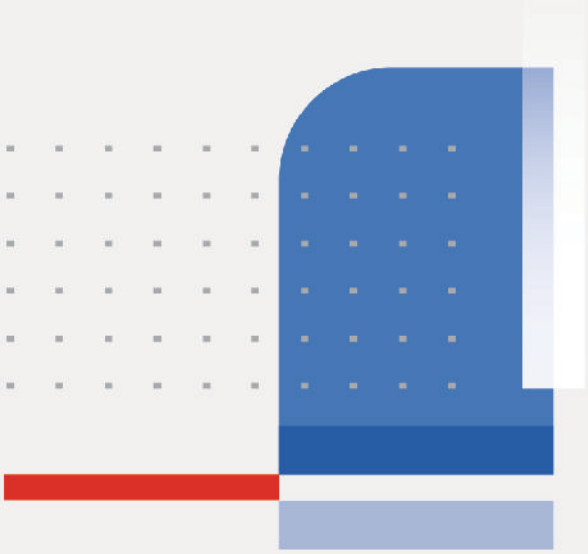
FORTINET CERTIFIED PROFESSIONAL Security Operations

FortiAnalyzer Analyst Study Guide

FortiAnalyzer 7.6



FORTINET Training Institute

Fortinet Training Institute - Library

https://training.fortinet.com

Fortinet Product Documentation

https://docs.fortinet.com

Fortinet Knowledge Base

https://community.fortinet.com/t5/Knowledge-Base/ct-p/knowledgebase

Fortinet Fuse User Community

https://community.fortinet.com/

Fortinet Forums

https://community.fortinet.com/t5/Support-Forum/bd-p/fortinet-discussion

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

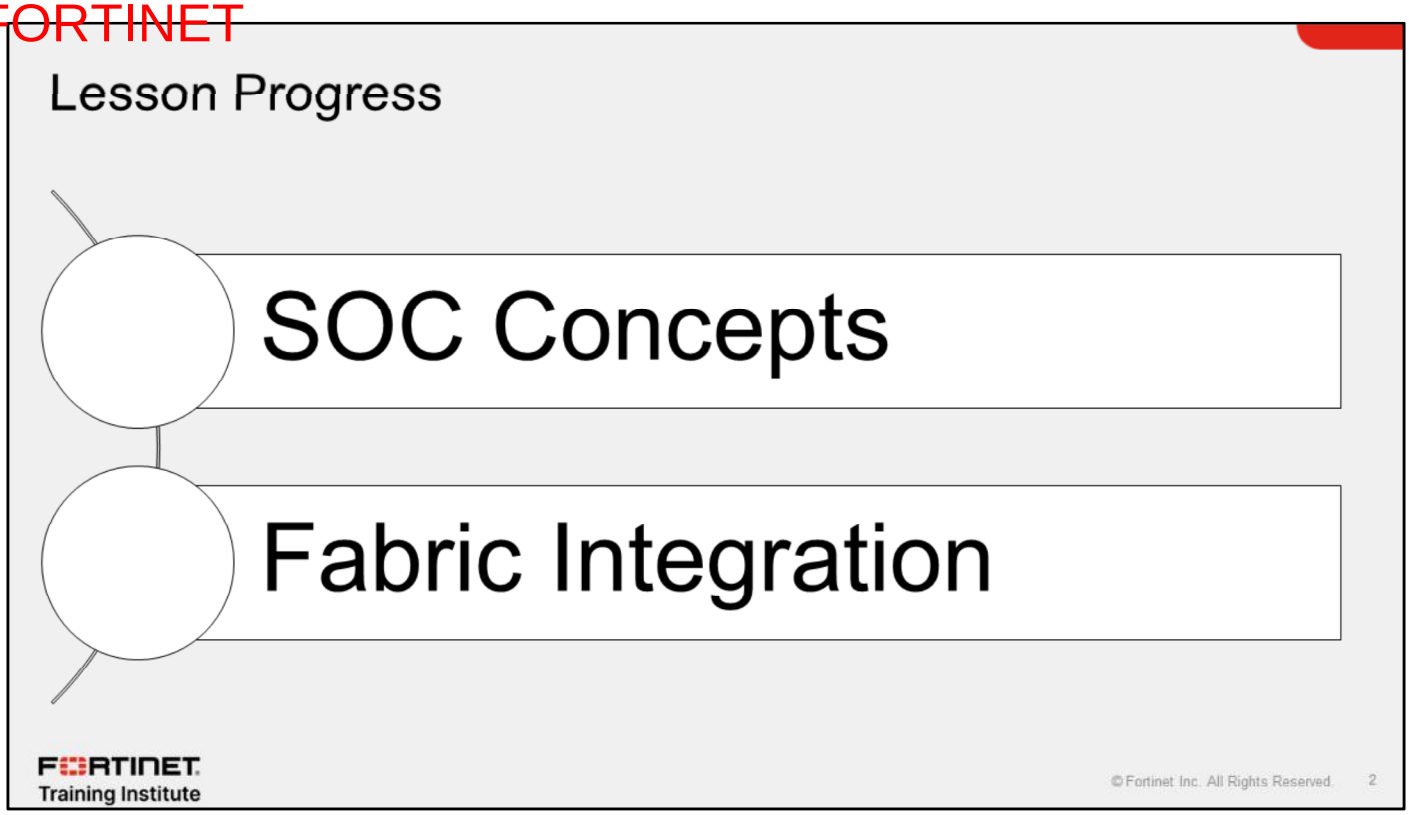
Fortinet Training Institute Helpdesk (training questions, comments, feedback)

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

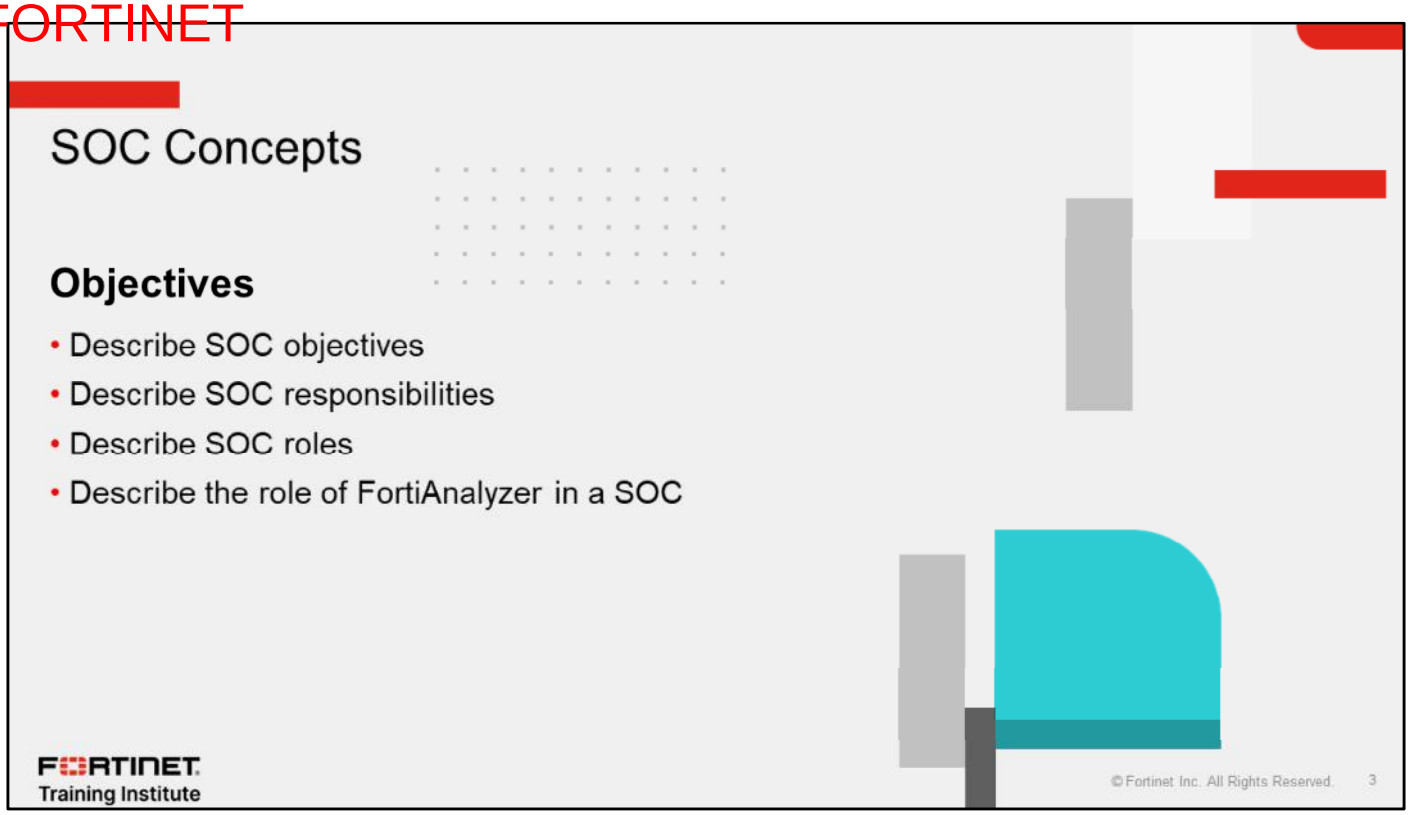
TABLE OF CONTENTS

01 SOC Concepts and Security Fabric 4
02 Log Data Flow and Navigation 32
03 Events, Indicators, and Incidents 72
04 FortiAI, Threat Hunting, and Troubleshooting 111
05 Reports 152
06 Playbooks 193
Supplementary - FortiOS Logging 223

In this lesson, you will learn about the key features and concepts of a SOC, and the role that FortiAnalyzer plays in it. You will also learn how to initially access FortiAnalyzer.

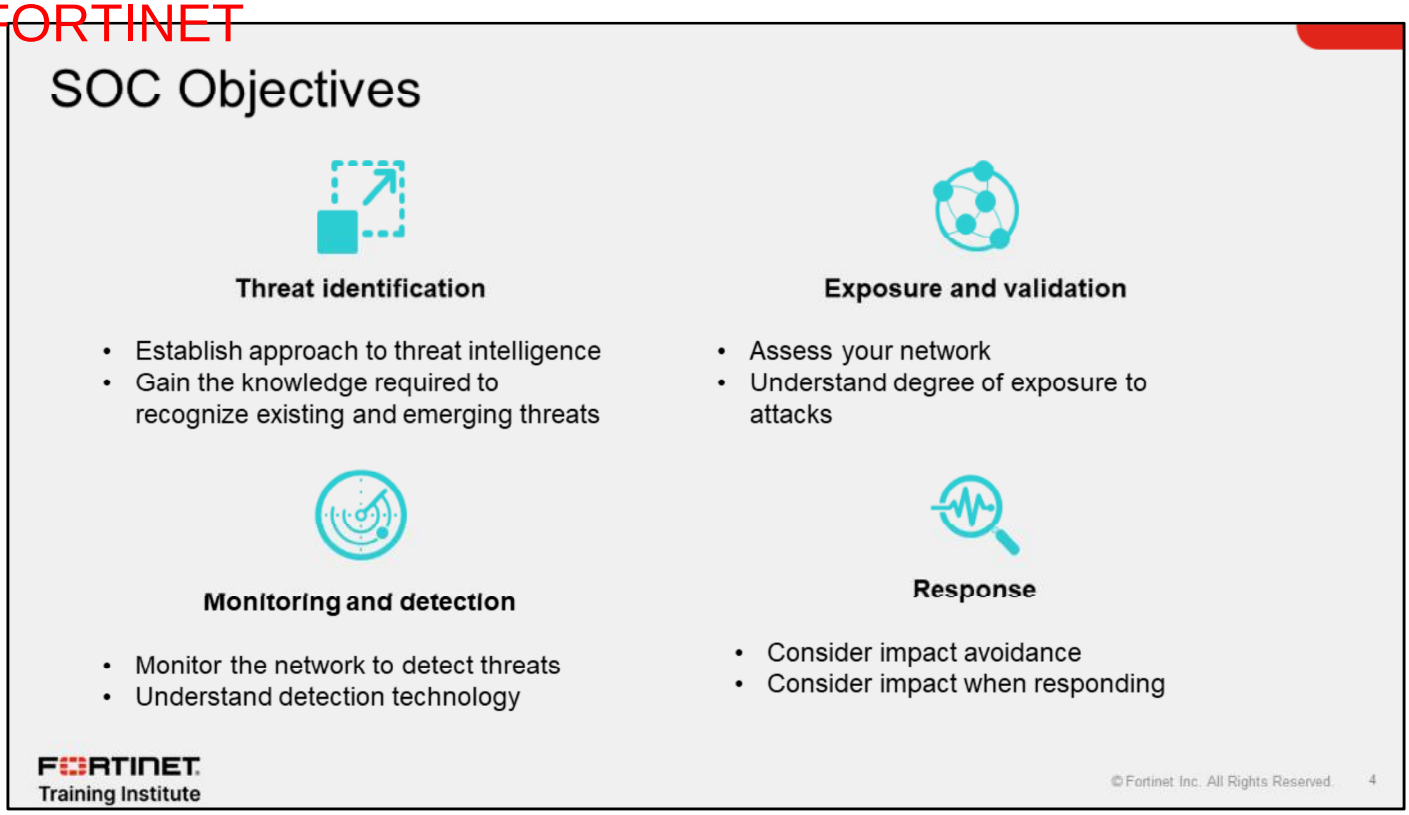


In this lesson, you will explore the topics shown on this slide.



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

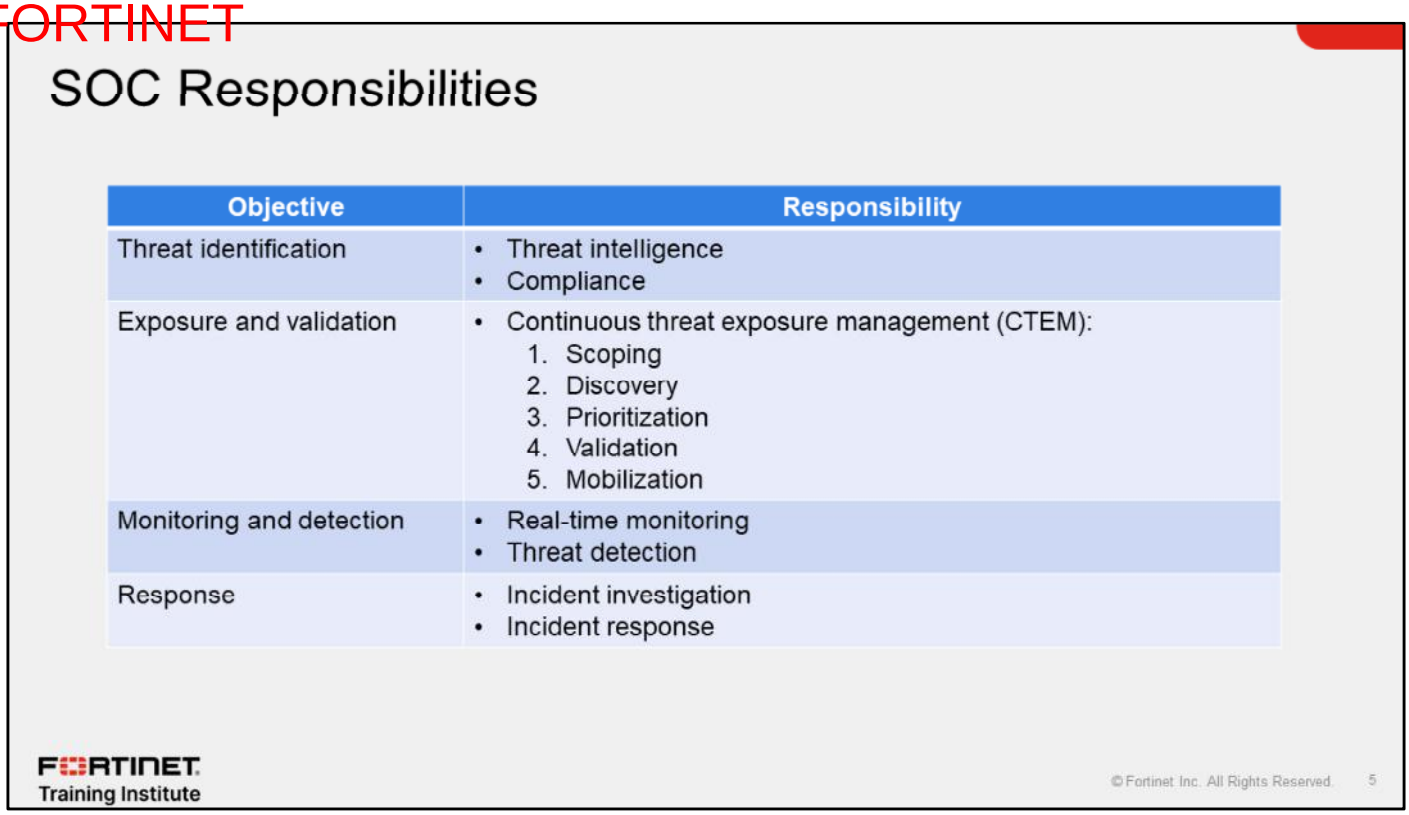
By demonstrating competence in SOC features and concepts, you will be able to better understand the FortiAnalyzer features in your network.



The SOC is a team that is dedicated to security operations. They are responsible for real-time security monitoring across the organization's IT infrastructure, including applications, networks, devices, and cloud environments.

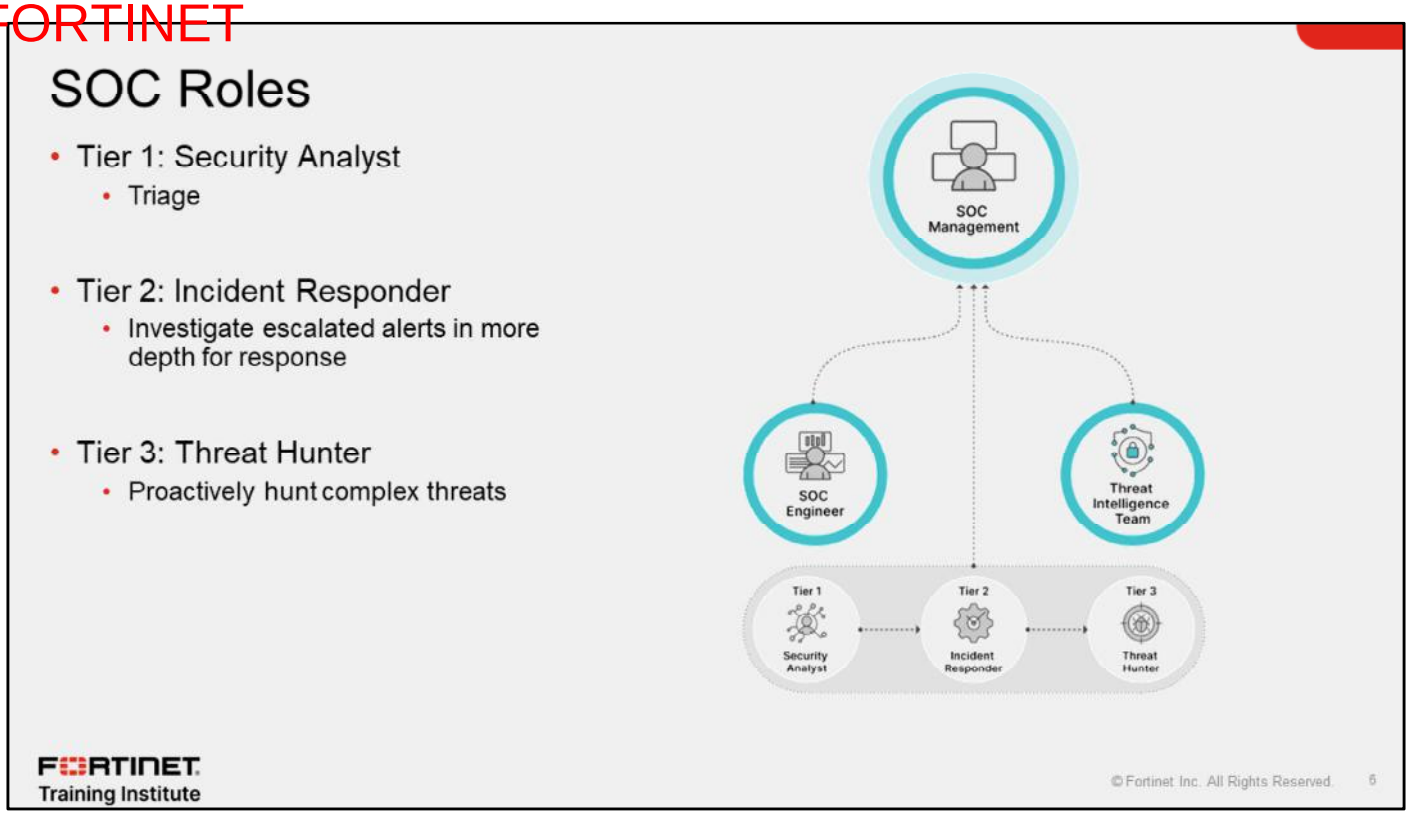
The SOC has four key objectives:

- Threat identification: This includes establishing an approach to threat intelligence, so the SOC has the knowledge required to recognize existing and emerging threats.
- Exposure and validation: This involves assessing your network to understand its degree of exposure to attacks. Continuously assessing the network's exposure is important for effective monitoring and detection.
- Monitoring and detection: The SOC monitors the network to detect threats. The SOC must understand where to place detection technology and the threats they are looking for to align objectives with the organization's needs and compliance requirements.
- Response: This should be considered in terms of impact avoidance; when the attack has already occurred and been detected, the SOC must consider the impact when responding.



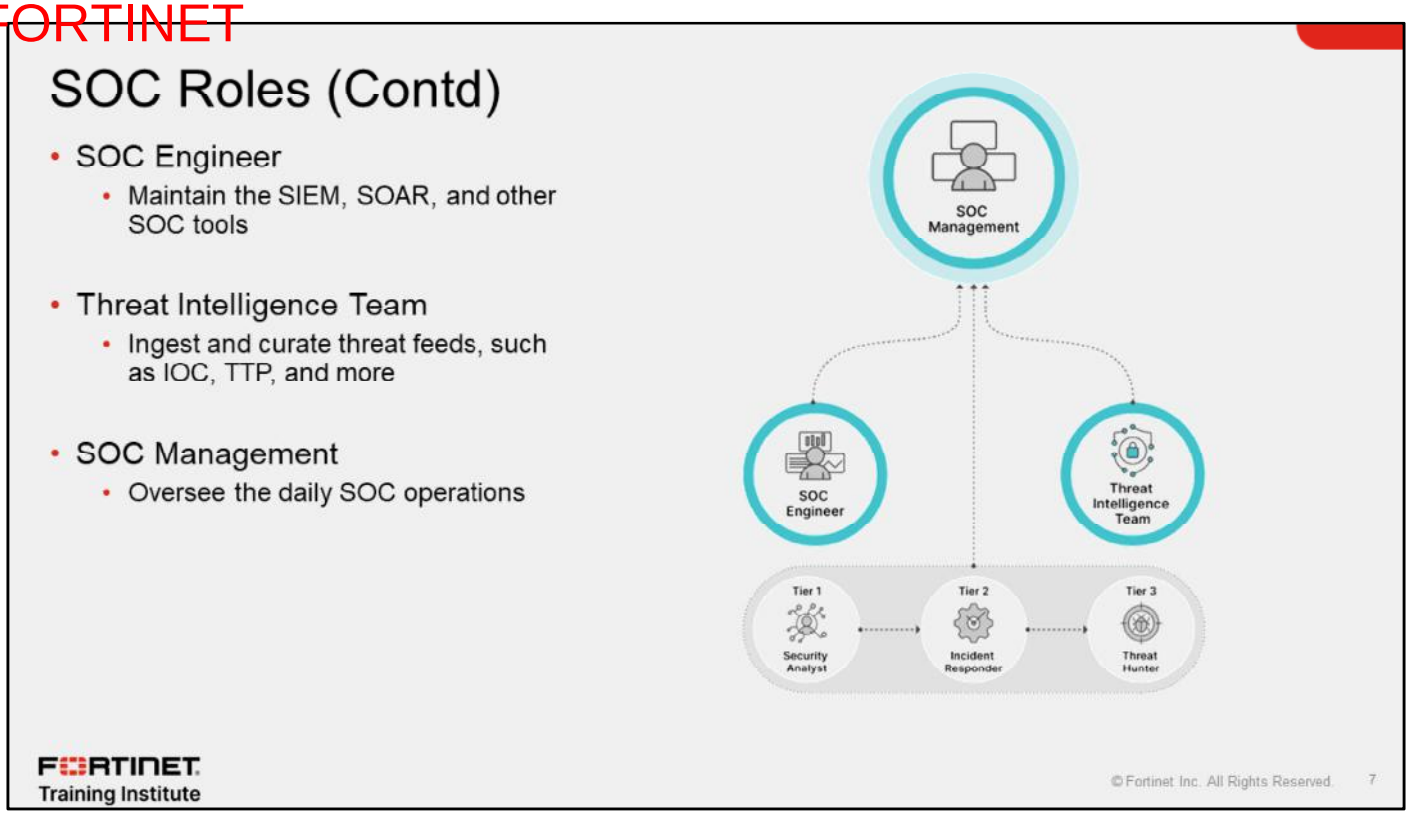
The SOC objectives can be further broken down into responsibilities for security operations:

- Threat intelligence: The SOC should stay updated on the latest cyberthreats to refine detection strategies and enhance defensive capabilities. Threats are constantly evolving, so it is important for a SOC to leverage support from other resources when possible.
- Compliance: The SOC must adhere to regulatory standards for its industry and geographical location while maintaining records of threats and incident responses.
- CTEM: This methodology for scoping, prioritizing, and validating threat exposure in the network allows the SOC to plan how to best mobilize its people and processes for security operations.
- Real-time monitoring: The SOC requires access to a lot of information to monitor network activity. This is accomplished using a data lake that stores information, including logs from all devices in the Security Fabric for threat detection. Dashboards, reports, and integrated security information and event management (SIEM) features monitor the network for threats and incidents.
- Threat detection: When monitoring the network, the SOC is also responsible for detecting active and potential threats. Tools such as SIEM and extended detection and response (XDR) systems can help gather and analyze telemetry data to identify potential threats. In addition, SIEM tools and third-party services are used to quickly identify incidents and emerging outbreaks in the network.
- Incident investigation: After they identify threats, the SOC is responsible for investigating these incidents further to ensure the attack does not lead to any further risks or compromise. Implementing measures such as isolating compromised systems during investigation can neutralize the threat and minimize damage from a security incident. Incident reporting is critical to ensuring the investigation is complete, tracking all the potentially affected systems and devices.
- Incident response: As part of incident investigation, the SOC also responds to threats by blocking IP addresses, domains, or URLs and coordinating recovery efforts for affected devices.



A SOC can include multiple roles that are responsible for maintaining an organization's security posture. Some roles can be organized in a tiered structure to monitor and respond to threats, while other roles are responsible for maintaining tools, processes, and strategic direction. When working with large organizations and SOCs, having multiple roles can help handle the volume or complexity of security operations.

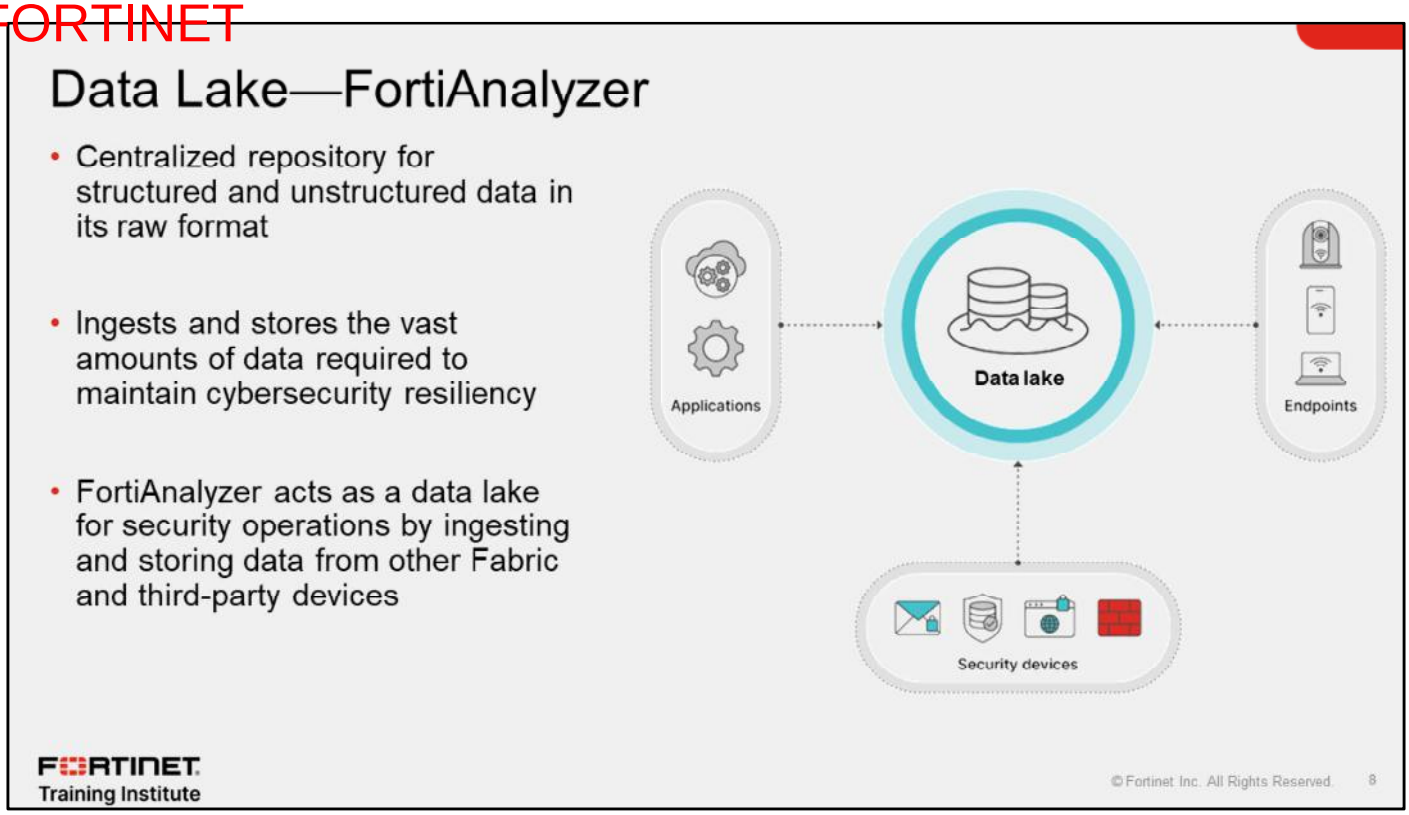
Tiered analysts are the core operational roles in the SOC for continuous monitoring and incident response. Regardless of the size of the organization and the SOC, a tiered structure can help manage threats to the network. This structure allows certain members to focus on monitoring and initial triage (tier 1) while others focus on escalated incident response for larger attacks where remediation may take more time (tier 2). In larger SOCs, a third tier is beneficial to proactively hunt larger threats by monitoring threat intelligence and testing the security posture of the network.



The SOC engineers are responsible for maintaining the security, orchestration, automation, and response (SOAR), SIEM, and other SOC tools and for ensuring tool uptime and performance. As part of this maintenance, they will design and plan to scale for the organization's future growth, ensuring the SOC can handle increased volume and more complex threats.

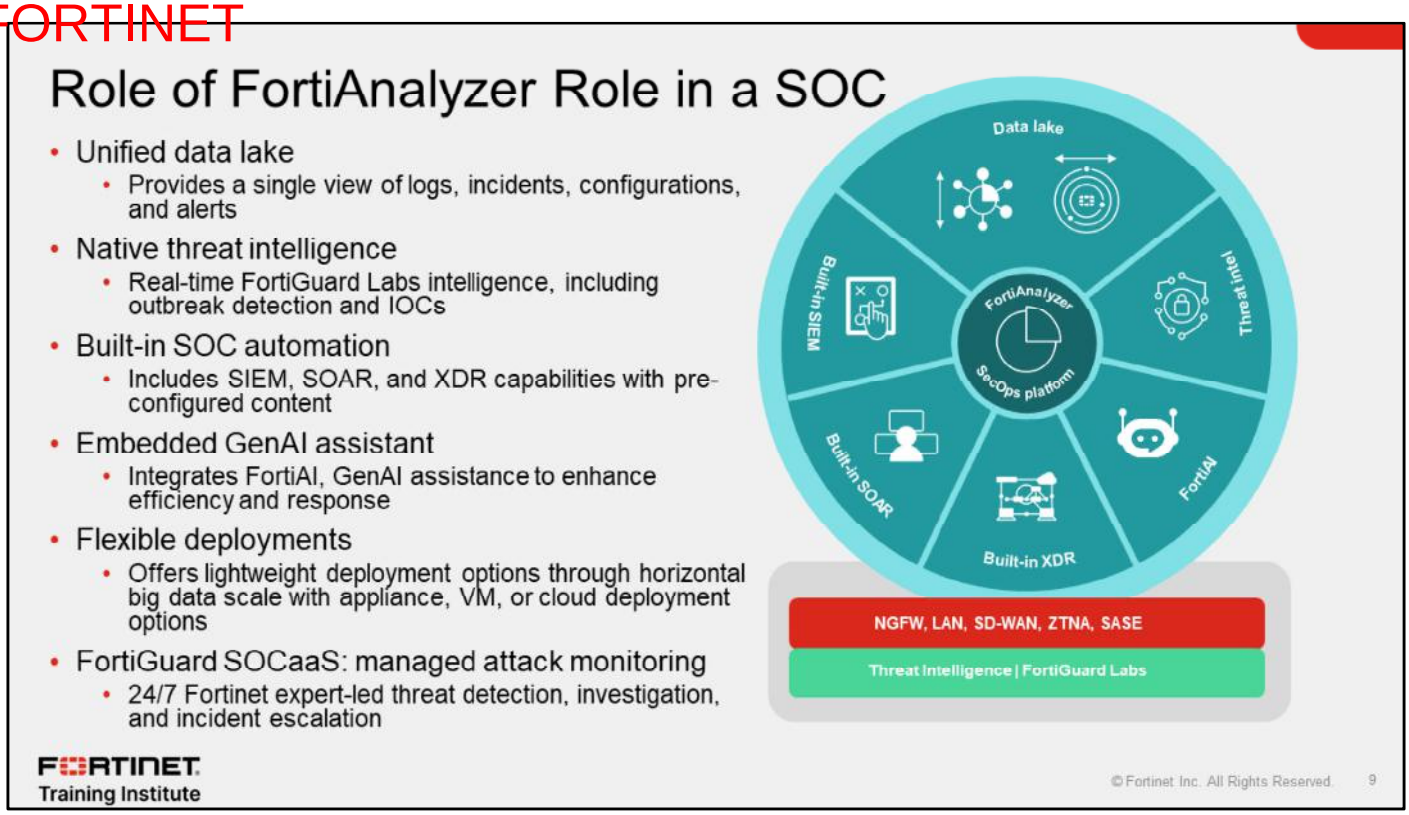
The threat intelligence team ingests and curates threat feeds, such as indicators of compromise (IOCs), tactics, techniques, and procedures (TTP), and more. They may also work with external intelligence sources, including Information Sharing and Analysis Centers (ISACs) and other vendors, to gain further insights and threat data. The team can also map threat intelligence to the MITRE ATT&CK framework, providing context to investigations and threat hunting.

SOC managers are responsible for overseeing the daily SOC operations. They can manage team schedules, develop and implement policies, and handle resource allocation. In larger SOCs, SOC team leads may be required to oversee the daily operations while managers focus on compliance, metrics, and other strategic duties to ensure a smoothly running SOC. SOC managers can also be responsible for communication and coordination with other relevant business units, such as IT.



In security operations, a data lake is used to ingest and store the vast amounts of data required to maintain cybersecurity resiliency. A data lake is a centralized repository where data is stored in structured and unstructured data in its raw format. This data can come from many different sources, and it is not siloed in the data lake. Instead, the data lake can be used as a single repository to investigate and correlate the data. This makes the data lake foundational to security operations and the responsibilities of the SOC, including real-time monitoring, threat detection, and incident investigation.

Fortinet's data lake offering is FortiAnalyzer. FortiAnalyzer acts as a data lake for security operations by ingesting and storing data from other Fortinet and third-party devices. Logs from third-party devices can be normalized for analysis and correlation using a suite of predefined log parsers, some of which are built-in with FortiAnalyzer and other premium log parsers that are available through FortiGuard licenses. Additionally, SIEM and SOAR functions are integrated in FortiAnalyzer, allowing the SOC to manage security operations efficiently.

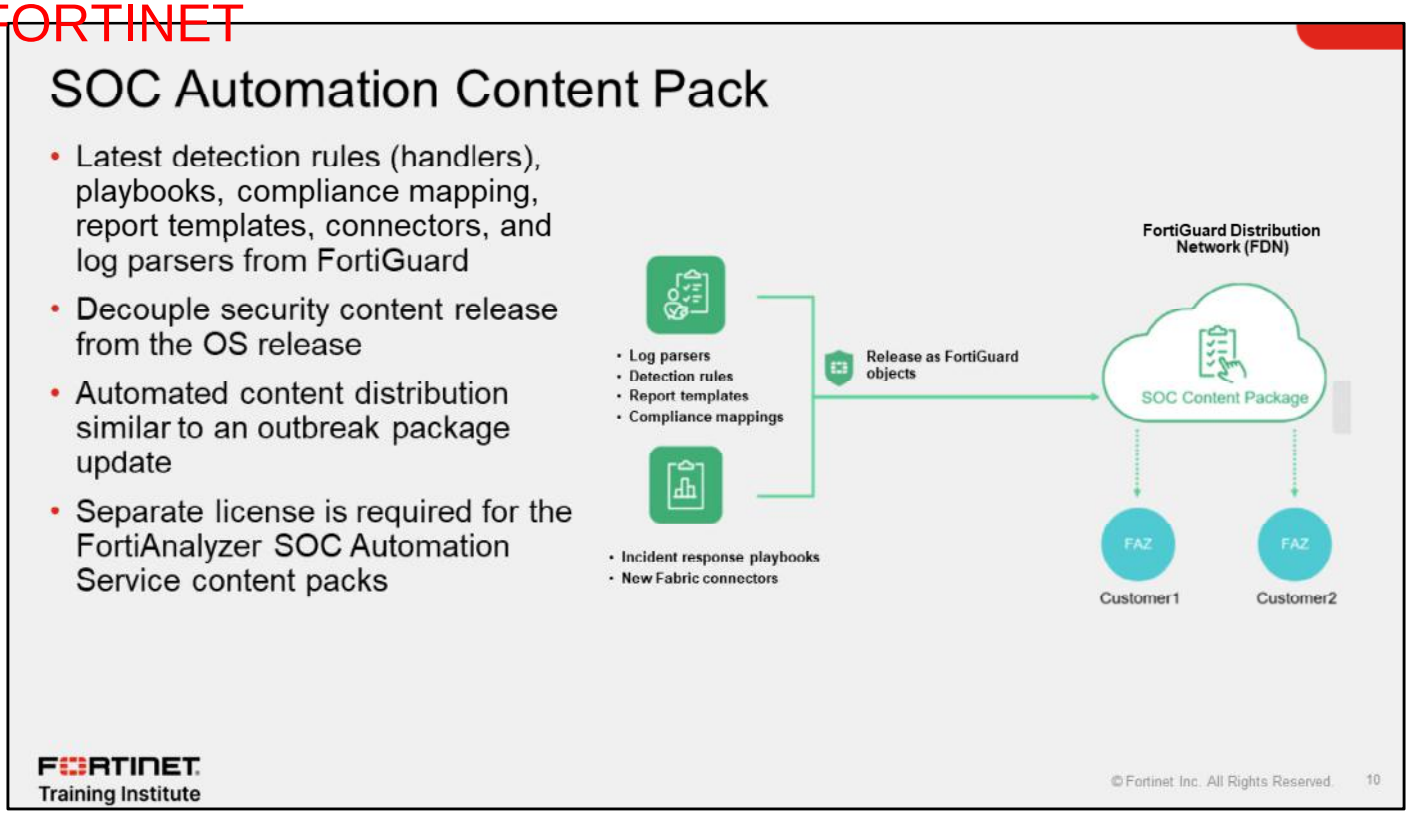


Over the past few years, FortiAnalyzer has been significantly enhanced, evolving from a logging and analytics tool into a comprehensive, modern security operations (SecOps) platform.

As the Fortinet Security Fabric data lake, FortiAnalyzer consolidates vast datasets and streamlines the management of logs, incidents, and reporting by unifying configurations, events, and alerts from across the Fortinet Security Fabric into a single view. With intuitive threat topologies and native intelligence from FortiGuard Labs, customers receive timely updates on the latest threats.

The Security Automation subscription further boosts SIEM/SOAR capabilities by providing prebuilt content packs that include event handlers, playbooks, and connectors that are updated monthly. The integration of FortiAI provides generative AI (GenAI) assistance embedded in FortiAnalyzer, enabling teams to respond quickly and effectively.

FortiAnalyzer also offers lightweight and flexible deployment options—whether as a physical appliance, a VM, or in the cloud—allowing organizations of all sizes to detect threats more intelligently, respond more swiftly, and scale horizontally using the FortiAnalyzer Fabric architecture.



The FortiAnalyzer SOC Automation Service, integrated with native SIEM and SOAR capabilities on the platform, offers a comprehensive suite of features, including third-party log parsers, advanced correlation rules, automation connectors, incident response playbooks, advanced analytics, and premium reports.

These tools empower SecOps teams to swiftly detect, investigate, and respond to security incidents.

You need a separate license for the FortiAnalyzer SOC Automation Service content packs.

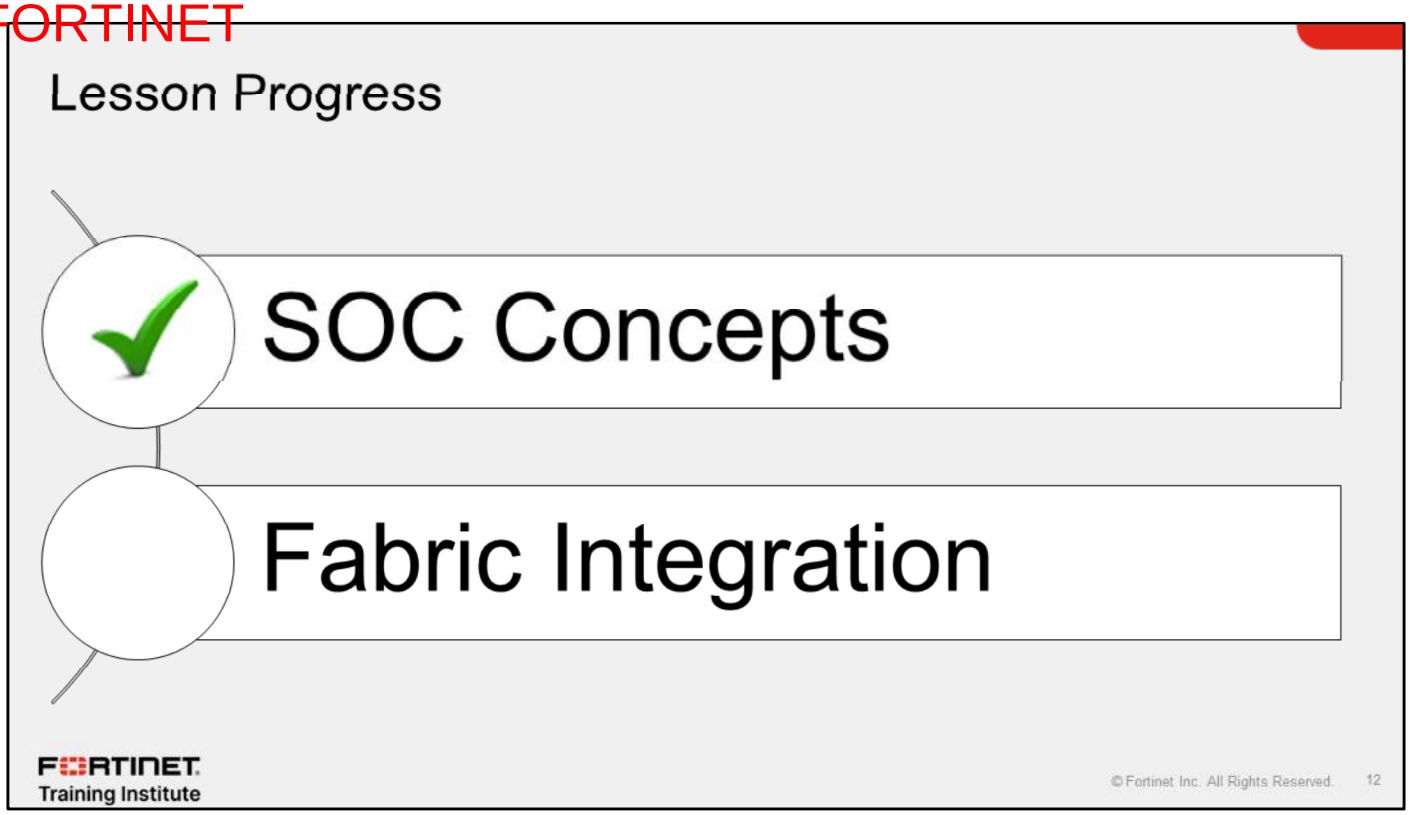
Knowledge Check

1. Which SOC team is responsible for ingesting and curating threat feeds such as IOCs?
   - A. Threat Hunter
   - ✓B. Threat Intelligence team

2. What is the role of FortiAnalyzer in a SOC?
   - A. Perform security orchestration, automation, and response
   - ✓B. Ingest and store all network data

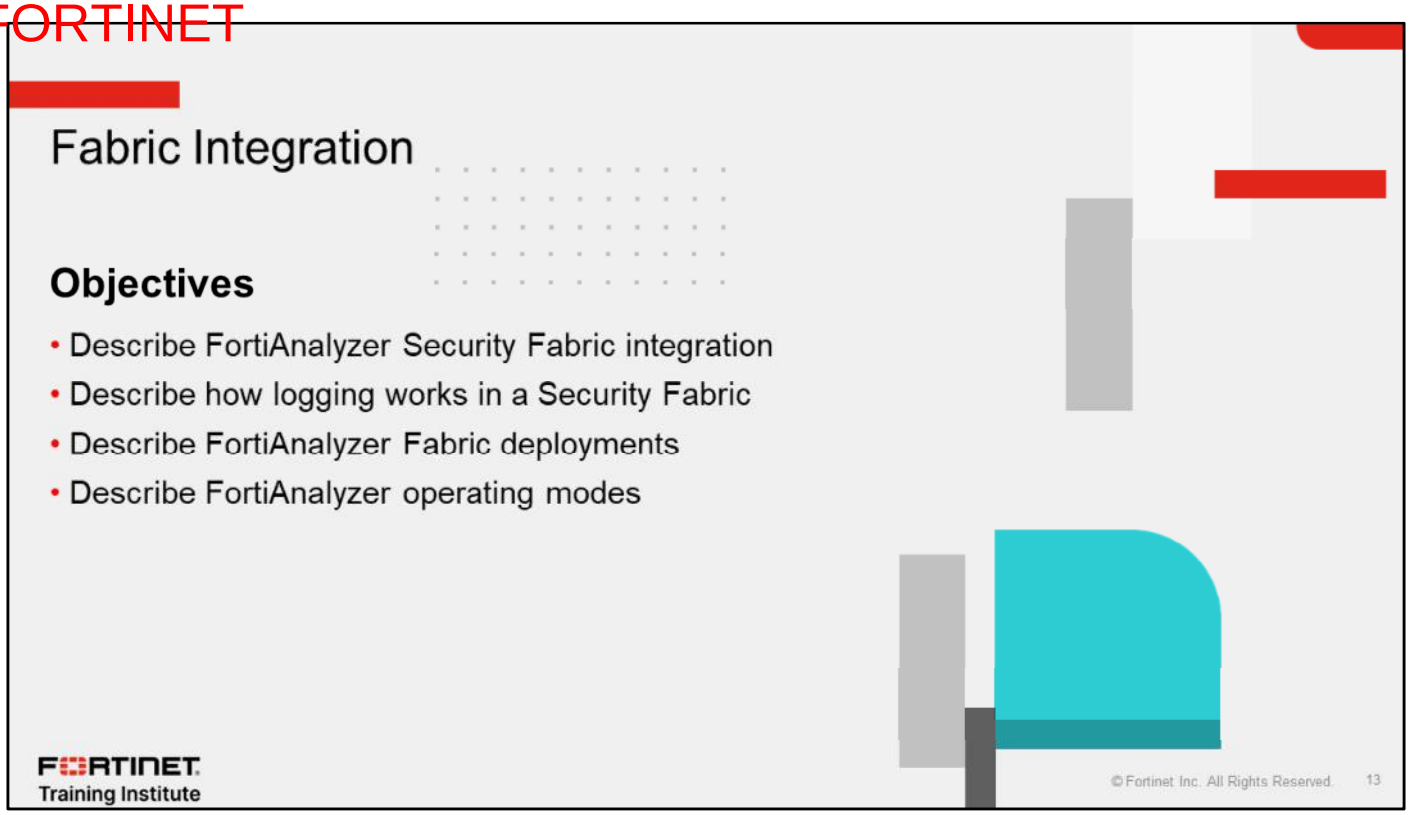
FORTINET Training Institute

 11



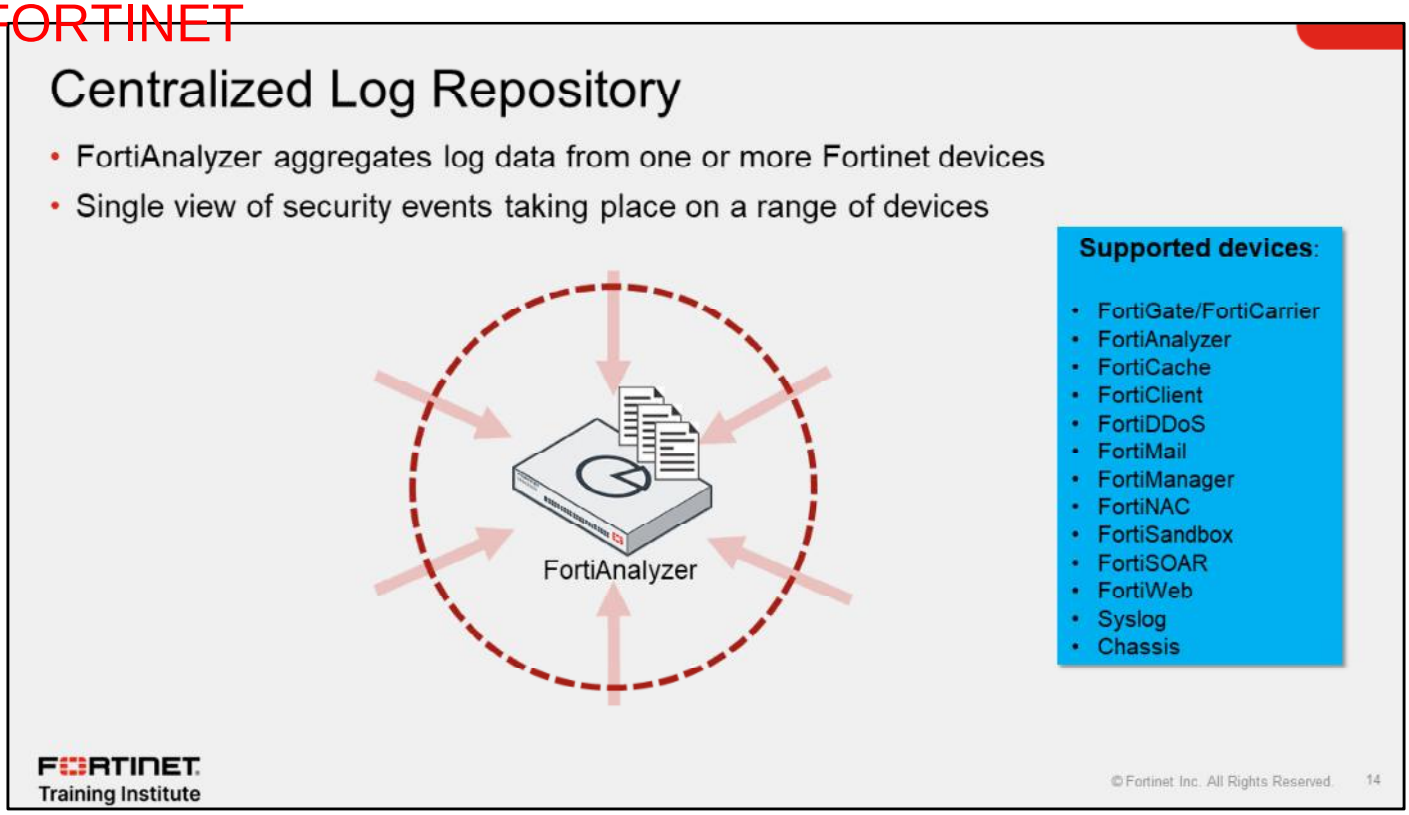
Good job! You now understand the SOC concepts.

Now, you will learn about FortiAnalyzer integration in the Security Fabric and FortiAnalyzer Fabric deployments.



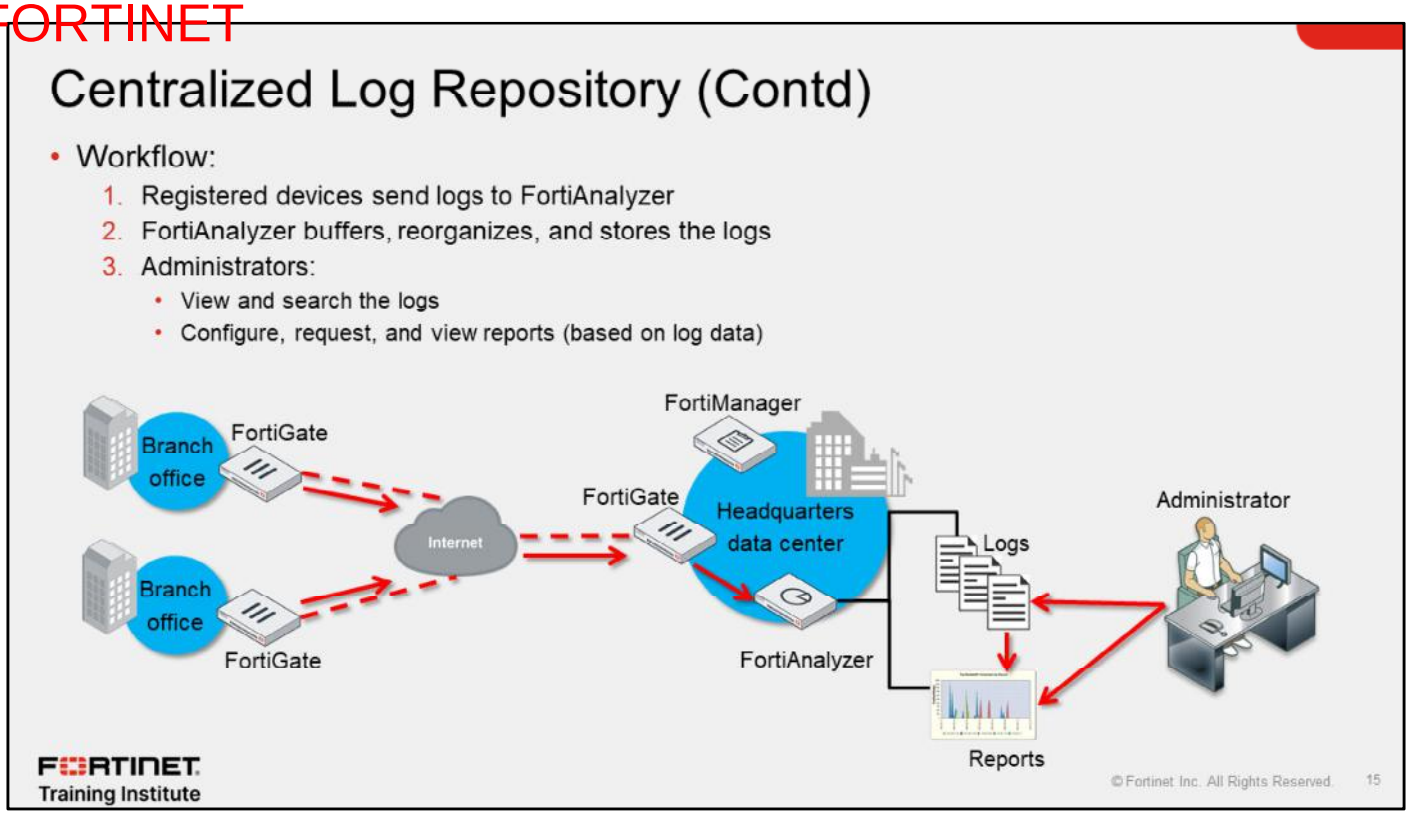
After completing this section, you should be able to achieve the objectives shown on this slide.

By demonstrating competence in Security Fabric integration, you will be able to explain how FortiAnalyzer integrates into and collects and correlates logs in a Security Fabric. You will also be able to describe how FortiAnalyzer Fabric deployments work and differentiate between the FortiAnalyzer operating modes.



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.

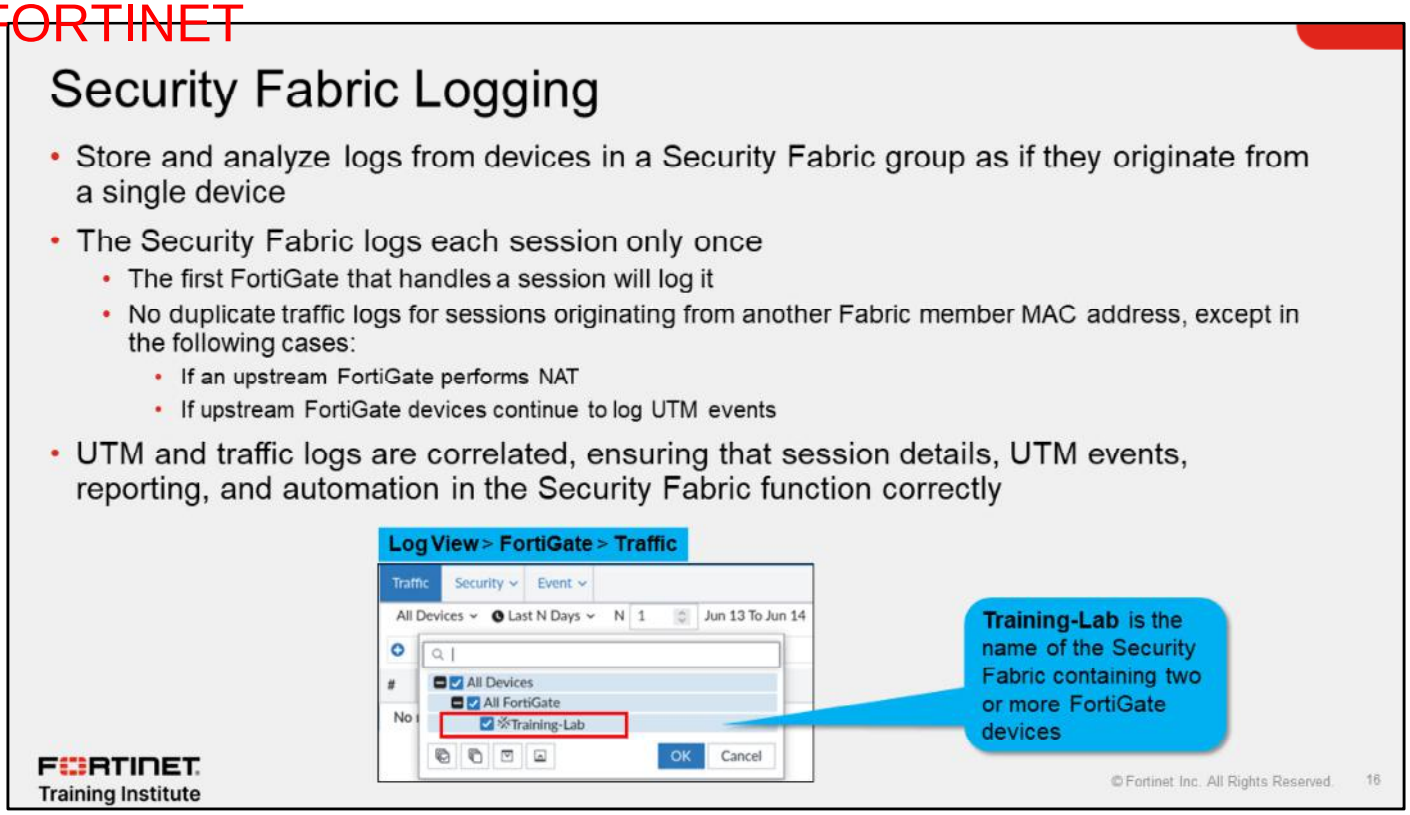
FortiAnalyzer can be integrated with many different Fortinet solutions. For a complete list, refer to the *FortiAnalyzer Release Notes* at `docs.fortinet.com`.



The logging and reporting workflow operates as follows:

1. Registered devices send their logs to FortiAnalyzer.
2. FortiAnalyzer collates and stores these logs in a manner that makes it easy to search and generate reports.
3. Administrators can access FortiAnalyzer using the GUI to manually view the logs or generate reports to analyze the data. They can also use the CLI for administrative tasks.

FortiAnalyzer can be easily integrated into a network, even across multiple sites. A typical topology may include several branch locations and a central headquarters. Each location's firewall is added into FortiAnalyzer, allowing the administrator to view logs and generate reports for the entire network from a single interface.



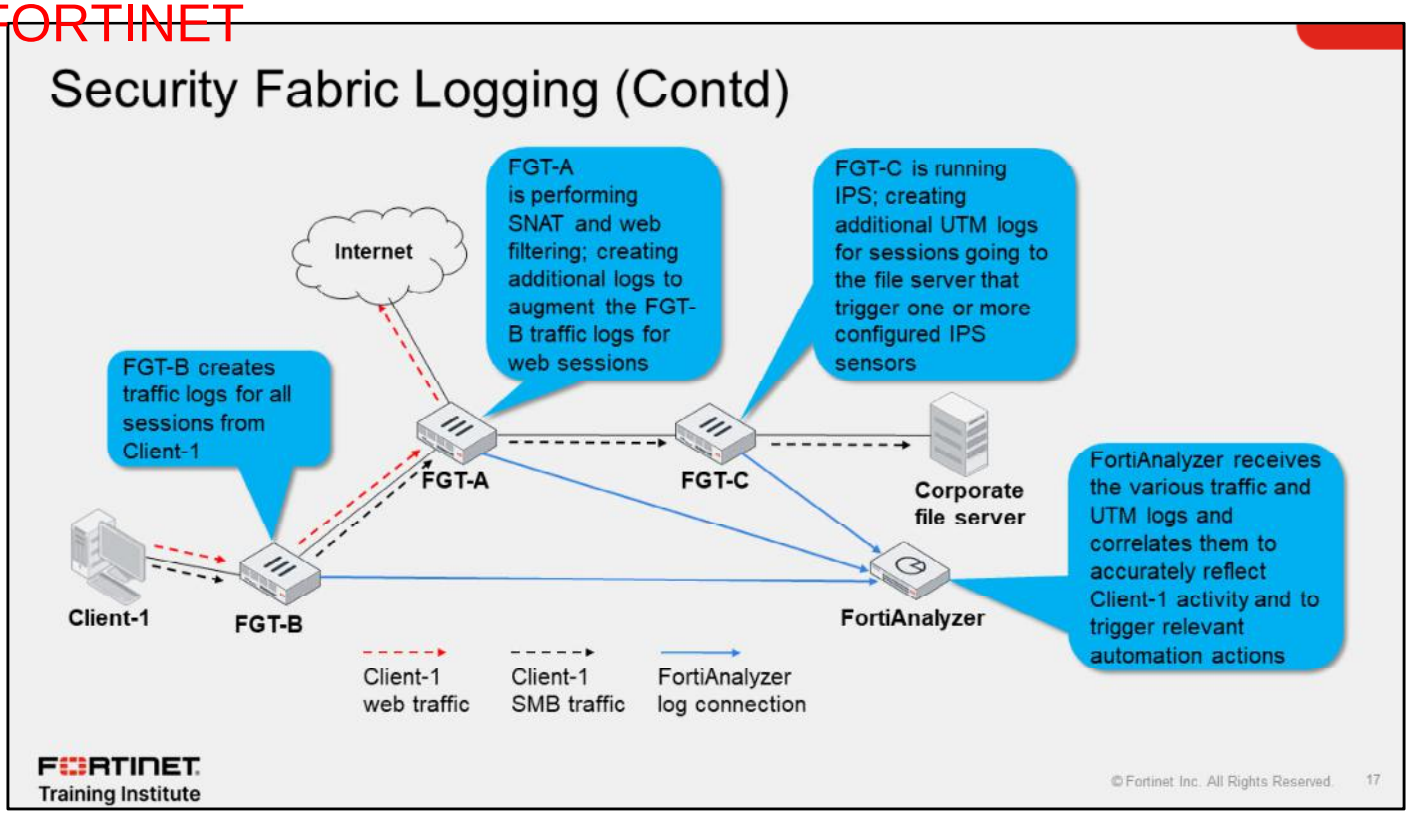
FortiAnalyzer supports the Security Fabric by storing and analyzing the logs from devices within a Security Fabric group as if they originate from a single device. It correlates traffic logs with corresponding unified threat management (UTM) logs, allowing it to report on sessions and bandwidth together with its UTM events.

Traffic logging for a session logging is always carried out by the first FortiGate that handled it in the Security Fabric. FortiGate devices in the Security Fabric know the MAC addresses of their upstream and downstream peers. If FortiGate receives a packet from a MAC address that belongs to another FortiGate in the Security Fabric, it does not generate a new traffic log for that session. This approach helps to prevent the repeated logging of the same session by multiple FortiGate devices.

One exception to this behavior is that if the upstream FortiGate performs network address translation (NAT), then another log is generated. The additional log is needed to record NAT details, such as translated ports and addresses.

When configured, upstream devices complete UTM logging, while FortiAnalyzer automatically performs UTM and traffic log correlation for the Security Fabric. This process ensures a concise and accurate record of any UTM events that may occur, requiring no additional configuration.

Note that each FortiGate in the Security Fabric logs traffic to FortiAnalyzer independently of the root or other leaf devices. If the root FortiGate is down, logging from leaf FortiGate devices to FortiAnalyzer continues to operate normally.



This slide illustrates how logging functions within the Security Fabric, ensuring full visibility while eliminating duplicate logs across the environment. Three FortiGate devices are configured in a Security Fabric along with a FortiAnalyzer device:

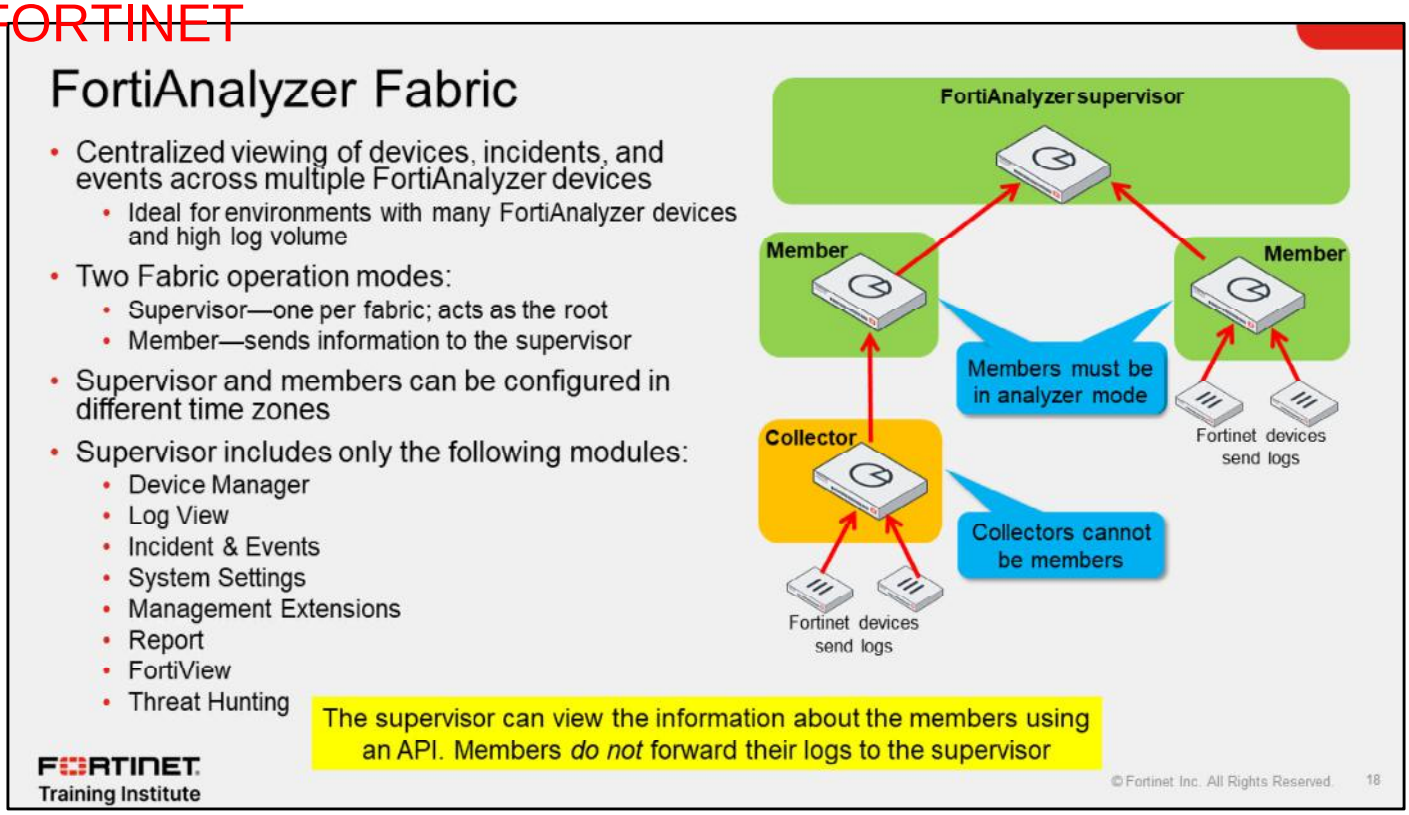
- FGT-A is installed between the corporate network and its ISP. It performs source network address translation (SNAT) on outbound communications for RFC-1918 hosts and applies web filtering for HTTP/HTTPS sessions.
- FGT-B is installed in the access layer, providing device detection, breach isolation, and basic denial-of-service (DoS) protection from the attached end-user LANs.
- FGT-C is installed in the data center, where it runs the intrusion prevention system (IPS) for all inbound communications to the servers behind it.

All traffic from Client-1 is first received by FGT-B, which creates traffic logs for the initial session.

The web session is then forwarded to FGT-A, which doesn't duplicate the initial traffic log but generates a new log due to SNAT being applied to the session. Additionally, FGT-A enforces a web filtering policy for this session and generates the relevant UTM logs as necessary.

The server message block (SMB) session is forwarded to FGT-A, which again doesn't duplicate the initial traffic log. Since FGT-A doesn't need to perform NAT or apply web filtering, it forwards the traffic to FGT-C. FGT-C also doesn't generate a duplicate traffic log, but performs IPS inspection according to its configuration. If a signature match is triggered that results in an action generating a log, it will log the event.

FortiAnalyzer receives the various traffic and UTM logs and automatically correlates them, ensuring they are linked for proper viewing, reporting, and automated actions.



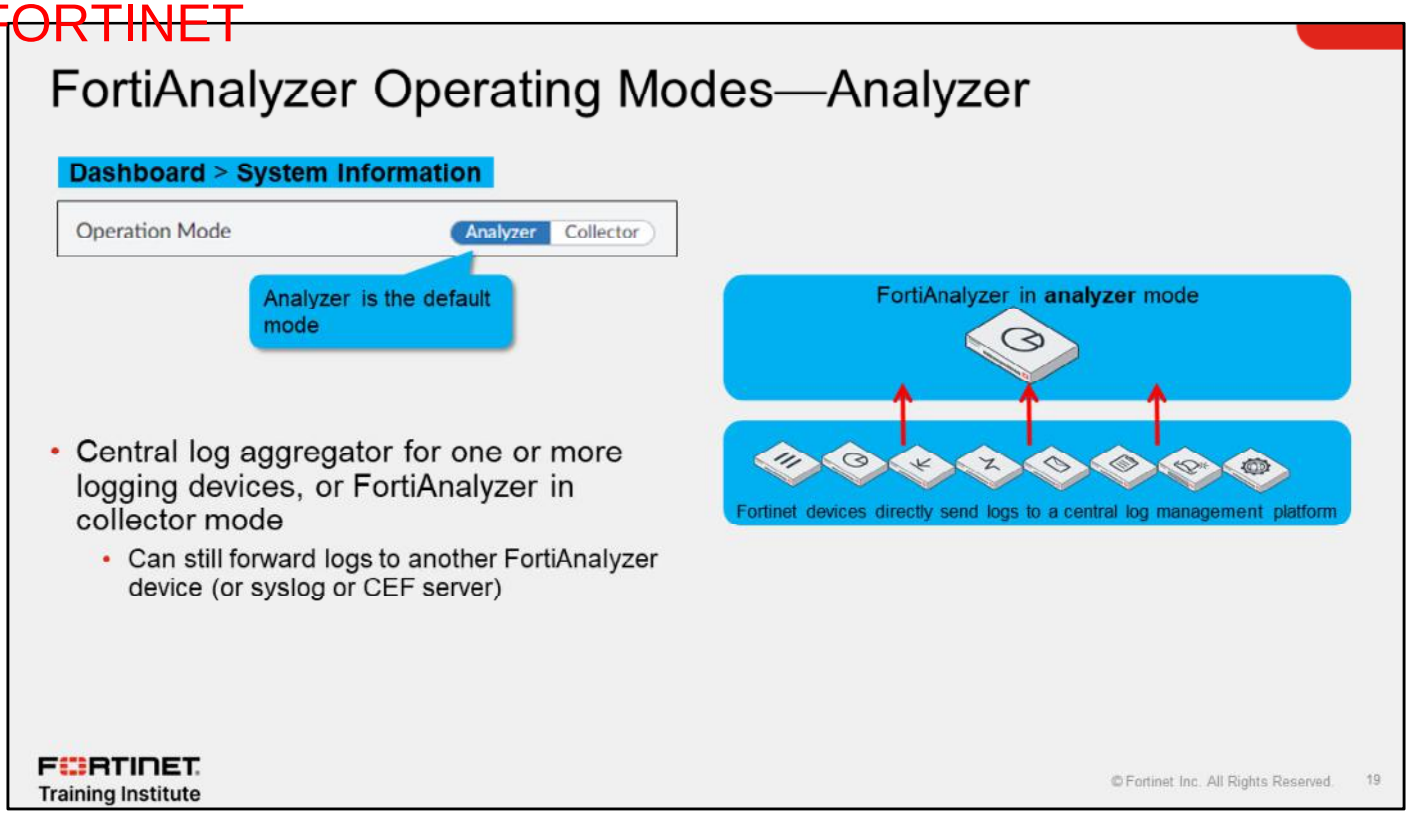
The FortiAnalyzer Fabric enables centralized monitoring of devices, incidents, and events across multiple FortiAnalyzer devices. It operates in two modes: supervisor and member.

The supervisor acts as the root device in the FortiAnalyzer Fabric. SOC administrators can use the supervisor to view member devices and their ADOMs, authorized logging devices, and incidents and events generated by members. Information regarding incidents and events is synchronized from members to the supervisor through an API.

Members are FortiAnalyzer devices that send information to the supervisor for centralized monitoring. When a device is configured as a member, it retains access to the features described in the *FortiAnalyzer Administration Guide*. Each member can create or raise incidents and events.

Devices configured with high availability (HA) can act as members; however, HA is not supported for FortiAnalyzer devices serving as the Fabric supervisor.

All members of the FortiAnalyzer Fabric don’t have to be in the same time zone settings as the supervisor.

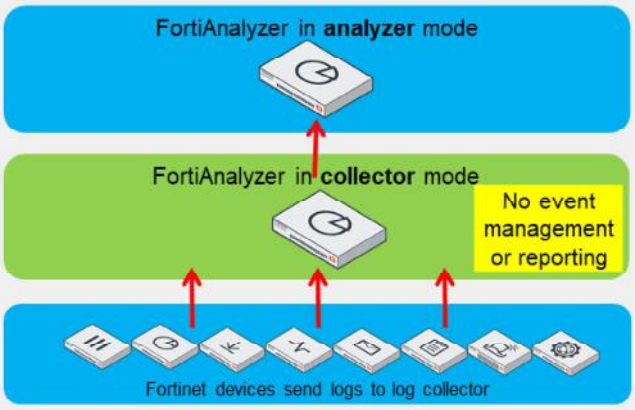


FortiAnalyzer has two modes of operation: analyzer and collector. The mode you select depends on your network topology and specific requirements. You can change the operating mode in the **System Information** widget on the dashboard.

In analyzer mode, the device acts as a central log aggregator for one or more log collectors. These could include a FortiAnalyzer operating in collector mode or any other supported device that sends logs. Analyzer is the default operating mode.

FortiAnalyzer Operating Modes—Collector

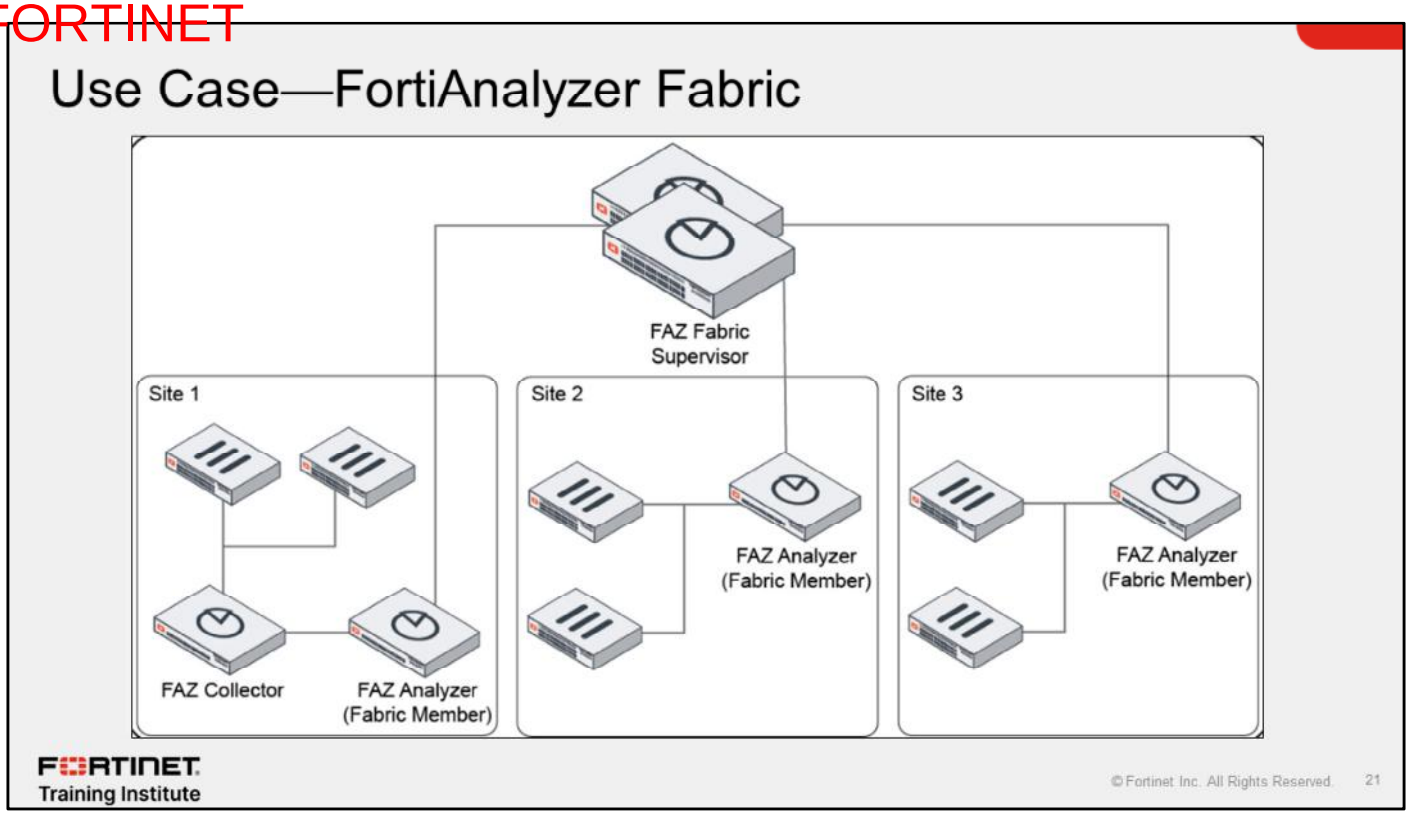
- Collects logs from multiple devices and forwards them to FortiAnalyzer in analyzer mode
  - Can aggregate logs to another FortiAnalyzer
  - However, can forward to syslog/CEF server in real-time forwarding mode only
- Not used for analytics—archiving only



FORTINET Training Institute

 20

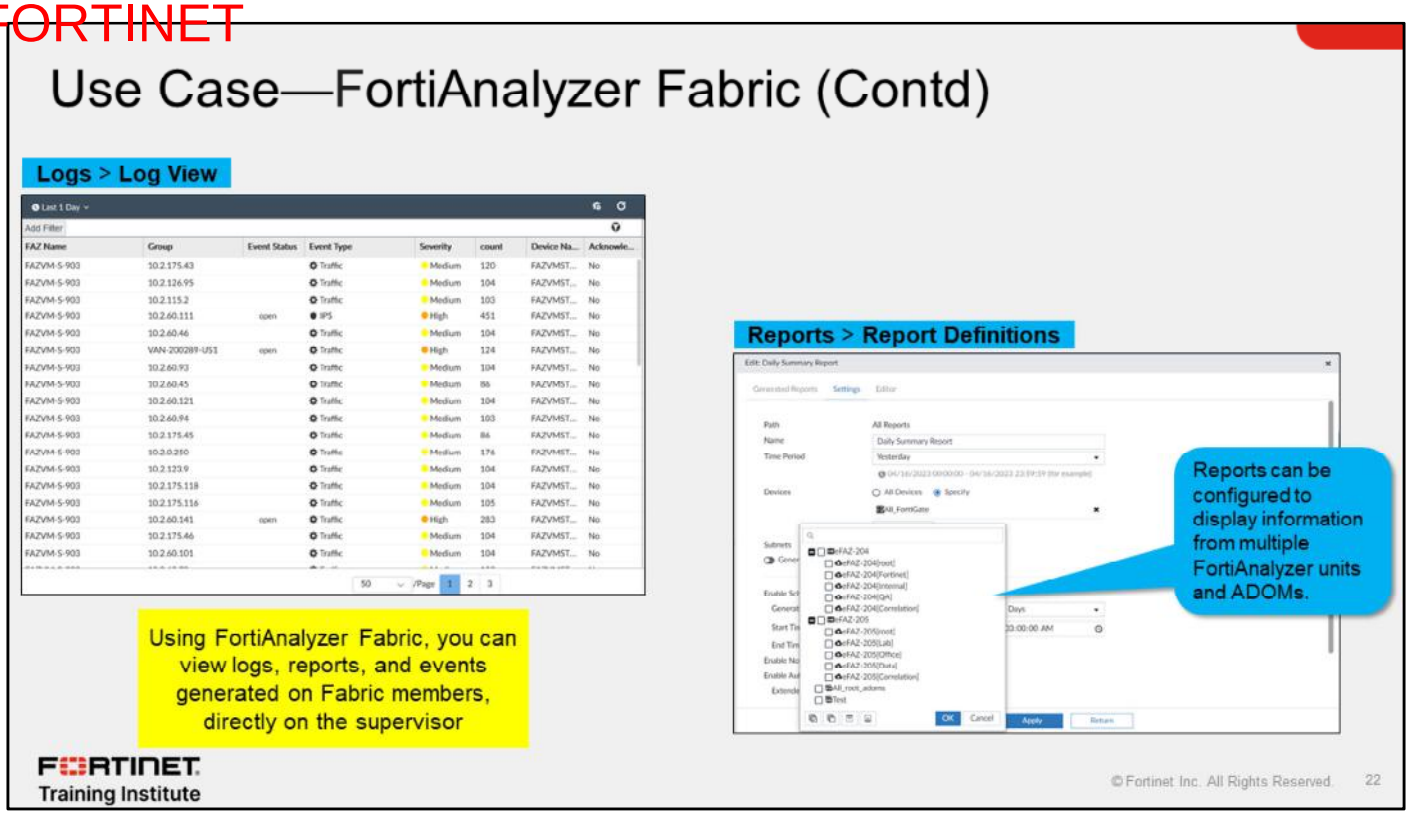
When operating in collector mode, the device collects logs from multiple devices and forwards them in their original binary format to another device, such as a FortiAnalyzer in analyzer mode. It can also send the logs to a syslog server or a Common Event Format (CEF) server, depending on the forwarding mode. A collector has fewer features compared to an analyzer, because its primary function is to collect and forward logs. It does not provide capabilities for event management or reporting.



This slide shows the use case for the FortiAnalyzer Fabric, which consists of a suitable architecture for multinational customers with subsidiaries worldwide. A multinational corporation with offices worldwide could use the Fabric Group to deploy a central analyzer at its headquarters and multiple regional collectors with their own FortiAnalyzer in analyzer mode. This architecture would give the central SOC global visibility while ensuring that log data is processed locally in each region first, thus satisfying both performance and regulatory requirements. This would make the analyzer-collector mode much more tangible.
The key differentiator here is that the regional SOC team can benefit from a fully functional analyzer, and not just have a historical log view available as on a collector. The collectors can be used to build points of presence in the different regions and forward the information to the central analyzer in the company's head office.

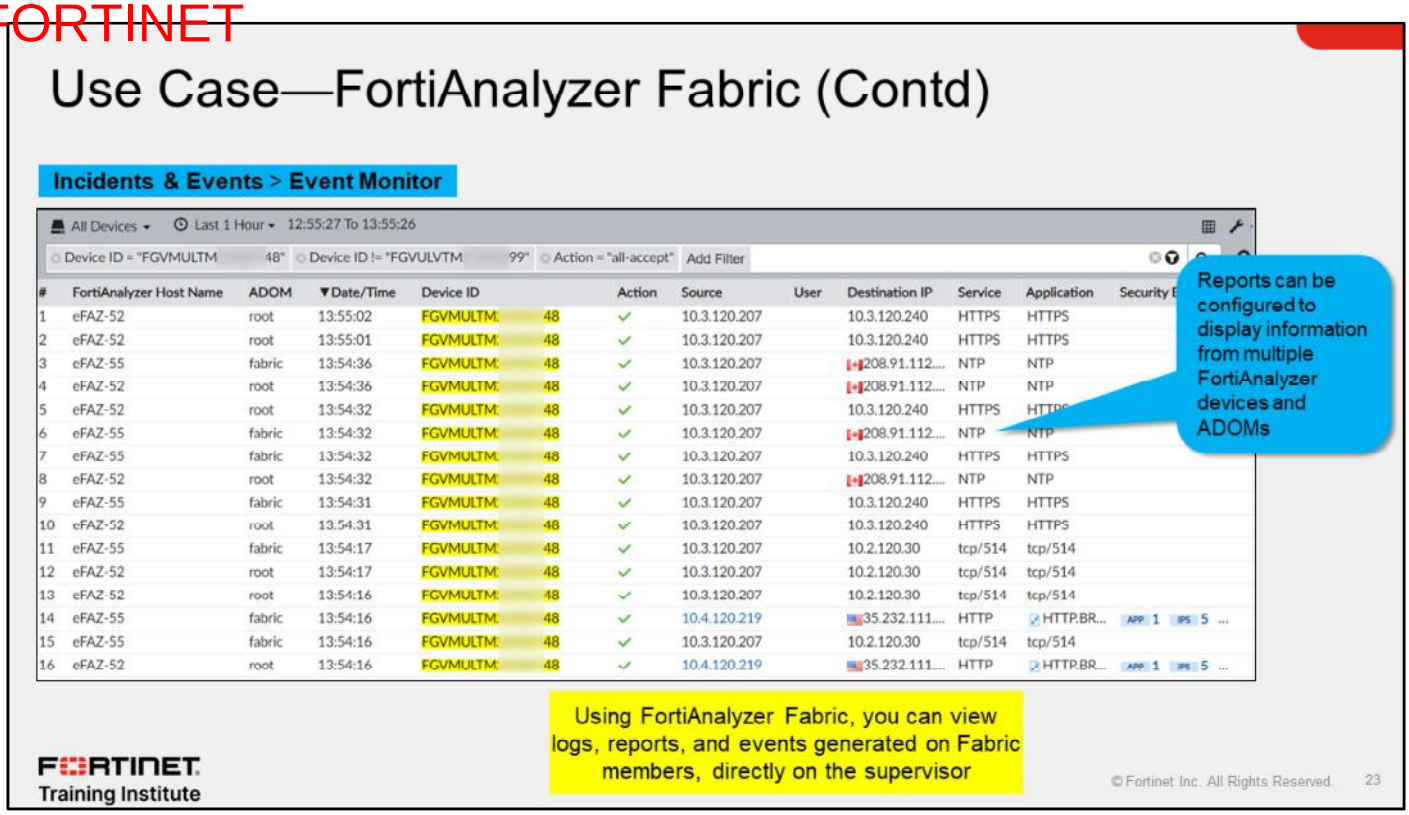
Advantages of this architecture are:
- Centralized visibility of managed devices, log view, incidents, and events is possible from a FortiAnalyzer supervisor.
- Single or multiple-tier deployments are supported (for example, Collector-Analyzer).

Some limitations of the FortiAnalyzer Fabric are:
- HA is not available on the supervisor.
- Scalability and redundancy are limited to each FortiAnalyzer deployment.
- You are not able to perform configuration changes or to run automation playbooks from the Fabric supervisor to members.



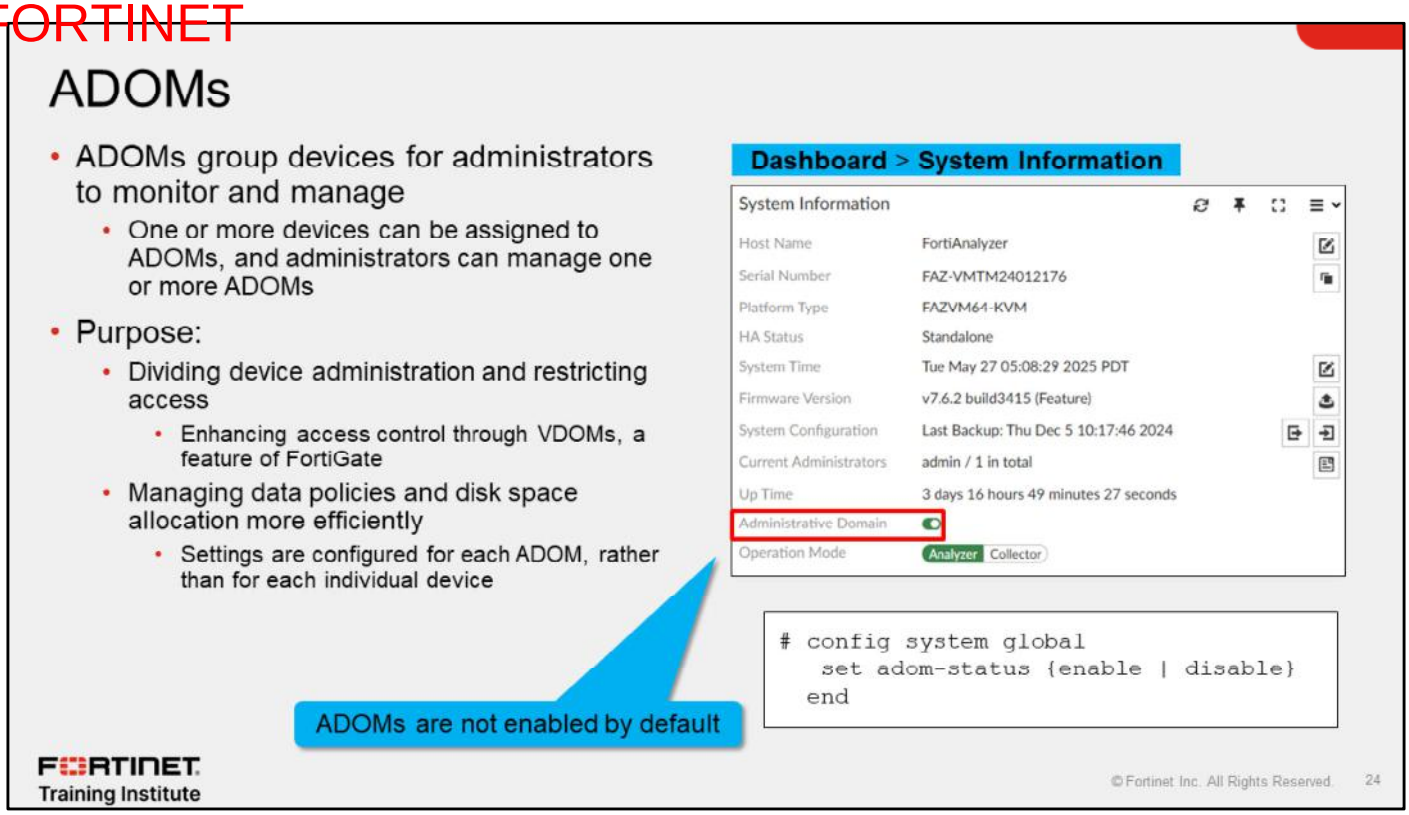
In the FortiAnalyzer Fabric supervisor, Log View displays logs collected on all FortiAnalyzer Fabric members. The logs contain the same information as displayed in the host FortiAnalyzer device they were collected on. In the example shown on this slide, the FortiAnalyzer Host Name column indicates which FortiAnalyzer the logs were collected on.

For reports, the FortiAnalyzer Fabric supervisor can fetch and aggregate data from multiple members in the FortiAnalyzer Fabric. This enables the SOC analysts at HQ to find correlations between sites and respond accordingly. In the example shown on this slide, the report can be configured to display information from multiple FortiAnalyzer devices and ADOMs.



Events generated by event handlers on the FortiAnalyzer Fabric members are visible on the supervisor. The SOC analysts can review these events for correlations between the members, so they can be managed together more efficiently rather than individually across the sites.

The event handlers must be configured on each of the FortiAnalyzer members; however, the related logs that trigger the event handler rules are visible from the supervisor.



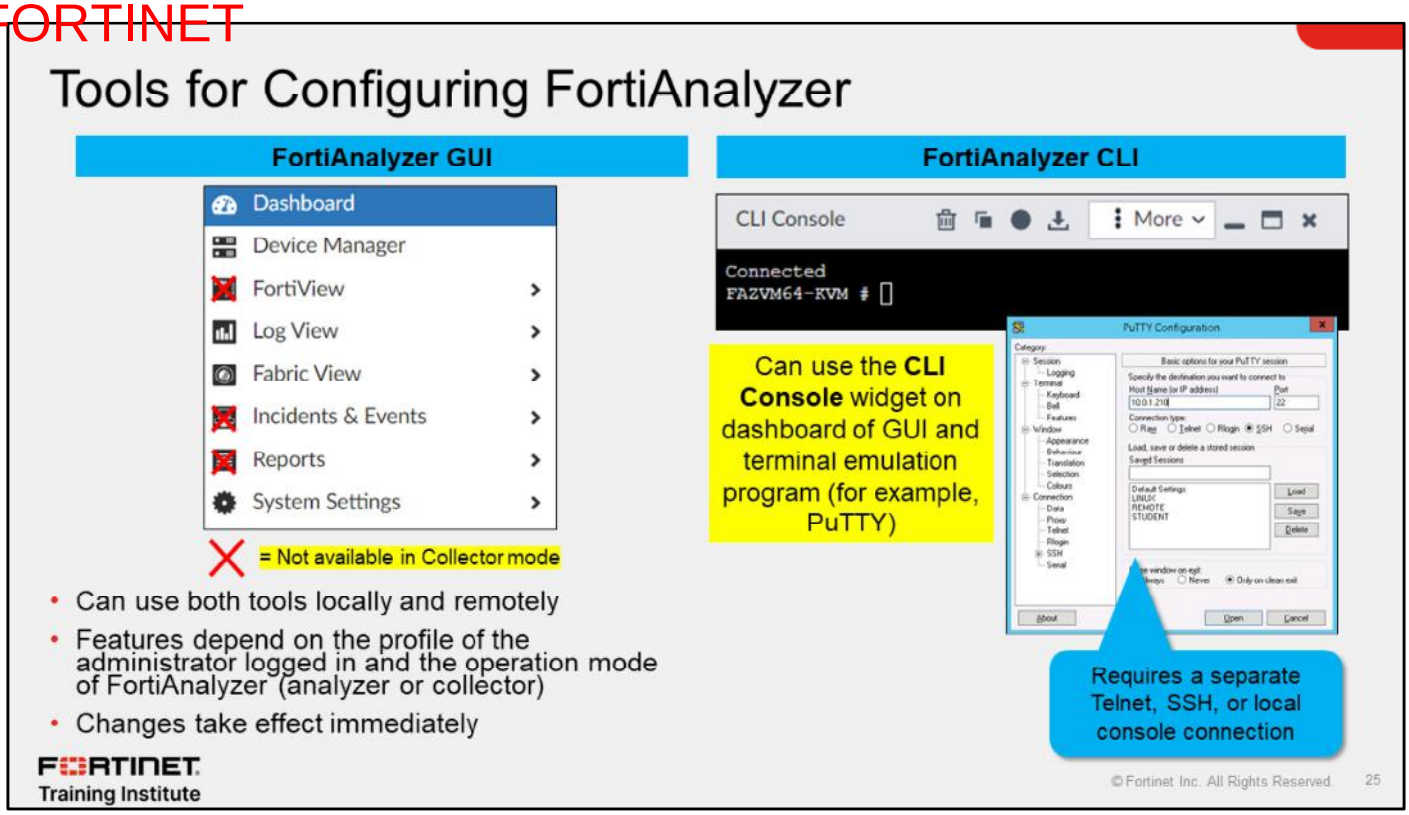
ADOMs allow you to group devices for efficient monitoring and management. For instance, administrators can manage devices based on their geographical location or business division.

The primary purposes of ADOMs are:
- To divide the administration of devices by ADOM and to control (or restrict) administrator access. If your network uses VDOMs, ADOMs can further limit access to data from the VDOM of a specific device.
- To manage data policies and disk space allocation more efficiently, which are set per ADOM.

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

All Fortinet devices that are part of a Security Fabric can be assigned to an ADOM of the Fabric type, allowing for rapid data processing and log correlation.

You will learn more about ADOMs in this course.



You can use both the GUI and CLI to configure and manage FortiAnalyzer. You can use both tools locally by connecting directly to FortiAnalyzer, or remotely, based on your configured settings. You can deny or permit access based on IP addresses.

When using the CLI, you can run commands through the **CLI Console** widget, available on the GUI dashboard, or through a terminal emulation application like PuTTY. Using PuTTY requires a separate Telnet, SSH, or local console (DB-9) connection.

The FortiAnalyzer features available on the GUI and CLI depend on the profile of the administrator logged in and the operation mode of FortiAnalyzer. For instance, in collector mode, the GUI doesn't include **FortiView**, **Reports**, or **Incidents & Events**. Additionally, if you log in with the Standard_User or Restricted_User administrator profiles, you will not have full access privileges; those are reserved for the Super_User profile. The CLI also includes some settings that are not available through the GUI.

Any configuration changes you make using the GUI and CLI take effect immediately upon applying the settings, requiring a reset of FortiAnalyzer or disrupting its services.

Note that the SQL database is disabled by default when FortiAnalyzer is in collector mode. Logs that rely on the SQL database are not available in this mode unless the SQL database is enabled through the CLI.

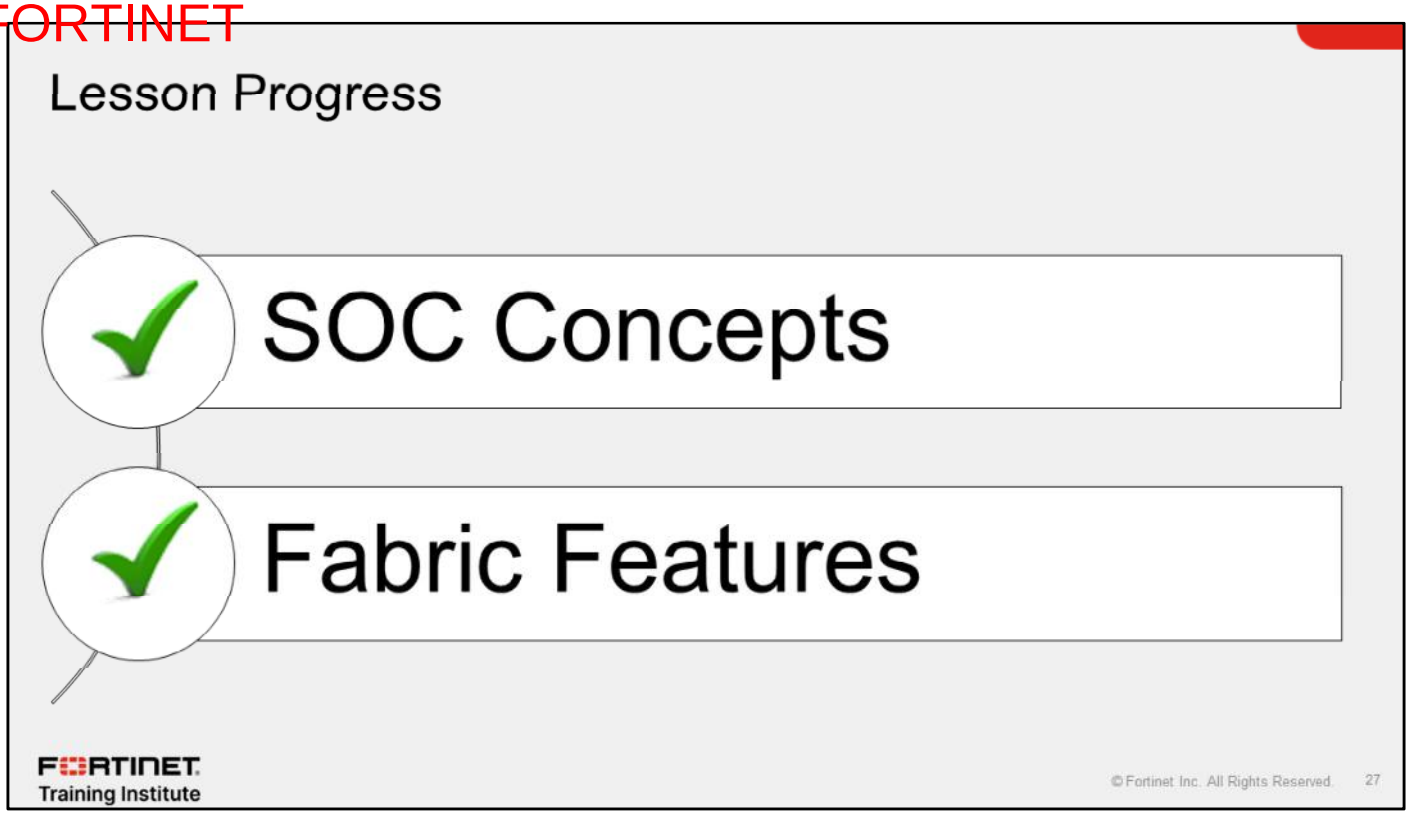
Knowledge Check

1. What is the default FortiAnalyzer operation mode?
   - ✓ A. Analyzer
   - B. Collector

2. What are the operation modes in a FortiAnalyzer Fabric?
   - ✓ A. Supervisor and member
   - B. Analyzer and collector

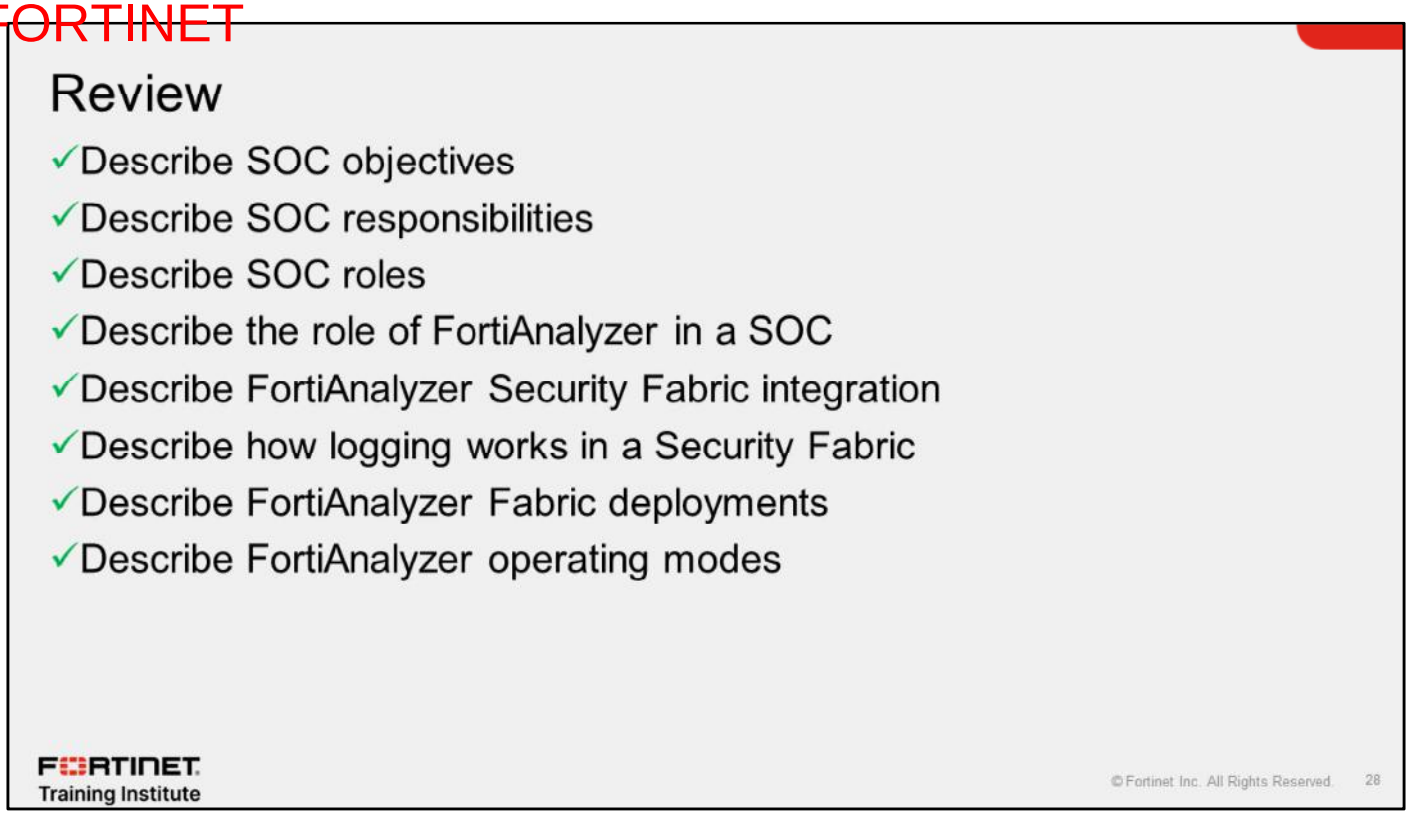
FORTINET Training Institute

 26

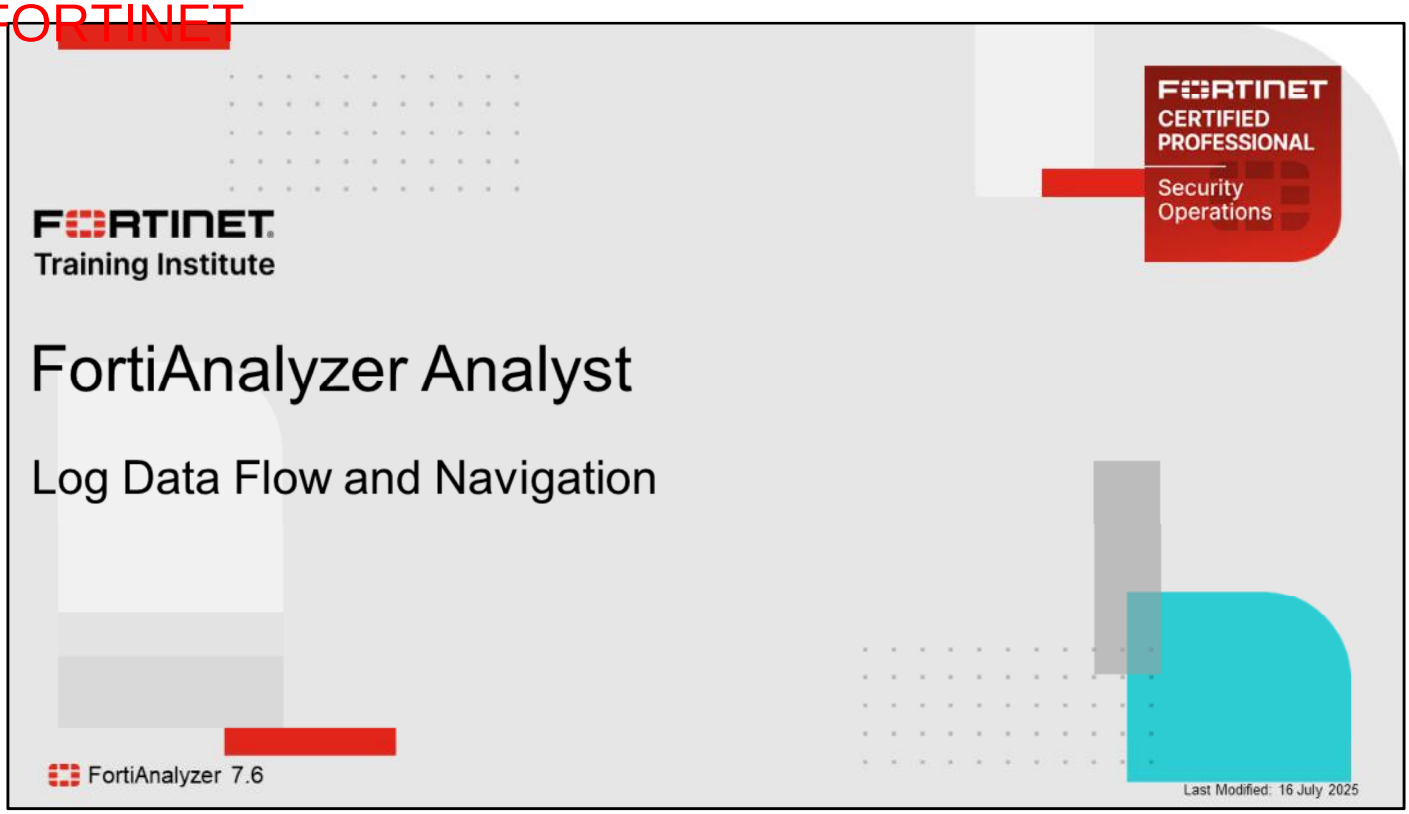


Congratulations! You have completed this lesson.

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

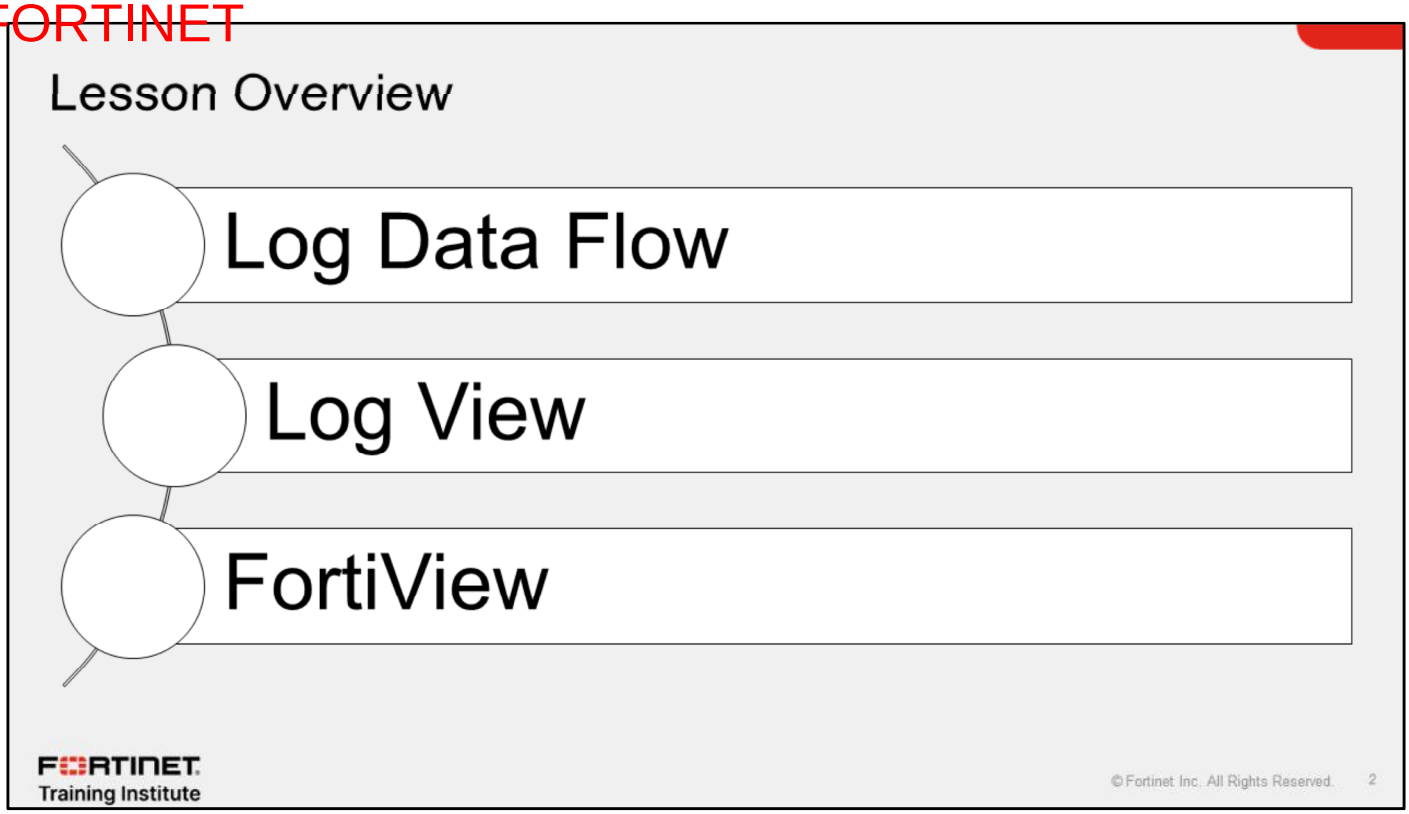


This slide shows the objectives that you covered in this lesson.

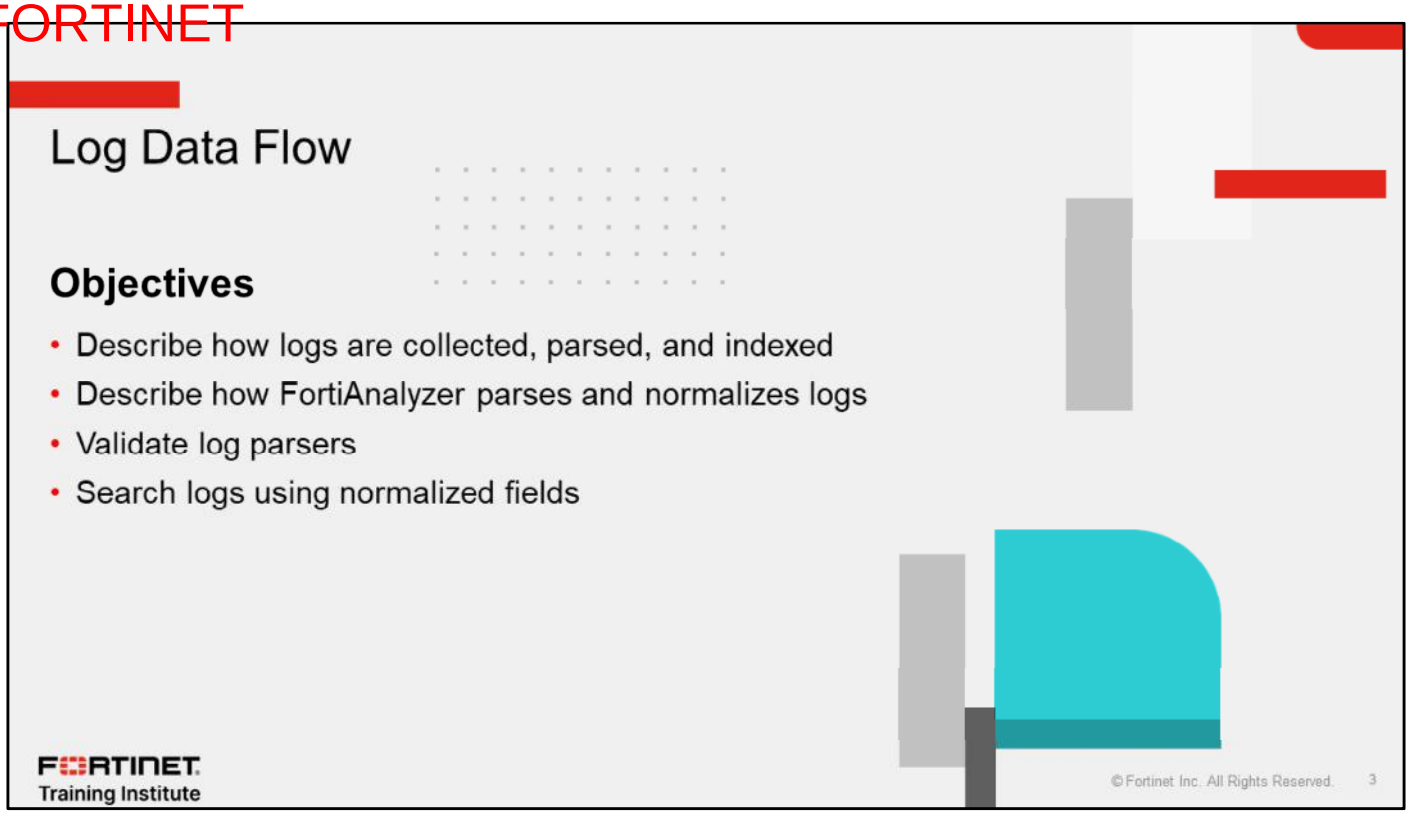


In this lesson, you will learn how to protect, view, and manage logs on FortiAnalyzer.

By understanding logging on FortiAnalyzer, you will be able to use log data to analyze network-based attacks, as well as troubleshoot and investigate network issues.



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



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

By demonstrating competence in understanding the purpose of log collection, log storage, and the log file workflow, you will have a better understanding of how logs are compiled and collected.

Purpose of Logs

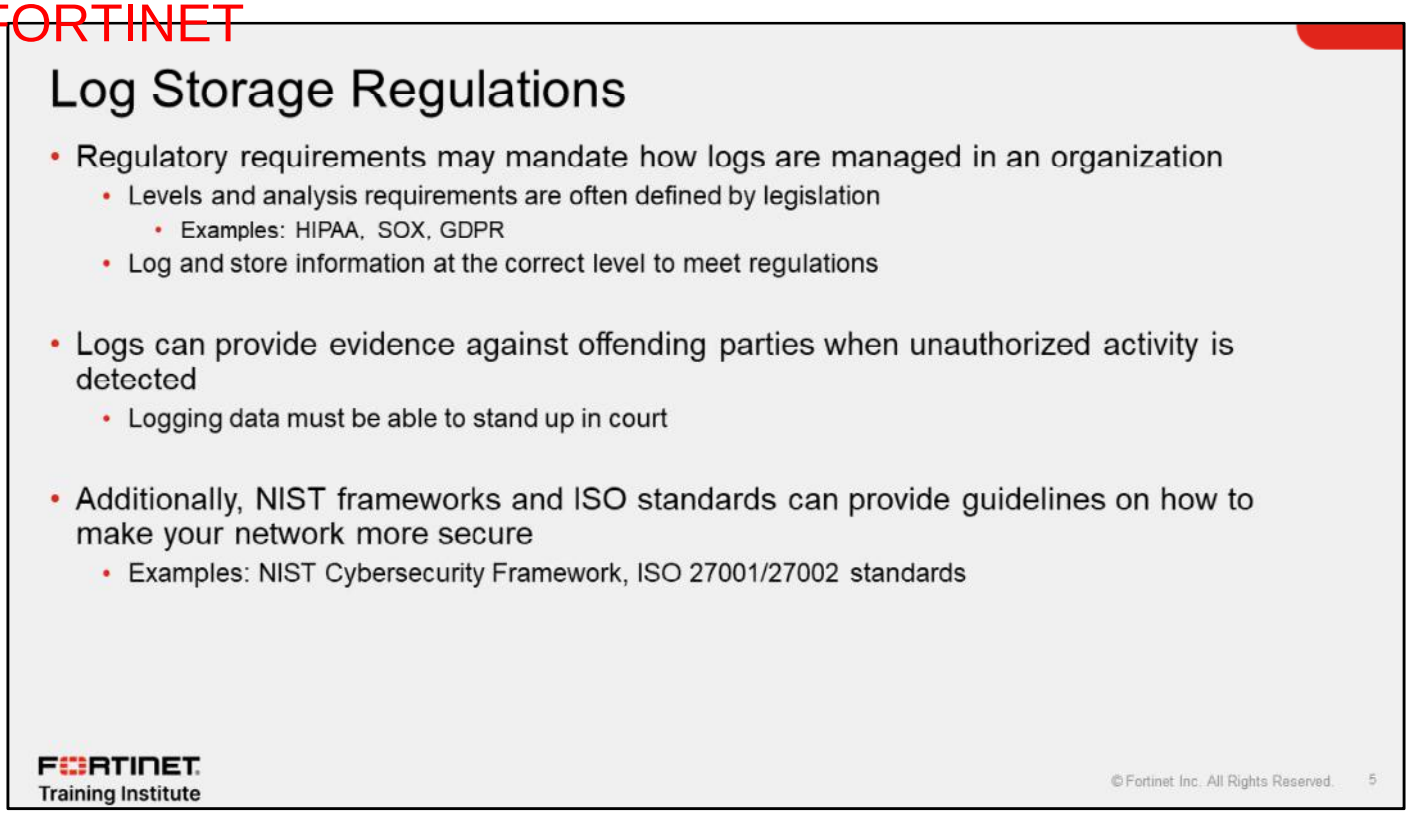
- Record information containing specific details about the network
- Troubleshoot ongoing issues with the network
- Determine load on network devices and establish baselines
- Track service use
- Support incident response and forensic analysis

FORTINET Training Institute

 4

Log messages help paint a picture of what is going on in your network. You can use logs for many purposes. You can use logs to troubleshoot your network, determine load on network devices, establish baselines, track service use, and support incident response and forensic analysis.

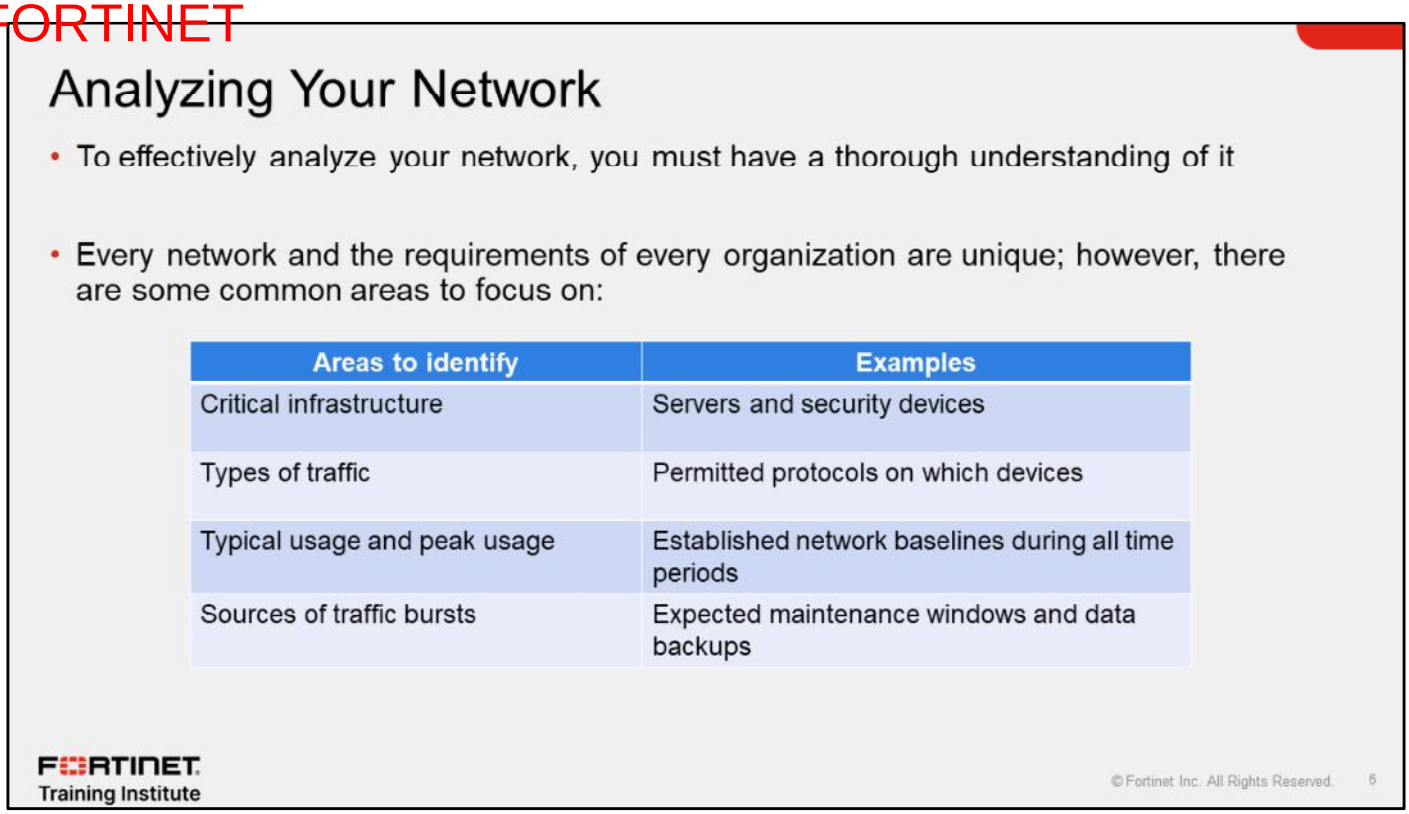
It is important to understand that logs are like a puzzle: You must put several pieces together to get a complete understanding of what is going on. You often need to review multiple log messages to determine the exact chain of events and activities that led to a breach. Examining a log in isolation often won't help you determine the best way to configure your network to prevent such breaches in the future. This is why centralized log storage is so important.



Regulations require organizations to log specific information, record data, and store it at the correct level. You must thoroughly understand the legislation that your organization must comply with, including the jurisdictions your organization falls under, and if there are any industry-specific regulations you must follow. For example, the financial and healthcare sectors may be subject to additional regulations, and certain private information may not be recorded.

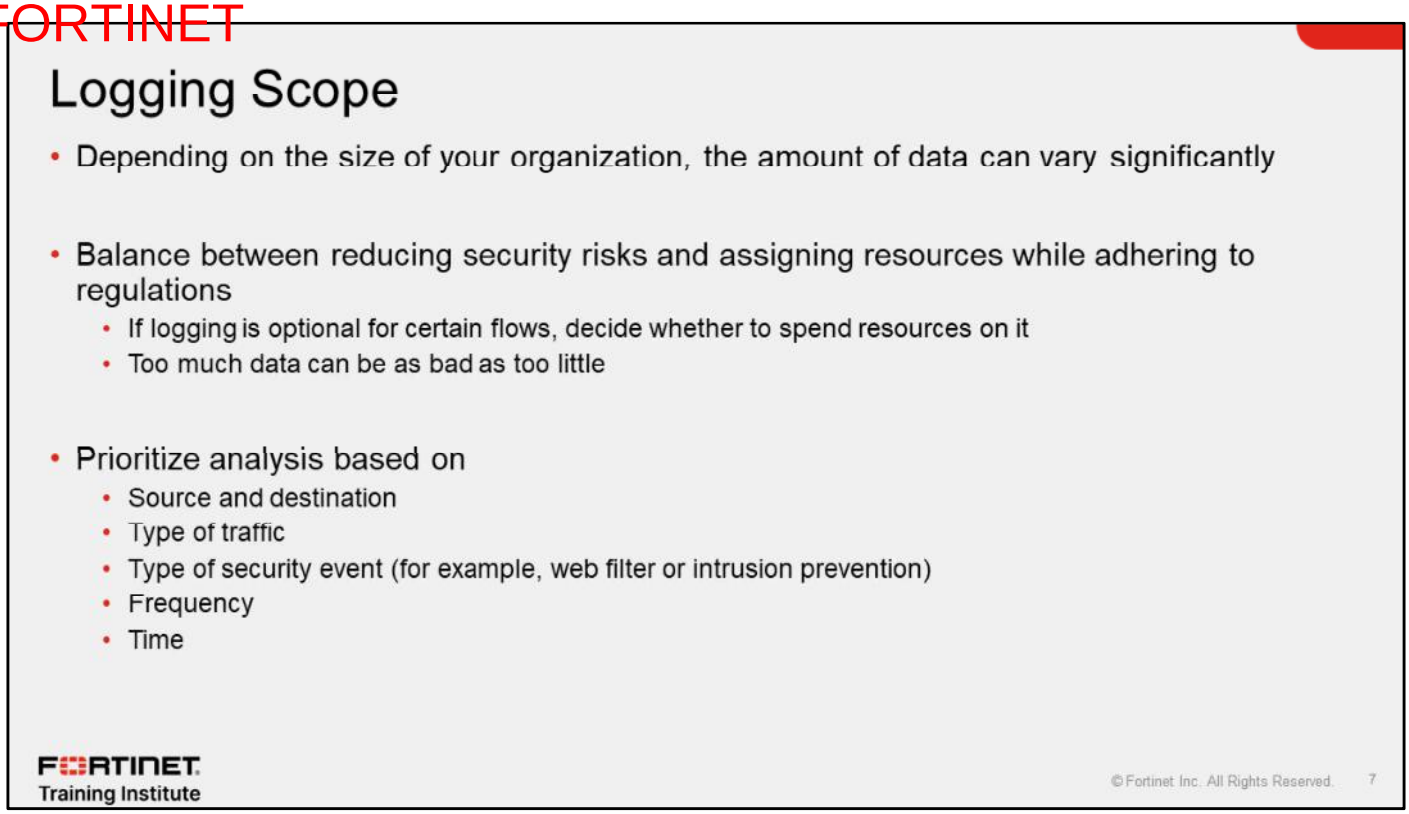
You can use log entries as evidence in cases of unauthorized or illegal activity. The data you use as evidence must be able to stand up in court, so it is vital that you are able to understand and analyze your logs.

Establishing your organization's security policies can be difficult, particularly if no existing policies are in place. When developing security policies for your organization, Fortinet recommends that you consult widely recognized frameworks and standards created by organizations such as the National Institute of Standards and Technology (NIST) and the International Organization for Standardization (ISO).



To effectively analyze the traffic in your organization, you must have a deep understanding of the network and be able to identify the following:

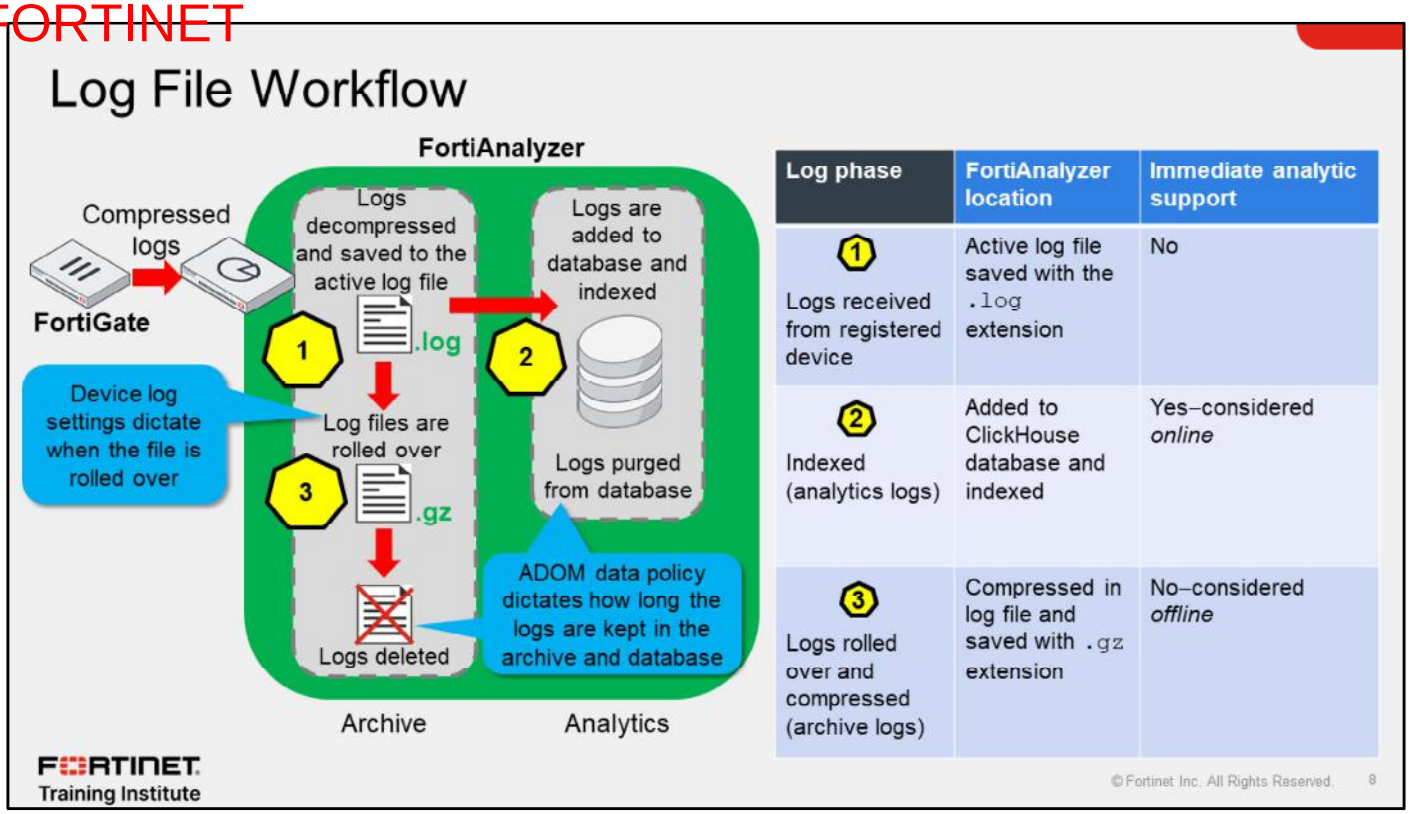
- Critical infrastructure, such as servers and security devices. These take the highest priority in any analysis.
- Expected traffic types. This includes knowing which protocols are permitted on which devices and being able to quickly identify abnormal traffic flows.
- Typical and peak usage levels. Establishing network baselines for traffic levels at all hours will help you recognize unexpected behavior, such as a higher-than-normal amount of traffic during a certain time period.
- Sources of traffic bursts. You can use this data to create a buffer for expected maintenance windows and data backups.



Depending on your organization's size, the amount of log data generated can become overwhelming. Logs are usually generated continuously, and one workstation can generate a large volume of logs in a short time. As an analyst, it is not practical to review every log entry. Most logs are normal: Using resources to analyze them yields no benefits.

Not everything in the network needs to be logged. For example, if your infrastructure team plans to conduct tests on an isolated network, you can work with them to disable logging beforehand. Guest devices on a restricted network also may not need to be logged.

In your analysis, prioritize factors such as the traffic type or types, the traffic sources and destinations, and if there are any security events associated with the traffic. In addition, if traffic is being sent at a frequency that is unexpected, whether you are seeing traffic more or less frequently than expected, further investigation is warranted. Knowing when your network is expected to produce traffic can also help you identify anomalous behavior, such as excessive traffic during off-hours.



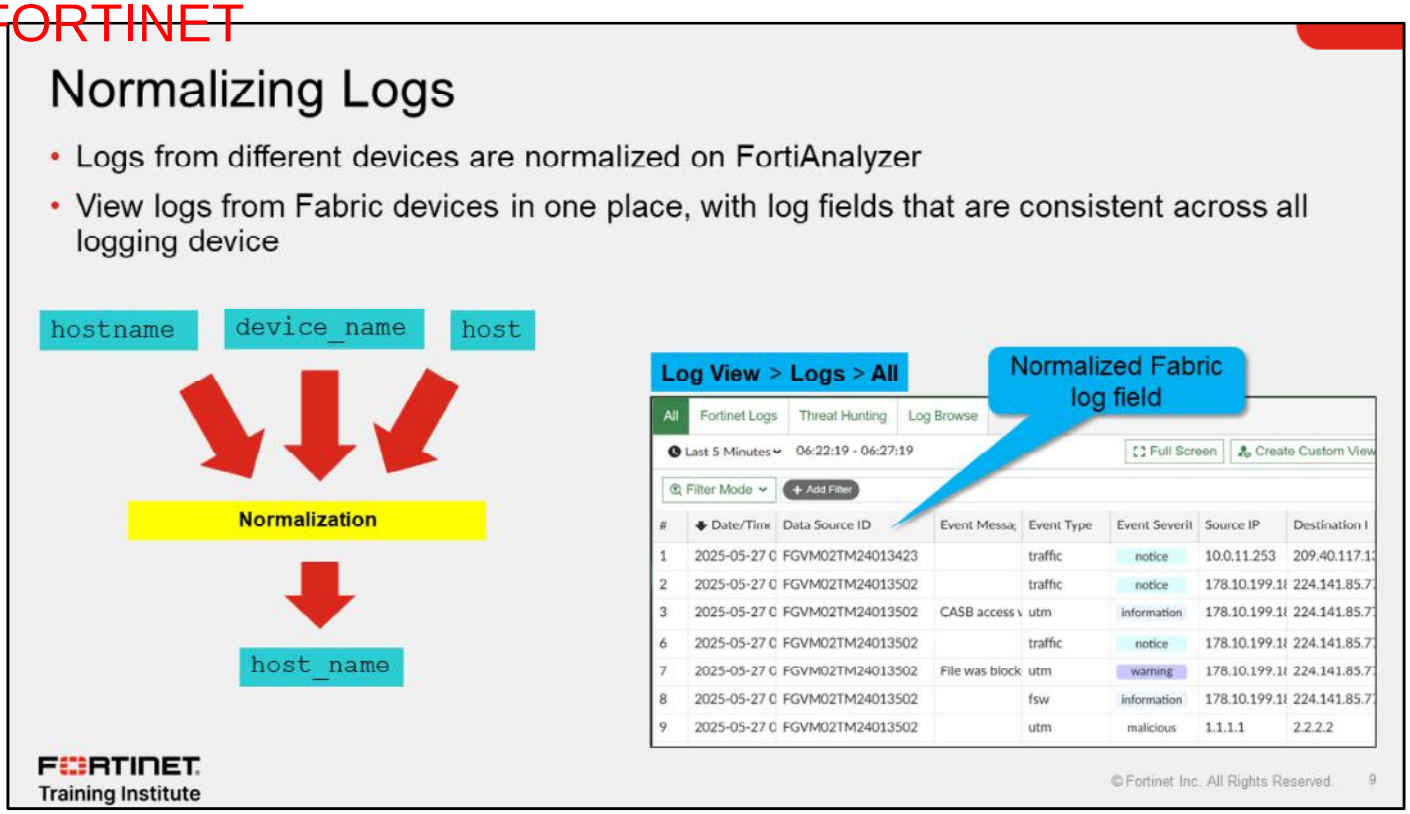
Log phase	FortiAnalyzer location	Immediate analytic support
1 Logs received from registered device	Active log file saved with the `.log` extension	No
2 Indexed (analytics logs)	Added to ClickHouse database and indexed	Yes–considered *online*
3 Logs rolled over and compressed (archive logs)	Compressed in log file and saved with `.gz` extension	No–considered *offline*

When registered devices send logs to FortiAnalyzer, logs enter the following automatic workflow:

1. Logs received are decompressed and saved in a log file on the FortiAnalyzer disk. The log file has the extension *.log*. For example, FortiAnalyzer saves FortiGate logs with the names *tlog.log* and *elog.log*, for traffic and event logs, respectively. Note that the tlog.log file includes FortiGate security logs.

2. At the same time, FortiAnalyzer indexes the saved logs in the SQL database to support analysis. Logs in the indexed phase are known as *analytics* logs. These logs are considered to be online and offer immediate analytic support. FortiAnalyzer purges analytics logs from the SQL database as specified in the ADOM data policy.

3. When the log file reaches a specified size, or at a set schedule, it is rolled over. The process of rolling a log file over consists of renaming the file, adding a timestamp, and then compressing it, which adds the `.gz` extension. These files are known as *archive* logs and are considered offline, so they don't offer immediate analytic support. Combined, archived logs count toward the archive quota and retention limits, and FortiAnalyzer deletes them based on the ADOM data policy.

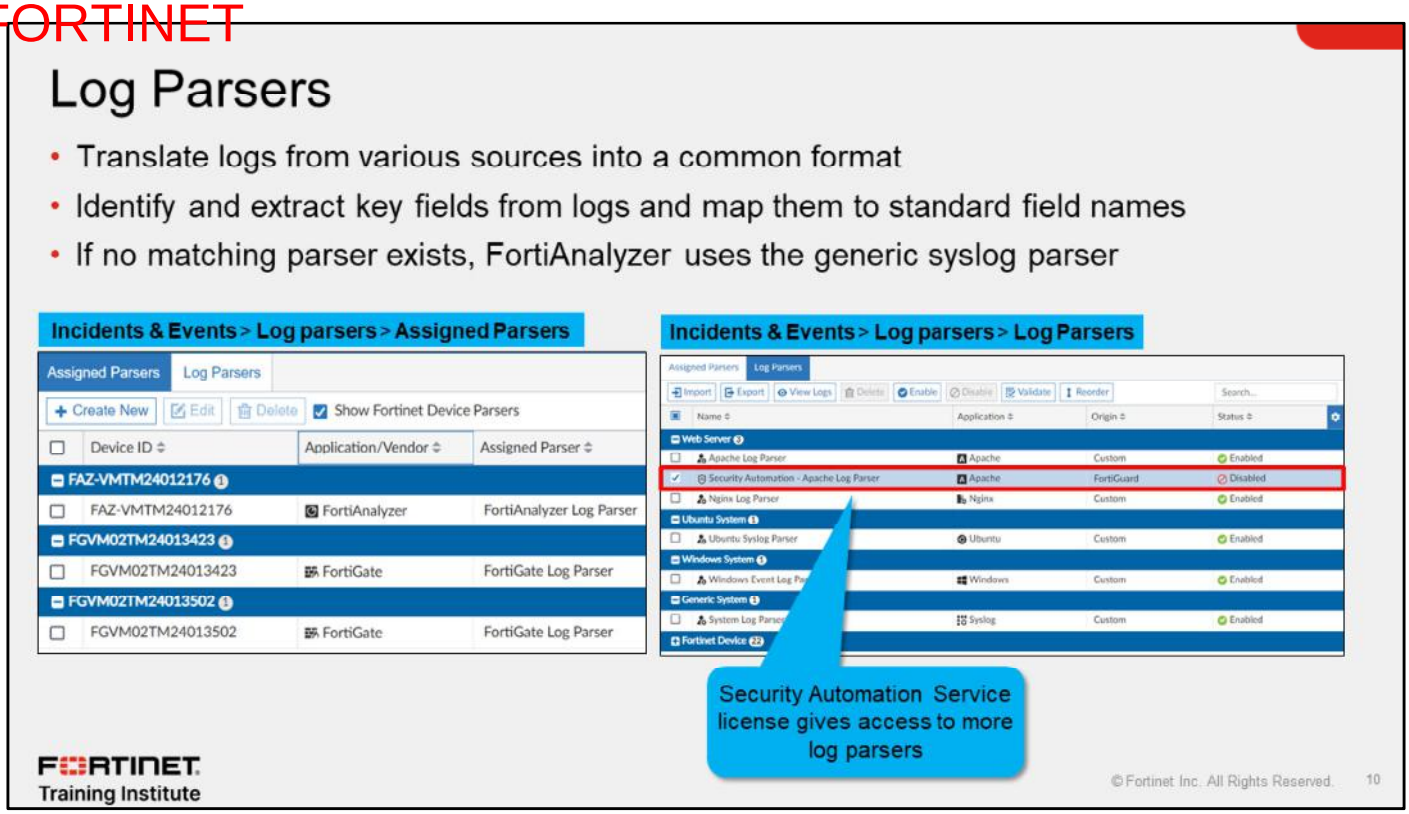


FortiAnalyzer can ingest logs from various sources. To make it easier for analysts to view and understand logs, FortiAnalyzer performs log normalization to display log fields that are consistent across all logging devices. Log normalization transforms disparate log entries into a standardized, structured format.

When FortiAnalyzer ingests logs, they are usually in their native, unstructured format. When you add a device to a Fabric ADOM, FortiAnalyzer creates a security information and event management (SIEM) database for that ADOM, where it stores all normalized logs. FortiAnalyzer uses predefined parsers to extract key fields from ingested logs and maps them to a consistent, standardized set of field names. After parsing and mapping, FortiAnalyzer inserts and indexes the log entries within the SIEM database.

Normalized logs provide a unified view and allow for easier correlation and faster investigation. For example, with standardized fields and values, FortiAnalyzer can correlate events from different devices, such as a traffic block on FortiGate and a failed login event on FortiAuthenticator. Log field correlation improves reporting accuracy and allows you to enrich log data with additional context like user identity or threat intelligence data.

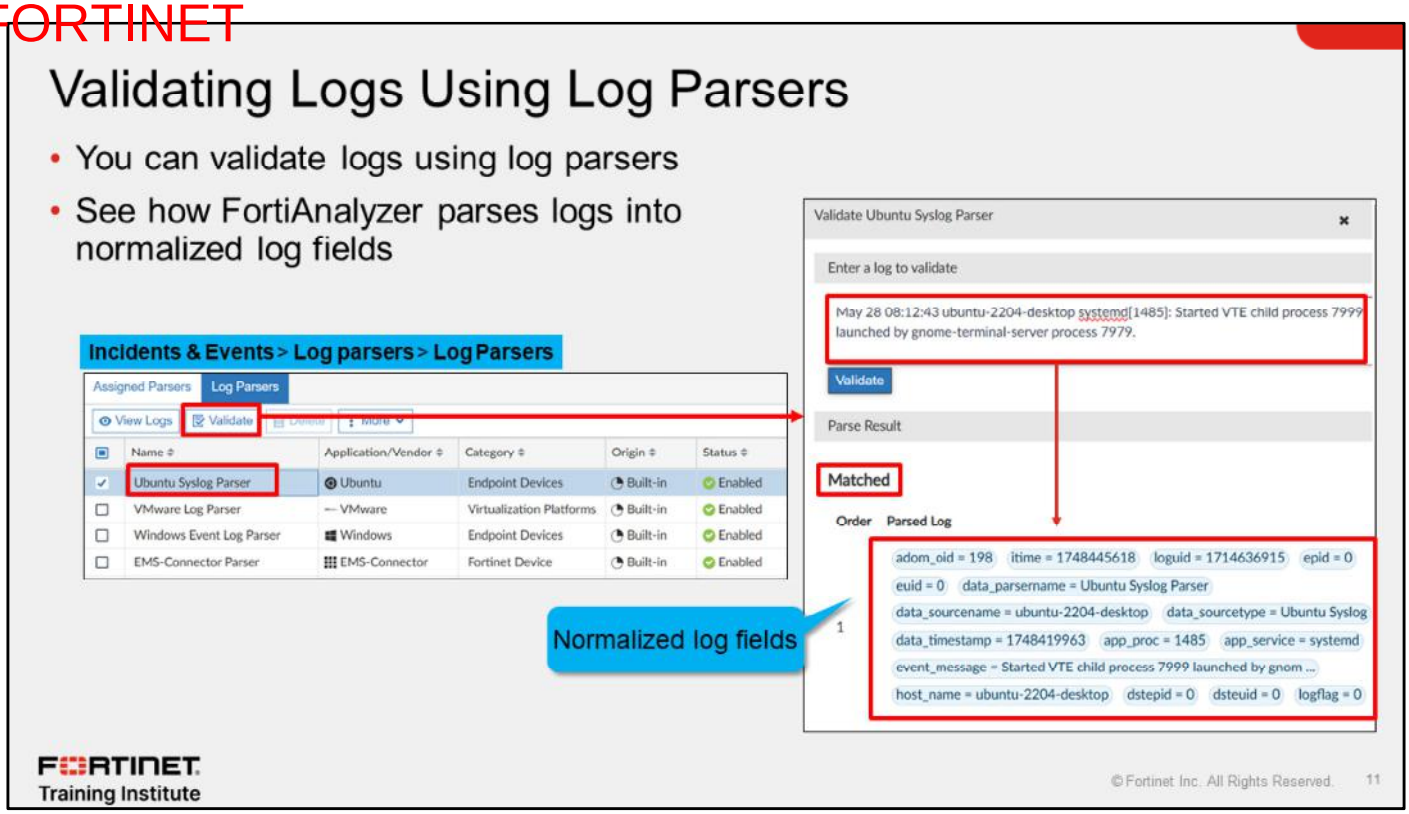
The *Fabric Normalization Reference* guide provides a comprehensive list of log field correlations between Fabric devices and FortiAnalyzer.



Log parsers interpret and transform raw, unstructured, or semistructured log messages into a standardized, structured format. Parsers are central to log normalization.

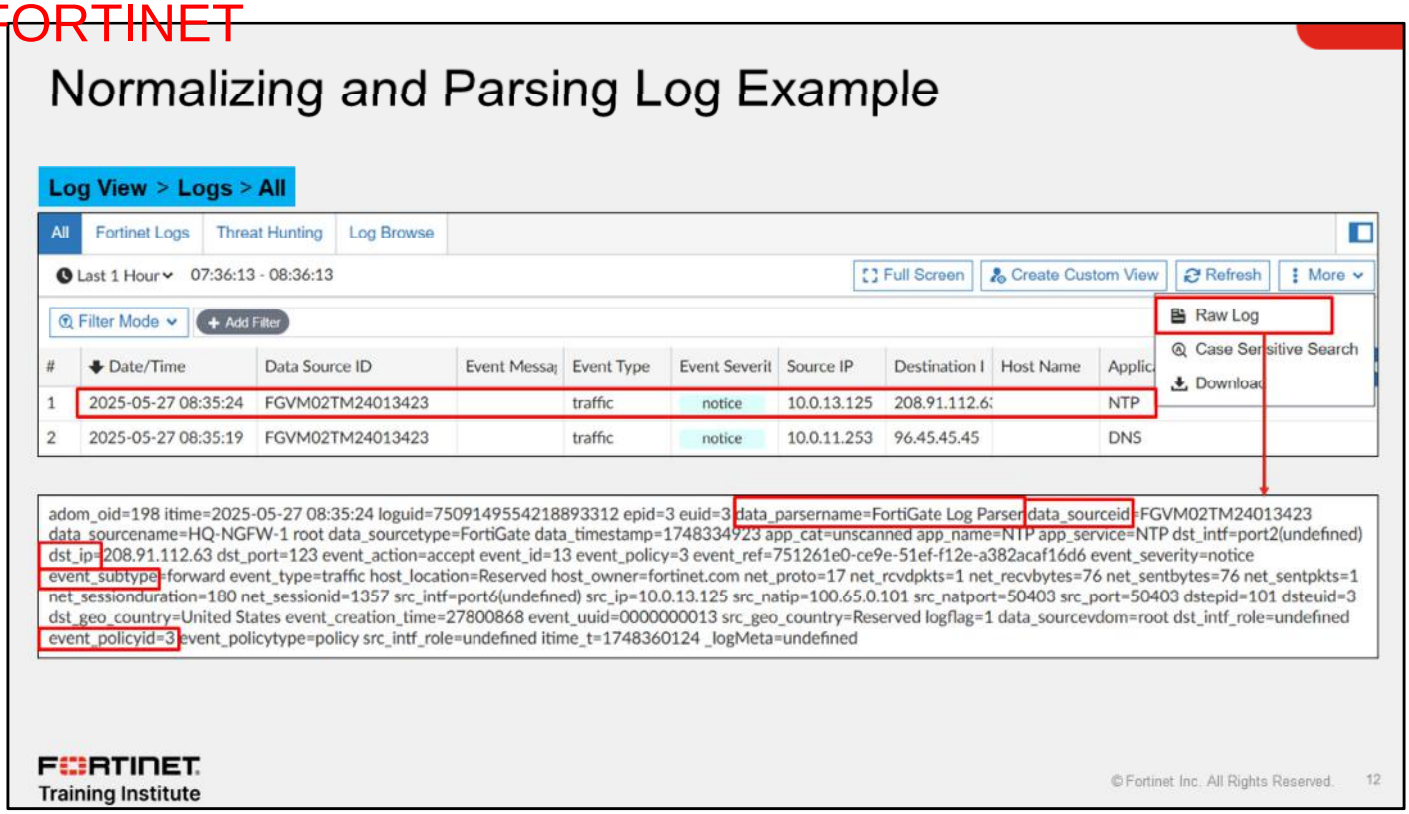
Parsers contain rule sets and predefined logic that FortiAnalyzer applies to incoming log data. Think of parsers as translators that convert device-specific or vendor-specific logs into a common schema on FortiAnalyzer. Parsers identify and extract key fields from log messages and map them to standardized field names. Some parsers can also standardize field values. For example, different devices may report traffic block actions differently: some might use “block” and others might use “deny”. In cases like this, parsers can convert the various values into a unified format—blocked.

FortiAnalyzer includes built-in parsers that parse, normalize, and correlate logs from Fortinet products as well as third-party applications. For example, there are built-in log parsers for Apache and Nginx web servers, and for security event logs from Windows and Linux hosts (with Fabric Agent integration). Additionally, the Security Automation Service license gives you access to even more log parsers.



The validate function allows you to test how a specific parser will process a raw log entry. This is useful when working with third-party logs or troubleshooting unexpected parsing issues.

This slide shows a validation example using the Ubuntu syslog parser. It shows how FortiAnalyzer takes the raw systemd log and parses and normalizes the various log fields.

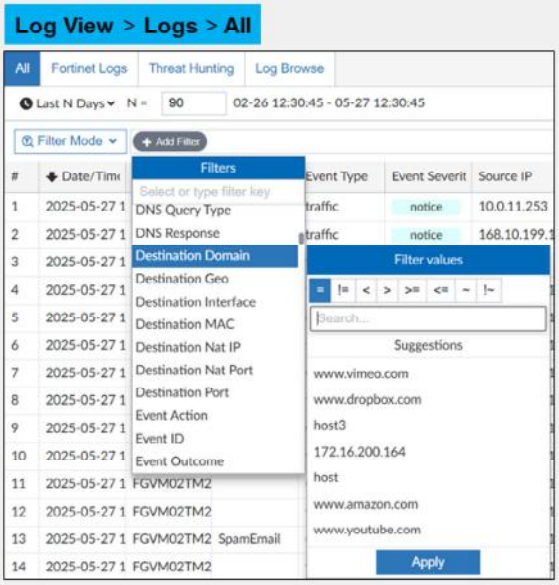


This slide shows a FortiGate event log that has been normalized by FortiAnalyzer using the FortiGate log parser. When you change the view to raw log format, you can see that common FortiGate log fields, such as `data_sourceid`, `dst_ip`, `event_subtype`, and `event_policyid`, have been converted to normalized log fields.

FortiAnalyzer performs normalization for every supported device log that it receives. Normalization makes it easier for you to search and view logs across all the devices in your network.

Searching Using Normalized Fields

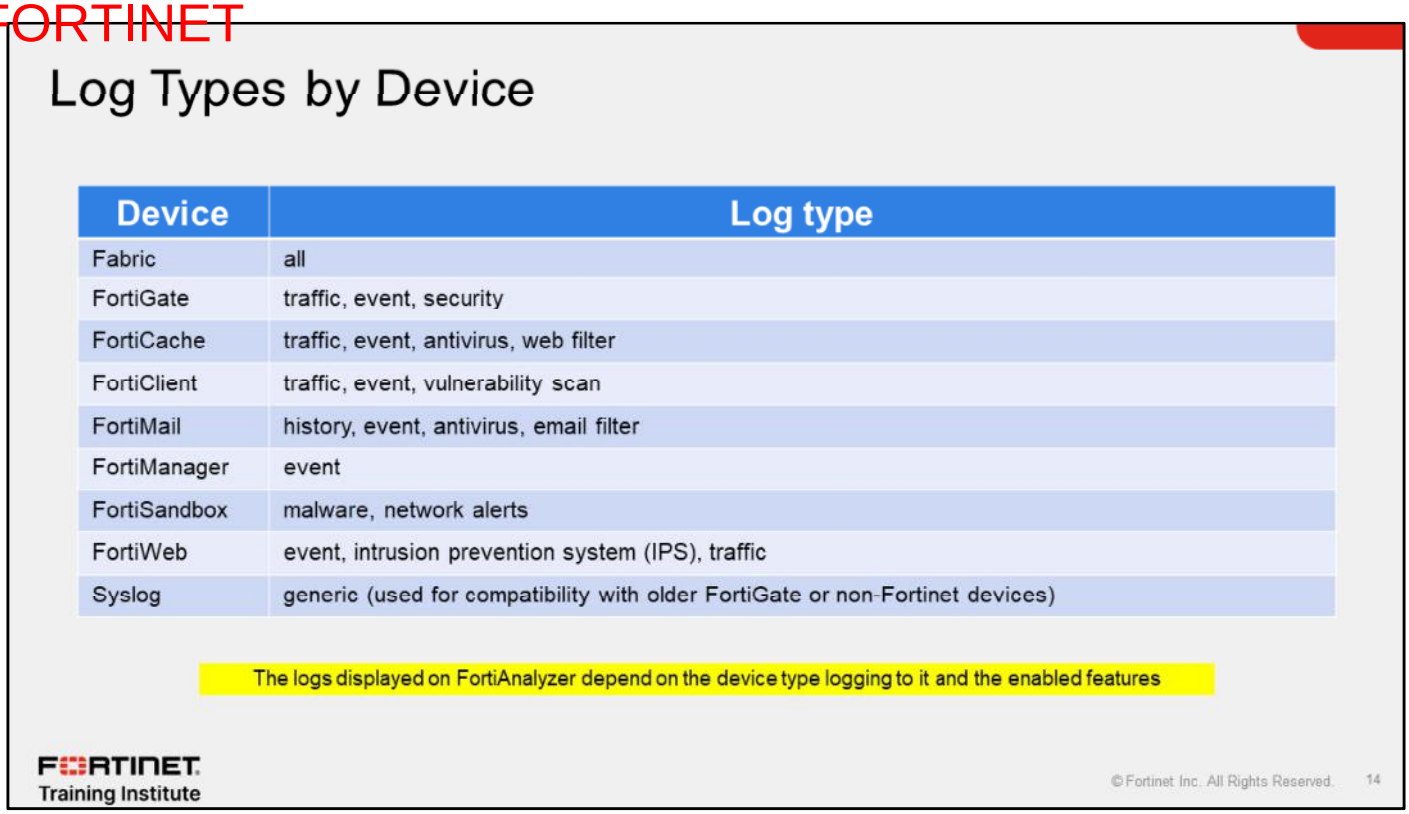
- It is easier to search for a corresponding log on normalized logs than on the actual device logs
- In this example, a search in the **Destination Domain** normalized field will look at the domain and hostname fields of the FortiGate log message



FORTINET Training Institute

 13

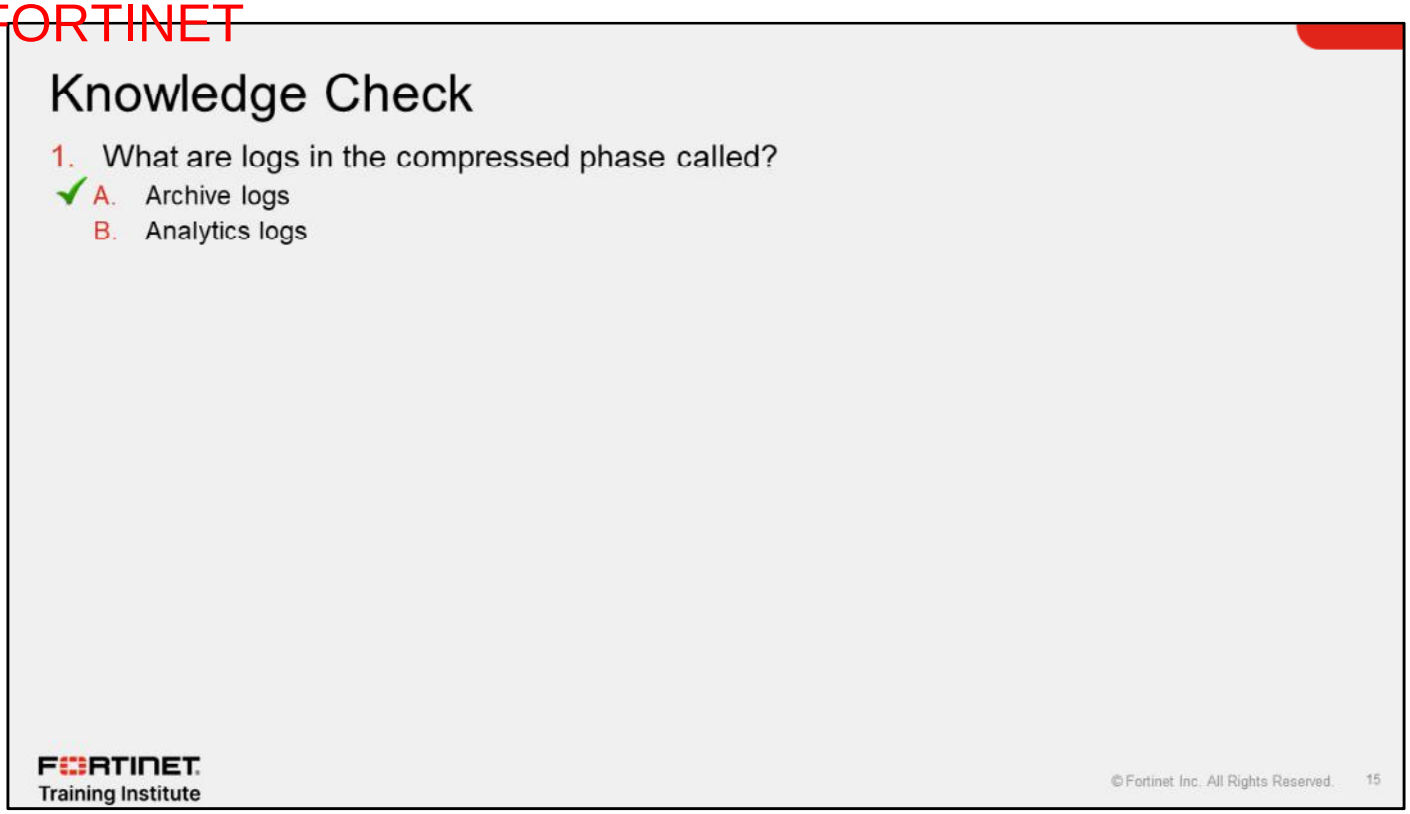
Searching for logs using normalized fields is more efficient than sifting through raw, device-specific logs. Native device logs use inconsistent field names and varying structures, which makes recalling or discovering relevant parameters challenging and time-consuming. When FortiAnalyzer parsers standardize and map these diverse fields into a unified format, you can execute consistent, targeted queries, which streamlines investigations.

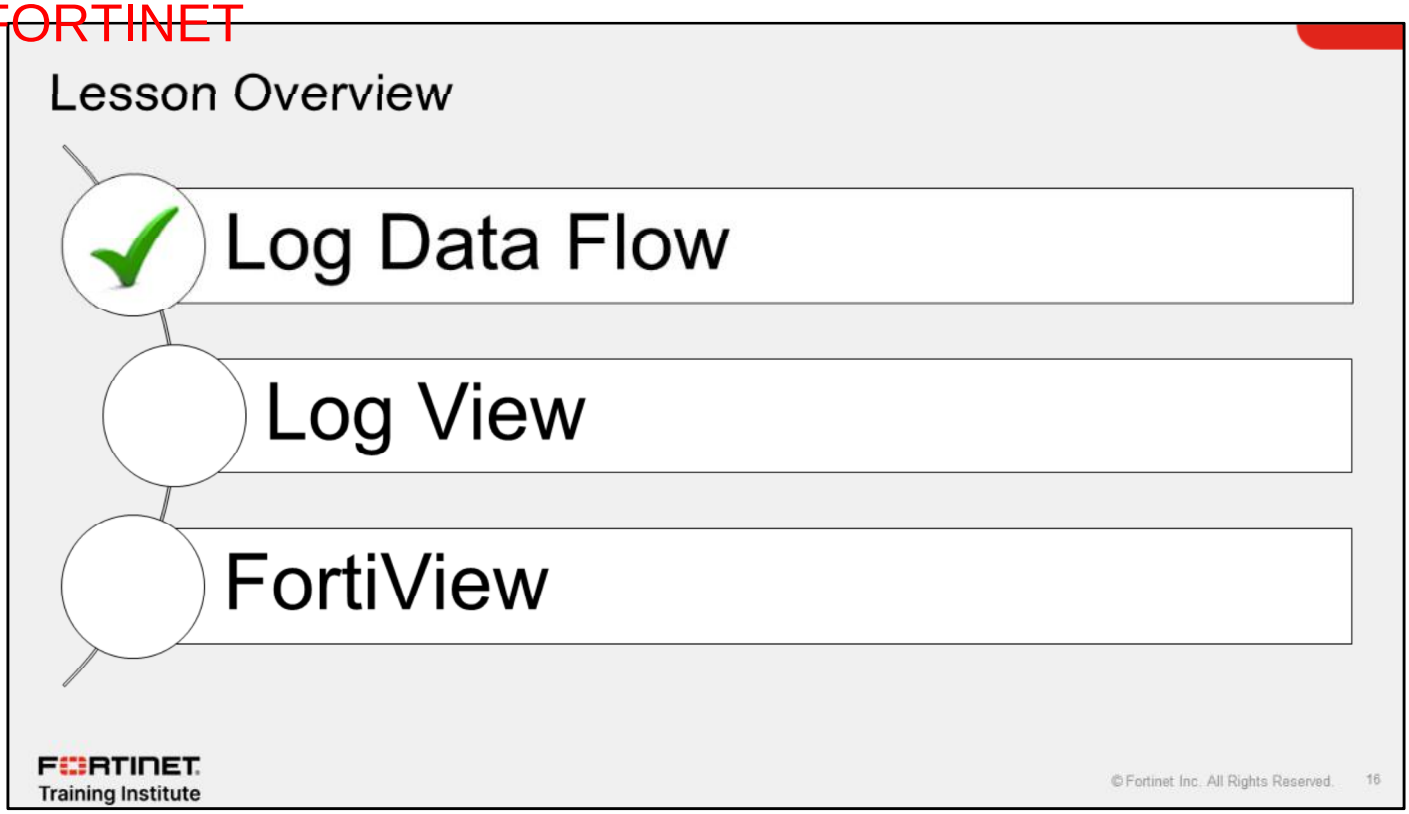


To analyze and interpret logs, you must understand the different log types and the information they contain, as well as which logs FortiAnalyzer collects from each supported device.

The logs displayed on FortiAnalyzer are dependent on the device type logging to it and the features you enabled. For example, FortiGate devices generate three log types: traffic logs, event logs, and security logs. Each log type has corresponding log subtypes.

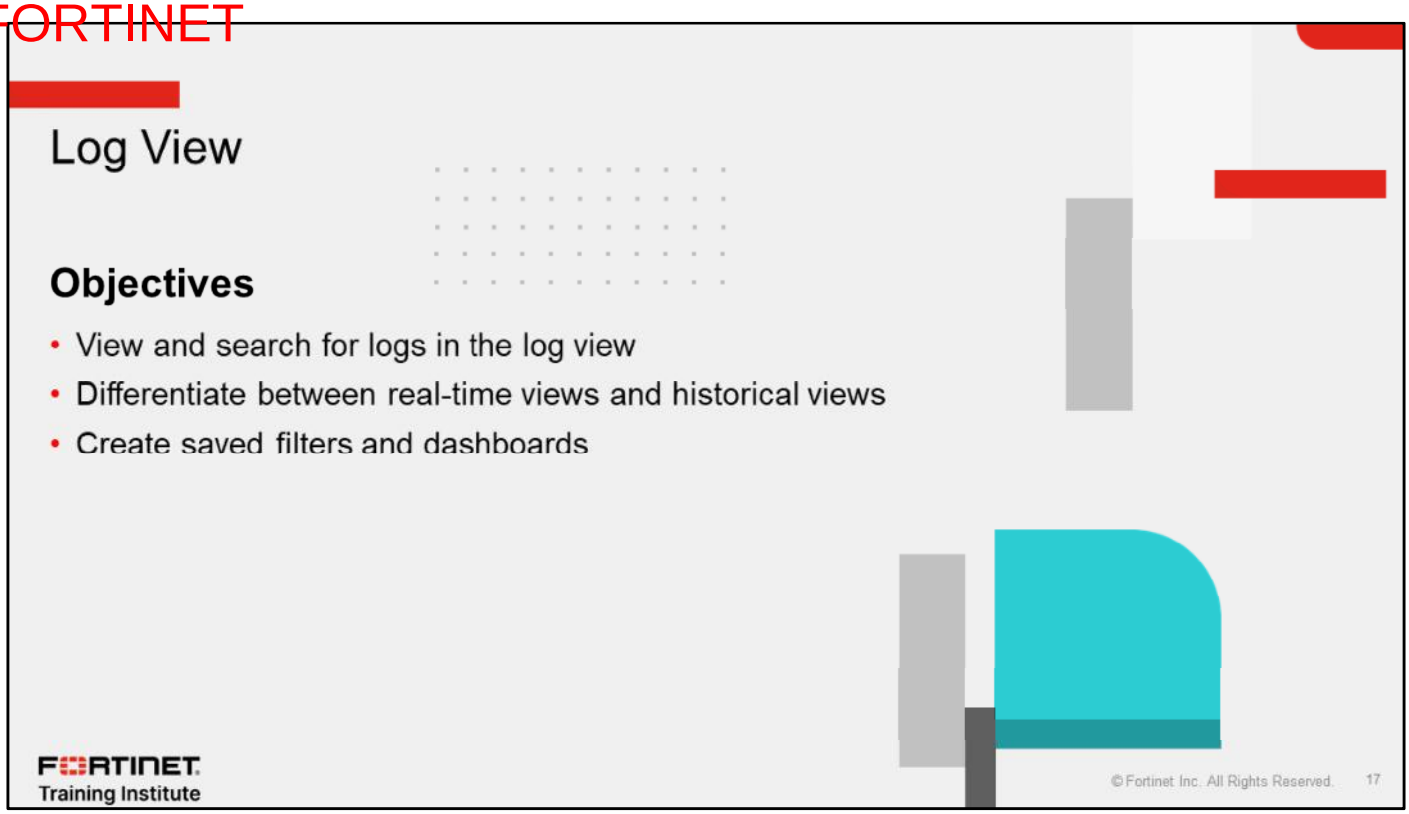
This table lists the log types and subtypes FortiAnalyzer collects from some supported devices. For the complete list, refer to the *FortiAnalyzer Administration Guide*.





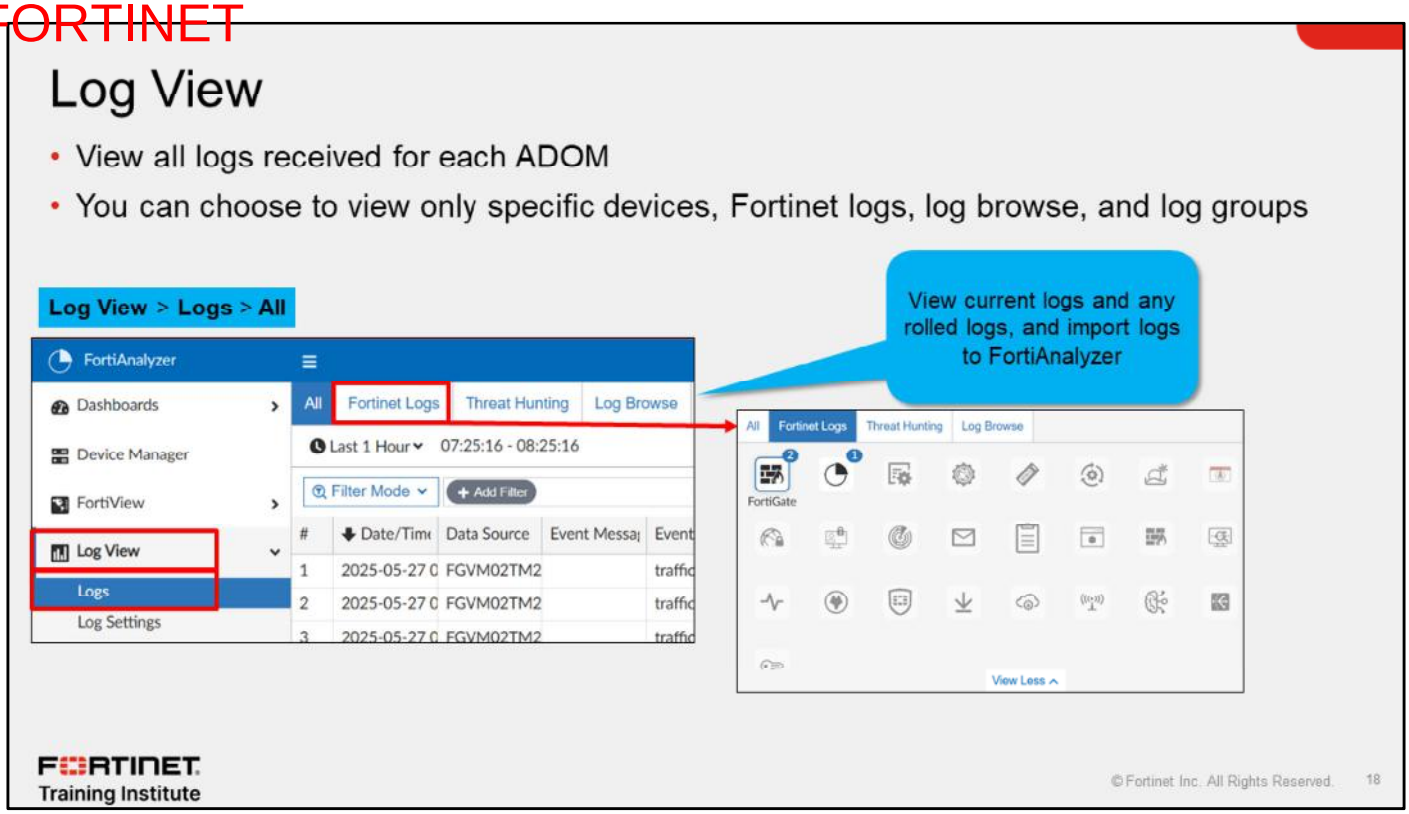
Good job! You now understand log data flow.

Now, you will learn about ways to navigate the FortiAnalyzer GUI to view and search your logs on FortiAnalyzer.



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

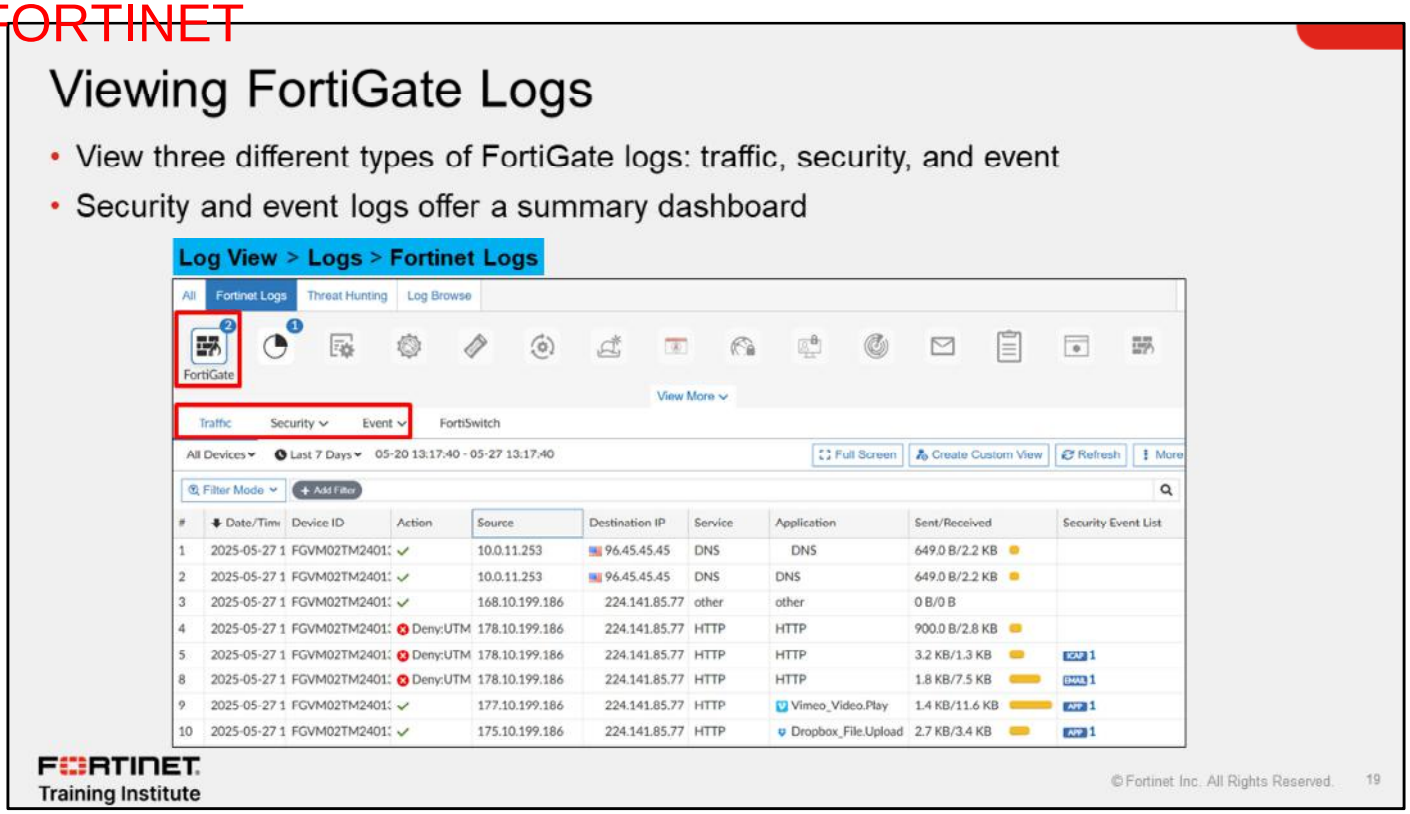
By demonstrating competence in viewing logs, log summaries, and dashboards, you will be able to find and view a variety of log-related information.



The log view allows you to view all log types received by FortiAnalyzer in normalized log format. When you enable ADOMs, the logging information for each ADOM is displayed.

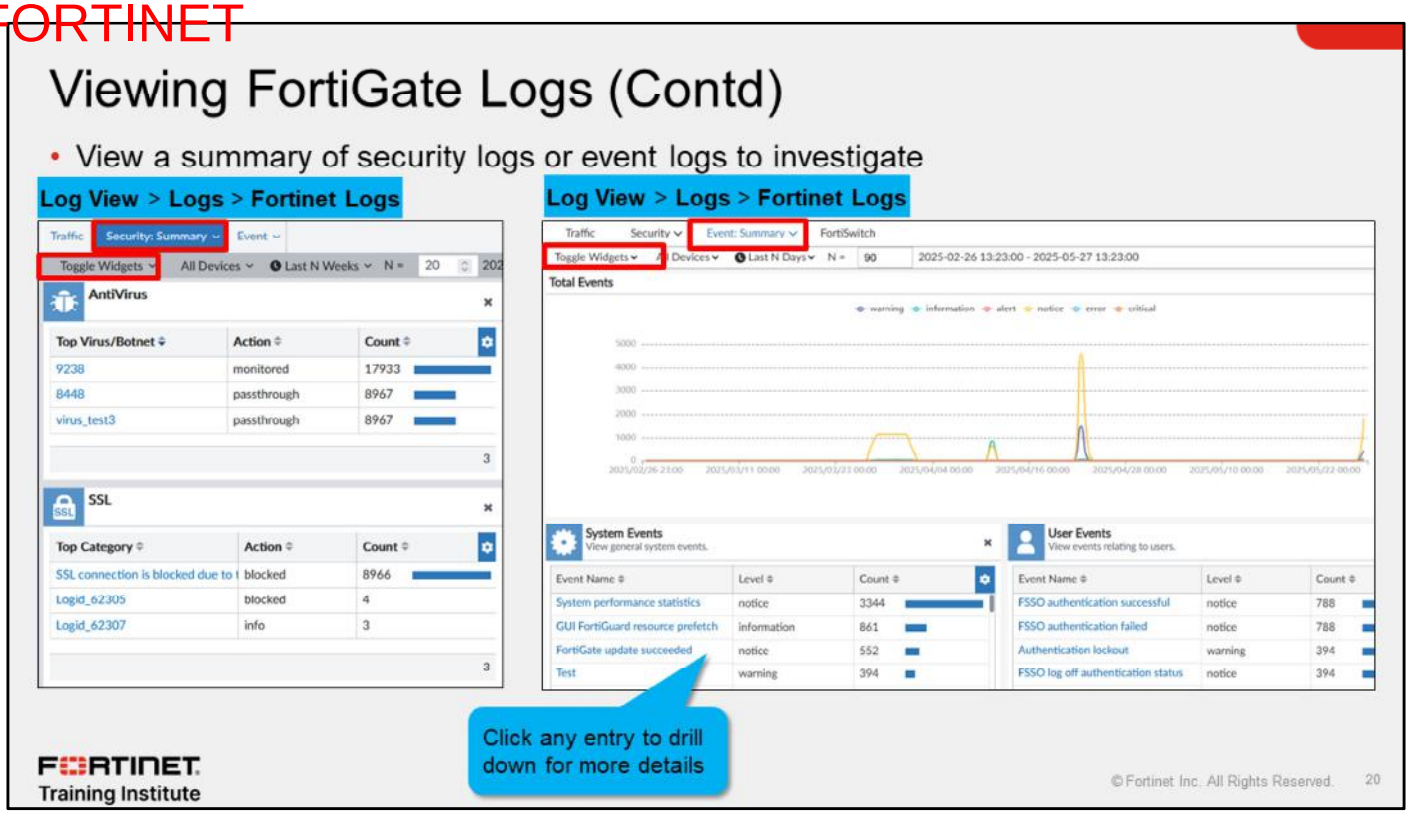
You can choose to view logs from specific devices, Fabric groups, or log groups. A log group is a group of devices placed together in a single logical object. Log groups are virtual, so they don't have SQL databases or occupy additional disk space. You can view logs generated by FortiAnalyzer, the current log files, and any rolled log files. You can also import logs from other FortiAnalyzer devices.

The options available in the log view vary, depending on the type of ADOM you create. In the example shown on this slide, the ADOM type is Fabric.



Traffic logs allow you to see the traffic traversing the firewalls, including details such as source, destination, service, action (whether the traffic is allowed), and more. Security logs allow you to view logs related to unified threat management (UTM) inspection. Event logs are generally related to firewall system operations.

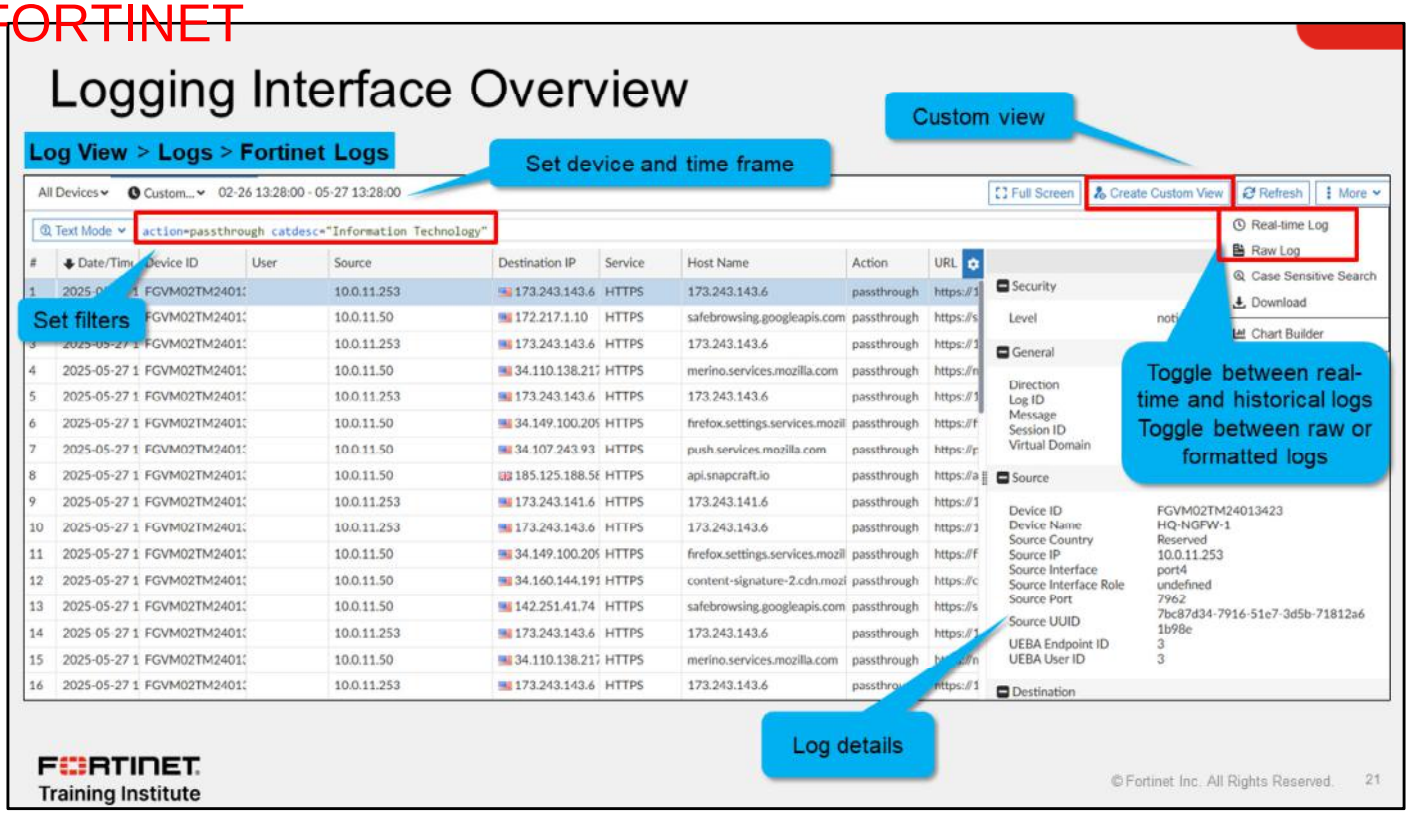
You can select the security or event log subtype you want to see or access a summary dashboard for an overview.



You can monitor all enabled security and event log types from their respective summary dashboards. Summary dashboards use multiple widgets to display the top logs for each subtype. You can add or remove widgets as needed.

The time filter set at the dashboard level affects the information included on all widgets simultaneously, so you must ensure that it is set correctly.

You can click the links in provided in summary dashboards to go to specific logs. Doing so takes you to the specific log subtype section with the appropriate filters applied to search for the specific log entries.

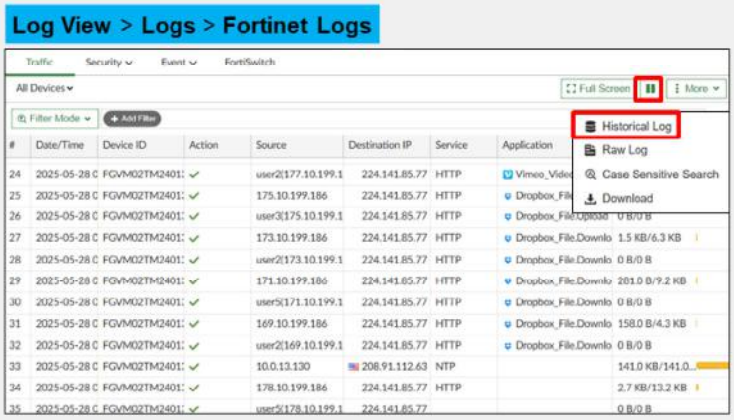


As a SOC analyst, you will frequently need to search through many logs. FortiAnalyzer makes it very easy to search based on any of the fields included in the logs.

To search for specific logs, you select the device and log type and then set the appropriate filters. You can create filters based on any available value, 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, view logs in real time or historically, or view logs as raw or formatted logs. To view more information about a log, double-click the log entry.

Real Time vs. Historical Log Views

- View historical logs with the option to specify a time period
- By default, historical logs are displayed
- When viewing logs in real time, you can pause the view to get a more detailed view of the logs

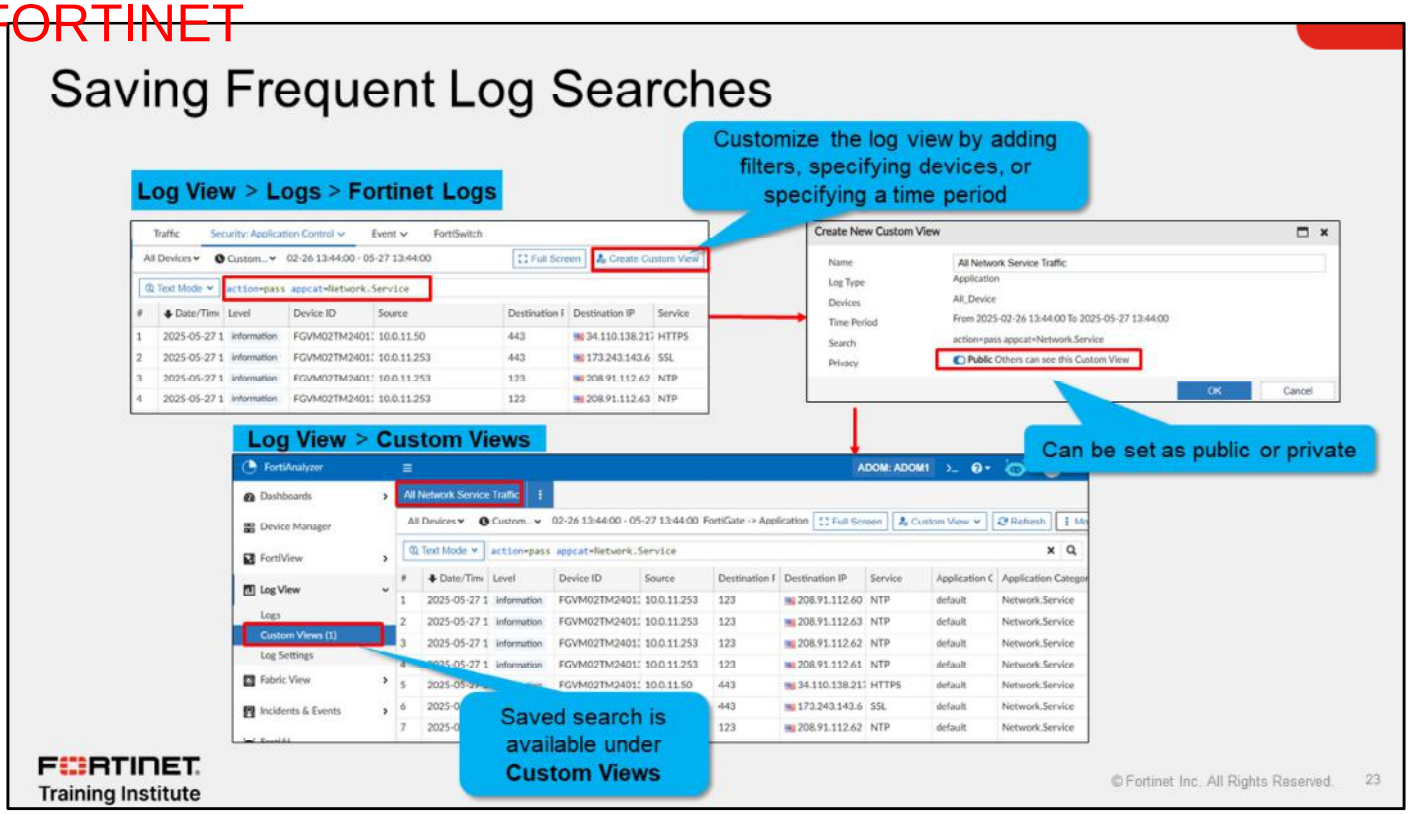


FORTINET Training Institute

 22

You can view historical logs with the option to specify a time period. By default, historical logs are displayed. You must be using the historical log view to use the custom view or chart builder features.

You can switch from viewing historical logs to viewing logs in real time. When viewing logs in real time, you can pause the display to get a more detailed view.



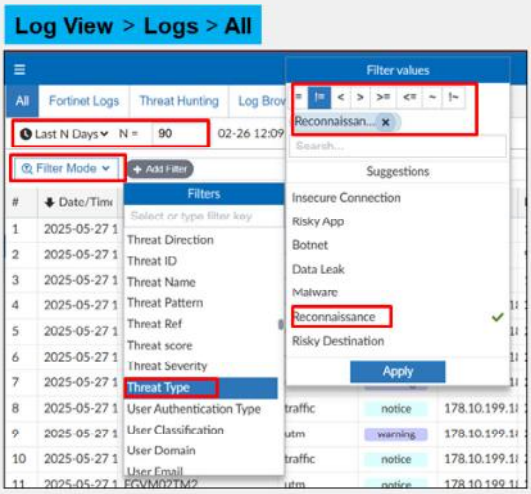
FortiAnalyzer allows you to save searches and build a custom view that you can go to directly whenever you are looking for logs using specific search parameters. This feature is very useful when you are performing a specific search frequently and repeatedly. You can set custom views as public or private. Public custom views can be viewed by all administrators, whereas private custom views can be viewed by only the creator of that view. Users cannot make changes to custom views created by other administrators but can save a copy.

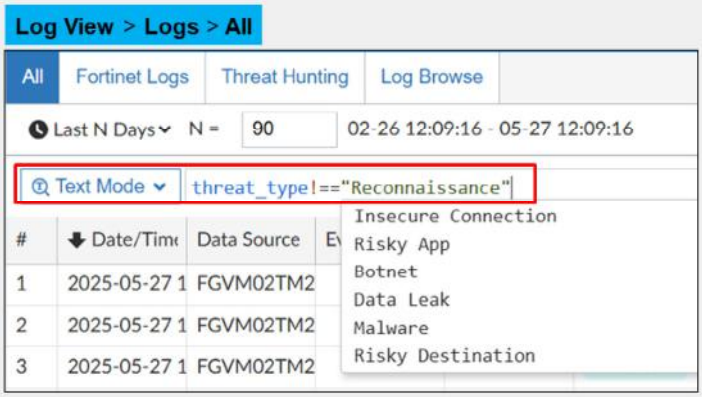
To create a custom view, you will need to add filters, specify a device, specify a time period, and give a name to the view. FortiAnalyzer pulls the time period and search filters that you specify. Custom views are available on the GUI.

This slide shows a custom view that includes all network service traffic logs received over the last 90 days.

Searching Logs

- Filter mode allows you to define your search criteria using the GUI
- Text mode allows you to type in your filter and conditions manually, or select a filter from history





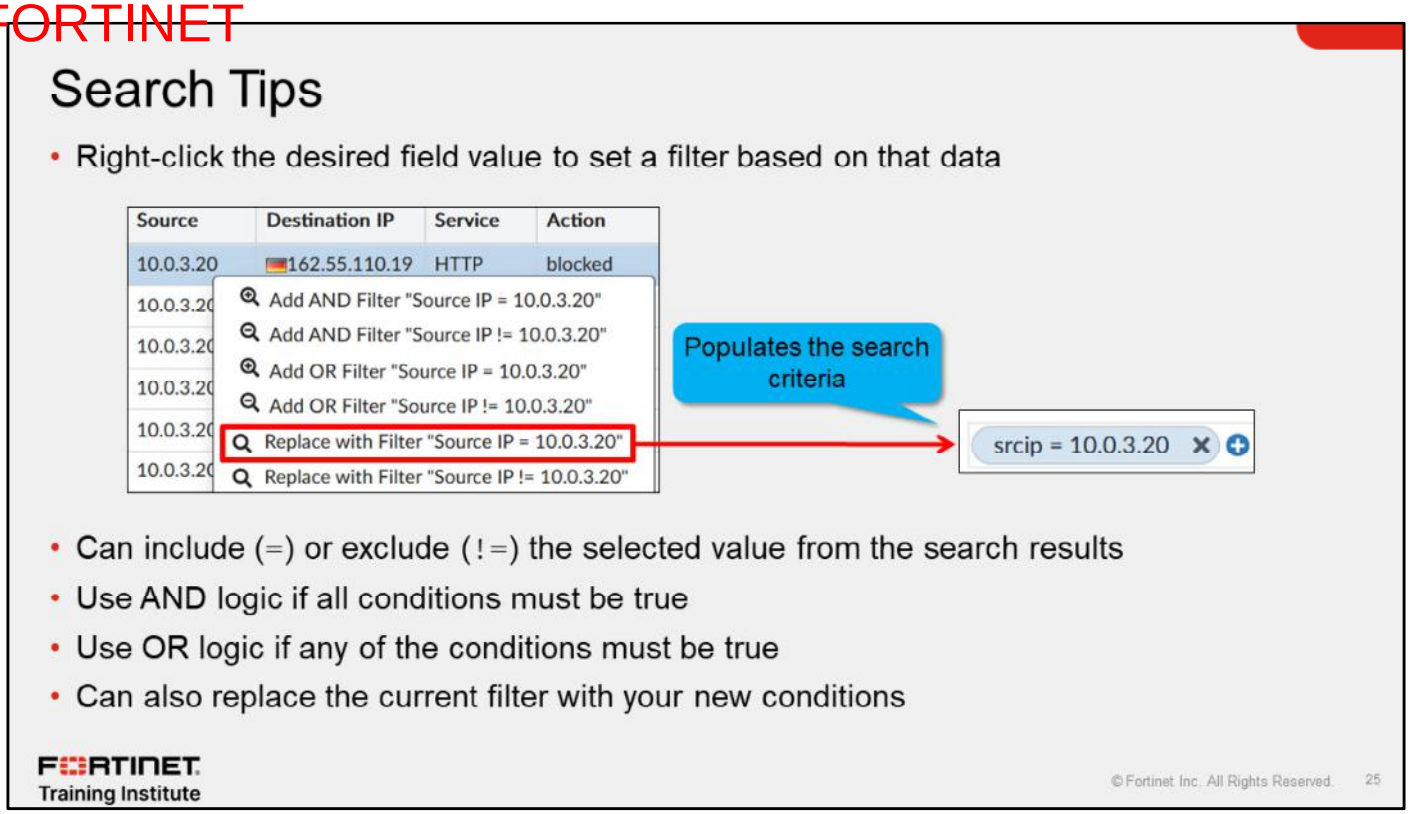
FORTINET Training Institute

 24

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

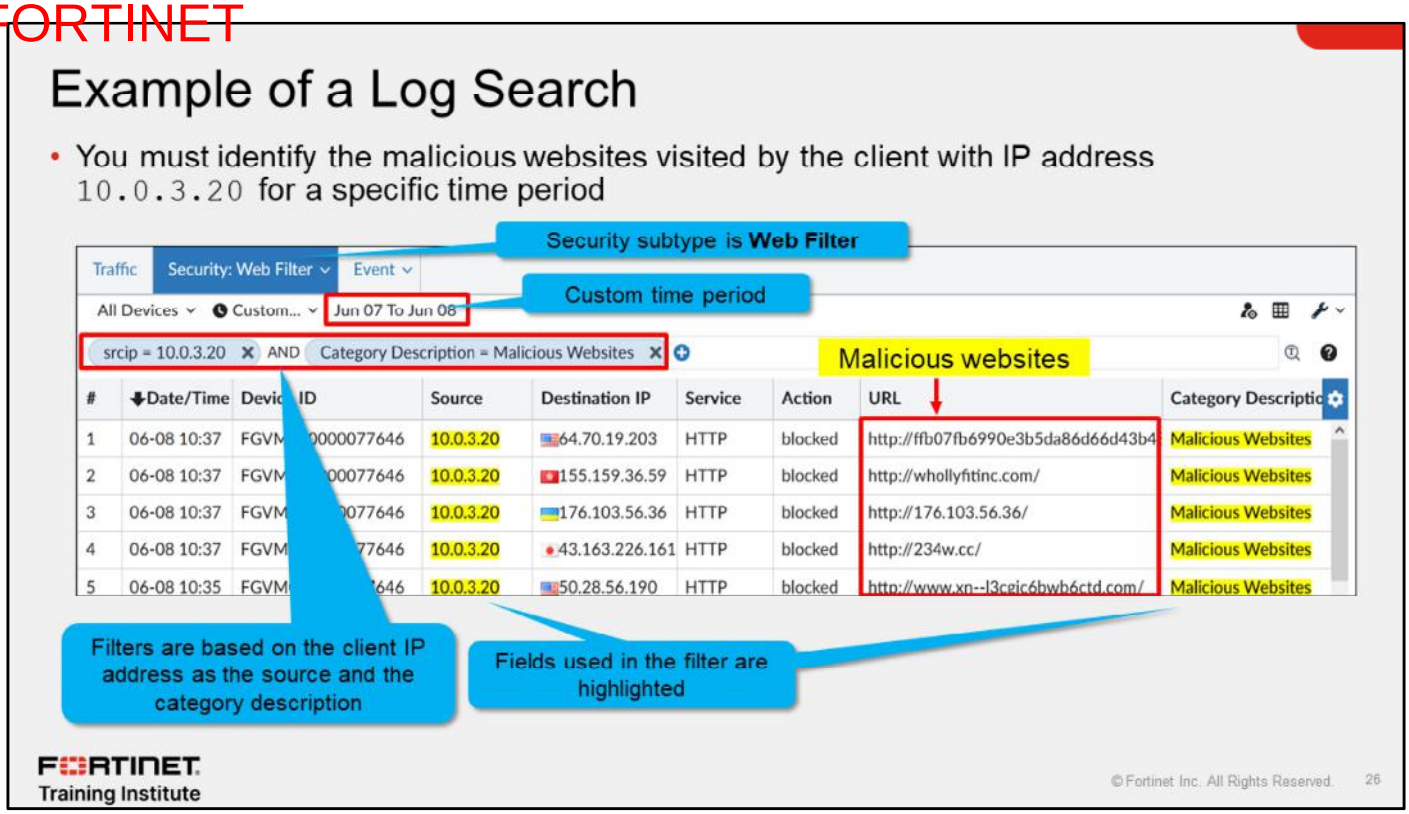
There are two modes you can use when you search for logs in the log view:
- Filter mode allows you to define your search criteria using the GUI.
- Text mode allows you to type in your filter and conditions or pick a filter from history.

Typing in filters manually is prone to syntax errors and spelling mistakes. Using the context menus in the GUI prevents you from making those mistakes.



Another useful tip is to right-click any field in the log entries to add the value to the filter. First, find a log in the log table that includes the data 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, and you can inject that value into the filter.

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

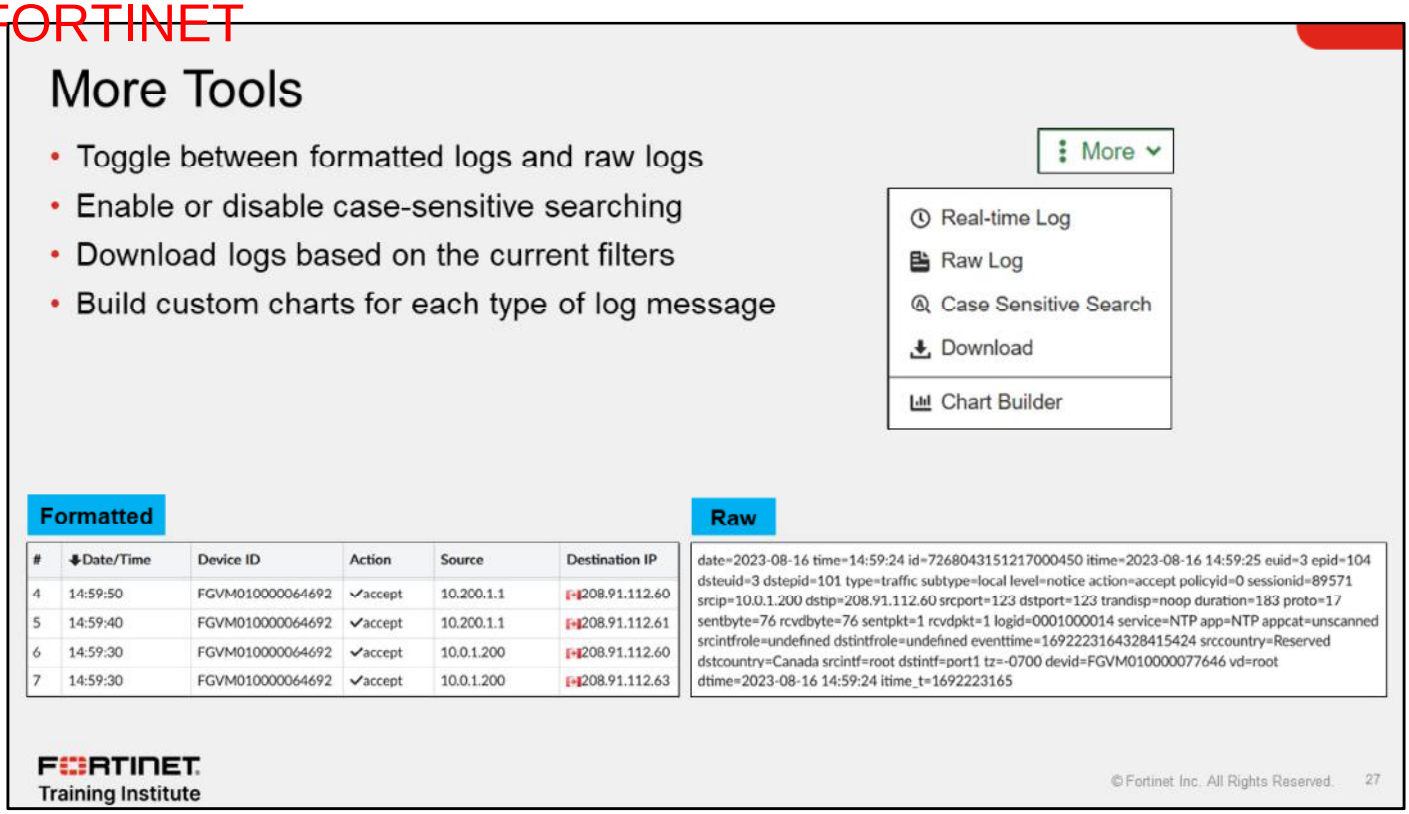


This slide shows an example of a filter applied in the log view. You can easily add a filter by right-clicking the desired log field and selecting whether you want that value included or excluded from the logs displayed.

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 add more filters or edit the current filters.

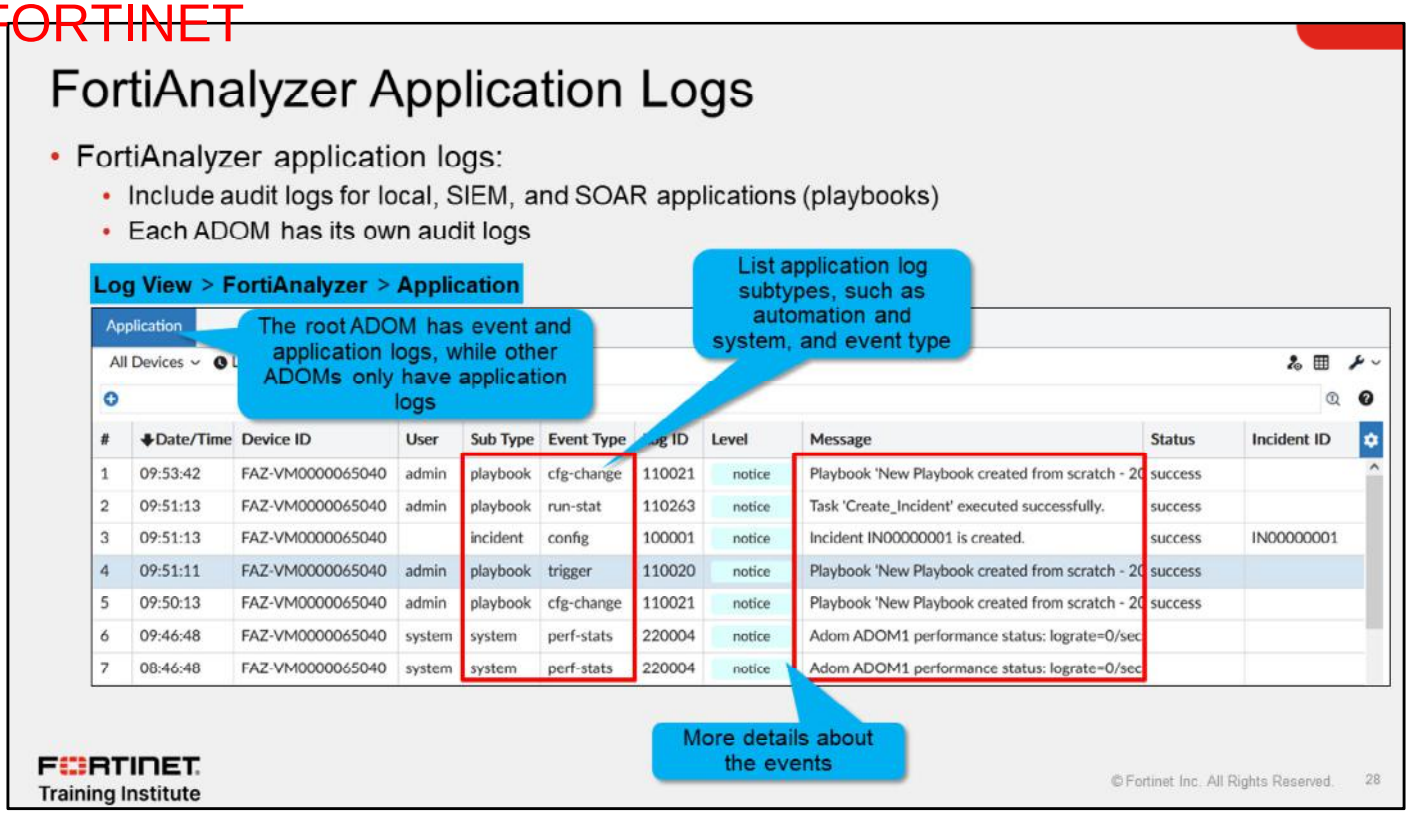


The FortiAnalyzer GUI provides options for viewing, searching, and downloading logs.

You can toggle between viewing formatted and raw logs. 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 provide syntax guidance. For example, there may be instances where you need to look up fields and values to use in text filters when configuring handlers.

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

You also use the chart builder feature to build custom charts for each type of log message.



FortiAnalyzer applications, such as incident management, logging events, and automation playbooks, generate local audit logs accessible in **Log View** under each ADOM.

Administrators can view both local event logs and application logs in the root ADOM. FortiAnalyzer event logs show system-wide information, whereas application logs are ADOM-specific. Non-root ADOMs show only application logs.

On this slide, you can see several logs that show that multiple automation tasks have succeeded. You also see the log rates of ADOM1.

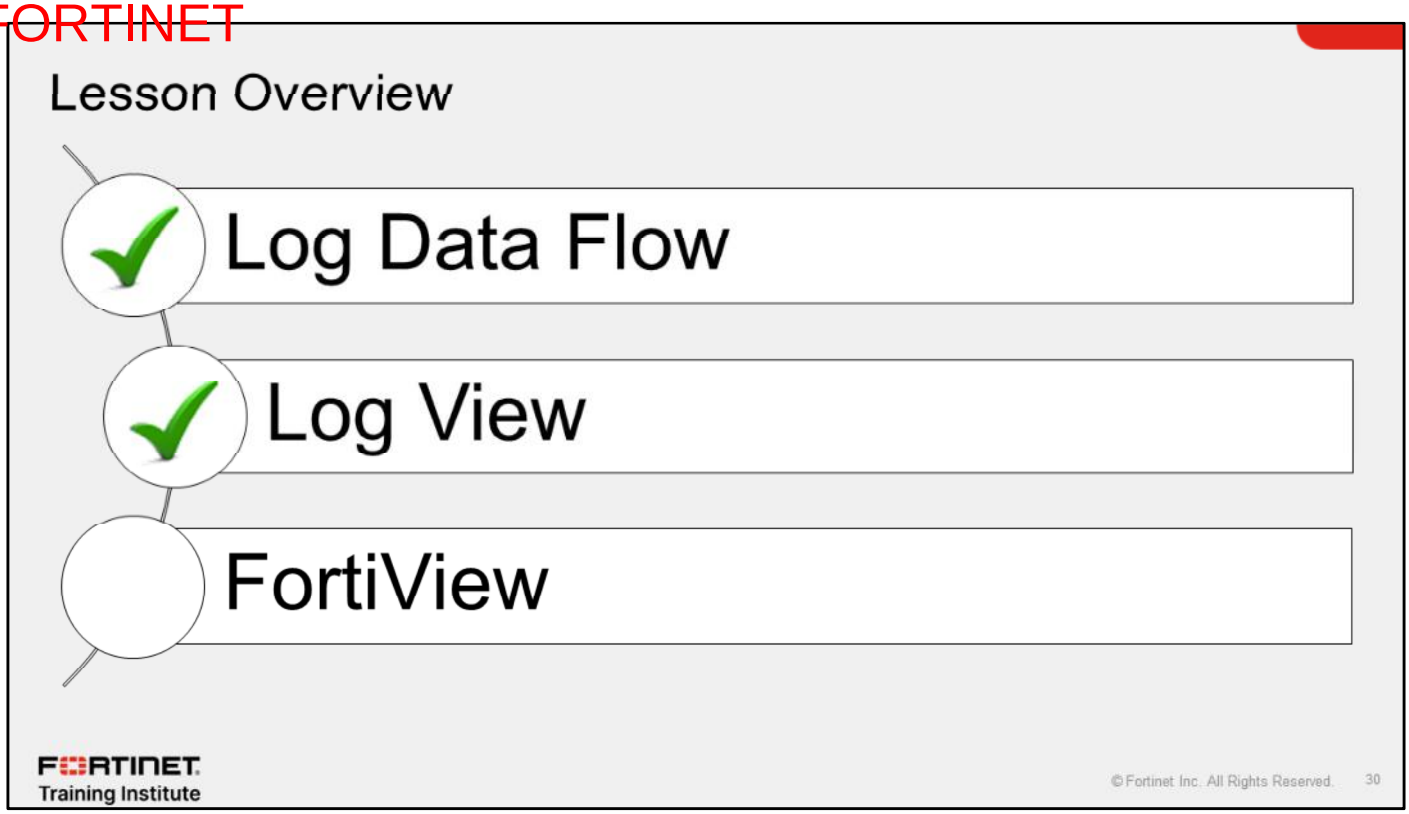
Knowledge Check

1. Which log view includes the chart builder feature?
   A. Real-time
   ✓ B. Historical

2. Saved searches appear under which log view?
   A. Logs
   ✓ B. Custom views

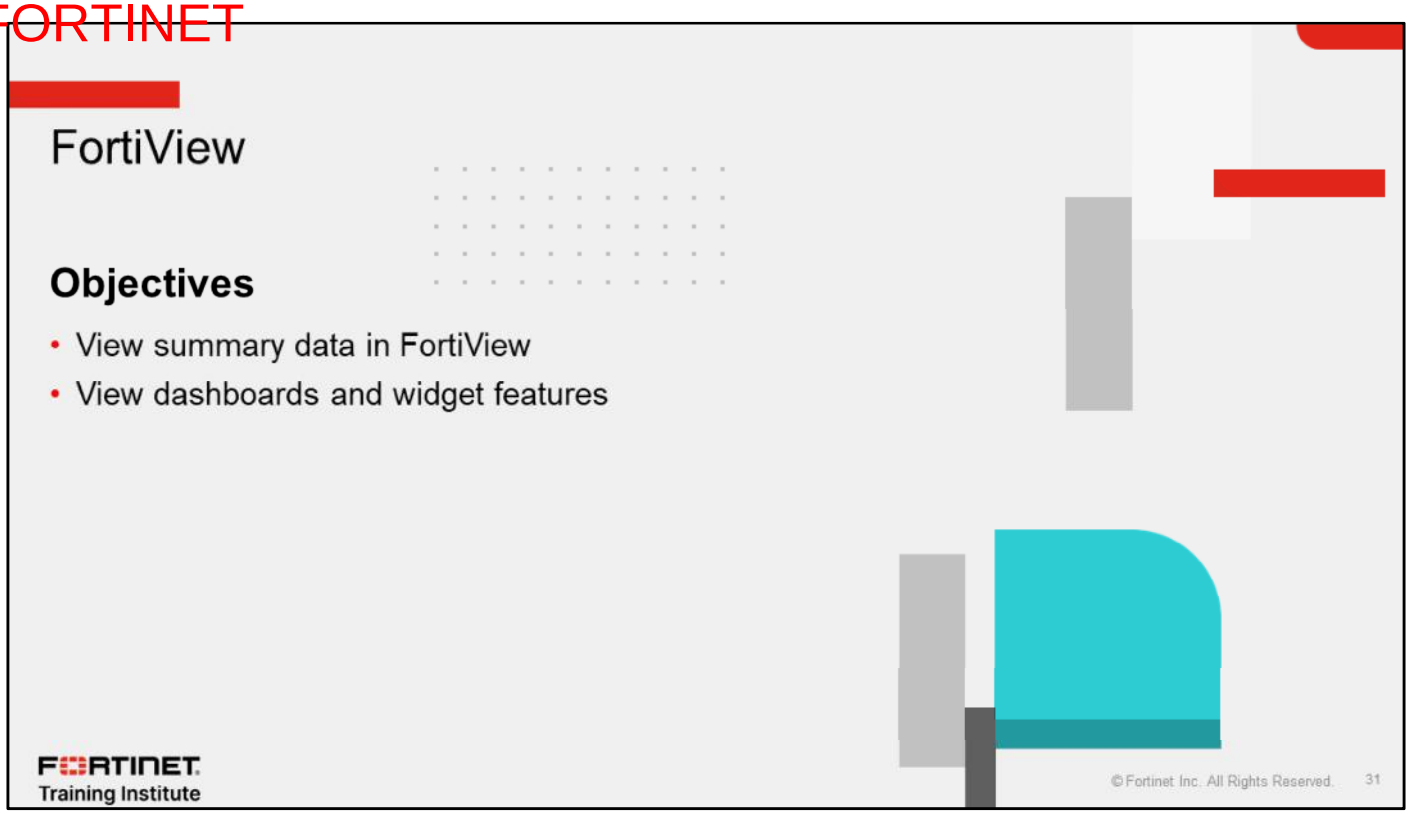
FORTINET Training Institute

 29



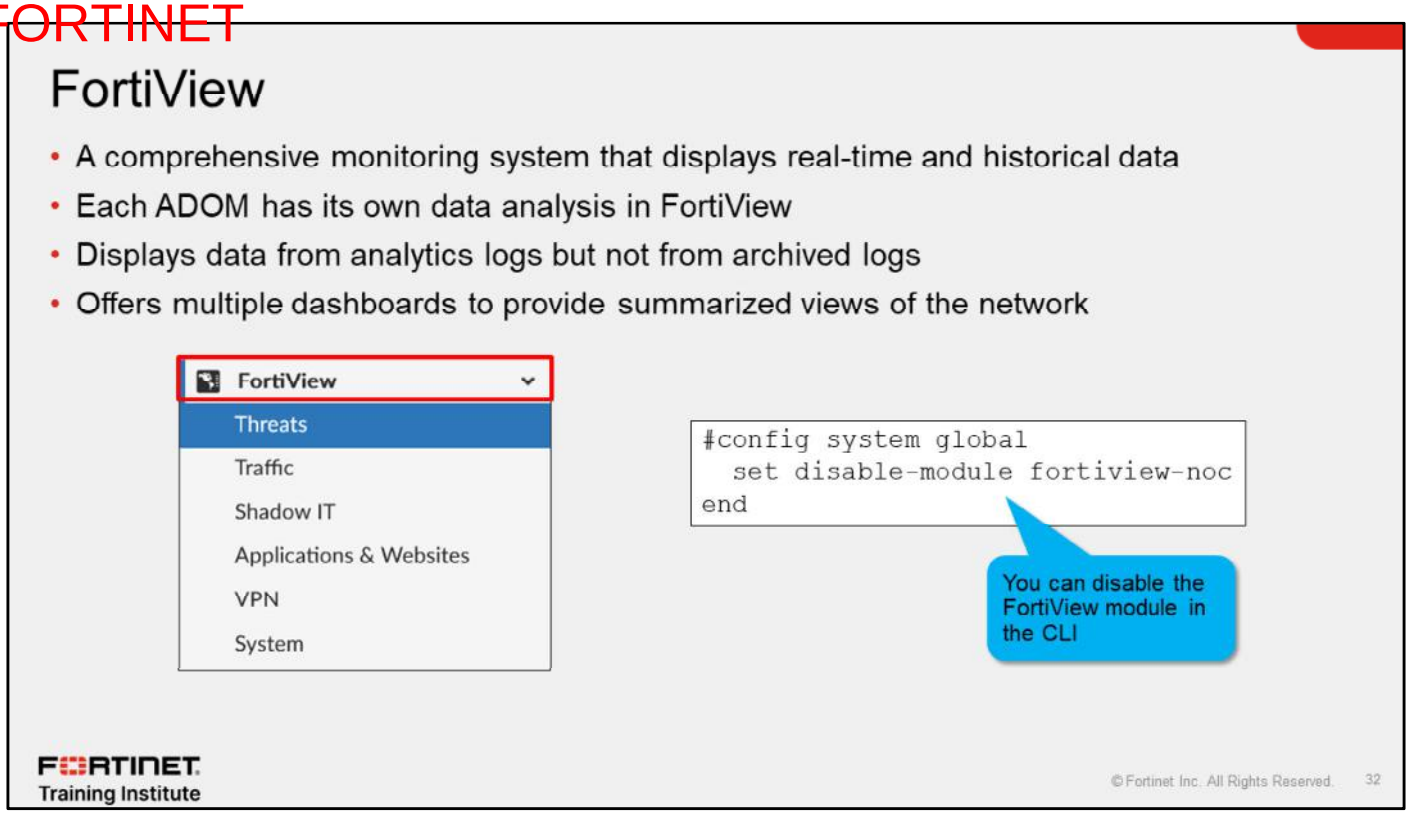
Good job! You now understand log view navigation.

Now, you will learn how to view summary data and widgets in FortiView.



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

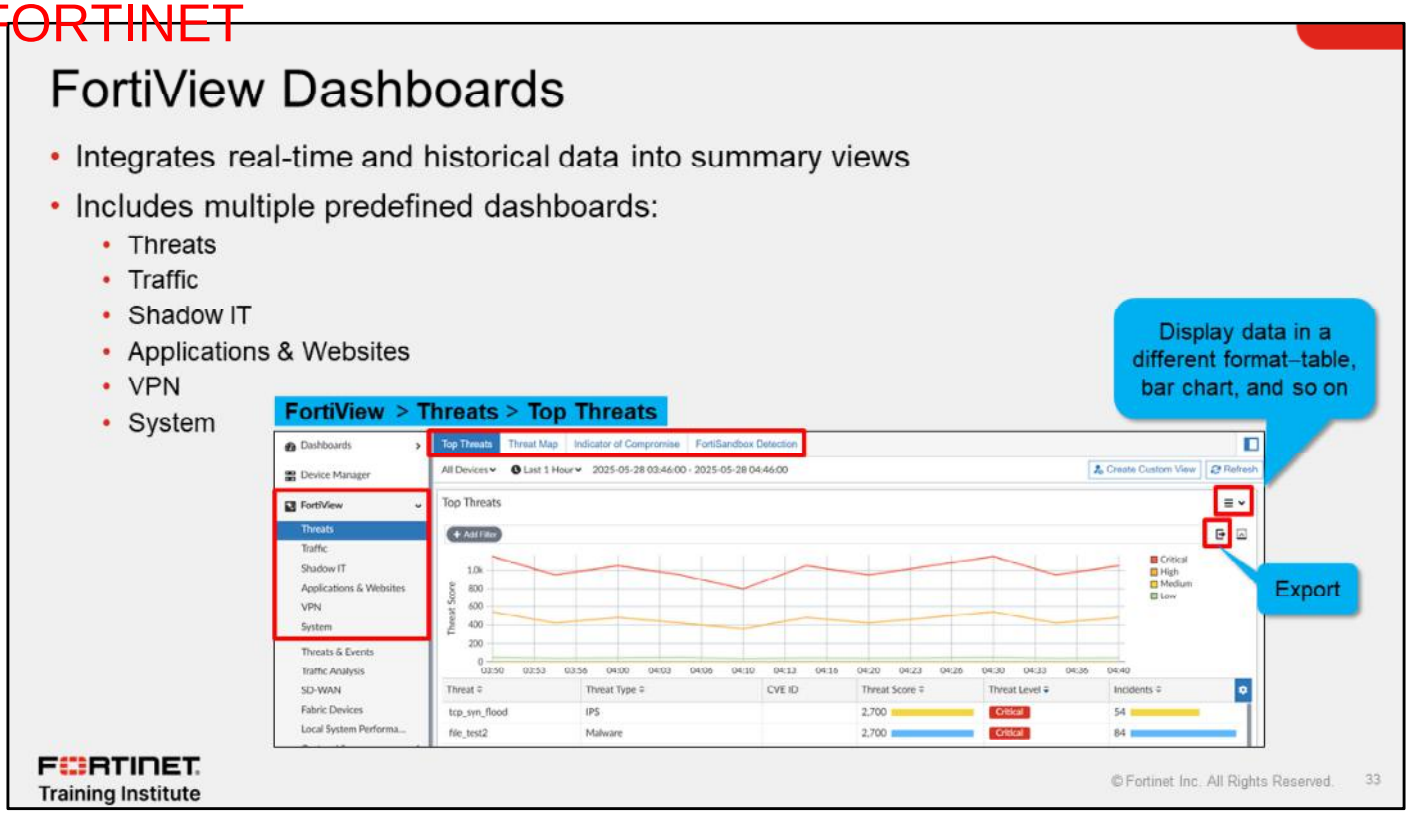
By demonstrating competence in viewing logs, log summaries, and dashboards, you will be able to find and view a variety information related to logs.



FortiView displays real-time and historical data and offers multiple dashboards to provide a summarized view of the information for your network. FortiView displays data from analytics logs; however, data from archive logs is not displayed in FortiView.

Each ADOM has its own data analysis view in FortiView. When viewing ADOM data, always ensure that you are in the correct ADOM.

You can disable the FortiAnalyzer FortiView module when you need to for performance tuning using the commands shown on this slide. When disabled, the GUI hides FortiView and stops background processing for this feature.

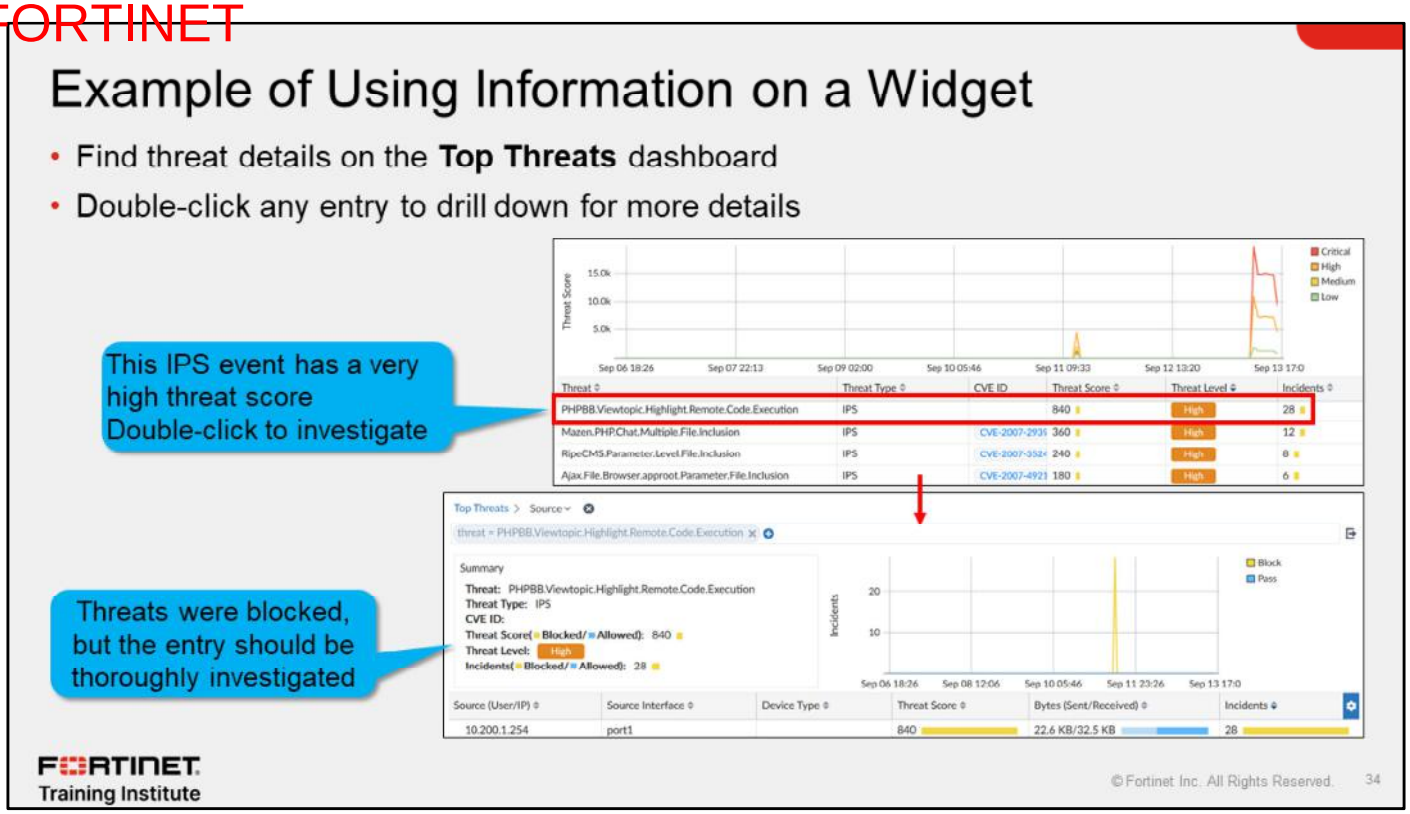


FortiView includes the following predefined dashboards that summarize different aspects of the network:

- **Threats** shows top threats, a global map showing traffic destinations, and more.
- **Traffic** shows the traffic source, destination, policy hits, and more.
- **Shadow IT** shows cloud applications (such as Dropbox and YouTube) and cloud users
- **Applications & Websites** shows the top applications, top domains, top website categories, and top browsing users.
- **VPN** shows SSL and IPsec dial-up users and site-to-site VPN users.
- **System** shows FortiAnalyzer logins, system events, and resource usage.

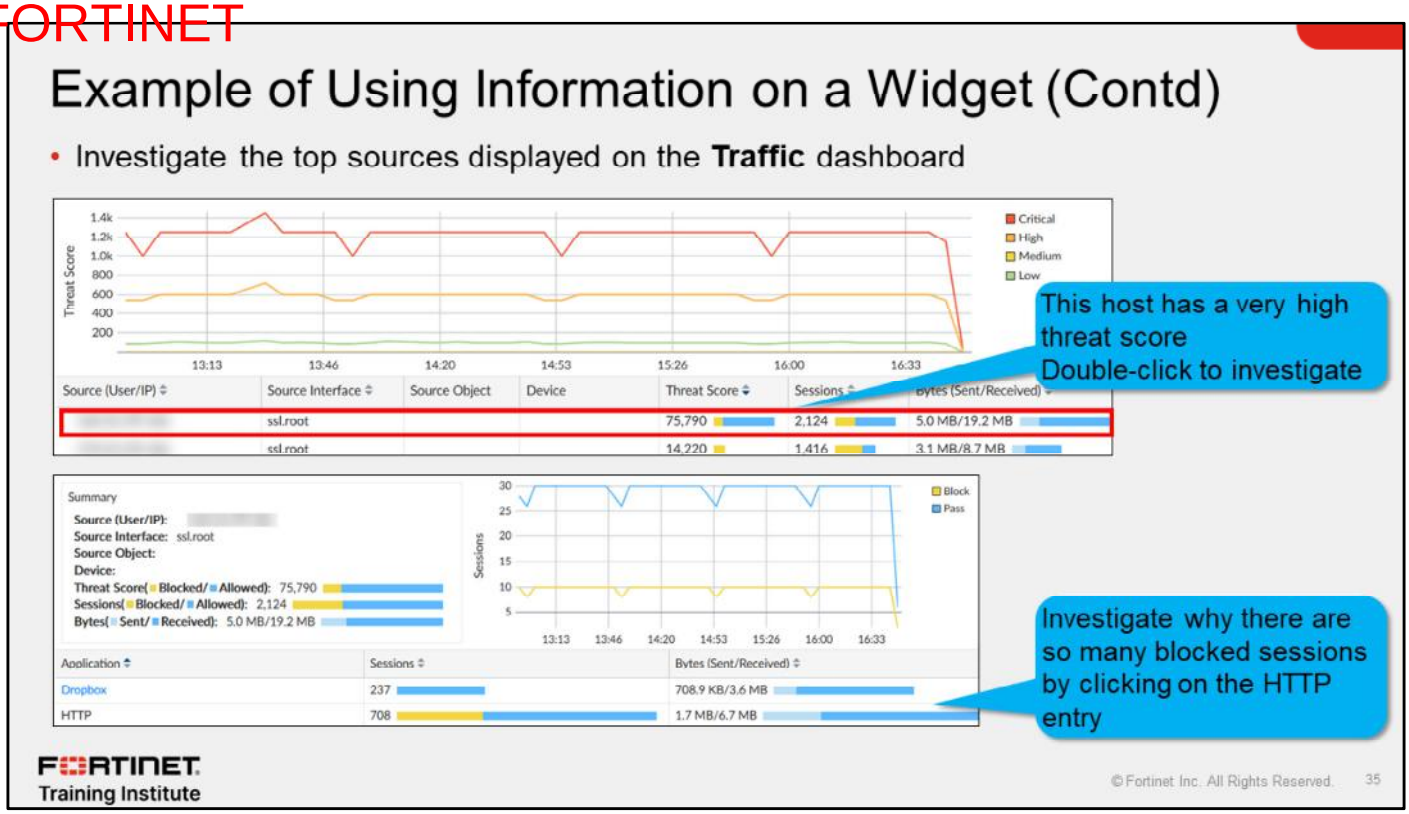
FortiView allows you to use multiple filters, enabling you to narrow your view to a specific time, by user ID or local IP address, by application, and more. You can also use multiple filters to investigate traffic activity, such as user uploads and downloads or videos watched on YouTube, on a network-wide user group or for individual users.

You can also export FortiView information as a PDF file or create a chart to use in reports.



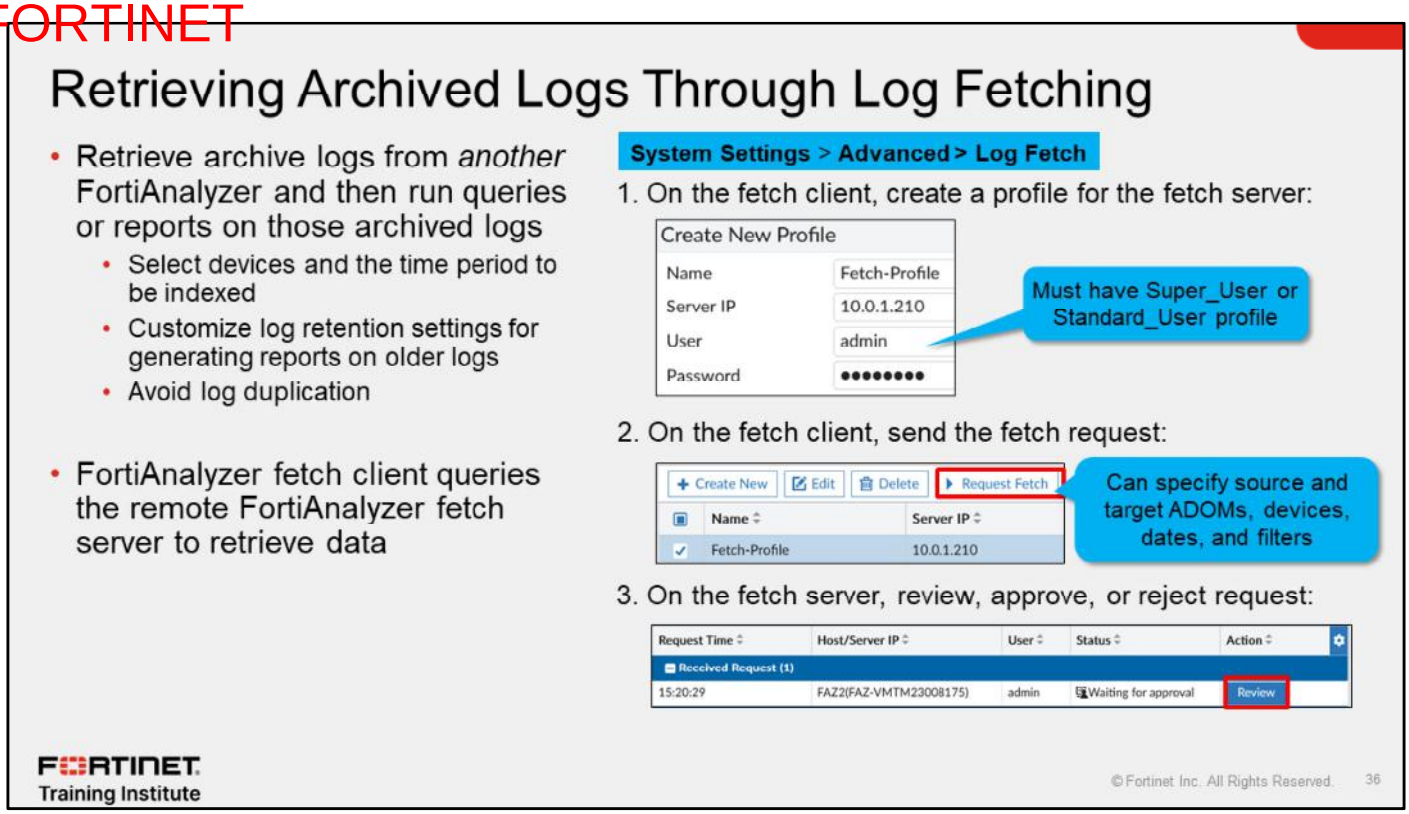
From the information displayed on a widget, you can find more details about a specific entry.

On this slide, the **Top Threats** widget displays the top 100 threats. The threat at the top of the list is an IPS event with a very high threat score. If you double-click that entry, you will see more details, like the source IP addresses related to this traffic. In this example, only one IP address is listed, indicating that this host has likely been compromised, and the analyst should report the findings. The IPS threats listed in the widget also include corresponding common vulnerabilities and exposures (CVE) ID numbers with hyperlinks that you can click to read more about the attack vectors, suggested impact, vulnerable software, and more.



You can use the information displayed on a widget to see more details about a specific entry.

In the example shown on this slide, the **Top Sources** widget was enlarged and customized to display the information in a table format and with full view. The top source on the list is a host that is accessing the network through SSL VPN, with a very high threat score. Double-clicking that host entry will provide more details, like the applications that are generating this traffic. In this example, HTTP is listed as the major source of blocked traffic from that host. More investigation is required to identify if this traffic is normal or if the client is compromised.

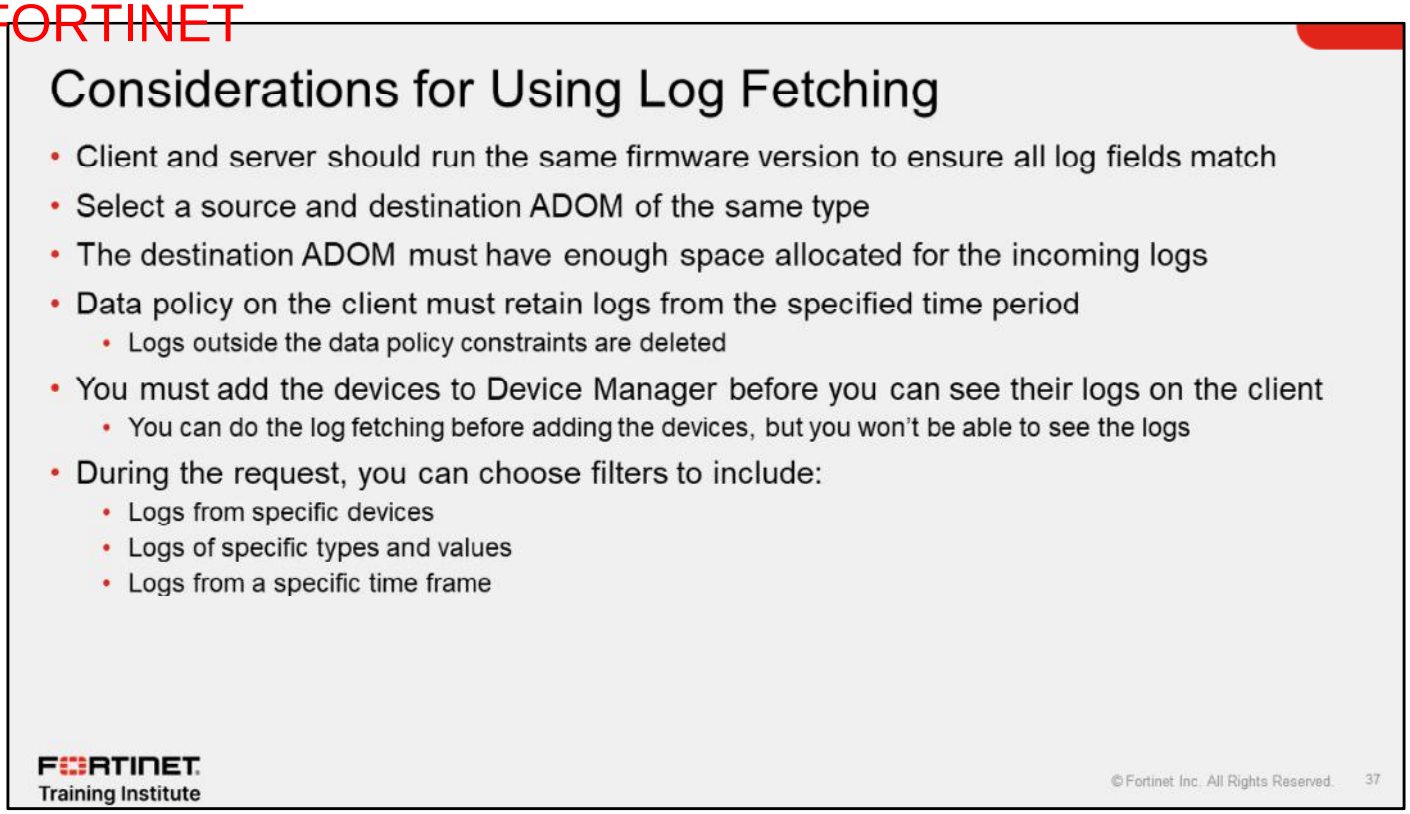


You can use FortiAnalyzer to fetch the archived logs of specified devices from another FortiAnalyzer and index that data. Then, you can run queries or reports for forensic analysis. Log fetching simplifies the generation of reports based on log data by:

- Allowing the administrative user to select the devices and time period to be indexed
- Allowing customized log retention settings for the indexed logs pulled into the ADOM to suit the purpose of report generation based on older logs
- Avoiding log duplication, which can occur during an import from an external backup source

The FortiAnalyzer device that fetches logs operates as the fetch client, and the other FortiAnalyzer device that sends logs operates as the fetch server. Log fetching can happen only between two FortiAnalyzer devices. A FortiAnalyzer device can perform either the fetch server or fetch client role, and it can perform two roles at the same time with different FortiAnalyzer devices at the other end.

You can establish only one log-fetching session at a time between two FortiAnalyzer devices.



There are a few things to consider when using log fetching:

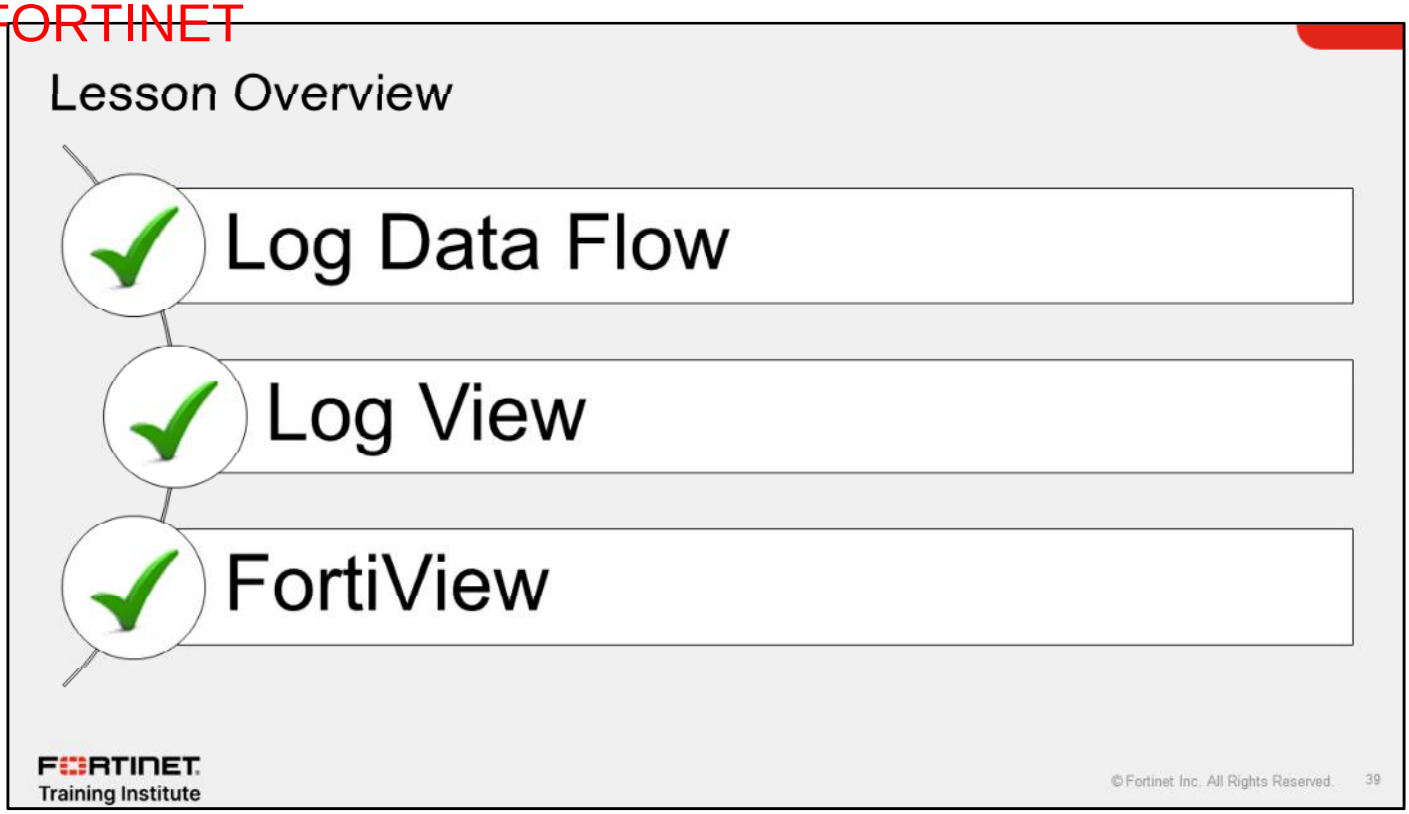
- The client and server devices should be running the same firmware to ensure all log fields match.
- The source and destination ADOMs must be of the same type.
- Ensure the destination ADOM has enough allocated space for the incoming logs.
- Verify the data policy on the client will not delete the incoming logs because they fall outside of the configured time frame.
- The incoming logs will be visible on the client only if the corresponding devices are added to Device Manager.
- Select only the required logs using the available filters in the request window.

Knowledge Check

1. Which logs does FortiAnalyzer use to populate FortiView data?
   - A. Archive logs
   - ✓ B. Analytics logs

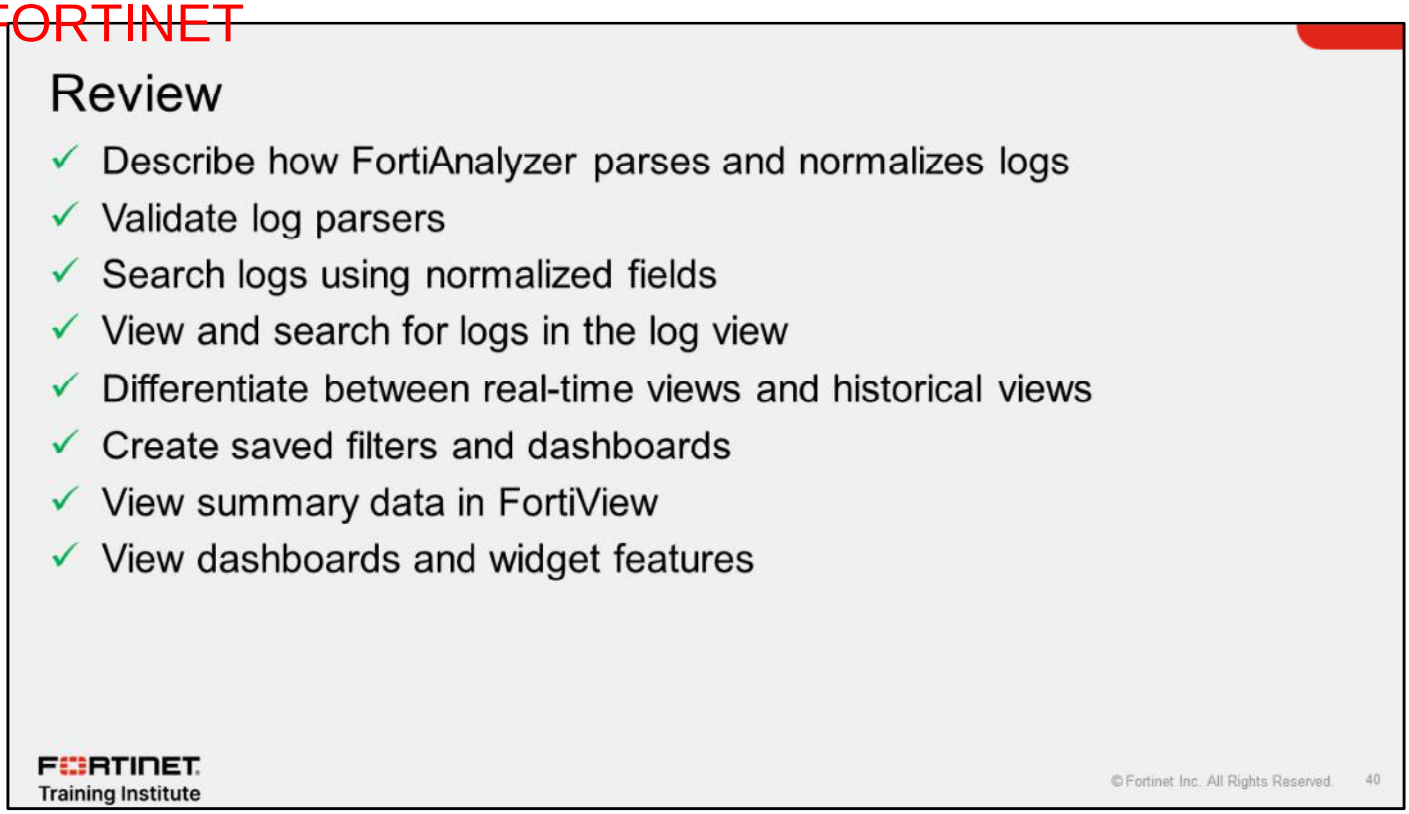
FORTINET Training Institute

 38



Congratulations! You have completed this lesson.

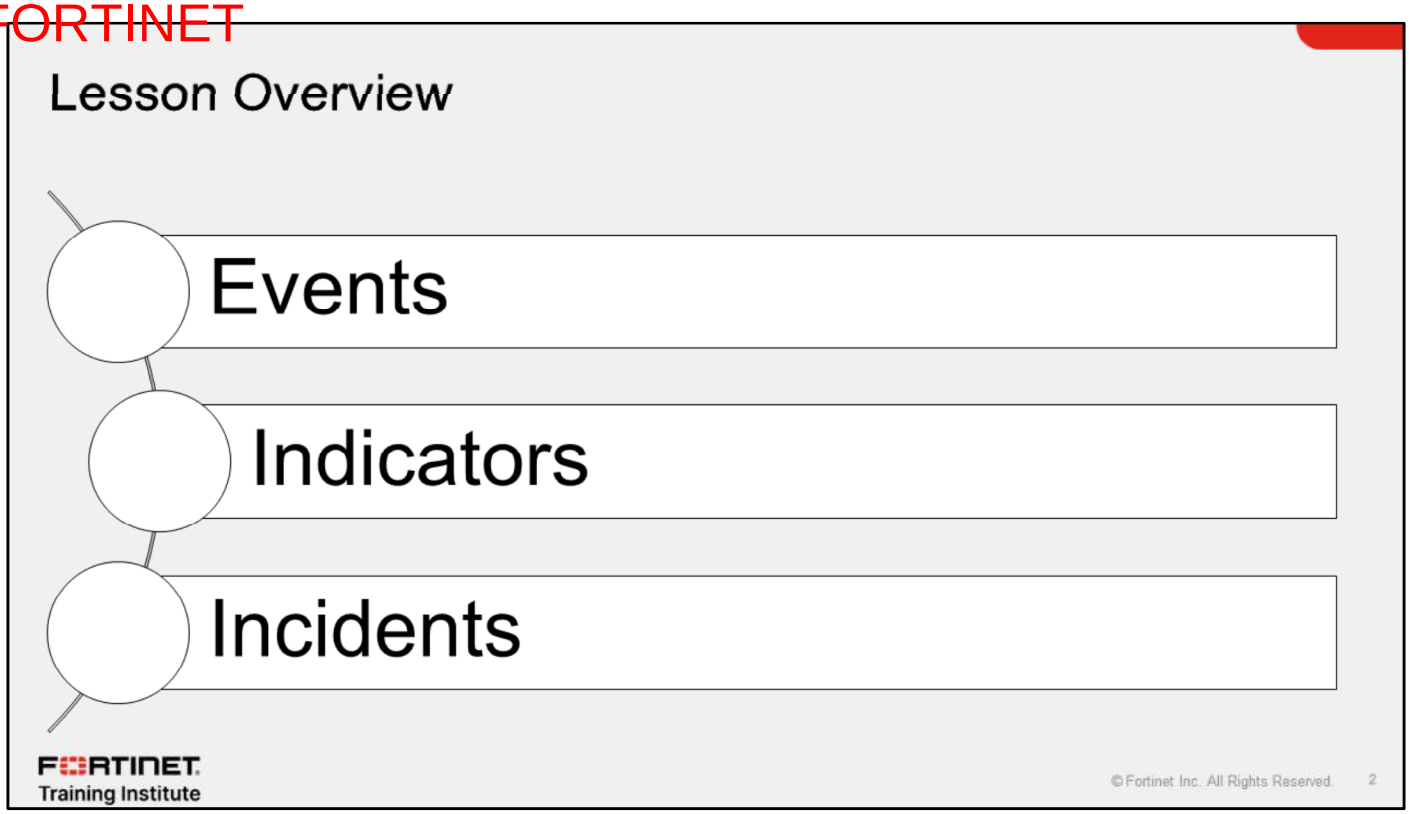
Now, you will review the objectives that you covered in this lesson.



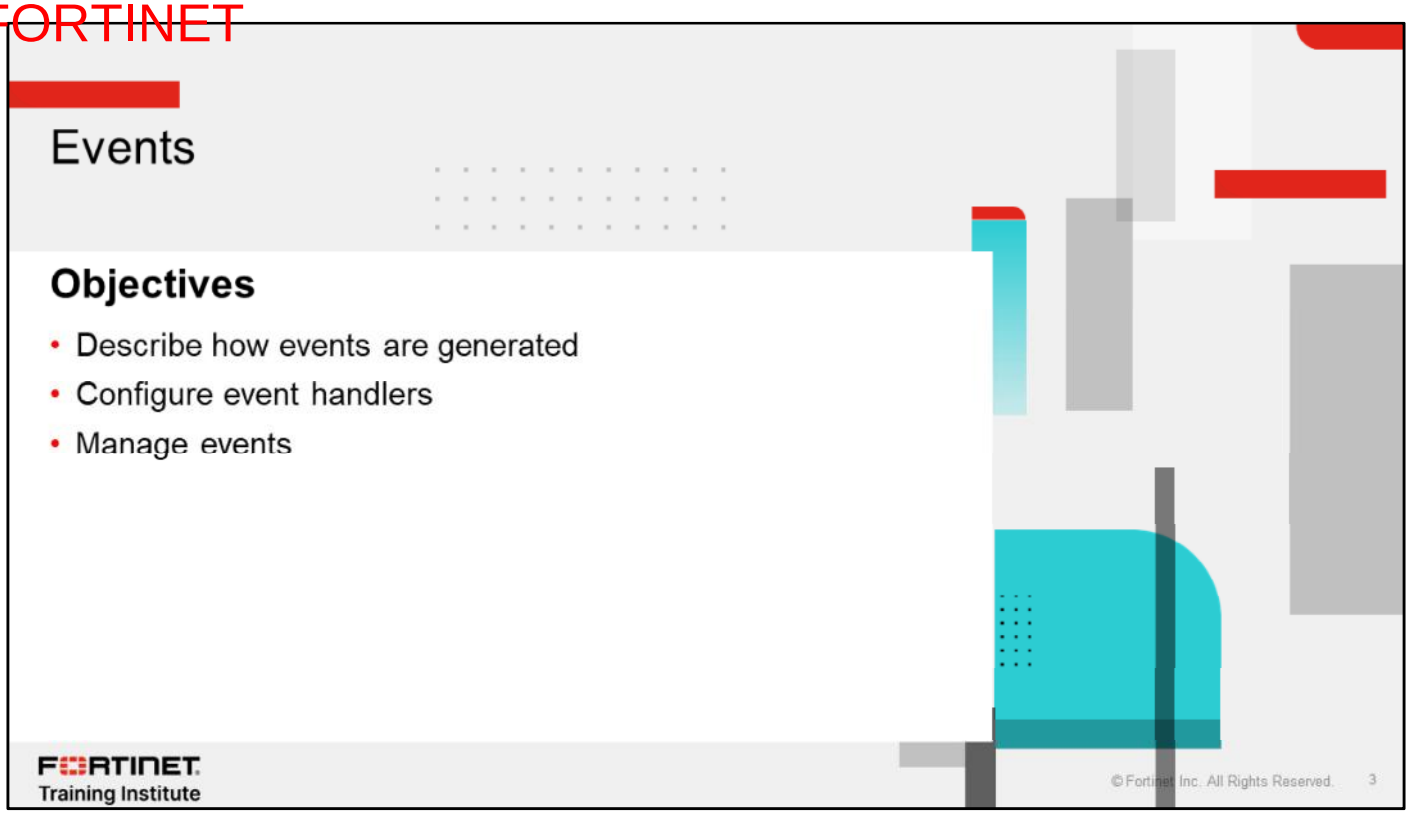
This slide shows the objectives that you covered in this lesson.

By mastering the objectives covered in this lesson, you learned how FortiAnalyzer parses and normalizes logs. You also learned various methods of searching for logs in log view, as well as how to view summary data, dashboards, and widgets in FortiView.

In this lesson, you will learn about events, indicators, and incidents on FortiAnalyzer, and how to configure them and use them to triage alerts as a SOC analyst.



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



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

By demonstrating competence in managing events and configuring event handlers, you will be able to handle the security events taking place in your environment.

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

Note: Subscription to the Security Automation Service provides FortiAnalyzer with real-time event handlers that can help detect zero-day attacks

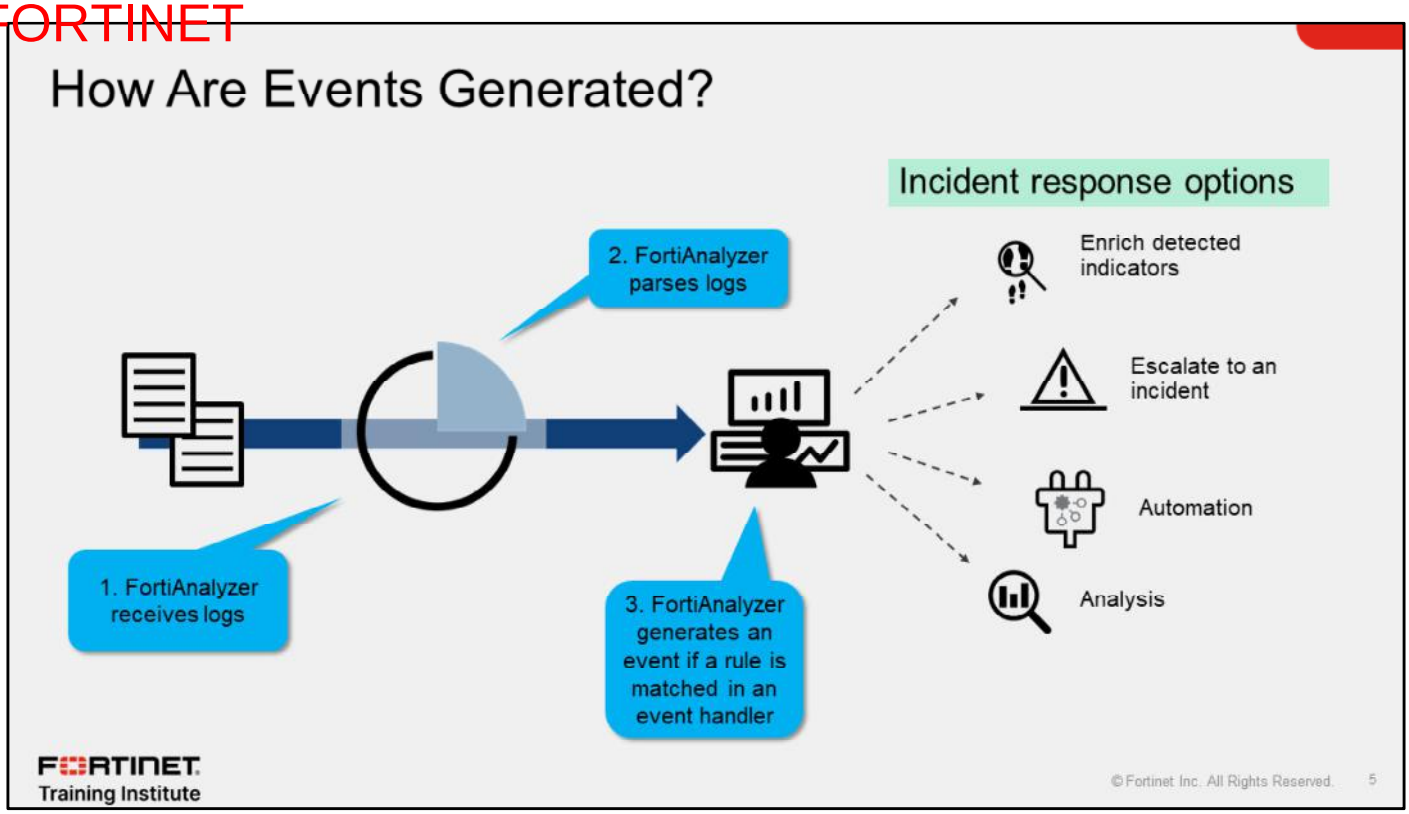
FORTINET Training Institute

 4

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. Subscription to the Security Automation Service provides FortiAnalyzer with real-time event handlers that can help detect zero-day attacks.

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.



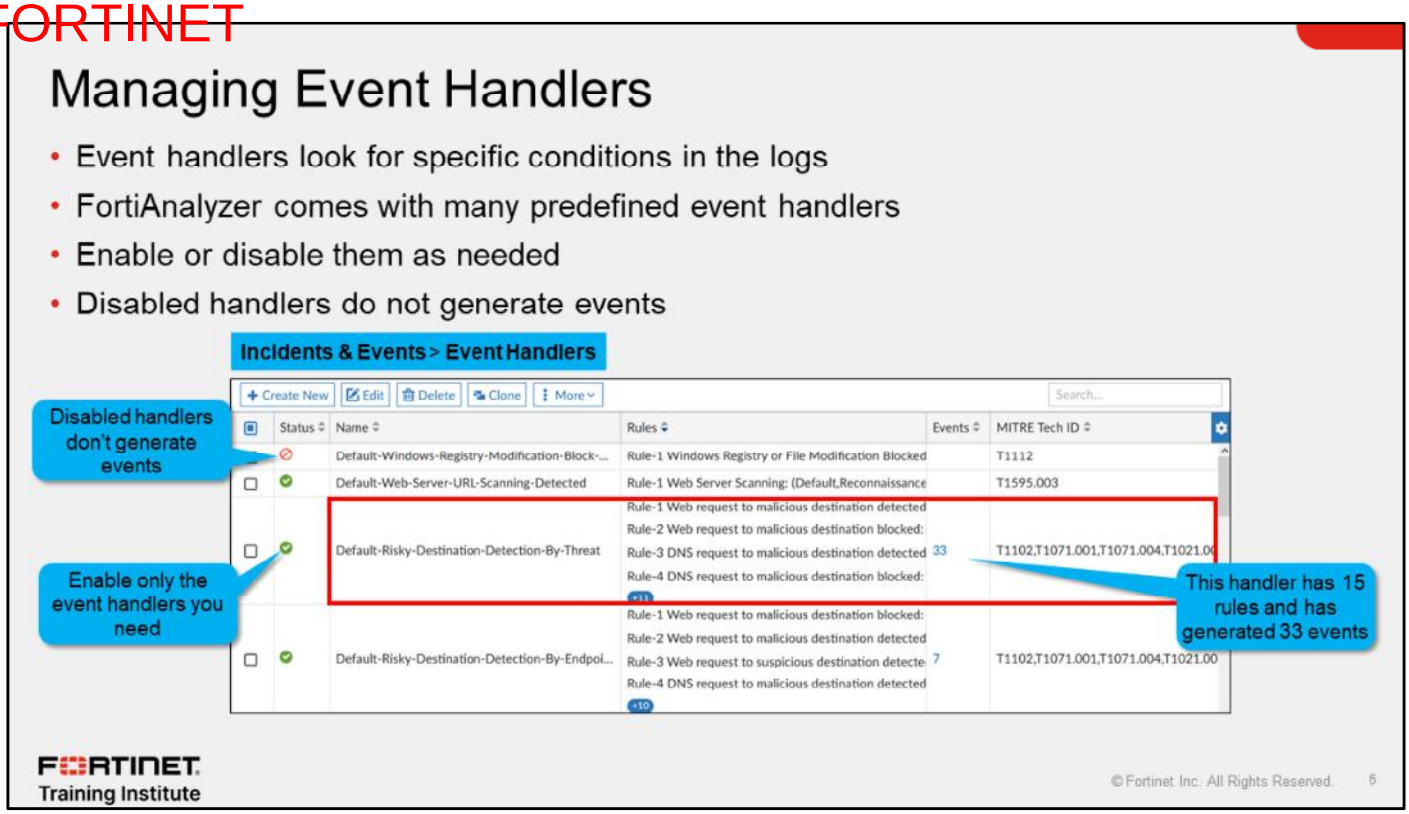
After receiving logs from other devices, and based on the details included in them, FortiAnalyzer uses event handlers to determine if new events need to be generated. Event handlers identify whether the information in the logs matches a series of configurable criteria, such as threat type, device type,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

FortiAnalyzer comes with many predefined event handlers that you can use, clone, and customize. You can also 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.

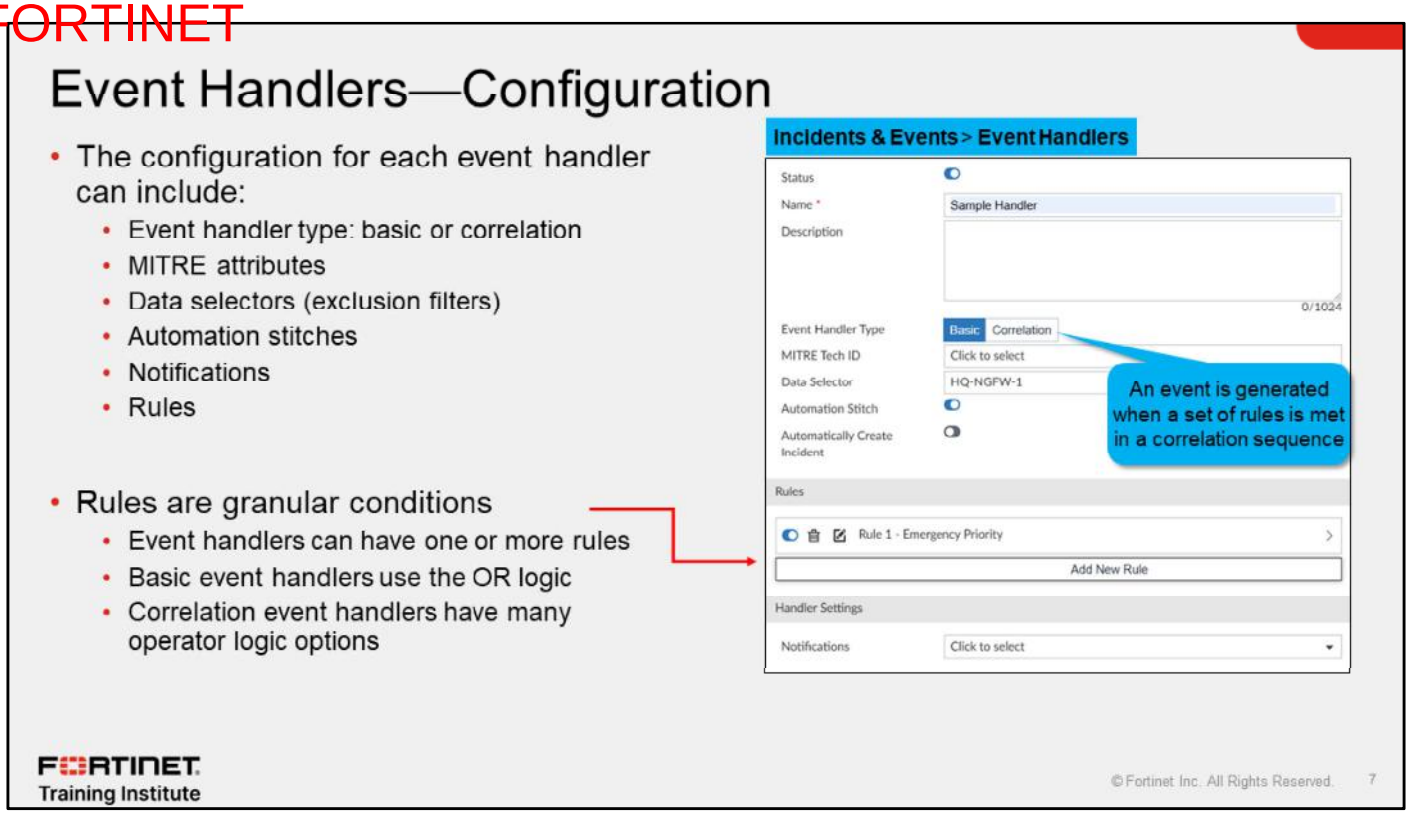
If events warrant further attention and investigation, you can escalate them into incidents. From there, you can correlate logs with an incident, look at an incident timeline, assign a priority and an analyst to review an incident, and more. For a large volume of generated events, you may leverage playbooks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

FortiAnalyzer can extract indicators such as IP addresses, domains, and URLs out of generated events and enrich them using FortiGuard and Virus Total enrichment services.



An event handler looks for specific conditions in the 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.

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



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, assign a name, write a description, and select the type: basic or correlation. When event handler type correlation is selected, an event is generated when a set of rules is met in the correlation sequence.

You can also choose which MITRE domain the event handler falls under, and then select from a list of tech 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*.

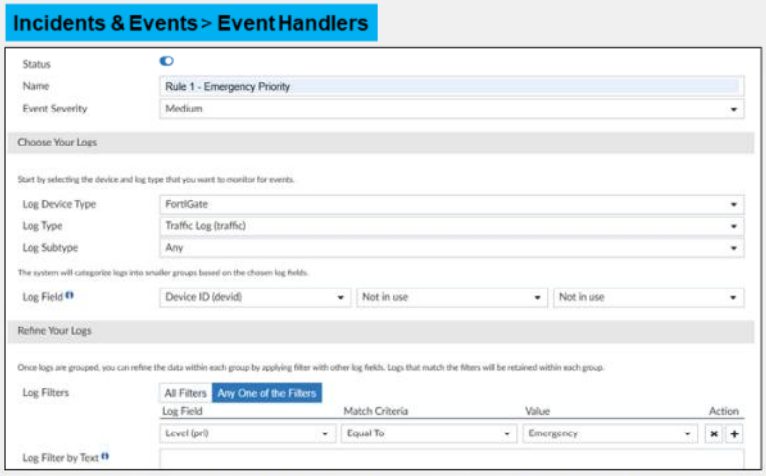
When a handler generates an event with the automation stitch option enabled, FortiAnalyzer sends a notification to the FortiGate automation framework, which then checks if there is a corresponding automation stitch in FortiOS. If there is one, the configured action is triggered.

The **Rules** section contains the fields that must match 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

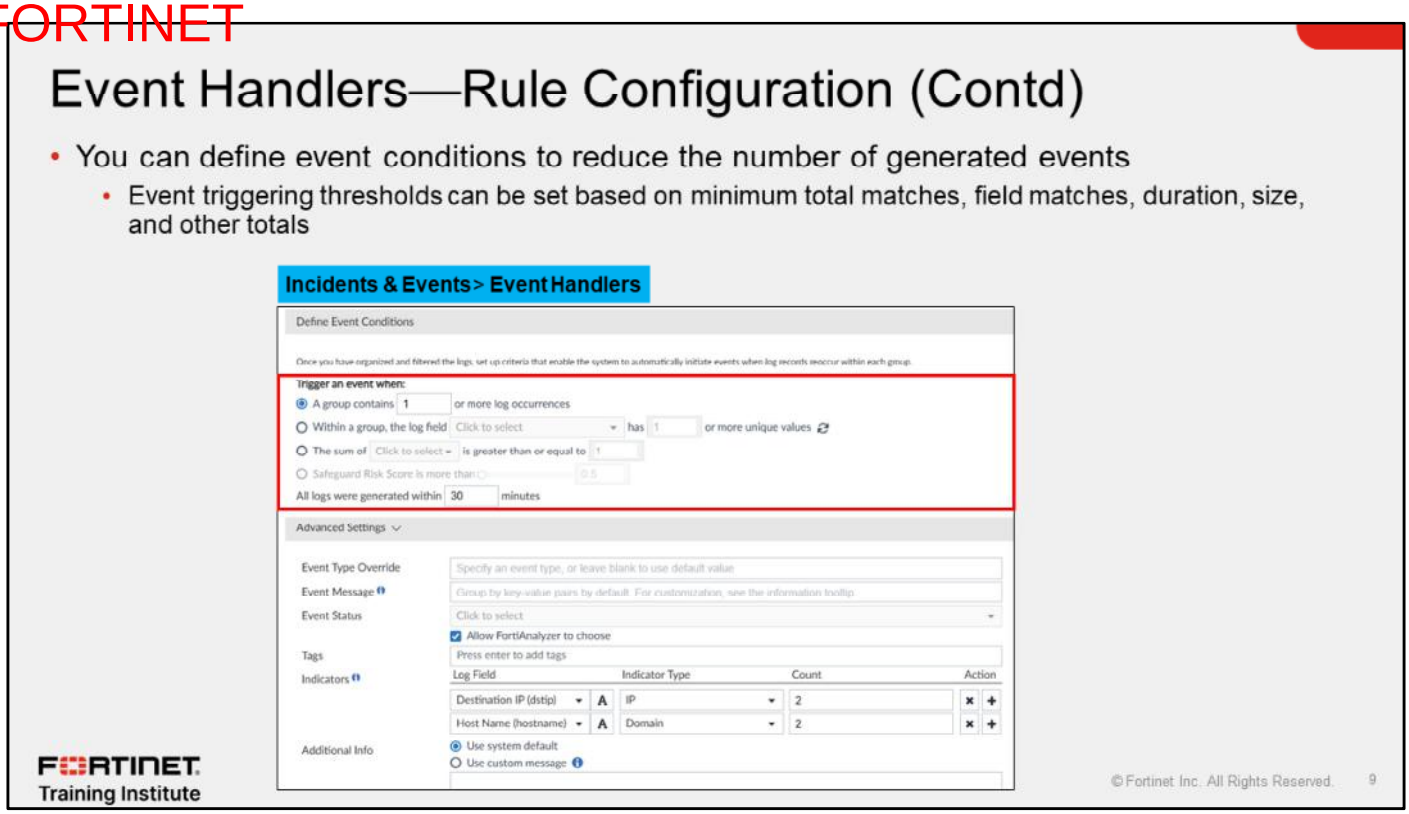


Note: The fields available in the rules depend on the selected device type

FORTINET Training Institute

 8

This slide shows the fields available for configuration inside a rule, including the log device type, log type, and log subtype. Note that within rules themselves both AND and OR logic are supported if there are multiple conditions. You can select common criteria to include in the filter in the **Log Field**. Alternatively, you can use generic text filters if you require precise filtering.

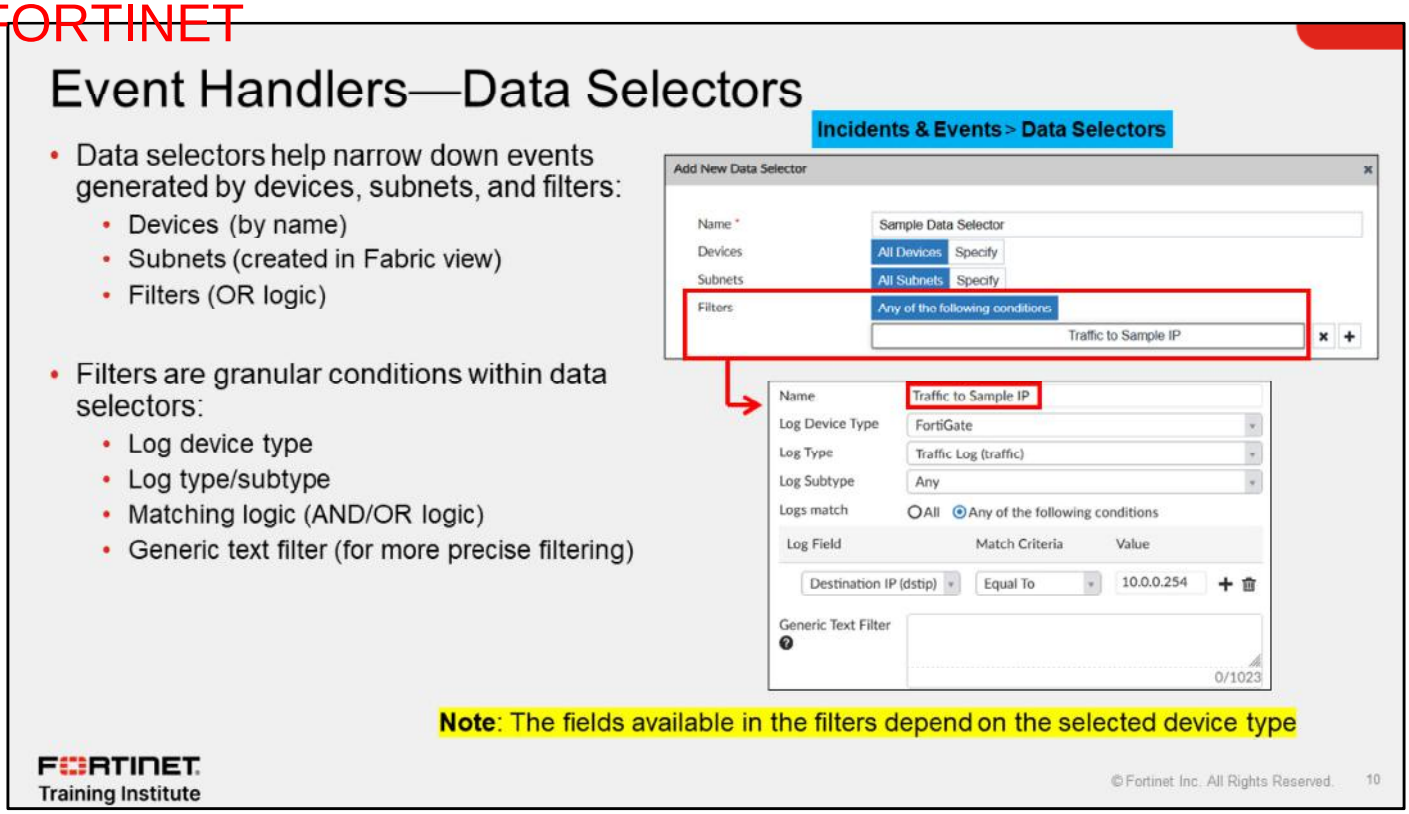


If an event handler is generating too many events in your environment, you can configure aggregation expression and aggregation duration settings.

The **Trigger an event when** section contains three options:
- You can set a threshold based on count, or the minimum number of matching logs.
- You can set a threshold based on a distinct field, such as a distinct source IP address or application.
- You can also set a threshold based on duration, sent/received bytes, and sent/received packets.

Duration is the minimum threshold in minutes to generate events. The duration and minimum threshold settings work together. To generate an event, the minimum number of matching logs (expression) must occur in the specified time period (duration).

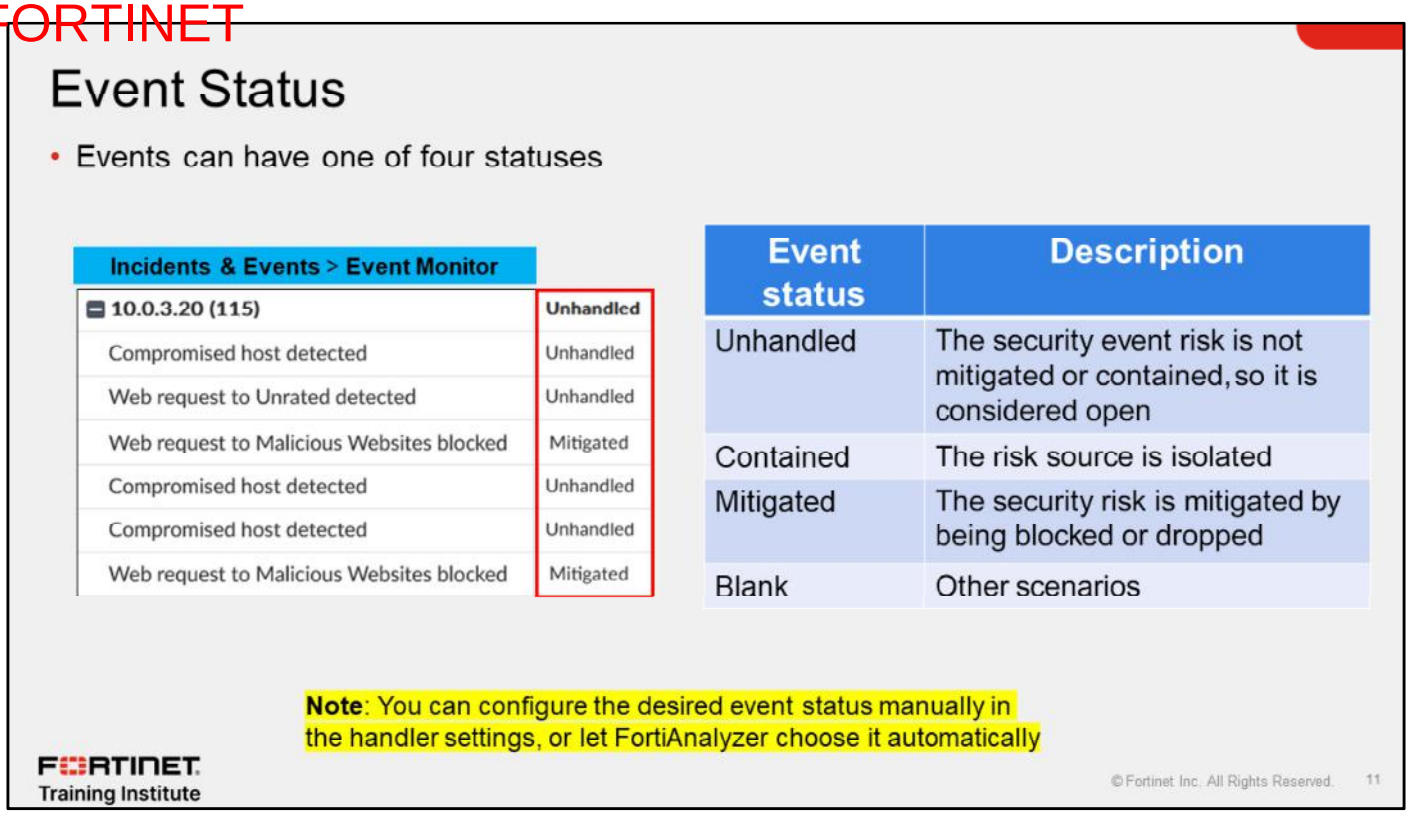
You can also specify event type, message, status, and severity for events.



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

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

This slide shows the fields that you can configure for a filter, including the log device type, log type, and log subtype. Note that filters support both AND and OR logic. When configuring a filter, you can select from common criteria on the GUI, or you can use generic text filters if you require precise filtering.



Events in FortiAnalyzer can have one of four statuses. The current status of an event determines if the security team needs to take further action or not.

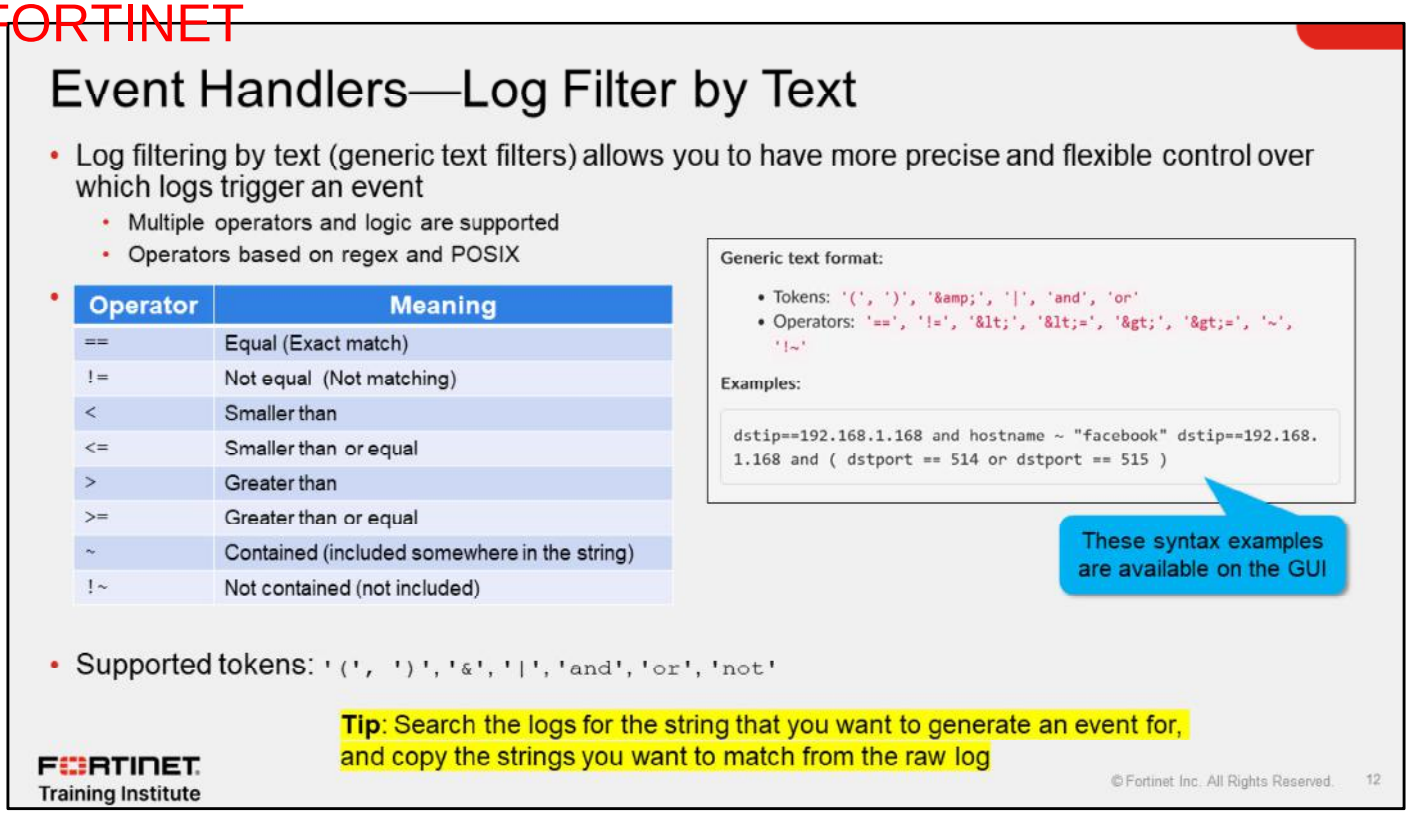
The possible statuses are:

- **Unhandled**: The security event risk is not mitigated or contained, so it is considered open.
  For example, an IPS/AV log with `action=pass` will have the event status **Unhandled**.
  Botnet and IoC events are also considered **Unhandled**.

- **Contained**: The risk source is isolated.
  For example, an antivirus log with quarantine `action` will have the event status **Contained**.

- **Mitigated**: The security risk is mitigated by being blocked or dropped.
  For example, an intrusion prevention system (IPS) or antivirus log with a block/drop `action` will have the event status **Mitigated**.

- **(Blank)**: A blank status indicates a state that the risk is state is something other than unhandled, contained, or mitigated.
  For example, both allow and block actions can be seen in logs associated with the event.



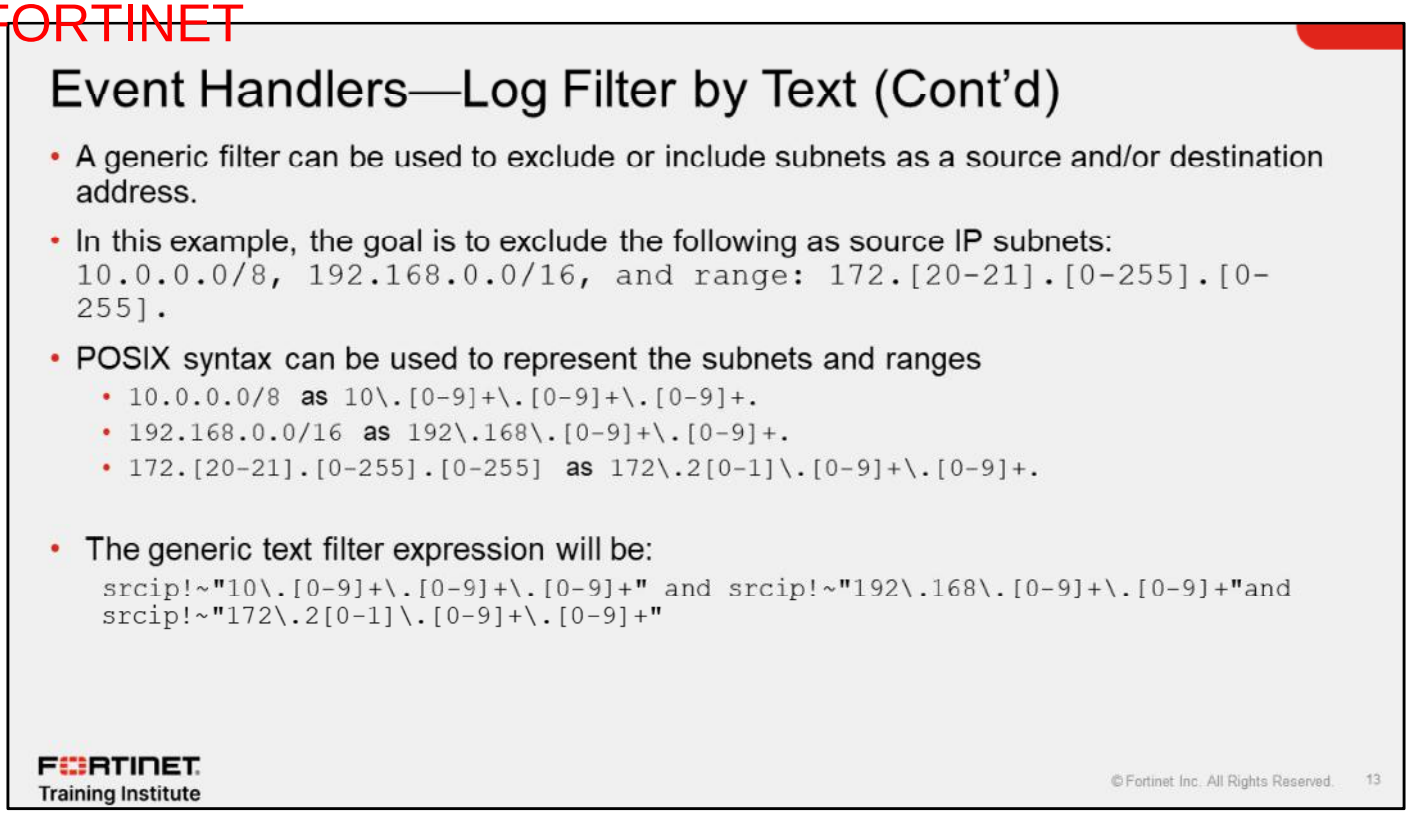
When you configure an event handler, you can use generic text filters for more precise and flexible control over which logs trigger an event. Text filters use operators based on regex and the Portable Operating System Interface (POSIX) standard.

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.

Example: `dstip==192.168.1.168 & hostname ~ "facebook"` matches all logs with a destination IP address field equal to `192.168.1.168` and a hostname field containing the string `facebook`.

You must use the escape character `"\"` if you need to include a reserved character in your filter.

To avoid syntax errors, search your raw logs for the log file for which you want to add an event handler and copy and paste the string you want to match.



In the example shown on this slide, the goal is to exclude the following as source IP subnets: `10.0.0.0/8, 192.168.0.0/16, and range: 172.[20-21].[0-255].[0-255].`

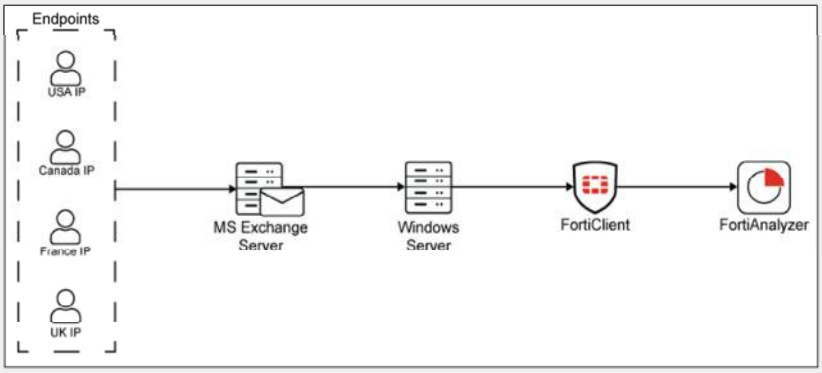
We see how the POSIX syntax will look like for each of the IP address subnets.

In the POSIX syntax:
- Slash '\' is needed to escape a period to include it as a valid character.
- [0-9] means any single digit between 0 and 9, and the plus '+' allows more digits.
- The syntax will also match octet '999', which would be wrong, but since it is already known that the logs include only valid IP addresses, it is not necessary to make the filter incredibly precise. The firewall already filters out these results when forming log messages.
- 2[0-1] - means: starting with 2 and the next digit is 0 or 1.

We then combine the three POSIX syntax subnets in and statements to form the expression that will be used in the generic text filter.

Predefined Event Handlers

- Predefined event handlers are available to detect suspicious activities in the MS Exchange Server
  - MS Exchange–Large Email
  - MS Exchange–Multiple Failed Deliveries
  - MS Exchange–Suspicious Email Activity

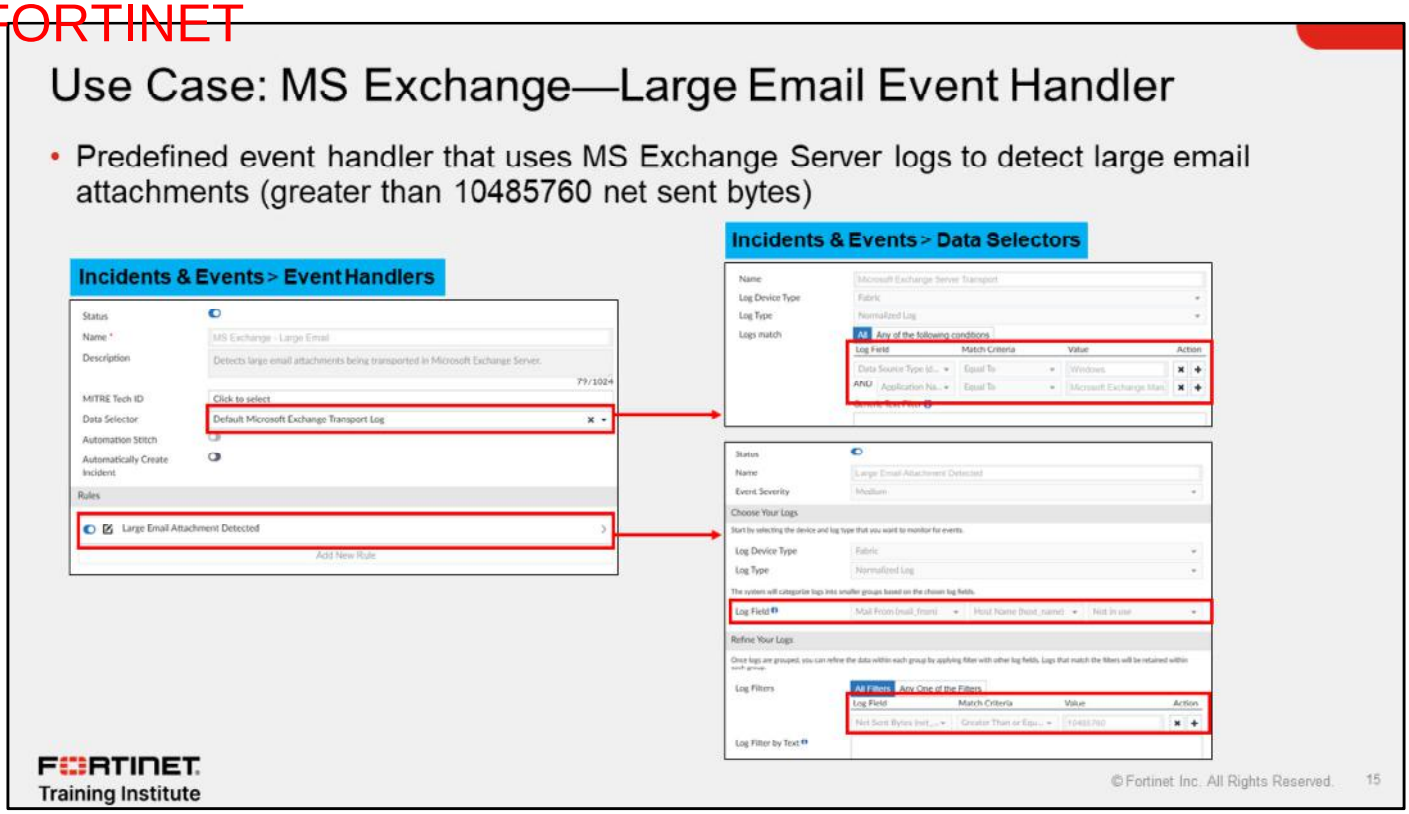


FORTINET Training Institute

 14

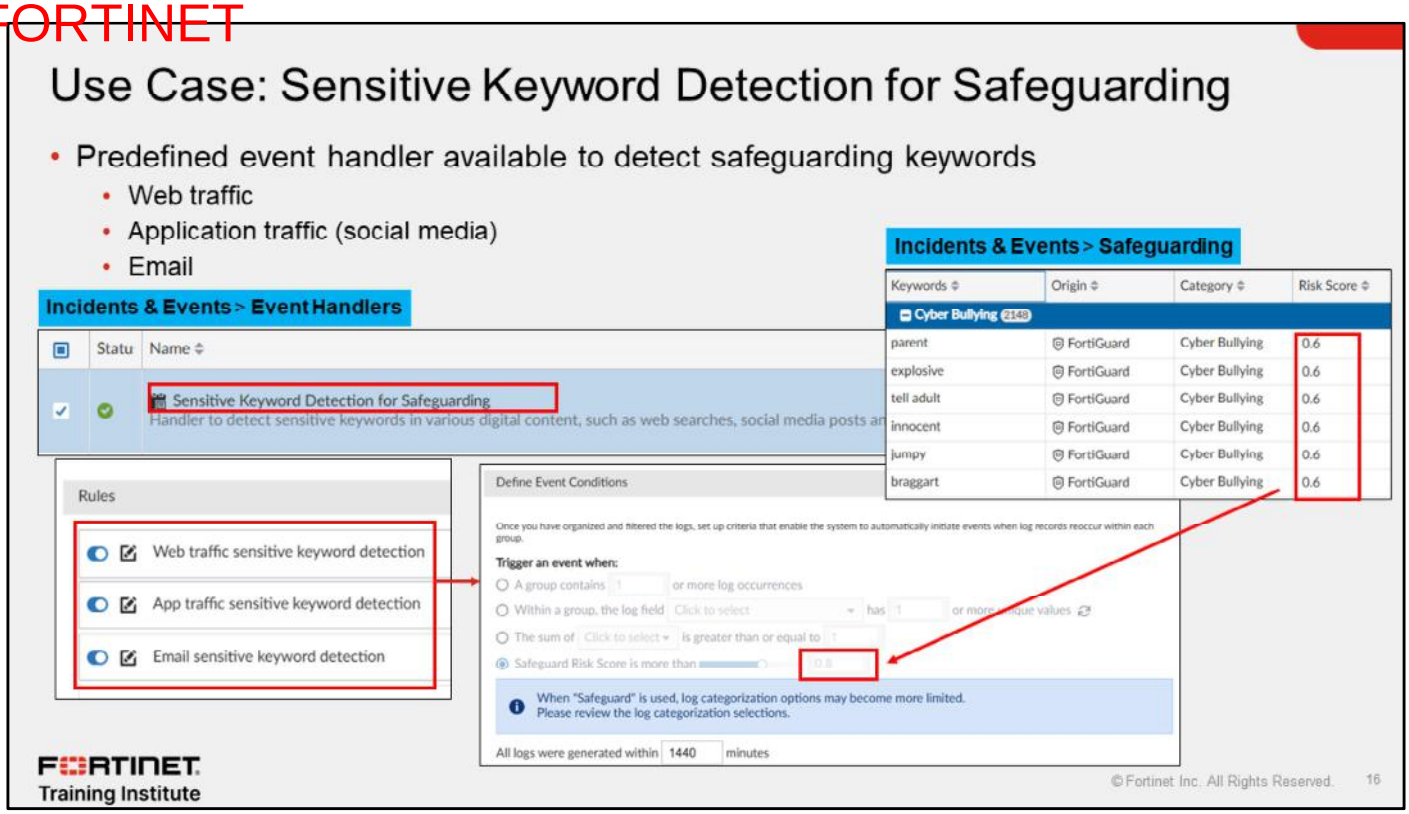
FortiAnalyzer comes with predefined event handlers that provide a starting point. You can quickly deploy the predefined event handlers for essential monitoring capabilities, especially in new deployments.

Since the predefined event handlers are configured following Fortinet's recommended best practices, they also serve as an essential learning tool. You can examine the filters and conditions and follow the same guidelines when configuring new handlers.



MS Exchange - Large Email is a predefined event handler that uses MS Exchange server logs to detect large email attachments (greater than 10485760 net sent bytes) being transported in the Microsoft Exchange server.

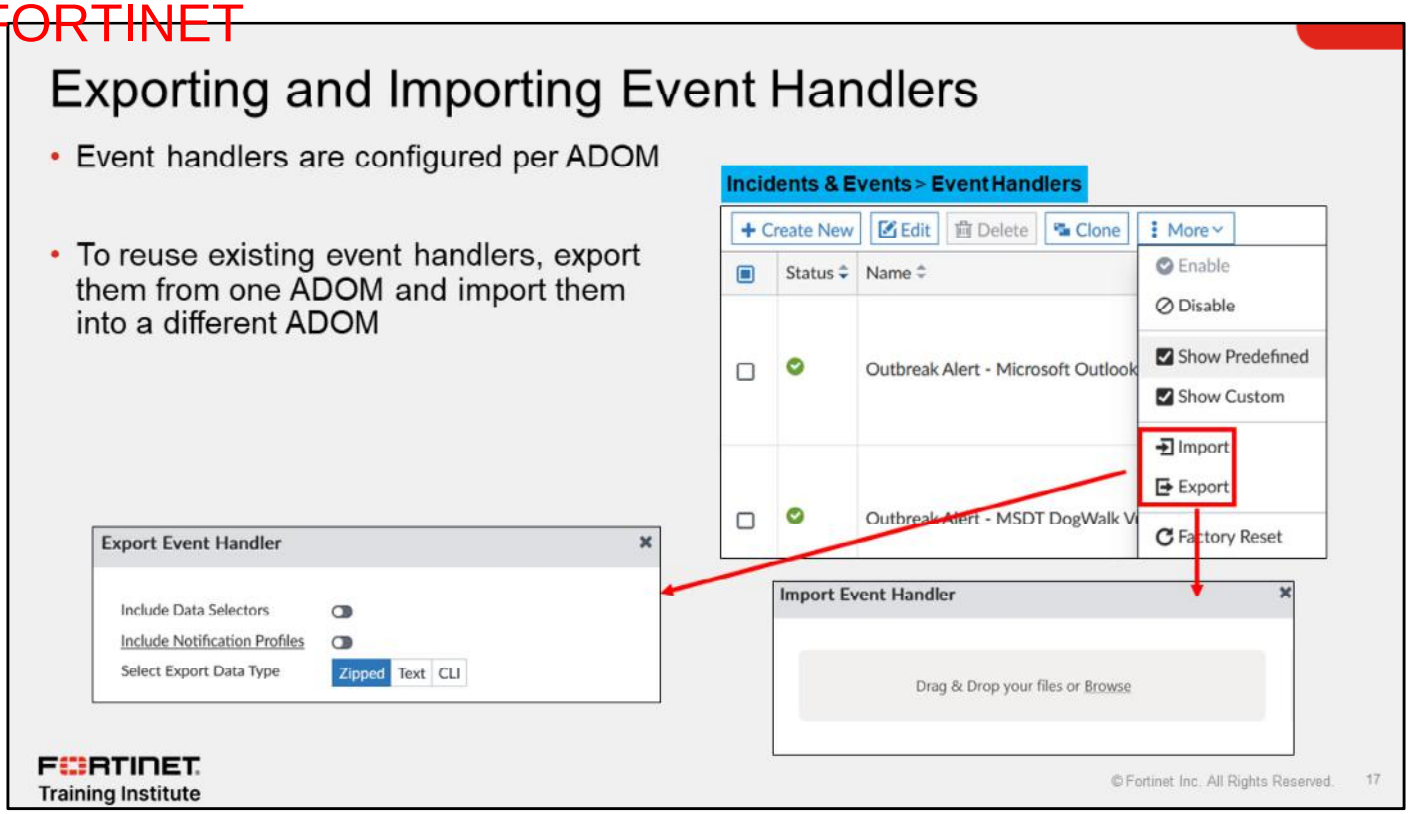
This event handler uses the predefined data selector, **Default Microsoft Exchange Transport Log**, to ensure the proper devices and logs are used to trigger events.



A predefined event handler is available to detect safeguarding keywords in logs for web traffic, application traffic (social media), and email. This event handler supports consistent monitoring for harmful content, allowing timely intervention.

When the rule has a log type of web filter, application control, and email filter, you can trigger an event when the safeguard risk score is more than a specified value. You can view the safeguard keywords and their associated risk scores on the **Safeguarding** page. For all rules in the **Sensitive Keyword Detection for Safeguarding** event handler, FortiAnalyzer triggers events when the safeguard risk score is more than 0.8.

The **Sensitive Keyword Detection for Safeguarding** event handler includes a separate rule for each of the log types that allow for this new trigger (web filter, application control, and email filter).



By default, event handlers are restricted to the ADOM where they were created. If you need to use the same settings in a different ADOM, exporting the event handlers saves you the time of creating them again.

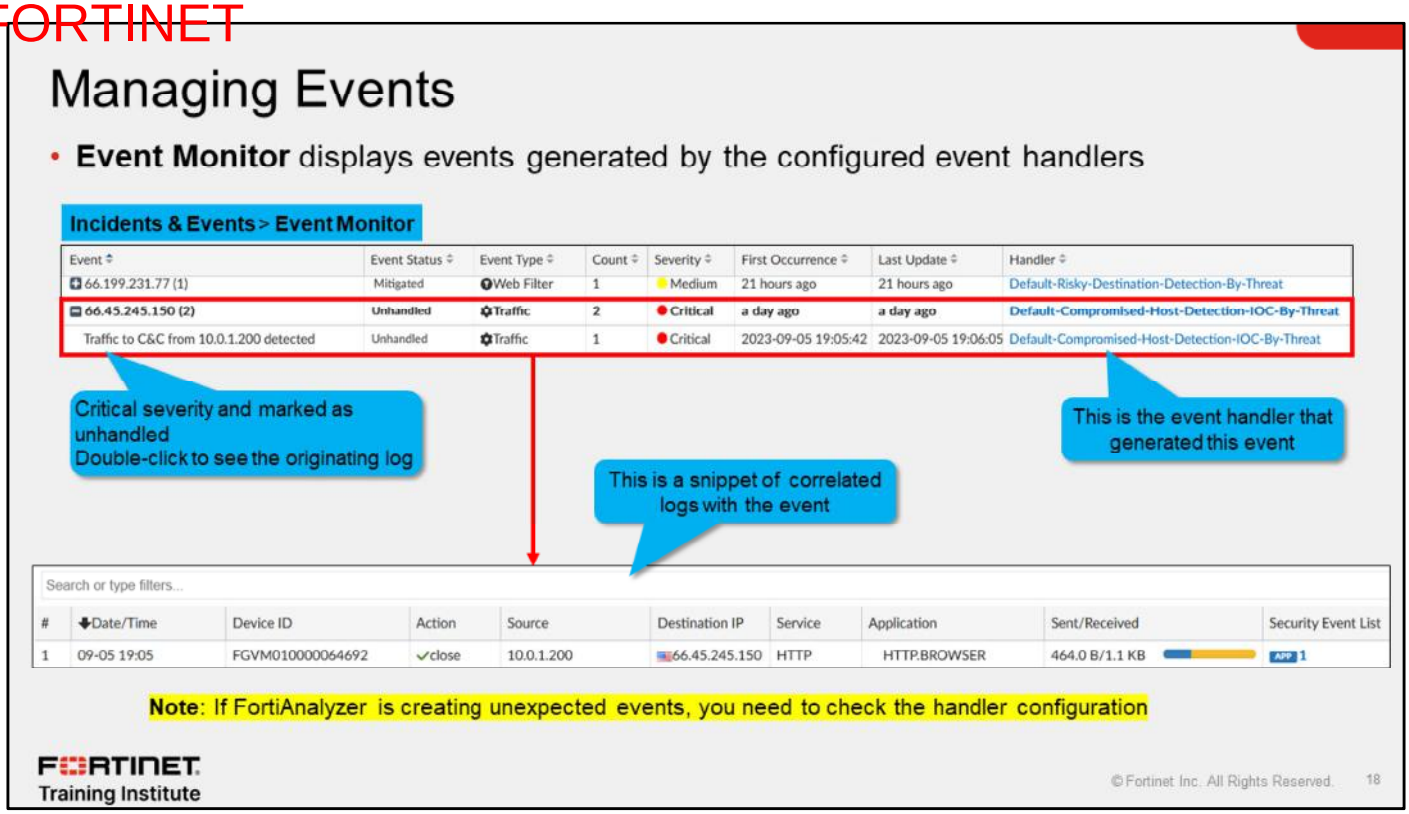
To export an event handler, in the **Event Handler** list, select one or more handlers, right-click, and then select **Export**.

A new window opens where you must choose if you want to include data selectors, notification profiles, and the type of file you want to create, whether zipped, text, or CLI configuration. Click **OK** to finish and save the file.

You can create subnets and subnet groups in the Fabric view and use them as filters in event handlers and reports.

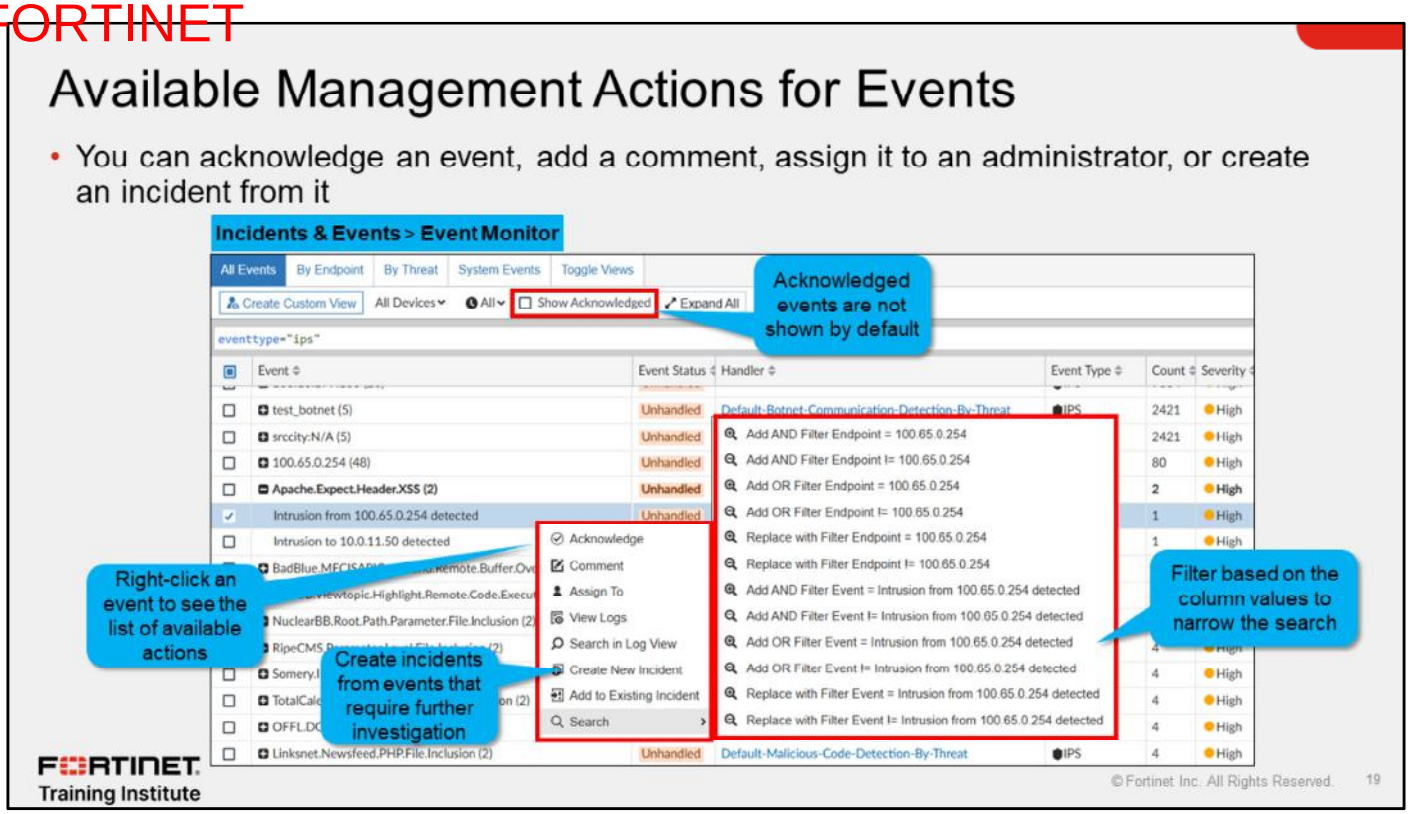
To import an event handler, in **Handlers**, right-click, and then select **Import**. You can drag and drop the file, or use the file browser to find the file.

If the imported handler name already exists, you can rename, replace, or skip the import.



After event handlers start generating events, you can view and examine them combined or divided by endpoint, threat, or system events.

You can double-click an event to see more details about it, including the information from the associated logs. Generally, you should give priority to events with an unhandled status or critical severity.



You can right-click an event to leave a comment for your records, acknowledge the event, assign it to an administrator (or yourself) for further investigation, or create an incident from it. You will learn about incidents in this lesson.

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. The exception could be an excessive number of mitigated events, which, despite being blocked, may indicate a compromised device. Additionally, if an event was used to generate an incident, you should also acknowledge it after you mark it as resolved.

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

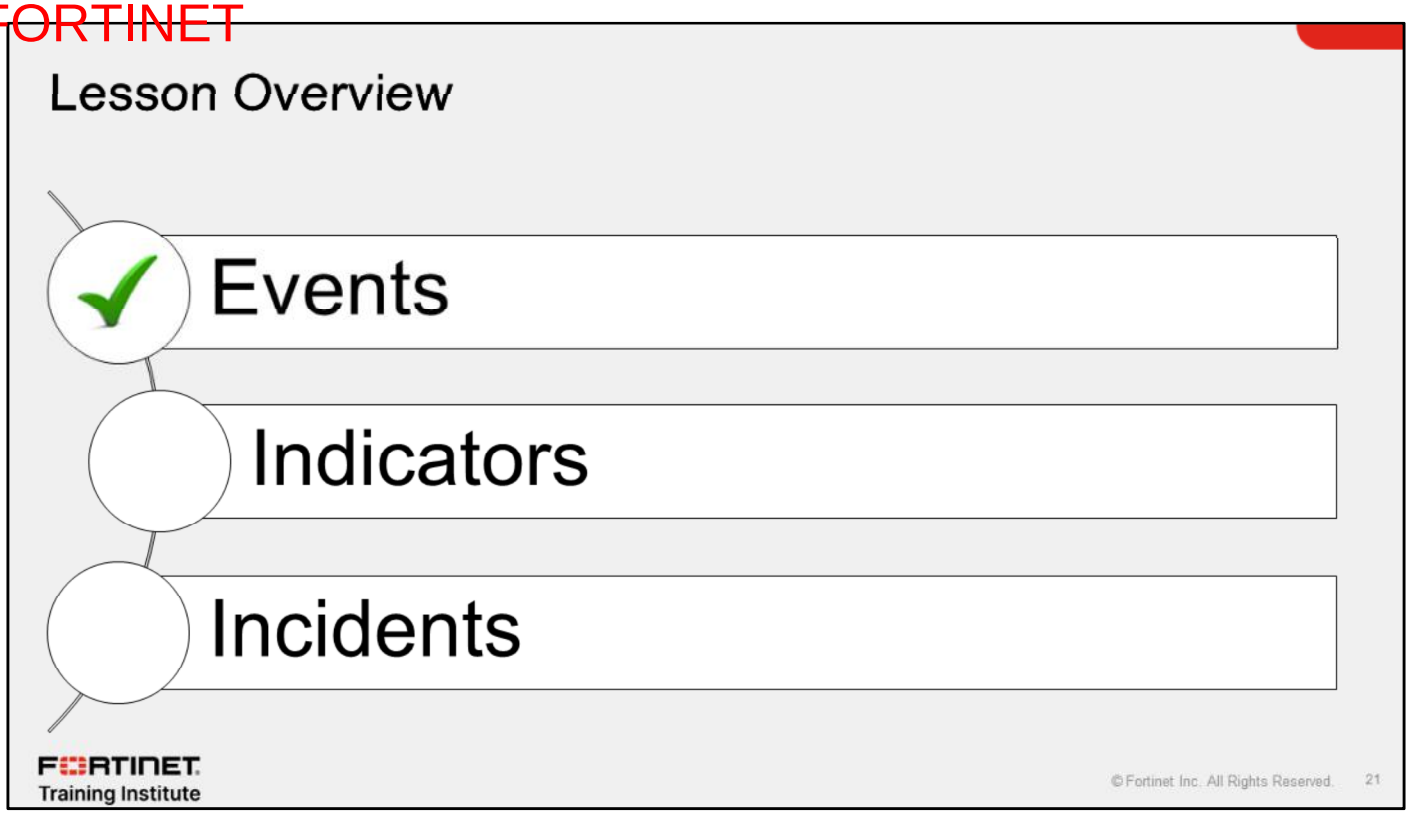
Knowledge Check

1. What are event handlers?
   - A. Threats identified by FortiGuard that generate events
   - ✓ B. A set of matching conditions in the logs that generate events

2. How do you create event handlers for all ADOMs?
   - A. Create the event handlers in the root ADOM.
   - ✓ B. Export handlers and then import them into the appropriate ADOMs.

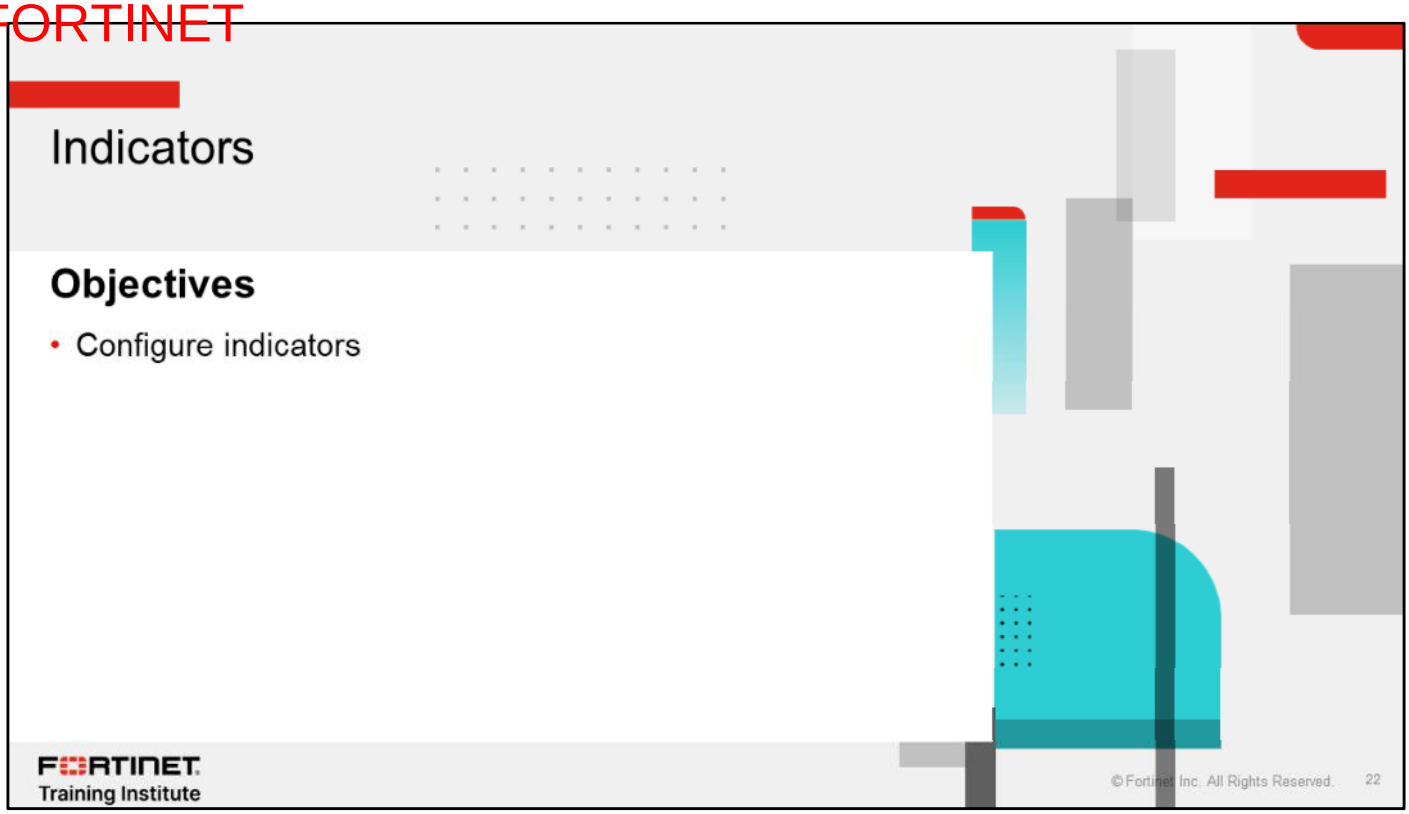
FORTINET Training Institute

 20



Good job! You now know how to manage events and configure event handlers.

Now, you will learn about indicators.

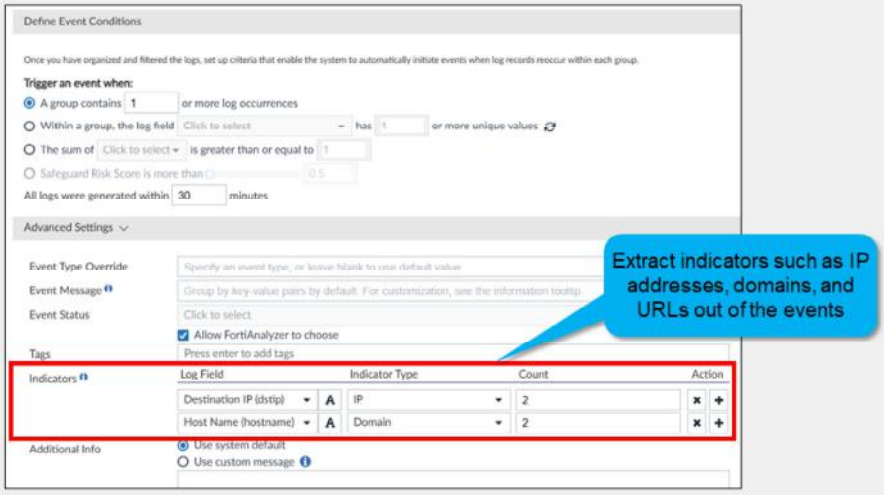


After completing this section, you should be able to achieve the objective shown on this slide.

By demonstrating competence in configuring indicators, you will be able to add more context and threat intelligence about suspicious artifacts when investigating security incidents.

What Are Indicators?

- Data extracted by FortiAnalyzer from events that could be harmful or malicious
- You can choose what type of data to extract from which events
- Indicator types
  - IP address
  - URL
  - Domain
- Indicator reputation
  - Malicious
  - Suspicious
  - Harmless
  - Undetected



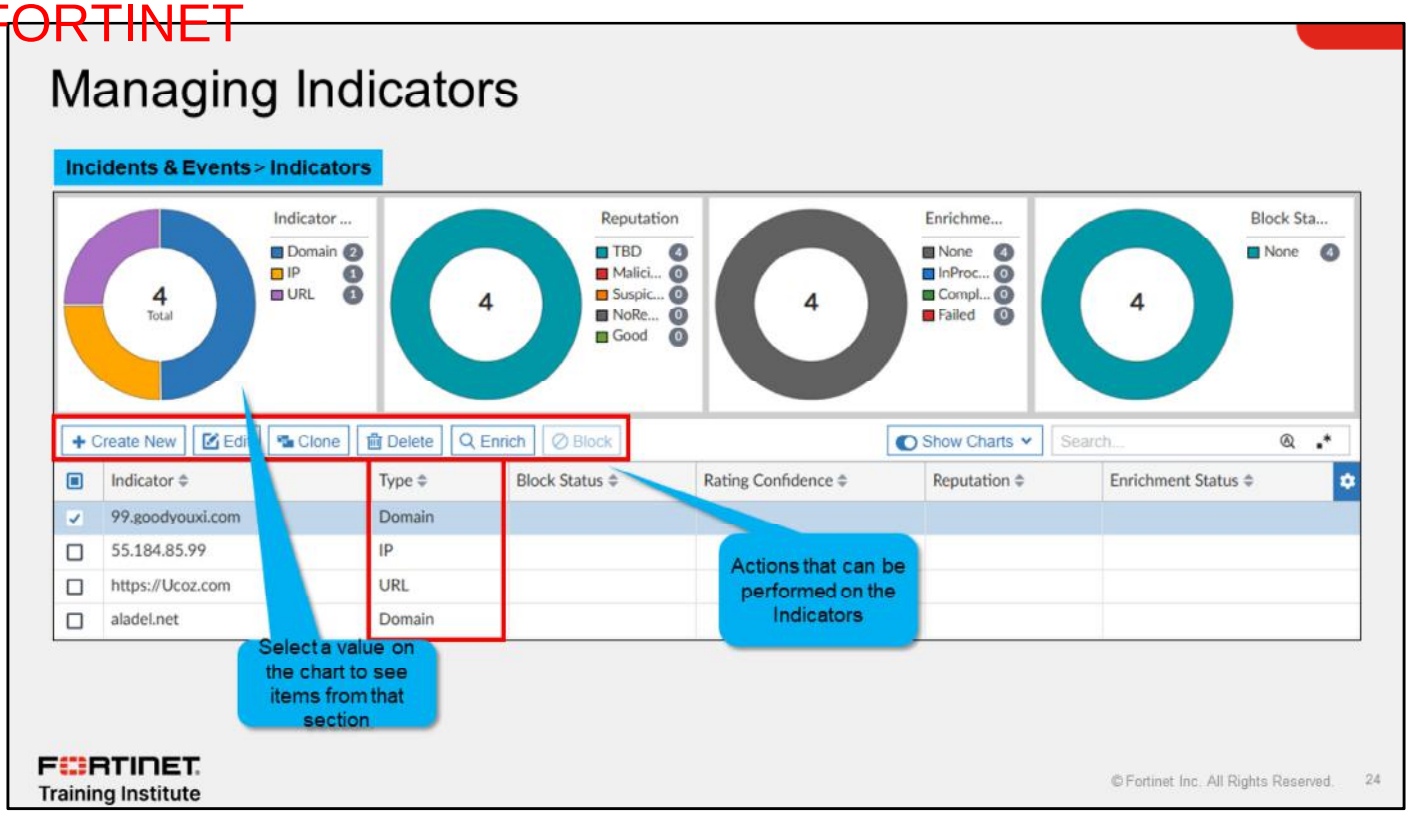
FORTINET Training Institute

 23

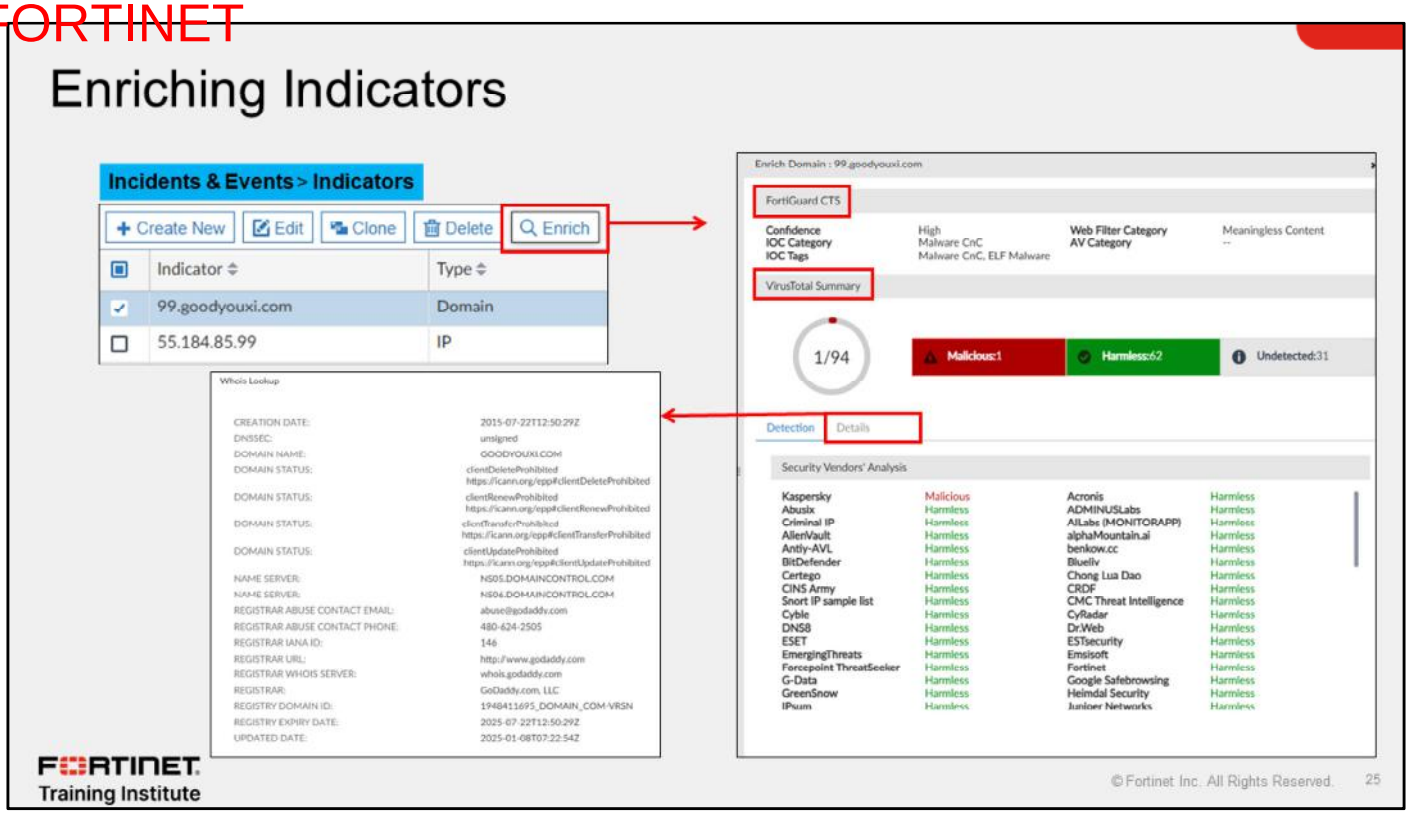
Indicators are data extracted by FortiAnalyzer from events that could be harmful or malicious. On FortiAnalyzer, you can choose which type of data to extract from which events by filtering while configuring the rules in event handlers. You can also manually create indicators on the **Indicator** page.

There are three types of indicators: IP addresses, URLs, and domains.

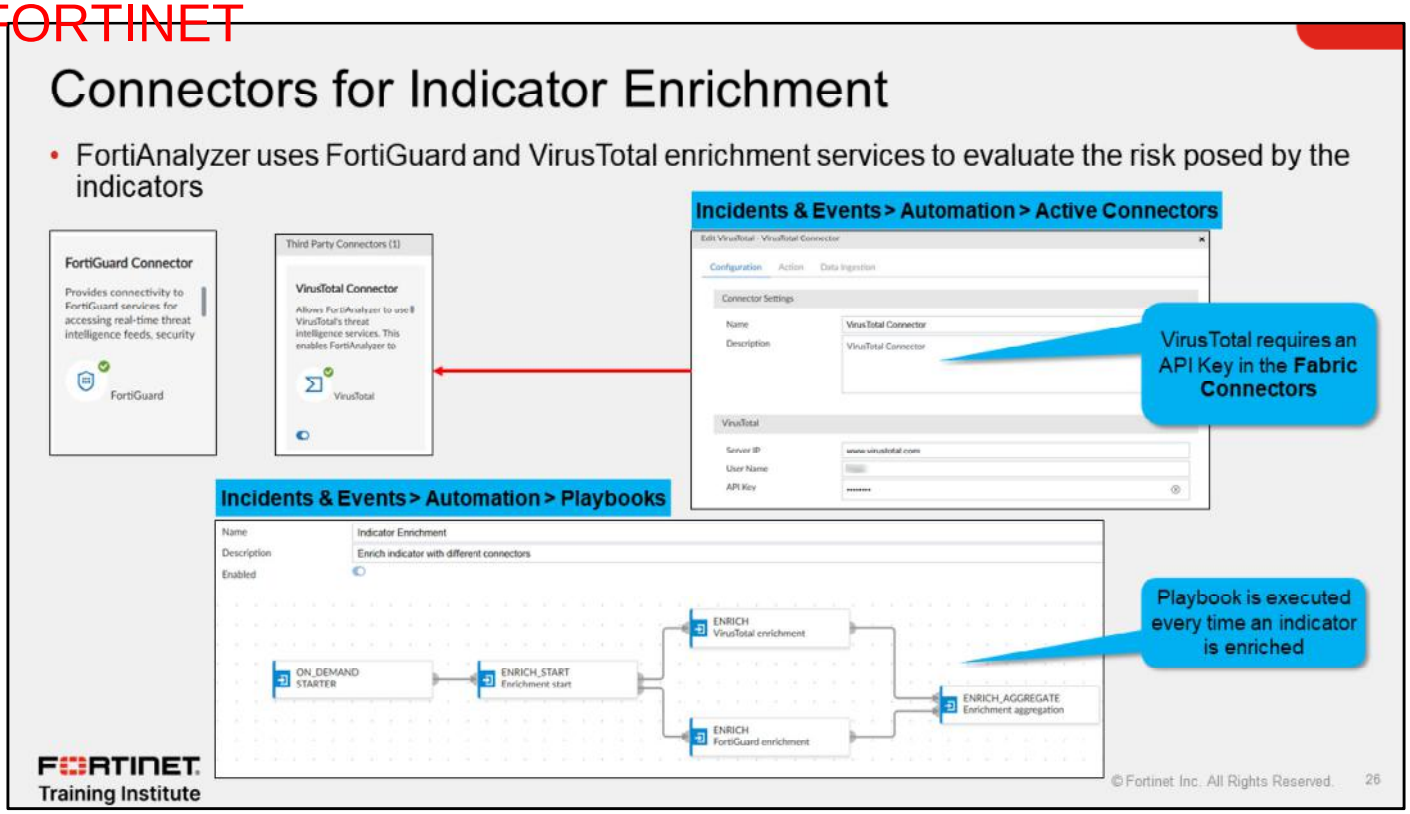
Also, after their enrichment, indicators can have one of four reputation types: malicious, suspicious, harmless, or undetected.



The **Indicators** chart consolidates all detected indicators for centralized analysis. This streamlines threat evaluation and enables SOC analysts to take swift action to mitigate risks. The indicators page allows you to view details about the indicators in a pie chart and tabular form. Select a value in any of the charts to apply the filter to all charts and the table view. To remove the filter, click the chart title.

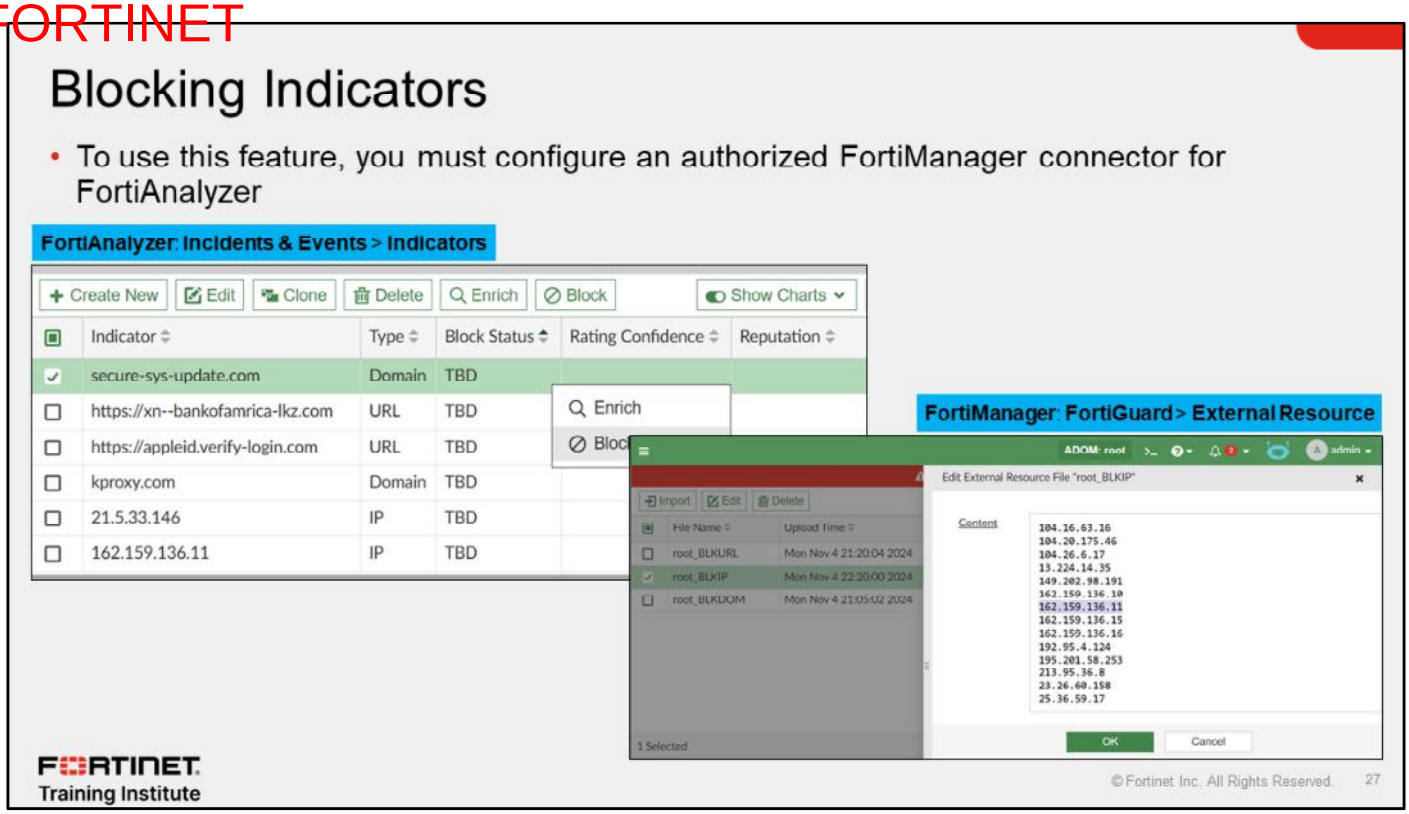


The indicator enrichment feature provides security analysts with comprehensive threat intelligence about identified IP addresses, domains, and URLs. Enriched context gives analysts an opportunity for a deeper understanding of security incidents, empowering them to make more informed and effective decisions. When you save an enrichment, it updates the existing entry in the history. A new entry will only be created when there are changes in the enrichment.



FortiAnalyzer uses FortiGuard and VirusTotal enrichment services to evaluate the risk posed by the indicators. FortiGuard is built in and ready to use, and VirusTotal requires you to configure an API key in the Fabric connectors.

FortiAnalyzer now offers a new predefined playbook called Indicator Enrichment. This playbook is read-only and enabled by default. It is executed every time an indicator is enriched.

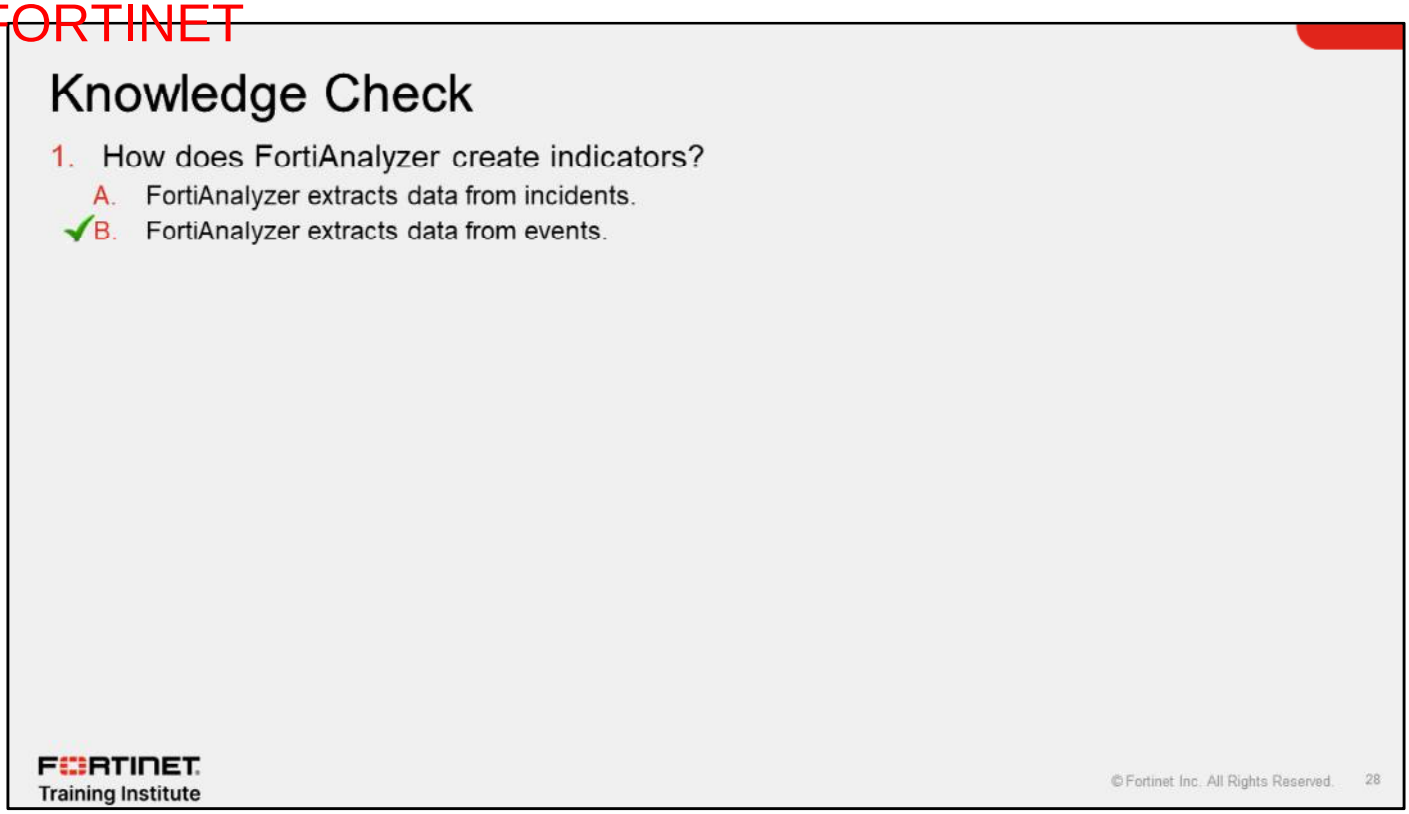


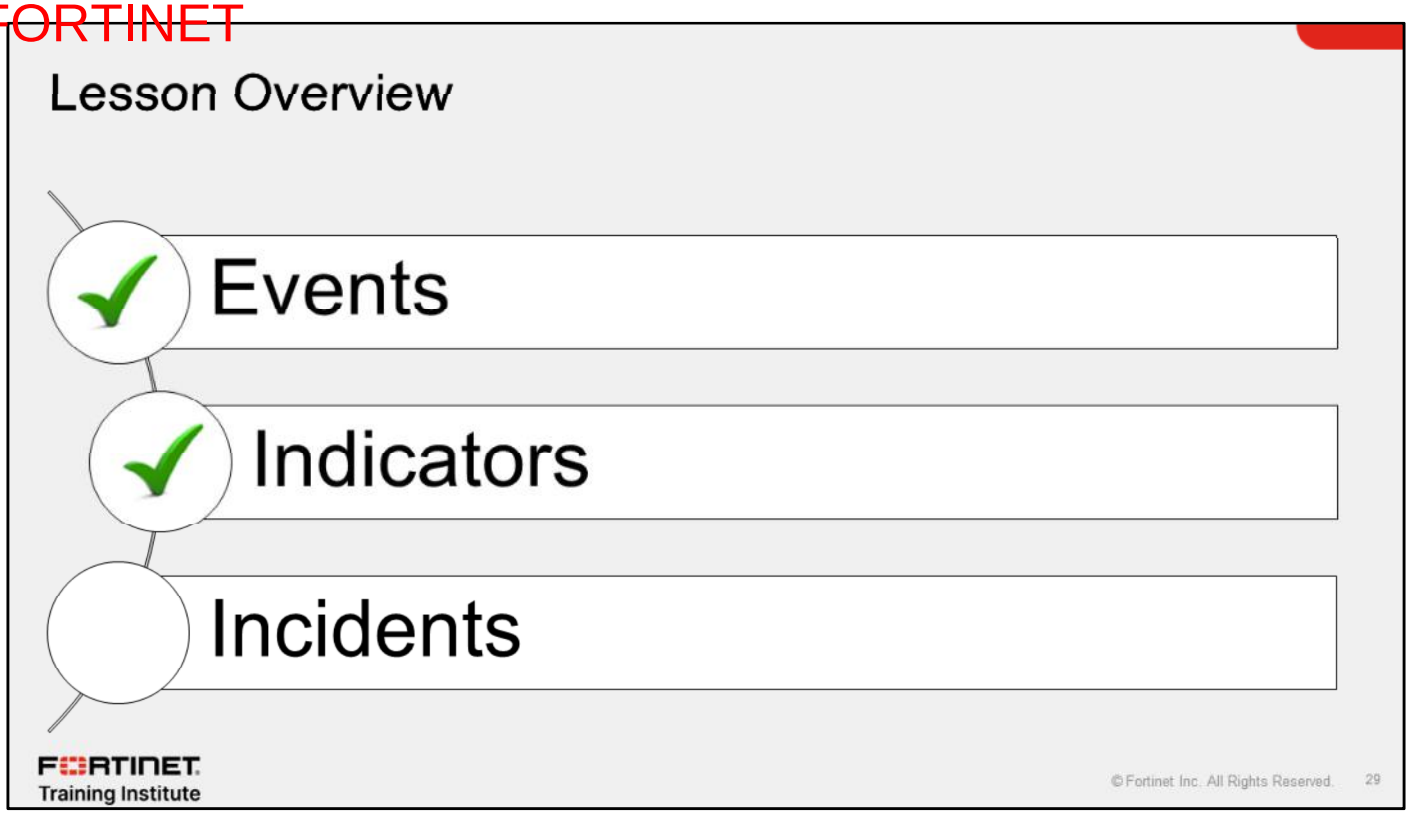
You can block suspicious indicators directly from FortiAnalyzer. This can help you reduce potential risks and quickly respond to known threats by blocking suspicious IP addresses, URLs, or domains. To use this feature, you must set up an authorized FortiManager connector for the FortiAnalyzer on the **Fabric Connector** page of FortiAnalyzer.

In the back end, a playbook called Block_indicator runs every 5 minutes to send the information to FortiManager. After the playbook is run, the indicator's status changes to **Blocked**. The **Blocked** status on FortiAnalyzer confirms that the list is updated on FortiManager, but it is not synced to FortiGate.

When the playbook runs successfully, the blocked indicator is pushed to the FortiManager **External Resource** list. Using this list in FortiManager, you can create threat feeds, security profiles, and policy blocks to push the policies to the identified FortiGate. You can also use this list to update all FortiGate devices to block the suspicious indicators.

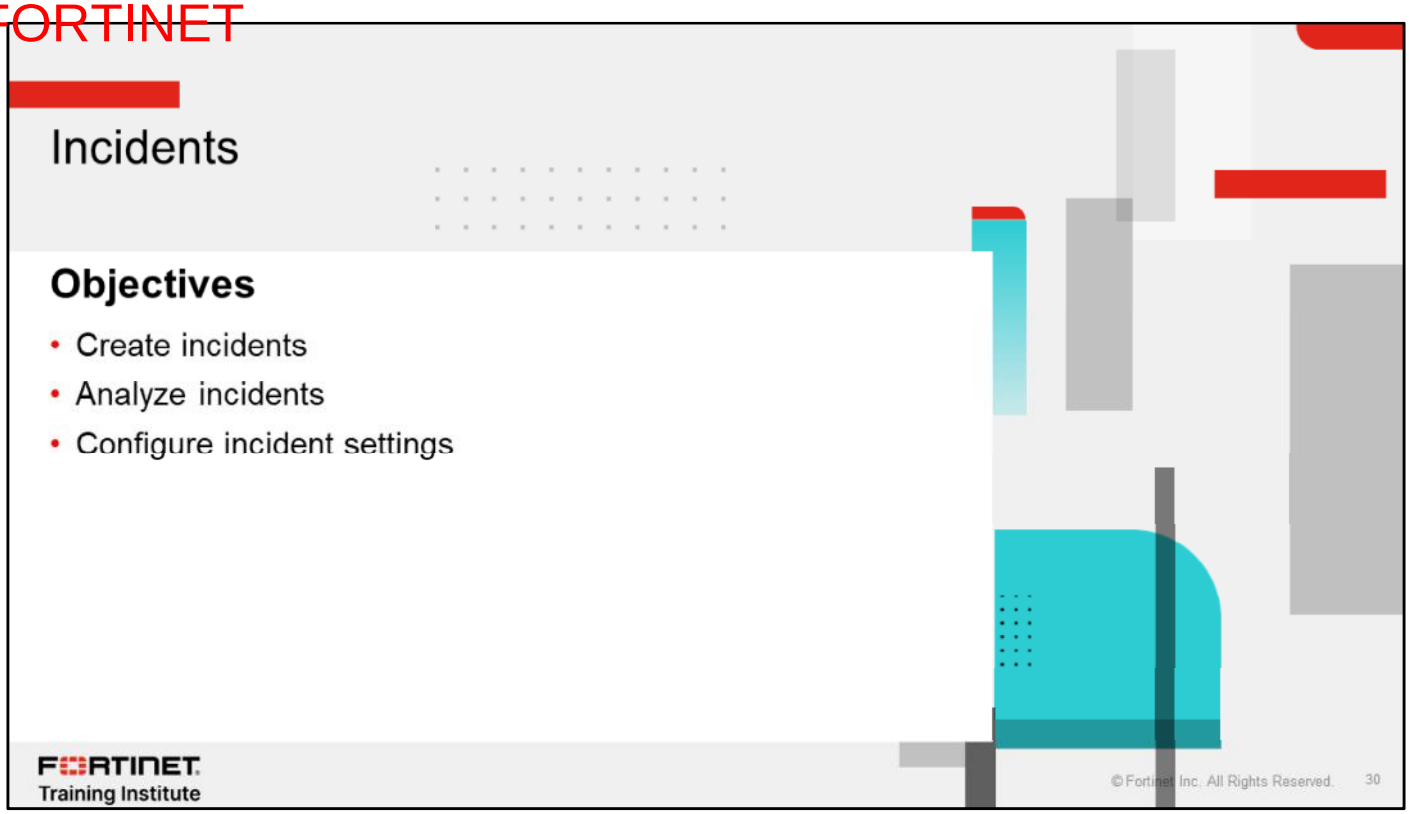
The FortiManager firmware version must be the same as FortiAnalyzer for the blocklist to be pushed to FortiGate devices.





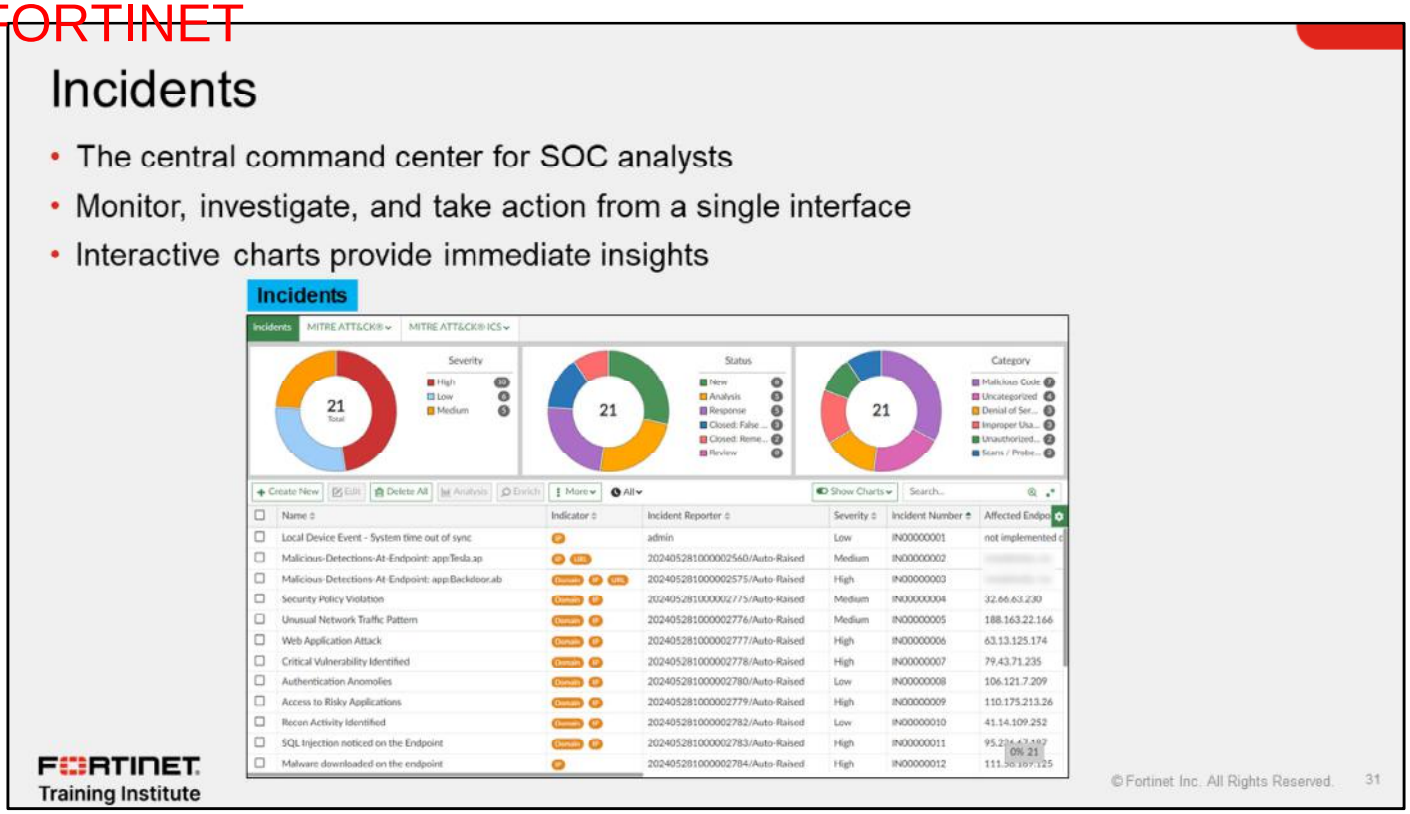
Good job! You now know how to manage and enrich indicators.

Now, you will learn about incidents.



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

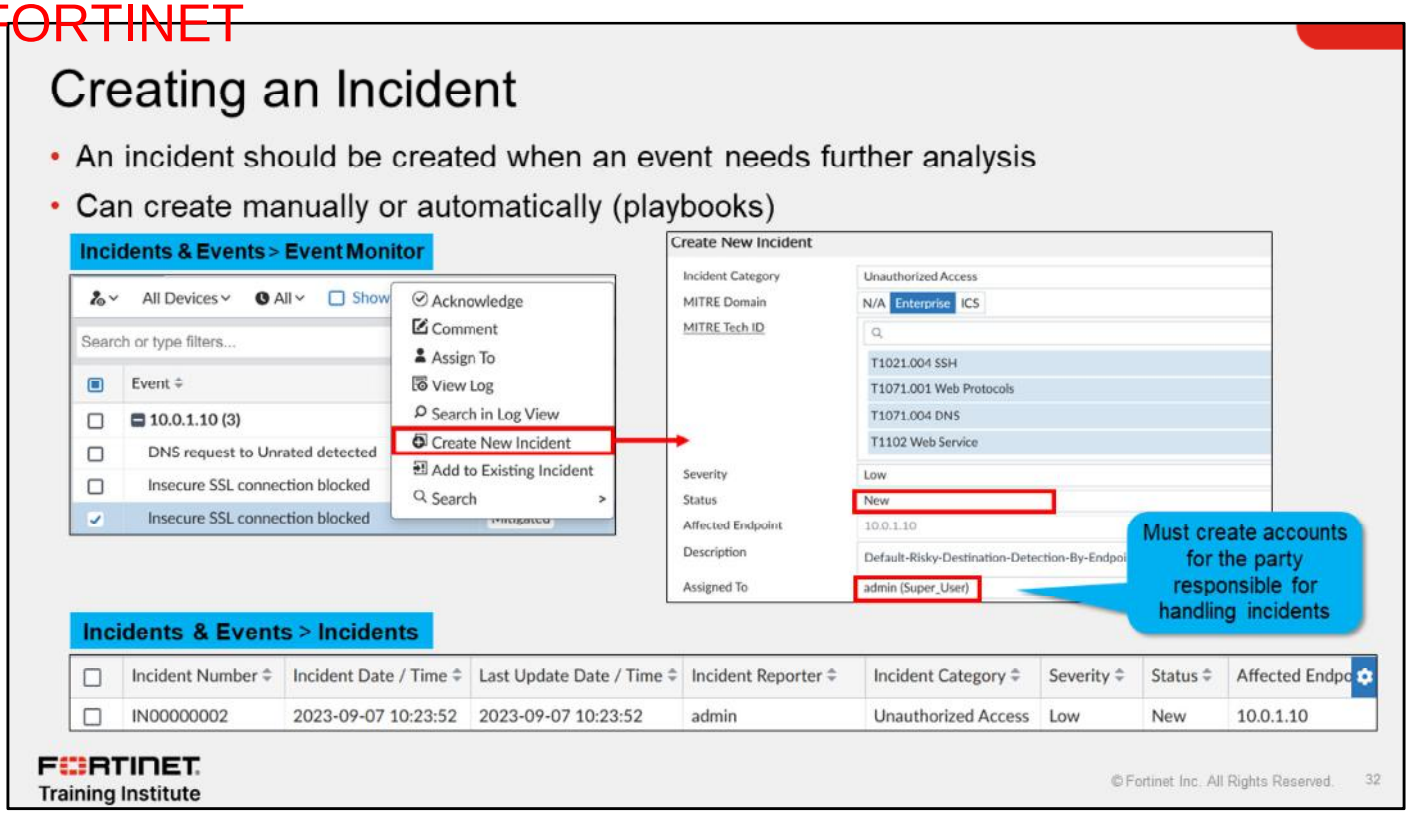
By demonstrating competence in creating and analyzing incidents, you will be able to investigate security incidents more efficiently in your organization.



The **Incidents** page is the central command center that allows security teams to manage, investigate, and respond to security threats efficiently.

An incident on FortiAnalyzer is a container for related security events. Key features of the **Incidents** page include prioritization at a glance, where interactive charts at the top provide immediate insights, allowing analysts to prioritize and filter incidents with ease.

The page also provides actionable intelligence, including the incident table, which places vital information, including columns like **Incident Name**, **Indicators**, and **Incident Reporter**, front and center for efficient decision-making.



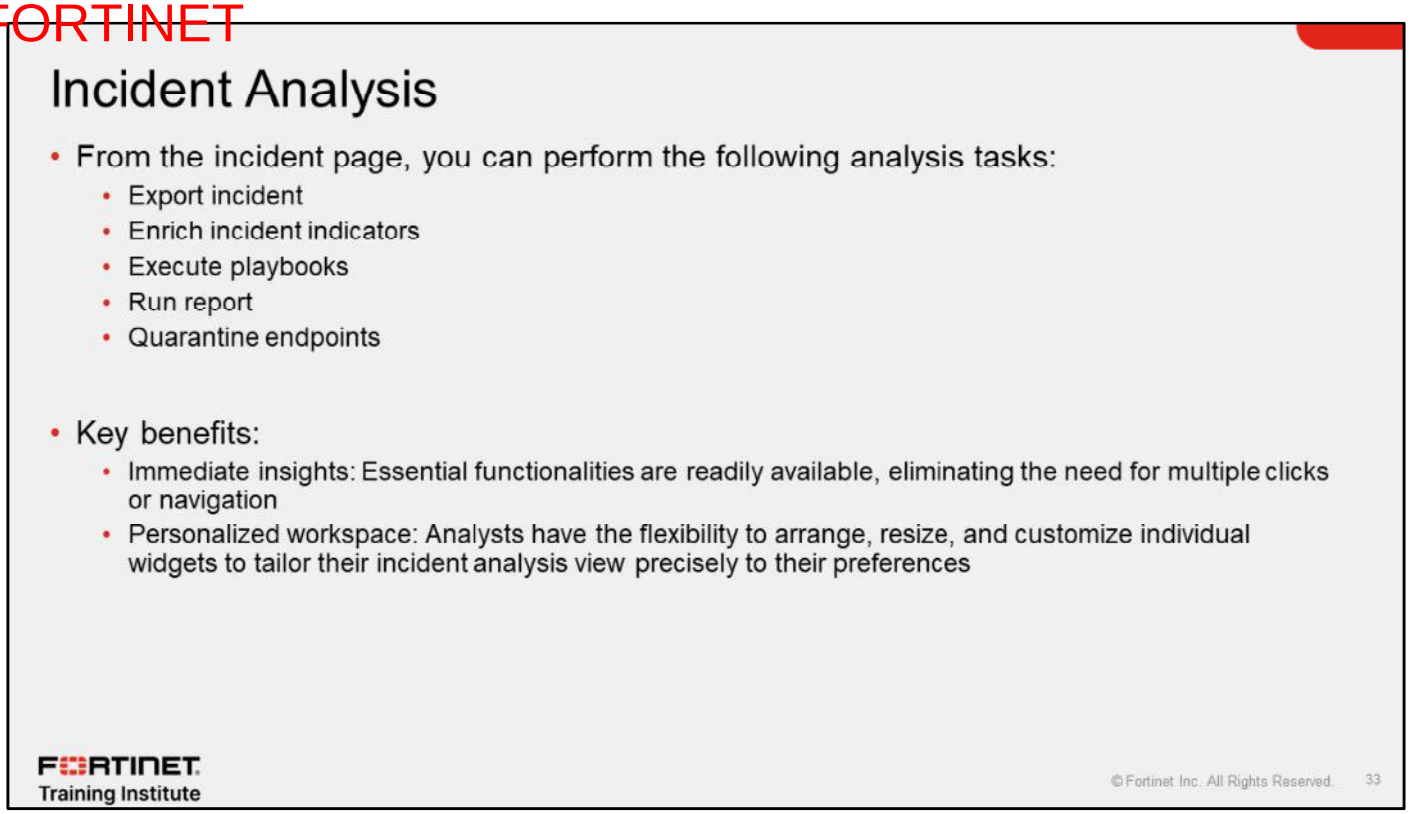
Not all events have the same impact on or importance in your network. Some events might need further analysis to prevent or mitigate security breaches. When you find an event that requires further scrutiny, you should create a new incident from that event. You can think of an incident as an event that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

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

In FortiAnalyzer, you create incidents manually by right-clicking the desired event and selecting the corresponding option.

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

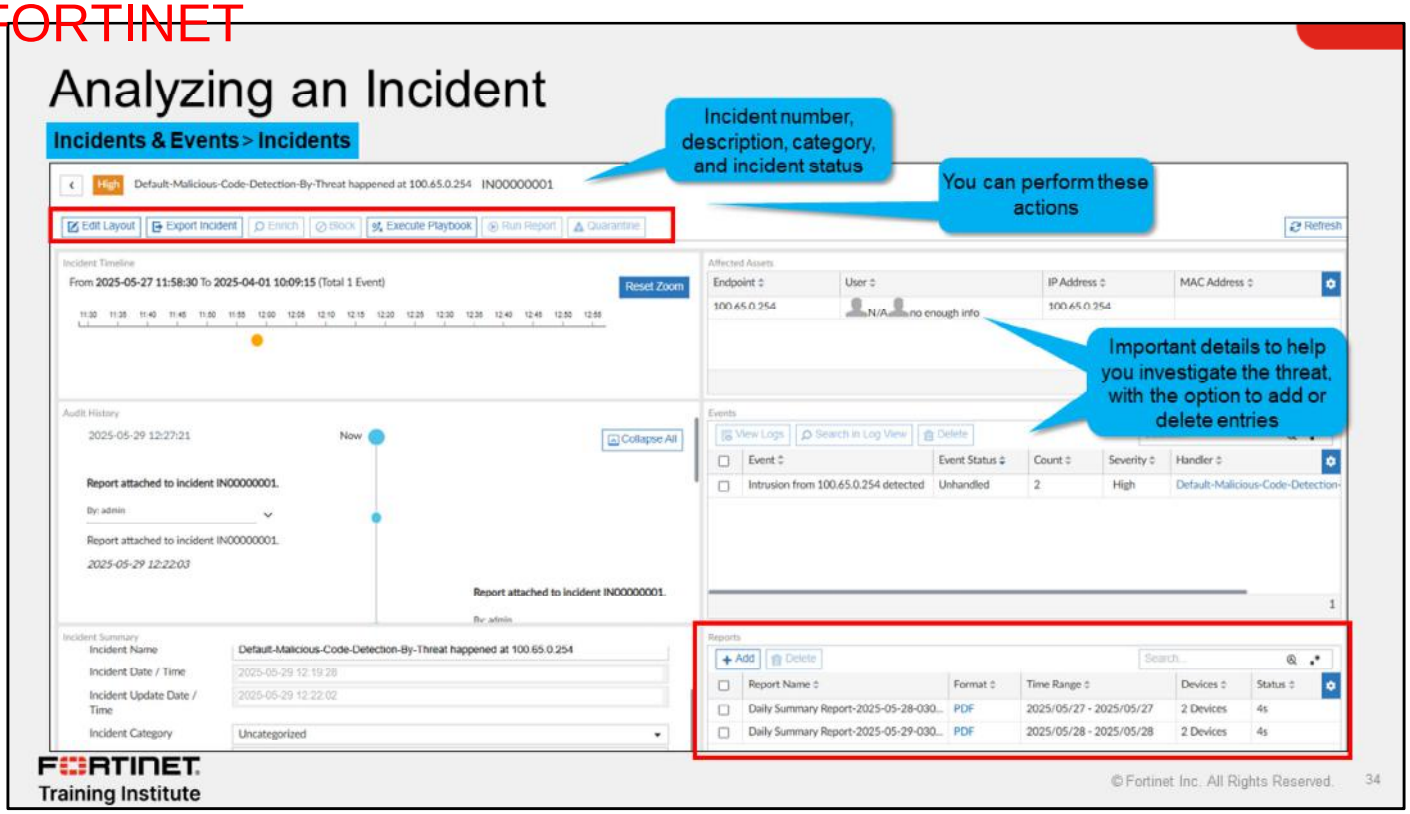
Once created, you can view incidents on the **Incidents** page.



Leveraging a customizable widget layout, you can now access all critical information and actions directly from a single, personalized dashboard.

From the incident page, you can perform the following analysis tasks: Export incident, enrich incident indicators, execute playbooks, run a report on the incident, and quarantine endpoints.

Key benefits include:
- Immediate insights: Essential functionalities are readily available, eliminating the need for multiple clicks or navigation. This translates to faster response times and improved efficiency.
- Personalized workspace: Analysts have the flexibility to arrange, resize, and customize individual widgets to tailor their incident analysis view precisely to their preferences.

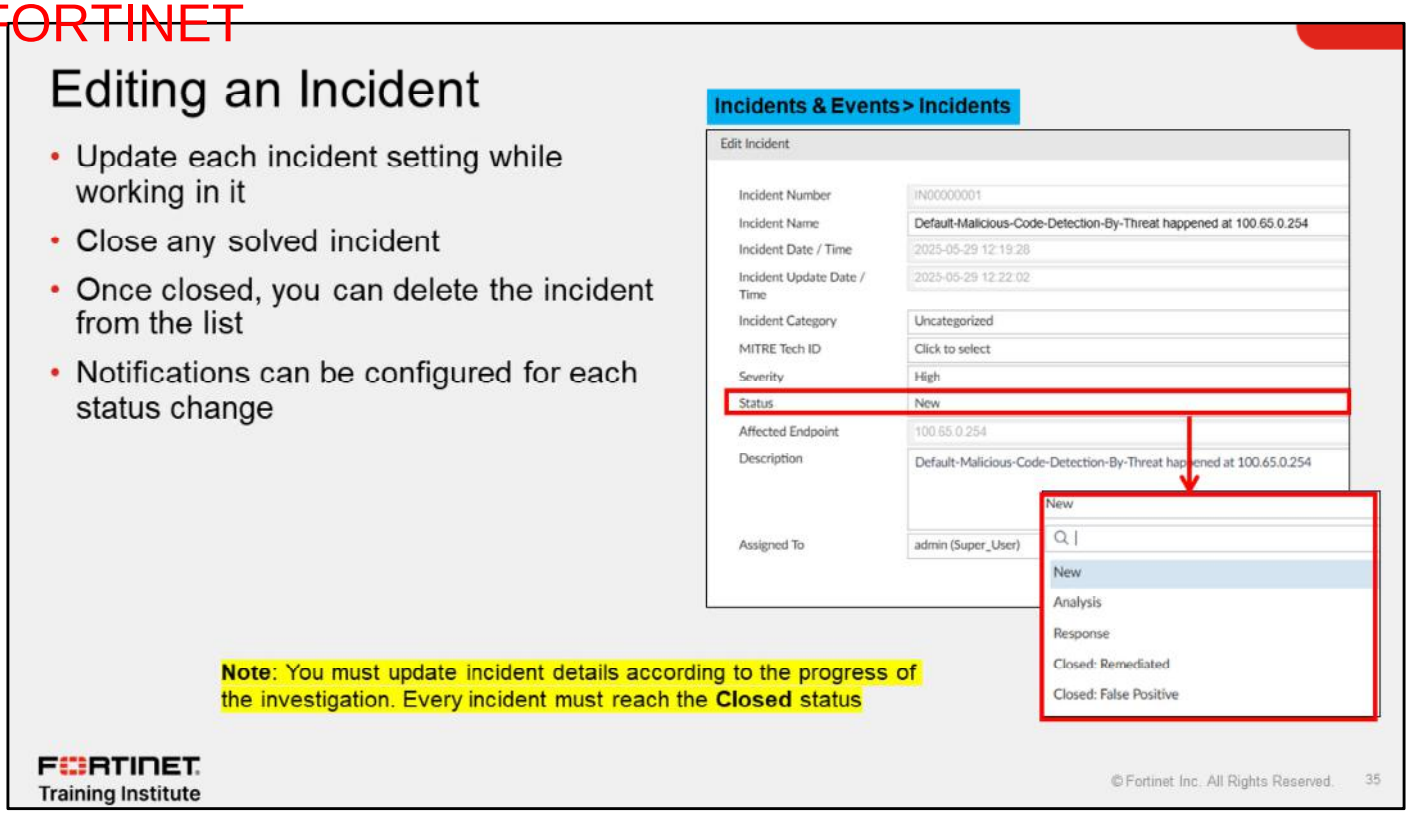


To view the details of an incident, go to **Incidents** and double-click the incident you want. You can also select an incident and then click **Analysis**.

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's timeline, the option to execute a playbook, audit history with any attached events and reports, and several more.

You can enrich indicators tied to the incident, block such indicators on FortiManager, and quarantine endpoints directly from the incident page.

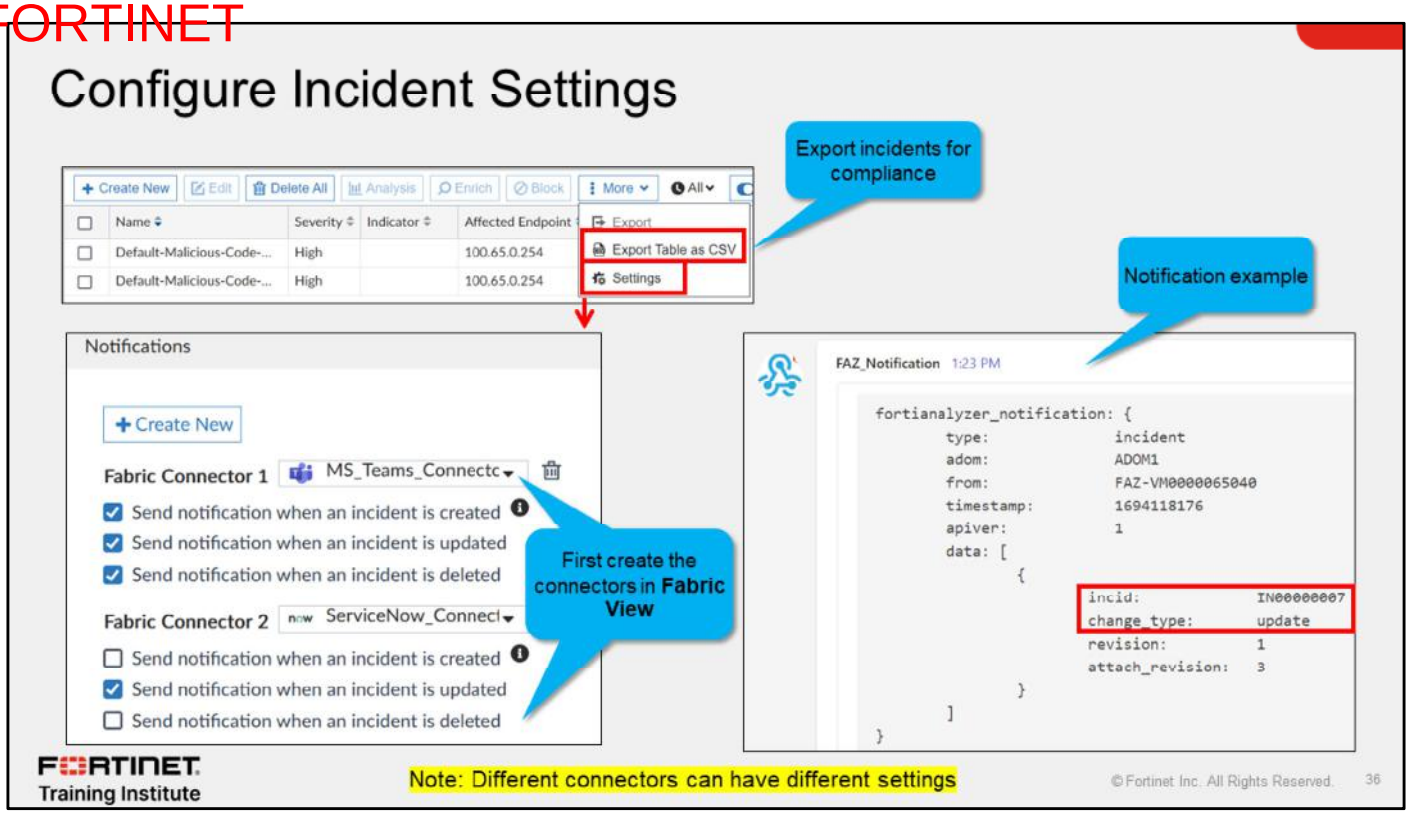
The list of events associated with the incident is also available under the tab with that name. From here, you can access the related logs by right-clicking the event of interest.



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

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.



Incidents usually undergo several stages during the analysis process. In most cases, it is important to notify all parties involved 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. For the notifications to be sent successfully, you must configure the receiving side of the connector. This slide shows a notification received in Teams for an updated incident.

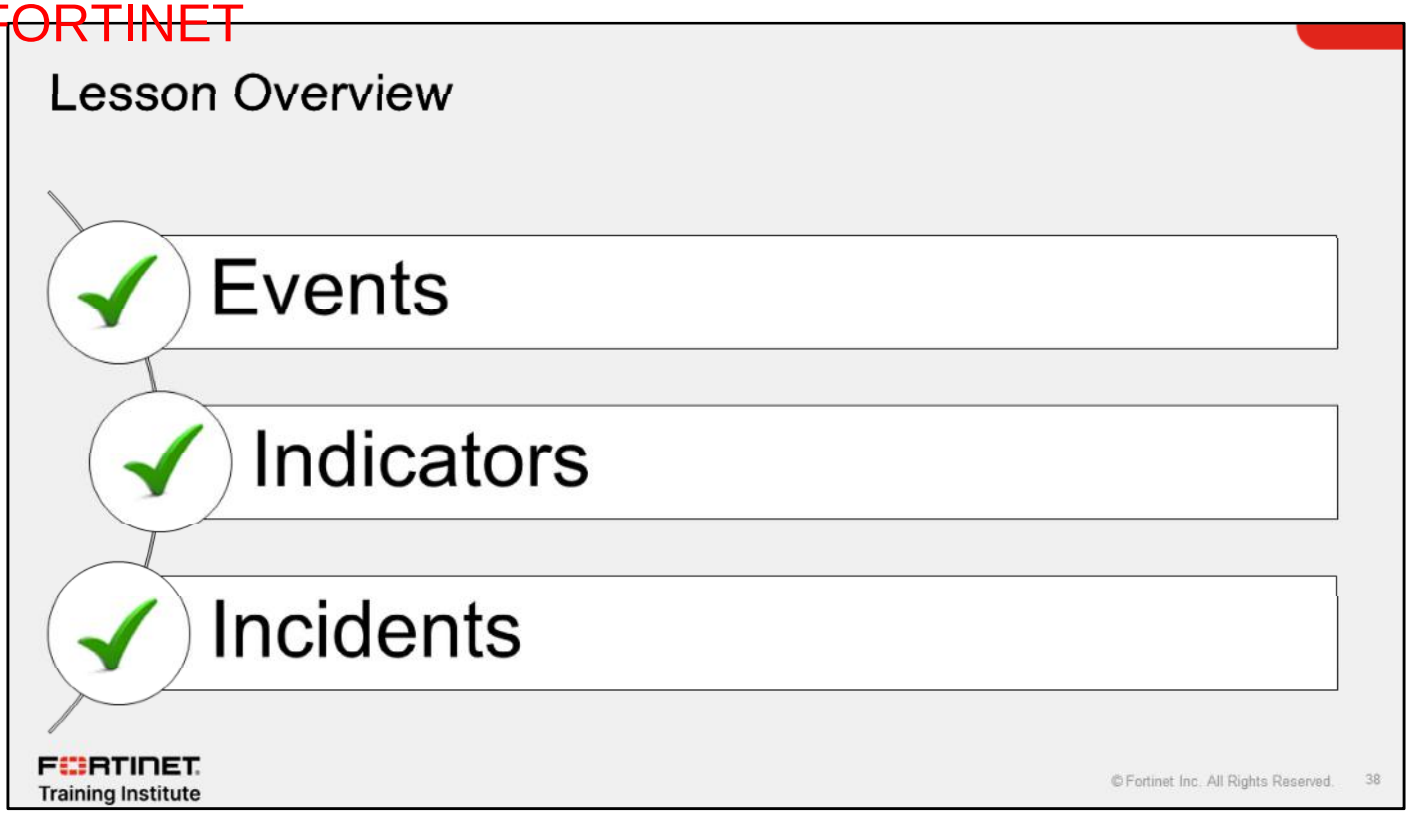
Knowledge Check

1. When would you raise an incident?
   - A. To change the status of an incident to **Unhandled**
   - ✓B. To further analyze events of interest

2. What is required to send notifications about incident updates?
   - ✓A. Existing Fabric connectors
   - B. Attaching a report to an incident

FORTINET Training Institute

 37



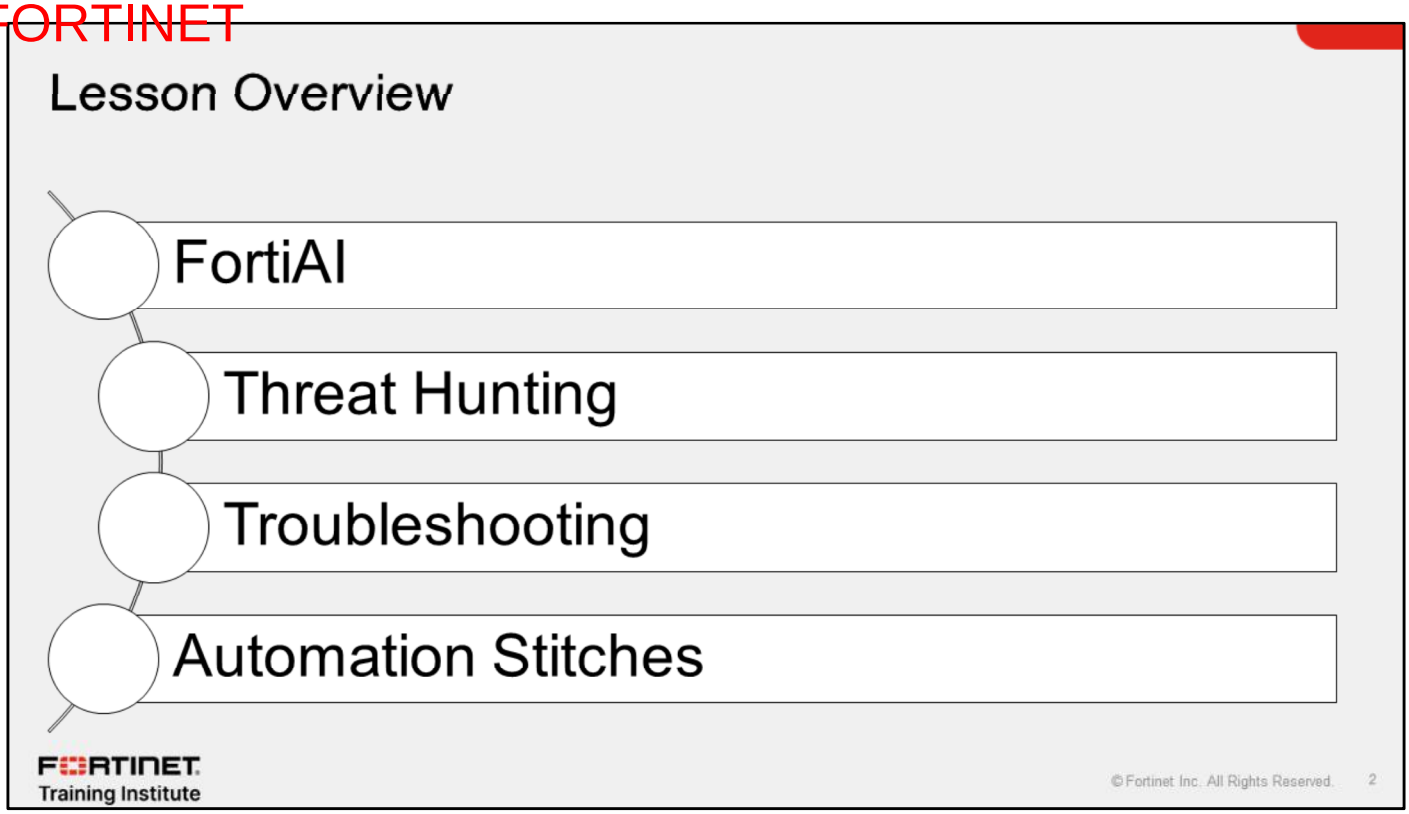
Congratulations! You have completed this lesson.

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

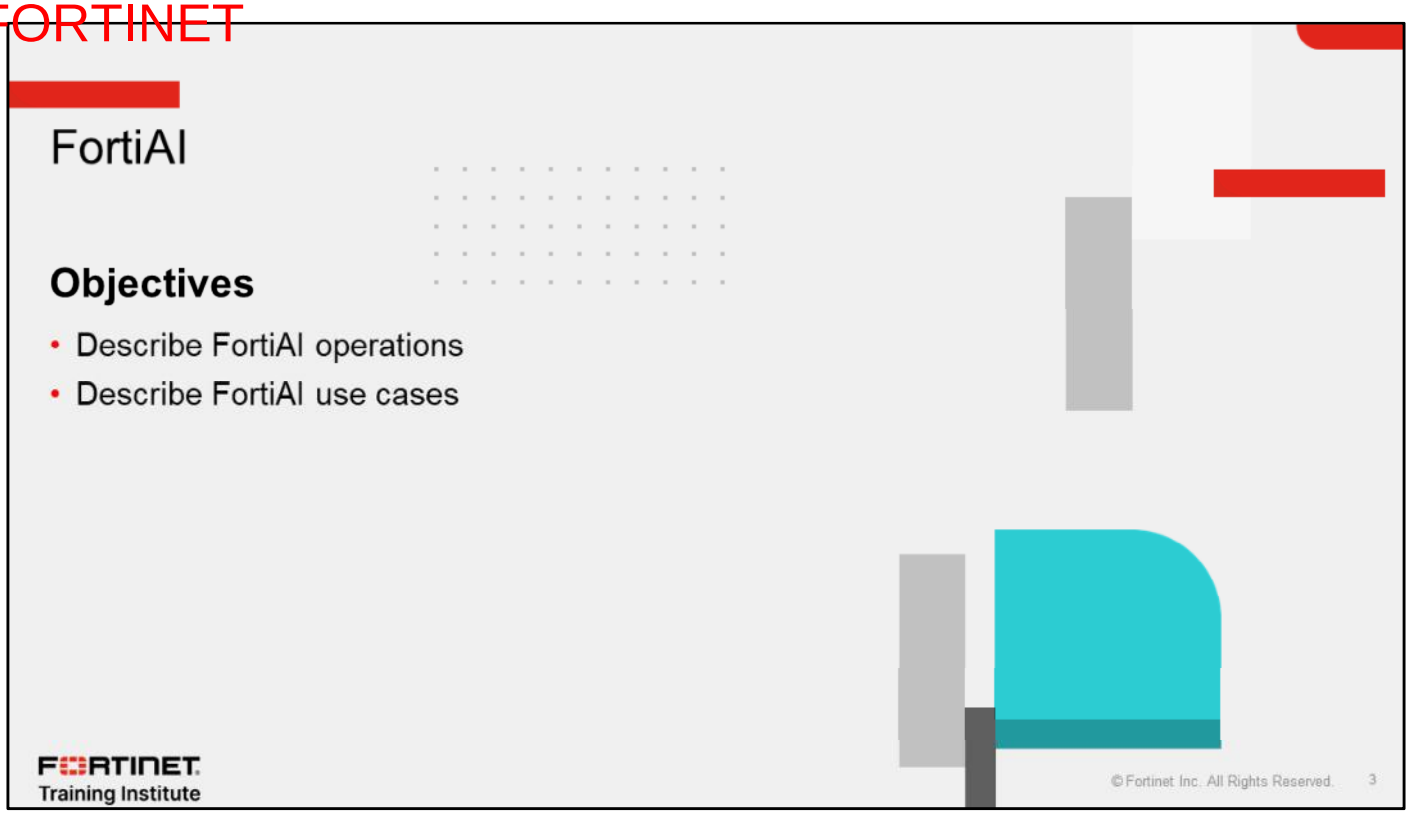
This slide shows the objectives that you covered in this lesson.

By mastering the objectives covered in this lesson, you learned about how to manage the various events, indicators, and incidents on FortiAnalyzer.

In this lesson, you will learn how to use FortiAI and other threat hunting tools on FortiAnalyzer.

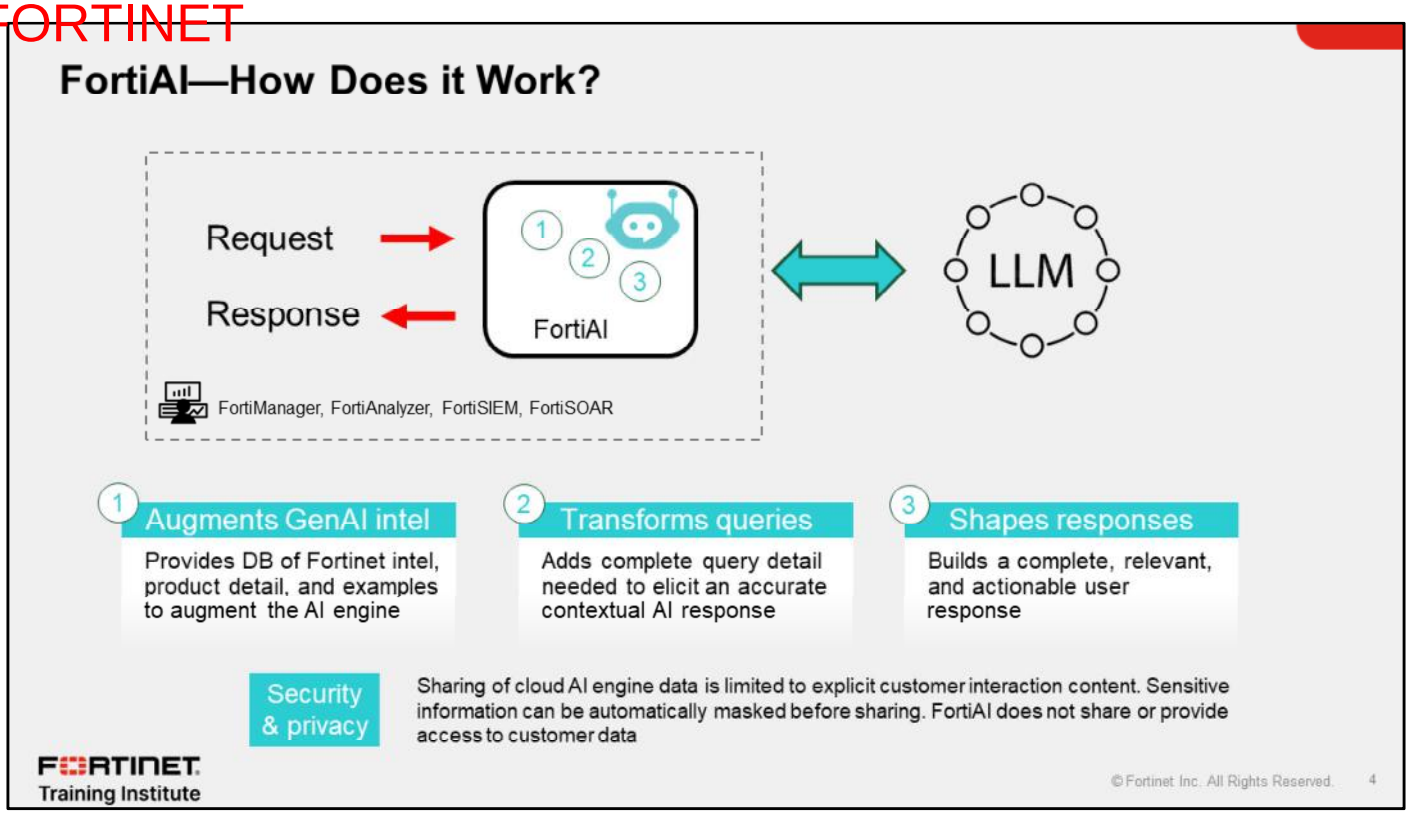


In this lesson, you will learn about the topics shown on this slide.



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

By demonstrating competence in describing FortiAI, you will be able to incorporate it into your workflow and automate many of your day-to-day activities.



FortiAI is not just a direct call to public generative AI (GenAI) services. Fortinet AI and product specialists continuously curate a database of proprietary threat intelligence, product-specific knowledge, use case examples, and more, serving as a supplemental data source to the GenAI model. When a user submits a prompt, relevant data from this database is also sent to the GenAI engine to provide a fully relevant contextual response. This process is known as retrieval-augmented generation (RAG).

However, producing an optimal response involves more than RAG. FortiAI converts simple natural language user prompts into precise queries that accurately reflect user intent and generate a contextual response. FortiAI then refines the received response to create a complete, relevant, and product-actionable user reply.

FortiAI Data Protection for FortiAnalyzer

Data protection	
Function callback	• Sends questions to the public LLM to generate a product-understandable query • Processes the query and the results locally
Data masking	• Masks IP addresses, MAC addresses, and usernames before sending to the public LLM • Unmasks data locally after the function callback
Secure proxy	• Passes all AI interactions through Fortinet proxies • Performs additional checks for data protection
Data privacy warnings	• Generates a warning prompt if data cannot be masked • Requires user confirmation before uploading to the public LLM

AI guardrails	
Defined boundaries	• Clear limits on AI capabilities • Unsupported queries generate "I'm not sure" or "I don't know" responses
Retrieval Augmented Generation	• Improves response accuracy by retrieving only relevant information • Provides references to support FortiAI responses

FORTINET Training Institute

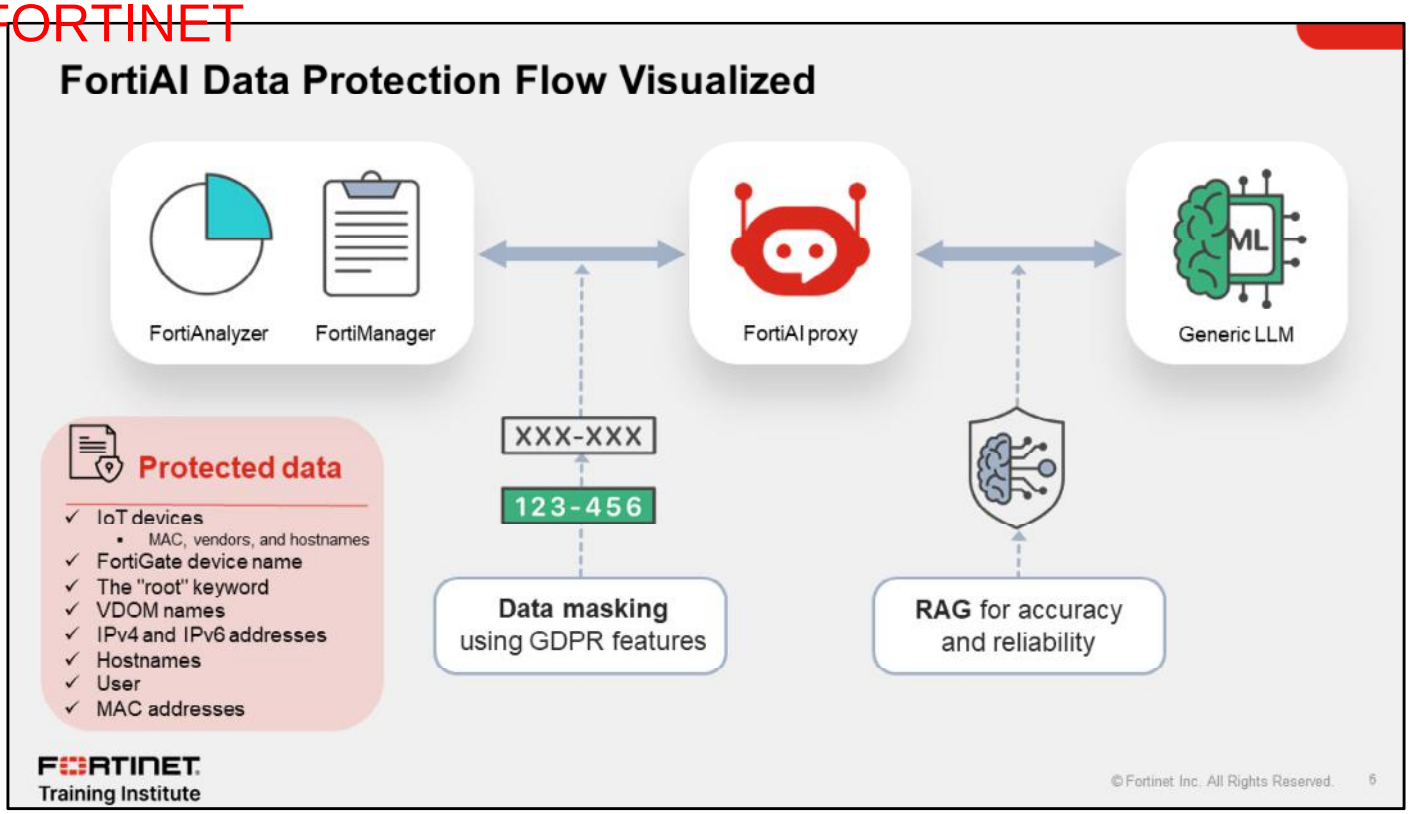
 5

Fortinet takes a multilayered approach to data protection.

Your query first goes to a public large language model (LLM). The LLM generates a product-specific query that the device can understand. Your local host then executes this generated query. This ensures that all results are processed directly on your premises. FortiAI automatically masks all sensitive information in queries—IP addresses, MAC addresses, and usernames. The LLM doesn't require this specific data to form the query. Once the function calls back to your local device, FortiAI unmasks the data locally, making it available on your system without ever exposing it to the cloud-based LLM in its original form.

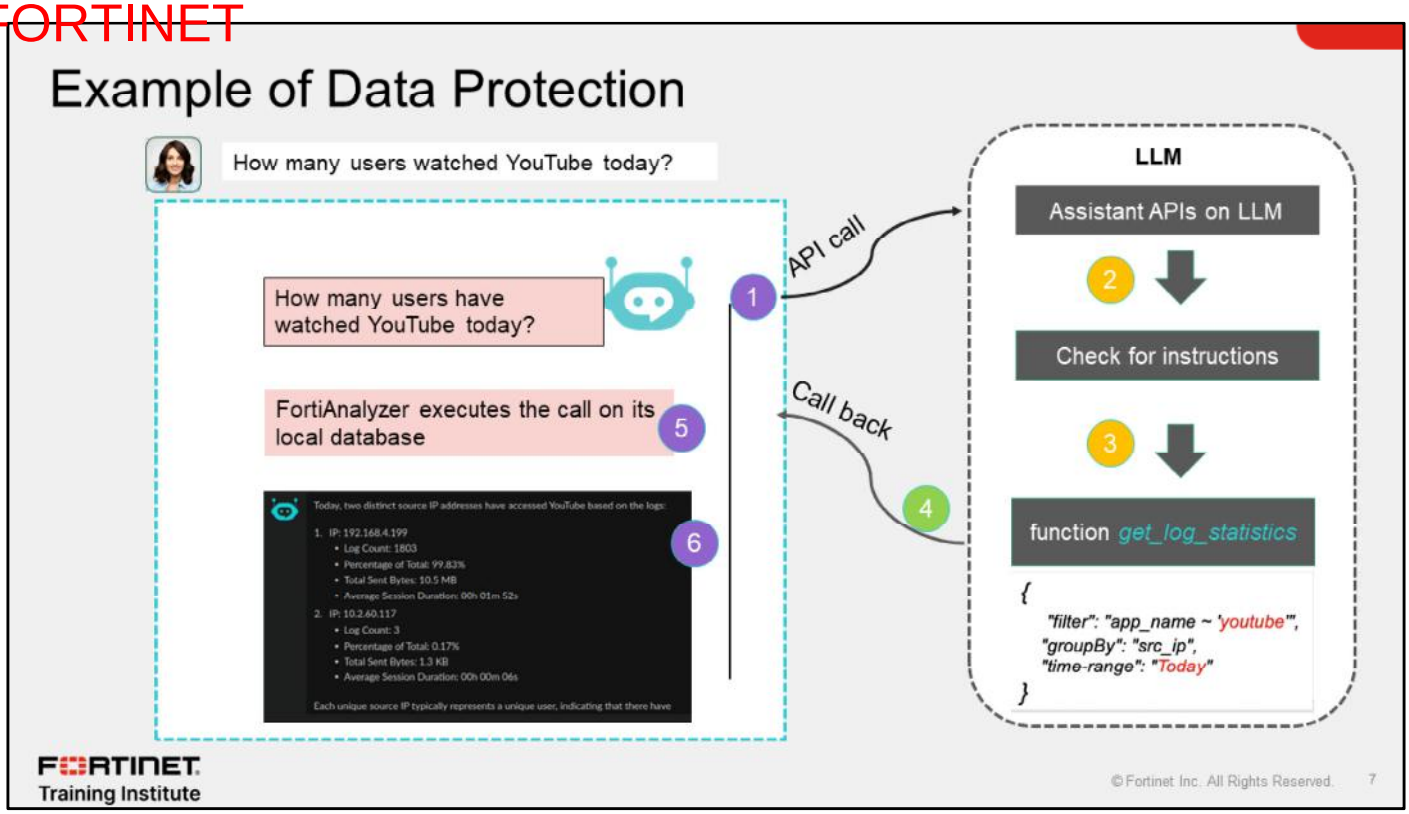
FortiAI routes all AI interactions through Fortinet proxies before they reach the LLM. The proxy performs additional security checks to ensure your data remains protected as it traverses the network. In scenarios where sensitive data, particularly in visual formats like images of network topologies, cannot be reasonably masked, FortiAI triggers a data privacy warning. This step gives you the option to confirm or cancel the upload before it's sent to the LLM.

The FortiAI assistant operates within explicitly defined boundaries. If an unsupported query is made (for instance, asking about weather, stock prices, or recipes), the AI will respond with "*I'm not sure*" or "*I don't know*". This mechanism prevents the AI from venturing into unrelated topics and helps maintain focus and security. RAG ensures the accuracy and relevance of the responses. This technology allows the AI to retrieve relevant information and provide references to support its answers.



This slide shows the flow of the proxied LLM connection from FortiAnalyzer. Requests are scrubbed with data masking on their way to the FortiAI proxy, which is hosted by Fortinet. The specific types of data that are protected are shown at the bottom left. These are examples and do not constitute the full list.

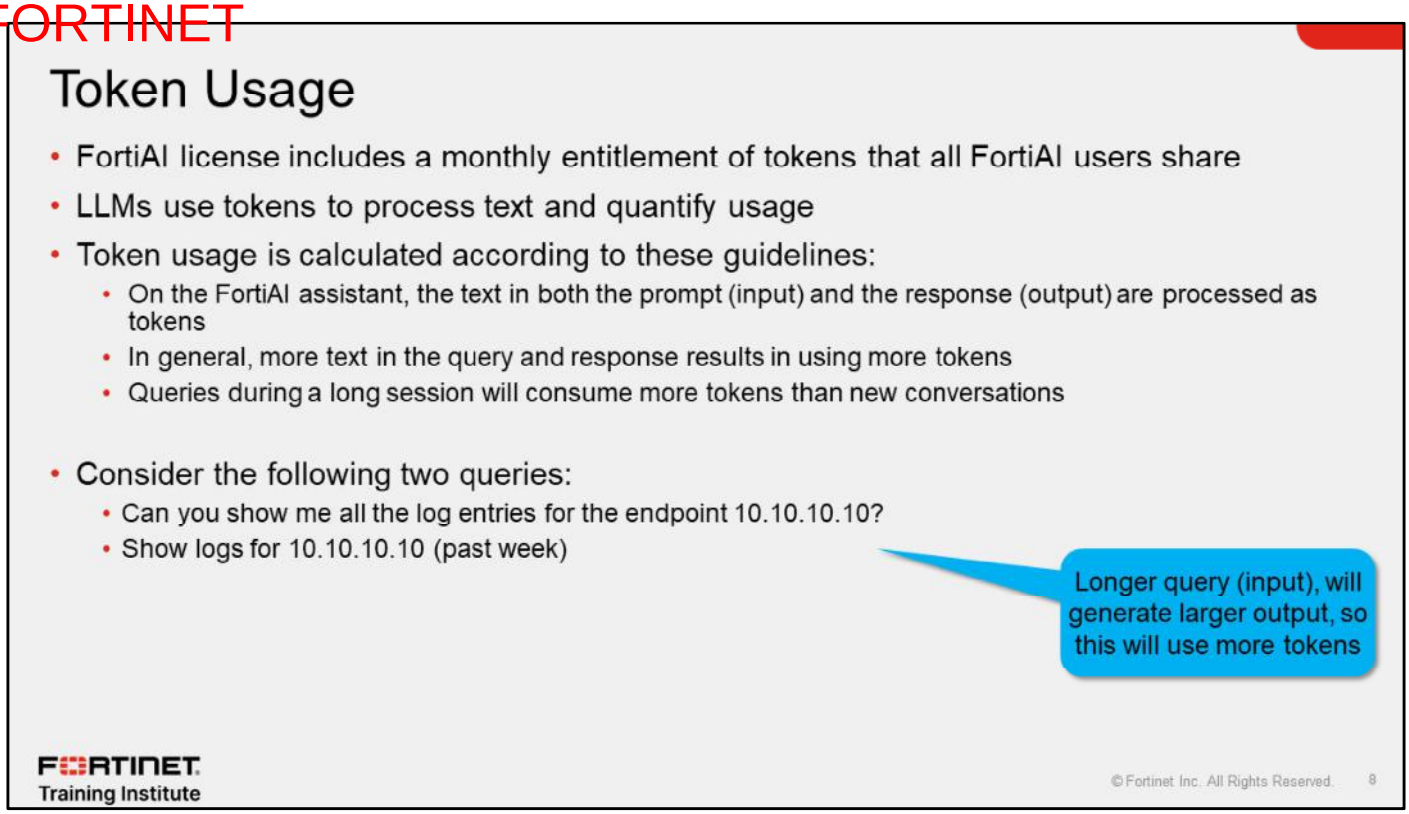
RAG, which is implemented between the proxy and the LLM, embeds several pieces of knowledge about FortiAnalyzer, such as the administrator guides, supporting documentation, Fortinet knowledge base, and others. This allows Fortinet to help restrict the answers and proposed actions by the FortiAI assistant to ensure they are relevant to the product, that the data supporting the AI response is from approved sources only, and minimize the chance of any irrelevant responses or unsupported actions.



This slide shows an example of data protection when using the FortiAI assistant on FortiAnalyzer. In this case, the user asks how many people have watched YouTube today. If you are the developer of an app that holds sensitive data, you could give the LLM access to the underlying logs, or you could send the relevant logs to the LLM to achieve a direct answer. However, this is neither safe nor desirable for data security reasons.

Instead, first, the FortiAI assistant determines if any of that sensitive information is needed to answer the query. FortiAnalyzer knows how to search for relevant logs and can be directed to do so with the appropriate query. It is not necessary to transmit any data about the logs themselves to answer the question. Instead, you need to know only the necessary query. The AI assistant hands this query to FortiAnalyzer, which conducts the search locally and provides the answer without the information ever having to leave FortiAnalyzer.

Now, suppose you make a query that does contain sensitive information, such as "*Show me how often the user at IP address* `10.10.10.209` *accessed YouTube today*". To form the query, you must send a value for the IP address to the proxy and then on to the LLM. The data scrubbing must replace the IP address `10.10.10.209` with something meaningless and irrelevant, such as `169.254.0.1`, and then ask the LLM to come back with the query. What is returned is a query that is formed to look for all instances of IP `169.254.0.1` accessing YouTube. The FortiAI assistant will simply replace the *dummy* value with the real IP address locally and run the query, which now gives you accurate results, without any sensitive information leaving the application.



The FortiAI license for FortiAnalyzer includes a monthly entitlement of tokens that all FortiAI users share.

LLMs use tokens to process text and measure usage. Token usage is calculated according to these guidelines:

- When you use the FortiAI assistant, both the prompt (input) and the response (output) are processed as tokens.
- While there isn't a strict one-to-one link between words or characters and tokens, generally, more text in the query and response results in using more tokens.
- Because the FortiAI assistant relies on session history to generate responses, queries during a long session will consume more tokens than those in new conversations.

Consider the following two queries:

- Can you show me all the log entries for the endpoint 10.10.10.10?
- Show logs for 10.10.10.10 (past week).

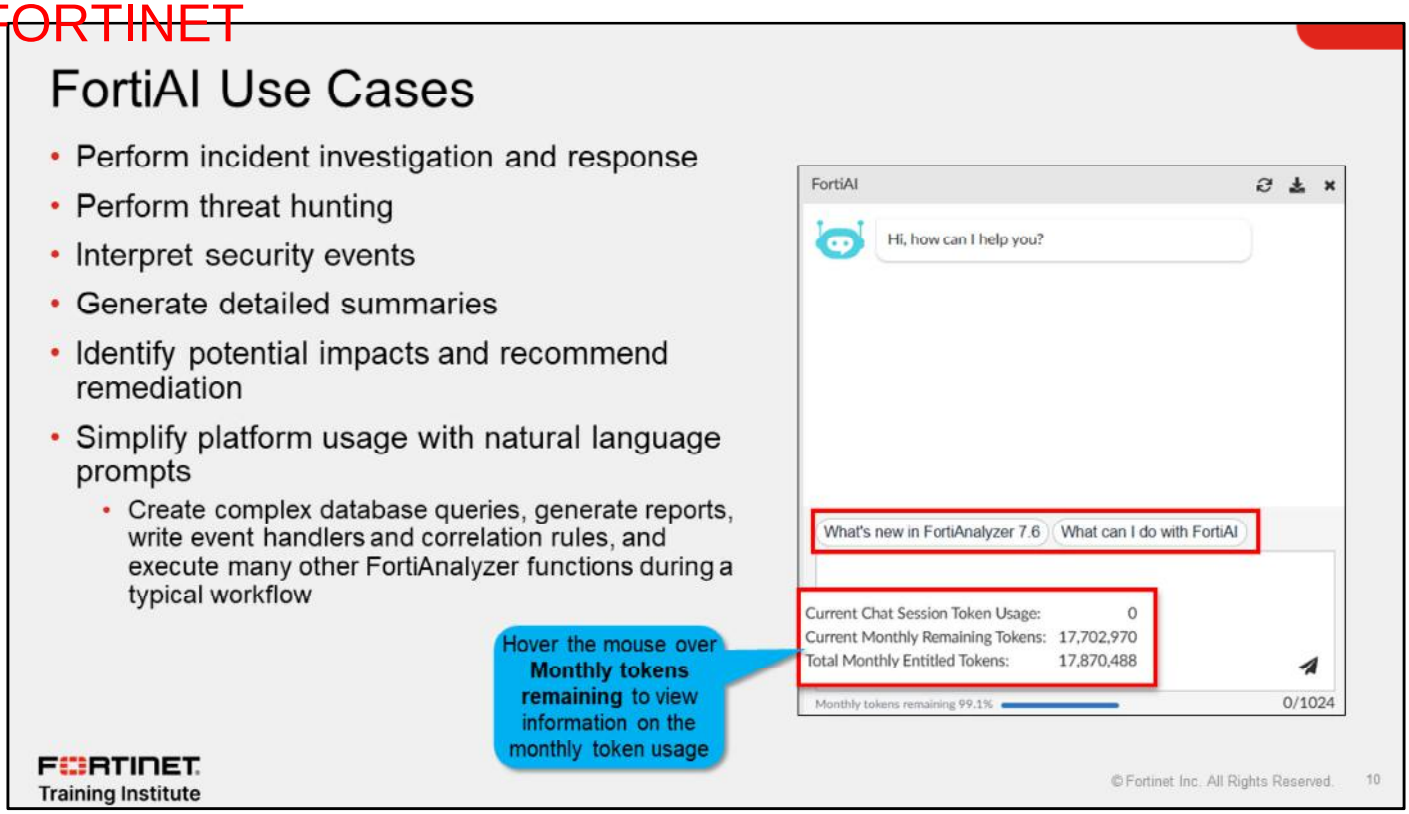
The total number of tokens used in the examples above depends on both the input (prompt) and the output (response). The first prompt contains more text, so it will use more tokens in the input. It also generates a larger response from FortiAI because it requests all log entries instead of just limiting the response to logs from the past week. Therefore, the first prompt will also use more tokens in the output.

When using FortiAI, your prompts should be directly related to the information the assistant is programmed to access, enabling efficient and effective data retrieval.

A valid prompt is a clear, well-defined question that the FortiAI assistant can easily interpret and process. It should be specific and relevant to the data or queries the FortiAI assistant is designed to handle. A valid prompt can be translated into precise SQL queries to retrieve accurate results on FortiAnalyzer.

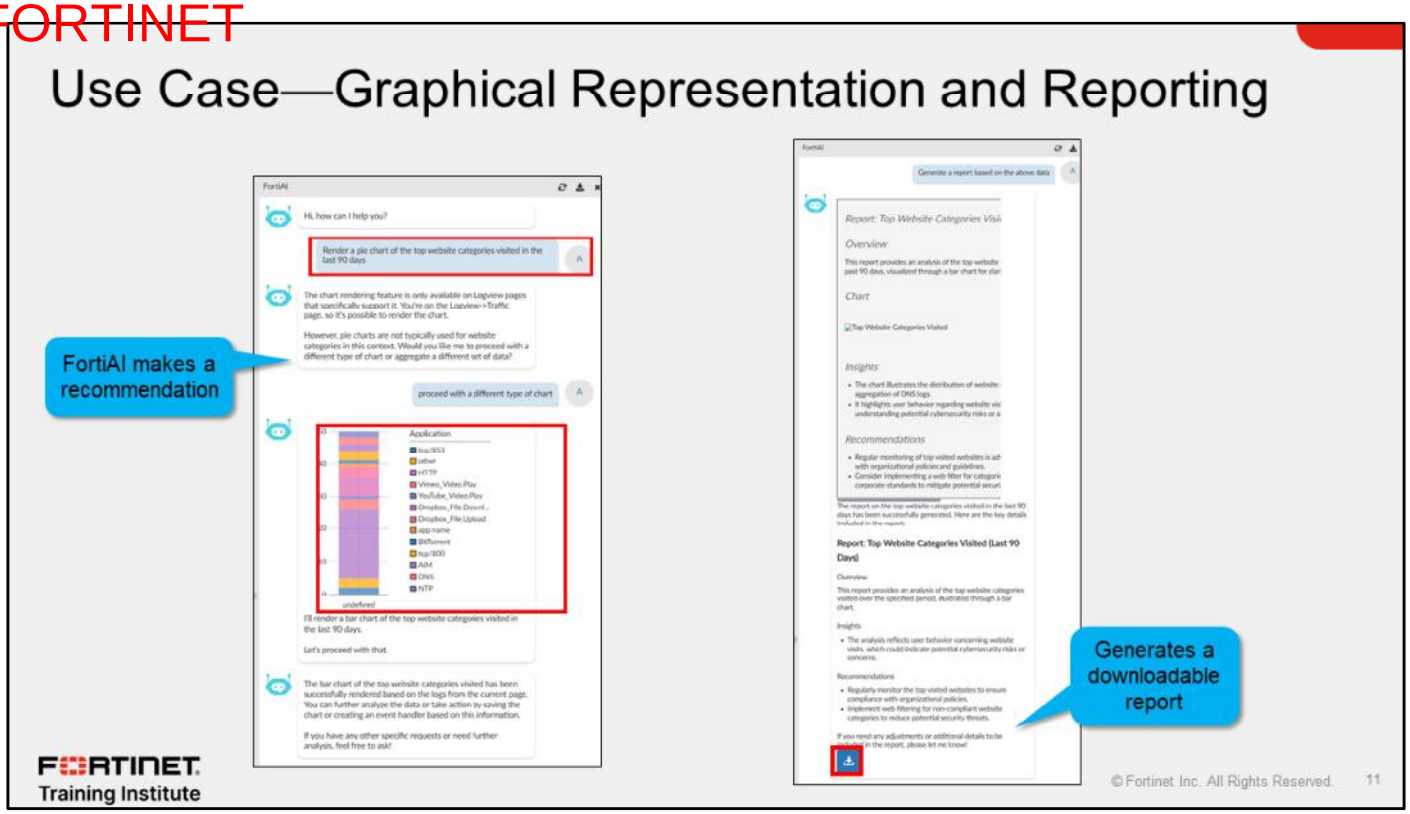
An invalid prompt is one that cannot be easily interpreted or processed by the FortiAI assistant. This typically includes prompts that are ambiguous, lack sufficient detail, or are outside the scope of the FortiAI assistant's capabilities.

Restarting the FortiAI assistant and eliminating the historical context is important for conserving tokens, so you should do this unless you really need to reference the chat's historical context to continue processing.



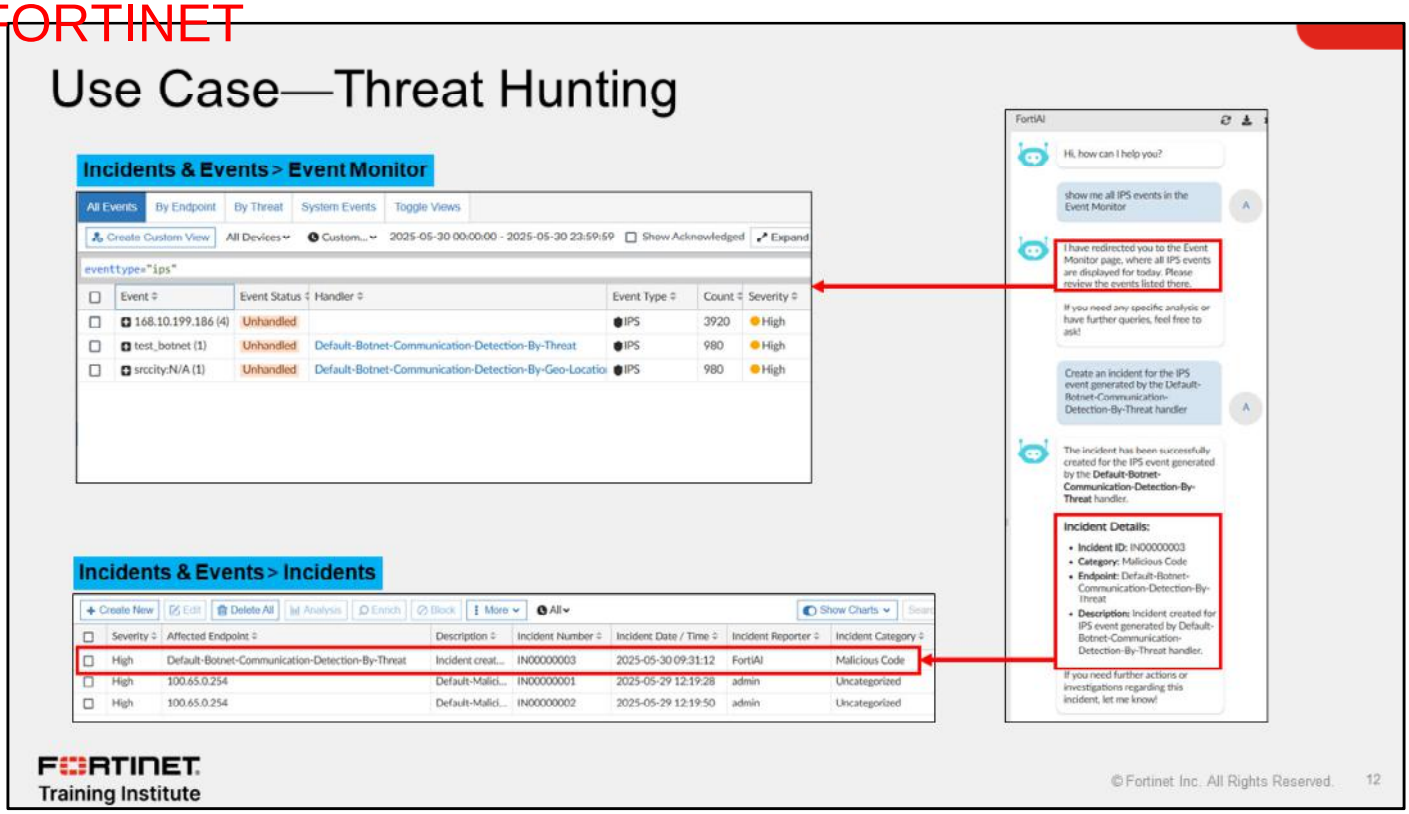
FortiAI can be used in FortiAnalyzer for incident investigation, response, and threat hunting. The assistant can interpret security events, generate detailed summaries, identify potential impacts, and make remediation recommendations.

FortiAI can also simplify platform usage with natural language prompts. For example, the assistant can create complex database queries, generate reports, write event handlers and correlation rules, and execute many other FortiAnalyzer functions during a typical workflow.



This slide shows how you can use FortiAI to generate a chart of the top website categories by application to make it easier to understand.

The image on the right shows how you can use FortiAI to generate a report based on the chart. FortiAI provides an action button to download the report.



This slide's example shows how you can use FortiAI to check for all intrusion prevention system (IPS) events generated in the event monitor. FortiAI redirects your FortiAnalyzer GUI page to the **Event Monitor** page.

Notice that the event handler **Default-Botnet-Communication-Detection-By-Threat** has generated an IPS event. This handler does not automatically create incidents when it generates an event, but you can ask FortiAI to create an incident based on this event.

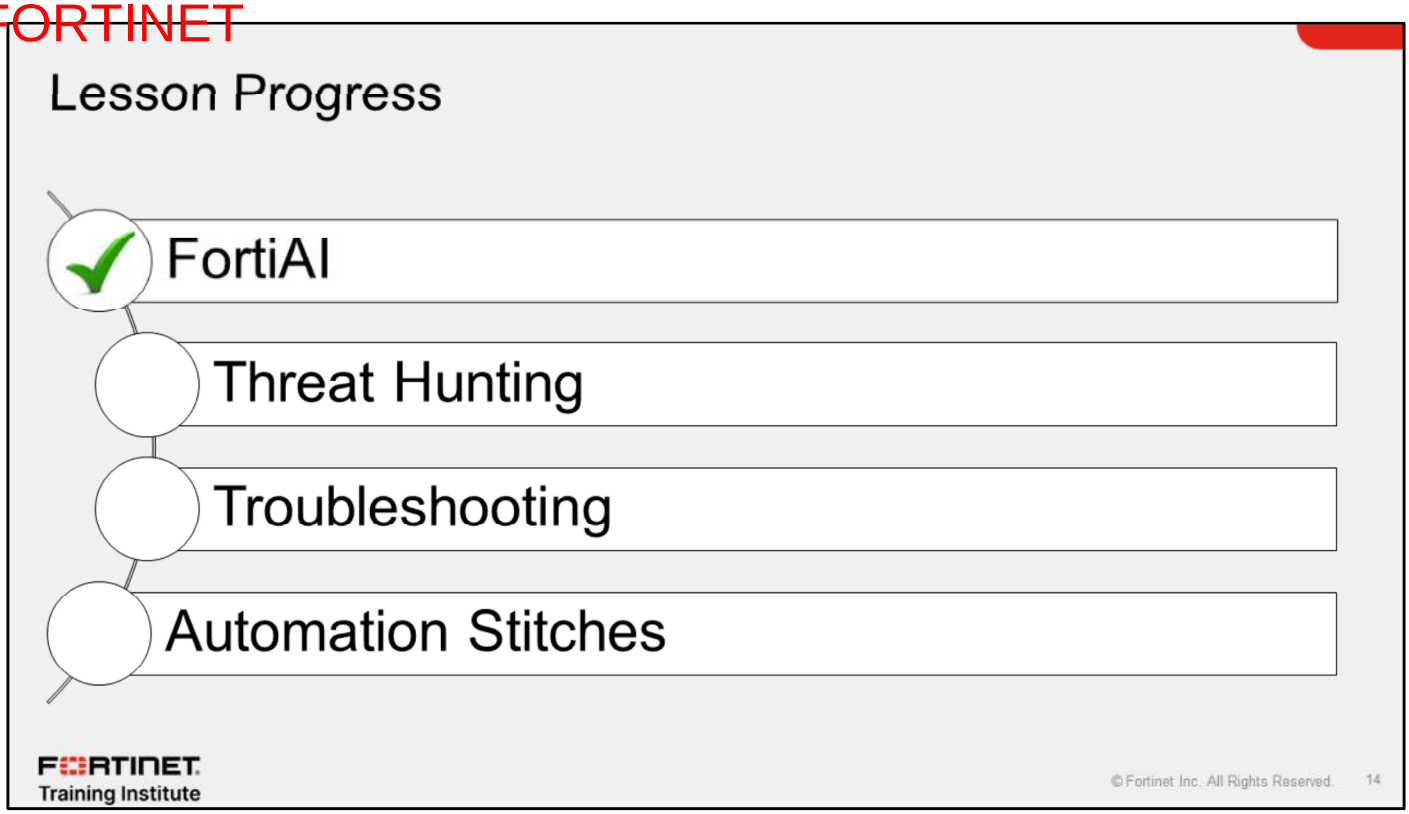
Knowledge Check

1. Which standard does FortiAI use when masking data for privacy and protection?
   - A. RAG
   - ✓B. GDPR

2. What is the purpose of retrieval-augmented generation (RAG) in FortiAI functionality?
   - ✓A. Provides references to support FortiAI responses.
   - B. Generates a warning prompt if sensitive data cannot be masked.

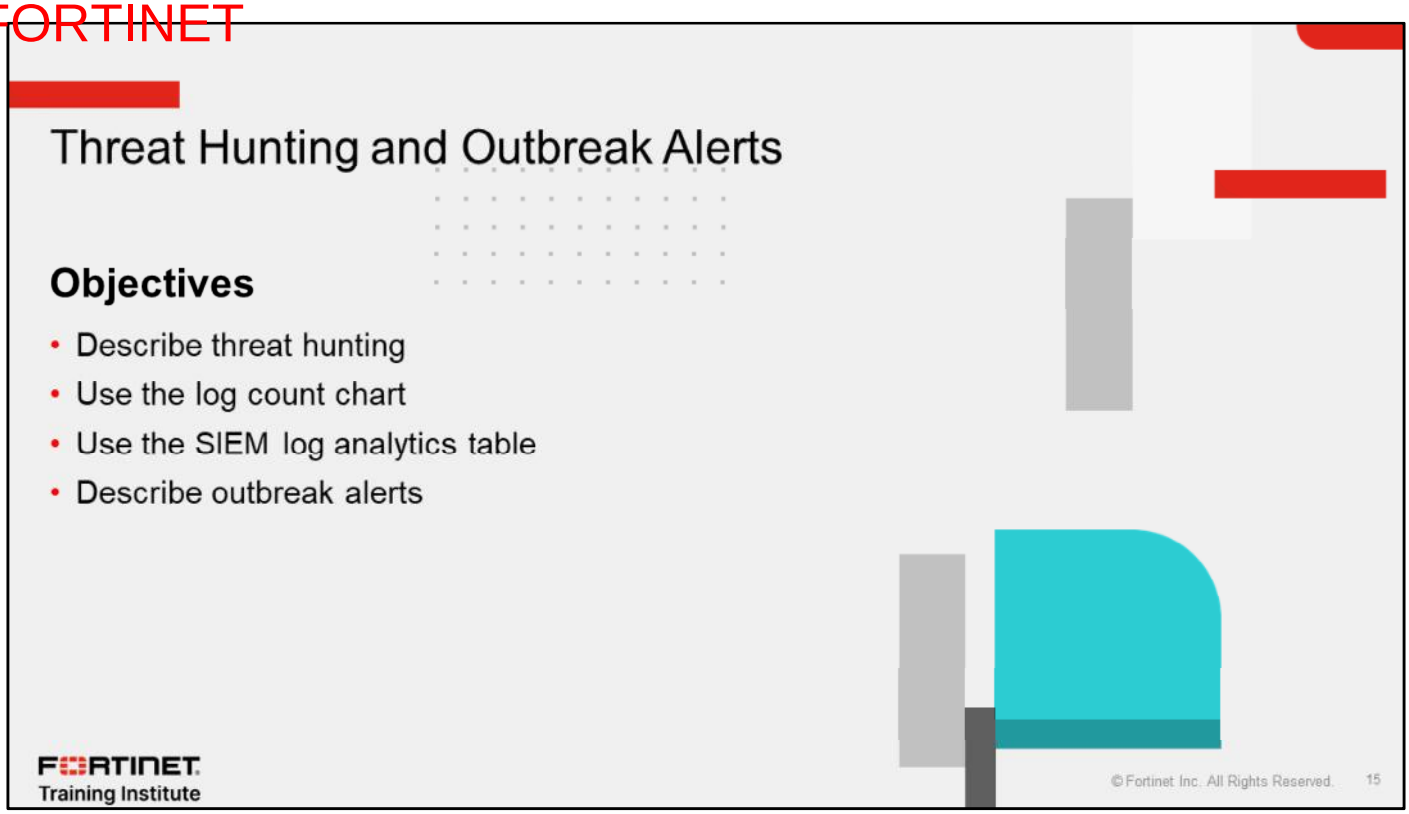
FORTINET Training Institute

 13



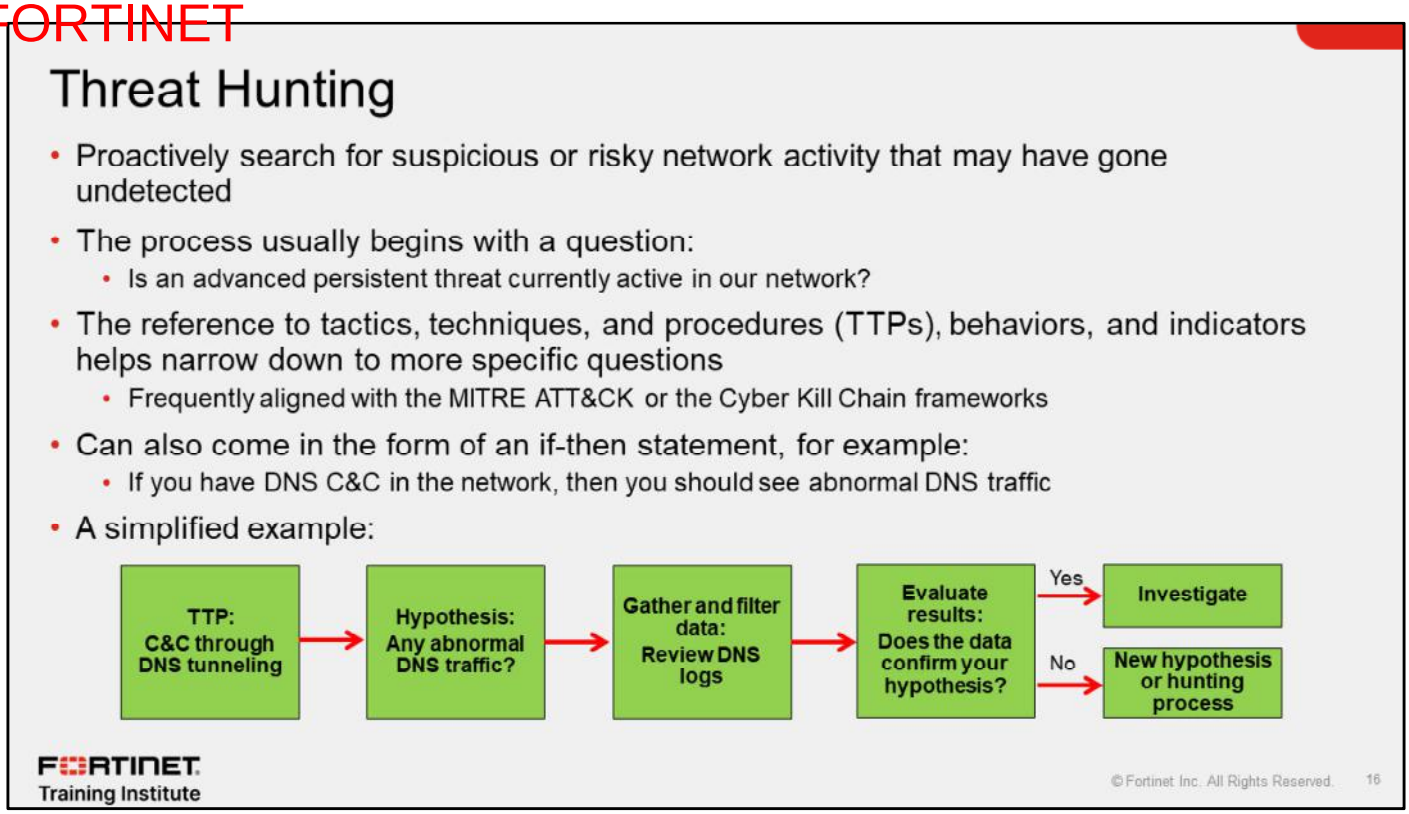
Good job! You now understand FortiAI.

Now, you will learn about FortiAnalyzer threat hunting.



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

By understanding how to use the threat hunting and outbreak alert tools, you will be able to take a more proactive approach in your SOC duties and keep your FortiAnalyzer updated with the latest outbreak information provided by FortiGuard.

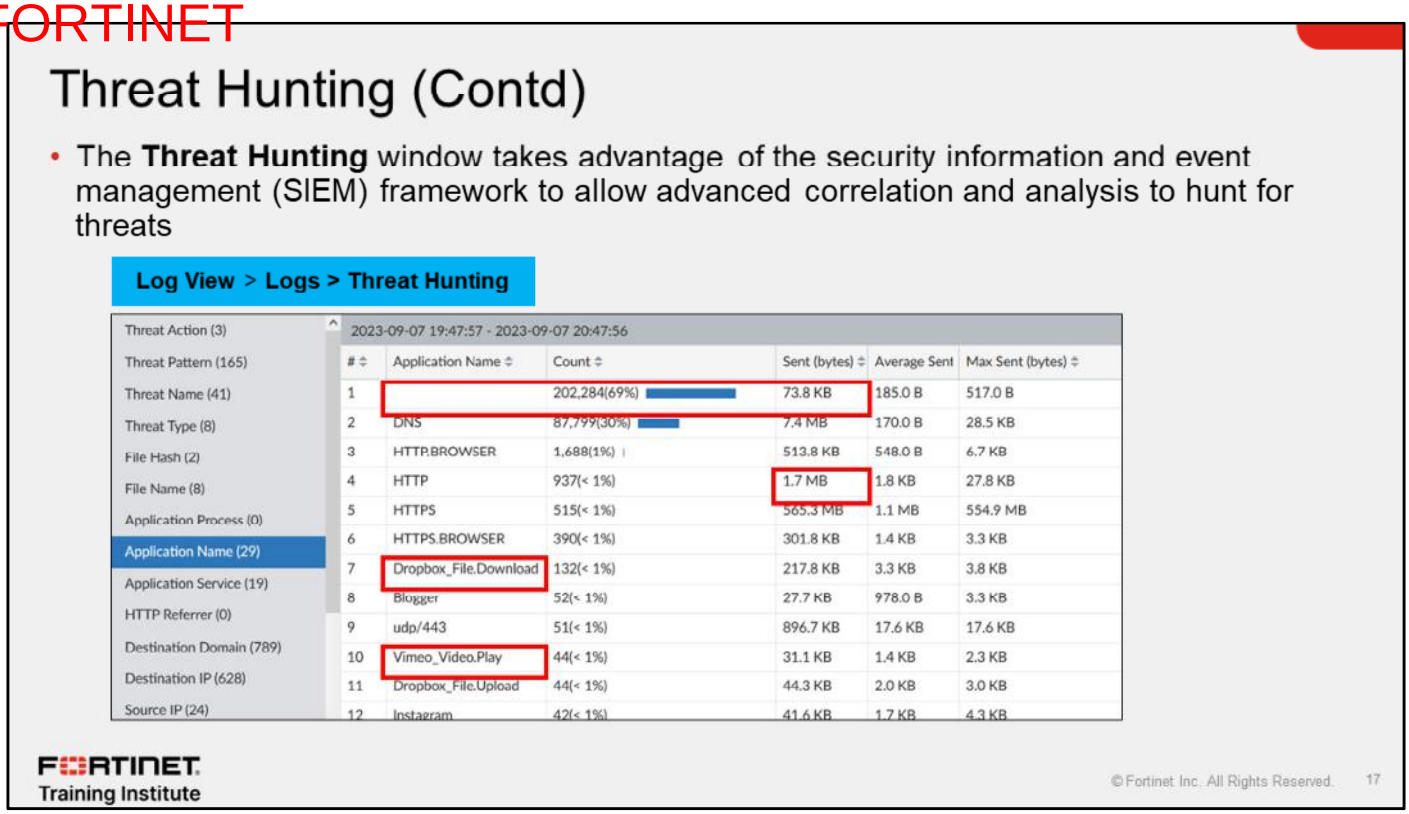


Threat hunting consists of proactively searching for suspicious or potentially risky network activity in your environment. The proactive approach helps the analyst find any threats that might have eluded detection by the current security solutions or configurations.

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 have a DNS command and control attack in your network, then you should see abnormal DNS traffic.

The process is frequently aligned to the MITRE ATT&CK or Cyber Kill Chain frameworks. This allows you to narrow down to more specific questions. The Cyber Kill Chain framework establishes a seven-step process to understand how a cyberattack is conducted and what steps you can take to secure your network. You can find more information on the Cyber Kill Chain framework on the Lockheed Martin website.

The frameworks are not mutually exclusive: You can use both frameworks together to help analyze and protect your network.



FortiAnalyzer's **Threat Hunting** window offers a SOC analytics dashboard using the SIEM database.

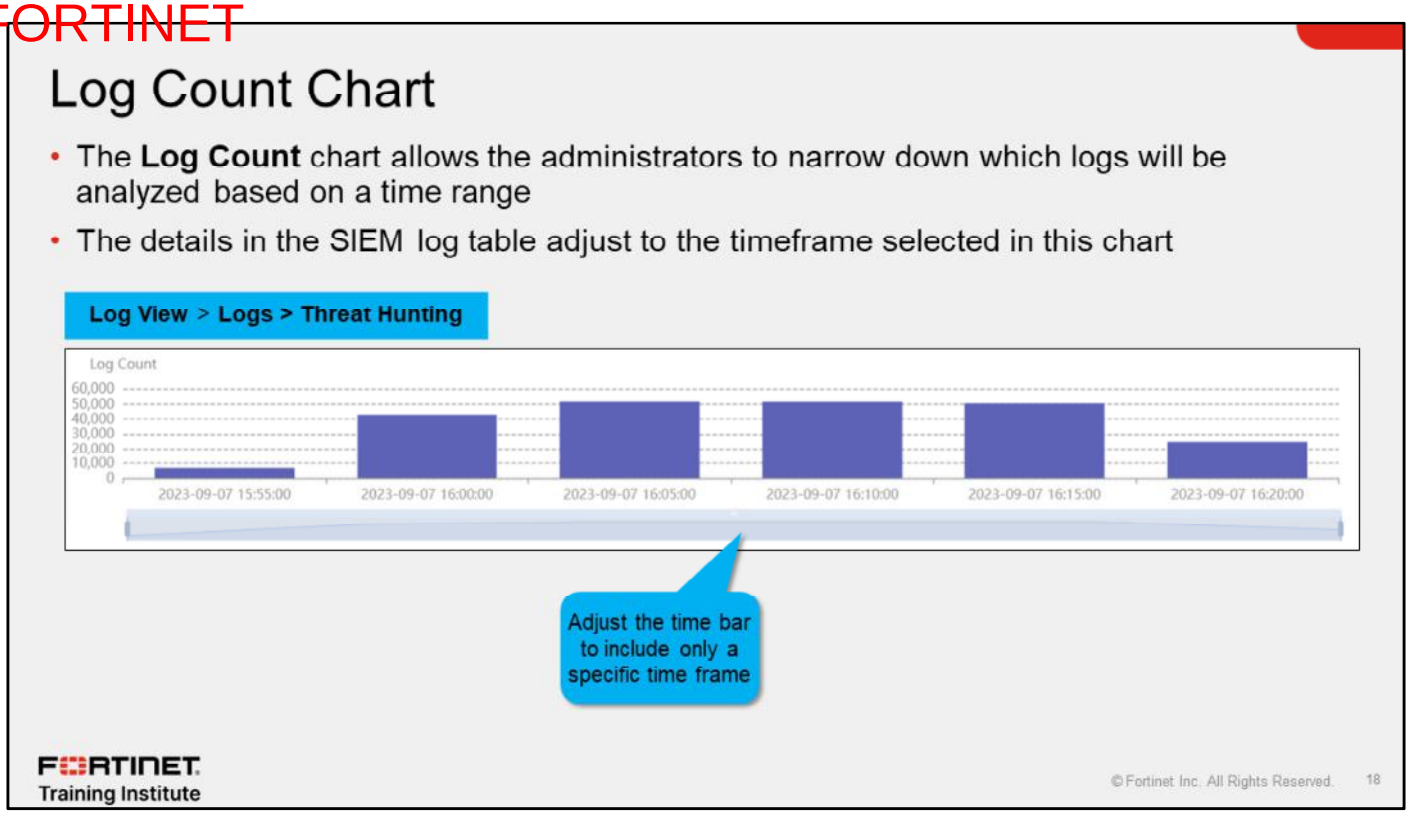
Threat Hunting uses cached data to allow SOC analysts to quickly drill down on logs in fields of interest. To view the **Threat Hunting** dashboard, click **Threat Hunting**. This dashboard includes a **Log Count** chart and SIEM log analytics table.

To change the displayed time range, select a time from the drop-down field in the upper-left corner of the dashboard. You can configure custom time ranges by selecting either **Last N Minutes**, **Last N Hours**, or **Last N Days**. Apply filters to the dashboard using **Add Filter** or by right-clicking a value in the table and selecting the corresponding filter. The SIEM log analytics table displays only logs matching the selected time range and filter.

In the left pane, click the field for which you want to view the corresponding data. The table displays 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.

By examining the information on this tool, you may produce a specific hypothesis. For example, based on the image on this slide, the following questions may arise:

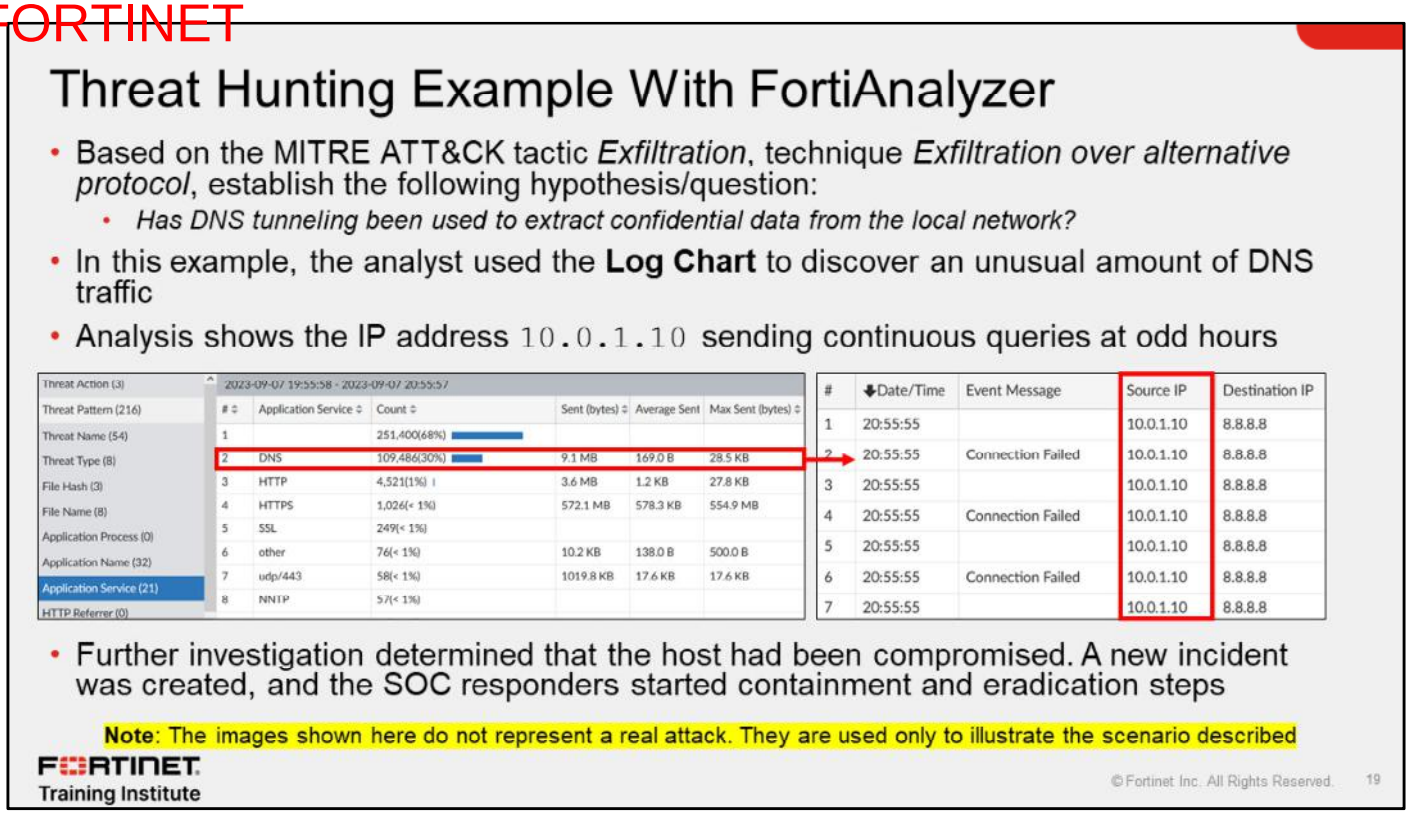
- Is the number of DNS logs for this time period expected?
- Is the amount of HTTPS data at this hour normal for your network?
- Should social media websites be allowed?
- Should cloud storage websites be allowed?



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 your mouse's scroll wheel 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 appear in the SIEM log analytics table.

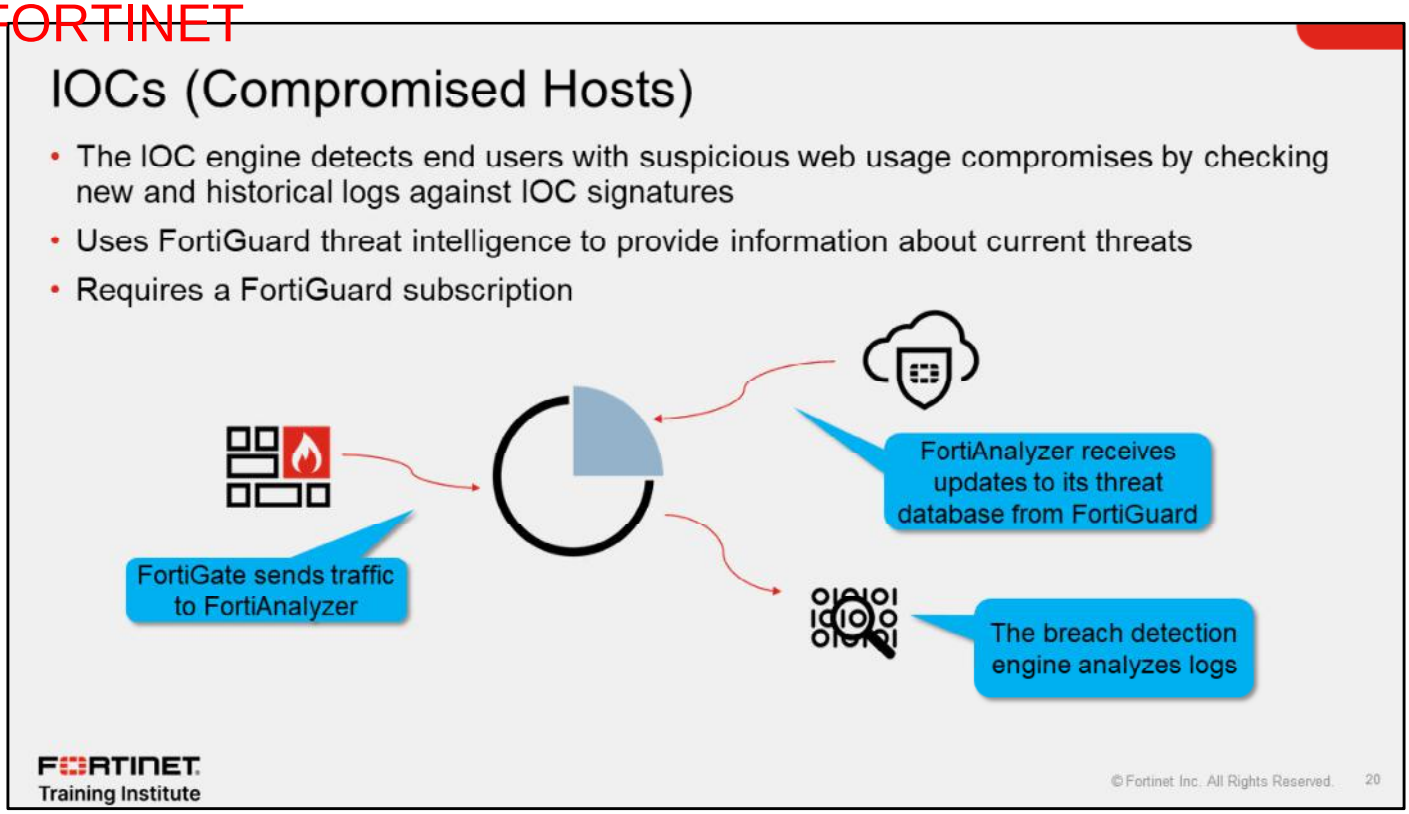


This slide illustrates an example of how an analyst can use FortiAnalyzer to perform a threat-hunting procedure.

Based on the MITRE ATT&CK framework, tactic *Exfiltration*, and technique *Exfiltration over alternative protocol*, the SOC team wants to answer the following question: *Has DNS tunneling been used to extract confidential data from the local network?*

Using the log chart, the analyst found that an unusual amount of DNS traffic was being generated, including outside normal business hours. By checking the details of the DNS logs, the analyst found that the host with IP address `10.0.1.10` was the main source for this abnormal traffic.

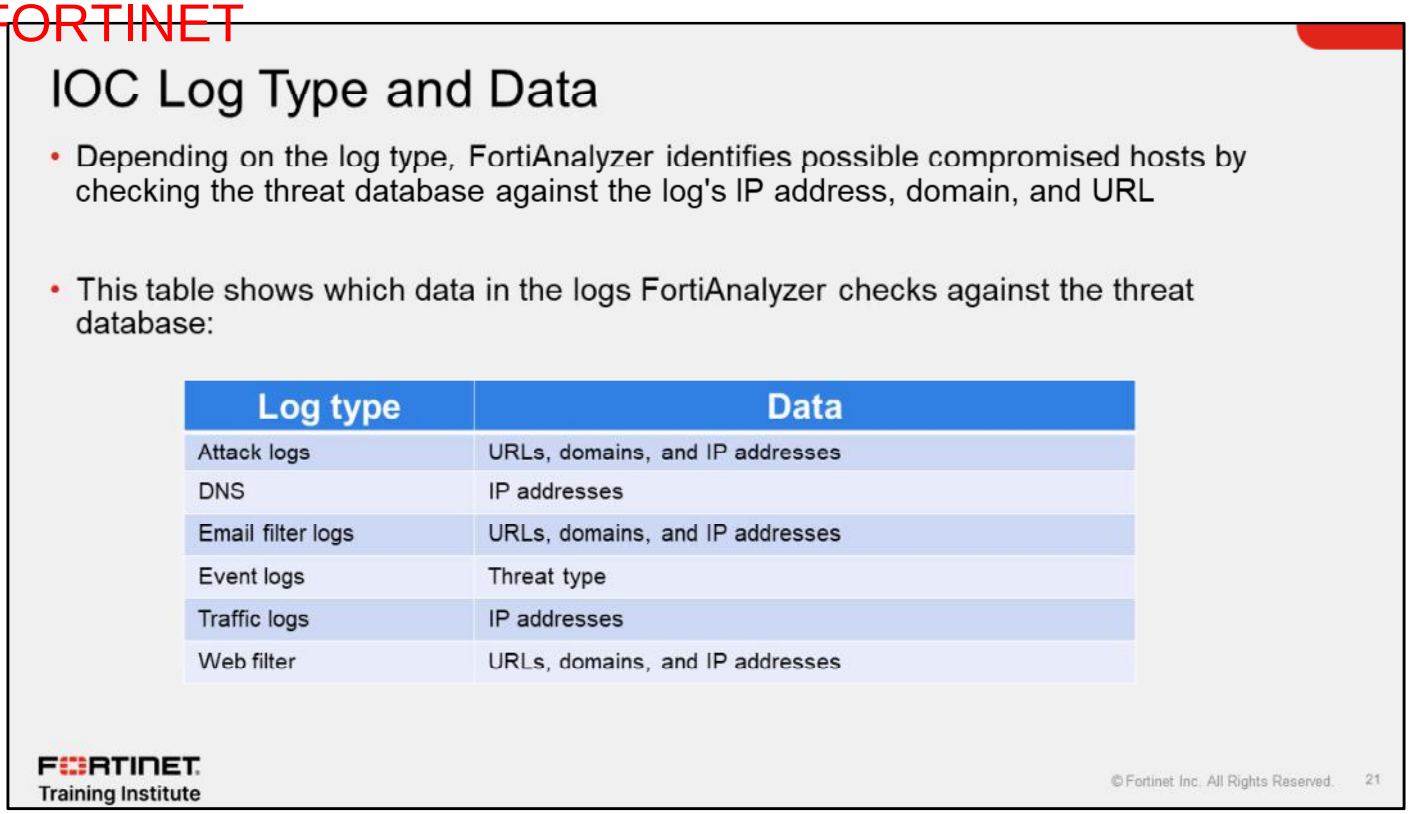
This triggered the creation of a new incident. The SOC team determined that the host had been compromised and proceeded to follow the steps in the company's security plan to contain and eradicate this breach.



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

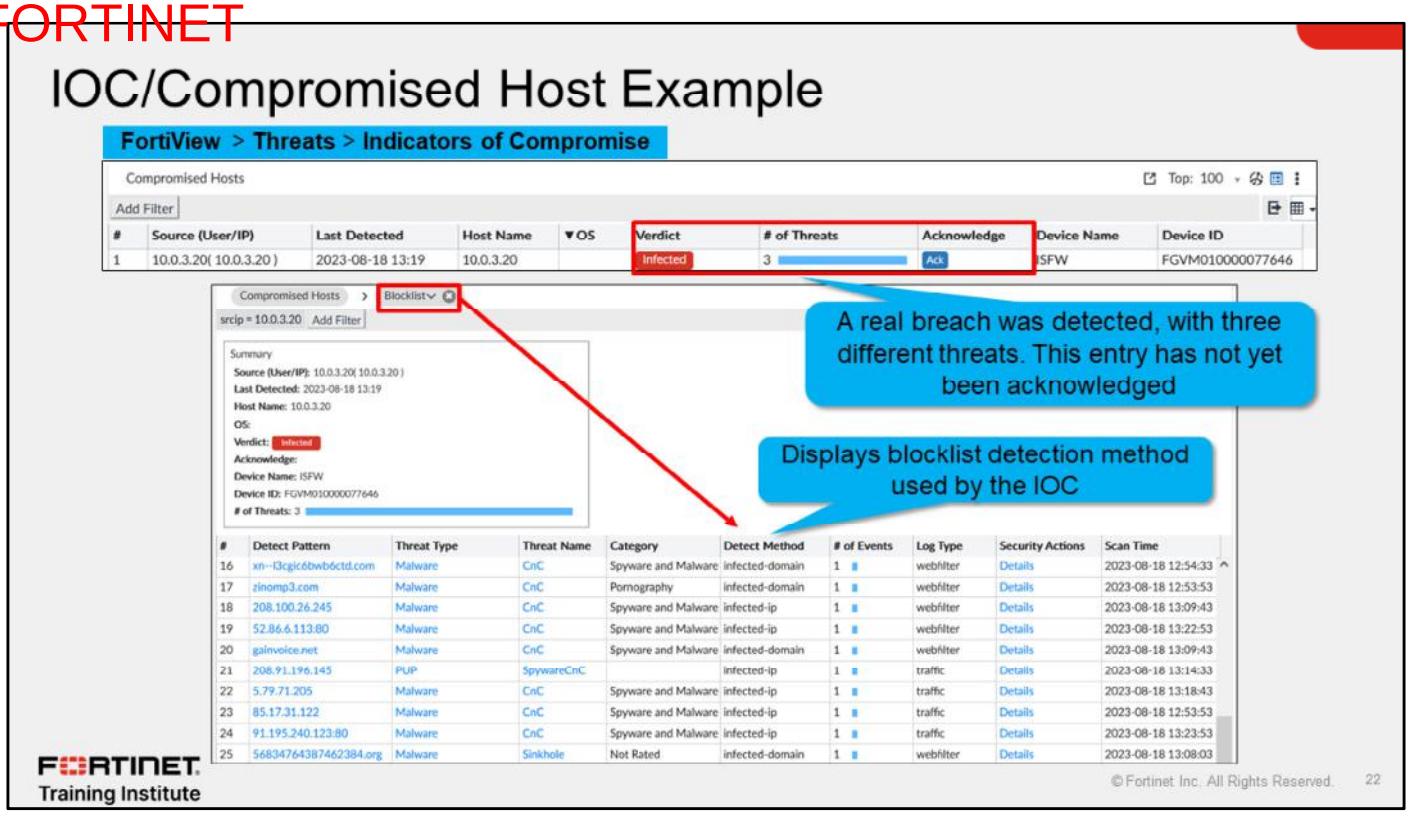
The IOC service on FortiAnalyzer uses the FortiGuard database to analyze web filtering, DNS, and traffic logs on FortiGate for breach detection. It is updated daily to reflect the real-world threat landscape. Note that antivirus logs, IPS logs, and similar logs aren't used because these threats have already been detected or prevented by these services on FortiGate. When FortiAnalyzer identifies a threat match, it assigns a threat score to the end user based on the overall ranking score. After 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**: Indicates a real breach. FortiAnalyzer found matches of the blacklisted IPs or domain generation algorithms (DGAs) in the web logs.
- **Suspicious**: Indicates a possible breach with varying degrees of confidence.



Depending on the log type, FortiAnalyzer identifies possible compromised hosts by checking the threat database against the log's IP address, domain, and URL. The table on this slide displays which data in the logs FortiAnalyzer checks against the threat database.

The results for each affected end user are displayed in an IOC. You can drill down from the table to review the details of the affected host, including the detection pattern and detection method for each IOC. You can also drill down further from these detections to examine the logs where the matches were initially found in FortiAnalyzer.



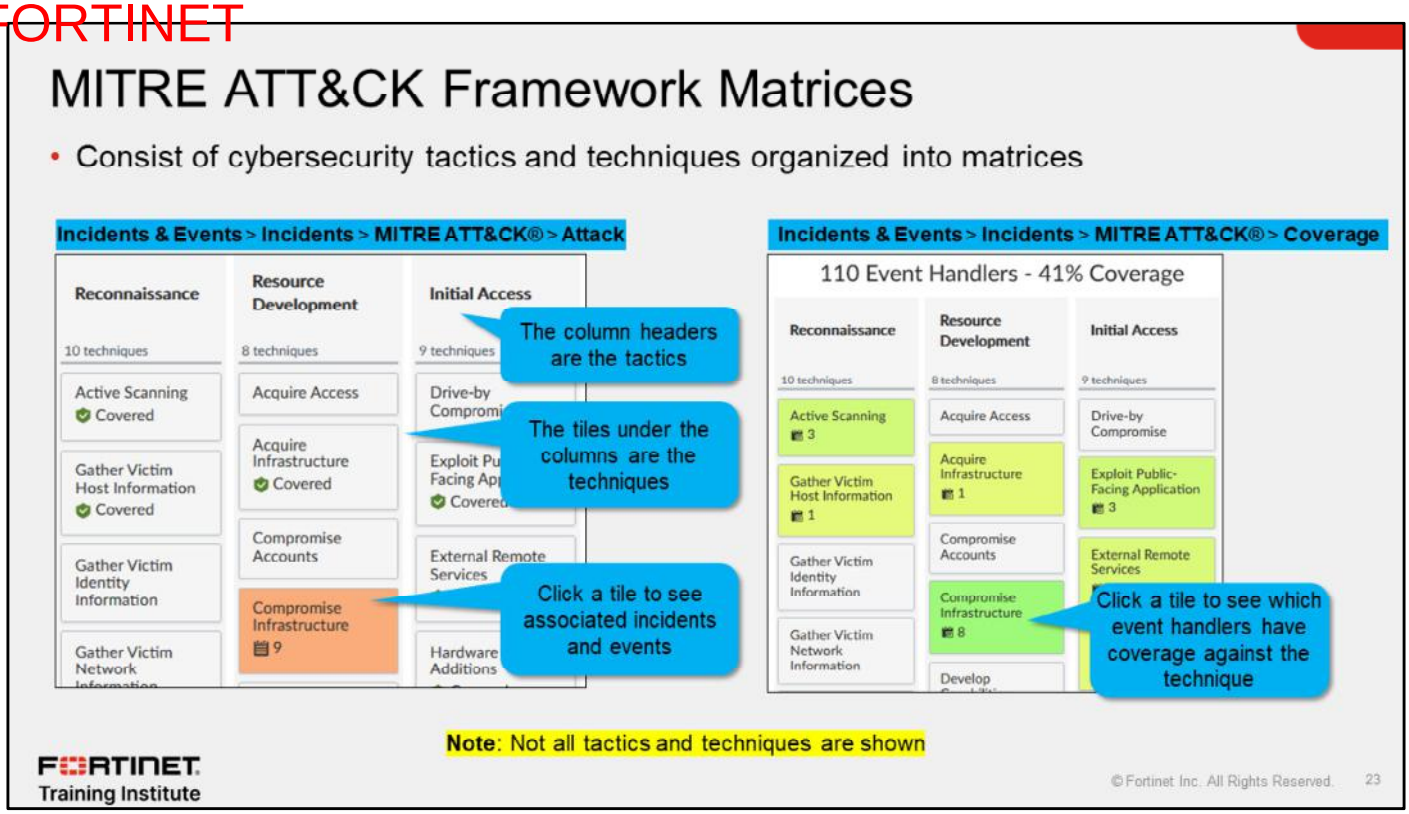
This slide presents an example of an IOC hit in FortiView. The IOC engine has confirmed a genuine breach, as indicated by the **Infected** verdict. The **# of Threats** column shows that three distinct threats are associated with this hit.

On the IOC FortiView, you can also:

- Filter the entries by specifying devices or a time period.
- Acknowledge the IOC by clicking **Ack** in the **Acknowledge** column. By default, you can view acknowledged IOCs, unless you configure the system not to 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 an 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 valid, you can report it as misrated by clicking on that entry.
- Suspicious (not shown on this slide), 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 endpoint's previous statistics for the same day, and then updates the score. If the score exceeds the threshold, that endpoint is listed or updated in **Compromised Hosts**.



The **MITRE ATT&CK®** and **MITRE ATT&CK® ICS** panes are based on the MITRE ATT&CK framework matrices. The MITRE ATT&CK framework provides a vast knowledge base of information about cybersecurity threats, including classifications, descriptions of attack vectors, real-life examples, mitigation steps, detection methodology, and so on. You can find more information about the framework on the MITRE website.

The column headers are the tactics in the matrices. They describe the adversary's objective for using techniques on your network, such as performing reconnaissance.

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

You can review the incidents and events associated with a technique, including their 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 in the **Coverage** window. It displays the number of event handlers and the percentage of coverage the FortiAnalyzer device has against attacks in the matrices. The number on each tile shows how many event handlers are associated with the technique. For example, the **Compromise Infrastructure** tile has eight associated event handlers. You can click a tile to view a list of event handlers related to the specific 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.

Outbreak Detection Service Overview

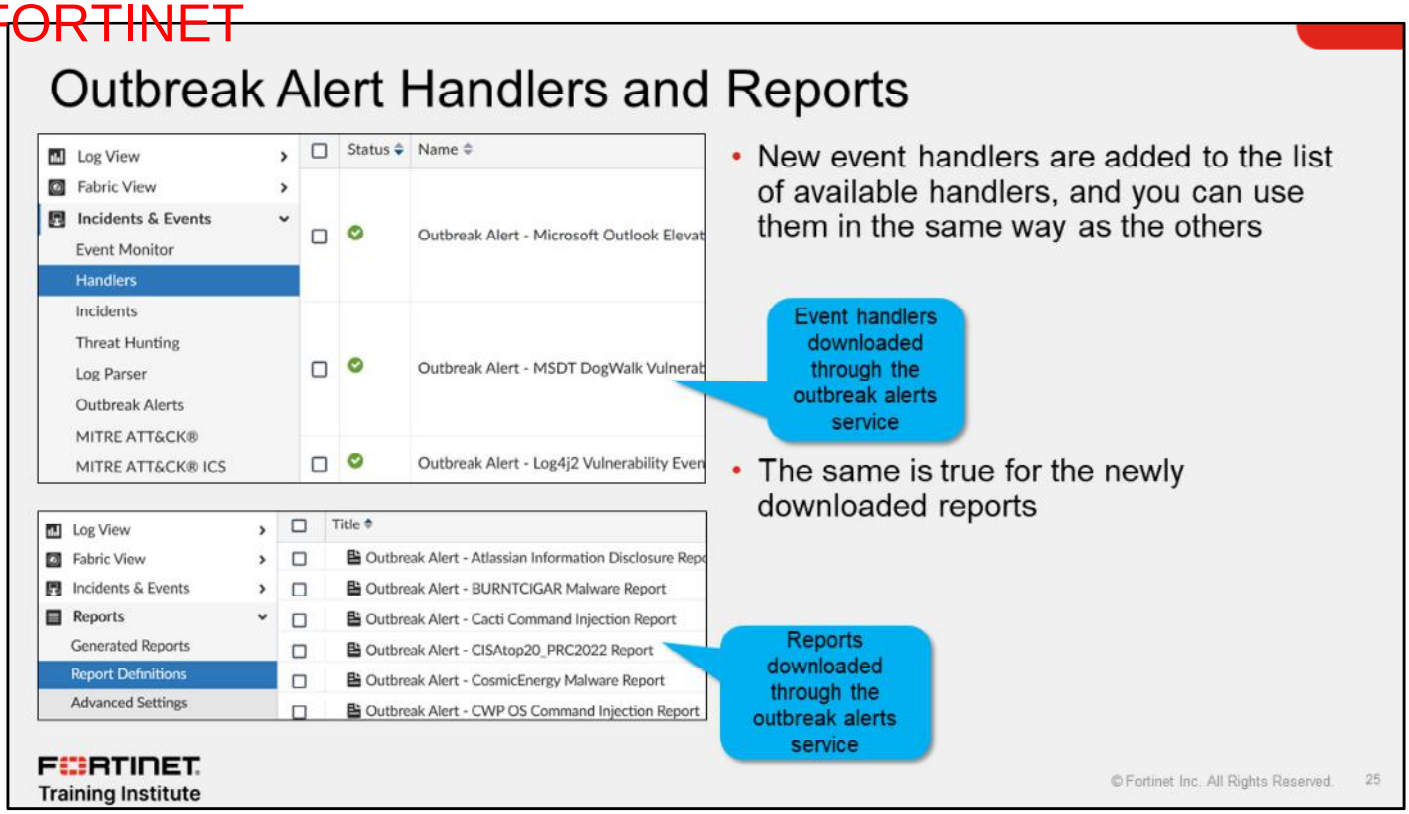
- Licensed feature
- Allows customers to receive information about malware outbreaks
- Automatically downloads new event handlers and reports related to the outbreaks

FORTINET Training Institute

 24

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** pane displays alerts from Fortinet, which are available on all ADOMs.



Once downloaded, the new handlers are available in the **Event Handler** list, and you can use them in the same ways described in an earlier section. That is, you can clone, export, import them, and so on.

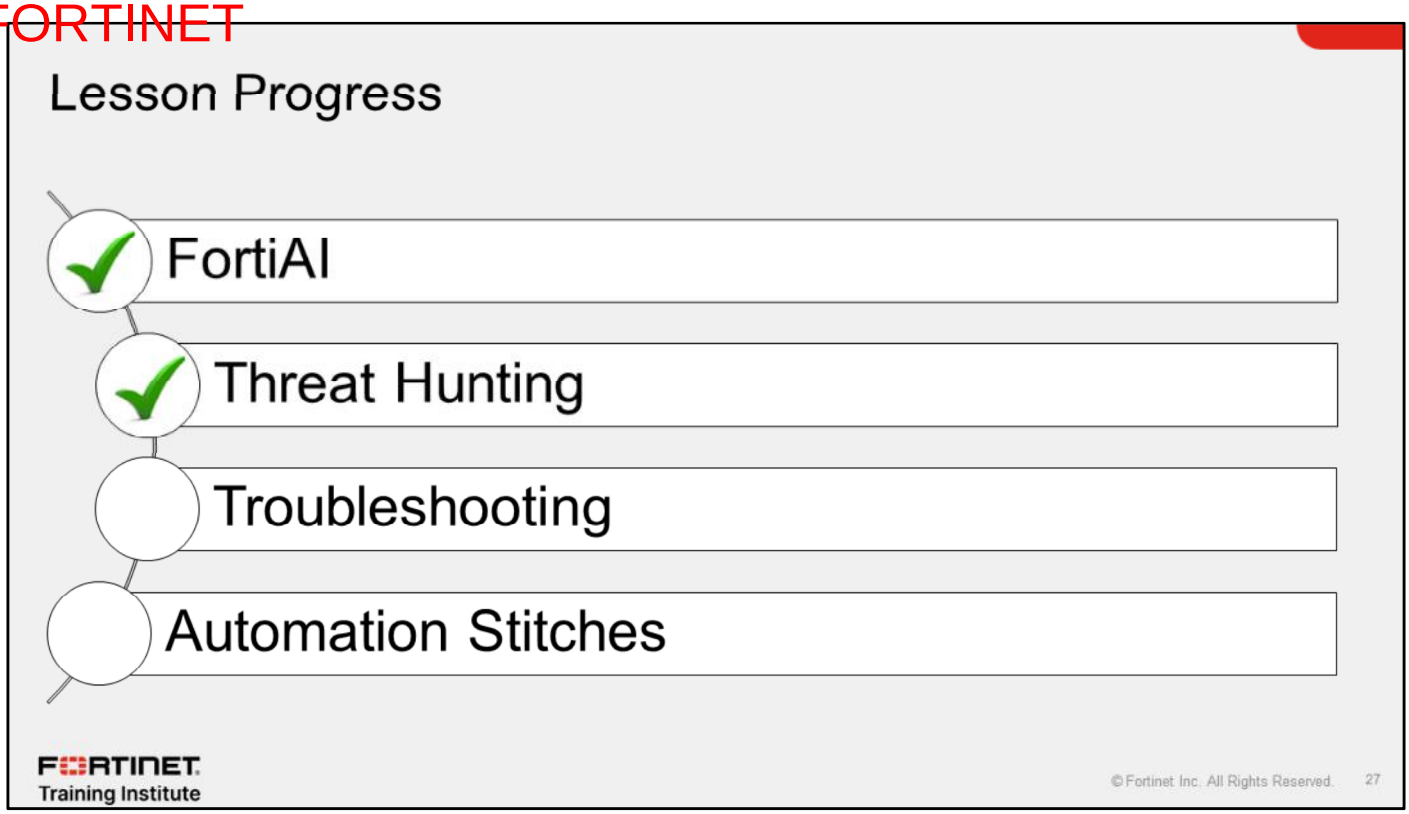
The same is true for the new reports.

Knowledge Check

1. Which feature allows the automatic download of new event handlers?
   - A. Threat-hunting SIEM table
   - ✓ B. Outbreak detection service

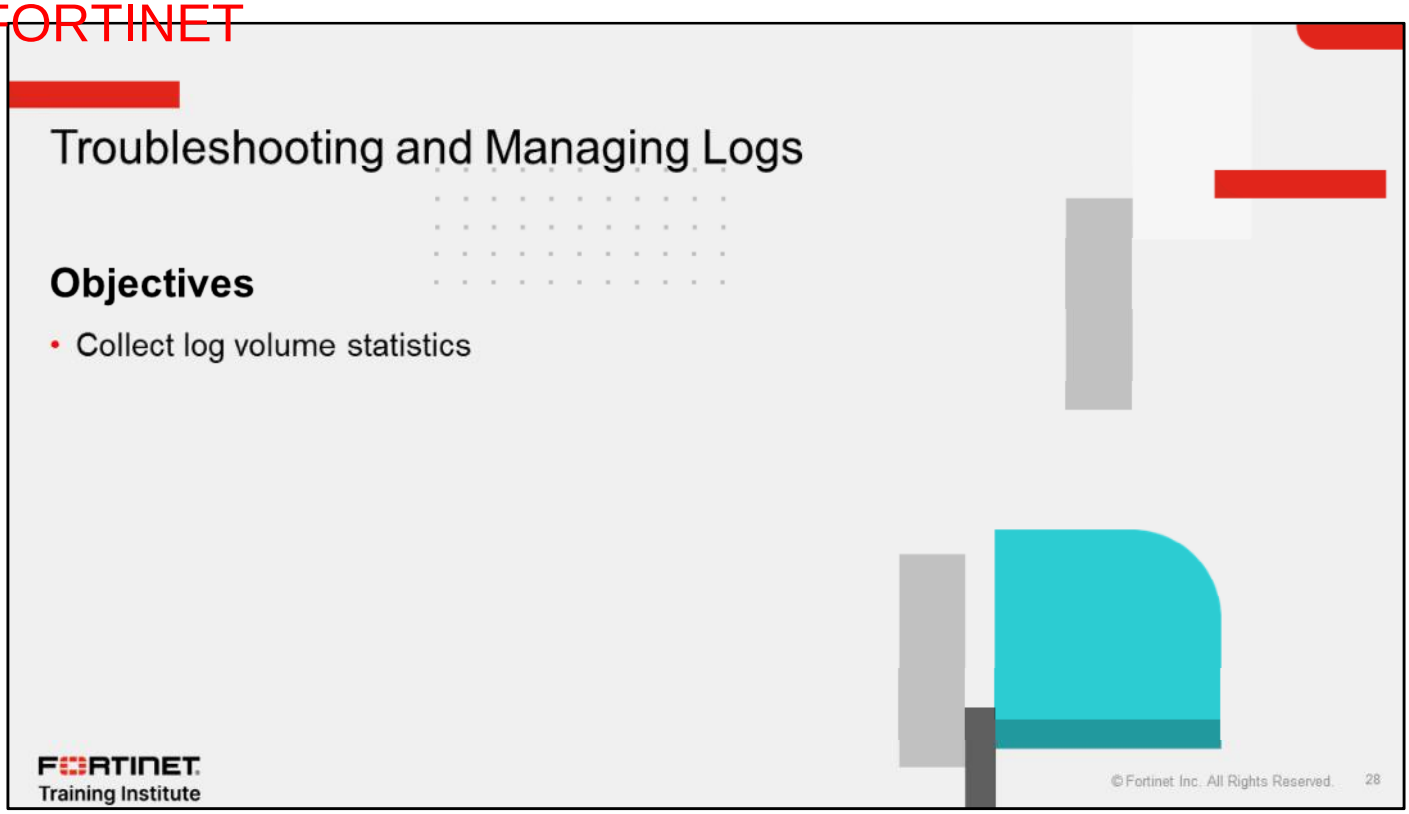
FORTINET Training Institute

 26



Good job! You now understand threat hunting.

Now, you will learn how to troubleshoot logging issues on FortiAnalyzer.



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

By demonstrating competence in collecting log statistics, you will be able to identify issues that may affect the performance of FortiAnalyzer.

Gathering Log Rate and Device Usage Statistics

- Use the following FortiAnalyzer CLI commands to troubleshoot logging issues

What to investigate	CLI command to use
What is the log receive rate for each second? What are the log receive rate totals? What is the device log rate? What is the log rate for each log type?	# diagnose fortilogd lograte # diagnose fortilogd lograte-total # diagnose fortilogd lograte-device # diagnose fortilogd lograte-type
What is the message receive rate for each second?	# diagnose fortilogd msgrate
What is the SQL insertion status?	# diagnose sql status sqlplugind
What is the device log usage for all logging devices?	# diagnose log device

- Example

```
FAZVM64-KVM # diagnose fortilogd lograte
last 5 seconds: 0.6, last 30 seconds: 2.2, last 60 seconds: 1.7
FAZVM64-KVM # diagnose fortilogd msgrate
last 5 seconds: 0.2, last 30 seconds: 0.4, last 60 seconds: 0.4
```

Difference between log rate and message rate: one log message can consist of multiple logs in LZ4 format

FORTINET Training Institute

 29

To understand the log volume and whether your disk quota is configured appropriately, you can use the CLI commands shown on this slide to gather log rate and device usage statistics.

For example, if your log volume is too high, you won't be able to retain your analytics logs or archive logs for the amount of time configured in the ADOM.

Gathering Log Rate and Log Volume per ADOM

- Use the following FortiAnalyzer CLI commands to calculate log rate and log volume per ADOM

What to investigate	CLI command to use
Log receive rate for all ADOMs or a specific ADOM?	`# diagnose fortilogd lograte-adom {all | adom-name}`
Log volume for all ADOMs or a specific ADOM?	`# diagnose fortilogd logvol-adom {all | adom-name}`

- Example

```
FAZVM64-KVM # diagnose fortilogd logvol-adom root
2025-04-22 2025-04-21 2025-04-20 2025-04-19 2025-04-18 2025-04-17 2025-04-16 average
adom 'root':
8.77 MB    10.15 MB   15.65 MB   17.68 MB   22.89 MB   22.64 MB   22.71 MB  17.21 MB
```

Volume of the last seven days and the average volume for the root ADOM

FORTINET Training Institute

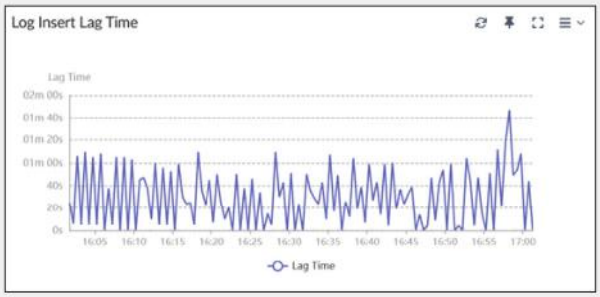
 30

To understand the log rate and log volume per ADOM, you can use the CLI commands shown on this slide to gather log rate and volume statistics. This is very useful in environments where the FortiAnalyzer administrator is using multiple ADOMs to manage multiple FortiGate devices, like managed security service providers (MSSPs).

Insert Rate vs. Receive Rate and Log Insert Lag

- **Insert Rate vs. Receive rate**
  - Insert rate = SQL insertion rate
    - Handled by sqlplugind
  - Receive rate = Raw receiving rate
    - Handled by fortilogd

Dashboard > Widgets



- **Log Insert Lag Time**
  - Amount of time between the log received and the log inserted in the database

FORTINET Training Institute

 31

You can view log insert rate, receive rate, and log insert lag time using the respective dashboard widgets. If these widgets are not already on the dashboard, you can add them by clicking **Toggle Widgets** in the upper-left corner and selecting the widgets from the list.

Insert Rate vs Receive Rate is a graph that shows the rate at which raw logs reach FortiAnalyzer (receive rate) and the rate at which they are indexed (insert rate) by the SQL database and the sqlplugind daemon (insert rate). The difference between these parameters should usually be consistent. Ideally, it should be as small as possible, but variations during the day can be expected. Create a baseline during normal operation and compare it to verify performance.

Log Insert Lag Time shows the amount of time between when a log was received and when it was indexed. Ideally, this parameter should be as small as possible, with only occasional spikes, according to the network activity being logged. You should create a good baseline to help with the identification of possible performance issues. Similarly, the lag time should be as small as possible, and variations during the day can be expected.

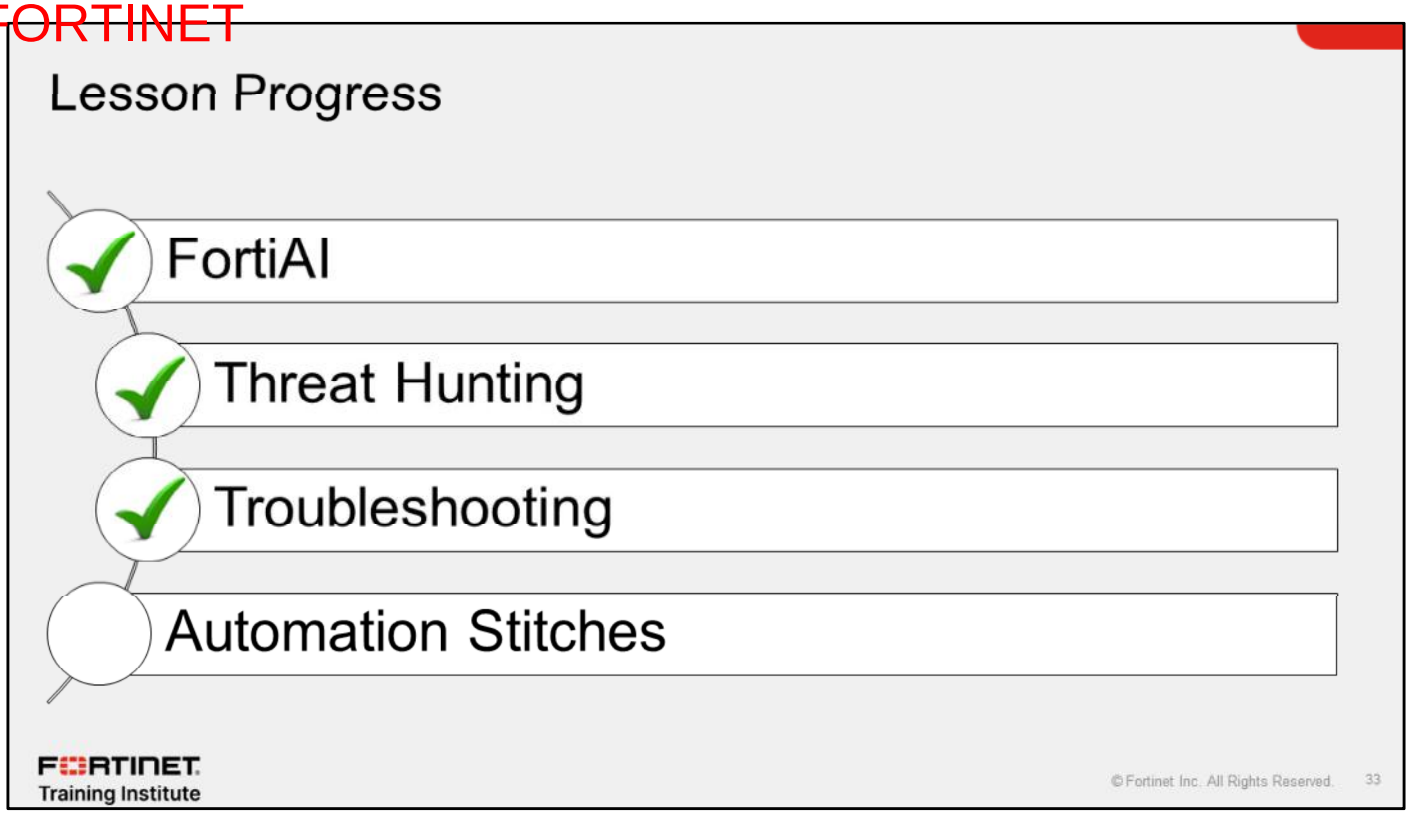
Knowledge Check

1. Which data does the CLI command `# diagnose fortilogd lograte` provide?
   - ✓ A. The log receive rate per second
   - B. The message receive rate per second

2. Which FortiAnalyzer process handles the insert rate?
   - A. fortilogd
   - ✓ B. sqlplugind

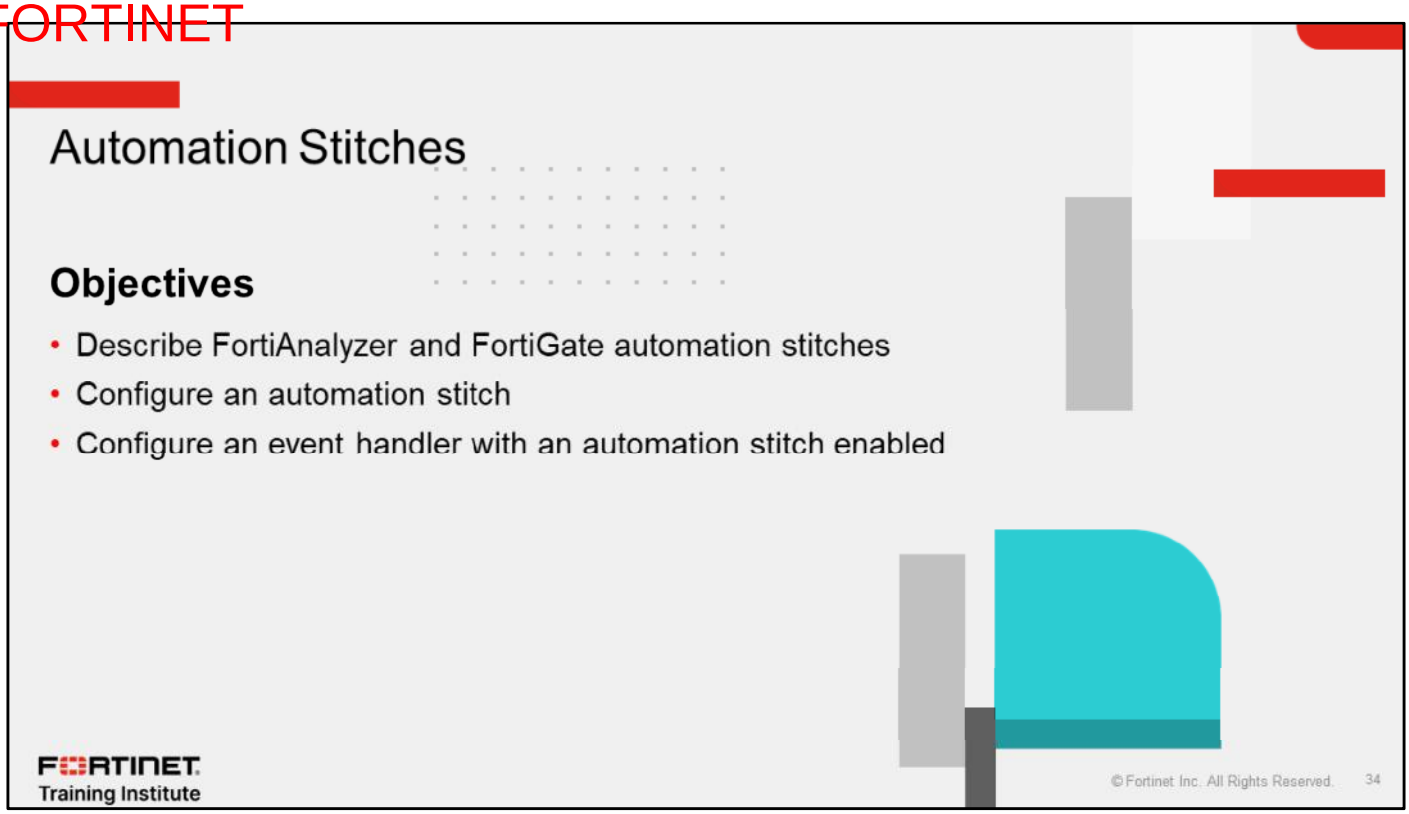
FORTINET Training Institute

 32



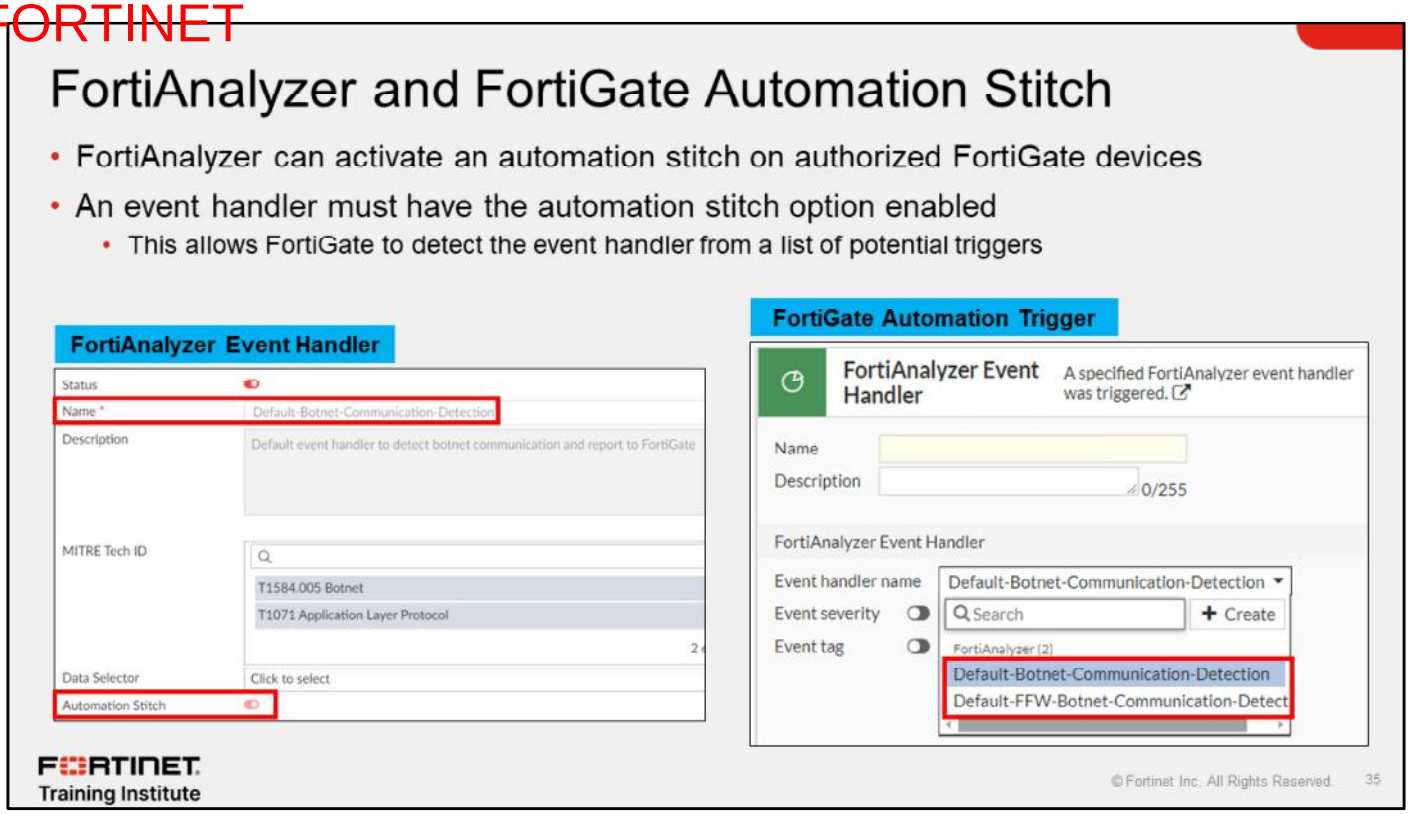
Good job! You now how to troubleshoot logging issues on FortiAnalyzer.

Now, you will learn about automation stitches on FortiAnalyzer.



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

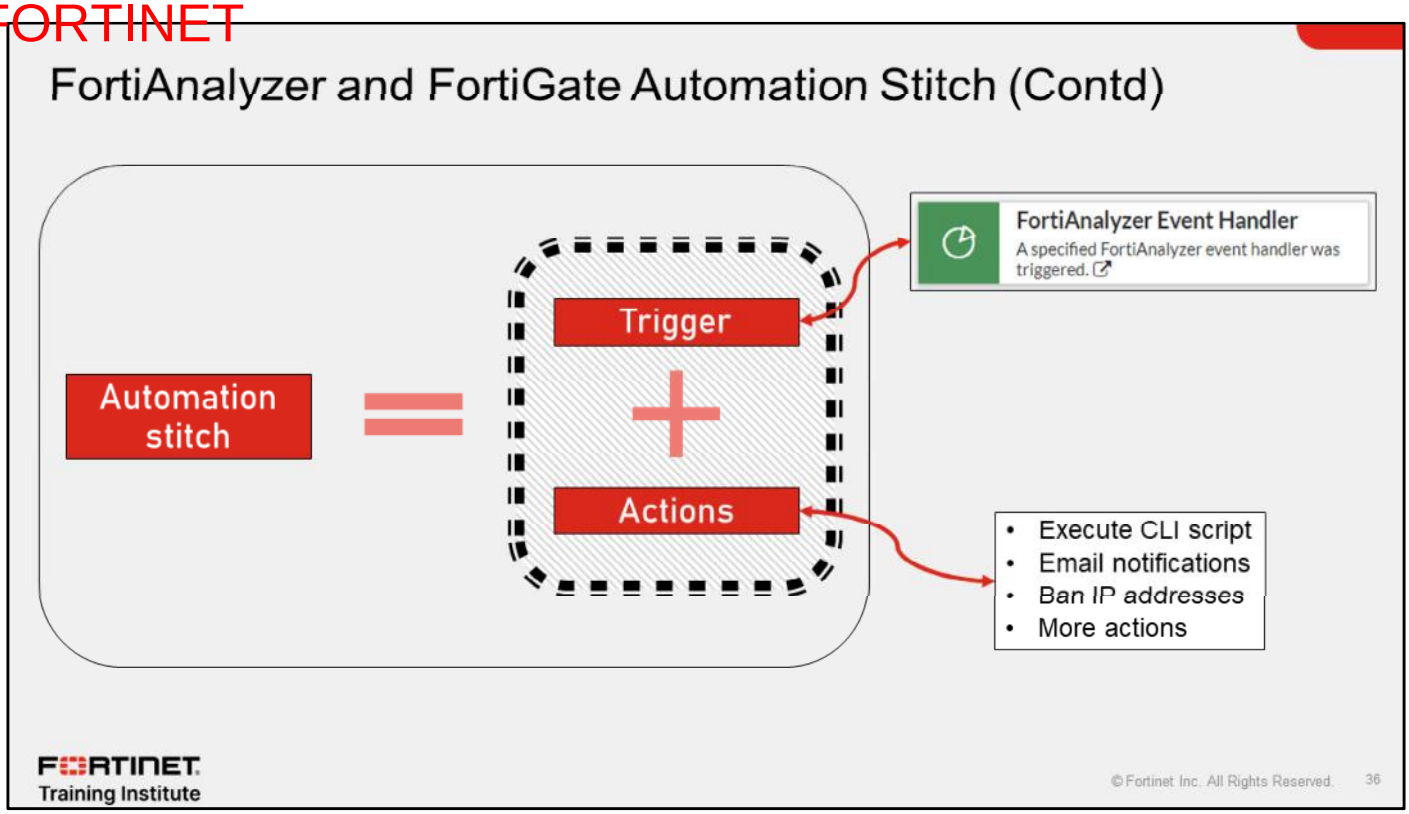
By demonstrating competence in understanding the purpose of playbooks and their components, you will be able to configure automation stitches between FortiAnalyzer and FortiGate.



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 perform a system action in response to the trigger.

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

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

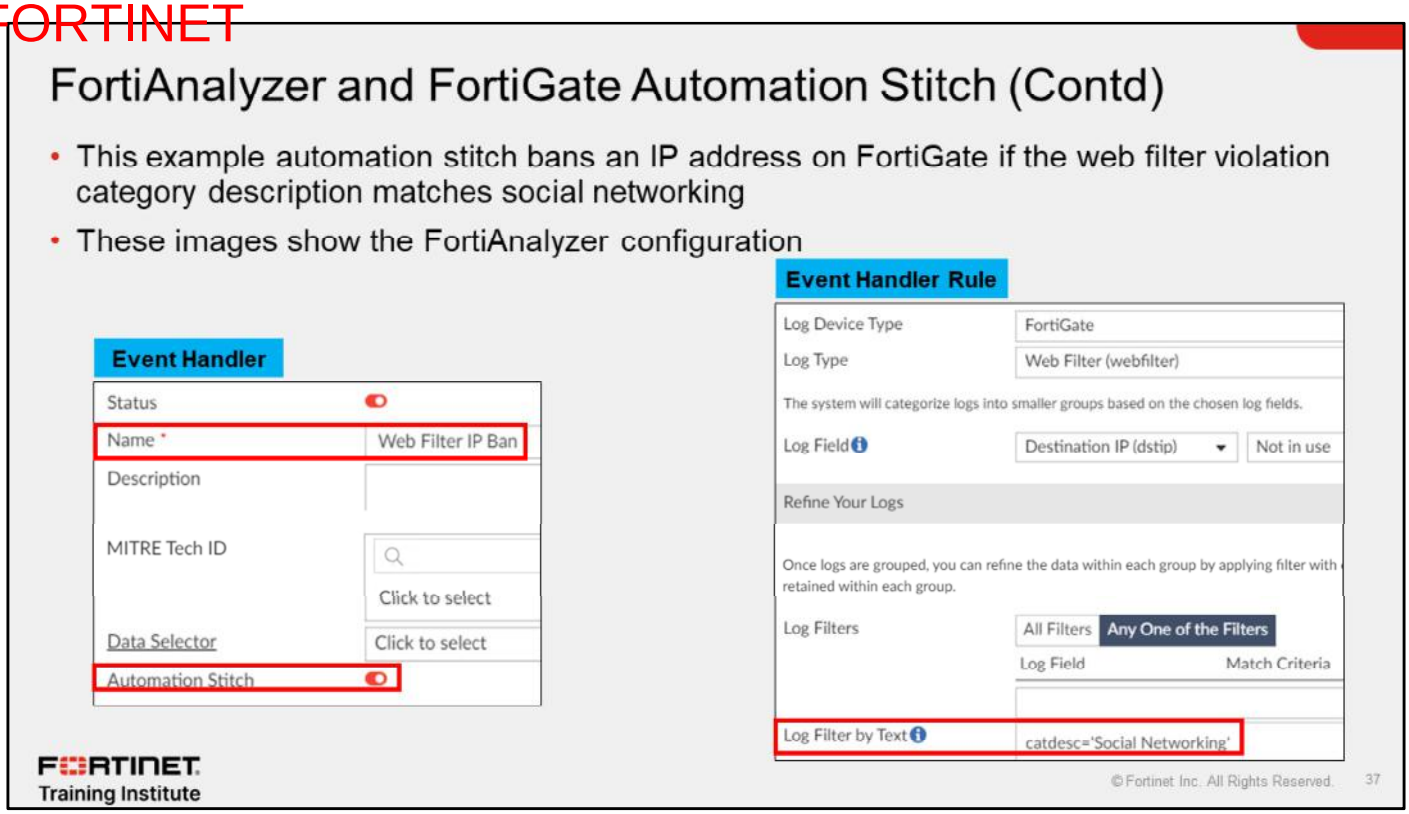


An automation stitch consists of two parts: the trigger and the action. The trigger is the condition or event that activates the action, such as a FortiAnalyzer event handler that generates an event. The action is what FortiGate does in response to the trigger. Automation stitches are configured on the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

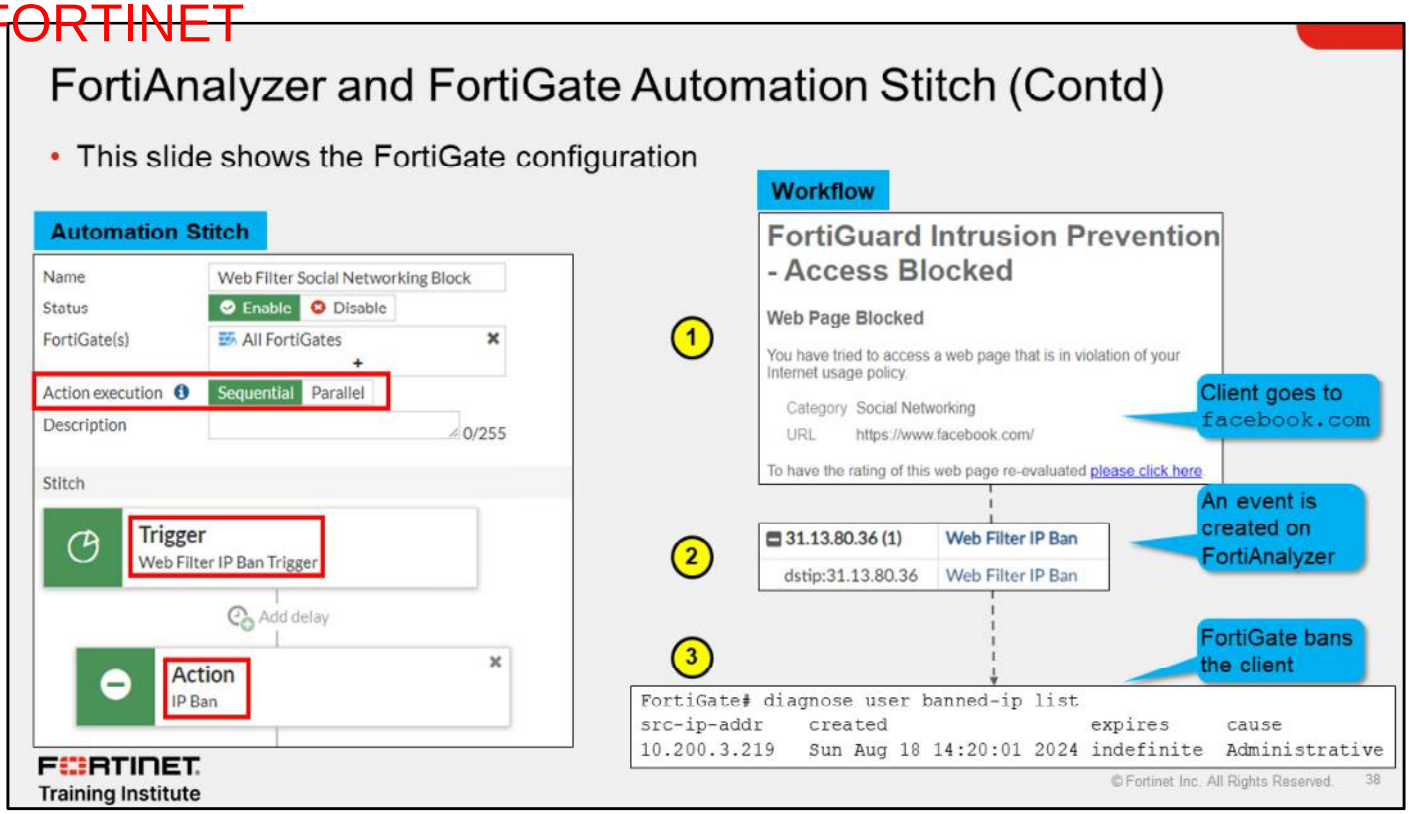
- Scalability: The configured event handlers can apply to all authorized FortiGate devices, or you can use data selectors to narrow the selection.
- Granularity: You have finer control over which logs generate an event.
- Centralized SOC view: You can create events and incidents on FortiAnalyzer in addition 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.

Many other types of triggers are available on FortiGate. However, this course focuses only on FortiAnalyzer event handlers as the automation trigger.



The example on this slide illustrates the configuration of an automation stitch integration with FortiGate. This automation stitch triggers an IP address ban for the source computer on the FortiGate device where the security event occurs. If the FortiGate is part of a Security Fabric, you can select which devices within the Security Fabric will activate the stitch.

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 specifies 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.



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 an automation stitch contains more than one action, FortiGate can perform them in sequence or in parallel. In sequential execution, actions 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 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:

1. 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.
2. On FortiAnalyzer, the **Web Filter IP Ban** event handler is triggered. This event handler has the automation stitch option enabled.
3. 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.

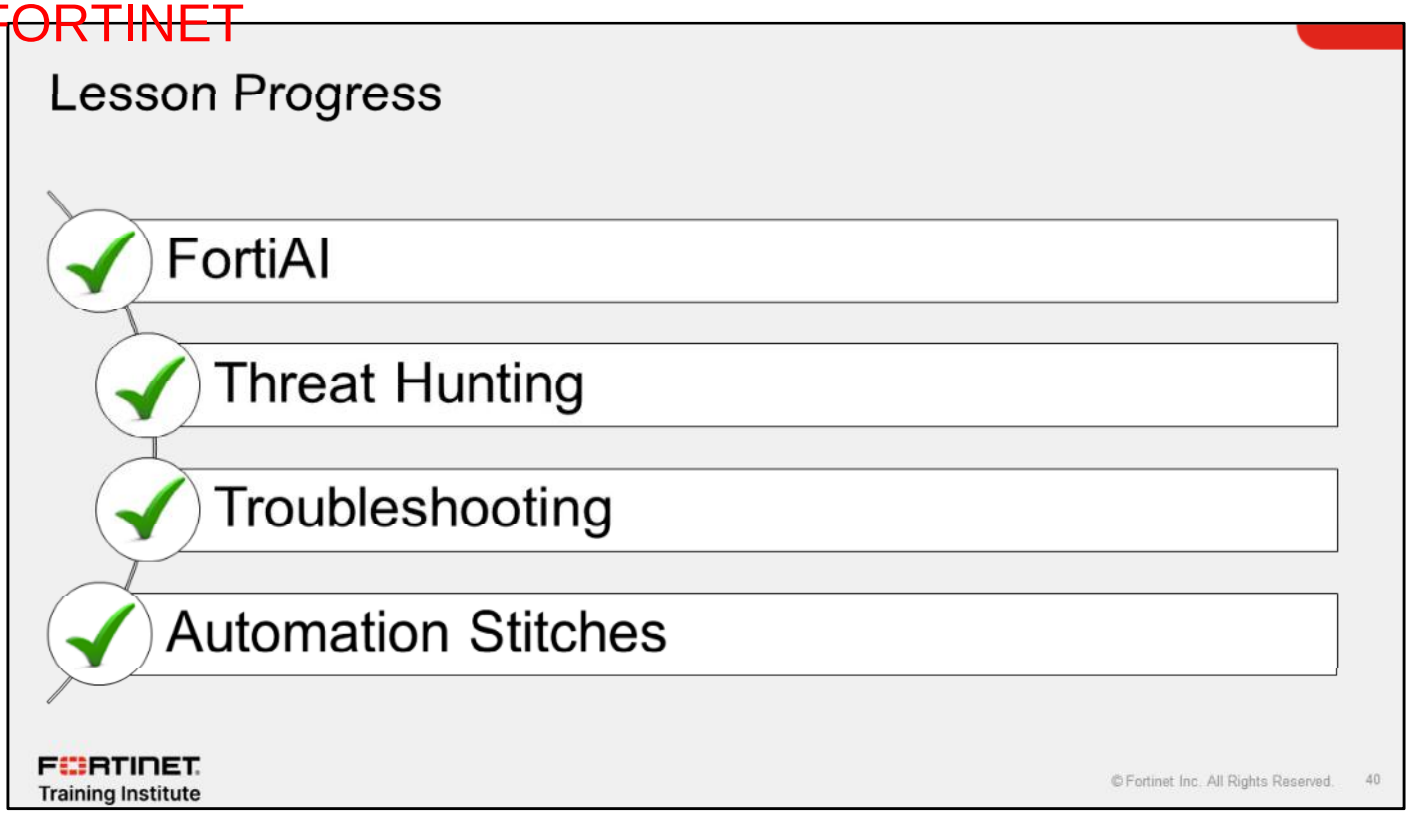
Note that, unlike the FortiClient EMS quarantine depicted earlier, which is a host-level block, this configuration is blocking at a network level. This means that the host is banned only for traffic traversing FortiGate. In contrast, the host-level block restricts all network activity on the compromised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

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

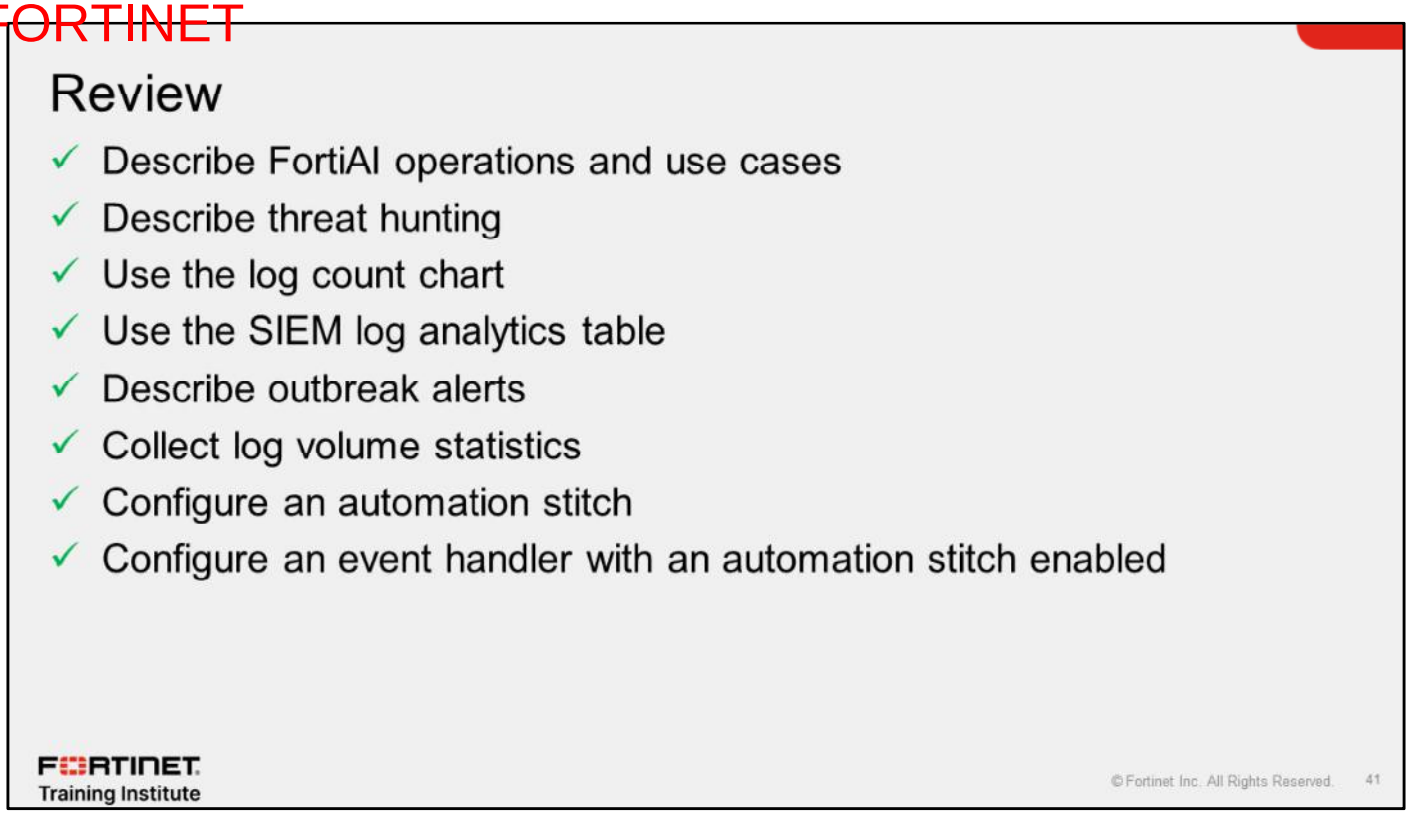
FORTINET Training Institute

 39

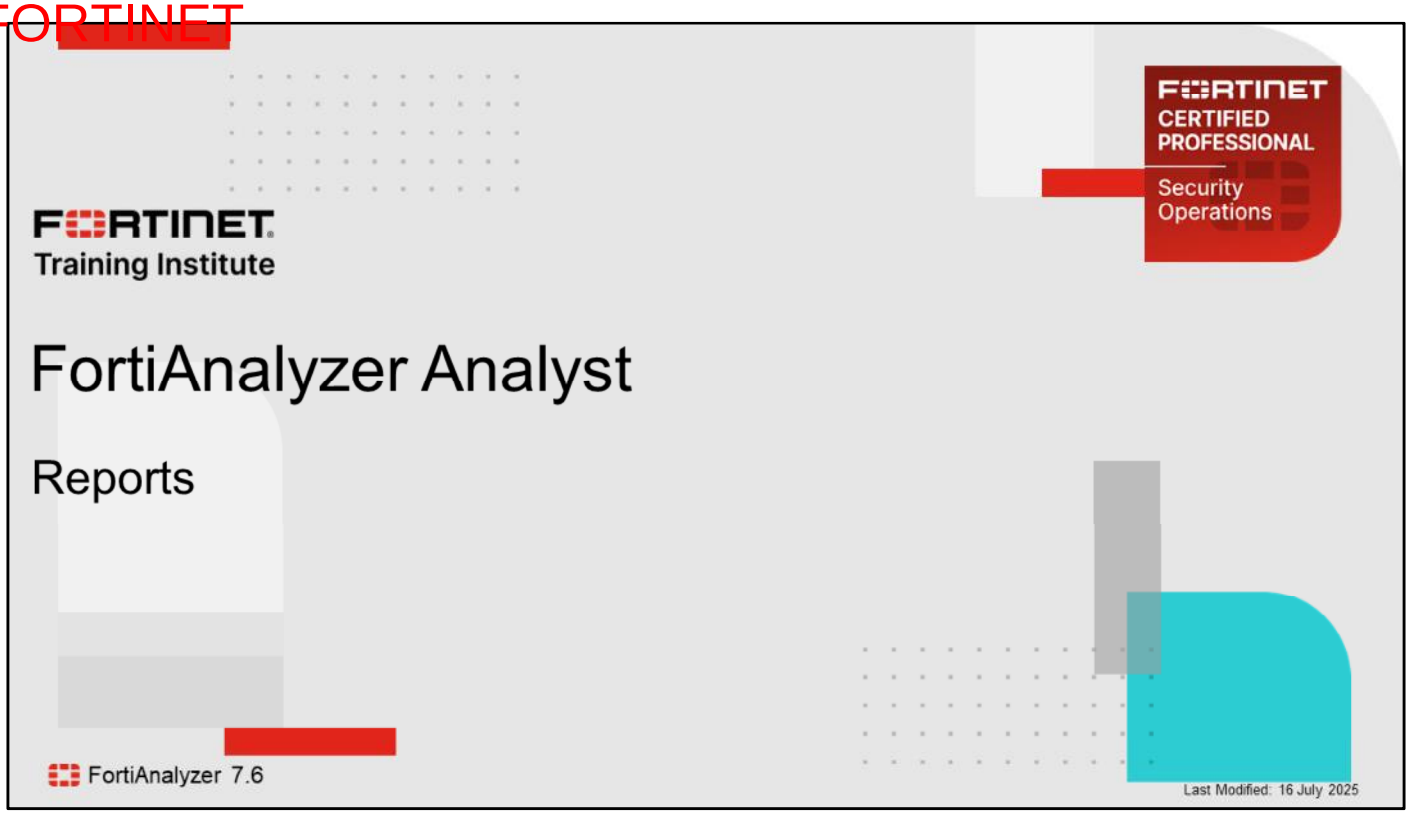


Congratulations! You have completed this lesson.

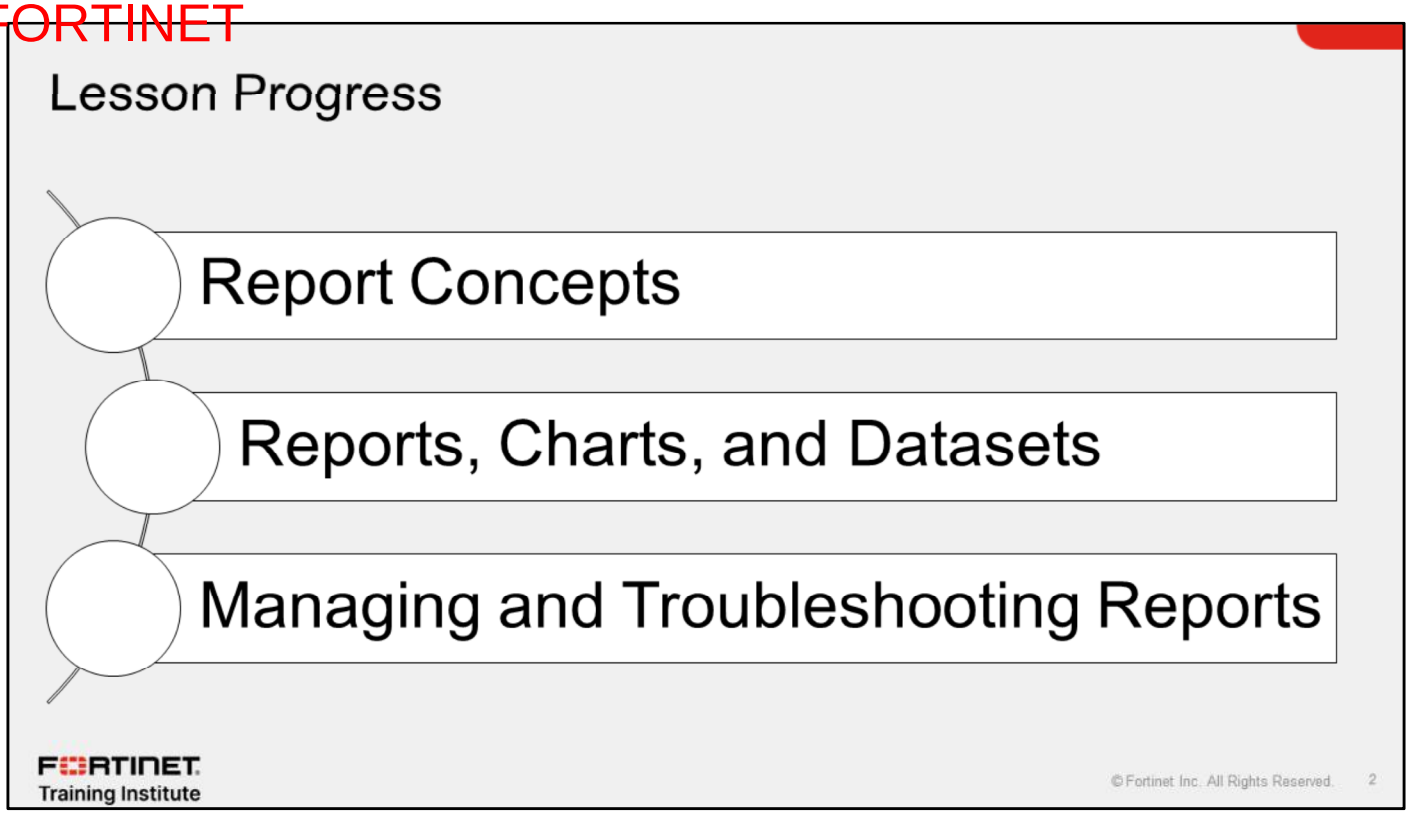
Now, you will review the objectives that you covered in this lesson.



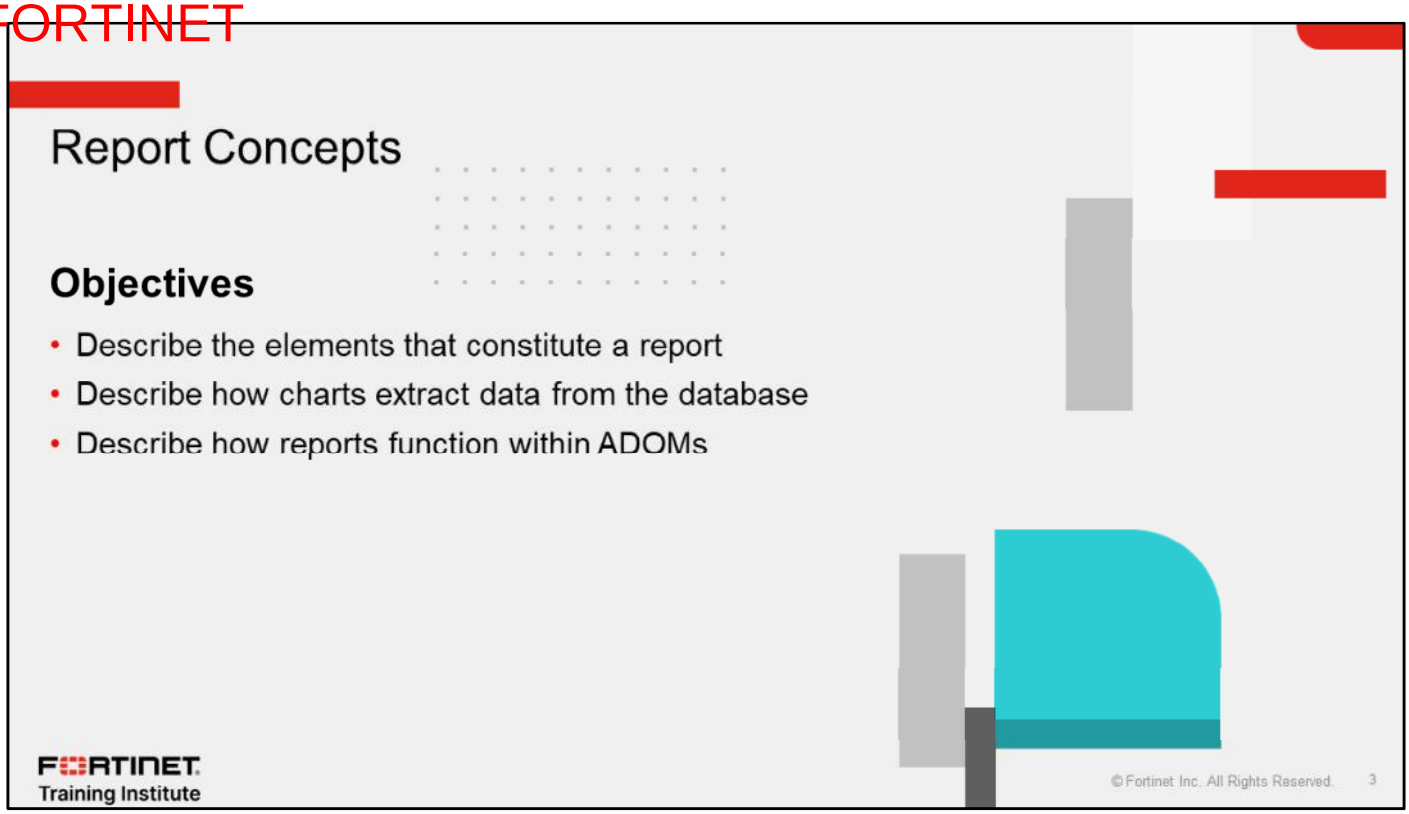
This slide shows the objectives that you covered in this lesson.



In this lesson, you will learn how to extract useful information from your logs for analysis purposes. You will also learn how data is formatted, stored, and organized in the database, and how to use the FortiAnalyzer reporting feature to view captured data for forensics and compliance.

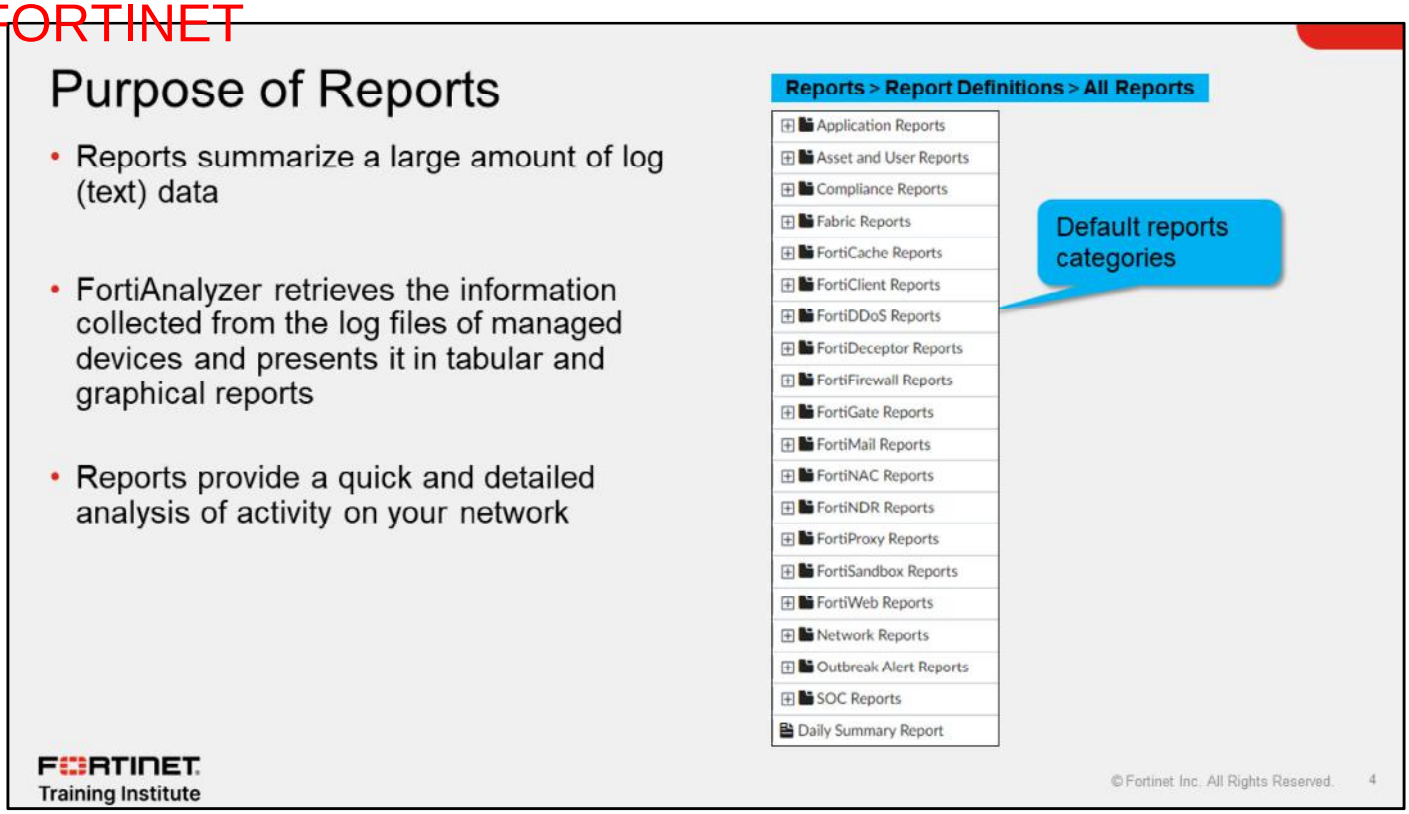


In this lesson, you will explore the topics shown on this slide.



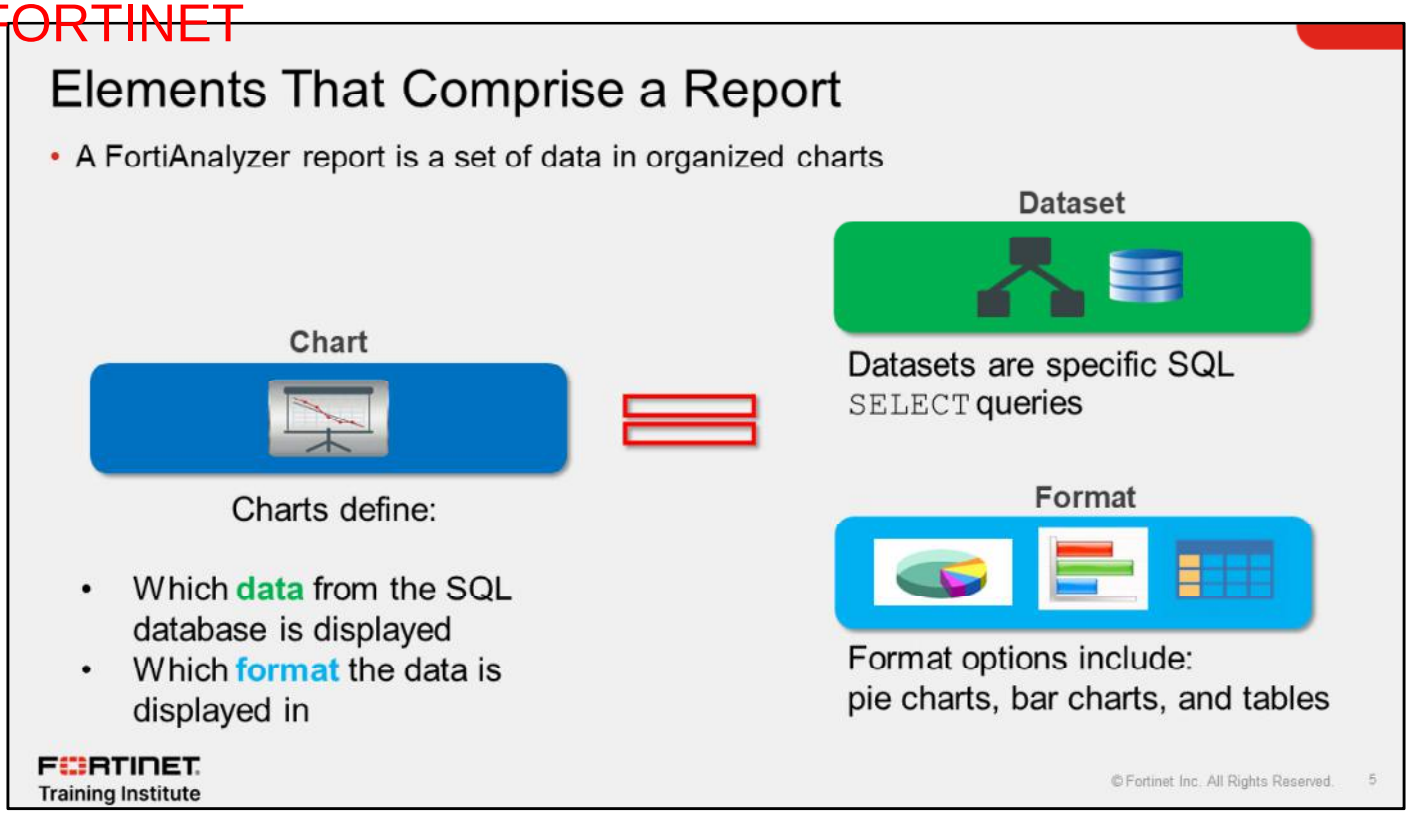
After completing this section, you should be able to achieve the objectives shown on this slide.

By demonstrating competence in understanding report concepts, you will be able to use reports more effectively to extract collected log data from your database.



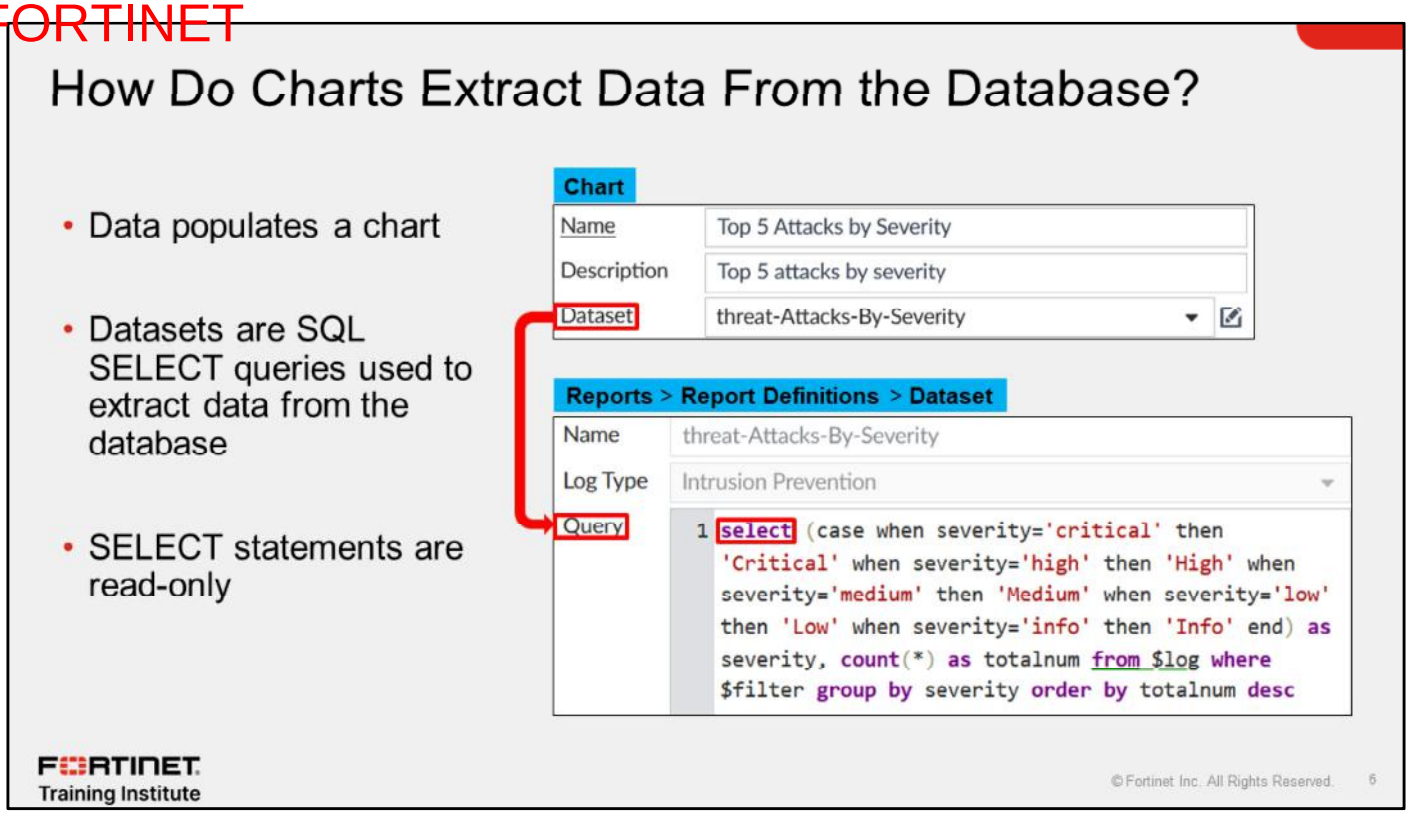
Reports summarize large amounts of logged data. Based on configured report parameters, FortiAnalyzer extracts data and presents it in a graphical manner that makes it easier and quicker to digest. The patterns and trends that reports reveal already exist as several points of data within your database, but it is difficult and time-consuming to manually locate, cross-reference, and analyze multiple log files, especially if you don't know what trend or pattern you are looking for. Once configured, reports provide a quick and detailed analysis of activity on your network. You can then use that information to better understand your network or improve your network security.

Note that reports generally do not provide recommendations or indicate problems. Administrators must be able to look beyond the data and charts to see what is happening within their network.



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, or tables)

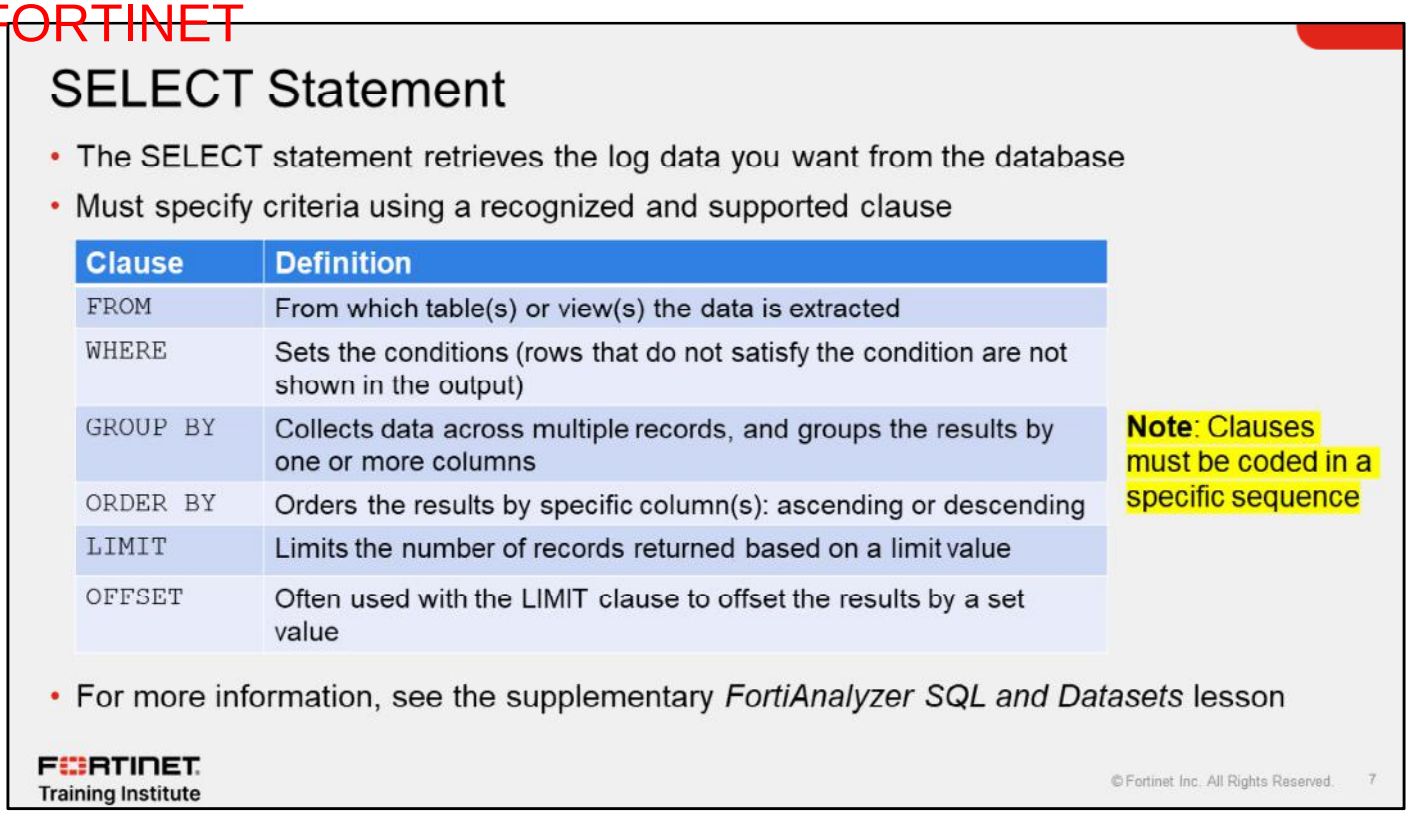


To populate a chart with specific log data that has been collected, stored, and sorted in the SQL database, reports rely on a dataset query to extract that log data. A dataset is a specific SQL `SELECT` query—a read-only statement that retrieves data from the database.

The `SELECT` statement is the first word used in a query—it is the declarative verb describing what you want done—and is followed by the column(s) from which you want to extract information. You can extract all entries, or you can use clauses to make the query more specific.

In the example on this slide, the **Top 5 Attacks by Severity** chart contains a dataset named **threat-Attacks-By-Severity**.

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.

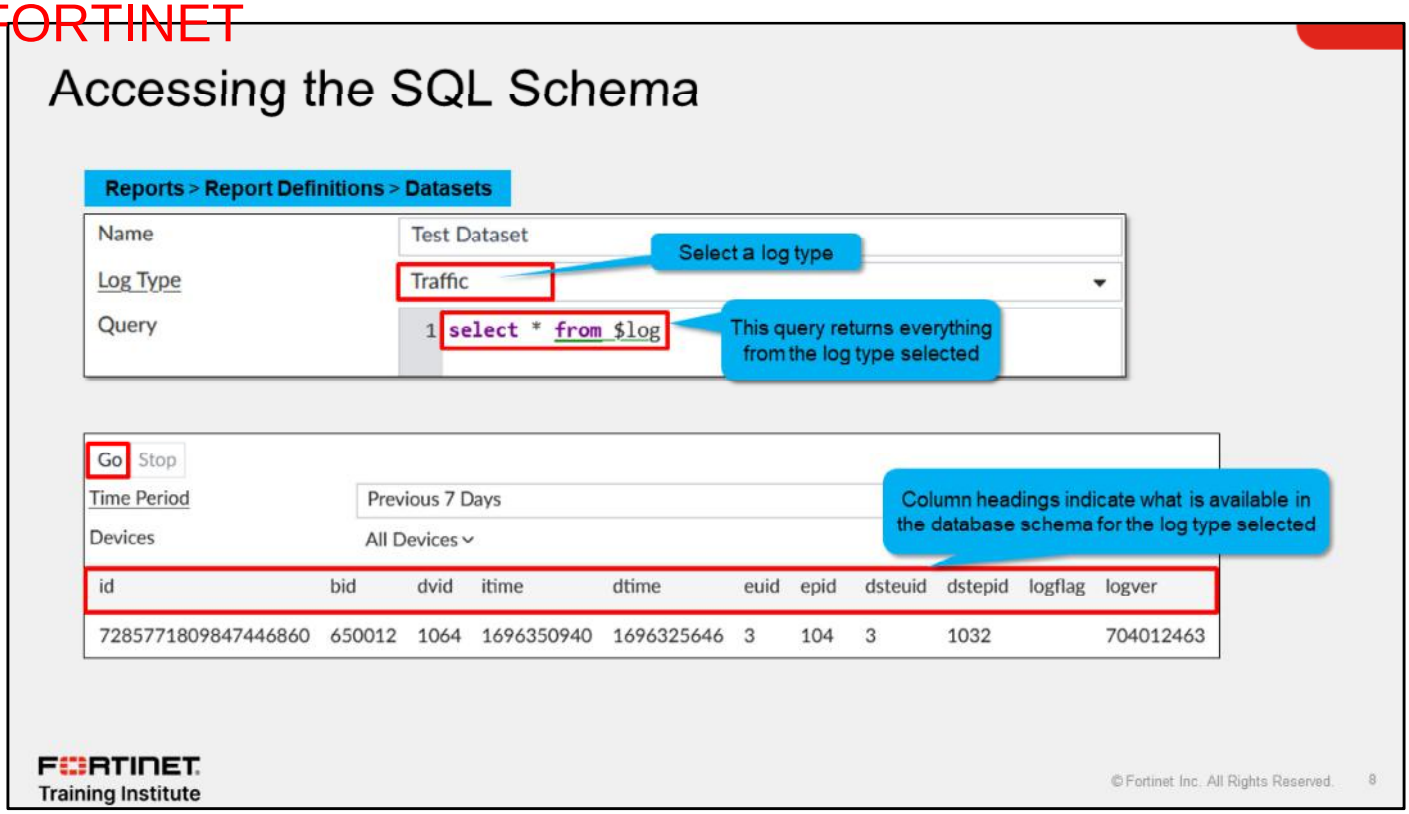


To extract the desired data, you must specify the criteria to be used. To put this criteria into a language that SQL understands, you must use one or more clauses recognized by the `SELECT` statement.

The main clauses FortiAnalyzer reports use are as follows:
- `FROM`, which specifies from which table(s) or view(s) the data is extracted.
- `WHERE`, which specifies the conditions. All rows that don't satisfy the condition are not shown in the output.
- `GROUP BY`, which collects data across multiple records and groups the results by one or more columns.
- `ORDER BY`, which orders the results by specific column(s). If **`ORDER BY`** is not given, the records are returned in whatever order the system finds the fastest to produce.
- `LIMIT`, which limits the number of records returned based on a specified value.
- `OFFSET`, which is a clause often used along with `LIMIT`, to offset results by the number specified. For example, if you place a limit of three records and an offset of one, the first record that would normally be returned is skipped and, instead, the second, third, and fourth records (three in total) are returned.

`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. Accordingly, following the `SELECT` keyword, 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 whichever ones you do use must be in the correct sequence.

For more information about SQL and datasets for use with FortiAnalyzer reports, see the supplementary *FortiAnalyzer SQL and Datasets* lesson.



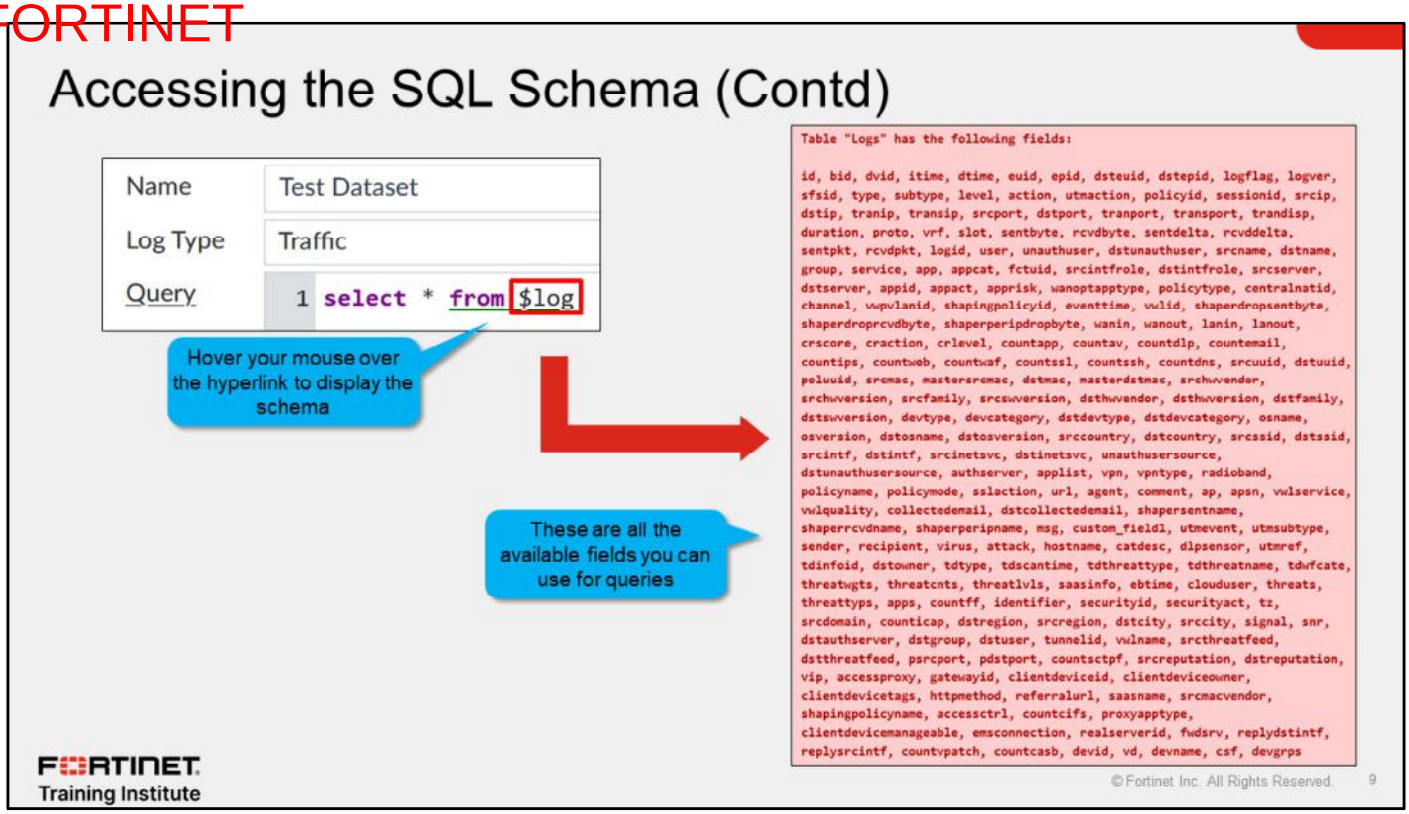
To create a query, you first need to know what is included in the database schema. The schema is the different fields or columns that are available from which you can extract information for reports. On FortiAnalyzer, you can obtain the schema for a specific log type by creating and testing the following dataset query:

```
SELECT * FROM $log
```

This query can be read as: “Select everything from the logs table.”

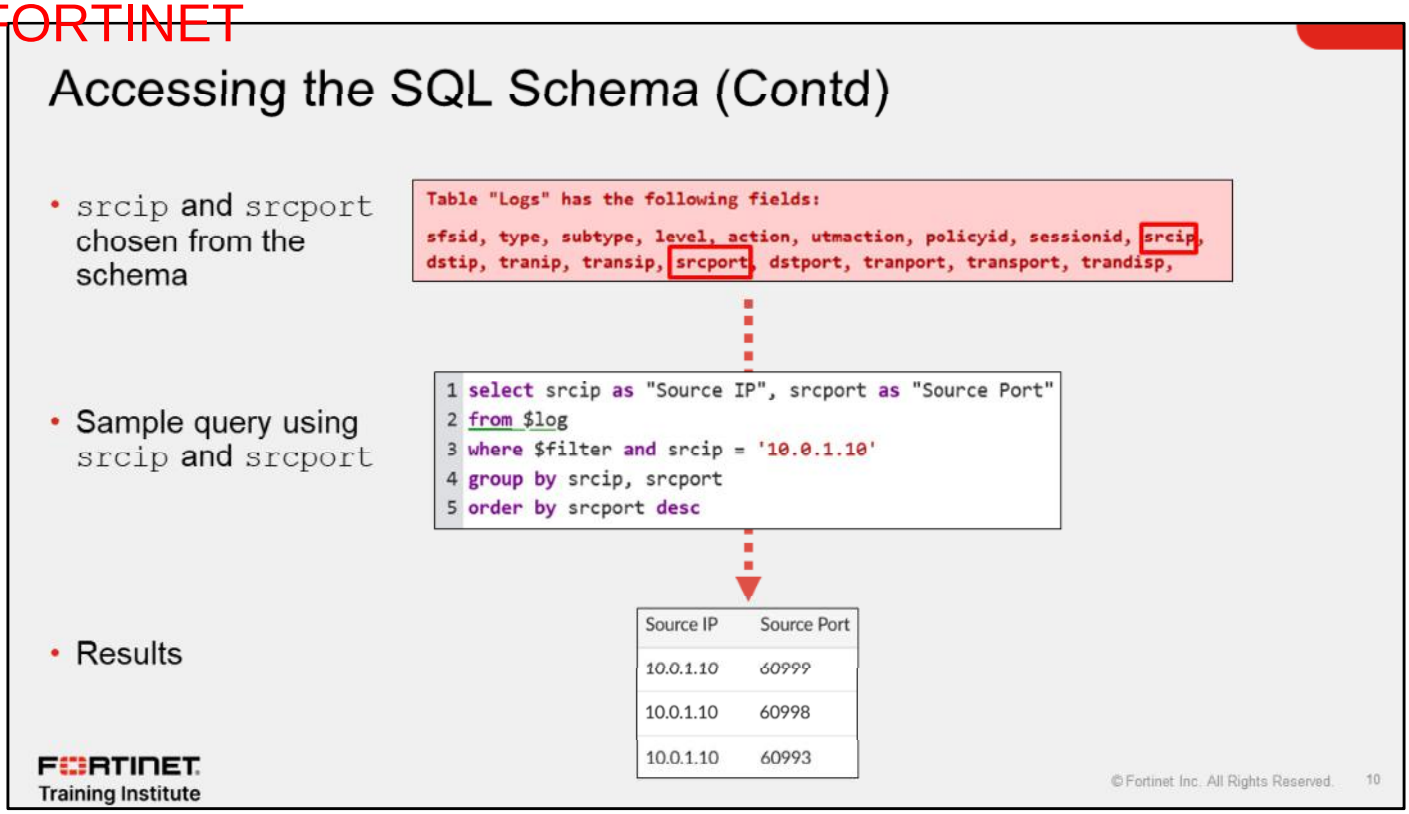
For traffic logs, for example, associate the **Traffic** log type with this dataset in the **Log Type** field. This query returns everything from the **Traffic** log type. The column heading names indicate what is available in the database schema for the log type selected. The * symbol returns all data. 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.



You can hover your mouse over the hyperlink in the query to open a window that displays all the available fields for that table.

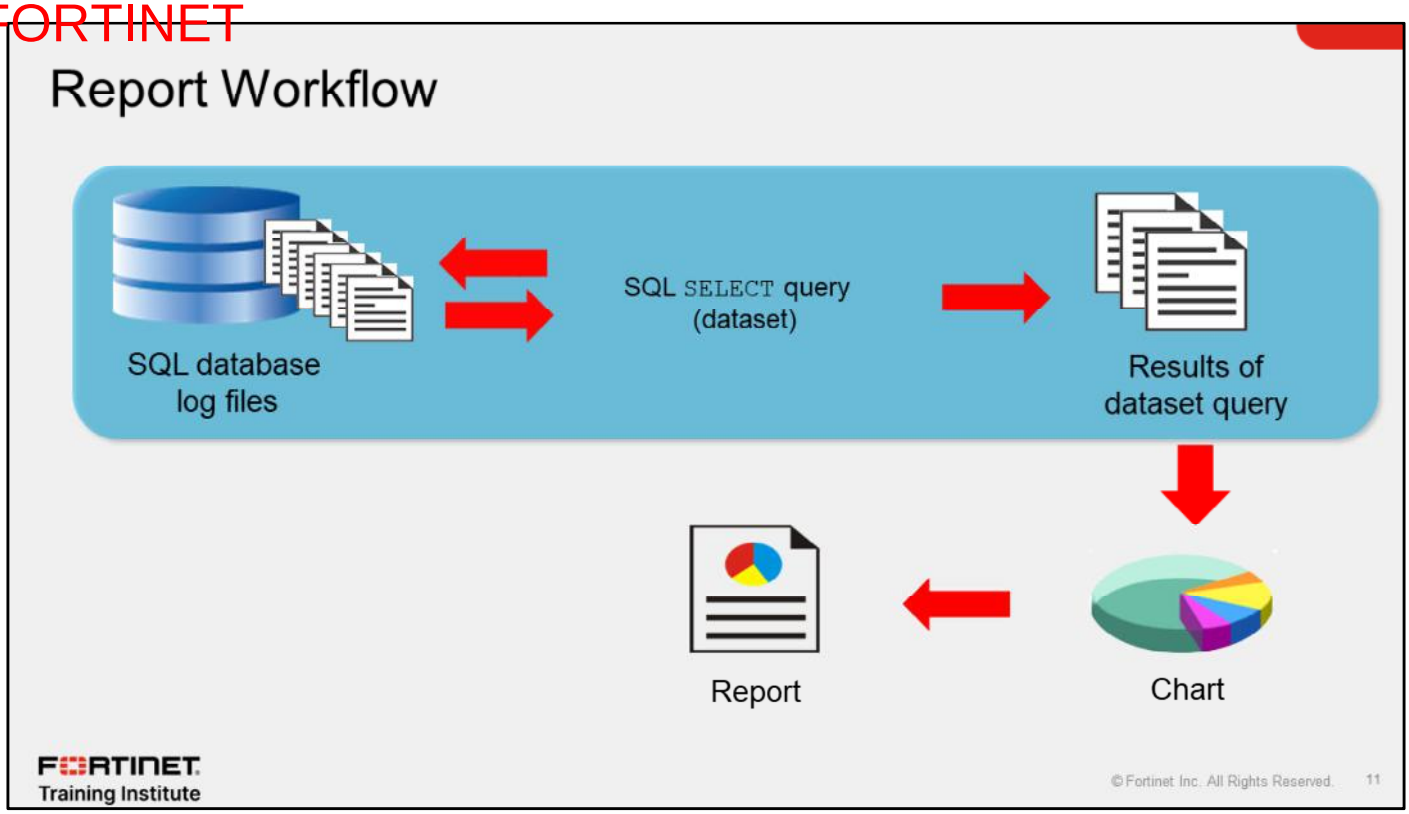
As this slide shows, the number of fields can be very large. For this reason, cloning and editing one of the predefined datasets may be the best approach, if none of them meet your requirements.



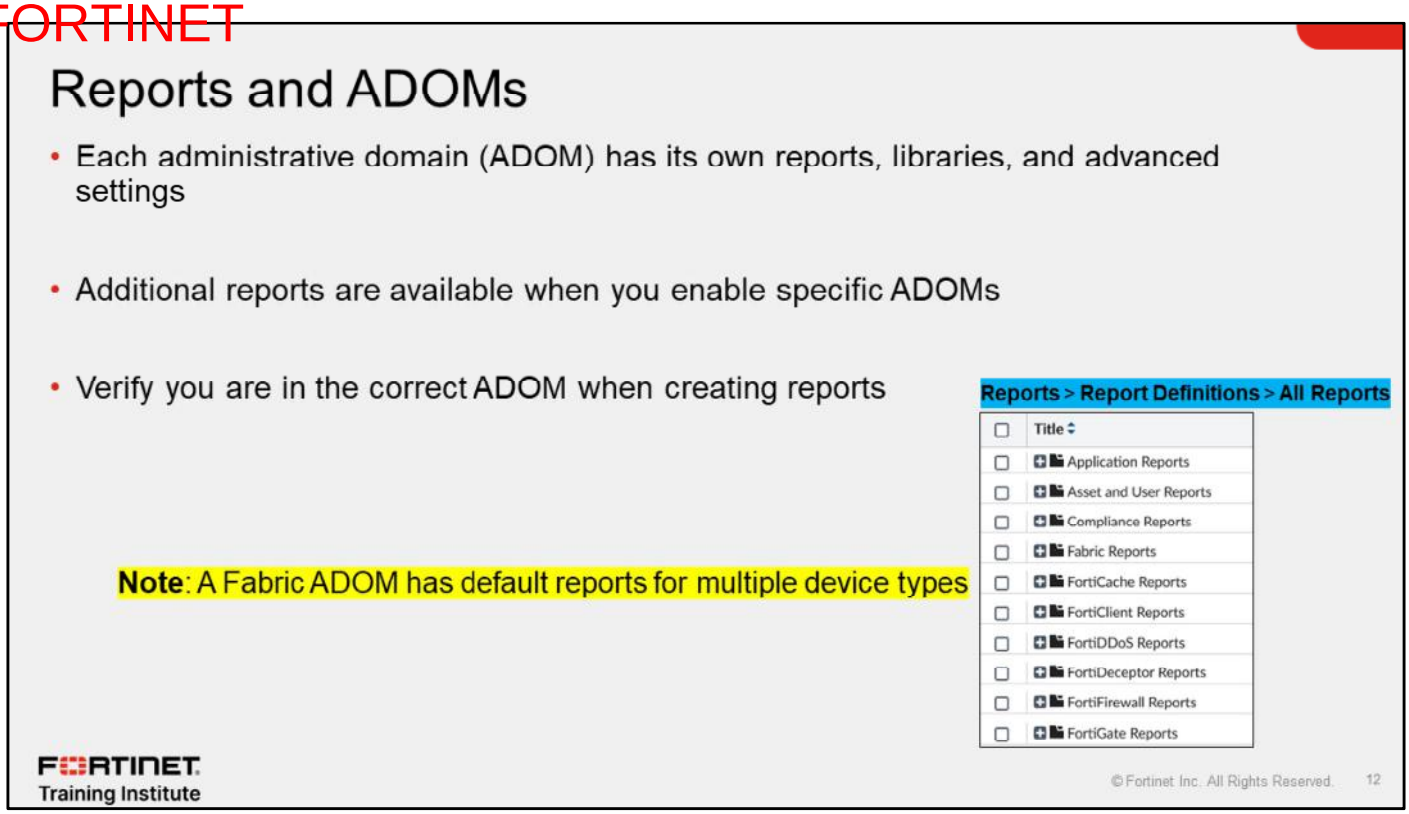
You can use the fields you identify in the schema to build your queries. For example, you can select `srcip` and `srcport` from the traffic log type and then create a query.

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.

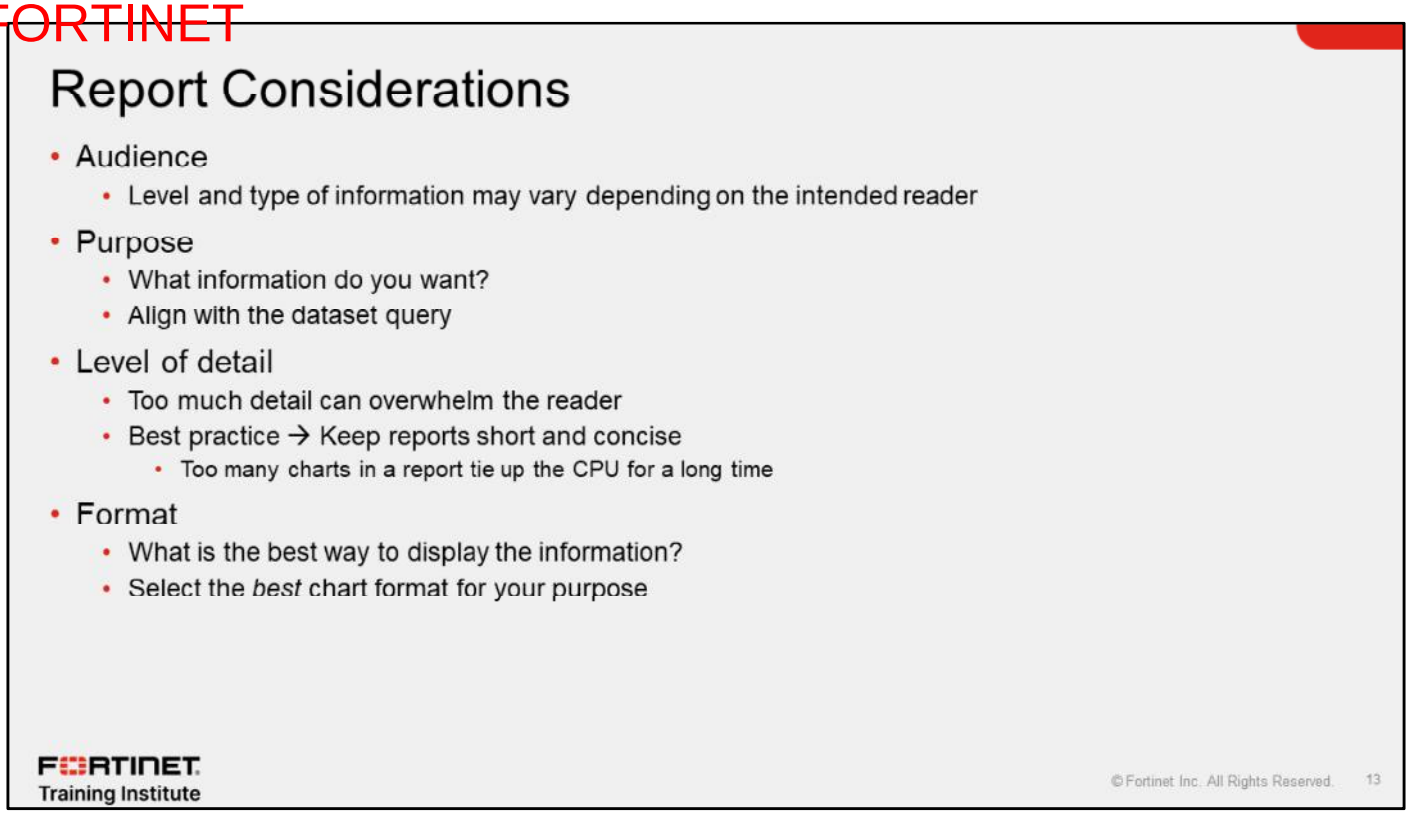


As this slide shows, the SQL database contains all logs. A SQL `SELECT` query polls the database for specific information. Based on the query, a subset of information stored in the logs is extracted. This subset of data populates a chart, and one or more charts exist within a report.



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.



Before you configure or create a report, there are certain factors you need to consider to ensure the report is as effective as possible.

The first consideration is your audience. Who's going to be reading this report? Depending on their role, knowledge base, and skill level, you may need to add, remove, or modify charts in order to convey the information appropriately.

The second consideration is your purpose. If you look at the predefined reports, each one focuses on a specific piece of information. They are based on specific datasets and contain charts that format the query. So, reports must be focused to be effective and easily digestible, and this is achieved by having a strong purpose.

The next consideration is the level of detail. A best practice is to keep reports short and concise. Not only do they focus your view of your network and users, but shorter reports have fewer charts and fewer queries to run. This helps with performance because large reports affect CPU and memory.

The final consideration is format. You need to know how you want to format the data so that it displays in the most digestible and informative way possible. A table chart, bar chart, and pie chart don't necessarily represent the same data with the same effectiveness. Based on your query, you may only be able to use one type of chart, but if options are available, you need to select the best chart. Think about how the data would best be represented visually, and about the audience consuming the data.

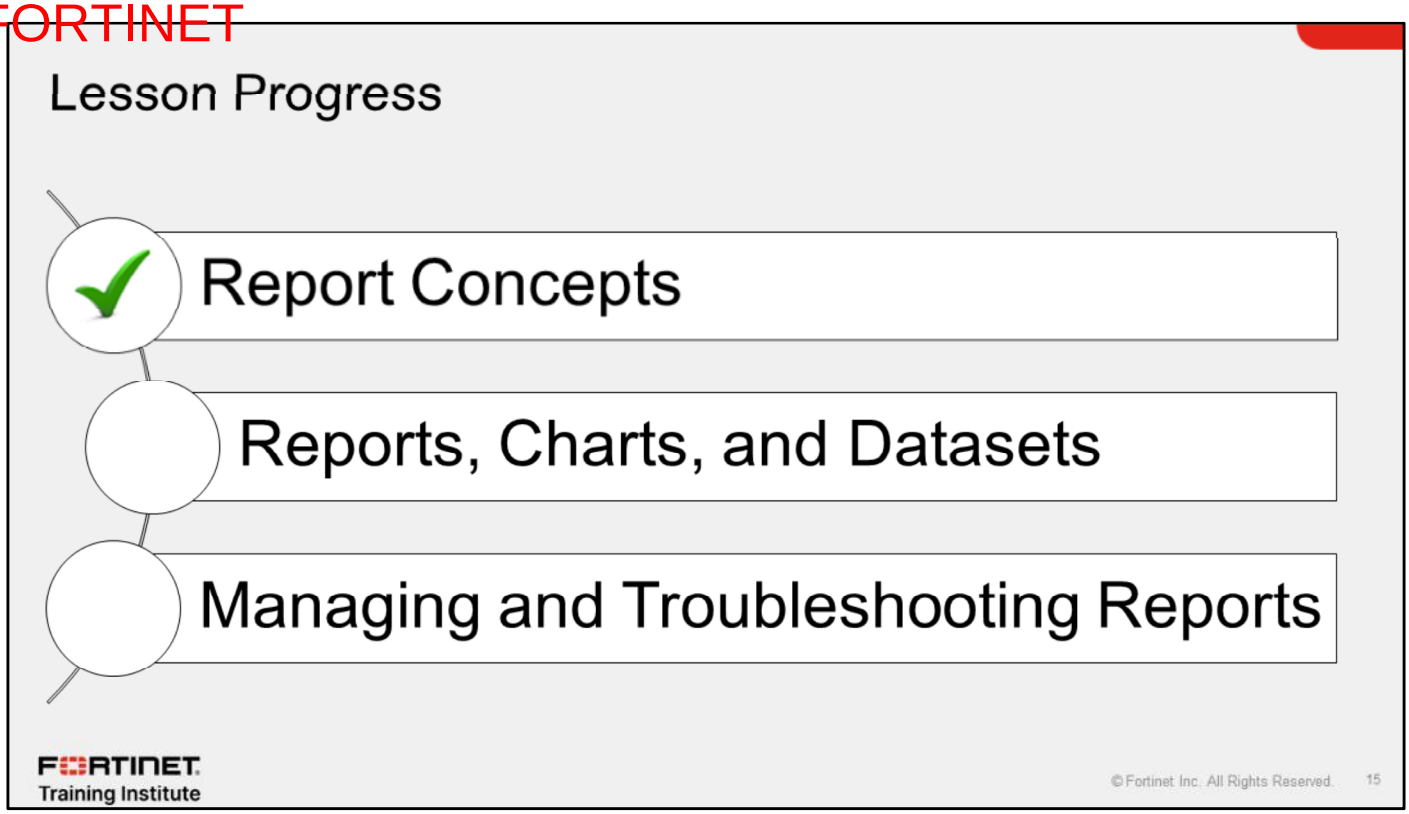
In addition to the chart format, you can change the report's design by adding separators, inserting page breaks, using images, and renaming charts.

Knowledge Check

1. On FortiAnalyzer, what is a dataset?
   - A. The database schema with all available fields in the table
   - ✓ B. A specific SQL SELECT query that retrieves data from the database

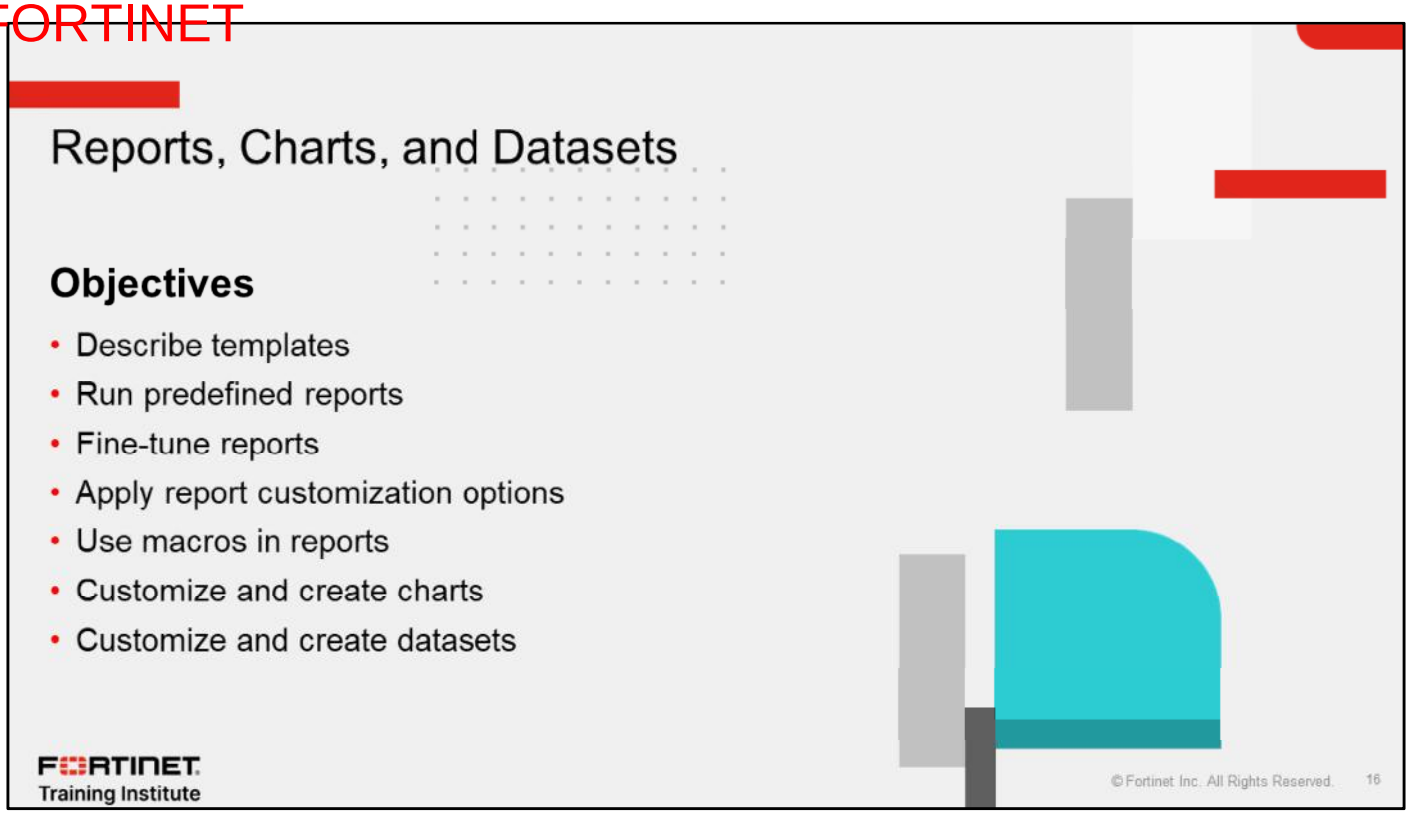
FORTINET Training Institute

 14



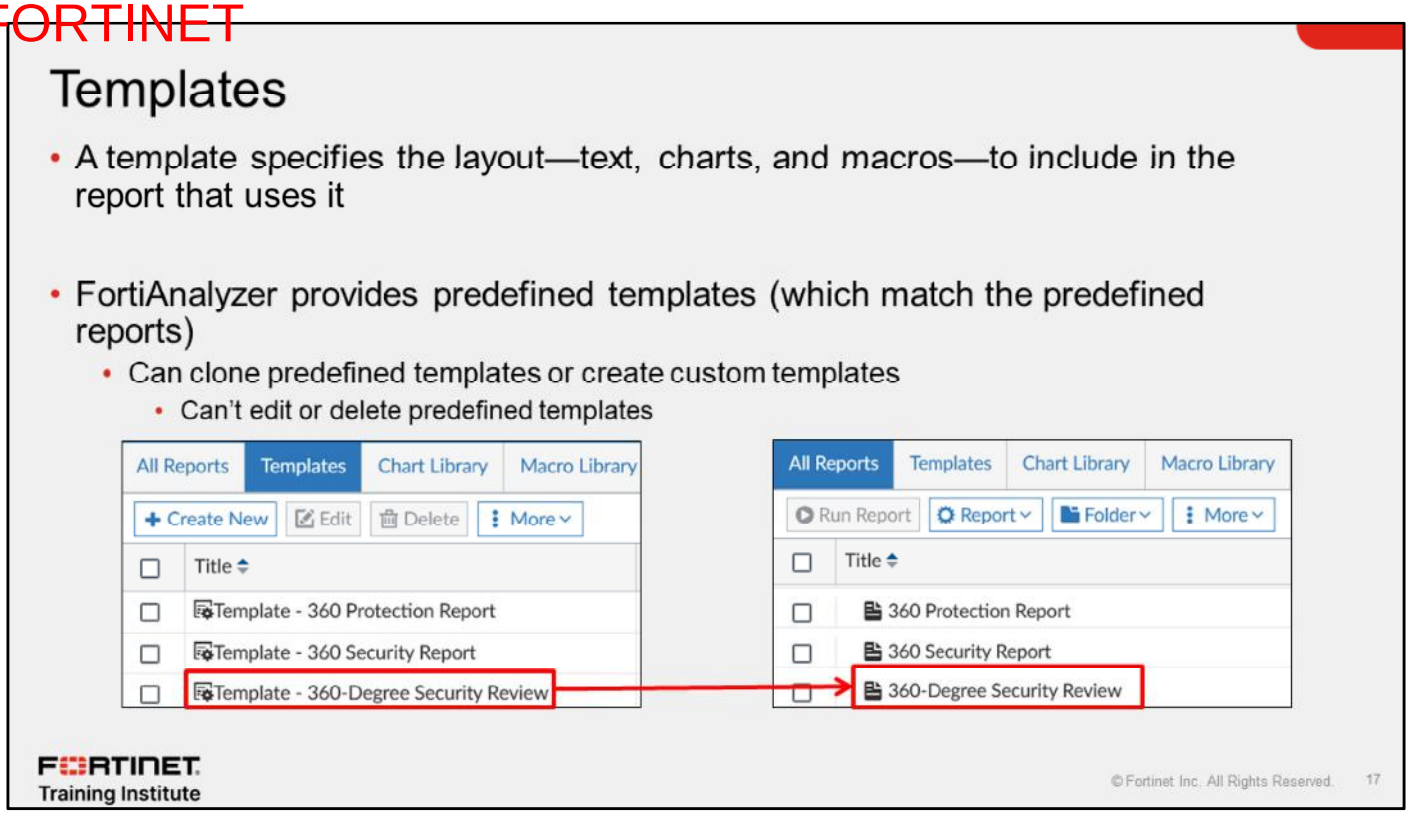
Good job! You now understand report concepts.

Now, you will learn how to generate and customize reports in FortiAnalyzer.



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

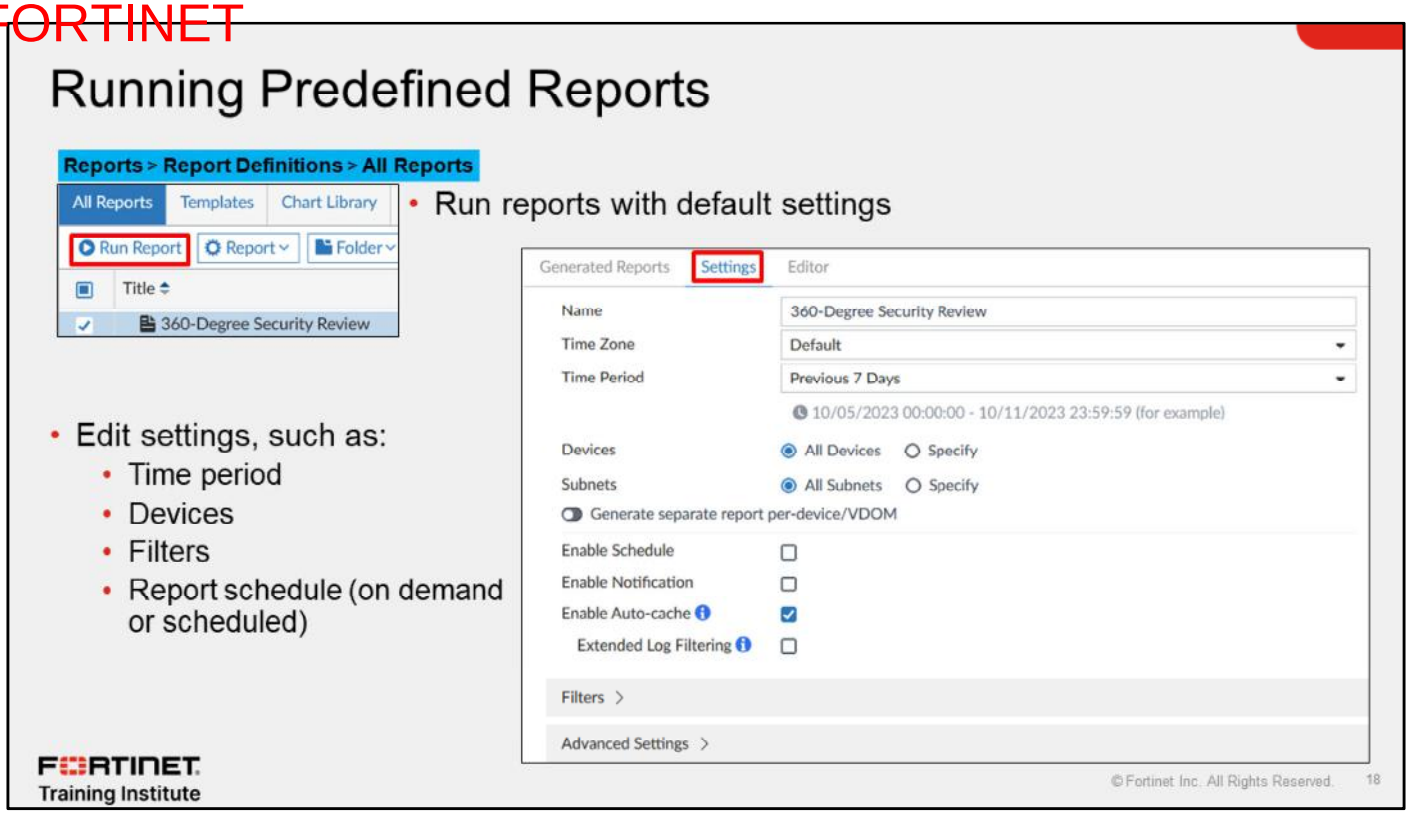
By demonstrating competence in report generation and customization, you will be able to generate reports specific to your requirements.



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 Template – 360-Degree Security Review template is the template used by the predefined 360-degree Security Review report.

Templates don't contain any data. Data is added 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.

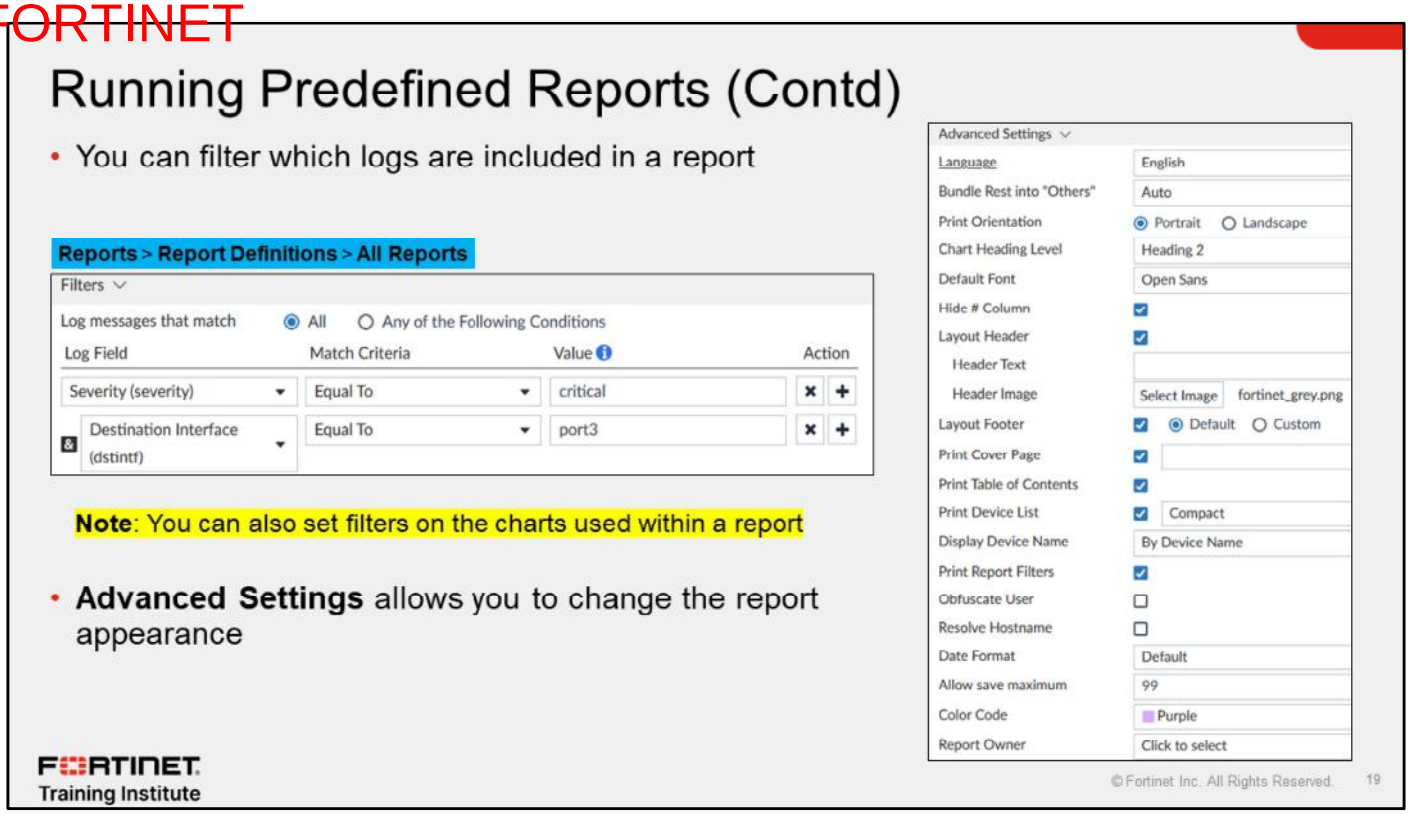


FortiAnalyzer also provides predefined reports, each associated with a predefined template (the layout). Predefined reports come with basic, default settings already configured. These basic settings define the time period in which the report runs, which device, or devices, to run the report on, and whether the report generates as a single report or separate reports per device or VDOM.

You can run the predefined reports *as is*, but at 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.

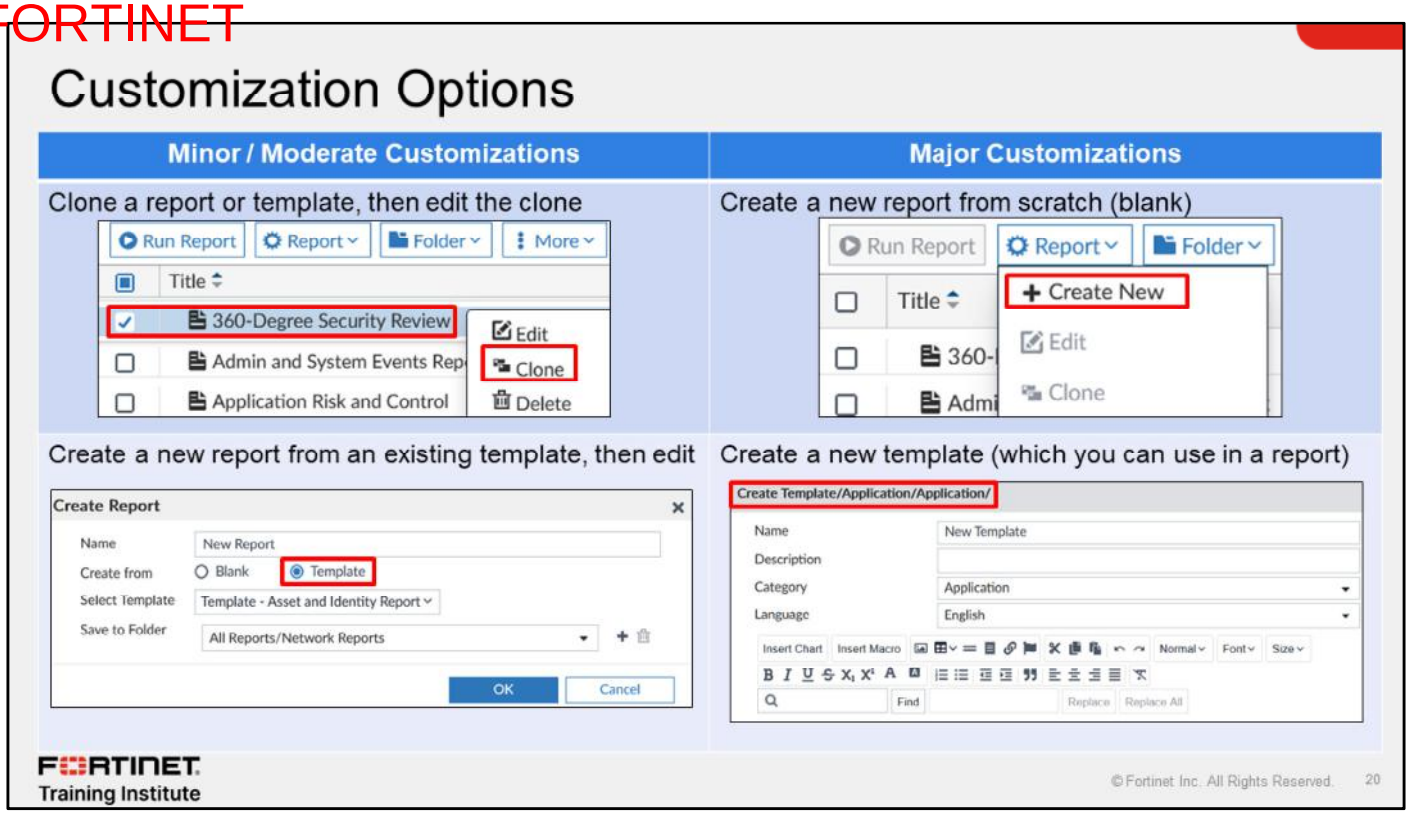
After it is generated, you can view a report in multiple formats, including HTML, PDF, XML, CSV, and JSON.



If a predefined report comes extremely close to meeting all 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 on 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**.



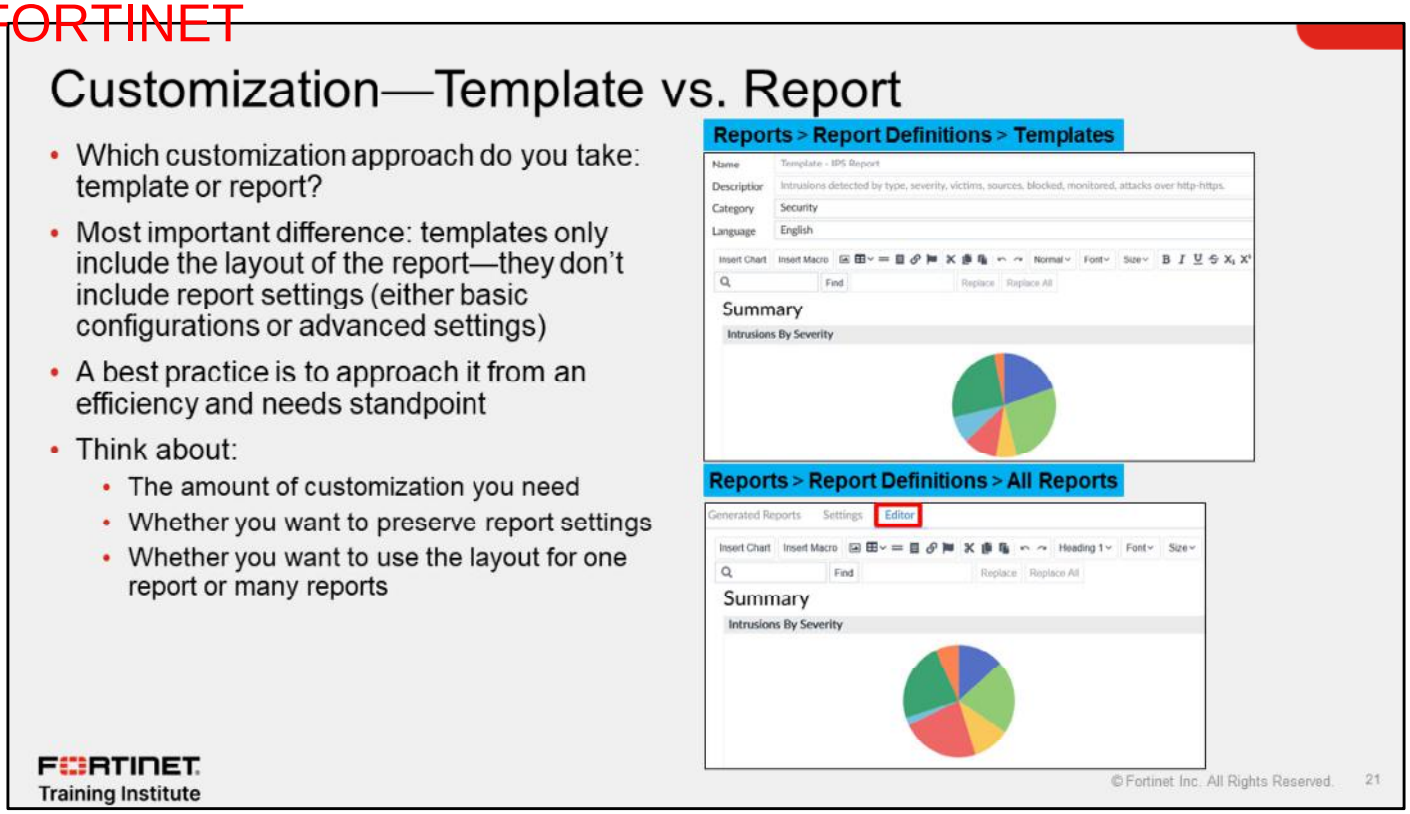
Predefined reports may not meet all your organization's requirements, even after you fine-tune the report settings. FortiAnalyzer provides you with the option to create new templates and reports from scratch, or you can customize existing templates and reports.

To make minor or moderate changes to existing templates or reports, you can use cloning. To use cloning, you clone a report or template and then edit the clone to suit your requirements.

For reports only, you can create a new report but base it 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 direct edits are not successful.

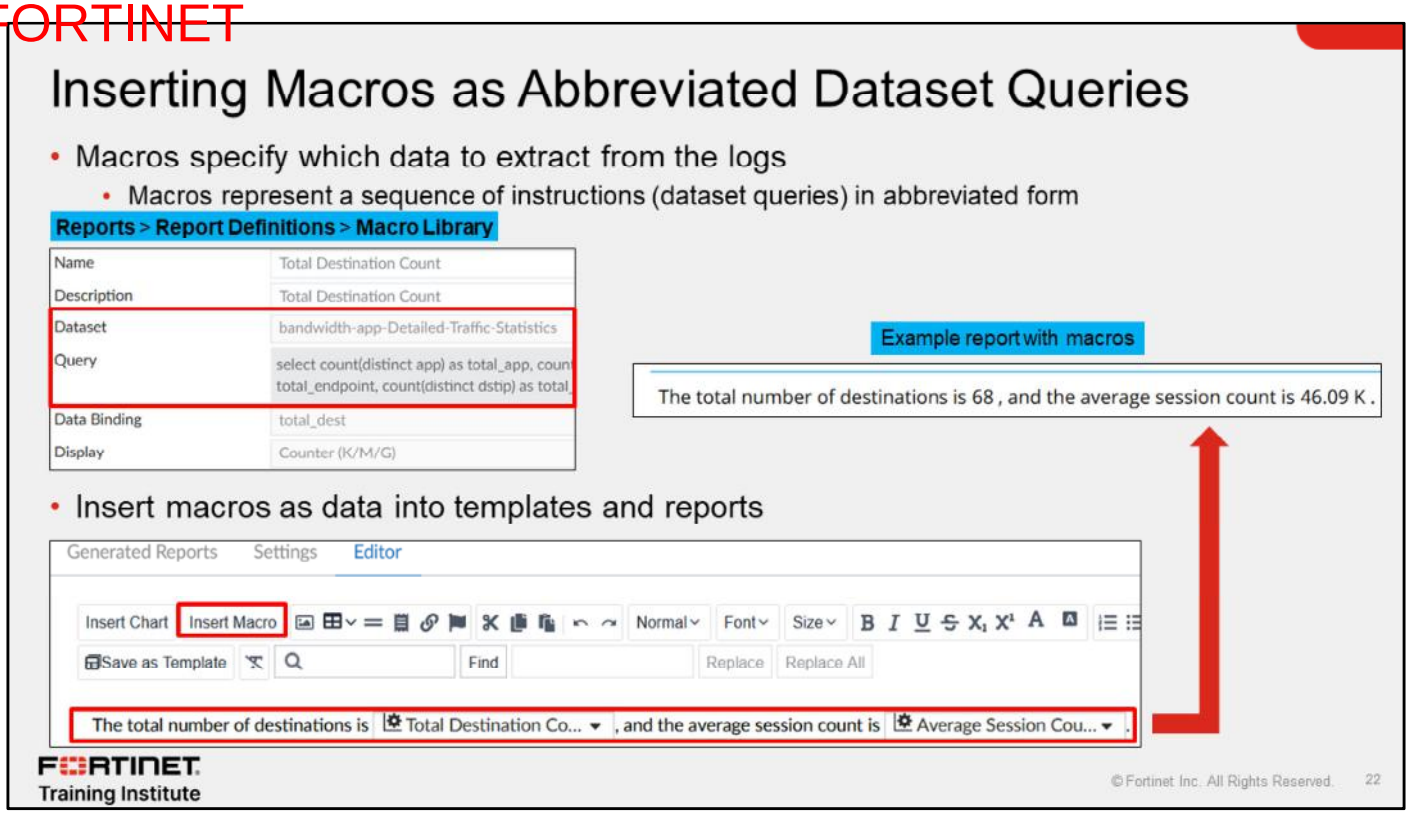
If you need to make major changes to existing templates or reports (if no report comes close to meeting your needs), you can create a new report or template from scratch.



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 know which customization approach to take? Do you approach the customization from the template side or the report side?

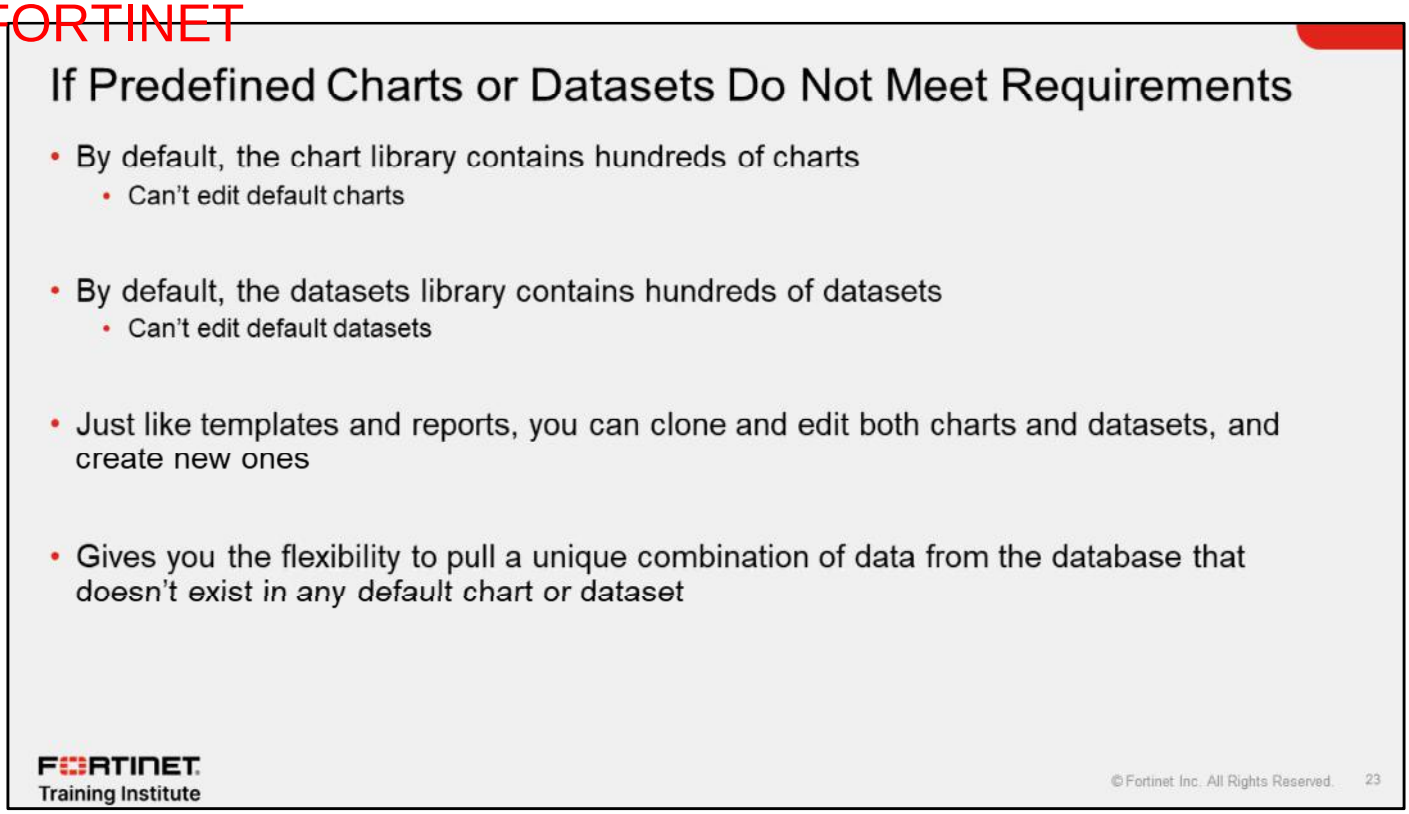
One of the most vital differences between templates and reports is that templates include only the details you can find under the **Editor** tab of the report—they don't include report settings (neither the basic configuration nor advanced settings). So, when deciding whether to perform customizations on the template side or the report side, the choice depends on what you want to preserve and what you want to modify.

In the end, there is no *correct* approach. Multiple methods can achieve the same results. A best practice is to approach the decision from an efficiency and needs standpoint.

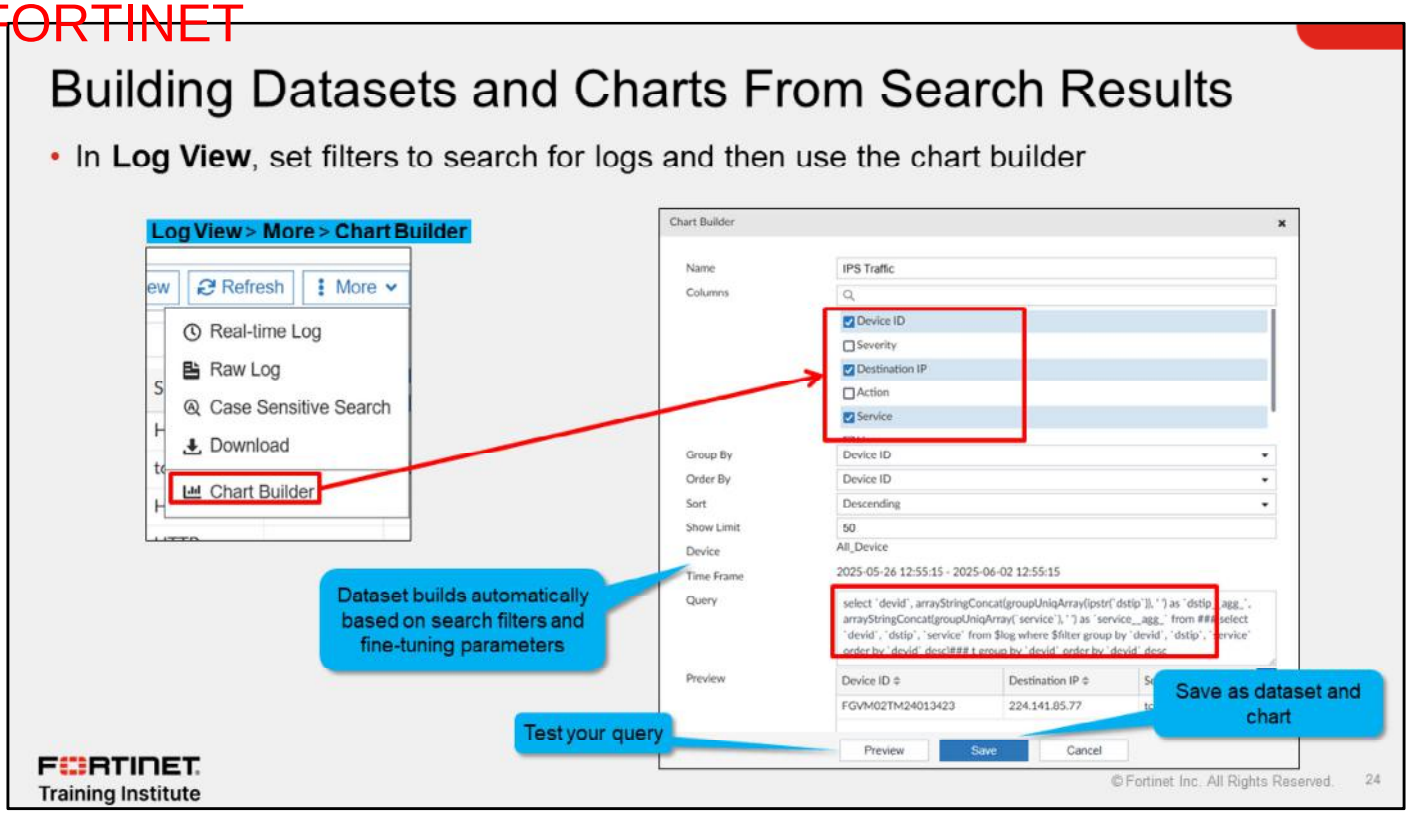


On FortiAnalyzer, macros specify which data to extract from the logs—they represent dataset queries in abbreviated form. You can insert macros as data in your reports, without having to use a chart to display the data. FortiAnalyzer provides predefined macros, or you can create your own custom macros.

Note that macros are ADOM-specific.

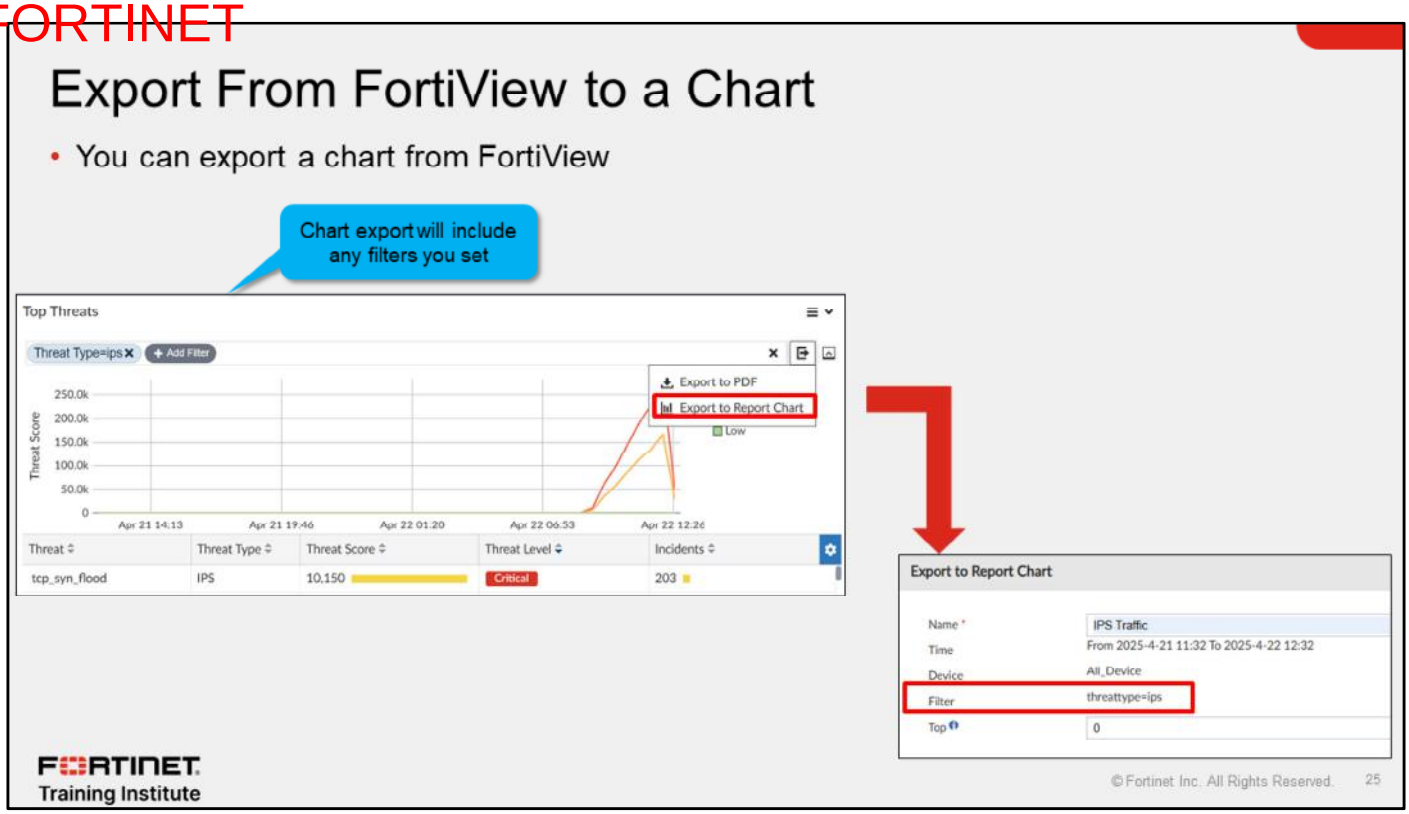


In some cases, simply adding or removing default charts from a report or template may not meet your requirements: You might need to pull a unique combination of data from the database when no predefined chart or dataset for that unique combination exists. In cases like these, you can either clone and edit charts and datasets or create new charts and datasets from scratch.



A quick way to build a custom dataset and chart is to use the chart builder tool. This tool allows you to build a dataset and chart automatically, based on your filtered search results. In **Log View**, set filters to return the logs you want. Then, in the **Tools** 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



You can export a chart from FortiView. The chart export includes any filters you set on FortiView.

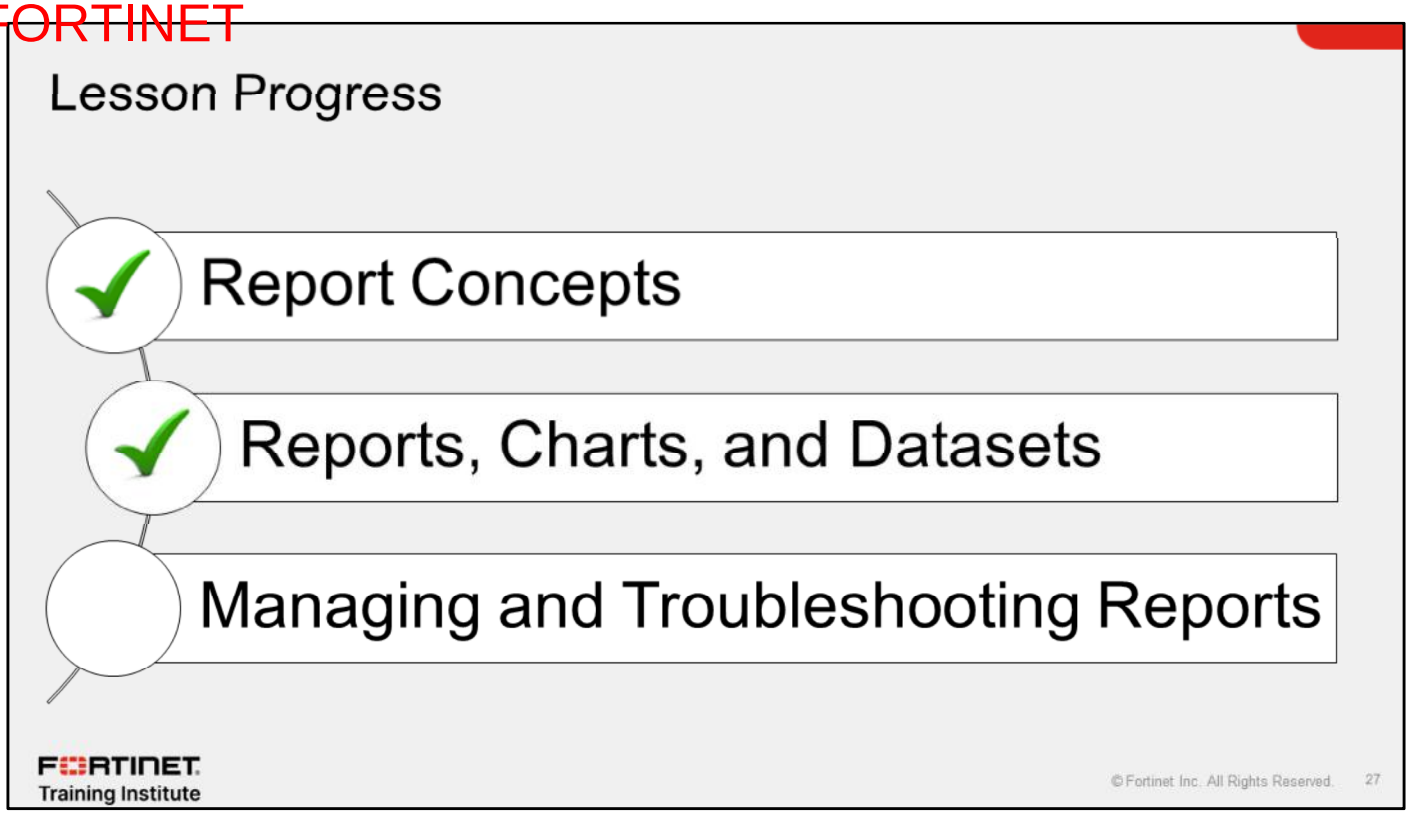
Knowledge Check

1. What is not found in templates?
   - ✓ A. Report schedule
   - B. Charts

2. Which statement about macros is true?
   - ✓ A. Macros are abbreviated dataset queries.
   - B. Macros cannot be customized.

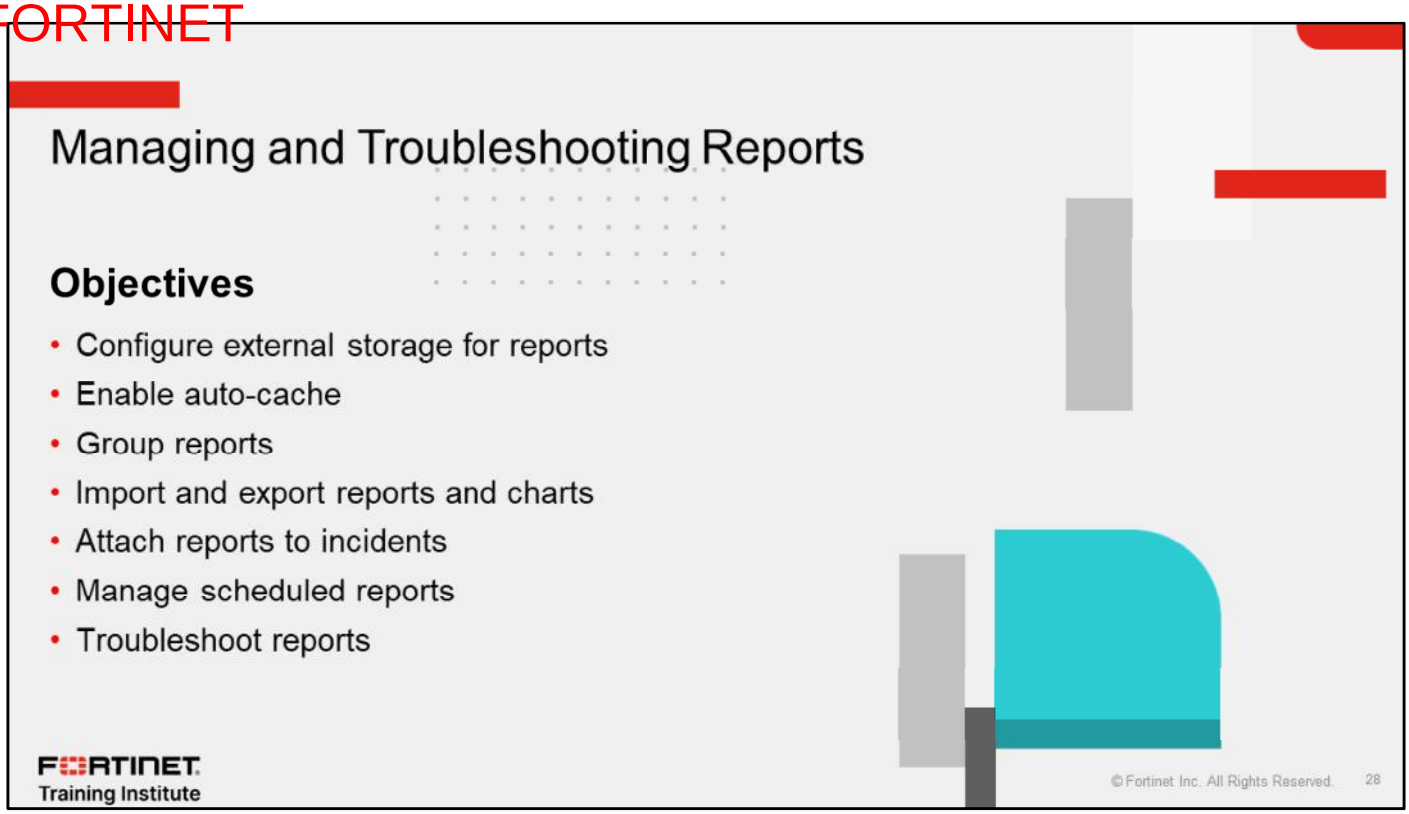
FORTINET Training Institute

 26



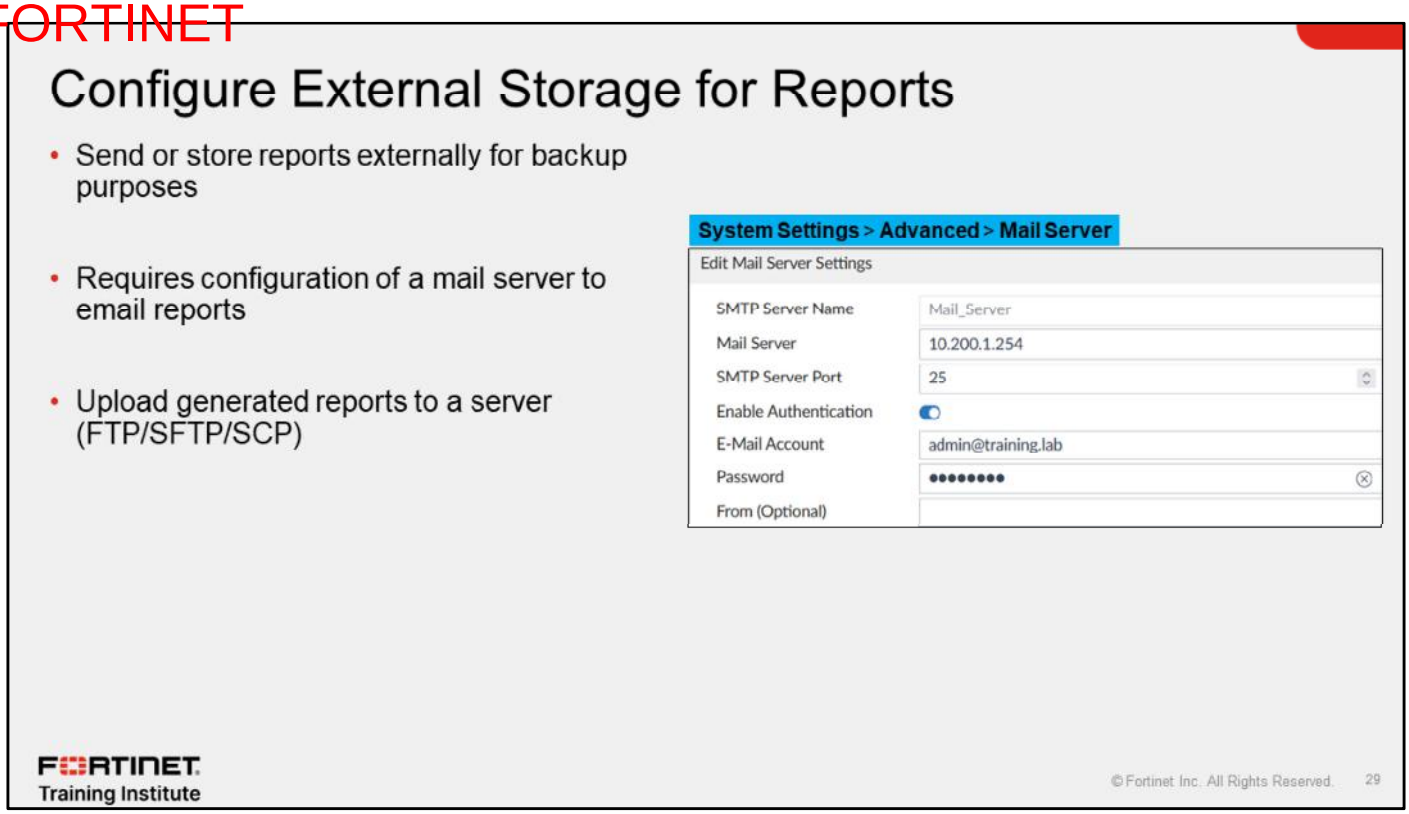
Good job! You now understand how to generate and customize reports, charts, and datasets.

Now, you will learn how to manage and troubleshoot reports.



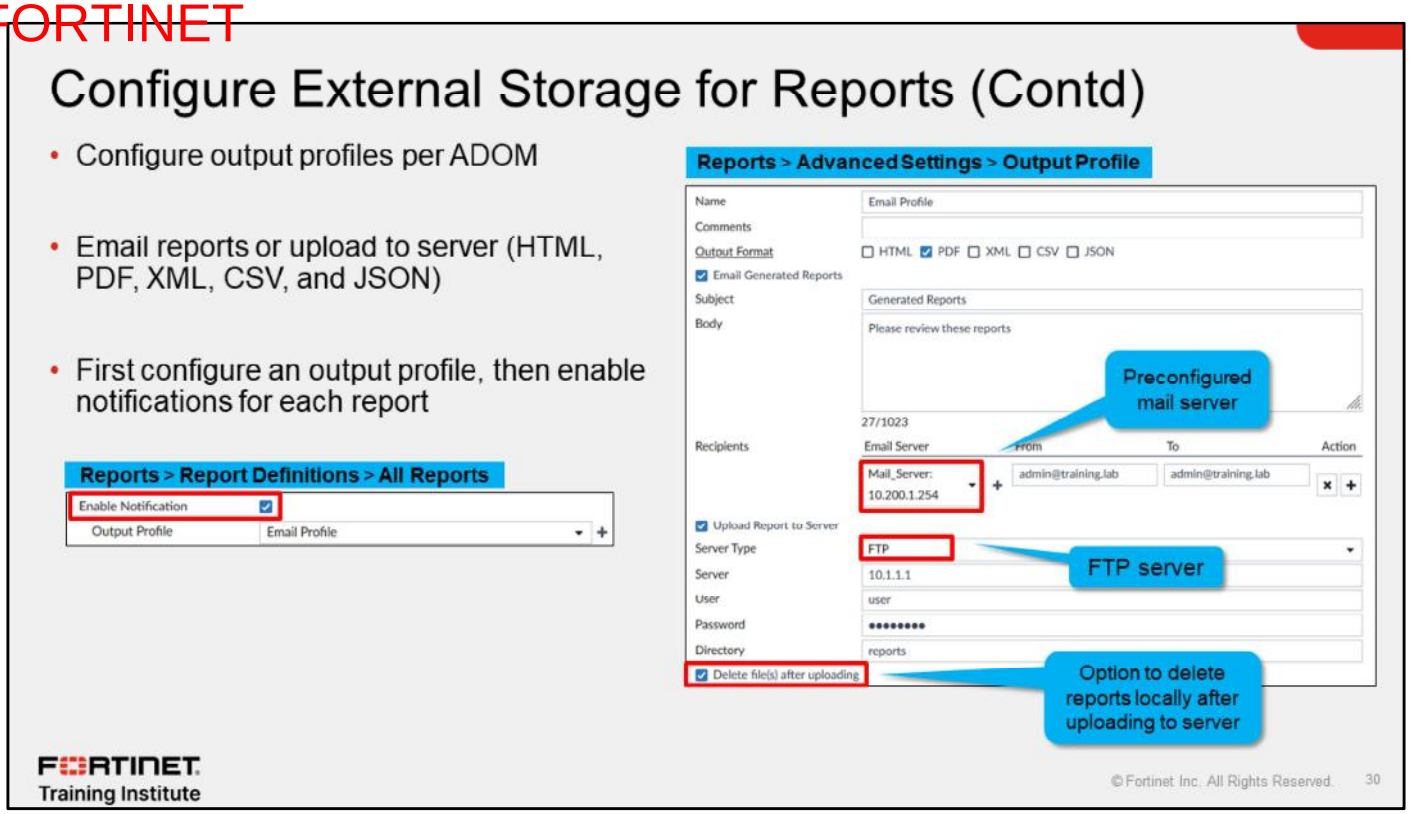
After completing this section, you should be able to achieve the objectives shown on this slide.

By demonstrating competence in report management, you will be able to handle, store, and more efficiently control reports and report generation.



You can configure FortiAnalyzer to email generated reports to specific administrators, or to upload generated reports to an external server.

To use any of these external storage methods, you must first set up the backend. To email generated reports, you must first configure a mail server, as shown on this slide. To upload logs to a server, you must first configure the mail server to accept connections from FortiAnalyzer.

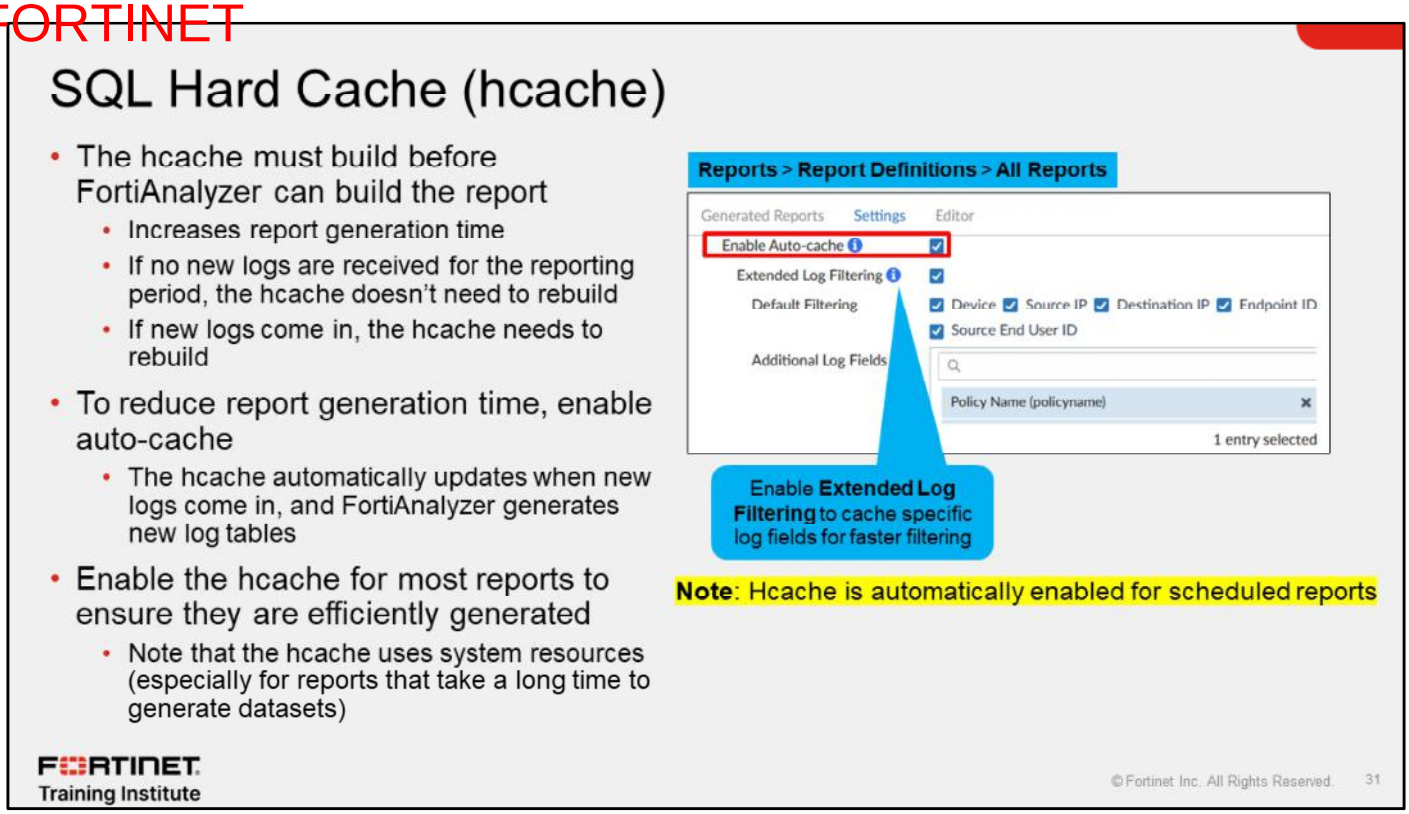


To send reports to an external location, you must enable notifications and select an appropriate output profile.

An output profile specifies the following:

- The format of the report, such as HTML, PDF HTML, XML, CSV, or JSON
- Whether to email generated reports or upload them to a server
  You can specify one or both options or create multiple output profiles. Server options include FTP, SFTP, and SCP.
- Whether to delete the report locally after uploading it to the server

If you enable ADOMs, each ADOM has its own output profiles.



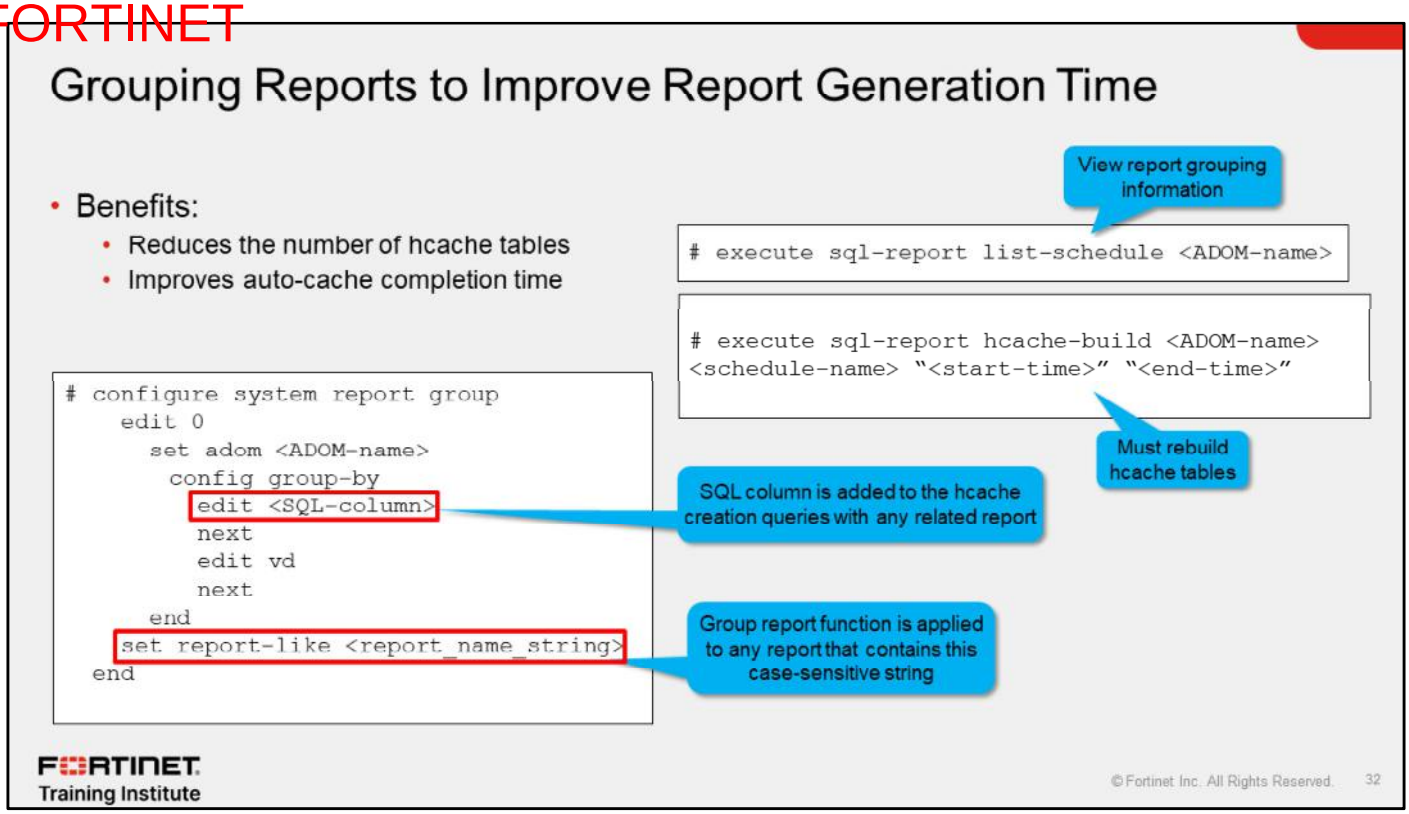
When a report is generated, the system builds the charts from precompiled SQL hard-cache data, known as the hcache. hcache is a proprietary FortiAnalyzer caching system that stays on the disk in the form of a database table. Unlike other caches, hcache tables are persistent and are not removed based on a set period of time.

If the hcache is not built when you run the report, the system must create the hcache first and then build the report, which adds time to the report generation. However, if FortiAnalyzer does not receive any new logs for the reporting period, when you run the report a second time, it is much faster because the hcache data is already precompiled.

To boost the report performance and reduce report generation time, you can enable auto-cache in the settings of the report. When you do this, the hcache is automatically updated when new logs come in and new log tables are generated.

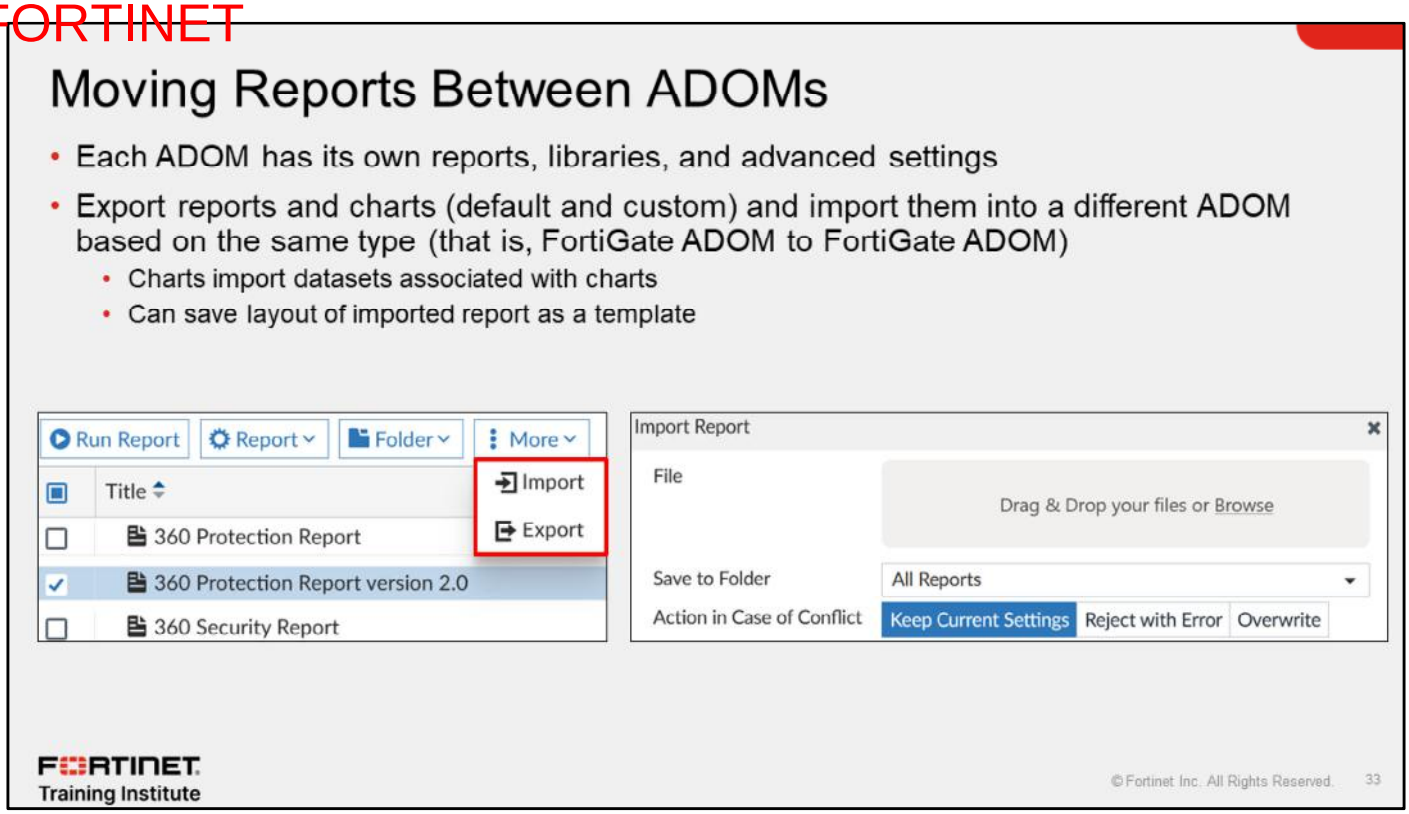
Note that the hcache is automatically enabled for scheduled reports. If you are not scheduling a report, you may want to consider enabling hcache. This ensures reports are efficiently generated. However, be aware that this process uses system resources, especially for reports that require a long time to assemble datasets. Monitor your system to ensure it can handle it.

Additionally, you can enable extended log filtering to cache specific log fields for faster filtering.



If the same (or similar) reports are run against many different FortiGate devices, you can significantly improve report generation time by grouping the reports. Report grouping can reduce the number of hcache tables and improve auto-cache completion time and report completion time.

After you configure report grouping using the `configure system report group` CLI command, you must rebuild the report hcache tables. You can rebuild the hcache tables for those reports.

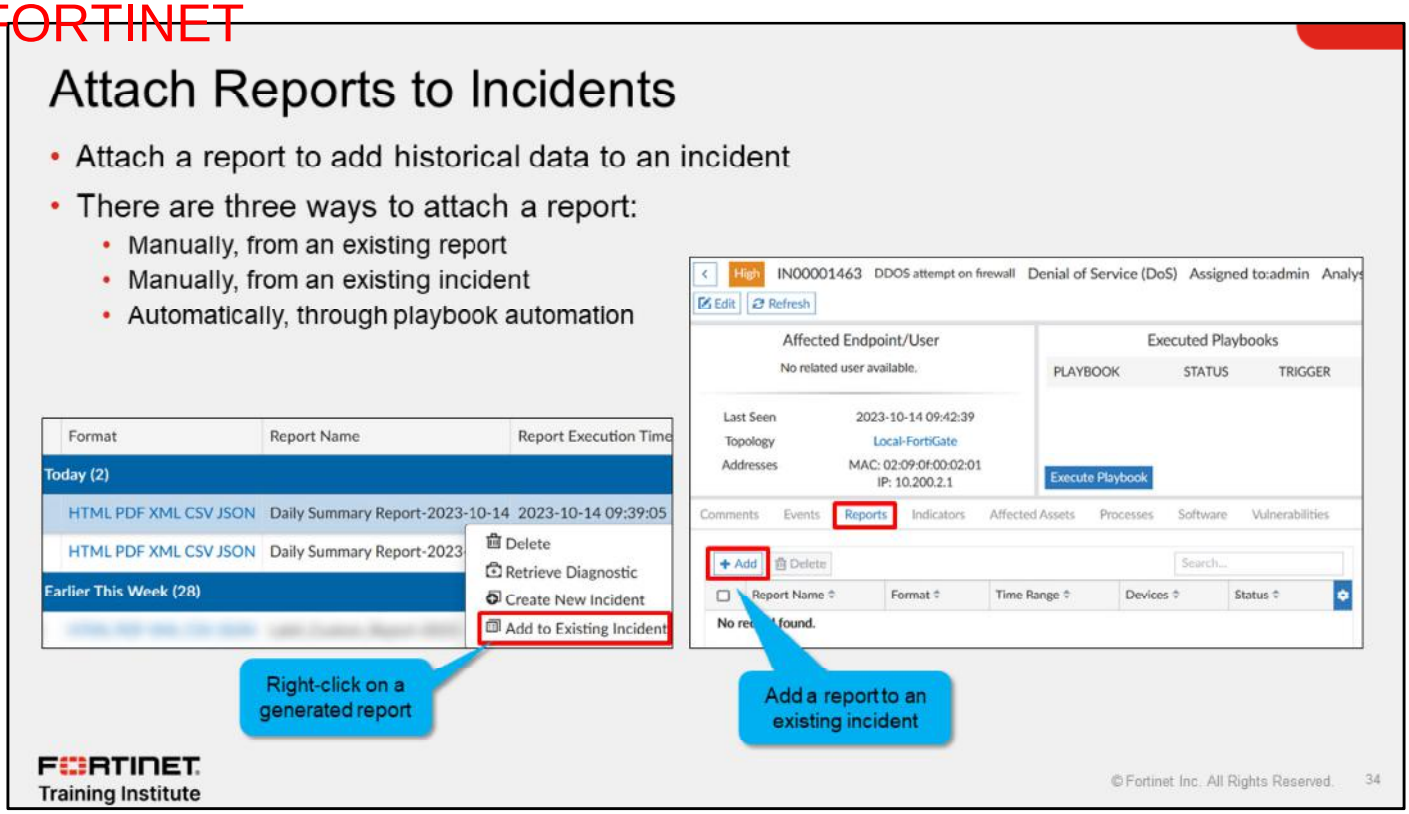


Remember, each ADOM has its own reports, libraries, and advanced settings. You can, however, import and export reports and charts (whether default or custom) into different ADOMs within the same FortiAnalyzer device or a different FortiAnalyzer device. Both ADOMs must be of the same type.

You can't export templates and datasets. However, when you import an exported report, you can save the layout of the report as a template. When you export a chart, the associated dataset is exported with it, so when you import an exported chart, the associated dataset is imported as well.

You can export and import reports through the right-click menu on the **Reports** page.

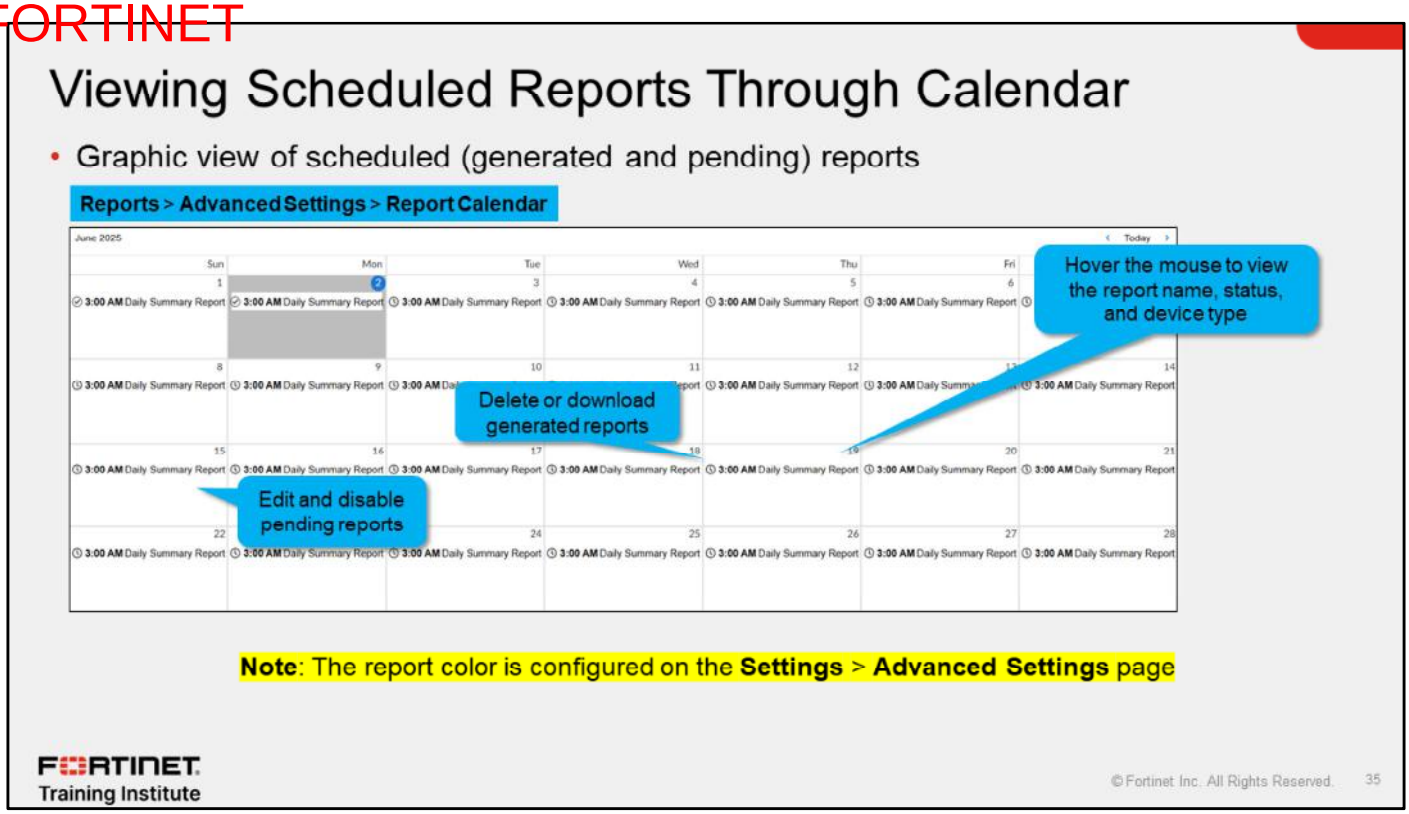
The chart library includes export and import functions in the toolbar.



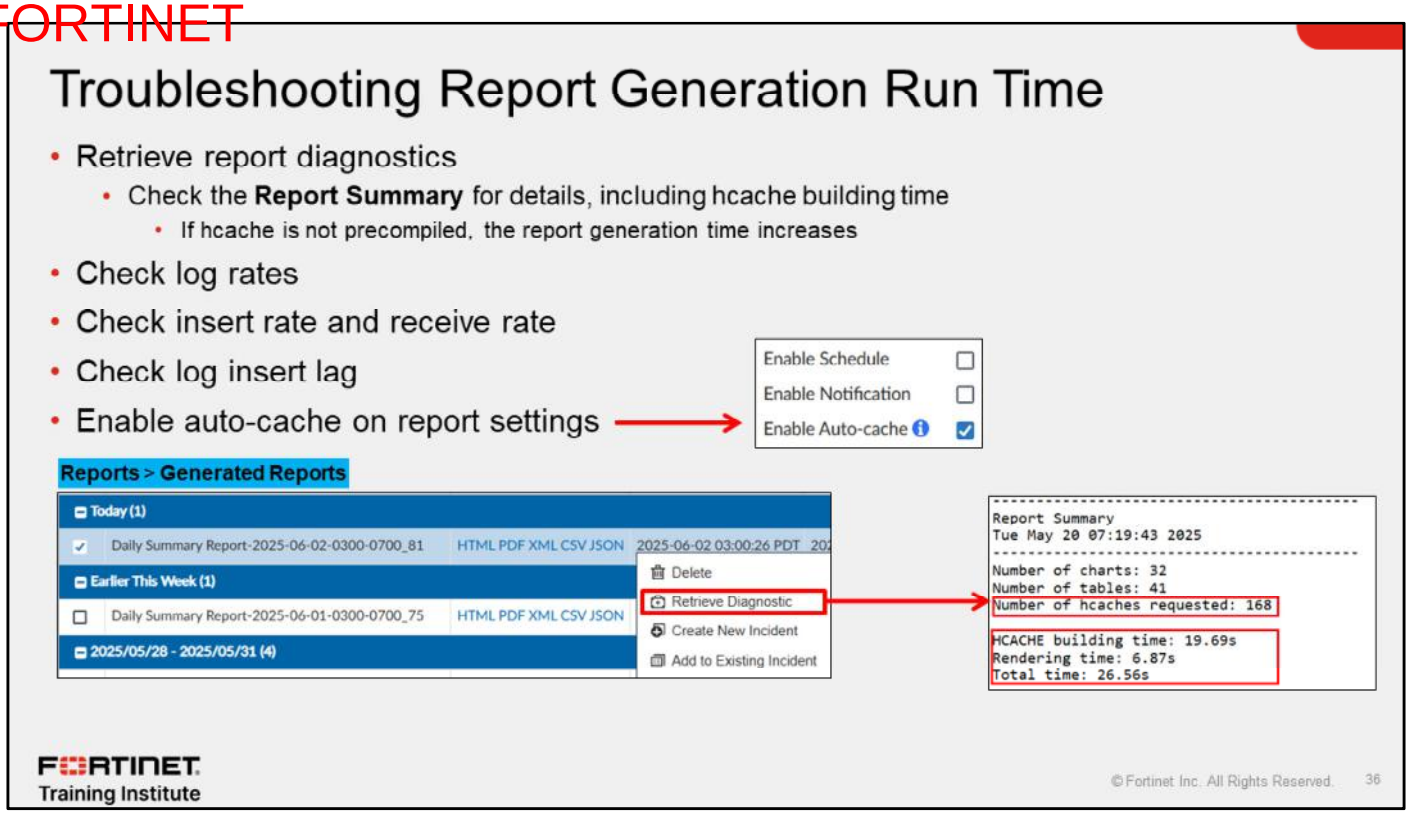
You can attach reports to incidents to add historical data in addition to real-time events.

These are the three ways that you can attach a report:
- Manually, from an existing report
- Manually, from an existing incident
- Automatically, through automation playbooks

This slide shows how to manually attach reports from an existing report and from an existing incident.

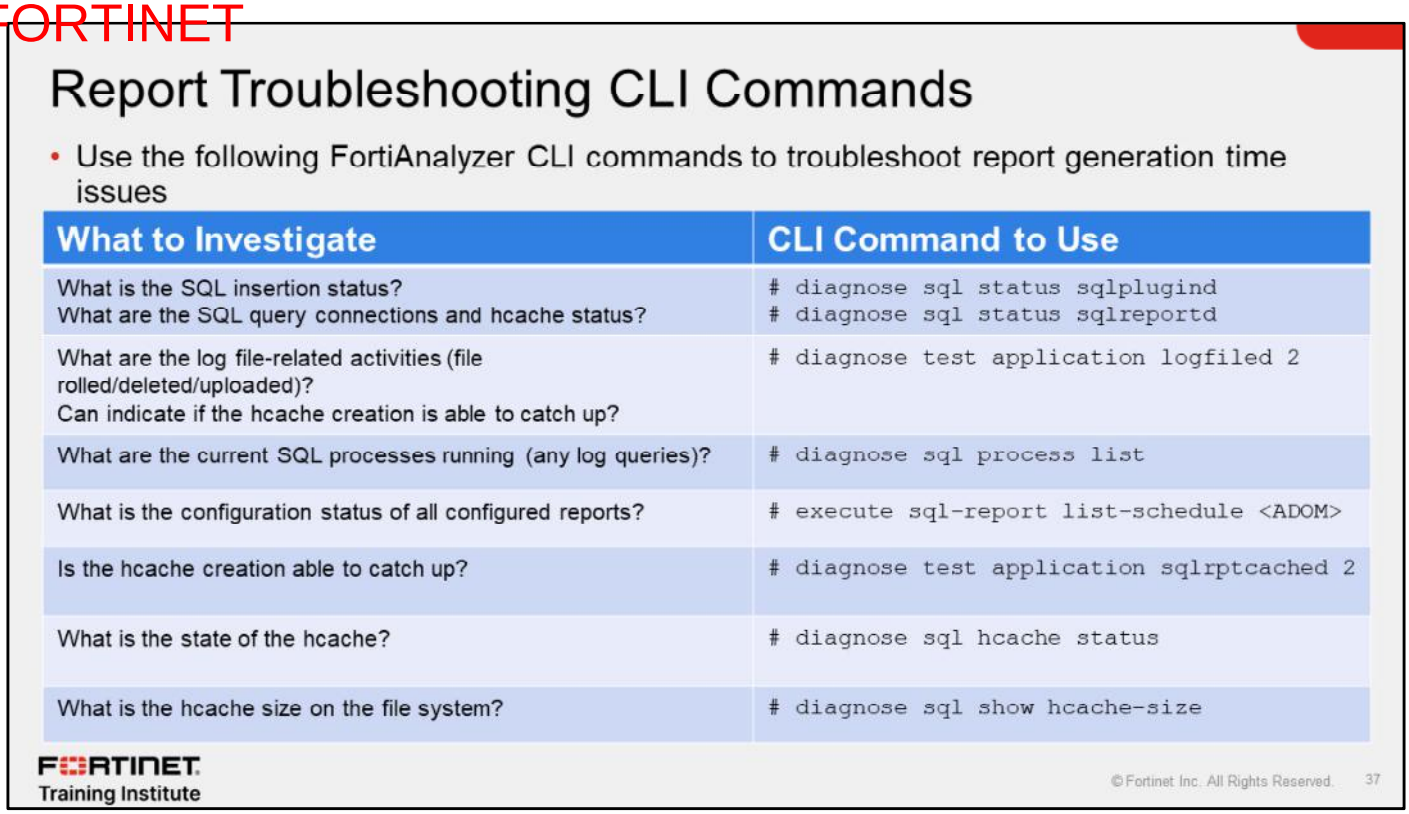


The report calendar provides an overview of all your scheduled reports. A check mark means the report was generated, and a clock icon means it is pending. When you hover your mouse over a scheduled report, a notification opens displaying the report name, status, device type, and start time. You can edit and disable upcoming, scheduled reports, as well as delete or download completed reports, by right-clicking the name of the report in the calendar. Note that you do not configure scheduling on this page. You configure scheduling in the specific report configuration. You can also configure reports to display in a specific color in the report calendar in the **Advanced Settings** window associated with the report.



If your network has a high volume of devices sending logs to FortiAnalyzer as well as high log volume, reports can take some time to generate. If you find reports are taking too long to generate, there are a few steps you can take to troubleshoot:

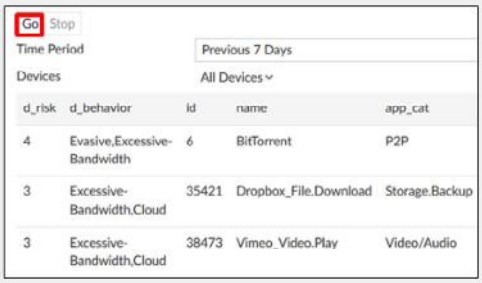
- Run diagnostics on your report and view the report summary at the end of the report. Look at the hcache time to see how long it took to build.
- Check your log rates to get an idea of log volumes.
- Check the insert rate, receive rate, and log insert lag. They can tell you the rate at which raw logs are reaching FortiAnalyzer (receive rate) and the rate at which they are indexed by the SQL database (insert rate) by the sqlplugind daemon. The log insert lag time tells you how many seconds the database is behind in processing the logs.
- Enable auto-cache in the report settings to boost the reporting performance and reduce report generation time. Scheduled reports have auto-cache enabled already.



This slide shows some CLI commands you can use to troubleshoot issues related to report generation time.

Empty Reports

- Check the time frame covered by the report
- Verify that you have logs from the time frame the report was run and from the device that the report was run for
- Test the datasets to ensure that the expected data is retrieved
  - If not, check the SQL query associated with the dataset



- Check the report advanced settings (such as user obfuscate)
  - Verify that the logs match any filter that you have set for the report

FORTINET Training Institute

 38

What happens if you run a report and it is empty or doesn't contain the desired information? Here are some troubleshooting tips:

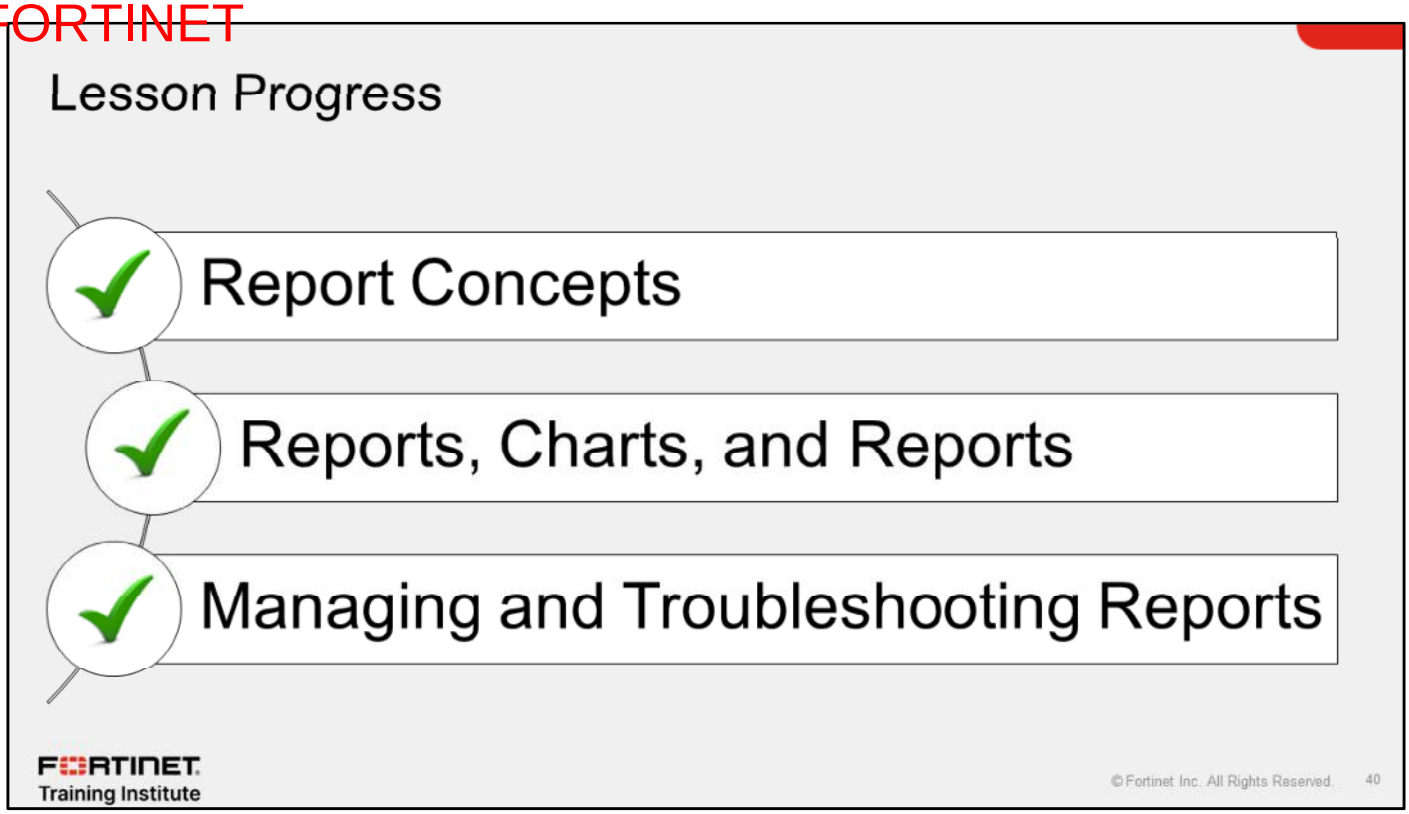
- Check the time frame covered by the report, which is listed within the report.
- Verify that you have logs from the time frame the report was run and from the device that the report was run for. A common cause of empty reports is logs being overwritten too quickly. In this case, the solution is to increase the disk quota and retention policy to ensure that logs are retained longer.
- Test the dataset in question and verify that it is retrieving the correct information. If it isn't, troubleshoot the SQL query because the dataset probably contains the error.
- Check your advanced settings for the report. A setting such as **user obfuscate** can result in abnormal usernames appearing in the report. Also, verify the filters attached to a report. It is possible that your filter is filtering out the desired logs.

Knowledge Check

1. Which data does the CLI command `# diagnose sql show hcache-size` provide?
   - ✓ A. Hcache size on the file system
   - B. State of the hcache

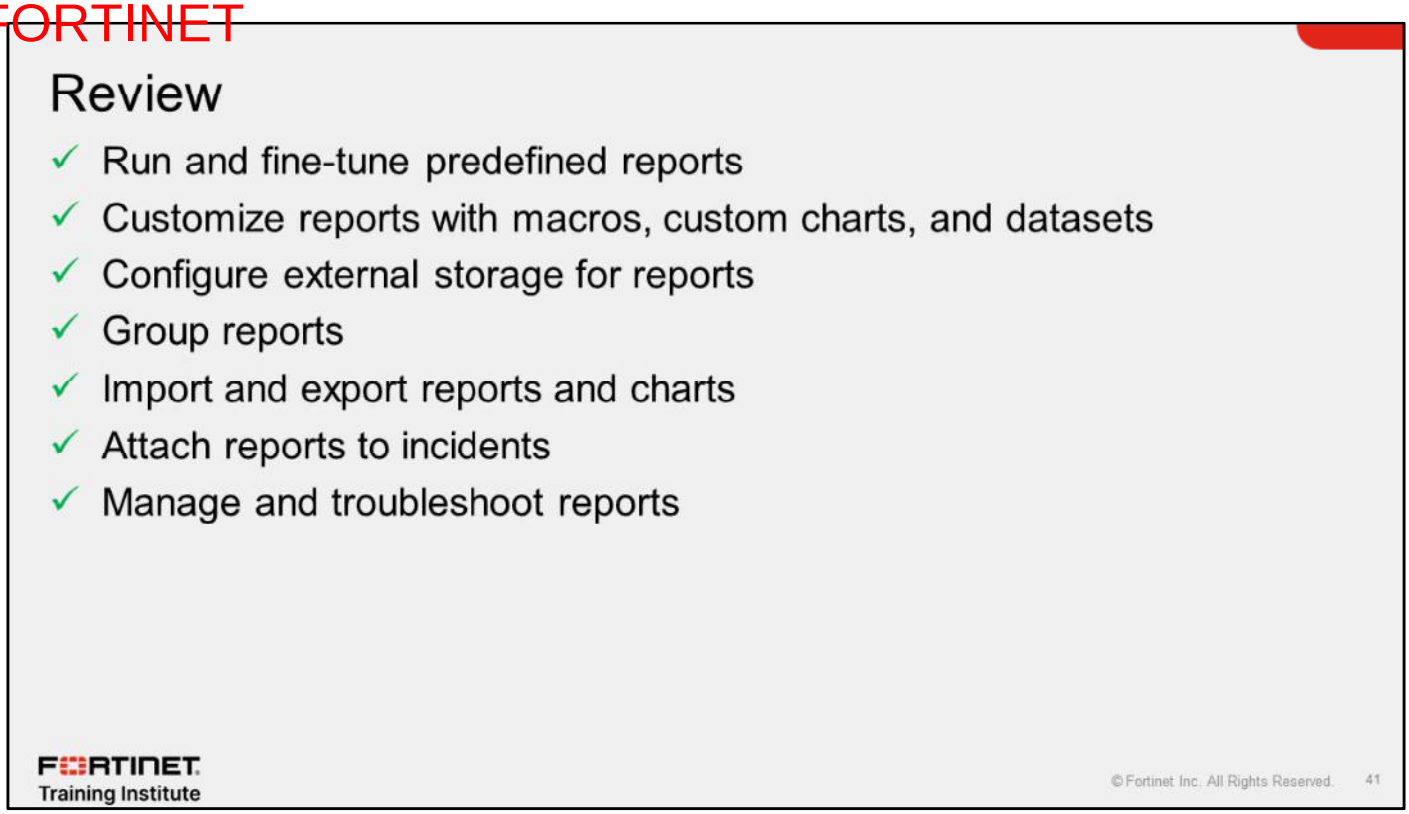
FORTINET Training Institute

 39



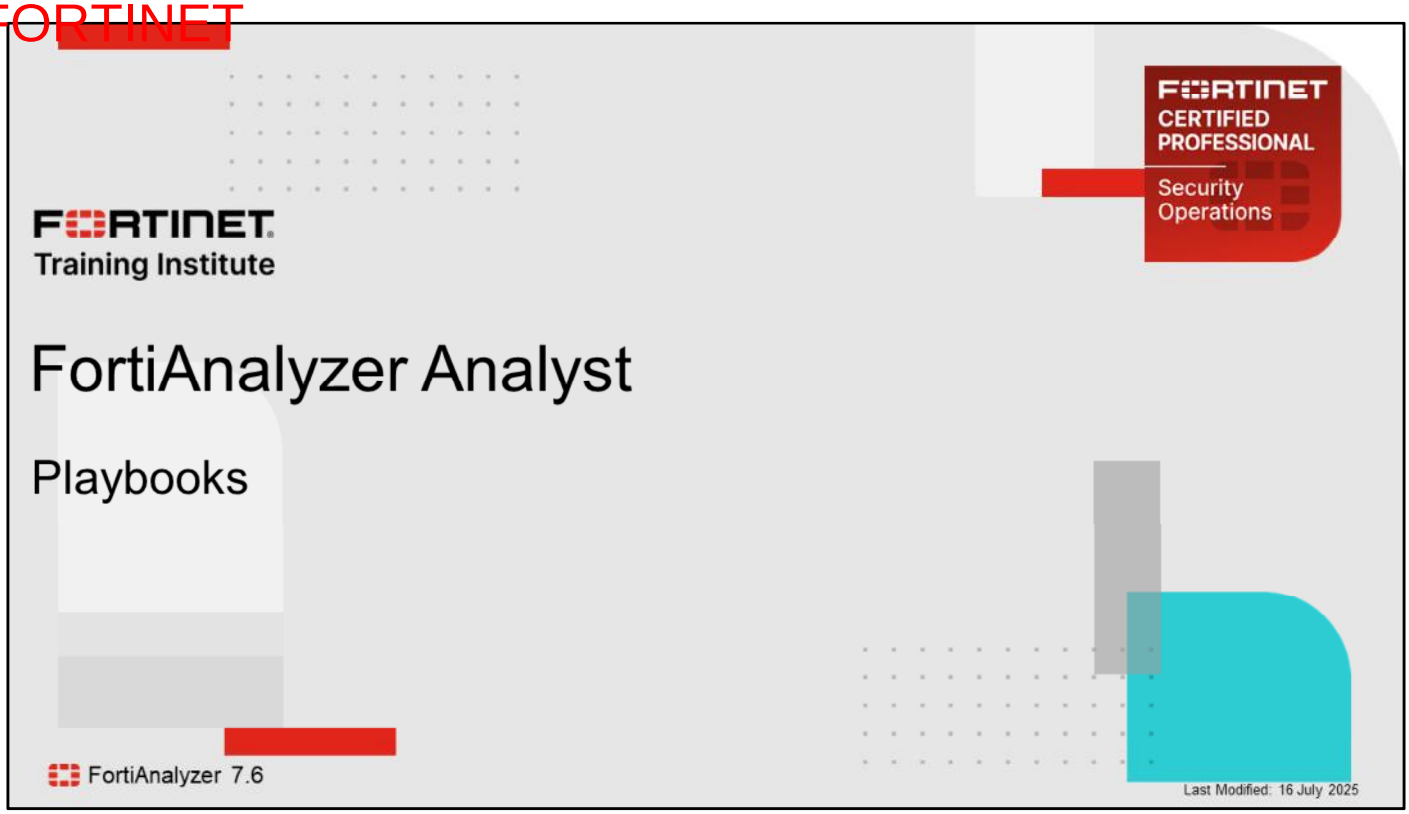
Congratulations! You have completed this lesson.

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

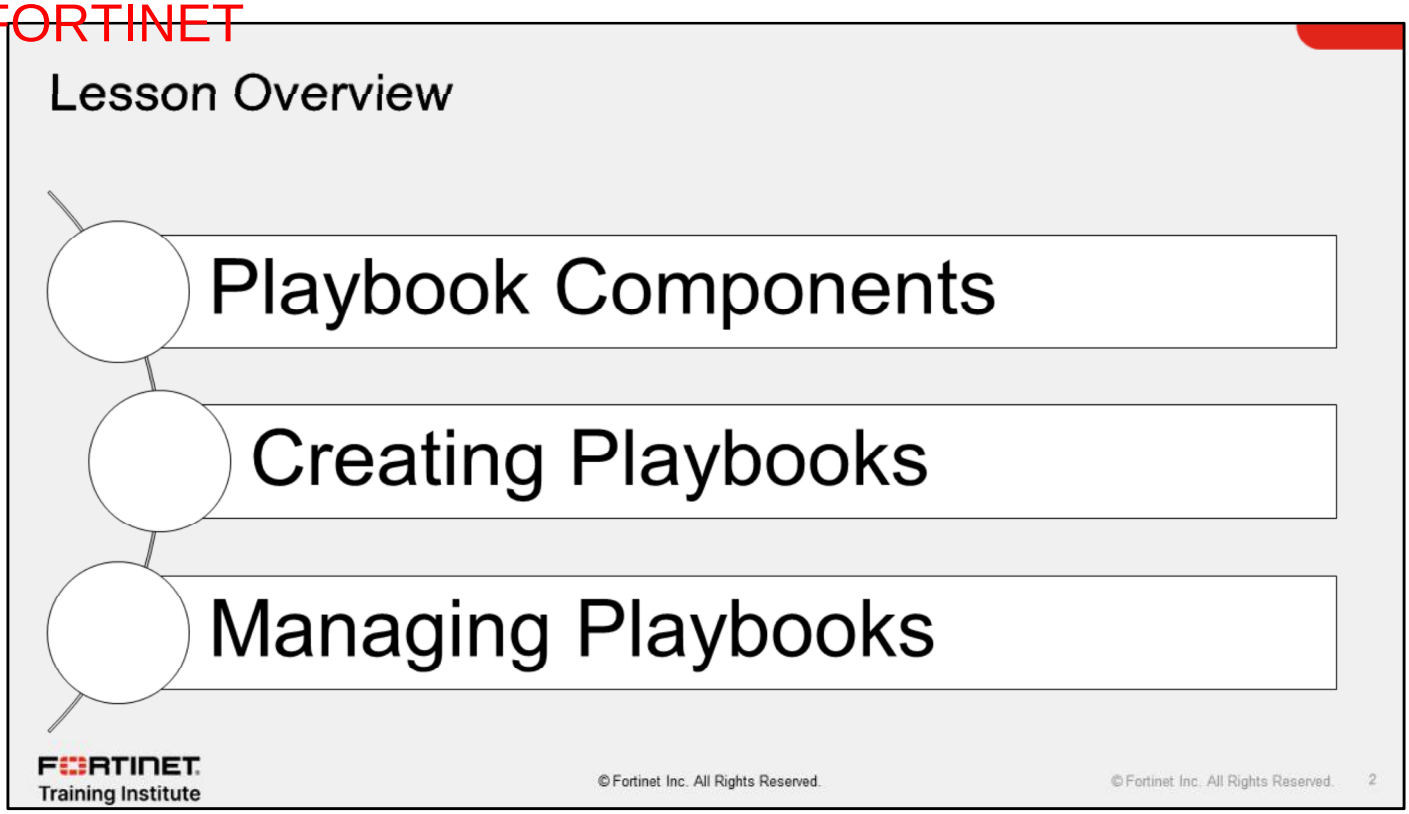


This slide shows the objectives that you covered in this lesson.

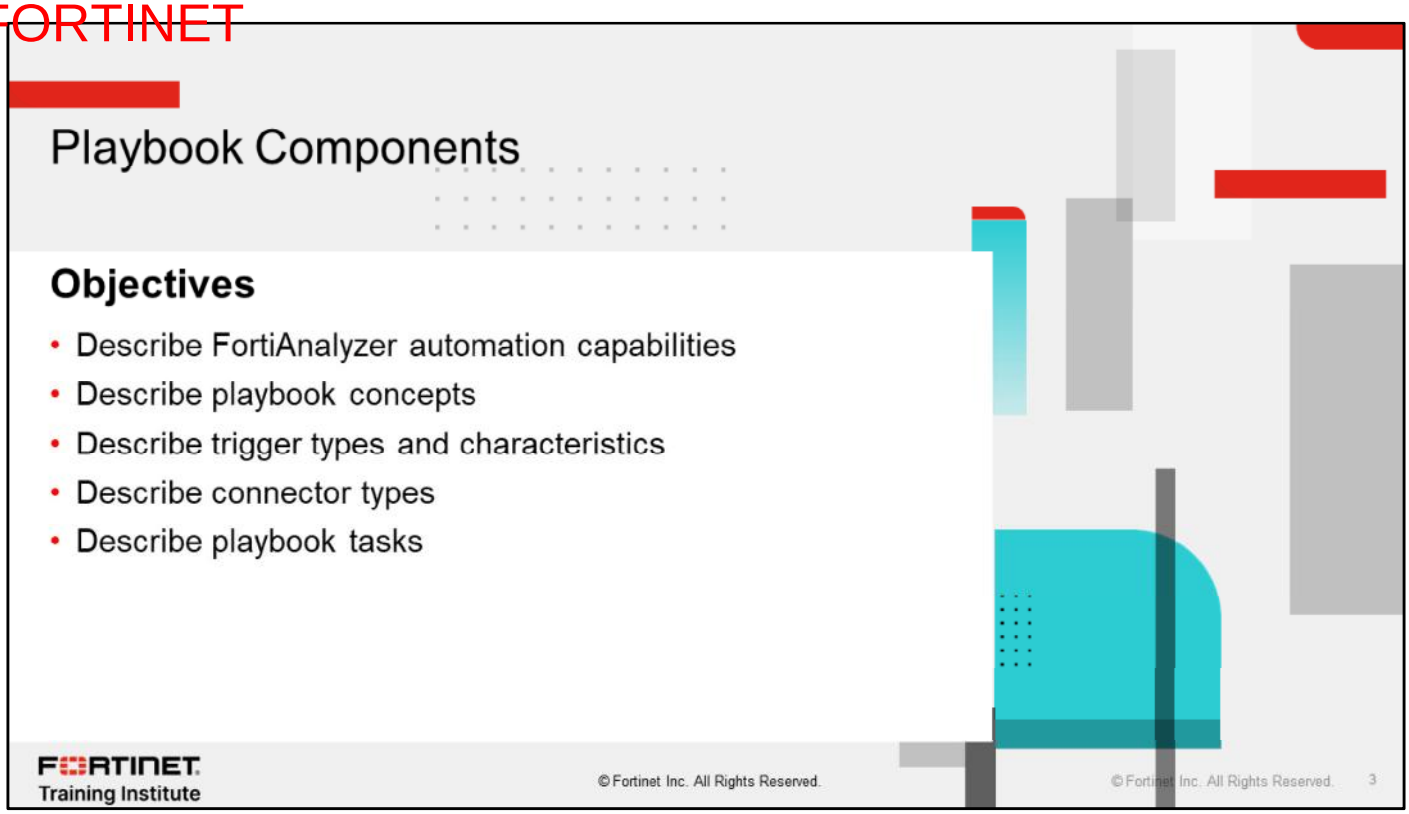
By mastering the objectives covered in this lesson, you learned how data is formatted, stored, and organized in the database, and how to use the FortiAnalyzer reporting feature to view and extract useful information from logs.



In this lesson, you will learn how to use the automation capabilities included in FortiAnalyzer.

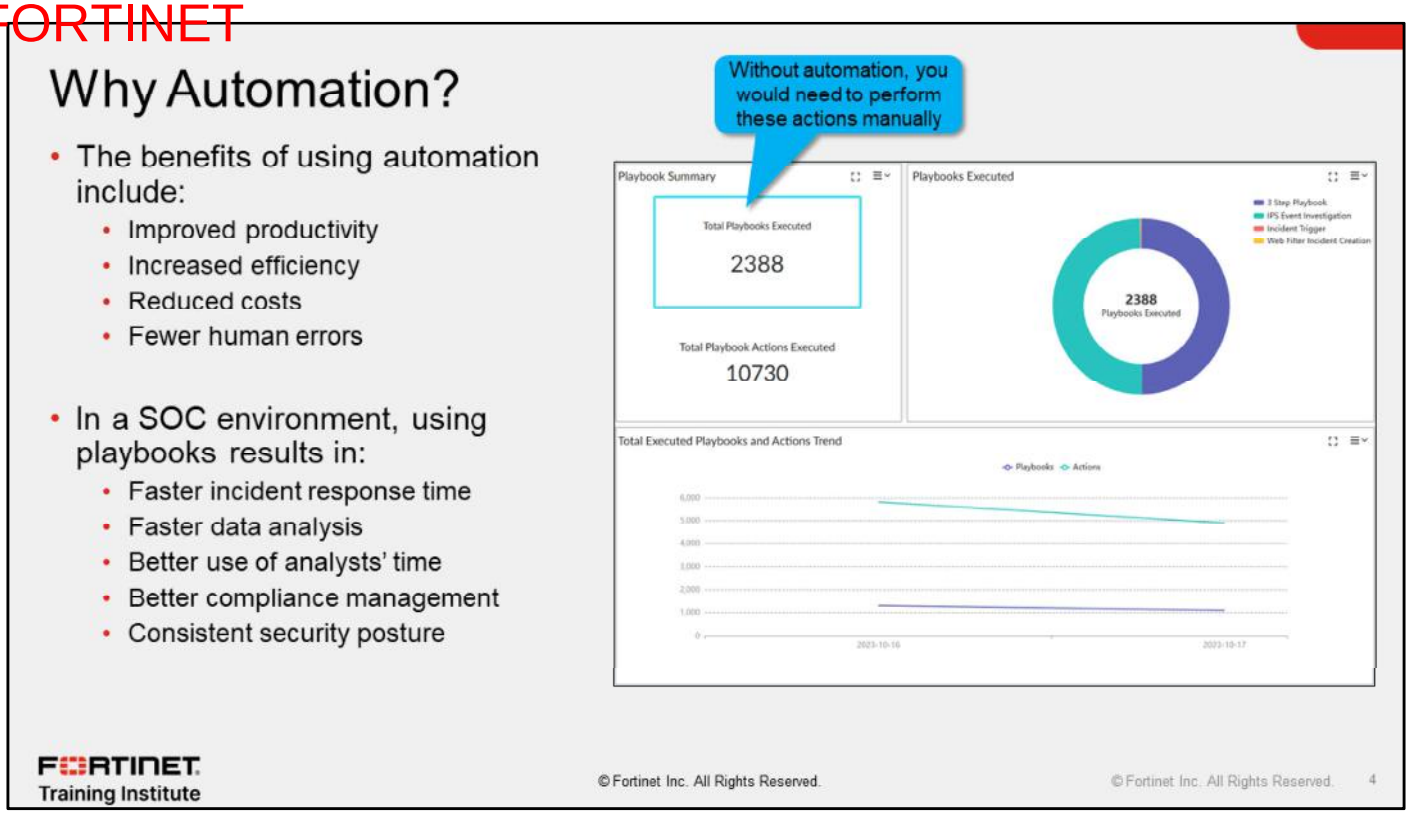


In this lesson, you will learn about the topics shown on this slide.



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.



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.

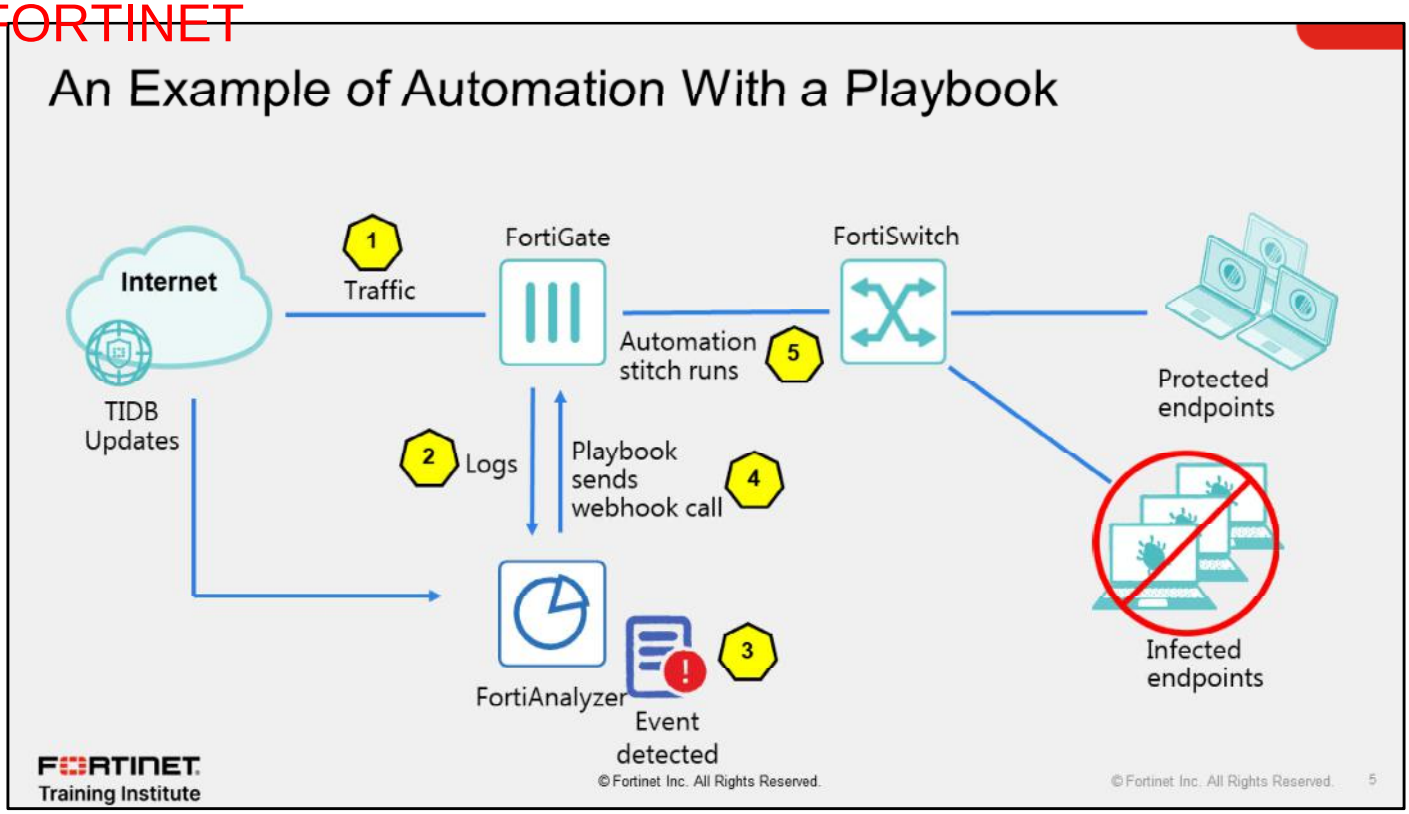
In a SOC environment, automation provides, among other results, faster response times, faster data analysis, better use of analyst time, better compliance management, and a more consistent security posture.

FortiAnalyzer allows SOC analysts to automate common and repetitive tasks with the use of playbooks.

FortiAnalyzer works with standalone devices but 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 FortiGate 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.

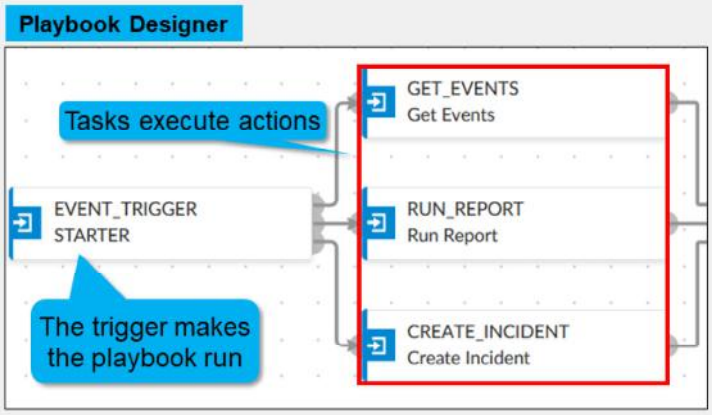


This slide shows an example of a playbook being used to automate tasks.

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

Playbook Concepts

- Playbooks allow you to automate common SOC tasks
  - They are created per ADOM
- Each playbook has only one trigger
  - It determines when a playbook executes
- Playbooks have one or more tasks
  - They are the actions that will take place
- The actions that can be performed by a task depend on the connector used
  - Different devices 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

FORTINET Training Institute

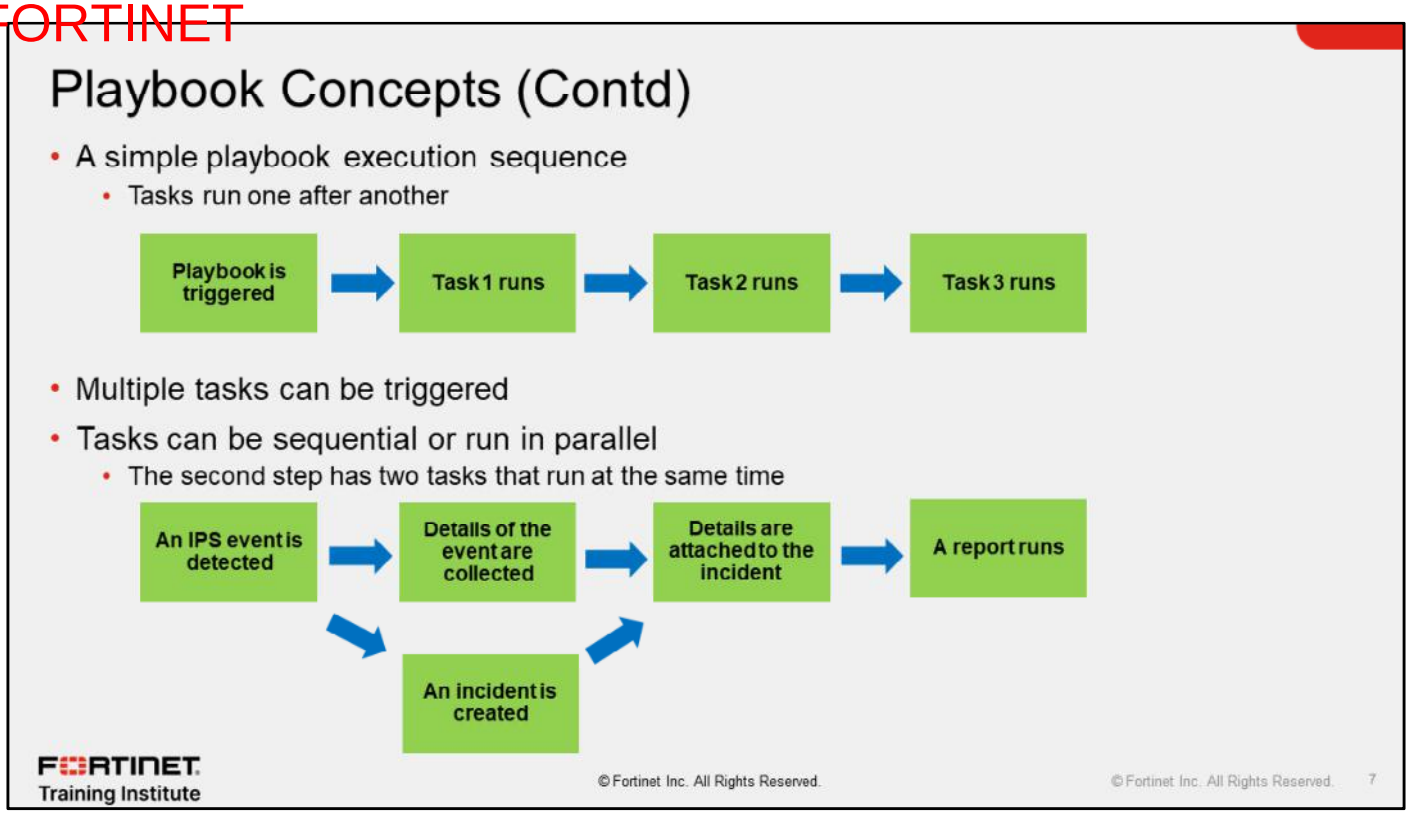
© Fortinet Inc. All Rights Reserved. 6

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.

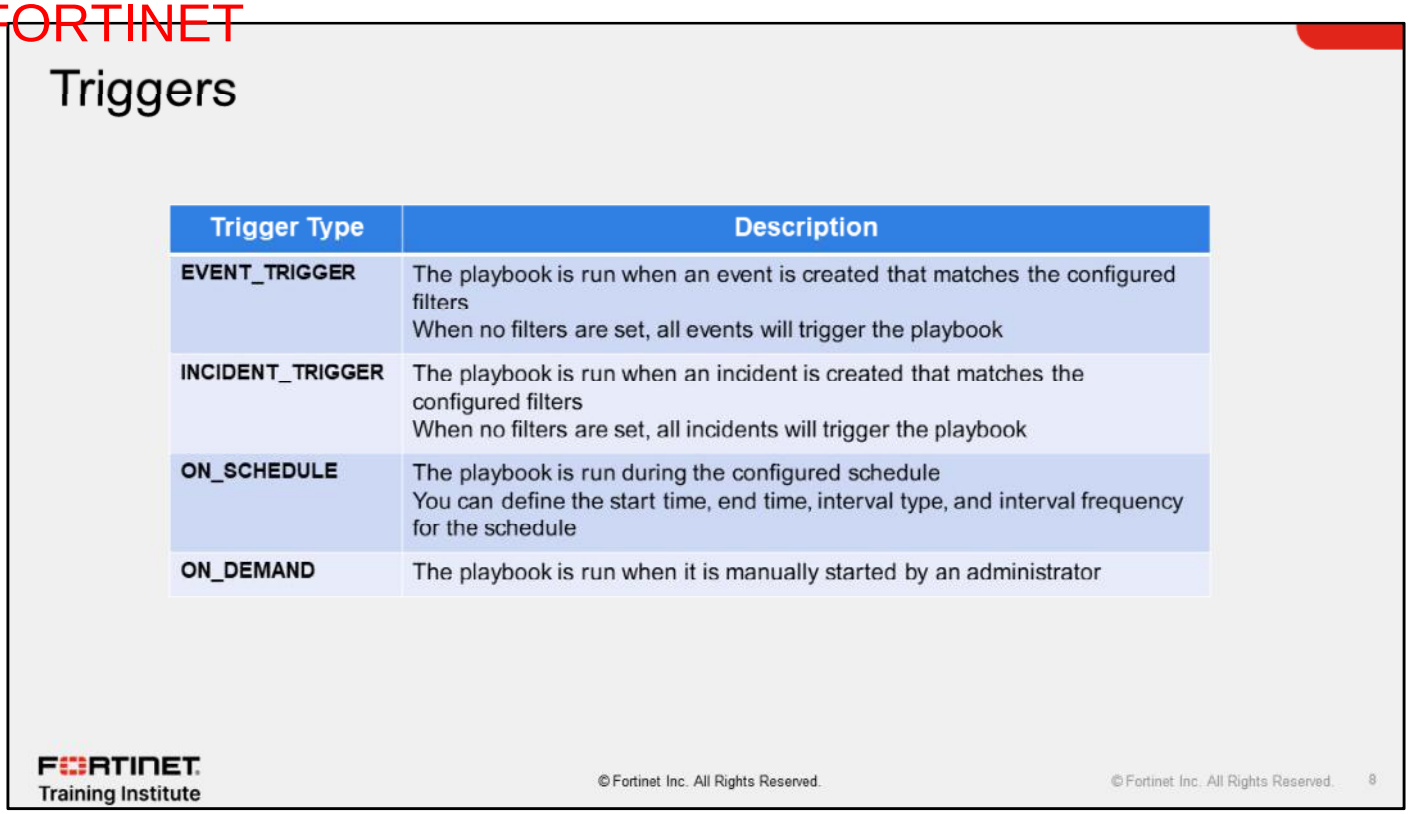
Each task includes the automated action that needs to take place. The available actions depend on the connector used. Connectors allow tasks to be performed on supported devices.

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.



In the simplest case, 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 next task can add those events to an incident.



Every playbook starts with a trigger that determines when the playbook is executed. Each playbook can include only one trigger.

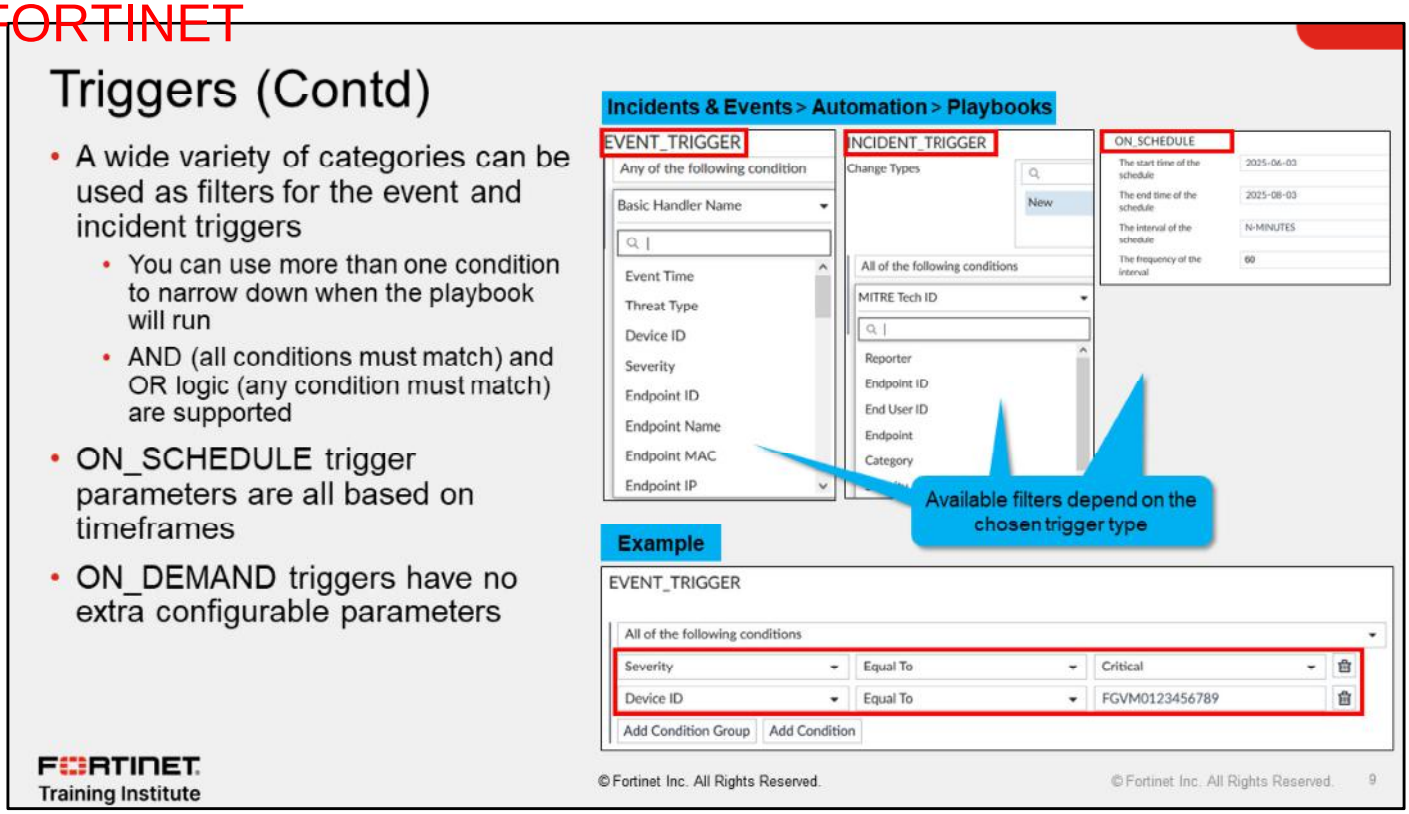
After a playbook is triggered, it flows through the configured tasks, as defined in the playbook designer.

The following four triggers are available:

- EVENT_TRIGGER: The playbook runs 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 runs 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 runs during the configured schedule. You can define the start time, the end time, the interval, and the interval frequency for the schedule.
- ON_DEMAND: The playbook runs when it is manually started by an administrator.

To run a playbook manually, go to **Playbook**, select the desired playbook, and click **Run**. Additionally, if present, you can run playbooks from the incident **Analysis** page.

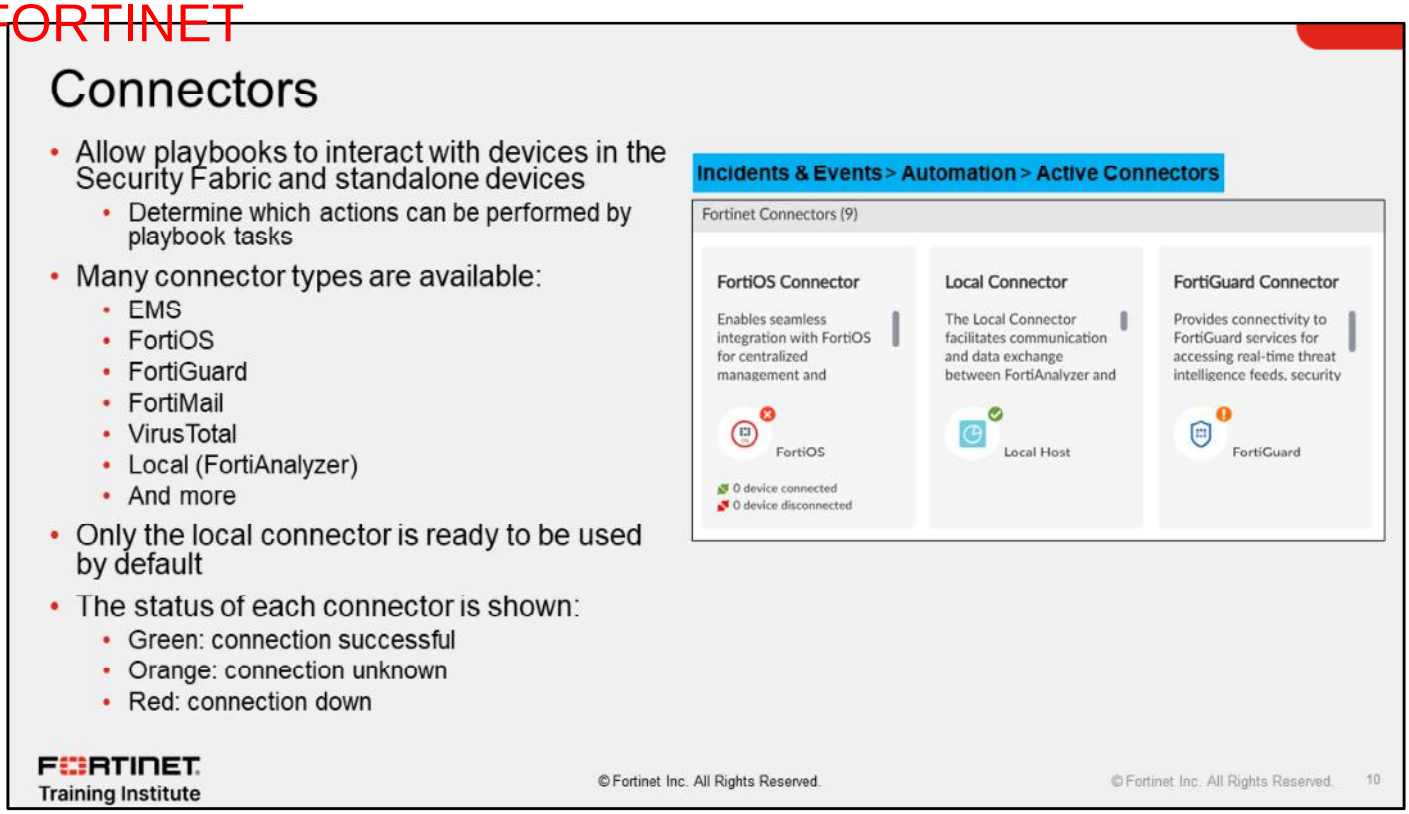
Note that playbooks with the ON_SCHEDULE trigger can also be executed manually. This allows you to test them outside of their configured time frame.



The trigger type you select determines the options you can use to specify exactly when you want the playbook to run.

For example, you can configure an event trigger to run only when FortiAnalyzer detects an event with critical severity on a specific device.

If you set more than one condition for a trigger, you can choose to either require all conditions to match, or any one condition to match.



Connectors determine which automated actions can be performed in playbooks. The available actions vary depending on the connector type used. Each type allows for different actions.

To view fabric connectors, click **Active Connectors**.

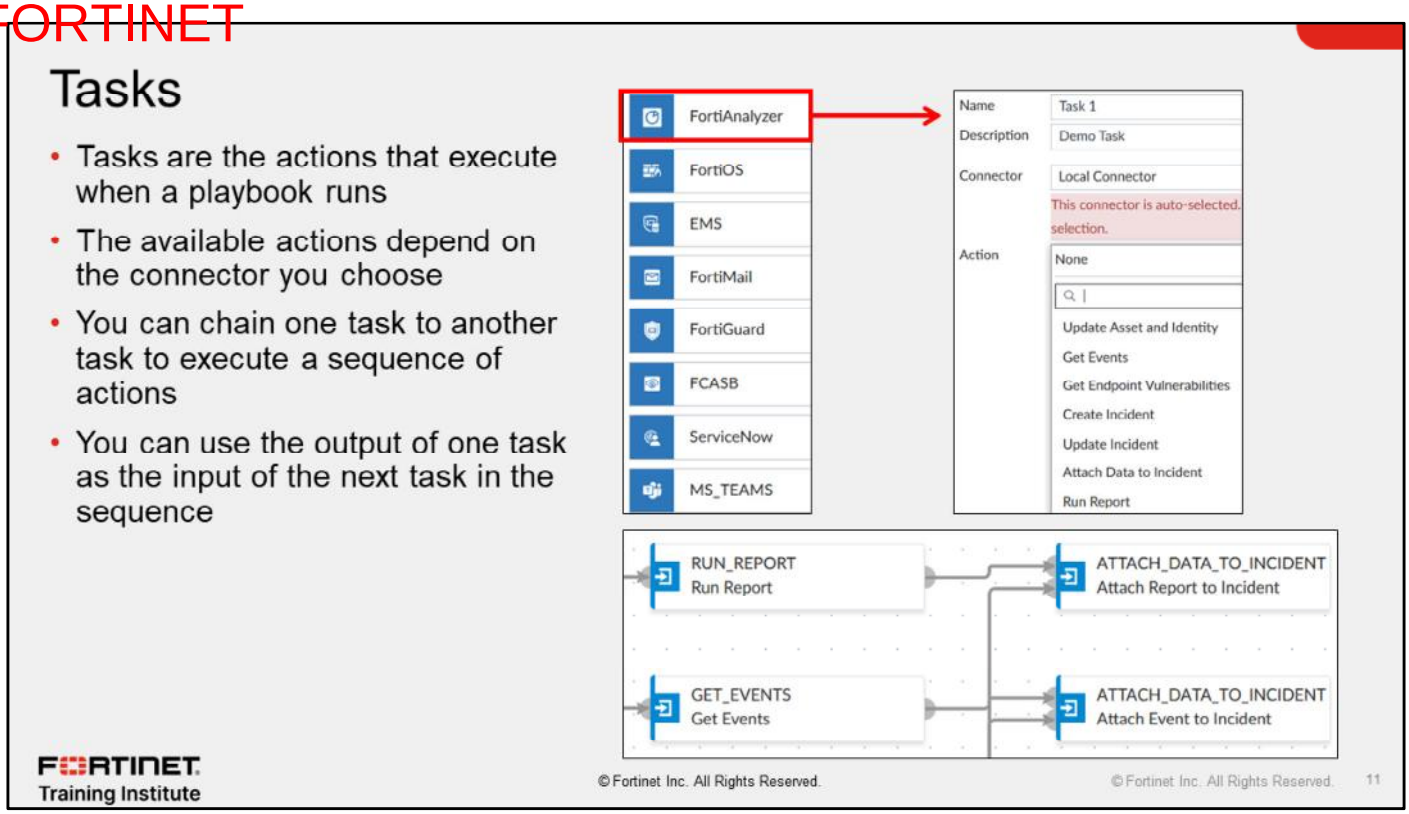
The status of connectors is indicated by a colored icon:

- Green: The API connection successful.
- Orange: The API connection is unknown.
- Red: The API connection is down.

You can see when the status was last updated by hovering your mouse over the status icon. Click the refresh icon to get an updated status.

By default, the local connector, which is for the local FortiAnalyzer, is ready to be used. Other connector types require extra configuration.

For example, the FortiOS connector will be listed as soon as the first FortiGate device is added to FortiAnalyzer. However, to see the actions related to that FortiOS connector, you must enable an automation rule using the Incoming Webhook Call trigger on FortiGate.



Tasks are the actions that take place after a playbook starts running. Each starter can trigger the execution of one or more tasks, and each task can perform one action.

Tasks can also be chained so that the output of one task becomes the input of the next task. For example, a task can be created to collect some data, and then provide that data to the next task, where it can then be added to a report.

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

You can configure tasks that use default input values or that take inputs from the trigger or from the preceding tasks.

You must configure automation rules on FortiGate before you can see the list of available actions on FortiOS connectors.

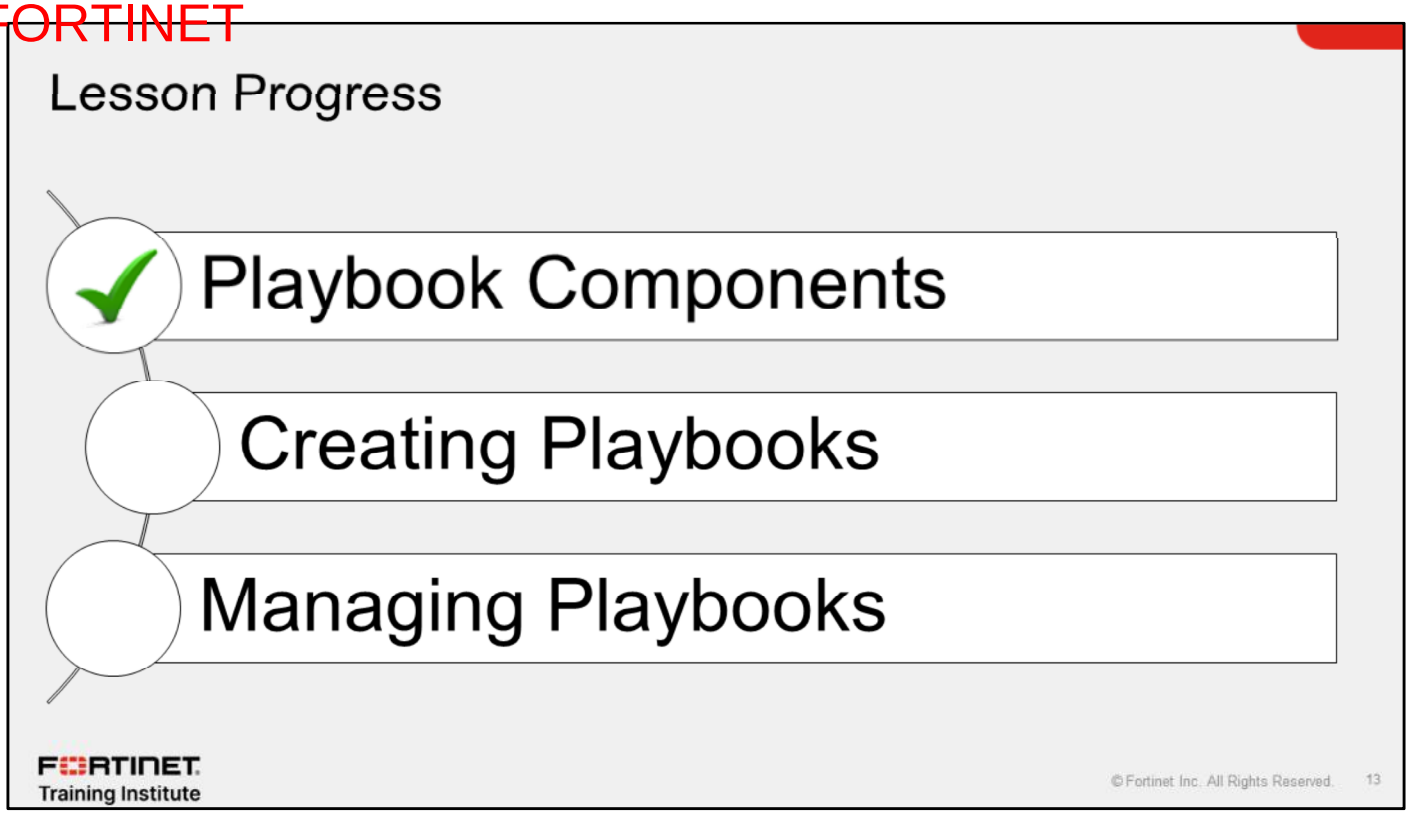
Knowledge Check

1. What determines which actions are available in a playbook task?
   - ✓A. The type of connector used
   - B. The type of trigger used

2. Which type of connector is enabled by default?
   - ✓A. Local host
   - B. FortiOS

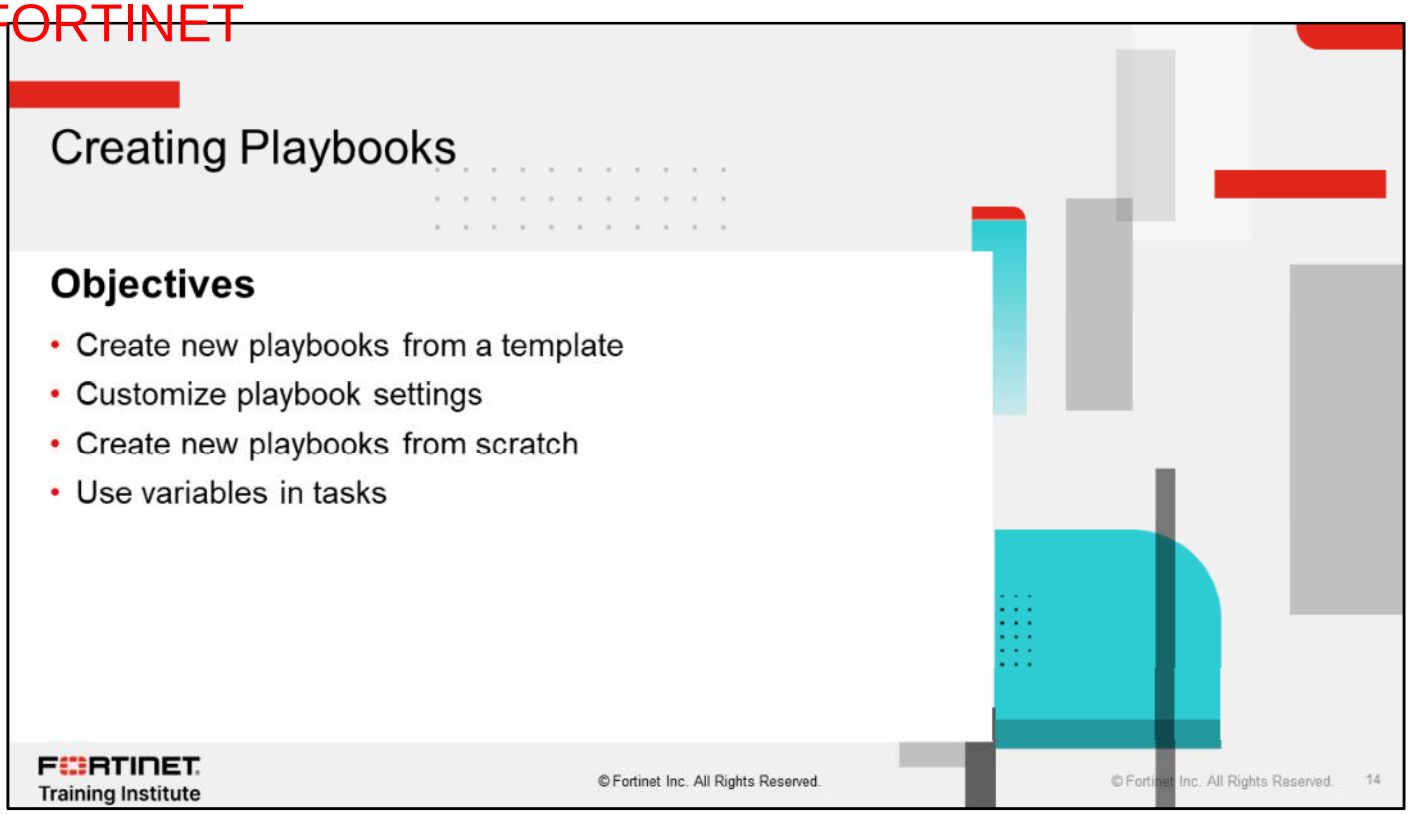
FORTINET Training Institute

© Fortinet Inc. All Rights Reserved. 12



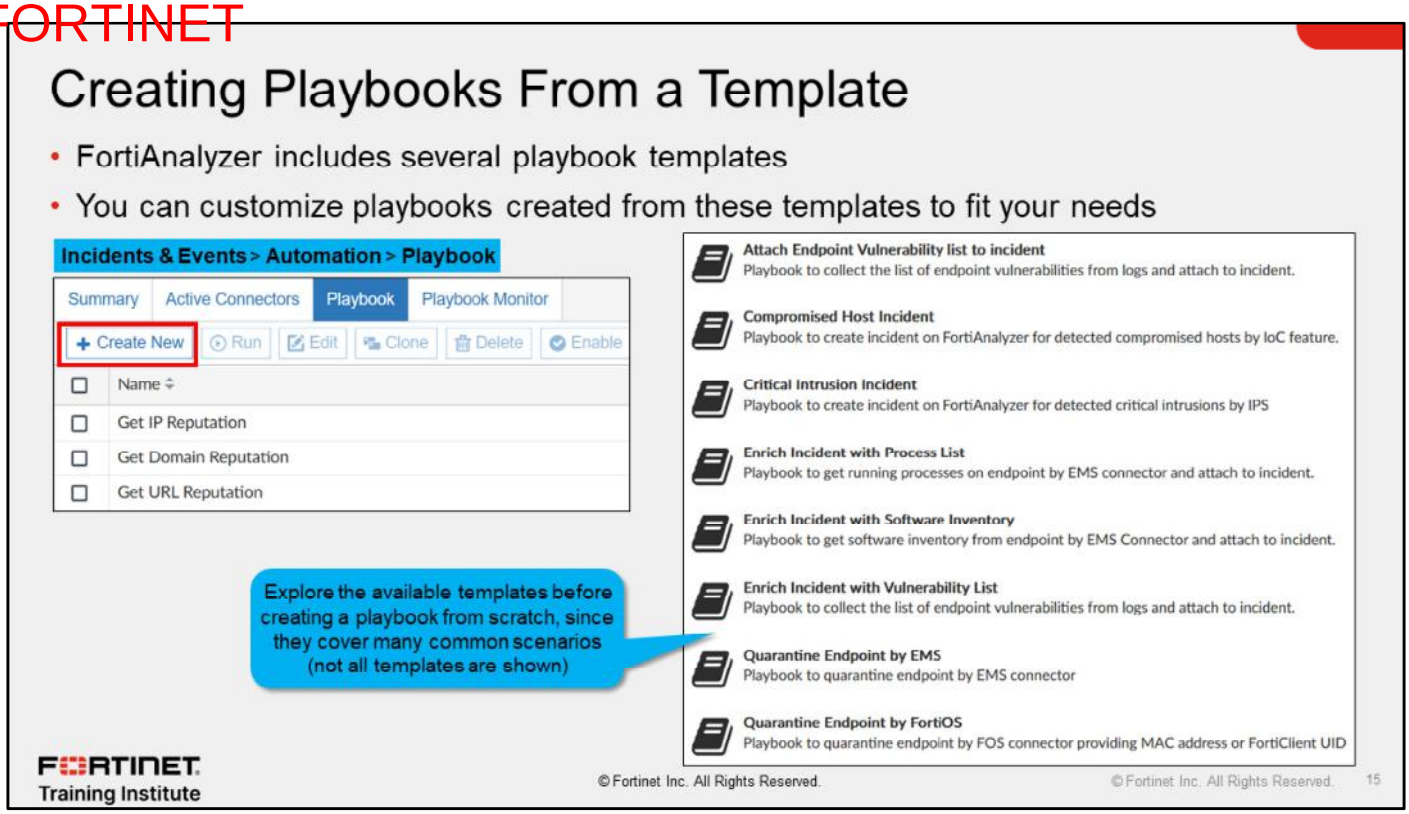
Good job! You now understand playbook components.

Now, you will learn how to create playbooks and use them to automate tasks.



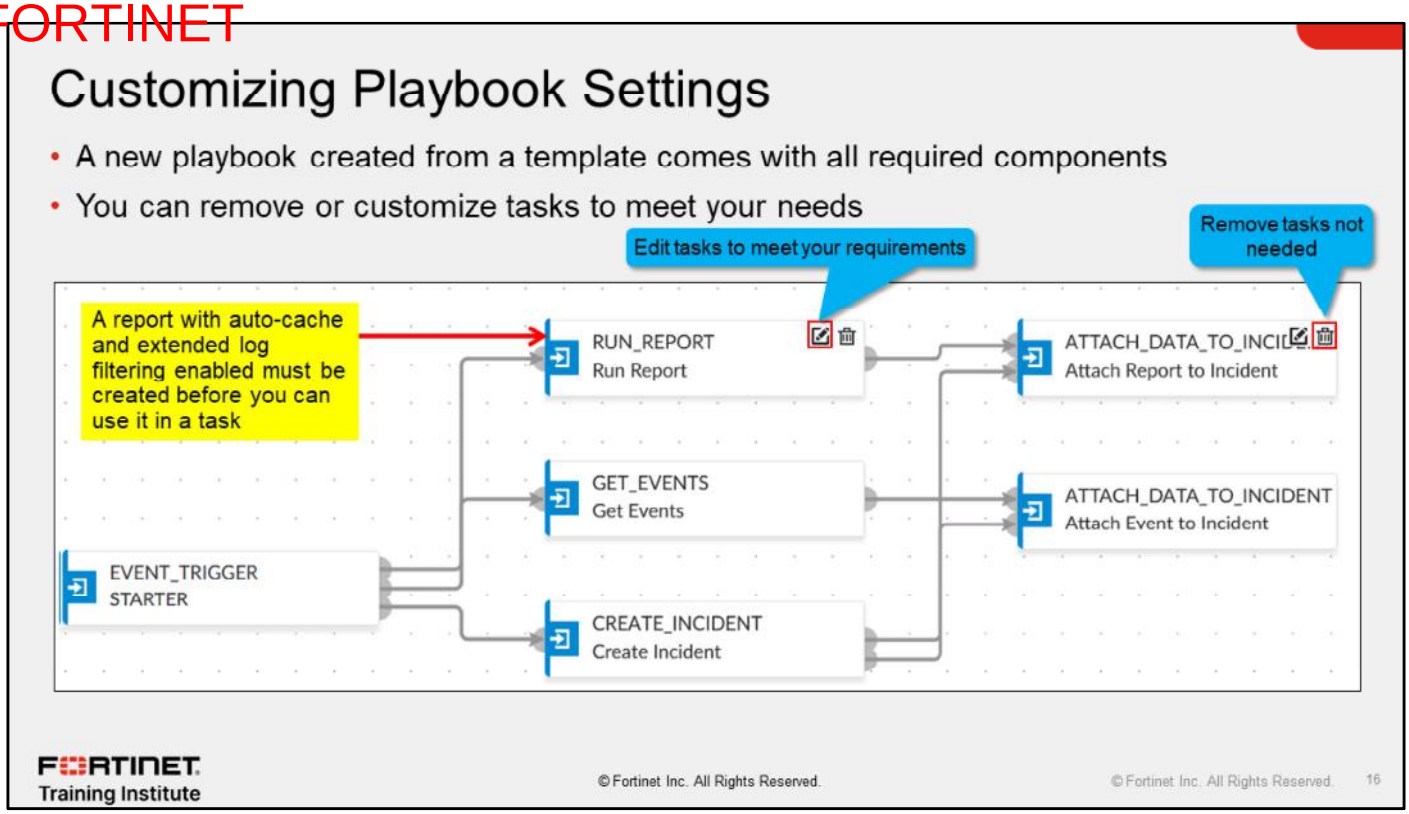
After completing this section, you should be able to achieve the objectives shown on this slide.

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



FortiAnalyzer includes several playbook templates that SOC analysts can customize. The templates included allow you 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) server IP addresses.
- Quarantine and run antivirus scans on endpoints.



When you select a playbook template, the playbook designer is displayed and automatically populated with a trigger and one or more tasks. The trigger type and the tasks included depend 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:

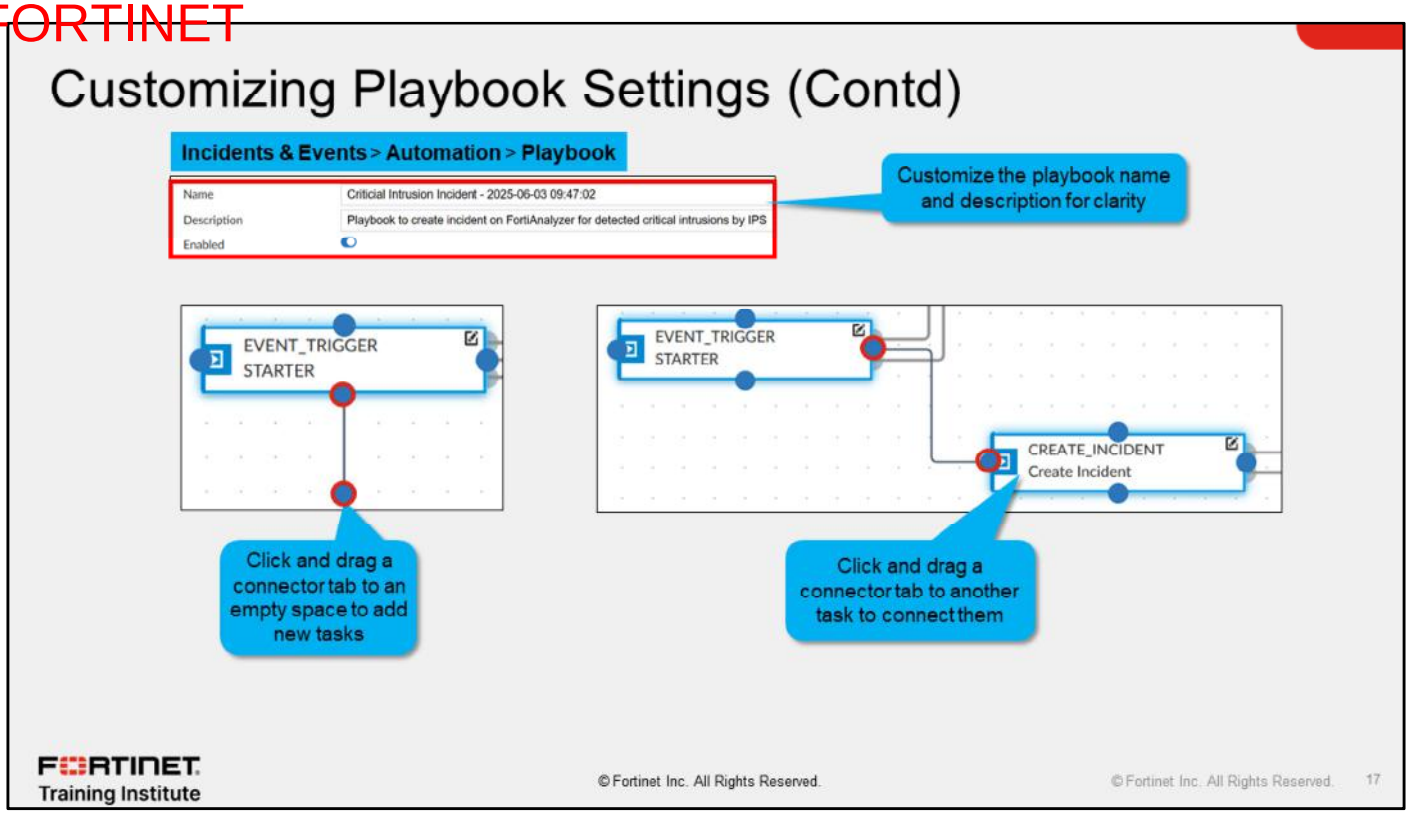
- Run when the specified event or events are generated.
- Create a new incident.
- Get the list of events specified in the task filter and add them to the incident.
- Run a report and attach it to the incident.

Running the playbook will result in the incident including relevant information that the analyst in charge can use during an incident investigation.

Note that to run a report as a task, it must already exist and have both auto-cache and extended log filtering enabled.

To edit any of the tasks, click the pencil icon in the upper-right corner. Remember to save the changes.

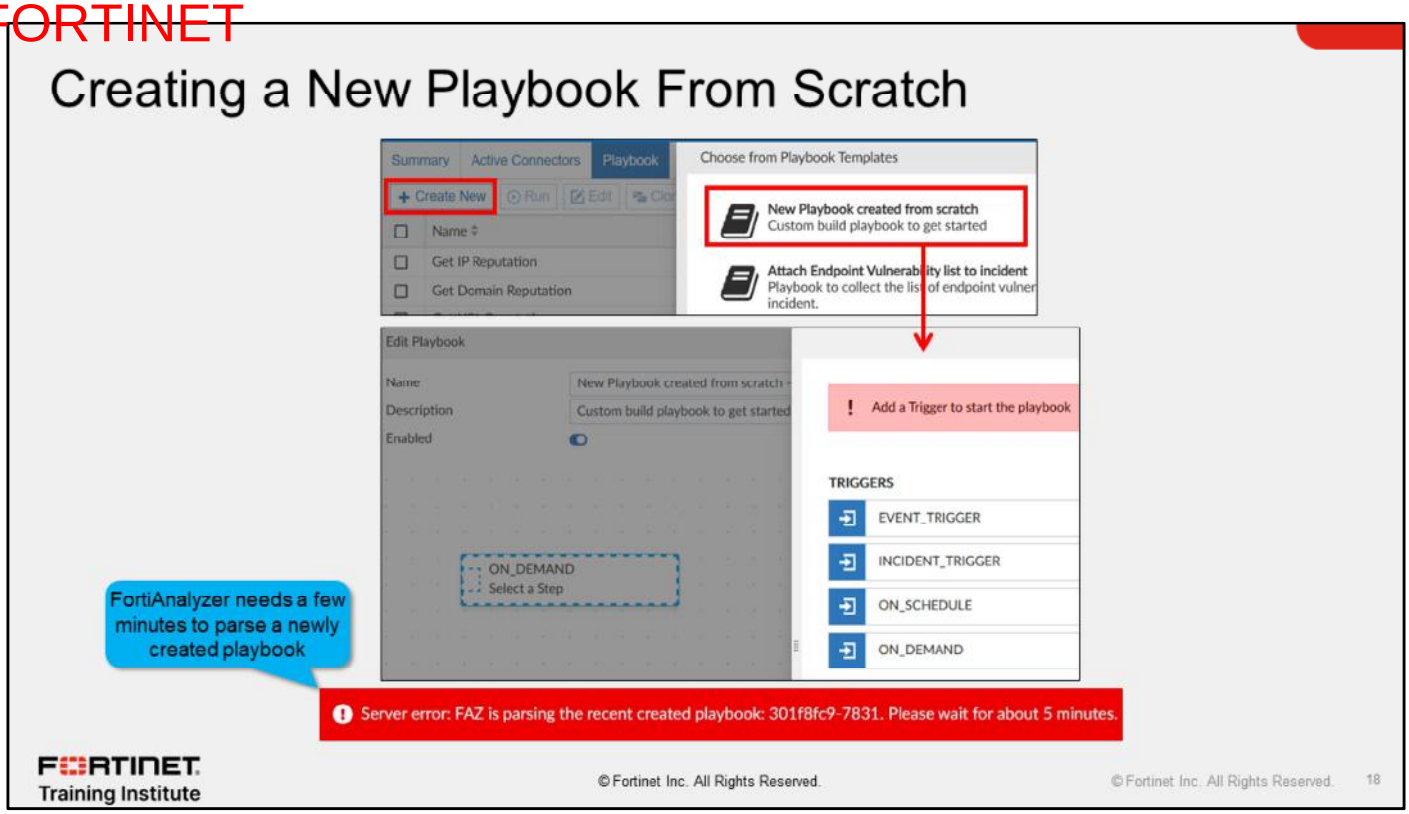
To remove a task, click the trash can icon in the upper-right corner.



By default, every new playbook created from a template comes with the same generic name, plus the date it was created, appended to the end. This can make them difficult to distinguish, so Fortinet recommends 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. An empty task will be displayed, and you will need to edit its settings.

To connect tasks to each other or to the trigger, click and drag a connector tab onto another connector tab.



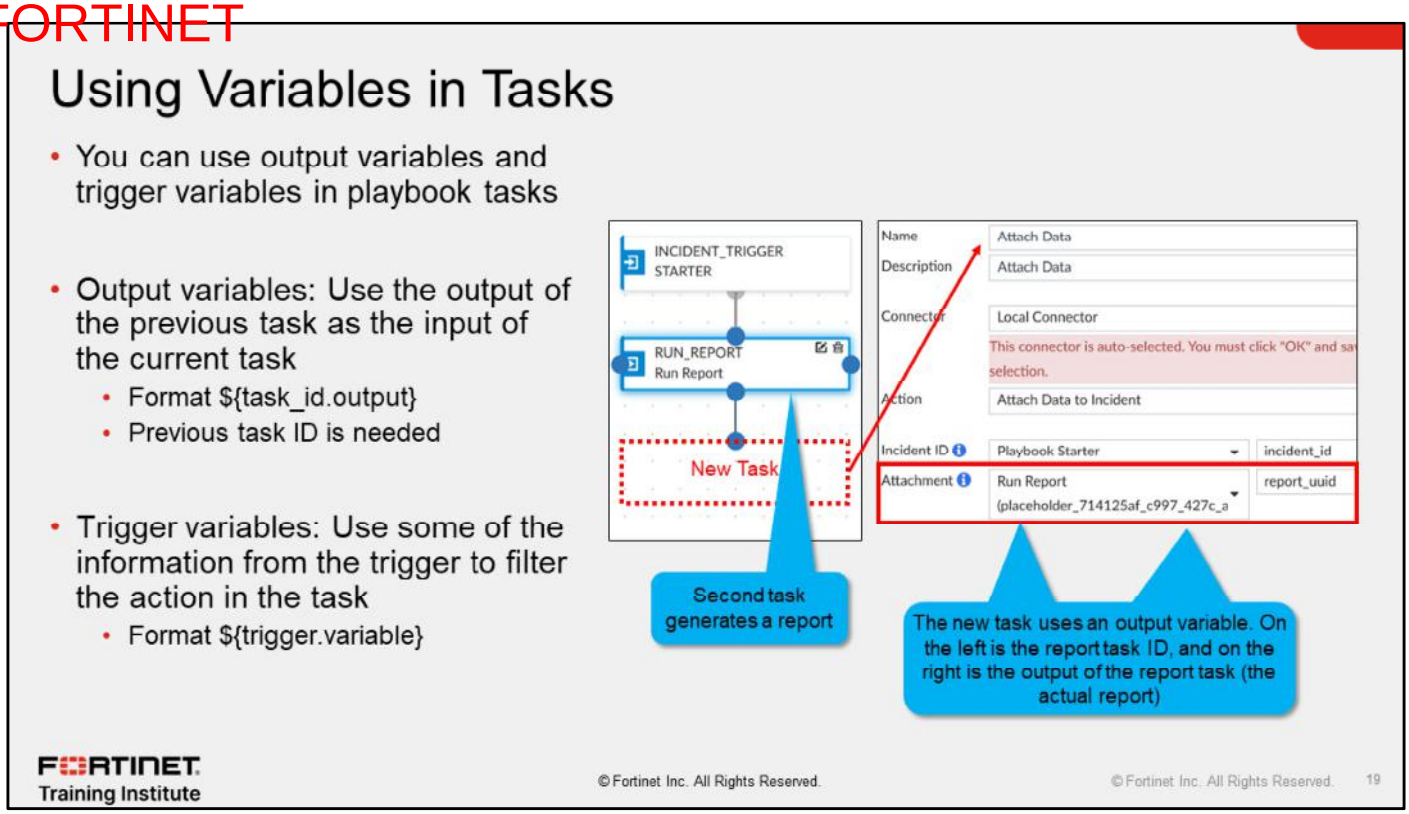
If none of the templates meets your needs, you can always create a playbook from scratch. To do so, click **Playbook** > **Create New**, and then select the first option in the list. The playbook designer will open.

First, you must select a trigger. Remember that, depending on the trigger type you choose, you have the option to add filters to make the playbook run only if the specified criteria is matched.

Then, you must add the task or tasks that you want to be executed by dragging and dropping the connector tabs.

When editing tasks, keep in mind that the actions can also include filters that will reduce the processing of unneeded data. For example, a task set to **Get Events** can use a filter to include only events generated by a specific event handler, or only events with a specific severity.

Also, keep in mind that after you create a new playbook, FortiAnalyzer will need a few minutes to parse it. For example, if you try to run a newly created playbook configured with an ON_DEMAND trigger before it is parsed, you will see an error, like the one shown on the slide, telling you why the playbook failed to run.



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

Output variables allow you to use the output from a preceding task as input to the current task.

An output variable consists of the task ID, followed by the task output, as shown on this slide.

On the slide, the new task being created will use the report generated by the previous task to add it to an incident.

Trigger variables allow you to use information from the trigger of a playbook when it has been configured with an incident or event trigger. For example, a single playbook can be triggered by more than one device. A **Run Report** action can include a filter for the endpoint IP address from the event that triggered the playbook.

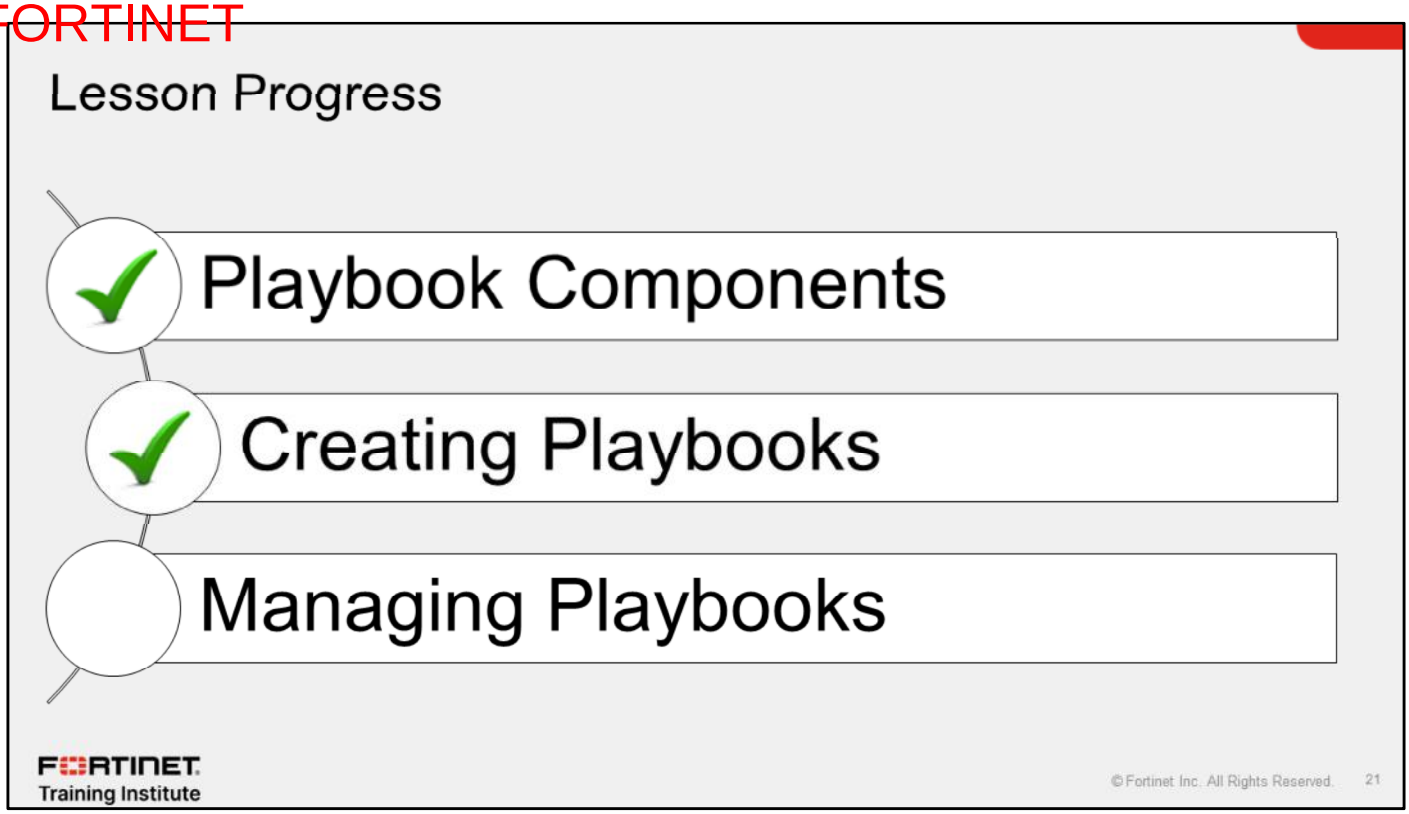
Knowledge Check

1. What is the purpose of an output variable?
   A. To use the input of one task as the output of another task
   ✓B. To use the output of one task as the input of another task

2. What is the first thing that you need to configure when creating a playbook from scratch?
   A. The connector type that will be used
   ✓B. The trigger type that will be used

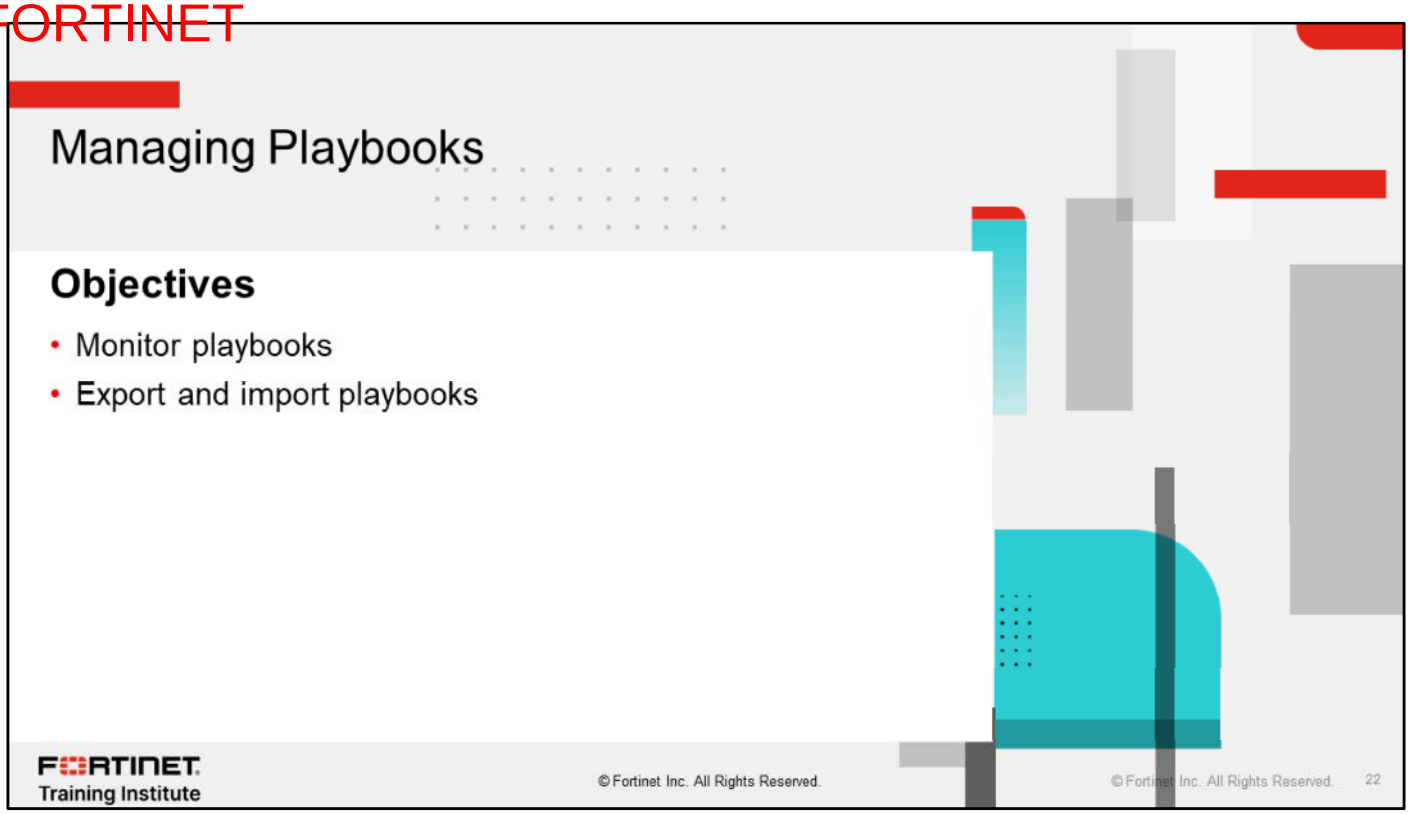
FORTINET Training Institute

© Fortinet Inc. All Rights Reserved. 20



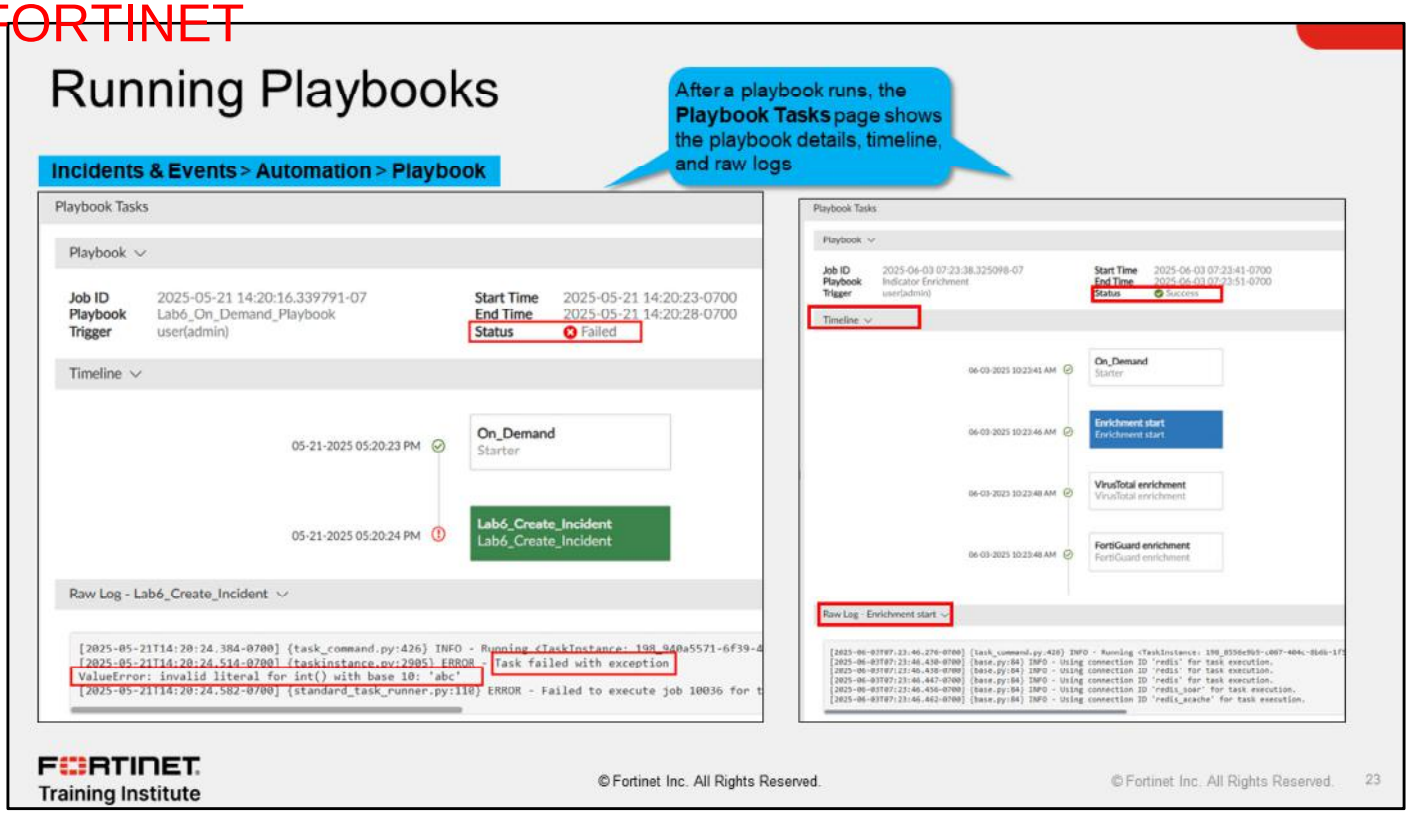
Good job! You now know how to create playbooks and use them to automate tasks.

Now, you will learn how to manage playbooks.



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

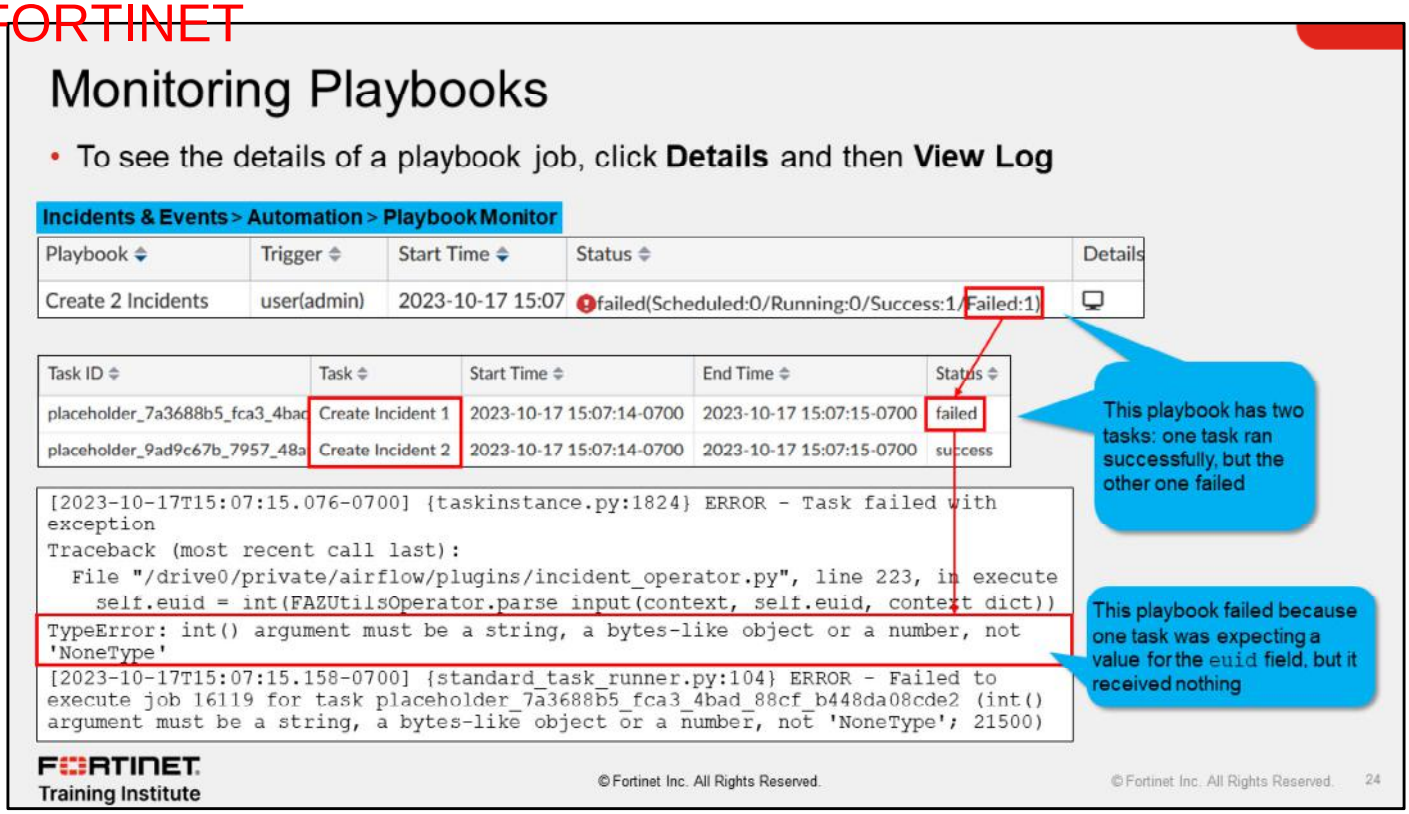
By demonstrating competence in monitoring playbooks, you will be able to identify whether all automated tasks ran successfully. You will also be able to export playbooks to another ADOM or device.



After you run a playbook, the **Playbook Tasks** page opens showing details such as the job ID, the playbook start and end times, and the status of the playbook.

You also see the playbook timeline and the raw logs of the playbook as it was running.

This slide shows two examples of a playbook after it was run: once when it failed and once when it was successful.



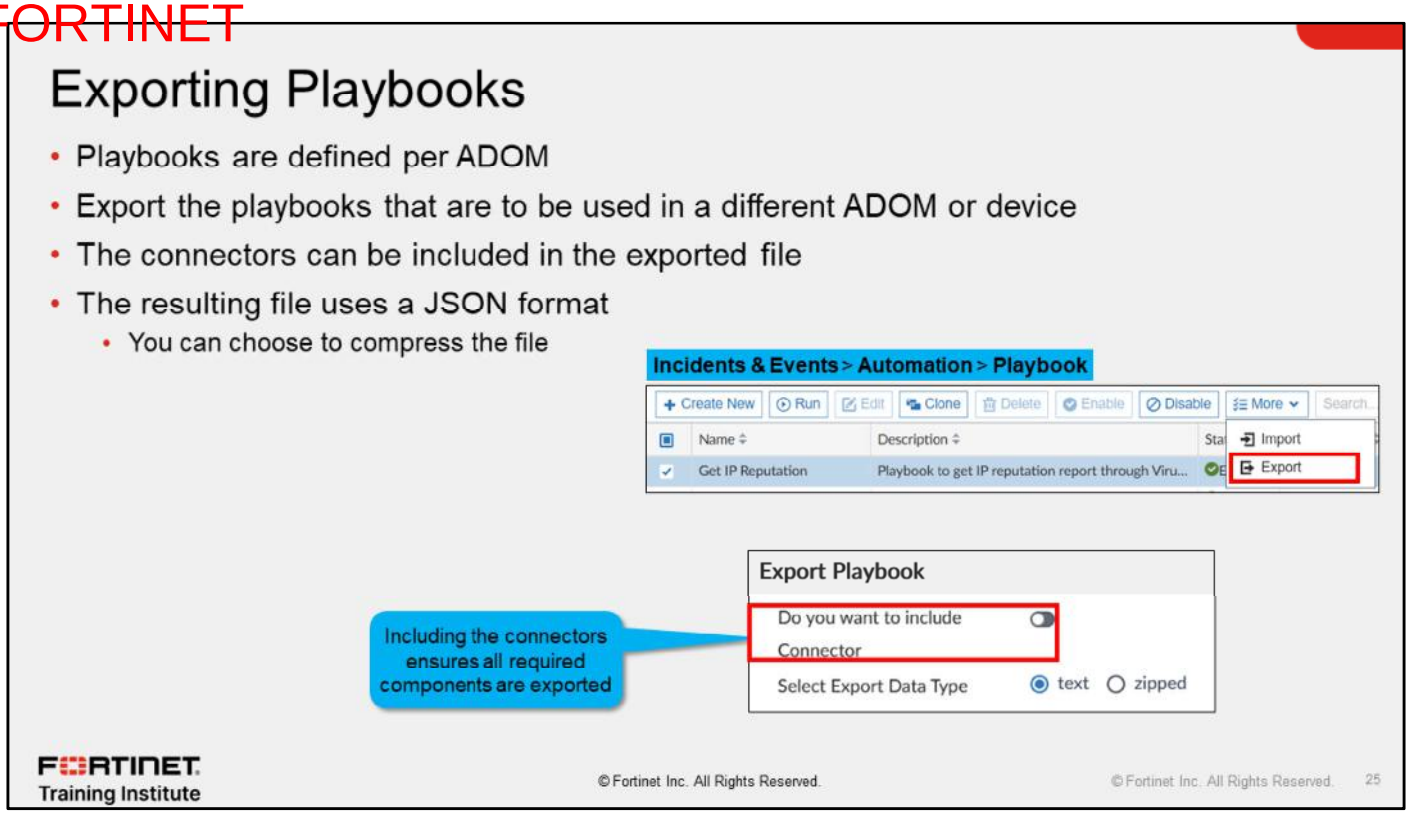
When troubleshooting playbooks, it is very useful to review their logs. Details about the execution of a playbook job are available in the associated log.

The status of a playbook can be one of the following:
- Running
- Success
- Failed

To see detailed logs, go to **Playbook Monitor**, select the desired entry, click the **Details** icon, and then click **View Log**.

Playbook jobs that include one or more failed tasks are labeled as **Failed** in **Playbook Monitor**. However, a failed status does not mean that all tasks failed. Some individual actions may have completed successfully.

In the example shown on the slide, the playbook has two tasks configured and only the task, named `Create Incident 1`, failed to run. Therefore, the playbook job is considered to have failed. The specific reason for the failure in the example is that the end user ID field expects a value; however, none was provided.



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

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

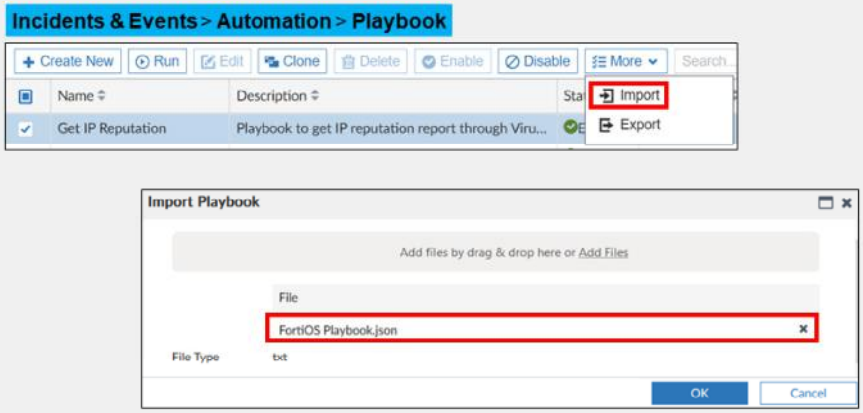
Configure the settings to export the selected playbook:

- **Do you want to include Connector**: When this setting is enabled, connectors required to run this playbook will be included in the exported file. This is recommended, for example, if a non-default connector like the EMS connector is configured, so that all required components are included in the resulting file.
- **Select Export Data Type**: Select the export file type as either plain text JSON or zipped/base 64 encoded JSON.

If you must be able to read the contents of the JSON file in plain text, you must choose the text version during the export process.

Importing Playbooks

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



FORTINET Training Institute

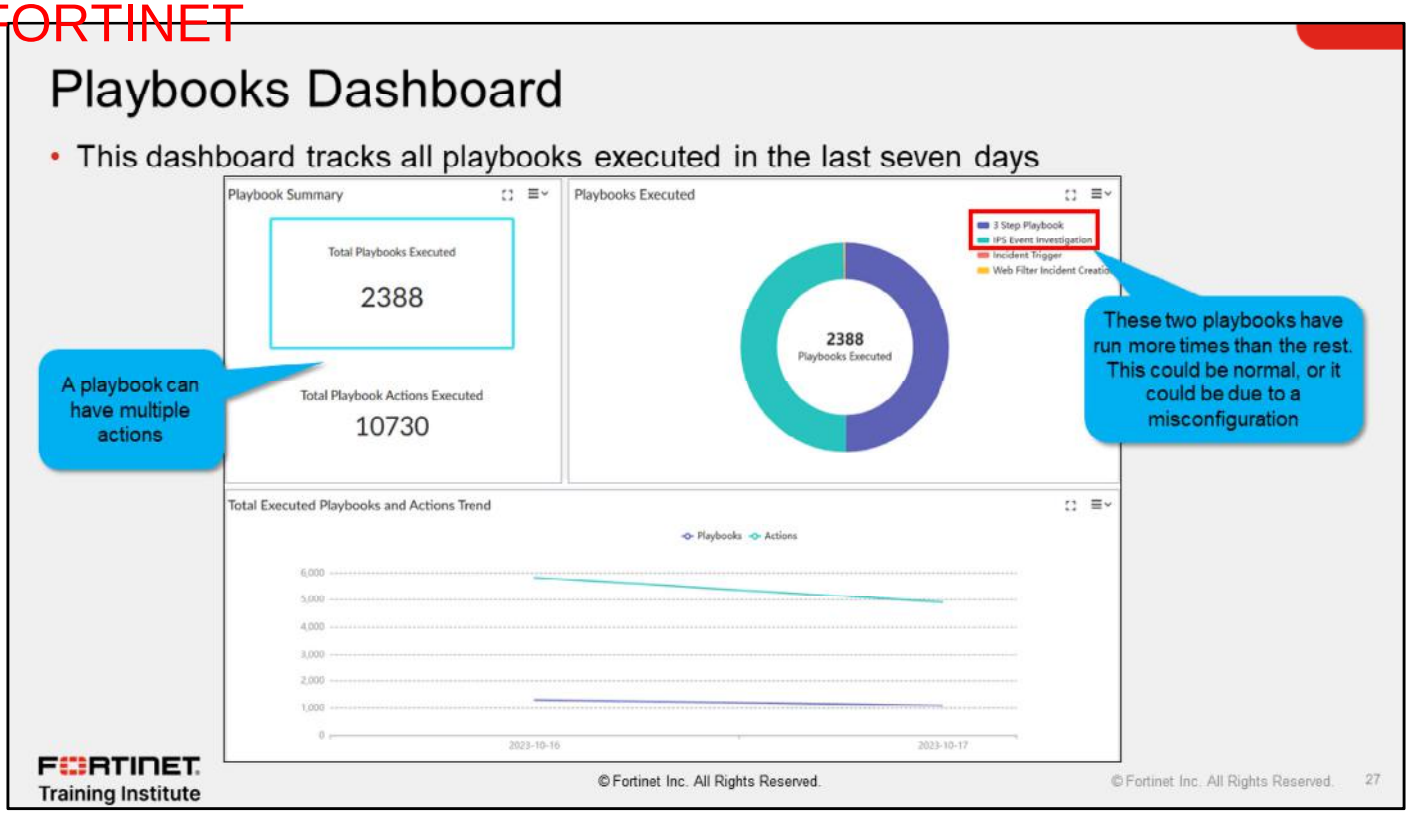
© Fortinet Inc. All Rights Reserved. 26

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

The **Import Playbook** window opens. Browse to select the playbook file that you want to import.

If the imported playbook has the same name as an existing playbook, to avoid conflicts, FortiAnalyzer will create a new name that includes a timestamp.

Playbooks are imported with the same status they had (enabled or disabled) when they were exported. Playbooks set to run automatically should be exported while they are disabled, to prevent the playbook from unintentionally running on the destination.



The **Playbooks** dashboard includes information organized and presented in these categories: **Total Playbooks Executed**, **Total Playbook Actions Executed**, **Playbooks Executed**, and **Total Executed Playbooks and Actions Trend**.

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 executed playbooks. It is the responsibility of the SOC analyst to ensure playbooks are correctly configured so they run only when required.

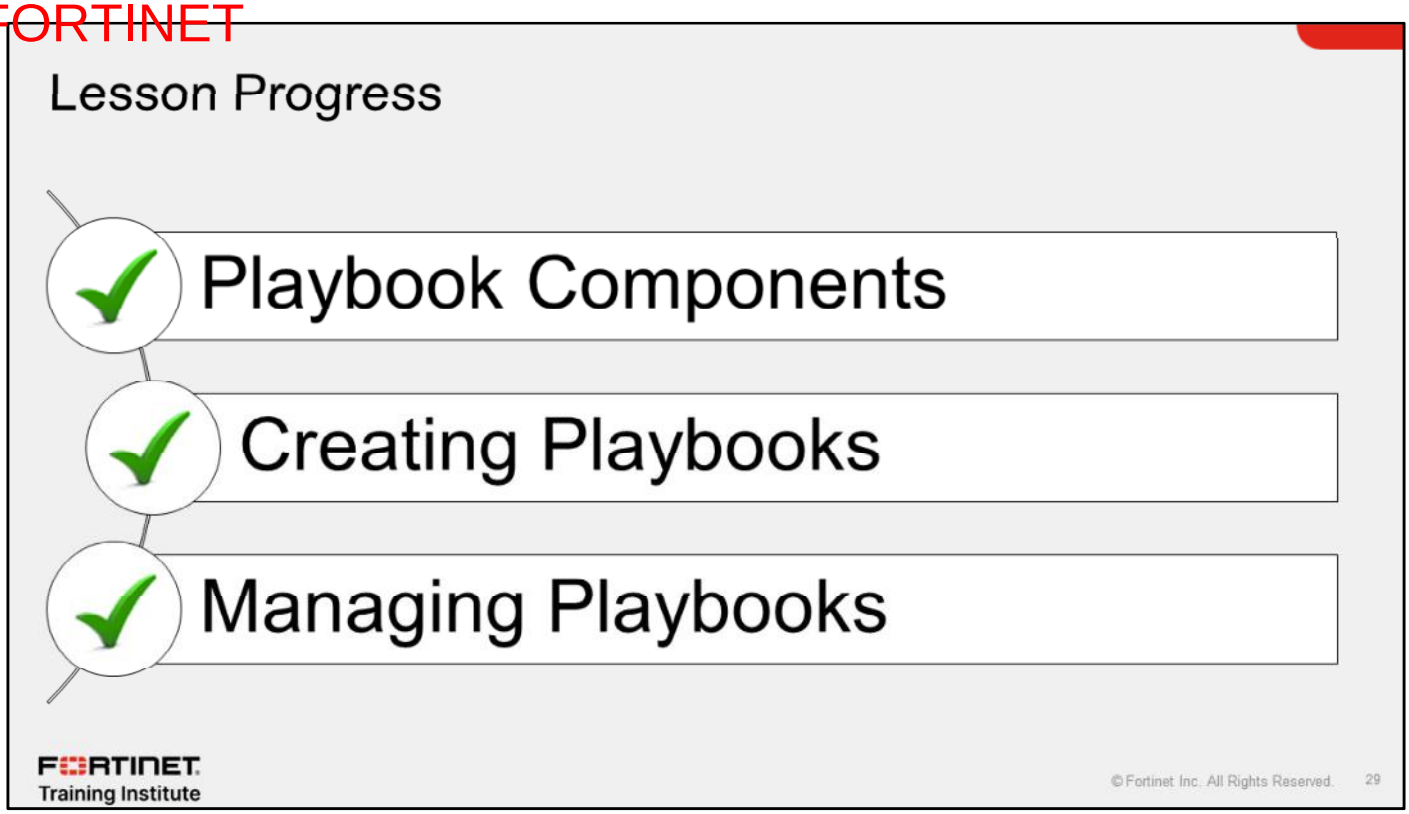
Knowledge Check

1. When is the execution of a playbook with three tasks considered to have failed?
   - A. When all three tasks fail
   - ✓B. When any of the three tasks fail

2. At what level are playbooks created?
   - ✓A. Per ADOM
   - B. Per device

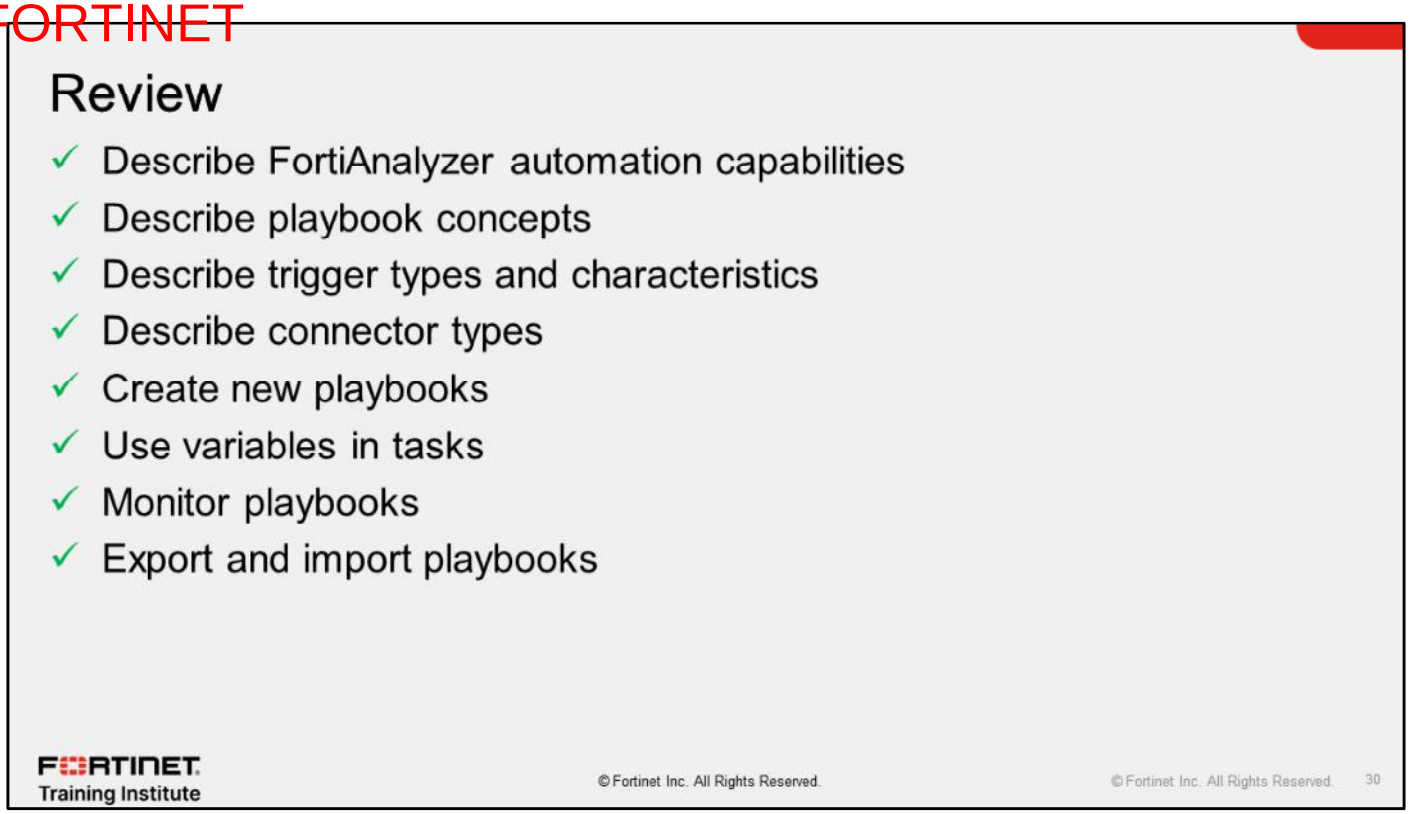
FORTINET Training Institute

© Fortinet Inc. All Rights Reserved. 28



Congratulations! You have completed this lesson.

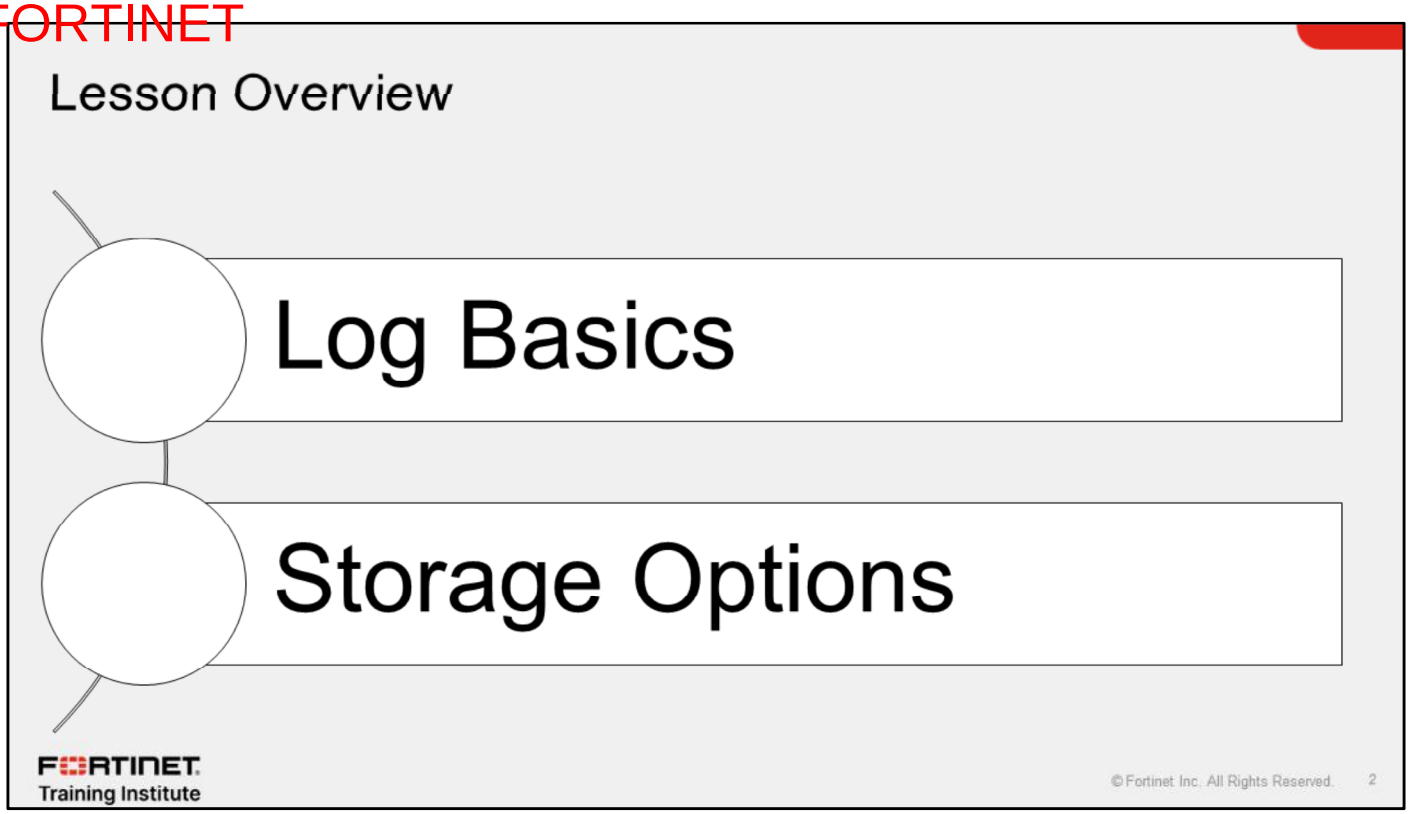
Now, you will review the objectives that you covered in this lesson.



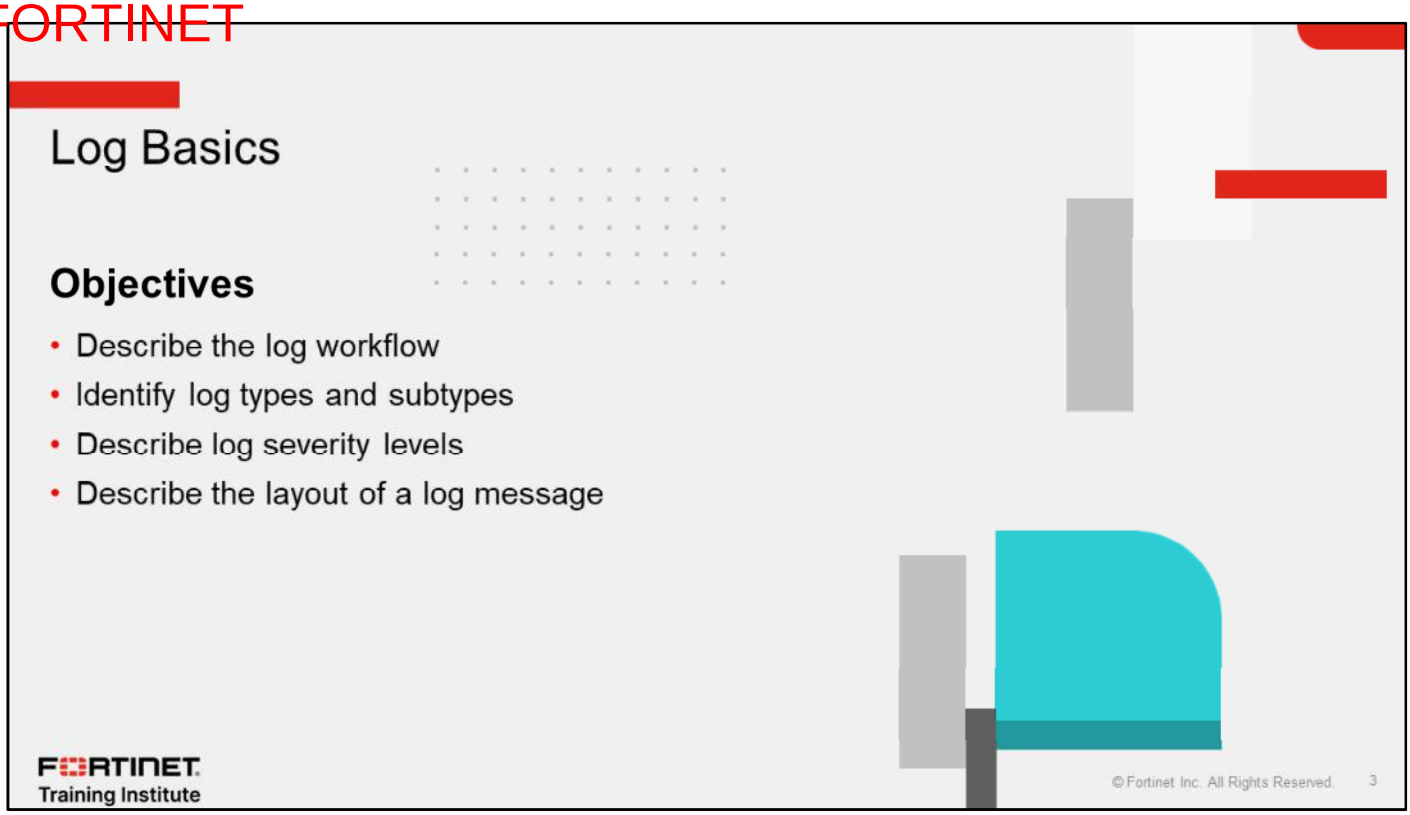
This slide shows the objectives that you covered in this lesson.

By mastering the objectives covered in this lesson, you learned what playbooks are and how you to create them to automate tasks in FortiAnalyzer. You also learned how to monitor and manage playbooks.

This supplemental material provides an overview of the log workflow and how logging works on FortiGate.

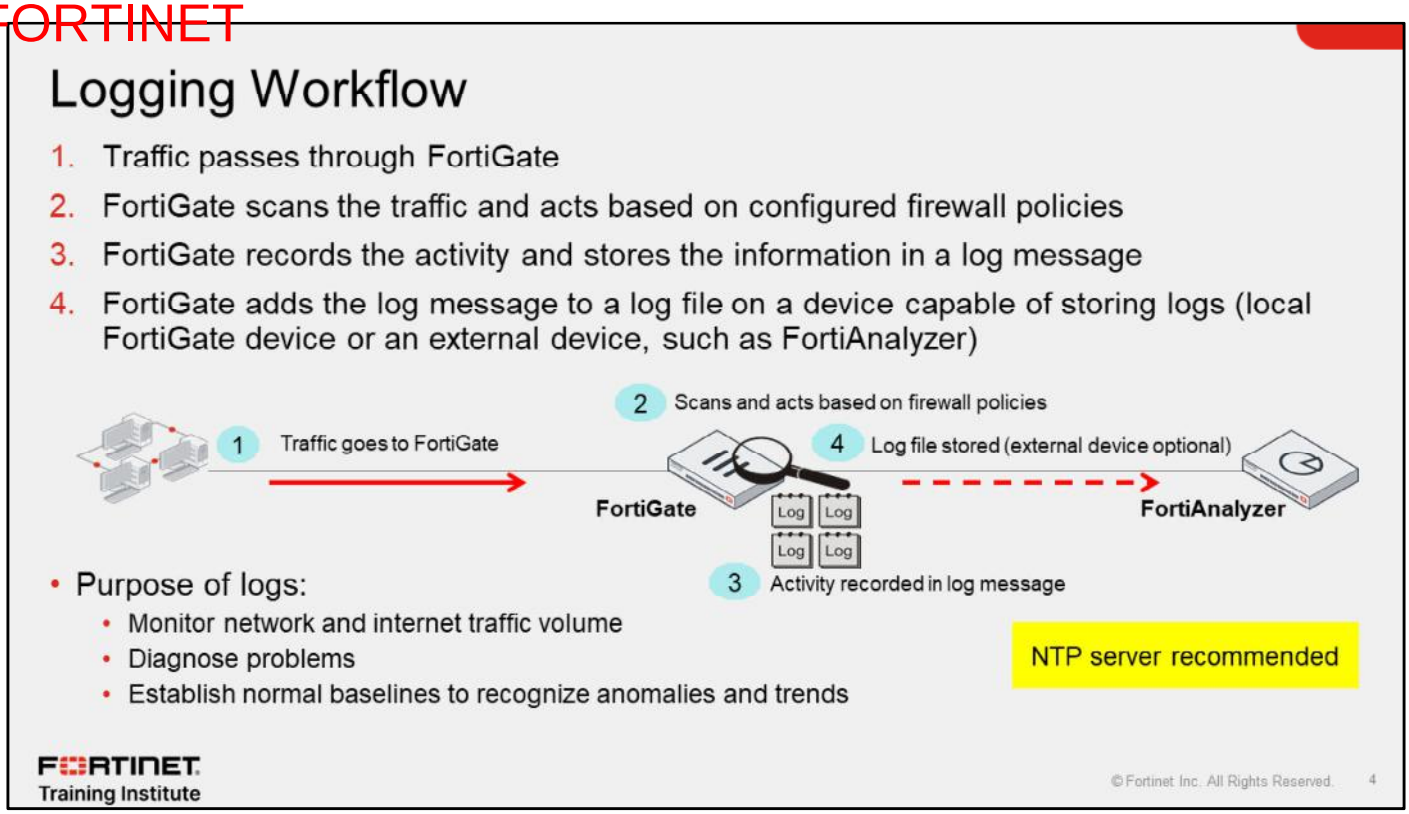


The supplemental material is covered in the topics shown on this slide.



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

By demonstrating competence in FortiAnalyzer logs and their structure, you will be able to use logs properly to obtain information about your FortiAnalyzer device.

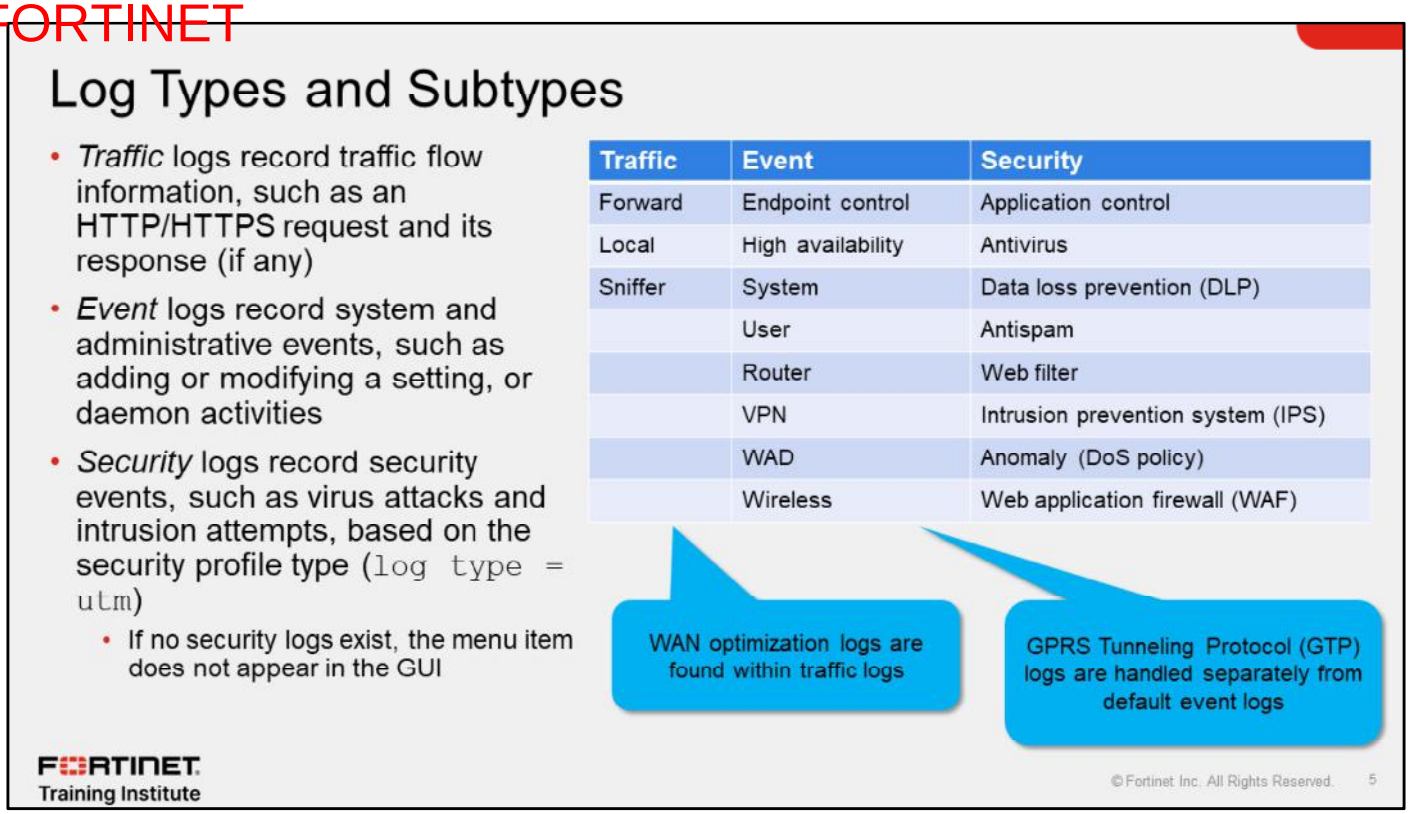


When traffic passes through FortiGate, FortiGate scans the traffic and then acts based on the firewall policies in place. FortiGate records this activity and stores the information in a log message. The log message is stored in a log file, which is then stored on a device capable of storing logs. FortiGate can store logs locally or send them to an external storage device, such as FortiAnalyzer.

Logs help you monitor your network traffic, locate problems, establish baselines, and more. Logs give you valuable insight into your network, enabling you to adjust your network security as needed.

Some organizations have legal requirements regarding logging, so it is important to be aware of your organization's policies during configuration.

For effective logging, your FortiGate system date and time should be accurate. You can either manually set the system date and time or configure FortiGate to keep its time correct automatically by synchronizing with a Network Time Protocol (NTP) server. Fortinet recommends the use of an NTP server.



FortiGate has three types of logs: traffic, event, and security. Each type is divided into subtypes.

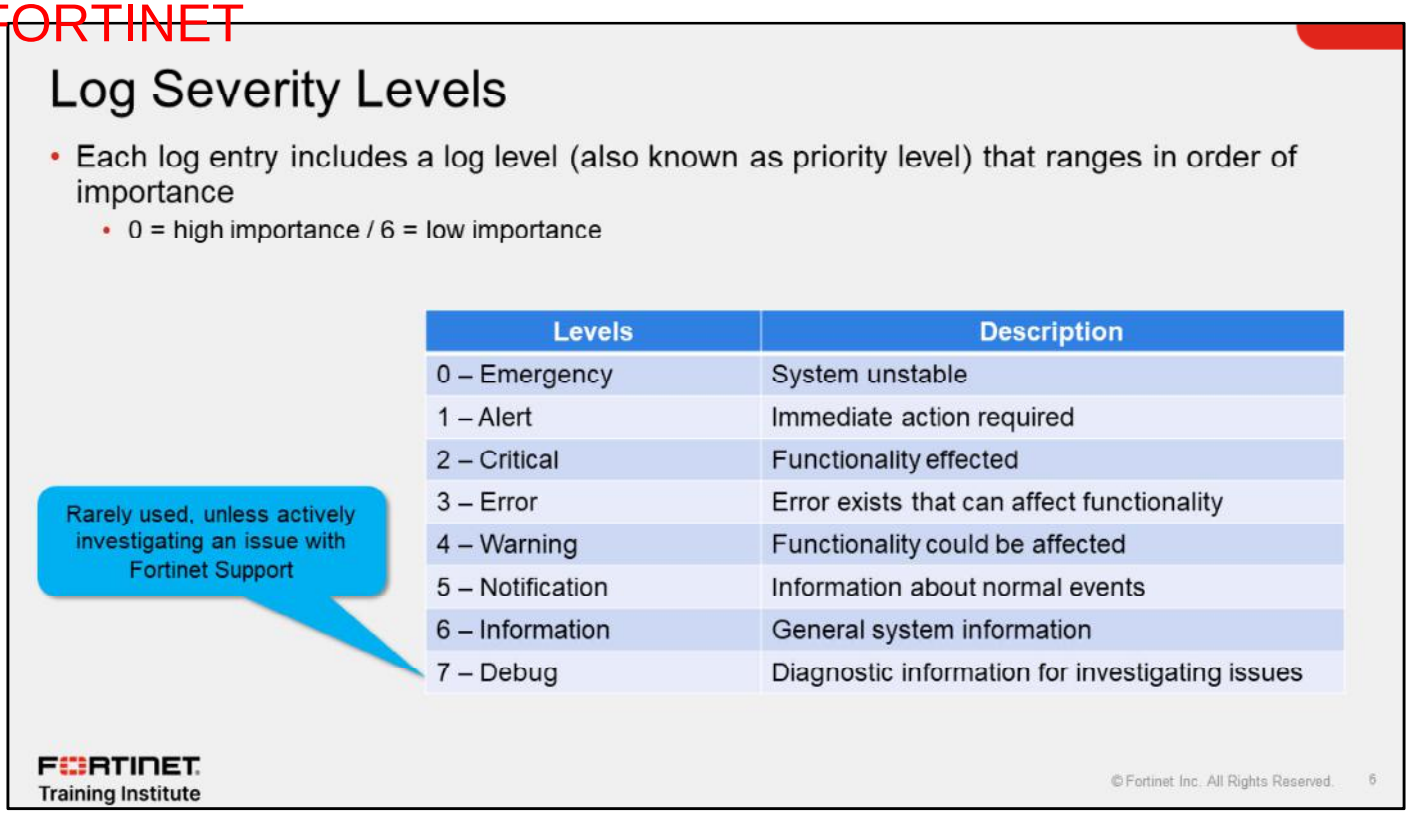
Traffic logs record traffic flow information, such as an HTTP/HTTPS request and its response. It contains the subtypes forward, local, and sniffer:

- Forward traffic logs contain information about traffic that FortiGate either accepted or rejected according to a firewall policy.
- Local traffic logs contain information about traffic sent directly to and from the FortiGate management IP addresses. They also include connections to the GUI and FortiGuard queries.
- Sniffer logs contain information related to traffic seen by the one-arm sniffer.

Event logs record system and administrative events, such as adding or modifying a setting, or daemon activities. Event logs contain subtypes named endpoint control, high availability, system, user, router, VPN, WAD, and wireless:

- System event logs contain information related to operations, such as automatic FortiGuard updates and GUI logins.
- User logs contain logon and logoff events for firewall policies with user authentication.
- Router, VPN, WAD, and wireless subtypes include logs for those features. For example, VPN contains IPsec and SSL VPN log entries.

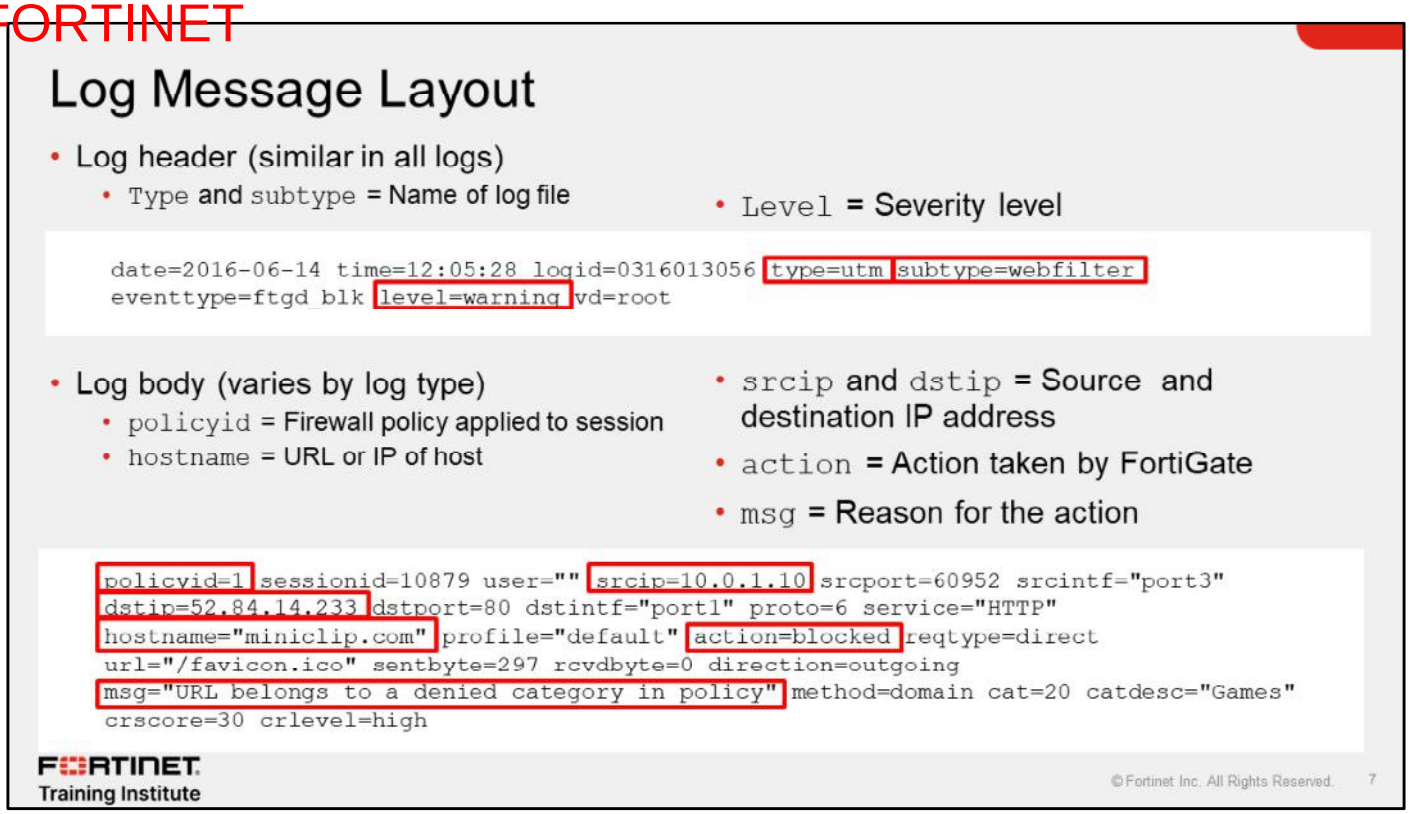
Security logs record security events, such as virus attacks and intrusion attempts. They contain log entries based on the security profile type (log type = utm), including application control, antivirus, DLP, anti-spam (email filter), web filter, intrusion protection, anomaly (DoS-policy), and WAF. Security logs and subtypes are visible in the GUI only if logs are created within it—if no security logs exist, the menu item does not appear.



Each log entry includes a log level (or priority level) that ranges in order of importance from Emergency to Information.

The Debug level adds diagnostic information to an event log. It is rarely used unless you are actively investigating an issue with Fortinet Support.

Generally, the lowest log level you should use is Information, but even this level generates many logs and can cause premature hard disk failure. Depending on the type of log and your organization's needs, you may want to use only Notification logs or higher.



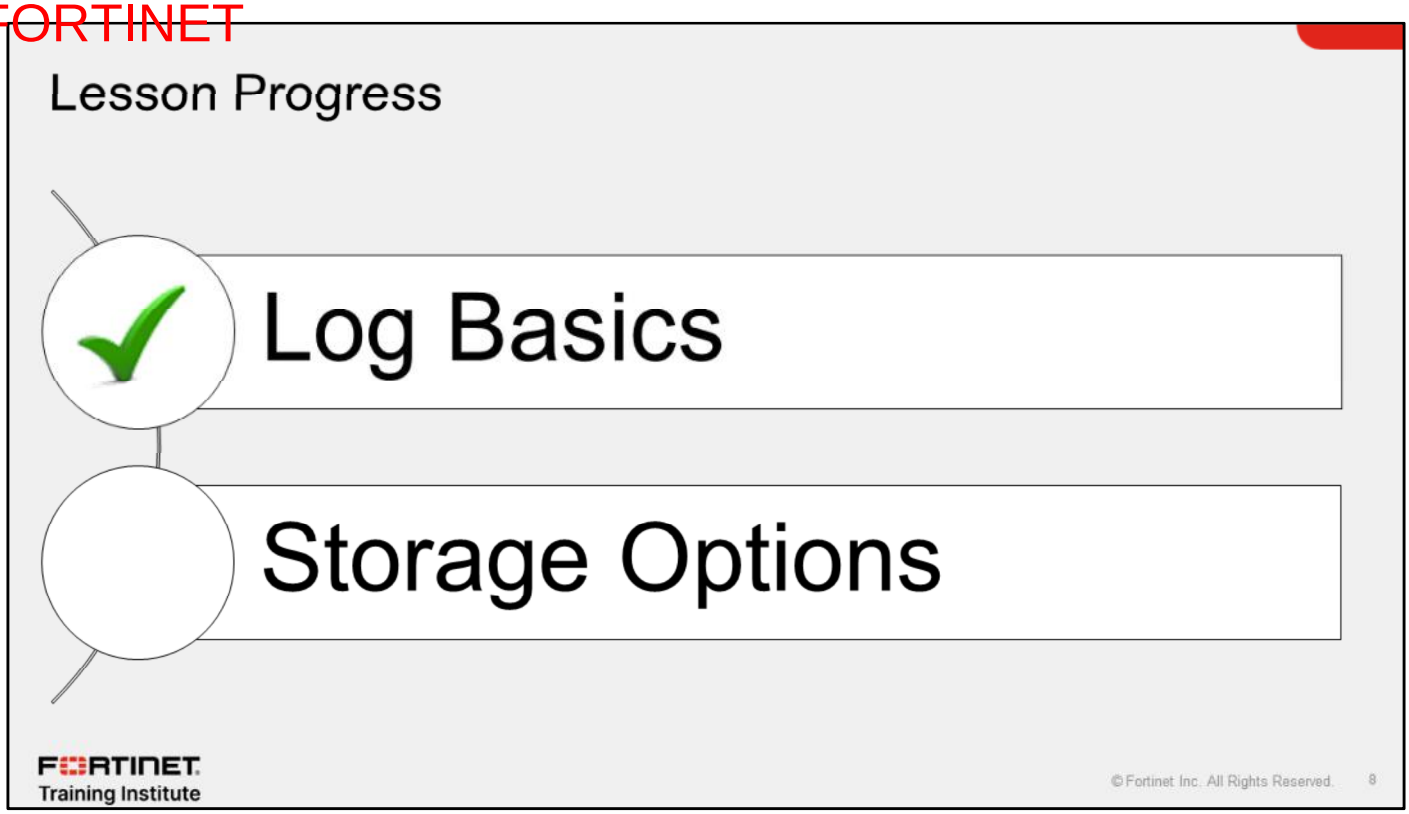
Every log message has a standard layout comprising two sections: a header and a body.

The header contains fields that are common to all log types, such as originating date and time, log identifier, log category, severity level, and VDOM. The value of each field is specific to the log message. In the raw log entry example shown on this slide, the log type is `UTM`, the subtype is `webfilter`, and the level is `warning`. The type and subtype of logs determine which fields appear in the log body.

The body, therefore, describes the reason the log was created and the actions that FortiGate took. These fields vary by log type. In the example shown on this slide, the fields are as follows:

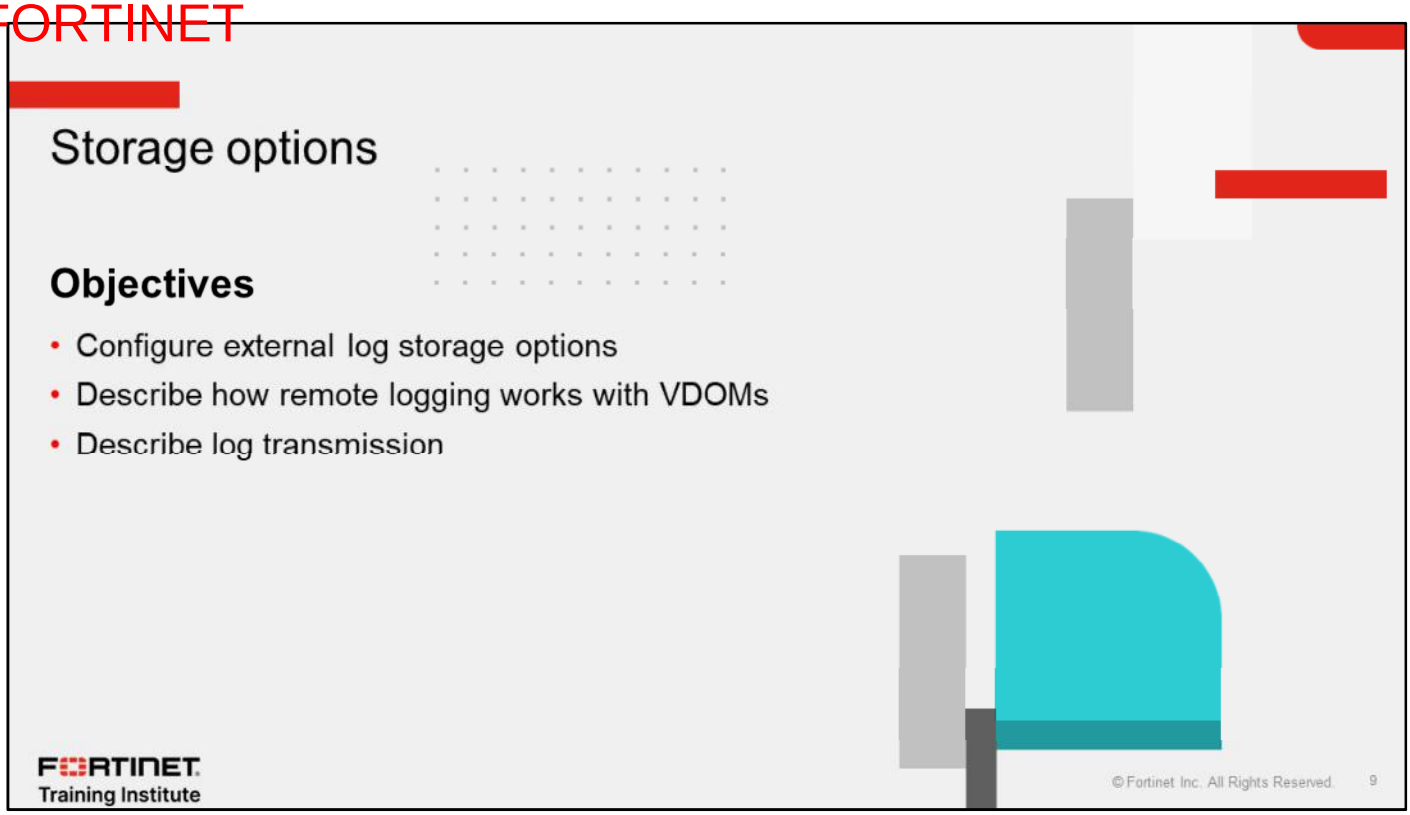
- The `policyid` field indicates which firewall rule matched the traffic.
- The `srcip` field indicates the source IP address.
- The `dstip` field indicates the destination IP address.
- The `hostname` field indicates the URL or IP of the host.
- The `action` field indicates what FortiGate did when it found a policy that matched the traffic.
- The `msg` field indicates the reason for the action taken. In this example, the action is `blocked`, which means that FortiGate prevented this IP packet from passing, and the reason is that it belongs to a denied category in the firewall policy.

If you log onto a third-party device, such as a syslog server, knowing the log structure is crucial to integration. For information on log structures and associated meanings, visit http://docs.fortinet.com.



Good job! You now understand the basics of logging on FortiGate devices.

Now, you will learn about log storage options.

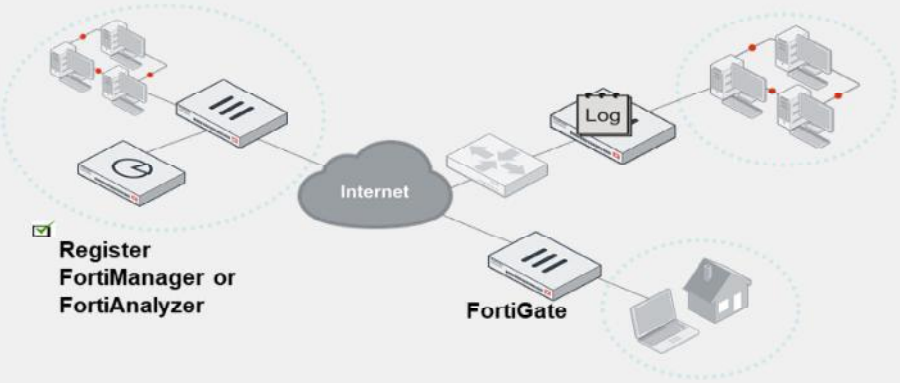


After completing this section, you should be able to achieve the objectives shown on this slide.

By demonstrating competence in the most common functions and operators used in FortiAnalyzer datasets, you will be able to configure appropriate storage options.

Log Storage—Remote

- FortiGate can send logs to both FortiAnalyzer and FortiManager (FortiGate must be a registered device)



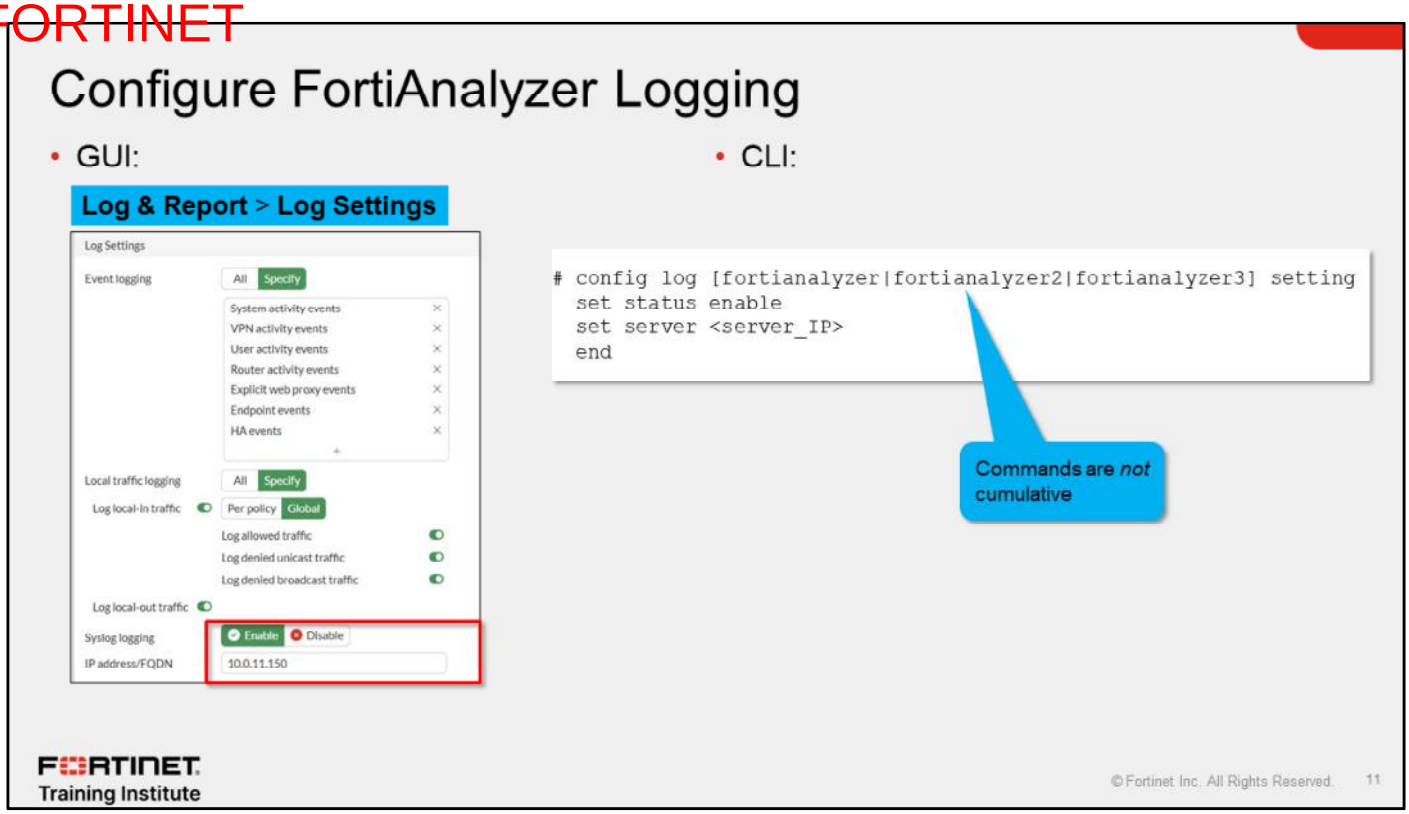
- Configure up to three separate FortiAnalyzer and FortiManager devices using the CLI
  - Multiple devices may be needed for redundancy
  - Generating and sending logs requires resources—be aware!

FORTINET Training Institute

 10

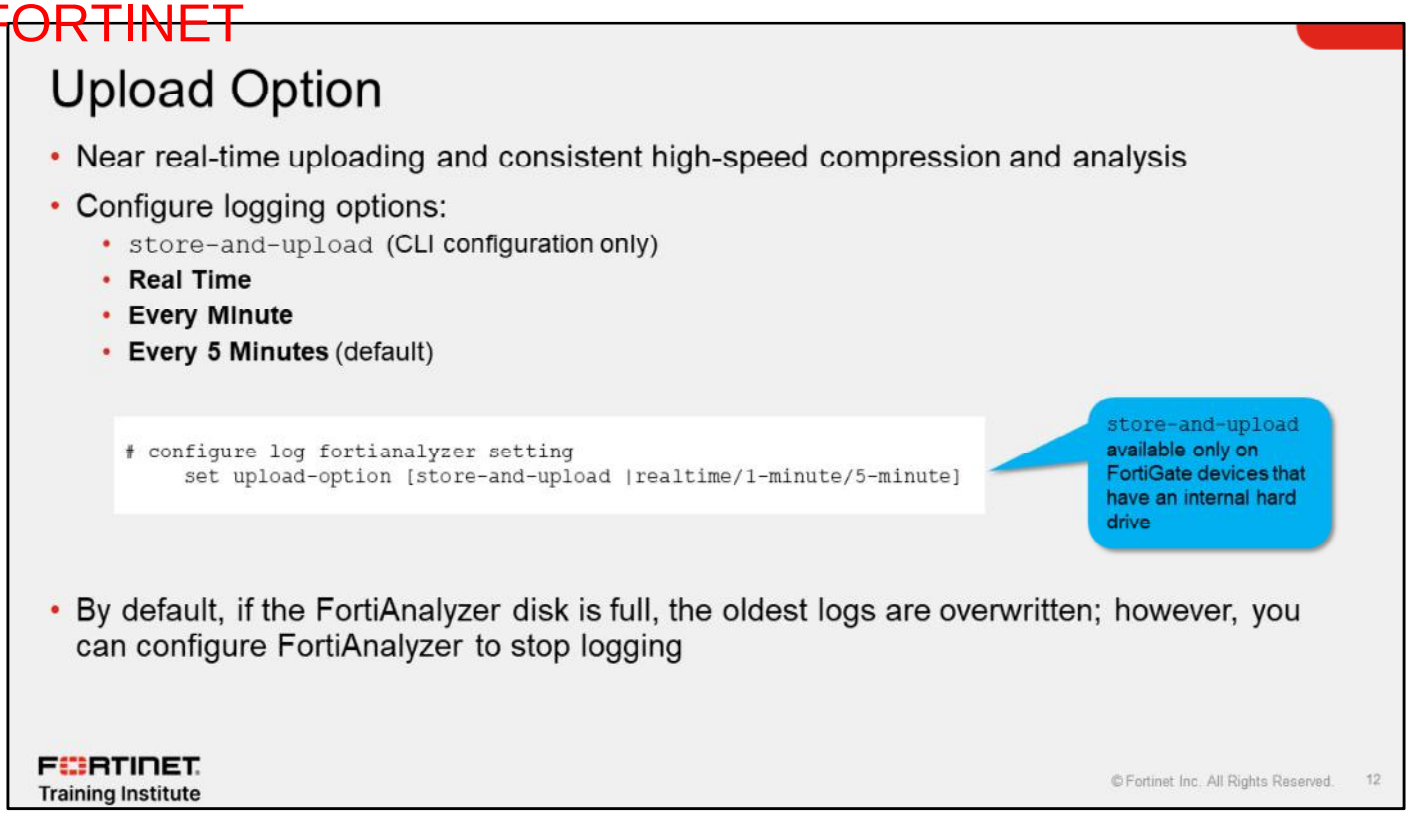
Configuring FortiGate to send logs to either FortiAnalyzer or FortiManager (with FortiAnalyzer features enabled) is the same. To enable FortiGate to send logs to these devices, you must register FortiGate with FortiAnalyzer or FortiManager. Once registered, FortiAnalyzer or FortiManager can begin accepting incoming logs from FortiGate.

Note that the **Test Connectivity** function on the GUI will indicate a failure until FortiGate is registered on FortiAnalyzer or FortiManager, because it has not yet been authorized to send logs.



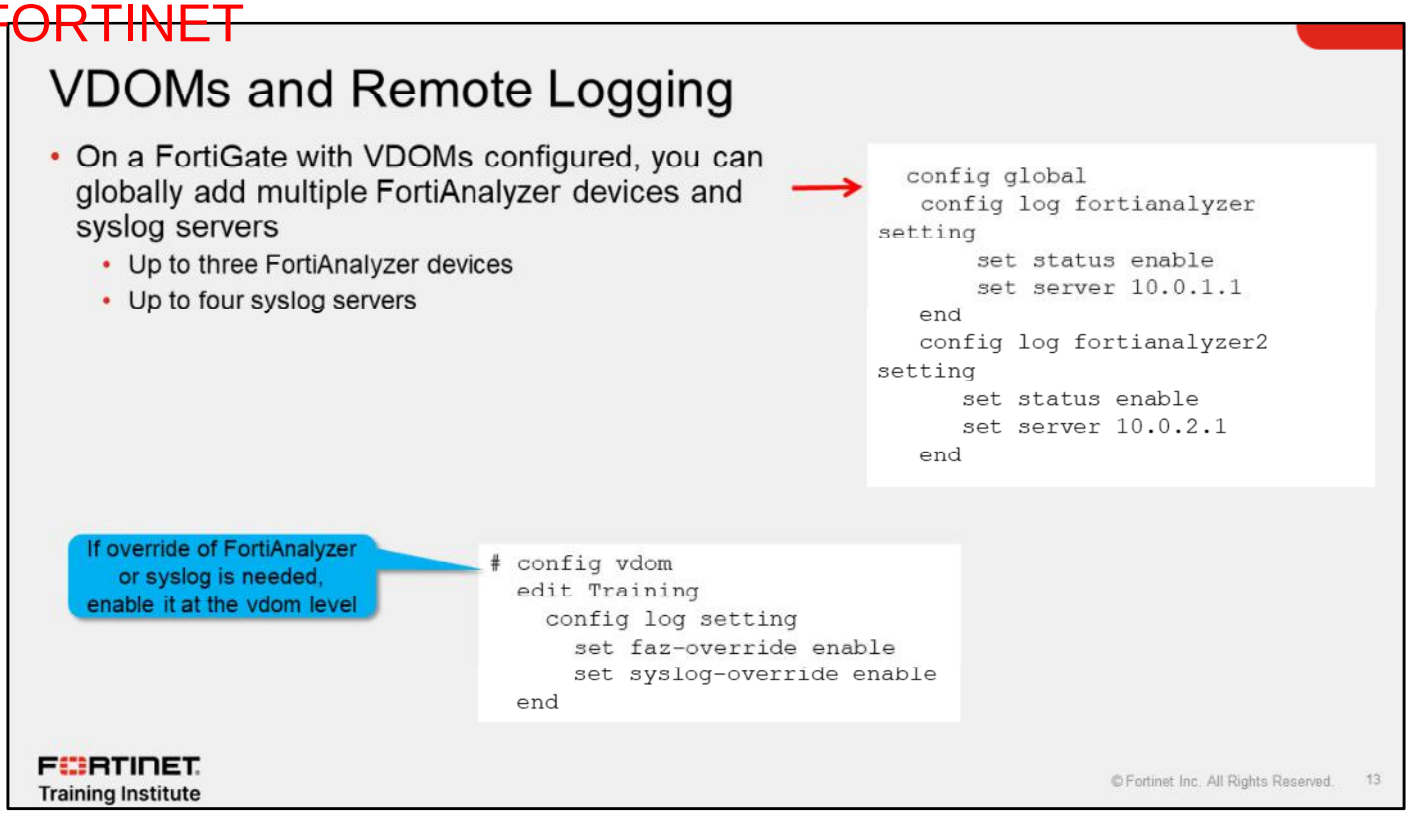
You can configure remote logging to FortiAnalyzer or FortiManager using either the GUI or the CLI.

- GUI: On the **Log Settings** page, enable **Syslog logging**, and then type the IP address of the remote logging device.
- CLI: For both FortiAnalyzer and FortiManager, use the `config log fortianalyzer setting` command. Even though FortiManager isn't explicitly mentioned in the command, it is used for FortiManager as well. Using the CLI, you can add up to three separate devices to increase redundancy for the protection of log data. The commands for the three devices are not cumulative. Generating logs uses system resources, so if FortiGate frequently creates and sends logs to multiple locations, CPU and RAM usage increase.

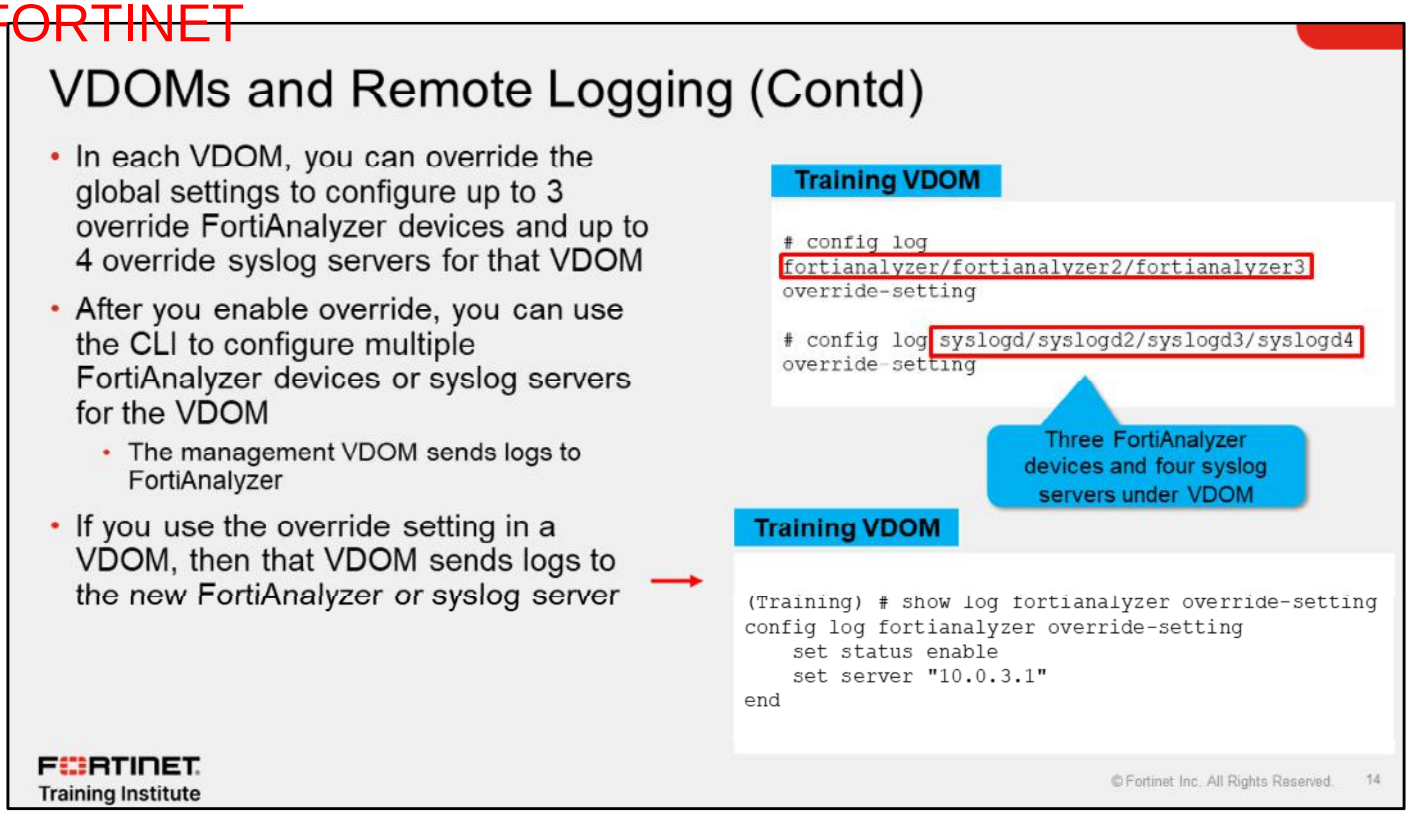


FortiGate allows near real-time uploading and consistent high-speed compression and analysis to FortiAnalyzer and FortiManager.

If your FortiGate model includes an internal hard drive, the `store-and-upload` option is available. This allows you to store logs on the disk and then upload them to FortiAnalyzer or FortiManager at a scheduled time (usually a low-bandwidth time). You can configure the store-and-upload option and a schedule on the CLI only.

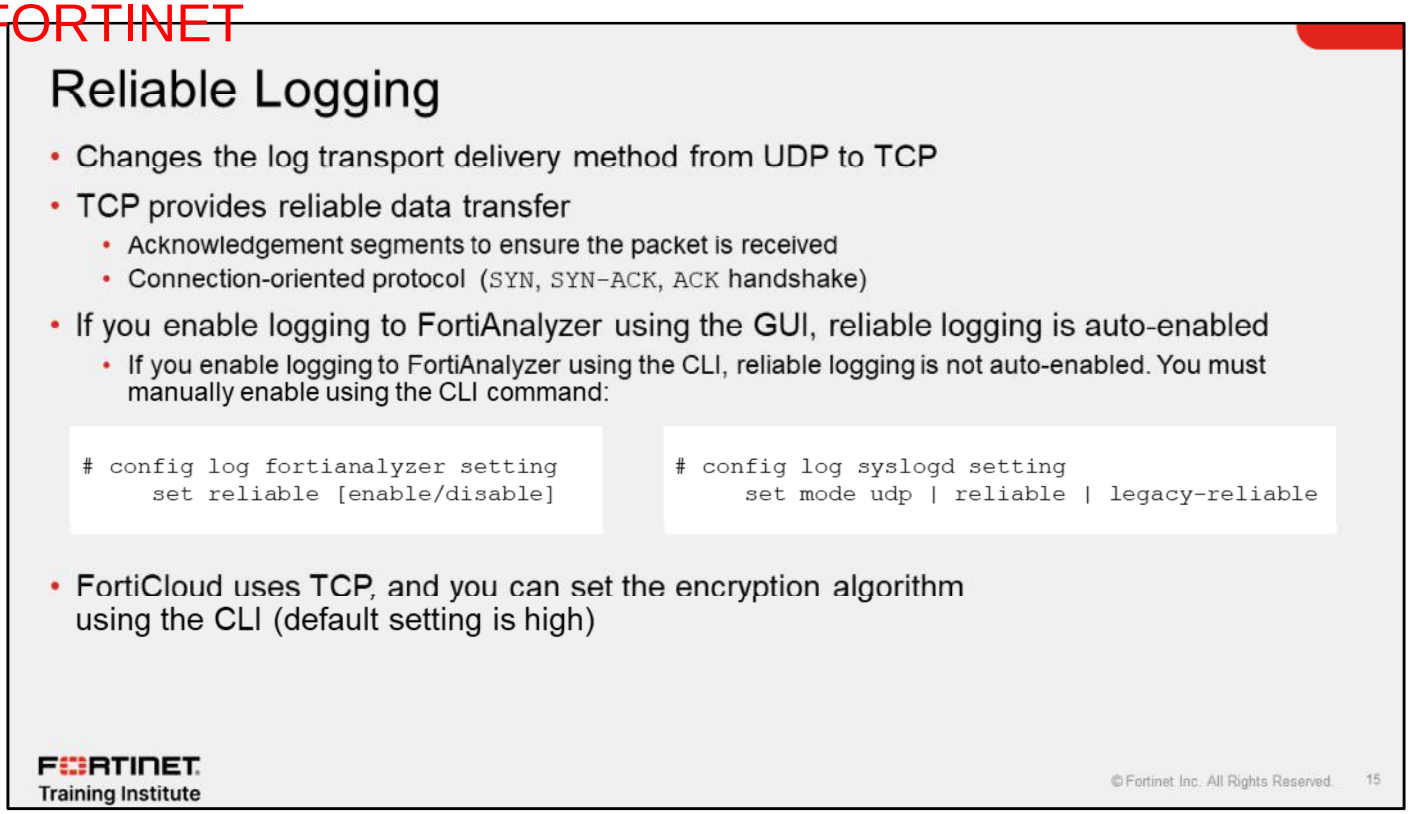


A FortiGate with VDOMs configured can support multiple FortiAnalyzer devices and syslog servers. In the global settings, you can configure up to three FortiAnalyzer devices and up to four syslog servers.



For each VDOM, you can override the global settings to configure up to three override FortiAnalyzer devices and up to four override syslog servers.

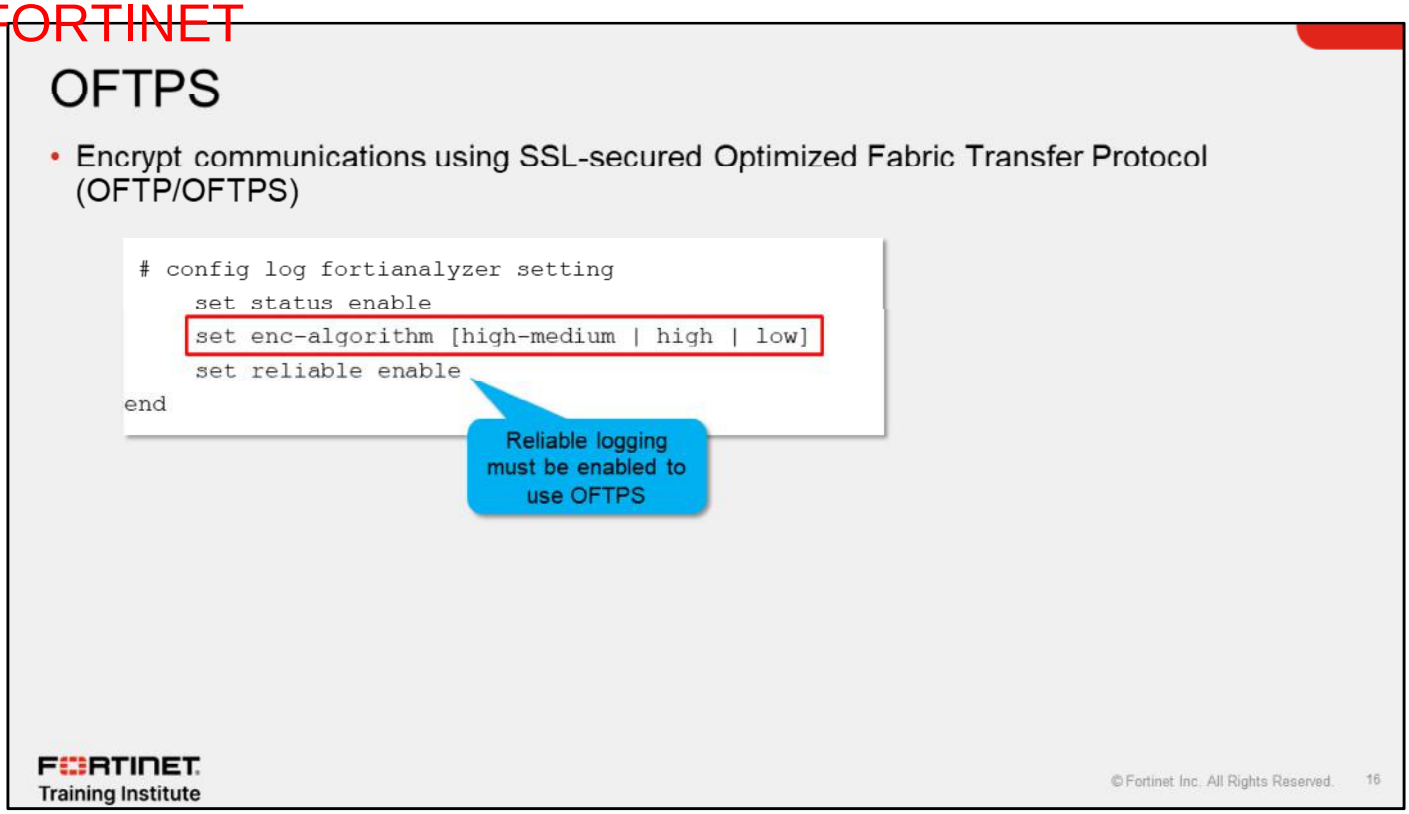
The management VDOM is responsible for sending logs to FortiAnalyzer devices and syslog servers. Therefore, if you use the override setting in a VDOM, that VDOM is responsible for sending logs to the new FortiAnalyzer or syslog server you configured for it.



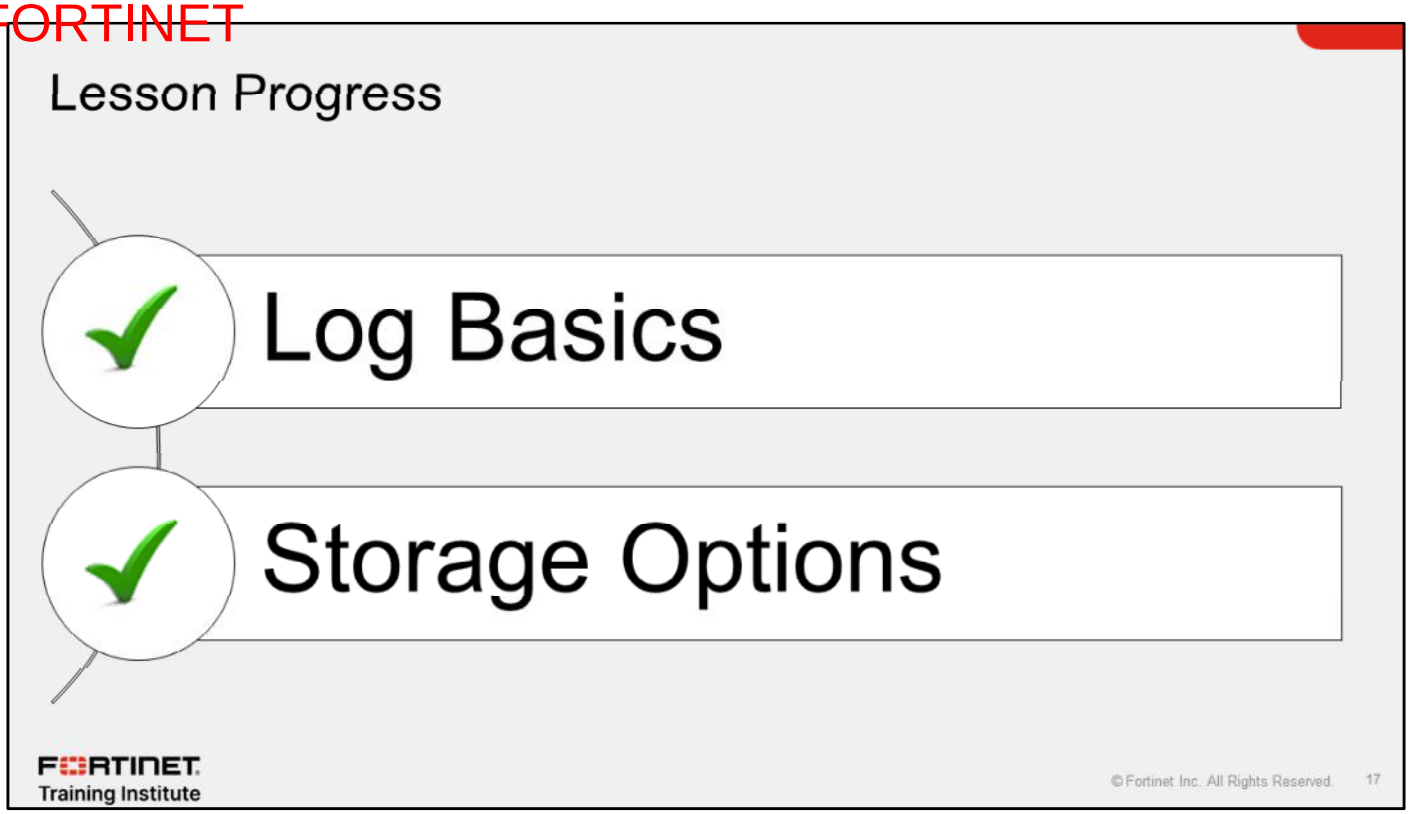
When you enable reliable logging on FortiGate, the log transport delivery method changes from UDP to TCP. TCP provides reliable data transfer, guaranteeing that the data transferred remains intact and arrives in the same order in which it was sent.

If you enable logging to FortiAnalyzer or FortiManager using the GUI, reliable logging is automatically enabled. If you enable logging using the CLI, you must enable reliable logging using the CLI command shown on this slide.

Logging to FortiCloud uses TCP, and you can set the encryption algorithm using the CLI (the default setting is high).

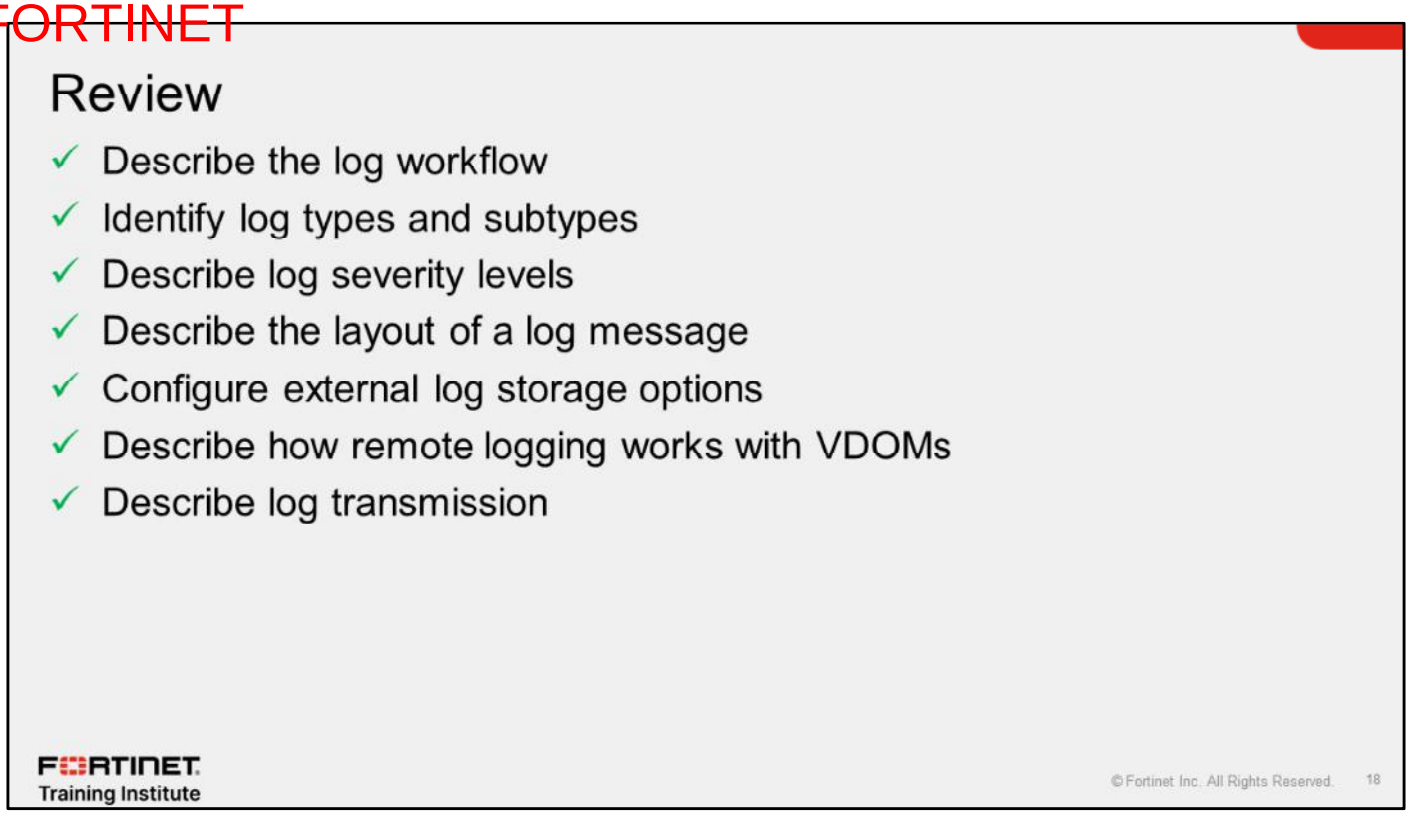


Optionally, if you use reliable logging, you can encrypt communications with SSL-encrypted OFTP traffic, ensuring that when a log message is generated, it is transmitted securely across an unsecured network. You can encrypt communications with SSL-secured OFTP by configuring the enc-algorithm setting on the CLI.



Congratulations! You completed this lesson.

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



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