

DO NOT REPRINT
© FORTINET

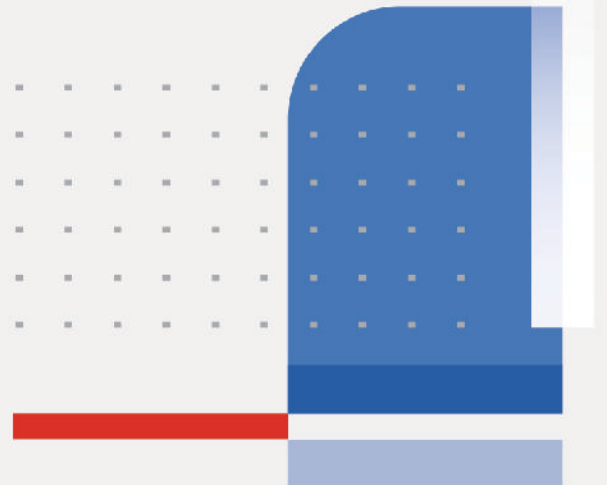
FORTINET
CERTIFIED
SOLUTION
SPECIALIST

Security
Operations

Security Operations Analyst Study Guide

FortiAnalyzer 7.4

FORTINET®
Training Institute



DO NOT REPRINT

© FORTINET

Fortinet Training Institute - Library

<https://training.fortinet.com>

Fortinet Product Documentation

<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 Product Support

<https://support.fortinet.com>

FortiGuard Labs

<https://www.fortiguard.com>

Fortinet Training Program Information

<https://www.fortinet.com/nse-training>

Fortinet | Pearson VUE

<https://home.pearsonvue.com/fortinet>

Fortinet Training Institute Helpdesk (training questions, comments, feedback)

<https://helpdesk.training.fortinet.com/support/home>



9/27/2024

TABLE OF CONTENTS

01 SOC Concepts and Security Frameworks.....

4

02 FortiAnalyzer Architecture.....

46

03 SOC Operations.....

82

04 SOC Automation.....

126

05 Attack Surface and Vectors.....

173

06 Reporting.....

217

DO NOT REPRINT
© FORTINET

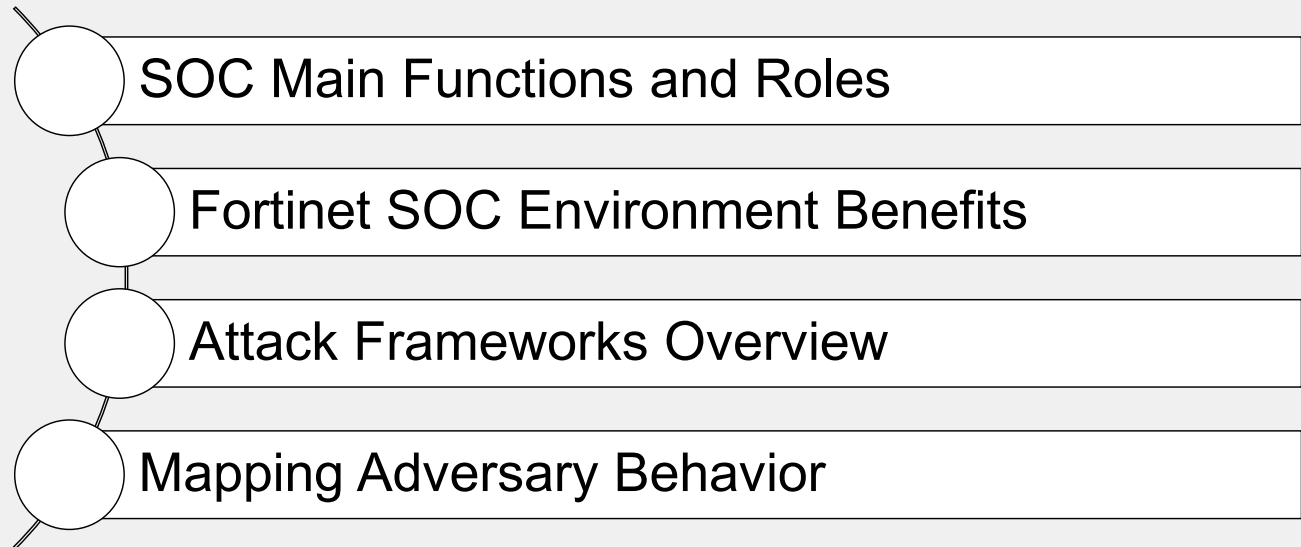


In this lesson, you will learn about the security operations center (SOC), including its importance in an organization, the roles it encompasses, and how it can protect your network.

SOCs are essential in today's cybersecurity landscape for protecting your organization's assets. Using skilled analysts and a tool like FortiAnalyzer, you can integrate logging, analytics, and reporting, all under a single pane of glass, which enables SOC to efficiently identify and respond to incidents, streamline data management, and improve operational efficiency with automation and real-time intelligence. This setup bolsters SOC agility and fortifies security frameworks, preparing teams to effectively combat cyber adversaries and highlighting the strategic benefits of FortiAnalyzer in security operations.

DO NOT REPRINT
© FORTINET

Lesson Overview



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

DO NOT REPRINT
© FORTINET

SOC Main Functions and Roles

Objectives

- Describe the main functions and roles within a SOC
- Describe the main challenges within a SOC

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

By demonstrating competence in understanding the main functions and roles within a SOC, you will be able to recognize its operational framework and organizational dynamics.

DO NOT REPRINT
© FORTINET

What Is a SOC?

Security Operations Center	Threat Monitoring	Continuous monitoring for security events and compromise indicators
	Threat Detection	Analyzing data for patterns and anomalies, and identifying malicious activities
	Incident Response	Swiftly responding, investigating, containing, and restoring from security incidents
	Threat Hunting	Proactively searching for hidden threats using advanced techniques
	Vulnerability Management	Identifying and prioritizing vulnerabilities, patching, and configuration
	Threat Intelligence	Gathering, analyzing, and sharing emerging threat information
	Reporting and Documentation	Documenting incidents, preparing reports, and tracking metrics
	Compliance and Regulations	Ensuring adherence to industry-specific regulations

FORTINET
Training Institute

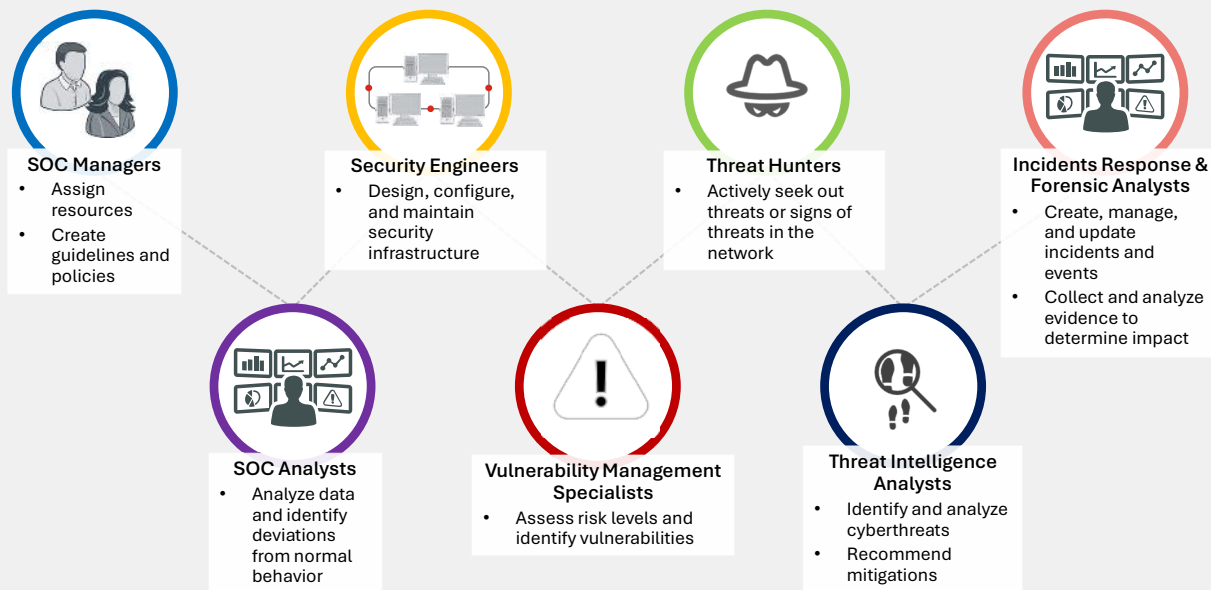
© Fortinet Inc. All Rights Reserved. 4

What are the main functions of a SOC? As this slide shows, a SOC team is responsible for numerous complex tasks that are performed on a daily basis.

A SOC plays a pivotal role in cybersecurity by monitoring, responding, collaborating, continuously improving security measures, and ensuring adherence to industry-specific regulations.

DO NOT REPRINT
© FORTINET

SOC Roles



FORTINET
Training Institute

© Fortinet Inc. All Rights Reserved. 5

To fulfill the numerous functions of a SOC, you will need the appropriate personnel with diverse skillsets to handle the following roles and responsibilities:

- **SOC Manager/Team Lead:** Organizes the day-to-day operations within the SOC, including but not limited to, assigning resources and creating guidelines and policies.
- **SOC Analysts:** Analyze logs on the network and identify any meaningful deviations from the established baselines.
- **Security Engineers:** Design, maintain, and configure the security infrastructure.
- **Vulnerability Management Specialists:** Assess the risk level of the network and identify vulnerabilities.
- **Threat Hunters:** Actively look for threats or signs of threats in the network.
- **Threat Intelligence Analysts:** Identify and analyze cyberthreats. They may use industry-standard attack frameworks to identify the attack vectors and provide recommendations for mitigation.
- **Incident Responders:** Create, manage, and update the security incidents and events on a network. They gauge the severity of events and inform management, as required.
- **Forensics Analysts:** Collect evidence, analyzing it, and determining the impact of a security incident.

Note that the responsibilities are not always clearly delineated. For example, a SOC manager may be responsible for some analyst-centric tasks, such as reviewing incidents. Or a SOC analyst may also be responsible for threat hunting tasks. In general, as an organization grows, it will have employees in more dedicated roles within a SOC. Regardless of how big a SOC is, all personnel must work together, communicate their findings, follow security policies, and react with precision to any threat.

Teams Within a SOC



In the context of SOC and cybersecurity, the terms purple team, red team, and blue team refer to different teams that work on identifying, assessing, and defending against security threats.

Red Team: the simulator

1. Purpose: Simulate adversaries and attempt to exploit vulnerabilities in an organization's systems, just like real-world attackers would.
2. Activities: Conduct penetration tests, vulnerability assessments, and other offensive security exercises.
3. Goal: Identify vulnerabilities and weaknesses in security controls before malicious actors can exploit them.

Blue Team: the defender

1. Purpose: Defend against adversaries and identify, respond to, and mitigate security incidents.
2. Activities: Monitor networks and systems for signs of malicious activity, conduct digital forensics, and implement security measures.
3. Goal: Detect, respond to, and recover from security incidents.

Purple Team: the orchestrator

1. Purpose: Collaborate and share knowledge while working to bridge the gap between the red and blue teams, ensuring that they communicate effectively and learn from each other.
2. Activities: Facilitate knowledge transfer between the red and blue teams, help implement mitigations based on red team findings, and assist in creating more realistic defensive drills.
3. Goal: Improve the organization's overall security posture by integrating the offensive and defensive expertise of the teams.

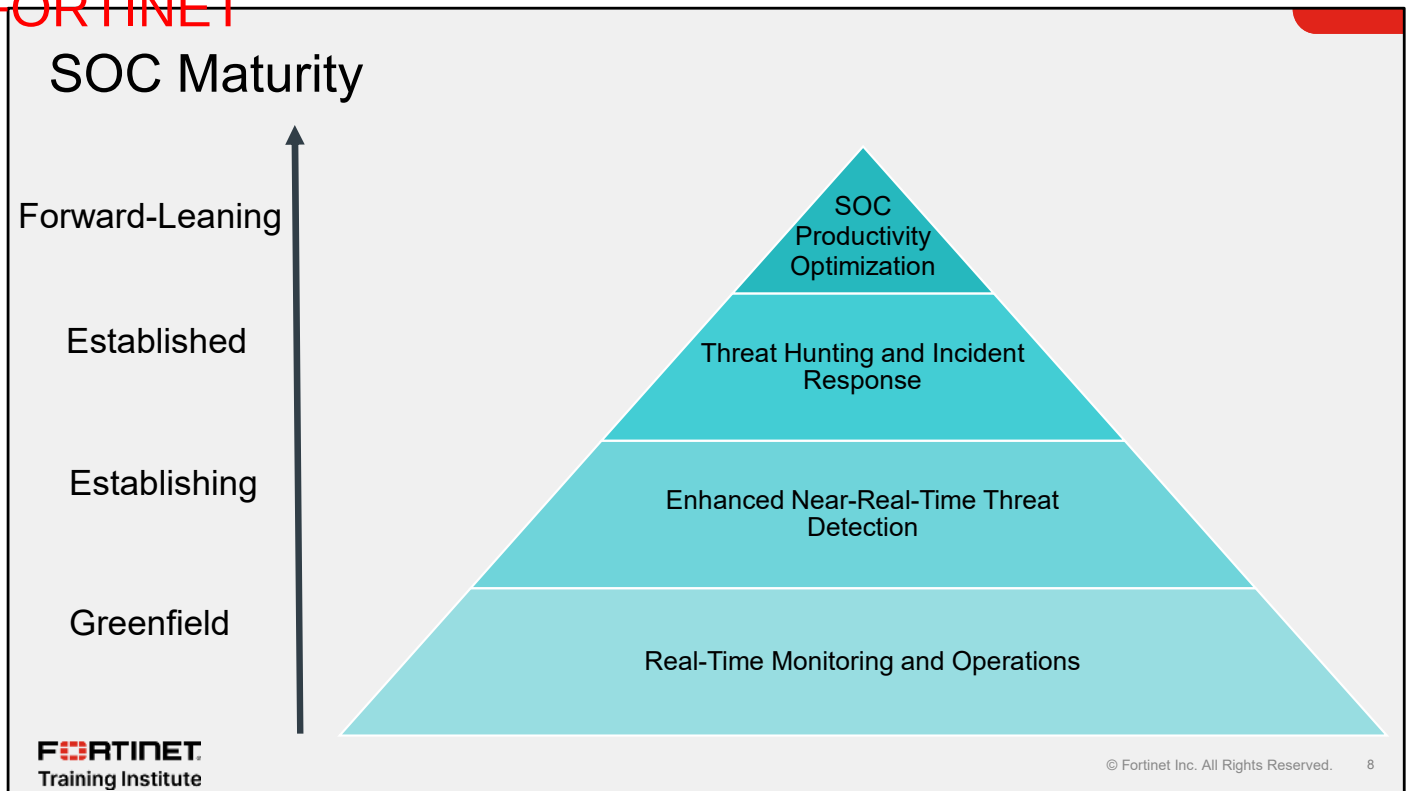
Reasons Why SOC's Fail or Succeed

	Scope	Technology	Implementation
Success	• Focused requirements and use cases • Realistic expectations • Appropriate application (current and future) • Compliant with regulations	• Strong understanding of the market and technology • Meets current and future requirements, and in-scope processes • High-fidelity outputs	• Resources allocated • Required skills identified and planned for • Impact on SOC playbooks understood
Failure	• Shallow and narrow coverage • Unrealistic expectations • Wrong focus (threat vector) • Non-compliance with regulations	• Lack of understanding of how tools work • Too many events (poor sources or poor tech) • Solution didn't deliver	• Too small—no team • Lacking key skills • No playbook—no process • Inconsistent responses

To succeed, a SOC requires security and risk management leaders to provide the correct methodology, technology, and personnel to combat cybersecurity threats. To maintain cybersecurity, a SOC must continue to evolve because threats are continuously evolving: The number of attack vectors and the methods used to exploit weaknesses in a network grow every year.

Successful SOC's have a solid understanding of the scope of the issues, the technologies being used or considered, and the processes being affected. As your SOC team grows, you must consider the impact that growth has on the scope, technology, and implementation requirements.

DO NOT REPRINT
© FORTINET



As a SOC matures and learns, it builds the processes required to treat basic incidents, and starts to differentiate event treatments based on event impact. At this stage, additional tools might be used to expedite the initial assessment, and alerts might be aggregated and augmented with additional context.

More mature organizations might need to strengthen their ability to perform root cause analysis of the incident and elimination of the threat. When a SOC closes an incident, they must ensure the risk of recurrence is correctly handled. The refinement of the end-to-end workflow will result in optimized orchestration, improved productivity, and overall forward movement of the SOC.

DO NOT REPRINT
© FORTINET

Knowledge Check

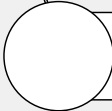
1. Which SOC role is responsible for investigating logs to identify problems?
☒ A. SOC analyst
☐ B. Threat hunter
2. What is the role of the red team in a SOC?
☐ A. To gather and analyze evidence, and determine scope of impact
☒ B. To assess and exploit vulnerabilities

DO NOT REPRINT
© FORTINET

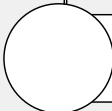
Lesson Progress



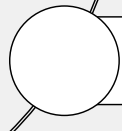
SOC Main Functions and Roles



Fortinet SOC Environment Benefits



Attack Frameworks Overview



Mapping Adversary Behavior



© Fortinet Inc. All Rights Reserved. 10

Good job! You now understand SOC main functions and roles.

Now, you will learn about the benefits of the Fortinet SOC.

DO NOT REPRINT
© FORTINET

Fortinet SOC Environment Benefits

Objectives

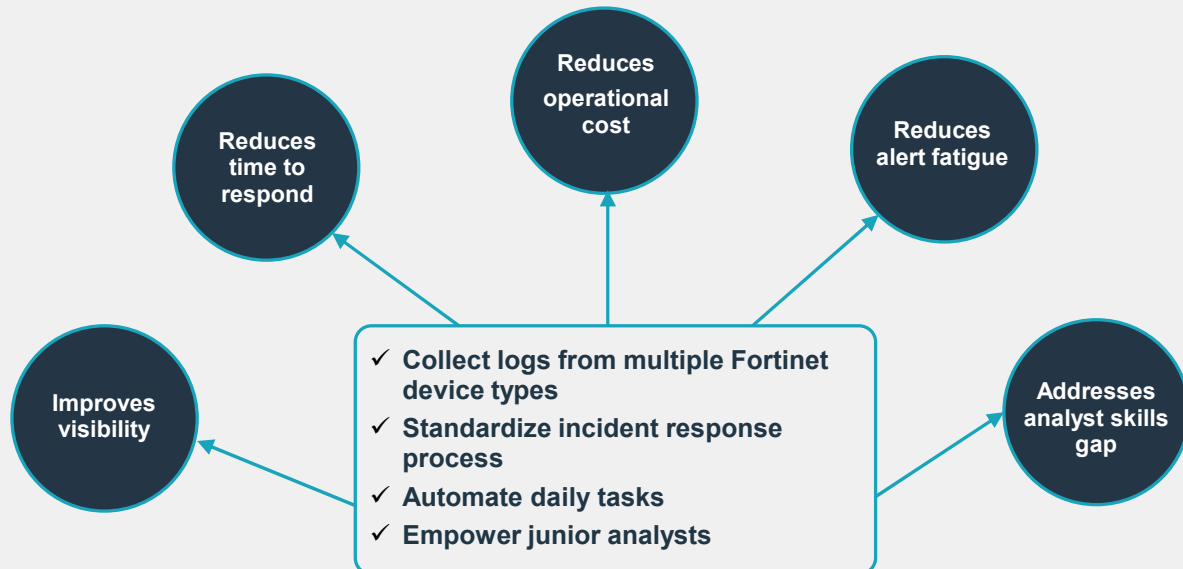
- Identify the challenges that can be solved by the Fortinet SOC
- Describe the Fortinet SOC solution workflow

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

By demonstrating competence in understanding the benefits of the Fortinet SOC, you will be able to select the correct tools to improve your network security.

DO NOT REPRINT
© FORTINET

Benefits of the Fortinet SOC Environment



FORTINET
 Training Institute

© Fortinet Inc. All Rights Reserved. 12

There are many benefits of leveraging the Fortinet SOC in your network.

FortiAnalyzer provides:

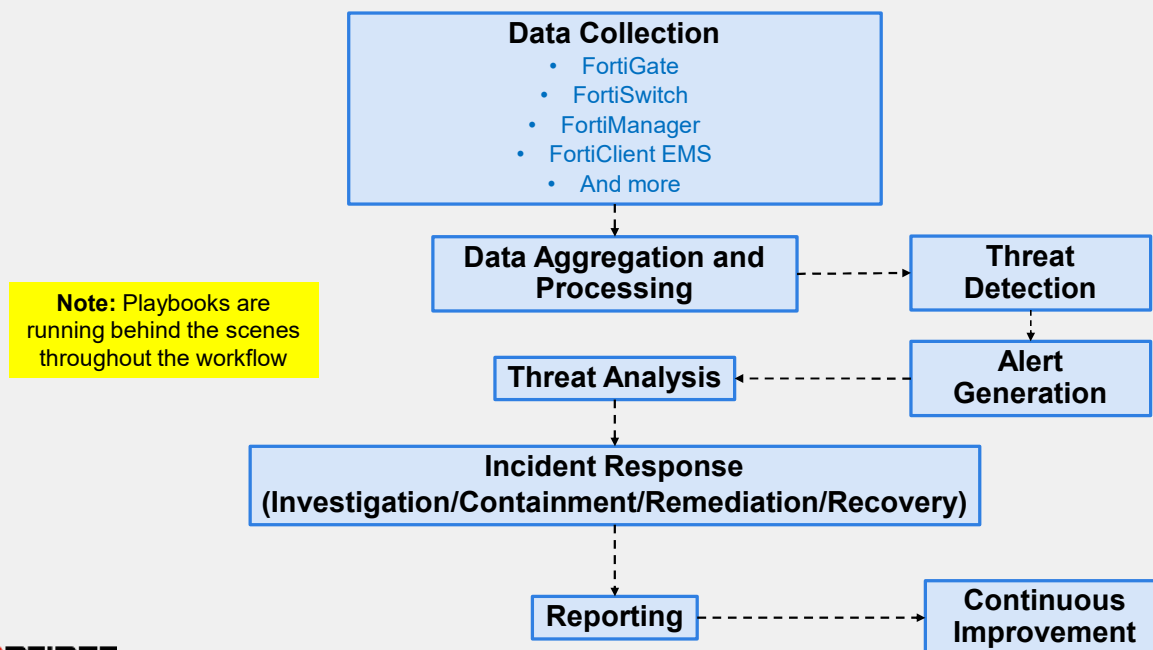
- Centralized logging with event correlation
- Integration with the Fortinet Security Fabric
- Integration with some third-party applications, such as Microsoft Teams and ServiceNow
- Device logging with event correlation and real-time threat detection
- Indicators of compromise (IOC) updated daily with the FortiGuard database
- Incidents and events management
- Automation with playbooks

When you use FortiAnalyzer in a SOC, you increase SOC productivity by addressing the following issues:

- Too many tools: Using a layered, multivendor approach can result in a SOC composed of multiple tools that don't work together and require analysts with specialized skillsets, working in silos. Fortinet SOC solves this.
- Volume of alerts: Automated false positive analysis and closure of tickets on third-party systems will manage alert fatigue
- Manual processes: Automated playbooks can convert most manual analyst processes.
- Ineffective collaboration: Specialization means that not all analysts are equal. Some analysts handle only specific types of incidents, such as phishing attacks, malware outbreaks, distributed denial-of-service (DDoS) attacks, and so on. Analysts can be assigned incidents based on their skillset.

DO NOT REPRINT
© FORTINET

Fortinet SOC Solution Workflow



FORTINET
Training Institute

© Fortinet Inc. All Rights Reserved. 13

The flow chart on this slide shows one possible workflow of the Fortinet SOC solution. FortiAnalyzer allows users to manage many components of the Fortinet SOC through its interface. Overall, Fortinet SOC works by continuously collecting and processing data from various sources to detect potential security threats and anomalies. When FortiAnalyzer detects a security threat, it generates alerts for the security team who then investigate and take the necessary action. Playbooks execute or run behind the scenes, continuously enriching the entire incident response flow. After the incident is handled, the SOC team can generate reports to further analyze the incident and improve processes.

- **Data Collection:** The SOC solution collects data from various sources, such as FortiGate, FortiSwitch, FortiManager, FortiSandbox, FortiClient EMS, and more.
- **Data Processing:** The SOC solution processes the collected data to identify potential security threats and anomalies.
- **Threat Detection:** The SOC solution uses threat intelligence to detect security threats, such as malware, phishing attempts, and suspicious network activity.
- **Alerting:** When the SOC solution detects a security threat, it generates alerts and notifications to the security team.
- **Incident Investigation:** The security team investigates alerts to determine the severity and scope of the security threat.
- **Containment:** If necessary, the security team takes action to contain the security threat and prevent it from spreading.
- **Remediation:** The security team takes action to remediate the security threat, such as removing malware or patching vulnerabilities.
- **Reporting:** The SOC solution generates reports to provide insights into the security posture of the organization and to help improve future security strategies.

DO NOT REPRINT

© FORTINET

Integration Examples

- Connectors allow playbooks to interact with devices in the Security Fabric and standalone devices
 - They determine which actions can be performed by playbook tasks
- Event handlers generate events when a rule is matched
 - FortiAnalyzer contains many predefined (default) event handlers for many Fortinet devices
 - You can also create your own event handlers

FortiOS connector		
FortiOS Connector		
Training-Lab		
Automation Rule	Automation Action(s)	Parameters
Lab5 webhook disable FW policy	Lab 5 disable firewall policy	policyid
Lab5 webhook enable FW policy	Lab 5 enable firewall policy	policyid

+ Create New Edit Delete Clone More					Search	
	Status	Name	Rules	Events	MITRE Tech ID	
☐		Default-Windows-Registry-Modification-Block...	Rule-1 Windows Registry or File N		T1112	
☐		Default-Web-Server-URL-Scanning-Detected	Rule-1 Web Server Scanning: (Def		T1595.003	
☐		Default-Risky-Destination-Detection-By-Threat	Rule-1 Web request to malicious c Rule-2 Web request to malicious c Rule-3 DNS request to malicious c Rule-4 DNS request to malicious c	33	T1102,T1071.00	

FORTINET
Training Institute

© Fortinet Inc. All Rights Reserved. 14

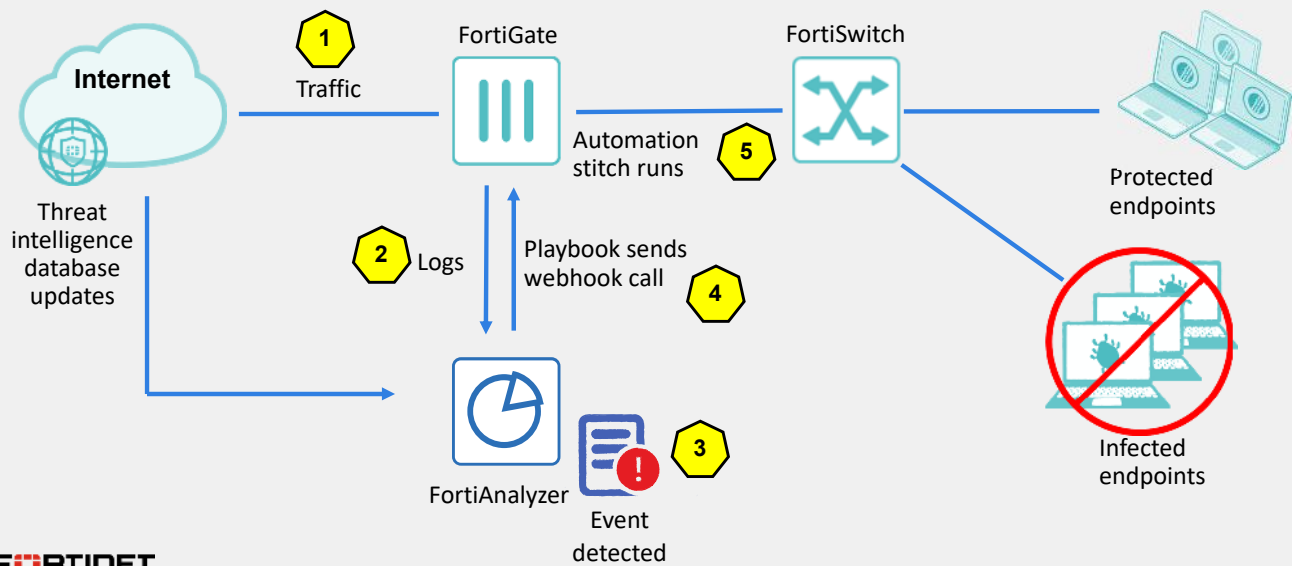
FortiAnalyzer can integrate with other Fortinet products and third-party applications. Connectors determine which automated actions can be performed by playbooks. The available actions will vary depending on the connector type used. Each connector type allows for different actions.

For FortiGate devices, you can also enable the automation stitch configuration in an event handler. When an event is generated by an event handler with automation stitch enabled, FortiAnalyzer sends a notification to the FortiGate automation framework. If an automation stitch is configured on the FortiGate device that corresponds to that FortiAnalyzer event handler, the notification will trigger the related automation stitch and activate an action in response. Some possible actions include FortiGate sending a custom email notification, executing a CLI script, or performing a system action in response to the trigger.

Event handlers generate events when one of their configured rules matches incoming logs on FortiAnalyzer. For example, the event handler can be configured with rules to match IP addresses, ports, or even a generic text string. There are many predefined event handlers for Fortinet devices, such as FortiGate, FortiSandbox, FortiMail, and FortiWeb. In addition to the predefined event handlers, you also have the option to create your own.

DO NOT REPRINT
© FORTINET

An Example of Automation With a Playbook



FORTINET
Training Institute

© Fortinet Inc. All Rights Reserved. 15

This slide shows an example of a playbook being used to automate tasks with FortiAnalyzer and other networking devices:

1. Traffic flows through FortiGate.
2. FortiGate sends logs to FortiAnalyzer.
3. FortiAnalyzer detects some suspicious traffic from the logs and an event handler on FortiAnalyzer generates an event.
4. The event triggers the execution of a playbook in FortiAnalyzer, which sends a webhook call to FortiGate.
5. FortiGate runs the automation stitch with the corrective or preventive actions.

DO NOT REPRINT
© FORTINET

Knowledge Check

1. What determines the possible actions a playbook task can perform?

- A. The event handler
- ✓ B. The connector

DO NOT REPRINT
© FORTINET

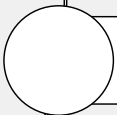
Lesson Progress



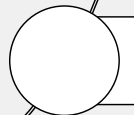
SOC Main Functions and Roles



Fortinet SOC Environment Benefits



Attack Frameworks Overview



Mapping Adversary Behavior

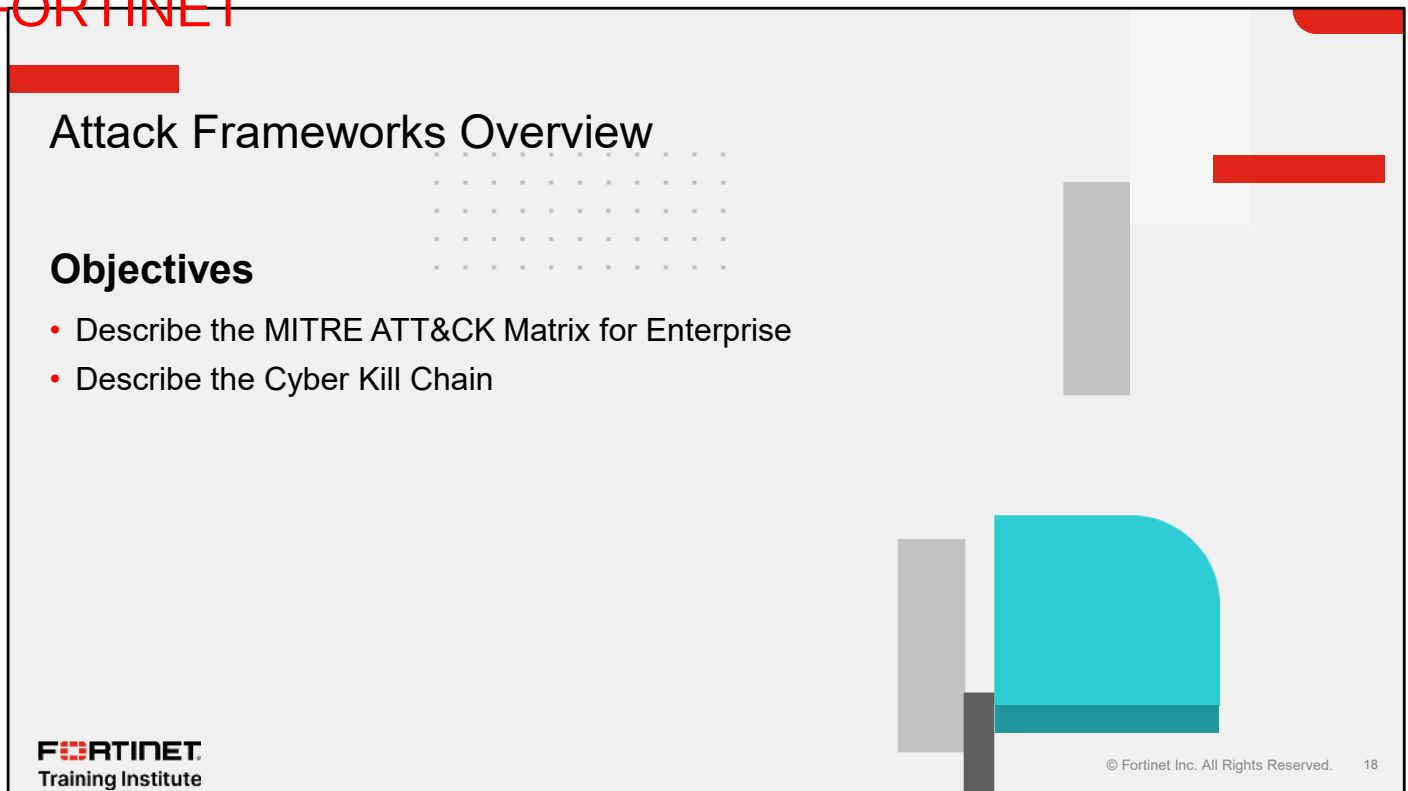


© Fortinet Inc. All Rights Reserved. 17

Good job! You now understand the benefits of the Fortinet SOC.

Now, you will learn about two industry-standard attack frameworks.

DO NOT REPRINT
© FORTINET



Attack Frameworks Overview

Objectives

- Describe the MITRE ATT&CK Matrix for Enterprise
- Describe the Cyber Kill Chain

FORTINET
Training Institute

© Fortinet Inc. All Rights Reserved. 18

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

By demonstrating competence in the industry-standard attack frameworks, you will be able to understand and identify attacks on your network.

MITRE ATT&CK Overview

ATT&CK = Adversarial Tactics, Techniques, and Common Knowledge

- Detailed mapping of adversary behavior framework
- Threat intelligence and adversary emulation use cases
- Guidelines for classifying and describing cyberattacks and intrusions
- 14 tactics categories consisting of "technical objectives" of an adversary
- Categories broken down further into specific techniques and subtechniques
- Created by the [MITRE Corporation](#) in 2013

Reconnaissance 10 techniques	Resource Development 8 techniques	Initial Access 10 techniques	Execution 14 techniques	Persistence 20 techniques	Privilege Escalation 14 techniques
Active Scanning (0/3)	Acquire Access	Content Injection	Cloud Administration Command	Account Manipulation (0/5)	Abuse Elevation Control Mechanism (0/5)
Gather Victim Host Information (0/4)	Acquire Infrastructure (0/8)	Drive-by Compromise	Command and Scripting Interpreter (0/9)	BITS Jobs	Access Token Manipulation (0/5)
Gather Victim Identity Information (0/3)	Compromise Accounts (0/3)	Exploit Public Facing Application	Container Administration Command	Boot or Logon Autostart Execution (0/14)	Account Manipulation (0/6)
Gather Victim Network Information (0/6)	Compromise Infrastructure (0/7)	External Remote Services	Deploy Container	Boot or Logon Initialization Scripts (0/5)	Boot or Logon Autostart Execution (0/14)
Gather Victim Org Information (0/4)	Develop Capabilities (0/4)	Hardware Additions	Exploitation for Client Execution	Browser Extensions	Boot or Logon Initialization
Phishing for Information (0/4)	Establish Accounts (0/3)	Phishing (0/4)	Inter-Process Communication (0/9)	Compromise Client Software Binary	
Search Closed Sources	Obtain Capabilities	Replication Through			

Note: Not all tactics and techniques are shown

What is MITRE ATT&CK?

ATT&CK stands for: Adversarial Tactics, Techniques, and Common Knowledge.

It is a framework that provides a detailed mapping of adversary behavior. It is widely used for threat intelligence and adversary emulation.

MITRE ATT&CK classifies and describes cyberattacks and intrusions through 14 tactics categories, each representing a technical objective of an adversary. Not all tactics are shown on this slide. These categories are further broken down into specific techniques and subtechniques.

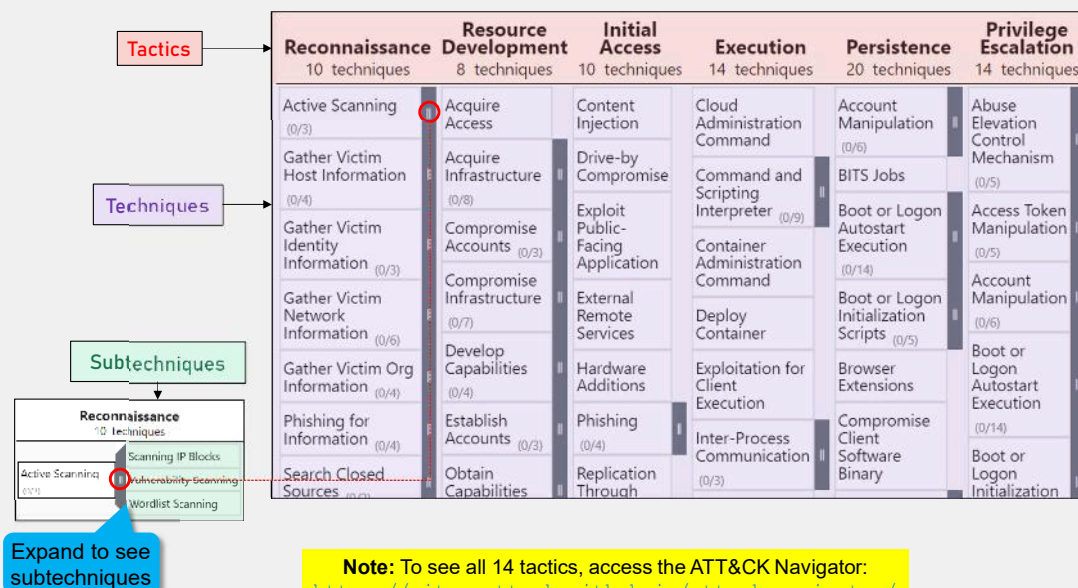
The framework serves as an alternative to the Cyber Kill Chain developed by Lockheed Martin and offers valuable insights for procedure, mitigation, and detection.

One of the main benefits of using MITRE ATT&CK framework is that it makes SOC's more effective. FortiAnalyzer integrates with the MITRE ATT&CK Navigator to provide a comprehensive security solution.

The MITRE ATT&CK Navigator can be used by various members of the SOC team, including security analysts, threat hunters, incident responders, and SOC managers, as a tool for visualizing and mapping observed or potential adversary techniques and tactics to the ATT&CK framework. Using the MITRE ATT&CK Navigator, SOC team members can enhance their understanding of the tactics and techniques used by adversaries, improve threat detection and response capabilities, and align their defensive strategies with industry best practices.

DO NOT REPRINT
© FORTINET

MITRE ATT&CK Overview (Contd)



FORTINET
Training Institute

© Fortinet Inc. All Rights Reserved. 20

Using the matrices, you can identify a tactic, a technique, and potentially, a subtechnique. To view a subtechnique, you must expand a technique that has one or more subtechniques. For example, the Active Scanning technique displays a 0/3 value, which means there are three subtechniques, but currently none are selected.

In the example shown of this slide, all three components are present:

- Tactics: Reconnaissance
- Technique: Active Scanning (T1595)
- subtechnique: Vulnerability Scanning (T1595.002)

Tactics represent the *why* of a technique or subtechnique. They explain what the adversary is trying to accomplish, such as performing reconnaissance. The tactics are not designed to be interpreted as stages or phases, and adversaries do not need to employ all tactics in the framework.

Techniques represent *how* an adversary fulfills their tactical goal by performing an action. For example, they may perform active scanning for reconnaissance. Some techniques may have subtechniques, which are more specific actions that are used to achieve their tactical goal. Furthermore, some techniques may fall under more than one tactic.

MITRE ATT&CK Procedure, Mitigation, and Detection

- Procedure examples include information about known bad actors who use a technique
- Mitigations represent security concepts and classes of technology that may prevent the successful execution of a technique or subtechnique
- Detection covers high-level security concepts and classes of technology that can detect the execution of a technique or subtechnique

Procedure Examples

ID	Name	Description
G0007	APT28	APT28 has performed large-scale scans in an attempt to find vulnerable servers. ^[2]
G0016	APT29	APT29 has conducted widespread scanning of target environments to identify vulnerabilities for exploit. ^[3]

Mitigations

ID	Mitigation	Description
M1056	Pre-compromise	This technique cannot be easily mitigated with preventive controls since it is based on behaviors performed outside of the scope of enterprise defenses and controls. Efforts should focus on minimizing the amount and sensitivity of data available to external parties.

Detection

ID	Data Source	Data Component	Detects
T85029	Network Traffic	Network Traffic Content	Monitor and analyze traffic patterns and packet inspection associated to protocol(s) that do not follow the expected protocol standards and traffic flows (e.g. extraneous packets that do not belong to established flows, gratuitous or anomalous traffic patterns, anomalous syntax, or structure). Consider correlation with process monitoring and command line to detect anomalous processes execution and command line arguments associated to traffic patterns (e.g. monitor anomalies in use of files that do not normally initiate connections for respective protocol(s)).
		Network Traffic Flow	Monitor network data for uncommon data flows. Processes utilizing the network that do not normally have network communication or have never been seen before are suspicious.

Note: Procedure, Mitigation, and Detection examples can be found at: <https://attack.mitre.org/>

Procedures are specific implementations adversaries have used for techniques or subtechniques. They are documented in the MITRE ATT&CK framework based on observation of *in-the-wild* usage and can span multiple techniques and subtechniques. Procedures are very dynamic in nature and difficult to scope in advance because variations can affect coverage capabilities, such as detection and mitigation.

Mitigations represent vendor-agnostic and implementation-agnostic security concepts and classes of technology that can prevent the successful execution of a technique or subtechnique. A mitigation can span several techniques and subtechniques.

Detection covers high-level security concepts and classes of technology that can detect the execution of a technique or subtechnique. In the example on this slide, the recommendation is to use monitoring to analyze network traffic patterns. In other techniques, there may be malicious files involved in the security threat. In general, if the technique or subtechnique is implemented or configured in a way that allows it to remove or quarantine a malicious attachment, it is considered a mitigation (and, most likely, also a detection). If the technique or subtechnique is only alerting but not preventing the delivery of the malicious attachment, it is a detection.

DO NOT REPRINT
© FORTINET

MITRE ATT&CK Framework Matrices in FortiAnalyzer

- Cybersecurity tactics and techniques organized into matrices

Incidents & Events > MITRE ATT&CK > Attack

Reconnaissance	Resource Development	Initial Access
10 techniques	8 techniques	9 techniques
Active Scanning ✔ Covered	Acquire Access	Drive-by Compromise
Gather Victim Host Information ✔ Covered	Acquire Infrastructure ✔ Covered	Exploit Public-Facing Application ✔ Covered
Gather Victim Identity Information	Compromise Accounts	External Remote Services
Gather Victim Network Information	Compromise Infrastructure 📅 9	Hardware Additions

The column headers are the tactics

The tiles under the columns are the techniques

Click a tile to see associated incidents and events

Incidents & Events > MITRE ATT&CK > Coverage

110 Event Handlers - 41% Coverage

Reconnaissance	Resource Development	Initial Access
10 techniques	8 techniques	9 techniques
Active Scanning 📅 3	Acquire Access	Drive-by Compromise
Gather Victim Host Information 📅 1	Acquire Infrastructure 📅 1	Exploit Public-Facing Application 📅 3
Gather Victim Identity Information	Compromise Accounts	External Remote Services
Gather Victim Network Information	Compromise Infrastructure 📅 8	Hardware Additions
	Develop	

Click a tile to see which event handlers have coverage against the technique or subtechnique

Note: Not all tactics and techniques are shown

FORTINET
Training Institute

© Fortinet Inc. All Rights Reserved. 22

The **MITRE ATT&CK** and **MITRE ATT&CK ICS** pages on FortiAnalyzer are based on the MITRE ATT&CK framework matrices.

The column headers are the tactics in the matrices. They describe the adversary's goal or objective—such as performing reconnaissance—when they use techniques on your network.

The tiles in the columns are the techniques in the matrices. They describe how an adversary can achieve their objective in your network, such as using active scanning to perform reconnaissance.

You can review the incidents and events associated with a technique, such as the severity, information on the technique and subtechnique, affected endpoints, and the total number of incidents and events. For example, the **Compromise Infrastructure** tile has nine associated events.

You can review event handler coverage on the **Coverage** section. It will show you the number of event handlers and the percentage of coverage that FortiAnalyzer has against attacks in the matrices. The number on each tile shows how many event handlers are associated with that technique. For example, the **Compromise Infrastructure** tile has eight associated event handlers. You can click a tile to view the list of event handlers related to that technique.

To leverage the MITRE ATT&CK ICS matrix, which is not depicted on this slide, the OT Security Service license is required on FortiAnalyzer.

DO NOT REPRINT
© FORTINET

Cyber Kill Chain Overview

- Framework developed by Lockheed Martin
- Identifies what adversaries have to complete in order to achieve their objectives on a target
- Derived from a military concept called kill chain
- Provide visibility and understanding of sophisticated attacks and attacker's tactics, techniques, and procedures
- Consists of seven steps that represent stages of advanced persistent threats (APT)

Reconnaissance	Gather information about the target
Weaponization	Use the gathered information to embed malware
Delivery	Transmission of the malware
Exploitation	Target system vulnerability
Installation	Malware is installed
Command & Control	Connection to an outside server is established
Actions on Objective	Attack on the network commences

FORTINET
 Training Institute

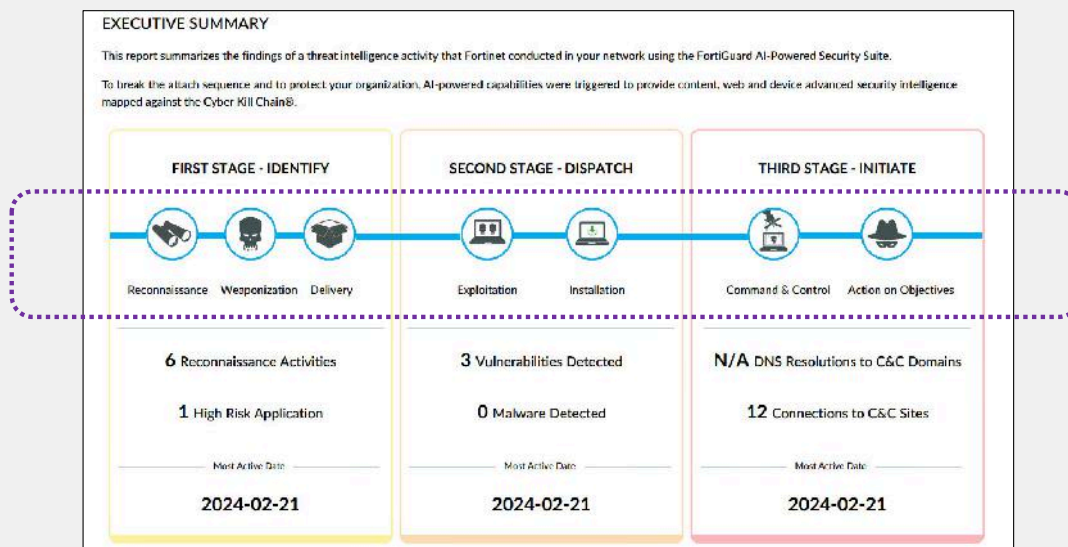
© Fortinet Inc. All Rights Reserved. 23

The Cyber Kill Chain is frequently referenced as a standard framework that provides a high-level description of adversary activities during advanced and persistent attacks. The Cyber Kill Chain conveys important high-level concepts in a way that is digestible for non-technical audiences, but it lacks the level of detail required when you need to drill down to the more technical aspects of adversary activity.

DO NOT REPRINT
© FORTINET

Cyber Kill Chain in FortiAnalyzer

- In FortiAnalyzer, the predefined threat report is mapped to the Cyber Kill Chain stages for correlation and pattern identification



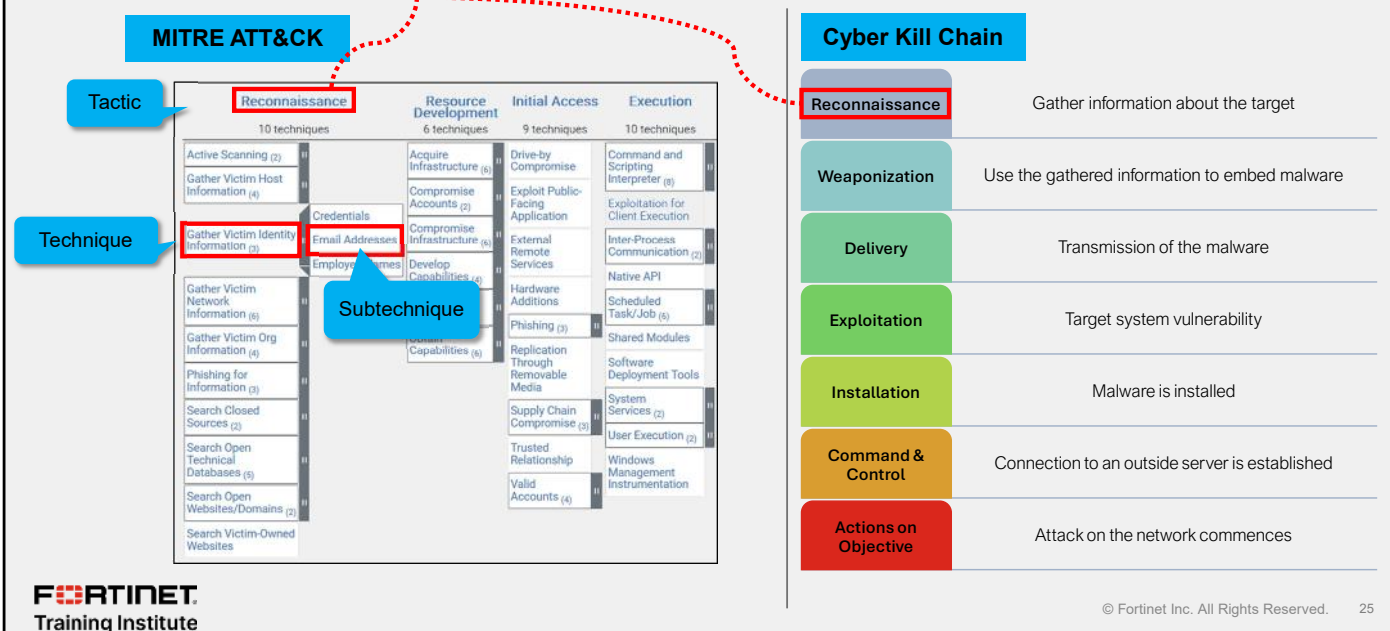
FORTINET
Training Institute

© Fortinet Inc. All Rights Reserved. 24

This slide shows part of a generated threat report, which is a predefined report included with FortiAnalyzer. This report maps the findings in the FortiAnalyzer report to stages of the Cyber Kill Chain. In this example report, FortiAnalyzer has identified potential security breaches and mapped suspicious network traffic to corresponding steps in the Cyber Kill Chain, such as reconnaissance activities; the use of risky, possibly weaponized applications; detected vulnerabilities that could be exploited; and connections to command-and-control server (C&C) sites.

Adversary Behavior—MITRE ATT&CK vs. Cyber Kill Chain

Scenario: Group ABC initially *probes* the potential target's email systems in search of valid email accounts



The MITRE ATT&CK model offers a comprehensive and detailed information about adversary behavior, enabling organizations to improve their defenses and incident response capabilities. The Cyber Kill Chain model provides a structured approach to identifying and disrupting attacks at different stages. Organizations often use aspects of both models, integrating them into their cybersecurity strategies to gain a more holistic view of threats and develop effective defensive measures.

MITRE ATT&CK model:

1. **Focus:** The model primarily focuses on documenting and categorizing adversary tactics, techniques, and procedures (TTPs) observed in real-world cyber attacks.
2. **Granularity:** It provides a highly granular and detailed view of adversary behavior, describing specific actions and techniques used throughout different stages of an attack.
3. **Coverage:** It covers a wide range of tactics and techniques across different platforms and attack vectors, offering a comprehensive view of adversary behavior.
4. **Application:** It is commonly used for threat intelligence, red teaming, and blue teaming activities. It helps organizations understand and simulate adversary behavior, assess their defenses, and improve their incident response capabilities.

Cyber Kill Chain model:

1. **Focus:** Focuses on the stages or phases of a cyber attack from initial reconnaissance to post-exploitation activities.
2. **Lifecycle perspective:** It provides a structured, step-by-step representation of an attacker's activities, aiming to identify and disrupt each stage of an attack.
3. **Sequential approach:** It follows a linear progression, emphasizing the sequential order of an attack's stages.
4. **Application:** It is commonly used for incident response, security operations, and vulnerability management. It helps organizations detect, respond to, and prevent cyber attacks by understanding an attacker's likely progression and targeting specific stages.

DO NOT REPRINT
© FORTINET

Knowledge Check

1. Which model or framework allows for a more detailed mapping of adversary behavior?
✓ A. MITRE ATT&CK
B. Lockheed Martin's Cyber Kill Chain
2. Which one is a MITRE ATT&CK tactic?
✓ A. Initial access
B. Exploitation

DO NOT REPRINT
© FORTINET

Lesson Progress



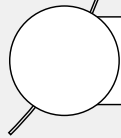
SOC Main Functions and Roles



Fortinet SOC Environment Benefits



Attack Frameworks Overview



Mapping Adversary Behavior

FORTINET
Training Institute

© Fortinet Inc. All Rights Reserved. 27

Good job! You now understand the attack frameworks.

Now, you will learn about mapping adversary behavior.

DO NOT REPRINT
© FORTINET

Mapping Adversary Behavior

Objectives

- Review a simulated attack
- Understand how to use the ATT&CK Navigator

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

By demonstrating competence in using the MITRE ATT&CK Navigator to map adversary behavior during a simulated attack, you will acquire the knowledge and expertise necessary to map adversary behavior when confronted with real-world cybersecurity threats.

Mapping Adversary Behavior

- Understanding adversary behavior is a crucial step in protecting your network and data
- Ask these two questions:
 - *Why?* What is the technical goal (*tactic*) of the threat actor?
 - *How?* What actions (*technique* or *subtechnique*) is the threat actor taking to achieve their goal?
- The more you understand the techniques and the tools bad actors use, the more effective you will be when formulating your strategy against threats
- In this section, you will review a use case to learn how to map adversary behavior to a mock report

Understanding adversary behavior is essential to safeguarding your organization from threat actors. It involves trying to anticipate the *why* and the *how* of the threat actors. For example, the technical goal of an adversary is to obtain initial access. In order to achieve their goal, they perform phishing by propagating a malicious link to users through email. After the phishing attempt is successful, the attacker may move on to their next goal, such as gaining privileged access on the network.

When trying to map adversary behavior, it is important that you avoid jumping to a conclusion without first performing a thorough evaluation. For example, you may see a technique that corresponds to multiple tactics, but you need to evaluate if all of them apply to your scenario. It is also important to not let biases impact your mapping, such as assuming that the most well-known or commonly seen exploit is the culprit.

Sources and references:

"Best Practices for MITRE ATT&CK® Mapping", Cybersecurity & Infrastructure Security Agency, 2023. Available online at <https://www.cisa.gov/sites/default/files/2023-01/Best%20Practices%20for%20MITRE%20ATTCK%20Mapping.pdf>

DO NOT REPRINT
© FORTINET

Use Case—Healthcare Sector



Cybercriminals are attempting to use a phishing attack to hold private data from your organization, a hospital, for ransom.

Threat: Potential breach exposing thousands of patients' data and putting patients at risk

Your goal: Prevent your computer systems from breaking down, prevent data from being compromised, and avoid disaster

Domain: Enterprise

Attacker: Group ABC

One effective way to show how adversary behavior mapping works is by using a use case. In this scenario, your organization, a hospital, is under threat by a fictional adversary, Group ABC. This group seeks to infiltrate your security with the goal of stealing private patient information.

You will use this mock scenario to learn how to map adversary behavior. When you complete the associated labs, you will have an opportunity to put what you learned from this lesson and use case into practice.

Mock Security Threat Report



This threat report describes a simulated attack by the fictional **Group ABC**. You will use this report to map the behavior.

This report builds upon threat research information that describes observed tactics, techniques, and procedures associated with Group ABC.

“Group ABC initially *performs passive reconnaissance to gather information about their target*, such as researching the employees and downloading publicly available files hosted on their corporate website. Group ABC then *probes their potential target's email systems in search of valid email accounts*, most likely based on lists of common usernames. Once they confirm valid email addresses on the target organization, Group ABC starts a *spearphishing* campaign against select users. The following are some common characteristics found in similar campaigns:

- a) The *spearphishing* emails usually contain an *attached malicious macro-enabled document*.
- b) Group ABC usually tries to leverage potential hierarchy or power relationships to *lure targets into downloading and opening malicious files*. They couple this with email content that conveys a sense of urgency, familiarity and/or penalties to the *email recipient* if they do not act immediately and as the message advises. Group ABC commonly sends the email to accounts that potentially belong to system administrators, management, HR, and so on.
- c) Group ABC generates *a new version of the malicious artifact* for each campaign, in order to prevent static detection based on file hash. However, the files look the same in terms of content and they all include malware identified in *CVE-2018-16858*.

This slide introduces a mock threat report, generated by FortiRecon, about Group ABC. As you read this mock report, pay close attention to the italicized text, which will help you map adversary behavior later. Observe that key verbs, such as “execute” and “probe”, have a strong correlation to the MITRE ATT&CK framework tactics.

This report describes some key elements that you, as part of the purple team, will use to build the mapping of their behavior using the MITRE ATT&CK Matrix for Enterprise.

DO NOT REPRINT
© FORTINET

Mock Security Threat Report (Contd)

After execution, the malware *establishes a reverse TCP control channel with a C&C server*. The channel uses TCP port 443 in order to evade basic security controls that may block communication to nonstandard ports on the internet.

After establishing initial access through *spearphishing* and malicious file execution, Group ABC uses a dropper to *install a new service on the target system*. *This process establishes persistence of the C&C channel*, even when the initially compromised host restarts.

After establishing persistence, Group ABC *tries to clear the security audit log* on the compromised target in order to *evade detection*.

With a persistent connection to the network, Group ABC will try to discover high priority targets using *active reconnaissance* and *moving laterally on the network to those targets*. They will use *dictionary attacks to discover credentials*.

After this initial setup, Group ABC *proceeds to exfiltrate confidential data that can be sold or ransomed*.



FORTINET
Training Institute



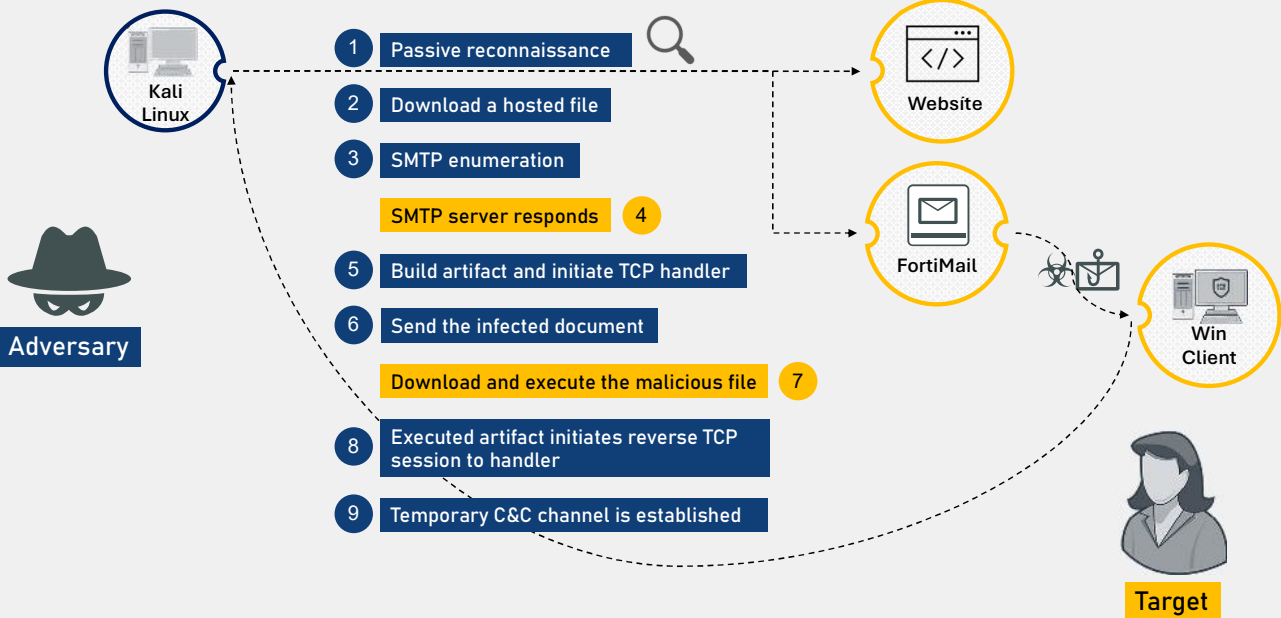
The *purple* team analyzes the threat report and identifies the key elements to build a mapping of Group ABC's behavior using the MITRE ATT&CK for Enterprise matrix

© Fortinet Inc. All Rights Reserved. 32

This slide continues the threat report on Group ABC.

DO NOT REPRINT
© FORTINET

Adversary Attack Flow—Exploitation Phase



FORTINET
Training Institute

© Fortinet Inc. All Rights Reserved. 33

This slide describes the exploitation phase of the adversary attack flow that you will execute during one of the lab exercises in this course. The attacking duties are handled by the red team, which aims to use the attack simulation to find holes in the organization's defenses. With the vulnerabilities discovered from the attack, the red team can work with the purple team to share knowledge with the blue team and improve the organization's security posture.

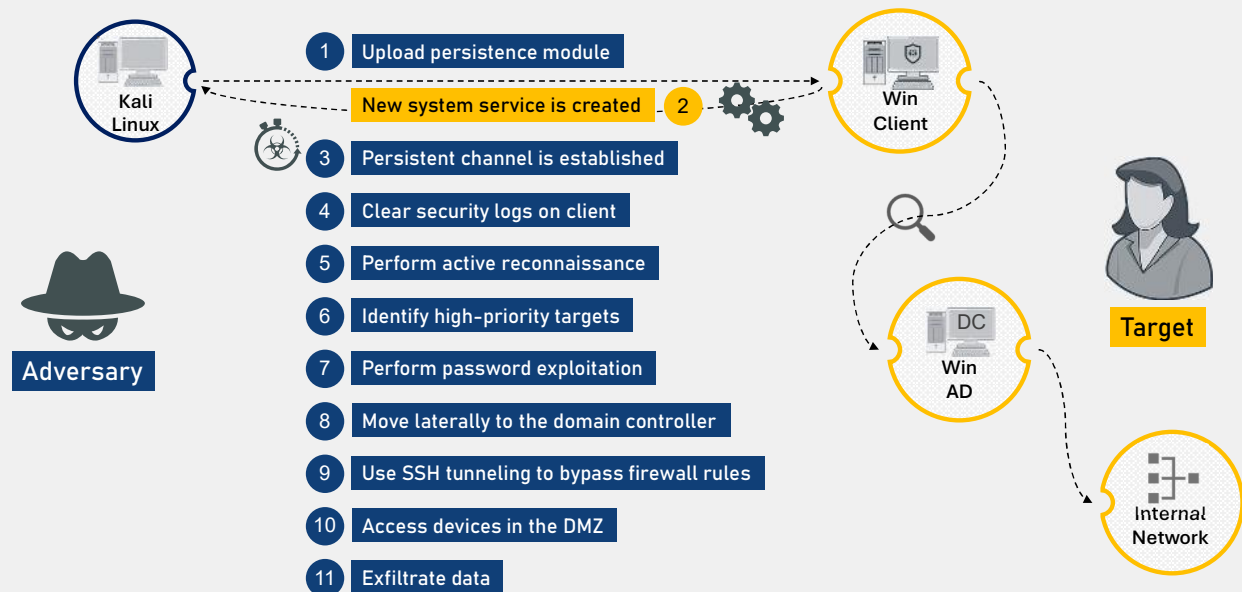
First, the adversary performs passive reconnaissance to gather information about the target. They collect information such as employee names, roles, background information, and more. They will also download a publicly-hosted document on the target's corporate website, to be used later as an attack vector. Next, the adversary uses SMTP enumeration to confirm valid email accounts, and then the target SMTP server responds.

The adversary builds a malicious payload, an infected document masquerading as a legitimate document downloaded earlier, and initiates a TCP handler. The infected document is sent back to the target, who then downloads and executes it. The executed artifact initiates a reverse TCP session to the listening handler, which creates a temporary C&C channel.

You will learn more about these topics in Lesson 6, *Attack Surface and Vectors*.

DO NOT REPRINT
© FORTINET

Adversary Attack Flow—Post-Exploitation Phase



FORTINET
Training Institute

© Fortinet Inc. All Rights Reserved. 34

This slide describes the post-exploitation phase of the adversary attack flow that you will execute during one of the lab exercises in this course. Post-exploitation refers to actions that are conducted after the adversary gains initial access to the compromised host.

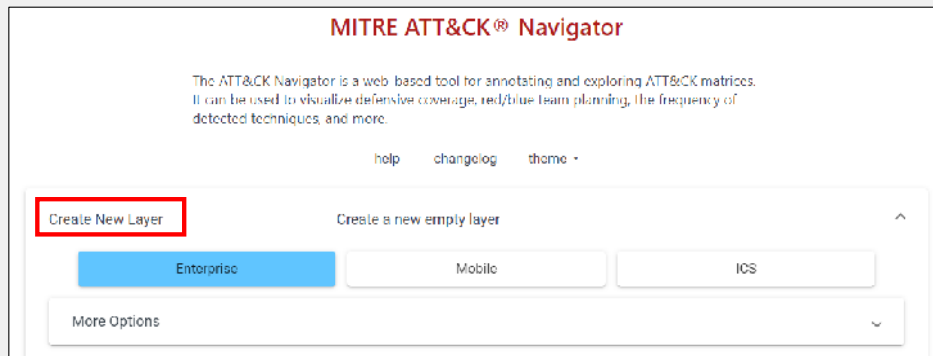
First, the adversary initiates a persistence artifact transfer through the temporary channel, which creates a new system process on the compromised host. The new process establishes a second reverse TCP session to the handler, which persists across reboots. Next, the adversary removes an indicator of compromise by deleting security logs that include the new service's creation.

The attacker then performs active reconnaissance using a mix of techniques, including port scanning and IP discovery, to find high-priority targets. The identified target is a domain controller, which the attacker will access using RDP by exploiting compromised passwords. Next, they will use SSH tunneling to bypass firewall rules that prevent LAN devices from accessing the DMZ. They will be able to gain access to crucial network infrastructure. Finally, the attacker will exfiltrate a sensitive file stored on the domain controller and achieve their objective.

You will learn more about these topics in Lesson 6, *Attack Surface and Vectors*.

Using the MITRE ATT&CK Navigator

- You can access the MITRE ATT&CK Navigator here:
<https://mitre-attack.github.io/attack-navigator/>
- There are three matrices:
 - Enterprise, Mobile, and Industrial Control System (ICS)
 - They offer different tactics, techniques, and subtechniques
- Click **Create New Layer** to select the matrix type

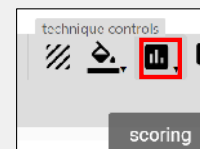
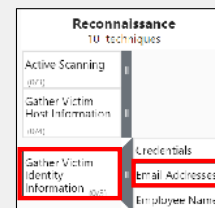


You can use the MITRE ATT&CK Navigator to map adversary behavior. It allows you to visualize the MITRE ATT&CK matrices and select tactics, techniques, and subtechniques. You can access the MITRE ATT&CK Navigator using the URL on this slide.

You can create a new layer, and select the **Enterprise**, **Mobile**, or **ICS** matrix. The enterprise option focuses more on traditional IT environments, the mobile option focuses more on mobile devices, and the ICS option focuses more on industrial environments and operational technologies. This course focuses on the enterprise option.

Using the MITRE ATT&CK Navigator (Contd)

- As an example, using information from the mock report, you can create a mapping:
 - Such as selecting the **Gather Victim Identity Information** technique, and the **Email Addresses** subtechnique
- You can also use the **scoring menu** in the top right-hand corner of the navigator by providing the techniques and subtechniques a score value
 - This will highlight the entries and make your mapping easier to read

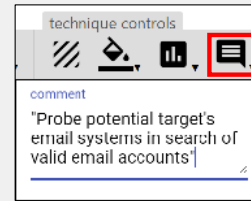


Using information from the mock report as an example, you can create a mapping. The mock report contains information about how Group ABC probes for email addresses, and then initiates a spearphishing campaign.

In the sample mapping shown on this slide, you can observe the **Gather Victim Identity Information** technique, **Email Addresses** subtechnique, and scoring options.

Using the MITRE ATT&CK Navigator (Contd)

- You can also add comments using the icon in the upper-right of the navigator
 - Use comments to detail the adversary procedures
- The example comment is listed under the **Email Addresses** subtechnique



Reconnaissance 10 techniques	Resource Development 7 techniques	Initial Actions 9 techniques
Active Scanning (0/3)	Acquire Infrastructure (0/6)	Drive-by Compromise
Gather Victim Host Information (0/4)	Compromise Accounts (0/2)	Exploit Facing Applications
Gather Victim Identity Information (1/3)	Compromise Email Addresses (1/589,002)	Extort Services
	Employee Names	Harvest Additions
Gather Victim Network Information (0/6)	Establish potential target's email systems in search of valid accounts	Phishing Through
Gather Victim Org Information (0/4)	Obtain email accounts	Reputation
Phishing for		

An important component of the MITRE ATT&CK framework are the adversary procedures.

The ATT&CK Navigator does not have a specific object to map procedures, but you can use the comment section of the subtechnique to annotate the Group ABC procedure that correspond to each tactic and technique.

For example, you can type in a pertinent comment in the mock report related to how Group ABC probed the email system of their potential targets in search of valid email accounts. In a real-world situation, you should collect and document as many details as possible about an adversary, so adding comments about procedures for every technique is recommended.

DO NOT REPRINT
© FORTINET

Example Mapping



The purple team identified the following information from the mock report:

Group ABC first performs a **Reconnaissance** (tactic) by using a list of common usernames to probe the target's email systems, in order to **Gather Victim Identity Information** (technique) and obtain **Valid Email Addresses** (subtechnique) existing on the target.

Report Phrase	Tactic	Technique	Subtechnique	Navigator Interface
"probe potential target's email systems in search of valid email accounts,"	Reconnaissance	Gather Victim Identity Information	Email Addresses	

The result of a mapping

FORTINET
Training Institute

© Fortinet Inc. All Rights Reserved. 38

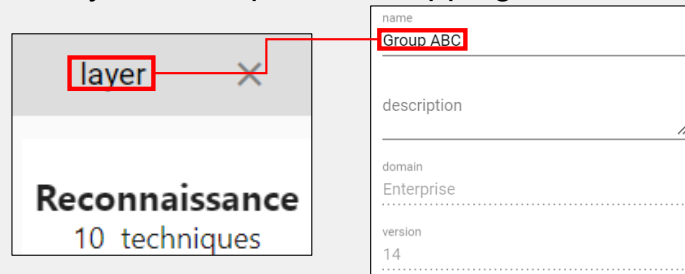
This slide shows an example from the mock report, to map the tactics, techniques, and procedures (TTPs) of Group ABC's attempt to compromise an email account.

As a member of the purple team, you will need to analyze a threat report, identify key elements, and use them to build a mapping of adversary behavior using the MITRE ATT&CK Navigator. Use the high-level steps on this slide to visualize the requirements you will need to complete a mapping.

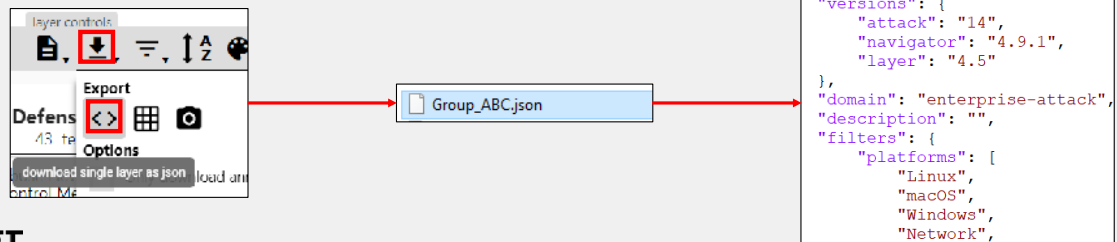
You will map out numerous TTPs in the lab exercises in this course.

Saving and Exporting the Mapping

- You can rename the layer and export the mapping for future use



- You can also download the mapping and send your findings to other SOC members as a JSON file



You can save your mapping, export it, and then send it to your entire SOC team to provide structured insight into an adversary's behavior.

When you save a mapping, be sure to give it a meaningful name. You can also download a mapping and save it as a JSON file. This allows you to have a backup that you can import into the navigator later, if needed.

You also have the options to export a mapping as an Excel file or an SVG file.

DO NOT REPRINT
© FORTINET

Knowledge Check

1. What is reconnaissance in the MITRE ATT&CK framework?

- A. It is a technique.
- B. It is a subtechnique.
- ✓ C. It is a tactic.

2. Which is considered a post-exploitation activity?

- A. Preparing a malicious payload
- ✓ B. Establishing persistence
- C. Sending a phishing email

DO NOT REPRINT
© FORTINET

Lesson Progress



SOC Main Functions and Roles



Fortinet SOC Environment Benefits



Attack Frameworks Overview



Mapping Adversary Behavior



© Fortinet Inc. All Rights Reserved. 41

Congratulations! You have completed this lesson.

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

DO NOT REPRINT
© FORTINET

Review

- ✓ Describe the main functions and roles within a SOC
- ✓ Identify the main challenges within a SOC
- ✓ Identify the challenges that can be solved by the Fortinet SOC
- ✓ Describe the MITRE ATT&CK Matrix for Enterprise
- ✓ Describe the Cyber Kill Chain
- ✓ Review a simulated attack
- ✓ Use the ATT&CK Navigator

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

By mastering the objectives covered in this lesson, you learned what a SOC is, what challenges can be solved by the Fortinet SOC, what industry-standard attack frameworks are, and how to map adversary behavior.

DO NOT REPRINT
© FORTINET

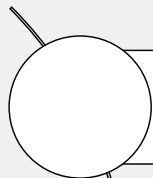


In this lesson, you will learn about the key features and concepts of FortiAnalyzer, including administrative domains (ADOMs), operation modes, and the FortiAnalyzer Fabric.

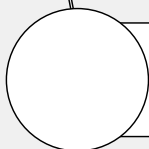
FortiAnalyzer integrates logging, analytics, and reporting into one system, so you can quickly identify and react to network security threats.

DO NOT REPRINT
© FORTINET

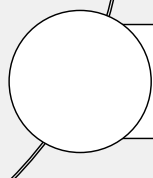
Lesson Overview



FortiAnalyzer Architecture



Operation Modes



FortiAnalyzer Fabric



© Fortinet Inc. All Rights Reserved. 2

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

DO NOT REPRINT
© FORTINET

FortiAnalyzer Architecture

Objectives

- Describe the purpose of FortiAnalyzer in a SOC
- Describe administrative domains (ADOMs)

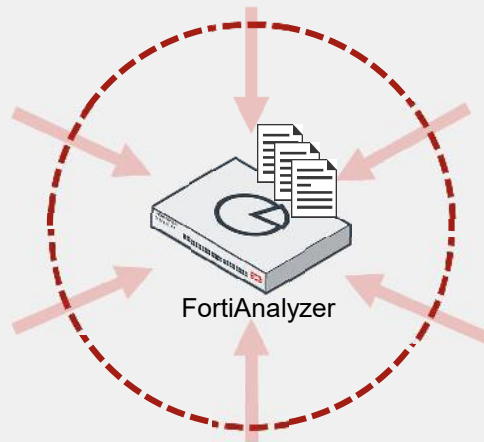
After completing this section, you should be able to achieve the objectives shown on this slide.

By demonstrating a competent understanding of FortiAnalyzer key features and concepts, you will be able to use the device effectively in your own network.

DO NOT REPRINT
© FORTINET

Centralized Log Repository

- FortiAnalyzer aggregates log data from one or more Fortinet devices
- Single view of security events taking place on a range of devices



Supported devices:

- FortiGate/FortiCarrier
- FortiAnalyzer
- FortiAuthenticator
- FortiCache
- FortiClient
- FortiDDoS
- FortiMail
- FortiManager
- FortiNAC
- FortiSandbox
- FortiWeb
- Syslog
- Chassis

Note: The list is not exhaustive

FORTINET
Training Institute

© Fortinet Inc. All Rights Reserved. 4

FortiAnalyzer aggregates log data from one or more Fortinet devices, thereby acting as a centralized log repository. Log aggregation provides a single channel for accessing your complete network data, so you don't need to access multiple devices, several times a day.

FortiAnalyzer can be integrated with many different Fortinet solutions. For a complete list, refer to the release notes at docs.fortinet.com.

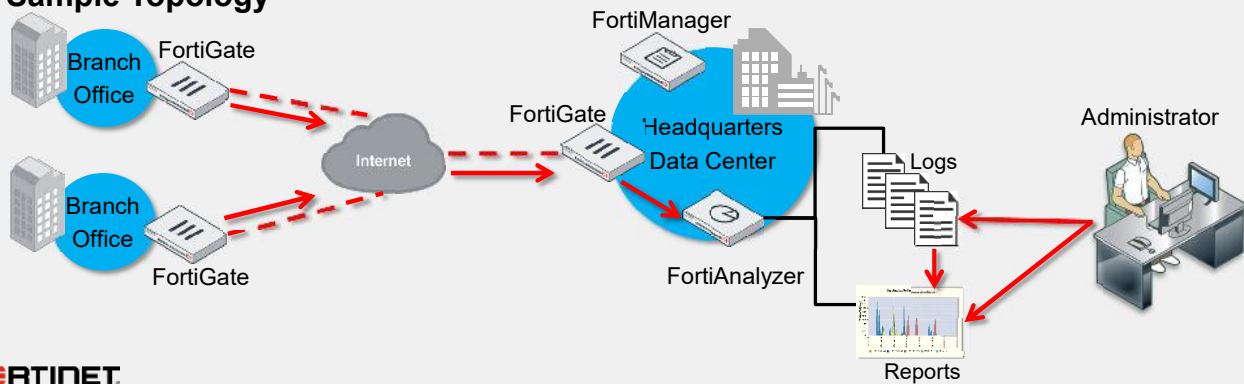
DO NOT REPRINT
© FORTINET

Centralized Log Repository (Contd)

Workflow

1. Registered devices send logs to FortiAnalyzer
2. FortiAnalyzer buffers, reorganizes, and stores the logs
3. Administrators:
 - View and search the logs
 - Configure, request, and view reports (based on log data)

Sample Topology



FORTINET
Training Institute

© Fortinet Inc. All Rights Reserved. 5

The logging and reporting workflow operates as follows:

1. Registered devices send logs to FortiAnalyzer.
2. FortiAnalyzer collates and stores those logs in a way that is easy to search and run reports.
3. Administrators can connect to FortiAnalyzer using the GUI to view the logs manually or generate reports to view the data. You can also use the CLI to perform administrative tasks.

You can easily integrate FortiAnalyzer into a network, even if there are multiple sites. A sample topology can include multiple branches and a headquarters. Each location's firewall is added into FortiAnalyzer, and the administrator can view logs and generate reports for the entire network, from a single interface.

Reports, Events, and Content Archiving

- **Reports**

- Network-wide reporting of device events, activities, and trends
- Archived, filtered, and mined for compliance or historical analysis purposes

- **Events**

- Identify and react to security threats quickly when configured conditions are met
- View events through **Event Monitor** (on the GUI), email, SNMP, or syslog
- Events that require further investigation can be used to generate new incidents

- **Content archiving**

- Simultaneously logs and archives full or summary copies of content transmitted over the network (email, FTP, NNTP, and web traffic)
- Typically used to prevent sensitive information from leaving your network

Some key features of FortiAnalyzer include reporting, alert generation, and content archiving.

FortiAnalyzer reports provide a clear picture of network events, activities, and trends occurring on supported devices. The reports collate information in logs so that you can interpret the information and, if necessary, take any required actions. You can archive and filter the network knowledge you glean from these reports, as well as mine it for compliance or historical analysis purposes.

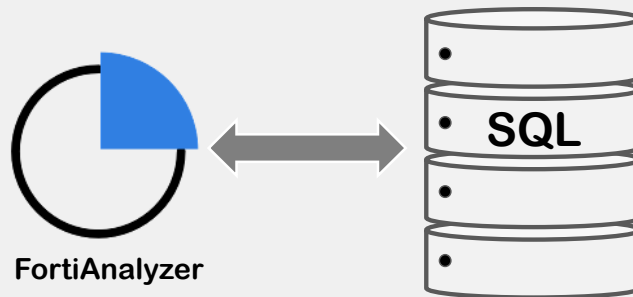
Monitoring your network around the clock is not realistic. FortiAnalyzer events provide you with a way to see and quickly react to threats, without having to constantly keep watch on your network. FortiAnalyzer can generate events when specific conditions in the logs are met—conditions you configure FortiAnalyzer to monitor for registered devices. You can view these events on the GUI, and you can also send them to multiple recipients by email, SNMP, or syslog. You can escalate events that require investigation into incidents.

Content archiving provides you with a way to simultaneously log and archive full or summary copies of the content transmitted over the network. You can use content archiving to prevent sensitive information from leaving your organization's network. You can also use it to record network use. The data loss prevention (DLP) engine can examine email, File Transfer Protocol (FTP), Network New Transfer Protocol (NNTP), and web traffic, but you must configure the archive setting for each rule in a DLP sensor on FortiGate, so you can specify what you want to archive.

DO NOT REPRINT
© FORTINET

Database Language Support

- FortiAnalyzer supports Structured Query Language (SQL) for logging and reporting
- FortiAnalyzer inserts log data into the SQL database for log view and report generation
- FortiAnalyzer uses a PostgreSQL database
- *Advanced reporting capabilities require some knowledge of SQL and databases*



SQL is the database language that FortiAnalyzer uses for logging and reporting.

Advanced reporting capabilities require some knowledge of SQL and databases. For example, you may need to compose custom SQL queries, known as datasets, to extract the data you require from the database.

DO NOT REPRINT
© FORTINET

ADOMs

- ADOMs group devices for administrators to monitor and manage
 - One or more devices are assigned to ADOMs and administrators are assigned to administer one or more ADOMs
- Purpose:
 - To divide administration of devices and restrict access
 - VDOMs, a feature of FortiGate, further restrict access
 - To more efficiently manage data policies and disk space allocation
 - Set for each ADOM (not for each device)

ADOMs are not enabled by default

Dashboard > System Information

System Information		
Host Name	FAZ-SiteB	
Serial Number	FAZ-VM1M24000908	
Platform Type	FAZVM64	
HA Status	Standalone	
System Time	Thu Sep 12 16:02:53 2024 PDT	
Firmware Version	v7.4.3-build2487 240514 (CA)	
System Configuration	Last Backup: Wed Jun 12 14:30:52 2024	
Current Administrators	admin / 1 in total	
Up Time	1 day 2 hours 47 minutes 16 seconds	
Administrative Domain	☐	
Operation Mode	Analyzer Collector	

```
# config system global
  set adom-status {enable | disable}
end
```

FORTINET
Training Institute

© Fortinet Inc. All Rights Reserved. 8

ADOMs allow you to group devices for management and monitoring. For example, administrators can manage devices that are grouped based on their geographical location or business division.

The purpose of ADOMs is to:

- Divide the administration of devices by ADOM and to control (restrict) administrator access. If your network uses VDOMs, ADOMs can further restrict access to data that comes from the VDOM of a specific device.
- Make the management of data policies and disk space allocation, which are set per ADOM, more efficient.

ADOMs are not enabled by default and can be configured only by the default admin administrator (or an administrator with the Super_User profile).

All Fortinet devices included in a Security Fabric can be placed into an ADOM of the Fabric type, allowing for fast data processing and log correlation.

DO NOT REPRINT
© FORTINET

Logging Interface Overview

The screenshot shows the FortiAnalyzer Logging Interface Overview. The main table displays log entries with columns: Date/Time, Device ID, Action, Source, Destination IP, Service, Application, and Sent/Received. The table is filtered for 'All Devices' and 'Last 7 Days' (Aug 09 To Aug 16). Callouts highlight the following features:

- Set filters:** A red box highlights the filter icon in the top left of the table.
- Set device and time frame:** A blue box highlights the 'All Devices' and 'Last 7 Days' dropdowns.
- Custom view:** A blue box highlights the 'Custom view' button in the top right.
- Column options:** A blue box highlights the 'Column options' button in the top right.
- Toggle real-time/historical logs:** A blue box highlights the 'Toggle real-time/historical logs' button in the top right.
- Toggle raw or formatted logs:** A blue box highlights the 'Toggle raw or formatted logs' button in the top right.
- Log details:** A blue box highlights the 'Log details' button in the bottom right.

The right pane shows details for a selected log entry, including Session ID, Transaction ID, Virtual Domain, Device ID, Device Name, Source Country, Source IP, Source Interface, Source Interface Role, Source Port, UEBA Endpoint ID, UEBA User ID, Destination, Destination Country, Destination End User ID, Destination Endpoint ID, Destination IP, Destination Interface, Destination Interface Role, Destination Port, Action, Policy ID, Application, Application Category, Protocol, Service, Duration, Downloaded Packets, and Upload Packets.

FORTINET Training Institute

© Fortinet Inc. All Rights Reserved. 9

As a SOC analyst, you will need to perform frequent searches within the usually large number of logs received. FortiAnalyzer makes it very easy to search based on any of the fields included in the logs.

To search for specific logs in **Log View**, select the device and log type, and then set the appropriate filters.

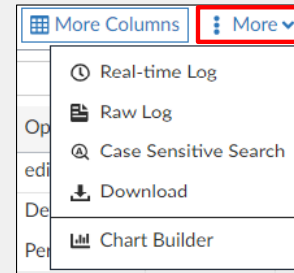
You can create filters based on any of the available values. For example, a filter for a specific device within the ADOM and a limited time frame.

You can also save a custom view, add or remove columns, and view logs in real time or historically, or as raw or formatted logs.

To view more information about a log, double-click the log entry. The details pane appears on the right side of the screen.

Tools

- Toggle between **formatted/raw** logs
 - Formatted logs are sortable and columns can be customized
 - Raw logs are more difficult to read, but can be useful in providing syntax guidance
- Toggle between **historical/real-time** logs
 - View historical logs with the option to specify a time period
 - Real-time logs are shown as they come in, but you can pause them
- Enable/disable case-sensitive search
- Download logs based on the current filters



Formatted

#	↓Date/Time	Device ID	Action	Source	Destination IP
4	14:59:50	FGVM010000064692	✓accept	10.200.1.1	10.208.91.112.60
5	14:59:40	FGVM010000064692	✓accept	10.200.1.1	10.208.91.112.61
6	14:59:30	FGVM010000064692	✓accept	10.0.1.200	10.208.91.112.60
7	14:59:30	FGVM010000064692	✓accept	10.0.1.200	10.208.91.112.63

Raw

```
date=2023-08-16 time=14:59:24 id=7268043151217000450 itime=2023-08-16 14:59:25 euid=3 epid=104
dsteuid=3 dstepid=101 type=traffic subtype=local level=notice action=accept policyid=0 sessionid=89571
srcip=10.0.1.200 dstip=208.91.112.60 srcport=123 dstport=123 transid=noop duration=183 proto=17
sentbyte=76 rcvbyte=76 sentpkt=1 rcvpkt=1 logid=0001000014 service=NTP app=NTP appcat=unscanned
srcintfrole=undefined dstintfrole=undefined eventtime=1692223164328415424 srccountry=Reserved
dstcountry=Canada srcintf=root dstintf=port1 tz=-0700 devid=FGVM010000077646 vd=root
dtime=2023-08-16 14:59:24 itime_t=1692223165
```

The **More** drop-down list provides tools for viewing, searching, and downloading your logs.

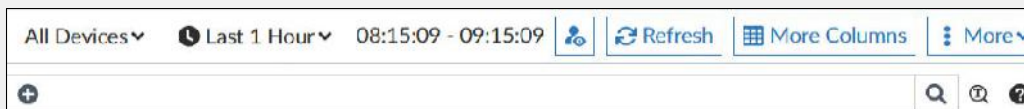
You can toggle between formatted and raw logs on the GUI. You can sort formatted logs and customize the columns to meet your requirements. You can show only the data you are looking for and omit the data you do not need.

Raw logs are more difficult to read, but can be useful in providing syntax guidance, such as looking up fields and values to use in text filters when configuring handlers.

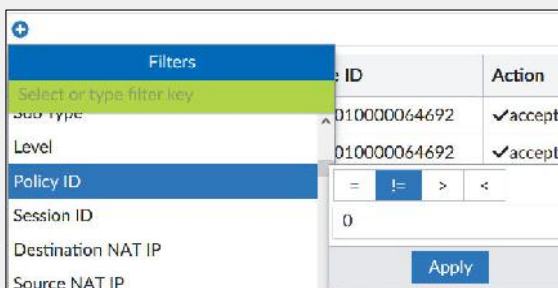
You can enable or disable case-sensitive searching to narrow down a query. You can also download logs, based on the current filters, as a text or CSV file.

Search Tips

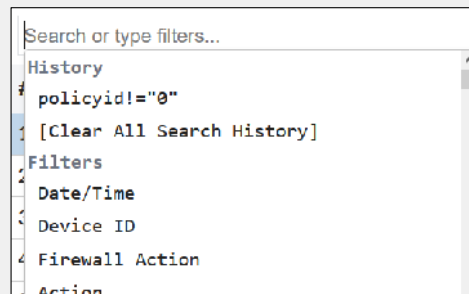
- Click on the magnifying glass to toggle between filter and text mode



- Filter mode allows you to click the filter search bar and define your search criteria using the GUI



- Text mode allows you to type in your filter and conditions manually, or pick a filter from history



If your search filters don't return the results you expected, the filter may be poorly constructed.

There are two modes to select from when you want to search for logs in **Log View**:

- Filter mode: Click the filter search bar and define your search criteria using the GUI.
- Text mode: Type in your filter and condition manually, or pick a filter from history.

Although you can type filters manually, doing so is very prone to syntax errors and spelling mistakes. Using the context menus in the GUI prevents you from making those mistakes.

DO NOT REPRINT
© FORTINET

Search Tips (Contd)

- Right-click the desired field value to set a filter based on that data

The screenshot shows a table with columns: Source, Destination IP, Service, and Action. The first row is highlighted: 10.0.3.20, 162.55.110.19, HTTP, blocked. A right-click context menu is open over the 'Source' column. The menu options are:

- Add AND Filter "Source IP = 10.0.3.20"
- Add AND Filter "Source IP != 10.0.3.20"
- Add OR Filter "Source IP = 10.0.3.20"
- Add OR Filter "Source IP != 10.0.3.20"
- Replace with Filter "Source IP = 10.0.3.20"** (highlighted with a red box)
- Replace with Filter "Source IP != 10.0.3.20"

A blue callout box labeled "Populates the search criteria" points to the selected option. A red arrow points from the selected option to a filter bar on the right that now contains "srcip = 10.0.3.20".

- Can include (=), or exclude (!=) the selected value from the search results
- Use the AND logic if all conditions must be true
- Use the OR logic if any of the conditions must be true
- Can also replace the current filter with your new conditions

Another useful tip is to right-click any field in the log entries to add the value into the filter. First, find a log in the log table that includes data that you want to search for. For example, if you want to search for any log entry that contains a specific IP address, right-click the desired value. A pop-up window will open for injecting that value into the filter.

You have the option to include or exclude the selected value, to use a single condition or multiple conditions, and use the logic of AND/OR to yield the desired results. You can also replace the current filter with the selected value.

Example of a Log Search

- You need to identify the malicious websites visited by the client with the IP address 10.0.3.20 for a specific time period

#	Date/Time	Device ID	Source	Destination IP	Service	Action	URL
1	06-08 10:37	FGVM-0000077646	10.0.3.20	64.70.19.203	HTTP	blocked	http://ffb07fb6990c3b5da86d66d43b4
2	06-08 10:37	FGVM-0000077646	10.0.3.20	155.159.36.59	HTTP	blocked	http://whollyfitinc.com/
3	06-08 10:37	FGVM-0000077646	10.0.3.20	176.103.56.36	HTTP	blocked	http://176.103.56.36/
4	06-08 10:37	FGVM-0000077646	10.0.3.20	43.163.226.161	HTTP	blocked	http://234w.cc/
5	06-08 10:35	FGVM-0000077646	10.0.3.20	50.28.56.190	HTTP	blocked	http://www.xp-13c6c6b6b6c6d.com/

Filters are based on the client's IP as the source, and the category description

Fields used in the filter are highlighted

This slide illustrates an example of a filter applied in **Log View**. You can easily add a filter by right-clicking the desired log field and select if you want that value included or excluded from the logs displayed.

In the example, the following parameters were selected to display malicious websites visited by a client machine:

- The log type selected is **Security**.
- The log subtype selected is **Web Filter**.
- The time frame is **Custom**.
- A filter was applied for the source IP address **10.0.3.20**.
- A filter was applied for the category description **Malicious Websites**.

If you need more granular results, you can always add more filters or edit the current ones.

DO NOT REPRINT
© FORTINET

Example of a Log Search (Contd)

- Search also supports wildcards
 - Use * for partial matches, which matches any sequence of characters, including an empty sequence
 - For example, the string *em perf* will match **System performance status**

Event

Application

All Devices

Last 1 Hour

19:03:04 - 20:03:04

Message=em perf

#	↓ Date/Time	Device ID	Message
1	2024-08-18 2	FAZ-VMTM24000	System performance status log rate low (10%)

Source IP=10

#	↓ Date/Time	Device ID	Action	Source
117	2024-08-18 2	FGVMSLTM24000	✓	10.200.3.1
118	2024-08-18 2	FGVMSLTM24000	✓	10.200.200.213

FORTINET
Training Institute

© Fortinet Inc. All Rights Reserved. 14

FortiAnalyzer supports the use of the * wildcard for partial matching. When you perform a partial search, you can filter with desired results without needing to type out the entire search string. A partial search is useful when you are looking for a wide range of results and you want to avoid having to type each search criterion, such as specifying multiple subnets using the AND condition.

Regex

- You can use regex in FortiAnalyzer to search logs or match a generic text filter
- This table lists common regex operators:

Operator	Function	Operator	Function
~	Matches the following regex pattern	+	Matches one or more of the preceding element
!~	Does not match the following regex pattern	\	Character escape for special characters
.	Matches any character		Used as an OR operator
[]	Matches any one character from a set or range	()	Used for grouping patterns together so that operators such as +, *, ?, can be applied to the group
*	Matches zero or more of the preceding element	^	Anchors the pattern to the beginning of the string
?	Matches zero or one of the preceding element	\$	Anchors the pattern to the end of the string

In FortiAnalyzer, you can use regex to perform a granular search for matching logs.

This slide includes some common regex operators that you can use to search in FortiAnalyzer.

Regex (Contd)

 matches the regex pattern

 does not match the regex pattern
(negate logic)

```
srcip~"10\.[0-9]+\.[0-9]+\.[0-9]+"
```

#	Source	Date/Ti
1	10.200.3.3	2024-06-1

```
srcip!~"10\.[0-9]+\.[0-9]+\.[0-9]+"
```

#	Source	Date/Ti
1	172.16.200.6	2024-06-1

```
srcip~"^(10\.[172\.(1[6-9]|2[0-9]|3[0-1])\.[192\.[168\.)]"
```

- Matches private IP address ranges with patterns *beginning* with 10. OR 172.16-31. OR 192.168.

In the examples shown on this slide, you can see two regex patterns using text mode filtering in FortiAnalyzer to filter the search results for the source IP addresses. The first example can be broken down as follows:

- ~ instructs FortiAnalyzer to treat the following string as a regular expression.
- \ is an escape character that instructs FortiAnalyzer to interpret the . as an actual character instead of a special character.
- [0-9]+ is a character class that matches any single digit from 0 to 9, and + indicates that the pattern should match one or more occurrences of the digit. In other words, [0-9]+ will match any number.
- The IP address 10.200.3.3 matches the requirements, so the result is shown in the search.

The second example can be broken down as follows:

- !~ instructs FortiAnalyzer to treat the following string as a regular expression, but the result needs to *not* match the regular expression.
- \ serves the same function as it does in the first example.
- [0-9]+ serves the same function as it does in the first example.
- The IP address 172.16.200.6 does not match the requirements of the regex pattern, so the result is shown in the search.

In the third example, private IP address ranges will match the search pattern because the ^ ensures the pattern begins with 10., or 172.16-31., or 192.168. IP addresses. The | character provides the OR logic.

You may also have noticed that the regex patterns on this slide include numbers outside of the valid IP ranges. For example, \.[0-9]+\.[0-9]+\.[0-9]+ would include IP addresses beyond 255 in an octet; however, this will not cause an issue. Because the devices sending the logs to FortiAnalyzer validate the IP addresses in their normal operations, the regex patterns do not need to be that precise.

DO NOT REPRINT
© FORTINET

Knowledge Check

1. What does FortiAnalyzer use for log viewing and report generation?
 - ✓ A. Queries on a database
 - B. Queries of plain text files

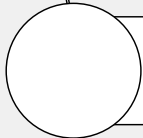
2. What is the purpose of using ADOMs?
 - ✓ A. To divide administration of devices, restrict access, and manage data policies
 - B. To reduce resource usage on FortiAnalyzer

DO NOT REPRINT
© FORTINET

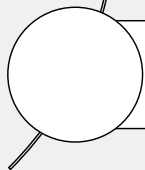
Lesson Progress



FortiAnalyzer Architecture



Operation Modes



FortiAnalyzer Fabric

Good job! You now understand FortiAnalyzer architecture.

Now, you will learn about FortiAnalyzer operation modes.

DO NOT REPRINT
© FORTINET

Operation Modes

Objectives

- Describe FortiAnalyzer operation modes
- Configure FortiAnalyzer collectors
- Configure FortiAnalyzer analyzers

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

By demonstrating competence in the configuration of collectors and analyzers, you can set up a topology in which FortiAnalyzer devices can work together to increase the overall performance of log receiving, analysis, and reporting.

DO NOT REPRINT
© FORTINET

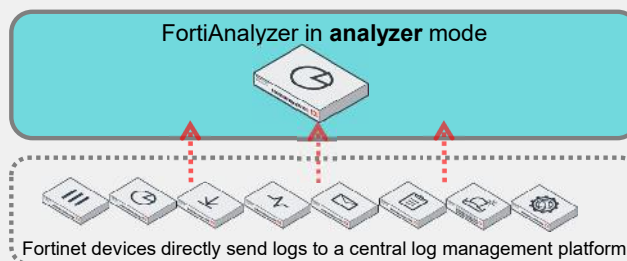
FortiAnalyzer Operation Modes—Analyzer

Dashboard > System Information

Operation Mode **Analyzer** Collector

Analyzer is the default operation mode

- Central log aggregator for one or more logging devices, or FortiAnalyzer in collector mode
 - Can still forward logs to another FortiAnalyzer (or syslog/CEF server)



FORTINET
Training Institute

© Fortinet Inc. All Rights Reserved. 20

FortiAnalyzer has two modes of operation: analyzer and collector. The operation mode you choose depends on your network topology and individual requirements.

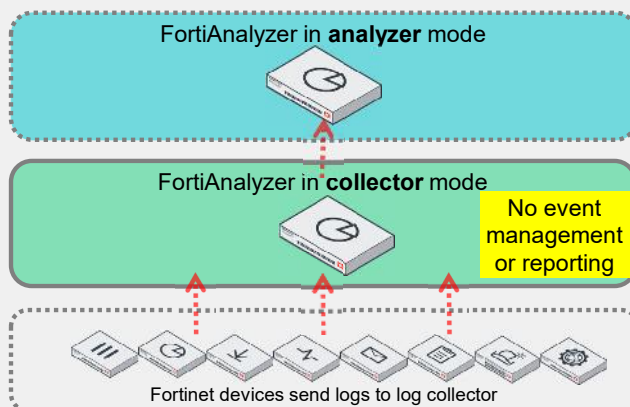
You can change the operation mode in the **System Information** widget on the dashboard.

When operating in analyzer mode, the device acts as a central log aggregator for one or more log collectors, such as a FortiAnalyzer device operating in collector mode, or any other supported device sending logs. Analyzer is the default operation mode.

DO NOT REPRINT
© FORTINET

FortiAnalyzer Operation Modes—Collector

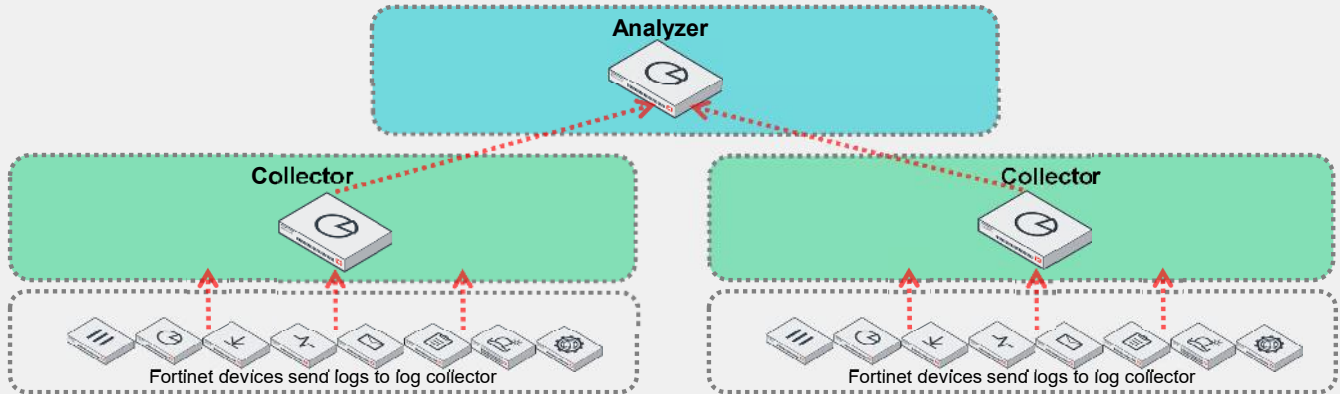
- Collects logs from multiple devices and forwards them to FortiAnalyzer in analyzer mode
 - Can aggregate logs to another FortiAnalyzer
 - Can *only* forward to syslog/CEF server in real-time forwarding mode
- Not used for analytics—archiving only



When operating in collector mode, FortiAnalyzer collects logs from multiple devices and then forwards those logs, in their original binary format, to another device, such as a FortiAnalyzer operating in analyzer mode. It can also send them to a syslog server or a common event format (CEF) server, depending on the forwarding mode. A collector does not have the same feature-rich options as an analyzer, because its only purpose is to collect and forward logs. It cannot perform event management or reporting.

DO NOT REPRINT
© FORTINET

Analyzer—Collector Collaboration



- Increase FortiAnalyzer performance by using both modes
- Offload the log-receiving task to the collector
- Analyzer focuses on data analysis and reporting
- Collector can help with slow or unreliable links by storing logs and forwarding them later
- On the collector, you should allocate most of the disk space to archive logs

FORTINET
Training Institute

© Fortinet Inc. All Rights Reserved. 22

By using both analyzer and collector modes, you increase FortiAnalyzer performance: Collectors offload the task of receiving logs from multiple devices from the analyzer. This allows the analyzer to focus on data analysis and reporting tasks.

Furthermore, because a collector is strictly dedicated to log collection, its log receiving rate and speed are maximized. If bandwidth is an issue, like in the case of slow WAN links, you can use the store and upload option to send logs only during low-bandwidth periods.

Because the collector does not perform any analytics tasks, you should allocate most of its disk space to archive logs.

DO NOT REPRINT
© FORTINET

Collector Configuration

- Enable collector operation mode
- Modify the data policy to focus on archiving
 - Set to 0 days for analytics
 - Set archive retention based on your organizational requirements
- Modify the disk utilization quota to focus on archiving
 - Allocate most disk space for archive log use
 - Set the analytics:archive ratio to 5%:95%

Dashboard > System Information

Operation Mode Analyzer Collector

System Setting > ADOMs

Data Policy		
Keep Logs for Analytics	0	Days
Keep Logs for Archive	365	Days

Analytics	5%	95%	Allocate disk space for analytics
Archive	95%	5%	Allocate disk space for archive

Note: You need to set the allocated disk quota to meet your requirements

FORTINET
Training Institute

© Fortinet Inc. All Rights Reserved. 23

You can change the operation mode to collector using the **System Information** dashboard widget. Once you change the operation mode, you will be logged out of FortiAnalyzer.

The next task is to configure the collector to focus on archiving. On this slide, you can see that analytics retention is set to 0 days, whereas archive retention is set to 365 days. Also, the analytics to archive ratio is set to 5% and 95%, respectively.

Note that the settings shown on this slide are only suggestions. The disk space configured, for example, is most likely insufficient for a production network.

Collector Configuration (Contd)

- Enable log forwarding on the collector
- Configure the required settings, including name, remote server type, server FQDN/IP, and other parameters
- Configure additional filters to forward matching logs, define fields to exclude, and mask sensitive fields

System Setting > Advanced > Log Forwarding

Name	FAZ-MSSP
Status	☒
Remote Server Type	FortiAnalyzer
Server FQDN/IP	10.0.1.236
Compression	☒
Reliable Connection	☒
Peer Certificate CN	
Sending Frequency	Real-time Every 1 Minute Every 5 Minutes
Log Forwarding Filters	
Device Filters	Select Device
Log Filters	☒
Enable Exclusions	☒
Enable Masking	☒

After you configure the data policy and disk utilization settings on the collector, you can configure log forwarding.

You will need to configure the following fields:

- **Name:** Type in a name for the log forwarding entry.
- **Remote Server Type:** Type FortiAnalyzer.
- **Server FQDN/IP:** Type in the target FortiAnalyzer address information.
- **Compression** (optional): Enable log message compression when the remote FortiAnalyzer also supports this format.
- **Reliable Connection** (optional): Enable this setting to use a TCP connection. Disable it to use a UDP connection.
- **Sending Frequency:** Select the frequency at which log forwarding will occur: in real time, every minute, or every 5 minutes.

You can also configure additional filters to control which type of logs are included or excluded, and whether you want to obfuscate fields:

- **Device Filters:** Select which devices are included.
- **Log Filters:** Select which log types are forwarded.
- **Enable Exclusions:** Enable to select which log types are excluded.
- **Enable Masking:** Enable to determine which fields will be masked before logs are forwarded.

DO NOT REPRINT
© FORTINET

Analyzer Configuration

- Modify the data policy to focus on analytics
 - Set the analytics retention based on your organizational requirements
 - Set to 0 days for archive
- Modify the disk utilization quota to focus on analytics
 - Set the analytics:archive ratio to 95%:5%

System Setting > ADOMs

Data Policy		
Keep Logs for Analytics	60	Days
Keep Logs for Archive	0	Days

Note: Analytics logs take up significantly more space than archive logs, so adjust your settings appropriately

Disk Utilization			
Allocated	13000	MB	Maximum Available: 30.4 GB
Analytics: Archive	95%	5%	☒ Modify
Alert and Delete When Usage Reaches	90%		

On the analyzer, configure the data policy and disk utilization to focus on analytics. In the example shown on this slide, the analytics retention is set to 60 days, whereas the archive retention is set to 0 days. There is a reason why the collector archive retention is set to 365 days, but the analyzer analytics retention is not set to the same range. The analytics to archive ratio is also set to 95% and 5%, respectively.

Remember that analytics logs take more space, so you must plan your data policy and disk utilization settings carefully. Archive logs are compressed, but analytics logs are not (in order for quick access). As a result, you can expect analytics logs to be approximately several times larger.

The settings shown on this slide are only suggestions. You must consider what your organization requires in your production network.

DO NOT REPRINT
© FORTINET

Knowledge Check

1. Which FortiAnalyzer operation mode do you use for analytics?
☒ A. Analyzer
☐ B. Collector
2. Which type of logs consume more disk space?
☒ A. Analytics
☐ B. Archive

DO NOT REPRINT
© FORTINET

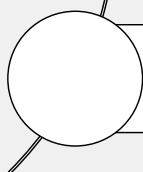
Lesson Progress



FortiAnalyzer Architecture



Operation Modes



FortiAnalyzer Fabric

Good job! You now understand FortiAnalyzer operation modes.

Now, you will learn about the FortiAnalyzer Fabric.

DO NOT REPRINT
© FORTINET

FortiAnalyzer Fabric

Objectives

- Describe the FortiAnalyzer Fabric
- Design FortiAnalyzer Fabric topologies
- Configure the FortiAnalyzer Fabric supervisor and members
- Manage Fabric groups

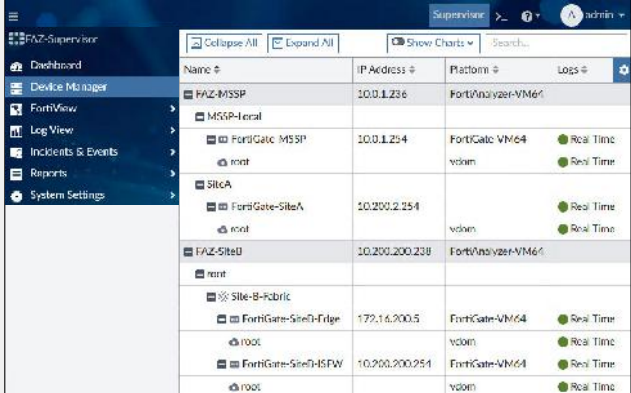
After completing this section, you should be able to achieve the objectives shown on this slide.

By demonstrating competence in the configuration of the FortiAnalyzer Fabric, you will be able to view logs, security incidents and events, and reports on one central FortiAnalyzer device.

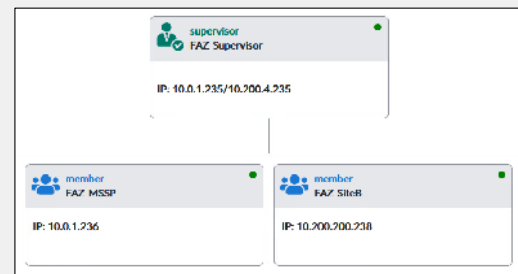
DO NOT REPRINT
© FORTINET

FortiAnalyzer Fabric

- Enables centralized viewing of devices, incidents, and events across multiple FortiAnalyzer devices
- Ideal for environments with multiple FortiAnalyzer devices and high log volume
- Two operation modes:
 - Supervisor—one per fabric; acts as the root
 - Member—sends information to the supervisor
- The supervisor includes these modules:
 - Device Manager
 - FortiView
 - Log View
 - Incidents & Events
 - Reports



Name	IP Address	Platform	Logs
FAZ-MSSP	10.0.1.236	FortiAnalyzer-VM64	
MSSP-Local			
FortiGate-MSSP	10.0.1.254	FortiGate-VM64	Real Time
root		vdn	Real Time
SiteA			
FortiGate-SiteA	10.200.2.254	FortiGate-VM64	Real Time
root		vdn	Real Time
FAZ-SiteB	10.200.200.238	FortiAnalyzer-VM64	
root			
Site-B-Fabric			
FortiGate-SiteB-Fridge	172.16.200.5	FortiGate-VM64	Real Time
root		vdn	Real Time
FortiGate-SiteB-HSFW	10.200.200.254	FortiGate-VM64	Real Time
root		vdn	Real Time



FORTINET
Training Institute

© Fortinet Inc. All Rights Reserved. 29

The FortiAnalyzer Fabric enables centralized viewing of devices, incidents, events, and reports across multiple FortiAnalyzers.

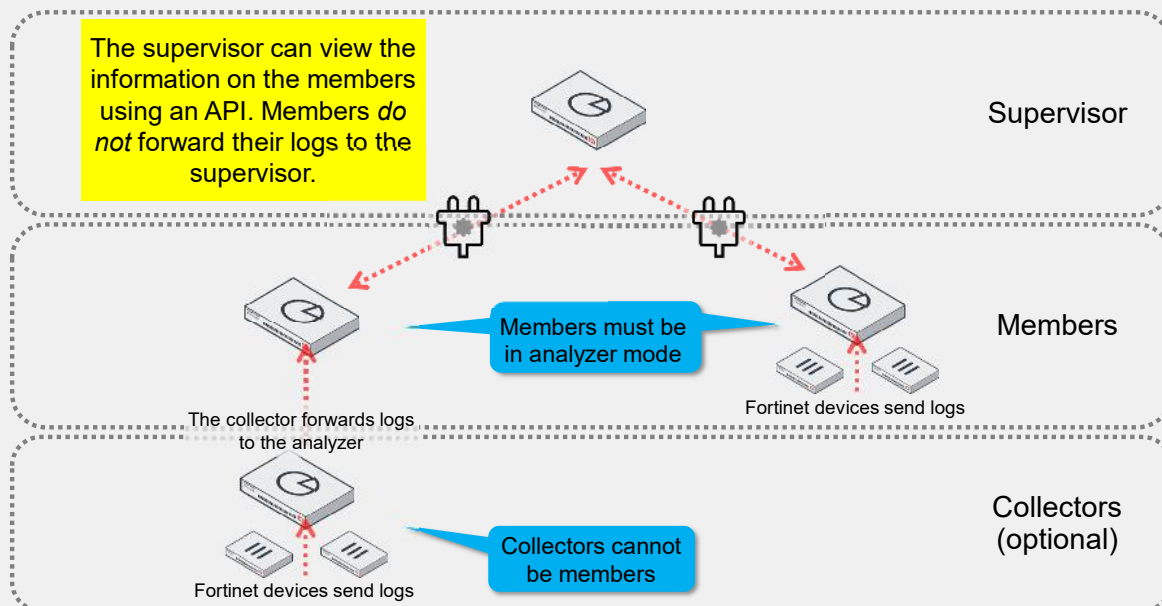
The FortiAnalyzer Fabric includes two operation modes: supervisor and member.

Supervisors act as the root device in the FortiAnalyzer Fabric. Security operations center (SOC) administrators can use the supervisor to view member devices and their ADOMs, authorized logging devices, as well as incidents and events created on members. FortiAnalyzer syncs the incident and event information from members to the supervisor using the API.

Members are devices in the FortiAnalyzer Fabric that send information to the supervisor for centralized viewing. When configured as a member, FortiAnalyzer devices continue to have access to the FortiAnalyzer features described in the *FortiAnalyzer Administration Guide*. FortiAnalyzer devices configured with high availability (HA) can become members. However, HA is not supported for FortiAnalyzers that are acting as the Fabric supervisor.

DO NOT REPRINT
© FORTINET

Sample FortiAnalyzer Fabric Topology



FORTINET
Training Institute

© Fortinet Inc. All Rights Reserved. 30

This slide shows a sample FortiAnalyzer Fabric topology comprising four FortiAnalyzer devices. The Fabric supervisor, depicted at the top, is configured to view information about two Fabric members. Logging devices cannot be registered to the Fabric supervisor. Instead, they are registered to one or more FortiAnalyzer devices in analyzer mode, which act as Fabric members.

Note that the FortiAnalyzer Fabric can also include downstream collectors that forward logs to Fabric members. In this sample topology, a single collector forwards logs to one of the members. The other member has no downstream collector, so devices send logs directly to it.

Configure the FortiAnalyzer Supervisor

- Configure the supervisor using the GUI:

System Settings > Fabric Management

Status	☒
Role	Supervisor Member
Cluster Name	MSSP Fabric
Session Port	6443
Secure Connection	☒

- Alternatively, on the CLI:
- (CLI only) Enable `soc-fabric` on the interface

```
# config system soc-fabric
set status enable
set name "MSSP-Fabric"
set supervisor <IP/DNS Name>
```

```
# config system interface
edit <port #>
set allowaccess soc-fabric <add other protocols you need>
end
```

Do not forget to add other administrative access protocols, such as HTTPS and SSH, as required. Existing settings will be overwritten.

To configure the Fabric supervisor, define the following fields:

- **Role:** Select **Supervisor**.
- **Cluster Name:** Type in a name that all FortiAnalyzer Fabric devices will use.
- **Session Port:** Type in a port number that all FortiAnalyzer Fabric devices will use, or the default port 6443.
- **Secure Connection:** Enable or disable TLS.

Note that the cluster name, session port, and secure connection settings must match the Fabric members.

You will also need to enable the `soc-fabric` administrative access option on any interface FortiAnalyzer is using to communicate with any Fabric member. You can perform this part of the configuration on the CLI only.

Note that you need to be careful when changing the administrative access on an interface, especially if it is the interface you use to manage FortiAnalyzer. In the example shown on this slide, if you enable only `soc-fabric`, existing administrative access protocols are overwritten. To prevent that from happening, you must define all your required protocols, such as HTTPS or SSH, and then also enable `soc-fabric`.

Configure the FortiAnalyzer Member

- Configure the member using the GUI:

System Settings > Fabric Management

Status	☒
Role	Supervisor Member
Cluster Name	MSSP-Fabric
IP	10.0.1.235
Session Port	6443
Secure Connection	☒

- Alternatively, on the CLI:
- (CLI only) Enable `soc-fabric` on the interface

```
# config system soc-fabric
  set status enable
  set name "MSSP-Fabric"
  set supervisor <IP/DNS Name>
```

```
# config system interface
  edit <port #>
    set allowaccess soc-fabric <add other protocols you need>
  end
```

Do not forget to add other administrative access protocols, such HTTPS and SSH, as required. Existing settings will be overwritten.

To configure the Fabric member, define the following fields:

- **Role:** Select **Member**.
- **Cluster Name:** Type in a name that all FortiAnalyzer Fabric devices will use.
- **IP:** Type the IP address of the Fabric supervisor.
- **Session Port:** Type in a port number that all FortiAnalyzer Fabric devices will use, or the default port 6443.
- **Secure Connection:** Enable or disable TLS.

Note that the cluster name, session port, and secure connection settings must match the Fabric supervisor.

You will also need to enable the `soc-fabric` administrative access option on the interface FortiAnalyzer is using to communicate with the Fabric supervisor. You can perform this part of the configuration on the CLI only.

DO NOT REPRINT
© FORTINET

Fabric Groups

- To filter information to specific FortiAnalyzer fabric members or ADOMs, you can create Fabric groups

System Settings > Fabric Groups

Create Fabric Group

Group Name: FAZ-MSSP-FAZ-SiteB

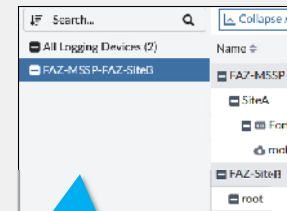
Description: Includes ADOMs MSSP Local and SiteA on FAZ-MSSP. Also includes all ADOMs on FAZ-SiteB

Add Member

Search

☐ FortiSandbox
☐ FortiWeb
☐ MSSP Local
☒ SiteA
☐ root
☒ FAZ-SiteB
☒ FortiAnalyzer
☒ FortiAuthenticator

FortiAnalyzer Fabric: Fabric Groups		
+ Create New Edit Delete		
Device Name	IP Address	Platform
FAZ-MSSP ①	10.0.1.236	FortiAnalyzer-VM64
SiteA		
FAZ-SiteB ②	10.200.200.236	FortiAnalyzer-VM64
root		
FortiAnalyzer		
FortiAuthenticator		



The fabric group can be used to filter devices



FORTINET
Training Institute

© Fortinet Inc. All Rights Reserved. 33

Depending on the number of devices added to the FortiAnalyzer Fabric, you may wish to limit the scope of information presented by the Fabric supervisor. You can filter information based on a specific set of FortiAnalyzer Fabric members or ADOMs by creating Fabric groups on the Fabric supervisor. Once created, the Fabric groups are listed under **Device Manager**, and can be used to filter results in **FortiView**, **Log View**, and **Reports**. In the example shown on this slide, the Fabric group **FAZ-MSSP-FAZ-SiteB** contains different ADOMs across two FortiAnalyzer Fabric members: **FAZ-MSSP** and **FAZ-SiteB**.

Without using Fabric groups, you can still filter information on the Fabric supervisor, but you will need to manually select the FortiAnalyzer devices and the ADOMs required. This could be time consuming if there are many devices in your topology. By leveraging Fabric groups, you can easily and quickly apply filters.

DO NOT REPRINT
© FORTINET

Knowledge Check

1. Which FortiAnalyzer operation mode must you configure Fabric members in?
 - ✓ A. Analyzer
 - B. Collector

2. Which statement about the Fabric supervisor is true?
 - A. All logging devices are registered to the Fabric supervisor.
 - ✓ B. Logging devices cannot be registered to the Fabric supervisor.

DO NOT REPRINT
© FORTINET

Lesson Progress



Introduction to FortiAnalyzer Architecture



Operation Modes



FortiAnalyzer Fabric

FORTINET
Training Institute

© Fortinet Inc. All Rights Reserved. 35

Congratulations! You have completed this lesson.

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

DO NOT REPRINT
© FORTINET

Review

- ✓ Manage administrative domains
- ✓ Describe FortiAnalyzer operation modes
- ✓ Configure FortiAnalyzer collectors and analyzers
- ✓ Design and deploy FortiAnalyzer Fabric deployments
- ✓ Manage Fabric groups

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

By mastering the objectives covered in this lesson, you learned about FortiAnalyzer key features and concepts, and how to use FortiAnalyzer effectively in your network.

DO NOT REPRINT
© FORTINET

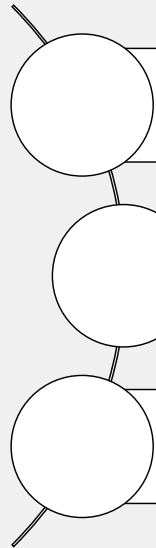


In this lesson, you will learn about the key features of FortiAnalyzer that make it essential to a SOC.

FortiAnalyzer integrates event monitors, event handlers, and incidents that can be generated from the logs it receives, so you can quickly identify and react to network security threats.

DO NOT REPRINT
© FORTINET

Lesson Overview



Concepts, Definitions, and Incident Handling

Events, Event Handlers, and Incidents

Threat Hunting

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

DO NOT REPRINT
© FORTINET

Concepts, Definitions, and Incident Handling

Objectives

- Describe FortiAnalyzer SOC features
- Describe basic concepts and definitions related to FortiAnalyzer SOC features
- Analyze *NIST SP 800-61 Computer Security Incident Handling Guide*

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

By demonstrating competence in FortiAnalyzer SOC concepts and definitions, you will be able to identify and describe the SOC-related features of FortiAnalyzer. You will also learn some guidelines for security incident handling.

FortiAnalyzer SOC Features

Incident Management



- Incident/case management
- Indicators attachment for incidents
- API to FortiSOAR for escalation

Automation



- Playbook templates and automation
- Connectors for playbooks
- Visual playbook editor
- Playbook execution
- Playbook monitor

Analytics



- Monitor and view log data with context of network activity
- Security Fabric analytics for devices within a Fabric ADOM

The legacy SOC operation had many disadvantages that are not manageable in the modern dynamic world. For example, it required analysts to handle too many alerts, often using separate interfaces, with the predictable loss of efficiency when trying to solve security breaches.

FortiAnalyzer provides solutions for modern SOC analysts that include:

- Complete incident lifecycle management capabilities, including alerts, monitoring, and escalation
- Automation framework using connectors and playbooks
- Analytics that provide insight and context of network activity, including normalized logs for Fortinet devices within a Fabric ADOM

Concepts and Definitions

Concept	Definition
Security information and event management (SIEM)	Fabric (SIEM) logs are a licensed feature that enables the FortiAnalyzer SIEM capabilities to parse, normalize, and correlate logs from Fortinet products, as well as security event logs of Windows and Linux hosts (with Fabric Agent integration).
Indicators of compromise (IOC)	The IOC service on FortiAnalyzer downloads the threat database from FortiGuard. The FortiGuard threat database contains the blocklist and suspicious list. IOC detects suspicious events and potentially compromised network traffic using sophisticated algorithms on the threat database.
Security event	A record of an observed occurrence on a monitored information system. If an event is relevant from an information security perspective, it can be considered a security event. On FortiAnalyzer, events are generated using event handlers. Also, a Windows audit log entry indicating a successful user login can be considered a security event.
Security incident	An event that indicates a malicious or abnormal occurrence. On FortiAnalyzer, incidents are escalated from events.
Indicator enrichment	Querying threat intelligence sources about an indicator to obtain security context information. A form of enrichment that is frequently used is checking the reputation of an indicator. For example, you can verify if a given file hash is associated with known malware.

This slide shows some of the basic concepts that you should be familiar with when working in a SOC environment.

SIEM is a technology that supports threat detection, compliance, and security incident management through the collection and analysis of security events, as well as a wide variety of other event and contextual data sources. Fabric (SIEM) logs are a licensed feature that enables the FortiAnalyzer SIEM capabilities to parse, normalize, and correlate logs from Fortinet products, as well as security event logs of Windows and Linux hosts (with Fabric Agent integration).

IOC are artifacts observed on a network or in an operations system where there is a high level of confidence that the artifacts indicate a computer intrusion.

A security event is a record of an observed occurrence on a monitored information system. If an event is relevant from an information security perspective, it can be considered a security event.

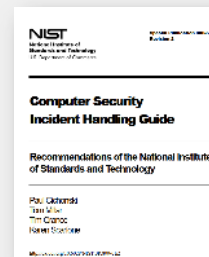
A security incident is an event that indicates a malicious or abnormal occurrence. On FortiAnalyzer, incidents are escalated from events.

Indicator enrichment queries threat intelligence sources for an indicator to obtain security context information. Checking the reputation of an indicator is a form of enrichment that is frequently used.

Even though these concept and definitions may vary depending on the source (including specific vendors and products), it's important to clarify a few definitions that are used during this training. Overall, the definitions follow either market conventions, established standards, or those of Fortinet solutions.

NIST SP 800-61 Incident Handling—Overview

- Defines incident handling as a lifecycle with four phases
- Assists in
 - Establishing computer security incident response capabilities
 - Handling incidents efficiently and effectively
- Focuses on
 - Analyzing incident-related data
 - Determining appropriate response
- Agnostic and broad approach
 - Can be followed independently of particular hardware, OS, protocols, or applications
 - Recommended practices for handling any type of incident



The content of this slide is based on copyright material from the National Institute of Standards and Technology (NIST) available online at <https://csrc.nist.gov/publications/detail/sp/800-61/rev-2/final>.

FORTINET
Training Institute

© Fortinet Inc. All Rights Reserved. 6

Incident handling is a process or life cycle, which means it's constantly in execution: Even after a single incident is resolved, the results feed back into the process for the next incident handling. The *inner* cycle defined by NIST comprises two phases: detection and analysis, and containment, eradication and recovery.

It's important to note that even these two phases represent a cycle, meaning two things:

- Containment, eradication and recovery can trigger detection and analysis steps
- Detection and analysis may trigger containment, eradication and recovery actions even before detection and analysis is fully concluded

Example: During detection and analysis, a SOC analyst may confirm a user account was compromised and immediately create a request for the IT team to temporarily disable the compromised user account (containment). In this case, a containment action may be taken even before detection and analysis is finished.

In mature SOC practices, a single person rarely executes all incident handling tasks, and even different teams may be involved in the process. The incident handling process also defines that certain steps must be executed by specific teams, or approved by a manager.

Sources and references:

- (1) Paul Cichonski, Thomas Millar, Tim Grance, Karen Scarfone, "SP 800-61 Rev. 2 Computer Security Incident Handling Guide", National Institute of Standards and Technology, August, 2021. Available online at <https://csrc.nist.gov/publications/detail/sp/800-61/rev-2/final>

NIST SP 800-61 Incident Handling—Detection and Analysis

- Prepare to handle any incident but focus on those that use common attack vectors, such as external and removable media, web, and email
- Signs of an incident
 - Precursors (relatively rare)—indicate an incident may occur in the future
 - Indicators (common)—indicate an incident may have occurred or may be occurring now
- Common sources of precursors and indicators
 - Intrusion detection and prevention systems (IDPSs)
 - Security information and event management (SIEM)
 - Antimalware and antispyware
 - OS-level monitoring (file integrity, processes, and so on)
 - Logs (OS, services, applications, and network devices)
 - Network flows



The content of this slide is based on copyright material from NIST available online at <https://csrc.nist.gov/publications/detail/sp/800-61/rev-2/final>.

FORTINET
Training Institute

© Fortinet Inc. All Rights Reserved. 7

The incident response process has several phases. The initial phase involves establishing and training an incident response team, and acquiring the necessary tools and resources. During preparation, the organization also attempts to limit the number of incidents that occur by selecting and implementing a set of controls based on the results of risk assessments.

Incident response methodologies typically emphasize preparation—not only establishing an incident response capability so that the organization is ready to respond to incidents, but also preventing incidents by ensuring that systems, networks, and applications are sufficiently secure.

For many organizations, the most challenging part of the incident response process is accurately detecting and assessing possible incidents—determining whether an incident has occurred and, if so, the type, extent, and magnitude of the problem. What makes this so challenging is a combination of three factors:

- Incidents may be detected through many different means, with varying levels of detail and fidelity. Automated detection capabilities include network-based and host-based IDPSs, antivirus software, and log analyzers. Incidents may also be detected through manual means, such as problems reported by users. Some incidents have overt signs that can be easily detected, whereas others are almost impossible to detect.
- The volume of potential signs of incidents is typically high.
- Deep, specialized technical knowledge and extensive experience are necessary for accurate and efficient analysis of incident-related data.

Precursors and indicators are identified using many different sources. The slide shows some of the most common ones.

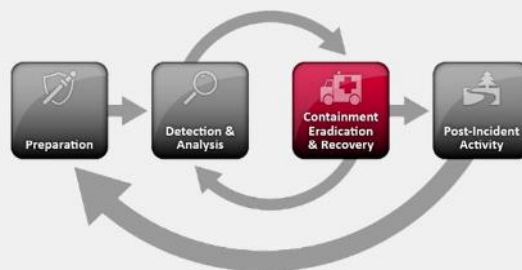
DO NOT REPRINT
© FORTINET

NIST SP 800-61 Computer Security Incident Handling— Containment, Eradication and Recovery

- Containment
 - Often required and should be considered early
 - Decision-making is an essential part
 - Strategies vary per incident
- Eradication and Recovery
 - Identify affected resources, attacking resources, and communication channels
 - Eliminate components of the incident (delete malware, disable compromised accounts, remove persistence, and so on)
 - Restore systems to normal operations
 - Confirm systems are working normally
 - Remediate vulnerabilities (if applicable)

Recovery may involve actions, such as:

- Restore systems from clean backups and snapshots
- Rebuild systems from scratch
- Replace compromised files with clean and reliable versions
- Install patches
- Change passwords



The content of this slide is based on copyright material from NIST available online at <https://csrc.nist.gov/publications/detail/sp/800-61/rev-2/final>.

FORTINET
Training Institute

© Fortinet Inc. All Rights Reserved. 8

Containment is about stopping the adversary from progressing toward their objectives. Containment is important before an incident overwhelms resources or increases damage. Most incidents require containment, so that is an important consideration early in the course of handling each incident. A very straightforward example of this is quarantining a compromised host to prevent the adversary from using it as a stepping stone to other phases of the attack.

Eradication means eliminating the threat. Using the compromised host example, this could involve removing malware and persistence mechanisms on the host. During eradication, it is important to identify all affected hosts within the organization so that they can be remediated. For some incidents, eradication is either not necessary, or is performed during recovery.

In recovery, administrators restore systems to normal operation, confirm that the systems are functioning normally, and (if applicable) remediate vulnerabilities to prevent similar incidents. Using the compromised host scenario, this could involve removing the host from quarantine so it can be used normally again on the network.

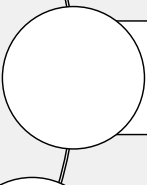
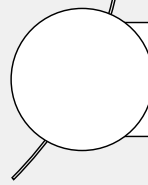
Knowledge Check

1. Which part of containment, eradication, and recovery does quarantining an infected host fall under?
 - ✓ A. Containment
 - B. Eradication
 - C. Recovery

2. On FortiAnalyzer, what is an incident?
 - A. A record of an observed occurrence on a monitored system
 - ✓ B. A security event that has been escalated

DO NOT REPRINT
© FORTINET

Lesson Overview

-  Concepts, Definitions, and Incident Handling
-  Events, Event Handlers, and Incidents
-  Threat Hunting

FORTINET
Training Institute

© Fortinet Inc. All Rights Reserved. 10

Good job! You now understand FortiAnalyzer SOC concepts and definitions.

Now, you will learn about events, incidents, and event handlers on FortiAnalyzer.

DO NOT REPRINT
© FORTINET

Events, Incidents, and Handlers

Objectives

- Analyze and manage events and event handlers
- Customize event handlers
- Analyze and create incidents

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

By demonstrating competence in events, incidents, and handlers, you can analyze and manage events and event handlers, and analyze and create incidents.

DO NOT REPRINT**© FORTINET**

Events and Event Handlers

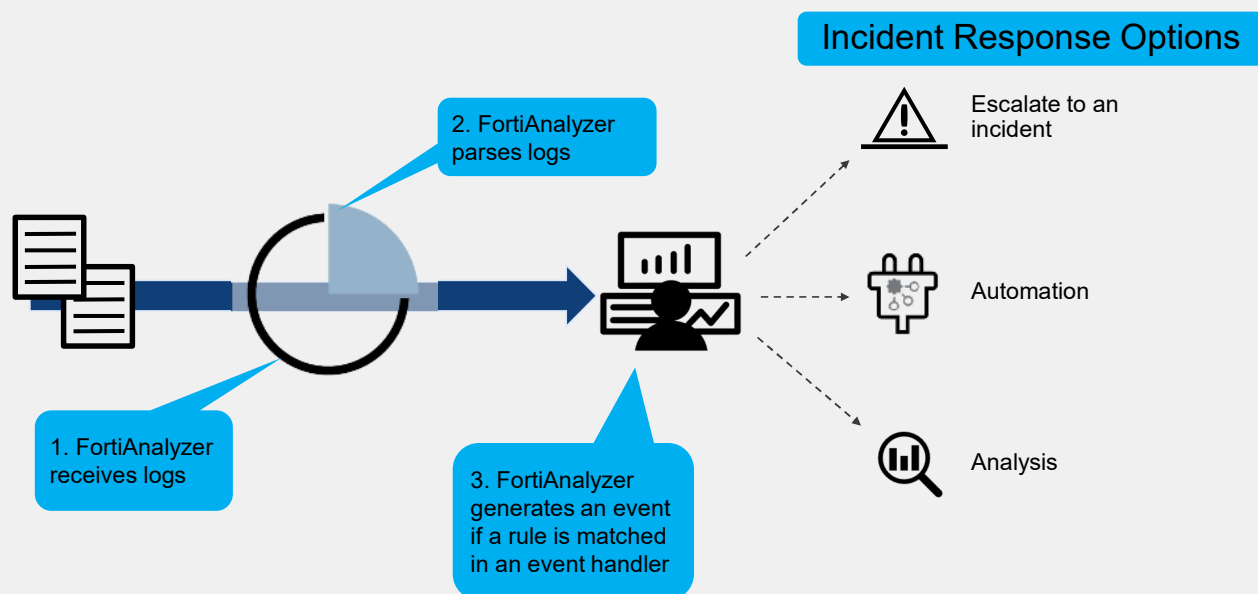
- Events are generated by event handlers
- FortiAnalyzer is preconfigured with many event handlers
- You can create custom event handlers to generate events
- FortiAnalyzer filters all incoming logs using event handlers
- If logs match the conditions configured in an event handler, FortiAnalyzer generates an event
- All the events that are generated can be viewed on the **Events Monitor** page

Event handlers generate events on FortiAnalyzer. FortiAnalyzer is preconfigured with many prebuilt event handlers. However, FortiAnalyzer provides analysts with the ability to custom build their own event handlers to generate events from logs that they determine are important.

FortiAnalyzer filters the logs it receives using event handlers and, if the logs received match the conditions that are set in the event handlers, FortiAnalyzer generates an event.

You can view all generated events on the **Events Monitor** page.

How Are Events Generated?



After receiving logs from other devices, and based on the details included in them, FortiAnalyzer uses event handlers to determine whether new events need to be generated. Event handlers identify whether the information in the logs matches a series of configurable criteria, such as threat type, device type, log type, and so on.

FortiAnalyzer comes with many predefined event handlers that you can use. You can also clone and customize them, or create custom event handlers from scratch.

You can view generated events under **Event Monitor**, where you can see them combined or further divided by endpoint, threat, and system events.

If events warrant further attention and investigation, you can escalate them to incidents. From there, you can correlate logs with the incident, look at an incident timeline, assign a priority and an analyst to review the incident, and more. If there is a large volume of generated events, you may leverage playbooks to create, handle, and resolve incidents.

DO NOT REPRINT
© FORTINET

Managing Event Handlers

- Event handlers look for specific conditions in logs
- Enable or disable event handlers as needed
- Disabled handlers do *not* generate events

Incidents & Events > Handlers

Disabled handlers don't generate events

Enable only the event handlers you need

Status	Name	Rules	Events	MITRE Tech ID
☐	Default-Windows-Registry-Modification-Block...	Rule: 1 Windows Registry or File Modification Blocked		T1112
☒	Default-Web-Server-URL-Scanning-Detected	Rule: 1 Web Server Scanning: (Default,Reconnaissance)		T1595.003
☒	Default-Risky-Destination-Detection-By-Threat	Rule: 1 Web request to malicious destination detected; Rule: 2 Web request to malicious destination blocked; Rule: 3 DNS request to malicious destination detected; Rule: 4 DNS request to malicious destination blocked;	33	T102,T1071.001,T1071.004,T1021.001
☒	Default-Risky-Destination-Detection-By-Endpoint...	Rule: 1 Web request to malicious destination blocked; Rule: 2 Web request to malicious destination detected; Rule: 3 Web request to suspicious destination detected; Rule: 4 DNS request to malicious destination detected	7	T1102,T1071.001,T1071.004,T1021.001

This handler has 15 rules and has generated 33 events

FORTINET
Training Institute

© Fortinet Inc. All Rights Reserved. 14

An event handler looks for specific conditions in logs and, if a match exists, generates an event with details that you can configure. FortiAnalyzer includes many predefined event handlers that you can enable to generate events. The names of predefined handlers start with “Default”.

You can also disable event handlers, as the first event handler in the example on this slide shows. Disabled handlers do *not* generate any events.

This slide shows a predefined event handler that has 15 rules and has generated over 33 events on the FortiAnalyzer device.

Event Handlers—Configuration

- The configuration for each event handler can include:

- MITRE attributes
- Data selectors (exclusion filters)
- Automation stitches
- Notifications
- Rules

Set MITRE ATT&CK domain and technique ID(s) the event handler provides coverage for

- Rules are granular conditions

- Event handlers can have one or more rules
- Basic event handlers use OR logic
- Correlation event handlers have many operator logic options

Get notified when an event handler is triggered

Incidents & Events > Handlers > Basic Handlers

The screenshot displays the configuration interface for the 'SOC SMTP Enumeration Data Handler'. Key fields include:

- Name:** SOC SMTP Enumeration Data Handler
- Description:** Adversaries may gather email addresses that can be used during targeting.
- MITRE Tech ID:** A dropdown menu is open, showing a list of selected techniques: T1589.002 Email Addresses and T1590.001 Domain Properties.
- Data Selector:** SOC SMTP Enumeration
- Automation Stitch:** Disabled (off)
- Rules:** A list of rules is shown, including 'SOC Antispam Rule 1'.
- Notifications:** SOC SMTP Enumeration Alert

Event handlers require configuration and fine-tuning to deliver only the desired events. The main configuration page for the event handler allows you to enable the handler, type a name, and write a description for it.

You can also choose which MITRE domain the event handler falls under, and then select from a list of technique IDs that correspond to the handler. Many predefined event handlers already have the MITRE attributes configured. You can view the MITRE ATT&CK framework matrices under **Incidents & Events**.

You can also add a data selector, which is a common filter that is applied before every rule configured in the event handler. Because of that, they are also known as *exclusion filters*.

When a handler generates an event with the automation stitch option enabled, FortiAnalyzer sends a notification to the FortiGate automation framework, which then checks if there is a corresponding automation stitch in FortiOS. If there is one, the configured action is triggered.

The **Rules** section contains the fields that must be matched up against logs in order to generate events. You can disable, edit, or delete rules for the handler. The basic handler type uses OR logic when evaluating multiple rules. The correlation handler type has many more operator logic choices.

You can select a notification profile to send alerts whenever an event is generated by the handler.

Event Handlers—Rule Configuration

- Rules have many customizable fields
 - Not every field is required

Note: The fields available in the rules depend on the **Log Device Type** value

Incidents & Events > Handlers > Basic Handlers

Status ●

Name: Antispam Rule 1

Event Severity: High

Choose Your Logs

Start by selecting the device and log type that you want to monitor for events.

Log Device Type: FortiMail

Log Type: Anti-Spam Log (spam)

The system will categorize logs into smaller groups based on the chosen log fields.

Log Field: Device Name (devname) From (from) Device ID (device_id)

Log Filters: All Filters Any One of the Filters

Log Field	Match Criteria	Value	Action

Log Filter by Text: type==spam

Supports most Fortinet products and third-party devices through syslog

Use the generic text filter to search using wildcard expressions or regular expressions

The screenshot on this slide shows the fields available for configuration inside a rule, including the log device type and log type. Depending on the log type, log subtypes may be available. Note that within rules themselves, both AND and OR logic are supported if there are multiple conditions. The **Log Field** drop-down lists present common criteria you can select to group events.

The **Log Filters** option allows you to select common filtering criteria from a list (by clicking the + icon) and add to the rule. You can also use generic text filters under **Log Filter by Text** if you require precise filtering.

DO NOT REPRINT

© FORTINET

Event Handlers—Rule Configuration (Contd)

- Define the condition that triggers an event
- There are three options:
 - Count: A minimum threshold count of matching logs
 - Log field value: Within a group, the log field <log field> has <integer> or more unique values
 - Sum: Multiple options such as duration, sent/received bytes, and sent/received packets
- Additionally, configure the following in relation to your selection:
 - Time: All logs were generated within <integer> minutes

Incidents & Events > Handlers > Basic Handlers

Trigger an event when:

☒ A group contains or more log occurrences

☐ Within a group, the log field has or more unique values

☐ The sum of is greater than or equal to

All logs were generated within minutes

Advanced Settings

Event Type Override

Event Message

Event Status

☒ Allow FortiAnalyzer to choose

Tags

Log Field	Indicator Type	Count	Action
+			

Additional Info

☐ Use system default

☒ Use custom message

Malware:\$(\$mname) with severity:\$(\$risk) found in file:\$(\$fname), Checksum:\$(\$md5) from \$(\$groupby2)

Used for data exfiltration and is only for log device type Fabric

FORTINET
Training Institute

© Fortinet Inc. All Rights Reserved. 17

If an event handler is generating too many events in your environment, you can configure the trigger conditions such as count or sum, and the duration settings.

The trigger condition has three options that you can choose from: count, log field value, and sum. Additionally, you can configure a time condition. The number of matching logs must occur in the specified duration in order to generate an event.

You can also configure the event type, message, status, and indicator.

DO NOT REPRINT

© FORTINET

Event Handlers—Data Selectors

- Data selectors help narrow down events generated by devices, subnets, and filters:

- Devices (by name)
- Subnets (created in Fabric View)
- Filters (OR logic)

- Filters are granular conditions within data selectors:

- Log device type
- Log type/subtype
- Matching logic (AND/OR logic)
- Generic text filter (for more precise filtering)

Incidents & Events > Handlers > Data Selectors

FORTINET
Training Institute

© Fortinet Inc. All Rights Reserved. 18

Data selectors help narrow down the events you want to see generated in event handlers. You can specify various criteria within the data selector, including the devices, subnets, and additional filters. You must configure a data selector first before you can apply it to an event handler.

Filters are granular rules to filter which types of logs match the data selector. You can create multiple filters per data selector. The data selector matches filters with OR logic.

The bottom screenshot on this slide shows the fields available for configuration inside a filter, including the log device type, log type, and log subtype. Note that filters support both AND and OR logic within themselves. The **Log Field** drop-down field presents common criteria you can select to include in the filter. Alternatively, you can use generic text filters if you require precise filtering.

Event Status

- Events can be set to one of four statuses

Incidents & Events > Event Monitor

10.0.3.20 (115)	Unhandled
Compromised host detected	Unhandled
Web request to Unrated detected	Unhandled
Web request to Malicious Websites blocked	Mitigated
Compromised host detected	Unhandled
Compromised host detected	Unhandled
Web request to Malicious Websites blocked	Mitigated

Event Status	Description
Unhandled	The security event risk is not mitigated or contained, so it is considered open
Contained	The risk source is isolated
Mitigated	The security risk is mitigated by being blocked or dropped
Blank	Other scenarios

Note: You can configure the desired event status manually in the handler settings, or let FortiAnalyzer choose it automatically

Events in FortiAnalyzer can be set to one of four statuses. The status determines if more action needs to be taken by the security team.

The **Unhandled** status means that the security event risk is not mitigated or contained, so it is considered open. For example, an intrusion prevention system (IPS) or antivirus log with an `action` value of `pass` has the event status set to **Unhandled**. Botnet and indicator or compromise (IOC) events are also considered unhandled.

The **Contained** status means that the risk source is isolated. For example, an antivirus log with an `action` value of `quarantine` has the event status set to **Contained**.

The **Mitigated** status means that the security risk is being blocked or dropped. For example, an IPS or antivirus log with the `action` value of `block` or `drop` has the event status set to **Mitigated**.

The **Event Status** field is empty in other scenarios. For example, you can see both `allow` and `block` actions in logs associated with that event.

Event Handlers—Generic Text Filters

- Generic text filters allow more precise and flexible control over which logs trigger an event
 - Multiple operators and logic are supported
- Supported operators:

Operator	Meaning
==	Equal (exact match)
!=	Not equal (not matching)
<	Smaller than
<=	Smaller than or equal to
>	Greater than
>=	Greater than or equal to
~	Contains the regular expression
!~	Does not contain the regular expression

Tokens: '(', ')', '&', '|', 'and', 'or', 'not'

Generic text format:

- Tokens: '(', ')', '&', '|', 'and', 'or'
- Operators: '==', '!=', '<', '<=', '>', '>=', '~', '!~'

Examples:

```
dstip==192.168.1.168 and hostname ~ "facebook" dstip==192.168.1.168 and ( dstport == 514 or dstport == 515 )
```

Log Filter by Text

Hover over this icon to see the tooltip in the GUI

Tip: Identify the logs that you want to generate events for, and from the raw view, copy the strings you want to match

When configuring an event handler, the use of generic text filters allows more precise and flexible control over which logs trigger an event. These filters use operators based on regex using the Portable Operating System Interface (POSIX) standard.

Event handlers support multiple operators and logic. You can hover your cursor over the question mark next to **Generic Text Filter** to display an example, as shown on this slide.

Keep in mind that you must use the escape character “\” if you need to include a reserved character in your filter, for example when separating different parts of a URL.

To avoid syntax errors, search raw logs to identify the logs you want to generate an event for, and directly copy and paste the strings you want to match in the handler.

DO NOT REPRINT
© FORTINET

Managing Events

- **Event Monitor** displays events generated by the configured event handlers

Incidents & Events > Event Monitor

All Events	By Endpoint	By Threat	System Events	Toggle View				
 All Devices	 Last 5 Minutes	☐ Show Acknowledged	 Expand All					
Search or type filters								
☐ Event	Event Status	Event Type	Count	Severity	First Occurrence	Last Update	Additional Info	Handler
☒ FortiMail (1)	Unhandled	Email Filter	11	Critical	a minute ago	a minute ago	Malware:(\$mname) with se	SMTP Enumeration Data Handler
☐ FortiMail Detected Spam from email@mail.com	Unhandled	Email Filter	11	Critical	2024-03-05 16:22:57	2024-03-05 16:23:07	Malware:(\$mname) with se	SMTP Enumeration Data Handler

Critical severity and marked as unhandled
Double-click to see the originating log

This is a snippet of **Log View** of correlated logs with the event

This is the event handler that generated this event

Note: If you are receiving unexpected events, check that the handler is configured correctly

View Correlated Logs

#	Date/Time	Device ID	Session ID	Client Name	Destination IP	From	To	Subject	Message
1	16:22:57	FEVMSLTM22000111	4260MsDw006655-4260MsDw00665		10.200.200.100	<email@mail.com>	2002@acmecorp.net	<2002@acmecorp.net>	User: unknown

FORTINET
Training Institute

© Fortinet Inc. All Rights Reserved. 21

After event handlers start generating events, you can examine them in the **All Events** tab.

You can see events combined on the **All Events** tab, or further divided by endpoint, threat, and system events.

Double-clicking an event provides more details about it, including the information from the associated logs. Generally, you should give priority to events with an unhandled status and/or critical severity.

Available Management Actions for Events

- You can acknowledge an event, add a comment, assign it to an administrator, or create an incident from it

Incidents & Events > Event Monitor

All Events | By Endpoint | By Threat | System Events | Toggle Views

All Devices | All | ☐ Show Acknowledged | ☒ Expand All

Search or type filters...

Event	Event Status	Event Type	Count	Severity	First
198.50.152.88 (2)	Unhandled	Traffic	2	Critical	a day
Traffic to C&C from 10.0.3.20 detected	Unhandled	Traffic			
Traffic to C&C from 10.0.1.200 detected	Unhandled	Traffic			
192.169.69.25 (2)	Unhandled	Traffic			
1/8.162.203.226 (2)	Unhandled	Traffic			
66.45.245.150 (2)	Unhandled	Traffic			
1/8.162.217.107 (4)	Unhandled	Traffic			
5.79.71.205 (4)	Unhandled	Traffic			
193.166.255.171 (2)	Unhandled	Traffic			

Right-click an event to see the list of available actions

Acknowledged events are not shown by default

Create incidents from events that require further investigation

Filter based on the column values to display events of interest only

Available actions for right-clicked event:

- Acknowledge
- Comment
- Assign To
- View Log
- Search in Log View
- Create New Incident
- Add to Existing Incident
- Filter by Event Type = Traffic
- Filter by Event Type != Traffic

Right-clicking an event allows you to enter a comment for your records, acknowledge the event, assign it to an administrator (or yourself) for further investigation, or create an incident from it.

Acknowledging an event removes it from the event list, but you can display it again by clicking **Show Acknowledged**. Generally, you can acknowledge mitigated events because the related traffic was blocked by the firewall.

An excessive number of mitigated events, despite being blocked repeatedly, may indicate a compromised device. Additionally, if an event is used to generate an incident, you should acknowledge it after you mark the incident as resolved.

You can use filters to display only the events of interest. For example, display only events related to IPS.

Creating an Incident

- Create an incident when an event needs further analysis
- Can create manually or automatically (playbooks)

Incidents & Events > Event Monitor

Must create accounts for party responsible for handling incidents

Incidents & Events > Incidents

☐	Incident Number	Incident Date / Time	Incident Reporter	Incident Category	Severity	Status	Affected Endpoint
☐	IN00000012	2024-08-13 15:15:22	admin	Scans / Probes / Attempted	Medium	New	10.200.3.219 (WIN-CLIENT)

Not all events have the same impact on or importance to your network. Some of them might need further analysis to prevent or mitigate security breaches. When an analyst finds an event that requires further scrutiny, they should create a new incident from that event. You can think of an incident as an event that could have negative consequences to your everyday operations.

You can create incidents manually or, preferably, automatically with the use of playbooks, taking advantage of FortiAnalyzer automation capabilities.

In FortiAnalyzer, to create incidents manually in **Event Monitor**, right-click an event and select the corresponding option.

Every incident includes a category, severity, status, affected endpoint and, optionally, a description, MITRE attributes, and an assigned analyst.

Once created, you can view incidents on the **Incidents** interface.

DO NOT REPRINT
© FORTINET

Analyzing an Incident

Incidents & Events > Incidents

Incident #, description, category, assignee, and incident status

Medium IN00300012 Default-Recon-Activity-By-Endpoint happened at WIN-CLIENT Scans / Probes / Attempted Access Assigned to: admin New
Created on: 2024-06-13 15:15:22 -0700
Last Modified on: 2024-06-13 15:15:23 0700 [Edit] [Refresh]

Affected Endpoint/User
bob
Last Seen: 2024-06-13 15:15:23
Topology: WIN-CLIENT
Addresses: MAC: 00:0c:29:ab:74:13
IP: 10.200.3.219

Executed Playbooks

Playbook	Status	Trigger
Execute Playbook		

Audit History

2024-06-13 15:17:00 Now
Events Attached to Incident:
By: admin
New Incident Created
By: admin
Start: 2024-06-13 15:15:23

Incident Timeline
From 2024-06-12 14:26:10 To 2024-06-12 14:27:55 (Total: 1 Event) [Reset Zoom]

Comments Events Reports Indicators Affected Assets Processes Software Vulnerabilities

Search in Log View

Event	Event Status	Event Type	Count	Severity	First Occurrence
IP scanning on Port: 443 detected	Unhandled	Traffic	1/1	Medium	2024-06-12 13:48:35

Important details to help you investigate the threat, with the option to add or delete entries

FORTINET
Training Institute

© Fortinet Inc. All Rights Reserved. 24

To view the details of an incident, go to **Incidents**, and then double-click the incident you want. You can also right-click an incident, and then select **Analysis**.

The **Analysis** page provides all the relevant information and access to the tools an administrator needs to perform a full investigation of the incident. Some of the details shown on this page include: the affected endpoint and user (if available), the incident timeline, any executed playbooks and the ability to run them, audit history with any attached events and reports, and several more.

At the bottom, these tabs provide more details: **Comments**, **Events**, **Reports**, **Indicators**, **Affected Assets**, **Processes**, **Software**, and **Vulnerabilities**. You can add or delete entries to focus your investigation.

The list of events associated with the incident is also available under the tab with that name. From here, you can access the related logs by right-clicking the event of interest. This opens the **Log View** in a different window.

DO NOT REPRINT
© FORTINET

Editing an Incident

- Update each incident setting while working in it
- Close any solved incident
- Once closed, you can delete the incident from the list
- Notifications can be configured for each status change

Note: You should update incident details according to the progress of the investigation. Every incident should reach the **Closed** status.

Incidents & Events > Incidents

Edit Incident

Incident Number: INDC000012

Incident Date / Time: 2024-08-13 15:15:22

Incident Category: Scans/Probes/Attempted Access

MITRE Tech ID: T1590 Gather Victim Network Information, T1595.001 Scanning IP Blocks (2 entries selected)

Severity: Medium

Status: New

Affected Endpoint: [Search]

Description: [Search]

Assigned To: [Search]

Keep the incident status up to date

FORTINET
Training Institute

© Fortinet Inc. All Rights Reserved. 25

It is important to keep all incident settings up to date. This allows you to keep track of the work being done to solve an incident.

When an incident is considered closed, you should change its status accordingly. Additionally, you can delete resolved incidents from the list.

You can configure FortiAnalyzer to send notifications after any changes to an incident status.

DO NOT REPRINT
© FORTINET

Configure Incidents Settings

Incidents & Events > Incidents

	+ Create New	Edit	Delete All	Analysis	Settings	All
☐	Incident Number	Incident Date / Time	Last Update Date / Time			
☐	IN00000007	2023-09-07 10:53:35	2023-09-07 10:56:54			
☐	IN00000006	2023-09-07 10:48:10	2023-09-07 10:48:11			

Notifications

+ Create New

Fabric Connector 1 MS_Teams_Connecto

- ☒ Send notification when an incident is created
- ☒ Send notification when an incident is updated
- ☒ Send notification when an incident is deleted

Fabric Connector 2 ServiceNow_Connecto

- ☐ Send notification when an incident is created
- ☒ Send notification when an incident is updated
- ☐ Send notification when an incident is deleted

First create the connectors in Fabric View

FAZ_Notification 1:23 PM

```
fortianalyzer_notification: {
  type: incident
  adom: ADOM1
  from: FAZ-VM0000065040
  timestamp: 1694118176
  apiver: 1
  data: [
    {
      incid: IN00000007
      change_type: update
      revision: 1
      attach_revision: 3
    }
  ]
}
```

Notification example

FORTINET
Training Institute

Note: Different connectors can have different settings

© Fortinet Inc. All Rights Reserved. 26

Incidents usually go through several stages during the analysis process. In most cases, it is important to make sure all parties involved are notified when the incident status changes.

You can configure FortiAnalyzer to send a notification to external platforms using preconfigured fabric connectors.

To configure notifications, in **Settings**, select a fabric connector from the drop-down field, and then choose the incident activity for which you want to send notifications.

You can add more than one fabric connector, each with the same or different notification settings. You must configure the receiving side of the connector for the notifications to be sent successfully. As an example, this slide shows a notification received in Microsoft Teams for an updated incident.

Use Case—Healthcare Sector



Your organization is a hospital targeted by cybercriminals through a phishing attack to ransom private data

Threat: Potential breach exposing thousands of patients' data and putting patients at risk

Our goal: *Configure event handlers to detect the tactics and techniques used by Group ABC*

Domain: Enterprise

Attacker: Group ABC



In the healthcare sector story from *Lesson 1—SOC Concepts and Security Frameworks*, the blue team prepares to build their detection capabilities by configuring custom event handlers on FortiAnalyzer to detect the various tactics and techniques used by Group ABC.

Blue Team Plan of Action—Detection Capabilities



- Configure custom event handlers and data selectors to identify:
 - Probing attacks that target email systems in search of valid email accounts
 - Spearphishing emails with attached malicious macro-enabled files
 - Operating system service creation
 - Network scans that identify high-priority targets
 - Defense evasion (clearing security audit logs on the compromised host)
 - Lateral movement and exploiting remote access
 - Data exfiltration



Using their knowledge of Group ABC's usual attacking methodologies, the blue team can configure custom event handlers and data selectors to protect against attacks listed on this slide. You will have the opportunity in the lab exercises to set up defenses as part of the blue team.

DO NOT REPRINT
© FORTINET

Mock Attack Example

Incidents & Events > Event Monitor

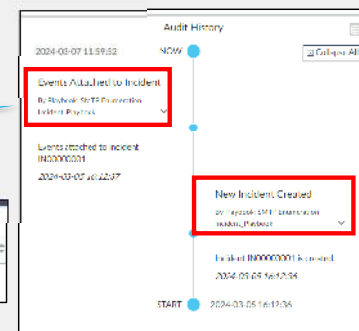
Event	Event Status	Event Type	Count	Severity	First Occurrence	Last Update	Additional Info	Handler
☐ MSOffice/Agent.NUOSZNYtr (1)	Unhandled	Malware	1	Critical	a few seconds ago	a few seconds ago		Spearphishing handler
☐ FortiSandbox Detected Malware from 100.64.1.20	Unhandled	Malware	1	Critical	2024-03-07 12:35:19	2024-03-07 12:35:39		Spearphishing handler
☐ FortiMail (2)	Unhandled	Email Filter	4955	Critical	4 hours ago	4 hours ago	Malware:\${mname} with s	SMTP Enumeration Data Handler
☐ FortiMail Detected Spam from email@mail.com	Unhandled	Email Filter	3303	Critical	2024-03-07 08:39:49	2024-03-07 08:42:33	Malware:\${mname} with s	SMTP Enumeration Data Handler
☐ FortiMail Detected Spam from email@mail.com	Unhandled	Email Filter	1552	Critical	2024-03-07 08:15:06	2024-03-07 08:16:51	Malware:\${mname} with s	SMTP Enumeration Data Handler

Events generated by custom event handlers configured by the blue team

Incidents & Events > Incidents

☐ Incident Number	☐ Incident Date / Time	☐ Last Update Date / Time	☐ Incident Reporter	☐ Incident Category	☐ Severity	☐ Status
IN00000001	2024-03-05 16:12:36	2024-03-05 16:12:37	SMTP Enumeration Incident_Playbook	Denial of Service (DoS)	High	New

Incident created on FortiAnalyzer to monitor the event



FORTINET
Training Institute

© Fortinet Inc. All Rights Reserved. 29

This slide shows an example of the events generated by the custom event handler that was created by the blue team to identify *probing attacks that target email systems in search of valid email accounts* and to detect *spearphishing* emails which may contain a *malicious macro-enabled document*.

DO NOT REPRINT
© FORTINET

Mock Attack Example (Contd)

Incidents & Events > MITRE ATT&CK

Attack	Coverage	
Refresh	Last 4 Hours	2024-03-07 08:37:11 - 2024-03-07 12:37:11
Reconnaissance	Resource Development	Initial Access
10 techniques	8 techniques	9 techniques
Active Scanning Covered	Acquire Access Covered	Drive-by Compromise Covered
Gather Victim Host Information Covered	Acquire Infrastructure Covered	Exploit Public-Facing Application Covered
Gather Victim Identity Information 1	Compromise Accounts Covered	External Remote Services Covered
Gather Victim Network Covered	Compromise Infrastructure Covered	Hardware Additions Covered
Gather Victim Org Information Covered	Develop Capabilities Covered	Phishing 1
Phishing for Information Covered	Establish Accounts Covered	Replication Through Removable Media Covered
	Obtain Capabilities Covered	
		Native API
Execution	Persistence	
51 techniques	19 techniques	
Cloud Administration Command Covered	Account Manipulation Covered	
Command and Scripting Interpreter Covered	BITS Jobs Covered	
Container Administration Command Covered	Run or Legon Autostart Execution Covered	
Deploy Container Covered	Boot or Logon Initialization Scripts Covered	
Exploitation for Client Execution Covered	Browser Extensions Covered	
Inter-Process Communication Covered	Compromise Client Software Binary Covered	

The attack is covered on FortiAnalyzer based on the MITRE ATT&CK page

FORTINET
Training Institute

© Fortinet Inc. All Rights Reserved. 30

This slide shows the **Reconnaissance** and **Initial Access** tactics, and the **Gather Victim Identity Information** and **Phishing** techniques that have corresponding event handlers providing coverage against these attack vectors.

DO NOT REPRINT
© FORTINET

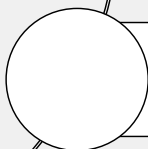
Knowledge Check

1. Which FortiAnalyzer feature generates events?
 - A. Playbooks
 - ✓ B. Event handlers

2. What does the *mitigated* event status mean?
 - ✓ A. The risk source is being blocked.
 - B. The risk source is being quarantined.

DO NOT REPRINT
© FORTINET

Lesson Overview

-  Concepts, Definitions, and Incident Handling
-  Events, Event Handlers, and Incidents
-  Threat Hunting

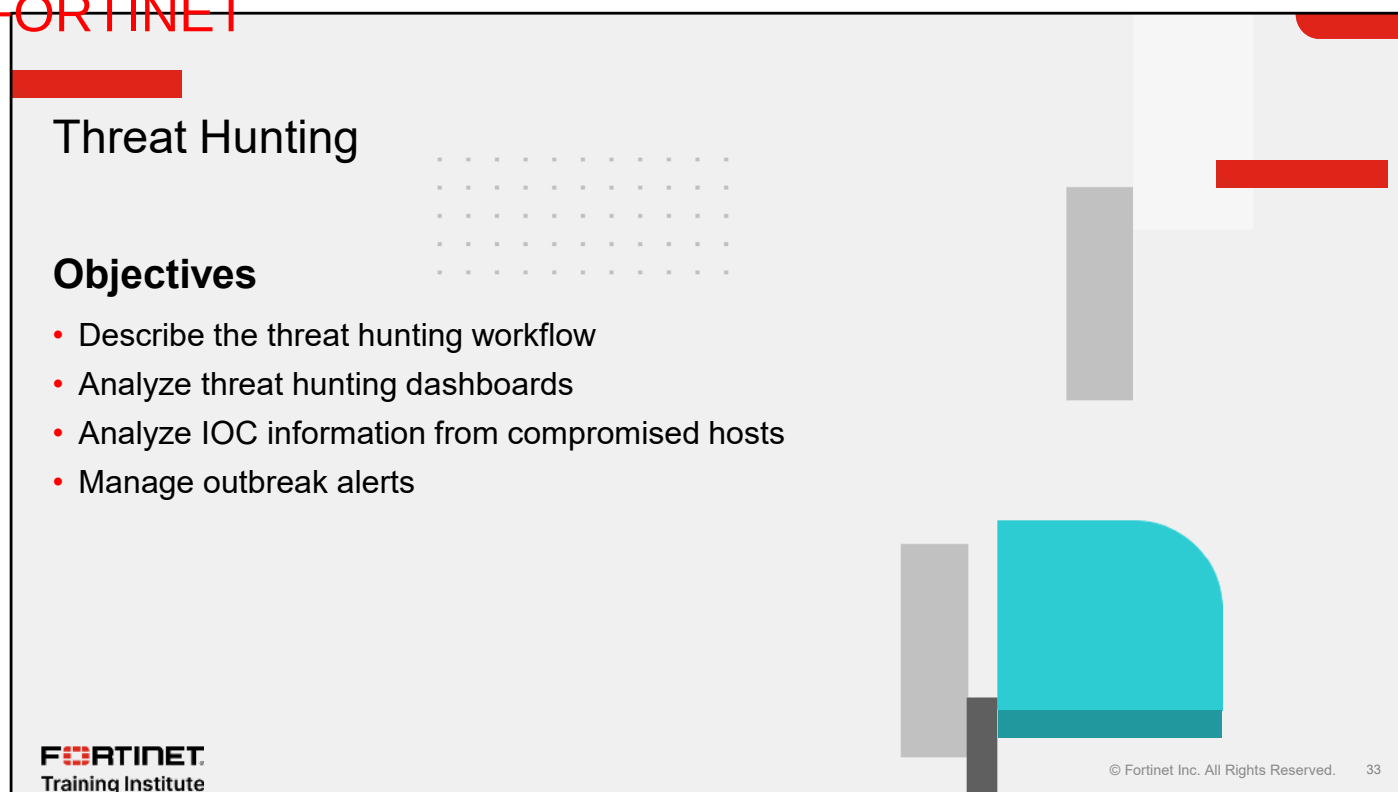
FORTINET
Training Institute

© Fortinet Inc. All Rights Reserved. 32

Good job! You now understand events, event handlers, and incidents.

Now, you will learn about threat hunting using FortiAnalyzer.

DO NOT REPRINT
© FORTINET

The slide features a light gray background with several decorative elements: a red horizontal bar at the top left, a grid of small dots in the upper center, a gray vertical bar on the right, a red horizontal bar on the right, and a large cyan rounded rectangle at the bottom right. The text is positioned on the left side of the slide.

Threat Hunting

Objectives

- Describe the threat hunting workflow
- Analyze threat hunting dashboards
- Analyze IOC information from compromised hosts
- Manage outbreak alerts

FORTINET
Training Institute

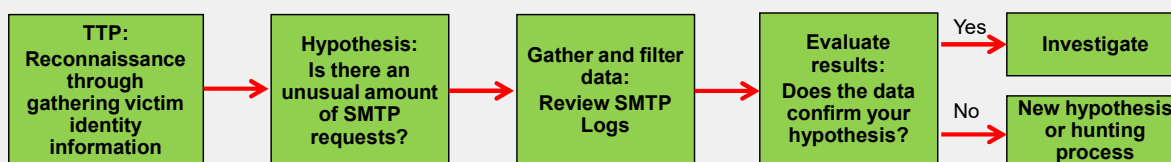
© Fortinet Inc. All Rights Reserved. 33

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 analyze FortiAnalyzer threat hunting dashboards and indicator of compromise (IOC) information from compromised hosts, as well as stay up-to-date on outbreak alerts.

Threat Hunting

- Proactively search for suspicious or risky network activity that may have gone undetected
- The process usually begins with a question:
 - Are any advanced persistent threats (APTs) currently active in the network?
- The reference to tactics, techniques, and procedures (TTPs), behaviors, and indicators helps to refine your questions further
 - Frequently aligned with the MITRE ATT&CK or the Cyber Kill Chain frameworks
- You can also create an if-then statement, for example:
 - If you suspect reconnaissance activities in the network, then you should see abnormal traffic trends
- A simplified example:



Threat hunting consists of proactively searching for suspicious or potentially risky network activity in your environment. The proactive approach helps the analyst find any threats that might have eluded detection by the current security solutions or configurations.

The threat hunting process usually starts with a broad question, or hypothesis, that determines which type of threat you are trying to find. You can also start with an if-then statement. For example, if you suspect reconnaissance activities in the network, then you should see abnormal traffic trends.

The process is frequently aligned to the MITRE ATT&CK or Cyber Kill Chain frameworks. This allows you to refine your questions further. The frameworks are not mutually exclusive: You can use both frameworks together to help analyze and protect your network.

Threat Hunting (Contd)

- The **Threat Hunting** dashboard takes advantage of the SIEM framework to allow for advanced correlation and analysis to hunt for threats

Incidents & Events > Threat Hunting

Threat Action (0)	2024-03-07 08:36:38 - 2024-03-07 08:41:37				
Threat Pattern (0)	#	Application Name	Count	Sent (bytes)	Session
Threat Name (0)	1		13,453(80%)		
Threat Type (0)	2	SMTP	2,770(16%)	1.6 MB	01s
File Hash (0)	3	tcp/555	388(2%)	19.7 KB	02s
File Name (0)	4	DNS	105(1%)	38.9 KB	05s
Application Process (0)	5	HTTPS	88(1%)	284.1 KB	24s
Application Name (10)	6	tcp/3081	54(< 1%)	4.0 KB	19s
Application Service (10)	7	HTTP	10(< 1%)	1.1 KB	16s
HTTP Referrer (0)	8	RSH	8(< 1%)	56.2 KB	18s
Destination Domain (0)	9	tcp/3888	8(< 1%)	608.0 B	19s
Destination IP (17)	10	tcp/3015	6(< 1%)	360.0 B	05s
Source IP (11)	11	udp/8014	4(< 1%)	1.2 MB	2c 24m 31s
Event Action (11)					

SOC analytics dashboard using the SIEM database

FortiAnalyzer includes the **Threat Hunting** dashboard, which offers a SOC analytics dashboard using the SIEM database.

Threat Hunting uses cached data to allow SOC analysts to quickly drill down on logs in fields of interest. This dashboard includes a **Log Count** chart and SIEM log analytics table.

You can configure a custom time range or apply filters to the dashboard to refine your search results further. Only logs matching the selected time range and filter are displayed in the SIEM log analytics table.

The dashboard view has various columns that display detailed statistics, including count (number of logs), percentage, sent bytes, and session duration information. Double-click an item in the table to view the detailed log information.

You must examine the information on the **Threat Hunting** dashboard and differentiate normal from anomalous behavior. For example, based on the image on this slide, you can ask the following questions:

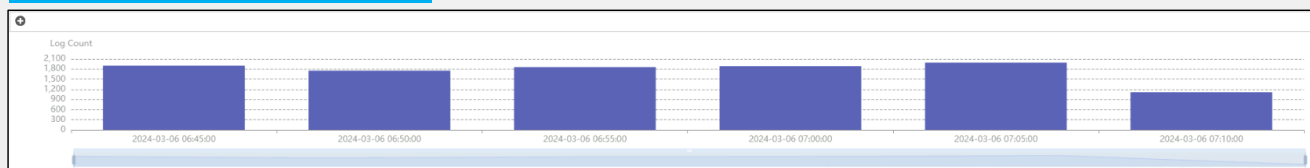
- Is the number of SMTP logs for this time period expected?
- Is the amount of SMTP connections at this hour normal?

DO NOT REPRINT
© FORTINET

Log Count Chart

- Use the **Log Count** chart to focus on the logs you must analyze based on a time range
- The details in the SIEM log table auto adjusts to the timeframe you select in this chart

Incidents & Events > Threat Hunting



Adjust the time bar to include only the desired time frame

FORTINET
Training Institute

© Fortinet Inc. All Rights Reserved. 36

The top of the **Threat Hunting** dashboard shows a chart displaying the total log count during the specified time range. This section is called the **Log Count** chart.

You can zoom in and out on the displayed time range by using the scroll wheel of your mouse, or by adjusting the time bar below the graph. You can adjust the time bar by dragging the start and stop bars on either side of the selected time range, or by clicking and dragging the entire time range to the left or right. For example, you could search for suspicious activity occurring outside business hours.

Only logs displayed within the time period visible in the chart are shown in the SIEM log analytics table.

Threat Hunting Example With FortiAnalyzer

- *Has reconnaissance been used to gather victim identity information from the mail server?*
- In this example, the analyst uses the log chart to discover an unusual number of SMTP requests
- Analysis shows that the IP address 100.64.1.20 is generating lots of queries within a short time period

Incidents & Events > Threat Hunting

2024-05-07 09:56:58 - 2024-05-07 09:41:57				
#	Application Name	Count	Size (bytes)	Session
1	SMTP	13,352 (145)	1.6 MB	0%
2	top-500	368 (28)	17.2 KB	02%
3	LINE	105 (18)	39.9 KB	00%
4	HTTPS	88 (15)	284.1 KB	04%
5	top-3000	545 (15)	4.0 KB	19%
6	HTTP	105 (18)	1.1 KB	18%
7	SSH	85 (15)	56.2 KB	18%
8	top-1000	45 (13)	205.0 B	19%
9	top-5000	65 (13)	160.0 B	03%
10	SSH	45 (13)	1.2 MB	20/24=33%
11	SSH	45 (13)	1.2 MB	20/24=33%

#	Time/Time	Data Source IP	Event Type	Event Source	Source IP	Destination IP	Application Name
1	08:41:57	FOUNDTM040003455	smtp	smtp	100.64.1.20	10.200.200.100	SMTP
2	08:41:57	FOUNDTM040003455	smtp	smtp	100.64.1.20	10.200.200.100	SMTP
3	08:41:57	FOUNDTM040003455	smtp	smtp	100.64.1.20	10.200.200.100	SMTP
4	08:41:57	FOUNDTM040003455	smtp	smtp	100.64.1.20	10.200.200.100	SMTP
5	08:41:57	FOUNDTM040003455	smtp	smtp	100.64.1.20	10.200.200.100	SMTP
6	08:41:57	FOUNDTM040003455	smtp	smtp	100.64.1.20	10.200.200.100	SMTP
7	08:41:57	FOUNDTM040003455	smtp	smtp	100.64.1.20	10.200.200.100	SMTP
8	08:41:57	FOUNDTM040003455	smtp	smtp	100.64.1.20	10.200.200.100	SMTP
9	08:41:57	FOUNDTM040003455	smtp	smtp	100.64.1.20	10.200.200.100	SMTP
10	08:41:57	FOUNDTM040003455	smtp	smtp	100.64.1.20	10.200.200.100	SMTP
11	08:41:57	FOUNDTM040003455	smtp	smtp	100.64.1.20	10.200.200.100	SMTP

- Further investigation determines that the queries are an external attacker gathering victim identity information
- A new incident is created, and the SOC responders can start containment and eradication steps

This slide illustrates an example of how an analyst can use FortiAnalyzer to perform a threat hunting procedure.

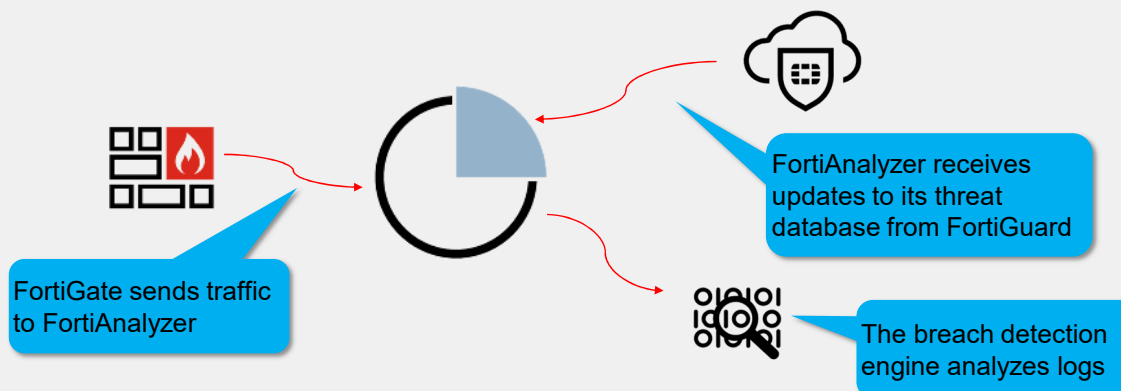
Based on the MITRE ATT&CK reconnaissance tactic, and the gather victim identity information technique, establish a question: *Has reconnaissance been used to gather victim identity information from the mail server?* This slide shows an example of the threat hunting used in this scenario.

Using the log chart, the analyst finds that an unusual amount of SMTP traffic is being generated, including outside normal operation hours. By analyzing the details of the SMTP logs, the analyst determines that the IP address 100.64.1.20 is the main source of this abnormal traffic.

This triggers the creation of a new incident. The SOC team determines that the host is compromised and initiates the SOC action plan to contain and eradicate this breach.

IOC (Compromised Hosts)

- The IOC engine detects end users with suspicious web usage compromises by checking new and historical logs against IOC signatures
- Uses FortiGuard threat intelligence to provide visibility of emerging threats
- Requires a FortiGuard subscription



The IOC engine detects end users with suspicious web usage by checking new and historical logs against the IOC signatures, which are based on a FortiGuard subscription.

The IOC service on FortiAnalyzer uses the FortiGuard database to analyze web filter, DNS, and traffic logs from FortiGate devices for breach detection. It is updated to provide coverage of emerging threats.

The breach detection engine does not analyze antivirus logs, IPS logs, and so on, because these threats are already detected or prevented on FortiGate. When a threat match is found, a threat score is assigned to the end user based on the overall ranking score.

When the check is completed, FortiAnalyzer aggregates all the threat scores of an end user and provides its verdict on the overall IOC of the end user. The verdict can be one of the following:

- **Infected** which indicates a real breach. This means that the breach detection engine found one or many matches of blocklisted IPs or domain generation algorithms (DGAs) in the web filter logs.
- **Suspicious** which indicates a *possible* breach with varying degrees of confidence.

Compromised Host IOC Example

FortiView > Threat & Events

Compromised Hosts

Add Filter

#	Source (User/IP)	Last Detected	Host Name	OS	Verdict	# of Threats	Acknowledged	Device Name	Device ID
1	10.0.3.20, 10.0.3.20	2023-08-18 13:19	10.0.3.20		Infected	3	☐	ISFW	FGVM010000077666

Compromised Hosts > Blocklist

srcip = 10.0.3.20 Add Filter

Summary

Source (User/IP): 10.0.3.20, 10.0.3.20
 Last Detected: 2023-08-18 13:19
 Host Name: 10.0.3.20
 OS:
 Verdict: **Infected**
 Acknowledged:
 Device Name: ISFW
 Device ID: FGVM010000077666
 # of Threats: 3

A real breach was detected, with three threat types and this entry hasn't been acknowledged yet

Displaying blocklist detection method used by the IOC

#	Detect Pattern	Threat Type	Threat Name	Category	Detect Method	# of Events	Log Type	Security Actions	Scan Time
16	xm-13cglc6bwb6cid.com	Malware	CnC	Spyware and Malware	Infected-domain	1	webfilter	Details	2023-08-18 12:51:33
17	pinompi.com	Malware	CnC	Remotography	Infected-domain	1	webfilter	Details	2023-08-18 12:53:53
18	208.100.26.245	Malware	CnC	Spyware and Malware	Infected-ip	1	webfilter	Details	2023-08-18 13:09:43
19	52.86.6.113.80	Malware	CnC	Spyware and Malware	Infected-ip	1	webfilter	Details	2023-08-18 13:22:53
20	gainwoks.net	Malware	CnC	Spyware and Malware	Infected-domain	1	webfilter	Details	2023-08-18 13:09:43
21	208.91.196.145	FUP	SpywareCnC		Infected-ip	1	traffic	Details	2023-08-18 13:14:33
22	5.79.71.205	Malware	CnC	Spyware and Malware	Infected-ip	1	traffic	Details	2023-08-18 13:18:43
23	85.17.31.122	Malware	CnC	Spyware and Malware	Infected-ip	1	traffic	Details	2023-08-18 12:53:53
24	91.195.210.123.80	Malware	CnC	Spyware and Malware	Infected-ip	1	traffic	Details	2023-08-18 13:23:53
25	56834764387462384.org	Malware	Sinkhole	Not Rated	Infected-domain	1	webfilter	Details	2023-08-18 13:08:00
26	corolbuan.com	Malware	Sinkhole	Phishing	Infected domain	1	webfilter	Details	2023-08-18 12:53:53

This slide shows an example of an IOC trigger in **FortiView**. The IOC engine has determined a real breach, as indicated by the **Infected** verdict. The **# of Threats** column indicates that three different threats are associated with this hit.

On the IOC FortiView, you can also:

- Filter the entries by specifying devices or a time period.
- Acknowledge the IOC. By default, you can view acknowledged IOCs, unless you configure the system to not show them. You can add a short comment when acknowledging an entry.
- Double-click an entry to drill down and view threat details.

When you double-click the desired entry, more details are displayed, and you can filter the view based on two categories:

- **Blocklist**, which indicates items marked as infected after checking the blocklist included in the IOC database downloaded from FortiGuard. You can verify that this traffic was blocked by clicking **Details** under the **Security Actions** column. If you believe that the IP address or domain listed under the **Detect Pattern** column is a valid one, you can report it as misrated by clicking that entry.
- **Suspicious**, which indicates a match was found in the suspicious list included in the IOC database downloaded from FortiGuard. In this case, FortiAnalyzer flags the endpoint for further analysis, compares the flagged log entries with the previous statistics of the endpoint for the same day, and then updates the score. If the score exceeds the threshold, that endpoint is listed or updated in **Compromised Hosts**.

Outbreak Detection Service Overview

- Licensed feature
- Allows customers to receive information about malware outbreaks
- Automatically downloads new event handlers and reports related to the outbreaks



The FortiAnalyzer Outbreak Detection Service is a licensed feature that allows FortiAnalyzer administrators to receive and view outbreak alerts, and automatically download related event handlers and reports from FortiGuard. Outbreak event handlers and reports are created in real time by Fortinet to detect and respond to emerging outbreaks.

The **Outbreak Alerts** window displays alerts from Fortinet, which are available on all ADOMs.

Outbreak Alert Handlers and Reports

- New event handlers are added to the list of available handlers, and you can use them in the same way as the rest in the list
- The same is true for the newly downloaded reports

Incidents & Events > Handlers

☐	Status ▾	Name ▾
☐	✓	Outbreak Alert - Microsoft Outlook Elevat
☐	✓	Outbreak Alert - MSDT DogWalk Vulnerat
☐	✓	Outbreak Alert - Log4j2 Vulnerability Ever

Event handlers downloaded through the outbreak alerts service

Reports > Report Definitions

☐	Title ▾
☐	Outbreak Alert - Atlassian Information Disclosure Repd
☐	Outbreak Alert - BURNTCIGAR Malware Report
☐	Outbreak Alert - Cacti Command Injection Report
☐	Outbreak Alert - CISATop20_PRC2022 Report
☐	Outbreak Alert - CosmicEnergy Malware Report
☐	Outbreak Alert - CWP OS Command Injection Report

Reports downloaded through the outbreak alerts service

Once downloaded, the new handlers are available under the **Event Handler** list. The same management and configuration functions are available for these handlers as the system default and custom handlers. That is, you can clone them, export them, import them, and so on.

The same is true for the new reports.

DO NOT REPRINT
© FORTINET

Knowledge Check

1. The IOC engine analyzes new and historical logs against IOC signatures for which type of hosts?
✓ A. End users
B. Fabric devices
2. The threat hunting dashboard uses which database?
✓ A. SIEM
B. TIDB

DO NOT REPRINT
© FORTINET

Lesson Overview

-  Concepts, Definitions, and Incident Handling
-  Events, Event Handlers, and Incidents
-  Threat Hunting

FORTINET
Training Institute

© Fortinet Inc. All Rights Reserved. 43

Congratulations! You have completed this lesson.

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

DO NOT REPRINT
© FORTINET

Review

- ✓ Describe basic FortiAnalyzer SOC concepts, definitions, and features
- ✓ Analyze and manage events, and customize event handlers
- ✓ Analyze and create incidents
- ✓ Describe the threat hunting workflow
- ✓ Analyze threat hunting dashboards
- ✓ Analyze IOC information from compromised hosts
- ✓ Manage outbreak alerts

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

By mastering the objectives covered in this lesson, you learned how to analyze and manage events, customize event handlers, and analyze and create incidents. You also learned how to perform threat hunting on FortiAnalyzer, analyze IOC information from compromised hosts, and manage outbreak alerts.

DO NOT REPRINT
© FORTINET

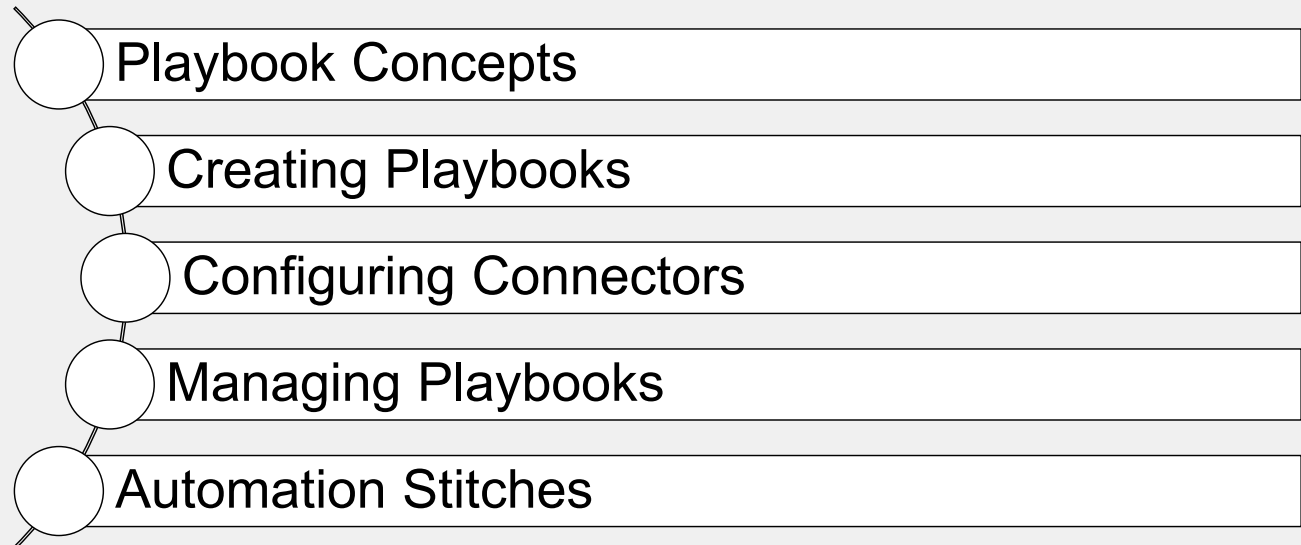


In this lesson, you will learn about the automation capabilities of FortiAnalyzer.

FortiAnalyzer integrates playbooks, connectors, and incidents that can be automated, so you can quickly identify and react to network security threats.

DO NOT REPRINT
© FORTINET

Lesson Overview



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

DO NOT REPRINT
© FORTINET

Playbook Concepts

Objectives

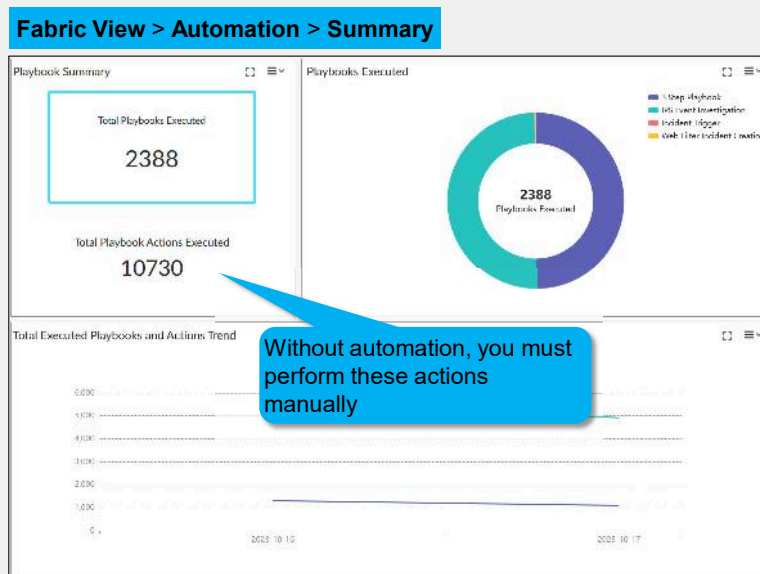
- Describe FortiAnalyzer automation capabilities
- Identify playbook components
- Describe trigger types and properties
- Describe playbook tasks

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

By demonstrating competence in understanding the purpose of playbooks and their components, you will be able to use playbooks effectively.

Why Automation?

- In general, the benefits of using automation include:
 - Improved productivity
 - Increased efficiency
 - Reduced costs
 - Fewer human errors
- In a SOC environment, the benefits of using playbooks results in:
 - Faster incident response time
 - Faster data analysis
 - Better use of analysts' time
 - Better compliance management
 - Consistent security posture



Automation is critical for security teams who are facing the ever-changing threat landscape. Generally speaking, automation improves productivity, reduces cost, increases efficiency, and minimizes human errors. In a SOC environment, these benefits provide, among other results, faster response time, faster data analysis, better use of analysts' time, better compliance management, and a more consistent security posture.

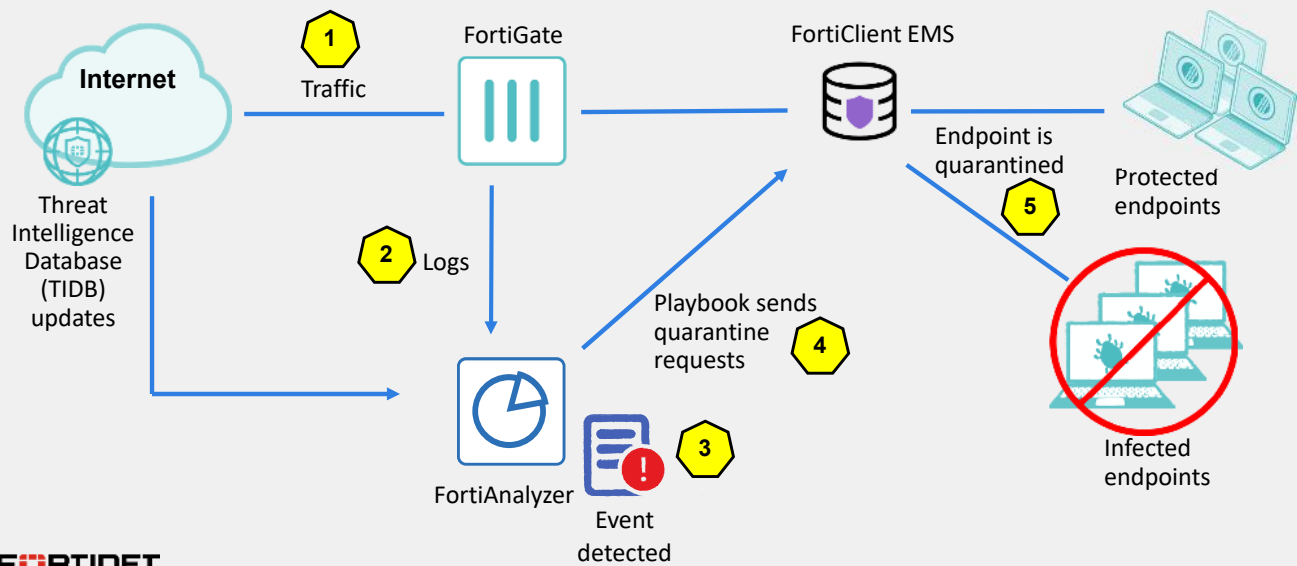
FortiAnalyzer allows SOC analysts to automate common and repetitive tasks using playbooks. FortiAnalyzer works with standalone devices, but it is also integrated with the Security Fabric. This integration allows FortiAnalyzer to communicate with other devices in the Security Fabric to detect security events, and trigger corrective or preventive actions automatically, by running automated playbooks.

For example, you can create playbooks that automatically generate a report, or instruct the FortiClient EMS server to quarantine a compromised host, just to mention two use cases. The available actions depend on the device type. Using devices that are compatible with the Security Fabric allows you to exploit their capabilities to their full extent.

In this lesson, you will learn more about these capabilities.

DO NOT REPRINT
© FORTINET

Automation With a Playbook



FORTINET
Training Institute

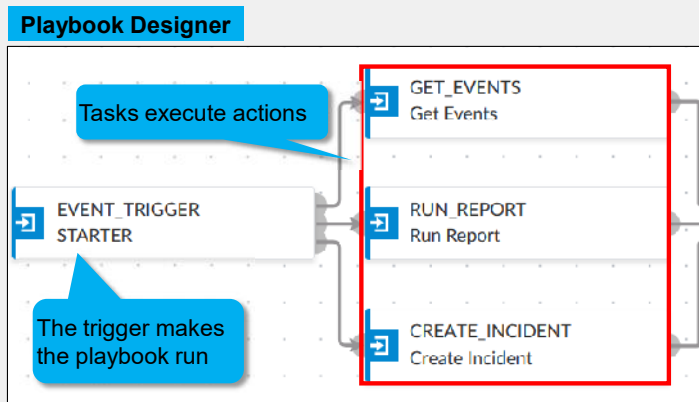
© Fortinet Inc. All Rights Reserved. 5

This slide shows an example of a playbook being used to automate tasks.

In this example, all network traffic traverses FortiGate. FortiGate sends all traffic and security logs to FortiAnalyzer. FortiAnalyzer detects suspicious activity and generates an event. This event triggers the execution of a playbook in FortiAnalyzer. The playbook sends a request to FortiClient EMS using the FortiClient EMS connector. FortiClient EMS then applies the corrective or preventive action.

Playbook Components

- Playbooks are ADOM-specific
- Each playbook has only one trigger
 - Determines when a playbook executes
- Playbooks have one or more tasks
 - Actions that will take place
- The actions that can be performed by a task depends on the connector
 - Different devices (connectors) allow different actions
- Playbooks can be created from built-in templates or from scratch



- Playbooks are created using an intuitive playbook designer
- Flow diagrams help you visualize the workflow

Playbooks include a starter event (trigger) that determines when a playbook runs, and one or more tasks that are executed.

After a playbook is triggered, it flows through the existing tasks defined within the playbook designer.

Each task includes the automated action that needs to take place. The available actions depend on the connector used. Connectors allow tasks to be performed on supported devices.

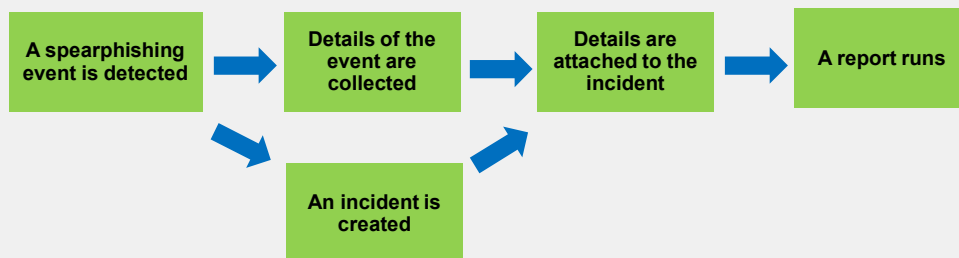
You can create playbooks from scratch or using predefined templates. Playbooks are available only in the ADOM where they were created, unless they are exported to a different ADOM.

Playbook Concepts

- A simple playbook execution sequence
 - Tasks run one after another



- Multiple tasks can be triggered
- Tasks can be sequential, or run in parallel



In the simplest design, a playbook consists of a trigger and a series of tasks that are executed one after the other. However, playbooks also allow for more complex designs that involve multiple tasks running simultaneously. Additionally, if needed, the output of one task can be used by the tasks that follow it.

For example, one task can collect specific events and the following task can add those events to an incident.

Triggers

Trigger type	Description
EVENT_TRIGGER	The playbook is run when an event is created that matches the configured filters When no filters are set, all events will trigger the playbook
INCIDENT_TRIGGER	The playbook is run when an incident is created that matches the configured filters When no filters are set, all incidents will trigger the playbook
ON_SCHEDULE	The playbook is run during the configured schedule You can define the start time, end time, interval type, and interval frequency for the schedule
ON_DEMAND	The playbook is run when it is manually started by an administrator

Every playbook starts with a trigger that determines when the playbook is executed. Each playbook can include only one trigger. After a playbook is triggered, it flows through the configured tasks, as defined in the playbook designer.

The event, incident, and on-schedule triggers are automatic and activates when specific conditions are met. You can use the on-schedule trigger for manual playbook execution.

Note that playbooks with the ON_SCHEDULE trigger can also be executed manually. This allows you to test them outside of their configured timeframe.

Triggers (Contd)

- Use more than one condition to limit playbook execution
- Apply logic to determine when and how conditions trigger events
 - Apply AND logic to enforce the rule that *all* conditions must match
 - Apply OR logic to enforce the rule that *any* conditions must match
- ON_SCHEDULE triggers parameters are all based on timeframes
- ON_DEMAND triggers have no extra configurable parameters

Fabric View > Automation > Summary

Example

The trigger type determines the options you can configure to control *when* the playbook will run. For example, you can configure an event trigger to run only when FortiAnalyzer detects an event with a particular event handler.

When configuring multiple conditions for a trigger, you can specify whether all conditions must match or any one condition must match.

Tasks

- Tasks are actions that are executed when the playbook runs
- Available actions depend on the connector
- Chain one task to another task to execute a sequence of actions
- The output of a task can be used as an input for the next task in the sequence

Fabric View > Automation > Playbook

FortiAnalyzer

FortiOS

EMS

FortiMail

FortiGuard

FCASB

ServiceNow

MS_TEAMS

Name: Task 1

Description: Demo Task

Connector: Local Connector

This connector is auto-selected selection.

Action:

None

Update Asset and Identity

Get Events

Get Endpoint Vulnerabilities

Create Incident

Update Incident

Attach Data to Incident

Run Report

RUN_REPORT
Run Report

ATTACH_DATA_TO_INCIDENT
Attach Report to Incident

GET_EVENTS
Get Events

ATTACH_DATA_TO_INCIDENT
Attach Event to Incident

Tasks are actions that are executed when the playbook runs. Each trigger event can start the execution of one or more tasks, and each task can perform one action.

You can also configure tasks so that the output of one task is used as an input by another task in sequence. For example, you can create a task to retrieve some data, and then provide that data to the next task for report generation.

When adding a new task, you must choose a relevant connector before you can select an action. On this slide, the actions associated with the local connector are shown. The available actions will vary depending on the connector type that you select.

You can configure tasks to use the default preconfigured values, or take inputs from the trigger or from preceding tasks. You must configure automation rules on FortiGate before you can see the list of available actions on FortiOS connectors.

DO NOT REPRINT
© FORTINET

Knowledge Check

1. Which trigger type must you use to manually run a playbook?
☐ A. Event_Trigger
☒ B. On_Demand
2. Which playbook element determines the available actions a task can perform?
☒ A. Connectors
☐ B. Trigger type

DO NOT REPRINT
© FORTINET

Lesson Progress



Playbook Concepts



Creating Playbooks



Configuring Connectors



Managing Playbooks



Automation Stitches

Good job! You now understand playbook concepts.

Now, you will learn how to create playbooks on FortiAnalyzer.

DO NOT REPRINT
© FORTINET

Creating Playbooks

Objectives

- Create new playbooks from a template
- Customize playbook settings
- Create new playbooks from scratch
- Use variables in tasks

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

By demonstrating competence in automating tasks with playbooks, you will be able to increase the efficiency of your organization's SOC operations.

Creating Playbooks From a Template

- FortiAnalyzer includes several playbook templates
- You can customize the playbooks created from these templates to fit your needs

Fabric View > Automation > Playbook

Summary	Connectors	Playbook	Playbook Monitor
+ Create New ▶ Run ✎ Edit 🗑 Delete ✔ Enable			
☐	Name ↕		
☐	Incident Trigger		
☐	Sample Playbook		

Explore the available templates before creating a playbook from scratch since they cover many common scenarios (not all templates are shown)

-  **Attach Endpoint Vulnerability list to incident**
Playbook to collect the list of endpoint vulnerabilities from logs and attach to incident.
-  **Compromised Host Incident**
Playbook to create incident on FortiAnalyzer for detected compromised hosts by IoC feature.
-  **Critical Intrusion Incident**
Playbook to create incident on FortiAnalyzer for detected critical intrusions by IPS
-  **Enrich Incident with Process List**
Playbook to get running processes on endpoint by EMS connector and attach to incident.
-  **Enrich Incident with Software Inventory**
Playbook to get software inventory from endpoint by EMS Connector and attach to incident.
-  **Enrich Incident with Vulnerability List**
Playbook to collect the list of endpoint vulnerabilities from logs and attach to incident.
-  **Quarantine Endpoint by EMS**
Playbook to quarantine endpoint by EMS connector
-  **Quarantine Endpoint by FortiOS**
Playbook to quarantine endpoint by FOS connector providing MAC address or FortiClient UID

FORTINET
Training Institute

© Fortinet Inc. All Rights Reserved. 14

FortiAnalyzer includes several playbook templates that SOC analysts can customize. You can use the templates to perform tasks such as:

- Investigate compromised host incidents and critical intrusion incidents.
- Enrich data for assets and identity, and for hosts under investigation.
- Block command-and-control (C&C) IP addresses.
- Quarantine and run antivirus scans on endpoints.

Customizing Playbook Settings

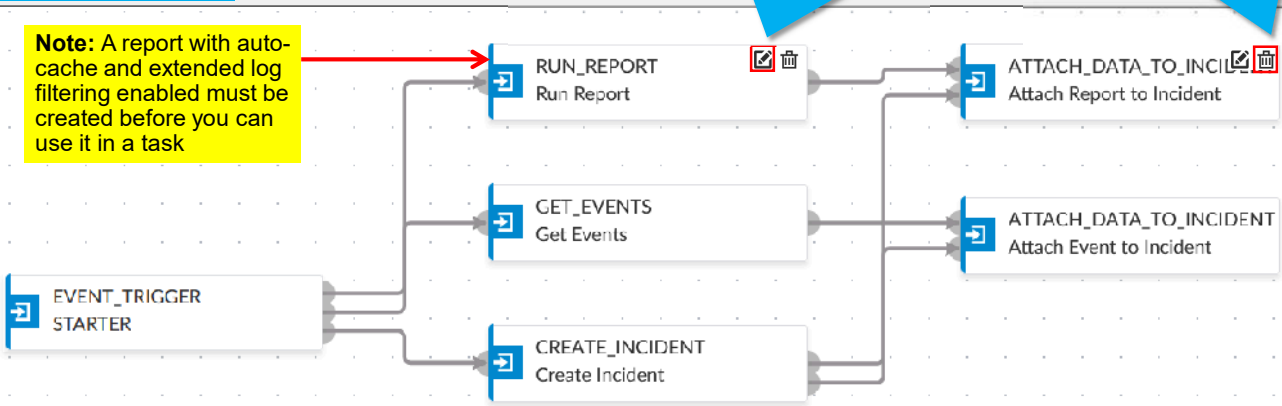
- A new playbook created from a template is preloaded with all required components
- You can remove or customize tasks to meet your needs

Playbook Designer

Note: A report with auto-cache and extended log filtering enabled must be created before you can use it in a task

Edit tasks to meet your requirements

Remove tasks not needed



FORTINET
Training Institute

© Fortinet Inc. All Rights Reserved. 15

After you select a playbook template, the playbook designer is displayed with a preconfigured trigger and one or more tasks. The preconfigured trigger and tasks will be different, based on the template you select. You can configure, add, or remove tasks to customize the playbook.

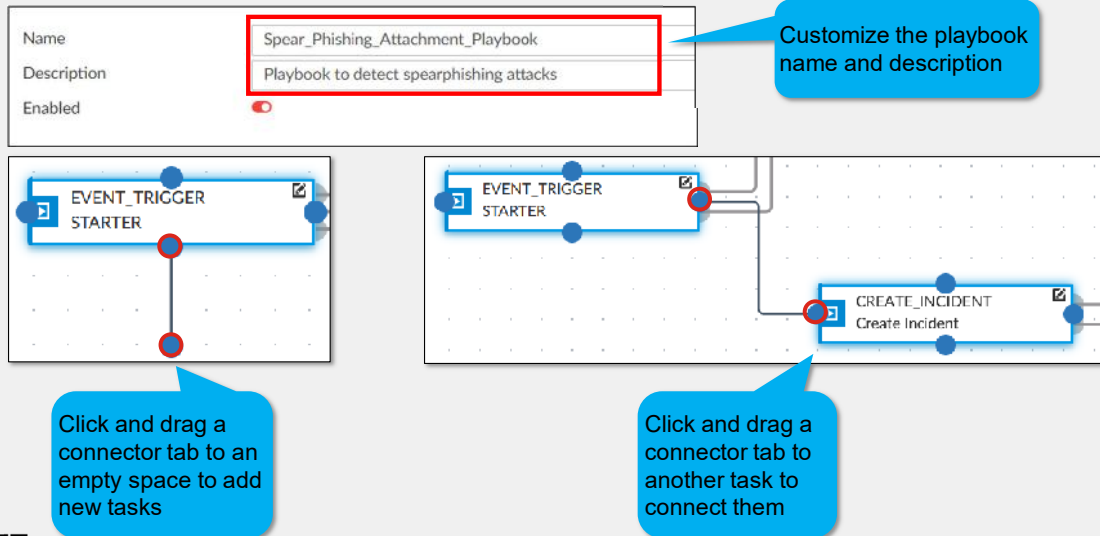
This slide shows an example of a playbook that will:

- Run when the specified event or events are generated.
- Create a new incident.
- Retrieve the list of events specified in the task filter and add them to the incident.
- Run a report and attach it to the incident.

After this playbook runs, the incident will include relevant information that the analyst can use during an incident investigation. Note that before configuring a task to run a report, you must verify that the report exists, and that the auto-cache and extended log filtering settings are enabled.

Customizing Playbook Settings (Contd)

Fabric View > Automation > Playbook



By default, every new playbook you create from a template is preconfigured with a generic name and time stamp. This can make them difficult to distinguish, so it's highly recommended that you edit the names and descriptions of new playbooks to something easily recognizable.

To add new tasks, click and drag the connector tabs attached to the current tasks or the trigger. This creates an empty task that you can configure. To connect tasks to each other or to the trigger, click and drag a connector tab onto another connector tab.

DO NOT REPRINT
© FORTINET

Creating a New Playbook From Scratch

Fabric View > Automation > Playbook

Summary Connectors **Playbook** Playbook Monitor

+ Create New Run Edit Delete Enable

Choose from Playbook Templates

- New Playbook created from scratch**
Custom build playbook to get started
- Attach Endpoint Vulnerability list to incident
Playbook to collect the list of endpoint vulnerab

Edit Playbook

Name: New Playbook created from scratch
Description: Custom build playbook to get started
Enabled: ☒

ON_DEMAND
Select a Step

TRIGGERS

- EVENT_TRIGGER
- INCIDENT_TRIGGER
- ON_SCHEDULE
- ON_DEMAND

Server error: FAZ is parsing the recent created playbook: 301f3fc9-7831. Please wait for about 5 minutes

FortiAnalyzer needs a few minutes to parse a newly created playbook

FORTINET
Training Institute

© Fortinet Inc. All Rights Reserved. 17

If none of the templates fits your needs, you can always create a playbook from scratch.

First, you must select a trigger. For some triggers, you can add filters to make sure that the playbook runs only if a specified condition is matched.

You must configure a task or multiple tasks that you want to execute. You can also configure filters to limit the action scope which will reduce unnecessary data processing. For example, when you configure a task to retrieve events, configure a filter to retrieve events generated by a specific event handler, or events with a specific severity.

Also, keep in mind that after you create a new playbook, FortiAnalyzer needs a few minutes to parse it. If you try to run a newly created playbook configured with an on-demand trigger *before* it is parsed, FortiAnalyzer generates an error message as shown on this slide.

Variables

- You can use output variables and trigger variables in playbook tasks
- Output variables: Output of previous task is the input of current task
 - Format: `${task_id.output}`
 - Previous task ID *required*
- Trigger variables: Use some of the information from the trigger to filter the action in the task
 - Format: `${trigger.variable}`

The screenshot shows the 'Fabric View > Automation > Playbook' configuration interface. On the left, a task flow diagram shows an 'INCIDENT_TRIGGER STARTER' followed by a 'RUN_REPORT Run Report' task. A blue callout bubble points to the 'RUN_REPORT' task with the text 'Second task generates a report'. Below the 'RUN_REPORT' task is a dashed red box labeled 'New Task'. On the right, the configuration details for the 'New Task' are shown. The 'Name' is 'Attach Data', 'Description' is 'Attach Data', 'Connector' is 'Local Connector', and 'Action' is 'Attach Data to Incident'. The 'Incident ID' is set to 'Playbook Starter' with a dropdown arrow, and the 'Attachment' is set to 'Run Report' with a dropdown arrow. A red box highlights the 'Incident ID' and 'Attachment' fields. A blue callout bubble points to the 'Attachment' field with the text 'The new task uses an output variable. On the left is the report task ID, and on the right is the output of the report task (the actual report)'.

Second task generates a report

New Task

Fabric View > Automation > Playbook

Name: Attach Data
Description: Attach Data
Connector: Local Connector
Action: Attach Data to Incident

Incident ID: Playbook Starter
Attachment: Run Report

The new task uses an output variable. On the left is the report task ID, and on the right is the output of the report task (the actual report)

© Fortinet Inc. All Rights Reserved. 18

You can use variables when configuring tasks. There are two types of playbook variables: output variables and trigger variables.

Use output variables to take the output from a preceding task as an input for the current task. An output variable consists of the task ID, followed by the task output, as shown on this slide.

The example shown on this slide shows a task configured to use a report as an input from a preceding task to update an incident.

Use trigger variables to take information from the trigger step of a playbook configured with an event or incident trigger. For example, a playbook configured with a report action requires filtering based on an endpoint IP address. You can retrieve this information from the triggering event using a trigger variable.

DO NOT REPRINT
© FORTINET

Knowledge Check

1. Which type of variable takes the output of a preceding task as the input of a current task?
 - A. Trigger variable
 - ✓ B. Output variable

DO NOT REPRINT
© FORTINET

Lesson Progress



Playbook Concepts



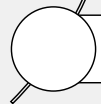
Creating Playbooks



Configuring Connectors



Managing Playbooks



Automation Stitches

Good job! You now understand how to create playbooks.

Now, you will learn about configuring connectors.

DO NOT REPRINT
© FORTINET

Configuring Connectors

Objectives

- Describe connector types
- Configure connector actions

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

By demonstrating competence in connectors, you will understand how FortiAnalyzer uses connectors in conjunction with playbooks to automate actions to be performed on other Fortinet devices.

DO NOT REPRINT
© FORTINET

Connectors

- Allow playbooks to interact with devices in the Security Fabric and other standalone devices
- Determine which actions can be performed by playbook tasks
- The local connector does not need any additional configuration
 - All other connector types must be configured
- The connector status icon is colour coded:
 - **Green**: connection successful
 - **Black**: connection unknown
 - **Red**: connection down

Fabric View > Automation > Connectors

FortiOS connector		
FortiOS Connector		
Training-Lab		
Automation Rule	Automation Action(s)	Parameters
Lab5 webhook disable FW policy	Lab 5 disable firewall policy	policyid
Lab5 webhook enable FW policy	Lab 5 enable firewall policy	policyid
Local Host connector		
Local Connector		
FortiGuard connector		
FortiGuard Connector		

Status icon

FORTINET
Training Institute

© Fortinet Inc. All Rights Reserved. 22

Connectors determine which automated actions playbooks can perform. Each connector type supports different actions.

You can quickly determine the API connection status of a connector, which is indicated by a colored status icon.

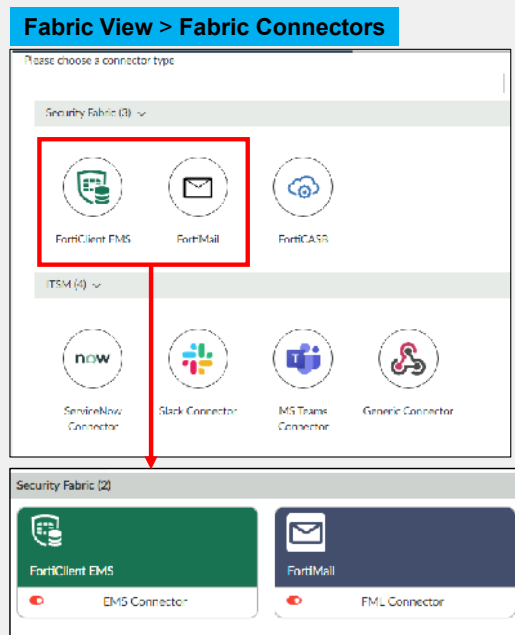
By default, you can use the local connector in playbooks without any additional configuration. All other connectors require additional configuration.

For example, the FortiOS connector is listed as soon as you add the first FortiGate device to FortiAnalyzer. However, to see the actions related to that FortiOS connector, you must enable an automation rule using an incoming webhook call trigger on the FortiGate device.

DO NOT REPRINT
© FORTINET

Connector Types

- Two types of connectors
 - Security Fabric
 - ITSM
- Security Fabric connectors:
 - FortiClient EMS
 - FortiMail
 - FortiCASB
- ITSM connectors:
 - Service Now
 - Slack
 - MS Teams
 - Generic: Support additional third-party ticketing platforms



FORTINET
Training Institute

© Fortinet Inc. All Rights Reserved. 23

On FortiAnalyzer, there are two types of connectors that you can configure on the **Fabric Connectors** page: Security Fabric and IT service management (ITSM)

Security Fabric connectors include FortiClient EMS, FortiMail, and FortiCASB connectors.

ITSM connectors include connecting to third-party service management or ticketing software such as Service Now, Slack, MS Teams, and so on. FortiAnalyzer also supports a generic connector type to facilitate integration with additional third-party ticketing software.

Connector Actions

- Connector actions are automated
- Each connector has its own set of actions
- Connector actions are predefined

Fabric View > Fabric Connectors

Configuration Action

Status	Name	Description	Filters/Parameters
Enabled	AV_FULL_SCAN	run full system scan on endpoints	id: cmd: av_full_scan
Enabled	AV_QUICK_SCAN	run quick system scan on endpoints	id: cmd: av_quick_scan
Enabled	GET_ENDPOINTS	retrieve list of endpoints and all of their...	id: cmd: get_endpoint
Enabled	GET_PROCESSES	retrieve list of running processes on en...	id: cmd: get_processes
Enabled	GET_SOFTWARE_INVENTORY	retrieve list of software and apps inst...	id: cmd: get_software_inventory
Enabled	QUARANTINE	quarantine endpoints	id: cmd: quarantine
Enabled	TAG_ENDPOINTS	tag endpoints on LMS	id: cmd: tag_endpoints
Enabled	UNQUARANTINE	unquarantine endpoints	id: cmd: unquarantine
Enabled	UNTAG_ENDPOINTS	untag endpoints on LMS	id: cmd: untag_endpoints
Enabled	VULN_SCAN	run vulnerability scan on endpoints	id: cmd: vuln_scan

FortiClient EMS
connector actions

Configuration

Action

Search...

Status	Name	Description	Filters/Parameters
Enabled	GET_EMAIL_STATISTICS	retrieve information of e...	id: cmd:
Enabled	GET_SENDER_REPUTA...	retrieve information suc...	id: cmd:
Enabled	ADD_SENDER_TO_BLO...	discard email received fro...	id: cmd:

99% 3

FortiMail
connector
actions

Each connector has its own set of predefined actions. These actions are automated and are performed in playbooks.

An example of when you might use a connector action in your network is to have a FortiClient EMS connector regularly retrieve a list of endpoints or perform quarantine actions on compromised endpoints.

All connector actions are predefined and cannot be modified.

Use Case

Fabric View > Automation > Playbooks

Name: Quarantine Endpoint by EMS
Description: Playbook to quarantine endpoint by EMS connector
Enabled: ☒

1

2

3

4

Manually Run Playbook Quarantine Endpoint by EMS

Endpoint: WIN (1031)
site: default
fctuid: CDABAF17B3724E72AA20B3D6E4B26948
incid: IN00000003

Playbook Tasks

Task ID	Task	Status	Raw Log
faz_attach_action_status_to_incident	Attach Status	success	Unavailable
ems_quarantine_endpoint	Quarantine Endpoint	success	Unavailable

Infected host is quarantined

Fabric View > Automation > Playbook Monitor

Job ID	Playbook	Trigger	Start Time	End Time	Status
2024-03-13 19:07:07-07	Quarantine Endpoint by EMS	user(admin)	2024-03-13 19:07:11-0700	2024-03-13 19:24:11-0700	Success[Scheduled:0/Running:0/Success:1]

FORTINET
Training Institute

© Fortinet Inc. All Rights Reserved. 25

This slide shows an example of a playbook using the FortiClient EMS connector.

FortiAnalyzer has generated an event indicating that a host is infected after downloading a malicious file. The analyst has configured a playbook with a FortiClient EMS connector to quarantine infected hosts.

The analyst performs the following actions:

- 1) Manually run the playbook because it is configured for an on-demand trigger.
- 2) Input the FortiClient host details, including endpoint number, FortiClient UID, FortiClient site, and an existing incident ID.

The playbook automates the following actions:

- 1) Execute a quarantine task on the infected host using the FortiClient EMS connector, and attach all related data to the incident.
- 2) Quarantine the host so the malicious file cannot move laterally and infect other hosts in the network.

DO NOT REPRINT
© FORTINET

Knowledge Check

1. Which connector requires additional configuration?
✓ A. FortiOS connector
B. Local connector
2. Which connector type allows integration with third-party ticketing applications?
A. Security Fabric
✓ B. ITSM

DO NOT REPRINT
© FORTINET

Lesson Progress

-  Playbook Concepts
-  Creating Playbooks
-  Configuring Connectors
-  Managing Playbooks
-  Automation Stitches

Good job! You now know how to configure connectors.

Now, you will learn about managing playbooks and connectors on FortiAnalyzer.

DO NOT REPRINT
© FORTINET

The slide features a light gray background with abstract geometric shapes in red, gray, and teal. A grid of small dots is positioned to the right of the title. The Fortinet logo is in the bottom left, and copyright information is in the bottom right.

Managing Playbooks

Objectives

- Monitor playbooks
- Export and import playbooks
- Review the mock threat report

FORTINET
Training Institute

© Fortinet Inc. All Rights Reserved. 28

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

By demonstrating competence in monitoring playbooks, you will be able to identify whether all automated tasks ran successfully. You will also be able to export playbooks to another ADOM or device.

Monitoring Playbooks

- To see the playbook execution logs, click **Details** and then **View Log**

Fabric View > Automation > Playbook Monitor

Playbook	Trigger	Start Time	End Time	Status	Details
Spear_Phishing_Attachment_Playbook	event(202403131000	2024-03-13 06:31:00-0700	2024-03-13 06:31:06-0700	failed(Scheduled:0/Running:0/Success:1/Failed:2)	

This playbook has three tasks: One task is successful but the other two failed

Fabric View > Automation > Playbook Monitor

Task ID		Task	Start Time	End Time	Status
☐	placeholder_4c03461e_adea_4970_8029_3abcb	Attach_Data_To_Incident	2024-03-13 06:31:05-0700	2024-03-13 06:31:05-0700	upstream failed
☒	placeholder_00f4d7f1_fac5_4354_a60a_3127ad	Incident_Spear_Phishing	2024-03-13 06:31:04-0700	2024-03-13 06:31:05-0700	failed
☐	placeholder_32b07c26_d3e6_4915_9891_f4b0	Get_Events	2024-03-13 06:31:02-0700	2024-03-13 06:31:05-0700	success

This task failed because it did not receive the input it was expecting from a preceding task

When you troubleshoot playbooks, you must review the logs. Details about the execution of a playbook are available in the associated log.

In the playbook monitor, all playbook jobs that include one or more failed tasks are assigned a failed status. A failed status, however, does not mean that all tasks in the playbook failed. Other task actions in the playbook may execute successfully.

In the example shown on this slide, the spearphishing attachment playbook has three configured tasks, two of which failed to run—incident spearphishing and attach data to incident. Therefore, the playbook job is considered to have failed.

Monitoring Playbooks (Contd)

Fabric View > Automation > Playbook Monitor

		Search...			
☐	Task ID	Task	Start Time	End Time	Status
☐	placeholder_4c03461e_adea_4970_8029_3abcb	Attach Date to Incident	2024-03-13 06:31:05-0700	2024-03-13 06:31:05-0700	upstream failed
☒	placeholder_00f4d7f1_fac5_4354_a60a_3127a6	Incident Spear Phishing	2024-03-13 06:31:04-0700	2024-03-13 06:31:05-0700	failed
☐	placeholder_32b07c26_d3e6_4915_9891_f4b02	Get Events	2024-03-13 06:31:02-0700	2024-03-13 06:31:05-0700	success

View the raw logs for failed playbooks to see more details

```
[2024-03-13T06:31:05.246-0700] {taskinstance.py:1937} ERROR - Task failed with exception
Traceback (most recent call last):
  File "/drive0/private/airflow/plugins/incident_operator.py", line 218, in execute
    self.epid = int(self.epid)
    ^^^^^^^^^^^^^^^^^
ValueError: invalid literal for int() with base 10: '100.64.1.20'
[2024-03-13T06:31:05.331-0700] {standard_task_runner.py:104} ERROR - Failed to
execute job 417 for task placeholder_00f4d7f1_fac5_4354_a60a_3127a6bc5cc7 (invalid
literal for int() with base 10: '100.64.1.20'; 1851)
```

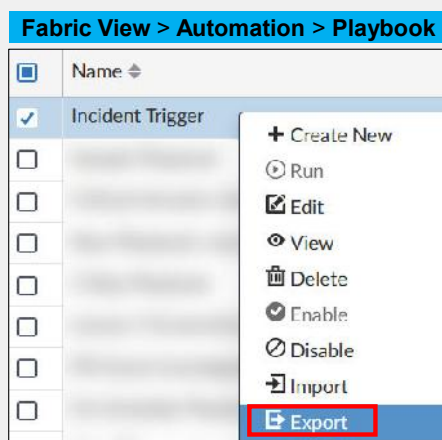
This playbook failed because a task was expecting an integer value for the `epid` variable, but received a Base 10 value (IP address) instead

To determine where exactly the task execution failed, you must view the raw logs.

The example on this slide shows the raw logs for the incident spearphishing task. The raw logs indicate that the task is expecting an integer value input for the `epid` variable but received a Base 10 IP address instead.

Exporting Playbooks

- Playbooks are defined per ADOM
- Export playbooks to use them in a different ADOM or FortiAnalyzer device
- You can include the connectors in the exported file
- The exported file is in JSON format
 - You can also compress the file



Including the connectors ensures all required components are exported



Playbooks are defined per ADOM. If you want to use an existing playbook in a different ADOM or a different FortiAnalyzer device, you must export the playbook.

To export a playbook, right-click the playbook, and then click **Export**. You can export more than one playbook at a same time by selecting multiple playbooks.

When exporting a playbook, you can choose to export the connectors. Connectors required to run the playbook will be included in the exported file. This will preserve the connector configuration with the playbook configuration.

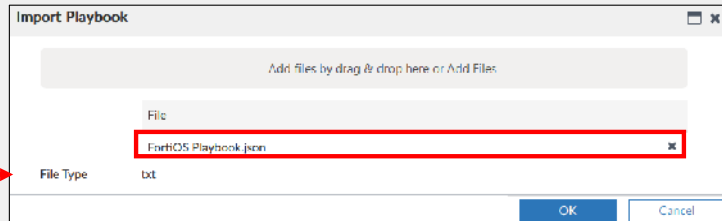
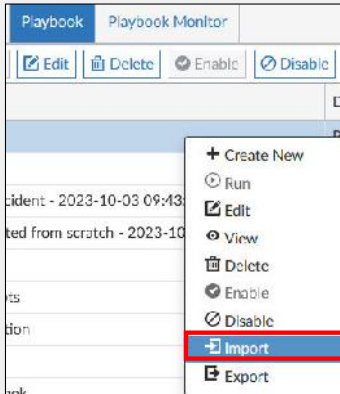
You can export the playbook in two formats: plain text JSON or zipped base 64 encoded JSON. If you want a human-readable file, then you must choose the text version during the export process.

DO NOT REPRINT
© FORTINET

Importing Playbooks

- Import a previously exported playbook on the destination ADOM or device

Fabric View > Automation > Playbook



FORTINET
Training Institute

© Fortinet Inc. All Rights Reserved. 32

To import a playbook, right-click anywhere on the playbook dashboard, and then click **Import**.

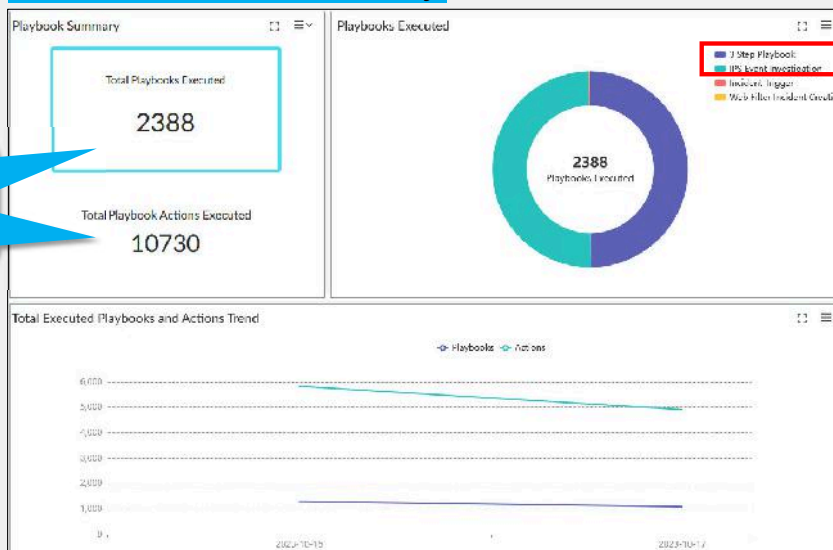
If the imported playbook has the same name as an existing playbook, to avoid conflicts, FortiAnalyzer will append a timestamp to the imported playbook name.

Playbooks are imported with the status they had (enabled or disabled) when they were exported. Playbooks with automatic triggers (incident or event) should be exported while they are disabled, to prevent the playbook from unintentionally running after import.

Playbooks Dashboard

- This dashboard tracks all playbooks executed in the last seven days

Fabric View > Automation > Summary



A playbook can have multiple actions

These two playbooks have run more than all of the other playbooks, which could be normal or caused by a misconfiguration

The playbook dashboard shows the number of playbooks executed, which playbooks have executed, playbook actions executed, and any trends in the total executed playbooks and actions.

This dashboard shows all the playbooks that have been executed in the last seven days, including their names, and the total number of actions performed. This information gives you an idea of how much time has been saved by automating tasks.

In the example shown on this slide, 2388 playbooks have been executed. However, 10,730 actions have been taken. This shows that one or more of the playbooks listed have more than one action configured. The image also shows the names of the most frequently executed playbooks. It is the responsibility of the SOC analyst to ensure playbooks are correctly configured so they run only when required.

DO NOT REPRINT
© FORTINET

Use Case—Healthcare Sector



Your organization is a hospital targeted by cybercriminals through a phishing attack to ransom private data

Threat: Potential breach exposing thousands of patients' data and putting patients at risk.

Our goal: *Automate actions using playbooks and connectors on FortiAnalyzer*

Domain: Enterprise

Attacker: Group ABC



In the healthcare sector story from *Lesson 1—SOC Concepts and Security Frameworks*, the blue team prepares to automate their actions using playbooks and connectors on FortiAnalyzer.

Blue Team Plan of Action—Automation



- Configure playbooks to run because of the following detection events:
 - Probing attacks that target email systems in search of valid email accounts
 - Spearphishing emails with attached malicious Microsoft Office macro-enabled files
- Configure the FortiClient EMS connector and playbooks to automate the following tasks:
 - Retrieve a list of all endpoints with FortiClient site and UUID information
 - Quarantine identified compromised host (*containment*)
 - Release sanitized host from quarantine (*recovery*)



Using their knowledge of playbooks on FortiAnalyzer, the blue team configures playbooks to run when an event handler triggers by identifying probing attacks by Group ABC. The *probing attack targets email systems in search of valid email accounts*. The blue team also configures playbooks to automatically run when an event is created after detecting *spearphishing* emails that contain an *attached malicious Microsoft Office macro-enabled file*. These playbooks create incidents that can be used to track and follow the investigation into these attacks. The playbooks also attach data from events created by the corresponding event handlers to these incidents for easy access.

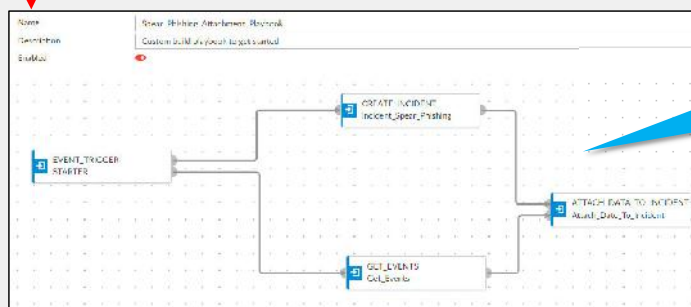
The blue team uses their knowledge of connectors on FortiAnalyzer to configure the FortiClient EMS connector. This automatically creates several playbooks, one of which the blue team uses to retrieve a list of all endpoints that include important data such as the FortiClient site and FortiClient UUID, which are updated in the FortiAnalyzer Asset Identity Center. The blue team also configures a playbook to use in the *containment* phase of incident handling. The containment phase playbook quarantines the identified compromised host following an investigation into the malicious file download. Finally, the blue team configures a playbook to use in the *recovery* phase of incident handling. The recovery playbook releases the sanitized host from quarantine.

Blue Team Plan of Action—Playbooks

Fabric View > Automation > Playbook

☐	Name	Description	Status	Created Time
☐	Spearphishing Attack Incident Playbook	Custom build playbook to get started	Enabled	02/08/2024
☐	SOC SMTP Enumeration Playbook	Playbook to generate Incident and add event data for SMTP Enumeration even...	Enabled	Yesterday at 3:00 AM
☐	Update Asset and Identity Database (EMS Connector)	Playbook to automatically update FortiAnalyzer Asset and Identity database...	Enabled	Last Sunday at 11:35 PM
☐	Get Vulnerabilities from EMS (EMS Connector)	Playbook to get vulnerabilities from EMS	Enabled	Last Sunday at 11:35 PM
☐	Get Software Inventory from EMS (EMS Connector)	Playbook to get software inventory from EMS	Enabled	Last Sunday at 11:35 PM
☐	Quarantine Endpoint by EMS	Playbook to quarantine endpoint by EMS connector	Enabled	Yesterday at 5:21 AM
☐	Unquarantine Endpoint by EMS	Playbook to unquarantine endpoint by EMS connector	Enabled	Yesterday at 5:40 AM

List of playbooks created by the blue team to detect attacks, and to quarantine and release hosts



Playbook configured to detect a spearphishing event

This slide shows all the playbooks that the blue team configures in response to the threat report about the Group ABC attack. These include a playbook that will run if FortiAnalyzer detects a reconnaissance tactic attempting to gather victim identity information through SMTP enumeration, as well a playbook that will trigger if FortiAnalyzer detects a spearphishing event. The list of playbooks also include quarantine and unquarantine playbooks that FortiAnalyzer will run using the FortiClient EMS connector during the *containment* and *recovery* phases of incident handling.

The slide shows an example of the blue team's spearphishing attack playbook.

Blue Team Plan of Action—Playbooks (Cont)

Fabric View > Automation > Playbook

Job ID	Playbook	Trigger	Start Time	End Time	Status
2024-03-11 02:35:40.462977-07	Update Asset and Identity Database (EMS Connector)		2024-03-12 02:35:40-0700	2024-03-12 02:35:47-0700	Success/Scheduled/Running/Success/2/Fail
2024-03-11 02:35:40.204669-07	Get Vulnerabilities from EMS (EMS Connector)		2024-03-12 02:35:40-0700	2024-03-12 02:35:45-0700	Success/Scheduled/Running/Success/1/Fail
2024-03-11 02:35:40.203954-07	Get Software Inventory from EMS (EMS Connector)		2024-03-12 02:35:40-0700	2024-03-12 02:35:45-0700	Success/Scheduled/Running/Success/1/Fail
2024-03-11 07:27:35-07	Update Asset and Identity Database (EMS Connector)	user(admin)	2024-03-11 07:27:38-0700	2024-03-11 07:27:43-0700	Success/Scheduled/Running/Success/1/Fail
2024-03-11 05:45:37-07	Unquarantine Endpoint by EMS	user(admin)	2024-03-11 05:45:40-0700	2024-03-11 05:45:45-0700	Success/Scheduled/Running/Success/3/Fail
2024-03-11 05:41:57-07	Unquarantine Endpoint by EMS	user(admin)	2024-03-11 05:42:00-0700	2024-03-11 05:42:05-0700	Success/Scheduled/Running/Success/1/Fail
2024-03-11 05:30:00-07	Quarantine Endpoint by EMS	user(admin)	2024-03-11 05:30:03-0700	2024-03-11 05:30:08-0700	Success/Scheduled/Running/Success/2/Fail
2024-03-11 05:22:57-07	Update Asset and Identity Database (EMS Connector)	user(admin)	2024-03-11 05:23:00-0700	2024-03-11 05:23:06-0700	Success/Scheduled/Running/Success/2/Fail
2024-03-11 04:11:23.830909-07	Spear_Phishing_Attachment_Playbook	event(202403111000)	2024-03-11 04:11:24-0700	2024-03-11 04:11:27-0700	Success/Scheduled/Running/Success/3/Fail
2024-03-10 01:35:40.462977-08	Update Asset and Identity Database (EMS Connector)		2024-03-11 02:35:40-0700	2024-03-11 02:35:47-0700	Success/Scheduled/Running/Success/2/Fail

All the playbooks that were run when FortiAnalyzer detected different attacks from the adversary Group ABC

Task ID	Task	Start Time	End Time	Status
task_id_4_03461e_ues_1970_3029_3020	Attach Date To Incident	2024-03-11 04:11:27-0700	2024-03-11 04:11:27-0700	success
task_id_5_2300a_24_0346_1915_3887_11000	Get Files	2024-03-11 04:11:29-0700	2024-03-11 04:11:29-0700	success
playbook_004e7f1_fac5_4374_astb_31276	Incident_Spear_Phishing	2024-03-11 04:11:25-0700	2024-03-11 04:11:26-0700	success

Incident Number	Incident Date / Time	Last Update Date / Time	Incident Reporter	Incident Category	Severity	Status	Affected Endpoint
INC00000002	2024-03-11 04:11:26	2024-03-11 05:45:44	Spear_Phishing_Attachment_Playbook	Unquarantined			
INC00000001	2024-03-08 08:05:40	2024-03-08 08:05:40	admin				

Incident auto generated by spearphishing playbook that was configured by the blue team

Audit History	
2024-03-11 04:11:26	NEW
Comment Attached to ...	
By Playbook: Unquarantine Incident by SPC	
Comment Attached to ...	
By Playbook: Quarantine Incident by SPC	
Events Attached to Inc...	
By Playbook: Spear_Phishing_Attachment_Playbook	
New Incident Created	
By Playbook: Spear_Phishing_Attachment_Playbook	
STRT	2024-03-11 04:11:26

This slide shows all the playbooks that were run on FortiAnalyzer during the Group ABC attack. This includes playbooks that were run to identify the SMTP enumeration attempts to gather victim identity information. A playbook was also run when a spearphishing attachment was detected by FortiSandbox.

The slide also shows the quarantine and unquarantine playbooks that were run using the FortiClient EMS connector to quarantine the infected host and then later to remove the sanitized host from quarantine.

It also includes the incident that was automatically generated when the spearphishing playbook was run to monitor the attack. The incident audit history shows the timeline of every action that was performed on this incident.

DO NOT REPRINT
© FORTINET

Knowledge Check

1. Which two playbook export formats are supported?
☒ A. JSON, ZIP
☐ B. CSV, YAML
2. When exporting playbooks, which connector configuration can you also export?
☐ A. Local connector
☒ B. FortiClient EMS connector

DO NOT REPRINT
© FORTINET

Lesson Progress

-  Playbook Concepts
-  Creating Playbooks
-  Configuring Connectors
-  Managing Playbooks
-  Automation Stitches

FORTINET
Training Institute

© Fortinet Inc. All Rights Reserved. 39

Congratulations! You have completed this lesson.

Now, you will learn about automation stitches between FortiAnalyzer and FortiGate.

DO NOT REPRINT
© FORTINET

Automation Stitches

Objectives

- Describe FortiAnalyzer and FortiGate automation stitches
- Configure an automation stitch
- Configure an event handler with an automation stitch enabled

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

By demonstrating competence in understanding the purpose of playbooks and their components, you will be able to configure automation stitches between FortiAnalyzer and FortiGate.

FortiAnalyzer and FortiGate Automation Stitch

- FortiAnalyzer can activate an automation stitch on authorized FortiGate devices
- An event handler must have the automation stitch option enabled
 - This allows FortiGate to detect the event handler from a list of potential triggers

FortiAnalyzer Event Handler

Status	
Name *	Default Botnet Communication Detection
Description	Default event handler to detect botnet communication and report to FortiGate
Mitre Tech ID	T1584.005 Botnet T1071 Application Layer Protocol
Data Selector	Click to select
Automation Switch	

FortiGate Automation Trigger

	FortiAnalyzer Event Handler A specified FortiAnalyzer event handler was triggered.
Name	
Description	0/255
FortiAnalyzer Event Handler	
Event handler name	Default-Botnet-Communication-Detection
Event severity	☐ Search + Create
Event tag	☐ FortiAnalyzer (2) ☒ Default-Botnet-Communication-Detection ☐ Default-FFW-Botnet-Communication-Detection

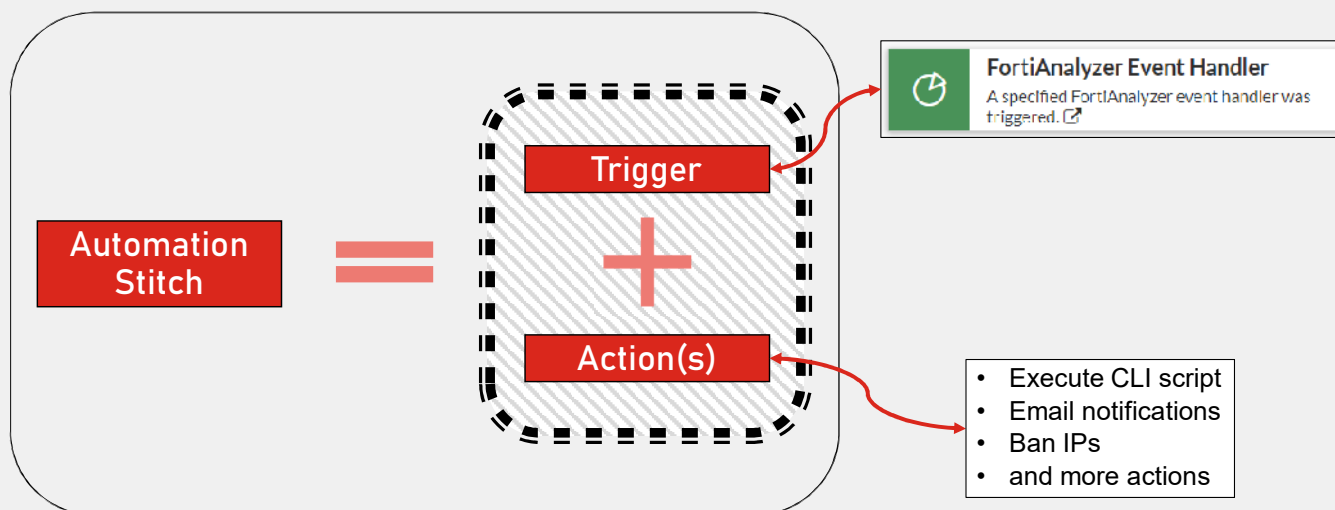
When a handler with automation stitch enabled generates an event, FortiAnalyzer sends a notification to the FortiGate automation framework. If an automation stitch is configured on FortiGate, the notification triggers the related automation stitch and activates an action in response. For example, FortiGate could send a custom email notification, execute a CLI script, and/or perform a system action in response to the trigger.

By default, there are two basic event handlers, Default-Botnet-Communication-Detection and Default-FFW-Botnet-Communication-Detection, that have an automation stitch enabled.

You can also enable automation stitches for any custom event handler.

DO NOT REPRINT
© FORTINET

FortiAnalyzer and FortiGate Automation Stitch (Contd)



An automation stitch consists of two parts: the trigger and the action or actions. The trigger is the condition or event that activates the action, such as a FortiAnalyzer event handler that generates an event. The action is what FortiGate does in response to the trigger. Automation stitches are configured on the Security Fabric root FortiGate.

While FortiGate can run automation stitches without having FortiAnalyzer in the topology, the advantages of having FortiAnalyzer in the workflow include:

- **Scalability:** The configured event handlers can apply to all authorized FortiGate devices, or you can use data selectors to narrow the selection.
- **Granularity:** You have finer control of which logs generate an event.
- **Centralized SOC view:** You can create events and incidents on FortiAnalyzer in addition to using its event correlation and reporting capabilities.
- **Playbooks:** You can perform more actions on FortiAnalyzer, such as automatically creating an incident if an event matches your conditions.

There are many other types of triggers available on FortiGate. However, in this course you will focus only on FortiAnalyzer event handlers as the automation trigger.

FortiAnalyzer and FortiGate Automation Stitch (Contd)

- This example automation stitch bans an IP address on FortiGate if the web filter violation category description matches social networking
- This slide shows the FortiAnalyzer configuration

Event Handler

Status	
Name *	Web Filter IP Ban
Description	
MITRE Tech ID	 Click to select
Data Selector	Click to select
Automation Stitch	

Event Handler Rule

Log Device Type	FortiGate		
Log Type	Web Filter (webfilter)		
The system will categorize logs into smaller groups based on the chosen log fields.			
Log Field	Destination IP (dstip)	Not in use	
Refine Your Logs			
Once logs are grouped, you can refine the data within each group by applying filter with retained within each group.			
Log Filters	All Filters	Any One of the Filters	
	Log Field	Match Criteria	
Log Filter by Text	catdesc='Social Networking'		

The example on this slide shows the configuration on FortiAnalyzer of an automation stitch integration with FortiGate. The automation stitch triggers an IP ban of the source machine on the FortiGate device that the security event occurs on, or, if the FortiGate is in a Security Fabric, you can choose on which devices in the Security Fabric the stitch will trigger.

First, you must create an event handler and enable the automation stitch option. You must then define a rule for that event handler that specifies which logs generate an event. In this case, the generic text filter is specifying the category description as social networking. If you are unsure about the log field, you can generate a log event, and then view the raw logs under **Log View** to see the names of the field and the associated properties.

FortiAnalyzer and FortiGate Automation Stitch (Contd)

- This slide shows the FortiGate configuration

Automation Stitch

Name: Web Filter Social Networking Block

Status: ☒ Enable ☐ Disable

FortiGate(s): All FortiGates

Action execution: ☒ Sequential ☐ Parallel

Description: 0/255

Stitch:

Trigger
Web Filter IP Ban Trigger

Add delay

Action
IP Ban

FORTINET
Training Institute

Workflow

FortiGuard Intrusion Prevention - Access Blocked

Web Page Blocked

You have tried to access a web page that is in violation of your Internet usage policy.

Category: Social Networking
URL: https://www.facebook.com/

To have the rating of this web page re-evaluated [please click here](#).

Client goes to facebook.com

An event is created on FortiAnalyzer

FortiGate bans the client

```
FortiGate# diagnose user banned-ip list
src-ip-addr  created  expires  cause
10.200.3.219  Sun Aug 18 14:20:01 2024  indefinite  Administrative
```

© Fortinet Inc. All Rights Reserved. 44

On FortiGate, you must create a trigger that references the created event handler. Next, you must specify the action or actions that you want to occur when the trigger happens. Finally, you must create the automation stitch by combining the trigger and action. In the example shown on this slide, the IP Ban action is a default action in FortiOS.

If there is more than one action in an automation stitch, FortiGate can perform them in sequence or in parallel. In sequential execution, actions will execute one after another, with an optional delay between each action. However, if any action in the chain fails, the entire chain stops. In parallel execution, all actions will execute simultaneously when the automation stitch is triggered. Note that in parallel execution, log action parameters (such as %%log%% or %%results%%) cannot be used because there is no subsequent action to pass this information to. In the example shown on this slide, since there is only one action, the sequential or parallel setting has the same effect.

In the example shown on this slide, the following workflow occurs:

- The client with the IP address of 10.200.3.219 tries to access facebook.com and FortiGate blocks it because of a web filter violation.
- On FortiAnalyzer, the Web Filter IP Ban event handler is triggered. This event handler has the automation stitch option enabled.
- On FortiGate, an automation stitch has that event handler configured as a trigger, and one configured action to ban the offending client. As a result, you can see that the device is banned indefinitely.

Note that unlike the FortiClient EMS quarantine depicted earlier, which is a host-level block, this configuration is blocking at a network level. This means that the host is banned only for traffic traversing FortiGate. In contrast, the host-level block restricts all network activity on the compromised host.

DO NOT REPRINT
© FORTINET

Knowledge Check

1. How many triggers and actions can each automation stitch support?
 - A. One trigger and one action
 - ✓ B. One trigger and multiple actions
 - C. Multiple triggers and multiple actions

DO NOT REPRINT
© FORTINET

Lesson Progress

-  Playbook Concepts
-  Creating Playbooks
-  Configuring Connectors
-  Managing Playbooks
-  Automation Stitches

FORTINET
Training Institute

© Fortinet Inc. All Rights Reserved. 46

Congratulations! You have completed this lesson.

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

DO NOT REPRINT
© FORTINET

Review

- ✓ Identify playbook components
- ✓ Describe trigger types and their properties
- ✓ Create and customize playbooks from a template
- ✓ Create new playbooks from scratch
- ✓ Use variables in tasks
- ✓ Configure connector actions
- ✓ Monitor playbooks
- ✓ Export and import playbooks
- ✓ Describe FortiAnalyzer and FortiGate automation stitches
- ✓ Configure an automation stitch
- ✓ Configure an event handler with an automation stitch enabled

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

By mastering the objectives covered in this lesson, you learned how to configure and use playbooks effectively to automate tasks on FortiAnalyzer. You also learned how to use connectors along with playbooks to send actions to other Fortinet devices and third-party applications.

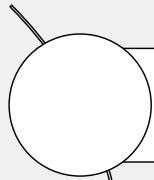
DO NOT REPRINT
© FORTINET



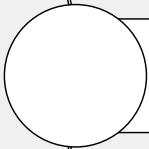
In this lesson, you will learn what constitutes the attack surface, and about common vectors that threat actors use against organizations. You will also learn how to capture traffic and perform basic traffic analysis on FortiAnalyzer, FortiGate, and endpoints.

DO NOT REPRINT
© FORTINET

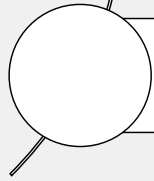
Lesson Overview



The Attack Surface



Attack Vectors



Reviewing Traffic Flows

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

DO NOT REPRINT
© FORTINET

The slide features a light gray background with abstract geometric shapes in red, gray, and teal. A grid of small dots is positioned to the right of the title. The Fortinet logo is in the bottom left, and the copyright notice is in the bottom right.

The Attack Surface

Objectives

- Describe the attack surface
- Describe how to identify the attack surface
- Describe how to reduce the attack surface

FORTINET
Training Institute

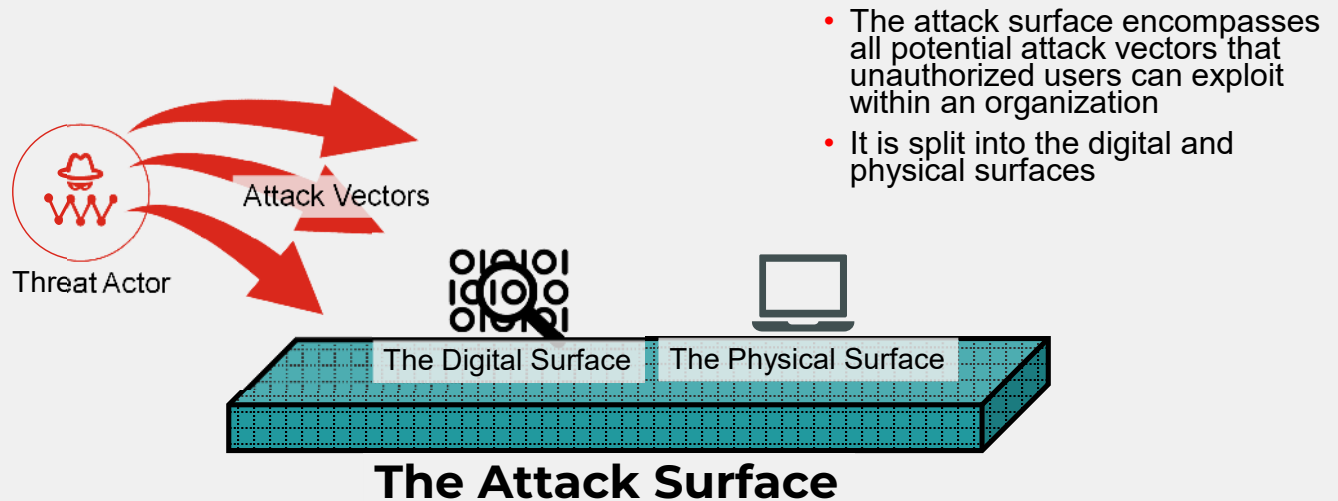
© Fortinet Inc. All Rights Reserved. 3

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

By demonstrating a competent understanding of the attack surface of an organization, you will be able to identify potential weaknesses in your organization. You will also be able to reduce the attack surface by implementing defensive mechanisms.

DO NOT REPRINT
© FORTINET

The Attack Surface—Introduction



FORTINET
Training Institute

© Fortinet Inc. All Rights Reserved. 4

The attack surface is the number of all possible points, or attack vectors, where an unauthorized user can access a system and extract data. The larger the attack surface, the harder it is to protect your organization.

The attack surface and attack vectors are different but related concepts. An attack vector is the method a cybercriminal uses to gain unauthorized access or breach a user's accounts or an organization's systems. On the other hand, the attack surface is the space that the cybercriminal attacks or breaches.

The size of the attack surface is not static. For example, if new vulnerabilities are discovered on any of the assets in an organization, the surface expands. As a result, it is imperative that a SOC remains vigilant in examining its attack surface, even if there are no discovered weaknesses at a point in time.

The attack surface is split into two categories: digital and physical.

Digital and Physical Attack Surfaces

Digital	Physical
Definition: Encompasses all the hardware and software that connect to an organization's network	Definition: Encompasses all devices that an attacker can gain physical access to
 Applications and code	 Desktop computers
 IP addresses and ports	 Laptops
 Servers (such as web, database, email)	 Hard drives
 Websites	 Mobile phones
 Shadow IT	 USB drives
 VPN endpoints	 Discarded hardware

The digital attack surface encompasses all the hardware and software that connect to an organization's network. These include applications, code, ports, servers, and websites, as well as shadow IT, which sees users bypass IT to use unauthorized applications or devices, often for the sake of convenience. An attacker can exploit the attack surface, for example, by exploiting vulnerabilities, phishing for sensitive information, or sending malware to unsuspecting users.

The physical attack surface comprises all devices that an attacker can steal or gain physical access to, in order to perform malicious activities. Examples include, but are not limited to, desktop computers, hard drives, laptops, mobile phones, and USB drives. The physical attack surface also includes improperly discarded hardware that contains user data and login credentials, users writing passwords on paper, and physical break-ins.

Identifying the Attack Surface

- To determine your network's attack surface, you must have a complete picture of all the assets
- You can use an IT asset management software to track your assets, including:
 - Hardware
 - Software
 - IP addressing
 - Location
 - Licensing
 - Configurations
 - Patching
 - Lifecycle (end of support & end of life)
 - Inventory (asset tagging)



To determine your network's attack surface, you must have a complete picture of all the assets in your organization. Every device that is unaccounted for is a potential security risk.

You can use IT asset management software to help track all of your assets:

- Hardware: desktop computers, laptops, servers, network devices, and peripherals
- Software: installed applications, virtualization, security software, and running services
- IP Addressing: allocation and management of IP addresses
- Location: physical location of assets within the organization, or the hosting data center
- Licensing: software licenses and compliance status
- Configurations: device and software configuration details
- Patching: status of patches and updates applied to devices
- Lifecycle: end-of-support and end-of-life dates for assets
- Inventory: comprehensive inventory management of all IT assets

Reducing the Physical Attack Surface

- Restrict physical access to the building as much as possible
 - Limit employee access to only what they need
 - Employees should never hold open a door to a restricted area—prevents tailgating
- Do not allow visitors in working areas
 - Instead, have public areas and meeting spaces that are open to visitors
- Limit the use of removable media
 - USB drives, for example, can be used maliciously in many ways, such as exfiltrating data or installing malware
 - Employees may be baited into plugging in malicious devices
- Guard devices
 - Allow access to recycling areas only to authorized people
 - Thoroughly destroy discarded hard drives
 - Users should always lock their device before they leave their desk
 - Store unattended devices securely

The physical attack surface ranges from physical buildings, to organization devices, to access cards. As a SOC analyst, you must be aware of the digital attack surface, which may receive more attention, but you also must be aware of the physical attack surface. Physical breaches can lead to significant cybersecurity risks. You can mitigate many risks to the physical attack surface using common sense, but failure to adhere to these guidelines can lead to catastrophic consequences.

- Restrict physical access to working areas. Employees must use their own access cards to enter restricted areas to prevent tailgating, by which an unauthorized person closely follows someone with legitimate access. Accurate accounting of who accessed which area at a specific time is essential for investigations if a security incident occurs. Allow visitors access only to public areas. Furthermore, use cameras to provide video evidence of building access.
- Restrict or ban removable media, such as USB drives. Attackers may bait users into inserting USB drives by labeling them with phrases such as “performance reviews”, “urgent attention needed”, or “financial reports.” You can use endpoint security, such as FortiClient EMS, to monitor or block removable media. You can send log entries to FortiAnalyzer for further investigation and incident handling.
- Store laptops securely, even when in the office. Employees are responsible for their assigned work devices, such as laptops and mobile phones, at all times, including after work hours. Even if a user's password is secure, or they use multifactor authentication (MFA), an attacker can exploit a workstation if the user does not lock it when they leave. Destroy discarded devices and hardware before sending them to a restricted area for recycling. A hard drive that can have its data recovered is a significant risk.

Reducing the Digital Attack Surface

- Servers and network equipment are usually stored and racked in data centers with stricter access
 - They are *generally* more secure; they *should* be in a more secure location
 - As such, you can consider them part of the digital attack surface, since an attacker is less likely able to infiltrate data centers
- Remove unnecessary devices or services
- Segment the network
 - Macrosegmentation: Isolate different networks and VLANs from one another
 - Microsegmentation: Isolate the workloads of individual applications
- Fine-tune the level of access given to users and devices
 - Implement a zero-trust model
- Review logs and security events and incidents to find abnormal behavior
- Conduct SOC blue, red, and purple team exercises regularly

To reduce your organization's digital attack surface, you can follow some best practices:

- Audit assets: Review your up-to-date list of all digital assets in the organization.
- Remove unnecessary devices and services: Consider whether all existing assets must be in production. Some devices and software may be legacy assets that are no longer actively managed.
- Segment: Divide the network using macrosegmentation and microsegmentation. With macrosegmentation, you can isolate broadcast domains and implement different levels of security based on the network and VLANs a device belongs to. For example, you can have a "Guest" network with limited access, whereas the "IT" network can access critical devices such as the "Server" network. With microsegmentation, you can further segment based on workloads of individual applications. For example, you can use FortiNAC to profile each device on or joining the network and assign a role.
- Define trust: Control and monitor the access of users and devices. Apply the principle of least privilege required for employees to fulfill their roles. Furthermore, you can adopt a zero-trust security model, which assumes that trust is *transient*. A device that is trusted now may become infected. As a result, you must monitor devices continuously in case a new assignment, such as quarantining, is required.
- Review logs and security events and incidents: Find traffic that has deviated from established baselines. You should also set up automated processes, such as event handlers on FortiAnalyzers, that create security events and incidents for interesting traffic, such as RDP connections to your domain controller.
- Test your security: Conduct regular SOC exercises to probe, identify, and improve the organization's security posture.

DO NOT REPRINT
© FORTINET

Knowledge Check

1. Which attack surface do USB drives belong to?
 - ✓ A. Physical
 - B. Digital

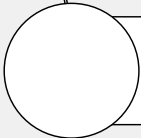
2. What is the definition of shadow IT?
 - ✓ A. Unauthorized devices and applications implemented by users.
 - B. Legacy devices and applications that are no longer actively managed.

DO NOT REPRINT
© FORTINET

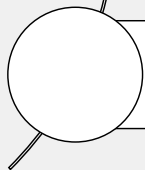
Lesson Progress



The Attack Surface



Attack Vectors

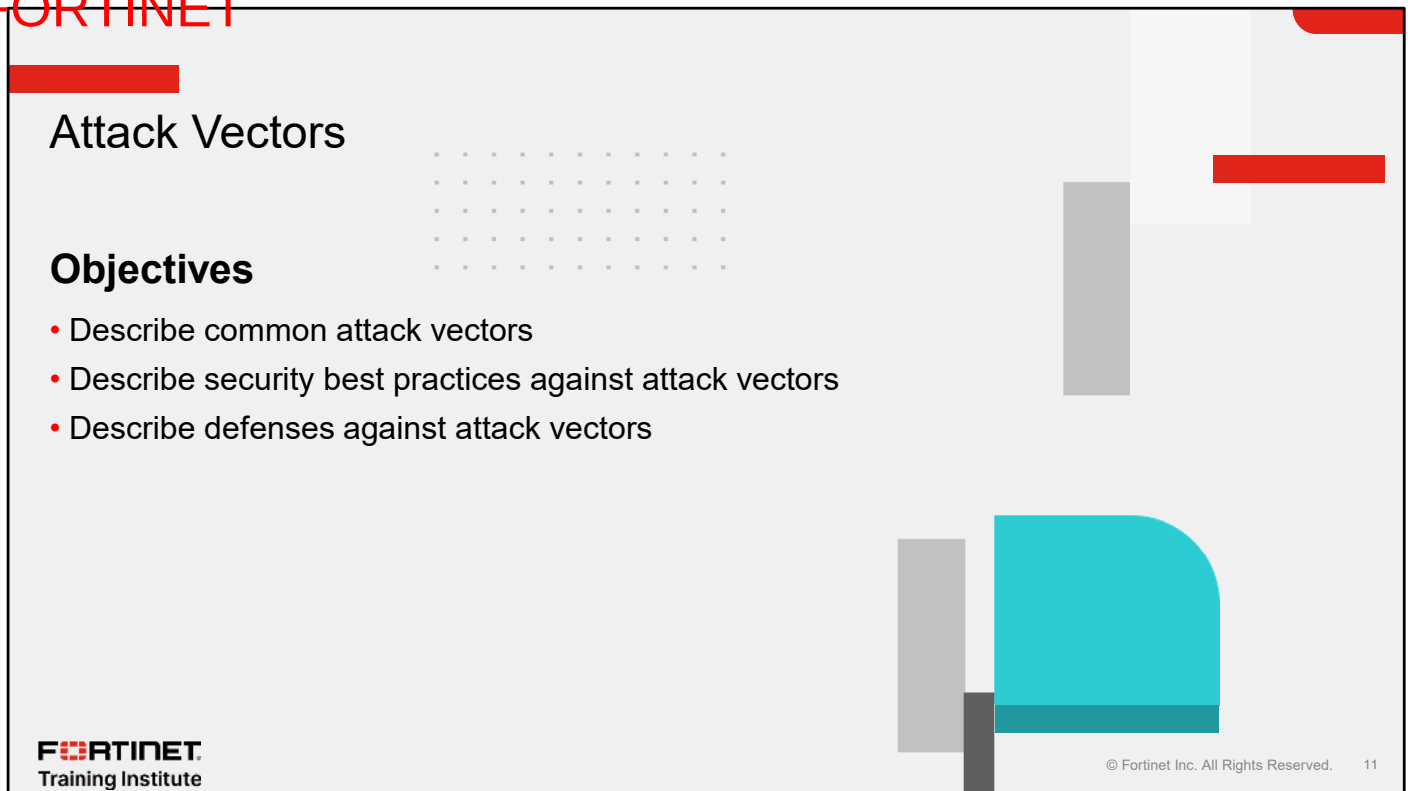


Reviewing Traffic Flows

Good job! You now understand the attack surface.

Now, you will learn about attack vectors.

DO NOT REPRINT
© FORTINET



Attack Vectors

Objectives

- Describe common attack vectors
- Describe security best practices against attack vectors
- Describe defenses against attack vectors

FORTINET
Training Institute

© Fortinet Inc. All Rights Reserved. 11

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

Attack vectors are the possible avenues that attackers use to gain unauthorized access to a network or system. From there, the attacker tries to achieve their goal, whether it is to steal information or adversely affect your organization. Understanding these vectors is crucial for building effective defense strategies and mitigating risks.

Attack Vectors Introduction

- As a SOC analyst, you should be able to identify attack vectors and formulate plans to defend them
- You can advise management with an action plan
- Attackers may follow a standard flow like the Cyber Kill Chain, or their steps can vary like the MITRE ATT&CK framework
- Attackers may have a specific goal in mind, which is dependent on the nature of the organization's business

As a SOC analyst, one of your responsibilities is to identify potential attack vectors and devise strategies with management to defend against them. This involves continuous monitoring of network activity, reviewing logs, analyzing security incidents, and staying current on emerging threats. By understanding the various ways attackers can infiltrate systems, you can implement proactive measures to mitigate risks and protect the organization's assets.

It is important to note that not all attacks follow the same rigid pattern, as discussed in *Lesson 1 – SOC Concepts and Security Frameworks*. An attacker may opt to perform fewer or additional steps than those included in the Cyber Kill Chain model, instead executing more minute, flexible tactics, techniques, and procedures (TTPs) as described in the MITRE ATT&CK framework.

Therefore, it is crucial that you have an understanding of the individual attack vectors in this section, and how they fit into the overall scheme of a potential attack.

DO NOT REPRINT
© FORTINET

Reconnaissance

- An attacker gathers information about a target **without directly interacting** with them

- Minor risk of detection

- Includes reading social platforms like Reddit, Facebook, Instagram, and LinkedIn

Passive

- An attacker gathers information about a target **by directly performing actions** on them

- Higher risk of detection

- Includes using tools like Nmap, Kali Linux, and DNS lookups

Active

FORTINET
Training Institute

© Fortinet Inc. All Rights Reserved. 13

When an attacker plans an attack, one of the most logical starting points is to gather information about the individual or organization they want to target.

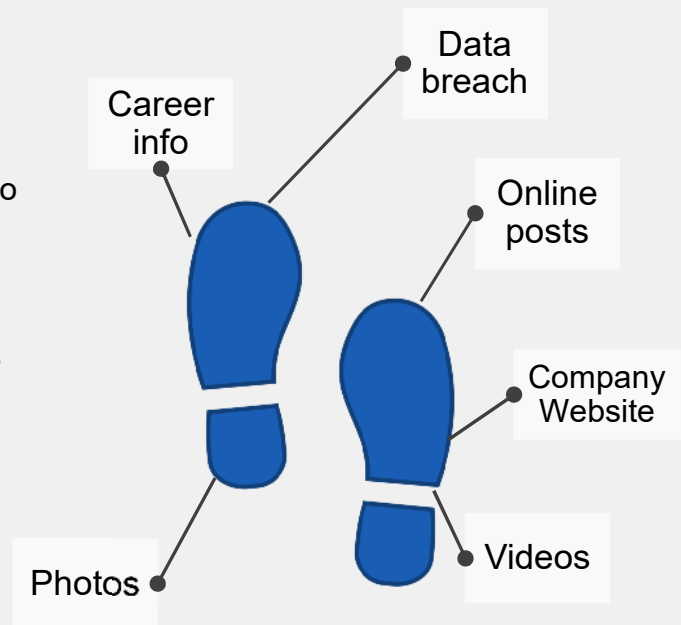
There are two main categories of reconnaissance: passive and active.

DO NOT REPRINT

© FORTINET

Passive Reconnaissance

- Your digital footprint is the trail of data you leave behind through your online activities
- Attackers can search through your profiles to gather information
- Your personal information can be used to spearfish or impersonate you, and access work resources



Passive reconnaissance involves a threat actor gathering information on a target for a potential attack. Users with a larger digital footprint are more vulnerable because more of their private information is exposed. Examples of where you may have inadvertently provided key information include:

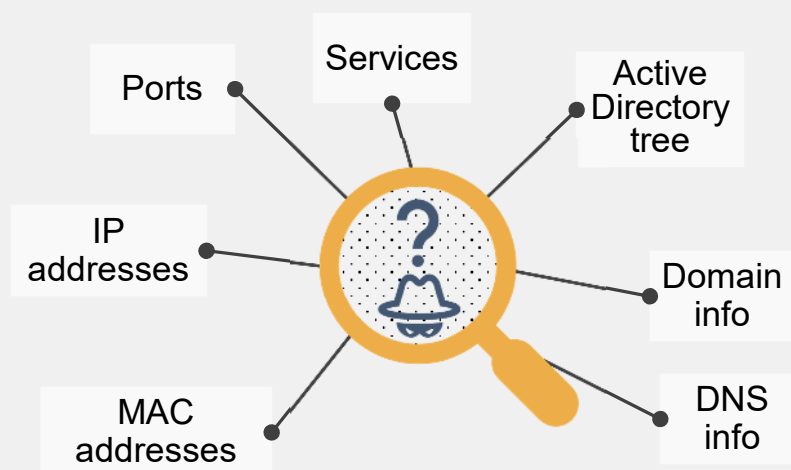
- Your resume is uploaded to a career development website. It may contain your email address, telephone number, and home address.
- Your social media profiles include details of where you have traveled to (business or personal).
- Your face and voice have been on streams or online videos.
- Your work or personal experiences are discussed online and searchable.
- Your private data was part of a data leak, which could be the fault of a third-party, such as a business you used your credit card to purchase goods from.
- Your company website contains contact information such as email addresses, telephone numbers, and locations.

There are some potential consequences for having your information publicly available:

- Financial institutions use personal information to validate your identity and an imposter can exploit that.
- Spearphishing targeting you is more believable because it contains your personal information.
- A threat actor can impersonate you and target your associates using your likeness.
- Your credentials (username and password) are exposed in a data leak.

To mitigate the risks of passive reconnaissance, you must educate your employees to limit what they share online, refrain from discussing work or sharing photos of the workplace on public websites, and update their passwords frequently.

Active Reconnaissance



Active reconnaissance involves a threat actor performing actions on a target to gather information. As a result, the attacker may leave behind more evidence. Many of these activities are more effective when an attacker has already gained entry to a network. However, they can conduct some of the reconnaissance from the internet through public-facing assets, such as a web server. Some actions that an attacker may conduct on your network include:

- IP addresses scanning: Discover active IP addresses in the target network. The attacker can identify live hosts on the network, and then see which services are enabled on them.
- Ports and services scanning: Identify which services and applications are running on open ports. The attacker is probing to see accessible network services and potential entry points, for example, testing to see if SSH is enabled on a device.
- MAC address discovery: Collect MAC addresses of devices on the network. A lookup of the organizationally unique identifier (OUI), which consists of the first six digits of a MAC address, tells you which vendor the device belongs to.
- Domain information: Perform DNS lookups to map domain names to IP addresses, discover subdomains, and attempt DNS zone transfers for detailed domain information.
- Active Directory (AD) Tree: Enumerate AD users, groups, and organizational units to understand user privileges and organizational structure.

After gathering information, the attacker can proceed to further attack phases, such as lateral movement to hosts with more access, and intercepting traffic through spoofing.

Social Engineering

- Refers to a range of attacks that manipulate users, including:
 - Baiting
 - Scareware
 - Phishing
 - Pretexting
 - Tailgating
- The victims are fooled into performing dangerous actions
- Information gathered from reconnaissance can make the attacker seem more trustworthy



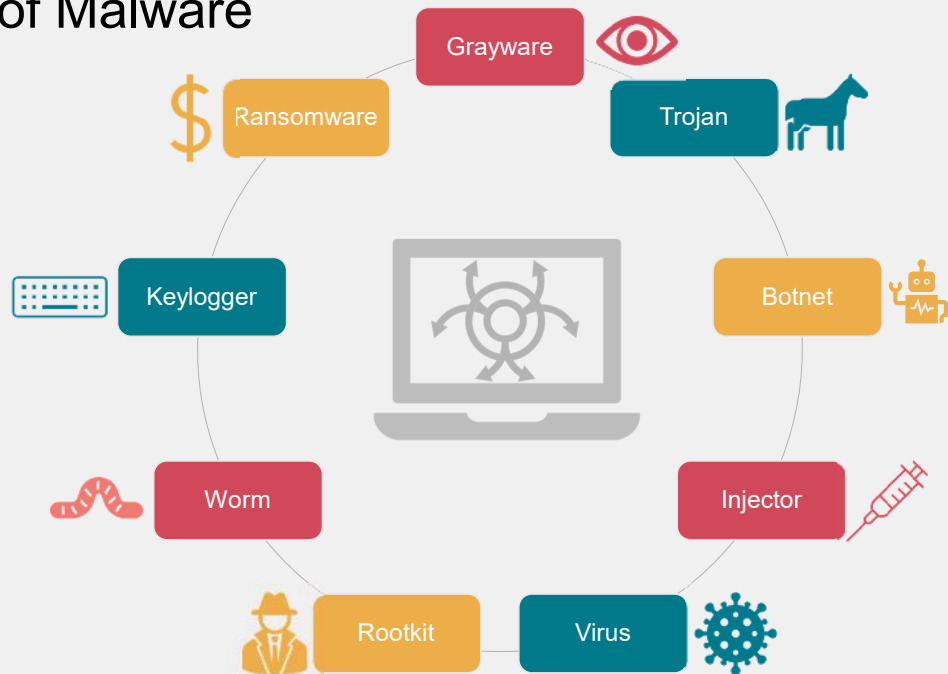
Social engineering attacks are based on manipulating users into performing malicious activities or divulging sensitive information. Attackers can present themselves as trustworthy by providing information that should be private. These attackers may prey on the users' sense of urgency, fear, curiosity, greed, or other emotions. Some social engineering attacks include:

- Baiting: enticing users with the prospect of a reward. For example, there could be an offer to redeem a free meal, or a USB drive labeled with 'Performance Reviews.'
- Scareware: scaring users into thinking their system is infected, and offering a solution that is malicious.
- Phishing: fooling users into clicking on something by creating a sense of urgency or appealing to their curiosity. Phishing could be targeted (known as spearphishing) and could also be in audio form (voice phishing).
- Pretexting: pretending to be a trusted source and getting the users to divulge sensitive information.
- Tailgating: entering an area that you are not authorized to be in. Attackers can clandestinely follow an authorized person who is unaware they are being followed. Or, they can present themselves as friendly and trustworthy, in the hopes of having the door held open for them.

Even though social engineering attempts may contain obvious spelling errors, grammatical mistakes, and illogical schemes, not all attempts are obvious scams: Some are well-crafted and hard to spot. In all of these social engineering methods, the more research the threat actor conducts before the attack, the more believable they can be. You should conduct periodic social engineering tests on internal users to see if they fall for them. Users must be educated on cybersecurity best practices. Because personnel may change as time passes, employee training is a continuous effort.

DO NOT REPRINT
© FORTINET

Types of Malware



FORTINET
Training Institute

© Fortinet Inc. All Rights Reserved. 17

Malware is an umbrella term that defines any type of malicious software. It is important to understand the different types of malware and what they are designed to do to a target network:

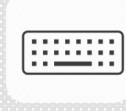
- **Grayware:** applications that behave in a manner that is irritating or undesirable but may not be as malicious or destructive as other malware types. Grayware includes spyware, adware, dialers, and remote access tools that are designed to harm the performance of computers on your network, often with the goal to display advertisements or track user behavior.
- **Trojans:** applications that appear to be legitimate software, designed to mislead users into installing them. Trojans can create backdoors or allow other malware to gain control of the system.
- **Botnet:** a collection of internet-connected programs communicating with each other to distribute malware. Infected machines can launch coordinated attacks against victims.
- **Injectors:** applications that inject malicious code into system processes to perform tasks on an attacker's behalf.
- **Viruses:** applications that link malicious code with clean code, waiting for a user to execute it. Once executed, viruses propagate quickly through an infected system, severely impacting operations.
- **Rootkits:** applications that grant the attacker privileged access. They attempt to stay hidden by replacing vital system executables.
- **Worms:** self-replicating applications that spread throughout a network without needing to be attached to an existing program or executed by a user, unlike a virus.
- **Keyloggers:** applications that are designed to capture users' keystrokes, often designed to farm user credentials or private information. Keyloggers can be hardware or software.
- **Ransomware:** applications that are used to lock down access, from a single device to an entire organization, with the goal of extracting money from victims in exchange for releasing the system.

Note that this slide includes common types of malware, but it is not exhaustive.

Compromised Credentials



Data Breach



Keylogging



Phishing



Password Manager

Note: You can visit websites such as <https://monitor.mozilla.org> or <https://haveibeenpwned.com> to see if your email account has been part of a data breach.

Even if your passwords meet or exceed security requirements, they can still be vulnerable. Your private information can be compromised through credential harvesting. There are many ways an attacker can harvest your credentials, but common ones include:

- **Data breach:** Your personal information was leaked in a data breach. The extent of the information varies, but could include usernames, passwords, addresses, and more. The data breach could be entirely a third party's fault, and you may not even be aware of the incident. Companies have a responsibility to disclose any suspected or confirmed cybersecurity incident to its customers, so that they can immediately change their credentials.
- **Phishing:** You are a victim of a phishing attempt and inadvertently provided private information to a threat actor.
- **Keylogging:** You or someone else installed keylogging malware on a device, and an attacker can store your keyboard strokes.
- **Password manager:** Your password manager, which is a repository of all credentials you've saved to online and offline resources, is compromised. You may have left your computer unlocked while you stepped away, or your device was stolen, allowing cached credentials to provide access. Having your password manager compromised is particularly dangerous because password managers can also include credit card numbers, personal identification information, and more.

Credentials that have been compromised are susceptible to further exploitation. For example, an attacker may include a compromised password in a dictionary file, and then use that dictionary file against a target to obtain network access.

Credential Attacks

Attack Name	Description
 Brute force	Try all combinations for a match
 Password spraying	Target multiple hosts with limited attempts (to avoid detection)
 Dictionary	Use a list of compiled passwords to find a match
 Credential stuffing	Use information from data breaches to find a match
 Man-in-the-middle	Intercept traffic to steal sensitive information
 Rainbow table	Precompile a list of passwords into hashes to find a matching hash

This slide includes credential attacks that threat actors can leverage to gain access to a target system:

- **Brute force:** Systematically try every possible combination of characters until a match is found.
- **Password spraying:** Similar to a brute force attack but targeting multiple hosts with fewer attempts on each one to avoid lockouts.
- **Dictionary:** A list of compiled passwords to try against a target system.
- **Credential stuffing:** Known user and password combinations obtained in data breaches are tried against a target system.
- **Man-in-the-Middle:** Traffic is intercepted by an attacker to extract private information.
- **Rainbow Table:** Password hashes are precompiled into a table and used to find matching hashes. If a match is found, the password used to generate the hash is known. However, with modern cryptography, salting, which combines a unique salt for each password, makes every hash unique. This is true even if two passwords are identical. The random salt value yields two different hashes as byproducts.

DO NOT REPRINT
© FORTINET

Credentials Best Practices

- As an organization:
 - Ban recycling passwords
 - Enforce password complexity
 - Enforce MFA across the organization
 - Set a short password validity period
 - Set a low limit for failed login attempts
- As an end user:
 - Don't use the same passwords for personal and business accounts
 - Check to see if the password has been compromised (using online search engines)
 - Check to see if your email account has been involved in data breaches
 - Never write down any passwords
 - Do not share MFA codes
 - Do not share your cell phone

This slide shows some best practices for both organizations and end users.

Software Vulnerabilities

- Search for software versions of assets in your organization and view a list of vulnerabilities
- Not all vulnerabilities are critical, but you need to be aware of all risks

The screenshot shows the 'Google » Chrome : Versions' page. It lists 9258 versions of Chrome. A table displays columns for Version, Language, Update, Edition, Target Platform, and Vulnerabilities. Two versions are highlighted: 124.0.6367.60 with 25 vulnerabilities and 107.0.5261.1 with 386 vulnerabilities. A blue callout bubble points to the 386 vulnerabilities for version 107.0.5261.1, stating 'Older versions have more known vulnerabilities'. A red box highlights the 'Vulnerability Details : CVE-2024-5274' link, which leads to a detailed view of the vulnerability.

Vulnerability Details : CVE-2024-5274

Type Confusion in V8 in Google Chrome prior to 125.0.6422.112 allowed a remote attacker to execute arbitrary code inside a sandbox via a crafted HTML page. (Chromium security severity: High)

Published 2024-05-28 15:15:10 Updated 2024-05-29 01:00:04

Source [Chrome](#)

View at [NVD](#), [CVE.org](#)

Vulnerability category: [Execute code](#)

As mentioned earlier in this lesson, you should have an updated list of all assets, including the software versions installed. Threat actors exploit vulnerabilities in unpatched software or firmware on both physical and virtual assets on the network, so you must be aware of all vulnerabilities, minor or critical, of the assets in your organization.

Common Vulnerabilities and Exposures (CVEs) is a standardized system that provides the public with information on discovered vulnerabilities. Each CVE entry provides a reference number, beginning with the letters CVE, followed by the year, and then the vulnerability entry number from that year. For example, this slide shows the entry CVE-2024-5274.

This slide illustrates the type of information you can find when you search for Google Chrome. Note that the image is edited to list two versions that are far apart, and there are many versions of Chrome in the list with known vulnerabilities not listed.

There are numerous websites that provide information on CVEs:

- www.nvd.nist.gov
- www.cve.com
- www.cvedetails.com

This slide includes information obtained from www.cvedetails.com.

DO NOT REPRINT

© FORTINET

Software Vulnerabilities (Contd)

- Common Platform Enumeration (CPE) is a standardized scheme to identify assets

- The CPE 2.3 format follows this syntax:

```
cpe:<cpe_version>:<part>:<vendor>:<product>:<version>:<update>:<edition>:<language>:<sw_edition>:<target_sw>:<target_hw>:<other>
```

- You can also search vulnerabilities based on a CPE string:

Search Vulnerabilities By CPE

CVE-2024-5499

Out of bounds write in Streams API in Google Chrome prior to 125.0.6422.141 allowed a remote attacker to execute arbitrary code inside a sandbox via a crafted HTML page. (Chromium security severity: High)

Source: Chrome

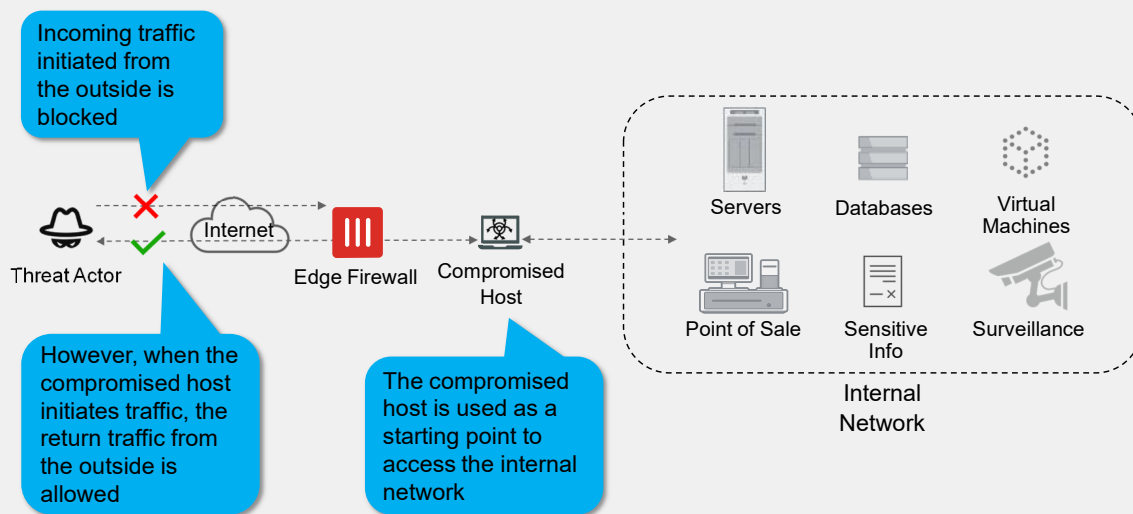
In addition to CVEs, a SOC analyst should also know about Common Platform Enumeration (CPE). CPE is a standardized naming scheme used to describe and identify classes of applications, operating systems, and hardware devices. The CPE Dictionary is hosted and maintained by NIST. The CPE 2.3 format follows this syntax, from left to right:

- CPE: indicates the entry is following the CPE format
- CPE Version: indicates the CPE specification
- Part: indicates the type of product (*a* for *application*, *o* for *operating system*, *h* for *hardware*)
- Vendor: the name of the vendor (such as Microsoft)
- Product: the name of the product (such as Windows 11_23h2)
- Version: the version of the product (such as 10.0.22631.2428)
- Update: the update level of the product (such as Service Pack 1)
- Edition: the edition of the product (such as Professional)
- Language: the language of the product
- sw_edition: the software edition of the product (such as Enterprise)
- target_sw: the target software platform (such as Windows)
- target_hw: the target hardware platform (such as x64)
- Other: any other relevant attributes

Not all fields are required, and you can use an asterisk as a wildcard to match anything. IT management tools can use information contained in CPEs to make automated decisions, such as looking up vulnerabilities or verifying security settings on the software.

DO NOT REPRINT
© FORTINET

Initial Access



FORTINET
Training Institute

© Fortinet Inc. All Rights Reserved. 23

As part of a cyber attack, a threat actor must gain a starting point to start exploiting a network, regardless of the end goal. The initial foothold may or may not be a critical device and, quite often, the compromised host is an end user's computer.

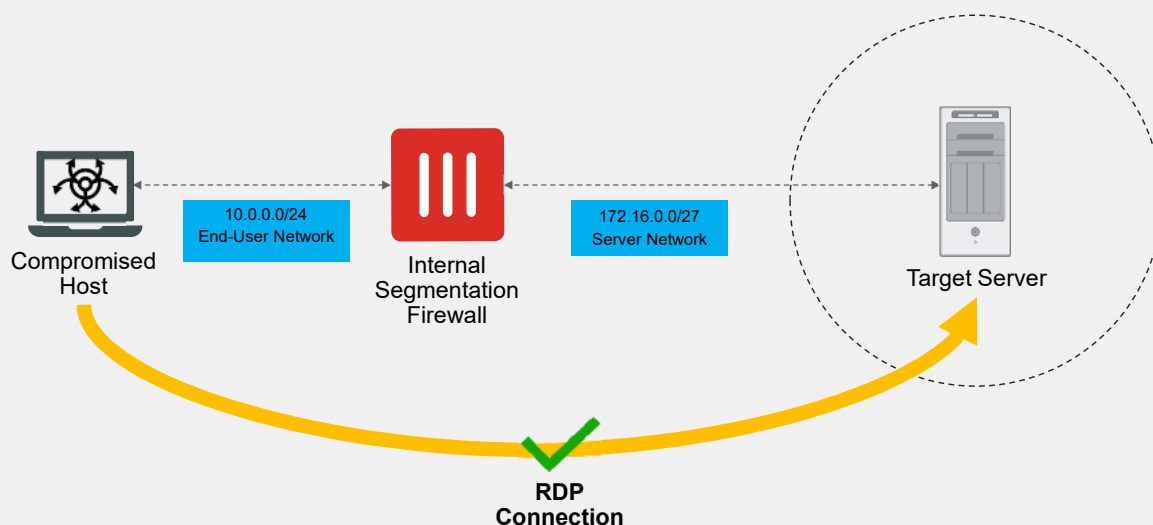
Depending on the firewall device, you may not need to explicitly define a deny action to block traffic. On FortiGate, for example, the default action is to deny all traffic with the implicit deny rule. In the example shown on this slide, incoming traffic initiated from the outside is blocked. However, traffic from a LAN segment to the internet is allowed. A common and simple firewall rule is to give end users access to the internet by permitting only common protocols, such as HTTPS and DNS. Despite the firewall blocking outside-initiated traffic, the compromised host, as the originator of the traffic, essentially bypasses that security measure, as the return flow from the outside is permitted by stateful firewalls.

It is also important to remember that initial access does not necessarily have to come from the outside. For example, internal threats and compromised physical access are both possible reasons for threats originating from the internal network. This is why it is important when thinking of security policies to focus both on north-south traffic as well as east-west internal traffic.

Assuming that the compromised host is a regular user endpoint that is not on the same subnet as some critical devices, the threat actor may attempt to move to a device with more access and privilege.

DO NOT REPRINT
© FORTINET

Lateral Movement



FORTINET
Training Institute

© Fortinet Inc. All Rights Reserved. 24

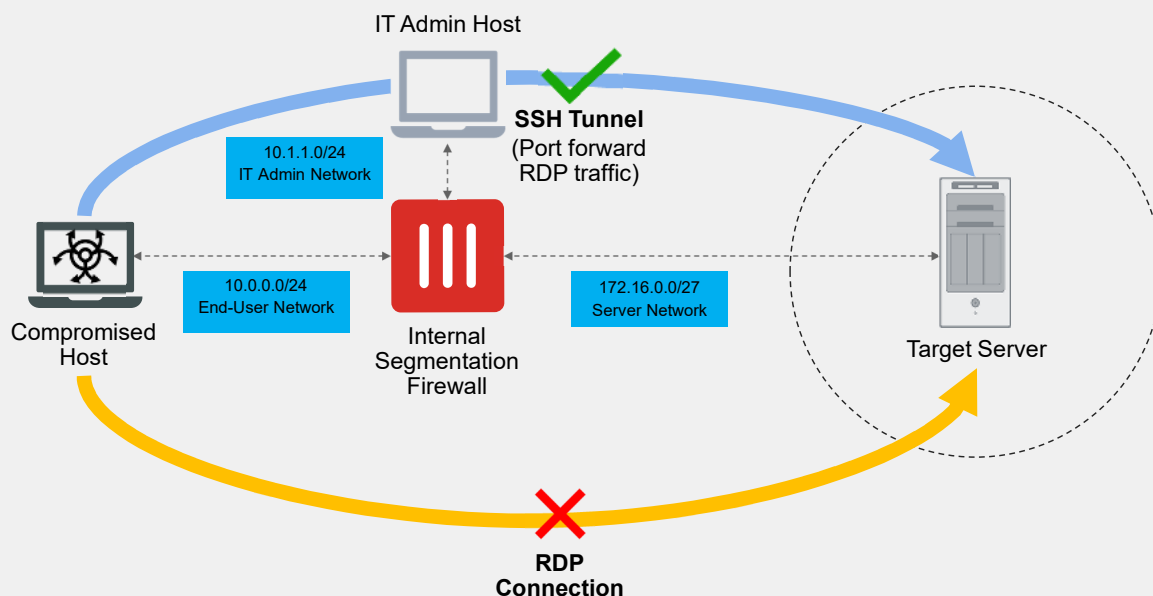
This slide shows a network misconfiguration that allows an attacker to use a compromised host to connect directly over RDP to a critical server.

This is why network segmentation is important. The internal segmentation firewall should be blocking RDP access from the end user network to the server subnet. Regular end users should never have access to critical infrastructure. Instead, only explicitly permitted hosts on a restrictive network should be given access to critical infrastructure.

Furthermore, the server itself should also have security measures implemented, such as disabling RDP on the target server, or implementing endpoint firewall rules on the target server to fine tune access.

DO NOT REPRINT
© FORTINET

Lateral Movement (Contd)



FORTINET
Training Institute

© Fortinet Inc. All Rights Reserved. 25

In this next example, RDP traffic is not allowed between the compromised host and the target server. However, there is a device on the IT Admin network that the compromised host can connect to over SSH, and that host can connect over RDP to the target server. The attacker can leverage a technique, known as SSH tunneling, to connect to the target server, using the IT admin host as a springboard.

This example highlights the importance of fully understanding the attack surface. Instead of thinking of security policies only between a lone source and destination, take a more holistic view of the network.

Restricting Lateral Movement

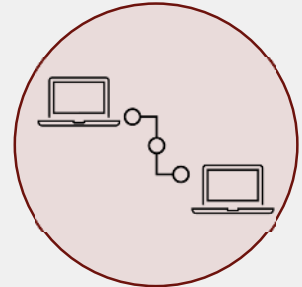
- Segment the network to reduce risk and exposure
- Implement zero trust network access
- Use multi-factor authentication for logins
- Keep approved accounts to a minimum
- Block network discovery mechanisms
- Monitor and log critical devices for suspicious logins and traffic flows
- Install software updates regularly

You can follow best practices to restrict lateral movement:

- Segmentation: Even if a device is compromised, the attacker has no avenue to move laterally. A network that has all clients and servers within the same subnet, known as a *flat* network, is especially dangerous because devices can communicate in their own subnet, without needing to traverse a layer 3 gateway, such as a firewall.
- Zero trust access: It is no longer safe to assume that if a device is connected to a network that it should be implicitly trusted. Adopting a zero-trust approach ensures that every access request is verified, no matter where the users are working from.
- Multi-factor authentication (MFA): Adds an extra layer of security in case users' credentials are compromised.
- Limit accounts: Only employees who require access should be granted it. Even authorized staff, such as the IT department, should have tiered access. Not every member of the IT infrastructure team, for example, should have read-write access to the network devices.
- Block network discovery: Preventing attackers from conducting active reconnaissance on the network reduces the chance of attackers being able to map out and understand your network.
- Monitor and review logs: Constantly monitor and review logs, such as creating event handlers on FortiAnalyzer to detect traffic on multiple ports coming from a single source IP address. The threshold needs to be tuned to your expectation for a baseline of your network.
- Update software: Unpatched firmware may contain many known vulnerabilities.

Persistence

- Used by attackers to maintain a connection with a compromised system
- Connection persists through reboots, log ins and log outs, and changed credentials
- Examples:
 - Modify registry keys to execute malicious programs during startup
 - Modify system services or create new services to run malicious programs
 - Modify logon scripts using Group Policy to execute malicious programs
 - Embed malicious macros in an office document
 - Place a malicious DLL in a location that makes an application run it



After attackers gain initial entry to a network, there are other actions they may perform. One action is to establish persistence with the compromised host. Persistence allows attackers to maintain a connection to a compromised host that persists across reboots, log ins and log outs, and changed credentials.

There are many ways for attackers to establish persistence, including (but not limited to):

- Modify Windows registry keys to execute malicious programs at startup. They can insert registry keys for the machine (HKEY_LOCAL_MACHINE) or for a specific user (HKEY_CURRENT_USER) to point to a malicious file.
- Modify legitimate system services or create new services to run malicious code at startup.
- Modify logon scripts using Group Policy to execute malicious programs.
- Embed malicious macros in an office document to exploit vulnerabilities.
- Use dynamic link library (DLL) hijacking. A DLL is a file that contains code and data that can be used by multiple programs at the same time. With DLL hijacking, the attacker places a malicious DLL file in a location where a legitimate application loads it. A program that does not specify the absolute path to the DLL file performs a search. The search order can be exploited by placing the DLL file in a location that is searched first before the legitimate DLL file.

Defense Evasion

- Used by attackers to avoid detection after they initiate an attack
- Examples:
 - Encrypt malicious payloads to bypass security measures
 - Execute malicious actions directly in memory without leaving files
 - Modify file timestamps to confuse time-based analysis
 - Create malicious processes with system-like names



Attackers may also attempt to evade detection and defenses by hiding their activities. Some examples include:

- Encrypting payloads: Attackers can encrypt their malicious payloads to evade detection by antivirus or other security solutions.
- Executing actions in memory: Attackers can execute malicious code in memory instead of writing files to disk. Memory-based malware may evade traditional security measures. FortiEDR, however, can detect and defuse file-less malware and other advanced attacks in real time.
- Modify file timestamps to confuse time-based analysis: Attackers may alter timestamps to obscure the timeline of their attack, making log correlation difficult.
- Create malicious processes with system-like names: Attackers can name the service as something inconspicuous to avoid detection. You can use tools like Process Explorer to see a detailed breakdown of each process running on the Windows operating system. Some information includes the digital signature of the executables, process name, parent process, the DLLs loaded, active connections, and more.

Privilege Escalation

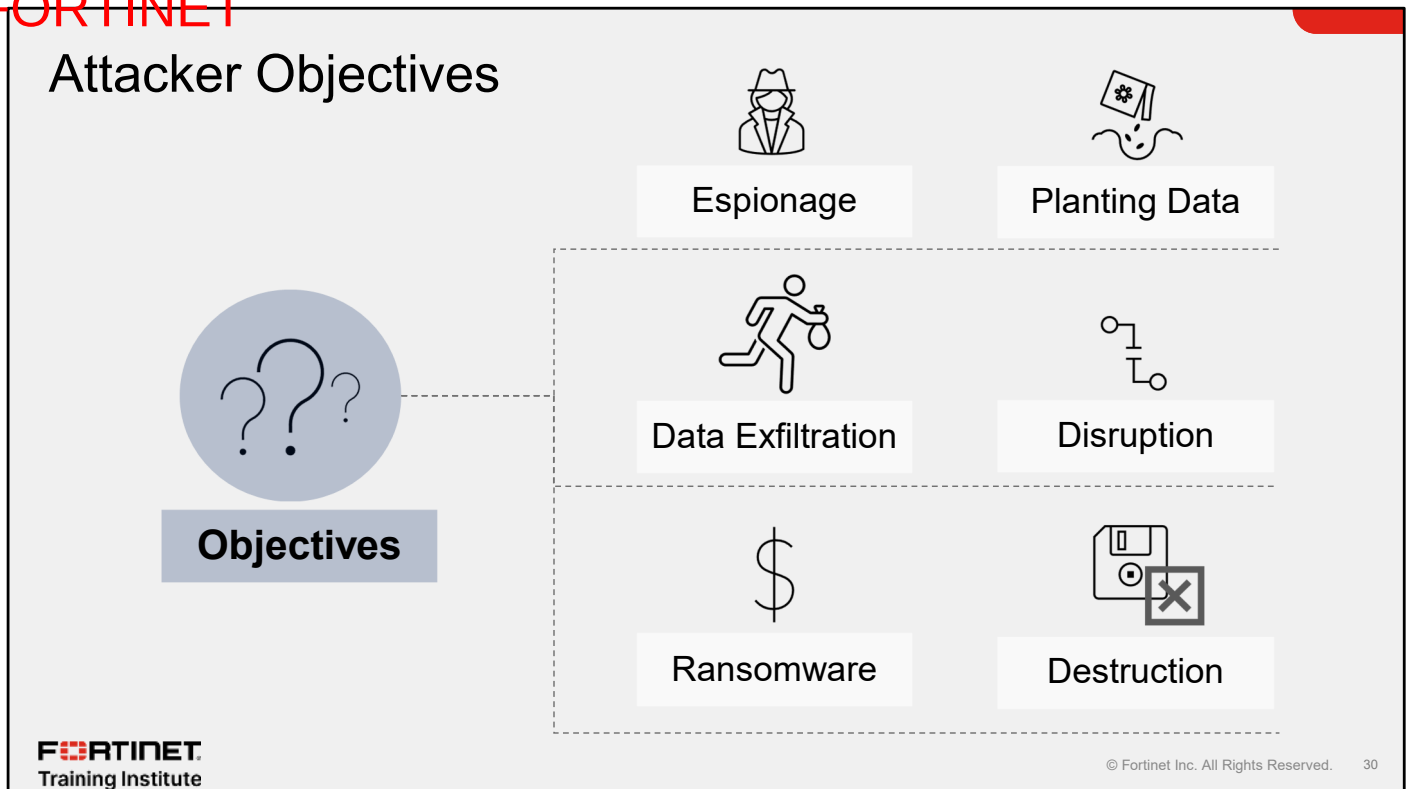
- Used by attackers to gain elevated access
- Examples:
 - Crack the password of known users on a network, or attempt through brute force
 - Exploit a vulnerability to gain unintended access
 - Impersonate tokens from a user with elevated privileges



Attackers may require privilege escalation in order to achieve their end goal on a network, particularly in a scenario where the initial compromised host is a segmented end-user machine. Privilege escalation allows attackers to perform more damaging actions and access sensitive data. Some examples include:

- Password attack: Attackers may conduct a brute force password attack or use a dictionary attack.
- Exploit vulnerabilities: Some vulnerabilities allow attackers to perform actions that require elevated privileges. For example, the operating system may have a vulnerability that lets a regular user obtain root access.
- Token impersonation: Attackers may copy a logged-in user's token to escalate privileges and bypass access controls.

DO NOT REPRINT
© FORTINET



Understanding the *why* of an attack may help you identify critical points. If you can anticipate the objectives of threat actors, it may help your organization formulate security practices and prioritize your most valuable assets.

This slide shows common objectives that a threat actor has in mind for a target:

- **Espionage:** gathering classified information for political, economic, or military purposes
- **Data exfiltration:** transferring data without authorization. The data can be used to leverage further attackers or could be sold to other parties.
- **Ransomware:** restricting access from a single device to an entire organization, with the goal of extracting money from victims in exchange for releasing the system.
- **Planting data:** injecting harmful, incriminating, or false information into a target system. The attacker may attempt blackmail or to settle a personal vendetta.
- **Disruption:** disrupting a target's daily operations, using techniques, such as distributed denial of service attacks, potentially causing significant financial loss.
- **Destruction:** destroying key services, such as deleting device configurations and corrupting databases. It is important to make backups for all critical devices in the organization. This includes configuration files, snapshots, database backups, and more. Ensure these backups are stored securely and regularly updated. Additionally, physically and digitally isolate the disaster recovery network from the rest of the organization to prevent attackers from accessing and destroying the backup data.

Event Handler Example

Incidents & Events > Handlers

Once logs are grouped, you can refine the data within each group by applying filter with other log fields. Logs that match the filters will be retained within each group.

Log Filters

All Filters **Any One of the Filters**

Log Field	Match Criteria	Value	Action
Destination Port (dstport)	Not Equal To	0	x +

Destination port does not equal to 0 (which means all other ports)

Optional generic text filter

Log Filter by Text ⓘ

Define the required number of matches within the specified time frame to trigger an event

Once you've organized and filtered the logs, set up criteria that enable the system to automatically initiate events when log records reoccur within each group.

Trigger an event when:

☒ A group contains 1000 or more log occurrences

☐ Within a group, the log field Click to select has 10 or more unique values

☐ The sum of Click to select is greater than or equal to 10

All logs were generated within 5 minutes

This slide shows an example of an event handler that generates an event if there are over a thousand occurrences of any destination port that does not equal 0 within 5 minutes, making this configuration a good way to identify port scanning attempts.

You can create similar event handlers using the *equal* operator to match remote access traffic to a critical server and set up notifications, such as:

- TCP 3389 & 10.1.1.1, or
- TCP 22 & 10.1.1.1

Multiple rules in a basic event handler are matched using an *or* logic, but the log filters inside each rule can follow the **All Filters** (*and*) or **Any One of the Filters** (*or*) logic.

There are other operators available, including Equal To, Not Equal To, Greater Than or Equal To, Less Than or Equal To, Greater Than, and Less Than. If you wish to exclude well-known ports, for example, you can use the Greater Than destination port 1024 configuration.

Depending on your network, you may need to fine-tune the settings, such as defining a unique value requirement for a log field.

Knowledge Check

1. Which reconnaissance method has a lower chance of detection?
☒ A. Passive
☐ B. Active
2. What can attackers do to evade detection?
☒ A. Rename their processes with legitimate-looking names.
☐ B. Establish persistence with the target machine.
3. Which type of malware can self-replicate across a network?
☐ A. Viruses
☒ B. Worms

DO NOT REPRINT
© FORTINET

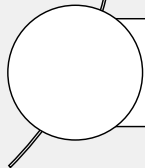
Lesson Progress



The Attack Surface



Attack Vectors



Reviewing Traffic Flows

FORTINET
Training Institute

© Fortinet Inc. All Rights Reserved. 33

Good job! You now understand attack vectors.

Now, you will learn about reviewing traffic flows.

DO NOT REPRINT
© FORTINET

Reviewing Traffic Flows

Objectives

- Describe how to capture traffic on Fortinet devices
- Describe how to capture traffic on an endpoint
- Describe how to use Wireshark to analyze packet captures

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

By demonstrating competence in capturing and analyzing traffic flows on FortiAnalyzer, FortiGate, and endpoints, you can identify potential threats and anomalies within your network. By capturing and analyzing traffic, you can gain insights into the behavior of network devices, and identify any deviations from baseline patterns that may indicate malicious activity.

Packet Capture—Introduction

- As a SOC analyst, you should know how to capture and review traffic flows, so that you can:
 - Analyze the traffic in real time or save a copy
 - Present evidence of a vulnerability or a suspected attack
 - Establish baselines for expected traffic flows
- To capture traffic on FortiAnalyzer and FortiGate on the CLI:

```
# diagnose sniffer packet <interface> '<filter>' <verbosity> <count> <timestamp>
```

- <interface> can be any or a specific interface (that is port1 or internal)
- <filter> follows tcpdump format
- <verbosity> specifies how much information to capture
- <count> the number of packets to capture
- <timestamp> print time stamp information
 - a – prints absolute UTC timestamp
 - l – prints local timestamp

As a SOC analyst, you should know how to capture and review traffic flows.

For example, you may want to know, in real-time, where a critical server is sending information to and receiving information from.

The logs and correlation tools on FortiAnalyzer provide important information. However, you may also wish to examine the packets and the payloads themselves. Packet captures allow you to conduct deeper investigations.

Packet Capture on FortiAnalyzer

Example Sniffer

DNS Traffic traversing port1, on level 1 verbosity, 4 packet limit, and in local system time

CLI Command to Use

```
# diagnose sniffer packet <interface>
<filter> <level> <count> <timestamp>
```

• Example output

```
FAZ# diag sniffer packet port1 'udp and port 53' 1 4 1
interfaces=[port1]
filters=[udp and port 53]
2023-06-28 16:29:17.741947 192.168.42.210.14610 -> 208.91.112.52.53: udp 27
2023-06-28 16:29:17.742016 192.168.42.210.14610 -> 208.91.112.52.53: udp 27
2023-06-28 16:29:17.745001 208.91.112.52.53 -> 192.168.42.210.14610: udp 155
2023-06-28 16:29:17.745047 208.91.112.52.53 -> 192.168.42.210.14610: udp 195
```

System Settings > Network

+ Create New		Edit	Delete	Search...		
☐	Interface	Filter Criteria	# Packets	Max Packet Count	Progress	Actions
☐	port1	port=53	4	4000	(4/4000)	Download

Can also capture using the GUI

In the example shown on this slide, the capture has the following characteristics:

- Traffic on port1
- UDP port 53 (DNS traffic)
- Level 1 verbosity
- Capture limit of four packets
- Local system time

FortiAnalyzer has a built-in packet sniffer, available on the GUI and CLI. It supports versatile filters and verbosity (1-3) levels. The higher the verbosity level, the more information the capture contains. For troubleshooting purposes, Fortinet Technical Support may request level 3 captures.

If you use the GUI to capture the packets, you do not need to use a conversion script. The downloaded file will be in PCAP format.

For more syntax information, consult the *CLI Reference* guide for FortiAnalyzer on docs.fortinet.com.

Packet Capture From the FortiGate CLI

Example Sniffer

ICMP traffic to and from 10.0.10.254, on level 6 verbosity, with no packet limit, and in local system time

CLI Command to Use

```
# diagnose sniffer packet <interface>
<filter> <level> <count> <timestamp>
```

• Example output

```
FortiGate# diagnose sniffer packet Students "icmp and host 10.0.10.254" 6 0 1
2021-05-26 07:43:28.653443 Students -- 10.0.10.2 -> 10.0.10.254: icmp: echo request
0x0000  0009 0f09 0003 5c85 7e32 16a2 0800 4500      .....\.~2....E.
0x0010  0054 9fef 4000 4001 71ba 0a00 0a02 0a00      .T..@.@.q.....
0x0020  0afe 0800 cec5 1686 0001 905e ae60 dff0      .....^.`..
0x0030  0900 0809 0a0b 0c0d 0e0f 1011 1213 1415      .....
0x0040  1617 1819 1a1b 1c1d 1e1f 2021 2223 2425      .....!"#$%
0x0050  2627 2829 2a2b 2c2d 2e2f 3031 3233 3435      &'()*+,-./012345
0x0060  3637
```

In the example shown on this slide, the capture has the following characteristics:

- Traffic on interface Students
- ICMP traffic to and from host 10.0.10.254
- Level 6 verbosity
- No packet capture limit
- Local system time

FortiGate has a built-in packet sniffer, available on the GUI and CLI. It supports versatile filters and verbosity (1-6) levels. The higher the verbosity level, the more information the capture contains. For troubleshooting purposes, Fortinet Technical Support may request level 6 captures.

For more syntax information, consult the *CLI Reference* guide for FortiGate on docs.fortinet.com.

DO NOT REPRINT
© FORTINET

Packet Capture From the FortiGate GUI

- Automatically convert packet capture to PCAP (no conversion script required)
- Embedded real-time analysis page

Network > Diagnostics > Packet Capture

Capture

NPU hardware acceleration must be disabled on the respective firewall policy to see all packets. To do so, set "autosync-offload" to "disable" in the CLI.

Interface:

Name:

Maximum captured packets:

Filters

Filtering syntax: **Basic** **Advanced**

Host:

Port:

Protocol number:

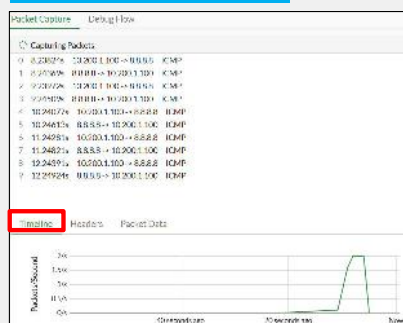
Set up filter to narrow down packet capture as much as possible

If your FortiGate model has internal storage, you can capture packets on the GUI. You can also download the respective PCAP file in case you prefer to review it using Wireshark or another packet analysis tool.

Before starting the packet capture, you should set up the packet capture filter by using either **Basic** or **Advanced** filter options. When you select **Basic**, you can indicate basic filter options, such as host address, port number, and protocol number. In case you want to use your own Berkeley Packet Filter (BPF) like you do on the CLI, you can choose **Advanced**.

Packet Capture From the FortiGate GUI (Contd)

Packet Capture > Timeline



- Useful to identify important traffic events

Packet Capture > Headers

Packet Capture		Debug Flow
Capturing Packets		
0	8.23824s	10.200.1.100 -> 8.8.8.8 ICMP
1	8.24369s	8.8.8.8 -> 10.200.1.100 ICMP
2	9.23972s	10.200.1.100 -> 8.8.8.8 ICMP
3	9.24509s	8.8.8.8 -> 10.200.1.100 ICMP
4	10.24077s	10.200.1.100 -> 8.8.8.8 ICMP
5	10.24613s	8.8.8.8 -> 10.200.1.100 ICMP
6	11.24281s	10.200.1.100 -> 8.8.8.8 ICMP
7	11.24821s	8.8.8.8 -> 10.200.1.100 ICMP
8	12.24391s	10.200.1.100 -> 8.8.8.8 ICMP
9	12.24924s	8.8.8.8 -> 10.200.1.100 ICMP

Timeline		Headers	Packet Data
IP		L4	
Source IP	10.200.1.100	Type	8
Destination IP	8.8.8.8	Code	0
Protocol	ICMP	Checksum	0x1eca

- Basic IP and layer 4 data

Packet Capture > Packet Data

Packet Capture		Debug Flow
Capturing Packets		
0	8.23824s	10.200.1.100 -> 8.8.8.8 ICMP
1	8.24369s	8.8.8.8 -> 10.200.1.100 ICMP
2	9.23972s	10.200.1.100 -> 8.8.8.8 ICMP
3	9.24509s	8.8.8.8 -> 10.200.1.100 ICMP
4	10.24077s	10.200.1.100 -> 8.8.8.8 ICMP
5	10.24613s	8.8.8.8 -> 10.200.1.100 ICMP
6	11.24281s	10.200.1.100 -> 8.8.8.8 ICMP
7	11.24821s	8.8.8.8 -> 10.200.1.100 ICMP
8	12.24391s	10.200.1.100 -> 8.8.8.8 ICMP
9	12.24924s	8.8.8.8 -> 10.200.1.100 ICMP

Timeline		Headers	Packet Data
Q Search			
0	02 00 0f 00 31 0c 02 09	0f 0e 00 31 00 00 45 00	[.....]
10	03 04 c3 05 48 00 3f 01	04 04 0e 28 01 64 08 03	[.....]
20	03 0e 00 0e 25 7c 16 e7	00 01 00 04 04 e7 08 09	[.....]
30	03 0e 25 a5 3d 00 00 09	0e 0e 10 11 10 13 14 75	[.....]
40	5 17 18 1c 1a 1b 1c 1d	14 1f 20 7 25 23 24 25	[.....]
50	25 27 28 2c 7a 2b 2c 2d	26 2f 30 3 30 33 34 35	[.....]
60	5 5 37		[.....]

- Full packet data in HEX and ASCII formats

This slide shows an example of the embedded real-time analysis tool included in the GUI packet capture tool on FortiGate. After you start the packet capture, the GUI starts displaying the captured packets based on the filter set.

The **Timeline** tab displays a graph with the number of captured packets per second. The graph is useful to quickly identify peaks of traffic related by important events in the network.

The **Headers** tab enables you to examine basic IP (layer 3) and layer 4 information on the packet.

The **Packet Data** tab enables you to examine the full packet data using hexadecimal format. Next to the hexadecimal packet data, FortiOS displays the equivalent output in ASCII format.

DO NOT REPRINT

© FORTINET

Packet Capture Verbosity Level

Level	IP Headers	Packet Payload	Ethernet Headers	Interface Name
1	•			
2	•	•		
3	•	•	•	
4	•			•
5	•	•		•
6	•	•	•	•

- FortiAnalyzer supports levels 1–3 only; FortiGate supports levels 1–6
- The most common levels are:
 - 4 – Prints the ingress and egress interfaces
 - You can verify how traffic is being routed, or if FortiGate is dropping packets
 - 3 or 6 – Prints the packet payload
 - You can convert this output to a PCAP file that you can open with a packet analyzer
 - If you don't specify a level, the sniffer uses level 1 by default

The verbosity level specifies how much information you want to display.

Note that FortiAnalyzer supports only levels 1–3, whereas FortiGate supports levels 1–6.

Use verbosity level 4 to take a quick look at how the traffic is flowing through FortiGate (if packets are arriving and how FortiGate is routing them out). You can also use level 4 to check if FortiGate is dropping packets.

Verbosity levels 3 and 6 provide the most output. Both show the IP payloads and Ethernet headers. You can save the output and export it to a PCAP file using a Perl script. Then, you can open the PCAP file with a packet analyzer, such as Wireshark, for further investigation. You can locate the Perl script that converts the sniffer output to PCAP on the Fortinet Knowledge Base website (kb.fortinet.com).

Packet Capture on an Endpoint

Example Sniffer

On NIC Ethernet2:
DNS traffic from and to host 172.17.98.107

Syntax Filter

dns && ip.addr == 172.17.98.107

The screenshot shows the Wireshark interface with the following details:

- Filter:** dns && ip.addr == 172.17.98.107
- Packet List:**

No.	Time	Source	Destination	Protocol	Length	Info
148	4.670612	172.17.98.107	8.8.8.8	DNS	72	Standard query 0x0005 A fortinet.com
149	4.671638	8.8.8.8	172.17.98.107	DNS	104	Standard query response 0x0005 A fortinet.com A 54.251.118.105 A 54.177.212.176
155	4.680791	172.17.98.107	8.8.8.8	DNS	72	Standard query 0x0006 AAAA fortinet.com
157	4.681422	8.8.8.8	172.17.98.107	DNS	116	Standard query response 0x0006 AAAA fortinet.com AAAA 54.251.118.105
- Packet Details (Packet 148):**
 - Ethernet II, Src: Dell (11:9f:d1:ac:1d:11:9f:d1), Dst: Fortinet (08:00:00:0c:29:00:00:00)
 - Internet Protocol Version 4, Src: 172.17.98.107, Dst: 8.8.8.8
 - User Datagram Protocol, Src Port: 5587, Dst Port: 53
 - Domain Name System (query)
 - Transaction ID: 0x0005
 - Flags: 0x0010 Standard query
 - Questions: 1
 - Answer RRs: 0
 - Authority RRs: 0
 - Additional RRs: 0
 - Queries
 - fortinet.com: type A, class IN
- Packet Bytes:** Shows raw hex and ASCII data for the packet.

FORTINET
Training Institute

© Fortinet Inc. All Rights Reserved. 41

This slide shows a real-time packet capture in Wireshark with the following characteristics:

- Traffic on the network adapter Ethernet2
- UDP port 53 (DNS traffic)
- Delta time of around 4 seconds since the packet capture started

In the lower-left pane, you can see more details about the packet. In the lower-right pane, you can see the payload information.

The number of packets is not listed in a sequence because the filters exclude non-matching results (packet 149 is followed by packet 155). Therefore, you can infer that there are many packets that are not DNS traffic. Note, if your traffic uses a custom port, such as an RDP session that uses a different listening port, you want to specify the port in the filter instead of the protocol, unless you have already configured Wireshark to recognize that custom port for the traffic type.

This slide provides only a basic introduction to Wireshark. There are many features that are not shown. For more detailed information, you can consult the official Wireshark documentation at <https://www.wireshark.org>.

DO NOT REPRINT
© FORTINET

Knowledge Check

1. Which packet capture method does not require a PCAP file conversion script?
☒ A. GUI
☐ B. CLI
2. Which packet capture setting is different between FortiAnalyzer and FortiGate?
☐ A. Timestamp
☒ B. Verbosity

DO NOT REPRINT
© FORTINET

Lesson Progress



The Attack Surface



Attack Vectors



Reviewing Traffic Flows

FORTINET
Training Institute

© Fortinet Inc. All Rights Reserved. 43

Congratulations! You have completed this lesson.

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

DO NOT REPRINT
© FORTINET

Review

- ✓ Describe the attack surface
- ✓ Describe how to identify the attack surface
- ✓ Describe how to reduce the attack surface
- ✓ Describe common attack vectors
- ✓ Describe security best practices against attack vectors
- ✓ Describe defenses against attack vectors
- ✓ Describe how to capture traffic on Fortinet devices
- ✓ Describe how to capture traffic on an endpoint
- ✓ Describe how to use Wireshark to analyze packet captures

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

By mastering the objectives covered in this lesson, you learned about the attack surface, the attack vectors that can comprise the attack surface, and how to review and capture traffic flows.

DO NOT REPRINT
© FORTINET

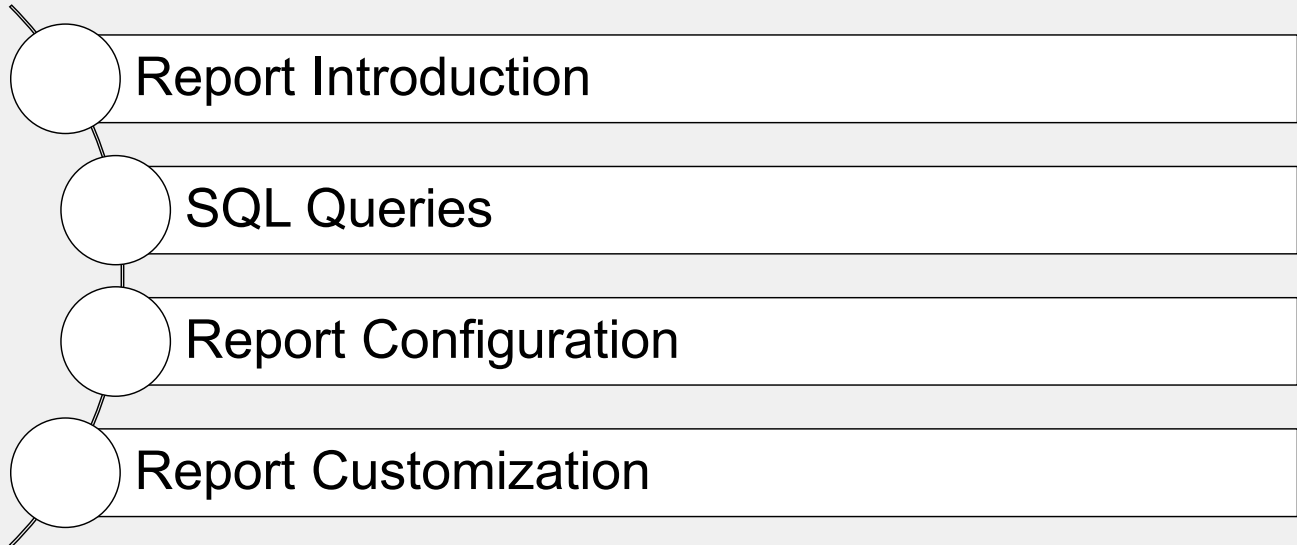


In this lesson, you will learn about cybersecurity reporting. As a SOC analyst, you will need to be skilled in documenting various scenarios that have happened in the network, in the form of reports. The purpose of the reports can range from detailing security incidents, analyzing traffic patterns, auditing user behavior, and more.

FortiAnalyzer provides comprehensive and flexible reporting, which enables organizations to collate, organize, and present data cohesively and effectively.

DO NOT REPRINT
© FORTINET

Lesson Overview



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

DO NOT REPRINT
© FORTINET

Report Introduction

Objectives

- Describe the considerations of SOC reporting
- Review the basic components of a FortiAnalyzer report

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

By demonstrating a competent understanding of what a cybersecurity report is, you will be able to identify your organization's requirements and create your own. You will also learn which components comprise a report in FortiAnalyzer so that you can create your own reports.

Purpose of Reports



- Reports can have different purposes depending on your requirements

- Some common purposes include:

Summarizing

Analyzing

Correlating

Recommending



The purpose of a report varies depending on what your organization's requirements are. However, there are some common purposes for reports, including:

Summarizing logs: Simplify and aggregate large amounts of logged data. Based on configured report parameters, FortiAnalyzer can extract data and present it in a graphical manner that makes it easier—and quicker—to digest.

Analyzing logs: Examine data at a deeper level to find patterns, trends, and insights that a summary cannot provide. For example, if you notice an interesting trend in network traffic, an analysis is required to prove your case and collect evidence. Moreover, a detailed analysis can both support a claim or refute a claim. If you believe a different team member has erroneously interpreted the data, you can use your own report to refute the findings.

Correlating logs: Compare and contrast sets of data. You can create a report that focuses on correlation to identify how different factors influence each other, providing context and establishing a link. For example, a correlation report in a cybersecurity context might link user behavior patterns during different working hours. On their own, without a baseline, the data does not reveal enough information. Together, however, the data gains context.

Recommending changes: Provide suggestions for changes by presenting log data. If you notice any deficiencies in security, a report is a good way to organize your findings and present them to stakeholders.

Report Types

- Within the SOC, the Red, Blue and Purple teams may be responsible for different types of reports
- The target audience should determine how technical the report is
- Examples:

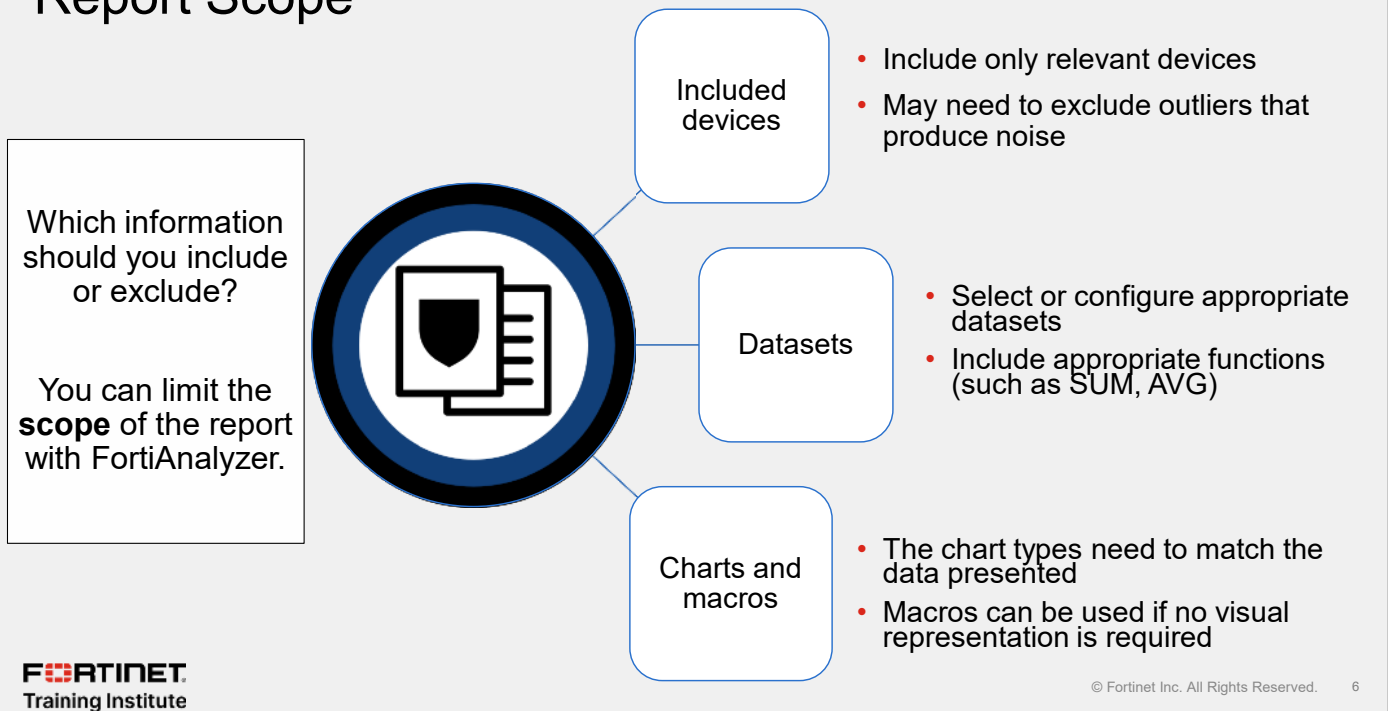
Team	Report Type
Red	Penetration testing
	Attack simulation
	Vulnerability findings
Blue	Incident response
	Monitoring
	Threat intelligence
Purple	Comprehensive security assessment
	Combined red and blue team reports
	Training exercise findings

Within the SOC team, the red, blue, and purple teams can provide different types of reports:

- The red team provides reporting on offensive security, such as penetration testing, attack simulations, and vulnerability findings.
- The blue team provides reporting on defensive security, such as incident response, monitoring, and threat intelligence.
- The purple team provides reporting on both offense and defense, such as bridging the knowledge gap between the red and blue teams, and training exercises

Depending on the intended audience, you can adjust the technical level of the report accordingly. The same type of report, such as an incident response report, can be tailored to two different target audiences. For example, if the report is targeted toward upper management, you may want to focus on the high-level findings. On the other hand, if the report is aimed toward a senior SOC team member, you should include technical details.

Report Scope



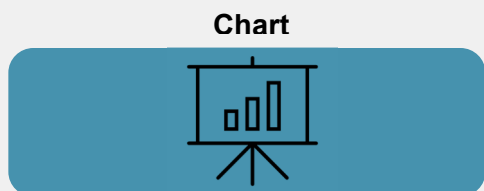
When configuring a report, you need to decide what to include and what to exclude. How you make those decisions depends on the *scope* of your report. Are you generating a report to detail a security incident, provide an overview of network traffic, investigate traffic patterns that traverse a firewall, or review VPN usage?

Some general guidelines for your reporting scope when using FortiAnalyzer:

- Include only relevant devices, and account for outliers that may skew the results: For example, if you are generating a report for bandwidth usage, you may want to exclude noisy data. You also want to ensure that you are generating a report for the proper timeframes. Continuing with the bandwidth example, if you design the report to provide insight on traffic that occurs during business hours, exclude traffic that occurs outside business hours and during maintenance windows, which can skew the data.
- Configure appropriate datasets: FortiAnalyzer uses datasets to extract information from the SQL database. To make the report easier to digest, you need to present the information in a logical manner, such as aggregating values to provide a bigger picture of the network.
- Select the right types of charts: You want to select the proper representation for the data that you have. For example, if you have many suspicious hosts sending traffic to unknown destinations, you may want to use a table. On the other hand, if you are concerned about which host is sending the most traffic on the network without needing to see the destination, a pie chart could be the better option. The different chart types and the use of macros are discussed later in the lesson.

FortiAnalyzer Report Elements

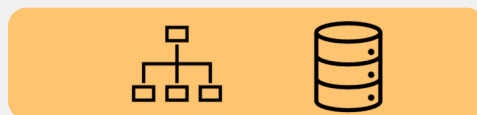
- A FortiAnalyzer report is a set of data organized in charts



- Which **data** from the SQL database is displayed
- Which **format** the data is displayed in

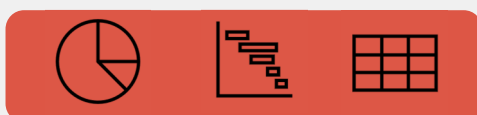


Dataset



- Datasets are specific SQL `SELECT` queries

Format



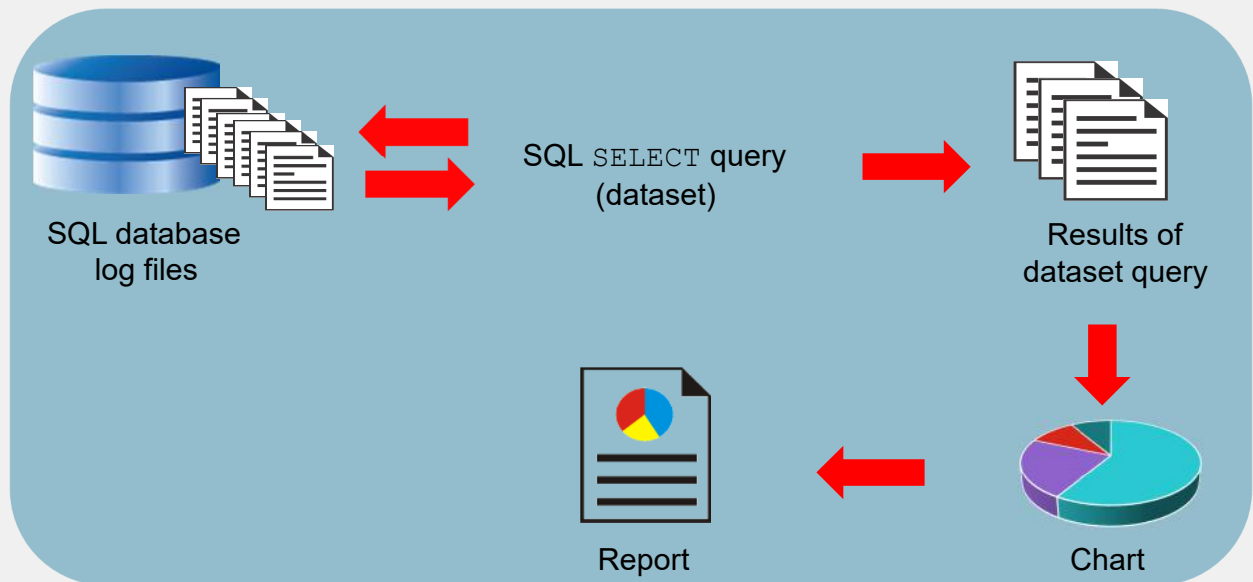
- Format options: pie charts, bar charts, tables, and more

A FortiAnalyzer report is a set of data organized in charts. Charts consist of two elements:

- Datasets: SQL `SELECT` queries that extract specific data from the database
- Format: how the data is displayed (for example, pie charts, bar charts, tables, and more)

DO NOT REPRINT
© FORTINET

Report Workflow



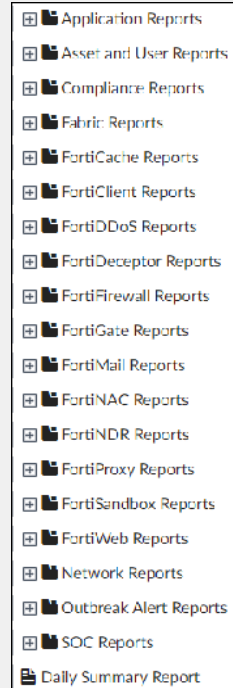
As the graphic on this slide shows, the FortiAnalyzer SQL database contains all the logs. More accurately, SQL is the *database language* that FortiAnalyzer uses for logging and reporting, while the underlying database management system is PostgreSQL. A SQL `SELECT` query polls the database for specific information. Based on the query, FortiAnalyzer extracts a subset of information stored in the logs.

This subset of data populates a chart, and a report contains one or more charts.

Reports and ADOMs

- Each ADOM has its own reports, libraries, and advanced settings
- Additional reports are available when specific ADOMs are enabled
- Verify you are in the right ADOM when creating reports

Note: A fabric ADOM has predefined reports for multiple device types



When you enable ADOMs, each ADOM has its own reports, libraries, and advanced settings. As such, make sure that you are in the correct ADOM before selecting a report.

Additional reports for specific Fortinet devices are available only when you enable ADOMs. This slide does not show all the available default report types. You can configure and generate reports for these devices within their respective ADOMs. These devices also have device-specific charts and datasets.

DO NOT REPRINT
© FORTINET

Knowledge Check

1. Charts consist of which two elements?
 - ✓ A. Dataset and format
 - B. Data and queries

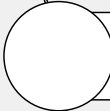
2. Which statement about reports is true?
 - A. Reports are ADOM-specific.
 - ✓ B. Reports are not ADOM-specific.

DO NOT REPRINT
© FORTINET

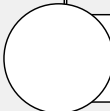
Lesson Overview



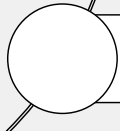
Report Introduction



SQL Queries



Report Configuration



Report Customization



© Fortinet Inc. All Rights Reserved. 11

Good job! You now understand the basics of reporting.

Now, you will learn about using SQL queries on FortiAnalyzer.

DO NOT REPRINT
© FORTINET

SQL Queries

Objectives

- Describe SQL basics
- Describe FortiAnalyzer schemas
- Use FortiAnalyzer tools for simplifying SQL queries

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

By demonstrating competence in basic SQL queries, you will be able to extract information from collected logs and present them in a logical manner.

SQL—The Declarative Language

```
SELECT dstip as destination_ip, count(*) as Session  
FROM $log WHERE $filter and dstip is not null GROUP  
BY dstip ORDER BY session desc LIMIT 7
```

- SQL is a *declarative* language: describes *what* needs to be done rather than *how* to do it
- All information in the database is represented as tables
 - Each table consists of a set of rows and columns
 - Two types of tables: user tables and system tables
- A *record* is a single row in a table

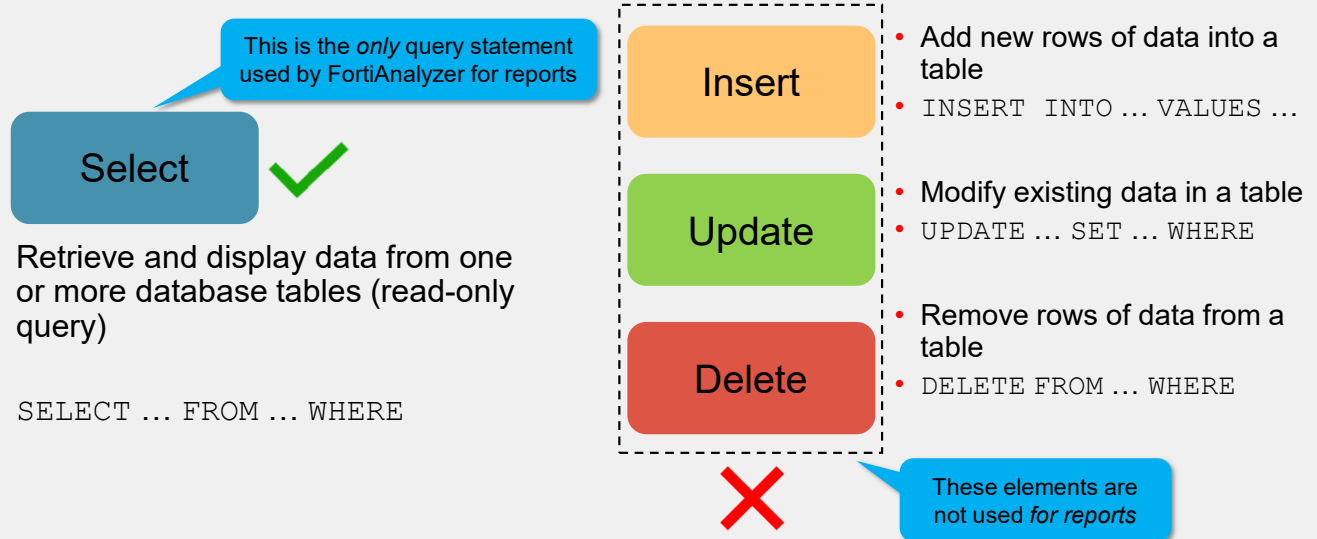
SQL is known as a declarative language—it describes *what* needs to be done rather than *how* to do it. In a declarative language, the focus is on the result. SQL is responsible for determining *how* best to achieve a result so that the user does not need to specify the steps to get there. As a SOC analyst, you do not need to know how SQL is retrieving records from the database. For FortiAnalyzer reports, your goal is to ask SQL what you want to query from the database.

In order to understand this example dataset, and more specifically, what it is querying, you need to understand SQL. In a SQL database, all information is represented as tables, and each table consists of a set of rows and columns. Each row is a record. There are two types of tables:

- User tables, which contain data that is stored in the database
- System tables, which contain the database metadata and system-related information

DO NOT REPRINT
© FORTINET

Basic Data Manipulation Constructs



To retrieve and manipulate data in a database, use the following SQL data manipulation language (DML) commands: SELECT, INSERT, UPDATE, and DELETE.

You use only the SELECT statement in FortiAnalyzer reports. It is a read-only query statement that you can use to retrieve data from the database.

SELECT Statement

Clauses	Definition
FROM	From which tables or views the data will be extracted
WHERE	Sets the conditions (only rows that satisfy the conditions appear in the output)
GROUP BY	Collects data across multiple records and groups the results by one or more columns
ORDER BY	Orders the results by specific columns, ascending or descending
LIMIT	Limits the number of records returned based on a limit value
OFFSET	Often used with the <code>LIMIT</code> clause to offset the results by a set value

Following
`SELECT`, you must
use these clauses
in a specific
sequence

To extract the desired data, you need to specify the criteria to be used. In order to put this criteria into a language that SQL understands, you must use one or more clauses recognized by the `SELECT` statement.

The main clauses FortiAnalyzer reports use are as follows:

- `FROM`, which specifies from the tables or views from which FortiAnalyzer extracts the data.
- `WHERE`, which specifies the conditions. Only rows that satisfy the conditions appear in the output. You can use `WHERE` with logical operators to narrow the query. Common logical operators include `AND`, `OR`, and `NOT`.
- `GROUP BY`, which collects data across multiple records and groups the unique results by one or more columns. You can use aggregate functions on the grouped results.
- `ORDER BY`, which orders the results by specific columns. Unless you use `ORDER BY`, FortiAnalyzer returns the records in the order it generates them.
- `LIMIT`, which limits the number of records FortiAnalyzer returns, based on a specified value.
- `OFFSET`, a clause often used along with `LIMIT`, which offsets results by the number specified. For example, if you place a limit of three records and an offset of one, FortiAnalyzer skips the first record and, instead, returns the second, third, and fourth records (three in total).

`FROM` is the only mandatory clause required to form a `SELECT` statement. The rest of the clauses are optional and serve to filter or limit, aggregate or combine, and control the sort. It is also important to note that the clauses must be coded in a specific sequence. Following `SELECT`, the statement must be followed by one or more clauses in the order in which they appear in the table shown on this slide. For example, you can't use the `WHERE` clause before the `FROM` clause. You don't have to use all optional clauses, but the clauses you do use must be in the correct sequence.

DO NOT REPRINT

© FORTINET

SELECT Statement (Contd)

Function	Definition
DISTINCT	Removes duplicate rows from the results
COALESCE	Returns the first non-null value from a list of expressions, or substitutes null with a default value
NULLIFNA	Filters out n/a values, often used with COALESCE
COUNT	Returns the number of rows that match the criteria
SUM	Returns the total sum of a column
AVG	Returns the average value of a column
MIN	Returns the minimum value of a column
MAX	Returns the maximum value of a column
FROM_DTIME	Returns the device timestamp without its time zone
FROM_ETIME	Returns FortiAnalyzer's timestamp without its time zone
AS	Creates an alias for a column or table
UPPER	Converts a string to uppercase letters
LOWER	Converts a string to lowercase letters

This slide lists some common functions you can use with `SELECT` queries. Functions in SQL require a following expression in parentheses. For example, to use `SUM`, you would need to specify `SUM(sentbyte)`.

- `DISTINCT`, which removes duplicate rows from the results. Only unique rows are returned. It does not allow you to use aggregate functions directly, unlike `GROUP BY`.
- `COALESCE`, which can be used with `SELECT` to return the first non-null value from a list of expressions or inserts a substitute value in place of null.
- `NULLIFNA`, which is often used along with `COALESCE`, to filter out n/a values and make them null. For example, `SELECT COALESCE(NULLIFNA('user'), NULLIFNA('srcip'))`, returns the actual value of the `user` column unless the value is n/a, in which case the value from `srcip` is returned. The `COALESCE` function checks the result of `NULLIFNA` and populates the first non-null value.
- Aggregate functions perform a calculation on a set of values and return a value. Examples include `COUNT`, which counts the number of rows in the results; `SUM`, which tabulates the total value of a column; `AVG`, which calculates the average of a column; `MIN`, which finds the minimum value; `MAX`, which finds the maximum value.
- The `UPPER` and `LOWER` functions are used to convert strings to a uniform set of cases (capitals or lowercase letters) to avoid case sensitivity issues and standardize output.
- In addition to standard SQL queries, `FROM_DTIME` and `FROM_ETIME` are FortiAnalyzer-specific functions: `etime` is generated by FortiAnalyzer when it receives a log, so it uses FortiAnalyzer's local timestamp. On the other hand, `dttime` uses the sending device's timestamp.

Accessing the SQL Schema

Reports > Report Definitions > Datasets

Name	Test Dataset
Log Type	Traffic
Query	1 select * from \$log

Select log type

This query returns everything from the log type selected

Go	Stop
Time Period	Previous 7 Days
Devices	All Devices

id	bid	dvid	itime	dtime	euid	epid	dsteuid	dstepid	logflag	logver
7285771809847446860	650012	1064	1696350940	1696325646	3	104	3	1032		704012463

Column headings indicate what is available in the database schema for the log type selected

To create a query, you first need to know what is included in the database schema. The schema includes the different fields, or columns, that are available, and from which you can extract information for reports. In FortiAnalyzer, you can obtain the schema for a specific log type by creating and testing the following dataset query:

```
SELECT * FROM $log
```

This query can be read as: "Select everything from the logs table." Note that you do *not* want to use `SELECT * FROM $log` in your actual query. You are only using this query temporarily to see the available fields in a table.

For traffic logs, for example, associate the **Traffic** log type with this dataset in the **Log Type** field. This query returns everything from the **Traffic** log type. The column heading names indicate what is available in the database schema for the log type selected. The * symbol returns all data. Note that not all column headings are shown in the example on this slide.

After you type the query in the **Query** field, click **Go** to run the query.

Accessing the SQL Schema (Contd)

Name	Test Dataset
Log Type	Traffic
Query	1 select * from \$log

Hover your mouse over the hyperlink to display the schema

These are all the available fields you can use for queries from the **Traffic** log table

Table "Logs" has the following fields:

```
id, bid, dvid, itime, dtime, euid, epid, dsteuid, dstepid, logflag, logver,
sfid, type, subtype, level, action, utmaction, policyid, sessionid, srcip,
dstip, tranip, transip, srcport, dstport, tranport, transport, trandisp,
duration, proto, vrf, slot, sentbyte, rcvbyte, sentdelta, rcvdelta,
sentpkt, rcvdpkt, logid, user, unauthuser, dstunauthuser, srcname, dstname,
group, service, app, appcat, fctuid, srcintfrole, dstintfrole, srcserver,
dstserver, appid, appact, apprisk, wanoptapptype, policytype, centralnatid,
channel, vupvlanid, shapingpolicyid, eventtime, vulid, shaperdropsentbyte,
shaperdroprcvbyte, shaperperipdropbyte, wanin, wanout, lanin, lanout,
csrcore, craction, crlevel, countapp, countav, countdlp, countemail,
countips, countweb, countwaf, countssl, countssh, countdns, srcuuid, dstuuid,
poluuid, srcmac, mastersrcmac, dstmac, masterdstmac, srchvender,
srchwversion, srcfamily, srcswversion, dsthvender, dsthwversion, dstfamily,
dstswversion, devtype, devcategory, dstdevtype, dstdevcategory, osname,
osversion, dstosname, dstosversion, srccountry, dstcountry, srcssid, dstssid,
srcintf, dstintf, srcinetsvc, dstinetsvc, unauthusersource,
dstunauthusersource, authserver, applist, vpn, vpntype, radioband,
policyname, policymode, sslaction, url, agent, comment, ap, apsn, vulservice,
vulquality, collectedemail, dstcollectedemail, shapersentname,
shaperrcvdname, shaperperipname, msg, custom_field1, utmevent, utmsubtype,
sender, recipient, virus, attack, hostname, catdesc, dlpsensor, utmref,
tdinfo, dstowner, tdtype, tdscantime, tdthreatype, tdthreatname, tdwfcat,
threatvgt, threatcnts, threatlvs, saasinfo, ebtime, clouduser, threats,
threattypes, apps, countff, identifier, securityid, securityact, tz,
srcdomain, counticap, dstregion, srcregion, dstcity, srccity, signal, snr,
dstauthserver, dstgroup, dstuser, tunnelid, vulname, srcthreadfeed,
dstthreadfeed, psrport, pdstport, countsctpf, srcreputation, dstreputation,
vip, accessproxy, gatewayid, clientdeviceid, clientdeviceowner,
clientdevicetags, httpmethod, referralurl, saasname, srcmacvender,
shapingpolicyname, accessctrl, countcifs, proxyapptype,
clientdevicemanageable, emsconnection, realserverid, fwdsvr, replydstintf,
replysrcintf, countvpatch, countcasb, devid, vd, devname, csf, devgrps
```

You can hover your mouse over the hyperlink in the query to open a window that displays all the available fields for that table. In this case, you are querying the **Traffic** log table.

As you can see on this slide, the number of fields can be very large, which makes it hard to know which fields you may want to use in your dataset. For this reason, cloning and editing one of the predefined datasets may be the best approach, if none of them meet your requirements.

Accessing the SQL Schema (Contd)

- srcip and srcport chosen from the schema

Table "Logs" has the following fields:

sfsid, type, subtype, level, action, utmaction, policyid, sessionid, **srcip**,
dstip, tranip, transip, **srcport**, dstport, tranport, transport, trandisp,

- Sample query using srcip and srcport

```
1 select srcip as "Source IP", srcport as "Source Port"
2 from $log
3 where $filter and srcip = '10.0.1.10'
4 group by srcip, srcport
5 order by srcport desc
```

- Results

Source IP	Source Port
10.0.1.10	60999
10.0.1.10	60998
10.0.1.10	60993

You can use the fields you identify in the schema to build your queries. For example, you can select `srcip` and `srcport` from the traffic log type, and then create a query.

In the example shown on this slide, the results return the same IP address, `10.0.1.10`, but there are three different source ports, sorted by descending order.

After validating that your query is returning the desired results, you can add the dataset to a chart, and then use the chart in a report.

Example Query

- Data populates a chart
- Datasets are SQL SELECT queries, used to extract data from the database
- The keywords from the previous slides are in purple

Chart

Name	Top 5 Attacks by Severity
Description	Top 5 attacks by severity
Dataset	threat-Attacks-By-Severity 

Dataset

Name	threat-Attacks-By-Severity
Log Type	Intrusion Prevention
Query	<pre>1 select (case when severity='critical' then 'Critical' when severity='high' then 'High' when severity='medium' then 'Medium' when severity='low' then 'Low' when severity='info' then 'Info' end) as severity, count(*) as totalnum from \$log where \$filter group by severity order by totalnum desc</pre>

In the example on this slide, the **Top 5 Attacks by Severity** chart contains a dataset named **threat-Attacks-By-Severity**. As discussed earlier in this lesson, charts are populated using data extracted by SQL queries, and then reports contain charts.

The dataset uses a SQL `SELECT` query to:

- Find intrusion prevention logs.
- Group logs with the same severity levels.
- Tally the total number of logs for each level.
- Sort each level in descending order.

Knowledge Check

1. Which clause is required after a `SELECT` statement?
 - ✓ A. `FROM`
 - B. `WHERE`

2. If `ORDER BY` is not specified, what is the default sorting setting?
 - A. Ascending
 - ✓ B. No sorting

DO NOT REPRINT
© FORTINET

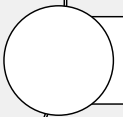
Lesson Overview



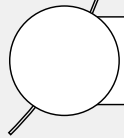
Report Introduction



SQL Queries



Report Configuration

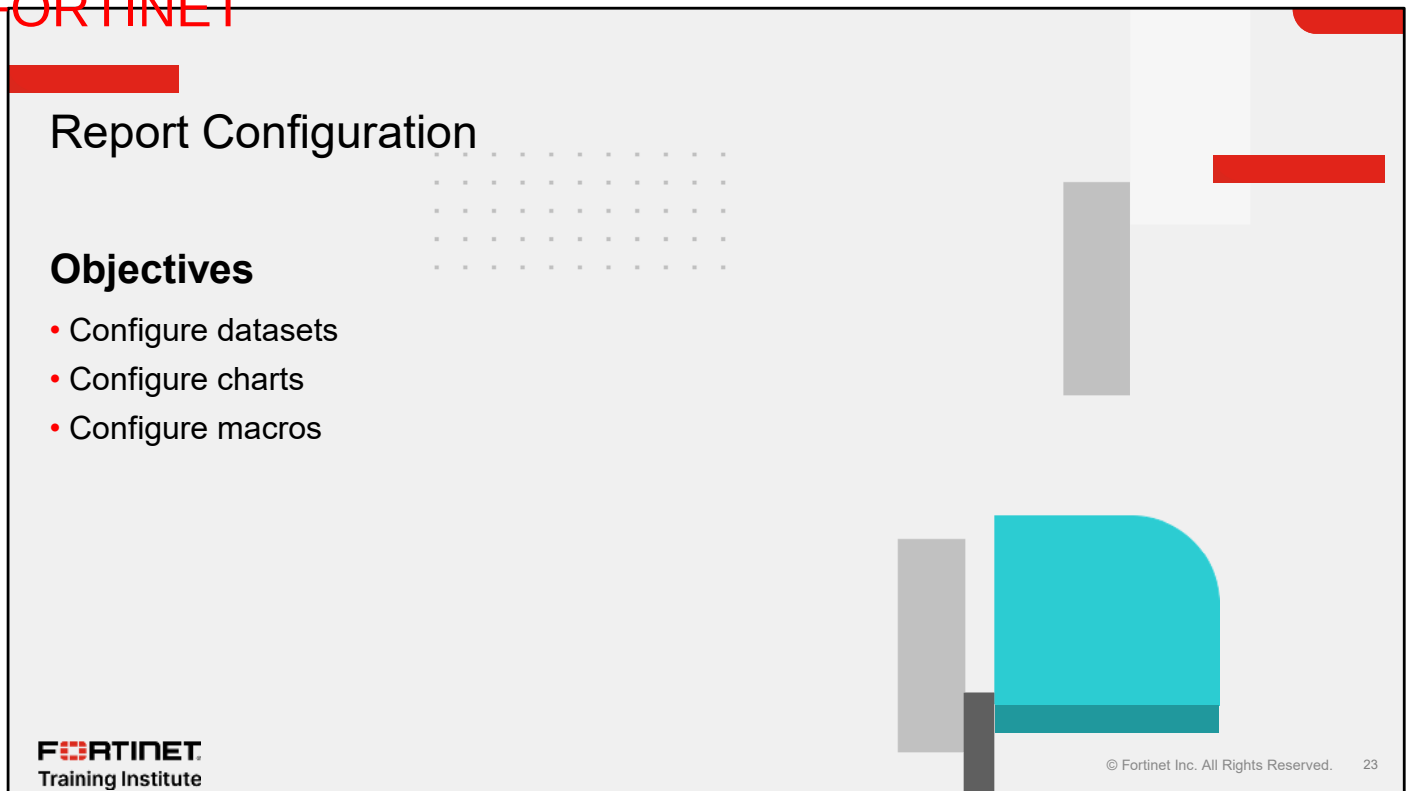


Report Customization

Good job! You now understand basic SQL queries on FortiAnalyzer.

Now, you will learn about configuring datasets, charts, and macros.

DO NOT REPRINT
© FORTINET

The slide features a light gray background with several decorative elements: a red horizontal bar at the top left, a grid of small gray dots in the upper center, a vertical gray bar on the right, a red horizontal bar on the right, and a large cyan rounded rectangle at the bottom right. The text is positioned on the left side of the slide.

Report Configuration

Objectives

- Configure datasets
- Configure charts
- Configure macros

FORTINET
Training Institute

© Fortinet Inc. All Rights Reserved. 23

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

By demonstrating competence in the configuration of datasets, charts, and macros, you will be able to present log data in a meaningful and organized manner. This will also allow you to granularly modify your reports if the requirements change.

If Predefined Charts or Datasets Do Not Meet Requirements

- By default, the **Chart Library** contains hundreds of charts, and the **Datasets** library contains hundreds of datasets
 - Can't edit default charts and datasets
- However, just like templates and reports, you can clone and edit both charts and datasets, and create new ones
- Gives you the flexibility to pull a unique combination of data from the database that doesn't exist in any default chart or dataset

In some cases, simply adding or removing default charts from a report or template may not meet your requirements: You might need to pull a unique combination of data from the database when no predefined chart or dataset for that unique combination exists. In this case, you can either clone and edit charts and datasets, or create new charts and datasets from scratch.

Configuring a Dataset

- Define a name and log type
- Define your SQL query

Reports > Report Definitions > Datasets

Name	threat-Top-Attacks-Blocked
Log Type	Intrusion Prevention
Query	<pre>1 select attack, count(*) as attack_count from \$log where \$filter and nullifna(attack) is not null and action not in ('detected', 'pass_session') group by attack order by attack_count desc</pre>

💡 Recommendations

Validate Analyze Query Format

This slide shows the predefined **threat-Top-Attacks-Blocked** dataset as an example.

You need to define a name, the log type, and the SQL query. FortiAnalyzer provides tools to create a new query or use an existing one as a basis. However, if you wish to modify a predefined dataset, you need to clone it and make changes to the clone. You cannot modify predefined datasets.

When creating or editing a dataset, click **Recommendations** to check similar predefined dataset queries. The query does not have to be complete or validated because FortiAnalyzer will try to extract log fields and function names from the input query string to find similar predefined datasets.

Once you create a dataset, you can click **Validate** to check the dataset query for errors. If the validation result contains a warning or error message, click **Show Examples** to review query examples on how to correct the issues.

To perform a detailed analysis on the SQL query, click **Analyze Query**. This function displays the SQL validation results, if the SQL goes through transformation, and enables you to view the hcache query used when a report using this dataset has enabled the auto-cache option for faster report generation.

Click **Format** to automatically format the SQL query you entered, making it easier to read, update, and detect errors.

Formatting a Query

Reports > Report Definitions > Datasets

Query

```
1 select attack, count(*) as attack_count from $log
where $filter and nullifna(attack) is not null
and action not in ('detected', 'pass_session')
group by attack order by attack_count desc
```

Recommendations

Validate

Analyze Query

Format

Click **Format** to change the query display to a readable format

```
SELECT
  attack,
  count(*) AS attack_count
FROM
  $log
WHERE
  $filter
  AND nullifna(attack) IS NOT NULL
  AND ACTION NOT IN ('detected', 'pass_session')
GROUP BY
  attack
ORDER BY
  attack_count DESC
```

Figuring out what a dataset does may seem daunting at first. However, when you break down a query into smaller pieces and apply formatting, the task becomes much easier. On this slide, you can see the predefined **threat-Top-Attacks-Blocked** dataset example again. The top image shows the query with the default formatting, with everything in one continuous sequence. The bottom image shows the same query after using the **Format** function. Keep in mind that the example shown on this slide is still a relatively simple query. More complex queries can contain complex nesting and multiple logic operators.

The query starts off with a **SELECT** query. Inside that query, **attack** is the column included in the result, and **count(*)** function counts the number of rows for each distinct value of **attack** and labels this column as **attack_count**. In other words, if there are two instances of “Phishing” in the **attack** column, the **attack_count** column will return 2.

The mandatory **FROM** clause follows. The log type is **Intrusion Prevention** (shown on the previous slide).

The **WHERE** clause follows, with the **filter** variable first, which are the constraints you defined in the GUI, such as the time range. Next, is the logical operator **AND**, which matches only traffic that is not null. Lastly, another **AND** follows, which excludes rows with the action **detected** and **pass_session**. The log data must match all three conditions.

The **GROUP BY** clause groups the rows by unique values in the **attack** column. If there are multiple columns in the **SELECT** clause, you need to specify all of them, except for aggregate functions, such as **COUNT**. This example shows only one non-aggregate column.

The table is sorted by the highest attack count to the lowest attack count using **ORDER BY**.

Specificity in the Dataset

- Use specific SQL queries to retrieve the exact logs you want without further filtering
- The downside is that if you need to adjust the filters (such as the device), you must change the SQL query
- Alternatively, specify filters in the report instead of the dataset so that you can use one dataset to generate different reports

Reports > Report Definitions > All Reports > Settings

Generated Reports	Settings	Editor
Path	All Reports/SOC Reports	
Name	Custom Security Analysis	
Time Zone	Default	
Time Period	Previous 7 Days	
	☐ Include additional data until the scheduled report run time 06/10/2024 00:00:00 - 06/16/2024 23:59:59 (for example)	
Devices	☒ All Devices ☐ Specify	
Subnets	☒ All Subnets ☐ Specify	
☒ Generate separate report per-device/VDOM		

It is important to consider how specific you want your datasets to be. By using very specific SQL queries, you can extract the desired data without the need for additional filtering. However, if you want to adjust filters later, such as changing the device filter, you will have to modify the SQL query itself. An alternative approach is to specify filters in the report settings rather than in the dataset. This method allows for more flexibility as you can reuse the same dataset to generate different reports by applying various filters at the report level. This way, one dataset serves multiple purposes, reducing the need for multiple datasets and simplifying the reporting process.

Configuring a New Chart

- Define a name, description (optional)
- Pick a dataset
- Pick a chart type
- Inherit, disable, or enable hostname resolution
- Toggle between **Sample Data** and **Real Data** in the preview section

Reports > Report Definitions > Chart Library

Common

Name

Custom Destination by Bandwidth Chart

Description

Custom Destination by Bandwidth Chart

Dataset

Top-Destinations-By-Bandwidth

Resolve Hostname

Inherit

Type

Table

Table Type

☐ Regular
 ☒ Ranked
 ☐ Drilldown

Order By

☐
☒

Sample Data

#	Column Title 1	Aggregate Title 1	% of Total
1	hitronhub.home	9,400,440	20.54%
2	fortinet-us.com	6,559,096	14.32%

When you create a new chart, you will need to define a name, pick a dataset, and pick a chart type. The description is optional.

Depending on the dataset and chart type selected, you will have further options for customization. For example, for the **Table** type, you can choose to rank the results based on the highest values.

Resolving hostnames when generating a report could take a long time if there is a lot of data, so consider disabling the option. These are the available options:

- Inherit: The chart will inherit the resolve hostname configuring of the report.
- Enabled: Resolving hostnames on FortiAnalyzer for this chart is enabled.
- Disabled: Resolving hostnames on FortiAnalyzer for this chart is disabled.

Once you have selected the parameters for your chart, you will see a preview of what it could look like. Note that the real chart may not look identical to the preview. You can also toggle between using sample data or real log data for the preview. If you do not have any data yet, or if you prefer a faster preview, use the **Sample Data** option.

Building Datasets and Charts From Search Results

- In **Log View**, set filters to search for logs and then use the chart builder

Log View > More > Chart Builder

Create Custom View Refresh More Columns More

Real-time Log Raw Log Case Sensitive Search Download Chart Builder

receive any log from device FortiMail[FE] De
performance status: log rate low (36%), k Per

Chart Builder

Name Traffic from 10.0.1.10

Columns Search...

☒ Date/Time
☒ Device ID
☐ User
☒ Destination IP
☒ Service
☐ Application
☐ Sensor

Query

select from _time(time) as time, 'devic', 'dstip', 'service'
from \$log where \$filter and (logflag&1>0) and (('srcip' =
inet('10.0.1.10/'))

Preview

Date/Time	Destination IP	Service
11:49:23		
2023-10-13 10:39:48	FGVM010000064692 8.8.8.8	DNS
2023-10-13 10:39:48	FGVM010000064692 8.8.8.8	DNS
2023-10-13 10:39:48	FGVM010000064692 8.8.8.8	DNS
2023-10-13 10:39:48	FGVM010000064692 8.8.8.8	DNS
2023-10-13 10:39:48	FGVM010000064692 8.8.8.8	DNS
2023-10-13 10:39:48	FGVM010000064692 8.8.8.8	DNS

Group By (None)

Order By (None)

Sort Descending

Show 50

Limit

Device All Devices

Time Last 7 Days

Frame

Search srcip="10.0.1.10"

Test your query Preview Save Cancel

Dataset builds automatically based on search filters and fine-tuning parameters

Save as dataset and chart

© Fortinet Inc. All Rights Reserved. 29

Use the **Chart Builder** tool to quickly build a custom dataset and chart. This tool is located in **Log View**, and allows you to build a dataset *and* a chart together automatically, based on your filtered search results. It is a great option for SOC analysts who do not find a suitable predefined dataset and chart combination, but who also do not want to write a SQL query.

In **Log View**, set filters to return the logs you want. Then, in the **More** menu, select **Chart Builder** to automatically build the search into a dataset and chart. You can also fine-tune the dataset further by:

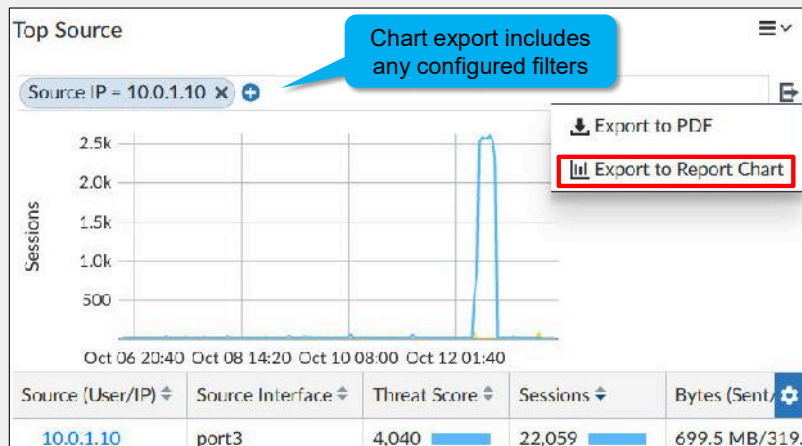
- Adding more columns
- Setting **Group By**, **Order By**, and **Sort** filters
- Setting a limit on results
- Setting the device and time frame

DO NOT REPRINT
© FORTINET

Export a Chart From FortiView

- Similar to the **Chart Builder** feature in **Log View**, you can export a chart from **FortiView**

FortiView



Export to Report Chart

Name	Source 10.0.1.10
Time	From 2023-10-6 16:26 To 2023-10-13 16:26
Device	
Filter	srcip=10.0.1.10
Top	0 0 for no limit

© Fortinet Inc. All Rights Reserved. 30

Similar to how you can use the **Chart Builder** feature in **Log View**, you can export a chart from FortiView. The chart export includes any filters you set on FortiView.

Macros

- Macros output query results in abbreviated form

Reports > Report Definitions > Macro Library

Name	Total Destination Count
Description	Total Destination Count
Dataset	bandwidth app Detailed-Traffic-Statistics
Query	select count(distinct app) as total_app, count(total_endpoint, count(distinct dstip) as total
Data Binding	total_dest
Display	Counter {K/M/G}

The total number of destinations is 68 , and the average session count is 46.09 K .

- Insert macros as data into templates and reports

Generated Reports Settings Editor

Insert Chart **Insert Macro** [Icons]

Save as Template [Icons] Find Replace Replace All

The total number of destinations is [Total Destination Co...] , and the average session count is [Average Session Cou...]

Output

In FortiAnalyzer, macros provide an abbreviated output of dataset queries. You can insert macros as data in your reports without having to use a chart to display the data. FortiAnalyzer provides predefined macros, or you can create your own custom macros.

This slide shows the configuration of the predefined **Total Destination Count** macro. Use the editor to insert the macro, preceded by the plain text string `The total number of destinations is,` and followed by `, and the average session count is,` and the **Average Session Count** macro.

Macros are useful if you do not require a visual representation of the data, but you still want to have a dataset query to extract data or perform a function with the data.

Note that macros are ADOM-specific.

Configuring Macros

- **Name, Description:** Type a name and description (optional)
- **Dataset:** Pick an existing dataset
- **Query:** Displays the dataset query
- **Data Binding:** Select a field in the results of the query to bind the macro
- **Display:** Select how the macro will display the data

Reports > Report Definitions > Macro Library

Name	Total Session Count
Description	Total Number of Sessions
Dataset	bandwidth-app-Detailed-Traffic-Statistics
Query	select count(distinct app) as total_app, count(distinct appcat) as total_appcat, count(distinct user_src) as total_users, count(distinct
Data Binding	total_sessions
Display	Counter (K/M/G)

This slide shows the configuration parameters for macros.

- Define a name and an optional description.
- Pick an existing dataset, which then populates the **Query** box.
- Pick which column in the query is going to be used for the macro. In the example on this slide, the macro will use data from the **total_sessions** column.
- Select the display, which affects how the macro will display the data. The options are:
 - **Bandwidth:** FortiAnalyzer adds KB, MB, or GB to the end of the macro, shortening large numbers and appending the units.
 - **Counter:** FortiAnalyzer adds K, M, or G to the end of the macro, shortening large numbers and appending the units: K (kilo, one thousand), M (mega, one million), and G (giga, one billion).
 - **Duration:** FortiAnalyzer adds a colon before the last two digits.
 - **Percentage:** FortiAnalyzer adds a percentage sign to the end of the macro.
 - **Text:** FortiAnalyzer doesn't add unit measurements.

The display configuration must match the data binding configuration. For example, if the data binding outputs time, the display should be in duration. If the output is bandwidth, then the bandwidth setting is correct. Otherwise, you may see strange results. For example, if you select percentage, but the data binding is for an IP address, you may see 10.0.0.1%.

Chart Types



When you configure a chart, you can define the chart type. This slide shows the available options. Depending on the chart type you select, you can further customize them. For example, you can sort data in the table type, or change the axis of the bar type.

Choosing the right chart type for your report is essential. For example, using a bubble chart to present information on total destination (by bandwidth usage) may not be as useful as actually showing the amount of traffic using a table.

In general, circular charts such as the pie, donut, and radar charts are hard to read when there is too much data to include. In this case, the bar or table charts may be more appropriate.

A bar chart may also be a poor option if one data result has a much higher number than other results, meaning that the chart displays one long bar while the other bars are so small that you cannot easily differentiate them.

Templates

- A template specifies the layout—text, charts, and macros—to include in the report that uses it
- FortiAnalyzer provides predefined templates (which match the predefined reports)
 - Can clone predefined templates or create custom templates
 - Can't edit or delete predefined templates

Reports > Report Definitions > Templates			
All Reports	Templates	Chart Library	Macro Library
+ Create New Edit Delete More ▾			
☐	Title ▴		
☐	Template - 360 Protection Report		
☐	Template - 360 Security Report		
☐	Template - 360-Degree Security Review		

Reports > Report Definitions > All Reports			
All Reports	Templates	Chart Library	Macro Library
Run Report Report ▾ Folder ▾ More ▾			
☐	Title ▴		
☐	360 Protection Report		
☐	360 Security Report		
☐	360-Degree Security Review		

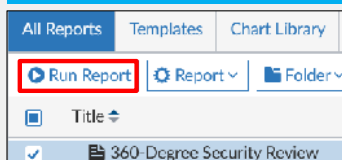
FortiAnalyzer provides predefined templates for reports. A template specifies the layout—text, charts, and macros—to include in the report that uses it. By default, these predefined templates are associated with their respective predefined reports. For example, the predefined **360-degree Security Review** report uses the **360-Degree Security Review** template.

Templates don't contain any data. FortiAnalyzer adds data to the report when you generate it.

You can't edit a predefined template, but you can clone it and edit the clone to fit your requirements. You can also create your own template from scratch.

Running Predefined Reports

Reports > Report Definitions > All Reports



- Run reports with default settings

- Optionally, edit settings:
 - Time period
 - Devices
 - Filters
 - Report schedule (on demand or scheduled)

FORTINET
Training Institute

© Fortinet Inc. All Rights Reserved. 35

FortiAnalyzer also provides predefined reports—each one associated with a predefined template (the layout). Predefined reports come with basic, default settings already configured. These basic settings define the time period in which to run the report; which devices to run the report on; and whether FortiAnalyzer generates a single report or separate reports per device or VDOM.

You can run the predefined reports *as is*, but, at a minimum, you should examine and adjust, if necessary, the basic default settings. You can right-click any predefined report and select **Edit** to change its settings. For example, if today is the first day FortiAnalyzer has been collecting logs, your report contains no data if the time period is set to **Previous 7 Days**. Previous <n> days is handled differently in FortiView than in reports. In reports, the current day is *not* included. You can specify a custom time period instead, or use a previous <n> minutes or previous <n> hours setting.

You can run reports on demand, or schedule them for a specific time by enabling scheduling.

After a report is generated, you can view a report in multiple formats, including HTML, PDF, XML, CSV, and JSON.

Running Predefined Reports (Contd)

- You can filter which logs to include in a report

Reports > Report Definitions > All Reports > Settings

Filters ▾

Log messages that match ☒ All ☐ Any of the Following Conditions

Log Field	Match Criteria	Value ⓘ	Action
Severity (severity) ▾	Equal To ▾	critical	✕ +
& Destination Interface (dstintf) ▾	Equal To ▾	port3	✕ +

Note: You can also configure filters on the charts a report uses

- Advanced Settings** allows you to change the report's appearance

Advanced Settings ▾

Language	English
Bundle Rest into "Others"	Auto
Print Orientation	☒ Portrait ☐ Landscape
Chart Heading Level	Heading 2
Default Font	Open Sans
Hide # Column	☒
Layout Header	☒
Header Text	
Header Image	Select Image fortinet_gray.png
Layout Footer	☒ ☒ Default ☐ Custom
Print Cover Page	☒
Print Table of Contents	☒
Print Device List	☒ Compact
Display Device Name	By Device Name
Print Report Filters	☒
Obfuscate User	☐
Resolve Hostname	☐
Date Format	Default
Allow save maximum	99
Color Code	Purple
Report Owner	Click to select

If a predefined report comes extremely close to meeting all of your requirements, you may be able to fine-tune its settings to fit your needs.

Fine-tuning encompasses minimal modifications, such as:

- Adding log message filters to further refine the log data that is included in the report
- Enabling queries to a pre-existing LDAP server to add an LDAP query to the report
- Configuring report language, print settings, and other settings. For example, you can print and customize the cover page, print the table of contents, print a device list, obfuscate users, and set the color code for the report to appear under **Report Calendar**.

DO NOT REPRINT
© FORTINET

Knowledge Check

1. What is the main difference between charts and macros?
 - A. Only charts use datasets.
 - ✓ B. Macros output query results in abbreviated form.

DO NOT REPRINT
© FORTINET

Lesson Overview



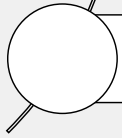
Report Introduction



SQL Queries



Report Configuration



Report Customization

Good job! You now understand how to configure the different components of FortiAnalyzer reports.

Now, you will learn about report customization options.

DO NOT REPRINT
© FORTINET

Report Customization

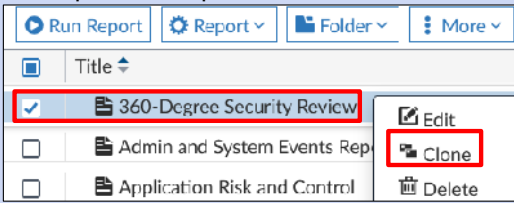
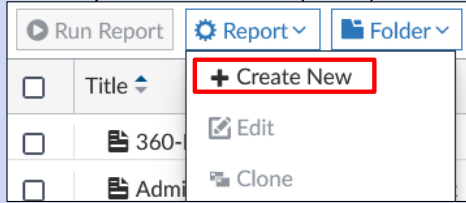
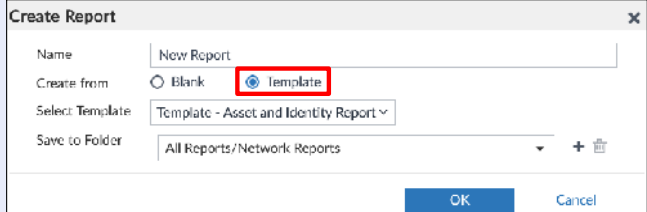
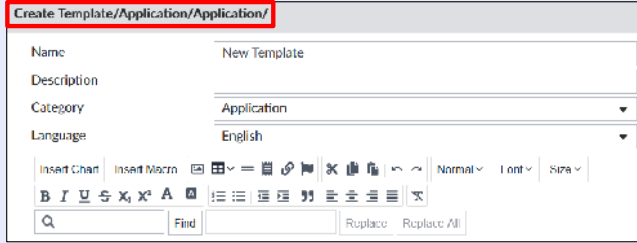
Objectives

- Describe report customization options
- Configure and generate custom reports

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

By demonstrating competence in customizing your reports, you can tailor them to your specific needs.

Customization—Template vs. Report

Minor/Moderate Customizations	Major Customizations
Clone a report or template, then edit the clone 	Create a new report from scratch (blank) 
Create a new report from an existing template, then edit 	Create a new template (to use in a report) 

FORTINET
Training Institute

© Fortinet Inc. All Rights Reserved. 40

Predefined reports may not meet all of your organization's requirements, even after you fine-tune the report settings. FortiAnalyzer allows you to create new templates and reports from scratch, or customize existing templates and reports.

To make small changes to existing templates or reports, you can clone a report or template and then edit the clone to suit your requirements.

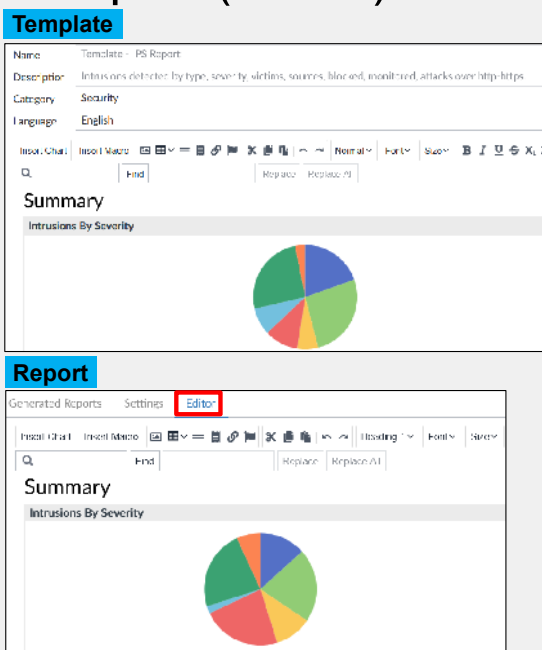
You can create a new report based on an existing template. Then, you can edit that new report to suit your requirements.

While you can edit the layout of predefined reports (but not templates) directly, it is a best practice to clone and edit predefined reports instead. This preserves the default reports if your edits to the report are not successful.

To make major changes to existing templates or reports (if no report comes close to meeting your needs), you can create a new report or template from scratch.

Customization—Template vs. Report (Contd)

- Which customization approach to take: template or report?
- Most important difference: templates only include the layout of the report, but not report settings (basic or advanced)
- Best practice is to approach it from an efficiency and needs standpoint
- Think about:
 - The amount of customization you need
 - Whether you want to preserve report settings
 - Whether you want to use the layout for one report or many reports



Templates and reports are closely related. As discussed earlier, you can clone and edit both reports and templates, and you can create both new reports and new templates. So, how do you decide whether to customize a template or a report?

One of the most vital differences between templates and reports is that templates include only the details you can find under the **Editor** tab of the report—they don't include report settings (neither the basic configuration nor advanced settings). So, when deciding whether to perform customizations on a template or a report, consider what you want to preserve and what you want to modify.

In the end, there is no *correct* approach. You can achieve the same results through multiple methods. A best practice is to approach the decision from an efficiency and needs standpoint.

Report Customization Settings

Reports > Report Definitions > Settings > Advanced Settings

Advanced Settings	
Language	English
Bundle Rest into "Others"	Auto
Print Orientation	☐ Portrait ☒ Landscape
Chart Heading Level	Heading 2
Default Font	Open Sans
Hide # Column	☐
Layout Header	☐
Layout Footer	☐
Print Cover Page	☐
Print Table of Contents	☐
Print Device List	☐
Display Device Name	By Device Name
Print Report Filters	☒
Obfuscate User	☐
Resolve Hostname	☐
Date Format	Default
Allow save maximum	99
Color Code	Bold Blue
Report Owner	Click to select
Enable Report Filter Caching	☒
Enable High Accuracy Caching	☐

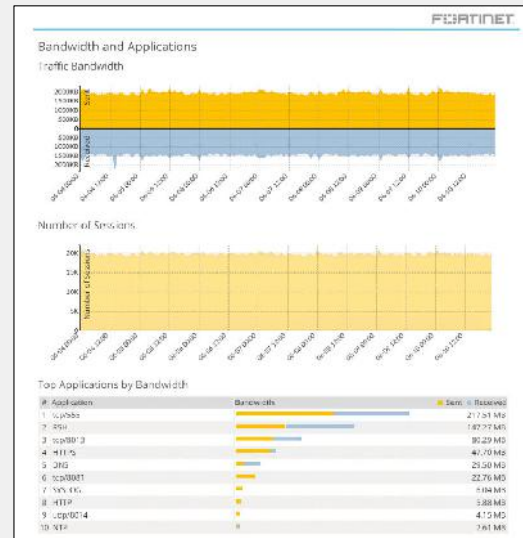
FortiAnalyzer provides many customization options for your reports. Under **Advanced Settings**, you can customize the selected report.

Many of the options are cosmetic, such as adding a header, a footer, a cover page, or changing the font. However, other settings are related to the function of the report, including:

- **Bundle Rest into "Others"**: Bundle the uncategorized results into an Others category.
- **Print (different elements)**: Include a cover page, a table of contents, and a list of included devices.
- **Obfuscate User**: Hide user information in the report. You may not want the users' identity to be included in the report.
- **Resolve Hostname**: FortiAnalyzer will try to resolve hostnames at the report level.
- **Enable Report Filter Caching**: Accelerate processing speed when generating multiple reports. In this case, all filters are applied when querying the hcache table, which may decrease the accuracy of the report.
- **Enable High Accuracy Caching**: Increase the maximum hcache rows, increasing data accuracy. Clear the checkbox to improve system performance. In this case, the filters are put inside the hcache to increase data accuracy.

Report Customization Settings (Contd)

Reports > Generated Reports



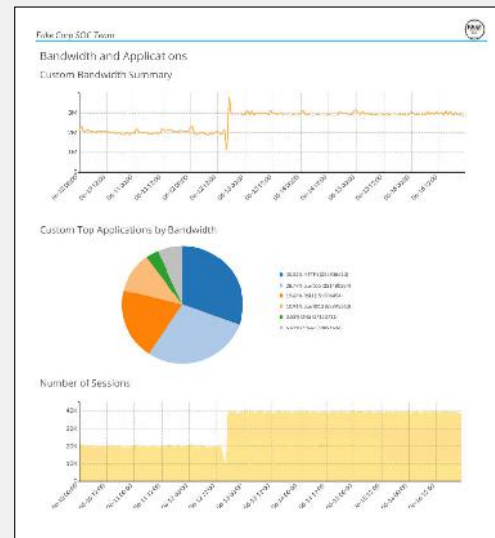
This slide shows two pages from the predefined **Security Analysis** report.

In the image on the left side of the slide, you can see a default cover page. On the right, you can see the preconfigured charts.

Note that the full report contains many more pages not depicted on this slide.

Report Customization Settings (Contd)

Reports > Generated Reports



This slide shows two pages from a customized **Security Analysis** report.

The cover page is different from the predefined report cover on the previous slide, and the chart types are different.

Note that the full report contains many more pages not depicted on this slide.

DO NOT REPRINT
© FORTINET

Knowledge Check

1. Which element do templates not contain?
 - ✓ A. Report settings
 - B. Report layout

2. Which setting protects the privacy of users?
 - ✓ A. **Obfuscate User**
 - B. **Resolve Hostname**

DO NOT REPRINT
© FORTINET

Lesson Overview



Report Introduction



SQL Queries



Report Configuration



Report Customization



Congratulations! You have completed this lesson.

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

DO NOT REPRINT
© FORTINET

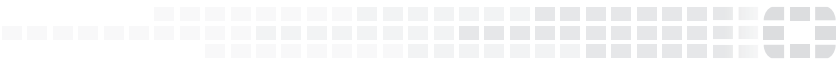
Review

- ✓ Describe the considerations of SOC reporting
- ✓ Review the basic components of a FortiAnalyzer report
- ✓ Describe SQL basics
- ✓ Describe FortiAnalyzer schemas
- ✓ Use FortiAnalyzer tools for simplifying SQL queries
- ✓ Configure datasets, charts, and macros
- ✓ Describe report customization options
- ✓ Configure and generate custom reports

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

By mastering these objectives, you gained an understanding of the basics of reporting in FortiAnalyzer and how SQL queries are utilized in the reporting process. Additionally, you learned how to configure the elements of a report, including datasets, charts, and macros. Finally, you discovered how to customize a report to suit specific needs.

DO NOT REPRINT
© FORTINET



No part of this publication may be reproduced in any form or by any means or used to make any derivative such as translation, transformation, or adaptation without permission from Fortinet Inc., as stipulated by the United States Copyright Act of 1976.

Copyright© 2024 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.