DO NOT REPRINT
© FORTINET
Braindumps.com

FortiEDR

Study Guide

for FortiEDR 5.0

Vouchers & Dumps are Available | WhatsApp

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

2/7/2022

Vouchers & Dumps are Available | WhatsApp +201224560923

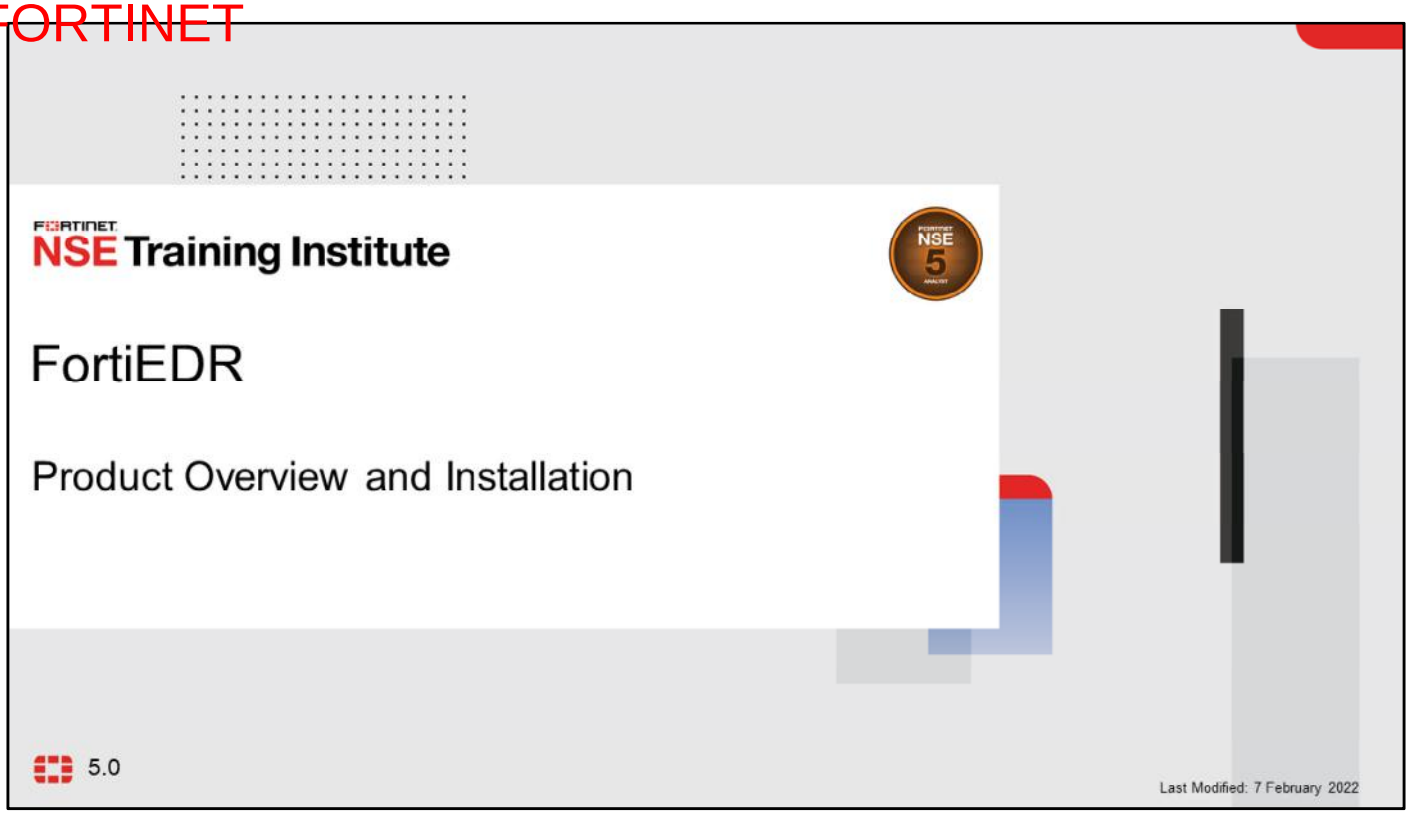
DO NOT REPRINT
© FORTINET
Brave-dumps.com

TABLE OF CONTENTS

01 Product Overview and Installation 4
02 Administration 28
03 Security Policies 69
04 Fortinet Cloud Service (FCS) and Playbooks 91
05 Communication Control 112
06 Events and Alerting 143
07 Threat Hunting and Forensics 171
08 Fortinet Security Fabric Integration and FortiXDR 199
09 RESTful API 223
10 Troubleshooting 240

Vouchers & Dumps are Available | WhatsApp +201224560923

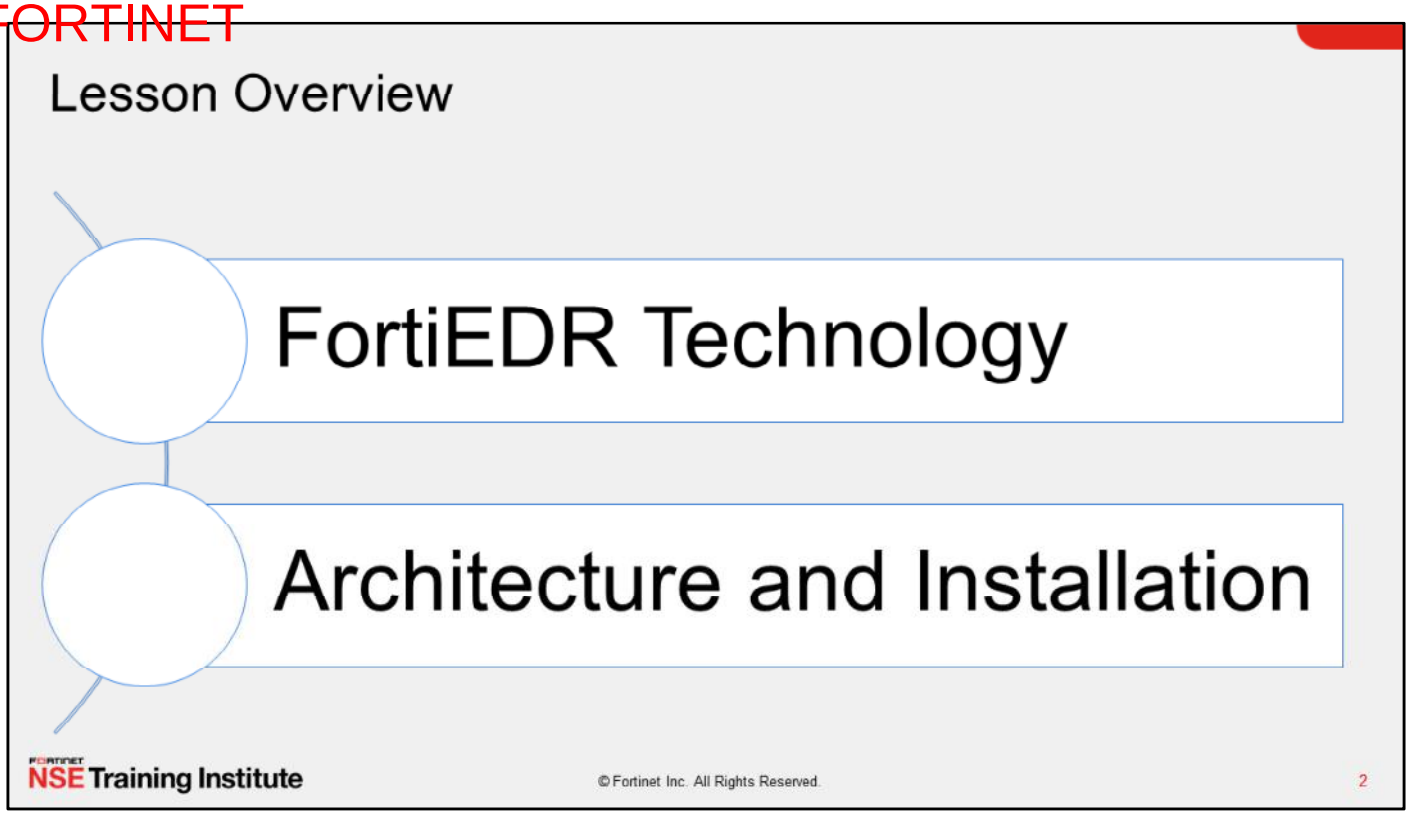
DO NOT REPRINT
© FORTINET
Brave-dumps.com



In this lesson, you will learn about what FortiEDR does and how it can be part of the Fortinet Endpoint solution.

Vouchers & Dumps are Available | WhatsApp +201224560923

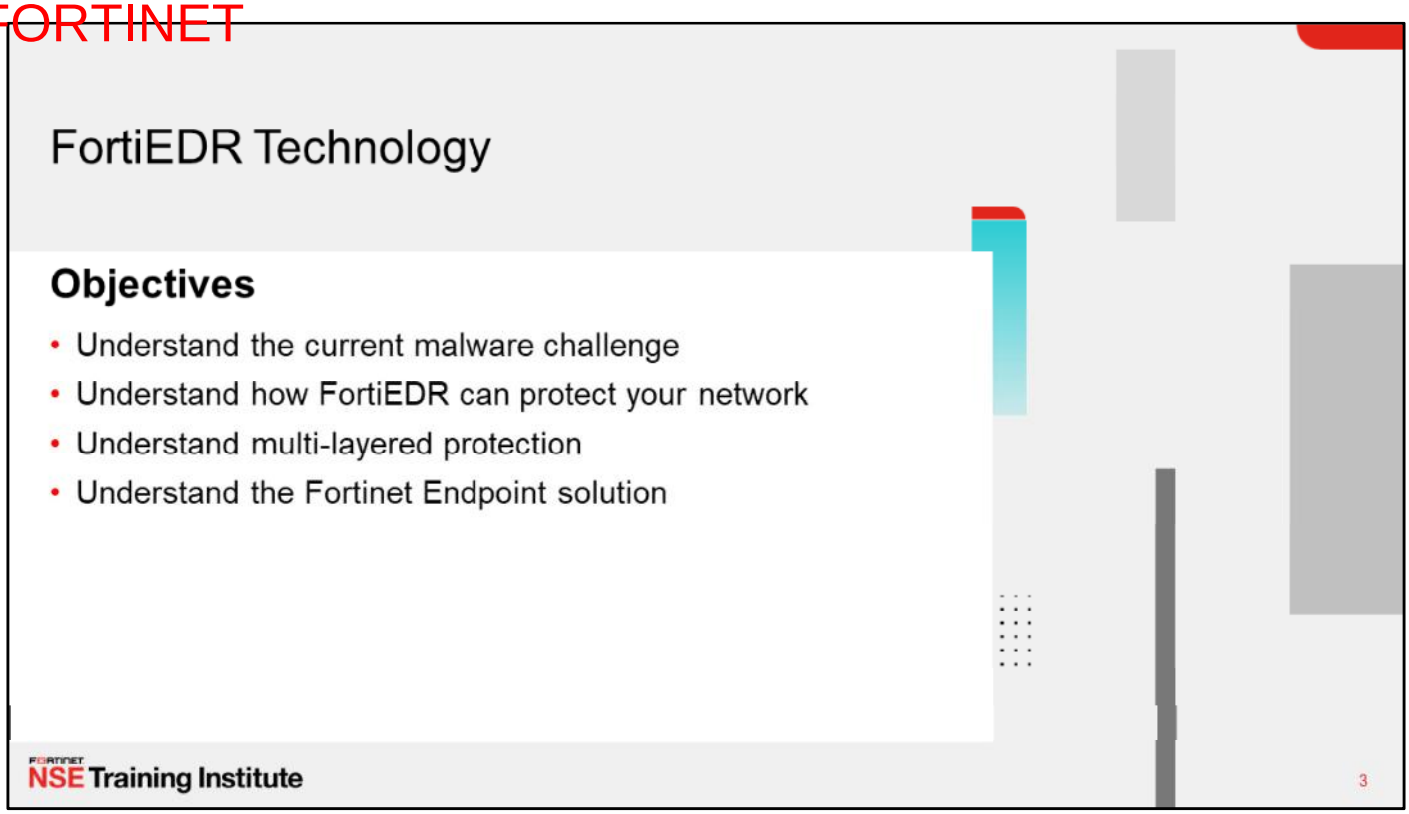
DO NOT REPRINT
© FORTINET
Brave-dumps.com



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 the current malware challenges, you will learn the importance of deploying FortiEDR and being part of the Fortinet Endpoint solution.

Vouchers & Dumps are Available | WhatsApp +201224560923

DO NOT REPRINT
© FORTINET
Brave-dumps.com

The Malware Challenge

- How do you stop an attack that hasn't been invented yet?
  - New types of malware in the last few years:
    - SpeakUp
    - PsMiner
    - BlackWater
    - GlitchPOS
    - Spectre/Meltdown
  - 350,000 new malicious and potentially unwanted programs registered by AV-TEST *every day*
  - Total of more than one billion known malware samples

NSE Training Institute

© Fortinet Inc. All Rights Reserved.

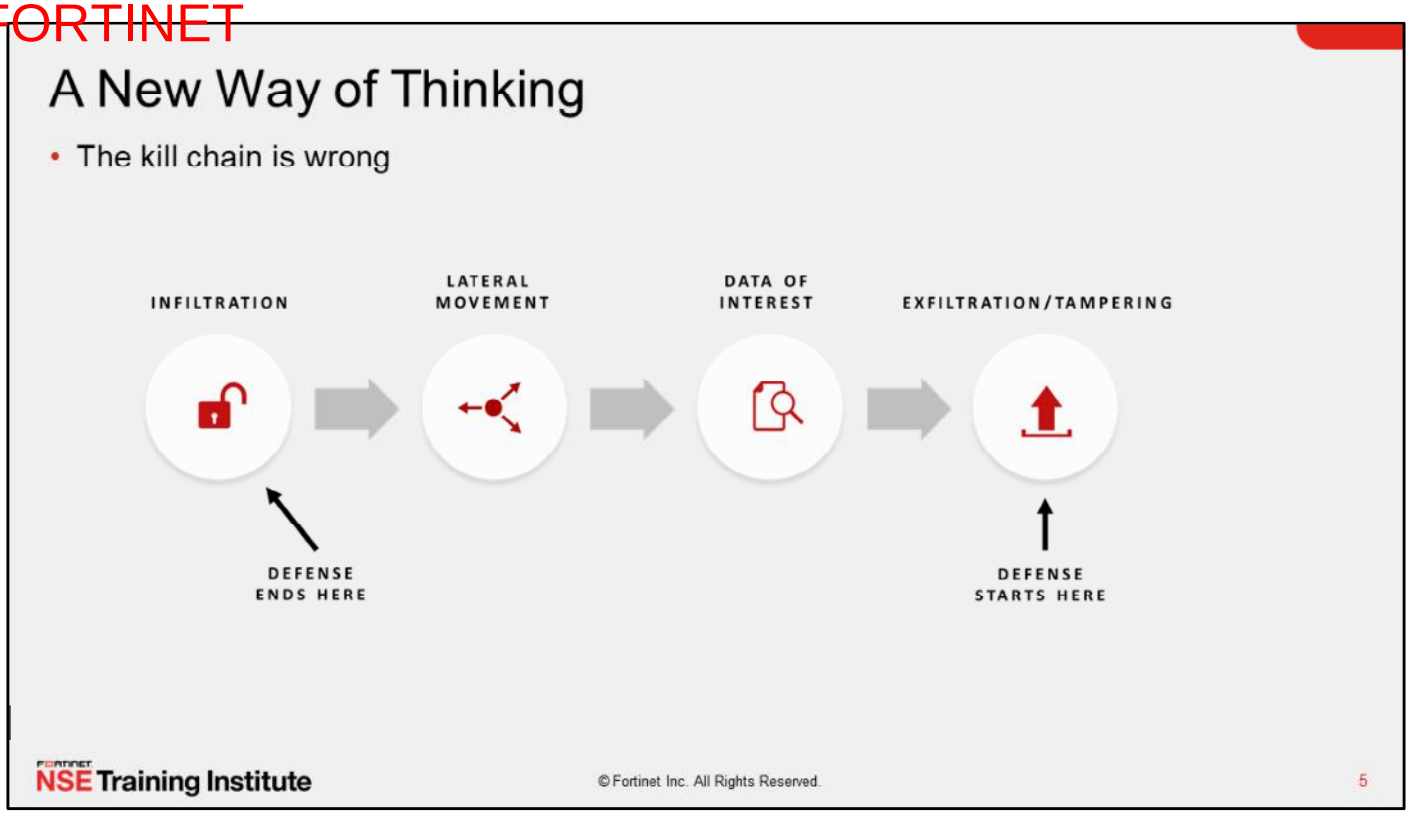
4

The malware landscape is constantly changing with new threat families appearing regularly. Existing threats are constantly evolving into new and harder-to-detect variations. AV-TEST registers about 350,000 new malicious and unwanted programs every day, totaling more than one billion samples.

How can security programs keep up and stop an attack that hasn't been invented yet?
FortiEDR answers the malware challenge.

Vouchers & Dumps are Available | WhatsApp +201224560923

DO NOT REPRINT
© FORTINET
Brave-dumps.com

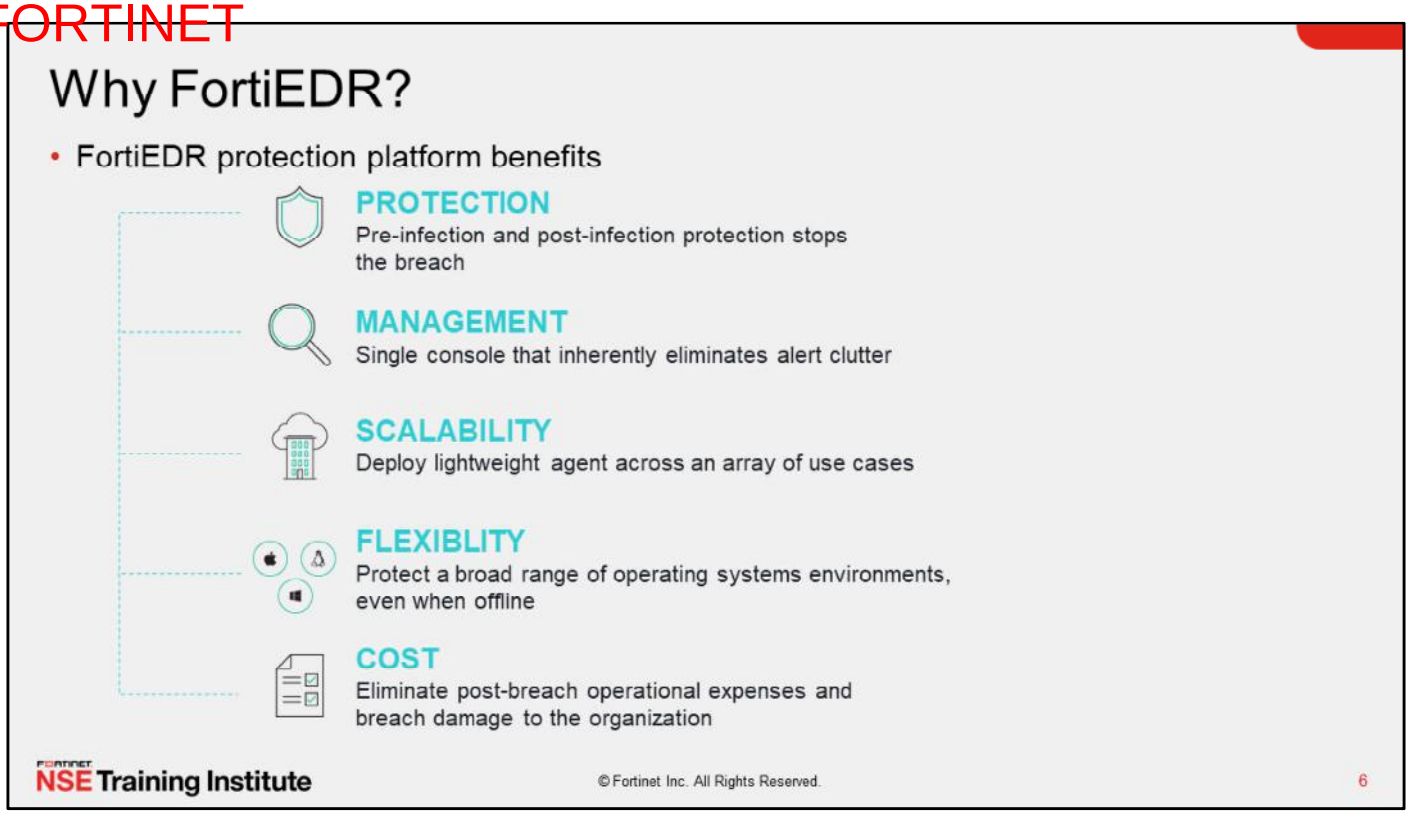


FortiEDR uses a different approach to detect malware than most security software. The FortiEDR approach focuses on the point of infiltration. It's a little bit like a bouncer at a club—they're trying to keep out anyone who might cause trouble. Once someone gets in though, they're not being watched as closely, so if they cause trouble—if they start a fight, for example—they're going to create some disruption before they get kicked out.

FortiEDR watches for malicious actions—attempts to steal or alter your data—then follows the chain from the point of the consequences back to the source of the initial process.

Vouchers & Dumps are Available | WhatsApp +201224560923

DO NOT REPRINT Brave-dumps.com
© FORTINET



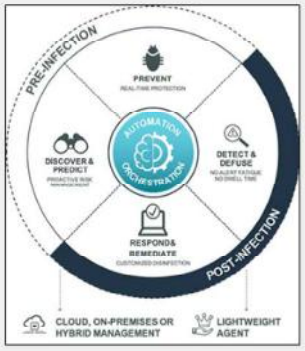
FortiEDR offers reliable protection with pre-infection and post-infection protection and can also stop even a highly sophisticated attack before it can inflict any harm. FortiEDR also offers centralized management, where an entire organization can be administered from a single console. FortiEDR is also highly scalable and flexible. FortiEDR agents are lightweight and can protect a broad range of operating systems deployed in small companies or large international corporations . Lastly, FortiEDR can save you money by eliminating both post-breach operational expenses and breach damage.

Vouchers & Dumps are Available | WhatsApp +201224560923

DO NOT REPRINT
© FORTINET
Brave-dumps.com

Multi-Layered Protection

- **Execution Prevention**
  - Machine learning, kernel-based next-generation antivirus
  - Feeds from a continuously updated cloud database
- **Data Exfiltration Prevention**
  - Discover and track applications and Internet of Things (IoT) devices
  - Common Vulnerabilities and Exposures (CVE) and application rating data enrichment
  - Risk-based proactive policies enable attack surface reduction
- **Ransomware Prevention**
  - Automated post-infection detection and blocking
  - Real-time automated prevention of ransomware encryption and data theft
  - OS-centric technology
  - Analysis of entire log history
  - Surgical containment
- **Threat Hunting**
  - Detecting, investigating, containing, and mitigating suspicious activities



NSE Training Institute

© Fortinet Inc. All Rights Reserved.

7

FortiEDR offers real-time next-generation antivirus (NGAV), which uses machine learning and a continuously-updated cloud database to detect known or simple threats and prevent them from executing.

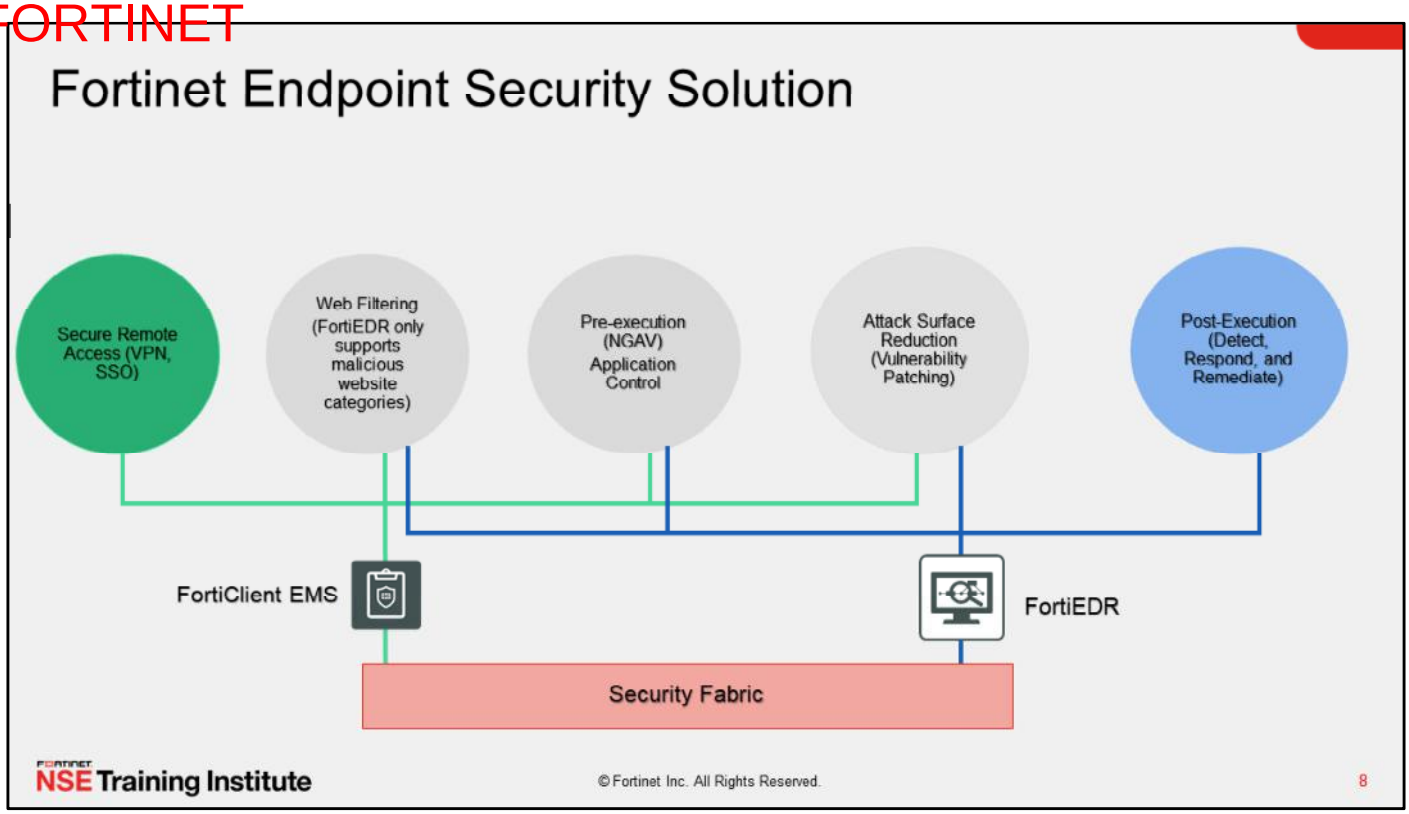
Next, FortiEDR offers real-time proactive risk mitigation. This gives you automated control over the non-malicious applications communicating over your network. FortiEDR will discover any application that establishes a connection and track its activity. FortiEDR offers reputation scoring and CVE data on each application version, allowing you to quickly identify whether an application that is not actively malicious might present a risk. You can use the reputation or CVE scores to proactively block any application version with known vulnerabilities or a poor reputation. That means, if a new vulnerability is detected in an old version of Google Chrome, for example, you can configure FortiEDR to block that version automatically, the moment the vulnerability is published, but still allow safer versions to access the internet. This reduces your attack surface.

If a sophisticated attack manages to get past FortiEDR NGAV, post-infection detection and blocking are activated. FortiEDR monitors the operating system at the kernel level. At every attempt to establish a connection, modify or encrypt data, FortiEDR evaluates the process and determines whether it is likely to be malicious. If there are indicators of malicious activity, the attempt is immediately blocked. FortiEDR also offers real-time orchestrated incident response. Every event is automatically classified based on how likely it is to be malicious. Based on that classification, you can configure a set of automated actions, including opening tickets, isolating the device, or remediating the threat.

Lastly, FortiEDR threat hunting feature uses a set of software tools for detecting, investigating, containing, and mitigating suspicious activities on endpoints. This data can be used to perform forensics on endpoints if needed.

Vouchers & Dumps are Available | WhatsApp +201224560923

DO NOT REPRINT
© FORTINET
Brave-dumps.com



Fortinet provides a complete endpoint security solution through the deployment of FortiClient EMS and FortiEDR. If FortiClient EMS is implemented, you can take advantage of the VPN, single sign-on and a more extensive web filtering feature, while the FortiEDR solution can prevent any post-execution suspicious activities. FortiEDR, just like FortiClient EMS, includes NGAV for pre-execution protection, vulnerability patching for attack surface reduction, application control to block any outdated or unwanted applications, and can be integrated into the Fortinet security fabric. You will learn more about the FortiEDR security fabric integration in a later lesson. Having these solutions implemented together can provide additional endpoint protection.

Vouchers & Dumps are Available | WhatsApp +201224560923

DO NOT REPRINT
© FORTINET
Brave-dumps.com

Knowledge Check

1. Which information is used by FortiEDR to determine if an application is at risk?
   - ✓ A. CVE data
   - B. Threat hunting data

2. Which feature in FortiEDR is used to reduce the attack surface?
   - A. NGAV
   - ✓ B. Vulnerability patching

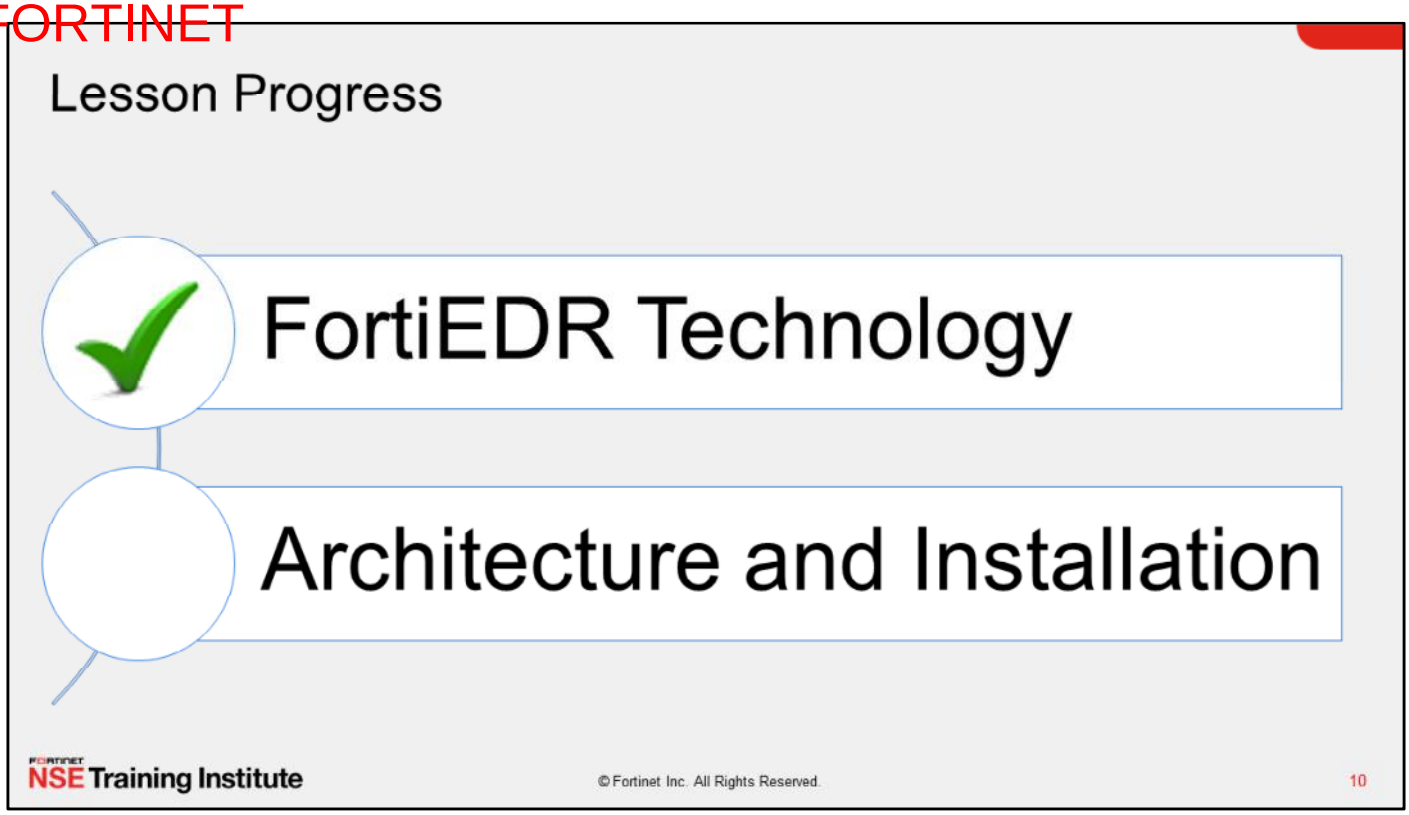
NSE Training Institute

© Fortinet Inc. All Rights Reserved.

9

Vouchers & Dumps are Available | WhatsApp +201224560923

DO NOT REPRINT
© FORTINET
Brave-dumps.com

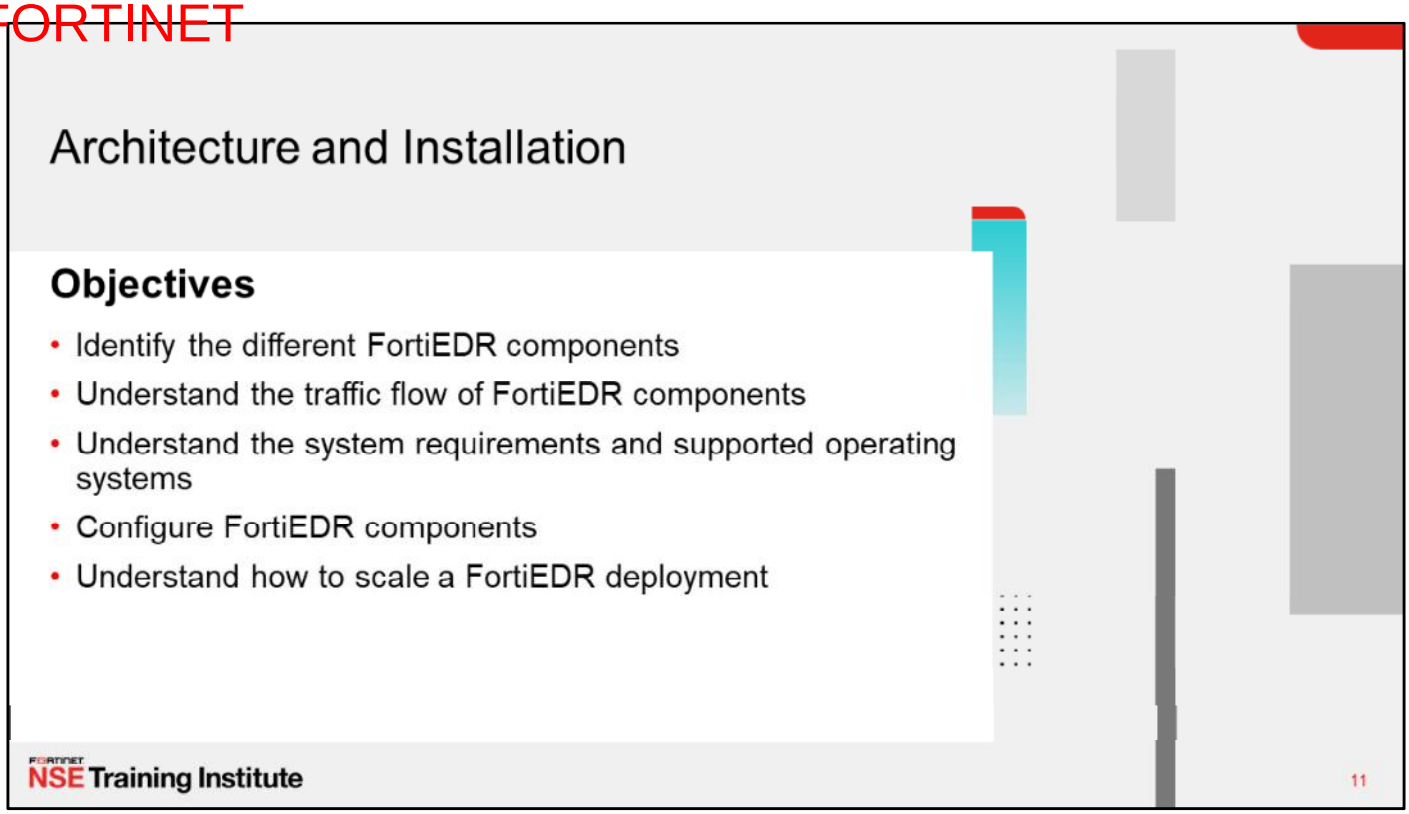


Good job! You now understand FortiEDR technology .

Now, you will learn about FortiEDR components and installation.

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 FortiEDR architecture, you will be able to identify the different components, understand the traffic flow, and configure options that will help you get FortiEDR up and running.

Vouchers & Dumps are Available | WhatsApp +201224560923

DO NOT REPRINT Brave-dumps.com
© FORTINET

FortiEDR Components

- **FortiEDR Collector**
  - Lean collector (agent) that resides deep inside the operating system on every communicating device in your enterprise, including desktops, laptops, and servers
- **FortiEDR Core**
  - The security policy enforcer and decision-maker
  - Detects and blocks suspicious connections
- **Threat Hunting Repository**
  - Find and delete known malware on any device within the system
  - Threat hunting license required
- **FortiEDR Aggregator**
  - Provides processing and load handling services for the Central Manager
  - Usually runs on the same system as the FortiEDR Central Manager in smaller installations
  - Large deployments may require multiple aggregators on separate servers
- **FortiEDR Central Manager**
  - Software-only central web user interface and back-end server for viewing and analyzing events and configuring the system
- **FortiEDR Cloud Services (FCS)**
  - Cloud based, software-only service that verifies classification of security events with high accuracy and acts accordingly
  - Responsible for managing all investigation actions

NSE Training Institute © Fortinet Inc. All Rights Reserved. 12

Start by identifying the major components that make up a FortiEDR installation.

The first component is the FortiEDR collector—the lean collector, or agent, that sits deep inside the operating system, down at the kernel level, and sees everything that happens on the device. It is installed on all the systems in your enterprise.

The core is the security policy enforcer and decision maker. It determines whether a connection establishment or write-to-disk operation is legitimate or should be blocked. The core may run on-premises, in the cloud, or a combination of both. If the collector is offline, it uses built-in policies at the collector level, to operate in autonomous mode. That means if the collector can't connect to the core, the device is still protected at the collector level.

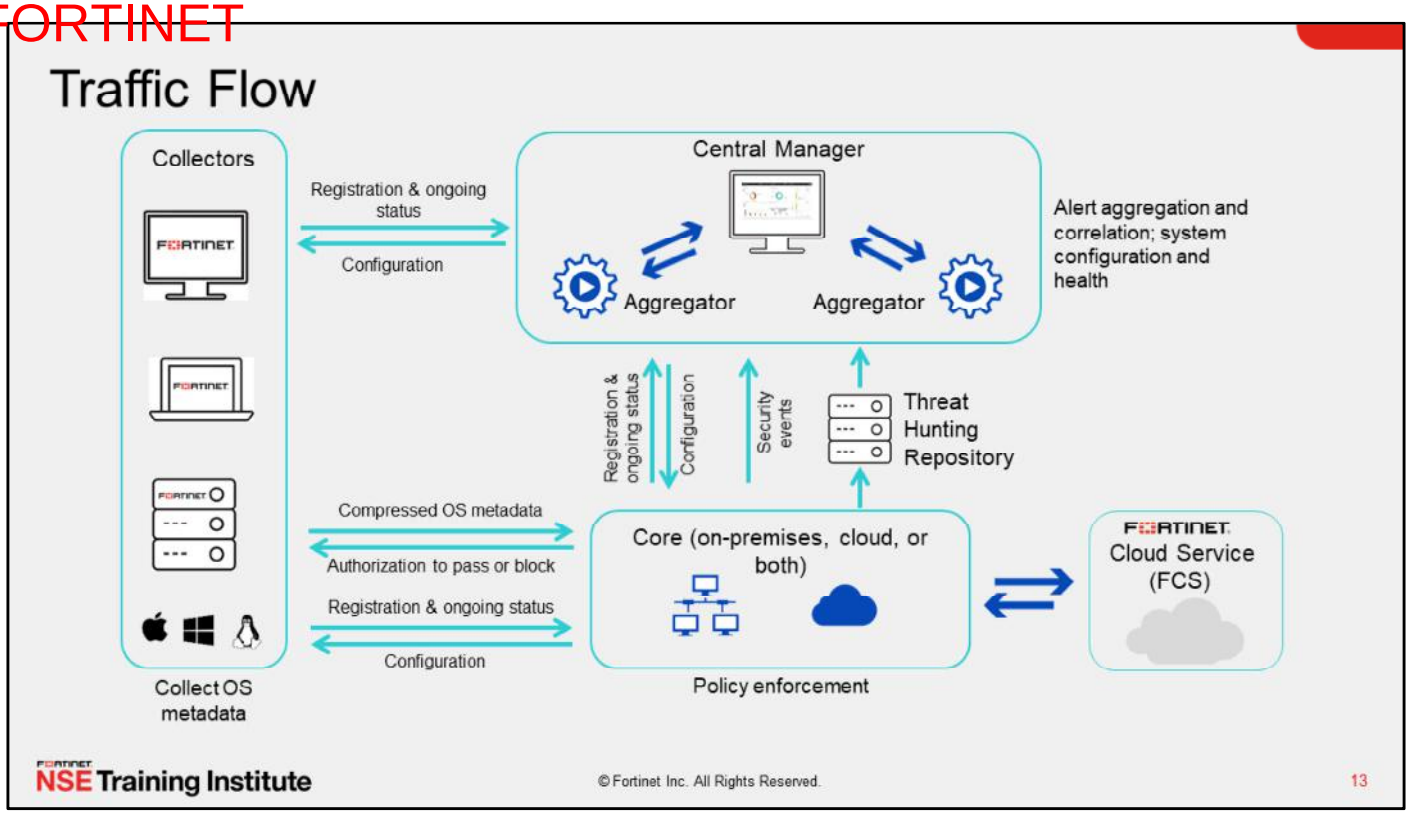
The FortiEDR aggregator provides processing and load handling services for the central manager. The FortiEDR central manager is the user interface and the back-end server for reviewing and analyzing events and configuring the system. In smaller deployments, these two components are usually installed on the same server. Larger deployments will require separate servers, and very large deployments may require multiple aggregators.

The threat hunting repository is an optional feature requiring a threat hunting license. It allows administrators to find and delete malware from any system within the enterprise.

FCS is a cloud based, software-only service that verifies classification of security events with high accuracy and acts accordingly based on these classifications. You will learn more about FCS in this course.

Vouchers & Dumps are Available | WhatsApp +201224560923

DO NOT REPRINT
© FORTINET
Brave-dumps.com



Now you'll learn how FortiEDR components communicate, starting with the FortiEDR collector. The first thing it does after it's installed is connect to the aggregator, which sends back a license and a configuration file. In that configuration file is a list of cores that the collector is allowed to talk to. There can be up to 11 cores communicating with one aggregator. The collector then checks the connection time to each core and chooses to use the fastest one.

The core handles policy enforcement. If there is a risky type of event, the collector sends compressed operating system metadata to the core for evaluation. The core sends back a go or no-go on the event based on existing policies. It then sends the alert data and the policy action to the aggregator, which passes it to the central manager. The central manager displays this data in the GUI. The core also sends alert data to FortiEDR Cloud Service (FCS), which conducts a deeper analysis of events. Lastly, the core sends information about executables detected on each collector to the threat hunting repository. It communicates to the central manager, where you can search for executables on the GUI.

Vouchers & Dumps are Available | WhatsApp +201224560923

DO NOT REPRINT
© FORTINET
Brave-dumps.com

Network Communication Requirements

Component	Destination	TCP/IP Port	Purpose
Collector	Aggregator	8081	Registration and status
Collector	Core	555	Compressed OS metadata
Core	Aggregator	8081	Registration status and events
Core	Threat hunting repository	443	Threat hunting capabilities
Core	FortiEDR Reputation Service: reputation.ensilo.com:443	443	Check reputation of applications
Aggregator	Manager	443	Events, configuration
Admin PC	Manager	443	GUI access
Manager	Syslog	6514	TCP and SSL recommended
Manager	SMTP Server	587	TLS protection recommended
Manager	Threat hunting repository	443	Hash and file queries
Manager	FortiEDR Cloud Service (FCS): cldsrv.ensilo.com:443 rbq.cldsrv.ensilo.com:443	443	Data sent to FCS

NSE Training Institute

© Fortinet Inc. All Rights Reserved.

14

This slide shows a chart of the full network communication requirements. Communication from the collector to the aggregator is done on a non-standard port—port 8081—and communication from the collectors to the core is done on port 555. Those ports are configurable—they can be changed, but most customers leave them unchanged. Communication from the core to the aggregator uses port 8081, and the core to the threat hunting repository uses port 443. The same ports are used for communication from the core to reputation services.

Vouchers & Dumps are Available | WhatsApp +201224560923

DO NOT REPRINT
© FORTINET
Brave-dumps.com

System Requirements

Component	Memory	Disk Space	Processor
Collector	60 MB	20 MB	Intel or AMD x86 (32-bit and 64-bit)
Core	8 GB	80GB	• Intel or AMD x86 64-bit • 2 CPUs to service 5k collectors
Aggregator	16 GB	80GB	• Intel or AMD x86 64-bit • Minimum 2 CPUs
Central Manager	16 GB	150 GB	• Intel or AMD x86 64-bit • Minimum 2 CPUs
Threat Hunting Repository	24 GB to service 4k collectors and store one month data	1.5 TB to service 4k collectors and store one month data	16 CPUs

NSE Training Institute

© Fortinet Inc. All Rights Reserved.

15

The collector requires an Intel or AMD x86 hypervisor-compatible processor: either 32-bit or 64-bit. The space requirements for the collector are minimal—you need 60 MB of RAM and 20 MB of disk space.

The core, aggregator, and central manager may be installed on a dedicated workstation or server, or on a virtual machine. You can install the aggregator and central manager together on one machine, or for larger deployments, you can install them separately. For disk space and memory, the core requires at least 8 GB of RAM and at least 80 GB of disk space. The aggregator and central manager require 16 GB of RAM. You will need at least 80 GB of disk space for the aggregator, 150 GB for the central manager. The threat hunting repository requires a minimum of 24 GB of RAM, and 1.5 TB of disk space to service 4000 collectors and retain one month of data. Each additional 2000 collectors would require 1.1 TB of disk space, 6 GB of RAM, and 6 CPUs.

All server components require Intel or AMD x86 64-bit hypervisor-compatible processors. You'll need to assign a static IP address or domain name to the core, aggregator, and central manager, and network connectivity is required between all system components.

Vouchers & Dumps are Available | WhatsApp +201224560923

DO NOT REPRINT Brave-dumps.com
© FORTINET

Supported Operating Systems

FortiEDR Collector

- **Windows**
  - Windows XP SP2/SP3, 7 SP1, 8, 8.1, 10, and 11
  - Windows Server 2003 SP2, R2 SP2, 2008 SP2, 2008 R2 SP1, 2012, 2012 R2, 2016, 2019, and 2022
- **MacOS**
  - El Capitan (10.11), Sierra (10.12), High Sierra (10.13), Mojave (10.14), Catalina (10.15), Big Sur (11) and Monterey (12)
- **Linux**
  - RedHat Enterprise Linux and CentOS 6.8+, 7.2+ and 8+, Ubuntu LTS 16.04.5+, 18.04 and 20.04 server, 64-bit only and Oracle Linux 8.2+
- **VDI Environments**
  - VMware Horizons 6 and 7 and Citrix XenDesktop 7

FortiEDR Core, Aggregator, Central Manager

- ISO format including a CentOS 7 image

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

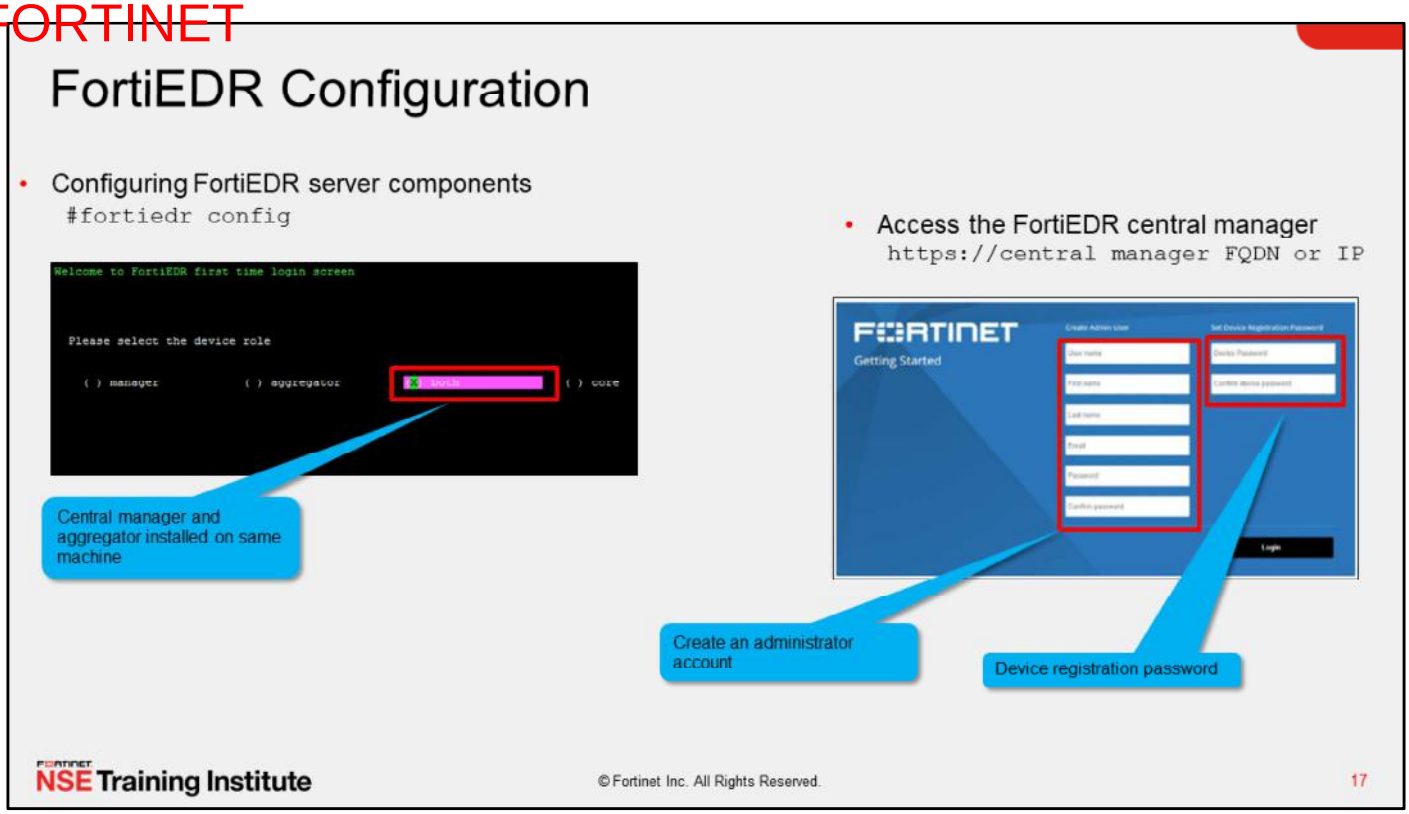
The collector lives at the kernel level inside the operating system. While a new operating systems bring a lot of changes over time, not a lot changes occur at the kernel level. So, FortiEDR supports versions from Windows XP, service pack 2, and up to Windows 11. On the server side, FortiEDR supports Windows Server 2003, release 2, service pack 2, and up to Windows Server 2022.

For a Mac operating system, FortiEDR supports El Capitan through Monterey. For Linux, FortiEDR supports Red Hat Enterprise Linux and its freeware version, CentOS version 6.8 through 6.10, and 7.2 through 7.7, and 8, all in 64-bit. FortiEDR supports Ubuntu LTS version 16.04.6, 18.04.1, 18.04.2, 20.04 server in 64-bit. Support for Oracle Linux 8.2 has also been added. For VMware, FortiEDR supports Horizon 6 and 7 and Citrix XenDesktop 7.

Note that the list of supported operating systems is dynamic. For the latest list, consult the latest version of the *FortiEDR Installation and Administration Guide*, or contact Fortinet support.

Vouchers & Dumps are Available | WhatsApp +201224560923

DO NOT REPRINT Brave-dumps.com
© FORTINET



FortiEDR central manager and aggregator can be installed using the same ISO file. After you install the ISO, log in with the default root account and enter `fortiedr config` to select the role that needs to be installed. If you are going to install central manager and aggregator on the same machine, select **both** as the role. After you complete the configuration, enter `fortiedr status` to verify that the required services are running. Central manager is the only system component with a GUI. You can access the central manager GUI using the URL format as shown on this slide. When you access the central manager GUI for the first time, you are required to create an administrator account and a device registration password. The device registration password is used to restrict the installation and uninstallation of aggregators, cores, and collectors.

FortiEDR core configuration is similar to the central manager and aggregator. The core needs to have connectivity to the local area network (LAN) in order to communicate with the collector. The core also needs to have connectivity to the aggregator and the FortiEDR reputation server.

Threat hunting repository consists of two installation files. Firstly, install the provided Kubernetes operating system and then install the FortiEDR repository software on it.

For more information on the installation, consult the latest version of the *FortiEDR Installation and Administration Guide.*

Vouchers & Dumps are Available | WhatsApp +201224560923

DO NOT REPRINT Brave-dumps.com
© FORTINET

Installing the Collector

- Information required
  - IP address of aggregator
  - Registration password: a secret password common to all FortiEDR collectors in a network or organization
- Windows
  - MSI installer
  - Create a silent installer pre-scripted with registration password, aggregator IP address, and optionally an organization (multi-tenancy only) and collector group assignment
  - Distribute through GPO or SCCM
- Mac
  - DMG installer
  - May be distributed with a JSON file configured with the desired settings
- Linux
  - Red Hat Enterprise and CentOS: RPM installer
  - Ubuntu: DEB installer
  - Run `fortiedrconfig.sh` to configure

Windows command line install

```
msiexec /i FortiEDRcollectorInstaller64.msi /qn AGG=10.0.0.1:8081
PWD=1234
```

CentOS command line install

```
sudo yum install FortiEDRcollectorInstaller_CentOS-
4.x.x.x86_64.rpm
sudo
/opt/FortiEDRcollector/scripts/fortiedrconfig.sh
```

Ubuntu command line install

```
sudo apt-get install
FortiEDRcollectorInstaller_Ubuntu-4.x.x.deb
sudo
/opt/FortiEDRcollector/scripts/fortiedrconfig.sh
```

NSE Training Institute © Fortinet Inc. All Rights Reserved. 18

The collector is very simple to install. The only information you need is the aggregator IP address and the registration password. The registration password is set during initial management server configuration and prevents unauthorized users from using your licenses.

On Windows, you can install the collector with an MSI file. You can create a self-installer that is preconfigured with the aggregator IP address, registration password, organization name for multi-tenancy environments, and collector group, if needed. Fortinet provides a custom installer generator to create your preconfigured file. In version 4.1 and later, you can also request a custom installer on the **ADMINISTRATION** tab of the management console.

You can deliver the collector the same way you would deliver any other MSI for installation, through a GPO object or Windows system center configuration Manager. An example command line installation script is shown on this slide. You can find detailed instructions in the *Installation and Administration* guide.

Installation on a Mac is done using a DMG file—just run the PKG file enclosed and proceed through the GUI. You can also create a silent installer for Macs using a JSON file configured with the registration password, aggregator IP, and any other desired settings. You can find detailed instructions in the *Installation and Administration* guide.

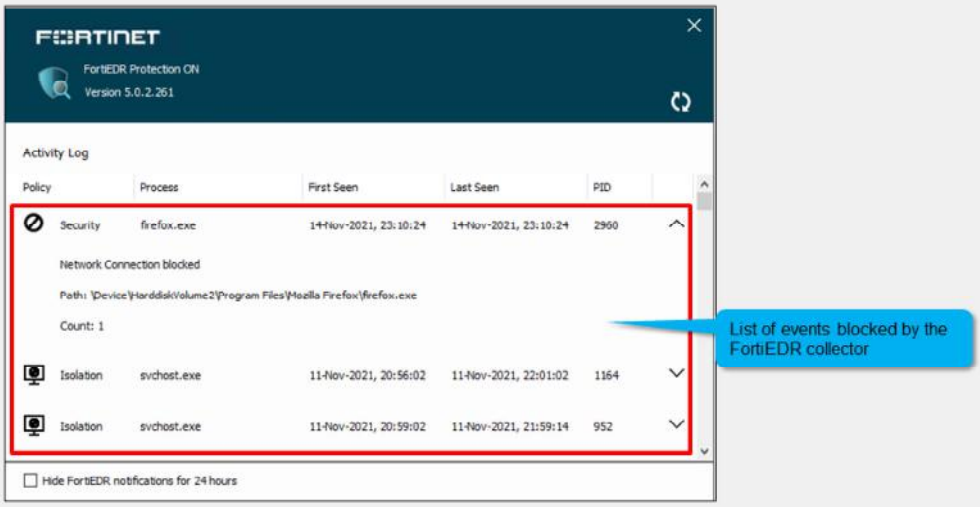
You can also install the collector on Linux machines. For Red Hat Enterprise and its freeware version, CentOS, you can use the provided RPM installer with the correct Linux distribution in the filename. This slide shows an example installation script for CentOS. After the installation is complete, run `fortiedrconfig.sh` to configure the aggregator IP, registration password, and any other information desired. For Ubuntu, use the DEB installer. This slide shows a sample script. Again, you'll need to configure the collector after installation by running `fortiedrconfig.sh`.

If you need help with installation, contact the Professional Services team at Fortinet.

Vouchers & Dumps are Available | WhatsApp +201224560923

DO NOT REPRINT
© FORTINET
Brave-dumps.com

Enhanced End-User Notification



NSE Training Institute

© Fortinet Inc. All Rights Reserved.

19

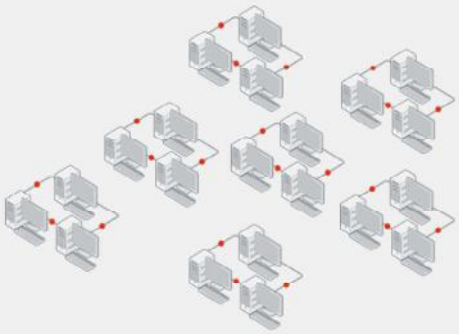
Starting with collector version 5, there is a user tray notification that provides an activity log of recent events and the collector version.

Vouchers & Dumps are Available | WhatsApp +201224560923

DO NOT REPRINT
© FORTINET
Brave-dumps.com

Scaling

- Collectors connect to the closest available core
  - Closest is based on time to travel to core
  - Collectors connect to one core at a time
  - Up to 11 cores may be configured per aggregator
- Aggregator location
  - For small installations, the aggregator and management server may be hosted on a single machine
  - If you have more than 5,000 collectors, the aggregator should be moved to a separate machine
  - Each aggregator can hold up to 10,000 collectors
- Central management server capacity
  - Each central manager can support up to 100,000 collectors



NSE Training Institute

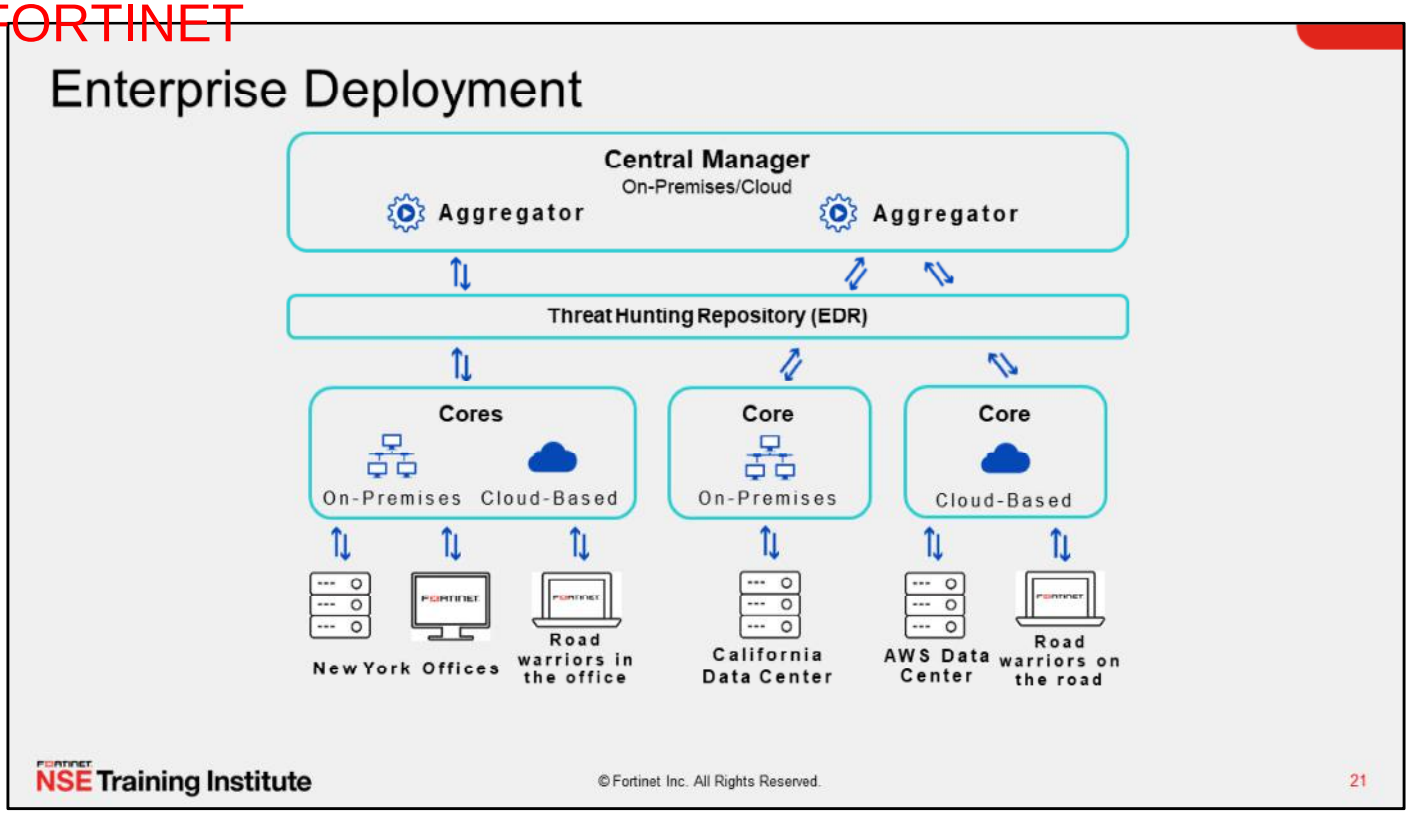
© Fortinet Inc. All Rights Reserved.

20

Collectors always connect to the closest available core. Determining the closest is based on the time to travel to the core. Collectors connect to one core at a time, but they can switch over very quickly to the next core. Up to 11 cores can be configured per aggregator. The aggregator is typically located on the same server as the management console, but in excess of about 5,000 machines, the aggregator should be moved to a separate machine. Up to 10,000 collectors can be configured per aggregator. Each central management server can support up to 100,000 collectors. These scaling numbers are constantly improving. Make sure to check with Fortinet or your service provider before engaging in a large scale deployment.

Vouchers & Dumps are Available | WhatsApp +201224560923

DO NOT REPRINT Brave-dumps.com
© FORTINET



In an enterprise deployment, the vast majority of our customers use a cloud-based central manager and cores, and some supplement that with a local core. This slide shows an example that explains why this model works well. This organization has on-site cores to support its servers, and a cloud-based core to support the cloud data center. But how does this work with employees? When workers are in the office, they can communicate with the on-premises core, so their compressed metadata doesn't need to go out over the network. But workers aren't always in the office. When they're working at home or on the road, they're covered by the cloud-based core. So. no matter where you are, you can connect to a core.

Vouchers & Dumps are Available | WhatsApp +201224560923

DO NOT REPRINT
© FORTINET
Brave-dumps.com

Knowledge Check

1. Which FortiEDR component is used for viewing and analyzing events?
   - ✓ A. Central manager
   - B. Aggregator

2. What is the purpose of the registration password?
   - A. To restrict access to the management console
   - ✓ B. To restrict collector installation and uninstallation

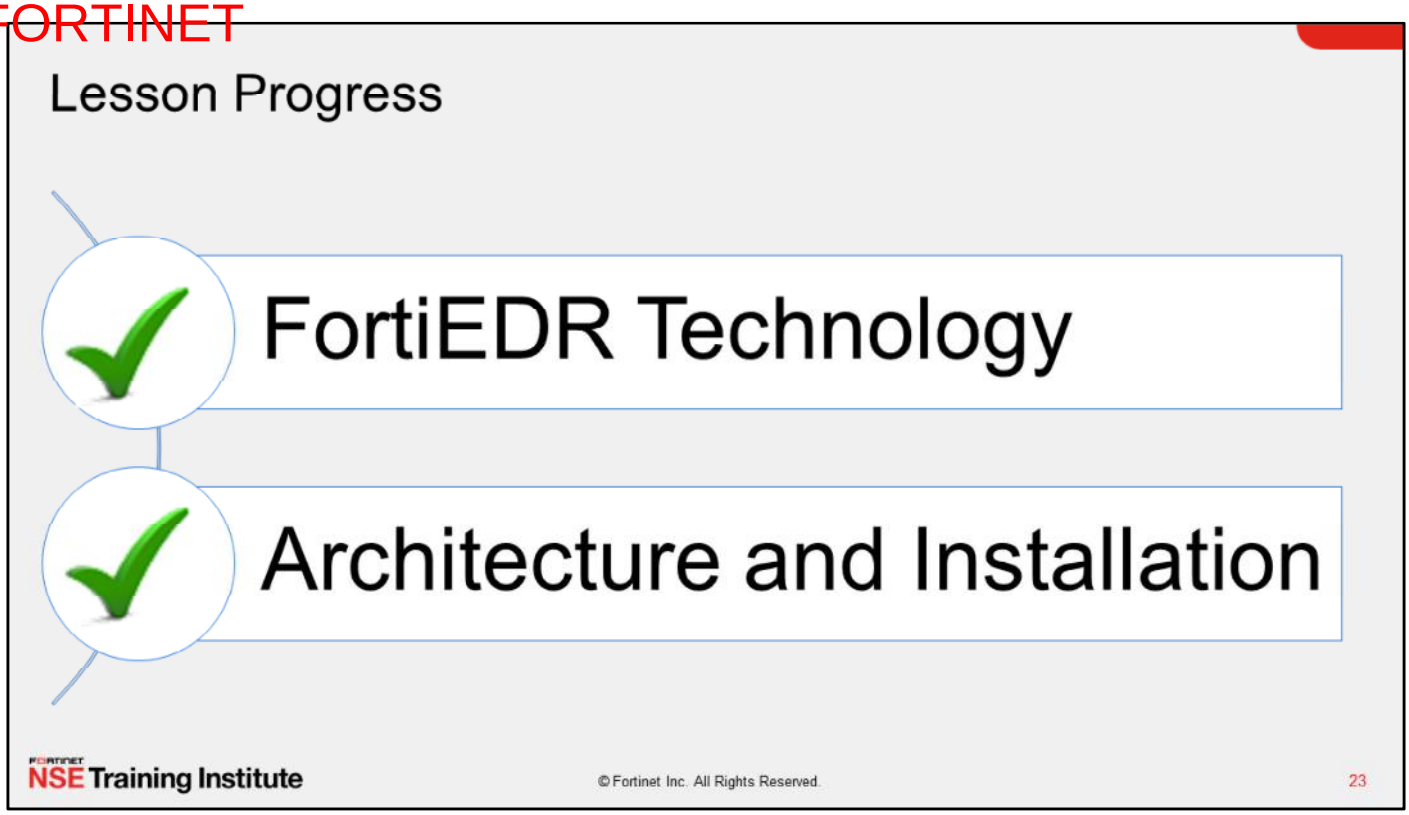
NSE Training Institute

© Fortinet Inc. All Rights Reserved.

22

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

Review

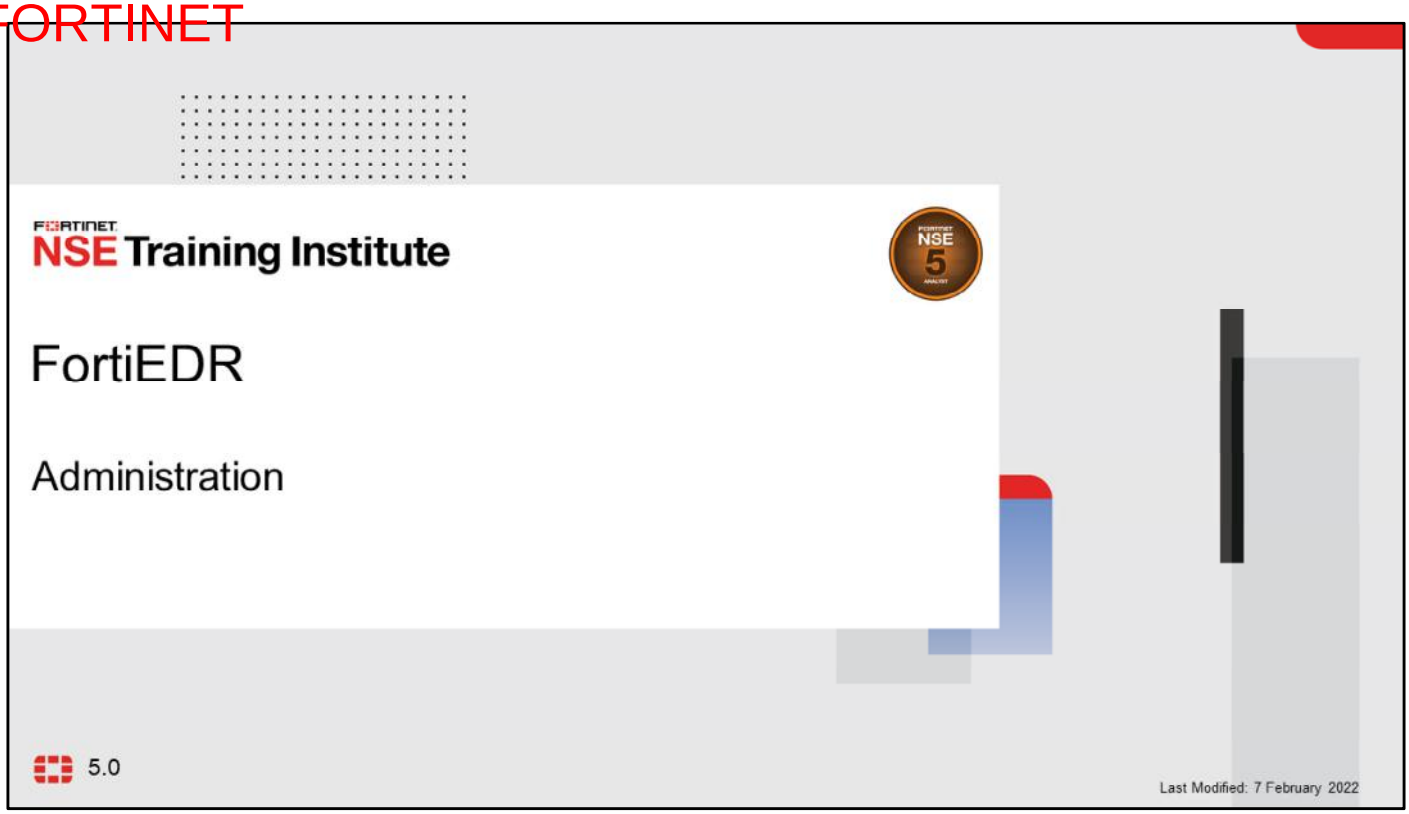
- ✓ Understand the current malware challenge
- ✓ Understand how FortiEDR can protect your network
- ✓ Understand multi-layered protection
- ✓ Understand the Fortinet Endpoint solution
- ✓ Identify the different FortiEDR components
- ✓ Understand the traffic flow of FortiEDR components
- ✓ Understand the system requirements and supported operating systems
- ✓ Configure FortiEDR components
- ✓ Understand how to scale a FortiEDR deployment

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

By mastering the objectives covered in this lesson, you learned what FortiEDR offers, and how to identify and configure the different FortiEDR components.

Vouchers & Dumps are Available | WhatsApp +201224560923

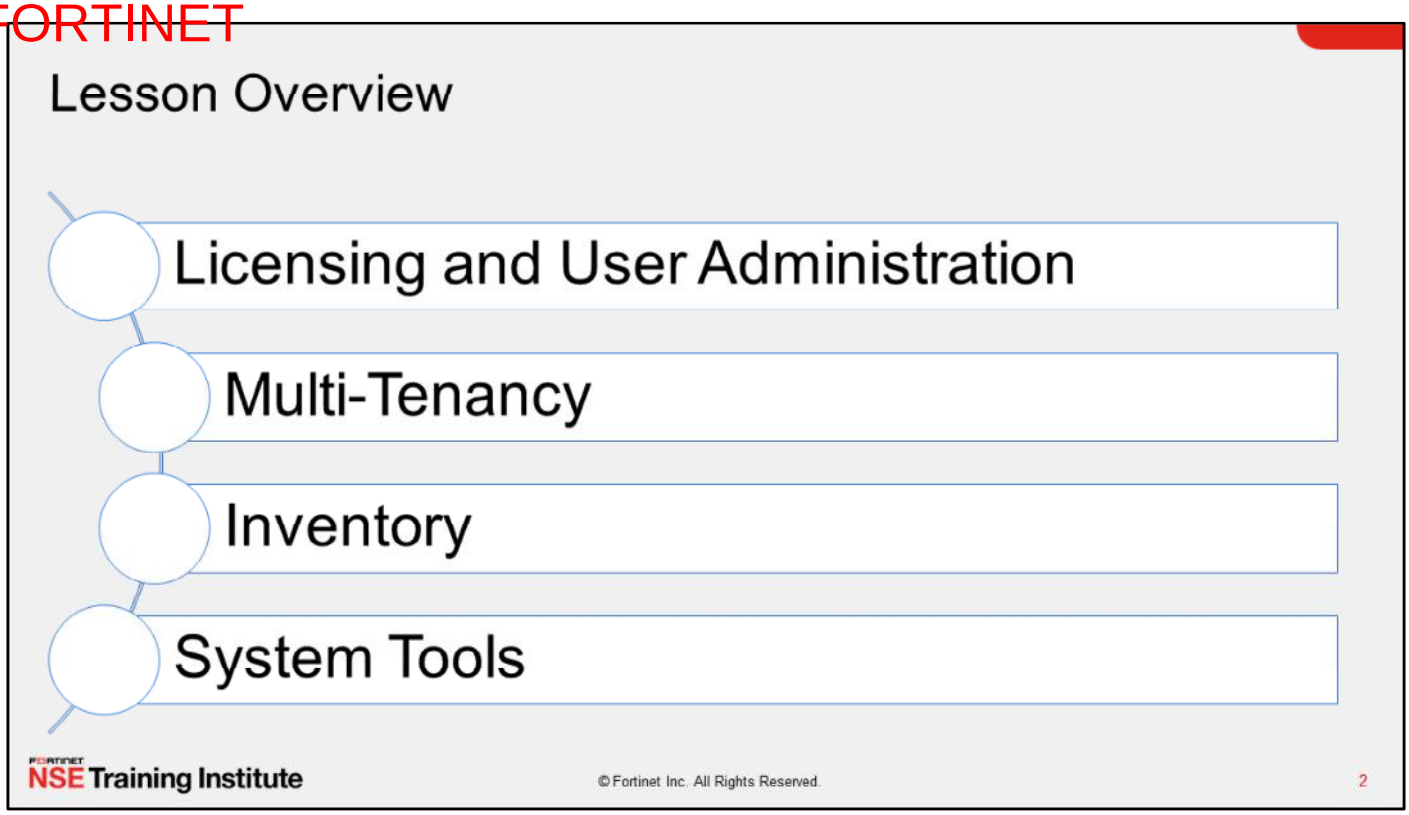
DO NOT REPRINT
© FORTINET
Brave-dumps.com



In this lesson, you will learn how to administer a FortiEDR deployment.

Vouchers & Dumps are Available | WhatsApp +201224560923

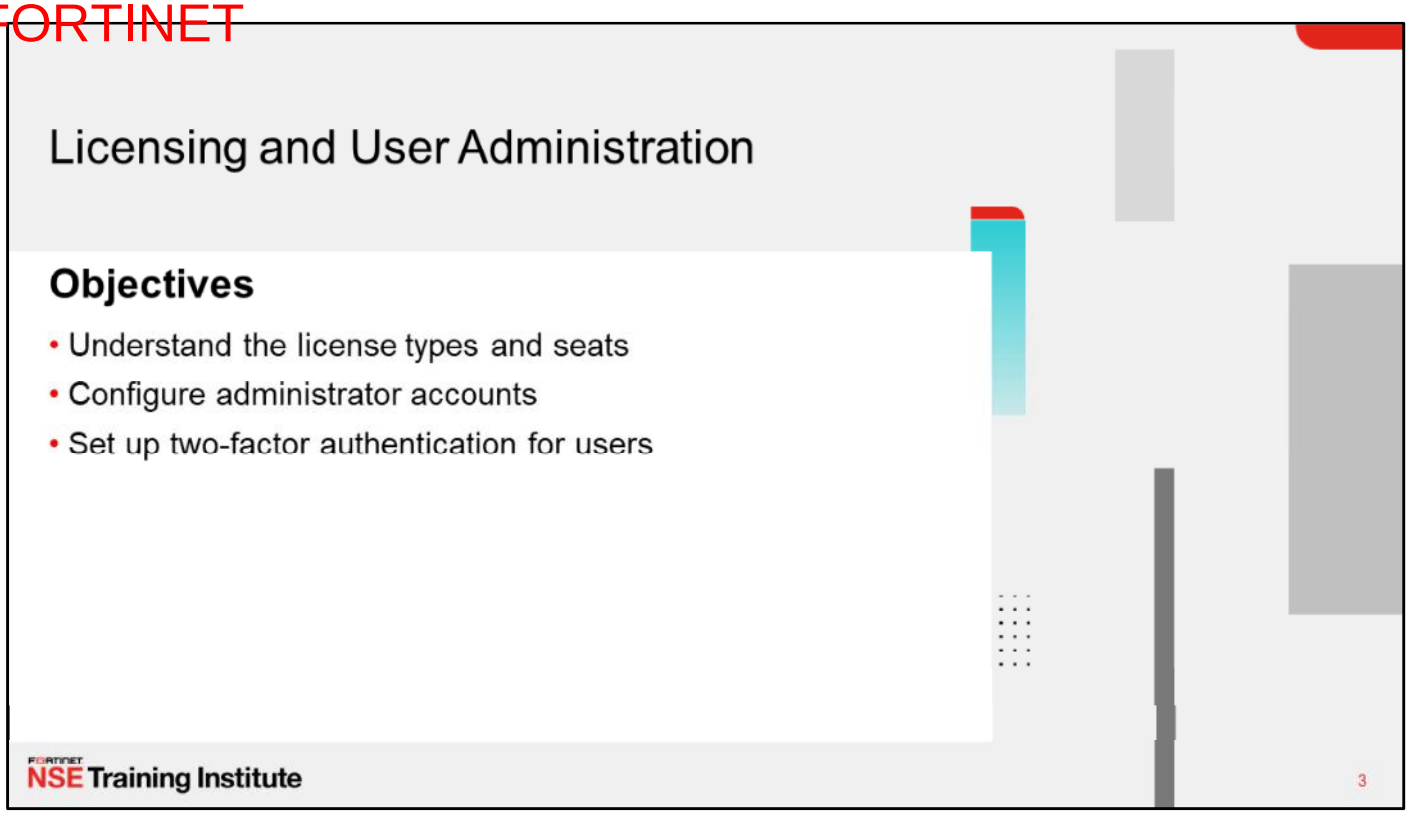
DO NOT REPRINT Brave-dumps.com
© FORTINET



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

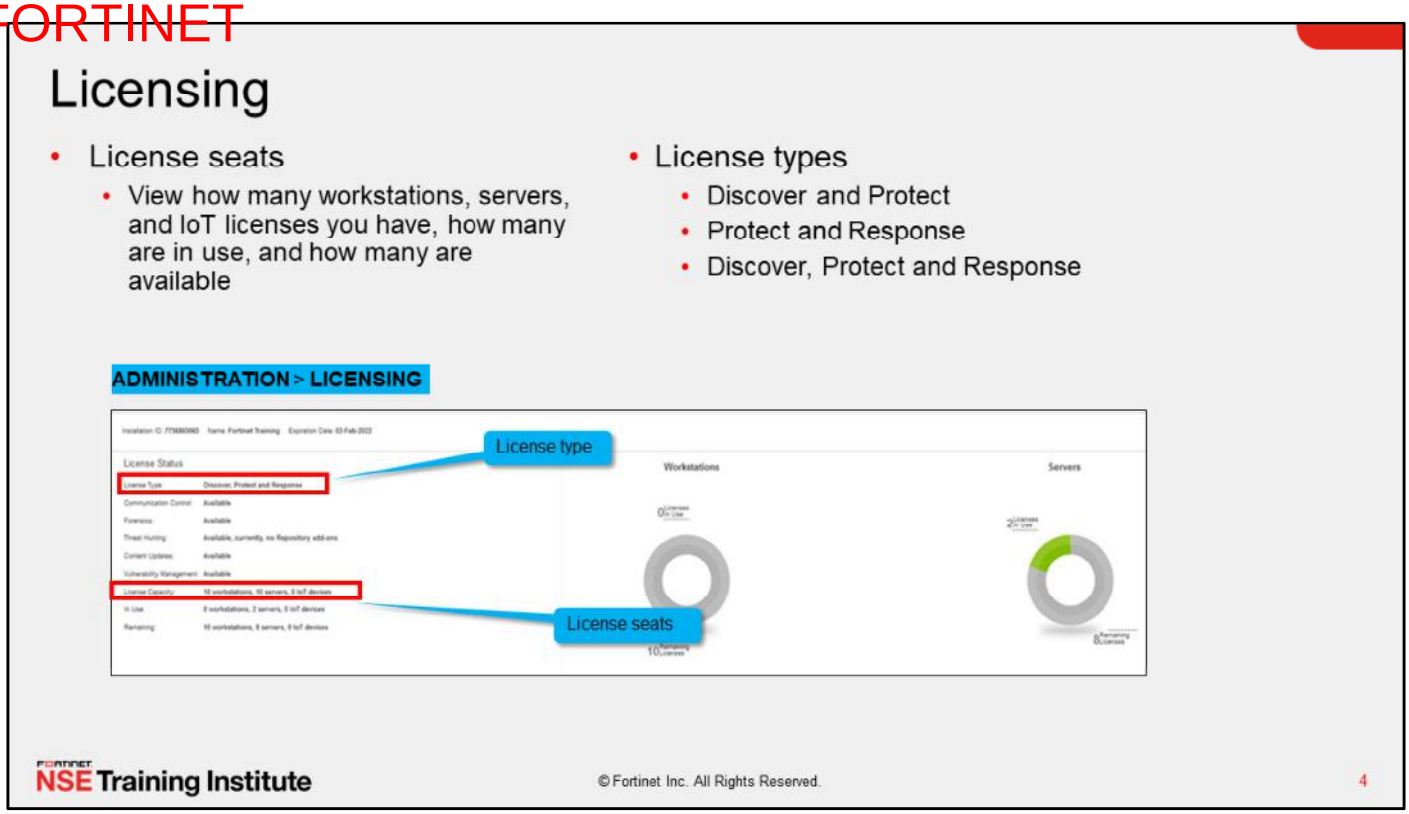


After completing this section, you should be able to achieve the objectives shown on this slide.

By demonstrating competence in licensing and user administration, you will be able to identify the license types and create user accounts in FortiEDR.

Vouchers & Dumps are Available | WhatsApp +201224560923

DO NOT REPRINT Brave-dumps.com
© FORTINET



To maintain your system health, you'll need to keep track of your license permissions and capacity. In the **ADMINISTRATION** tab under **LICENSING**, you'll see your license type listed, along with the features available with that license. The example on this slide shows a Discover, Protect and Response license, and all the FortiEDR features are available.

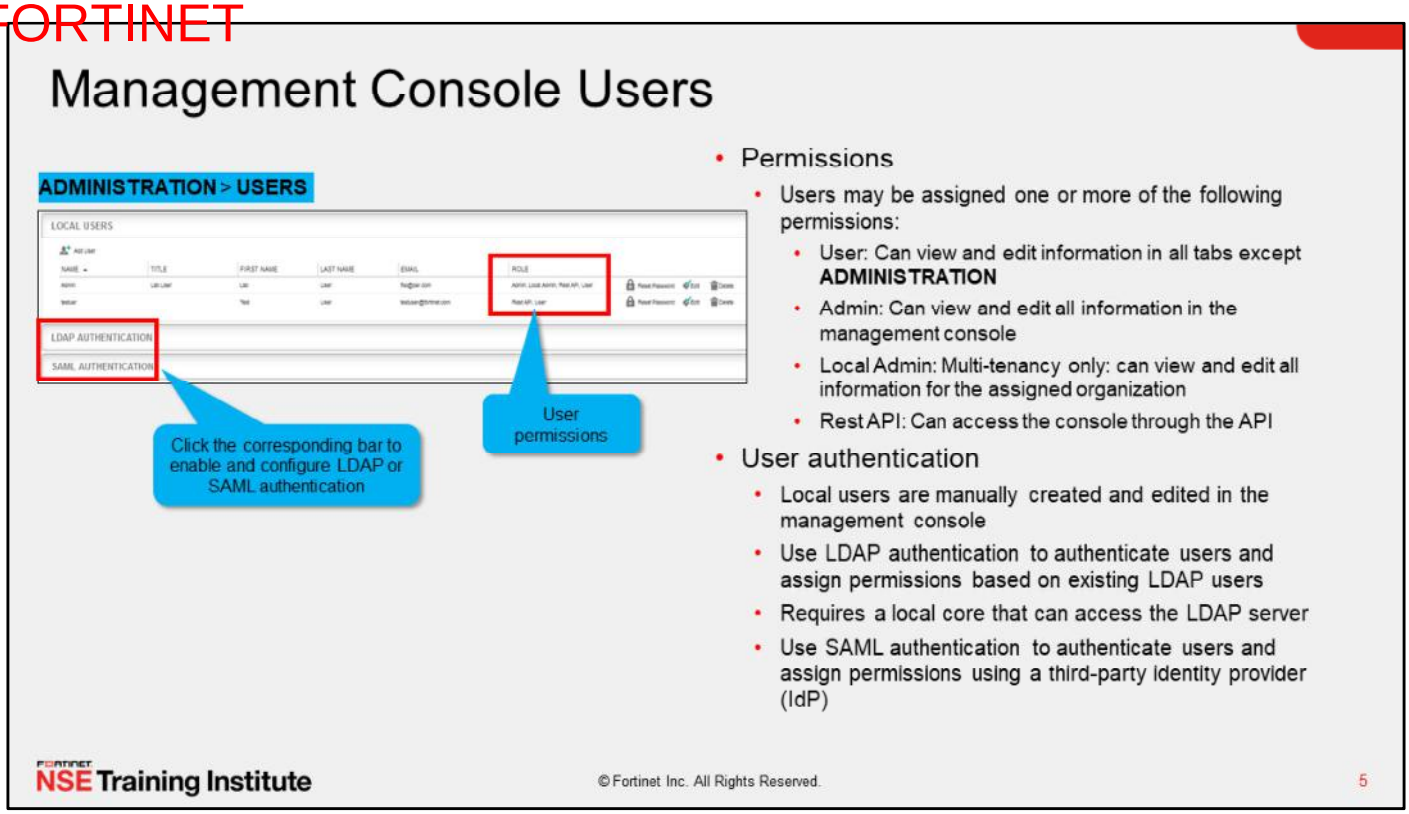
You can also see information about your license usage. There are three types of license seats. Workstations cover most of your end users. Server licenses apply to any collector installed on a server, including all Linux versions. On the right, you can see a visual representation of the license seats in use and those remaining for workstations and servers. IoT devices include all non-workstation devices connected to your network, such as printers, smart phones, or media players.

FortiEDR offers three different license types. Discover and Protect includes asset discovery, attack surface reduction ,USB device control, along with the kernel-based NGAV and web filtering. Protect and Response also offers kernel-based NGAV and web filtering as well as automated incident response using playbooks, and the ability to perform such as removing files, terminating malicious processes, reversing persistent changes, notifying users, isolating applications and devices, and opening tickets. Discover, Protect and Response is a combination of the other two license types. All license types have add-on features as well. For more details, contact Fortinet sales.

When you renew or extend your license, you'll get a new license string. To update your management console, click **Update License** and paste the string into the window.

Vouchers & Dumps are Available | WhatsApp +201224560923

DO NOT REPRINT Brave-dumps.com
© FORTINET



Now you'll learn about management console users. You can find a list of your organization's management console users on the **ADMINISTRATION** tab under **USERS**. There are four levels of permission. The default level is User. A User can view and edit information for their organization on every tab of the management console except **ADMINISTRATION**, which is hidden to them.

Users with Admin permissions can view and edit information anywhere on the management console. Local admins exist only for multi-tenant environments. Users with Local admins have the same permissions as Admin users, but only within their organization. All other organizations are hidden to them. You'll learn more about multi-tenancy in a later section.

A user must have rest API permissions to access the management console through API. Rest API users generally also have user or admin permissions.

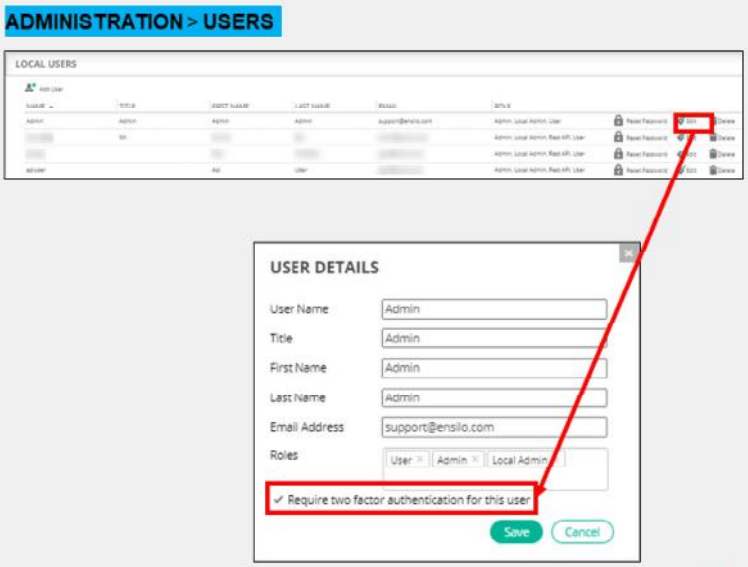
There are three ways to create management console users. The first is manually, under **LOCAL USERS**. These users are created and managed individually through the management console. You can also use LDAP authentication to authenticate users and assign permissions based on existing LDAP users. Be aware that LDAP requires a local core with access to the LDAP server. Lastly, you can connect to a third-party identity provider to authenticate users using SAML authentication.

Vouchers & Dumps are Available | WhatsApp +201224560923

DO NOT REPRINT Brave-dumps.com
© FORTINET

Configuring Two-Factor Authentication

- You can enable and configure two-factor authentication on the **Administration** tab of the management console
  - In the column on the left, click **Users**
  - For each user who should log in with two-factor authentication, click **Edit** on the user row
  - In the **USER DETAILS** window, select the **Require two factor authentication for this user** checkbox
- If a user loses their authentication token, click **Reset Password** and select **Reset the Two-Factor authentication** radio button
- You can enable two-factor authentication for all LDAP logins on the **LDAP AUTHENTICATION** panel



NSE Training Institute

© Fortinet Inc. All Rights Reserved.

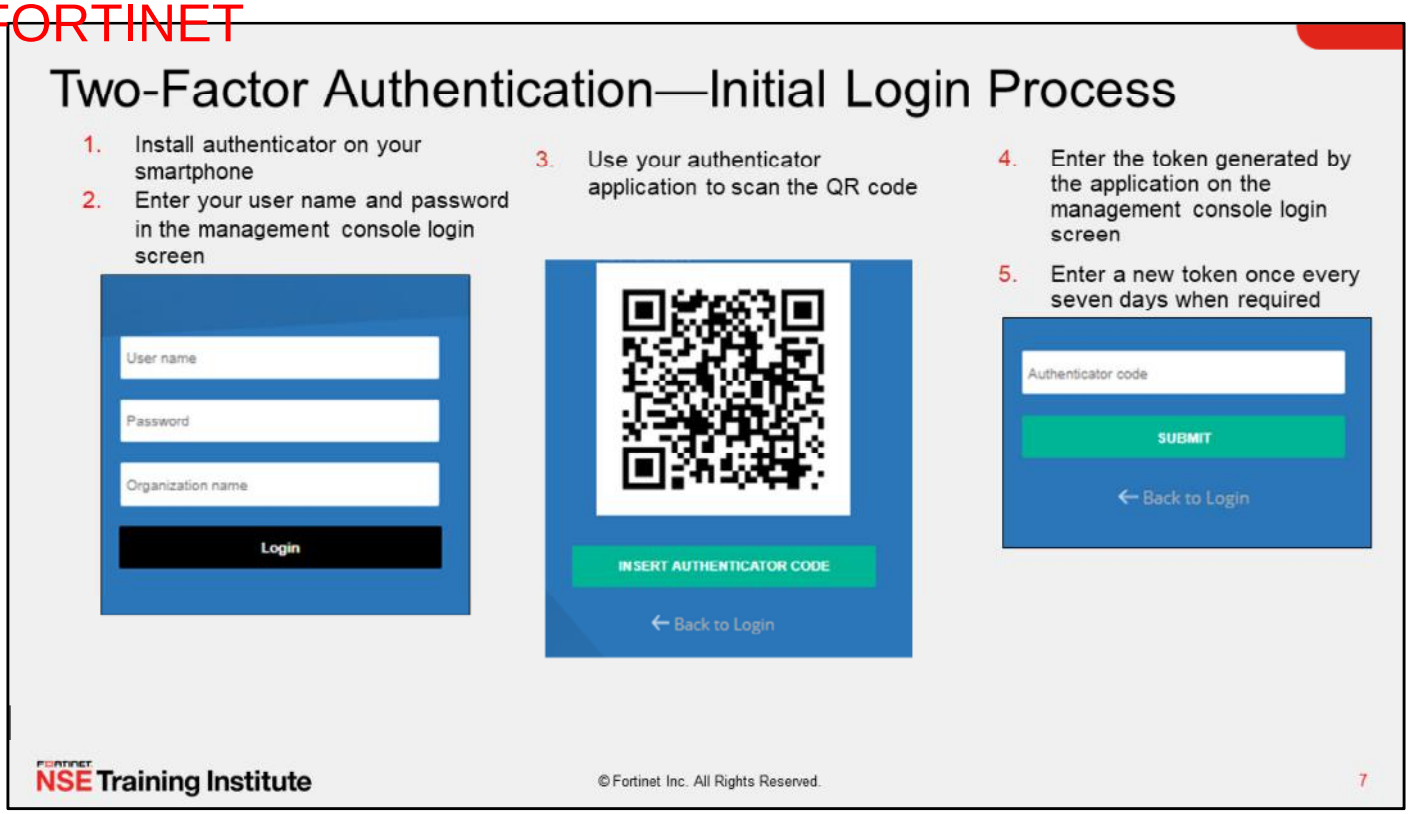
6

When you create management console users manually, you have the option to enable two-factor authentication. Just click **Edit** next to a user, and in **User Details**, select **Require two factor authentication for this user**, then click **Save**. You can also enable two-factor authentication when you're creating a new user.

Click **Reset password** in the user list to reset the user's token or password. If you are using LDAP authentication, open the **LDAP AUTHENTICATION** panel and select **Require two-factor authentication for all LDAP logins**.

Vouchers & Dumps are Available | WhatsApp +201224560923

DO NOT REPRINT Brave-dumps.com
© FORTINET



FortiEDR two-factor authentication works with any standard authenticator application. Install an authenticator application on your smartphone if you don't already have one. On the login screen of the console, type your username and password, and your organization name, if you're in a multi-tenant environment. You'll see a QR code like the one in the center. Scan it with your authenticator application on your phone. This associates a specific token generated in the application with your FortiEDR login. Enter the token generated by the application to complete the setup process.

After you've set up your two-factor authentication, the next time you log in will be the same as usual. You will enter your name and password—and organization name, if applicable—and log in. Enter a new token once every seven days. When you see the authentication screen on the right, repeat step 4, and you'll be set for the next week.

Vouchers & Dumps are Available | WhatsApp +201224560923

DO NOT REPRINT
© FORTINET
Brave-dumps.com

Knowledge Check

1. Which user permission is required to view and edit all information in the management console?
   A. Local Admin
   ✓ B. Admin

2. Which remote authentication protocol does the FortiEDR management console support?
   A. LDAP
   ✓ B. Radius

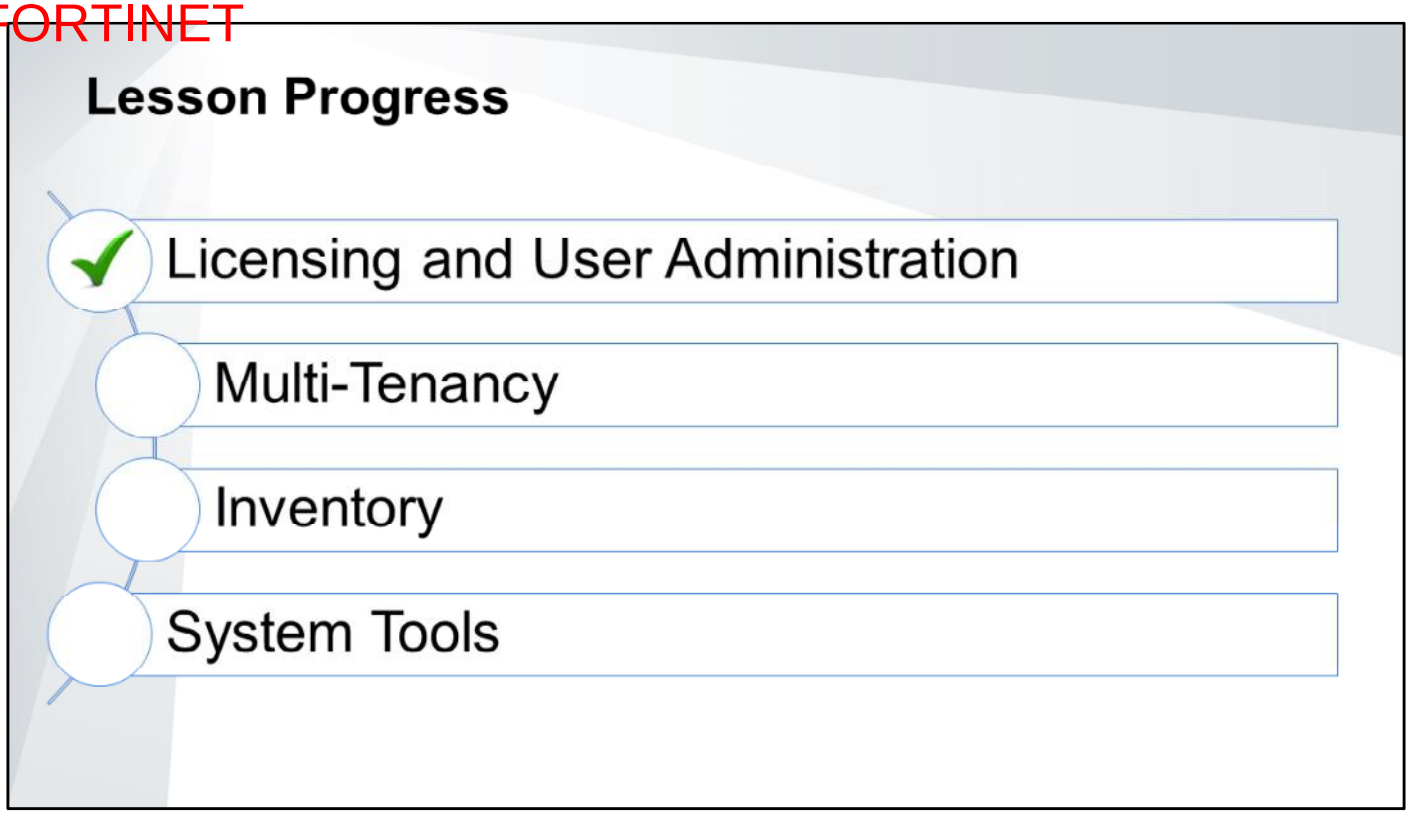
NSE Training Institute

© Fortinet Inc. All Rights Reserved.

8

Vouchers & Dumps are Available | WhatsApp +201224560923

DO NOT REPRINT
© FORTINET
Brave-dumps.com

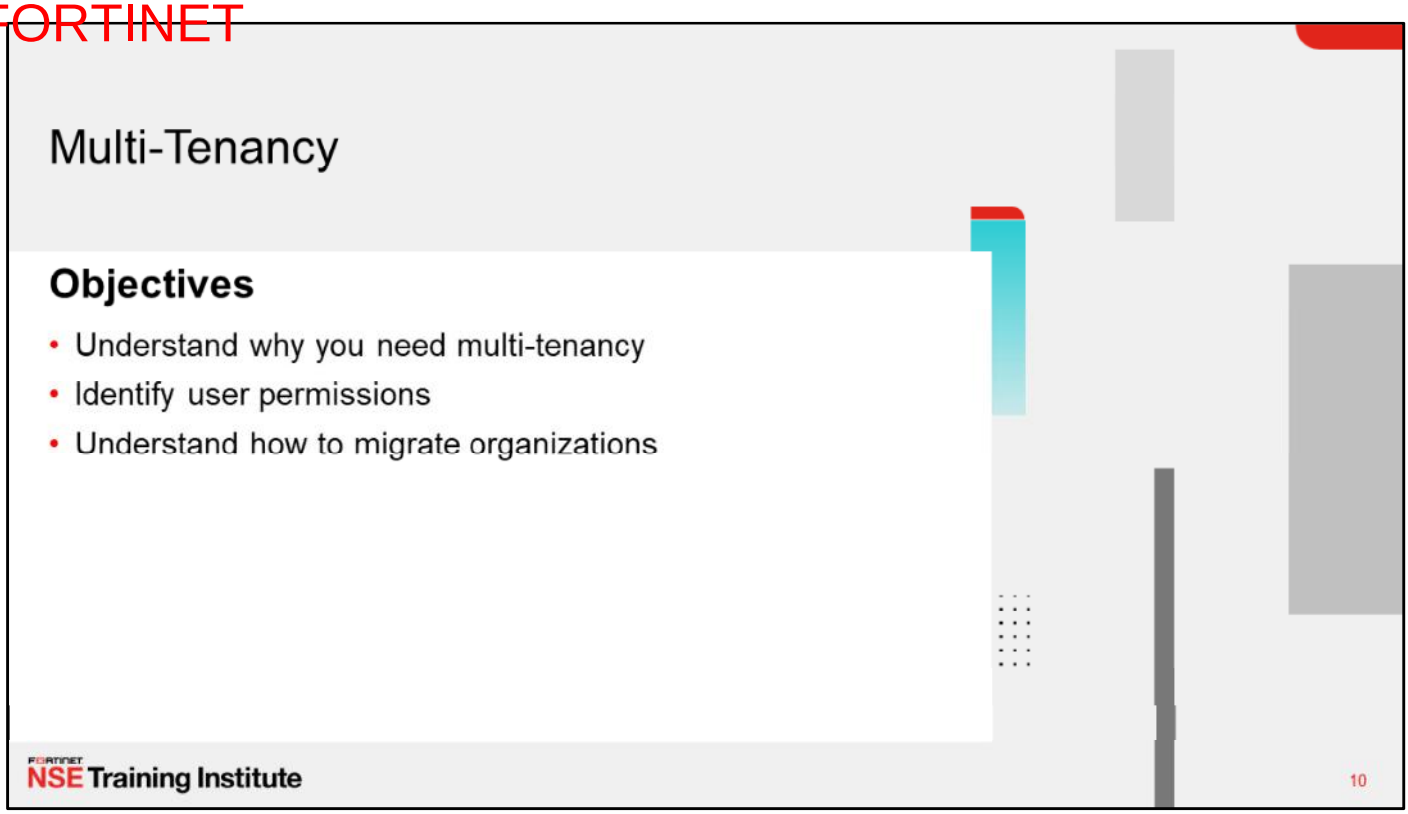


Good job! You now understand FortiEDR licensing and user administration.

Now, you will learn about multi-tenancy.

Vouchers & Dumps are Available | WhatsApp +201224560923

DO NOT REPRINT
© FORTINET
Brave-dumps.com

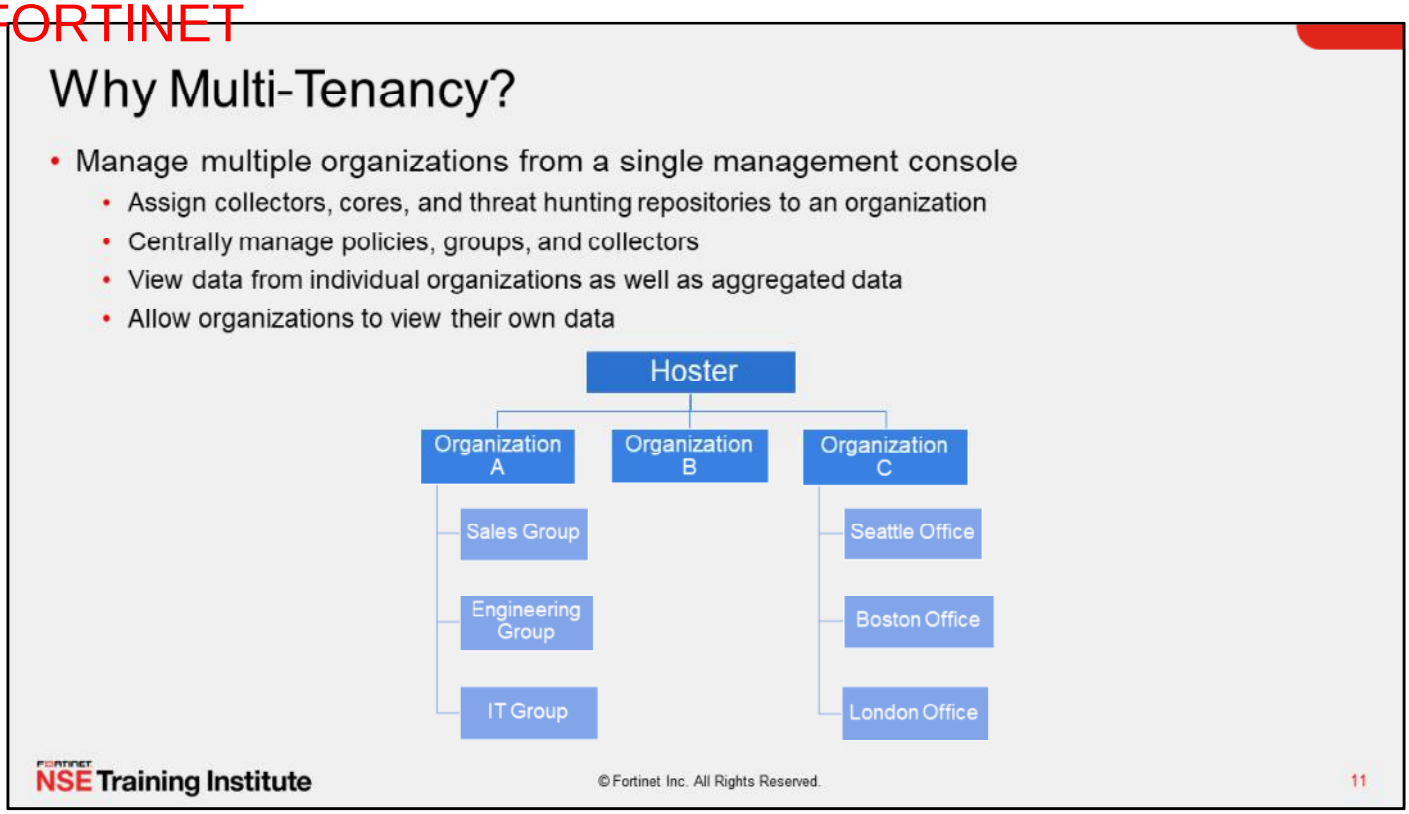


After completing this section, you should be able to achieve the objectives shown on this slide.

By demonstrating competence in multi-tenancy, you will be able to configure and manage a multi-tenant FortiEDR management console.

Vouchers & Dumps are Available | WhatsApp +201224560923

DO NOT REPRINT Brave-dumps.com
© FORTINET



So, the first question is, why multi-tenancy? The primary use case is to manage multiple organizations from a single management console. For example, using multi-tenancy, a managed service provider (MSP) requires logins to only one or two consoles to manage multiple organizations efficiently and effectively. You can assign collectors and threat hunting repositories to an organization, and you can assign cores to individual organizations. You can manage policies, groups, and collectors from all your organizations in one place. Hosters also have the ability to view an individual organization's data, or see aggregated data for all organizations.

If you host multiple organizations on a single console, multi-tenancy also allows you to give administrators from a single organization access to their own console. Previously, client administrators couldn't access their own alerts in this scenario because their alerts couldn't be separated from the alerts of other customers. Now you can let administrators log in and view only their own organization's data.

Vouchers & Dumps are Available | WhatsApp +201224560923

DO NOT REPRINT Brave-dumps.com
© FORTINET

User Permissions

- A hoster Admin (Admin) can:
  - Create, modify, and delete organizations
  - View and manage system components, events, and policies from all organizations
- A Local Admin can:
  - View and manage system components, events, and policies assigned to their organization
  - View and manage administrative data within their organization
- A User can:
  - View and manage system components, events, and policies assigned to their organization

Permissions	Admin	Local admin	User
View Single Organization Data	Yes	Yes	Yes
Edit Single Organization Settings and Data	Yes	Yes	Yes
View and Manage Single Organization Administrative Settings	Yes	Yes	No
Create and Manage Organizations	Yes	No	No
View All Organizations	Yes	No	No
View Global Data	Yes	No	No

NSE Training Institute © Fortinet Inc. All Rights Reserved. 12

As you learned on the previous slide, the user level determines what you can do on the management console. If you're an Admin, you can create, modify, and delete organizations, and you can view and manage system components, events, and policies for all organizations. You can see all the organizations in your environment, as well as global data. Going forward in this lesson, *Admin* will always refer to the hoster Admin.

A Local Admin can view and manage system components, events, and policies assigned to their own organization, as well as administrative settings for their own organization, but they can't see or do anything outside of their own organization. This role is essentially the same as the Admin, except it’s limited to a single organization.

A User can also view and edit single organization data, but can't see or access the **ADMINISTRATION** tab. A User can view and modify security events, policies, communication control and inventory, but they can’t retrieve the registration password, edit the end-user notification settings, create a new console user, or any of the other functions found on the **ADMINISTRATION** tab.

Vouchers & Dumps are Available | WhatsApp +201224560923

DO NOT REPRINT Brave-dumps.com
© FORTINET

Login Screen

- **Organization name** field
  - When logging in to a multi-tenant environment, users must enter their assigned organization as well as their **User name** and **Password**
  - Organization name is case-sensitive
  - If the **Organization name** field is blank, the user is logged in to the default organization if their permissions allow

NSE Training Institute

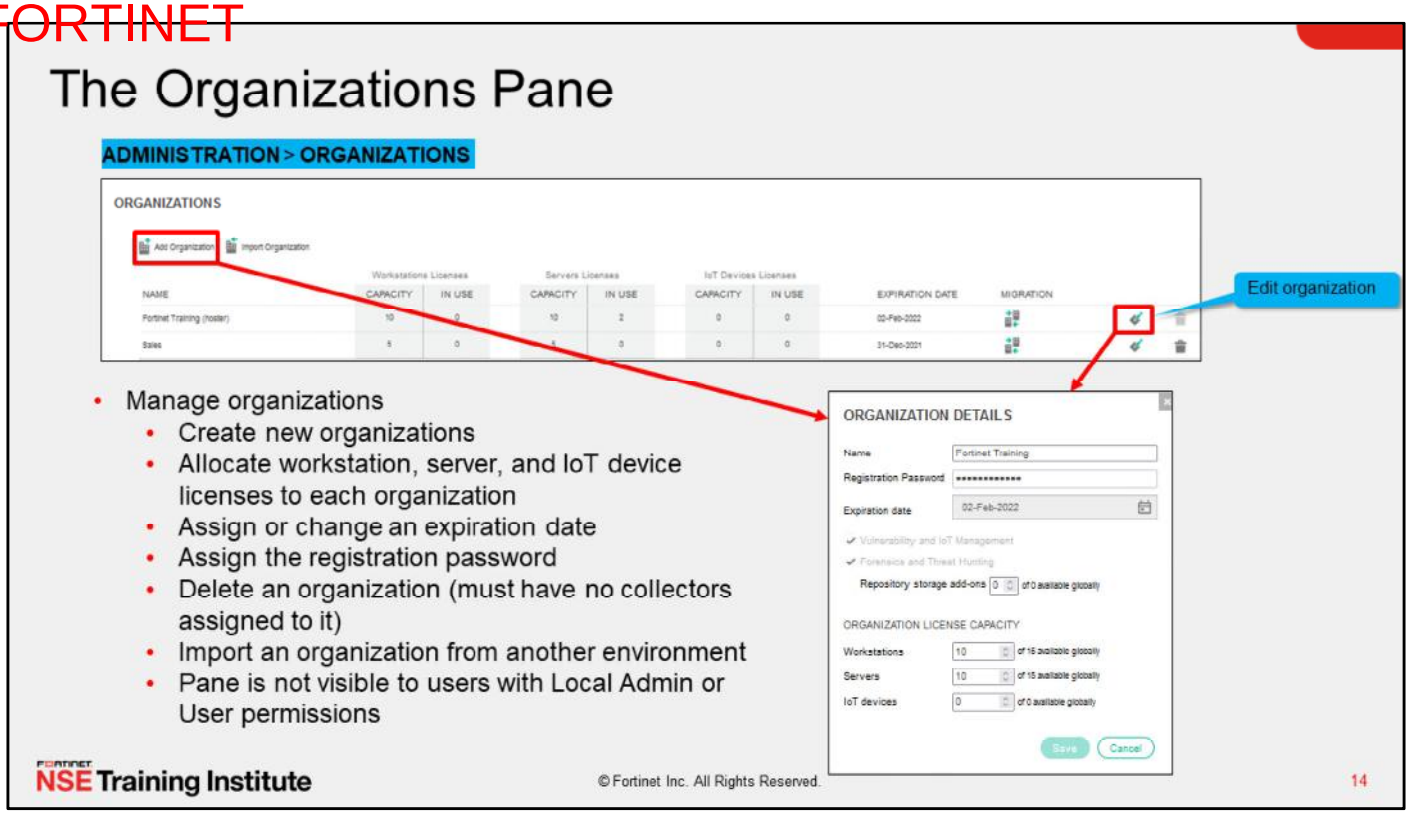
© Fortinet Inc. All Rights Reserved.

13

The login screen of a multi-tenant environment has an **Organization name** field. When logging in to a multi-tenant environment, users must enter the name of their assigned organization as well as their **User name** and **Password**. The organization name is case sensitive, so be sure to tell management console users exactly how to enter it. If this field is left empty, the user is logged in to the default organization, if their permissions allow. In a single-tenant organization, the organization field doesn't appear.

Vouchers & Dumps are Available | WhatsApp +201224560923

DO NOT REPRINT Brave-dumps.com
© FORTINET



Only users with Admin permissions can view the **ORGANIZATIONS** pane of the **ADMINISTRATION** tab. Hoster Admins can create and edit organizations and allocate license seats for each organization, including the number of workstations, servers, and IoT devices that are allocated to the organization. You can also set or change each organization's license expiration date. License seats and expiration dates are contingent on the hoster organization's license with Fortinet. You'll learn more about that on the next slide.

In multi-tenant environments, registration passwords are organization-specific, so they're part of the organization settings as well. If needed, you can delete organizations. Note that you can't delete an organization without removing all the collectors assigned to it, either by deleting them from the system or moving them to another organization. You can also import an organization from another environment using the migration tool.

You'll see the **ORGANIZATION DETAILS** dialog box when you create a new organization or edit an existing one. Only hoster Admins can assign and edit organization details. First, you'll see the organization's name. You'll use the name to assign collectors to the organization during installation and to move existing collectors to the organization. Users with Local Admin and User permissions will also use the organization name to log in to the management console. Remember that the organization name is case-sensitive when you log in to the console, so make sure all users know exactly how their organization is entered here. Organizations are also assigned a unique ID in the background, so you can change the name if you need to without affecting the collectors assigned to the organization.

The **Registration Password** is organization specific, and it allows organizations to validate collector installations and uninstallations. This makes it harder for malware to disable or remove the collector, and also prevents users from uninstalling the collector accidentally.

Vouchers & Dumps are Available | WhatsApp +201224560923

DO NOT REPRINT Brave-dumps.com
© FORTINET

Hoster Admin Views

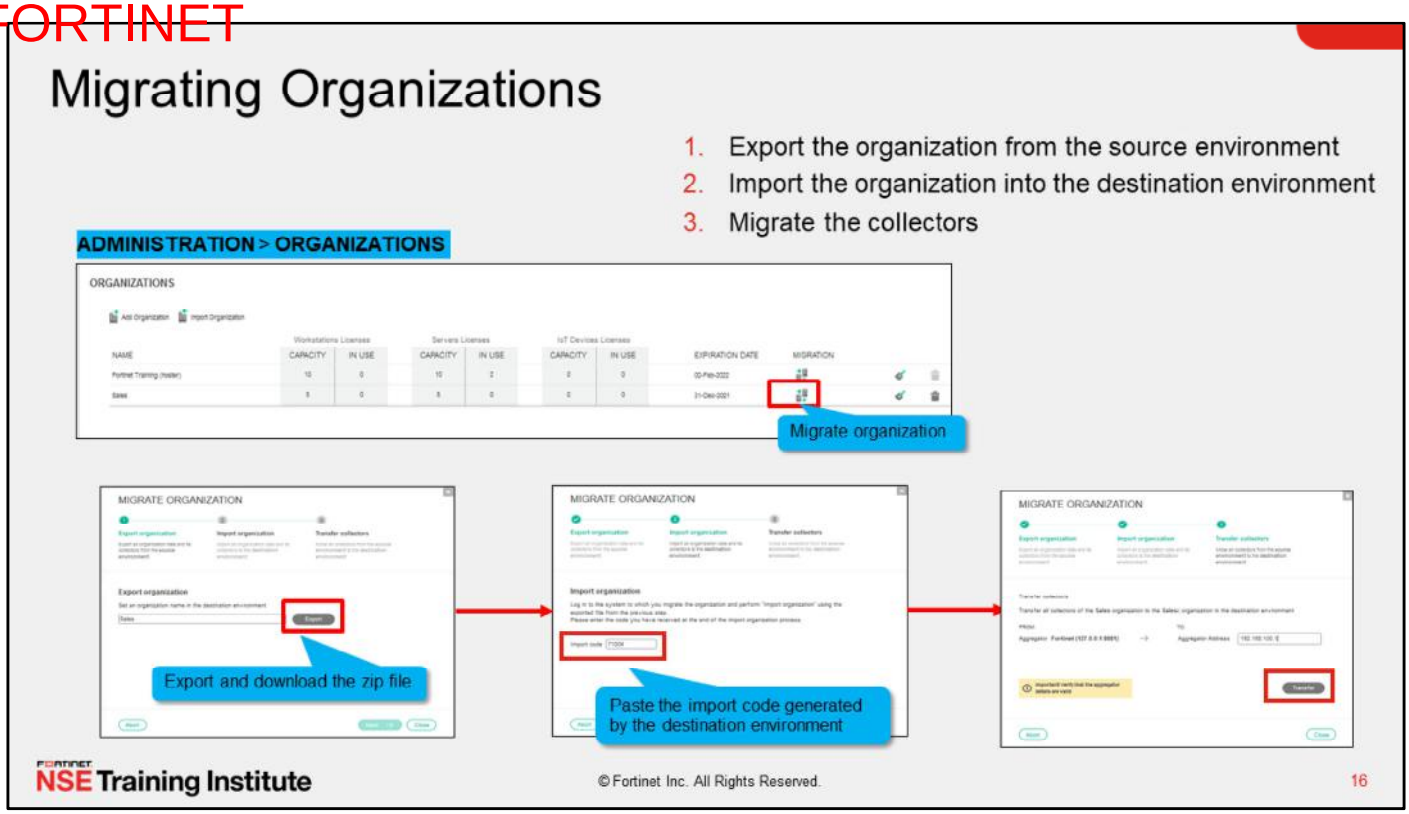
- **Hoster View**
  Aggregated data for all organizations, including:
  - Security events
  - Exceptions
  - Security policies
  - System components
  - Administrative data
- **Organization View**
  - Exceptions, exclusions
  - Application usage data and aggregated application data
  - Threat-hunting settings
  - Security policies
  - System components
  - Administrative data

NSE Training Institute © Fortinet Inc. All Rights Reserved. 15

Users with Admin permissions have two views to choose from. The first is the **Hoster view**. This allows you to view aggregated data from all organizations, including security events, exceptions, security policies, system components, and administrative data. You can also drill down into a specific organization by selecting it from the drop-down list on the upper left. In the **Organizations** view, you can see data specific to a particular organization, including security events, exceptions, application usage data, aggregated application data, security policies, system components, threat-hunting settings, and administrative data for the selected organization.

Vouchers & Dumps are Available | WhatsApp +201224560923

DO NOT REPRINT Brave-dumps.com
© FORTINET



If you have multiple FortiEDR environments, you might want to move an organization from one to another—for example, from a POC environment to a customer environment. You can do that on the **ADMINISTRATION** tab under **ORGANIZATIONS**. You'll need Admin permissions for both the source and destination environments.

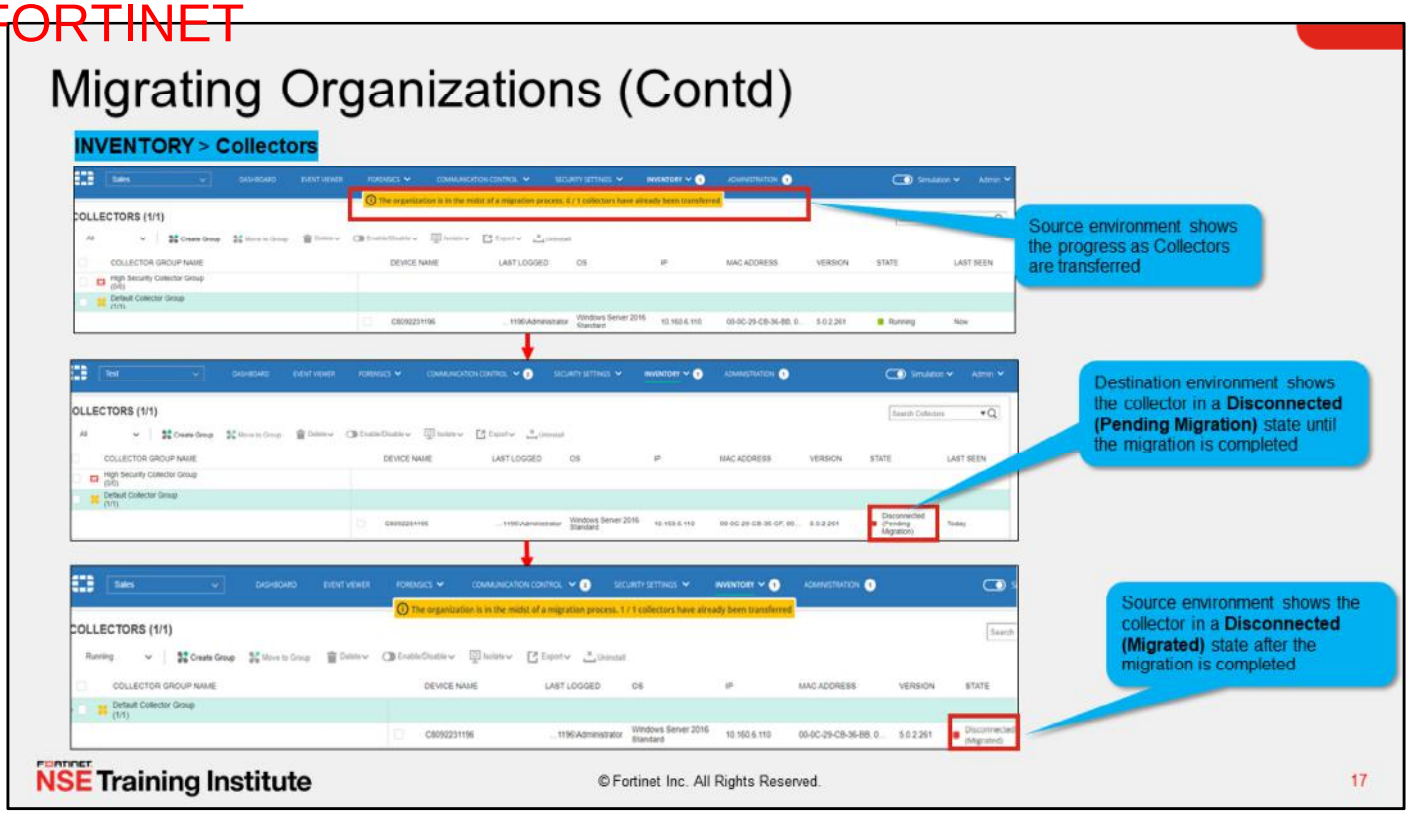
The first step is to export the organization from the old environment. Click the migration button on the organization's row. The **MIGRATE ORGANIZATION** dialog box opens. Type the name you want to use in the new environment. You must choose a name that does not already exist in the destination environment. Then click the **Export** button. FortiEDR generates a zip file containing all the organization's data and destinations. This may take several minutes, depending on the size of the organization. When the file is generated, click **Download** and save the file locally.

Next, you must import the organization into your target environment. On a new browser tab or window, log in to the destination management console and browse to the **ORGANIZATIONS** pane of the **ADMINISTRATION** tab. Click the **Import Organization** button, browse to the zip file you downloaded earlier, and click **Import**. The import process may take several minutes to complete. Once it is finished, an **Import code** appears in the dialog box under the progress bar. Copy the code. Next, return to the source management console. Paste the import code in step of the **MIGRATE ORGANIZATION** dialog box. If you closed the dialog box or management console earlier, you can return to this step by clicking the **Continue Migration** button in the organization row. Once you've entered the code, click **Next** to continue.

The final step is migrating the collectors. In the **MIGRATE ORGANIZATION** dialog box, type the aggregator address and port of the target environment. Then, click the **Transfer** button and wait for the transfer process to complete.

Vouchers & Dumps are Available | WhatsApp +201224560923

DO NOT REPRINT Brave-dumps.com
© FORTINET



When the migration process begins, there will be a progress indicator on the source environment showing the collectors are being transferred. On the destination environment click the **INVENTORY** tab and select **Collectors.** The collectors will have a **Disconnected (Pending Migration)** state until the migration is completed. Once the migration has successfully completed, the source environment shows the collectors as **Disconnected (Migrated)** and the destination environment shows the collectors in a **Running** state. Until the migration process is completed the collectors remain connected and protected by the source environment.

Vouchers & Dumps are Available | WhatsApp +201224560923

DO NOT REPRINT
© FORTINET
Brave-dumps.com

Knowledge Check

1. Which pane on the FortiEDR management console can only be viewed by a hoster Admin?
   A. USERS
   ✓ B. ORGANIZATIONS

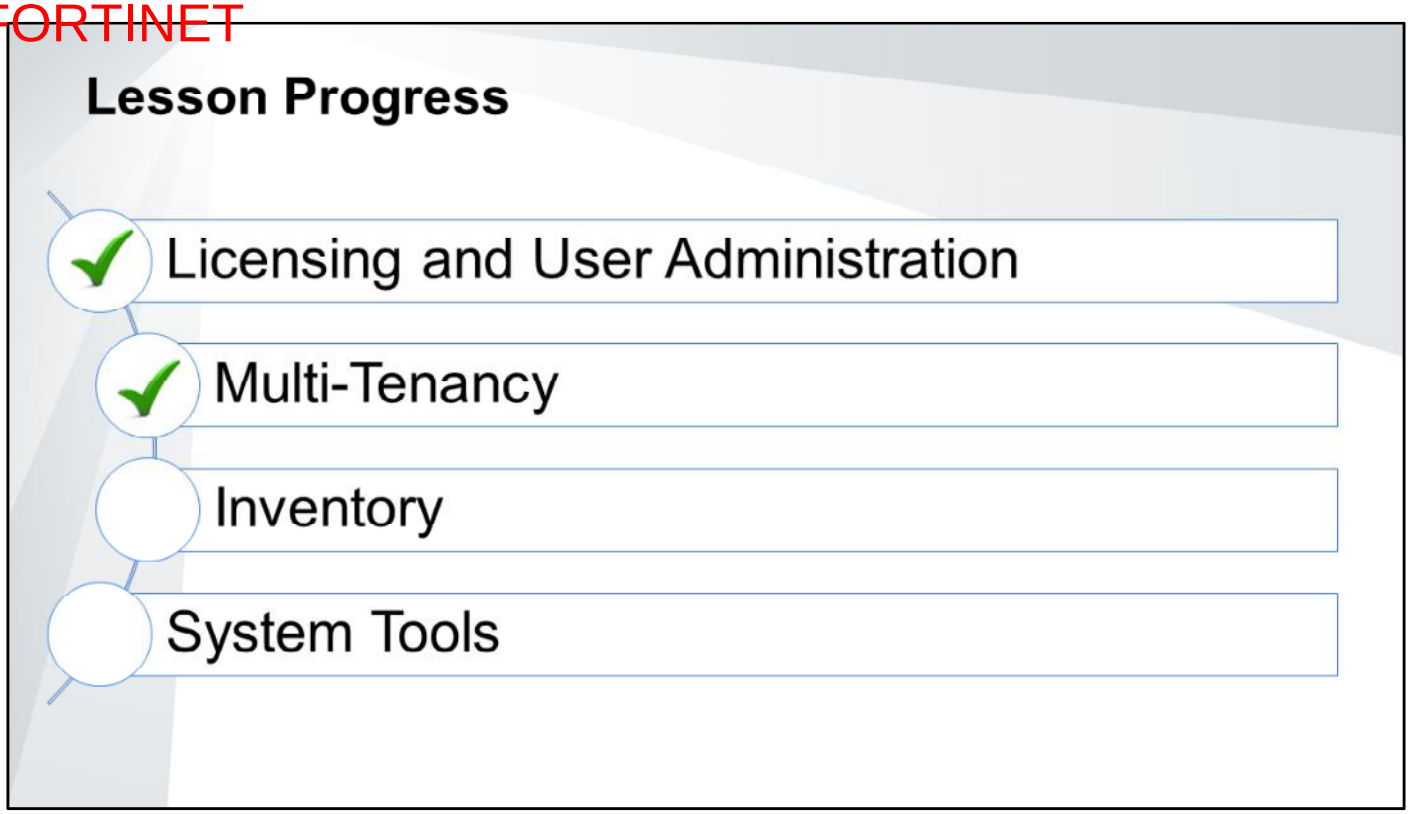
NSE Training Institute

© Fortinet Inc. All Rights Reserved.

18

Vouchers & Dumps are Available | WhatsApp +201224560923

DO NOT REPRINT
© FORTINET
Brave-dumps.com

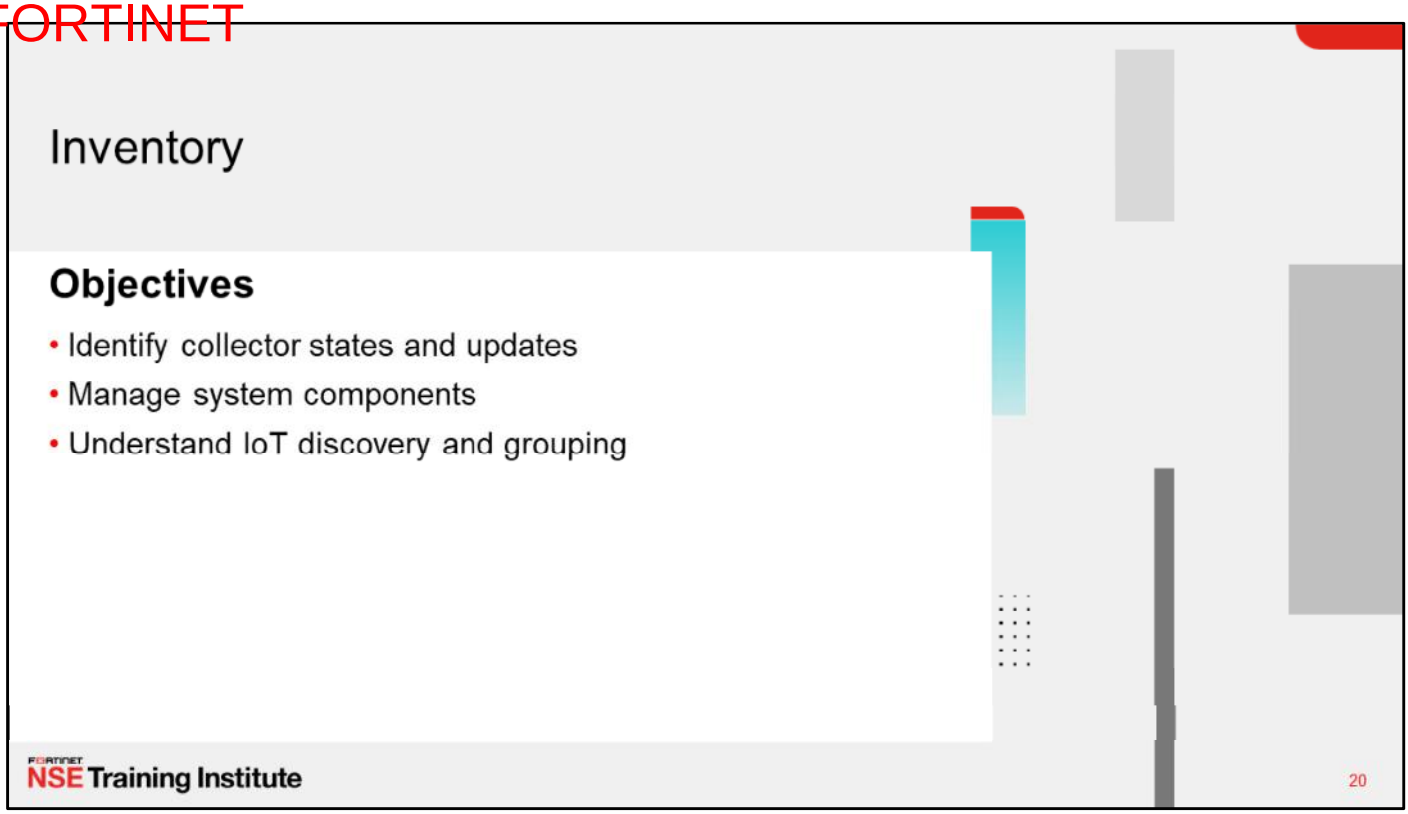


Good job! You now understand multi-tenancy

Now, you will learn about FortiEDR inventory.

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 FortiEDR inventory, you will be able to understand the management of system components.

Vouchers & Dumps are Available | WhatsApp +201224560923

DO NOT REPRINT Brave-dumps.com
© FORTINET

Managing Collectors

- By default only degraded collectors are shown **Under INVENTORY > Collectors**
- To view all collectors in your system, click **Show All Collectors**

- Uninstalling a collector
  - You can uninstall collectors remotely from the **Inventory** tab if they are connected
  - You may also uninstall a collector manually from the device
- Deleting a collector
  - Delete uninstalled collectors from the management console to reduce clutter
  - Deleting a collector does not uninstall it from the device

NSE Training Institute

© Fortinet Inc. All Rights Reserved.

21

To display a list of all the collectors in your ,click the **INVENTORY** tab and select **Collectors**. By default, you'll see only collectors that are in a degraded state. This is to draw your attention to collectors that are not performing correctly and need your attention. Click **Show All Collectors** to see all collectors, organized by collector group. You can also view all collectors by clicking the drop-down filter at the top of the list and selecting **All**. You can filter by other states too. You'll learn more about collector states in this lesson. Select **Unmanaged** to view all the workstations and servers in your system that do not have the FortiEDR collector installed. These devices are not protected.

The numbers next to each collector group indicate how many collectors you can see in the current view and the total number of collectors in the group. For example, if you set the filter to show only collectors that are disabled, you might see only one collector out of the 10 that are in the group.

You can create collector groups by clicking **Create Group**. Then, select the checkbox for each collector you want to move, click **Move to Group**, and select your newly created group.

To uninstall a collector, you can do so remotely from the **INVENTORY** tab of the management console. You can remotely uninstall a device only when it is connected. You can also manually uninstall the collector from the device itself. You will need the registration password to manually uninstall the collector. You learned about the registration password in the previous lesson. You can retrieve it from the **TOOLS** panel of the **ADMINISTRATION** tab.

Deleting a collector removes it from the management console. You can delete a collector even while it is disconnected. However, if you delete a collector without uninstalling, it will reappear on your **INVENTORY** tab if the device connects to your network again.

Vouchers & Dumps are Available | WhatsApp +201224560923

DO NOT REPRINT Brave-dumps.com
© FORTINET

Collector States

- To view the status of individual collectors, check the **INVENTORY** tab of the management console
- **Running**: The FortiEDR collector is working with no issues
- **Running (Autonomously)**: The Core is temporarily inaccessible, so policies will be enforced by the FortiEDR collector
- **Disconnected**: The device is offline, powered down, or not connected to the FortiEDR Aggregator
- **Disconnected (Expired)**: The device has not connected to the system in more than 30 days
  - FortiEDR automatically frees the license for other users
- **Pending Reboot**: The FortiEDR collector is ready to run after this device is rebooted
  - Device must be rebooted manually
- **Disabled**: The FortiEDR collector was disabled in the FortiEDR Central Manager
- **Degraded**: The FortiEDR collector is prevented from performing to its full capacity
  - A degraded status may be caused by compatibility issues or a lack of resources on the device

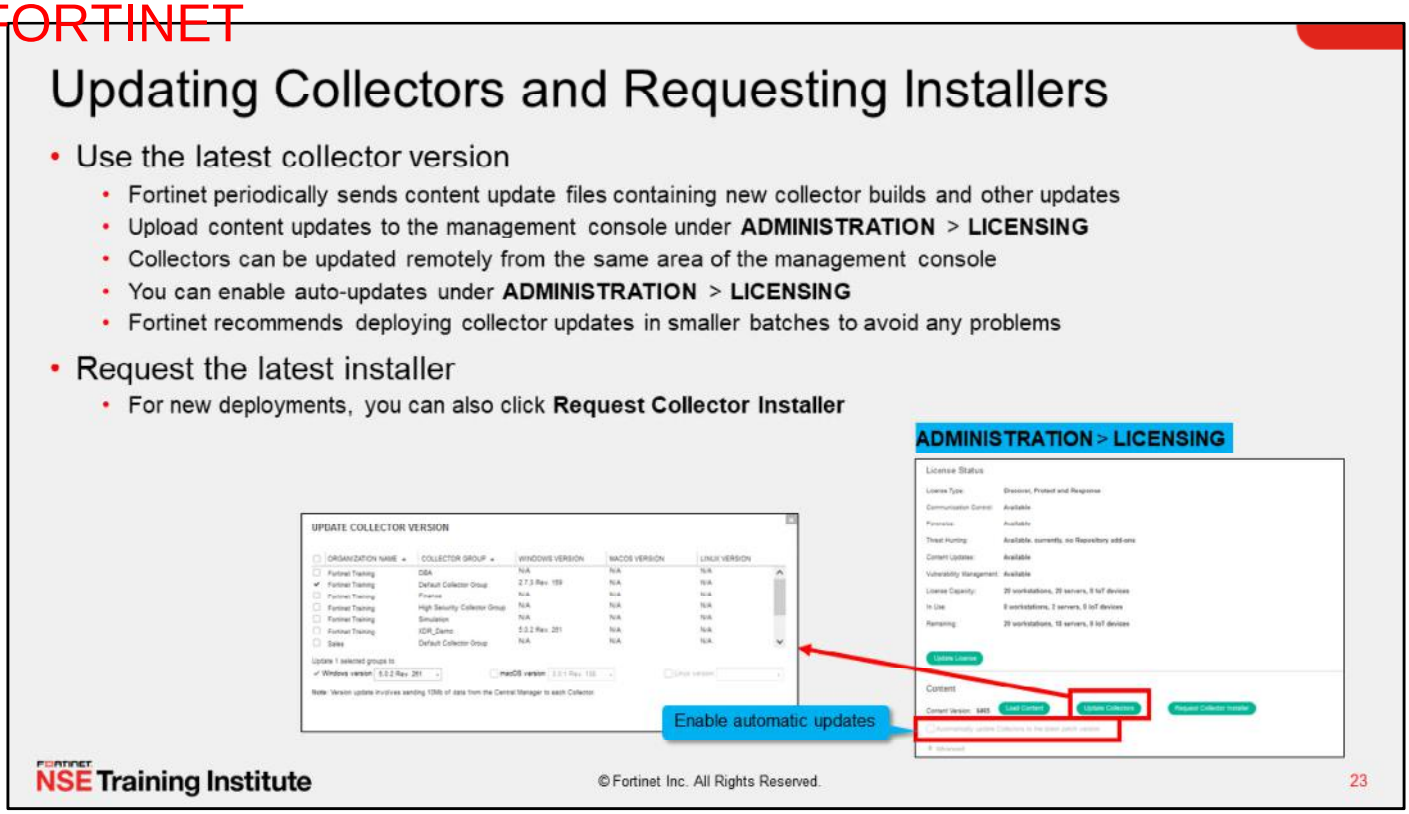
NSE Training Institute © Fortinet Inc. All Rights Reserved. 22

Here's a short overview of the collector states:

- **Running** means working with no issues.
- If the Core is temporarily inaccessible, the collector enforces policies on its own, and its state is displayed as **Running (Autonomously)**.
- **Disconnected** means the device is not connected to the aggregator, often because it's powered down.
- If a collector hasn't connected to the system in more than 30 days, FortiEDR automatically releases its license seat. The collector isn't removed from the system.
- In a few rare cases, generally relating to compatibility issues with antivirus software, you must reboot the FortiEDR collector. In these cases, the collector won't load until after the reboot, and you'll see the status listed as **Pending Reboot**.
- If a collector is **Disabled**, it was probably disabled from the management console. This may occasionally be necessary for troubleshooting.
- **Degraded** shows an issue is preventing the collector from performing at full capacity. This should be investigated to identify the source of the problem.

Vouchers & Dumps are Available | WhatsApp +201224560923

DO NOT REPRINT Brave-dumps.com
© FORTINET



Always make sure you're using the latest collector version on all devices. New versions of the collector are delivered through content updates, which you can upload on the **ADMINISTRATION** tab of the management console under **LICENSING**. You can upgrade collectors remotely from same place. Fortinet recommends deploying collector updates in smaller batches to avoid any problems. When you move a collector to a new collector group, the collector checks for updates, so any major changes to collector group assignment should also be done in phases. After the collector has been updated, you can request the installer files from the management console.

In the example shown on this slide, **Update Collectors** was clicked to open the **Update Collector Groups** window. The **Default Collector Group** group, which is currently running Windows version 2.7.3 Rev 159, is shown in the example. The **Windows** checkbox was selected, and version **5.0.2 Rev 261** was selected in the drop-down list. Click **Update** to begin updating the selected group.

Vouchers & Dumps are Available | WhatsApp +201224560923

DO NOT REPRINT Brave-dumps.com
© FORTINET

Isolation Mode and the High Security Collector Group

- High Security Collector Group
  - The High Security Collector Group is built into the FortiEDR system and cannot be deleted
  - Management console users may choose which policies to apply
  - Fortinet recommends applying strict policies to this group to help contain infections
- Isolation mode
  - Collectors in isolation mode are automatically assigned to the isolation policy in communication control
  - The isolation policy blocks communication from all applications by default
  - Collectors in isolation mode are marked with a specific icon in the **INVENTORY** tab
  - Only new sessions after device isolation are blocked, not existing sessions
  - ICMP and incoming RDP connection are not blocked

NSE Training Institute © Fortinet Inc. All Rights Reserved. 24

Isolation mode and the High Security Collector Group are security measures that provide additional protection to a collector after an attack. These measures can be particularly helpful during deployment when collectors are still in simulation mode. If an attack occurs during this phase, you can increase security on any affected collectors without rushing the entire deployment group into prevention mode.

FortiEDR comes with a built-in High Security Collector Group, which cannot be deleted. This group is intended as a temporary quarantine for infected collectors. Fortinet recommends applying strict policies to this group, and making sure that those policies are always in prevention mode.

Isolation mode is also intended to prevent infections from spreading from affected devices. Collectors in this mode are assigned to a special isolation policy in communication control, which automatically blocks all application communication by default. If needed, you can configure specific applications, like security or remediation tools, to be allowed to communicate when isolated. By design, ICMP and incoming RDP connection are allowed on an isolated unit to assist IT in determining that the machine is on and physically connected to the network. Isolation mode as well as any communication control denial that is performed by the collector takes effect only on new network sessions.

Vouchers & Dumps are Available | WhatsApp +201224560923

DO NOT REPRINT Brave-dumps.com
© FORTINET

System Components

- By default only degraded cores, aggregators are shown under **INVENTORY** > **System Components**
- To view all cores, aggregators in your system, click **Show All Cores** or **Show All Aggregators**
- To view all repositories click **Repositories**
- **System Components** information:
  - Core
    - IP address, version, state
    - Deployment Mode (cloud or on-premise)
    - Functionality
      - Core only
      - JumpBox
      - Both (Core + JumpBox)
  - Aggregators
    - IP address, version, state
    - Connected collectors
  - Repositories
    - IP address and state

NSE Training Institute

© Fortinet Inc. All Rights Reserved.

25

You can view information about the system components on the **INVENTORY** tab under **System Components**. By default, only cores and aggregators that are in a degraded state are displayed. To view all cores or aggregators, click **Show All Cores** or **Show All Aggregators**.

The information displayed for each core is the IP address, whether it's a cloud or an on premise deployment, the version, and whether the core is running or disconnected.

Click in the **FUNCTIONALITY** column for a core to configure it as **Core only**, **JumpBox**, or **Both**:

- **Core only**: Provides basic core functionalities like event processing, communication control handling, and so on.
- **JumpBox**: Allows the core to connect to LDAP, FortiAnalyzer, and so on.
- **Both**: Enables both the Core only and JumpBox functions.

Depending on the number of events processed by the core, it may be suitable to have dedicated cores for Core only and JumpBox functionality.

The information displayed for each aggregator is the IP address, the number of connected collectors, the version, and whether the aggregator is running or disconnected.

Click on **REPOSITORIES** to see all the installed repositories. The information displayed for each repository is the IP address and whether the repository is running or disconnected.

Vouchers & Dumps are Available | WhatsApp +201224560923

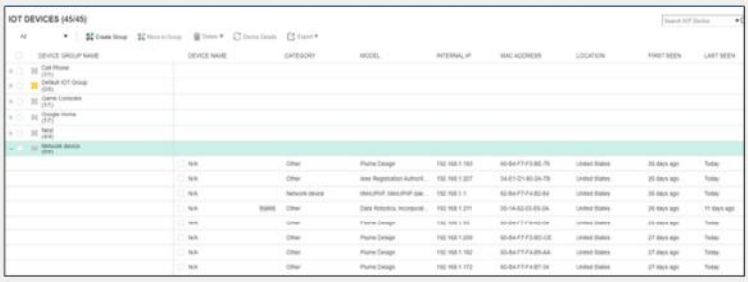
DO NOT REPRINT Brave-dumps.com
© FORTINET

Managing IoT Devices

- Detecting IoT devices
  - Scan for devices
  - Enable ongoing device discovery
  - Perform ad hoc scans as needed
- Viewing IoT devices
  - Displays device name, category, model, IP address, MAC address, location, and first and last seen dates
  - Devices discovered within the last three days are marked as **New**
  - Devices not seen in the last week are marked as **Expired**
- Organizing IoT devices
  - Optionally auto-group devices by type
  - You can manually add groups and move devices as you would with collectors

ADMINISTRATION > TOOLS

INVENTORY > IoT Devices



NSE Training Institute

© Fortinet Inc. All Rights Reserved.

26

You can view IoT devices, like printers, smartphones, or media players, that are connected to your network. You can scan for devices on the **ADMINISTRATION** tab of the management console. Choose **TOOLS**, and you'll see **IOT DEVICE DISCOVERY** options. Select the **Perform ongoing device discovery** checkbox to enable continuous monitoring for IoT devices. FortiEDR uses the existing collectors in your network to probe for neighboring devices. You can exclude specific collector groups, if desired. You can also perform an ad hoc discovery if needed.

Discovered devices are listed in the **INVENTORY** tab under **IoT Devices**. For each device, you can see the device name, category (media device, mobile, and so on), model, internal IP address, MAC address, location, and first and last dates the device was seen. If a device was discovered in the past three days, it is marked as **New**, so you can quickly identify new devices that may need to be reviewed. Devices that have not been seen in the last week are marked as **Expired**.

You can enable automatic grouping by device type in the **IOT DEVICE DISCOVERY** area where you configure device scans. If you do not select this option, all devices go into the default group. You can also create new groups and move devices as needed.

Vouchers & Dumps are Available | WhatsApp +201224560923

DO NOT REPRINT
© FORTINET
Brave-dumps.com

Knowledge Check

1. Which state will a collector be in, if it is prevented from performing to its full capacity?
   A. Degraded
   ✓ B. Disconnected

2. What functionality does the core need to connect to LDAP servers?
   A. JumpBox
   ✓ B. Core only

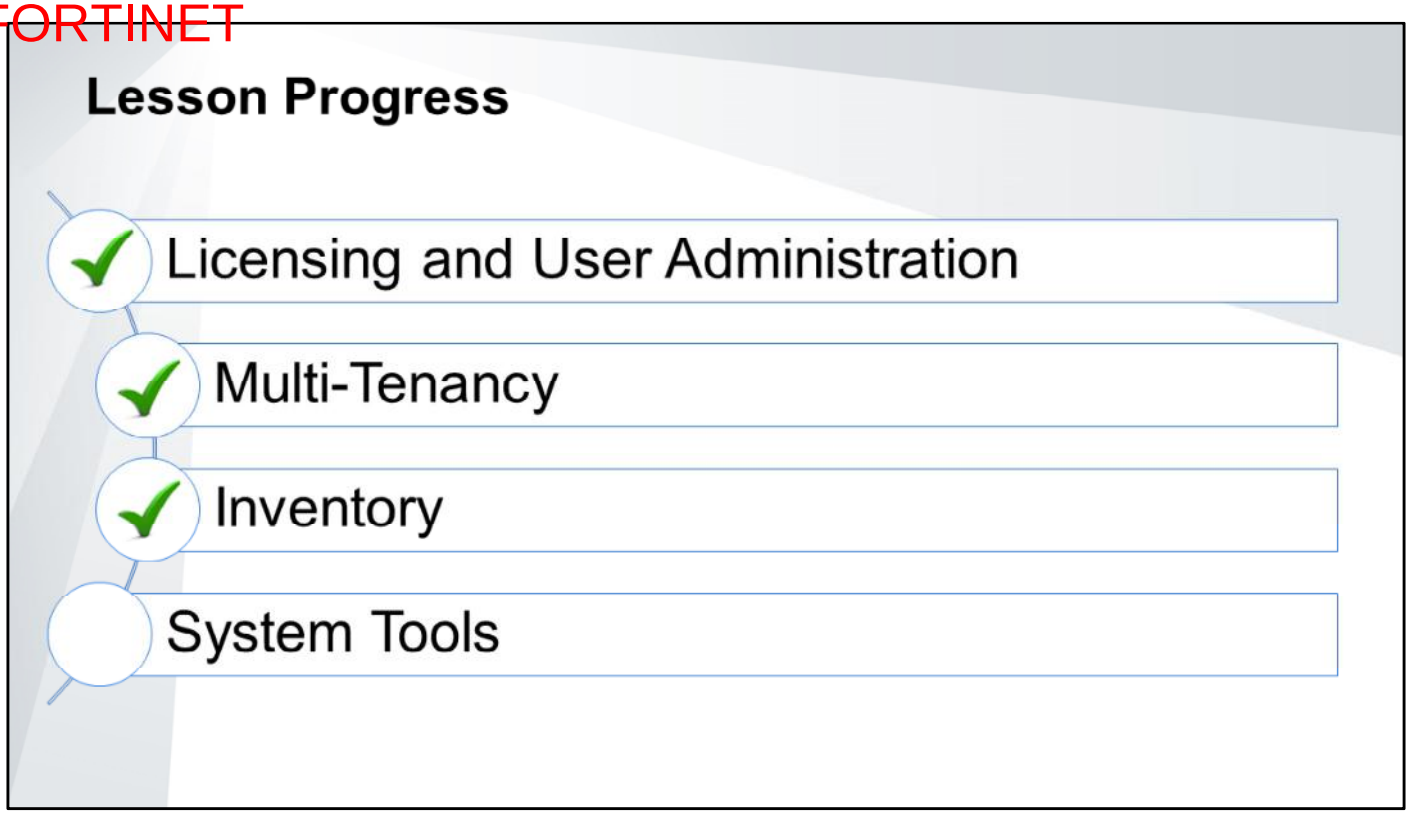
NSE Training Institute

© Fortinet Inc. All Rights Reserved.

27

Vouchers & Dumps are Available | WhatsApp +201224560923

DO NOT REPRINT
© FORTINET
Brave-dumps.com

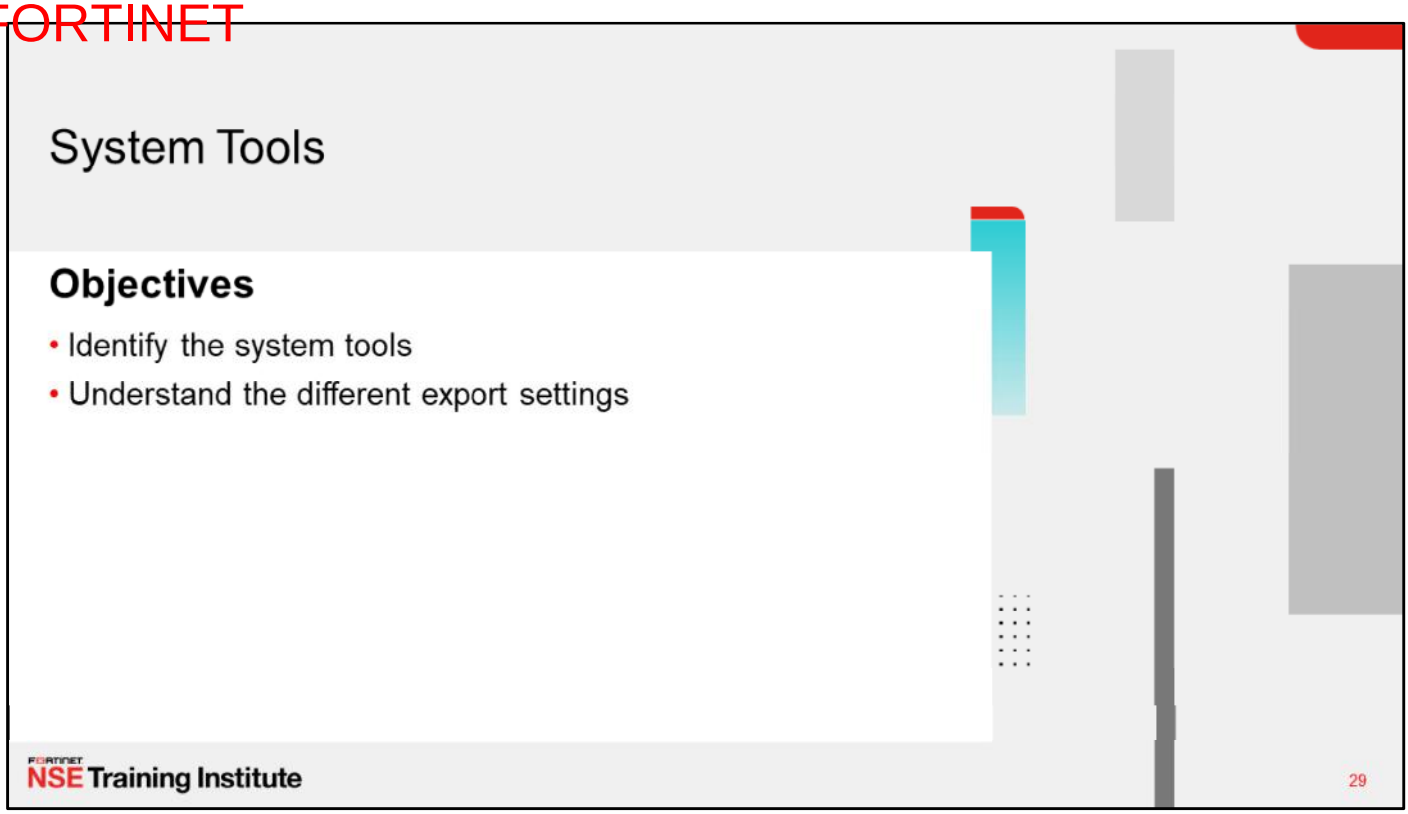


Good job! You now understand FortiEDR inventory.

Now, you will learn about system tools.

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.

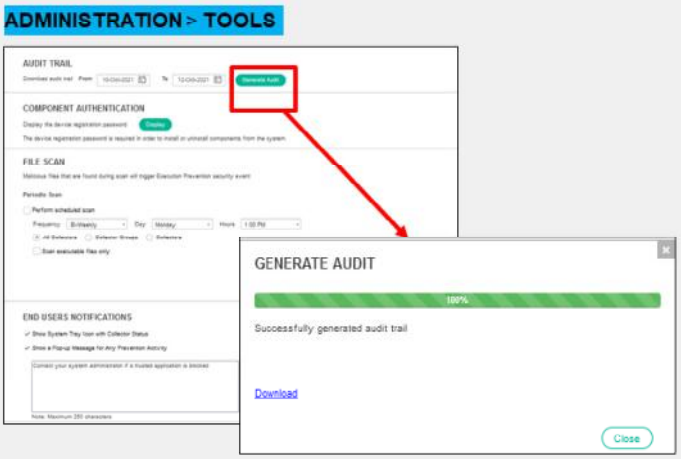
By demonstrating competence in FortiEDR system tools, you will be able to understand the configuration and integration of system tools.

Vouchers & Dumps are Available | WhatsApp +201224560923

DO NOT REPRINT Brave-dumps.com
© FORTINET

Generating an Audit Trail

- Get a record of every user action on the management console
  - Creates a CSV file listing the following for each user action:
    - Date: (yyyy-mm-dd hh:mm:ss)
    - Sub-system: (example: Configuration, Administration, Events, Inventory)
    - Username
    - Description



NSE Training Institute

© Fortinet Inc. All Rights Reserved.

30

You can generate an audit trail to keep track of user actions on the management console. Every user action in the management console is logged—user logins, changes to an event status, viewing events in Forensics, and so on. On the **ADMINISTRATION** tab, select **TOOLS** from the menu on the left and you'll see **AUDIT TRAIL**. Choose a date range and click **Generate Audit**. You can download a CSV file to your local machine showing the date, sub-system, user, and a description of each action. You can also send the audit trail to your SIEM solution through syslog.

Vouchers & Dumps are Available | WhatsApp +201224560923

DO NOT REPRINT Brave-dumps.com
© FORTINET

Component Authentication

- Device registration password
  - To install or uninstall a collector, you must supply the device registration password
  - This password is defined during initial system installation
  - The device registration password is the same for all collectors in the environment, or in the same organization in a multi-tenant environment
- Retrieving the registration password
  - In the console, click **ADMINISTRATION** > **TOOLS**
  - Click **Display** under **COMPONENT AUTHENTICATION**
  - A pop-up window opens showing the retrieved password

NSE Training Institute

© Fortinet Inc. All Rights Reserved.

31

The registration password is used to authenticate components of your FortiEDR installation. If you're in a mixed environment, perhaps a university, and you've bought 500 licenses to protect a specific group of users, you don't want unauthorized users registering. You can protect the installation with a password that only legitimate users would know and have access to the self-installer.

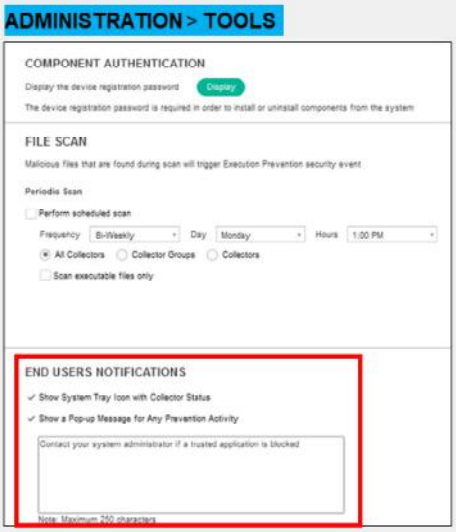
When you install and configure the central manager for the first time, you define an authentication password. You use that password to authenticate other components in your network. Each collector that registers in your FortiEDR network must provide the authentication password during installation. If the password is entered incorrectly, the collector does not register, and the device is not protected. You also need to provide the device registration password to disable or uninstall a collector. You can find this password in the **ADMINISTRATION** tab, under **TOOLS**. In the **COMPONENT AUTHENTICATION** section, click **Display** to see the registration password. Remember that the registration password is case sensitive. You can copy the password and paste it into any other window you need.

Vouchers & Dumps are Available | WhatsApp +201224560923

DO NOT REPRINT Brave-dumps.com
© FORTINET

Configuring End-User Notifications

- Configure what information users receive about the collector status and activity
- Select the checkboxes to enable options:
  - System tray icon with collector status:
    - Protection on
    - Protection off
    - Degraded
    - Isolation mode
  - Pop-up message for prevention activities
- Customize pop-up notifications
  - Example: If a trusted application has been blocked, contact the help desk at help@example.com
- User notifications are configured globally
  - For multi-tenant installations, user notifications are configured for each organization



NSE Training Institute
© Fortinet Inc. All Rights Reserved.

FortiEDR allows you to customize the information your end users receive about the collector and its activities. You can configure these settings on the **TOOLS** panel of the **ADMINISTRATION** tab .

You can enable system tray icons, which show the current status of the collector—protection on, protection off, degraded, or isolation mode. These icons may be helpful for troubleshooting purposes.

You can also show the user a pop-up notification that appears when a process has been blocked by the FortiEDR security policies. You can customize the text shown in the notification. For example, some customers may choose to include information about how to contact the help desk.

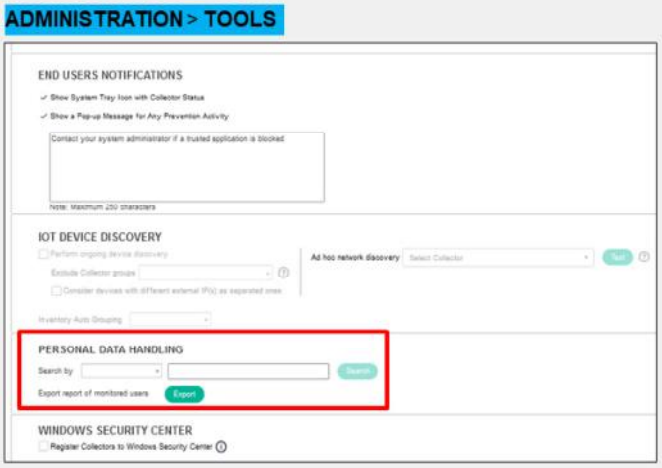
If you are running a multi-tenancy environment, note that user notifications are configured for each organization.

Vouchers & Dumps are Available | WhatsApp +201224560923

DO NOT REPRINT Brave-dumps.com
© FORTINET

Personal Data Handling

- Find, report, and delete personal data for any user
  - GDPR compliant
  - Search for data by:
    - Device name
    - IP address
    - MAC address
    - Username
  - To fully delete all data for an individual user, search for data related to each of the above criteria:
    - Deleting data for a username, for example, does not necessarily remove all data associated with that user's IP address, MAC address, or device name
  - **Note**: To comply with GDPR, personal data deletion is not included in the audit logs



NSE Training Institute

© Fortinet Inc. All Rights Reserved.

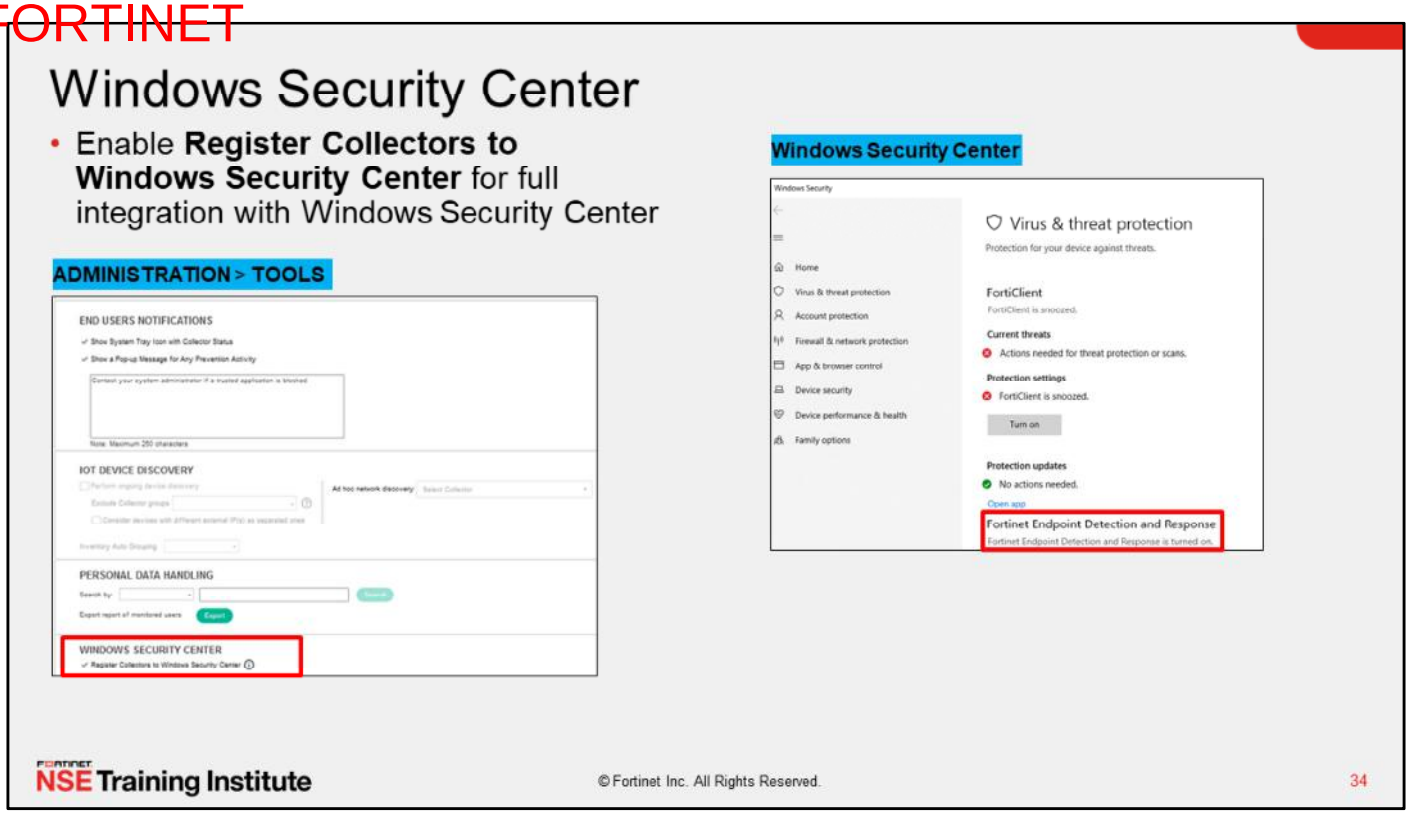
33

Administrators can find and delete personal data for any user on the **TOOLS** panel of the **ADMINISTRATION** tab under **PERSONAL DATA HANDLING**. To find all of a specific user's data, search by device name, IP address, MAC address, and username, and delete the results for each search. Data may be associated with the user's IP address, for example, that did not come up in a search for the username. So to be fully general data protection regulation (GDPR) compliant, you must search for all addresses and names associated with the user.

To comply with GDPR, no record can be kept of personal data, including its removal, if the user requests that their data be deleted. As a result, if an administrator deletes a user's data, the audit trail does not retain a record of that action.

Vouchers & Dumps are Available | WhatsApp +201224560923

DO NOT REPRINT Brave-dumps.com
© FORTINET



Microsoft has certified FortiEDR as an antivirus and threat protection application, it can be fully integrated with Windows Security Center. You can enable windows security center registration for collectors the in **TOOLS** panel of the **ADMINISTRATION** tab under **WINDOWS SECURITY CENTER**. After the collector has successfully registered with Windows Security Center, FortiEDR is listed as an antivirus and threat protection application. Your system is still fully protected even if you choose not register FortiEDR with Windows Security Center.

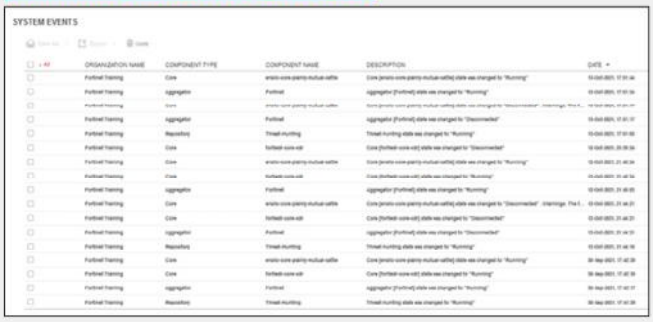
Vouchers & Dumps are Available | WhatsApp +201224560923

DO NOT REPRINT Brave-dumps.com
© FORTINET

System Events

- Track events affecting the protection of user devices
  - Security issues logged
  - Core is down/restored
  - Aggregator is down/restored
  - Collector protection is OFF (state changed to degraded/disabled)/restored
  - License issues logged:
  - License expiration (21/7/0 days until the expiration date)
  - License capacity (90%/95%/100% of license capacity consumed)
  - New collector added to the system
- Manage system events
  - Events trigger real-time notifications through configured email or syslog
  - Export events to Excel or PDF

ADMINISTRATION > SYSTEM EVENTS



NSE Training Institute

© Fortinet Inc. All Rights Reserved.

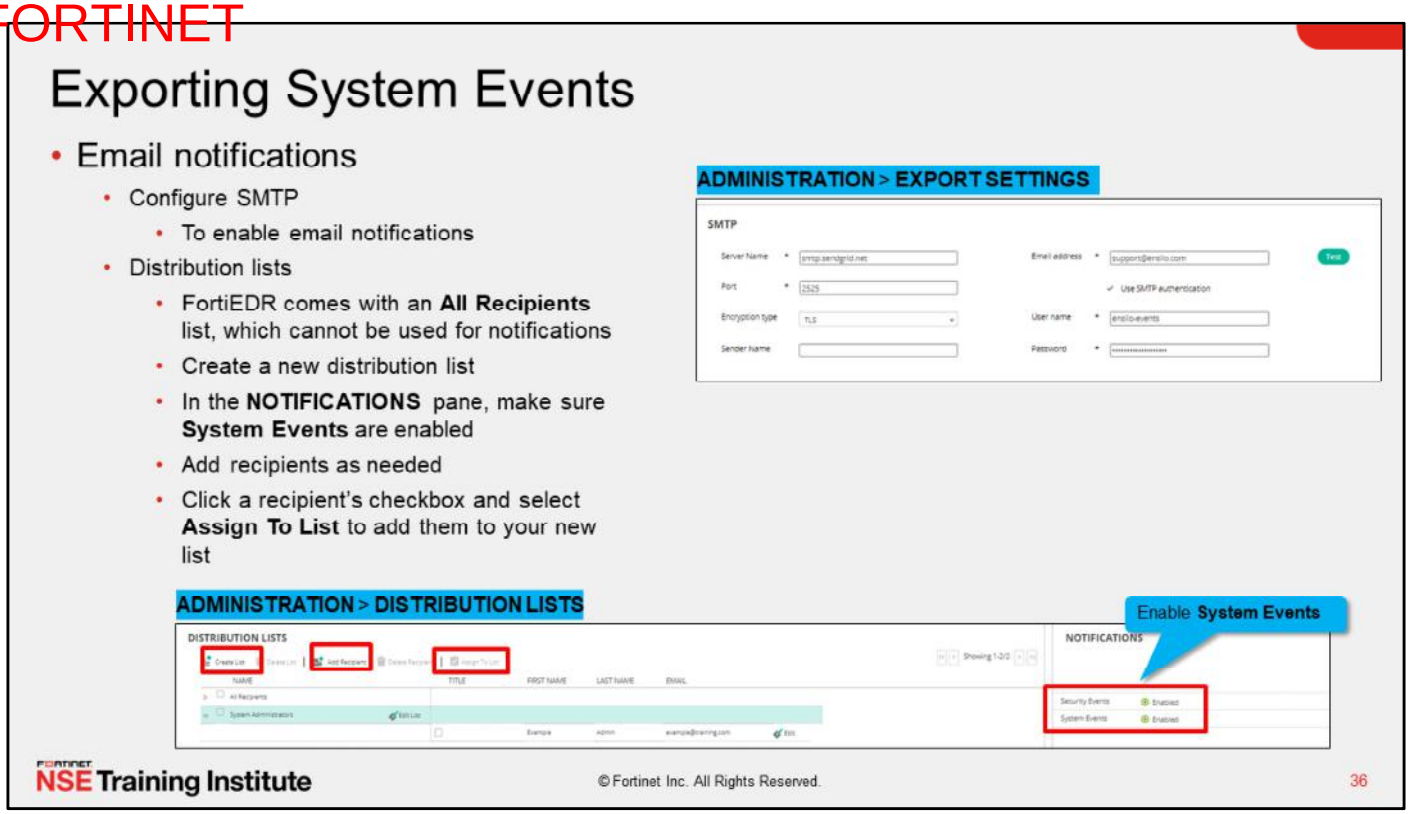
35

System events are events that affect the protection of user devices. Examples of system events include, when the core is down, the aggregator is down, or collectors are turned off or turned on. Adding a new collector generates a system event. Licensing issues are tracked as system events—for example, when a license is close to its expiration date (21, 7, or 0 days) or close to the license capacity.

It's very easy to manage system events. they trigger real-time notifications through any configured email or syslog output, or you can export the events to an Excel or PDF file.

Vouchers & Dumps are Available | WhatsApp +201224560923

DO NOT REPRINT Brave-dumps.com
© FORTINET



There are two ways to configure system event notifications. You can configure one or both. The first method is email notifications. To enable email notifications, click the **ADMINISTRATION** tab on the management console and click **EXPORT SETTINGS**. Enter standard SMTP settings to enable email notifications. Be careful with these—if you delete or accidentally alter them, all your email alerts will be disabled.

After you configure the SMTP settings, click **Distribution Lists** in the left-hand list to configure your email distribution list. Your FortiEDR installation comes preconfigured with an **All Recipients** list. You cannot configure notifications for this list, so you need to create a new list by clicking the **Create List** button. With your new list highlighted, check the **NOTIFICATIONS** area to the right. Make sure that **System Events** is enabled. You may choose to include **Security Events** as well—events that violated FortiEDR security policies—or set **Security Events** to **Disabled**, if you don't want to send them to this list. You will learn more about security event notifications in a later lesson.

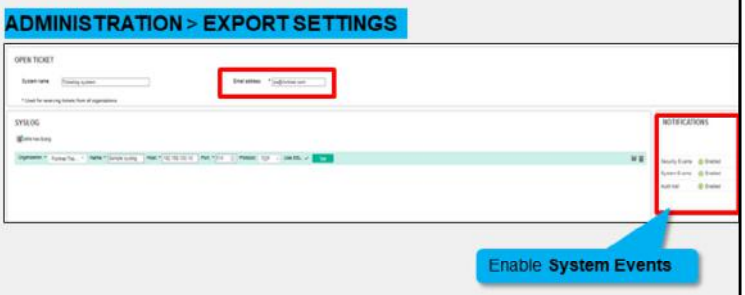
After you've set up your list, click **Add Recipient** and enter the first name, last name, and email for your first recipient. New recipients are added to the **All Recipients** list. Select the checkbox next to the recipient or recipients you want to include in your list and click **Assign to List** to add them to your custom list.

Vouchers & Dumps are Available | WhatsApp +201224560923

DO NOT REPRINT Brave-dumps.com
© FORTINET

Exporting System Events (Contd)

- Syslog notifications
  - Automatically send FortiEDR event data to specified Security Information and Event Management (SIEM) solutions through syslog
  - Click **Define New Syslog** to add a new syslog, if needed
    - Enter standard syslog parameters
    - Click **Test** to verify parameters
    - Click the **Save** button to the right:
  - With your syslog highlighted, check the **Notifications** area to the right
  - Make sure **System Events** are enabled
- Ticket notifications
  - Send events to event management tool
  - Enter **System name** and **Email address**, the destination where all tickets will be sent
    - Click the **Save** button to the right:



NSE Training Institute © Fortinet Inc. All Rights Reserved. 37

The second method is to send system event notifications through syslog. Configure syslog on the **ADMINISTRATION** tab of the management console under **EXPORT SETTINGS**. If your syslog parameters have not been added, click **Define New Syslog** and enter standard syslog parameters. You can send messages over TCP or UDP, choose port, and enable SSL. Use comma-delimited rather than name-value pairs. When you've entered your parameters, click **Test** to verify, then click **Save**. Highlight the syslog and check the **NOTIFICATIONS** pane on the right. Make sure **System Events** are enabled. You may also choose to include notifications about security events or the audit trail.

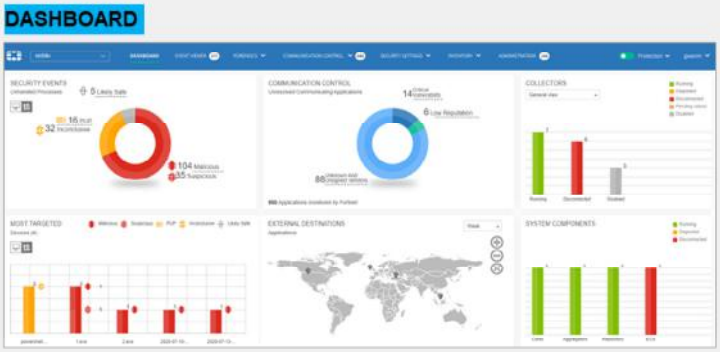
You can also send events to event management tools such as Jira or ServiceNow. You need to configure **System name** and an **Email address**, where all the events are sent to in the **Open Ticket** section. This feature automatically opens a ticket and attaches the relevant events to it. You must configure an email feed on the event management tool for this feature to work. You can find configuration examples in the *FortiEDR Installation and Administration* guide.

Vouchers & Dumps are Available | WhatsApp +201224560923

DO NOT REPRINT Brave-dumps.com
© FORTINET

Dashboard Overview

- Charts
  - SECURITY EVENTS
  - COMMUNICATION CONTROL
  - MOST TARGETED
  - EXTERNAL DESTINATIONS
  - Health charts
    - COLLECTORS
    - SYSTEM COMPONENTS



NSE Training Institute

© Fortinet Inc. All Rights Reserved.

38

This slide shows the dashboard you'll see every time you start a new session. It has charts that give you a quick view of your system status, including: unhandled security events and communicating applications, the most-targeted-devices or most common malicious processes, and the health and status of all your system components. You'll also see a map showing the location of any IP addresses that were involved in security events—the addresses the processes tried to connect to.

Vouchers & Dumps are Available | WhatsApp +201224560923

DO NOT REPRINT
© FORTINET
Brave-dumps.com

Knowledge Check

1. Where is every user action in the management console logged?
   - ✓ A. Audit trail
   - B. System event

2. In the tools pane, where can an administrator retrieve the device registration password?
   - A. Personal Data Handling
   - ✓ B. Component Authentication

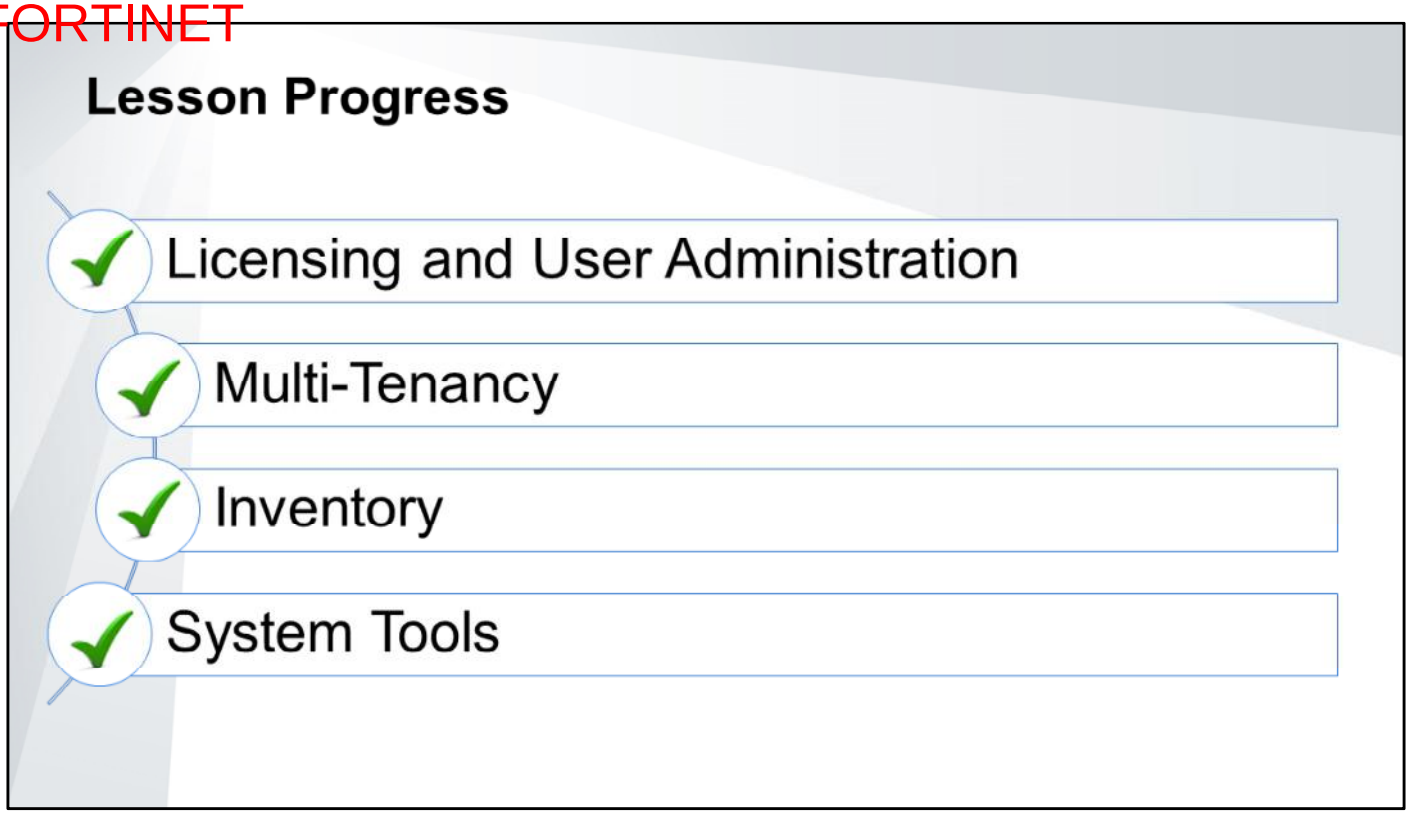
NSE Training Institute

© Fortinet Inc. All Rights Reserved.

39

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

Review

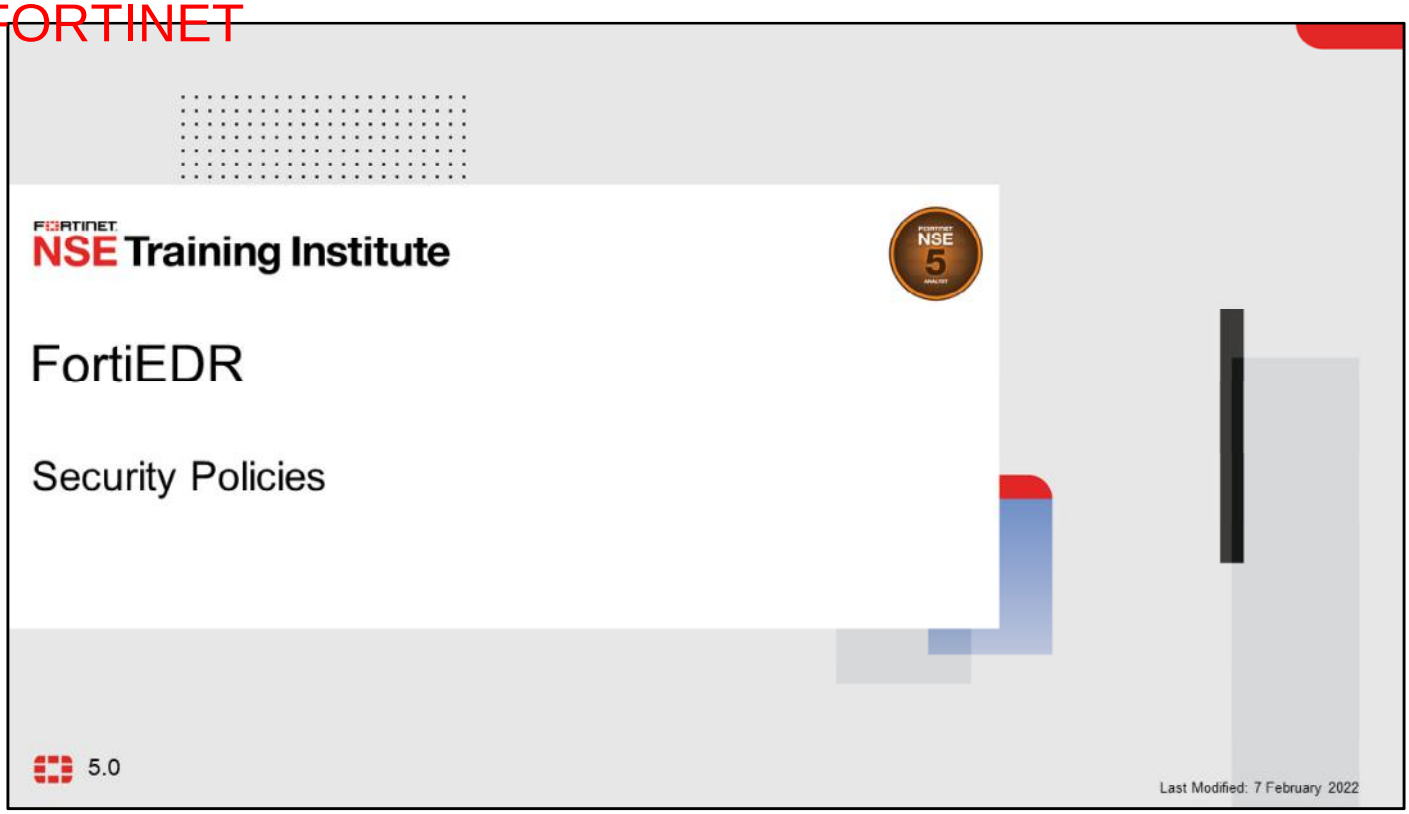
- ✓Understand the license types and seats
- ✓Configure Administrator accounts
- ✓Set up two-factor authentication for users
- ✓Understand why you need multi-tenancy
- ✓Identify user permissions
- ✓Understand how to migrate organizations
- ✓Identify collector states and updates
- ✓Manage system components
- ✓Understand IoT discovery and grouping
- ✓Identify the system tools
- ✓Understand the different export settings

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

By mastering the objectives covered in this lesson, you learned how to administer FortiEDR management console, configure multi-tenancy, and identify system tools.

Vouchers & Dumps are Available | WhatsApp +201224560923

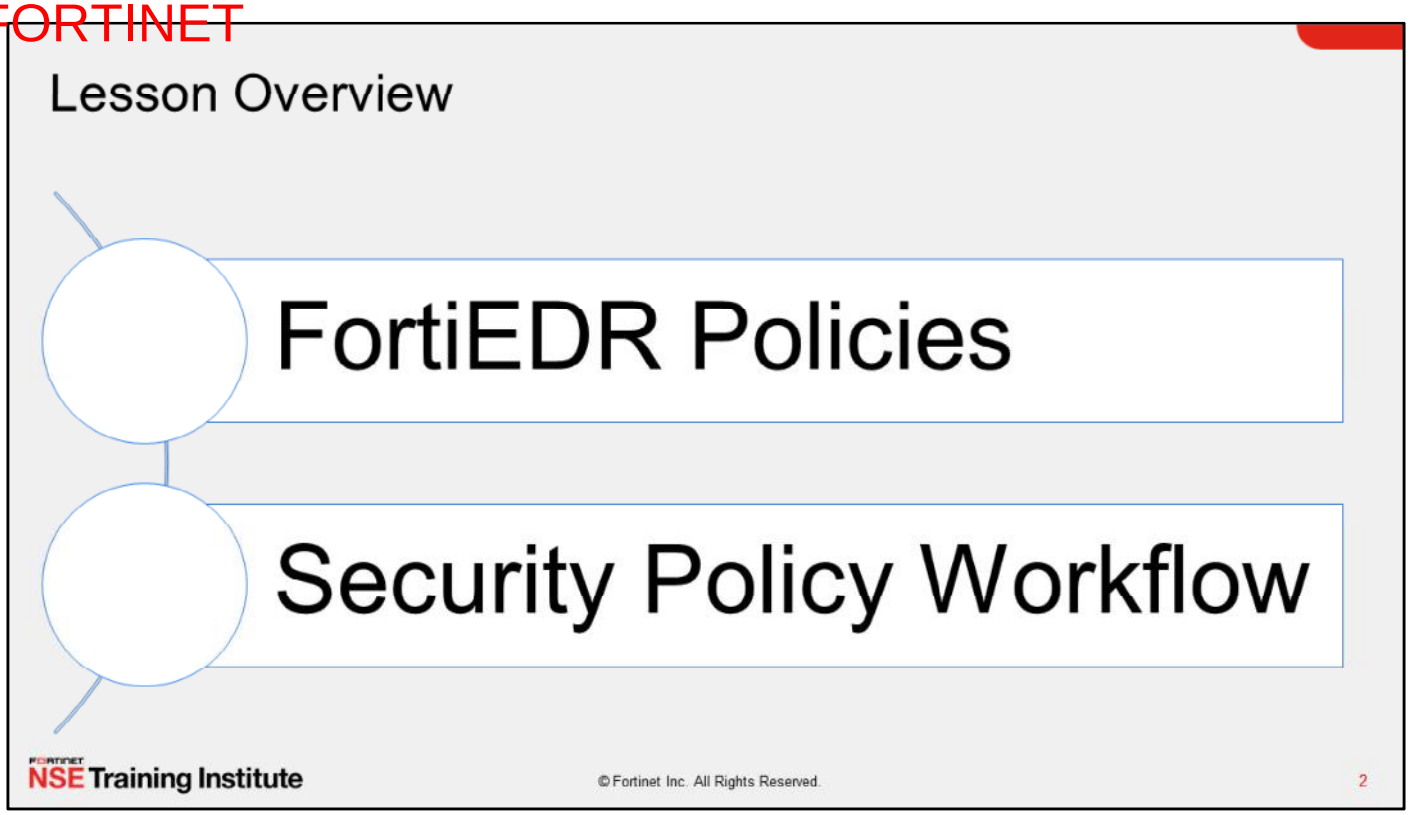
DO NOT REPRINT
© FORTINET
Brave-dumps.com



In this lesson, you will learn about security policies in a FortiEDR deployment.

Vouchers & Dumps are Available | WhatsApp +201224560923

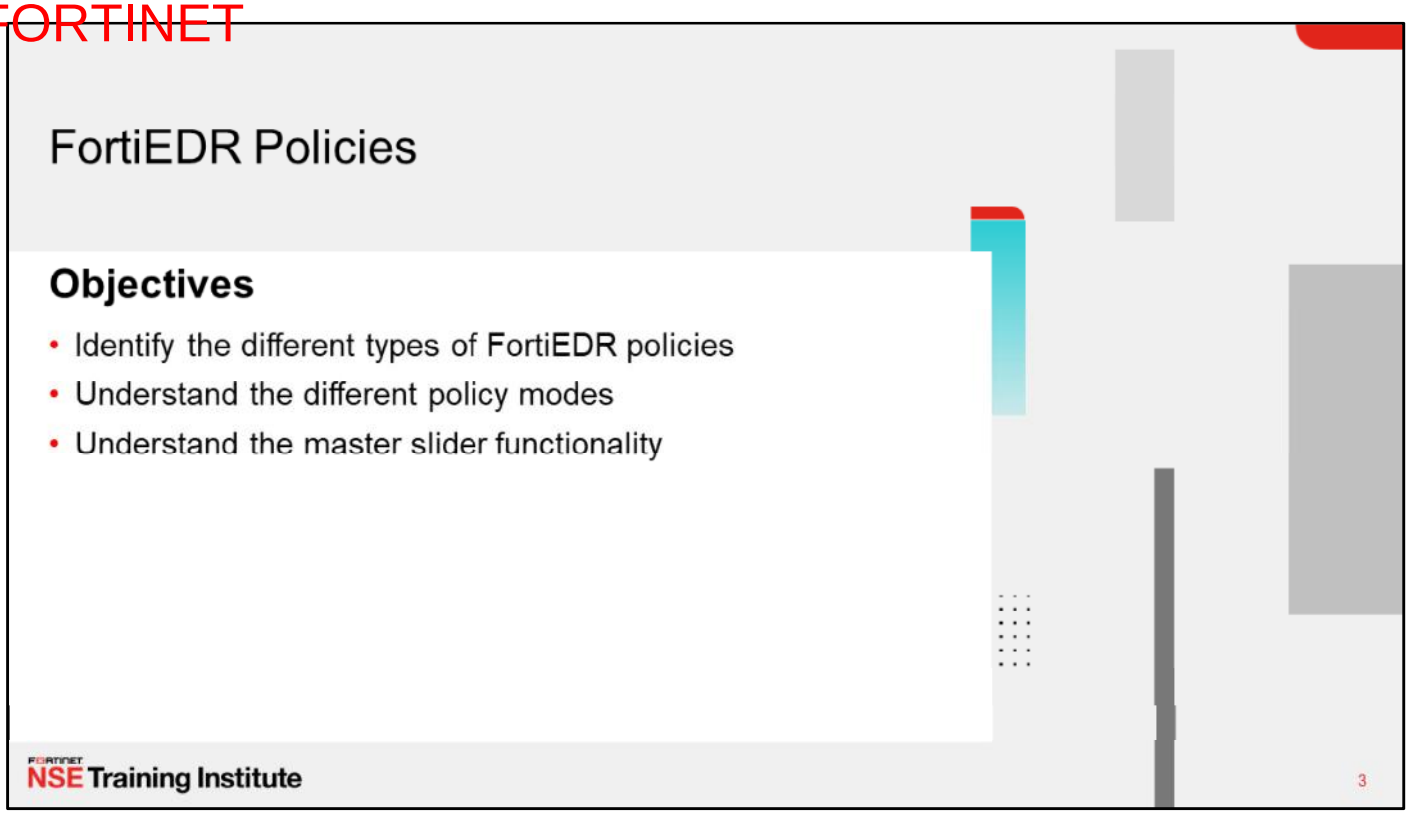
DO NOT REPRINT Brave-dumps.com
© FORTINET



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

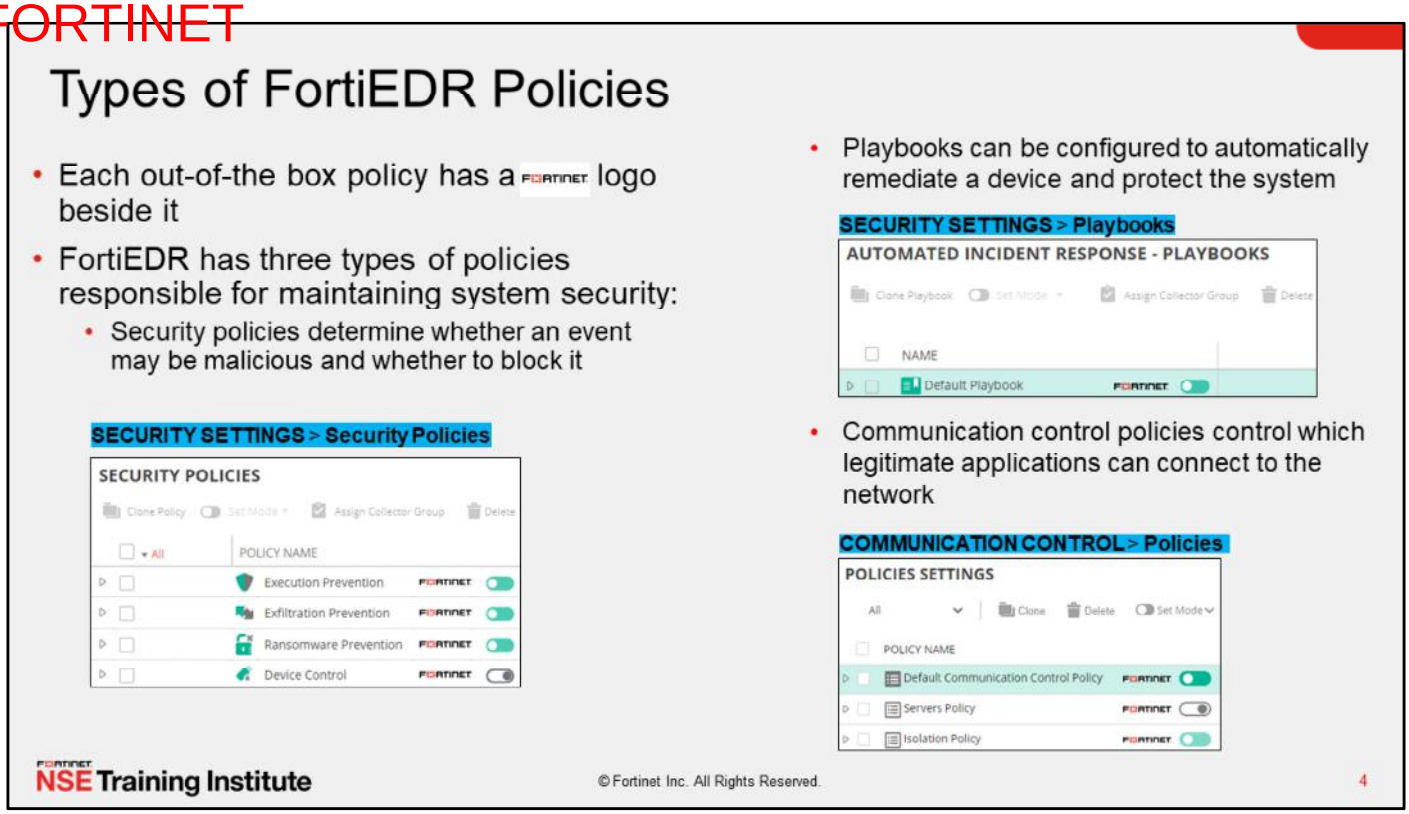


After completing this lesson, you should be able to achieve the objectives shown on this slide.

By demonstrating competence in FortiEDR policies, you will understand the different types and modes of policies.

Vouchers & Dumps are Available | WhatsApp +201224560923

DO NOT REPRINT Brave-dumps.com
© FORTINET



FortiEDR has three types of policies that work together to maintain your system's security. The most important type of policies are security policies. These policies determine whether a process is malicious or not. Next are playbooks, or automated incident response. If FortiEDR catches a potentially malicious process, you can use playbooks to automatically remediate the device and protect the rest of your network. Lastly are communication control policies. These policies apply to programs that are not malicious, but may be insecure or banned by company policy. Communication control policies decide which applications are allowed to communicate through the network and which are blocked.

Vouchers & Dumps are Available | WhatsApp +201224560923

DO NOT REPRINT Brave-dumps.com
© FORTINET

Collector Groups and Policies

- **What are collector groups?**
  - Collectors are organized into groups
  - Groups can reflect organizational groups, geographies, or roles
- **Assigning groups to policies**
  - Policies are assigned at the collector group level
  - Each group should be assigned to one of each of the following policies:
    - Execution Prevention
    - Ransomware Prevention
    - Exfiltration Prevention
    - Device Control and Extended Detection (if needed)
    - Playbook
    - Communication Control
  - Multiple groups may be assigned to one policy

NSE Training Institute © Fortinet Inc. All Rights Reserved. 5

Now you will learn more about how to organize collectors. Each collector belongs to one collector group. You can create customized collector groups organized by work group, role, geography, or any other criteria that makes sense for your organization.

Policies are assigned at the collector group level. For full protection, each group should be assigned to one of each of the following policies: Execution Prevention, Ransomware Prevention, Exfiltration Prevention, Communication Control, and playbook. If you are using Device Control and Extended Detection in your organization, you should also assign a device control and extended detection policy.

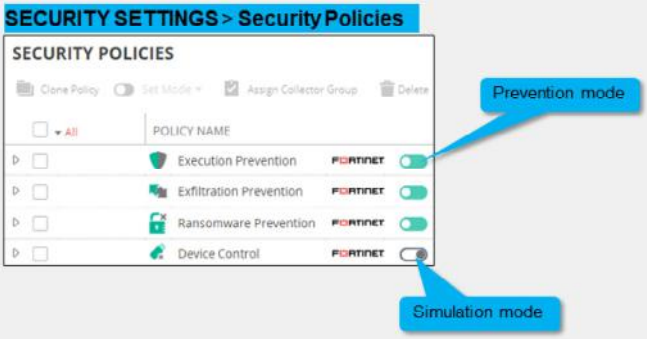
You can assign many groups to a single policy.

Vouchers & Dumps are Available | WhatsApp +201224560923

DO NOT REPRINT Brave-dumps.com
© FORTINET

Simulation vs. Prevention Mode

- Prevention: Policies enforced
  - A green mode slider indicates the policy is in prevention mode
  - Security policies: Any events that violate the policy rules are automatically blocked
  - Communication control policies: Any applications set to **Deny** are blocked from communicating
  - Playbooks: All actions are carried out as configured
- Simulation: Notification only
  - A white and gray mode slider indicates a policy in simulation mode
  - Security policies: FortiEDR issues an alert for events that violate a policy rule, but does not block them
  - Communication control policies: Rules are not enforced
  - Playbooks: Notifications are sent, but no other actions are carried out
  - FortiEDR comes out of the box set to this mode
- Simulation vs. prevention applies per policy
  - Each individual policy can be set to either prevention or simulation mode



NSE Training Institute

© Fortinet Inc. All Rights Reserved.

6

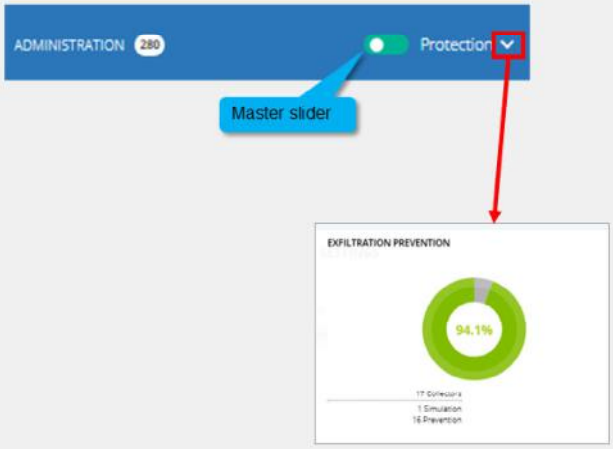
FortiEDR policies can operate in one of two modes: prevention, or blocking mode, and simulation, or logging mode. When operating in prevention mode, FortiEDR actively enforces the policy. In most cases, the event is blocked in real time, preventing harm to the device or system. If the event is suspicious, but could possibly be legitimate, FortiEDR logs it for review. When operating in simulation mode, FortiEDR issues an alert, but does not block any processes. Since each policy is set to simulation or prevention mode separately, you can enforce some policies while others are in simulation mode.

Vouchers & Dumps are Available | WhatsApp +201224560923

DO NOT REPRINT Brave-dumps.com
© FORTINET

The Master Slider

- For emergency use only
  - Resets all policies to simulation mode
  - Affects playbooks and communication control policies as well as security policies
- Master slider state and collector protection
  - When the master slider is in protection mode, it does not mean that all of the collectors are protected, only that they may be
  - Click the arrow to the right of the slider to see charts illustrating how many collectors are in protection mode for each policy
  - When the master slider is in simulation mode, no collectors are being actively protected
- Best practice is to move collectors into a simulation mode group
  - Move individual collectors into a simulation group for troubleshooting, and then move them back to their original group when finished
  - Does not affect protection of the other collectors in the group



NSE Training Institute

© Fortinet Inc. All Rights Reserved.

7

On the console, the slider in the upper-right corner of the window is the master slider for protection versus simulation mode. The master slider is intended for emergency use only, because setting the master slider to simulation mode places *all* policies into simulation mode.

Note that when the slider says **Protection**, like it does in the example shown on this slide, it does not mean that every collector is assigned to a policy in protection mode. Some collector groups may still be assigned to policies in simulation mode. Click the down arrow beside the master slider to see a breakdown of how many collectors are protected by each type of policy. For example, in the donut chart to the right, you can see that 94.1% of collectors are assigned to an Exfiltration Prevention policy in protection mode. The number will vary across policy types. When the master slider is set to **Simulation**, *all* policies are set to simulation mode and no collector groups are actively protected.

If you want to place a collector in simulation mode as part of troubleshooting, the best method is to move the individual collector into a designated simulation group, rather than disturb an entire group. After troubleshooting is complete, move the collector back into its original group.

Vouchers & Dumps are Available | WhatsApp +201224560923

DO NOT REPRINT
© FORTINET
Brave-dumps.com

Knowledge Check

1. Which FortiEDR policy can identify and block malicious events?
   - ✓ A. Security policy
   - B. Communication Control policy
2. In which mode does FortiEDR actively enforce the policy?
   - ✓ A. Prevention mode
   - B. Simulation mode

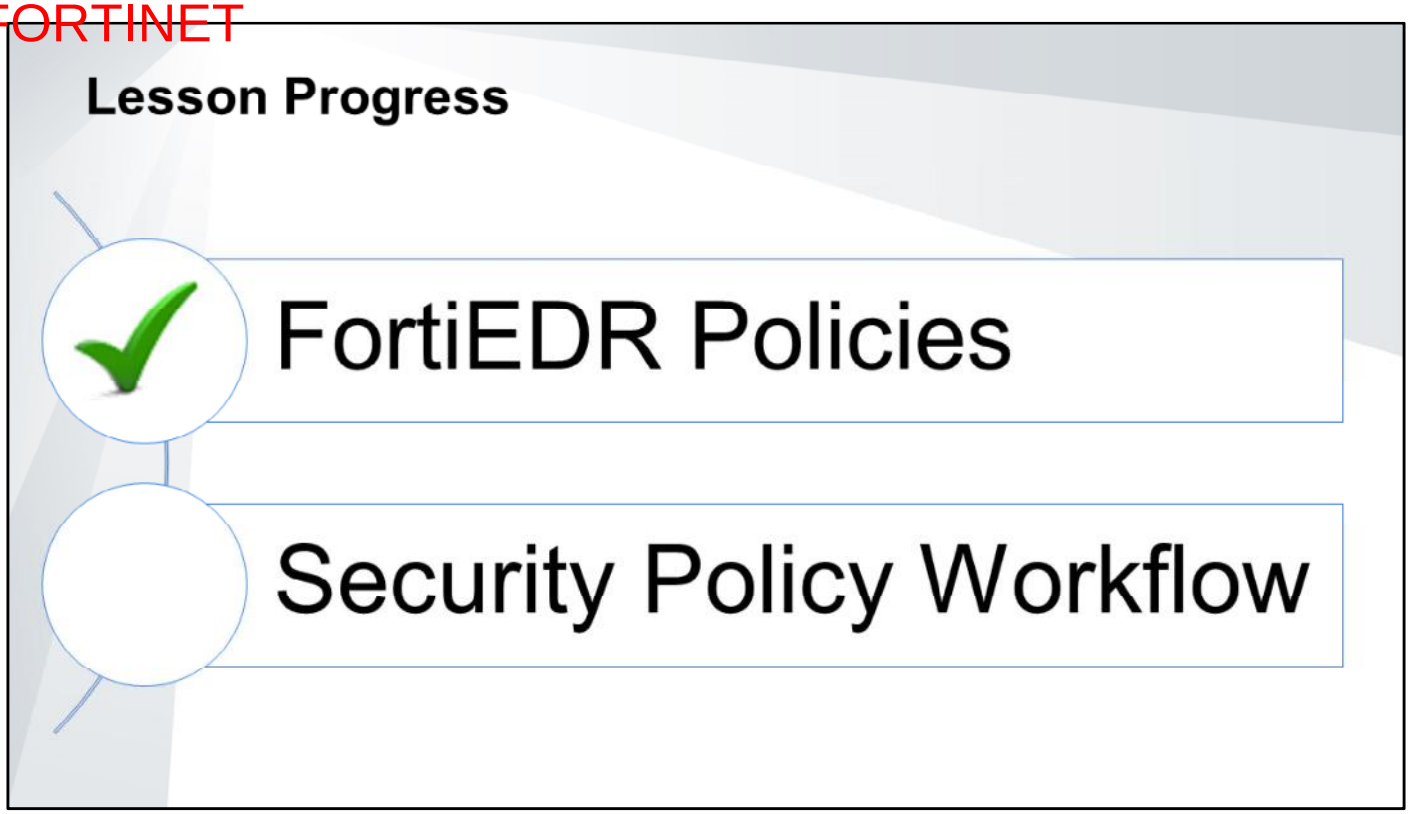
NSE Training Institute

© Fortinet Inc. All Rights Reserved.

8

Vouchers & Dumps are Available | WhatsApp +201224560923

DO NOT REPRINT
© FORTINET
Brave-dumps.com



Good job! You now understand the different FortiEDR policies and modes.

Now, you will learn about security policies.

Vouchers & Dumps are Available | WhatsApp +201224560923

DO NOT REPRINT Brave-dumps.com
© FORTINET

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

By demonstrating competence in security policies, you will understand how they work and how they can be configured.

Vouchers & Dumps are Available | WhatsApp +201224560923

DO NOT REPRINT Brave-dumps.com
© FORTINET

What is NGAV?

- Each file is checked against the NGAV engine:
  - When a file is saved, read, or executed on a device, the FortiEDR collector checks it against the NGAV engine
  - The file is given a score representing the NGAV engine's level of confidence that the file is malicious
  - Files with higher scores are more likely to be malicious—for example, a score above 90% indicates a high certainty that the file is malicious
  - The NGAV engine uses the confidence score to decide whether to allow the file, block it, or log it
- NGAV works online or offline
  - If the collector is in autonomous mode, the decision on how to handle the file is made at the collector level
- NGAV is the first line of defense
  - Pre-infection protection automatically blocks simple attacks
- NGAV is powered by machine learning
  - Our research team feeds millions of pre-classified samples of known good and bad files and real-world examples of malware into the machine
  - The machine generates an algorithm to recognize whether or not a file is likely to be safe
    - Compare this to signature-based systems, which can only load a small portion of the signatures at a time
- NGAV is continuously updated
  - The machine-generated algorithm is updated on an ongoing basis, allowing Fortinet to update the NGAV engine as needed
  - Updates to NGAV are made through the existing update process, regular content updates through the console

NSE Training Institute

© Fortinet Inc. All Rights Reserved.

11

What is NGAV? It's the first line of defense. Execution Prevention—the FortiEDR next-generation antivirus (NGAV) policy—picks up all the simple or known attacks and stops them before they execute.

The FortiEDR NGAV engine is powered by machine learning. Our research team feeds millions of pre-classified samples of good and bad files and real-world malware into the NGAV engine. It then generates an algorithm to determine whether or not a file is likely safe or malicious. In comparison, a signature-based system can load only a small number of the signatures at a time, and it can't detect malware it's never seen before.

Fortinet adds samples to the NGAV engine on an ongoing basis so that the algorithm stays up-to-date. You receive these updates through regular content updates, which you can upload to the console.

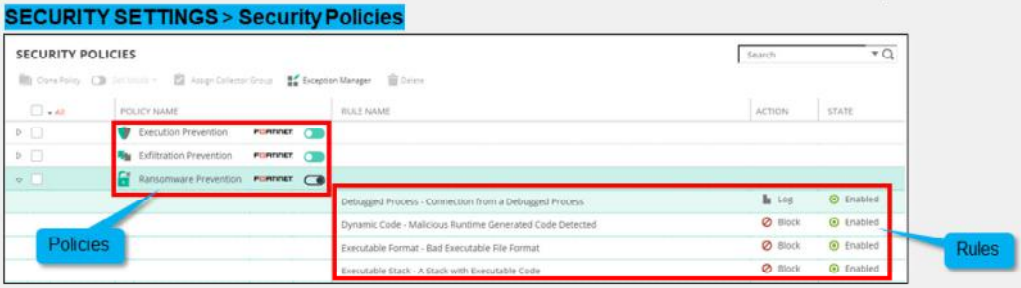
How does NGAV work? When a file is saved, read, or executed on a device, the collector checks it against the NGAV engine. FortiEDR examines the file in real time and assigns it a score based on the likelihood that the file is malicious. The higher the score, the more likely it is that the file is malicious. Any score above 90% indicates a high certainty that the file is malicious. Based on the assigned score, the NGAV engine decides whether to allow, block, or log the file. This process works whether or not the collector is online. When the collector is offline, it goes into autonomous mode, and it decides how to handle files independently.

Vouchers & Dumps are Available | WhatsApp +201224560923

DO NOT REPRINT Brave-dumps.com
© FORTINET

How Security Policies Work

- Policies
  - Collector groups are assigned to policies
  - Policies are set to prevention or simulation mode at the top level
  - Policies in simulation mode do not block malware
    - Use policies in simulation mode only for tuning or troubleshooting
- Rules
  - Each policy contains a set of rules, which are delivered out of the box
  - Rules are automatically assigned an action (log or block) based on their severity
    - You can change the assigned action of an individual rule if desired
  - Each rule can be individually enabled (default: recommended) or disabled



NSE Training Institute © Fortinet Inc. All Rights Reserved. 12

Now, you'll learn how security policies work. Security policies are at the heart of FortiEDR protection. You can configure your security policies in the management console—click the **SECURITY SETTINGS** tab and select **Security Policies**. Collector groups are assigned to policies, which are set to prevention or simulation mode at the top level. Remember, policies in simulation are not actively blocking malware. You'll see an event in the **EVENT VIEWER**, but no process will be blocked. Use policies in simulation mode only for initial tuning or troubleshooting purposes.

Each policy is made up of a set of rules, which are delivered out of the box. Rules are automatically assigned an action (**Log** or **Block**) based on their severity. Management console users can change the assigned action of an individual rule if desired. Each rule can also be individually enabled or disabled. By default, all rules in most policies are enabled, and Fortinet does not recommend disabling them. If you don't want to enforce a specific rule, it is better to set it to **Log**. That way, you have a record of the violation if a problem occurs, but the rule isn't enforced.

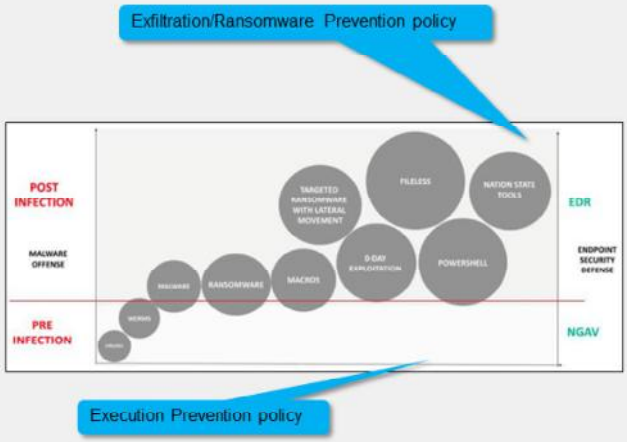
Vouchers & Dumps are Available | WhatsApp +201224560923

DO NOT REPRINT Brave-dumps.com
© FORTINET

Security Policies

FortiEDR provides the following out-of-the-box security policies:

- **Execution Prevention** (NGAV policy): Prevents suspicious files from executing
- **Exfiltration Prevention**: Prevents malicious actors from stealing data
- **Ransomware Prevention**: Prevents malicious actors from encrypting data
- **Device Control**: Detects and blocks use of specific classes of USB devices such as mass storage devices
- **Extended Detection**: Detects malicious activities across the network and operates only in simulation mode



NSE Training Institute

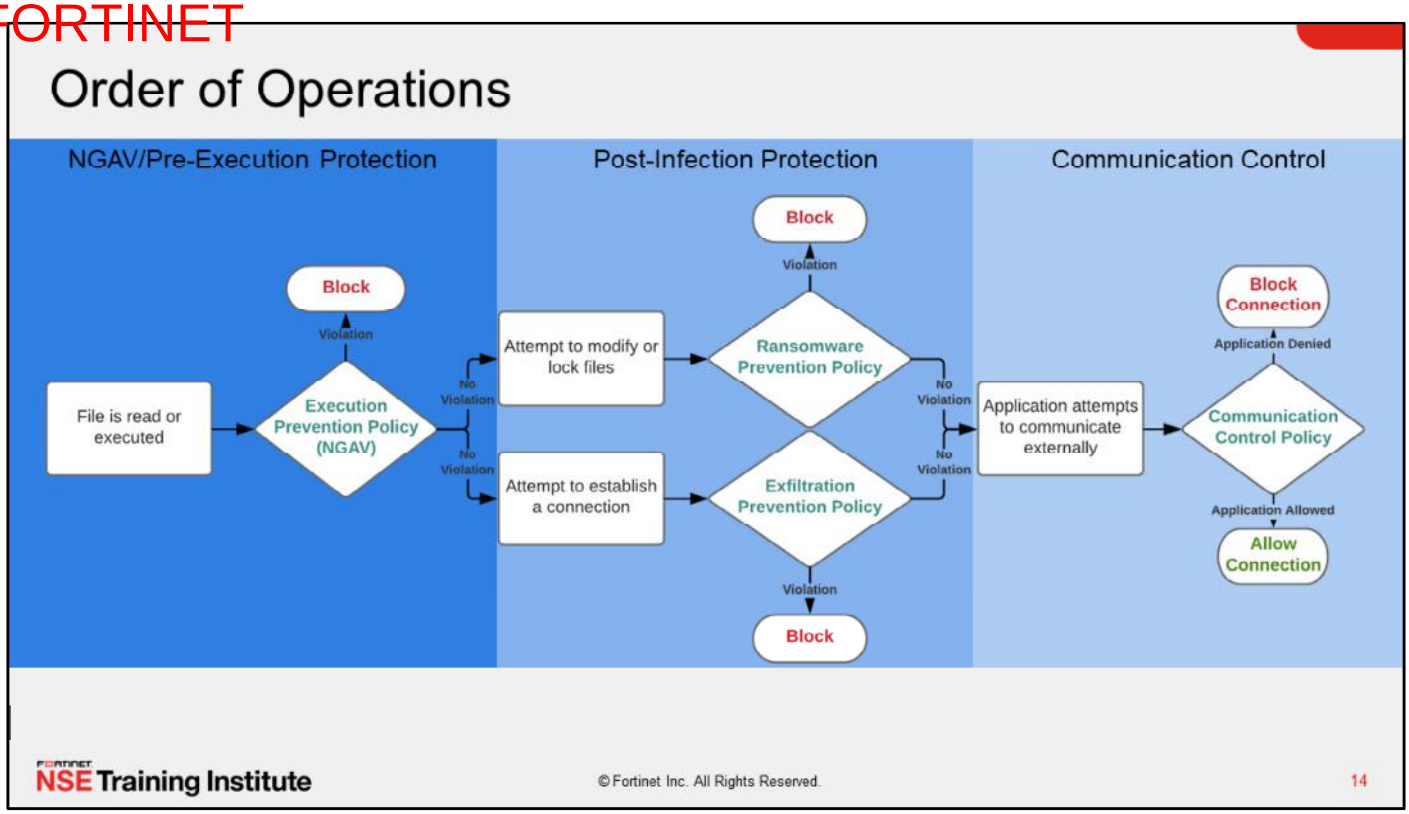
© Fortinet Inc. All Rights Reserved.

13

Now you will learn about security policies. FortiEDR comes out of the box with five security policies, each with its own purpose. Execution Prevention, or next-generation antivirus, stops malicious files from executing. This policy catches simple or known attacks before they start. If the attack manages to bypass execution prevention, two other policies that detect suspicious behavior and stop it before it can inflict harm. Exfiltration Prevention stops malicious actors from connecting to the network and stealing data, while Ransomware Prevention prevents malicious actors from encrypting your data. You can also enable Device Control, which detects and blocks the use of specific classes of USB devices, such as mass storage devices. You don't have to block mass storage devices, but it's a really helpful feature in environments with very sensitive data. Starting with FortiEDR version 5.0, Extended Detection policy has been added to the predefined policy list. Extended Detection policies work only in simulation mode, meaning it will not block any activity. They will correlate data from multiple security systems and identify any malicious activities. You will learn more about Extended Detection later in the course.

Vouchers & Dumps are Available | WhatsApp +201224560923

DO NOT REPRINT Brave-dumps.com
© FORTINET



Here's another way to look at the order of operations. Again, the Execution Prevention policy is the first line of defense. If there's a violation, the file is blocked. If it gets through, post-infection protection kicks in. The Ransomware Prevention policy watches for any attempts to lock or modify files, and the Exfiltration Prevention policy watches for attempts to establish a connection. If either one of these policies detects a violation, the process is blocked. If no security policy rules are violated, the file is checked by the Communication Control policy when it attempts to connect to the network. As we discussed in earlier lessons, Communication Control policy manages programs that aren't malicious, but may be undesirable or insecure. If a file gets through to the communication control engine, we've already determined that it's not actually malware.

Vouchers & Dumps are Available | WhatsApp +201224560923

DO NOT REPRINT Brave-dumps.com
© FORTINET

Device Control Policies

- What is device control?
  - High-security organizations or departments may need to block devices because of industry regulations
  - Choose specific classes of USB devices to block
  - Examples:
    - Mass storage devices
    - USB hubs
    - CDC-data devices
    - Application-specific devices
- Enabling device control
  - Set Device Control policy to prevention mode
  - Click the state icon (set to **Disabled** by default) to toggle the state to **Enabled**
  - If your organization does not need to restrict USB devices, leave the Device Control policy in simulation mode and the rules in a disabled state

NSE Training Institute

© Fortinet Inc. All Rights Reserved.

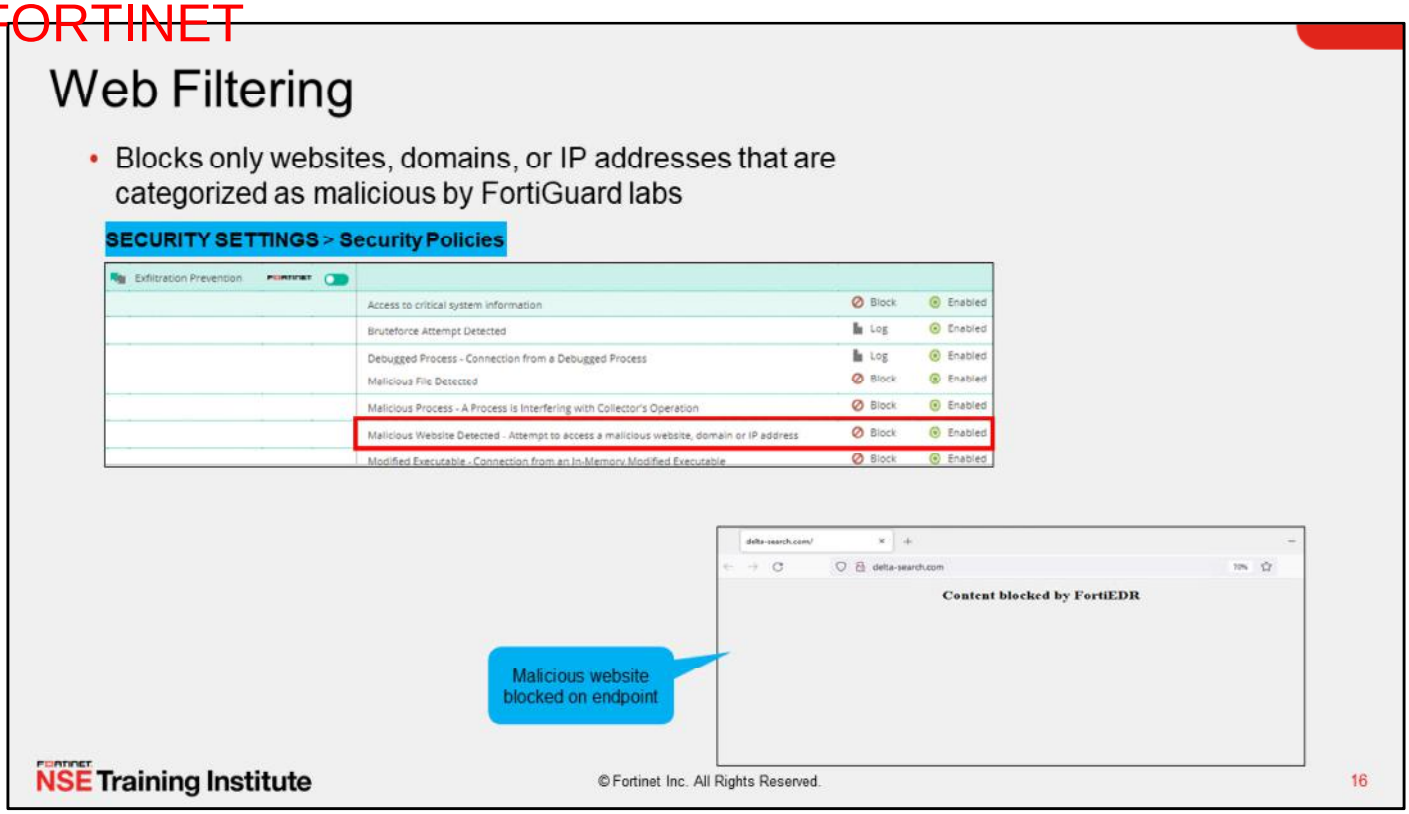
15

Device Control policies work a little differently than the other security policies. Some organizations in a high-security field, like health care, need to restrict USB devices because of industry regulations. Device Control policies allows you to block specific classes of USB devices, such as mass storage devices, USB hubs, CDC-data devices, or application-specific devices.

In Device Control, all rules are disabled by default. Find the rule for each device class you want to block and click the state icon to toggle the state to **Enabled**. If your organization does not need to restrict USB devices, you can leave the Device Control policy in simulation mode and the rules disabled. No device will be blocked, and no notifications are generated for USB devices unless they are infected and violate rules in a different security policy.

Vouchers & Dumps are Available | WhatsApp +201224560923

DO NOT REPRINT Brave-dumps.com
© FORTINET



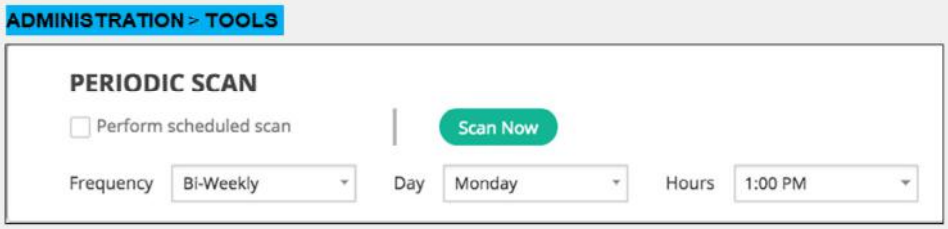
Starting with FortiEDR 5.0, you can apply a web filtering rule in the Exfiltration Prevention policy. A website, domain, or IP address that has been identified as malicious by FortiGuard labs, can be blocked using this policy. You can enable this rule in your Exfiltration Prevention policy—click the **SECURITY SETTINGS** tab and select **Security Policies**. Expand the **Exfiltration Prevention** policy and change the state of the rule **Malicious Website Detected - Attempt to access a malicious website, domain or IP address** to **Enabled.** Then change the action of that rule to **Block.** When an endpoint monitored by the FortiEDR collector, tries to access a website, in a malicious category it is blocked.

Vouchers & Dumps are Available | WhatsApp +201224560923

DO NOT REPRINT Brave-dumps.com
© FORTINET

Scheduled Device Scans

- Schedule full disc scans of all devices
  - Search and destroy—find and remediate dormant threats before they attempt to execute
  - Perform scans whenever needed by clicking **Scan Now**
  - Schedule periodic scans at your preferred time and frequency
  - File scans occur in the background and consume a small amount of resources from the device



NSE Training Institute

© Fortinet Inc. All Rights Reserved.

17

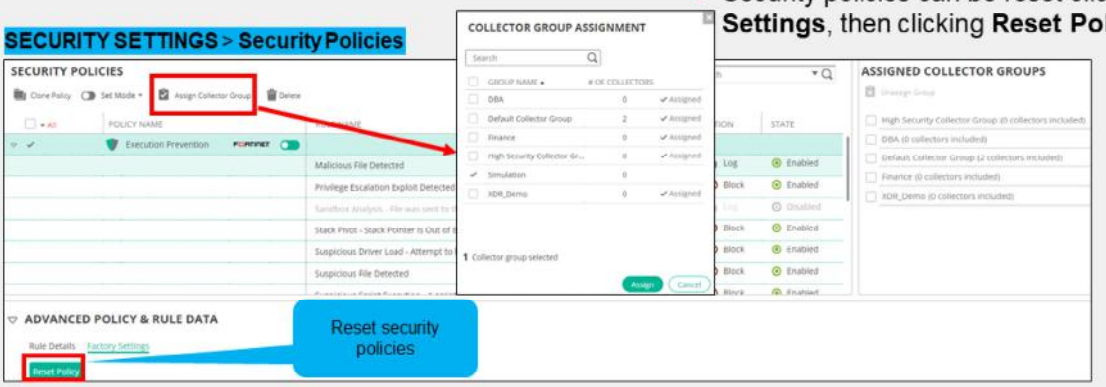
One of the requirements for antivirus replacement certification is to allow users to schedule periodic scans of all their devices so they can find and remediate dormant threats. Remember, your computers are constantly being monitored by the collector, so you don't actually need to schedule scans, but if you want to, the functionality is available in the **ADMINISTRATION** tab of the management console, under **TOOLS**. You can select your preferred time and frequency, and the files are scanned in the background. The scan uses a small amount of resources on the device.

Vouchers & Dumps are Available | WhatsApp +201224560923

DO NOT REPRINT Brave-dumps.com
© FORTINET

Security Policy Assignment

- Collector groups are assigned to policies
  - The **Assigned Collector Groups** pane shows the collector groups that are assigned to the highlighted policy
  - Click **Assign Collector Group** to add collectors to the selected policy
- Remember that each collector group should be assigned to one Execution Prevention, one Exfiltration Prevention, and one Ransomware Prevention policy
- Device Control and Extended Detection policies are optional
- Security policies can be reset clicking **Factory Settings**, then clicking **Reset Policy**



NSE Training Institute © Fortinet Inc. All Rights Reserved. 18

As you learned earlier, collector groups are assigned to policies. When you click on a policy to highlight it, you'll see the collector groups currently assigned to that policy listed in the **Assigned Collector Groups** pane on the right. You can add collector groups to a policy by selecting the policy's checkbox and clicking the **Assign Collector Group** button. That opens the **Collector Group Assignment** window, where you can choose which groups to assign. A warning appears if the selected group is currently assigned to another policy of the same type—for example, another Execution Prevention policy. Click **Yes** to remove the group from its old policy and add it to your selected one. Remember that, for full protection, each collector group should be assigned to one Execution Prevention, one Exfiltration Prevention, and one Ransomware Prevention policy. Device Control policies are optional. If you are in a high-security environment that requires restricting USB device access, assign your collector groups to a Device Control policy as well.

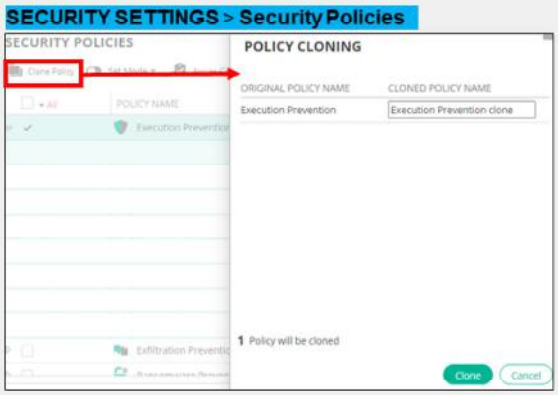
At the bottom of the tab is **ADVANCED POLICY & RULE DATA** for the highlighted policy and rule. If it's collapsed, click the white arrow to expand the pane. First are the **Rule Details**—you'll see a brief description of the rule, and Fortinet's recommendations for handling an event that violated that rule. Click **Factory Settings** to reset the selected policy to its initial state.

Vouchers & Dumps are Available | WhatsApp +201224560923

DO NOT REPRINT Brave-dumps.com
© FORTINET

Cloning Security Policies

- **Creating custom policies**
  - Your installation may have multiple copies of each policy type, each with its own rules and settings
  - To create a new policy, clone an existing one and customize the settings in your cloned copy
  - Create a custom policy when you have a group requiring different levels of security
- **Use cases**
  - Deployment requires a set of policies in simulation mode and one in prevention mode
    - A newly deployed group requiring tuning should be assigned to policies in simulation mode
    - The high security collector group requires strict enforcement of all policies and should always be assigned to policies in prevention mode
  - A development group may require a policy with certain rules deactivated (for example, debugged process)



NSE Training Institute © Fortinet Inc. All Rights Reserved. 19

In some cases, you may want to create multiple policies to accommodate different groups.

For example, newly deployed groups should be assigned to policies in simulation mode until tuning is complete. However, the High Security Collector Group, should always be assigned to policies in prevention mode, even during deployment. You'll need to maintain a set of policies in simulation mode and another set in prevention mode.

You may also have collector groups with specific needs that require different settings than other groups. For example, developers may need certain rules disabled because of the nature of their day-to-day work. You can create as many copies of policies as you need.

You can clone a policy to create customized copies to apply to different groups. Select the checkbox next to one of the existing policies and click the **Clone Policy** button. You can then assign your copy a new name and customize its settings as needed. In general, you should have two copies of each policy type—one in prevention mode and one in simulation mode. Always assign the High Security Collector Group to the policies in prevention mode. During tuning, this protects collectors in case of an infection. Fortinet recommends creating a collector group called Simulation, which should be assigned to the policies that are in simulation mode. After initial tuning, when all collectors should be assigned to policies in prevention mode, you can temporarily move individual collectors into the simulation group if needed for troubleshooting.

Vouchers & Dumps are Available | WhatsApp +201224560923

DO NOT REPRINT
© FORTINET
Brave-dumps.com

Knowledge Check

1. Which security policy has all the rules disabled by default?
   A. Exfiltration Prevention
   ✓ B. Device Control
2. What is the purpose of deploying the Ransomware Prevention policy?
   ✓ A. To prevent malicious actors from encrypting data
   B. To prevent malicious actors from stealing data

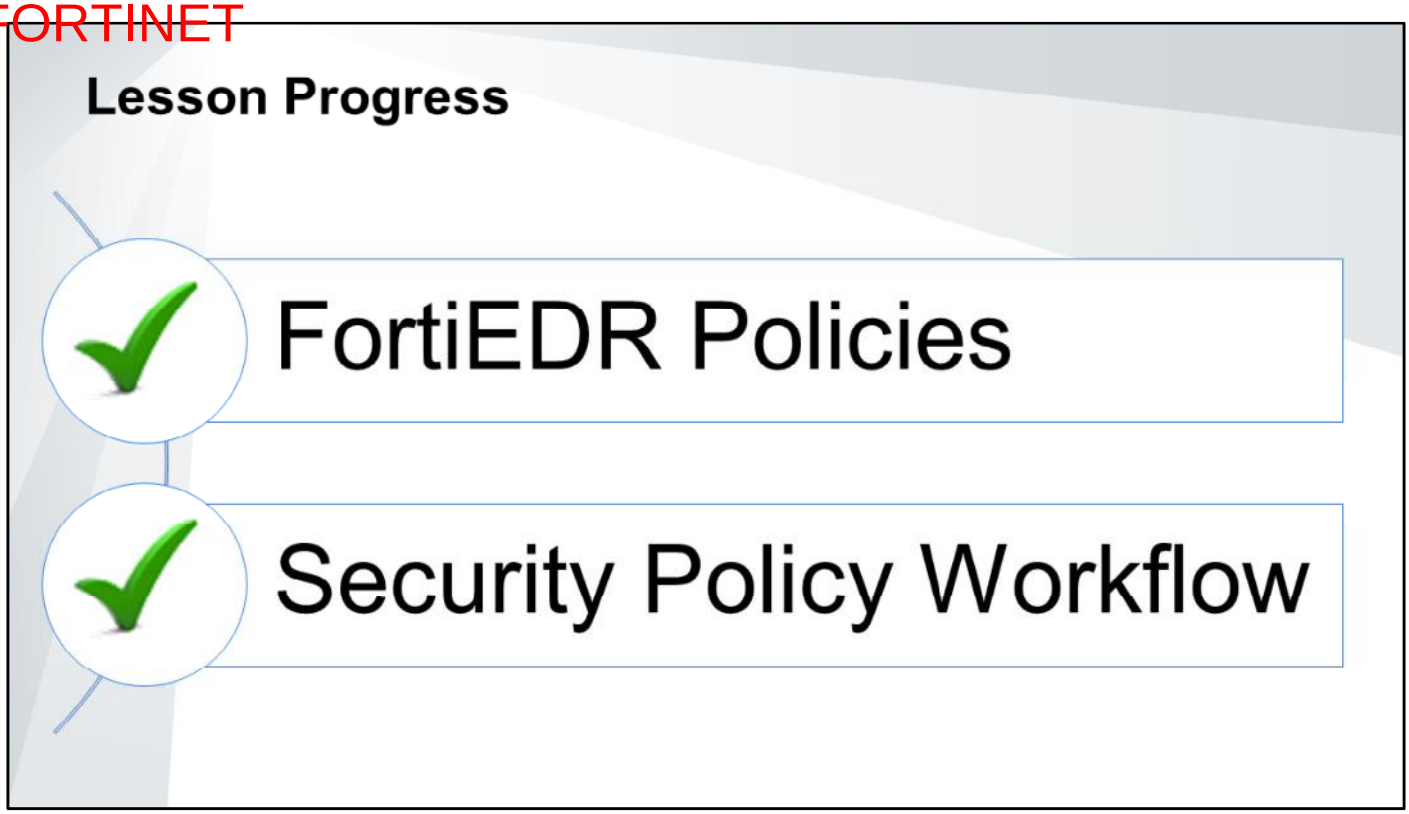
NSE Training Institute

© Fortinet Inc. All Rights Reserved.

20

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

Review

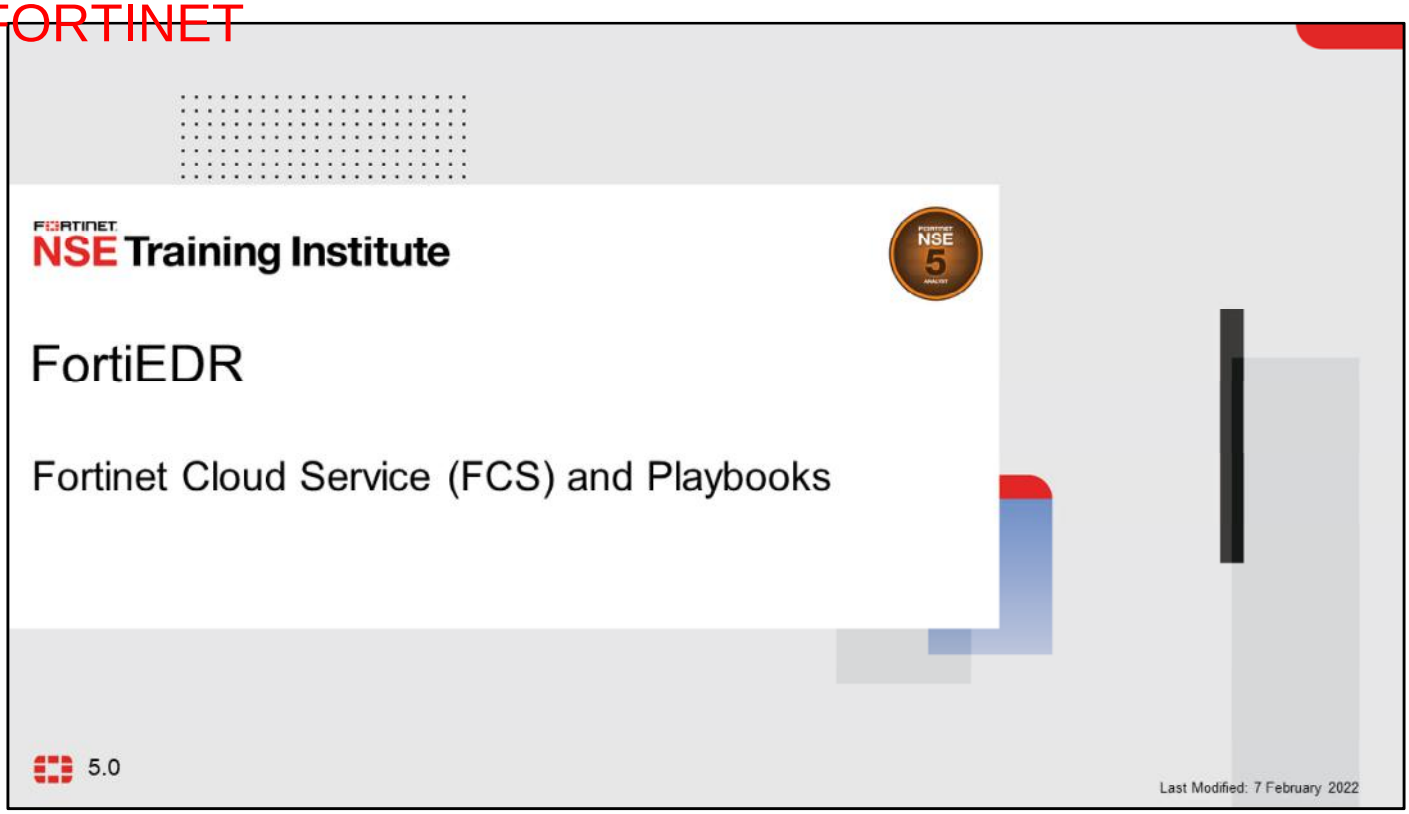
- ✓ Know what NGAV is and how it works
- ✓ Identify the different types of FortiEDR policies
- ✓ Understand the different policy modes
- ✓ Understand the master slider functionality
- ✓ Understand how security policies work
- ✓ Identify the predefined security policies
- ✓ Assign security policies
- ✓ Clone security policies

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

By mastering the objectives covered in this lesson, you learned how security policies work.

Vouchers & Dumps are Available | WhatsApp +201224560923

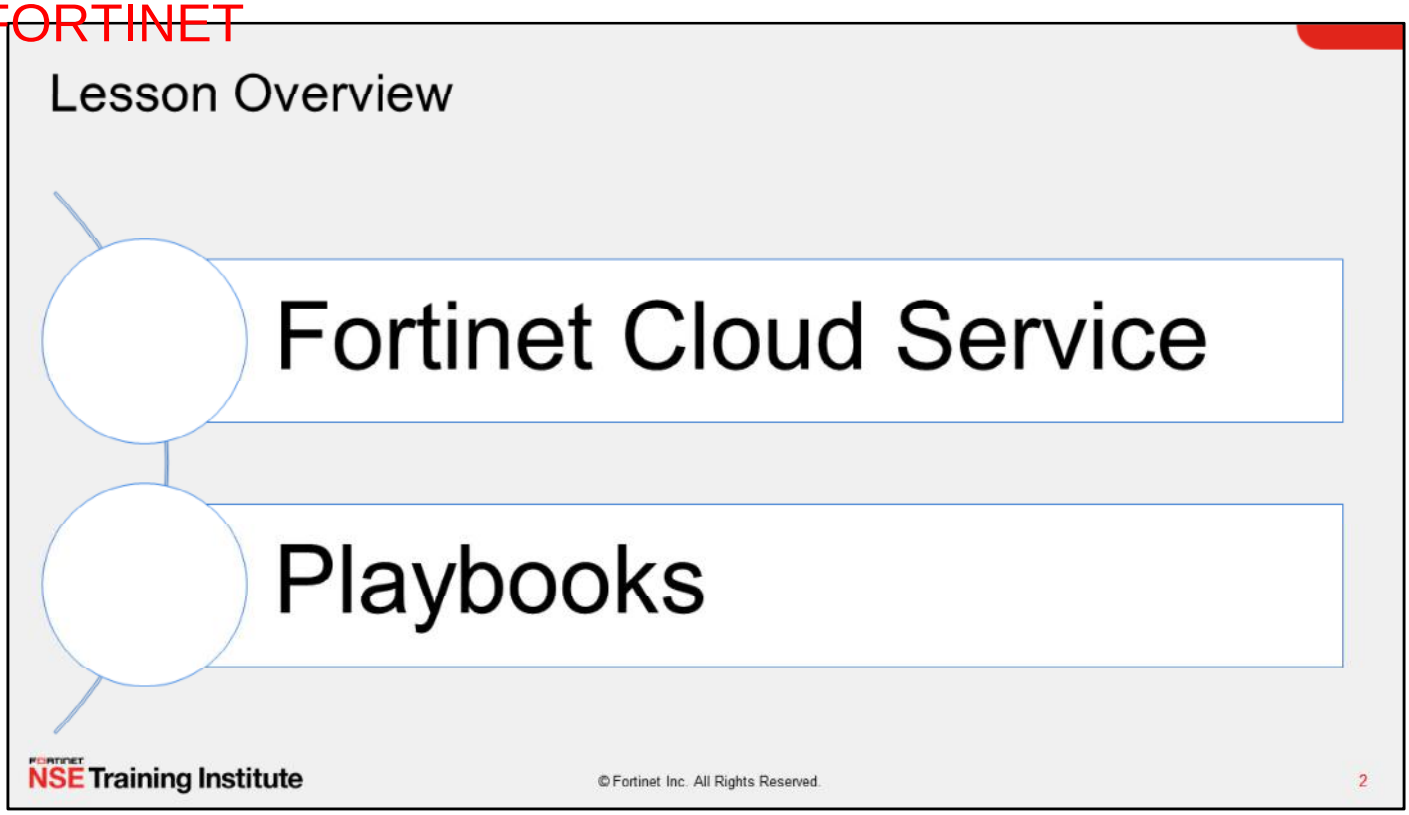
DO NOT REPRINT
© FORTINET
Brave-dumps.com



In this lesson, you will learn what the Fortinet Cloud Service is, why it is needed, how it works, and about playbooks.

Vouchers & Dumps are Available | WhatsApp +201224560923

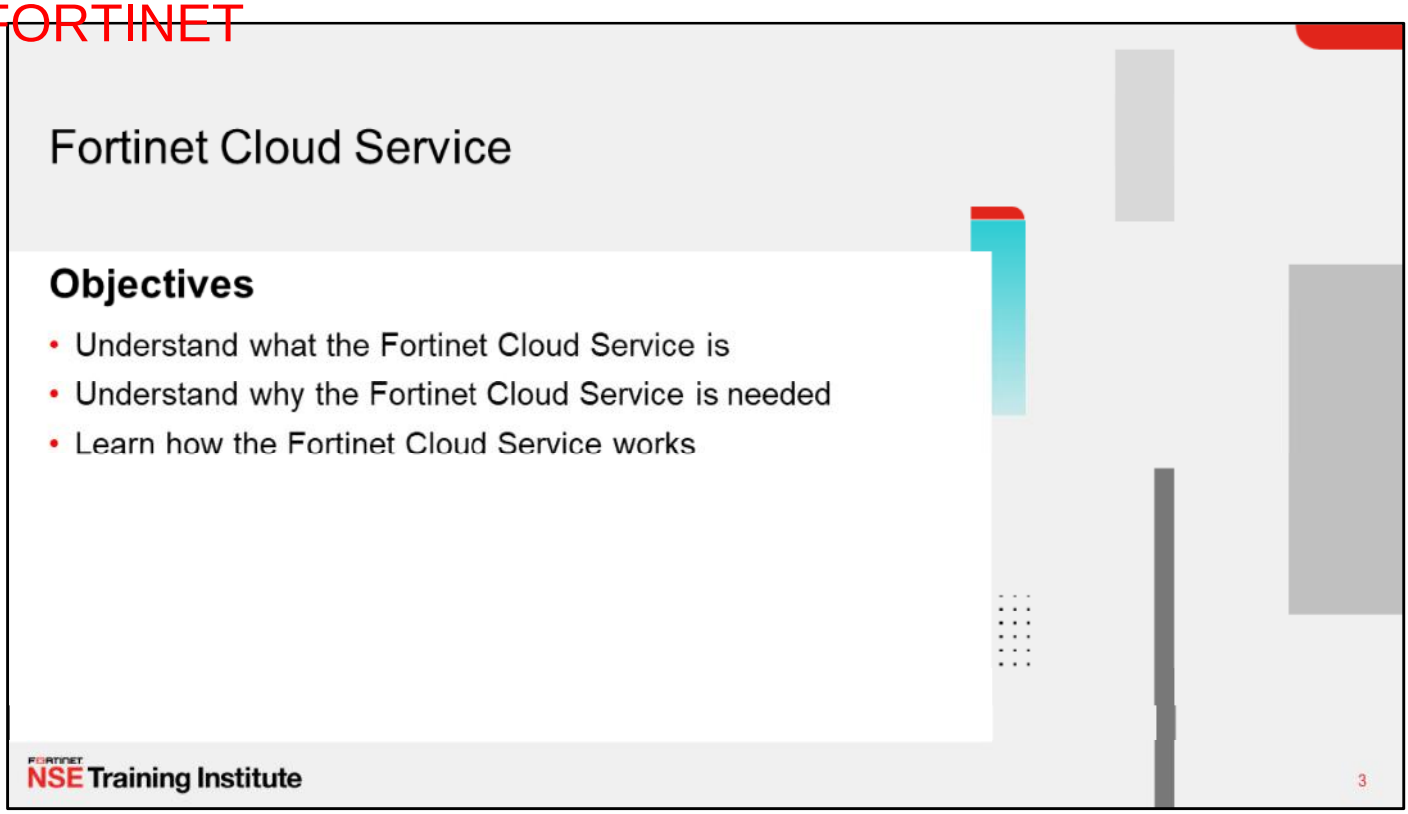
DO NOT REPRINT
© FORTINET
Brave-dumps.com



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.

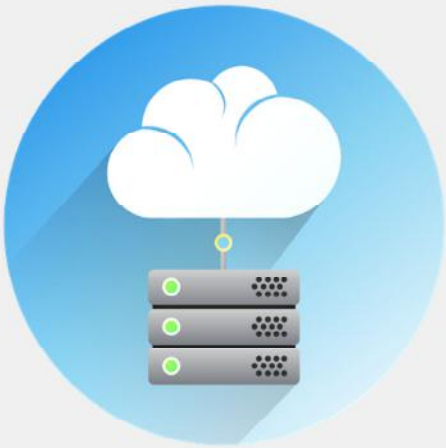
By demonstrating competence in using the Fortinet Cloud Service, you will be able to handle events management tasks.

Vouchers & Dumps are Available | WhatsApp +201224560923

DO NOT REPRINT
© FORTINET
Brave-dumps.com

Fortinet Cloud Service

- What is the Fortinet Cloud Service?
  - Centralized system that handles event management tasks
  - Evaluates events after they happen:
    - Verifies classification and reclassifies if needed
    - Carries out assigned playbook actions
- Why is the Fortinet Cloud Service needed?
  - Improved accuracy—conducts in-depth analysis of events that cannot be performed in real time
  - Reduces ambiguous classifications
    - Ultimate goal is to classify all events as either malicious or safe
  - Reduces amount of human analysis needed



NSE Training Institute

© Fortinet Inc. All Rights Reserved.

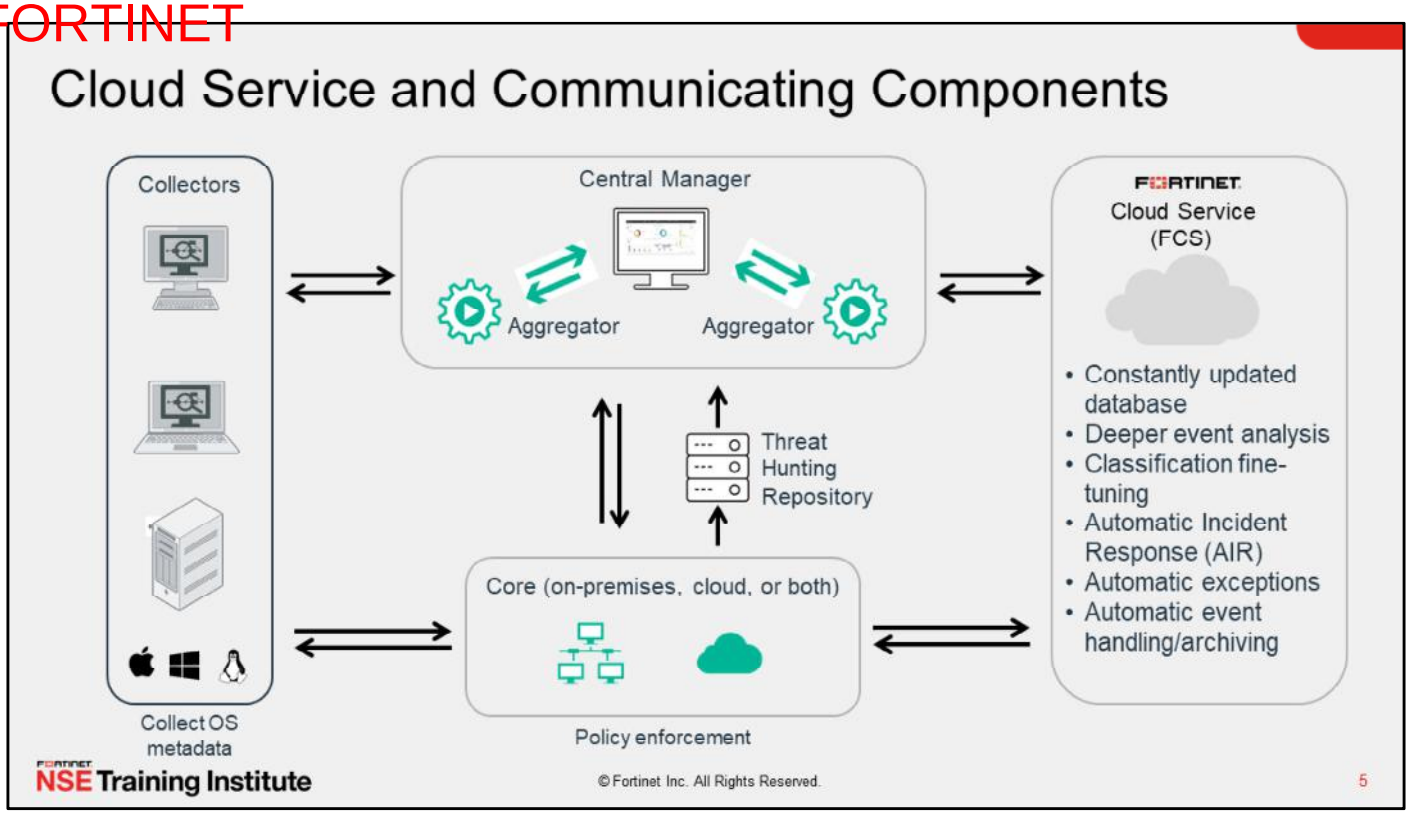
4

FCS, is a centralized system that handles event management tasks. It evaluates each event after it happens. The core makes the initial decision to block or allow and classifies the event, then sends the data to FCS for further analysis. FCS verifies the classification and changes it if needed, then carries out any assigned playbook actions for that classification. FCS is responsible for managing all investigation actions, like putting a collector into isolation mode, and remediation actions, like deleting a malicious file, in the playbooks.

The main advantage of FCS is that it improves the accuracy of event classification. In order to stop malware from causing harm, you must decide in real time whether a process should be blocked or allowed. That's what the core does. FCS then conducts an in-depth analysis of the event, which would not be possible in real time, and fine-tunes the classification. Ultimately, the goal is to classify all events as either malicious or safe, so there is less need for time-consuming manual human analysis.

Vouchers & Dumps are Available | WhatsApp +201224560923

DO NOT REPRINT
© FORTINET
Brave-dumps.com



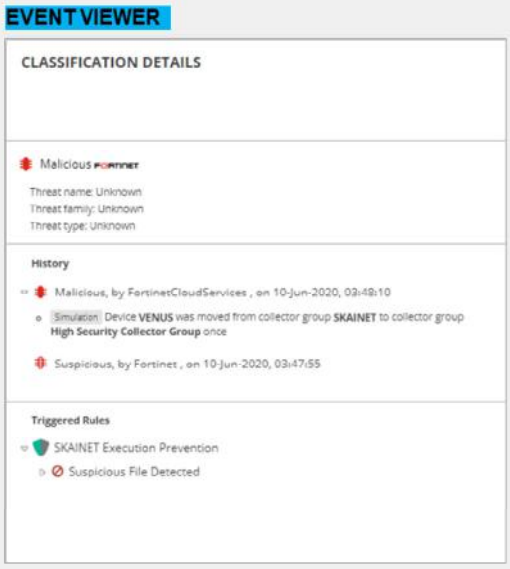
Now, you'll take a look at how FCS fits into the Fortinet infrastructure. As you saw in previous lessons, the core receives event data from the collectors and sends back a verdict—allow or block. The core also sends event data, including a preliminary classification, to the central manager through the aggregator, and on to FCS. FCS maintains a constantly updated database of event and malware data, which it uses to conduct in-depth event analysis and fine-tune the classification level assigned by the core. FCS also handles investigation and remediation tasks configured in playbooks. After remediating a malicious event, FCS automatically marks it as handled. If FCS reclassifies an event as safe, it automatically creates an exception so the same event is not blocked if it occurs again. FCS sends all this information back to the central manager, which displays it in the event viewer of the management console.

Vouchers & Dumps are Available | WhatsApp +201224560923

DO NOT REPRINT
© FORTINET
Brave-dumps.com

How Does the Fortinet Cloud Service Work?

- FCS evaluates every event
  - Analysis is based on its extensive database of previous events
- Why does FCS revise classifications?
  - The core can evaluate events and carry out actions in almost no time
  - FCS requires a few seconds to evaluate
  - A malicious actor can encrypt or steal your data in a few seconds
  - The core provides immediate protection; FCS provides fine-tuning
- FCS controls playbook actions
  - Playbook actions are carried out by FCS
    - If FCS is not available, no action will be taken

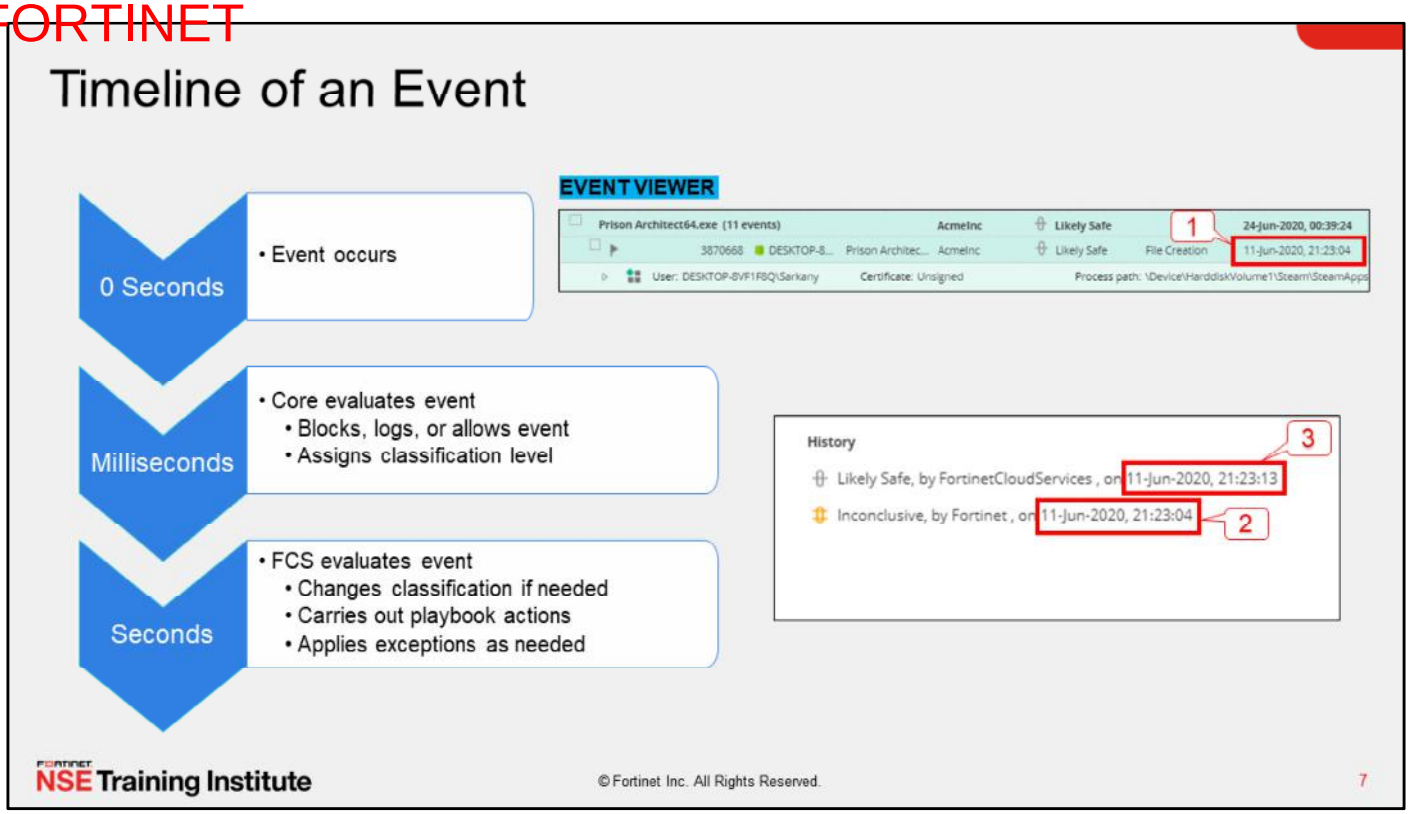


NSE Training Institute © Fortinet Inc. All Rights Reserved. 6

Now, you'll take a closer look at how FCS works. First, it automatically evaluates each event based on its extensive database of previous events. All that information is extremely useful in increasing Fortinet accuracy, but it does take a few seconds to process. That's why the initial classification happens at the core. The core can evaluate an event and make a decision to block or allow it almost instantaneously. That's important because an attacker doesn't need more than a few milliseconds to encrypt or steal data, so you must be able react in real time. After the core makes its decision, FCS fine-tunes the classification. The playbook actions are carried out based on the classification approved by FCS. For example, in the event you see on the right, the Fortinet core classified the event as suspicious. If you look in the **Triggered Rules** section, you can see that the event violated the **Suspicious File Detected** rule in the **Execution Prevention** policy, so Fortinet blocked it, which you can see by the red icon next to the rule. Then FCS analyzed the event and upgraded the classification to **Malicious**—it verified that the event was bad based on previous event data. Based on this **Malicious** classification, FCS would have moved the affected collector into the **High Security collector Group**, but the playbook was in simulation mode. You can tell by the gray **Simulation** label right before the playbook action.

Vouchers & Dumps are Available | WhatsApp +201224560923

DO NOT REPRINT
© FORTINET
Brave-dumps.com



Take a look at the timeline of a typical event. The time the event first occurs is the starting point. If you look at the event on the right side, you can see that the event happened on June 11th at 21:23 and 4 seconds. Within milliseconds of the event, the core evaluated it, classified it, and assigned one of three actions—block, allow, or log, depending on the policy settings configured. In the example shown on this slide, you can see the **History** section of the **Classification Details** pane for the event. The initial classification, at the bottom, was assigned by the core — it classified the event as **Inconclusive** at 21:23 and 4 seconds—within one second of the initial event. Next, FCS received the event data and carried out an additional evaluation, applying playbook actions or exceptions as needed. Again, looking at the **History**, you can see that FCS revised the classification to **Likely Safe** at 21:23 and 13 seconds. Still quick, but in this case about nine seconds slower than the core. In this example, you don't see any playbook actions listed because no playbook actions are selected for **Likely Safe** events.

Vouchers & Dumps are Available | WhatsApp +201224560923

DO NOT REPRINT
© FORTINET
Brave-dumps.com

Alert Aggregation, Classification, and FCS

- Review: Event aggregation
  - FortiEDR aggregates similar raw data items into a single event
  - New events are added to existing events if they match the process, the action, and type of rule
    - Example: `driverupdate.exe` makes multiple attempts to connect to the network. All attempts are aggregated into the same event
  - Events are aggregated into alerts
  - For convenience and easier navigation, FortiEDR aggregates events either by device or by process
    - Example: All events involving `driverupdate.exe` are aggregated into one alert
- Aggregation and classification
  - Different events involving the same process may be assigned different classifications
  - The classification process considers not only the process but the type of activity detected
    - Example: `Notepad.exe` is a well-known text editing application.
      - If `notepad.exe` violated a FortiEDR rule while writing to disk—perhaps due to a careless software revision—FCS would likely reclassify the event as safe
      - If `notepad.exe` started a service, opened a port, and began listening, FCS would likely reclassify the event as malicious because this behavior is not expected for a text editor

NSE Training Institute © Fortinet Inc. All Rights Reserved. 8

ForiEDR aggregates events to make them easier for you to review. Raw data items are aggregated into a single event based on the process, action attempted, and rules violated. For example, if a file called `driverupdate.exe` makes multiple attempts to connect to the network, perhaps breaking the non-standard communication rule, each attempt would be aggregated into one event.

Events are then aggregated into alerts. You can aggregate events by device or by process. For example, if you choose the **Process** view, all events involving the file `driverupdate.exe` are aggregated into one alert.

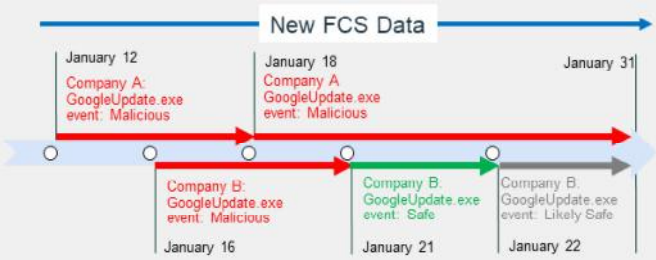
If you are viewing events by process, you may notice that different events involving the same process can have different classifications. The reason for this is that the classification is based not only on the process itself, but also on what it was attempting to do. For example, take `notepad.exe`. It's a very common text editing application found on virtually all Windows machines, which is known to be safe. Normally, `notepad.exe` does not generate any alerts, but if it were to violate a FortiEDR rule while writing to disk—perhaps because of a careless software revision—it would generate an alert. After reviewing the event, FCS would probably reclassify that event as safe. You'd expect `notepad.exe` to write to disk, so this behavior doesn't raise any red flags. But say `notepad.exe` suddenly started a service, opened a port, and began listening. That's not how a text editor behaves, so FCS would probably reclassify this event as malicious. It's the same signed executable in both cases, but in the second event it's behaving strangely and could have been hijacked by a malicious process.

Vouchers & Dumps are Available | WhatsApp +201224560923

DO NOT REPRINT
© FORTINET
Brave-dumps.com

FCS Updates

- When does FCS update an event?
  - FCS evaluates each new event as it occurs
  - If an event occurs again, FCS re-evaluates the event
  - If new FCS information is available, FCS updates the existing event classification based on the new data
- FCS and old events
  - If an event has not reoccurred, FCS does not update the event classification based on any new information available
  - To be re-evaluated, an event must reoccur in the same environment and be aggregated with the original event
  - Similar events in different environments may be classified differently if they occurred at different times



NSE Training Institute
© Fortinet Inc. All Rights Reserved.

When does FCS update an event? FCS evaluates each new event as it occurs. If the same event occurs again—for example, if a process makes another attempt to connect to an IP address—FCS re-evaluates the event. If new information is available at that time, FCS updates the existing event's classification as needed. In the example on the right side of this slide, 24 raw data items are aggregated into the highlighted event. Each time a new raw event occurred, FCS re-evaluated the event. On January 16, when the initial event occurred, FCS classified it as **Malicious**. Five days later, a new raw event occurred and, based on new data, FCS changed its classification to **Safe**. A day after that, the event occurred again, and FCS reclassified it again, this time as **Likely Safe**. You can see these changes on the **Classification Details** pane under **History**.

FCS does not evaluate past events unless they reoccur. The recurrence must be aggregated with the original event in the same environment. This means that two companies with similar events may see different classifications if their events occurred at different times.

Look at the timeline to the right on the right side of this slide. Company A had two raw events involving `GoogleUpdate.exe`, on January 12 and January 18. Company B has three raw events involving the same process and the same rule violation, with the last one occurring on January 22. FCS has acquired new data throughout this time period, and revised its classification twice—once on January 21, and again on January 22. Company A had no new occurrences after FCS revised its classification. If each company reviews its events at the end of the month, Company A will find the event classified as **Malicious**, as classified on January 18, while Company B will find its event classified as **Likely Safe**, the current classification as of January 22.

Vouchers & Dumps are Available | WhatsApp +201224560923

DO NOT REPRINT
© FORTINET
Brave-dumps.com

Is FCS Running?

- Check the **System Components** health chart
  - If the FCS bar is green, FCS is up and running

NSE Training Institute

© Fortinet Inc. All Rights Reserved.

10

How do you know if FCS is running in your environment? The quickest way to tell is by checking the **DASHBOARD**. At the bottom right corner of the dashboard, you'll find the **SYSTEM COMPONENTS** health chart. FCS is the fourth bar shown—if it's green, then FCS is up and running.

Vouchers & Dumps are Available | WhatsApp +201224560923

DO NOT REPRINT
© FORTINET
Brave-dumps.com

Knowledge Check

1. Which feature is a benefit of using FCS?
   - ✓ A. Automated Incident Response
   - B. Threat hunting capabilities

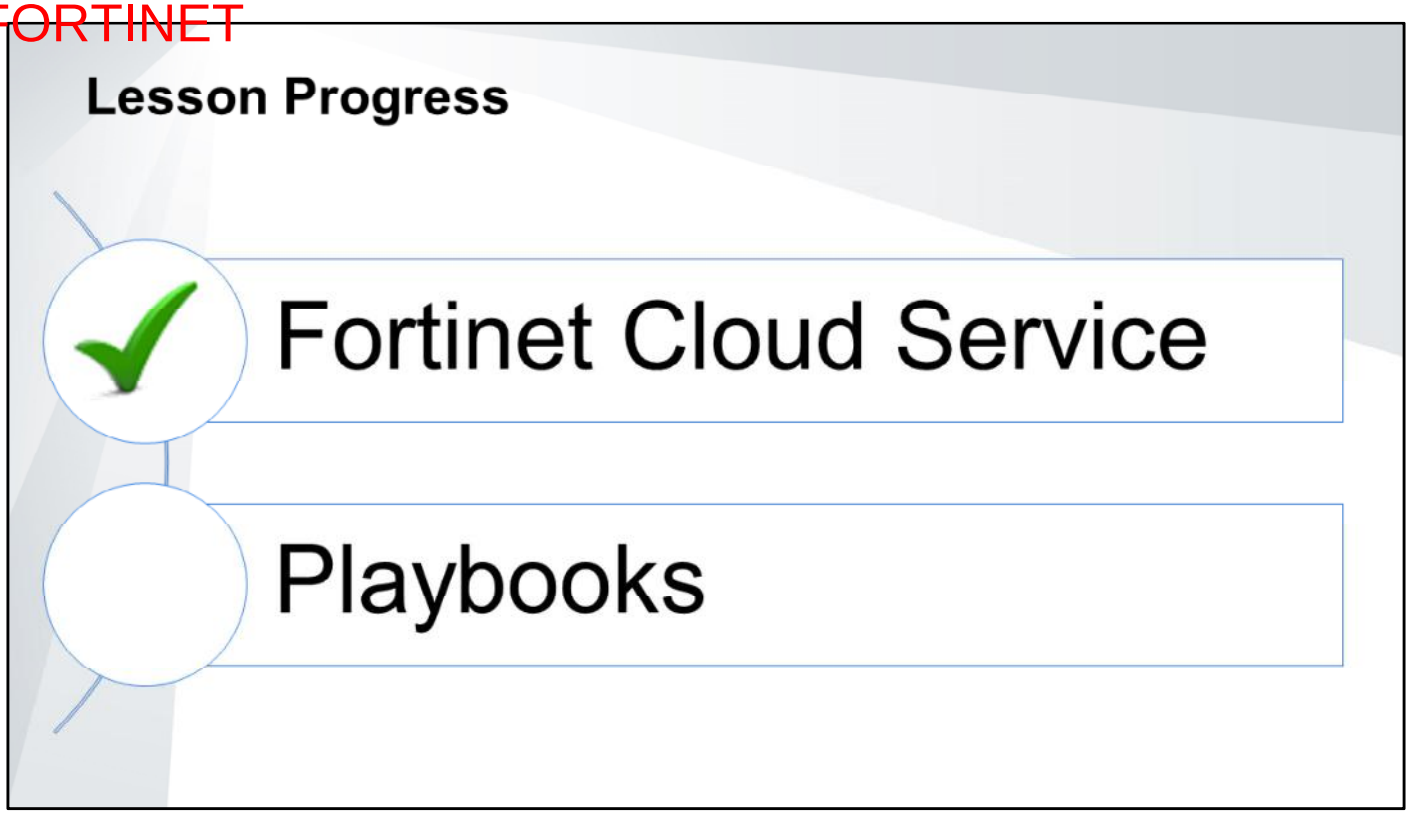
NSE Training Institute

© Fortinet Inc. All Rights Reserved.

11

Vouchers & Dumps are Available | WhatsApp +201224560923

DO NOT REPRINT
© FORTINET
Brave-dumps.com

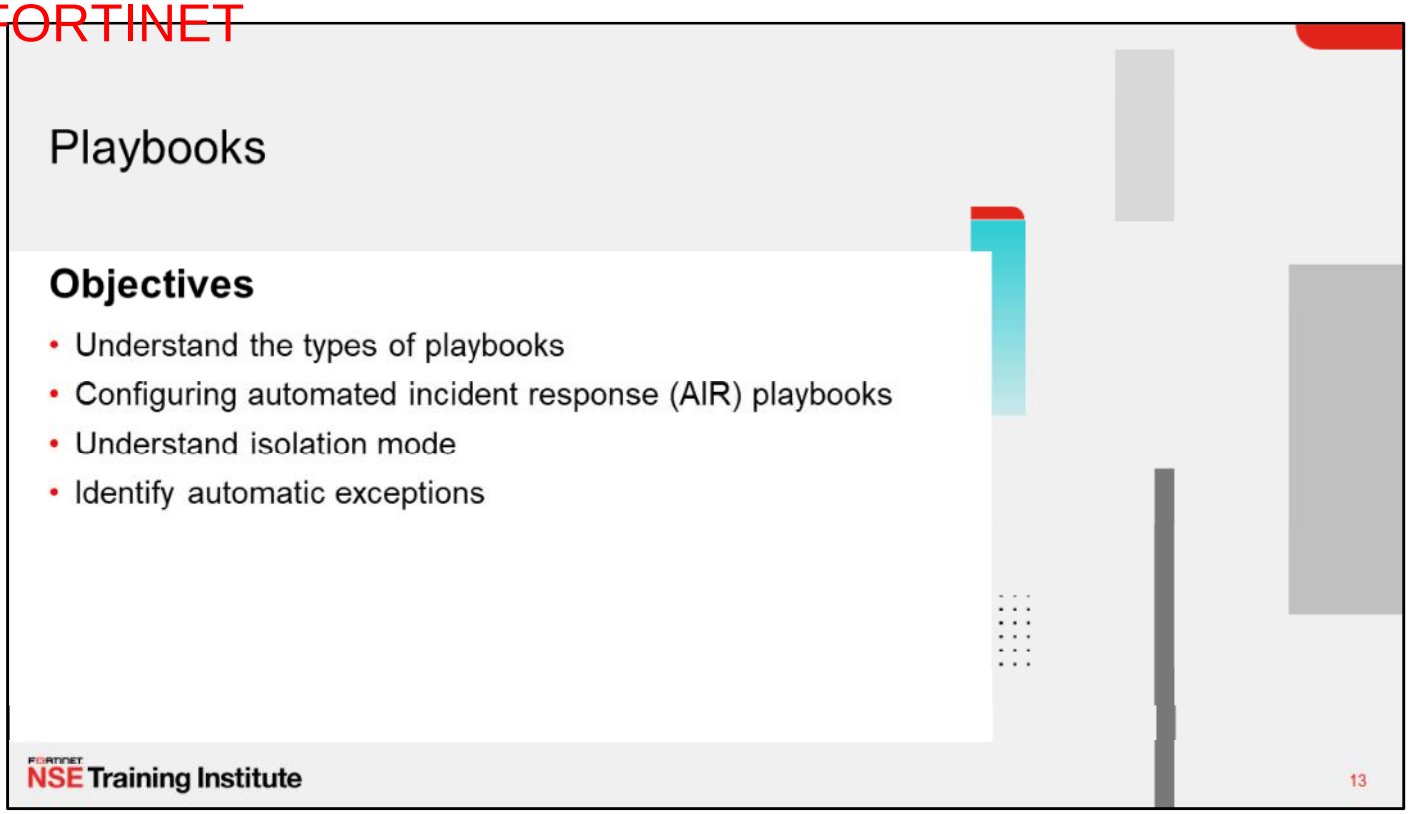


Good job! You now understand about the Fortinet Cloud Service.

Now, you will learn about playbooks.

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 playbooks, you will be able to understand the FortiEDR AIR solution.

Vouchers & Dumps are Available | WhatsApp +201224560923

DO NOT REPRINT
© FORTINET
Brave-dumps.com

Types of Playbooks

- Automated Incident Response (AIR) playbooks
  - Enabled and configured on the **SECURITY SETTINGS** tab of the management console under **Playbooks**
  - Powered by FCS
  - Control event notifications and isolation, protection, and remediation of infected devices
- FCS playbooks
  - Enabled by request to Fortinet support
  - Powered by FCS
  - Apply automatic exceptions to safe events based on Fortinet proprietary knowledge

NSE Training Institute © Fortinet Inc. All Rights Reserved. 14

Fortinet uses two types of playbooks. The first is AIR. These playbooks are powered by FCS and can be configured on the **SECURITY SETTINGS** tab of the management console.

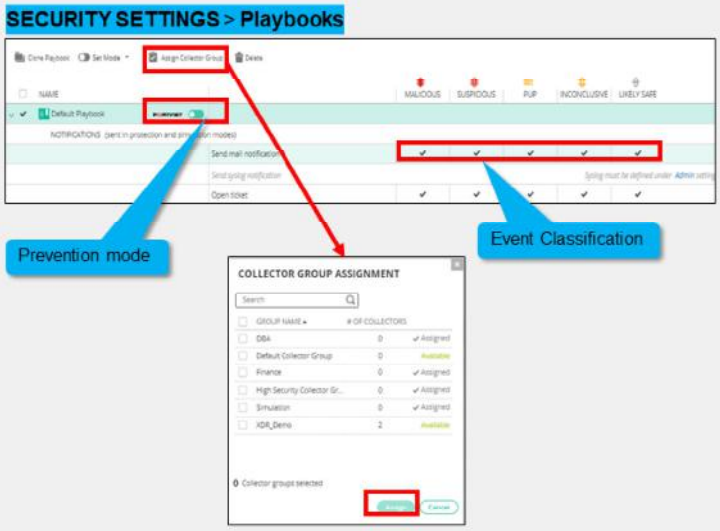
FCS playbooks can be enabled by Fortinet support on request. These playbooks use the Fortinet proprietary knowledge to identify safe events and create automatic exceptions. You'll learn more about automatic exceptions in this lesson.

Vouchers & Dumps are Available | WhatsApp +201224560923

DO NOT REPRINT Brave-dumps.com
© FORTINET

AIR playbooks

- What are playbooks?
  - A playbook is an automated set of steps FortiEDR takes when an event occurs
  - Different actions may be assigned based on the classification of the event
  - A playbook can be cloned to create multiple versions
- Playbook modes
  - In prevention mode, FortiEDR sends notifications and takes further action, such as isolating the affected device, based on preconfigured settings
  - In simulation mode, notifications are based on the configured settings, but FortiEDR takes no further action
- Playbooks and collector groups
  - Each collector group is assigned to one playbook
  - By default, all collector groups are assigned to the default playbook



NSE Training Institute

© Fortinet Inc. All Rights Reserved.

15

A playbook is an automated set of actions that FortiEDR performs when an event occurs. You can assign different actions for different classification levels. For example, you may keep notifications enabled for events at all classification levels, but terminate the process and clean persistent data only when the classification is malicious.

You can clone a playbook to create versions with different settings. The default playbook comes out of the box in simulation mode. When a playbook is in simulation mode, you will still receive notifications as configured, but no other actions are taken. You can see what FortiEDR would have done in response to a specific event by looking at the classification details panel in the **EVENT VIEWER**. You'll learn more about that in another lesson. If a playbook is in prevention mode, FortiEDR carries out all actions as configured.

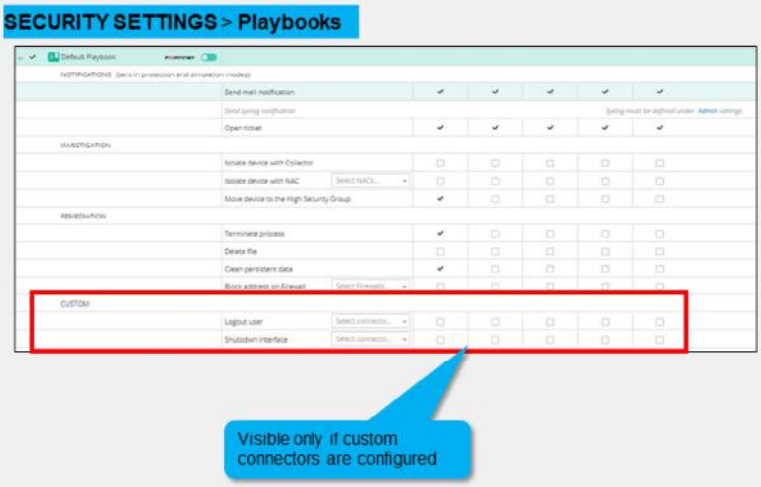
Each collector group is assigned to one—and only one—playbook. By default, all collector groups are assigned to the **Default Playbook**.

Vouchers & Dumps are Available | WhatsApp +201224560923

DO NOT REPRINT Brave-dumps.com
© FORTINET

AIR Playbooks (Contd)

- Four types of actions can be performed by playbook policies:
  - Notifications
    - Email, Syslog, Open ticket
  - Investigation
    - Isolate device
    - Isolate device with FortiNAC
    - Move device to High Security Group
  - Remediation
    - Terminate process
    - Delete file
    - Clean persistent data
    - Block address on FortiGate Firewall
  - Custom
    - Customized actions with custom connector



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

You can alter the playbook action to suit your needs. AIR playbooks control event notifications—email, syslog, or open ticket—and can automatically isolate a device with a collector or using FortiNAC, move it to the High Security Group, and remediate it. As part of the remediation configuration, the malicious IP address can also be added to FortiGate to block future transactions. You can add custom actions to the playbook, after you configure custom connectors and actions. You'll learn more about that in another lesson.

Vouchers & Dumps are Available | WhatsApp +201224560923

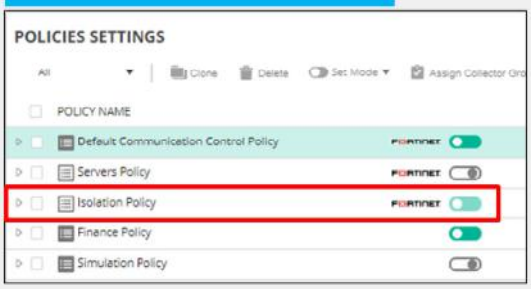
DO NOT REPRINT Brave-dumps.com
© FORTINET

Isolation Mode

- Playbooks and isolation mode
  - You can configure AIR playbooks to place collectors automatically in isolation mode when an event occurs
  - You can also move collectors into or out of isolation mode manually on the **INVENTORY** tab
- How isolation mode works
  - Collectors in isolation mode are automatically assigned to the **Isolation Policy** in **COMMUNICATION CONTROL**
  - The **Isolation Policy** blocks all applications by default
    - You can allow specific applications as needed
  - Collectors in isolation mode are marked with a red icon on the **INVENTORY** tab

INVENTORY > Collectors

COMMUNICATION CONTROL > Policies



NSE Training Institute

© Fortinet Inc. All Rights Reserved.

17

Isolation mode is a collector state used to help contain infections while they are being investigated and remediated. AIR playbooks can be configured to place collectors automatically into isolation mode when an event is triggered. For example, you could configure a playbook so that all collectors that trigger an event classified as malicious are automatically put into isolation mode.

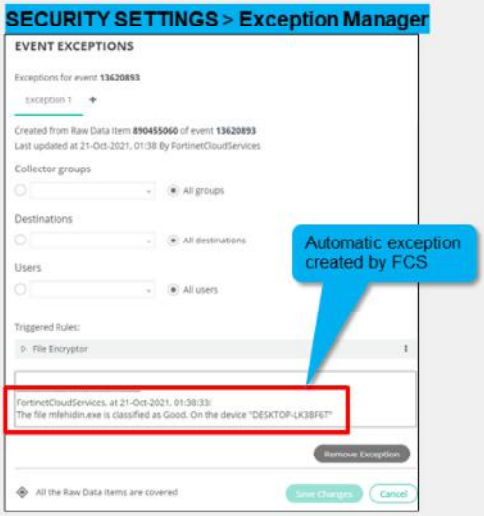
Isolation mode is a state. It doesn't affect the collector group assignment—a collector can be in isolation mode and still remain in its usual collector group. However, collectors in isolation mode, are automatically assigned to the **Isolation Policy** in **COMMUNICATION CONTROL**, rather than their group's policy. The isolation policy is built in and, by default, it blocks all applications from communicating. You can allow specific applications as needed, such as helpdesk or security software. A best practice is to allow only applications you may need to remotely remediate the device. You can manually put collectors into or out of isolation mode on the **INVENTORY** tab using the **Isolate** drop-down list. Collectors in isolation mode are marked with a red indicator icon.

Vouchers & Dumps are Available | WhatsApp +201224560923

DO NOT REPRINT
© FORTINET
Brave-dumps.com

Automatic Exceptions

- What is an automatic exception?
  - When FCS analyzes an event, it may find that a blocked event was in fact safe
  - FCS can create automatic exceptions to prevent these events from reocurring
  - Automatic exceptions are controlled by FCS playbooks
- Why should you enable automatic exceptions?
  - Automatic exceptions allow increased productivity
    - Processes will not be blocked again once FCS determines that they are safe and creates an exception
  - Your management console is less cluttered
    - Fewer events to wade through
    - Fewer exceptions to create
  - If FCS playbooks are enabled, the system owner MUST follow up on all automated exceptions



NSE Training Institute
© Fortinet Inc. All Rights Reserved.

If you enable FCS playbooks, FCS can create exceptions automatically. When FCS analyzes an event, it may find that an event that was initially blocked by the core was, in fact, safe. It can change the classification to safe in these cases but, to make sure the event is not blocked again, it can also create an automatic exception. You can see an example on the right side of this slide. This exception has a note saying it was created by FCS, and you can see the date, time, and the reason the exception was applied.

Why should you enable automatic exceptions? There are advantages for both the end user and the system administrators. End users can be more productive, because the safe process will not be blocked again. They don't have to call tech support to sort it out, it's just automatically allowed. For the administrator, there's less work—your event viewer won't be cluttered with safe events that you need to investigate and create exceptions for. Note that if automatic exceptions are enabled, the system owner must follow up on all automated exceptions. Fortinet is not liable for any exceptions created by FCS.

Vouchers & Dumps are Available | WhatsApp +201224560923

DO NOT REPRINT
© FORTINET
Brave-dumps.com

Knowledge Check

1. In playbook policies, which action is device isolation part of?
   A. Remediation
   ✓ B. Investigation

2. Which type of playbook controls automatic exceptions in the exception manager?
   A. AIR
   ✓ B. FCS

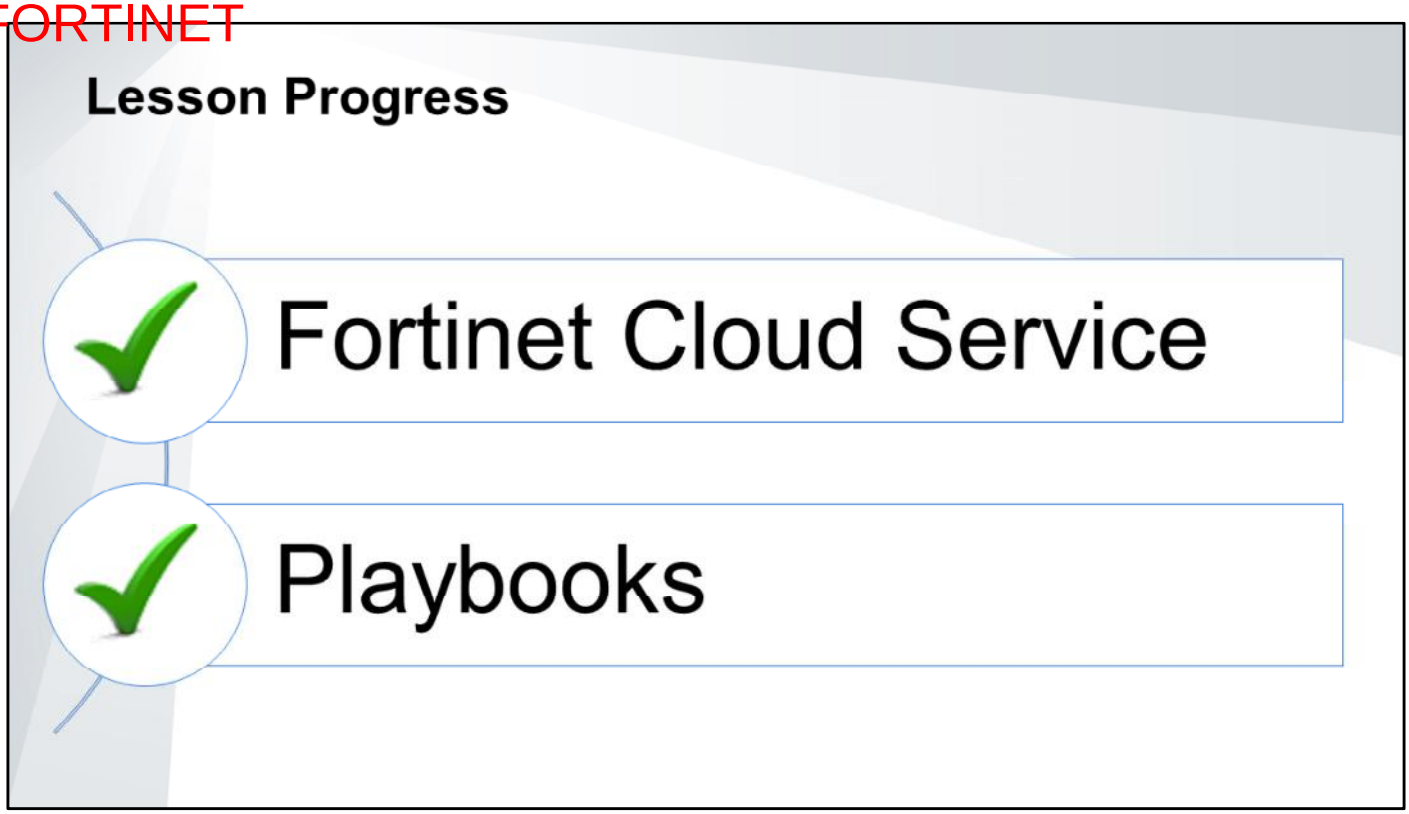
NSE Training Institute

© Fortinet Inc. All Rights Reserved.

19

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

Review

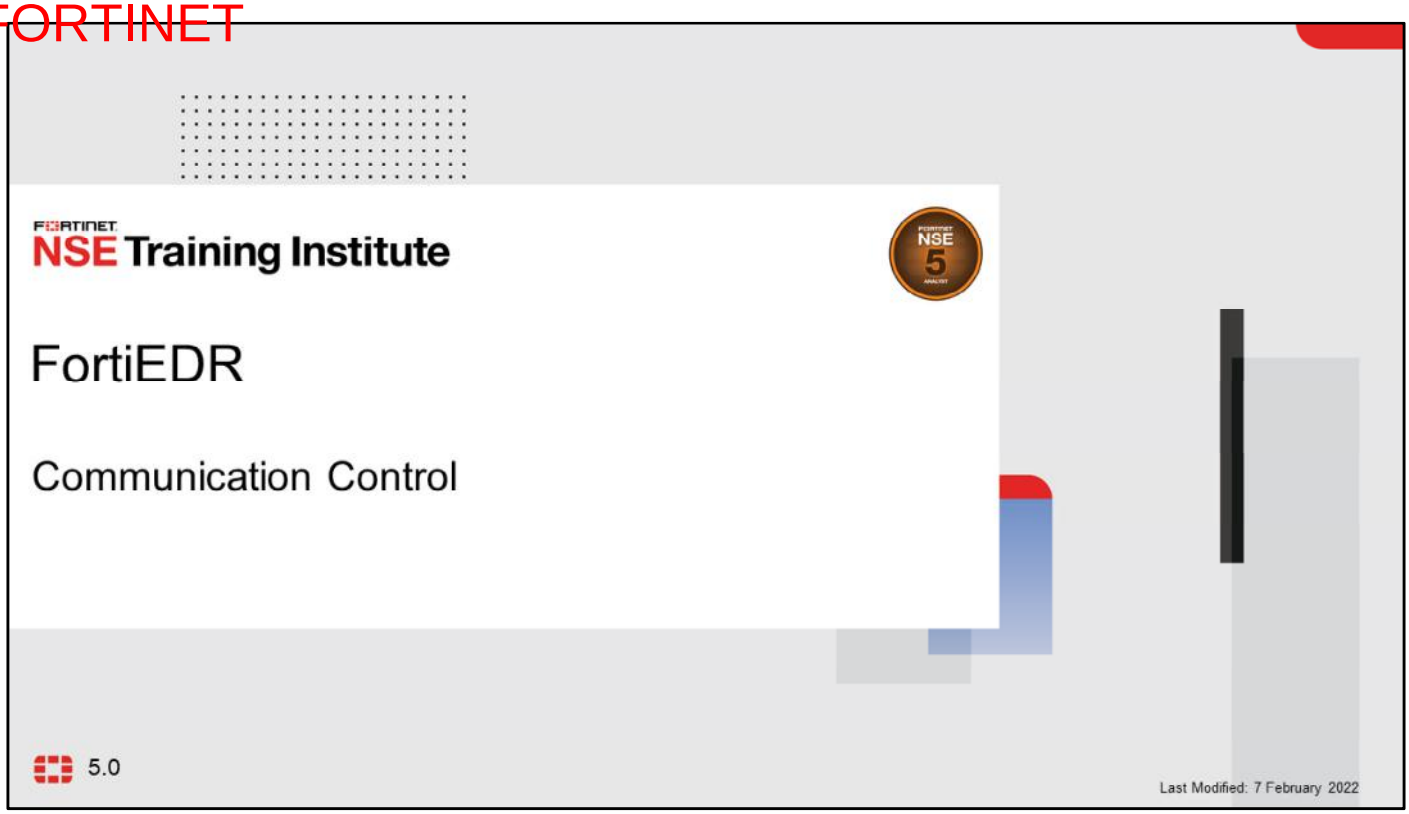
- ✓ Understand what the Fortinet Cloud Service is
- ✓ Understand why the Fortinet Cloud Service is needed
- ✓ Learn how the Fortinet Cloud Service works
- ✓ Understand the types of playbooks
- ✓ Configure AIR playbooks
- ✓ Understand isolation mode
- ✓ Identify automatic exceptions

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

By mastering the objectives covered in this lesson, you learned how the Fortinet Cloud Service works. You also learned about its integration with playbooks.

Vouchers & Dumps are Available | WhatsApp +201224560923

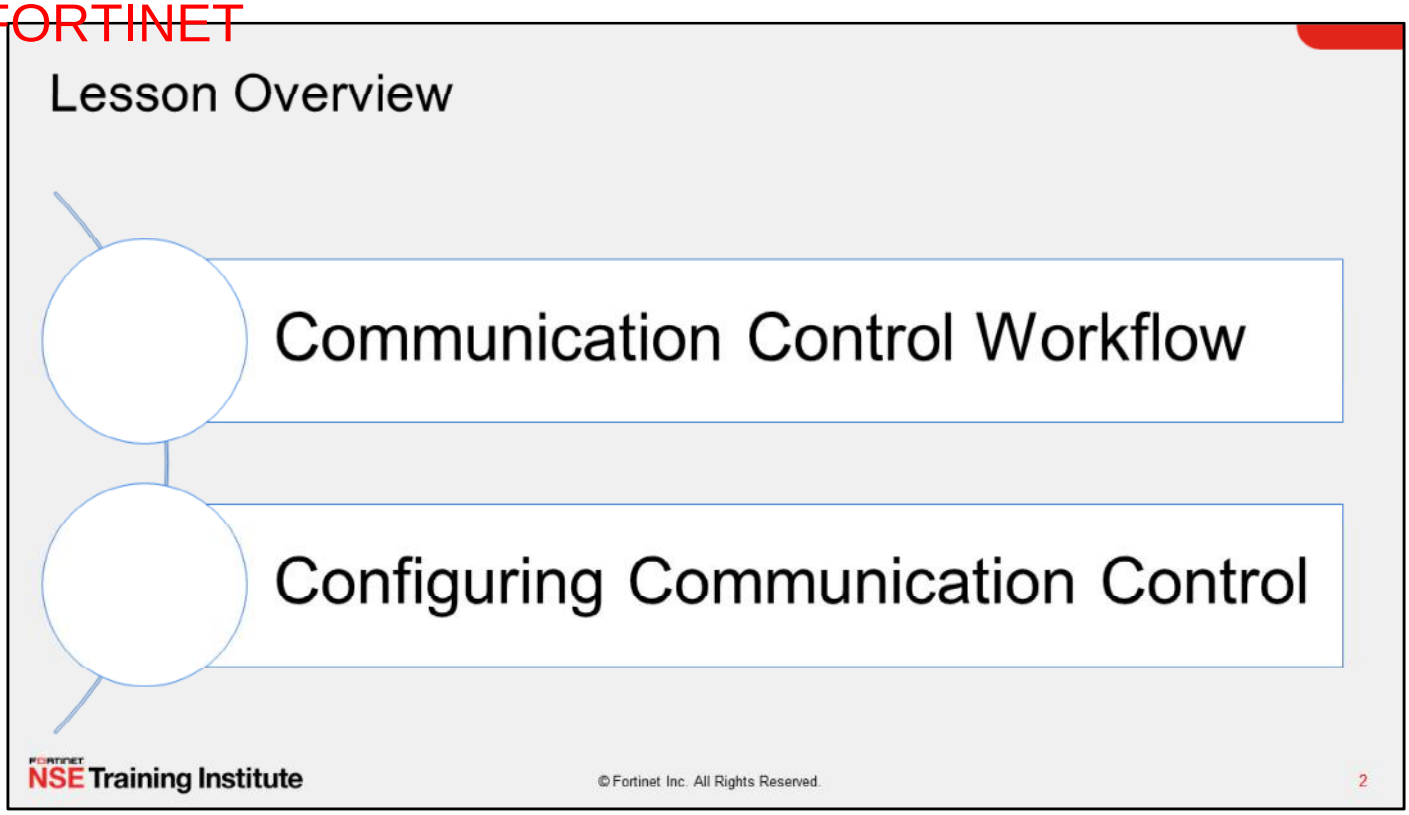
DO NOT REPRINT Brave-dumps.com
© FORTINET



In this lesson, you will learn how to use communication control.

Vouchers & Dumps are Available | WhatsApp +201224560923

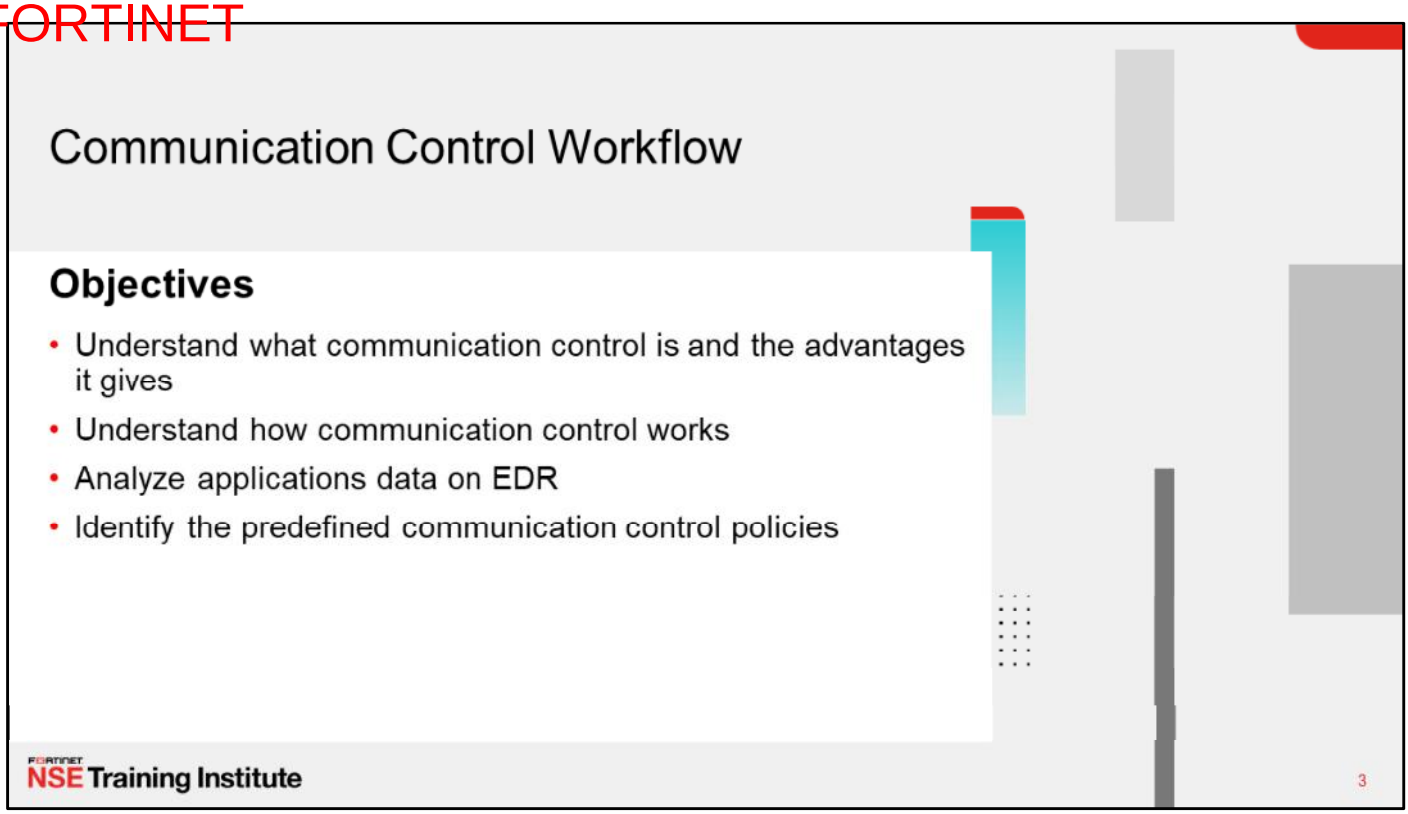
DO NOT REPRINT Brave-dumps.com
© FORTINET



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 communication control, you will understand the workflow.

Vouchers & Dumps are Available | WhatsApp +201224560923

DO NOT REPRINT
© FORTINET
Brave-dumps.com

What Is Communication Control?

- What about applications that don't break the rules?
  - Some applications, while not inherently malicious, are undesirable or risky to use (for example, BitTorrent)
  - These applications do not trigger events, but you may wish to proactively block them from sending or receiving information over the network
- Communication control monitors all applications that communicate over the network
  - Applications that communicate over the internet pose the highest security risk
  - Monitoring only these applications reduces noise
- Choose which applications to block from communicating
  - Communication is blocked at the group level, so you can allow an application for one group but block it for another
  - Administrators can block a specific version of an application if it is known to have security vulnerabilities, but allow later versions that fix the issue

NSE Training Institute

© Fortinet Inc. All Rights Reserved.

4

First of all, what is communication control? Some applications are not malicious, but are inherently risky to use, for example, any torrent applications, like BitTorrent. These applications don't trigger an event because they're not malware, but you may want to proactively prevent them from sending information over the network.

Communication control monitors all applications that communicate over the network. The applications that communicate over the internet pose the most security risk, and monitoring only those applications narrows the problem set significantly, so that you can focus on potential vulnerabilities.

Communication control gives you the ability to choose which applications to block from communicating. They're not actually removed from the computer, but communication is blocked. Communication control policies are assigned at the group level, just like security policies, so you can allow an application for one group, but block it for another. You can also block a specific version of an application if it's known to have security vulnerabilities, while allowing later versions that fix the issue.

Vouchers & Dumps are Available | WhatsApp +201224560923

DO NOT REPRINT Brave-dumps.com
© FORTINET

Why Communication Control?

- Avoids productivity inhibitors: Non-authorized applications can still execute
  - FortiEDR blocks them only from communicating over the network
- Frictionless application control: Reduces user requests from security or IT to approve applications
- Manageability: Handles only applications that communicate externally
- Reputation scoring: Each application version receives a score of one (known bad) to five (known good), allowing easy identification of potentially dangerous applications
- Vulnerability scoring: FortiEDR uses up-to-the-minute common vulnerabilities and exposures (CVE) data to assign a vulnerability score to each application version, pinpointing exposed areas
- Risk mitigation: Create rules to automatically block current and future application versions based on reputation, vulnerability, or vendor

NSE Training Institute

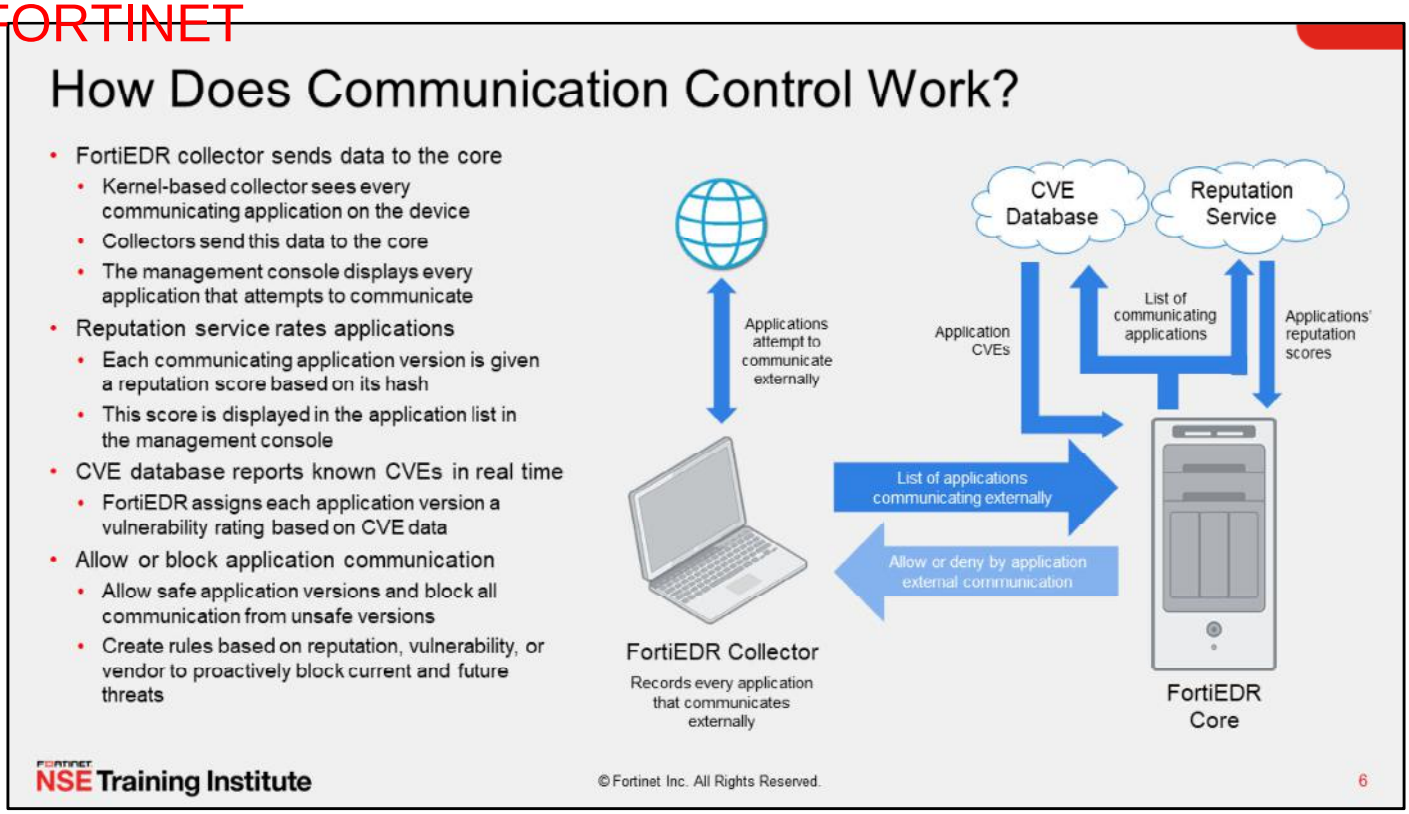
© Fortinet Inc. All Rights Reserved.

5

Why use communication control? The first key advantage is avoiding productivity inhibitors. Blocked applications can still execute, they just can't communicate. Second is frictionless control, which reduces the number of user requests to approve applications. Third is manageability. Security or IT needs to handle only the applications that communicate externally. Fourth, FortiEDR offers reputation scoring. Each version of every application is assigned a score, from 1 (known bad) to 5 (known good). These scores allow you to easily identify potentially dangerous applications. Fifth, FortiEDR uses up-to-the-minute CVE data to assign a vulnerability score to each application version. That means you can pinpoint exposed areas. Lastly, you can mitigate risk by automatically blocking undesirable applications from communicating. You can set rules to block any version of any application if it meets specified criteria. For example, you might block anything with a reputation score of one, any version with a high or critical vulnerability score, or any application from a specified vendor.

Vouchers & Dumps are Available | WhatsApp +201224560923

DO NOT REPRINT Brave-dumps.com
© FORTINET



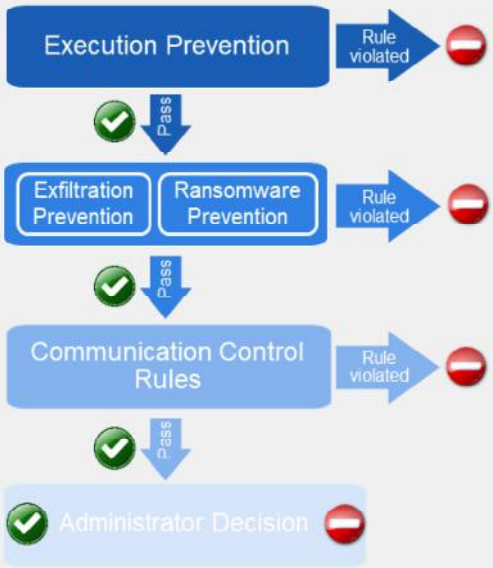
How does communication control work? It starts at the FortiEDR collector. The collector is installed at the kernel level, so it can see everything that happens on the device. One of the things that the collector is watching is which applications are communicating on the user's end device. It sends this data to the core, for evaluation. The core sends the file hash to the reputation service, which returns a reputation score. The core also consults the CVE database and receives a list of CVEs for each application version. This list is constantly updated, so you are informed about new vulnerabilities as soon as they are discovered. All the applications and versions that have been detected are displayed in the management console, along with their reputation and vulnerability scores, so you can easily spot potentially troublesome applications. Each application and version is allowed to communicate or denied communication based on manual settings or configured rules. The core sends this information back to the collector, which regulates connections from that device based on the verdict it received from the core.

Vouchers & Dumps are Available | WhatsApp +201224560923

DO NOT REPRINT Brave-dumps.com
© FORTINET

Communication Control Policies vs. Security Policies

- Order of operations:
  1. Execution prevention catches simple known threats when they are *read* or *executed*
  2. Post-infection prevention policies (exfiltration prevention and ransomware prevention) are processed whenever a *file is modified* or a *connection established*
  3. If the security policies allow an application to communicate, communication control evaluates the application version and blocks communication based on predetermined rules
  4. Communication control blocks communication from application versions manually set to *deny*
- Advantages of processing order:
  - Malware applications be very noisy or, in some cases, very numerous
  - Malicious traffic is taken care of by the security policies, allowing the communication control system to focus on tracking legitimate applications



NSE Training Institute

© Fortinet Inc. All Rights Reserved.

7

How do communication control policies work with security policies? The first thing to know is the order of operations. All the traffic coming from the collector—every attempt to execute a program, modify a file, or connect to the network—is processed at the core. The security policies are processed first. Execution prevention is enforced when a file is read or executed. If the process doesn't violate the execution prevention policy, the collector watches for any attempts to connect to the network or modify files. The core checks these actions against the security policy rules and blocks anything that might be malicious. If the process makes a connection that FortiEDR determines was not malicious, then the application is evaluated by communication control. First, the process is evaluated based on communication control policy rules. Does the application have a poor reputation or known vulnerabilities? Is it produced by a blocked vendor? If no rules are violated, then communication is allowed or denied based on the actions chosen in advance by an admin or console user. You'll learn more about that process later in this lesson.

The reason for the order of operations is that the communication control system is designed to track legitimate applications, not malware. The applications may be risky or undesirable, but they're not actually malicious. Malware is handled by the security policies and tracked through events. Malware applications can be very noisy and, in some cases, very numerous. A single event may include many attempted connections. Eliminating the malware traffic before it reaches communication control allows users to focus on tracking legitimate applications.

Vouchers & Dumps are Available | WhatsApp +201224560923

DO NOT REPRINT Brave-dumps.com
© FORTINET

Virtual Patching and Risk Mitigation

- What is virtual patching?
  - Configure rules that allow or block any application version—even ones that don't exist yet—based on selected criteria
  - Rules can be based on CVE vulnerability, reputation, or vendor
- Why use virtual patching?
  - Reduce attack surface: Instantly block any version of any application from communicating
  - Reduce administration requirements: Because vulnerable versions can be proactively blocked, administrators can spend less time reviewing new applications and versions

NSE Training Institute © Fortinet Inc. All Rights Reserved. 8

FortiEDR can proactively block any application versions based on the criteria you select. This is a great feature because it allows you to block future versions that don't exist yet. After you put the rule in place, any application that fits your criteria—for example, anything with a reputation score of two or less, or anything with a vulnerability rating of critical—is blocked from communicating. You can also proactively block specific vendors and all their current and future products and versions.

Setting risk mitigation rules means your attack surface is much smaller. Any version of any application can be blocked instantly and automatically. You don't have to spend a lot of time on the console evaluating each version and blocking the ones you don't trust. FortiEDR instantly blocks serious threats as they arise, and you can review other applications on your own time, as needed. For example, say a critical vulnerability is discovered in an old version of Java. If you set a rule blocking anything with a critical vulnerability, that version is immediately blocked from communicating, preventing malicious actors from exploiting the vulnerability to access your system. Other versions of Java are unaffected.

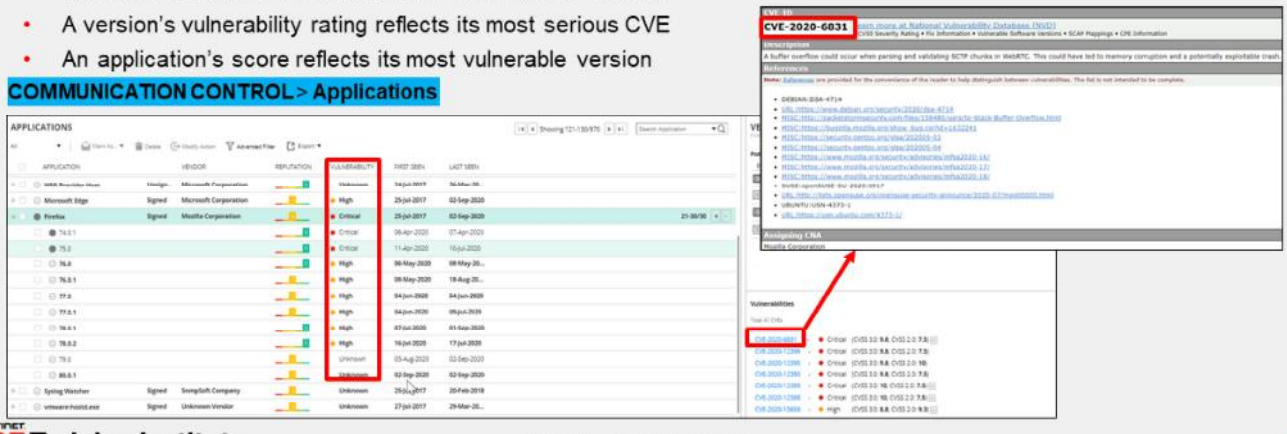
Vouchers & Dumps are Available | WhatsApp +201224560923

DO NOT REPRINT Brave-dumps.com
© FORTINET

Vulnerability Assessment

- FortiEDR displays CVE data for every communicating application in your organization
  - Based on known CVEs, each application version is assigned a vulnerability rating from **Unknown** (no known vulnerabilities) to **Critical** (highly exploitable)
  - CVEs apply to individual versions
  - Click a version to view its CVEs
  - Click a CVE number to view details on an external website
  - A version's vulnerability rating reflects its most serious CVE
  - An application's score reflects its most vulnerable version

COMMUNICATION CONTROL > Applications



NSE Training Institute

© Fortinet Inc. All Rights Reserved.

9

Vulnerability scores are another great tool for evaluating risks in your environment. Fortinet uses up-to-the-minute CVE data to assign a vulnerability score to each application version. Vulnerability scores range from unknown (no known vulnerabilities) to critical (highly exploitable vulnerabilities). As with reputation scores, the application's vulnerability score reflects its most vulnerable version. That's why in this example, Firefox is listed as **Critical**, even though some versions shown here have a high vulnerability score, and others have no known vulnerabilities. Click a version to view a list of known vulnerabilities and their severity. In the example shown on this slide, one of the versions with critical vulnerabilities is selected. You can see which version is selected by checking at the top of the **Version Details** pane. You can see that there are 41 known CVEs. Remember, vulnerabilities are version-specific, so you won't see any vulnerabilities if you highlight an application and not a specific version. If you click on a CVE identifier, you can view all the details about that CVE on an external website. Notice that not all the vulnerabilities are critical in this case. FortiEDR bases a version's score on its most exploitable vulnerability. Again, this draws your attention to potential problems. A version with at least one critical CVE is rated as **Critical**, and an application with at least one critical version is rated *critical*. As a reminder, you can only see vulnerability data if you have a Predict and Protect or Predict, Protect and Response license.

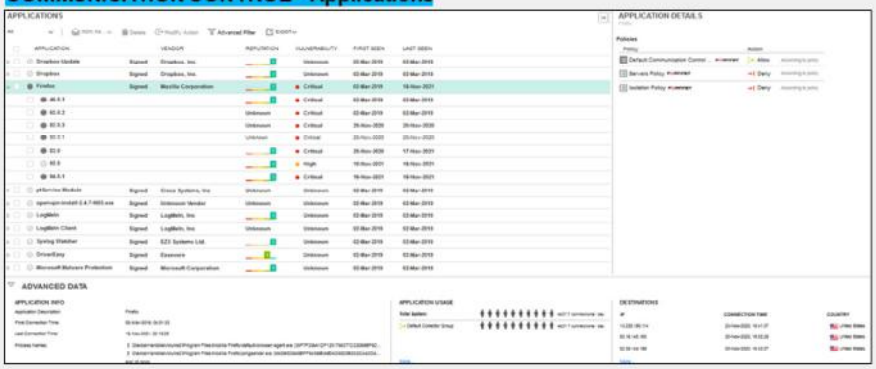
Vouchers & Dumps are Available | WhatsApp +201224560923

DO NOT REPRINT Brave-dumps.com
© FORTINET

The Applications Subtab

- **Version Details** or **Application Details** shows details about the highlighted application or version
  - View the assigned action (**Allow** or **Deny** communication) for the highlighted application or version in each communication control policy
  - View a list of known vulnerabilities, if any, in the highlighted version
- The applications list identifies all applications in your organization *that have communicated externally*
  - Versions are nested under each application
  - For each application and version, you'll see:
    - Vendor
    - Reputation score
    - Vulnerability rating
    - First and last dates it tried to communicate

COMMUNICATION CONTROL > Applications



NSE Training Institute

© Fortinet Inc. All Rights Reserved.

10

Now you will learn about the **COMMUNICATION CONTROL** in the management console. Start with a very high-level overview of the **Applications** subtab. You can access this screen by clicking the **COMMUNICATION CONTROL** tab and selecting **Applications**. The first thing you notice is the applications list. The applications list identifies all applications in your organization that have communicated externally. If an application has never tried to establish a connection, it won't show up here. Click an application to view all the versions of that application that have communicated from your environment. For each application and each of its versions, you see the vendor, the reputation score, the vulnerability rating, and the first and last dates it tried to communicate.

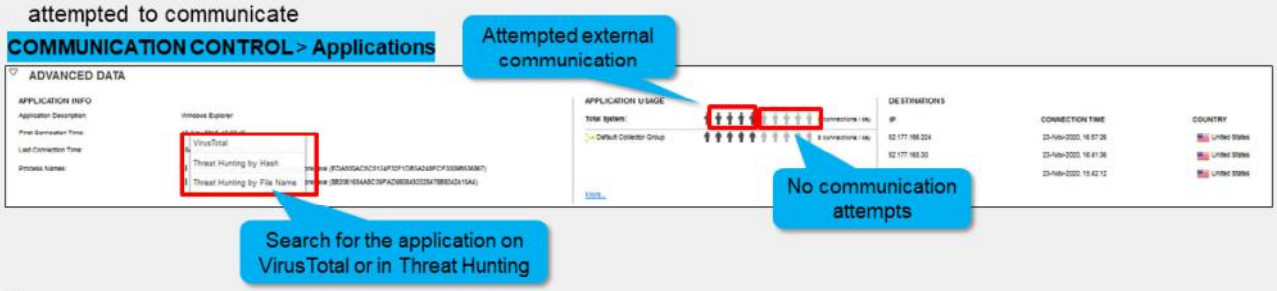
On the right, you see the **Version Details** or **Application Details** pane, depending on whether you highlighted an application or a specific version. The application and version, if applicable, are shown at the top. Below that, you can see the assigned action for the highlighted application or version in each communication control policy. In this example, you are looking at information about a specific version of Dropbox, which is allowed in three of the policies shown and denied in one. You can scroll down to see more policies. Underneath the policies information is the **Vulnerabilities** pane. If the highlighted version has known CVEs, you see them listed here. If there are no known vulnerabilities, or you have selected an application but not a specific version, you don't see this panel.

Vouchers & Dumps are Available | WhatsApp +201224560923

DO NOT REPRINT Brave-dumps.com
© FORTINET

Advanced Application Data

- **Application Usage**
  - View the percent of collectors that attempted to communicate externally through the selected application
  - View the total number of connections per day for the selected application or version
  - Click **More** to view additional details
- **Destinations**
  - View the last five IP addresses with which the selected application or version communicated or attempted to communicate
- Select an application or version from the applications list to view detailed information
- **Application Info**
  - View high-level information about the selected application
  - Click the vertical ellipsis (⋮) next to the process name to search for the application
    - on VirusTotal
    - in Threat Hunting by Hash
    - in Threat Hunting by File Name



© Fortinet Inc. All Rights Reserved.

You can see more details about the highlighted application in the **Advanced Data** panel. The **Application Info** section shows you the following high-level information about the selected application: a brief description, the first and last connection time, and the process name. If you click the vertical ellipsis to the left of the process name, you can search for the application on VirusTotal, or you can search the threat hunting database by hash or file name.

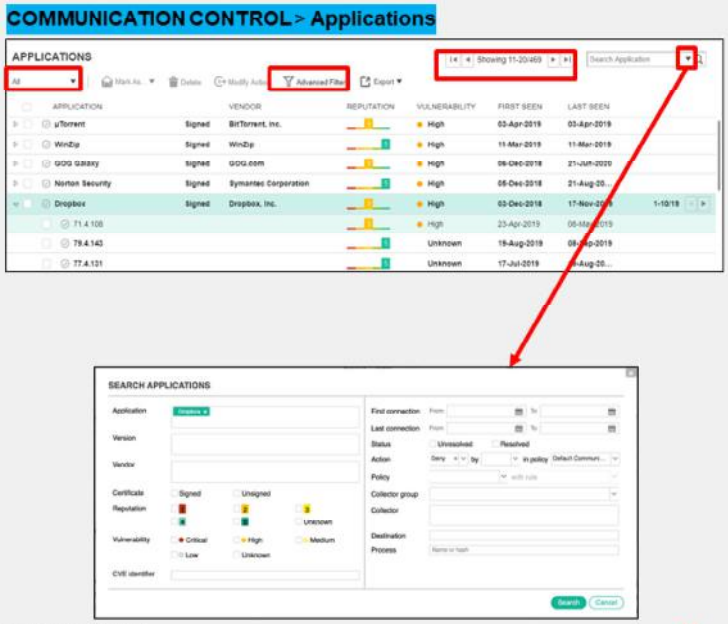
In the **Application Usage** section, you can view the total number of connections per day for the selected application, and the distribution across collector groups. If you click **More,** you can see details, such as the device names, and you can export the details to an Excel file. In the **Destinations** section, you can view the last five IP addresses with which the selected application communicated. You can also click **More** to see a more complete list of up to 50 destinations, and export the list to a Microsoft Excel file.

Vouchers & Dumps are Available | WhatsApp +201224560923

DO NOT REPRINT Brave-dumps.com
© FORTINET

Navigating the Applications List

- Filtering applications
  - Use the status filter to view:
    - **Unresolved** or **Resolved** applications
    - **Unknown Vendors**
    - **Low Reputation**
    - **Critical CVE**
    - **Unread**
    - **All**
  - Use the **Advanced Filter** to customize your filter rules and edit rules
- Browsing and sorting applications
  - By default, applications are listed by the date they were first seen
  - Click on a column header to sort by that column
  - Use the arrows at the top to browse applications
- Searching for applications
  - Enter a search term in the search bar
  - Click the gray arrow in the search bar to do an advanced search
  - Click the **X** inside the search bar to clear results and show all items



NSE Training Institute

© Fortinet Inc. All Rights Reserved.

12

Take a look at how to navigate the applications list. First, you can sort applications. By default, applications are listed by the date they were first seen communicating. Click on a column heading if you want to sort by a different criteria. Then, use the arrows at the top to browse through the list. The applications list displays ten applications at a time.

You can also filter the applications list to focus on a particular set. Use the status filter at the top left to view only resolved or unresolved applications, applications with unknown vendors, low reputations, or critical CVEs, unread applications, or all applications. The advanced filter allows you to customize your filter and create a rule based on that filter. You'll learn more about how to do that later in this lesson.

Lastly, you can use the search feature. You can enter a search term right into the search bar, or click the gray arrow on the right side of the search bar to do an advanced search. In the **Search Applications** window, you can use any combination of the criteria you see in the image on the lower right: application name, vendor, and version, certificate status, reputation, connection dates, selected action, and so on. When you are finished, click the **X** in the search bar to clear the results.

Vouchers & Dumps are Available | WhatsApp +201224560923

DO NOT REPRINT Brave-dumps.com
© FORTINET

Understanding Reputation Scoring

- Reputation-based analysis
  - Each version of an application is assigned a score from **1** (known bad) to **5** (trusted)
  - You can configure rules to automatically block application versions with a low reputation score
  - Management console users can quickly identify potential threats
- An application reputation score is based on the *lowest score* of the application versions
  - If a generally trusted application, such as Microsoft Office, has a lower-than-expected score, it may have vulnerabilities in a particular version, which is reflected in the application score
  - This score may not reflect the reliability of other versions of the application
  - If a generally reliable application has a vulnerable version, you can block that version from communicating while allowing safer versions of the application to operate normally

COMMUNICATION CONTROL > Applications

Microsoft Office	Microsoft Corporation	3	Unknown	13-Jun-2017	03-Jan-2020	110/141
16.0.11629.20196	Signed	3	Unknown	03-Jun-2019	26-Jun-2019	
16.0.11629.20210	Signed	5	Unknown	06-Jun-2019	26-Jun-2019	
16.0.11629.20214	Signed	5	Unknown	09-Jun-2019	25-Jun-2019	
16.0.11629.20246	Signed	5	Unknown	15-Jun-2019	01-Jul-2019	
16.0.11629.20244	Signed	5	Unknown	16-Jun-2019	05-Jul-2019	
16.0.11727.20188	Signed	5	Unknown	26-Jun-2019	11-Jul-2019	
16.0.11727.20086	Signed	5	Unknown	26-Jun-2019	26-Jun-2019	

NSE Training Institute

© Fortinet Inc. All Rights Reserved.

13

Take a closer look at reputation scores. The reputation score is useful when you are deciding which applications and versions should be allowed to communicate. Each new hash is sent to the reputation service, which sends back a score on a scale of 1 (bad) to 5 (trusted). The score is displayed in the applications list, so you can quickly identify potential threats. You can set up rules to block communication from application versions with low reputation scores.

Notice that each application version has its own reputation score. The application score is based on the *lowest* reputation score of its versions. So, in this example, you can see that Microsoft Office has a score of 3, meaning there is mixed evidence about its reliability. Microsoft Office is a well-known and trusted application, and you can see that it's signed by Microsoft, so why would it have a low score? Take a look at the versions. Most of them are rated 5, but one older version, shown at the top of the list, is rated 3. The lowest score is applied to the application so that management console users are alerted to any potential issues. In other words, a low-scoring application is a signal that you should check for insecure application versions, but there may be other versions of the same application that are safe. You can deny communication from a particular version of an application. In this case, you may choose to block the version with a possible problem, but allow all the others that are rated 5.

Vouchers & Dumps are Available | WhatsApp +201224560923

DO NOT REPRINT Brave-dumps.com
© FORTINET

Understanding Communication Control Policies

- Configure rules to automatically block communication from current and future applications and versions based on:
  - Reputation score
  - Vulnerability rating
  - Vendor
- Console users may also manually allow or block individual applications or versions as needed
- Each collector group is assigned to one communication control policy
  - You can assign more than one collector group to the same policy
- Create exceptions to the default by denying or allowing communication from applications or specific versions
- Applications are allowed or denied on a per-policy basis
  - An application may be allowed in one policy but denied in another
  - Each policy has a default action:
    - **Allow** for the Default Communication Control policy and its clones
      - Recommended in most cases
    - **Deny** for the Servers Policy, Isolation Policy, and their clones
      - Use for special cases only

COMMUNICATION CONTROL > Policies

NSE Training Institute
© Fortinet Inc. All Rights Reserved.

Communication control policies are found on the **Policies** subtab in **COMMUNICATION CONTROL**. They determine whether or not an application or version can communicate. Each policy has a preset default action of **Allow** or **Deny**. You can determine the default action of a policy by the icon to the left of the policy name in the list. A gray icon means the policy allows communication by default. A white icon means the policy denies communication by default. You can also see the default policy action by clicking the policy to view its details. In the example shown on this slide, the **Default Communication Control Policy** is selected and the default action is **Allow**. This policy is one of the three built-in policies. The other built-in policies, the Servers Policy and Isolation Policy, have a default action of **Deny**. These are special cases where higher security outweighs potential productivity inhibitors. Most policies should have a default action of **Allow**.

For each policy, you can create exceptions to the default action. For example, if the default action is **Allow**, you can block individual applications or versions from communicating. You will learn more about this process in detail later in this lesson.

There are two ways to set an exception. First, you can create policy rules. Rules allow you to automate communication control. Decide on a set of criteria, and FortiEDR will automatically deny communication from any application or version, current or future, that fits your criteria. You can configure rules based on reputation score, vulnerability rating, or vendor. Console users can also manually allow or block applications or versions as needed. So, if an application has a reputation score of three, but it's on your company's block list, you can set it to **Deny**.

Communication control policies are assigned at the collector group level. Each collector group is assigned to one policy—by default, the **Default Communication Control Policy**. A policy can have as many groups assigned to it as you want. Applications are allowed or denied per policy, so an application may be allowed to communicate in one policy but denied in another. For example, you might allow a specific application for most users, but deny it for HR because they handle sensitive data. Again, Fortinet strongly recommends allowing communication by default in all client policies.

Vouchers & Dumps are Available | WhatsApp +201224560923

DO NOT REPRINT Brave-dumps.com
© FORTINET

Built-In Communication Control Policies

- **Isolation Policy**
  - Automatically applied to any collectors placed in isolation mode
  - You can't assign collector groups to this policy
  - Denies all applications by default
  - Allows only applications or tools that are needed to investigate and remediate the device
- **Default Communication Control Policy**
  - The default policy for all collector groups
  - Allows all applications to communicate by default
  - Blocks unsafe vendors, applications, or versions from communicating externally
- **Servers Policy**
  - Denies all applications by default
  - Allows applications that are needed to run your servers
  - FortiEDR automatically allows certain applications that are known to be safe
    - Example: applications signed by Microsoft

COMMUNICATION CONTROL > Policies

POLICY NAME	RULE	AFFECTED APPS	ACTION	STATE
Default Communication Control Policy		Total: 18 denied apps By user: 1 Allow, 2 Deny		
	Reputation is less than or equal to 1	7 applications	Deny	Disabled
	Vulnerability is greater than or equal to Critical	18 applications	Deny	Disabled
	Vendor is within 3 vendors	16 applications	Deny	
	Default rule (if none of the rules apply)	952 applications	Allow	
Servers Policy		Total: 778 denied apps By user: 0 Allow, 0 Deny		
Isolation Policy		Total: 966 denied apps By user: 1 Allow, 0 Deny		

NSE Training Institute

© Fortinet Inc. All Rights Reserved.

15

As you learned previously, FortiEDR comes with three built-in communication control policies: **Default Communication Control Policy**, **Isolation Policy**, and **Servers Policy**. When you create a collector group, it is automatically assigned to the **Default Communication Control Policy**. By default, it allows all applications to communicate. That default can't be changed, but you can choose to block communication from unsafe or undesirable applications or versions.

The second built-in policy is the **Servers Policy**. This is one of the few cases where communication is denied by default, because servers require a much higher degree of protection. FortiEDR automatically unblocks some common applications that are definitely safe, like applications that are signed by Microsoft. Review the list of applications and allow anything you need to run your servers.

Lastly, there is the **Isolation Policy**. The **Isolation Policy** is different from other policies because you can't assign collector groups to the **Isolation Policy**. If a device is infected and put into isolation mode, that collector is automatically be assigned to the **Isolation Policy**, no matter what group it belongs to. Isolation is another rare policy where **Deny** is the default setting. Isolation mode is a temporary state intended to contain any infections until the device is remediated. This means the device can't be connecting to the network trying to spread its infection. You should allow only applications that are needed to investigate and remediate the device.

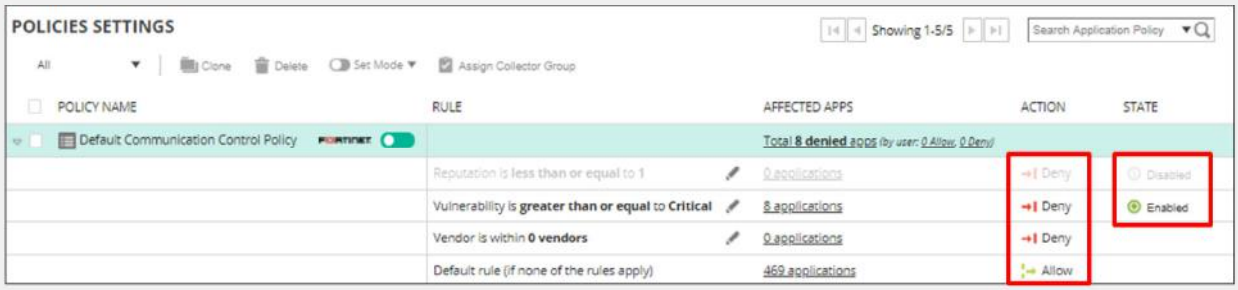
Vouchers & Dumps are Available | WhatsApp +201224560923

DO NOT REPRINT Brave-dumps.com
© FORTINET

Communication Control Rules

- Reputation and vulnerability rules are disabled by default
  - Click the **Disabled** icon in the **State** column to enable a rule
  - Editing a rule automatically switches its state to **Enabled**
- Each communication control policy has built-in policy rules
- The rules vary depending on the default action of the policy:
  - If the default action is **Allow**, you can set exceptions for applications with low reputation scores, poor vulnerability ratings, or by vendor
  - If the default action is **Deny**, you can set exceptions for specific trusted vendors

COMMUNICATION CONTROL > Policies



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

Now take a closer look at how policy rules work. As you learned on earlier, you can use rules to proactively reduce your attack surface. Rules apply to existing applications *and* to applications that haven't been installed in your network yet, even ones that haven't been developed yet.

Each policy has three rules: one based on reputation score, one on vulnerability rating, and one on vendor. Rules create exceptions to the default action. That means if a policy allows communication by default, which should apply to nearly all your collectors, you can use rules to deny unsafe applications or unsafe vendors. If the default action is deny, like the **Servers Policy**, you can use rules to allow communication from trusted vendors.

By default, the reputation and vulnerability rules are disabled. You can enable one or both rules by clicking on the **Disabled** icon in the **State** column. You can toggle between **Enabled** and **Disabled**. Editing a rule will automatically set its state to **Enabled**.

Vouchers & Dumps are Available | WhatsApp +201224560923

DO NOT REPRINT
© FORTINET
Brave-dumps.com

Knowledge Check

1. What is the reputation of an application if it is assigned a score of 1?
   - ✓ A. Bad
   - B. Trusted
2. Which policy cannot have collector groups assigned to it?
   - ✓ A. Isolation
   - B. Servers

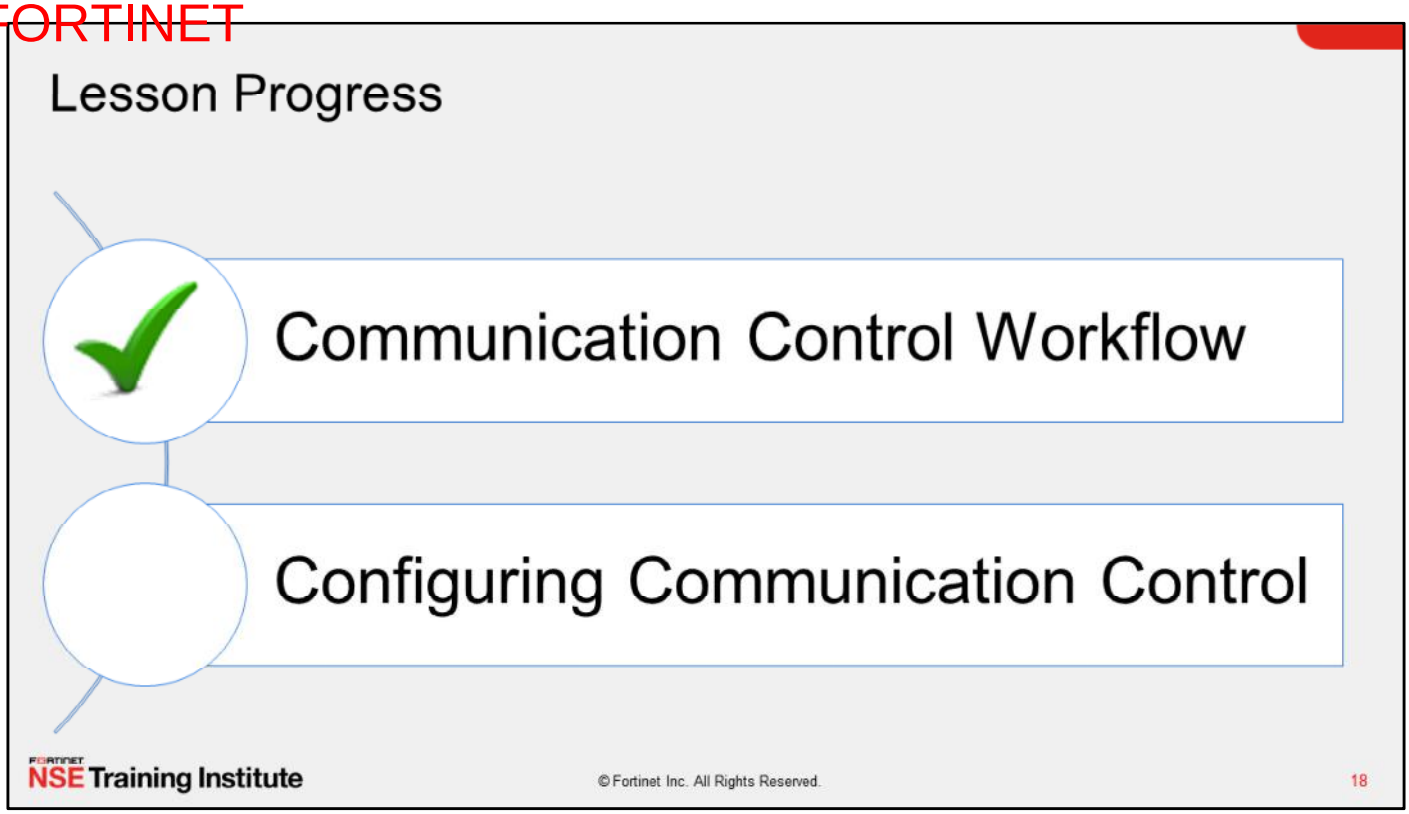
NSE Training Institute

© Fortinet Inc. All Rights Reserved.

17

Vouchers & Dumps are Available | WhatsApp +201224560923

DO NOT REPRINT Brave-dumps.com
© FORTINET

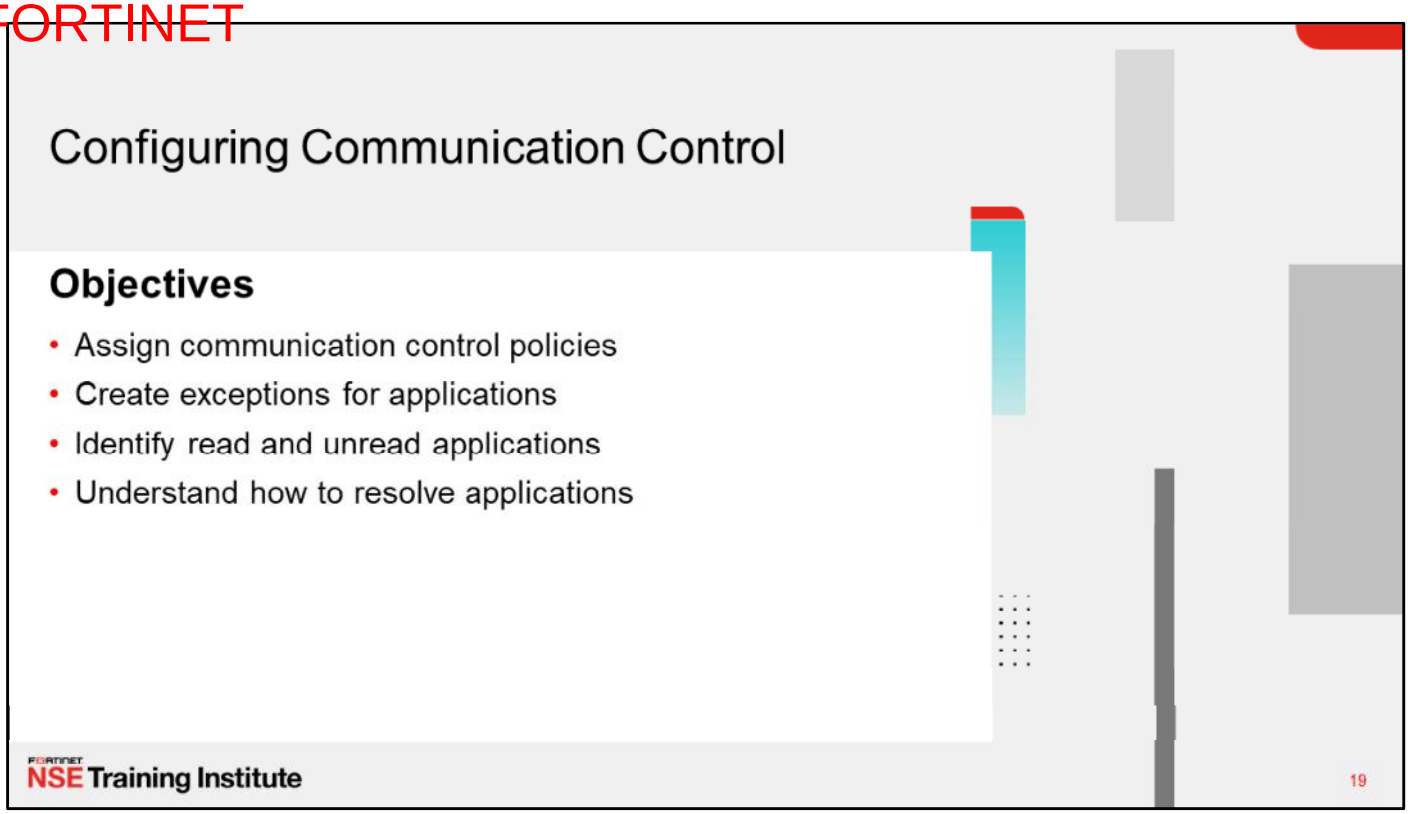


Good job! You now understand the communication control workflow.

Now, you will learn about configuring communication control policies.

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.

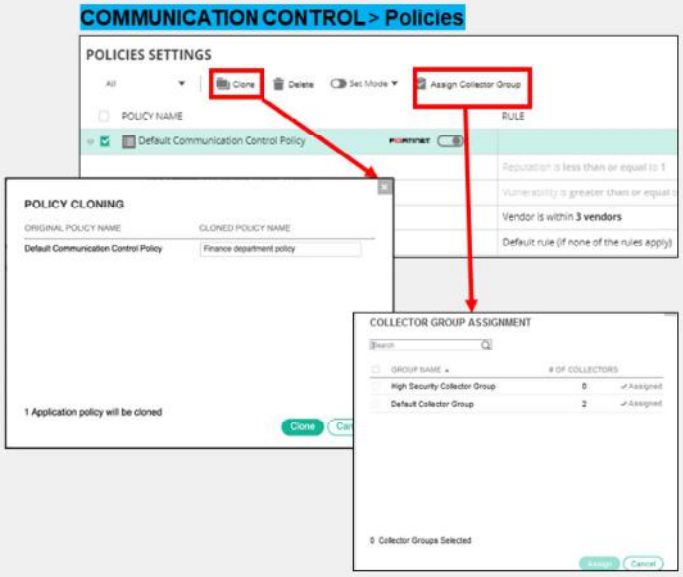
By demonstrating competence in communication control policy configuration, you will understand how they work and be able to fine-tune them.

Vouchers & Dumps are Available | WhatsApp +201224560923

DO NOT REPRINT Brave-dumps.com
© FORTINET

Creating a Communication Control Policy

- Create a new policy if you want to assign different policies to different collector groups
  - For example, you may want to create a separate, more restrictive policy for a finance or HR group
  - Fortinet recommends creating a simulation policy for troubleshooting
- Clone an existing policy to use its settings
  - On the **Policies** subtab, select the checkbox for the policy you want to clone, and click **Clone**
  - After you clone a policy, you can adjust its settings as needed



© Fortinet Inc. All Rights Reserved.

How do you create a communication control policy? As you learned earlier, create additional policies if you want to allow different applications for different groups of users—for example, if you want to restrict your finance department more than your other users. Fortinet also recommends creating a simulation policy to help you troubleshoot potential blocking issues.

To create a new policy, clone an existing one. Select the checkbox next to the policy you want to clone and click **Clone**. The new policy has the same settings—all the same blocked and allowed applications—as the original, and you can change the policy rules and actions as needed. Note that you can't change the default action for your new policy, so make sure you clone a policy with the desired default action. In almost all cases, that means you should clone the **Default Communication Control Policy** or a previously created clone.

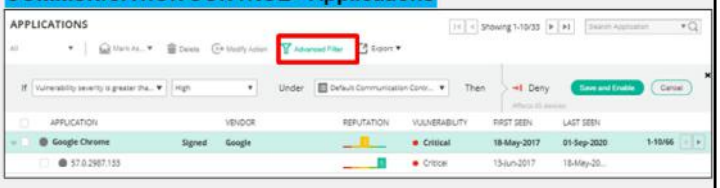
Vouchers & Dumps are Available | WhatsApp +201224560923

DO NOT REPRINT Brave-dumps.com
© FORTINET

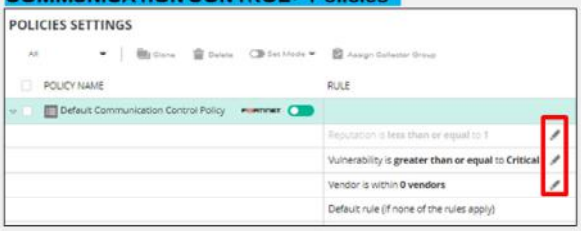
Editing Communication Control Rules

- Reputation and vulnerability rules
  - On the **Applications** subtab:
    1. Click **Advanced Filter**
    2. Select filter criteria
    3. Click **Setup rule**
    4. Select a policy from the drop-down list
    5. Click **Save and Enable**
  - On the **Policies** subtab:
    1. Click the pencil icon in the rule's row
    2. You will see the applications list with the advanced filter displaying the current rule parameters
    3. Edit the criteria as needed
    4. Click **Save and Enable**

COMMUNICATION CONTROL > Applications



COMMUNICATION CONTROL > Policies



NSE Training Institute

© Fortinet Inc. All Rights Reserved.

21

Rules have a default configuration, which you can edit as needed. There are a few ways to do this. If you are editing a rule based on reputation or vulnerability, you can edit it from the **Applications** subtab by using the **Advanced Filter**. In the example shown on this slide, the list is filtered to show only applications whose vulnerability severity is high or greater. Click **Setup rule** to see a drop-down list of all the available policies for that criteria. For this example, you can choose any policy with a default action of **Allow**. You can see that the **Default Communication Control Policy** is selected. After you select a policy, just click **Save and Enable**. Note that each policy has only one rule based on each criteria, so you're replacing the existing rule criteria, not creating a new one. In this example, you have changed the vulnerability rule to block anything with a high or critical vulnerability rating rather than the default setting, which only blocks critical vulnerabilities.

You can also edit a rule from the **Policies** subtab by clicking the pencil icon in its row. You'll see the applications list with the **Advanced Filter** set to display the current rule parameters. Change the parameters as needed, then click **Save and Enable**. Be aware that each policy has its own set of rules, so if you created multiple policies you'll have to edit them all separately if needed. That means you can apply stricter rules to groups that require more security.

Editing vendor rules is a different process. You can open the **Exclude Vendors** window by clicking the pencil icon in the rule's row or by selecting **Vendor** in the **Advanced Filter** drop-down list. Select the checkboxes next to each vendor that should be treated as an exception—denied in standard policies or allowed in server or isolation policies. Each vendor has a **Signed** and **Unsigned** checkbox, so you could deny all unsigned applications for a group that handles sensitive data, or allow only signed applications from trusted vendors in the **Servers Policy**.

Vouchers & Dumps are Available | WhatsApp +201224560923

DO NOT REPRINT Brave-dumps.com
© FORTINET

Policy Modes and Rule States

- Review: Policy modes determine whether or not a policy is enforced
  - Policies in simulation mode do not block any application from communicating (default for most policies)
  - Policies in prevention mode block communication based on your chosen settings and rules
  - Click on the mode slide for a policy to toggle between simulation and prevention mode
  - The **Isolation Policy** is always in prevention mode
- Rule states determine whether a rule is enforced or completely ignored
  - Disabled rules are never enforced
  - Enabled rules are enforced *if the policy is in prevention mode*
  - Click on the policy **STATE** to toggle between **Enabled** and **Disabled**

COMMUNICATION CONTROL > Policies

NSE Training Institute

© Fortinet Inc. All Rights Reserved.

22

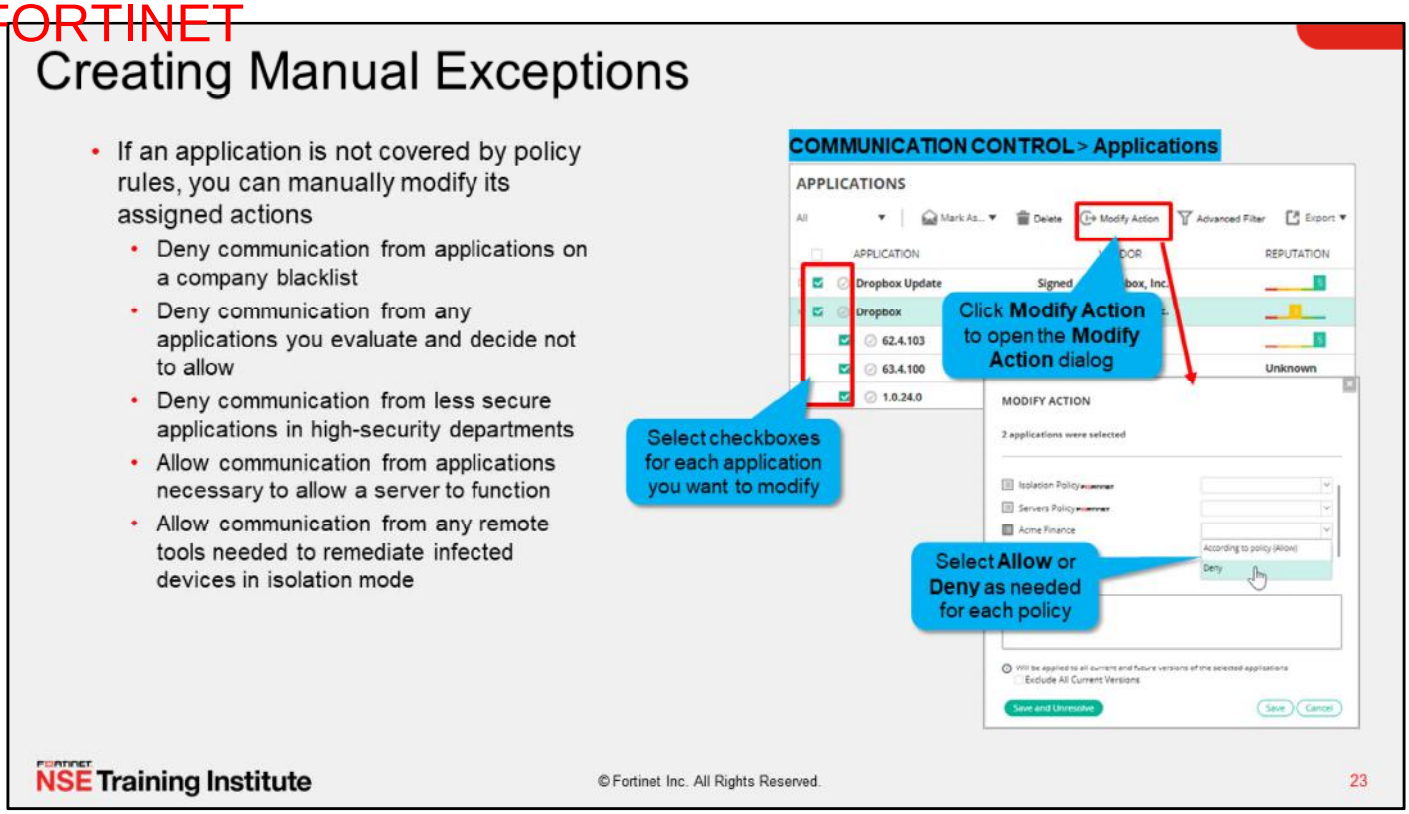
Just like security policies, communication control policies can be in simulation or prevention mode. In simulation mode, no applications are blocked from communicating. In prevention mode, communication is allowed or denied based on the settings you've chosen. Out of the box, policies are in simulation mode. You can enable them when you finish the tuning phase, which you'll learn about later in this lesson. The exception is the **Isolation Policy**. As you learned earlier, this policy works differently from the others. One of the things that are different is its mode, which is permanently set to prevention mode. This is to ensure that infected devices that have been placed in isolation mode are always protected and contained.

Rules also have their own states that you can enable or disable. Reputation and vulnerability-based rules are disabled out of the box. That means they are not enforced, regardless of the selected policy mode. When you decide on the right settings for a policy rule, click the state icon at the end of the row to enable it. It's a toggle, so click the disabled icon (gray and white) to enable a rule, or click the enabled icon (a green target) to disable it. Once you have enabled a rule, it is enforced, but only if the policy is in prevention mode. If the policy is in simulation mode, the rule is not enforced.

In other words, if you want to enforce a rule, make sure its state is enabled and its policy is in prevention mode.

Vouchers & Dumps are Available | WhatsApp +201224560923

DO NOT REPRINT Brave-dumps.com
© FORTINET



Now take a look at how to change an action manually. You only need to change an action for an application or version if it isn't covered by an existing rule and you want to create an exception. There are a number of circumstances where this might be needed. First, if an application has no serious vulnerabilities and a reputation score of 3 or better, but it is on a pre-existing company block list, you must manually change its action to **Deny**. You must also manually change the action of an application to **Deny** if you evaluated it during the tuning process and decided to block it, or if you decided to block it in high-security environments while allowing it in other areas. In the **Servers Policy**, you must change an application's action to **Allow** if it is necessary for the server to function, while in the **Isolation Policy**, you should set the action of an application to **Allow** if it is needed for remote investigation and remediation.

You can change the action of an application for a single policy or several at once. Just select the checkbox for the application to select all versions, or select individual versions, then click **Modify Action**. For client policies like the **Default Communication Control Policy**, where the default action should be **Allow**, select **Deny** from the drop-down list next to each policy where you want to block the selected application or versions. If you select the application and all its versions, the exception is applied to all current and future versions. In the example shown on this slide, all versions of Dropbox and Dropbox Update are blocked from the **Acme Finance** policy. Dropbox is not an inherently dangerous application; in fact, you can see in the example on this slide that the version on the top has a reputation score of 5. In general, it's a known and trusted entity. But in this case, you don't want to allow file sharing applications like Dropbox in sensitive environments like the finance department, so you must change it to **Deny** in that policy. Users assigned to the default policy can still use Dropbox.

The process for setting exceptions in the **Servers Policy** and **Isolation Policy** is the same, except that you select **Allow** from the policy drop-down list rather than **Deny**.

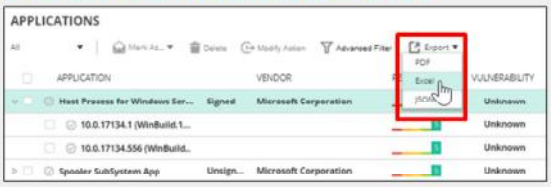
Vouchers & Dumps are Available | WhatsApp +201224560923

DO NOT REPRINT Brave-dumps.com
© FORTINET

Applications Reports

- Applications reports are useful for evaluating communication control policies
- To generate a report:
  - In the applications list, do one of the following:
    - Filter or use the search options to narrow the list to only the applications you want to export
    - Select the checkboxes of the applications you want to export
    - Use no filters or search terms to export the full applications list
  - Click **Export**, then select the file type: PDF, Excel, or JSON
  - When the report is generated, click the blue **Download** link to save the report to your hard drive

COMMUNICATION CONTROL > Applications

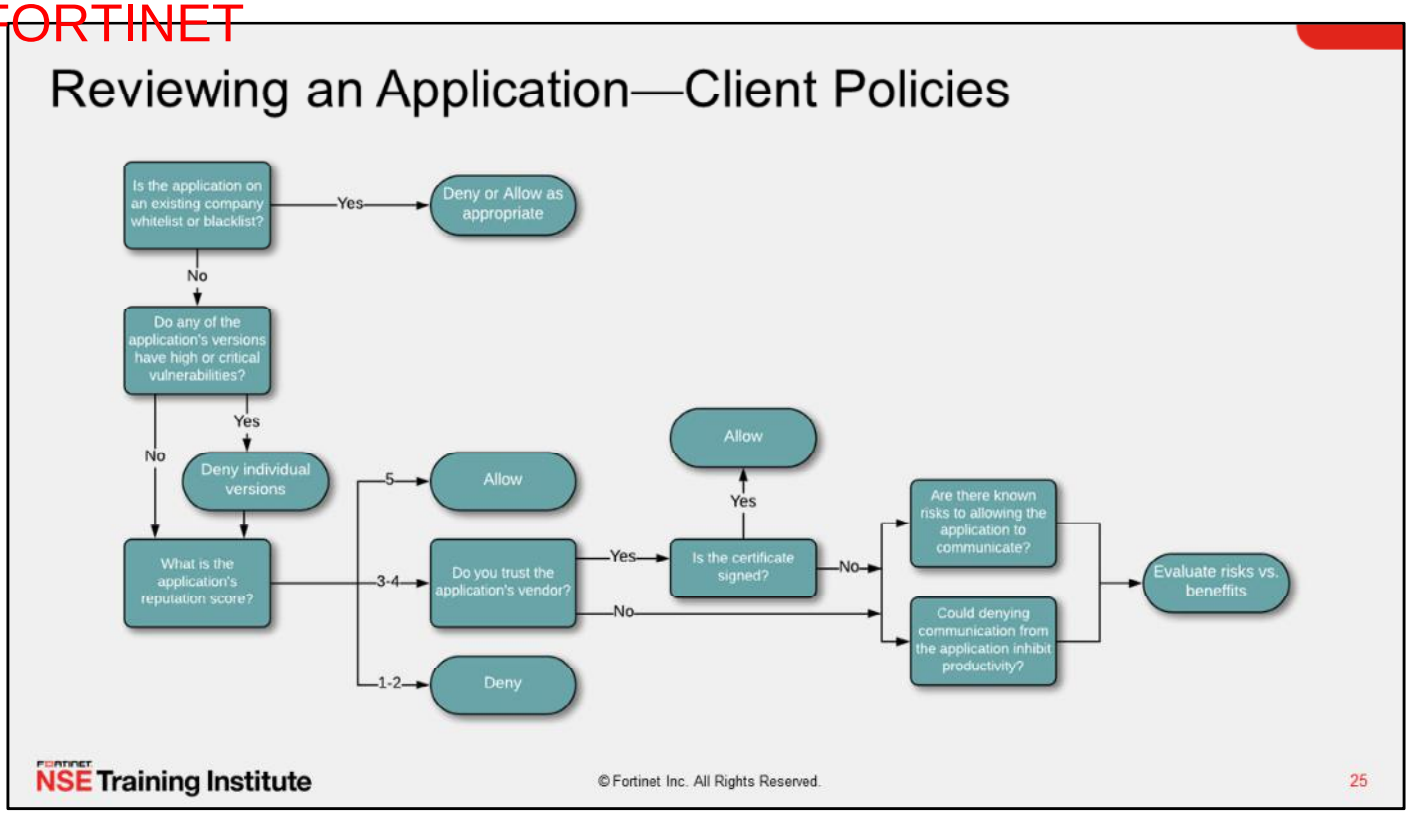


NSE Training Institute
© Fortinet Inc. All Rights Reserved.

The applications report is a great tool for evaluating communication control policies. When you generate a report, the list reflects the applications shown in the selected view. For example, if you do a search, the report includes only the results of the search. The same thing occurs if you filter the list; if you show only unresolved applications, the report shows only the unresolved applications. You can also manually select checkboxes for specific items to export a small set of applications. If you want a complete report, set the filter to **All**, clear any search results, and clear the checkboxes of any applications. After you have got the list you want to export, click **Export** at the top of the applications list, and then select a format. You can export to PDF, Excel, or JSON. A pop-up window opens, showing the progress. After your report is ready, click the blue **Download** link and save it to your hard drive.

Vouchers & Dumps are Available | WhatsApp +201224560923

DO NOT REPRINT Brave-dumps.com
© FORTINET



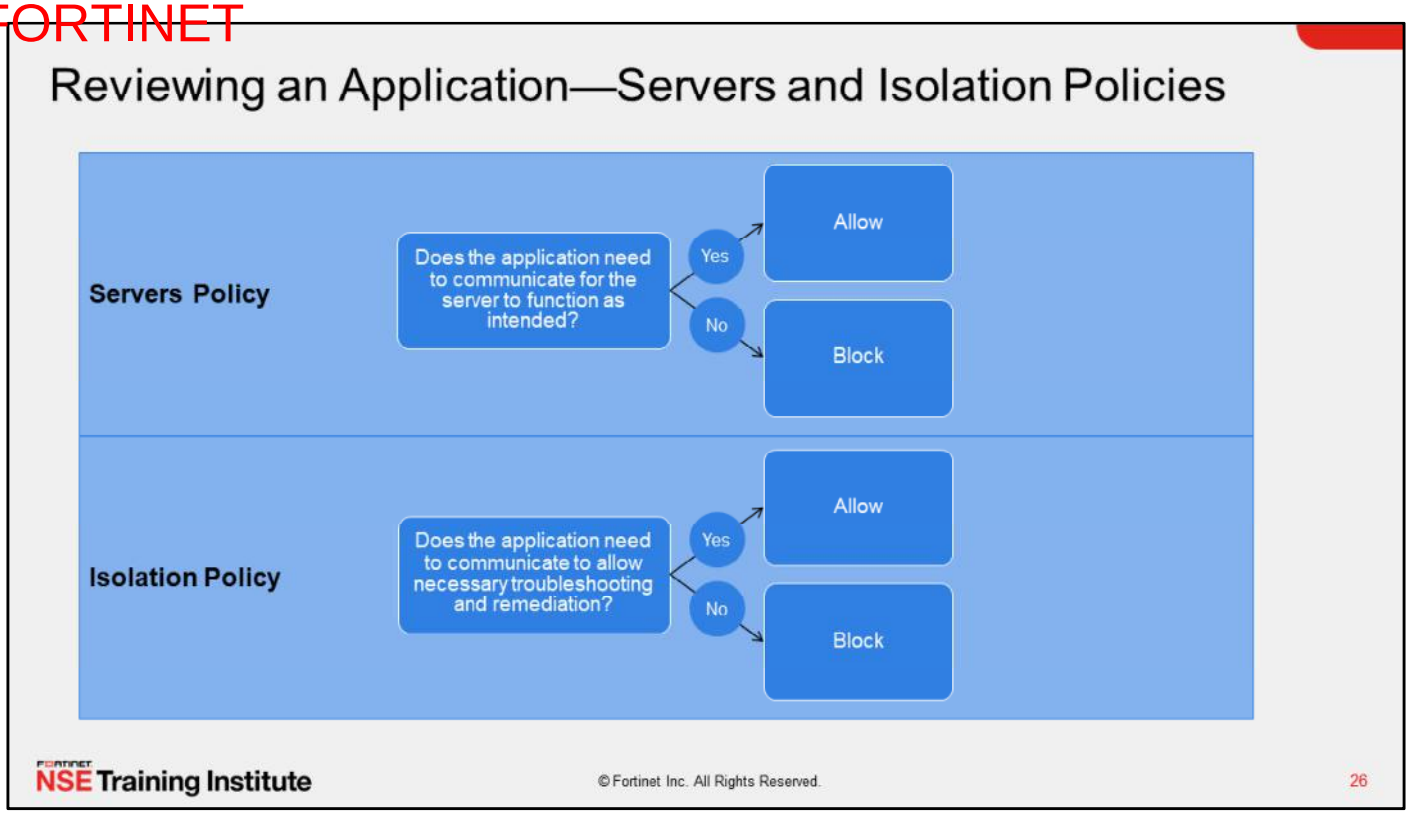
Now take a closer look at the decision-making process for general client policies. These are the policies applied to most of your users, where the default action is allow. For each application, ask these questions as you decide whether to allow or deny the application. First, is the application on an existing blocklist or allowlist? If it is, you can use that list to make your decision.

If not, the first thing to look at is the vulnerability rating of the application, if you have access to it. If the rating is *critical* or *high*, block communication from the versions with known CVEs. Remember, you can configure rules to do this step for you automatically, so this should just be a double check.

Next, check the reputation score. Block anything scored 1 or 2, and allow anything scored 5. Again, you can set rules within your policy to automatically block anything with a poor reputation. If it's in between, or marked **Unknown**, the next question is: Do you trust the vendor? If you do, check whether the certificate is signed. If it is, you can allow the application. If it's unsigned, or if you don't necessarily trust the vendor, then evaluate the risks and benefits. Are there known risks in allowing the application to communicate? And does blocking the application from communicating cause any potential productivity inhibitors? Use your judgement. You may want to research the application online to see if other companies trust it.

Vouchers & Dumps are Available | WhatsApp +201224560923

DO NOT REPRINT Brave-dumps.com
© FORTINET



The process for reviewing **Servers Policy** and **Isolation Policy** is pretty straightforward. When reviewing the **Servers Policy**, you need to ask one question: Does the application need to communicate to allow the server to function as intended? If yes, change the action to **Allow**. If the server can function without it, leave it at **Deny**.

The process for reviewing the **Isolation Policy** is similar. You need to know whether the application needs to communicate to allow necessary troubleshooting and remediation of infected devices. If the answer is yes, change the action to **Allow**. If the answer is no, leave it at **Deny**.

Vouchers & Dumps are Available | WhatsApp +201224560923

DO NOT REPRINT Brave-dumps.com
© FORTINET

Read or Unread

- Unread applications and versions are displayed in **bold**
  - Read applications and versions are displayed in plain text
- Versions are marked as read when you click them
  - An application is marked as read when all of its versions are read
- You can use the **Mark As** menu to change the read/unread status of applications or versions
  1. Select the checkbox or checkboxes
  2. In the **Mark As** drop-down list, select **Mark as read** or **Mark as unread**

NSE Training Institute

© Fortinet Inc. All Rights Reserved.

27

Application versions are marked as read after you view their details. Unread applications are displayed in bold, while read applications are in plaintext. An application is marked as read when all its versions have been read. You can change the status of an item by selecting its checkbox and selecting choose **Mark as read** or **Mark as unread** in the **Mark As** drop-down list. For example, you might want to mark an application as read without clicking every version, or you might mark an application as unread if you want someone else to look at it.

Vouchers & Dumps are Available | WhatsApp +201224560923

DO NOT REPRINT Brave-dumps.com
© FORTINET

Marking an Application as Resolved

- When you review an application and apply any necessary policy changes, mark it as resolved
  - Resolving applications tells other management console users that you have already evaluated the application
- Mark an application or version as resolved in the **Modify Action** window
  - Do one of the following to open the **Modify Action** window:
    - Click the **Unresolved** icon (●)
    - Select the checkbox next to an item, and then click **Modify Action**
  - In the **Modify Action** window:
    - Change assigned actions if needed
    - Enter a comment explaining how and when you resolved the application
    - Click **Save and Resolve**
- Fortinet Cloud Service (FCS) may also mark a version as resolved after evaluating its reputation and known CVEs
  - FCS may subsequently mark as unresolved if new vulnerabilities are discovered

NSE Training Institute

© Fortinet Inc. All Rights Reserved.

28

To remove an application or version from the *to-review* list, you must change the status of that item.

After you review an item and make necessary policy changes, mark it as resolved. Marking an item as resolved tells other users that they don't need to review that item.

To resolve an item, open the **Modify Action** window. You can open the window by clicking the gray **Unresolved** icon beside the application or version or by selecting the checkbox and clicking **Modify Action**. You can streamline your workflow by clicking **Save and Resolve** after you change the action associated with an item. If you don't need to change the action, use the same process, but don't make any changes. You can type a note, if needed, and click then **Save and Resolve**. Be aware that if the **Applications** filter is set to show only unresolved events, an application does not show in the list after you mark it as resolved. If you need to find it again, you can change the filter to show all.

FCS may also mark a version as resolved after evaluating its reputation and known CVEs. If new vulnerabilities are discovered, FCS may mark the version as unresolved, putting it back on your review list.

Vouchers & Dumps are Available | WhatsApp +201224560923

DO NOT REPRINT Brave-dumps.com
© FORTINET

Knowledge Check

1. Isolation policy is always set in which mode?
   A. Simulation
   ✓ B. Prevention
2. You set a specific application to **Deny**, but there are still some instances of the program communicating externally. Why might this be?
   ✓ A. The application is not denied in all communication control policies.
   B. The application is known to be safe, so it will always be allowed to communicate.

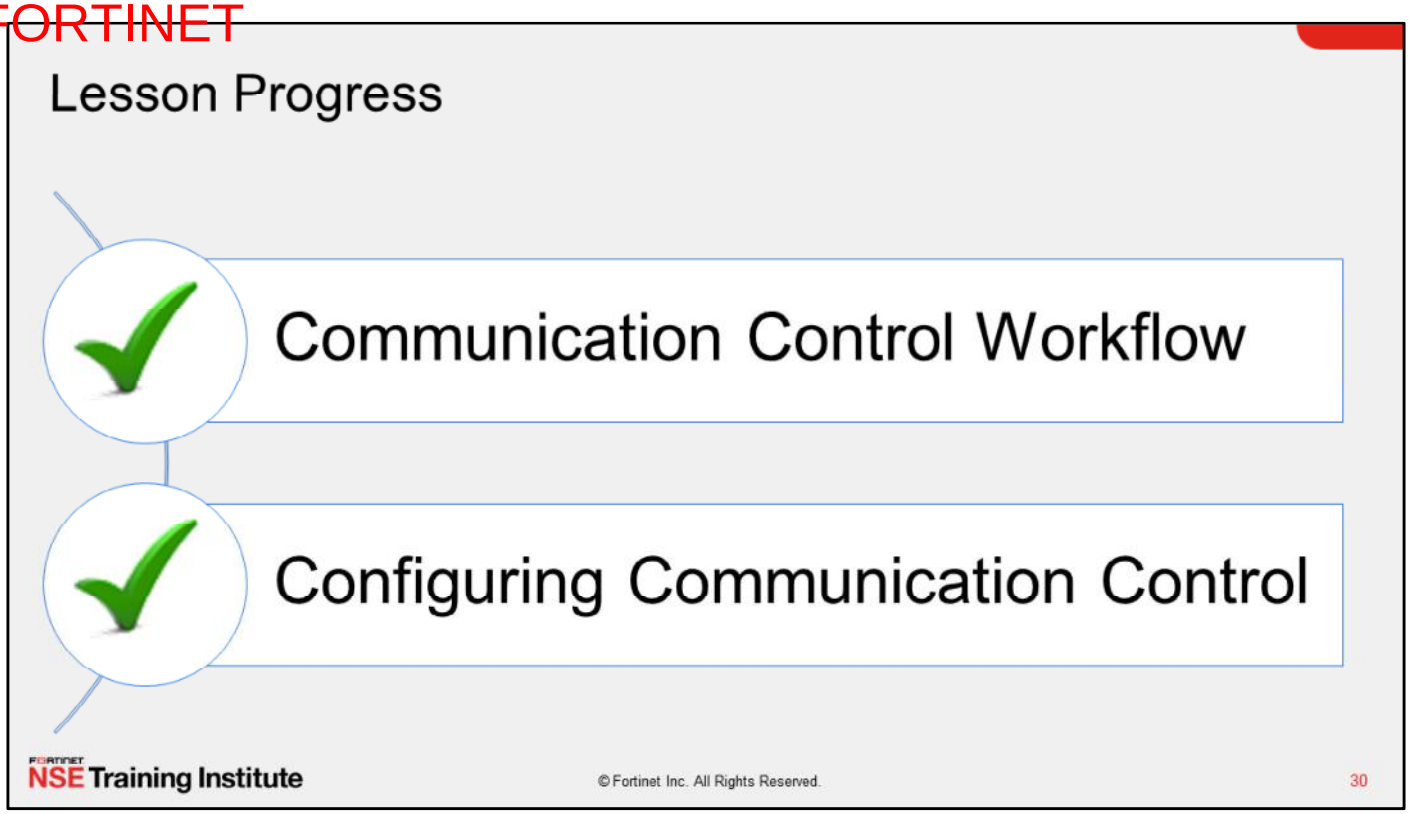
NSE Training Institute

© Fortinet Inc. All Rights Reserved.

29

Vouchers & Dumps are Available | WhatsApp +201224560923

DO NOT REPRINT Brave-dumps.com
© FORTINET



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

Review

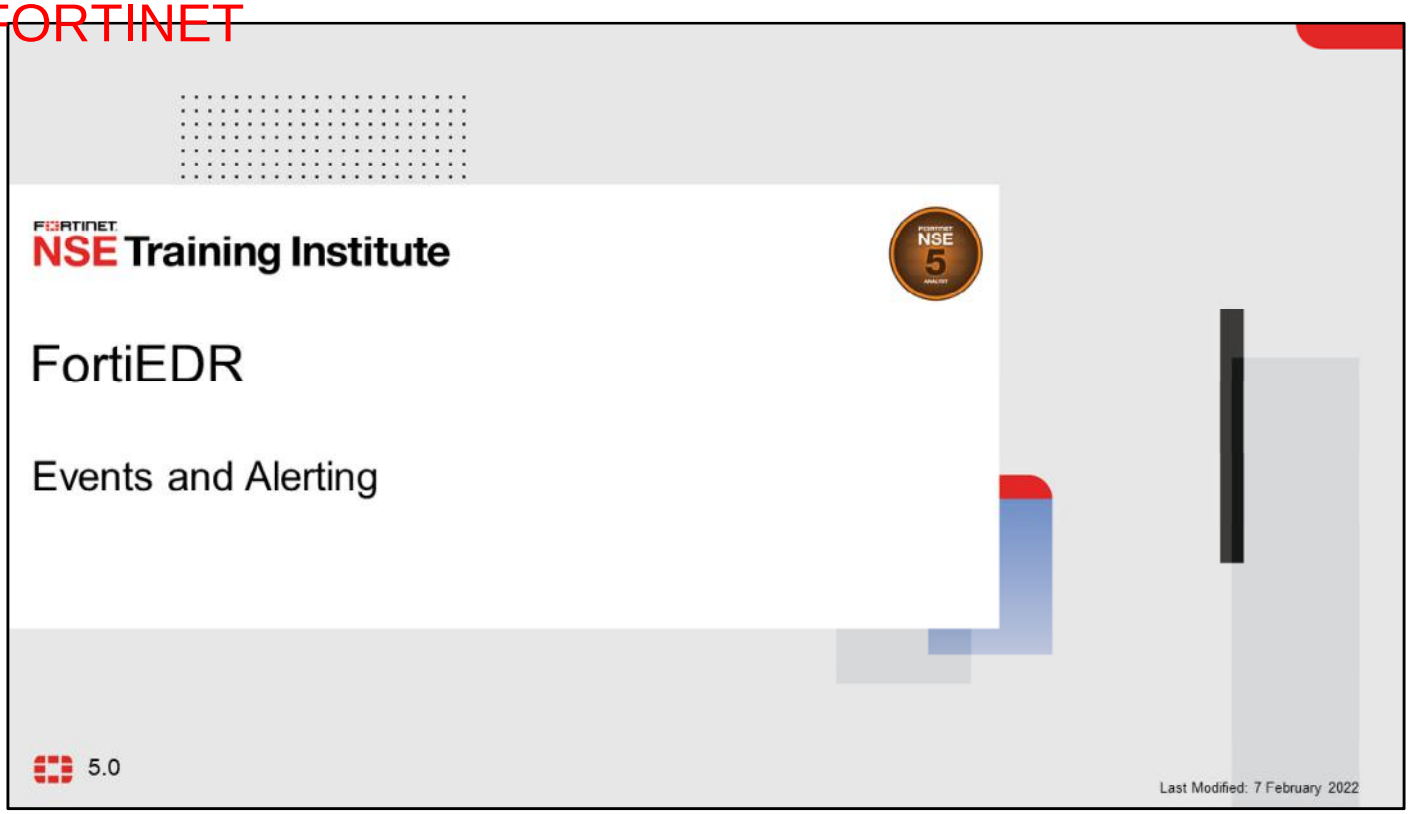
- ✓ Understand what communication control is and the advantages it provides
- ✓ Understand how communication control works
- ✓ Analyze applications data on EDR
- ✓ Identify the predefined communication control policies
- ✓ Assign communication control policies
- ✓ Create exceptions for applications
- ✓ Identify read and unread applications
- ✓ Understand how to resolve applications

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

By mastering the objectives covered in this lesson, you learned how to configure and manage communication control policies and rules.

Vouchers & Dumps are Available | WhatsApp +201224560923

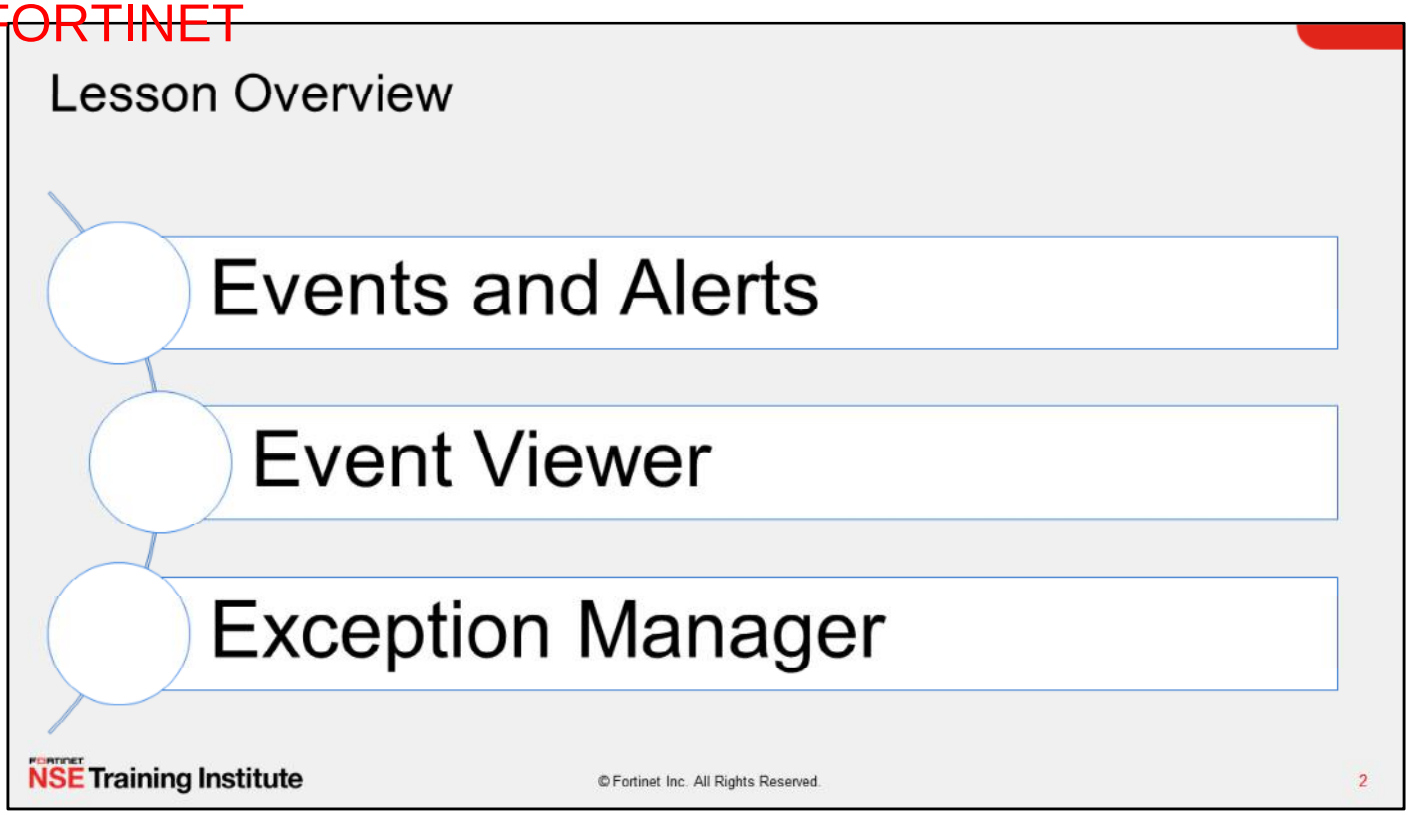
DO NOT REPRINT
© FORTINET
Brave-dumps.com



In this lesson, you will learn about events and alerting.

Vouchers & Dumps are Available | WhatsApp +201224560923

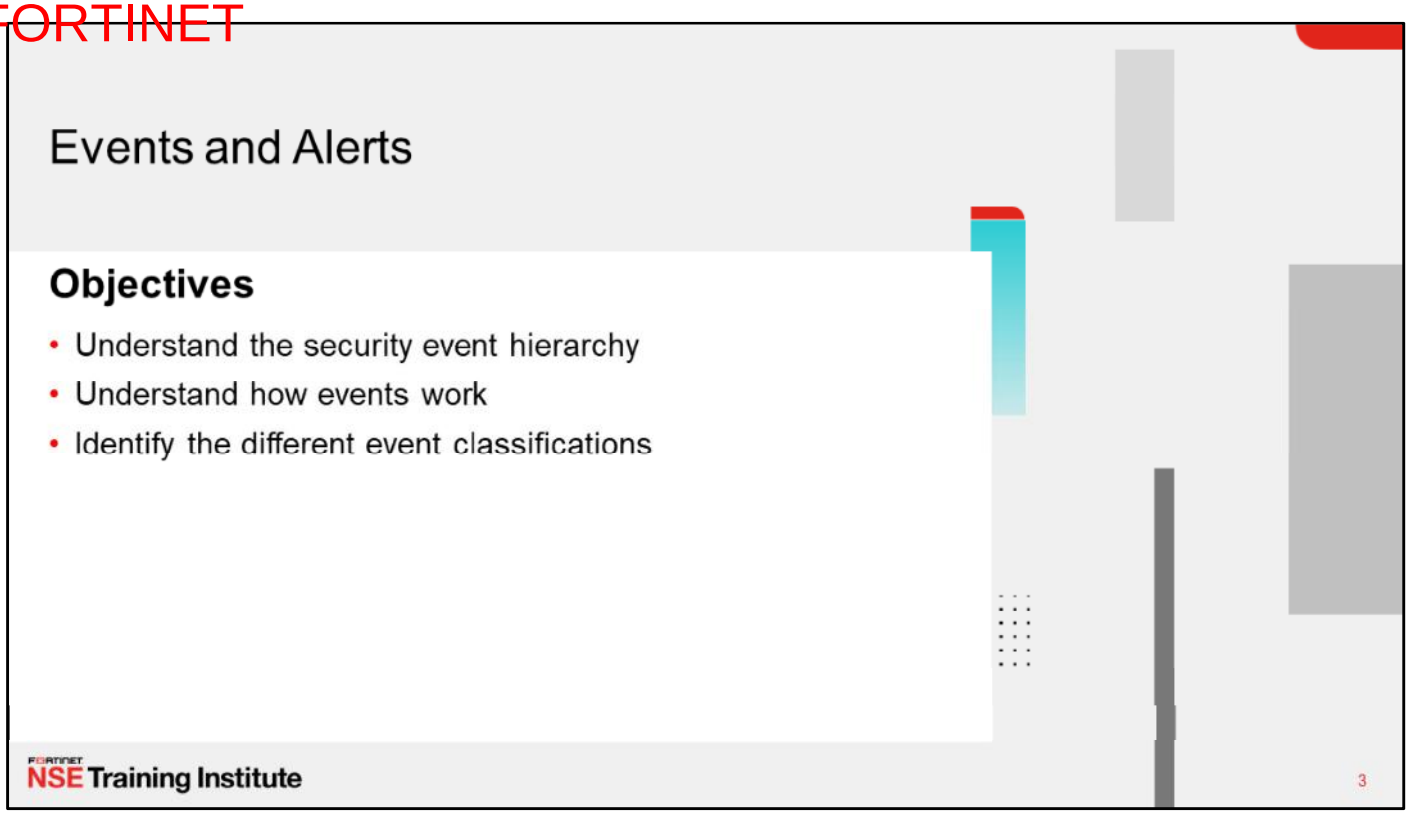
DO NOT REPRINT
© FORTINET
Brave-dumps.com



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

Vouchers & Dumps are Available | WhatsApp +201224560923

DO NOT REPRINT Brave-dumps.com
© FORTINET

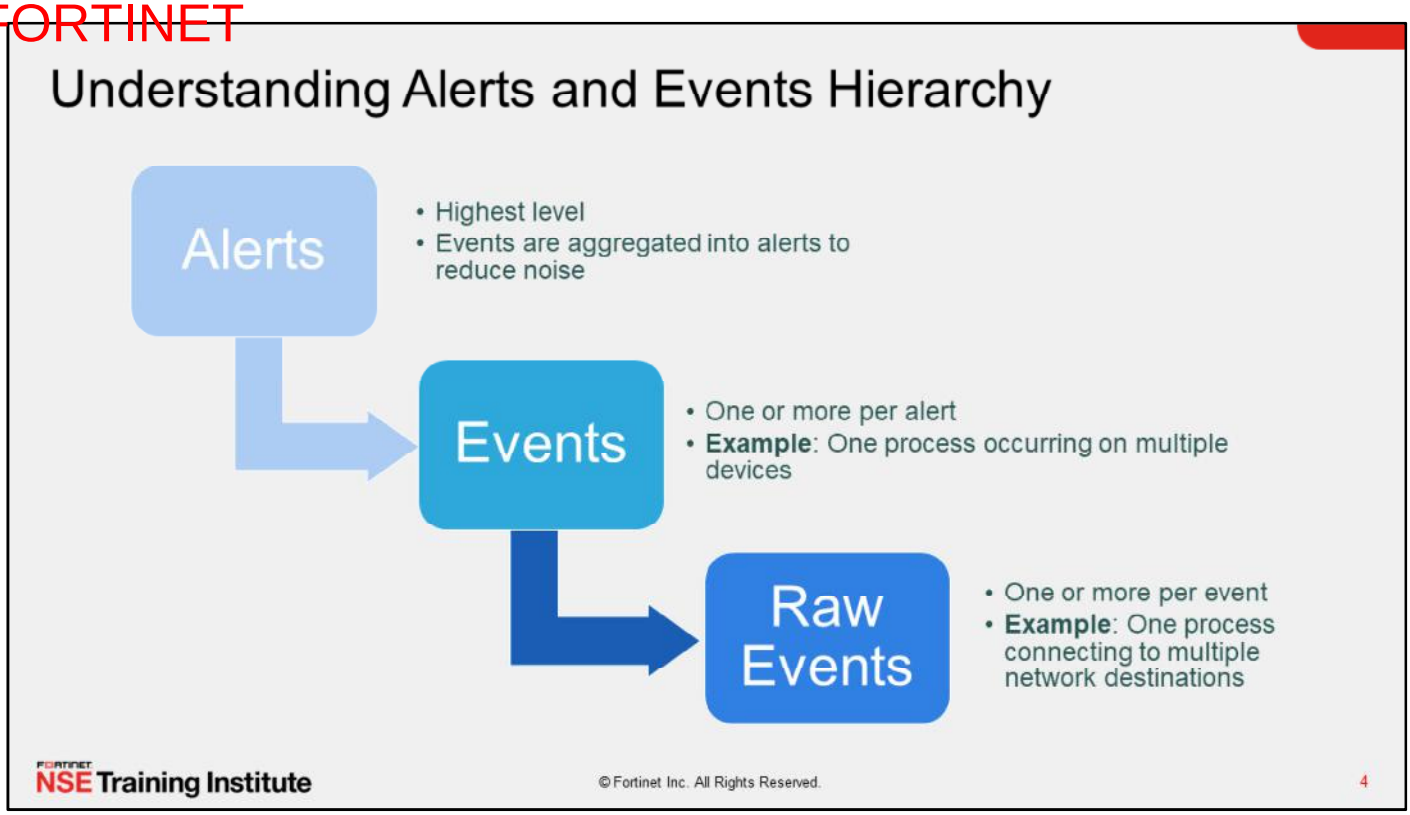


After completing this lesson, you should be able to achieve the objectives shown on this slide.

By demonstrating competence in events and alerts, you will understand the security event hierarchy and be able to identify its classifications.

Vouchers & Dumps are Available | WhatsApp +201224560923

DO NOT REPRINT
© FORTINET
Brave-dumps.com



When you are reviewing security events, you want to have enough information to decide on a course of action, but not so much information that it becomes overwhelming. FortiEDR aggregates security event data so that you can start with a high-level alert and drill down to get more detail as needed. For example, let's say a piece of malware is triggered on three separate devices. Each time the process is triggered on a new device, a separate event is created. If you aggregate events by process, all the events will be part of the same alert: three events rolled up into one alert. If that malware tried to communicate across the network, it could attempt to connect to many network destinations, and each attempted connection to a new destination would result in a separate a raw event. Many raw events are rolled up into a single event, and then, at the highest level, those single events are rolled up into alerts.

Vouchers & Dumps are Available | WhatsApp +201224560923

DO NOT REPRINT Brave-dumps.com
© FORTINET

How Events Work

- Policies and rules
  - FortiEDR comes out of the box with five policies:
    - Execution Prevention (NGAV)
    - Exfiltration Prevention
    - Ransomware Protection
    - Device Control
    - eXtended Detection
  - Each policy is made up of a set of specific rules
  - Collectors send snapshots of activity on the device
  - If the activity violates one or more rules, FortiEDR creates an event
- Blocking and logging
  - Each rule is assigned an action based on its severity: **Block** or **Log**
  - If multiple rules are violated by one event, the most serious rule determines the action
  - The assigned action for each rule can be edited in **SECURITY SETTINGS** > **Security Policies**

SECURITY SETTINGS > Security Policies

EVENT VIEWER

NSE Training Institute
© Fortinet Inc. All Rights Reserved.
5

How does FortiEDR detect and handle security events? FortiEDR comes out of the box with five security policies: Execution Prevention (or NGAV), Exfiltration Prevention, Ransomware Prevention, Device Control, and eXtended Detection. These policies are each made up of a set of rules related to the behavior of a file or process. The FortiEDR collector, which is installed on every device in your network, takes snapshots of activity on the device. When an activity violates a rule, you receive an event. For example, you can see that the event in the example shown on this slide violated the **Malicious File Detected** rule. Malicious file detected means that FortiEDR recognized the file as malicious. When a file is flagged based on machine learning or other analysis, FortiEDR generates an alert whenever it sees that file.

Rules are assigned actions. In most cases, the default action is **Block**. If an event violates the rule, FortiEDR will automatically block it. For less serious rules—behaviors that are suspicious but could be legitimate—the default action is **Log**. If needed, you can change these actions on the **SECURITY SETTINGS** tab. When an event violates more than one rule, the more serious violation determines the action. In other words, if one rule is set to **Block** and one is set to **Log**, and the event violates both rules, the event will be blocked. You can see the action taken at the end of the event row.

Vouchers & Dumps are Available | WhatsApp +201224560923

DO NOT REPRINT Brave-dumps.com
© FORTINET

Event Actions

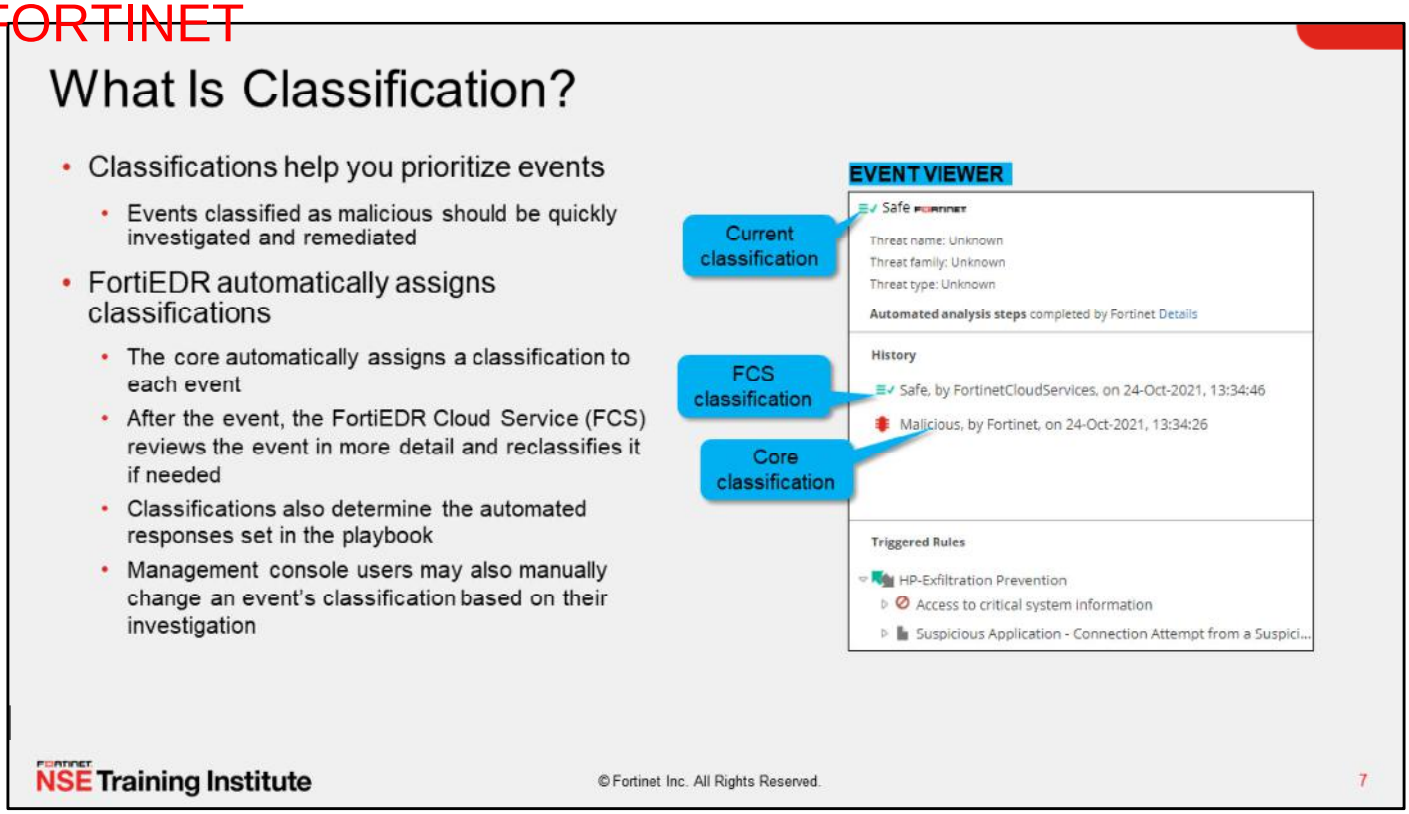
- **Block**
  - Security policy in prevention mode
  - Rule action set to **Block**
  - Exfiltration attempt blocked and event is logged in **EVENT VIEWER**
- **Simulated Block**
  - Security policy in simulation mode
  - Rule action set to **Block**
  - No exfiltration attempt blocked, but an event is logged in **EVENT VIEWER**
- **Log**
  - The rule action is set to **Log** instead of **Block** in the security policy
  - Event is logged in **EVENT VIEWER**

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

This slide shows all the event actions. An event on **EVENT VIEWER** with an action of **Block,** means the exfiltration attempts on the collector were blocked by the policies in prevention mode. An event with an action of **Simulated Block**, means the policy is simulation mode and the exfiltration attempt would have been blocked if in prevention mode. An event with action with **Log**, means the rule in a security policy is only logging the event and not blocking it.

Vouchers & Dumps are Available | WhatsApp +201224560923

DO NOT REPRINT Brave-dumps.com
© FORTINET



Classifications are a guide to help you prioritize events. A classification of *malicious* indicates that you should investigate and remediate the event as quickly as possible, but likely safe events are less urgent. You will learn about each classification on the next slide.

How are classifications assigned? When an event takes place, the core automatically assigns it a classification. In the example shown on this slide, in the **History** section, you can see that the event was first classified as malicious. This is part of the immediate response to the event. You'll notice the time stamp is 24 October 2021 at 13:34 and 26 seconds. After the event, the FCS reviews it in more detail and decides whether the original classification should be changed. If you look at the example again, you'll see that FCS reclassified the event as safe. FCS took slightly longer to respond to the event—you'll notice the time stamp is 13:34 and 46 seconds, which is about 20 seconds after the core logged the event. So the core responds instantly to the event, and then FCS fine-tunes the classification, if needed.

As a management console user, you can also manually reclassify an event based on your analysis. For example, if you investigated a suspicious event and verified that it was caused by malware, you can mark it as *malicious* so if it comes up again, you'll know it's bad, and you won't have to investigate it again. You will learn more about reclassifying events in this lesson.

Vouchers & Dumps are Available | WhatsApp +201224560923

DO NOT REPRINT Brave-dumps.com
© FORTINET

Event Classifications

Status	Symbol	Definition	Recommended Action
Malicious		Events that are verified to have malicious capability, are intended to harm the infected device, and have no commercially viable use	Remediate
Suspicious		Events that behave in ways that strongly indicate malware, but are not verified malware	Review and remediate
Inconclusive		Further investigation needed to determine if event is malicious	Administrator review
Potentially Unwanted Programs (PUPs)		Events triggered by programs that are bundled with legitimate software or commercial software that may be used for malicious purposes (example: torrents)	Administrator to review whether the program should be removed (recommended) or allowed
Likely Safe		Events that probably carry no risk, and are most likely legitimate	Administrator review
Confirmed Safe Software		Events triggered by legitimate software that was intended for use by the customer (example: security software)	No action necessary

NSE Training Institute

© Fortinet Inc. All Rights Reserved.

8

This slide shows all the event classifications. First on the list are *malicious* events. These are the most serious events—they are bad, they have no potential use, and you should remediate the device.

Second are *suspicious* events. Suspicious events are most likely malware, but it hasn't been verified. You should review these events to make sure they're not legitimate, then remediate the device as needed.

The third category is *inconclusive*. This classification indicates that there is conflicting information, or not enough information to determine if the event is malware. You should review these events. If you determine that the events are malicious, remediate the device. If you determine that they are safe, you can create an exception so it won't come up again.

Next are *potentially unwanted programs*, or PUPs. These are not necessarily malware, but they are processes that you should not run. Often these programs are bundled with legitimate software—browser plugins, for example—or they may be high-risk applications like torrents. You should review these events and decide whether to remove the program or create an exception to allow it.

The last two categories are the least serious. A *likely safe* classification means that the event is probably legitimate. It is not possible to verify it 100%, but you can assume that there is very little risk. Review these events to make sure they look OK, then create an exception. Software that is classified as *confirmed safe* is definitely legitimate. Normally, you will not see safe events in your events list. If FortiEDR determines that an event is confirmed safe, it automatically creates an exception and marks the event as expired. If the process runs again, it will be allowed.

Vouchers & Dumps are Available | WhatsApp +201224560923

DO NOT REPRINT
© FORTINET
Brave-dumps.com

Knowledge Check

1. Which FortiEDR component reviews the event in more detail and decides whether the original classification should be changed?
   A. Core
   ✓ B. FCS

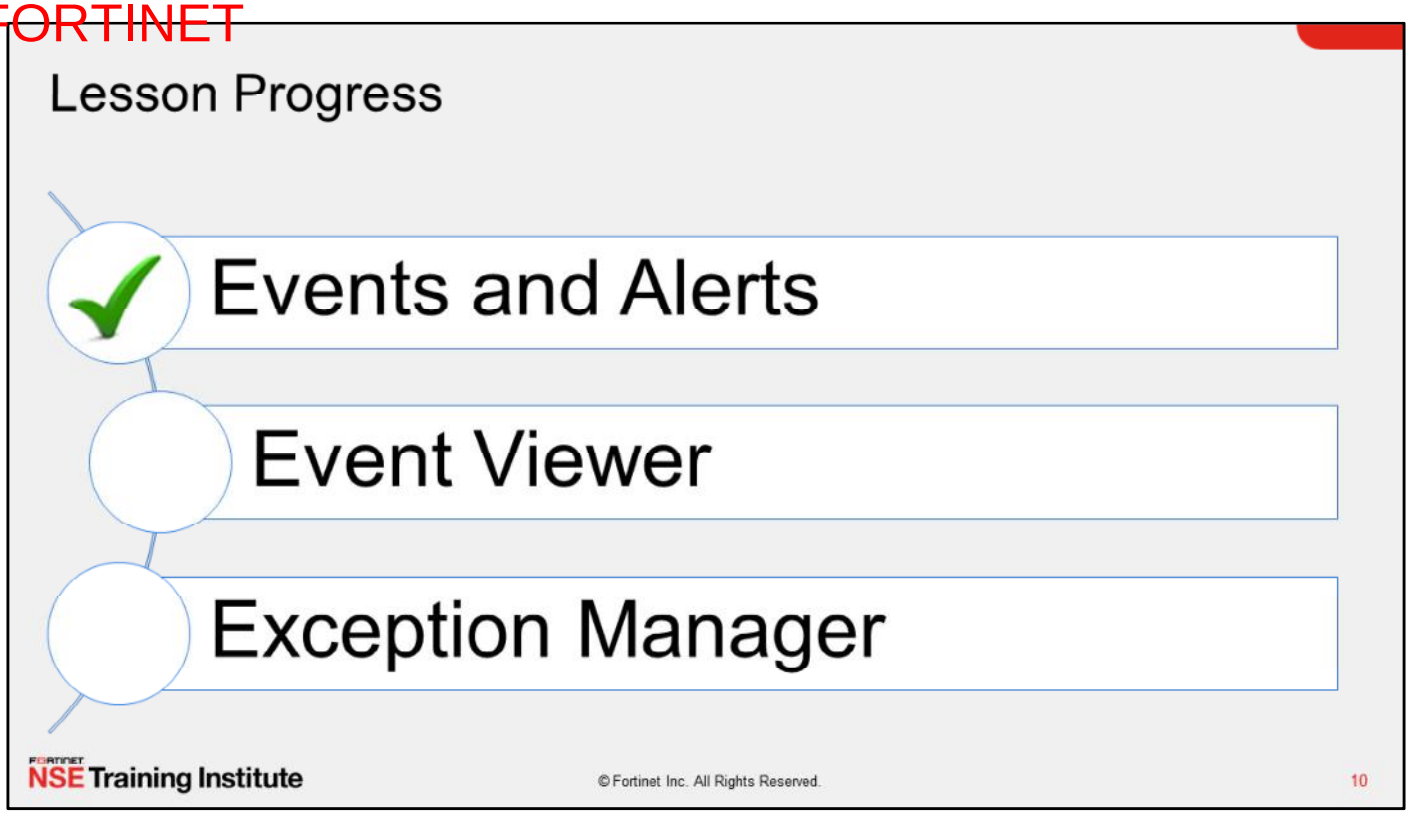
NSE Training Institute

© Fortinet Inc. All Rights Reserved.

9

Vouchers & Dumps are Available | WhatsApp +201224560923

DO NOT REPRINT
© FORTINET
Brave-dumps.com

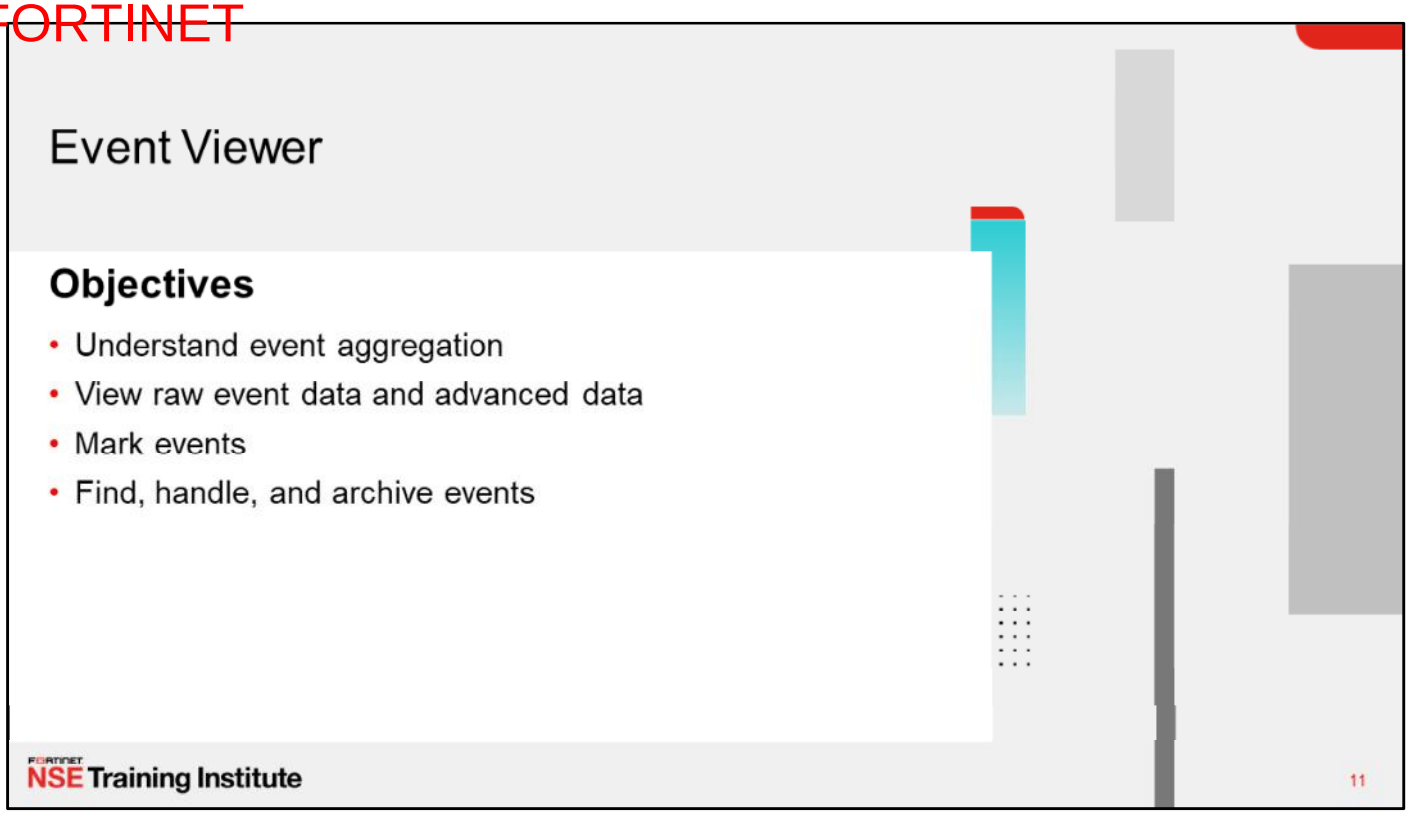


Good job! You now understand events and alerts.

Now, you will learn about the event viewer.

Vouchers & Dumps are Available | WhatsApp +201224560923

DO NOT REPRINT Brave-dumps.com
© FORTINET



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

By demonstrating competence in using the event viewer, you will know how to navigate through the FortiEDR event viewer.

Vouchers & Dumps are Available | WhatsApp +201224560923

DO NOT REPRINT Brave-dumps.com
© FORTINET

Understanding Alerts and Events

- Events are aggregated into alerts by device or by process
  - Each alert may include one or more events
    - The number of events is displayed next to the device or process name
  - An alert's **Classification** reflects the *most serious* classification level of the events it contains
  - An alert's **Received** date reflects the first time an event was triggered
  - An alert's **Last Updated** date reflects the last time an event was triggered
  - Click an alert row to view associated events
- Raw events are aggregated into events
  - Each event is assigned a unique event **ID**
  - Click an event row to view more details
  - An event is made up of one or more raw events
  - Click the arrow beneath the event checkbox to view raw event details

NSE Training Institute

© Fortinet Inc. All Rights Reserved.

12

Now look at event aggregation in a little more detail. Events are aggregated into alerts by device or process. Each method of aggregation is useful for different types of investigation. For example, you may want to choose the process view if you want to see the impact of a single malware process across your network. In the example shown on this slide, the events are aggregated by process. You can see that the network has two events that involve `ConnectivityTestAppNew.exe`. If you're troubleshooting a specific device, you might want to choose the device view so you can see all the events involving that device. If you want to see the events in an alert, just click on the alert in the list to expand it.

The alert classification comes from the most serious event classification within that alert. So, if an alert contains one event classified as *malicious* and three events classified as *inconclusive*, the alert would be classified as *malicious*. This classification system is intended to draw your attention to the most urgent events. An alert also gets its received date from the events—the most recent date that an event was first received is the alert received date—in this example, 5th of December 2021.

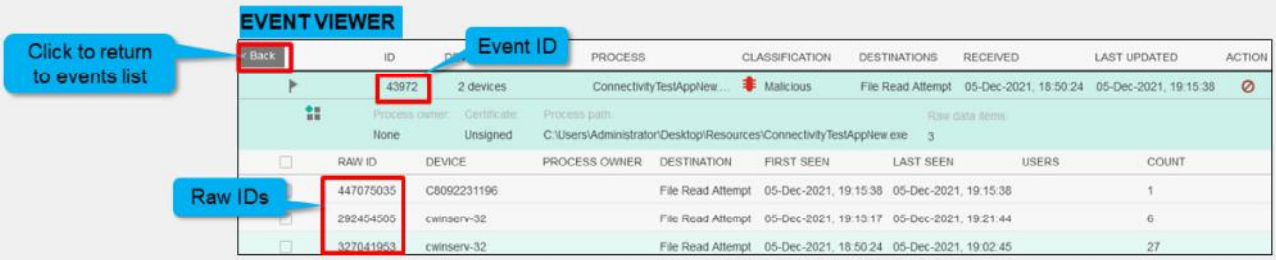
Raw events are aggregated into events. Each event is assigned a unique event ID. In this example, the first **ConnectivityTestAppNew** event listed is event **44010**. If you click the row, you'll see more detail: the user, the path, and whether the certificate was signed. At the end of the row, you'll also see the number of **Raw data items—**in this example, **3**. An event may be associated with just one raw event, or hundreds. To view raw event details, click the triangle on the left end of the row.

Vouchers & Dumps are Available | WhatsApp +201224560923

DO NOT REPRINT Brave-dumps.com
© FORTINET

Viewing Raw Event Data

- In the example, raw IDs 447075035, 292454505, and 327041953 belong to the same event: event ID 43972
- View process destinations
  - Where applicable, you can view the destination for each raw event, including external IP address
- View each piece of raw data collected by FortiEDR that led to the event
- Raw events vs. events
  - Each piece of raw event data is assigned a raw ID



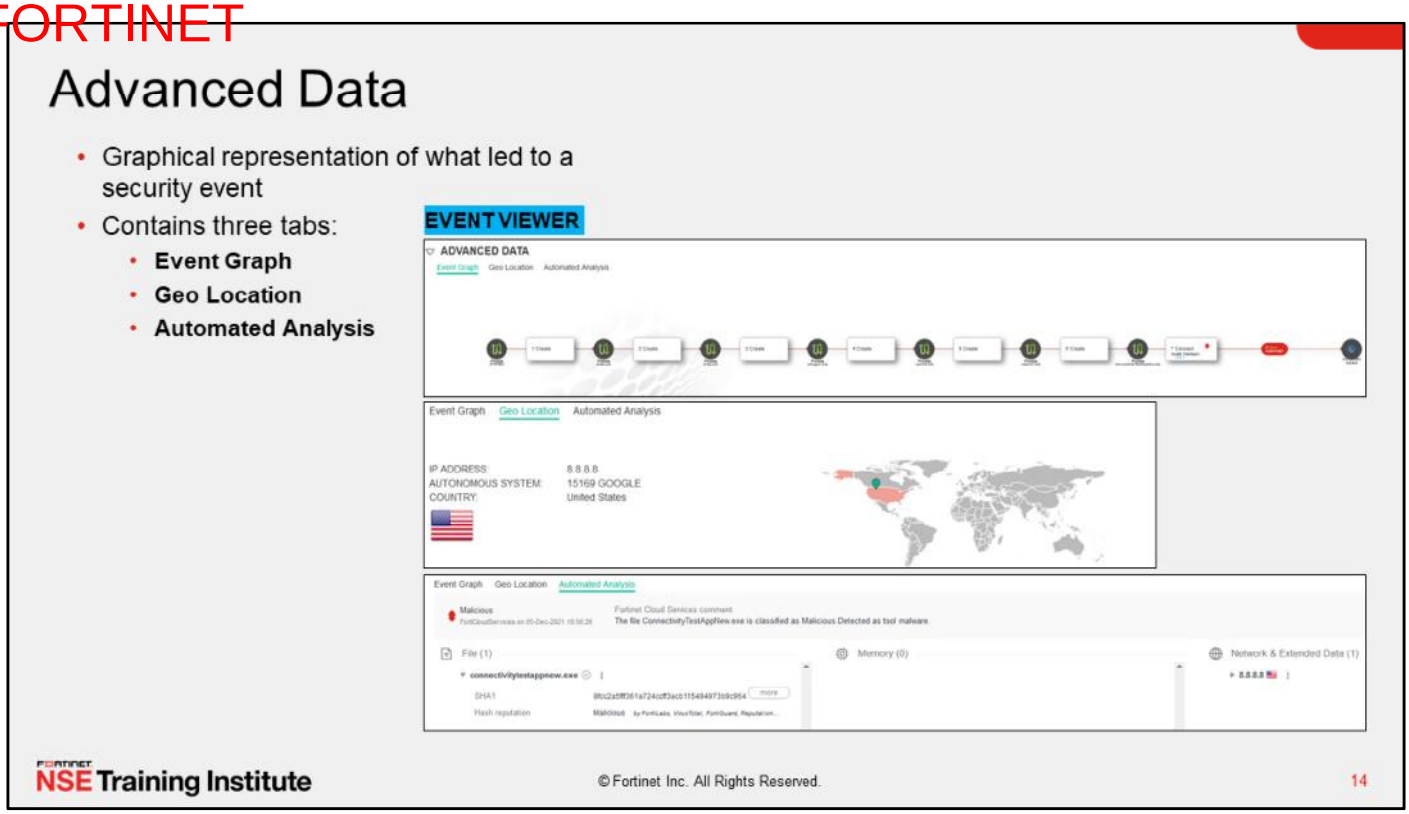
NSE Training Institute © Fortinet Inc. All Rights Reserved. 13

The example on this slide shows the raw event data—you can see each piece of raw data collected by FortiEDR that led to the event. In this example, you can see event 43972, and there are three raw events within that event, each with its own raw ID. The file was read thirty four times on December 5. You'll notice that each raw event is assigned a raw ID. These are separate from the event ID.

Wherever applicable, you can view the external destination of each raw event on the **ADVANCED DATA** pane.

Vouchers & Dumps are Available | WhatsApp +201224560923

DO NOT REPRINT Brave-dumps.com
© FORTINET



The **ADVANCED DATA** pane shows a graphical representation of what led to a security event. It consists of three tabs: **Event Graph**, **Geo Location**, and **Automated Analysis.** The **Event Graph** tab is always shown, and the other two tabs are displayed only if relevant data is available. The **Event Graph** tab shows a flow of operating system events that led to a security event. The **Geo Location** shows the destination country of the security event. The **Automated Analysis** tab shows how FortiEDR classified an event and a summary of what was analyzed.

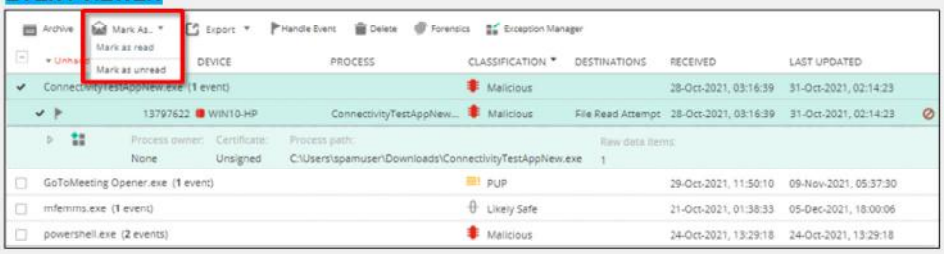
Vouchers & Dumps are Available | WhatsApp +201224560923

DO NOT REPRINT Brave-dumps.com
© FORTINET

Marking Events as Read or Unread

- Read or unread
  - Unread items *have not* been clicked and viewed by a management console user
    - Unread items are shown in **bold** text
  - Read items *have* been clicked and viewed by a management console user
    - Read items are shown in plain text
  - An alert is marked as read if all the events it contains are marked as read
- Mark as read or unread
  - Select the checkbox next to the event
  - Click the **Mark as** drop-down list and select **Mark as read** or **Mark as unread**
  - Clicking an event causes it to be marked as read

EVENT VIEWER



NSE Training Institute

© Fortinet Inc. All Rights Reserved.

15

Another way of indicating event status is by marking it as read or unread. When you click on an event row, that event is automatically marked as *read*. An alert is marked as read if all its events are read. Read events are shown in plain text, unread events are bold.

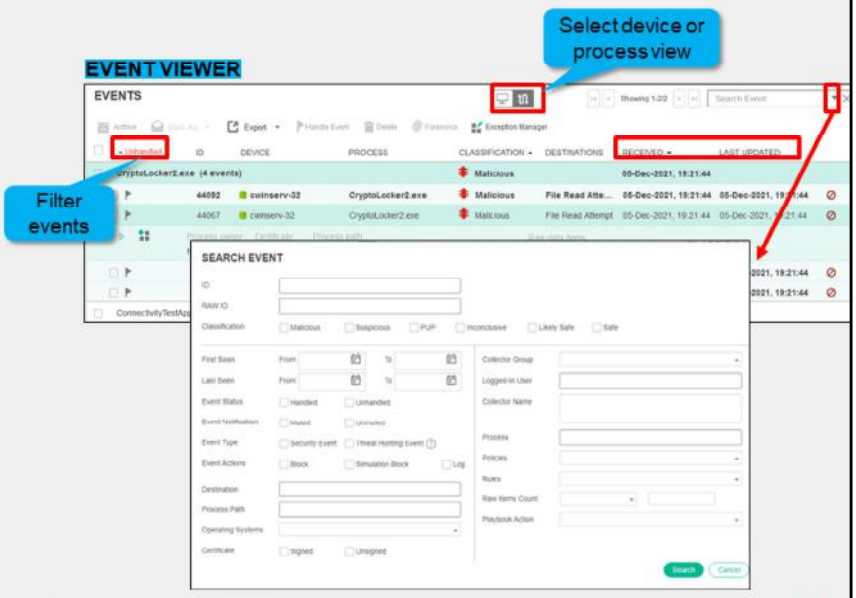
You can manually mark an event as read or unread. For example, you might revert an event status to unread if you want somebody else to look at it. Select the event checkbox—In the **Mark As** drop-down, select **Mark as read** or **Mark as unread**.

Vouchers & Dumps are Available | WhatsApp +201224560923

DO NOT REPRINT Brave-dumps.com
© FORTINET

Finding Events

- Filter by status
  - By default, only **Unhandled** events are shown
- Sort by date
  - Click **RECEIVED** to sort alerts by the first event occurrence
  - Click **LAST UPDATED** to sort alerts by the most recent event occurrence
- Choose device or process view
  - **Device** view is useful if you are investigating a specific user issue
  - **Process** view is useful if you need to find all devices affected by a specific process
    - For event tuning, the **Process** view is generally the most efficient choice
- Search for specific events
  - Enter your search term (event ID, process, user, and so on) in the search field
  - Click the gray arrow in the search field to open the advanced search window



NSE Training Institute

© Fortinet Inc. All Rights Reserved.

16

How do you find an event? Often, you'll want to view your highest priority items first. One way to do this is to filter by status. By default, only unhandled events are shown, so you can focus on events that haven't been dealt with. You can also use the filter to view unread events, archived events, or device control events—events related to devices that have been blocked by your device control policy, if enabled.

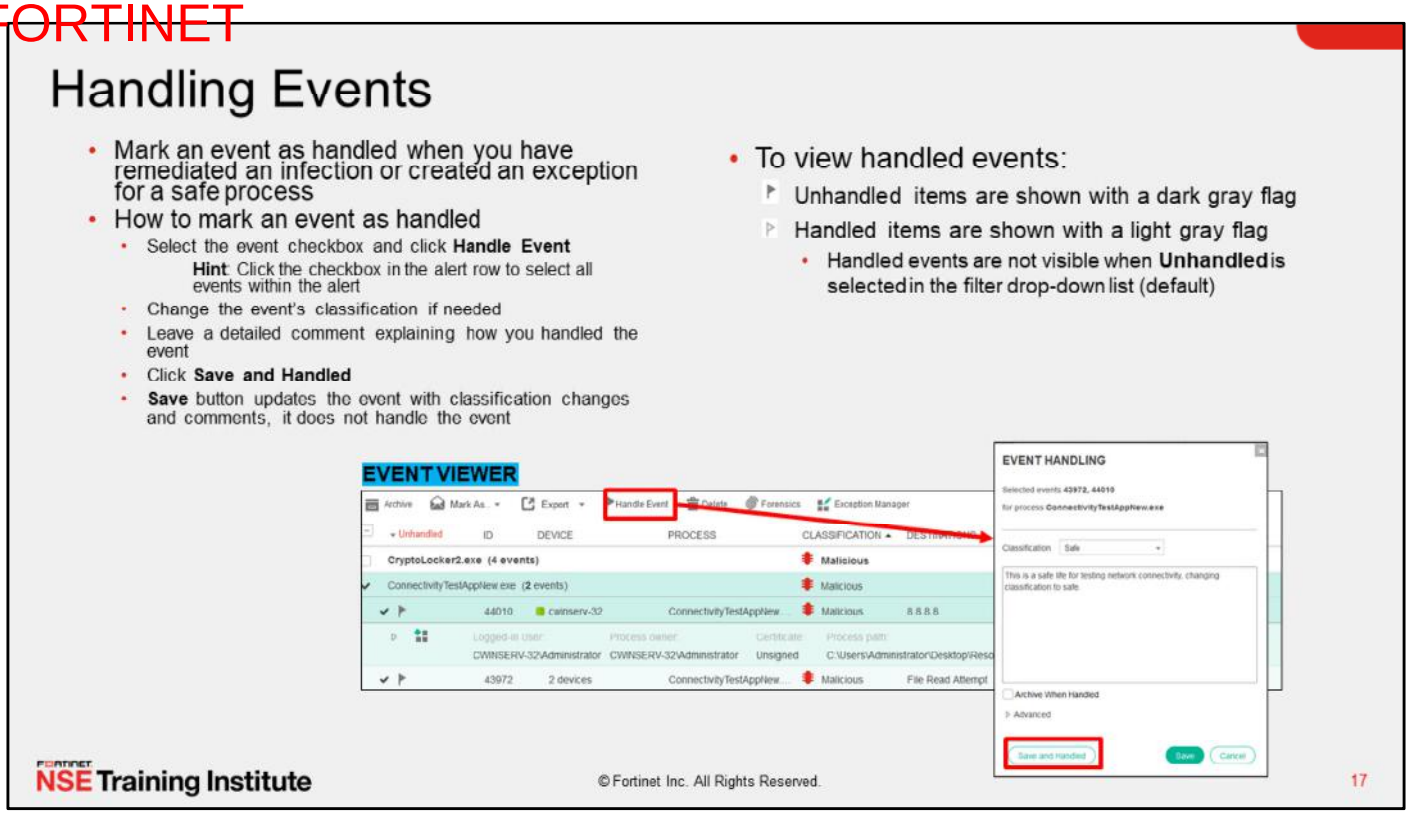
You can also use sorting to help prioritize events. You can sort by any column heading in the events list. Sorting by date is a great way to see what's actively affecting your system. You'll notice two dates for each event—one is received, which is the first occurrence of that event, and the second is last updated, which is the most recent occurrence of an event. In some cases, like the example you see on this slide, the two dates are the same, but sometimes the event happened several different times, so these dates might be days or weeks apart.

Device and process views are also designed to help you work more efficiently. In device view, you can see all the events that happened on a particular device. This can be useful if you are investigating a problem reported by a particular user. Select the process view and you can find all the devices that are affected by a particular process. This is a useful view for finding all the instances of a particular process—how many times has this malware affected my environment? Process view is also generally the most efficient choice for event tuning. You'll learn more about event tuning in a later course.

If you're looking for a specific event, you can use the search function. To do a simple search, enter your search term in the search field at the top of the list. If you already know the event ID, you can enter it here and you'll find it right away. If you want to search by more than one criteria, you can click the little gray arrow towards the right side of the search field to open the advanced search window. There, you can search by a combination of any of the criteria in the window, which you can see in this example on the lower right. For example, you might search for blocking events affecting a particular collector, or events on a certain day involving a specific process and classified as *malicious*.

Vouchers & Dumps are Available | WhatsApp +201224560923

DO NOT REPRINT Brave-dumps.com
© FORTINET



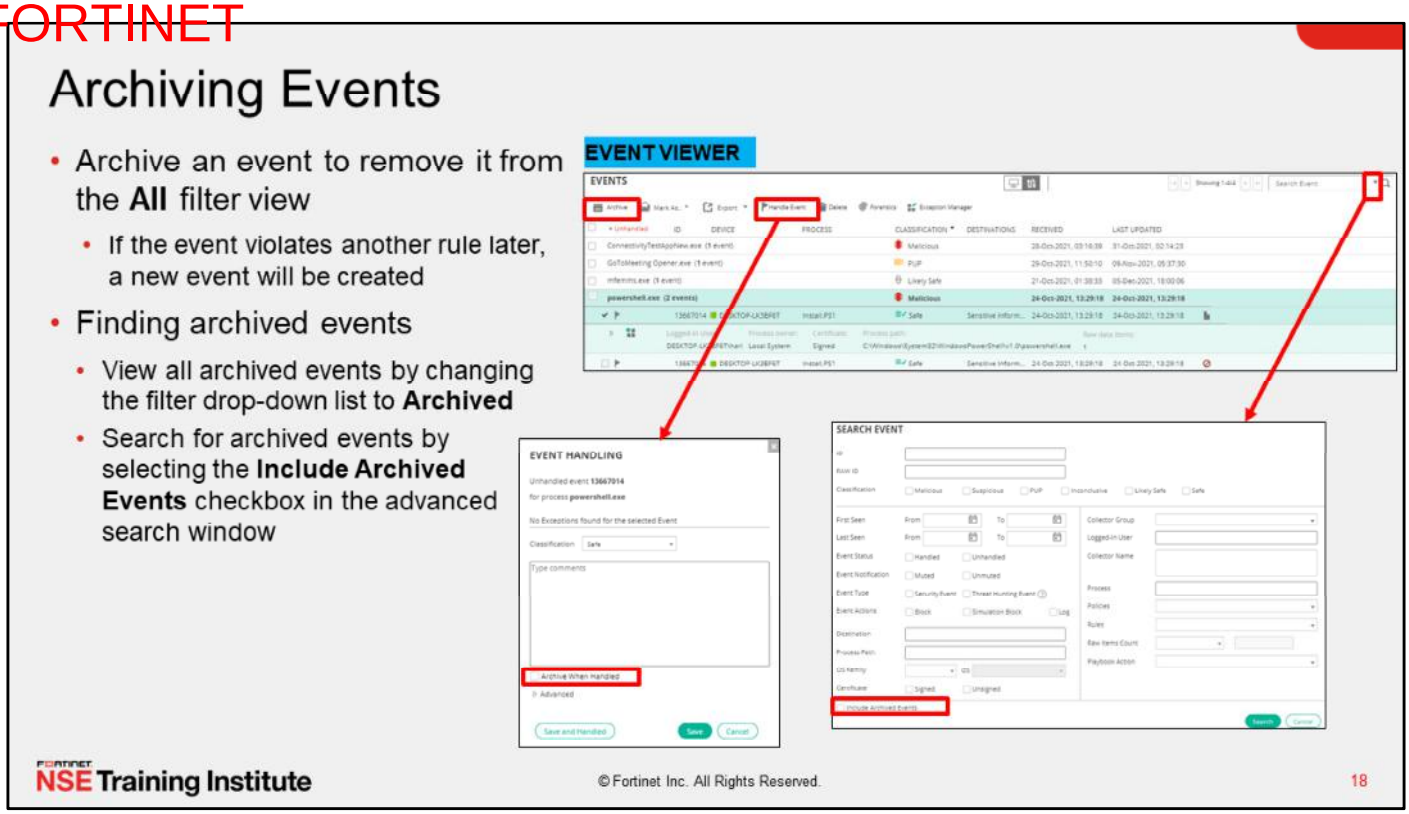
There are a couple of different ways to mark an event that you have dealt with. First, you can mark the event as **Handled**. When you mark an event as **Handled**, other management console users know you have already investigated and dealt with the event, either by remediating the infection or creating an exception for a safe process.

To handle an event, select the checkbox associated with the event. You can select the checkbox for an individual event, or for all the events in an alert. Then click the **Handle Event** button. The **Event Handling** pop-up window will open. You can use the settings in this window to change the event classification. For example, you can change a classification of inconclusive to a classification of safe or malicious, depending on your findings. The best practice is to include a comment explaining how you handled the event. Then click **Save and Handled**.

Unhandled items are shown with a dark gray flag, and handled items are shown with a light gray flag. If you want to see handled events, select **All**. The default view is **Unhandled**, which shows only events that haven't yet been dealt with; essentially, your to-do list. If an event recurs, it will be automatically marked as **Unhandled** so you will know further investigation is needed.

Vouchers & Dumps are Available | WhatsApp +201224560923

DO NOT REPRINT Brave-dumps.com
© FORTINET



You can also archive an event. Archived events are not in the events list, even when the filter is set to **All**. To archive an event, select its checkbox and click the **Archive** button at the top of the list. You can also select the **Archive When Handled** checkbox in the **Event Handling** window to archive and mark as handled in one step.

You can view all the archived events by changing the filter drop-down list on the left to **Archived**. You can also search for archived events in the advanced search window by selecting **Include Archived Events**. If an archived event recurs, a new event will be created and will appear in your main event list.

Vouchers & Dumps are Available | WhatsApp +201224560923

DO NOT REPRINT Brave-dumps.com
© FORTINET

Knowledge Check

1. Which one would create multiple raw events in a single event?
   - ✓ A. One suspicious process attempting to communicate with multiple destinations
   - B. Multiple suspicious processes on the same device

2. What does it mean if an aggregated alert row is marked as *malicious*?
   - A. The most serious classification of all the events contained in the alert is malicious.
   - ✓ B. The classification for all events contained in the alert is malicious.

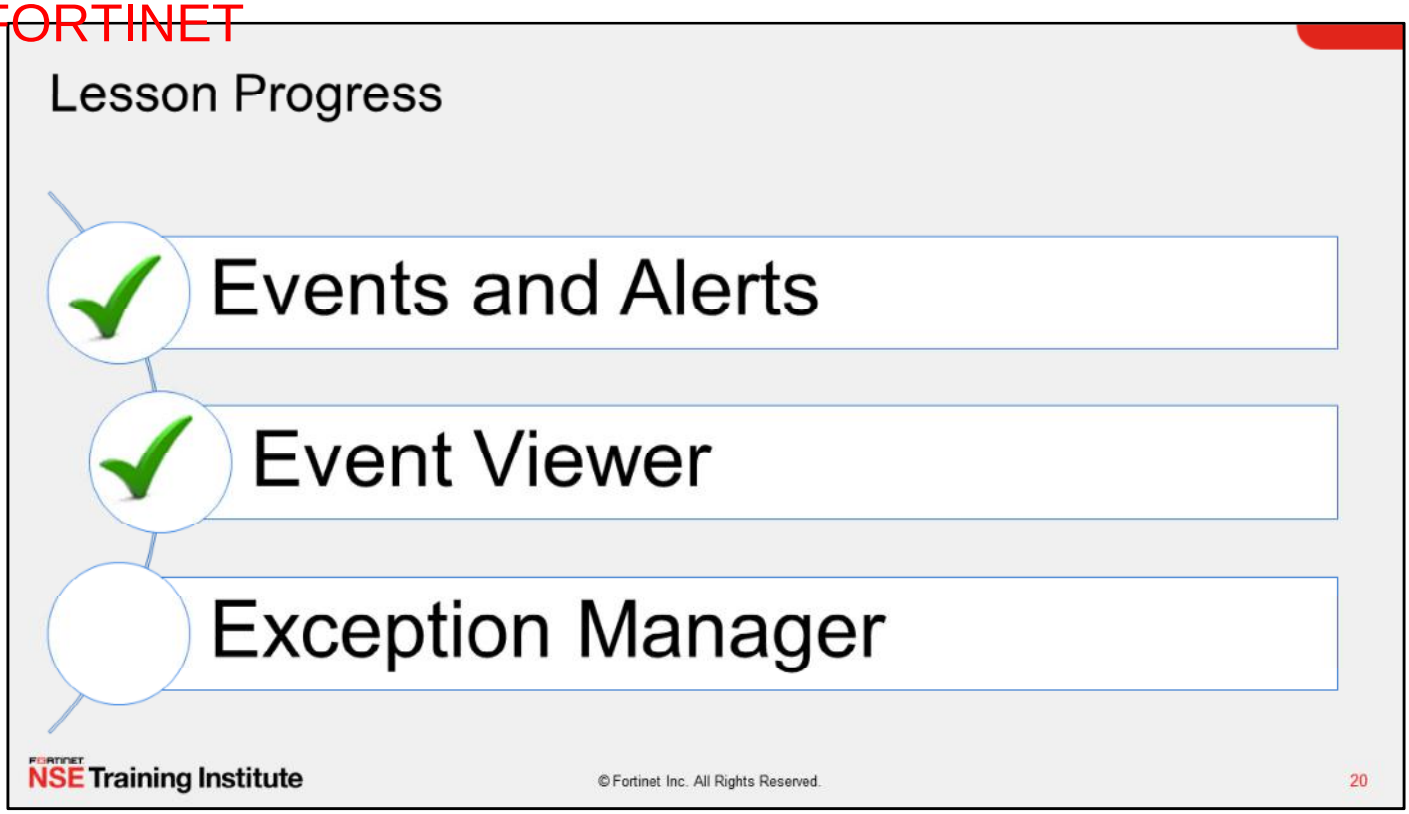
NSE Training Institute

© Fortinet Inc. All Rights Reserved.

19

Vouchers & Dumps are Available | WhatsApp +201224560923

DO NOT REPRINT Brave-dumps.com
© FORTINET

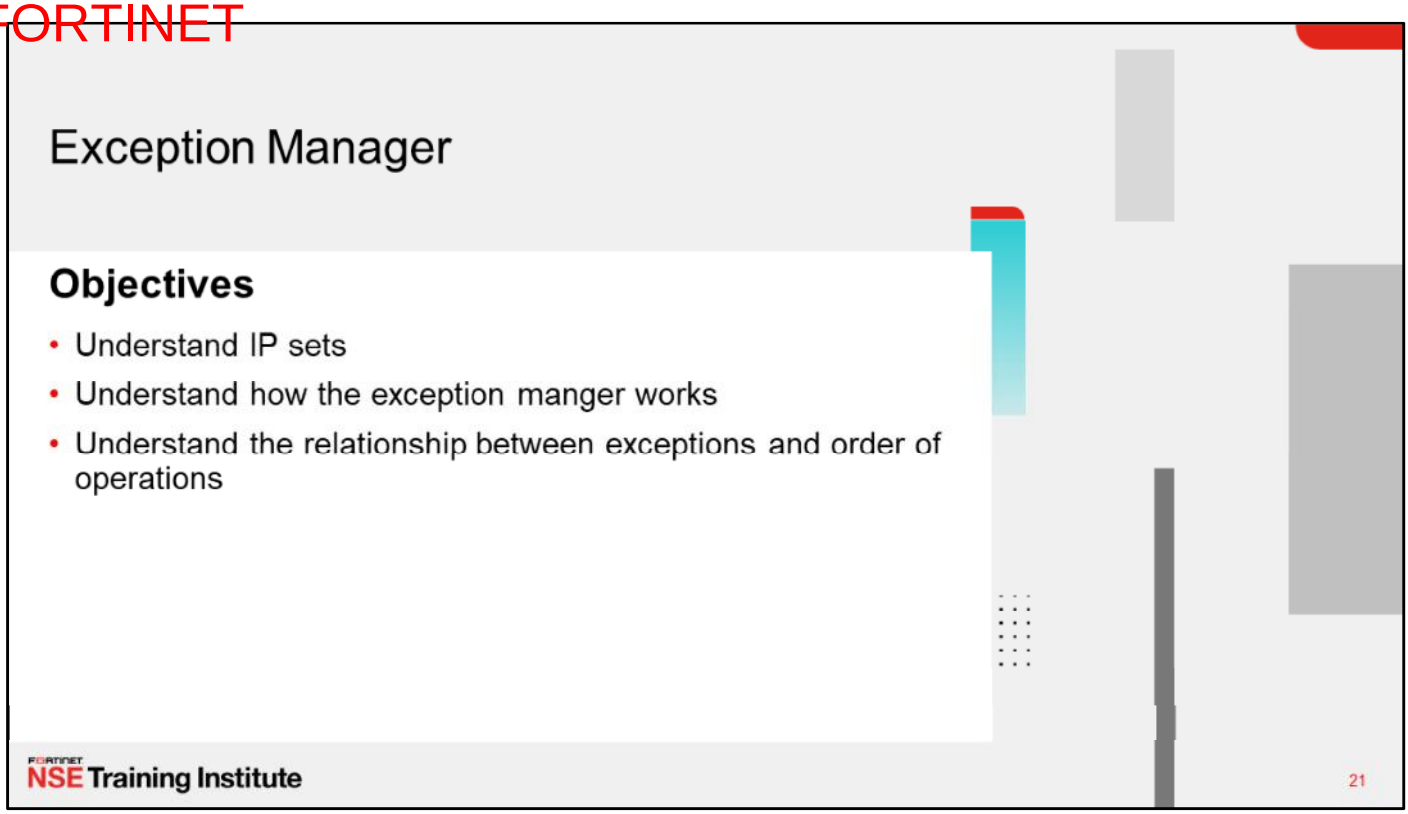


Good job! You now understand event viewer.

Now, you will learn about the exception manager.

Vouchers & Dumps are Available | WhatsApp +201224560923

DO NOT REPRINT Brave-dumps.com
© FORTINET



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

By demonstrating competence in using the exception manager, you will understand how to create and edit exceptions.

Vouchers & Dumps are Available | WhatsApp +201224560923

DO NOT REPRINT Brave-dumps.com
© FORTINET

IP Sets

- Define sets of allowed IP addresses to serve as allowed destinations in event exceptions
  - **Examples**: AWS IPs, database servers, domain controllers, Google IPs, credit card servers
- Click **Define new IP set** to add an IP set
  - IPs may be defined by:
    - Individual IP address(es) (e.g 192.168.23.2)
    - A range of addresses (e.g. 192.168.23.1-192.168.23.232)
    - A subnet (mask) (e.g. 192.168.0.0/16)
  - Add excluded IPs to exclude specific IP addresses from an allowed range
- FortiEDR comes pre-configured with an internal destinations IP set
  - You cannot edit addresses in this set
  - You can add to its included IPs and excluded IPs lists

ADMINISTRATION > IP SETS

NSE Training Institute

© Fortinet Inc. All Rights Reserved.

22

IP sets allow you to define a set of specific IP addresses, like AWS IPs, database servers, domain controllers, and so on. You can apply IP sets to an event exception—for example, you can allow a process to communicate only with Google IPs or only with your credit card servers.

You can create as many IP sets as you need. Add IP addresses individually, by range, or by subnet. You can also exclude specific IP addresses from an allowed range.

FortiEDR comes out of the box with an internal destinations IP set. You can't edit the IP addresses in the list, but you can add to it and put addresses in the excluded IPs list.

Vouchers & Dumps are Available | WhatsApp +201224560923

DO NOT REPRINT
© FORTINET
Brave-dumps.com

How Exceptions Work

- What are exceptions?
  - If you are certain that an event is safe, create an exception to ensure that it will not be blocked again
- Exceptions and rules
  - When traffic is evaluated by the anti-malware engine, an alert is created for each rule triggered
  - If an event violated multiple rules, you may need to create multiple exceptions
- Best practices
  - Minimize paths and destinations covered by the exception
  - Apply exceptions to all groups unless you have a specific reason not to
    - A collector moved to another group will lose all of its exceptions unless they are applied to all groups

NSE Training Institute

© Fortinet Inc. All Rights Reserved.

23

Say you've investigated an event and you're sure it's safe. Your next step is to create exceptions. An exception is a way of indicating that even though a process breaks a rule, you have determined that it is safe. So, if that process breaks the same rule again, FortiEDR won't block it.

The best practice is to minimize the paths and destinations covered by the exception. You can use **IP Sets** and add wildcards to file paths to reduce the need to apply the exception to all destinations or any path. You will learn about exception settings in detail in a later lesson.

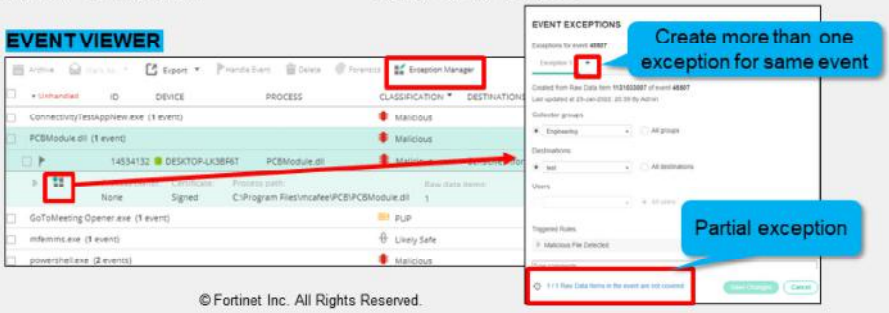
Fortinet also suggests applying exceptions to all groups unless you have a specific reason not to. Exceptions are applied to collector groups rather than individual collectors, so if a collector moves to another group, it will lose its exceptions unless the same exceptions are applied to both the new and old group. Applying exceptions eliminates this problem and reduces helpdesk requests.

Vouchers & Dumps are Available | WhatsApp +201224560923

DO NOT REPRINT Brave-dumps.com
© FORTINET

Managing Exceptions

- Viewing exceptions
  - Click the **Exception Manager** button to view all exceptions that have been added to your environment or click **SECURITY SETTINGS** > **Exception Manager**
  - Search exceptions by a single criteria (Event ID, process, and so on), or click **Advanced** to search by multiple criteria (process, path, rule, group, destination, or comments)
  - Edit or delete existing exceptions if needed
  - Export a list of exceptions as a PDF or Excel file
- Creating and editing an exception
  - When you click an event to view its details, you'll see the **Exceptions** button on the left
  - The **Exceptions** button indicates whether the selected event is covered by an existing exception:
    - No existing exceptions: Click to create a new exception
    - Existing exception: Click to edit exception
  - Click the **Exceptions** button to add a new exception or edit an existing one
  - Partial exceptions can be created and it does not apply on all devices



NSE Training Institute

© Fortinet Inc. All Rights Reserved.

24

Now take a quick look at how to apply and manage exceptions. When you click on an event in the events list to view its details, you can see the **Exception** button on the left. When you click the **Exception** button, you can see whether the selected event is already covered by an existing exception. When you see the icon without a pencil, with the green diamond at the upper left, there's no existing exception. Click this button to create a new exception. If you see the icon with the green pencil at the upper right, there is at least one existing exception. Click this button to view the exception and edit it if needed. For example, you might want to know when the exception was created so you can determine whether the event you're looking at happened before or after the exception was created. If it happened after, you may need to widen the parameters. You'll learn more about that on the next slide.

You can click the **Exception Manager** button if you want to see all the exceptions that are in place in your environment. You can search the exceptions for a particular process, event ID, and so on, or you can use the advanced search to look for multiple criteria at once. You can edit exceptions directly from the exception manager—just click the exception icon on the right side of the exception row. It's the same icon you saw in the events list for events with an existing exception. You can also delete exceptions—just click the trash icon at the end of the row. You also have the option to export a list of exceptions to a PDF or Excel file.

Vouchers & Dumps are Available | WhatsApp +201224560923

DO NOT REPRINT
© FORTINET
Brave-dumps.com

Exceptions and Order of Operations

- FortiEDR enforces its security policies in a specific order
  - Execution prevention policies are enforced when a file is read or launched
  - Exfiltration prevention policies are enforced when a connection is established
  - Ransomware prevention policies are enforced when a file is modified
- In prevention mode, the process is often stopped by the first blocking rule
  - If you create an exception to the first rule, the process may encounter further blocking events if it runs again, which will require further exceptions

NSE Training Institute

© Fortinet Inc. All Rights Reserved.

25

Now take a look at the relationship between exceptions and order of operations. Security policies are made up of rules, and exceptions apply to specific rule violations. FortiEDR enforces its policies in a specific order. First, when the file is read or attempts to execute, it's checked against the execution prevention, or NGAV, policy. This is where most infections are stopped. If the process is allowed to continue, the post-infection prevention policies kick in—exfiltration prevention checks all attempted network connections, and ransomware prevention checks all attempts to alter files.

Why does this matter? In prevention mode, the process is often stopped by the first blocking rule. For example, if it's stopped by the suspicious file detected rule in execution prevention, it won't be checked by the exfiltration or ransomware prevention policies. That means if you create an exception allowing the process to run even if it violates the Suspicious File Detected rule, you might not see any other violated rules. The process never launched, so it was never checked by the other policies. When you put your exception in place, the process may still encounter further blocking events if it violates other.

Vouchers & Dumps are Available | WhatsApp +201224560923

DO NOT REPRINT
© FORTINET
Brave-dumps.com

Knowledge Check

1. Which one can an exception be applied to?
   A. Collector
   ✓ B. Collector Group

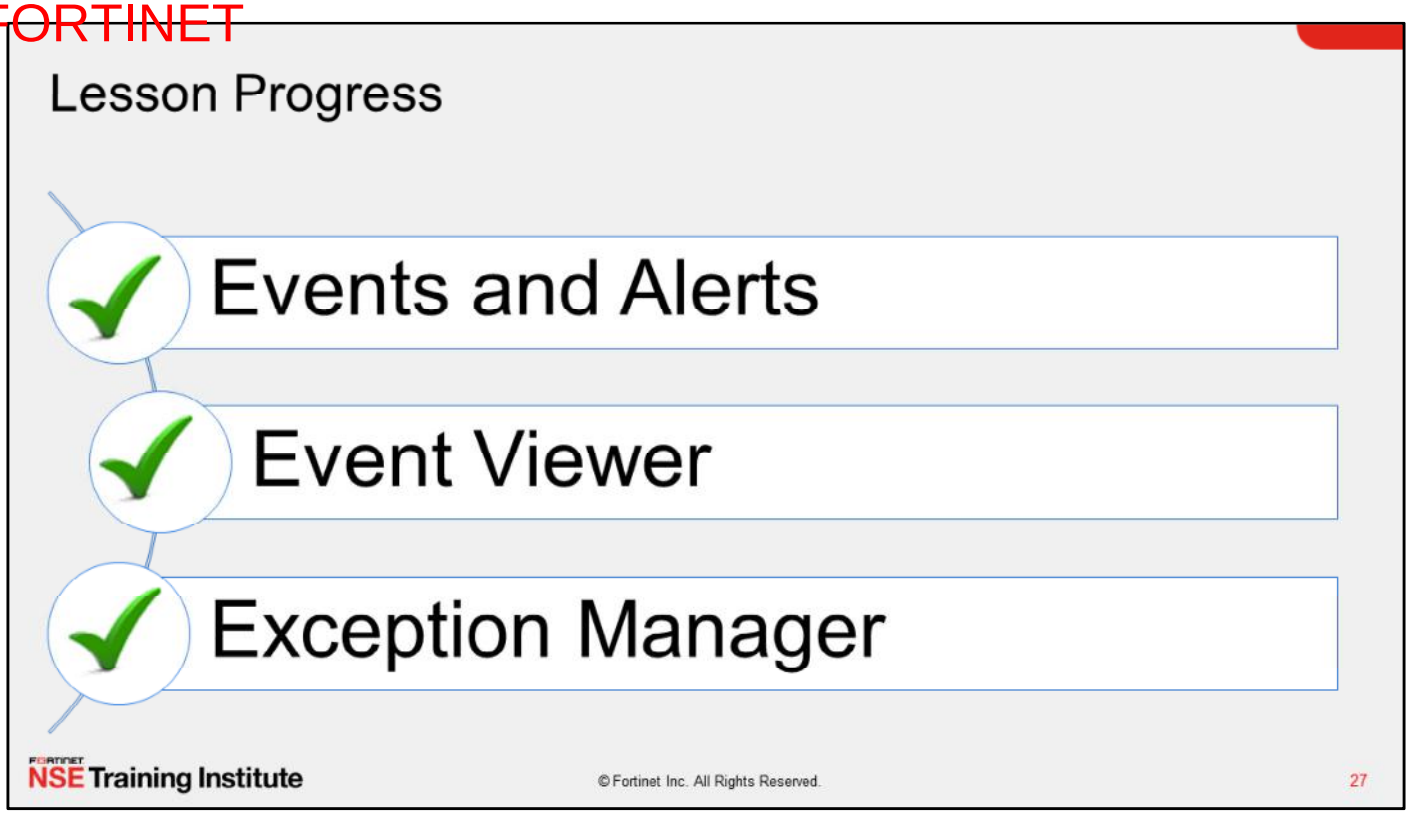
NSE Training Institute

© Fortinet Inc. All Rights Reserved.

26

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

Review

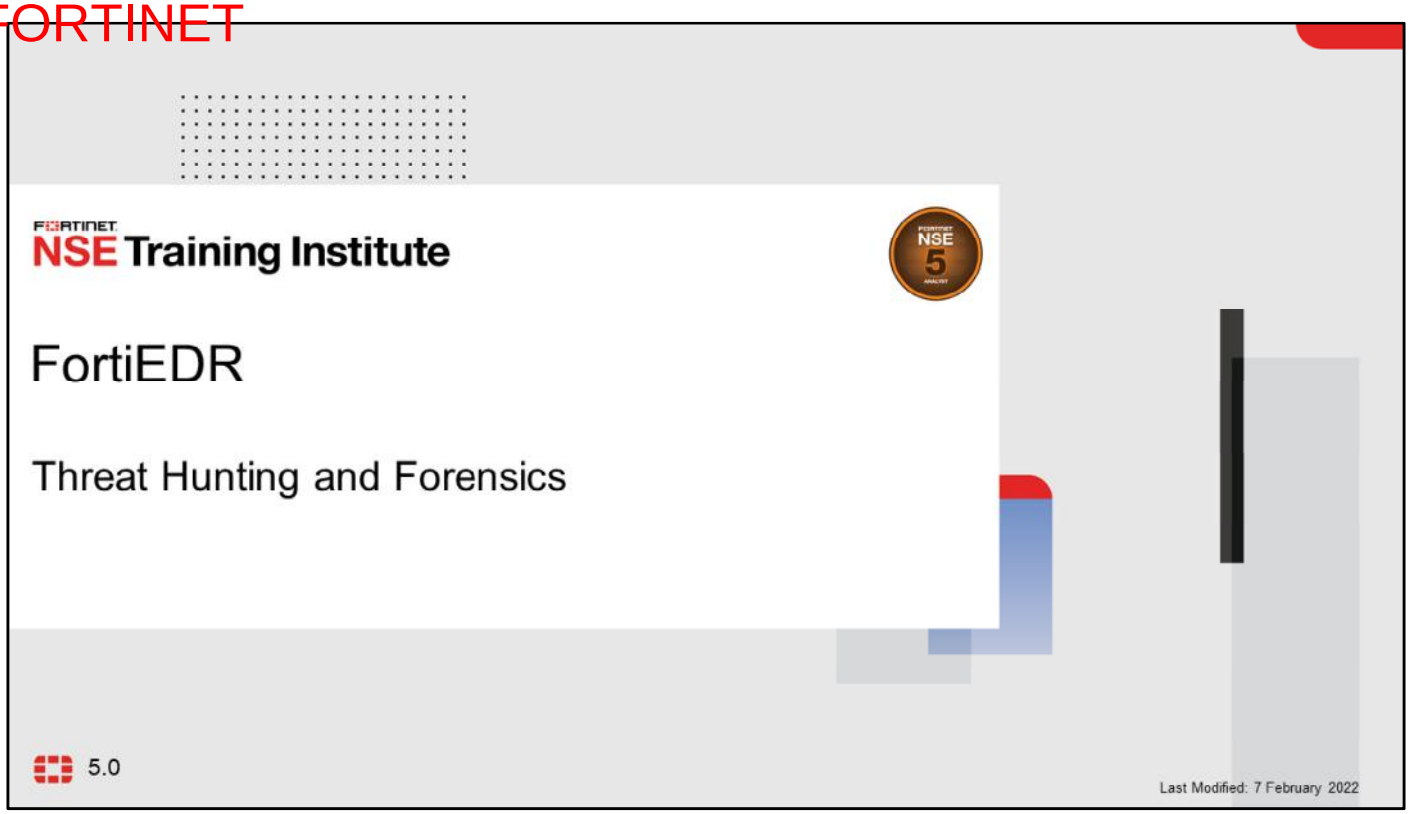
- ✓ Understand the security event hierarchy
- ✓ Understand how events work
- ✓ Identify the different event classifications
- ✓ Understand event aggregation
- ✓ View raw event data and advanced data
- ✓ Mark events
- ✓ Find, handle, and archive events
- ✓ Understand IP Sets
- ✓ Understand how exception manger works
- ✓ Understand the relationship between exceptions and order of operations

This slide shows the objectives covered in this lesson.

By mastering the objectives covered in this lesson, you learned more about FortiEDR security events and alerts.

Vouchers & Dumps are Available | WhatsApp +201224560923

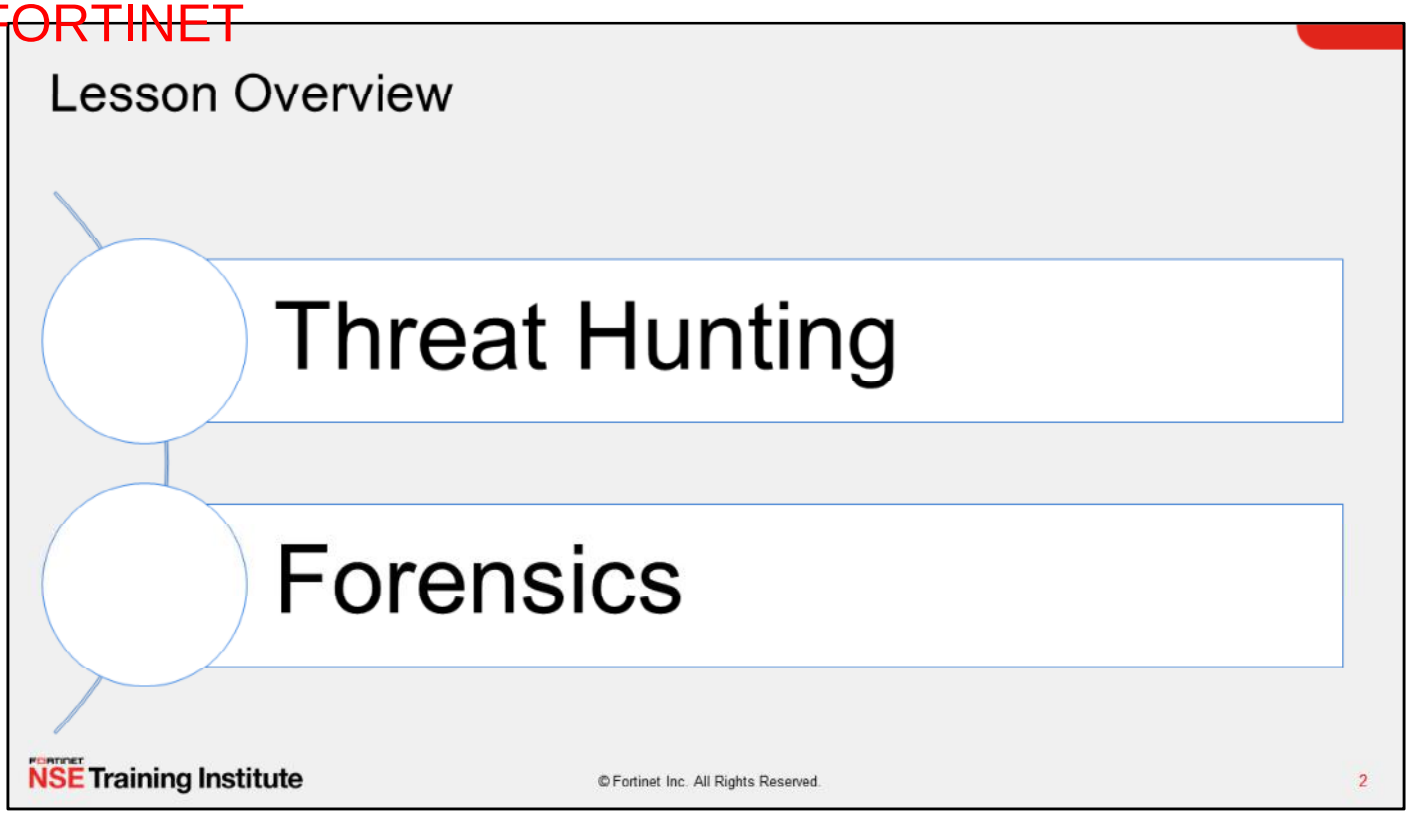
DO NOT REPRINT
© FORTINET
Brave-dumps.com



In this lesson, you will learn how to use threat hunting and forensics features on the FortiEDR console.

Vouchers & Dumps are Available | WhatsApp +201224560923

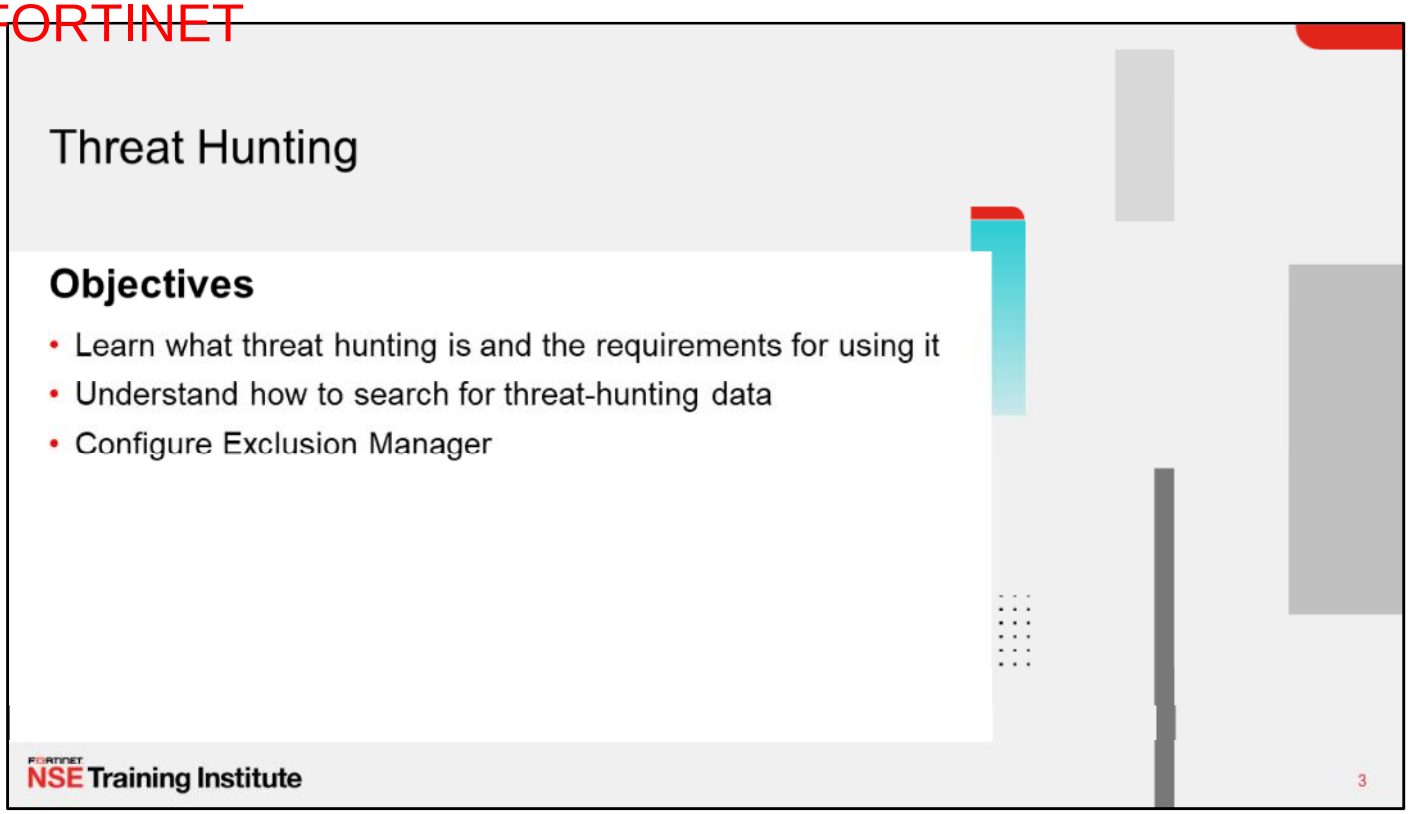
DO NOT REPRINT
© FORTINET
Brave-dumps.com



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 threat hunting, you will be able to query threat hunting data and create exclusion lists.

Vouchers & Dumps are Available | WhatsApp +201224560923

DO NOT REPRINT Brave-dumps.com
© FORTINET

Threat Hunting Overview

- What is threat hunting?
  - Searching for many types of indicators of compromise (IOCs) and malware across the environment
  - Searching based on hash, files, registry keys and values, network, processes, and event logs
  - Currently supported only for Windows endpoints
- Threat hunting requirements:
  - Add-on license
  - Central manager installed before repository server
  - Minimum 24 GB RAM, 16 CPUs, and 1.5 TB disk space to service 4000 collectors and retain one month of data

NSE Training Institute

© Fortinet Inc. All Rights Reserved.

4

The threat-hunting module records the details of every device in your organization. Management console users can then search the entire environment for IOCs and malware. Searching can based on hash, files, registry keys and values, network, processes, and event logs. Currently threat hunting is supported only for Windows endpoints.

Threat hunting allows management console users to find and remediate dormant threats before they execute. Essentially it's a search and destroy operation. Threat hunting also helps you unravel the story behind what was initially attacked, what else was attacked, and so on.

To use the threat-hunting feature, you require a license. The threat hunting repository requires a minimum of 24 GB of RAM and 1.5 TB disk space to service 4000 collectors and retain one month of data. You must install the central manager before installing the threat-hunting repository server. For more details about server requirements, see the *FortiEDR Installation and Administration Guide*.

Vouchers & Dumps are Available | WhatsApp +201224560923

DO NOT REPRINT
© FORTINET
Brave-dumps.com

Which Data Is Collected ?

- Threat hunting uses activity events from endpoints
- FortiEDR can collect five different categories of activity events:
  - Registry key actions
  - File actions
  - Process actions
  - Network actions
  - Event log actions

NSE Training Institute

© Fortinet Inc. All Rights Reserved.

5

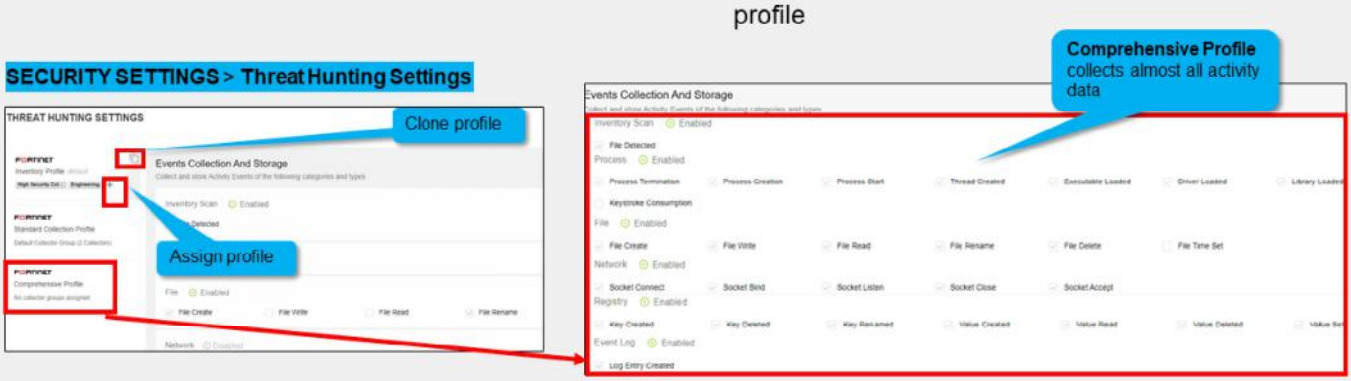
Threat hunting uses activity events, which consists of a source (usually a process), an action (activity event type), and a target (where the source performs the designated action on the target). Each time an action is performed on an endpoint, the collector sends several properties, based on the threat-hunting profile, to the threat-hunting repository through the core. FortiEDR can collect five different categories of activity events from endpoints: registry key actions, file actions, process actions, network actions, and event log actions.

Vouchers & Dumps are Available | WhatsApp +201224560923

DO NOT REPRINT Brave-dumps.com
© FORTINET

Threat-Hunting Profile

- A threat-hunting profile can control the type of activity data to be collected from endpoints
- Collector groups are assigned to threat hunting profiles
- Three default profiles are **Inventory Profile**, **Standard Collection Profile**, and **Comprehensive Profile**
- **Inventory Profile** collects basic file actions only
- **Comprehensive Profile** collects almost all data from endpoints and is more resource-intensive
- New collector groups are assigned to the default **Inventory Profile**
- New profiles can be created by cloning an existing profile



NSE Training Institute

© Fortinet Inc. All Rights Reserved.

6

To control the type of activity data collected from endpoints, you can configure threat hunting on the **Threat Hunting Settings** tab in **SECURITY SETTINGS**.

The three default profiles are **Inventory Profile**, **Standard Collection Profile**, and **Comprehensive Profile**. You can create a new profile by cloning an existing profile. The benefit of creating a new profile is that you can customize activity events by selecting the required categories and types. **Comprehensive Profile** collects almost all data from endpoints and is the most resource-intensive profile.

New collector groups are assigned to the default **Inventory Profile**. Depending on your organization's requirements, the collector groups can be assigned to one of the default profiles or to a new profile.

Vouchers & Dumps are Available | WhatsApp +201224560923

DO NOT REPRINT Brave-dumps.com
© FORTINET

Querying Threat-Hunting Data

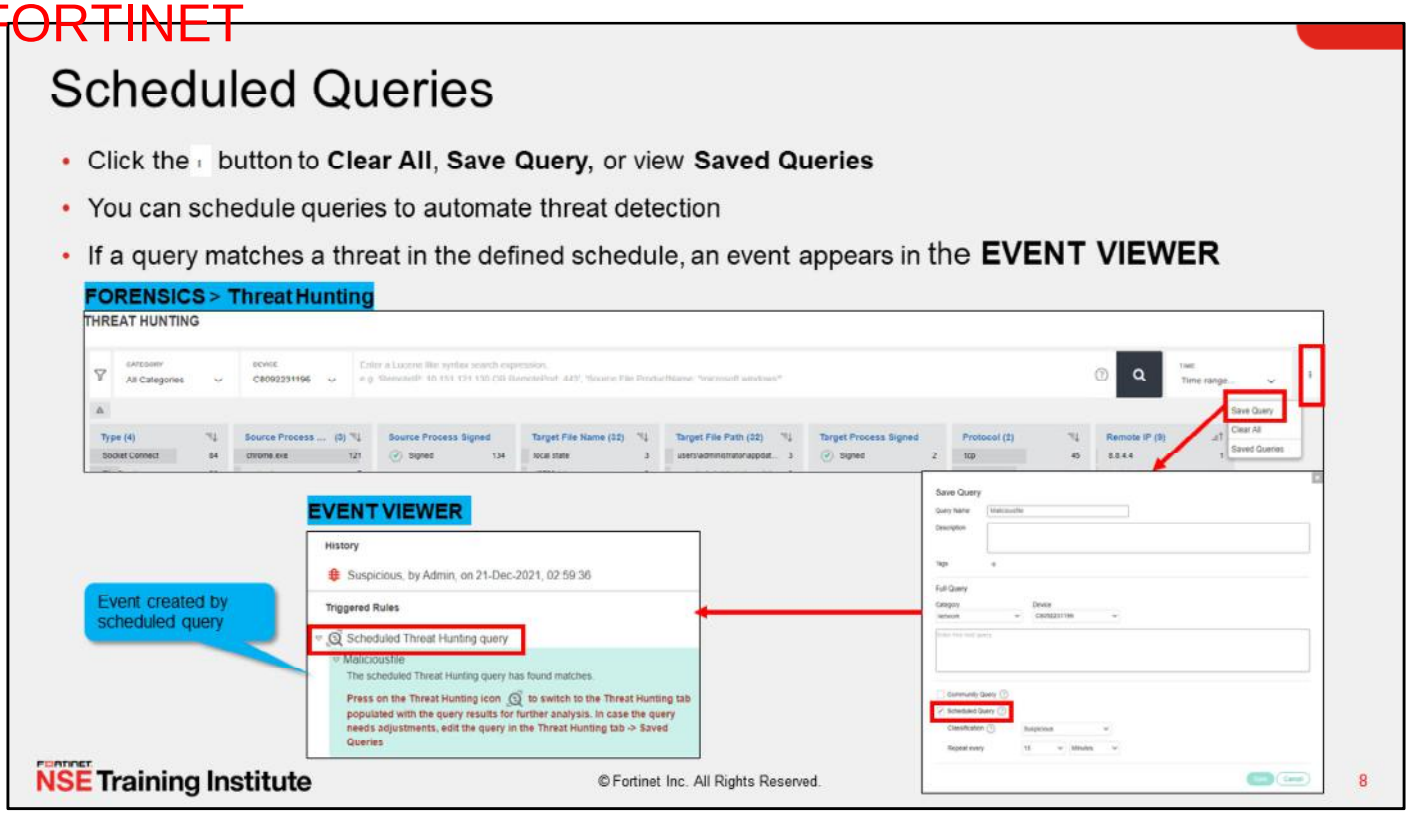
- The **Threat Hunting** data page is available for collectors running 5.0 or later
- Four built-in filters:
  - Category—filter the specific activity events
  - Device—filter by specific devices
  - Time—default filter is **last hour**
  - Free-text query—filter is based on Lucene syntax
    - For example, if you need to find data for remote IP address 192.168.100.10, the Lucene syntax would be `RemoteIP: 192.168.100.10`

NSE Training Institute
© Fortinet Inc. All Rights Reserved.

The **THREAT HUNTING** data page is available only for collectors running FortiEDR version 5.0 or later. You can view threat-hunting data on the **Threat Hunting** tab in **FORENSICS**. You can filter the data by activity event categories, specific devices, and time. Lucene syntax is supported for free-text queries, and has an autocomplete helper drop-down list. For more details about Lucene syntax, see the *FortiEDR Installation and Administration Guide*.

Vouchers & Dumps are Available | WhatsApp +201224560923

DO NOT REPRINT Brave-dumps.com
© FORTINET



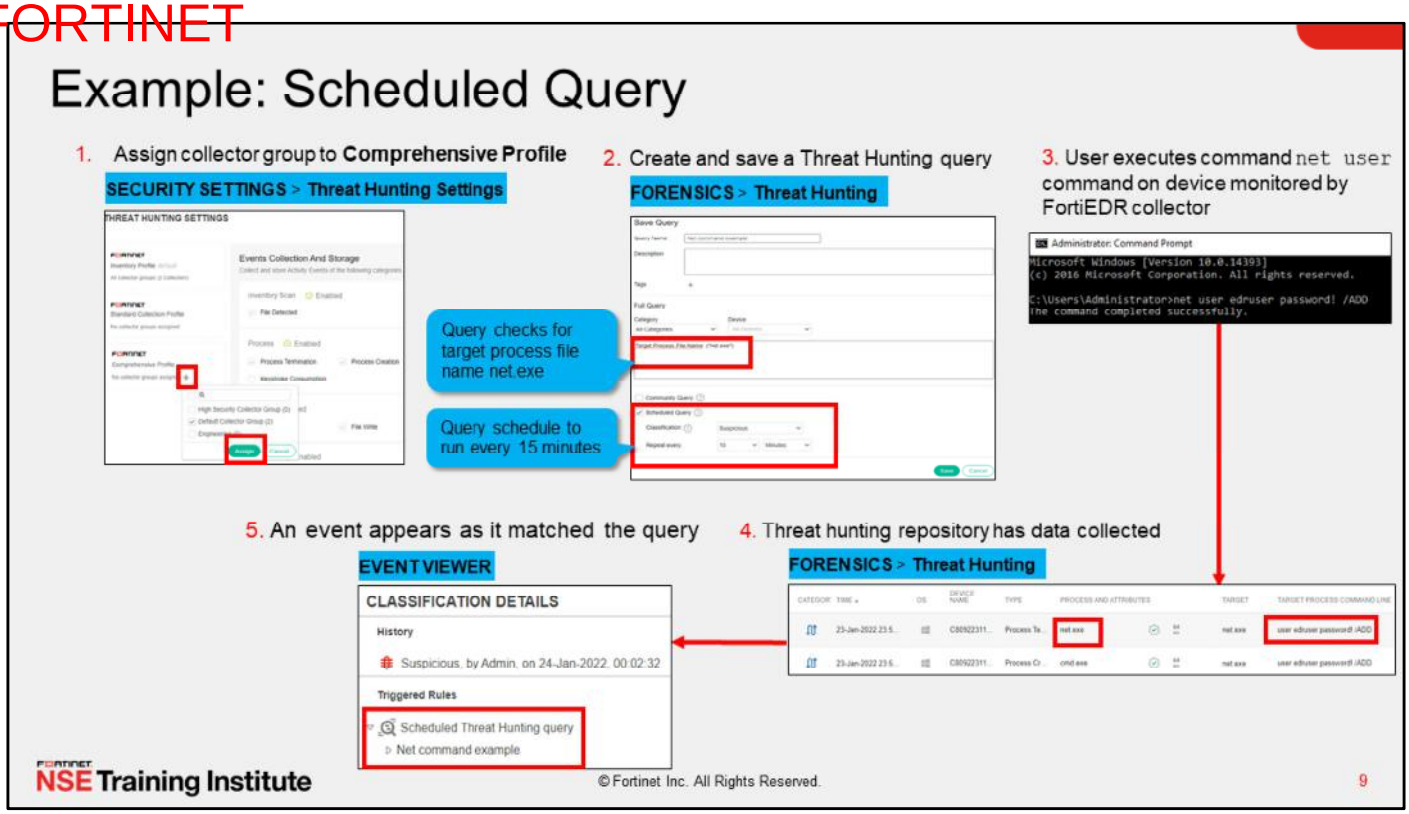
To clear the contents of a filter, click **Clear All** on the far right of the filters. To save a query, click **Save Query** as shown on this slide. Enter a **Query Name**, select a filter value from the **Category, Device and Time** drop-down lists and then click **Save**.

You can schedule queries to automate threat detection. If a query matches a threat in the defined schedule, an event appears in the **EVENT VIEWER**, and email and syslog notifications are generated.

To schedule a query, enable S**cheduled Query** in the **Save Query** window. Select the **Classification** of the security event from the drop-down list and configure the frequency in the **Repeat Every/On** section.

Vouchers & Dumps are Available | WhatsApp +201224560923

DO NOT REPRINT Brave-dumps.com
© FORTINET



This slide shows the flow of events to trigger a scheduled query event.

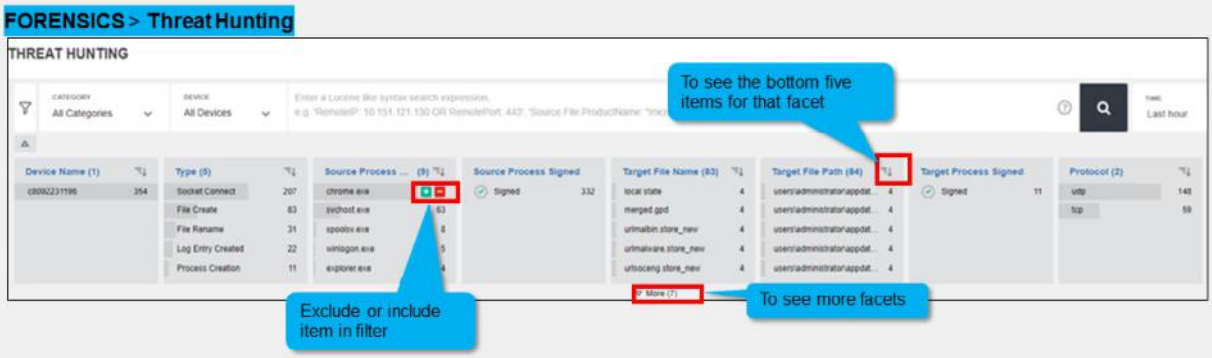
1. On the **SECURITY SETTINGS** tab, select **Threat Hunting Settings,** and then assign the collector group to a **Comprehensive Profile**, so almost all data can be collected from endpoints.
2. On the **FORENSICS** tab, select **Threat Hunting,** and then create a query to run every 15 minutes and check for the target process file name `net.exe`.
3. Run the `net user` command on an endpoint monitored by the FortiEDR collector, as shown in the slide. The `net user` command will not trigger any FortiEDR rules because the activity is not suspicious.
4. The threat hunting repository will contain the data about the `net user` command execution.
5. The scheduled query is run every 15 minutes, and when the query matches a threat (`net.exe`), an event appears in the **EVENT VIEWER**.

Vouchers & Dumps are Available | WhatsApp +201224560923

DO NOT REPRINT Brave-dumps.com
© FORTINET

Facets

- Aggregated view of the activity events tables
- Assist in adding criteria to the filters
  - Click the green plus to include the item in the filter
  - Click the red minus to exclude the item from the filter
- Each facet pane summarizes the top five items for that facet
  - Click to see the bottom five items for that facet



NSE Training Institute

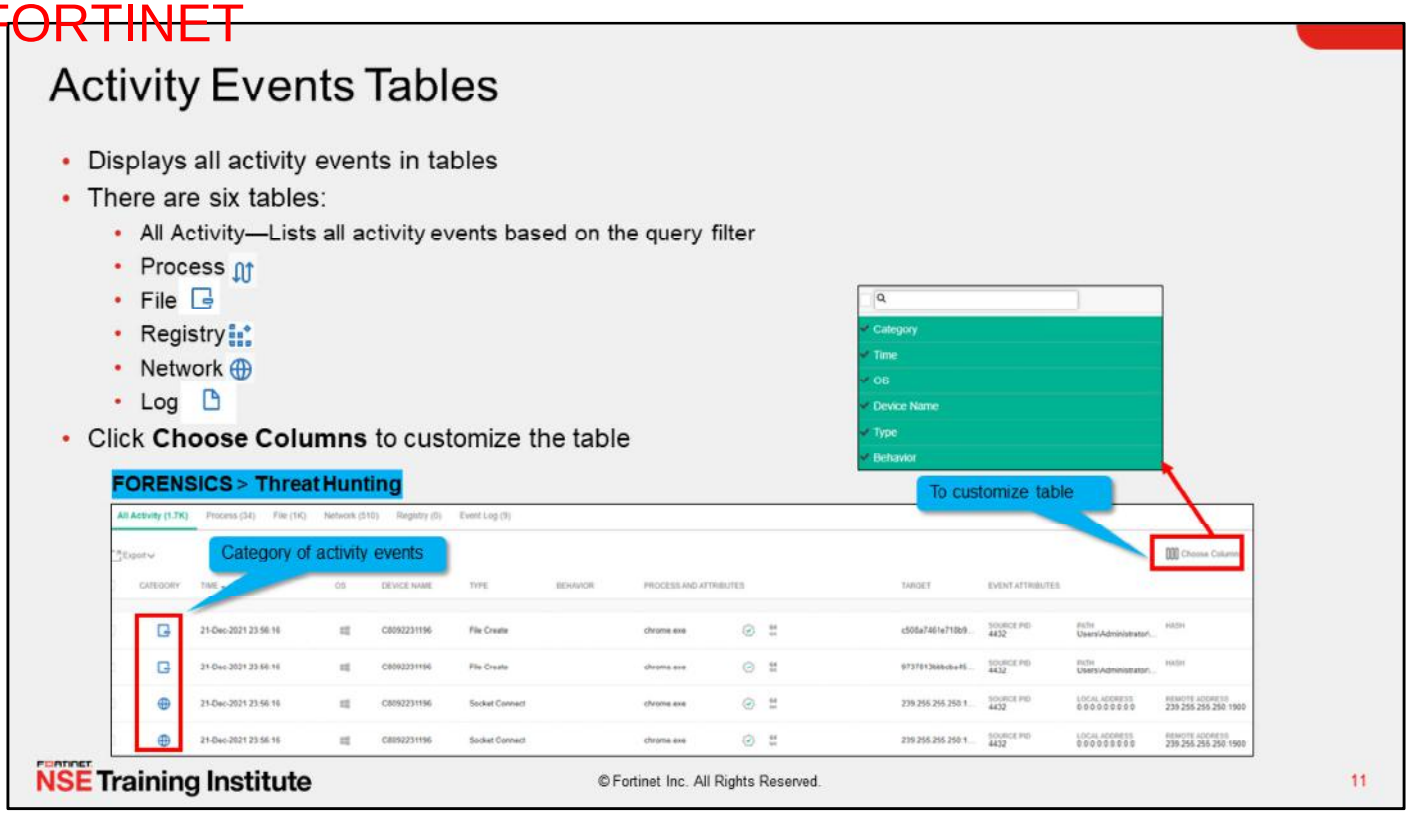
© Fortinet Inc. All Rights Reserved.

10

The real-time collection of threat-hunting data from endpoints, creates numerous activity events. Facets displays this data in tables in an aggregated form. Each facet pane displays a summary of the top five items for that facet. Click on the arrow as shown in the example to switch the ordering to display the bottom five items for that specific facet. To see additional facets, click the **More** link. You can use facets to filter data. Click the green plus sign beside an item on the facet to include the item in a query, and click the red minus button to exclude the item.

Vouchers & Dumps are Available | WhatsApp +201224560923

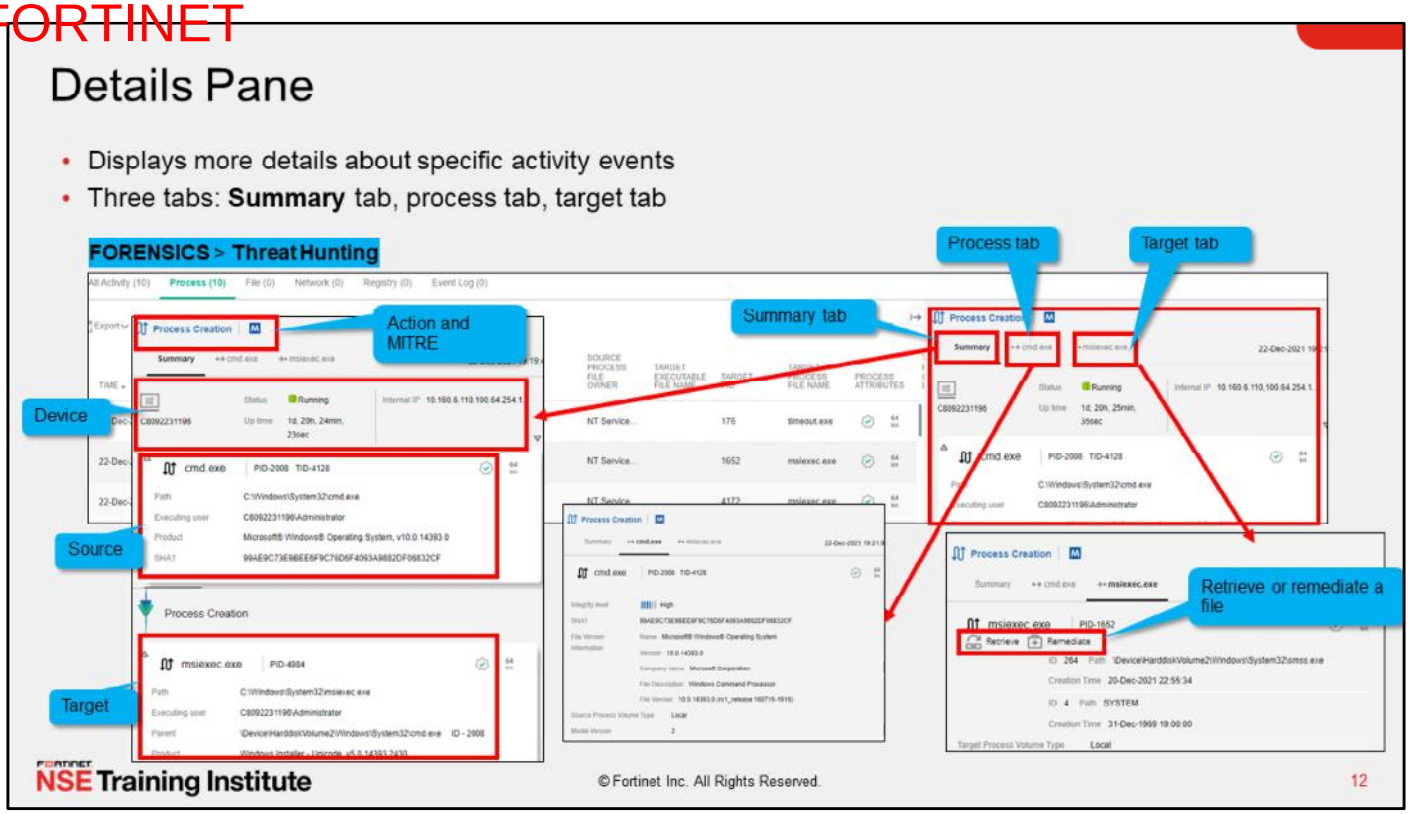
DO NOT REPRINT Brave-dumps.com
© FORTINET



The six activity events tables consist of one table for each activity event category and the **All Activity** table, which displays all activity event categories. Click **Choose Columns** to add or remove columns from the displayed data results. You can add filters to activity events tables in the same way as facets.

Vouchers & Dumps are Available | WhatsApp +201224560923

DO NOT REPRINT Brave-dumps.com
© FORTINET



Click anywhere in a row in the activity event table on a specific activity event to display a pane with full details of that activity event. The details pane includes three tabs: **Summary** tab, process tab, and target tab.

The **Summary** tab displays a summary of the activity event. The top section shows the action, which is the activity event type, and a MITRE icon if the activity is associated with MITRE techniques. You can hover over the MITRE icon to see the MITRE details. The next section shows the endpoint details, such as device name, connectivity status, uptime, and IP addresses. The source section displays details about the source process. The last section displays details about the target process.

The process tab displays additional details about the source process, and the target tab displays additional details about the target process. The target tab is displayed only if the target of the activity event is of type Process or File. Upon malware detection, click the **Retrieve** button to download a copy of the file, or you can delete the file using the **Remediate** button in the target tab.

Vouchers & Dumps are Available | WhatsApp +201224560923

DO NOT REPRINT Brave-dumps.com
© FORTINET

Threat Hunting (Legacy)

- **Threat Hunting (Legacy)** page is available only in environments that were upgraded to version 5.0 from an earlier version
- Search for hashes and files that were collected before the upgrade
- Data is displayed on the legacy page for collectors running versions earlier than 5.0

FORENSICS > Threat Hunting (Legacy)

NSE Training Institute

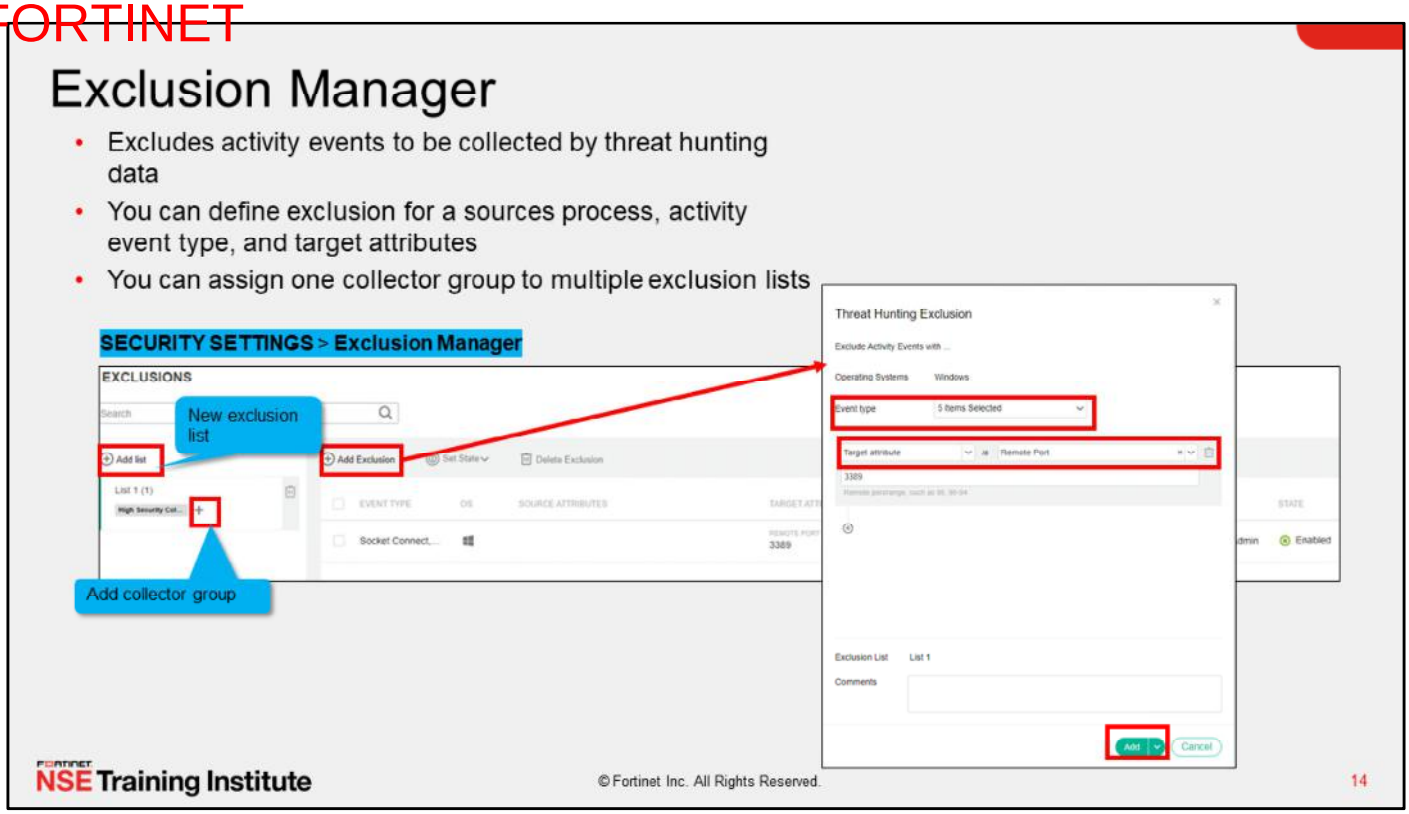
© Fortinet Inc. All Rights Reserved.

13

The legacy threat-hunting page is available only in environments that were upgraded to FortiEDR version 5.0 from an earlier version. You can view the legacy page on the **Threat Hunting (Legacy)** tab in **FORENSICS**. You can search all hashes and files that FortiEDR collected before the upgrade to version 5.0. Threat-hunting data for collectors running versions earlier than 5.0 are also available on the legacy page.

Vouchers & Dumps are Available | WhatsApp +201224560923

DO NOT REPRINT Brave-dumps.com
© FORTINET



You can access the Exclusion Manager on the **Exclusion Manager** tab in **SECURITY SETTINGS**. You can use the Exclusion Manager to exclude activity events to be collected by threat hunting data. Click **Add list** and enter a name for the exclusion list. After you create a list, click **Add Exclusion** to exclude activity events. In the **Threat Hunting Exclusion** pane, you can define exclusions for a source process, activity event type, and target attributes. After you define the attributes, click **Add** to save the exclusion list. The last step is to assign a collector group to the exclusion list. You can assign a collector group to multiple exclusion lists.

Vouchers & Dumps are Available | WhatsApp +201224560923

DO NOT REPRINT
© FORTINET
Brave-dumps.com

Knowledge Check

1. What is the function of facets on the threat hunting tab?
   A. To automate threat detection
   ✓ B. To display an aggregated view of the activity event tables

2. Which tab in the details pane shows the device name and IP address?
   ✓ A. Summary tab
   B. Target tab

NSE Training Institute

© Fortinet Inc. All Rights Reserved.

15

Vouchers & Dumps are Available | WhatsApp +201224560923

DO NOT REPRINT
© FORTINET
Brave-dumps.com

Good job! You now understand threat hunting.

Now, you will learn about forensics.

Vouchers & Dumps are Available | WhatsApp +201224560923

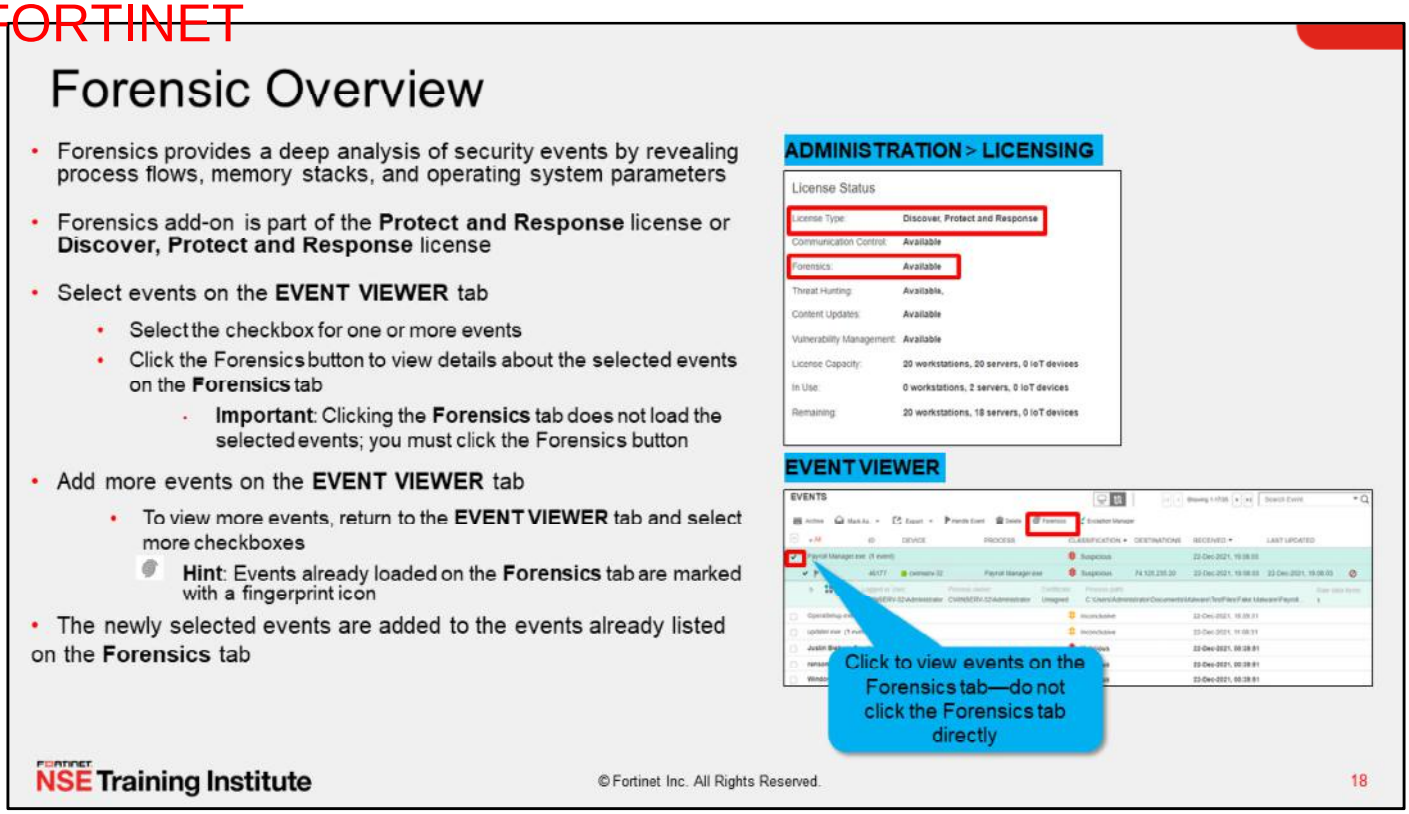
DO NOT REPRINT
© FORTINET
Brave-dumps.com

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

By demonstrating competence in forensics, you will be able to use forensics to investigate security events.

Vouchers & Dumps are Available | WhatsApp +201224560923

DO NOT REPRINT Brave-dumps.com
© FORTINET



Forensics provides a deep analysis of security events, by revealing process flows, memory stacks, and operating system parameters. The forensics add-on is part of the **Protect and Response** license or **Discover, Protect and Response** license.

You can select events from the **EVENT VIEWER** tab to view on the **Forensics** tab, where you can analyze them in depth. Select the checkbox for one or more events, and then click the **Forensics** button. The event is loaded onto the **Forensics** tab. Make sure you click the **Forensics** button, *not* the **Forensics** tab. If you click the **Forensics** tab, it opens without loading the selected events.

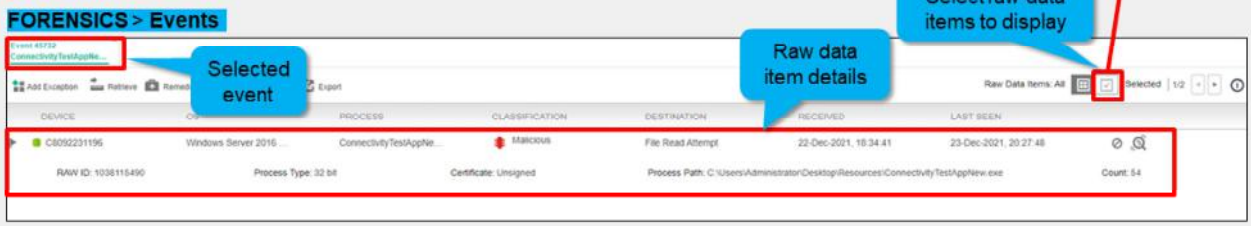
To add events, return to the **EVENT VIEWER** tab and repeat the same steps. You'll see a fingerprint next to the events that are already loaded in **Forensics**. Click the **Forensics** button again to add your new selections to the events you've already loaded.

Vouchers & Dumps are Available | WhatsApp +201224560923

DO NOT REPRINT Brave-dumps.com
© FORTINET

Raw Data Items

- Scroll through raw data items for an event
  - A single event may contain multiple raw data items
  - Use the arrow at the upper-left of the pane to scroll through items
- Filter to display only selected raw data items
  - Click **Selected raw data items** to select the items you want to view
  - In the pop-up window, select which items you want to display, then click **Close**
  - To restore all raw data items, click **All raw data items**

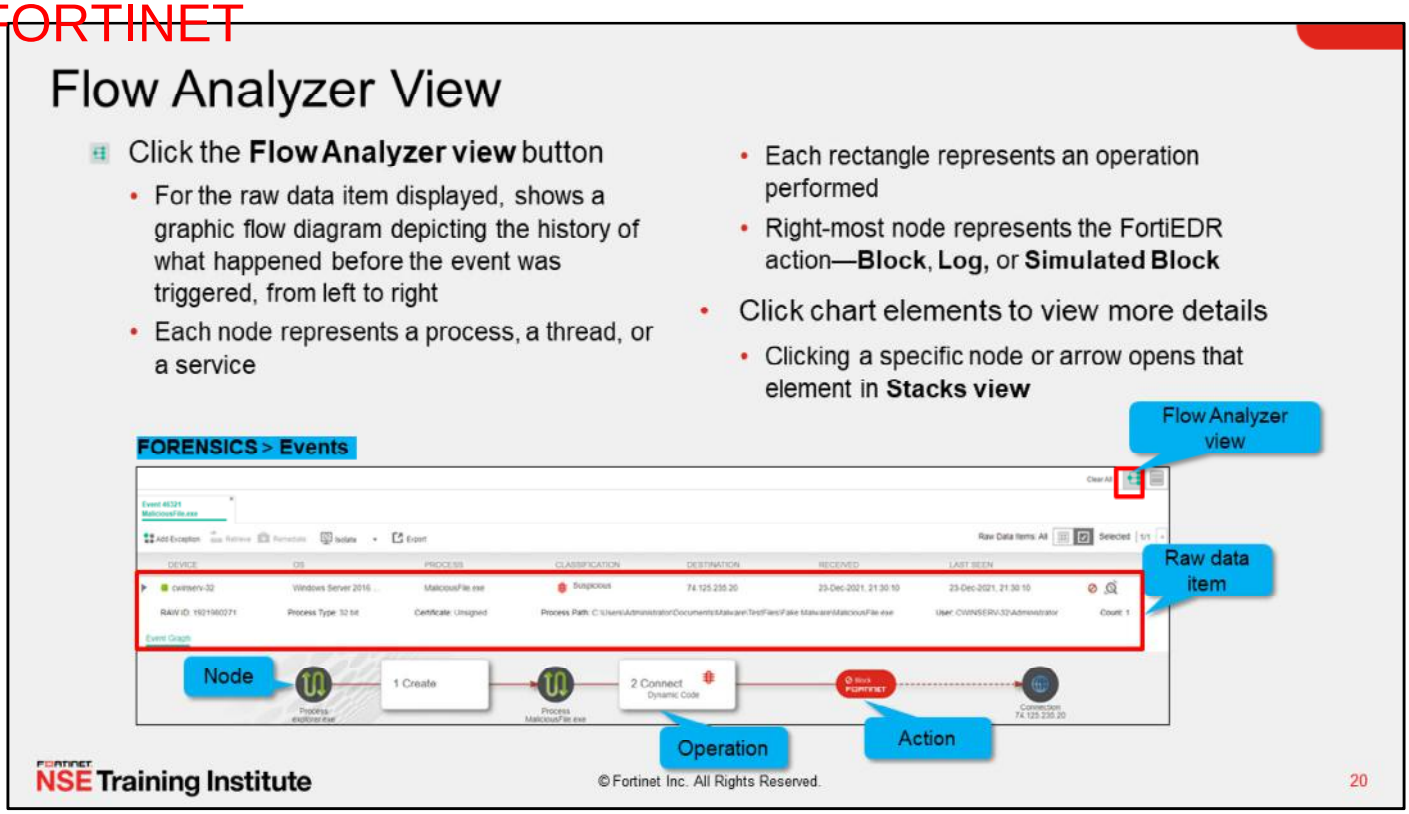


© Fortinet Inc. All Rights Reserved.

A single event may be made up of one or more raw events. The raw event data is shown on the upper portion of the **FORENSICS** tab. You can use the arrows on the upper-right of the pane to browse through each raw data item. If you want to focus on specific raw events, you can click **Selected raw data items**, then select the checkboxes for each raw event you want to see. You can click **All raw data items** to restore the hidden raw events.

Vouchers & Dumps are Available | WhatsApp +201224560923

DO NOT REPRINT Brave-dumps.com
© FORTINET



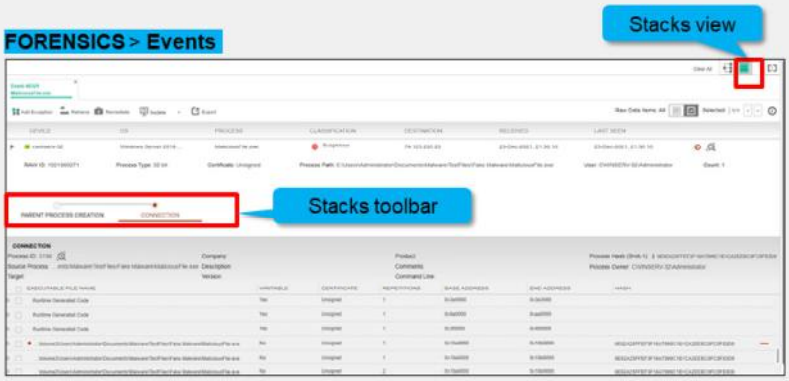
When you first load an event onto the **FORENSICS** tab, you'll see the Flow Analyzer view. The process flow diagram for the selected raw event is similar to the one shown in the **EVENT VIEWER** tab. Each node represents a process, flow, or service involved in the selected raw event. The white rectangles represent an operation performed. For example, in the event shown on this slide, you can see that the process `explorer.exe` created the process `MaliciousFile.exe`. The series of events shown in this example generally means that the user launched the process—`MaliciousFile.exe`. As you continue to examine the sample, you can see `MaliciousFile.exe` attempting to connect to the IP address shown, but FortiEDR blocks the connection because it violates the dynamic code rule. You can click any of these elements to see details in the Stacks view.

Vouchers & Dumps are Available | WhatsApp +201224560923

DO NOT REPRINT Brave-dumps.com
© FORTINET

Stacks View

- Click the **Stacks view** button
  - View details about the selected process and its sub-process(es)
- Stacks toolbar
  - For the raw data item displayed, shows the stacks collected in each step prior to the rule violation
  - A red dot ● means that a rule violation was observed in this stack
  - Click a stack name to view the collected data for that stack
  - **Hint**: The name of the currently displayed stack appears in red



NSE Training Institute

© Fortinet Inc. All Rights Reserved.

21

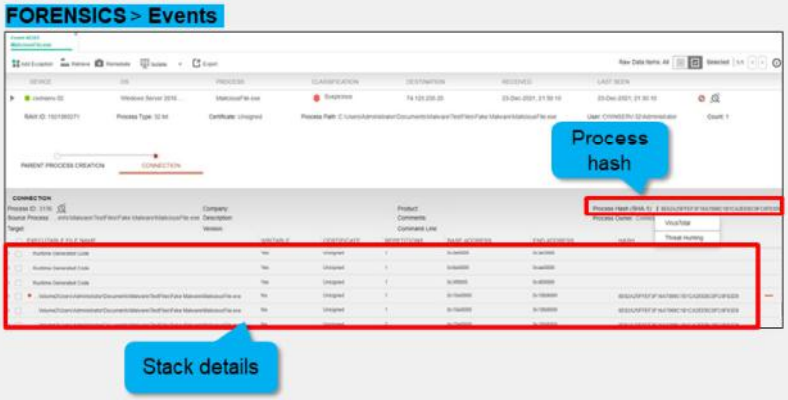
Here's an example of the Stacks view. You can click each stack in the stacks toolbar to see all the collected data for that stack. Red dots indicate where a violation occurred, so you can quickly find the source of the problem. For example, in the stacks toolbar, you can see that the violation was in the **Connection** stack. The selected stack name is shown in red—in this case, the **Connection** stack. You'll see all the collected details for the selected stack below the stacks toolbar. You'll learn more about the stacks details next.

Vouchers & Dumps are Available | WhatsApp +201224560923

DO NOT REPRINT Brave-dumps.com
© FORTINET

Stack Details

- For the selected stack, you see:
  - The executable file name
  - Whether that file is writeable
  - Whether the certificate was signed
  - How many repetitions were detected in the stack
  - The base address and end address in memory
- The process and subprocess that triggered the FortiEDR event is marked with a red dot ●
- Click on a row to view further details about that subprocess
- Click the three vertical dots next to the **Process Hash** to search the **Threat Hunting** tab or **VirusTotal** for that hash



NSE Training Institute

© Fortinet Inc. All Rights Reserved.

22

Details about the main process of the selected stack—the file name, the publisher, and so on—as well as the main process hash, are shown on the pane. Click the three vertical dots next to the **Process hash** to search for the hash in the **Threat Hunting** tab or to use **VirusTotal**. VirusTotal is a useful investigation tool. It shows you how other prominent security programs have classified a file—malicious or safe—and the name assigned to the threat represented by the file.

You can also view a list of every subprocess in the stack and its details. The number of subprocesses you see depends on the stack. The red dot next to the first executable in the list, indicates that a rule violation occurred there. Click a subprocess to view more information. Each subprocess has its own hash, which you can look up in VirusTotal or Threat Hunting.

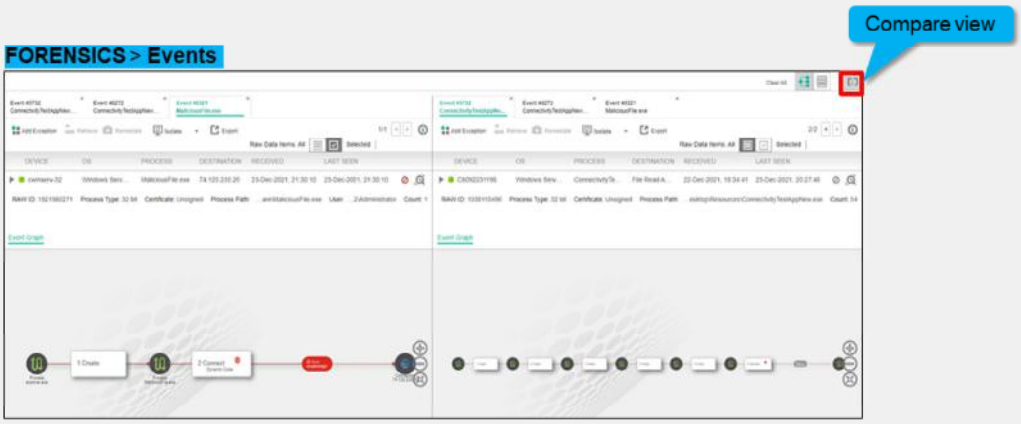
Vouchers & Dumps are Available | WhatsApp +201224560923

DO NOT REPRINT Brave-dumps.com
© FORTINET

Compare View

Click the **Compare View** button

- Two events can be viewed side-by-side



NSE Training Institute

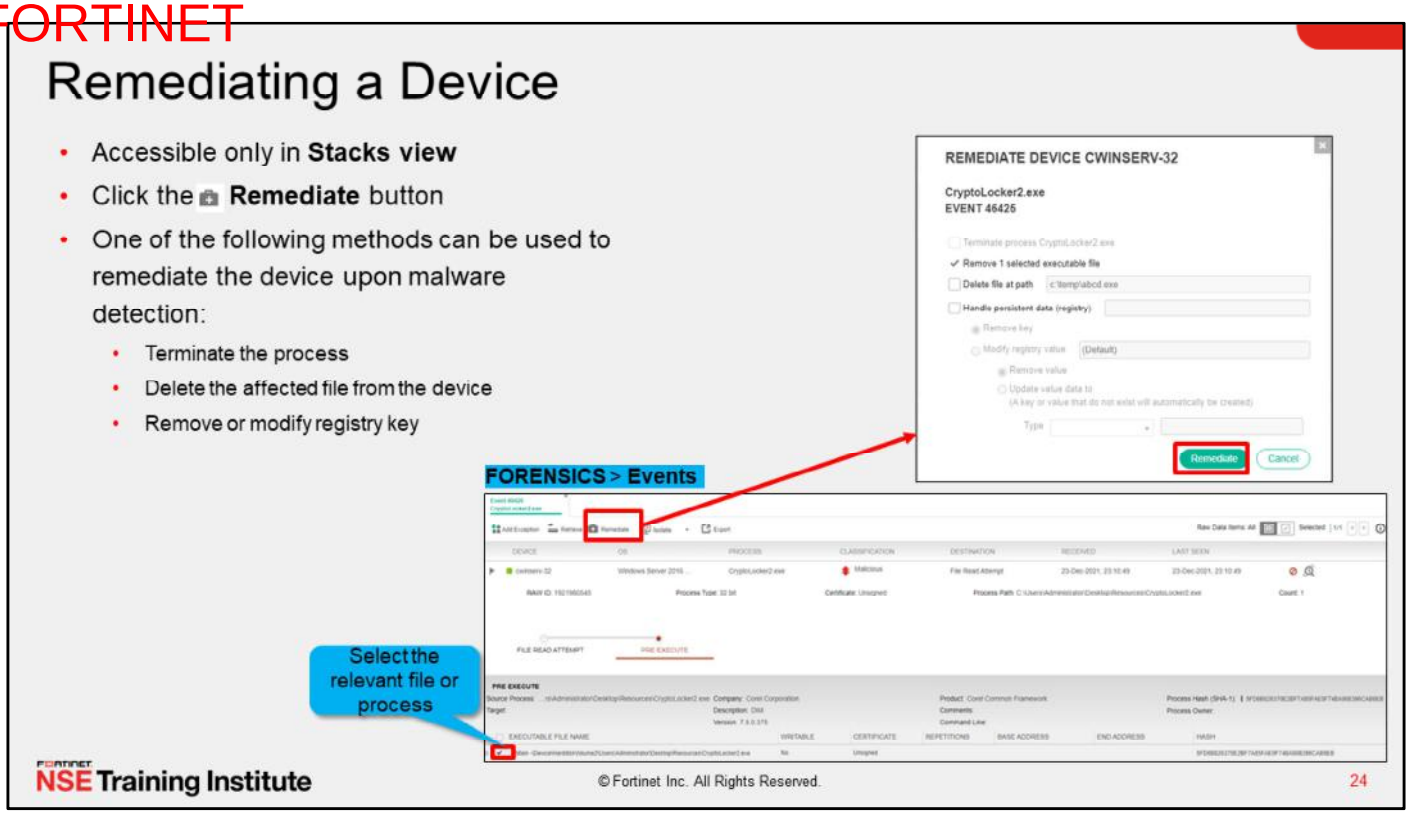
© Fortinet Inc. All Rights Reserved.

23

This slide shows an example of the **Compare view**. You can view two events side-by-side, and they both can be either in the **Flow Analyzer view** or **Stacks view**.

Vouchers & Dumps are Available | WhatsApp +201224560923

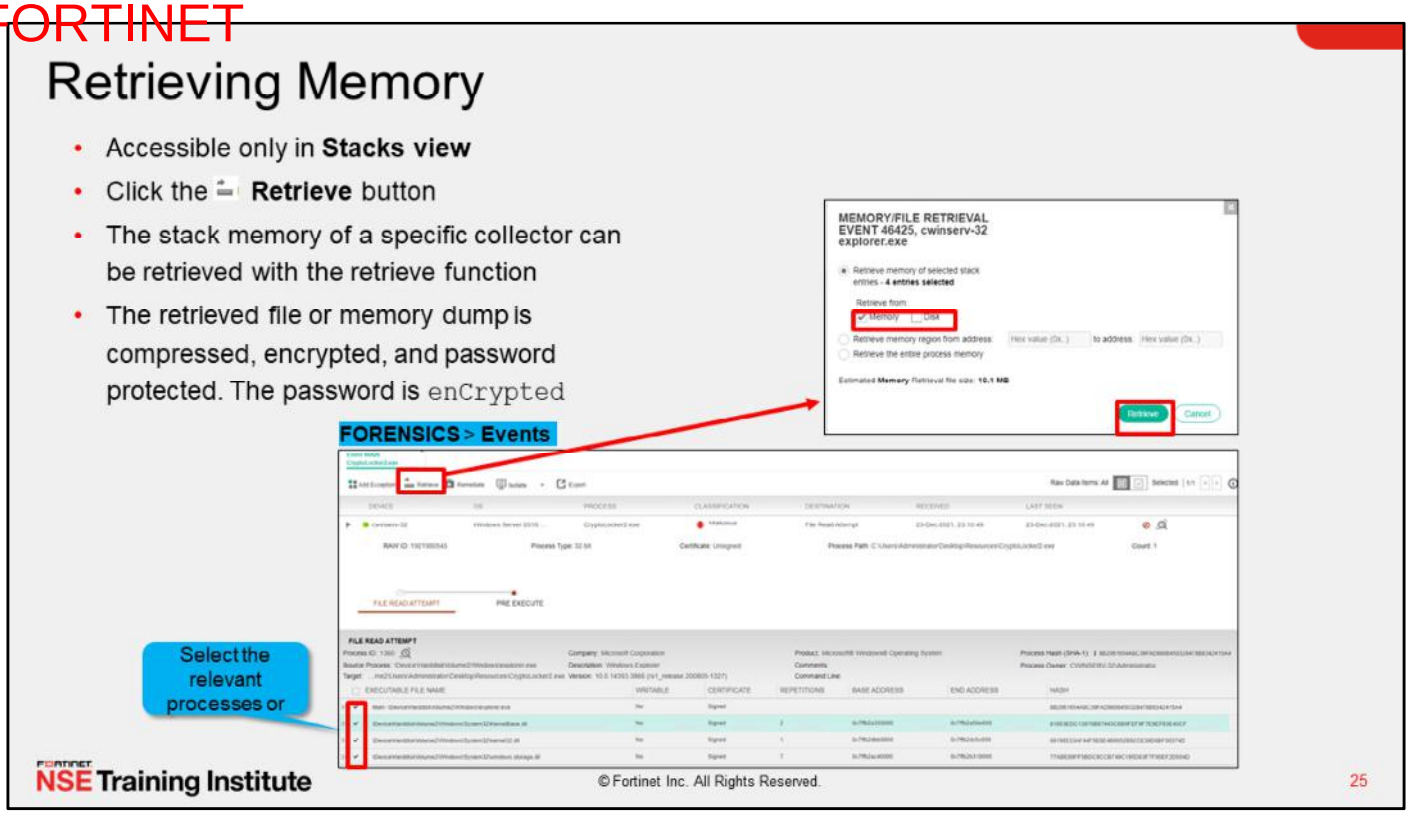
DO NOT REPRINT Brave-dumps.com
© FORTINET



After malware is detected on a device, one of the following methods can be used to remediate the device—terminate the process, delete the affected file from device, or remove or modify the registry key. In the **Stacks view,** click the process of interest and select the checkbox of the relevant file. Click **Remediate,** and then select an action for remediating the device.

Vouchers & Dumps are Available | WhatsApp +201224560923

DO NOT REPRINT Brave-dumps.com
© FORTINET



Use the **Stacks view** to retrieve the stack memory of a specific collector. The stack memory helps you analyze the memory dump from the device and a copy of the file, if applicable. Click the process of interest, and then select the checkboxes of the relevant files and processes. Click **Retrieve,** and then select an action for remediating the device. In the **MEMORY/FILE RETRIEVAL** window, specify whether to retrieve from **Memory, Disk,** or both, and whether to retrieve from a specific memory region or the entire process memory. The retrieved file or memory dump is compressed, encrypted, and password protected. The password to unzip the retrieved file is `enCrypted`.

Vouchers & Dumps are Available | WhatsApp +201224560923

DO NOT REPRINT
© FORTINET
Brave-dumps.com

Knowledge Check

1. On the **FORENSICS** tab, which view shows details about the selected process and its sub-processes?
   - ✓ A. Stacks view
   - B. Flow Analyzer view

2. On the **FORENSICS** tab, what does a red dot in the stacks toolbar indicate?
   - A. A stack containing unhandled events
   - ✓ B. A stack where a rule violation occurred

NSE Training Institute

© Fortinet Inc. All Rights Reserved.

26

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

Review

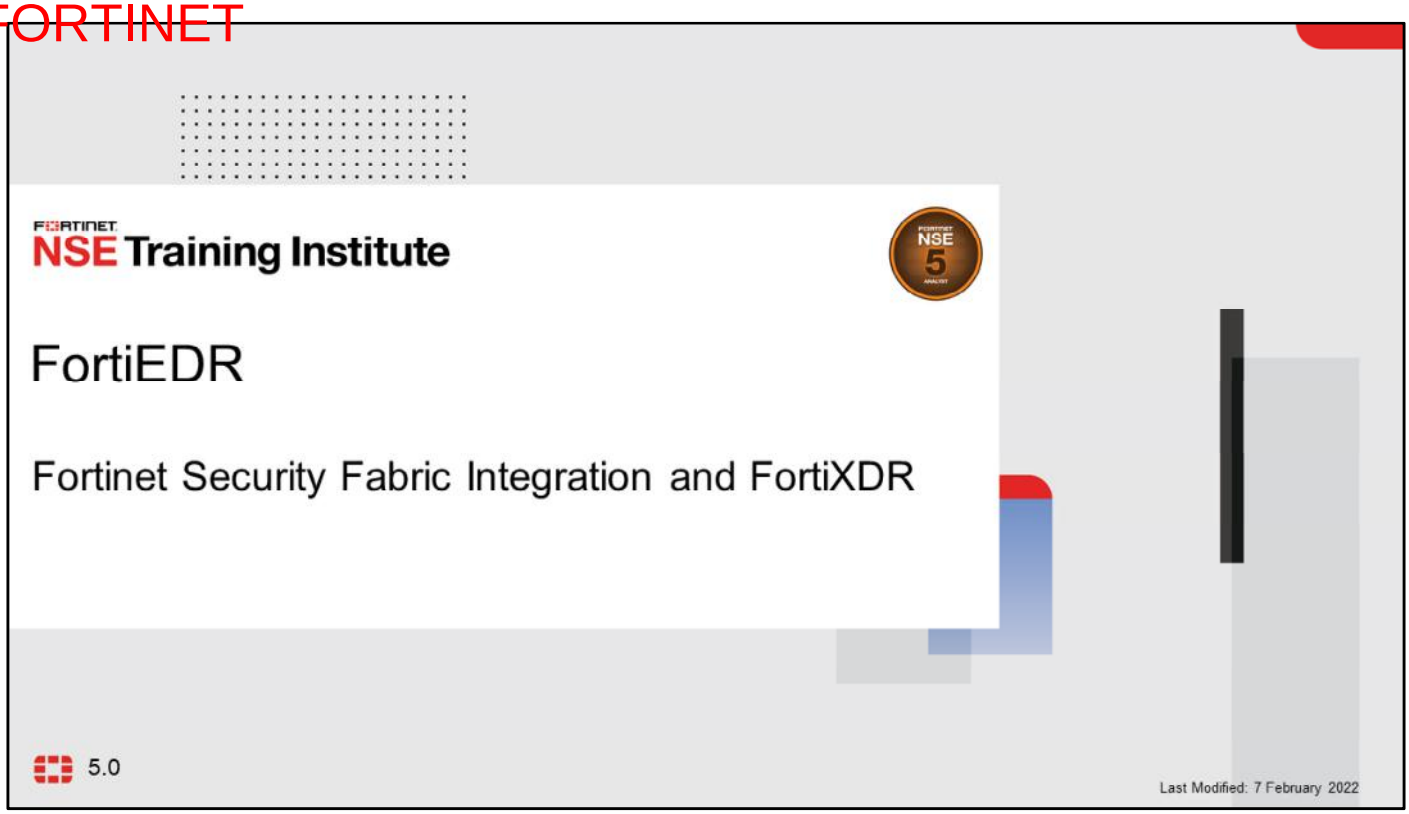
- ✓ Know what threat hunting is and the requirements for using it
- ✓ Understand how to search for threat-hunting data
- ✓ Configure Exclusion Manager
- ✓ Understand how to add security events to forensics
- ✓ Identify the different forensics views
- ✓ Understand how to remediate a device and retrieve memory from specific devices

This slide shows the objectives covered in this lesson.

By mastering the objectives covered in this lesson, you learned how to use threat hunting and forensics in an investigation.

Vouchers & Dumps are Available | WhatsApp +201224560923

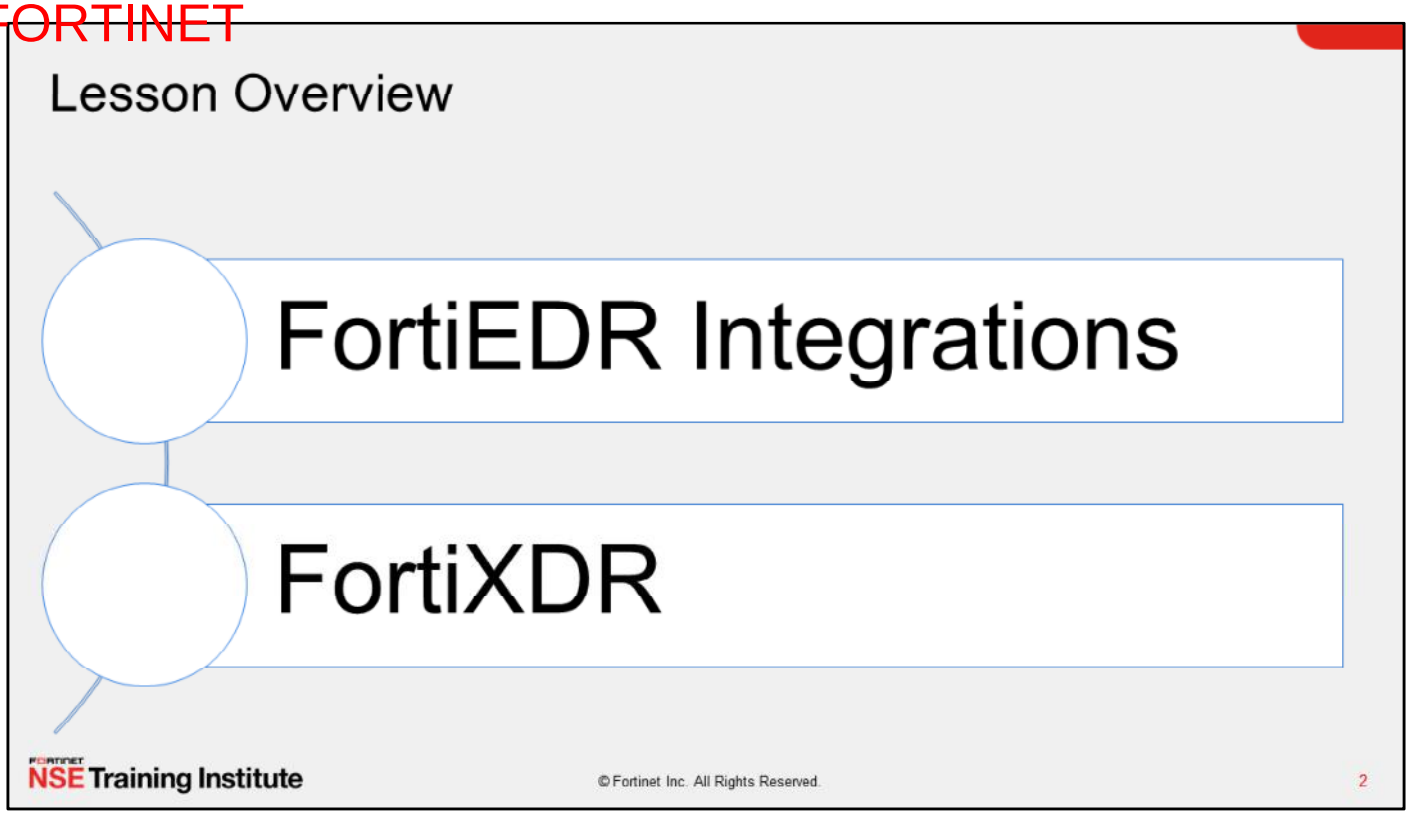
DO NOT REPRINT
© FORTINET
Brave-dumps.com



In this lesson, you will learn about Fortinet Security Fabric integration and FortiXDR.

Vouchers & Dumps are Available | WhatsApp +201224560923

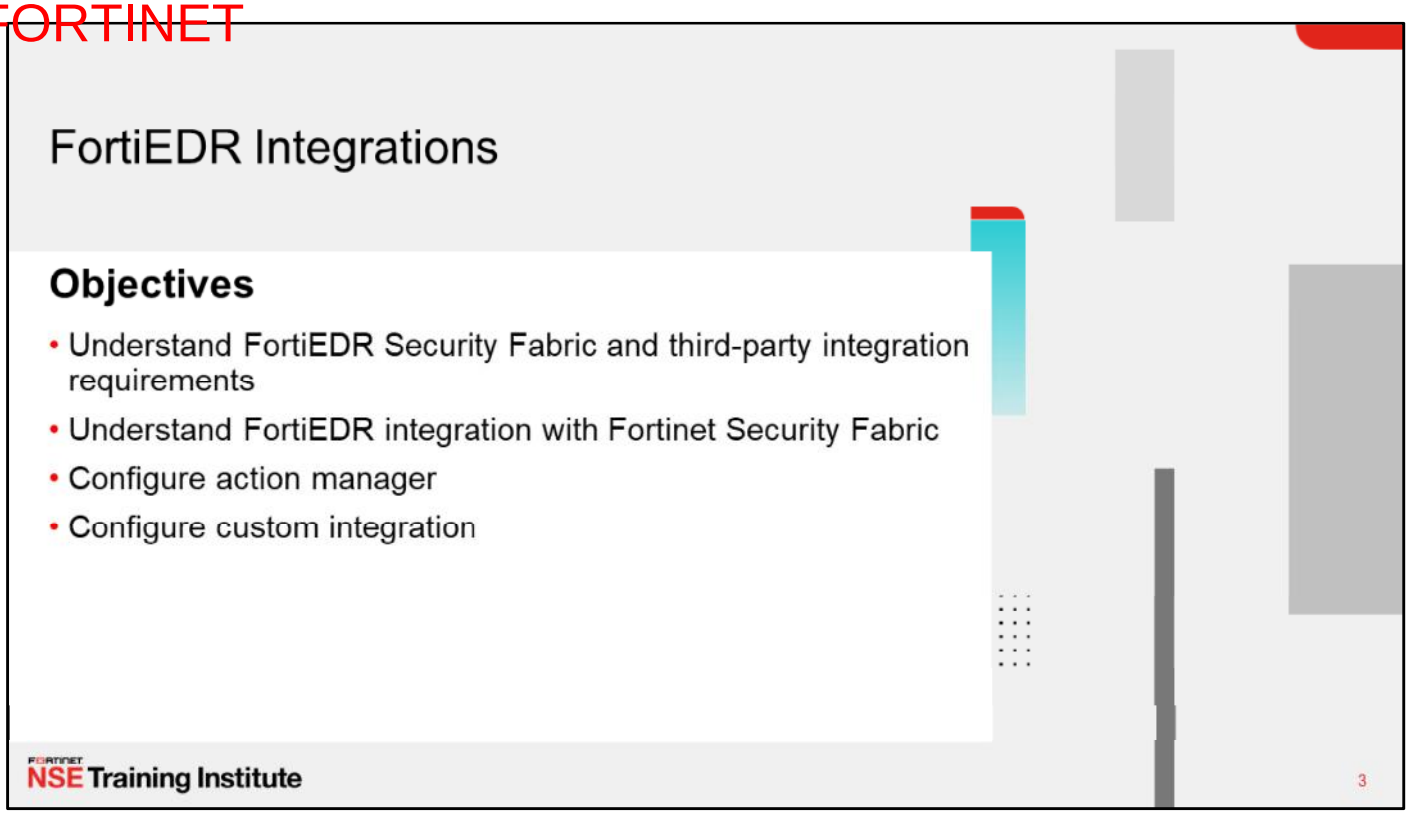
DO NOT REPRINT
© FORTINET
Brave-dumps.com



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 the Fortinet Security Fabric and third-party integrations, you will be able to configure connectors and understand the automated incident response.

Vouchers & Dumps are Available | WhatsApp +201224560923

DO NOT REPRINT Brave-dumps.com
© FORTINET

Fortinet Security Fabric and Third-Party Integrations

- Integrate with security devices:
  - Firewall: Automatically add malicious IP addresses to blocked lists
  - Network access control (NAC): Isolate a device using a FortiNAC device
  - Sandbox: Automatically send malicious files to FortiSandbox for analysis
  - Custom Connector: Third-party integration for automated incident response
- FortiEDR requirements:
  - Central manager connected to FCS
  - On-premises core with jumpbox functionality
  - A valid API user with access to connectors

NSE Training Institute

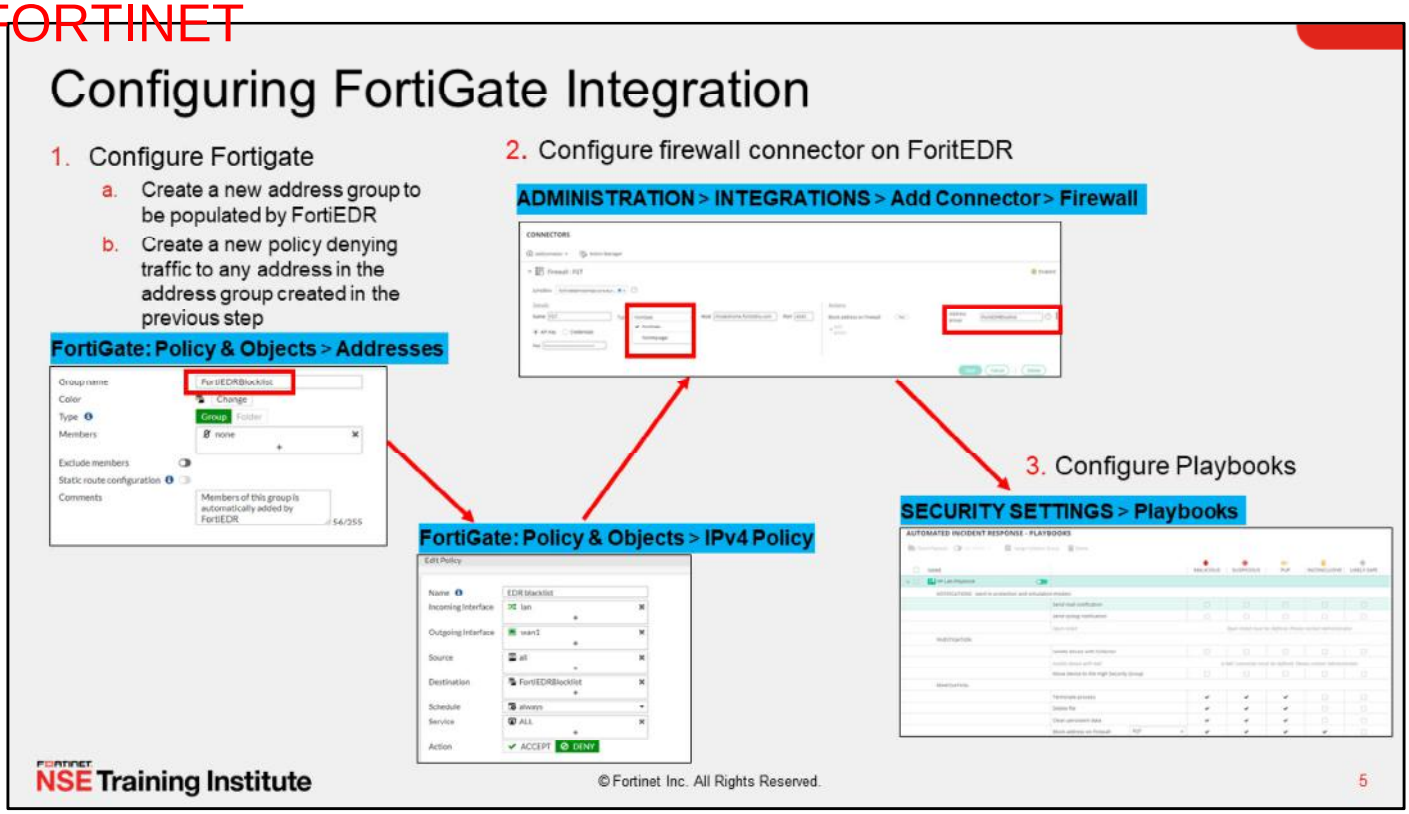
© Fortinet Inc. All Rights Reserved.

4

FortiEDR version 5.0.3 can be integrated with multiple connectors for automated incident response. You can configure your integration using RESTful API or on the **ADMINISTRATION** tab of the management console under **INTEGRATIONS**. Be aware that you also need to configure connectors as well to integrate with FortiEDR. To configure your integrations on FortiEDR, you will need an on-premises core with jumpbox functionality and a valid API user able to access FortiGate, FortiManager, FortiSandbox, and/or FortiNAC . You'll also need a central manager that is connected to Fortinet Cloud Service. These connectors can be used as part of the automated extended response.

Vouchers & Dumps are Available | WhatsApp +201224560923

DO NOT REPRINT
© FORTINET
Brave-dumps.com



To integrate FortiEDR with your FortiGate installation, start by configuring FortiGate. In the left-hand menu, click to expand **Policy & Objects**, then select **Addresses**. Create a new address group. FortiEDR will populate this group with malicious IP addresses involved in security events. Next, click **IPv4 Policy** in the left-hand menu under **Policy & Objects**. Create a new policy to deny traffic to any addresses in the address group you just created.

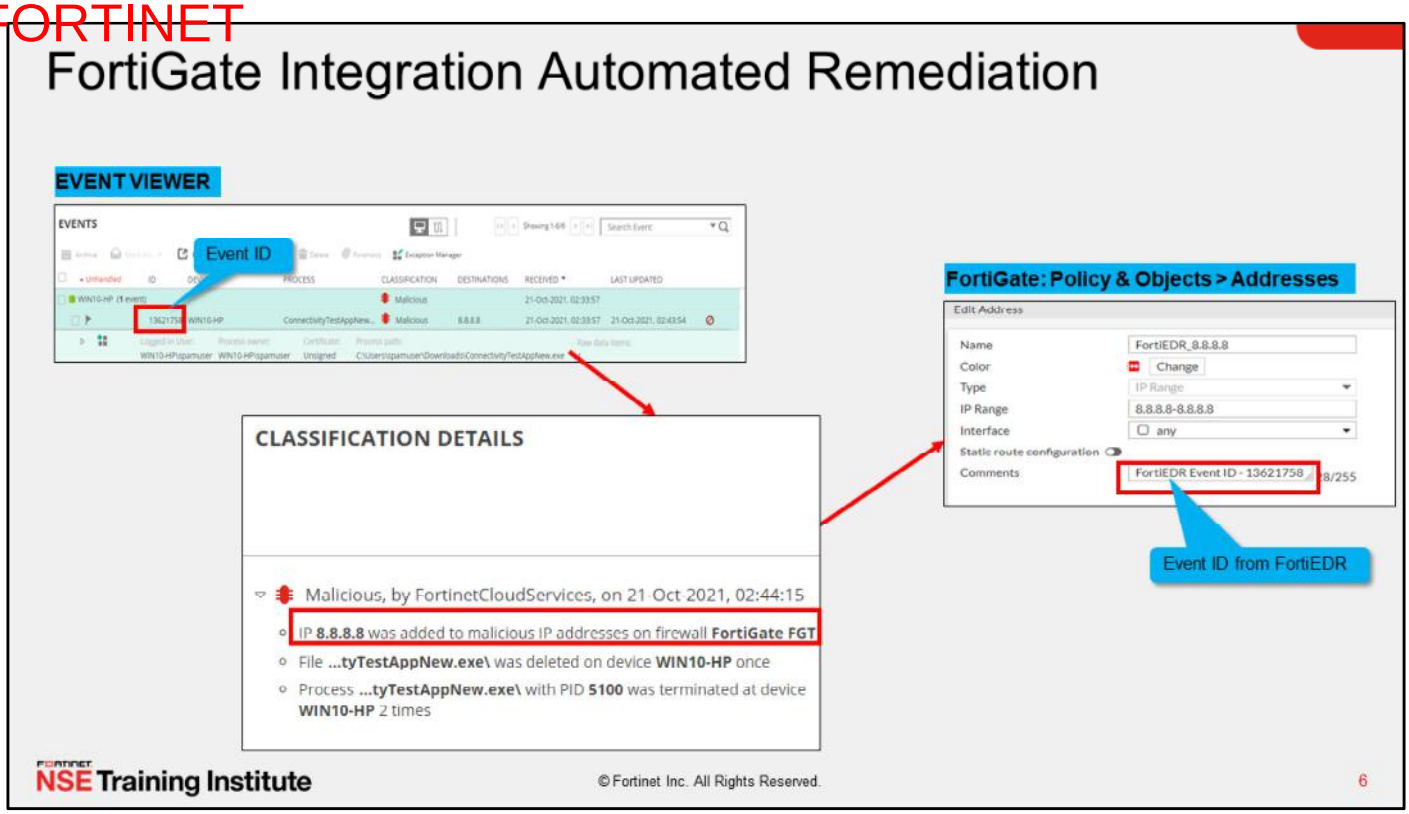
Next, you'll need to configure the connector in the FortiEDR management console. On the **ADMINISTRATION** tab, click **INTEGRATIONS**. Click **Add Connector** and choose **Firewall** in the drop-down list. Choose a core to communicate with FortiGate. Add a name to identify the firewall and in type dropdown select **FortiGate** or **FortiManager**, only if it is a managed FortiGate. Then enter the firewall IP or DNS address, port, API key or credentials, and the address group you created in FortiGate. You can either use the default **Block address on Firewall** action or create a custom action.

After your connector is configured, the last step is configuring your playbooks to automatically send malicious IP addresses to FortiGate. Under **SECURITY SETTINGS**, choose **Playbooks**, for each playbook you want to configure, find the **Block address on Firewall** rule in the **REMIDIATION** section or **CUSTOM** section if custom action is configured. Select your configured firewall—the name here is the name you entered when configuring the connector earlier. Lastly, choose which event classifications will trigger this action.

If you prefer to use the API, you can find detailed instructions in the *FortiEDR Fabric Integration Guide.*

Vouchers & Dumps are Available | WhatsApp +201224560923

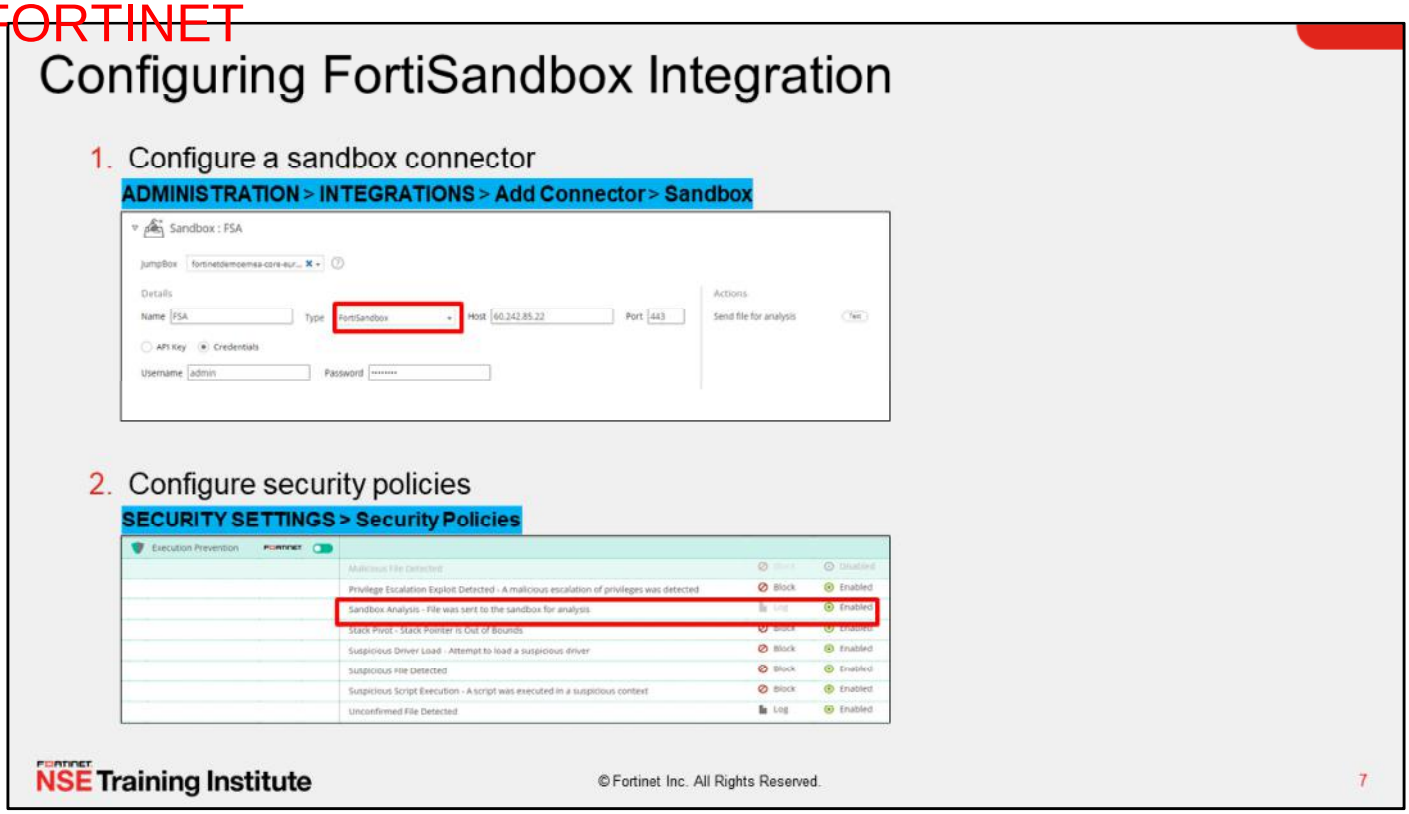
DO NOT REPRINT Brave-dumps.com
© FORTINET



When a security event is triggered for malicious activity towards an IP address, FortiEDR sends that IP information to the Fortigate and an address object is automatically created with an event ID. That address object is added to the address group that was configured initially on the Fortigate. Any traffic towards that IP address will be blocked by the Fortigate deny policy, which was configured previously as well. In the example shown, FortiEDR has detected malicious activity towards IP address `8.8.8.8`. As part of the playbook configuration, an automated incident response is triggered to add `8.8.8.8` to the FortiGate connector and block further activities towards this IP on the FortiGate.

Vouchers & Dumps are Available | WhatsApp +201224560923

DO NOT REPRINT Brave-dumps.com
© FORTINET



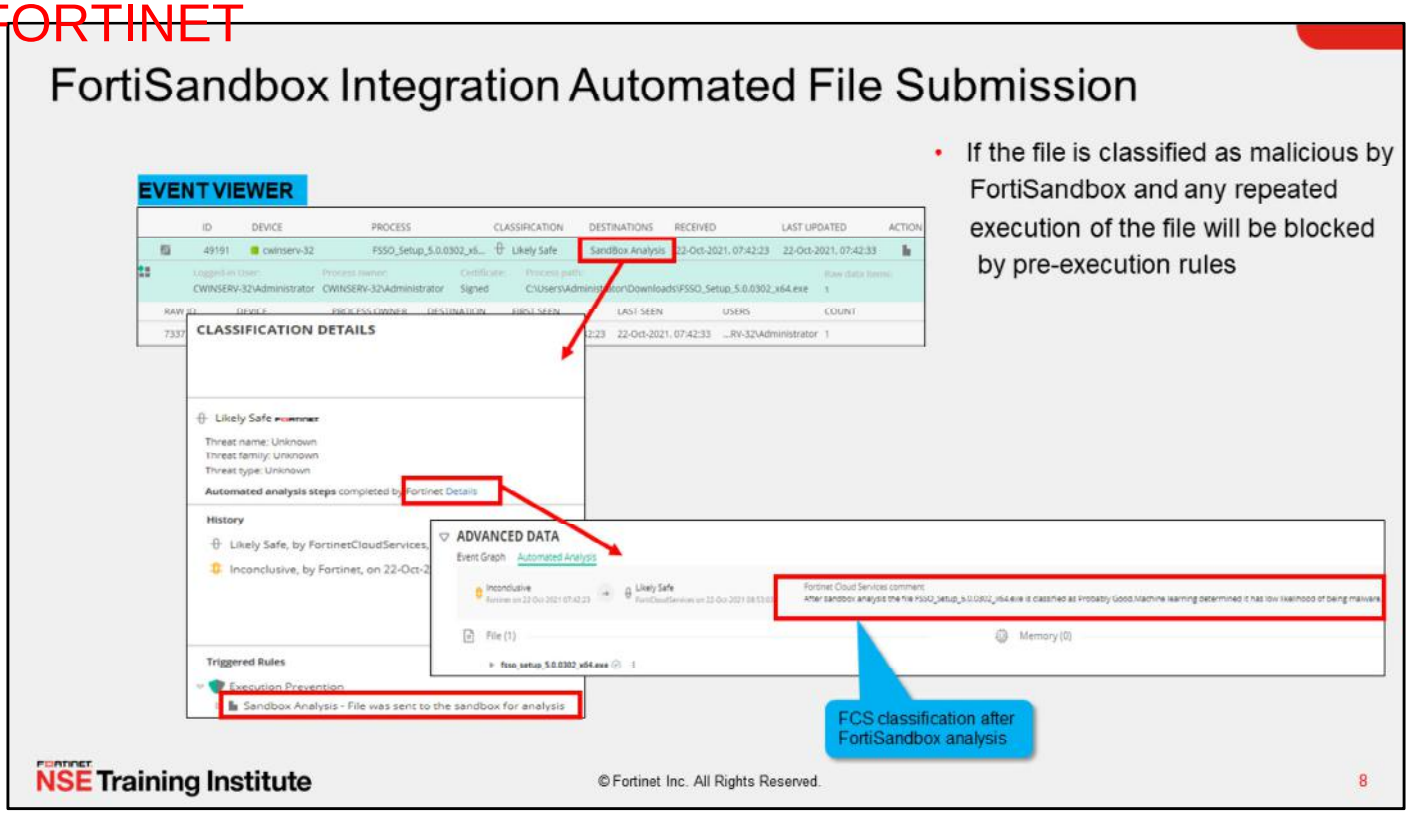
You can configure a connector with your FortiSandbox installation.

First, set up the connector in the FortiEDR management console. On the **ADMINISTRATION** tab, select **INTEGRATIONS**. Click **Add Connector** and choose **Sandbox** in the drop-down list. Select the on-premises core you want to communicate with FortiSandbox. Enter a name for the sandbox, then enter its IP or DNS address, the port, and the API key or credentials to access it.

Next, you'll need to configure your security policies to enforce the sandbox analysis rule. This is one of the few rules that are set to **Disabled** by default. Under **SECURITY SETTINGS**, choose **Security Policies**, and locate the execution prevention policy and click to view its rules. You should see the sandbox analysis rule. It should be grayed out, and the icon in the state column should say **Disabled**. Click the **Disabled** icon to toggle the state to **Enabled**. If you have clones of the execution prevention policy, repeat these steps for them. Now if an event violates the sandbox analysis rule, the file will automatically be sent to FortiSandbox for analysis.

Vouchers & Dumps are Available | WhatsApp +201224560923

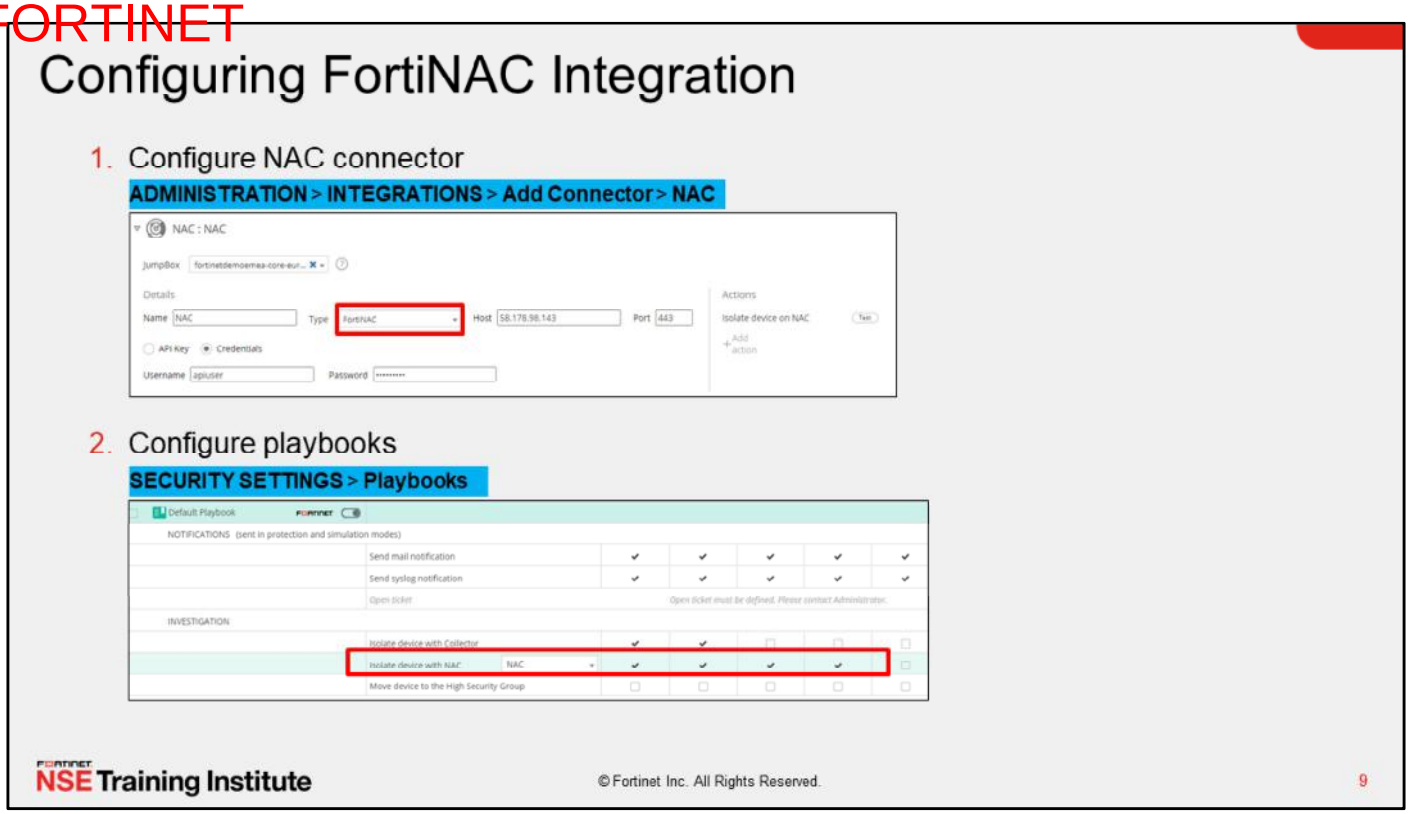
DO NOT REPRINT Brave-dumps.com
© FORTINET



A file that has not been previously analyzed or met a combination of conditions, like downloaded from the internet and not signed by a known vendor will trigger a sandbox event. Then the file will be sent to FortiSandbox for further analysis. If the file is safe, it will be classified as safe and is archived. If FortiSandbox determines the file is malicious, it will classify as non-safe and any repeated execution of the same file will be blocked by one of the pre-execution rules. In this example, the executable was classified as **Inconclusive** by FortiEDR and then sent to FortiSandbox for further analysis. After the sandbox analysis, FCS reclassified the event as **Likely Safe**.

Vouchers & Dumps are Available | WhatsApp +201224560923

DO NOT REPRINT Brave-dumps.com
© FORTINET



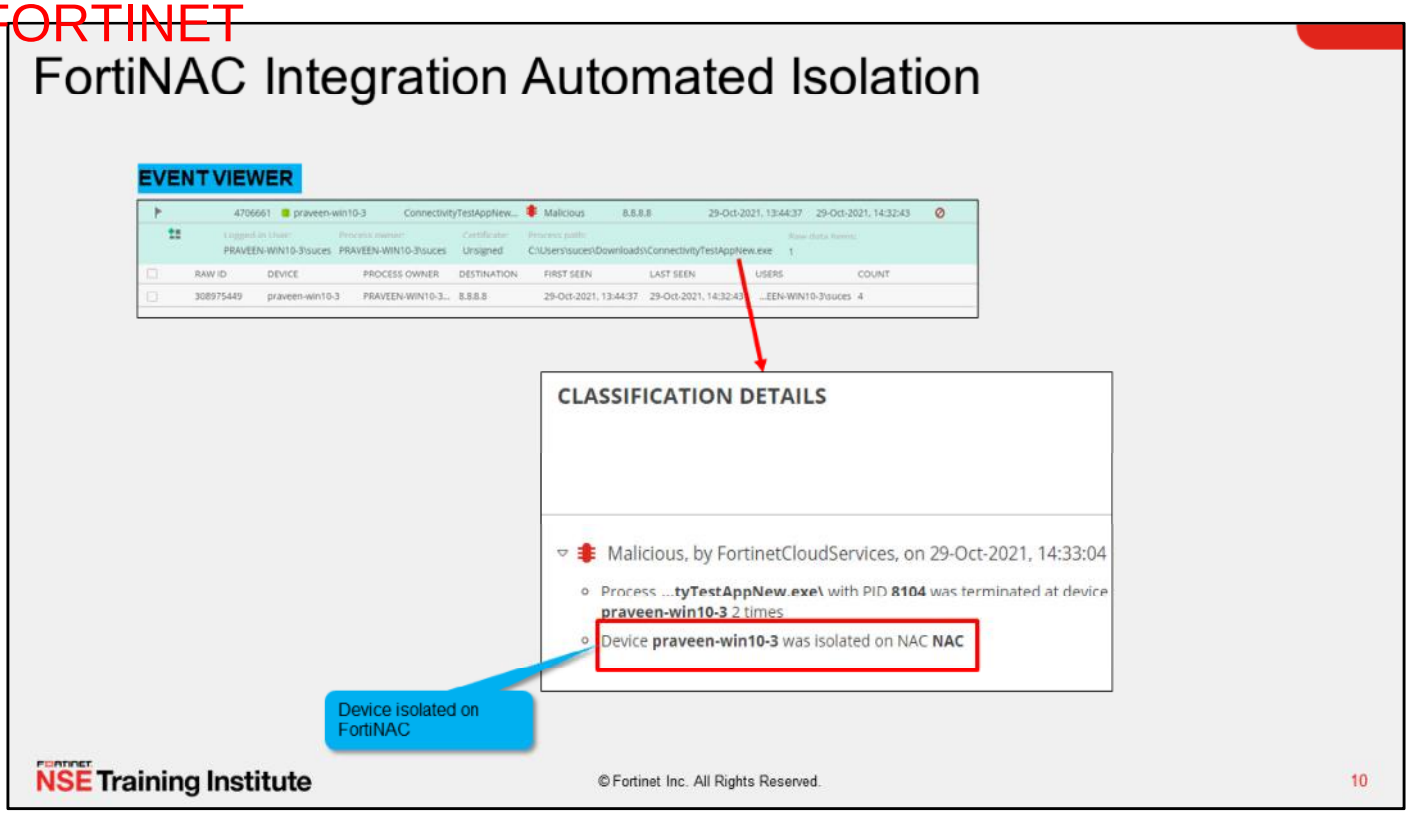
You can also configure a connector with your FortiNAC installation.

First, set up the connector in the FortiEDR management console. On the **ADMINISTRATIONS** tab, select **INTEGRATIONS**. Click **Add Connector** and choose **NAC** in the drop-down list. Select the on-premises core you want to communicate with FortiNAC. Enter a name for the FortiNAC, then enter its IP or DNS address, the port, and the API key or credentials to access it. You can either use the default **Isolate device on NAC** action or create a custom action.

Once your connector is configured, the last step is configuring your playbooks to automatically isolate the device using FortiNAC. Under **SECURITY SETTINGS**, choose **Playbooks**, for each playbook you want to configure, find the **Isolate device with NAC** rule in the **INVESTIGATION** section or **CUSTOM** section if custom action is configured. Select your configured NAC name here is the name you entered when configuring the connector earlier. Lastly, choose which event classifications will trigger this action.

Vouchers & Dumps are Available | WhatsApp +201224560923

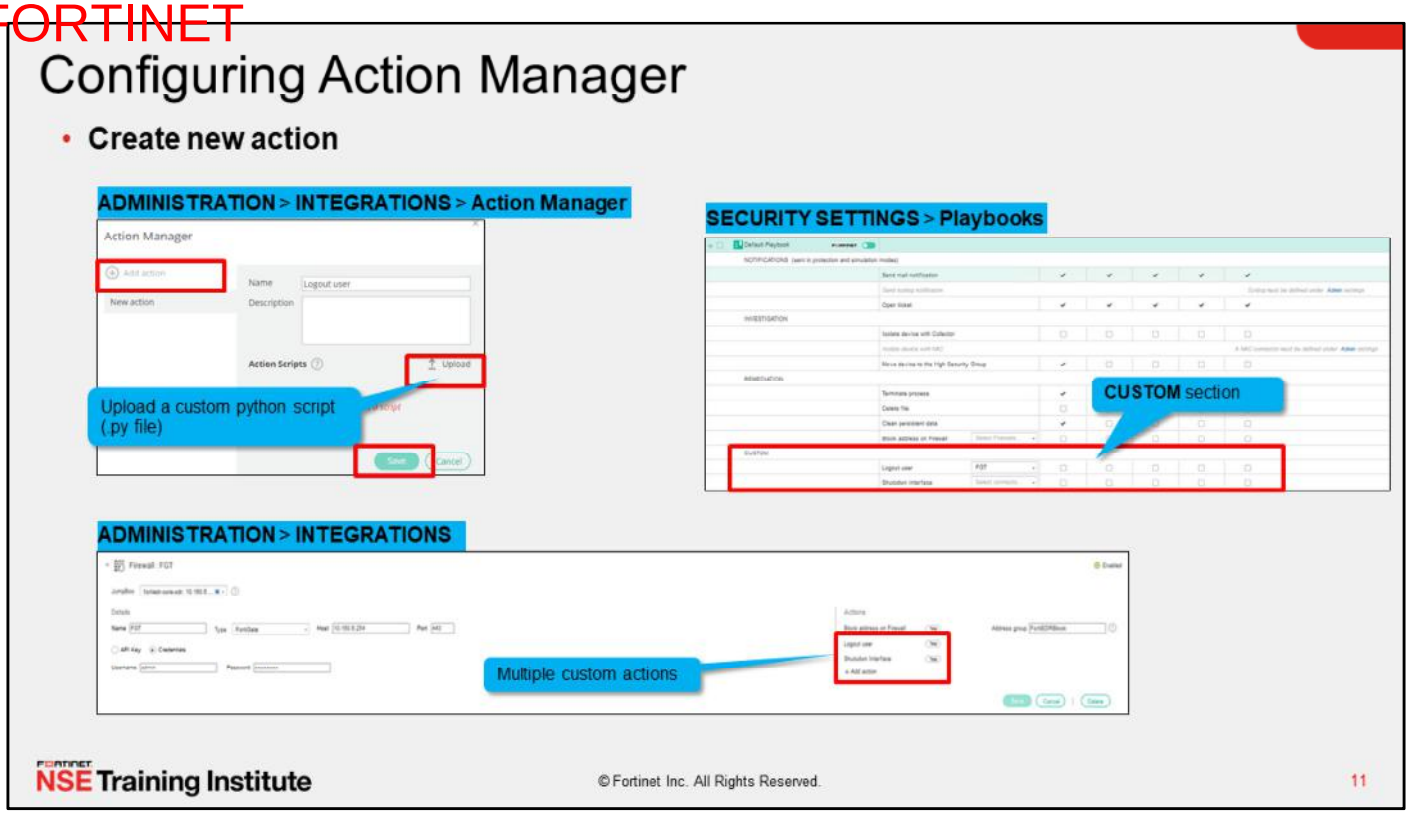
DO NOT REPRINT Brave-dumps.com
© FORTINET



In the example shown on this slide, there was a malicious event detected on the endpoint and per the playbook configuration, the endpoint was isolated on FortiNAC as part of the automated incident response.

Vouchers & Dumps are Available | WhatsApp +201224560923

DO NOT REPRINT Brave-dumps.com
© FORTINET



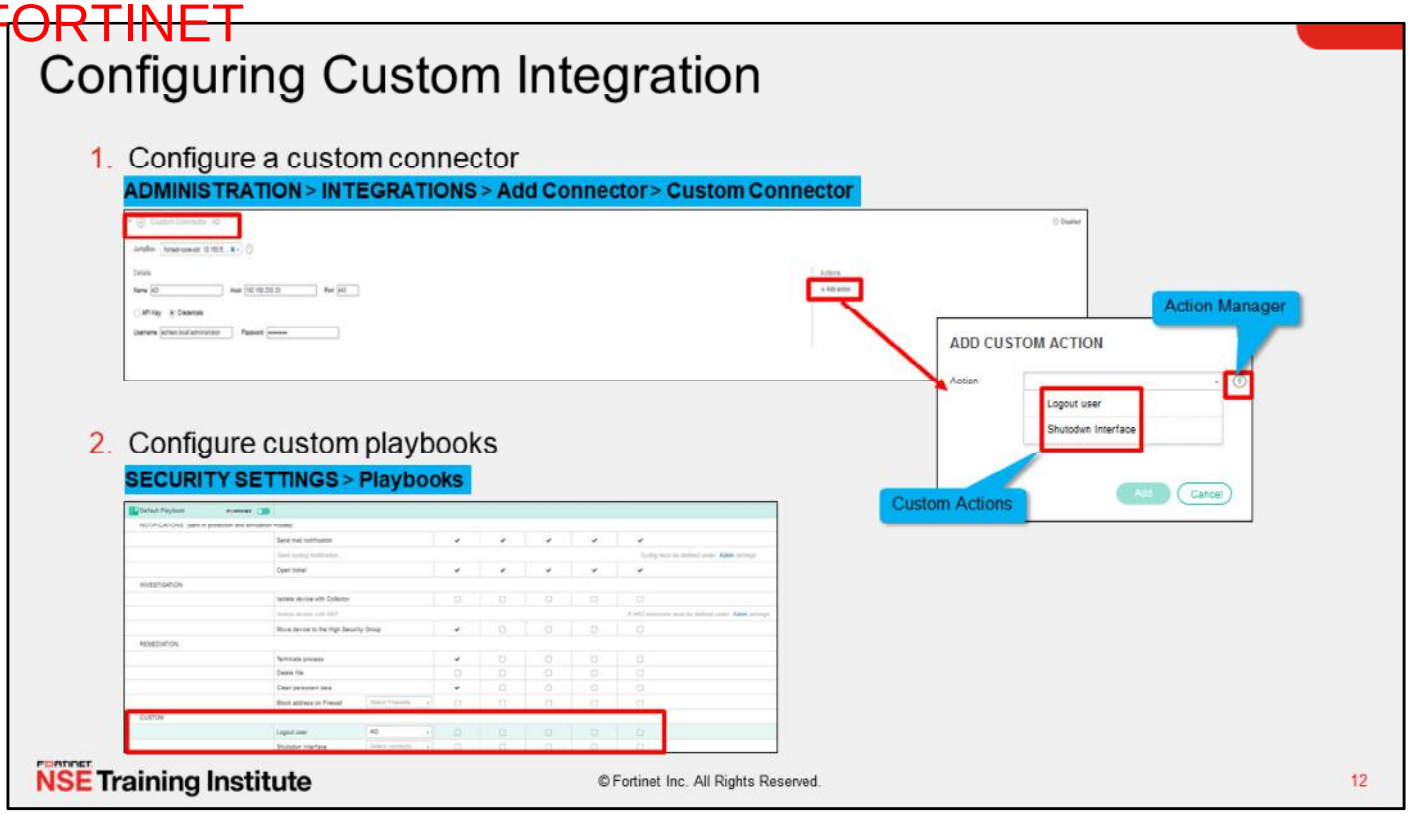
You can configure custom action using the action manager, which can be used with Firewall, NAC, and Custom connectors.

On the **ADMINISTRATION** tab, select **INTEGRATIONS**. Click **Add Action Manager** and click **Add action.** Then enter a name for the action, and upload a python script, which will do an API call to perform the relevant action. Finally, click **Save** to save the action. You can add multiple actions to the same connector configuration.

Once your connector is configured with a custom action, the last step is configuring your playbooks to automatically to execute this action. Under **SECURITY SETTINGS**, choose **Playbooks**, for each playbook you want to configure, find the action name in the **CUSTOM** section. Select the configured connector name earlier, and then choose which event classifications will trigger this action.

Vouchers & Dumps are Available | WhatsApp +201224560923

DO NOT REPRINT Brave-dumps.com
© FORTINET



Custom connectors can also be integrated with FortiEDR.

On the **ADMINISTRATION** tab, select **INTEGRATIONS**. Click **Add Connector** and choose **Custom Connector** in the drop-down list. Select the on-premises core you want to communicate with the custom connector. Enter a name for the custom connector, then enter its IP or DNS address, the port, and the API key or credentials to access it. You can use custom actions by clicking **Add action** and selecting an action from the **Action** drop-down, for already configured custom actions or click the plus icon to open the **Action Manager**.

Once your connector is configured, the last step is configuring your playbooks to automatically execute a custom defined action for your connector. Under **SECURITY SETTINGS**, choose **Playbooks**, for each playbook you want to configure, find the action name in the **CUSTOM** section. Select your configured FortiGate, FortiNAC and/or custom connector. Lastly, choose which event classifications will trigger this action.

Vouchers & Dumps are Available | WhatsApp +201224560923

DO NOT REPRINT
© FORTINET
Brave-dumps.com

Knowledge Check

1. Which security settings feature does FortiEDR use to send files to FortiSandbox for analysis?
   A. Playbooks
   ✓ B. Security Policies

2. Custom actions can be configured for which connectors?
   A. FortiSandbox
   ✓ B. FortiNAC

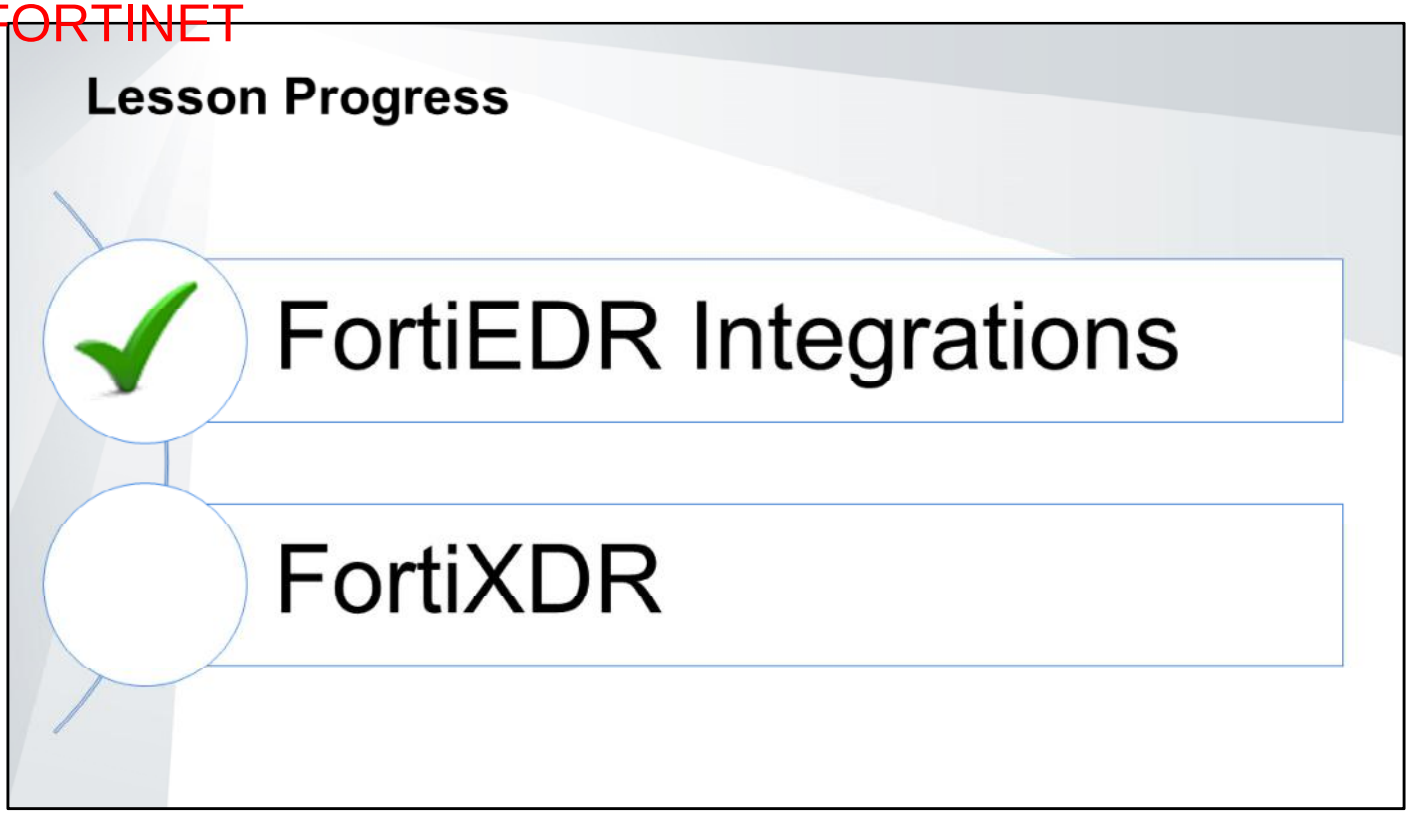
NSE Training Institute

© Fortinet Inc. All Rights Reserved.

13

Vouchers & Dumps are Available | WhatsApp +201224560923

DO NOT REPRINT
© FORTINET
Brave-dumps.com

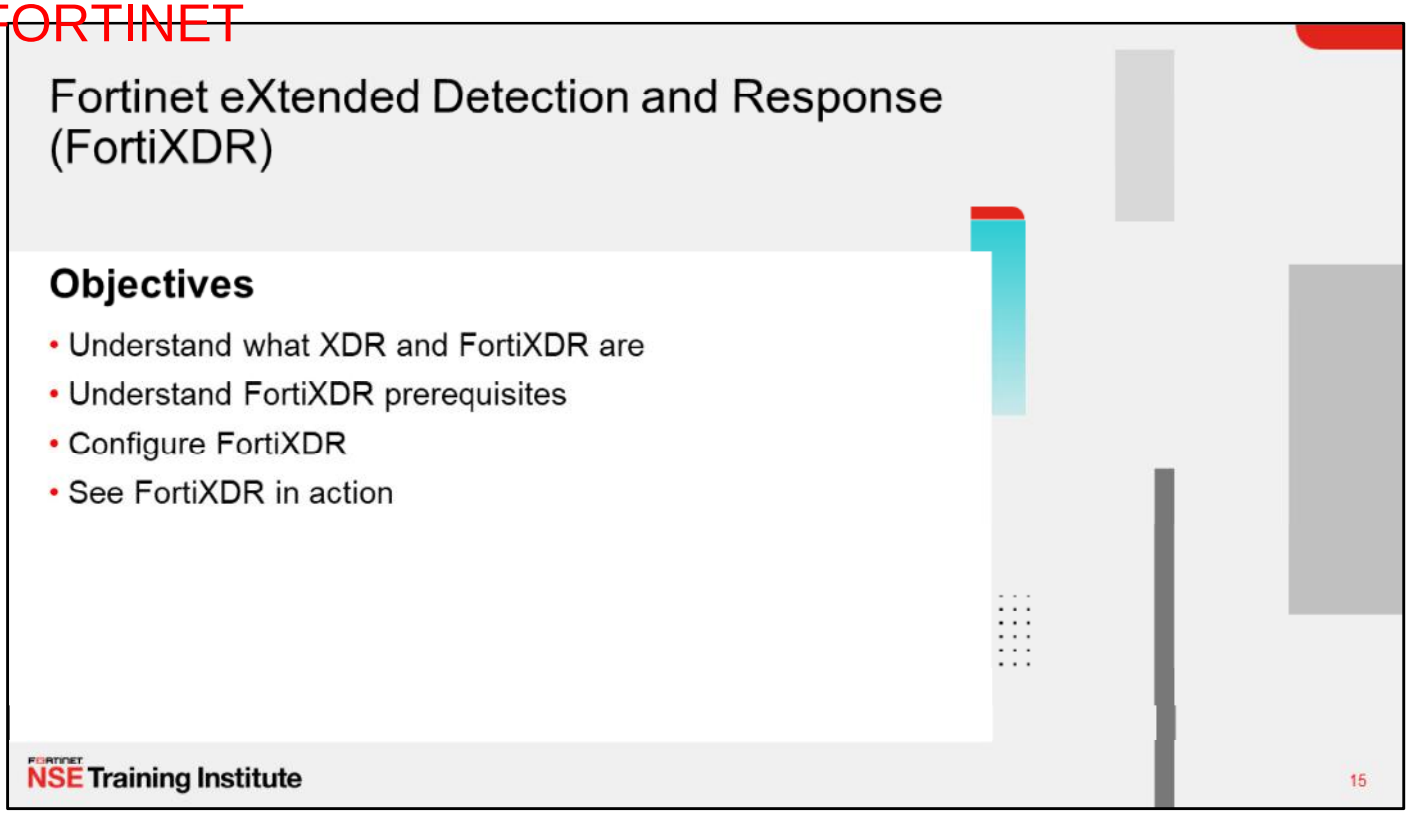


Good job! You now understand the Fortinet Security Fabric and third-party integrations, and their automated incident response.

Now, you will learn about FortiXDR.

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 FortiXDR, you will be able to understand the FortiXDR flow and configure extended detection on the FortiEDR console.

Vouchers & Dumps are Available | WhatsApp +201224560923

DO NOT REPRINT
© FORTINET
Brave-dumps.com

What is XDR and FortiXDR?

- XDR is defined by Gartner as a unified security incident detection and response platform that automatically collects and correlates data from multiple proprietary security components
- FortiXDR can be integrated with the Fortinet Security Fabric to analyze and correlate data across the entire attack surface
- FortiXDR uses a three-step approach to find and prevent cyberattacks:
  1. Extended detection
  2. Extended investigation
  3. Extended response

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

Gartner defines eXtended detection and response (XDR) as a unified security incident detection and response platform that automatically collects and correlates data from multiple proprietary security components. An XDR solution analyzes data from different security devices to detect and respond to threats from the entire attack surface.

Fortinet eXtended detection and response (FortiXDR) can be integrated with the Fortinet Security Fabric. Using its broad coverage of attack surface, it can provide the perfect XDR solution. FortiXDR uses a three-step approach to find and prevent a cyberattack:

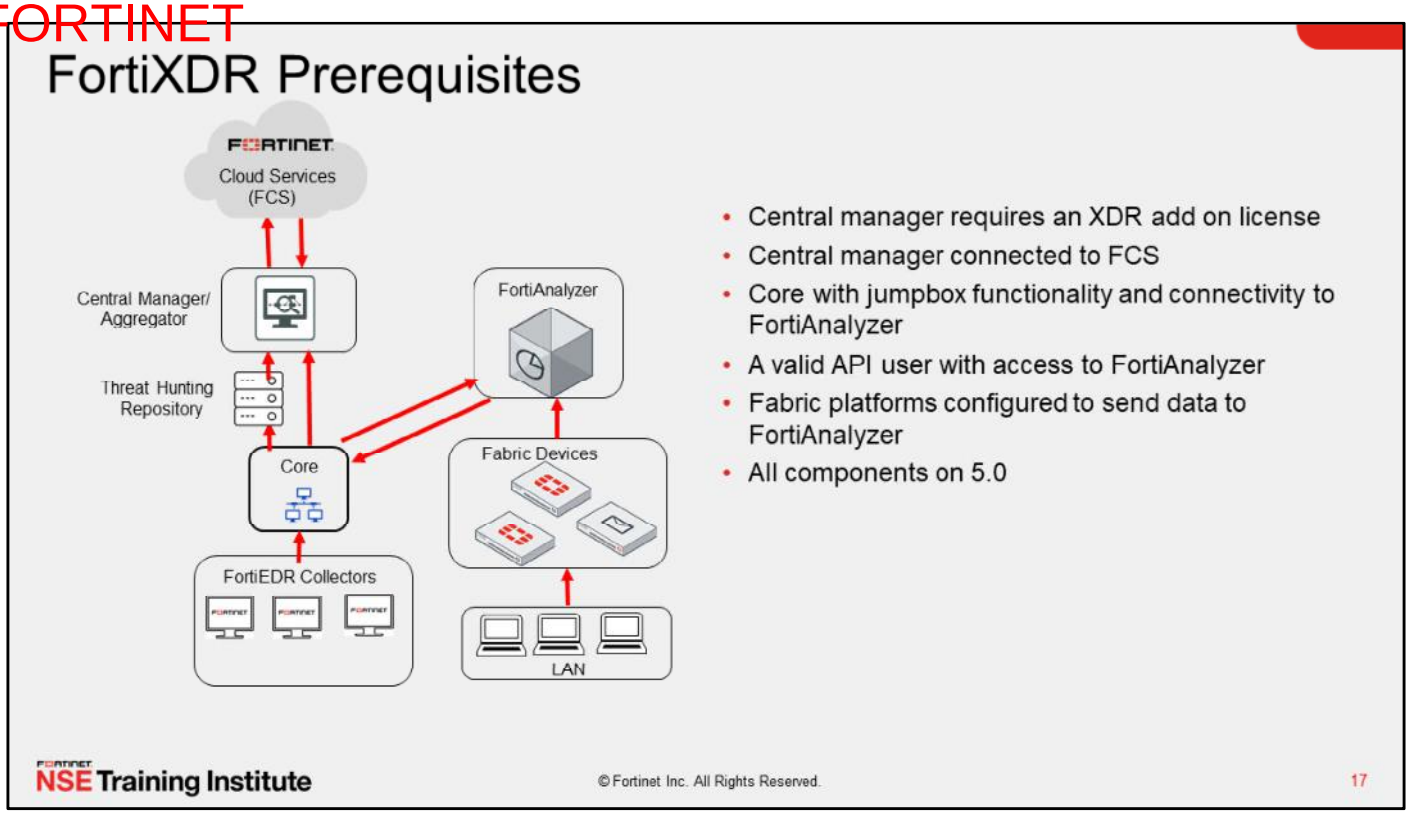
1. Extended detection: FortiXDR analyzes and correlates data that is shared across the Fortinet Security Fabric.

2. Extended investigation: FortiXDR uses artificial intelligence (AI) to detect threats and automates the full investigation, rather than relying on human resources. It uses a dynamic control flow engine, which is continuously trained using the threat data and research data provided by Fortiguard labs.

3. Extended response: FortiXDR relies on playbooks for it's automated incident response. FortiXDR can leverage the connectors and third party components configured on FortiEDR as part of its response.

Vouchers & Dumps are Available | WhatsApp +201224560923

DO NOT REPRINT Brave-dumps.com
© FORTINET

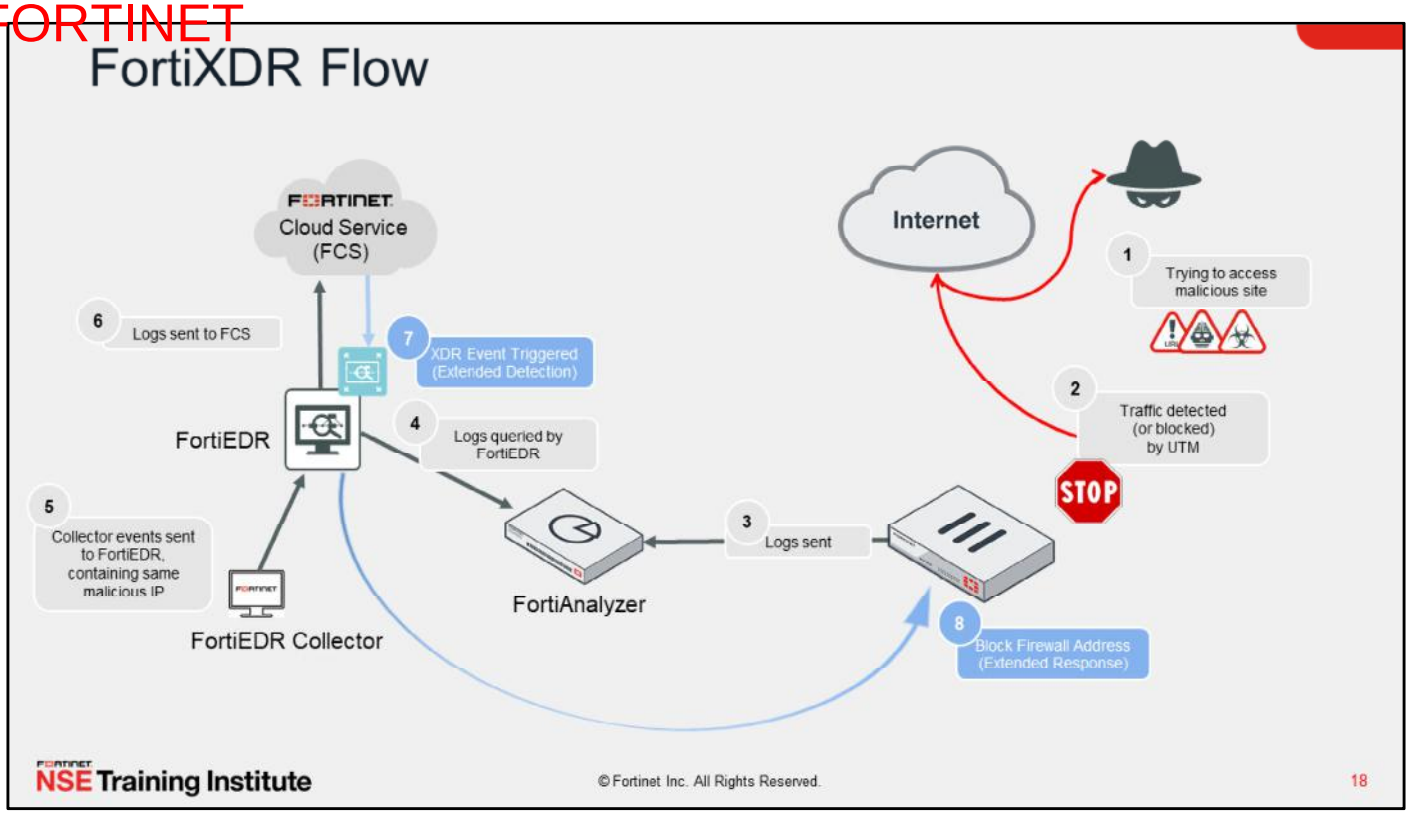


To extend threat detection, FortiEDR central manager can be integrated with FortiAnalyzer through the core to pull data from one or more fabric platforms. These aggregated data, along with the data from collectors are sent to FCS, where it is correlated and analysed to detect any malicious activity across the entire surface attack. If any malicious activity is found a security event is generated and playbooks can be used for automated extended response.

The central manager requires an XDR add on top of the Protect and Respond or Discover, Protect and Respond license, for the FortiXDR functionality to work. The central manager is required to have access to FCS as well. The core needs to be configured with a jumpbox functionality and needs to be able to connect to FortiAnalyzer, with a valid API user. Fabric devices such as FortiGate, FortiMail needs to be configured to send logs to FortiAnalyzer, in order for the central manager to query data. All FortiEDR components must be on 5.0 or higher firmware.

Vouchers & Dumps are Available | WhatsApp +201224560923

DO NOT REPRINT
© FORTINET
Brave-dumps.com

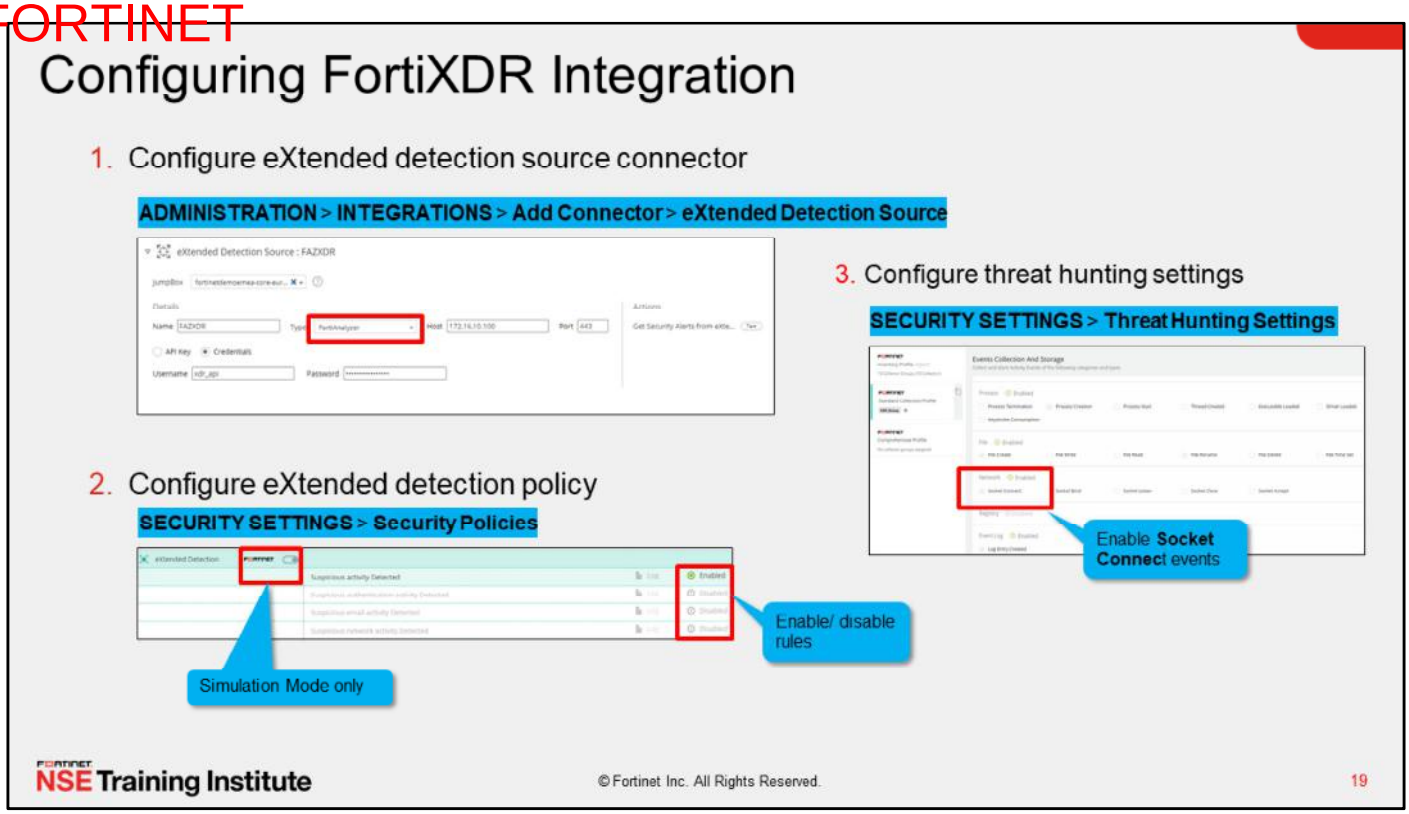


This slide shows the flow of events to trigger an XDR event by FCS, and its automated incident response.

1. A station attempts to access content that is considered a security risk, such as a malicious website.
2. FortiGate blocks access to the site, based on the firewall policy defined with a web filter profile.
3. FortiGate sends a log record to FortiAnalyzer regarding the violation committed.
4. FortiEDR Central Manager queries FortiAnalyzer for these logs at regular intervals through the API.
5. FortiEDR collector sends OS metadata to FortiEDR Central Manager via the core.
6. All these logs are sent to FCS, where they are correlated and analyzed.
7. FCS determines a malicious event has occurred, and sends back an XDR event to the FortiEDR central manager, as part of its extended detection.
8. As part of its automated incident response configuration, FortiEDR will notify FortiGate to block the malicious IP address.

Vouchers & Dumps are Available | WhatsApp +201224560923

DO NOT REPRINT Brave-dumps.com
© FORTINET



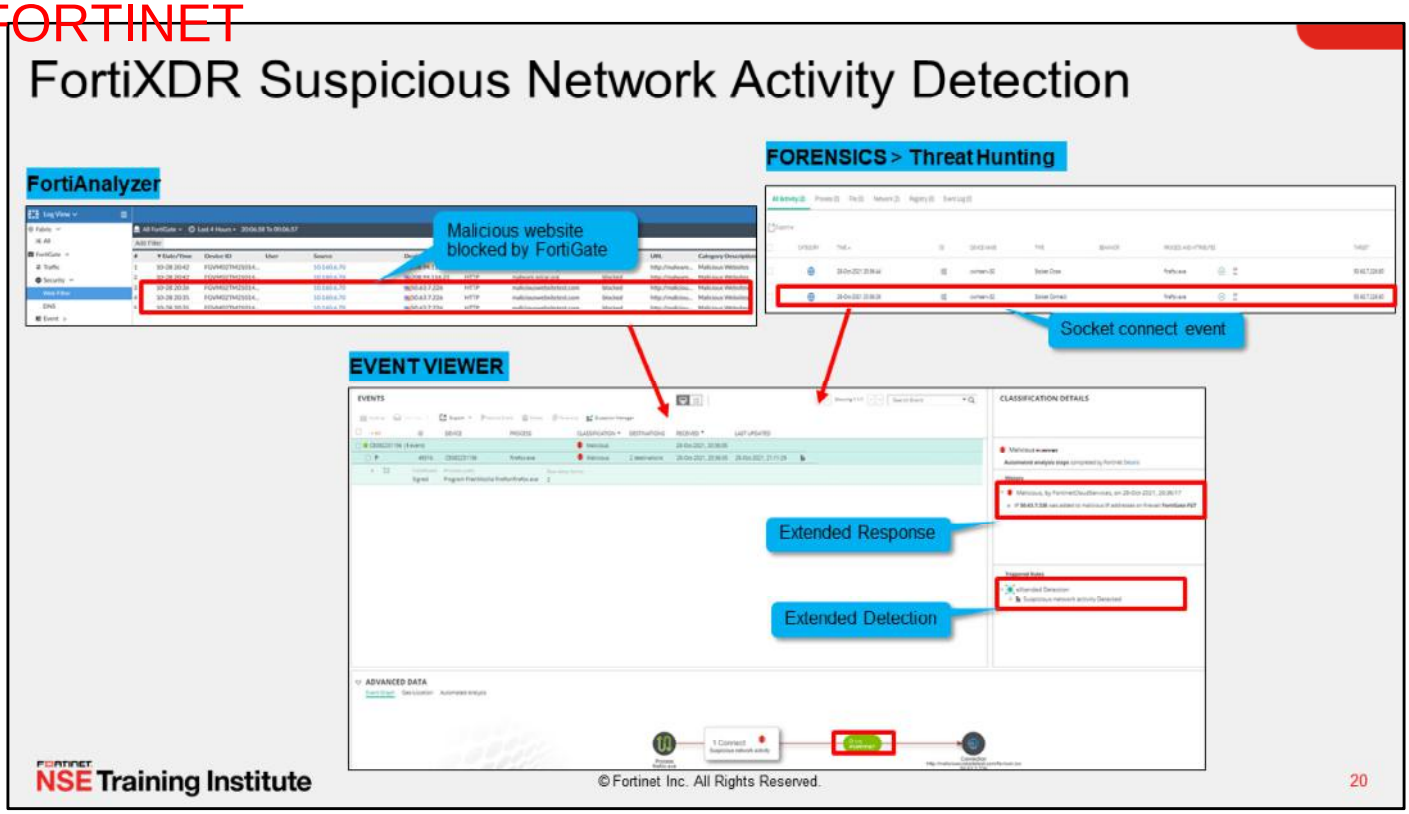
To integrate FortiXDR, you need to first setup the connector in the FortiEDR management console. On the **ADMINISTRATION** tab, select **INTEGRATIONS**. Click **Add Connector** and choose **eXtended Detection source** in the drop-down list. Select the on-premises core you want to communicate with FortiAnalyzer. Enter a name for the FortiAnalyzer, then enter its IP or DNS address, the port, and the API key or credentials to access it.

Next, you'll need to configure your security policies to enforce the extended detection. Under **SECURITY SETTINGS**, choose **Security Policies**, locate the **eXtended Detection** policy, and click to view its rules. You should four different rules for different suspicious activities. The policy should be grayed out, and the icon in the state column should say **Disabled**. Click the **Enabled** or **Disabled** icon to toggle the state to **Enabled**. If you have clones of the eXtended detection policy, repeat these steps for them. This policy operates only in simulation mode and does not block any events. This policy provides visibility into data across multiple security systems to identify malicious activity by applying analytics and correlating data from various systems.

The last step is configuring your threat hunting settings to enable a correlation of activity seen on Fortinet Fabric components with the activity seen by FortiEDR. Under **SECURITY SETTINGS**, choose **Threat Hunting Settings**, and add your collector group to the built in **Standard Collection Profile** or **Comprehensive Profile**. You can also clone one of these policies and at least enable **Socket Connect** events under the **Network** category for extended detection to work.

Vouchers & Dumps are Available | WhatsApp +201224560923

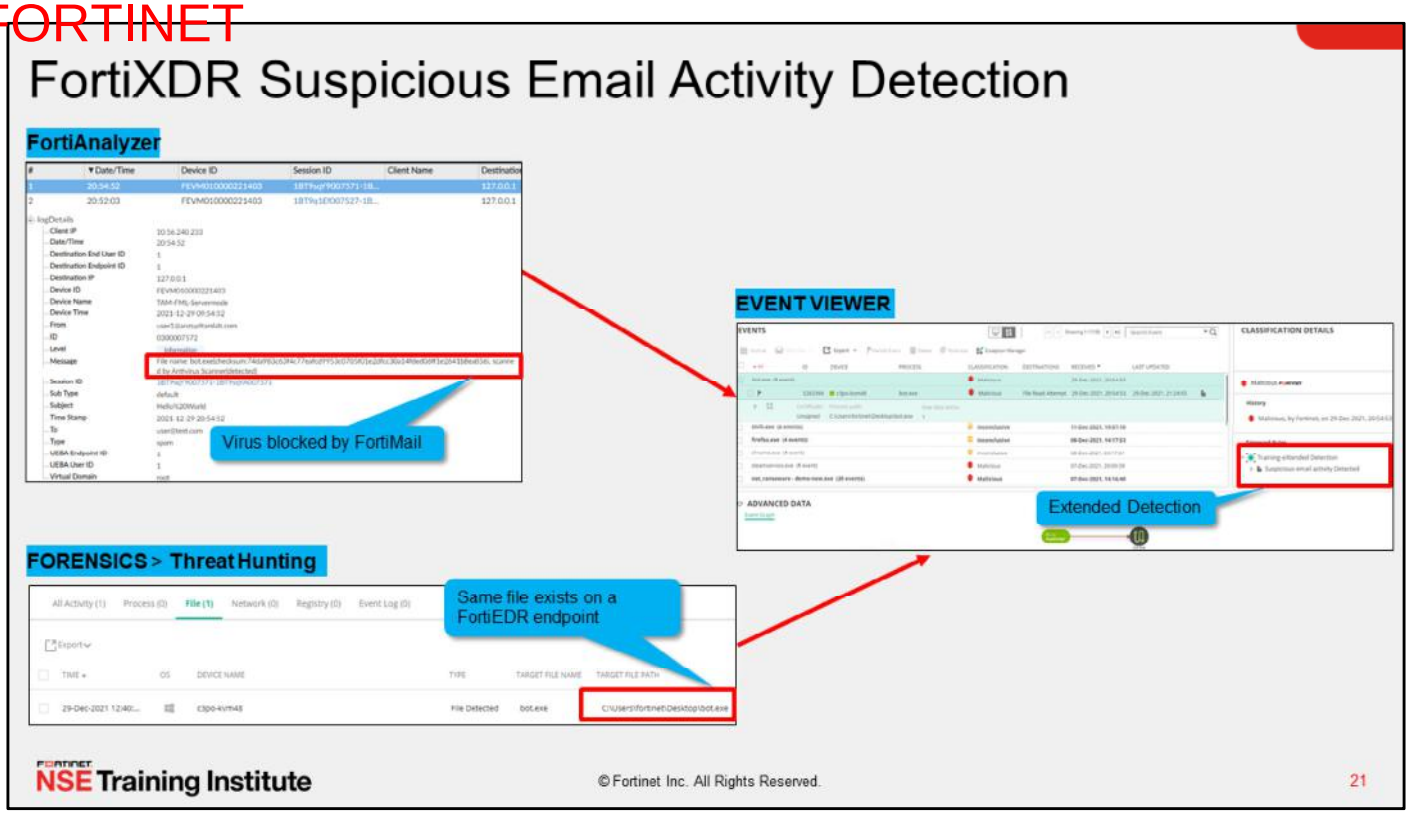
DO NOT REPRINT Brave-dumps.com
© FORTINET



In this example, the FortiGate is configured to block malicious websites and send logs to the FortiAnalyzer. When an endpoint behind the FortiGate, accesses a malicious website, a log entry is created on the FortiAnalyzer. FortiXDR service on FCS analyses these logs and inspects threat hunting data for the same destinations on FortiEDR endpoints. After the full analysis is done, FortiXDR triggers an XDR **Suspicious network activity** event in the **EVENT VIEWER** on central manager console. In this scenario, there is a playbook configured to add the malicious IP to the FortiGate block list as part of it extended response.

Vouchers & Dumps are Available | WhatsApp +201224560923

DO NOT REPRINT Brave-dumps.com
© FORTINET



In this example, FortiMail is configured to block virus attachments and also send logs to the FortiAnalyzer. In this example, an email client behind the FortiMail is sending a virus attachment: **bot.exe**. FortiMail blocks this email, and a log entry is created on FortiAnalyzer. FortiXDR service on FCS analyses these logs and inspects threat hunting data for the same file and hash on FortiEDR endpoints. After the full analysis is done, FortiXDR triggers an XDR **Suspicious email activity** event in the **EVENT VIEWER** on central manager console. Since there is no automatic response configured in this example, manual mitigation steps are required to investigate this event.

Vouchers & Dumps are Available | WhatsApp +201224560923

DO NOT REPRINT
© FORTINET
Brave-dumps.com

Knowledge Check

1. Which policy mode is used by eXtended detection policy?
   A. Protection
   ✓ B. Simulation

2. Which device can be configured as an eXtended detection source?
   ✓ A. FortiAnalyzer
   B. FortiSIEM

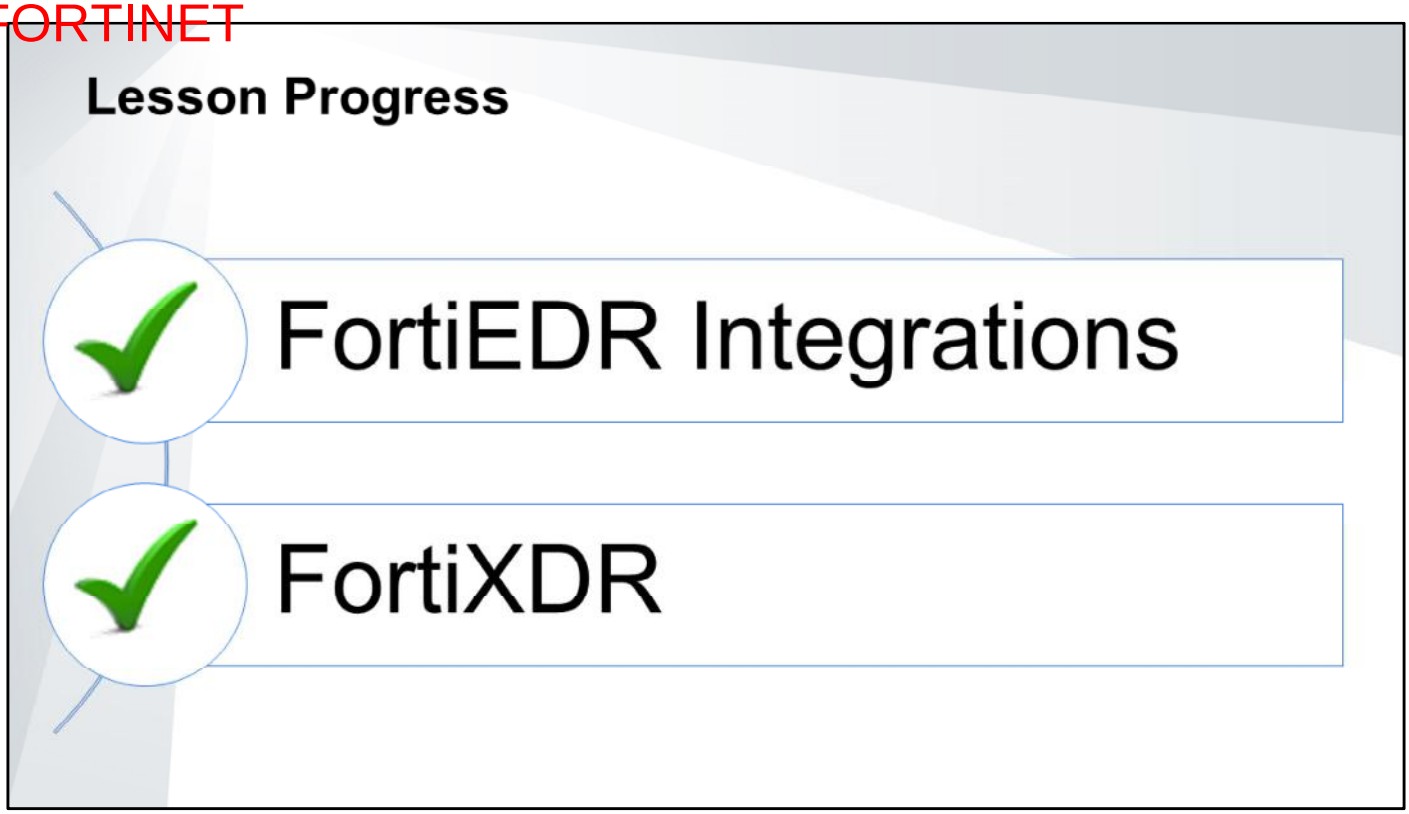
NSE Training Institute

© Fortinet Inc. All Rights Reserved.

22

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

Review

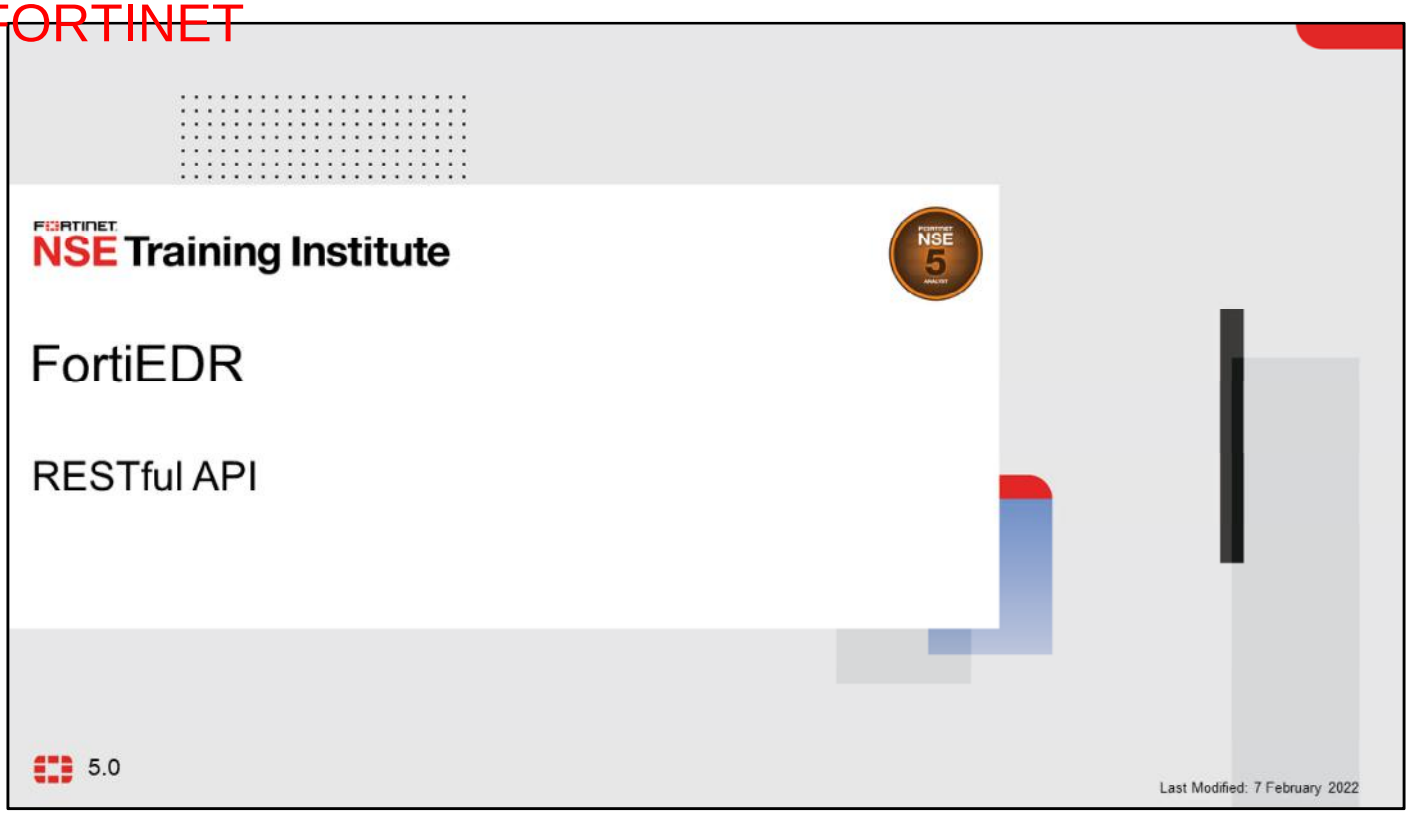
- ✓Understand FortiEDR Security Fabric and third-party integration requirements
- ✓Understand FortiEDR integration with Fortinet Security Fabric
- ✓Configure action manager
- ✓Configure custom integration
- ✓Understand what XDR and FortiXDR are
- ✓Understand FortiXDR prerequisites
- ✓Configure FortiXDR
- ✓See FortiXDR in action

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

By mastering the objectives covered in this lesson, you learned how to integrate Fortinet Security Fabric devices and FortiXDR with FortiEDR .

Vouchers & Dumps are Available | WhatsApp +201224560923

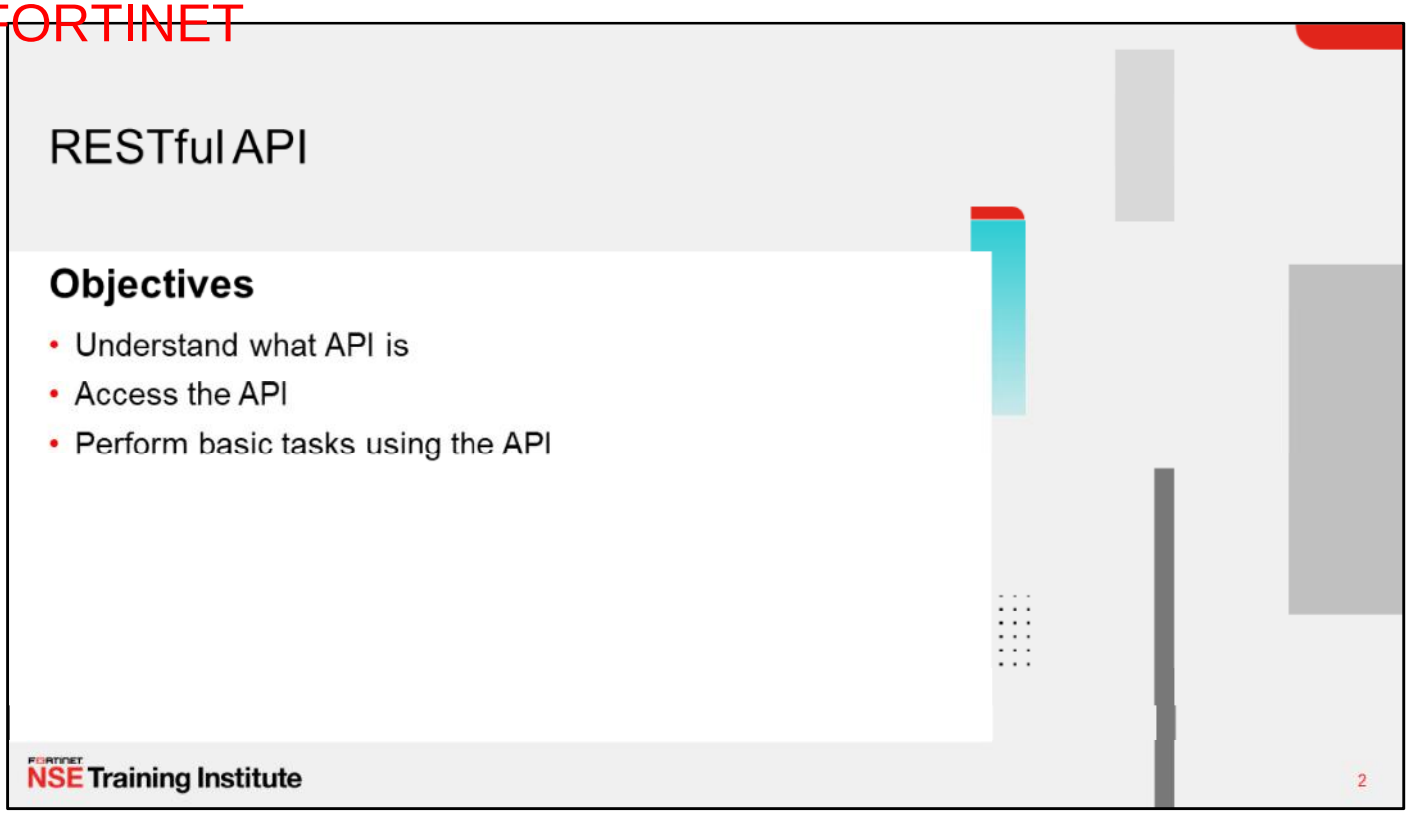
DO NOT REPRINT
© FORTINET
Brave-dumps.com



In this lesson, you will learn how to use RESTful API with FortiEDR.

Vouchers & Dumps are Available | WhatsApp +201224560923

DO NOT REPRINT Brave-dumps.com
© FORTINET



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

By demonstrating competence in RESTful API, you will be able to use RESTful API to interact with the FortiEDR management console.

Vouchers & Dumps are Available | WhatsApp +201224560923

DO NOT REPRINT
© FORTINET
Brave-dumps.com

What is API?

- The API allows you to easily integrate FortiEDR functionality into your organization's existing software
- The FortiEDR central manager supports a REST HTTP-based API for accessing:
  - Security data
  - Communication control data
  - Device and software configuration and operations
- The API duplicates the functionality of the management console user interface
  - Manage device and software configuration
  - Analyze events
  - Remediate devices

NSE Training Institute

© Fortinet Inc. All Rights Reserved.

3

What is the API? You can easily integrate FortiEDR's functionality into your organization's existing software. The FortiEDR central manager supports REST HTTP-based API for accessing security and communication control data, as well as device and software configuration and operations. Essentially, it's a way of programmatically duplicating the functionality of the management console. You can manage device and software configuration, analyze events, and remediate devices, all without having to use the management console.

Vouchers & Dumps are Available | WhatsApp +201224560923

DO NOT REPRINT Brave-dumps.com
© FORTINET

How Does RESTful API Work?

- Features:
  - REST based over HTTP
  - SSL encryption
  - JSON format
  - Token and password-based authentication
    - **Hint**: For password authentication, be sure the user is assigned the **Admin** and **Rest API** roles
- Methods
  - GET to read
  - POST or PUT to update

NSE Training Institute

© Fortinet Inc. All Rights Reserved.

4

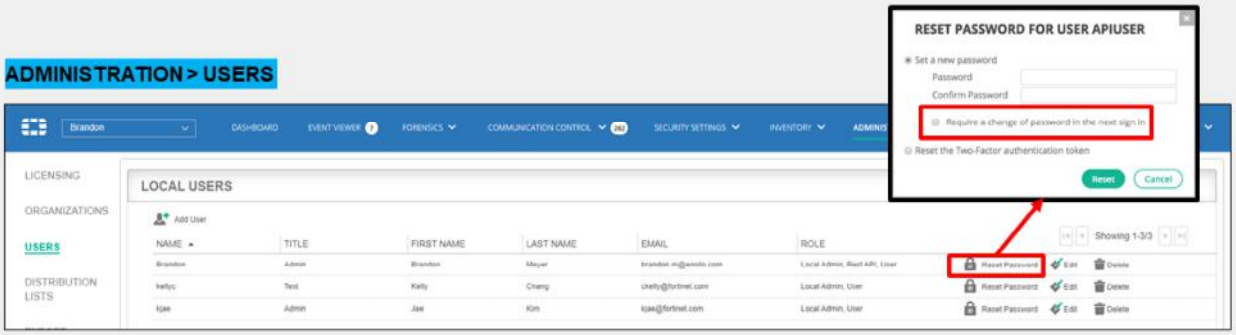
How does RESTful API work? It's REST-based over HTTP. It uses SSL encryption, and it passes back protocol information in JSON format. You can use either token-based or password-based authentication. To use password-based authentication, you need to make sure that the user is assigned the **Admin** and **Rest API** roles. You can do that in the **ADMINISTRATION** tab of the management console under **USERS**. The API uses a few different methods—GET to read data, POST or PUT to update. It also has DELETE and a few other commands. You will learn about methods in this lesson.

Vouchers & Dumps are Available | WhatsApp +201224560923

DO NOT REPRINT Brave-dumps.com
© FORTINET

API User Access

- When you create a new user in the management console, you must reset the password before the user can log in
  - In the **USERS** pane in the **ADMINISTRATION** tab, find the newly created user and click **Reset Password**
  - Clear the **Require a change of password in the next sign in** checkbox



NSE Training Institute

© Fortinet Inc. All Rights Reserved.

5

One of the most common issues reported is an *unauthorized* message when a new user tries to use the API for the first time. The reason for this is the password reset requirement. New users are forced to change their passwords the first time they log in to the management console. Since you can't reset your password with the API, you get an error message. The solution is pretty simple. To resolve this issue, in the management console, in the **ADMINISTRATION** tab, click **USERS**. Find the user in the list and click **Reset Password**. The **Reset Password** dialog opens. Clear the **Require a change of password at the next sign-in** checkbox, then enter the password and click **Reset**. The user should now be able to log in through the API. Alternatively, you can ask users to log in to the management console and reset their password before using API calls.

Vouchers & Dumps are Available | WhatsApp +201224560923

DO NOT REPRINT Brave-dumps.com
© FORTINET

Accessing the API

- Method 1: Curl

```
curl -k -H -i -u <username:password>
    https://<FortiEDRHOST>/management-
    rest/organizations/list-organizations
```

- Method 2: Postman application

```
GET
https://<FortiEDRHOST>/management-
    rest/organizations/list-organizations
```

```
curl.exe -k -H -i  -u apiuser:password https://10.160.6.100/management-rest/organizations/list-organizations
[ {
  "name" : "Fortinet Training",
  "organizationId" : 1,
  "workstationsAllocated" : 20,
  "serversAllocated" : 20,
  "iotAllocated" : 0,
  "workstationsInUse" : 0,
  "serversInUse" : 2,
  "iotInUse" : 0,
  "expirationDate" : "2022-02-02",
  "vulnerabilityAndIoT" : true,
  "forensicsAndEDR" : true,
  "verificationCode" : null,
  "isAdminAccount" : true
} ]
```

NSE Training Institute

© Fortinet Inc. All Rights Reserved.

6

There are a couple of ways to access the API. The first method is to use a CLI application, like Curl. This slide shows a typical Curl request. If you're using a self-signed certificate for your central manager, which is the default setting, use `-k` to bypass the certificate verification. Enter `-H` followed by the authorization type and credentials, then enter the URL parameters. The example command returns a list in JSON format containing organization name, allocated seats, seats in use, expiration date, and so on.

The second method is to use a GUI application like Postman or Insomania. You see the same request you just saw in Curl, but formatted for Postman. First, select the **GET** method, then enter the URL parameters: `https://<FortiEDRHOST>/management-rest/organizations/list-organizations`. In the image on the slide, you can see a command in the application itself. You can see **GET** at the top left, then the URL parameters—in this example, you're asking for a list of all the organizations in a multi-tenant environment. Below that, you can see the **Authorization** tab. Choose **Basic Auth** in the **TYPE** drop-down list, and enter a username and password. You'll learn more about authentication in this lesson. At the bottom you can see what came back from that request—a JSON file listing all the organizations. You can see the organization name, allocated seats, seats in use, expiration date, and so on.

Vouchers & Dumps are Available | WhatsApp +201224560923

DO NOT REPRINT Brave-dumps.com
© FORTINET

Quick Reference Table of Commands

- Below are a selection of useful API commands
- See the *FortiEDR RESTful API* guide for a complete list

Commands	Method	Description
list-events	GET	Outputs all the events in the system that match the condition(s) you specify in the call
list-raw-data-items	GET	Outputs the raw data items for an event ID
update events	PUT	Updates the read/unread, handled/unhandled, or archived/unarchived state of an event
create exception	POST	Adds an exception to a specific event
list-products	GET	Outputs a list of all the communicating applications in the system within the specified parameters
list-collectors	GET	Outputs a list of the collectors in the system within the specified parameters
delete-collectors	DELETE	Deletes a specified collector
get-event-file	GET	Retrieves a file or memory
remediate-device	PUT	Terminates a process and removes an executable on the specified device
set-system-mode	PUT	Switch the entire system to Simulation or Prevention mode
list-system-events	GET	Outputs a list of system events matching the specified parameters

NSE Training Institute

© Fortinet Inc. All Rights Reserved.

7

This slide shows a selection of useful API commands. You can get a full list with detailed instructions in the *FortiEDR RESTful API* guide.

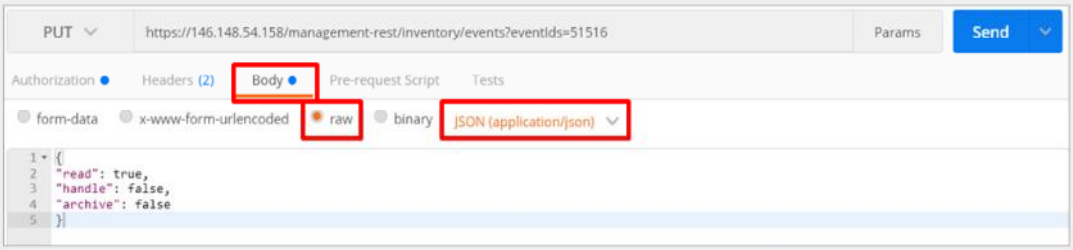
Vouchers & Dumps are Available | WhatsApp +201224560923

DO NOT REPRINT Brave-dumps.com
© FORTINET

Postman App

- Enter the URL parameters in the URL field at the top of the right-hand panel
- For requests requiring body parameters:
  1. Click the **Body** tab
  2. Select the **raw** radio button
  3. Select **JSON (application/json)** in the **Format** drop-down menu
  4. Enter **Body** parameters as needed

- Advantages of using Postman:
  - Easy interaction with the API
  - Clean interface
  - Saves API request history
- Tips
  - Remember to select the correct request type (GET, POST, DELETE, or PUT)



NSE Training Institute

© Fortinet Inc. All Rights Reserved.

8

Why use Postman? It's a very easy way to interact with the API—it's a clean and simple interface, and it saves API request history, so you can have a working list of what you've done previously, and you can reuse a request to save you from having to enter in all the information again.

Here are a few tips on using a Postman. First, make sure you select the correct request method on the left side of the screen. In the example shown on this slide, you can see a **PUT** request. Next to that are the URL parameters. You'll learn more about body parameters later in this lesson. You can also consult the *FortiEDR RESTful API Guide* for a complete list of options. Some request types require body parameters. In that case, select the **Body** tab, select **raw**, and then select **JSON (application/json)** format from the drop-down list on the right side of the screen. Then you can type your body parameters into the text field. The example shown on this slide changes the status of event 51516.

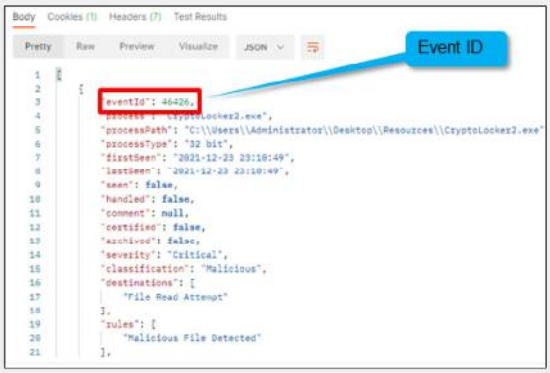
Vouchers & Dumps are Available | WhatsApp +201224560923

DO NOT REPRINT Brave-dumps.com
© FORTINET

Example Workflow—Find Threats

- Get a list of events
  - View list of malicious or suspicious events with block actions with Postman:

```
GET
https://<FortiEDRHOST>/management-rest/events/list-events?classifications=Malicious,Suspicious&actions=Block
```



NSE Training Institute © Fortinet Inc. All Rights Reserved. 9

Take a look at an example workflow using the API. In this scenario, you'll be investigating threats in a FortiEDR environment. First, you need a list of events classified as malicious or suspicious and with an action of block or simulation block.

At this point, you're retrieving information rather than changing anything, so you're using the `GET` method. Then, you'll enter the URL parameters. You've seen a few examples already, but this time you're looking for a list of events, so start with `https`, then enter your FortiEDR host. You can use the IP address or the name for example, `acme.fortiedr.com`. After the host address, always enter `management-rest` followed by the category, `events`, and then the call—in this case, `list-events`. Then you'll add the search criteria. You can search for multiple search parameters at once by using an ampersand in between parameters. In this case, you're searching for `classifications` and `actions`. You can also enter multiple values for each criterion by separating them with a comma. In this case, we're looking for two possible classifications and two possible actions.

This search returns a list in JSON format. There is quite a bit of information about each event—the event ID, process, path, dates, status, which rules were violated, and so on. To continue the example workflow, let's say we're investigating the event shown on this slide. Note the event ID, 46426. Next, you'll use that ID in a new request.

Vouchers & Dumps are Available | WhatsApp +201224560923

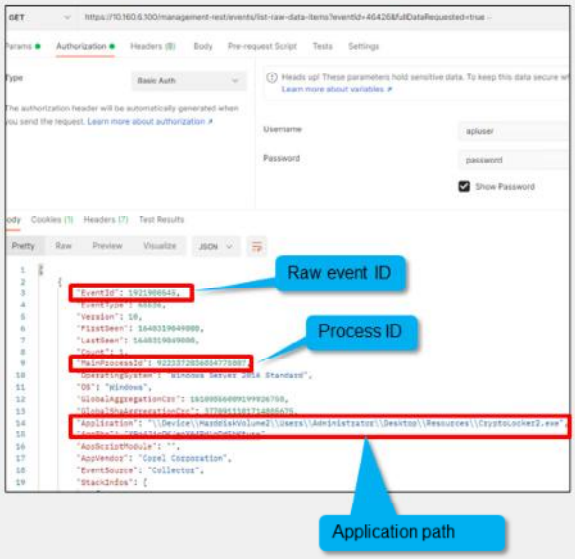
DO NOT REPRINT Brave-dumps.com
© FORTINET

Example Workflow—Get Raw Event Details

- Use the event ID, retrievable from the events list returned by the previous search, to retrieve raw event data using Postman:

  GET
  https://<*FortiEDRHOST*>/management-rest/events/list-raw-data-items?eventId=<*00000*>&fullDataRequested=true

- Find and copy the raw **EventID**, **Main Process ID**, and **Application** path that caused the alert
  - You will use these to retrieve a sample of the malware
  - You must convert an application path to URL encoded format



© Fortinet Inc. All Rights Reserved.

Now get the raw event details for the event ID you just copied. You'll send another GET request, this time asking for the raw data items for the event ID, and then add `fullDataRequested=true`.

Again, you'll receive a JSON list, this time showing the details about the raw items. Use this information to retrieve the executable. To do that, you'll need the raw **EventId**, **MainProcessId**, and the **Application** path. Copy each of these values into a separate text file so you can use them later to retrieve a sample of the malware. There are a couple of things to remember. First, the **EventId** field here is not the same as the event ID you copied in the previous slide. This is the *raw* event ID, which is what you need to retrieve the file. You must convert an application path to URL encoded format.

Vouchers & Dumps are Available | WhatsApp +201224560923

DO NOT REPRINT Brave-dumps.com
© FORTINET

Example Workflow—Get a Sample of Malware

- Use the raw EventId, Main Process ID, and Application file path retrieved in the previous step to retrieve a sample of the malware that caused the *event*

  ```
  GET
  https://<FortiEDRHOST>/management-rest/forensics/get-event-file?rawEventId=<raw event ID>&processId=<Main Process ID>&filePaths=<full path>
  ```

- You will see a file like the one shown in the screen capture
  - This is binary copy of the executable, saved as a password-protected zip file
- To save the zip file to your hard drive for analysis, click the **Send** drop-down menu, and select **Send and Download**

NSE Training Institute

© Fortinet Inc. All Rights Reserved.

11

Now use the information you just got to retrieve the executable using a GET command. Then enter the URL parameters. In this case, you're looking for information stored in forensics, so change the parameters to `forensics`, followed by the `get-event-file` command. Then use the information you just copied—the raw event ID, process ID, and application path—to tell the system exactly what file you're looking for.

If you click **Send**, your results will look something like what you see in the upper-right area of the screen. It looks like gibberish, but it's actually a password-protected zip file containing the file you requested. To get that file in a usable format, you use **Send and Download**. Use the **Send** drop-down menu to select **Send and Download**. Now you can save the zip file locally. To extract the executable, enter the password—`enCrypted`, with a capital C.

Vouchers & Dumps are Available | WhatsApp +201224560923

DO NOT REPRINT Brave-dumps.com
© FORTINET

Example Workflow—Delete the Executable

- If a collector has been attacked, you may want to temporarily move it to the built-in **High Security Collector Group** for additional protection:

```
PUT
https://<FortiEDRHOST>/management-rest/forensics/remediate-
device?device=<VICTIM>&executablesToRemove=%5CDevice%5CHarddiskVolume2%5CUsers%5CAdministrator
%5CDesktop%5CResources%5CCryptoLocker2.exe
```

- If you look on the device, you should see that the malicious file has been removed

NSE Training Institute © Fortinet Inc. All Rights Reserved. 12

Next, remove the malicious executable from the user's device. You can do this using a PUT request. This is a forensics function, so enter `forensics/remediate-device`. Then, specify the device name and the name and path of the executable you want to remove, using the format you see here. The file should disappear from the device, as the example on this slide shows.

Vouchers & Dumps are Available | WhatsApp +201224560923

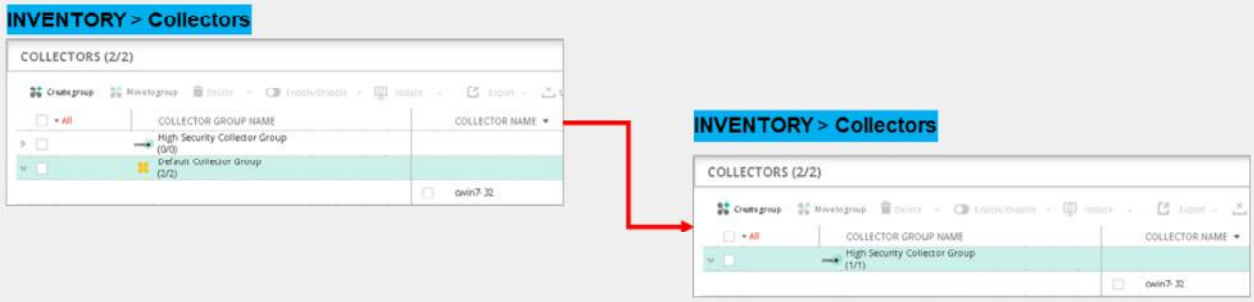
DO NOT REPRINT Brave-dumps.com
© FORTINET

Example Workflow—Move the Infected Collector

- If a collector has been attacked, you may want to temporarily move it to the built-in **High Security Collector Group** for additional protection:

```
PUT
https://<FortiEDRHOST>/management-rest/inventory/move-collectors?collectors=<VICTIM>&targetCollectorGroup=High Security Collector Group
```

- To verify the results, find the collector in the **INVENTORY** tab of the central manager



© Fortinet Inc. All Rights Reserved.

After you've retrieved the executable, evaluate it by testing it in a secure sandbox environment. For example, say you verify that the file is malicious. You might want to put the affected collector into the **High Security Collector Group** to contain the infection until you fully remediate the device. To do that, send a PUT command. You're sending information related to inventory, so enter `inventory/move-collectors`. Then enter the collector name and the target group—in this case, the **High Security Collector Group**. You can verify the result in the management console. The example on this slide shows you that you successfully moved `cwin7-32` from the **Default Collector Group** to the **High Security Collector Group**.

Vouchers & Dumps are Available | WhatsApp +201224560923

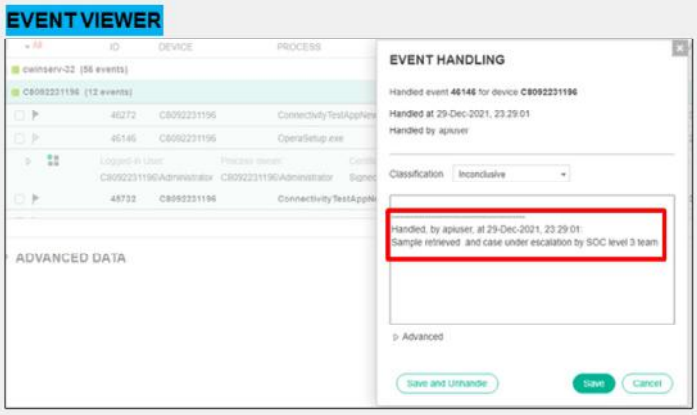
DO NOT REPRINT Brave-dumps.com
© FORTINET

Example Workflow—Mark the Event as Read and Handled

- Once you are confident that you have successfully resolved the infection, you can mark the event as **Handled** using the API:

```
PUT
https://<FortiEDRHOST>/management-rest/events?eventIds=<ID>
Body:
{
"handle": true,
"comment": "Sample retrieved and case under escalation by SOC level 3 team"
}
```

- To verify the results, find the event in the **EVENT VIEWER** tab of the management console and click on the **Handled** flag



NSE Training Institute
© Fortinet Inc. All Rights Reserved.

After you remediate the device or create an exception, mark the event as **Handled** so that other management console users know you've already dealt with it. You can also mark it as **Read**. To change the event status, send a PUT request. You must modify the event in the `events` category. Then, you must specify the event ID. This time, you must complete the body field. Set `read` to `true` and `handle` to `false`, meaning the event is no longer *to handle*. It's always a good idea to add a comment explaining how you handled the event and any other relevant information. You can verify your changes in the **EVENT VIEWER** tab of the management console. In the image on this slide, you can see that the event is **Handled** and your comment has been added to the **EVENT HANDLING** window. If you look closely, in the background you can see a light-colored flag, which indicates that the event has been handled, and the event is in plain text, meaning it is marked as read.

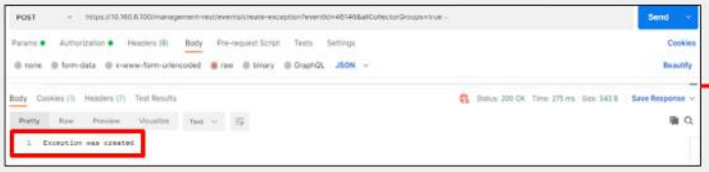
Vouchers & Dumps are Available | WhatsApp +201224560923

DO NOT REPRINT Brave-dumps.com
© FORTINET

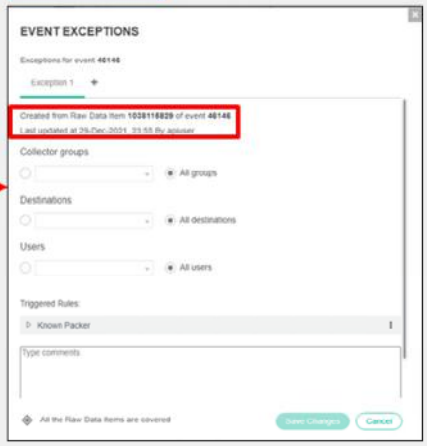
Example—Create an Exception

- Once you have examined the file as safe, an exception can be created for the event using API

```
POST
https://<FortiEDRHOST>/management-rest/events/create-exception?eventId=<EventID>&allCollectorGroups=true
```



EVENT VIEWER



© Fortinet Inc. All Rights Reserved.

This slide shows an alternative scenario. Say you examine the file that triggered an alert and find that it isn't malware. In that case, you might want to create an exception. You can do that through the API as well. Use a **POST** command. In the `events` category, in the URL parameters, enter `events/create-exception`. Then, you must specify the exception parameters—the event ID it applies to, then the collector groups you want to apply the exception to, which, in the example shown on this slide, is the `Sales Group`, and not all collector groups. We can also specify destinations. The example shown on this slide shows that the exception is applied to collector groups, all destinations, and all users.

Vouchers & Dumps are Available | WhatsApp +201224560923

DO NOT REPRINT Brave-dumps.com
© FORTINET

Knowledge Check

1. Which format should you use for FortiEDR API requests?
   - ✓ A. JSON
   - B. XML
2. A new user is not able to make successful API requests using Postman. What is a likely reason?
   - ✓ A. The user has not been assigned the Rest API role
   - B. You have exceeded the allowed number of authorized API users

NSE Training Institute

© Fortinet Inc. All Rights Reserved.

16

Vouchers & Dumps are Available | WhatsApp +201224560923

DO NOT REPRINT
© FORTINET
Brave-dumps.com

Review

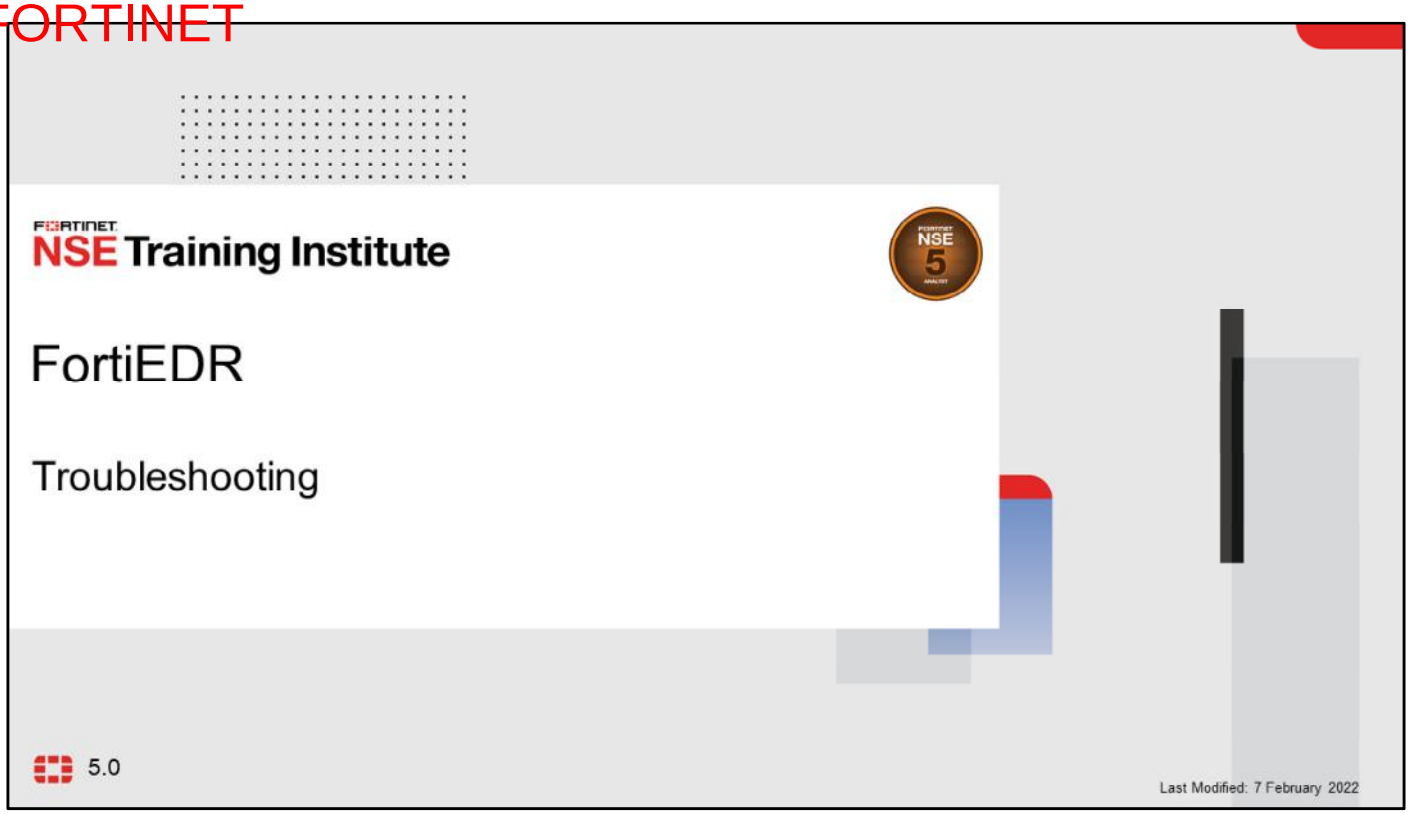
- ✓ Understand what the API is
- ✓ Access the API
- ✓ Perform basic tasks using the API

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

By mastering the objectives covered in this lesson, you learned how to use the RESTful API with FortiEDR.

Vouchers & Dumps are Available | WhatsApp +201224560923

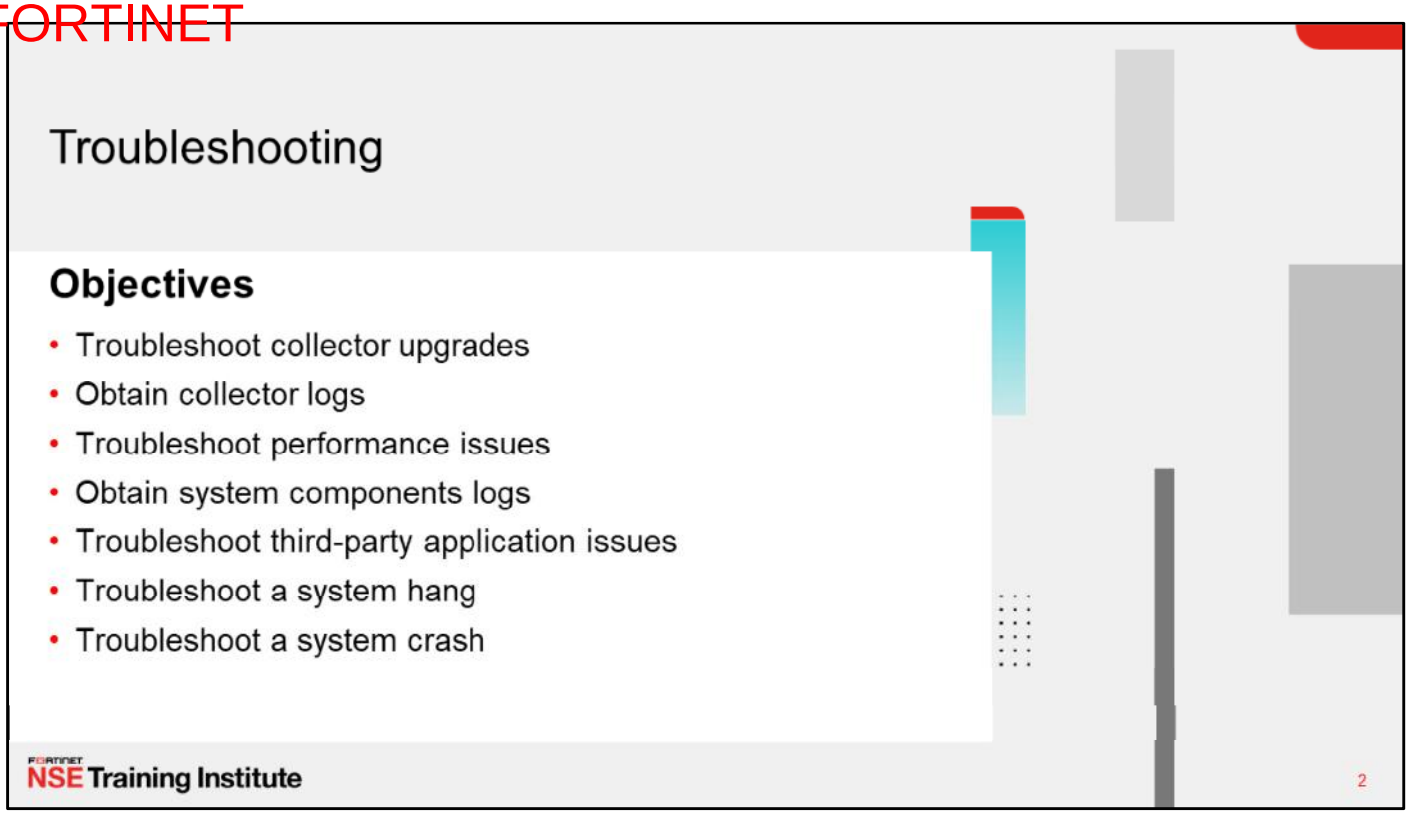
DO NOT REPRINT
© FORTINET
Brave-dumps.com



In this lesson, you will learn about troubleshooting.

Vouchers & Dumps are Available | WhatsApp +201224560923

DO NOT REPRINT Brave-dumps.com
© FORTINET



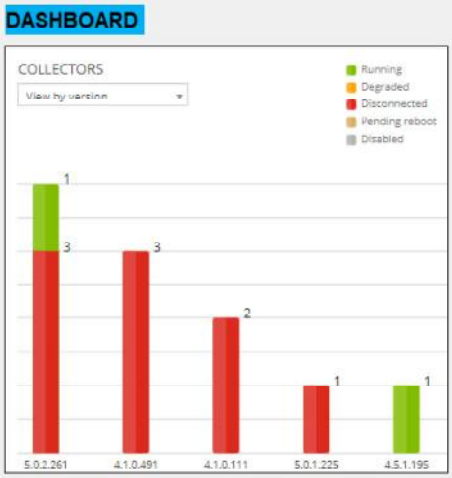
By demonstrating competence in advanced troubleshooting, you will be able to troubleshoot collector upgrades, and obtain collector logs to troubleshoot performance issues, including issues with third-party applications, a system hang, and a system crash.

Vouchers & Dumps are Available | WhatsApp +201224560923

DO NOT REPRINT Brave-dumps.com
© FORTINET

Troubleshooting Collector Upgrades

- If you have trouble upgrading a collector, follow these steps to troubleshoot:
  1. Verify upgrade settings on the management console
  2. Restart the device
  3. Obtain collector logs:
     a. If the device is connected, download collector logs from the management console
     b. If the device is offline, obtain the logs locally
  4. If working with local logs, locate the point where the failure occurred
  5. Send logs to Fortinet support
  6. Update the collector locally
  7. If requested, run Process Monitor at the same time as the installation and send logs to Fortinet support (rare)



NSE Training Institute

© Fortinet Inc. All Rights Reserved.

3

This slide provides an overview of the troubleshooting process for collector upgrades. You will learn more about these steps later in this lesson. First verify the settings on the management console. You don't want to go through the whole troubleshooting process only to discover that the collector group was set to the wrong version.

Next, restart the device. Usually, upgrading the FortiEDR collector does not require a restart but, occasionally, compatibility issues—usually with antivirus software—require a restart.

Third, locate the collector logs. You can do this on the local machine, or you can download them through the management console, if it's connected. If you're working with local logs, you can go through them to locate the point where the failure occurred, or send them to Fortinet support. Logs obtained through the management console are encrypted, so you must send them to Fortinet support for decryption and analysis.

Next, try updating the collector locally using the installer file.

Lastly, on rare occasions where the collector logs do not provide enough information, Fortinet support may request that you run Process Monitor at the same time as the installation and return the logs. You don't need to do this unless specifically requested by support.

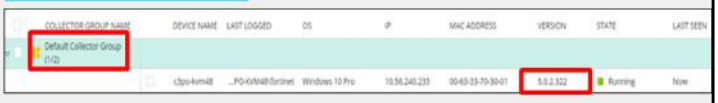
Vouchers & Dumps are Available | WhatsApp +201224560923

DO NOT REPRINT Brave-dumps.com
© FORTINET

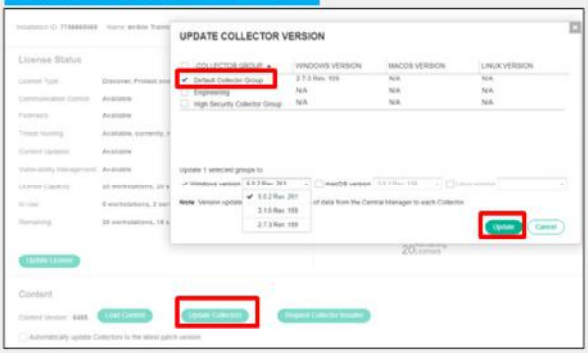
Collector Upgrades—Verifying Settings

- Locate the collector group assignment:
  1. On the **INVENTORY** tab of the management console, search for the device name
     - Remember to click **Show all collectors** before beginning your search
  2. Note the collector group assigned to the device
  3. Verify the collector version of the device
- Check the **Upgrade Collectors** dialog:
  1. Click the **ADMINISTRATION** tab
  2. In the **LICENSING** panel, click the **Update Collectors** button
  3. In the **UPDATE COLLECTOR VERSION** dialog, locate the assigned collector group and verify that the collector version shown is the one you expected

INVENTORY > Collectors



ADMINISTRATION > LICENSING



NSE Training Institute

© Fortinet Inc. All Rights Reserved.

4

Again, the first step in troubleshooting upgrades is verifying your settings on the console. First, you need the collector group assignment for the device you're investigating. As you learned in previous lessons, you can locate that by clicking the **INVENTORY** tab and searching for the device name. The search results show the collector group assigned to the device, and its version. Verify that the version number is what you were expecting, and make a note of the collector group name. Remember, by default, you see only **Degraded** collectors, so make sure you click the blue **Show all Collectors** link.

After you have your collector group assignment, you can check the assigned version on the **LICENSING** panel of the **ADMINISTRATION** tab. Click the **Update Collectors** button. The **UPDATE COLLECTOR VERSION** dialog opens. Locate the collector group you noted earlier and make sure it's assigned to the correct collector version.

Note that in a multi-tenant environment, Fortinet recommends performing device upgrades from the Hoster view.

Vouchers & Dumps are Available | WhatsApp +201224560923

DO NOT REPRINT Brave-dumps.com
© FORTINET

Exporting Collector Logs

- If the device is currently connected, you can retrieve the collector logs using the management console:
  1. On the **INVENTORY** tab, locate the collector
  2. Select the checkbox next to the collector
  3. In the **Export** drop-down list, select **Collector Logs**
  4. Save the logs on your local hard drive
- Remote log protection
  - The logs are encrypted and downloaded to a password-protected zip file
  - Send them to Fortinet support for decryption and analysis

NSE Training Institute © Fortinet Inc. All Rights Reserved. 5

Now, you will learn about the process of retrieving collector logs. The easiest way to get the logs is through the management console, which you can do if the device is currently connected to your network. Locate the collector on the **INVENTORY** tab and select its checkbox. Then, click the **Export** drop-down list and select **Collector Logs**. Save the logs locally. They are downloaded into a password-protected zip file. The collector files themselves are encrypted to prevent tampering, so you must send them to Fortinet support for decryption and analysis.

Vouchers & Dumps are Available | WhatsApp +201224560923

DO NOT REPRINT Brave-dumps.com
© FORTINET

Obtaining Collector Logs Locally

- Windows
  - Open the command prompt as Administrator
  - Run the following command:

```
"C:\Program Files\Fortinet\FortiEDR\FortiEDRCollectorService.exe" --support
```

  - Gather the files from the following location: %TEMP%\program_data_archive_support.zip
- Linux
  - Run the following command in terminal:

```
sudo /opt/FortiEDRCollector/bin/FortiEDRCollector --support
```

  - Gather the logs from the following location: /tmp/program_data_archive_support.zip
- macOS
  - Run the following command in terminal:

```
/Applications/FortiEDR.app/FortiEDRCollector --support
```

NSE Training Institute

© Fortinet Inc. All Rights Reserved.

6

In the event that the collector is not connected to the FortiEDR central manager, you can download the collector logs locally . You can use the CLI commands shown on this slide to download the collector logs.

Vouchers & Dumps are Available | WhatsApp +201224560923

DO NOT REPRINT Brave-dumps.com
© FORTINET

Checking FortiEDR Services Locally

- Windows
  - Open the command prompt as Administrator
  - Run the following command:

```
>"C:\Program Files\Fortinet\FortiEDR\FortiEDRCollectorService.exe" --status
  FortiEDR Service: Up
  FortiEDR Driver: Up
  FortiEDR Status: Running
```

- Linux
  - Run the following command in terminal:

```
#/opt/FortiEDRCollector/control.sh --status
  FortiEDR Service: Up
  FortiEDR Driver: Up
  FortiEDR Status: Running
```

- macOS
  - Run the following command in terminal:

```
sudo /Applications/FortiEDR.app/fortiedr_collector.sh status
FortiEDR Service: Up
FortiEDR NetworkExtension: Up
FortiEDR EndPoint Extension: Up
FortiEDR Status: Running
```

NSE Training Institute

© Fortinet Inc. All Rights Reserved.

7

On the collector, if you need to verify the FortiEDR installation is successful and there are no configuration or communication issues, use the CLI commands shown on this slide.

Vouchers & Dumps are Available | WhatsApp +201224560923

DO NOT REPRINT Brave-dumps.com
© FORTINET

Collector Does Not Display on INVENTORY Tab

- Newly installed collectors may not display on the **INVENTORY** tab, or, sometimes the collectors show in a **disconnected** state
  - Perform the following troubleshooting steps:
    - Verify network connectivity between FortiEDR Collector > FortiEDR Core > FortiEDR Aggregator > FortiEDR Central Manager console
    - Validate that ports 555 and 8081 are open (make sure that Telnet is enabled)
      - On the collector, run `telnet` to verify that the ports are open

```
telnet <aggregator IP> 8081
telnet <core IP> 555
```

      - On the collector, run `netstat` to verify communication is established
        - Windows

```
netstat -an | findstr 8081
netstat -an | findstr 555
```

        - macOS and Linux

```
netstat -an | grep 8081
netstat -an | grep 555
```

NSE Training Institute © Fortinet Inc. All Rights Reserved. 8

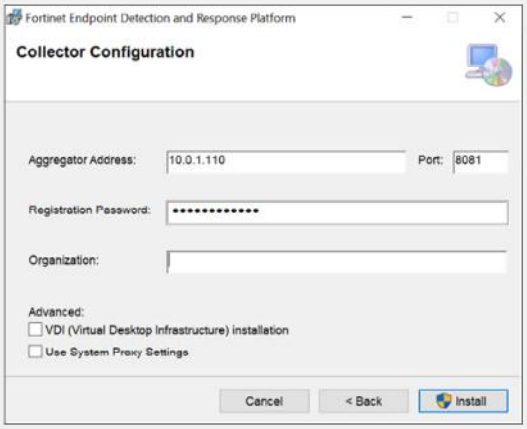
Newly installed collectors don't show on the **INVENTORY** tab of the central manager console and sometimes collectors are seen in a **disconnected** state. To troubleshoot the connection issues, verify that there is network connectivity between all the FortiEDR components. Validate that ports 555 and 8081 are open and no third-party applications are blocking these ports. Command line tools, like `telnet` and `netstat` can verify if these ports are available.

Vouchers & Dumps are Available | WhatsApp +201224560923

DO NOT REPRINT Brave-dumps.com
© FORTINET

Collector Upgrades—Advanced Troubleshooting

- Run the upgrade locally using the installer file
  - Remember, you need your organization's **Registration Password** for all local installations
  - Run process monitoring `ProcMon`
  - On rare occasions, Fortinet support may need additional information not included in the collector logs
- In these cases, Fortinet may request that you run `ProcMon`, a free Sysinternals tool from Microsoft, at the same time as the installation
  1. Run `ProcMon` at the same time as the installation
  2. Save the `ProcMon` log to a PML file
  3. Get the installer logs using the parameter `/l*vx log.txt`
  4. Send the results to Fortinet support



NSE Training Institute

© Fortinet Inc. All Rights Reserved.

9

If you're still having trouble with upgrading your collector, run the installer file locally on the end user's machine. To do this, you will need your organization's registration password, which you can locate on the **ADMINISTRATION** tab of the management console under **TOOLS**.

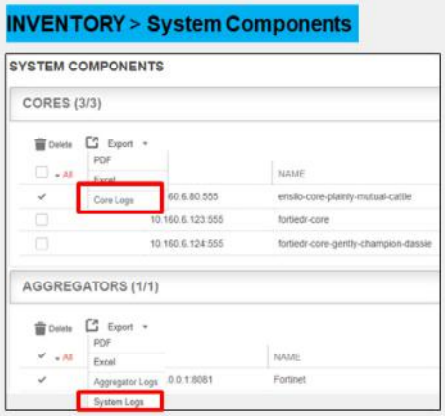
If Fortinet support needs additional information not included in the collector logs, they may request that you run ProcMon, which is a free Sysinternals tool from Microsoft. This happens rarely, but if it's needed, run ProcMon while performing the installation and save the ProcMon log to a PML file. Then, obtain the installer logs using the parameter `/l*vx log.txt`. and send these logs to Fortinet support.

Vouchers & Dumps are Available | WhatsApp +201224560923

DO NOT REPRINT Brave-dumps.com
© FORTINET

Exporting System Component Logs

- You can retrieve the core and aggregator logs using the management console:
  - Core Logs:
    1. On the **INVENTORY > System Components** tab, locate the core
    2. Select the checkbox next to the core
    3. In the **Export** drop-down list, select **Core Logs**
    4. Save the logs on your local hard drive
  - Aggregator Logs:
    1. On the **INVENTORY > System Components** tab, locate the aggregator
    2. Select the checkbox next to the core
    3. In the **Export** drop-down list, select **Aggregator Logs**
    4. Save the logs on your local hard drive



© Fortinet Inc. All Rights Reserved.

The easiest way to get the logs is through the management console, which you can do if the components are currently connected to your network. Locate the core or aggregator on the **INVENTORY** tab under **System Components,** and, select its checkbox. Then click the **Export** drop-down list and select **Core Logs** or **Aggregator Logs**. Save the logs locally. They are downloaded into a password-protected zip file. Send these files to Fortinet support for decryption and analysis.

Vouchers & Dumps are Available | WhatsApp +201224560923

DO NOT REPRINT Brave-dumps.com
© FORTINET

Troubleshooting Performance Issues

- If a device is experiencing application slowness, system hanging, or blue screen of death (BSoD), follow these steps to troubleshoot:
  1. Restart the device
  2. Disable the collector on the management console
  3. Upgrade the collector if newer versions are available
  4. Perform additional troubleshooting based on the nature of the problem:
     - Third-party app performance issue: record the steps to reproduce the problem
     - System hang:
       a. Create a manual crash dump
       b. Gather a full memory dump while the system is hanging
     - System crash, or BSoD:
       a. Verify that BSoD occurred
       b. Gather a full memory dump while the system is hanging
  5. Gather collector logs while the device is running
  6. Open a support ticket with Fortinet

NSE Training Institute

© Fortinet Inc. All Rights Reserved.

11

If you're troubleshooting performance issues on a device, begin by restarting. If that doesn't help, disable the collector on the management console. If the issue persists, upgrade the collector if there is a newer version available.

If the performance issue continues, your next step depends on what type of problem you're investigating. You will learn about each of these procedures on the next slides. If it's a performance issue with a third-party app, you must record the steps to reproduce the issue. For a system hang, create a manual crash dump, then gather a full memory dump while the system is hanging. For a system crash, or blue screen of death (BSoD), verify that the BSoD occurred, then gather a full memory dump while the system is hanging.

If you still need more information, try gathering collector logs while the device is running, using the procedures you just completed. If you need help, file a ticket with Fortinet support.

Vouchers & Dumps are Available | WhatsApp +201224560923

DO NOT REPRINT Brave-dumps.com
© FORTINET

Performance Issues—Basic Troubleshooting

- Generic steps
  1. Disable the collector from the management console
  2. Determine the collector version
     - Look for newer versions in the **Update Collectors** dialog in the management console or open a support ticket
     - Apply any available updates to the affected collector
  3. Replicate the issue and record the steps to reproduce it

NSE Training Institute

© Fortinet Inc. All Rights Reserved.

12

Now, you will go through these steps in a little more detail. If you're having performance issues, the first thing to try is disabling the collector, which you can do on the management console. If the problem persists when the collector is disabled, the problem is not likely to be related to FortiEDR.

The next step is to check the collector version. You learned earlier about how to locate the current version of the collector. Look for newer collector versions available in the **Update Collectors** dialog you saw earlier in this lesson. Alternatively, you can open a support ticket with Fortinet support to learn the latest collector version. If there are updates available, apply them to the affected collector and see if the performance improves.

If you are still experiencing issues, replicate the issue and record the steps to reproduce it. You will learn more about this on the next slides.

Vouchers & Dumps are Available | WhatsApp +201224560923

DO NOT REPRINT Brave-dumps.com
© FORTINET

Performance Issue With a Third-Party Application

1. Check for blocking events
   a. On the management console, search the event viewer for any blocking events involving the executable file name
   b. If you locate any blocking events, verify that they are safe, then create an exception
2. Check communication control
   a. If the problem involves a blocked network connection, check the communication control policies
   b. Click **COMMUNICATION CONTROL** > **Policies** and identify which policy has been applied to the affected user's collector group
   c. Search the applications list for the application
   d. Check the policies to make sure that the application is not set to **Deny**
3. Retrieve collector logs

NSE Training Institute © Fortinet Inc. All Rights Reserved. 13

If your performance issue involves a third-party application, start by checking for blocking events. On the management console, click the **EVENT VIEWER** tab and search for the executable file name of the application you're investigating. If you locate any blocking events, verify that they're safe. It is possible that an event involving a seemingly safe process is, in fact, malicious—for example, a malicious macro can run in a legitimate copy of Microsoft Word, or a malicious program may be masquerading as a legitimate app. After you verify that the event is safe, you can create an exception to allow the safe process to run.

If there are no blocking events and the application you're investigating cannot connect to the network, check the Communication Control policies. First, click the **COMMUNICATION CONTROL** tab, and then select **Policies**. Look for the policy that is applied to the user's collector group. Then, search the applications list for the application. Highlight the application and check the **Policies** panel to make sure the user's policy hasn't been set to deny communication from that application. Check individual versions too—sometimes an older version is blocked for older versions with known vulnerabilities but allowed for newer, safer versions.

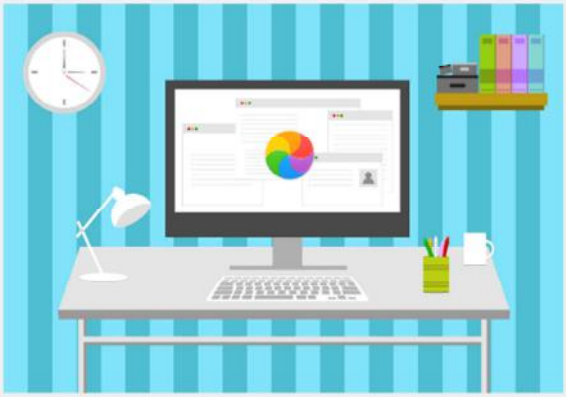
If you still haven't found the source of the problem, retrieve the collector logs using the procedures that were outlined earlier.

Vouchers & Dumps are Available | WhatsApp +201224560923

DO NOT REPRINT Brave-dumps.com
© FORTINET

System Hang

- Manual crash dump
  - Create a manual crash dump using the applicable Microsoft instructions or a third-party utility, such as Bang
- Full memory dump
  - Gather a full memory dump while the system is hanging
  - Zip the memory dump
  - Make a note of the Sha256 to validate file integrity
- Retrieve collector logs



NSE Training Institute

© Fortinet Inc. All Rights Reserved.

14

If you're experiencing a system hang, start by creating a manual crash dump using the applicable instructions from Microsoft or a third-party utility, such as Bang.

Next, gather a full memory dump while the system is hanging. You will learn the details of this process later in this lesson. After you finish, zip the memory dump and make note of the Sha256 to validate file integrity.

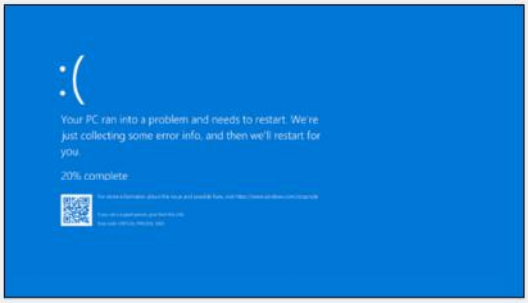
Lastly, retrieve the collector logs for the affected device. Again, refer to the procedures you learned earlier in this lesson.

Vouchers & Dumps are Available | WhatsApp +201224560923

DO NOT REPRINT Brave-dumps.com
© FORTINET

System Crash

- BSoD verification
  - If BSoD occurred, there will be a memory dump and stop code
    - Check the file at `%SYSTEM%\memory.dmp`
  - In the Windows Event Viewer Application Log, search for "`Kernel Power`" to locate any records of a BSoD
- Full memory dump
  - Gather a full memory dump while the system is hanging
  - Zip the memory dump
  - Make a note of the Sha256 to validate file integrity
- Retrieve collector logs
  - Retrieve the collector logs for the affected device using the procedures outlined earlier in this lesson



NSE Training Institute © Fortinet Inc. All Rights Reserved. 15

If you're investigating a system crash, start by verifying that the BSoD occurred. You should locate a memory dump and stop code in the `memory.dmp` file in the `System` folder. You can also check the Windows Event Viewer Application Log. Search for `kernel power` to locate any records of a BSoD.

Next, create a full memory dump while the system is hanging. Zip the memory dump file and make a note of the Sha256.

Lastly, as with the previous procedures, retrieve the collector logs, either locally or through the management console, as described earlier in this lesson.

Vouchers & Dumps are Available | WhatsApp +201224560923

DO NOT REPRINT Brave-dumps.com
© FORTINET

Knowledge Check

1. How can you decrypt collector logs?
   A. Use a Base64 converter.
   ✓ B. Send them to Fortinet Support.

2. Which information do you need to perform an upgrade locally?
   A. The assigned collector group
   ✓ B. The organization's registration password

NSE Training Institute

© Fortinet Inc. All Rights Reserved.

16

Vouchers & Dumps are Available | WhatsApp +201224560923

DO NOT REPRINT Brave-dumps.com
© FORTINET

Review

- ✓ Troubleshoot collector upgrades
- ✓ Obtain collector logs
- ✓ Troubleshoot performance issues
- ✓ Obtain system components logs
- ✓ Troubleshoot third-party application issues
- ✓ Troubleshoot a system hang
- ✓ Troubleshoot a system crash

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

By mastering the objectives covered in this lesson, you learned some useful tips for troubleshooting FortiEDR.

Vouchers & Dumps are Available | WhatsApp +201224560923

DO NOT REPRINT
© FORTINET
Brave-dumps.com

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© 2022 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