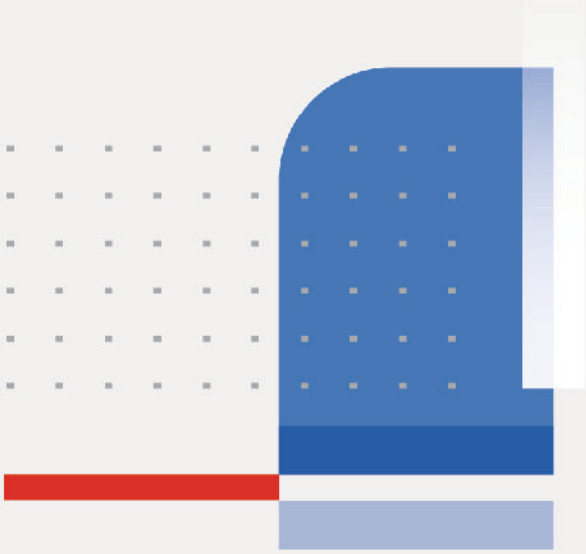
FORTINET CERTIFIED PROFESSIONAL
Security Operations

FortiAnalyzer Analyst Study Guide

FortiAnalyzer 7.4

FORTINET
Training Institute



Fortinet Training Institute - Library

https://training.fortinet.com

Fortinet Product Documentation

https://docs.fortinet.com

Fortinet Knowledge Base

https://kb.fortinet.com

Fortinet Fuse User Community

https://fusecommunity.fortinet.com/home

Fortinet Forums

https://forum.fortinet.com

Fortinet Product Support

https://support.fortinet.com

FortiGuard Labs

https://www.fortiguard.com

Fortinet Training Program Information

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

Fortinet | Pearson VUE

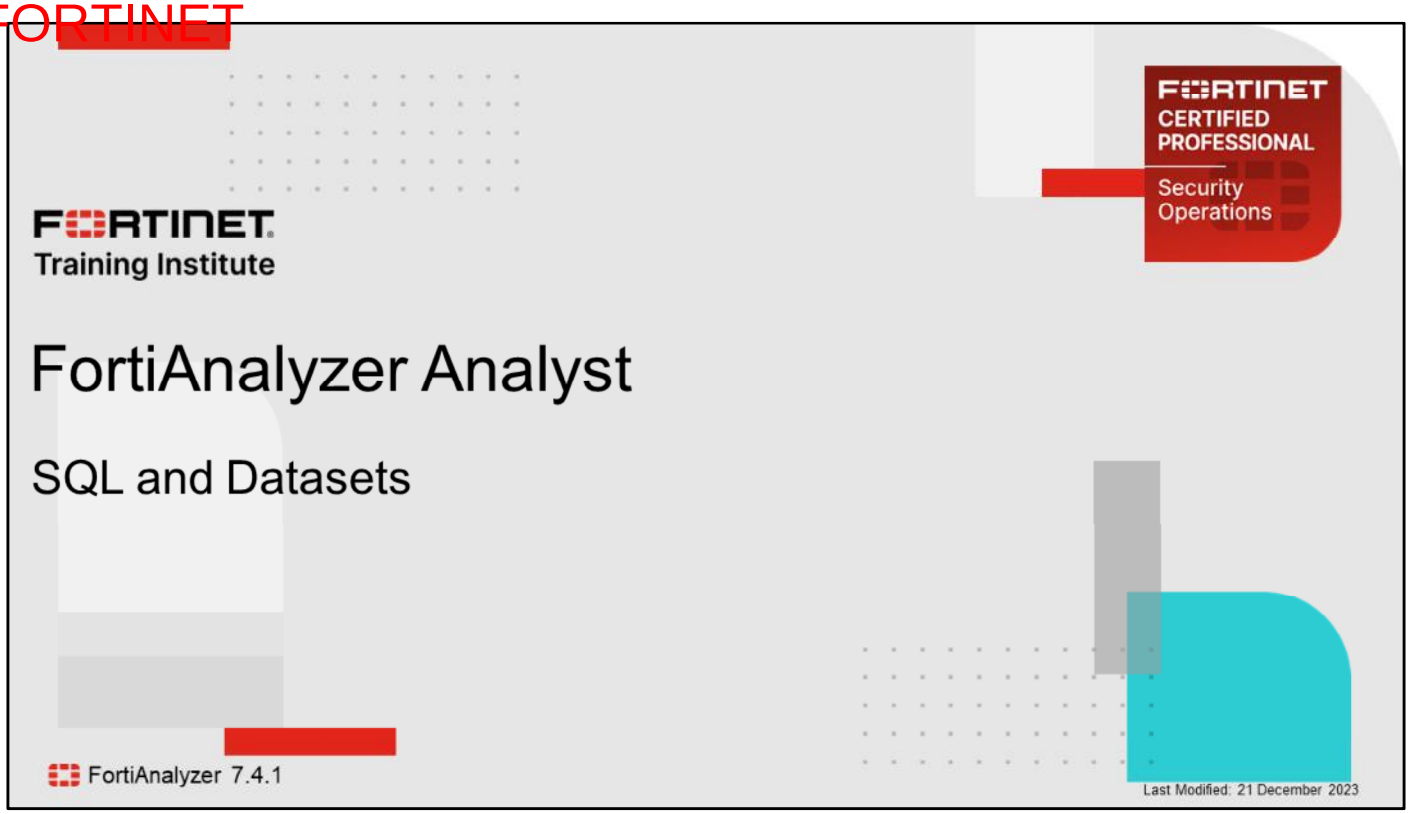
https://home.pearsonvue.com/fortinet

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

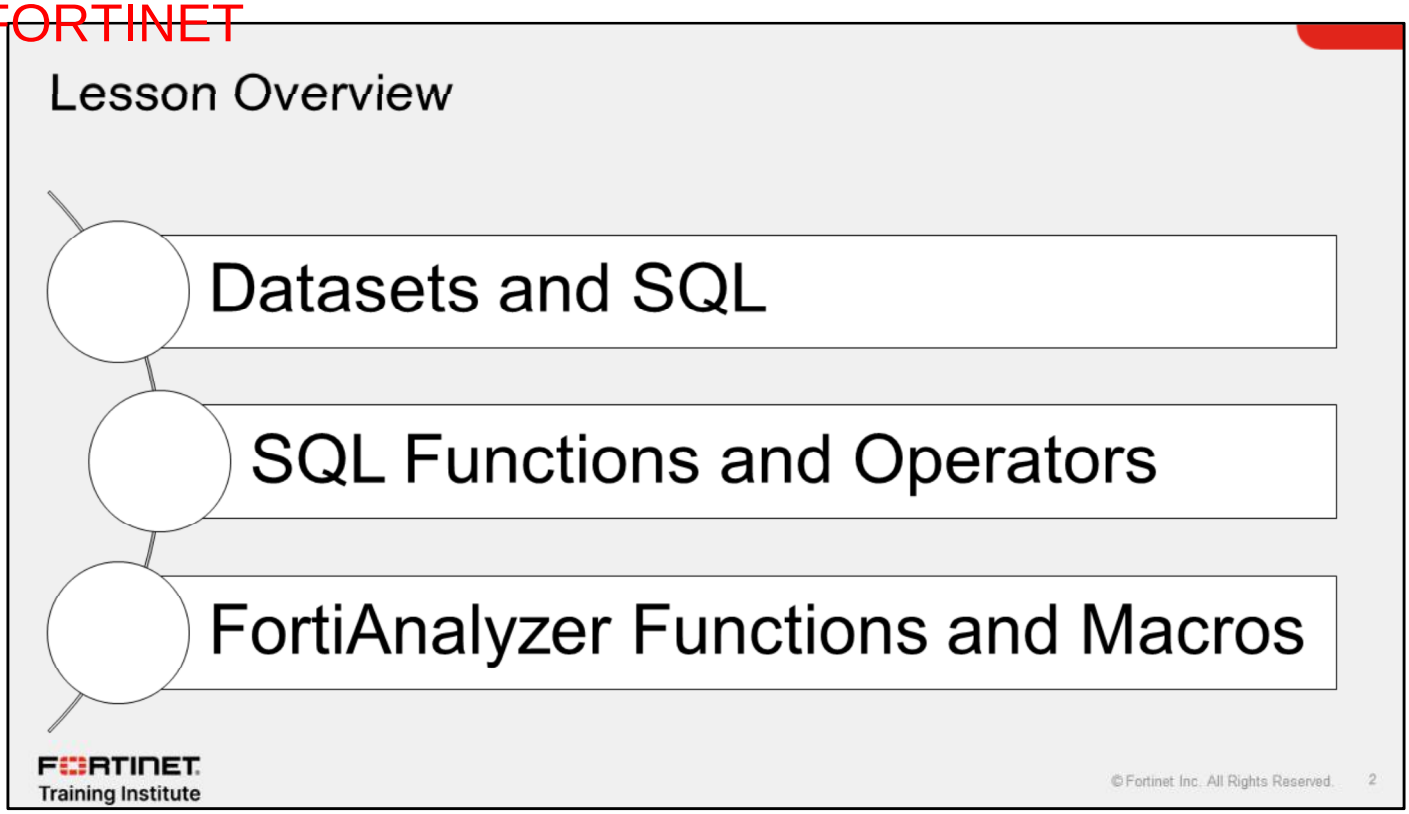
https://helpdesk.training.fortinet.com/support/home

12/21/2023

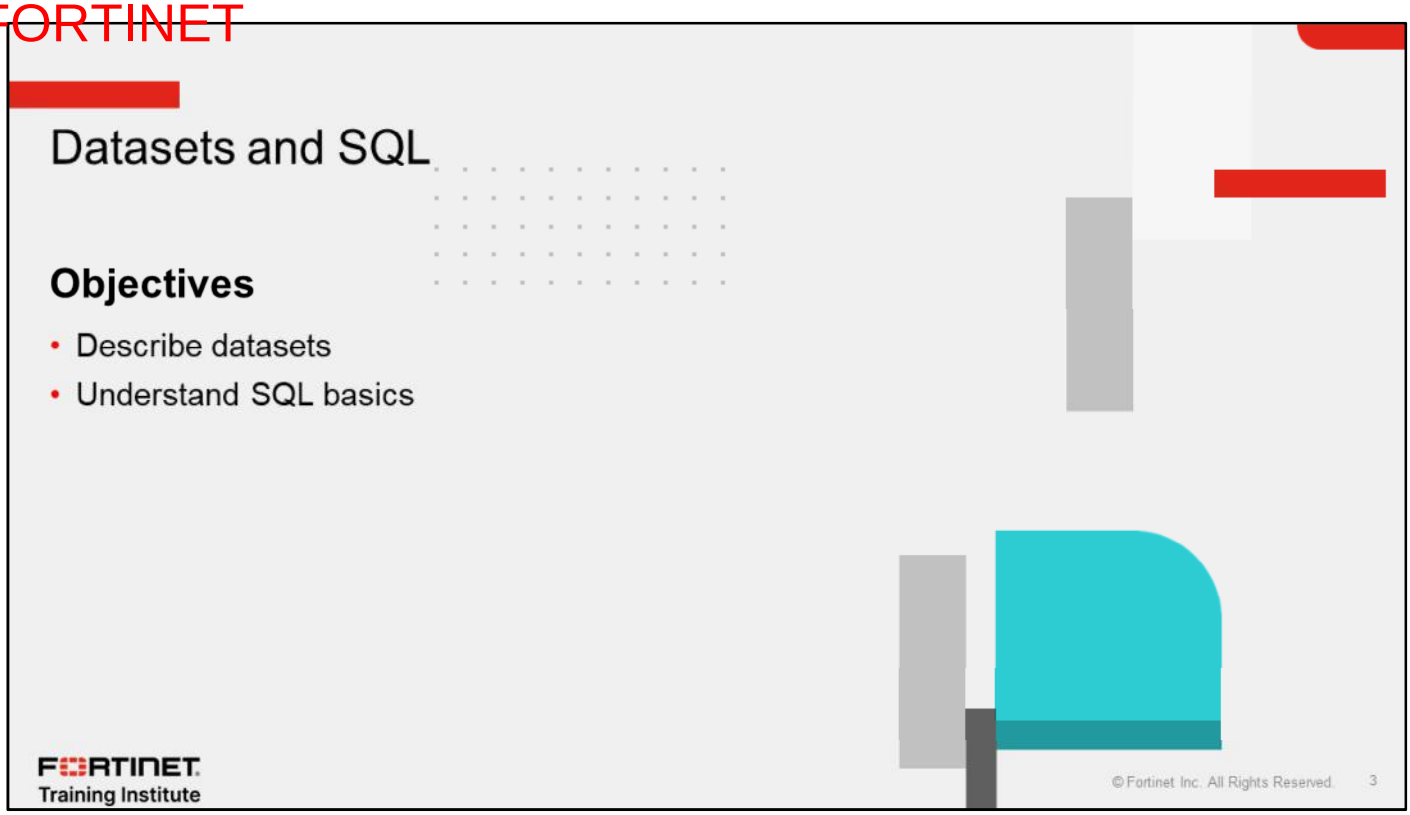
TABLE OF CONTENTS



This supplemental material provides an overview of SQL and datasets. Teaching a comprehensive lesson on SQL is out of scope for FortiAnalyzer training, so the goal of this material is to provide you with the information you need to modify or create datasets for the purpose of extracting data for reports.

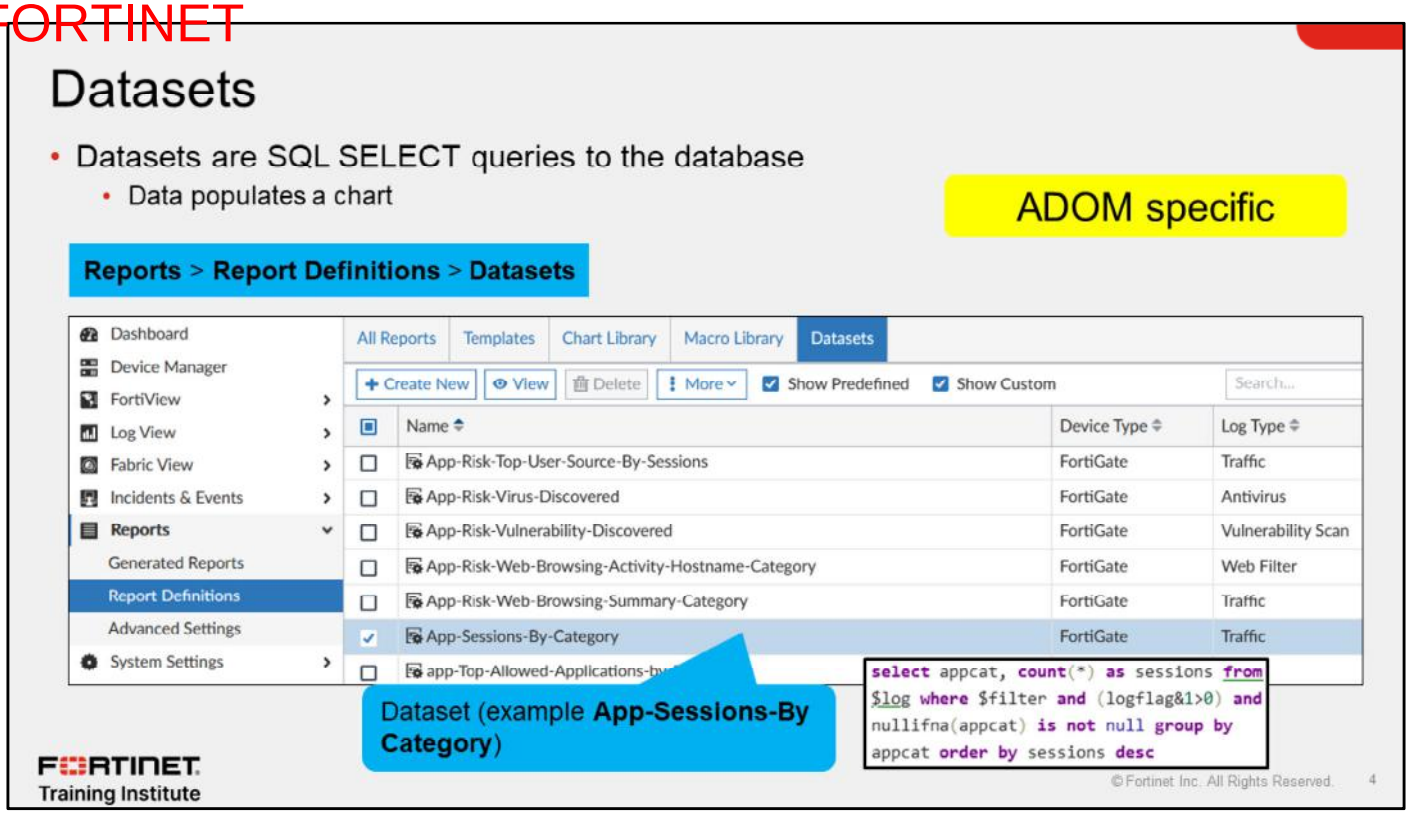


The supplemental material is covered in the topics shown on this slide.



This section covers datasets. Datasets define what data is extracted from the database and represented in the chart on a report.

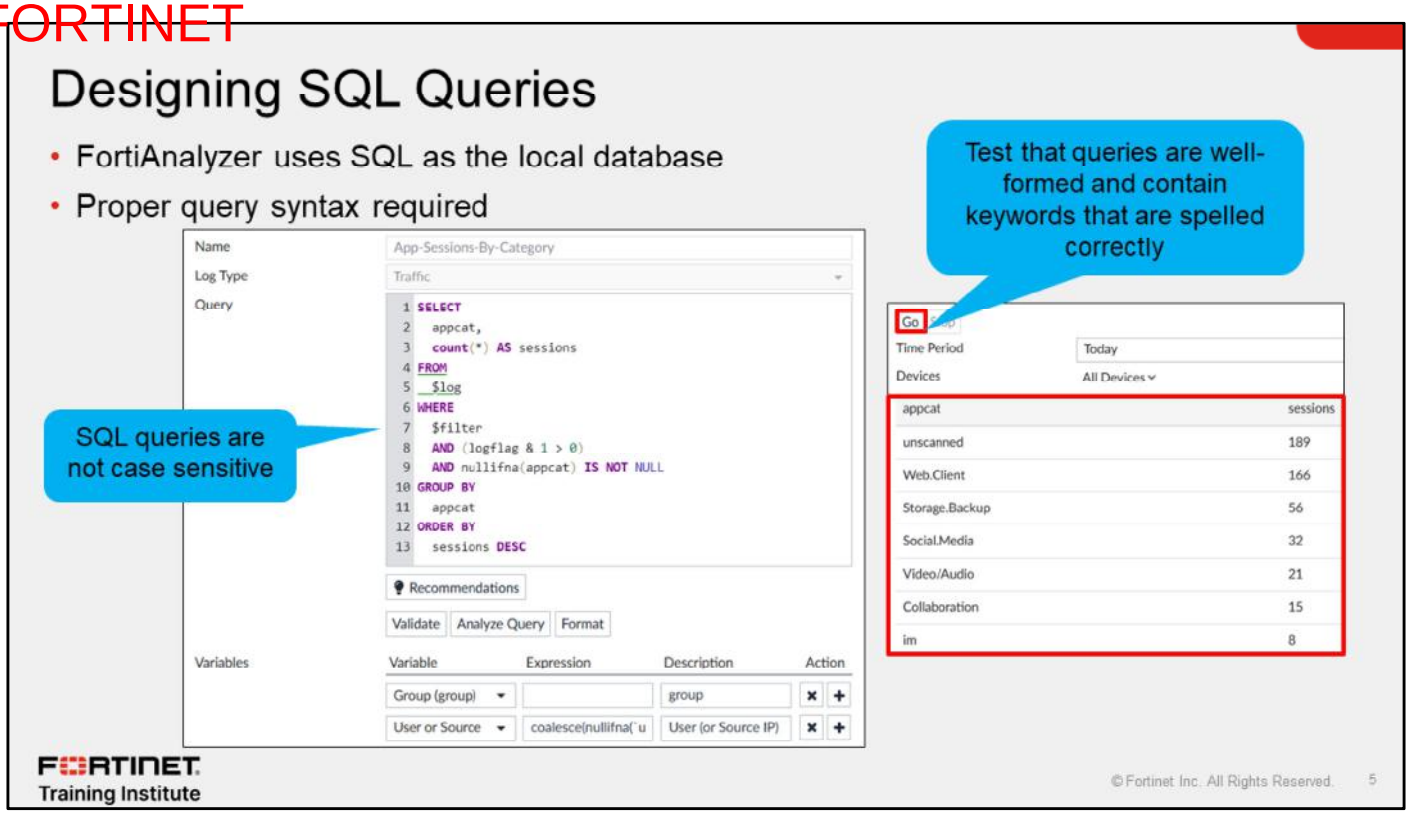
FortiAnalyzer provides predefined datasets that address the most common queries. However, if you need to modify those datasets or create your own, you need to understand SQL.



A dataset is an SQL `SELECT` query. The result of that query—the specific data polled from the database—is what populates a chart.

FortiAnalyzer includes many predefined datasets that contain some of the most common database queries. You can view the predefined datasets from the **Datasets** page.

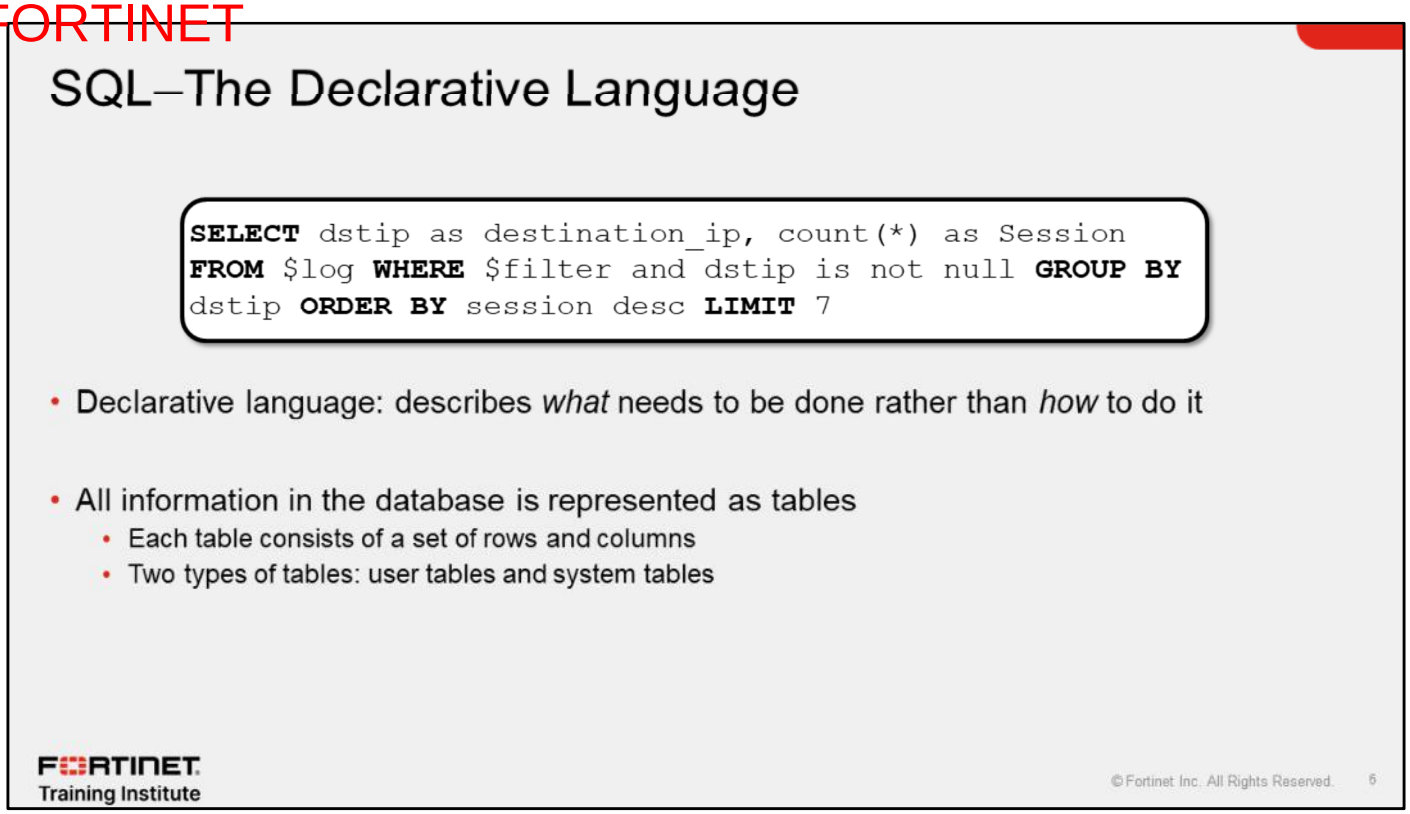
This slide shows an example of the default **App-Sessions-By-Category** dataset.



When you are building your queries, you must use SQL syntax to interface with the database. When creating or editing datasets, you can click **Validate** to check if the SQL query is valid, or see what errors are returned. You can also click **Go** to test your query. If the query is formed correctly, and the data you are querying is available in the database, the results appear. If the query is not formed correctly, you will see an error message.

You can also click **Format** to format the entered SQL query, making it easier to read, update, and detect errors. The screenshot on this slide shows a formatted SQL query.

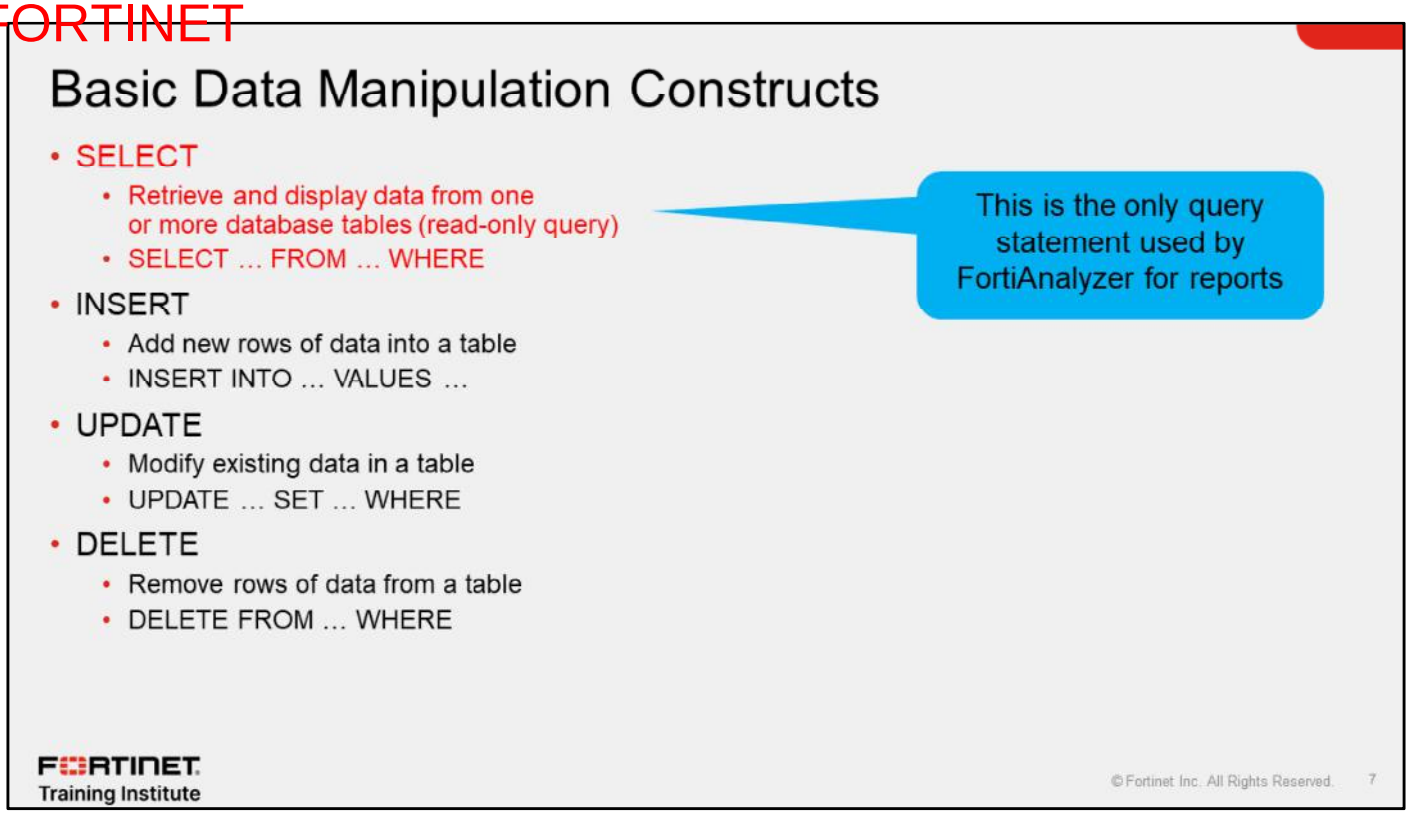
Note that SQL queries are not case sensitive.



Now take a closer look at the query itself. In order to understand this example dataset, and more specifically, what it is querying, you need to understand SQL. SQL is what is known as a declarative language—it describes *what* needs to be done rather than *how* to do it.

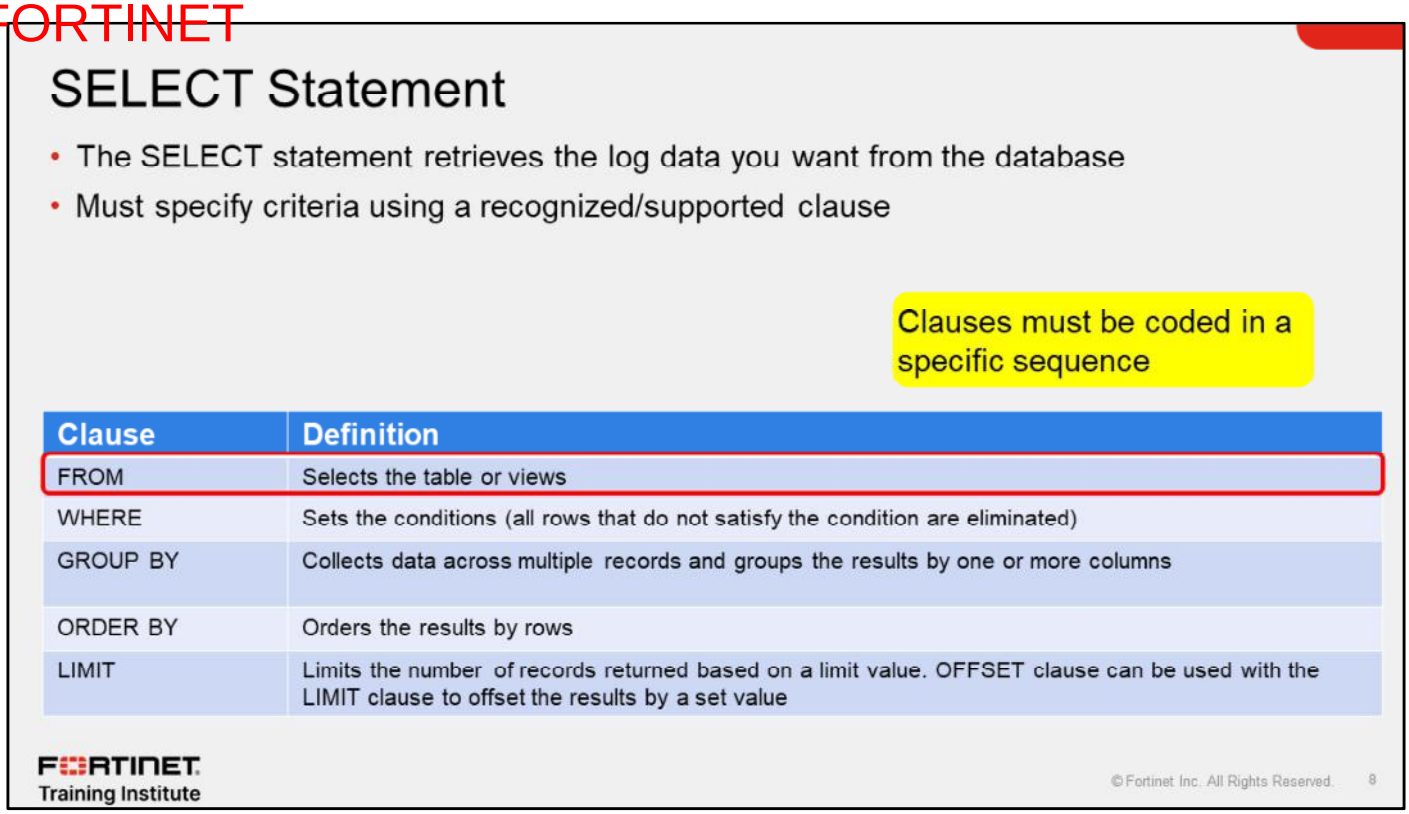
In a SQL database all information is represented as tables, and each table consists of a set of rows and columns. There are two types of tables:

- User tables, which contain information that is in the database
- System tables, which contain the database description



In order to retrieve and manipulate data in the database, you need to use data manipulation language, which is a family of syntax elements used by SQL. These syntax elements are SELECT, INSERT, UPDATE, and DELETE. These are the first words used in a query—they are the declarative verbs describing what you want done.

As far as FortiAnalyzer reports are concerned, only the SELECT statement is used. It is purely a read-only query statement that is used to retrieve data from the database.

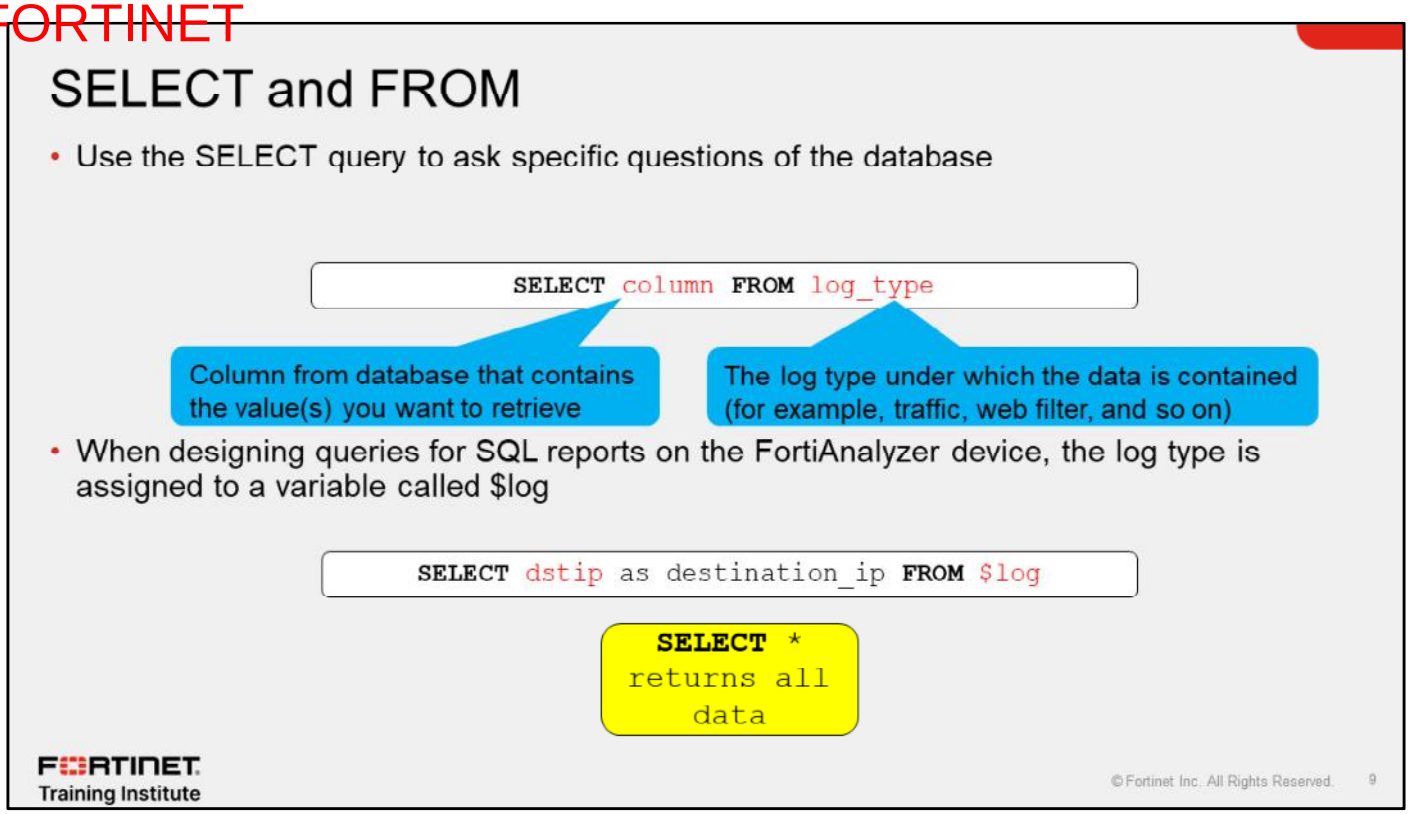


The SELECT statement is used to query the database and retrieve log data. In order to pull the data you want, you must specify the criteria. For example, let's say you want to query the database for a list of employees who work in the IT department. In order to put this criteria into a language that SQL understands, you must use a clause recognized by the SELECT statement.

The main clauses FortiAnalyzer reports use are:

- FROM, which specifies the table.
- WHERE, which specifies the conditions. All rows that do not satisfy the condition are eliminated from 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 rows. If ORDER BY is not given, the rows are returned in whatever order the system finds the fastest to produce. And finally,
- LIMIT, which limits the number of records returned based on a specified value. OFFSET is another clause often used along with LIMIT, which offset the 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. This is to say that following the SELECT keyword, the statement must be followed by one or more clauses in the order they appear in this table provided. For example, you cannot use the WHERE clause before the FROM clause. You do not have to use all optional clauses, but the ones you do use must be in the correct sequence.



SELECT is the first word used in any SQL query that involves FortiAnalyzer reports. This is a declarative statement that instructs the program to query the column in the database for the information you want returned. For example:

```
SELECT dstip
```

`Dstip` is the column name for destination IP in the SQL schema. Note that you can select more than one column name and you can also have the column name appear under a more user friendly name in the results table by appending the command with "`as <friendly_name_of_column>`. For example, `SELECT dstip as destination_ip`. In the results table, the values for `dstip` will appear under a column named **destination_ip**.

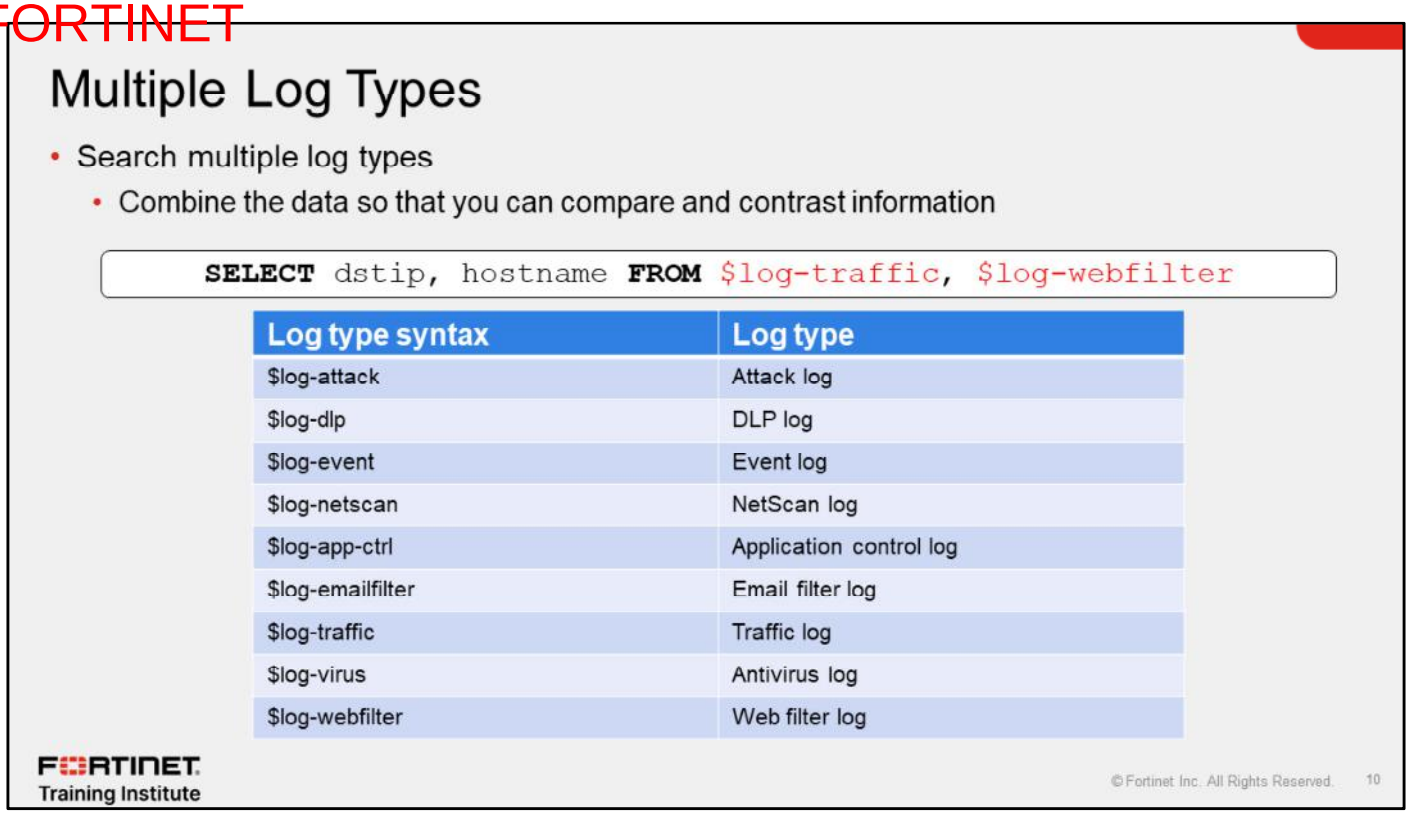
If you want to return all data, you can use the `*` symbol. For example, `SELECT *`. Though most of the time that is more information that you require.

At minimum, you must use the FROM clause with your SELECT statement. This instructs the program where the information is located.

For example:

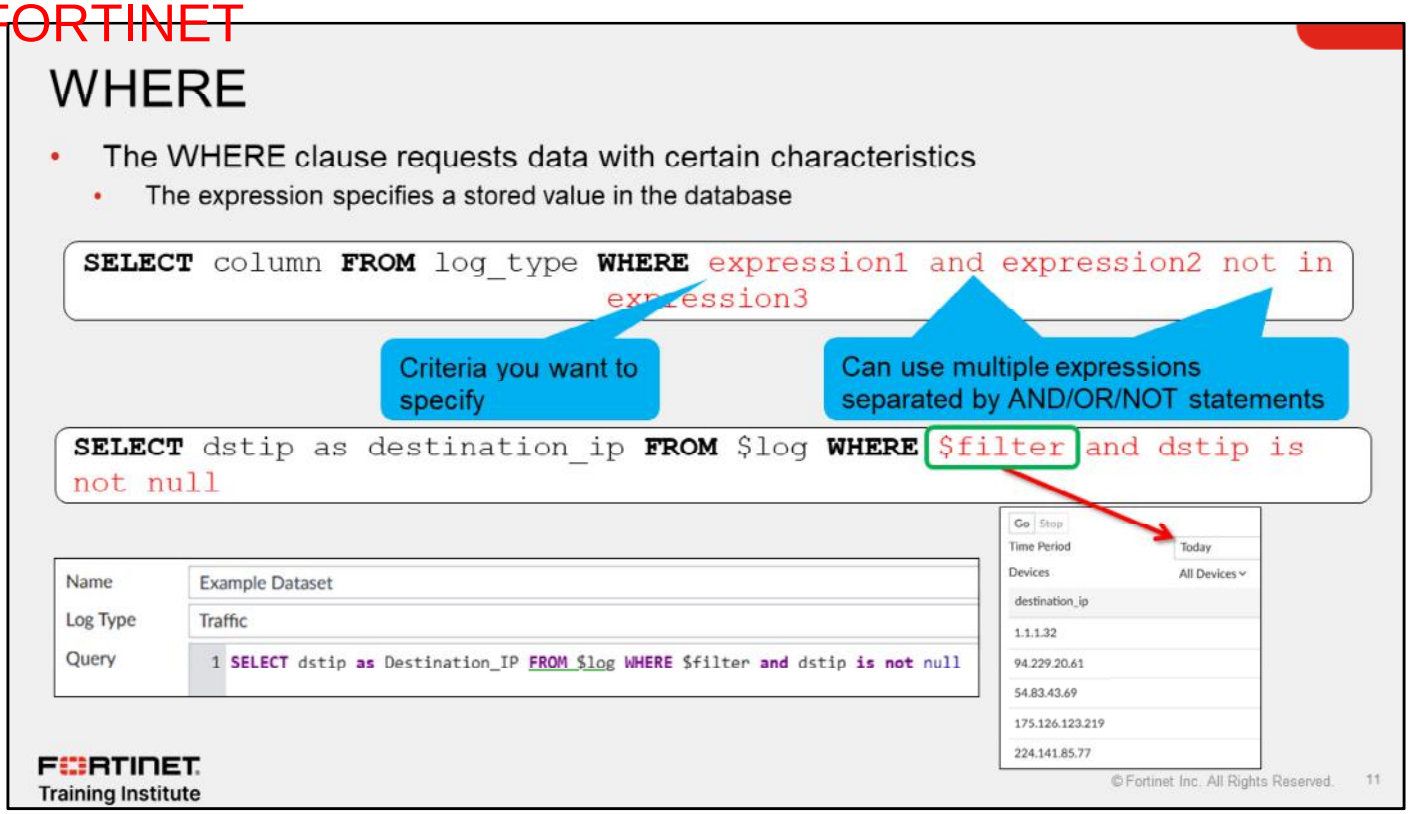
```
FROM $log
```

Here `$log` refers to the logs in the log type selected for the dataset, such as traffic logs or web filter logs.



You can search multiple log types in order to combine the data so that you can compare and contrast information. To do this, use the log type syntax associated with the specific log type. For example, if you want to search both the traffic logs and web filter logs, use:

```
FROM $log-traffic, $log-webfilter
```



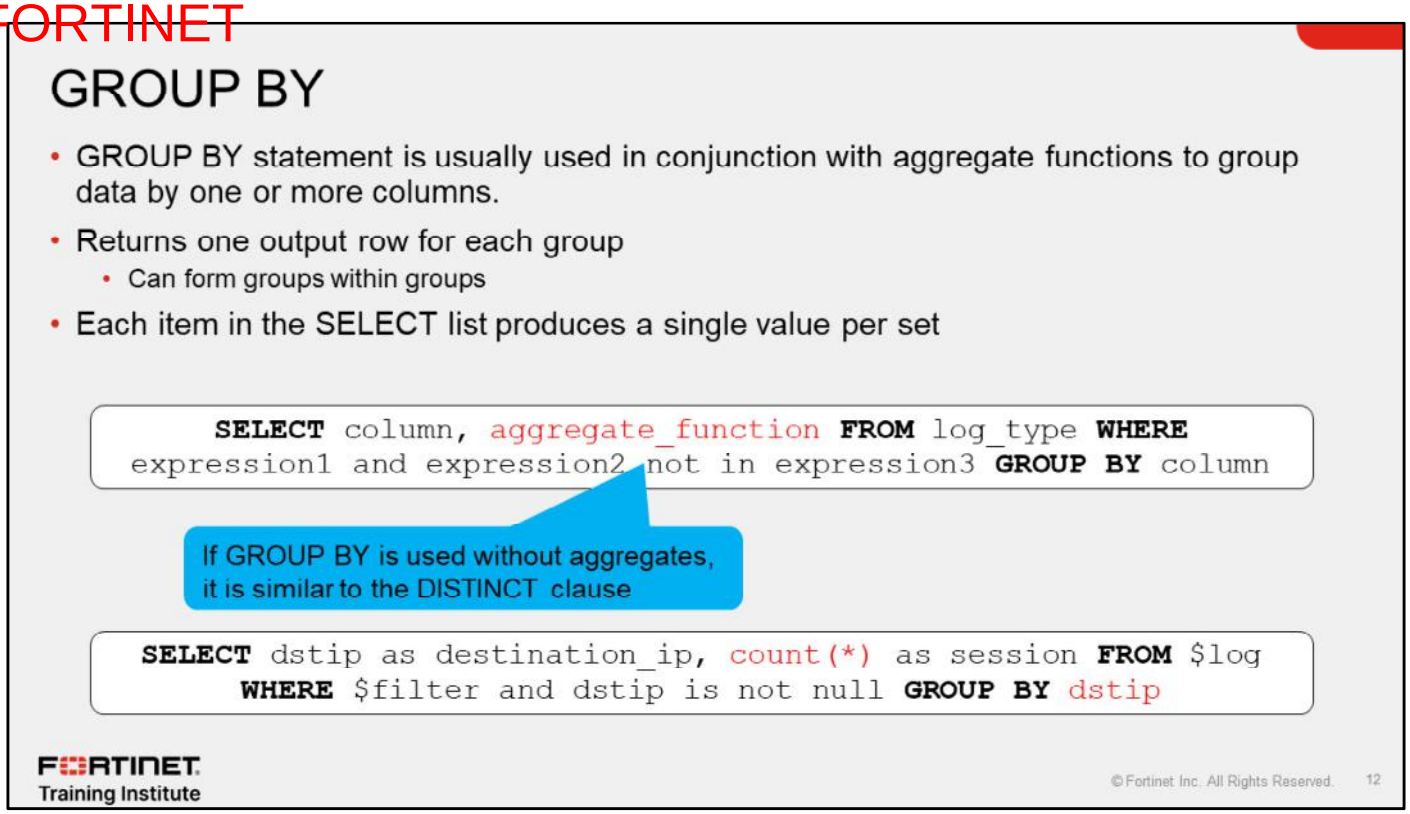
Out of all the optional clauses, the WHERE statement is really the heart of the query, because this is where you specify the criteria.

The WHERE statement must always come after the FROM statement.

In this example, the first expression is `$filter`, which is used to restrict the results to the time period you select. While the time period is not added to the query itself, it is specified by way of a drop-down box when creating the dataset through the FortiAnalyzer GUI.

The second expression is `dstip`, which is the destination IP, while the third expression is NULL.

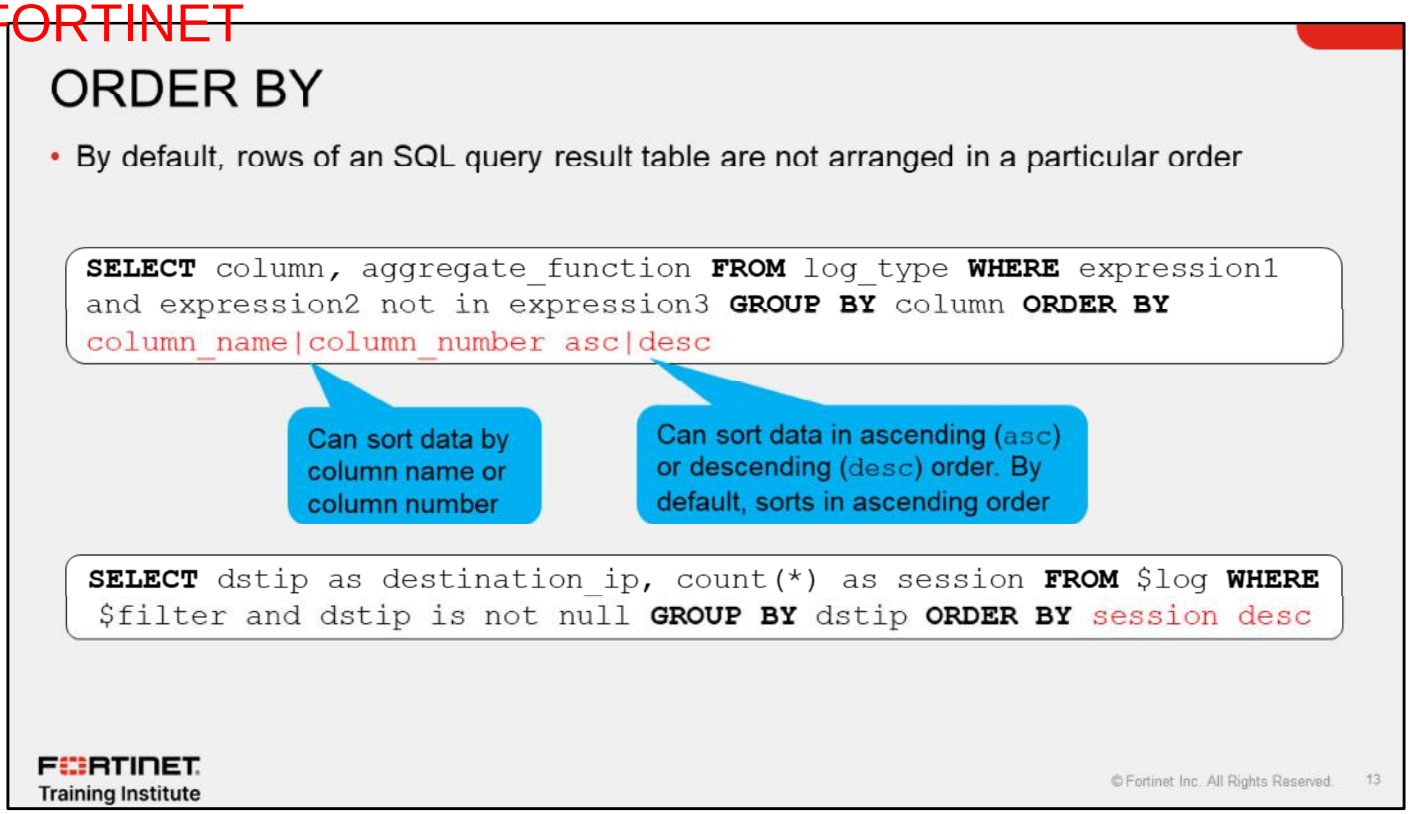
SQL supports logic operators as well, so you can use AND/OR/NOT statements in order to build out the query. Operators are also covered in this material.



The GROUP BY clause is used to create one output row for each group. It is usually used with an aggregate function within the SELECT statement. We will cover aggregate functions later, but essentially they perform a calculation on a set of values and return a single value. If it is not used with an aggregate function, it is similar to the DISTINCT clause, in that it removes duplicates from the result set of a SELECT statement.

In this example, the GROUP BY clause is use with an aggregate function. The aggregate function is `count(*)`, which selects all rows in a table, even if some columns contain a NULL value.

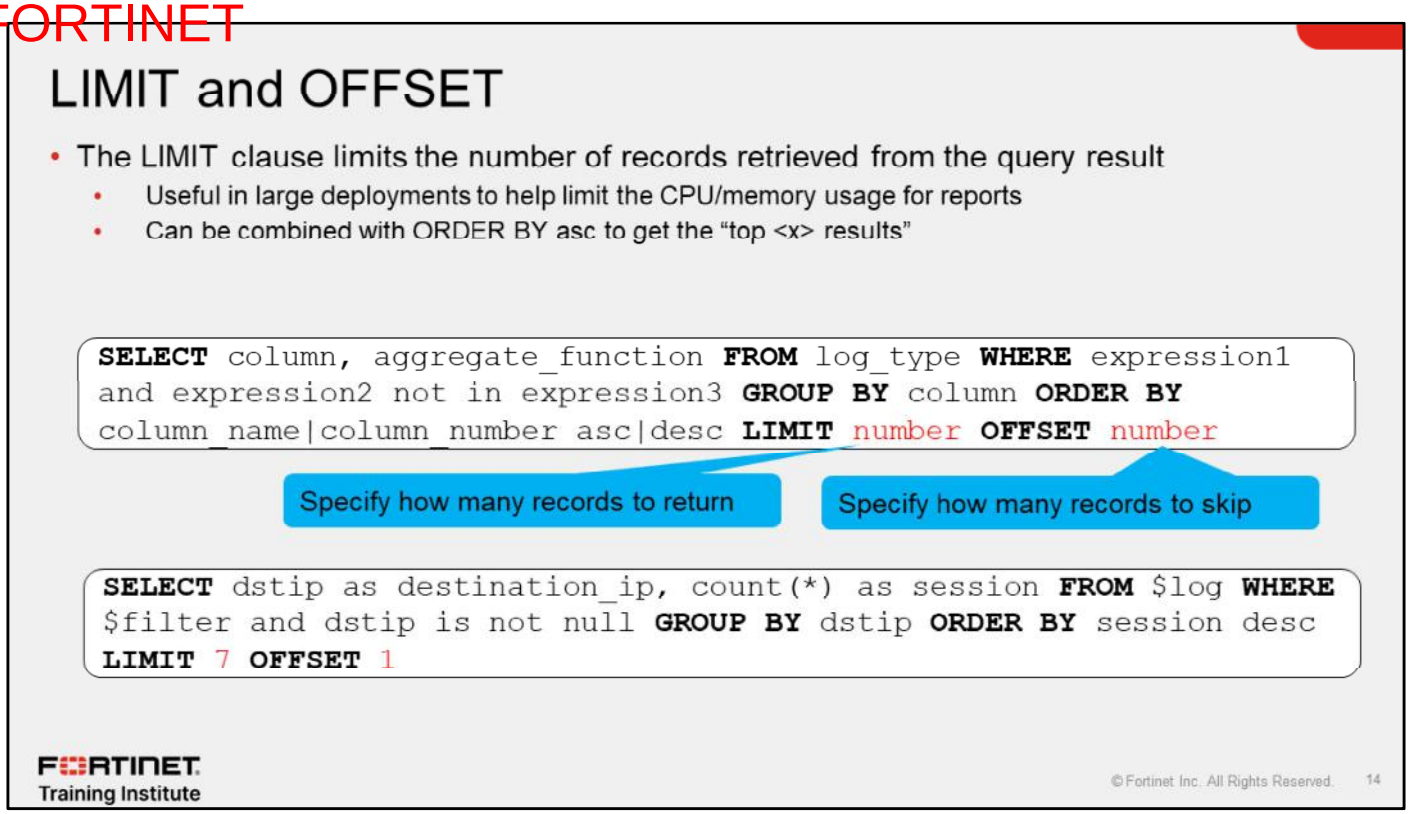
In this example, we are grouping by `dstip` (destination IP).



ORDER BY is a clause that allows you to sort queries by column name or column number. By default, rows of an SQL query result table are not arranged in a particular order, so you can use the ORDER BY clause to sort column values in either ascending (`asc`) or descending (`desc`) order. If you use this clause and do not specify ascending or descending, the default is ascending.

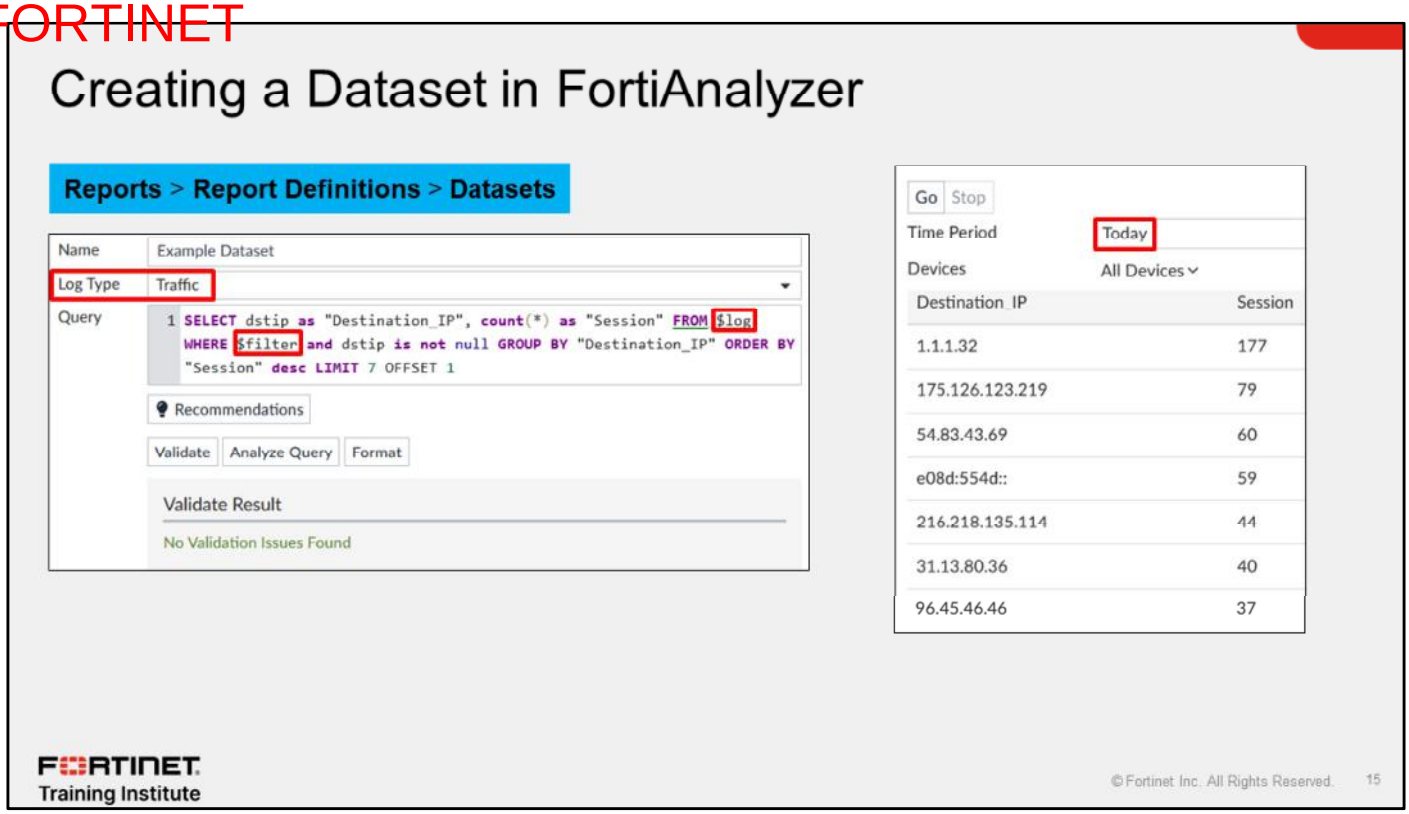
You can order multiple columns and specify different sort orders for each. For example, you can sort one column in ascending order and another column in descending order.

In this example, we are ordering by session in descending order.



By default, all results that satisfy the conditions specified in the query are returned. However, if you want to retrieve only a subset of records, you can place a limit on the number of records returned. To do this, use the LIMIT clause and specify the number of results you want. For example, `LIMIT 7`. Applying limits can ensure that the query doesn't use unnecessary CPU or memory, especially if you have a large-scale deployment with lots of devices logging to FortiAnalyzer. You can also combine LIMIT with ORDER BY asc to get the "top <x> results" (or desc for the "bottom <x> results").

In conjunction with the LIMIT clause, you can use the OFFSET clause. This offsets the results by a set value. For example, if you place a limit of seven records and an offset of one, the first record that would normally be returned is skipped and two through eight are returned instead.

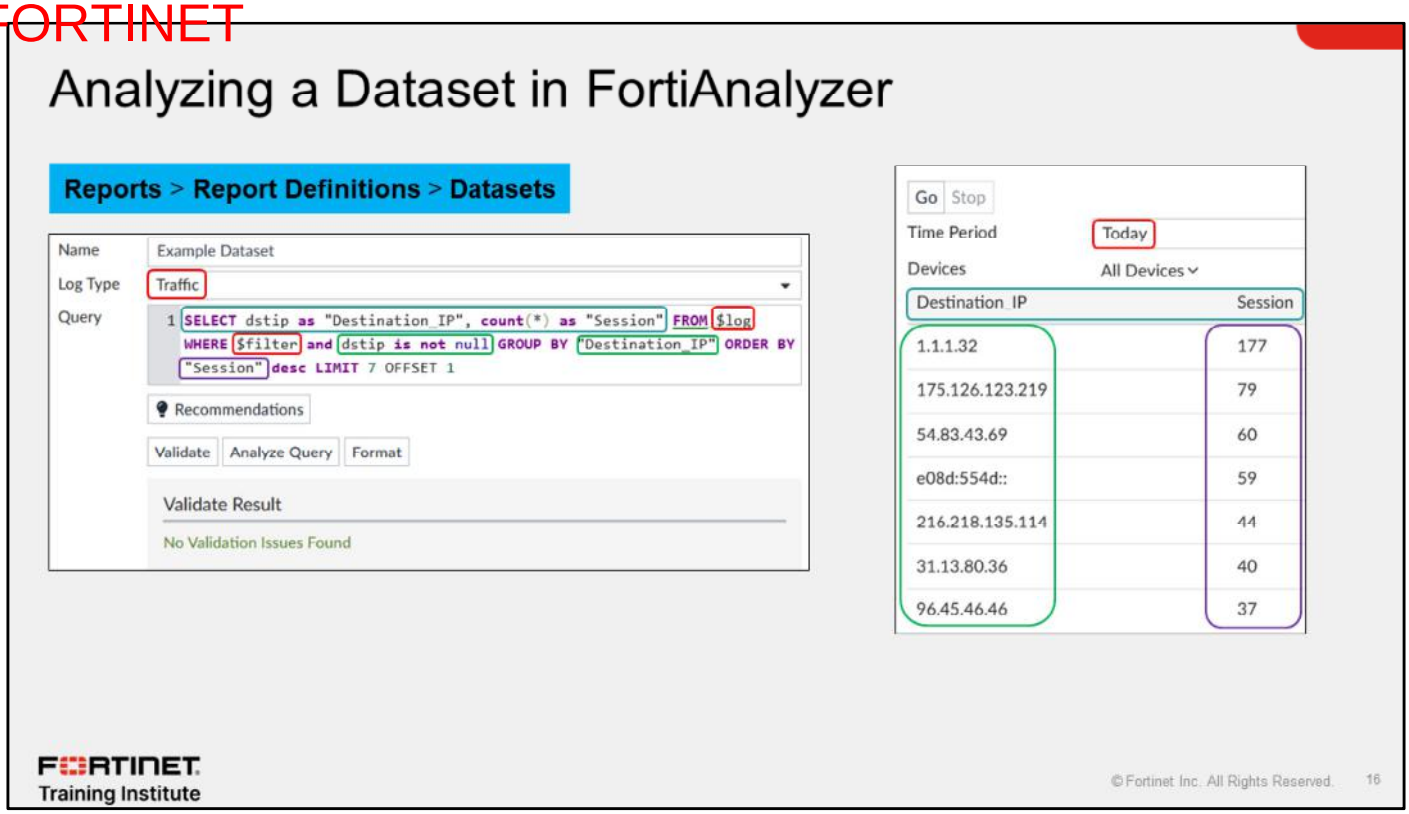


As you have been learning about the main SQL clauses, you have also been forming a full dataset query along the way. To see a visual of the query, you can use the dataset **Go** feature in the GUI. The feature is intended to test or modify a query in order to get the specific output you want.

Ensure you select the log type for the query. The query uses the generic `$log`, but it references the log type specified in the **Log Type** field (in this example, **Traffic**). You can enter the specific log type in the query instead (for example, `$log-traffic`). If you want to view this query on a different log type later, it's less risky and easier to change your selection in the **Log Type** field than in the actual dataset query itself.

You must also specify the device or devices on which to use this query. In this example, **All Devices** is specified.

You must also specify a time period for this query. You can use the `$filter` expression with the WHERE clause to limit the results to the time period that you specify in the **Time Period** field.



Now align the written query with the visual results to fully understand how the query is interpreted by FortiAnalyzer.

`SELECT dstip as "Destination_IP", count(*) as "Session"`: This says, select the destination IP address and call the column "`Destination_IP`". Select the count (all data) and call the column "`Session`".

`FROM $log`: This says, query the traffic log for the data, which is specified in the **Log Type** field.

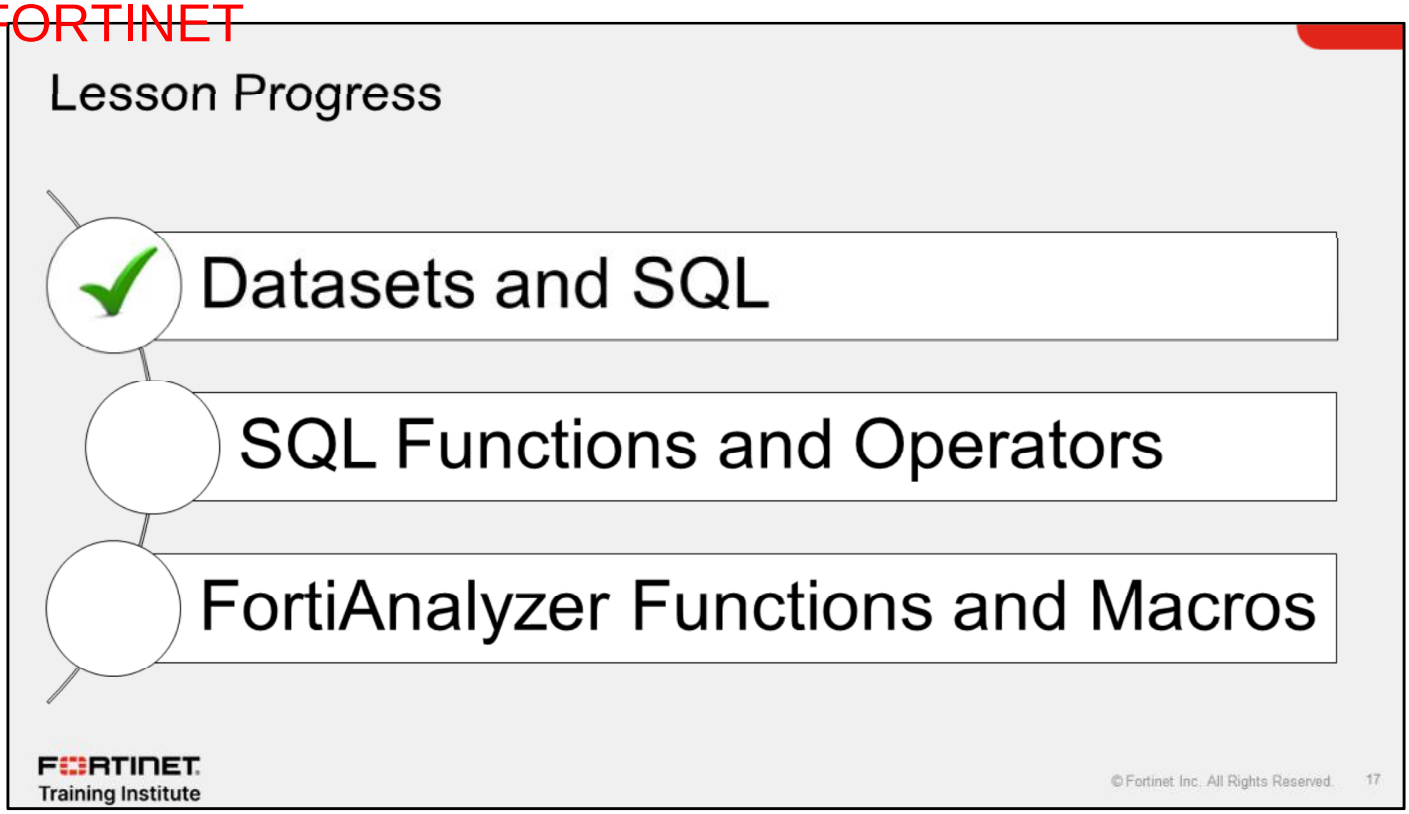
`WHERE $filter and dstip is not null`: This says, limit the results to the time period specified, which is **Today**, according to the selection in the **Time Period** field, and provide only the destination IP addresses that are not null. Note that "null" represents unknown data—it does not represent zero.

`GROUP BY dstip`: This says, group the results by destination IP. You previously specified that the destination IP should be put in a column called "`Destination_IP`".

`ORDER BY session desc`: This says, order the results by session in descending order. Note that the results go from high (177) to low (37).

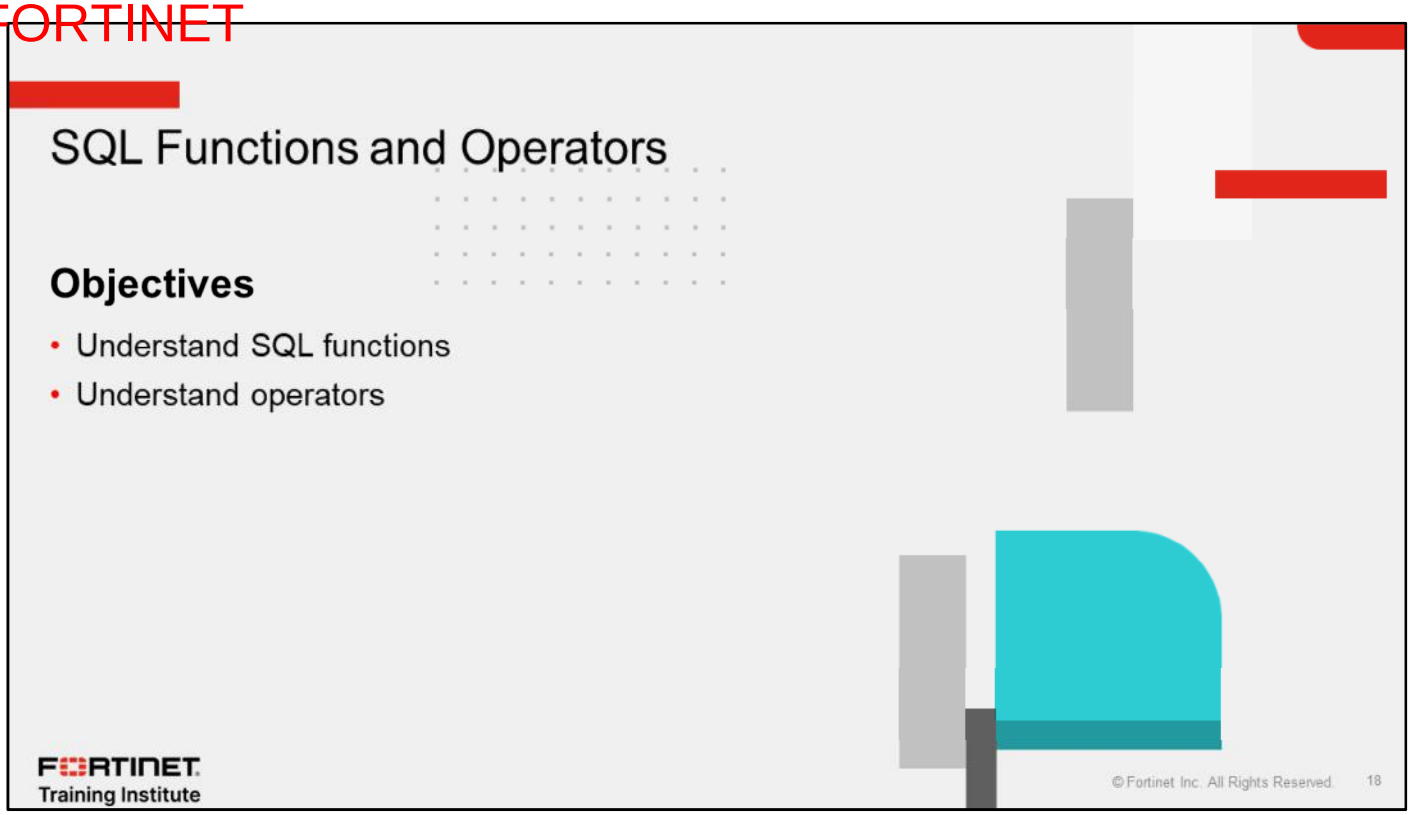
`LIMIT 7`: This says, provide only the first seven results.

`OFFSET 1`: This says, skip the first result, but still limit the results to the next seven (that is, two through eight).

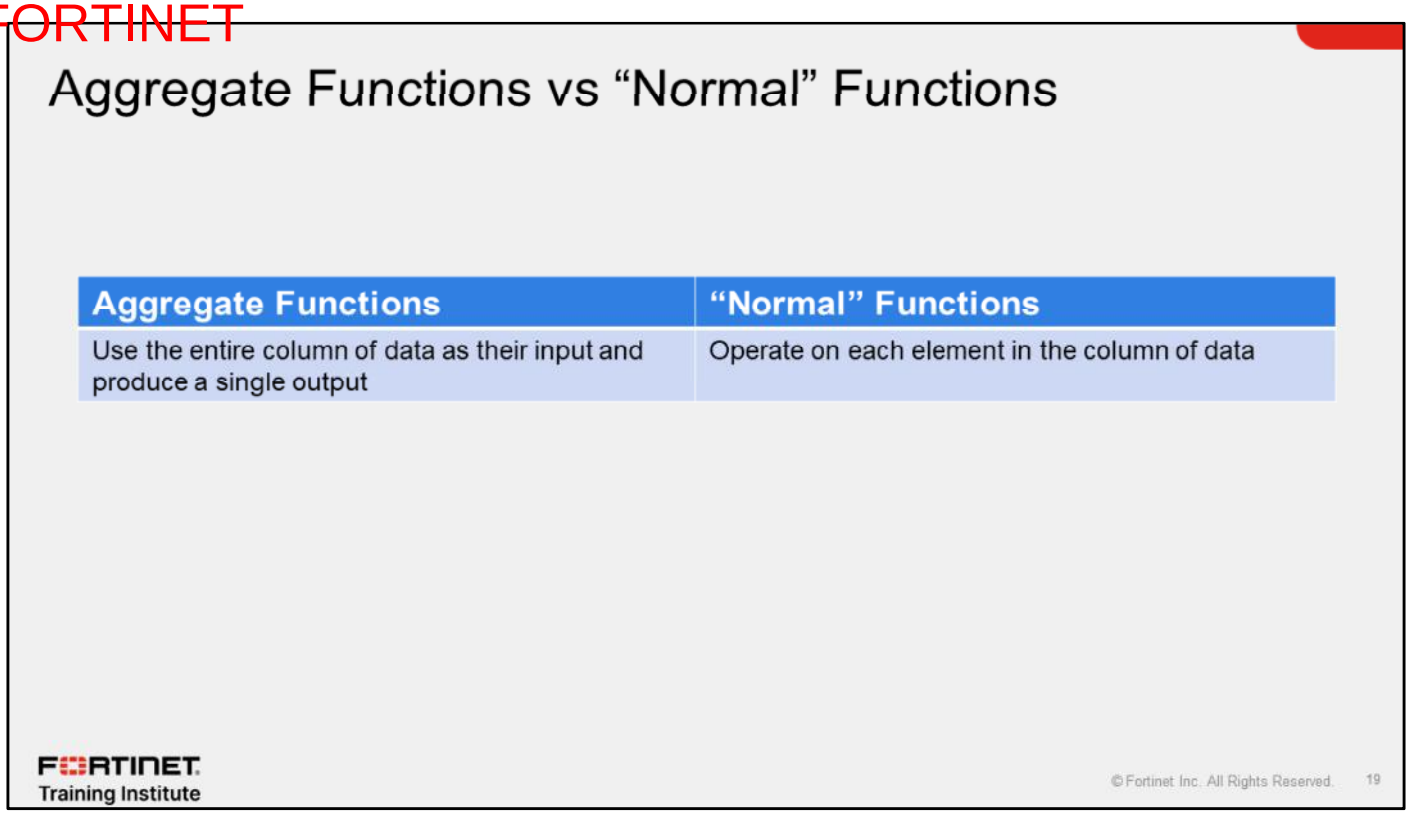


Good job! You now understand datasets and SQL.

Now, you will learn about SQL functions and operators.

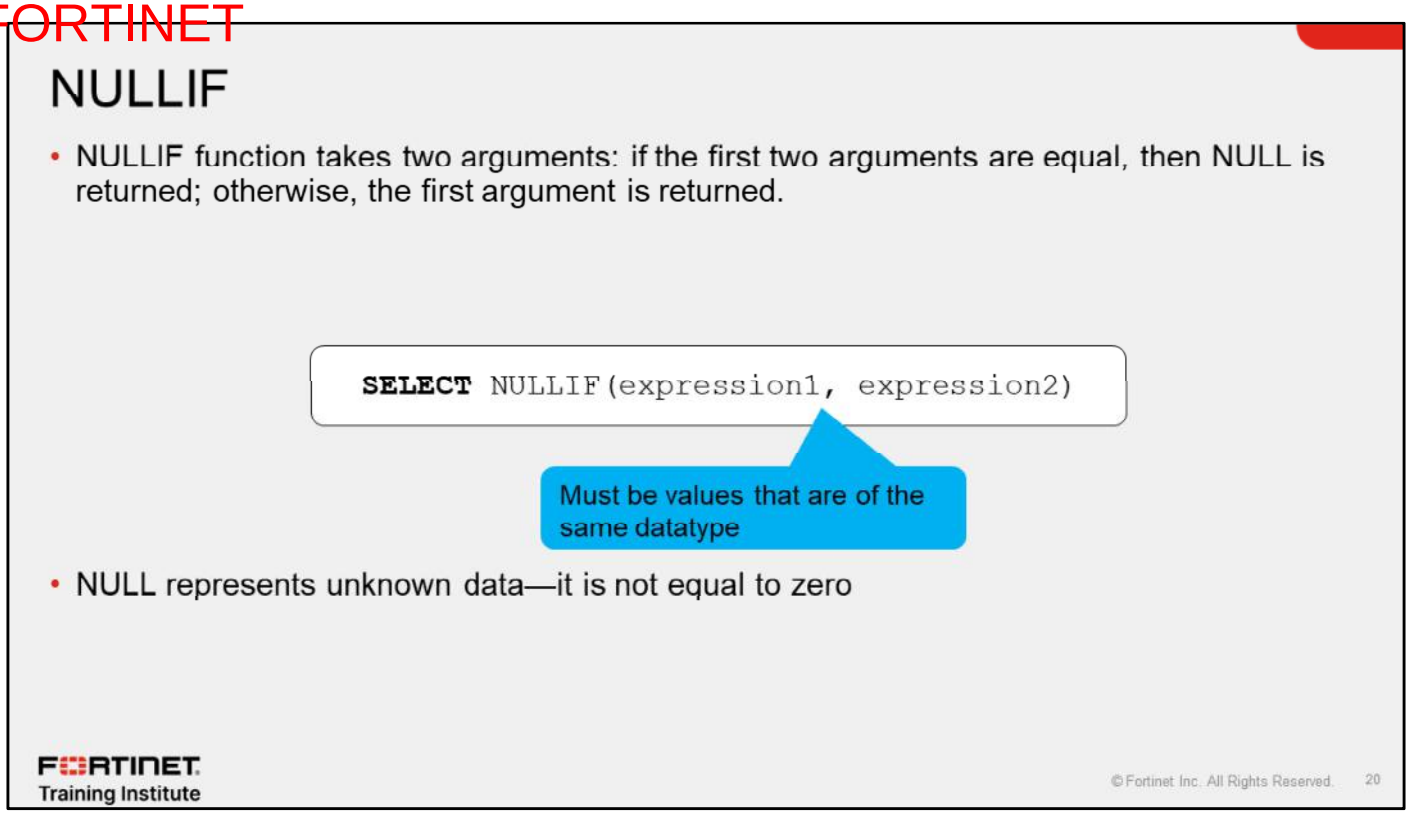


This section covers a few of the most common functions and operators used in FortiAnalyzer datasets—it is not intended as a complete and exhaustive list.

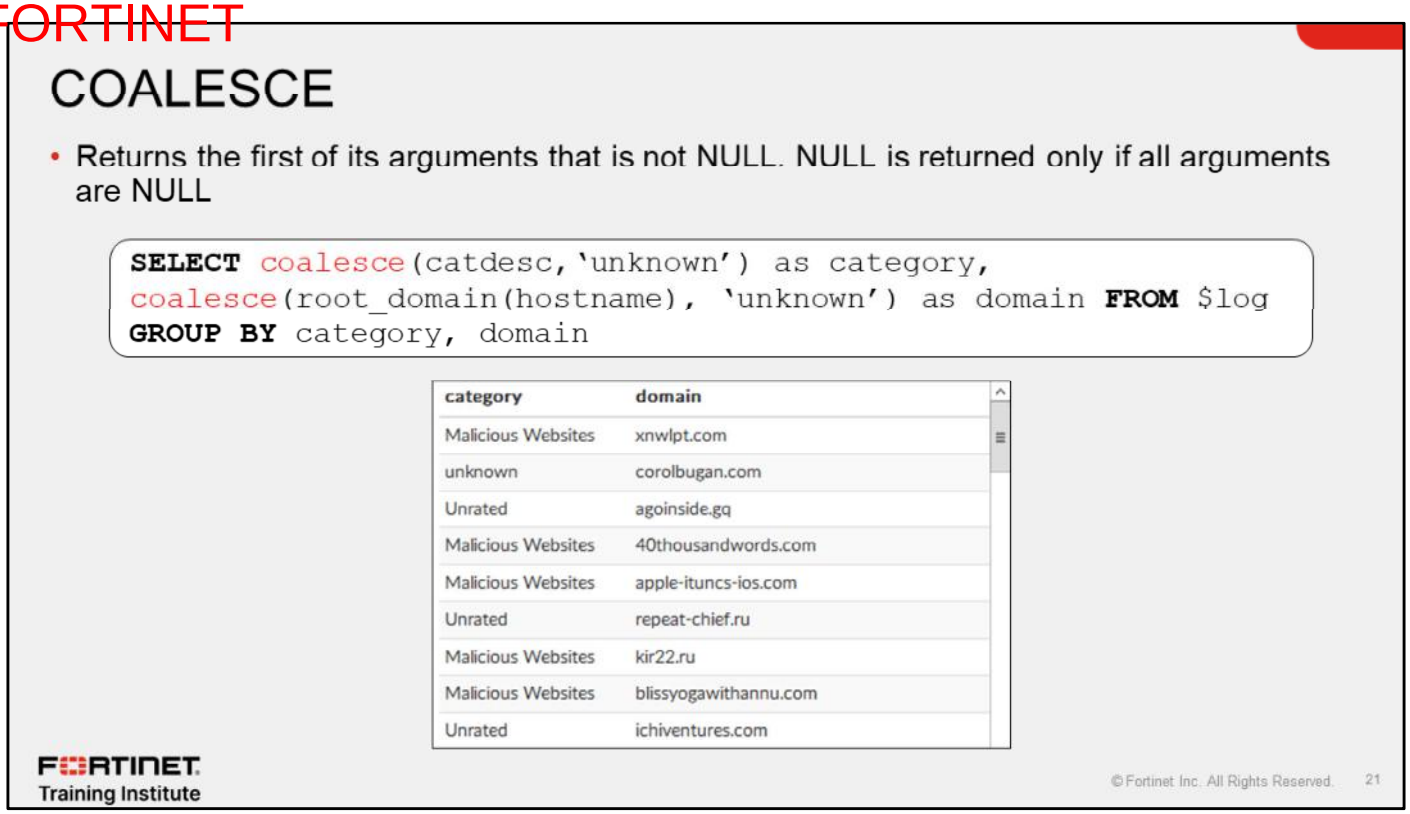


SQL has two types of functions: aggregate functions and “normal” functions.

Aggregate functions use the entire column of data as their input and produce a single output. “Normal” functions operate on each element in the column of data.



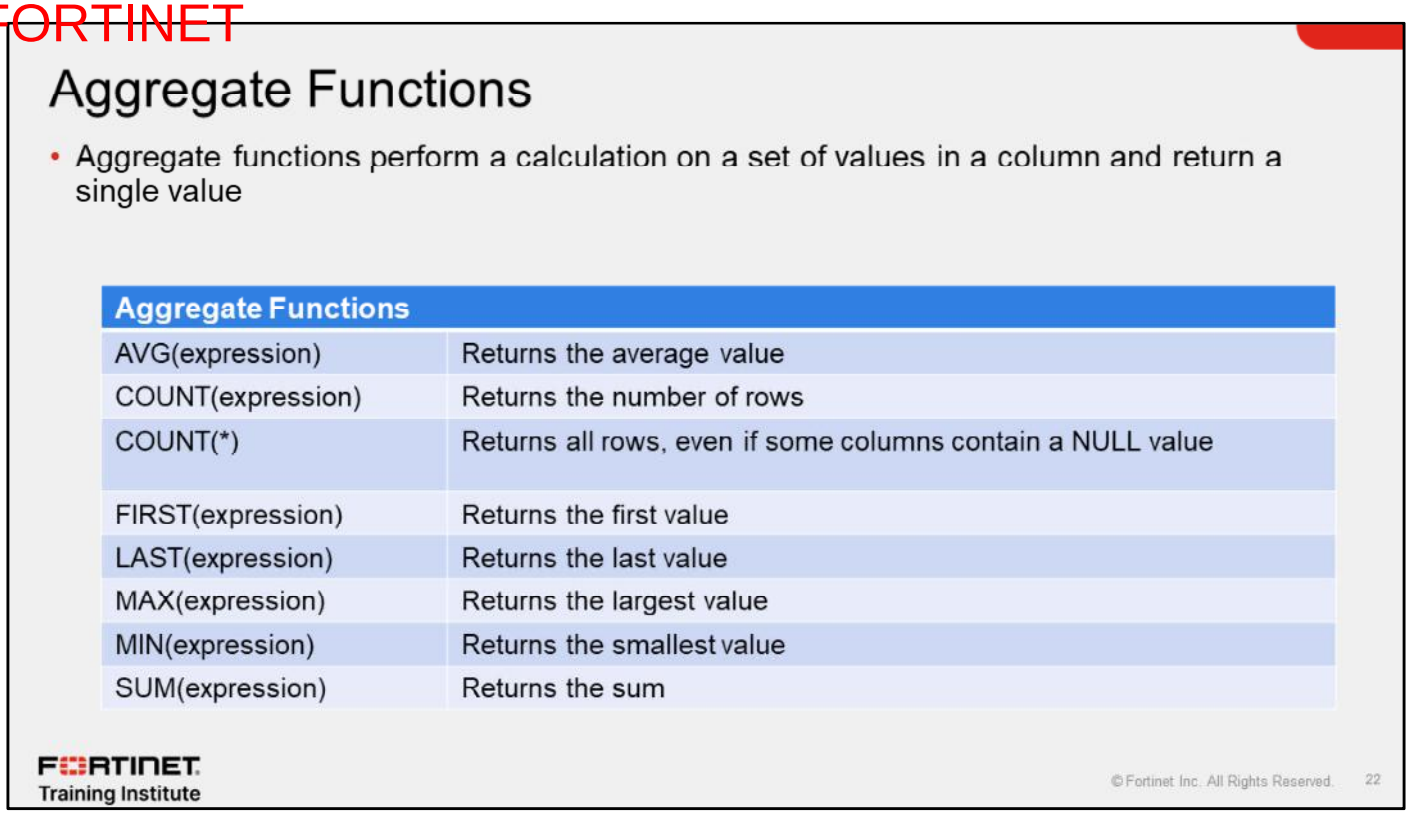
One common function used in FortiAnalyzer datasets is NULLIF. The NULLIF function takes two arguments. If the first two arguments are equal, then NULL is returned; otherwise, the first argument is returned. Note that NULL represents unknown data—it does not represent zero.



Another common function used in FortiAnalyzer datasets is COALSECE. The COALESCE function returns the first non-NULL expression among its arguments. Null is returned only if all arguments are null. It is often used to substitute a default value for null values when data is retrieved for display.

COALESCE is used with the SELECT statement. It takes one or more expressions as an argument. The values do not have to be string data types—they can be any data type (and also different data types). The syntax is:

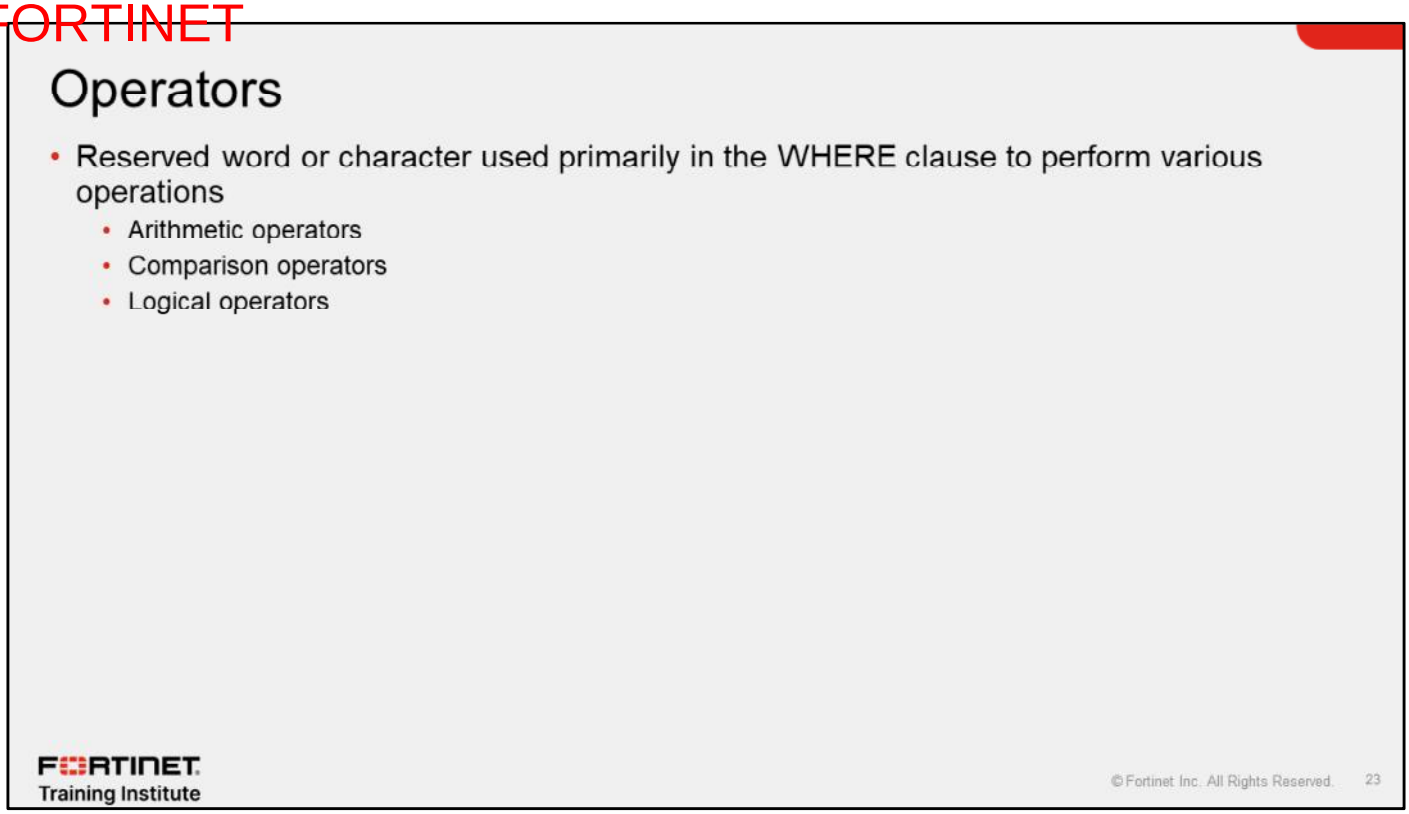
```
COALESCE (expression 1, expression 2, …)
```



Aggregate functions are a special category with different rules, as they operate on entire columns of data instead of discrete values. These functions perform a calculation on a set of values in a column and returns a single value. Although aggregate functions are usually used in conjunction with the GROUP BY clause, these functions can be used on their own in a SELECT statement.

This table includes a list of aggregate functions used in SQL. All can take an expression as an argument and ignore null values, except for count. Count can take an asterisk as an argument. The asterisk in this case means all rows are returned, even if some columns contain a NULL value.

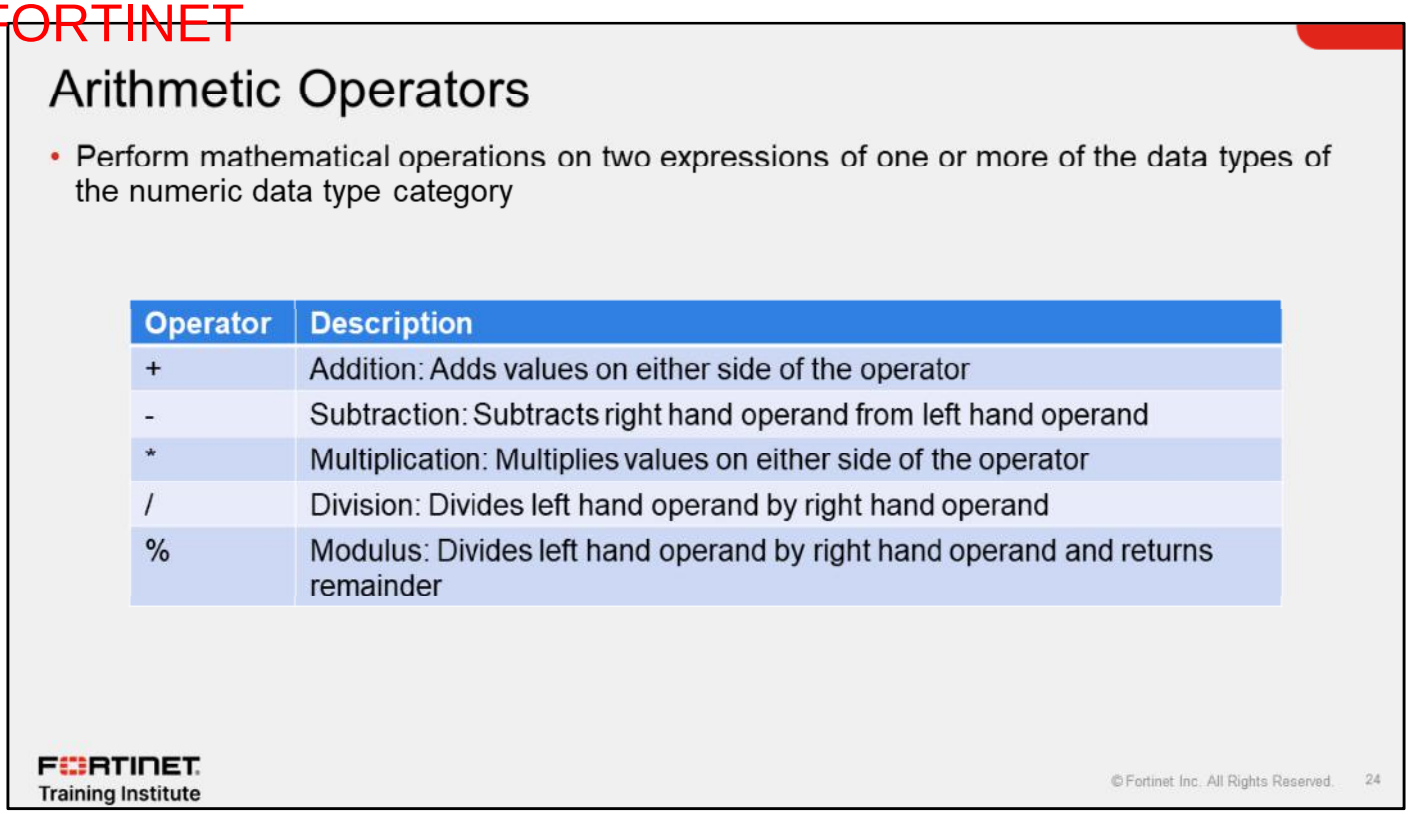
An example of an expression used with an aggregate function is `SELECT count(unauthuser)`. This returns the number of unauthorized users.



An operator is a reserved word or a character used primarily in an SQL statement's WHERE clause to perform various operations.

There are three types of operators:

- Arithmetic operators
- Comparison operators
- Logical operators



Here are some examples of arithmetic operators. Arithmetic operators perform mathematical operations on two expressions of one or more of the data types of the numeric data type category.

Comparison Operators

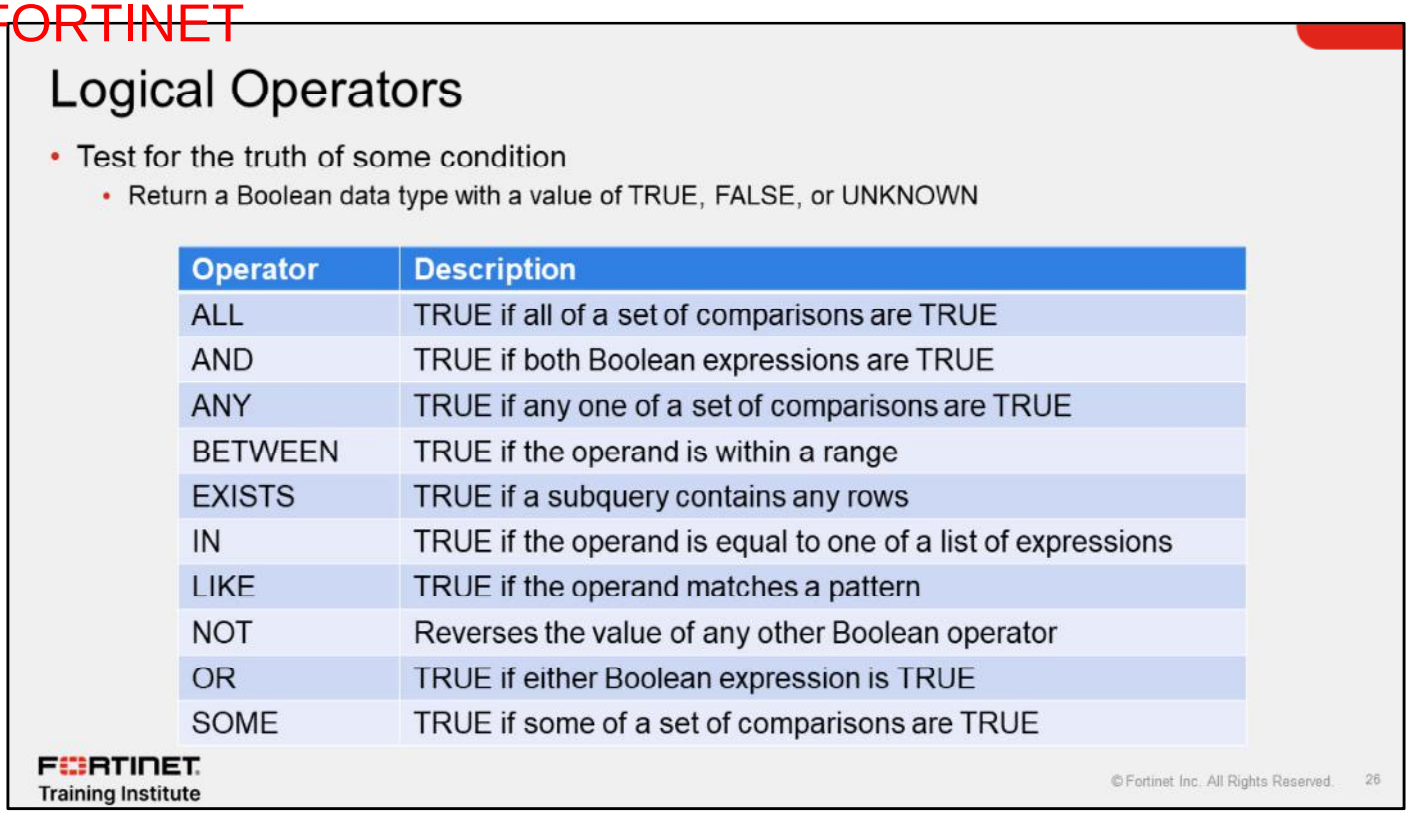
- Test whether two expressions are the same
  - Can be used on all expressions except text, ntext, or image data types

Operator	Description
=	Equal to
>	Greater than
<	Less than
>=	Greater than or equal to
<=	Less than or equal to
<>	Not equal to
!=	Not equal to (not ISO standard)
!<	Not less than (not ISO standard)
!>	Not greater than (not ISO standard)

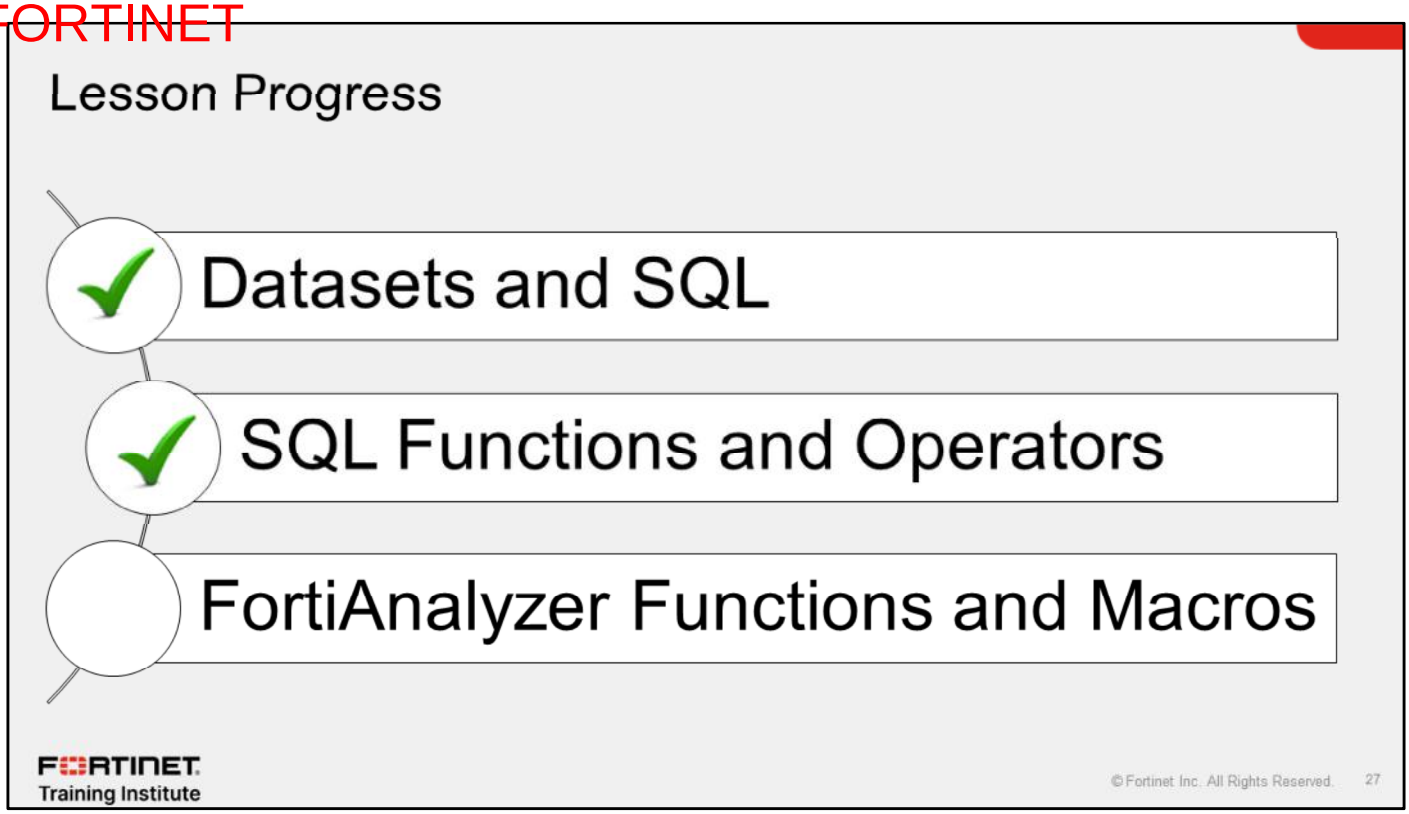
FORTINET Training Institute

 25

Here are some examples of comparison operators. Comparison operators test whether two expressions are the same and can be used on all expressions except expressions of the text, ntext, or image data types.

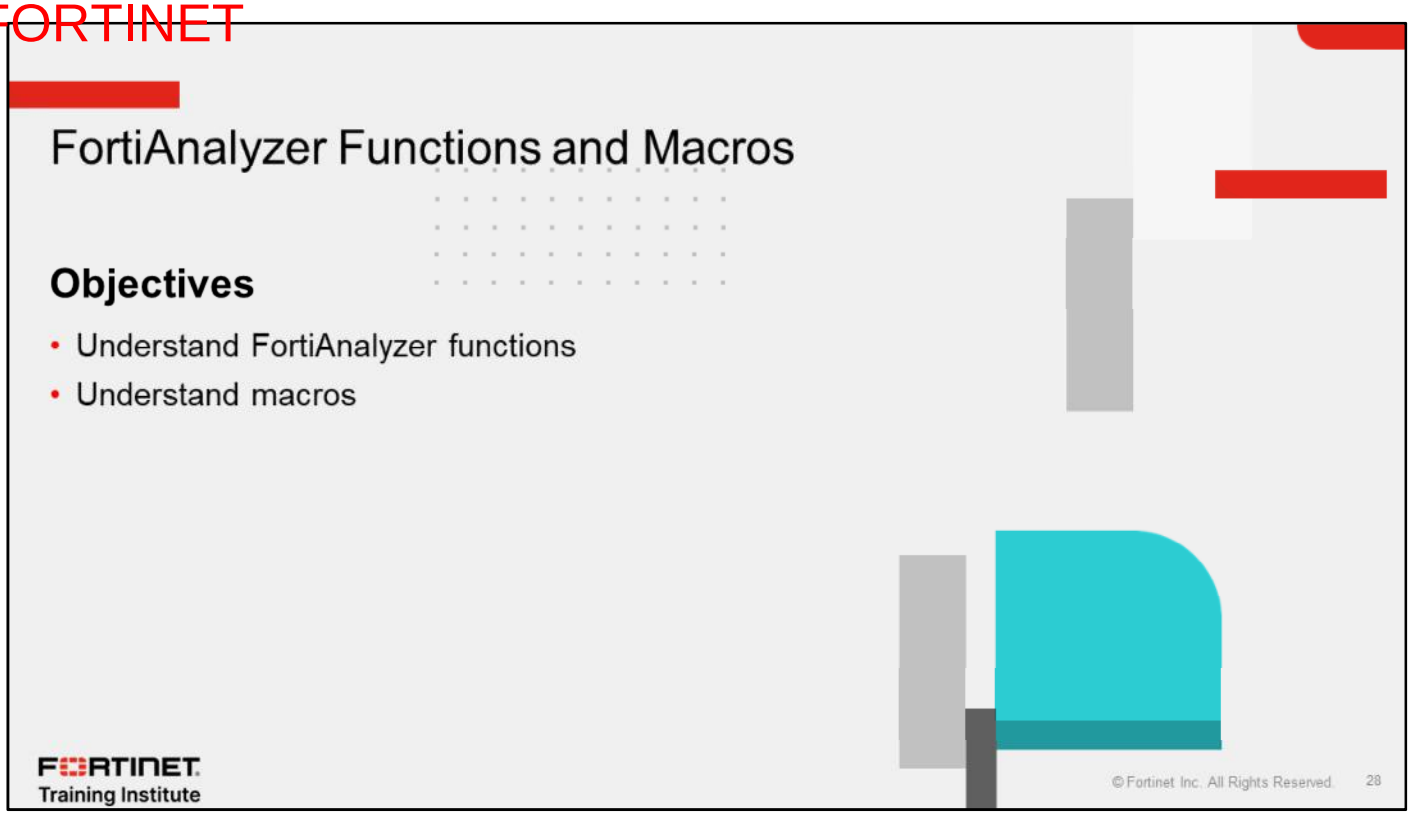


Here are some examples of logical operators. Logical operators test for the truth of a condition. Like comparison operators, they return a Boolean data type with a value of TRUE, FALSE, or UNKNOWN.



Good job! You now understand SQL functions and operators.

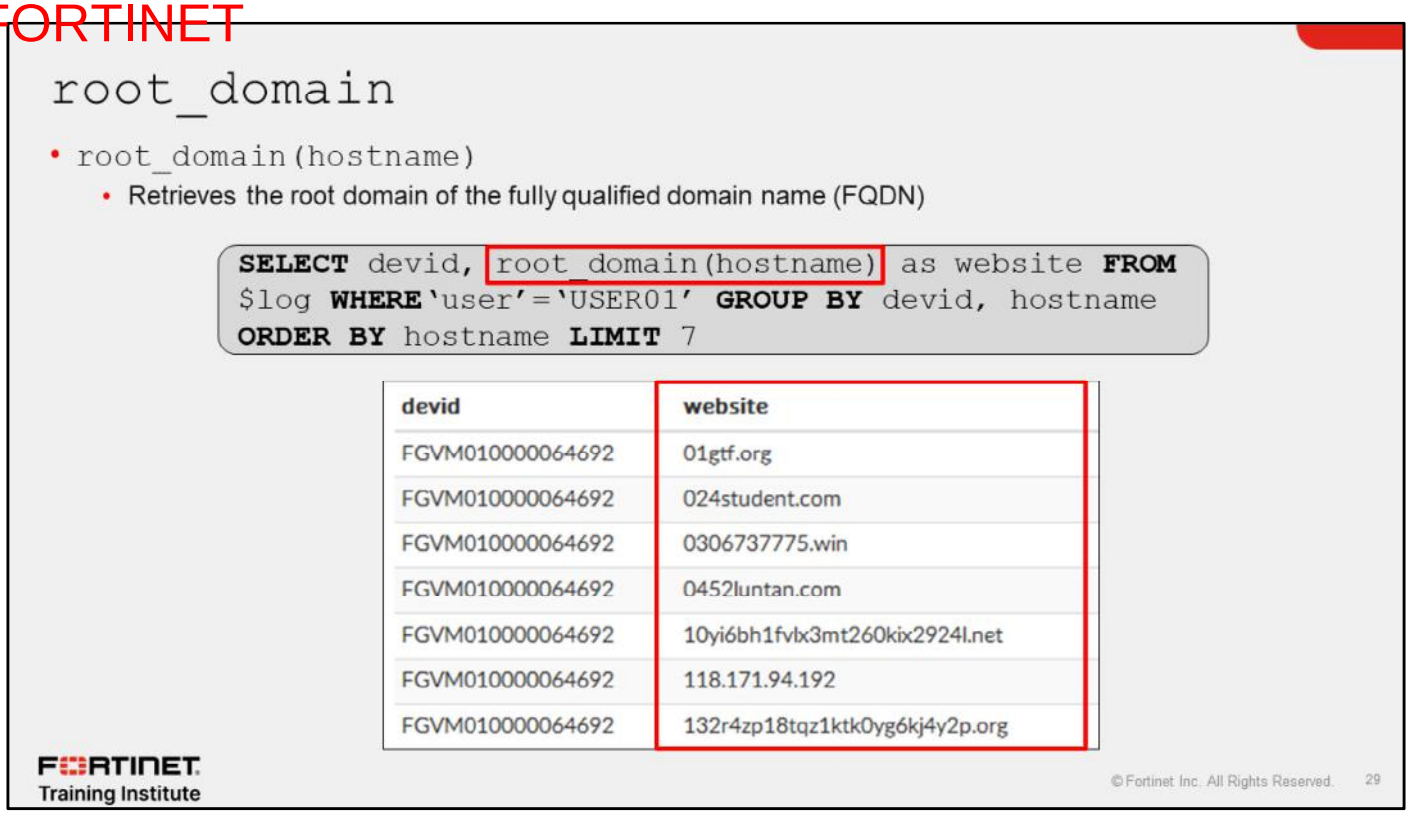
Now, you will learn about FortiAnalyzer functions and macros.



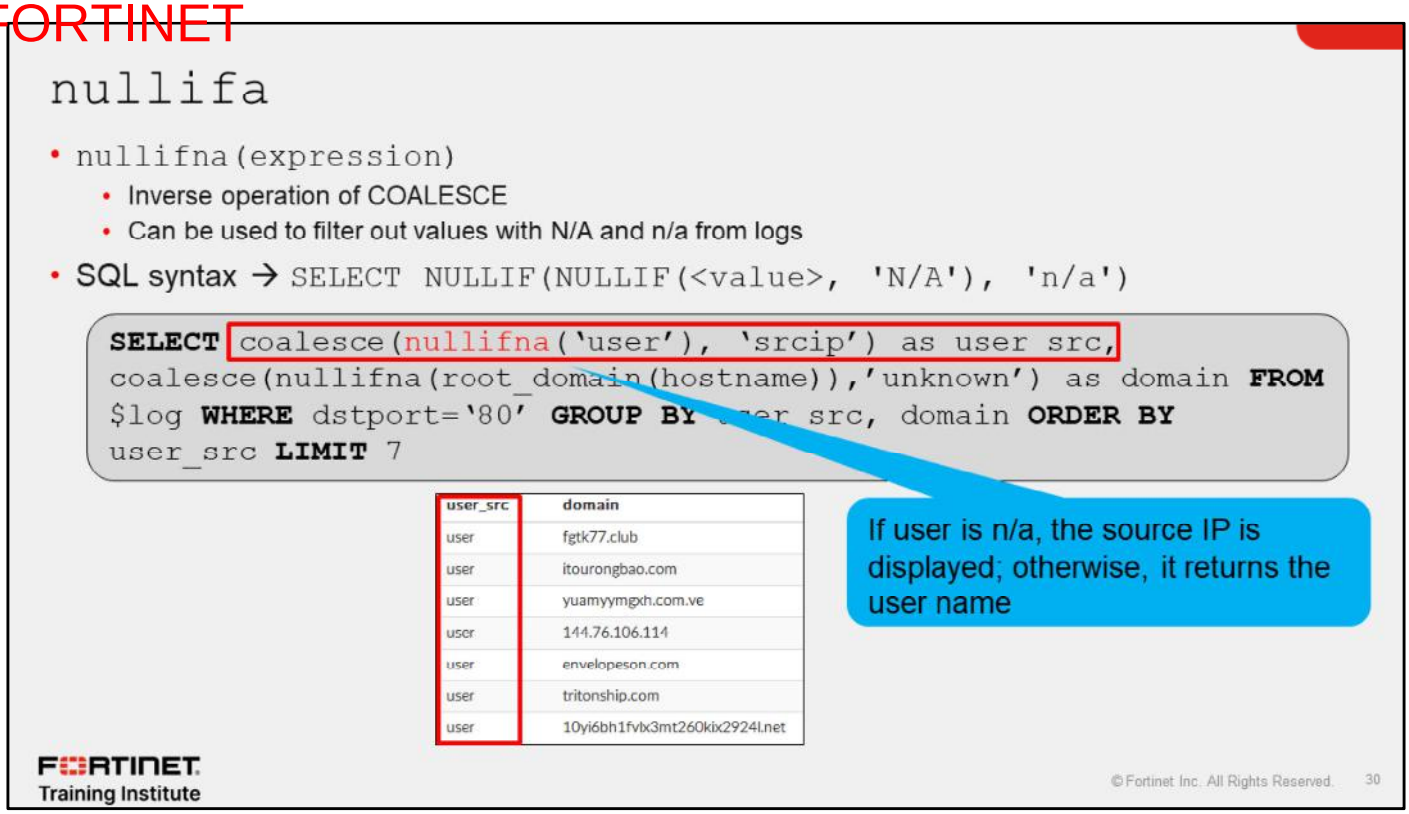
This section covers FortiAnalyzer functions and macros.

FortiAnalyzer includes some built-in functions that are based on known SQL functions, but scripted differently.

FortiAnalyzer also includes macros, which are best described as lengthy or complex SQL statements scripted more simplistically. An SQL macro can be used anywhere in a query where an ordinary SQL expression can be used.

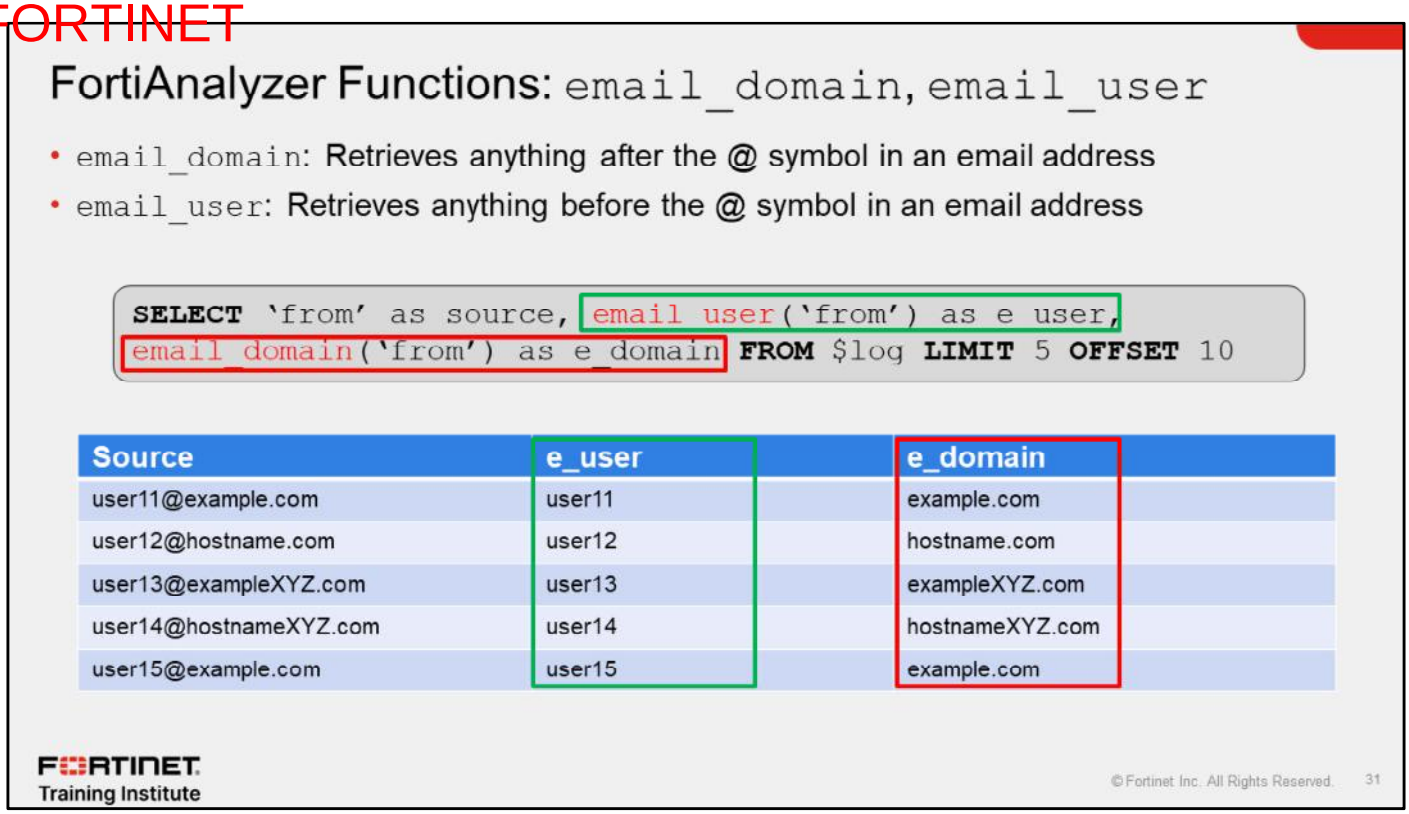


One FortiAnalyzer-specific function is `root_domain(hostname)`. This provides the root domain of the fully qualified domain name. As specified by the query, in this example `root_domain(hostname)` is listed under the **website** column in ascending order. Unless otherwise specified, ascending order is the default for the ORDER BY clause.



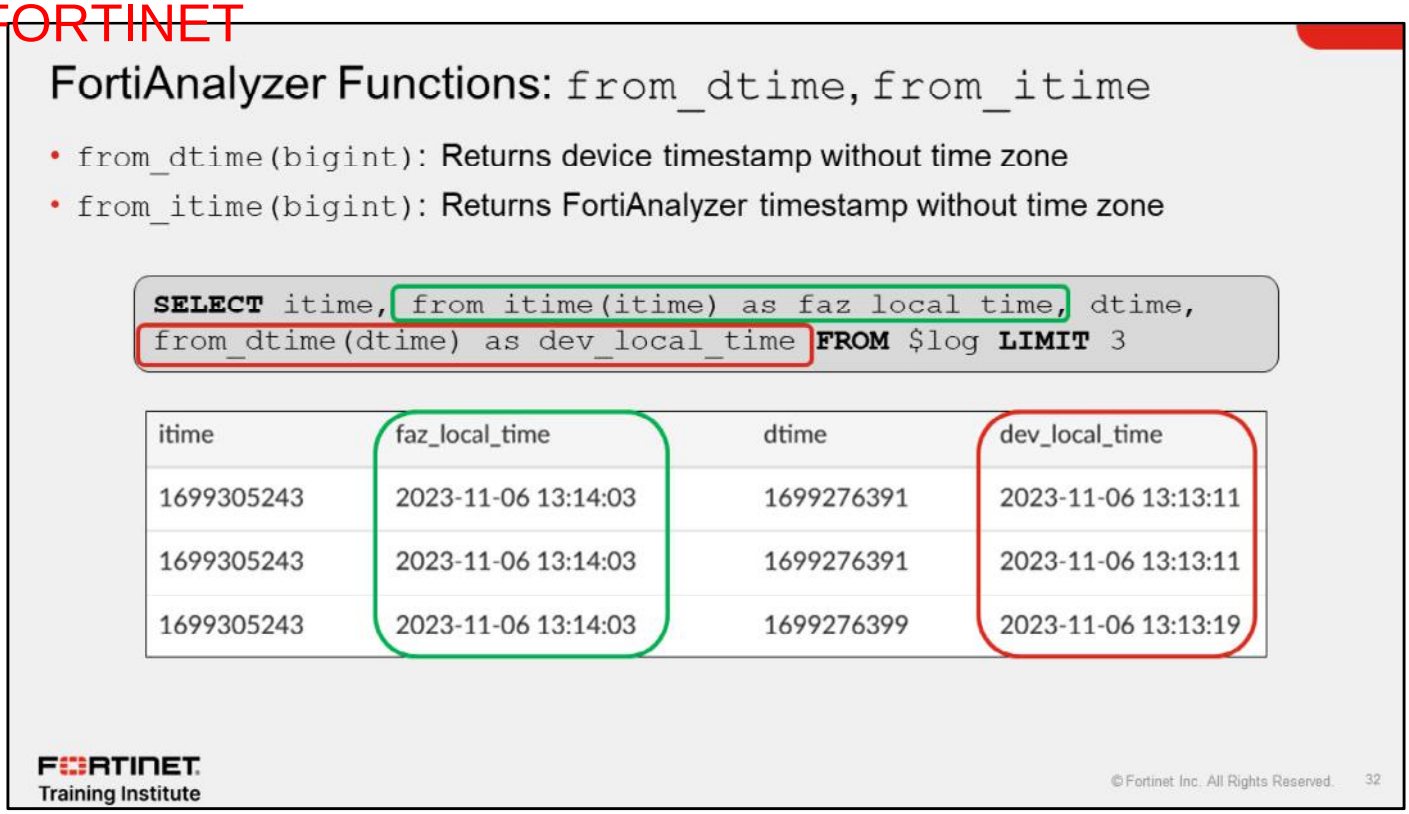
Another FortiAnalyzer-specific function is nullifna, which takes an expression as an argument. The actual SQL syntax this is based on is SELECT NULLIF(NULLIF(expression, 'N/A'), 'n/a').

In this example, if the user is n/a the source IP is displayed; otherwise, it returns the user name. It performs the inverse operation of the COALESCE function.



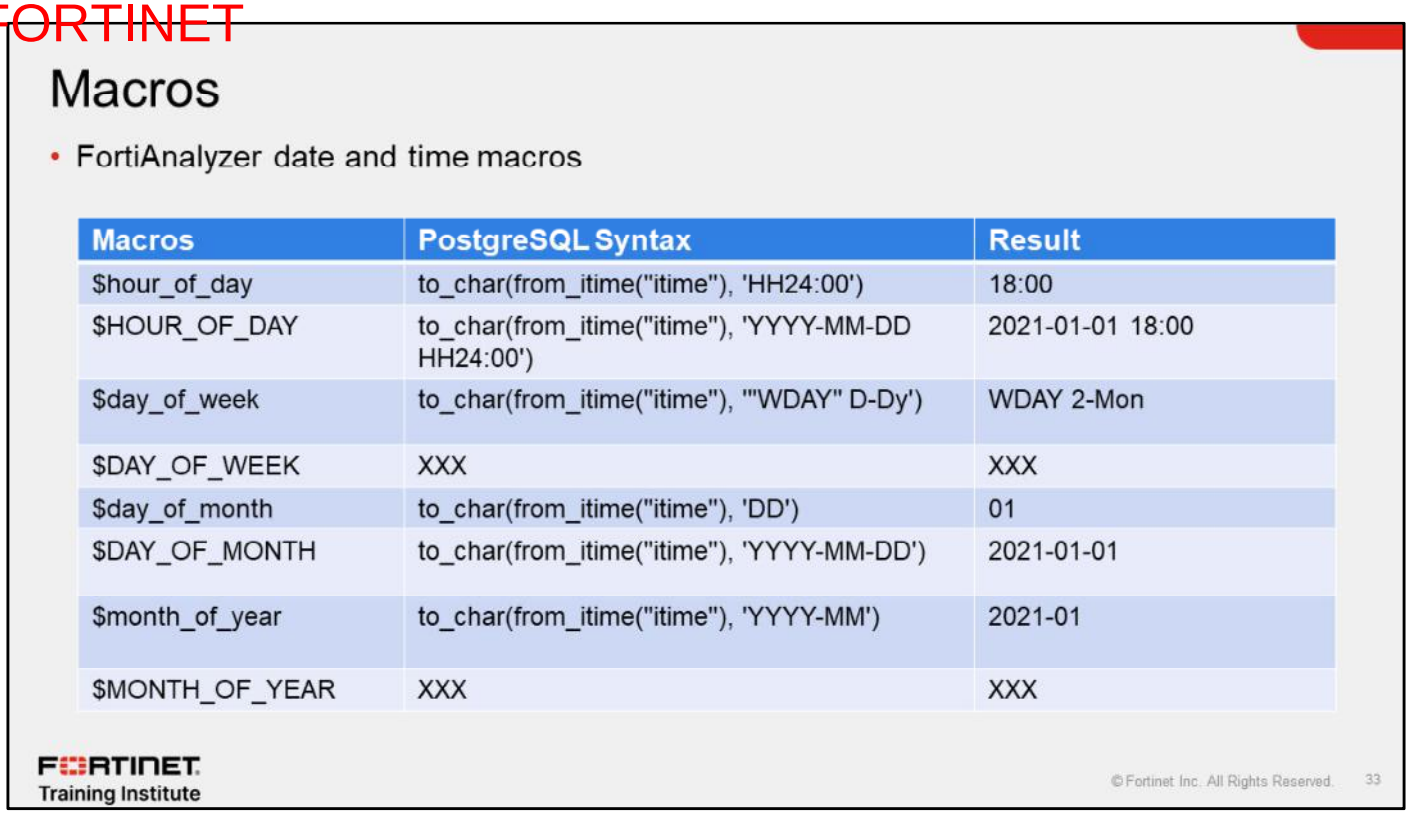
`email_domain` and `email_user` are other FortiAnalyzer-specific functions. `email_domain` retrieves anything that comes after the @ symbol in an email address—the domain. `email_user` retrieves anything that comes before the @ symbol in an email address.

As specified by the query, in this example `email_user` displays in the column **e_user**, while `email_domain` displays in the column **e_domain**.

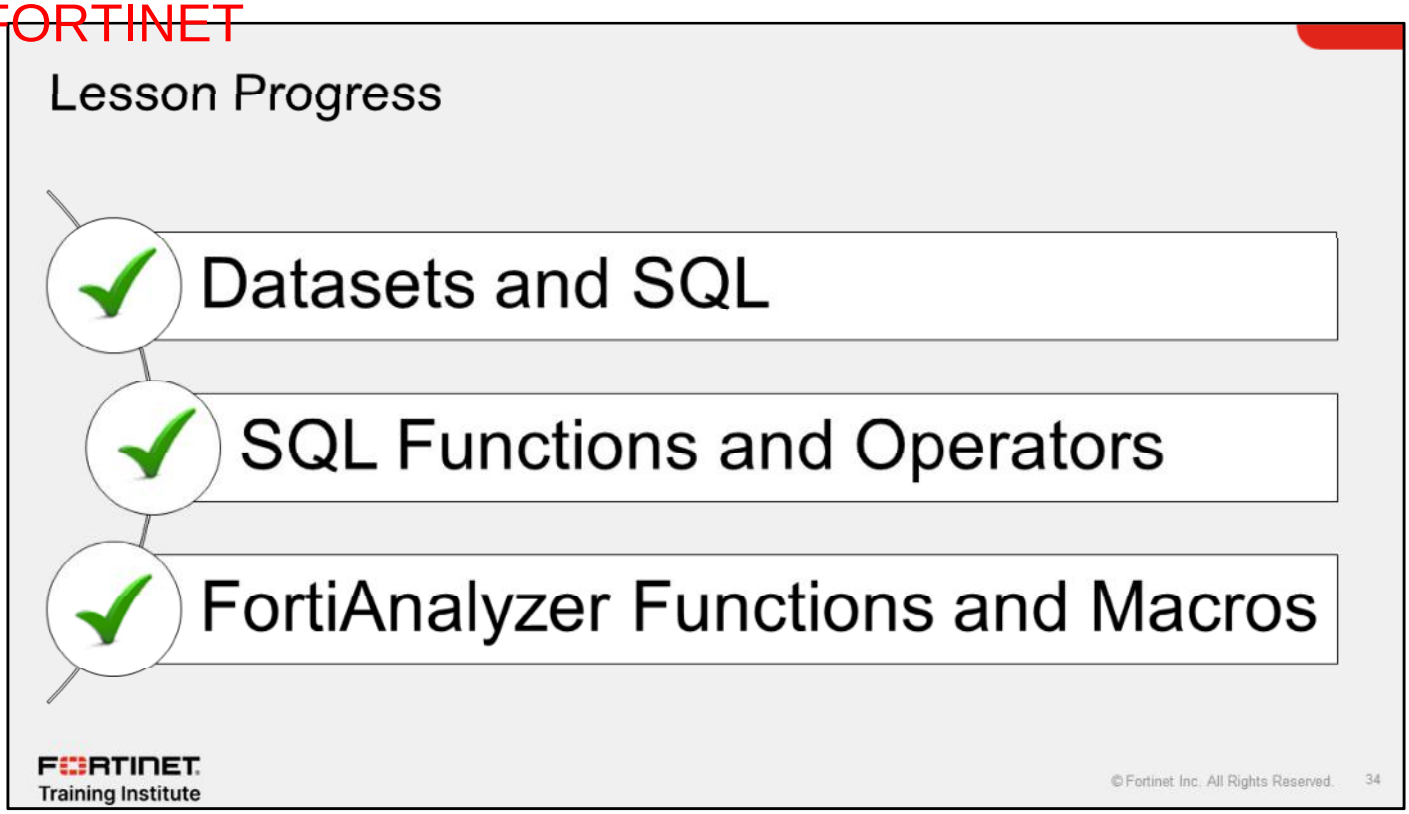


from_dtime and from_itime are other FortiAnalyzer-specific functions. from_dtime returns the device timestamp without the time zone, while from_itime returns the FortiAnalyzer's timestamp without the time zone.

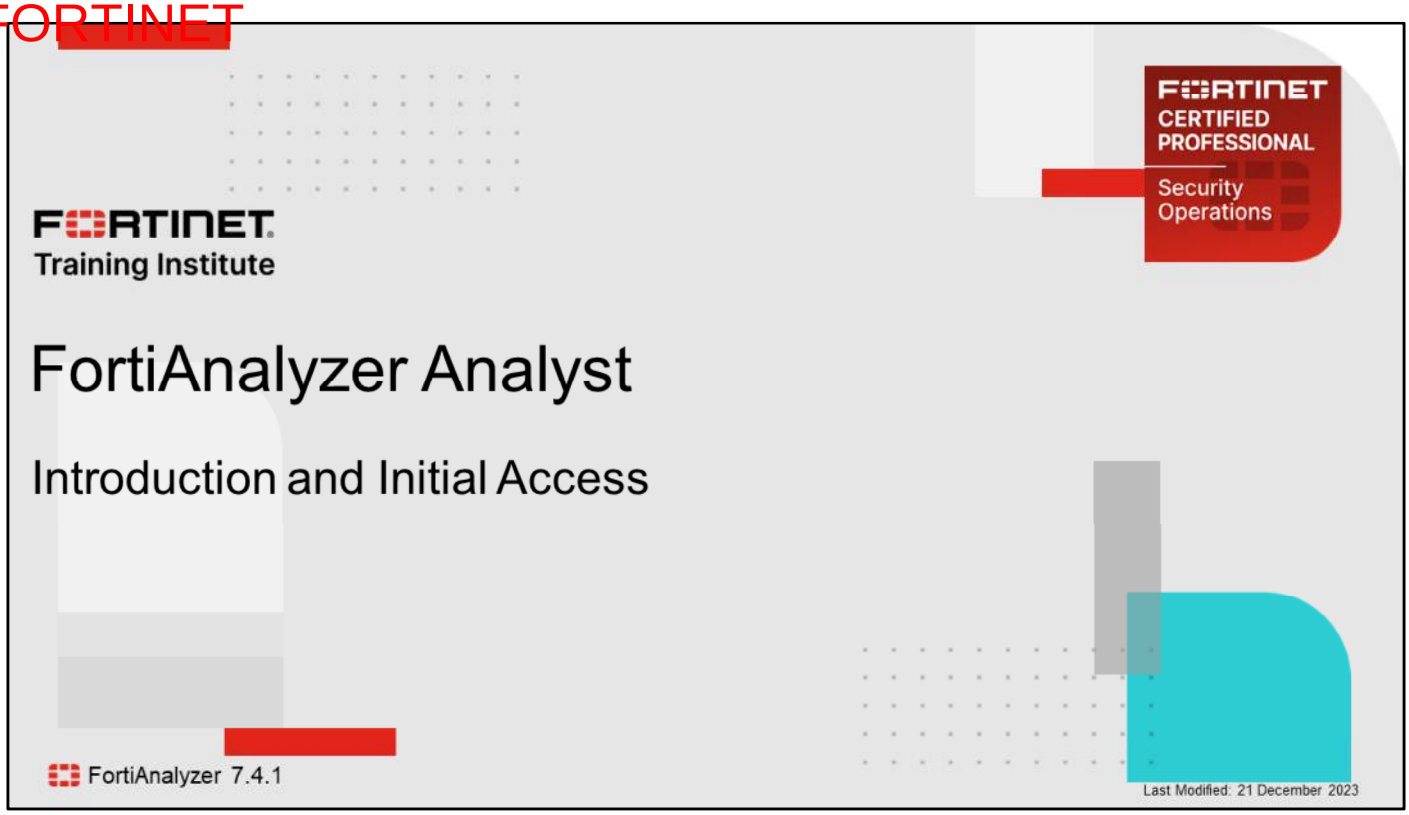
As specified by this query, from_itime appears in the column **faz_local_time**, while from_dtime appears in the column **dev_local_time**.



Here are some common date and time macros used in FortiAnalyzer. Macros are simple substitutions for more complex SQL statements—usually created for SQL statements that are frequently used.

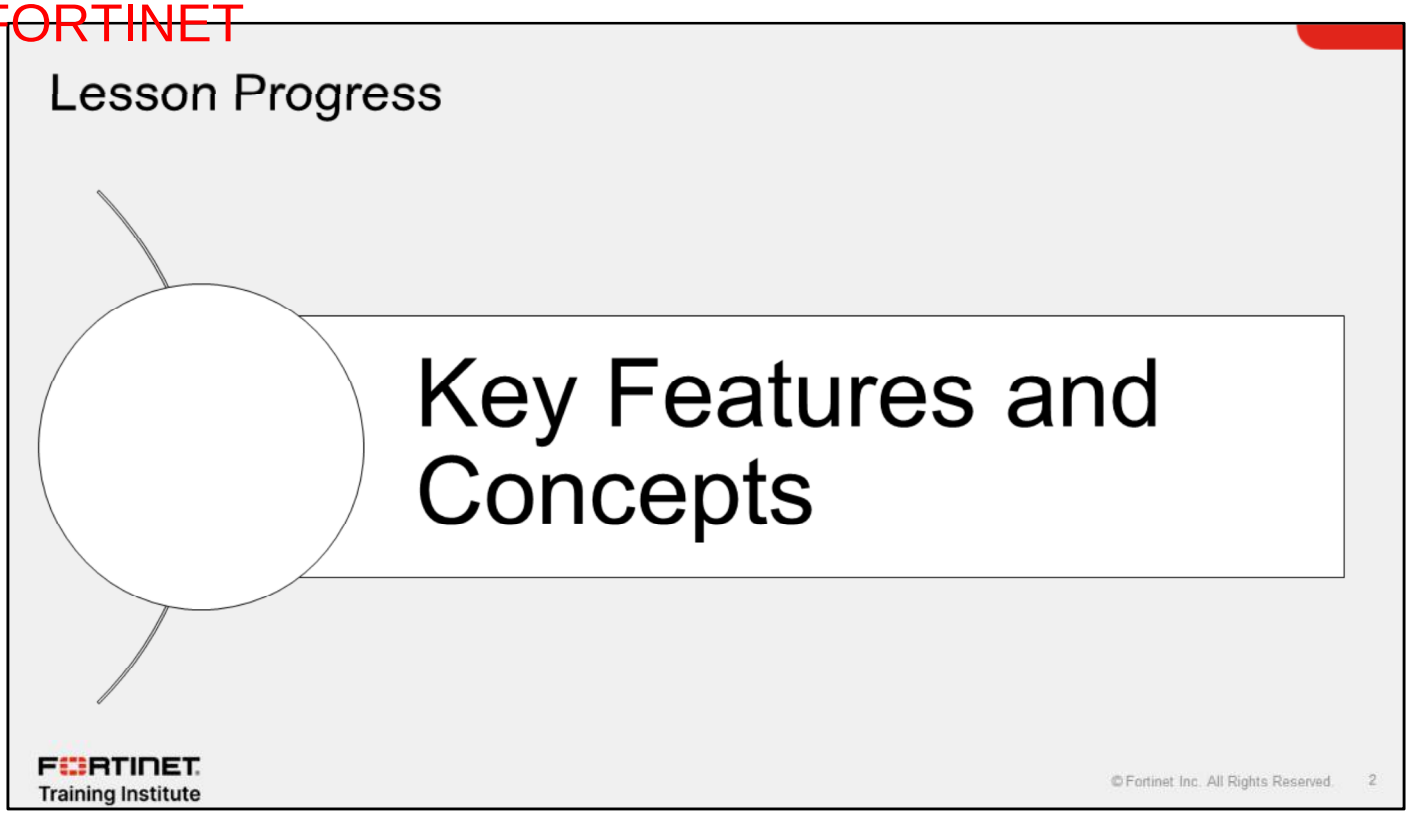


Congratulations! You have come to the end of this material.

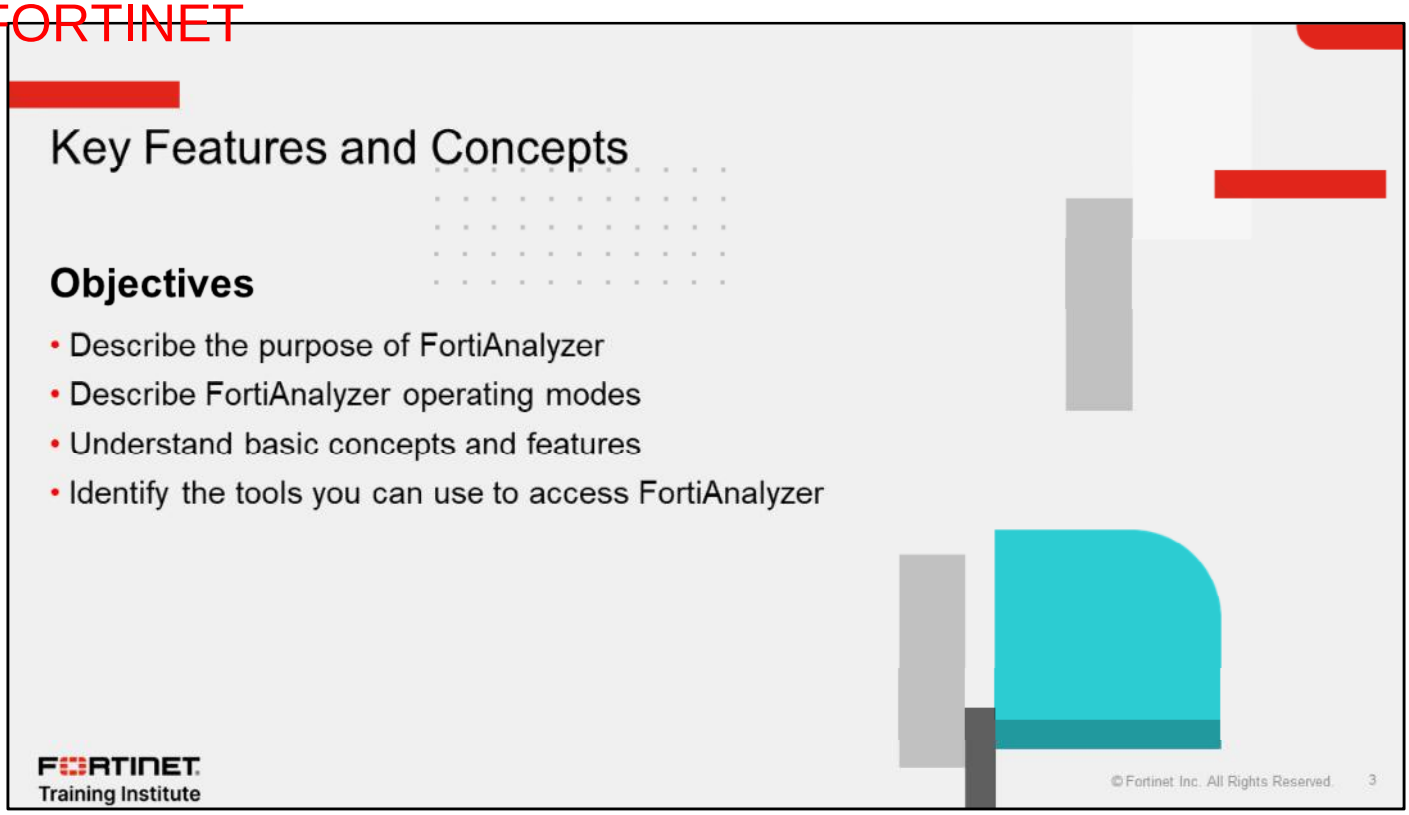


In this lesson, you will learn about the key features and concepts of FortiAnalyzer, and how to initially access FortiAnalyzer.

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

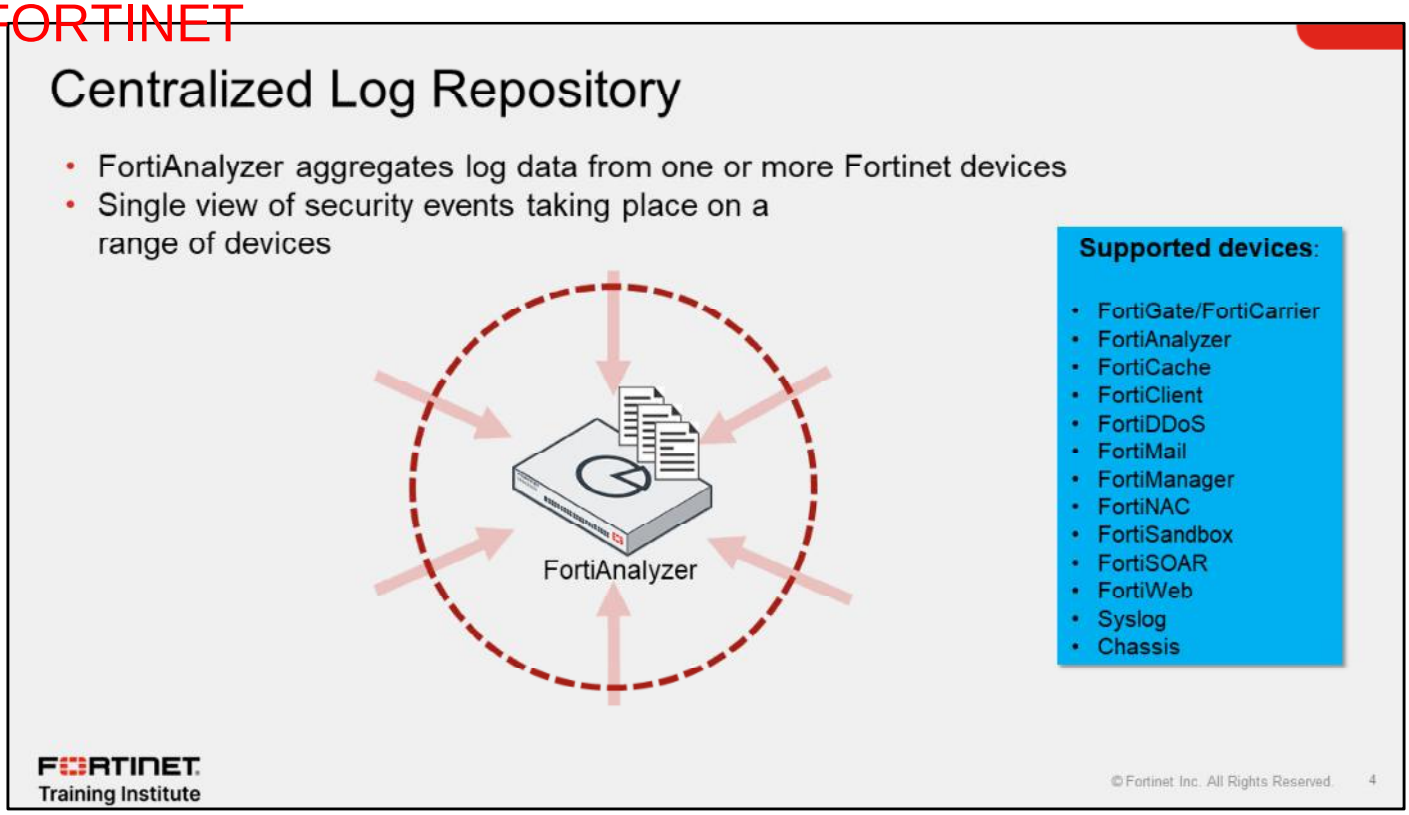


In this lesson, you will explore the topic shown on this slide.



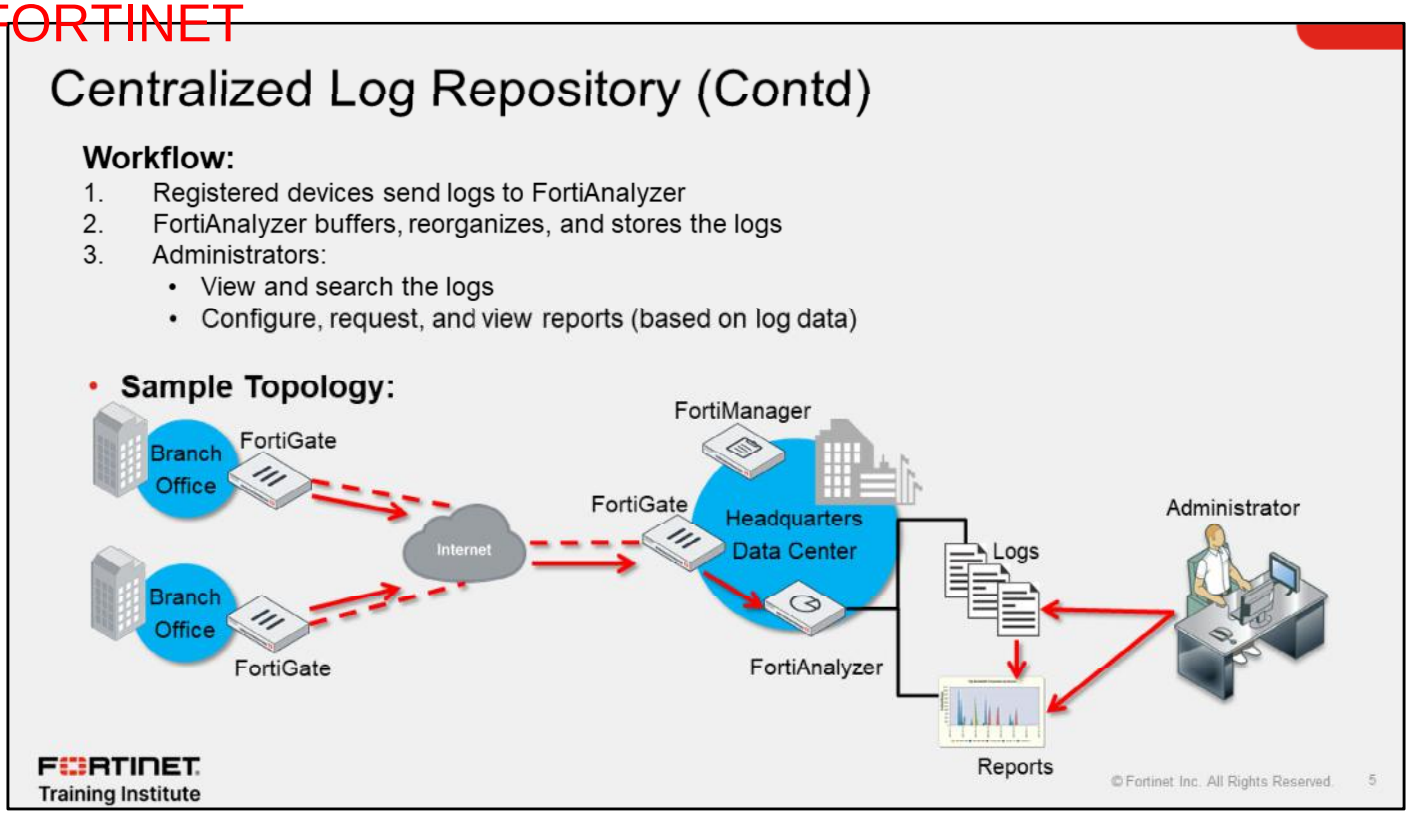
After completing this section, you should be able to achieve the objectives shown on this slide.

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



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

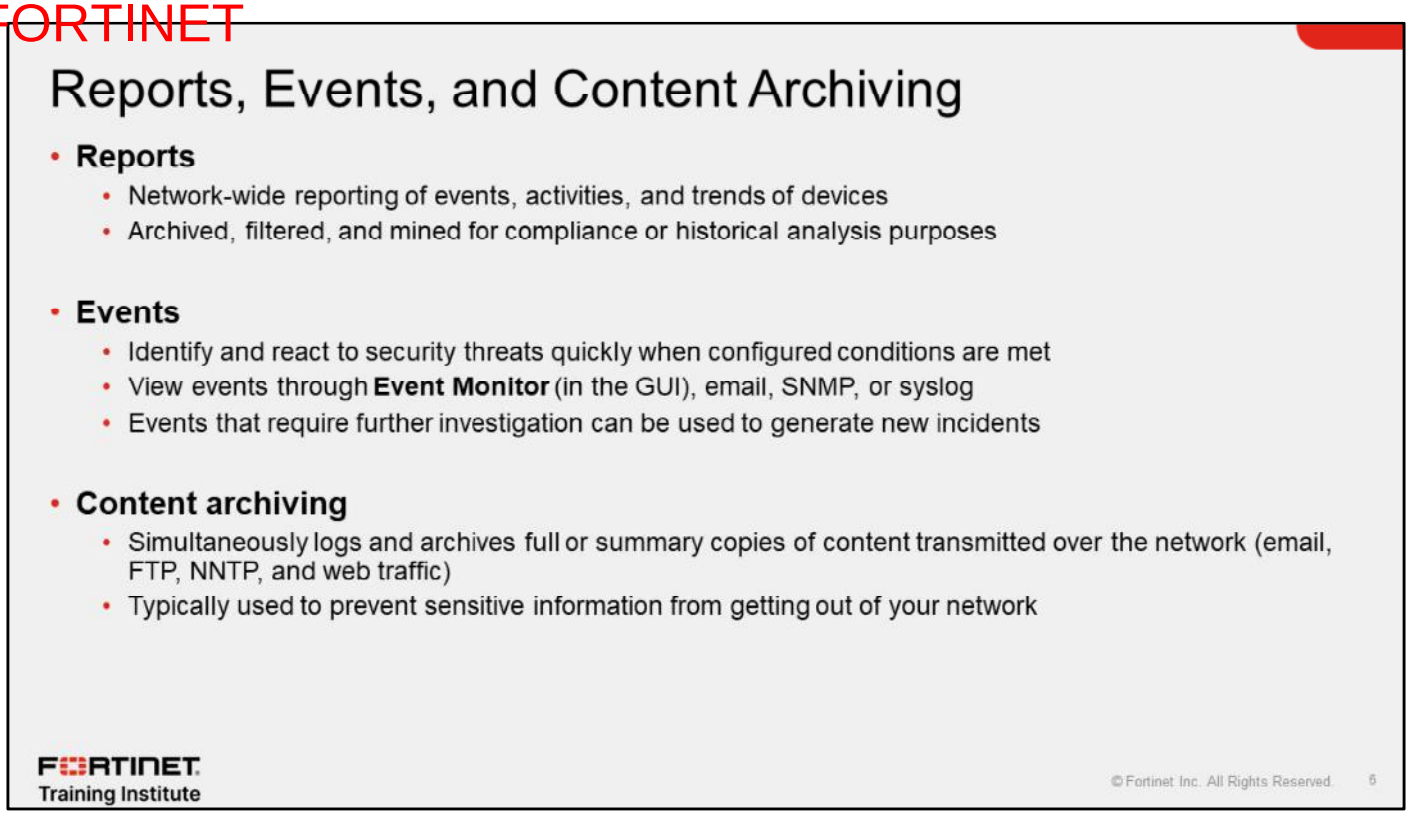
FortiAnalyzer can be integrated with many different Fortinet solutions. For a complete list, refer to the release notes at docs.fortinet.com.



The logging and reporting workflow operates as follows:

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

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

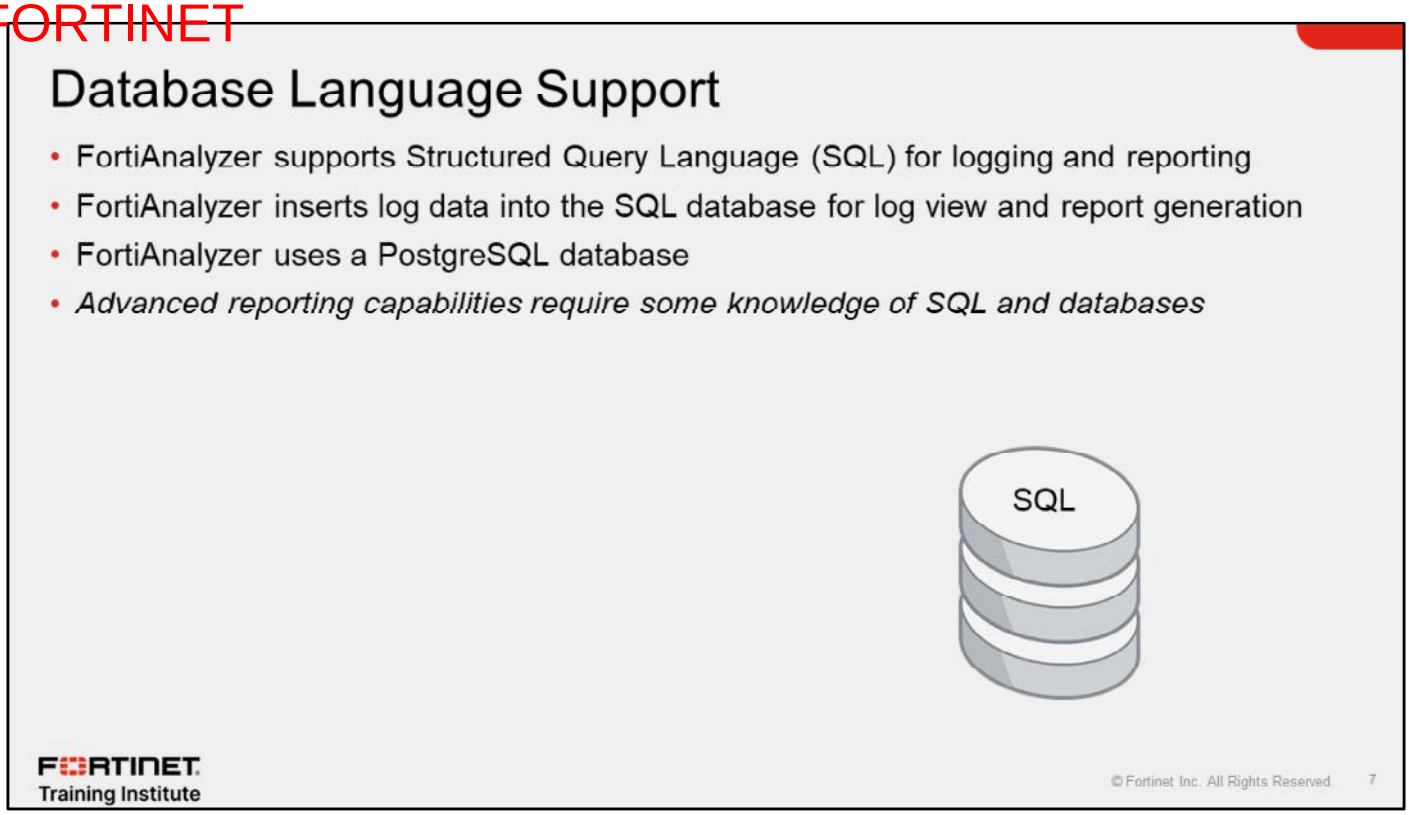


Some key features of FortiAnalyzer include reporting, alert generation, and content archiving.

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

FortiAnalyzer events allow you to react quickly to threats because it's not realistic to physically monitor your network around the clock. The system can generate events when specific conditions in the logs are met—conditions you have configured FortiAnalyzer to monitor for registered devices. You can see your events on the GUI, and you can also send them to multiple recipients by email, SNMP, or syslog. Additionally, events that required further investigation can be used to generate new incidents.

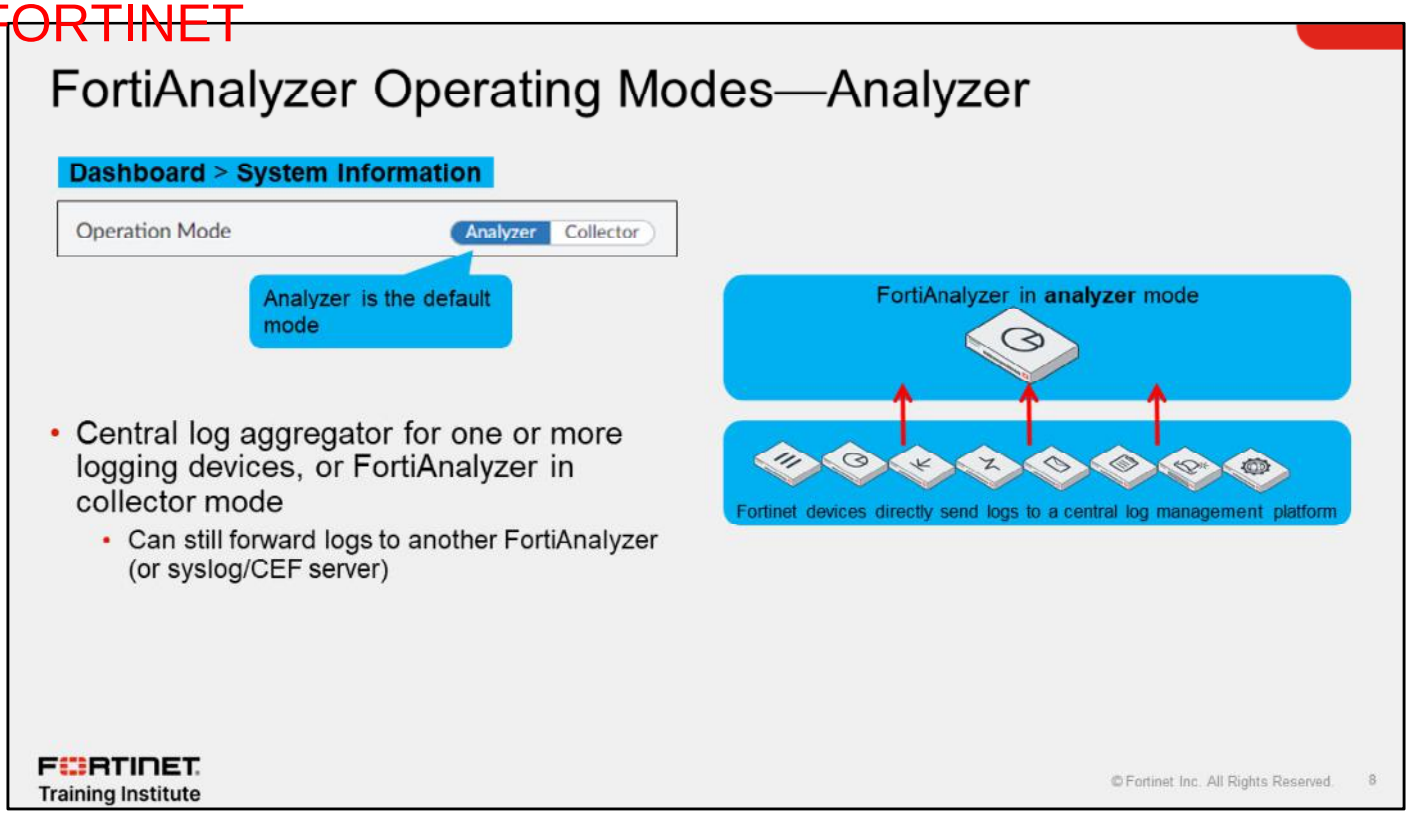
Content archiving provides a way to simultaneously log and archive full or summary copies of the content transmitted over the network. You typically use content archiving to prevent sensitive information from getting out of your organization's network. You can also use it to record network use. The data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



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

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

For more information on SQL and FortiAnalyzer, refer to the supplementary lesson *SQL Datasets*.



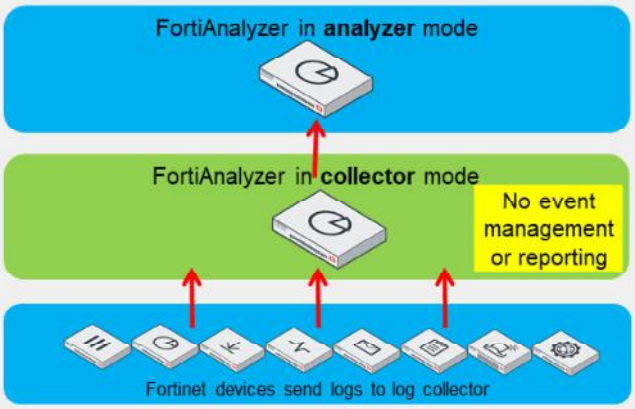
FortiAnalyzer has two modes of operation: analyzer and collector. The mode of operation you choose depends on your network topology and individual requirements.

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

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



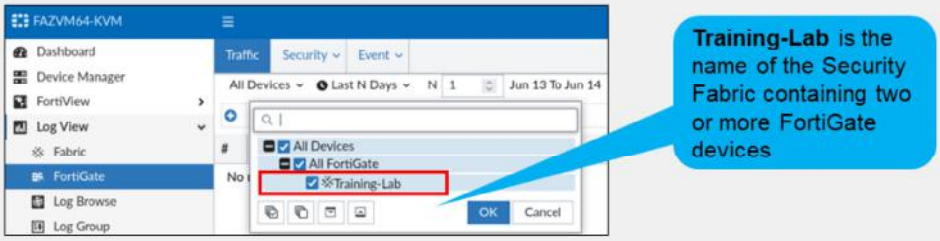
FORTINET Training Institute

 9

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

Security Fabric Logging

- Store and analyze logs from devices in a Security Fabric group as if the logs are from a single device
- The Security Fabric logs each session once
  - The first FortiGate that handles a session
  - No duplicate traffic logs for sessions coming from another fabric member's MAC address with the following exceptions:
    - If an upstream FortiGate performs NAT
    - Upstream FortiGate devices still log UTM events
- UTM and traffic logs are correlated so session details, UTM events, reporting and automation in the Security Fabric work correctly



FORTINET Training Institute

 10

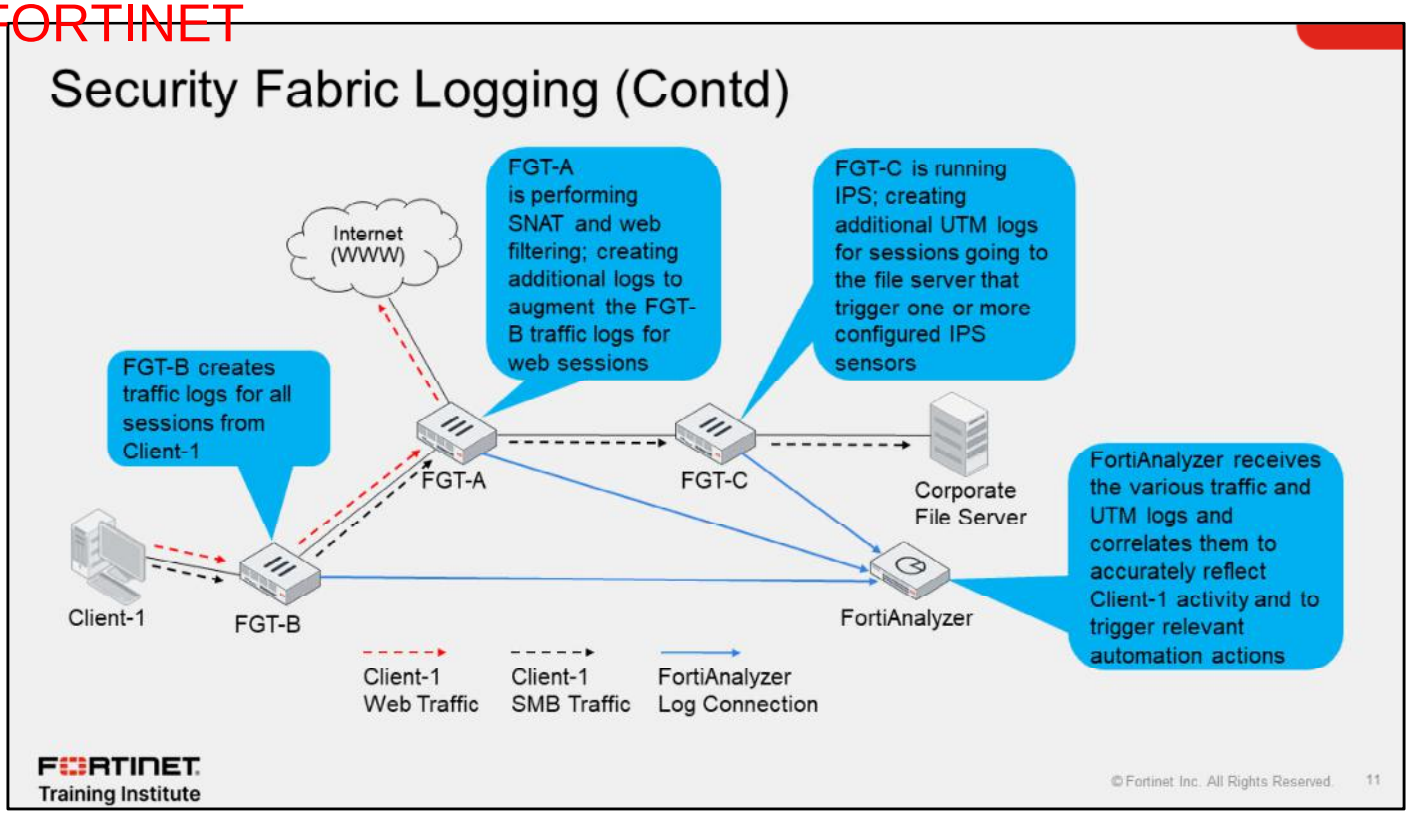
FortiAnalyzer supports the Security Fabric by storing and analyzing the logs from the devices in a Security Fabric group as if the logs are from a single device. FortiAnalyzer correlates traffic logs to corresponding UTM logs so that it can report sessions and bandwidth together with its unified traffic management (UTM) threats.

A session's traffic logging is always done 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 helps to eliminate the repeated logging of a 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.

Upstream devices complete UTM logging, if configured, and FortiAnalyzer performs UTM and traffic log correlation for the Security Fabric, in order to provide a concise and accurate record of any UTM events that may occur. No additional configuration is required for this to take place because FortiAnalyzer performs this function automatically.

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



This slide shows how logging functions in the Security Fabric to give full visibility while eliminating duplicate logs throughout the environment. There are three FortiGate devices configured in a Security Fabric along with a FortiAnalyzer device:

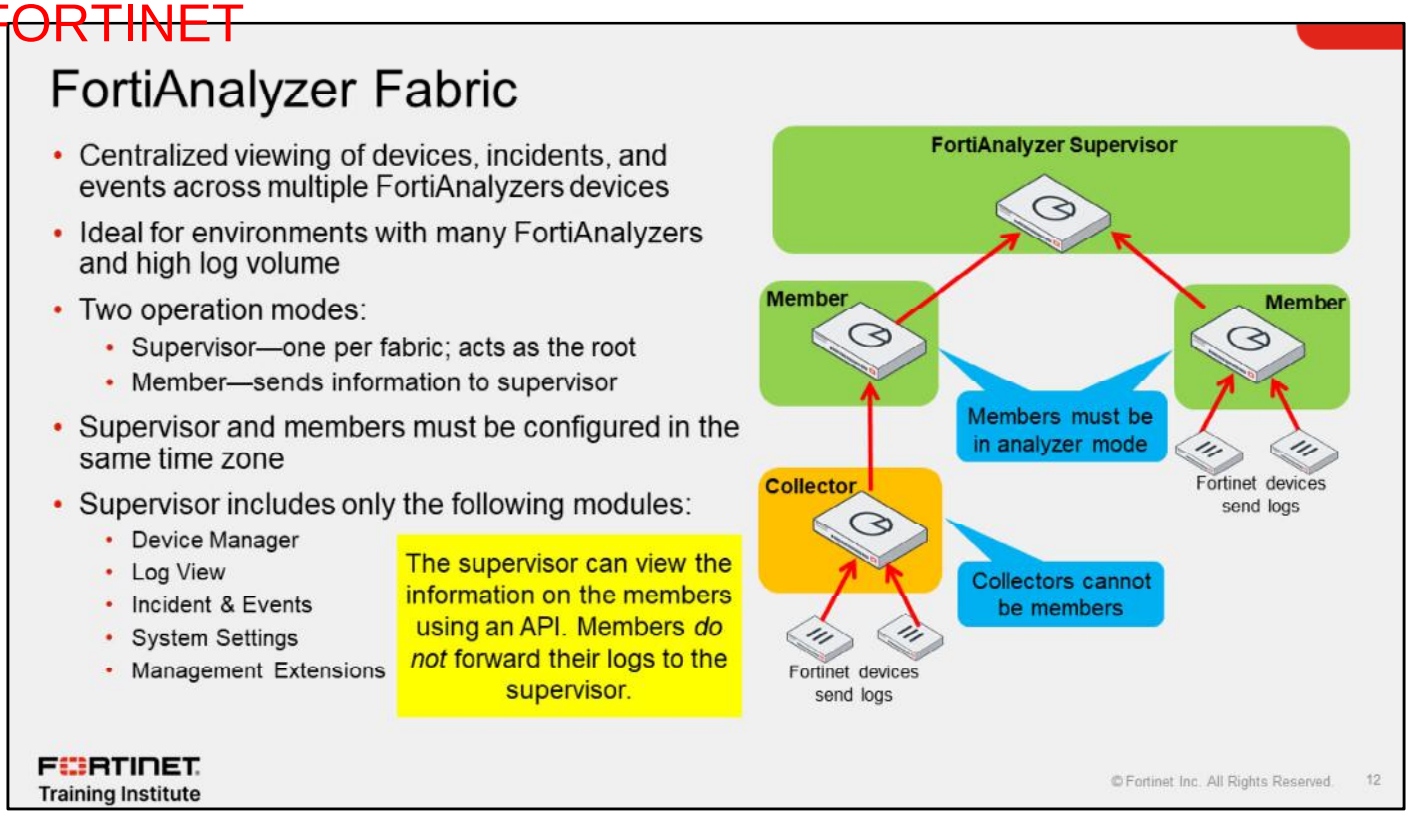
- FGT-A is installed between the corporate network and its internet service provider, where it performs SNAT on outbound communications for RFC-1918 hosts, as well as web filtering for HTTP/HTTPS sessions.
- FGT-B is installed in the access layer, providing device detection, breach isolation, and basic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

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

The web session is forwarded to FGT-A, which doesn't duplicate the initial traffic log, but does generate a traffic log as a result of source network address translation (SNAT) being applied to the session. Additionally, FGT-A applies a web filtering policy to this session and generates the relevant UTM logs, if appropriate.

The server message block (SMB) session is forwarded to FGT-A, which does not duplicate the initial traffic log. FGT-A doesn't need to perform NAT or apply web filtering, so it forwards the traffic to FGT-C. FGT-C also does not generate a duplicate traffic log, but it performs IPS inspection based on its configuration and, should a signature match be triggered that results in an action generating a log, logs the event.

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



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

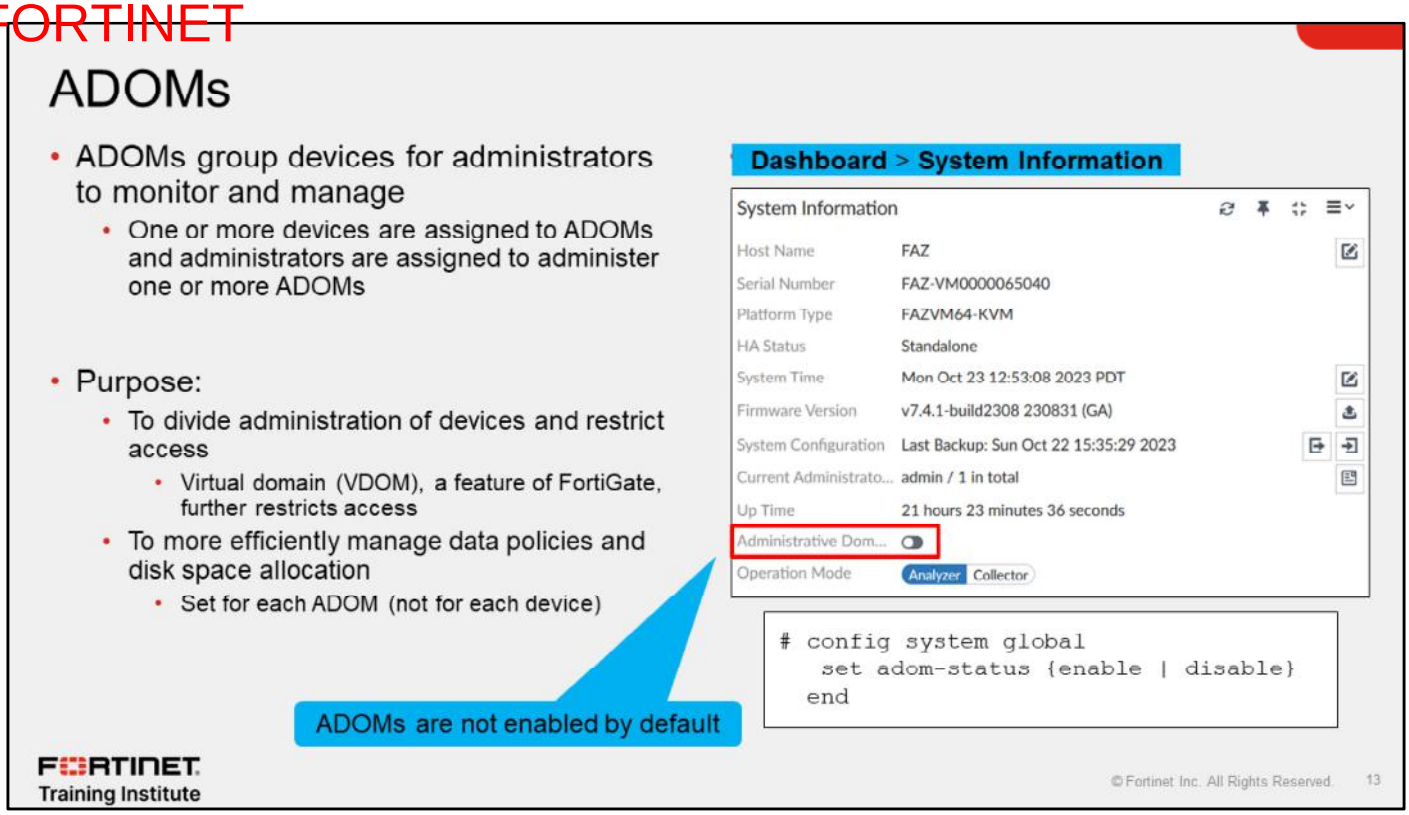
FortiAnalyzer Fabric includes two operation modes: supervisor and member.

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

Members are devices in the FortiAnalyzer Fabric that send information to the supervisor for centralized viewing. When configured as a member, FortiAnalyzer devices continue to have access to the FortiAnalyzer features identified in the *FortiAnalyzer Administration Guide*. Incidents and events are created or raised from each member.

FortiAnalyzers configured with high availability (HA) can become members. However, HA is not supported for FortiAnalyzers acting as the fabric supervisor.

All FortiAnalyzer Fabric members must be configured with the same time zone settings as the supervisor.



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

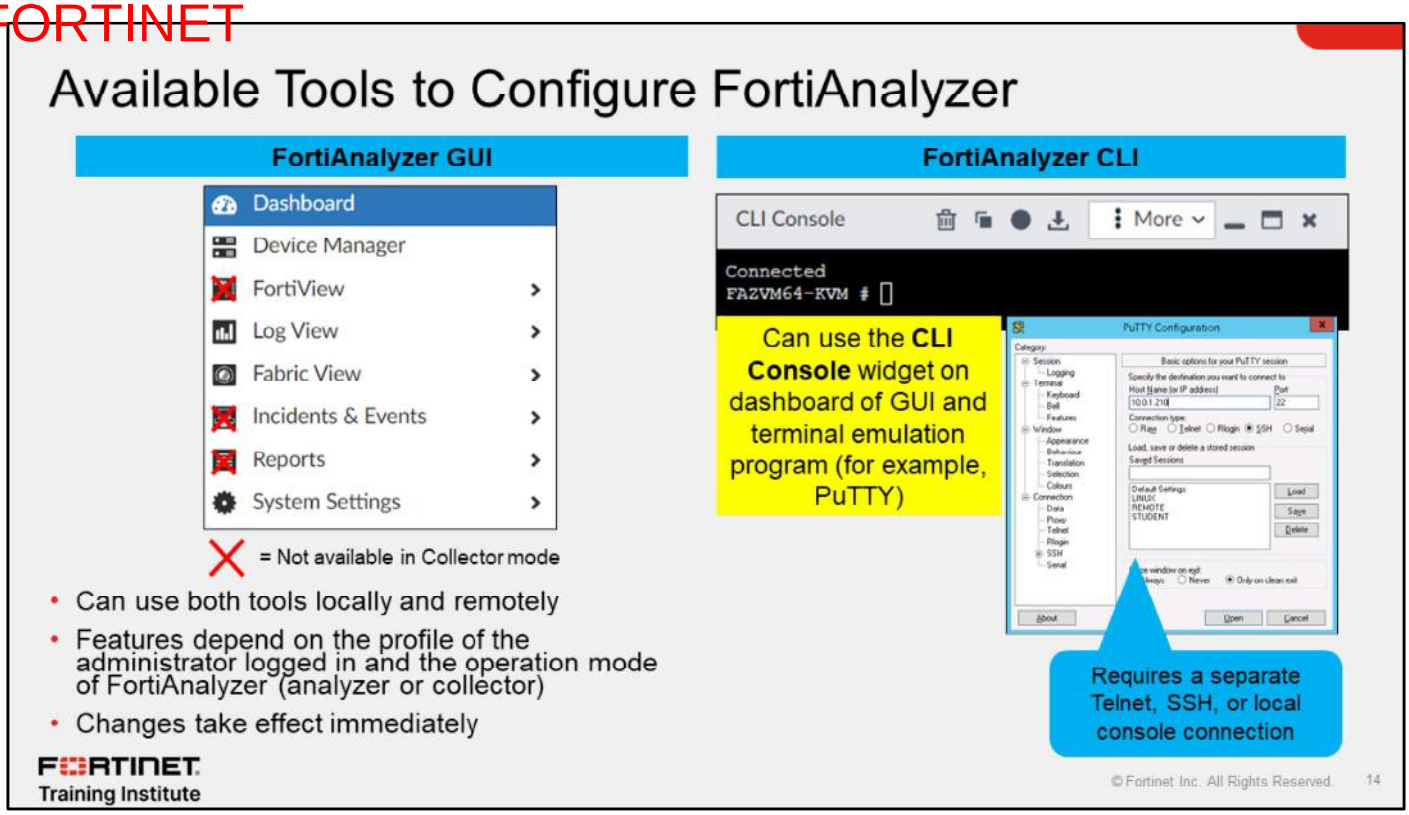
The purpose of ADOMs is to:

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

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

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

You will learn more about ADOMs in this course.



The GUI and CLI are the two configuration tools you can use to manage FortiAnalyzer. You can use both tools locally by connecting directly to FortiAnalyzer, and remotely, based on your configured settings. You can deny or permit access based on IP address.

When you use the CLI, you can run commands through the **CLI Console** widget, available on the GUI dashboard, and through a terminal emulation application, such as 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 example, when operating in collector mode, the GUI doesn't include **FortiView**, **Reports**, or **Incidents & Events**. Also, if you are logged in with the Standard_User or Restricted_User administrator profiles, full access privileges, like those granted to the Super_User profile, are not available. 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, without resetting the FortiAnalyzer system or interrupting services.

Note that the SQL database is disabled, by default, when FortiAnalyzer is in collector mode, so logs that require the SQL database are not available in collector mode unless the SQL database is enabled on the CLI.

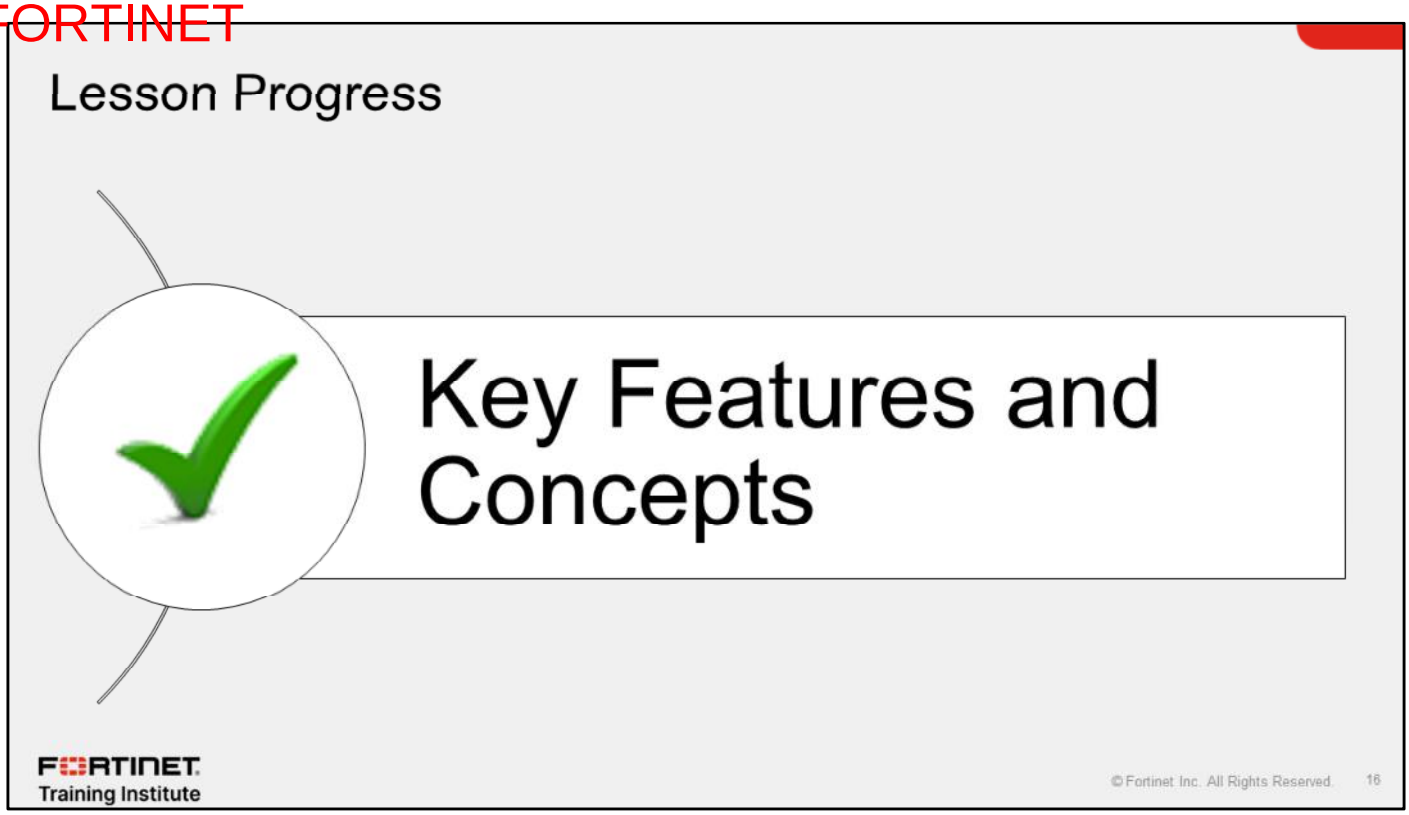
Knowledge Check

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

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

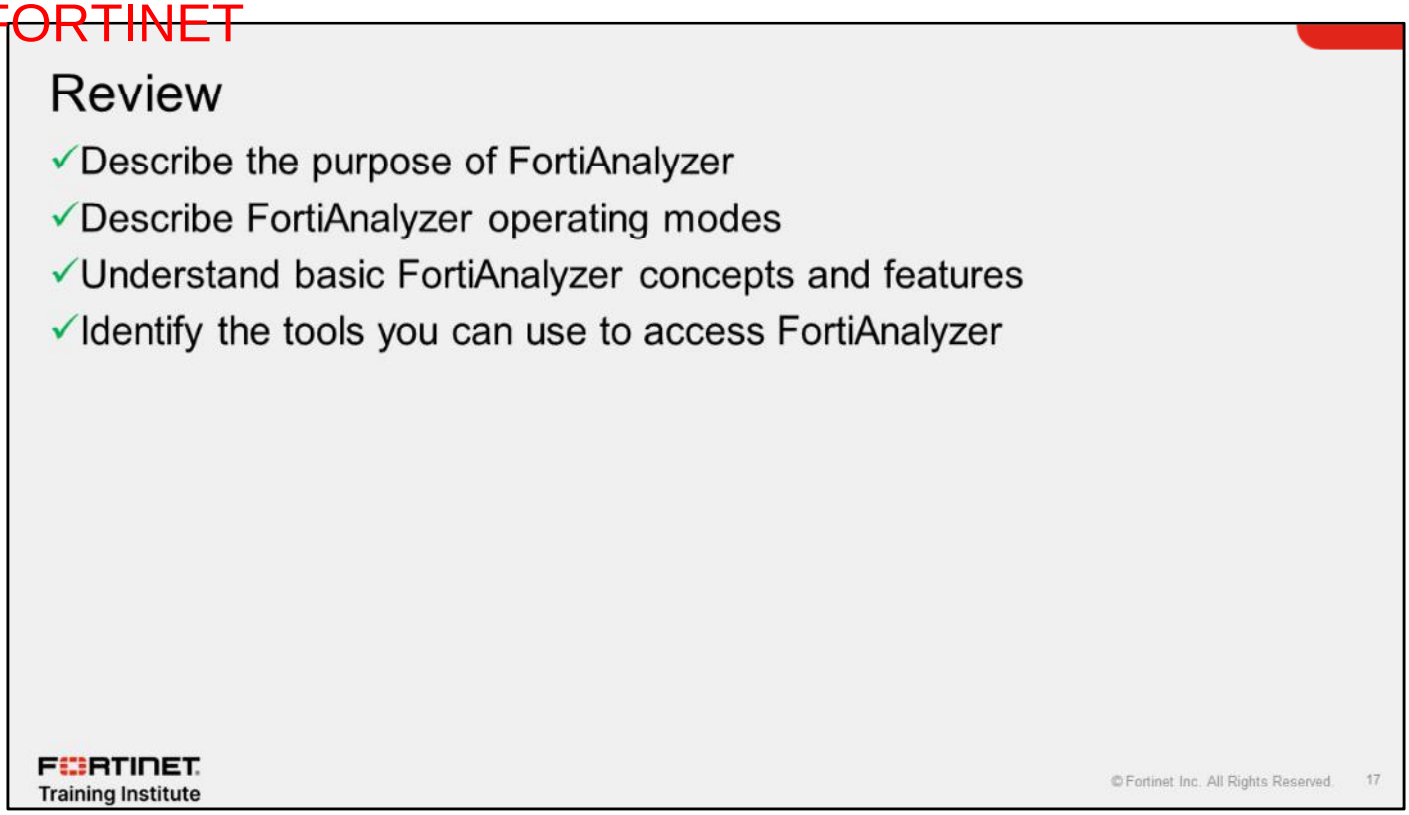
FORTINET Training Institute

 15

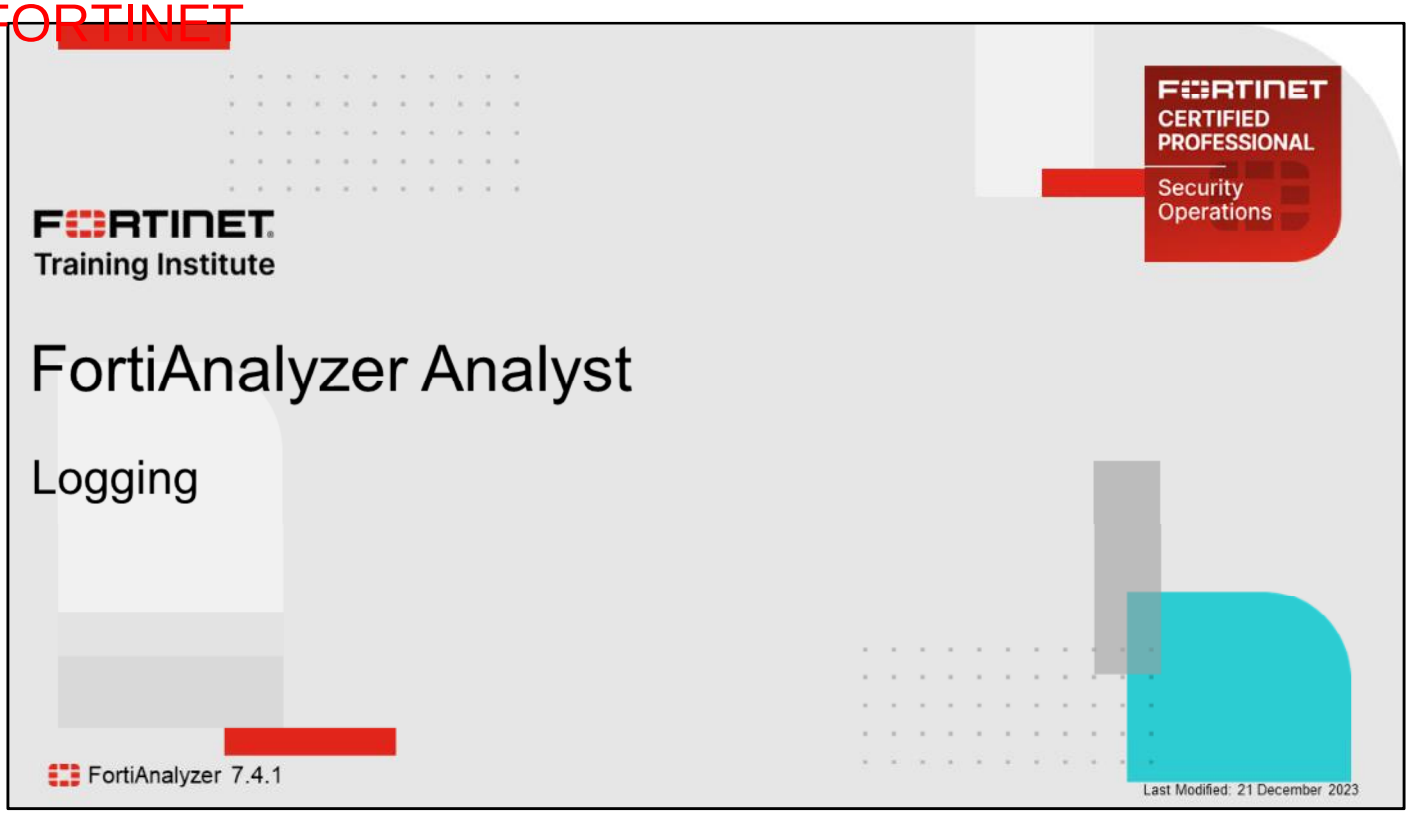


Congratulations! You have completed this lesson.

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

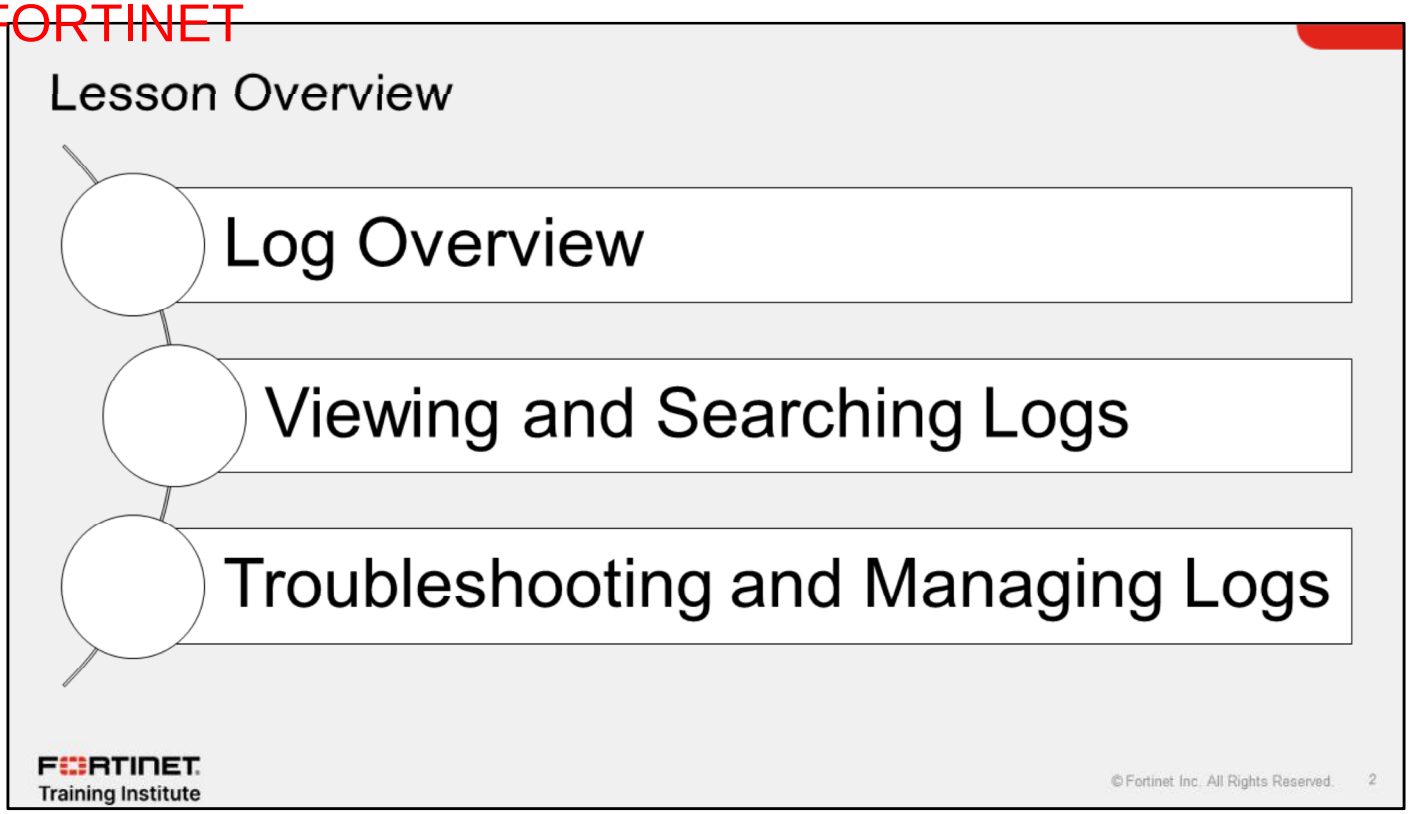


This slide shows the objectives that you covered in this lesson.

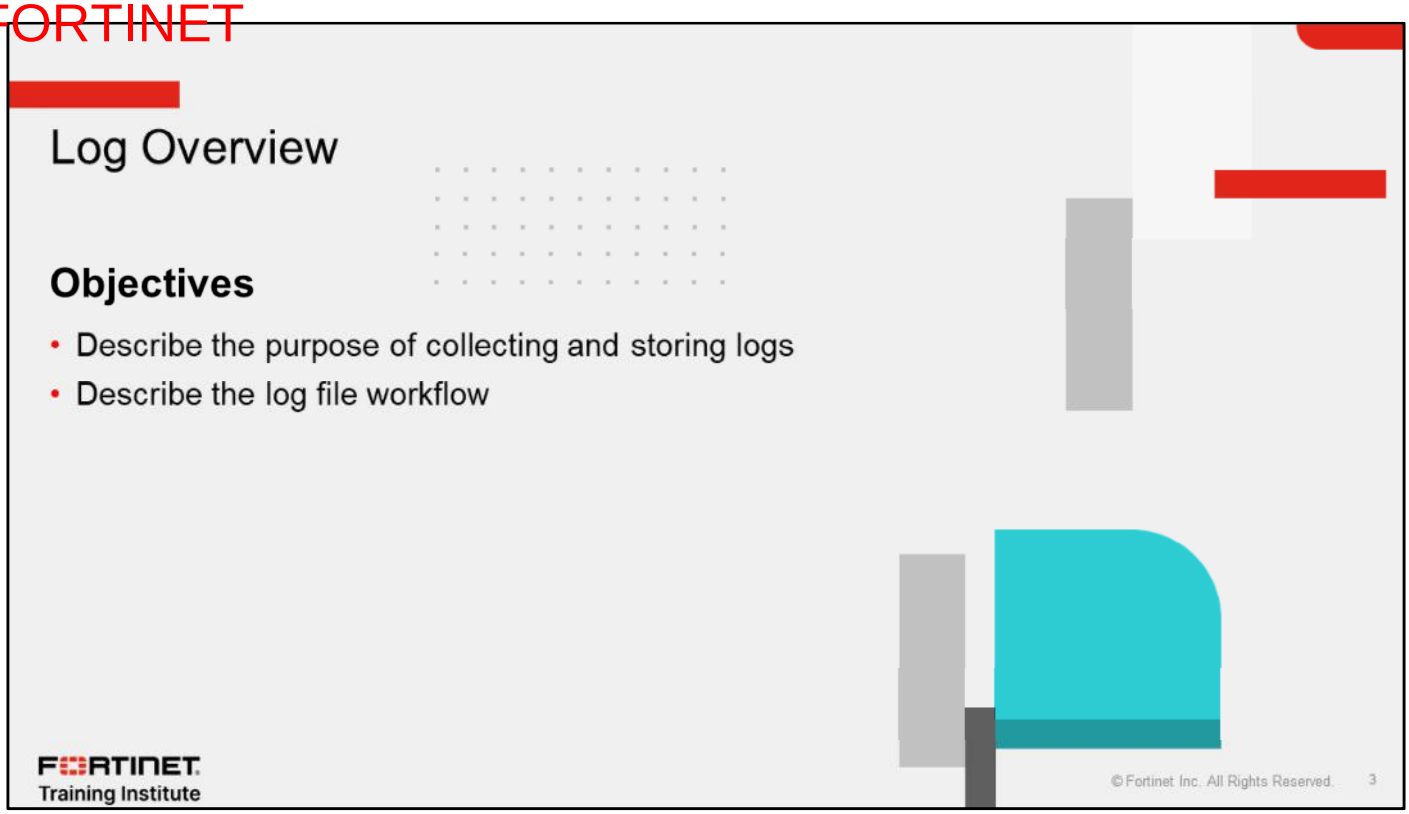


In this lesson, you will learn how to protect, view, and manage logs on FortiAnalyzer.

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.

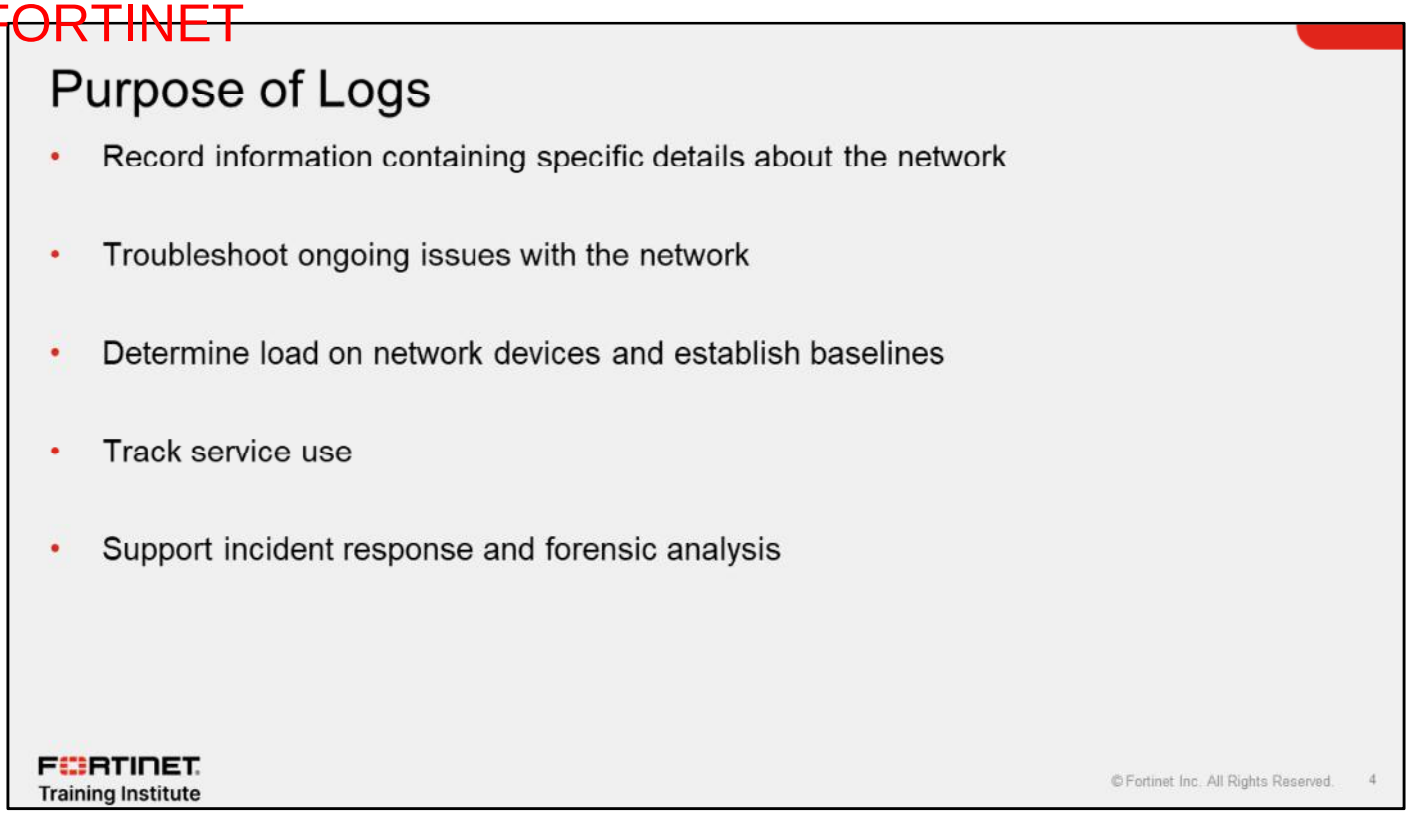


In this lesson, you will learn about the topics shown in this slide.



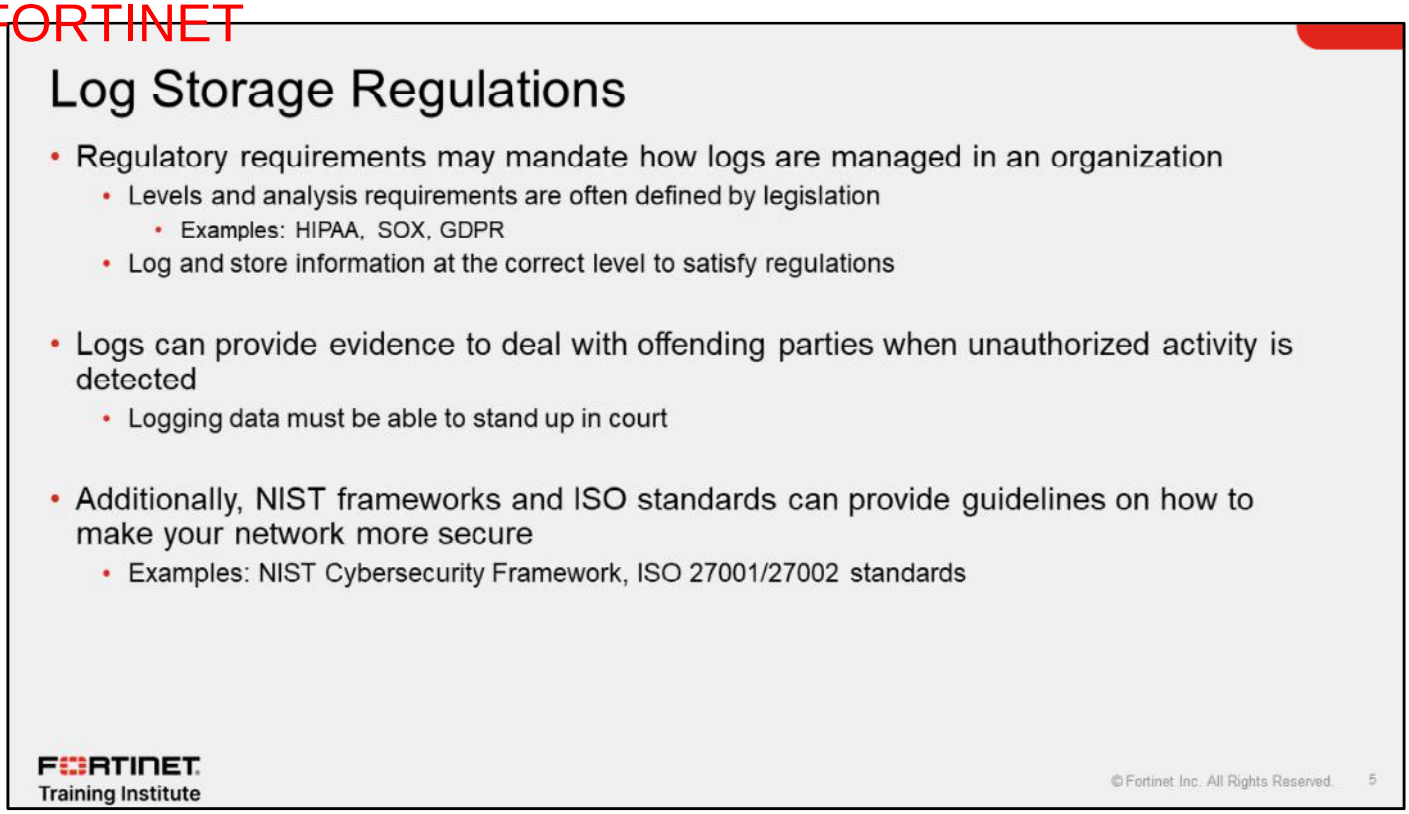
After completing this section, you should be able to achieve the objectives shown on this slide.

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.



Log messages help paint a picture of what is going on in your network. There are many uses for logs. They can help with troubleshooting the network, determine load on network devices, establish baselines, track service use, and support incident response and forensic analysis.

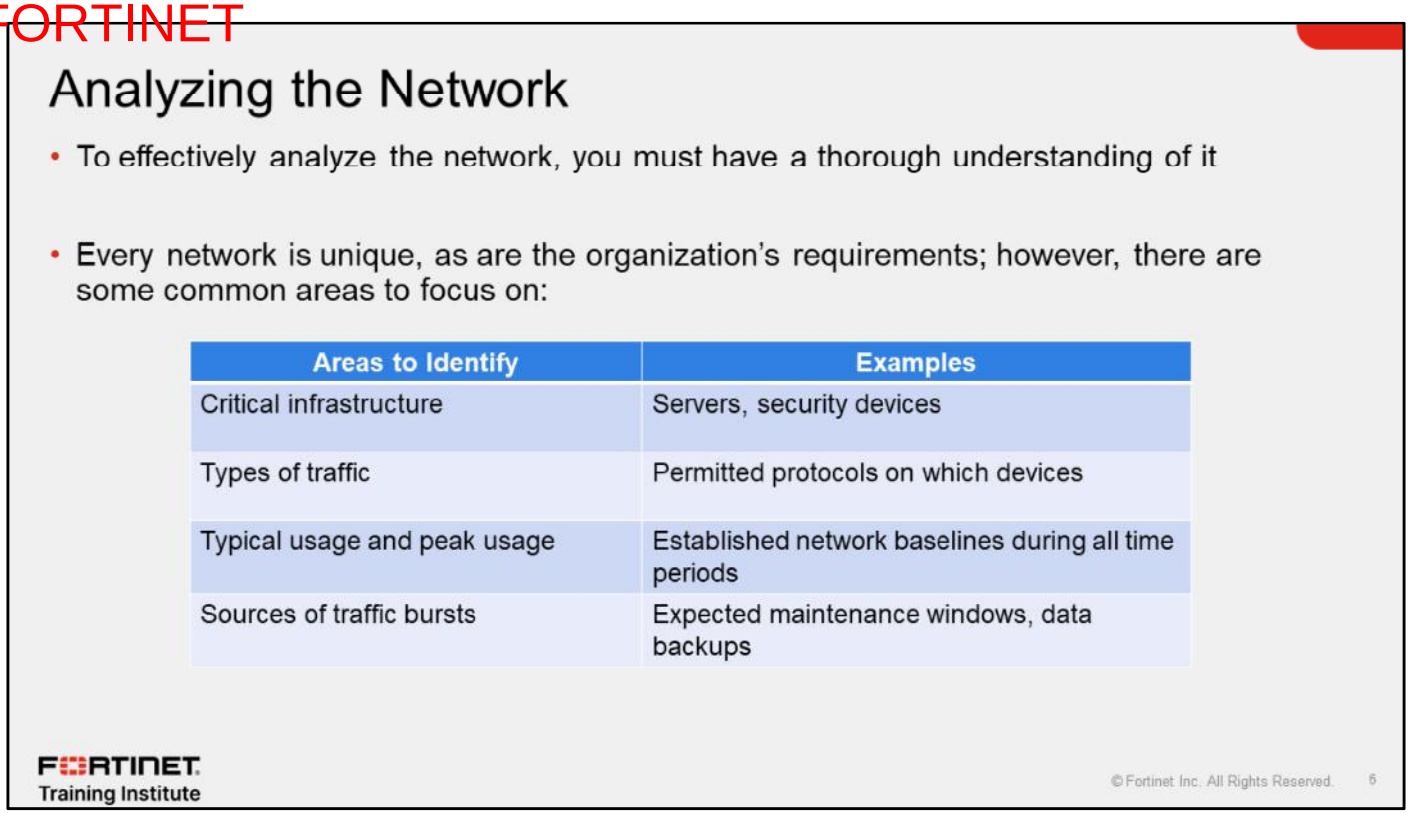
However, it is important to understand that logs are like a puzzle, and you must put several pieces together in order to get a complete understanding of what is going on. Multiple log messages are often required to determine the exact chain of activity that leads to a breach—a log in isolation often won't help you to best configure your network to prevent such breaches in the future. This is why centralized log storage is so important.



Regulations require that companies log specific information, record data, and store it at a correct level. It is crucial to thoroughly understand the legislation your organization must comply with, including the jurisdictions it falls under, and if there are 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.

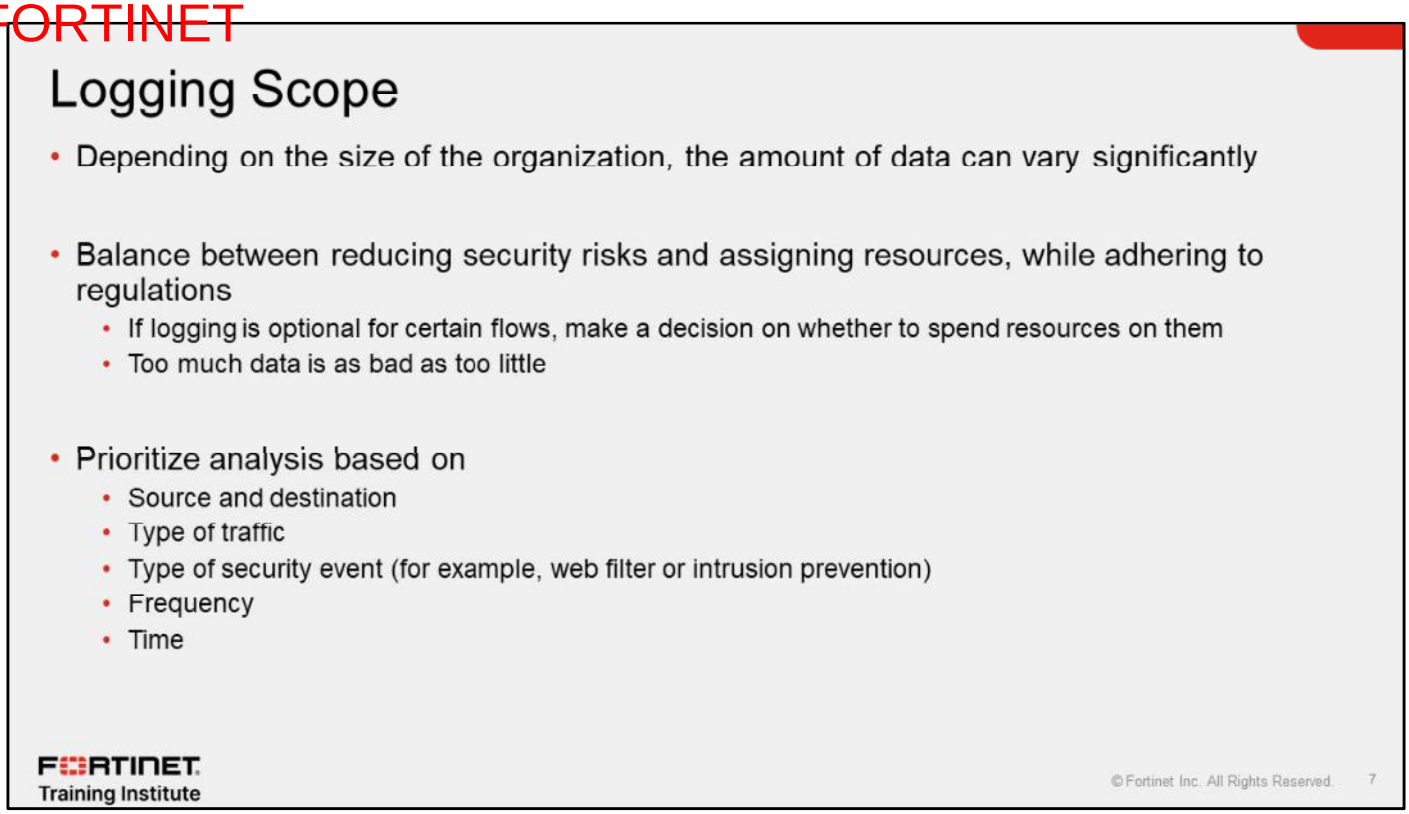
Log entries can be used as evidence in cases of unauthorized or illegal activity. The data must be able to stand up in court, so being able to understand and analyze your logs is very important.

It is often difficult to establish your organization's security policies, particularly if there are no existing ones in place. Instead of coming up with ideas on your own, you can consult widely recognized frameworks and standards created by organizations such as NIST and ISO.



To effectively analyze your organization's traffic, you need to have a deep understanding of the network. You must be able to identify:

- Critical infrastructure, such as servers and security devices, which are higher priority in any analysis
- Expected types of traffic, including knowing which protocols are permitted on which devices and being able to quickly identify abnormal traffic flows
- Typical usage and peak usage, which will help you to establish network baselines during all hours and allow you to recognize unexpected behavior, such as too much traffic for a certain time period
- Sources of traffic bursts, in order to create a buffer for expected maintenance windows, and data backups



Depending on the size of your organization, the amount of log data generated can become overwhelming. Logs are usually continuously generated, and one workstation can generate a large volume of logs in a short time. As an analyst, it is not practical to go through every log entry. Most logs are normal, and spending resources on analyzing them yield no benefits.

Keep in mind that not everything in the network needs to be logged. For example, if the infrastructure team is conducting tests on an isolated network, you can work with them to disable logging beforehand. Guest devices that are on a restricted network also may not need to be logged.

In your analysis, you should prioritize factors, such as the traffic type or types being seen, where the traffic is coming from or going to, 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 Types by Device

Device	Log type
Fabric	All
FortiGate	• Traffic [forward, local, sniffer, multicast] • Event [Endpoint, HA, Compliance, Security Rating, SDN Connector, SD-WAN, Switch-controller, FortiExtender, System, User, Router, VPN, Wan Opt. & Cache, WiFi] • Security [Application Control, AntiVirus, Data Leak Prevention, Web Application Firewall, Web Filter, Email Filter, File Filter, DNS, Intrusion Prevention, SSH, SSL, VoIP, Vulnerability Scan, FortiClient]
FortiCache	Traffic, Event, Antivirus, Web Filter
FortiClient	Traffic, Event, Vulnerability Scan
FortiMail	History, Event, Antivirus, Email Filter
FortiManager	Event
FortiSandbox	Malware, Network Alerts
FortiWeb	Event, Intrusion Prevention System (IPS), Traffic
Syslog	Generic (used for compatibility with older FortiGate or for non-Fortinet devices)

The logs displayed on your FortiAnalyzer depend on the device type logging to it and the enabled features

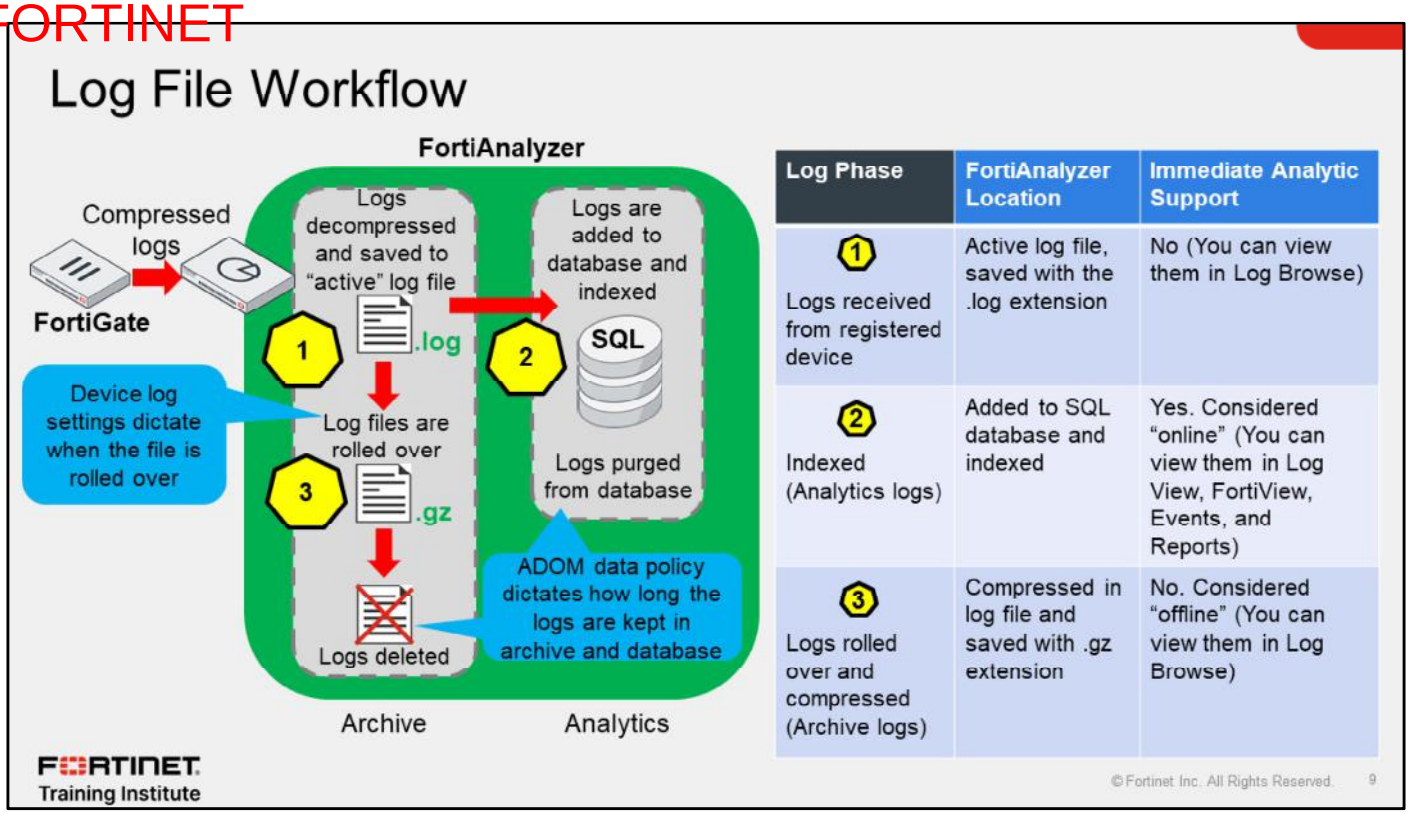
FORTINET Training Institute

 8

To be able to analyze and interpret your logs, it is important to understand the different log types and what information they contain, as well as what logs FortiAnalyzer collects from each supported device.

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

This table lists the log types and subtypes FortiAnalyzer collects from some of the supported devices. Refer to the *FortiAnalyzer Administration Guide* for the complete list.



Log Phase	FortiAnalyzer Location	Immediate Analytic Support
1 Logs received from registered device	Active log file, saved with the .log extension	No (You can view them in Log Browse)
2 Indexed (Analytics logs)	Added to SQL database and indexed	Yes. Considered "online" (You can view them in Log View, FortiView, Events, and Reports)
3 Logs rolled over and compressed (Archive logs)	Compressed in log file and saved with .gz extension	No. Considered "offline" (You can view them in Log Browse)

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 online and offer immediate analytic support. You can view these logs using **Log View**, **FortiView**, **Incident & Events**, and **Reports**. FortiAnalyzer purges analytics logs from the SQL database as specified in the ADOM data policy.

3. Eventually, when the log file reaches a configured size, or at a set schedule, it is rolled over. The process of rolling 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, they count toward the archive quota and retention limits, and FortiAnalyzer deletes them based on the ADOM data policy. You can view these logs using **Log Browse**.

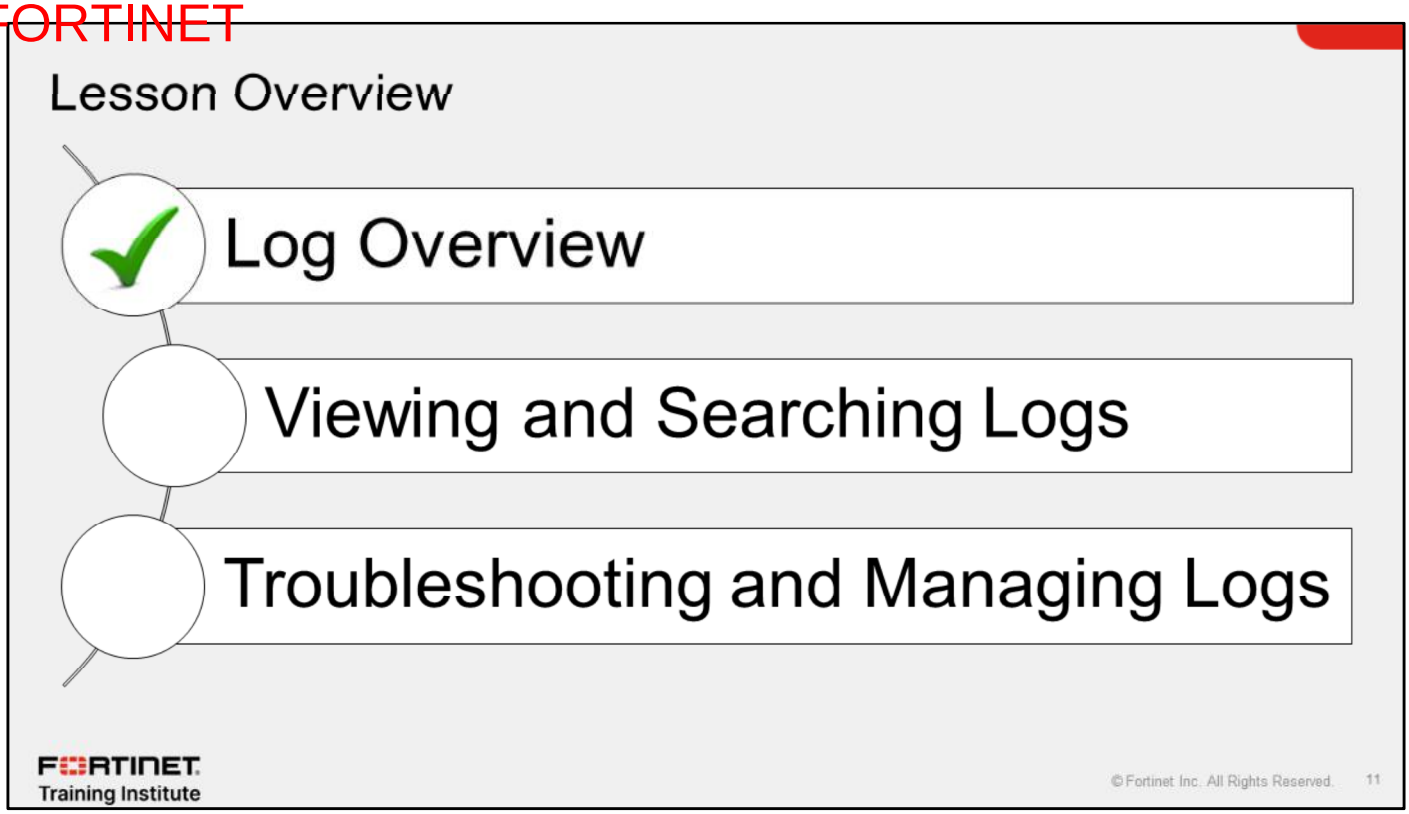
Knowledge Check

1. Logs in the compressed phase are known as _____ logs.
   - ✓A. Archive logs
   - B. Analytics logs

2. What happens when a log file saved on FortiAnalyzer disks reaches the size configured in the device log settings?
   - ✓A. The log file is rolled over.
   - B. The log file is stored for analytic support.

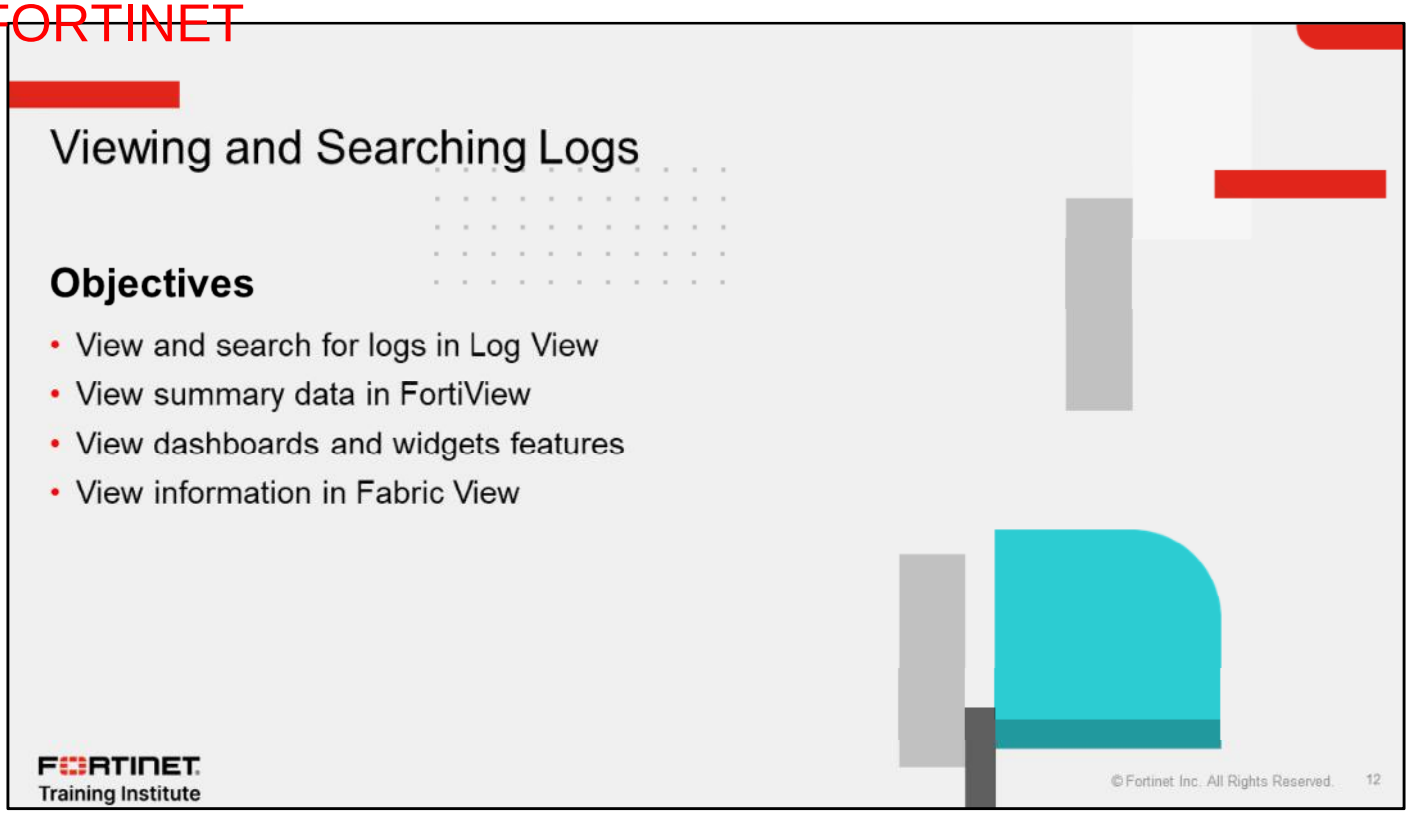
FORTINET Training Institute

 10



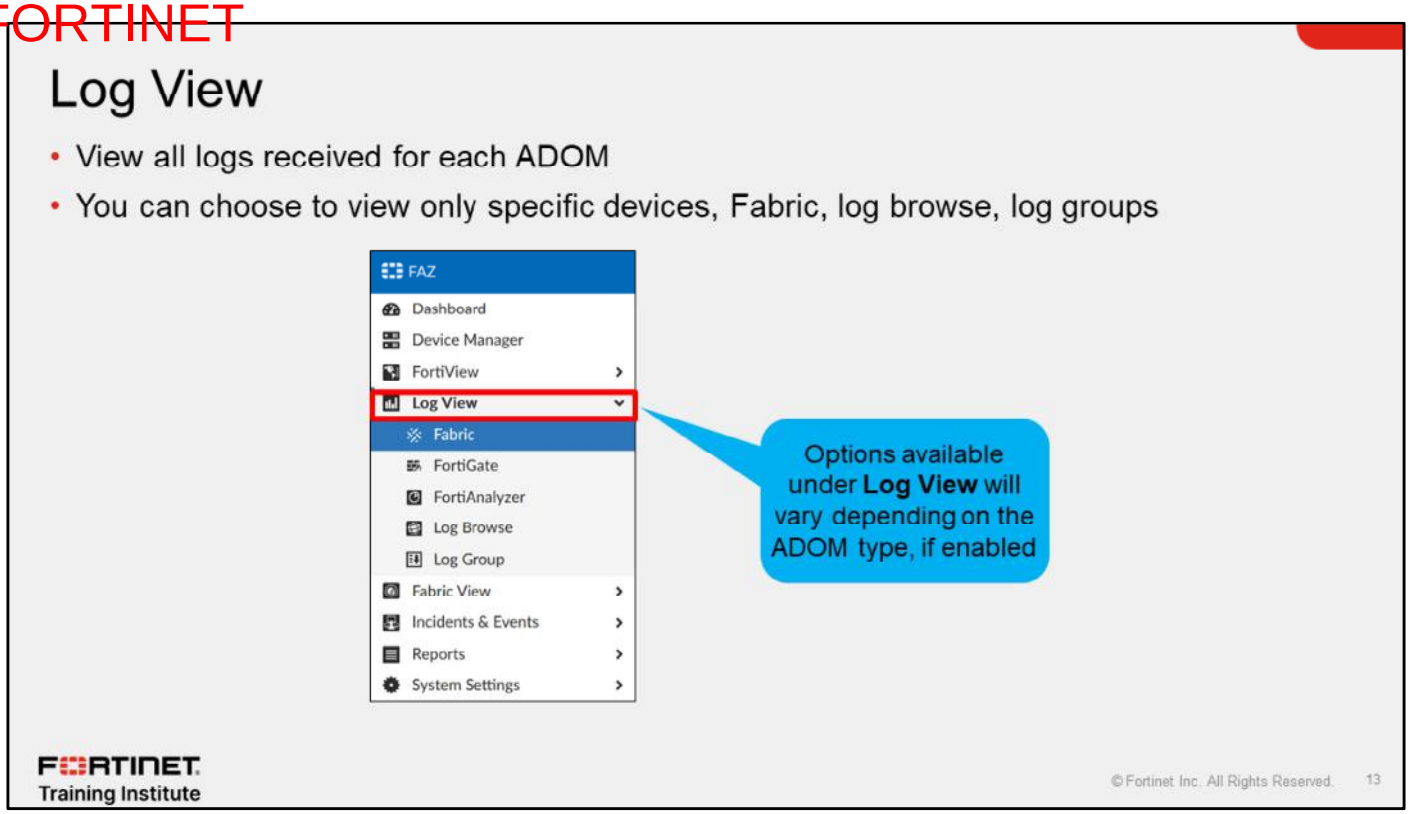
Good job! You now understand the purpose of log collection, log storage, and the log file workflow.

Now, you will learn about ways 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 information related to logs.



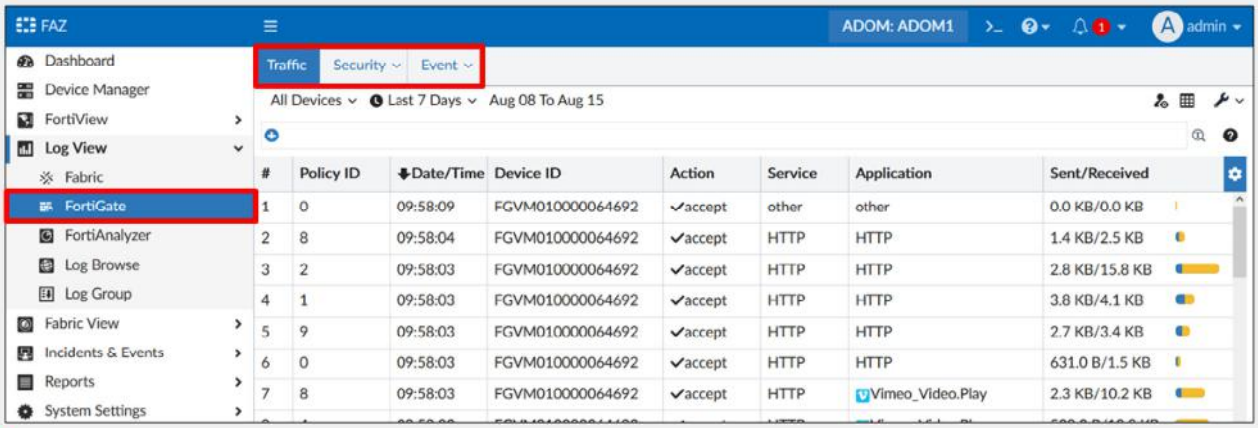
Log View allows you to view all log types being received by FortiAnalyzer. When ADOMs are enabled, each ADOM has its own logging information displayed.

You can choose to view logs from specific devices, Fabric or log groups, which 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 also view logs generated by FortiAnalyzer, and view the current log files and any rolled log files using **Log Browse**.

The options available under **Log View** vary, depending on the type of ADOM you create. In the example shown on this slide, the ADOM type is Fabric.

Viewing FortiGate Logs

- Can view three different types of FortiGate logs: **Traffic**, **Security**, and **Event**
- Security and event logs offer a summary dashboard
- Use the drop-down arrows to select a log subtype, such as web filtering (security logs) and system (event logs)



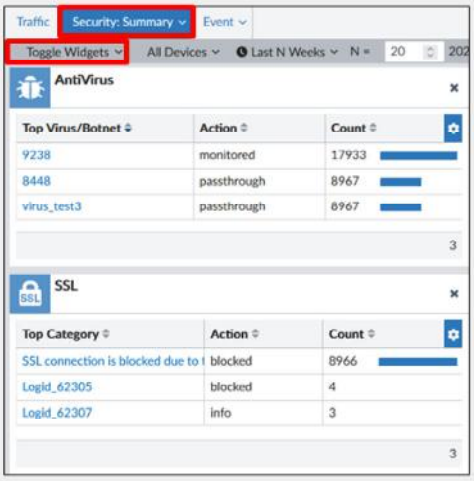
FortiGate, under **Log View**, provides log entries for all three types of FortiGate logs: **Traffic**, **Security**, and **Event**.

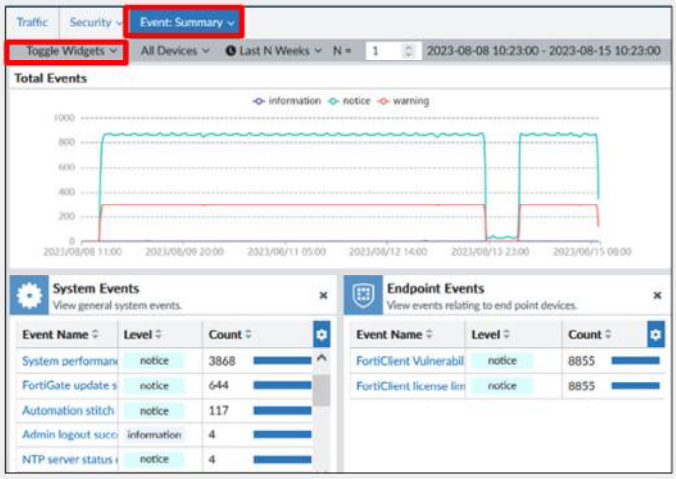
Traffic logs allow you to view traffic traversing the firewalls, including details such as source, destination, service, action (whether the traffic is allowed), and more. Security logs allow you to view logs related to unified threat management (UTM) inspection. Event logs are generally related to the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

You can use a drop-down menu to specify which security or event log subtype you want to see, or access their summary dashboard for an overview.

Viewing FortiGate Logs (Contd)

- View a summary of security logs or event logs to investigate
- Click on any entry to drill down for more details





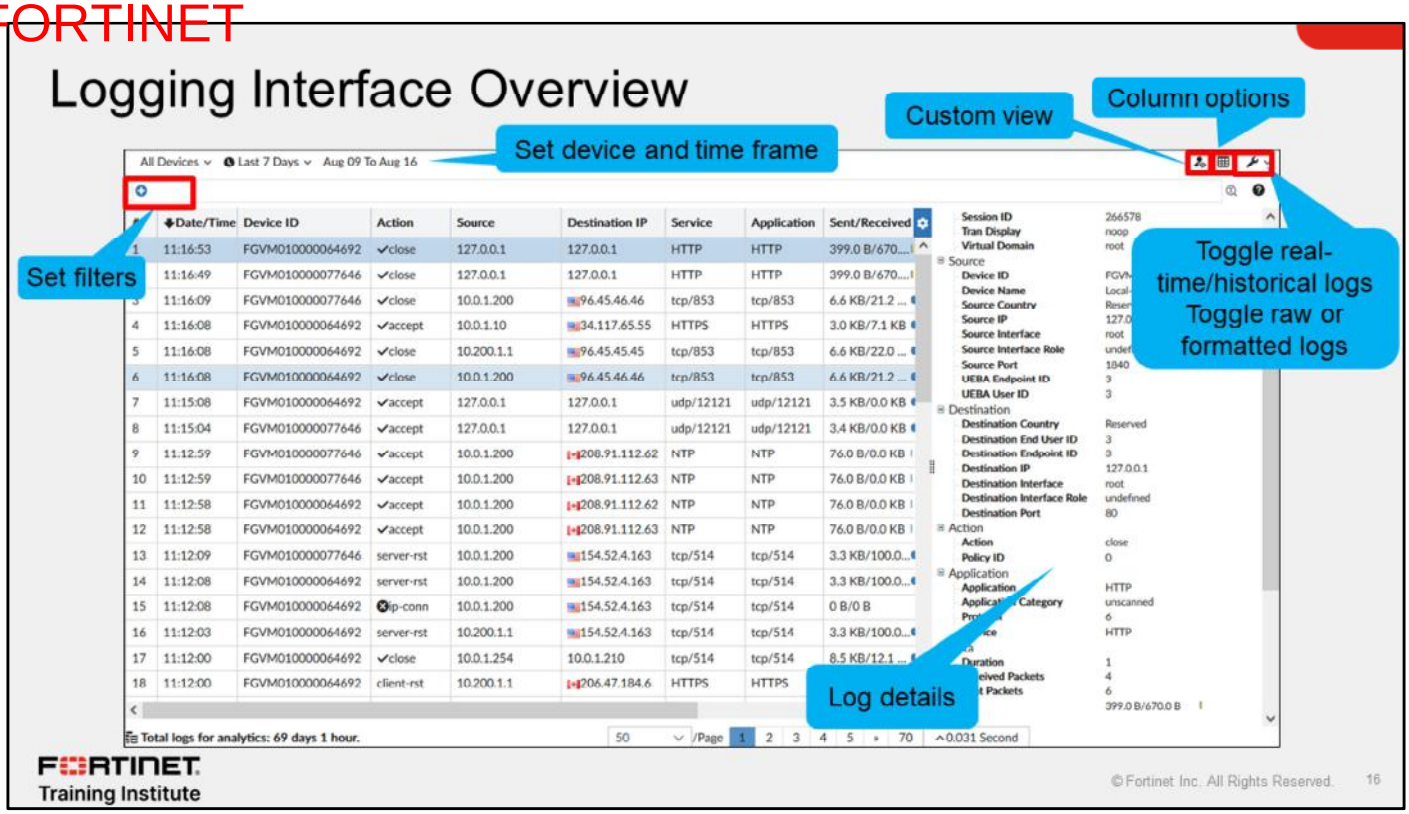
FORTINET Training Institute

 15

You can monitor all enabled security and event log types from their respective summary dashboards. This dashboard displays the top logs for each subtype in multiple widgets. You can add or remove widgets as needed.

You must ensure that the time filter set at the dashboard level is correct because it affects the information included on all widgets simultaneously.

From this dashboard, it is very easy to go to the specific logs by clicking the links provided. Doing so takes you to the specific log subtype section, with the appropriate filters applied to search for the specific log entries.



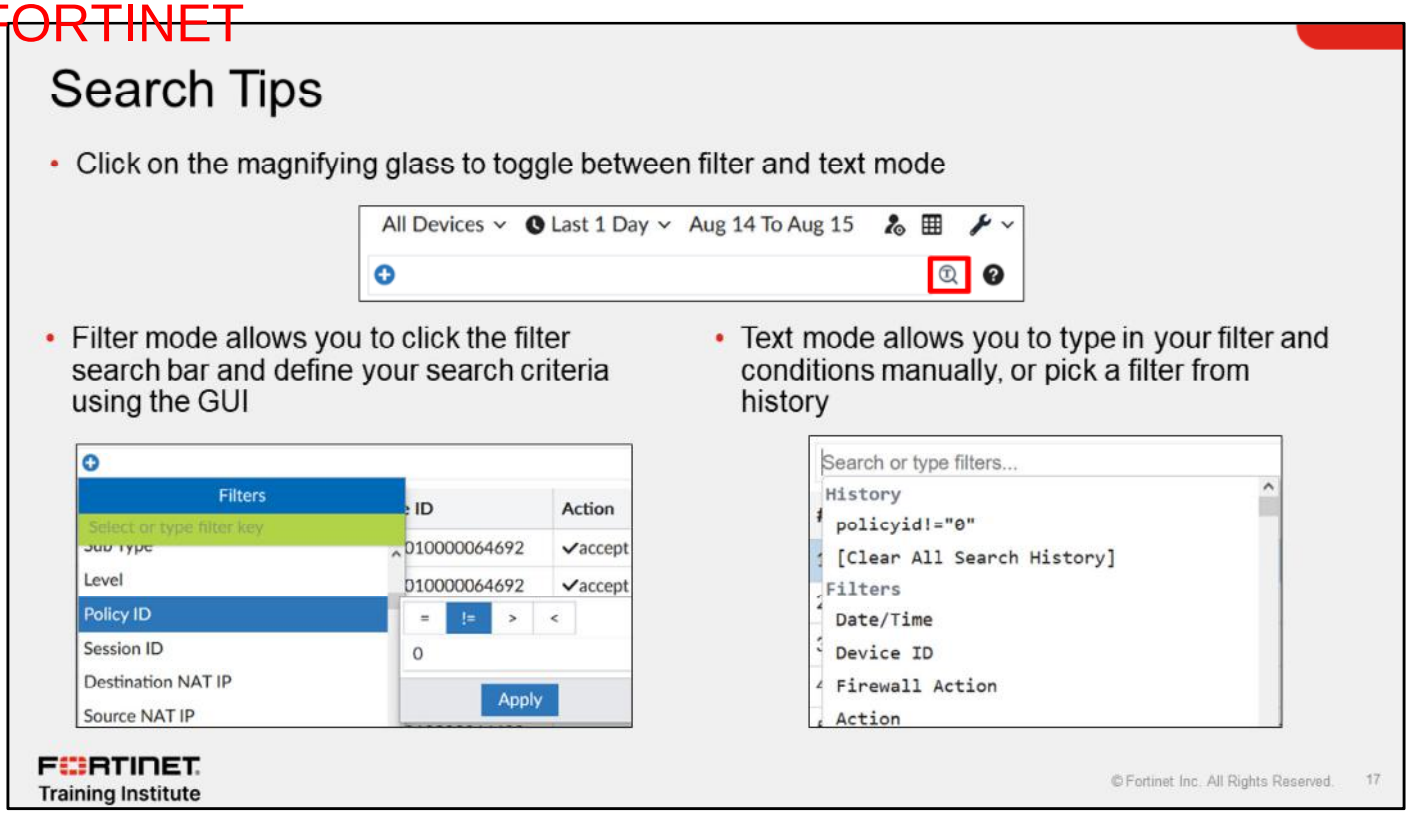
As a SOC analyst, you will need to perform frequent searches within the usually large number of logs received. FortiAnalyzer makes it very easy to search based on any of the fields included in the logs.

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

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

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

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

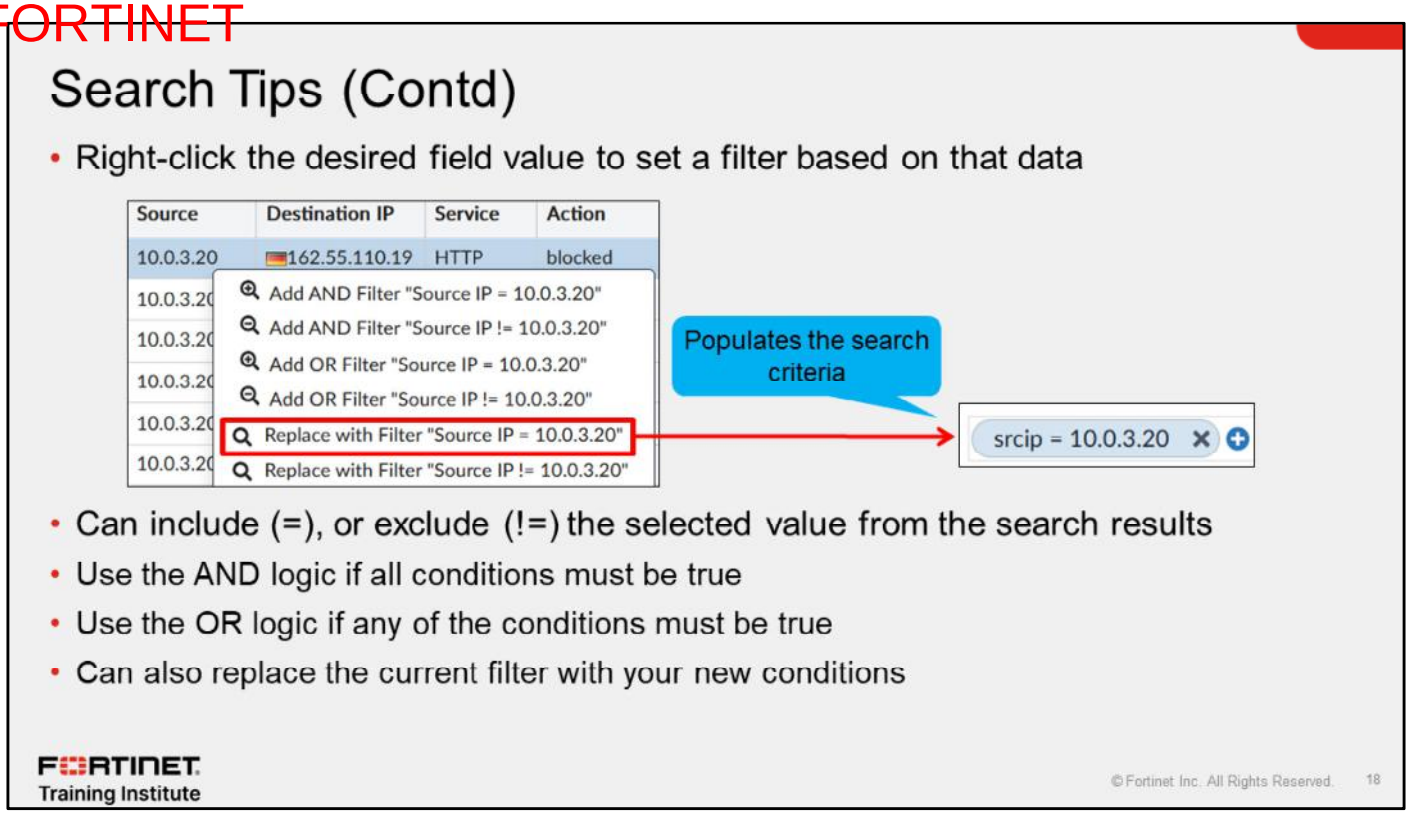


If your search filters don't return the results you expected, the filter may be poorly constructed.

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

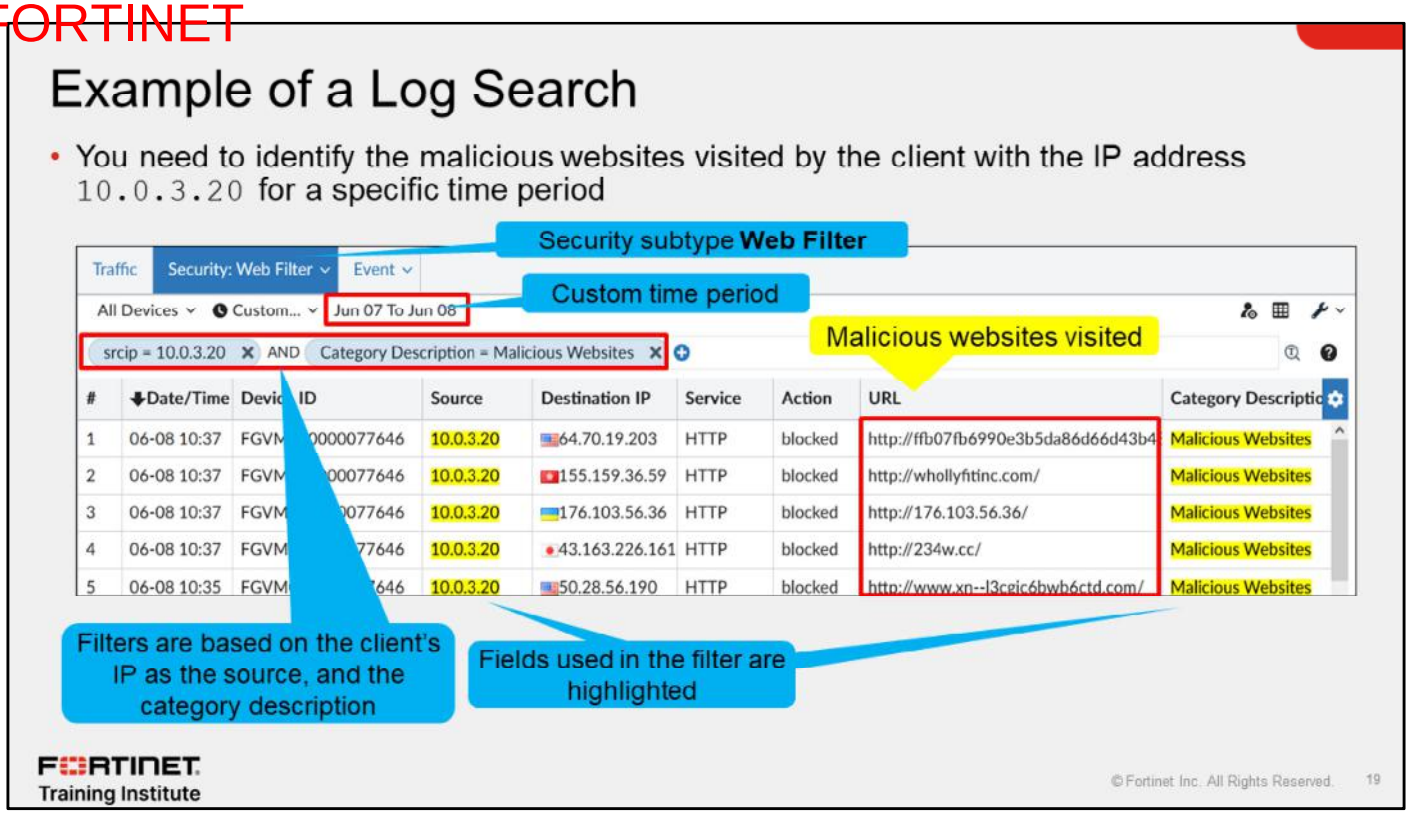
- Filter mode: Click the filter search bar and define your search criteria using the GUI.
- Text mode: Type in your filter and condition manually, or pick a filter from history.

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



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

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

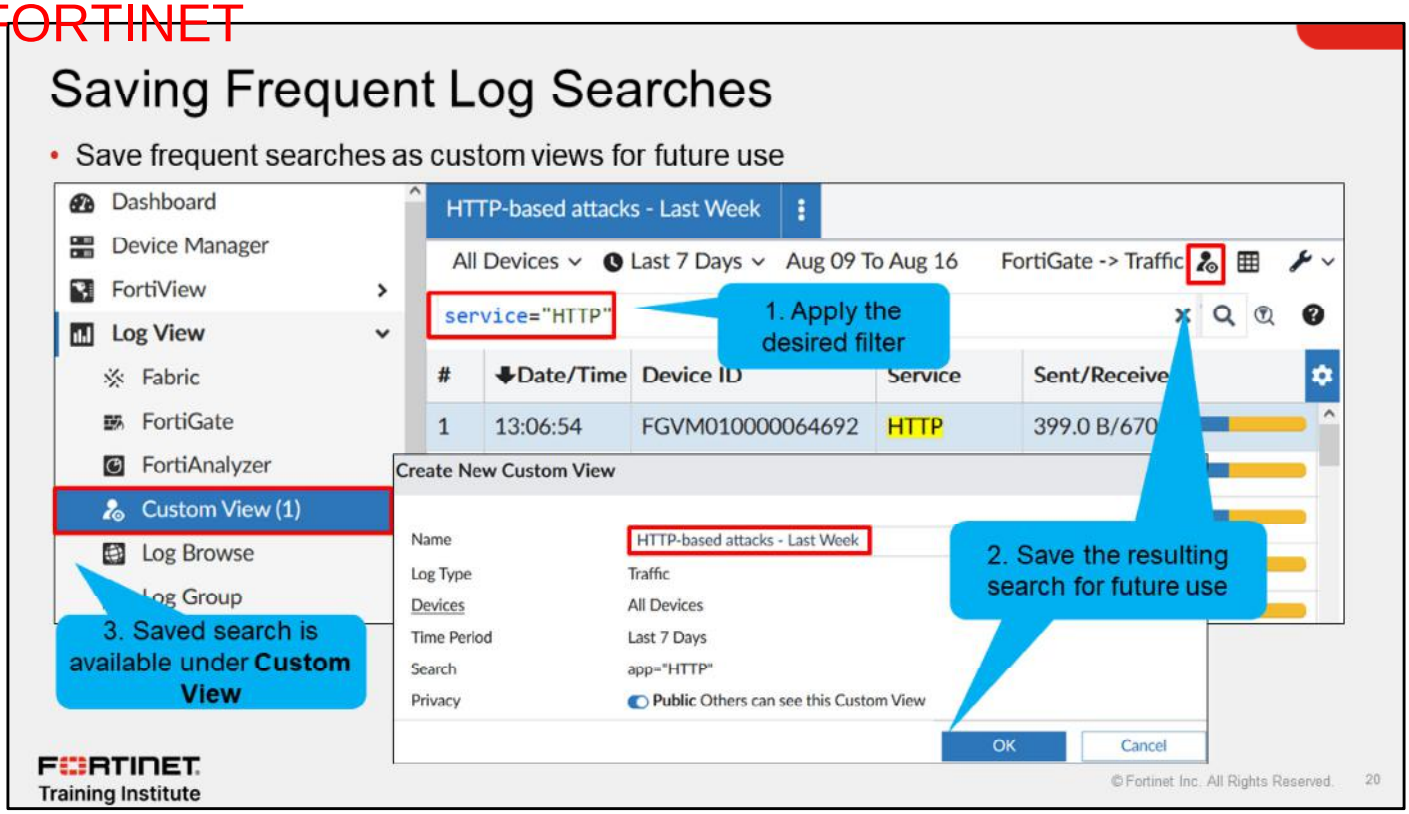


This slide illustrates an example of a filter applied in **Log View**. You can easily add a filter by right-clicking the desired log field and select if you want that value included or excluded from the logs displayed.

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

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

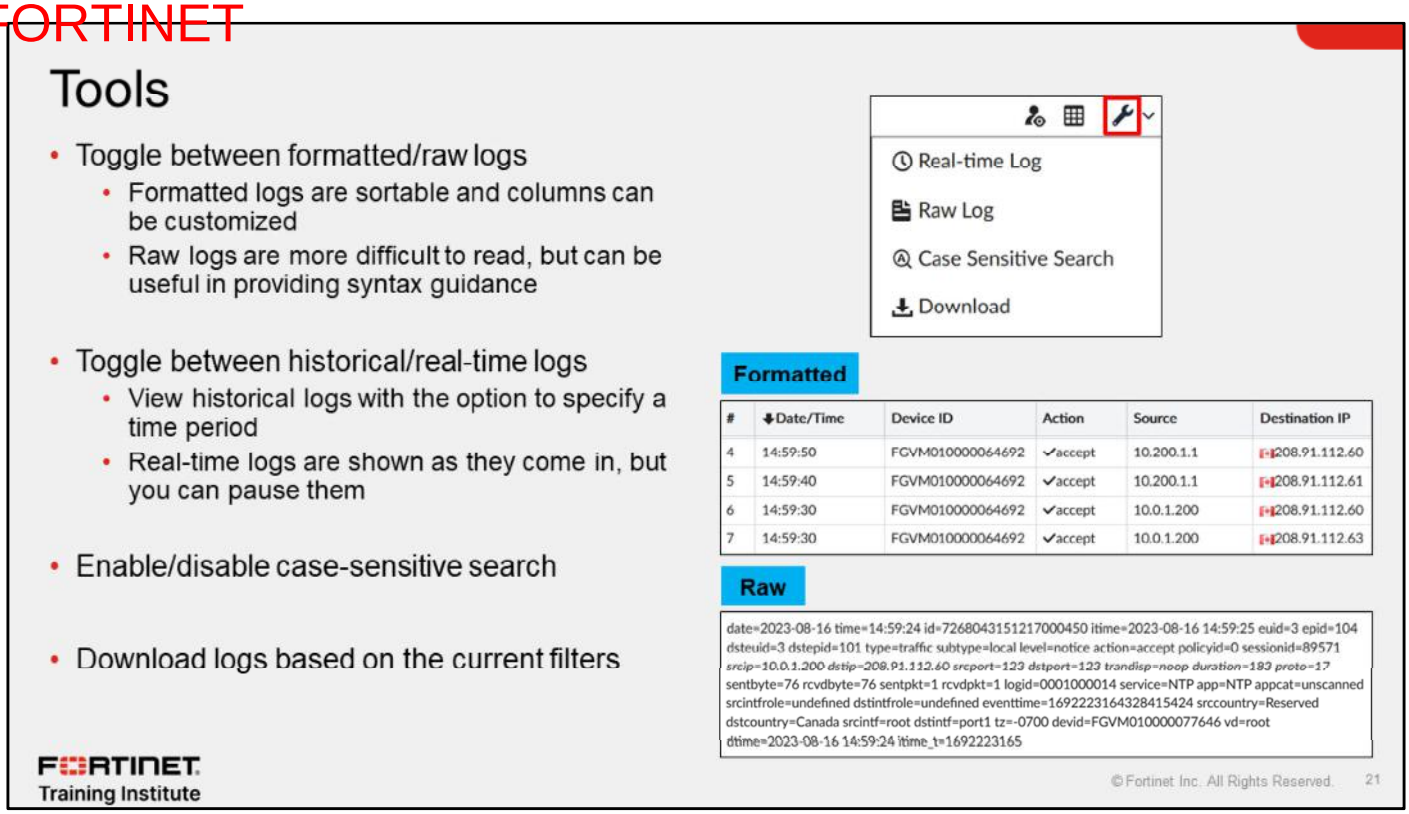
If you need more granular results, you can always add more filters or edit the current ones.



You can save frequent searches as custom views using the **Custom View** icon on the tool bar. This will save you, and your team, time when performing future investigations with similar search parameters. Saved searches are especially useful, for example, when you need to use longer filters frequently, or when specific time frames are part of the filter.

To save a search, apply the required filters, conduct your search, and then save it as a custom view. Custom views are public by default, but you can choose to make the ones you create private.

This slide shows a custom view that includes all HTTP traffic logs received over the last seven days.

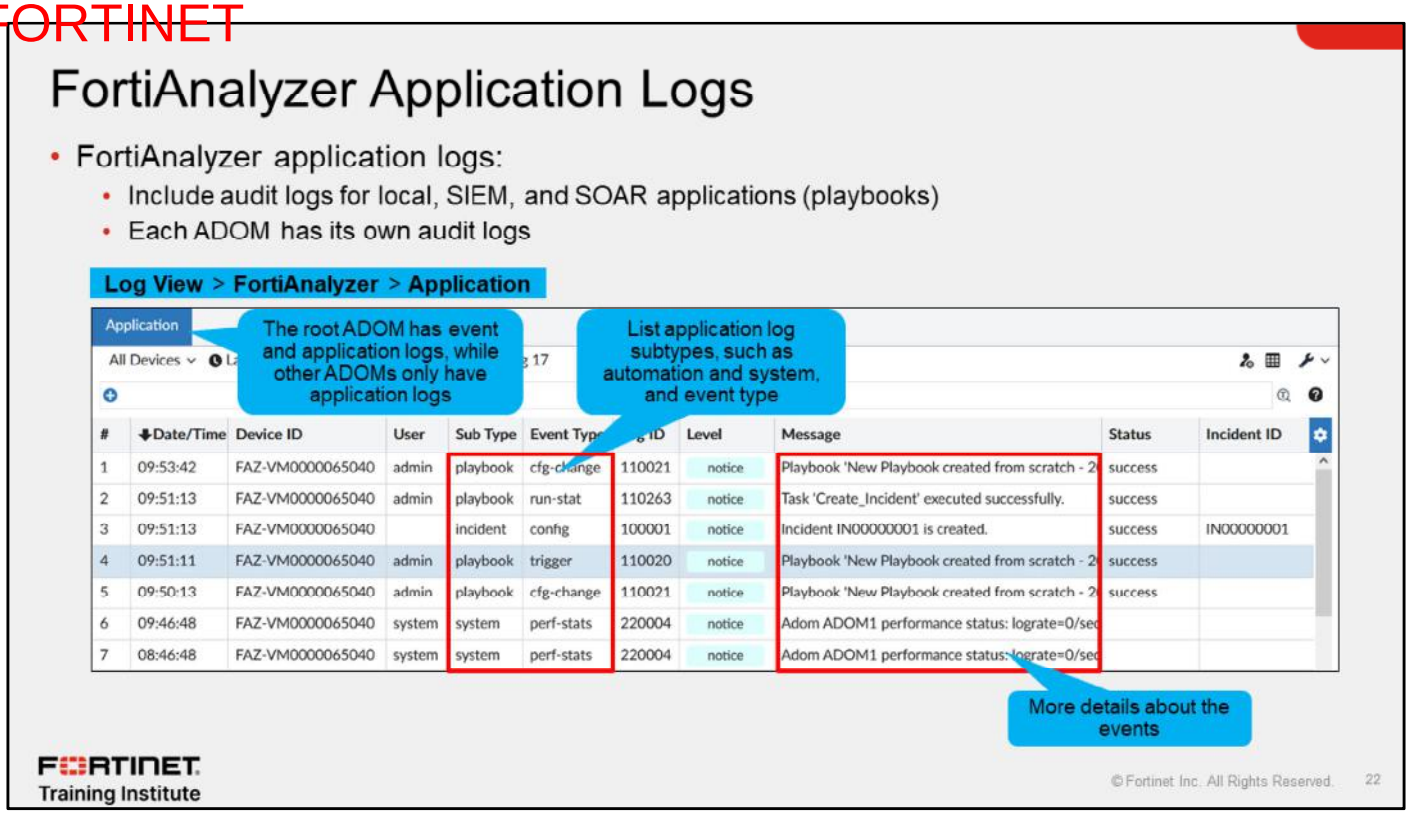


The **Tools** drop-down list provides options for viewing, searching, and downloading your logs.

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

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

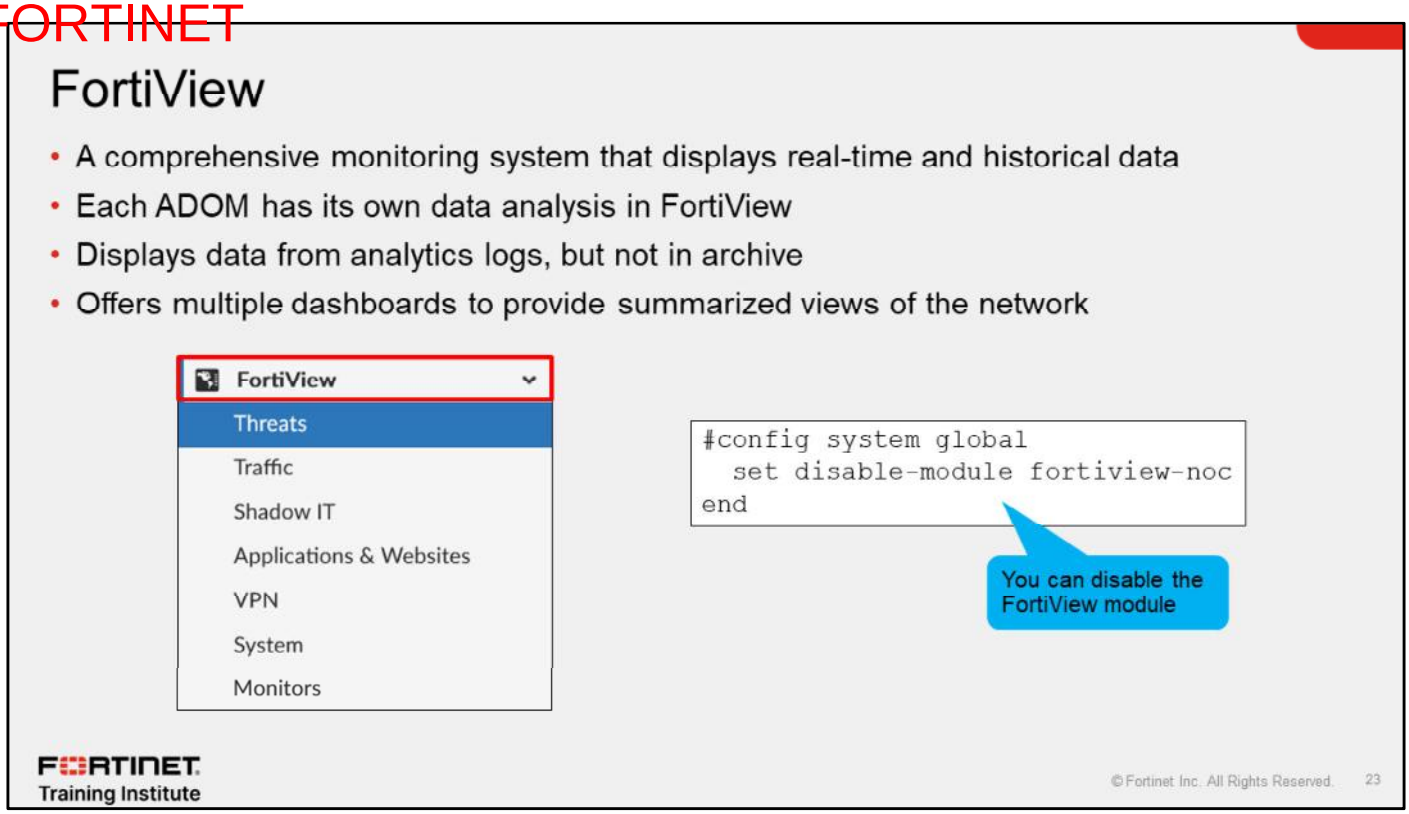
You can enable or disable case-sensitive searching to narrow down a query. You can also download logs, based on the current filters, as a text or CSV file.



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

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

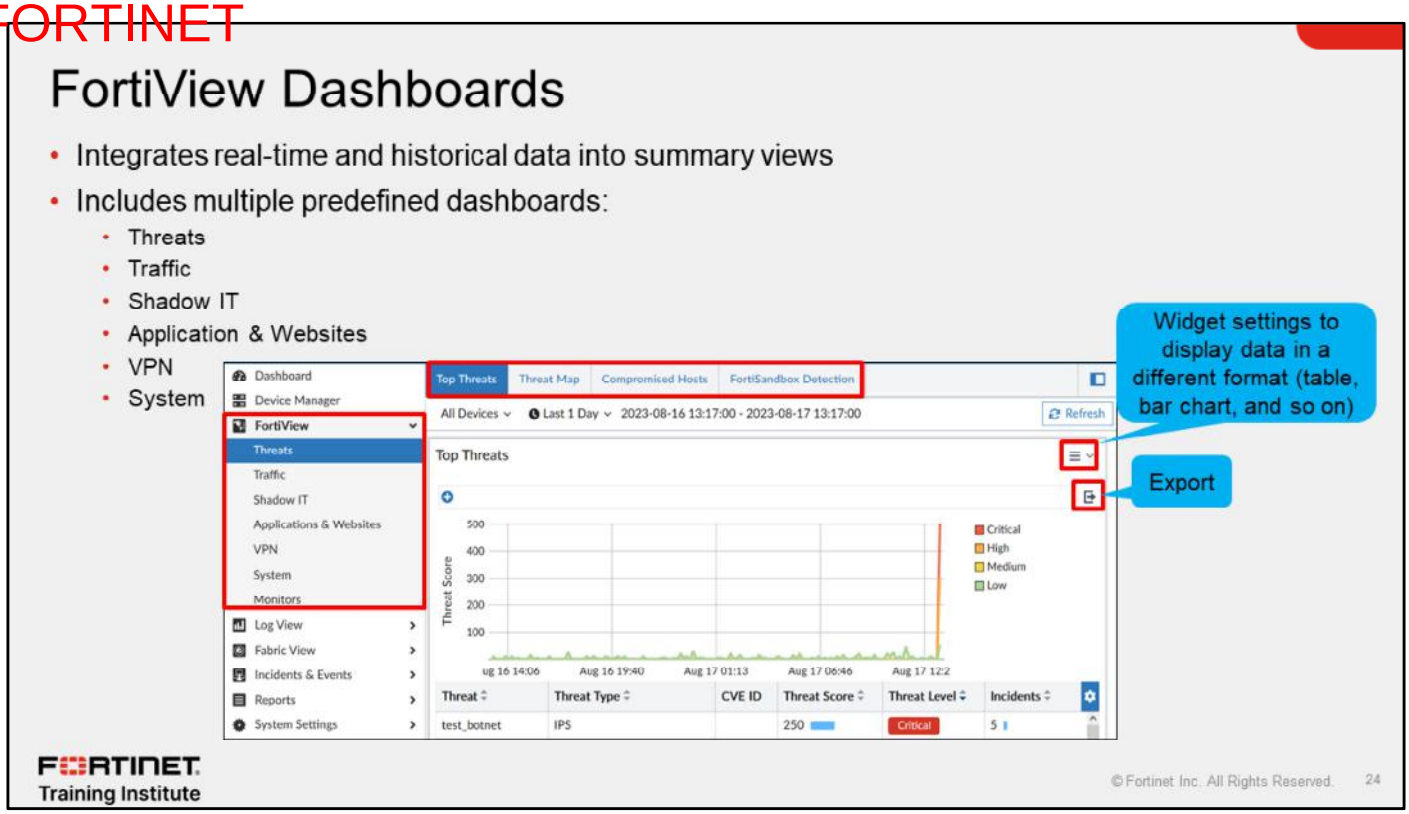
On this slide, you can see several logs that show that multiple automation tasks have succeeded. You also see the log rates of ADOM1.



FortiView is a comprehensive monitoring system that displays real-time and historical data. It offers multiple dashboards to provide summarized 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 on the FortiView pane, so ensure you are in the correct ADOM before viewing the contents of FortiView panes.

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

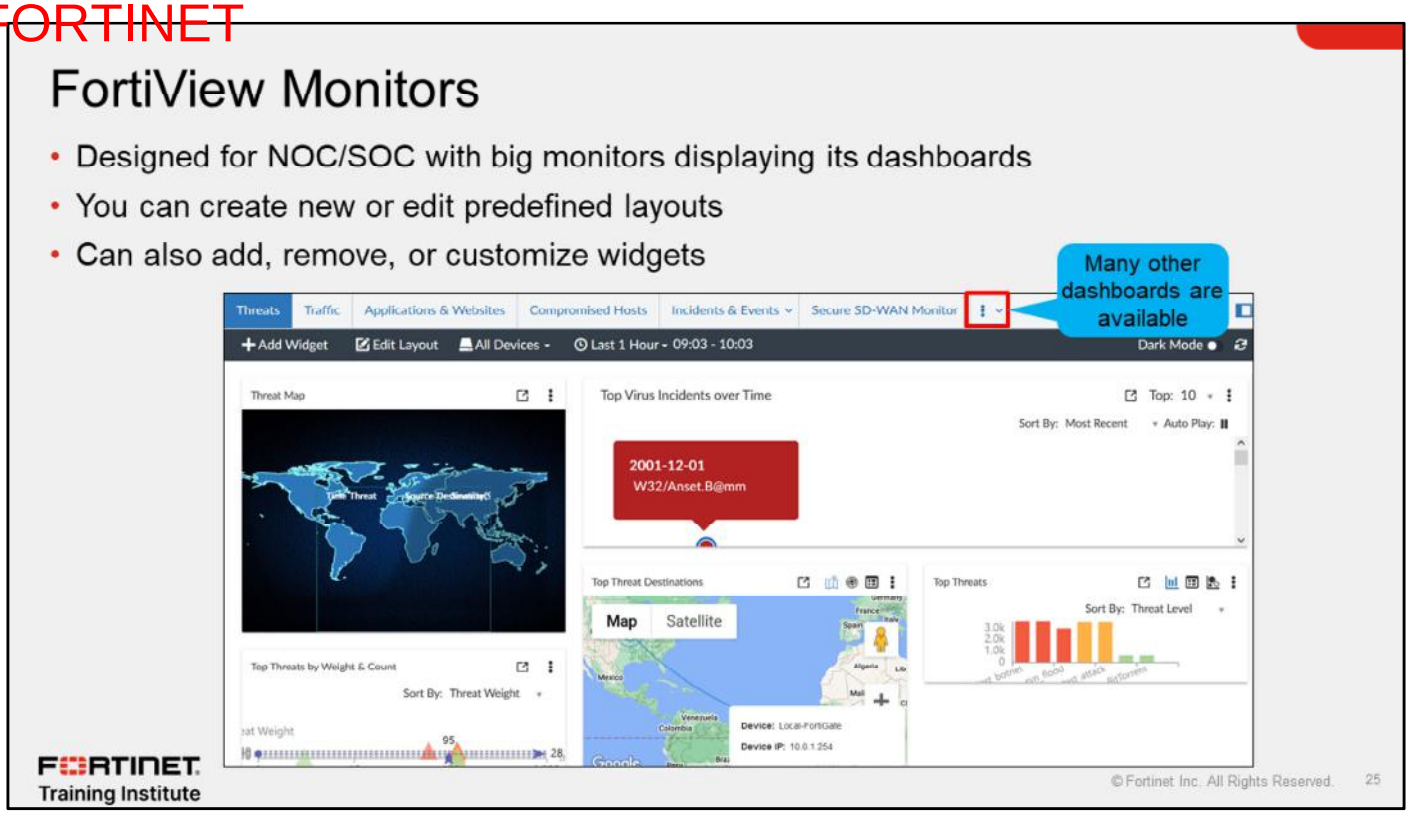


FortiView includes multiple dashboards to summarize different aspects of the network:

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

FortiView allows you to use multiple filters in the consoles, enabling you to narrow your view to a specific time, by user ID or local IP address, by application, and others. You can use it to investigate traffic activity, such as user uploads and downloads, or videos watched on YouTube on a network-wide user group or on an individual-user level.

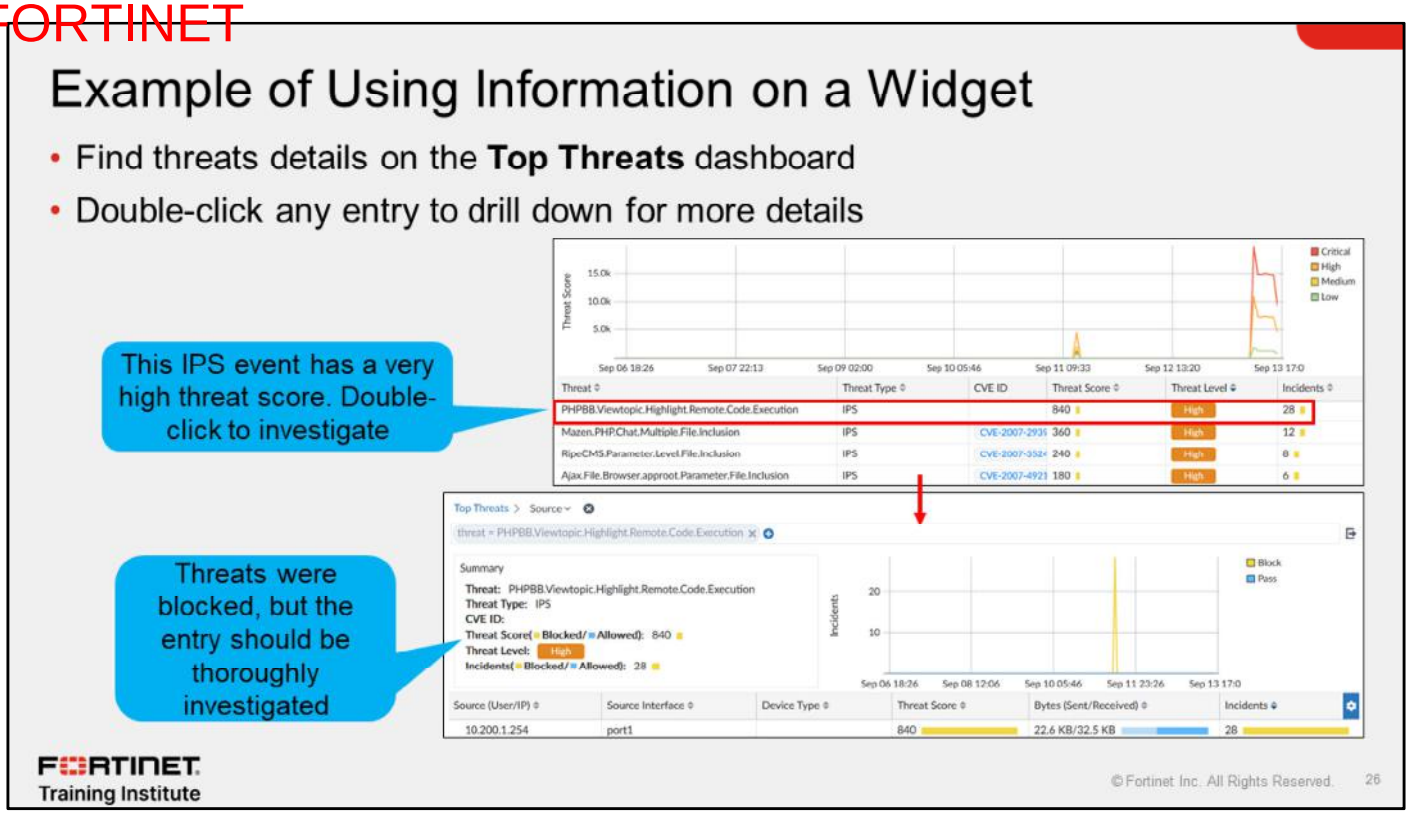
You can also export FortiView information as a PDF file, or create a chart to use in your own reports.



The **Monitors** function is designed for NOCs and SOCs to display multiple dashboards on large monitors. Centralized monitoring and awareness help you to effectively monitor network events, threats, and security alerts.

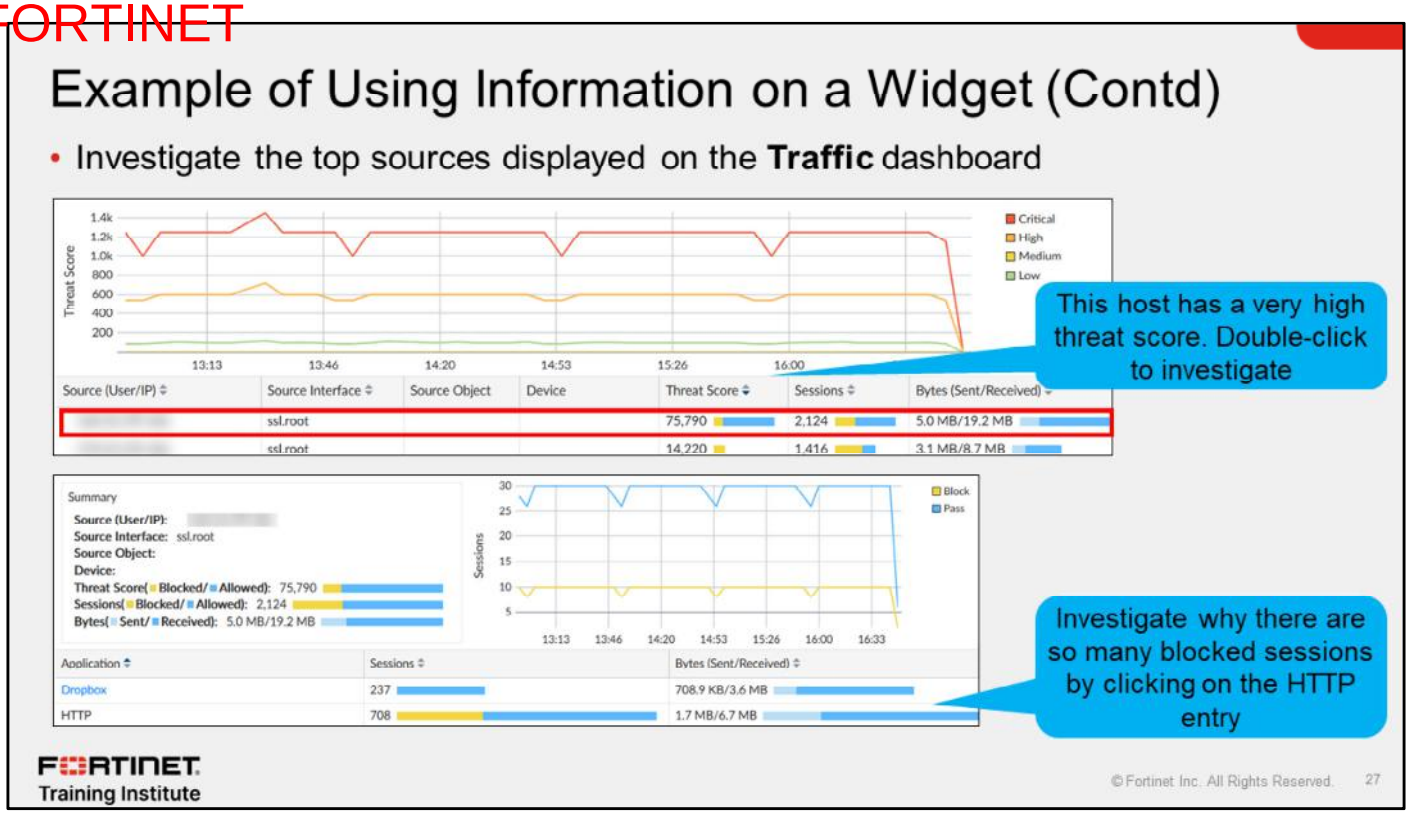
Dashboards display both real-time monitoring and historical trends using widgets that you can remove, resize, and customize. You can also add new widgets to the dashboards. You can choose which dashboards you want to display, and configure key dashboards to be larger than other dashboards. If the predefined dashboards do not fulfill your requirements, you can create custom views.

For a full list of predefined monitor dashboards and available widgets, refer to the *FortiAnalyzer Administration Guide*.



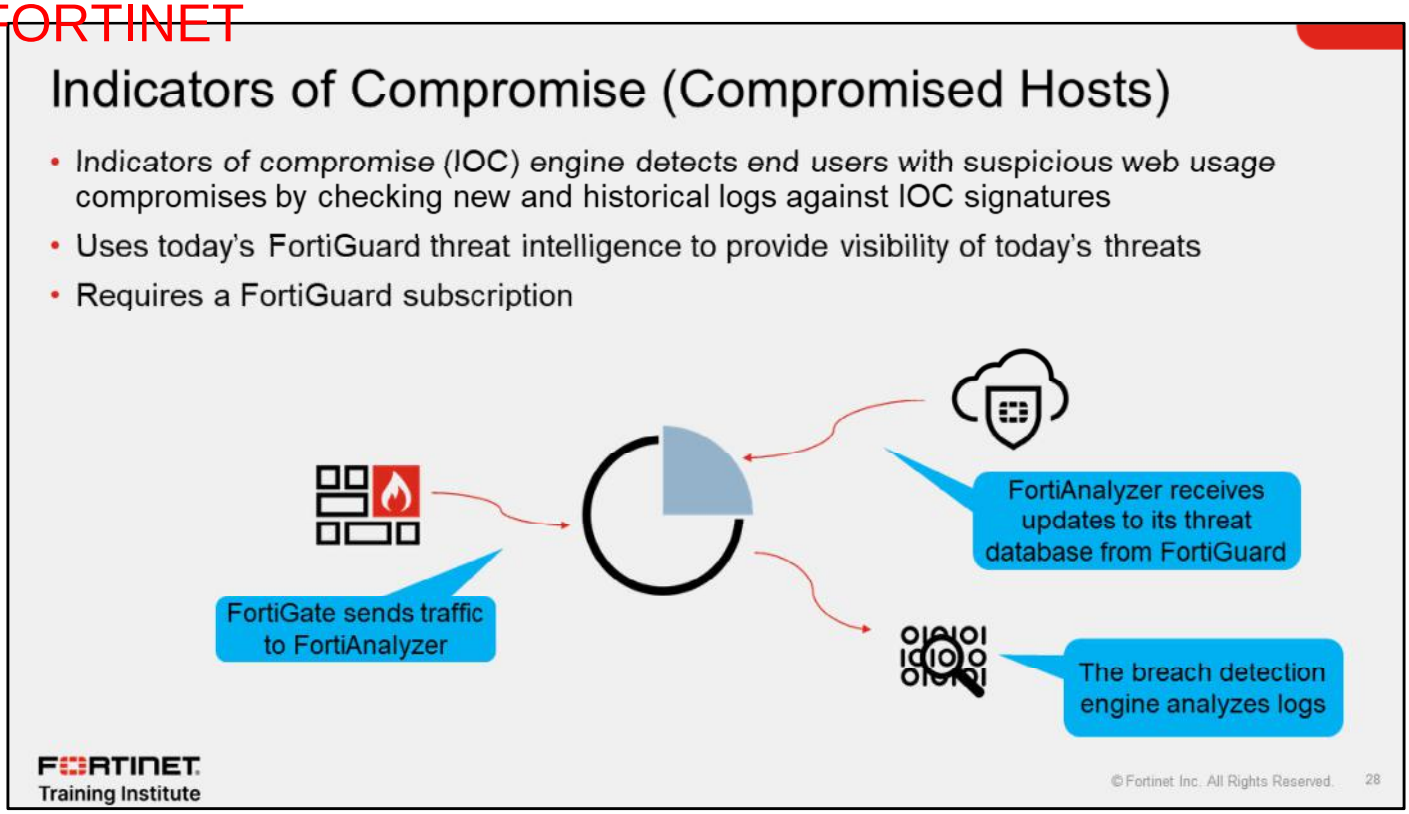
From the information displayed on a widget, you can find more details about a specific entry.

For example, 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. Double-clicking that entry will provide more details, like the source IP addresses related to this traffic. In this example, only one IP address is listed. This host has likely been compromised, and the analyst should report the findings. The IPS threats listed in the widget also have their corresponding CVE ID number hyperlinked, which you can click to read more about the attack vectors, suggested impact, vulnerable software, and more.



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

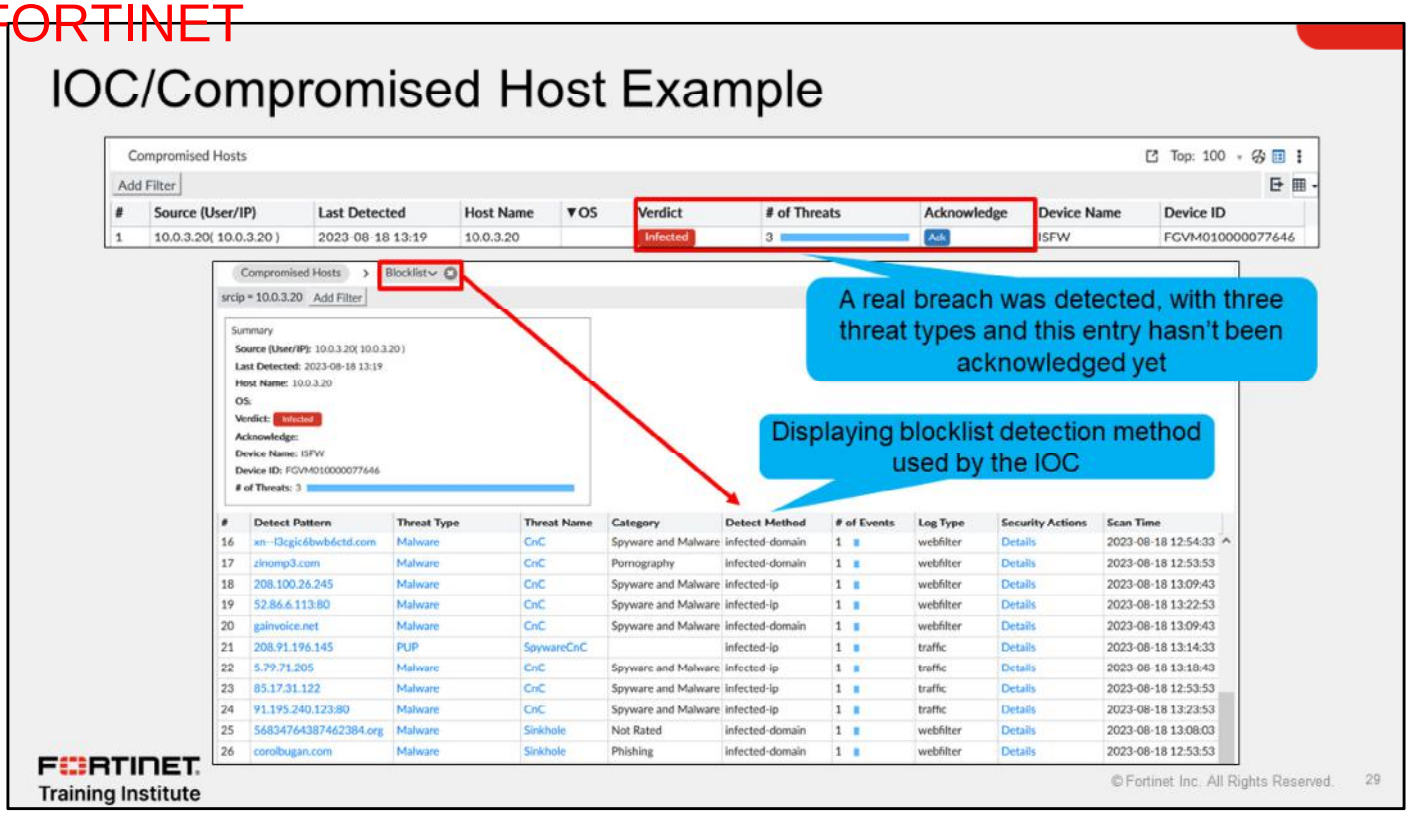
For example, on this slide, the **Top Sources** widget was enlarged and customized to display the information in a table format and with full view. The top source on the list is a host accessing the network through SSL VPN, with a very high threat score. Double-clicking that host entry will provide more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



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 filter, DNS, and traffic logs on the FortiGate for breach detection. It is updated daily to reflect the real-world threat landscape. Note that antivirus logs, IPS logs, and so on, won't be used since those threats have already been detected or prevented by these services on FortiGate. When a threat match is found, a threat score is given to the end user based on the overall ranking score. When the check is completed, FortiAnalyzer aggregates all the threat scores of an end user and gives its verdict on the overall IOC of the end user. The verdict can be one of the following:

- **Infected**: indicates a real breach. A match or matches of the blacklisted IPs or domain generation algorithms (DGAs) have been found in the web logs.
- **Suspicious**: indicates a possible breach with varying degrees of confidence.



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

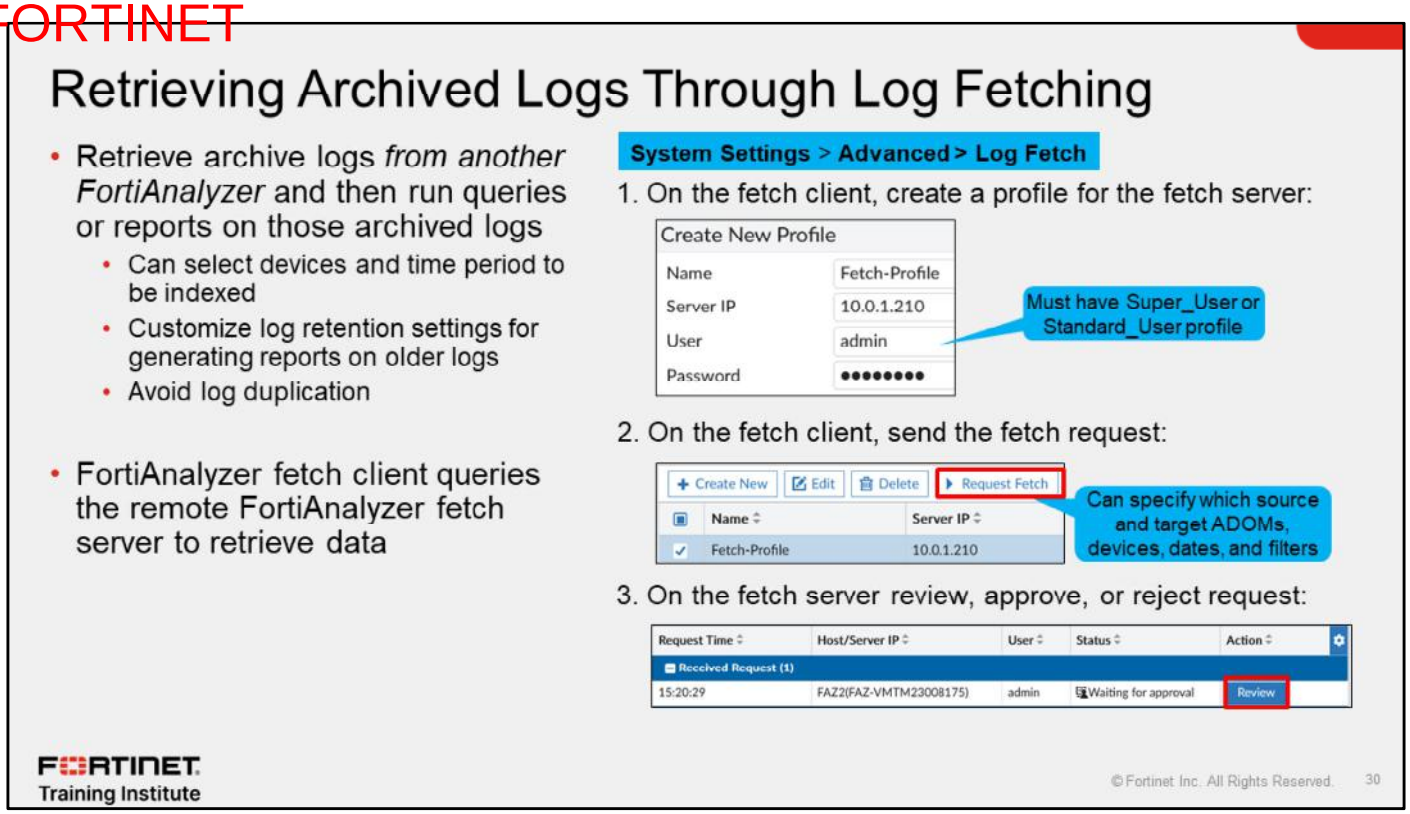
On the IOC FortiView, you can also:

- 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 to not show them. A short comment can be added when acknowledging an entry.
- Double-click an entry to drill down and view threat details.

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

- Blocklist, which indicates items marked as infected after checking the blocklist included in the IOC database downloaded from FortiGuard. You can verify that this traffic was blocked by clicking **Details** under the **Security Actions** column. If you believe that the IP address or domain listed under the **Detect Pattern** column is a valid one, you can report it as misrated by clicking 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**.

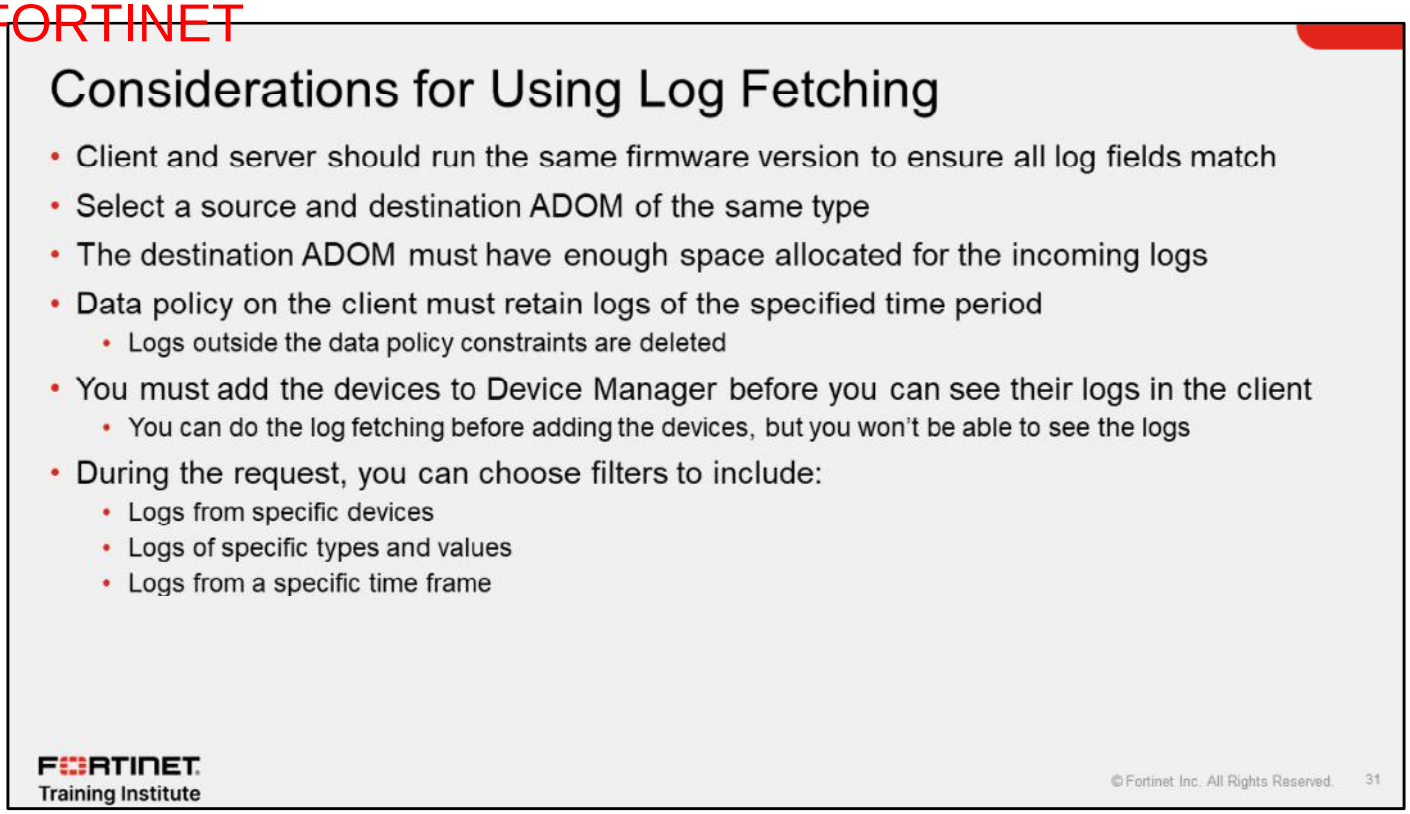


Using FortiAnalyzer, you can enable log fetching. This allows FortiAnalyzer to fetch the archived logs of specified devices from another FortiAnalyzer, index the data, and you can then run queries or reports on for forensic analysis. Log fetching greatly simplifies the generation of reports based upon 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

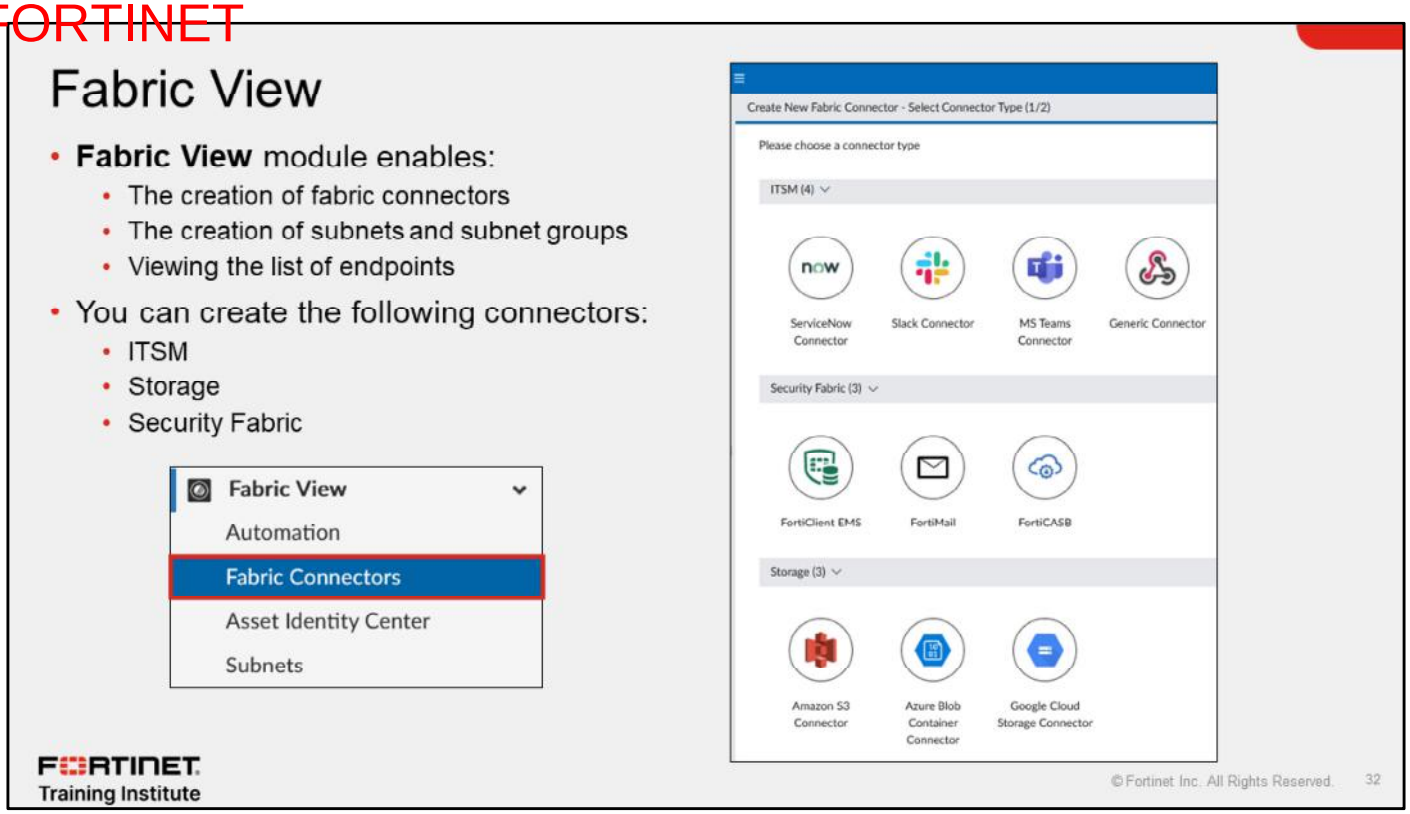
The FortiAnalyzer device that fetches logs operates as the fetch client, and the other FortiAnalyzer device that sends logs operates as the fetch server. Log fetching can happen only between two FortiAnalyzer devices. A FortiAnalyzer device can perform either the fetch server or client role, and it can 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 time frame configured.
- The incoming logs will be visible on the client only if the corresponding devices are added to Device Manager.
- Select only the required logs by using the available filters in the request dialog window.

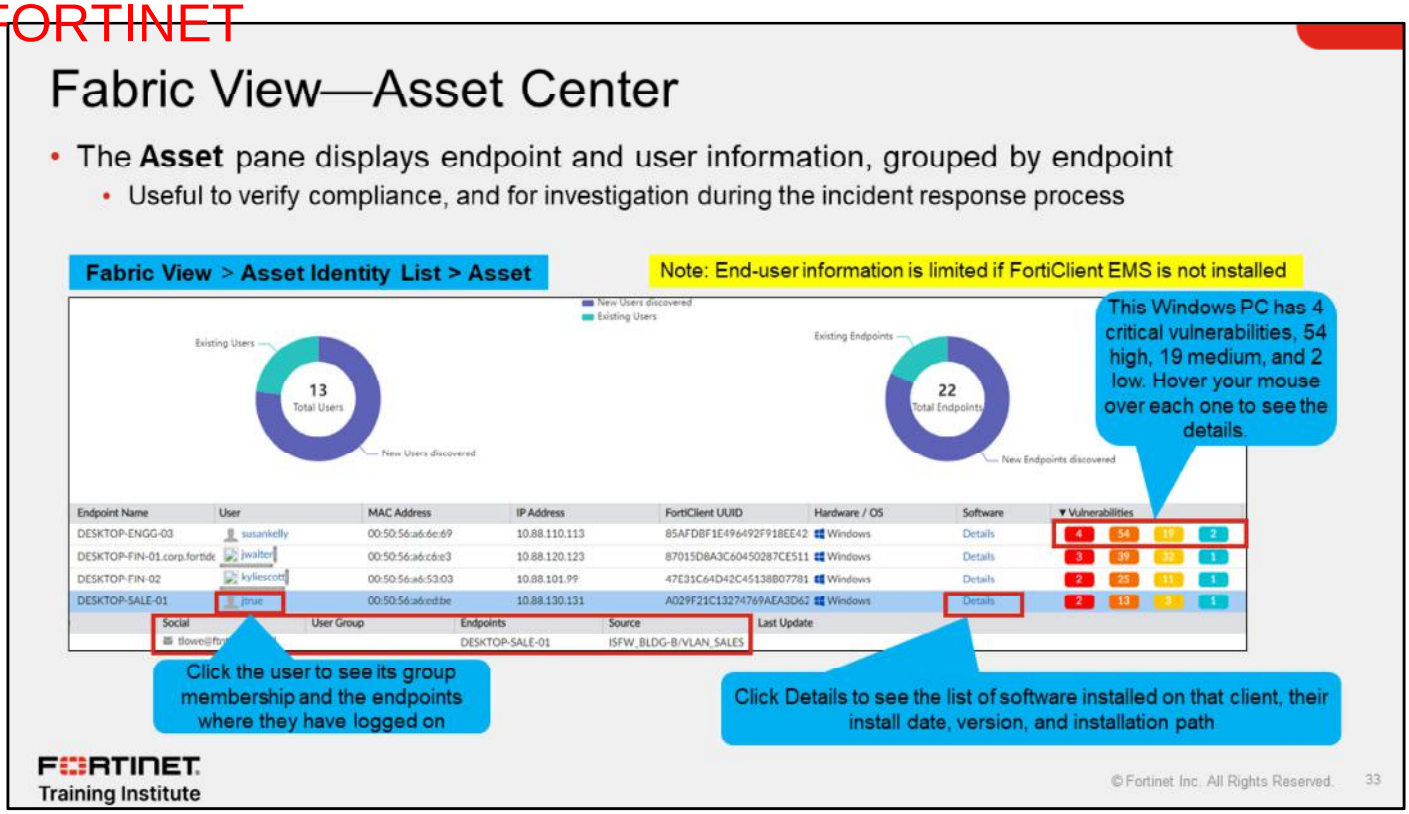


You can use the **Fabric View** module to view a list of endpoints, create subnet and subnet groups, and create fabric connectors. You can use FortiAnalyzer to create the following three types of fabric connectors:

- ITSM connectors, which include ServiceNow, Slack, and Generic (webhook)
- Storage connectors, which include Amazon S3, Microsoft Azure Blob container, and Google Cloud Storage
- Security Fabric connectors, which include FortiClient EMS (to execute EMS operations on endpoints), FortiMail, and FortiCASB

Fabric connectors enrich incident response-related actions available on FortiAnalyzer. For example, the creation of a new FortiClient EMS connector will add new automation playbooks related to endpoint management. Automation is explored in another lesson.

Subnets and subnet groups can be used to limit the scope of event handlers and reports.

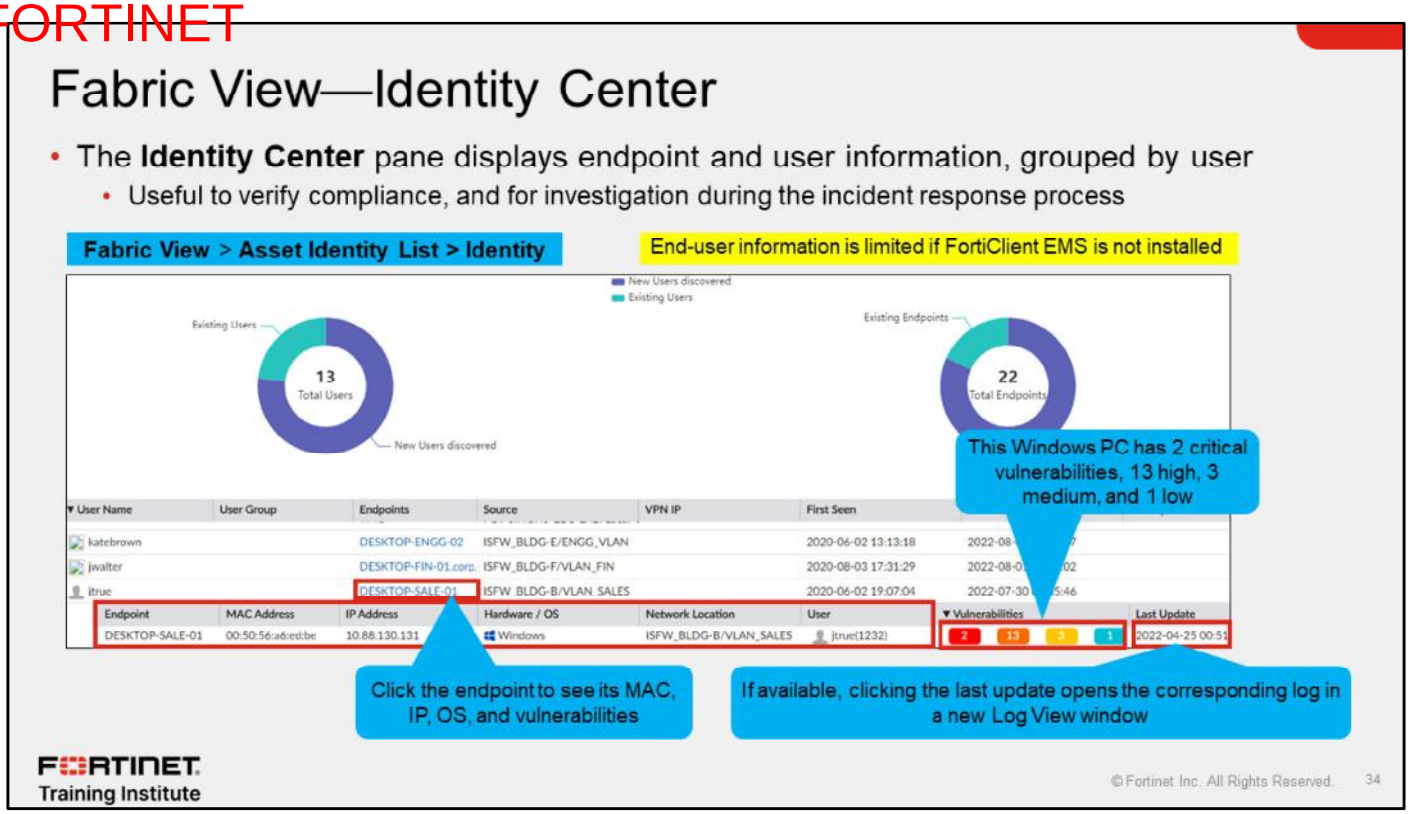


The **Fabric View** > **Asset Center** pane is the central location for security analysts to view endpoint and user information to make sure they are compliant. Endpoints are important assets in a network as they are the main entry points in a cybersecurity breach.

The **Asset Center** pane is useful for the following:
- Incident response: Check assets that are infected or vulnerable as part of your SOC analysis and incident response process.
- Compliance: Identify unknown and non-compliant users and endpoints.

For example, this slide shows information about four hosts that are running Microsoft Windows. Clicking **Details** displays all the software installed on each host. This can be used to identify unauthorized or unlicensed applications. In the **Vulnerabilities** column, details about missing updates is shown divided by severity. The vulnerabilities listed can be both for the operating system and the applications installed. This is extremely useful to identify systems that are not compliant with the update cycle of the company, and that represent a security weakness.

Note that the information displayed is limited if there is no FortiClient EMS in your installation:
- Endpoints are detected based on MAC address and displayed by IP address instead of host name.
- User-related information might not be available.
- Detailed information such as OS version, avatar, and social ID information is not available.



The **Fabric View** > **Identity Center** pane displays a list of users and endpoints in the network from relevant logs, and correlates them with FortiAnalyzer modules. The **Identity Center** is useful for user and endpoint mapping. Some users might use multiple endpoints in the network, endpoints might use different interfaces to connect, network interfaces might have multiple IP addresses, and so on.

A map of users and their endpoints gives you better visibility when you analyze logs, events, and incidents. This also helps with your reporting.

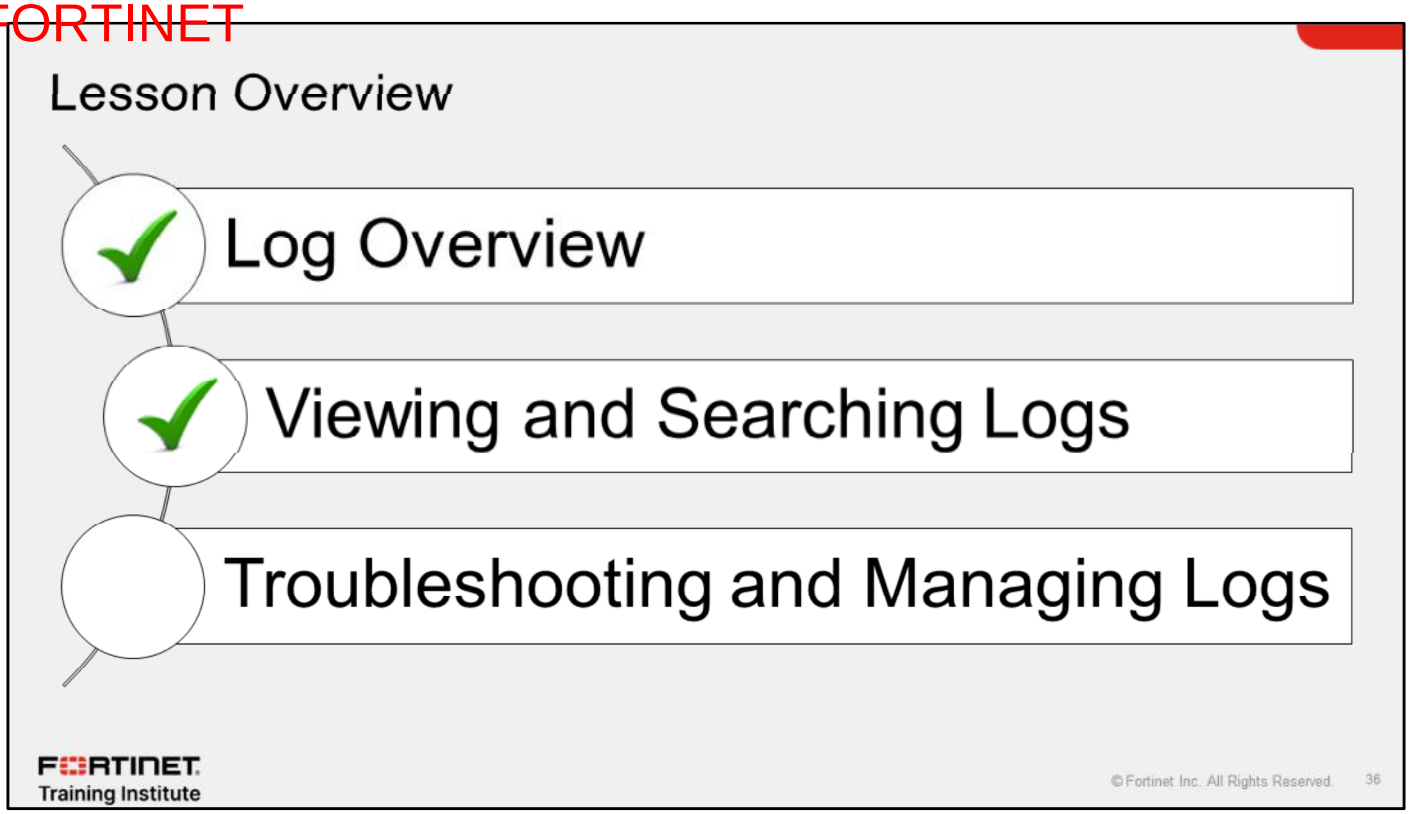
Note that end-user information is limited if there is no FortiClient EMS in your installation:
- Endpoints are detected based on MAC address and displayed by IP address instead of host name.
- User-related information might not be available.
- Detailed information such as OS version, avatar, and social ID information is not available.

Knowledge Check

1. Which FortiAnalyzer feature allows you to obtain the archive logs of specified devices from another FortiAnalyzer device?
   A. Log forwarding in aggregation mode
   ✓B. Log fetching

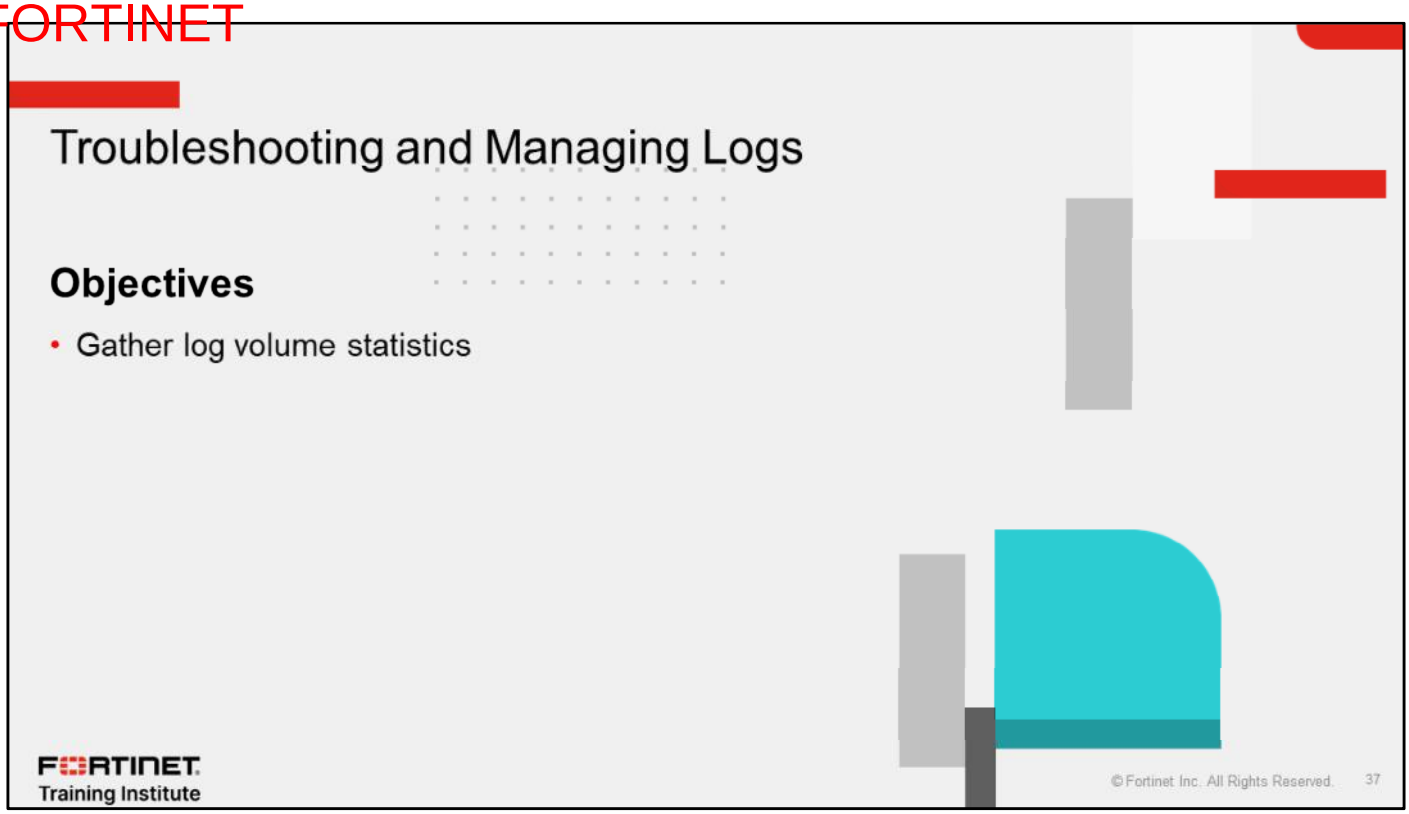
FORTINET Training Institute

 35



Good job! You now understand how to view and search your logs.

Now you will learn how to troubleshoot and manage your logs.



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

By demonstrating competence in gathering log statistics, you will be able to identify possible 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

 38

To understand your 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

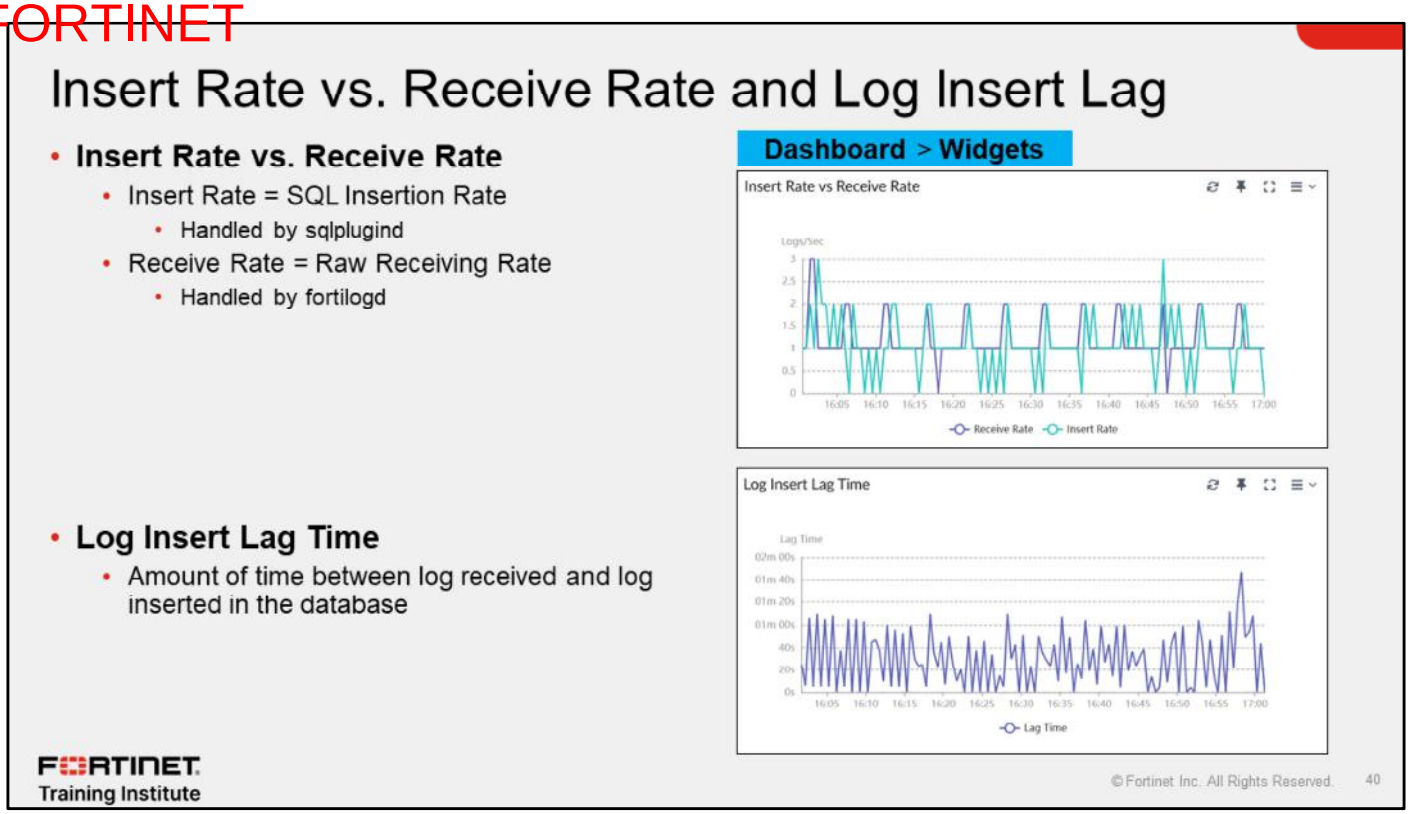
```
FAZVM64-KVM # diagnose fortilogd logvol-adom root
2022-08-22 2022-08-21 2022-08-20 2022-08-19 2022-08-18 2022-08-17 2022-08-16 average
adom 'root':
8.77 MB    10.15 MB   15.65 MB   17.68 MB   22.89 MB   22.64 MB   22.71 MB  17.21 MB
```

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

FORTINET Training Institute

 39

To understand your 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 the environments where the FortiAnalyzer administrator is using multiple ADOMs to manage multiple FortiGate devices, like in the case of managed security supervisor providers (MSSPs).



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** on 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. Usually, the difference between these parameters should be consistent. Ideally, the difference between these two parameters should be as small as possible, but variations during the day can be expected. Create a baseline during normal operation and compare 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.

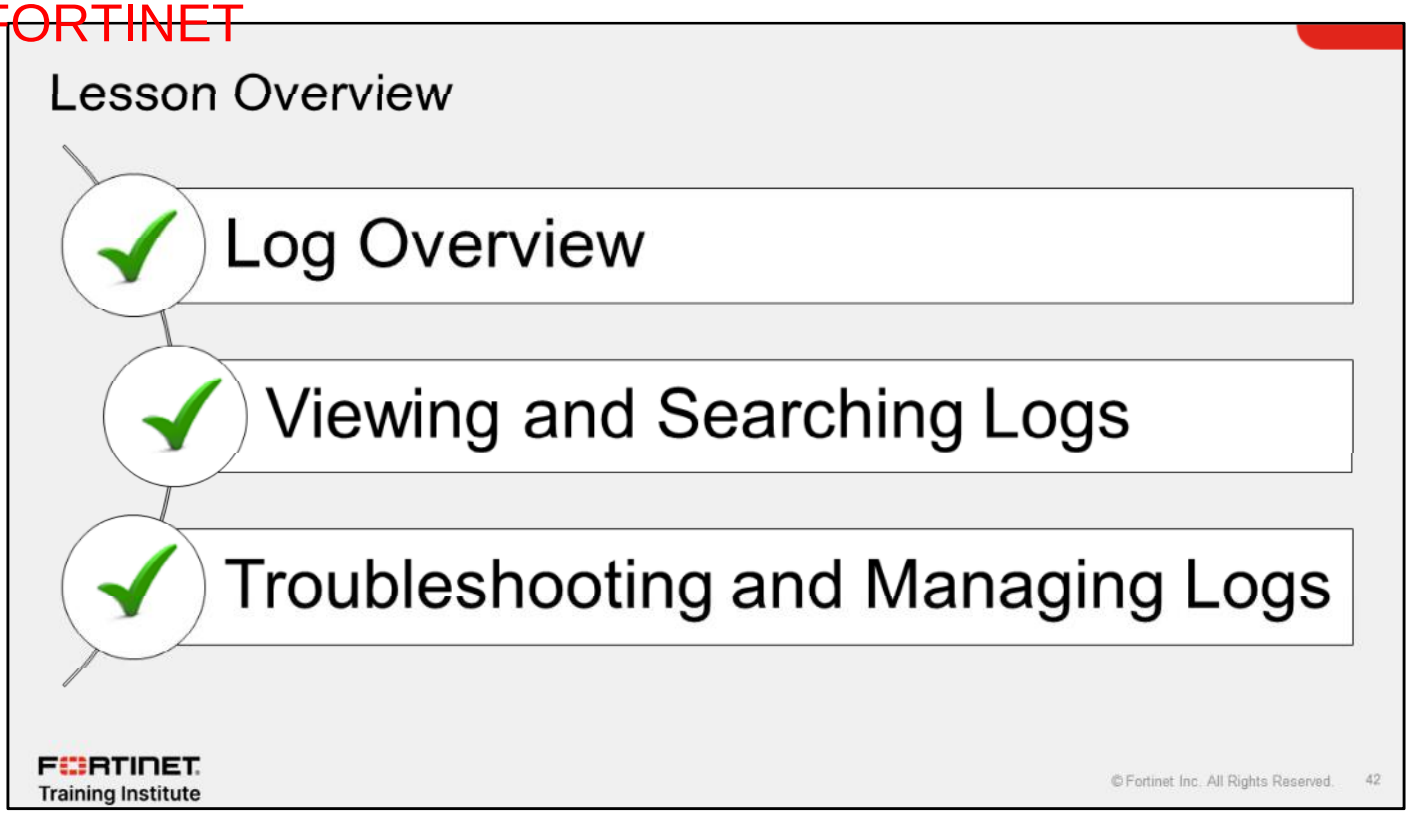
Knowledge Check

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

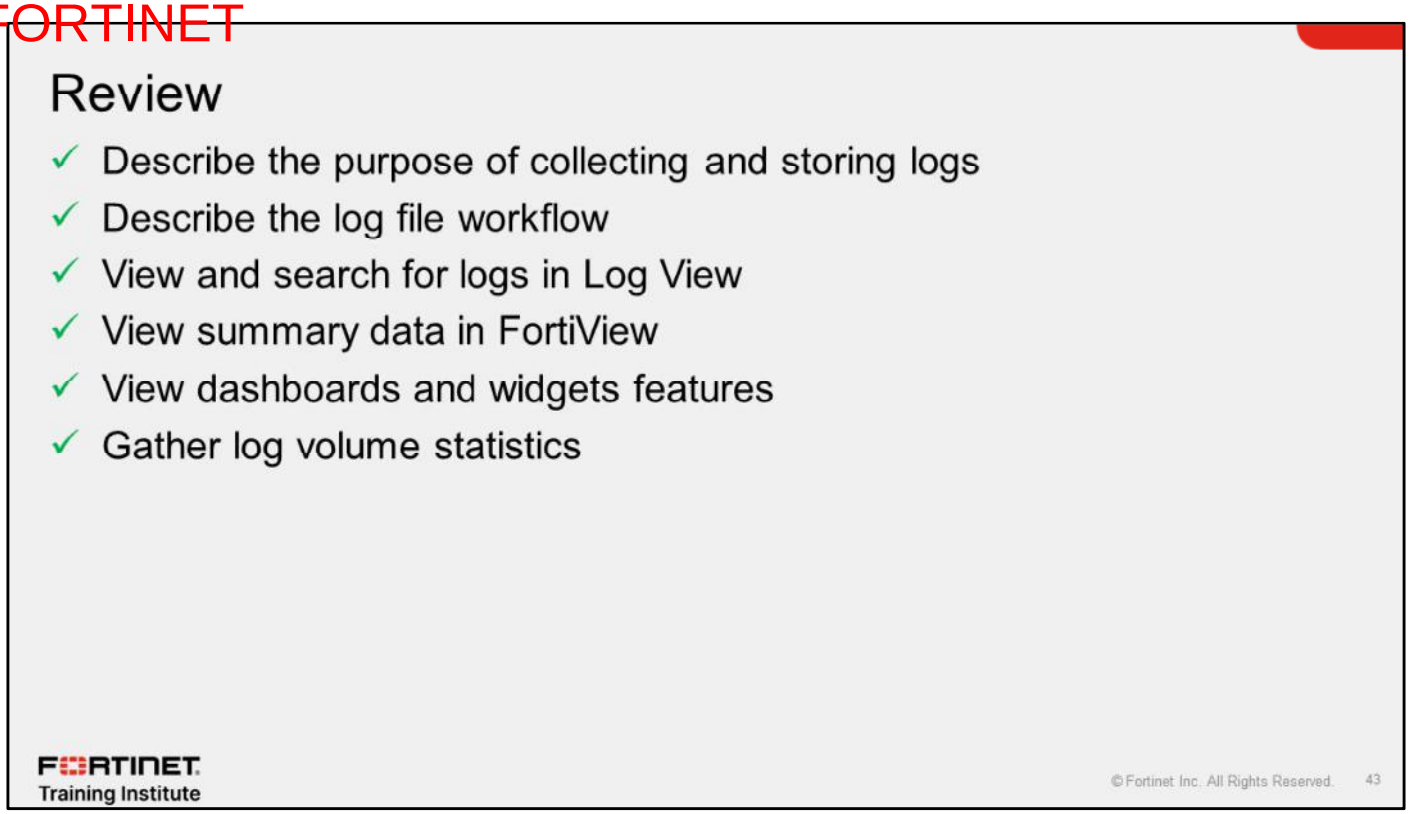
FORTINET Training Institute

 41



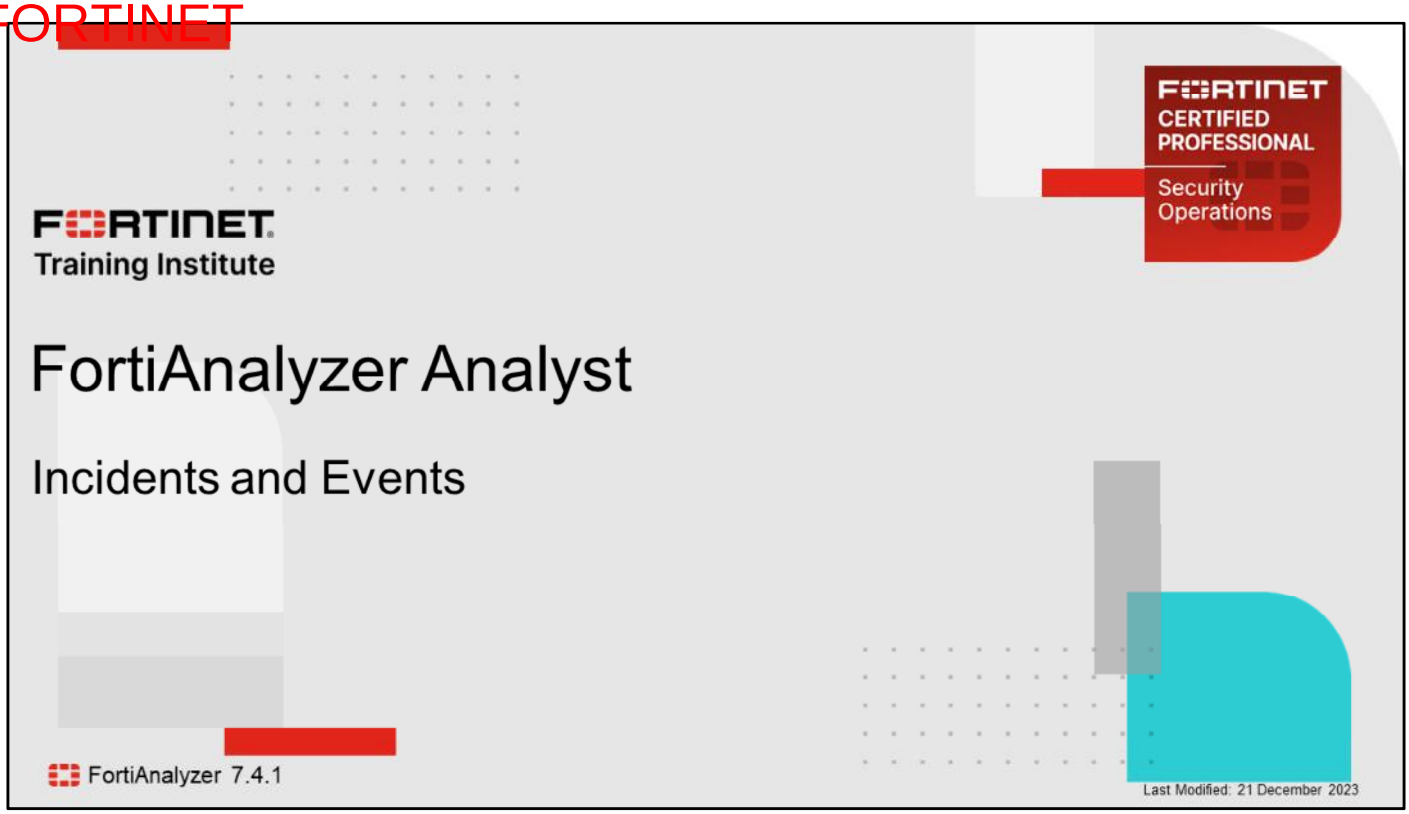
Congratulations! You have completed this lesson.

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

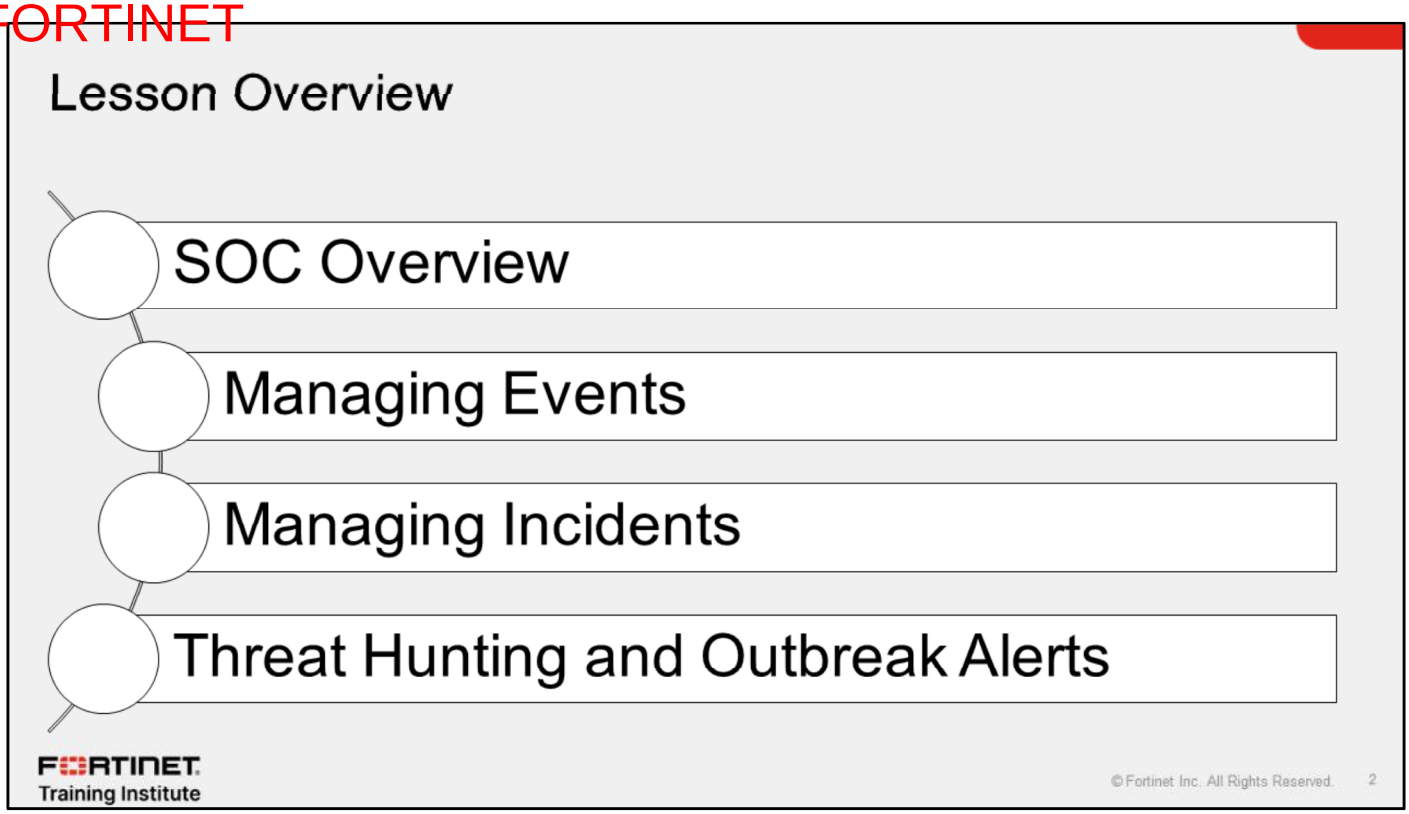


This slide shows the objectives that you covered in this lesson.

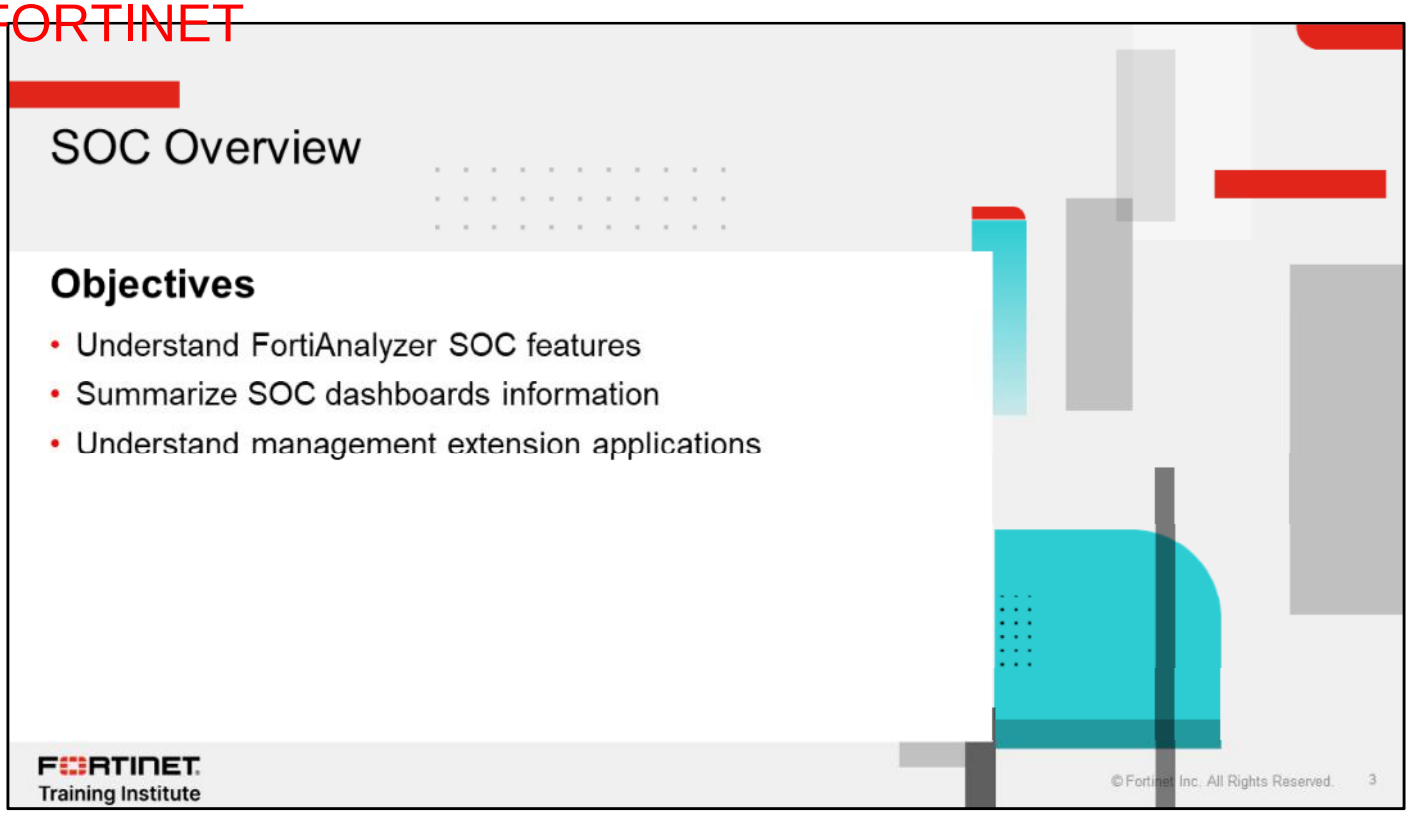
By mastering the objectives covered in this lesson, you learned how to use logs effectively in your system.



In this lesson, you will learn about the SOC features in FortiAnalyzer, and how to configure them.

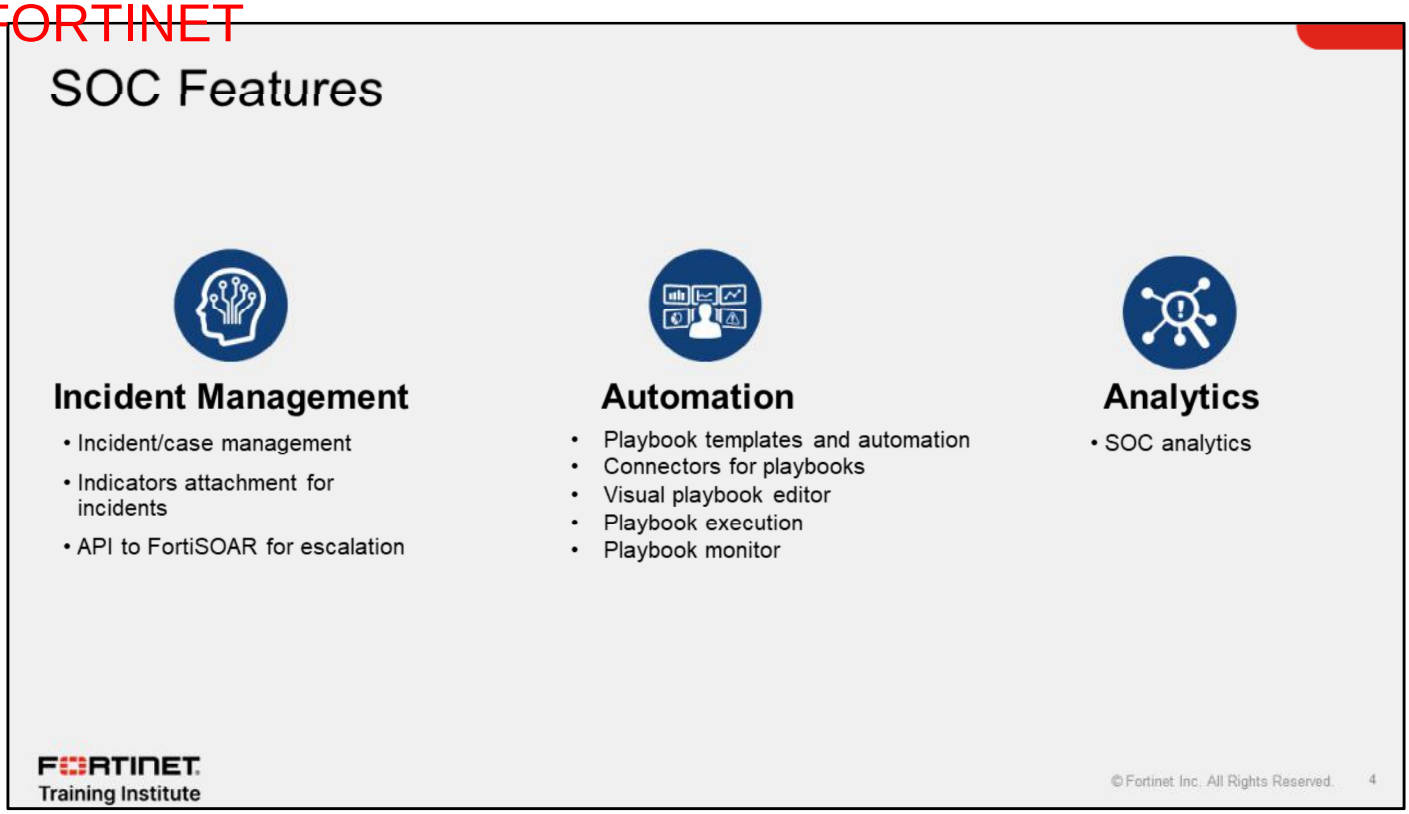


In this lesson, you will learn about the topics shown on this slide.



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

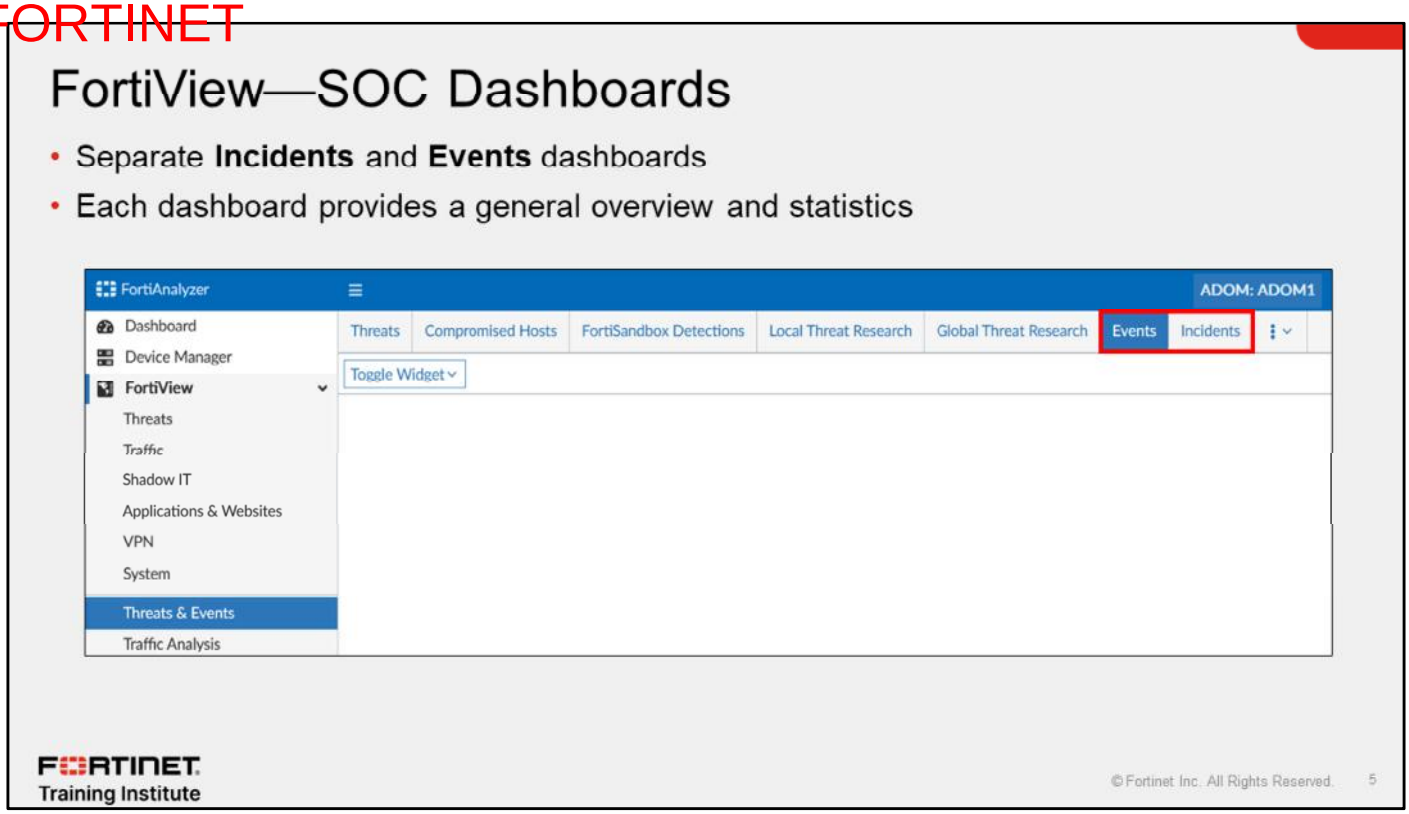
By demonstrating competence in understanding SOC features and SOC dashboards, you will be able to use them efficiently in your network.



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

FortiAnalyzer provides a more complete solution for modern SOC analysts that include:

- Incident management: Provides complete incident lifecycle management capabilities, including alerts, monitoring, and escalation.
- Automation: Run common tasks without any manual intervention, leading to a much more efficient operation.
- Fabric analytics: Provides visibility throughout the network from a single interface.

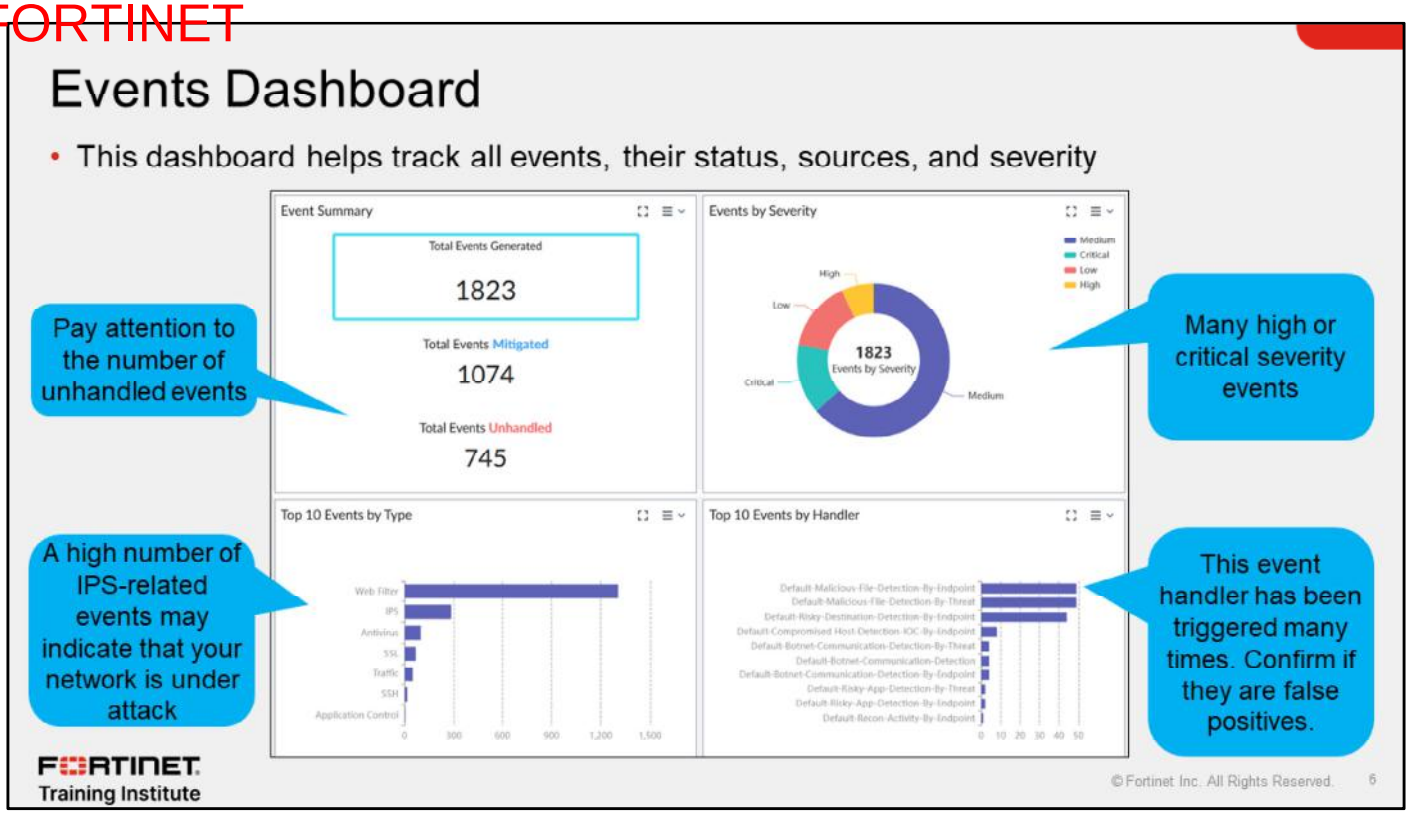


FortiView includes dashboards that provide a general overview and statistics about events and incidents in your environment. Data is presented in several formats and you can get more detail by hovering your mouse over a section of interest.

These dashboards enable customers to effectively monitor SOC productivity, and identify gaps to improve performance and efficiency.

Combined, these dashboards provide a good overview of how your SOC team is doing and if there are some areas that need to be improved.

These dashboards are read-only and not customizable. The information they display is updated automatically based on other actions that occur in the background, such as when new events are generated.

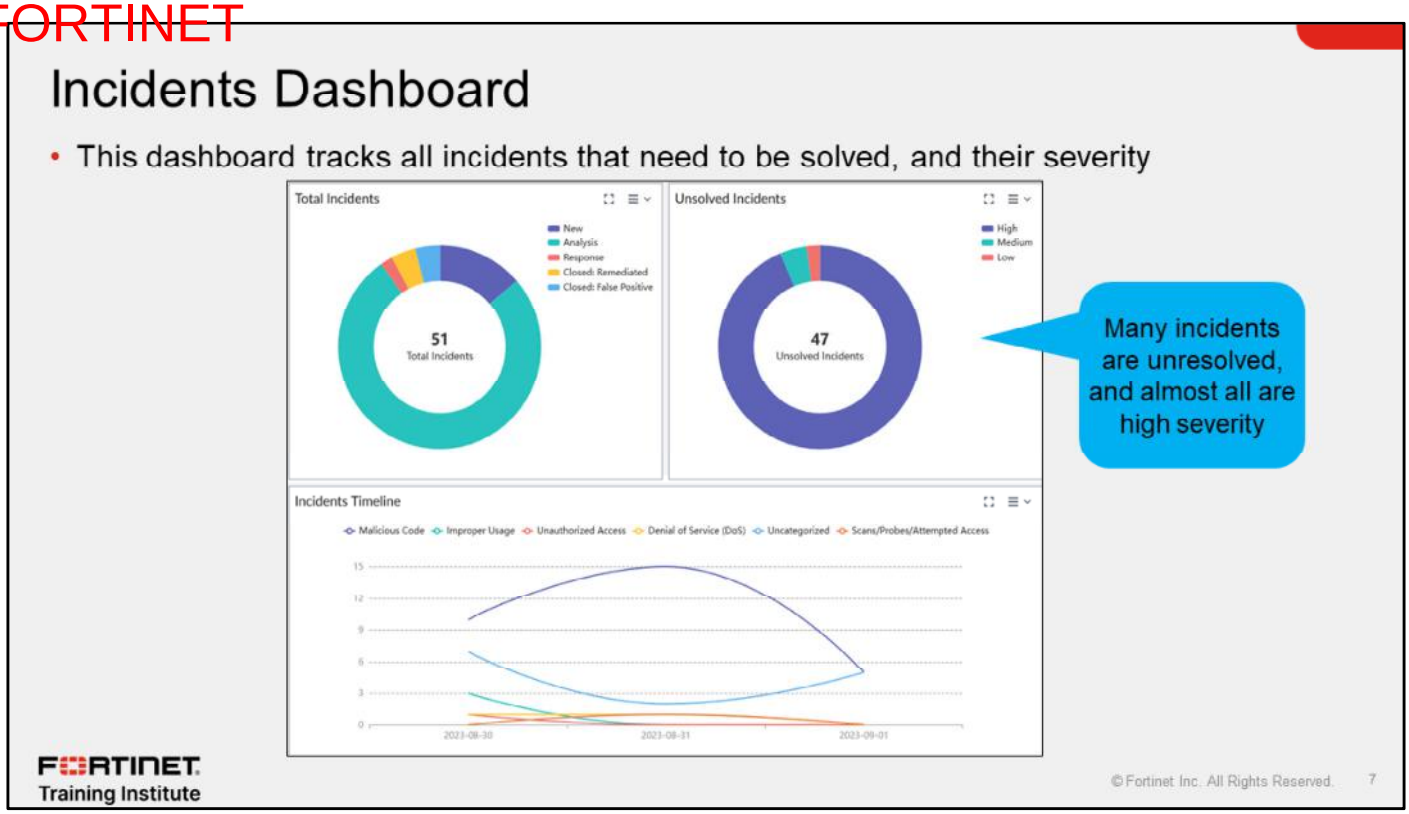


The **Events** dashboard includes **Event Summary**, **Events by Severity**, **Top 10 Events by Type**, and **Top 10 Events by Handler**.

Using this dashboard, the SOC team can identify which events to address with more urgency based on their severity and status, as well as keep track of the most common event types occurring in the network. The dashboard displays the information in several graphic formats, using different colors for each event category.

For example, this slide shows that approximately one-third of the events are classified as critical, and there are 745 unhandled events.

To manage events, you must use the **Event Monitor** section under **Incidents & Events**. You will learn about this later in this lesson.

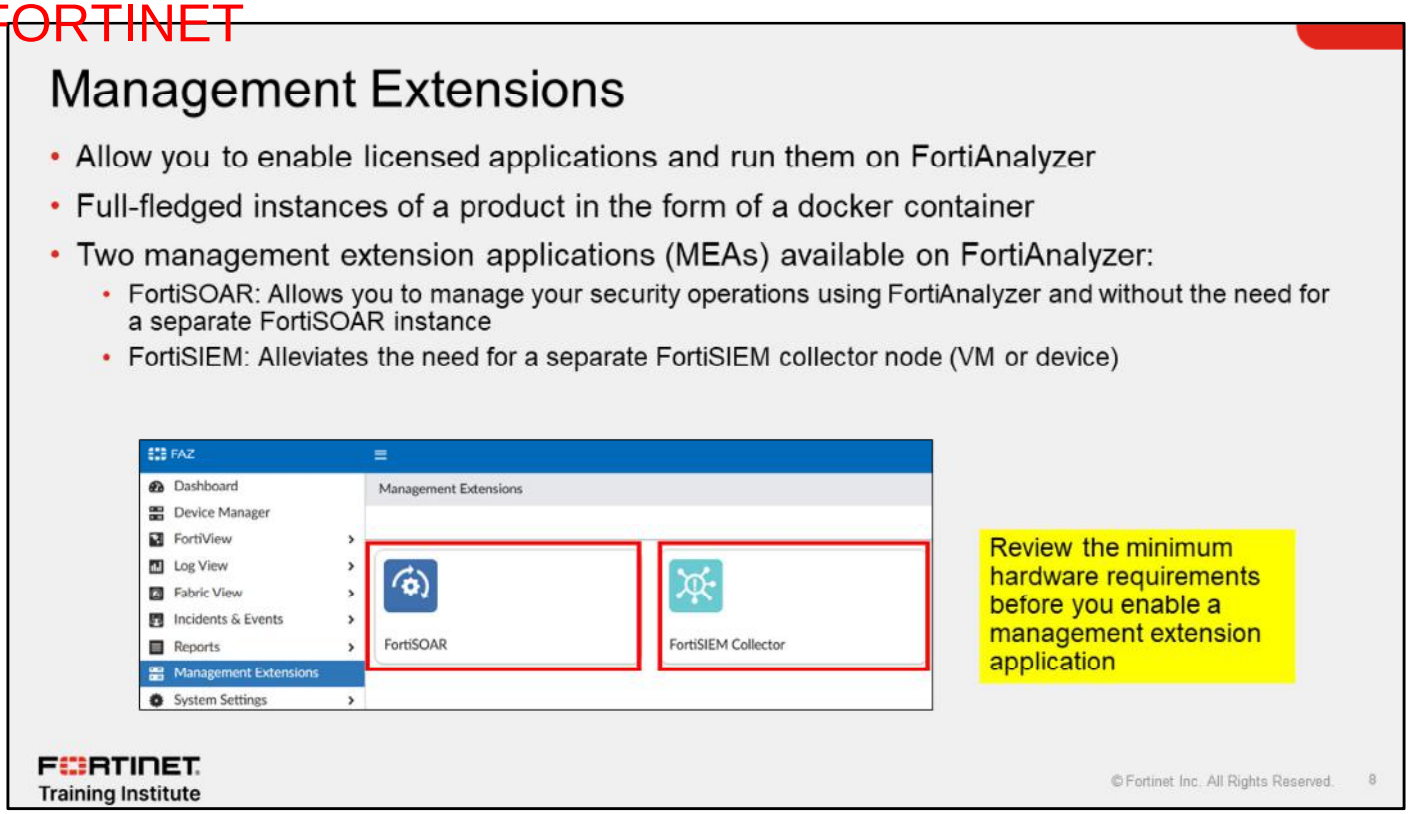


The **Incidents** dashboard includes **Total Incidents**, **Unsolved Incidents**, and **Incidents Timeline**.

This dashboard offers a clear representation of how many incidents need attention or are still being handled by the analysts. It also offers a color-coded representation of incident severity.

In the example shown on this slide, all the incidents are still unsolved despite most of them being high severity. In a real scenario, this would be unacceptable.

To start analyzing and eventually solving incidents, you must use the **Incidents** section under **Incidents & Events**. This is covered later in this lesson.



Management extensions allow you to enable licensed applications and run them on FortiAnalyzer.

A management extension application (MEA) is full-fledged running instance of a product in the form of a docker container. Installed MEAs enable you to use and monitor different solutions from Fortinet using a single pane of glass.

Two MEAs available:
- FortiSOAR: Includes a limited trial by default. Full functionality available when licensed.
- FortiSIEM: SIEM collector functionality only. Must be registered on a licensed FortiSIEM Supervisor.

The FortiSOAR MEA allows you to manage your security operations using FortiAnalyzer and without the need for a separate FortiSOAR instance. It is, in fact, a fully operational FortiSOAR instance.

The FortiSIEM MEA makes FortiAnalyzer a SIEM collector, alleviating the need for a separate FortiSIEM collector node (VM or device), when you already have a FortiAnalyzer deployed.

Review the minimum hardware requirements before you enable an MEA.

The MEA pane is visible on the GUI only when docker status is enabled and at least one MEA is enabled and downloaded.

For more information about each management extension, refer to the corresponding administrator guide in the *Fortinet Documentation Library*.

Knowledge Check

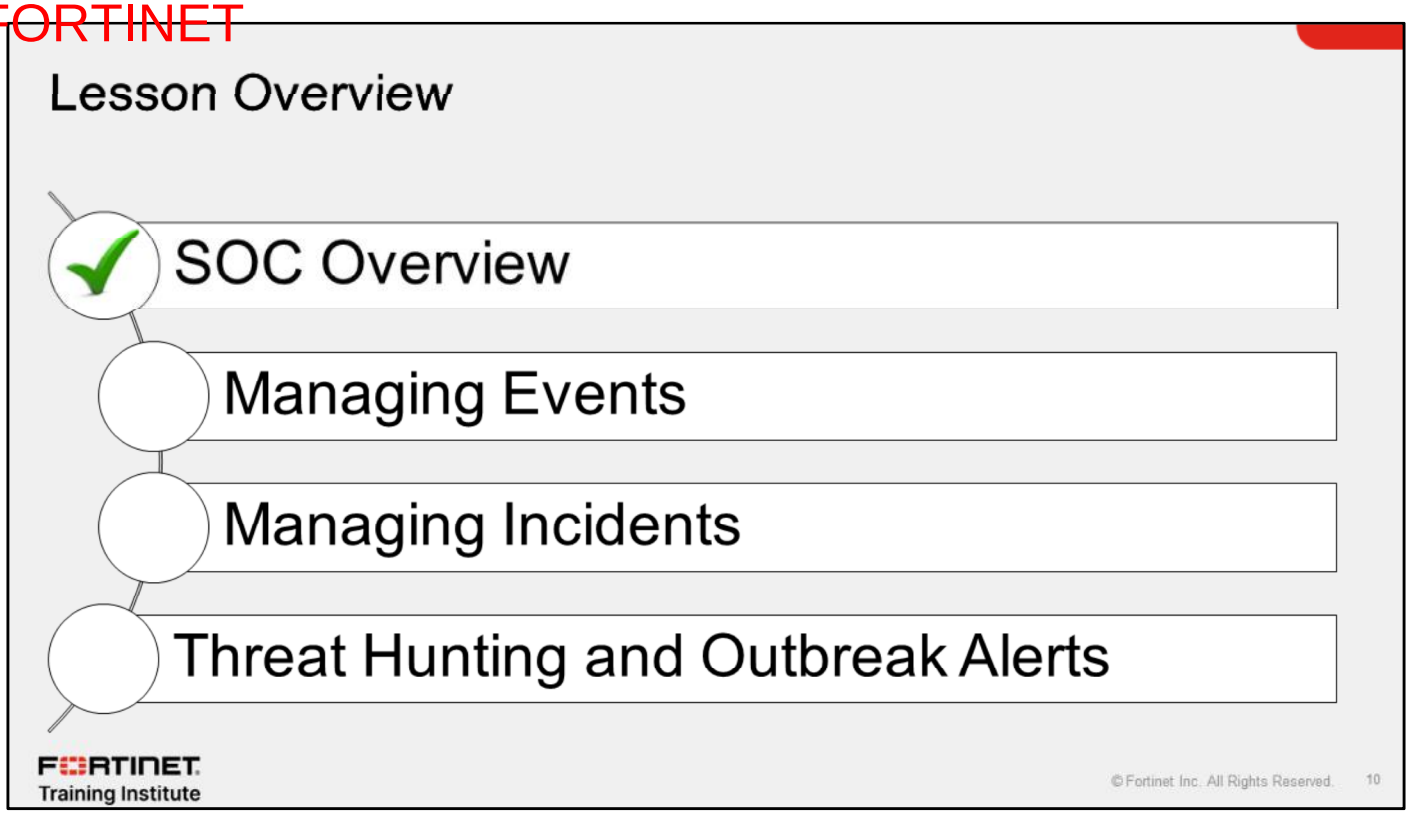
1. What are MEAs in FortiAnalyzer?

✓ A. Licensed applications that are installed and run on FortiAnalyzer

B. Dashboard widget extensions that are installed and run on FortiAnalyzer

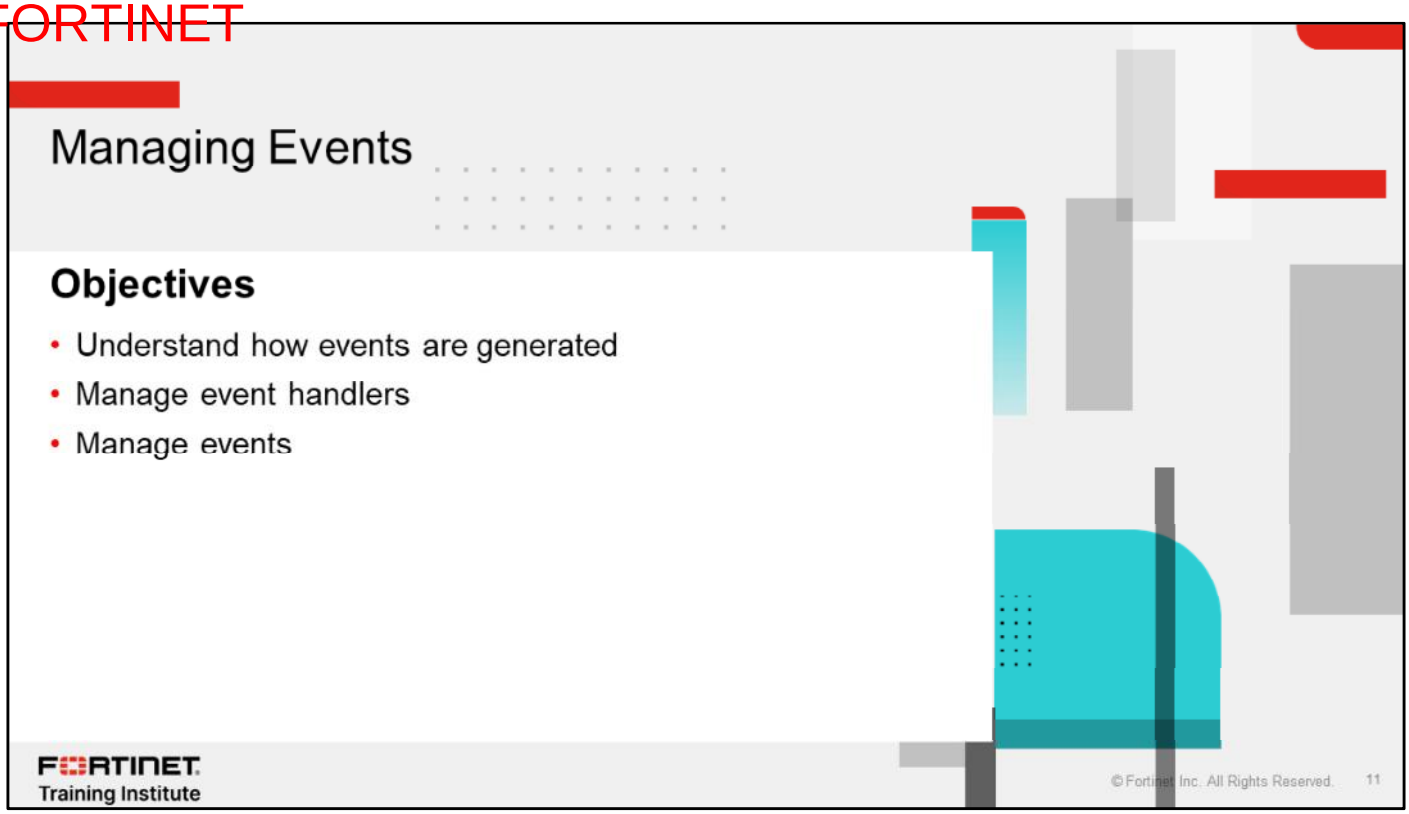
FORTINET Training Institute

 9



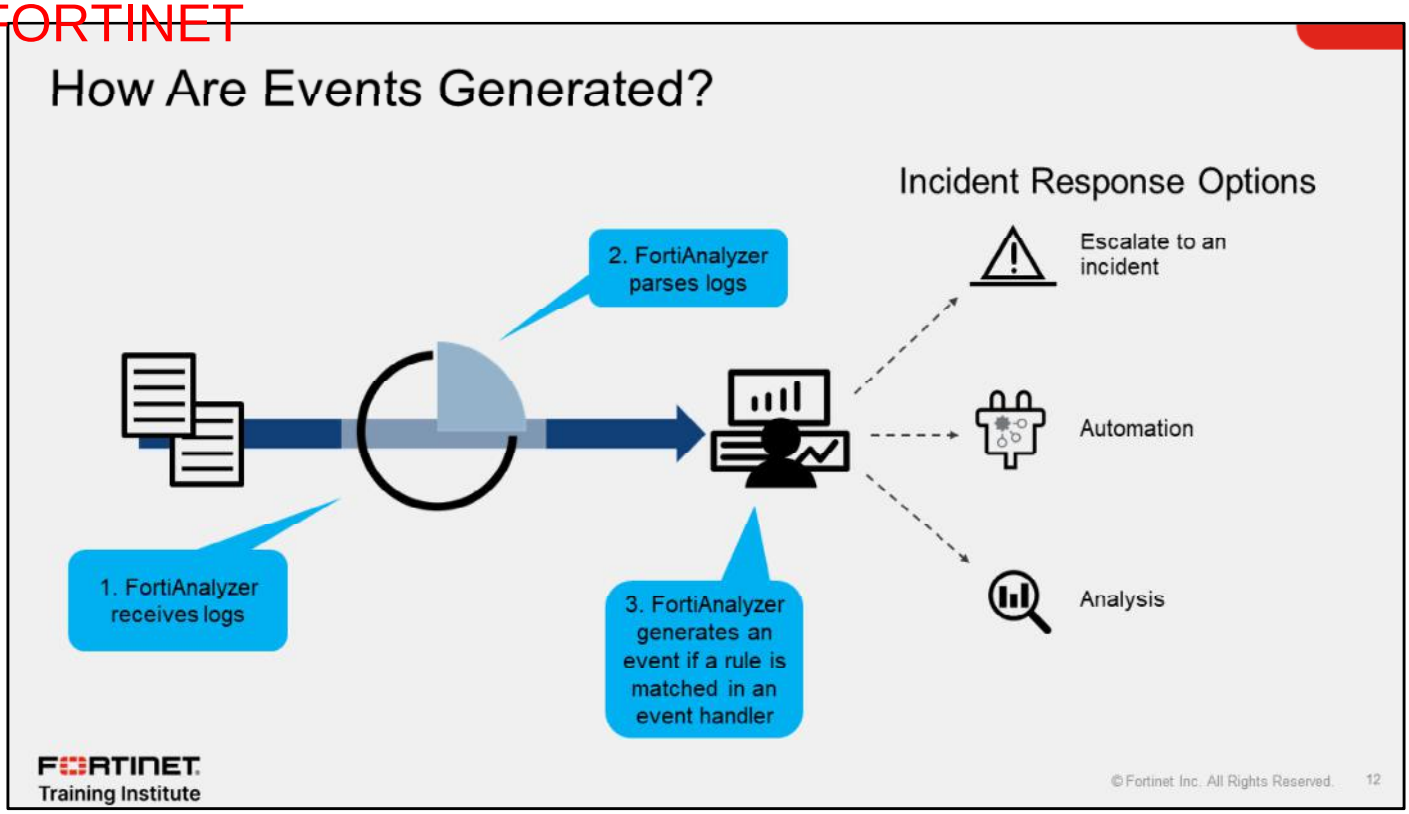
Good job! You now understand SOC features and the dashboard.

Now, you will learn how to manage events.



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

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



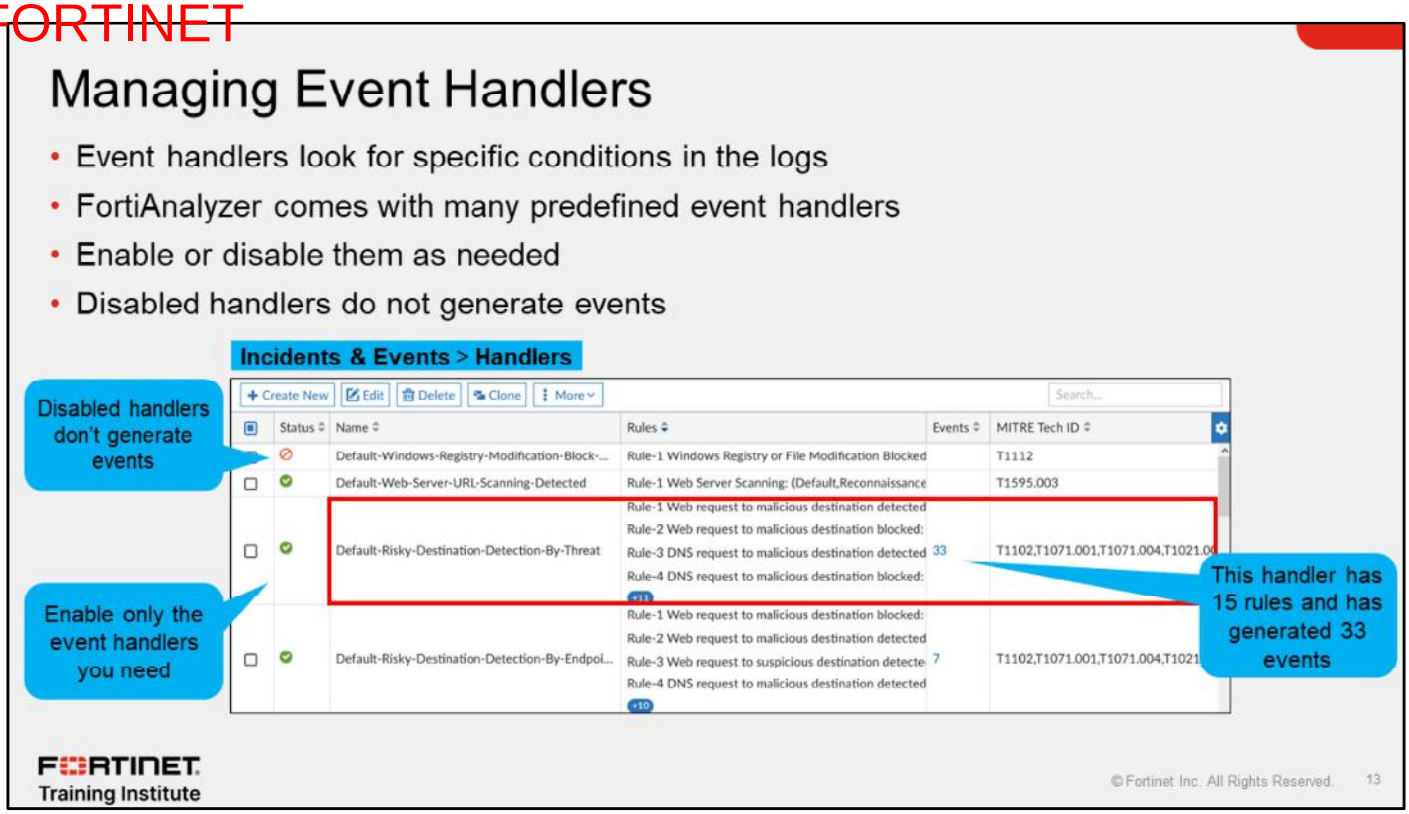
After receiving logs from other devices, and based on the details included in them, FortiAnalyzer uses event handlers to determine if new events need to be generated. Event handlers identify if the information in the logs matches a series of configurable criteria, such as threat type, device type, log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

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

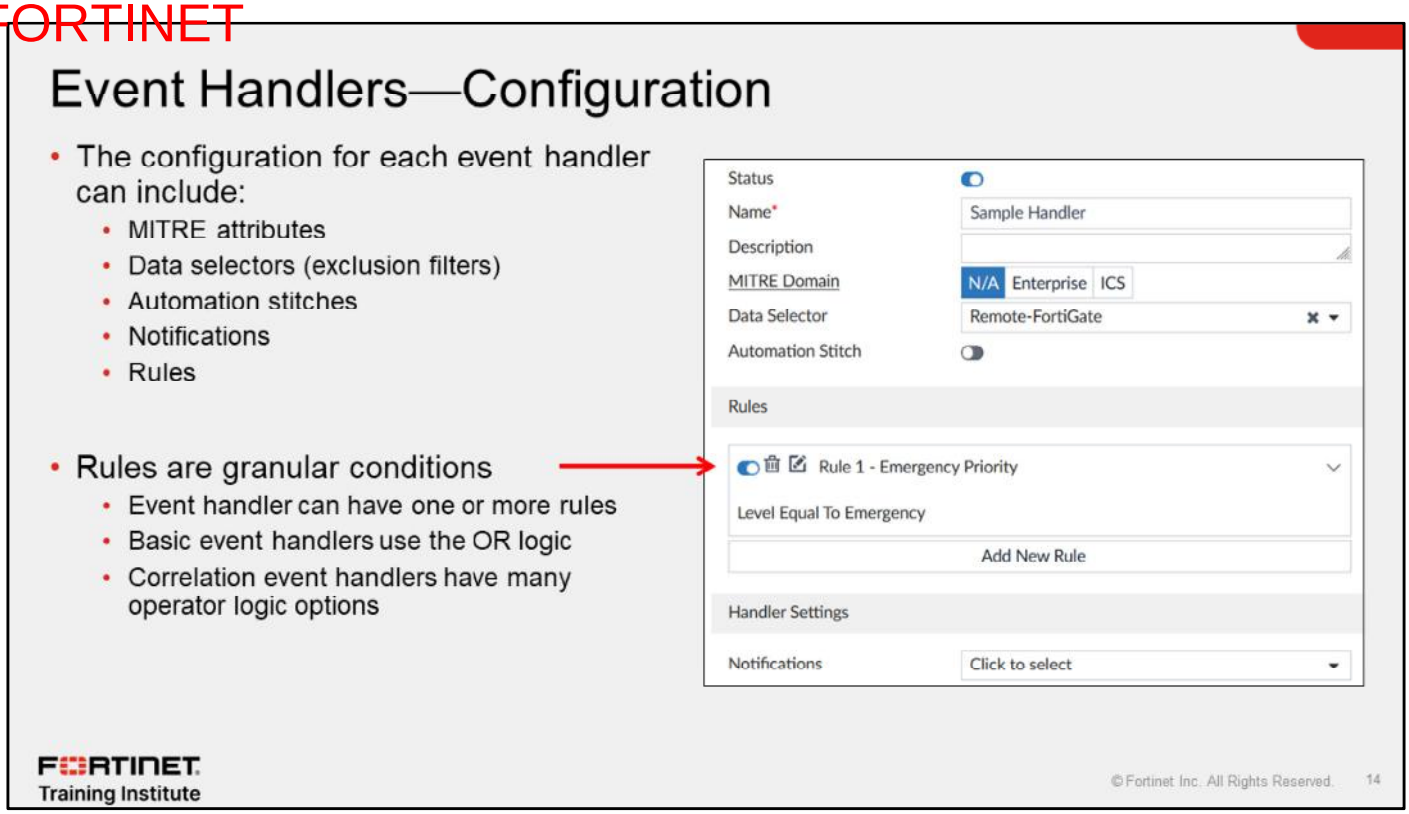
If events warrant further attention and investigation, you can escalate them into incidents. From there, you can correlate logs with the incident, look at an incident timeline, assign a priority and an analyst to review the incident, and more. If there are a large volume of generated events, you may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

Automation will be covered in more detail in a later lesson.



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 it 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, type a name, and write a description for it.

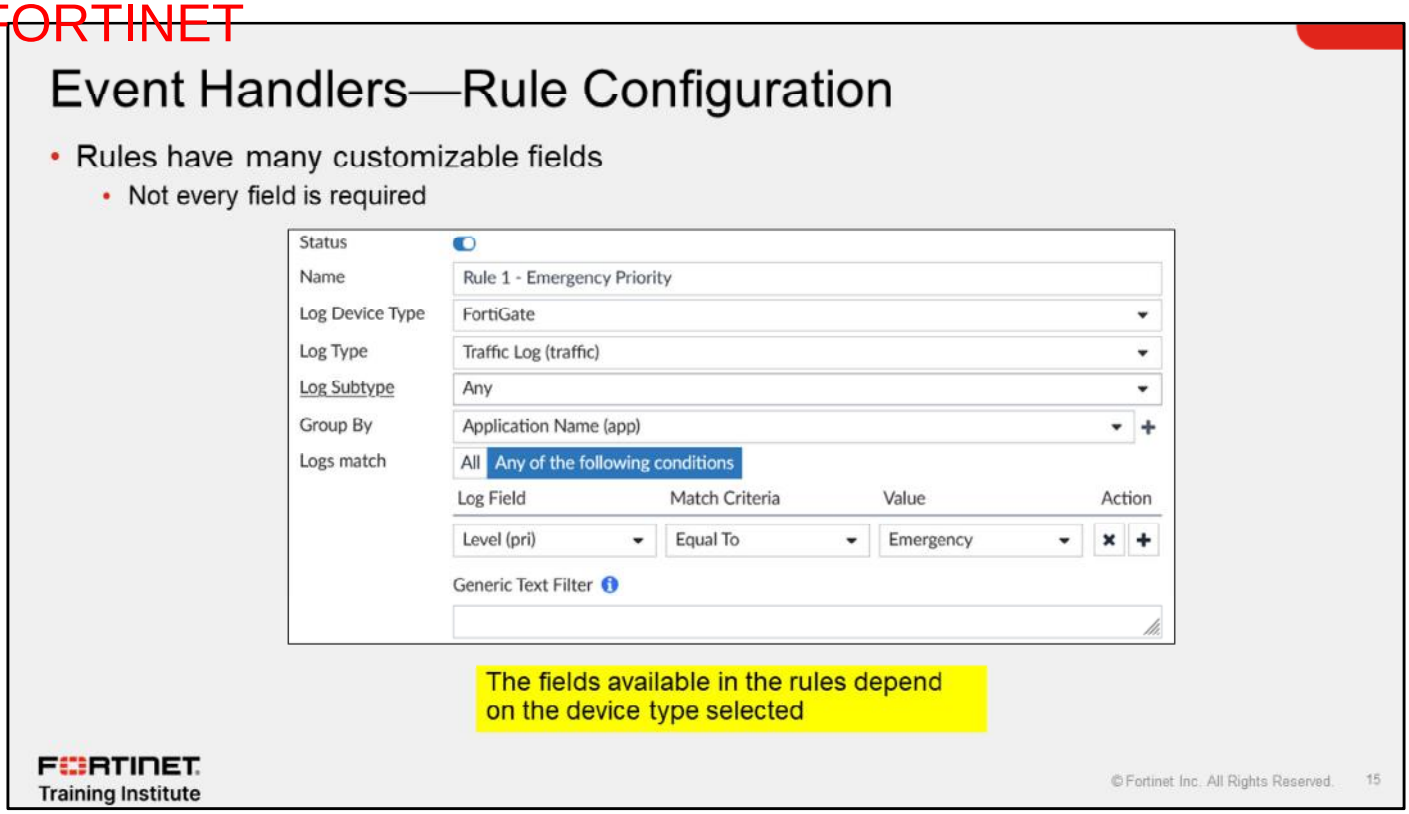
You can also choose which MITRE domain the event handler falls under, and then select from a list of tech IDs that correspond to the handler. Many predefined event handlers already have the MITRE attributes configured. You can view the MITRE ATT&CK framework matrices under **Incidents & Events**.

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*.

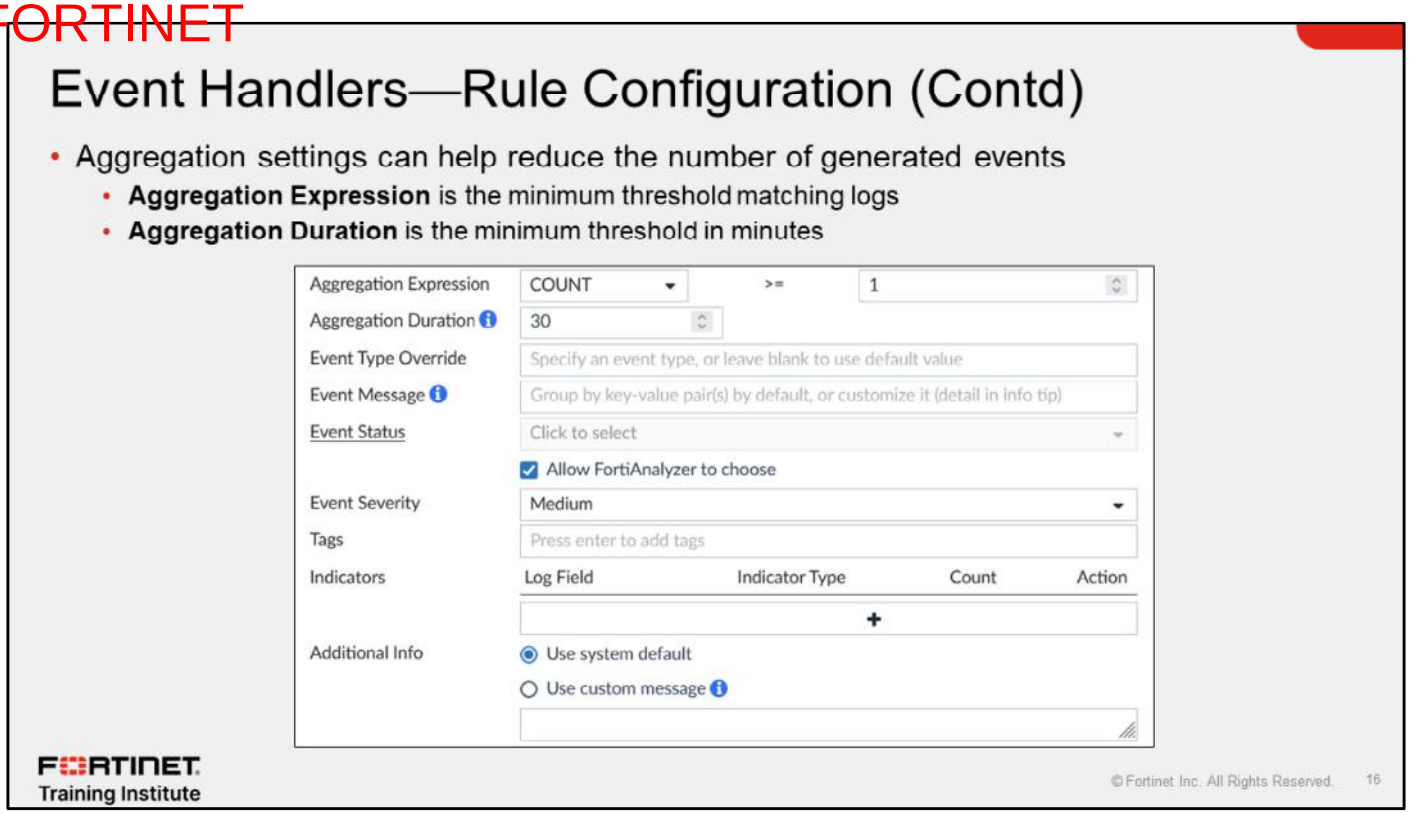
When a handler generates an event with the automation stitch option enabled, FortiAnalyzer sends a notification to the FortiGate automation framework, which then checks if there is a corresponding automation stitch in FortiOS. If there is one, the configured action is triggered.

The **Rules** section contains the fields that must be matched up against logs in order to generate events. You can disable, edit, or delete rules for the handler. The basic handler type use an 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.



The screenshot on 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/OR logic are supported if there are multiple conditions. The **Log Field** drop-down field presents common criteria you can select to include in the filter. Alternatively, you can use generic text filters if you require precise filtering.



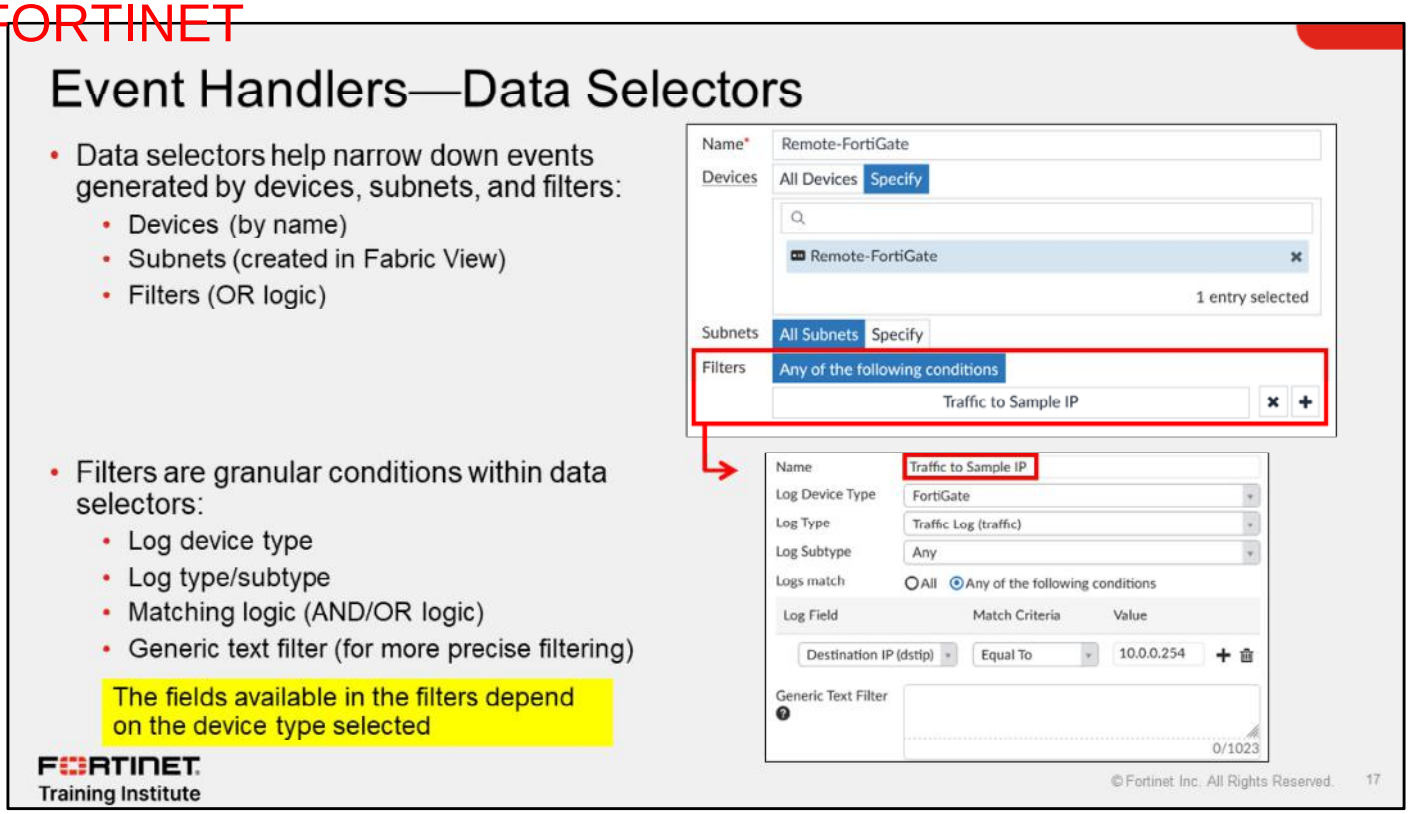
If an event handler is generating too many events in your environment, you can configure the aggregation expression and aggregation duration settings.

Aggregate Expression has three options:
- COUNT – A minimum threshold count of matching logs.
- COUNT_DISTINCT – Select the field that must be distinct, such as a distinct source IP or application.
- SUM – Has multiple options such as duration, sent/received bytes, and sent/received packets.

Aggregate Duration is the minimum threshold in minutes to generate events.

These two settings work together. The number of matching logs (expression) must occur in the number of (duration) in order to generate an event.

You can also set the event type, message, status, and severity.



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

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

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

Event Status

- Events can be in one of four statuses
  - It is important to understand what each one of them means

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

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

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

FORTINET Training Institute

 18

Events in FortiAnalyzer can be in one of four statuses. The current status will determine if more actions need to be taken by the security team or not.

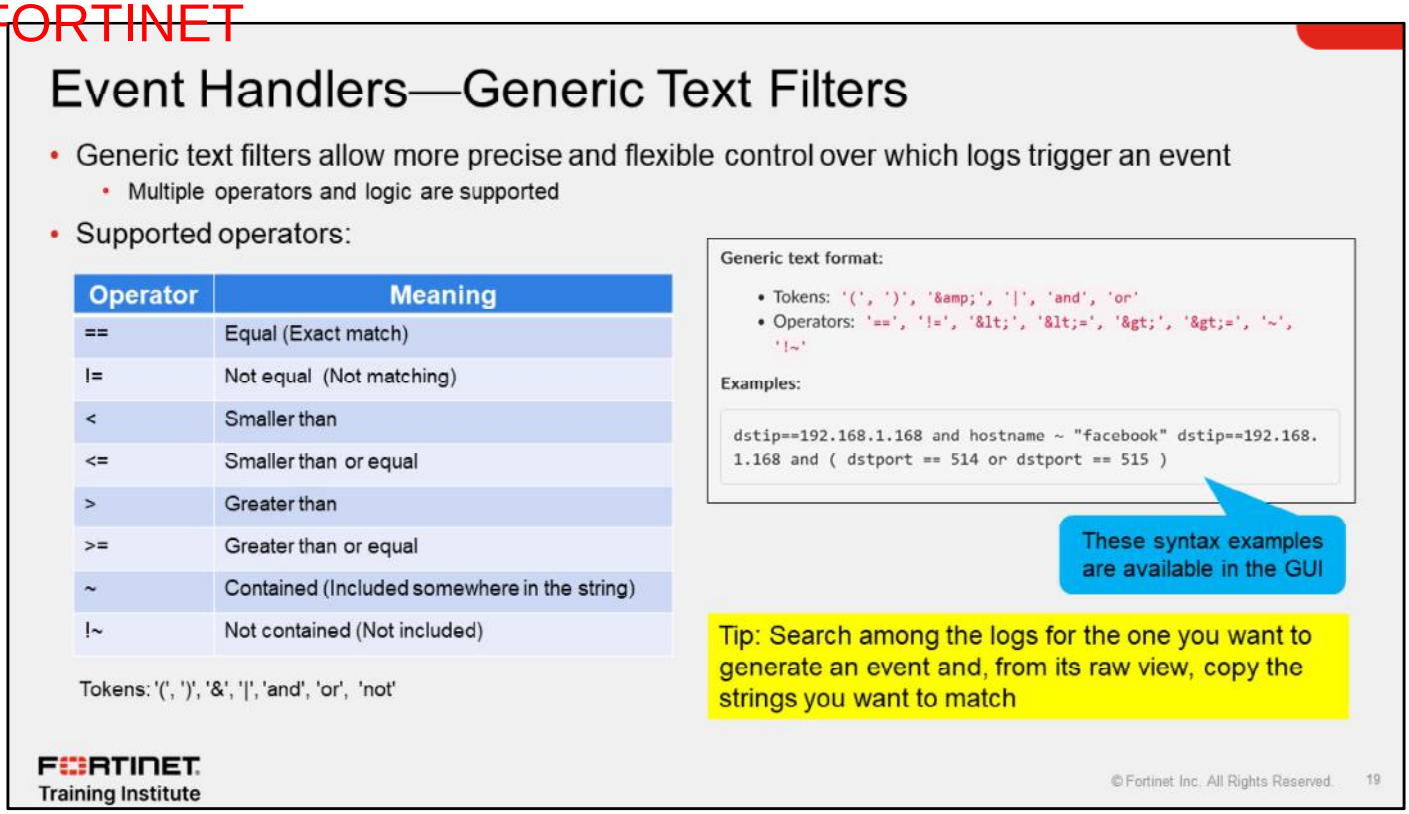
The possible statuses are:

- **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 AV log with `action=quarantine` will have the event status **Contained**.

- **Mitigated:** The security risk is mitigated by being blocked or dropped.
  For example, an IPS/AV log with `action=block/drop` will have the event status **Mitigated**.

- **(Blank):** Other scenarios.
  For example, both allow and block actions can be seen in logs associated with that event.



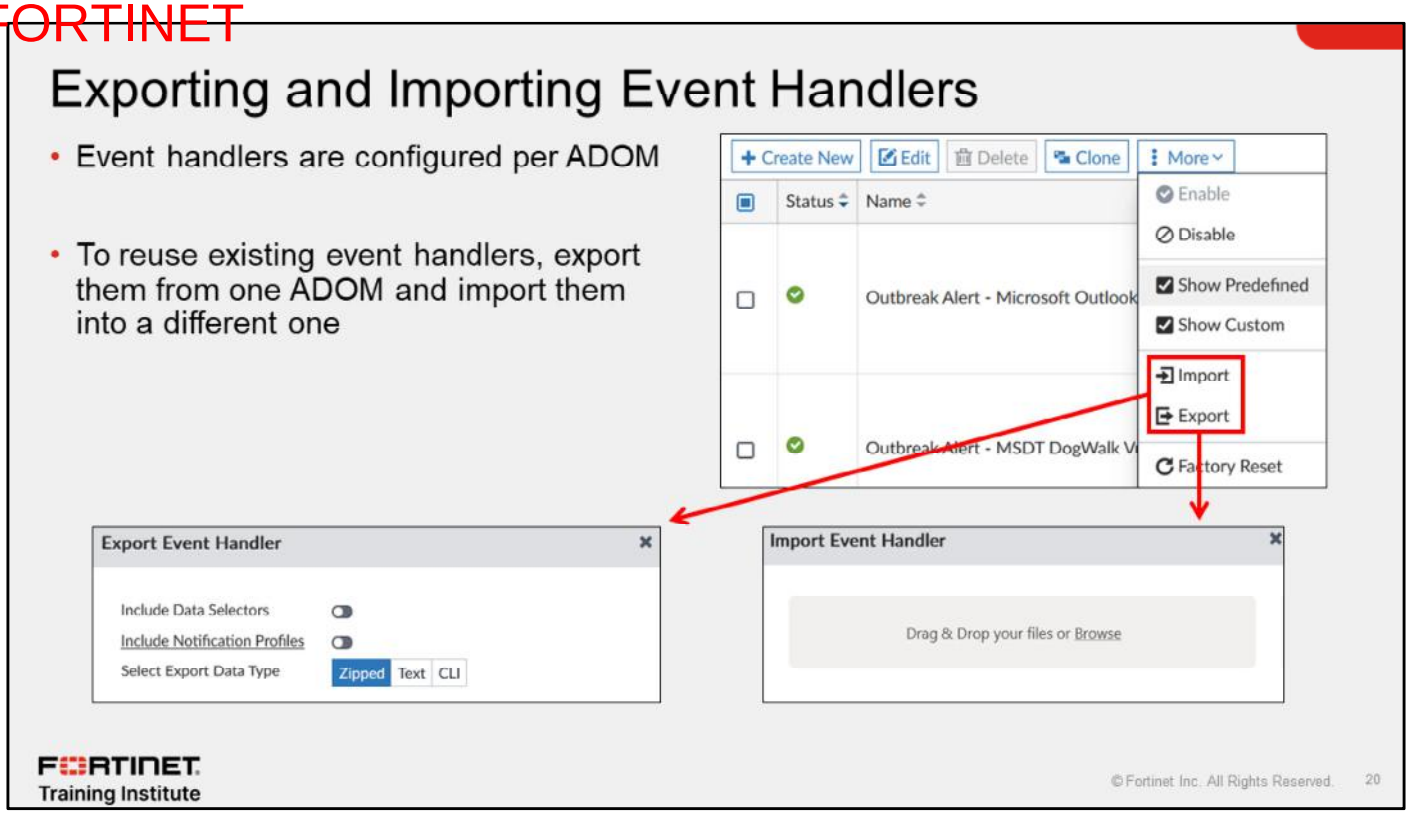
When configuring an event handler, the use of generic text filters allows more precise and flexible control over which logs trigger an event. These filters use operators based on regex and the Portable Operating System Interface (POSIX) standard.

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 field equal to `192.168.1.168` and with the hostname field containing the string `facebook` in it.

Keep in mind that you must use the escape character "\" if you need to include a reserved character in your filter.

As a tip to avoid syntax errors, you can search your raw logs for the log file that you want to add an event handler for, and copy and paste the string you want to match.



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.

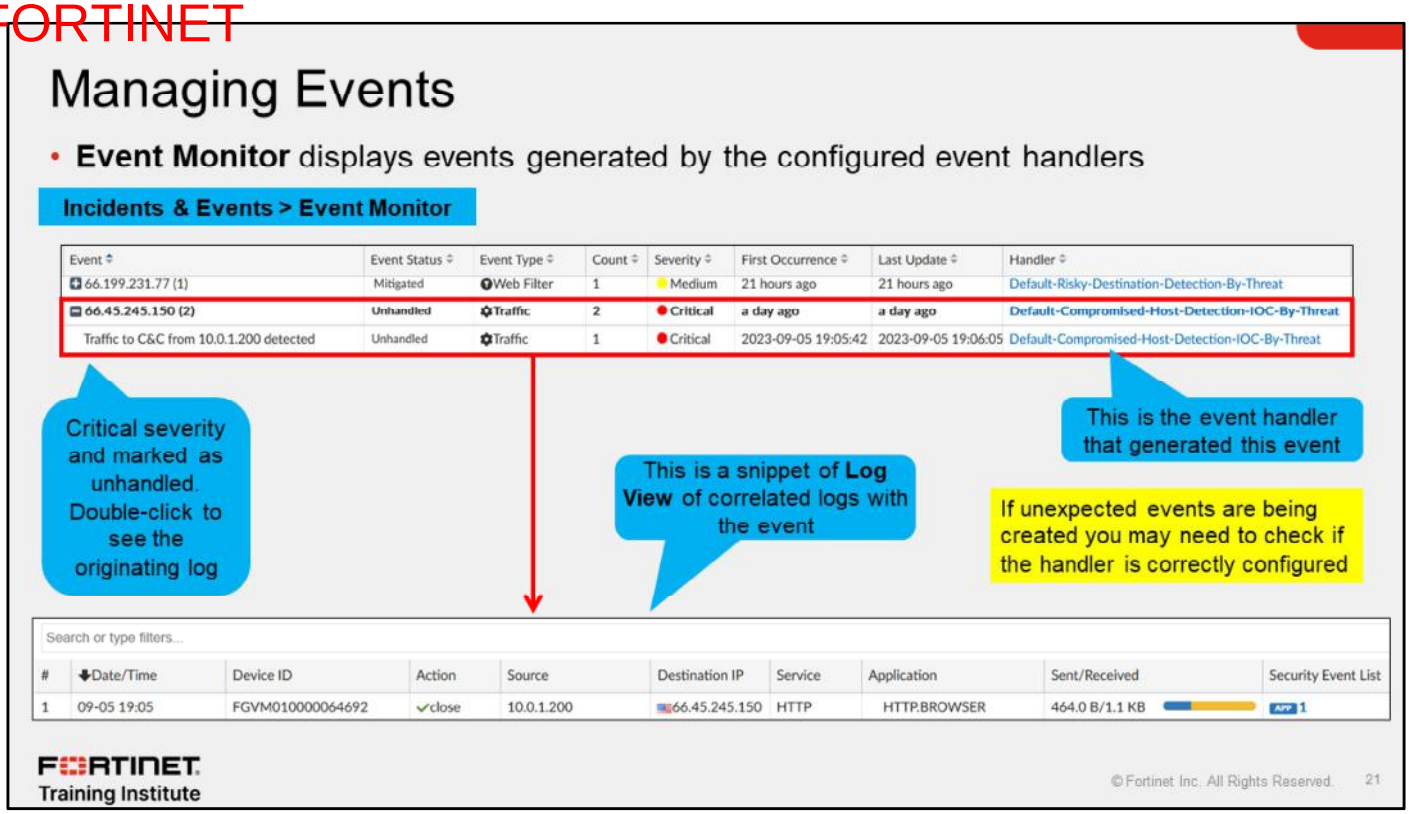
To export an event handler, in the **Event Handler** list, select one or more handlers from the list, right-click, and then select **Export**.

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 **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.

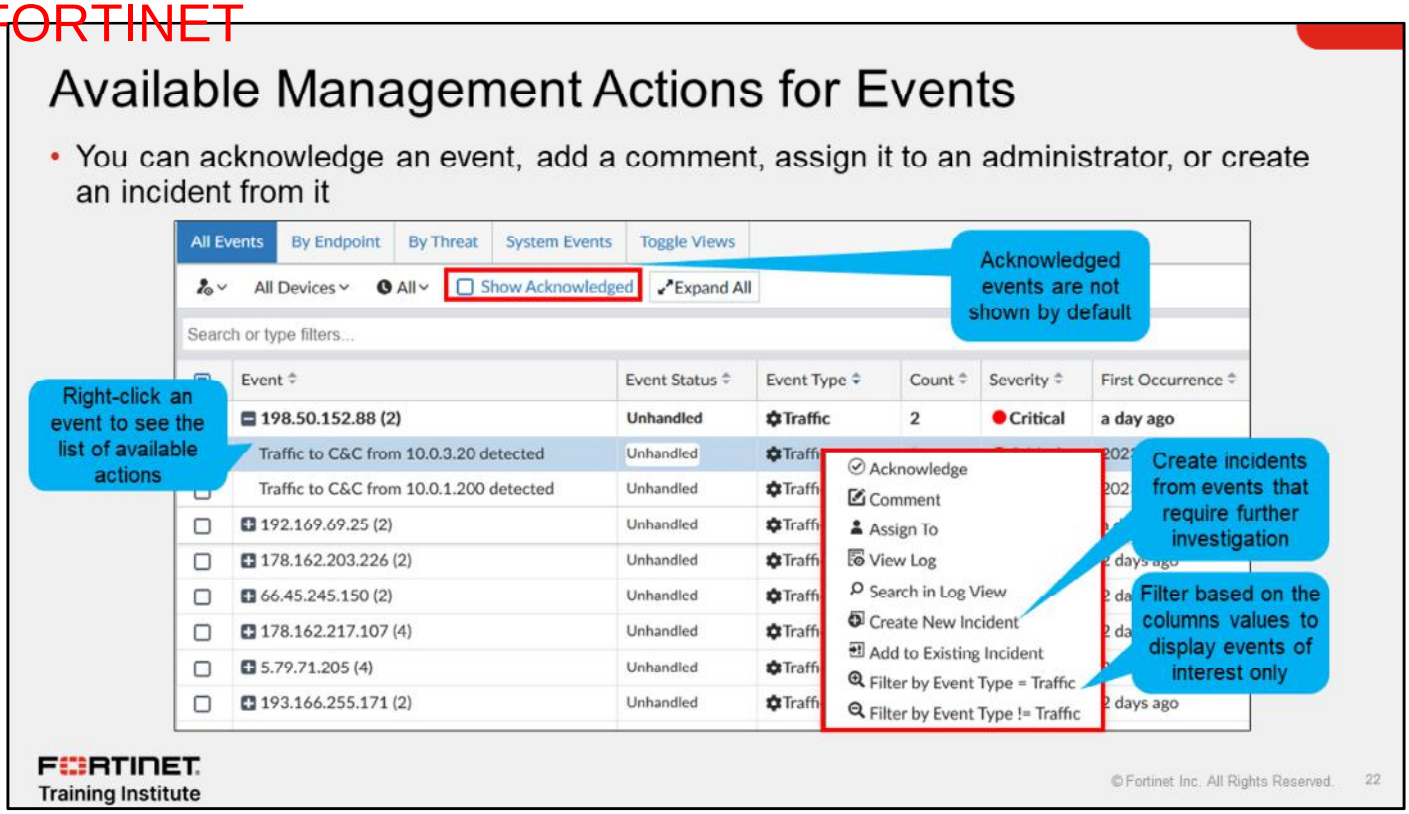
If the imported handler's name already exists, you have the option to rename, replace, or skip the import.



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

You can see them combined under **All Events**, or further divided by endpoint, threat, and system events.

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



Right-clicking an event allows you 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 the next section.

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 the incident 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.

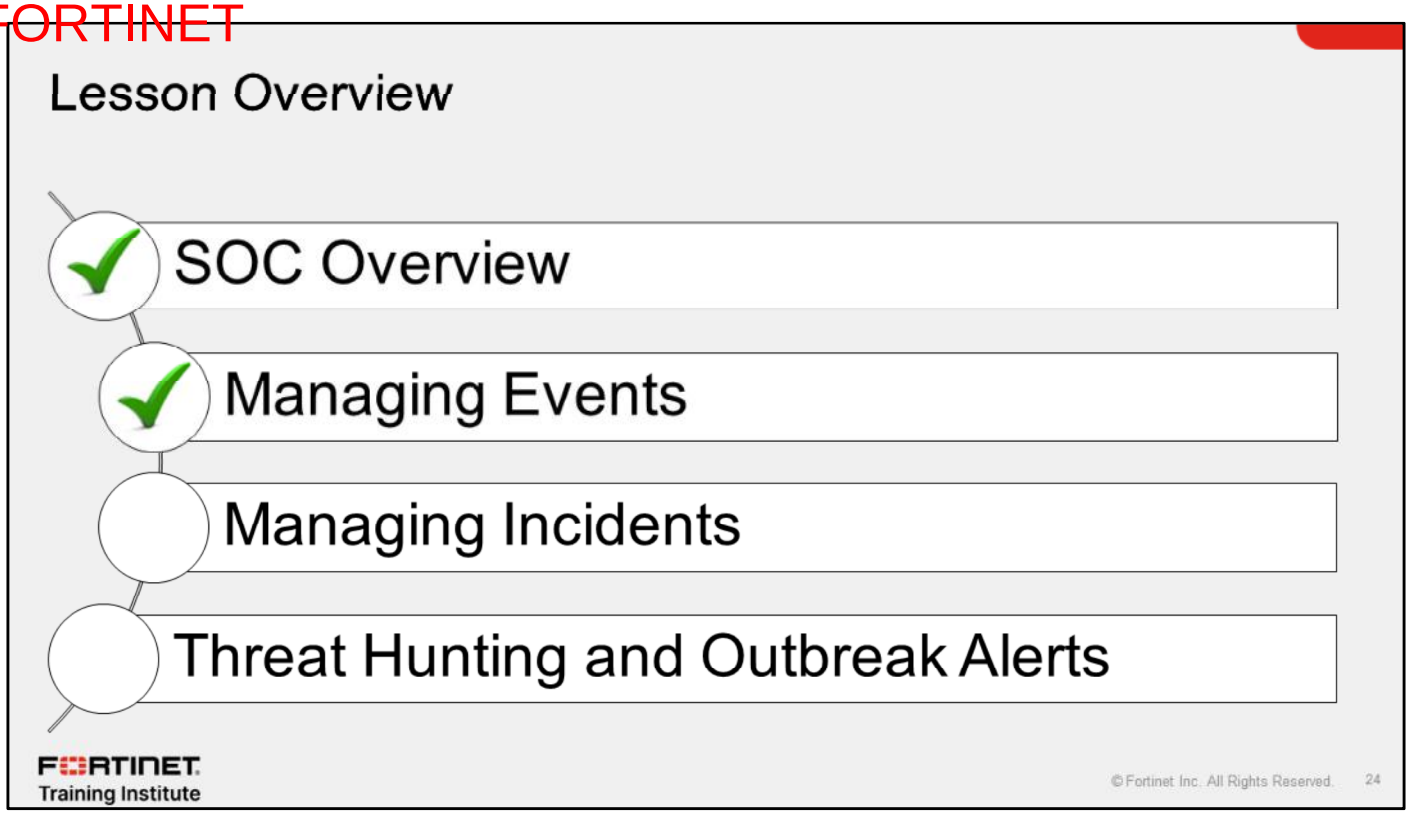
Knowledge Check

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.

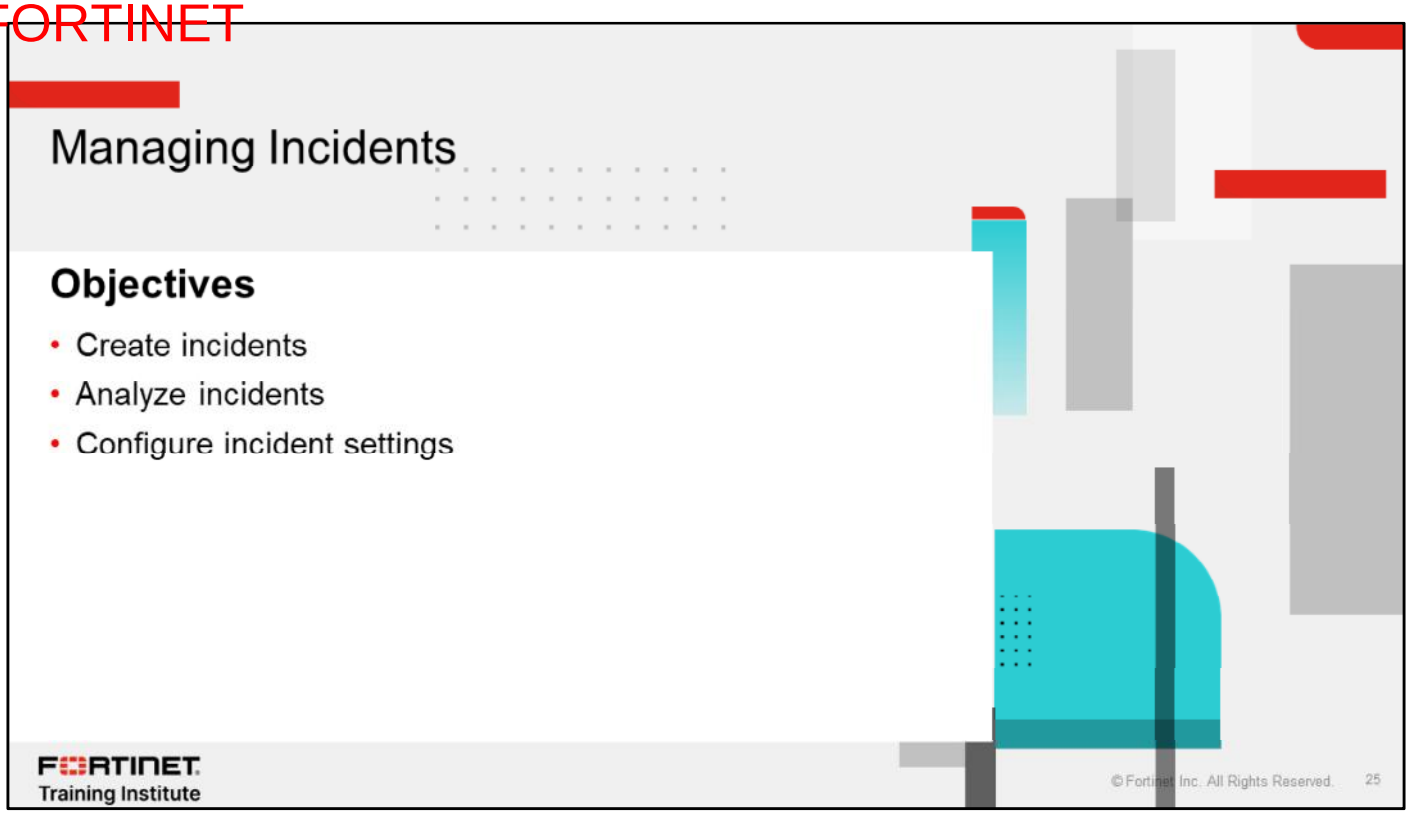
FORTINET Training Institute

 23



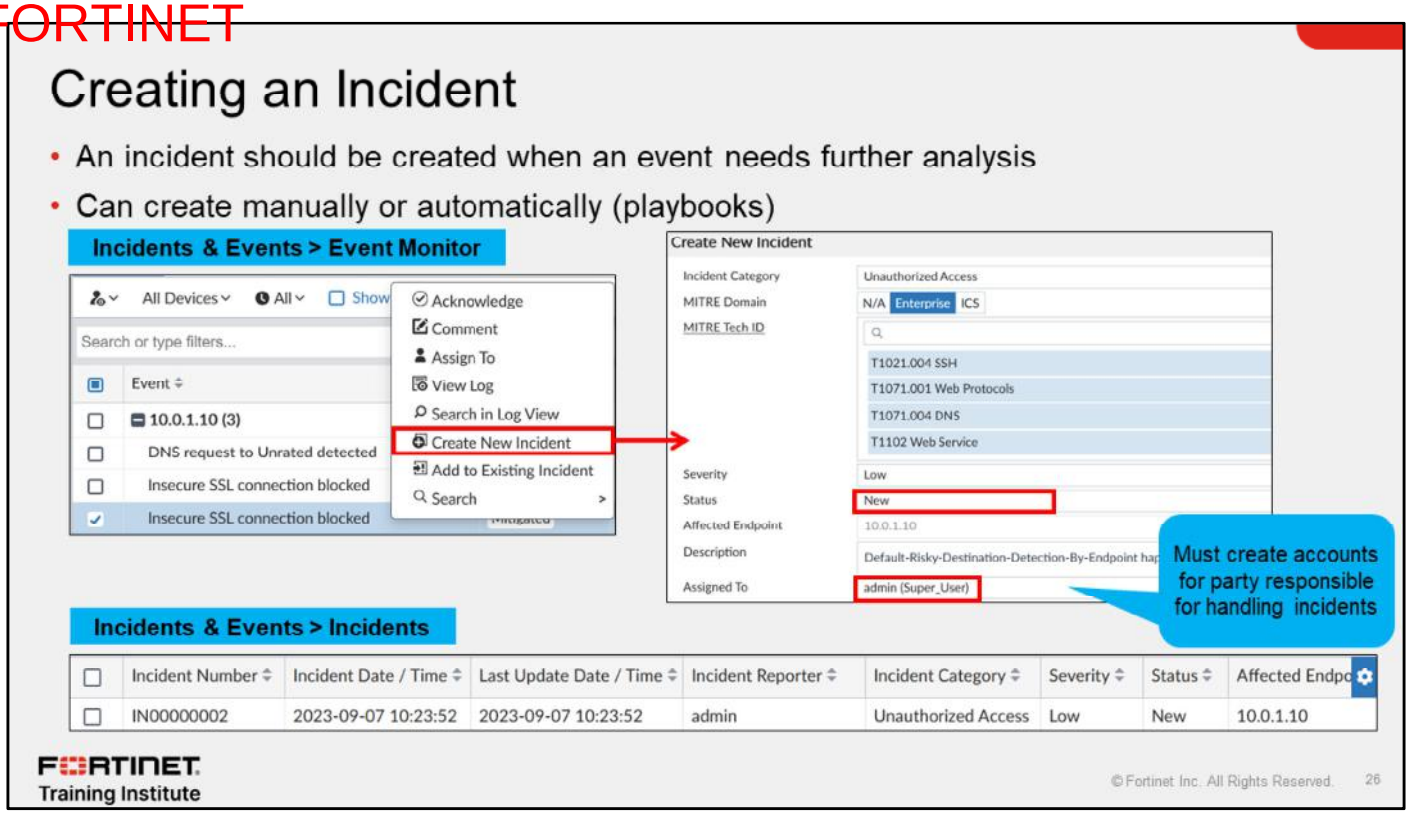
Good job! You now know how to manage events.

Now, you will learn how to manage incidents.



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

By demonstrating competence in managing incidents, you will be able to improve your efficiency in investigating security incidents in your organization.



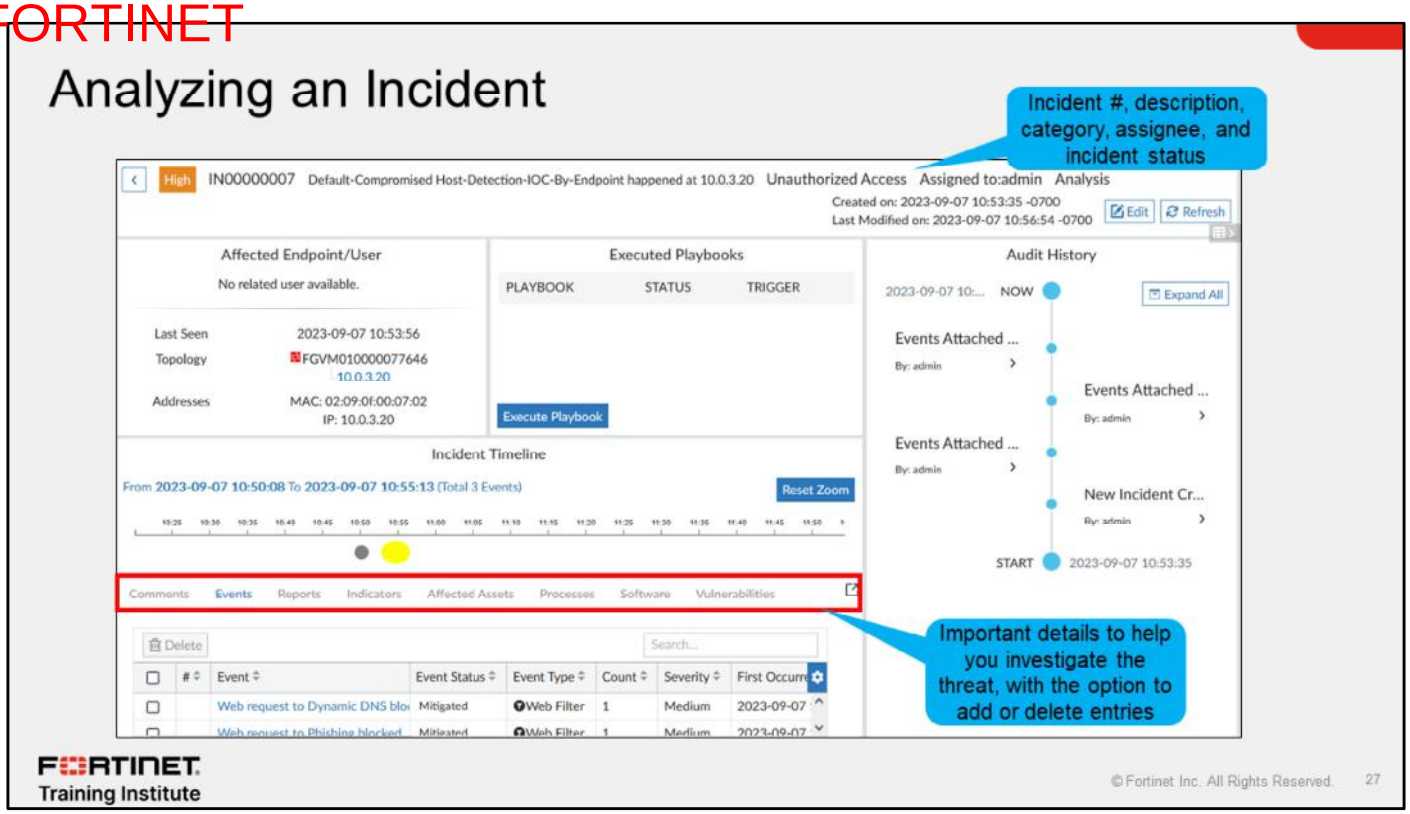
Not all events have the same impact or importance on your network. Some of them might need further analysis to prevent or mitigate security breaches. When an analyst finds an event that requires further scrutiny, they should create a new incident from that event. You can think of an incident as an event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

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

In FortiAnalyzer, you create incidents manually from **Event Monitor** 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** interface.

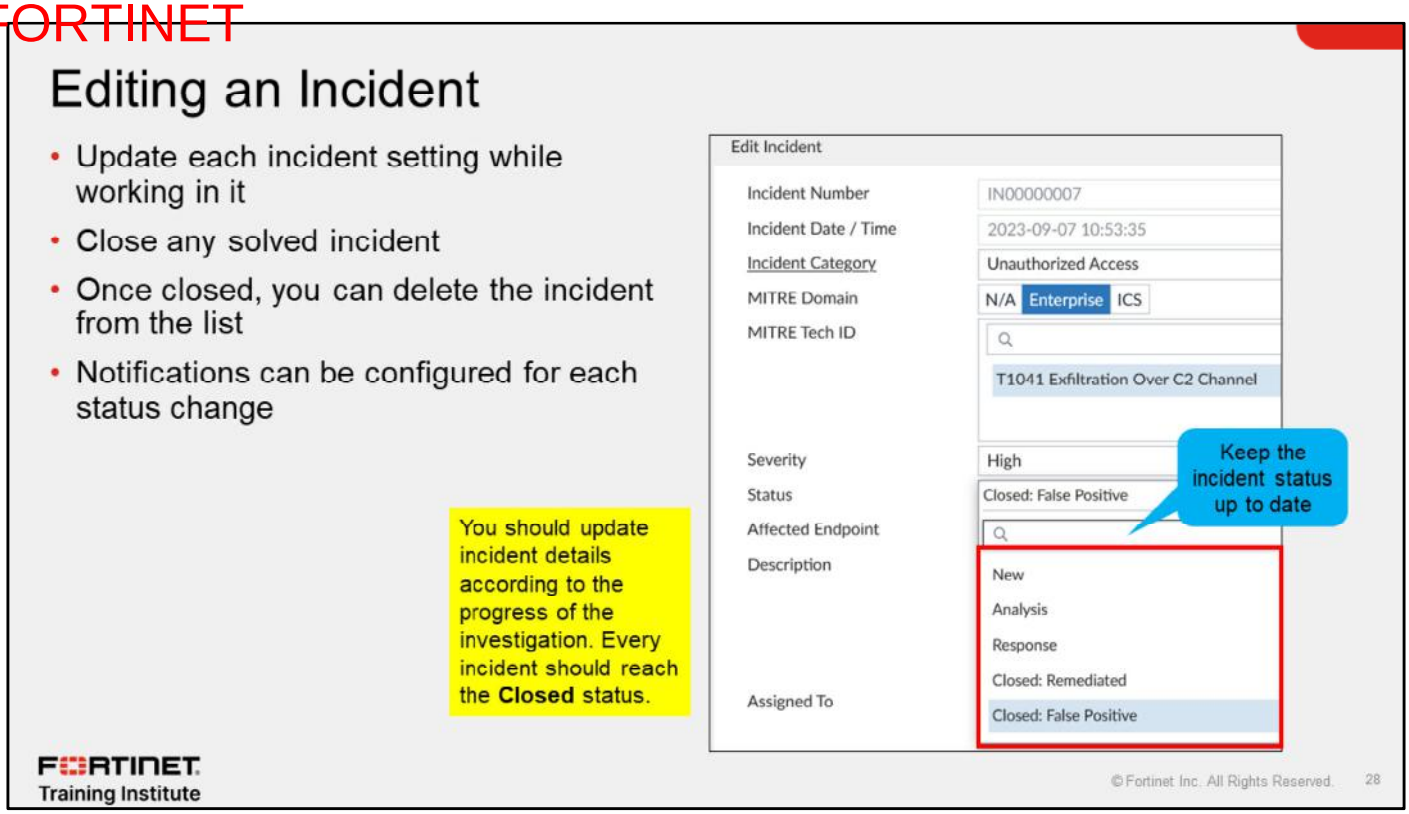


To view the details of an incident, go to **Incidents**, and double-click on the incident you want. You can also right-click an incident, and then select **Analysis**.

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

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

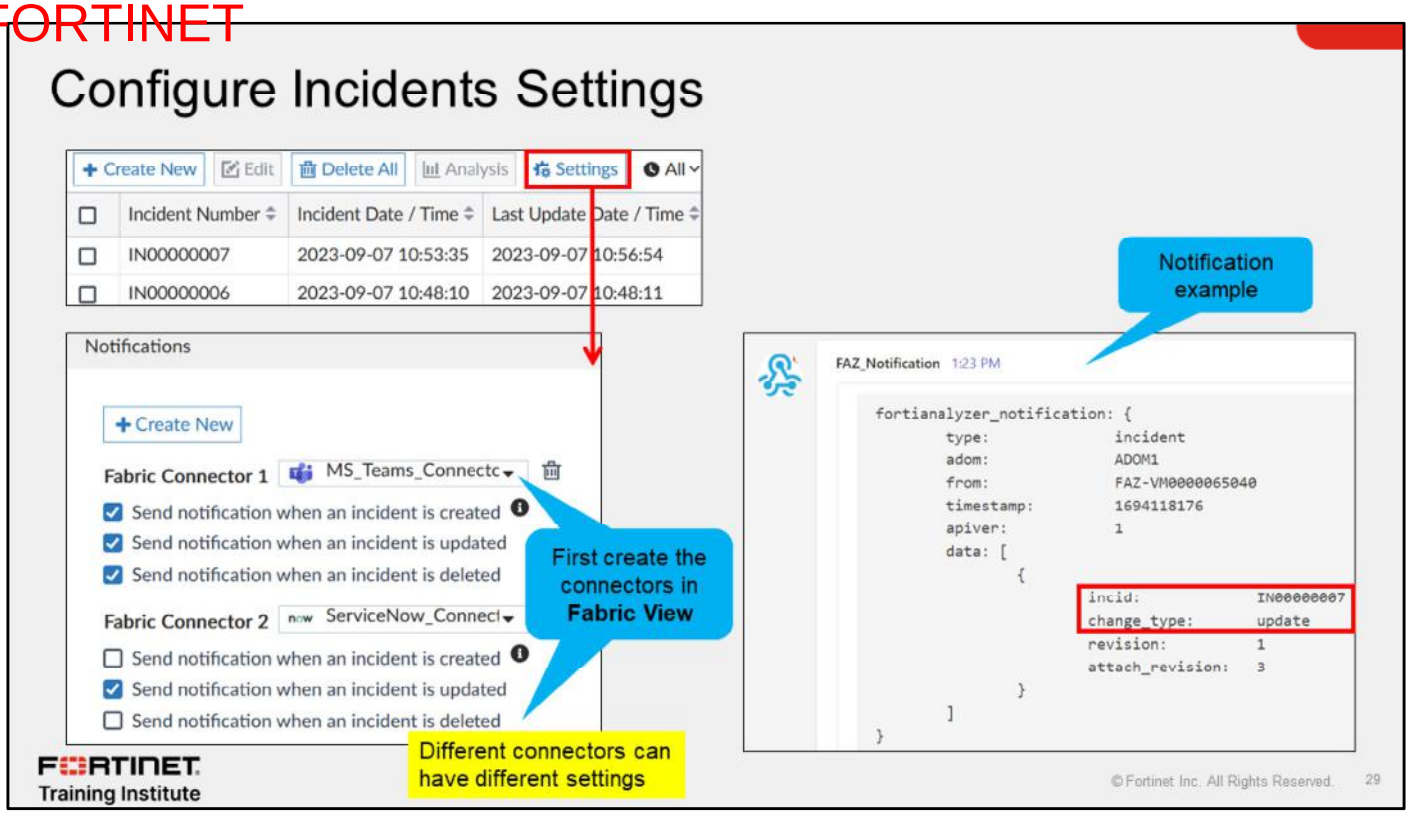
The list of events associated with the incident is also available under the tab with that name. From here, you can access the related logs by right-clicking the event of interest. This will open **Log View** in a different window.



It is important to keep all incidents 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, resolved incidents can be deleted from the list.

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



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

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

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

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

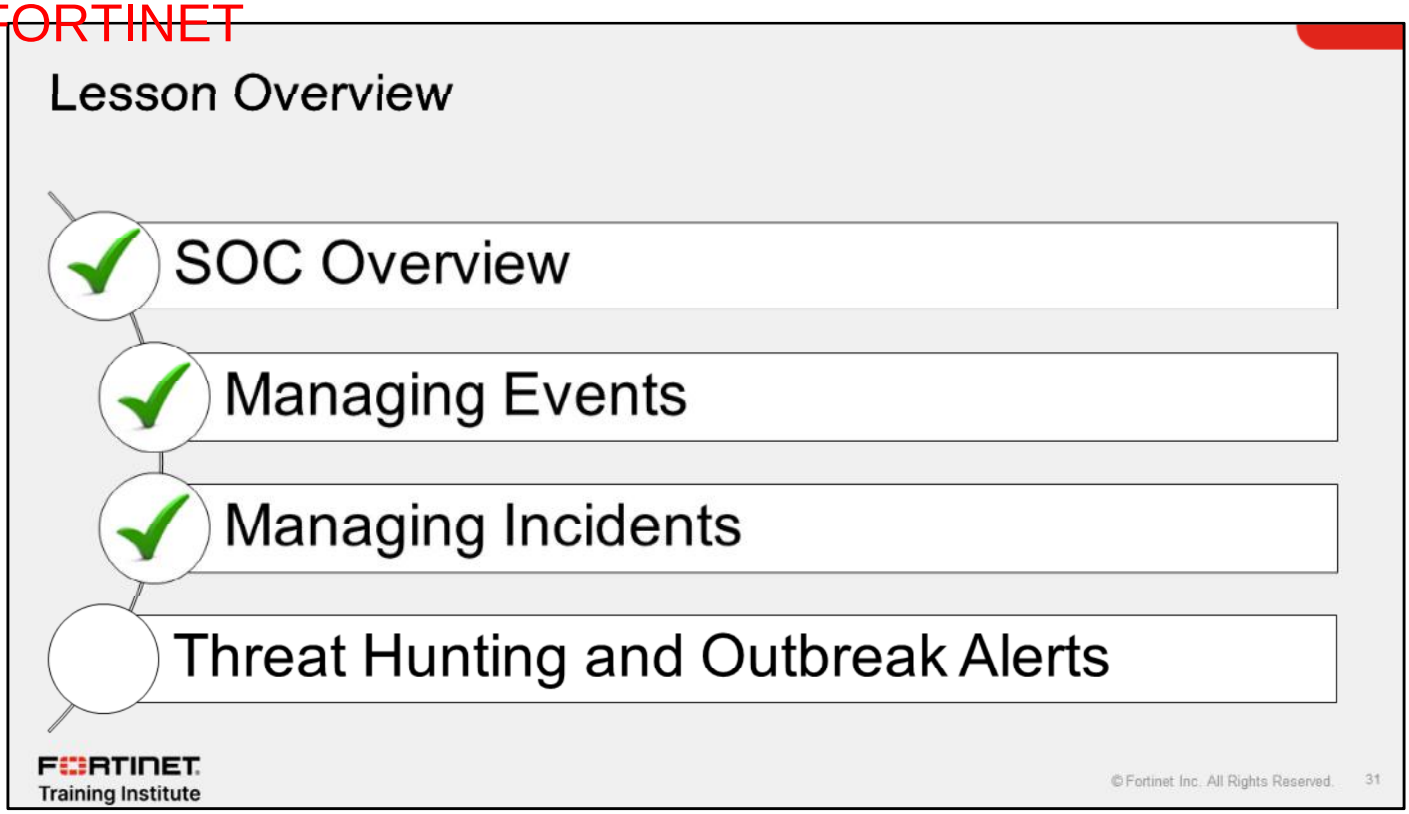
Knowledge Check

1. When would a security administrator 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

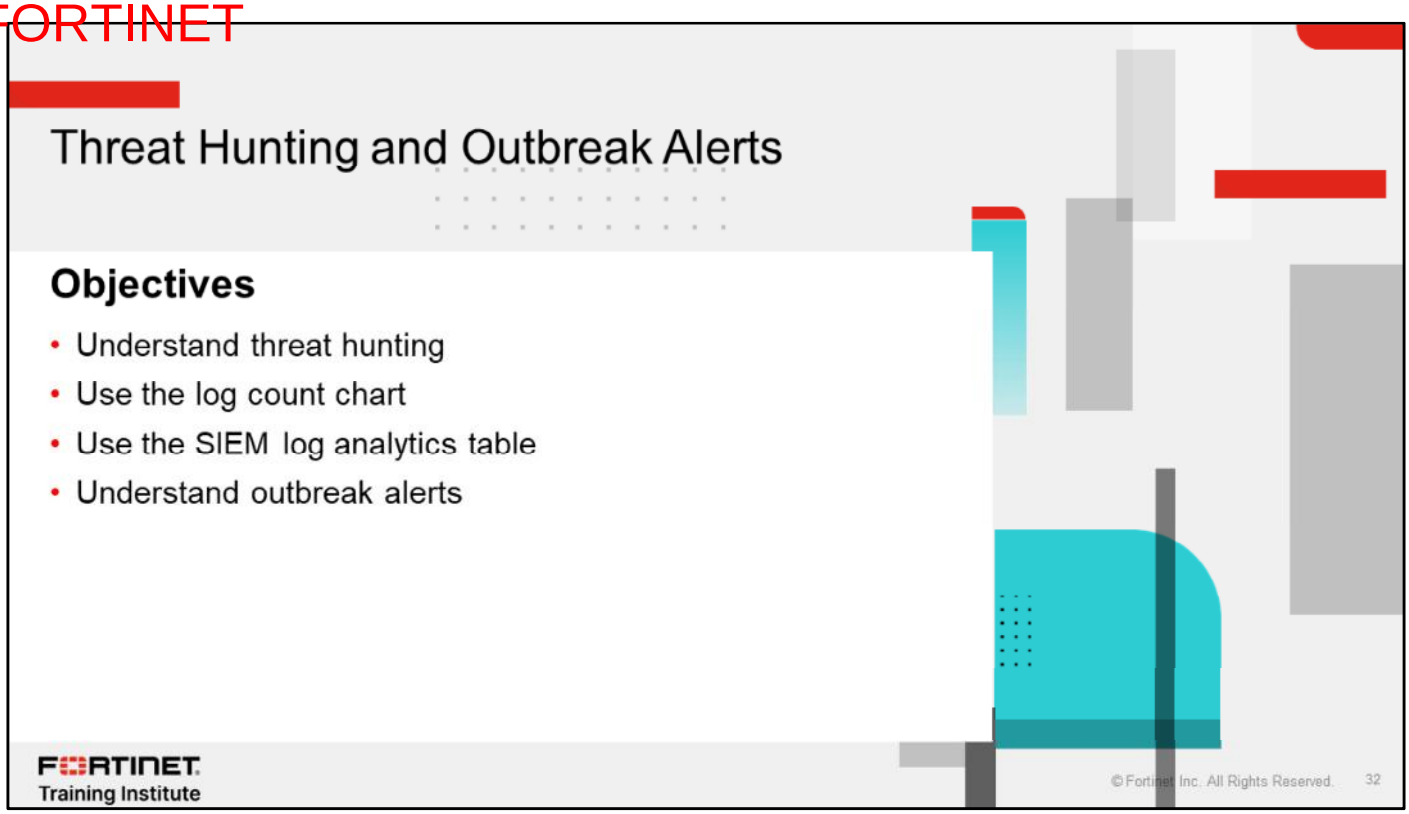
FORTINET Training Institute

 30



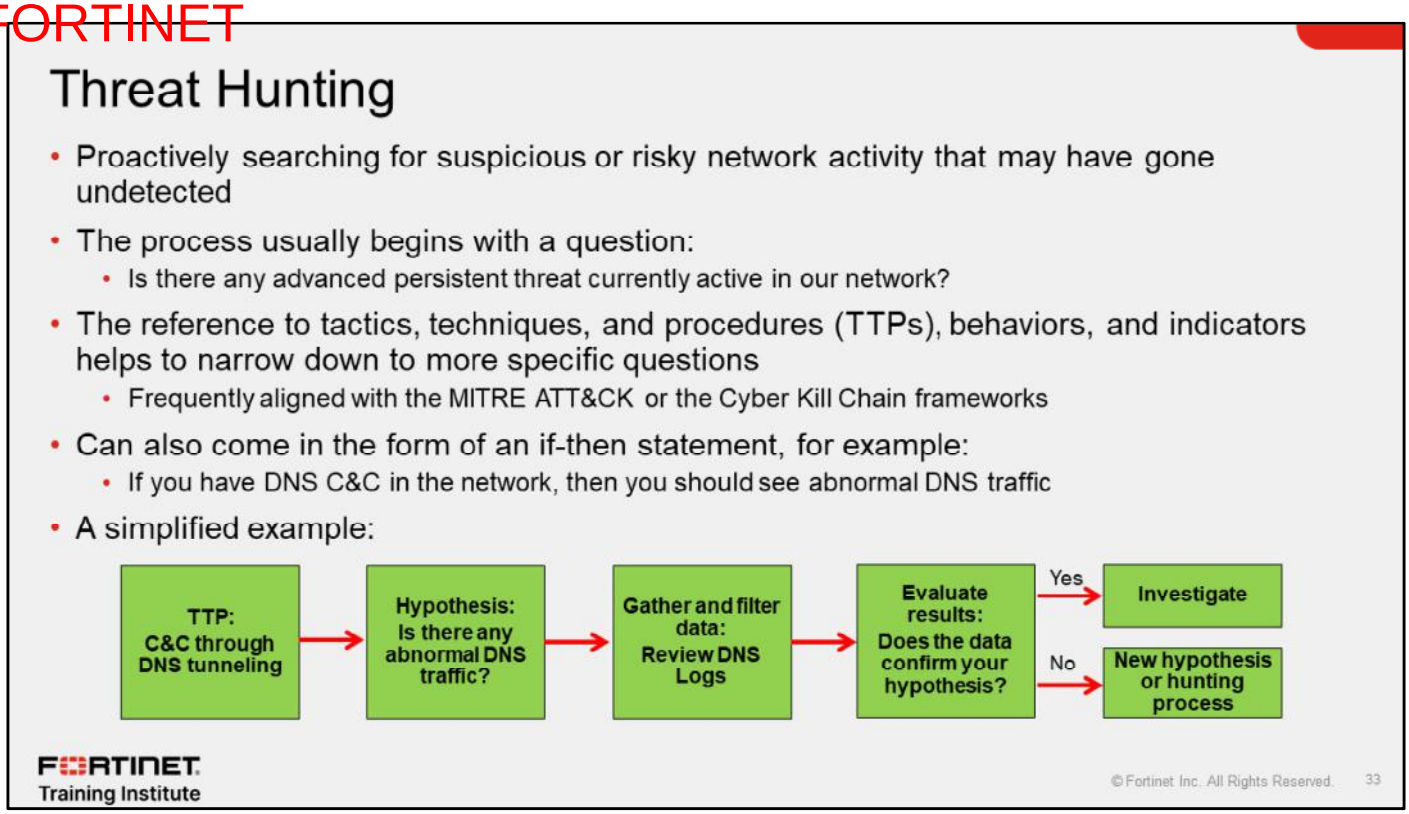
Good job! You now understand how to manage incidents.

Now, you will learn how about threat hunting and outbreak alerts.



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 alerts 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.

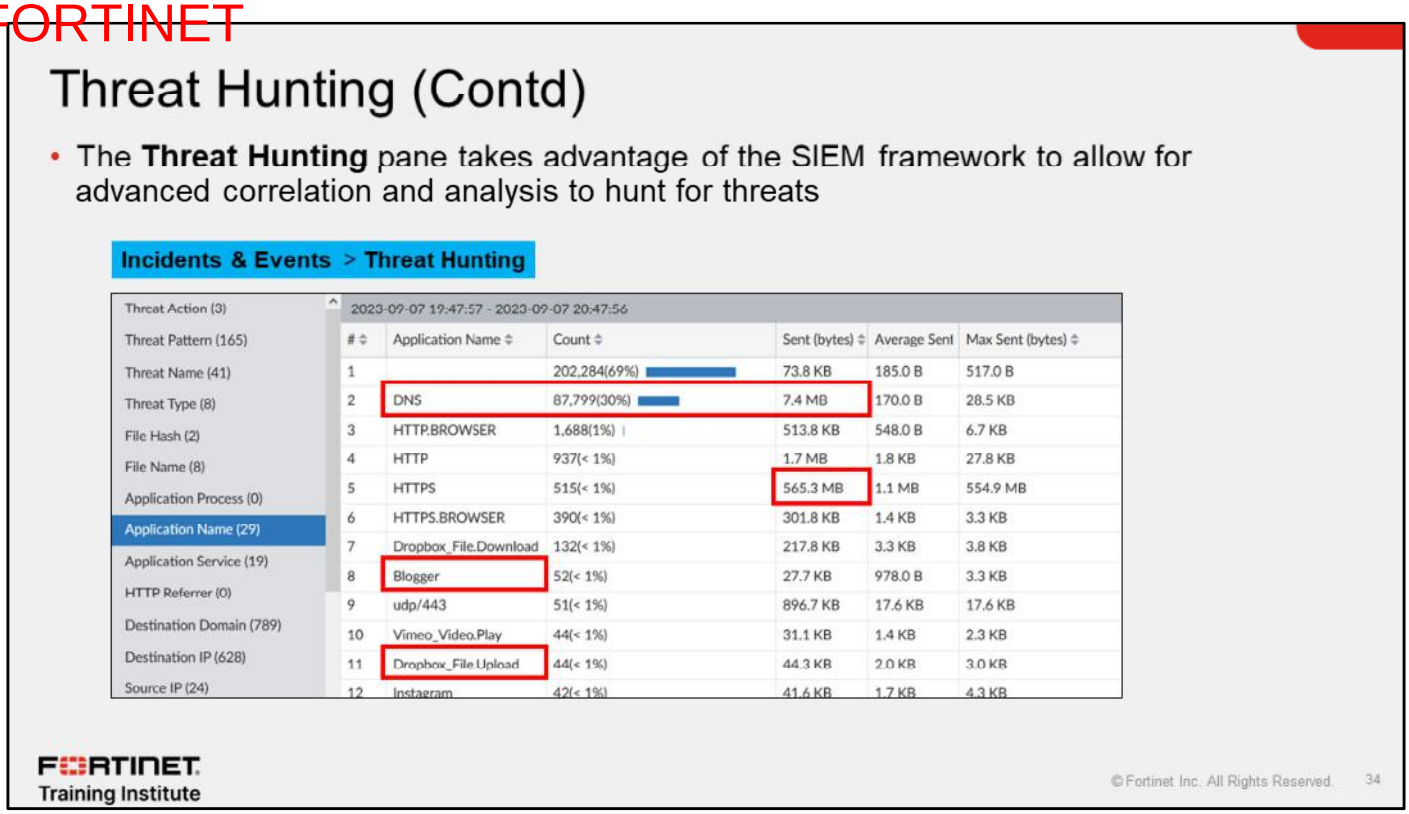


Threat hunting consists of proactively searching for suspicious or potentially risky network activity in your environment. The proactive approach helps the analyst find any threats that might have eluded detection by the current security solutions or configurations.

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 MITRE ATT&CK framework was introduced earlier in this lesson. 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 includes the **Threat Hunting** pane, which offers a SOC analytics dashboard using the SIEM database.

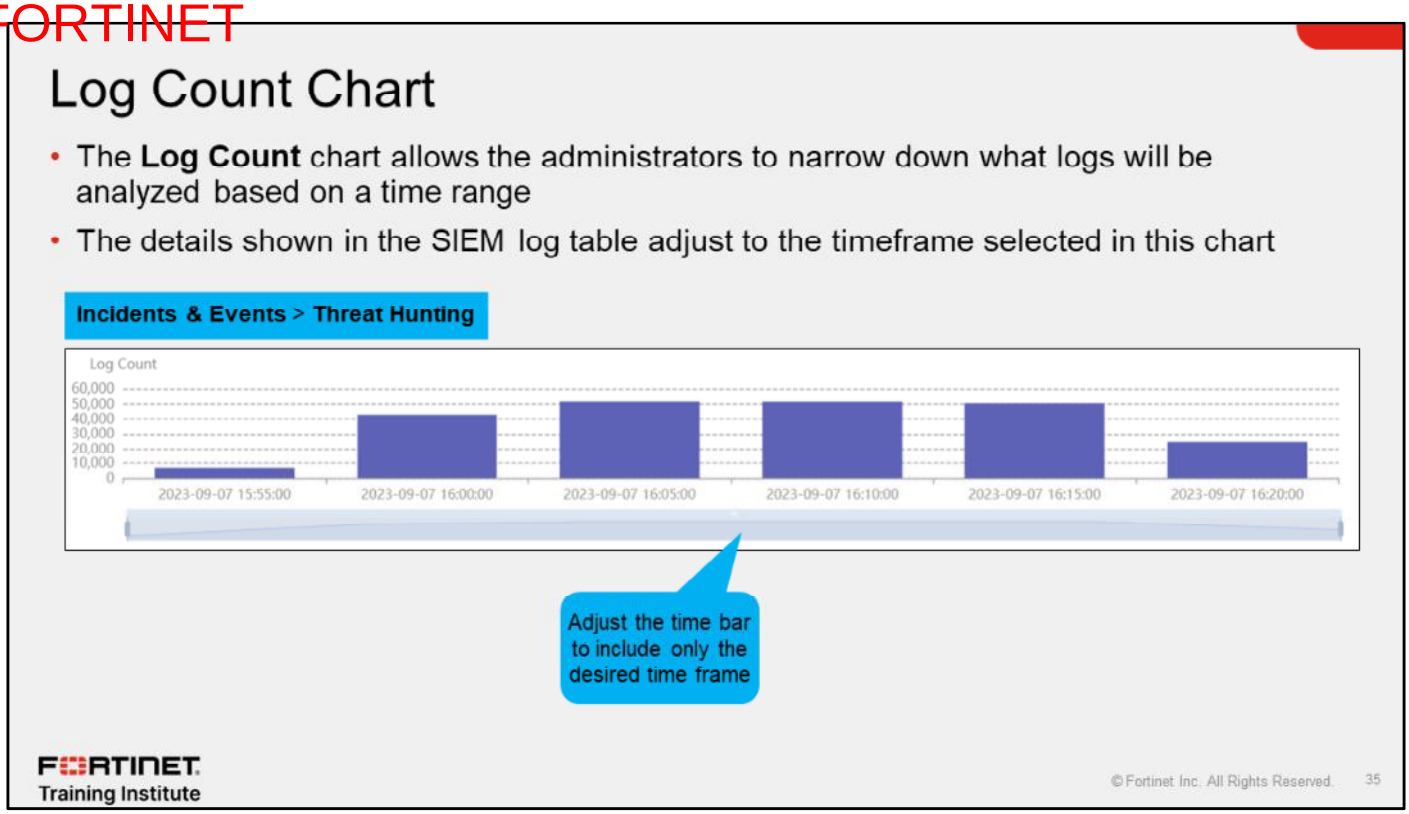
Threat Hunting uses cached data to allow SOC analysts to quickly drill down on logs in fields of interest. To view the **Threat Hunting** dashboard, click **Threat Hunting**. This dashboard includes a **Log Count** chart and SIEM log analytics table.

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. Only logs matching the selected time range and filter are displayed in the SIEM log analytics table.

In the left pane, click the field you want to view corresponding data in the table. 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 open 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?



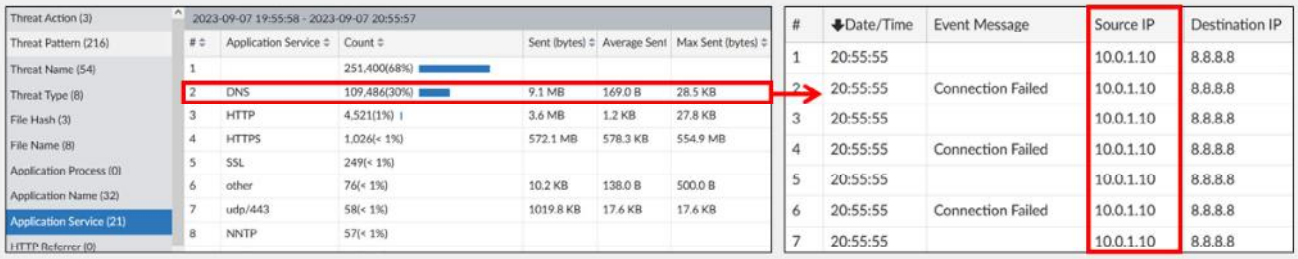
The top of the **Threat Hunting** dashboard shows a chart displaying the total log count during the specified time range. This section is called the **Log Count** chart.

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 are shown in the SIEM log analytics table.

Threat Hunting Example With FortiAnalyzer

- Based on the MITRE ATT&CK tactic *Exfiltration*, technique *Exfiltration over alternative protocol*, establish the following hypothesis/question:
  - *Has DNS tunneling been used to extract confidential data from the local network?*
- In this example, the analyst used the **Log Chart** to discover an unusual amount of DNS traffic
- Analysis shows the IP address `10.0.1.10` sending continuous queries at odd hours



- Further investigation determined that the host had been compromised. A new incident was created and the SOC responders can start containment and eradication steps

Note: The images shown here do not represent a real attack. They are used only to illustrate the scenario described.

FORTINET Training Institute

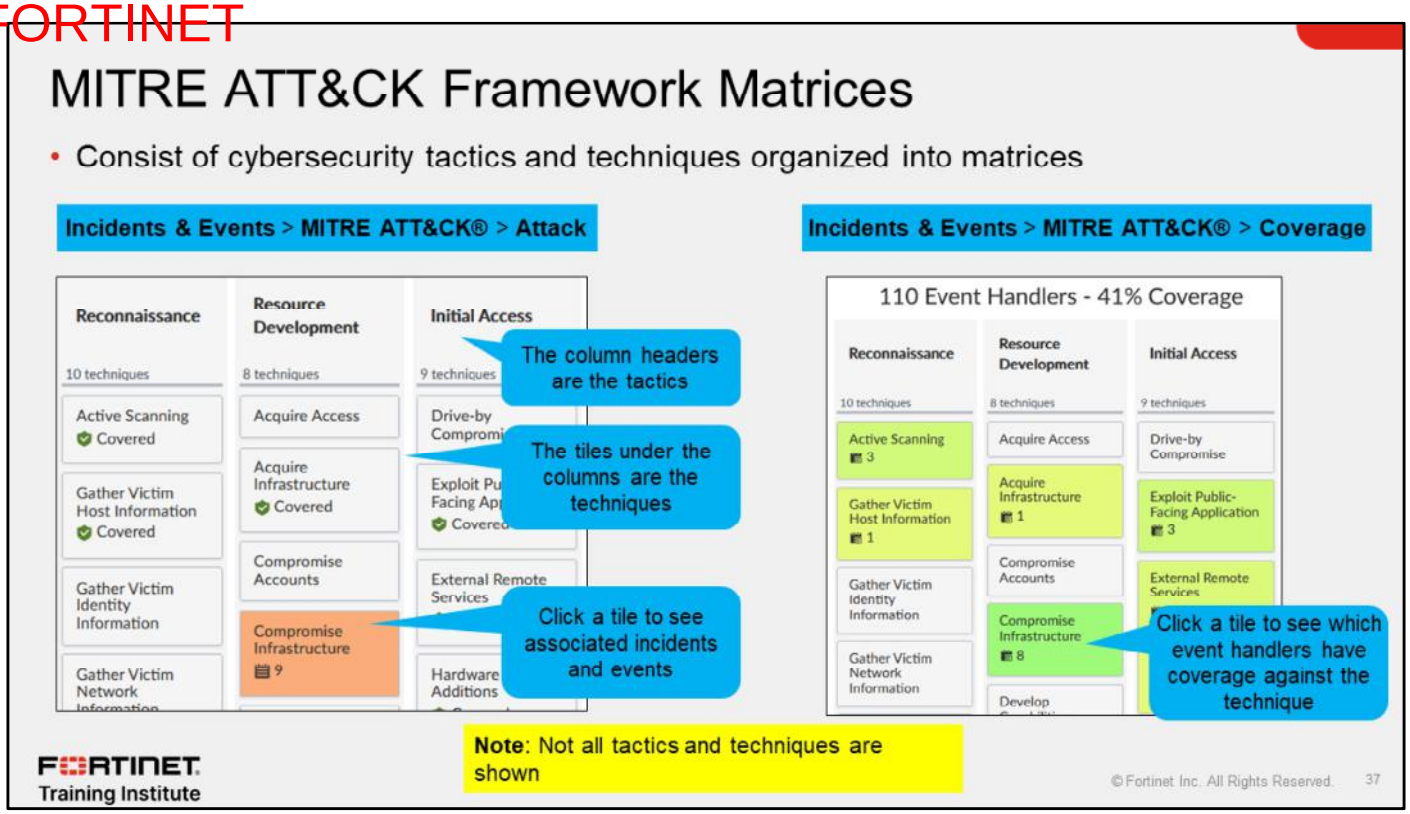
 36

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*, 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 operation 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 **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 on cybersecurity threats, including classifications, descriptions of attack vectors, real-life examples, mitigation steps, detection methodology, and so on. You can find more information on the framework on the MITRE website.

The columns 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, such as the severity, information on the technique and sub-technique, affected endpoints, and the total number of incidents and events. For example, the **Compromise Infrastructure** tile has nine associated events.

You can review event handler coverage on the **Coverage** pane. It will show you the number of event handlers and what 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

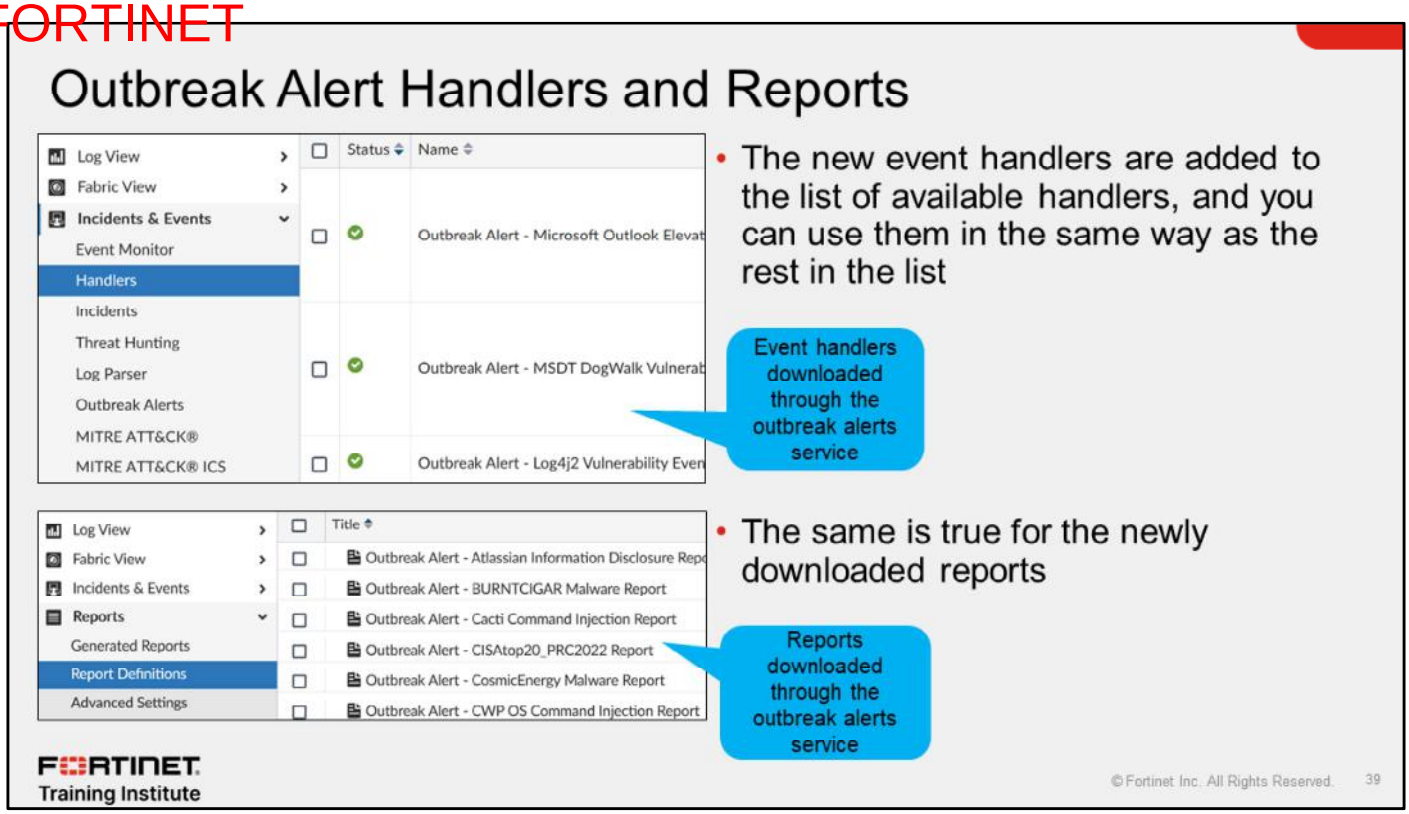
- Licensed feature
- Allows customers to receive information about malware outbreaks
- Automatically downloads new event handlers and reports related to the outbreaks

FORTINET Training Institute

 38

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 under the **Event Handler** list, and they can be used in the same ways described in an earlier section. That is, you can clone, export, import them, and so on.

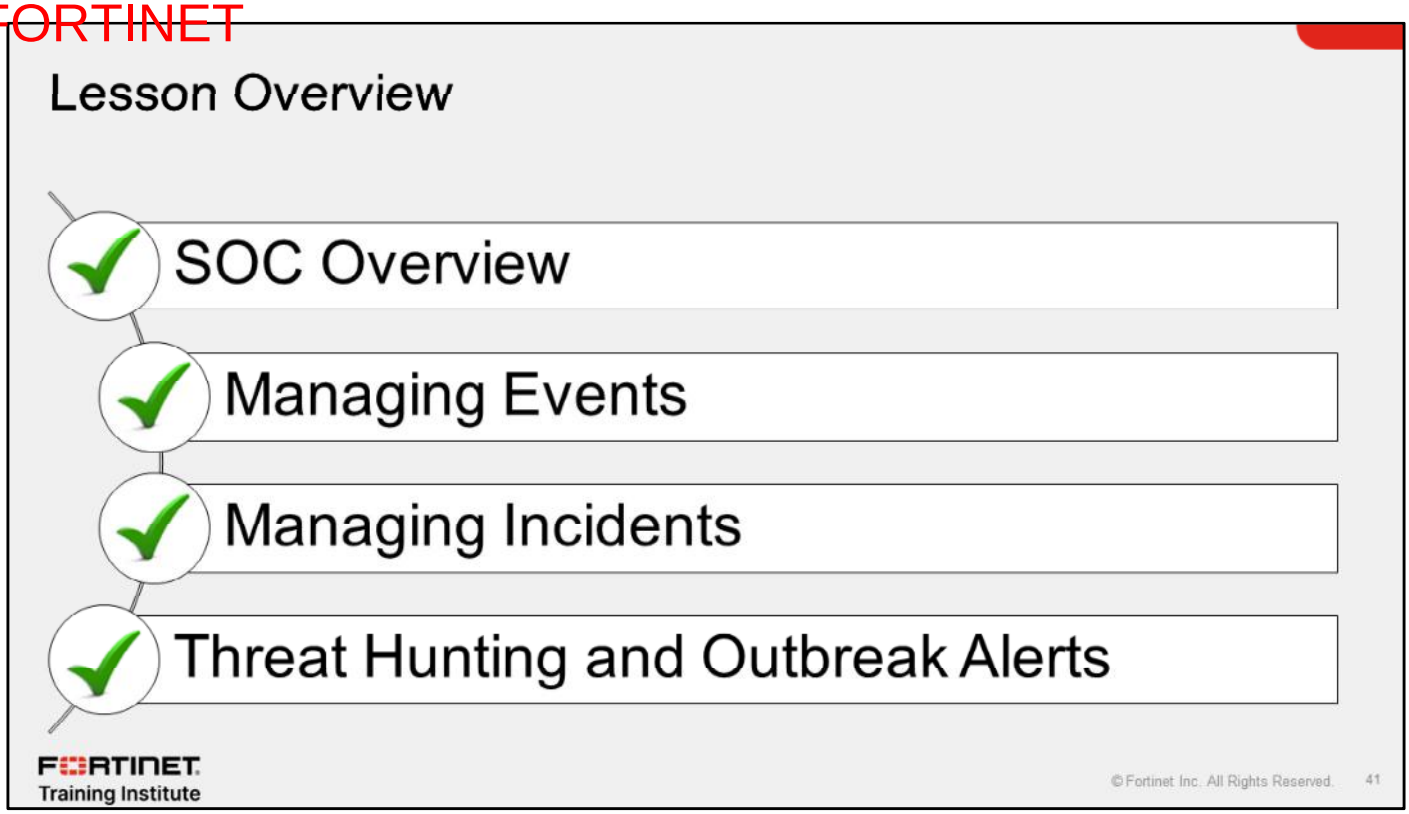
The same is true for the new reports.

Knowledge Check

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

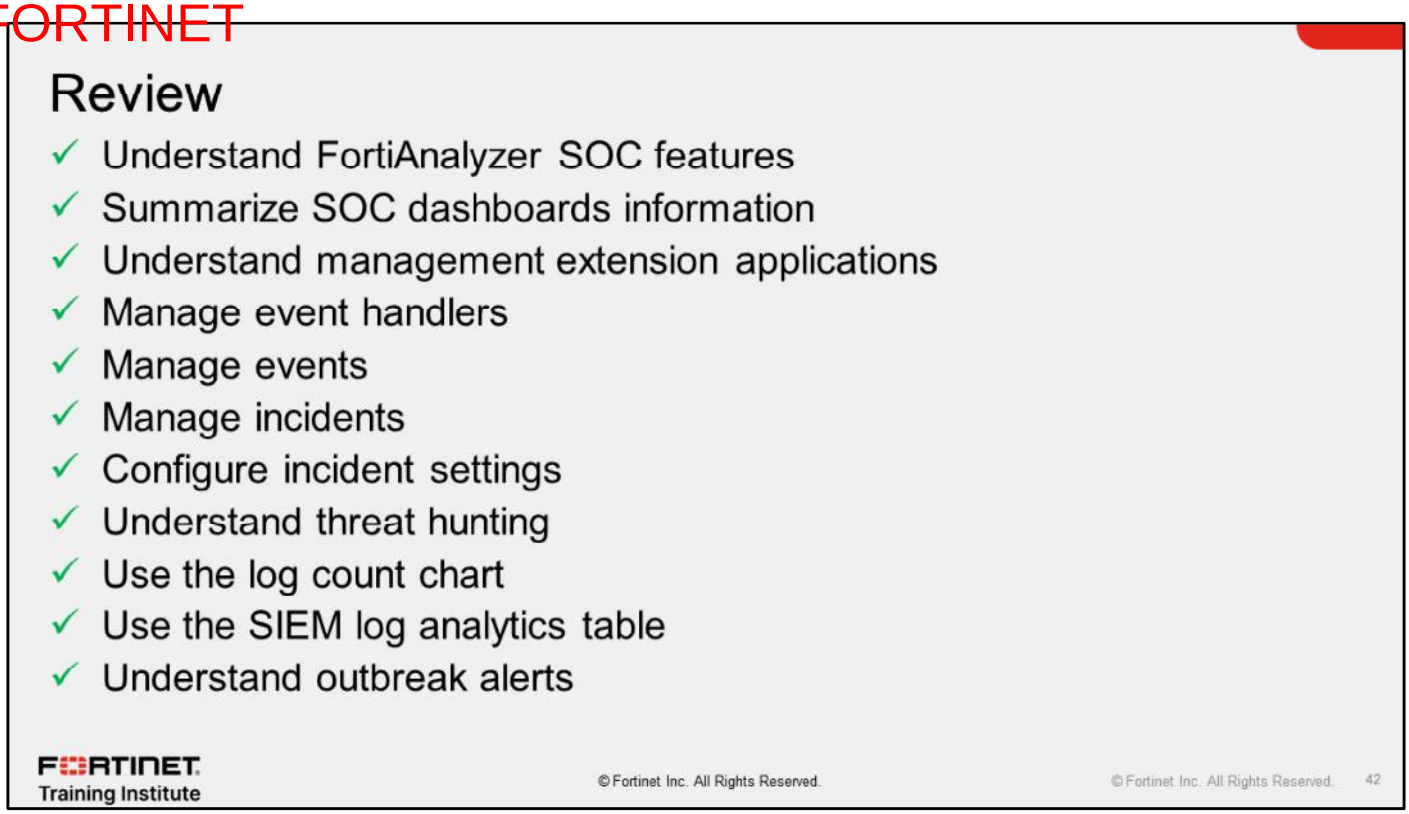
FORTINET Training Institute

 40



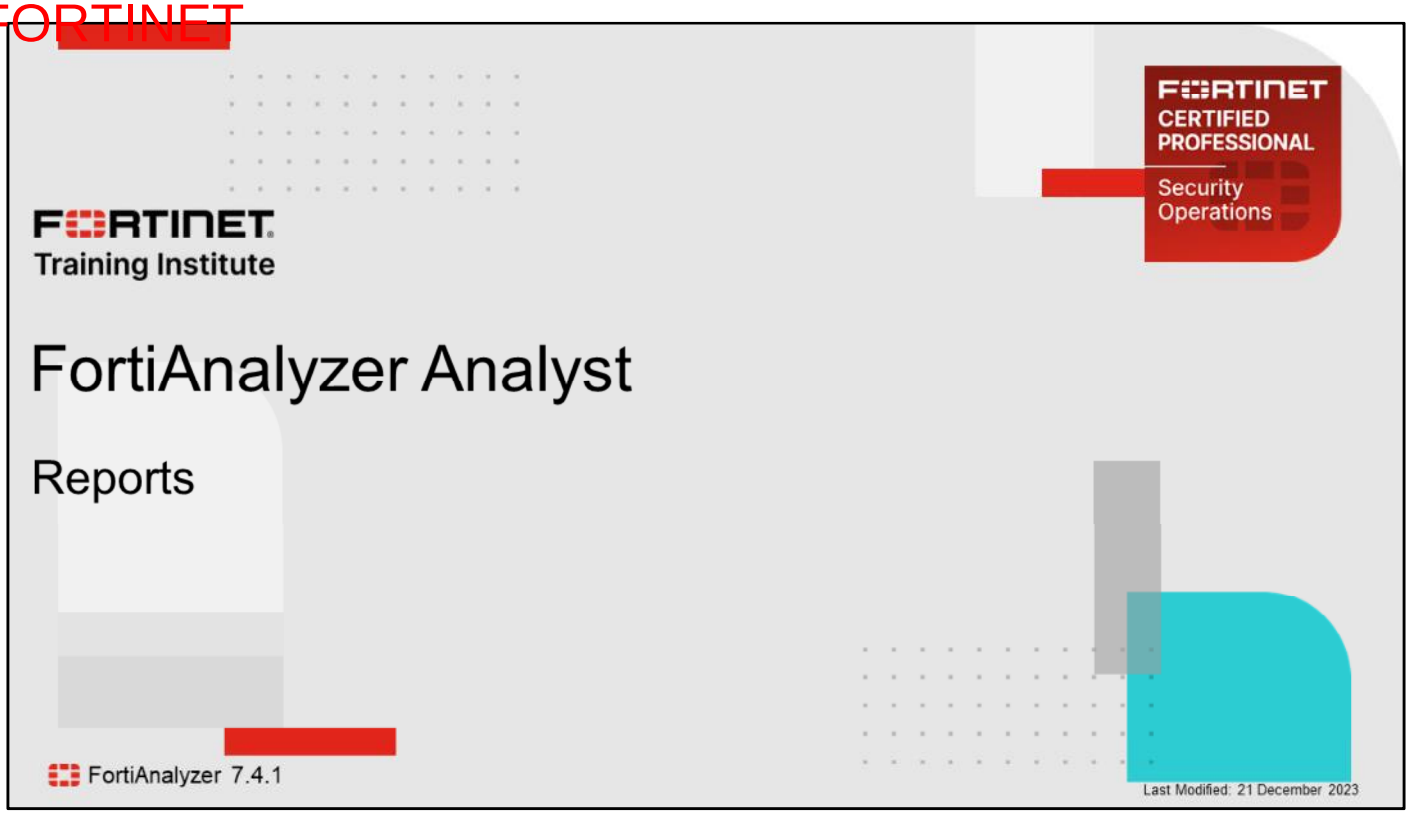
Congratulations! You have completed this lesson.

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

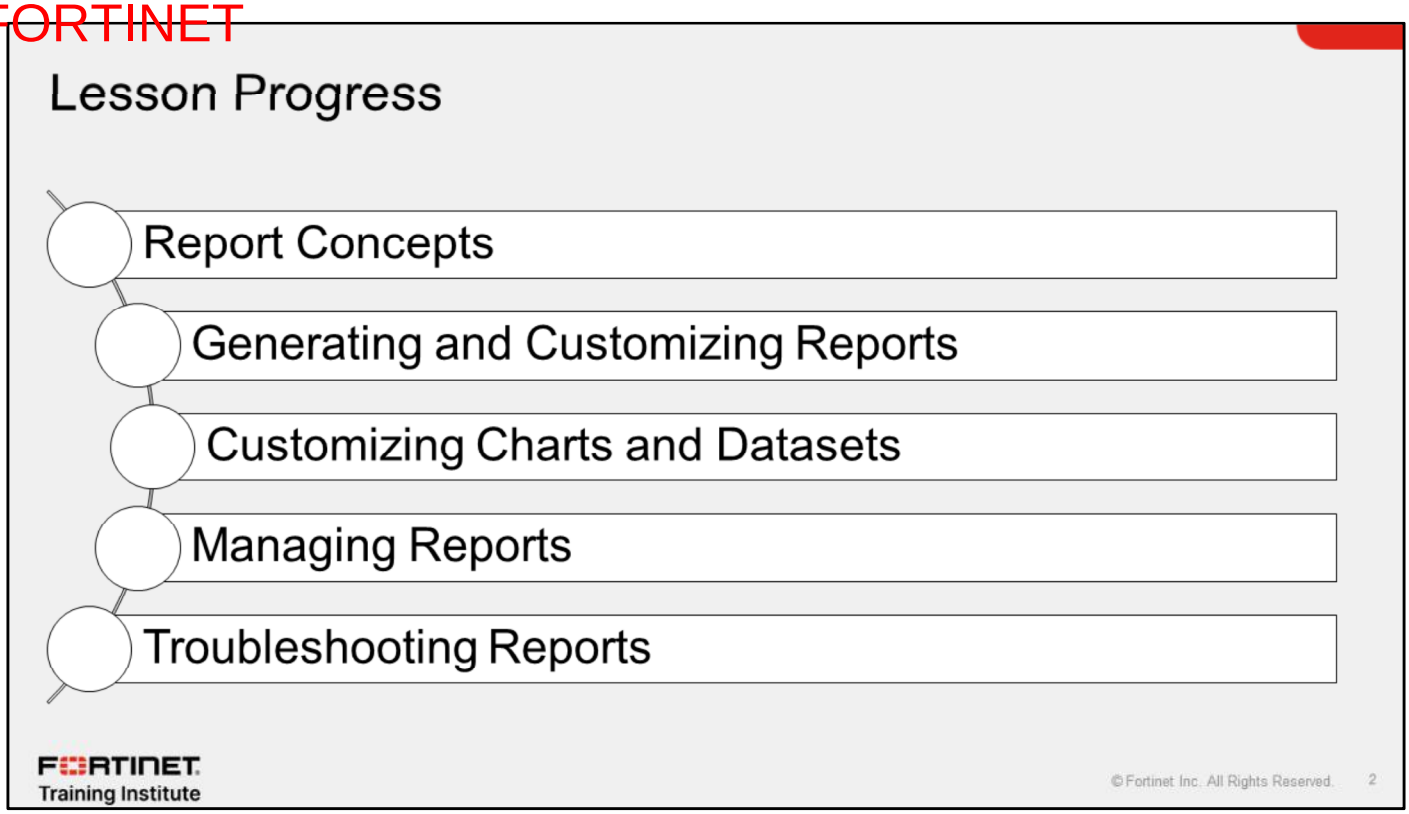


This slide shows the objectives that you covered in this lesson.

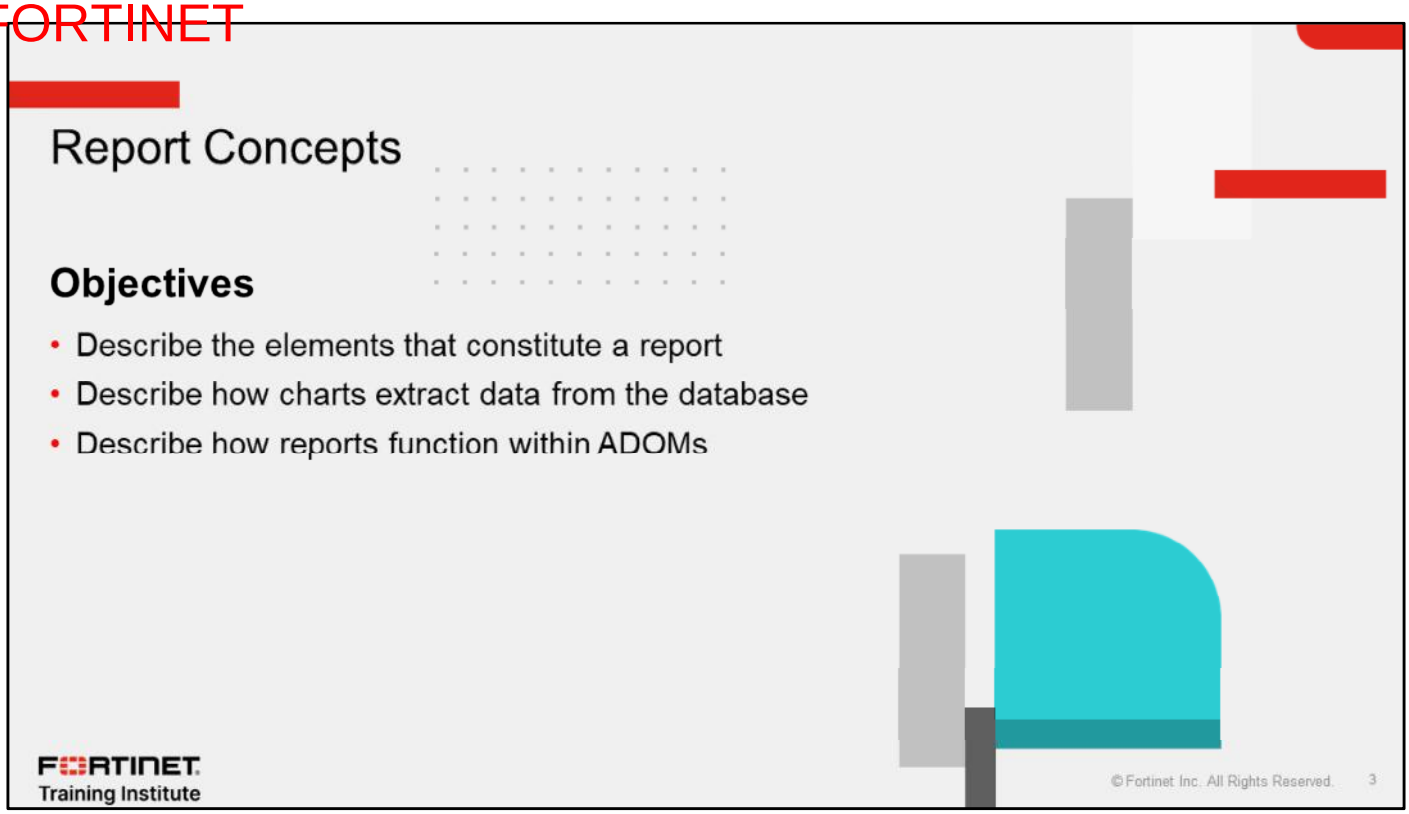
By mastering the objectives covered in this lesson, you learned about SOC components and features, and how to use them in your network.



In this lesson, you will learn how to extract useful information from your logs for analysis purposes. To do this, you will 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.

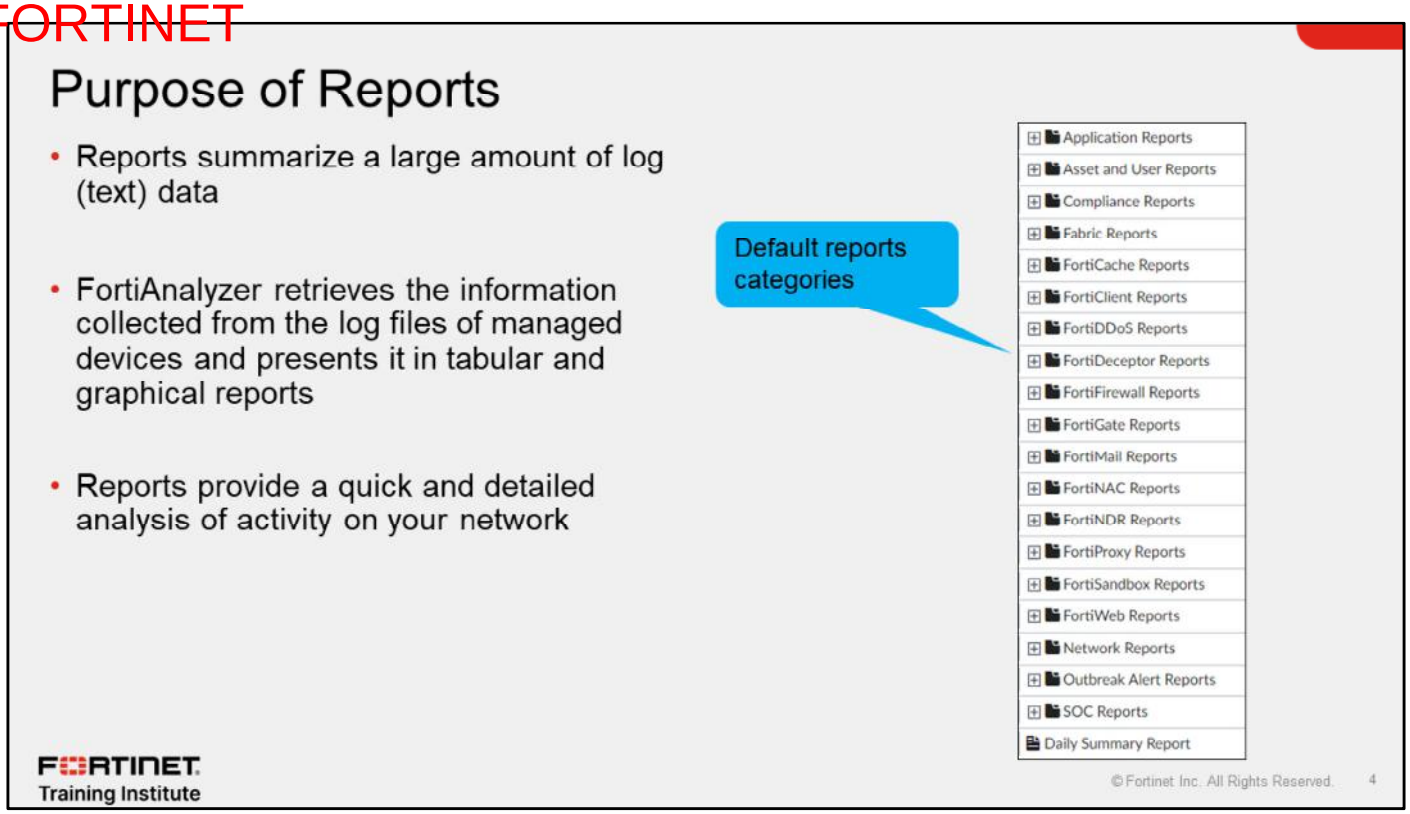


In this lesson, you will explore the topics shown on this slide.



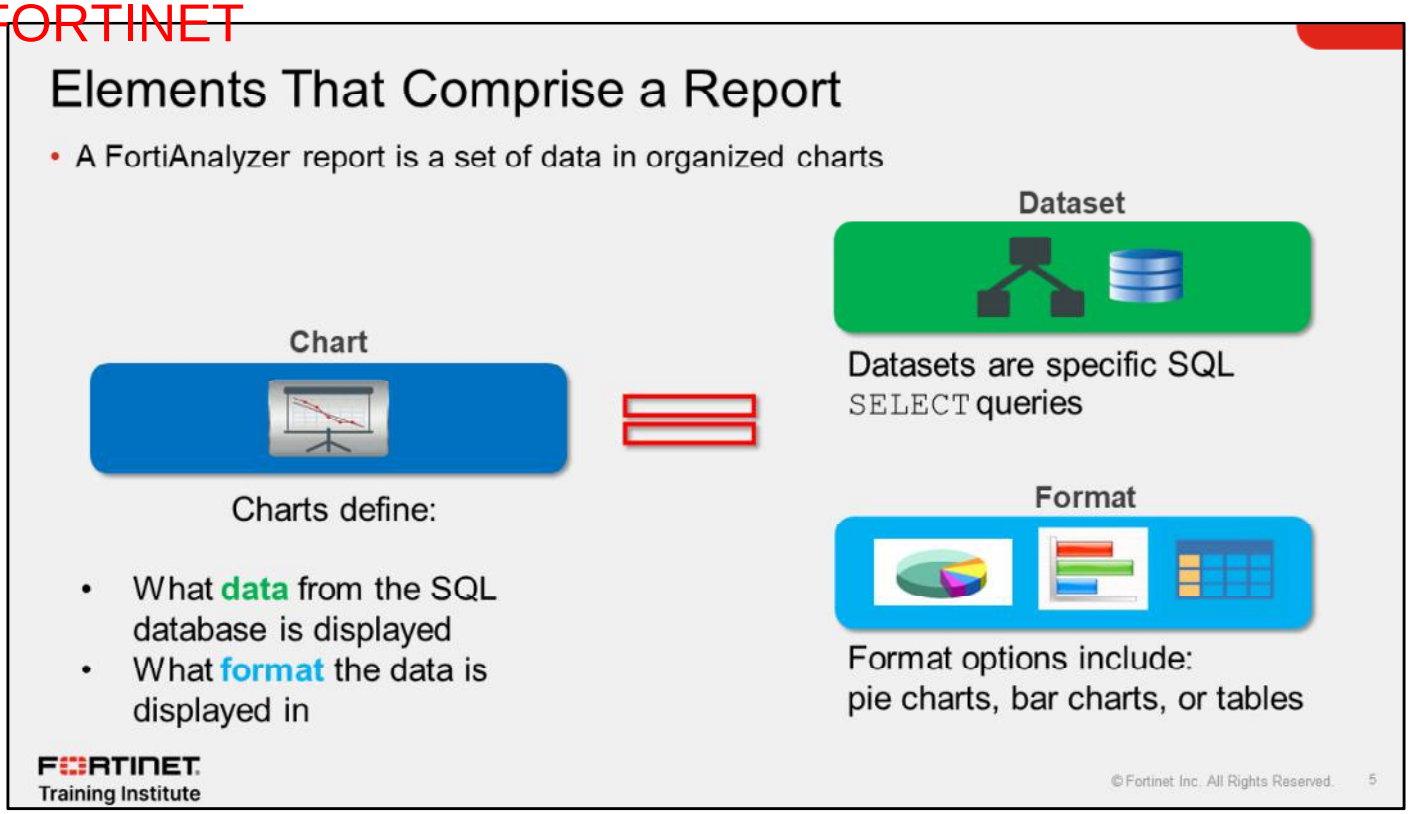
After completing this section, you should be able to achieve the objectives shown on this slide.

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



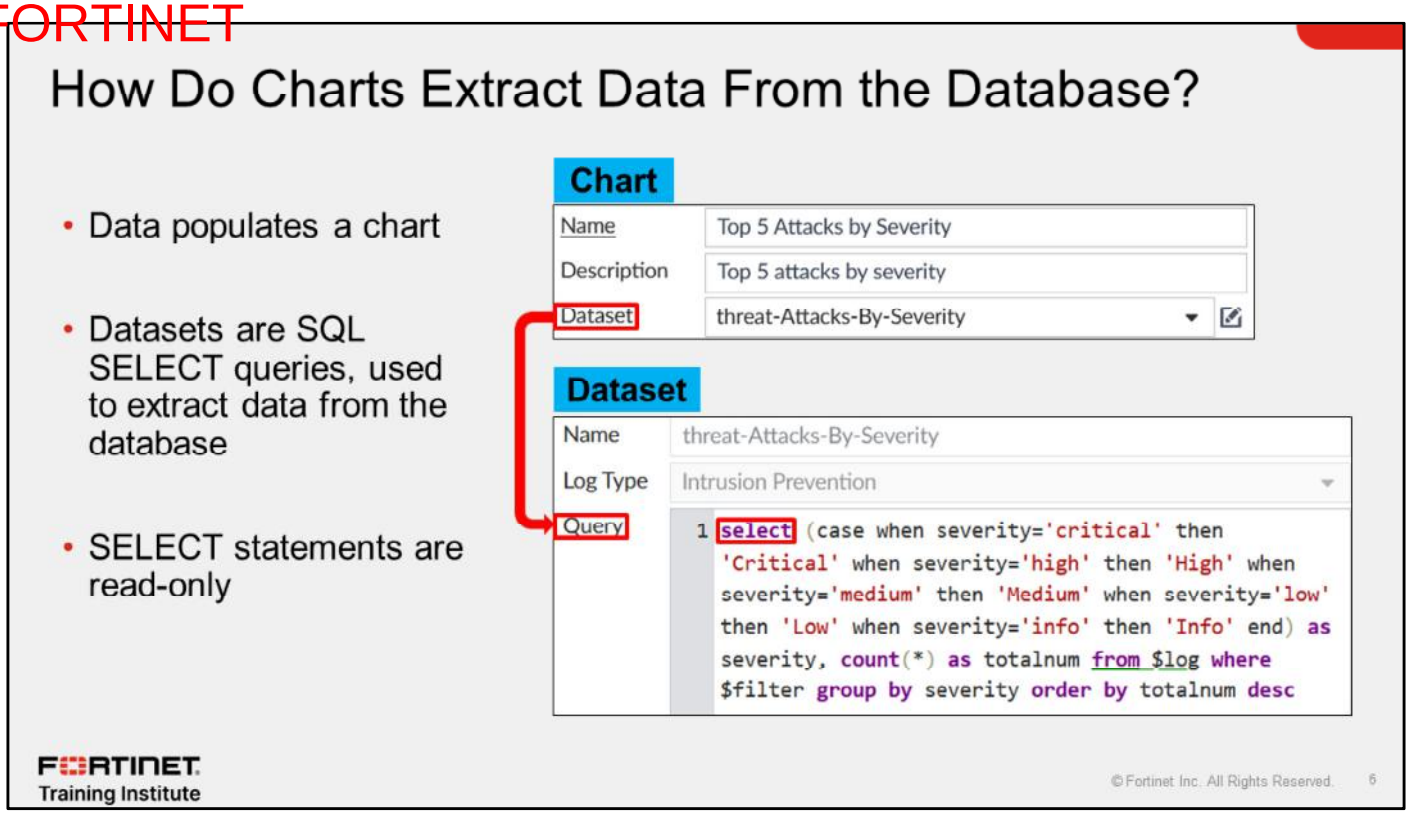
The purpose of a report is to summarize large amounts of logged data. Based on configured report parameters, FortiAnalyzer extracts data and presents it in a graphical manner that makes it easier—and quicker—to digest. The patterns and trends that reports reveal already exist as several points of data within your database, but it would be 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 any recommendations or give any indication of 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)

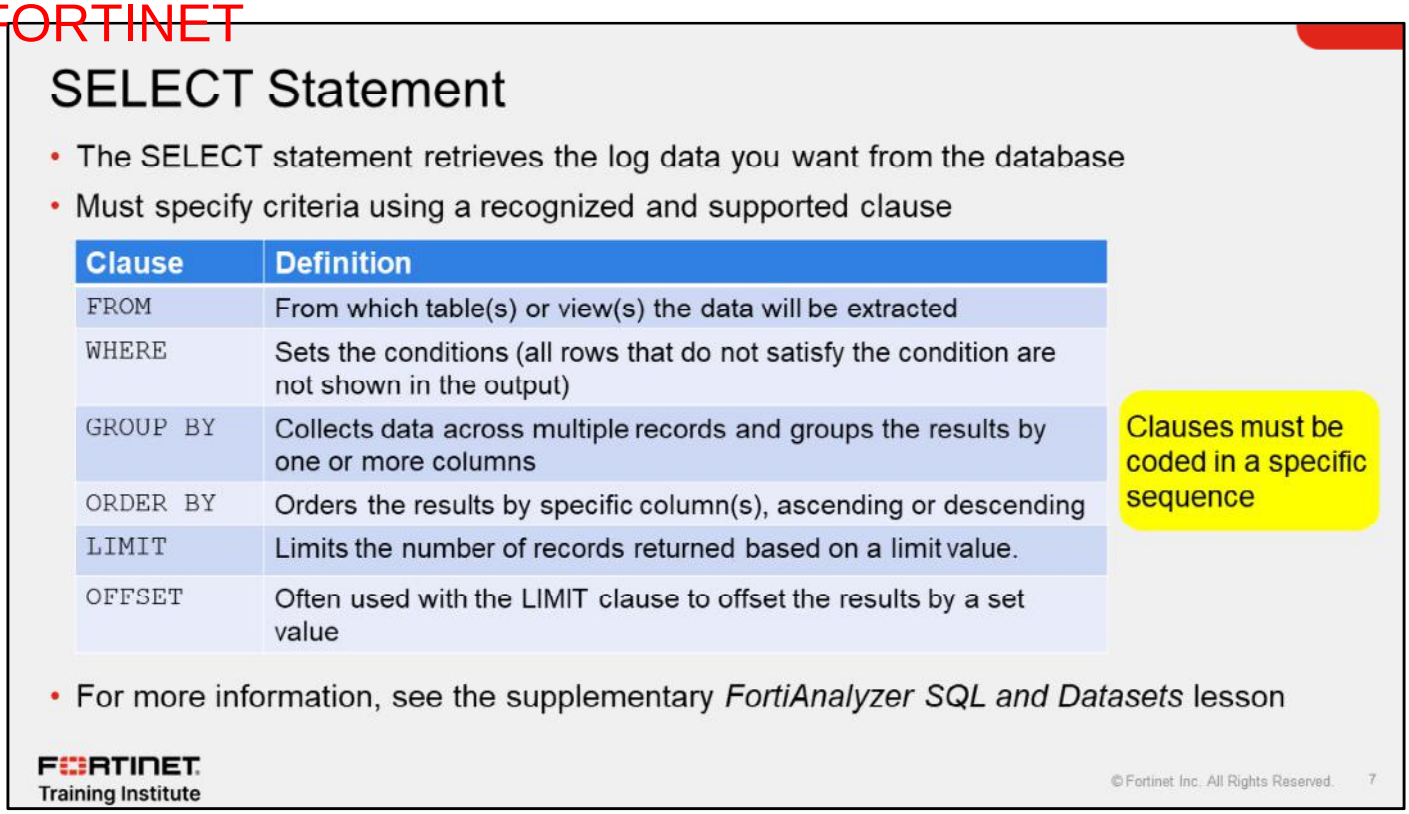


In order to populate a chart with specific log data that has been collected, stored, and sorted in the SQL database, reports rely on a dataset query to extract that log data. A dataset is a specific SQL `SELECT` query—a read-only statement that retrieves data from the database.

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.

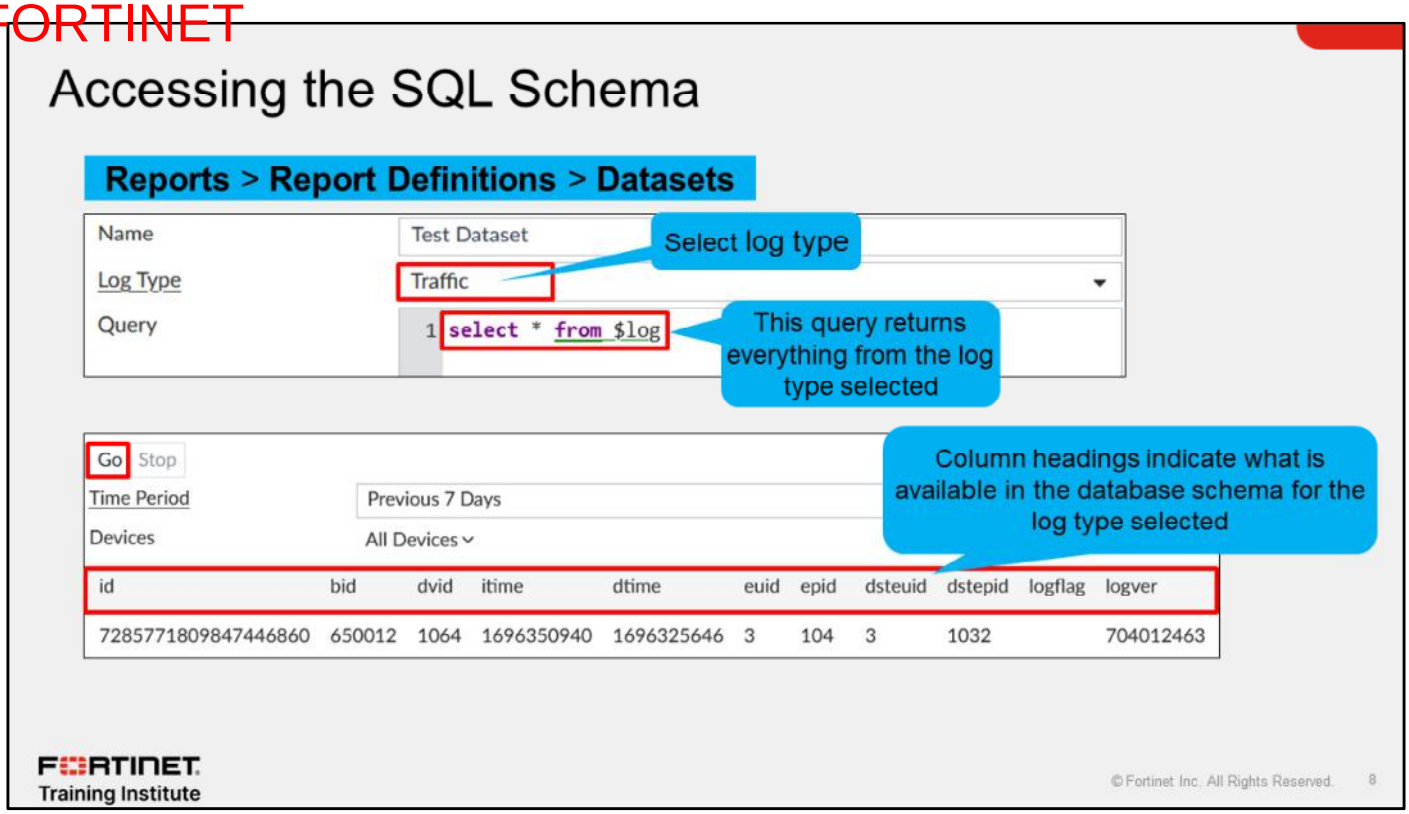


To extract the desired data, you need to specify the criteria to be used. In order to put this criteria into a language that SQL understands, you must use one or more clauses recognized by the `SELECT` statement.

The main clauses FortiAnalyzer reports use are as follows:
- `FROM`, which specifies from 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`, clause often used along with `LIMIT`, which 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 on SQL and datasets for use with FortiAnalyzer reports, see the supplementary *FortiAnalyzer SQL and Datasets* lesson.



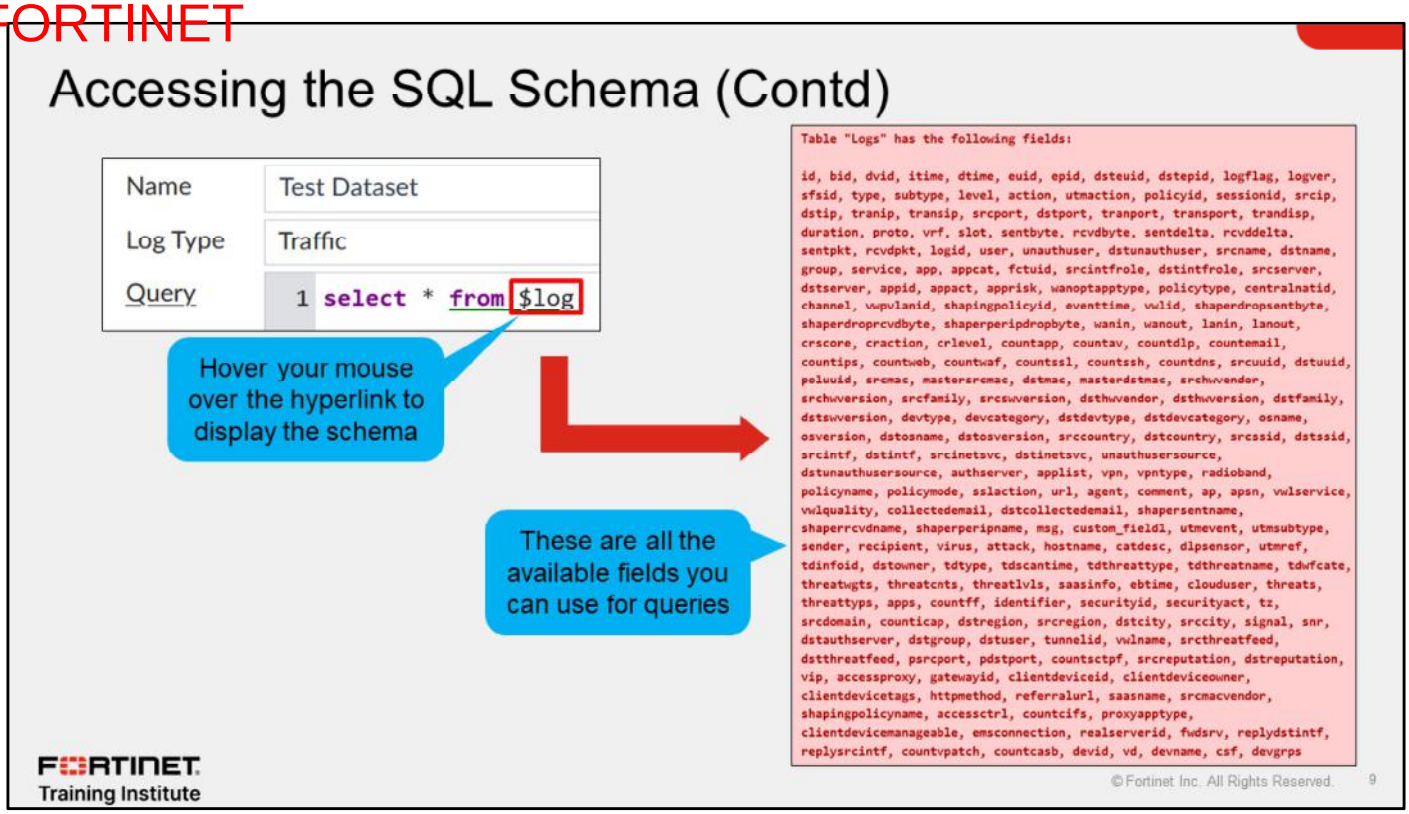
To create a query, you first need to know what is included in the database schema. The schema is the different fields, or columns, that are available, and from which you can extract information for reports. In FortiAnalyzer, you can obtain the schema for a specific log type by creating and testing the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

```
SELECT * FROM $log
```

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

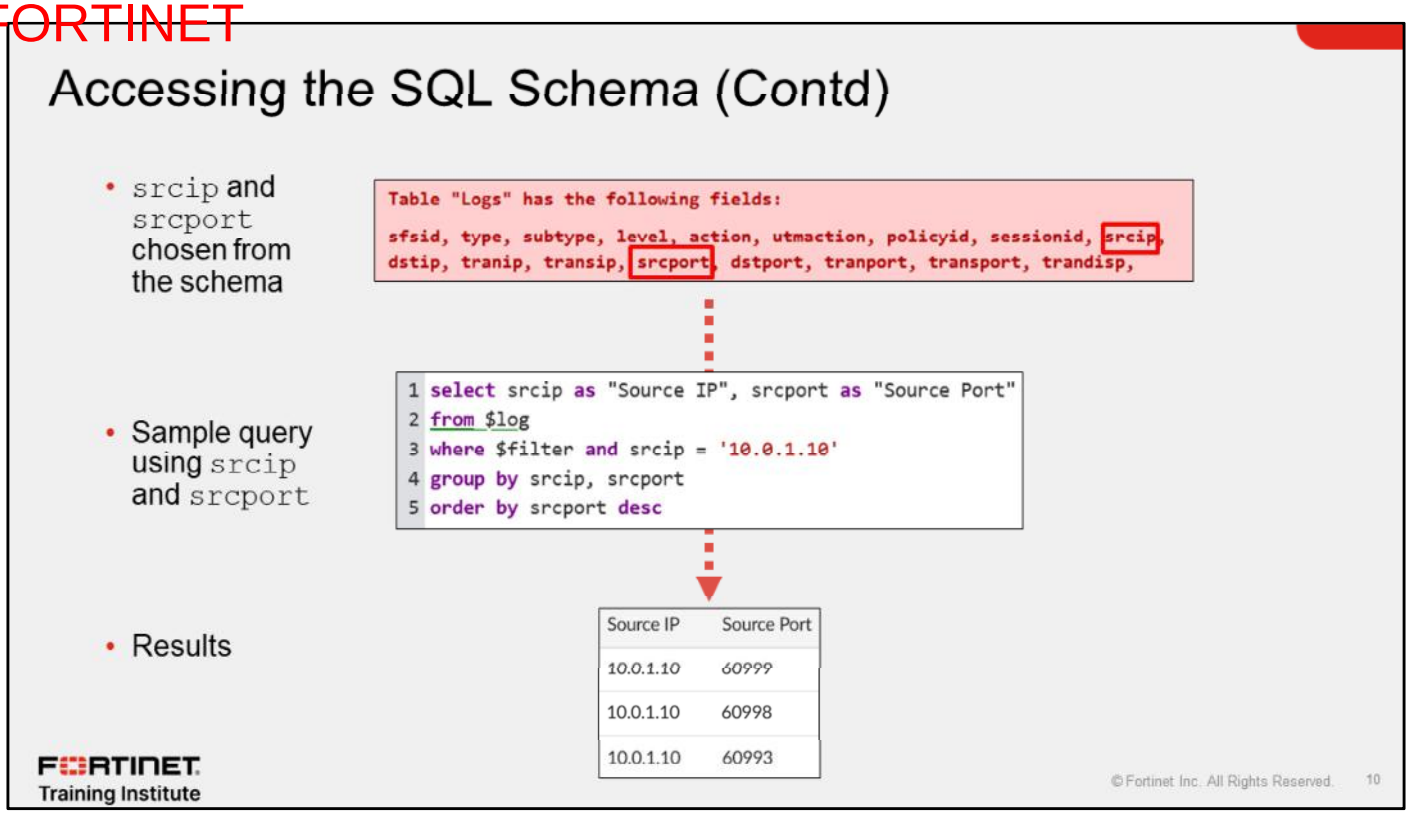
For traffic logs, for example, associate the **Traffic** log type with this dataset in the **Log Type** field. This query returns everything from the **Traffic** log type. The column heading names indicate what is available in the database schema for the log type selected. The * symbol returns all data.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

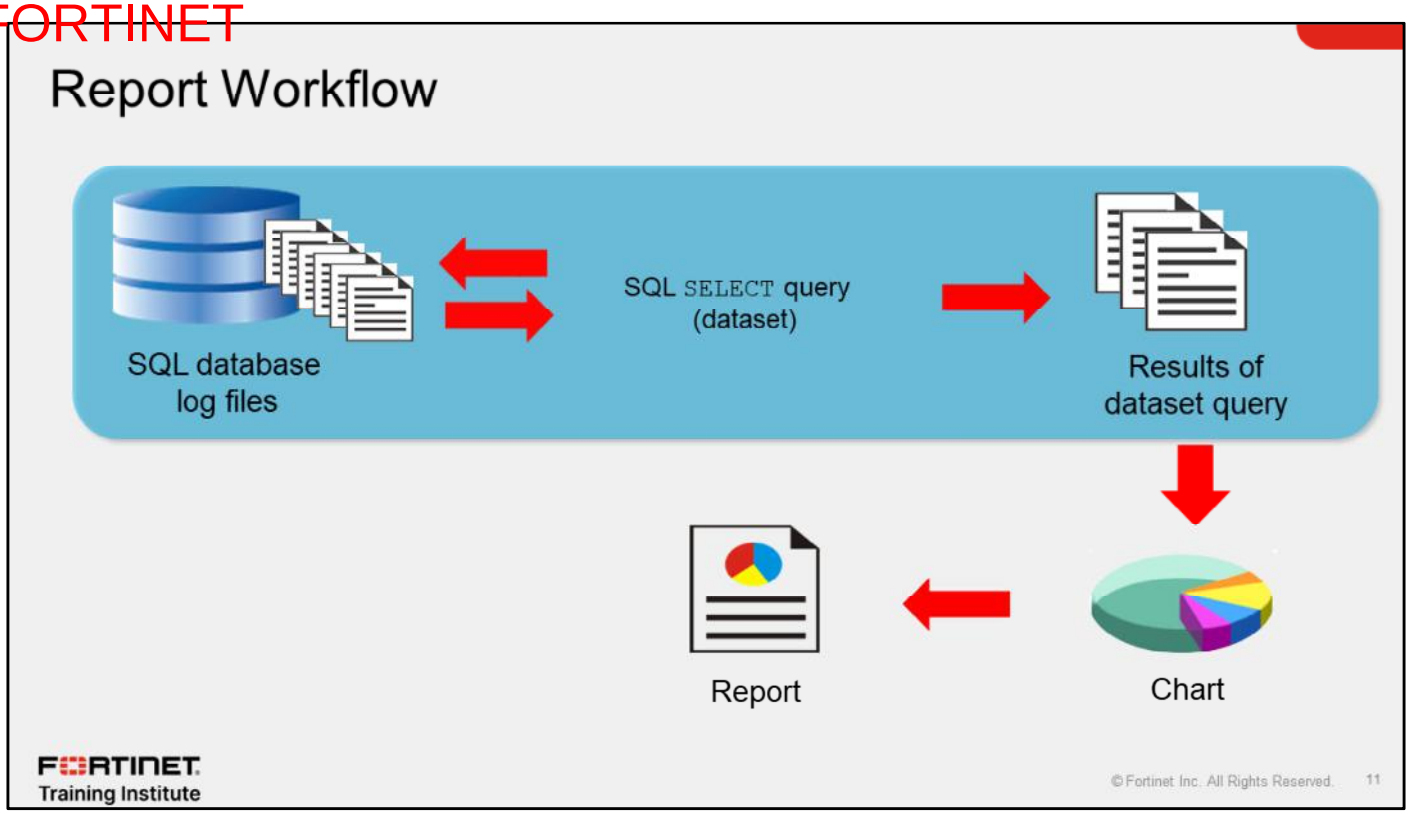
As you can see on this slide, the number of fields can be very large. For this reason, cloning and editing one of the predefined datasets may be the best approach, if none of them meet your requirements.



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.



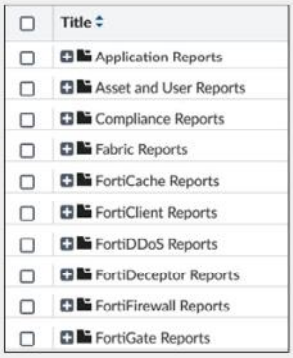
As the graphic on this slide shows, the SQL database contains all the logs. A SQL `SELECT` query polls the database for specific information. Based on the query, a subset of information stored in the logs is extracted.

This subset of data populates a chart, and one or more charts exist within a report.

Reports and ADOMs

- Each ADOM has its own reports, libraries, and advanced settings
- Additional reports are available when specific ADOMs are enabled
- Verify you are in the right ADOM when creating reports

Note: A fabric ADOM has default reports for multiple device types

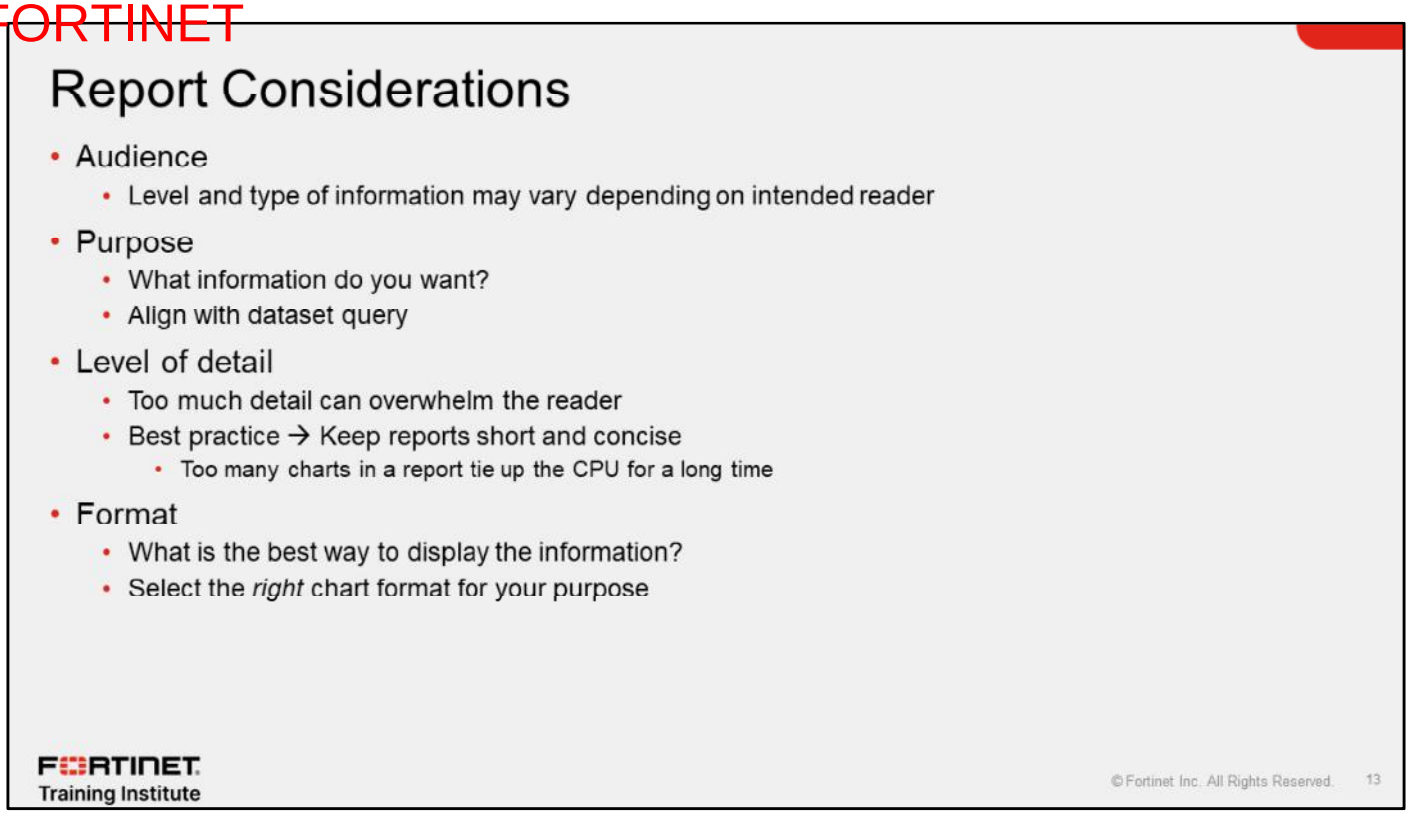


FORTINET Training Institute

 12

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 looking at this report? Depending on what they want to see and their level of skill, 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 that query. So, reports must be focused in order 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 the 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 right chart. Think about how the data would best be represented visually, and about the audience consuming the data.

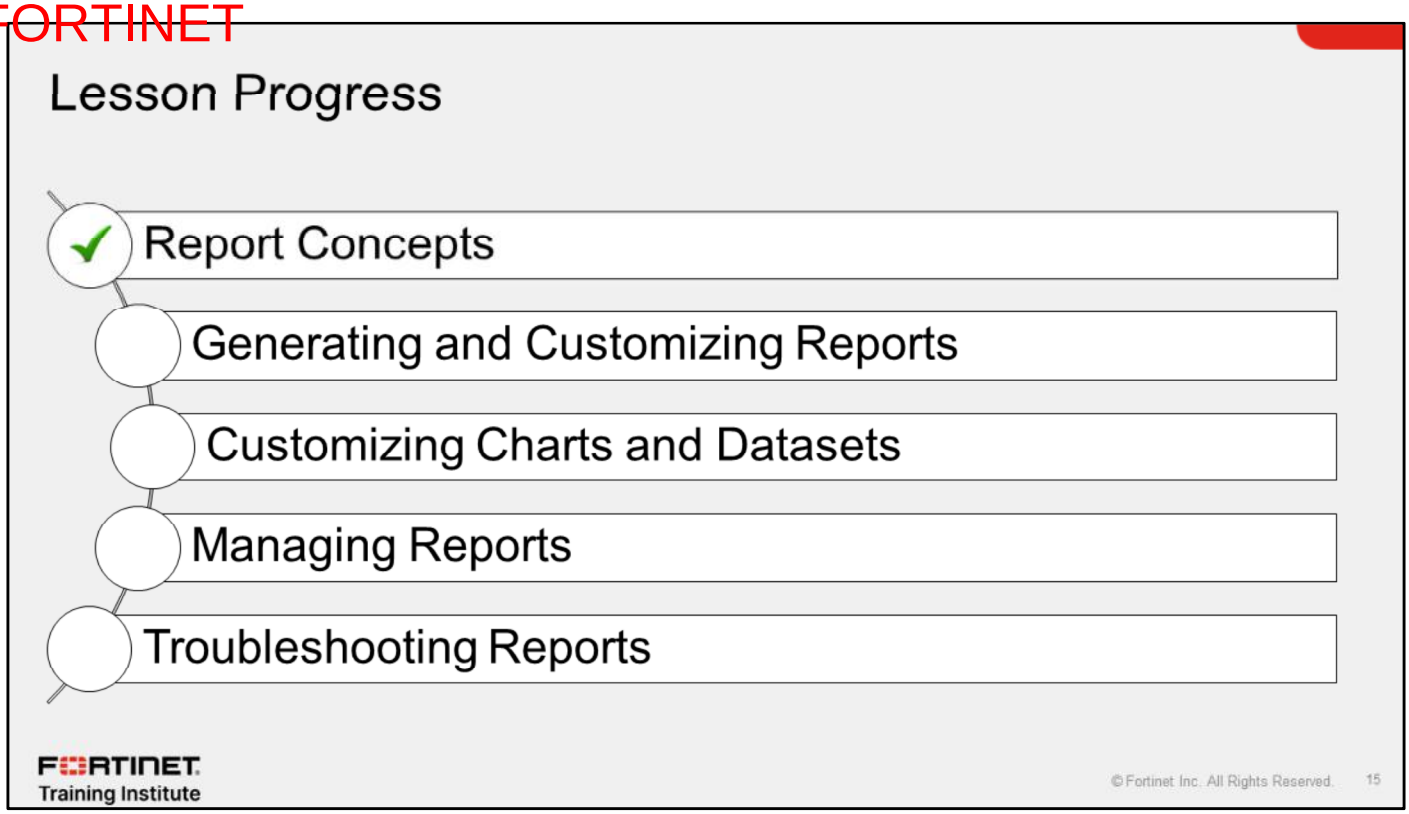
Aside from the chart format, you can also change the design of the report by adding separators, page breaks, images, and renaming charts.

Knowledge Check

1. In 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

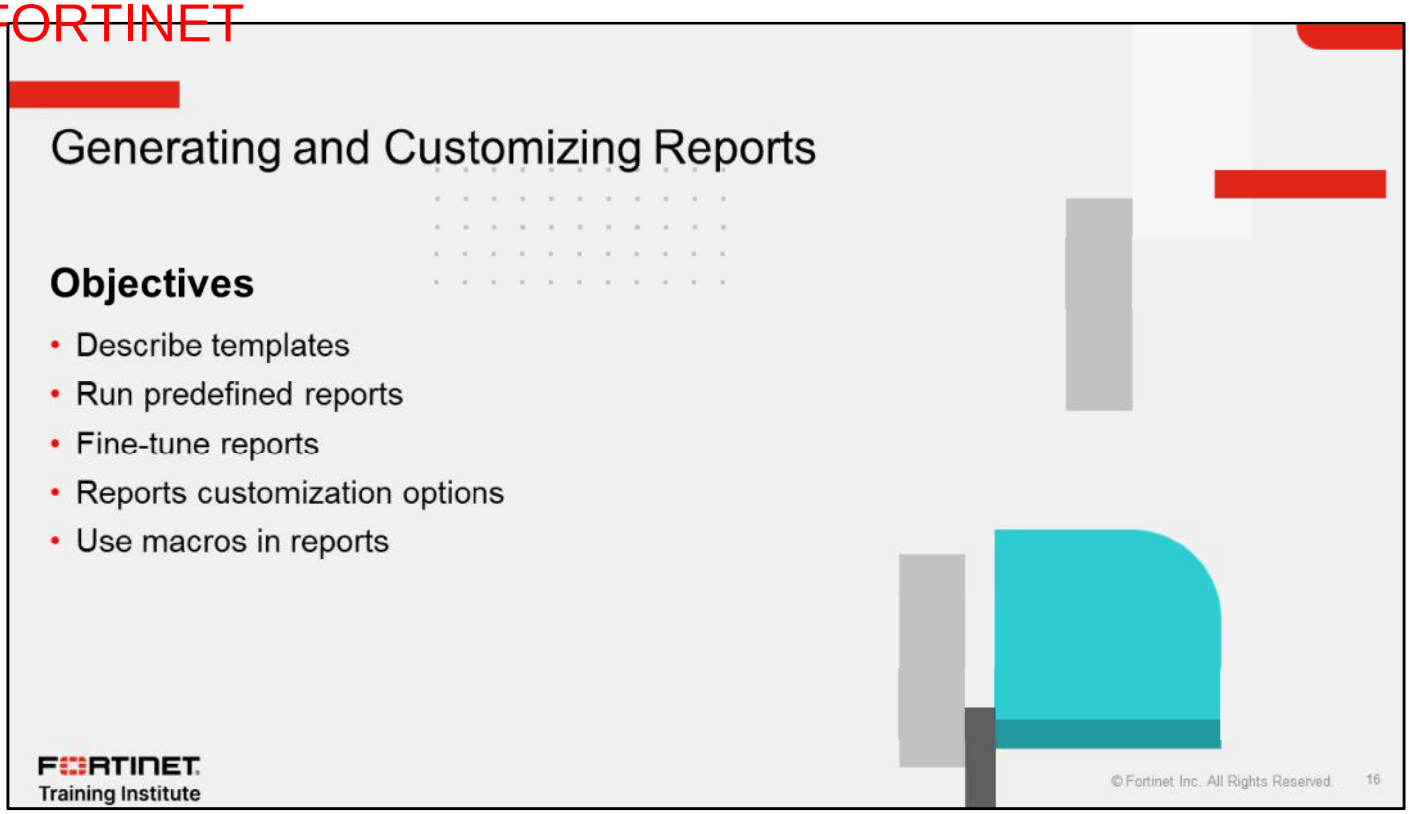
FORTINET Training Institute

 14



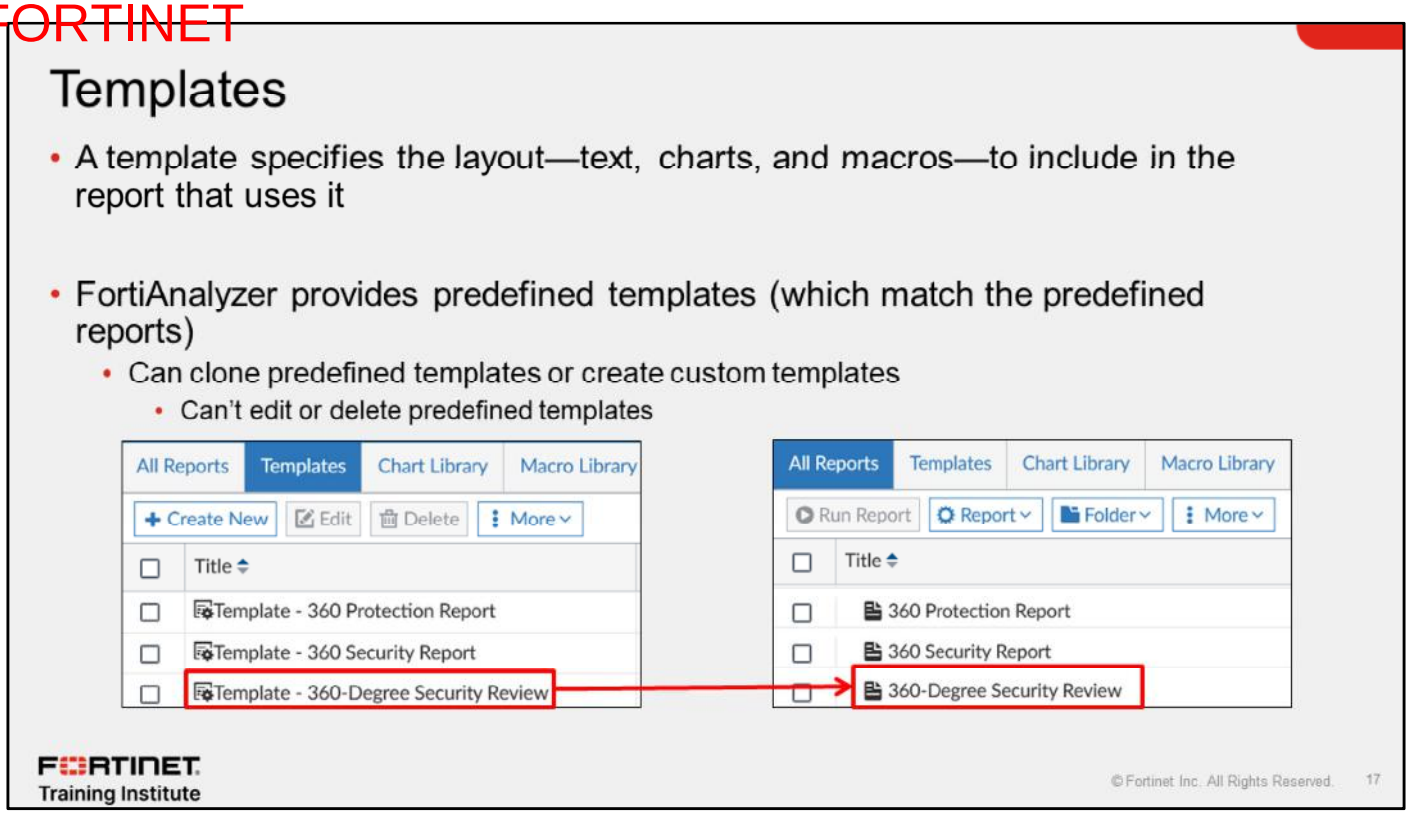
Good job! You now understand report concepts.

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.

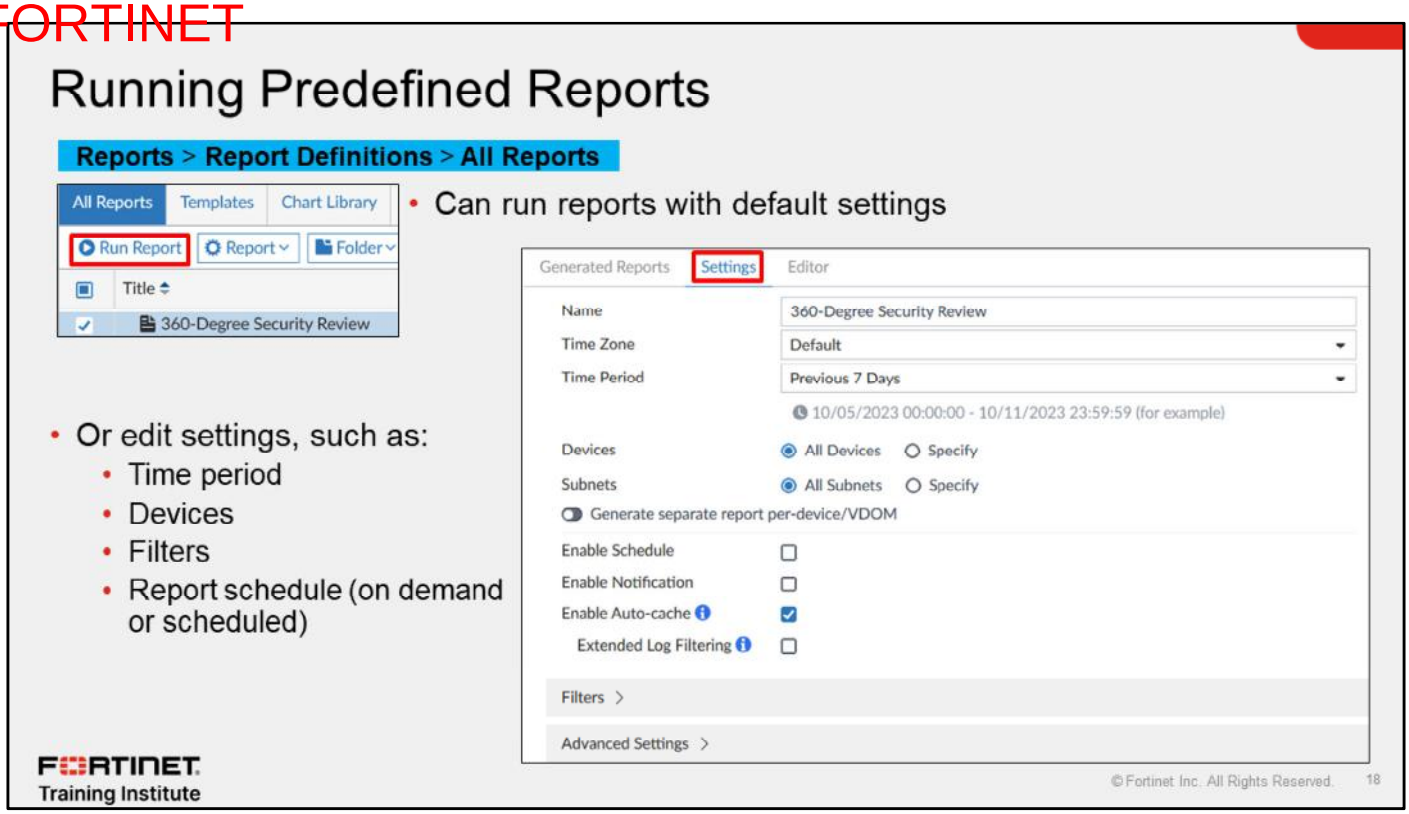
By demonstrating competence in report generation and customization, you will be able to generate reports specific to your requirements.



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.

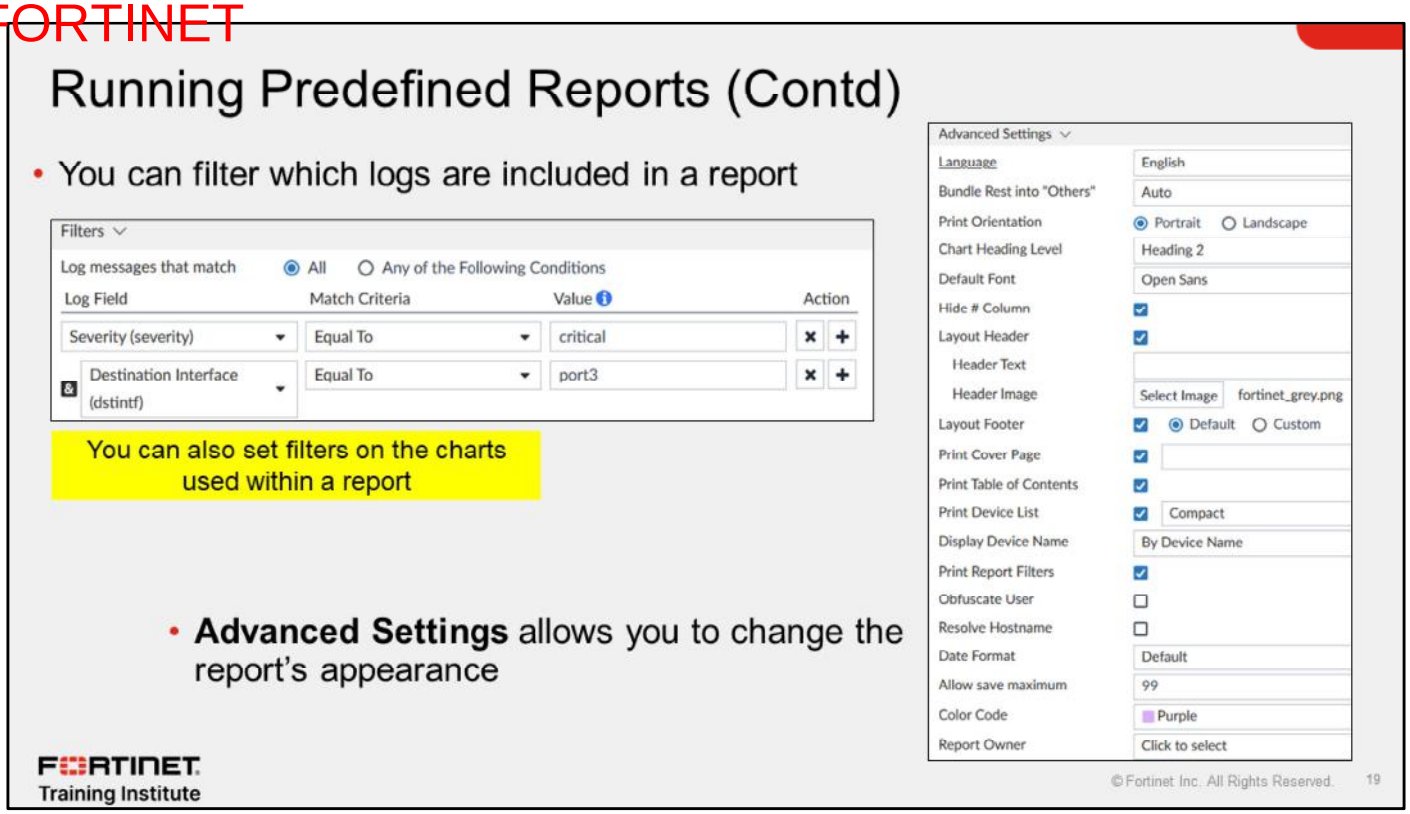


FortiAnalyzer also provides predefined reports—each one associated with a predefined template (the layout). Predefined reports come with basic, default settings already configured. These basic settings define the time period in which to run the report; which device, or devices, to run the report on; 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.

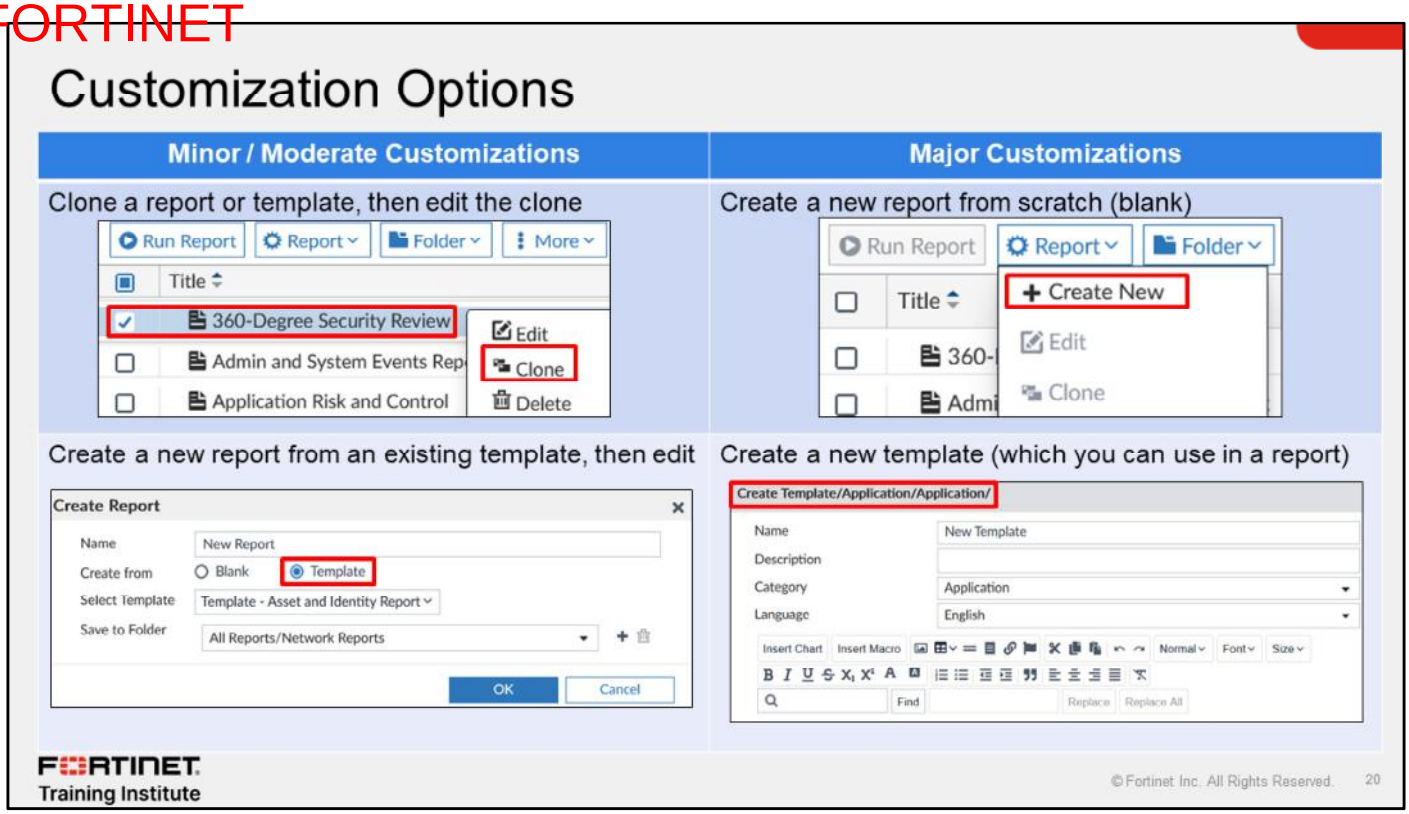
After it is generated, you can view a report in multiple formats, including HTML, PDF, XML, CSV, and JSON.



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 to a pre-existing LDAP server to add an LDAP query to the report
- Configuring report language, print settings, and other settings. For example, you can print and customize the cover page, print the table of contents, print a device list, obfuscate users, and set the color code for the report to appear under **Report Calendar**.



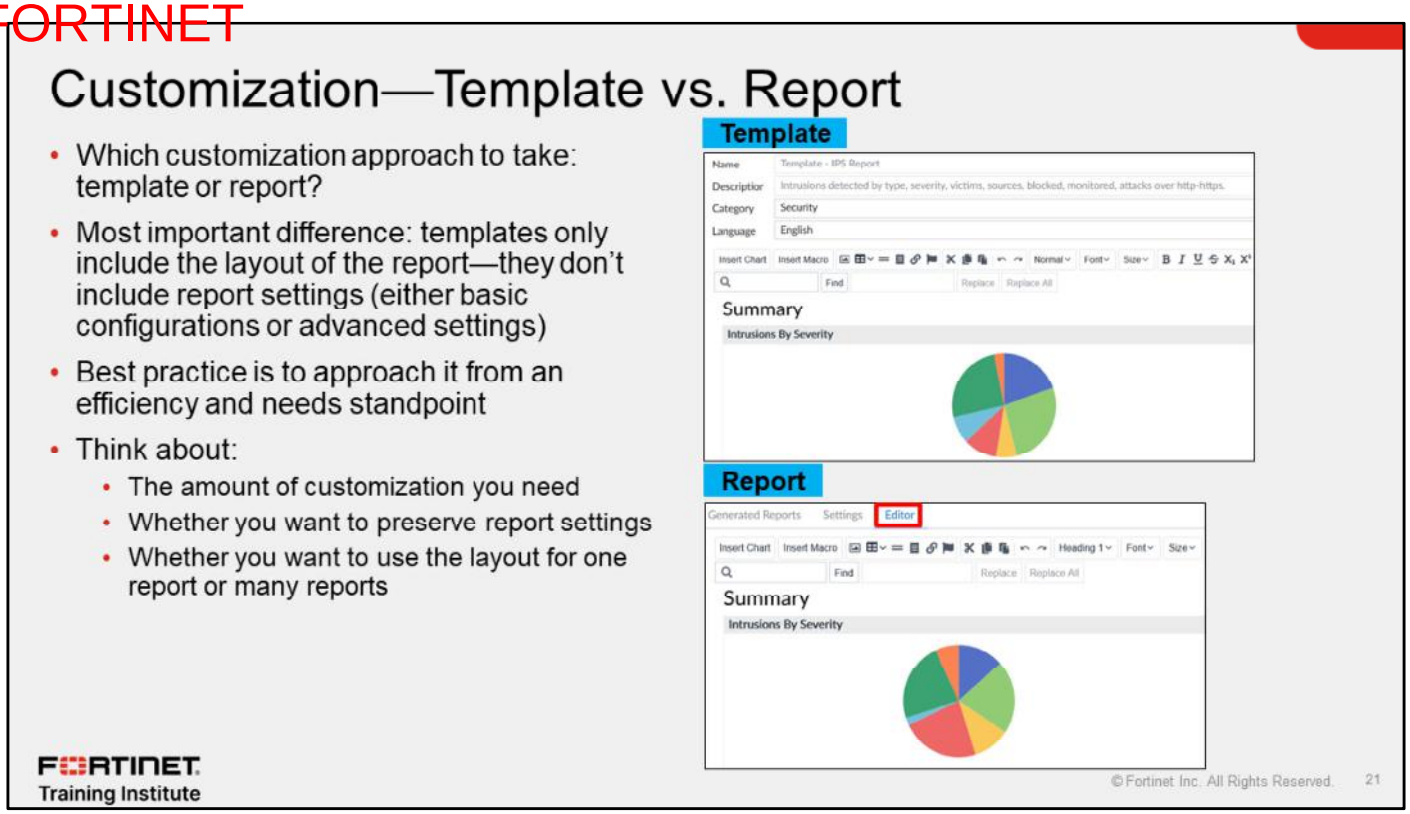
Predefined reports may not meet all of your organization's requirements, even after you fine-tune the report settings. FortiAnalyzer provides you with the option to create new templates and reports from scratch, or you can customize existing templates and reports.

To make minor or moderate changes to existing templates or reports, you can use cloning. To use cloning, you would 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 to the report are not successful.

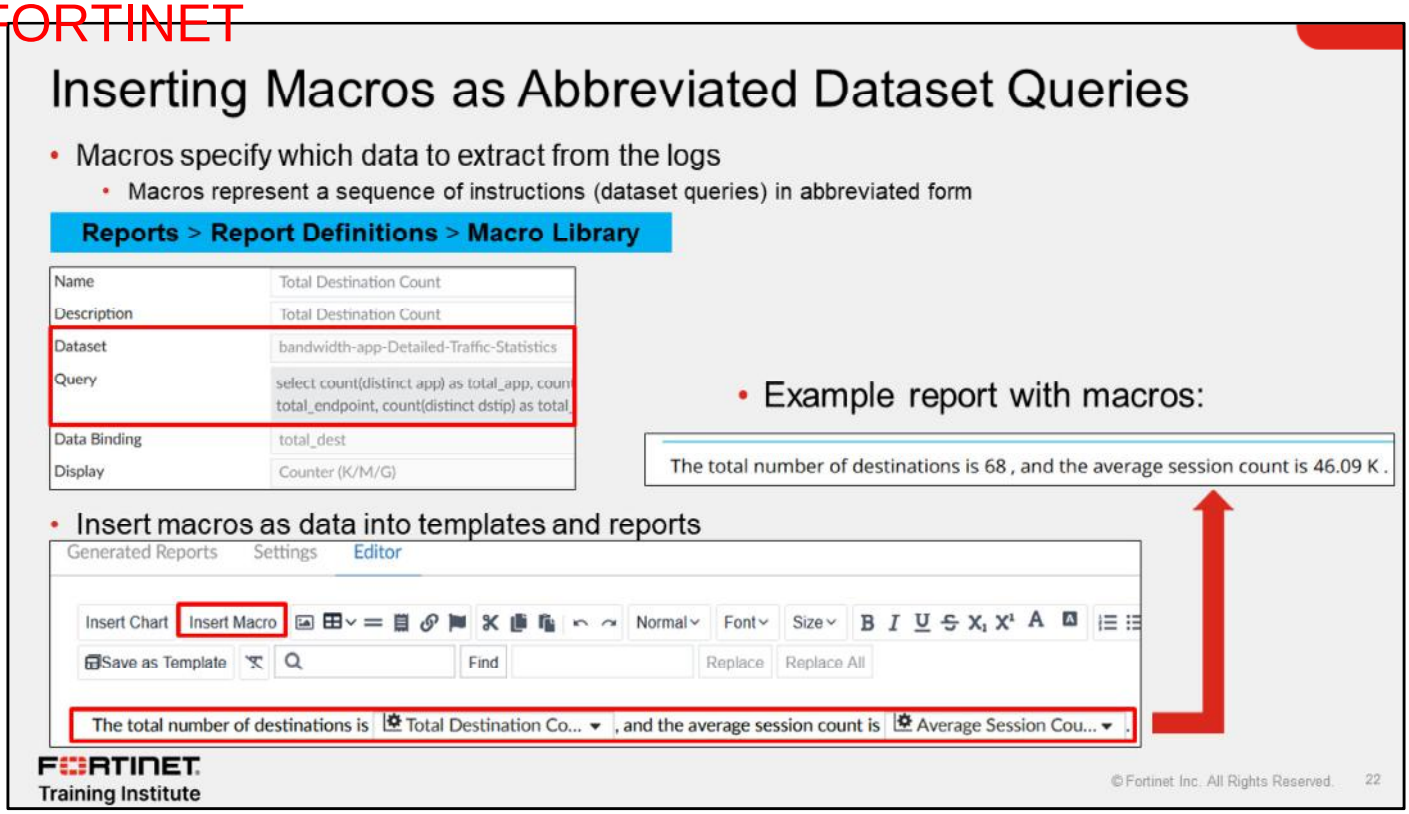
If you need to make major changes to existing templates or reports (if no report comes close to meeting your needs), you can create a new report or template from scratch.



Templates are 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, it depends on what you want to preserve and what you want to modify.

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



In 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.

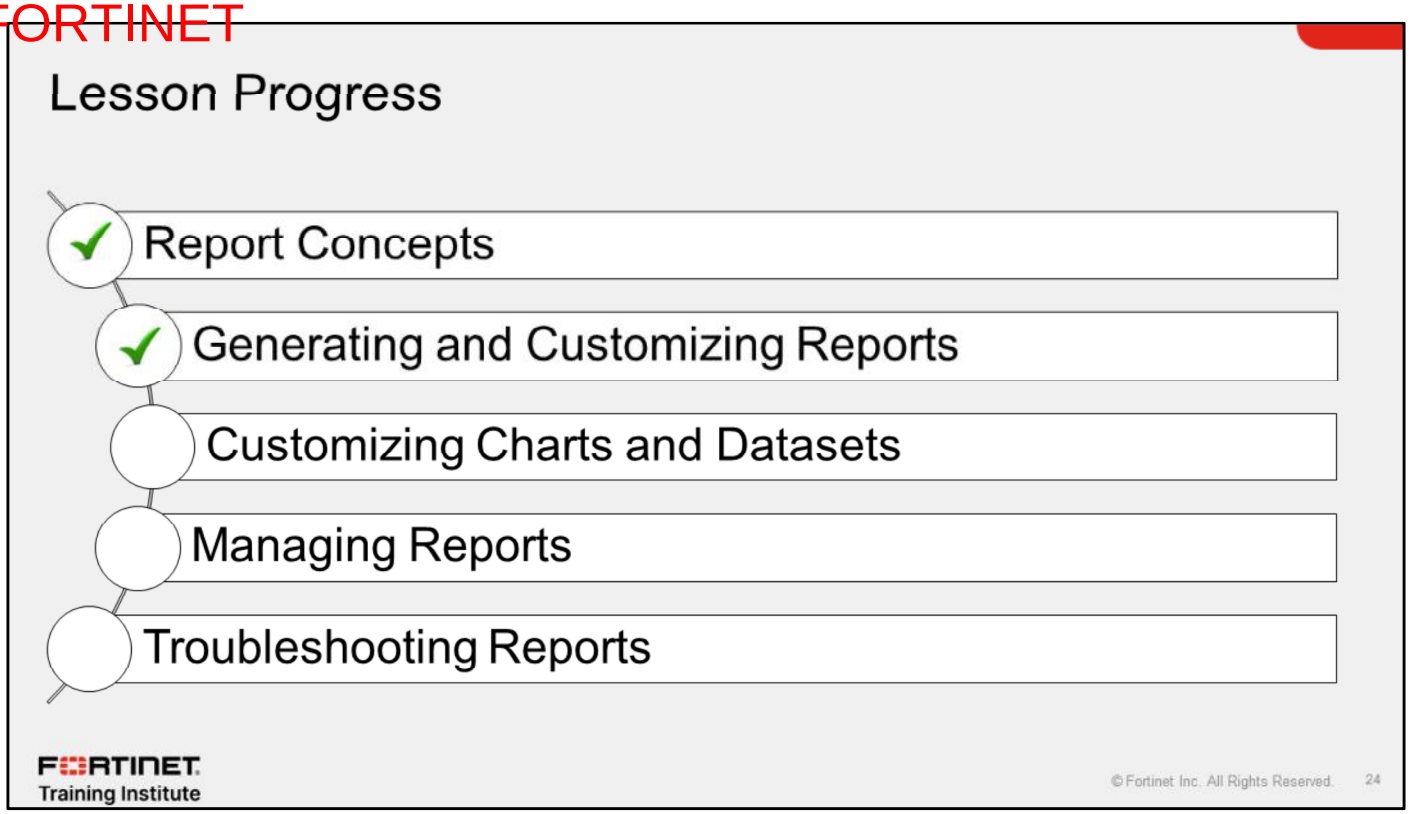
Note that macros are ADOM specific.

Knowledge Check

1. Templates do not contain _____.
   - ✓A. report schedules
   - B. charts
2. Which statement about macros is true?
   - ✓A. Macros are abbreviated dataset queries.
   - B. Macros cannot be customized.

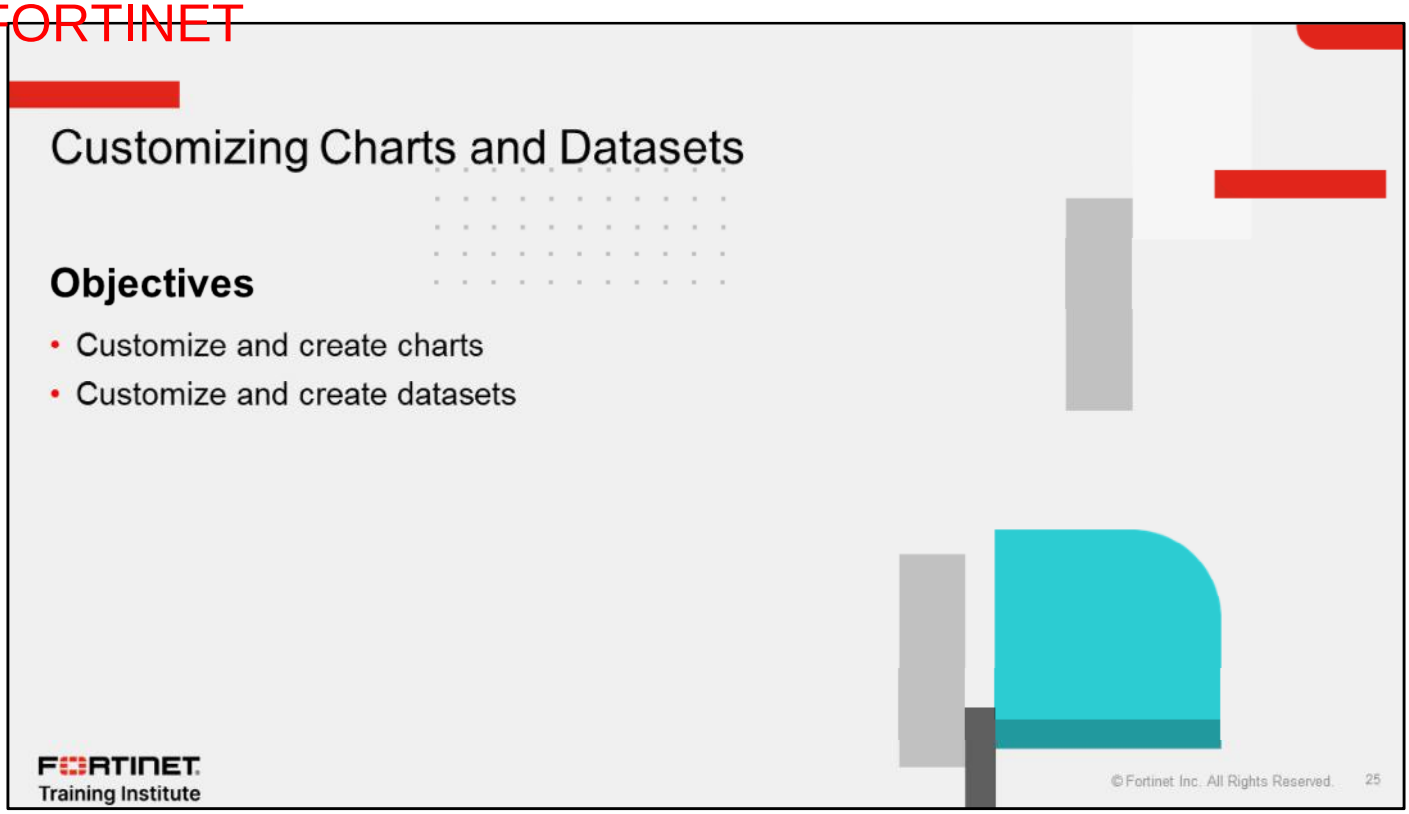
FORTINET Training Institute

 23



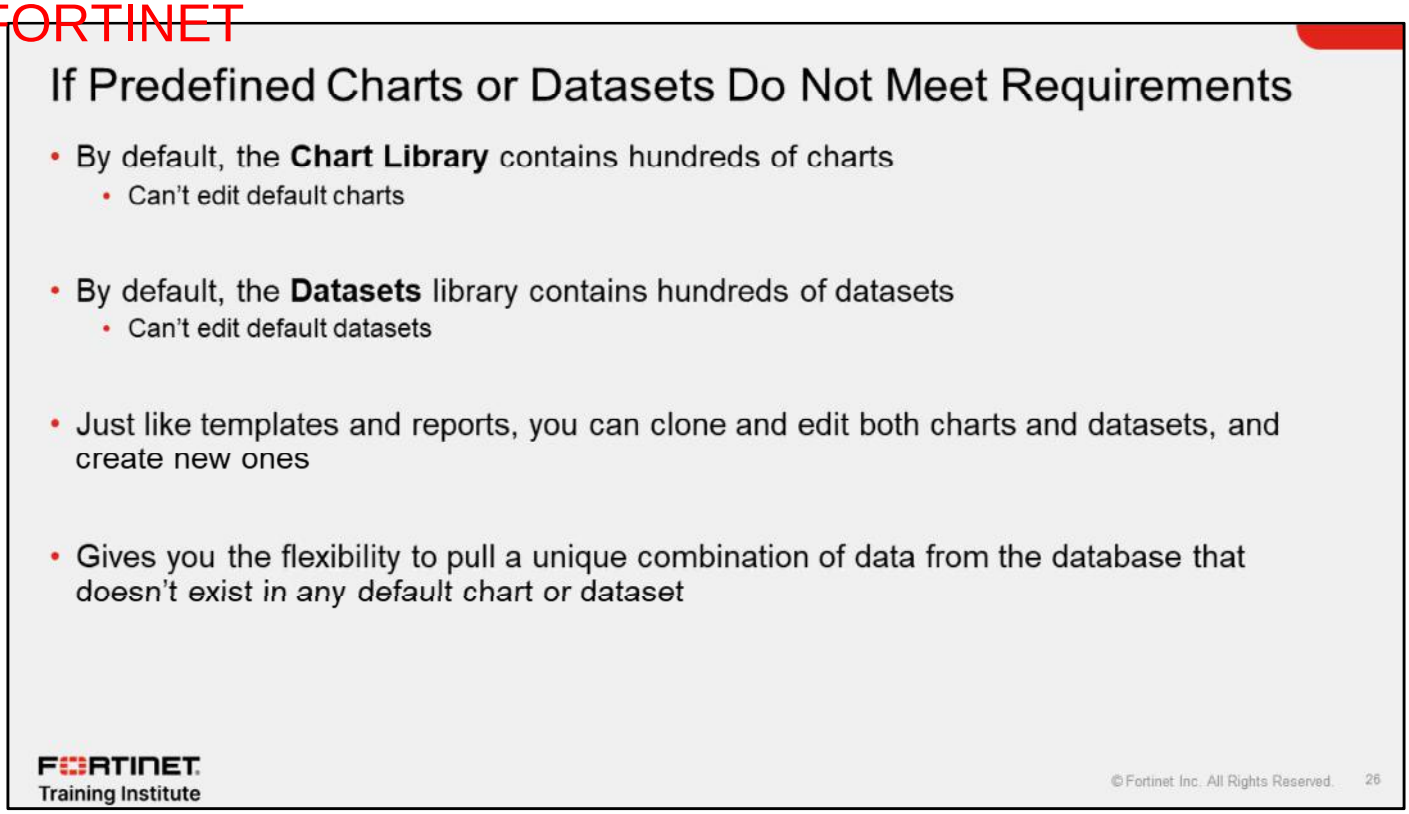
Good job! You now understand how to customize reports.

Now, you will learn how to customize charts and datasets.

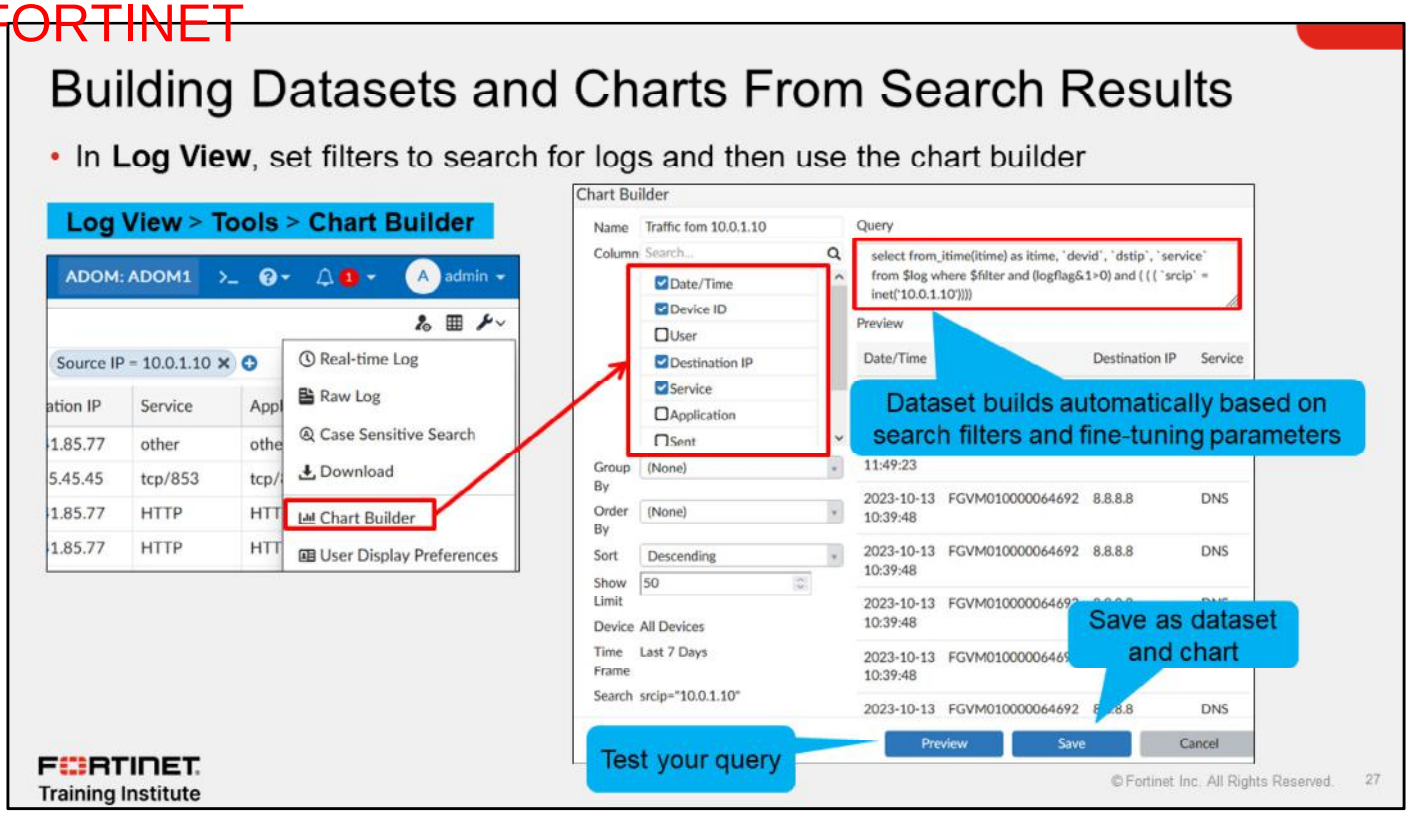


After completing this section, you should be able to achieve the objectives shown on this slide.

By demonstrating competence in chart and dataset customization, you will be able to extract unique combinations of data from the database specific to your requirements.

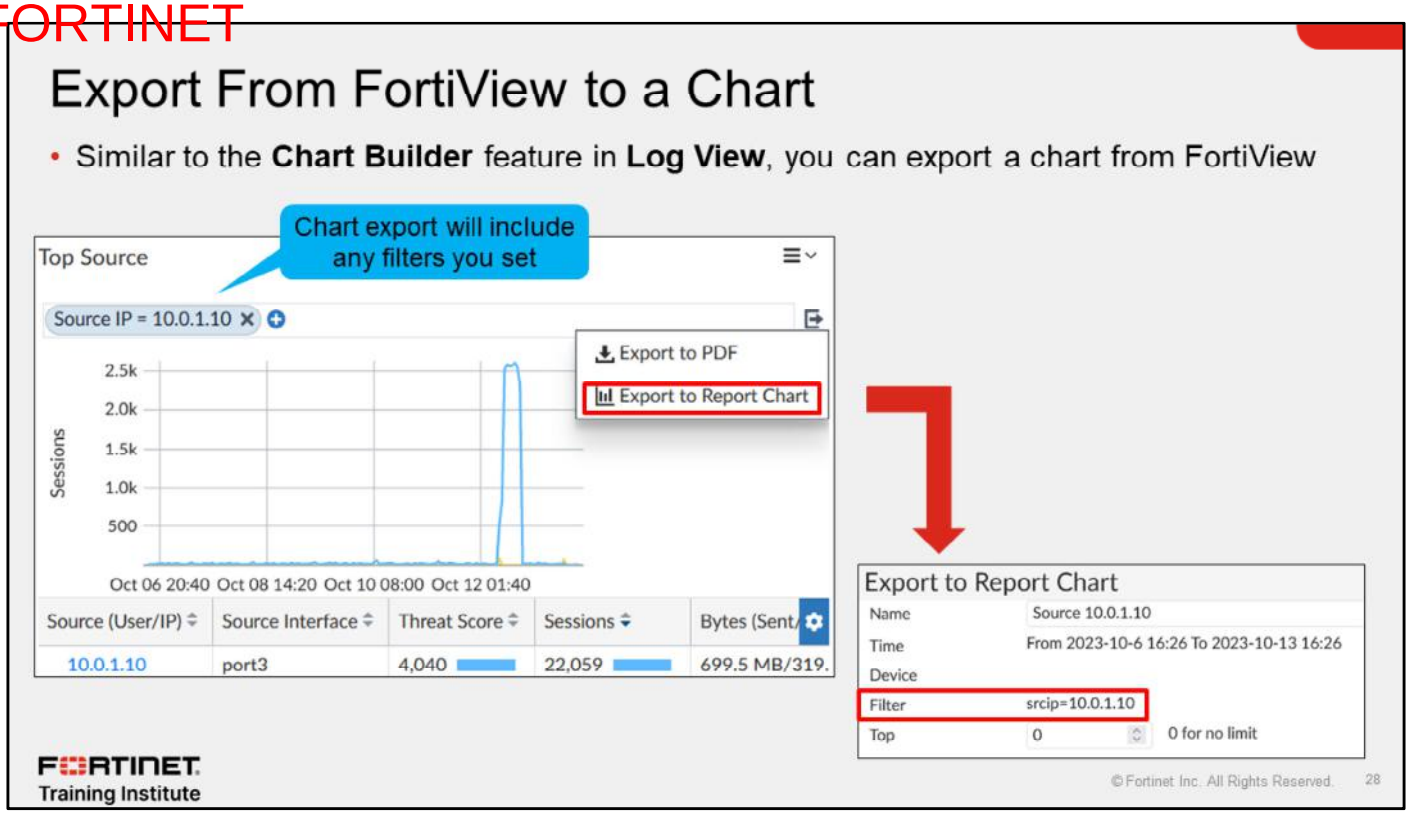


In some cases, simply adding or removing default charts from a report or template may not meet your requirements: You might need to pull a unique combination of data from the database when no predefined chart or dataset for that unique combination exists. In this case, you can either clone and edit charts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



A quick way to build a custom dataset and chart is to use the chart builder tool. This tool is located in **Log View**, and 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



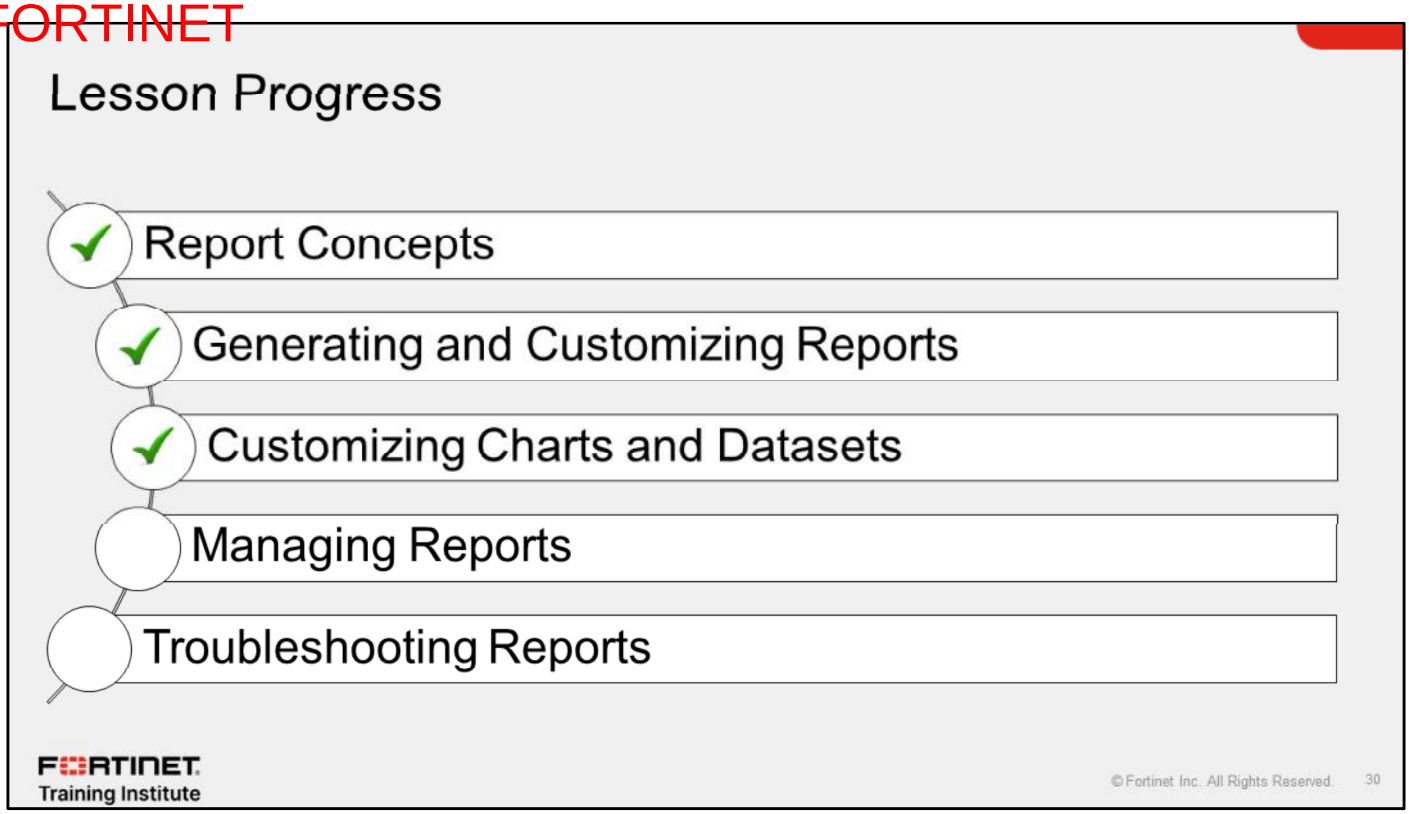
Similar to how you can use the **Chart Builder** feature in **Log View**, you can export a chart from FortiView. The chart export includes any filters you set on FortiView.

Knowledge Check

1. Which FortiAnalyzer feature allows you to automatically build a dataset and chart based on a filtered search result?
   - ✓ A. Export to Report Chart (FortiView)
   - B. Dataset Library

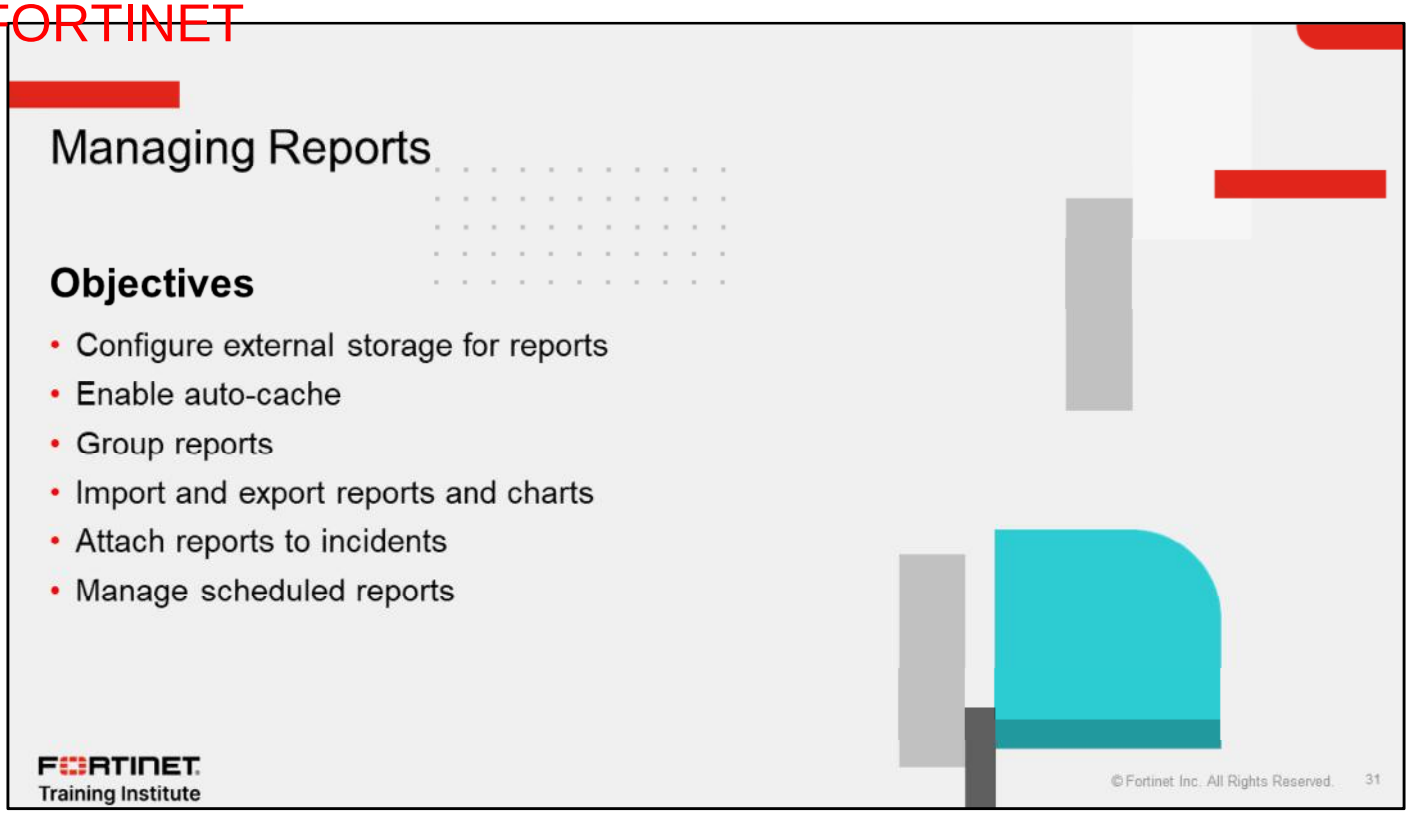
FORTINET Training Institute

 29



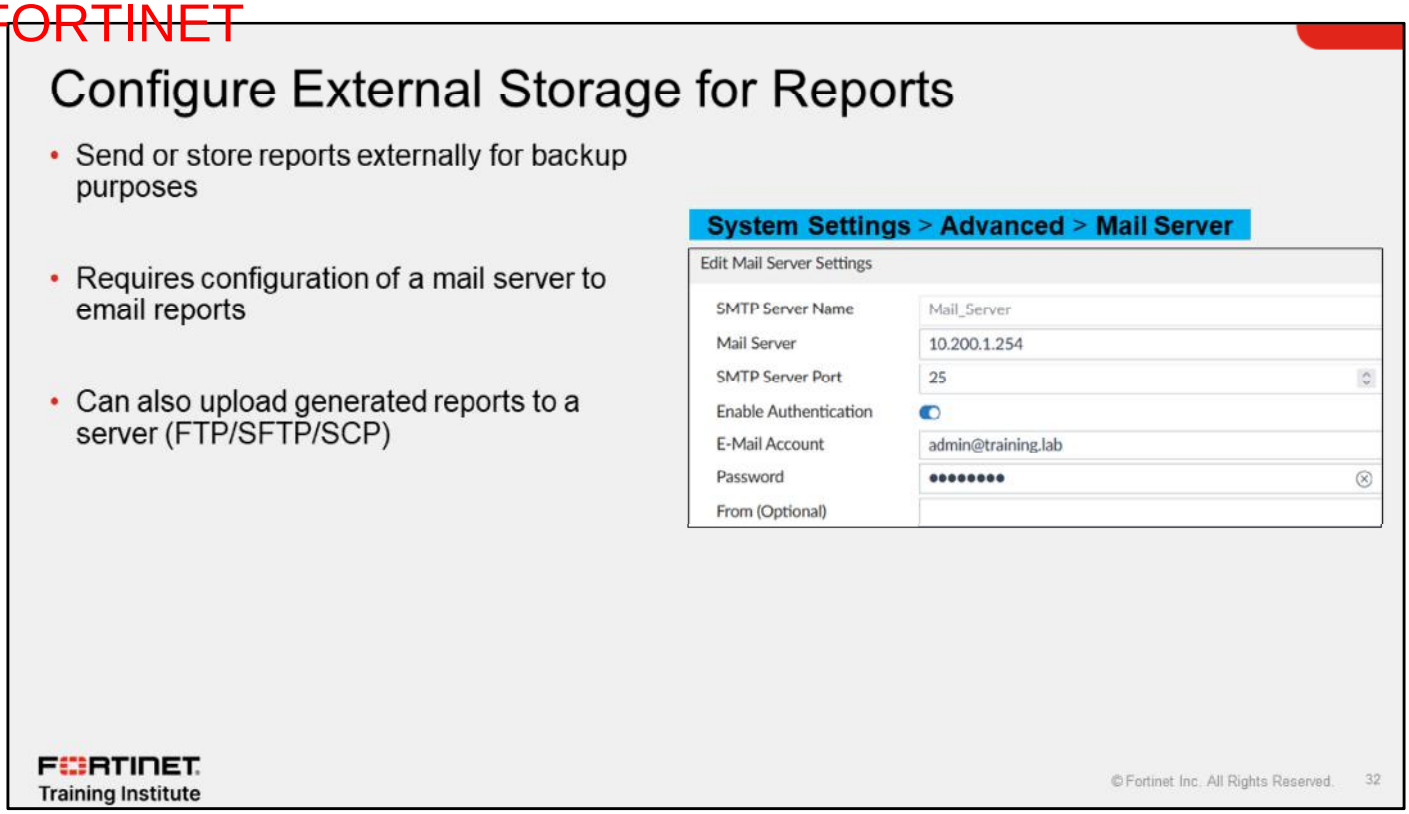
Good job! You now understand how to customize charts and datasets.

Now, you will learn how to manage reports.



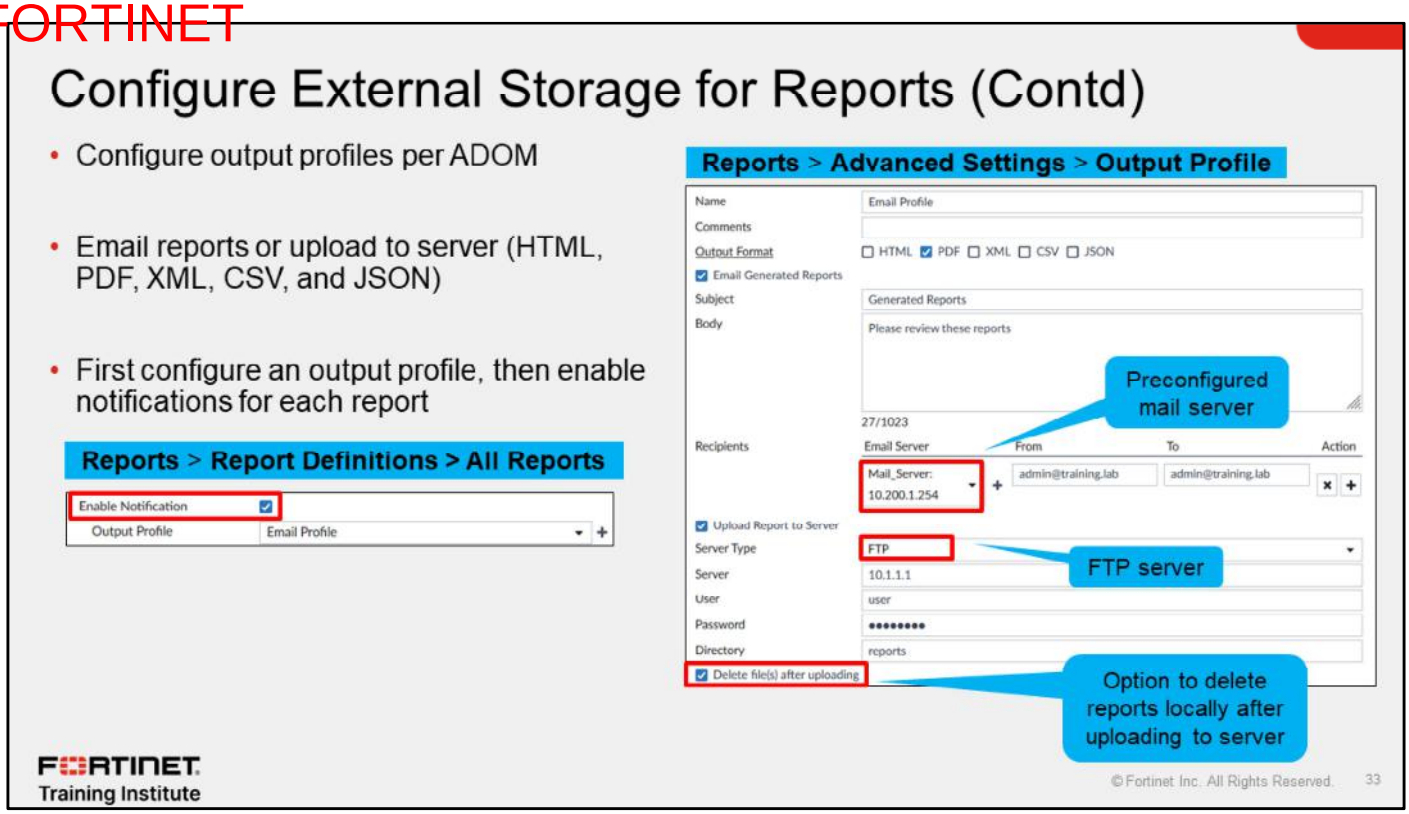
After completing this section, you should be able to achieve the objectives shown on this slide.

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.

In order to use any of these external storage methods, you must first set up the back end. 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.

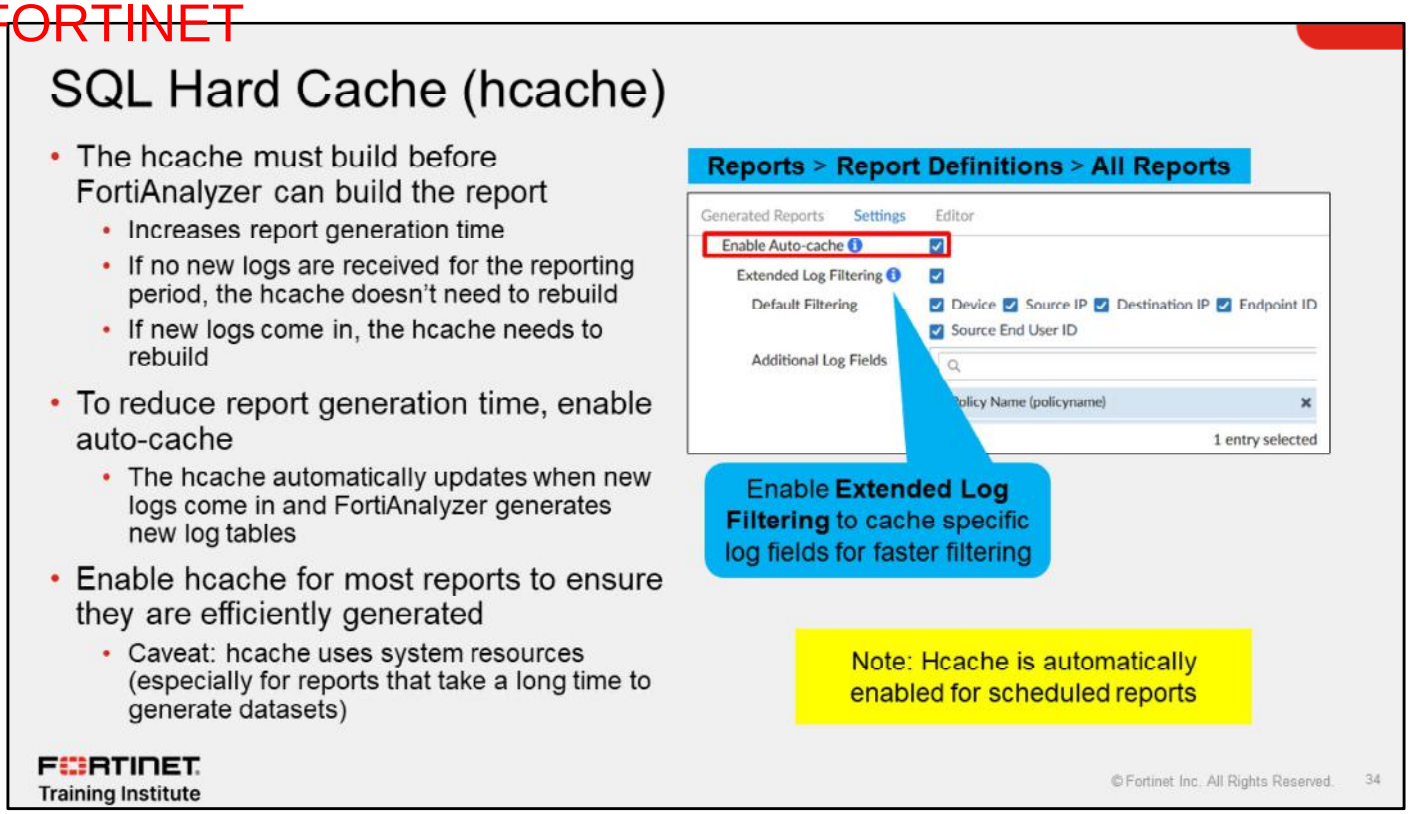


To send reports to an external location, you must enable notifications and select an appropriate output profile.

An output profile specifies the following:

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

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

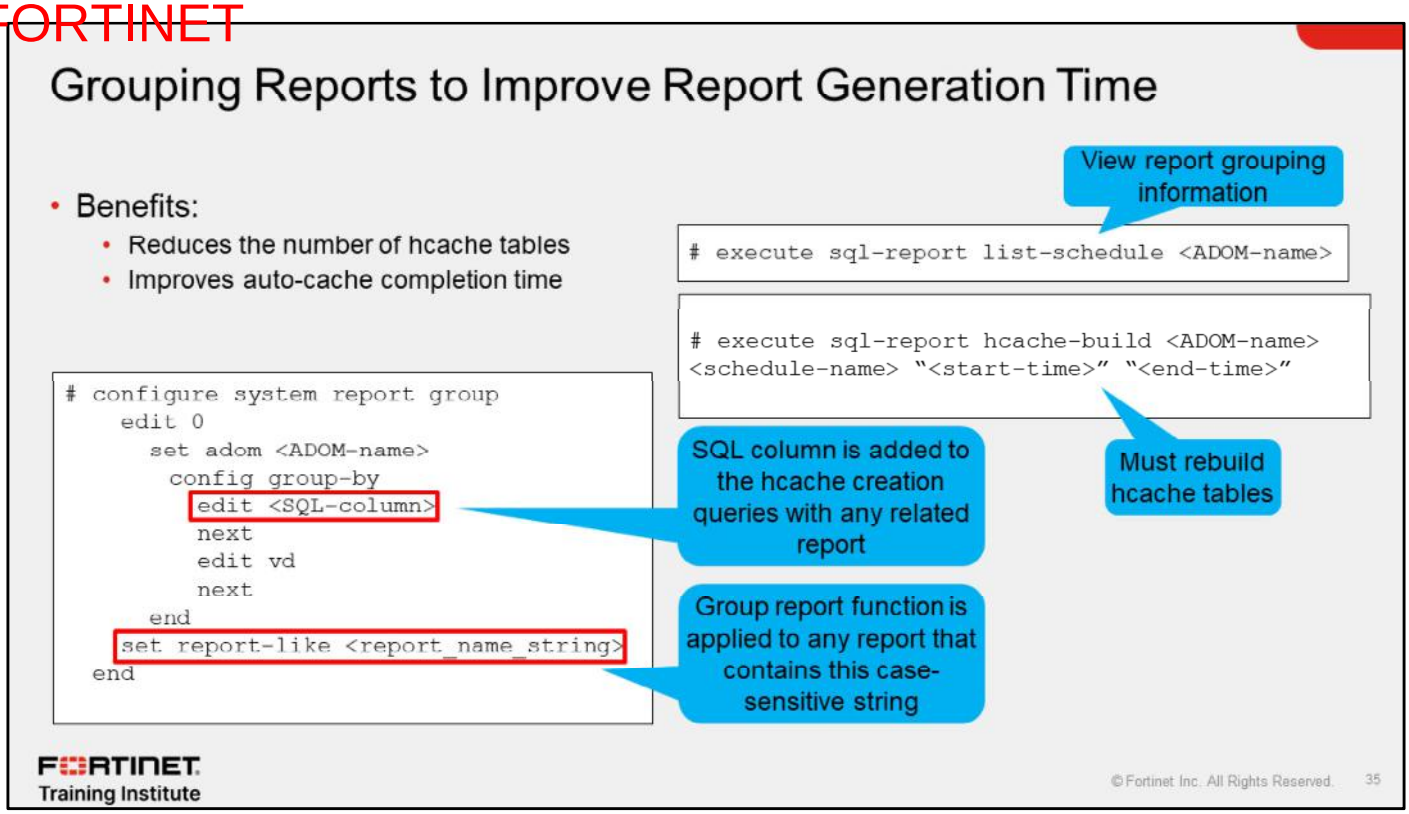


When a report generates, the system builds the charts from precompiled SQL hard-cache data, known as the hcache. If the hcache is not built when you run the report, the system must create the hcache first and then build the report. This adds time to the report generation. However, if FortiAnalyzer does 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. In this case, the hcache is automatically updated when new logs come in and new log tables are generated.

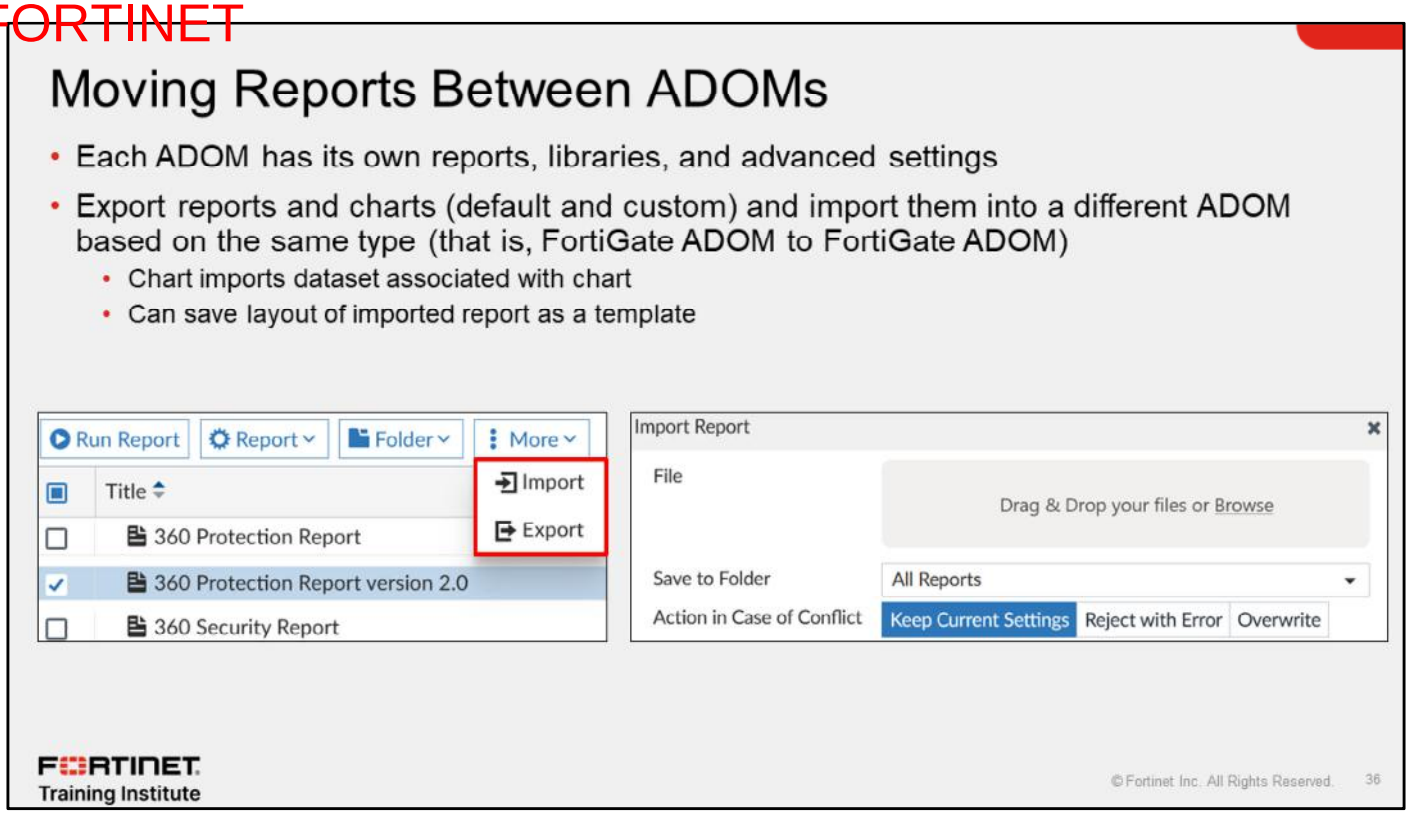
Note that hcache is automatically enabled for scheduled reports. If you are not scheduling a report, you may want to consider enabling hcache. This ensures reports are efficiently generated. However, be aware that this process uses system resources, especially for reports that require a long time to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

Additionally, you can opt for enabling **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 specific reports.

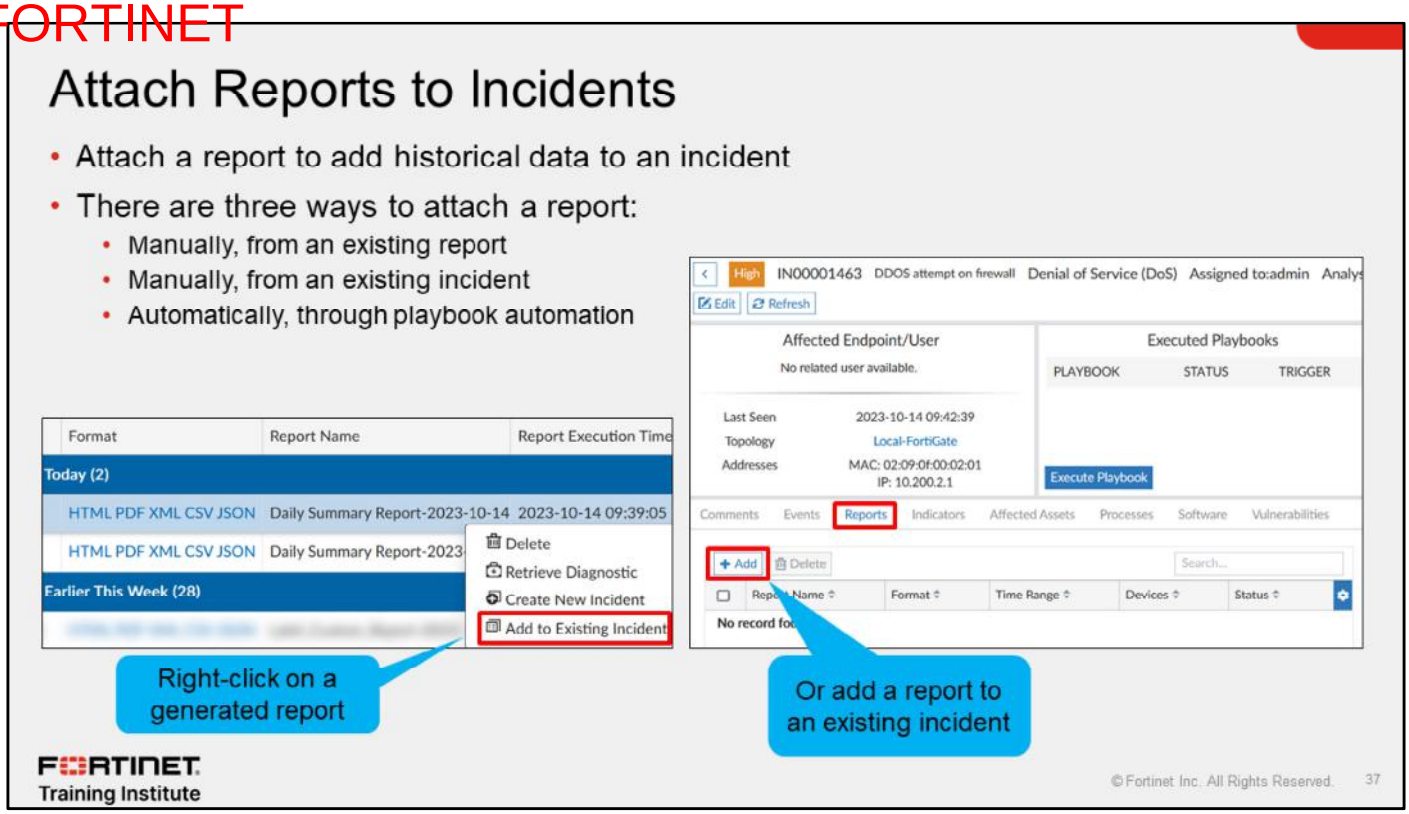


Remember, each ADOM has its own reports, libraries, and advanced settings. You can, however, import and export reports and charts (whether default or custom) into a different ADOM within the same FortiAnalyzer device or a different FortiAnalyzer device. Both ADOMs must be of the same type.

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.

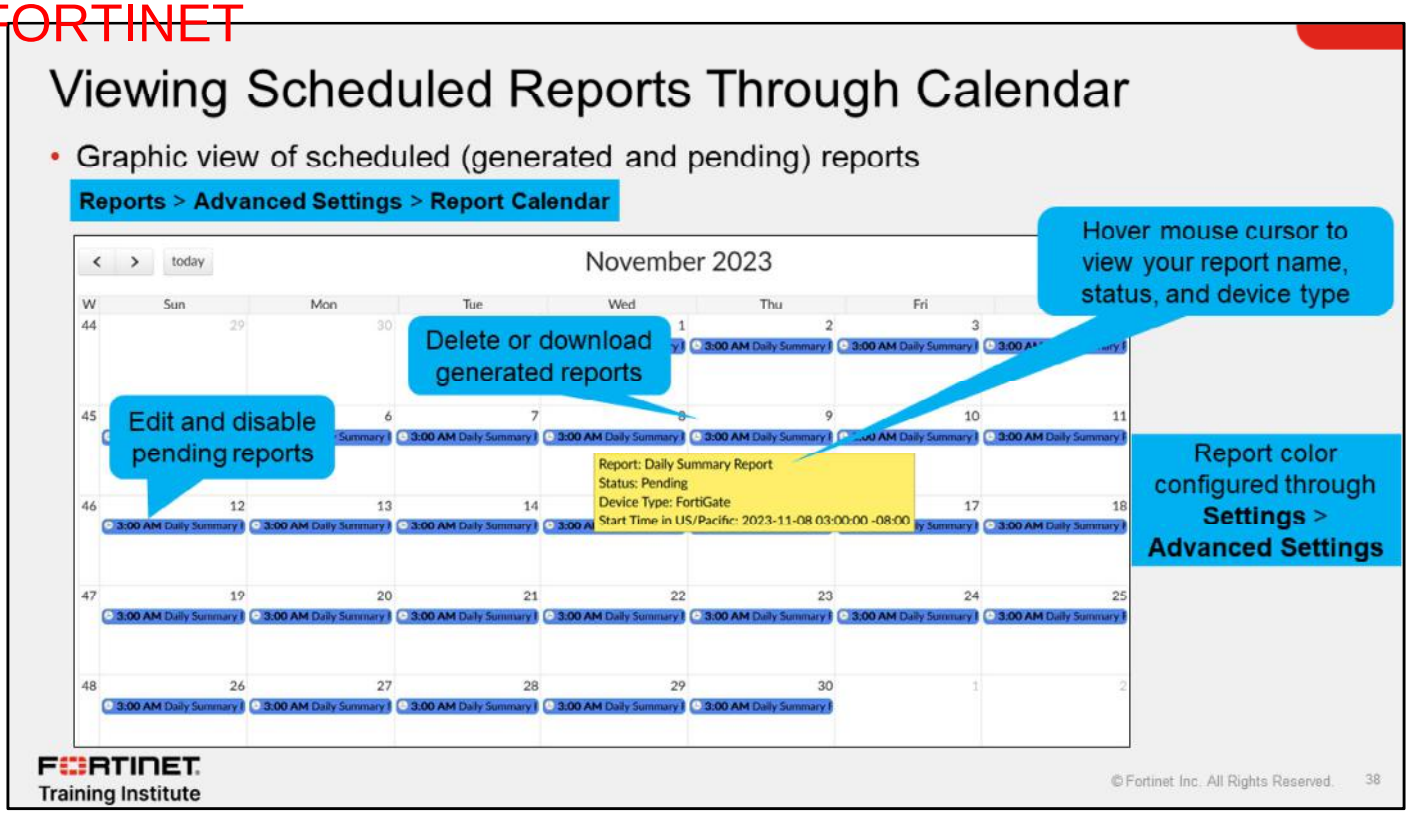
The **Chart Library** includes the export and import functions in the toolbar.



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 cursor 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.

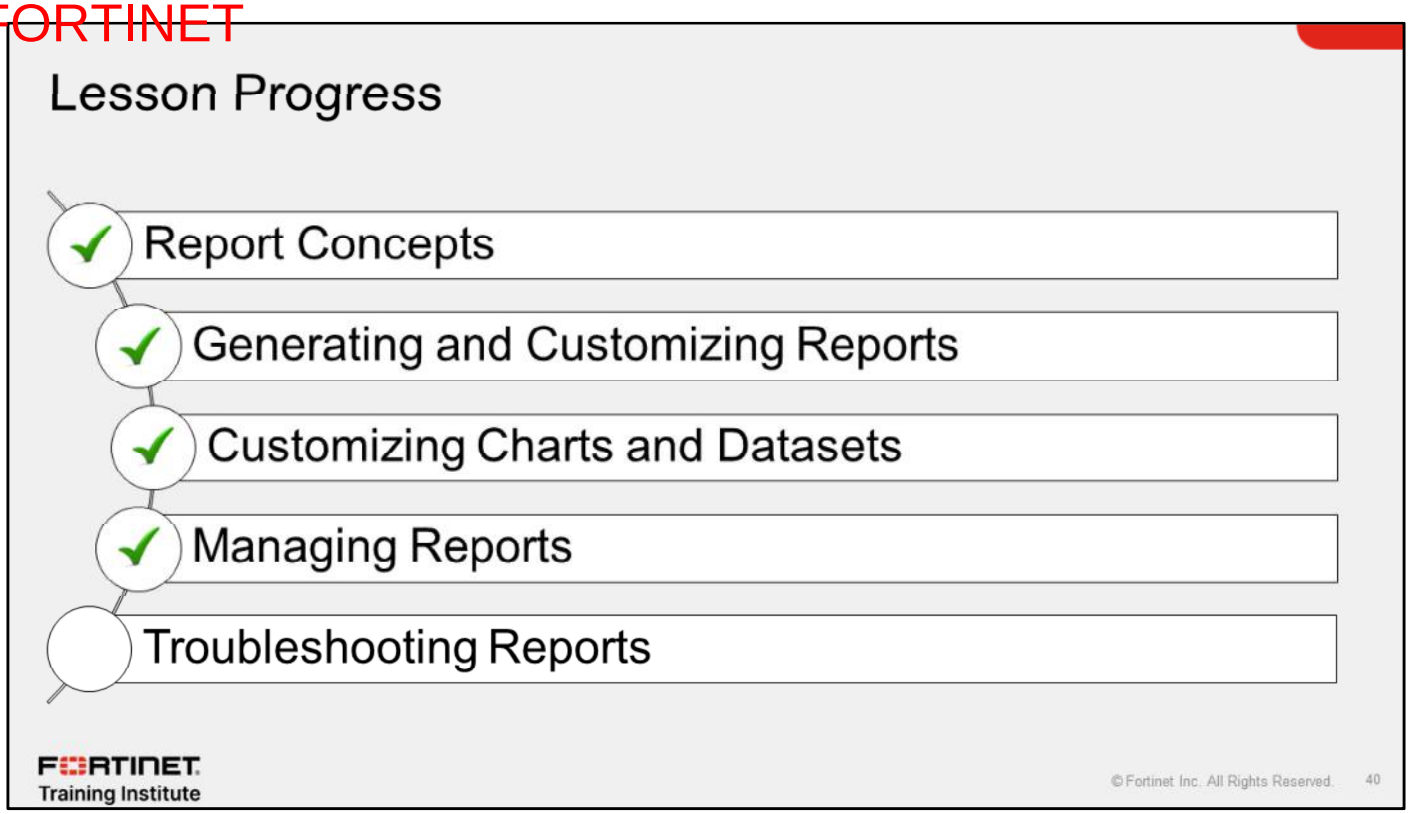
Knowledge Check

1. What is the purpose of the auto-cache setting on reports?
   - ✓A. To automatically update the hcache when new logs arrive
   - B. To reduce the log insert lag rate

2. Where are reports scheduled?
   - A. In the **Report Calendar**
   - ✓B. In the scheduling configuration of a report

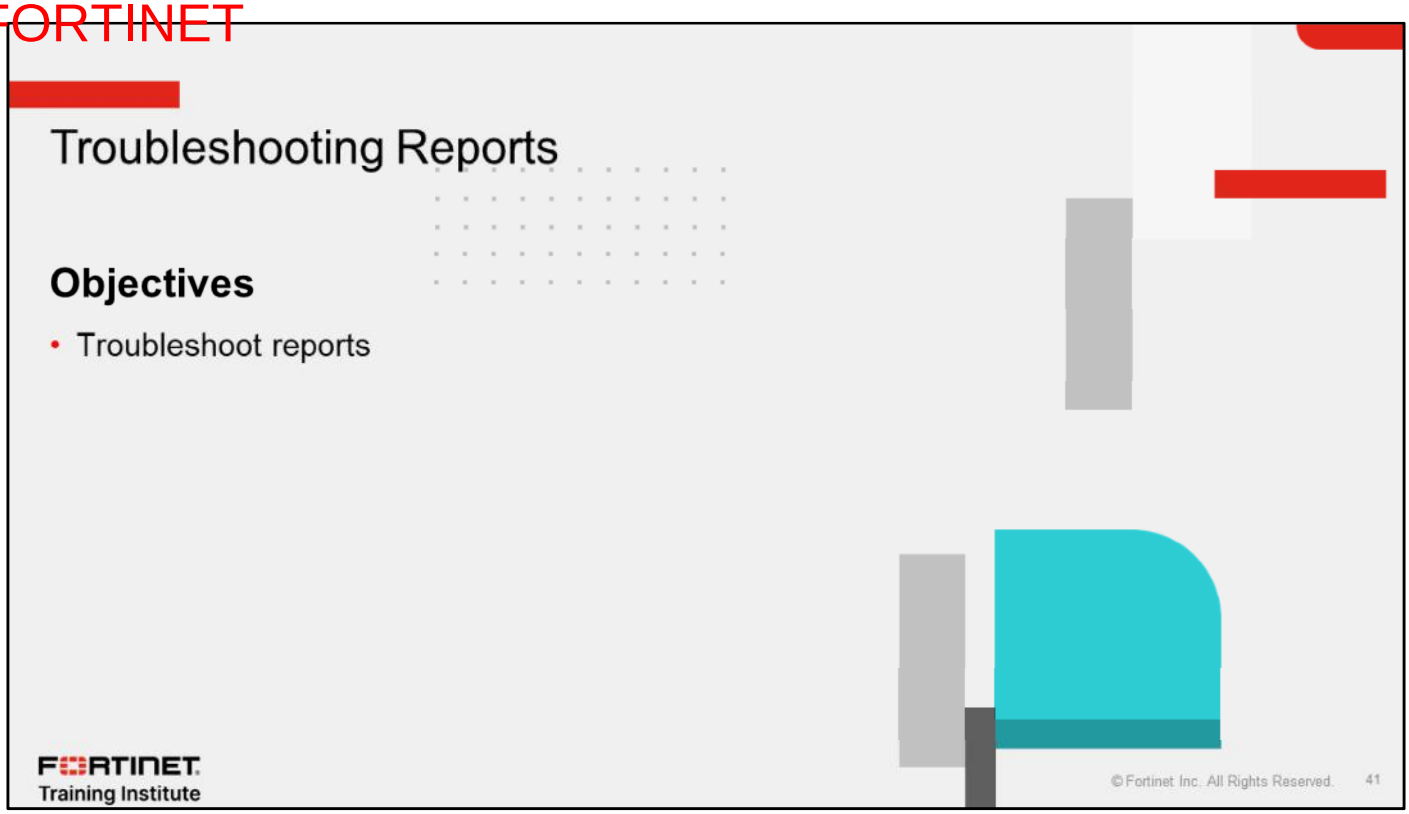
FORTINET Training Institute

 39



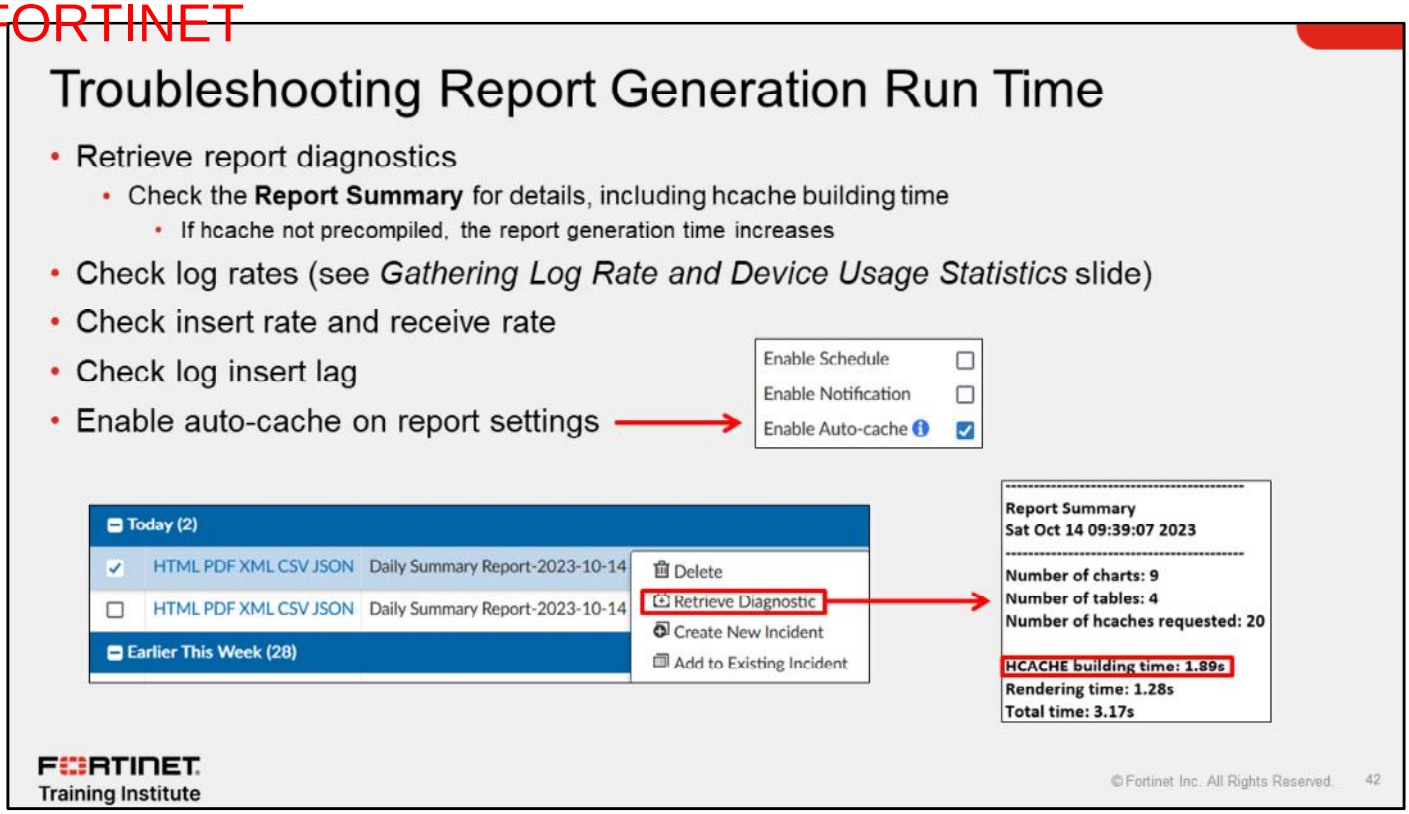
Good job! You now understand how to manage reports.

Now, you will learn about report troubleshooting.



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

By demonstrating competence in report troubleshooting, you will be able to avoid, identify, and solve common reporting issues.



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 the 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.

Report Troubleshooting CLI Commands

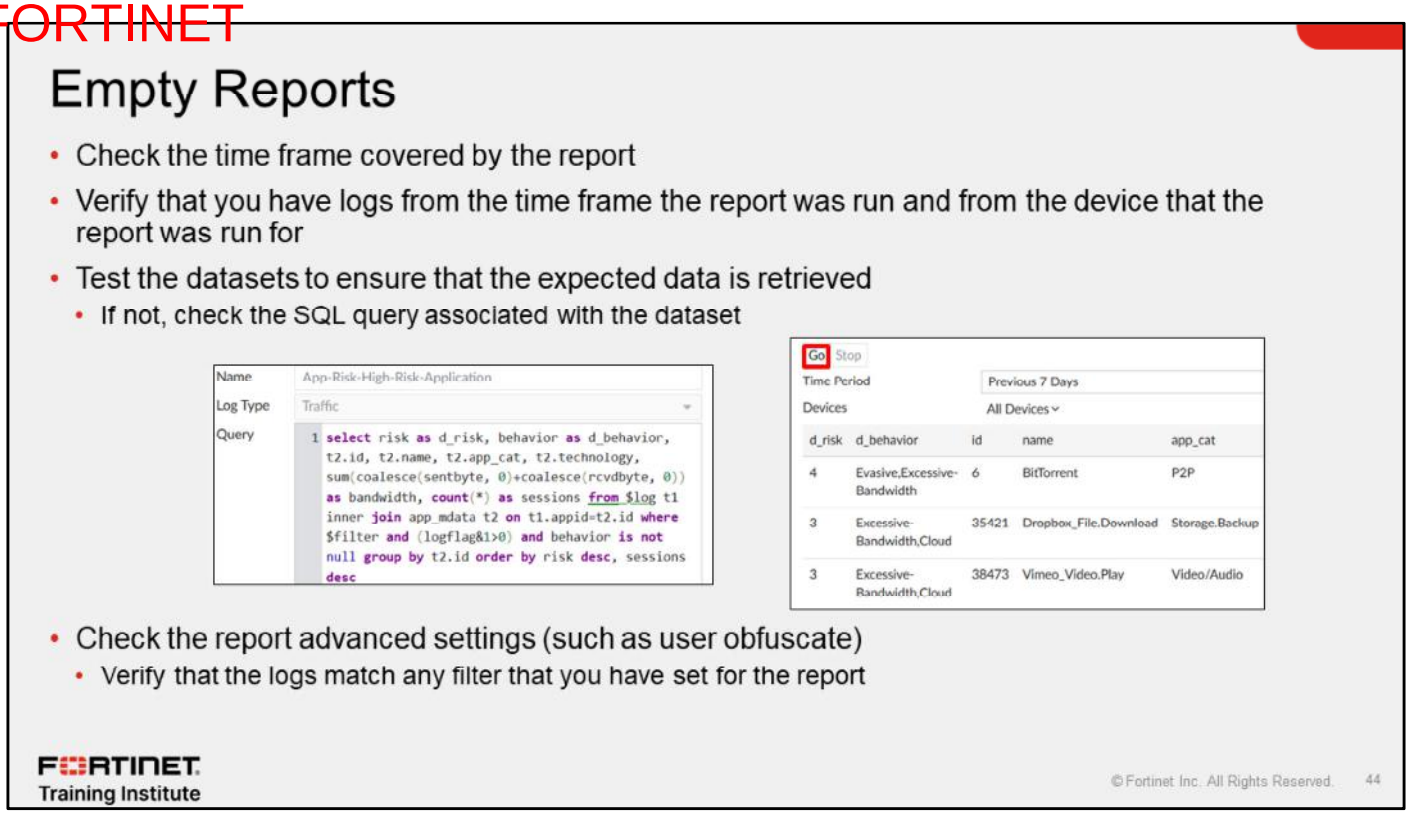
- Use the following FortiAnalyzer CLI commands to troubleshoot report generation time issues

What to Investigate	CLI Command to Use
What is the SQL insertion status? What are the SQL query connections and hcache status?	# diagnose sql status sqlplugind # diagnose sql status sqlreportd
Is the hcache creation able to catch up? What are the log file-related activities (file rolled/deleted/uploaded)	# diagnose test application logfiled 2
What are the current SQL processes running (any log queries)?	# diagnose sql process list
What is the configuration status of all configured reports?	# execute sql-report list-schedule <ADOM>
What is the state of the hcache?	# diagnose test application sqlrptcached <level>
What is the hcache size on the file system?	# diagnose sql show hcache-size

FORTINET Training Institute

 43

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



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

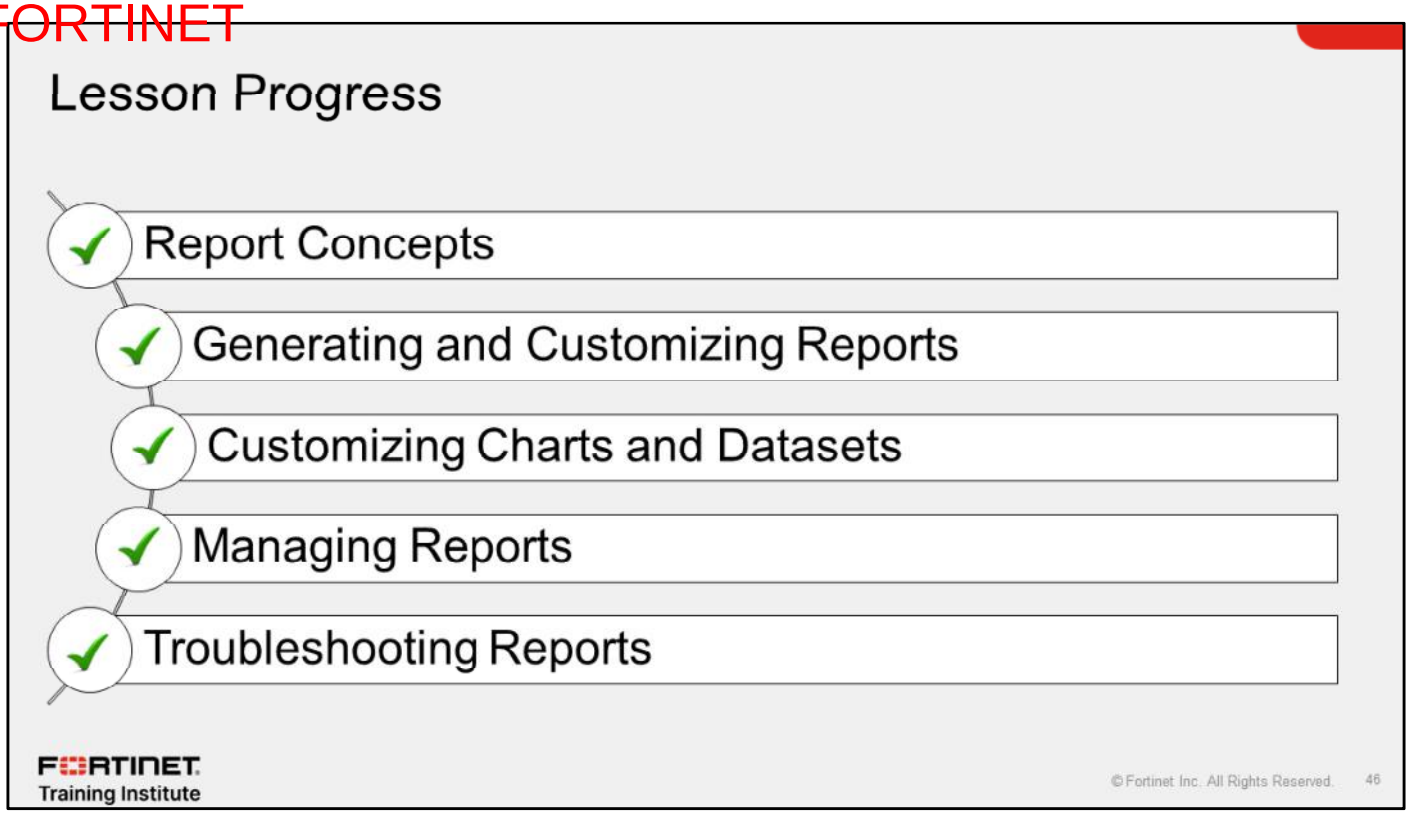
- Check the time frame that is covered by the report. This time frame is listed within the report.
- Verify that you have logs from the time frame the report was run and from the device that the report was run for. A common cause of empty reports is logs being overwritten too quickly. In this case, the 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, then troubleshoot the SQL query, because it is probably the dataset that contains the error.
- Check your report advanced settings. 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

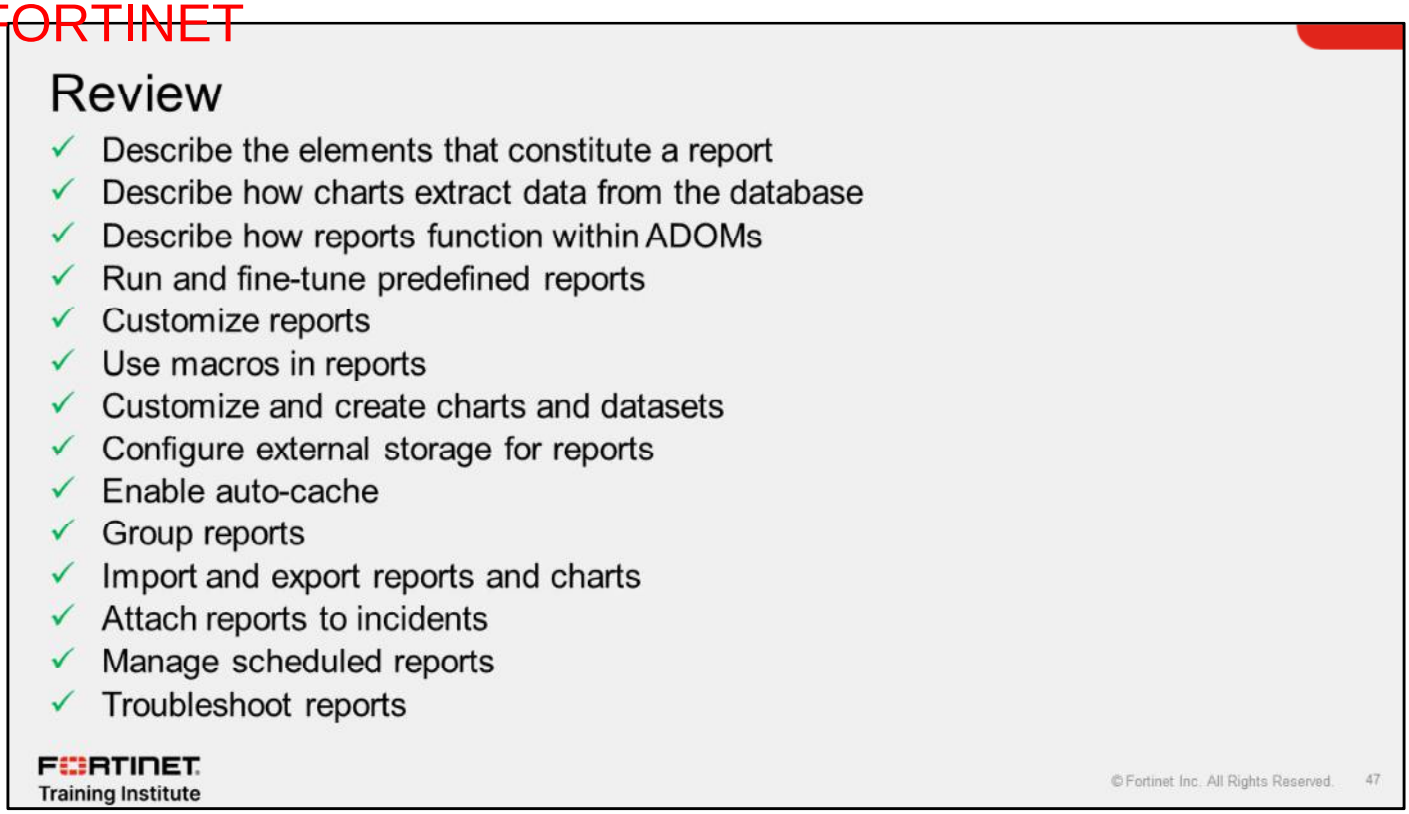
FORTINET Training Institute

 45



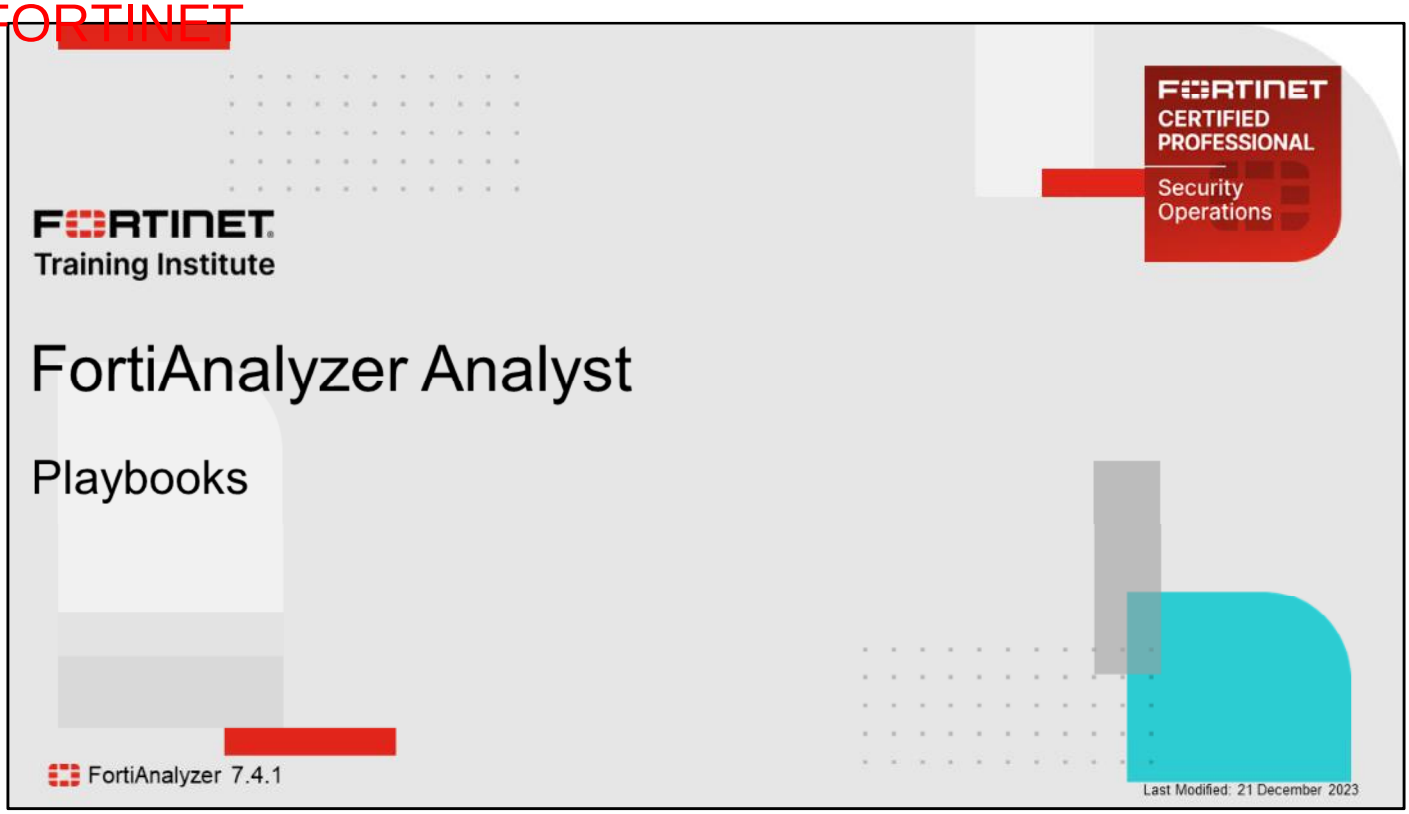
Congratulations! You have completed this lesson.

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

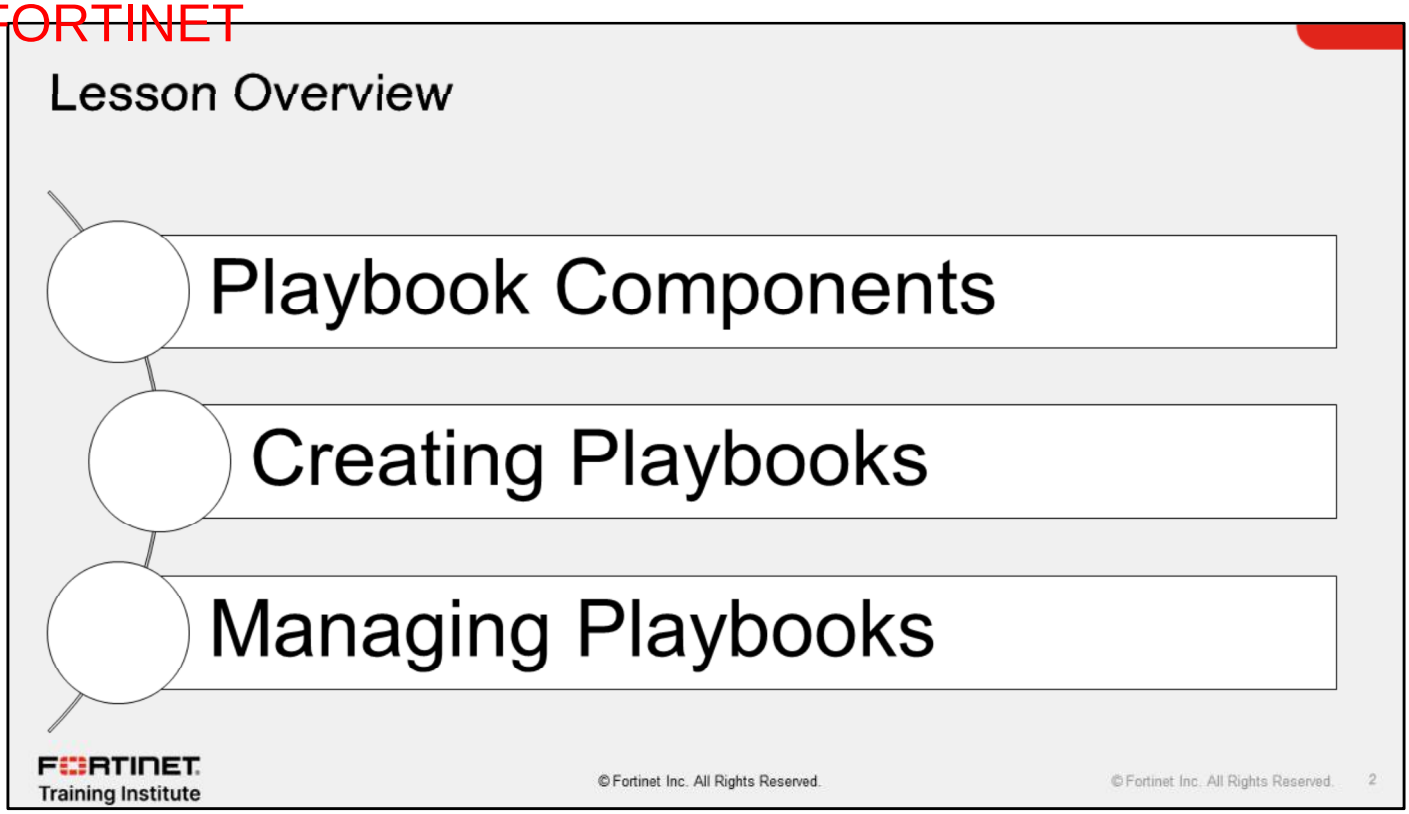


This slide shows the objectives that you covered in this lesson.

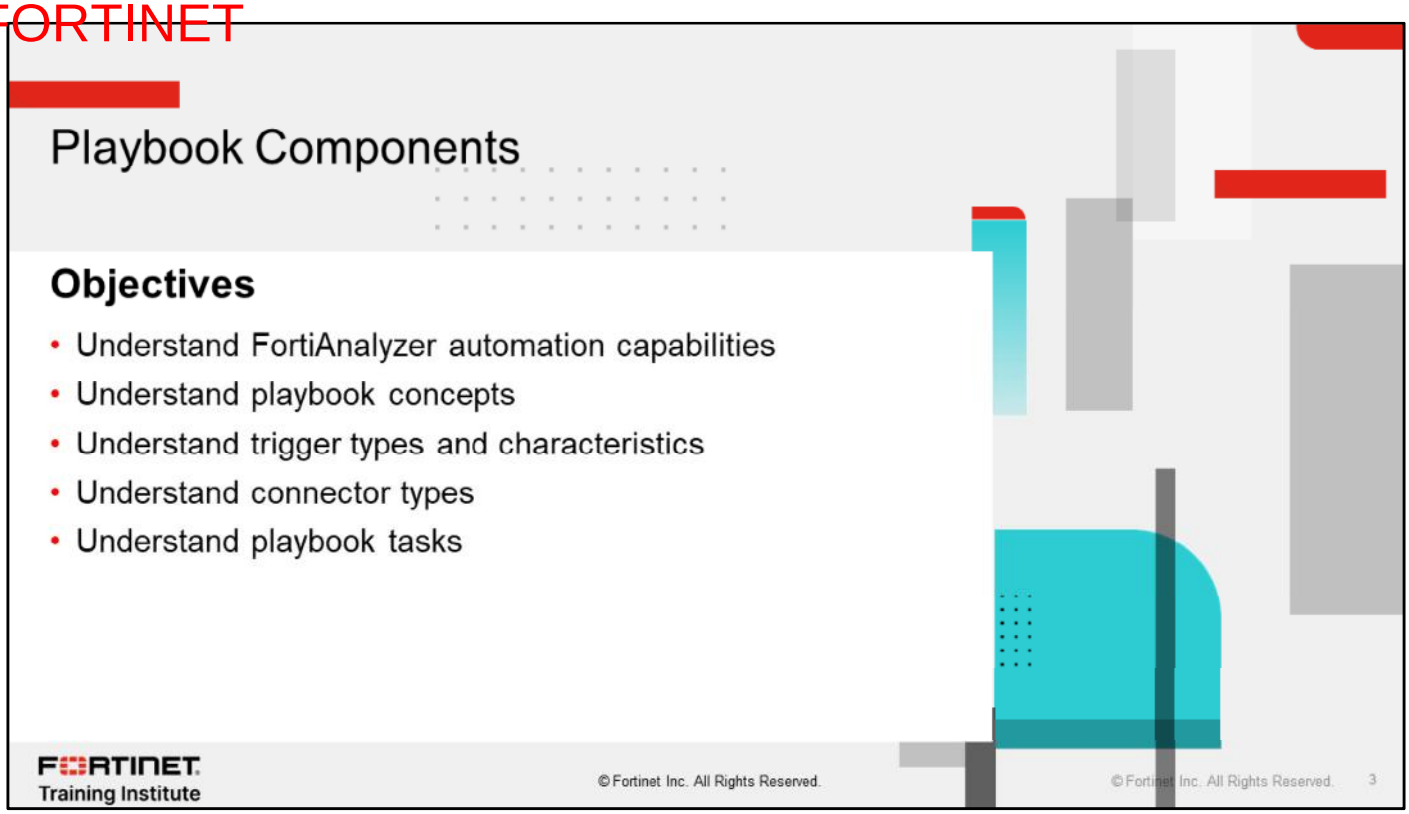
By mastering the objectives covered in this lesson, you learned how to understand how data is formatted, stored, and organized in the database, and how to use the FortiAnalyzer reporting feature to view and extract useful information from logs.



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

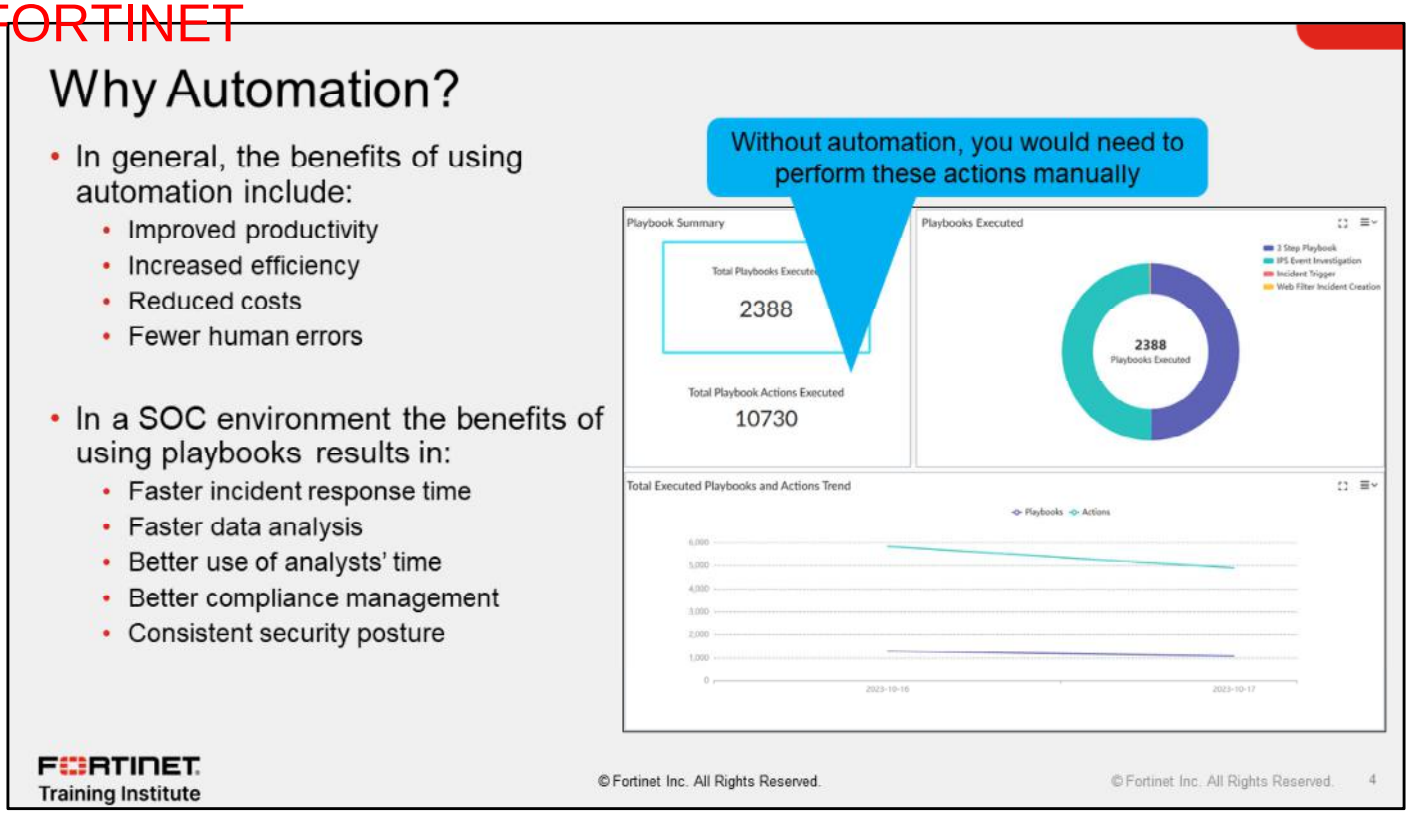


In this lesson, you will learn about the topics shown on this slide.



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.

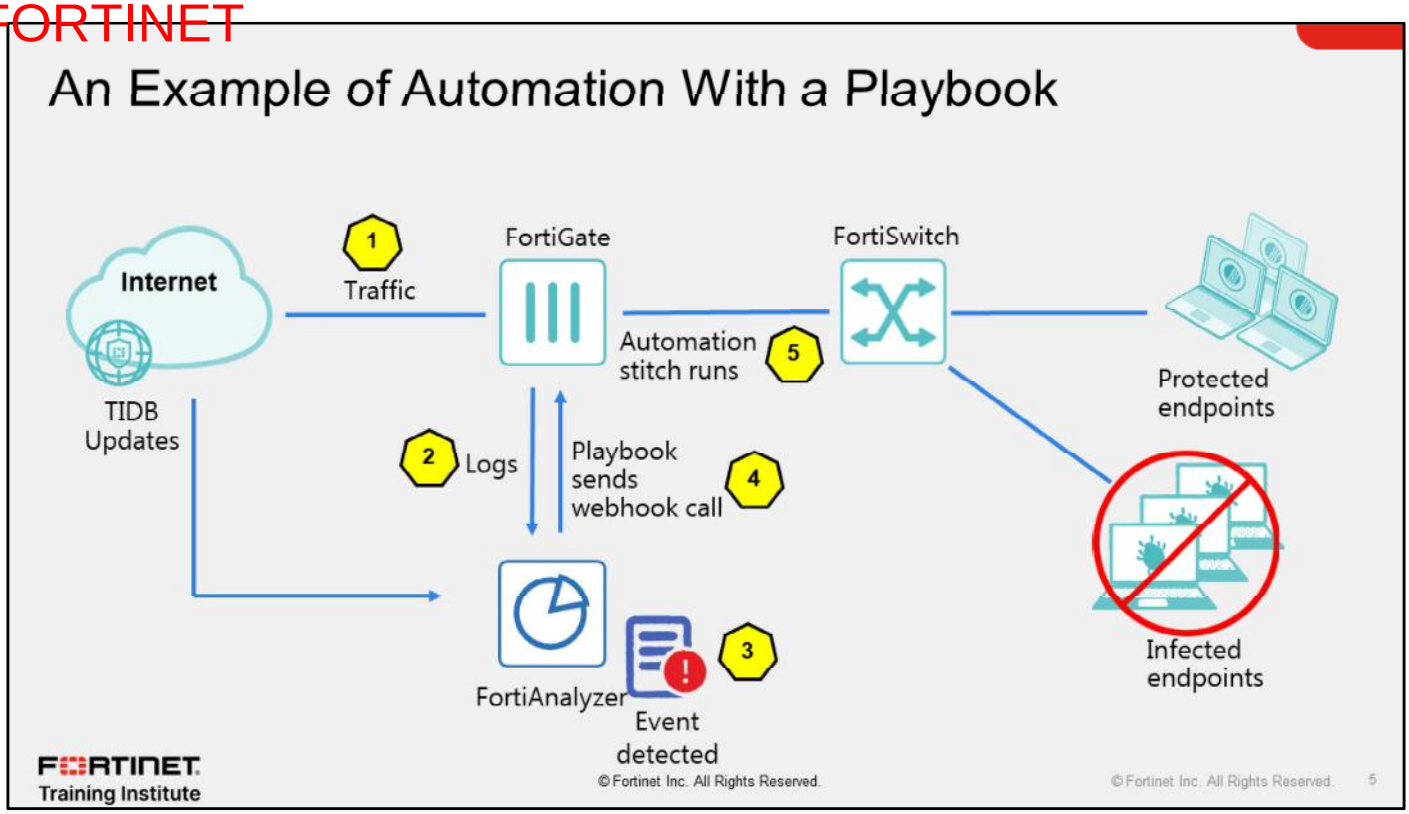
In a SOC environment, these benefits provide, among other results, faster response time, faster data analysis, better use of analysts time, better compliance management, and a more consistent security posture.

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

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

For example, you can create playbooks that automatically generate a report, or instruct a FortiGate device 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.

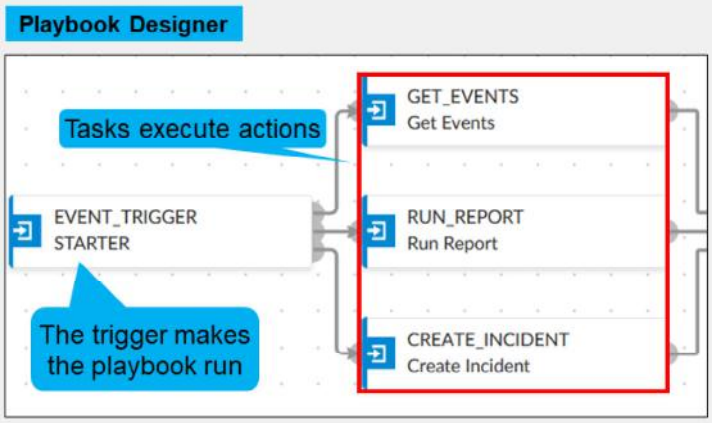


This slide shows an example of a playbook being used to automate tasks.

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 in 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
  - 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 work the flow

FORTINET Training Institute

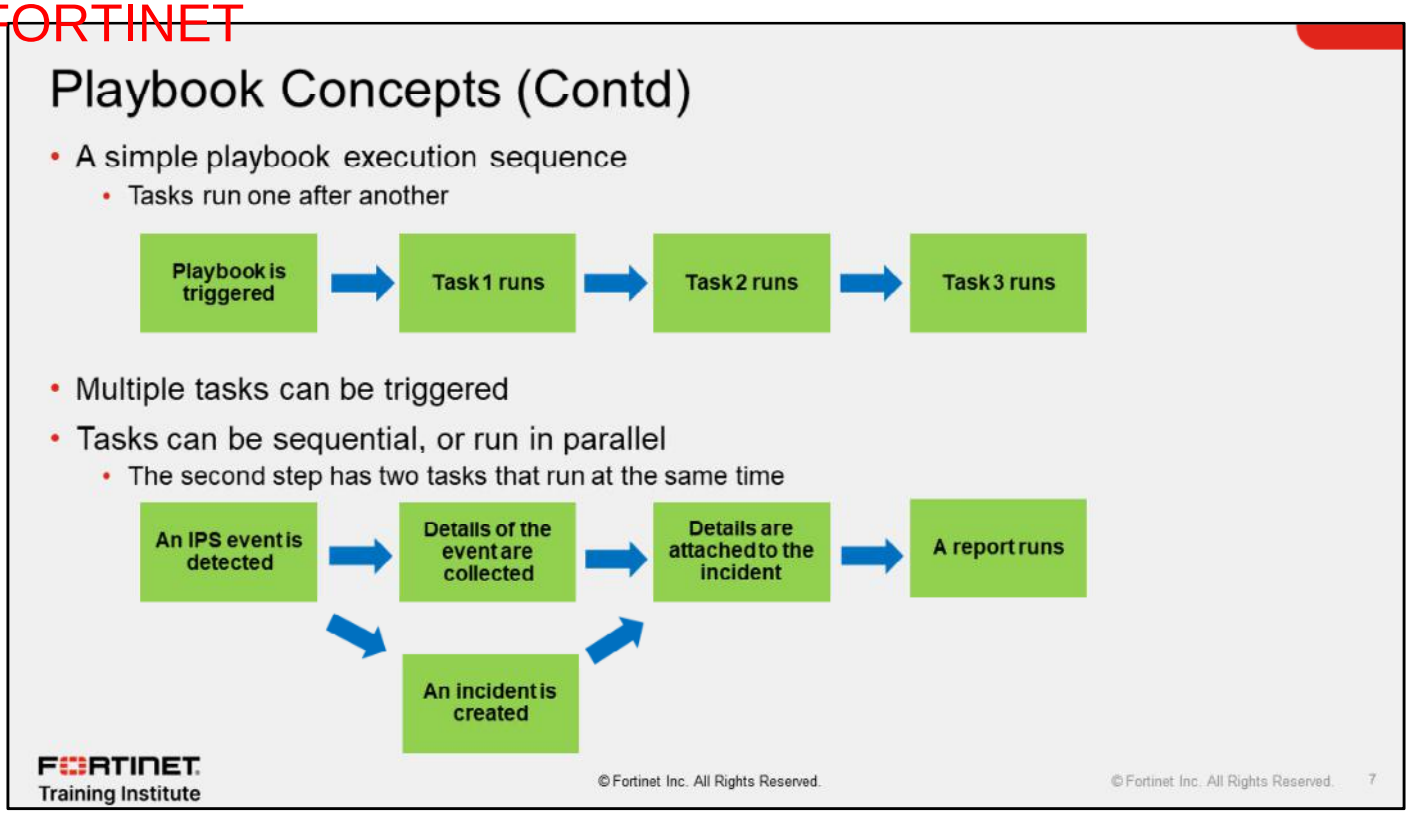
© Fortinet Inc. All Rights Reserved. 6

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.

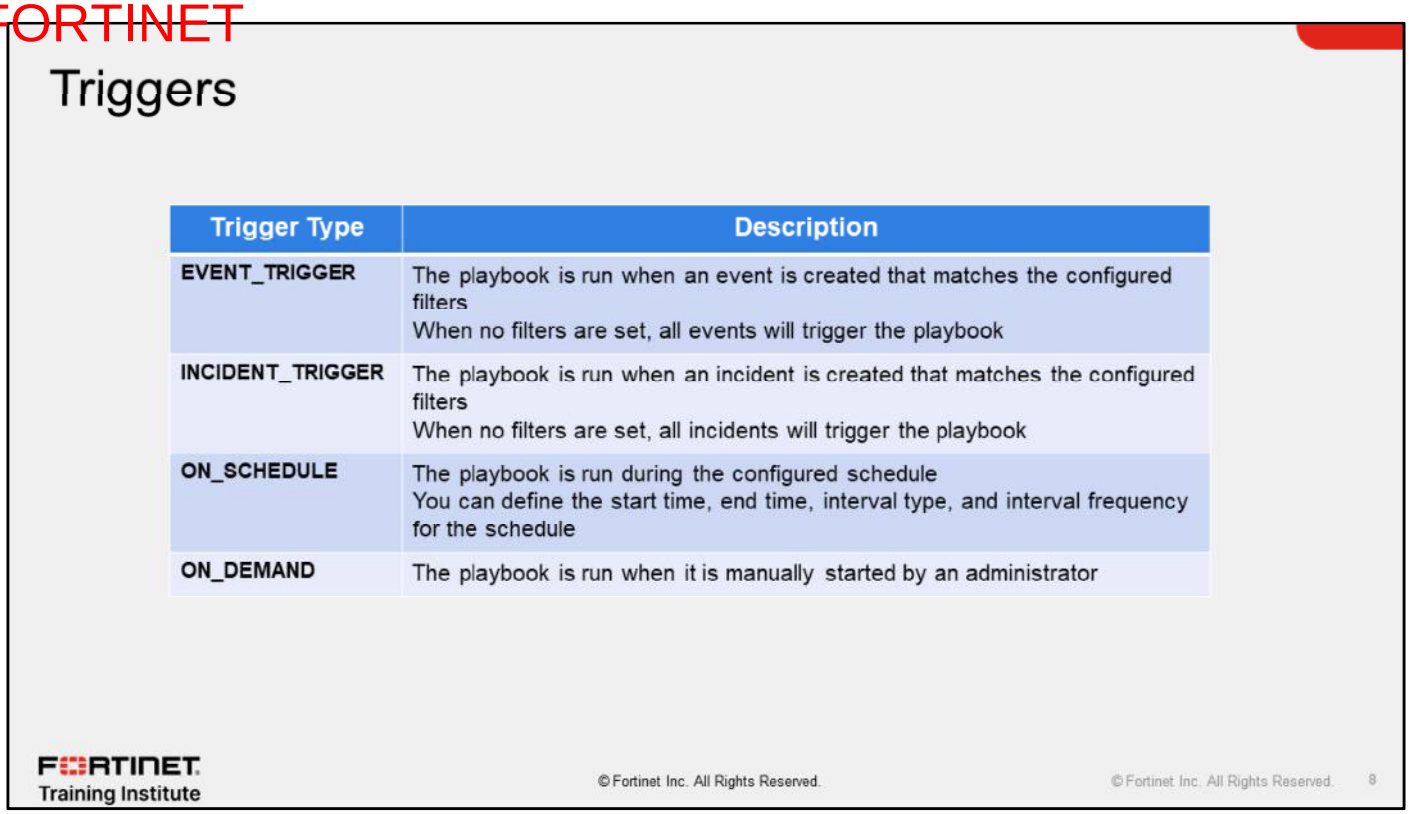
Each task includes the automated action that needs to take place. The available actions depend on the connector used. Connectors allow tasks to be performed on supported devices.

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 following 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.

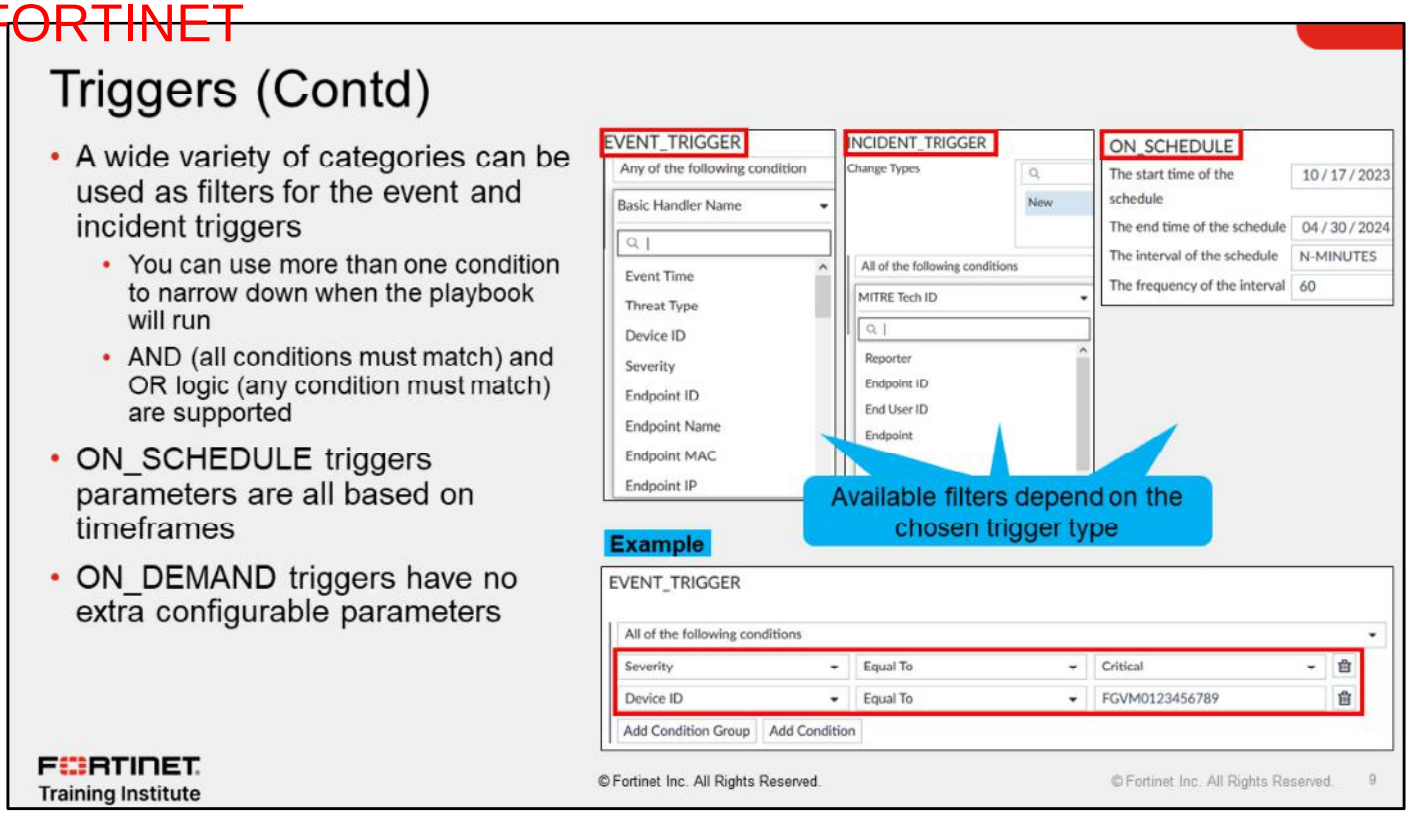
After a playbook is triggered, it flows through the configured tasks, as defined in the playbook designer.

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.

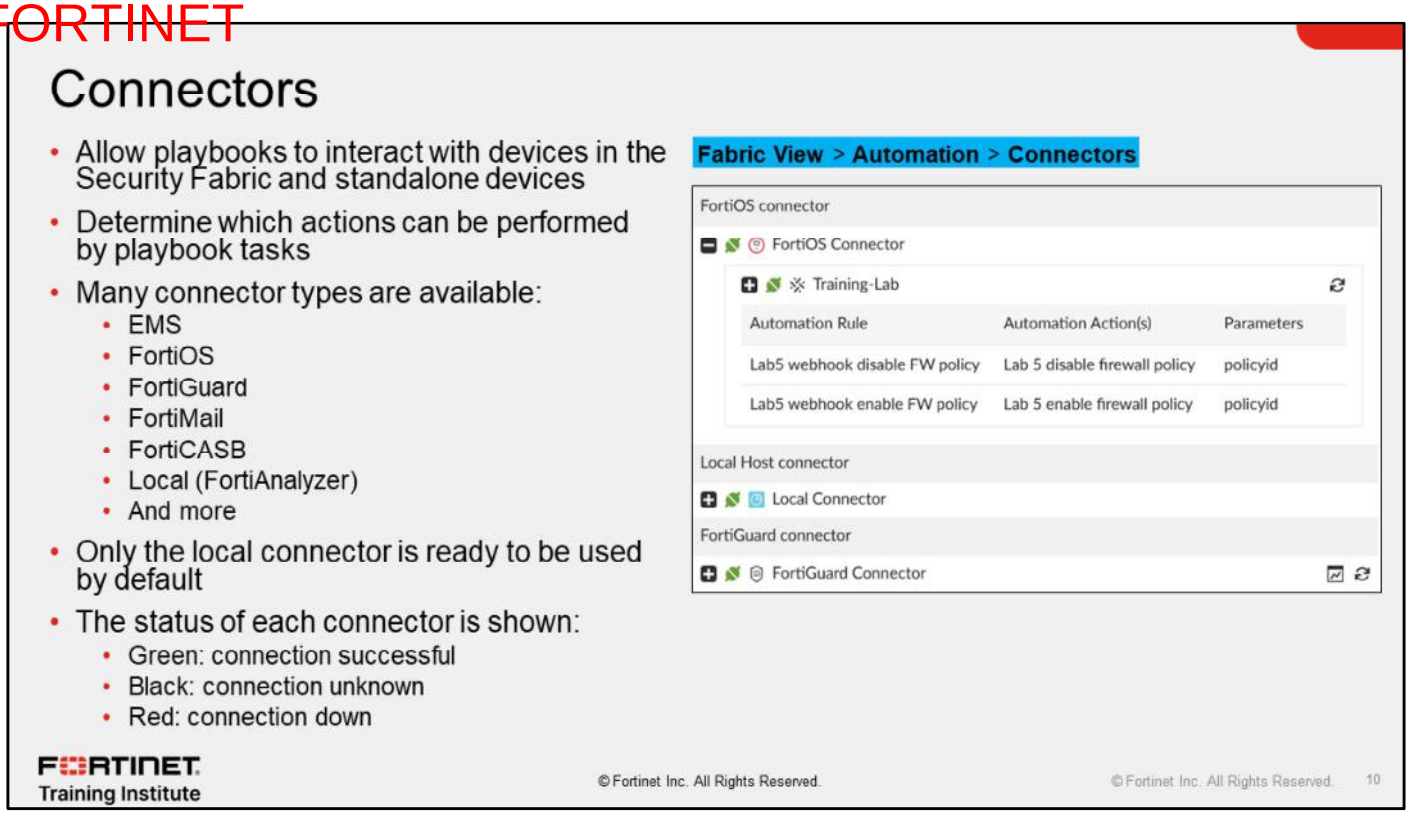
Note that playbooks with the ON_SCHEDULE trigger can also be executed manually. This allows you to test them outside of their configured timeframe.



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 will vary depending on the connector type used. Each type allows for different actions.

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

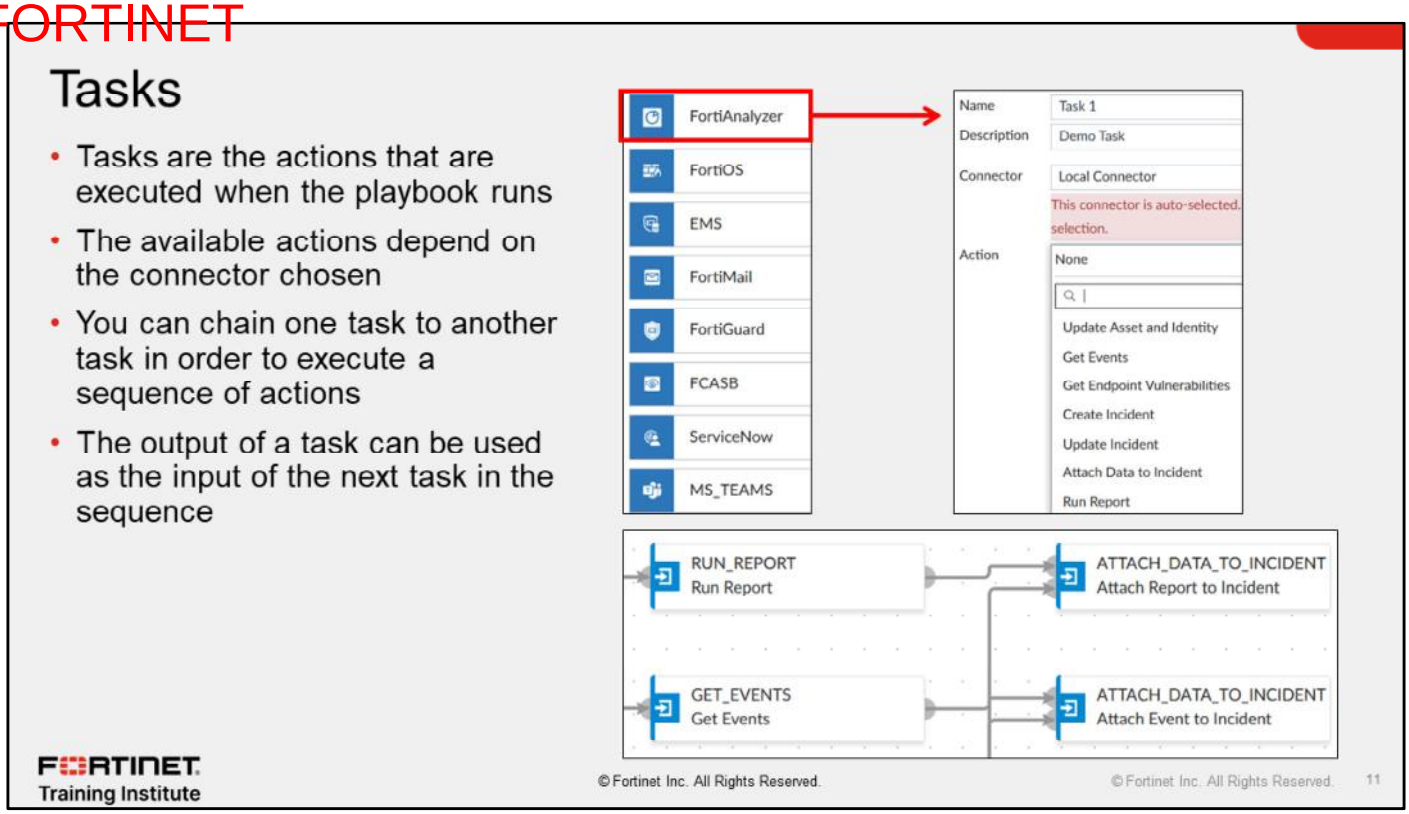
The status of connectors is indicated by a colored icon:

- Green: The API connection successful.
- Black: 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, in order to see the actions related to that FortiOS connector, you must enable an automation rule using the **Incoming Webhook Call** trigger on the FortiGate side.



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 get 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 will 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.

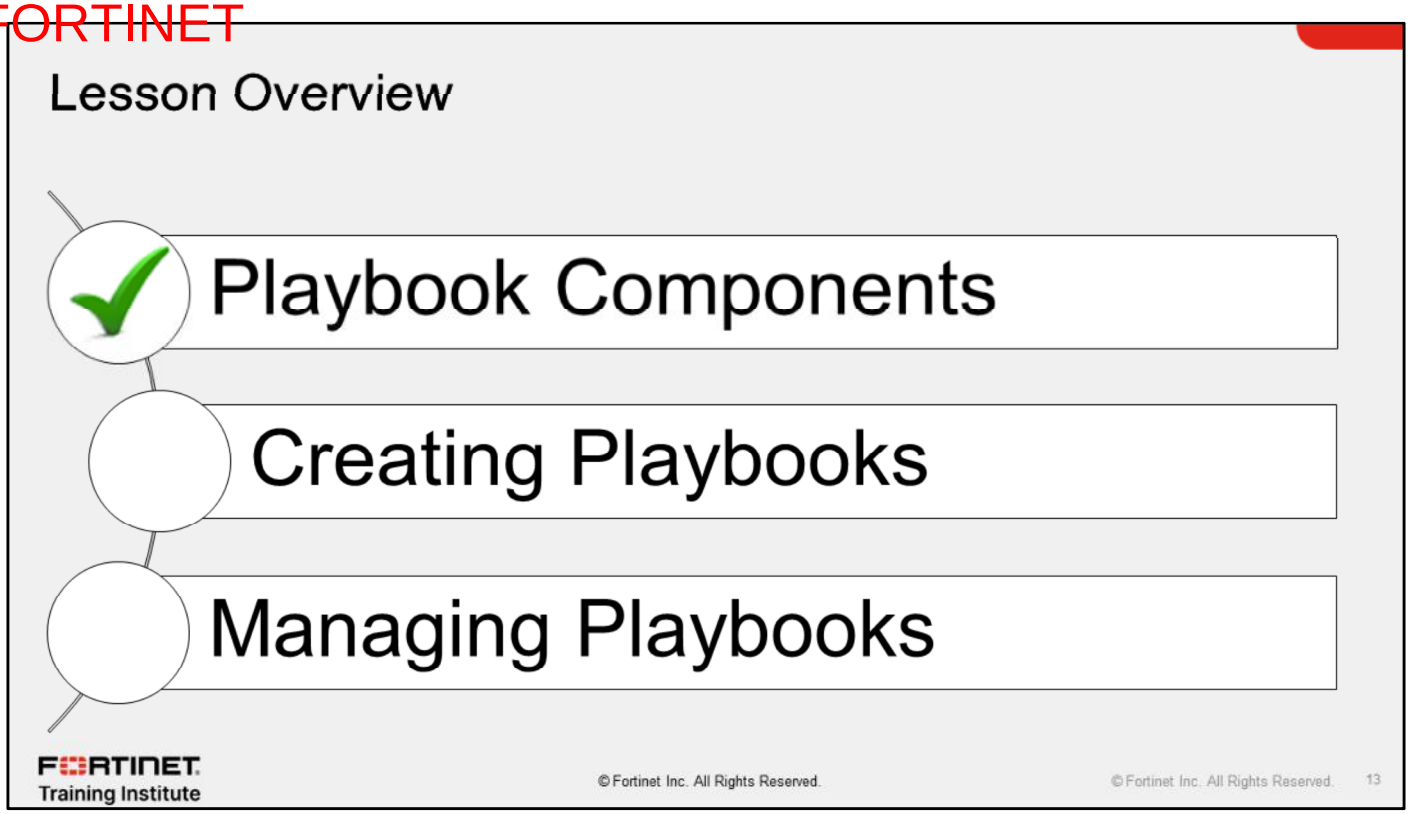
Knowledge Check

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

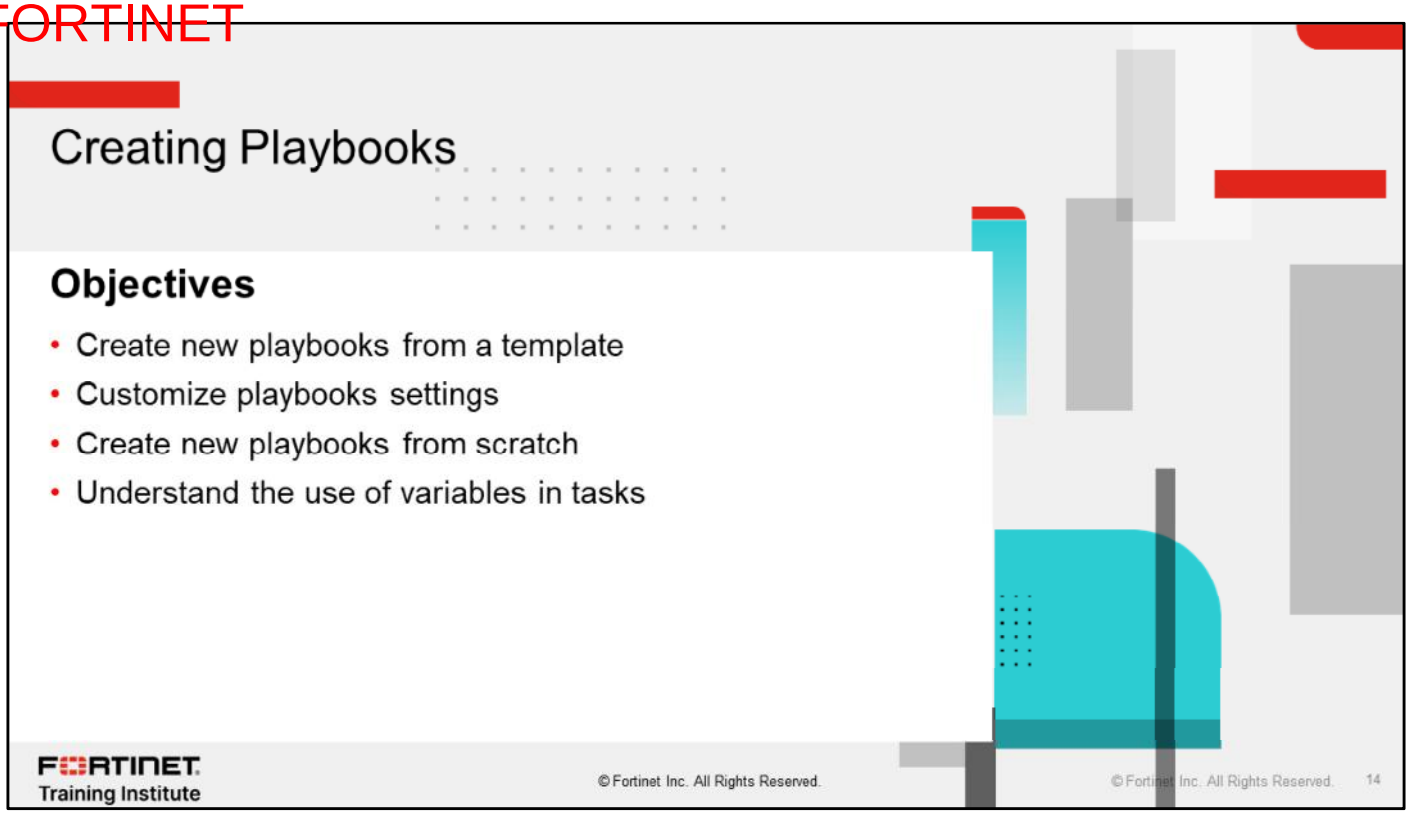
FORTINET Training Institute

© Fortinet Inc. All Rights Reserved. 12



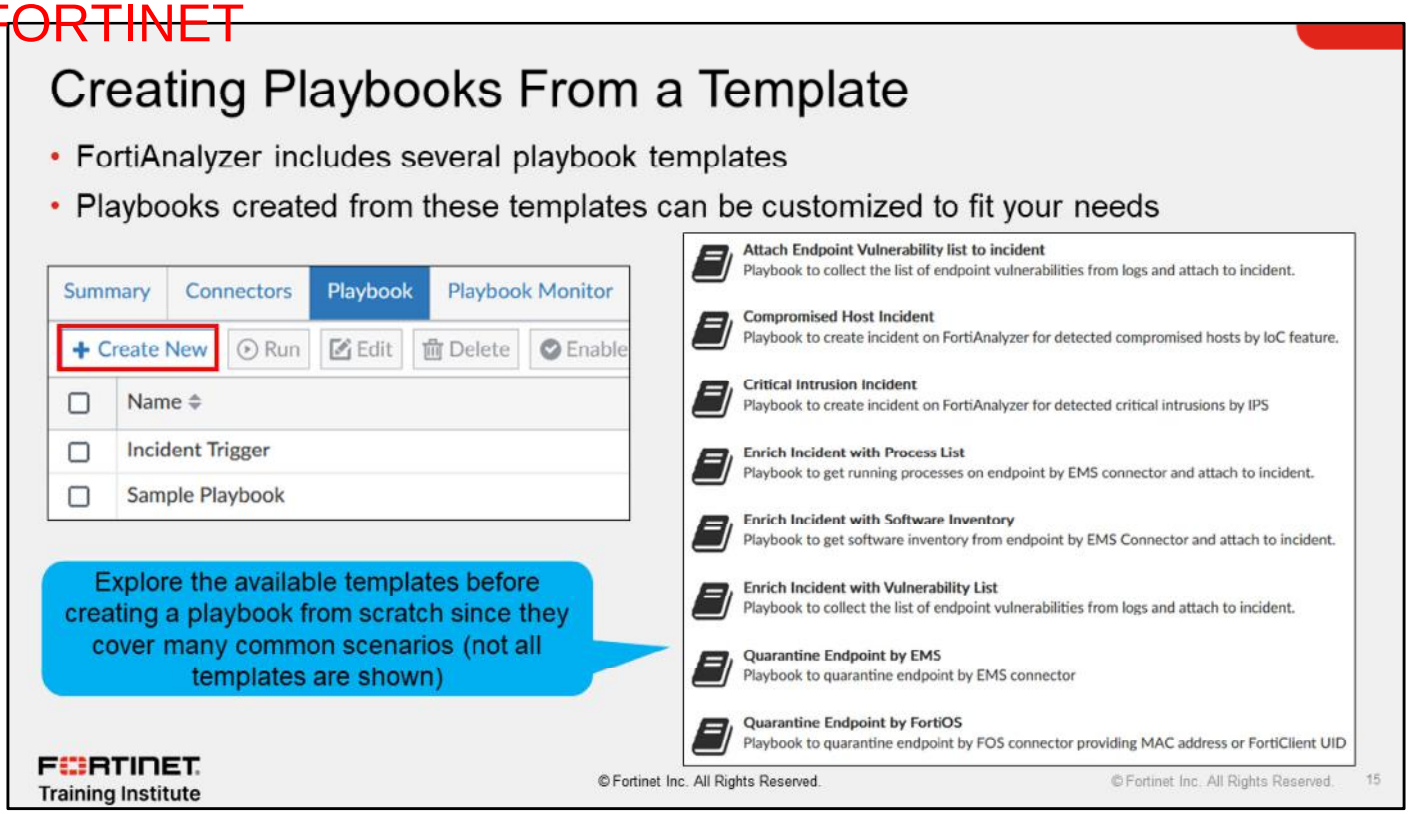
Good job! You now understand playbook components.

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 efficiency in your organization's SOC operations.



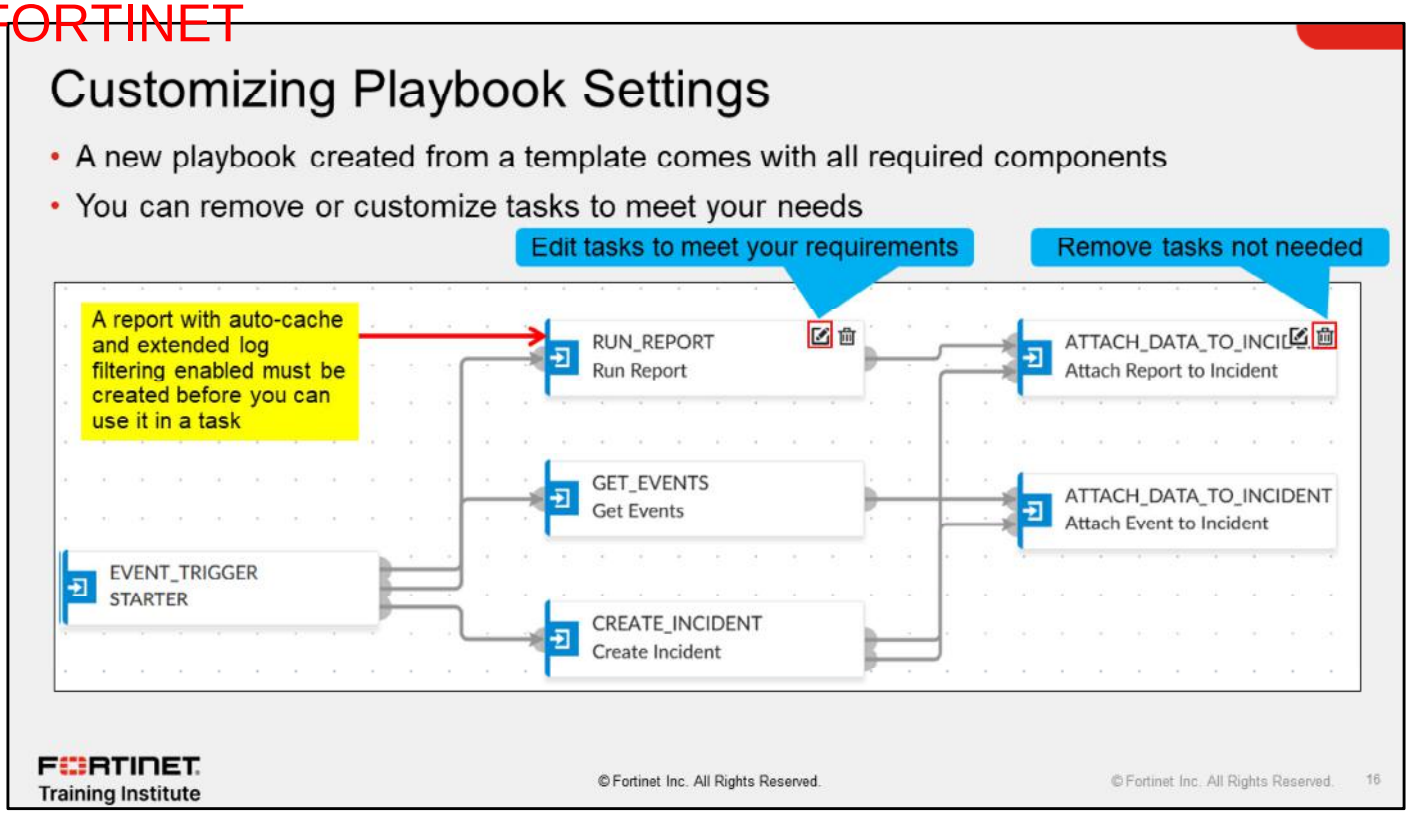
FortiAnalyzer includes several playbook templates that SOC analysts can customize. The templates included allow you to perform tasks such as:

- 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) IP addresses.
- Quarantine and run antivirus scans on endpoints.

To create a new playbook from a template, click **Playbook** > **Create New**.

Next, select a playbook template with a description that responds to your needs and the playbook designer will open.

You will learn more about creating a playbook from scratch in this lesson.



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:

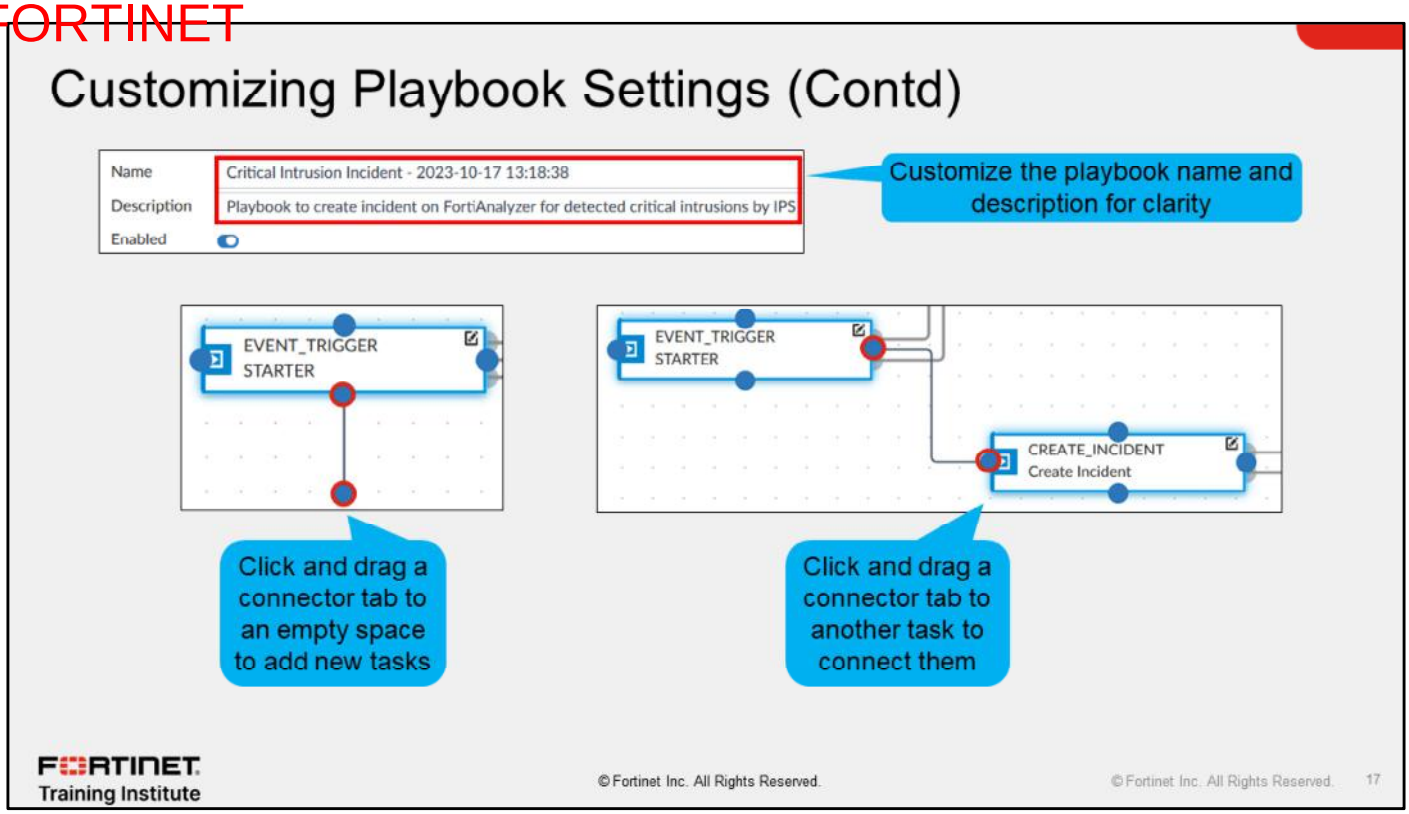
- Run when the specified event or events are generated.
- Create a new incident.
- Get the list of events specified in the task filter and add them to the incident.
- Run a report and attach it to the incident.

As a result of running the playbook, the incident will include relevant information that the analyst in charge can use during an incident investigation.

Note that to be able to run a report as a task, that report must already exist, and it must 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.

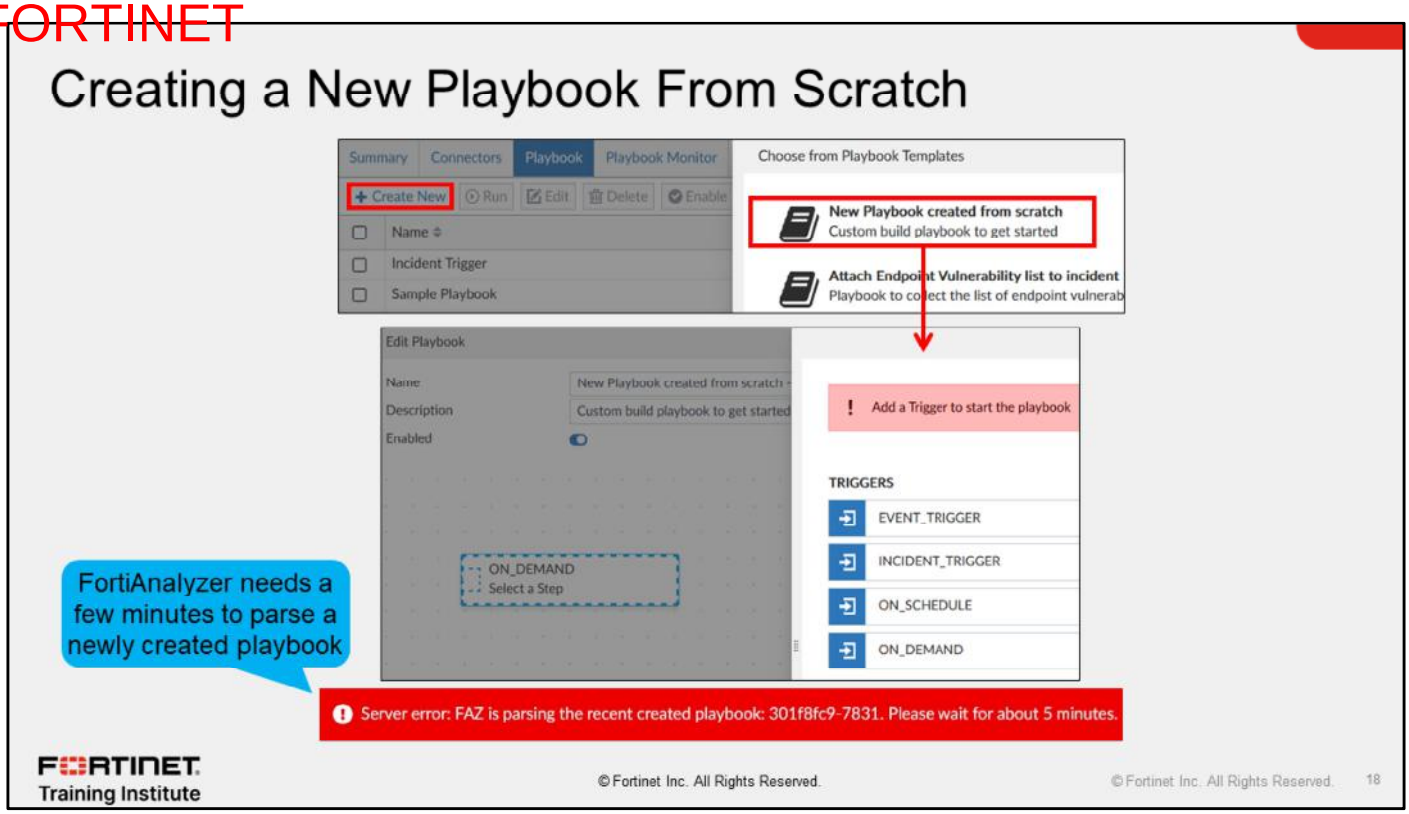
To remove a task, click the trash can icon in the upper-right corner.



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 it's highly recommended that you edit the names and descriptions of new playbooks to something easily recognizable.

To add new tasks, click and drag the connector tabs attached to the current tasks or the trigger. 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.



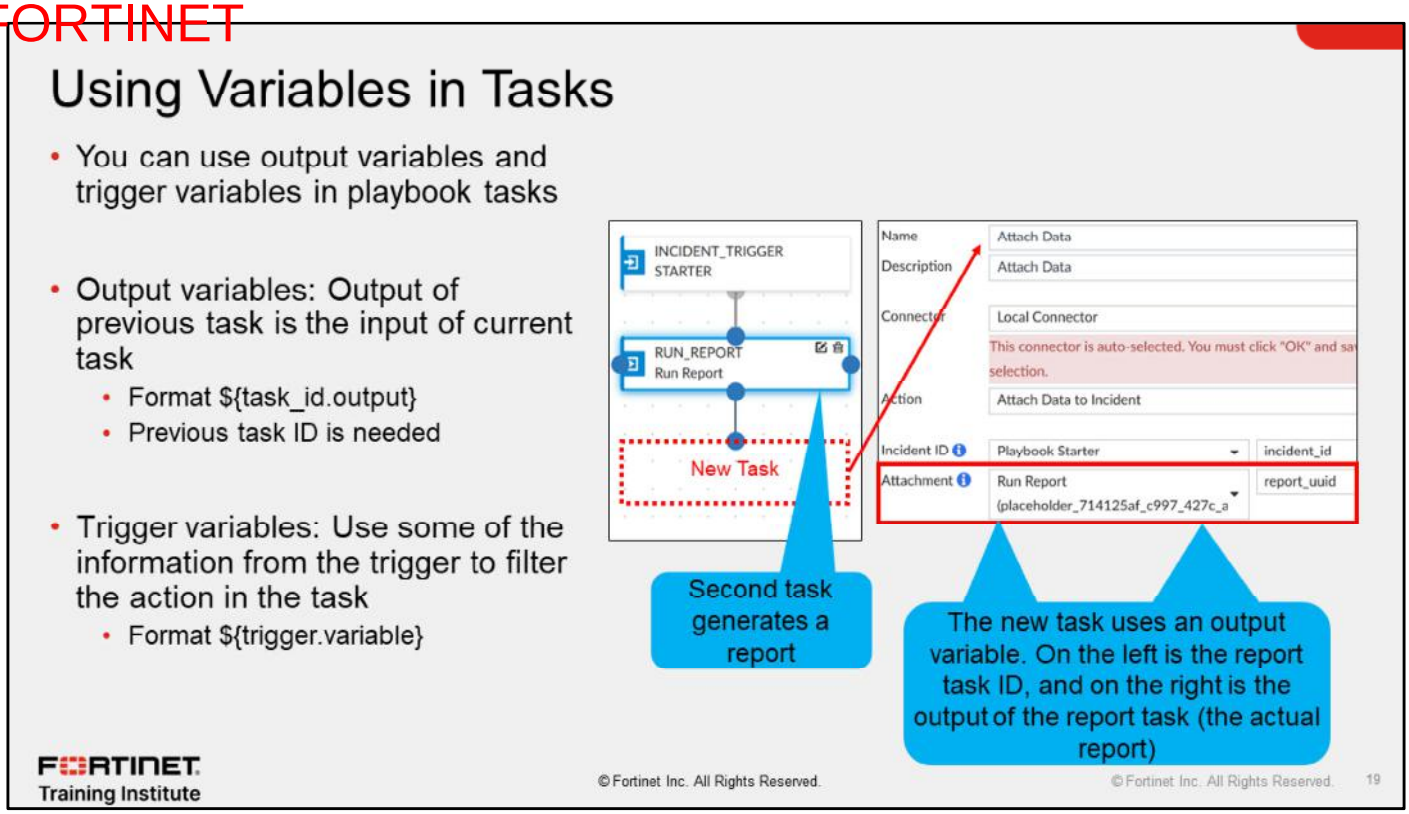
If none of the templates serves your needs, you can always create a playbook from scratch. To do so, click **Playbook** > **Create New**, and then select the first option in the list. The playbook designer will open.

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

You then need to 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 use 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 an 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.

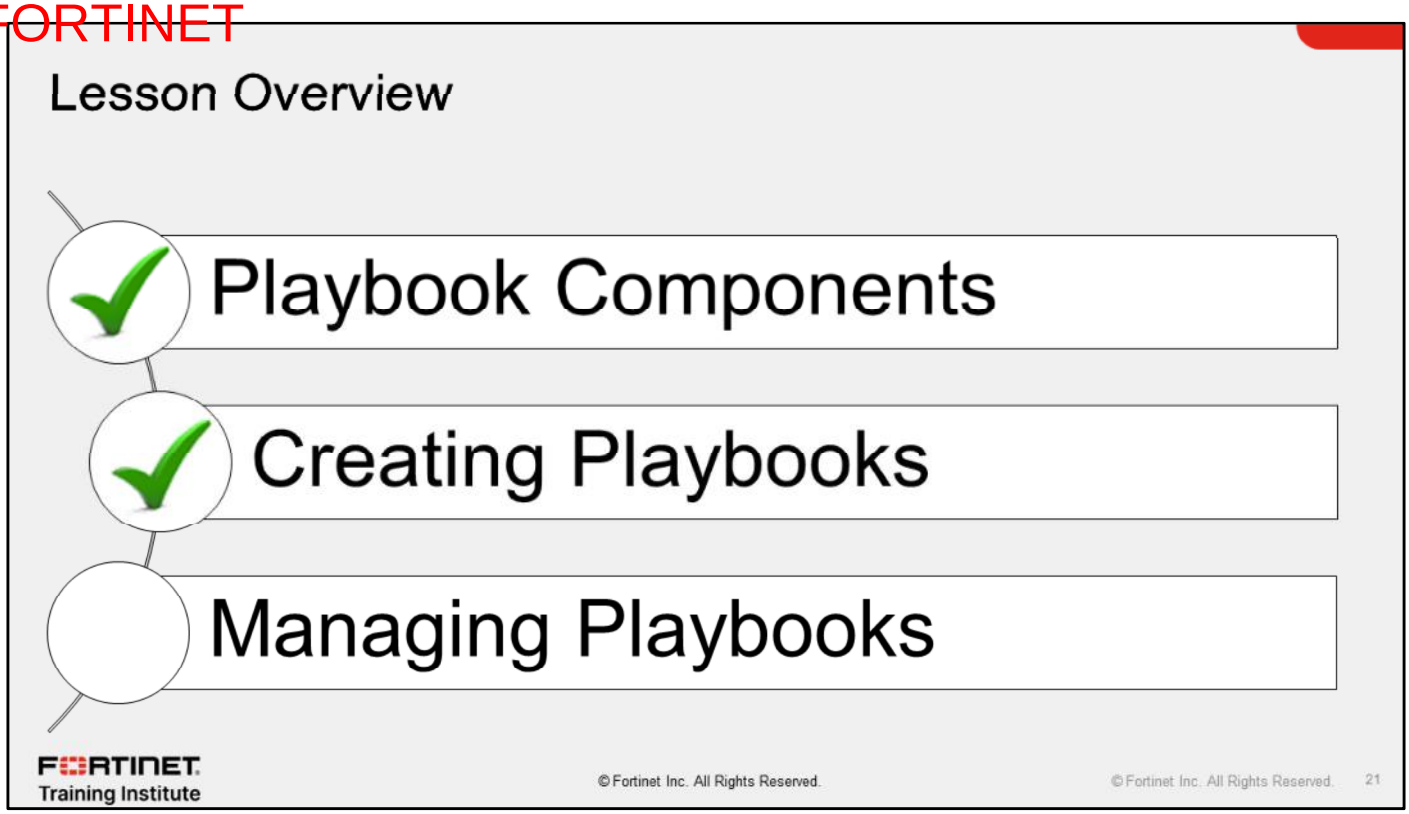
Knowledge Check

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

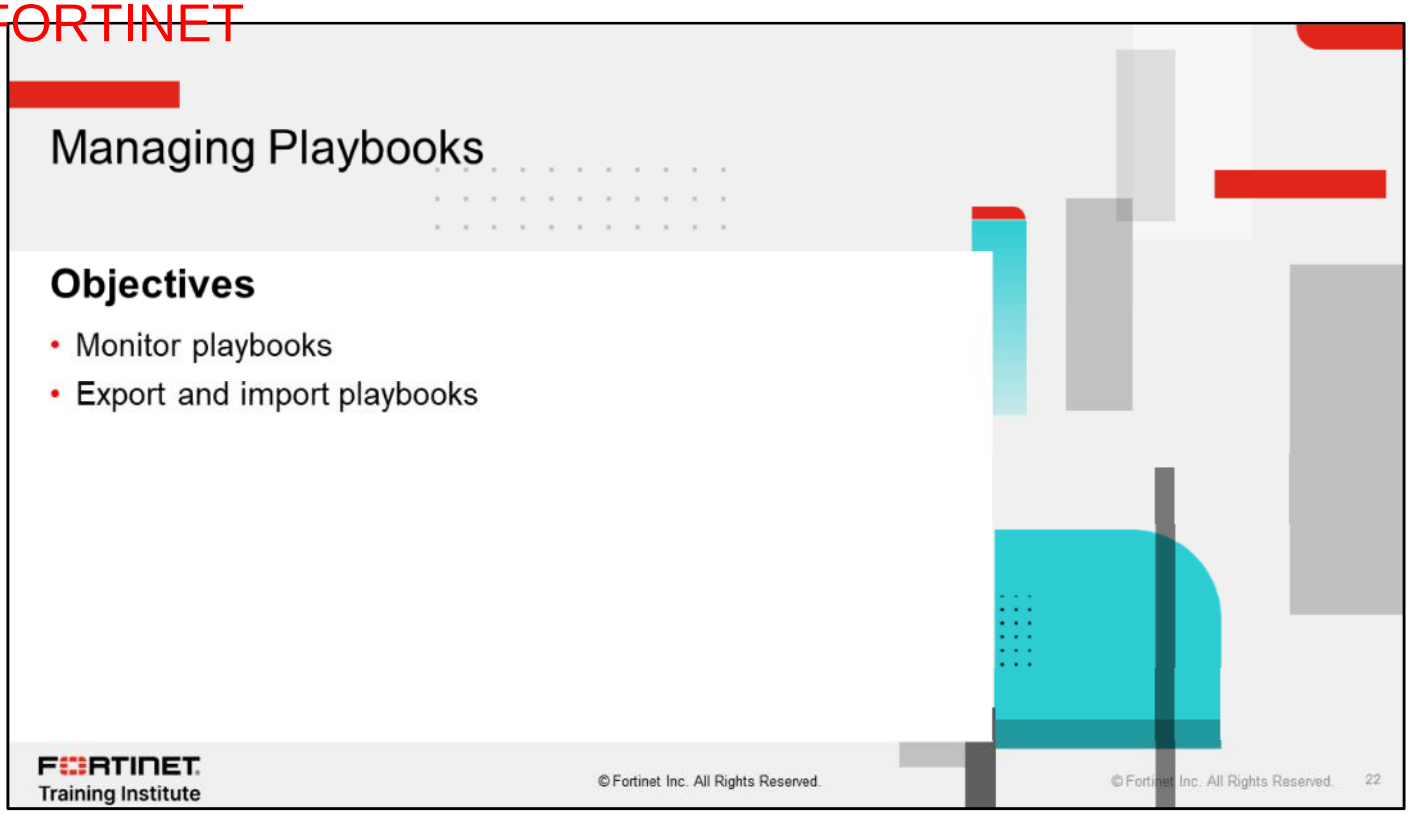
FORTINET Training Institute

© Fortinet Inc. All Rights Reserved. 20



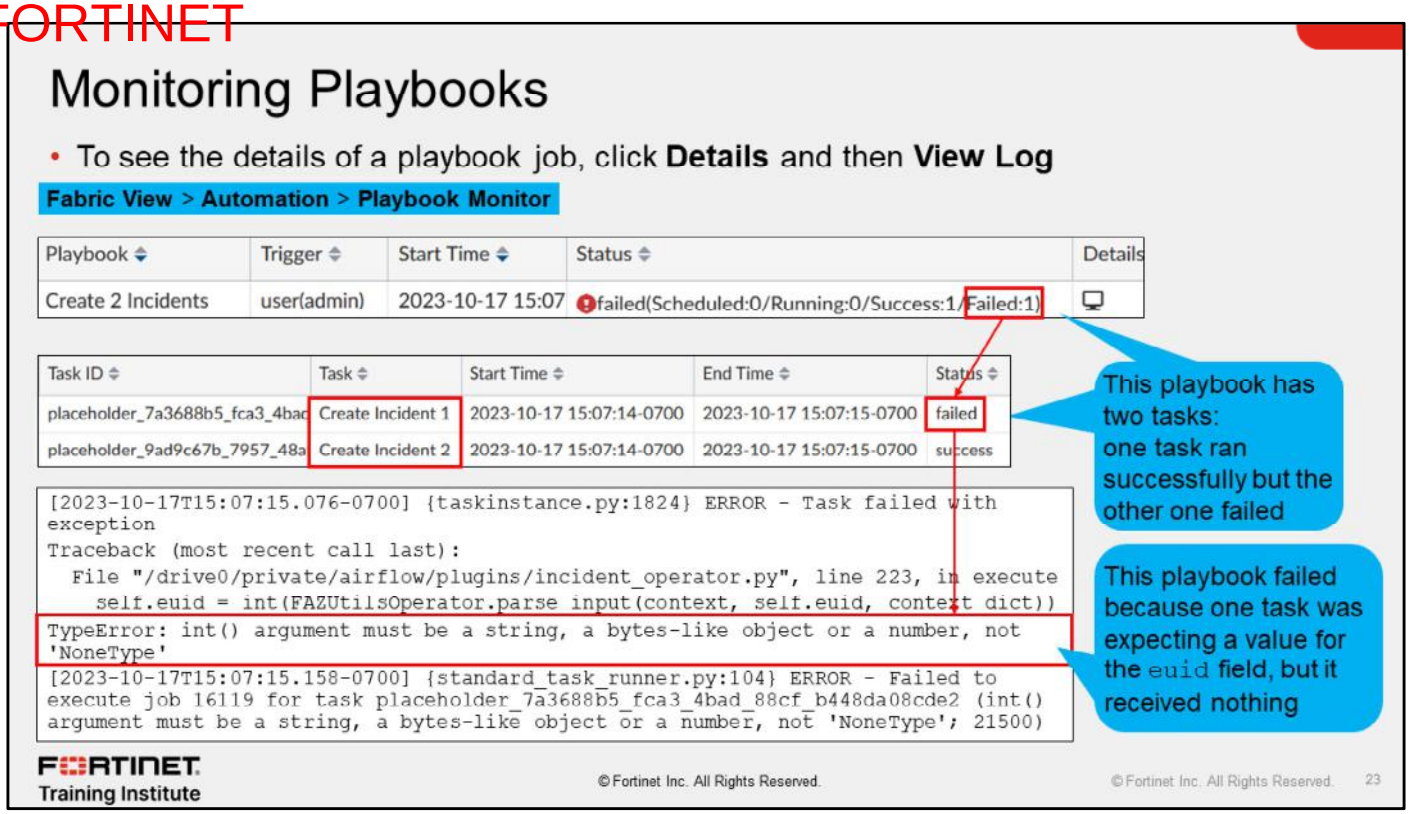
Good job! You now know how to create playbooks and use them to automate tasks.

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 if all automated tasks ran successfully or not. You will also be able to export playbooks to another ADOM or device.



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.

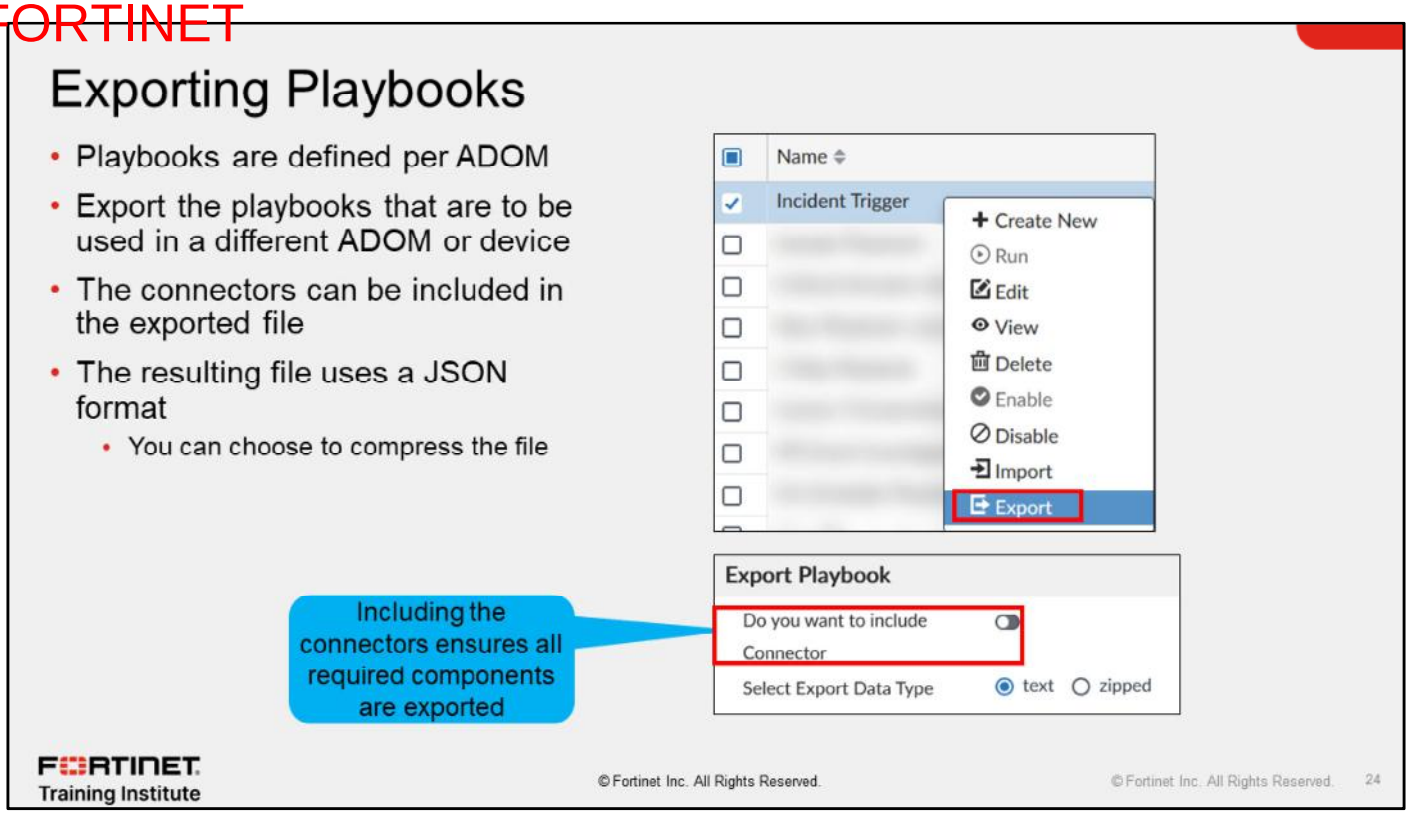
The status of a playbook can be one of the following:

- 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**. A failed status, however, 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.



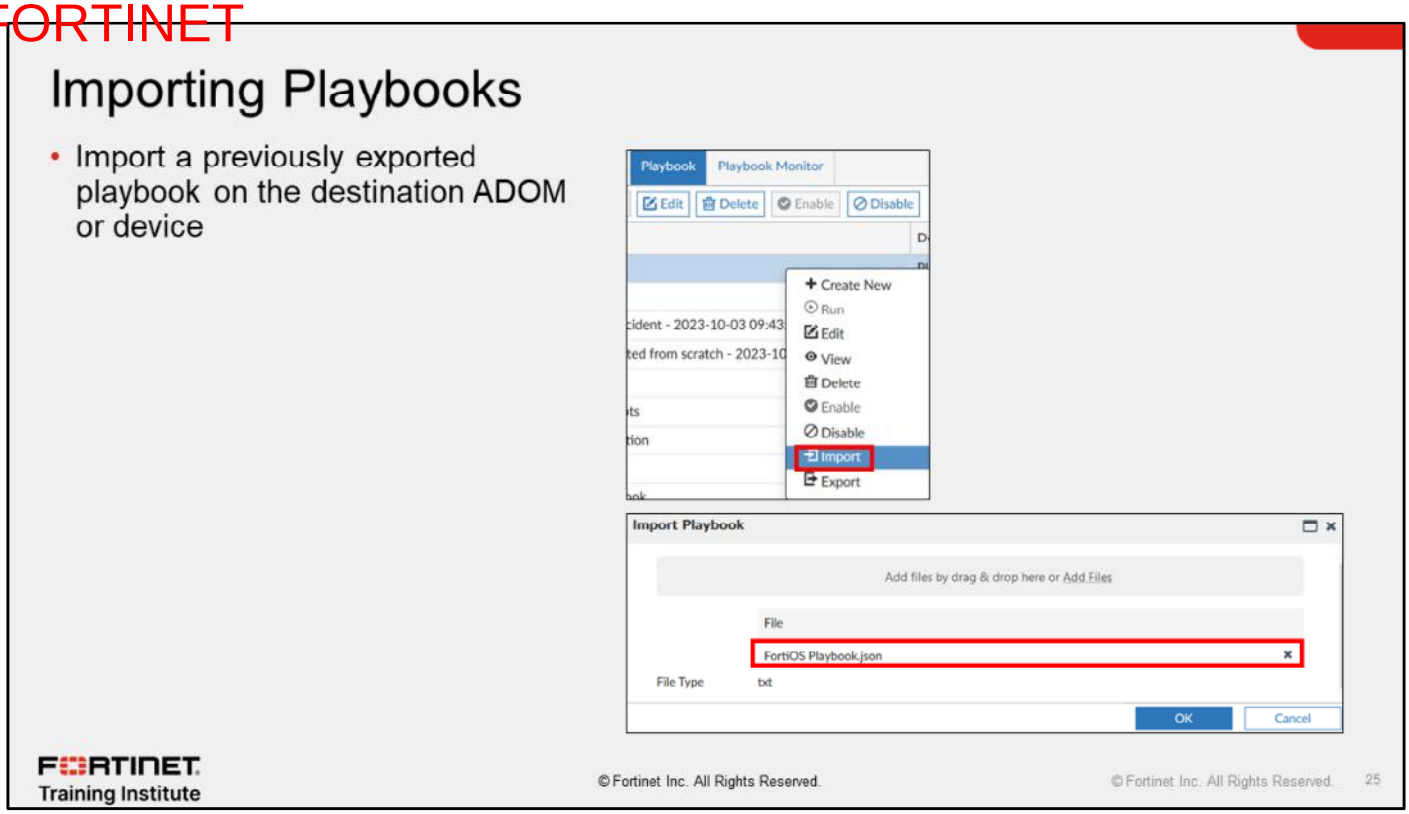
Playbooks are defined per ADOM. If you want to use an existing playbook on a different ADOM or a different FortiAnalyzer device, you can export the playbook.

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

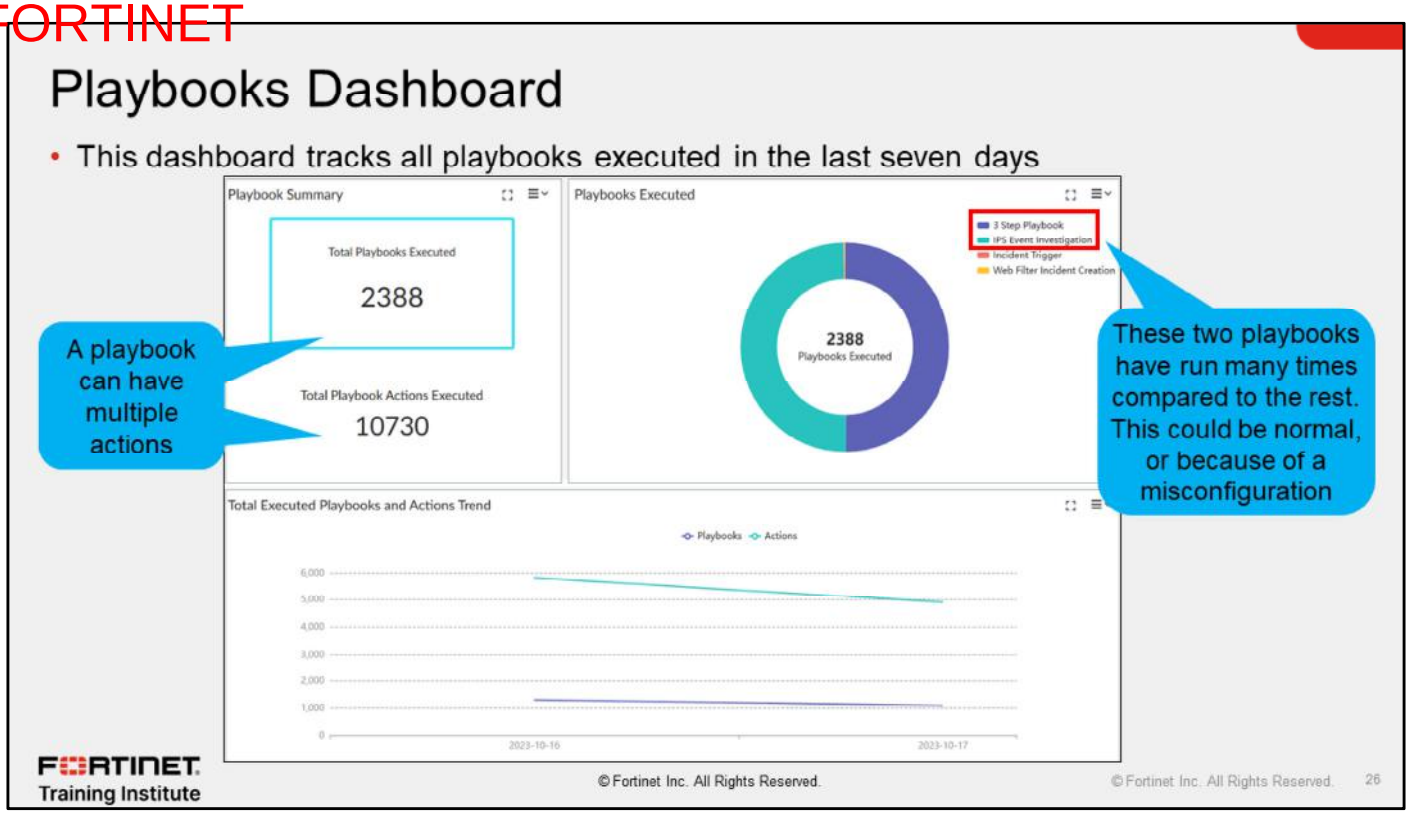


To import a playbook, right-click anywhere on the playbook dashboard, and then click **Import**.

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.

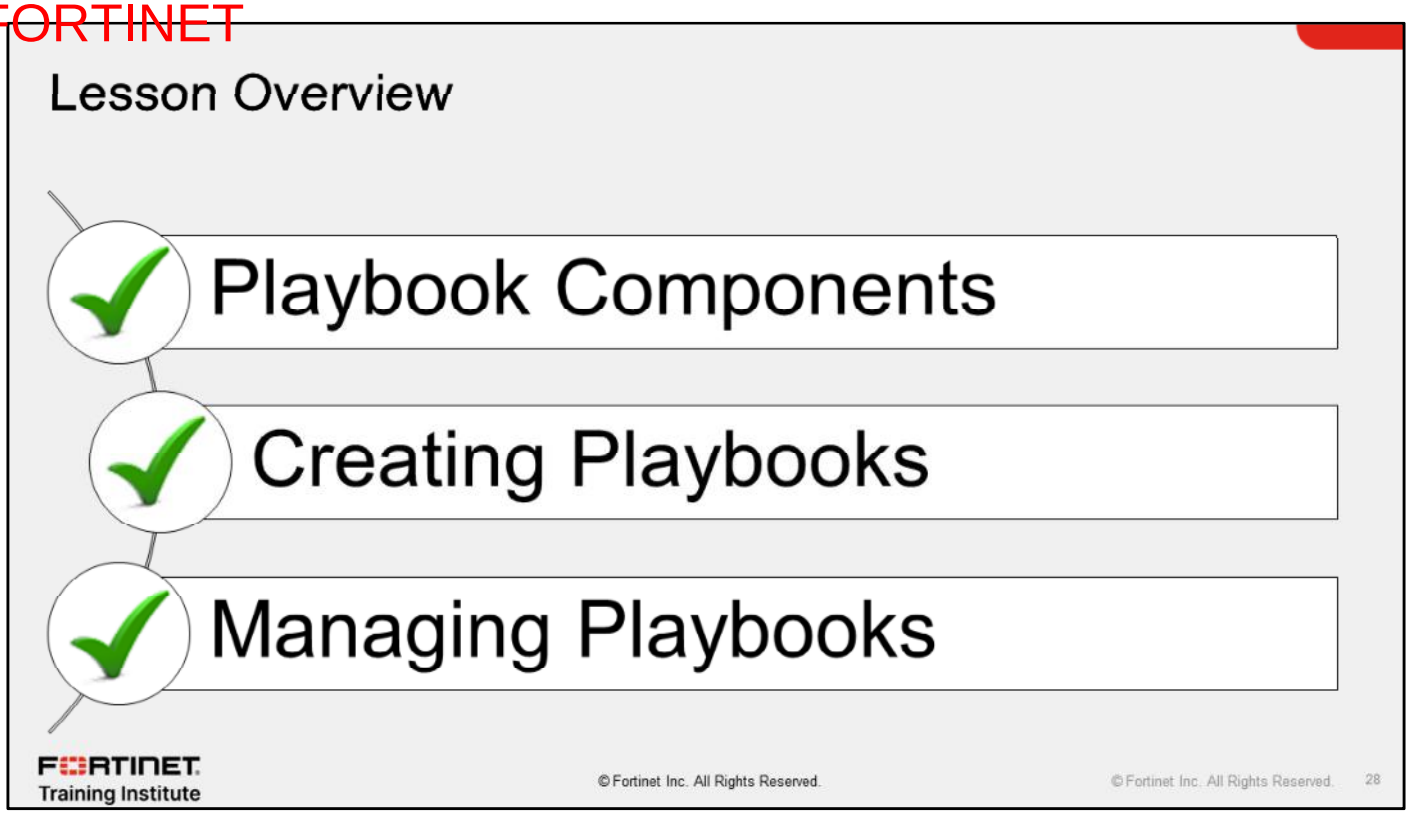
Knowledge Check

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

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

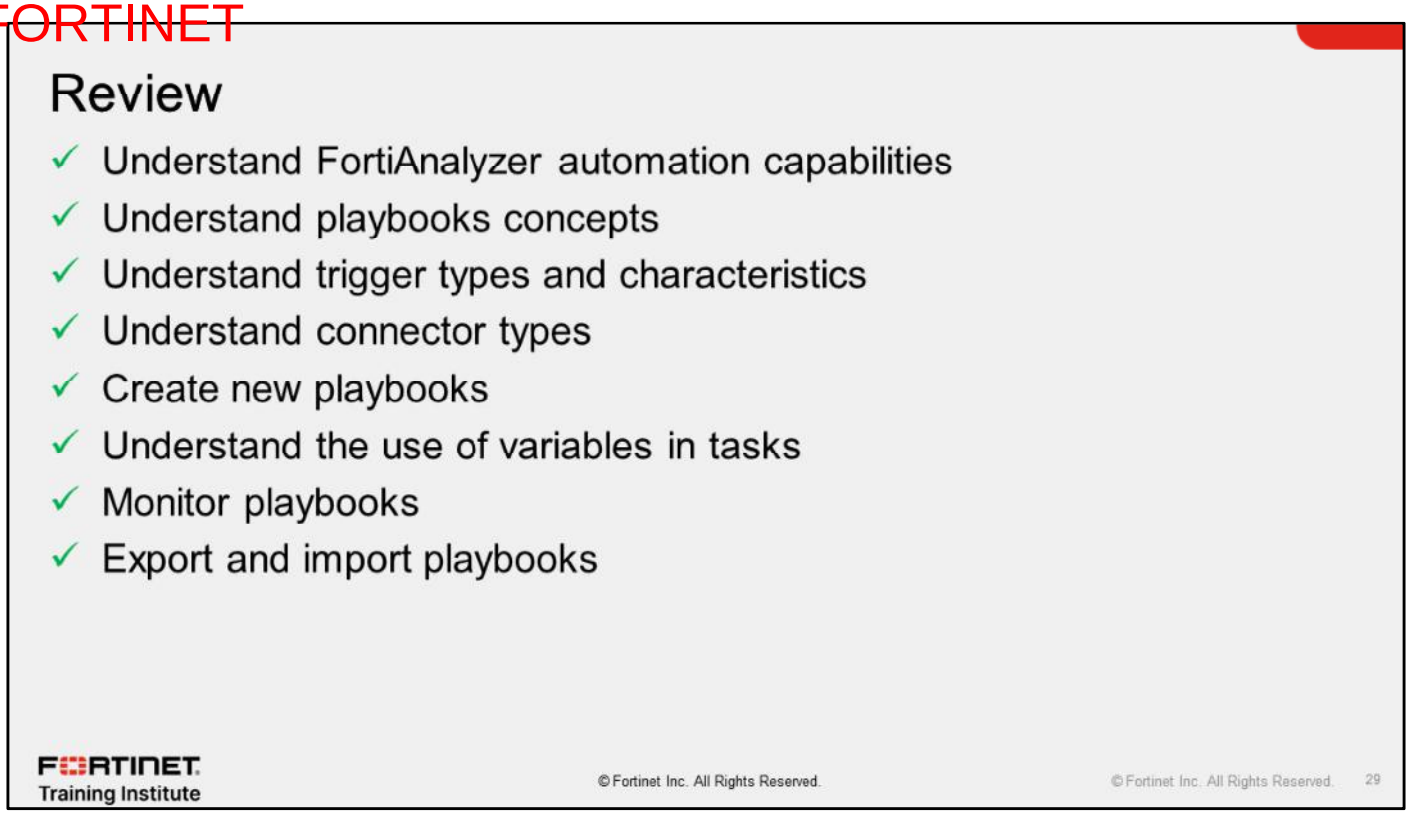
FORTINET Training Institute

© Fortinet Inc. All Rights Reserved. 27



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.