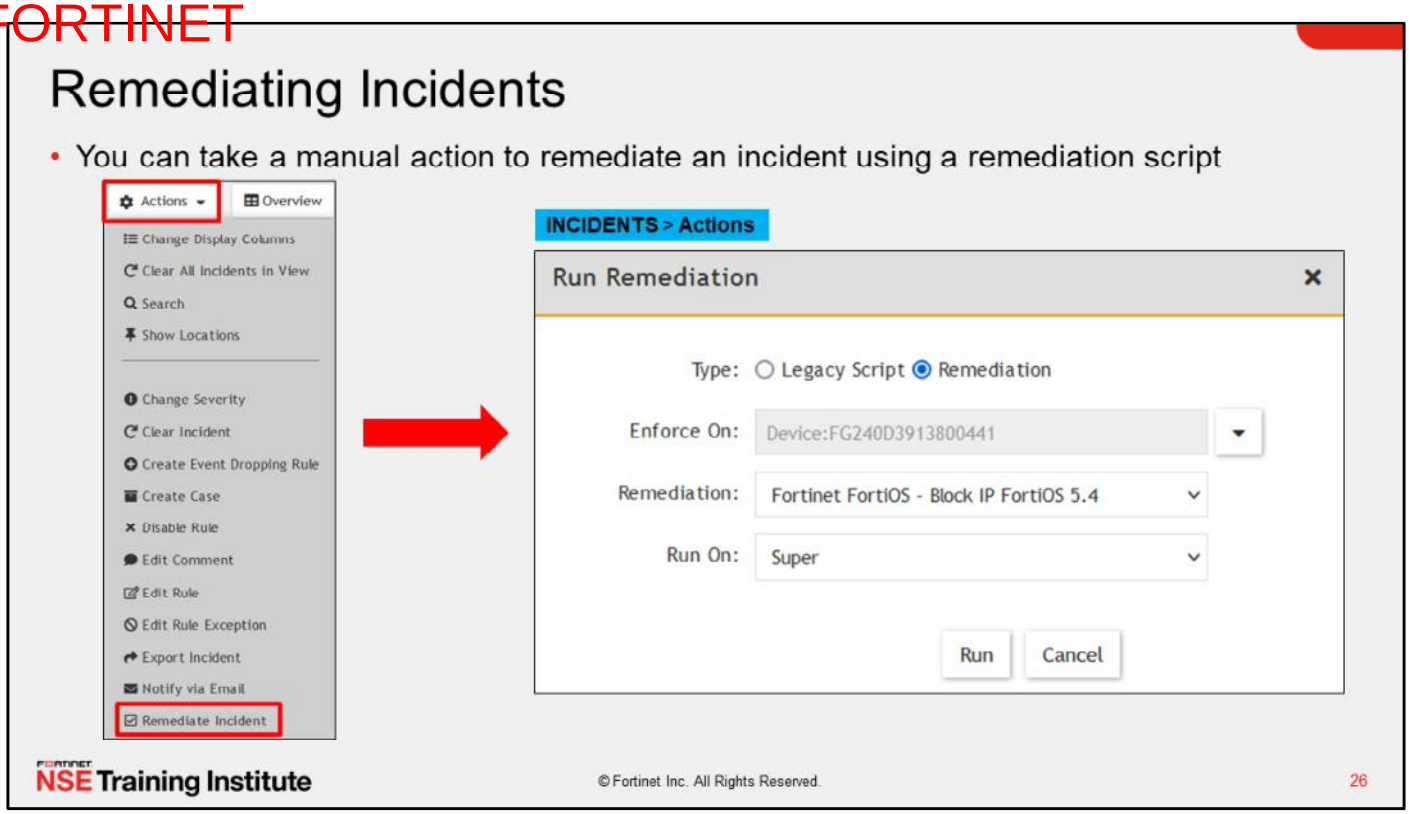
DO NOT REPRINT Brave-dumps.com
© FORTINET



A mitigation library is provided with 30 remediation scripts to take action on devices. Users can write their own remediation scripts and add them to the library from the FortiSIEM GUI.

Vouchers & Dumps are Available | WhatsApp +201224560923

DO NOT REPRINT Brave-dumps.com
© FORTINET

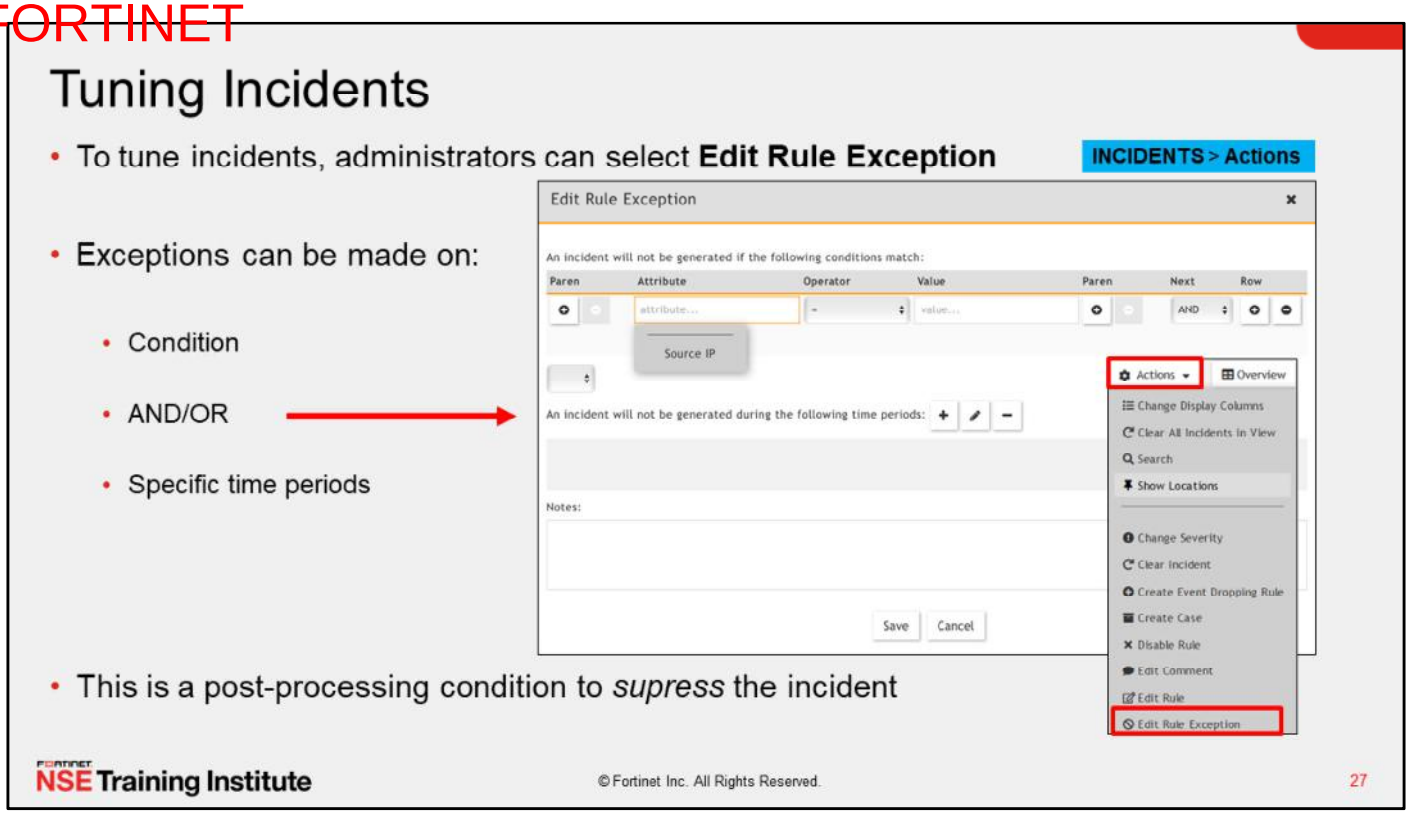


You can take a manual action to remediate an incident using a remediation script from one of 30 prebuilt scripts from mitigation library, or a custom remediation script.

To remediate an incident, select an incident , then in the incident **List** view, in the **Actions** drop-down list, select a **Remediate Incident** option. A dialog box for **Run Remediation** appears, where you can select a prebuilt or custom **Remediation** script for the selected device.

Vouchers & Dumps are Available | WhatsApp +201224560923

DO NOT REPRINT Brave-dumps.com
© FORTINET



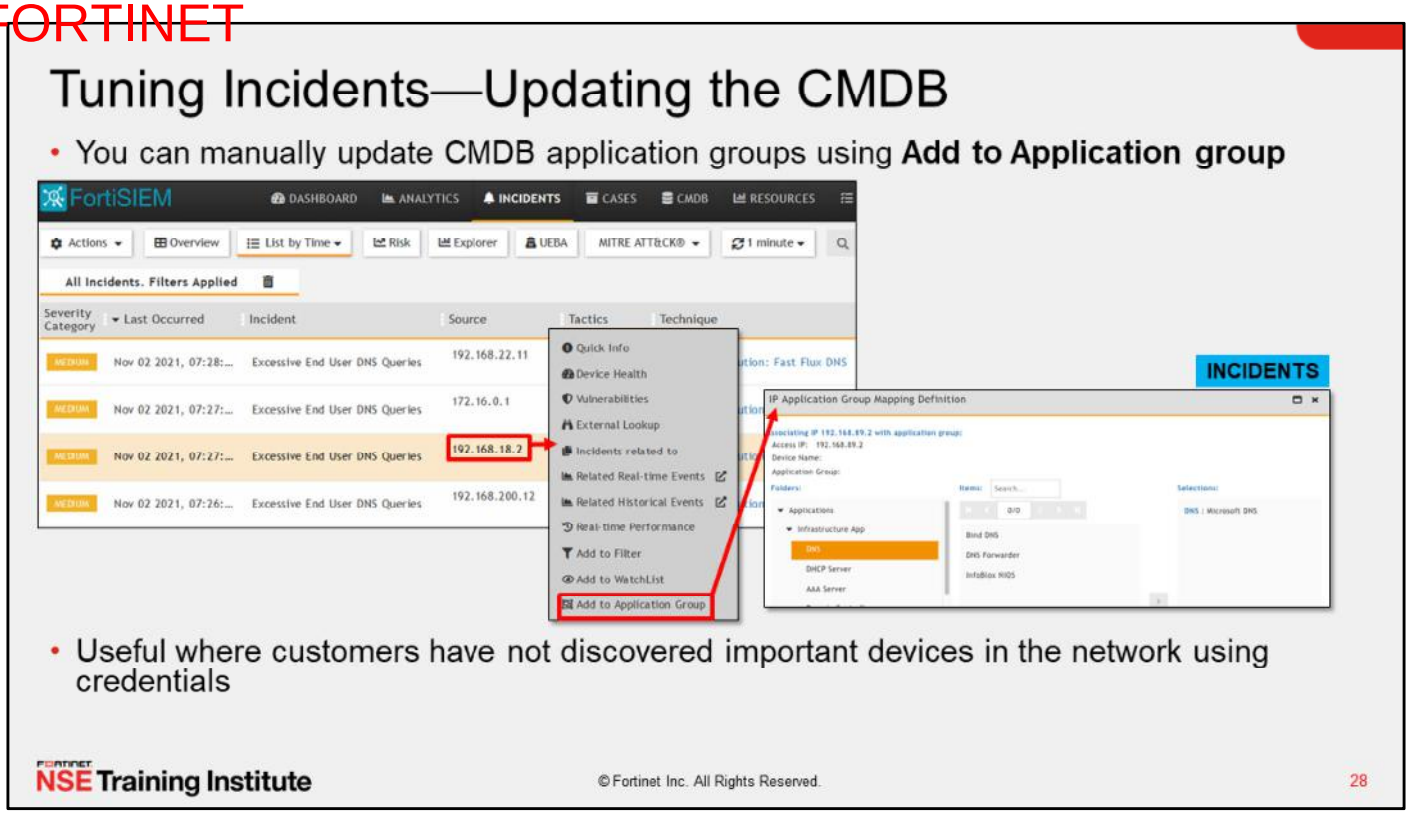
Over time, you may notice that some rules are too sensitive and, therefore, generate noisy incidents. FortiSIEM allows you to tune incidents by adding exceptions to rules.

To add exceptions to rules for an incident, in the **Actions** drop-down list, select **Edit Rule Exception**. You can make exceptions only for attributes that appear in this list. These are the attributes associated with the incident definition, including the **Aggregated** and **Group By** attributes.

You can also create exceptions based on specific time periods. For example, you can specify an AND condition for a specific time period, you can specify an OR condition for a specific time period. This is called a post-processing condition, which instantly suppresses the triggered incident.

Vouchers & Dumps are Available | WhatsApp +201224560923

DO NOT REPRINT
© FORTINET
Brave-dumps.com

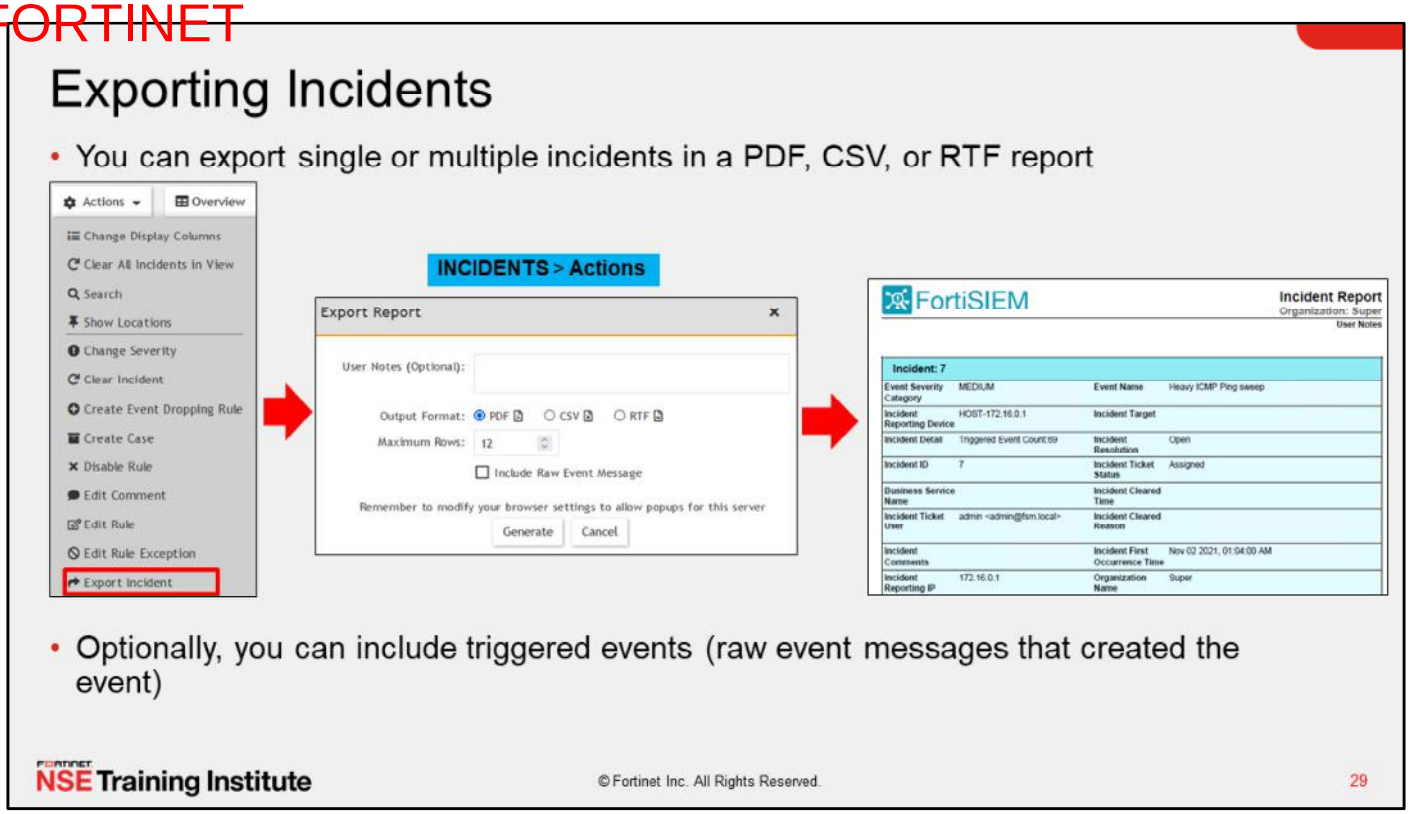


Another method to help with incident tuning is to select **Add to Application group** for an incident **Source** or incident **Target**. This attribute adds the IP address manually to the application groups. This is useful in scenarios where customers have not discovered important devices in the network using credentials.

A credential discovery populates the application groups automatically.

Vouchers & Dumps are Available | WhatsApp +201224560923

DO NOT REPRINT Brave-dumps.com
© FORTINET

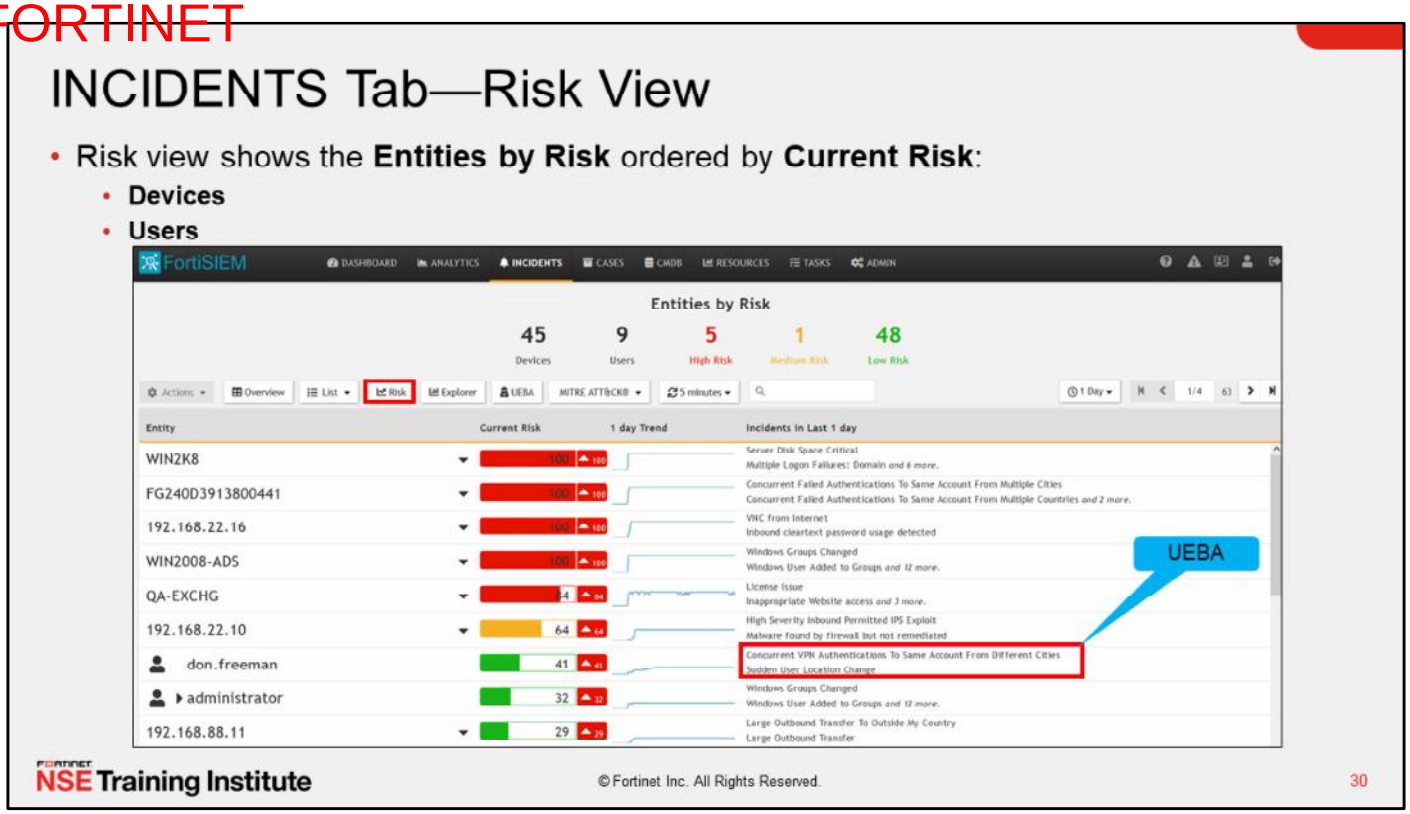


On the Incident **List** view, select an incident and then select **Export Incident** from the **Actions** drop-down list. You can export single or multiple incidents as either a PDF, CSV, or RTF report.

When you perform an export, you have the option to include the triggered **Events**, which are the **Raw Event Messages** from which the event was created.

Vouchers & Dumps are Available | WhatsApp +201224560923

DO NOT REPRINT
© FORTINET
Brave-dumps.com



The **Risk** view shows the **Devices** and **Users** ordered by risk. Risk is calculated based on the triggering incidents using a proprietary algorithm that incorporates asset criticality, incident severity, frequency of incident occurrence and vulnerabilities found. Risk is computed only for devices in the CMDB, private IP addresses, and users found in logs or discovered through LDAP.
Devices and users are categorized by risk as follows:

- **Devices**: The number of devices with risk
- **Users**: The number of users with risk
- **High Risk**: The number of devices and users with high risk
- **Medium Risk**: The number of devices and users with medium risk
- **Low Risk**: The number of devices and users with low risk

Several machine learning-based user and entity behaviour analytics (UEBA) models are part of the FortiSIEM inbuilt rule library:

- Detect simultaneous logins from two different countries.
- Detect simultaneous logins from two improbable geo-locations.
- Login behavior anomaly—log on to servers and at times that one does not typically log on and so on.
- Detecting traffic to dynamically generated domains.

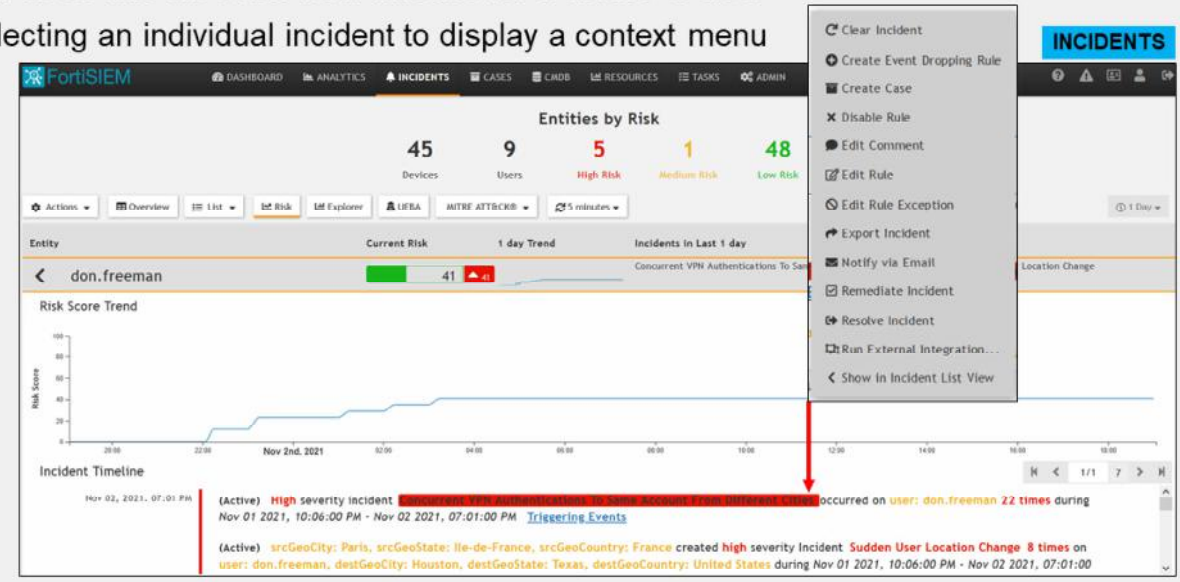
UEBA is defined as a cybersecurity process about detection of insider threats, targeted attacks, and financial fraud. UEBA solutions look at patterns of human behavior, and then apply algorithms and statistical analysis to detect meaningful anomalies from those patterns, anomalies that indicate potential threats. Instead of only tracking only devices or security events, UEBA tracks system users.
FortiSIEM has a large number of built-in behavioral anomaly rules that work out of the box but can be adapted by the user to their own environment. FortiSIEM provides framework where the user can write new rules using the GUI, test them with real events, and then deploy them in the system. To see only the above categories of devices and users in the **Risk** view, click on any of the five categories listed.

Vouchers & Dumps are Available | WhatsApp +201224560923

DO NOT REPRINT Brave-dumps.com
© FORTINET

Risk View—Drill Down

- Drill down into the **Risk** view timeline for a device or user
- Selecting an individual incident to display a context menu



NSE Training Institute © Fortinet Inc. All Rights Reserved. 31

The **Risk** view displays the following:

- Device or user name
- Current risk (current value, up or down)
- 24-hour risk trend
- Incidents in Last 24 hours

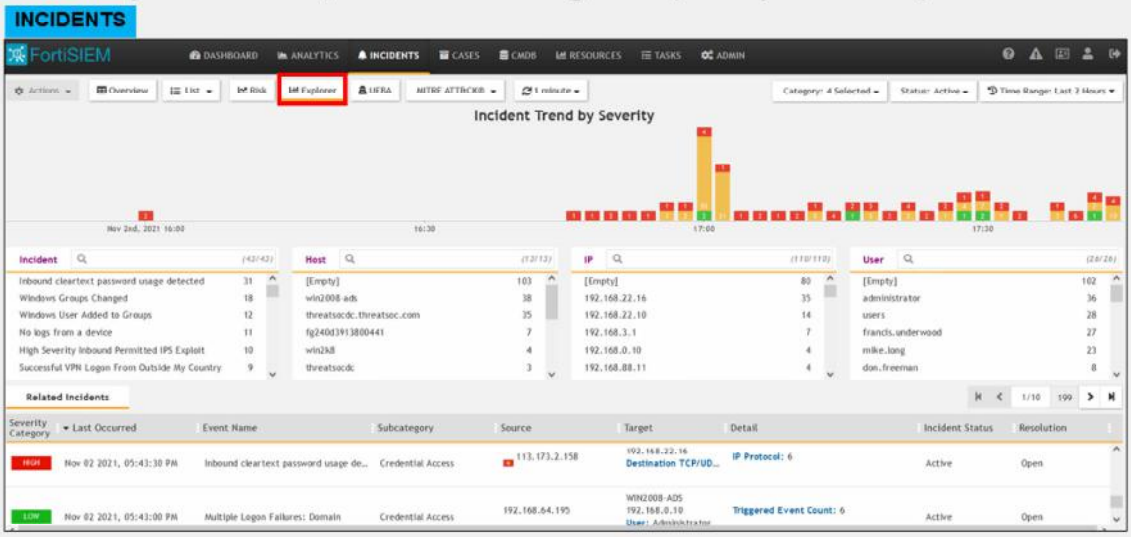
To drill down, click on a risk row. The incidents that led to this risk are shown in a timeline. You can select an incident, and select any action from **Action** menu in the same way you can on the **List** view.

Vouchers & Dumps are Available | WhatsApp +201224560923

DO NOT REPRINT Brave-dumps.com
© FORTINET

INCIDENTS Tab—Explorer View

- The Incident **Explorer** view allows you to correlate actors **IP**, **Host**, and **User** across multiple incidents, without creating multiple reports in separate tabs.



NSE Training Institute © Fortinet Inc. All Rights Reserved. 32

The Incident **Explorer** view allows you to correlate actors (IP, Host, User) across multiple incidents, without creating multiple reports in separate tabs. Incident trends, Actor and Incident detail are displayed on the same page. You can choose an actor and see all the incidents that actor is part of. You can then choose a time range and narrow down the incidents. Time ranges, actors, and incidents can be chosen in any order. Each time a selection is made, the rest of the dashboard updates to reflect that selection.

The incident **Explorer** view is divided into three layers

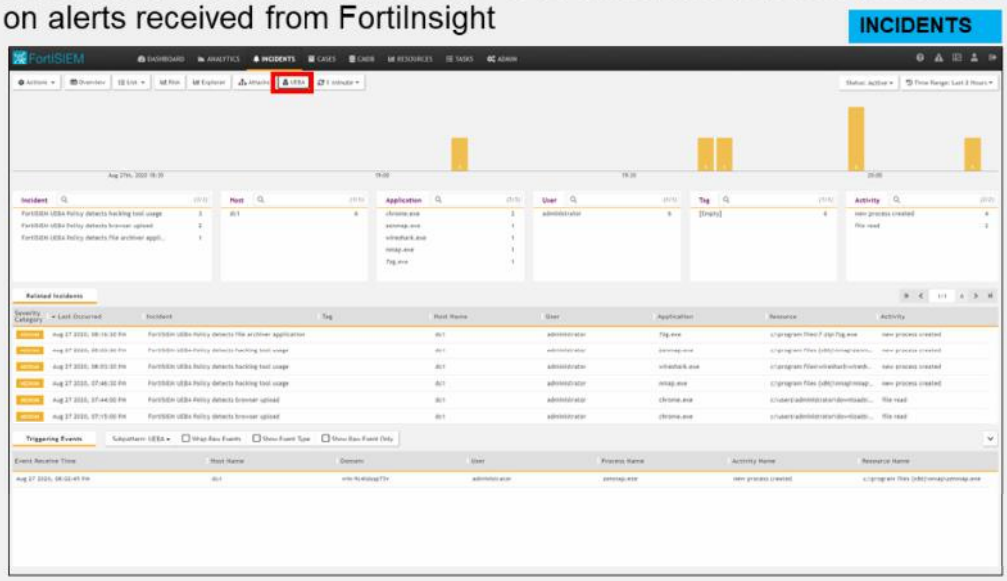
- The top section displays the **Incident Trend By Severity**. The graph displays the incident counts over time, organized by severity, then by count.
- Each bar in the graph represents the number of incidents at a given time. The colors reflects the incidents severity: Red is high severity, yellow is medium severity, and green is low severity. The numbers in the bars reflect the number of unique incidents triggered in the selected time window.
- The middle section displays panels **for Incidents**, **Hosts**, **IP**, and **Users**. You can filter the items in the panels by **Category**, **Status**, and **Time Range**.
- The bottom section displays the Incidents table with these headings: **Severity Category**, **Last Occurred**, **Event Name**, **Subcategory**, **Source**, **Target**, **Detail**, **Incident Status**, and **Resolution**.
- Drill down is available from the **Target**, **Detail**, **Resolution** columns.

Vouchers & Dumps are Available | WhatsApp +201224560923

DO NOT REPRINT Brave-dumps.com
© FORTINET

INCIDENTS Tab—UEBA View

- The UEBA incident dashboard shows the UEBA incidents that the AI module creates based on alerts received from FortiInsight



NSE Training Institute

© Fortinet Inc. All Rights Reserved.

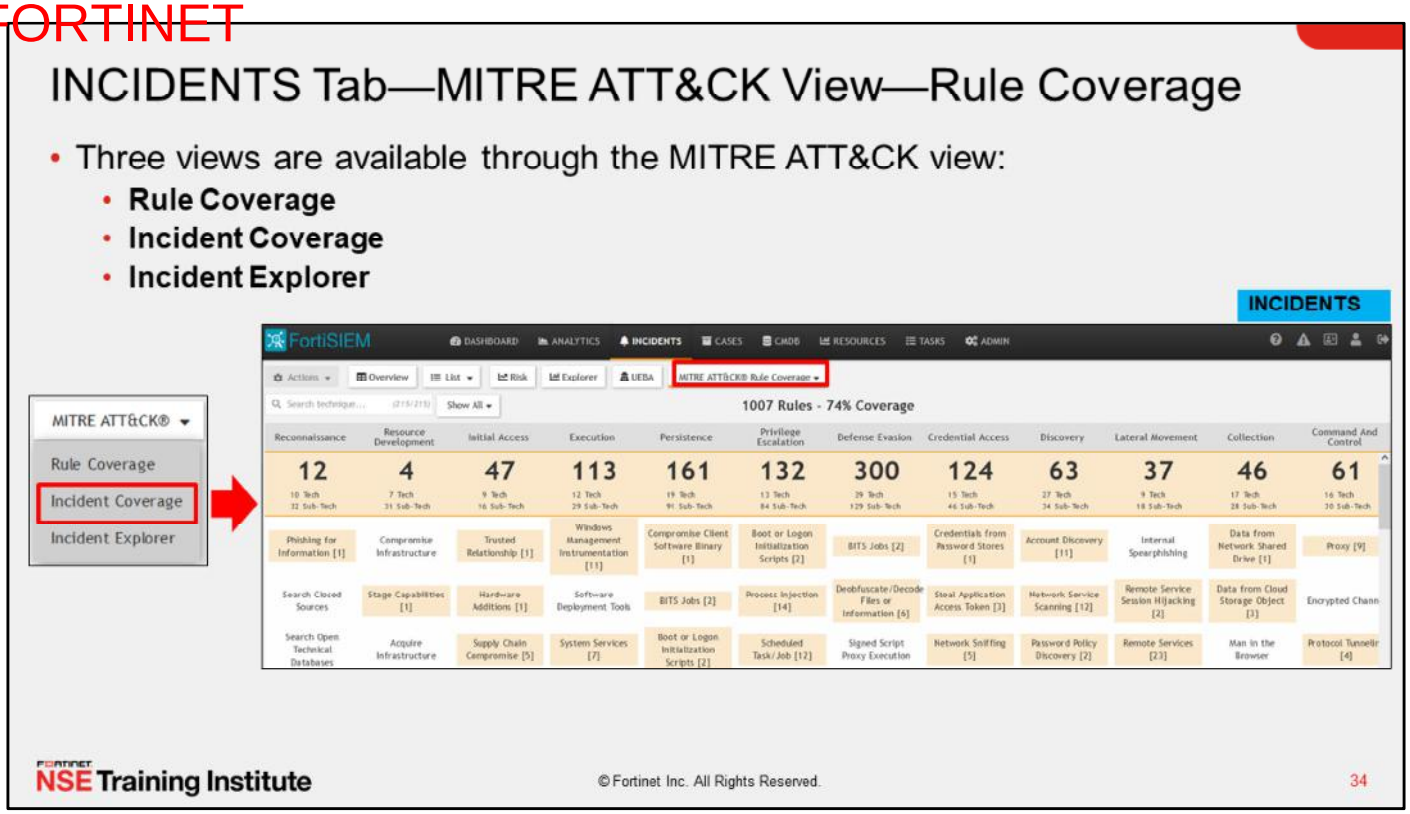
33

The UEBA incident dashboard shows the UEBA incidents that the AI module creates. The attribute list table provides the following information about AI alerts received from FortiInsight:

- **Incident**: The name of the incident that was detected
- **Host**: The host name or IP address where the alert originated
- **Application**: The name of the application that is the source of the incident
- **User**: The Windows agent user
- **Tag**: The tag used to categorize the alert
- **Activity**: The description of the activity that raised the alert

Vouchers & Dumps are Available | WhatsApp +201224560923

DO NOT REPRINT Brave-dumps.com
© FORTINET



Three views are available through the MITRE ATT&CK view:

- **Rule Coverage:** This view provides an overview of the tactics and techniques that FortiSIEM covers as defined by MITRE corporation.
- **Incident Coverage:** This view provides an overview of the security incidents detected by FortiSIEM that fall under the tactics and techniques as defined by MITRE corporation.
- **Incident Explorer:** This view maps security incidents detected by FortiSIEM into attack categories defined by MITRE corporation.

The **Rule Coverage** view provides an overview of the tactics and techniques that FortiSIEM covers as defined by MITRE Corporation. The top row displays the number of rules and the percentage of MITRE techniques that FortiSIEM covers. In the main row header, the bolded number that appears under each tactic indicates the number of rules that are covered under it. Clicking a tactic here will show all the rules that belong to it. Each tactic cell also lists the number of major techniques (Tech) and sub techniques (Sub-Tech) related to the involved tactic. All major techniques related to a tactic are listed underneath their respective tactic column. Tactics and techniques covered by FortiSIEM rules are indicated by a light yellow background.

You can hover your mouse cursor over any major technique to view the following information:

- The total number of rules covered by the technique (security category)
- The number of rules covered by each sub-technique (if applicable)

Vouchers & Dumps are Available | WhatsApp +201224560923

DO NOT REPRINT Brave-dumps.com
© FORTINET

MITRE ATT&CK View—Incident Coverage

- The **Incident Coverage** dashboard shows MITRE ATT&CK coverage for incidents
- The top row displays the number of incidents detected by FortiSIEM in the time range specified



NSE Training Institute
© Fortinet Inc. All Rights Reserved.
35

The **Incident Coverage** view provides an overview of the security incidents detected by FortiSIEM that fall under the tactics and techniques as defined by MITRE Corporation. The top row displays the number of incidents detected by FortiSIEM in the time range specified. In the main row header, the bolded number that appears under each tactic indicates the number of incidents associated with a specific tactic. Clicking a tactic displays all related detected incidents. Each tactic cell also lists the number of major techniques (Tech) and sub-techniques (Sub-Tech) related to the involved tactic and incidents. All major techniques related to a tactic are listed underneath their respective tactic column. Tactics and techniques covered by FortiSIEM rules are indicated by a light yellow background.

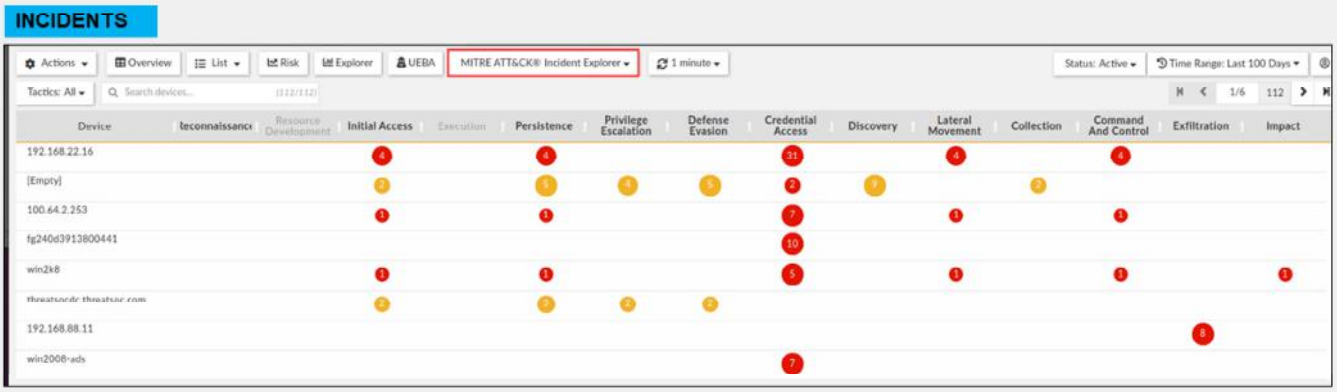
You can hover your mouse cursor over any major technique to view the following information:
- The total number of incidents triggered by this technique
- The number of incidents triggered by each sub-technique (if applicable)

Vouchers & Dumps are Available | WhatsApp +201224560923

DO NOT REPRINT
© FORTINET
Brave-dumps.com

MITRE ATT&CK View—Incident Explorer

- The **Incident Explorer** view maps security incidents detected by FortiSIEM into attack categories defined by MITRE
- The incident explorer displays a host-centric, interactive ATT&CK view



NSE Training Institute

© Fortinet Inc. All Rights Reserved.

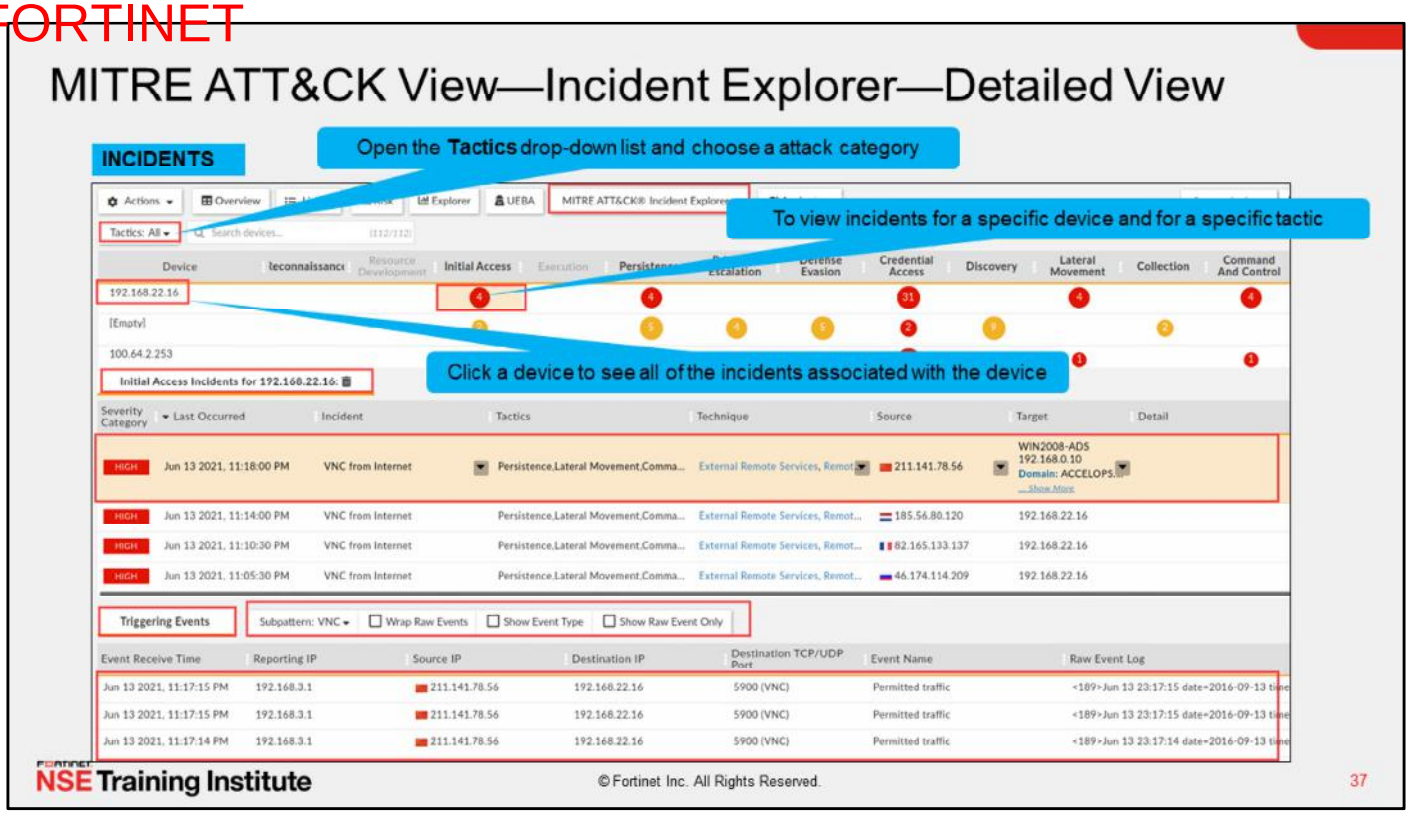
36

The **Incident Explorer** view maps security incidents detected by FortiSIEM into attack categories defined by MITRE Corporation. The **Incident Explorer** shows a host-centric, interactive ATT&CK view. The number in the middle of the circle indicates the number of incidents in that category. The size of the circle is relative to the number of incidents.

The color of the circle indicates the severity of the incident: red=high severity, yellow=medium severity, and green=low severity.

Vouchers & Dumps are Available | WhatsApp +201224560923

DO NOT REPRINT Brave-dumps.com
© FORTINET



You can populate the table in any of these ways:

- Click a device to see all of the incidents associated with the device.
- Click the **Tactics** drop-down list and choose one of the attack categories.
- Click the number in the middle of the circle to view incidents for a specific device and for a specific tactic.

Vouchers & Dumps are Available | WhatsApp +201224560923

DO NOT REPRINT
© FORTINET
Brave-dumps.com

Knowledge Check

1. What are the four categories of incidents?
   - ✓A. **Performance**, **Availability**, **Security**, and **Change**
   - B. **Devices**, **Users**, **High Risk**, and **Low Risk**

2. A FortiSIEM administrator wants to view the top impacted hosts by severity. Which incidents tab view will provides this information by default?
   - ✓A. **Overview**
   - B. **List**
   - C. **Risk**

NSE Training Institute

© Fortinet Inc. All Rights Reserved.

38

Vouchers & Dumps are Available | WhatsApp +201224560923

DO NOT REPRINT
© FORTINET
Brave-dumps.com

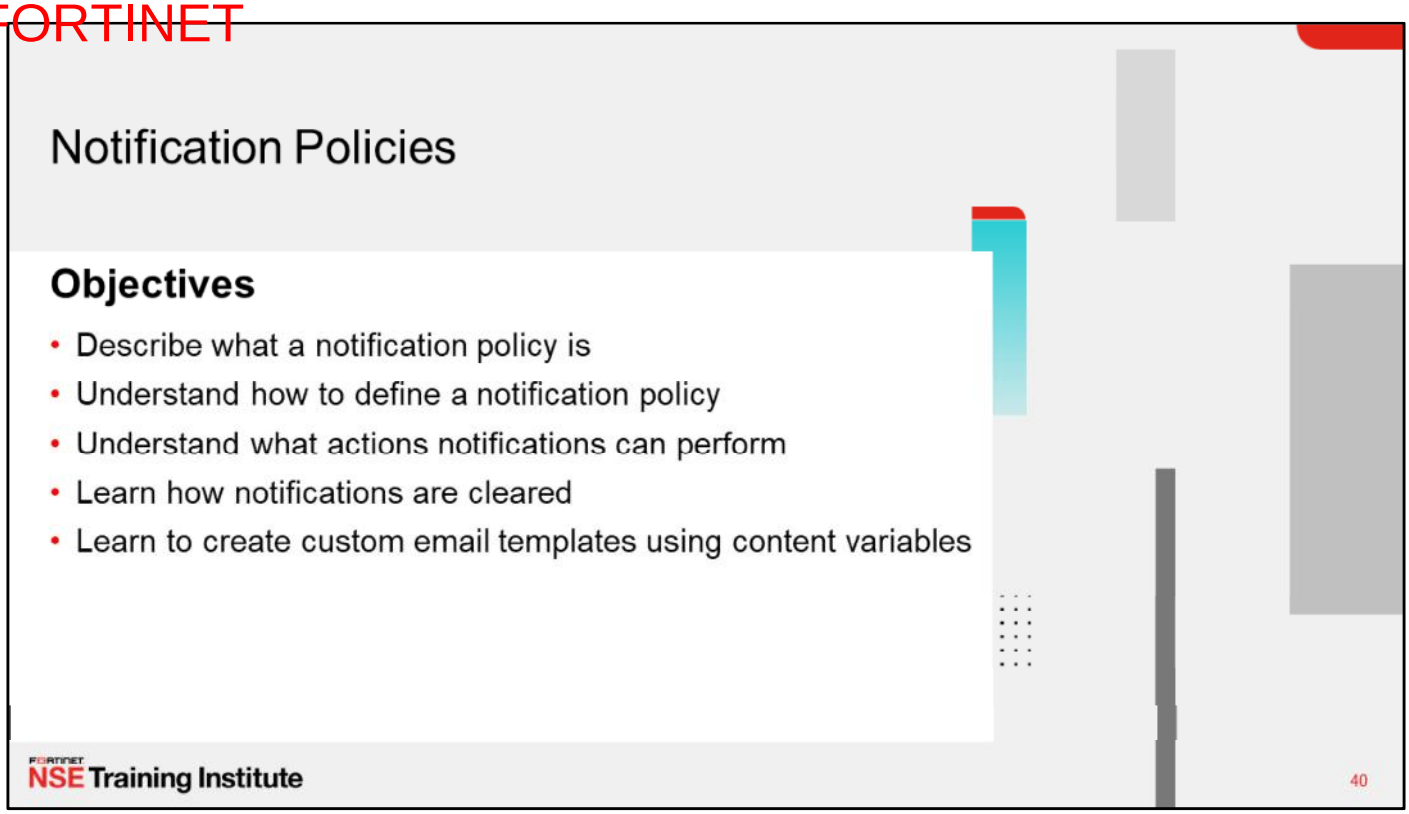


Good job! You now understand incidents.

Now, you will examine notification policies.

Vouchers & Dumps are Available | WhatsApp +201224560923

DO NOT REPRINT
© FORTINET
Brave-dumps.com

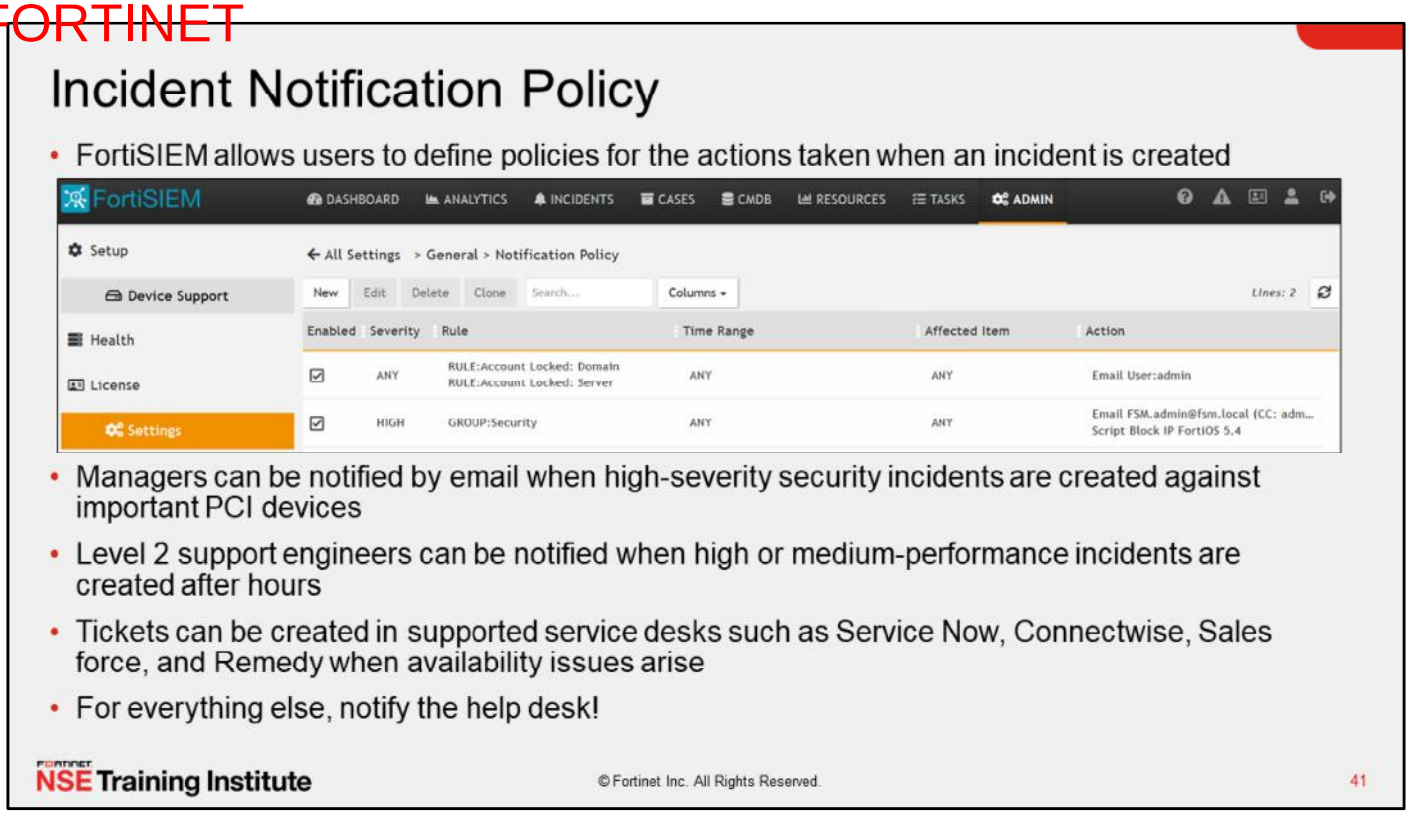


After completing this section, you should be able to achieve the objectives shown on this slide.

By demonstrating competence in notification policies, you will be able to manage and notify users of incidents in your network.

Vouchers & Dumps are Available | WhatsApp +201224560923

DO NOT REPRINT
© FORTINET
Brave-dumps.com



FortiSIEM allows users to define policies for the actions that are taken when an incident is created.

The severity of an incident is determined by the rule itself. Each rule has a severity rating. You can use this information as a trigger in the notification policy.

For example, managers can be notified by email when high-severity security incidents are created against important PCI devices.

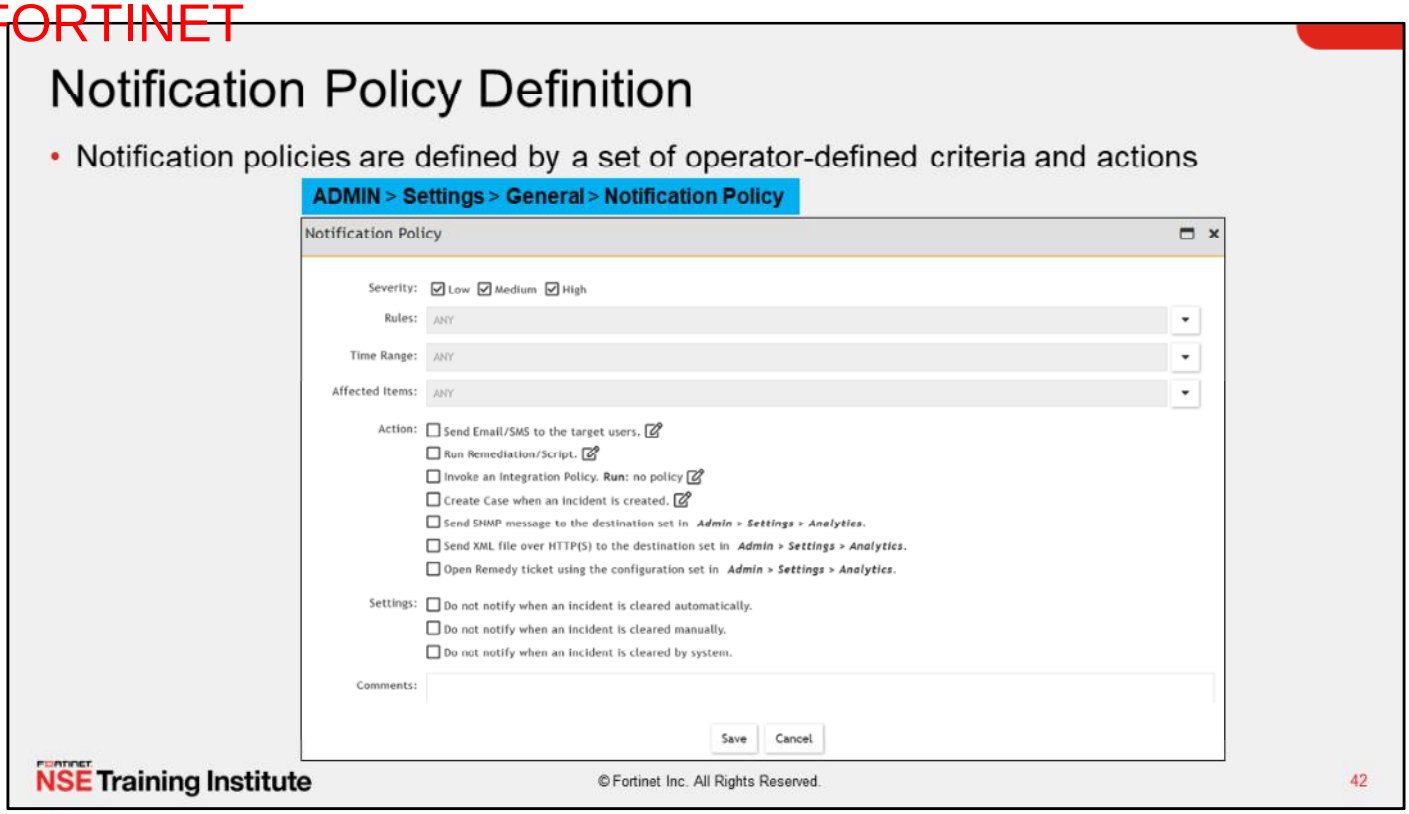
Level 2 support engineers can be notified when high or medium-performance incidents are created after hours. You can define time ranges within the policy to decide when to send notifications.

You can create tickets in supported service desks such as Service Now, Connectwise, and Remedy, when availability issues arise.

You can report everything else by email to the help desk!

Vouchers & Dumps are Available | WhatsApp +201224560923

DO NOT REPRINT
© FORTINET
Brave-dumps.com



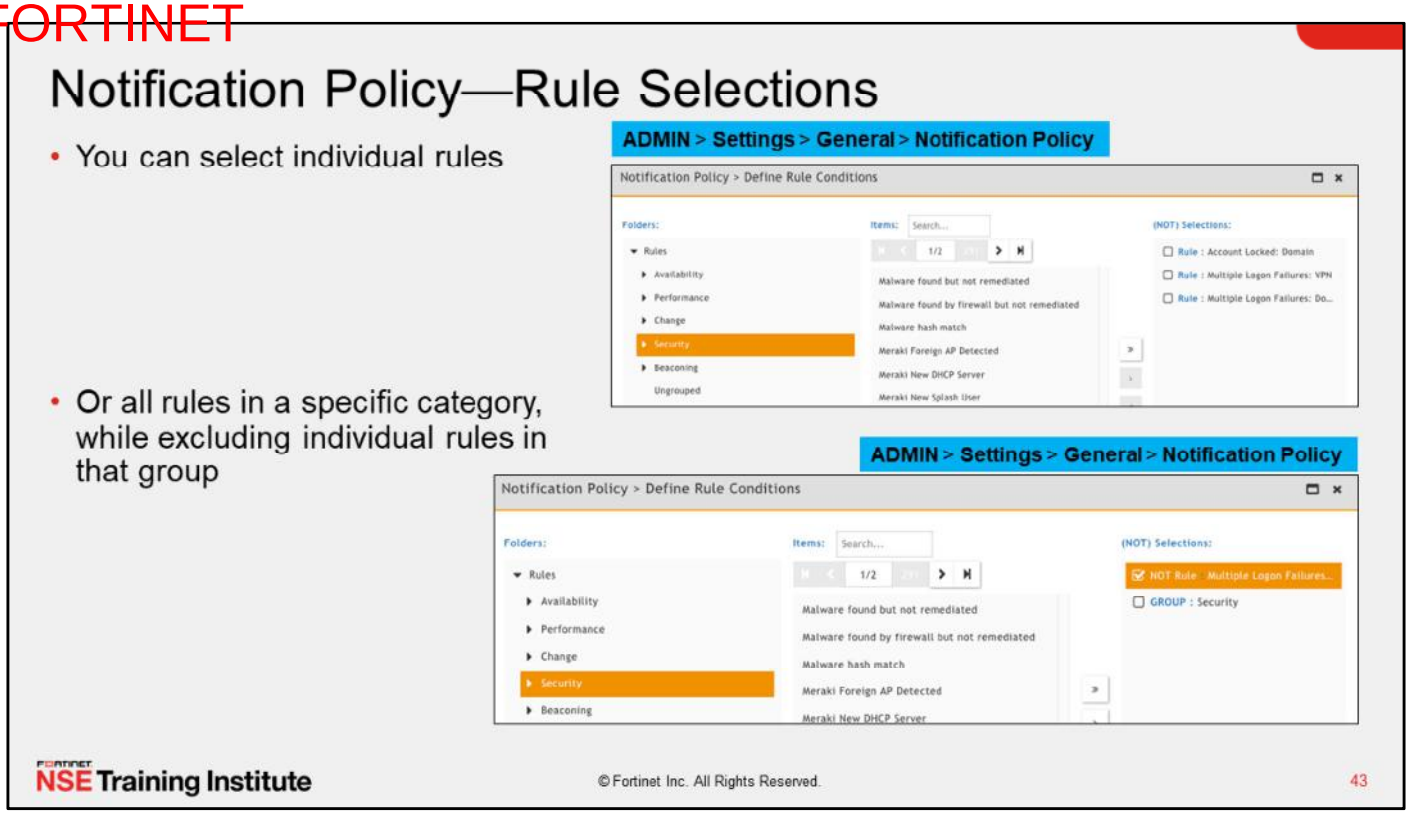
Notification policies are defined by a set of operator-defined criteria and actions.

The defining criteria are: the rule **Severity**, the associated **Rules**, a **Time Range**, and the **Affected Items**.

You can create as many notification policy definitions as you need.

Vouchers & Dumps are Available | WhatsApp +201224560923

DO NOT REPRINT
© FORTINET
Brave-dumps.com



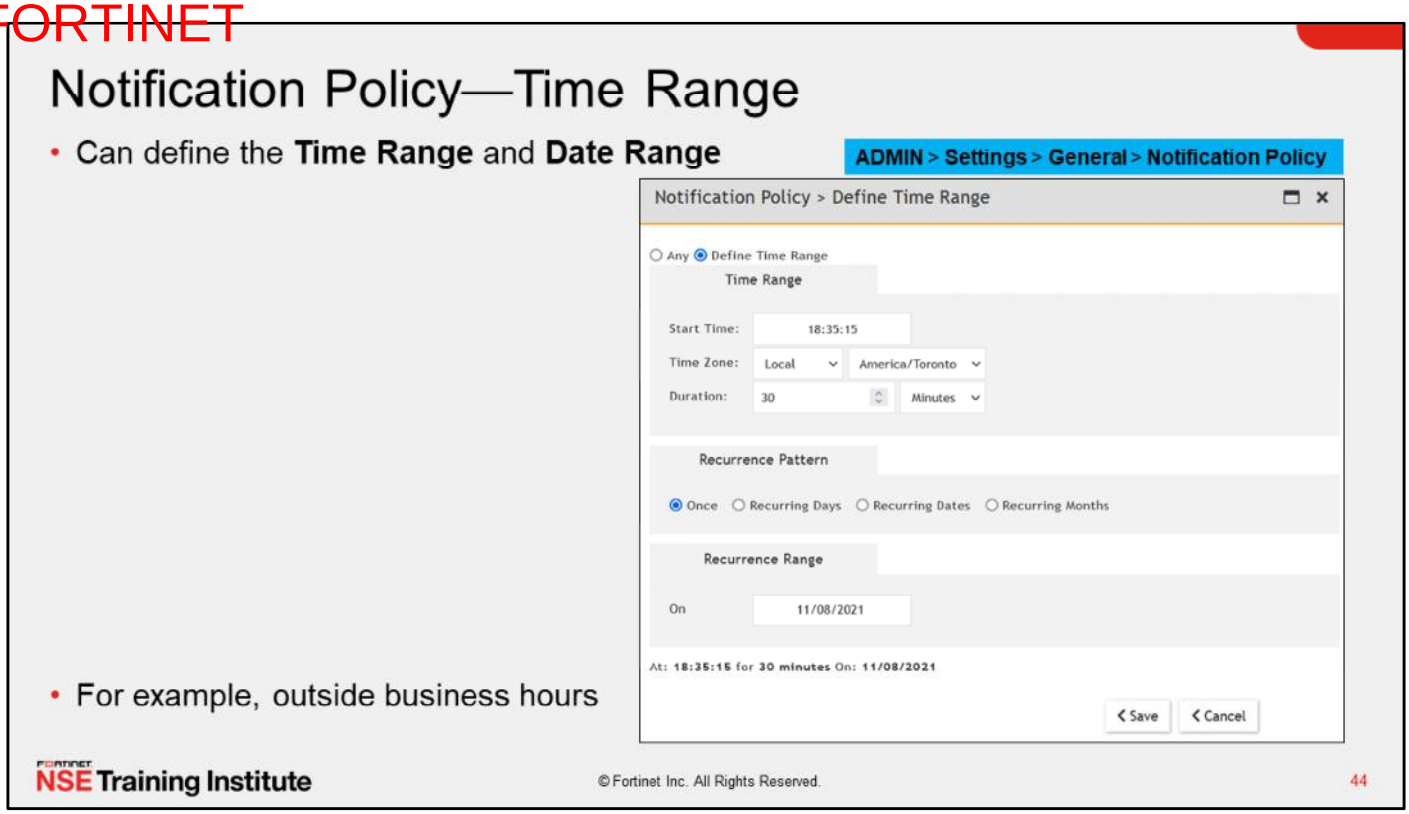
When selecting which rules the notification policy is associated with, you can select individual rules or a category of rules.

If you select a category of rules, you can also select individual rules in that category, and then select the **NOT** option to exclude a specific rule (or rules) in the category.

You also have the option to select **Any** rule to associate the policy with all the rules in the system.

Vouchers & Dumps are Available | WhatsApp +201224560923

DO NOT REPRINT Brave-dumps.com
© FORTINET



You can also define time and date ranges.

For example, you can set a time and date range to create a policy that is related to rules or incidents that are triggered outside business hours, or within a certain date range.

If the **Duration** field is set to zero, then the time range is not considered when evaluating this time expression.

If an **End Date** is not specified, then you have the choice of indicating whether the **Start Date** represents a single date (on this date only) or the beginning of a recurring date span (from this date forward).

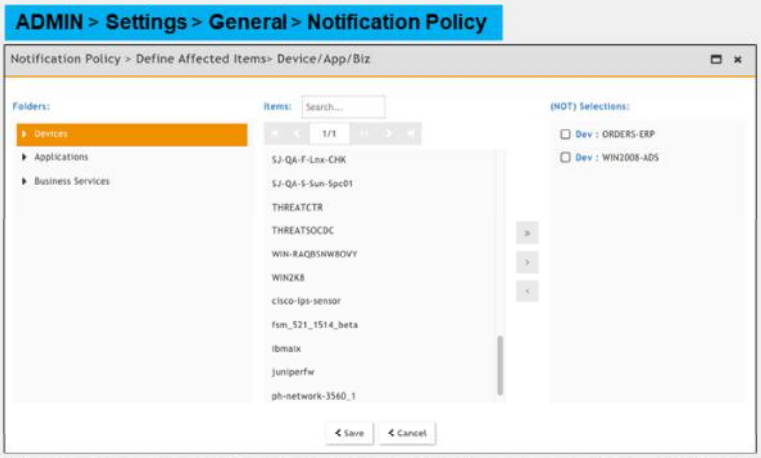
You can also specify specific recurring days of the week or month, and specific recurring months.

Vouchers & Dumps are Available | WhatsApp +201224560923

DO NOT REPRINT Brave-dumps.com
© FORTINET

Notification Policy—Affected Items

- **Affected Items** are the incident target devices
- You can select either individual devices or device categories referencing the CMDB



- The category could also be an application group, business service, or IP address or range

NSE Training Institute © Fortinet Inc. All Rights Reserved. 45

Affected Items are the incident target devices. You can select either individual devices or device categories referencing the CMDB.

The category could also be an application group or business service, or you can define an IP address or range manually.

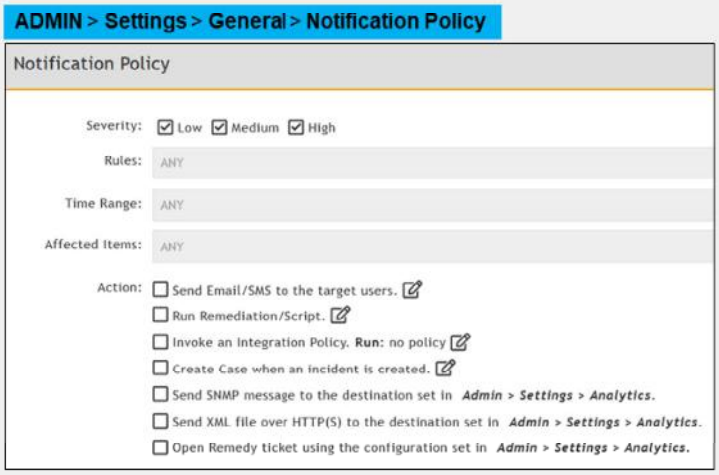
In a previous example in which managers were notified by email when high-severity security incidents were created against important PCI devices, the notification policy had the rules criteria set to Group:Security, which is to say, all the rules in the security group. There are more than 200 rules in that group, which will cover all of the devices in the network. However, you are interested only in devices that belong to the PCI services group, you can use the **Affected Items** criteria to focus the policy on a sub-set of devices covered by the rule set.

Vouchers & Dumps are Available | WhatsApp +201224560923

DO NOT REPRINT Brave-dumps.com
© FORTINET

Notification Policy—Actions

- Define actions for something to occur when the policy criteria matches
- Such as:
  - Send an alert to the console, with the option to play a sound
  - Invoke an integration policy for ticketing with third-party systems
  - Send an SNMP message or POST an XML file using or HTTPS
  - Open a remedy ticket or create a ticket in FortiSIEM's own Case feature
  - Send an email or SMS message, or run a script



NSE Training Institute

© Fortinet Inc. All Rights Reserved.

46

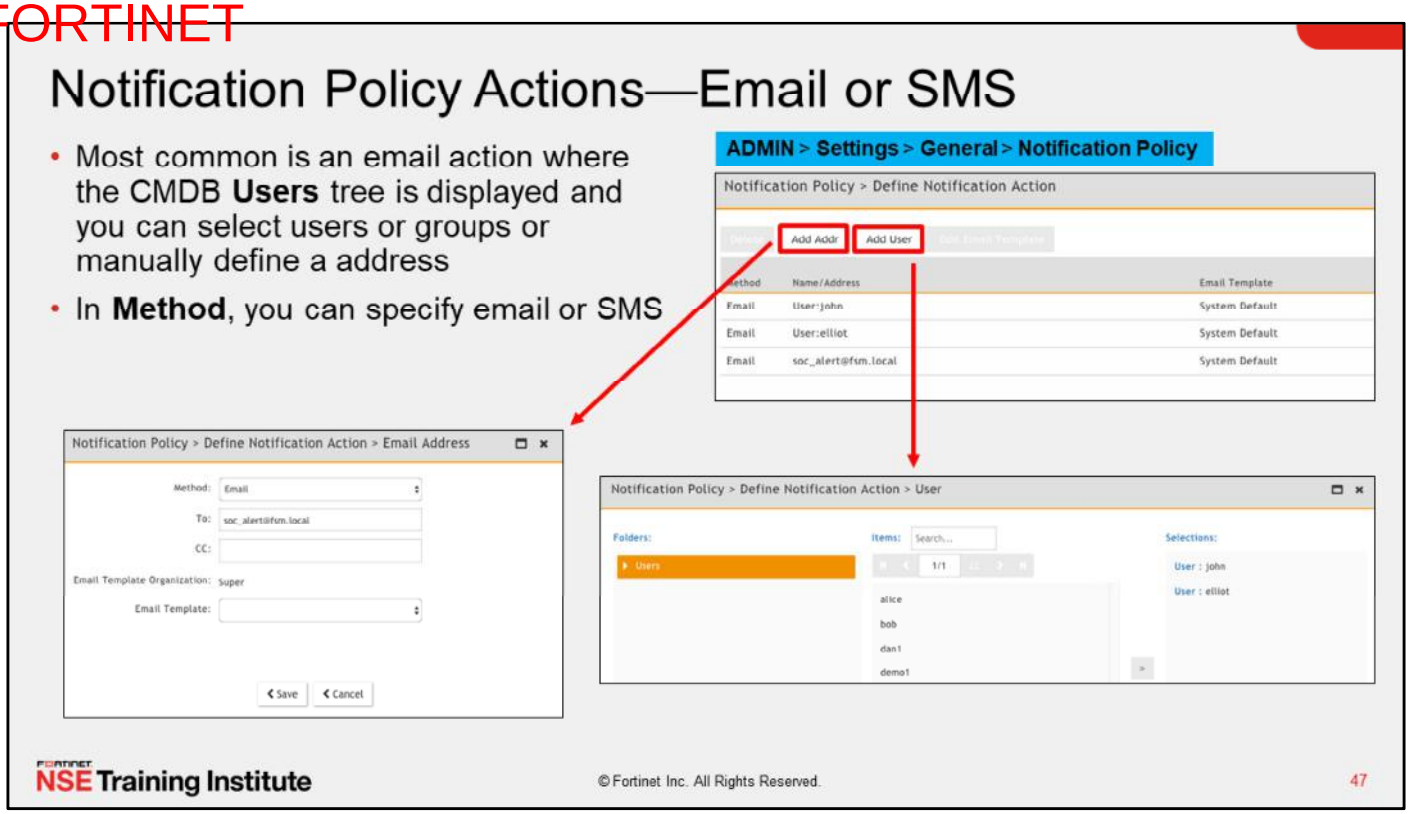
You can select a notification **Action** to occur as part of a notification policy.

You can set the system to perform any combination of the actions, from sending an alert to the console with the option to play a sound, to invoking an integration policy that FortiSIEM uses for integration with third-party CMDB and help desk or workflow systems, such as Connectwise, ServiceNow, Remedy or Salesforce.

You can also send email notifications and SMS messages to individuals or to groups.

Vouchers & Dumps are Available | WhatsApp +201224560923

DO NOT REPRINT
© FORTINET
Brave-dumps.com



The most common notification policy action is an email message.

If FortiSIEM is connected to your LDAP server, all of your users are listed in the CMDB **User** tree. You can select individual users or groups to notify. Alternatively, you can specify an email address manually.

In the **Method** column, in the drop-down list, you can choose to send the notification either as an **Email** or an **SMS** message on a user-by-user basis.

If you select **Email**, then you can select the email template to use for a specific user. Different users can be sent email messages that use different templates. It is not necessary to send the same email to everyone being notified by this policy.

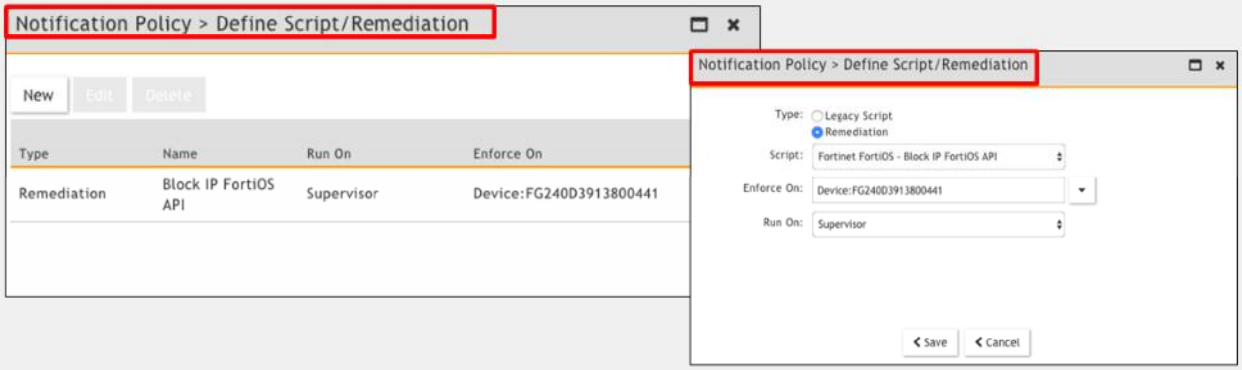
You can also have the system run a script. After you provide the script location, you can specify whether the script will run on the **Supervisor** or a **Collector**.

Vouchers & Dumps are Available | WhatsApp +201224560923

DO NOT REPRINT
© FORTINET
Brave-dumps.com

Notification Policy Actions—Run a Remediation Script

- **Define Script/Remediation**: Allows the user to define multiple automated remediation actions
- **Enforce On**: Determines which the script will be running from
- **Run On**: Identifies whether the script runs from the supervisor or a collector



NSE Training Institute

© Fortinet Inc. All Rights Reserved.

48

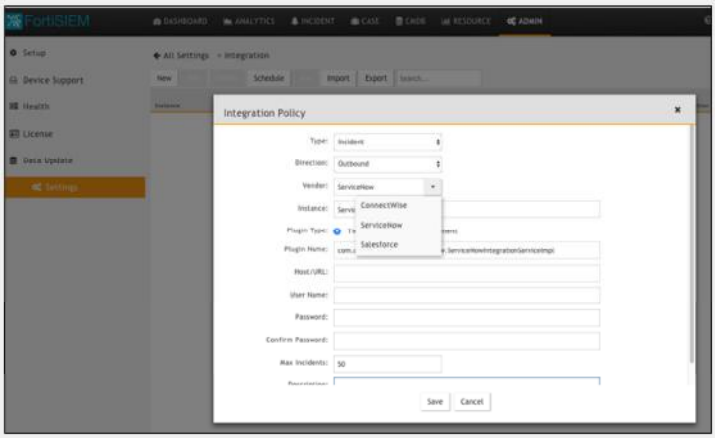
You can perform remediation manually (for example, by selecting an incident that has already occurred to remediate) or by using a notification policy to automatically perform a remediation action when an incident occurs. For automatic remediation, define a remediation script for a scenario. You can check the existing Remediation scripts in **ADMIN** > **Settings** > **General** > **Notification** > **Remediation** settings. Mitigation scripts can, for example, block an IP address in a firewall or disable a user in Active Directory.

Vouchers & Dumps are Available | WhatsApp +201224560923

DO NOT REPRINT
© FORTINET
Brave-dumps.com

Notification Policy Actions—Integration Policy

- **Integration Policy** actions reference what is defined in **ADMIN > Settings > General > External Integration**
- Can define **Outbound** and **Inbound** incident notification integrations with Service Now, Connectwise, and Salesforce



NSE Training Institute

© Fortinet Inc. All Rights Reserved.

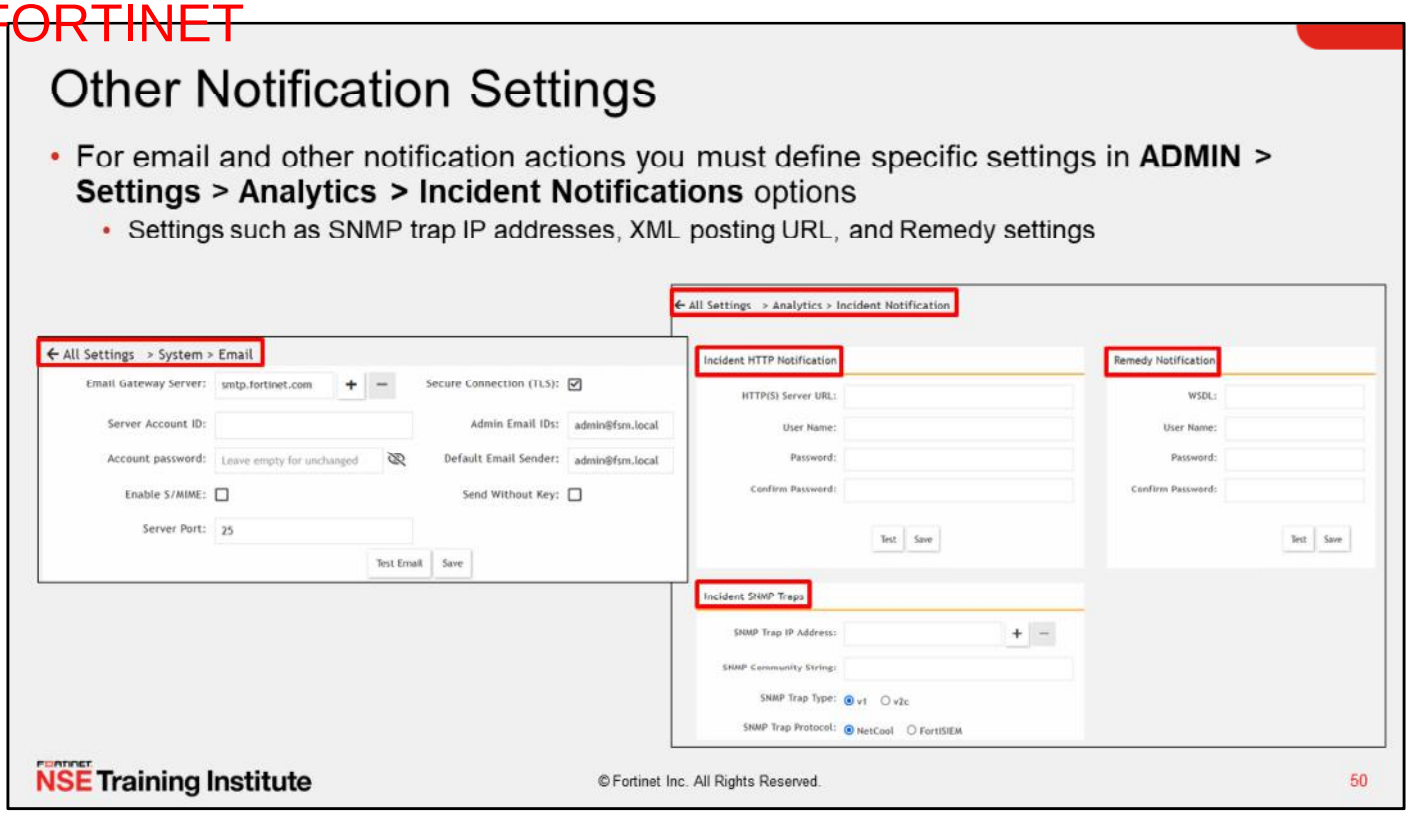
49

The **Integration Policy** tab displays the integration policies that you defined in **ADMIN** > **Settings** > **General** > **External Integration.**

You can define **Outbound** and **Inbound** incident notification integrations with Connectwise, Service Now, and SalesForce here.

Vouchers & Dumps are Available | WhatsApp +201224560923

DO NOT REPRINT
© FORTINET
Brave-dumps.com



As you learned previously, for email and other notification actions to take place, you must define specific settings in **ADMIN** > **Settings** > **Analytics > Incident Notifications**.

You must specify the email settings if you intend to have the system send email notifications. Additionally, you can define other protocols such as SNMP traps, XML posting URLs, and Remedy integration settings.

The following options are available:
- **Incident SNMP Traps**
- **Incident HTTP Notification** (XML posting URLs)
- **Remedy Notification**

Vouchers & Dumps are Available | WhatsApp +201224560923

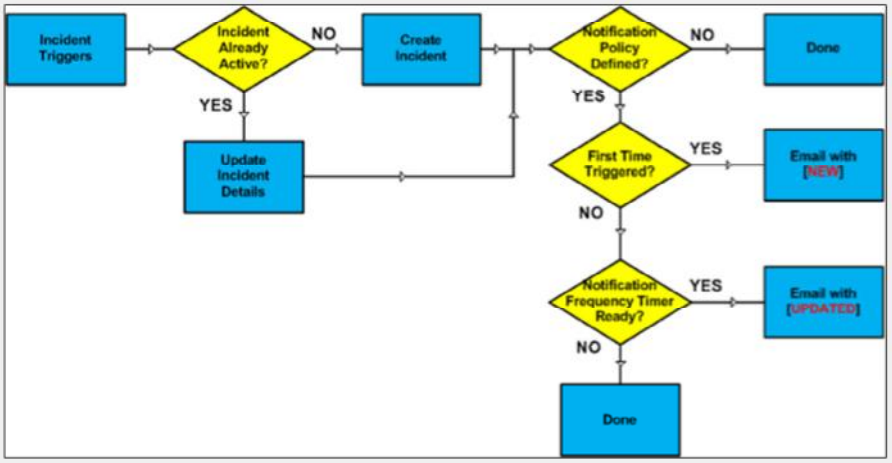
DO NOT REPRINT Brave-dumps.com
© FORTINET

Incident Notification Email Workflow with Default Template

- Logical incident notification process
- Notification frequency is an individual value set on every rule
  - Minimum notification frequency is 15 minutes

RESOURCES > Rules

Notification: 24 Hours



NSE Training Institute

© Fortinet Inc. All Rights Reserved.

51

This slide shows the incident notification email workflow when you use the default template.

The first time an incident triggers, the system looks at whether an incident is already active is for the same condition. If not, then the system creates an incident. If an incident is already open for the same condition, the system updates the incident details, including the incident count, and the last seen time.

Next, the system determines whether if there is a notification policy is defined for this incident and the conditions that are being tracked. If policy is defined, then the system completes this process. If a policy is defined, the system determines whether this is the first time that this incident has occurred. If it is the first time, the system will send a notification email using the default template with NEW in the subject header.

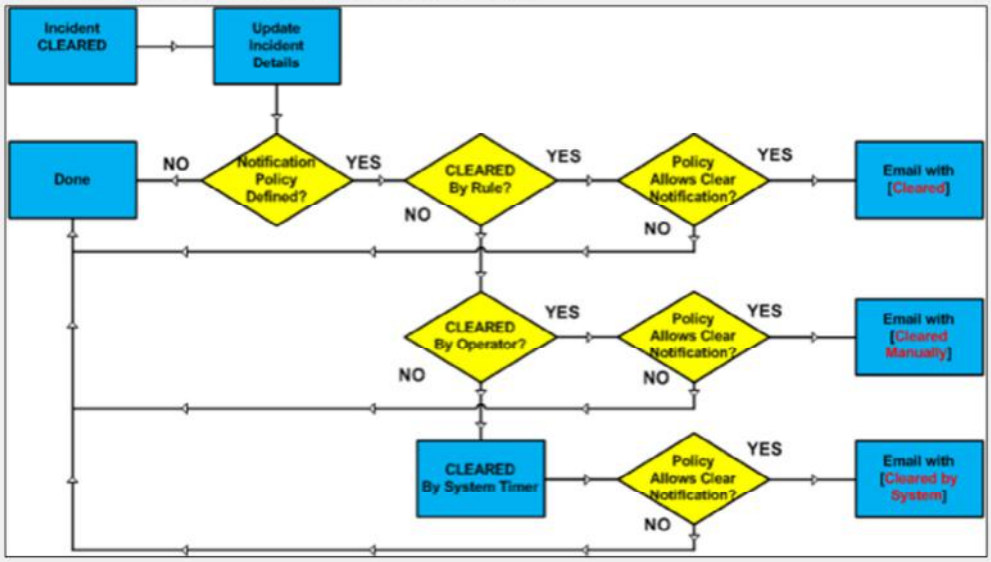
You can set a notification frequency value for each rule. The minimum is 15 minutes, but you can override it with whatever value you like. The idea is that, rather than sending an email every time an incident occurs, further notifications are sent based on this frequency timer. If the incident triggered several times within that notification frequency period, only the first email is sent. But, once the notification frequency period elapses, the next time the incident occurs, another email notification is sent. This time, the subject header includes the word UPDATED.

Vouchers & Dumps are Available | WhatsApp +201224560923

DO NOT REPRINT
© FORTINET
Brave-dumps.com

Cleared Incident Notifications

- Logical notification process for cleared incidents



NSE Training Institute

© Fortinet Inc. All Rights Reserved.

52

If you recall from the incident section, you can also clear incidents. Incidents can be cleared automatically, by a clear condition on the rule; manually, by an operator, or by the system clear function.

If the incident was cleared automatically, and the policy allows clear notifications, then the system sends an email with the word CLEARED in the subject header.

If the incident was cleared manually, and the policy allows clear notifications, then the system sends an email with the words CLEARED MANUALLY in the subject header.

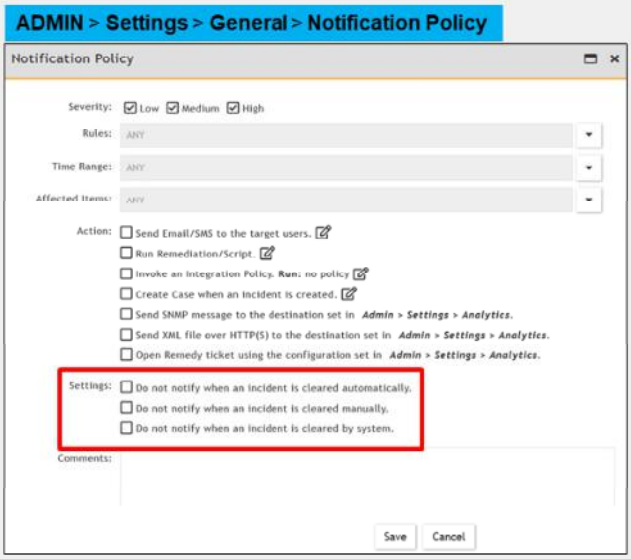
If the incident was cleared by the system timer, and the policy allows clear notifications, then the system sends an email with the words CLEARED BY SYSTEM in the subject header.

Vouchers & Dumps are Available | WhatsApp +201224560923

DO NOT REPRINT
© FORTINET
Brave-dumps.com

Disable Notifications of Cleared Incidents

- If you do not want to send emails when incidents are cleared, you can set this per notification policy
- **Note**: The default action is to notify



NSE Training Institute

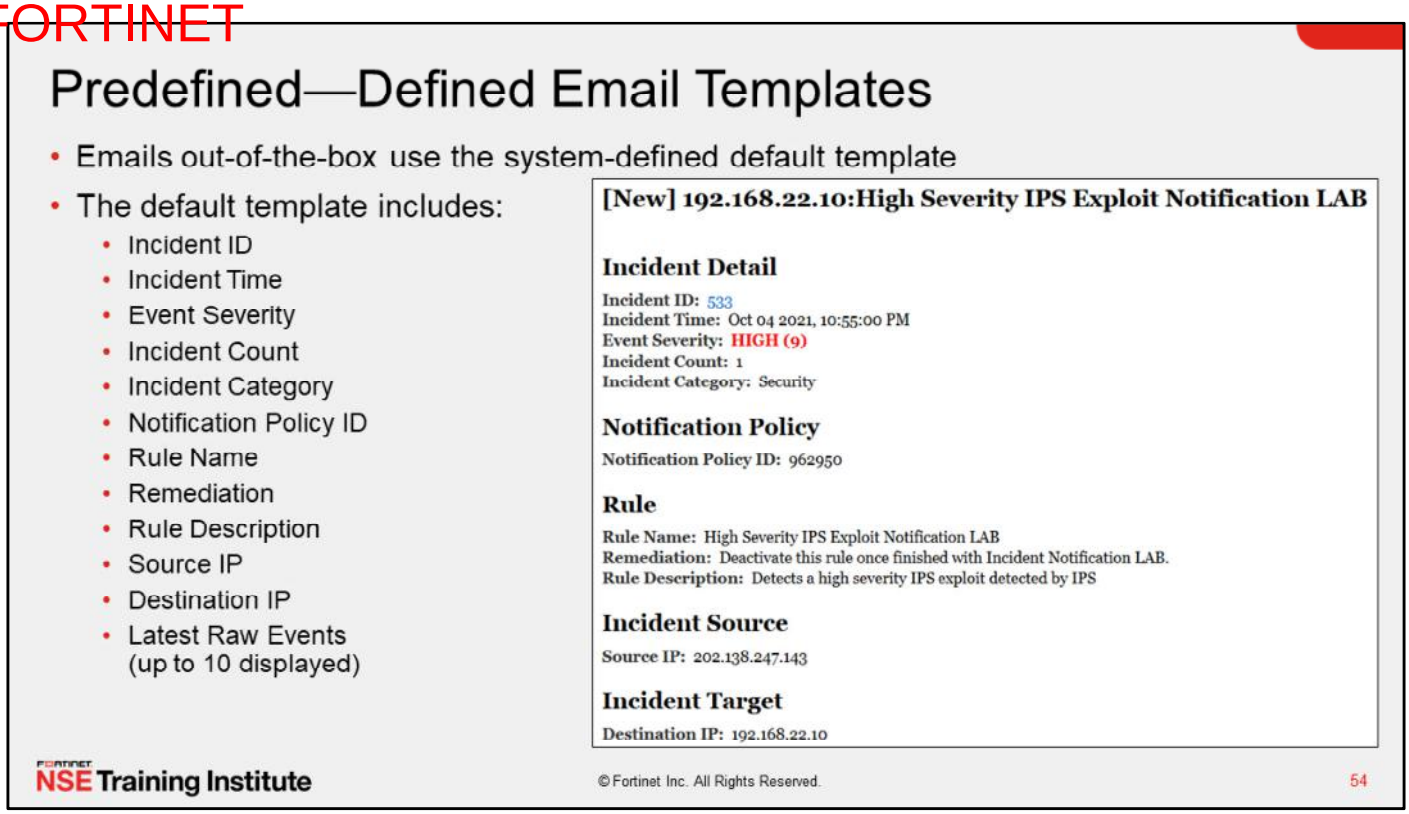
© Fortinet Inc. All Rights Reserved.

53

In the policy definitions, you can specify whether or not you want to be notified when an incident is cleared. When an incident clears, the system updates the incident's details by changing its status from active to one of the cleared conditions. The system is set to send a notification of the change in status, but you can opt in or out of this notification in the incident notification policy. Not only do you have the option to be notified when an incident is cleared, but you can also be informed of how the incident was cleared.

Vouchers & Dumps are Available | WhatsApp +201224560923

DO NOT REPRINT
© FORTINET
Brave-dumps.com

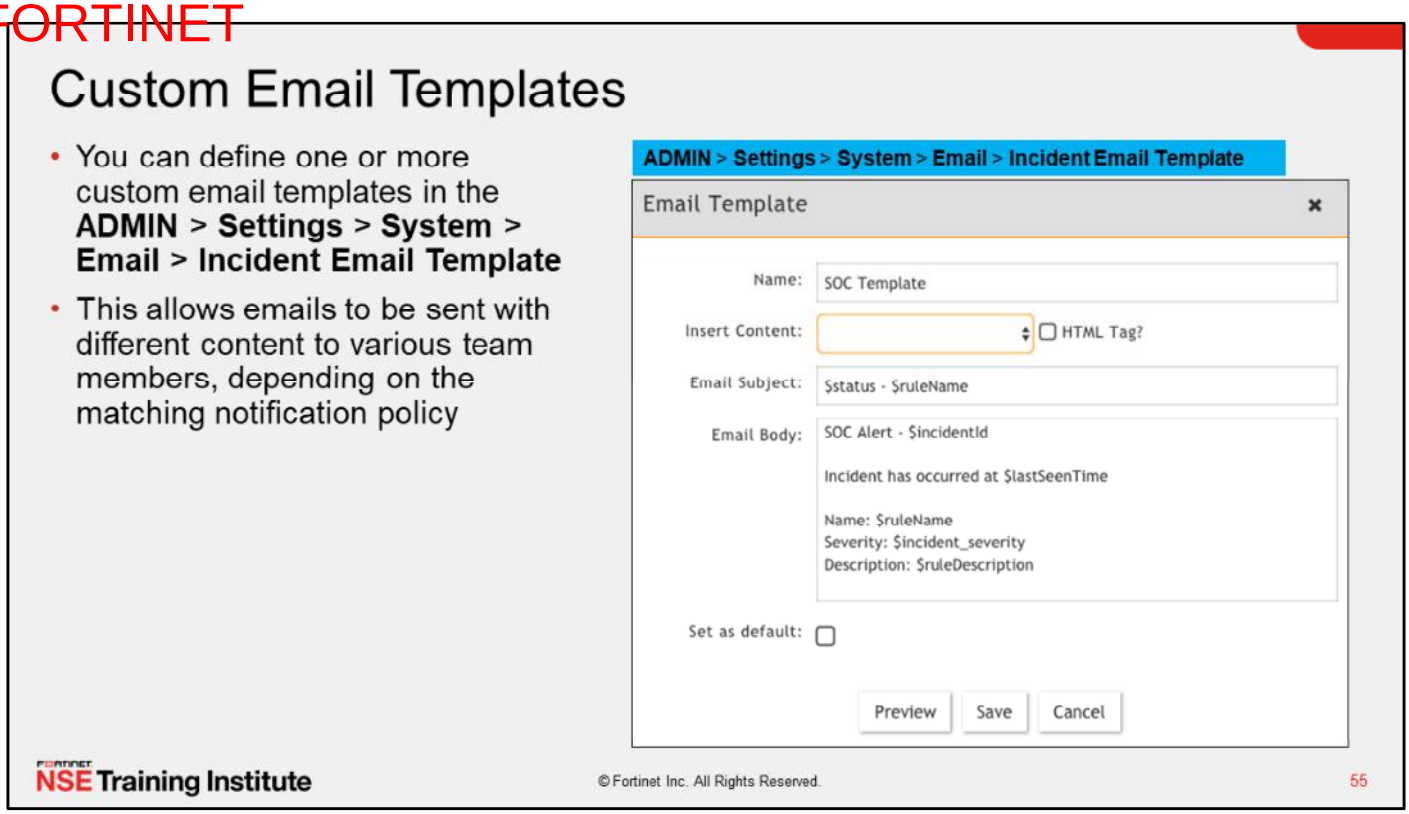


If you don’t specify a template within a notification policy, emails use the predefined default template.

The body text of the default template includes the incident ID, the time that the incident occurred, the severity of the incident, incident count, and the rule name and description. It can even include up to the last 10 raw events.

Vouchers & Dumps are Available | WhatsApp +201224560923

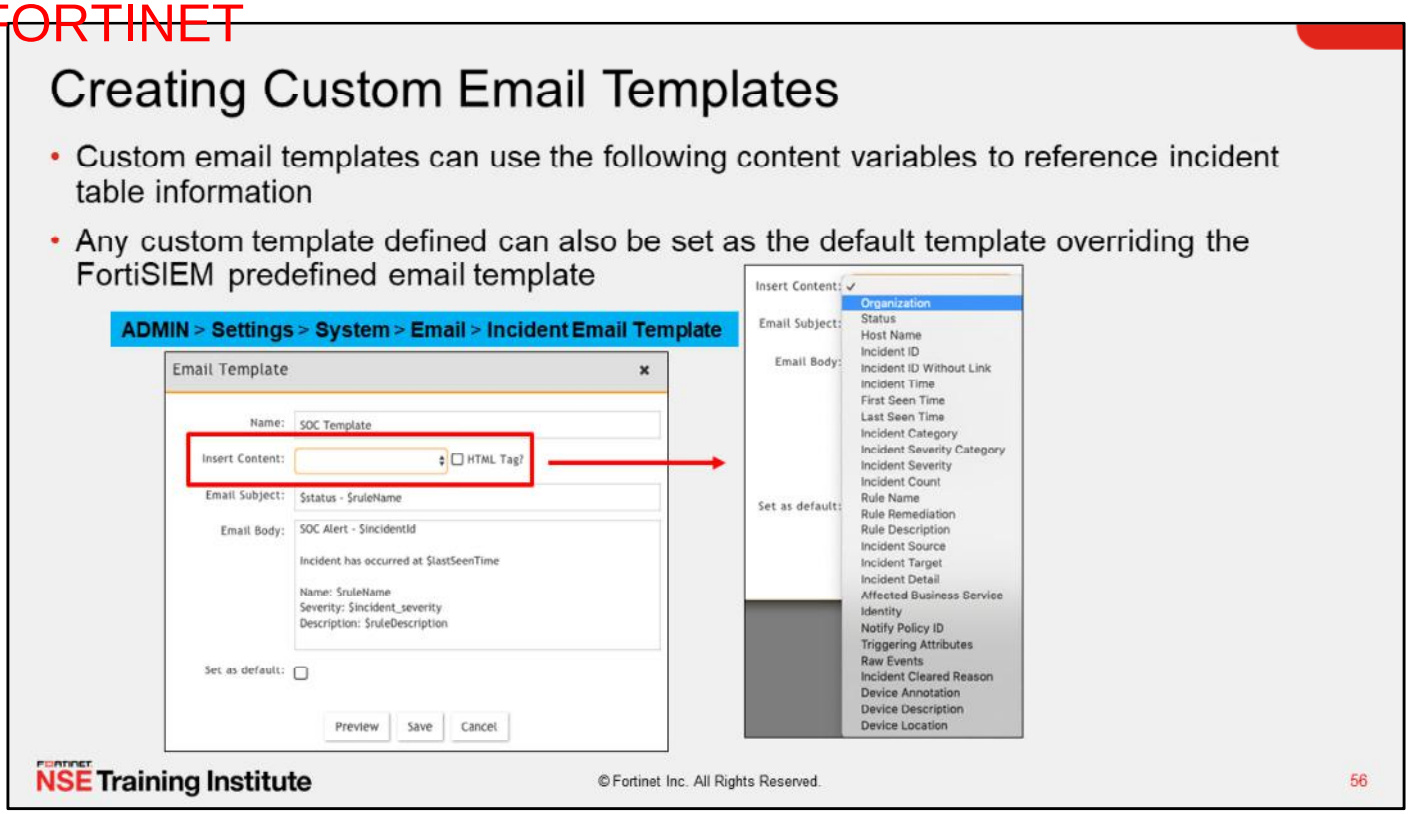
DO NOT REPRINT
© FORTINET
Brave-dumps.com



You can create one or more custom email templates on the **Email Templates** tab by clicking **ADMIN** > **Settings** > **System** > **Email** > **Incident Email Template**. Using custom email templates allows you to send emails with different text and content to various team members, depending on the matching notification policy.

Vouchers & Dumps are Available | WhatsApp +201224560923

DO NOT REPRINT
© FORTINET
Brave-dumps.com



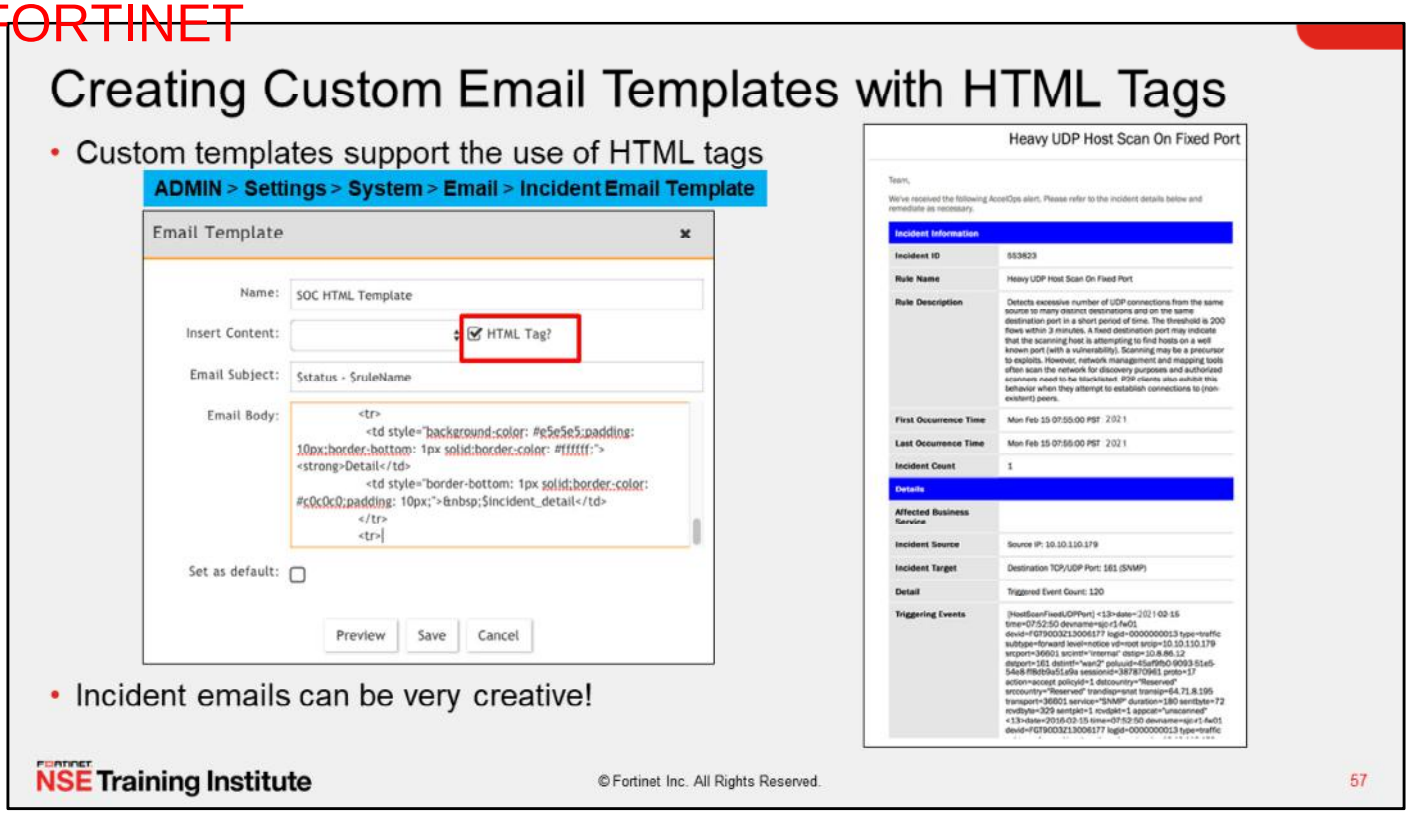
You can create custom email templates, which can use content variables to reference incident table information. The system substitutes the variables with the event details when it generates the email.

You can use these variables in both the subject and body fields of the email template. For example, you can write your own text and then enter the content for the rule name, rule description, rule remediation, status, and so on.

You can create as many custom email templates as you like, and you can set any one of them as the default template, overriding the FortiSIEM predefined email template.

Vouchers & Dumps are Available | WhatsApp +201224560923

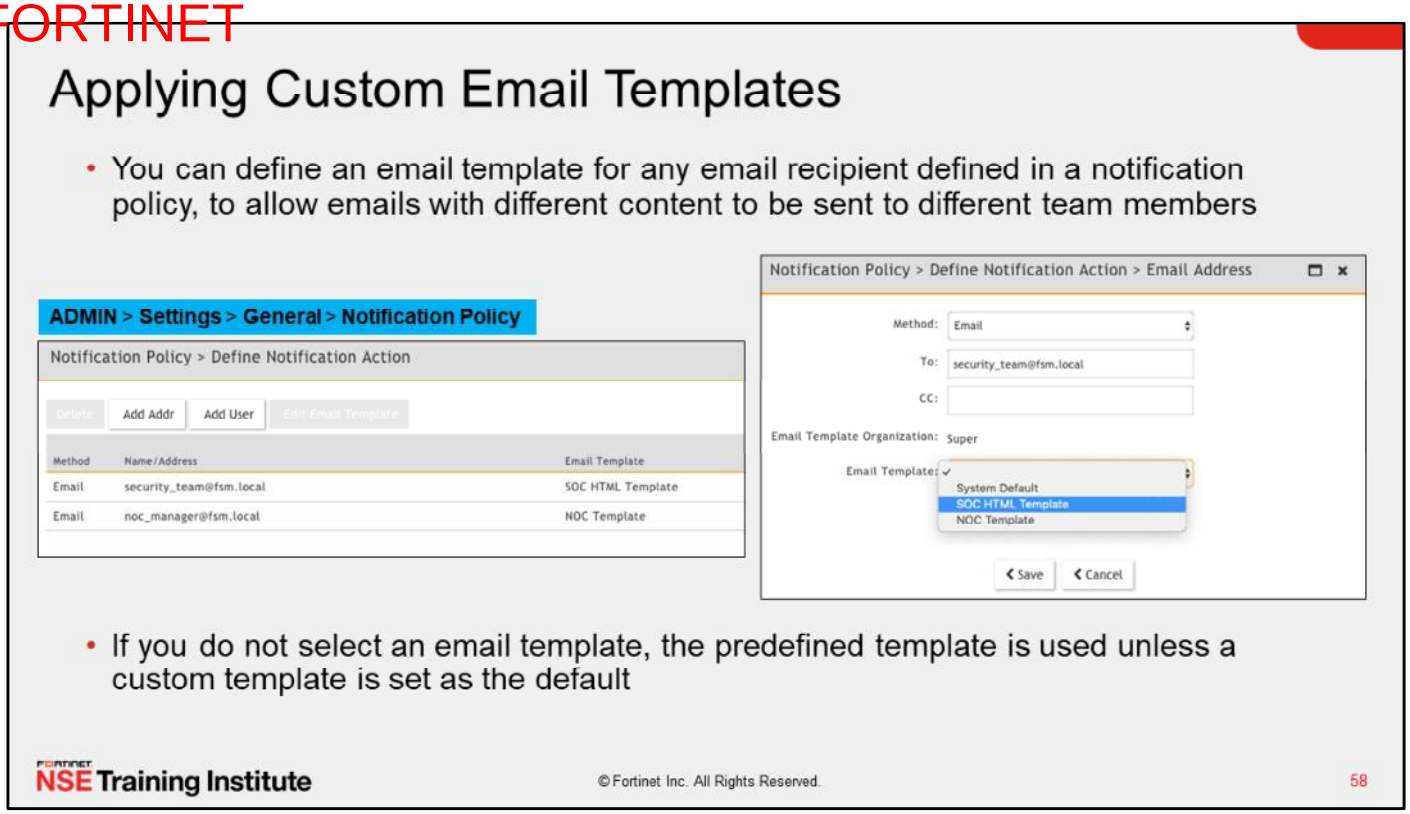
DO NOT REPRINT
© FORTINET
Brave-dumps.com



Custom templates support the use of HTML tags. If you look at the example shown on the right side of the slide, you will see that incident emails can be very creative and much better looking than standard text emails.

Vouchers & Dumps are Available | WhatsApp +201224560923

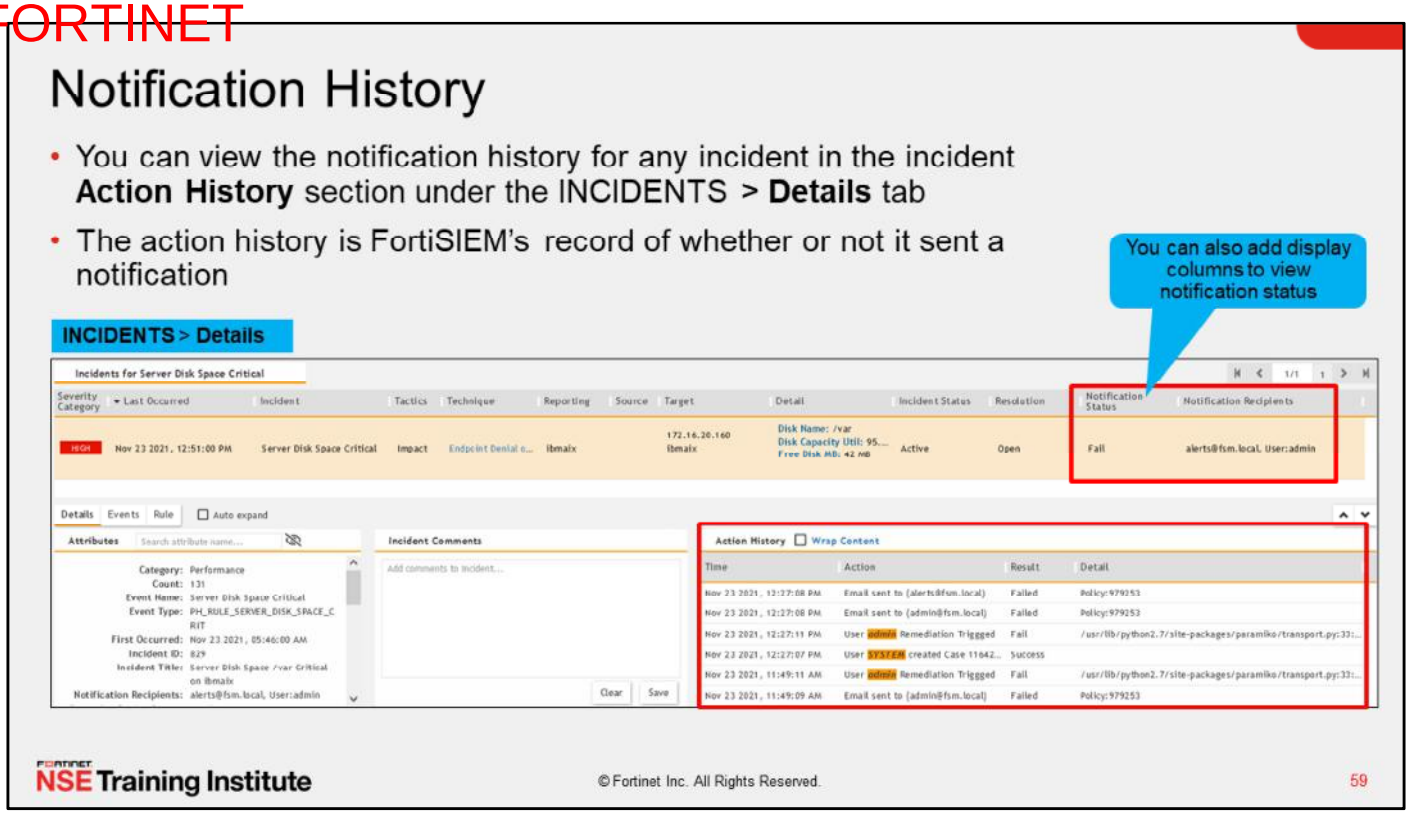
DO NOT REPRINT
© FORTINET
Brave-dumps.com



As mentioned earlier, when email is selected as the notification method in the **Notification Actions** window for a user, a drop-down list appears in the email template column. In the drop-down list, select the template you want to use for this user. Note that different users or groups can receive email based on different templates. If no email template is selected, the predefined default template is used unless a custom template is set as the default.

Vouchers & Dumps are Available | WhatsApp +201224560923

DO NOT REPRINT
© FORTINET
Brave-dumps.com



On the **INCIDENTS** tab **List** view, you can view the notification history for any incident. Select an incident, and click the **Details** tab then, in the **Action History** section you can view the incident action and notification history.

The **Action History** section displays FORTISIEM's record of whether or not it successfully sent a notification. It provides some detailed information, such as the date and time the notification was sent, the incident ID, policy number, and the users emailed as part of this notification.

You can also add display columns to view notification status.

Vouchers & Dumps are Available | WhatsApp +201224560923

DO NOT REPRINT
© FORTINET
Brave-dumps.com

Knowledge Check

1. What is the minimum notification frequency value?
   A. Five minutes
   ✓ B. Fifteen minutes

NSE Training Institute
© Fortinet Inc. All Rights Reserved.

Vouchers & Dumps are Available | WhatsApp +201224560923

DO NOT REPRINT
© FORTINET
Brave-dumps.com

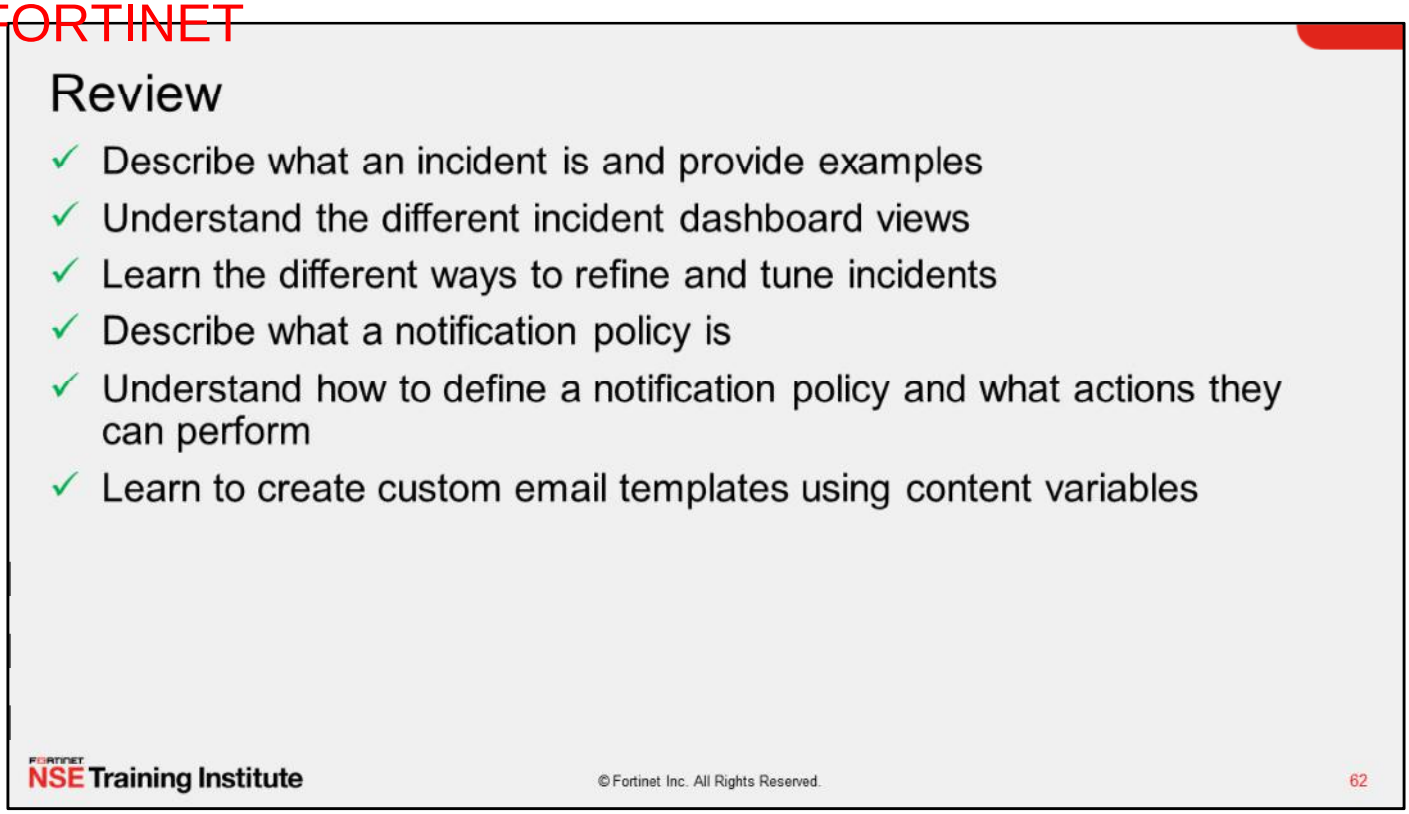


Congratulations! You have completed this lesson.

Now, you will review the objectives that you covered in this lesson.

Vouchers & Dumps are Available | WhatsApp +201224560923

DO NOT REPRINT
© FORTINET
Brave-dumps.com

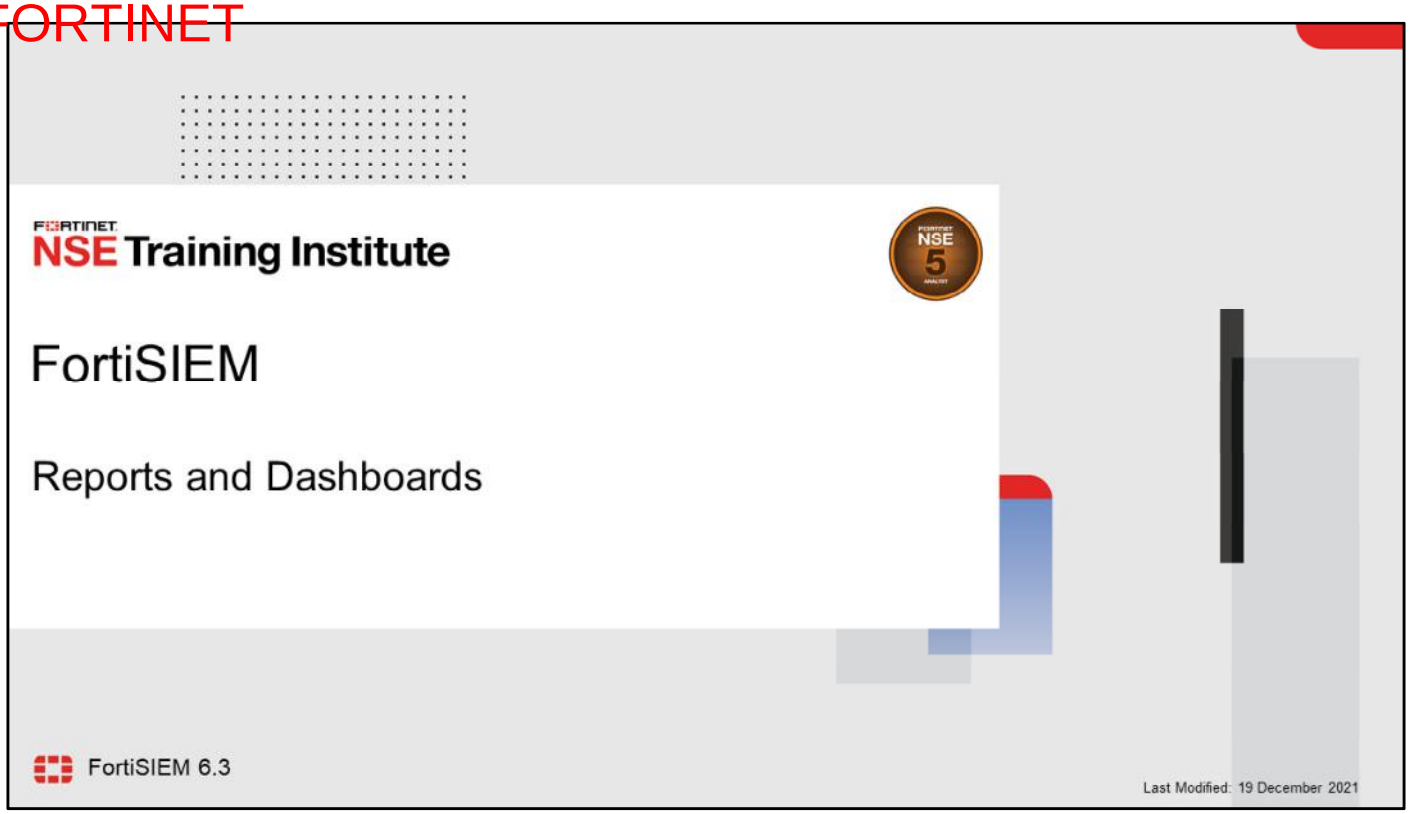


This slide shows the objectives that you covered in this lesson.

By mastering the objectives covered in this lesson, you learned what incidents are and how to define a notification policy.

Vouchers & Dumps are Available | WhatsApp +201224560923

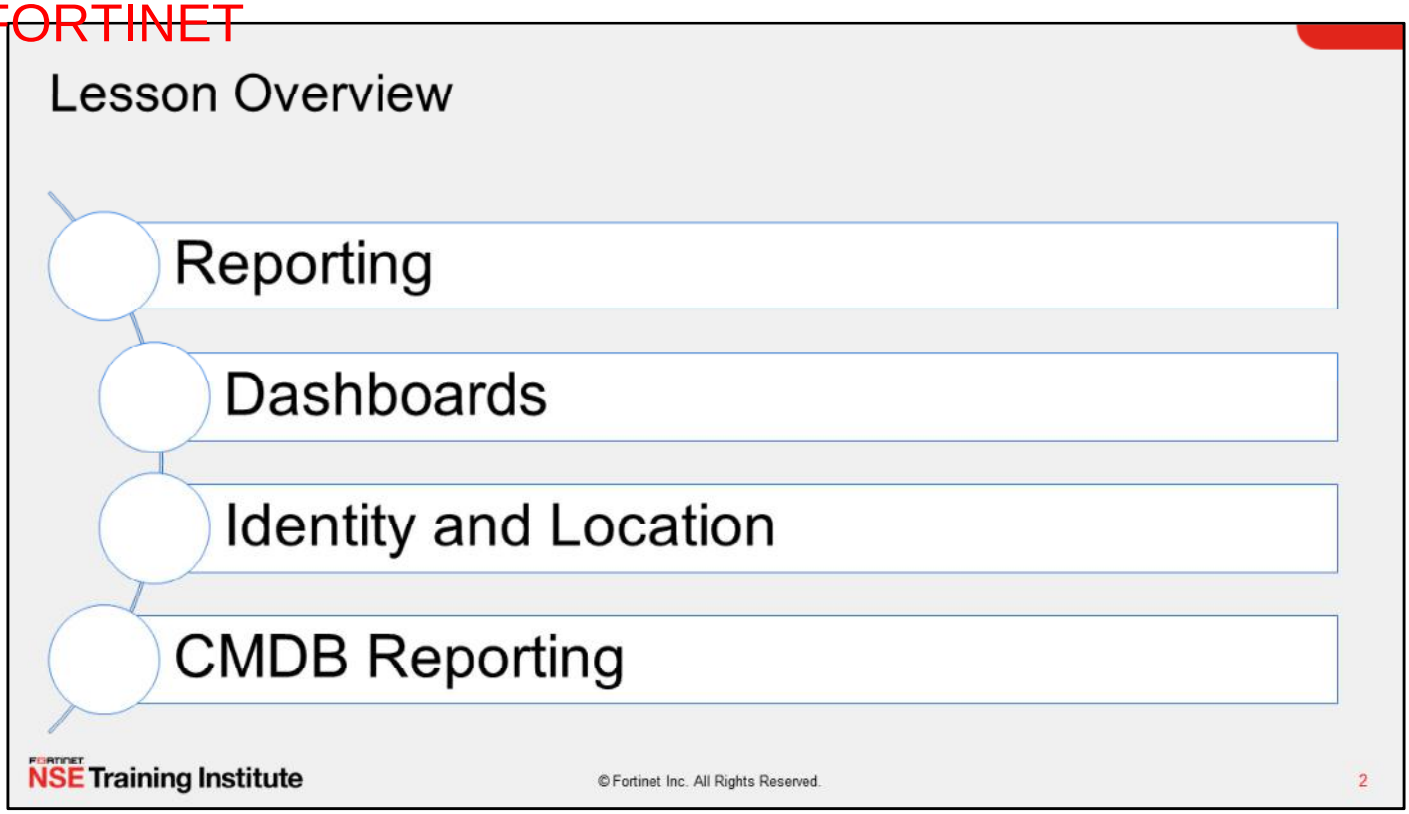
DO NOT REPRINT
© FORTINET
Brave-dumps.com



In this lesson, you will learn about some of the reporting and dashboard functions available on FortiSIEM.

Vouchers & Dumps are Available | WhatsApp +201224560923

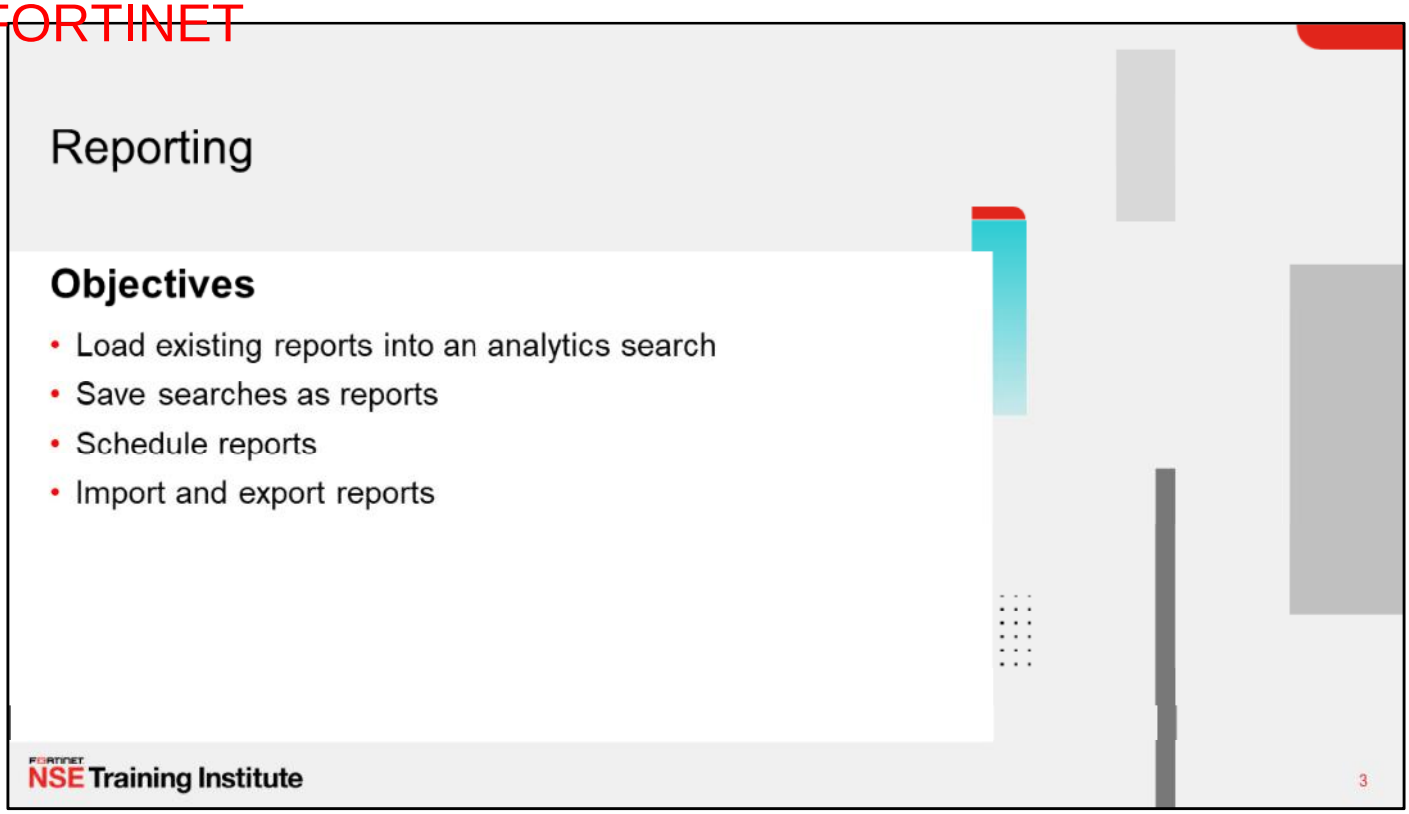
DO NOT REPRINT
© FORTINET
Brave-dumps.com



In this lesson, you will explore the topics shown on this slide.

Vouchers & Dumps are Available | WhatsApp +201224560923

DO NOT REPRINT
© FORTINET
Brave-dumps.com

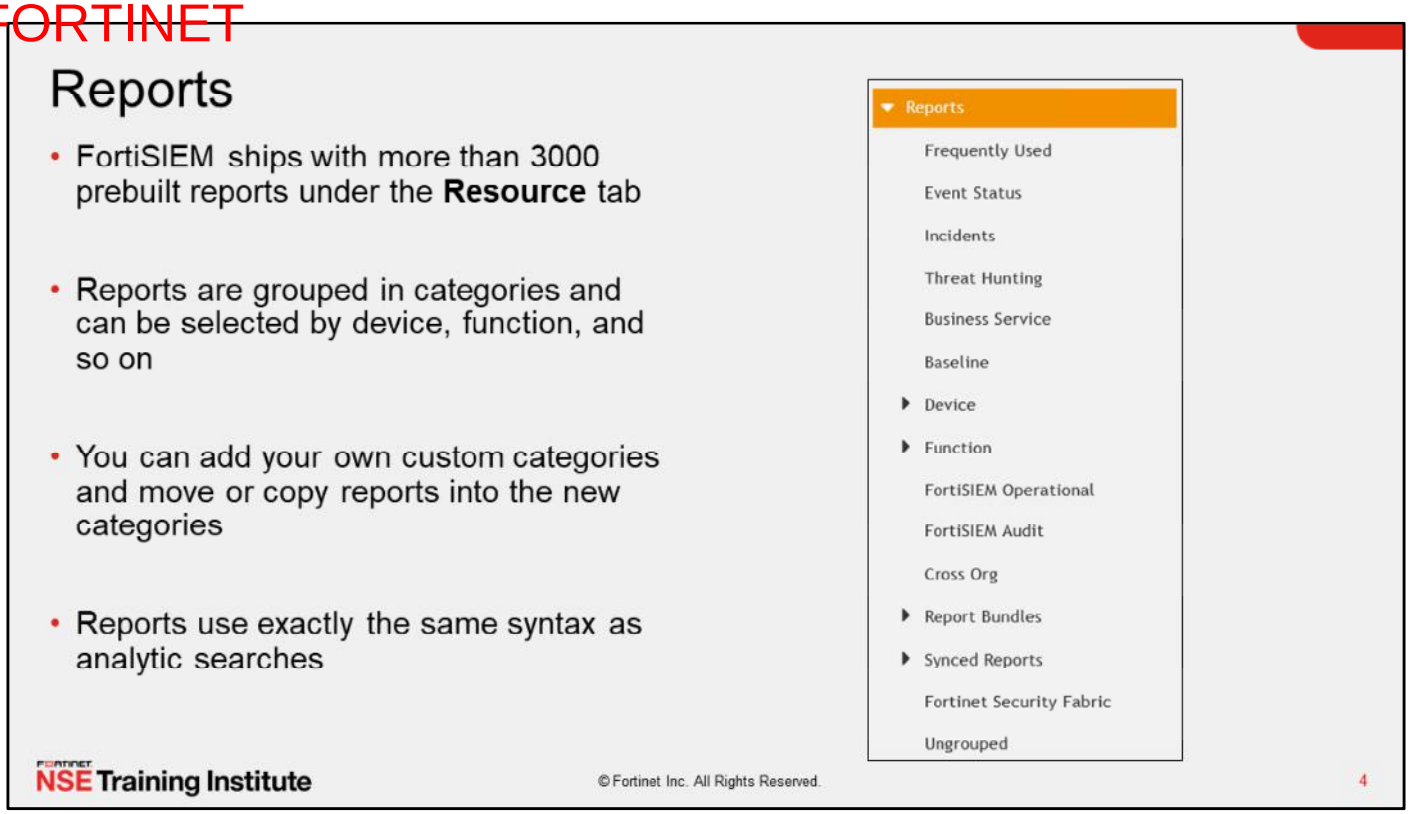


After completing this section, you should be able to achieve the objectives shown on this slide.

By demonstrating competence in reporting, you will be able to load, save, schedule, and import reports in FortiSIEM.

Vouchers & Dumps are Available | WhatsApp +201224560923

DO NOT REPRINT
© FORTINET
Brave-dumps.com



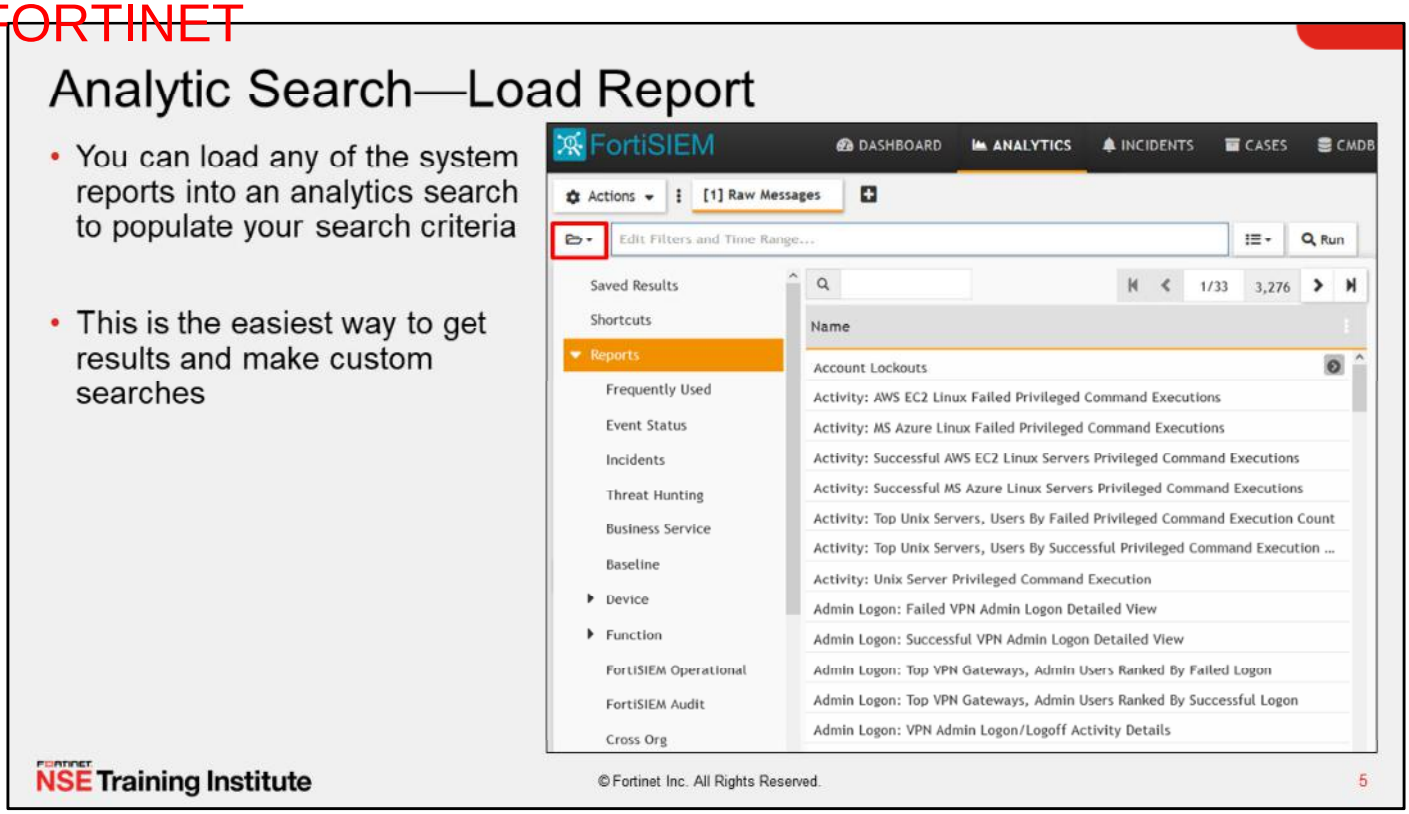
FortiSIEM ships with more than 3000 prebuilt reports. You can find reports by clicking **RESOURCES** > **Reports**.

The reports are grouped in several different categories and subcategories, making is easier for you to find the report you are looking for. You can add custom categories, and move or copy reports into the new groups.

Reports use the same syntax as analytic searches, making it easier for you to build your own custom reports and save them in the reports tree.

Vouchers & Dumps are Available | WhatsApp +201224560923

DO NOT REPRINT
© FORTINET
Brave-dumps.com



You can load any of the system reports into an analytics search to populate your search criteria. If you click the folder icon, you can then select a report group and, in the right pane, select a report, and then click the white arrow to run the report. This action populates the search criteria.

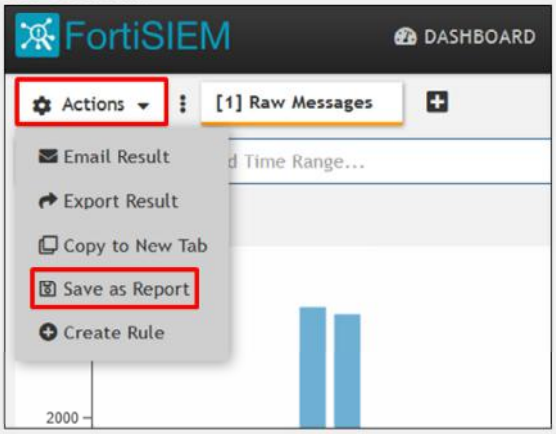
This is the easiest way to get quick results and make your own custom searches.

Vouchers & Dumps are Available | WhatsApp +201224560923

DO NOT REPRINT
© FORTINET
Brave-dumps.com

Saving a Search as a Report

- Multiple options are available after running an historical search:
- Produce an instant report by exporting the results as a PDF, CSV, or RTF file
- Email the results as a PDF, CSV, or RTF file
- Save the search criteria and display columns as a report definition



- You can load saved reports back into the GUI at any time and run them as scheduled reports

NSE Training Institute
© Fortinet Inc. All Rights Reserved.
6

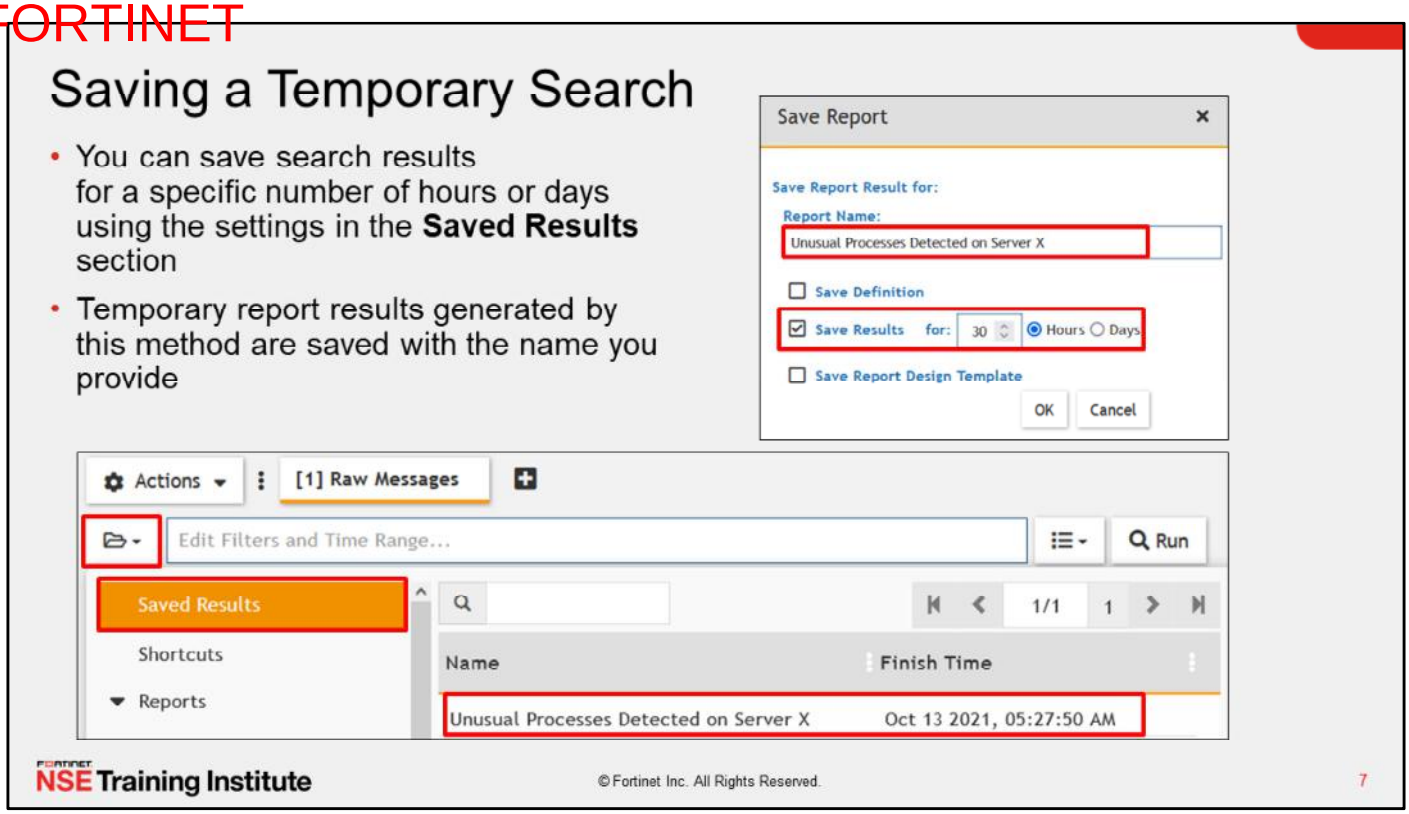
You can save historical search results as a report.

After running an historical search, you can handle the results in a number of ways. You can do any of the following:
- Produce an instant report by exporting the results as a PDF, CSV, or RTF file.
- Email the results as a PDF, CSV, or RTF file.
- Save the search criteria and the display columns together as an XML file, in a report definition.

Note that you can load saved reports back into the GUI at any time, and run them as scheduled reports.

Vouchers & Dumps are Available | WhatsApp +201224560923

DO NOT REPRINT
© FORTINET
Brave-dumps.com

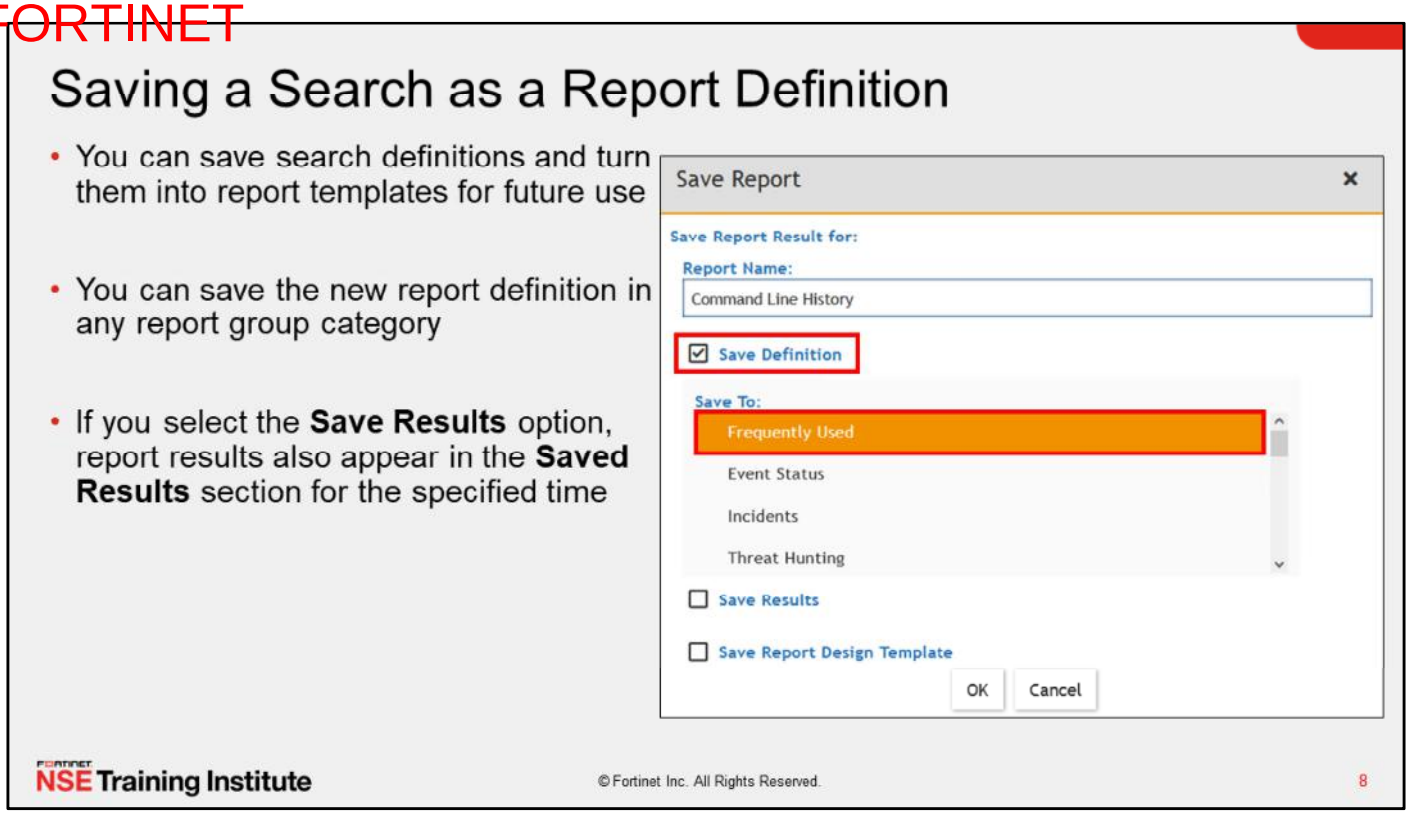


You can save the search results in the **Saved Results** section for a specified number of hours or days. If you leave the **Save Definition** option clear in the **Save Report** window, you can specify that the report be saved for a specific number of hours or days. After this time period, the reports are automatically deleted.

Temporary search results generated by this method are saved with the name you provide.

Vouchers & Dumps are Available | WhatsApp +201224560923

DO NOT REPRINT
© FORTINET
Brave-dumps.com



Alternatively, you can save searches and turn them into report definitions for future use by selecting the **Save Definition** option and providing a name for the report.

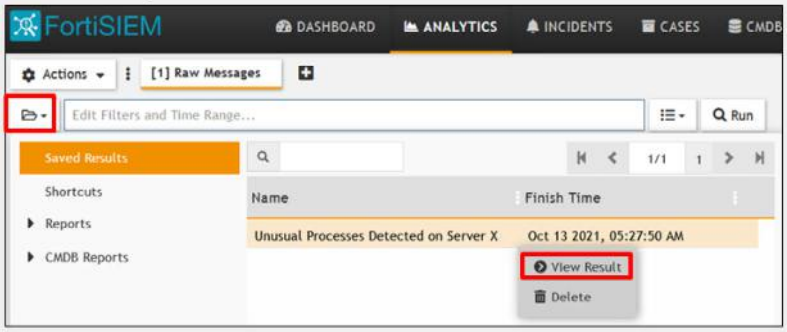
You can save the new report definition in any report category group. In the example shown on this slide, the report definition is saved in the report category group **Frequently Used**, but you can move it to another category, if you prefer. If you select the **Save Results** option, report results also appear in the **Saved Results** section for the specified time period.

Vouchers & Dumps are Available | WhatsApp +201224560923

DO NOT REPRINT
© FORTINET
Brave-dumps.com

Viewing Cached Results From Saved Results

- You can retrieve saved report results from the **Saved Results** section



- Select a search result, click the white down arrow, and hen click **View Results** to bring the search back onto the **ANALYTICS** tab
- You can also delete report results on this page
- **Note**: In this section, there is no way you can determine how much time is left before saved search results are removed

NSE Training Institute

© Fortinet Inc. All Rights Reserved.

9

To retrieve report results from the **Saved Results** section:

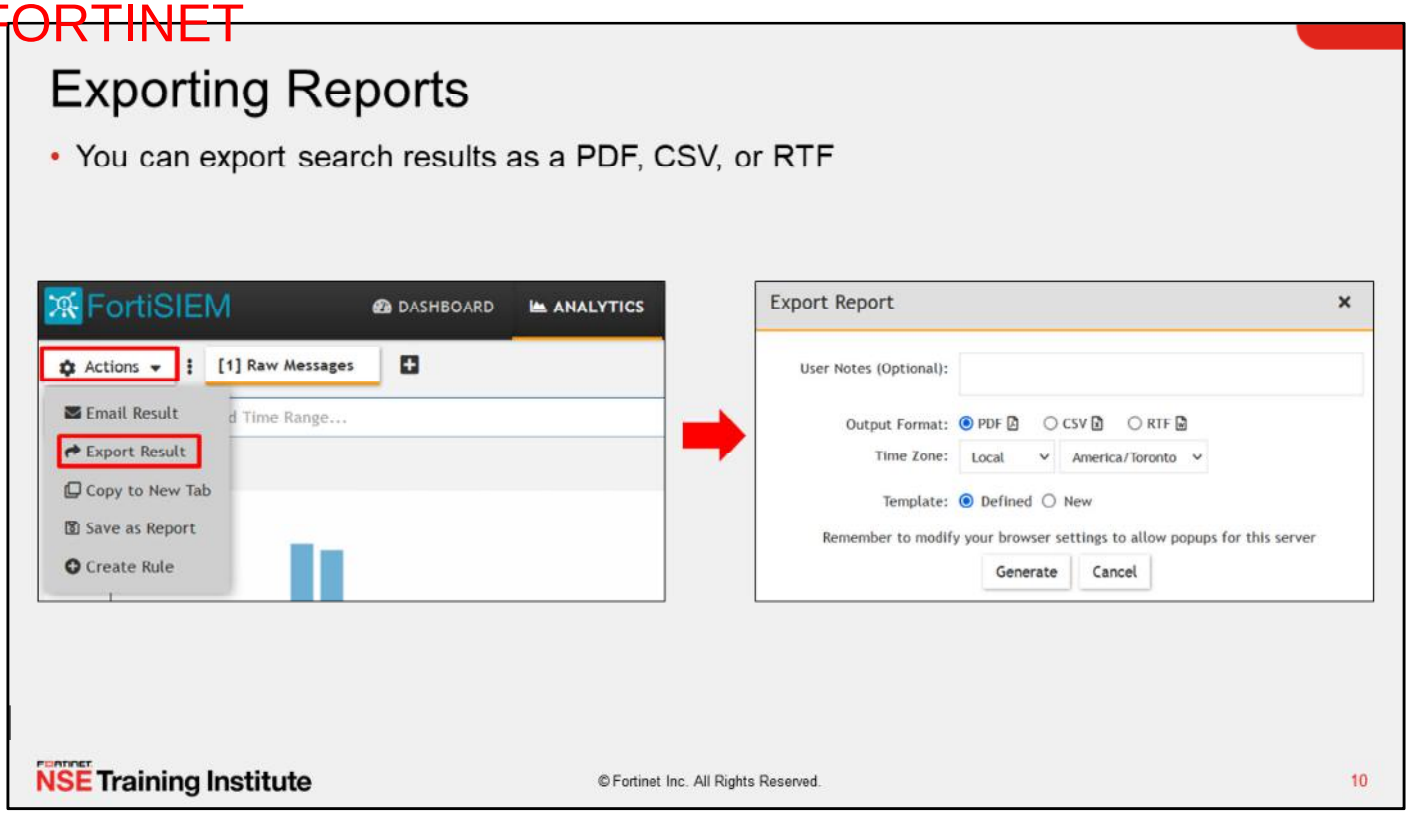
1. Select the search result that you want to retrieve.
2. Click the white down arrow, and then click **View Results** to bring the search back onto the **ANALYTICS** tab

You can also delete reports on this page.

Note: When you save the report, you can enter a specific number of hours or days to keep that report result, but, in this section, there is no way you can determine how much time is left before the report is automatically removed.

Vouchers & Dumps are Available | WhatsApp +201224560923

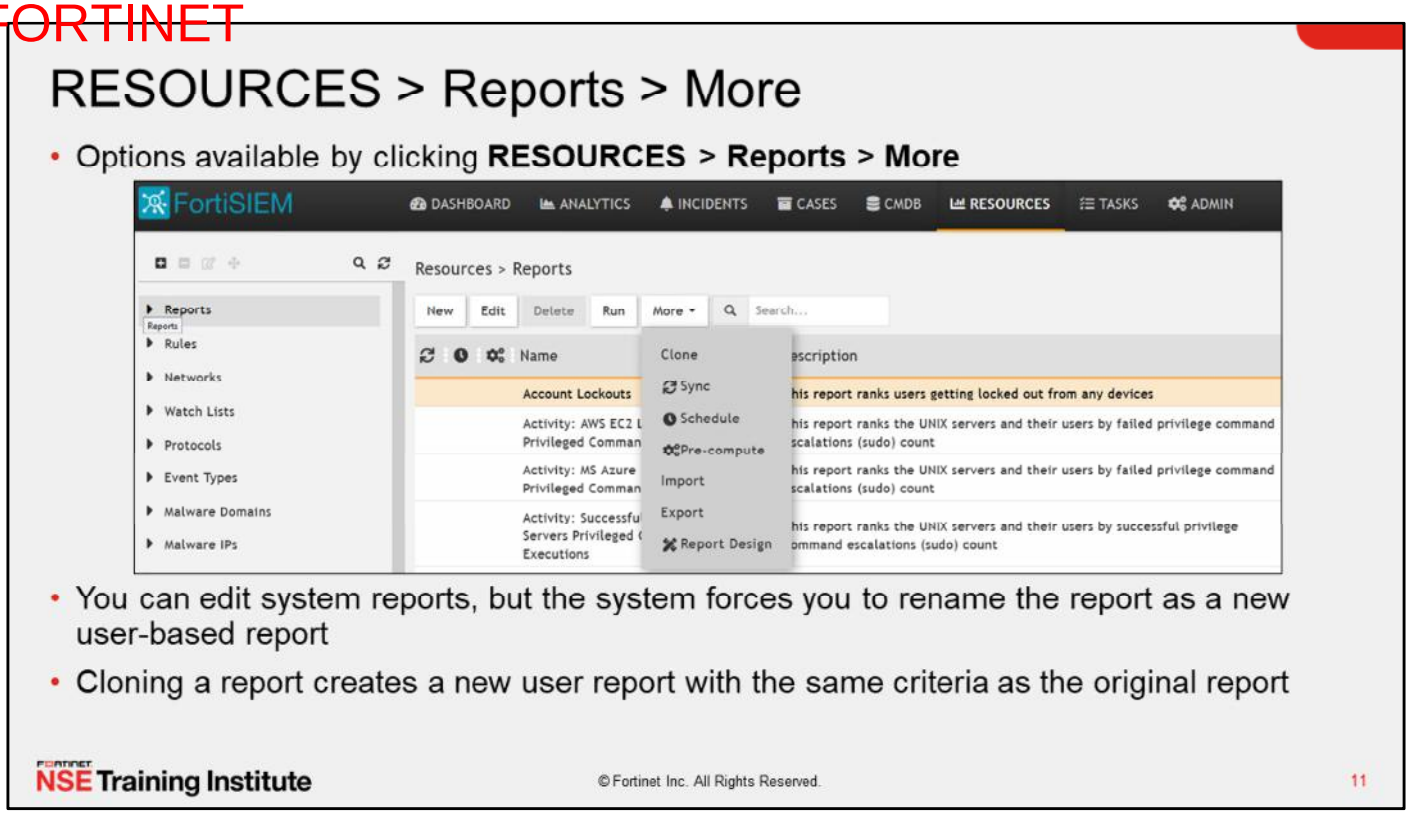
DO NOT REPRINT Brave-dumps.com
© FORTINET



You can export current search results as a PDF, CSV, or RTF.

Vouchers & Dumps are Available | WhatsApp +201224560923

DO NOT REPRINT
© FORTINET
Brave-dumps.com



There are a number of options available to you under **RESOURCES** > **Reports** > **More**.

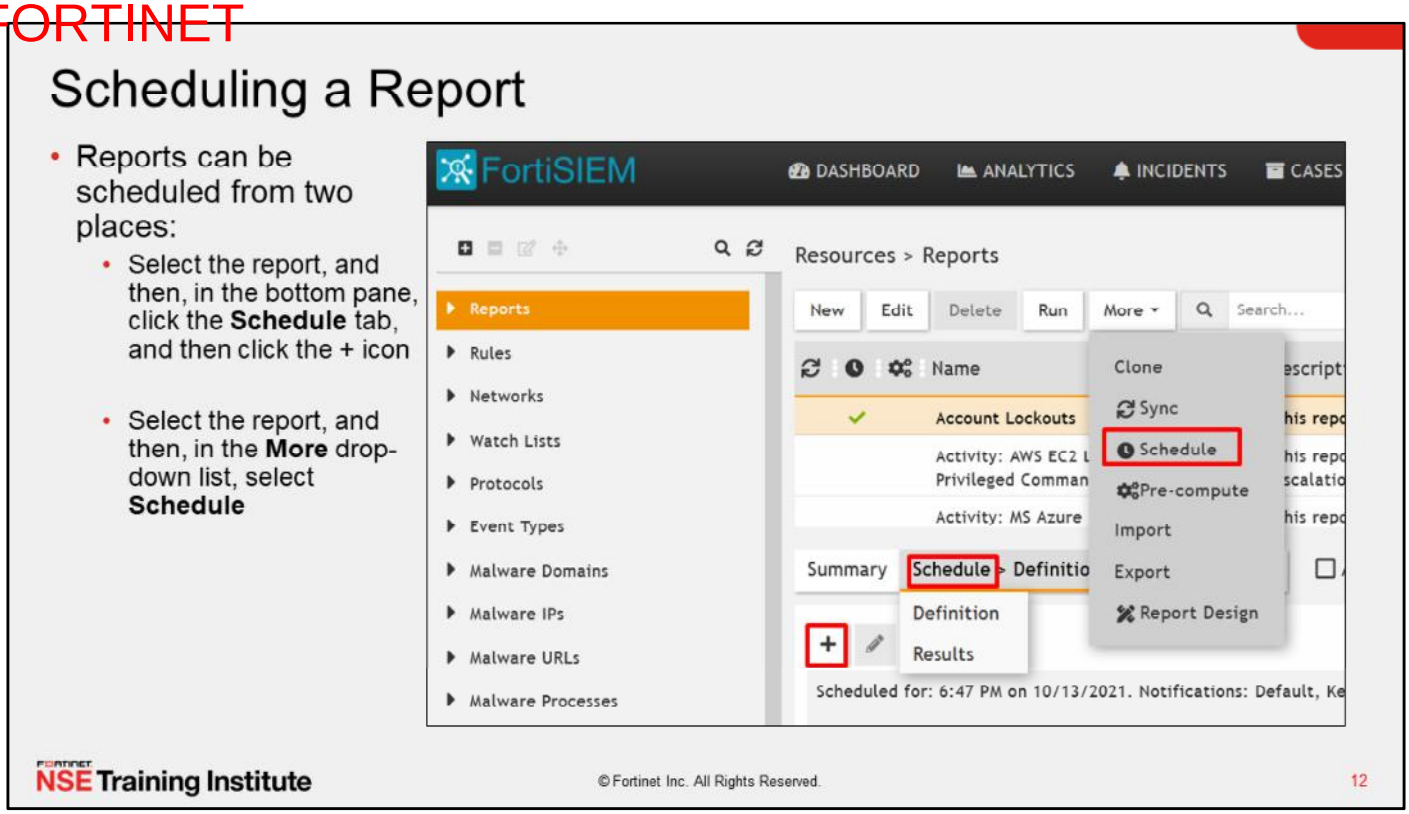
You can edit a report, clone a report template, and search for a report. There are importing and exporting options that you can use to share report templates with other FortiSIEM systems. You can run a report immediately by clicking **RUN**, or schedule a report to run later.

When the delete option associated with a selected report is grayed out, it means the selected report is a system report in FortiSIEM and cannot be deleted. You can edit system reports, but the system forces you to rename the report as a new user-based report.

To give a custom look to your PDF report, you can use the **Report Design** option to create a custom PDF report template.

Vouchers & Dumps are Available | WhatsApp +201224560923

DO NOT REPRINT
© FORTINET
Brave-dumps.com



There are two places in the GUI where you can schedule a report.

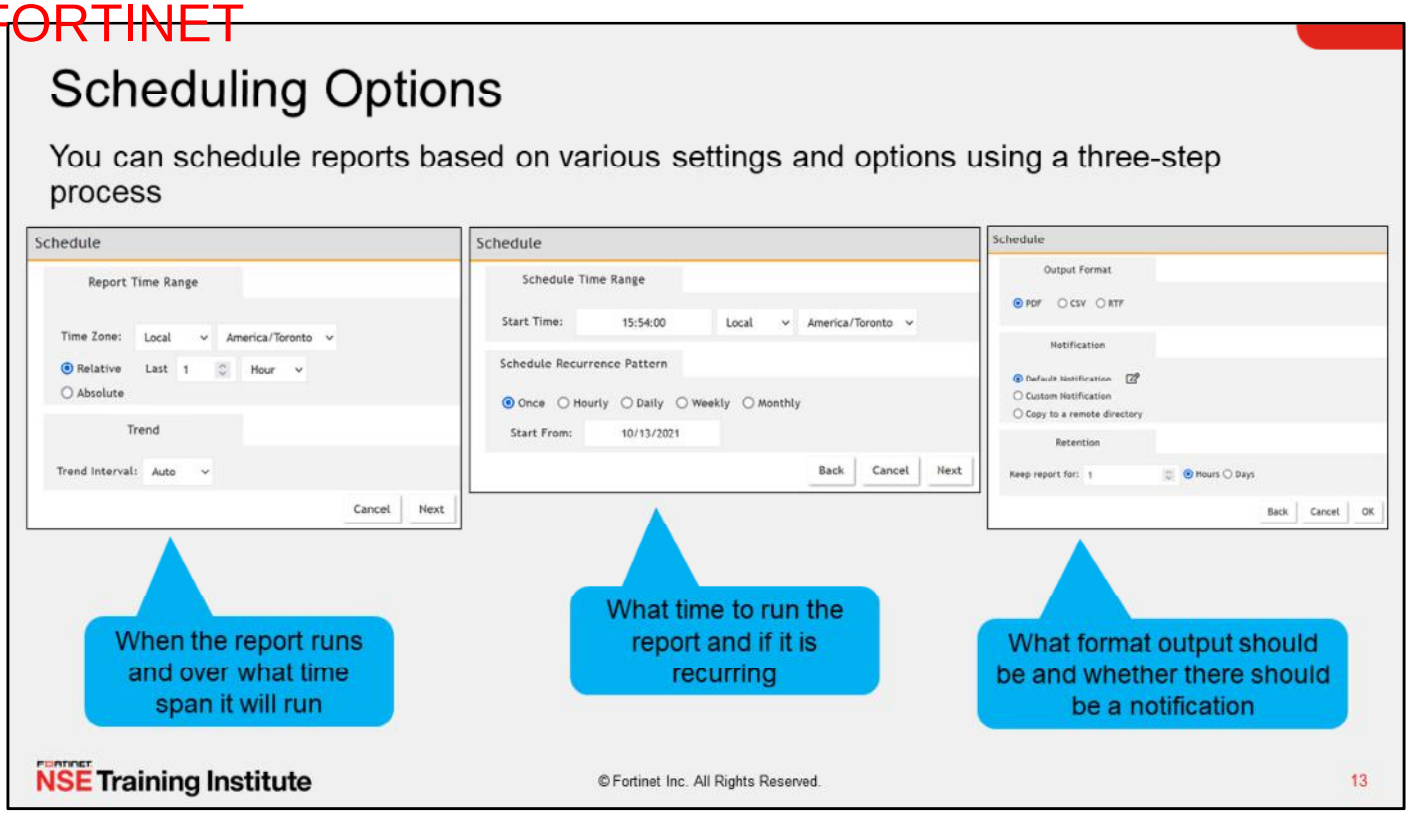
The first is to select a report, and then, in the bottom pane, click the **Schedule** tab, then click the white plus (**+**) icon to specify when you want it to run.

The second is to select a report, and then, in the **More** drop-down list, select **Schedule**.

The functionality is the same for both of these methods.

Vouchers & Dumps are Available | WhatsApp +201224560923

DO NOT REPRINT Brave-dumps.com
© FORTINET

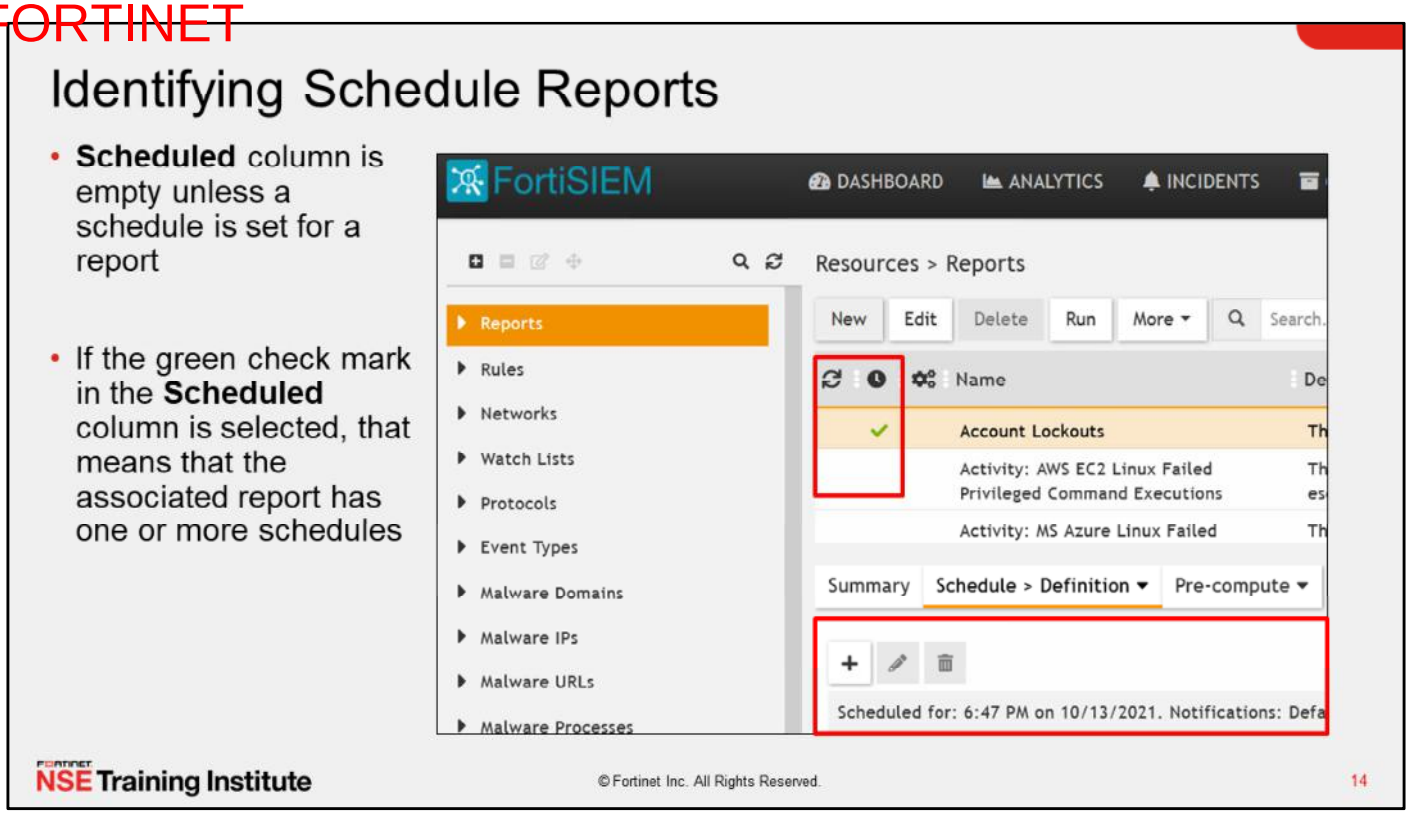


When you schedule a report, you have several options, including:

- The time range the report captures
- When the report is run and how often: once, hourly, daily, weekly, or monthly
- What output format the file is saved as: PDF or CSV
- Whether or not notifications are sent
- How long the results are retained

Vouchers & Dumps are Available | WhatsApp +201224560923

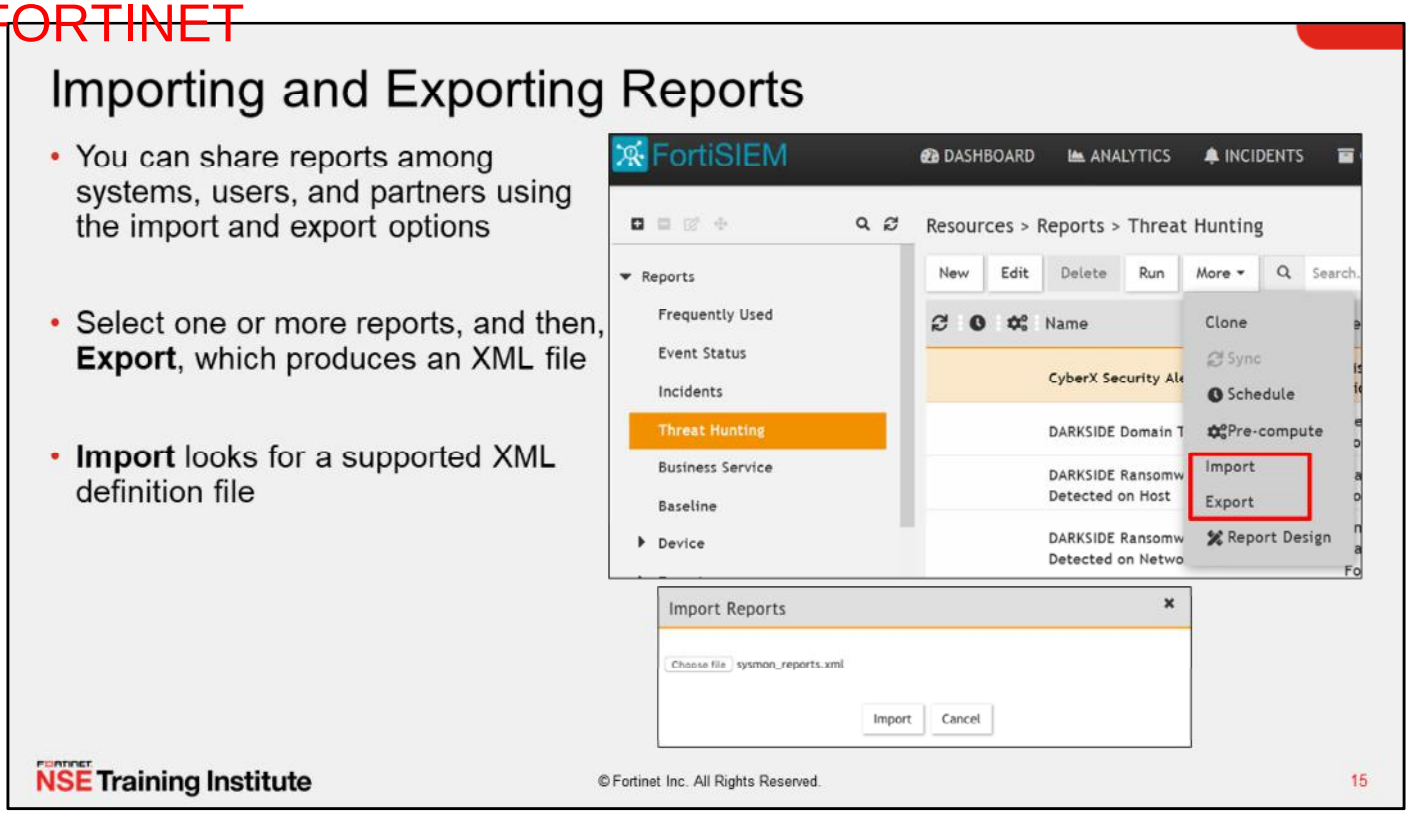
DO NOT REPRINT
© FORTINET
Brave-dumps.com



The **Scheduled** column is empty when no schedule is set for a report. When you see a green check mark in the **Scheduled** column, it indicates that a schedule has been created for that report.

Vouchers & Dumps are Available | WhatsApp +201224560923

DO NOT REPRINT Brave-dumps.com
© FORTINET



FortiSIEM makes it very easy to share reports among systems, users, and partners by using the importing and exporting options.

To export a report, select one or more reports, and then, in the **More** drop-down list, click **Export**. FortiSIEM copies an XML version of the report to be saved. You can share the saved XML file in an email or Notepad file to send it to another user. After the recipient receives the file, in the **More** drop-down list, they can click **Import**, click **Choose File,** select the XML file, and click **Import**. This allows them to create an exact copy of the report. This is an easy way to get a report that was prepared in a lab environment into the production system.

Vouchers & Dumps are Available | WhatsApp +201224560923

DO NOT REPRINT
© FORTINET
Brave-dumps.com

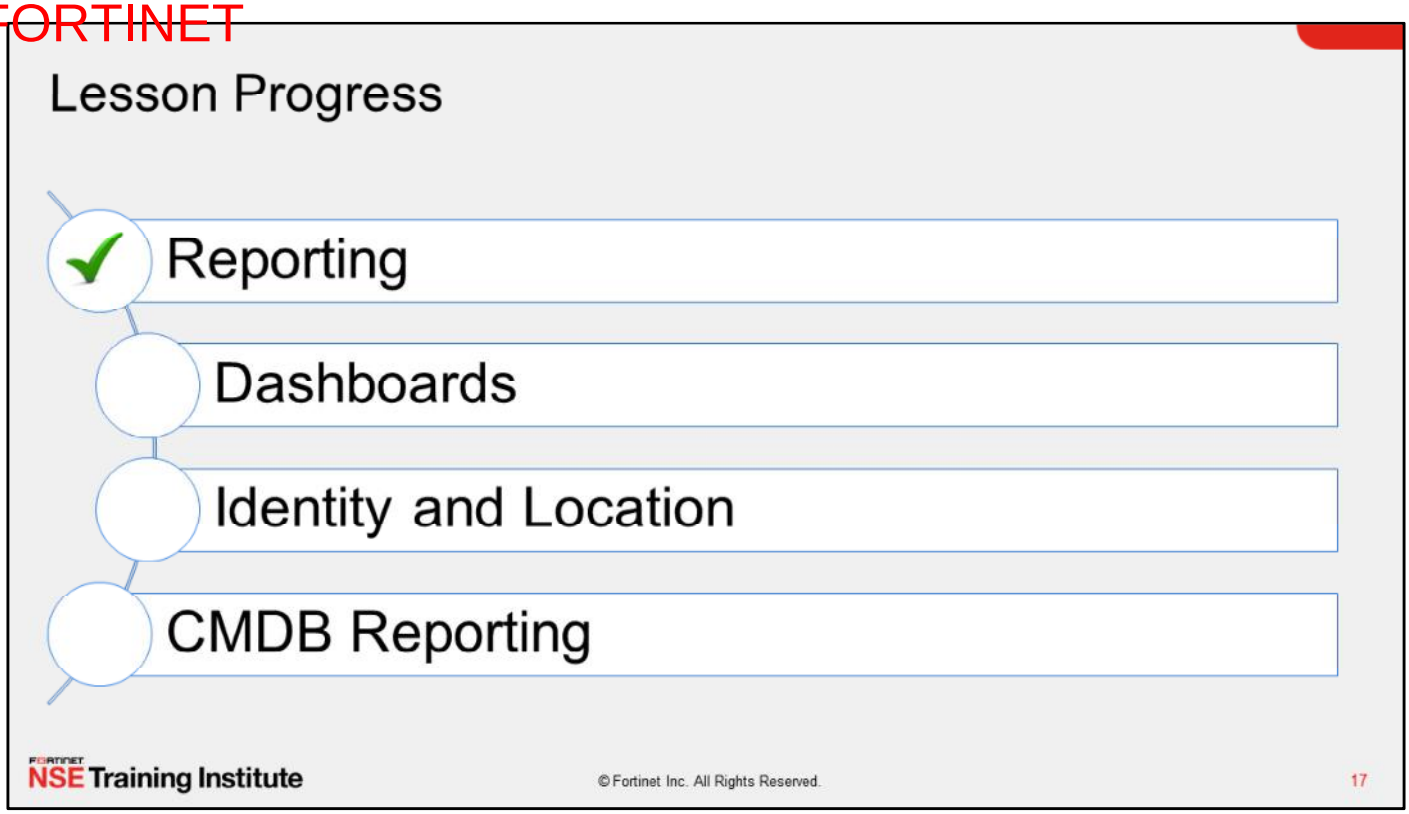
Knowledge Check

1. Which statement about FortiSIEM reports is correct?
   - ✓ A. FortiSIEM does not allow you to delete system reports
   - B. FortiSIEM does not allow you to delete user reports

NSE Training Institute
© Fortinet Inc. All Rights Reserved.
16

Vouchers & Dumps are Available | WhatsApp +201224560923

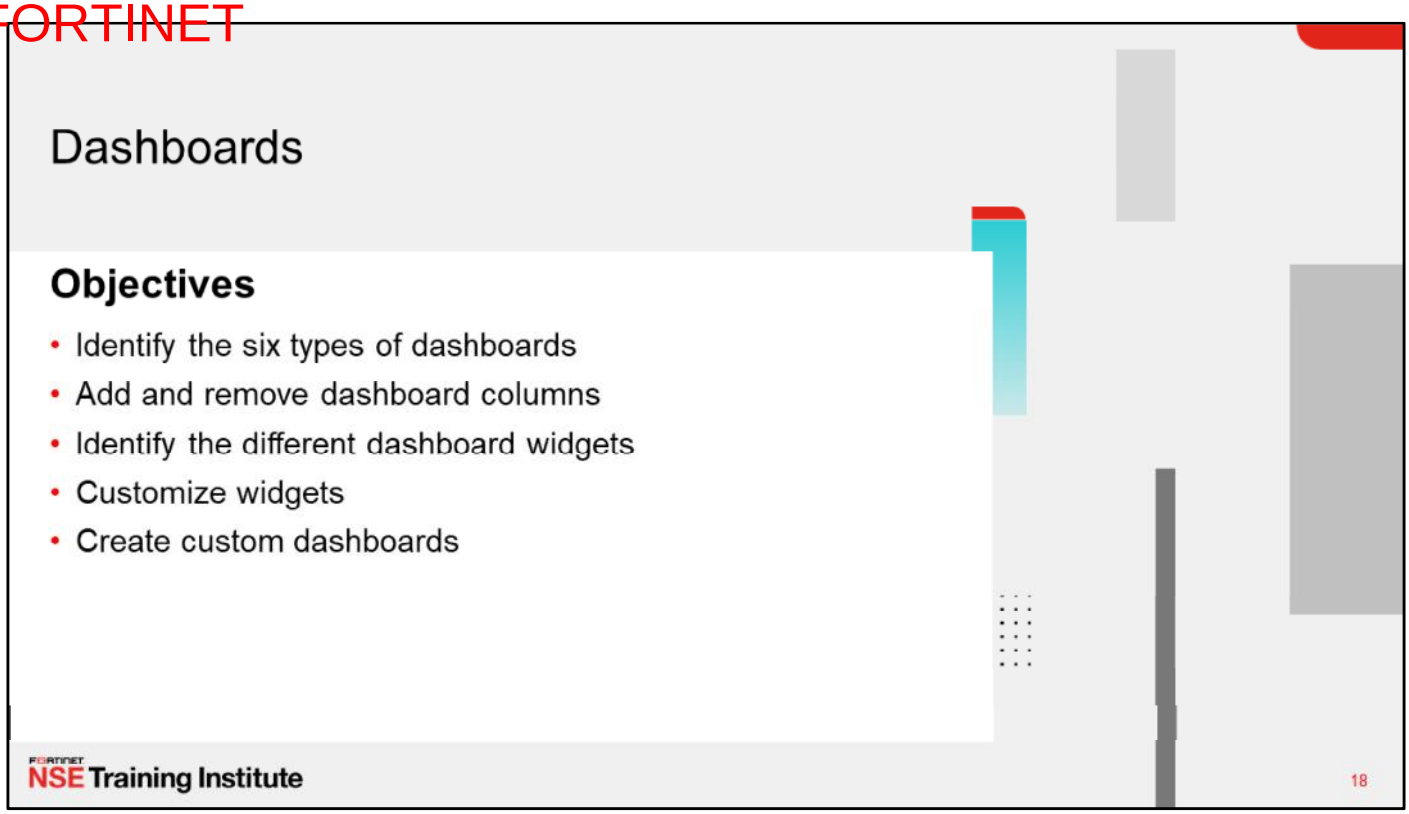
DO NOT REPRINT
© FORTINET
Brave-dumps.com



Good job! You now understand reporting. Now, you'll learn about dashboards.

Vouchers & Dumps are Available | WhatsApp +201224560923

DO NOT REPRINT
© FORTINET
Brave-dumps.com

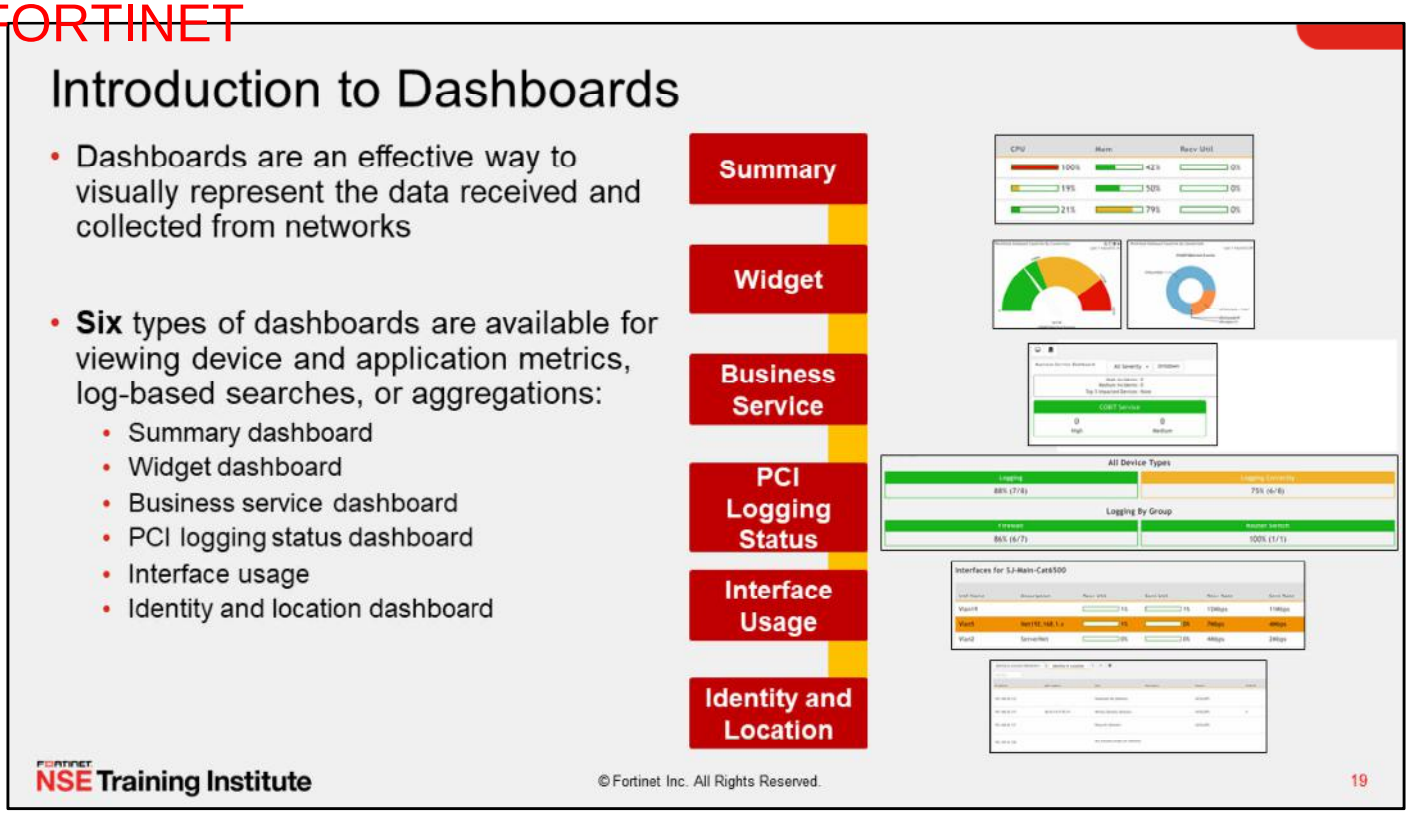


After completing this section, you should be able to achieve the objectives shown on this slide.

By demonstrating competence in dashboards, you will be able to identify, modify, create, and customize dashboards.

Vouchers & Dumps are Available | WhatsApp +201224560923

DO NOT REPRINT
© FORTINET
Brave-dumps.com



Dashboards are an effective way to visualize the data that has been received or collected from the devices in your network. There are four types of dashboards available for viewing device and application metrics, as well as any log-based search or aggregation of data:

- Summary dashboard
  - Summary dashboards show a near real-time view of health, uptime, incidents, and other key performance metrics of many devices, in a single spreadsheet format—each row is a device and each column is a metric.
- Widget dashboard.
  - Widget dashboards offer a traditional Top N dashboard view—one chart for one metric
- Business service dashboard
  - Business service dashboards provide a top-down view of business service health
- PCI Logging Status dashboard
  - The PCI Logging Status dashboard provides an overview of which devices in PCI are logging and logging correctly
- Interface usage
  - This dashboard provides an overview of the use of individual interfaces of router and firewall devices
- Identity and Location dashboards
  - Identity and Location dashboards provide a tabular view of network-identity to user-identity mappings

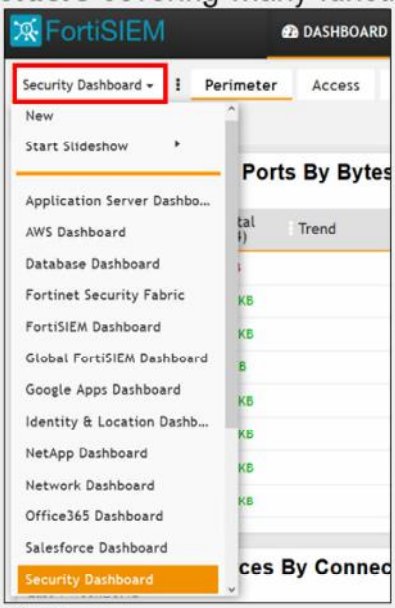
FortiSIEM comes with many default summary and widget dashboards.

Vouchers & Dumps are Available | WhatsApp +201224560923

DO NOT REPRINT
© FORTINET
Brave-dumps.com

Dashboards by Function

- FortiSIEM provides several built-in dashboard **folders** covering many functional areas:
- Network Dashboard
- Server Dashboard
- VMWare Dashboard
- Web Server Dashboard
- Application Server Dashboard
- AWS Dashboard
- Database Dashboard
- FortiSIEM Dashboard
- Fortinet Security Fabric
- Identity & Location Dashboard
- Security Dashboard



NSE Training Institute

© Fortinet Inc. All Rights Reserved.

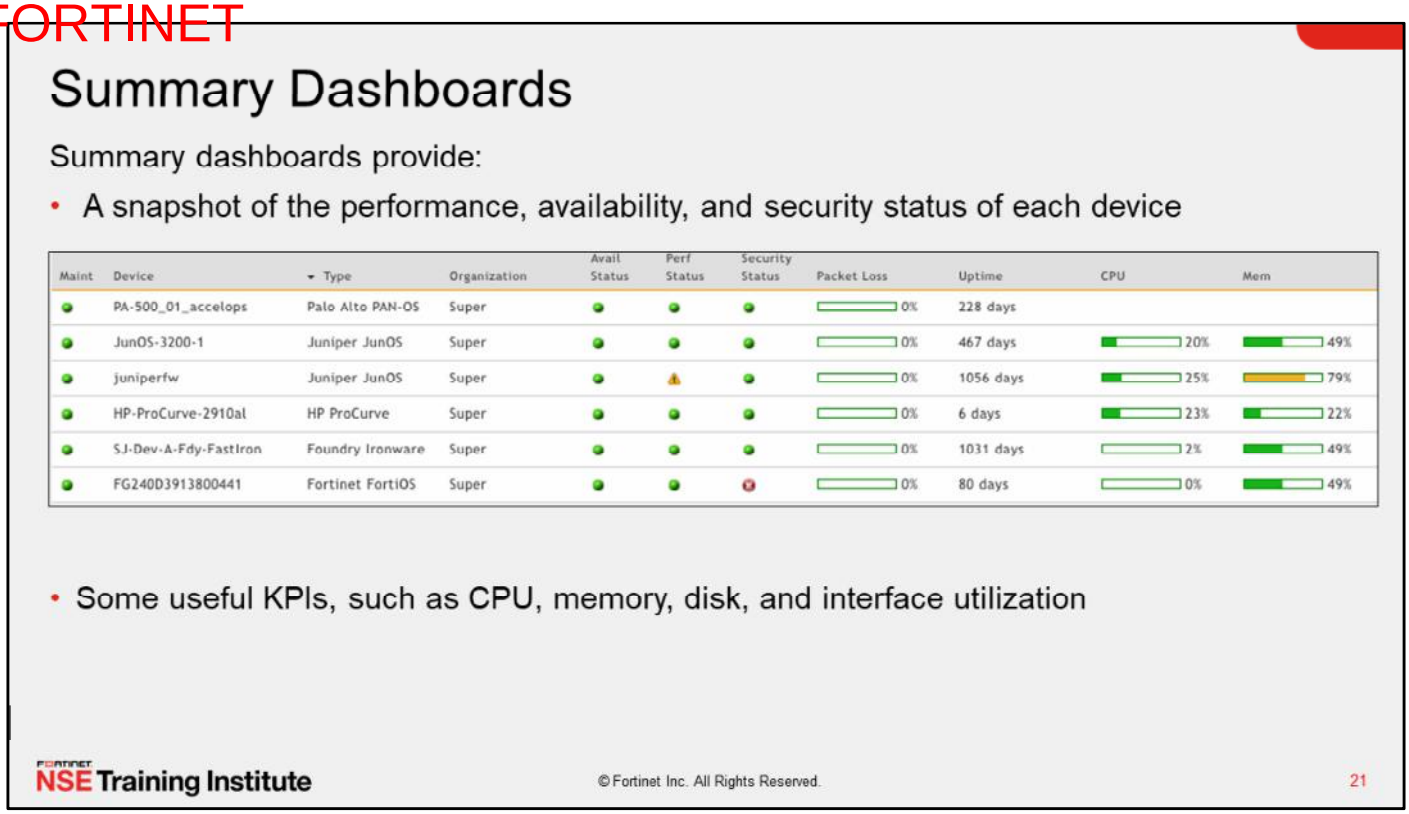
20

FortiSIEM provides a dashboard by function option. This function provides many default dashboards that are grouped by a common classification of device, such as servers, environmental devices, network devices, and so on.

An important thing to note is that multiple users can share any dashboard created under this category.

Vouchers & Dumps are Available | WhatsApp +201224560923

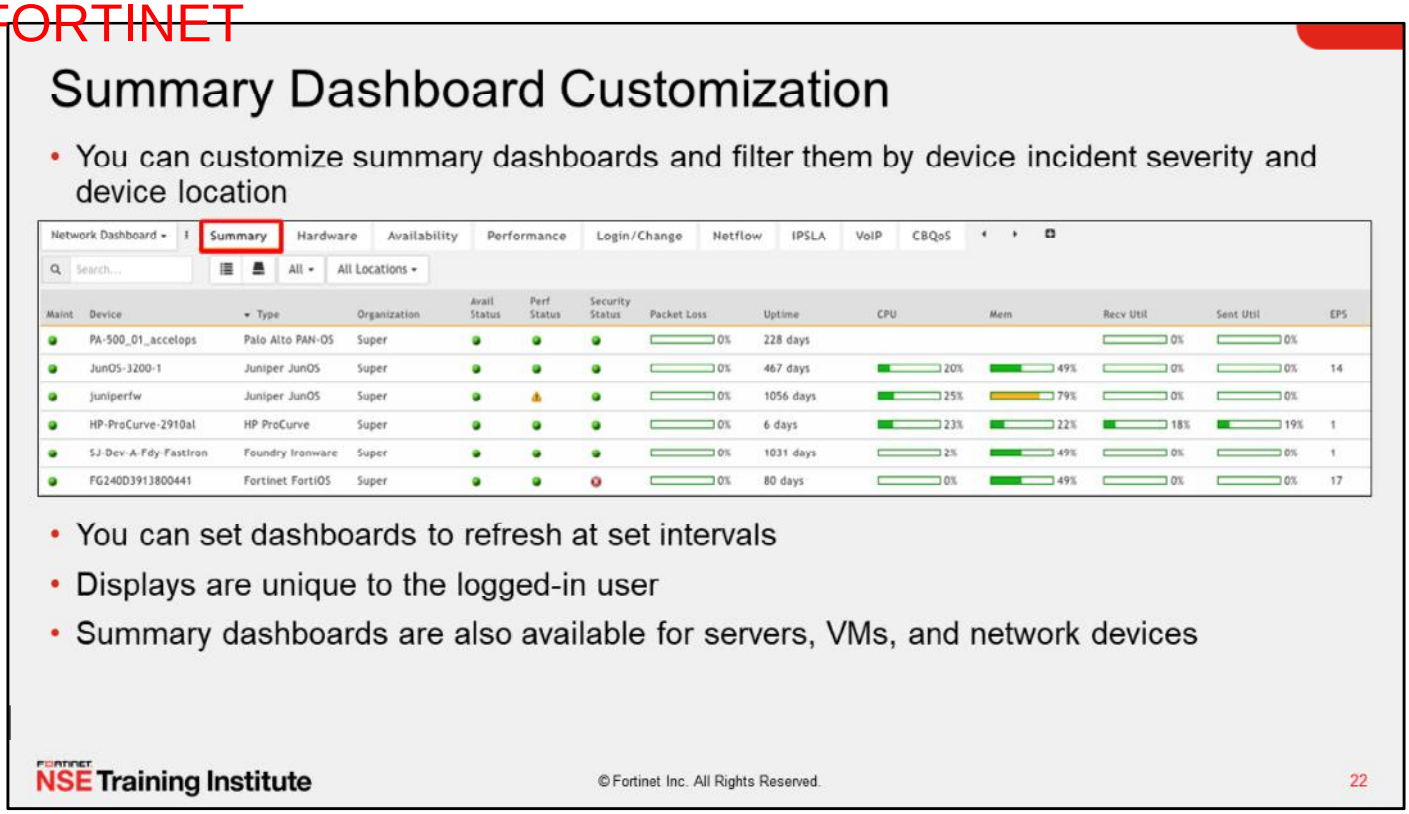
DO NOT REPRINT
© FORTINET
Brave-dumps.com



Summary dashboards provide a snapshot of the performance, availability, and security status of each device in your environment. They also return some useful key performance indicators (KPIs), such as CPU, memory, disk, and interface utilization.

Vouchers & Dumps are Available | WhatsApp +201224560923

DO NOT REPRINT
© FORTINET
Brave-dumps.com



You can customize summary dashboards and add whatever metrics you require to these kinds of views. You can filter by device incident severity and device location.

You can also set an interval for the dashboard refresh rate in a drop-down list at the top of the page. The default setting is three minutes, but you can choose from 1, 2, 3, 5, and 10-minute intervals.

These displays are unique to the logged-in user. If you customize these displays, the change is visible only to you.

There are summary dashboards specifically for servers, VMWare devices, and network devices.

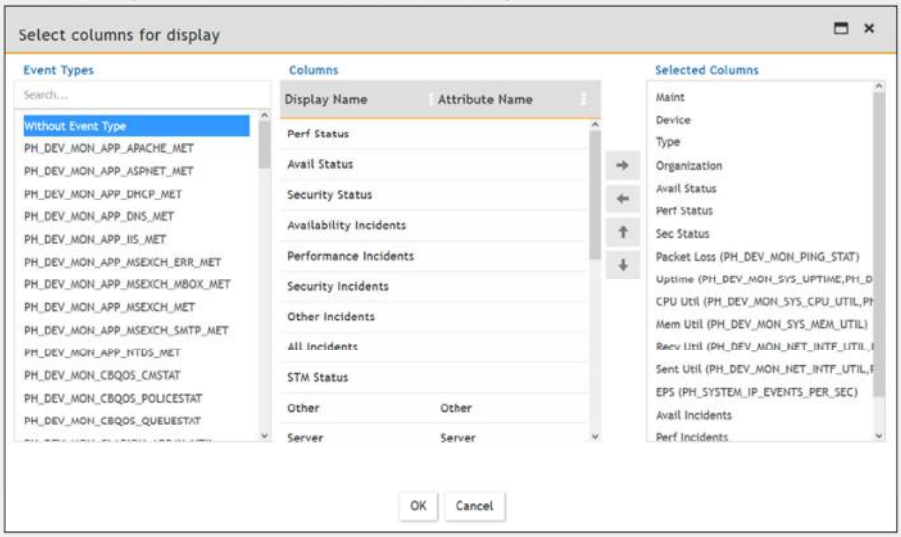
Vouchers & Dumps are Available | WhatsApp +201224560923

DO NOT REPRINT
© FORTINET
Brave-dumps.com

Adding and Removing Summary Dashboard Columns

- Add or remove columns from summary dashboards as necessary





NSE Training Institute

© Fortinet Inc. All Rights Reserved.

23

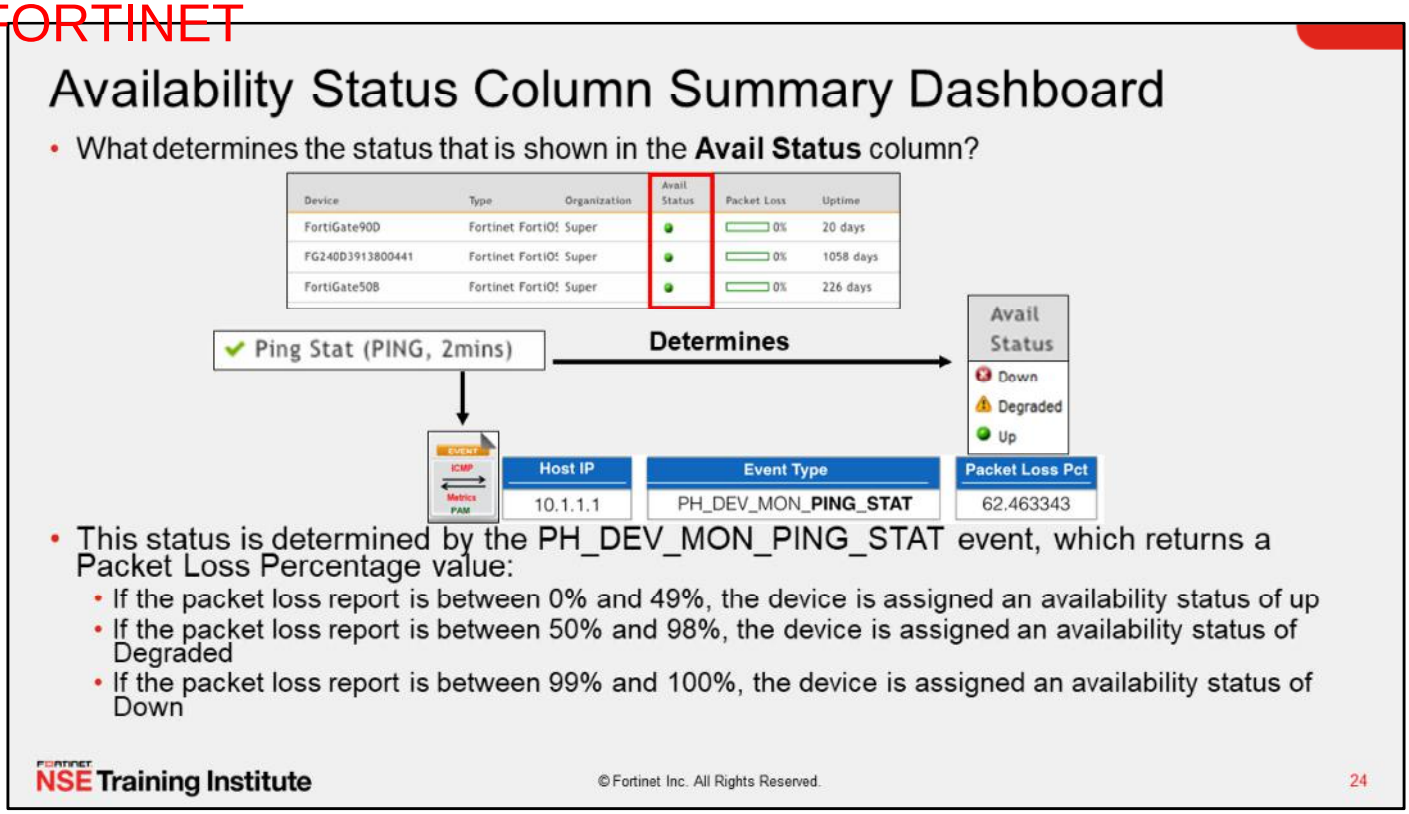
You can customize the summary dashboard. You can add, remove, and reorder columns as necessary. In the **Select columns for display** window, the left pane lists the event types that contain the metrics that you might want to add to the dashboard.

The middle pane lists the metrics that are available for the selected event type.

On the right, you can add or remove metrics to the display. You can also move a metric up and down the list, which controls the order of the columns being displayed from left to right.

Vouchers & Dumps are Available | WhatsApp +201224560923

DO NOT REPRINT
© FORTINET
Brave-dumps.com



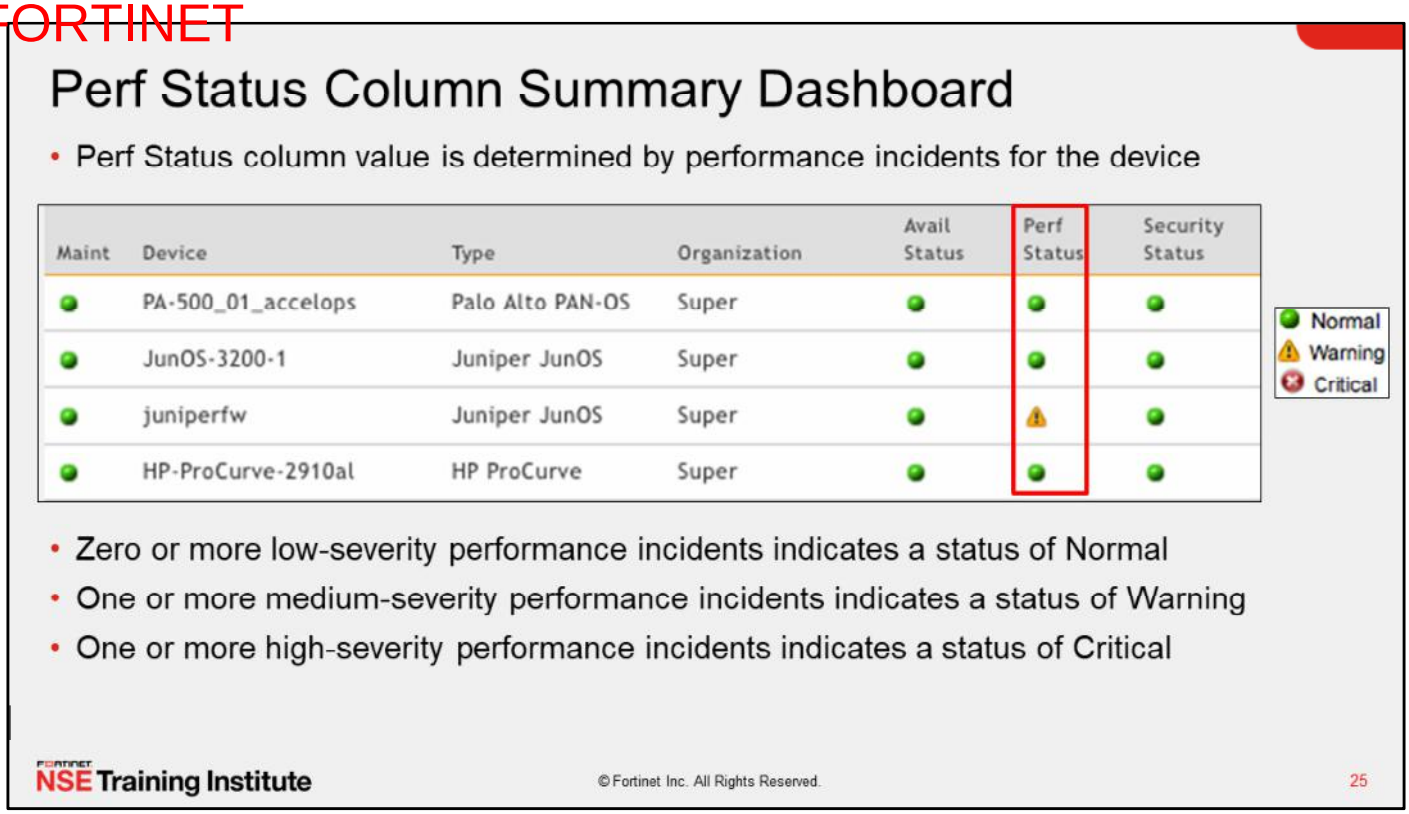
The status that is shown in the availability status column can be Down, Degraded, or Up.

This status is determined by the PH_DEV_MON_PING_STAT event, which returns a packet loss percentage:

- If the packet loss report is between 0% and 49%, the device is assigned an availability status of Up.
- If the packet loss report is between 50% and 98%, the device is assigned an availability status of Degraded.
- If the packet loss report is between 99% and 100%, the device is assigned an availability status of Down.

Vouchers & Dumps are Available | WhatsApp +201224560923

DO NOT REPRINT
© FORTINET
Brave-dumps.com

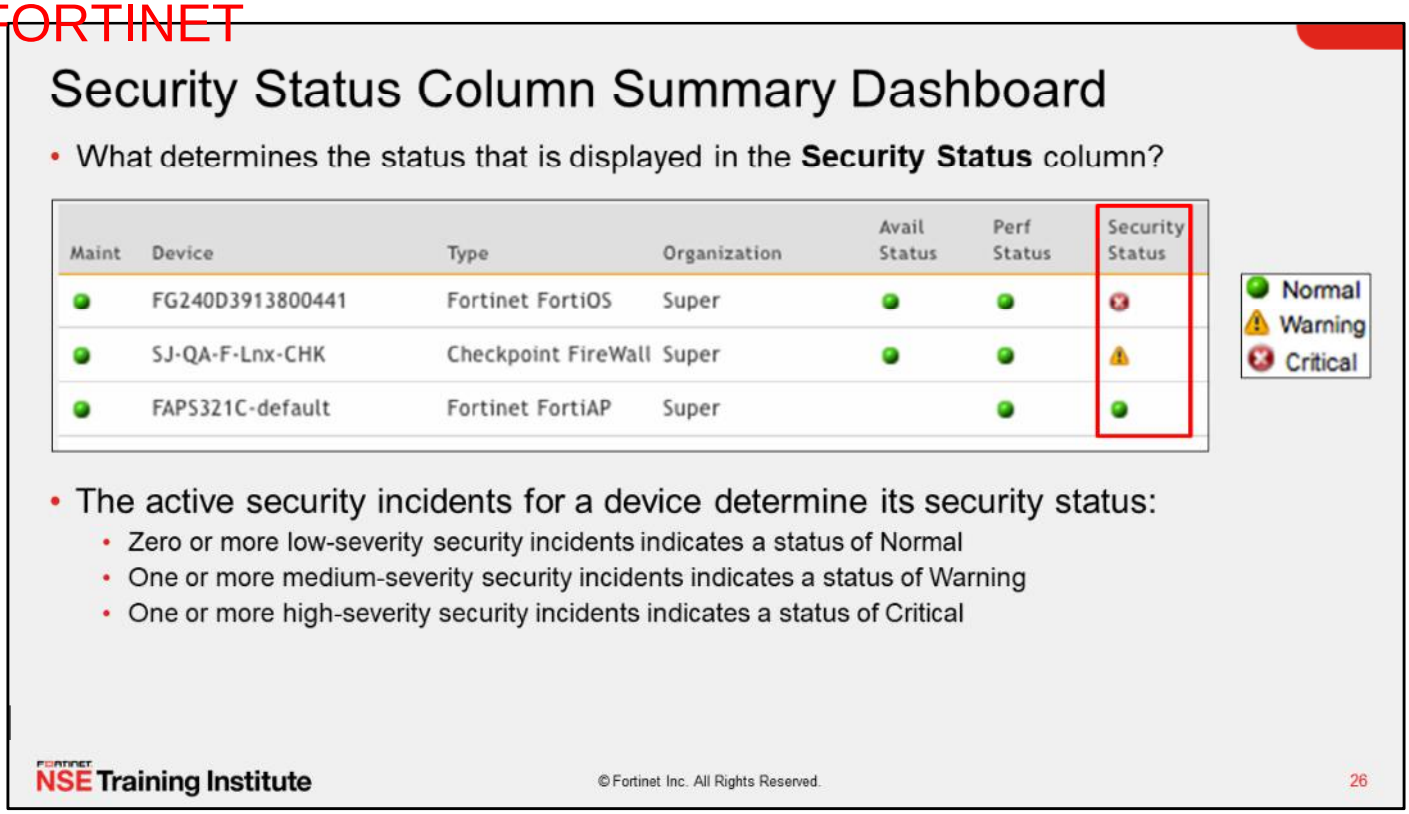


The status displayed in the **Perf Status** column is determined by performance incidents associated with a device.

- If there are currently no performance incidents or only low-performance incidents for a device, then it will be assigned a performance status of Normal.
- If there are one or more medium-severity performance incidents for a device, then it will be assigned a performance status of Warning.
- If there are one or more high-severity performance incidents for a device, then it will be assigned a status of Critical.

Vouchers & Dumps are Available | WhatsApp +201224560923

DO NOT REPRINT
© FORTINET
Brave-dumps.com



The **Security Status** column shows the security status of the device. The device status can be: Normal, Warning, or Critical.

The active security incidents for a device determine its security status:

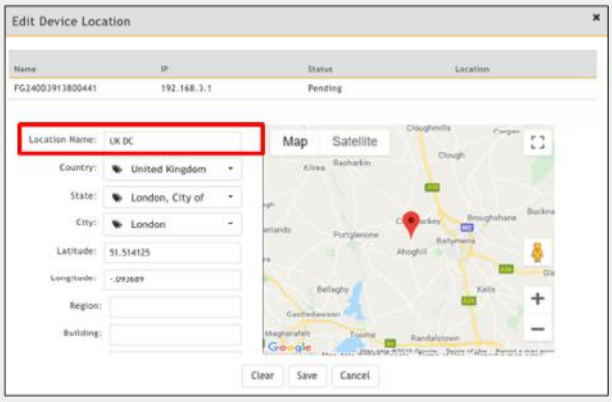
- If there are no security incidents or only low-severity incidents for a device, then that device is assigned a security status of Normal.
- If there are one or more medium-severity incidents for a device, then that device is assigned a security status of Warning.
- If there are one or more high-severity incidents for a device, then that device is assigned a security status of Critical.

Vouchers & Dumps are Available | WhatsApp +201224560923

DO NOT REPRINT
© FORTINET
Brave-dumps.com

Setting a Single Device Location

- You can define a location for a single device using the **Location** option on the **CMDB** tab



- The **Country**, **State**, and **City** fields are used for local IP geolocation enrichment through the parser
- The entry in the **Location Name** field is used in the dashboard **Location** column

NSE Training Institute

© Fortinet Inc. All Rights Reserved.

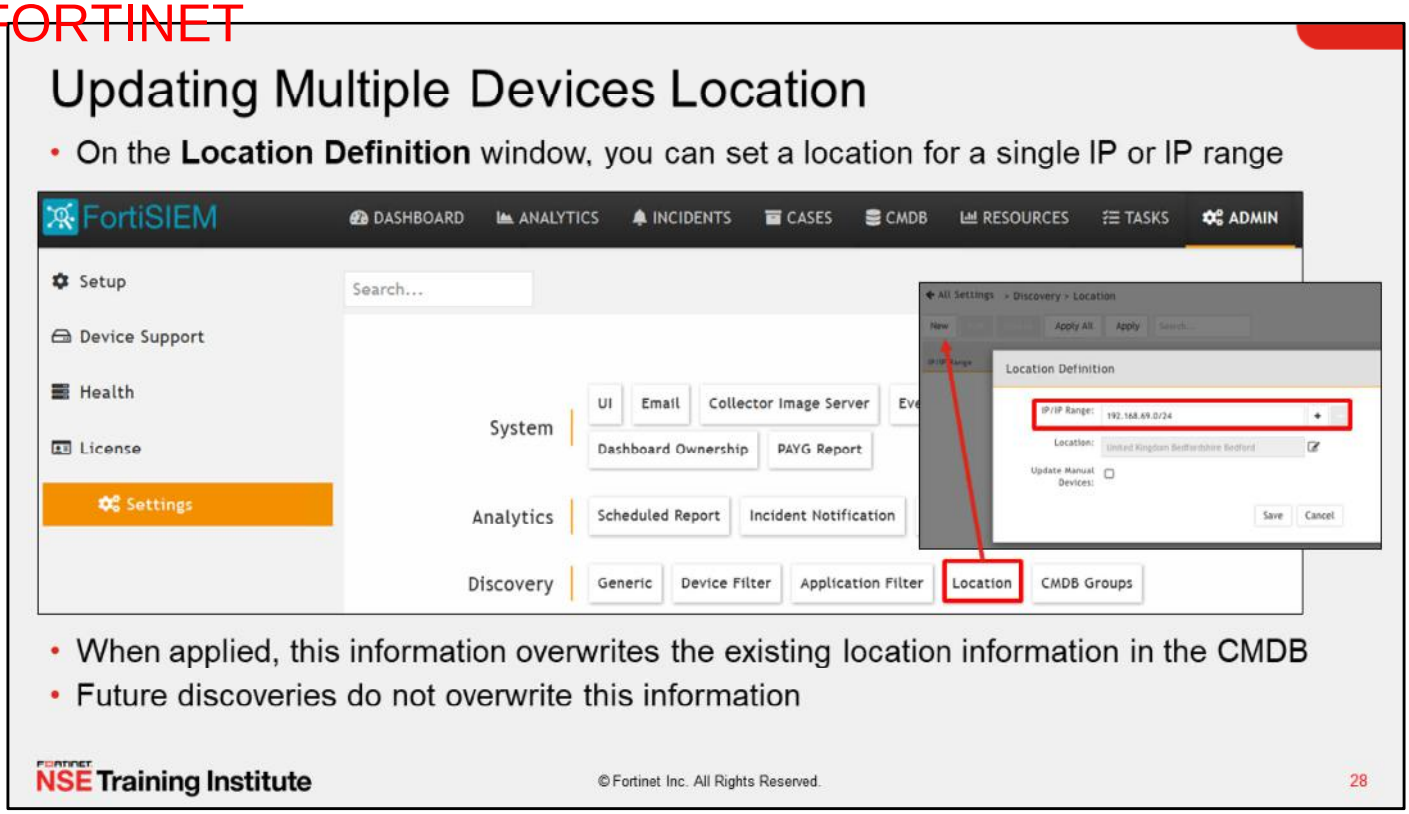
27

You have two options for setting a location for your device. For a single device, you can set the location through the CMDB. On the **CMDB** tab, in the upper-right corner, select the **Location** option from the **Actions** drop-down list. In the **Edit Location** window, you can select values for the **Country**, **State**, and **City** fields. There are also fields where you can set values for latitude, longitude, and even for building and floor, if you want to include that level of detail. These values are used for local IP geolocation enrichment by the parser.

The entry in the **Location Name** field is used in the dashboard **Location** column.

Vouchers & Dumps are Available | WhatsApp +201224560923

DO NOT REPRINT
© FORTINET
Brave-dumps.com



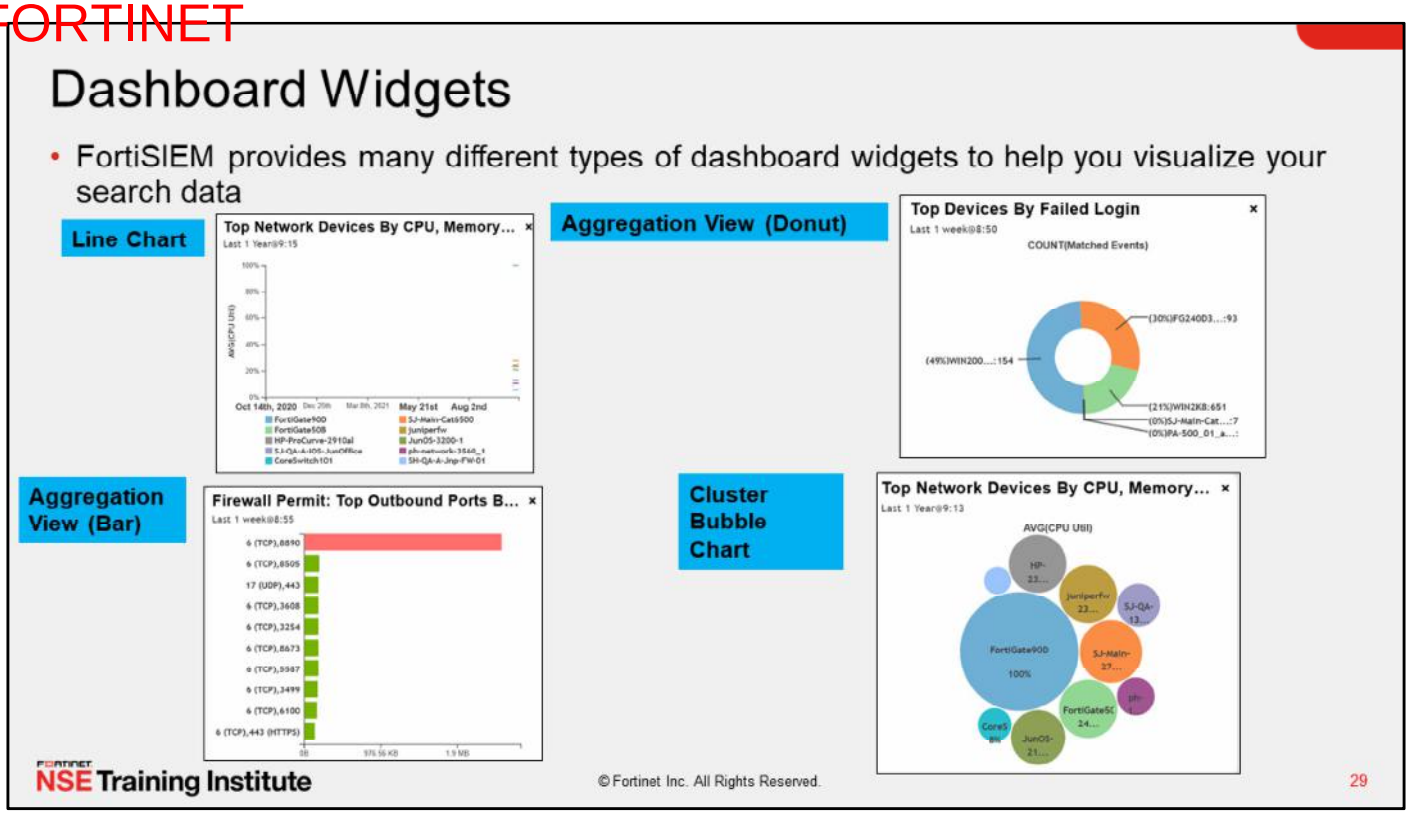
You can also update a location for multiple devices at once.

If you click **Admin** > **General Settings** > **Discovery** > **Location**, you can set a location for an individual IP or an IP Range. If you click the edit icon next to the **Location** field, the **Location Definition** window opens.

When you apply information here, it overwrites the existing location information found in the CMDB, and future discoveries do not overwrite this information.

Vouchers & Dumps are Available | WhatsApp +201224560923

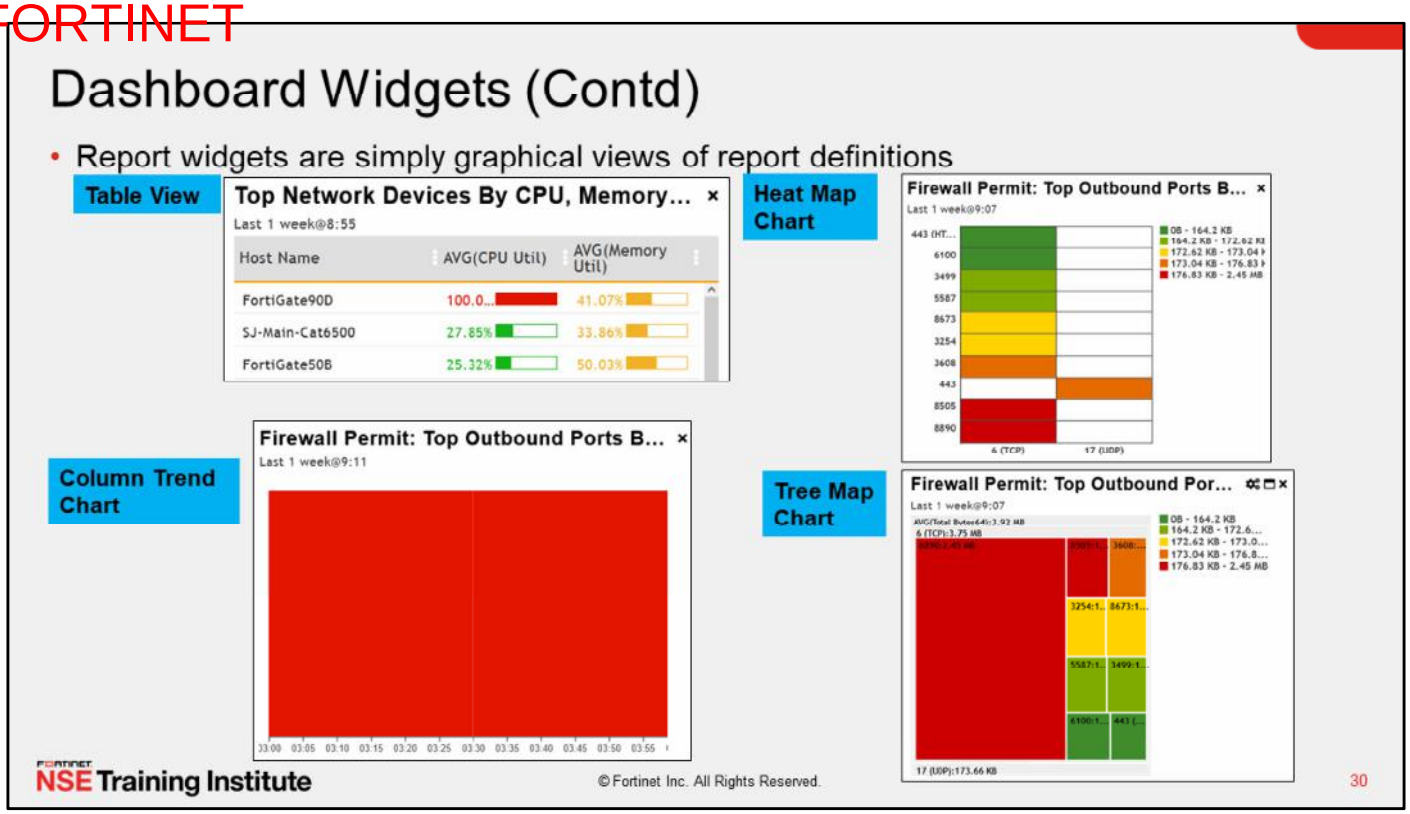
DO NOT REPRINT
© FORTINET
Brave-dumps.com



Dashboard widgets provide you with different ways to visualize your search data. Each dashboard widget represents a report in the FortiSIEM system. This slide shows some examples of the widgets that are available: line chart, donut (pie chart), bar chart, and cluster bubble view. The combo view type widget shows the current value, as well as a view of the trend of the value over time.

Vouchers & Dumps are Available | WhatsApp +201224560923

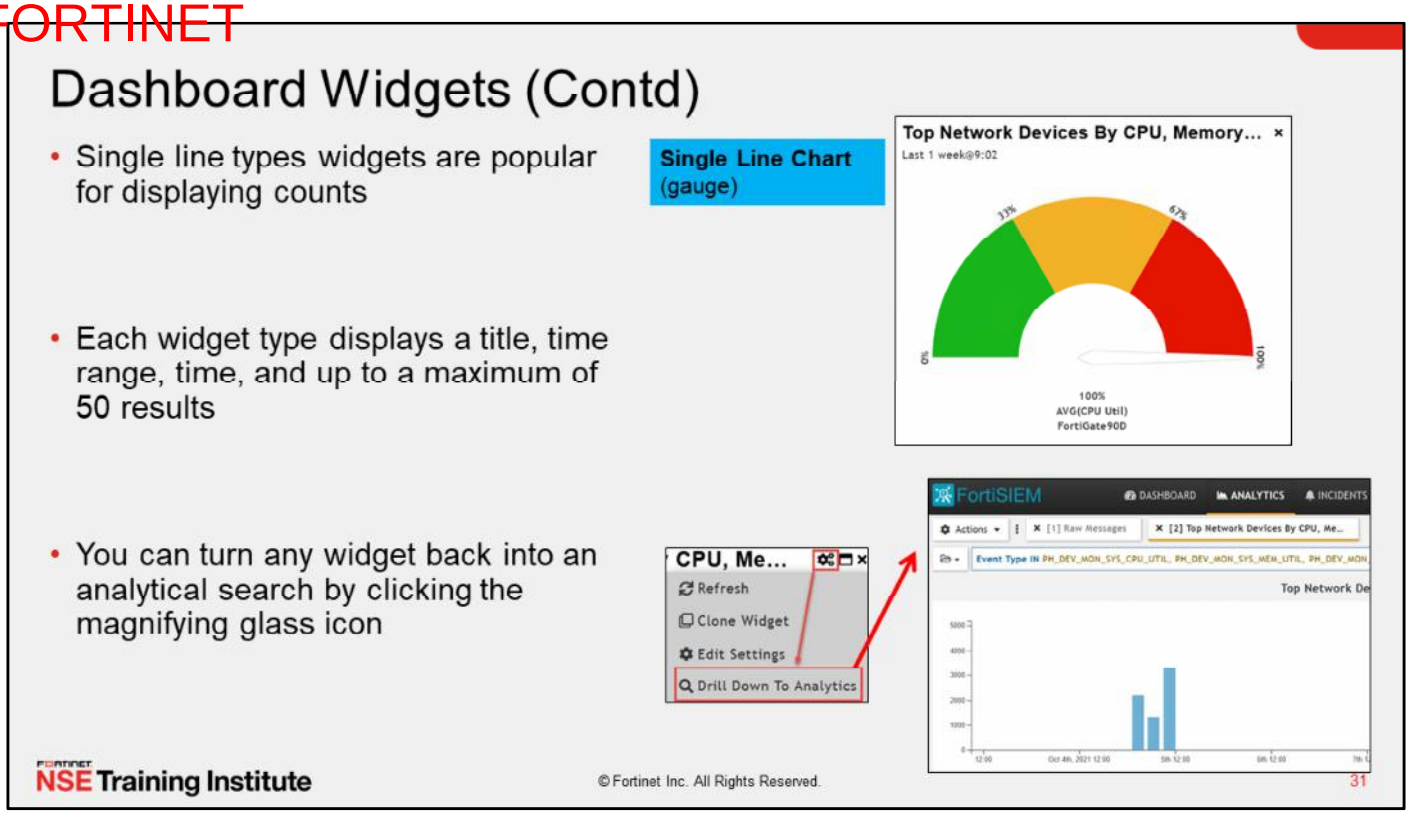
DO NOT REPRINT Brave-dumps.com
© FORTINET



Other examples of dashboard widgets include table view, column trend chart, heat map chart, and tree map chart. All of these widgets provide a graphical view of report definitions.

Vouchers & Dumps are Available | WhatsApp +201224560923

DO NOT REPRINT
© FORTINET
Brave-dumps.com



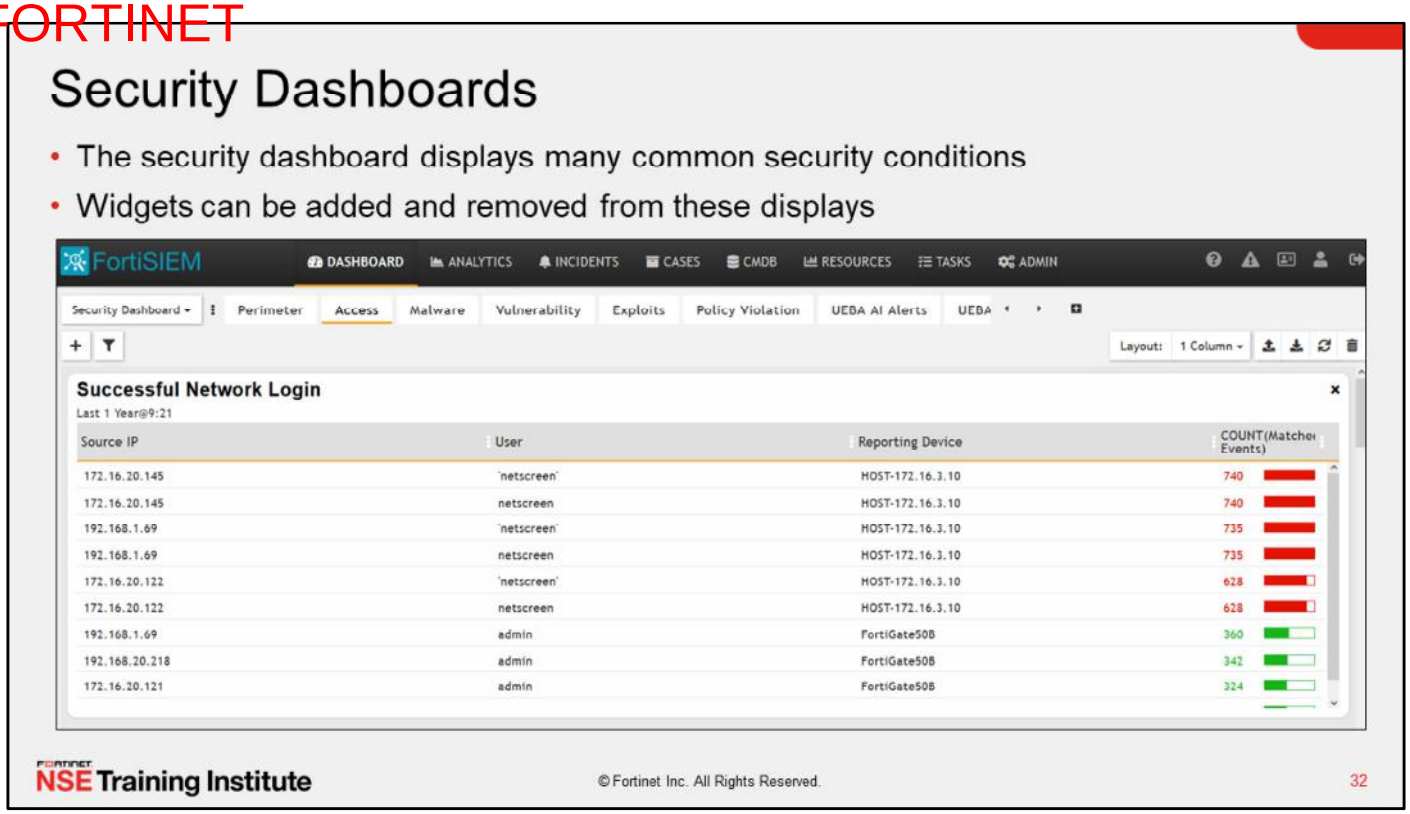
The single line view can display a single value, such as a count of the number of matched events, or a gauge.

On any widget type, you can customize:
- The title
- The time range for the search
- The refresh interval
- The result limit, up to a maximum of 50 results

You can turn any widget back into an analytical search, by clicking the magnifying glass icon.

Vouchers & Dumps are Available | WhatsApp +201224560923

DO NOT REPRINT Brave-dumps.com
© FORTINET

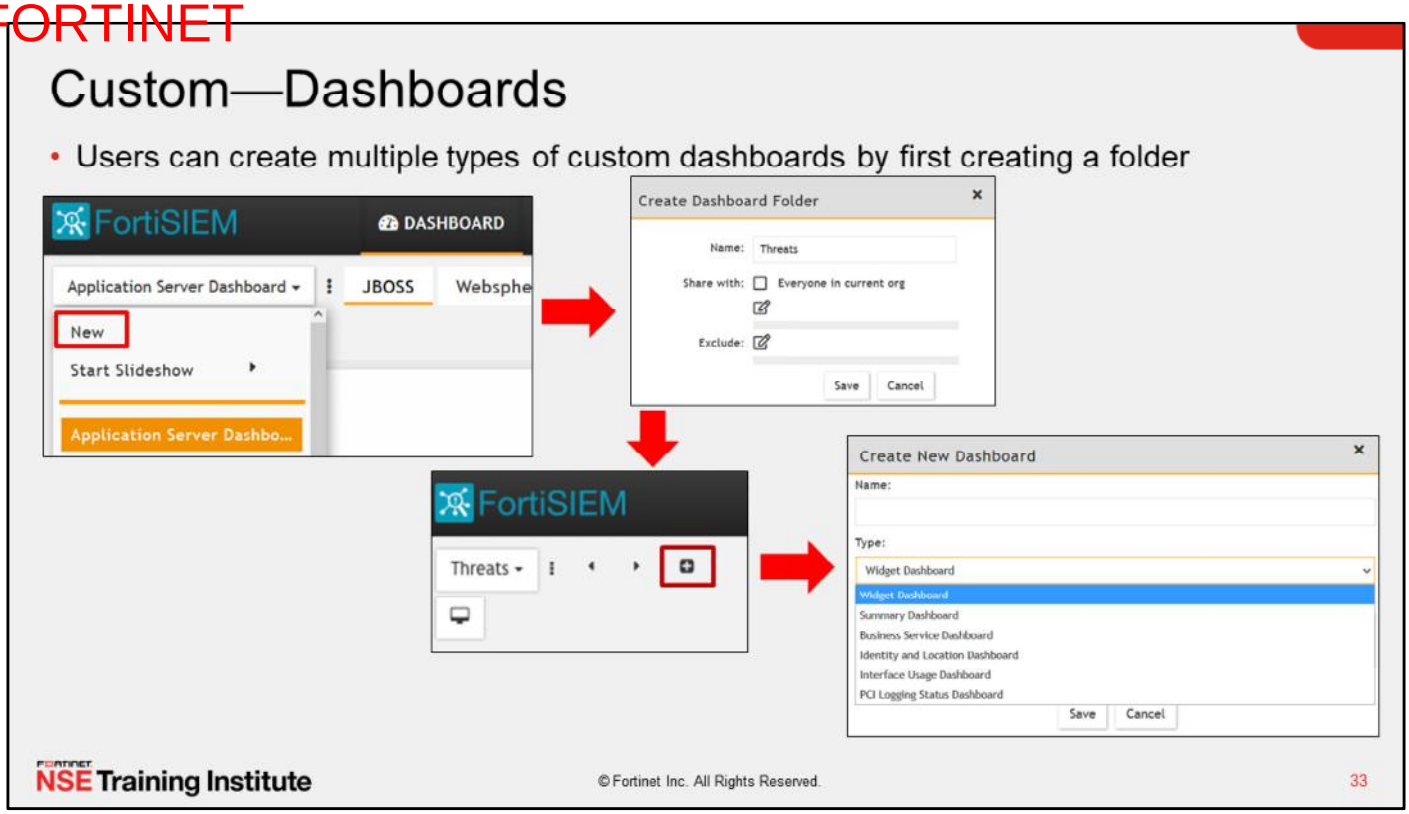


FortiSIEM comes with many of out-of-the-box dashboards. One of these is the security dashboard. The security dashboard displays many common security conditions, such as the top outbound ports, top firewalls by high port bytes, top audit event categories, top security event by count, and so on.

You can add or remove widgets from any default dashboard, as required.

Vouchers & Dumps are Available | WhatsApp +201224560923

DO NOT REPRINT Brave-dumps.com
© FORTINET



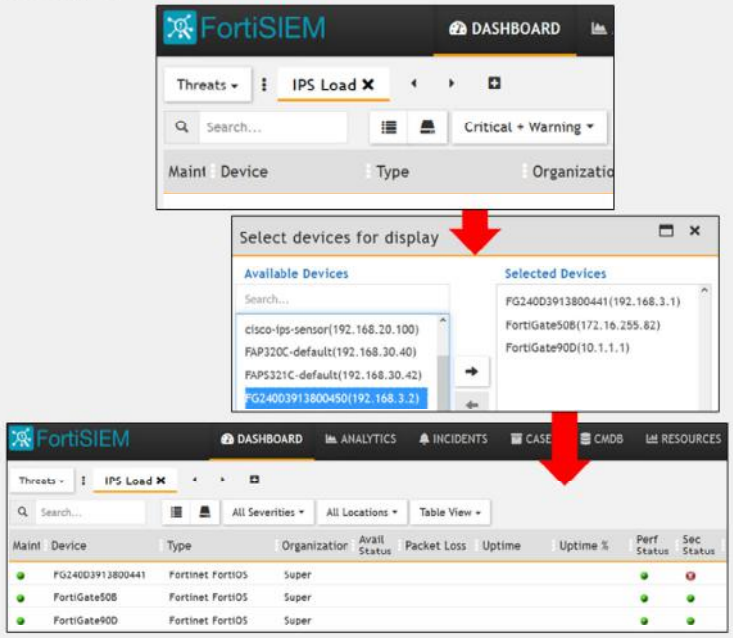
FortiSIEM allows multiple custom summary, or custom widget dashboards to be created by users. Users can create custom dashboards that are related to their individual job function.

Vouchers & Dumps are Available | WhatsApp +201224560923

DO NOT REPRINT
© FORTINET
Brave-dumps.com

Custom—Summary Dashboard

- You must add devices to the custom summary dashboards
- Dashboard is empty by default
- Use the device icon and select devices from available devices
- Use case: You can create summary dashboards for just the devices a user manages



NSE Training Institute

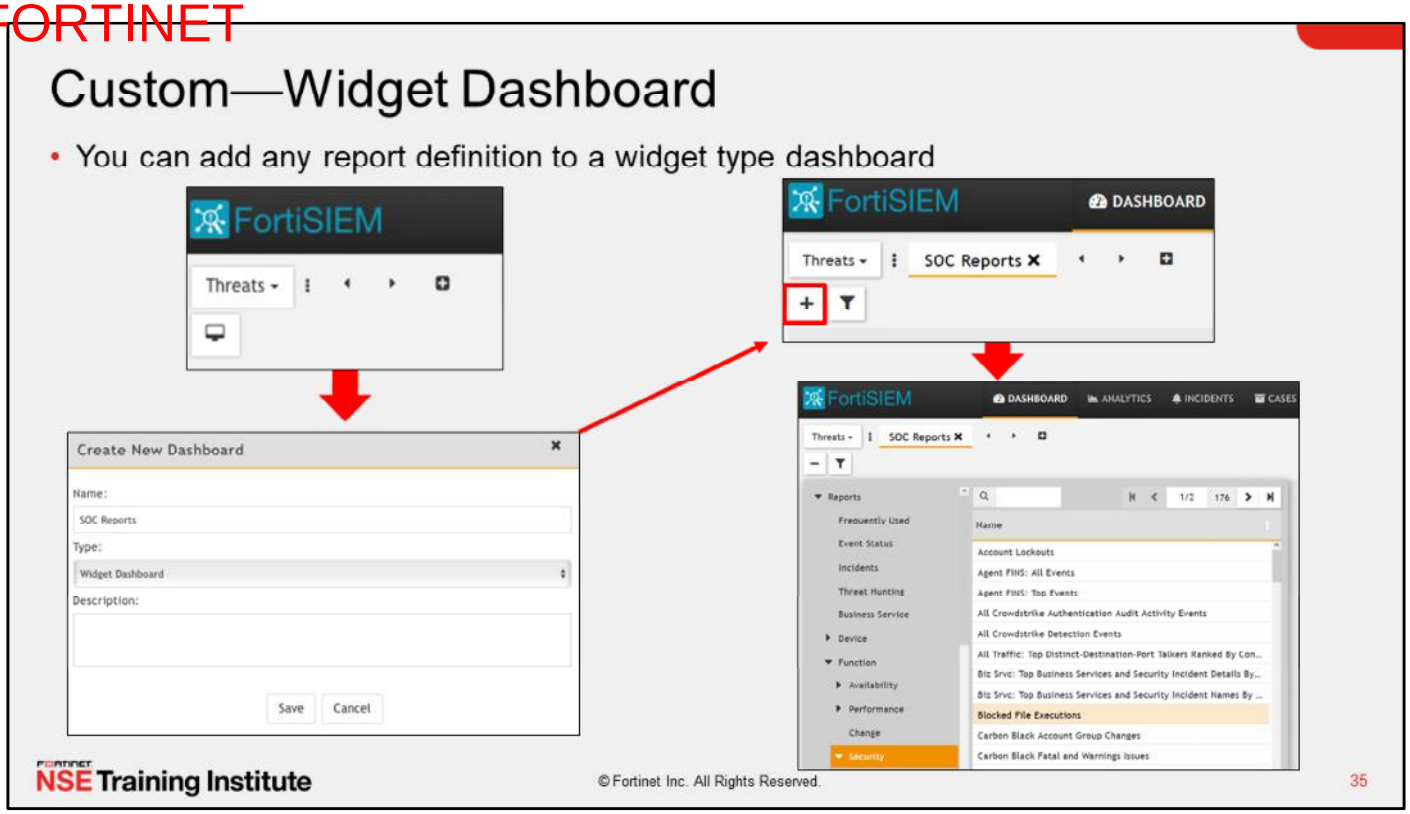
© Fortinet Inc. All Rights Reserved.

34

You must add devices to the custom summary dashboards display. This allows a summary dashboard to be created just for the devices a user manages or the devices that a particular user is responsible for.

Vouchers & Dumps are Available | WhatsApp +201224560923

DO NOT REPRINT Brave-dumps.com
© FORTINET



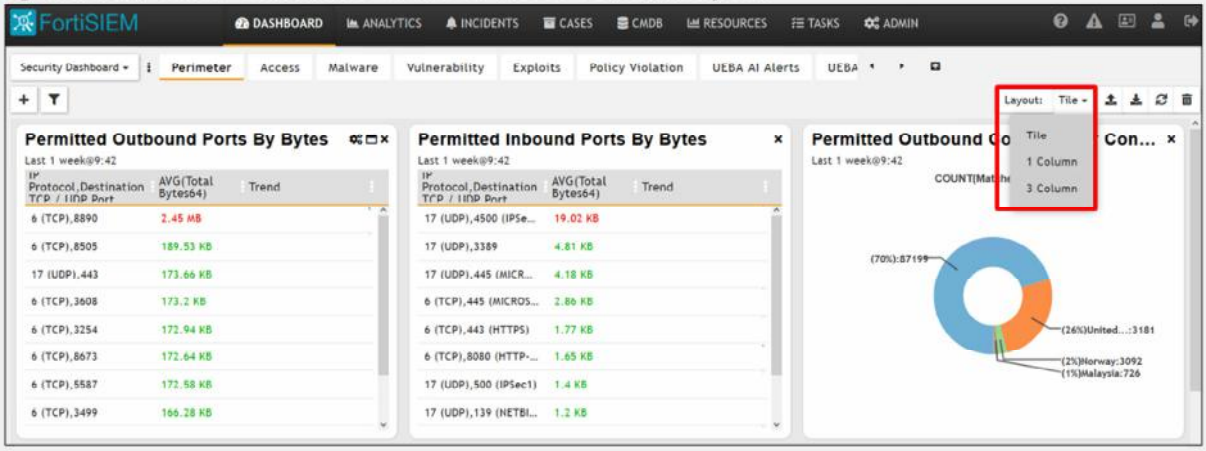
Custom widget dashboards essentially provide a blank canvas to which you can add any report definition as a widget type. Select a report, and then click the white arrow icon to add as widgets to the dashboard. You can then edit and configure the settings for that widget, such as a bar chart, map, and so on. You can add CMDB reports to a widget dashboard as well.

Vouchers & Dumps are Available | WhatsApp +201224560923

DO NOT REPRINT
© FORTINET
Brave-dumps.com

Customizing Widget Dashboard Layouts

- Widget dashboards can have a tile or fixed column layout



- Tile separates the view into a number of squares, or tiles, that allow you to drag each widget around the screen

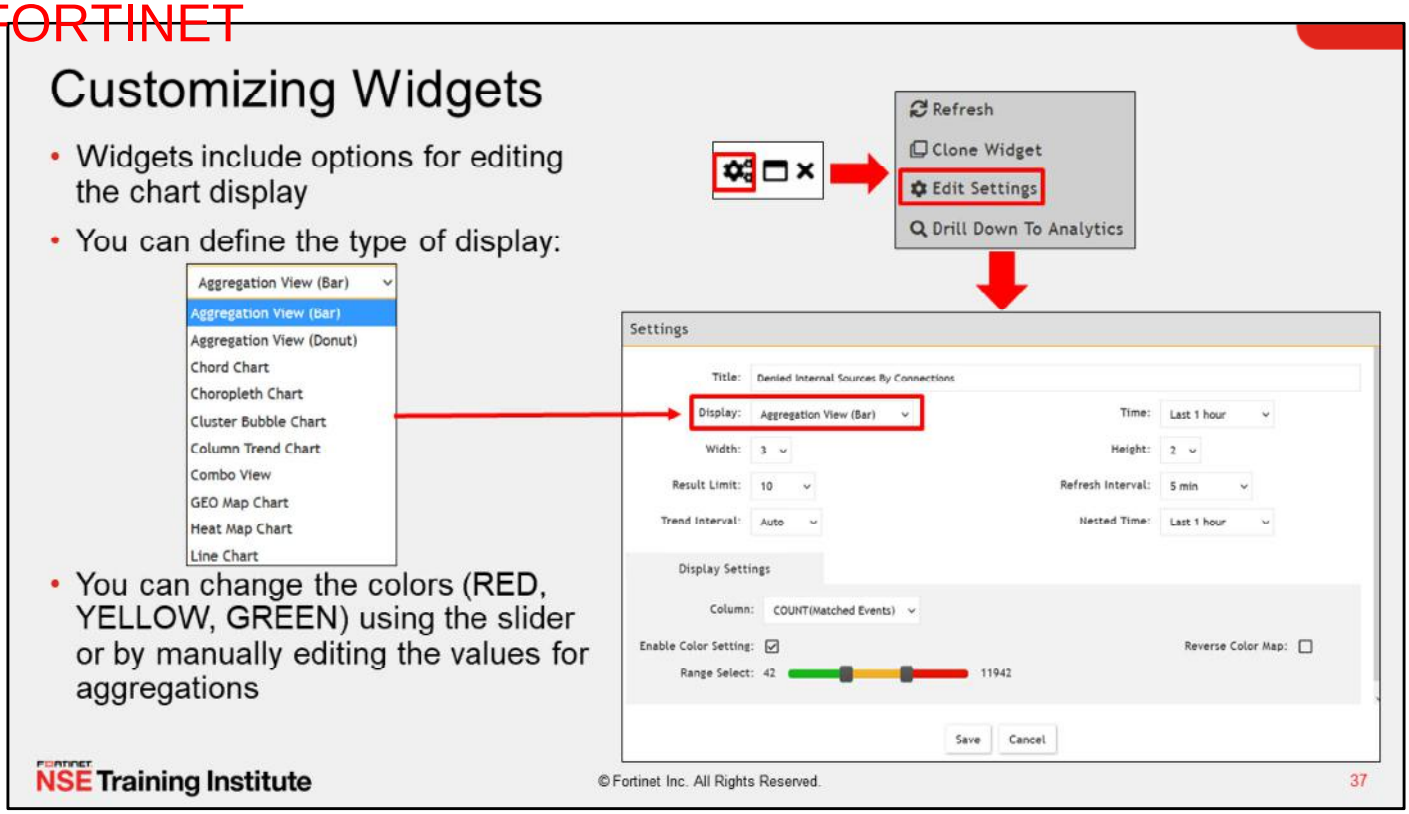
NSE Training Institute
© Fortinet Inc. All Rights Reserved.
36

Each widget dashboard can have a tiled layout or a defined number of columns layout.

You set the layout type using the **Layout Columns** drop-down list in the upper-right corner of the window. If you select **Tile**, the view is divided into a number of squares, or tiles, that allow you to drag each widget around the screen. You can move and size widgets to suit your needs.

Vouchers & Dumps are Available | WhatsApp +201224560923

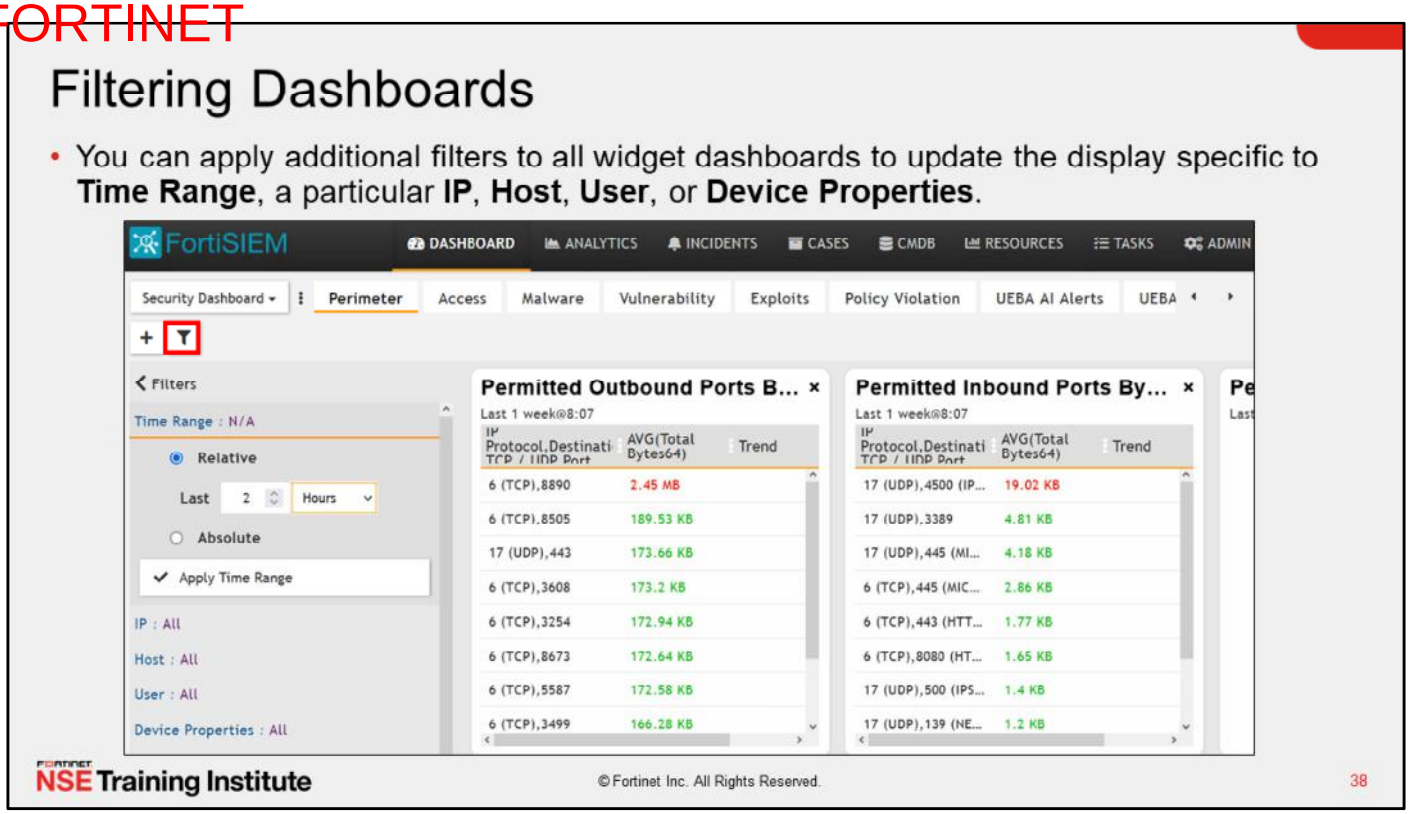
DO NOT REPRINT Brave-dumps.com
© FORTINET



You can customize most widgets in some way. For example, in the upper-right corner of most widgets, you'll find an edit chart display icon, which looks like a gear. The display options allow you to control the colors that are display in that widget. You can enter values directly, or use the slider to select the threshold values.

Vouchers & Dumps are Available | WhatsApp +201224560923

DO NOT REPRINT Brave-dumps.com
© FORTINET



You can search data for specific event attributes simultaneously in all the widgets in a dashboard. To do this, click the filter button on left side and select the values. You can search for the following event attributes:

- **Time Range**
- **IP** address (Source, Destination, Host)
- **Host** name (Source, Destination)
- **User**
- **Device Properties** defined in **ADMIN** > **Device Support** > **Custom Properties**.

For example, if you choose to filter on IP = 10.1.1.1, then only the entries for Source IP or Destination IP or Host IP = 10.1.1.1 are shown on all the widgets.

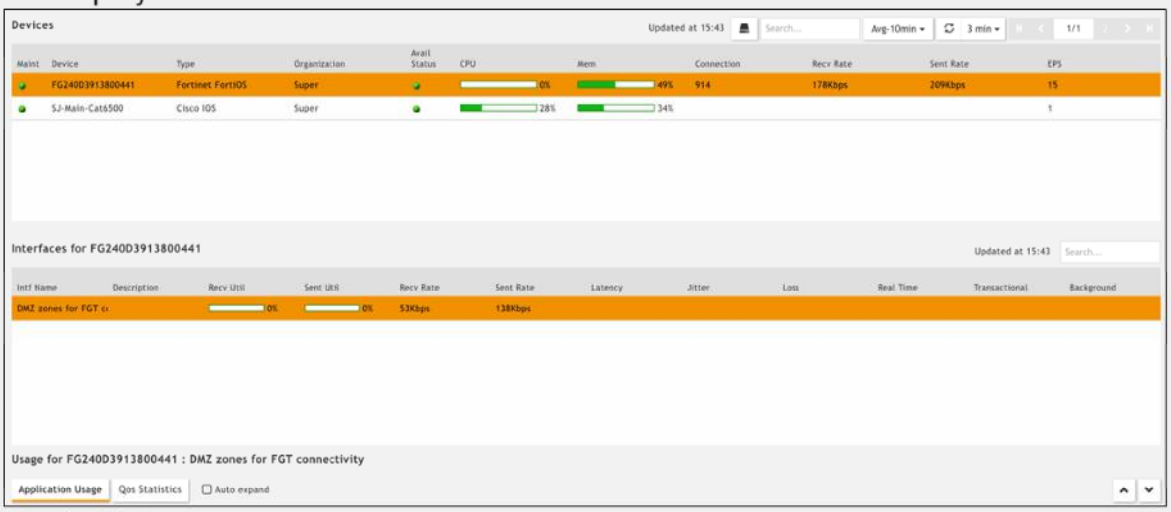
The values you can search are prepopulated by searching through the data in various widgets. You can only search for a value if it is present in any widget on the dashboard. Without filters, a dashboard shows precomputed results—so they load quickly. However, when you search, all the reports on the widget dashboard are run in an ad hoc mode. Subsequently, search results may return relatively slowly.

Vouchers & Dumps are Available | WhatsApp +201224560923

DO NOT REPRINT Brave-dumps.com
© FORTINET

Interface Usage Dashboards

- Allow monitoring in more detail of specific interfaces on selected devices
- After you select an interface, **Application Usage** (from Netflow) and **Qos Statistics** widgets display more data



NSE Training Institute

© Fortinet Inc. All Rights Reserved.

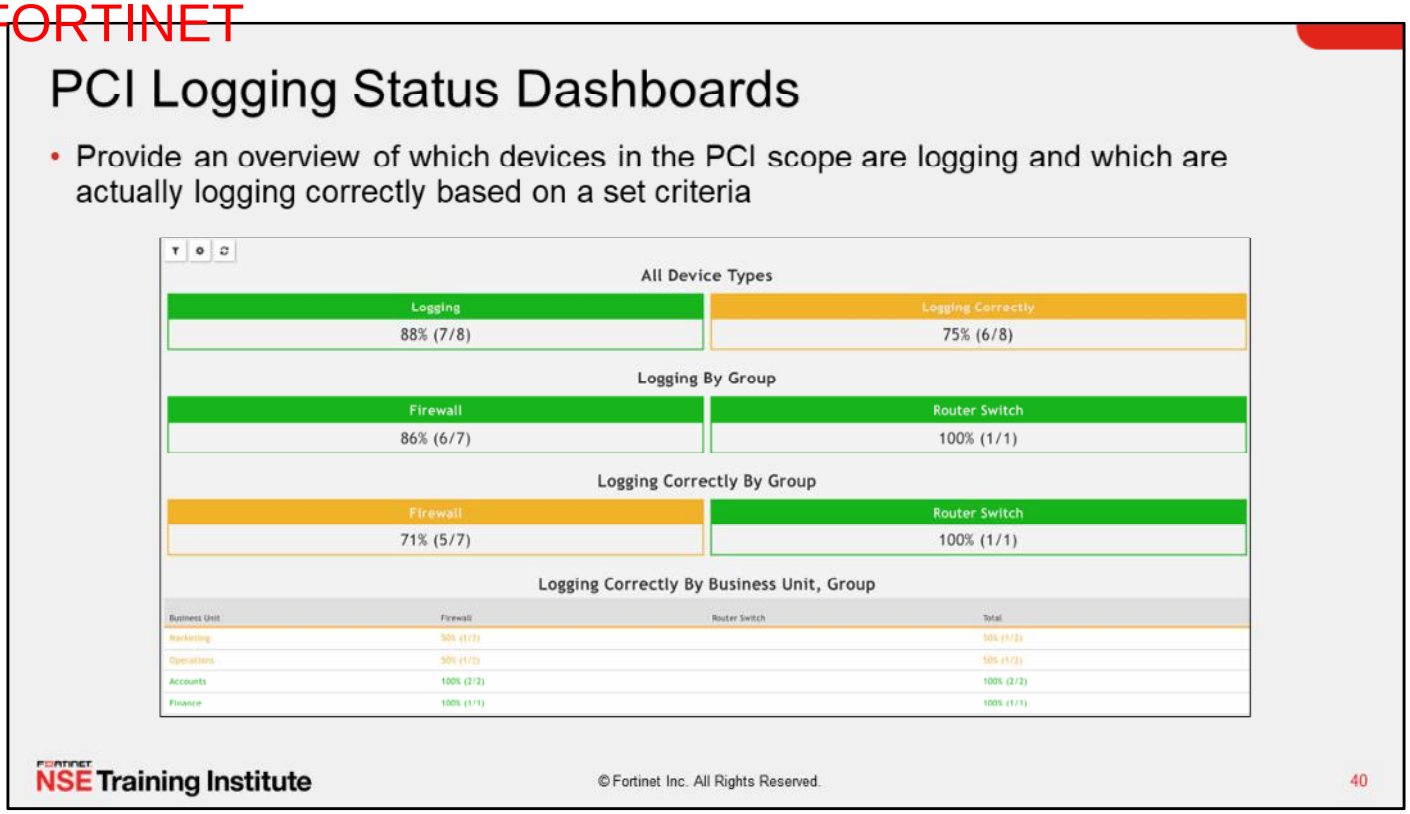
39

This dashboard provides an overview of the usage of individual interfaces of router and firewall devices. The dashboard has three levels:

- The upper view shows device level metrics in a tabular form.
- After you select a device in the upper view, the middle table shows the basic interface-level metrics, such as received and sent bytes.
- You can drill down and get application-level usage and QoS metrics for a specific device interface. To do this, select a device in the upper view and a specific interface in the middle view.

Vouchers & Dumps are Available | WhatsApp +201224560923

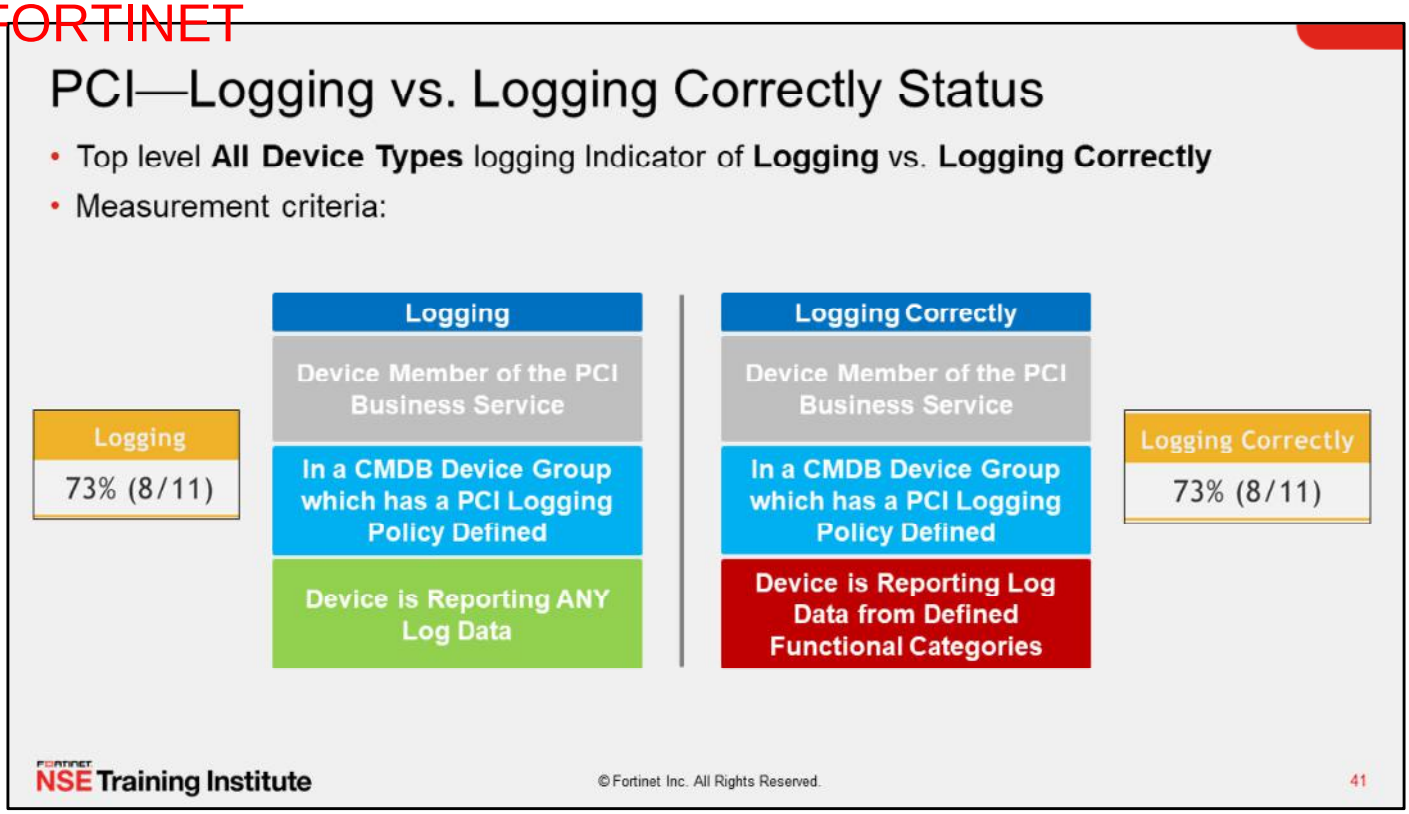
DO NOT REPRINT
© FORTINET
Brave-dumps.com



A PCI Logging Status dashboard provides an overview of which devices in PCI are logging and logging correctly. The devices are displayed by CMDB device groups (for example Windows, Linux, Firewalls, and so on) and by business units.

Vouchers & Dumps are Available | WhatsApp +201224560923

DO NOT REPRINT
© FORTINET
Brave-dumps.com

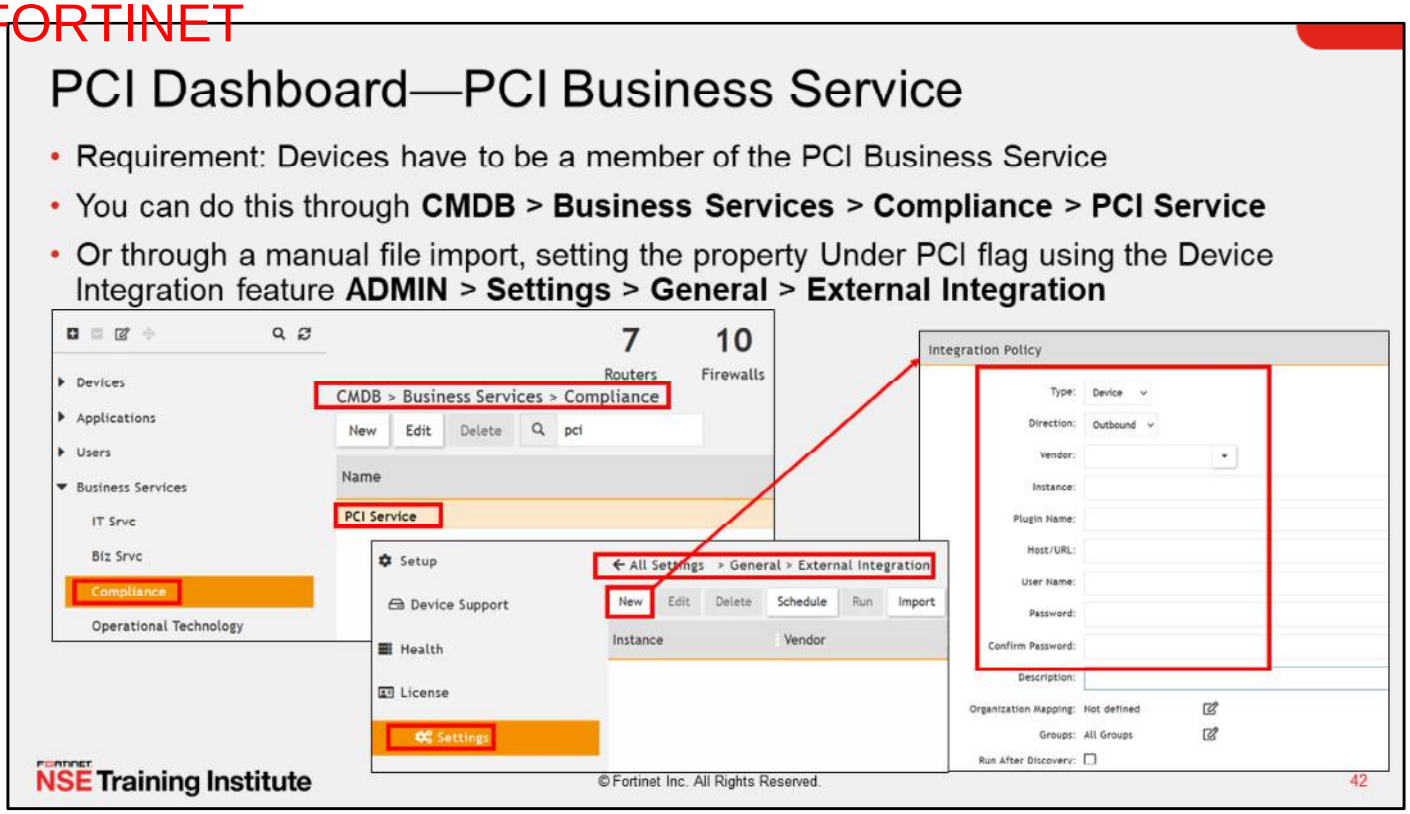


The PCI Logging Status Dashboard displays:

- **Logging**: Percentage of PCI devices logging within the time period **lastLogTimeLimit** (default 1 day)
- **Logging Correctly**: Percentage of PCI devices logging correctly

Vouchers & Dumps are Available | WhatsApp +201224560923

DO NOT REPRINT Brave-dumps.com
© FORTINET



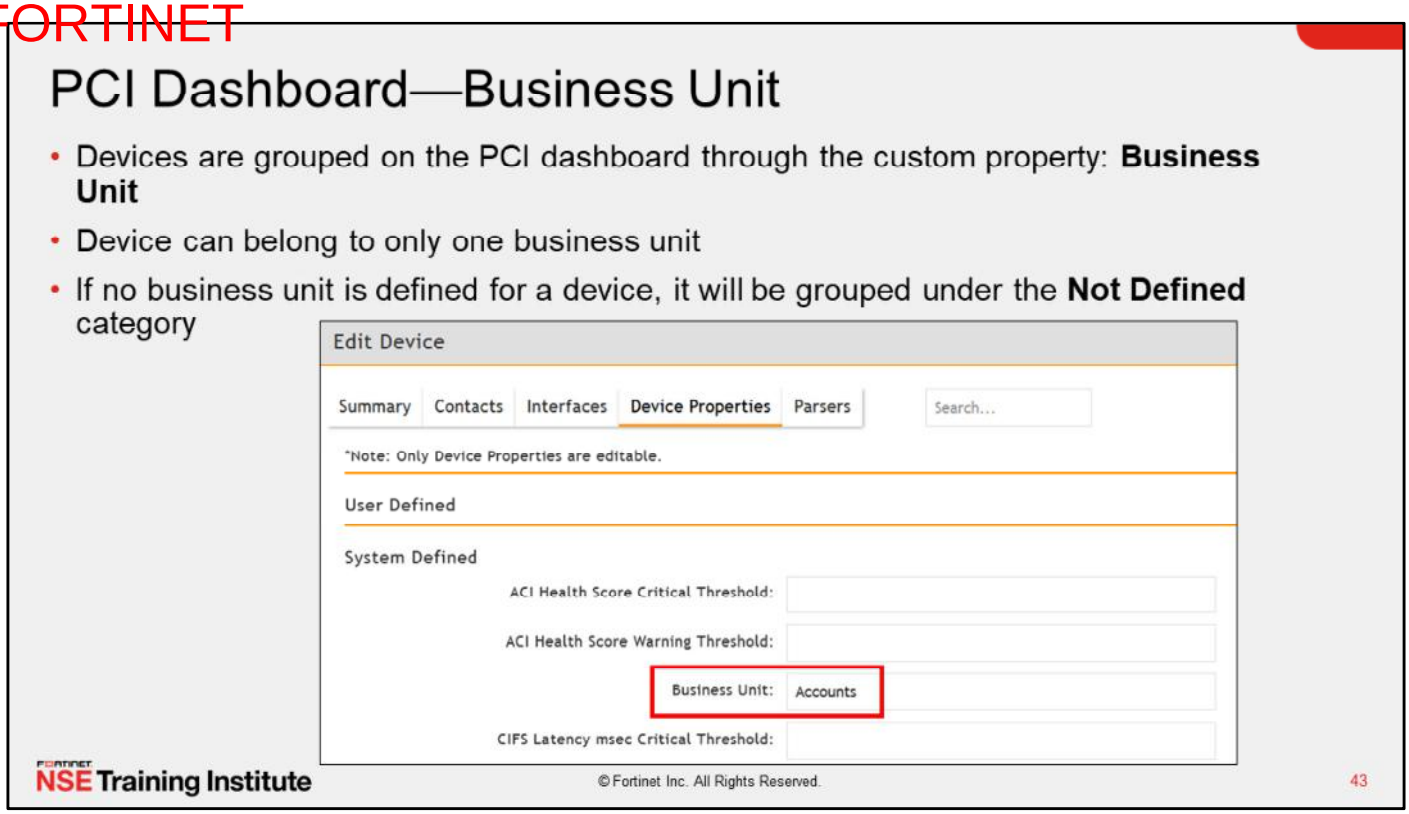
Devices on the PCI Logging Status Dashboard belong to the PCI Business Service. You can assign devices to the PCI Business Service in one of the following ways:

- Manually:
  a) Click **CMDB** > **Business Services** > **Compliance** > select the **PCI Service** > click **Edit** and add **Devices**.
  b) Click **Save**.

- Device import:
  a) Prepare a CSV file containing device host names and is PCI property. Host names must match the host names in the CMDB. The is PCI device property takes TRUE or FALSE values.
  b) Click **ADMIN** > **Settings** > **General** > **External Integration**.
  c) Click **New** and, in the **Type** drop-down list, select **Device**, and then, in the **Direction** drop-down list, select **Inbound**.
  d) Choose the **Host/URL** on the supervisor node, and then place the CSV file there.
  e) Click **Save**.
  f) Select the instance, and then click **Run**.

Vouchers & Dumps are Available | WhatsApp +201224560923

DO NOT REPRINT Brave-dumps.com
© FORTINET



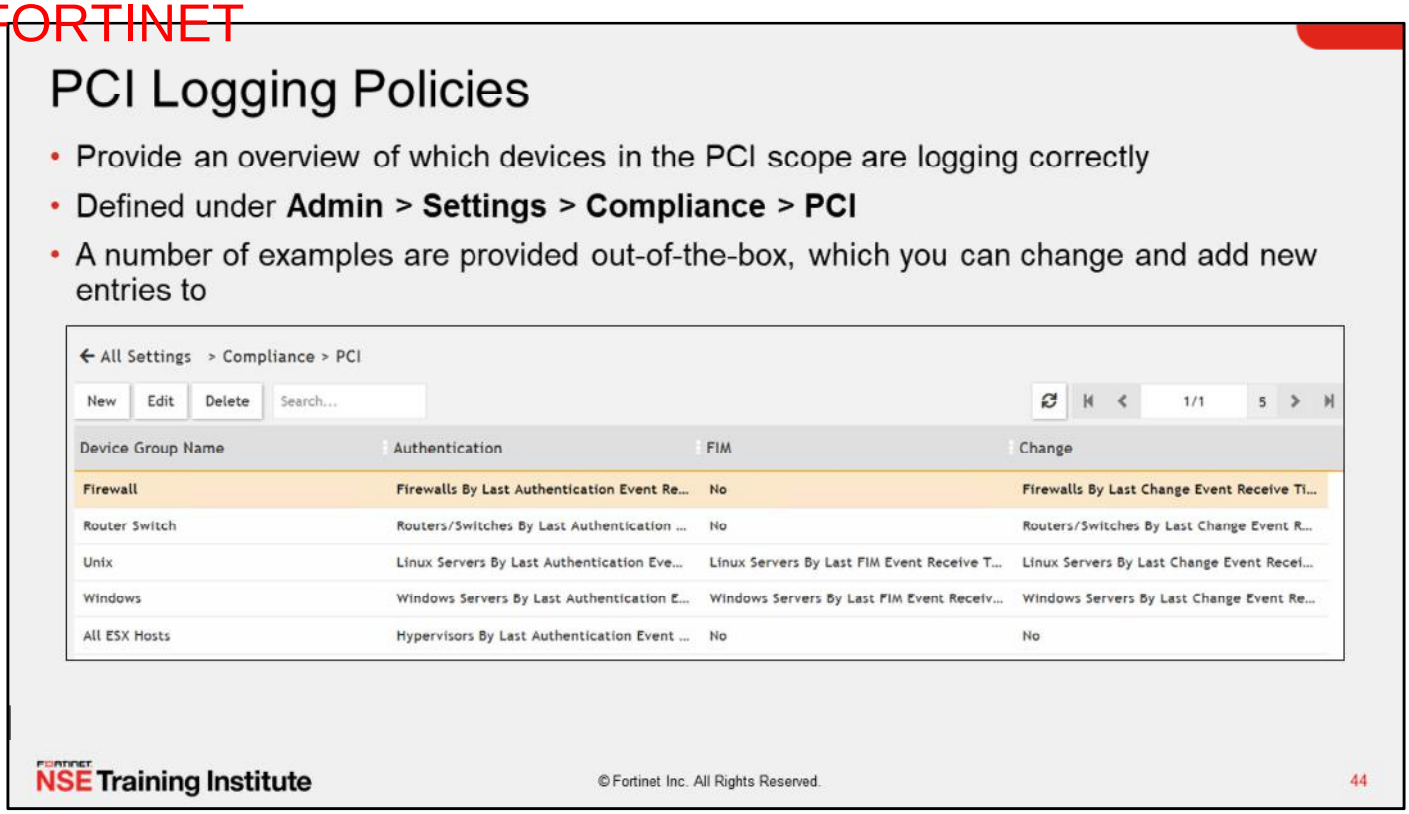
For the PCI Logging dashboard to display the devices logging and logging correctly by business units, the **Business Unit** property needs to be set for a device. You can do this in the following way:

a) Click **CMDB**, and then select one or more devices.
b) Click **Edit**, select **Device Properties**, and then set the **Business Unit**.

Devices can belong to only to one business unit. If no business unit is defined for a device, it is grouped under the **Not Defined** category.

Vouchers & Dumps are Available | WhatsApp +201224560923

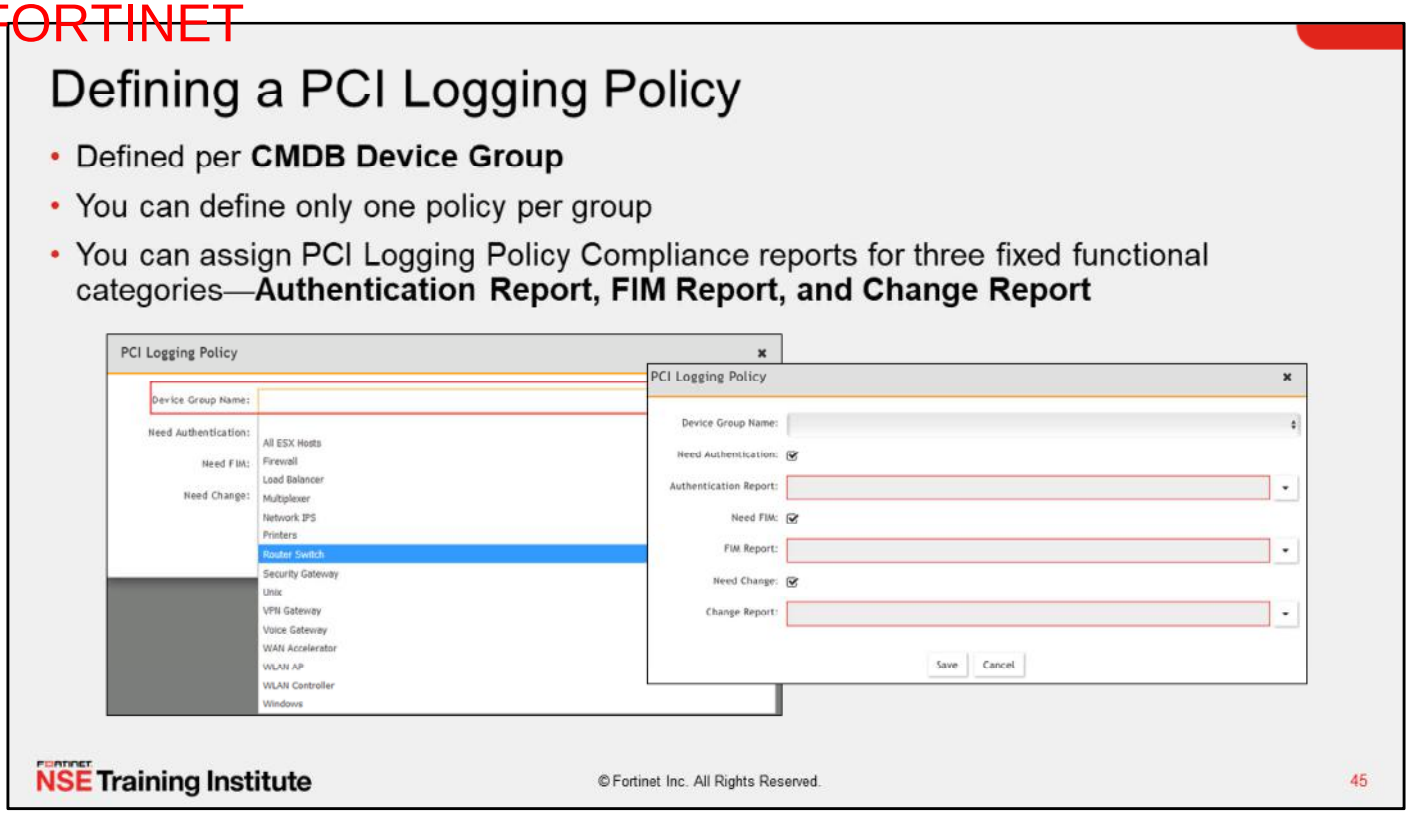
DO NOT REPRINT
© FORTINET
Brave-dumps.com



PCI logging policies specify whether a CMDB device group needs to correctly send logs in the various functional categories—Authentication, FIM, and Change. Currently, these three functional categories are fixed. You can specify PCI logging policies in **ADMIN** > **Settings** > **Compliance** > **PCI**. Several PCI logging policies are predefined, which you can change and add new entries to.

Vouchers & Dumps are Available | WhatsApp +201224560923

DO NOT REPRINT
© FORTINET
Brave-dumps.com



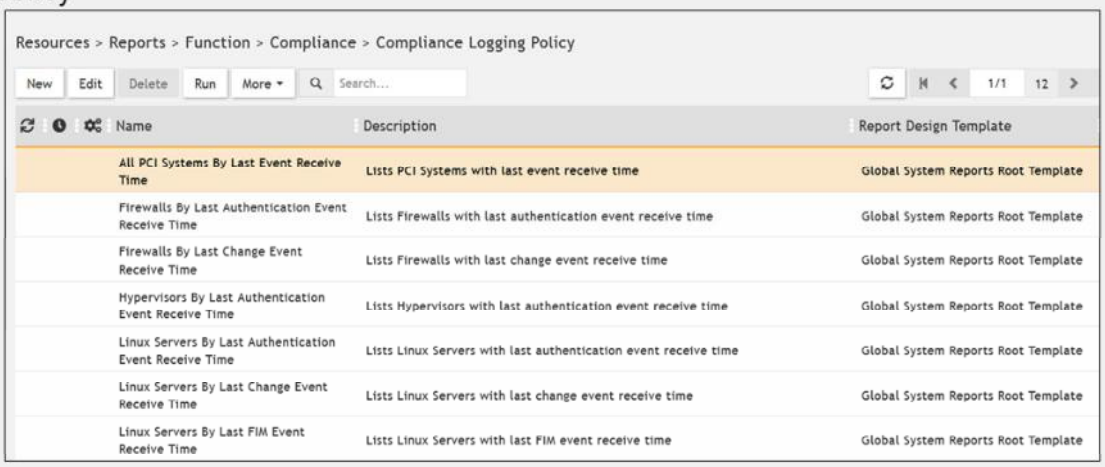
While defining a PCI logging policy, you must select a device group. You can define only one policy per group. You can assign PCI Logging Policy Compliance reports for three fixed functional categories—**Authentication Report**, **FIM Report**, and **Change Report**.

Vouchers & Dumps are Available | WhatsApp +201224560923

DO NOT REPRINT
© FORTINET
Brave-dumps.com

PCI Compliance Logging Policy Reports

- Defined under **Resources > Reports > Function > Compliance > Compliance Logging Policy**
- You must define a report in this location, or else it is not available for selection through the policy



NSE Training Institute

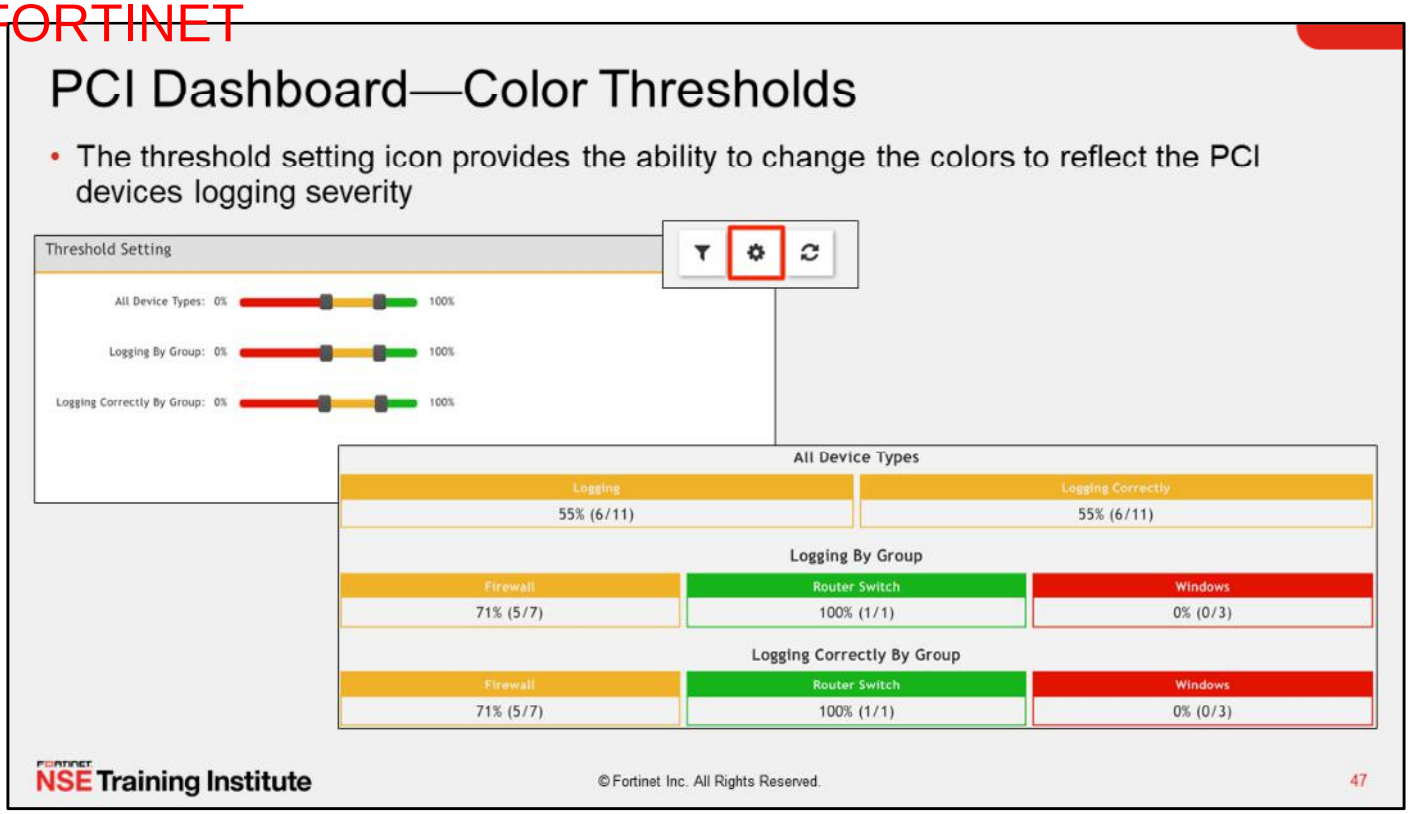
© Fortinet Inc. All Rights Reserved.

46

You can define PCI compliance logging policy reports by clicking **Resources** > **Reports** > **Function** > **Compliance** > **Compliance Logging Policy**. These reports specify the criteria for devices in a device group to be correctly logging Authentication, FIM, and change events.

Vouchers & Dumps are Available | WhatsApp +201224560923

DO NOT REPRINT
© FORTINET
Brave-dumps.com



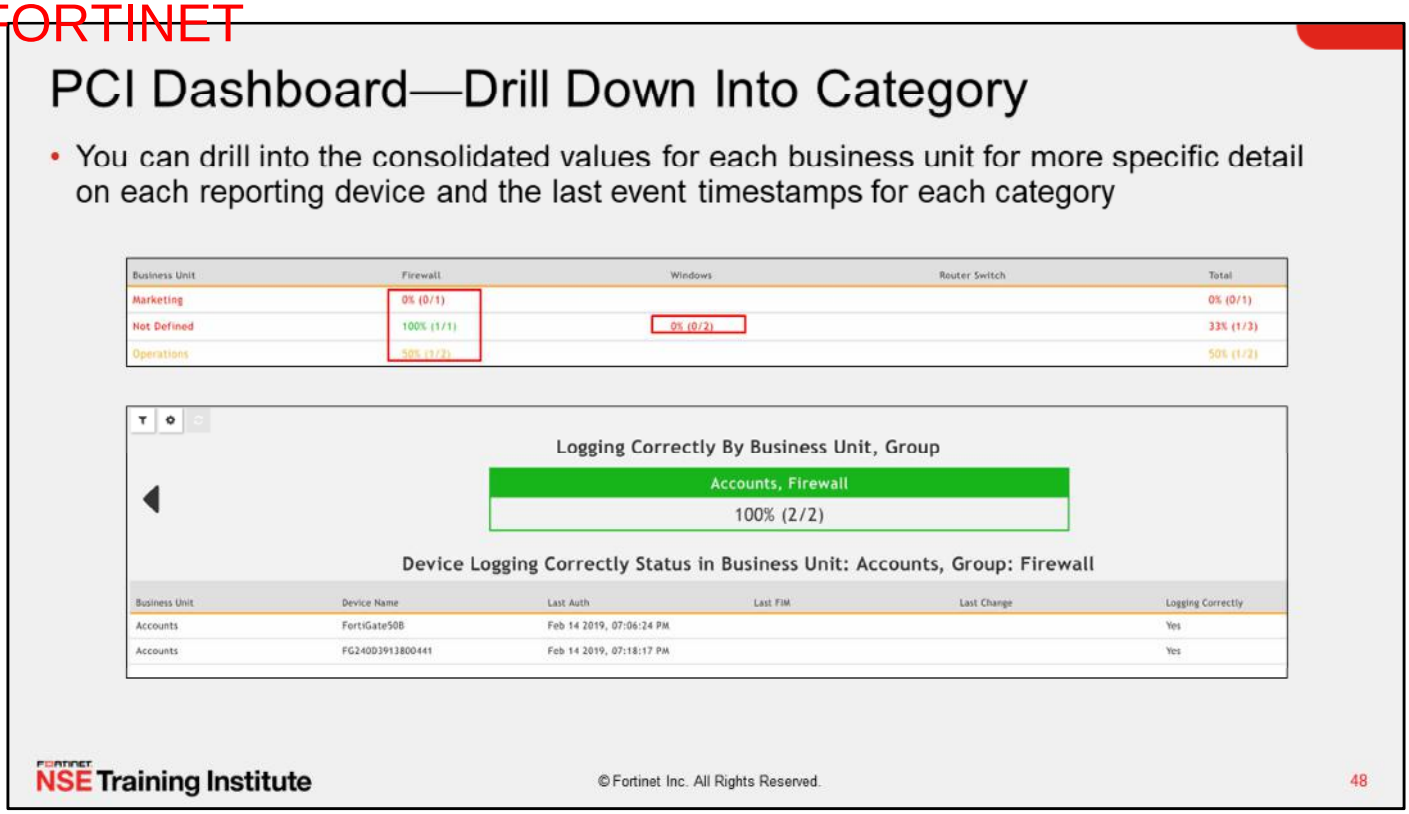
The threshold setting icon provides the ability to change the colors to reflect the PCI devices logging severity. The displays are color coded as red, yellow, and green according to the tunable thresholds defined in **Dashboard** > **Threshold Setting**. By default:

- Red – less than 50%
- Yellow – between 50% and 80%
- Green – higher than 80%

If you click the entries, the devices in violation are shown in a tabular format along with the last time they reported events in each category.

Vouchers & Dumps are Available | WhatsApp +201224560923

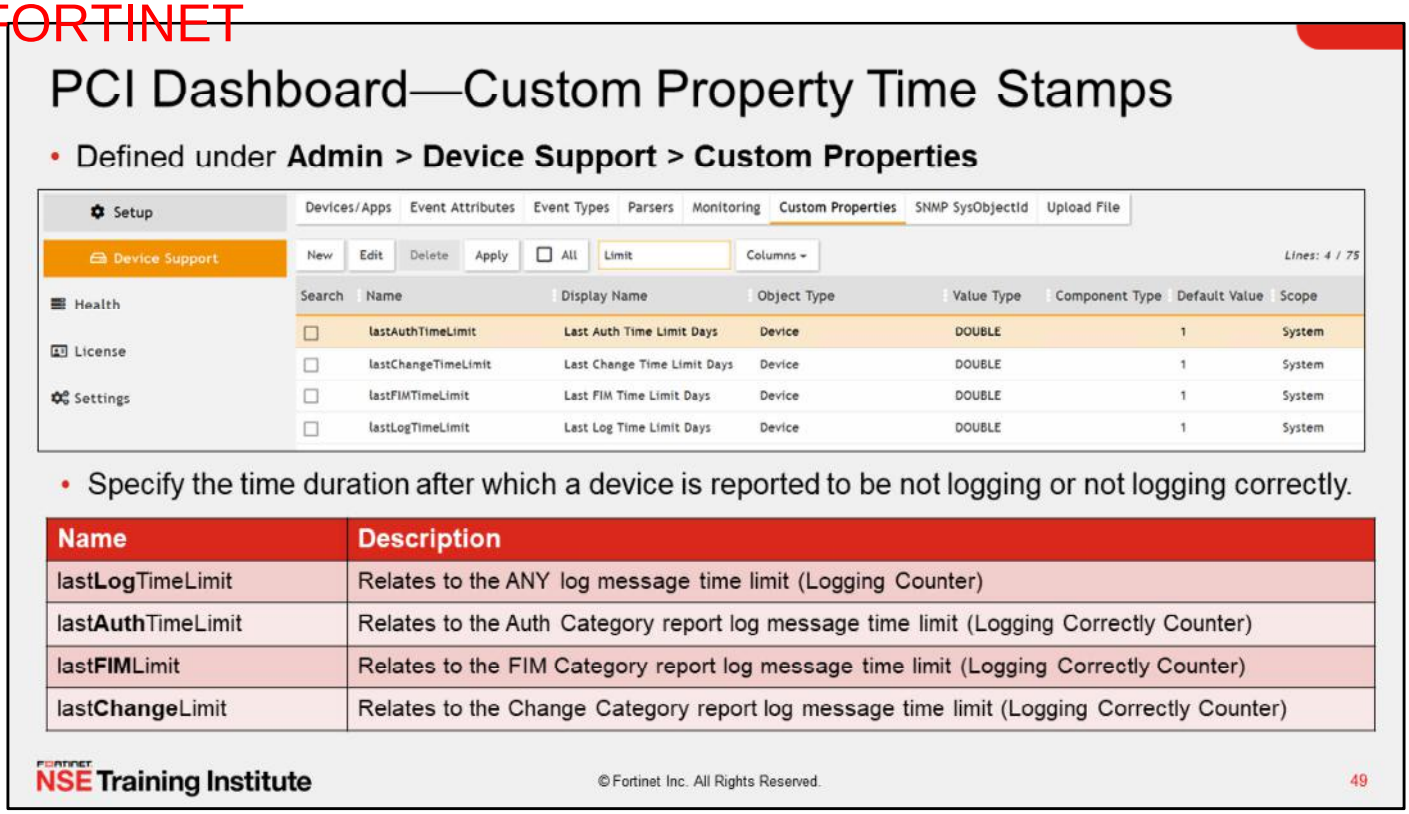
DO NOT REPRINT
© FORTINET
Brave-dumps.com



You can drill into the consolidated values for each business unit for more specific detail on each reporting device and the last event timestamps for each category.

Vouchers & Dumps are Available | WhatsApp +201224560923

DO NOT REPRINT
© FORTINET
Brave-dumps.com



Specify the time duration after which a device is reported to be not logging or not logging correctly. You define four properties in **ADMIN** > **Device Support** > **Custom Properties**:

- **lastAuthTimeLimit** - time limit for authentication logs (default 1 day)
- **lastFIMTimeLimit** - time limit for FIM logs (default 1 day)
- **lastChangeTimeLimit** - time limit for authentication log (default 1 day)
- **lastLogTimeLimit** - time limit for sending any log (default 1 day)

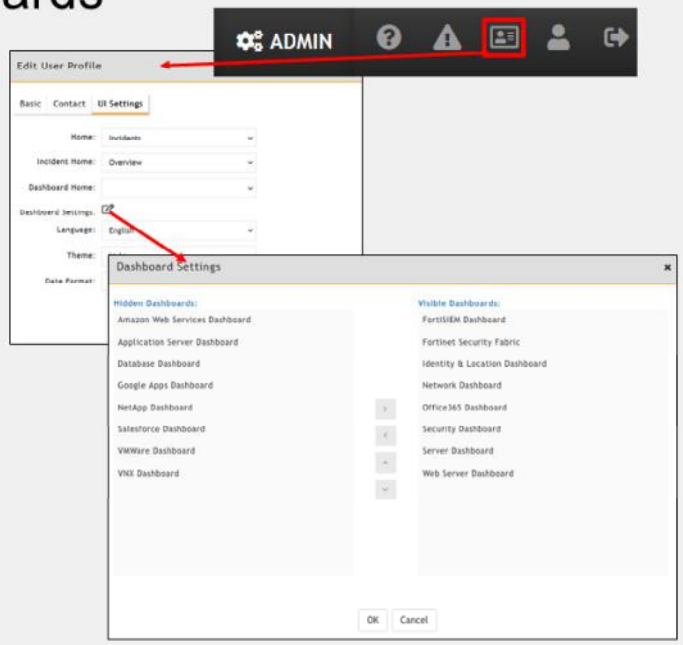
Similar to any other device property, you can change the global defaults and set them on a per-device basis.

Vouchers & Dumps are Available | WhatsApp +201224560923

DO NOT REPRINT Brave-dumps.com
© FORTINET

Hiding Unwanted Dashboards

- Not all customers use the same products and so some of the out-of-the-box dashboards provide no value
- Therefore the **Dashboard Settings** option under **User Profile** icon > **UI Settings** provides the ability to hide unwanted default or user-created dashboards
- This setting relates to the logged-in user



NSE Training Institute

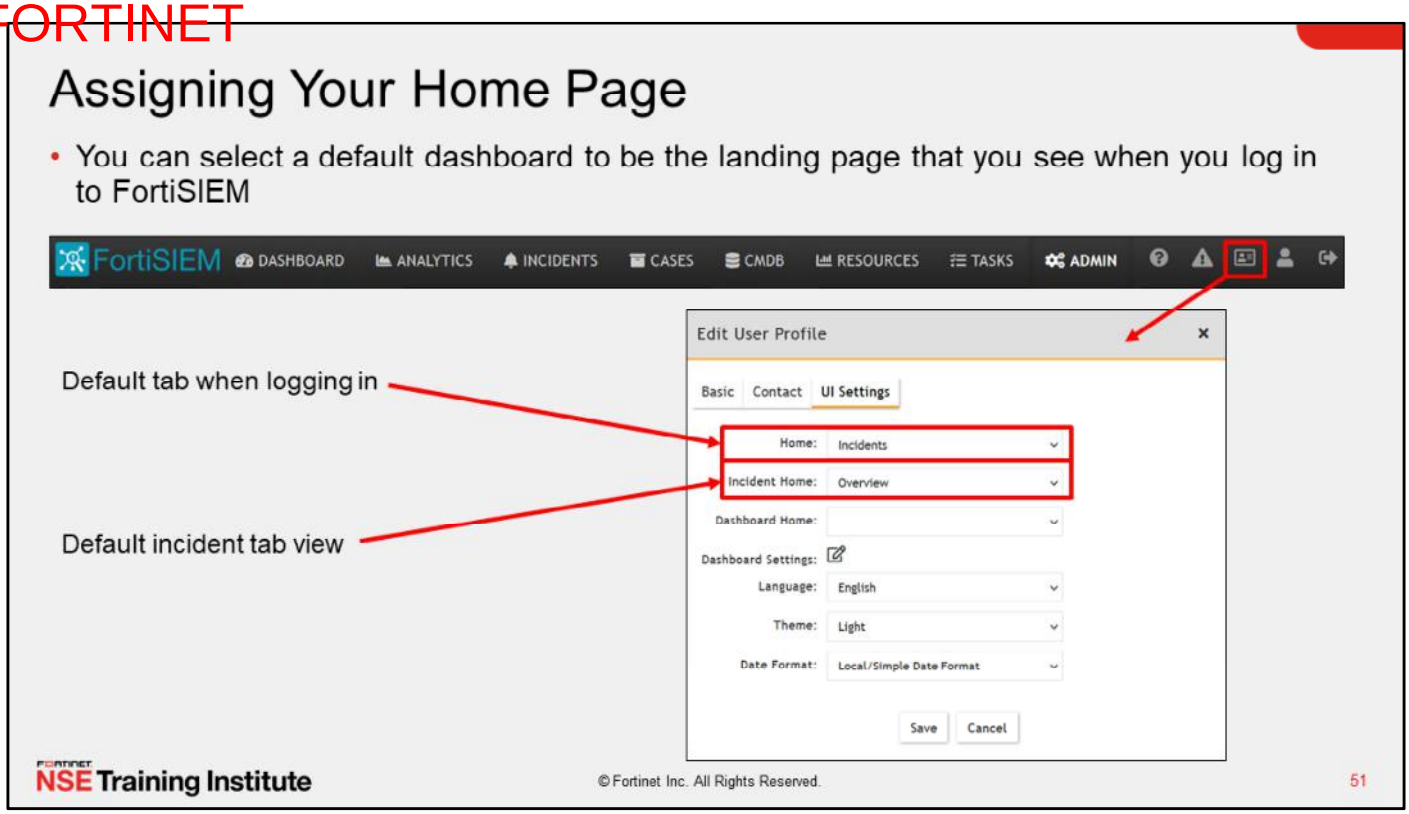
© Fortinet Inc. All Rights Reserved.

50

Not every customer uses the same products, and so some of the out-of-the-box dashboards provide no value. You can hide those dashboards by modifying the **Dashboard Settings** option under **User Profile** icon > **UI Settings** . This setting relates to the logged-in user.

Vouchers & Dumps are Available | WhatsApp +201224560923

DO NOT REPRINT
© FORTINET
Brave-dumps.com

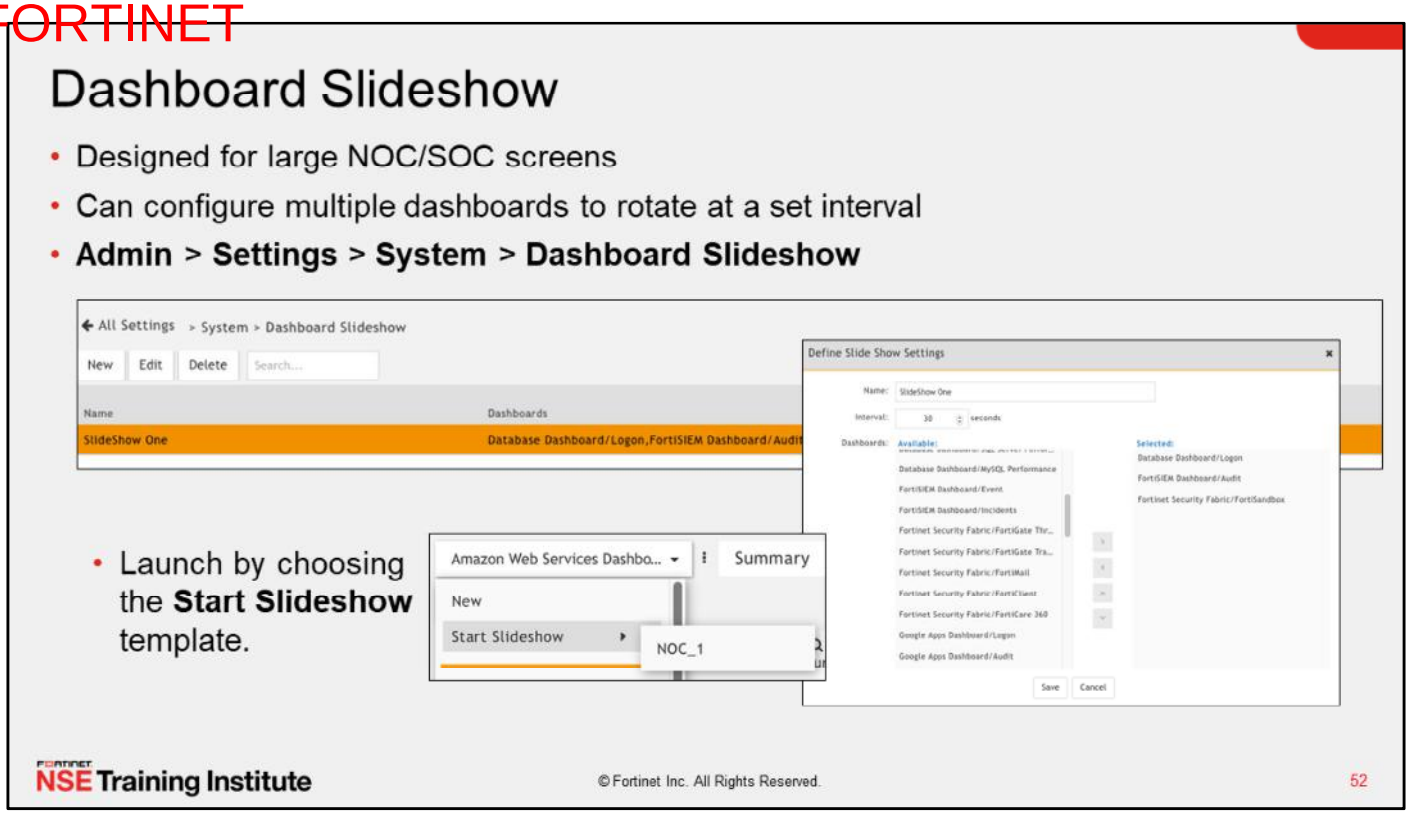


You can select a default dashboard to be the landing page that you see when you log in to FortiSIEM.

To do this, click the **User Profile** icon > **UI Settings** > and then select the **Home** that you want to use as your home page. **Save** your settings, and the next time you log in, the first dashboard you see is the one that you selected as the home page.

Vouchers & Dumps are Available | WhatsApp +201224560923

DO NOT REPRINT
© FORTINET
Brave-dumps.com



Use **Dashboard Slide Show Settings** to select a set of dashboards and display them in a slideshow mode on big monitors to cover the entire display. This is useful for network and security operation centers. You can configure multiple dashboards to rotate at a set interval, and launch the slideshow by selecting **Start Slideshow** template.

Vouchers & Dumps are Available | WhatsApp +201224560923

DO NOT REPRINT
© FORTINET
Brave-dumps.com

Knowledge Check

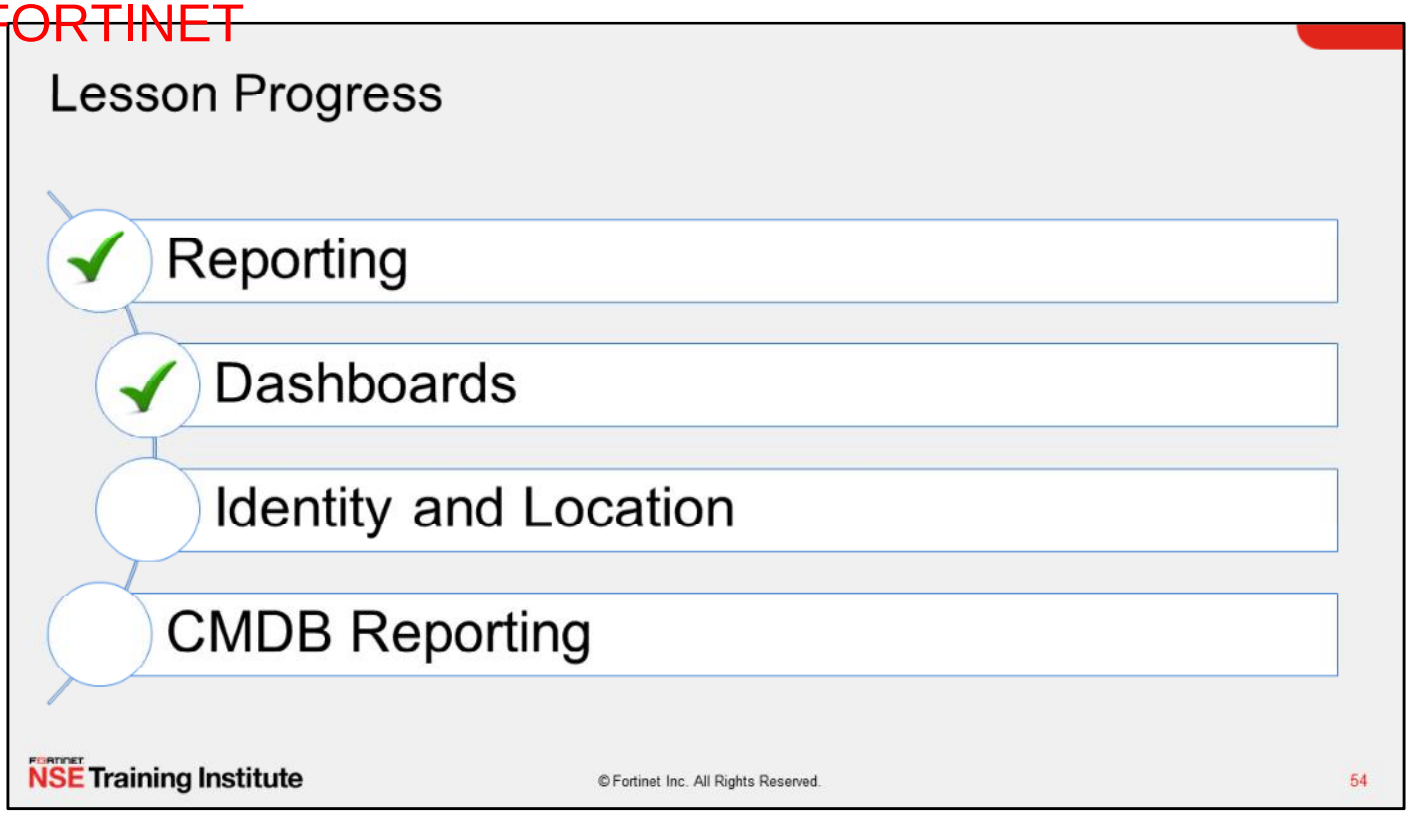
1. If the reported packet loss is between 50% and 98%, which status is assigned to the device in the **Available** column of the summary dashboard?

✓A. Degraded
B. Up
C. Down

NSE Training Institute
© Fortinet Inc. All Rights Reserved.
53

Vouchers & Dumps are Available | WhatsApp +201224560923

DO NOT REPRINT
© FORTINET
Brave-dumps.com

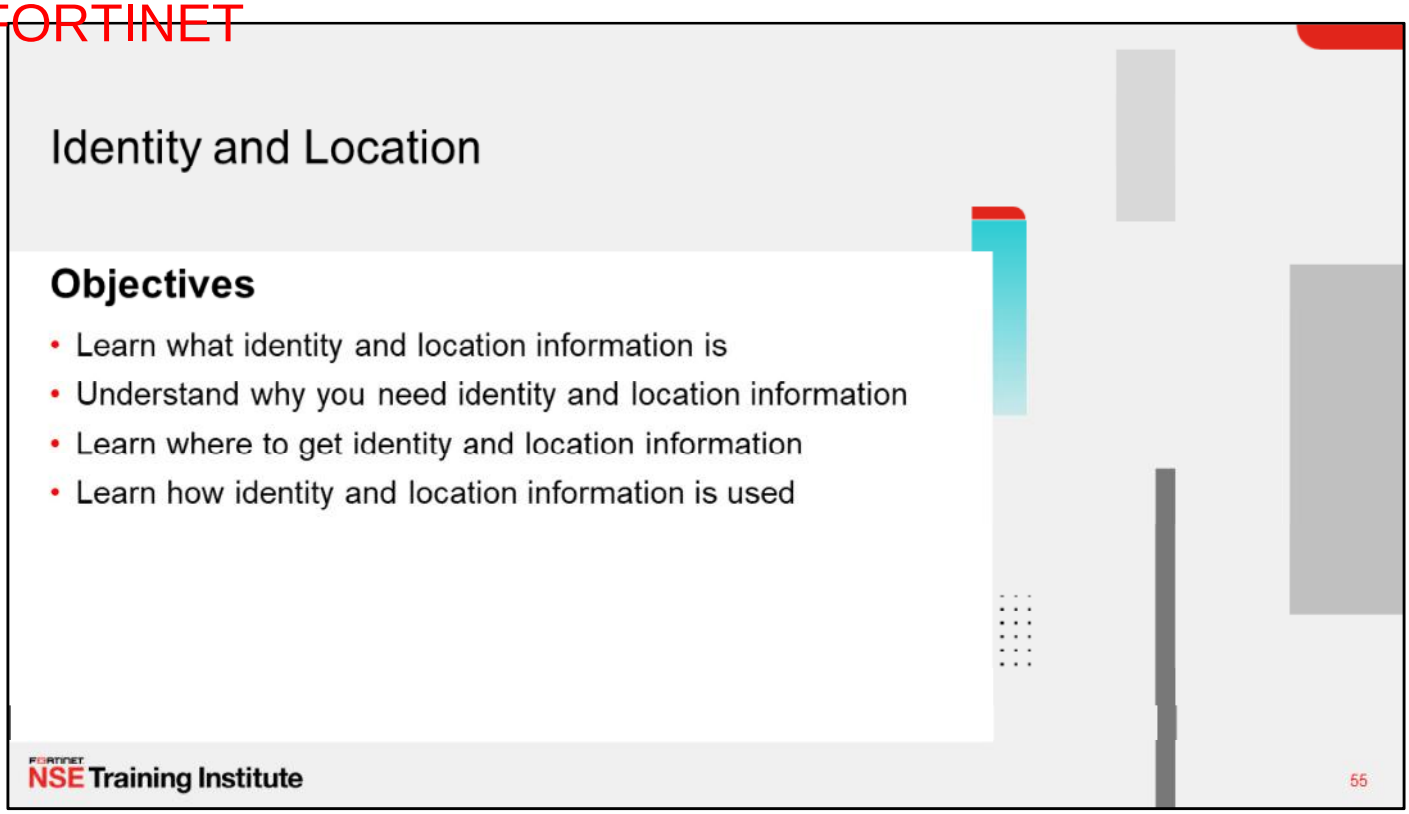


Good job! You now understand dashboards.

Now, you will learn about identity and location.

Vouchers & Dumps are Available | WhatsApp +201224560923

DO NOT REPRINT
© FORTINET
Brave-dumps.com

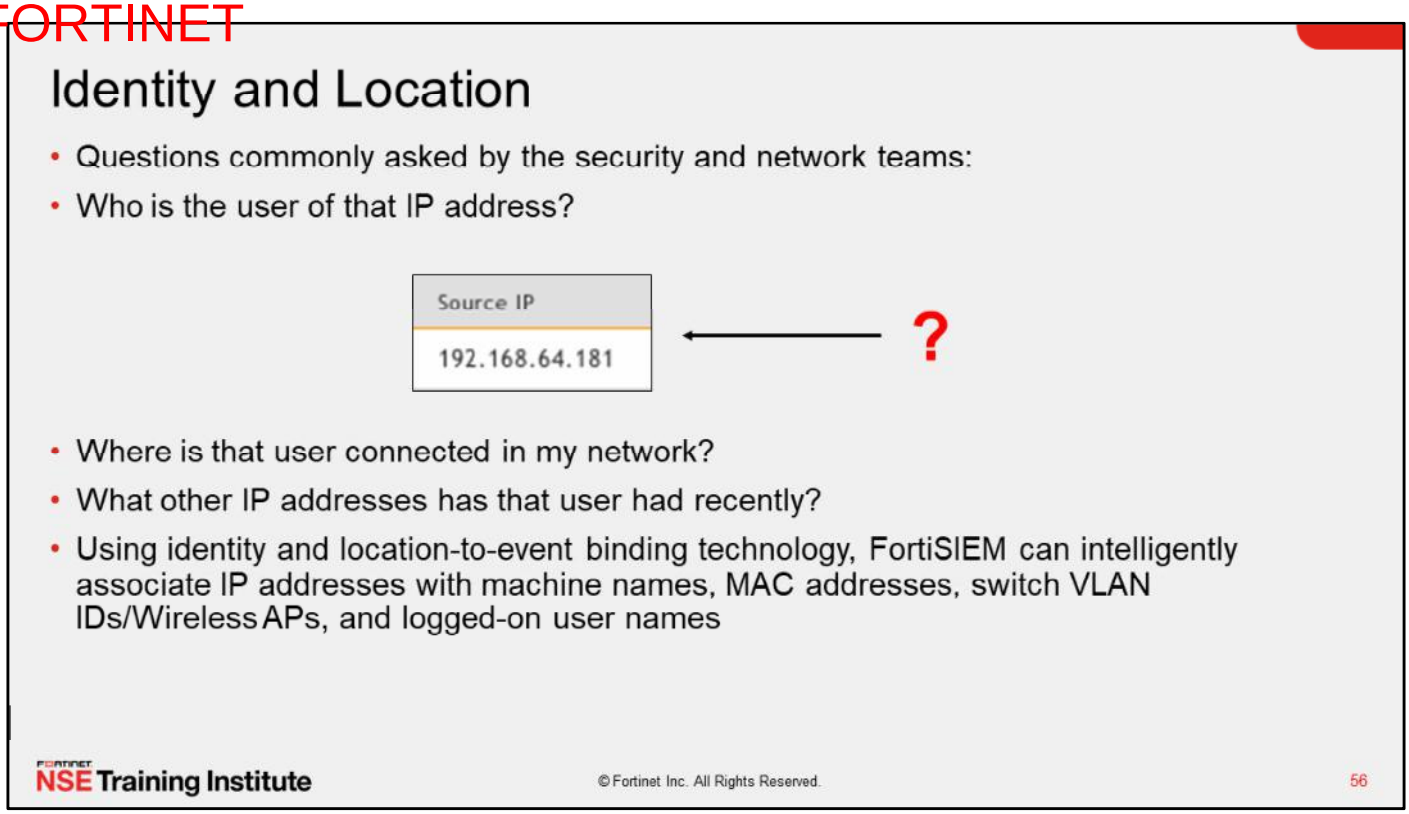


After completing this section, you should be able to achieve the objectives shown on this slide.

By demonstrating competence in understanding location and identity information, you will be able to use it effectively in managing your network.

Vouchers & Dumps are Available | WhatsApp +201224560923

DO NOT REPRINT
© FORTINET
Brave-dumps.com



There are some questions commonly asked by security and network teams.

Who is the user of that IP address?

- Maybe there has been a virus alert, or maybe you have seen a particular source going to a particular destination or a certain country

Where is that user connected in my network?

- Are they a wireless user?
- Are they connected to a particular switch port?

What other IP addresses has that user had recently?

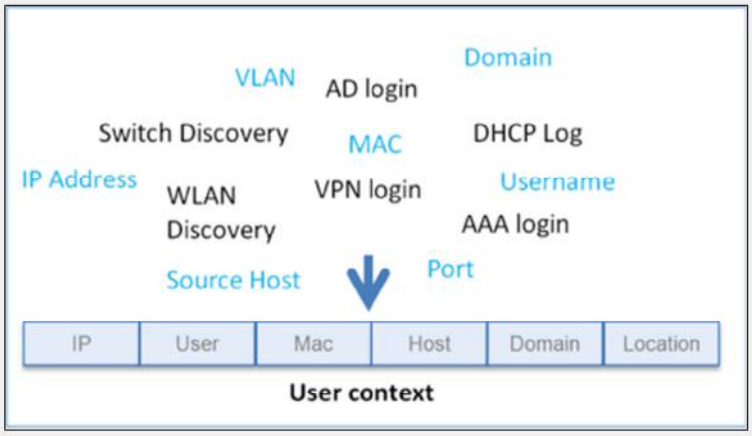
Using identity and location event binding technology, FortiSIEM can intelligently associate IP addresses with machine names, MAC addresses, switch VLAN IDs, wireless access points, and logged on user names, and saves them in the identity and location report.

Vouchers & Dumps are Available | WhatsApp +201224560923

DO NOT REPRINT
© FORTINET
Brave-dumps.com

Identity and Location Information Sources

- Identity and location requires multiple sources of information to successfully build a user context
- Example information sources:
  - Switch/WLAN discoveries
  - DHCP logs
  - Active Directory login events
  - VPN logs
  - AAA logs



- This data is correlated in memory and stored in the identity and location report

NSE Training Institute

© Fortinet Inc. All Rights Reserved.

57

Identity and location requires multiple sources of information to be successful and build up what is referred to as a user context.

User context is a user's information sources, including:

- Switch/VLAN discoveries
- DHCP events
- Active Directory login events
- VPN logs
- AAA logs

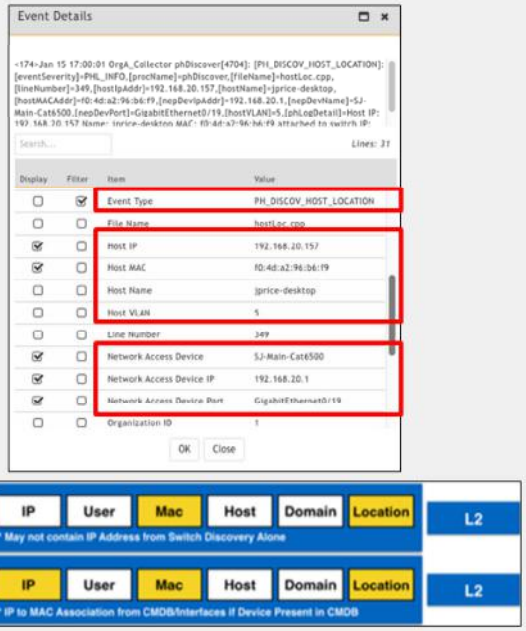
This data is correlated in memory and then stored in the identity and location report. FortiSIEM can then reference this information later when performing other tasks, such as enriching user-related fields when parsing events.

Vouchers & Dumps are Available | WhatsApp +201224560923

DO NOT REPRINT
© FORTINET
Brave-dumps.com

Layer 2 Discovery

- Layer 2 switch discovery contains useful information, such as the MAC address associated with a particular port and the VLAN
- If a device is already present in the CMDB and has had a full GUI discovery, the interface table contains an IP address that corresponds with the MAC address of the device
- This information comes from a **PH_DISCOV_HOST_LOCATION** event



NSE Training Institute

© Fortinet Inc. All Rights Reserved.

58

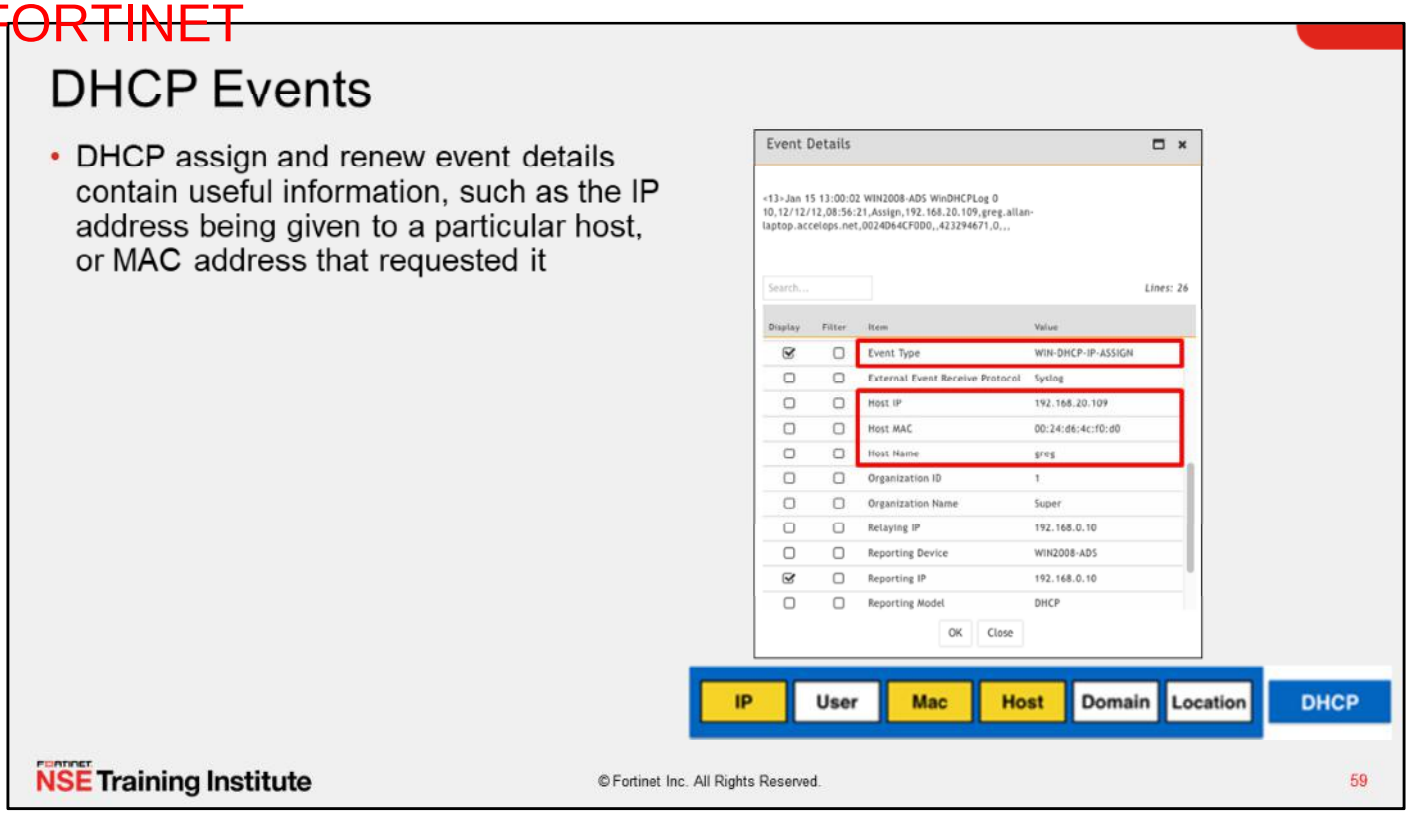
When a Layer 2 switch is discovered, FortiSIEM collects useful information, such as the MAC addresses associated with a particular port and VLAN. This information comes from a PH_DISCOV_HOST_LOCATION event.

If the device is already present in the CMDB, and has had a full GUI discovery, the interface table contains an IP address for that device, along with the corresponding MAC address.

From an identity perspective, if you look at the information required for a full user context, you don't have all the pieces. All you have is a MAC address and a location (meaning a switch port) for that MAC address, and, perhaps, an IP address.

Vouchers & Dumps are Available | WhatsApp +201224560923

DO NOT REPRINT
© FORTINET
Brave-dumps.com



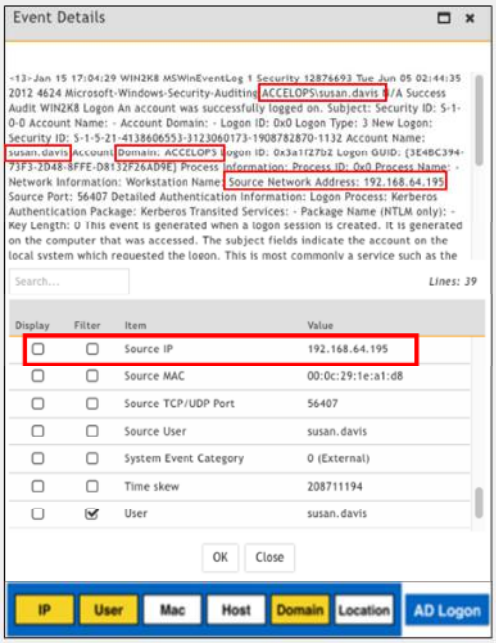
The DHCP assign and renew events also contain useful information, such as the IP address given to a particular host, or the MAC address that requested it. Again, the DHCP events alone won't give you all the information you need to create a user context, but it will provide an IP address, a MAC address, and a host name.

Vouchers & Dumps are Available | WhatsApp +201224560923

DO NOT REPRINT
© FORTINET
Brave-dumps.com

Windows AD Events

- Windows AD login event details contain the IP address, user, and domain of the user performing an authentication



NSE Training Institute

© Fortinet Inc. All Rights Reserved.

60

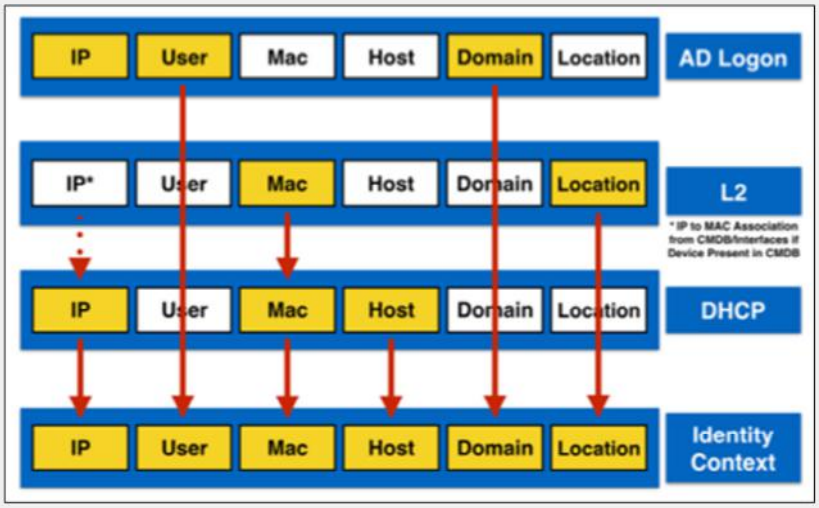
Windows Active Directory (AD) login events contain the IP address, user, and domain of the user performing an authentication to the network. But again, from an identity context perspective, it doesn't give you all of the details required for a user context.

Vouchers & Dumps are Available | WhatsApp +201224560923

DO NOT REPRINT
© FORTINET
Brave-dumps.com

Putting It All Together

- The event information is correlated and kept up-to-date in FortiSIEM memory to give a full user-identity context



NSE Training Institute

© Fortinet Inc. All Rights Reserved.

61

Now, put them all together!

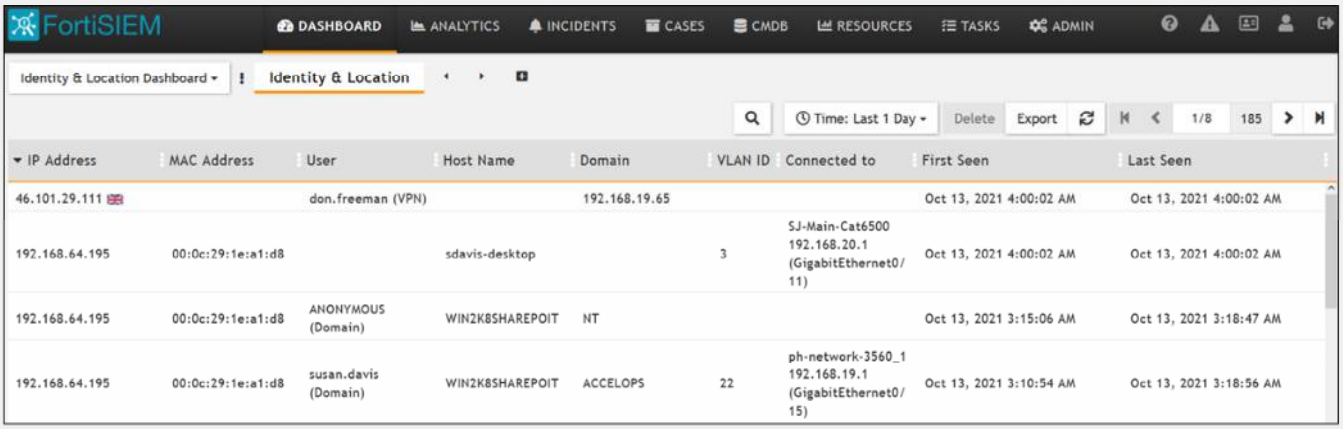
FortiSIEM correlates all the event information in memory and keeps it up-to-date to give you a full user identity context. By taking the various fields out of each of the different events, FortiSIEM can complete a full identity context for each user, and save it in an **Identity and Location Report**.

Vouchers & Dumps are Available | WhatsApp +201224560923

DO NOT REPRINT Brave-dumps.com
© FORTINET

After Configuration

- After the identity and location table is created, instant context is available in the FortiSIEM GUI



NSE Training Institute

© Fortinet Inc. All Rights Reserved.

62

After you have fully created identity and location, this information is available on the FortiSIEM GUI.
In the **Dashboard** section, the **Identity & Location Dashboard** in the dashboard type drop-down list on the left side allows you to search for specific users, IP addresses, MAC address, and location.

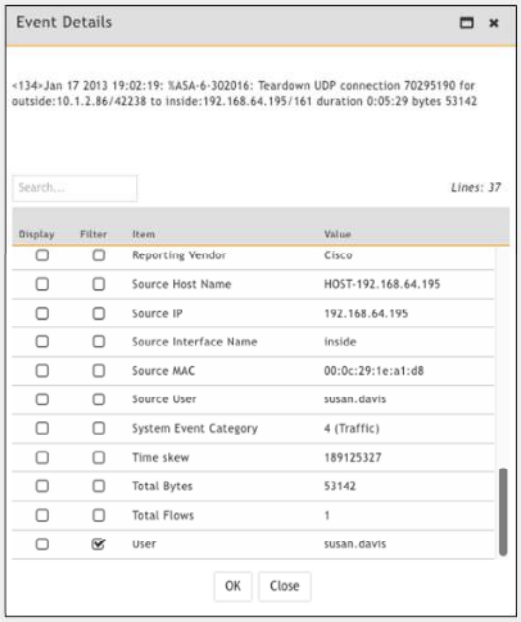
Identity and location dashboards provide a tabular view of network-identity to user-identity mappings.

Vouchers & Dumps are Available | WhatsApp +201224560923

DO NOT REPRINT
© FORTINET
Brave-dumps.com

After Configuration—User Parsing

- Incoming events that reference an IP entry in the **Identity & Location Dashboard** table is enriched with user information
- In this example **Raw Event Log** contains an internal IP address, but no user information
- But, in the structured data, the **User, Source Host Name**, and **Source MAC** fields are enriched by the parser because this IP is in the **Identity & Location** table



NSE Training Institute

© Fortinet Inc. All Rights Reserved.

63

Any incoming events that reference an IP address that has an entry in the **Identity & Location Dashboard** table is enriched with user information.

For example, the **Raw Event Log** references an internal IP address, but there is no user information in the log itself. But, if the IP address is in the **Identity& Location** table, then the parsing engine enriches this event with the **User**, **Source Host Name**, and **Source MAC** fields, as you can see in the example structured data produced after parsing.

After you have this information from the parser, you can reference those fields in reports, for example, to determine where user Susan Davis has connected from today.

Vouchers & Dumps are Available | WhatsApp +201224560923

DO NOT REPRINT
© FORTINET
Brave-dumps.com

Knowledge Check

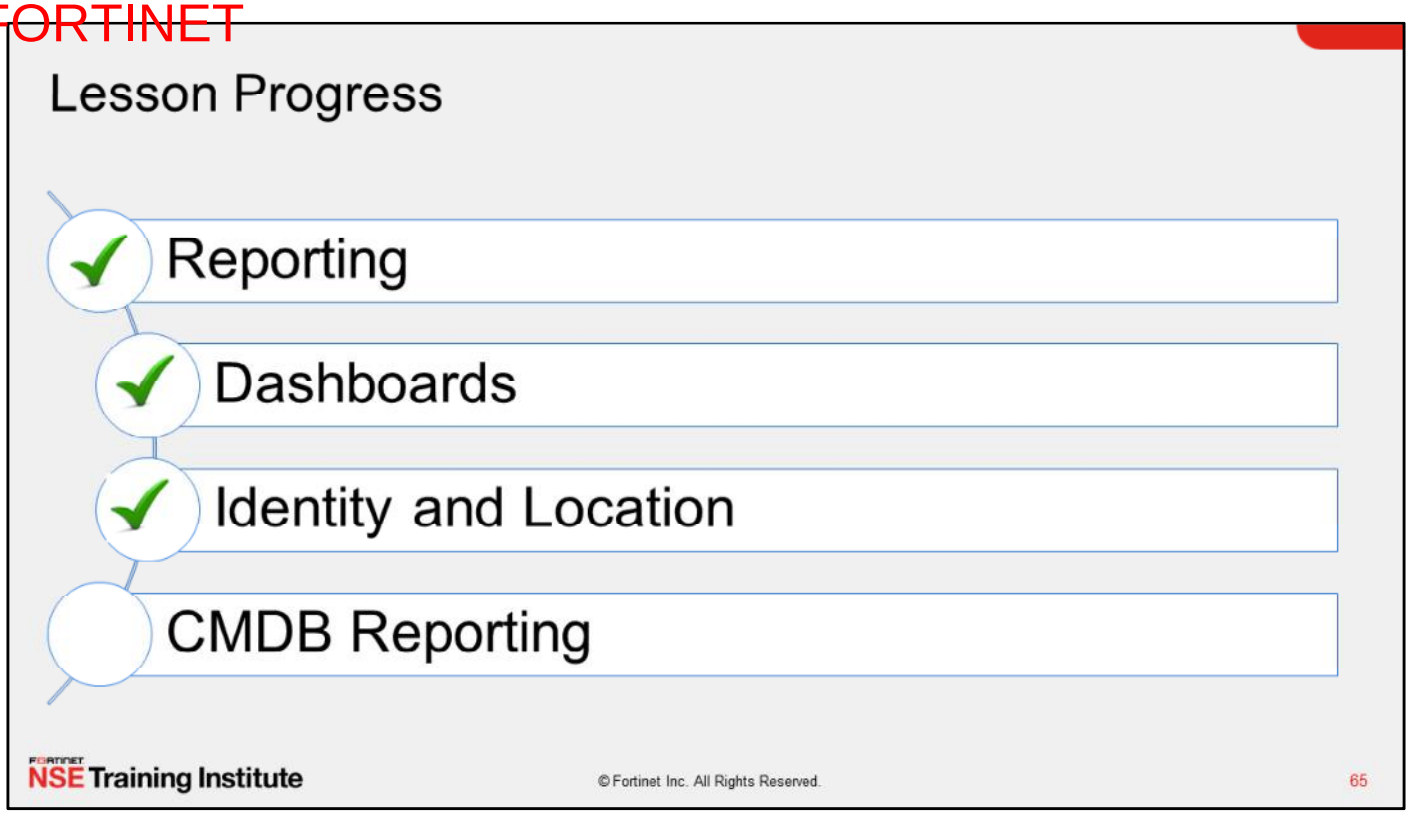
1. Which FortiSIEM event types collects useful information, such as the MAC addresses associated with a particular port and VLAN?

✓A. PH_DISCOV_HOST_LOCATION
B. PH_DEV_MON_PING_STAT
C. WIN-DHCP_IP_ASSIGN

NSE Training Institute
© Fortinet Inc. All Rights Reserved.
64

Vouchers & Dumps are Available | WhatsApp +201224560923

DO NOT REPRINT
© FORTINET
Brave-dumps.com

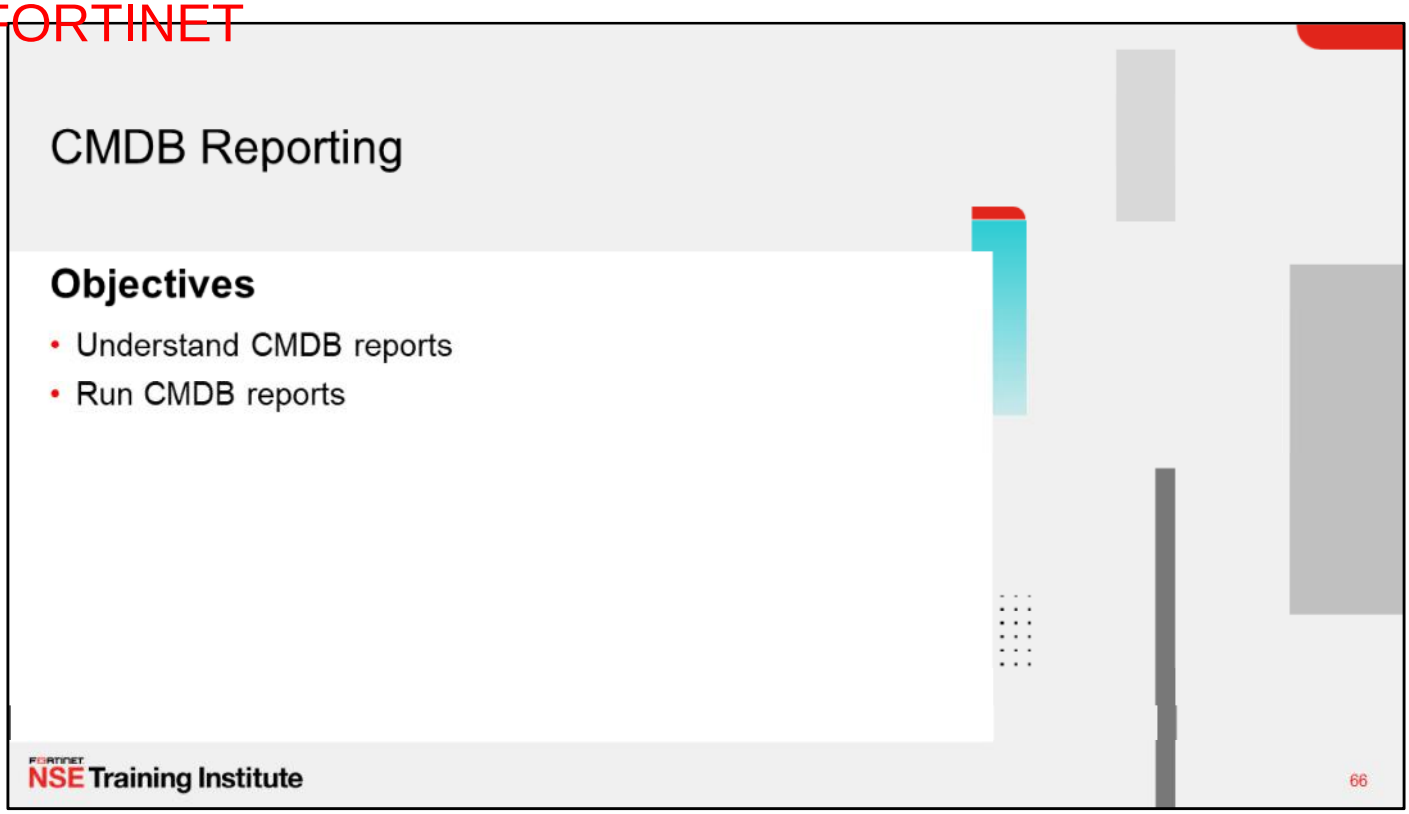


Good job! You now understand identity and location information.

Now, you will learn about configuration management database (CMDB) reporting.

Vouchers & Dumps are Available | WhatsApp +201224560923

DO NOT REPRINT
© FORTINET
Brave-dumps.com



After completing this section, you will be able to achieve the objectives shown on this slide.

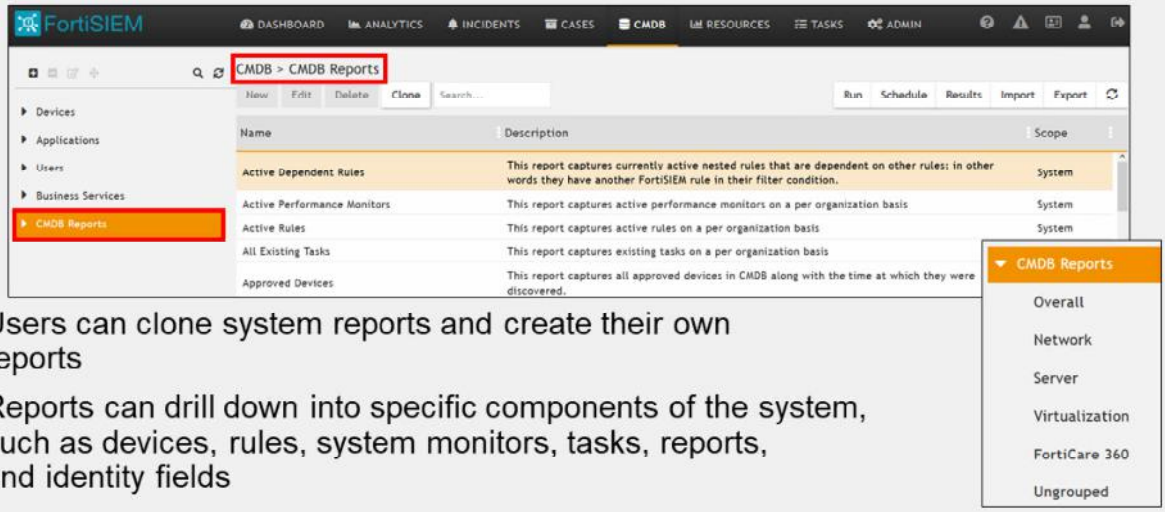
By demonstrating competence in CMDB reports, you will be able to understand and run them as part of managing your network.

Vouchers & Dumps are Available | WhatsApp +201224560923

DO NOT REPRINT
© FORTINET
Brave-dumps.com

CMDB Reports

- Feature contains a number of predefined system reports related to the contents of the CMDB



- Users can clone system reports and create their own reports
- Reports can drill down into specific components of the system, such as devices, rules, system monitors, tasks, reports, and identity fields

The FortiSIEM CMDB contains a lot of useful information, including system configurations, such as rules and report definitions.

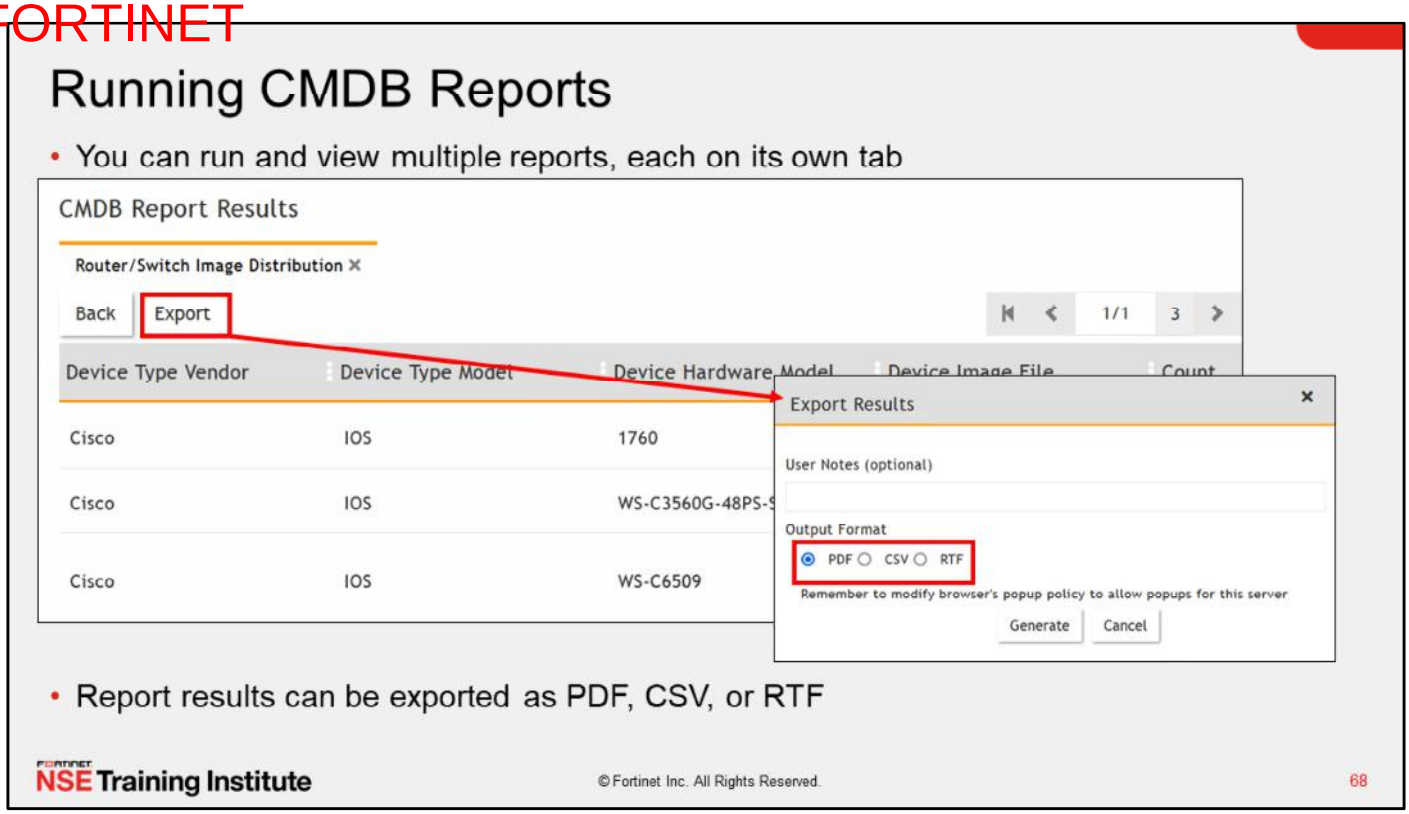
The CMDB reporting feature contains a number of predefined system reports related to the contents of the CMDB.

Users can clone existing system reports, or create their own reports from scratch. These reports follow the same logic as rules and analytic reports in that, if you edit a system report, it forces you to save it with a different name.

These reports can drill down into specific components of the system, such as devices, rules, system monitors, tasks, reports, identity fields, and more.

Vouchers & Dumps are Available | WhatsApp +201224560923

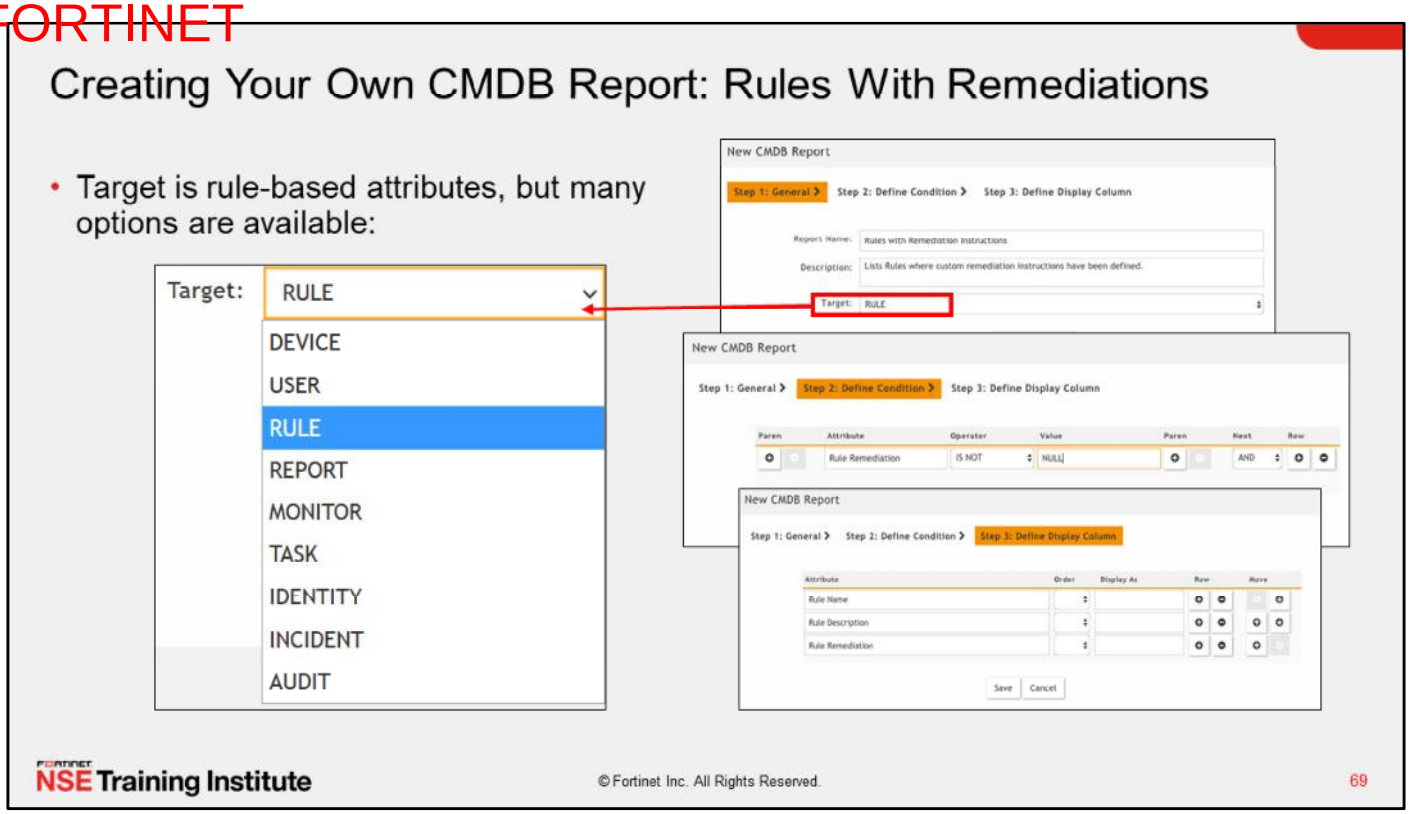
DO NOT REPRINT
© FORTINET
Brave-dumps.com



When you run CMDB reports, you can run and view multiple reports, each on its own tab. You can export the results as a PDF, CSV, or RTF file.

Vouchers & Dumps are Available | WhatsApp +201224560923

DO NOT REPRINT
© FORTINET
Brave-dumps.com



This slide shows an example of a CMDB report created for rules and remediation instructions:

Step 1: General: Provide a name and description for the report. Select the target of the report. The target determines which attributes are returned as part of the query.
Step 2: Define Conditions: Conditions are filters for the target attribute group. In the example shown on this slide, the **Rule Remediation** attribute is not `NULL`.
Step 3: Define Display Columns: The display columns selected in this example are: **Rule Name**, **Rule Description**, and **Rule Remediation**.

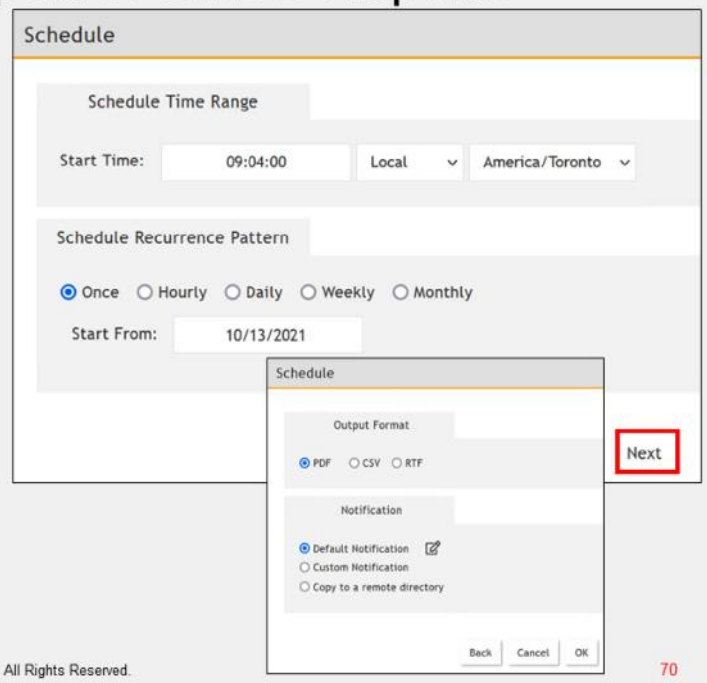
Vouchers & Dumps are Available | WhatsApp +201224560923

DO NOT REPRINT
© FORTINET
Brave-dumps.com

Scheduling an Import or Export of CMDB Reports



- You can schedule every CMDB report with a PDF, CSV, or RTF output format
- You can also import or export CMDB report definitions as XML to be shared across FortiSIEM devices



NSE Training Institute

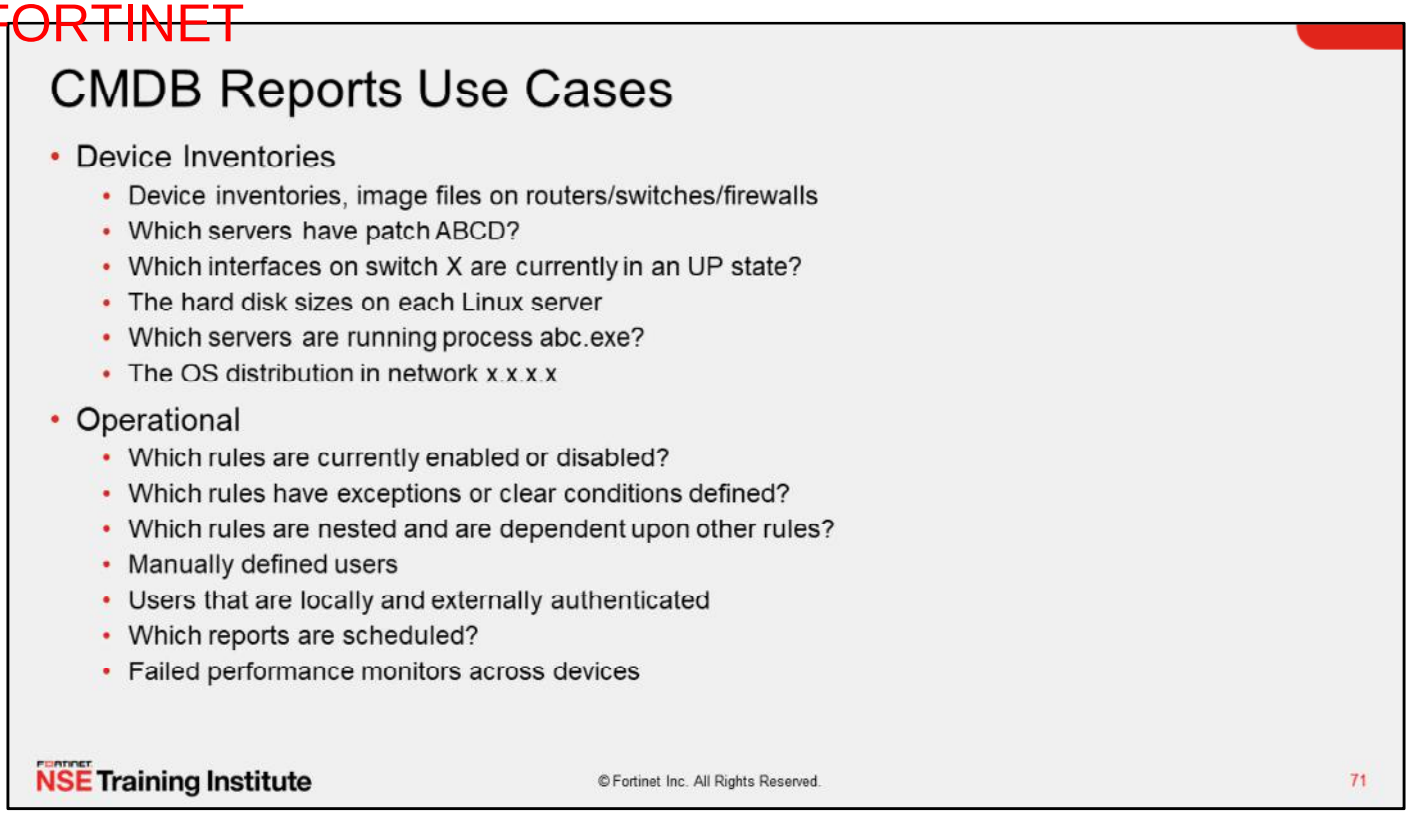
© Fortinet Inc. All Rights Reserved.

70

You can schedule CMDB reports, and have the output delivered to a specified email address as a PDF, CSV, or RTF file. You can import or export CMDB report definitions as XML and share them across different FortiSIEM devices.

Vouchers & Dumps are Available | WhatsApp +201224560923

DO NOT REPRINT
© FORTINET
Brave-dumps.com



So what are some of the use cases for the CMDB reporting feature?

One use case for CMDB reports is device inventories. In FortiSIEM, you can run a device inventory report to look at image files on all routers, switches, and firewalls to identify vulnerable firmware versions. You can look at what servers have certain patches installed, or which interfaces on a switch are currently in an up or down state. You can also find answers to these questions:

- What are the hard disk sizes on each Linux server in your network?
- Which servers are running a particular process, such as Exchange or IIS?
- What is the OS distribution in the network? For example, how many Windows 2003 servers do you have in comparison to 2008?

CMDB reports can also answer questions about FortiSIEM operations, such as:

- Which rules are currently enabled or disabled on the system?
- Which rules have exceptions or clear conditions defined?
- Which rules are nested or dependant on other rules? In FortiSIEM, rules can also reference other rules.
- Which users are manually defined?
- Which users are locally and externally authenticated?
- Which reports are scheduled?
- Which devices have failed performance monitors?

There are many other use cases. The FortiSIEM reporting feature is rich with in-depth information about the devices in your network, as well as FortiSEIM itself.

Vouchers & Dumps are Available | WhatsApp +201224560923

DO NOT REPRINT
© FORTINET
Brave-dumps.com

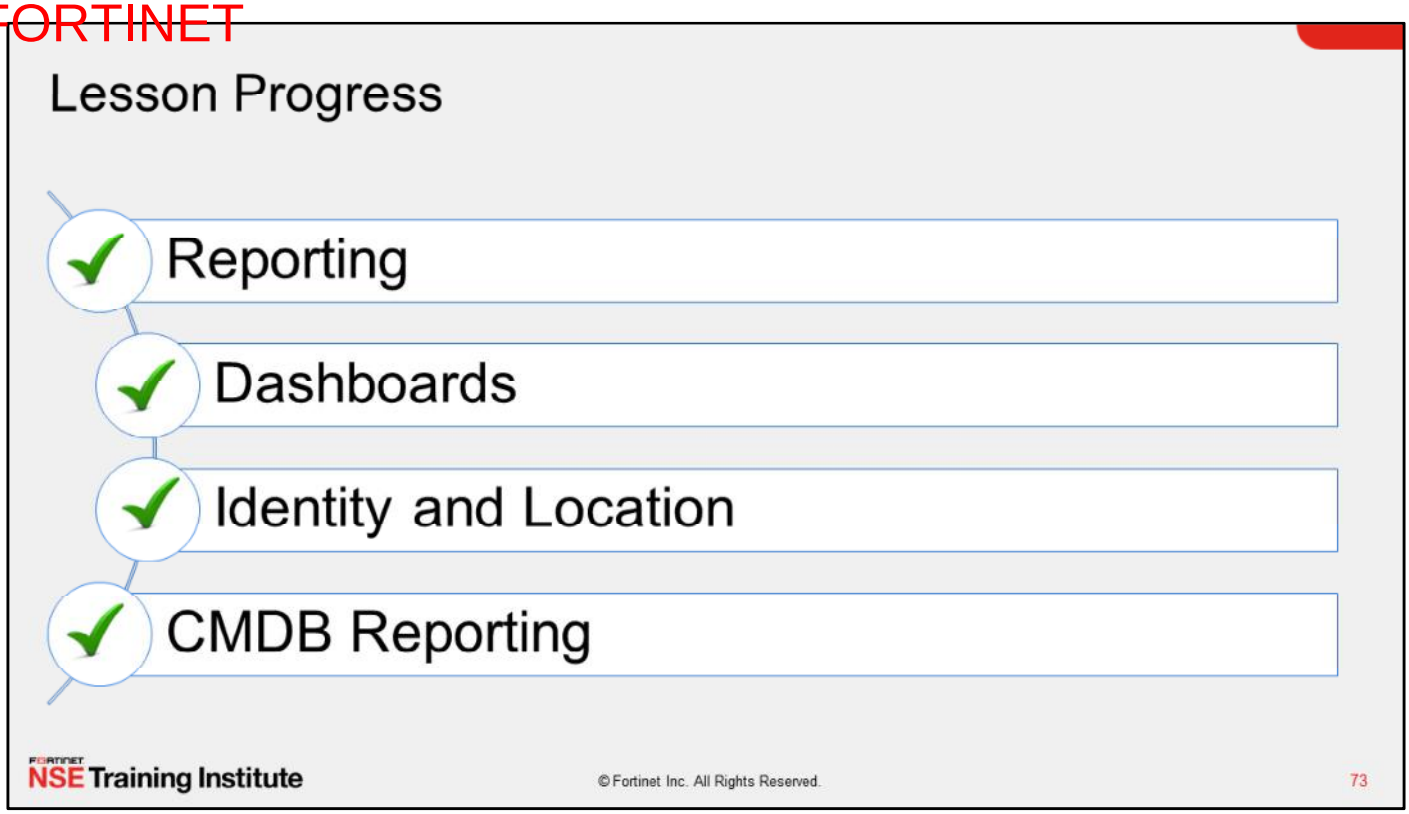
Knowledge Check

1. Which statement about CMDB reports is correct?
   - ✓ A. CMDB report definitions can be imported as XML files
   - B. CMDB report definitions can be imported as RTF files

© Fortinet Inc. All Rights Reserved.

Vouchers & Dumps are Available | WhatsApp +201224560923

DO NOT REPRINT
© FORTINET
Brave-dumps.com

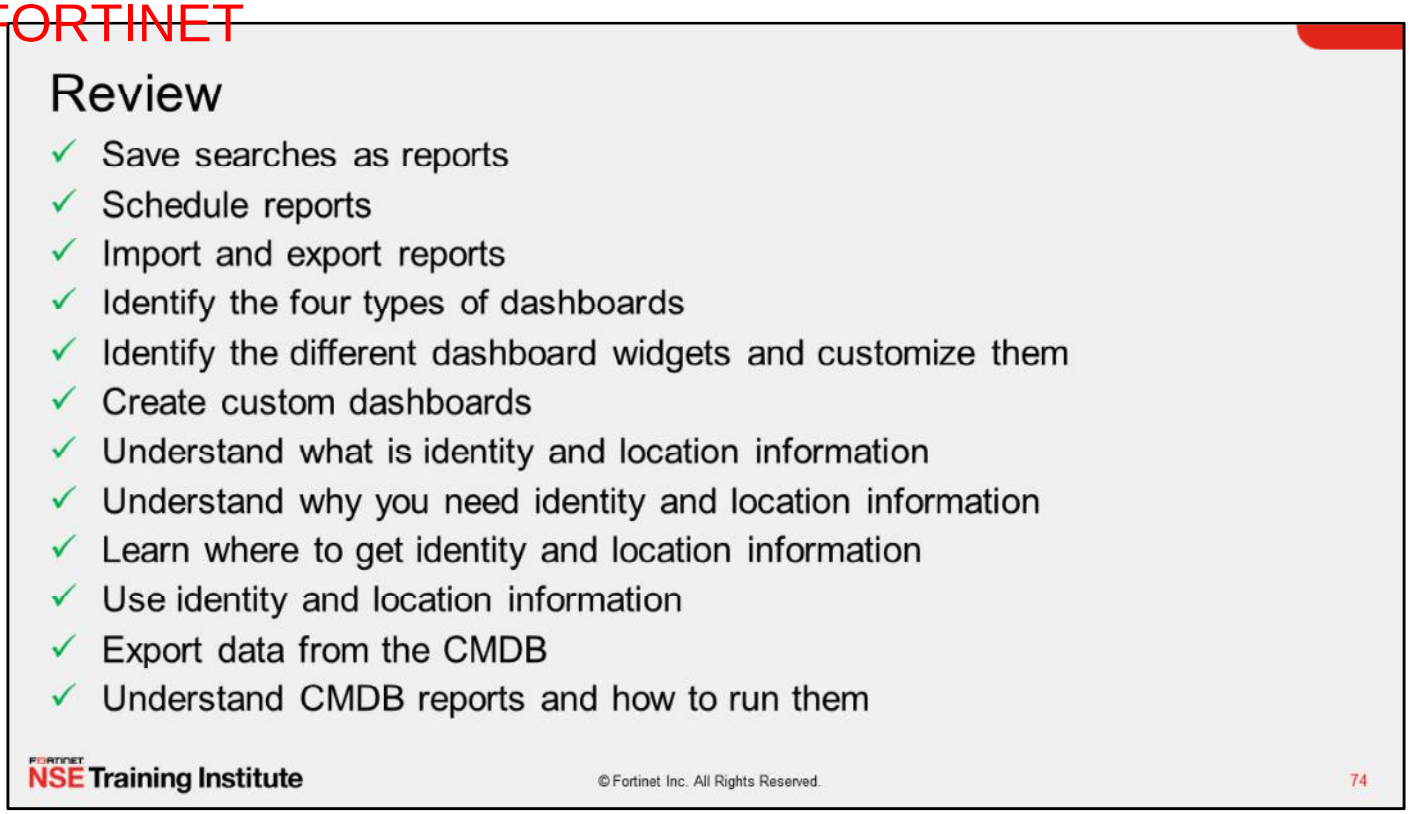


Congratulations! You have completed this lesson.

Now, you will review the objectives that you covered in this lesson.

Vouchers & Dumps are Available | WhatsApp +201224560923

DO NOT REPRINT
© FORTINET
Brave-dumps.com

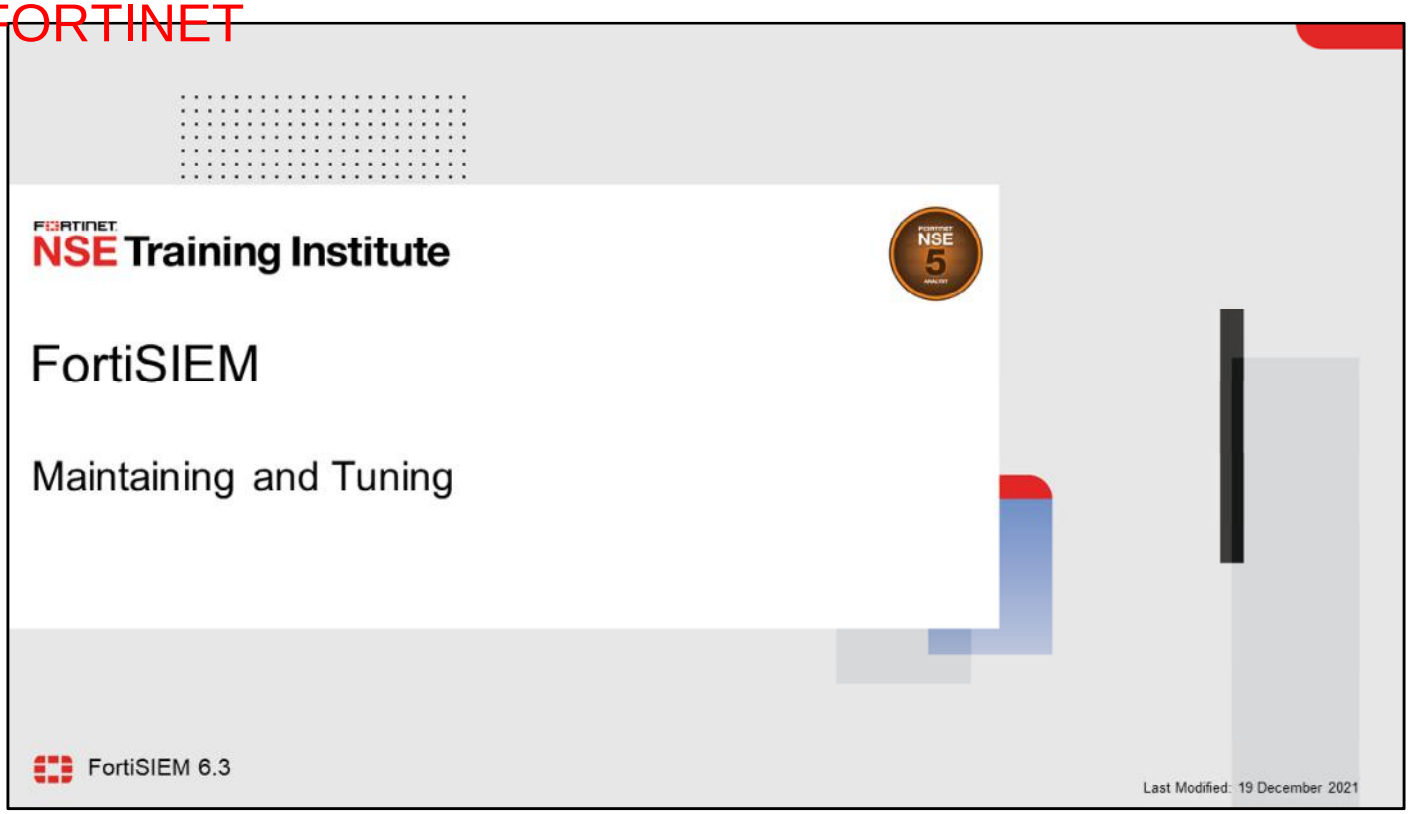


This slide shows the objectives that you covered in this lesson.

By mastering the objectives covered in this lesson, you learned how to effectively use reporting, dashboards, identity information, and location information as part of managing your network.

Vouchers & Dumps are Available | WhatsApp +201224560923

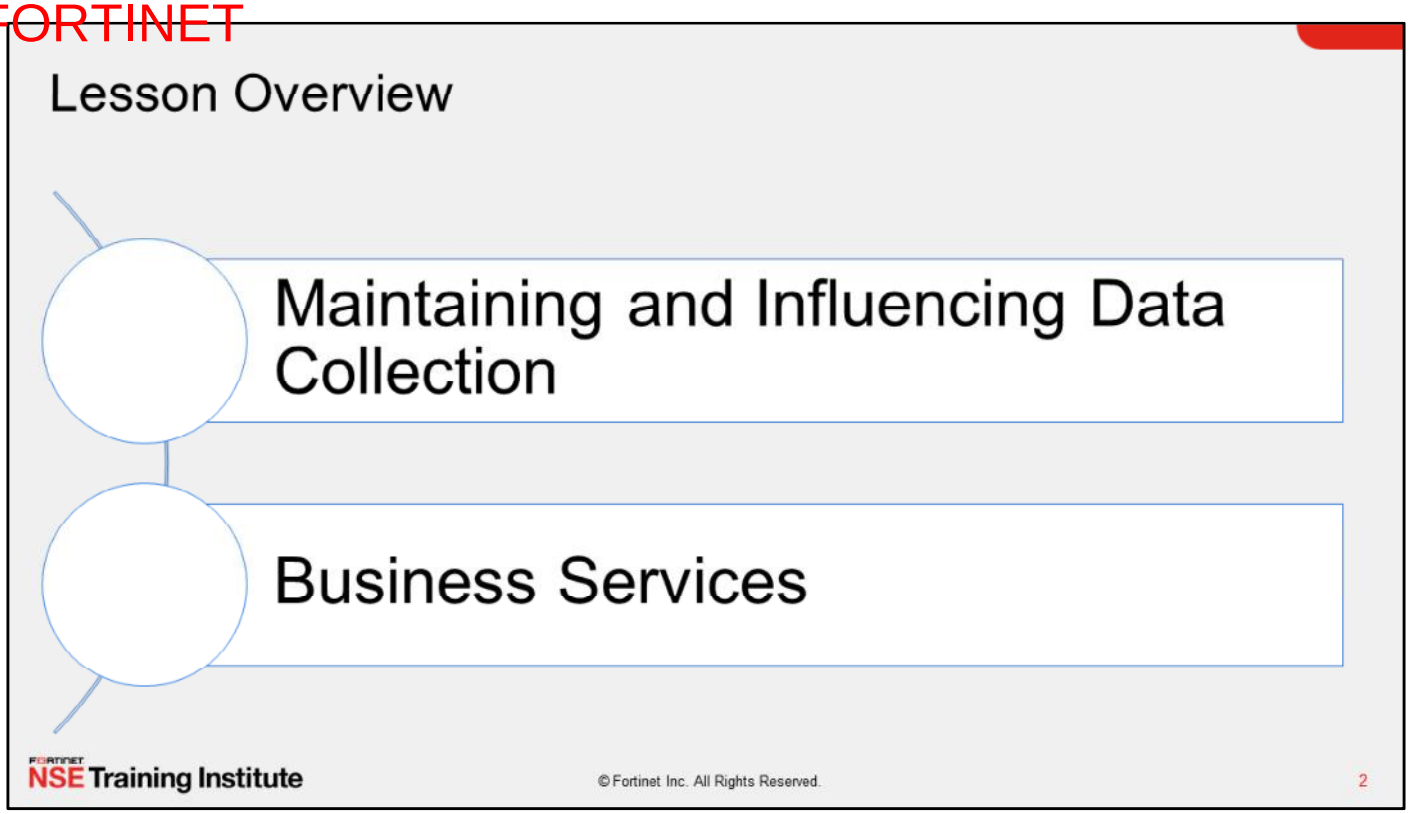
DO NOT REPRINT
© FORTINET
Brave-dumps.com



In this lesson, you will learn about ways to tune the FortiSIEM data collection and notification processes.

Vouchers & Dumps are Available | WhatsApp +201224560923

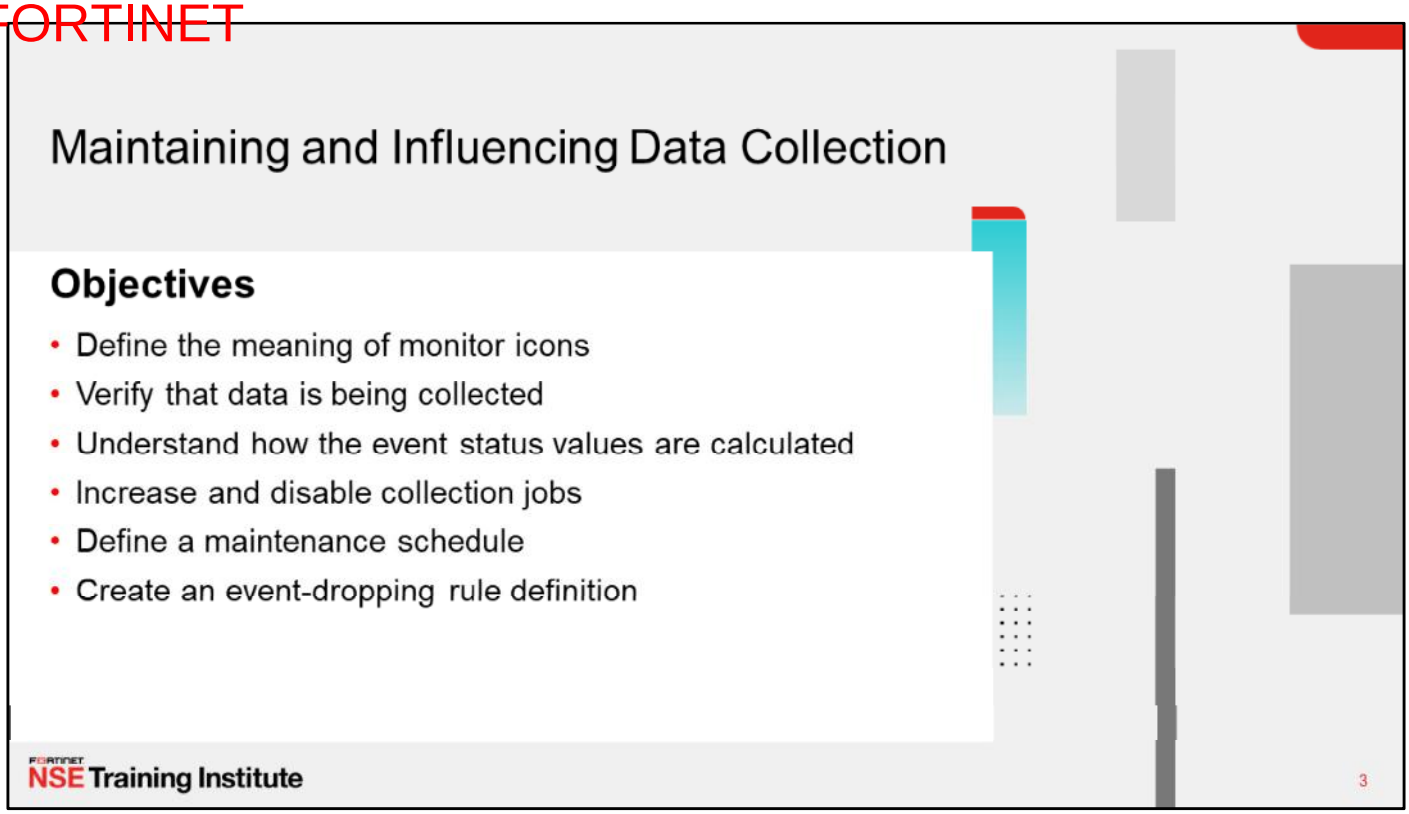
DO NOT REPRINT
© FORTINET
Brave-dumps.com



In this lesson, you will explore the topics shown on this slide.

Vouchers & Dumps are Available | WhatsApp +201224560923

DO NOT REPRINT
© FORTINET
Brave-dumps.com

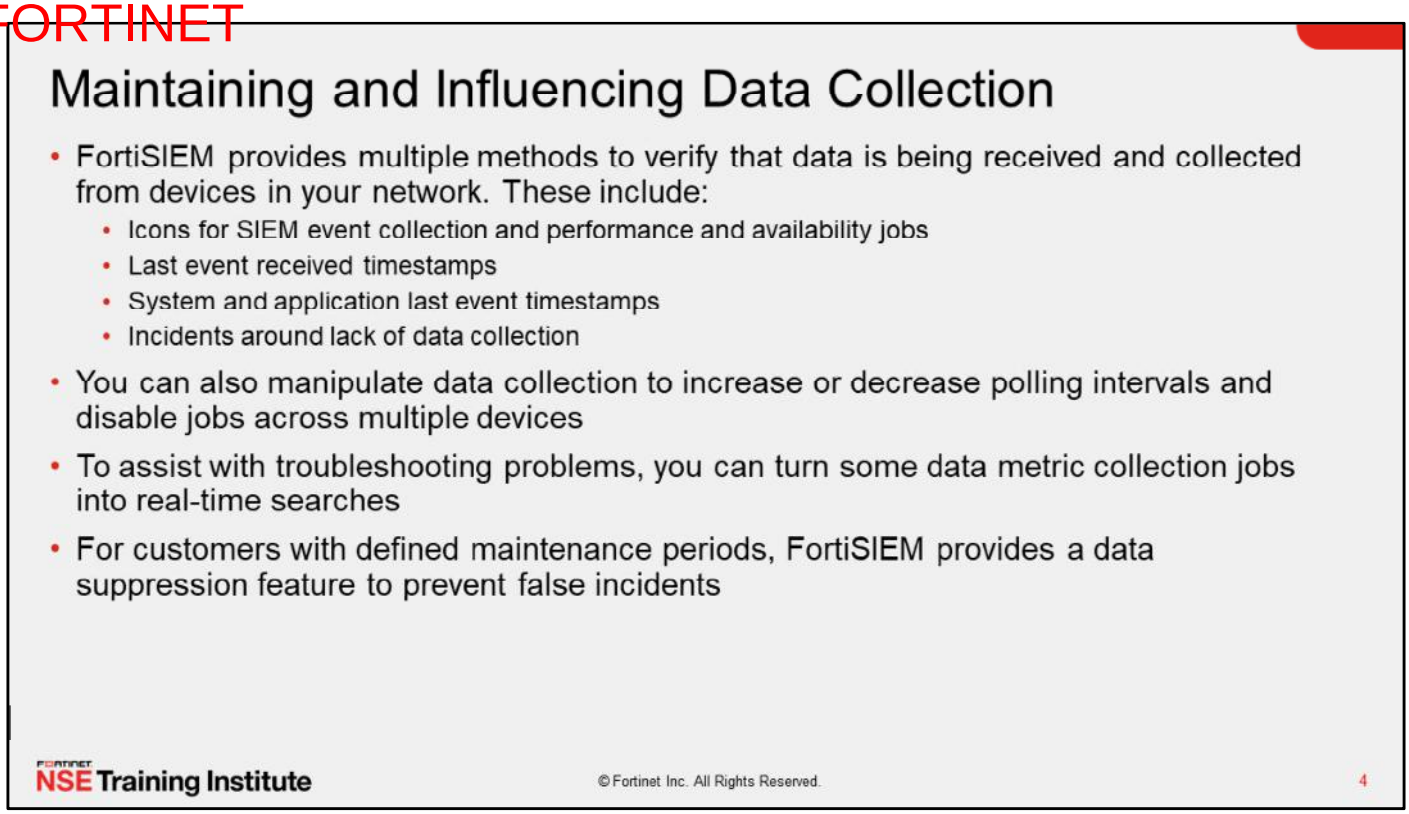


After completing this section, you should be able to achieve the objectives shown on this slide.

By demonstrating competence in maintaining and influencing data collection, you will reduce the impact of false positives in your network.

Vouchers & Dumps are Available | WhatsApp +201224560923

DO NOT REPRINT
© FORTINET
Brave-dumps.com



From a monitoring standpoint, you want to make sure that you are constantly collecting data. However, from a compliance standpoint, you want to make sure that the data you are collecting is the *right* data from the *right* devices and applications.

FortiSIEM provides methods that you can use to verify that data is being received and collected from the devices in your network.

Some of the methods include:

- Icons for different jobs, such as the SIEM event collection jobs, and performance and availability jobs
- Timestamps for the last event received
- Timestamps for the last events received for each system and application
- Rules that generate incidents caused by a lack of data collection

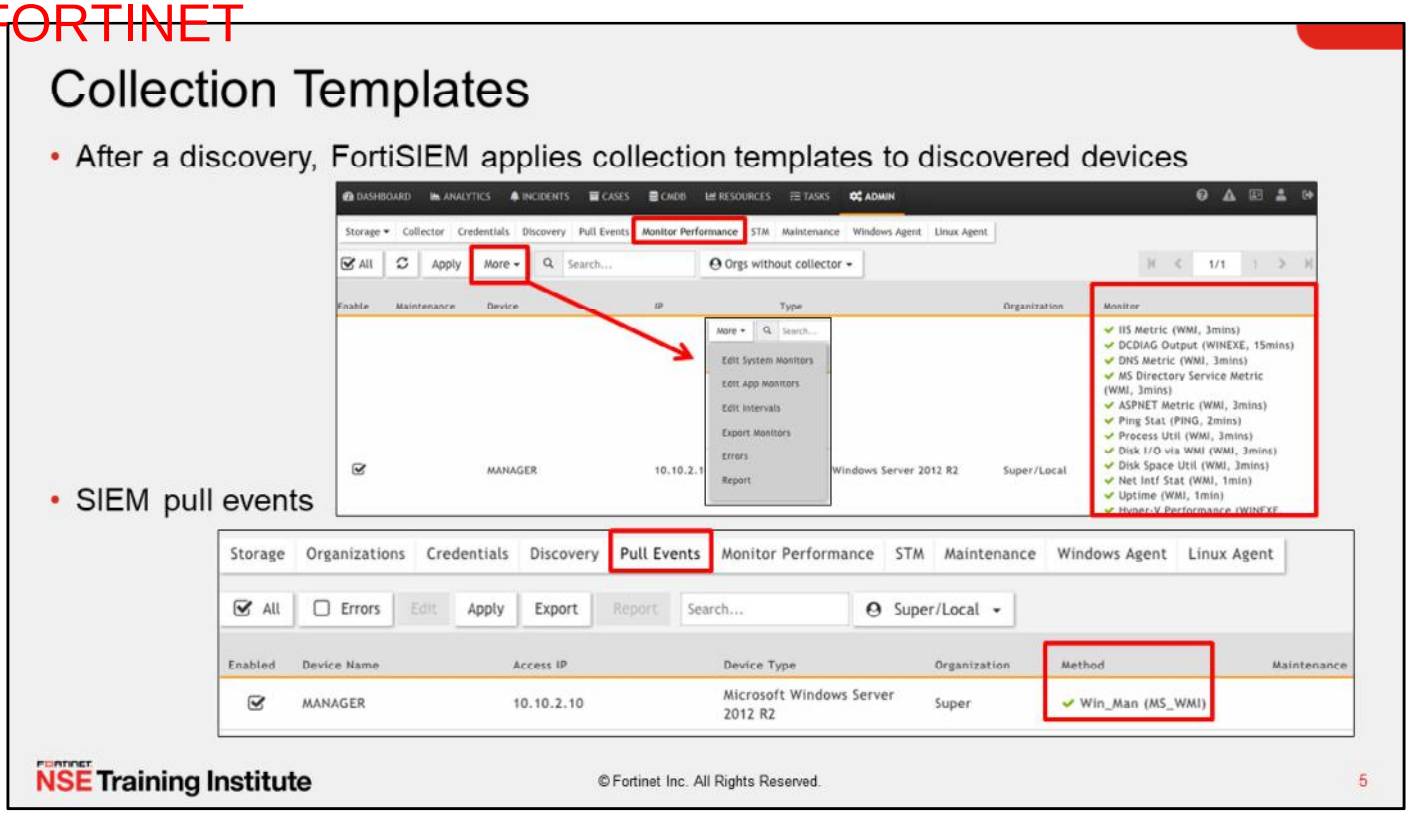
You can also manipulate data collection by increasing and decreasing polling times and disabling jobs across multiple devices.

To assist with troubleshooting, you can turn some metric collection jobs into real-time searches.

There is also a maintenance calendar feature for customers who have defined maintenance windows. You can use this feature to temporarily suppress collection jobs from specific devices, which helps prevent false incidents being generated from a device that is being worked on.

Vouchers & Dumps are Available | WhatsApp +201224560923

DO NOT REPRINT Brave-dumps.com
© FORTINET

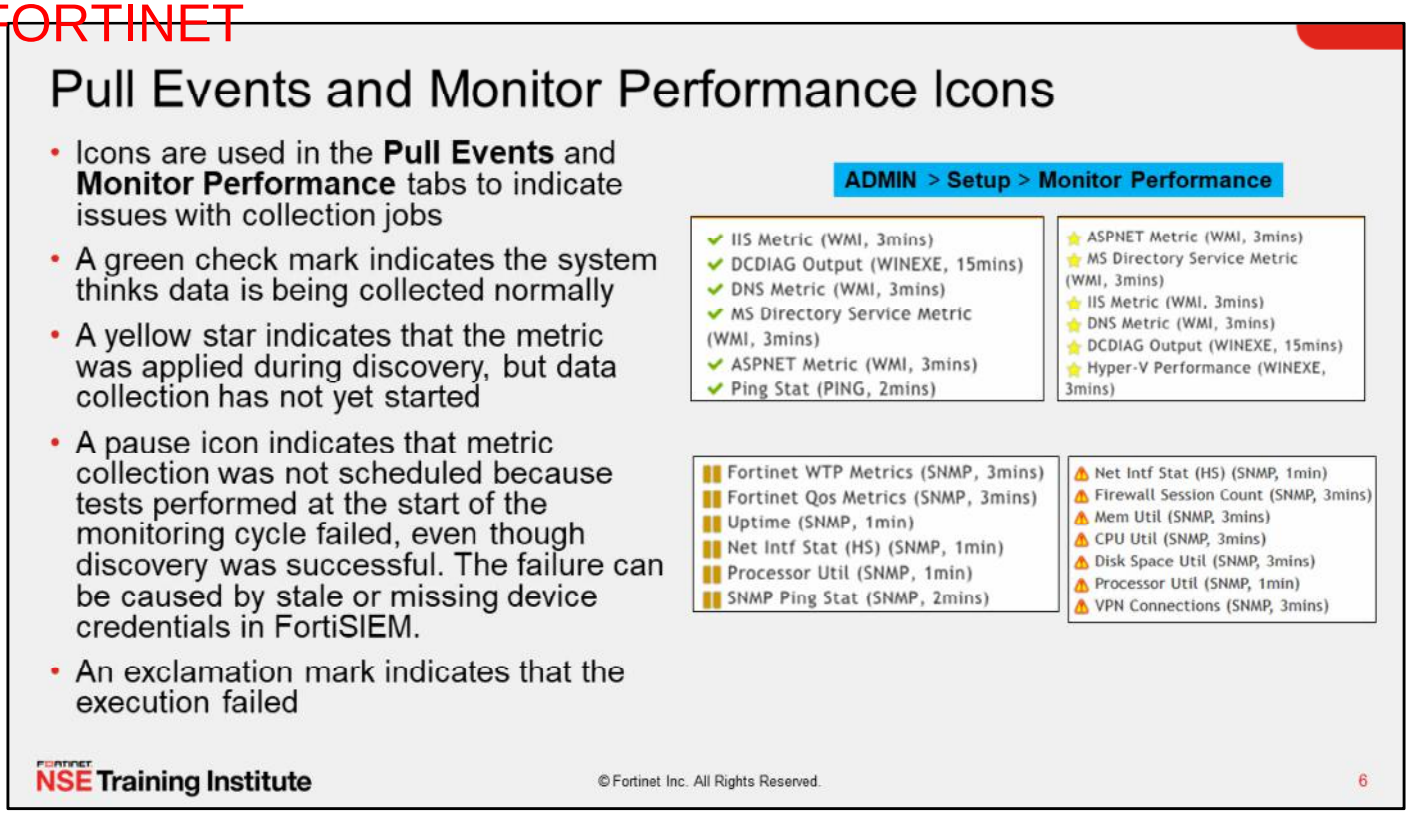


After a FortiSIEM performs a discovery, it applies collection templates to the discovered devices. On the **ADMIN** > **Setup** page, on the **Monitor Performance** tab, you can see the system monitor collection jobs that FortiSIEM applied have been applied to collect the performance data from each device. You can also see the application monitor collection jobs that have been applied.

FortiSIEM also creates collection jobs for SIEM or security-related data that you can see on the **Pull Events** tab. These jobs can collect data such as Windows event logs using WMI, or VMWare logs using VMWare's own API.

Vouchers & Dumps are Available | WhatsApp +201224560923

DO NOT REPRINT
© FORTINET
Brave-dumps.com



Icons are used in the **Pull Events** and **Monitor Performance** tabs to indicate issues with collection jobs. If there is green check mark next to a metric, it indicates that data collection status is normal.

If you see a yellow star against a device metric, this indicates that the metric was applied during discovery, but data collection has not yet started. So, if you open this page immediately after performing a discovery, you would likely see many yellow stars. If you wait a few minutes, then press refresh, you should see the yellow stars disappear as metric collection begins.

If you see a pause icon, this indicates that metric pulling was not scheduled for this device. The reason for this could be because tests performed at the very beginning of the monitoring cycle failed, even though discovery was successful. This is typically caused by stale or missing device credentials. It is possible that the credentials that were used during the initial discovery were changed on the device, and not updated in FortiSIEM.

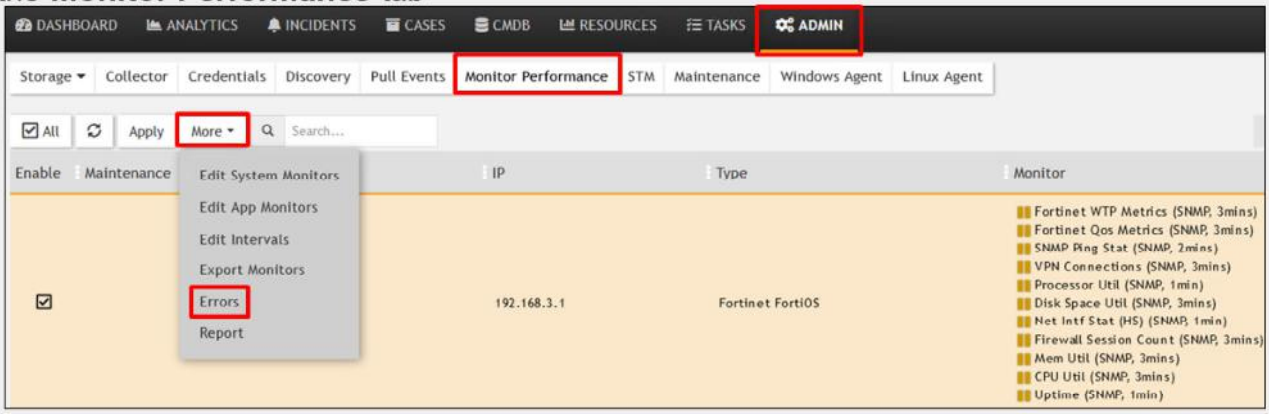
If you see an exclamation mark against a device metric, this indicates that the execution of this metric collection failed. The most likely cause is that FortiSIEM can't reach the device or the provided credentials are incorrect.

Vouchers & Dumps are Available | WhatsApp +201224560923

DO NOT REPRINT
© FORTINET
Brave-dumps.com

Viewing Collection Errors

- You can view more information about any reported errors by clicking **More > Errors** in the **Monitor Performance** tab



- **Note**: In some cases, reported errors may be due to particular metrics not being available on a monitored device

NSE Training Institute

© Fortinet Inc. All Rights Reserved.

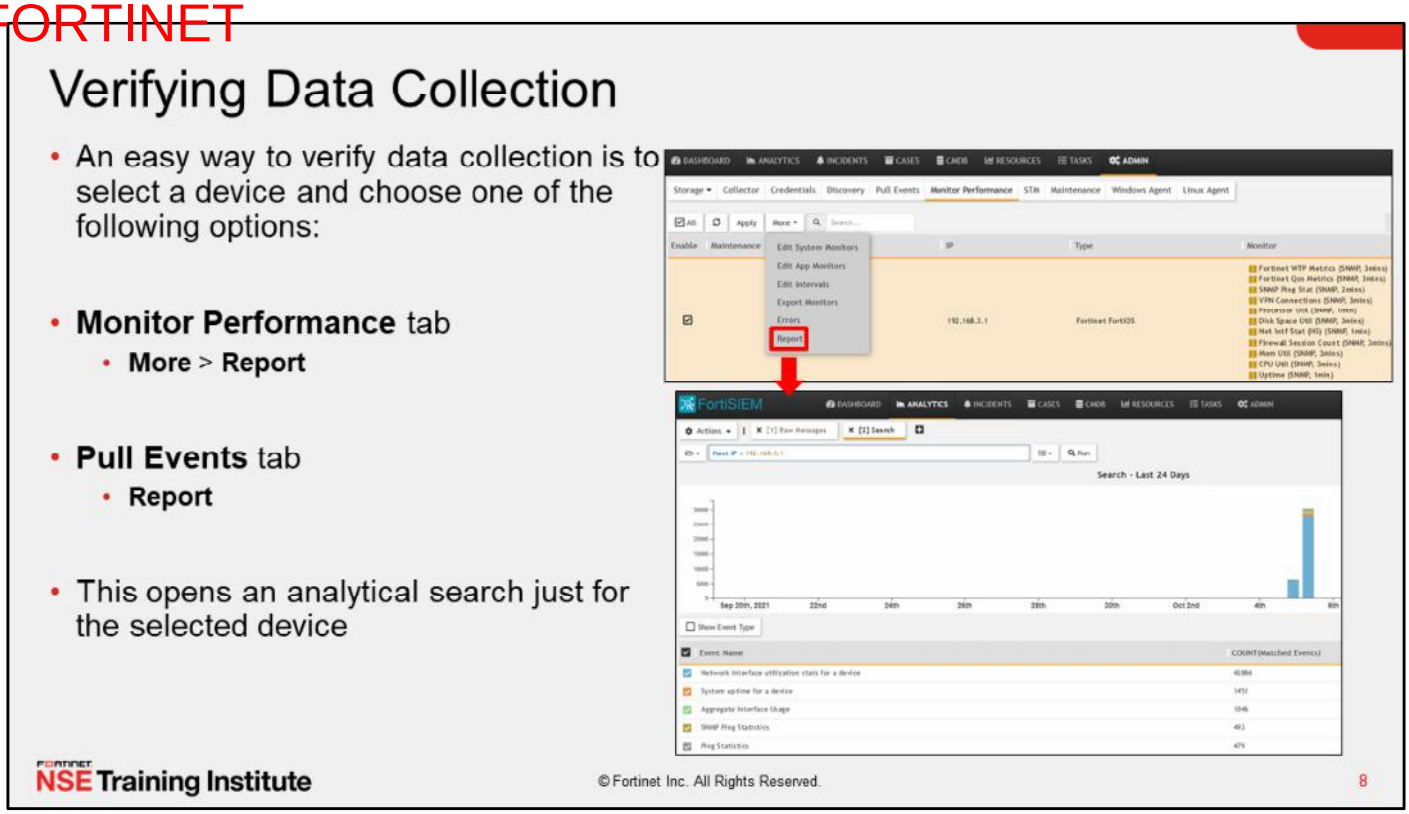
7

You can see more information about any reported errors by clicking **More**> **Errors** on the **Monitor Performance** tab.

Note that, in some cases, errors may be due to a particular metric not being available on a particular device, rather than an issue. For example, FortiSIEM may indicate that it can't find the SNMP data for the remote access VPNs, whereas, for example, the FortiGate firewall simply doesn't have any remote access VPNs configured.

Vouchers & Dumps are Available | WhatsApp +201224560923

DO NOT REPRINT Brave-dumps.com
© FORTINET



An easy way to verify data collection is to select a specific device and choose one of the following options:

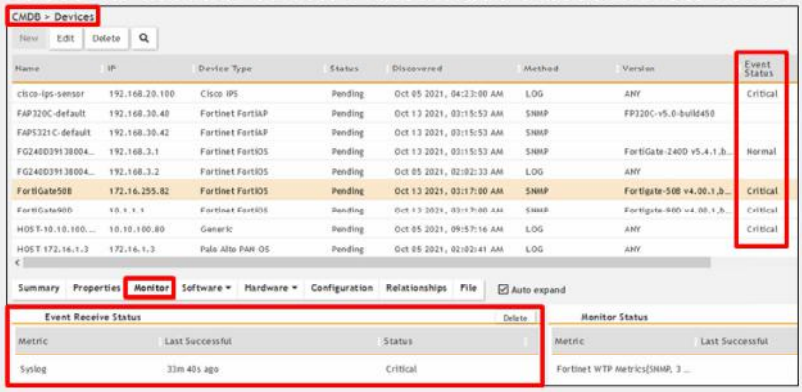
- Under the **Monitor Performance** tab, select a device, then select **Report** from the **More** drop-down list. This opens an analytical search that queries for performance data from the selected device.
- Under the **Pull Events** tab, which shows the security metrics collected by FortiSIEM, select a device and then click **Report**. This opens an analytical search that queries data for the selected device.

Vouchers & Dumps are Available | WhatsApp +201224560923

DO NOT REPRINT Brave-dumps.com
© FORTINET

Event Receive Status

- In the CMDB, FortiSIEM records receive times and calculates an event status for each device



- **Event Receive Status** monitoring is related to receiving SIEM data, such as syslog and Netflow, as well as SIEM collection jobs, such as WMI event logs and VM_SDK
- Select a device and then click the **Monitor** tab to view the last event receive time. This value is updated every two minutes.

NSE Training Institute

© Fortinet Inc. All Rights Reserved.

9

FortiSIEM records receive times and calculates an event receive status for each device in the CMDB. Event receive status monitoring is related to SIEM data, such as syslog and Netflow, as well SIEM collection jobs, such as WMI event logs and VMWare SDK API-related pulls.

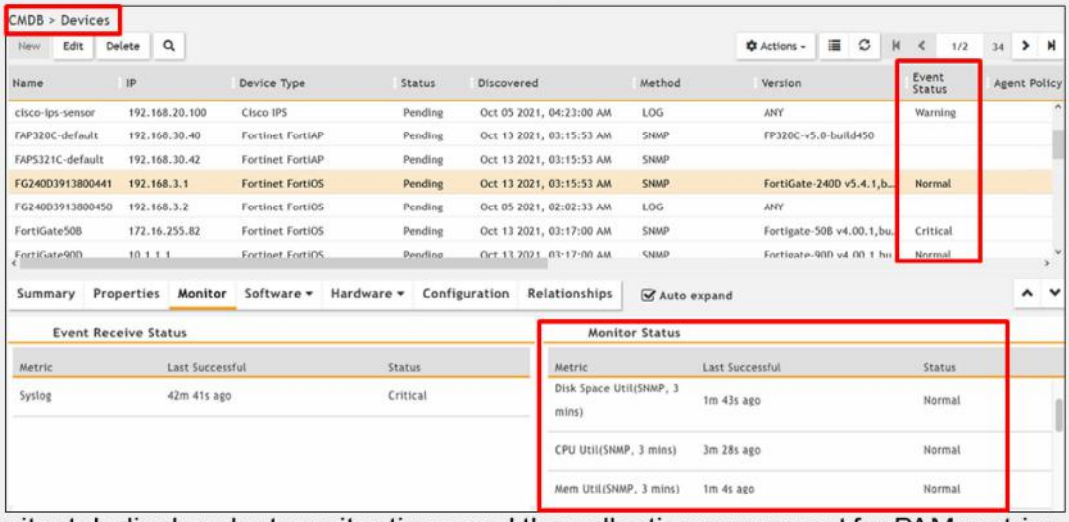
Select a device, and then click the **Monitor** tab to view the last event receive time. This status is updated every two minutes.

Vouchers & Dumps are Available | WhatsApp +201224560923

DO NOT REPRINT Brave-dumps.com
© FORTINET

Performance Monitor Status

- The CMDB records receive times and calculates a performance monitor status for each device



- The Monitor tab displays last monitor times and the collection component for PAM metrics

NSE Training Institute © Fortinet Inc. All Rights Reserved. 10

The CMDB also records receive times for performance-related data, and calculates a performance monitor status for each device.

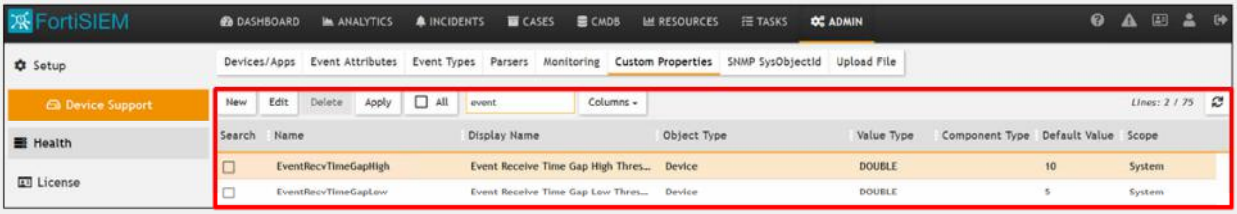
Select a device in the CMDB and, on the details pane, click the **Monitor** tab to display the collection component for the PAM metrics and the last monitored times. The components listed here are the same components listed for this device under **ADMIN** > **Setup** > **Monitor Performance** tab. The listed components include disk space, network interface, CPU, memory, and so on.

Vouchers & Dumps are Available | WhatsApp +201224560923

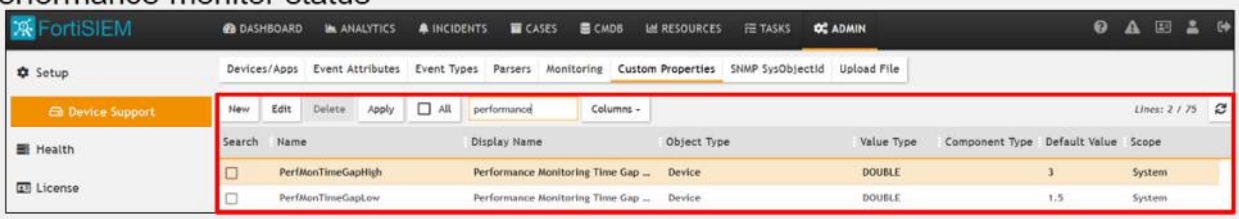
DO NOT REPRINT Brave-dumps.com
© FORTINET

Determining the Monitor Status

- The status fields in the CMDB (normal, warning, critical) are determined by global thresholds, which can be overridden by setting a per-device threshold
- Event receive status



- Performance monitor status



NSE Training Institute

© Fortinet Inc. All Rights Reserved.

11

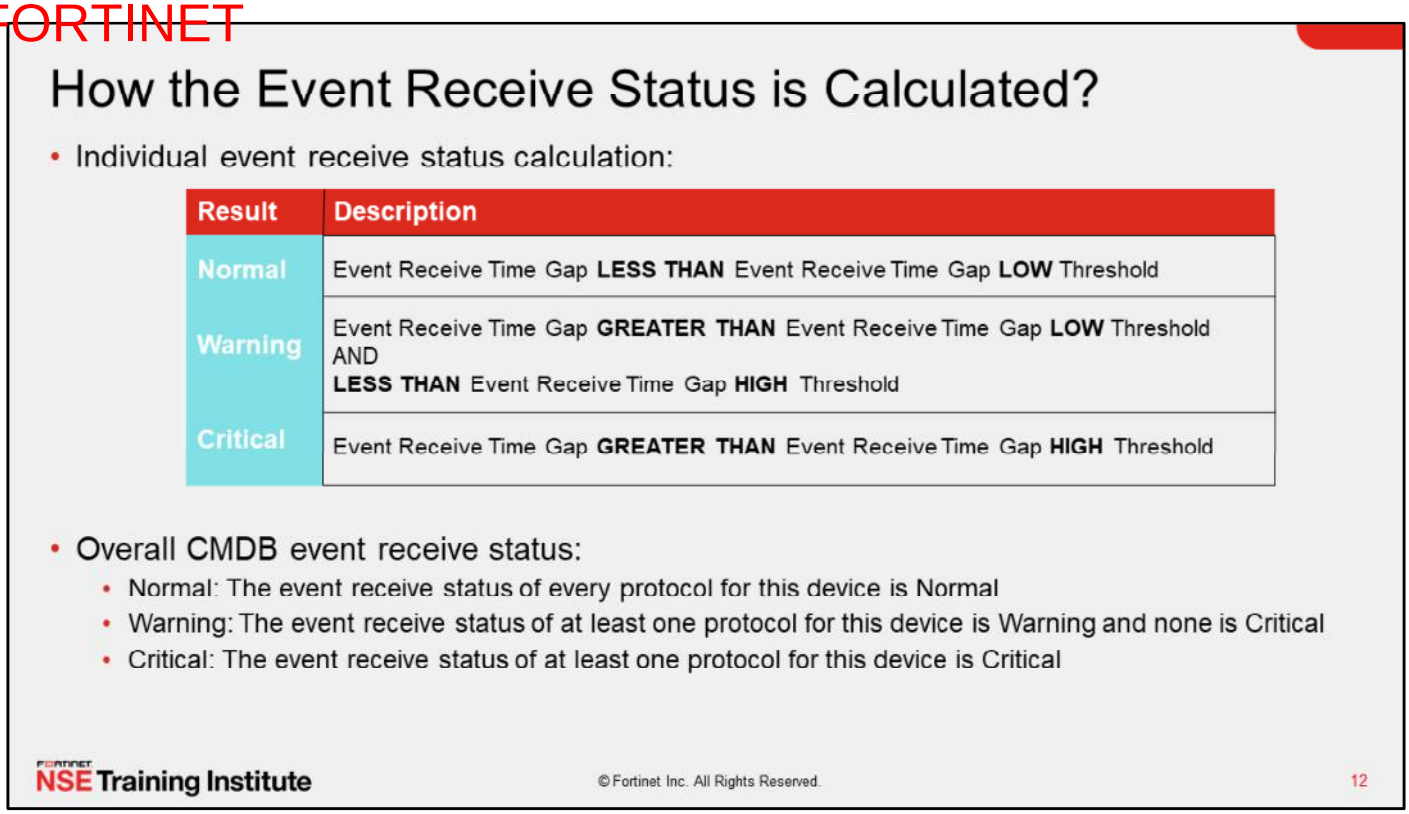
How the system determines the monitor status is governed by global thresholds. You can override global thresholds by setting a per device threshold in the CMDB.

For the event receive status, if you search for the word *Event* on the **Admin** > **Device Support** > **Custom Properties** tab, you will see **Event Receive Time Gap High** threshold and **Event Receive Time Gap Low** threshold. These thresholds are displayed in minutes. The low threshold has a default value of 10 minutes and the high threshold has a default value of 20 minutes.

If you search for the word *Perf* you will see the **Performance Monitoring Time Gap High** threshold and **Performance Monitoring Time Gap Low** threshold. These thresholds are displayed as multiples of the polling interval. For example, if the polling interval is 3 minutes, then the high threshold would be 15 minutes (the displayed value of 5 multiplied by the 3-minute polling interval), and the low threshold would be 5 minutes (1.5 times 3 minutes).

Vouchers & Dumps are Available | WhatsApp +201224560923

DO NOT REPRINT
© FORTINET
Brave-dumps.com



How is the event receive status calculated?

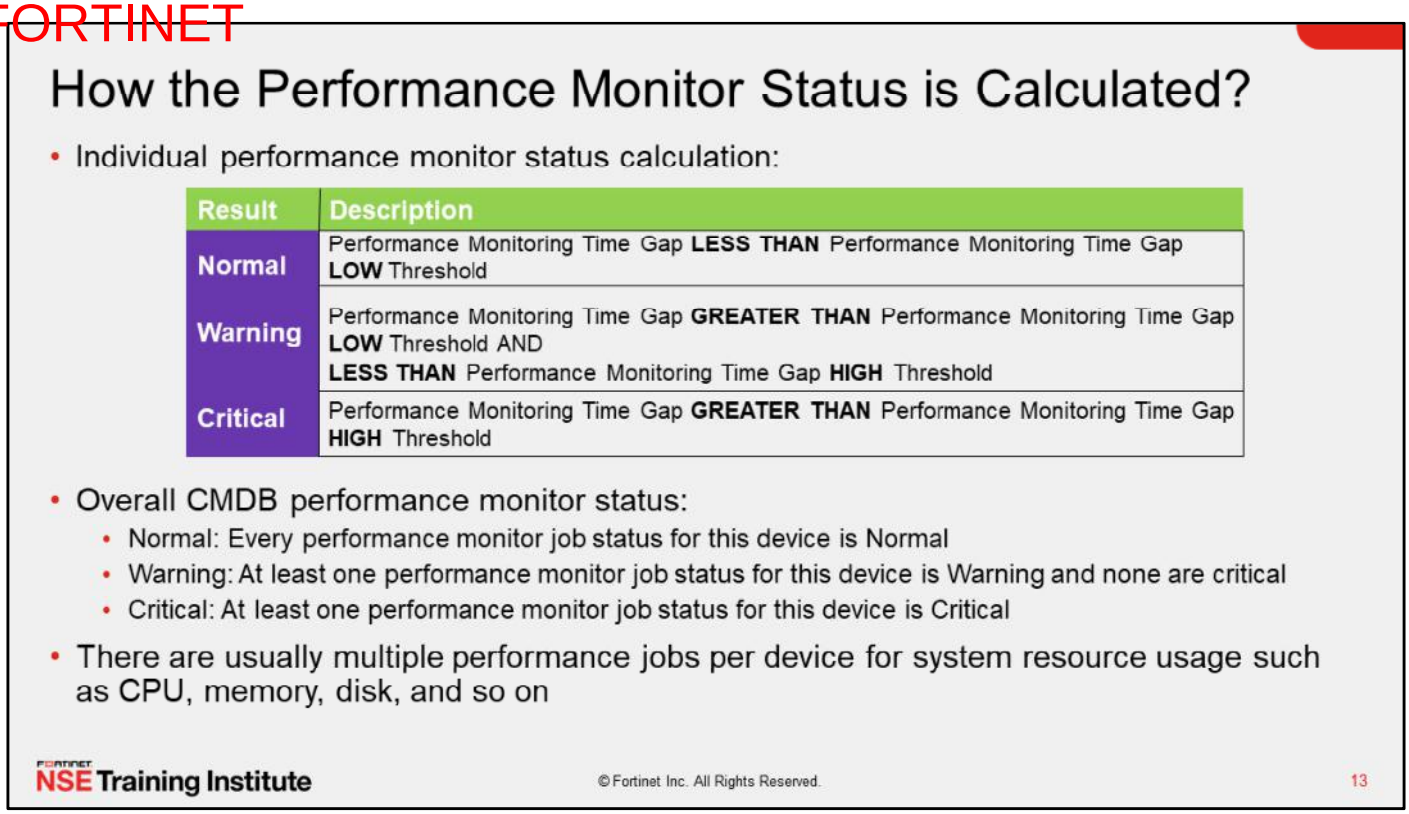
There is an individual value for the event receive status on the **Monitor** tab.
The status will be one of the following:
- Normal: The event receive status gap is less than the Low threshold.
- Warning: The gap is greater than the Low threshold and less that the High threshold.
- Critical: The event receive status gap is greater than the High threshold.

There is also an overall CMDB event receive status, which applies to the device as a whole.
This status will show as one of the following:
- Normal: The event receive status of every protocol for this device is Normal.
- Warning: The event receive status of at least one protocol for the device is Warning and none are Critical.
- Critical: The event receive status of at least one protocol for this device is Critical.

Note that the event receive status is referring to the SIEM data, or security data, of the reporting device. Some devices may report more than one method such as syslog, Netflow, WMI, and so on.

Vouchers & Dumps are Available | WhatsApp +201224560923

DO NOT REPRINT
© FORTINET
Brave-dumps.com



How is performance monitoring status calculated?

There is a separate performance monitoring status for each performance job listed on the **Monitor** tab for each device in the CMDB. The performance jobs for a device include CPU, memory, disk, and so on. Possible statuses are:

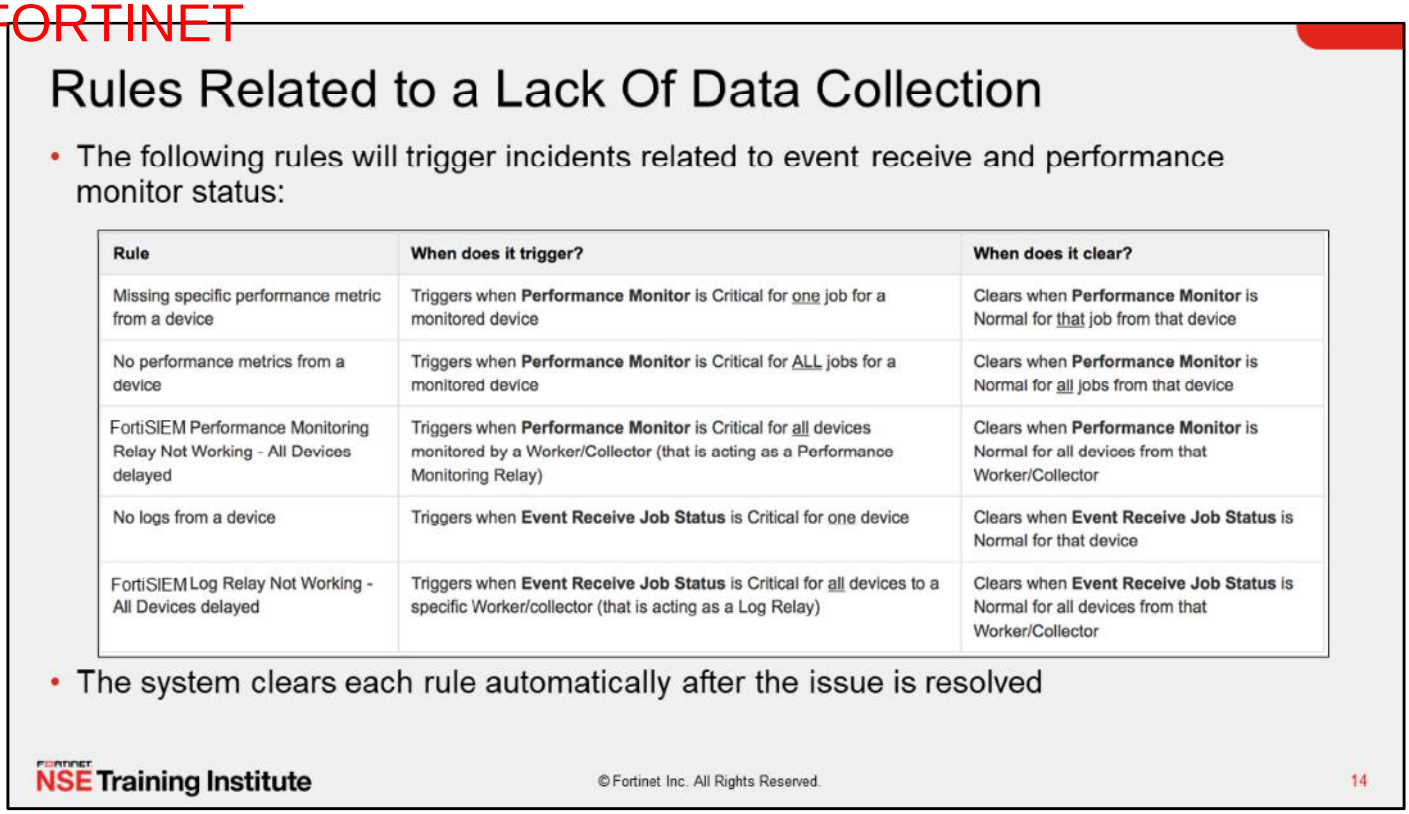
- Normal: The performance monitoring time gap is less than the Low threshold.
- Warning: The performance monitoring time gap is greater than the Low threshold and less than the High threshold.
- Critical: The performance monitoring time gap is greater than the High threshold.

There is also an overall performance monitor status in the top line of the CMDB entry, which will be one of the following:

- Normal: Every job is Normal.
- Warning: At least one job is Warning but none are Critical.
- Critical: At least one job is Critical.

Vouchers & Dumps are Available | WhatsApp +201224560923

DO NOT REPRINT
© FORTINET
Brave-dumps.com



There are a number of rules related to a lack of data collection. The system clears each rule automatically after the issue is resolved.

Rules include:

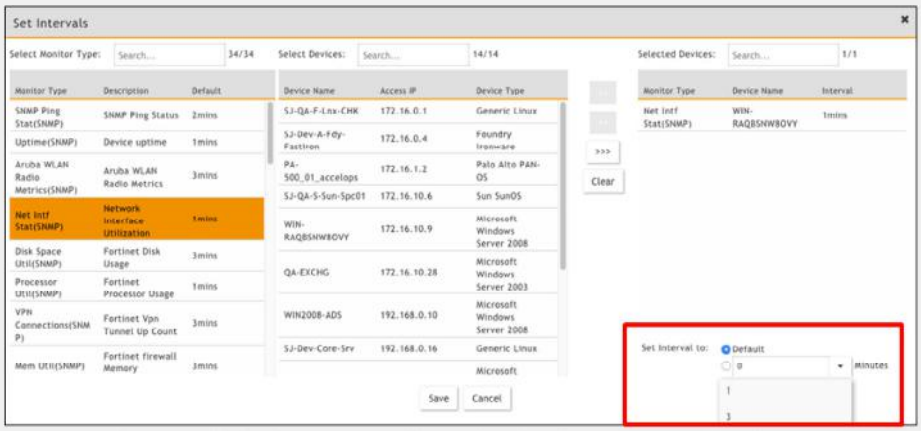
- The rule “Missing specific performance metric from a device” triggers when the performance monitor status is Critical for one job for a monitored device.
- The rule “No performance metrics from a device” triggers when performance monitor status is Critical for all jobs for a monitored device.
- The rule “FortiSIEM Performance Monitoring Relay Not Working – All Devices delayed” triggers when performance monitor status is Critical for all devices monitored by a worker or collector (that is, acting as a performance. monitoring relay).
- The rule “No logs from a device” triggers when the event receive job status is Critical for one device.
- The rule “FortiSIEM Log Relay Not Working – All Devices delayed” triggers when the event receive job status is Critical for all devices monitored by a specific worker or collector (that is, acting as a log relay).

Vouchers & Dumps are Available | WhatsApp +201224560923

DO NOT REPRINT Brave-dumps.com
© FORTINET

Increasing and Disabling System and Application Monitor Jobs

- In rare cases, you may need to change the frequency with which a performance job is collected, or you may need to disable a metric across multiple devices
- You can make these changes using options on the **Monitor Performance** tab



- **Note**: You must understand the impact to the rules before you make these changes

© Fortinet Inc. All Rights Reserved.

In rare cases, you may need to change the frequency with which a performance job is collected, or you may need to disable a metric across multiple devices.

To make these changes:

1. Click **Admin** > **Setup**, then click the **Monitor Performance** tab.
2. On the **Monitor Performance** tab, click the **More** drop-down list, and then select **Edit Interval**. The **Set Intervals** window opens displaying a list of all the monitor types that are being collected in your network. If you select a specific monitor type, all the devices that are currently using that system monitor will be listed in the **Select Devices** section.
3. Choose individual devices or all devices by moving them to the **Selected Devices** pane.
4. Now, you can change the polling interval or disable it.

You should understand the impact on the rules before you make these changes, for example:

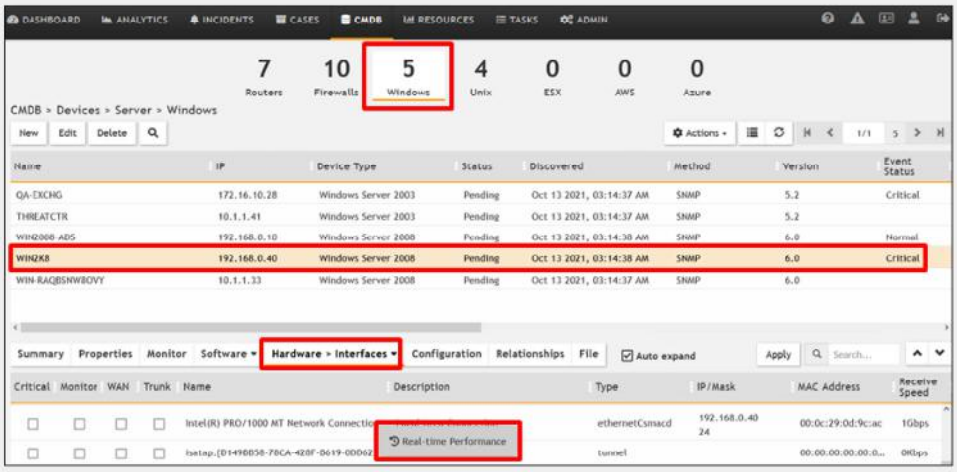
- The current polling interval for the CPU utilization metric on a specific device is two minutes.
- You have a rule that references the CPU utilization metric and is designed to calculate the average CPU utilization over a 10-minute time period.
- You decide to change the polling interval for that metric from two minutes, to 15 minutes.
- Once this change is made, the rule has, at most, one metric to calculate with (not an average), and, at times, the rule might not have any values at all. This might generate errors.

Vouchers & Dumps are Available | WhatsApp +201224560923

DO NOT REPRINT
© FORTINET
Brave-dumps.com

Real-Time Performance Metrics

- View the **Real Time Performance Metrics** for a device by selecting **Action/Real Time Performance** or selecting an interface in the **Interfaces** tab
- Designed to troubleshoot performance and availability issues in a more real-time format



NSE Training Institute
© Fortinet Inc. All Rights Reserved.
16

To view real-time performance metrics for a device in the CMDB, select a device and, on the **Interfaces** tab on the lower pane, select an interface, and then select **Real-Time Performance Metrics** from the drop-down list.

This feature is designed to troubleshoot performance and availability issues in a more real-time format.

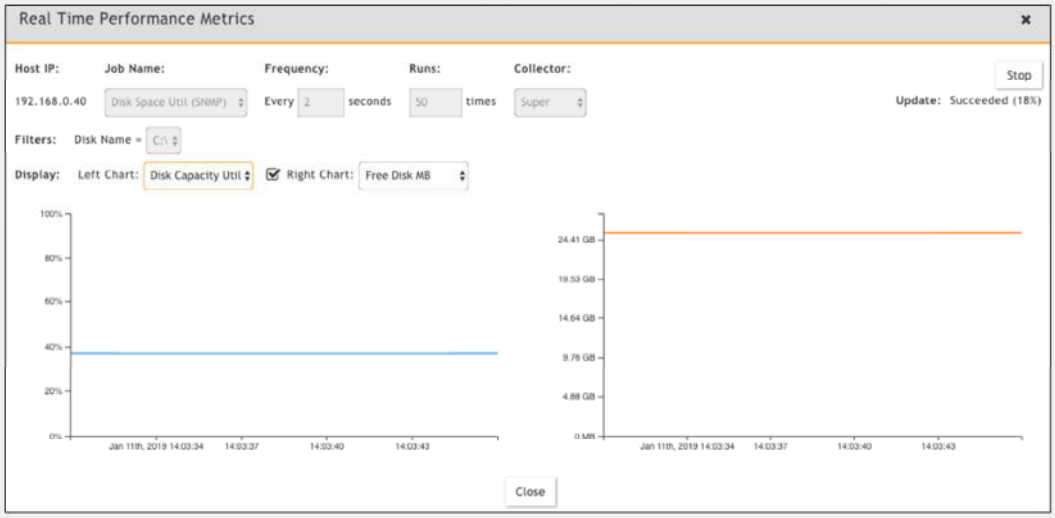
Vouchers & Dumps are Available | WhatsApp +201224560923

DO NOT REPRINT
© FORTINET
Brave-dumps.com

Results of Real-Time Performance Metrics

- You can select and run different collection jobs for a defined frequency over a number of samples

CMDB > Select device > **Actions** > **Real Time Performance**



NSE Training Institute

© Fortinet Inc. All Rights Reserved.

17

When you select **Real-Time Performance Metrics** from the device drop-down list in the CMDB, the **Real Time Performance Metrics** pop-up window opens. There, you can select different collection jobs and run them for a defined frequency, over a number of samples. For example, you could run a job every 20 seconds, 50 times.

For some jobs, you can display two attribute values at a time. For example, you could choose to show both received bytes and sent bytes for an interface.

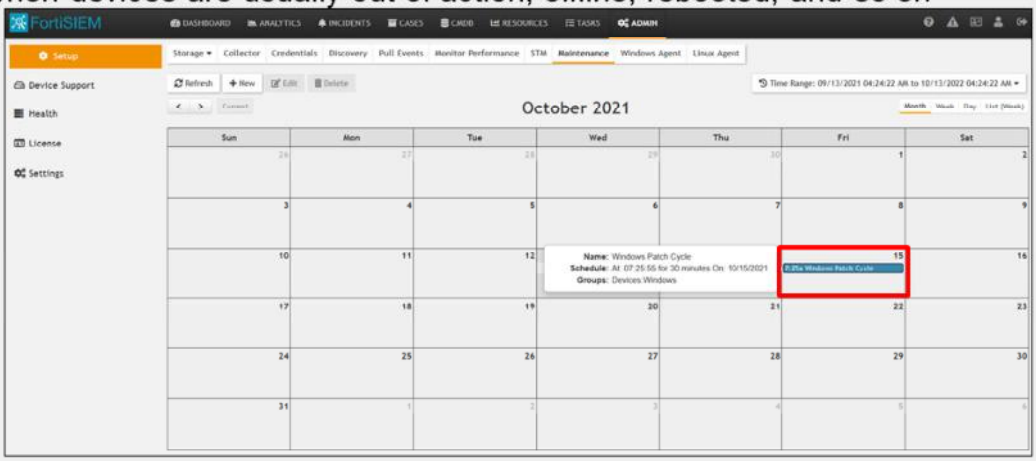
FortiSIEM uses the same event framework to collect data from devices in real-time and display them on the GUI; however, these events are not stored in the event database, nor do they trigger incidents.

Vouchers & Dumps are Available | WhatsApp +201224560923

DO NOT REPRINT Brave-dumps.com
© FORTINET

Maintenance Calendar

- The maintenance calendar is designed to assist customers who have set maintenance periods when devices are usually out of action, offline, rebooted, and so on



- When you add a device to the maintenance calendar, it is not monitored during the set time period, therefore, PAM-related alerts are not triggered

NSE Training Institute

© Fortinet Inc. All Rights Reserved.

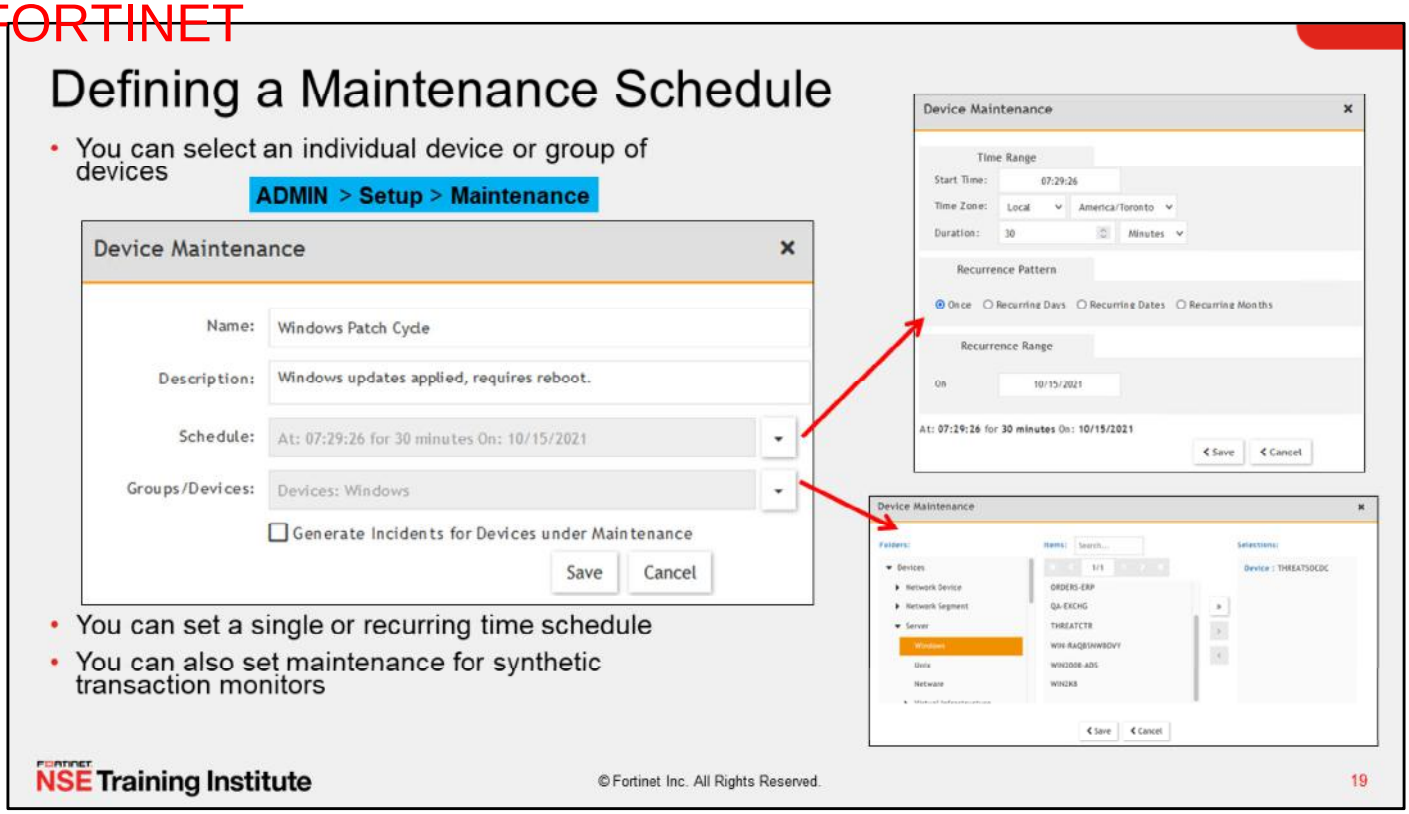
18

The maintenance calendar feature is designed to assist customers who set maintenance periods in their network. During maintenance periods, devices are usually out of action, taken offline, taken out of the rack, having the power supply changed, being rebooted, and so on. When a device is unavailable like this, it would cause FortiSIEM to determine that something is wrong in the network or on a specific device, and trigger incidents. This results in a false positive notifications.

To prevent these type of false positives, the maintenance calendar includes an event suppression feature. When you add a device to the maintenance calendar, that device is not monitored during the set time intervals. PAM data is not collected and, therefore, alerts are not triggered for those devices.

Vouchers & Dumps are Available | WhatsApp +201224560923

DO NOT REPRINT Brave-dumps.com
© FORTINET



To define a maintenance schedule for a device or a group of devices, browse the CMDB tree to select a device.

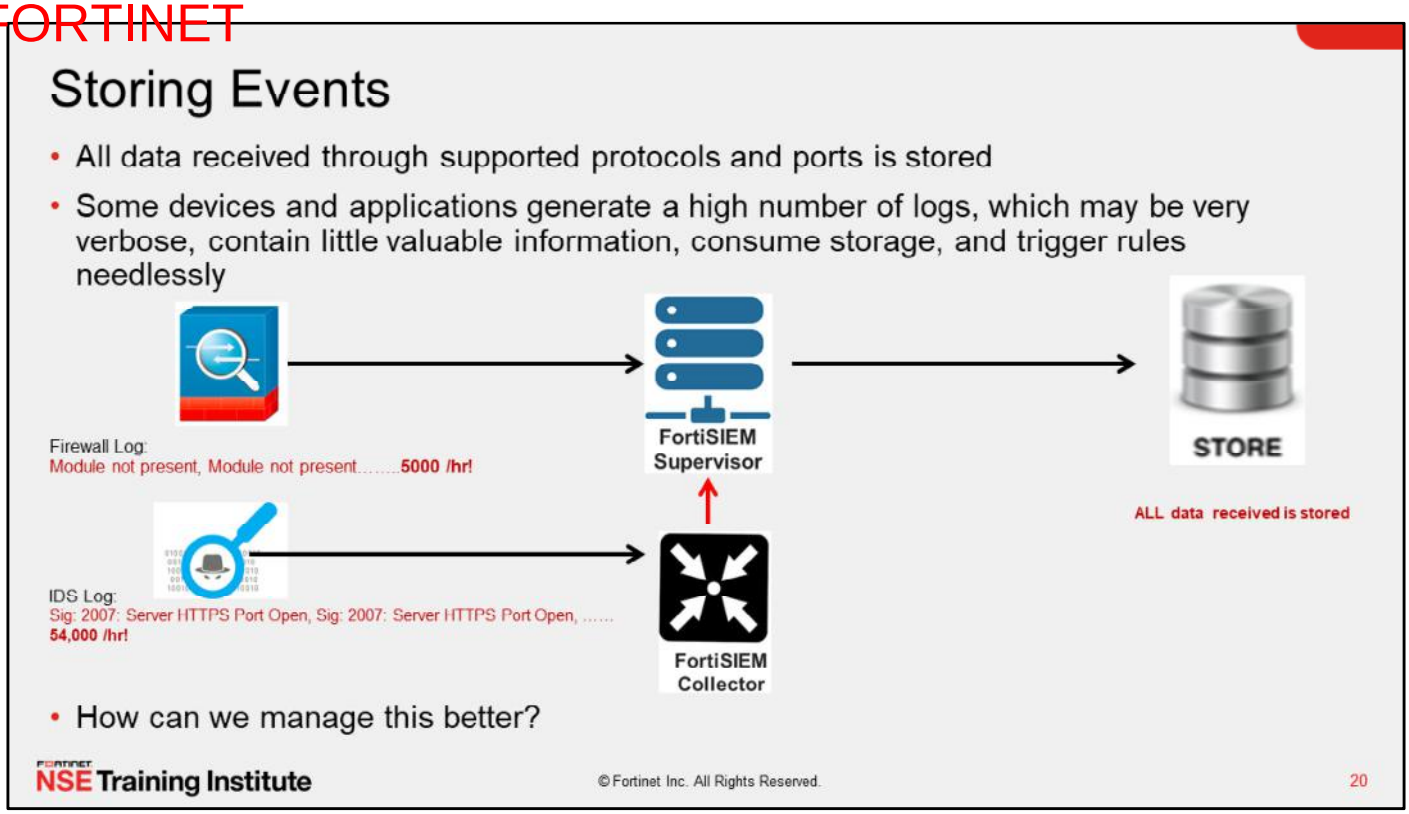
The example on this slide shows that every Friday at 6:00PM for one hour, a specific server or group of Windows devices undergoes maintenance.

When you set a schedule, you can set a single time or a recurring time.

You can also create a maintenance schedule for synthetic transaction monitors.

Vouchers & Dumps are Available | WhatsApp +201224560923

DO NOT REPRINT
© FORTINET
Brave-dumps.com



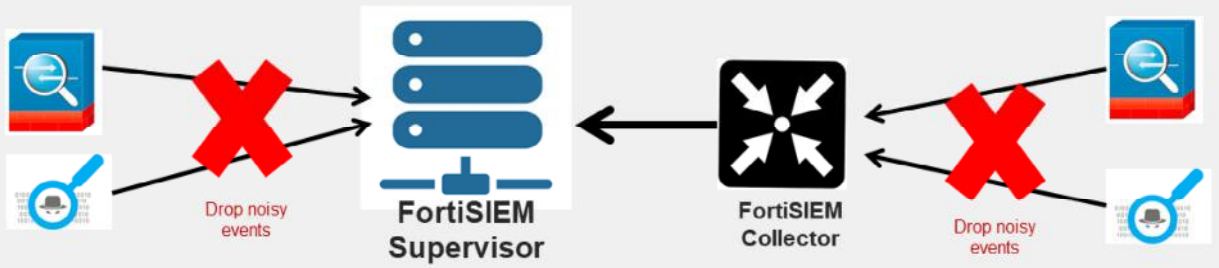
All data received by FortiSIEM through supported protocols and ports is stored, whether that data is understandable or not. However, some devices and applications generate a high number of logs, which may be very verbose, contain very little valuable information, consume storage, and trigger rules needlessly. How can you manage this better?

Vouchers & Dumps are Available | WhatsApp +201224560923

DO NOT REPRINT
© FORTINET
Brave-dumps.com

Option One—Drop Events

- FortiSIEM drops the event at the first entry point



- If your deployment doesn't use collectors, the event is dropped by the worker or supervisor where the events are received
- If your deployment uses collectors, events are dropped by the collectors

NSE Training Institute

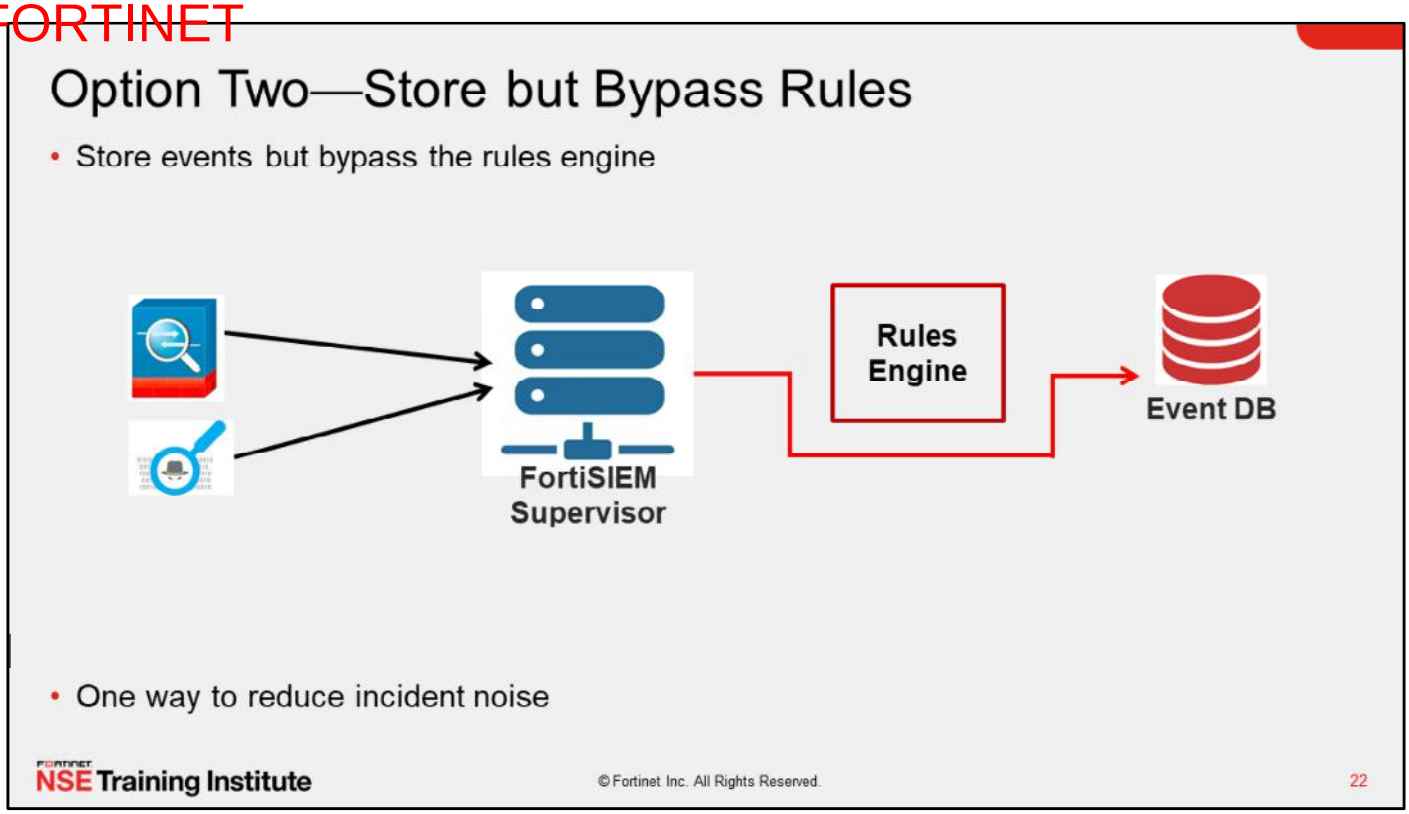
© Fortinet Inc. All Rights Reserved.

21

FortiSIEM has an event-dropping feature. This feature includes two options to help you manage needlessly noisy endpoints. The first option drops the event at the collection point. If you are sending events directly to the FortiSIEM supervisor or worker, the event can be dropped by either of them. If you are sending the events to a collector, the collector drops the events and the dropped events are not be forwarded to the FortiSIEM cluster.

Vouchers & Dumps are Available | WhatsApp +201224560923

DO NOT REPRINT
© FORTINET
Brave-dumps.com



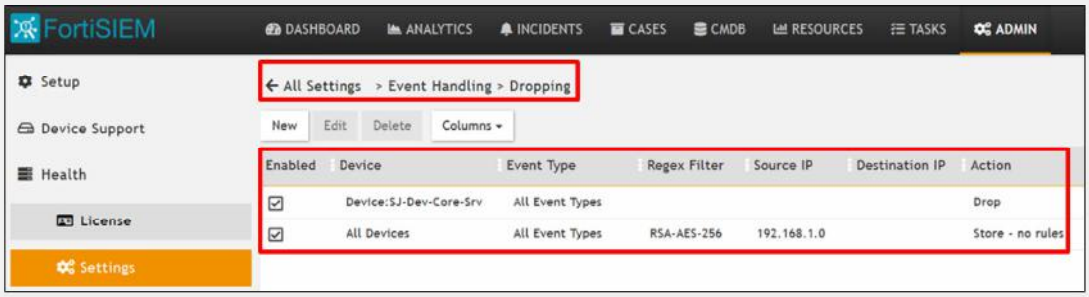
The second option is to store the messages but bypass the rules engine. Perhaps there are devices or applications sending a lot of noisy events that you need to collect for compliance purposes. But, these same events are triggering rules needlessly, over and over again. Using this option, you store the data but don't apply the rules engine to it.

Vouchers & Dumps are Available | WhatsApp +201224560923

DO NOT REPRINT
© FORTINET
Brave-dumps.com

Event Dropping Rules

- Configure event dropping rules by clicking **ADMIN** > **Settings** > **Event Handling** > **Dropping**



- Allows dropping rules for every organization or just selected organizations
- Dropped events do not count towards licensed events per second (EPS)
- Events that are stored contain event information available for searches, dashboards, and reports, but do not trigger rules

NSE Training Institute

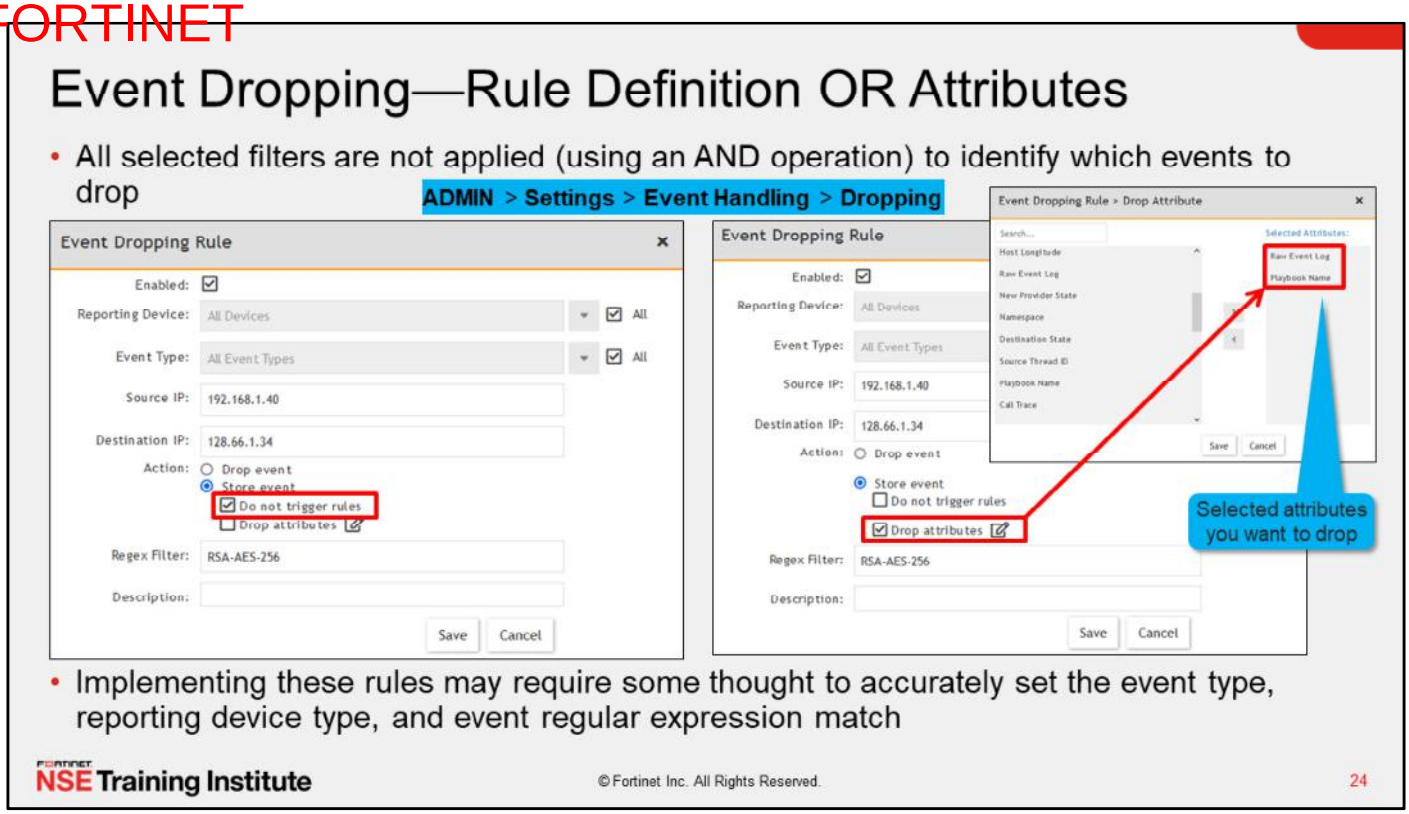
© Fortinet Inc. All Rights Reserved.

23

Configure event dropping rules by clicking **ADMIN** > **Settings** > **Event Handling** >**Dropping**. If you use the service provider edition of FortiSIEM, you can create event-dropping rules for every organization, or select organizations. If you do use the event-dropping feature, dropped events do not count toward licensed events per second (EPS). If you use the option to store the events but bypass the rules engine, this data is available for searches and dashboards, but rules based on that data are not triggered.

Vouchers & Dumps are Available | WhatsApp +201224560923

DO NOT REPRINT
© FORTINET
Brave-dumps.com



All selected filters in the event dropping rule definition are applied using an AND operation to identify which events to drop.
The options that you can set in the **Event Dropping Rule** window are:

- **Reporting Device**
  - You can select multiple devices, all, or none
- **Event Type**
  - The event type you want to drop, or whether you want to drop all events from the selected devices
- **Source IP**
- **Destination IP**
- **Action**
  - Drop the event
  - Store the event, but do not trigger rules
  - Store the event but drop selected attributes
- **Regex Filter**
  - Applies a regex filter to the message

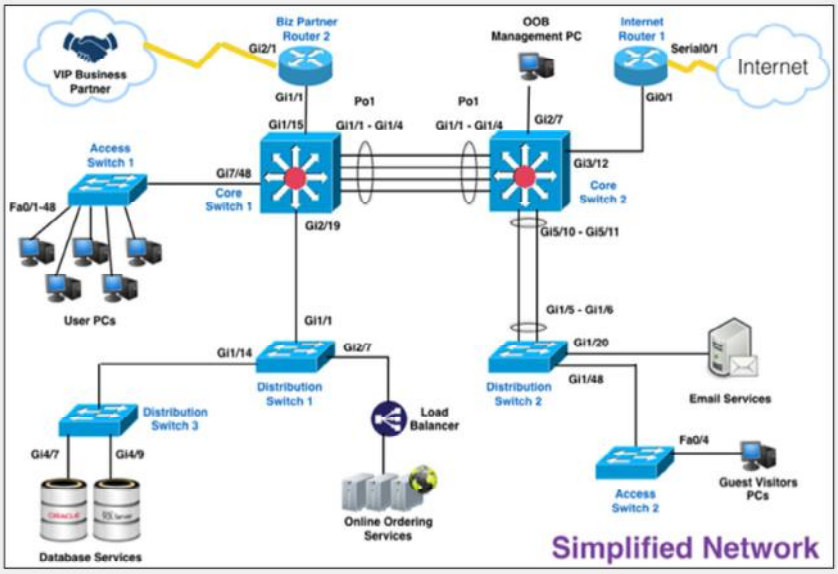
Implementing these rules may require some thought to accurately set the event type, reporting device type, and event regular expression filter. Just be careful you don't start dropping messages that you actually need to collect.

Vouchers & Dumps are Available | WhatsApp +201224560923

DO NOT REPRINT
© FORTINET
Brave-dumps.com

Host Interface Critical Flag

- Which network interfaces are important to the business?



© Fortinet Inc. All Rights Reserved.

In the next two slides, you'll learn about the host interface critical flag. The host interface critical flag is another example of where FortiSIEM can enrich network interface utilization events. The simplified network diagram shown on this slide illustrates this discussion.

The network diagram contains some core switches and a couple of routers. One router connects to the internet, and one router connects to a very important business partner. There is an access switch connecting user PCs to Core switch 1. Core switch 1 also connects to some distribution switches that, in turn, connect to some of the services being delivered to the business, such as database services, online ordering, and so on.

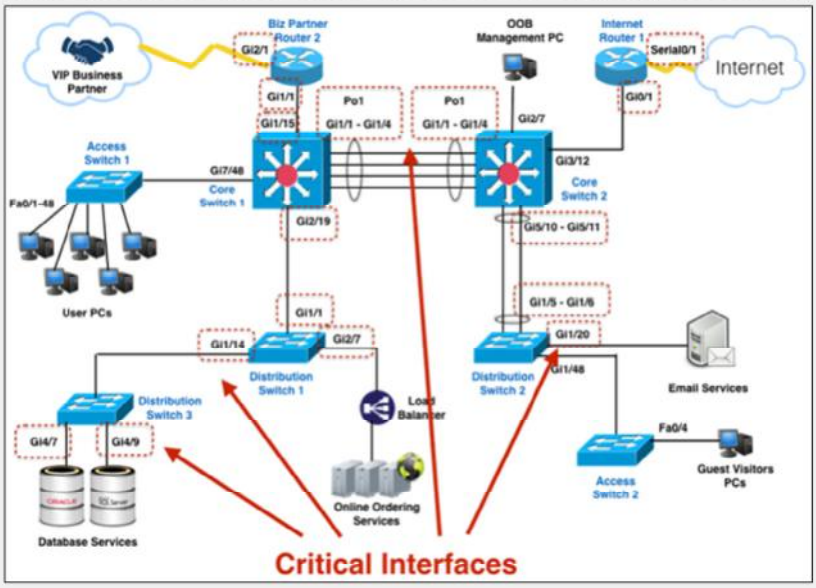
An administrator would want to identify which interfaces are important to the business.

Vouchers & Dumps are Available | WhatsApp +201224560923

DO NOT REPRINT
© FORTINET
Brave-dumps.com

Host Interface Critical Flag (Contd)

- Operators can define which interfaces on network devices are critical, which sets an attribute in events



NSE Training Institute

© Fortinet Inc. All Rights Reserved.

26

FortiSIEM allows administrators to define which interfaces on network devices are critical.

One of the attributes contained in an interface event is the host interface critical attribute. Its value is set to **No** by default. But, if an interface on a device is set as critical, then any event coming from that interface would have the host interface critical attribute set to **Yes**.

In the simplified network diagram shown on this slide, you can see that some of the interfaces have been identified as critical. Router 2, for example, has a link to the VIP business partner. If this link goes down, you want to know immediately.

If some of the core switch interfaces go down, especially the links to the distribution switches, this could take part of the network down. Similarly, the distribution switches, which have interfaces going to critical services, such as databases, are critical to the network.

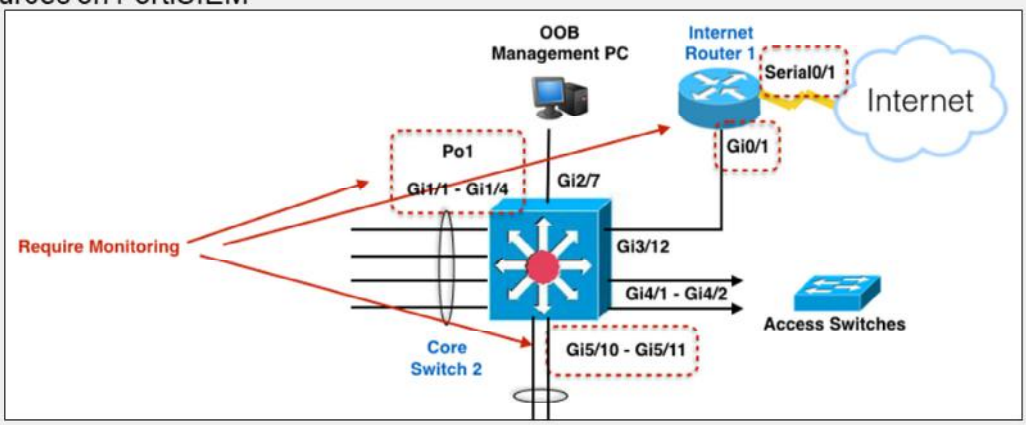
Network devices send syslog messages continuously, so when a port goes up or down, a syslog is produced. However, not all of the syslog messages are important. By identifying which interfaces are critical, you can be alerted only when a critical interface has an issue.

Vouchers & Dumps are Available | WhatsApp +201224560923

DO NOT REPRINT
© FORTINET
Brave-dumps.com

Monitoring Interfaces

- Upon discovery, all network interfaces are monitored on each device, which can consume a lot of resources on FortiSIEM



- Hence the FortiSIEM allows operators to define exactly which interfaces to monitor and IGNORE all others for each device in the CMDB

NSE Training Institute

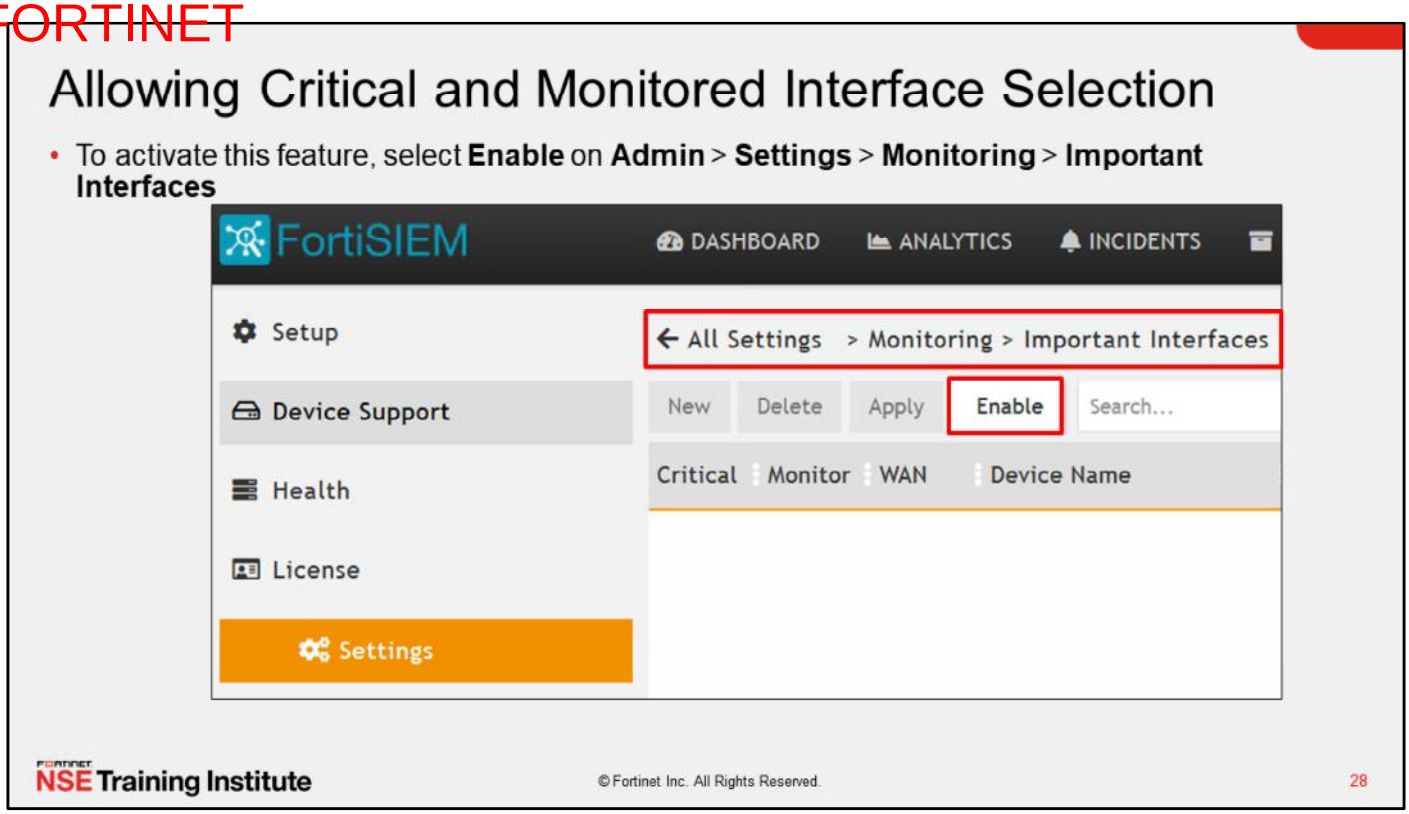
© Fortinet Inc. All Rights Reserved.

27

Upon discovery, FortiSIEM monitors all network interfaces on each device, which can consume a lot of resources on FortiSIEM.

Vouchers & Dumps are Available | WhatsApp +201224560923

DO NOT REPRINT
© FORTINET
Brave-dumps.com

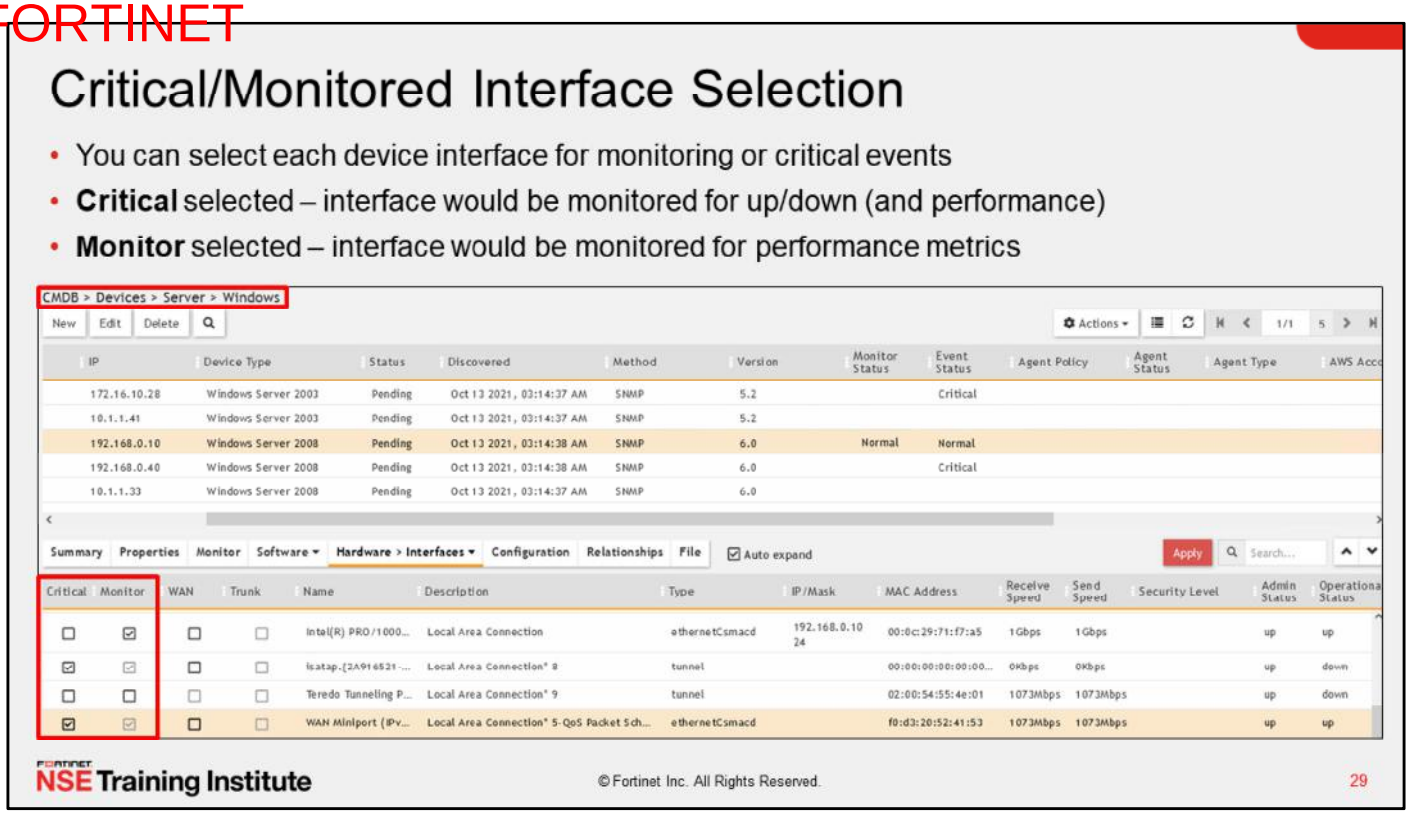


By default, this feature is disabled whether it is an upgrade or a new installation. If this feature is disabled, FortiSIEM monitors all interface utilization and up or down events.

To activate this feature, select **Enable** in **ADMIN** > **Settings** > **Monitoring** > **Important Interfaces**.

Vouchers & Dumps are Available | WhatsApp +201224560923

DO NOT REPRINT
© FORTINET
Brave-dumps.com



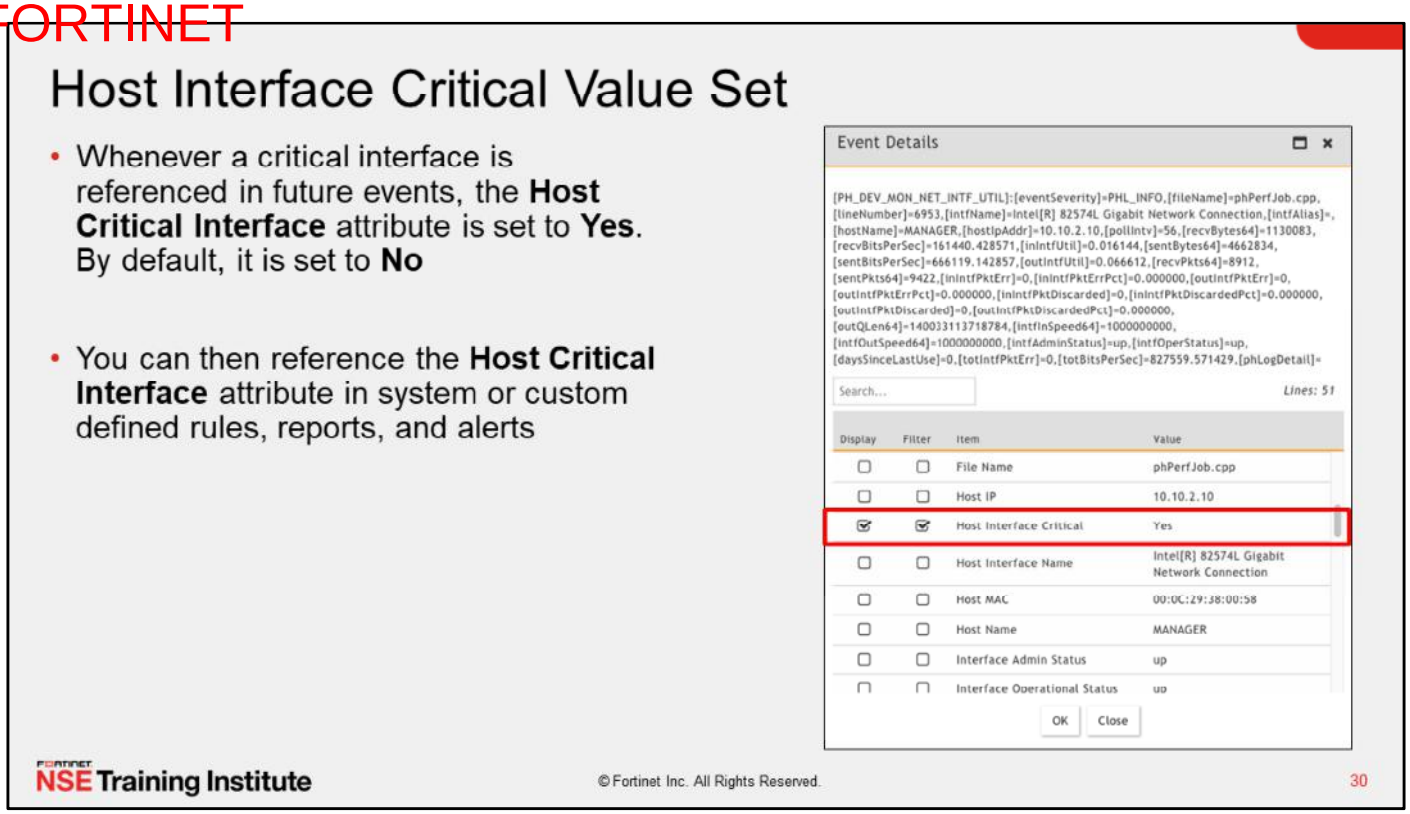
You can select each device interface for monitoring or critical events.

FortiSIEM provides two ways to set the critical interface flag on devices:
- In the CMDB, select the **Interface** tab for the device. In the **Critical** or **Monitored** column, select the **Critical or Monitor** checkbox for an important interface.
- Alternatively, click **ADMIN** > **Settings** > **Monitoring** > **Critical Interfaces**.

If you select **Critical** for an interface, FortiSIEM also monitors the interface.

Vouchers & Dumps are Available | WhatsApp +201224560923

DO NOT REPRINT
© FORTINET
Brave-dumps.com



After an interface is identified as critical, whenever that interface is referenced in future events, whether it is in a syslog message, or a performance event such as the **PH_DEV_MON_NET_INTF_UTIL**, FortiSIEM enriches the events by setting the **Host Critical Interface** attribute to **Yes**. Otherwise, this attribute has the default value of **No**.

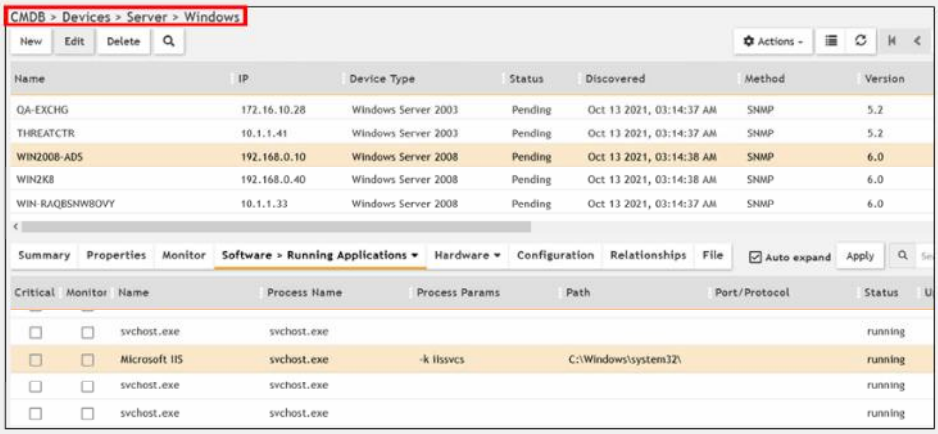
You can then reference this attribute in any of the out-of-box, or custom, rules and alerts.

Vouchers & Dumps are Available | WhatsApp +201224560923

DO NOT REPRINT
© FORTINET
Brave-dumps.com

Process Monitoring After Discovery

- By default, FortiSIEM monitors all running processes on a server device upon discovery, even if only one or two processes are required, which can consume a significant amount of system resources



- Hence, FortiSIEM allows operators to define exactly which processes to monitor and *ignore* all others for each server device

NSE Training Institute

© Fortinet Inc. All Rights Reserved.

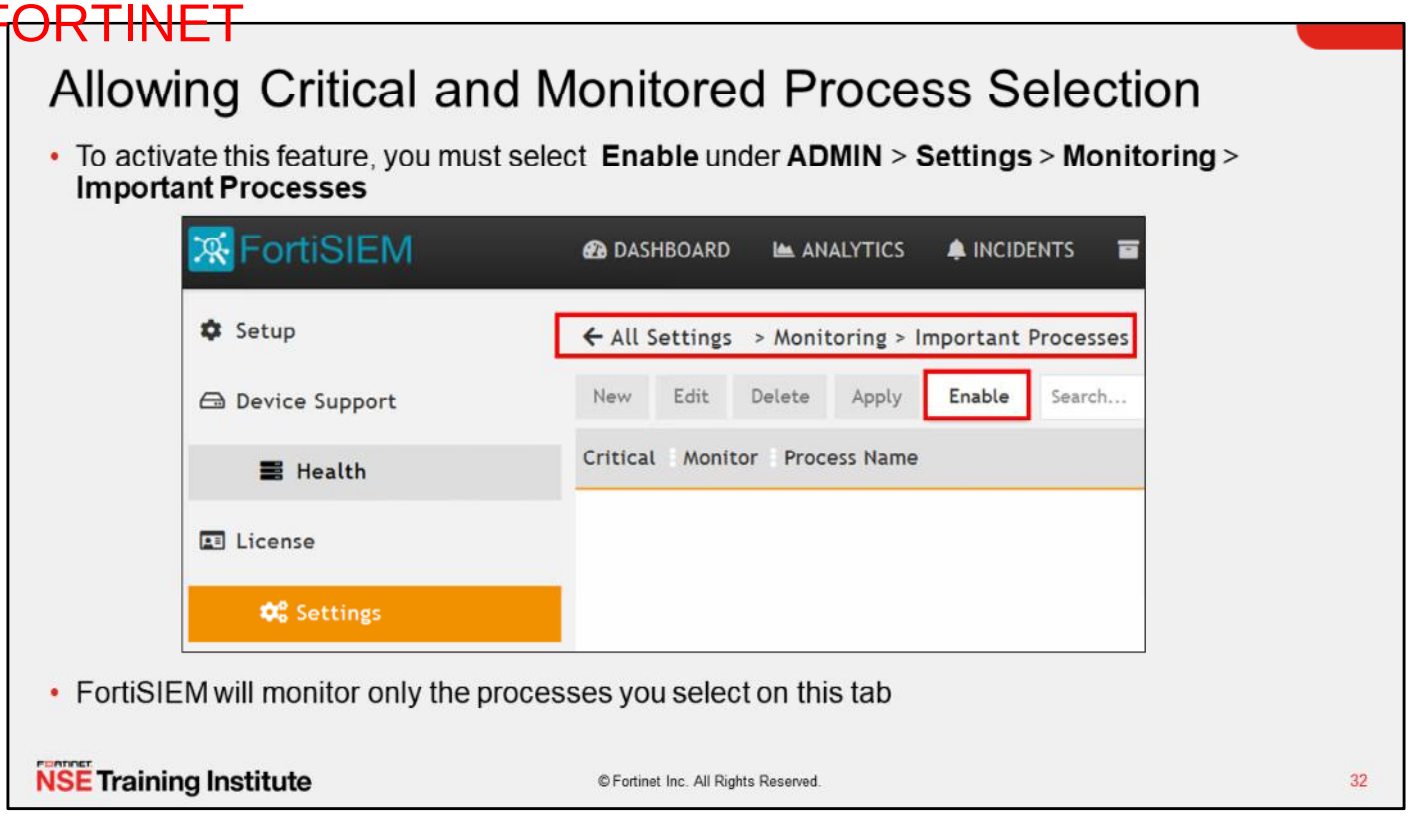
31

By default, FortiSIEM monitors all running processes on a server device upon discovery, even if only one or two processes are required, which can consume a significant amount of system resources.

Hence, FortiSIEM allows operators to define exactly which processes to monitor and *ignores* all others for each server device.

Vouchers & Dumps are Available | WhatsApp +201224560923

DO NOT REPRINT
© FORTINET
Brave-dumps.com

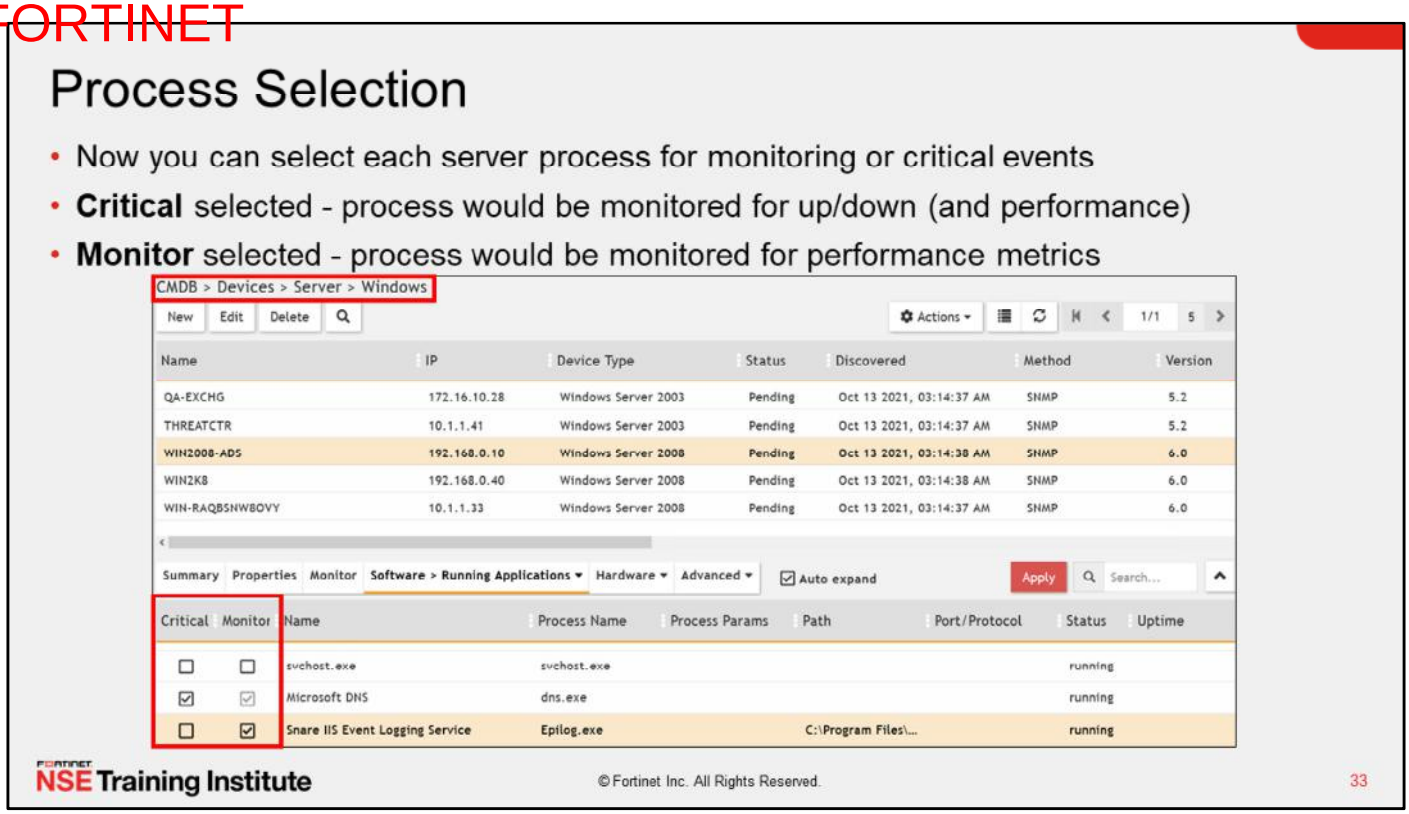


To activate this feature, you must select **Enable** under **ADMIN**> **Settings** > **Monitoring** > **Important Processes**.

FortiSIEM monitors only the processes you select on this tab.

Vouchers & Dumps are Available | WhatsApp +201224560923

DO NOT REPRINT Brave-dumps.com
© FORTINET



Now, you can select each server process for monitoring or critical events.

- **Critical** selected - process would be monitored for up/down (and performance)
- **Monitor** selected - process would be monitored for performance metrics

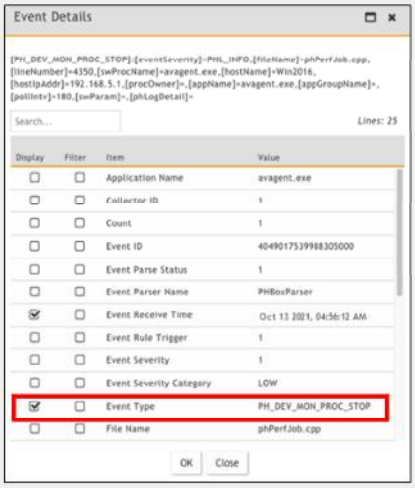
If you select **Critical** for a process, the system also monitors the process.

Vouchers & Dumps are Available | WhatsApp +201224560923

DO NOT REPRINT Brave-dumps.com
© FORTINET

Important Processes Events

- When you identify an important process, FortiSIEM produces the following events:





- Rules and alerts can reference when a process STOPS or STARTS

NSE Training Institute © Fortinet Inc. All Rights Reserved. 34

When you define an important process on a server, FortiSIEM produces the following events:

- **PH_DEV_MON_PROC_STOP** when a process **STOPS** on a system
- **PH_DEV_MON_PROC_START** when a process **STARTS** on a system

Rules and alerts can then reference these attributes.

Vouchers & Dumps are Available | WhatsApp +201224560923

DO NOT REPRINT
© FORTINET
Brave-dumps.com

Knowledge Check

1. What determines the status fields in the CMDB (normal, warning, critical)?
   - ✓ A. Global thresholds
   - B. Reporting device

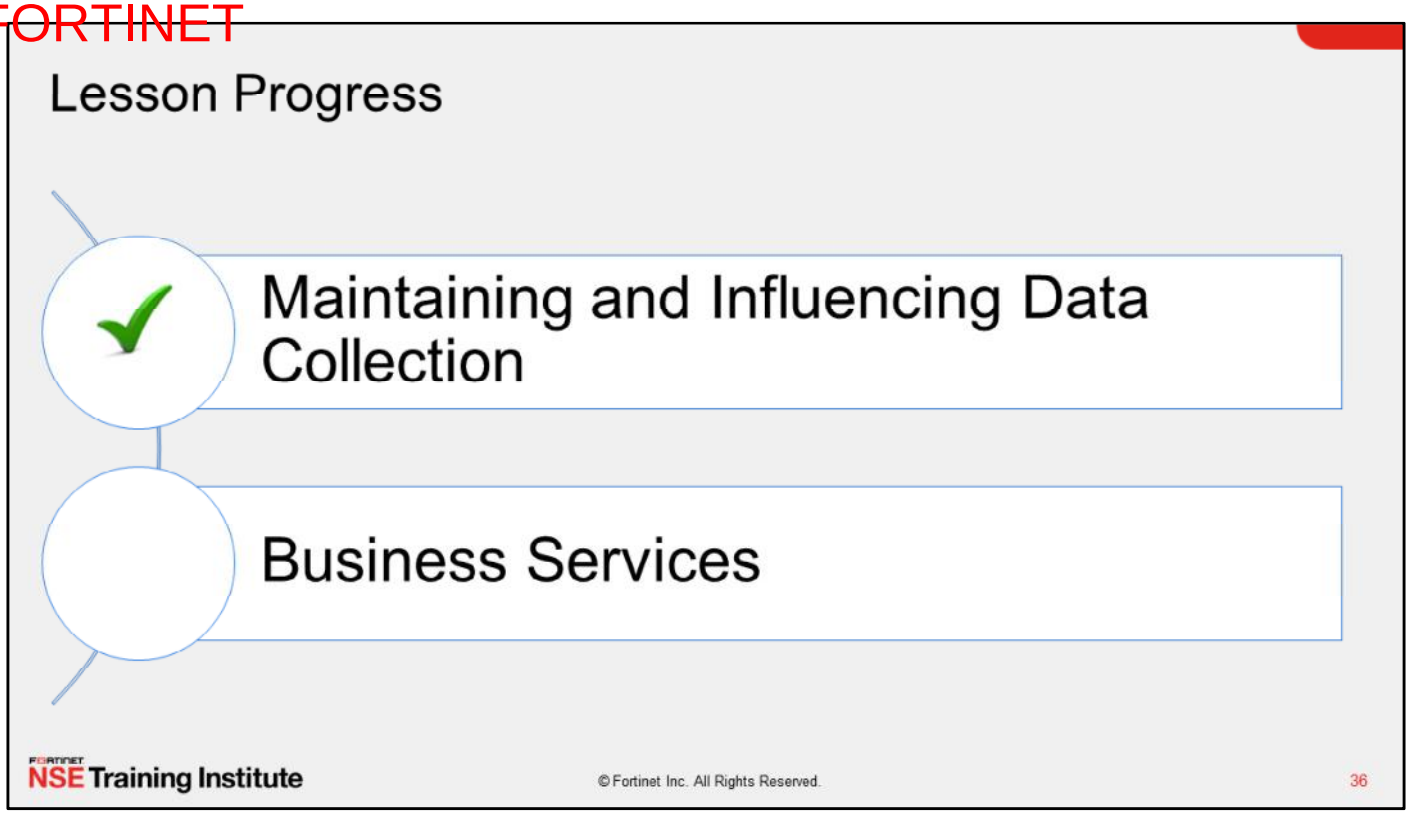
NSE Training Institute

© Fortinet Inc. All Rights Reserved.

35

Vouchers & Dumps are Available | WhatsApp +201224560923

DO NOT REPRINT
© FORTINET
Brave-dumps.com

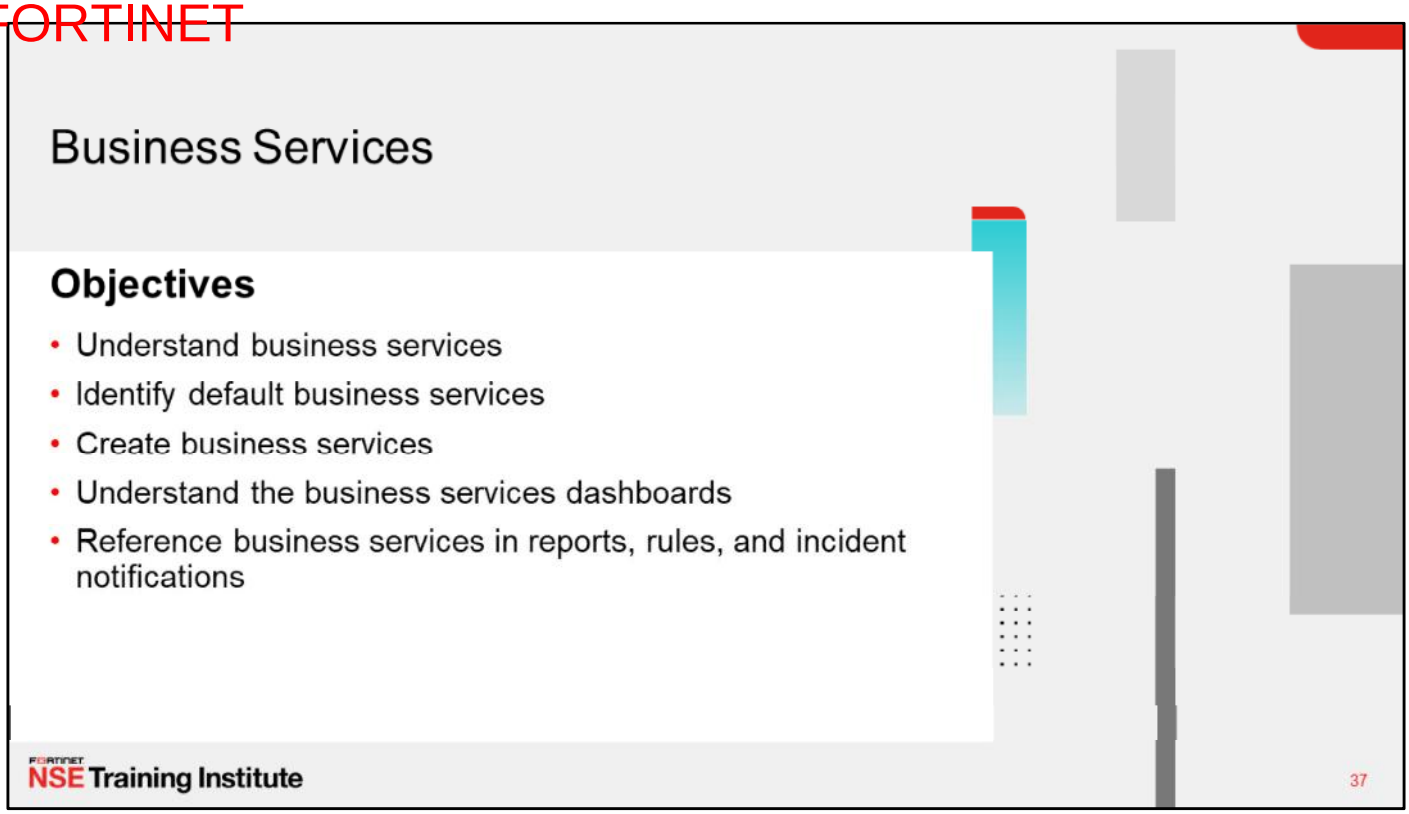


Good job! You now understand how to maintain and influence data collection.

Now, you will examine business services.

Vouchers & Dumps are Available | WhatsApp +201224560923

DO NOT REPRINT
© FORTINET
Brave-dumps.com



After completing this section, you should be able to achieve the objectives shown on this slide.

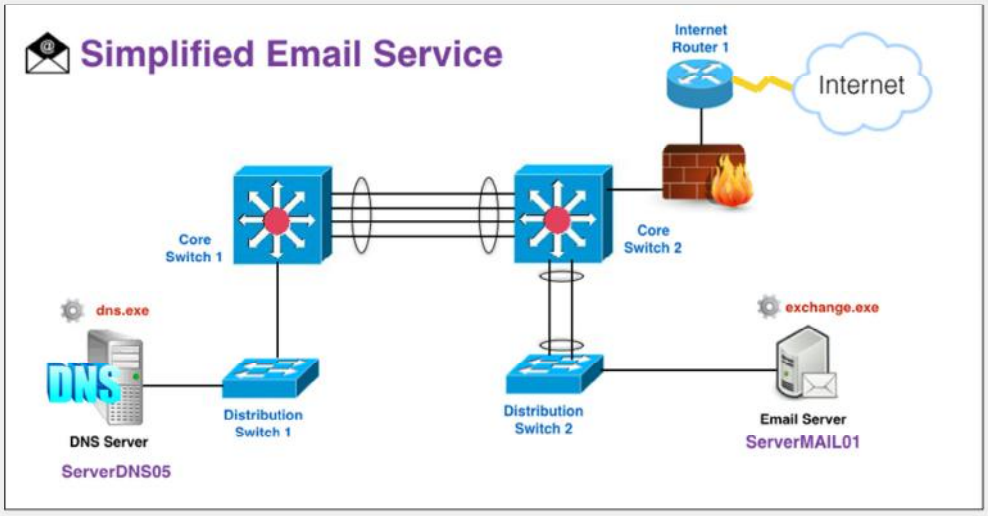
By demonstrating competence in business services, you will be able to track service-level metrics, efficiently respond to incidents on a prioritized basis, record business impact, provide business intelligence on IT best practices, report on compliance, and improve IT services.

Vouchers & Dumps are Available | WhatsApp +201224560923

DO NOT REPRINT
© FORTINET
Brave-dumps.com

Scenario: Business Services Simplified Network

- Consider a simple network with routers, switches, and servers
- What happens to the email service delivery If…



NSE Training Institute

© Fortinet Inc. All Rights Reserved.

38

FortiSIEM has a feature called Business Services, but before you examine the details of this feature, look at a scenario first that helps illustrate the feature.

Consider a really simple network with a number of routers, switches, and servers, which are the devices that are delivering an email service to a business.

If you look at the example shown on this slide, you can see an email server and that is running the `exchange.exe` service. Emails rely on DNS, so there is also a separate DNS server running the `dns.exe` service.

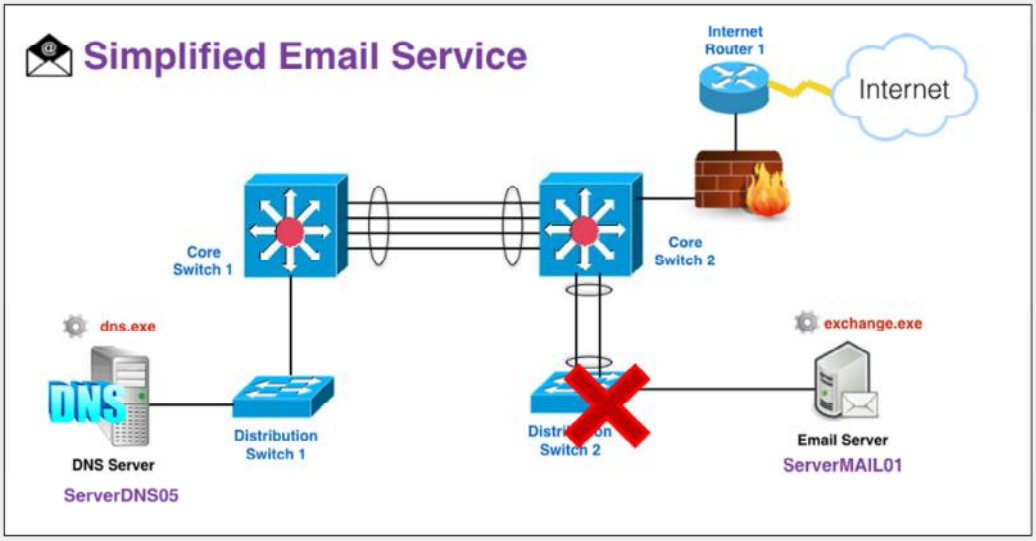
There are also a couple of core switches and a router that connects to the internet.

Vouchers & Dumps are Available | WhatsApp +201224560923

DO NOT REPRINT
© FORTINET
Brave-dumps.com

Scenario: Business Services Simplified Network—PSU Failure

- What happens if the PSU on Distribution Switch 2 fails?



NSE Training Institute

© Fortinet Inc. All Rights Reserved.

39

What happens to the email delivery if the power supply fails on Distribution Switch 2?

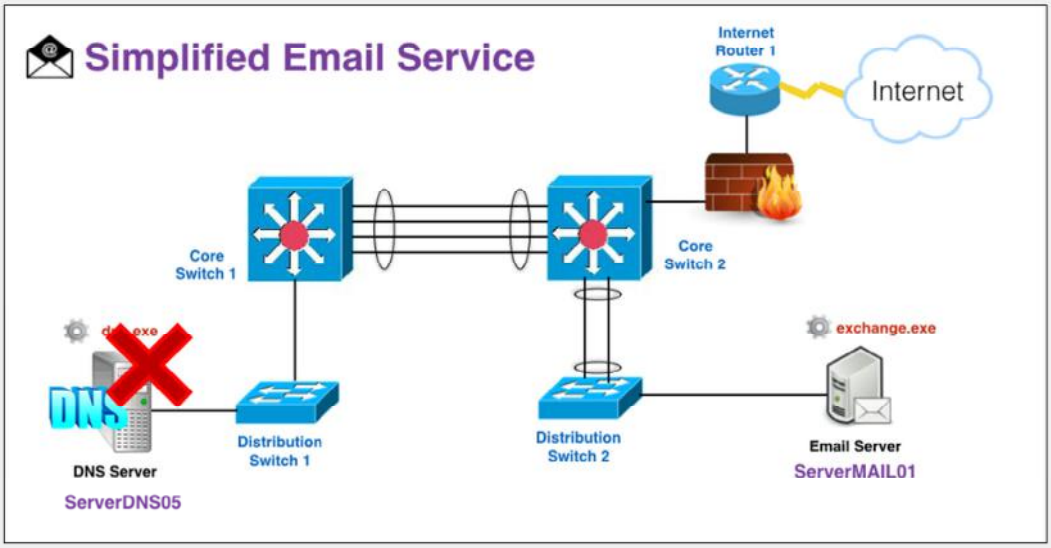
Obviously, if the power supply for that distribution switch fails, then network communications to the email server fails, and the service delivery for the email is impacted.

Vouchers & Dumps are Available | WhatsApp +201224560923

DO NOT REPRINT
© FORTINET
Brave-dumps.com

Scenario: Business Services Simplified Network—DNS Process

- What happens the DNS process hangs on ServerDNS05?



NSE Training Institute

© Fortinet Inc. All Rights Reserved.

40

What happens if the DNS service fails on the DNS server?

If the DNS process fails, then obviously DNS queries cannot be resolved anymore, which affects the email service delivery to the business.

While internal email may continue to work, your external emails fail.

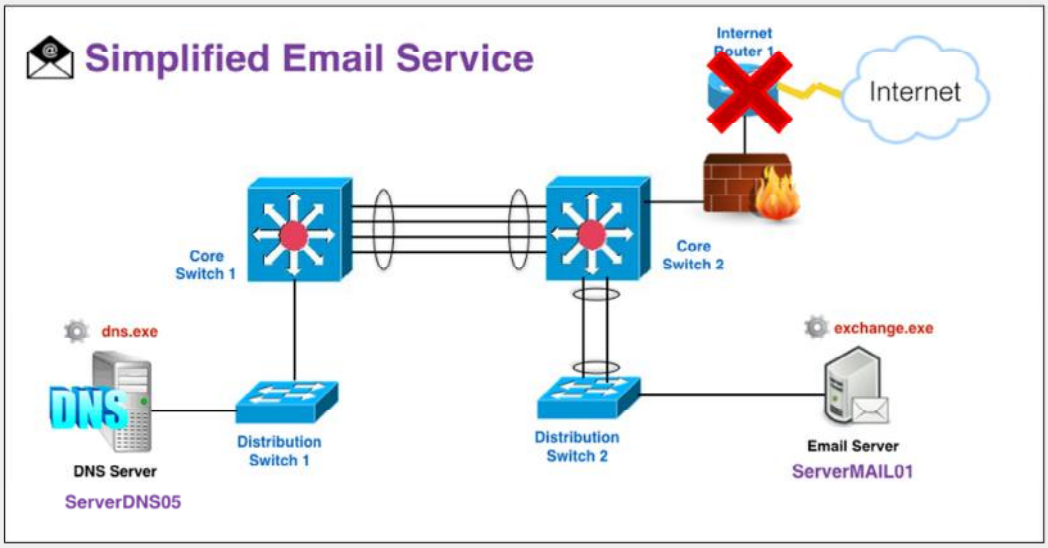
Again, a DNS service failure impacts the email service delivery to the business.

Vouchers & Dumps are Available | WhatsApp +201224560923

DO NOT REPRINT
© FORTINET
Brave-dumps.com

Scenario: Business Services Simplified Network—Router Failure

- What happens if the internet router fails?



NSE Training Institute
© Fortinet Inc. All Rights Reserved.
41

What happens if the internet router fails?

Whether it is the device itself, or whether it is the link that the internet connection is provided over, if the router or connection fails then any external email is not delivered.

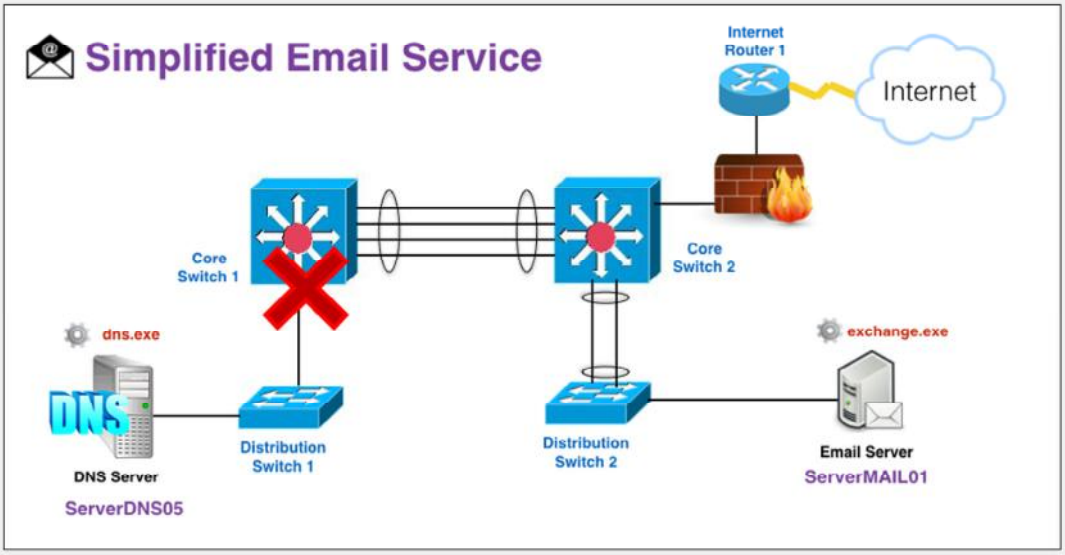
Once again, an internet router failure impacts service delivery for the email service.

Vouchers & Dumps are Available | WhatsApp +201224560923

DO NOT REPRINT
© FORTINET
Brave-dumps.com

Scenario: Business Services Simplified Network—Interface Fault

- What happens if the uplink interface on Core Switch 1 degrades with packet errors?



NSE Training Institute

© Fortinet Inc. All Rights Reserved.

42

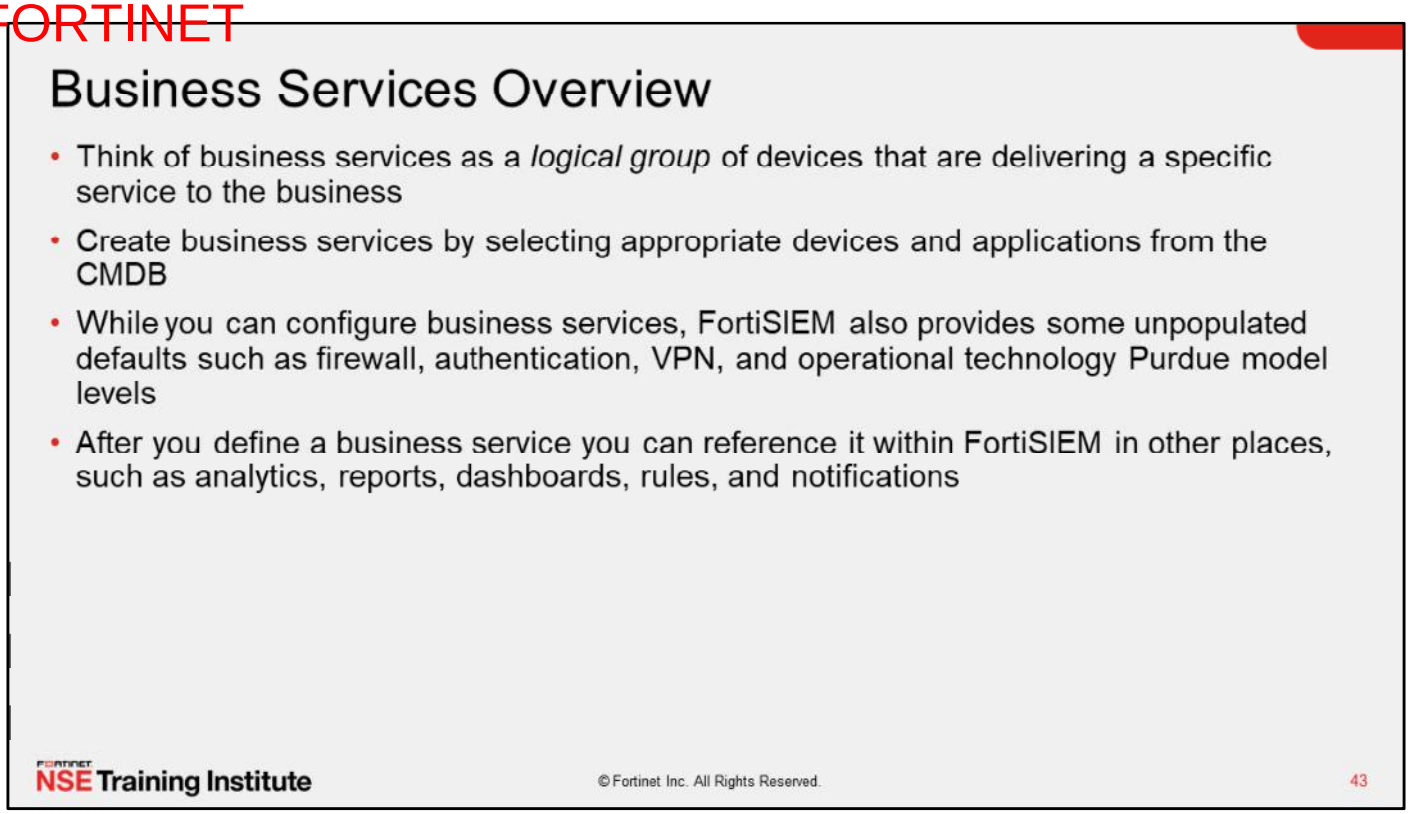
What happens if the uplink interface on Core Switch 1, which connects to Distribution Switch 1, degrades with several packet errors?

This will have an impact on the email service because the DNS server may not be available.

As a service within FortiSIEM, there are several devices, applications, and components that make up a service.

Vouchers & Dumps are Available | WhatsApp +201224560923

DO NOT REPRINT
© FORTINET
Brave-dumps.com



In FortiSIEM, think of a business a *logical group* of devices that are delivering a specific service to the business.

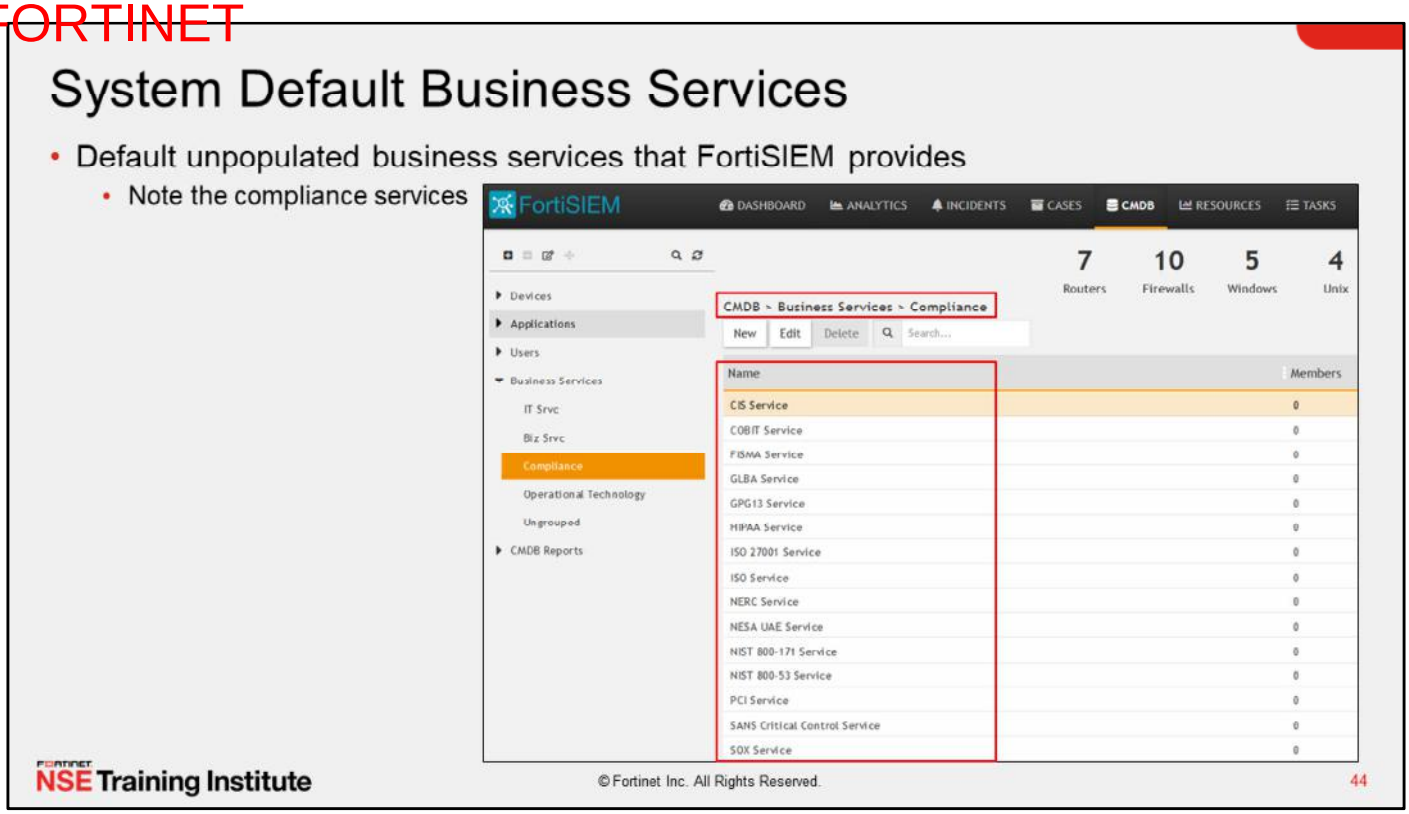
You create business services by selecting appropriate devices and applications from the CMDB.

While services are configurable by an administrator, FortiSIEM also provides some unpopulated default groups, such as the firewall business service, authentication business service, and VPN business service in which administrators can manually define which of their devices belong to those services.

After you define a service, you can reference it elsewhere within FortiSIEM in other places, such as, analytics, reports, dashboards, rules, and notifications.

Vouchers & Dumps are Available | WhatsApp +201224560923

DO NOT REPRINT Brave-dumps.com
© FORTINET



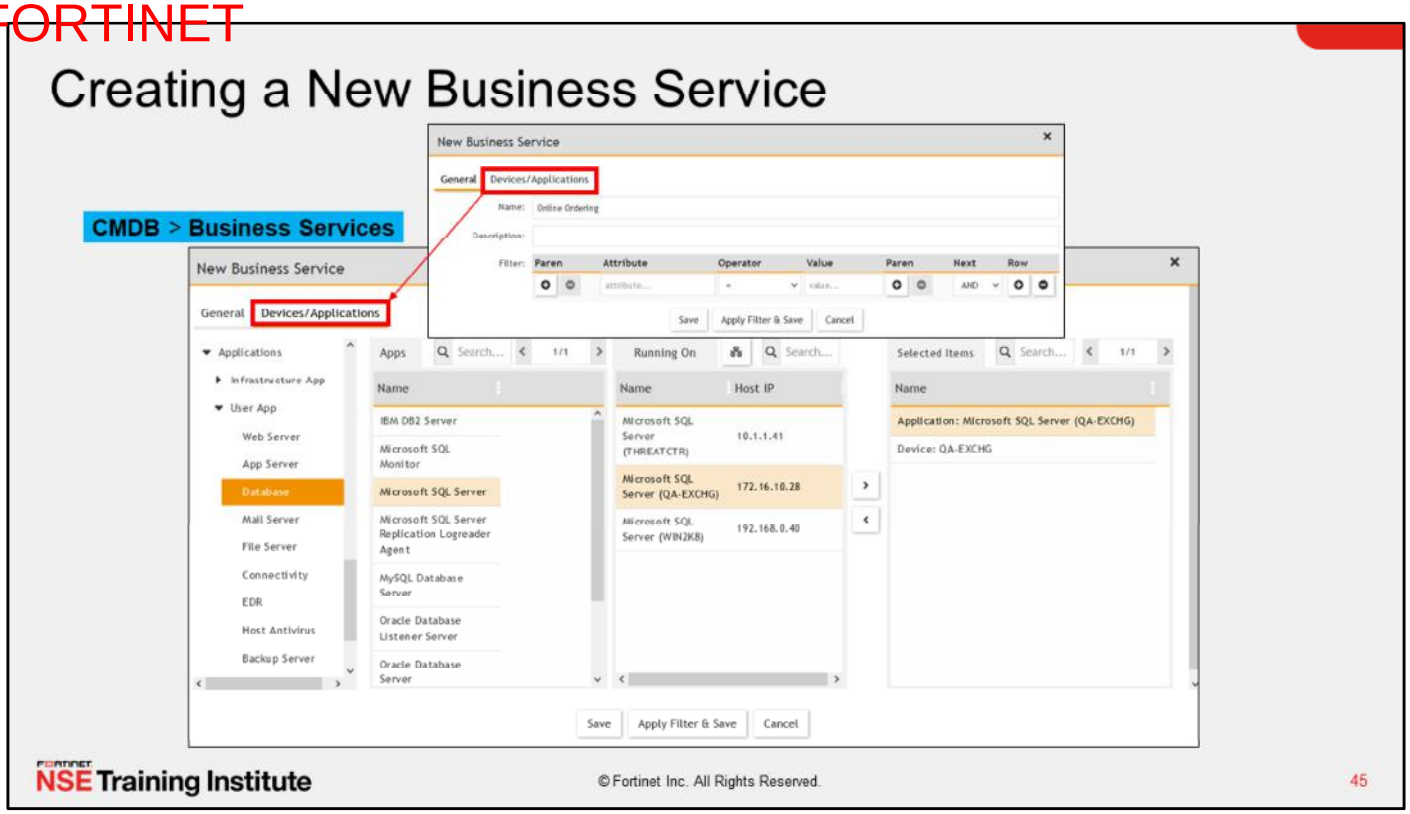
FortiSIEM provides a number of unpopulated default business services groups.

As you can see, there are a few services for compliance purposes, such as FISMA Services, HIPPA, GPG13, NERC, and PCI.

Any administrator can manually add devices, such as firewalls to the firewall service, DHCP and DNS servers to the DHCP/DNS services, or any of your PCI devices to the PCI service, and so on.

Vouchers & Dumps are Available | WhatsApp +201224560923

DO NOT REPRINT Brave-dumps.com
© FORTINET



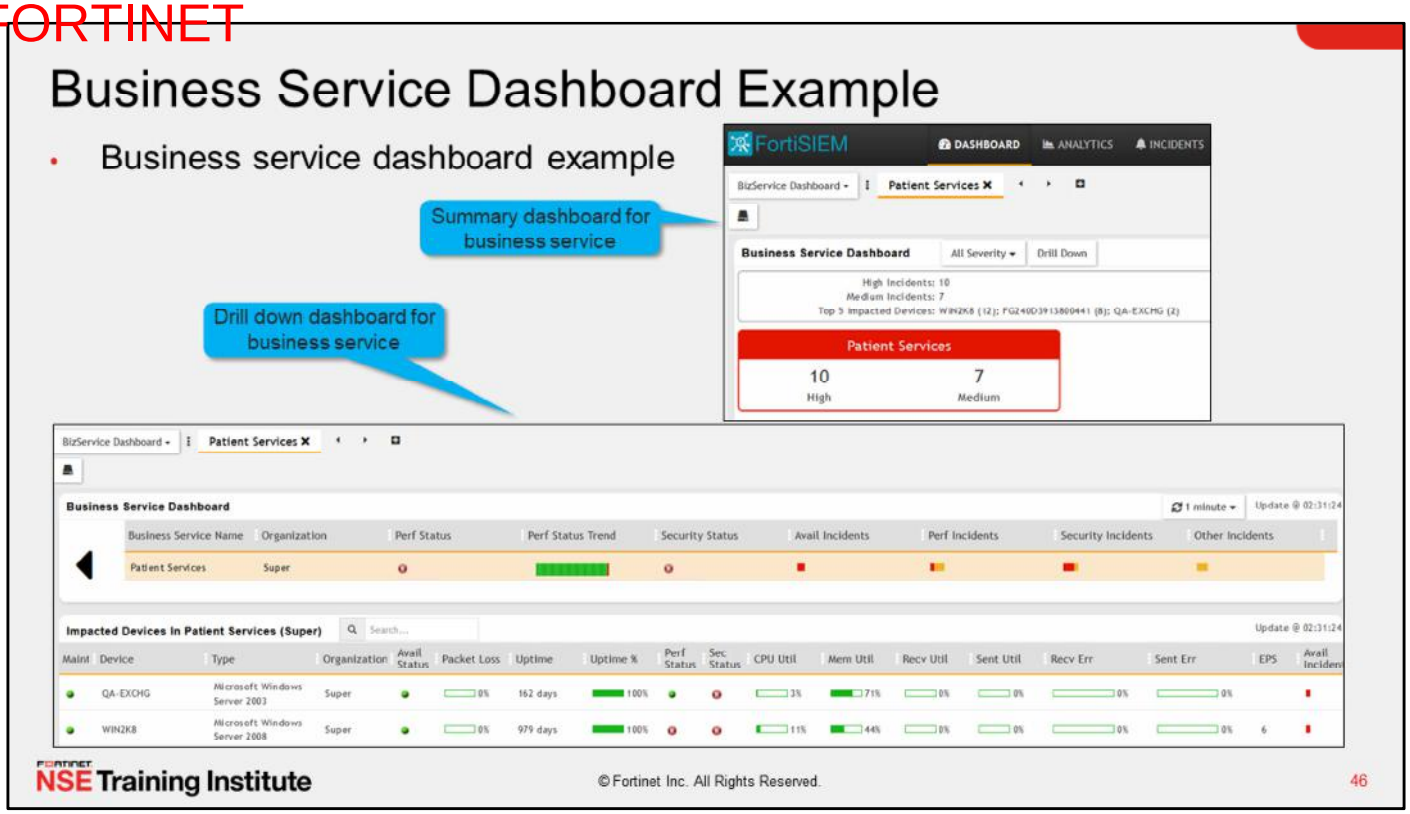
You can configure business services under the **CMDB** > **Business Services**.

Click **New**. A New **Business Service** window opens. Here, you give the business service a name and an optional description. Then, you select individual devices or devices running a particular application from the CMDB Tree and add them to the **Selected Devices/Applications** column.

Note the L2/L3 network devices section at the bottom of the example shown on this slide. If you discover any Layer 2 or Layer 3 devices within your environment, the system lists any of these network devices that are adjacent to any of the devices you have selected for this group. This gives you the option to add those network devices to the business service group.

Vouchers & Dumps are Available | WhatsApp +201224560923

DO NOT REPRINT Brave-dumps.com
© FORTINET



This slide shows an example of a business service dashboard.

Business service dashboards provide a top-down view of business service health. You can see the incidents related to each business service and then drill-down into the impacted devices and incidents.

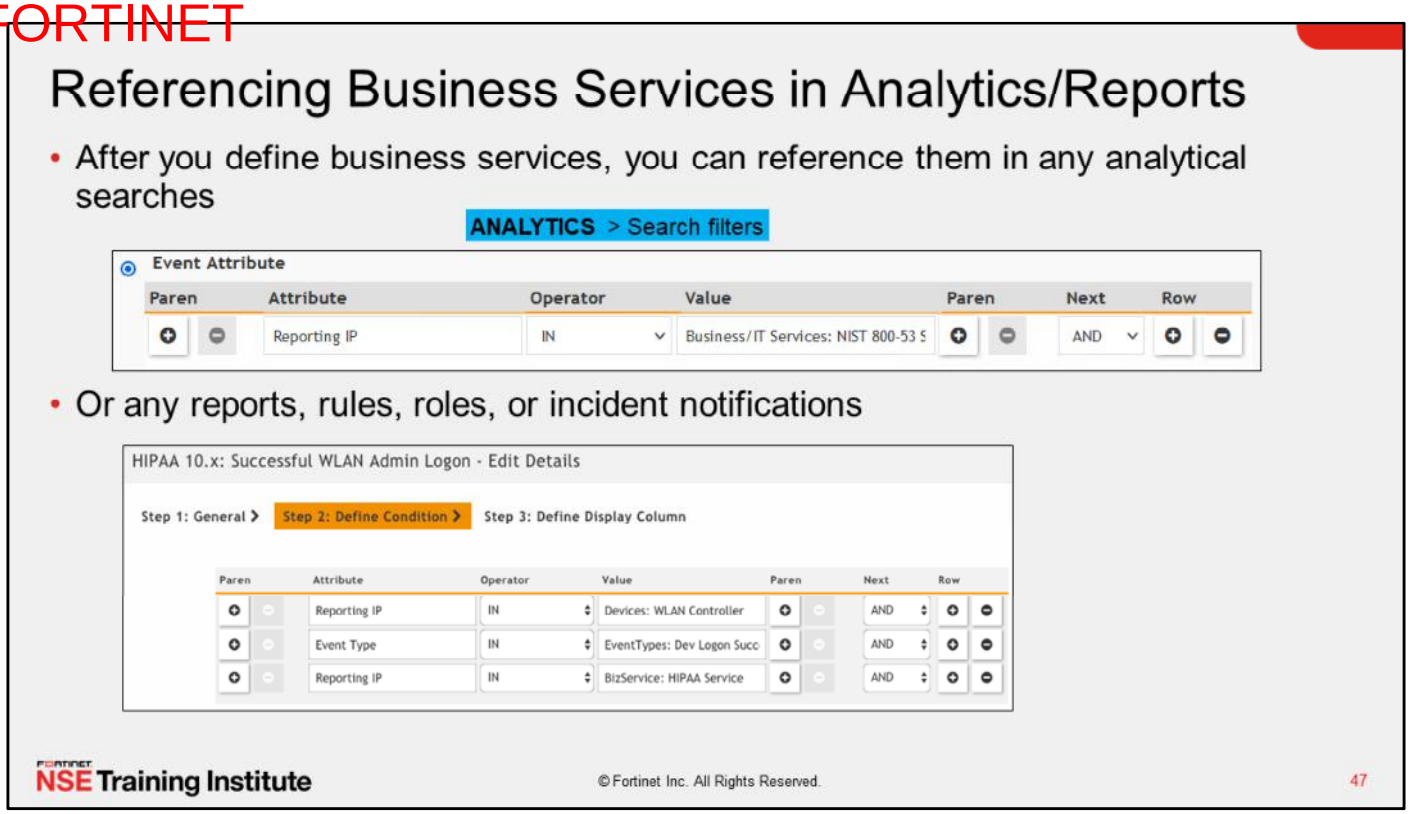
You need to manually create a new dashboard group for a business service, and then create a business service dashboard in the custom dashboard group.

You can also add a business service dashboard for your business service in predefined functional dashboard groups.

The example on this slide shows a dashboard group you added called **BizService Dashboard.** Then you created a business service dashboard named **Patient Services.**

Vouchers & Dumps are Available | WhatsApp +201224560923

DO NOT REPRINT
© FORTINET
Brave-dumps.com



After you define business services, you can reference them in any of the analytical searches.

To reference business services, identify the reporting IP, use the operator IN, and then choose the particular business service from the CMDB.

You can also reference business services in any report because, after all, reports are just searches. The same goes for rules, roles, or incident reports.

Vouchers & Dumps are Available | WhatsApp +201224560923

DO NOT REPRINT
© FORTINET
Brave-dumps.com

Knowledge Check

1. Which services are system-defined business services?
   - A. Ordering online services
   - ✓ B. PCI service
   - C. Patient services

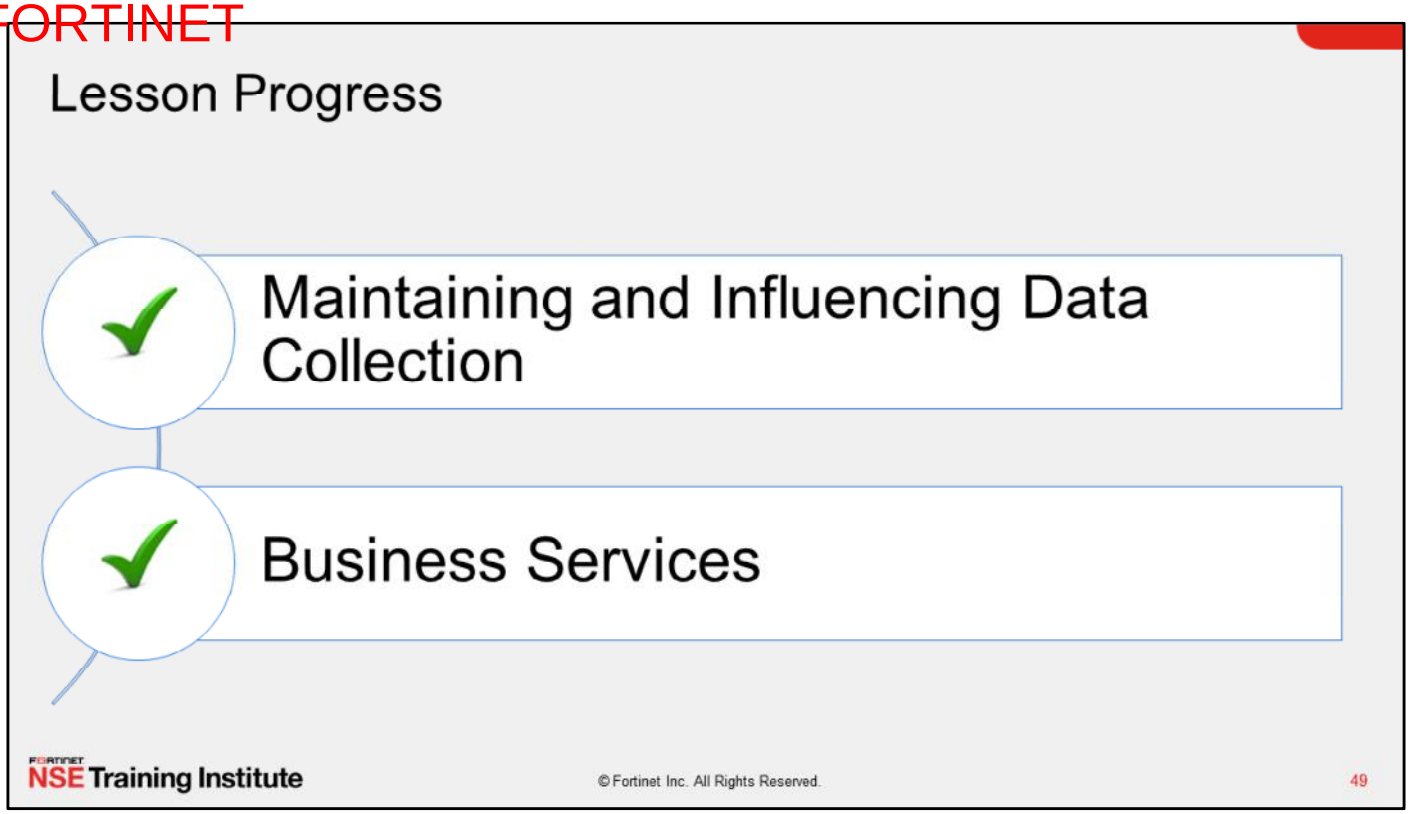
NSE Training Institute

© Fortinet Inc. All Rights Reserved.

48

Vouchers & Dumps are Available | WhatsApp +201224560923

DO NOT REPRINT
© FORTINET
Brave-dumps.com

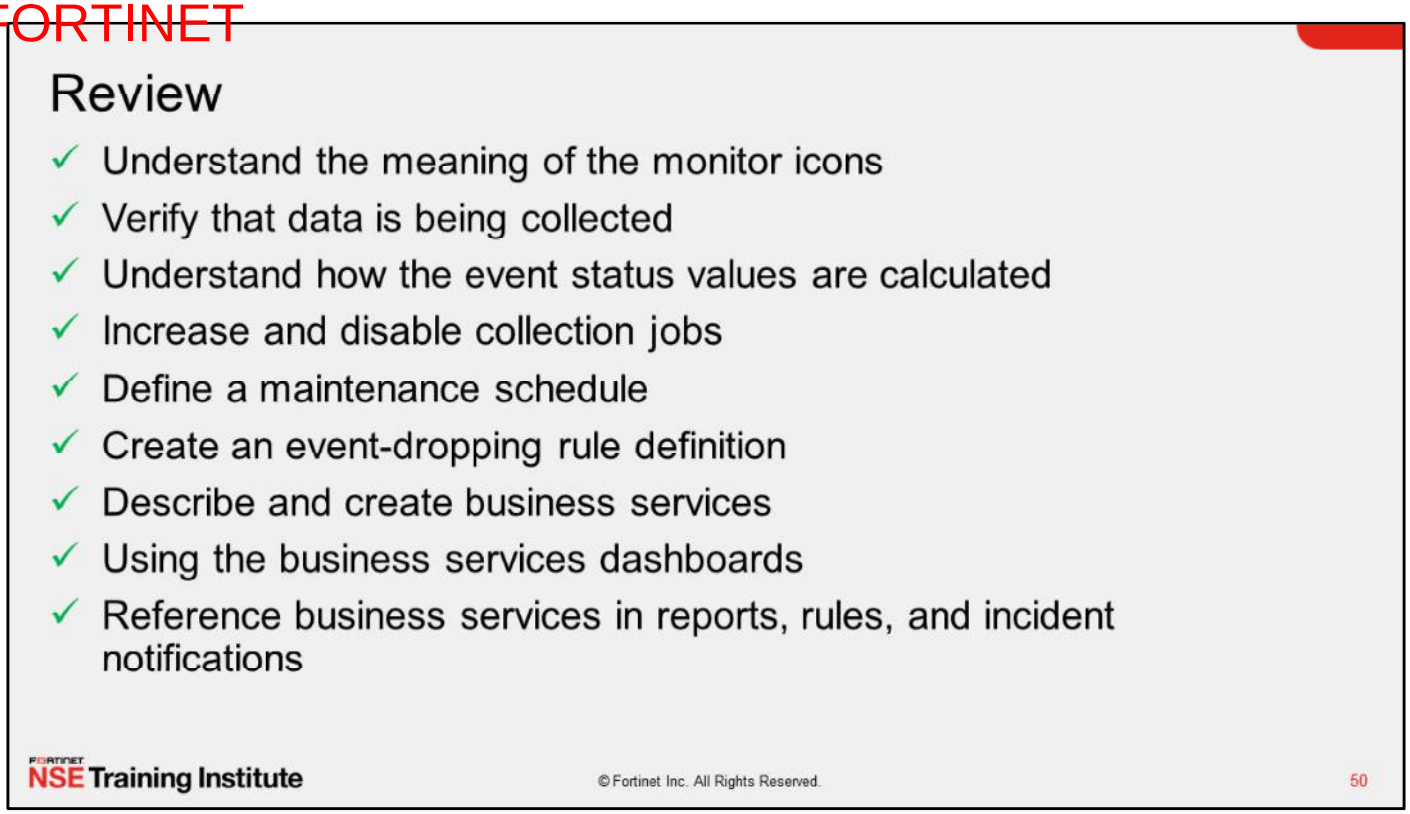


Congratulations! You have completed this lesson.

Now, you will review the objectives that you covered in this lesson.

Vouchers & Dumps are Available | WhatsApp +201224560923

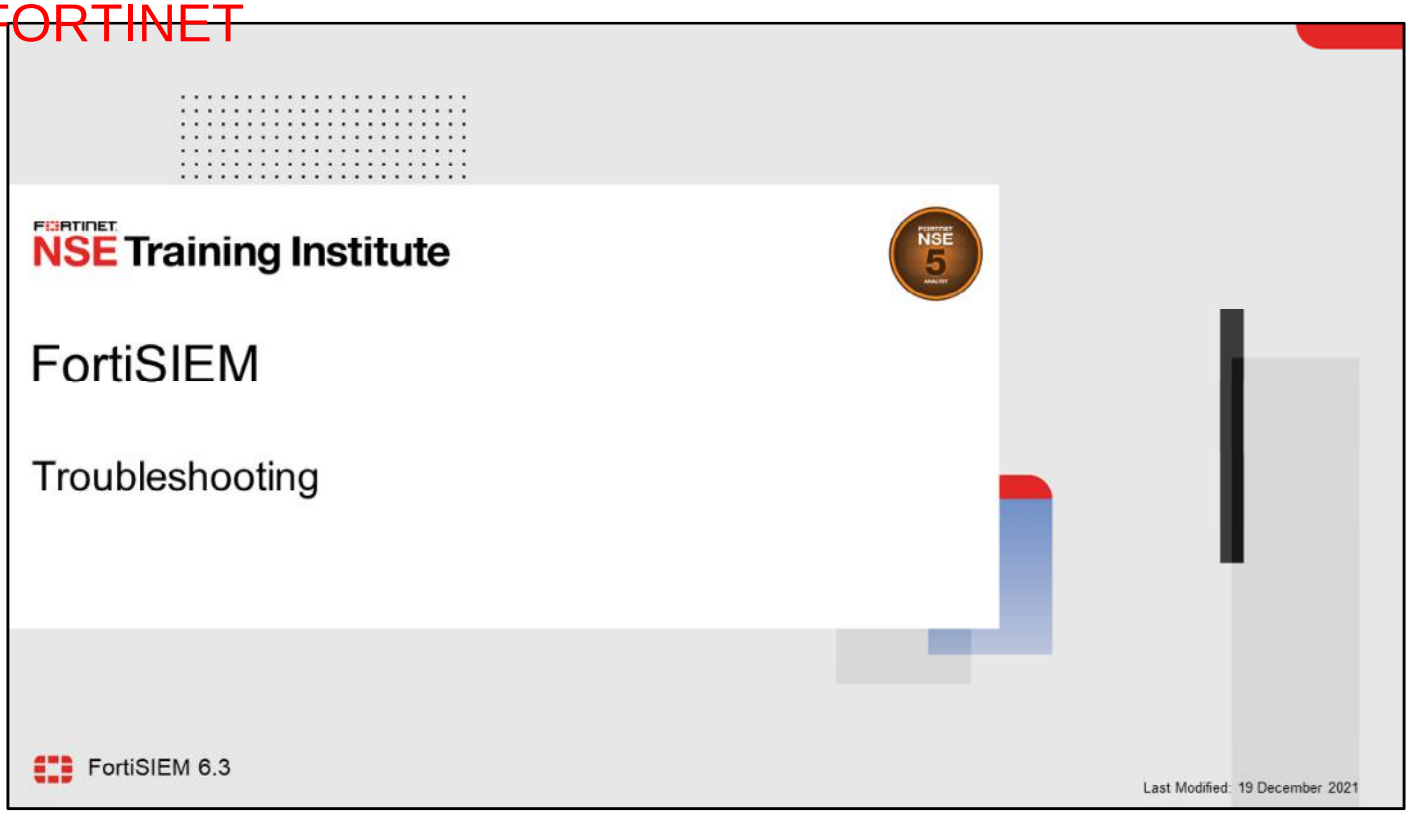
DO NOT REPRINT
© FORTINET
Brave-dumps.com



This slide shows the objectives that you covered in this lesson.

Vouchers & Dumps are Available | WhatsApp +201224560923

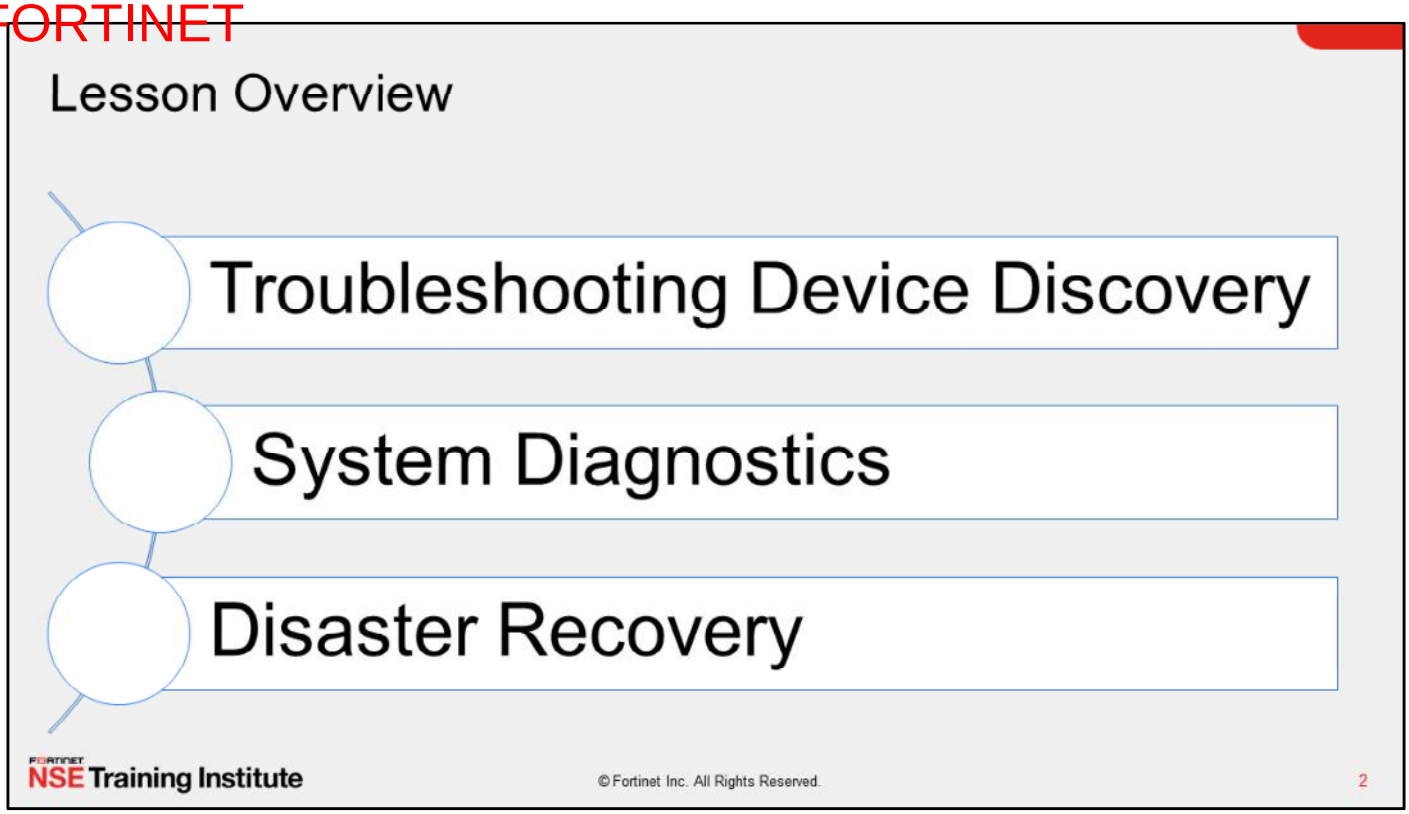
DO NOT REPRINT
© FORTINET
Brave-dumps.com



In this lesson, you will learn about FortiSIEM diagnostic commands and troubleshooting tools. You will also learn about the disaster recovery feature.

Vouchers & Dumps are Available | WhatsApp +201224560923

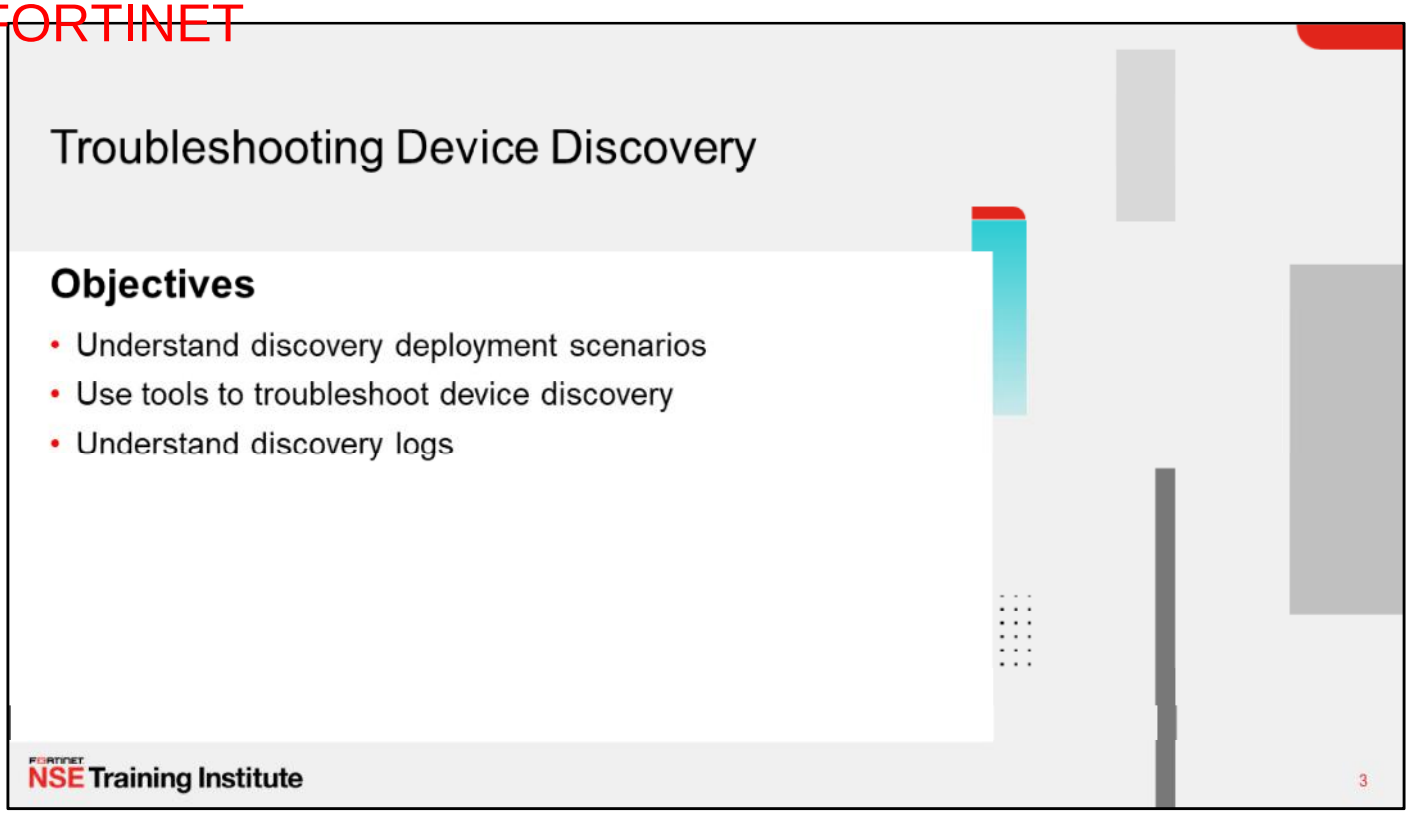
DO NOT REPRINT
© FORTINET
Brave-dumps.com



In this lesson, you will learn about the topics shown on this slide.

Vouchers & Dumps are Available | WhatsApp +201224560923

DO NOT REPRINT
© FORTINET
Brave-dumps.com



After completing this section, you should be able to achieve the objectives shown on this slide.

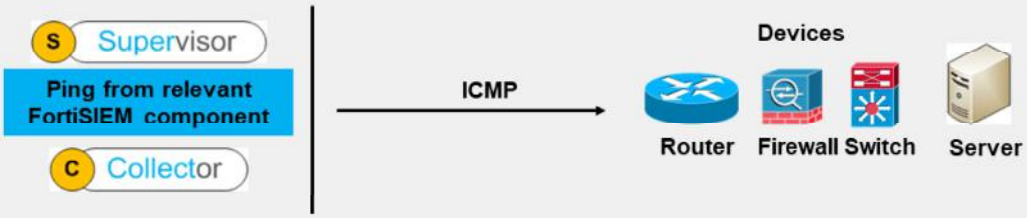
By demonstrating competence in troubleshooting device discovery, you will be able to diagnose device discovery problems.

Vouchers & Dumps are Available | WhatsApp +201224560923

DO NOT REPRINT
© FORTINET
Brave-dumps.com

Use of Ping During Test Connectivity and Discovery

- Discovery uses ICMP



- FortiSIEM pings the device first when performing a discovery or a testing of credentials
- It is recommended that you allow ICM access between FortiSIEM and devices because ICMP is also used to collect availability metrics for a device
- Alternatively, you can select **Do not Ping** and availability metrics are not collected

NSE Training Institute

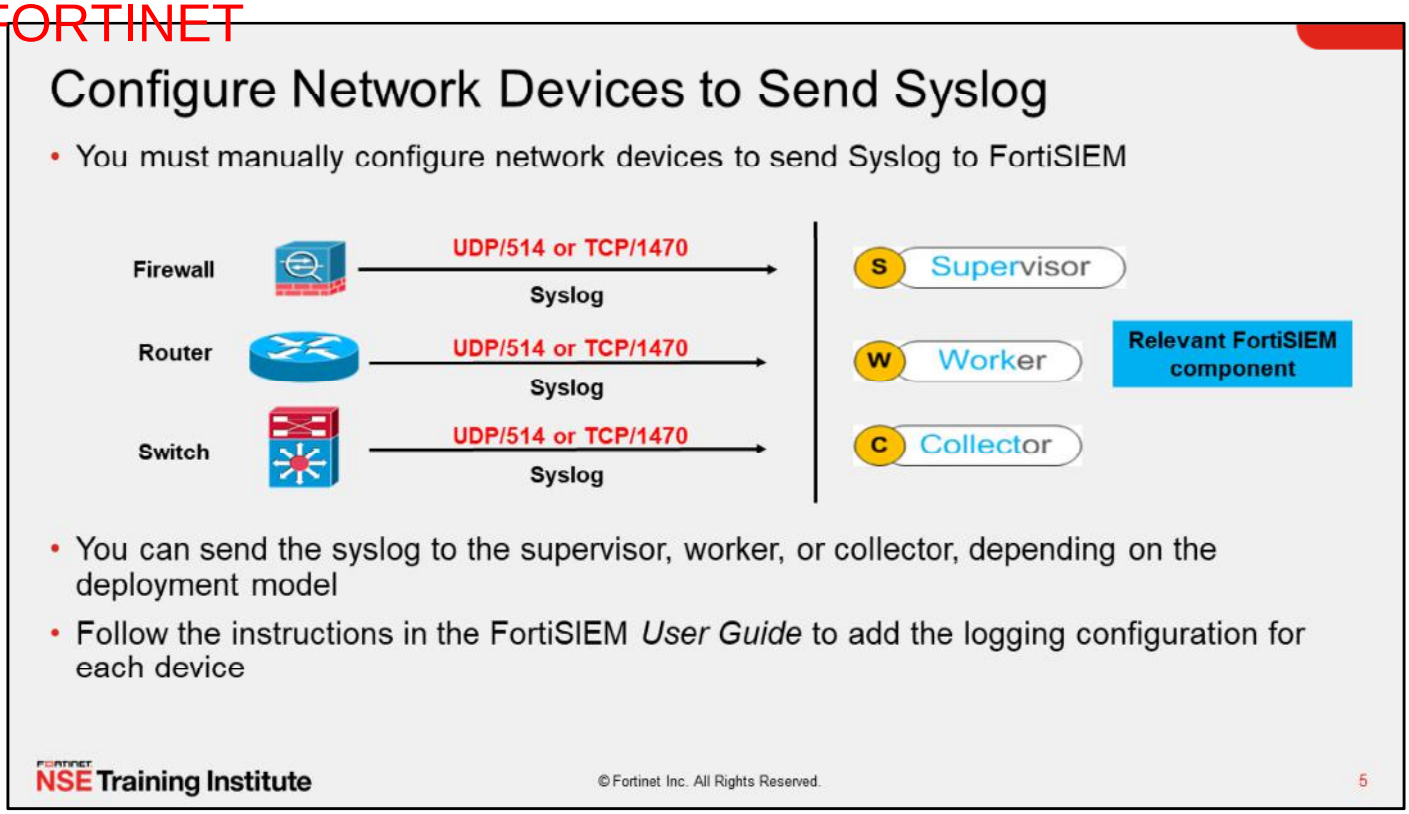
© Fortinet Inc. All Rights Reserved.

4

If you enable **Ping Device Before Discovery**, then FortiSIEM pings the device first when performing a discovery or a testing of credentials. ICMP is also used to collect availability metrics for a device; therefore, it is recommended that you allow ICMP access between FortiSIEM and devices. Alternatively, you can select **Do not Ping**, and availability metrics are not collected.

Vouchers & Dumps are Available | WhatsApp +201224560923

DO NOT REPRINT
© FORTINET
Brave-dumps.com

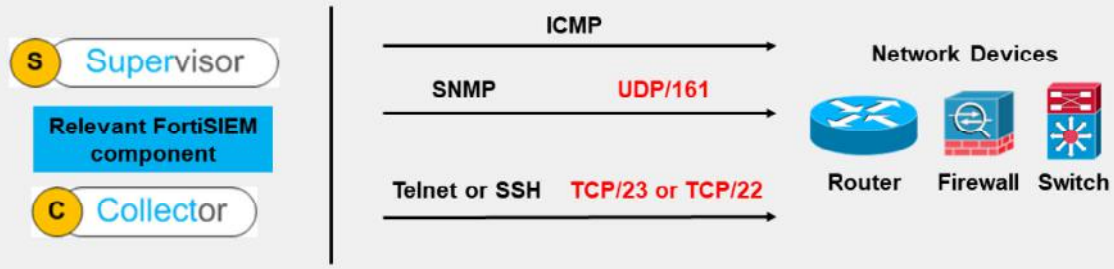


You must manually configure network devices to send the syslog to FortiSIEM. You can send the syslog to the supervisor, worker or collector, depending on the deployment model. Follow the instructions in the FortiSIEM *User Guide* to add the specific logging configuration for each device.

Vouchers & Dumps are Available | WhatsApp +201224560923

DO NOT REPRINT
© FORTINET
Brave-dumps.com

Discovery of Network Devices



- SNMP is mandatory
- Telnet or SSH is typically used for device configuration pulling
- Only the supervisor or a designated collector performs discovery
- Devices usually have ACLs that determine which IP address can poll for SNMP or log in through Telnet or SSH

NSE Training Institute

© Fortinet Inc. All Rights Reserved.

6

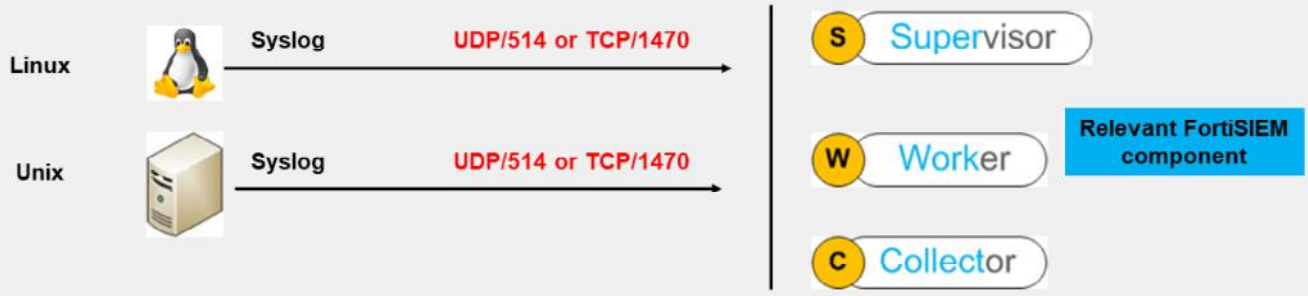
SNMP is mandatory for the discovery of network devices. Telnet or SSH is typically used for device configuration pulling. Only the supervisor or a designated collector performs discovery. Devices usually have ACLs that determine which IP address can poll for SNMP or log in through Telnet or SSH.

Vouchers & Dumps are Available | WhatsApp +201224560923

DO NOT REPRINT
© FORTINET
Brave-dumps.com

Configure Linux and Unix Servers to Send Syslog

- You must manually configure the server to send Syslog to FortiSIEM



- Syslog may be sent to the supervisor, worker, or collector, depending on the deployment model
- Follow the instructions in the FortiSIEM *User Guide* to add the specific logging configuration to the server

NSE Training Institute

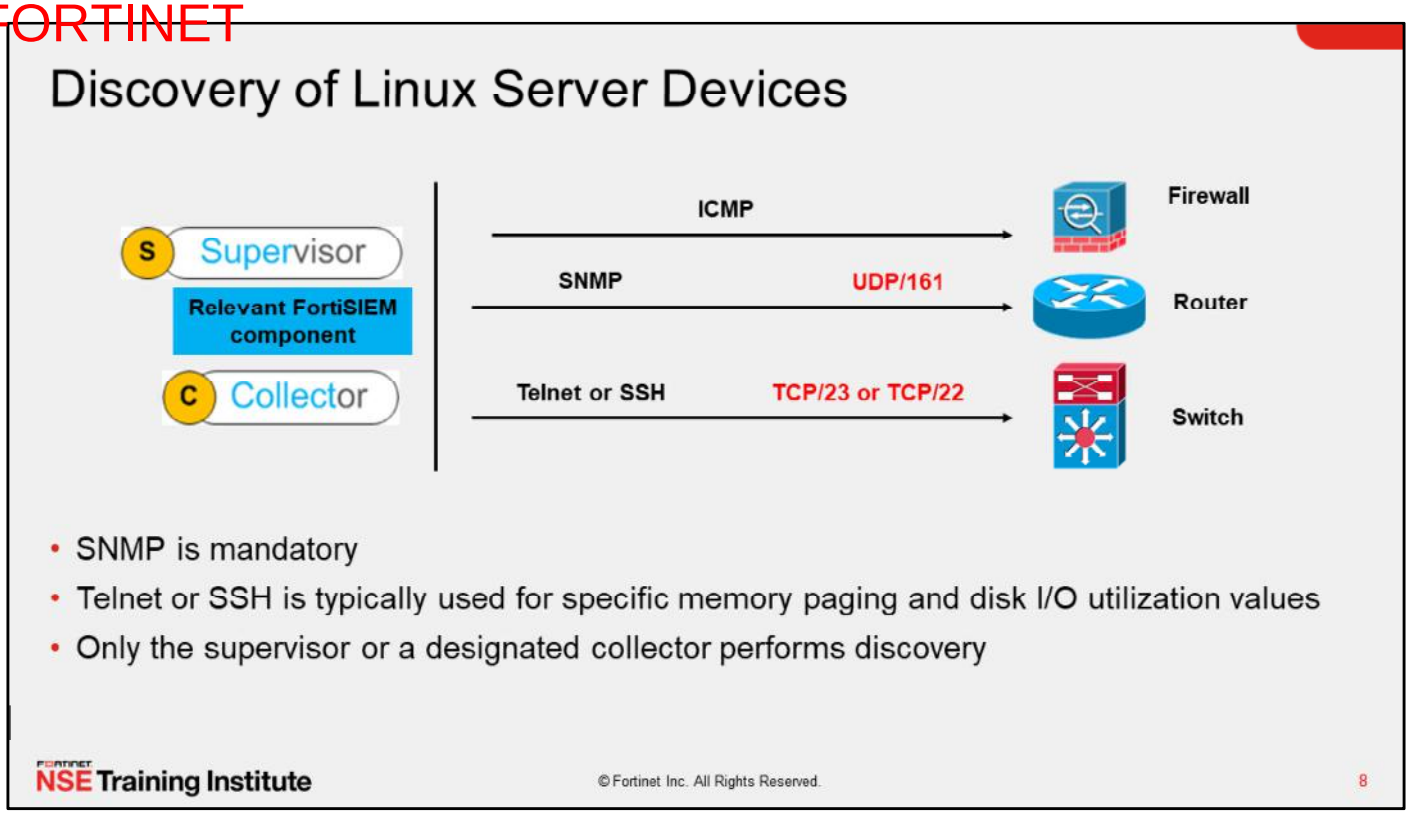
© Fortinet Inc. All Rights Reserved.

7

You must manually configure Unix and Linux servers to send the syslog to FortiSIEM. You can send the syslog to the supervisor, worker, or collector, depending on the deployment model. Follow the instructions in the *FortiSIEM User Guide* to add the specific logging configuration to the server.

Vouchers & Dumps are Available | WhatsApp +201224560923

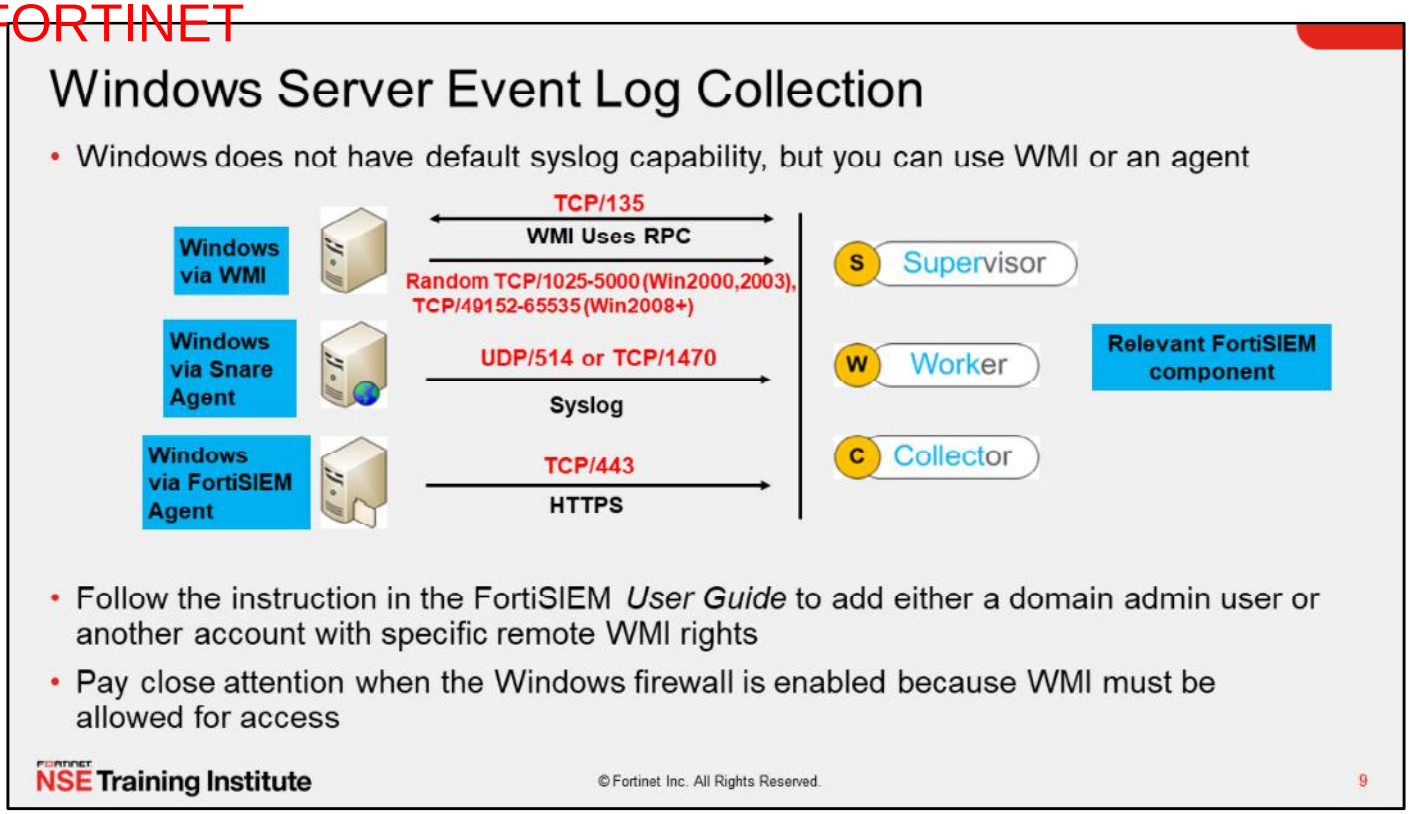
DO NOT REPRINT
© FORTINET
Brave-dumps.com



SNMP is mandatory for the discovery of Linux servers. Telnet or SSH is typically used for specific memory paging and disk I/O utilization values. Only the supervisor or a designated collector performs discovery.

Vouchers & Dumps are Available | WhatsApp +201224560923

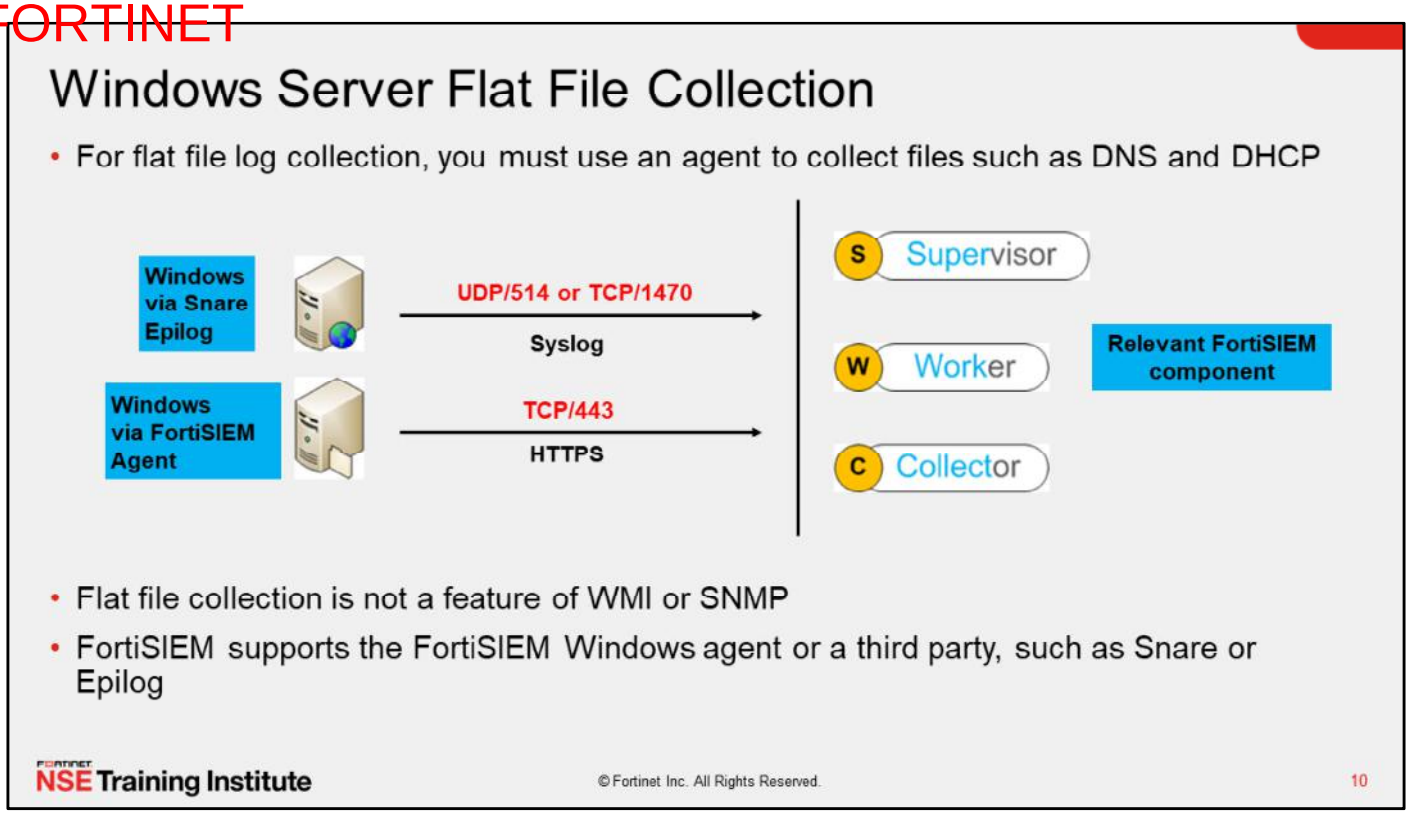
DO NOT REPRINT
© FORTINET
Brave-dumps.com



Windows does not have a default syslog capability, but you can use either WMI or an agent. Follow the instructions in the *FortiSIEM User Guide* to add either a domain administrator user or another account with specific remote WMI rights. Also, pay close attention when the Windows firewall is enabled because WMI must be allowed for access.

Vouchers & Dumps are Available | WhatsApp +201224560923

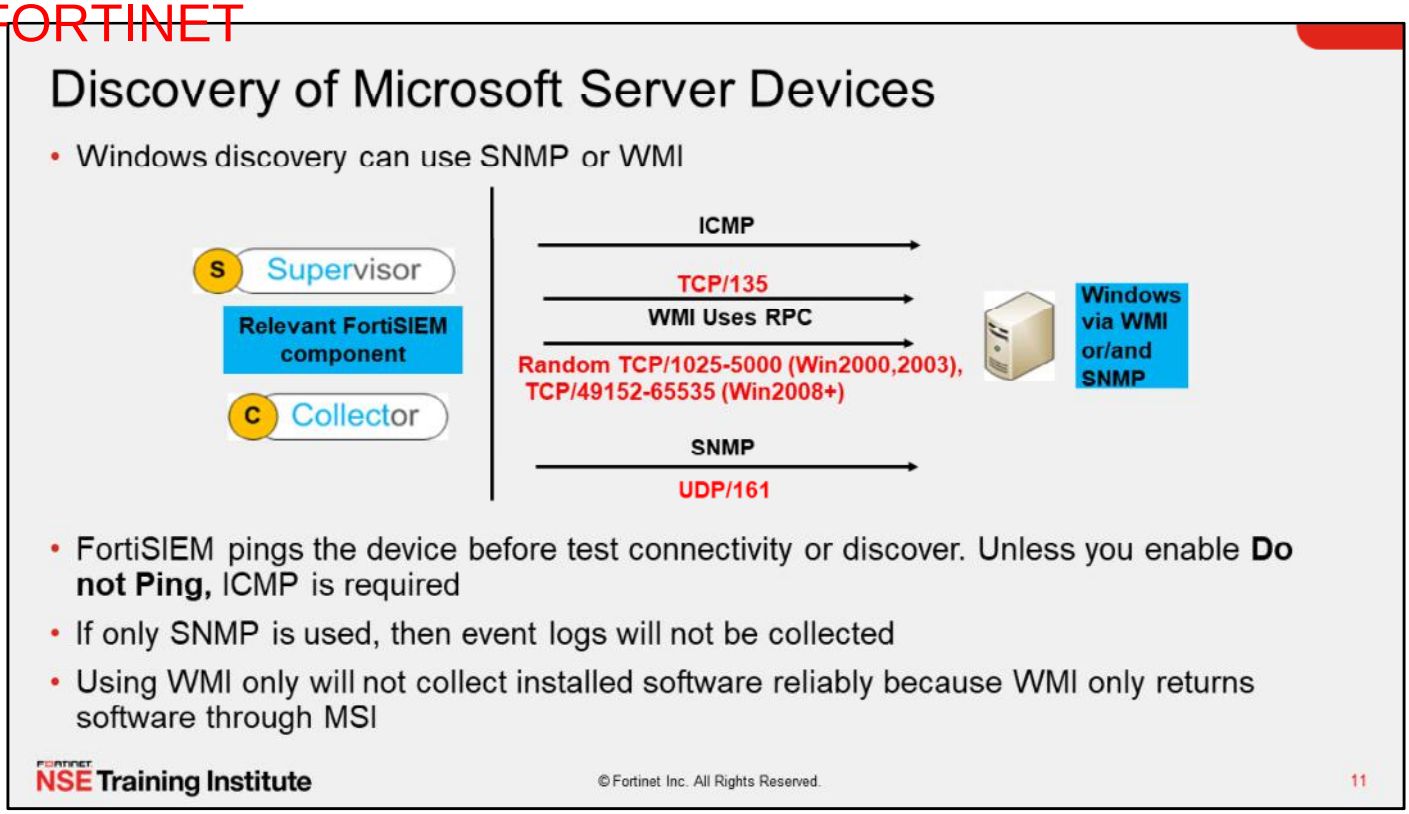
DO NOT REPRINT
© FORTINET
Brave-dumps.com



For flat file log collection, you must use an agent to collect files such as DNS and DHCP. Flat file collection is not a feature of WMI or SNMP. FortiSIEM supports the FortiSIEM Windows agent or a third party, such as Snare or Epilog.

Vouchers & Dumps are Available | WhatsApp +201224560923

DO NOT REPRINT
© FORTINET
Brave-dumps.com



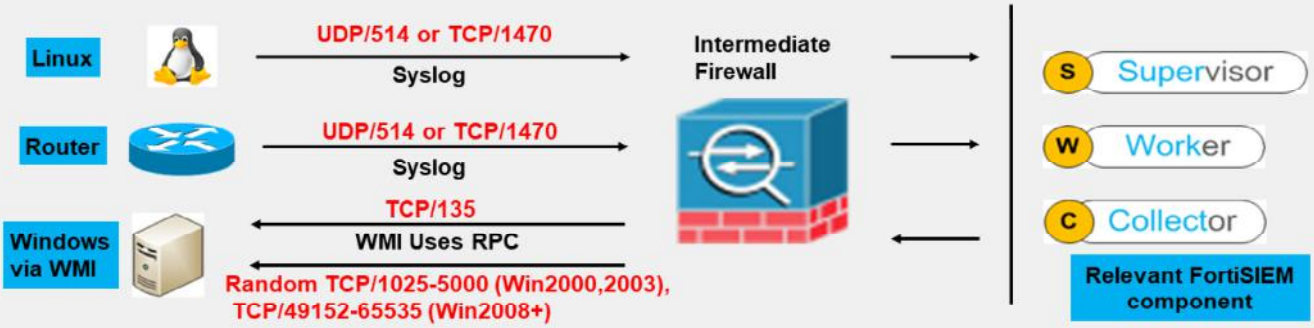
For Windows device discovery, you can use SNMP or WMI. FortiSIEM pings the device before test connectivity or discovery unless you select **Do not Ping**, so for device discovery ICMP is required. If only SNMP is used, then event logs aren't collected. Using WMI only will not collect installed software reliably due to WMI only returning software through MSI.

Vouchers & Dumps are Available | WhatsApp +201224560923

DO NOT REPRINT
© FORTINET
Brave-dumps.com

Log Collection—Intermediate Devices

- Watch for intermediate devices between the reporting device and the relevant FortiSIEM component



- Firewall rules or ACLs will need to be modified to allow this traffic
- For WMI, the random ports can be set to a specific value
  - https://docs.microsoft.com/en-us/windows/win32/wmisdk/setting-up-a-fixed-port-for-wmi?redirectedfrom=MSDN

NSE Training Institute

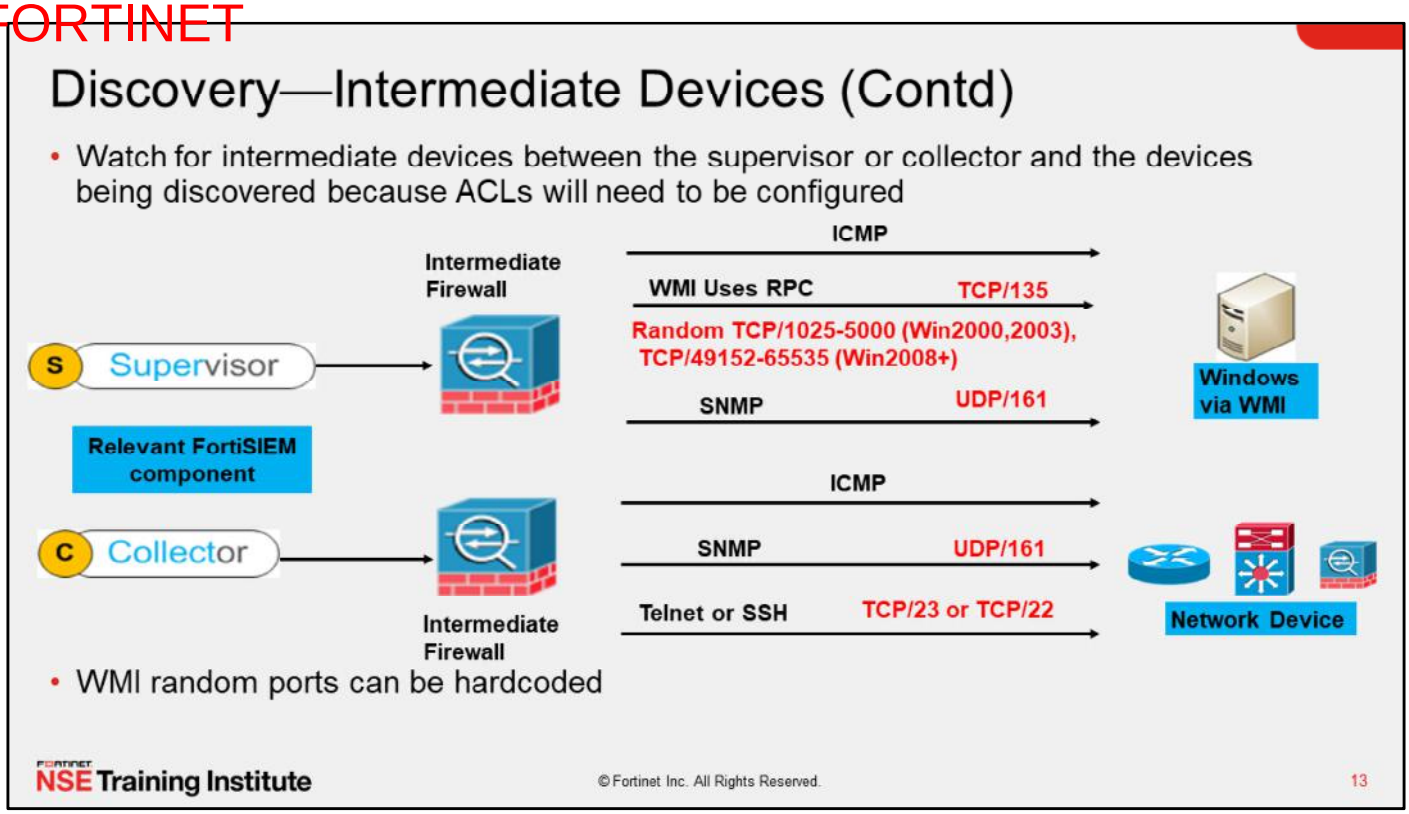
© Fortinet Inc. All Rights Reserved.

12

If there are intermediate devices between the reporting device and the relevant FortiSIEM component, then firewall rules or access control lists (ACLs) will need to be modified to allow this traffic. For WMI, random ports can be set to a specific value.

Vouchers & Dumps are Available | WhatsApp +201224560923

DO NOT REPRINT
© FORTINET
Brave-dumps.com



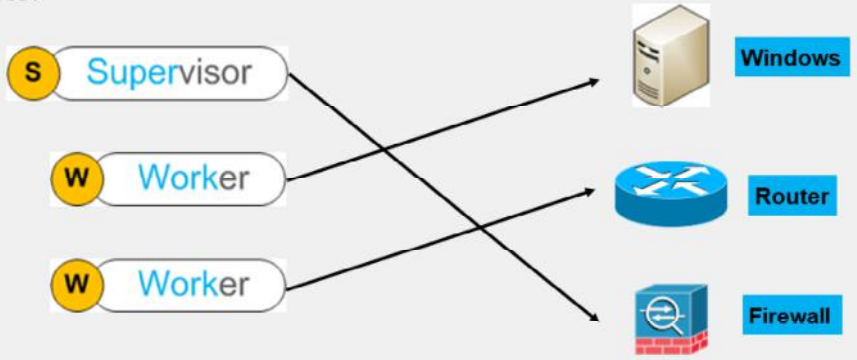
If there are intermediate devices between the supervisor or collector and the devices being discovered then ACLs will need to be configured to include those devices. WMI random ports can be hardcoded.

Vouchers & Dumps are Available | WhatsApp +201224560923

DO NOT REPRINT
© FORTINET
Brave-dumps.com

Data Collection After Discovery by the Supervisor

- After discovery by the supervisor, FortiSIEM will load balance data collection amongst the FortiSIEM cluster



- You must ensure that monitored servers and devices include the supervisor IP and all worker IP addresses for any ACLs related to SNMP polling and Telnet/SSH access
- Be aware of any older network devices that only allow a limited number of SNMP pollers

NSE Training Institute

© Fortinet Inc. All Rights Reserved.

14

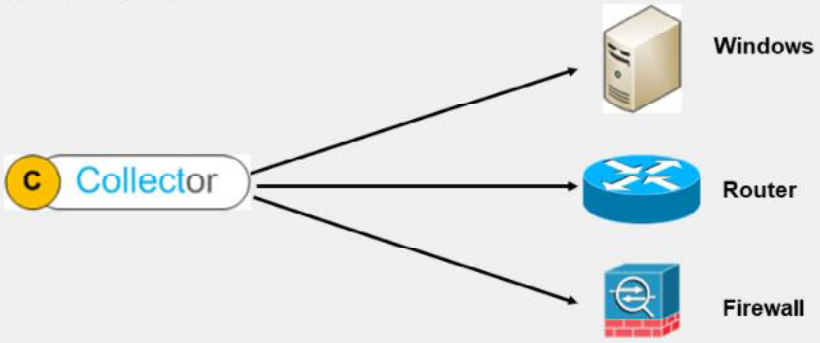
After discovery by the supervisor, FortiSIEM will load balance data collection amongst the FortiSIEM cluster. You must ensure that monitored servers and devices include the supervisor IP and all worker IP addresses for any ACLs related to SNMP polling and Telnet/SSH access.

Vouchers & Dumps are Available | WhatsApp +201224560923

DO NOT REPRINT
© FORTINET
Brave-dumps.com

Data Collection After Discovery by a Collector

- After discovery by a collector, a one-to-one relationship is formed between the discovered device and collector



- After the relationship is formed, only the discovering collector performs the data collection
- The collector should be the destination for syslog from the network devices

NSE Training Institute

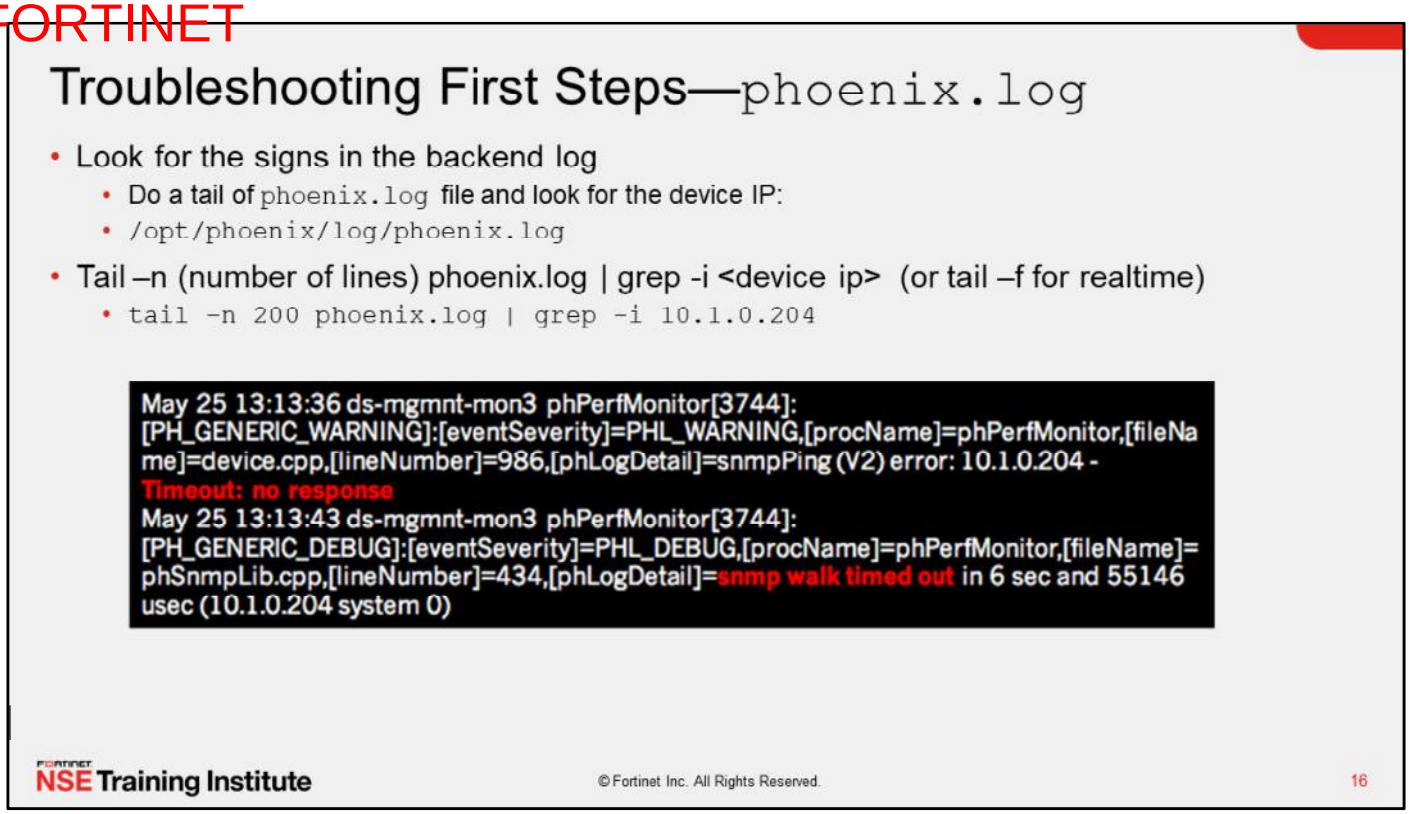
© Fortinet Inc. All Rights Reserved.

15

After a device is discovered by a collector, a one-to-one relationship is formed between that device and that collector. After that relationship is formed, only that collector will perform data collection. The collector should be the destination for syslog from the network devices.

Vouchers & Dumps are Available | WhatsApp +201224560923

DO NOT REPRINT
© FORTINET
Brave-dumps.com



You can use the `tail` option that outputs `phoenix.log` file when investigating issues. The `tail` command is a command-line utility that outputs the last part of files given to it through standard input. The command writes the results of its review to standard output. By default, the `tail` returns the last ten lines of each file that it is given. The command may also be used to follow a file in real-time and watch as new lines are written to it.

Vouchers & Dumps are Available | WhatsApp +201224560923

DO NOT REPRINT Brave-dumps.com
© FORTINET

Troubleshooting Commands—Tcpdump

- tcpdump <options>
  - http://www.tcpdump.org/tcpdump_man.html
- Show traffic from FortiSIEM to a specific host
  - tcpdump -i eth0 dst host <ip>

```
[root@AccelOps_3_1_1 ~]# tcpdump dst host 192.168.70.2
tcpdump: verbose output suppressed, use -v or -vv for full protocol decode
listening on eth0, link-type EN10MB (Ethernet), capture size 96 bytes
12:41:27.615868 IP AccelOps_3_1_1.test.local.36346 > 192.168.70.2.snmp:  C=accelops GetBulk(33)  N=0 M=10 E:cisco.
9.48.1.1.1.7.1
12:41:27.633013 IP AccelOps_3_1_1.test.local.36346 > 192.168.70.2.snmp:  C=accelops GetRequest(33)  E:cisco.9.48.1
.1.1.7.1
```

- Are you receiving syslog traffic from a device to FortiSIEM?
  - tcpdump -i eth0 src host <ip> and dst port 514

```
[root@AccelOps_3_1_1 ~]# tcpdump src host 192.168.69.1 and dst port 514
ctcpdump: verbose output suppressed, use -v or -vv for full protocol decode
listening on eth0, link-type EN10MB (Ethernet), capture size 96 bytes
12:38:35.339341 IP 192.168.69.1.syslog > AccelOps_3_1_1.test.local.syslog: SYSLOG local0.info, length: 161
12:38:35.341481 IP 192.168.69.1.syslog > AccelOps_3_1_1.test.local.syslog: SYSLOG local0.info, length: 167
12:38:35.379700 IP 192.168.69.1.syslog > AccelOps_3_1_1.test.local.syslog: SYSLOG local0.info, length: 154
```

NSE Training Institute

© Fortinet Inc. All Rights Reserved.

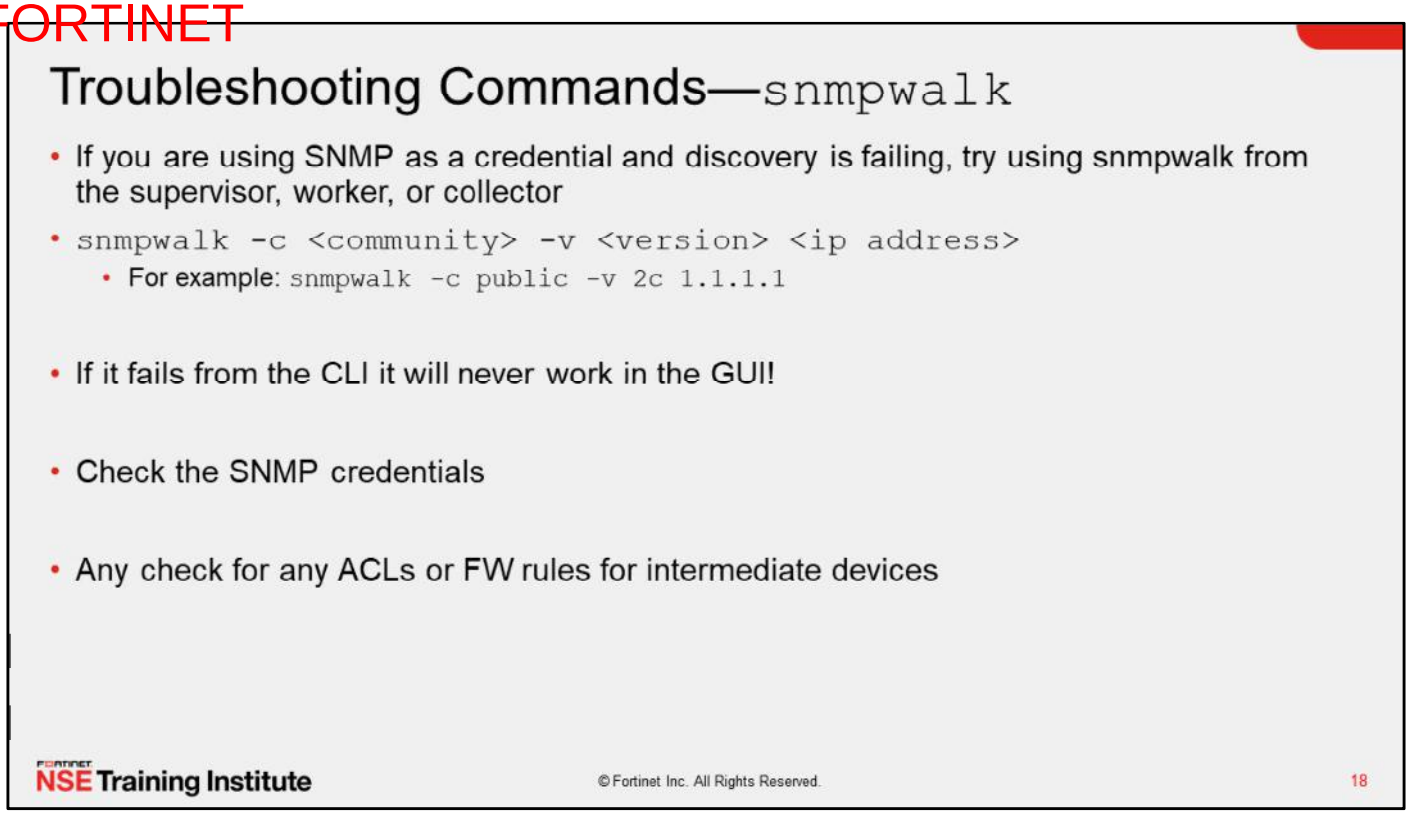
17

The `tcpdump` prints out a description of the contents of packets on a network interface that matches the boolean *expression*. The description is preceded by a time stamp, printed, by default, as hours, minutes, seconds, and fractions of a second since midnight.

You can use `tcpdump` to show traffic from a specific host, or you can check that the syslog is received from a specific device.

Vouchers & Dumps are Available | WhatsApp +201224560923

DO NOT REPRINT
© FORTINET
Brave-dumps.com



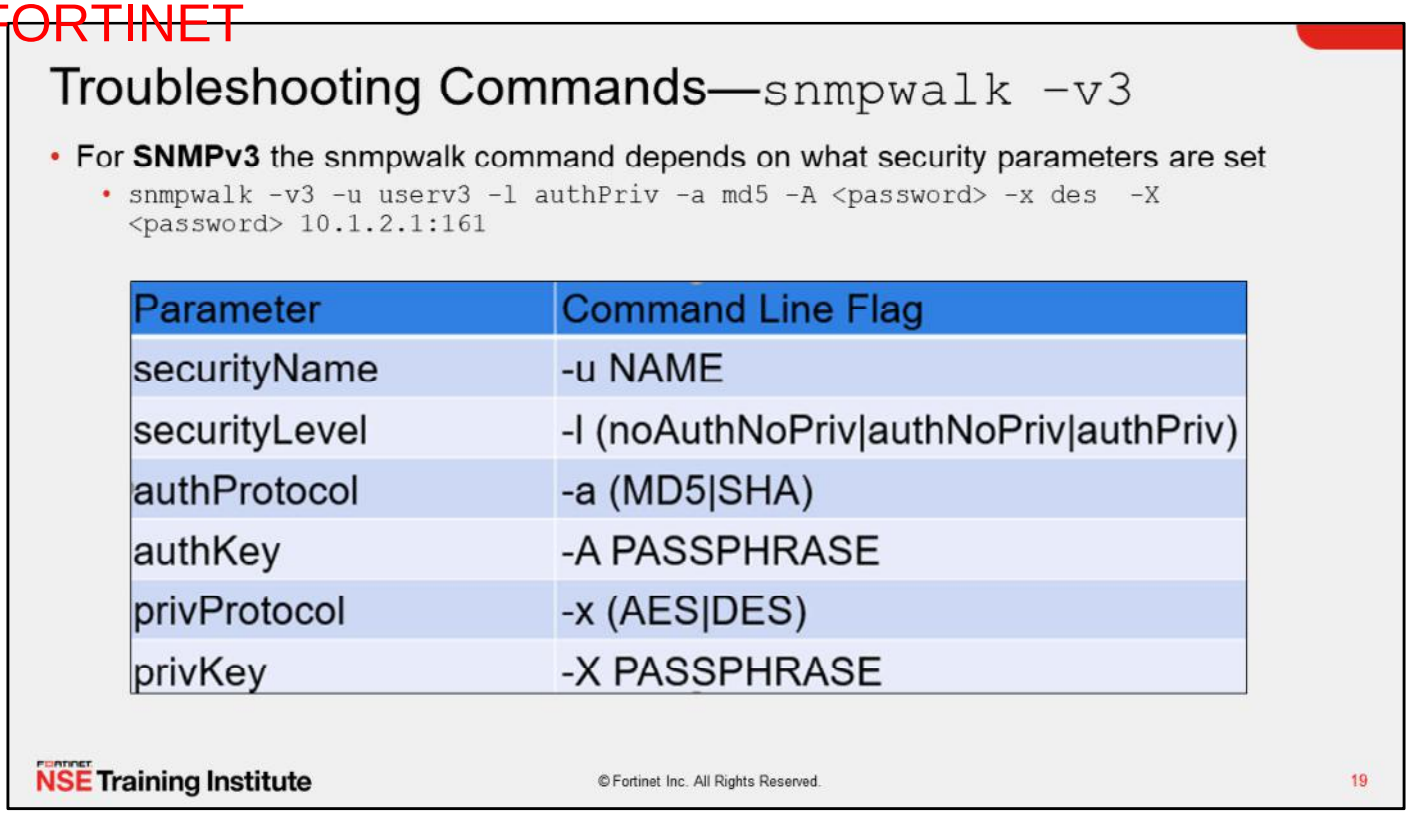
If SNMP is being used as a credential and discovery is failing, try an `snmpwalk` from the supervisor, the worker, or the collector.

If the `snmpwalk` command is unsuccessful, check the device configuration.

- Is the SNMP agent configured on the device?
- Is the SNMP agent enabled?
  - Some devices require an additional checkbox to enable the agent.
- Is the SNMP host correctly configured on the network device?
  - If the FortiSIEM solution is discovering the device from a collector, the host will be the IP of the collector not the supervisor.

Vouchers & Dumps are Available | WhatsApp +201224560923

DO NOT REPRINT
© FORTINET
Brave-dumps.com



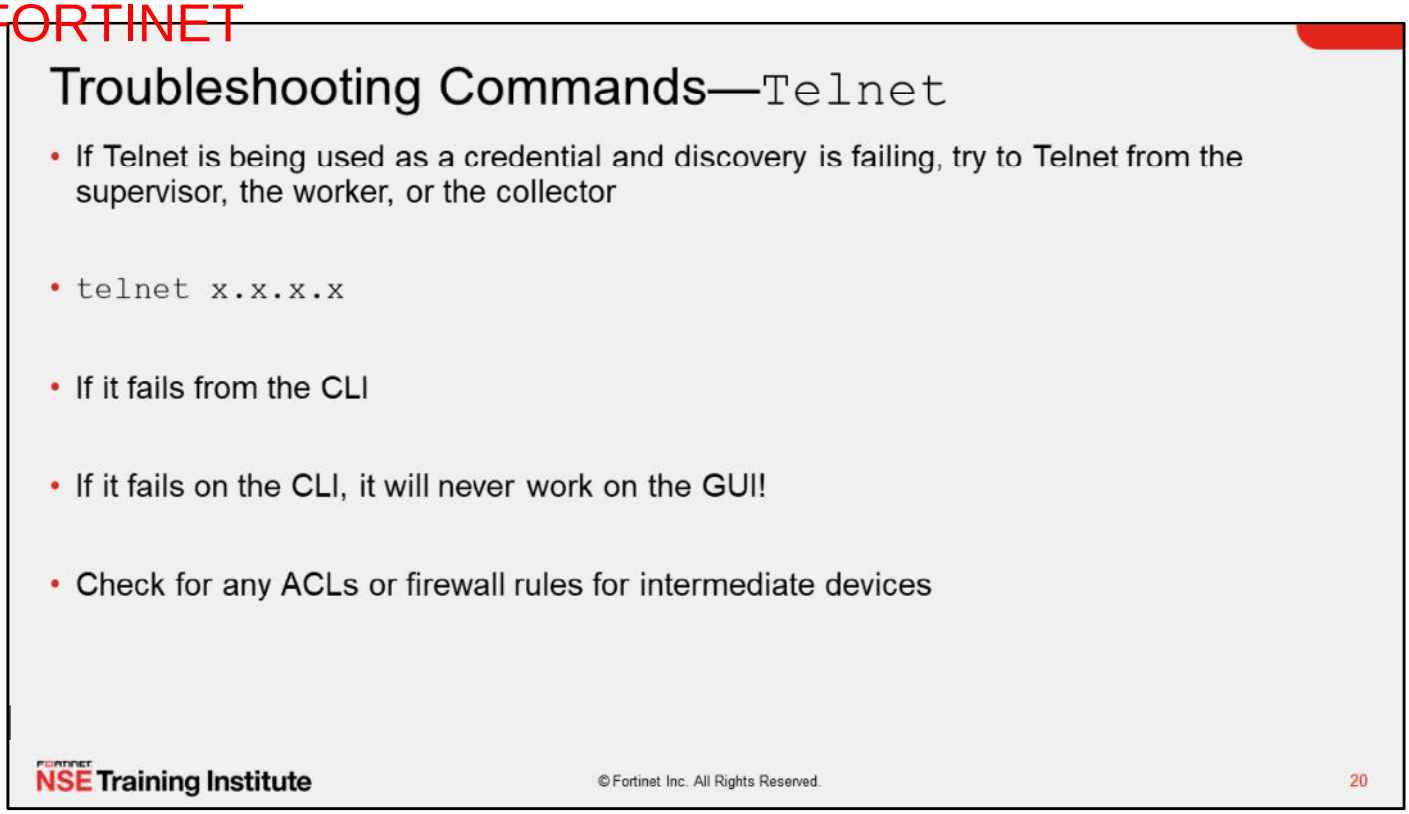
For SNMPv3, the `snmpwalk` command depends on what security parameters are set. The table on this slide lists the command line flags for various parameters.

When troubleshooting SNMPv3, consider testing a basic SNMPv2c configuration to establish whether the more complex SNMPv3 configuration is at fault. Also check the network connectivity.

- SNMP uses UDP port161 for queries and port162 for traps. Are they open between the devices?
- Any firewall or NAT device between the FortiSIEM node and the network device may change the source IP address of the SNMP query that the network device receives.

Vouchers & Dumps are Available | WhatsApp +201224560923

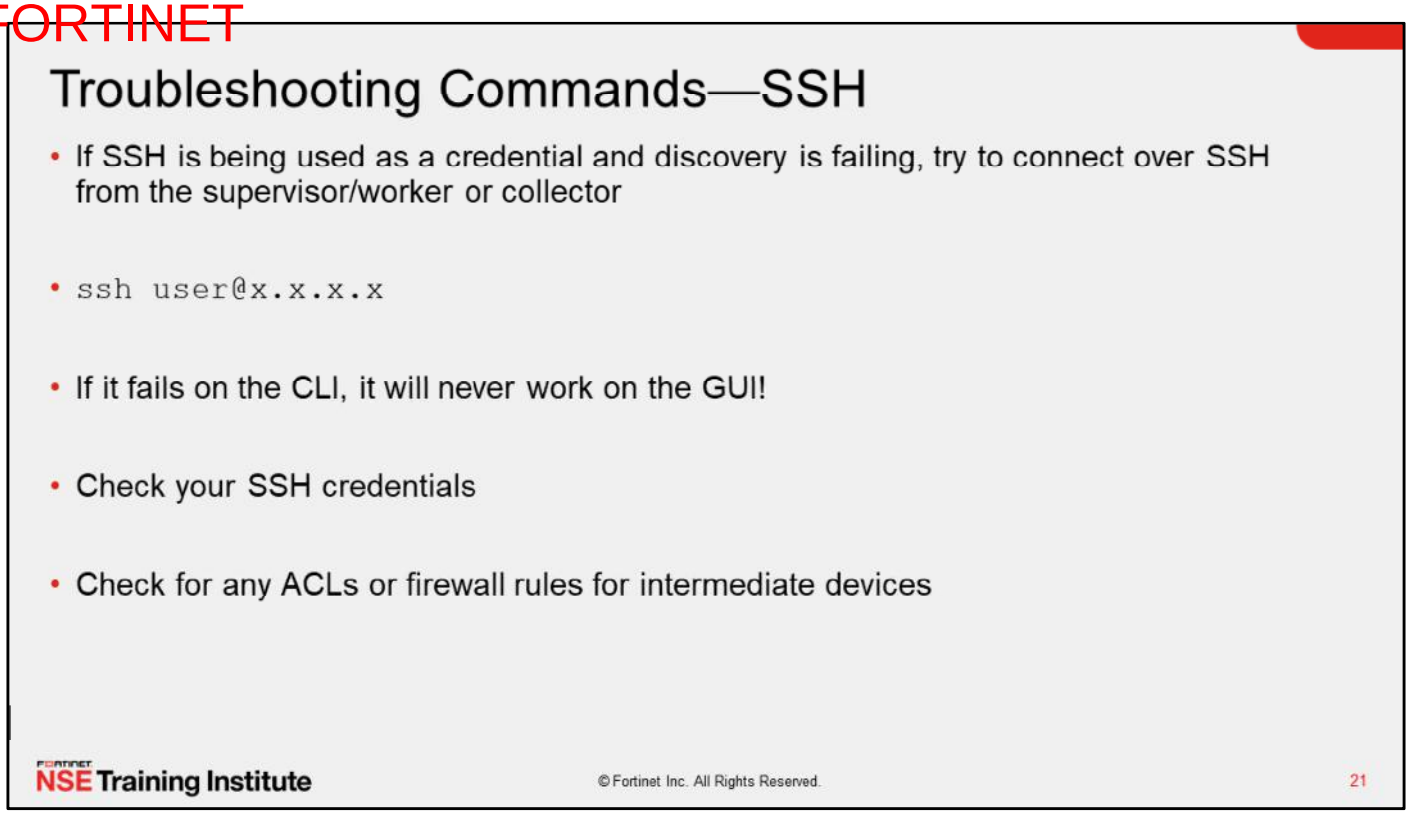
DO NOT REPRINT
© FORTINET
Brave-dumps.com



If you are using Telnet as a credential and discovery method but it is failing, try to connect over Telnet from the CLI of the supervisor, the worker, or the collector. If Telnet fails on the CLI, then it will not work from the GUI. If Telnet fails on the CLI then check the Telnet credentials, the ACLs, or the firewall rules for intermediate devices.

Vouchers & Dumps are Available | WhatsApp +201224560923

DO NOT REPRINT
© FORTINET
Brave-dumps.com



If you are using SSH as a credential and discovery is failing, try to connect over SSH from the supervisor, worker, or collector CLI.

Vouchers & Dumps are Available | WhatsApp +201224560923

DO NOT REPRINT
© FORTINET
Brave-dumps.com

Troubleshooting Commands—Configuration Pull Failed

- FortiSIEM uses expect scripts to pull the configuration from devices
  - `cd /opt/phoenix/bin`
    - `./getCmdOutViaSSH.exp {ssh|telnet} hostIP port user password enablePassword <Command> ouput_file_name`
  - For example connect over SSH to a Cisco switch
  - `./getCmdOutViaSSH.exp ssh 22 192.168.1.2 user pass pass2 "show conf" ssh_test_result.txt`
  - Perform `more` operation on `<test result file name>` to see if you managed to pull the configuration
    - For example: `more ssh_test_result.txt`
- Note that if the device does not have a second password, enter the same password twice.

NSE Training Institute

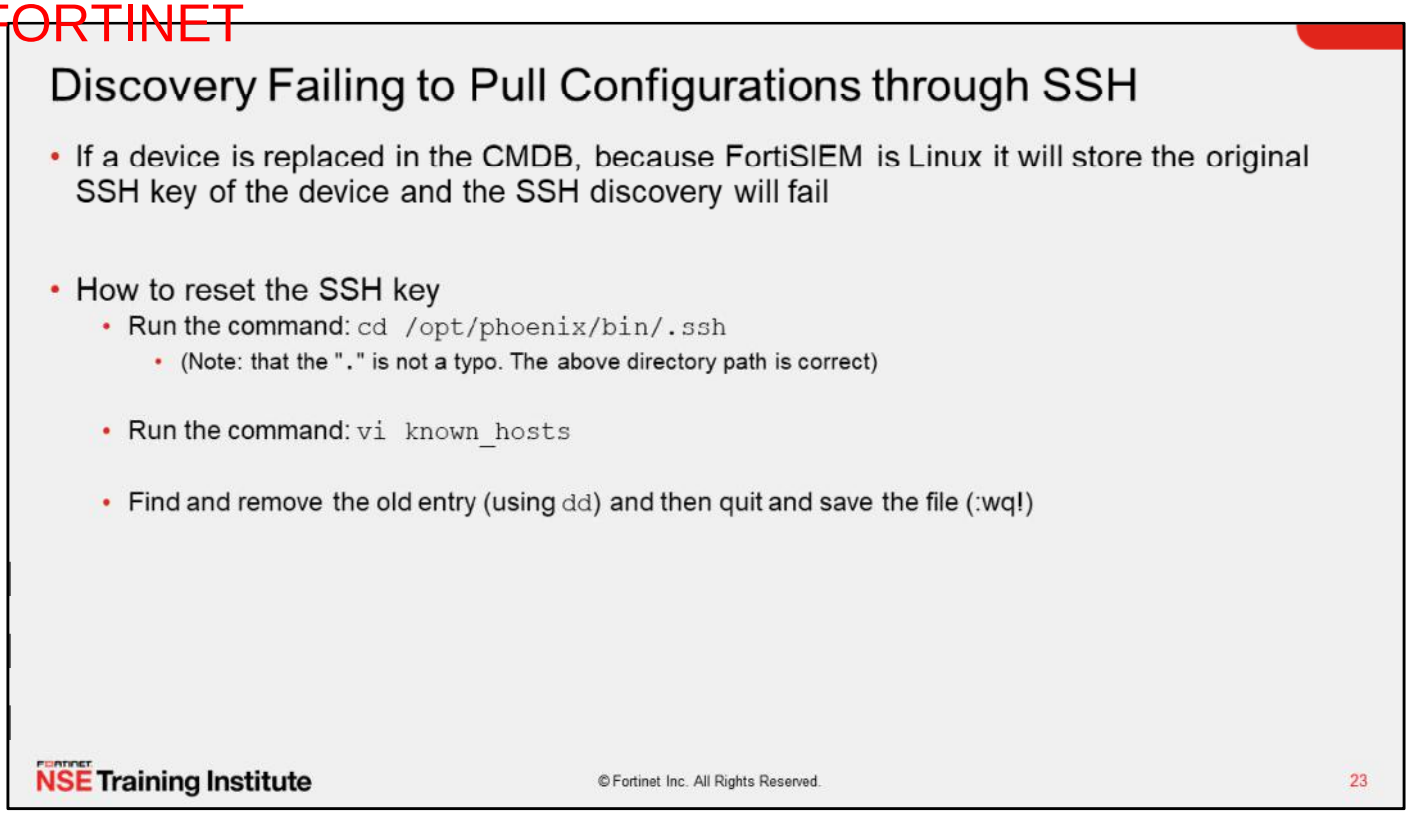
© Fortinet Inc. All Rights Reserved.

22

FortiSIEM uses expect scripts to pull the configuration. You can use the `getCmdOutput` command to check the validity of privileged SSH credentials used to pull configurations from devices.

Vouchers & Dumps are Available | WhatsApp +201224560923

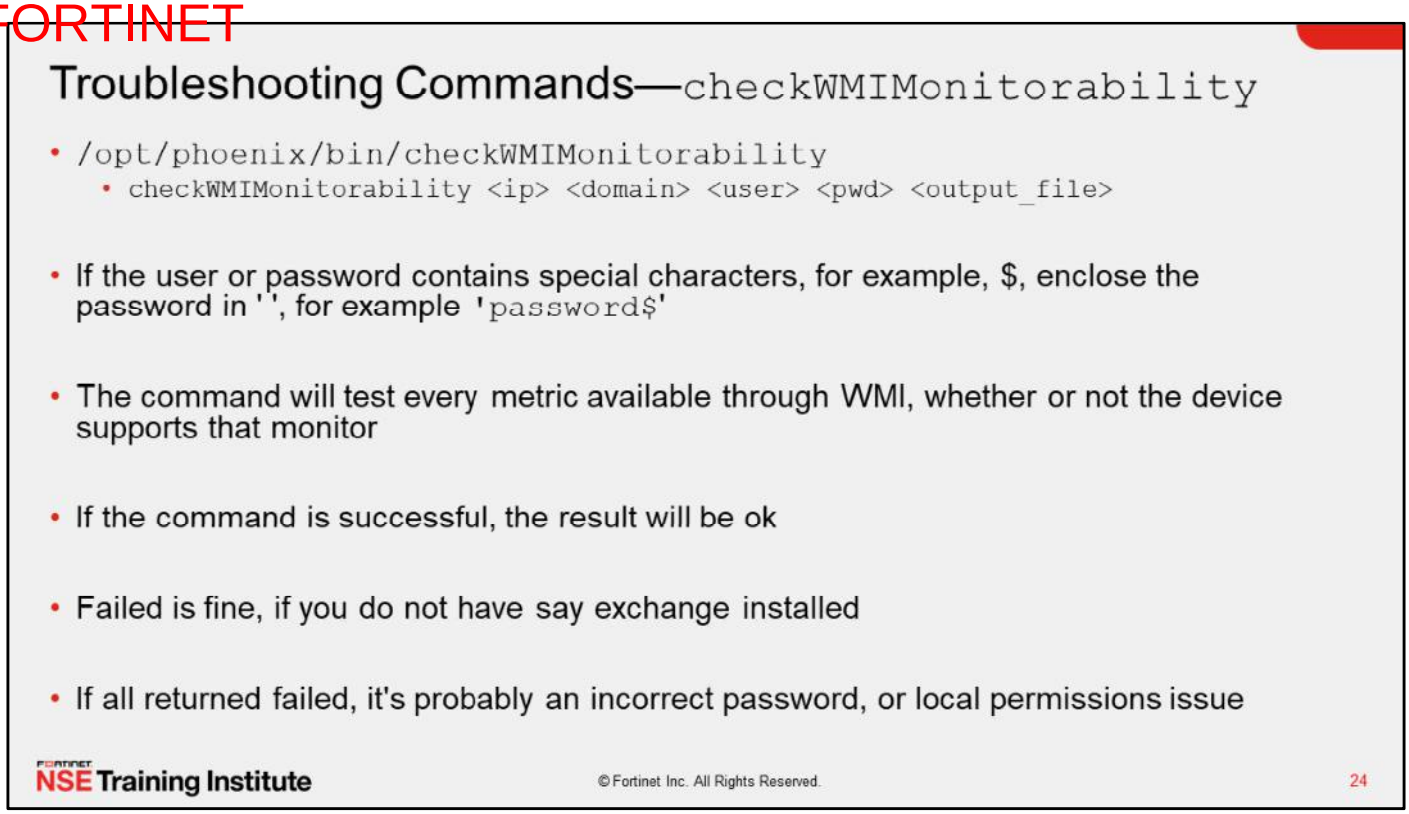
DO NOT REPRINT
© FORTINET
Brave-dumps.com



If a device is replaced in the CMDB, since FortiSIEM is Linux it will store the original SSH key of the device and the SSH discovery will fail. To reset the SSH key, follow the instructions shown on slide.

Vouchers & Dumps are Available | WhatsApp +201224560923

DO NOT REPRINT
© FORTINET
Brave-dumps.com



This slide shows how to check WMI monitor ability. The command shown on this slide will test every metric available through WMI, whether or not the device, supports that monitor.

If there is no response from the server, check the following:
- The WMI configuration has been correctly applied to the remote server.
- The WMI protocol is allowed through the Windows firewall on the remote server.
- The traffic is not being blocked by an intermediate network device.
- The discovery process is not being blocked by host antivirus, host IDS, or endpoint protection software.

Vouchers & Dumps are Available | WhatsApp +201224560923

DO NOT REPRINT
© FORTINET
Brave-dumps.com

Command Result—checkWMIMonitorability

- more <output_file_name>

```
[root@AccelOps_3_1_1 bin]# checkWMIMonitorability 192.168.69.8 test administrator password test_result
```

```
[root@AccelOps_3_1_1 bin]# more test_result
Win32_ComputerSystem (basic) ...ok
Win32_OperatingSystem (basic) ...ok
Win32_BIOS (basic) ...ok
Win32_QuickFixEngineering (patch) ...ok
Win32_Processor (processor info) ...ok
Win32_WindowsProductActivation (os serial) ...ok
Win32_Service (service info) ...ok
Win32_Process (process info) ...ok
Win32_Product (installed software) ...ok
Win32_PerfRawData_Tcpip_NetworkInterface...ok
Win32_NetworkAdapterConfiguration...ok
Win32_PerfRawData_PerfProc_Process (process performance) ...ok
Win32_PerfRawData_PerfDisk_PhysicalDisk (disk performance) ...ok
Win32_PerfRawData_PerfOS_Memory (memory performance) ...ok
Win32_PerfFormattedData_DNS_DNS (DNS metrics) ...ok
Win32_PerfFormattedData_DHCPServer_DHCPServer (DHCP metrics) ...ok
Win32_PerfFormattedData_W3SVC_WebService (web server metrics) ...ok
Win32_PerfRawData_MSExchangeIS_MSExchangeIS (exchange rpc metrics) ...failed
Win32_PerfRawData_MSExchangeIS_MSExchangeISMailbox (exchange mailbox metrics) ...failed
Win32_PerfRawData_MSExchangeIS_MSExchangeISPublic (exchange public mailbox metrics) ...failed
Win32_PerfRawData_SMTPSVC_SMTPServer (exchange SMYP metrics) ...failed
Win32_PerfFormattedData_ASPNET_ASPNET (ASP NET metrics) ...failed
Win32_PerfRawData_NTDS_NTDS (Active Directory metrics) ...ok
Win32_NTLogEvent(source: Security)...ok
Win32_NTLogEvent(source: Application)...ok
Win32_NTLogEvent(source: System)...ok
```

NSE Training Institute

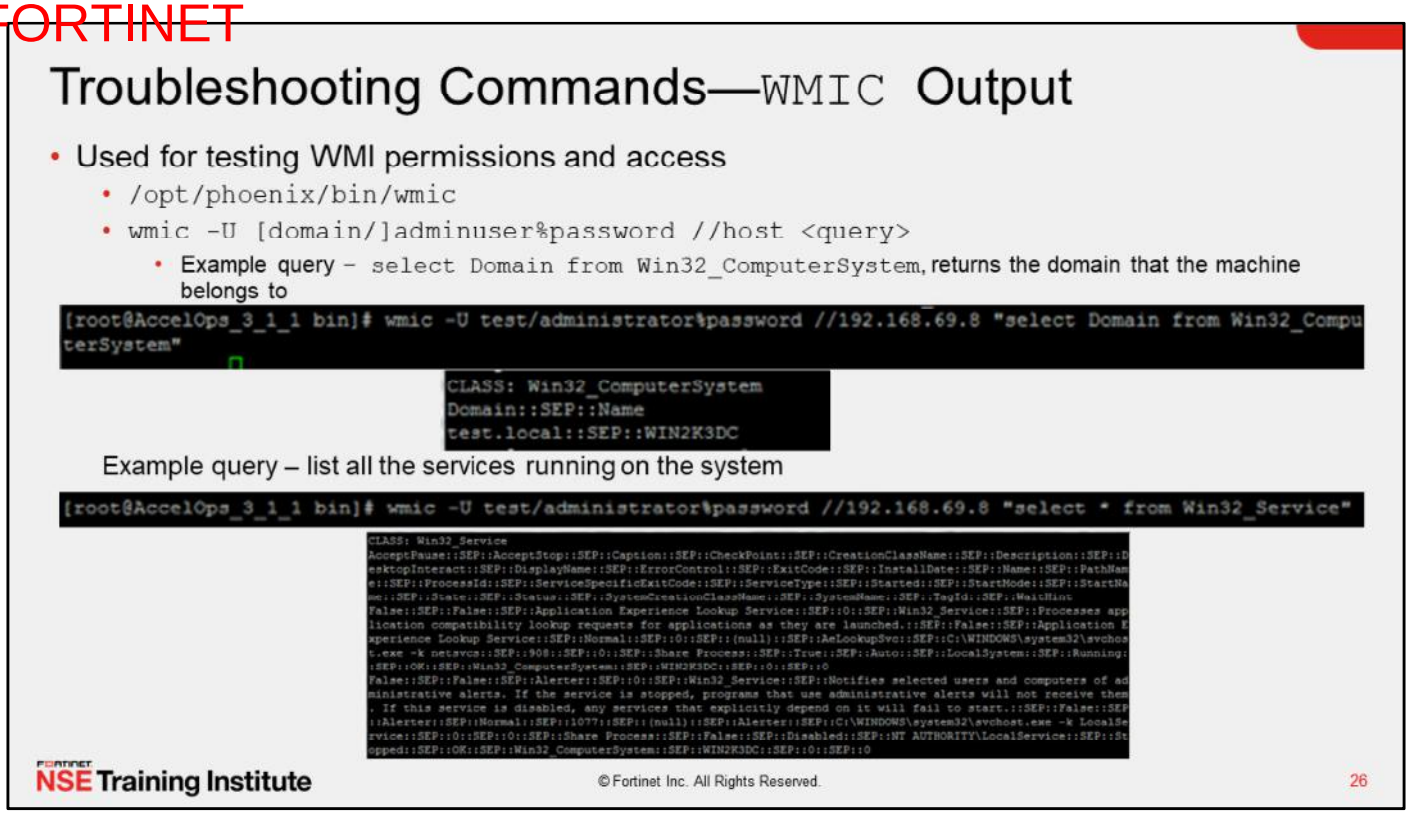
© Fortinet Inc. All Rights Reserved.

25

The sample logs on this slide show `WMI` monitor ability results.

Vouchers & Dumps are Available | WhatsApp +201224560923

DO NOT REPRINT
© FORTINET
Brave-dumps.com



You can use `WMIC` command for testing WMI permissions and access. This slide shows a few examples of `WMIC` command output.

Vouchers & Dumps are Available | WhatsApp +201224560923

DO NOT REPRINT
© FORTINET
Brave-dumps.com

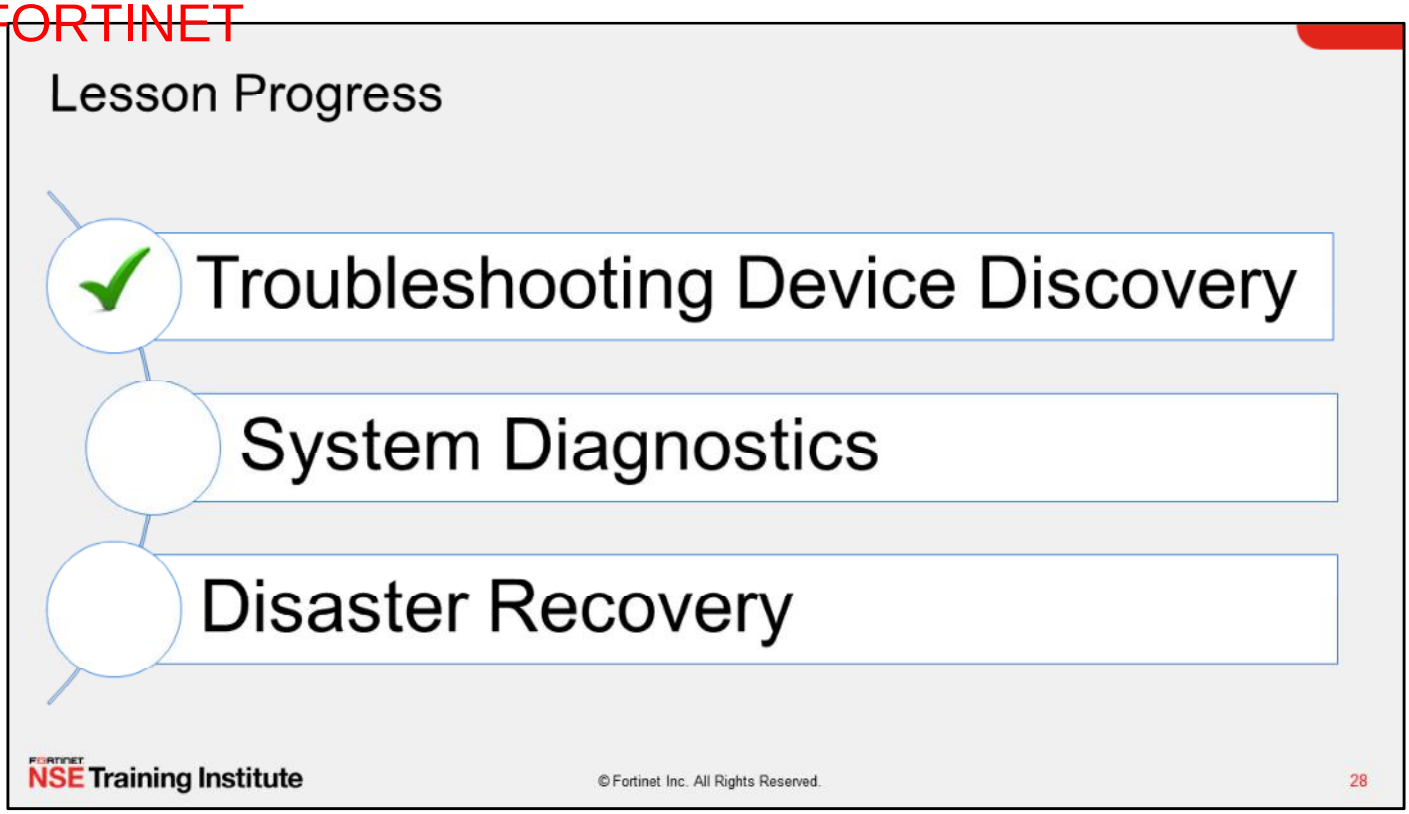
Knowledge Check

1. Which log file shows device discovery logs?
   A. ssh_test_result.log
   ✓B. phoenix.log

NSE Training Institute
© Fortinet Inc. All Rights Reserved.
27

Vouchers & Dumps are Available | WhatsApp +201224560923

DO NOT REPRINT
© FORTINET
Brave-dumps.com

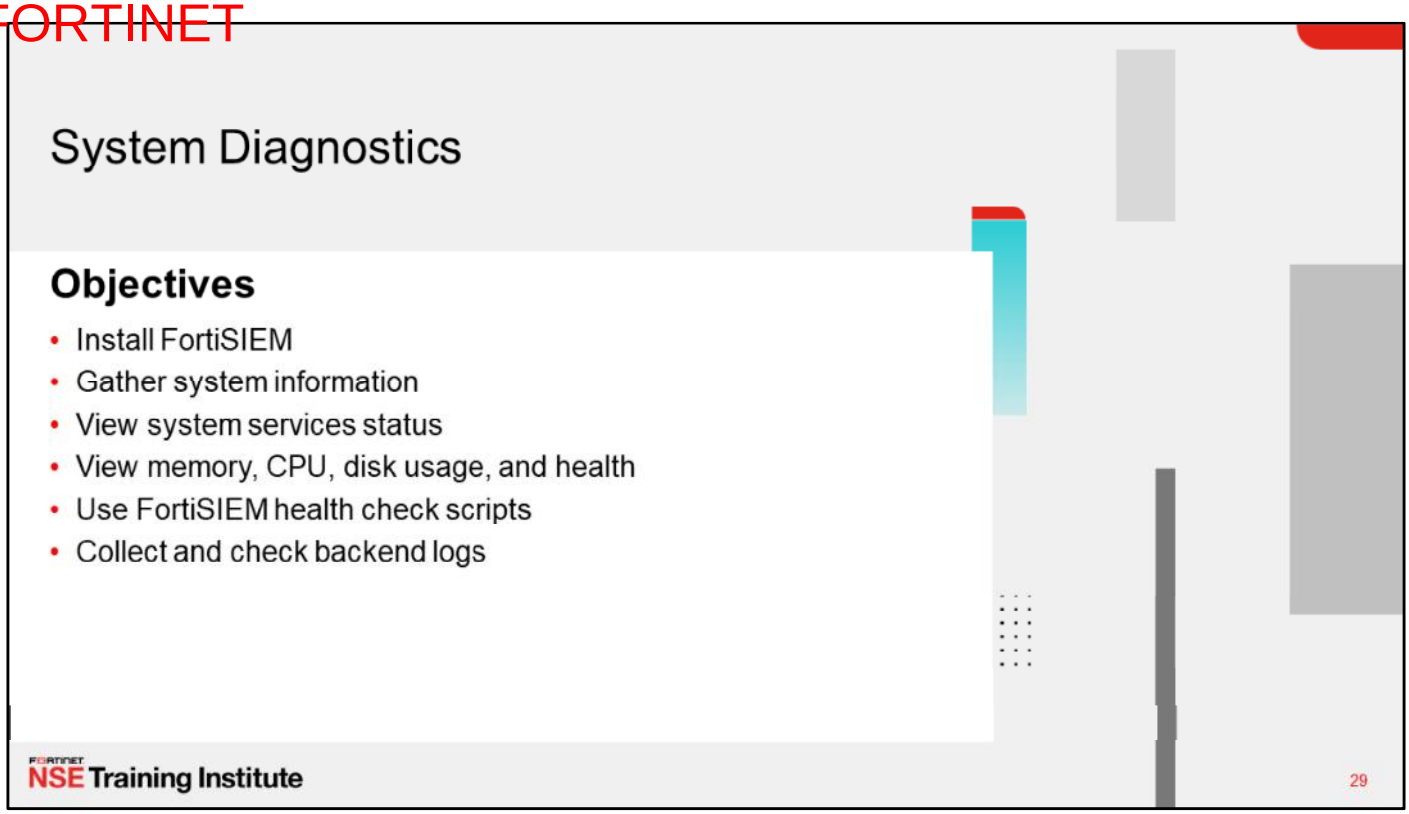


Good job! You now understand how to troubleshoot device discovery problems.

Now, you will learn about FortiSIEM system diagnostics.

Vouchers & Dumps are Available | WhatsApp +201224560923

DO NOT REPRINT
© FORTINET
Brave-dumps.com

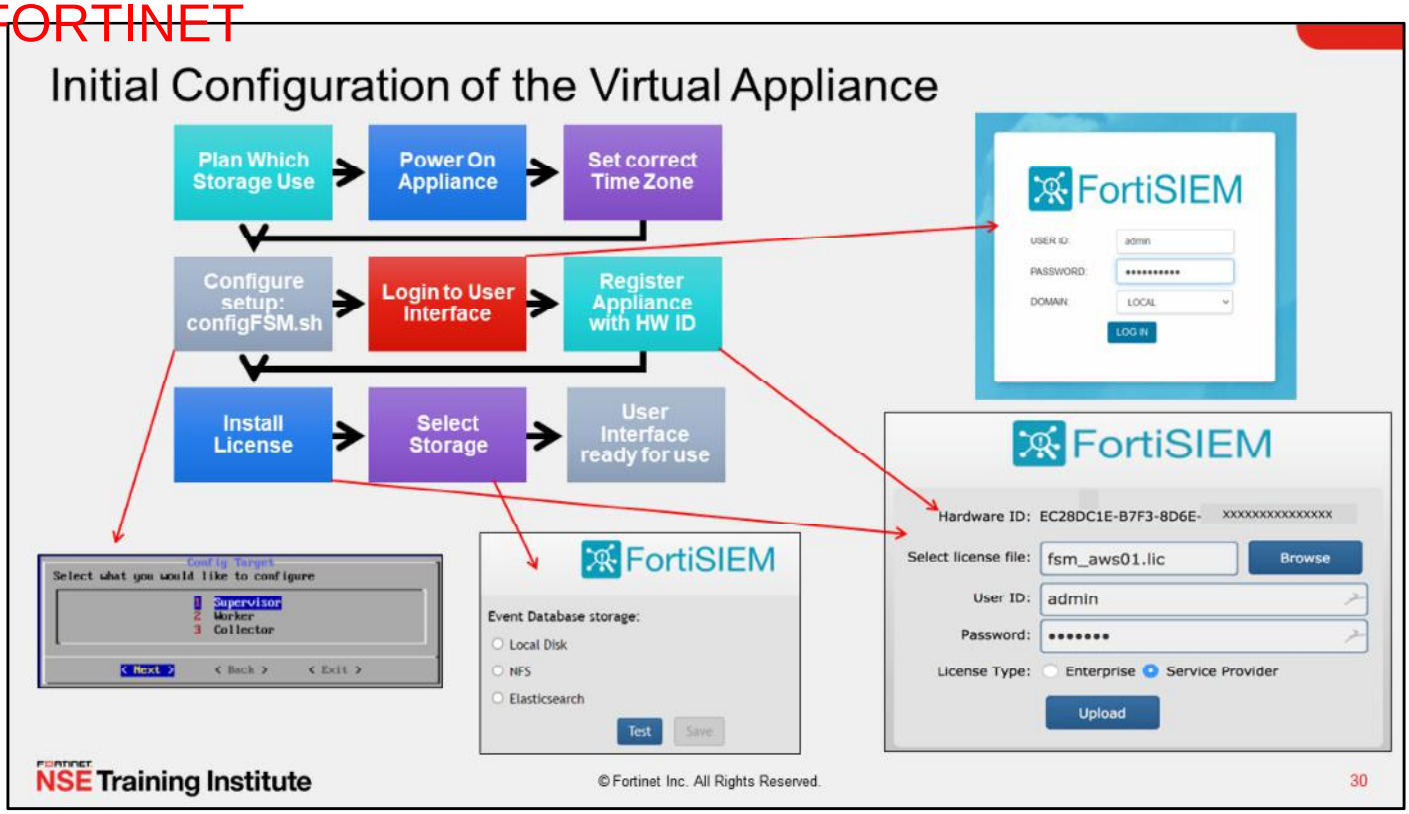


After completing this section, you should be able to achieve the objectives shown on this slide.

By demonstrating competence in system diagnostics, you will be able to discover and diagnose general information about the status of FortiSIEM.

Vouchers & Dumps are Available | WhatsApp +201224560923

DO NOT REPRINT Brave-dumps.com
© FORTINET



Installing the virtual appliance is straightforward.
First, decide what type of installation you want to deploy and request the appropriate license. For example, will you need a simple enterprise license or a multi-tenant license? Will you need Windows agents?
Download the correct virtual appliance for your hypervisor. For example, will you deploy FortiSIEM on VMware, Windows Hyper-V, Amazon Web Services (AWS), or Redhat KVM?
After you've imported the virtual appliance into your virtualization network, and *before* you start the VM, you must change some settings on the VM. For example, depending on your network, you must set the correct amount of memory and number of CPUs.
If the network will be a single-supervisor network, you can use NFS or local storage. If you plan to use a local virtual disk, remember to add it *before* you start the VM. Note that the maximum virtual disk size is 2 TB.

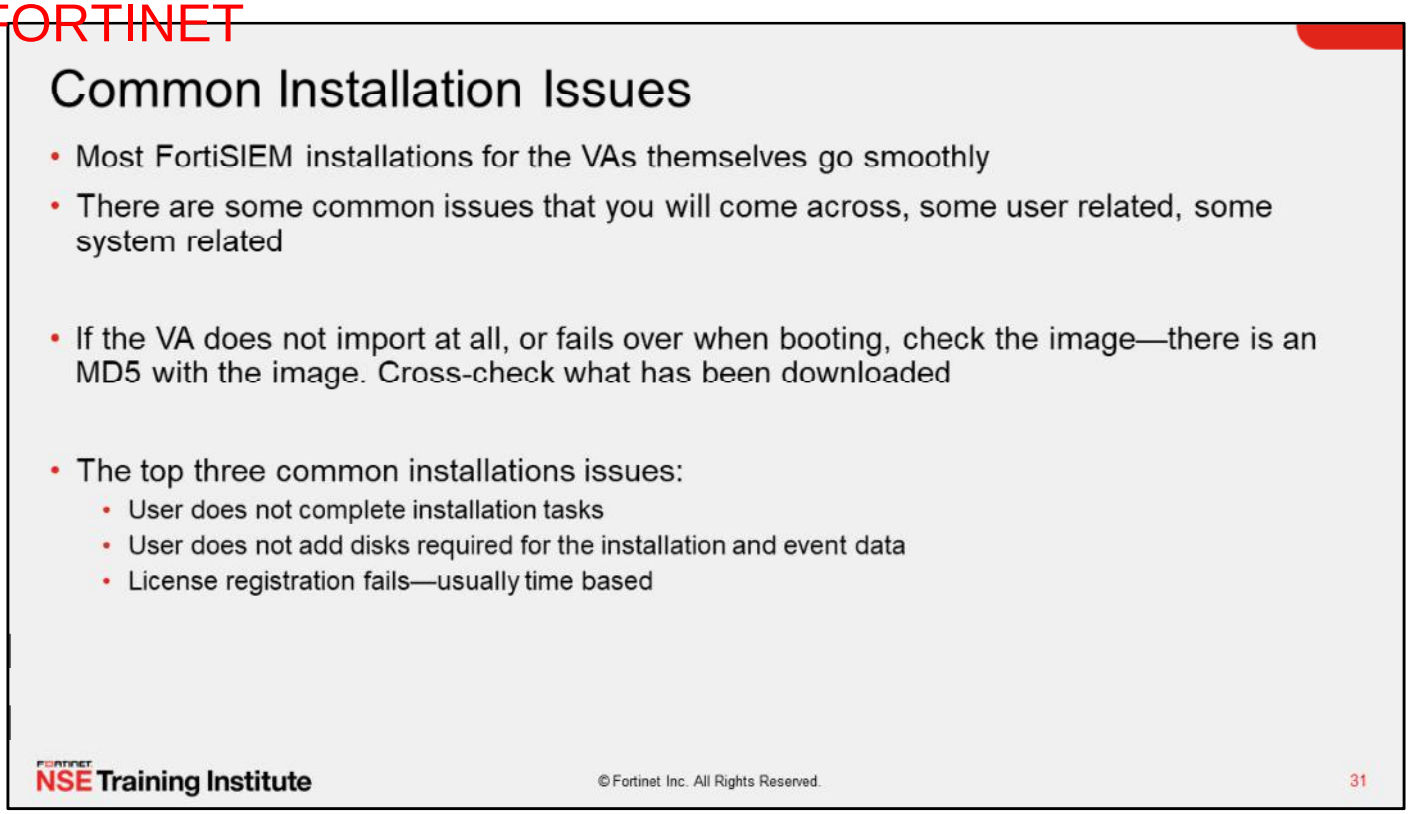
The installation process for any FortiSIEM deployment consists of the following steps:

1. Request a license.
2. Download the correct virtual appliance for your hypervisor.
3. Import the virtual appliance into your hypervisor network.
4. Plan which storage to use.
5. Edit the virtual appliance hardware settings:
    - Add memory and CPU based on the needs of the network.
    - If not using NFS/Elastic Search, add a local virtual disk for the event database for the virtual machine.
6. Start and configure the virtual appliance in the hypervisor console.
7. Register the virtual appliance.

Finally, start the virtual appliance and configure some basic settings, such as the time zone and event database location (NFS or virtual disk).
For more information, refer to the *FortiSIEM User Guide.*

Vouchers & Dumps are Available | WhatsApp +201224560923

DO NOT REPRINT
© FORTINET
Brave-dumps.com



Most FortiSIEM installations for the VAs themselves go smoothly, there are some common issues that you will come across—some user related, some system related. If the VA does not import at all, or fails over when booting, check the image. There is an MD5 with the image, cross-check what has been downloaded.

The top three common installations issues:
- User does not complete installation tasks.
- User does not add disks required for the installation and event data.
- License registration fails—usually time based.

Vouchers & Dumps are Available | WhatsApp +201224560923

DO NOT REPRINT
© FORTINET
Brave-dumps.com

Installation Issue—License Troubleshooting

- The license process requires two key pieces of information, which must be correctly and accurately entered into FortiCare
  - The license registration code: This is the code received on the Fortinet license certificate
  - The system hardware ID, or UUID: This is a system specific code that is displayed on the license page of the GUI



NSE Training Institute

© Fortinet Inc. All Rights Reserved.

32

The license process requires two key pieces of information, which must be correctly and accurately entered into FortiCare:

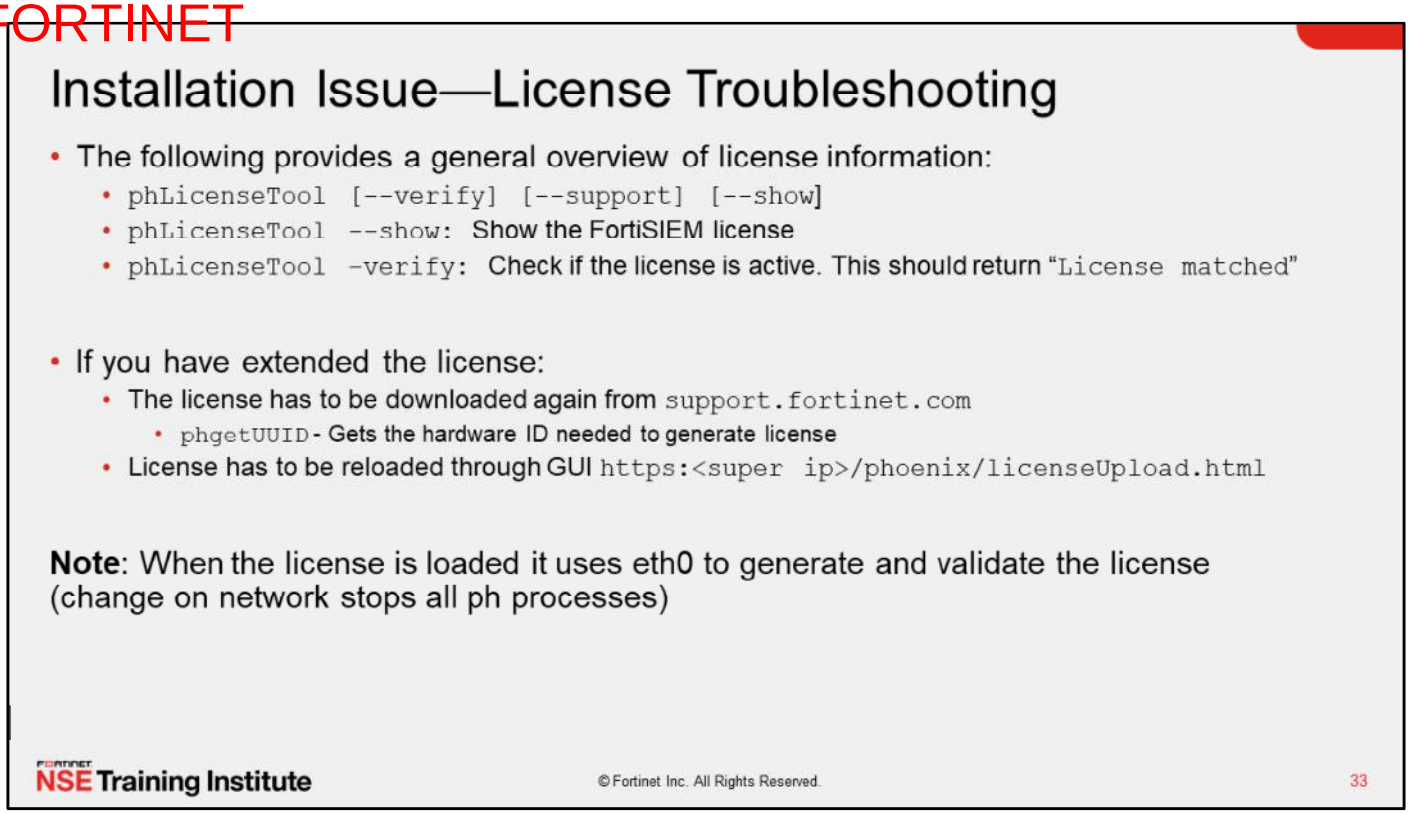
- The license registration code: This is the code received on the Fortinet license certificate.
- The system hardware ID, or UUID. This is a system-specific code that is displayed on the license page of the GUI.

If you enter either of these incorrectly into the FortiCare license registration screen, the license will be invalid and you must open a FortiCare customer services ticket to correct them.

Ensure the system has internet connectivity to allow the license validation process to complete. If it is not possible to provide internet access you must complete the offline license procedure.

Vouchers & Dumps are Available | WhatsApp +201224560923

DO NOT REPRINT
© FORTINET
Brave-dumps.com



This slide shows the CLI commands you can use to view license information.

If you have extended the license:

- The license has to be downloaded again from support.fortinet.com.
  - `phgetUUID` - Gets the Hardware ID needed to generate the license.
- The license must be reloaded using the FortiSIEM GUI.

Vouchers & Dumps are Available | WhatsApp +201224560923

DO NOT REPRINT
© FORTINET
Brave-dumps.com

Installation Issue—Offline License Registration

- `phLicenseTool` - Offline License Registration procedure
- SSH into FortiSIEM, User: `root` Password: `<password>`
  - `cd /opt/phoenix/bin`
  - `./phLicenseTool --collect license_req.dat`

```
[root@AccelOpsTest bin]# ./phLicenseTool --collect license_req.dat
[PH_GENERIC_DEBUG]:[eventSeverity]=LM_DEBUG,[procName]=<unknown>,[fileName]=phMi
scUtils.cpp,[lineNumber]=992,[phLogDetail]=Interface eth0 IP = 192.168.69.109
License information collected to the output file: license_req.dat
```

- Email this file back to support and they will return a license file to you
  - You can use WinSCP or similar to copy file from FortiSIEM
  - Copy this file to `/opt/phoenix/bin`
  - `./phLicenseTool --install license.dat`
  - Reboot - You should now be good to go

NSE Training Institute

© Fortinet Inc. All Rights Reserved.

34

When you apply the license, all looks fine, you enter your license details, and the system looks like it has been accepted, but then the license screen returns, and asks for the license details again.

The commonommon issue here is the time of the virtual machine. Also, check the ESX box itself for the time, and run a `phstatus` command to confirm the VA time is correct.

You can use `phLicenseTool`—the offiline offline license registration procedure, by using the commands shown on this slide.

Vouchers & Dumps are Available | WhatsApp +201224560923

DO NOT REPRINT
© FORTINET
Brave-dumps.com

Installation—Adding Additional VA Interfaces

- How do I add a an additional interface to the FortiSIEM VM?
- Steps:
  1. Power off the virtual machine
  2. Add the extra interface
  3. Power back on the virtual machine
  4. Connect over SSH to FortiSIEM
  5. Change directory:
     - `cd /etc/sysconfig/network-scripts`
  6. Clone the configuration file for eth0:
     - `cp ifcfg-eth0 ifcfg-eth1`
  7. `vi ifcfg-eth1`
  8. Edit the device and IP address (delete the gateway)
  9. Save the file
  10. Restart the networking services
      - service network restart

```
DEVICE=eth1
BOOTPROTO=none
ONBOOT=yes
TYPE=Ethernet
IPADDR=192.168.69.45
NETMASK=255.255.255.0
BROADCAST=192.168.69.255
```

NSE Training Institute

© Fortinet Inc. All Rights Reserved.

35

This slide shows the steps you can follow to add additional virtual machine network interfaces.

Vouchers & Dumps are Available | WhatsApp +201224560923

DO NOT REPRINT
© FORTINET
Brave-dumps.com

Installation—Temporary Routes

- How do I view the routing table in FortiSIEM?
- On CLI type: `route`:

```
[root@AccelOps3_1_2 ~]# route
Kernel IP routing table
Destination     Gateway         Genmask         Flags Metric Ref    Use Iface
192.168.69.0    *               255.255.255.0   U     0      0        0 eth0
169.254.0.0     *               255.255.0.0     U     0      0        0 eth0
default         192.168.69.1    0.0.0.0         UG    0      0        0 eth0
```

- Add a route:

```
route add -net 10.0.0.0/24 gw 192.168.69.203
```

- Delete a route:

```
route del -net 10.0.0.0/24 gw 192.168.69.203
```

- Add or delete the default GW:

```
route add default gw 192.168.69.2
```

NSE Training Institute

© Fortinet Inc. All Rights Reserved.

36

This slide shows how you can add temporary routes on FortiSIEM.

Vouchers & Dumps are Available | WhatsApp +201224560923

DO NOT REPRINT
© FORTINET
Brave-dumps.com

Installation—Making Routes Persistent

- To make these persistent, the static route configuration is stored in `/etc/sysconfig/network-scripts/route-int` file
  - For example: `/etc/sysconfig/network-scripts/route-eth0`
- Define the static routes in the format:
  - `<network/mask> via <gateway ip> dev <interface>`

```
20.20.20.0/24 via 192.168.69.100 dev eth0
30.30.30.0/24 via 192.168.69.200 dev eth0
```

- Routes will not appear in the routing table until you restart the network service:
  - `service network restart`

NSE Training Institute

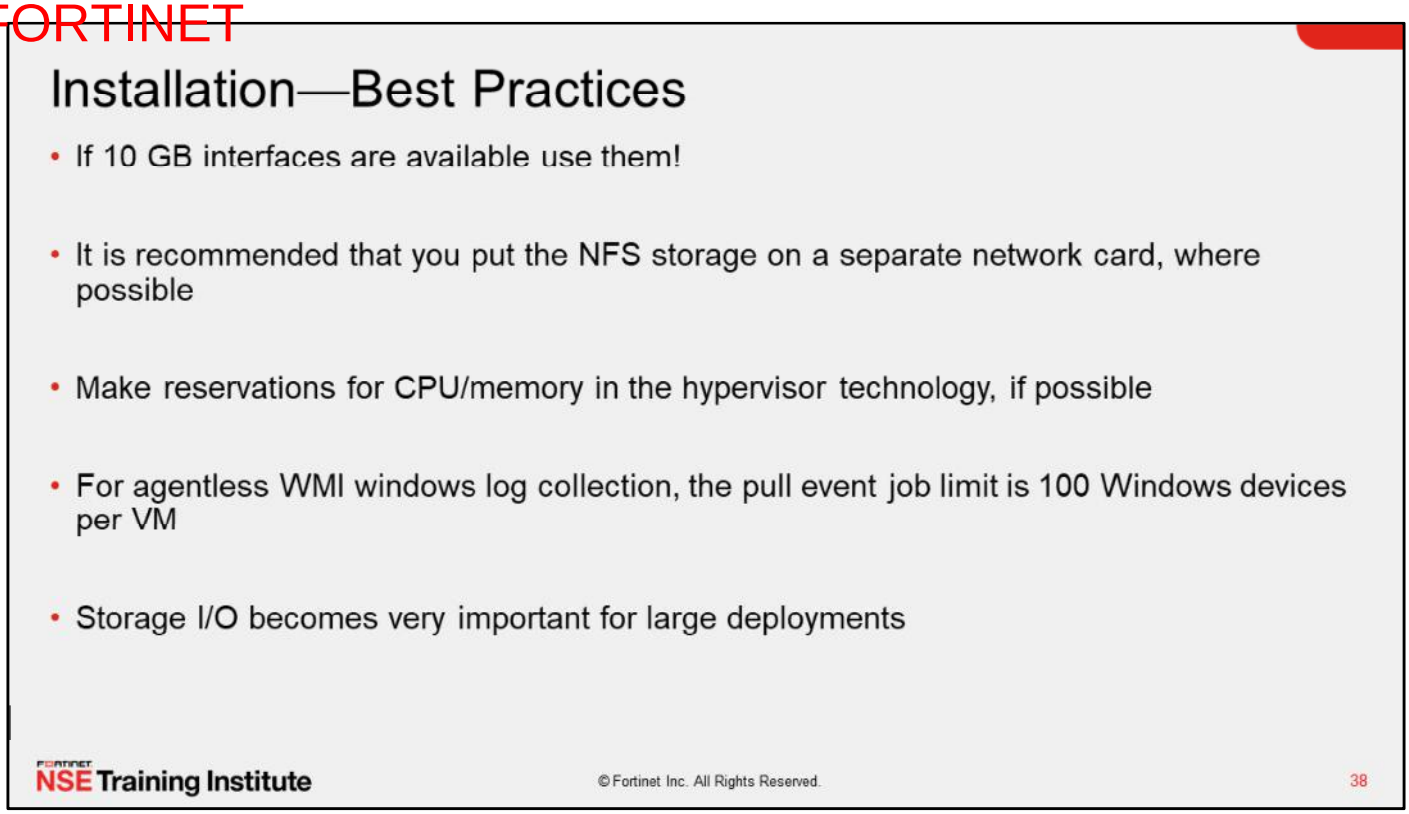
© Fortinet Inc. All Rights Reserved.

37

This slide shows you can make routes persistent in FortiSIEM.

Vouchers & Dumps are Available | WhatsApp +201224560923

DO NOT REPRINT
© FORTINET
Brave-dumps.com



Use the following best practices when you are installing FortiSIEM:

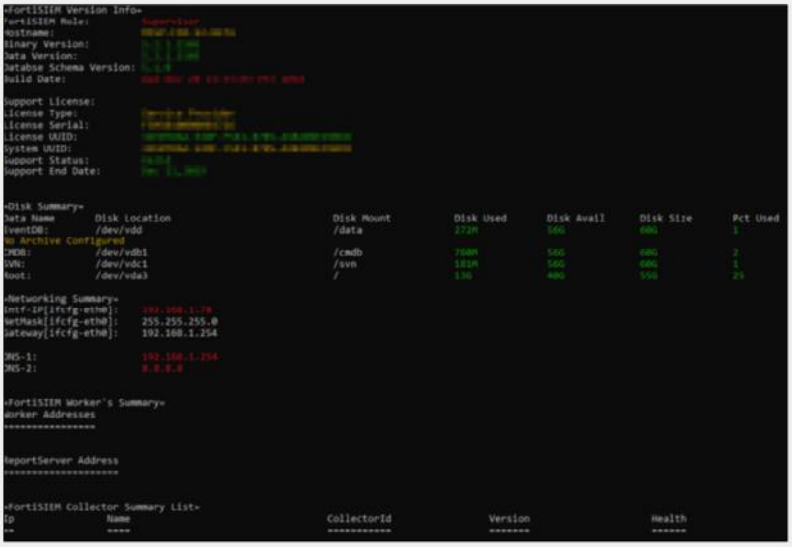
- If 10 GB interfaces are available, use them.
- It is recommended that you put the NFS storage on a separate network card, where possible.
- Make reservations for CPU/memory in the hypervisor technology, if possible.
- For agentless WMI windows log collection, the pull event job limit is 100 Windows devices per VA.
- Storage I/O becomes very important for large deployments.

Vouchers & Dumps are Available | WhatsApp +201224560923

DO NOT REPRINT
© FORTINET
Brave-dumps.com

Gathering System Information

- The script provides a general overview of system information:
  - /opt/phoenix/bin/phshowVersion.sh
- phshowVersion.sh
  - Provides license information
  - Provides version information
  - Local disk usage
  - Local network details
  - Workers address list
  - Collector details



NSE Training Institute

© Fortinet Inc. All Rights Reserved.

39

If you need to gather information about the FortiSIEM system, you can use the script `phshowVersion.sh`. The script provides a general overview of system information that includes:

- License information
- Version information
- Local disk usage
- Local network details
- Workers address list
- Collector details

Vouchers & Dumps are Available | WhatsApp +201224560923

DO NOT REPRINT
© FORTINET
Brave-dumps.com

Troubleshooting Commands—Viewing System Services Status

- Phstatus
  - Useful information: system load, CPU and memory usage, and uptime of various back-end processes
  - The system time is shown in the upper-right corner

```
Every 1.0s: /opt/phoenix/bin/phstatus.py                    FSM_NSE5.local: Tue Nov  9 18:30:03 2021

System uptime:  18:30:04 up 4 days,  2:53,  1 user,  load average: 3.66, 2.26, 2.13
Tasks: 28 total, 1 running, 27 sleeping, 0 stopped, 0 zombie
Cpu(s): 0 cores, 21.0%us, 1.0%sy, 0.0%ni, 75.9%id, 0.0%wa, 3.0%hi, 0.1%si, 0.0%st
Mem: 24468876k total, 14526592k used, 801552k free, 5244k buffers
Swap: 26058744k total, 933960k used, 25124784k free, 10124352k cached


PROCESS                 UPTIME          CPU%        VIRT_MEM      RES_MEM

phParser                4-02:49:26      2           2447m         1460m
phQueryMaster           4-02:49:43      0           1124m         106m
phRuleMaster            4-02:49:43      0           1699m         962m
phRuleWorker            4-02:49:43      0           1429m         795m
phQueryWorker           4-02:49:43      0           1459m         582m
phDataManager           4-02:49:43      0           3828m         1915m
phDiscover              4-02:42:41      0           745m          242m
phReportWorker          4-02:49:43      0           1491m         666m
phReportMaster          4-02:49:43      0           750m          88m
phIpIdentityWorker      4-02:49:43      0           1044m         567m
phIpIdentityMaster      4-02:49:43      0           525m          38m
phAgentManager          4-02:49:43      0           1560m         75m
phCheckpoint            4-02:49:43      0           315m          46m
phPerfMonitor           4-02:49:43      11          1546m         782m
phReportLoader          4-02:49:43      0           835m          285m
phDataPurger            4-02:49:43      0           777m          214m
phEventForwarder        4-02:49:43      0           547m          35m
phMonitor               4-02:49:48      0           1313m         583m
Apache                  4-02:53:43      0           306m          15m
Rsyslogd                4-02:52:43      0           190m          5056k
Node.js-charting        1-20:21:42      0           614m          60m
Node.js-pm2             4-02:52:37      0           705m          62m
phFortiInsightAI        4-02:53:43      0           13996m        325m
AppSvr                  4-02:52:35      5           11168m        3917m
DBSvr                   4-02:53:43      0           425m          32m
phAnomaly               4-02:49:46      0           982m          52m
SVNLite                 4-02:53:43      0           9955m         482m
Redis                   4-02:52:38      0           91m           46m
```

NSE Training Institute
© Fortinet Inc. All Rights Reserved.
40

You can use the `phstatus` to view the summary of which services are running. This command provides useful information, for example, system load, CPU and memory usage, and the uptime of various back-end processes. All services should be up, as shown in the example on the slide.

If services are down this may indicate:
- The system is still starting. It can take several minutes for the system to start following a reboot.
- The system is not licensed. Services will not start if you have an invalid license applied to the system.
- There is a more serious technical problem with the system and it requires further investigation.

Vouchers & Dumps are Available | WhatsApp +201224560923

DO NOT REPRINT
© FORTINET
Brave-dumps.com

FortiSIEM Components Processes and Functions

Process	Function	Supervisor	Worker	Collector
phMonitor	Monitors other processes	★	★	★
phDiscover	Pulling basic data from target	★		★
phPerfMonitor	Execute Performance Job	★	★	★
phAgentManager	Execute event pulling job	★	★	★
phCheckpoint	Execute checkpoint monitoring	★	★	★
phEventPackager	Uploading event/svn file to super/worker			★
phParser	Parsing event to shared store (SS)	★	★	★
phDataManager	Save event from SS to Event DB	★	★	
phRuleMaster	Decide if rules fire	★		
phRuleWorker	Aggregate data for rules	★	★	
phQueryMaster	Merge data from QueryWorker	★		
phQueryWorker	Execute Query task	★	★	
phReportMaster	Merge data from ReportWorker	★		
phReportWorker	Aggregate data for Reports	★	★	
phIdentityMaster	Merge IP Identity info	★	★	
phIdentityWorker	Collect IP Identity info	★	★	
Apache	Receive event/svn file from collector	★	★	

NSE Training Institute

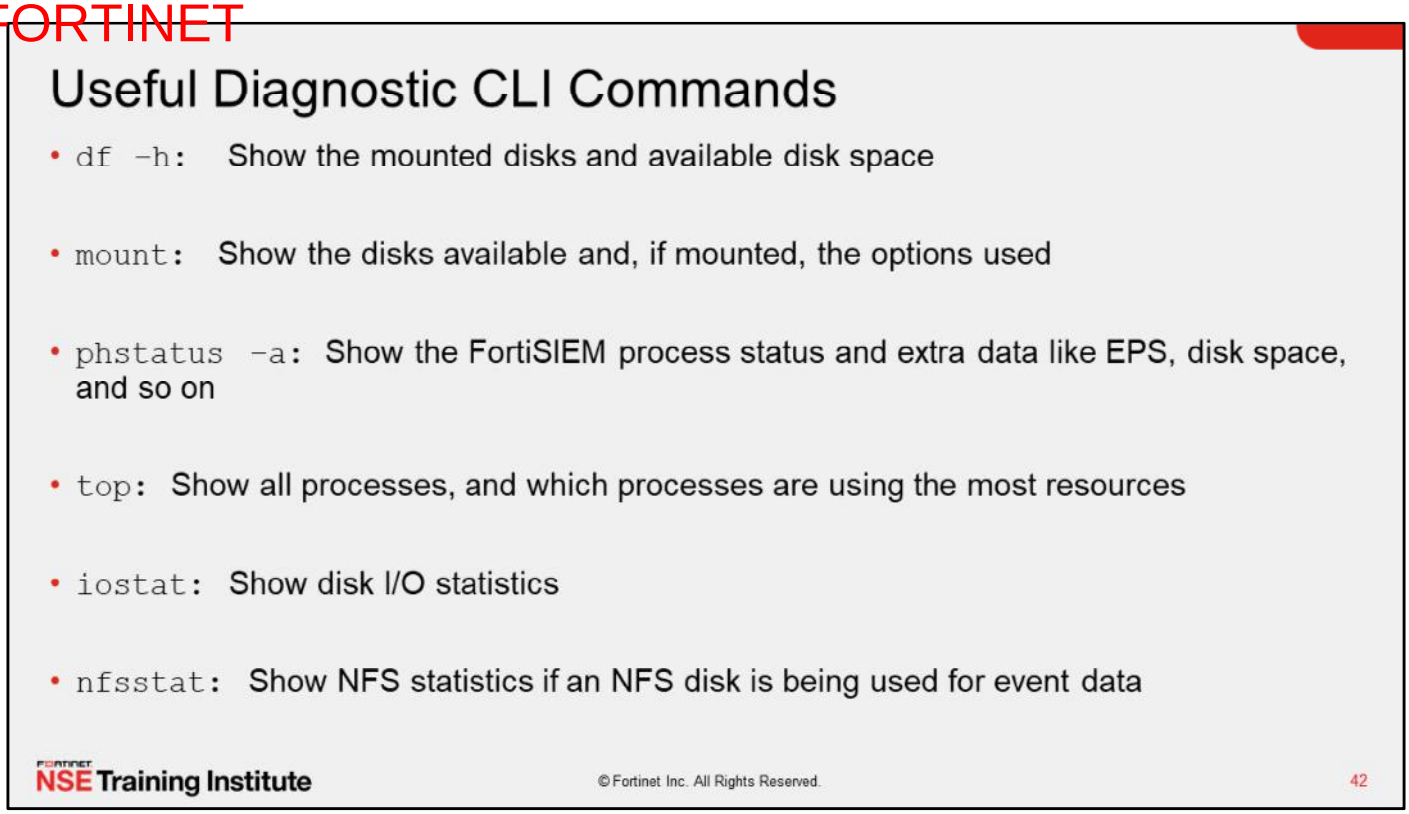
© Fortinet Inc. All Rights Reserved.

41

This slide shows FortiSIEM processes based on components. All back-end processes run mainly on the supervisor. The workers and collectors are responsible for dedicated tasks, so fewer processes will run based on the requirement to perform tasks.

Vouchers & Dumps are Available | WhatsApp +201224560923

DO NOT REPRINT
© FORTINET
Brave-dumps.com

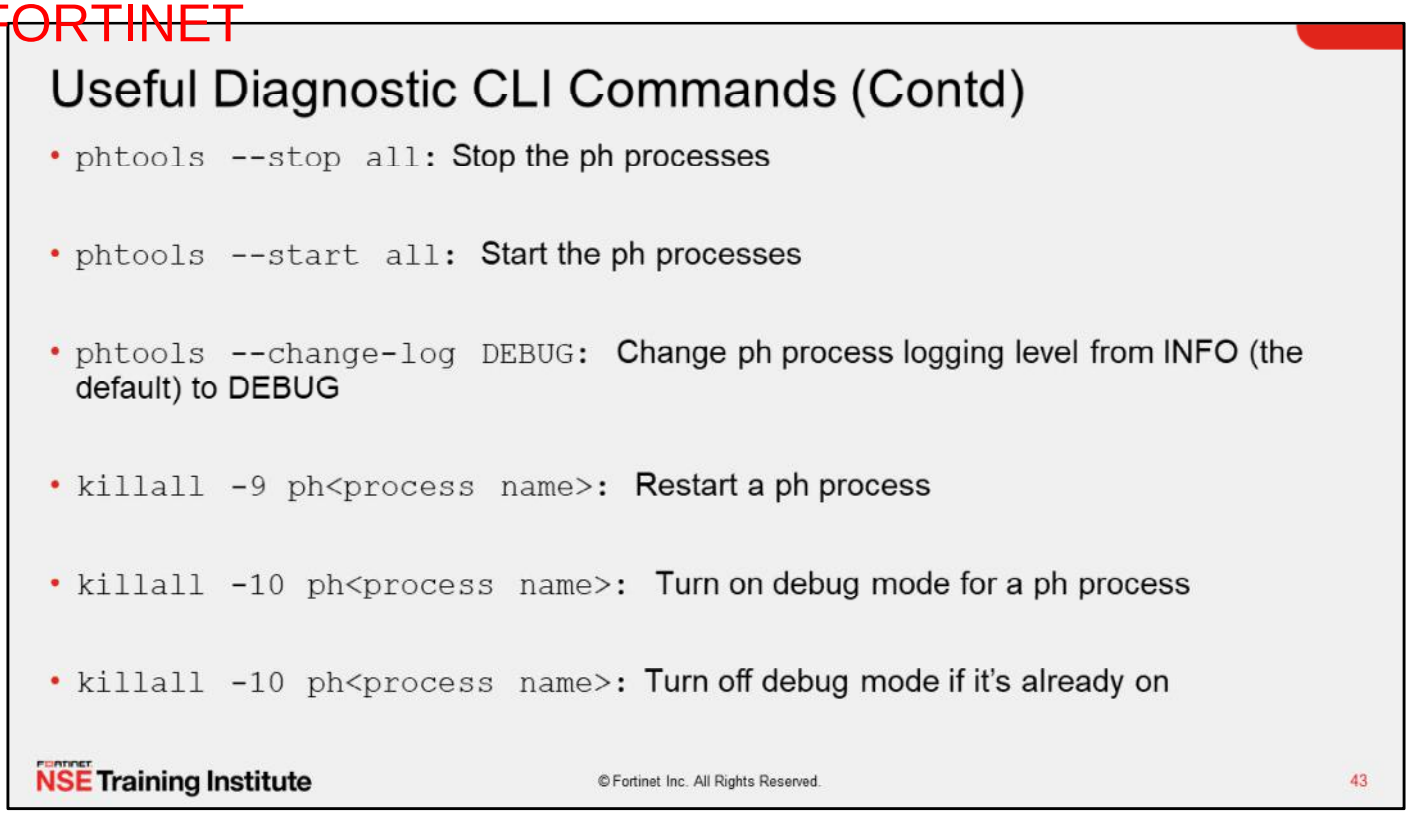


This slide shows some diagnostics CLI commands:

- `df -h`: Show the mounted disks, and available disk space.
- `mount`: Show the disks available, and, if mounted, the options used.
- `phstatus.sh`: Show the FortiSIEM process status.
- `phstatus -a`: Show the FortiSIEM process status and extra data like events per seconds (EPS), disk space, and so on.
- `top`: Show all processes, and which processes are using the most resources.
- `iostat`: Show disk I/O statistics.
- `nfsstat`: Show NFS statistics if an NFS disk is being used for `/data`.

Vouchers & Dumps are Available | WhatsApp +201224560923

DO NOT REPRINT
© FORTINET
Brave-dumps.com

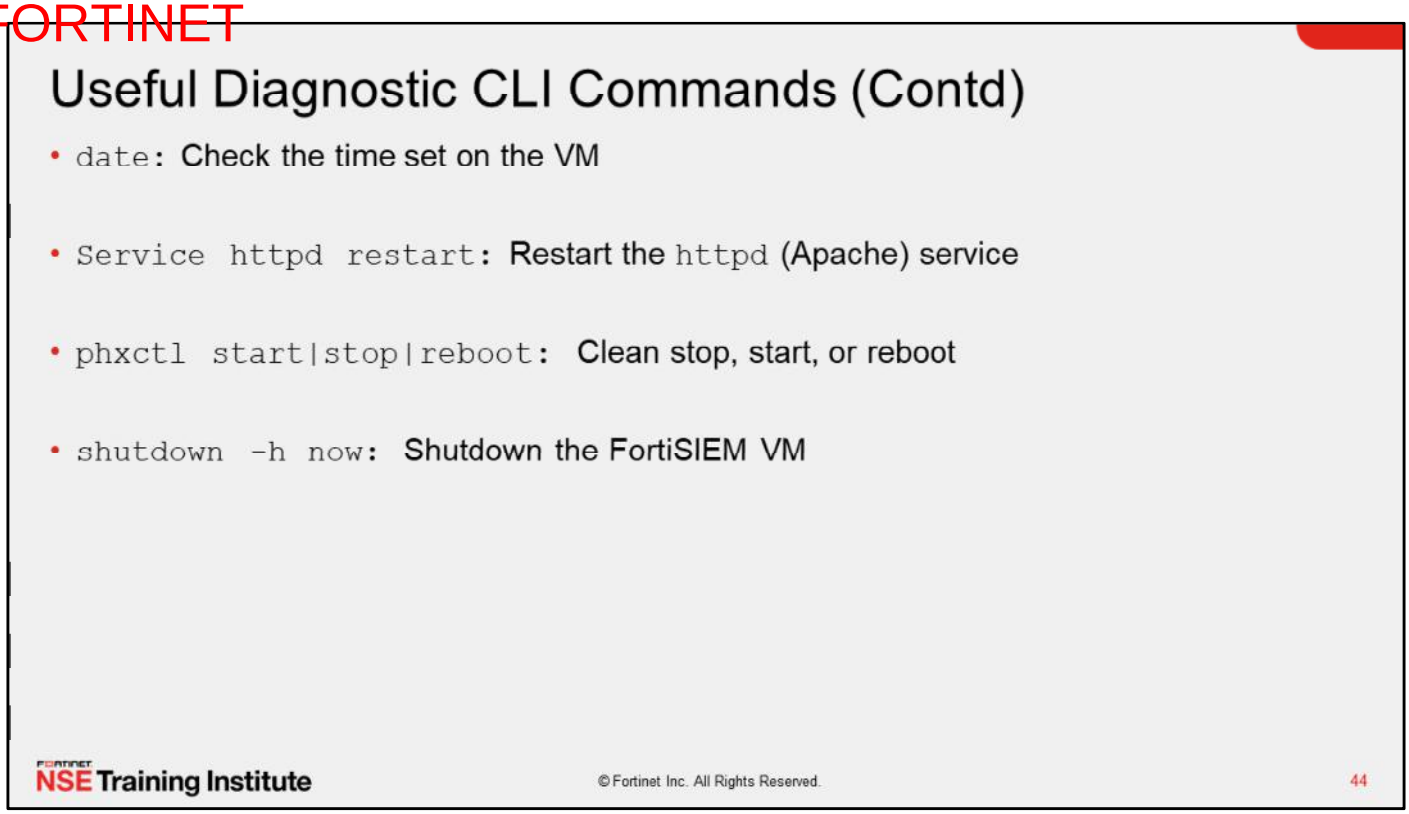


This slide shows use of few more useful diagnostic CLI commands.

- `phtools --stop all`: Stop the ph processes.
- `phtools --start all`: Start the ph processes.
- `phtools --change-log DEBUG`: Change ph process logging level from INFO (the default) to DEBUG.
- `killall -9 ph<process name>`: Restart a ph process.
- `killall -10 ph<process name>`: Turn on debug mode for a ph process.
- `killall -10 ph<process name>`: Turn off debug mode if it's already on.

Vouchers & Dumps are Available | WhatsApp +201224560923

DO NOT REPRINT
© FORTINET
Brave-dumps.com

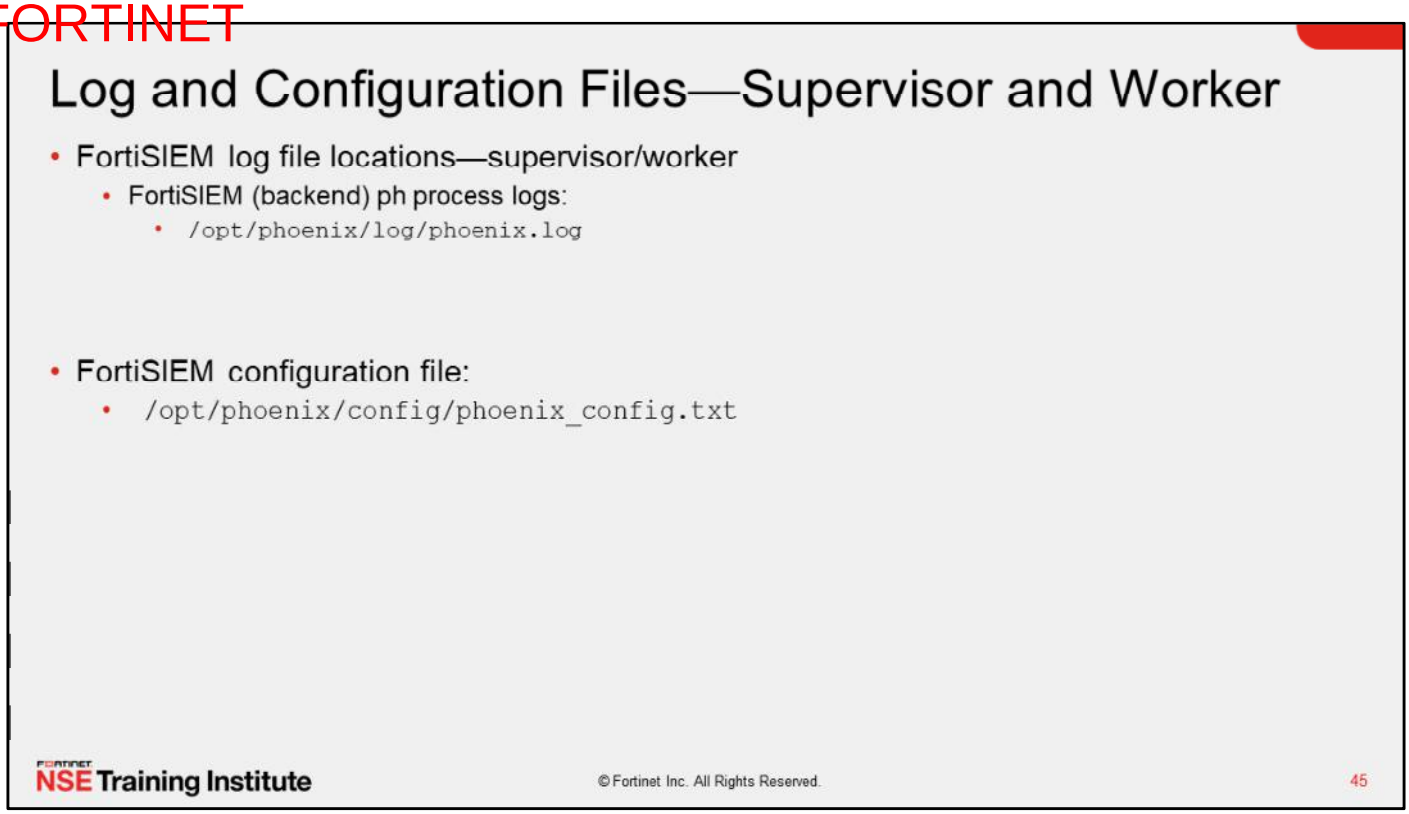


This slide shows more CLI diagnostic commands:

- `date`: Check the time set on the VM.
- `service httpd restart`: Restart the httpd (Apache) service.
- `phxctl start|stop|reboot`: Clean stop,start or reboot.
- `shutdown -h now`: Shut down the FortiSIEM VM.

Vouchers & Dumps are Available | WhatsApp +201224560923

DO NOT REPRINT
© FORTINET
Brave-dumps.com

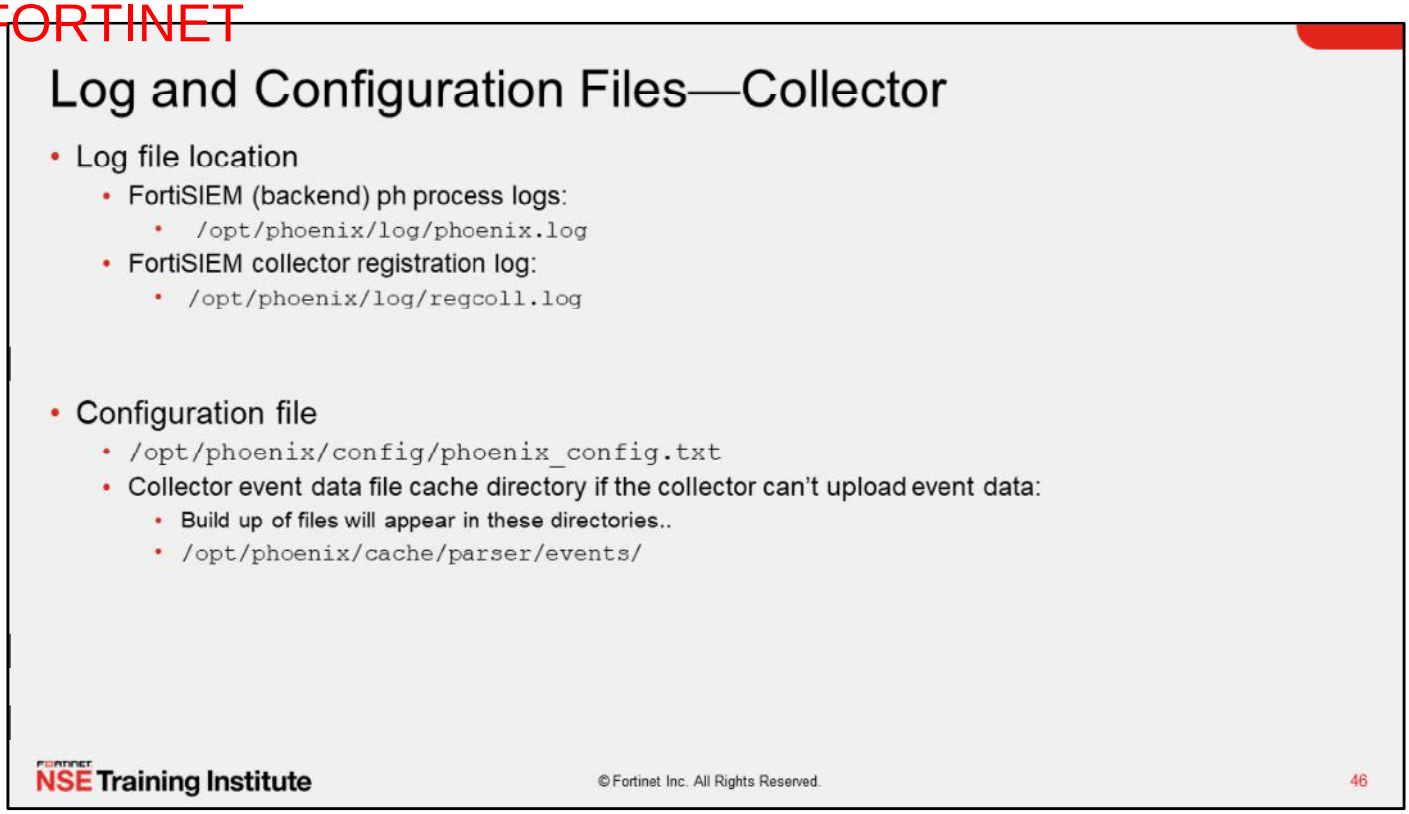


This slide shows the back-end configuration files for processes and applications running FortiSIEM. The main configuration file of FortiSIEM is `phoenix_config.txt`.

The slide also shows some useful log files, which you can use to diagnose problems, and their location paths. You can check back-end process logs on FortiSIEM in the main log file: `phoenix.log`.

Vouchers & Dumps are Available | WhatsApp +201224560923

DO NOT REPRINT
© FORTINET
Brave-dumps.com



You can check back-end process logs on the collector in the file `phoenix.log` and, if you need to check the collector registration logs, you can find them in `regcoll.log`.

If you need to make any configuration changes, you need modify `phoenix_config.txt`. If collector is unable to upload event data to the supervisor, it will store files in the `/opt/phoenix/cache/parser/events/` folder.

Vouchers & Dumps are Available | WhatsApp +201224560923

DO NOT REPRINT
© FORTINET
Brave-dumps.com

FortiSIEM—Health Check Scripts

- Provides overall summary and view of FortiSIEM health
- Health check scripts available from version 5.3.0 of FortiSIEM
  - /opt/phoenix/bin/get-fsm-health.py
- Three ways to get the information:
  - ./get-fsm-health.py <super-ip> -u ec2-user -k <ssh key> -n <# nodes> -o fsm-aws.txt
  - ./get-fsm-health.py <super-ip> -u <user> -p <password> -n <# nodes> -o fsm- remote.txt
  - ./get-fsm-health.py -local -o fsm-health.txt

```
[root@FSM_NSE5 bin]# get-fsm-health.py --local
------------------------------------------------------------
                    Health Check
============================================================
Tue Nov 09 18:55:45 EST 2021
--------------------
Fetching Information from Local.
- Host Info ..................................... succeeded.
- FortiSIEM Version ............................. succeeded.
- FortiSIEM License info ........................ succeeded.
- Configuration ................................. succeeded.
- CMDB Info ..................................... succeeded.
- Largest CMDB Tables ........................... succeeded.
- EPS Info ...................................... succeeded.
- Worker Upload Event Queue Info ................ succeeded.
- Inline Report Queue ........................... succeeded.
- Active Queries ................................ succeeded.
- Load Average .................................. succeeded.
- CPU Usage Details ............................. succeeded.
- Top 5 Processes by CPU ........................ succeeded.
- Memory Usage .................................. succeeded.
- Swap Usage .................................... succeeded.
- Top 5 Processes by Resident Memory ............ succeeded.
- Disk Usage .................................... succeeded.
- IOStat ........................................ succeeded.
- Top 5 Processes by IO ......................... succeeded.
- NFSIOStat ..................................... succeeded.
- NFS Disk Operations Time (second) ............. succeeded.
- Top 10 Slow EventDB Queries ( > 1 min) Today ..... succeeded.
- Top 5 Rule with Large Memory Today ............ succeeded.
- FortiSIEM Process Uptime Less Than 1 day ...... succeeded.
- Top 5 log files in /var/log ................... succeeded.
- FortiSIEM Shared Store Status ................. succeeded.
- App Server Exceptions Today ................... succeeded.
- Backend Errors Today .......................... succeeded.
- Backend Segfaults Today ....................... succeeded.
- Patched files ................................. succeeded.
- Outstanding Discovery Jobs .................... succeeded.
- FortiSIEM Log File Size ....................... succeeded.
- FortiSIEM Fall Behind Jobs .................... succeeded.
- FortiSIEM Jobs Distribution ................... succeeded.
------------------------------------------------------------
                    Data Collection
============================================================
All data was collected.
```

NSE Training Institute

© Fortinet Inc. All Rights Reserved.

47

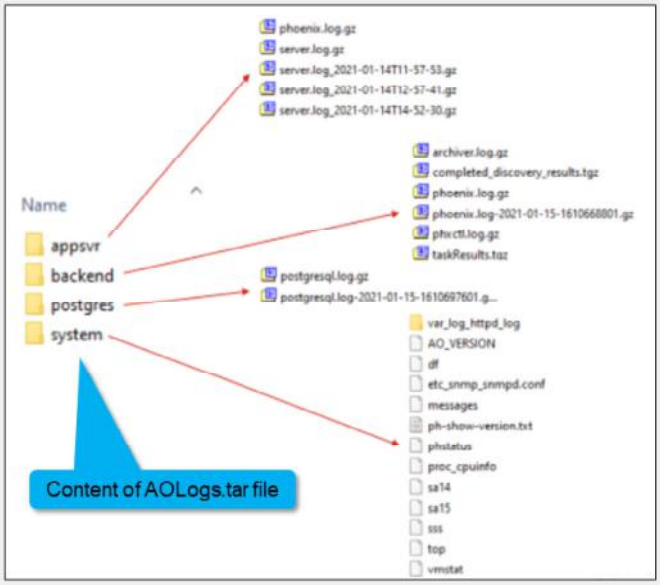
The health check scripts provides an overall summary and view of FortiSIEM health. It sends the results to standard output, but it is always recommended to send the results to an external file.

Vouchers & Dumps are Available | WhatsApp +201224560923

DO NOT REPRINT
© FORTINET
Brave-dumps.com

Collecting Back-end Logs for Fortinet Support

- The `phziplogs` command provides overall log summary, and support will need logs to troubleshoot issues:
  - `phziplogs`
    - `cd /opt/phoenix/bin`
      - `./phziplogs <directory> <number_of_days>`
      - `For example ./phziplogs /tmp/mycase 1`
- This will create a directory with your case number as well as collect logs for the number of days to go back to
- This grabs lots of information including `phoenix.log` files, and so on
- It compresses them in a zipfile ready for uploading to support
- The log name will still be `AOLogs.tar`



NSE Training Institute

© Fortinet Inc. All Rights Reserved.

48

To collect back-end logs, connect over SSH to FortiSIEM machine using `root` as the username and the password you set, and execute the command for `phziplogs` shown on this slide. This will create a directory with your case number, as well as collect logs for the number of days to go back to. The `phziplogs` command collects the logs after enabling debug, if needed. After logs have been collected, remember to disable debug. The longest length in time is seven days for a back-end pull for each node super, worker, and collector.
The log name will still be `AOLogs.tar`. The slide shows an example of content of `AOLogs.tar` file.

Vouchers & Dumps are Available | WhatsApp +201224560923

DO NOT REPRINT
© FORTINET
Brave-dumps.com

Knowledge Check

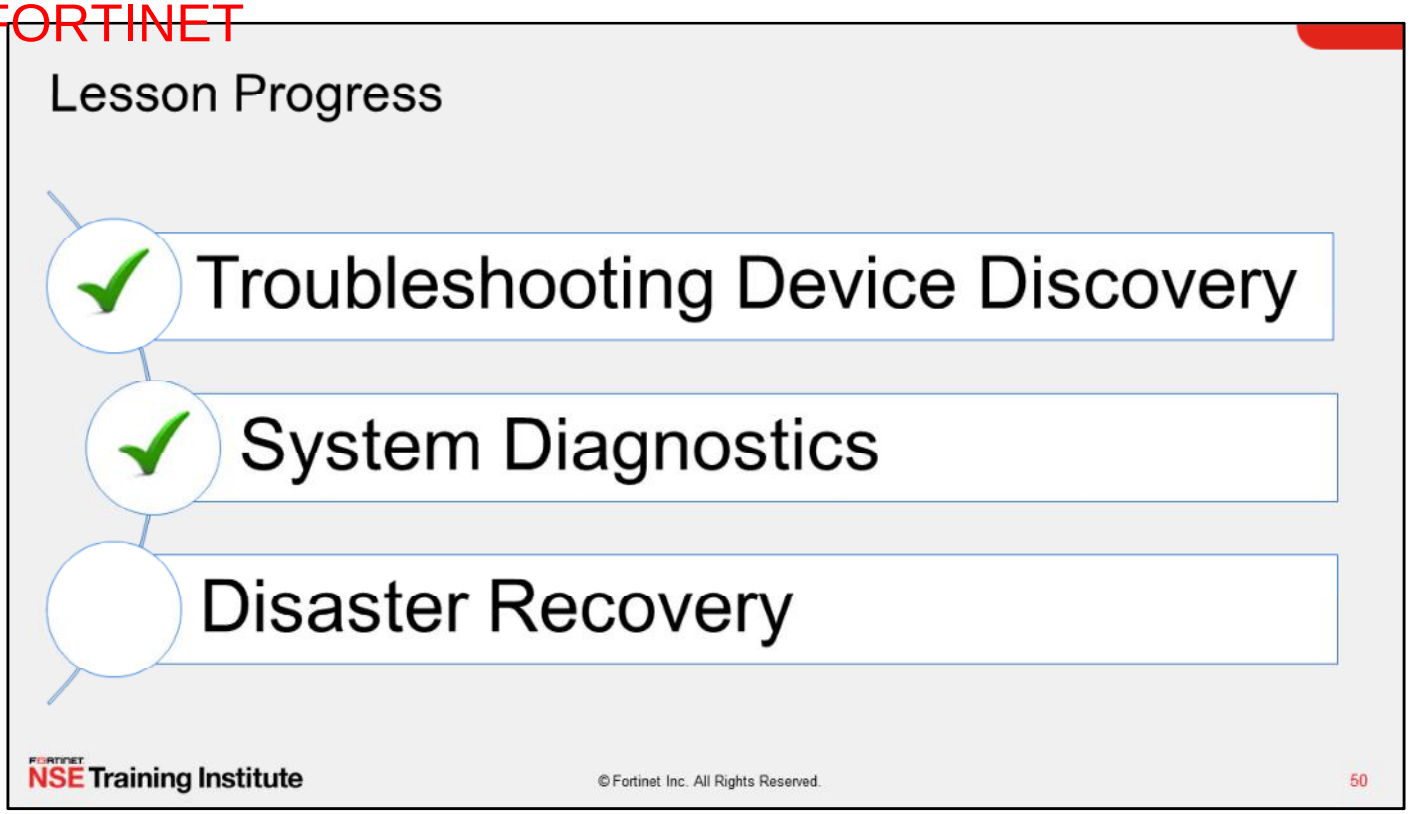
1. An administrator wants to check FortiSIEM license information. Which script will provide FortiSIEM license information?

✓ A. `phshowVersion.sh`
B. `phstatus.sh`

NSE Training Institute
© Fortinet Inc. All Rights Reserved.

Vouchers & Dumps are Available | WhatsApp +201224560923

DO NOT REPRINT
© FORTINET
Brave-dumps.com

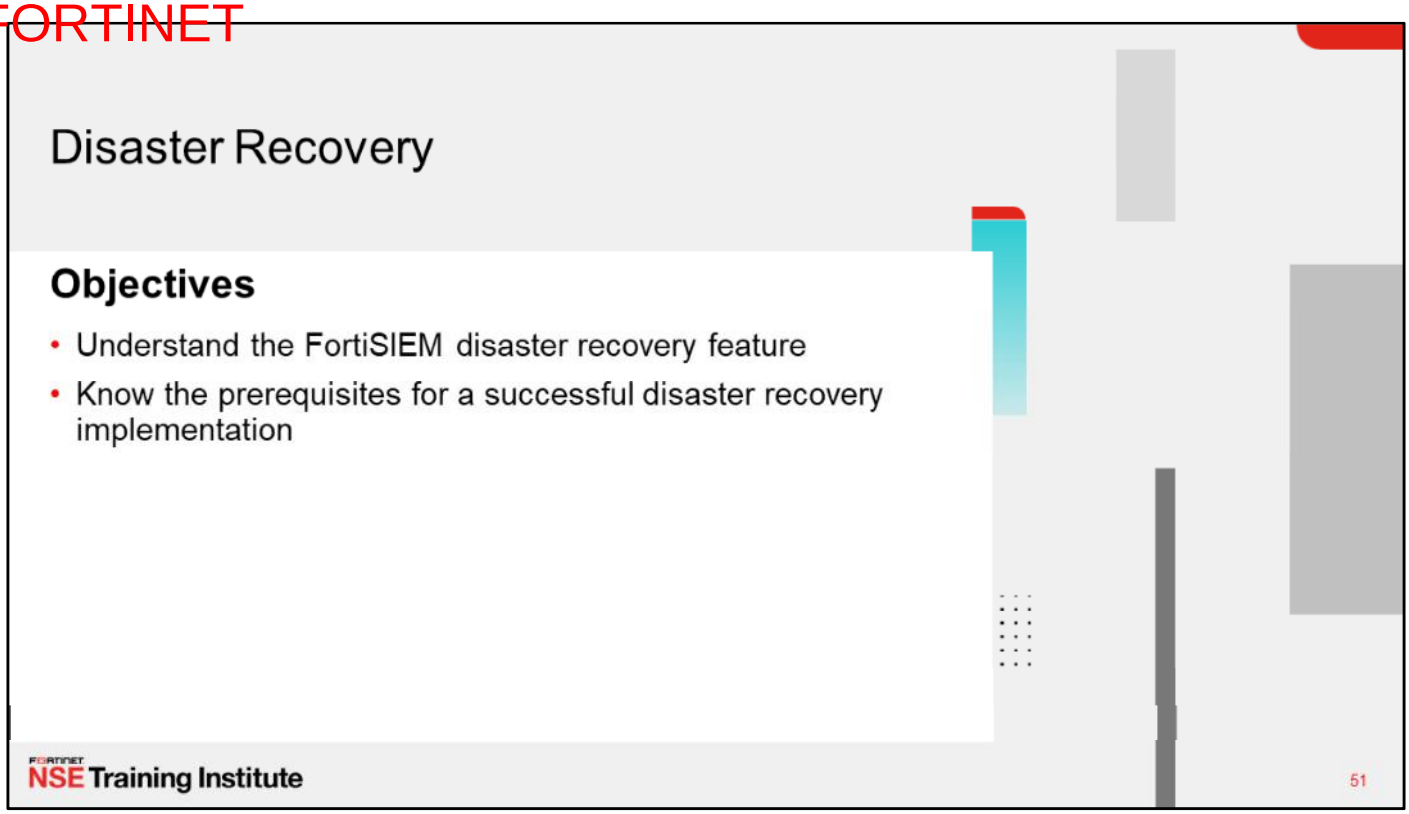


Good job! You now understand FortiSIEM system diagnostics.

Now, you will learn about the disaster recovery feature.

Vouchers & Dumps are Available | WhatsApp +201224560923

DO NOT REPRINT
© FORTINET
Brave-dumps.com



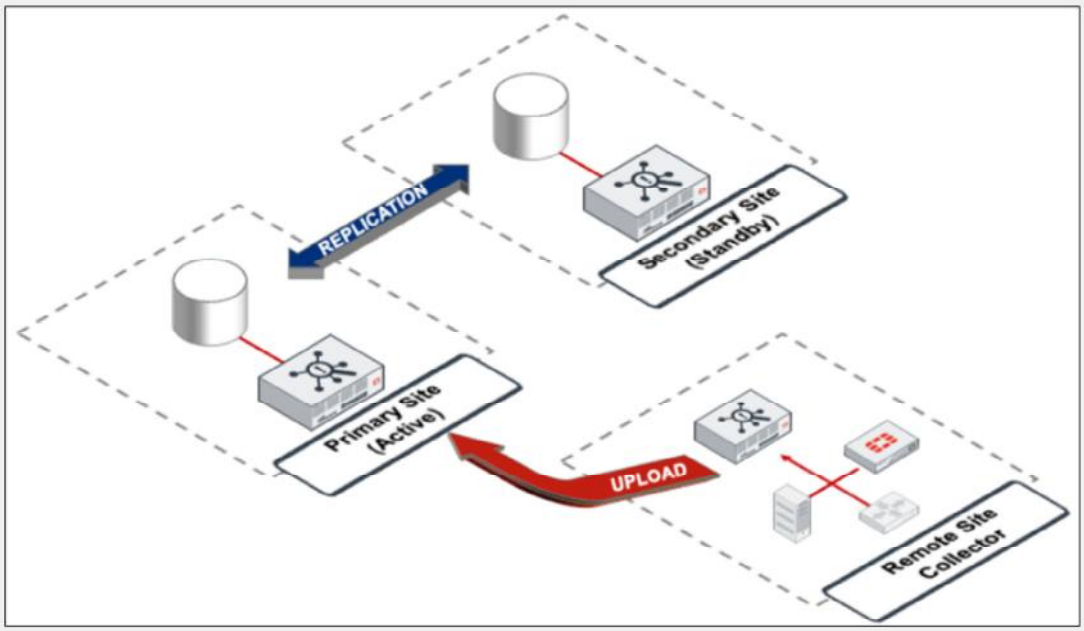
After completing this section, you should be able to achieve the objectives shown on this slide.

By demonstrating competence in FortiSIEM disaster recovery, you will be able to understand and implement disaster recovery operations in your network.

Vouchers & Dumps are Available | WhatsApp +201224560923

DO NOT REPRINT
© FORTINET
Brave-dumps.com

Understanding the FortiSIEM Disaster Recovery Feature



NSE Training Institute

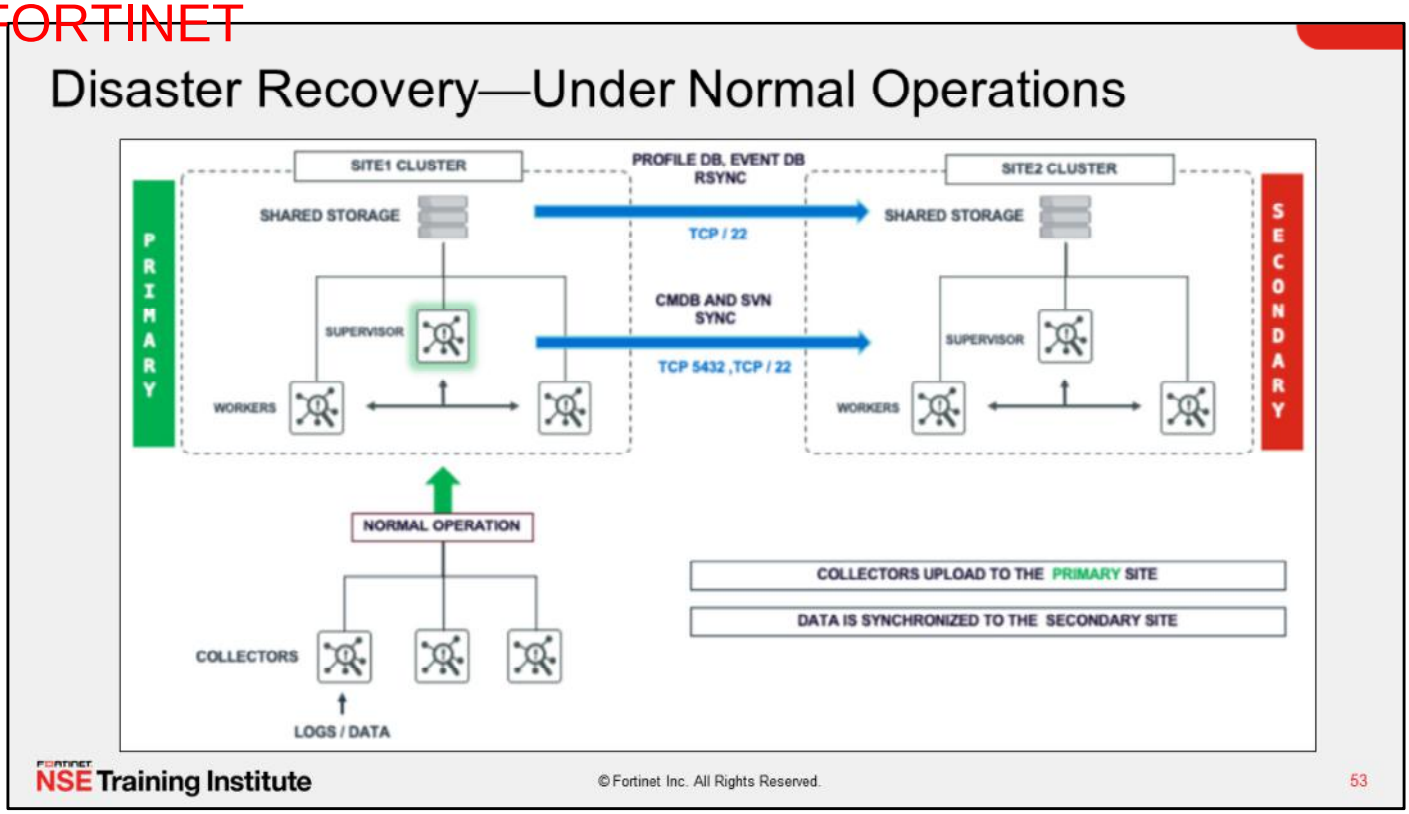
© Fortinet Inc. All Rights Reserved.

52

FortiSIEM has a replication feature, designed for those customers who require full disaster recovery capabilities, where one site is designated to be the primary (active) site, site 1, and the other the secondary (hot standby) site, site 2. The two systems replicate the primary site (site 1) database. This requires a second fully licensed FortiSIEM system, where site 1 (primary) and site 2 (secondary) are set up identically in terms of supervisor, workers, and event storage.

Vouchers & Dumps are Available | WhatsApp +201224560923

DO NOT REPRINT
© FORTINET
Brave-dumps.com



Under normal operations, if collectors are being used, these upload to site 1, the primary site, and buffer by design, when this site is not available. If disaster recovery is set up and a disaster occurs, then these same collectors will revert to uploading to site 2, the secondary site, which will now be designated as the primary, or active, site.

FortiSIEM runs as a single node for SMB or as a cluster with supervisor, worker, and collectors nodes.

To provide disaster recovery features, FortiSIEM must have a secondary system ready on standby to take over operations, with the following databases replicated from the primary site:

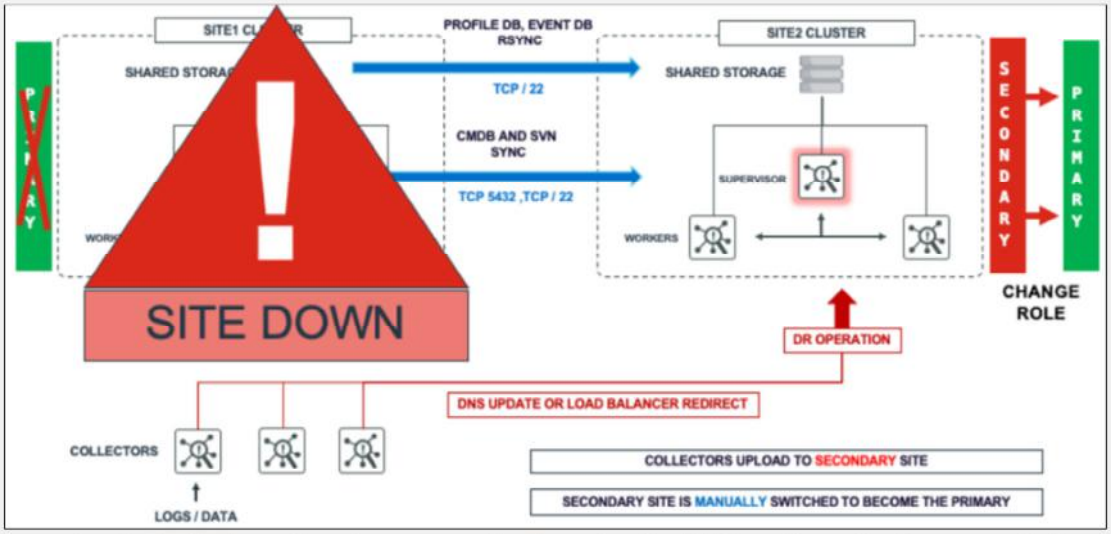
- The CMDB residing in a PostgresSQL database.
- Device configurations residing in SVN-lite on the supervisor node
- Profile data residing on SQLite databases on the supervisor node
- Event database stored in FortiSIEM EventDB (on local disk or NFS)

FortiSIEM supports disaster recovery for Elasticsearch-based environments as well.

Vouchers & Dumps are Available | WhatsApp +201224560923

DO NOT REPRINT
© FORTINET
Brave-dumps.com

Disaster Recovery—When Disaster Strikes



There are two tasks that must be done manually: changing the DNS configuration to ensure that users log on to the secondary server, and promoting the secondary supervisor to the primary role using the `phsecondary2primary` command

NSE Training Institute

© Fortinet Inc. All Rights Reserved.

54

When disaster strikes :

- The secondary (site 2) must become the primary FortiSIEM.
- You must make changes to the DNS configuration so that users log on to the secondary supervisor (site 2), and that collectors will send events to secondary workers.

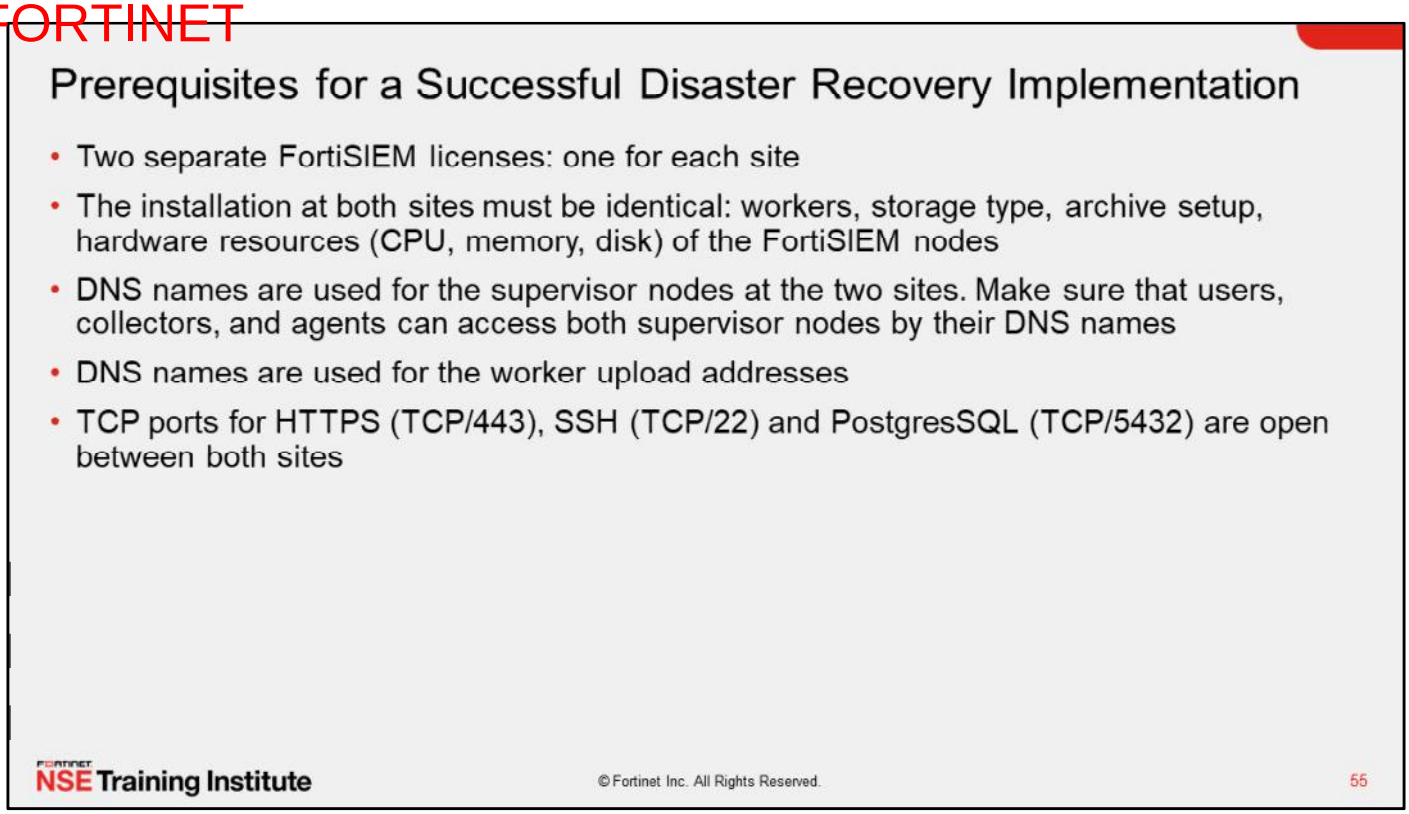
When the former primary (Site 1) is recovered and powered up, it will sync missing data with the secondary site (site 2, the active primary FortiSIEM) after it is added back as a new secondary site.

When you decide to return to the predisaster setup, you can switch the roles of primary (site 2) and secondary (site 1).

Note that in addition to making the required DNS changes manually, you must also perform the process for promoting the secondary supervisor to the primary supervisor node manually on the FortiSIEM CLI using the `phsecondary2primary` command.

Vouchers & Dumps are Available | WhatsApp +201224560923

DO NOT REPRINT
© FORTINET
Brave-dumps.com



For a successful disaster recovery implementation you need:

- Two separate FortiSIEM licenses: one for each site
- Identical installations at both sites: workers, storage type, archive setup, and hardware resources (CPU, memory, disk) of the FortiSIEM nodes
- DNS names are used for the supervisor nodes at the two sites. Make sure that users, collectors, and agents can access both supervisor nodes by their DNS names.
- DNS names are used for the worker upload addresses.
- TCP ports for HTTPS (TCP/443), SSH (TCP/22), and PostgresSQL (TCP/5432) are open between both sites.

Disaster recovery operation configuration is available for both EventDB or Elasticsearch-based environments. For more information, refer to the *FortiSIEM User Guide* on `https://docs.fortinet.com` for configuration of disaster recovery operations in EventDB or Elasticsearch-based environments.

Vouchers & Dumps are Available | WhatsApp +201224560923

DO NOT REPRINT
© FORTINET
Brave-dumps.com

Knowledge Check

1. To implement a successful disaster recovery operation, what must be identical in both the primary and secondary sites?

✓ A. Supervisor, workers, and storage type
B. Supervisor, collectors, and storage type

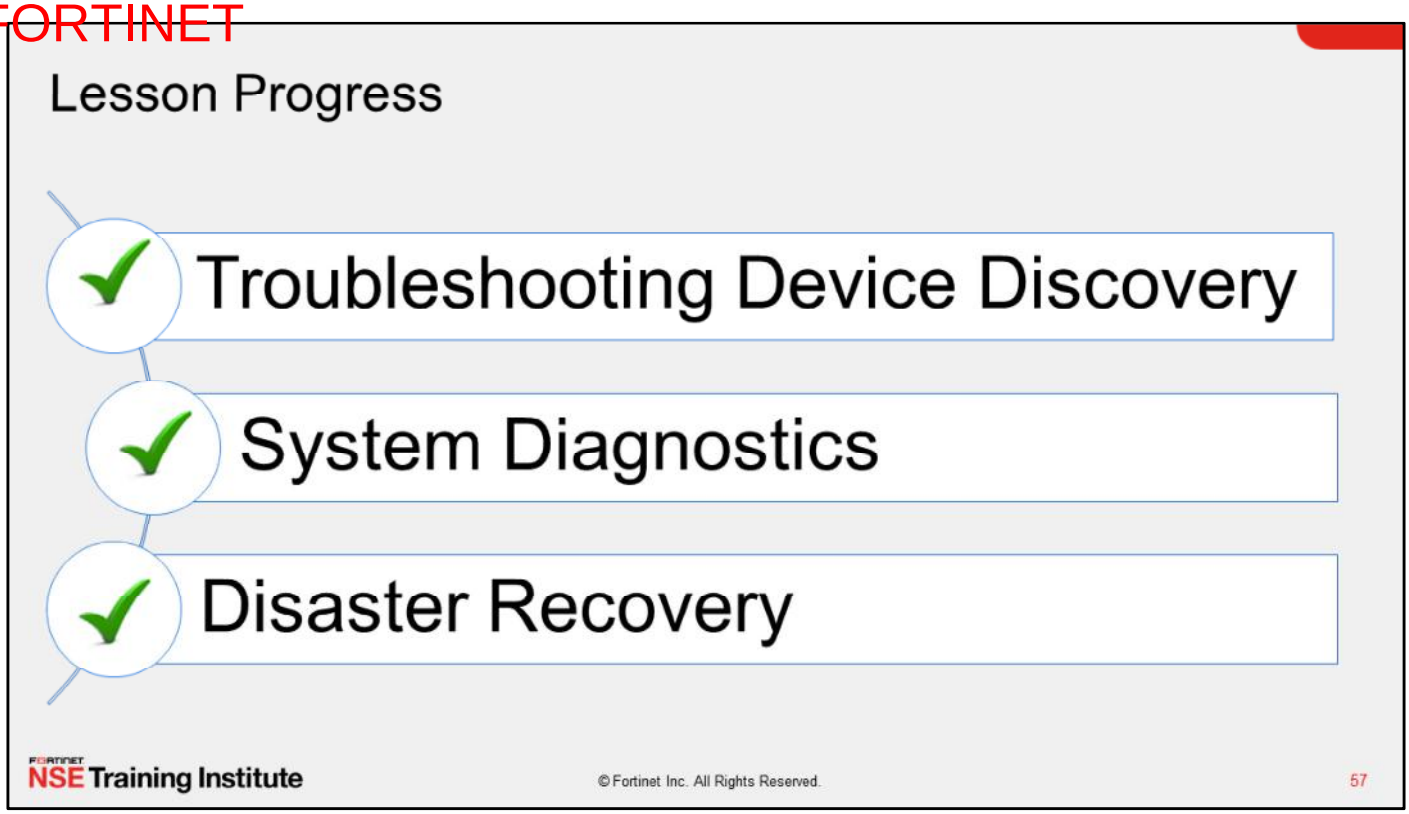
NSE Training Institute

© Fortinet Inc. All Rights Reserved.

56

Vouchers & Dumps are Available | WhatsApp +201224560923

DO NOT REPRINT
© FORTINET
Brave-dumps.com

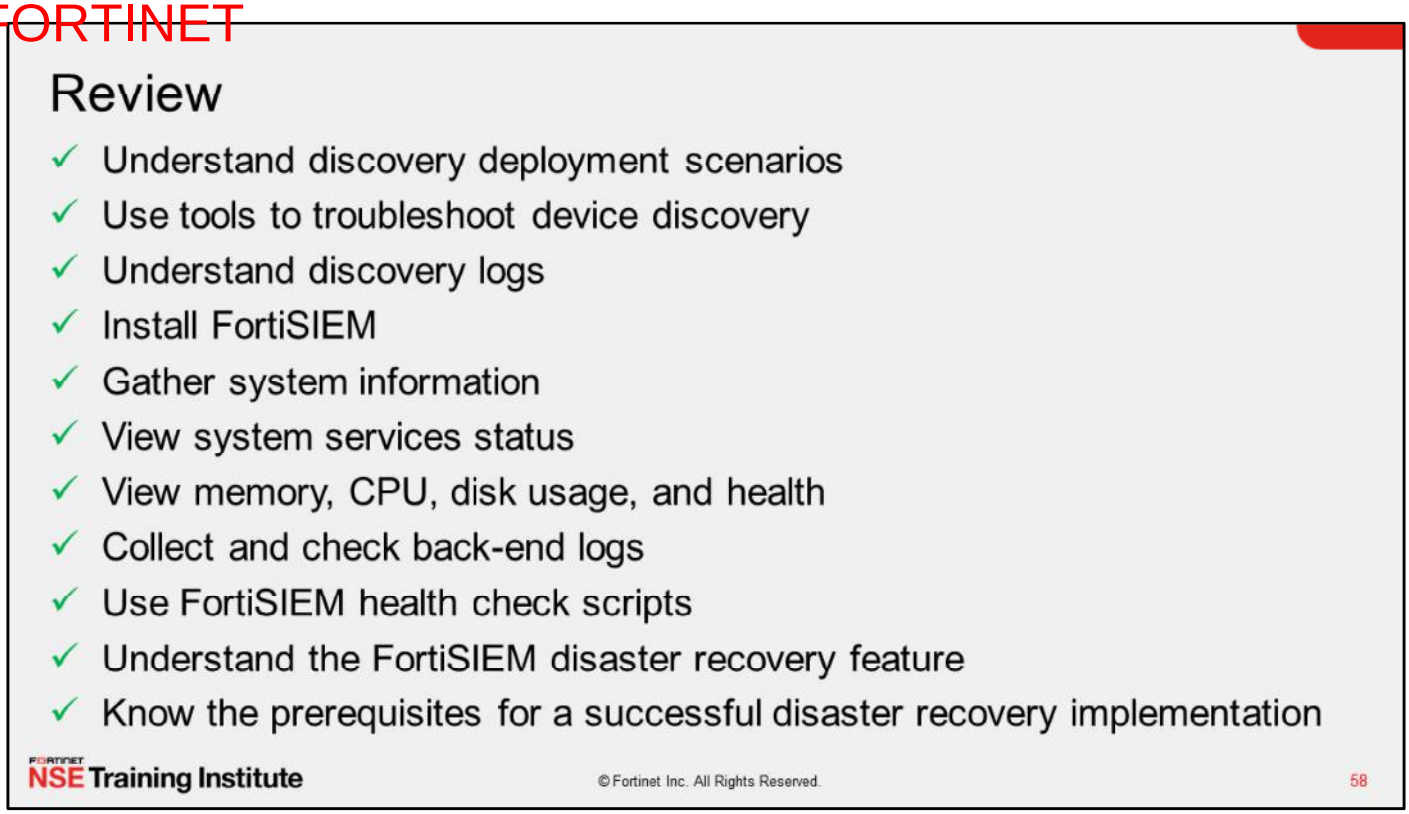


Congratulations! You have completed this lesson.

Now, you will review the objectives that you covered in this lesson.

Vouchers & Dumps are Available | WhatsApp +201224560923

DO NOT REPRINT
© FORTINET
Brave-dumps.com



This slide shows the objectives that you covered in this lesson.

By mastering the objectives you covered in this lesson, you will be able to troubleshoot device discovery, perform system diagnostics, and implement disaster recovery operation for FortiSIEM.

Vouchers & Dumps are Available | WhatsApp +201224560923

DO NOT REPRINT
© FORTINET
Brave-dumps.com



FORTINET

No part of this publication may be reproduced in any form or by any means or used to make any derivative such as translation, transformation, or adaptation without permission from Fortinet Inc., as stipulated by the United States Copyright Act of 1976.

Copyright© 2021 Fortinet, Inc. All rights reserved. Fortinet®, FortiGate®, FortiCare® and FortiGuard®, and certain other marks are registered trademarks of Fortinet, Inc., in the U.S. and other jurisdictions, and other Fortinet names herein may also be registered and/or common law trademarks of Fortinet. All other product or company names may be trademarks of their respective owners. Performance and other metrics contained herein were attained in internal lab tests under ideal conditions, and actual performance and other results may vary. Network variables, different network environments and other conditions may affect performance results. Nothing herein represents any binding commitment by Fortinet, and Fortinet disclaims all warranties, whether express or implied, except to the extent Fortinet enters a binding written contract, signed by Fortinet's General Counsel, with a purchaser that expressly warrants that the identified product will perform according to certain expressly-identified performance metrics and, in such event, only the specific performance metrics expressly identified in such binding written contract shall be binding on Fortinet. For absolute clarity, any such warranty will be limited to performance in the same ideal conditions as in Fortinet's internal lab tests. In no event does Fortinet make any commitment related to future deliverables, features, or development, and circumstances may change such that any forward-looking statements herein are not accurate. Fortinet disclaims in full any covenants, representations,and guarantees pursuant hereto, whether express or implied. Fortinet reserves the right to change, modify, transfer, or otherwise revise this publication without notice, and the most current version of the publication shall be applicable.

Vouchers & Dumps are Available | WhatsApp +201224560923