

DO NOT REPRINT
© FORTINET



FortiAnalyzer Analyst Study Guide

FortiAnalyzer 7.4

FORTINET®
Training Institute

DO NOT REPRINT

© FORTINET

Fortinet Training Institute - Library

<https://training.fortinet.com>

Fortinet Product Documentation

<https://docs.fortinet.com>

Fortinet Knowledge Base

<https://kb.fortinet.com>

Fortinet Fuse User Community

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

Fortinet Forums

<https://forum.fortinet.com>

Fortinet Product Support

<https://support.fortinet.com>

FortiGuard Labs

<https://www.fortiguard.com>

Fortinet Training Program Information

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

Fortinet | Pearson VUE

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

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

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



12/21/2023

TABLE OF CONTENTS

00 SQL and Datasets.....	4
01 Introduction and Initial Access.....	38
02 Logging.....	55
03 Incidents and Events.....	98
04 Reports.....	140
05 Playbooks.....	187

DO NOT REPRINT

© FORTINET



FortiAnalyzer Analyst

SQL and Datasets

 FortiAnalyzer 7.4.1

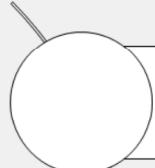
Last Modified: 21 December 2023

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.

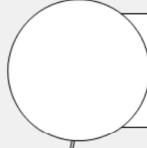
DO NOT REPRINT

© FORTINET

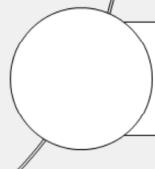
Lesson Overview



Datasets and SQL



SQL Functions and Operators



FortiAnalyzer Functions and Macros

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

DO NOT REPRINT

© FORTINET

Datasets and SQL

Objectives

- Describe datasets
- Understand SQL basics



© Fortinet Inc. All Rights Reserved.

3

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.

DO NOT REPRINT

© FORTINET

Datasets

- Datasets are SQL SELECT queries to the database
 - Data populates a chart

ADOM specific

The screenshot shows the FortiAnalyzer interface with the following details:

- Left Sidebar:** Includes links for Dashboard, Device Manager, FortiView, Log View, Fabric View, Incidents & Events, Reports (selected), Generated Reports, Report Definitions (selected), Advanced Settings, and System Settings.
- Top Navigation Bar:** Contains tabs for All Reports, Templates, Chart Library, Macro Library, and Datasets (selected). Below the tabs are buttons for Create New, View, Delete, More, Show Predefined (checked), Show Custom (checked), and a Search bar.
- Dataset List:** A table showing predefined datasets. The 'App-Sessions-By-Category' dataset is selected (indicated by a checked checkbox) and highlighted with a blue callout. Other datasets listed include App-Risk-Top-User-Source-By-Sessions, App-Risk-Virus-Discovered, App-Risk-Vulnerability-Discovered, App-Risk-Web-Browsing-Activity-Hostname-Category, App-Risk-Web-Browsing-Summary-Category, and app-Top-Allowed-Applications-hv.
- Callout:** A blue callout points to the 'App-Sessions-By-Category' dataset, containing the text "Dataset (example App-Sessions-By Category)".
- Code Block:** A code box shows the SQL query for the selected dataset:


```
select appcat, count(*) as sessions from
$log where $filter and (logflag&1>0) and
nullifna(appcat) is not null group by
appcat order by sessions desc
```
- Page Footer:** Includes the Fortinet Training Institute logo and copyright information: © Fortinet Inc. All Rights Reserved. 4

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.

DO NOT REPRINT

© FORTINET

Designing SQL Queries

- FortiAnalyzer uses SQL as the local database
- Proper query syntax required

SQL queries are not case sensitive

The screenshot shows the FortiAnalyzer interface. On the left, there's a sidebar with 'Name' (App-Sessions-By-Category), 'Log Type' (Traffic), and 'Query'. The main area has a code editor with the following SQL query:

```

1 SELECT
2     appcat,
3     count(*) AS sessions
4 FROM
5     $log
6 WHERE
7     $filter
8     AND (logflag & 1 > 0)
9     AND nullifna(appcat) IS NOT NULL
10 GROUP BY
11     appcat
12 ORDER BY
13     sessions DESC

```

Below the code editor are 'Recommendations', 'Validate', 'Analyze Query', and 'Format' buttons. A 'Variables' section contains two rows: 'Group (group)' and 'User or Source'. The 'User or Source' row has a dropdown set to 'coalesce(nullifna(`u`))' and a 'User (or Source IP)' input field.

Test that queries are well-formed and contain keywords that are spelled correctly

The screenshot shows the results of the executed SQL query. It includes a 'Time Period' (Today) and 'Devices' (All Devices) filter. The results table has columns 'appcat' and 'sessions'. The data is as follows:

appcat	sessions
unscanned	189
Web.Client	166
Storage.Backup	56
Social.Media	32
Video/Audio	21
Collaboration	15
im	8

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.

DO NOT REPRINT**© FORTINET**

SQL—The Declarative Language

```
SELECT dstip as destination_ip, count(*) as Session  
FROM $log WHERE $filter and dstip is not null GROUP BY  
dstip ORDER BY session desc LIMIT 7
```

- Declarative language: describes *what* needs to be done rather than *how* to do it
- All information in the database is represented as tables
 - Each table consists of a set of rows and columns
 - Two types of tables: user tables and system tables



© Fortinet Inc. All Rights Reserved.

6

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

DO NOT REPRINT**© FORTINET**

Basic Data Manipulation Constructs

- **SELECT**
 - Retrieve and display data from one or more database tables (read-only query)
 - `SELECT ... FROM ... WHERE`
- **INSERT**
 - Add new rows of data into a table
 - `INSERT INTO ... VALUES ...`
- **UPDATE**
 - Modify existing data in a table
 - `UPDATE ... SET ... WHERE`
- **DELETE**
 - Remove rows of data from a table
 - `DELETE FROM ... WHERE`

This is the only query statement used by FortiAnalyzer for reports



© Fortinet Inc. All Rights Reserved.

7

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.

DO NOT REPRINT**© FORTINET**

SELECT Statement

- The SELECT statement retrieves the log data you want from the database
- Must specify criteria using a recognized/supported clause

Clauses must be coded in a specific sequence

Clause	Definition
FROM	Selects the table or views
WHERE	Sets the conditions (all rows that do not satisfy the condition are eliminated)
GROUP BY	Collects data across multiple records and groups the results by one or more columns
ORDER BY	Orders the results by rows
LIMIT	Limits the number of records returned based on a limit value. OFFSET clause can be used with the LIMIT clause to offset the results by a set value

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.

DO NOT REPRINT**© FORTINET**

SELECT and FROM

- Use the SELECT query to ask specific questions of the database

```
SELECT column FROM log_type
```

Column from database that contains
the value(s) you want to retrieve

The log type under which the data is contained
(for example, traffic, web filter, and so on)

- When designing queries for SQL reports on the FortiAnalyzer device, the log type is assigned to a variable called \$log

```
SELECT dstip as destination_ip FROM $log
```

```
SELECT *
returns all
data
```

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.

DO NOT REPRINT**© FORTINET**

Multiple Log Types

- Search multiple log types
 - Combine the data so that you can compare and contrast information

```
SELECT dstip, hostname FROM $log-traffic, $log-webfilter
```

Log type syntax	Log type
\$log-attack	Attack log
\$log-dlp	DLP log
\$log-event	Event log
\$log-netscan	NetScan log
\$log-app-ctrl	Application control log
\$log-emailfilter	Email filter log
\$log-traffic	Traffic log
\$log-virus	Antivirus log
\$log-webfilter	Web filter log

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
```

DO NOT REPRINT

© FORTINET

WHERE

- The WHERE clause requests data with certain characteristics
 - The expression specifies a stored value in the database

```
SELECT column FROM log_type WHERE expression1 and expression2 not in
expression3
```

Criteria you want to specify

Can use multiple expressions separated by AND/OR/NOT statements

```
SELECT dstip as destination_ip FROM $log WHERE $filter and dstip is
not null
```

Name	Example Dataset
Log Type	Traffic
Query	1 SELECT dstip as Destination_IP FROM \$log WHERE \$filter and dstip is not null

Go Stop
Time Period
Today
Devices:
All Devices ▾
destination_ip
1.1.1.32
94.229.20.61
54.83.43.69
175.126.123.219
224.141.85.77

© Fortinet Inc. All Rights Reserved.

11



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.

DO NOT REPRINT

© FORTINET

GROUP BY

- GROUP BY statement is usually used in conjunction with aggregate functions to group data by one or more columns.
- Returns one output row for each group
 - Can form groups within groups
- Each item in the SELECT list produces a single value per set

```
SELECT column, aggregate_function FROM log_type WHERE  
expression1 and expression2 not in expression3 GROUP BY column
```

If GROUP BY is used without aggregates,
it is similar to the DISTINCT clause

```
SELECT dstip as destination_ip, count(*) as session FROM $log  
WHERE $filter and dstip is not null GROUP BY dstip
```

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 used 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).

DO NOT REPRINT**© FORTINET**

ORDER BY

- By default, rows of an SQL query result table are not arranged in a particular order

```
SELECT column, aggregate_function FROM log_type WHERE expression1  
and expression2 not in expression3 GROUP BY column ORDER BY  
column_name | column_number asc|desc
```

Can sort data by
column name or
column number

Can sort data in ascending (asc)
or descending (desc) order. By
default, sorts in ascending order

```
SELECT dstip as destination_ip, count(*) as session FROM $log WHERE  
$filter and dstip is not null GROUP BY dstip ORDER BY session desc
```

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.

DO NOT REPRINT**© FORTINET**

LIMIT and OFFSET

- The **LIMIT** clause limits the number of records retrieved from the query result
 - Useful in large deployments to help limit the CPU/memory usage for reports
 - Can be combined with **ORDER BY asc** to get the “top <x> results”

```
SELECT column, aggregate_function FROM log_type WHERE expression1  
and expression2 not in expression3 GROUP BY column ORDER BY  
column_name|column_number asc|desc LIMIT number OFFSET number
```

Specify how many records to return

Specify how many records to skip

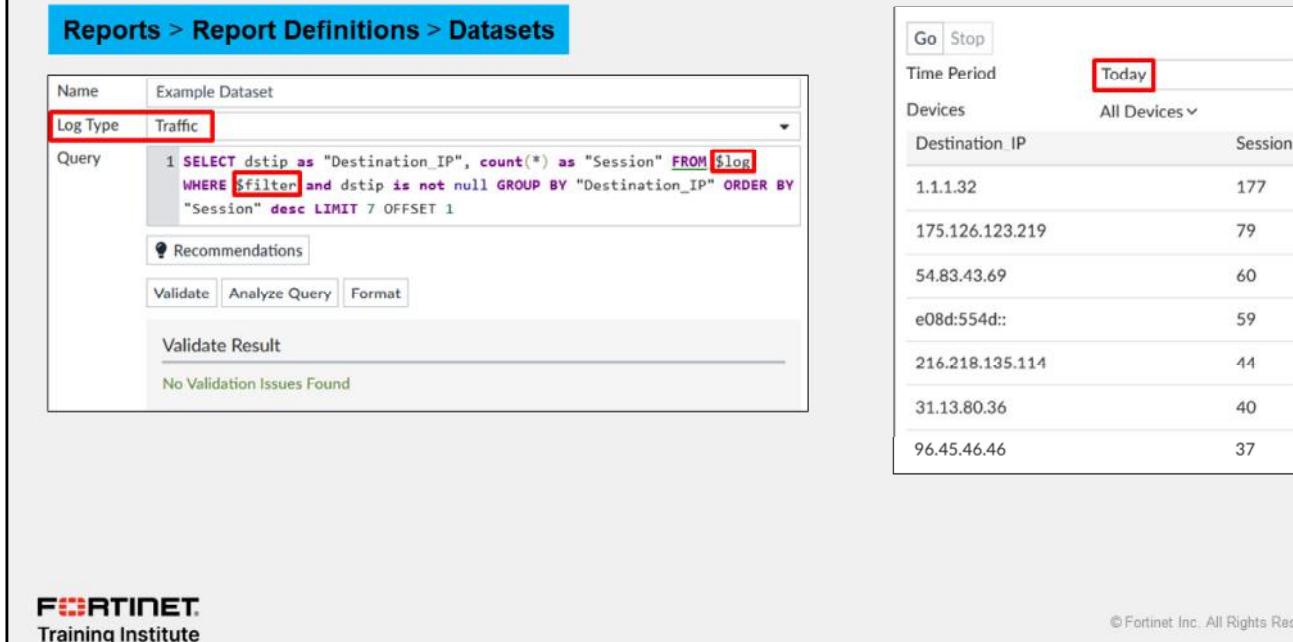
```
SELECT dstip as destination_ip, count(*) as session FROM $log WHERE  
$filter and dstip is not null GROUP BY dstip ORDER BY session desc  
LIMIT 7 OFFSET 1
```

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.

DO NOT REPRINT
© FORTINET

Creating a Dataset in FortiAnalyzer



The screenshot shows the FortiAnalyzer interface for creating a dataset. On the left, under 'Reports > Report Definitions > Datasets', a new dataset named 'Example Dataset' is being configured. The 'Log Type' is set to 'Traffic'. The 'Query' field contains the following SQL-like code:

```
1 SELECT dstip as "Destination_IP", count(*) as "Session" FROM $log
WHERE $filter and dstip is not null GROUP BY "Destination_IP" ORDER BY
"Session" desc LIMIT 7 OFFSET 1
```

Below the query, there are buttons for 'Recommendations', 'Validate', 'Analyze Query', and 'Format'. The 'Validate Result' section below says 'No Validation Issues Found'.

On the right, a table displays the results of the query. The columns are 'Destination IP' and 'Session'. The data is as follows:

Destination IP	Session
1.1.1.32	177
175.126.123.219	79
54.83.43.69	60
e08d:554d::	59
216.218.135.114	44
31.13.80.36	40
96.45.46.46	37

At the bottom left is the Fortinet Training Institute logo, and at the bottom right are copyright and page number information: © Fortinet Inc. All Rights Reserved. 15.

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.

DO NOT REPRINT
© FORTINET

Analyzing a Dataset in FortiAnalyzer

The screenshot shows the FortiAnalyzer interface for creating and running a report definition. On the left, under 'Reports > Report Definitions > Datasets', a new dataset named 'Example Dataset' is being configured. The 'Log Type' is set to 'Traffic'. The 'Query' field contains the following SQL-like query:

```
1 SELECT dstip as "Destination IP", count(*) as "Session" FROM $log
WHERE $filter and dstip is not null GROUP BY "Destination IP" ORDER BY
"Session" desc LIMIT 7 OFFSET 1
```

Below the query, there are buttons for 'Recommendations', 'Validate', 'Analyze Query', and 'Format'. A 'Validate Result' section indicates 'No Validation Issues Found'. To the right, the results of the query are displayed in a table titled 'Destination IP' and 'Session'. The table shows the following data:

Destination IP	Session
1.1.1.32	177
175.126.123.219	79
54.83.43.69	60
e08d:554d::	59
216.218.135.114	44
31.13.80.36	40
96.45.46.46	37

At the bottom left is the Fortinet Training Institute logo, and at the bottom right is the copyright notice: © Fortinet Inc. All Rights Reserved. 16

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).

DO NOT REPRINT

© FORTINET

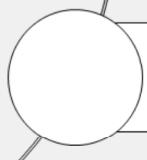
Lesson Progress



Datasets and SQL



SQL Functions and Operators



FortiAnalyzer Functions and Macros

Good job! You now understand datasets and SQL.

Now, you will learn about SQL functions and operators.

DO NOT REPRINT

© FORTINET

SQL Functions and Operators

Objectives

- Understand SQL functions
- Understand operators



© Fortinet Inc. All Rights Reserved.

18

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.

DO NOT REPRINT

© FORTINET

Aggregate Functions vs “Normal” Functions

Aggregate Functions	“Normal” Functions
Use the entire column of data as their input and produce a single output	Operate on each element in the column of data



© Fortinet Inc. All Rights Reserved.

19

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.

DO NOT REPRINT

© FORTINET

NULLIF

- NULLIF function takes two arguments: if the first two arguments are equal, then NULL is returned; otherwise, the first argument is returned.

```
SELECT NULLIF(expression1, expression2)
```

Must be values that are of the same datatype

- NULL represents unknown data—it is not equal to zero

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.

DO NOT REPRINT**© FORTINET**

COALESCE

- Returns the first of its arguments that is not NULL. NULL is returned only if all arguments are NULL

```
SELECT coalesce(catdesc, 'unknown') as category,
coalesce(root_domain(hostname), 'unknown') as domain FROM $log
GROUP BY category, domain
```

category	domain
Malicious Websites	xnwipt.com
unknown	corolbugan.com
Unrated	agoinside.gq
Malicious Websites	40thousandwords.com
Malicious Websites	apple-ituncs-ios.com
Unrated	repeat-chief.ru
Malicious Websites	kir22.ru
Malicious Websites	blissyogawithannu.com
Unrated	ichiventures.com

Another common function used in FortiAnalyzer datasets is COALESCE. 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, ...)

DO NOT REPRINT**© FORTINET**

Aggregate Functions

- Aggregate functions perform a calculation on a set of values in a column and return a single value

Aggregate Functions

AVG(expression)	Returns the average value
COUNT(expression)	Returns the number of rows
COUNT(*)	Returns all rows, even if some columns contain a NULL value
FIRST(expression)	Returns the first value
LAST(expression)	Returns the last value
MAX(expression)	Returns the largest value
MIN(expression)	Returns the smallest value
SUM(expression)	Returns the sum



© Fortinet Inc. All Rights Reserved.

22

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.

DO NOT REPRINT

© FORTINET

Operators

- Reserved word or character used primarily in the WHERE clause to perform various operations
 - Arithmetic operators
 - Comparison operators
 - Logical operators



© Fortinet Inc. All Rights Reserved.

23

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

DO NOT REPRINT**© FORTINET**

Arithmetic Operators

- Perform mathematical operations on two expressions of one or more of the data types of the numeric data type category

Operator	Description
+	Addition: Adds values on either side of the operator
-	Subtraction: Subtracts right hand operand from left hand operand
*	Multiplication: Multiplies values on either side of the operator
/	Division: Divides left hand operand by right hand operand
%	Modulus: Divides left hand operand by right hand operand and returns remainder

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.

DO NOT REPRINT**© FORTINET**

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)

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.

DO NOT REPRINT**© FORTINET**

Logical Operators

- Test for the truth of some condition
 - Return a Boolean data type with a value of TRUE, FALSE, or UNKNOWN

Operator	Description
ALL	TRUE if all of a set of comparisons are TRUE
AND	TRUE if both Boolean expressions are TRUE
ANY	TRUE if any one of a set of comparisons are TRUE
BETWEEN	TRUE if the operand is within a range
EXISTS	TRUE if a subquery contains any rows
IN	TRUE if the operand is equal to one of a list of expressions
LIKE	TRUE if the operand matches a pattern
NOT	Reverses the value of any other Boolean operator
OR	TRUE if either Boolean expression is TRUE
SOME	TRUE if some of a set of comparisons are TRUE

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.

DO NOT REPRINT

© FORTINET

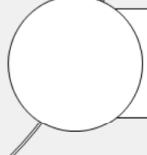
Lesson Progress



Datasets and SQL



SQL Functions and Operators



FortiAnalyzer Functions and Macros

Good job! You now understand SQL functions and operators.

Now, you will learn about FortiAnalyzer functions and macros.

DO NOT REPRINT**© FORTINET**

FortiAnalyzer Functions and Macros

Objectives

- Understand FortiAnalyzer functions
- Understand macros



© Fortinet Inc. All Rights Reserved. 28

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.

DO NOT REPRINT

© FORTINET

root_domain

- `root_domain(hostname)`
 - Retrieves the root domain of the fully qualified domain name (FQDN)

```
SELECT devid, root_domain(hostname) as website FROM
$log WHERE 'user'='USER01' GROUP BY devid, hostname
ORDER BY hostname LIMIT 7
```

devid	website
FGVM010000064692	01gtf.org
FGVM010000064692	024student.com
FGVM010000064692	0306737775.win
FGVM010000064692	0452luntan.com
FGVM010000064692	10yi6bh1fvlx3mt260kix2924l.net
FGVM010000064692	118.171.94.192
FGVM010000064692	132r4zp18tqz1ktk0yg6kj4y2p.org

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.

DO NOT REPRINT

© FORTINET

nullifna

- nullifna (expression)
 - Inverse operation of COALESCE
 - Can be used to filter out values with N/A and n/a from logs
- SQL syntax → SELECT NULLIF(NULLIF(<value>, 'N/A'), 'n/a')

```
SELECT coalesce(nullifna('user'), 'srcip') as user src,
coalesce(nullifna(root_domain(hostname)), 'unknown') as domain FROM
$log WHERE dstport='80' GROUP BY user src, domain ORDER BY
user_src LIMIT 7
```

user_src	domain
user	fgtk77.club
user	itourongbao.com
user	yuamyyimgxh.com.ve
user	144.76.106.114
user	envelopeson.com
user	tritonship.com
user	10yi6bh1fvlx3mt260kix2924l.net

If user is n/a, the source IP is displayed; otherwise, it returns the user name

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.

DO NOT REPRINT**© FORTINET****FortiAnalyzer Functions:** email_domain, email_user

- email_domain: Retrieves anything after the @ symbol in an email address
- email_user: Retrieves anything before the @ symbol in an email address

```
SELECT 'from' as source, email user('from') as e_user,
email domain('from') as e_domain FROM $log LIMIT 5 OFFSET 10
```

Source	e_user	e_domain
user11@example.com	user11	example.com
user12@hostname.com	user12	hostname.com
user13@exampleXYZ.com	user13	exampleXYZ.com
user14@hostnameXYZ.com	user14	hostnameXYZ.com
user15@example.com	user15	example.com

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.

DO NOT REPRINT

© FORTINET

FortiAnalyzer Functions: `from_dtime`, `from_itime`

- `from_dtime(bigint)`: Returns device timestamp without time zone
- `from_itime(bigint)`: Returns FortiAnalyzer timestamp without time zone

```
SELECT itime, from_itime(itime) as faz_local_time, dtime,
       from_dtime(dtime) as dev_local_time FROM $log LIMIT 3
```

itime	faz_local_time	dtime	dev_local_time
1699305243	2023-11-06 13:14:03	1699276391	2023-11-06 13:13:11
1699305243	2023-11-06 13:14:03	1699276391	2023-11-06 13:13:11
1699305243	2023-11-06 13:14:03	1699276399	2023-11-06 13:13:19

`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**.

DO NOT REPRINT**© FORTINET**

Macros

- FortiAnalyzer date and time macros

Macros	PostgreSQL Syntax	Result
\$hour_of_day	to_char(from_itime("itime"), 'HH24:00')	18:00
\$HOUR_OF_DAY	to_char(from_itime("itime"), 'YYYY-MM-DD HH24:00')	2021-01-01 18:00
\$day_of_week	to_char(from_itime("itime"), "'WDAY' D-Dy")	WDAY 2-Mon
\$DAY_OF_WEEK	XXX	XXX
\$day_of_month	to_char(from_itime("itime"), 'DD')	01
\$DAY_OF_MONTH	to_char(from_itime("itime"), 'YYYY-MM-DD')	2021-01-01
\$month_of_year	to_char(from_itime("itime"), 'YYYY-MM')	2021-01
\$MONTH_OF_YEAR	XXX	XXX

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.

DO NOT REPRINT

© FORTINET

Lesson Progress



Datasets and SQL



SQL Functions and Operators



FortiAnalyzer Functions and Macros

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

DO NOT REPRINT**© FORTINET**

FortiAnalyzer Analyst

Introduction and Initial Access

A small red square icon with a white outline of a monitor or analyzer symbol.

FortiAnalyzer 7.4.1

Last Modified: 21 December 2023

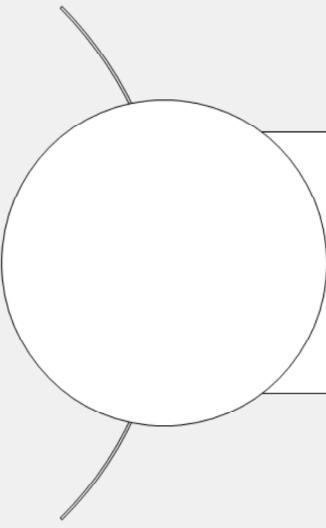
In this lesson, you will learn about the key features and concepts of FortiAnalyzer, and how to initially access FortiAnalyzer.

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

DO NOT REPRINT

© FORTINET

Lesson Progress



Key Features and Concepts

FORTINET
Training Institute

© Fortinet Inc. All Rights Reserved.

2

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

DO NOT REPRINT

© FORTINET

Key Features and Concepts

Objectives

- Describe the purpose of FortiAnalyzer
- Describe FortiAnalyzer operating modes
- Understand basic concepts and features
- Identify the tools you can use to access FortiAnalyzer



© Fortinet Inc. All Rights Reserved.

3

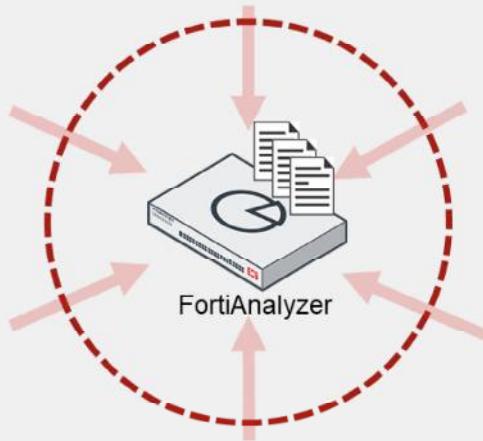
After completing this section, you should be able to achieve the objectives shown on this slide.

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

DO NOT REPRINT
© FORTINET

Centralized Log Repository

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



Supported devices:

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

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

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

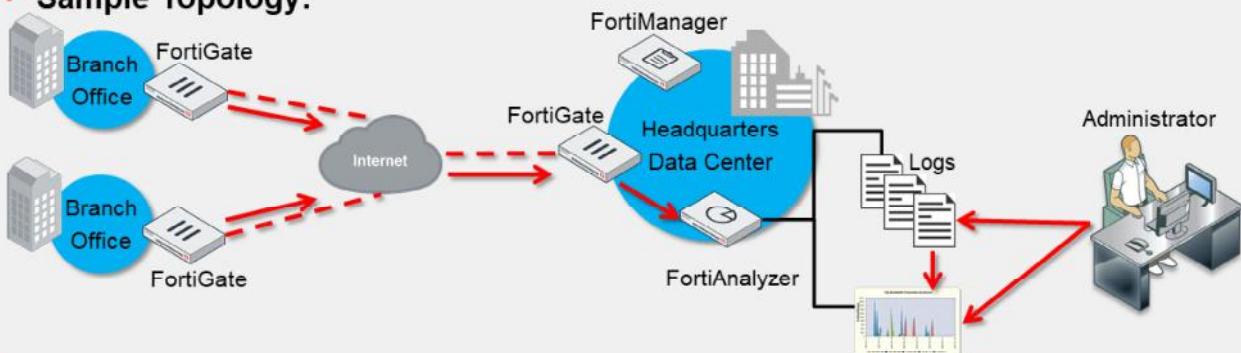
DO NOT REPRINT
© FORTINET

Centralized Log Repository (Contd)

Workflow:

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

- **Sample Topology:**



FORTINET
 Training Institute

© Fortinet Inc. All Rights Reserved.

5

The logging and reporting workflow operates as follows:

1. Registered devices send logs to FortiAnalyzer.
2. FortiAnalyzer collates and stores those logs in a way that is easy to search and run reports.
3. Administrators can connect to FortiAnalyzer using the GUI to view the logs manually, or generate reports to 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.

DO NOT REPRINT**© FORTINET**

Reports, Events, and Content Archiving

- **Reports**

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

- **Events**

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

- **Content archiving**

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



© Fortinet Inc. All Rights Reserved.

6

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.

DO NOT REPRINT
© FORTINET

Database Language Support

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



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

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

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

DO NOT REPRINT
© FORTINET

FortiAnalyzer Operating Modes—Analyzer

Dashboard > System Information

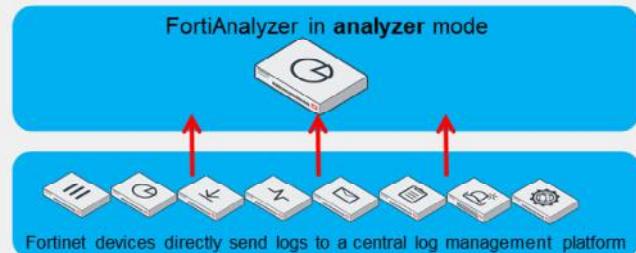
Operation Mode

Analyzer

Collector

Analyzer is the default mode

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



FORTINET
Training Institute

© Fortinet Inc. All Rights Reserved.

8

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

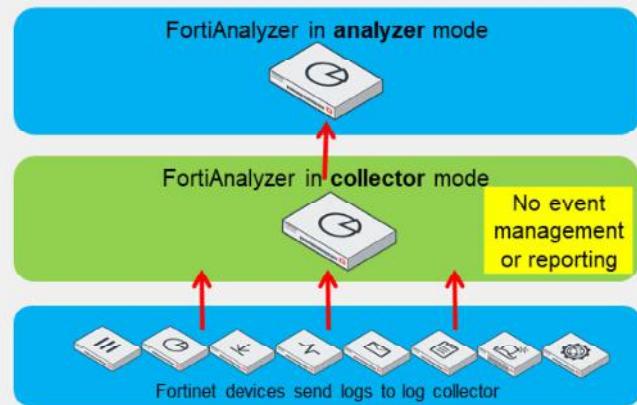
You can change the operating mode in the **System Information** widget on the dashboard.

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.

DO NOT REPRINT
© FORTINET

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



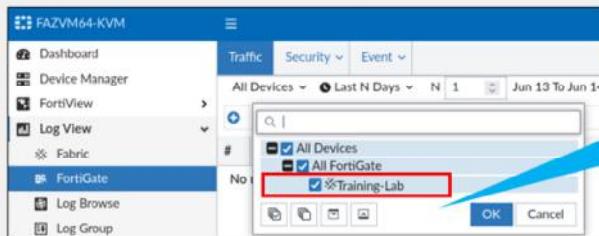
When operating in collector mode, the device collects logs from multiple devices and then forwards those logs, in their original binary format, to another device, such as a FortiAnalyzer operating in analyzer mode. It can also send them to a syslog server or a common event format (CEF) server, depending 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.

DO NOT REPRINT

© FORTINET

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



Training-Lab is the name of the Security Fabric containing two or more FortiGate devices

FORTINET
Training Institute

© Fortinet Inc. All Rights Reserved.

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.

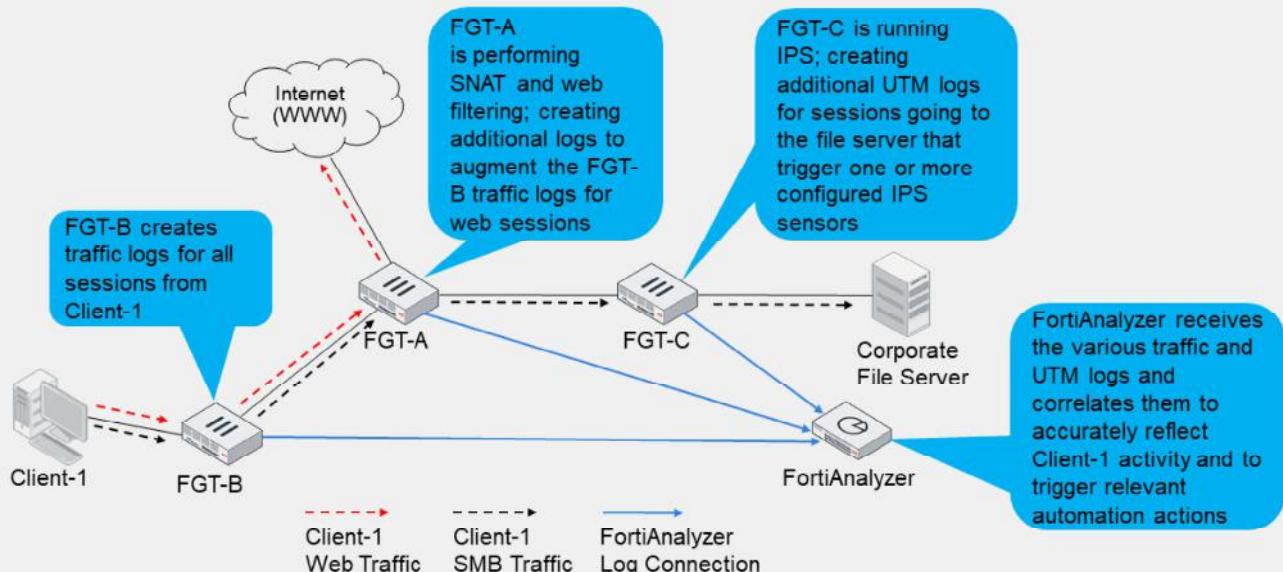
One exception to this behavior is that if the upstream FortiGate performs network address translation (NAT), then another log is generated. The additional log is needed to record NAT details, such as translated ports and addresses.

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.

DO NOT REPRINT
© FORTINET

Security Fabric Logging (Contd)



FORTINET
Training Institute

© Fortinet Inc. All Rights Reserved.

11

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.

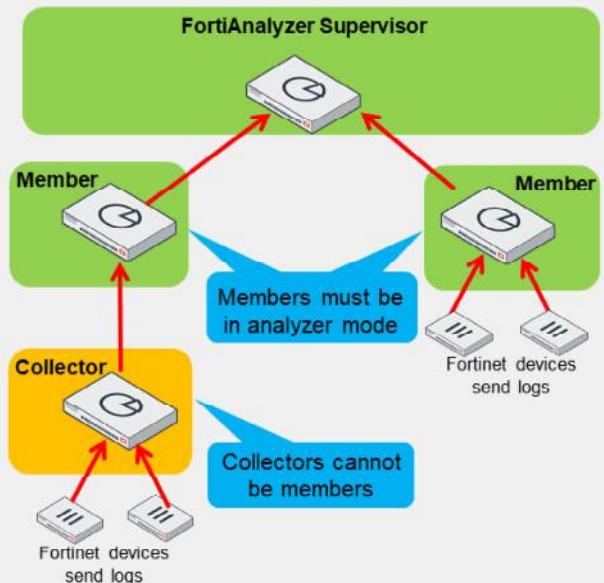
DO NOT REPRINT

© FORTINET

FortiAnalyzer Fabric

- Centralized viewing of devices, incidents, and events across multiple FortiAnalyzers devices
- Ideal for environments with many FortiAnalyzers and high log volume
- Two operation modes:
 - Supervisor—one per fabric; acts as the root
 - Member—sends information to supervisor
- Supervisor and members must be configured in the same time zone
- Supervisor includes only the following modules:
 - Device Manager
 - Log View
 - Incident & Events
 - System Settings
 - Management Extensions

The supervisor can view the information on the members using an API. Members *do not* forward their logs to the supervisor.



FORTINET
Training Institute

© Fortinet Inc. All Rights Reserved.

12

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.

DO NOT REPRINT

© FORTINET

ADOMs

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

ADOMs are not enabled by default

Dashboard > System Information

System Information

Host Name	FAZ
Serial Number	FAZ-VM0000065040
Platform Type	FAZVM64-KVM
HA Status	Standalone
System Time	Mon Oct 23 12:53:08 2023 PDT
Firmware Version	v7.4.1-build2308 230831 (GA)
System Configuration	Last Backup: Sun Oct 22 15:35:29 2023
Current Administrato...	admin / 1 in total
Up Time	21 hours 23 minutes 36 seconds
Administrative Dom...	<input type="checkbox"/>

Operation Mode Analyzer Collector

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

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.

DO NOT REPRINT
© FORTINET

Available Tools to Configure FortiAnalyzer

The screenshot shows two side-by-side interfaces. On the left is the 'FortiAnalyzer GUI' dashboard, which includes links for Device Manager, FortiView, Log View, Fabric View, Incidents & Events, Reports, and System Settings. A note below the dashboard states: 'X = Not available in Collector mode'. On the right is the 'FortiAnalyzer CLI' interface, featuring a 'CLI Console' window titled 'Connected FAZVM64-KVM #'. A yellow callout box over this window contains the text: 'Can use the CLI Console widget on dashboard of GUI and terminal emulation program (for example, PuTTY)'. Below the CLI console is a 'PUTTY Configuration' dialog box showing connection settings for Host Name (IP address) 10.0.1.210, Port 22, and Connection type SSH. A blue callout box points to this dialog with the text: 'Requires a separate Telnet, SSH, or local console connection'. At the bottom left is the Fortinet Training Institute logo, and at the bottom right are copyright and page number information.

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.

DO NOT REPRINT

© FORTINET

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

DO NOT REPRINT

© FORTINET

Lesson Progress



Key Features and Concepts

FORTINET
Training Institute

© Fortinet Inc. All Rights Reserved.

16

Congratulations! You have completed this lesson.

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

DO NOT REPRINT

© FORTINET

Review

- ✓ Describe the purpose of FortiAnalyzer
- ✓ Describe FortiAnalyzer operating modes
- ✓ Understand basic FortiAnalyzer concepts and features
- ✓ Identify the tools you can use to access FortiAnalyzer



© Fortinet Inc. All Rights Reserved.

17

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

DO NOT REPRINT

© FORTINET

FORTINET
Training Institute



FortiAnalyzer Analyst

Logging

 FortiAnalyzer 7.4.1

Last Modified: 21 December 2023

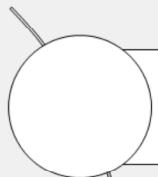
In this lesson, you will learn how to protect, view, and manage logs on FortiAnalyzer.

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.

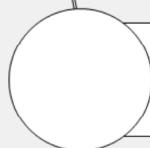
DO NOT REPRINT

© FORTINET

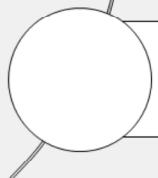
Lesson Overview



Log Overview



Viewing and Searching Logs



Troubleshooting and Managing Logs

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

DO NOT REPRINT

© FORTINET

Log Overview

Objectives

- Describe the purpose of collecting and storing logs
- Describe the log file workflow



© Fortinet Inc. All Rights Reserved.

3

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.

DO NOT REPRINT**© FORTINET**

Purpose of Logs

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



© Fortinet Inc. All Rights Reserved.

4

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.

DO NOT REPRINT**© FORTINET**

Log Storage Regulations

- Regulatory requirements may mandate how logs are managed in an organization
 - Levels and analysis requirements are often defined by legislation
 - Examples: HIPAA, SOX, GDPR
 - Log and store information at the correct level to satisfy regulations
- Logs can provide evidence to deal with offending parties when unauthorized activity is detected
 - Logging data must be able to stand up in court
- Additionally, NIST frameworks and ISO standards can provide guidelines on how to make your network more secure
 - Examples: NIST Cybersecurity Framework, ISO 27001/27002 standards



© Fortinet Inc. All Rights Reserved.

5

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.

DO NOT REPRINT**© FORTINET**

Analyzing the Network

- To effectively analyze the network, you must have a thorough understanding of it
- Every network is unique, as are the organization's requirements; however, there are some common areas to focus on:

Areas to Identify	Examples
Critical infrastructure	Servers, security devices
Types of traffic	Permitted protocols on which devices
Typical usage and peak usage	Established network baselines during all time periods
Sources of traffic bursts	Expected maintenance windows, data backups

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

DO NOT REPRINT**© FORTINET**

Logging Scope

- Depending on the size of the organization, the amount of data can vary significantly
- Balance between reducing security risks and assigning resources, while adhering to regulations
 - If logging is optional for certain flows, make a decision on whether to spend resources on them
 - Too much data is as bad as too little
- Prioritize analysis based on
 - Source and destination
 - Type of traffic
 - Type of security event (for example, web filter or intrusion prevention)
 - Frequency
 - Time



© Fortinet Inc. All Rights Reserved. 7

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.

DO NOT REPRINT**© FORTINET**

Log Types by Device

Device	Log type
Fabric	All
FortiGate	<ul style="list-style-type: none"> 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 Inc. All Rights Reserved.

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.

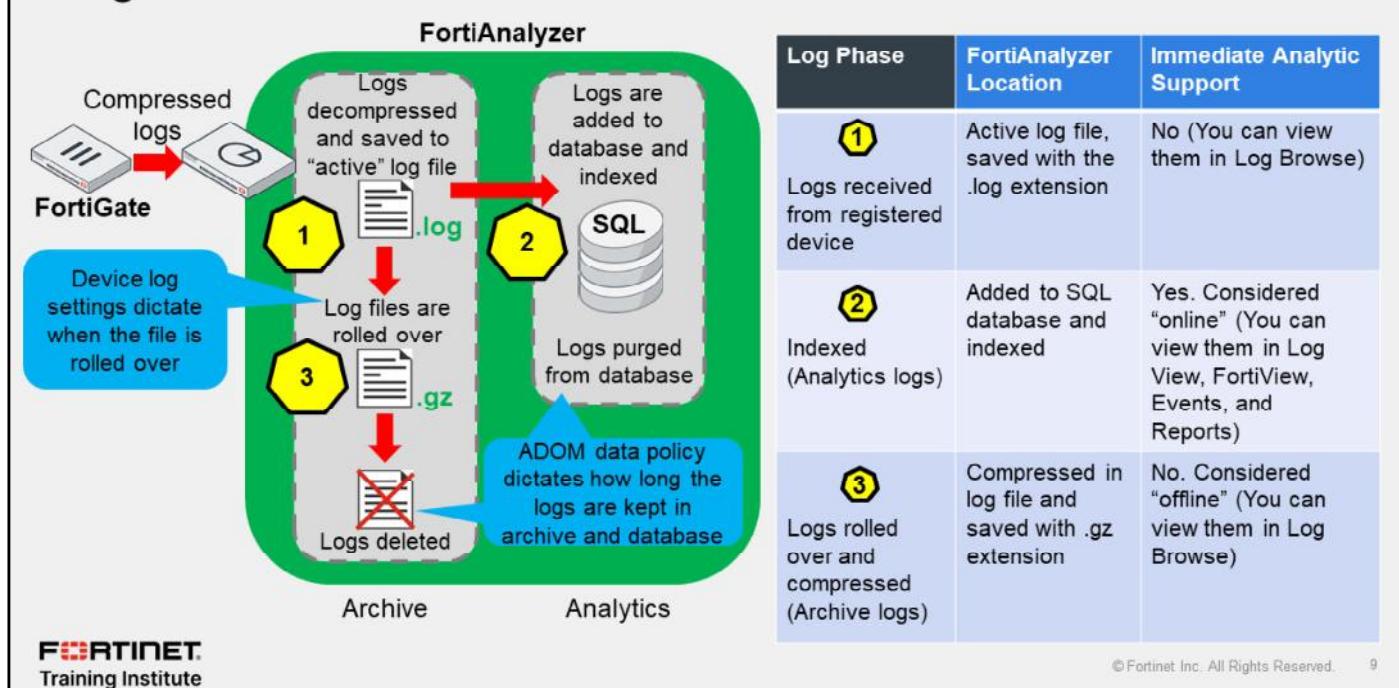
The logs displayed on your FortiAnalyzer are dependent on the device type logging to it and the features enabled. For example, FortiGate devices generate three log types: traffic logs, event logs, and security logs. Each log type has corresponding log subtypes. The logs displayed on your FortiAnalyzer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

DO NOT REPRINT

© FORTINET

Log File Workflow



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**.

DO NOT REPRINT**© FORTINET**

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.

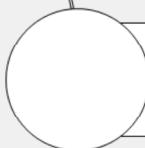
DO NOT REPRINT

© FORTINET

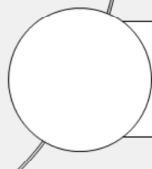
Lesson Overview



Log Overview



Viewing and Searching Logs



Troubleshooting and Managing Logs

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.

DO NOT REPRINT

© FORTINET

Viewing and Searching Logs

Objectives

- View and search for logs in Log View
- View summary data in FortiView
- View dashboards and widgets features
- View information in Fabric View



© Fortinet Inc. All Rights Reserved.

12

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

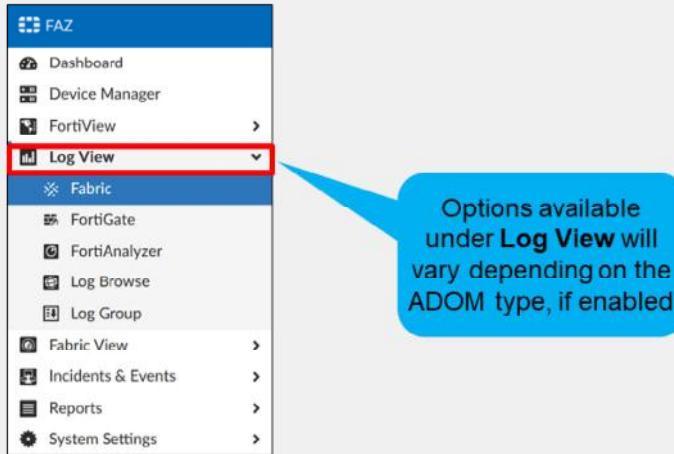
By demonstrating competence in viewing logs, log summaries, and dashboards, you will be able to find and view a variety information related to logs.

DO NOT REPRINT

© FORTINET

Log View

- View all logs received for each ADOM
- You can choose to view only specific devices, Fabric, log browse, log groups



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.

DO NOT REPRINT

© FORTINET

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)

The screenshot shows the FortiGate management interface with the 'Log View' section selected. The 'Traffic' tab is active. The log list displays several entries, with the first entry for 'FortiGate' highlighted by a red box. The columns include #, Policy ID, Date/Time, Device ID, Action, Service, Application, and Sent/Received.

#	Policy ID	Date/Time	Device ID	Action	Service	Application	Sent/Received
1	0	09:58:09	FGVM010000064692	✓accept	other	other	0.0 KB/0.0 KB
2	8	09:58:04	FGVM010000064692	✓accept	HTTP	HTTP	1.4 KB/2.5 KB
3	2	09:58:03	FGVM010000064692	✓accept	HTTP	HTTP	2.8 KB/15.8 KB
4	1	09:58:03	FGVM010000064692	✓accept	HTTP	HTTP	3.8 KB/4.1 KB
5	9	09:58:03	FGVM010000064692	✓accept	HTTP	HTTP	2.7 KB/3.4 KB
6	0	09:58:03	FGVM010000064692	✓accept	HTTP	HTTP	631.0 B/1.5 KB
7	8	09:58:03	FGVM010000064692	✓accept	HTTP	Vimeo_Video.Play	2.3 KB/10.2 KB

FORTINET
Training Institute

© Fortinet Inc. All Rights Reserved.

14

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

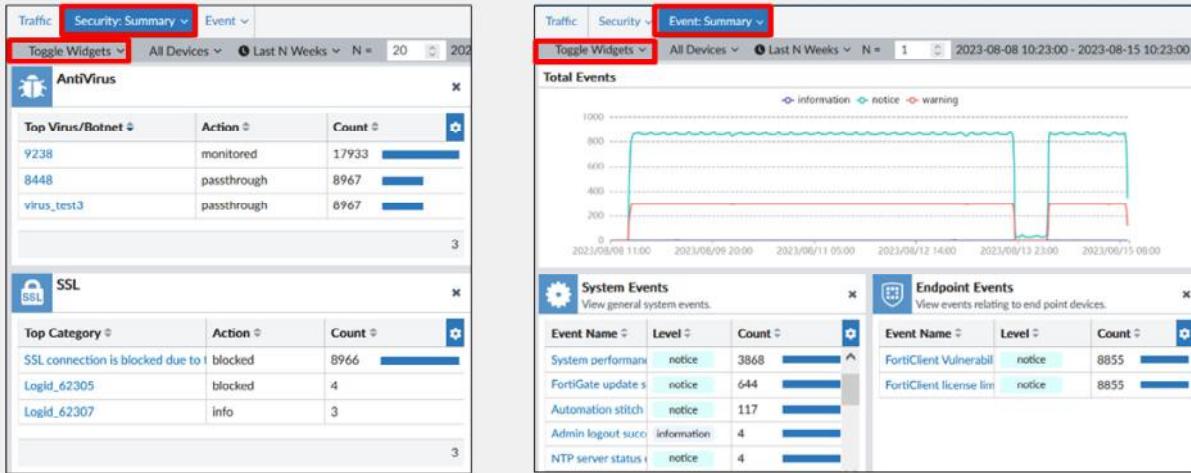
Traffic logs allow you to view traffic traversing the firewalls, including details such as source, destination, service, action (whether the traffic is allowed), and more. Security logs allow you to view logs related to unified threat management (UTM) inspection. Event logs are generally related to the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

DO NOT REPRINT
© FORTINET

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

© Fortinet Inc. All Rights Reserved. 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.

DO NOT REPRINT

© FORTINET

Logging Interface Overview

Set filters

Set device and time frame

Custom view

Column options

Toggle real-time/historical logs

Toggle raw or formatted logs

Log details

Date/Time	Device ID	Action	Source	Destination IP	Service	Application	Sent/Received
11:16:53	FGVM010000064692	✓close	127.0.0.1	127.0.0.1	HTTP	HTTP	399.0 B/670.0 B
11:16:49	FGVM010000077646	✓close	127.0.0.1	127.0.0.1	HTTP	HTTP	399.0 B/670.0 B
11:16:09	FGVM010000077646	✓close	10.0.1.200	96.45.46.46	tcp/853	tcp/853	6.6 KB/21.2 KB
11:16:08	FGVM010000064692	✓accept	10.0.1.10	34.117.65.55	HTTPS	HTTPS	3.0 KB/7.1 KB
11:16:08	FGVM010000064692	✓close	10.200.1.1	96.45.45.45	tcp/853	tcp/853	6.6 KB/22.0 KB
11:16:08	FGVM010000064692	✓close	10.0.1.200	96.45.46.46	tcp/853	tcp/853	6.6 KB/21.2 KB
11:15:08	FGVM010000064692	✓accept	127.0.0.1	127.0.0.1	udp/12121	udp/12121	3.5 KB/0.0 KB
11:15:04	FGVM010000077646	✓accept	127.0.0.1	127.0.0.1	udp/12121	udp/12121	3.4 KB/0.0 KB
11:12:59	FGVM010000077646	✓accept	10.0.1.200	206.91.112.62	NTP	NTP	76.0 B/0.0 KB
11:12:59	FGVM010000077646	✓accept	10.0.1.200	208.91.112.63	NTP	NTP	76.0 B/0.0 KB
11:12:58	FGVM010000064692	✓accept	10.0.1.200	208.91.112.62	NTP	NTP	76.0 B/0.0 KB
11:12:58	FGVM010000064692	✓accept	10.0.1.200	208.91.112.63	NTP	NTP	76.0 B/0.0 KB
11:12:09	FGVM010000077646	server-rst	10.0.1.200	154.52.4.163	tcp/514	tcp/514	3.3 KB/100.0 KB
11:12:08	FGVM010000064692	server-rst	10.0.1.200	154.52.4.163	tcp/514	tcp/514	3.3 KB/100.0 KB
11:12:08	FGVM010000064692	ip-conn	10.0.1.200	154.52.4.163	tcp/514	tcp/514	0 B/0 B
11:12:03	FGVM010000064692	server-rst	10.200.1.1	154.52.4.163	tcp/514	tcp/514	3.3 KB/100.0 KB
11:12:00	FGVM010000064692	✓close	10.0.1.254	10.0.1.210	tcp/514	tcp/514	8.5 KB/12.1 KB
11:12:00	FGVM010000064692	client-rst	10.200.1.1	206.47.184.6	HTTPS	HTTPS	4.6 KB/0.0 KB

Total logs for analytics: 69 days 1 hour.

50 /Page 1 2 3 4 5 > 70 ~0.031 Second

FORTINET
Training Institute

© Fortinet Inc. All Rights Reserved. 16

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.

DO NOT REPRINT

© FORTINET

Search Tips

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



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

Filters	ID	Action
Select or type filter key	010000064692	✓accept
Sub-type		
Level		
Policy ID	=	
Session ID		
Destination NAT IP		
Source NAT IP		

Search or type filters...

History
policyid!="0"
[Clear All Search History]

Filters

- Date/Time
- Device ID
- Firewall Action
- Action

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

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

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

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

DO NOT REPRINT

© FORTINET

Search Tips (Contd)

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

Source	Destination IP	Service	Action
10.0.3.20	162.55.110.19	HTTP	blocked
10.0.3.20			
10.0.3.20			
10.0.3.20			
10.0.3.20			
10.0.3.20			
10.0.3.20			

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

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

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

DO NOT REPRINT

© FORTINET

Example of a Log Search

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

The screenshot shows the FortiAnalyzer Log View interface. At the top, there are tabs for 'Traffic', 'Security: Web Filter', and 'Event'. The 'Security: Web Filter' tab is selected. Below it, there's a 'Custom time period' section set from 'Jun 07 To Jun 08'. The main search bar contains the filter 'srcip = 10.0.3.20 AND Category Description = Malicious Websites'. The results table has columns: #, Date/Time, Device ID, Source, Destination IP, Service, Action, URL, and Category Description. Five log entries are listed, all showing 'blocked' action and 'HTTP' service. The 'Category Description' column for all entries is 'Malicious Websites'. A yellow callout points to the 'Category Description' column with the text 'Malicious websites visited'. Two blue callouts point to the filter bar: one to 'srcip = 10.0.3.20' with the text 'Filters are based on the client's IP as the source, and the category description' and another to 'Category Description = Malicious Websites' with the text 'Fields used in the filter are highlighted'.

#	Date/Time	Device ID	Source	Destination IP	Service	Action	URL	Category Description
1	06-08 10:37	FGVM-0000077646	10.0.3.20	64.70.19.203	HTTP	blocked	http://fffb07fb6990e3b5da86d66d43b4...	Malicious Websites
2	06-08 10:37	FGVM-0000077646	10.0.3.20	155.159.36.59	HTTP	blocked	http://whollyfitinc.com/	Malicious Websites
3	06-08 10:37	FGVM-0000077646	10.0.3.20	176.103.56.36	HTTP	blocked	http://176.103.56.36/	Malicious Websites
4	06-08 10:37	FGVM-0000077646	10.0.3.20	43.163.226.161	HTTP	blocked	http://234w.cc/	Malicious Websites
5	06-08 10:35	FGVM-0000077646	10.0.3.20	50.28.56.190	HTTP	blocked	http://www.xn--l3cgic6bw6ctd.com/	Malicious Websites

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

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

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

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

DO NOT REPRINT

© FORTINET

Saving Frequent Log Searches

- Save frequent searches as custom views for future use

The screenshot shows the FortiAnalyzer Log View interface. On the left, a sidebar lists navigation options: Dashboard, Device Manager, FortiView, Log View (selected), Fabric, FortiGate, FortiAnalyzer, Custom View (1) (highlighted in blue), Log Browse, and Log Group. A callout bubble points to 'Custom View (1)' with the text '3. Saved search is available under Custom View'.

The main pane displays a table titled 'HTTP-based attacks - Last Week'. The filter bar at the top includes 'All Devices', 'Last 7 Days' (set to 'Aug 09 To Aug 16'), and 'FortiGate > Traffic'. A red box highlights the filter 'service="HTTP"'. A callout bubble points to this filter with the text '1. Apply the desired filter'.

A modal window titled 'Create New Custom View' is open. It contains fields: Name ('HTTP-based attacks - Last Week'), Log Type ('Traffic'), Devices ('All Devices'), Time Period ('Last 7 Days'), Search ('app="HTTP"'), and Privacy ('Public'). A callout bubble points to the 'Name' field with the text '2. Save the resulting search for future use'.

At the bottom right of the modal are 'OK' and 'Cancel' buttons. The footer of the slide includes the Fortinet Training Institute logo and copyright information: '© Fortinet Inc. All Rights Reserved. 20'.

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.

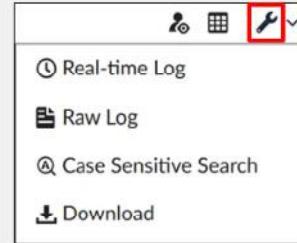
This slide shows a custom view that includes all HTTP traffic logs received over the last seven days.

DO NOT REPRINT

© FORTINET

Tools

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



Formatted

#	Date/Time	Device ID	Action	Source	Destination IP
4	14:59:50	FGVM010000064692	✓accept	10.200.1.1	208.91.112.60
5	14:59:40	FGVM010000064692	✓accept	10.200.1.1	208.91.112.61
6	14:59:30	FGVM010000064692	✓accept	10.0.1.200	208.91.112.60
7	14:59:30	FGVM010000064692	✓accept	10.0.1.200	208.91.112.63

Raw

```
date=2023-08-16 time=14:59:24 id=7268043151217000450 itime=2023-08-16 14:59:25 euid=3 epid=104
dsteuid=3 dstepid=101 type=traffic subtype=local level=notice action=accept policyid=0 sessionid=89571
srcip=10.0.1.200 dstip=208.91.112.60 srcport=123 dstport=123 transp noop duration=193 proto=17
sentbyte=76 rcvbyte=76 sentpkt=1 rcvdpkt=1 logid=0001000014 service=NTP app=NTP appcat=unscanned
srcintfrole=undefined dstintfrole=undefined eventtime=1692223164328415424 sccountry=Reserved
dstcountry=Canada srcintf=root dstintf=port1 tz=-0700 devid=FGVM010000077646 vd=root
dtime=2023-08-16 14:59:24 itime_t=1692223165
```

© Fortinet Inc. All Rights Reserved. 21

FORTINET
Training Institute

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.

DO NOT REPRINT

© FORTINET

FortiAnalyzer Application Logs

- FortiAnalyzer application logs:
 - Include audit logs for local, SIEM, and SOAR applications (playbooks)
 - Each ADOM has its own audit logs

Log View > FortiAnalyzer > Application

#	Date/Time	Device ID	User	Sub Type	Event Type	Log ID	Level	Message	Status	Incident ID
1	09:53:42	FAZ-VM0000065040	admin	playbook	cfg-change	110021	notice	Playbook 'New Playbook created from scratch - 2'	success	
2	09:51:13	FAZ-VM0000065040	admin	playbook	run-stat	110263	notice	Task 'Create_Incident' executed successfully.	success	
3	09:51:13	FAZ-VM0000065040		incident	config	100001	notice	Incident IN00000001 is created.	success	IN00000001
4	09:51:11	FAZ-VM0000065040	admin	playbook	trigger	110020	notice	Playbook 'New Playbook created from scratch - 2'	success	
5	09:50:13	FAZ-VM0000065040	admin	playbook	cfg-change	110021	notice	Playbook 'New Playbook created from scratch - 2'	success	
6	09:46:48	FAZ-VM0000065040	system	system	perf-stats	220004	notice	Adom ADOM1 performance status: lograte=0/sec		
7	08:46:48	FAZ-VM0000065040	system	system	perf-stats	220004	notice	Adom ADOM1 performance status: lograte=0/sec		

FORTINET
Training Institute

© Fortinet Inc. All Rights Reserved. 22

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.

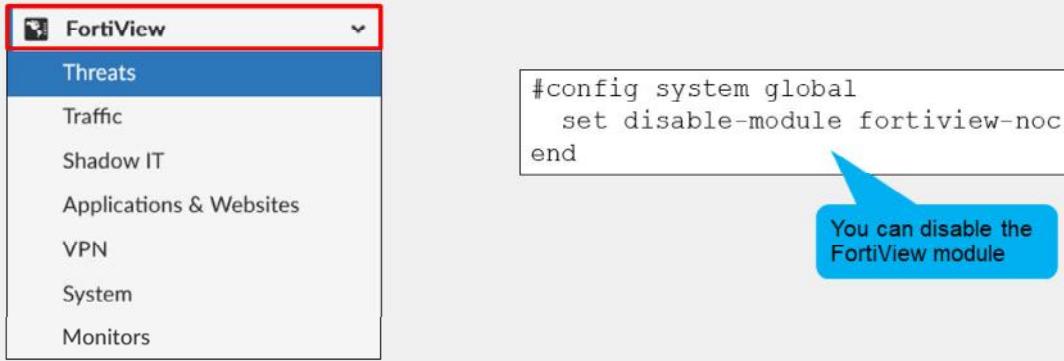
On this slide, you can see several logs that show that multiple automation tasks have succeeded. You also see the log rates of ADOM1.

DO NOT REPRINT

© FORTINET

FortiView

- A comprehensive monitoring system that displays real-time and historical data
- Each ADOM has its own data analysis in FortiView
- Displays data from analytics logs, but not in archive
- Offers multiple dashboards to provide summarized views of the network



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.

DO NOT REPRINT

© FORTINET

FortiView Dashboards

- Integrates real-time and historical data into summary views
- Includes multiple predefined dashboards:
 - Threats
 - Traffic
 - Shadow IT
 - Application & Websites
 - VPN
 - System



FORTINET
Training Institute

© Fortinet Inc. All Rights Reserved. 24

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.

DO NOT REPRINT

© FORTINET

FortiView Monitors

- Designed for NOC/SOC with big monitors displaying its dashboards
- You can create new or edit predefined layouts
- Can also add, remove, or customize widgets

The screenshot shows a dashboard titled 'Threats' with several widgets. One widget displays a world map with threat density. Another shows 'Top Virus Incidents over Time' with a red box highlighting '2001-12-01 W32/Anset.B@mm'. A third widget shows 'Top Threat Destinations' with a map of Europe and Africa. A fourth widget is a bar chart for 'Top Threats' with categories like 'denial of service', 'malware', 'port attack', and 'DoS'. The top navigation bar includes tabs for Threats, Traffic, Applications & Websites, Compromised Hosts, Incidents & Events, and Secure SD-WAN Monitor. There are also buttons for '+ Add Widget', 'Edit Layout', 'All Devices', and time filters ('Last 1 Hour - 09:03 - 10:03'). A 'Dark Mode' switch is on the right.

FORTINET
Training Institute

© Fortinet Inc. All Rights Reserved.

25

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*.

DO NOT REPRINT

© FORTINET

Example of Using Information on a Widget

- Find threats details on the **Top Threats** dashboard
- Double-click any entry to drill down for more details

This screenshot shows the FortiAnalyzer Top Threats dashboard. A specific IPS event is highlighted with a red border. A callout bubble points to this entry with the text: "This IPS event has a very high threat score. Double-click to investigate". Below the main dashboard, a detailed view of the selected threat is shown in a new window. This detailed view includes a summary table and a timeline chart. A second callout bubble points to the summary table with the text: "Threats were blocked, but the entry should be thoroughly investigated".

Threat	Threat Type	CVE ID	Threat Score	Threat Level	Incidents
PHPBB.Viewtopic.Highlight.Remote.Code.Execution	IPS		840	High	28
Maze.PHP.Chat.Multiple.File.Inclusion	IPS	CVE-2007-2931	360	High	12
RipeCMS.Parameter.Level.File.Inclusion	IPS	CVE-2007-3584	240	High	8
Ajax.File.Browser.approot.Parameter.File.Inclusion	IPS	CVE-2007-4921	180	High	6

Summary:

- Threat: PHPBB.Viewtopic.Highlight.Remote.Code.Execution
- Threat Type: IPS
- CVE ID:
- Threat Score: Blocked/ Allowed: 840
- Threat Level: High
- Incidents Blocked/ Allowed: 28

Source: 10.200.1.254

Device Type: port1

Threat Score: 840

Bytes (Sent/Received): 22.6 KB/32.5 KB

Incidents: 28

© Fortinet Inc. All Rights Reserved. 26

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.

DO NOT REPRINT

© FORTINET

Example of Using Information on a Widget (Contd)

- Investigate the top sources displayed on the **Traffic** dashboard



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

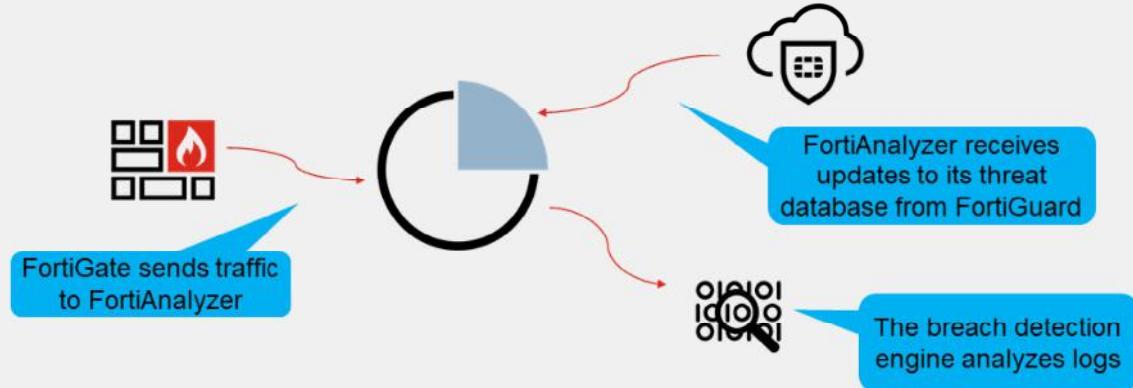
For example, on this slide, the **Top Sources** widget was enlarged and customized to display the information in a table format and with full view. The top source on the list is a host accessing the network through SSL VPN, with a very high threat score. Double-clicking that host entry will provide more 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.

DO NOT REPRINT

© FORTINET

Indicators of Compromise (Compromised Hosts)

- Indicators of compromise (IOC) engine detects end users with suspicious web usage compromises by checking new and historical logs against IOC signatures
- Uses today's FortiGuard threat intelligence to provide visibility of today's threats
- Requires a FortiGuard subscription



FORTINET
Training Institute

© Fortinet Inc. All Rights Reserved. 28

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.

DO NOT REPRINT

© FORTINET

IOC/Compromised Host Example

The screenshot shows the FortiView interface for 'Compromised Hosts'. A single entry is selected for the IP 10.0.3.20, which is marked as 'Infected' with a count of 3 threats. A red box highlights the 'Acknowledge' column, which contains the word 'Ack' with a blue progress bar. A red arrow points from this box to a callout bubble stating: 'A real breach was detected, with three threat types and this entry hasn't been acknowledged yet'.

Below the main table, a detailed view of the threat entry is shown, with another red box highlighting the 'Blocklist' filter button. A red arrow points from this button to a second callout bubble stating: 'Displaying blocklist detection method used by the IOC'.

#	Source (User/IP)	Last Detected	Host Name	OS	Verdict	# of Threats	Acknowledge	Device Name	Device ID
1	10.0.3.20(10.0.3.20)	2023-08-18 13:19	10.0.3.20		Infected	3	<div style="width: 50%;">Ack</div>	ISFW	FCVM010000077646

Below the main table, a detailed view of the threat entry is shown:

#	Detect Pattern	Threat Type	Threat Name	Category	Detect Method	# of Events	Log Type	Security Actions	Scan Time
16	xn--l0gic0dwebfctd.com	Malware	CnC	Spyware and Malware	infected-domain	1	webfilter	Details	2023-08-18 12:54:33
17	zlnomp3.com	Malware	CnC	Pornography	infected-domain	1	webfilter	Details	2023-08-18 12:53:53
18	208.100.26.245	Malware	CnC	Spyware and Malware	infected-ip	1	webfilter	Details	2023-08-18 13:09:43
19	52.86.6.113:80	Malware	CnC	Spyware and Malware	infected-ip	1	webfilter	Details	2023-08-18 13:22:53
20	gainvoice.net	Malware	CnC	Spyware and Malware	infected-domain	1	webfilter	Details	2023-08-18 13:09:43
21	208.91.196.145	PUP	SpywareCnC		infected-ip	1	traffic	Details	2023-08-18 13:14:33
22	5.79.71.205	Malware	CnC	Spyware and Malware	infected-ip	1	traffic	Details	2023-08-18 13:18:49
23	85.17.31.122	Malware	CnC	Spyware and Malware	infected-ip	1	traffic	Details	2023-08-18 12:53:53
24	91.195.240.123:80	Malware	CnC	Spyware and Malware	infected-ip	1	traffic	Details	2023-08-18 13:23:53
25	56834764387462384.org	Malware	Sinkhole	Not Rated	infected-domain	1	webfilter	Details	2023-08-18 13:08:03
26	corolbugan.com	Malware	Sinkhole	Phishing	infected-domain	1	webfilter	Details	2023-08-18 12:53:53

FORTINET
Training Institute

© Fortinet Inc. All Rights Reserved. 29

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**.

DO NOT REPRINT

© FORTINET

Retrieving Archived Logs Through Log Fetching

- Retrieve archive logs from another FortiAnalyzer and then run queries or reports on those archived logs
 - Can select devices and time period to be indexed
 - Customize log retention settings for generating reports on older logs
 - Avoid log duplication
- FortiAnalyzer fetch client queries the remote FortiAnalyzer fetch server to retrieve data

System Settings > Advanced > Log Fetch

1. On the fetch client, create a profile for the fetch server:

Create New Profile	
Name	Fetch-Profile
Server IP	10.0.1.210
User	admin
Password	*****

Must have Super_User or Standard_User profile

2. On the fetch client, send the fetch request:

<input type="button" value="Create New"/>	<input type="button" value="Edit"/>	<input type="button" value="Delete"/>	<input style="background-color: #0072bc; color: white; border: none; padding: 2px 10px; border-radius: 5px; font-weight: bold; font-size: 10px; margin-right: 10px;" type="button" value="Request Fetch"/>
<input checked="" type="checkbox"/> Name	Server IP		
Fetch-Profile 10.0.1.210			

Can specify which source and target ADOMs, devices, dates, and filters

3. On the fetch server review, approve, or reject request:

Request Time	Host/Server IP	User	Status	Action
Received Request (1)				
15:20:29	FAZ2(FAZ-VMTM23008175)	admin	Waiting for approval	<input style="background-color: #0072bc; color: white; border: none; padding: 2px 10px; border-radius: 5px; font-weight: bold; font-size: 10px;" type="button" value="Review"/>

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.

DO NOT REPRINT**© FORTINET**

Considerations for Using Log Fetching

- Client and server should run the same firmware version to ensure all log fields match
- Select a source and destination ADOM of the same type
- The destination ADOM must have enough space allocated for the incoming logs
- Data policy on the client must retain logs of the specified time period
 - Logs outside the data policy constraints are deleted
- You must add the devices to Device Manager before you can see their logs in the client
 - You can do the log fetching before adding the devices, but you won't be able to see the logs
- During the request, you can choose filters to include:
 - Logs from specific devices
 - Logs of specific types and values
 - Logs from a specific time frame

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

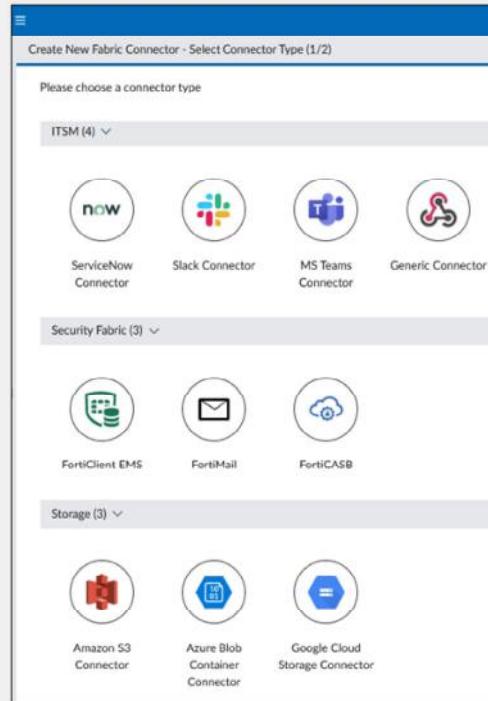
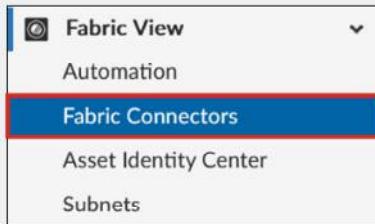
- The client and server devices should be running the same firmware to ensure all log fields match.
- The source and destination ADOMs must be of the same type.
- Ensure the destination ADOM has enough allocated space for the incoming logs.
- Verify the data policy on the client will not delete the incoming 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.

DO NOT REPRINT

© FORTINET

Fabric View

- **Fabric View** module enables:
 - The creation of fabric connectors
 - The creation of subnets and subnet groups
 - Viewing the list of endpoints
- You can create the following connectors:
 - ITSM
 - Storage
 - Security Fabric



FORTINET
Training Institute

© Fortinet Inc. All Rights Reserved. 32

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.

DO NOT REPRINT

© FORTINET

Fabric View—Asset Center

- The **Asset** pane displays endpoint and user information, grouped by endpoint
 - Useful to verify compliance, and for investigation during the incident response process

Fabric View > Asset Identity List > Asset

Note: End-user information is limited if FortiClient EMS is not installed

This Windows PC has 4 critical vulnerabilities, 54 high, 19 medium, and 2 low. Hover your mouse over each one to see the details.

Click the user to see its group membership and the endpoints where they have logged on

Click Details to see the list of software installed on that client, their install date, version, and installation path

FORTINET
Training Institute

© Fortinet Inc. All Rights Reserved. 33

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.

DO NOT REPRINT

© FORTINET

Fabric View—Identity Center

- The **Identity Center** pane displays endpoint and user information, grouped by user
 - Useful to verify compliance, and for investigation during the incident response process

Fabric View > Asset Identity List > Identity

End-user information is limited if FortiClient EMS is not installed

User Name	User Group	Endpoints	Source	VPN IP	First Seen	Last Update
katebrown		DESKTOP-ENGG-02	ISFW_BLDG-E/ENGG_VLAN		2020-06-02 13:13:18	2022-08-01 17:07:07
lwalter		DESKTOP-FIN-01.corp.	ISFW_BLDG-F/VLAN_FIN		2020-08-03 17:31:29	2022-08-01 17:02:02
jtrue		DESKTOP-SALE-01	ISFW_BLDG-B/VLAN_SALES		2020-06-02 19:07:04	2022-07-30 15:54:46
DESKTOP-SALE-01	00:50:56:a6:ed:bc	10.88.130.131	Windows	ISFW_BLDG-B/VLAN_SALES	jtrue(1232)	2 13 1 1 1 1 1

Click the endpoint to see its MAC, IP, OS, and vulnerabilities

This Windows PC has 2 critical vulnerabilities, 13 high, 3 medium, and 1 low

If available, clicking the last update opens the corresponding log in a new Log View window

FORTINET
Training Institute

© Fortinet Inc. All Rights Reserved. 34

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.

DO NOT REPRINT

© FORTINET

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

DO NOT REPRINT

© FORTINET

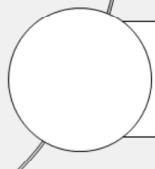
Lesson Overview



Log Overview



Viewing and Searching Logs



Troubleshooting and Managing Logs

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

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

DO NOT REPRINT

© FORTINET

Troubleshooting and Managing Logs

Objectives

- Gather log volume statistics



© Fortinet Inc. All Rights Reserved. 37

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.

DO NOT REPRINT
© FORTINET

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?	# diagnose fortilogd lograte
What are the log receive rate totals?	# diagnose fortilogd lograte-total
What is the device log rate?	# diagnose fortilogd lograte-device
What is the log rate for each log type?	# 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 Inc. All Rights Reserved. 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.

DO NOT REPRINT
© FORTINET

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

© Fortinet Inc. All Rights Reserved. 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).

DO NOT REPRINT

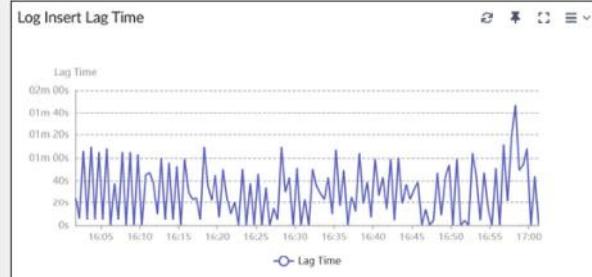
© FORTINET

Insert Rate vs. Receive Rate and Log Insert Lag

- **Insert Rate vs. Receive Rate**

- Insert Rate = SQL Insertion Rate
 - Handled by sqlplugind
- Receive Rate = Raw Receiving Rate
 - Handled by fortilogd

Dashboard > Widgets



- **Log Insert Lag Time**

- Amount of time between log received and log inserted in the database

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.

DO NOT REPRINT

© FORTINET

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

DO NOT REPRINT

© FORTINET

Lesson Overview



Log Overview



Viewing and Searching Logs



Troubleshooting and Managing Logs

Congratulations! You have completed this lesson.

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

DO NOT REPRINT

© FORTINET

Review

- ✓ Describe the purpose of collecting and storing logs
- ✓ Describe the log file workflow
- ✓ View and search for logs in Log View
- ✓ View summary data in FortiView
- ✓ View dashboards and widgets features
- ✓ Gather log volume statistics



© Fortinet Inc. All Rights Reserved. 43

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.

DO NOT REPRINT

© FORTINET

FORTINET
Training Institute



FortiAnalyzer Analyst

Incidents and Events

 FortiAnalyzer 7.4.1

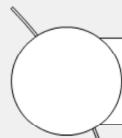
Last Modified: 21 December 2023

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

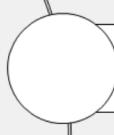
DO NOT REPRINT

© FORTINET

Lesson Overview



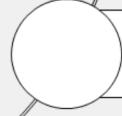
SOC Overview



Managing Events



Managing Incidents



Threat Hunting and Outbreak Alerts

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

DO NOT REPRINT

© FORTINET

SOC Overview

Objectives

- Understand FortiAnalyzer SOC features
- Summarize SOC dashboards information
- Understand management extension applications

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.

DO NOT REPRINT**© FORTINET**

SOC Features



Incident Management

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



Automation

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



Analytics

- SOC analytics

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.

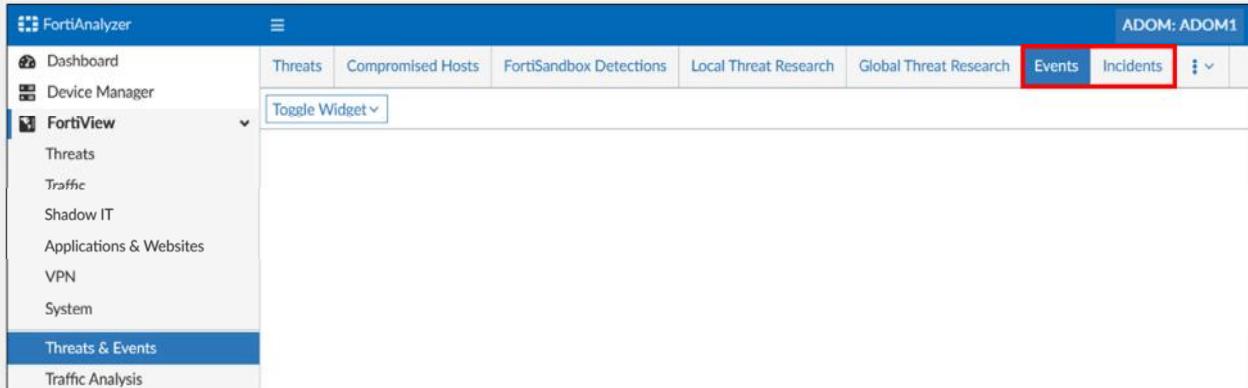
FortiAnalyzer provides a more complete solution for modern SOC analysts that include:

- 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.

DO NOT REPRINT
© FORTINET

FortiView—SOC Dashboards

- Separate **Incidents** and **Events** dashboards
- Each dashboard provides a general overview and statistics



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.

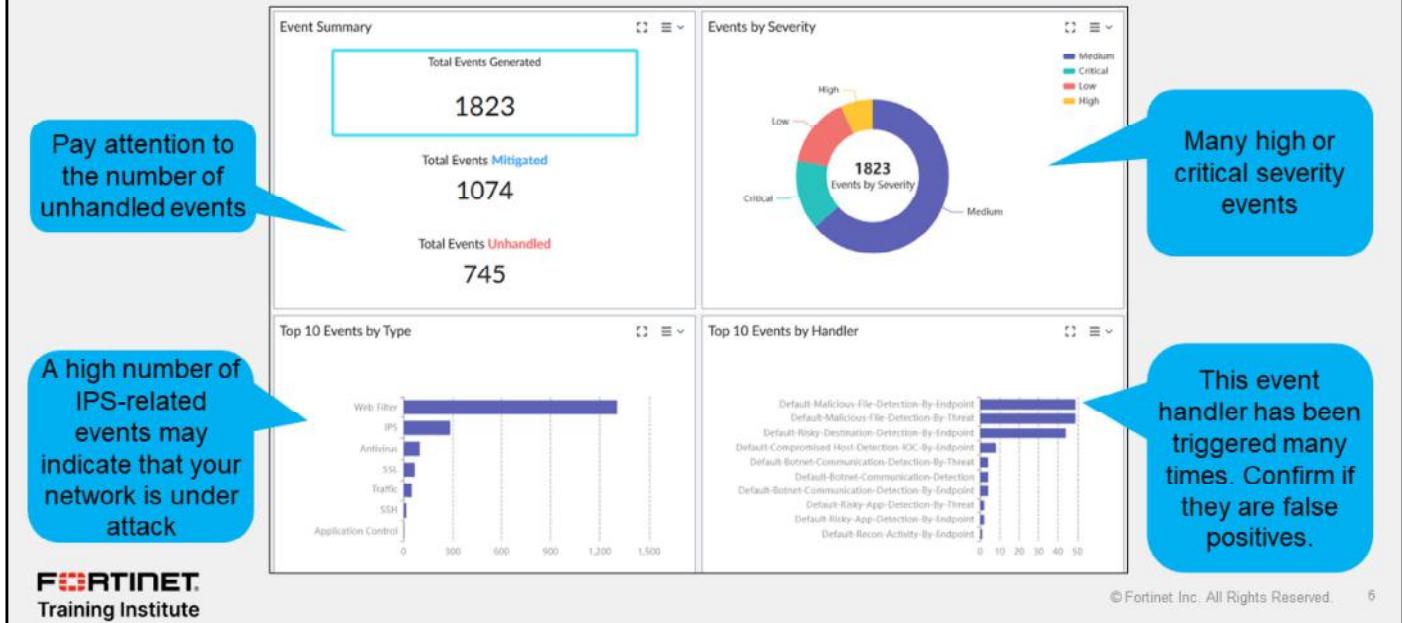
These dashboards are read-only and not customizable. The information they display is updated automatically based on other actions that occur in the background, such as when new events are generated.

DO NOT REPRINT

© FORTINET

Events Dashboard

- This dashboard helps track all events, their status, sources, and severity



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.

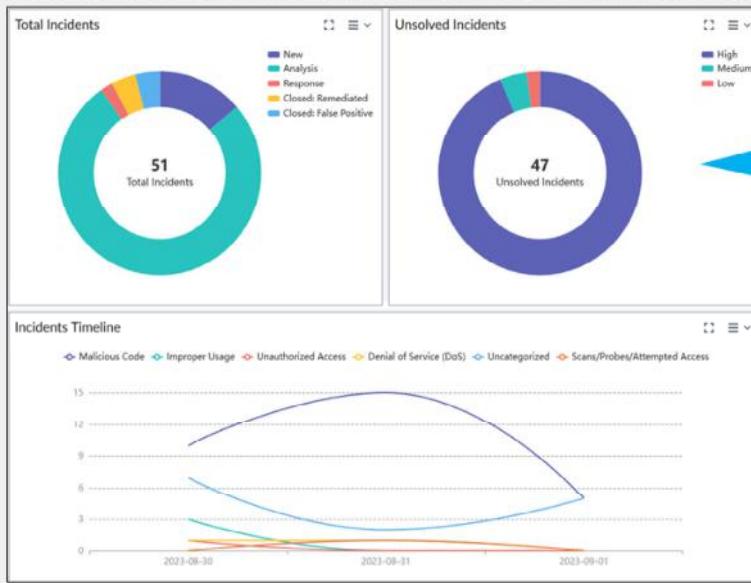
For example, this slide shows that approximately one-third of the events are classified as critical, and there are 745 unhandled events.

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

DO NOT REPRINT
© FORTINET

Incidents Dashboard

- This dashboard tracks all incidents that need to be solved, and their severity



Many incidents are unresolved, and almost all are high severity

FORTINET
Training Institute

© Fortinet Inc. All Rights Reserved. 7

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.

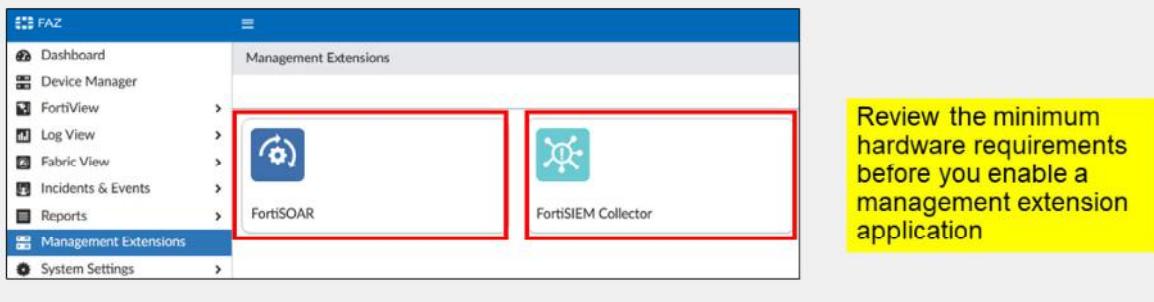
To start analyzing and eventually solving incidents, you must use the **Incidents** section under **Incidents & Events**. This is covered later in this lesson.

DO NOT REPRINT

© FORTINET

Management Extensions

- Allow you to enable licensed applications and run them on FortiAnalyzer
- Full-fledged instances of a product in the form of a docker container
- Two management extension applications (MEAs) available on FortiAnalyzer:
 - FortiSOAR: Allows you to manage your security operations using FortiAnalyzer and without the need for a separate FortiSOAR instance
 - FortiSIEM: Alleviates the need for a separate FortiSIEM collector node (VM or device)



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*.

DO NOT REPRINT

© FORTINET

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

DO NOT REPRINT

© FORTINET

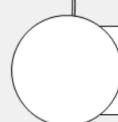
Lesson Overview



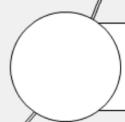
SOC Overview



Managing Events



Managing Incidents



Threat Hunting and Outbreak Alerts

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

Now, you will learn how to manage events.

DO NOT REPRINT

© FORTINET

Managing Events

Objectives

- Understand how events are generated
- Manage event handlers
- Manage events

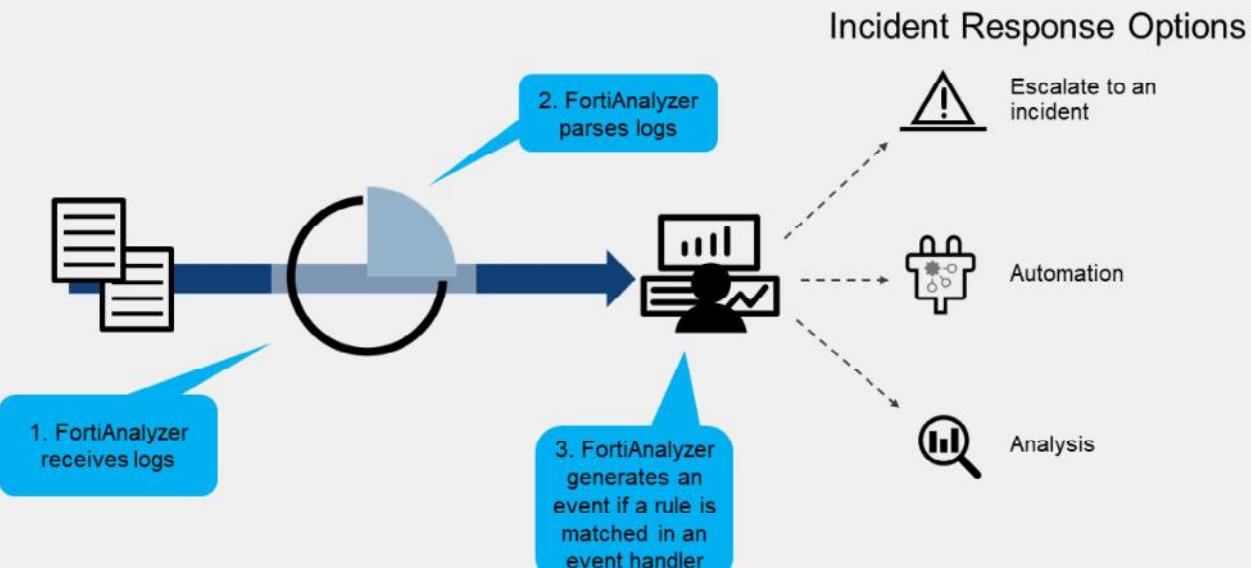
After completing this section, you should be able to achieve the objectives shown on this slide.

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

DO NOT REPRINT

© FORTINET

How Are Events Generated?



FORTINET
Training Institute

© Fortinet Inc. All Rights Reserved. 12

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.

DO NOT REPRINT

© FORTINET

Managing Event Handlers

- Event handlers look for specific conditions in the logs
- FortiAnalyzer comes with many predefined event handlers
- Enable or disable them as needed
- Disabled handlers do not generate events

Incidents & Events > Handlers

Status	Name	Rules	Events	MITRE Tech ID
<input checked="" type="checkbox"/>	Default-Web-Server-URL-Scanning-Detected	Rule-1 Web request to malicious destination detected Rule-2 Web request to malicious destination blocked: Rule-3 DNS request to malicious destination detected Rule-4 DNS request to malicious destination blocked: +11	33	T1112, T1595.003
<input checked="" type="checkbox"/>	Default-Risky-Destination-Detection-By-Threat	Rule-1 Web request to malicious destination blocked: Rule-2 Web request to malicious destination detected Rule-3 Web request to suspicious destination detected Rule-4 DNS request to malicious destination detected +10	7	T1102, T1071.001, T1071.004, T1021.001
<input checked="" type="checkbox"/>	Default-Risky-Destination-Detection-By-Endpoint			T1102, T1071.001, T1071.004, T1021.001

Disabled handlers don't generate events

Enable only the event handlers you need

This handler has 15 rules and has generated 33 events

FORTINET
Training Institute

© Fortinet Inc. All Rights Reserved. 13

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.

DO NOT REPRINT
© FORTINET

Event Handlers—Configuration

- The configuration for each event handler can include:
 - MITRE attributes
 - Data selectors (exclusion filters)
 - Automation stitches
 - Notifications
 - Rules
- Rules are granular conditions
 - Event handler can have one or more rules
 - Basic event handlers use the OR logic
 - Correlation event handlers have many operator logic options

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.

DO NOT REPRINT

© FORTINET

Event Handlers—Rule Configuration

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

The screenshot shows the configuration interface for a rule named "Rule 1 - Emergency Priority". The rule is set to log to a FortiGate device using the "Traffic Log (traffic)" type and "Any" subtype. It is grouped by "Application Name (app)". The "Logs match" section indicates "All Any of the following conditions". A table below defines a single condition: "Level (pri)" is compared to "Emergency" using the "Equal To" criteria. There is also a "Generic Text Filter" section.

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

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.

DO NOT REPRINT
© FORTINET

Event Handlers—Rule Configuration (Contd)

- Aggregation settings can help reduce the number of generated events
 - **Aggregation Expression** is the minimum threshold matching logs
 - **Aggregation Duration** is the minimum threshold in minutes

The screenshot shows the 'Event Handler' configuration window. Under the 'Aggregation' tab, the 'Aggregation Expression' is set to 'COUNT >= 1'. The 'Aggregation Duration' is set to '30'. Under 'Event Type Override', there is a note: 'Specify an event type, or leave blank to use default value'. Under 'Event Message', it says 'Group by key-value pair(s) by default, or customize it (detail in info tip)'. Under 'Event Status', there is a dropdown menu with 'Click to select' and a checked checkbox 'Allow FortiAnalyzer to choose'. Under 'Event Severity', it is set to 'Medium'. Under 'Tags', there is a field 'Press enter to add tags'. Under 'Indicators', there is a table:

Log Field	Indicator Type	Count	Action
			+

Under 'Additional Info', there are two radio buttons: 'Use system default' (selected) and 'Use custom message'.

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.

DO NOT REPRINT

© FORTINET

Event Handlers—Data Selectors

- Data selectors help narrow down events generated by devices, subnets, and filters:
 - Devices (by name)
 - Subnets (created in Fabric View)
 - Filters (OR logic)
- Filters are granular conditions within data selectors:
 - Log device type
 - Log type/subtype
 - Matching logic (AND/OR logic)
 - Generic text filter (for more precise filtering)

The fields available in the filters depend on the device type selected

The screenshot shows the FortiAnalyzer configuration interface for creating a data selector named 'Remote-FortiGate'. The 'Devices' section lists 'All Devices' and 'Specify' (selected), with 'Remote-FortiGate' listed under 'Specify'. The 'Subnets' section lists 'All Subnets' and 'Specify'. The 'Filters' section is expanded, showing 'Any of the following conditions' with a single condition: 'Traffic to Sample IP'. A red box highlights the 'Filters' section, and a red arrow points to the detailed configuration window below.

Name	Traffic to Sample IP
Log Device Type	FortiGate
Log Type	Traffic Log (traffic)
Log Subtype	Any
Logs match	<input type="radio"/> All <input checked="" type="radio"/> Any of the following conditions
Log Field	Destination IP (dstip)
Match Criteria	Equal To
Value	10.0.0.254
Generic Text Filter <input type="text"/> 0/1023	

Training Institute

© Fortinet Inc. All Rights Reserved.

17

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.

DO NOT REPRINT

© FORTINET

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)	
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

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.

DO NOT REPRINT

© FORTINET

Event Handlers—Generic Text Filters

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

Operator	Meaning
<code>==</code>	Equal (Exact match)
<code>!=</code>	Not equal (Not matching)
<code><</code>	Smaller than
<code><=</code>	Smaller than or equal
<code>></code>	Greater than
<code>>=</code>	Greater than or equal
<code>~</code>	Contained (Included somewhere in the string)
<code>!~</code>	Not contained (Not included)

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

Generic text format:

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

Examples:

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

These syntax examples
are available in the GUI

Tip: Search among the logs for the one you want to generate an event and, from its raw view, copy the strings you want to match

When configuring an event handler, the use of generic text filters allows more precise and flexible control over which logs trigger an event. These filters use operators based on regex 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.

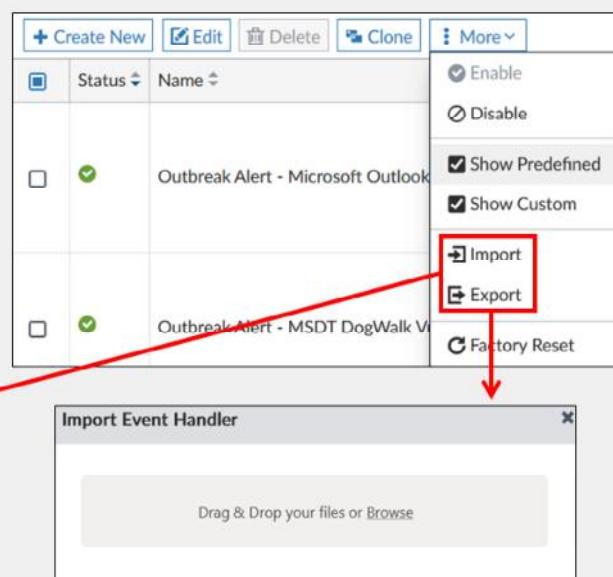
Keep in mind that you must use the escape character “\” if you need to include a reserved character in your filter.

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.

DO NOT REPRINT
© FORTINET

Exporting and Importing Event Handlers

- Event handlers are configured per ADOM
- To reuse existing event handlers, export them from one ADOM and import them into a different one



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.

DO NOT REPRINT
© FORTINET

Managing Events

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

Incidents & Events > Event Monitor

Event	Event Status	Event Type	Count	Severity	First Occurrence	Last Update	Handler
66.199.231.77 (1)	Mitigated	Web Filter	1	Medium	21 hours ago	21 hours ago	Default-Risky-Destination-Detection-By-Threat
66.45.245.150 (2)	Unhandled	Traffic	2	Critical	a day ago	a day ago	Default-Compromised-Host-Detection-IOC-By-Threat
Traffic to C&C from 10.0.1.200 detected	Unhandled	Traffic	1	Critical	2023-09-05 19:05:42	2023-09-05 19:06:05	Default-Compromised-Host-Detection-IOC-By-Threat

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

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

This is the event handler that generated this event
If unexpected events are being created you may need to check if the handler is correctly configured

Search or type filters...

#	Date/Time	Device ID	Action	Source	Destination IP	Service	Application	Sent/Received	Security Event List
1	09-05 19:05	FGVM010000064692	✓ close	10.0.1.200	66.45.245.150	HTTP	HTTP.BROWSER	464.0 B / 1.1 KB	APP 1

FORTINET.
Training Institute

© Fortinet Inc. All Rights Reserved. 21

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.

DO NOT REPRINT

© FORTINET

Available Management Actions for Events

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

The screenshot shows the FortiAnalyzer interface for managing events. At the top, there's a navigation bar with tabs like 'All Events', 'By Endpoint', 'By Threat', 'System Events', and 'Toggle Views'. Below the navigation is a search bar and some filters. A red box highlights the 'Show Acknowledged' checkbox, which is unchecked. A blue callout bubble says: 'Acknowledged events are not shown by default'. Another blue callout bubble on the left says: 'Right-click an event to see the list of available actions'. On the right, a large red box highlights a context menu for an event. This menu includes options like 'Acknowledge', 'Comment', 'Assign To', 'View Log', 'Search in Log View', 'Create New Incident', 'Add to Existing Incident', 'Filter by Event Type = Traffic', and 'Filter by Event Type != Traffic'. Blue callout bubbles point to these options: 'Create incidents from events that require further investigation', 'Filter based on the columns values to display events of interest only', and 'Filter by Event Type = Traffic'.

Event	Event Status	Event Type	Count	Severity	First Occurrence
198.50.152.88 (2)	Unhandled	Traffic	2	Critical	a day ago
Traffic to C&C from 10.0.3.20 detected	Unhandled	Traffic			2 days ago
Traffic to C&C from 10.0.1.200 detected	Unhandled	Traffic			2 days ago
+ 192.169.69.25 (2)	Unhandled	Traffic			2 days ago
+ 178.162.203.226 (2)	Unhandled	Traffic			2 days ago
+ 66.45.245.150 (2)	Unhandled	Traffic			2 days ago
+ 178.162.217.107 (4)	Unhandled	Traffic			2 days ago
+ 5.79.71.205 (4)	Unhandled	Traffic			2 days ago
+ 193.166.255.171 (2)	Unhandled	Traffic			2 days ago

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.

DO NOT REPRINT**© FORTINET**

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.

DO NOT REPRINT

© FORTINET

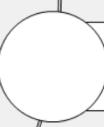
Lesson Overview



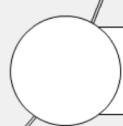
SOC Overview



Managing Events



Managing Incidents



Threat Hunting and Outbreak Alerts

Good job! You now know how to manage events.

Now, you will learn how to manage incidents.

DO NOT REPRINT

© FORTINET

Managing Incidents

Objectives

- Create incidents
- Analyze incidents
- Configure incident settings



© Fortinet Inc. All Rights Reserved.

25

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.

DO NOT REPRINT

© FORTINET

Creating an Incident

- An incident should be created when an event needs further analysis
- Can create manually or automatically (playbooks)

The screenshot shows the FortiAnalyzer interface. On the left, under 'Incidents & Events > Event Monitor', there is a list of events. One event, '10.0.1.10 (3)', is selected. A context menu is open over this event, with the 'Create New Incident' option highlighted by a red box and an arrow pointing to the right.

To the right, a 'Create New Incident' dialog box is displayed. It contains fields for:

- Incident Category:** Unauthorized Access (selected)
- MITRE Domain:** N/A Enterprise ICS
- MITRE Tech ID:** T1021.004 SSH, T1071.001 Web Protocols, T1071.004 DNS, T1102 Web Service
- Severity:** Low
- Status:** New (highlighted with a red box)
- Affected Endpoint:** 10.0.1.10
- Description:** Default-Risky-Destination-Detection-By-Endpoint hap
- Assigned To:** admin (Super_User) (highlighted with a red box)

A blue callout bubble on the right side of the dialog box contains the text: 'Must create accounts for party responsible for handling incidents'.

At the bottom of the interface, there is another section titled 'Incidents & Events > Incidents' showing a table of incidents. The first incident listed is IN00000002, which corresponds to the event selected in the Event Monitor.

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.

DO NOT REPRINT

© FORTINET

Analyzing an Incident

High INO0000007 Default-Compromised Host-Detection-IOC-By-Endpoint happened at 10.0.3.20 Unauthorized Access Assigned to:admin Analysis

Created on: 2023-09-07 10:53:35 -0700 Last Modified on: 2023-09-07 10:56:54 -0700

Affected Endpoint/User

No related user available.

Last Seen 2023-09-07 10:53:56
Topology FGVM010000077646
10.0.3.20

Addresses MAC: 02:09:01:00:07:02
IP: 10.0.3.20

Executed Playbooks

PLAYBOOK	STATUS	TRIGGER

Execute Playbook

Incident Timeline

From 2023-09-07 10:50:08 To 2023-09-07 10:55:13 (Total 3 Events)

Audit History

- 2023-09-07 10:... NOW **Expand All**
- Events Attached ... By: admin >
- Events Attached ... By: admin >
- Events Attached ... By: admin >
- New Incident Cr... By: admin >
- START 2023-09-07 10:53:35

Comments Events Reports Indicators Affected Assets Processes Software Vulnerabilities

Events

#	Event	Status	Type	Count	Severity	First Occurred
1	Web request to Dynamic DNS blocked	Mitigated	Web Filter	1	Medium	2023-09-07
2	Web request to Phishing blocked	Mitigated	Web Filter	1	Medium	2023-09-07

© Fortinet Inc. All Rights Reserved. 27

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.

DO NOT REPRINT

© FORTINET

Editing an Incident

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

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

Edit Incident	
Incident Number	IN00000007
Incident Date / Time	2023-09-07 10:53:35
Incident Category	Unauthorized Access
MITRE Domain	N/A Enterprise ICS
MITRE Tech ID	T1041 Exfiltration Over C2 Channel
Severity	High
Status	Closed: False Positive
Affected Endpoint	(Search)
Description	New Analysis Response Closed: Remediated Closed: False Positive
Assigned To	

Keep the incident status up to date

FORTINET
Training Institute

© Fortinet Inc. All Rights Reserved. 28

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.

DO NOT REPRINT
© FORTINET

Configure Incidents Settings

The screenshot shows the FortiAnalyzer interface for managing incidents. At the top, there's a toolbar with buttons for 'Create New', 'Edit', 'Delete All', 'Analysis', 'Settings' (which is highlighted with a red box), and a dropdown for 'All'. Below the toolbar is a table listing two incidents:

Incident Number	Incident Date / Time	Last Update Date / Time
IN00000007	2023-09-07 10:53:35	2023-09-07 10:56:54
IN00000006	2023-09-07 10:48:10	2023-09-07 10:48:11

A blue arrow points from the 'Settings' button in the toolbar down to the 'Notifications' section. This section contains two connector configurations:

- Fabric Connector 1 (MS_Teams_Connectc...):**
 - Send notification when an incident is created
 - Send notification when an incident is updated
 - Send notification when an incident is deleted
- Fabric Connector 2 (ServiceNow_Connectc...):**
 - Send notification when an incident is created
 - Send notification when an incident is updated
 - Send notification when an incident is deleted

A yellow box highlights the text 'Different connectors can have different settings'. A blue callout bubble points to the 'Fabric Connector 1' section with the text 'First create the connectors in Fabric View'.

To the right, a 'Notification example' is shown in a separate window titled 'FAZ_Notification 1:23 PM'. It displays a JSON message received via Teams:

```

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

```

A red box highlights the 'incid' field in the JSON message. The bottom right corner of the slide includes the Fortinet Training Institute logo and the text '© Fortinet Inc. All Rights Reserved. 29'.

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.

DO NOT REPRINT**© FORTINET**

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

DO NOT REPRINT

© FORTINET

Lesson Overview



SOC Overview



Managing Events



Managing Incidents



Threat Hunting and Outbreak Alerts

Good job! You now understand how to manage incidents.

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

DO NOT REPRINT**© FORTINET**

Threat Hunting and Outbreak Alerts

Objectives

- Understand threat hunting
- Use the log count chart
- Use the SIEM log analytics table
- Understand 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.

DO NOT REPRINT

© FORTINET

Threat Hunting

- Proactively searching for suspicious or risky network activity that may have gone undetected
- The process usually begins with a question:
 - Is there any advanced persistent threat currently active in our network?
- The reference to tactics, techniques, and procedures (TTPs), behaviors, and indicators helps to narrow down to more specific questions
 - Frequently aligned with the MITRE ATT&CK or the Cyber Kill Chain frameworks
- Can also come in the form of an if-then statement, for example:
 - If you have DNS C&C in the network, then you should see abnormal DNS traffic
- A simplified example:



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

The threat hunting process usually starts with a broad question, or hypothesis, that determines which type of threat you are trying to find. You can also start with an if-then statement. For example, if you 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.

DO NOT REPRINT

© FORTINET

Threat Hunting (Contd)

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

Incidents & Events > Threat Hunting

Threat Action (3)		2023-09-07 19:47:57 - 2023-09-07 20:47:56			
#	Application Name	Count	Sent (bytes)	Average Sent	Max Sent (bytes)
1		202,284(69%)	73.8 KB	185.0 B	517.0 B
2	DNS	87,799(30%)	7.4 MB	170.0 B	28.5 KB
3	HTTP.BROWSER	1,688(1%)	513.8 KB	548.0 B	6.7 KB
4	HTTP	937(< 1%)	1.7 MB	1.8 KB	27.8 KB
5	HTTPS	515(< 1%)	565.3 MB	1.1 MB	554.9 MB
6	HTTPS.BROWSER	390(< 1%)	301.8 KB	1.4 KB	3.3 KB
7	Dropbox_File.Download	132(< 1%)	217.8 KB	3.3 KB	3.8 KB
8	Blogger	52(< 1%)	27.7 KB	978.0 B	3.3 KB
9	udp/443	51(< 1%)	896.7 KB	17.6 KB	17.6 KB
10	Vimeo_Video.Play	44(< 1%)	31.1 KB	1.4 KB	2.3 KB
11	Dropbox_File.Upload	44(< 1%)	44.3 KB	2.0 KB	3.0 KB
12	Instagram	42(< 1%)	41.6 KB	1.7 KB	4.3 KB

FORTINET
Training Institute

© Fortinet Inc. All Rights Reserved. 34

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?

DO NOT REPRINT

© FORTINET

Log Count Chart

- The **Log Count** chart allows the administrators to narrow down what logs will be analyzed based on a time range
- The details shown in the SIEM log table adjust to the timeframe selected in this chart

Incidents & Events > Threat Hunting



Adjust the time bar
to include only the
desired time frame

FORTINET
Training Institute

© Fortinet Inc. All Rights Reserved. 35

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.

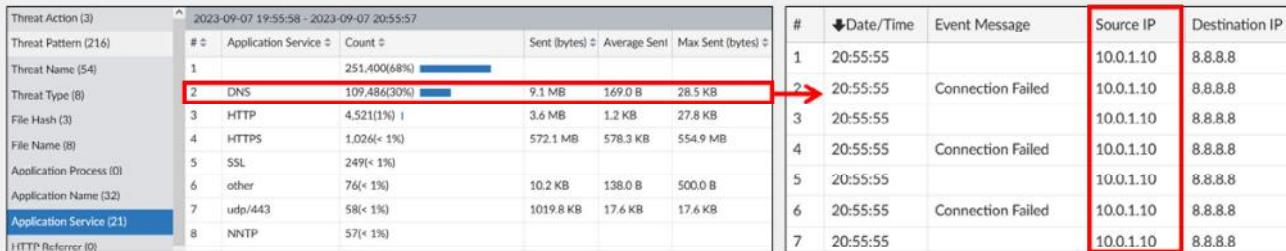
Only logs displayed within the time period visible in the chart are shown in the SIEM log analytics table.

DO NOT REPRINT

© FORTINET

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



The screenshot shows two tables side-by-side. The left table is a summary of threat actions, and the right table is a detailed log of DNS events.

Threat Action (3)

2023-09-07 19:55:58 - 2023-09-07 20:55:57				
#	Application Service	Count	Sent (bytes)	Average Sent
1		251,400(68%)		
2	DNS	109,486(30%)	9.1 MB	169.0 B
3	HTTP	4,521(1%)	3.6 MB	1.2 KB
4	HTTPS	1,026(< 1%)	572.1 MB	578.3 KB
5	SSL	249(< 1%)		554.9 MB
6	other	76(< 1%)	10.2 KB	138.0 B
7	udp/443	58(< 1%)	1019.8 KB	17.6 KB
8	NNTP	57(< 1%)		

Threat Pattern (216)

#	Date/Time	Event Message	Source IP	Destination IP
1	20:55:55		10.0.1.10	8.8.8.8
2	20:55:55	Connection Failed	10.0.1.10	8.8.8.8
3	20:55:55		10.0.1.10	8.8.8.8
4	20:55:55	Connection Failed	10.0.1.10	8.8.8.8
5	20:55:55		10.0.1.10	8.8.8.8
6	20:55:55	Connection Failed	10.0.1.10	8.8.8.8
7	20:55:55		10.0.1.10	8.8.8.8

- 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.

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.

DO NOT REPRINT

© FORTINET

MITRE ATT&CK Framework Matrices

- Consist of cybersecurity tactics and techniques organized into matrices

Incidents & Events > MITRE ATT&CK® > Attack

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

The column headers are the tactics
The tiles under the columns are the techniques
Click a tile to see associated incidents and events

Incidents & Events > MITRE ATT&CK® > Coverage

110 Event Handlers - 41% Coverage		
Reconnaissance	Resource Development	Initial Access
10 techniques	8 techniques	9 techniques
Active Scanning 3	Acquire Access	Drive-by Compromise
Gather Victim Host Information 1	Acquire Infrastructure 1	Exploit Public-Facing Application 3
Gather Victim Identity Information	Compromise Accounts	External Remote Services
Gather Victim Network Information	Compromise Infrastructure 8	Develop

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

Note: Not all tactics and techniques are shown

FORTINET
Training Institute

© Fortinet Inc. All Rights Reserved. 37

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.

DO NOT REPRINT
© FORTINET

Outbreak Detection Service Overview

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



The screenshot shows the FortiAnalyzer interface with the 'Incidents & Events > Outbreak Alerts' tab selected. The main pane displays an alert titled 'Agent Tesla Malware Attack' with the sub-section 'New Agent Tesla variant in the wild'. It includes a link to a blog post and CVE details. A sidebar on the left lists months from 2020 to 2023. The bottom right corner shows copyright information: © Fortinet Inc. All Rights Reserved. 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.

DO NOT REPRINT
© FORTINET

Outbreak Alert Handlers and Reports

	Status	Name
<input type="checkbox"/>	<input checked="" type="checkbox"/>	Outbreak Alert - Microsoft Outlook Elevator
<input type="checkbox"/>	<input checked="" type="checkbox"/>	Outbreak Alert - MSDT DogWalk Vulnerability
<input type="checkbox"/>	<input checked="" type="checkbox"/>	Outbreak Alert - Log4j2 Vulnerability Event

- The new event handlers are added to the list of available handlers, and you can use them in the same way as the rest in the list

Event handlers
downloaded
through the
outbreak alerts
service

	Title
<input type="checkbox"/>	Outbreak Alert - Atlassian Information Disclosure Report
<input type="checkbox"/>	Outbreak Alert - BURNTIGAR Malware Report
<input type="checkbox"/>	Outbreak Alert - Cacti Command Injection Report
<input type="checkbox"/>	Outbreak Alert - CISAtop20_PRC2022 Report
<input type="checkbox"/>	Outbreak Alert - CosmicEnergy Malware Report
<input type="checkbox"/>	Outbreak Alert - CWP OS Command Injection Report

- The same is true for the newly downloaded reports

Reports
downloaded
through the
outbreak alerts
service

FORTINET.
Training Institute

© Fortinet Inc. All Rights Reserved. 39

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.

DO NOT REPRINT

© FORTINET

Knowledge Check

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

DO NOT REPRINT

© FORTINET

Lesson Overview



SOC Overview



Managing Events



Managing Incidents



Threat Hunting and Outbreak Alerts

Congratulations! You have completed this lesson.

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

DO NOT REPRINT**© FORTINET**

Review

- ✓ Understand FortiAnalyzer SOC features
- ✓ Summarize SOC dashboards information
- ✓ Understand management extension applications
- ✓ Manage event handlers
- ✓ Manage events
- ✓ Manage incidents
- ✓ Configure incident settings
- ✓ Understand threat hunting
- ✓ Use the log count chart
- ✓ Use the SIEM log analytics table
- ✓ Understand outbreak alerts



© Fortinet Inc. All Rights Reserved.

© Fortinet Inc. All Rights Reserved. 42

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.

DO NOT REPRINT

© FORTINET



FortiAnalyzer Analyst

Reports

 FortiAnalyzer 7.4.1

Last Modified: 21 December 2023

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.

DO NOT REPRINT

© FORTINET

Lesson Progress



Report Concepts



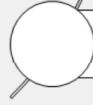
Generating and Customizing Reports



Customizing Charts and Datasets



Managing Reports



Troubleshooting Reports

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

DO NOT REPRINT

© FORTINET

Report Concepts

Objectives

- Describe the elements that constitute a report
- Describe how charts extract data from the database
- Describe how reports function within ADOMs



© Fortinet Inc. All Rights Reserved.

3

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.

DO NOT REPRINT**© FORTINET**

Purpose of Reports

- Reports summarize a large amount of log (text) data
- FortiAnalyzer retrieves the information collected from the log files of managed devices and presents it in tabular and graphical reports
- Reports provide a quick and detailed analysis of activity on your network

Default reports categories

	Application Reports
	Asset and User Reports
	Compliance Reports
	Fabric Reports
	FortiCache Reports
	FortiClient Reports
	FortiDDoS Reports
	FortiDeceptor Reports
	FortiFirewall Reports
	FortiGate Reports
	FortiMail Reports
	FortiNAC Reports
	FortiNDR Reports
	FortiProxy Reports
	FortiSandbox Reports
	FortiWeb Reports
	Network Reports
	Outbreak Alert Reports
	SOC Reports
	Daily Summary Report

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.

DO NOT REPRINT

© FORTINET

Elements That Comprise a Report

- A FortiAnalyzer report is a set of data in organized charts

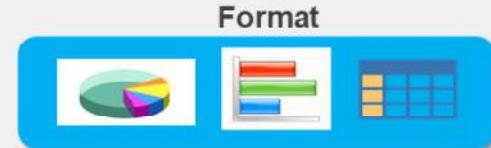


Charts define:

- What **data** from the SQL database is displayed
- What **format** the data is displayed in



Datasets are specific SQL SELECT queries



Format options include:
pie charts, bar charts, or tables

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)

DO NOT REPRINT

© FORTINET

How Do Charts Extract Data From the Database?

- Data populates a chart
- Datasets are SQL SELECT queries, used to extract data from the database
- SELECT statements are read-only

The screenshot shows two windows side-by-side. The left window is titled 'Chart' and contains fields for 'Name' (Top 5 Attacks by Severity), 'Description' (Top 5 attacks by severity), and 'Dataset' (set to 'threat-Attacks-By-Severity'). The right window is titled 'Dataset' and contains fields for 'Name' (threat-Attacks-By-Severity), 'Log Type' (Intrusion Prevention), and a 'Query' section. A red arrow points from the 'Dataset' field in the Chart window to the 'Query' section in the Dataset window. Inside the 'Query' section, a red box highlights the SQL code:

```

1 select (case when severity='critical' then
'Critical' when severity='high' then 'High' when
severity='medium' then 'Medium' when severity='low'
then 'Low' when severity='info' then 'Info' end) as
severity, count(*) as totalnum from $log where
$filter group by severity order by totalnum desc

```

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.

DO NOT REPRINT

© FORTINET

SELECT Statement

- The SELECT statement retrieves the log data you want from the database
- Must specify criteria using a recognized and supported clause

Clause	Definition
FROM	From which table(s) or view(s) the data will be extracted
WHERE	Sets the conditions (all rows that do not satisfy the condition are not shown in the output)
GROUP BY	Collects data across multiple records and groups the results by one or more columns
ORDER BY	Orders the results by specific column(s), ascending or descending
LIMIT	Limits the number of records returned based on a limit value.
OFFSET	Often used with the LIMIT clause to offset the results by a set value

Clauses must be coded in a specific sequence

- For more information, see the supplementary *FortiAnalyzer SQL and Datasets* lesson



© Fortinet Inc. All Rights Reserved.

7

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.

DO NOT REPRINT

© FORTINET

Accessing the SQL Schema

Reports > Report Definitions > Datasets

Name	Test Dataset	Select log type
Log Type	Traffic	
Query	1 <code>select * from \$log</code>	This query returns everything from the log type selected

Go Stop Time Period Previous 7 Days Devices All Devices

id	bid	dvid	itime	dtime	euid	epid	dsteuid	dstepid	logflag	logver
7285771809847446860	650012	1064	1696350940	1696325646	3	104	3	1032		704012463

Column headings indicate what is available in the database schema for the log type selected

FORTINET
Training Institute

© Fortinet Inc. All Rights Reserved. 8

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.

DO NOT REPRINT
© FORTINET

Accessing the SQL Schema (Contd)

Name	Test Dataset
Log Type	Traffic
Query	<code>1 select * from \$log</code>

Hover your mouse over the hyperlink to display the schema

These are all the available fields you can use for queries

Table "Logs" has the following fields:

```

id, bid, dvid, itime, dtime, euid, epid, dsteuid, dstepid, logflag, logver,
sfsid, type, subtype, level, action, utmaction, policyid, sessionid, srchip,
dstip, tranip, transip, srccport, dstport, transport, transport, trandisp,
duration, proto, vrf, slot, sentbyte, rcvdbyte, sentdelta, rcvddelta,
sentpkt, rcvdpkt, logid, user, unauthuser, dstunauthuser, srcrename, dstname,
group, service, app, appcat, fctuid, srcintfrole, dstintfrole, srccserver,
dstserver, appid, appact, apprisk, wanoptapptype, polictype, centralnatid,
channel, wuplanid, shapingpolicyid, avantime, valid, shaperdropsanhyte,
shaperdroprcvdbyte, shaperperipdropbyte, wanin, wanout, lanin, lanout,
crscore, craction, clevel, countapp, countav, countdp, countemail,
countips, countweb, countwaf, countssl, countssh, countdns, srcuuid, dstuuid,
poluid, srccmac, mastersrcmac, dstmac, masterdstmac, srchinvendor,
srchinversion, srccfamily, srccversion, dsthwvendor, dsthvversion, dstfamily,
dstswversion, devtype, devcategory, dstdevtype, dstdevcategory, osname,
osversion, datosname, datosversion, srccountry, srccssid, dstssid,
srcintf, dstintf, srcinetsvc, dstinetsvc, unauthusersource,
dstunauthusersource, authserver, applist, vpn, vpntype, radioband,
policyname, policymode, ssaction, url, agent, comment, ap, apsn, vulservice,
vulquality, collectedemail, dstcollectedemail, shapersentname,
shaperrcvdname, shaperperipname, msg, custom_field1, utmevent, utmsubtype,
sender, recipient, virus, attack, hostname, catdesc, dipsensor, utmref,
tdinfoid, dstowner, tdtype, tdscantime, tdthreattype, tdmfcate,
threatugts, threatcnts, threatlvs, saasinfo, ebtime, clouduser, threats,
threattyps, apps, countff, identifier, securityid, securityact, tz,
srccdomain, counticap, dtregion, srcregion, dstcity, srccity, signal, snr,
dstauthserver, dstgroup, dstuser, tunneld, vulname, srcthreatfeed,
dstthreatfeed, psrccport, pdstport, countcptf, srcreputation, dstreputation,
vip, accessproxy, gatewayid, clientdeviceid, clientdeviceowner,
clientdevicetags, httpmethod, referralurl, saasname, srccmacvendor,
shapingpolicyname, accessctrl, countcifs, proxyapptype,
clientdevicemanageable, emsconnection, realserverid, fudsrv, replydstintf,
repliesrcintf, countvpatch, countcasb, devid, vd, devname, csf, devgrps

```

© Fortinet Inc. All Rights Reserved.

9

FORTINET
Training Institute

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.

DO NOT REPRINT

© FORTINET

Accessing the SQL Schema (Contd)

- srcip and srcport chosen from the schema

Table "Logs" has the following fields:

sfsid, type, subtype, level, action, utmaction, policyid, sessionid, srcip, dstip, tranip, transip, srcport, dstport, transport, transport, trandisp,

- Sample query using srcip and srcport

```
1 select srcip as "Source IP", srcport as "Source Port"
2 from $log
3 where $filter and srcip = '10.0.1.10'
4 group by srcip, srcport
5 order by srcport desc
```

- Results

Source IP	Source Port
10.0.1.10	60999
10.0.1.10	60998
10.0.1.10	60993

© Fortinet Inc. All Rights Reserved. 10

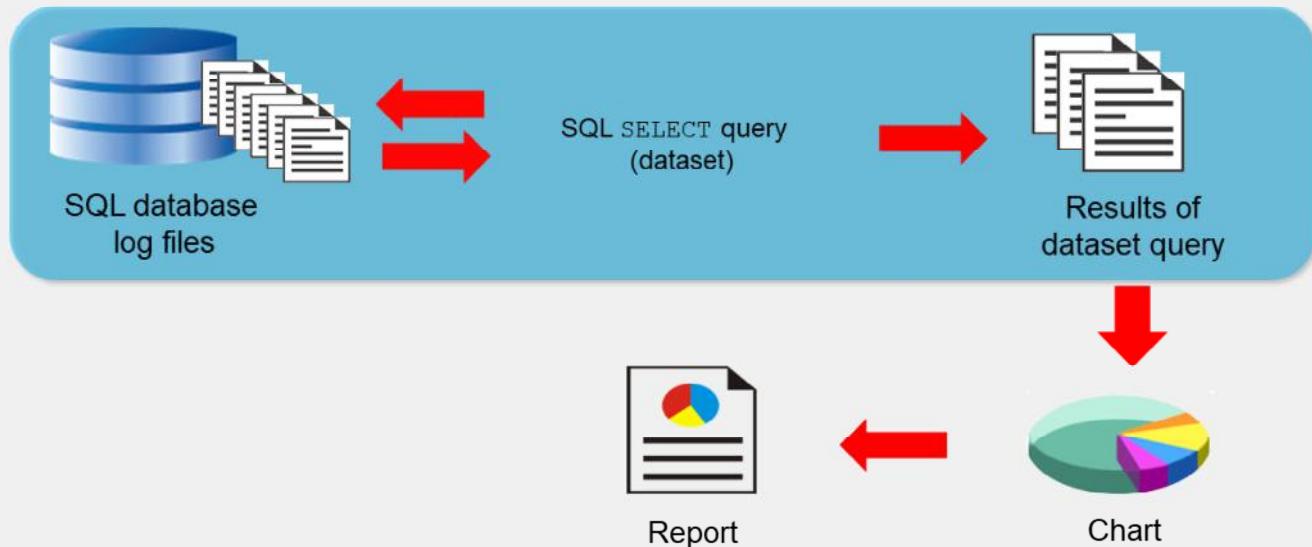
You can use the fields you identify in the schema to build your queries. For example, you can select srcip and srcport from the traffic log type, and then create a query.

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.

DO NOT REPRINT**© FORTINET**

Report Workflow



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.

DO NOT REPRINT**© FORTINET**

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

<input type="checkbox"/>	Title
<input type="checkbox"/>	Application Reports
<input type="checkbox"/>	Asset and User Reports
<input type="checkbox"/>	Compliance Reports
<input type="checkbox"/>	Fabric Reports
<input type="checkbox"/>	FortiCache Reports
<input type="checkbox"/>	FortiClient Reports
<input type="checkbox"/>	FortiDDoS Reports
<input type="checkbox"/>	FortiDeceptor Reports
<input type="checkbox"/>	FortiFirewall Reports
<input type="checkbox"/>	FortiGate Reports

When you enable ADOMs, each ADOM has its own reports, libraries, and advanced settings. As such, make sure that you are in the correct ADOM before selecting a report.

Additional reports for specific Fortinet devices are available only when you enable ADOMs. This slide does not show all the available default report types. You can configure and generate reports for these devices within their respective ADOMs. These devices also have device-specific charts and datasets.

DO NOT REPRINT**© FORTINET**

Report Considerations

- Audience
 - Level and type of information may vary depending on intended reader
- Purpose
 - What information do you want?
 - Align with dataset query
- Level of detail
 - Too much detail can overwhelm the reader
 - Best practice → Keep reports short and concise
 - Too many charts in a report tie up the CPU for a long time
- Format
 - What is the best way to display the information?
 - Select the *right* chart format for your purpose

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.

DO NOT REPRINT

© FORTINET

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

DO NOT REPRINT

© FORTINET

Lesson Progress



Report Concepts



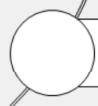
Generating and Customizing Reports



Customizing Charts and Datasets



Managing Reports



Troubleshooting Reports

Good job! You now understand report concepts.

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

DO NOT REPRINT

© FORTINET

Generating and Customizing Reports

Objectives

- Describe templates
- Run predefined reports
- Fine-tune reports
- Reports customization options
- Use macros in reports



© Fortinet Inc. All Rights Reserved.

16

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

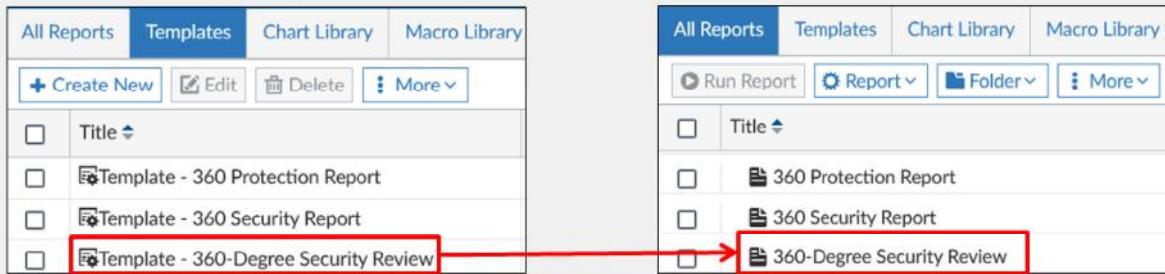
By demonstrating competence in report generation and customization, you will be able to generate reports specific to your requirements.

DO NOT REPRINT

© FORTINET

Templates

- A template specifies the layout—text, charts, and macros—to include in the report that uses it
- FortiAnalyzer provides predefined templates (which match the predefined reports)
 - Can clone predefined templates or create custom templates
 - Can't edit or delete predefined templates



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.

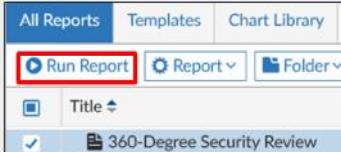
Templates don't contain any data. Data is added to the report when you generate it.

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.

DO NOT REPRINT
© FORTINET

Running Predefined Reports

Reports > Report Definitions > All Reports



- Can run reports with default settings

Generated Reports		Settings	Editor
Name	360-Degree Security Review		
Time Zone	Default		
Time Period	Previous 7 Days 10/05/2023 00:00:00 - 10/11/2023 23:59:59 (for example)		
Devices	All Devices	Specify	<input checked="" type="radio"/>
Subnets	All Subnets	Specify	<input checked="" type="radio"/>
<input type="checkbox"/> Generate separate report per-device/VDOM			
Enable Schedule	<input type="checkbox"/>		
Enable Notification	<input type="checkbox"/>		
Enable Auto-cache	<input checked="" type="checkbox"/>		
Extended Log Filtering	<input type="checkbox"/>		
Filters >			
Advanced Settings >			

FORTINET
Training Institute

© Fortinet Inc. All Rights Reserved. 18

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.

DO NOT REPRINT
© FORTINET

Running Predefined Reports (Contd)

- You can filter which logs are included in a report

Filters ▾

Log messages that match All Any of the Following Conditions

Log Field	Match Criteria	Value 	Action
Severity (severity)	Equal To	critical	 
Destination Interface (dstintf)	Equal To	port3	 

You can also set filters on the charts used within a report

Advanced Settings ▾

Language	English
Bundle Rest into "Others"	Auto
Print Orientation	<input checked="" type="radio"/> Portrait <input type="radio"/> Landscape
Chart Heading Level	Heading 2
Default Font	Open Sans
Hide # Column	<input checked="" type="checkbox"/>
Layout Header	<input checked="" type="checkbox"/>
Header Text	
Header Image	Select Image fortinet_grey.png
Layout Footer	<input checked="" type="checkbox"/> <input checked="" type="radio"/> Default <input type="radio"/> Custom
Print Cover Page	<input checked="" type="checkbox"/>
Print Table of Contents	<input checked="" type="checkbox"/>
Print Device List	<input checked="" type="checkbox"/> Compact
Display Device Name	By Device Name
Print Report Filters	<input checked="" type="checkbox"/>
Obfuscate User	<input type="checkbox"/>
Resolve Hostname	<input type="checkbox"/>
Date Format	Default
Allow save maximum	99
Color Code	Purple
Report Owner	Click to select

© Fortinet Inc. All Rights Reserved.

19



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.

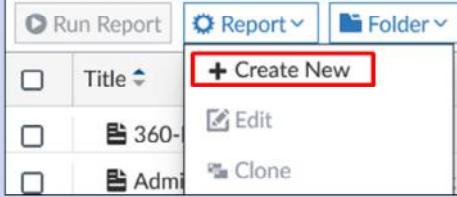
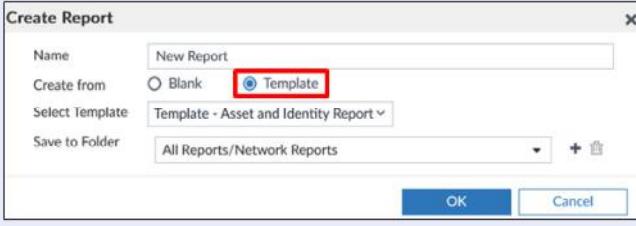
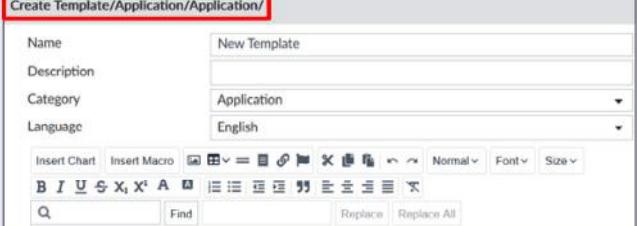
Fine-tuning encompasses minimal modifications, such as:

- 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**.

DO NOT REPRINT

© FORTINET

Customization Options

Minor / Moderate Customizations	Major Customizations
<p>Clone a report or template, then edit the clone</p> 	<p>Create a new report from scratch (blank)</p> 
<p>Create a new report from an existing template, then edit</p> 	<p>Create a new template (which you can use in a report)</p> 

FORTINET
Training Institute

© Fortinet Inc. All Rights Reserved. 20

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.

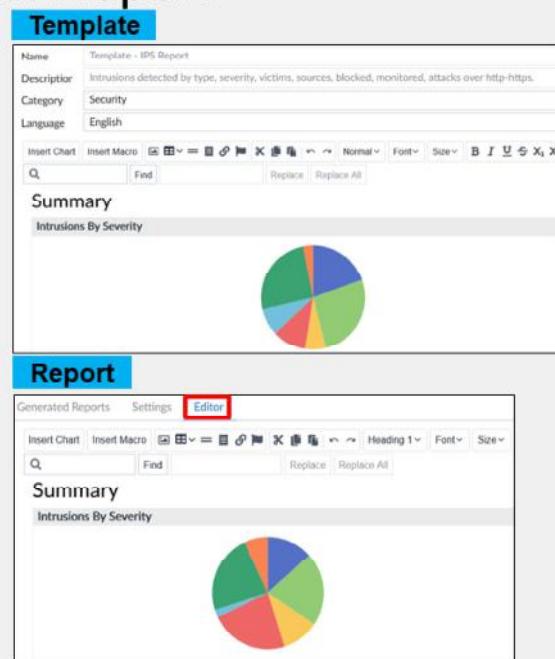
If you need to make major changes to existing templates or reports (if no report comes close to meeting your needs), you can create a new report or template from scratch.

DO NOT REPRINT

© FORTINET

Customization—Template vs. Report

- Which customization approach to take: template or report?
- Most important difference: templates only include the layout of the report—they don't include report settings (either basic configurations or advanced settings)
- Best practice is to approach it from an efficiency and needs standpoint
- Think about:
 - The amount of customization you need
 - Whether you want to preserve report settings
 - Whether you want to use the layout for one report or many reports



FORTINET
Training Institute

© Fortinet Inc. All Rights Reserved. 21

Templates and reports are closely related. As discussed earlier, you can clone and edit both reports and templates, and you can create both new reports and new templates. So, how do you know which customization approach to take: Do you approach the customization from the template side or the report side?

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

DO NOT REPRINT

© FORTINET

Inserting Macros as Abbreviated Dataset Queries

- Macros specify which data to extract from the logs
 - Macros represent a sequence of instructions (dataset queries) in abbreviated form

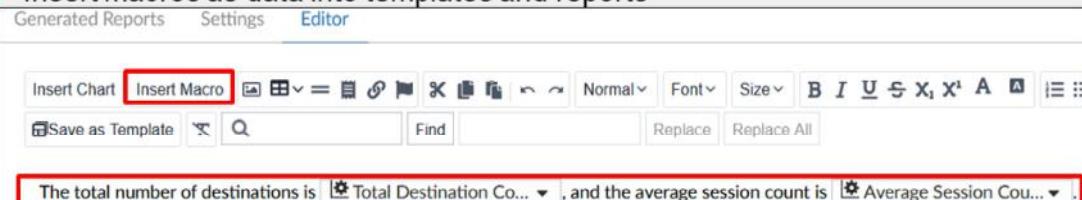
Reports > Report Definitions > Macro Library

Name	Total Destination Count
Description	Total Destination Count
Dataset	bandwidth-app-Detailed-Traffic-Statistics
Query	select count(distinct app) as total_app, count(total_endpoint, count(distinct dstip) as total)
Data Binding	total_dest
Display	Counter (K/M/G)

- Example report with macros:

The total number of destinations is 68 , and the average session count is 46.09 K .

- Insert macros as data into templates and reports



© Fortinet Inc. All Rights Reserved. 22

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.

DO NOT REPRINT

© FORTINET

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.

DO NOT REPRINT

© FORTINET

Lesson Progress



Report Concepts



Generating and Customizing Reports



Customizing Charts and Datasets



Managing Reports



Troubleshooting Reports

Good job! You now understand how to customize reports.

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

DO NOT REPRINT

© FORTINET

Customizing Charts and Datasets

Objectives

- Customize and create charts
- Customize and create datasets



© Fortinet Inc. All Rights Reserved.

25

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.

DO NOT REPRINT

© FORTINET

If Predefined Charts or Datasets Do Not Meet Requirements

- By default, the **Chart Library** contains hundreds of charts
 - Can't edit default charts
- By default, the **Datasets** library contains hundreds of datasets
 - Can't edit default datasets
- Just like templates and reports, you can clone and edit both charts and datasets, and create new ones
- Gives you the flexibility to pull a unique combination of data from the database that doesn't exist in any default chart or dataset

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

DO NOT REPRINT
© FORTINET

Building Datasets and Charts From Search Results

- In **Log View**, set filters to search for logs and then use the chart builder

The screenshot shows the FortiAnalyzer Log View interface. On the left, there's a table of log entries with columns for Source IP, Service, Application, and others. A red arrow points from the 'Chart Builder' button in the table header to the 'Chart Builder' window on the right. The 'Chart Builder' window has a 'Name' field set to 'Traffic from 10.0.1.10'. The 'Column' section is expanded, showing checkboxes for Date/Time, Device ID, User, Destination IP, Service, and Application, with Destination IP checked. A query editor shows a complex SQL-like search query. Below the query is a preview table with several log entries. A blue callout bubble says 'Dataset builds automatically based on search filters and fine-tuning parameters'. At the bottom of the 'Chart Builder' window is a 'Test your query' button, a 'Save' button, and a 'Cancel' button. A blue callout bubble also points to the 'Save' button with the text 'Save as dataset and chart'. The bottom right corner of the window says '© Fortinet Inc. All Rights Reserved. 27'.

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

DO NOT REPRINT
© FORTINET

Export From FortiView to a Chart

- Similar to the **Chart Builder** feature in **Log View**, you can export a chart from FortiView

The screenshot shows the FortiView interface with a chart titled "Top Source". The Y-axis is labeled "Sessions" with values 0.5k, 1.0k, 1.5k, 2.0k, and 2.5k. The X-axis shows dates from Oct 06 to Oct 12. A single blue line represents a session spike reaching nearly 2.5k sessions. Above the chart, a blue callout bubble says "Chart export will include any filters you set". On the right, a context menu is open with options "Export to PDF" and "Export to Report Chart". The "Export to Report Chart" option is highlighted with a red box. A large red arrow points down to a separate window titled "Export to Report Chart". This window contains the following fields:

Name	Source 10.0.1.10
Time	From 2023-10-6 16:26 To 2023-10-13 16:26
Device	
Filter	srcip=10.0.1.10
Top	0

At the bottom of the FortiView interface, there is a "FORTINET Training Institute" logo and copyright information: "© Fortinet Inc. All Rights Reserved. 28".

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.

DO NOT REPRINT

© FORTINET

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

DO NOT REPRINT

© FORTINET

Lesson Progress



Report Concepts



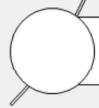
Generating and Customizing Reports



Customizing Charts and Datasets



Managing Reports



Troubleshooting Reports

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

Now, you will learn how to manage reports.

DO NOT REPRINT

© FORTINET

Managing Reports

Objectives

- Configure external storage for reports
- Enable auto-cache
- Group reports
- Import and export reports and charts
- Attach reports to incidents
- Manage scheduled reports



© Fortinet Inc. All Rights Reserved. 31

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.

DO NOT REPRINT
© FORTINET

Configure External Storage for Reports

- Send or store reports externally for backup purposes
- Requires configuration of a mail server to email reports
- Can also upload generated reports to a server (FTP/SFTP/SCP)

System Settings > Advanced > Mail Server

Edit Mail Server Settings	
SMTP Server Name	Mail_Server
Mail Server	10.200.1.254
SMTP Server Port	25
Enable Authentication	<input checked="" type="checkbox"/>
E-Mail Account	admin@training.lab
Password	*****
From (Optional)	

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.

DO NOT REPRINT
© FORTINET

Configure External Storage for Reports (Contd)

- Configure output profiles per ADOM
- Email reports or upload to server (HTML, PDF, XML, CSV, and JSON)
- First configure an output profile, then enable notifications for each report

Reports > Report Definitions > All Reports

Enable Notification <input checked="" type="checkbox"/>	Output Profile Email Profile
---	------------------------------

Reports > Advanced Settings > Output Profile

Name: Email Profile
Comments:
Output Format: HTML PDF XML CSV JSON
 Email Generated Reports
Subject: Generated Reports
Body: Please review these reports
27/1023
Recipients: Email Server
From: To Action
Mail_Server: 10.200.1.254 + admin@training.lab admin@training.lab x +
 Upload Report to Server
Server Type: FTP
10.1.1.1
User: user
Password:
Directory: reports
 Delete file(s) after uploading

FORTINET
Training Institute

© Fortinet Inc. All Rights Reserved. 33

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, 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.

DO NOT REPRINT

© FORTINET

SQL Hard Cache (hcache)

- The hcache must build before FortiAnalyzer can build the report
 - Increases report generation time
 - If no new logs are received for the reporting period, the hcache doesn't need to rebuild
 - If new logs come in, the hcache needs to rebuild
- To reduce report generation time, enable auto-cache
 - The hcache automatically updates when new logs come in and FortiAnalyzer generates new log tables
- Enable hcache for most reports to ensure they are efficiently generated
 - Caveat: hcache uses system resources (especially for reports that take a long time to generate datasets)

Reports > Report Definitions > All Reports

Generated Reports Settings Editor

Enable Auto-cache

Extended Log Filtering

Default Filtering Device Source IP Destination IP Endpoint ID Source End User ID

Additional Log Fields

Policy Name (policyname)

1 entry selected

Enable **Extended Log Filtering** to cache specific log fields for faster filtering

Note: Hcache is automatically enabled for scheduled reports

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.

DO NOT REPRINT

© FORTINET

Grouping Reports to Improve Report Generation Time

- Benefits:

- Reduces the number of hcache tables
- Improves auto-cache completion time

```
# configure system report group
edit 0
  set adom <ADOM-name>
  config group-by
    edit <SQL-column>
      next
    edit vd
      next
  end
  set report-like <report name string>
end
```

execute sql-report list-schedule <ADOM-name>

execute sql-report hcache-build <ADOM-name>
<schedule-name> "<start-time>" "<end-time>"

SQL column is added to
the hcache creation
queries with any related
report

Group report function is
applied to any report that
contains this case-
sensitive string

View report grouping
information

Must rebuild
hcache tables

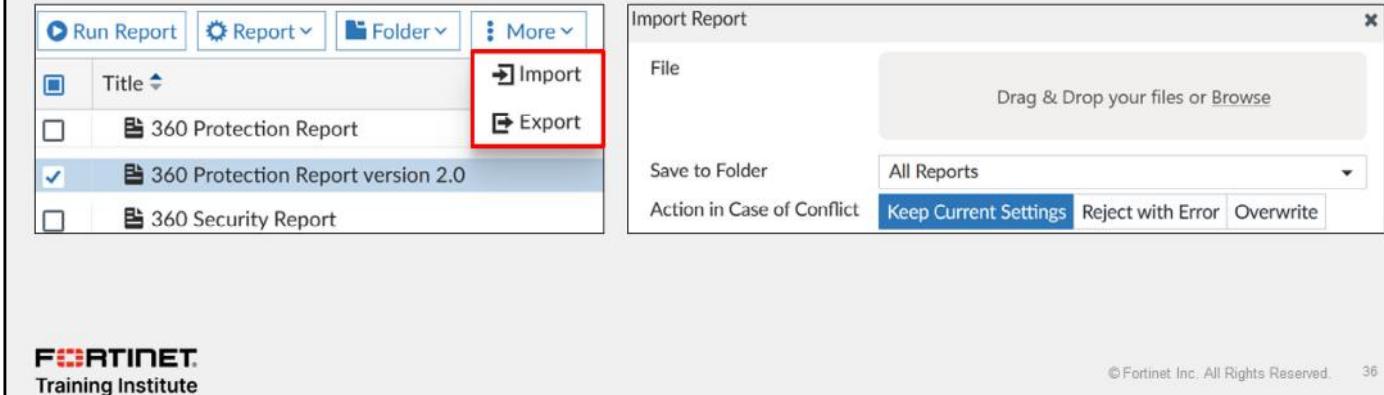
If the same (or similar) reports are run against many different FortiGate devices, you can significantly improve report generation time by grouping the reports. Report grouping can reduce the number of hcache tables and improve auto-cache completion time and report completion time.

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.

DO NOT REPRINT
© FORTINET

Moving Reports Between ADOMs

- Each ADOM has its own reports, libraries, and advanced settings
- Export reports and charts (default and custom) and import them into a different ADOM based on the same type (that is, FortiGate ADOM to FortiGate ADOM)
 - Chart imports dataset associated with chart
 - Can save layout of imported report as a template



The screenshot shows the FortiAnalyzer interface. On the left, there is a list of reports under 'Report' tab:

- Title
- 360 Protection Report
- 360 Protection Report version 2.0** (selected)
- 360 Security Report

To the right of the list is a toolbar with buttons: Run Report, Report (dropdown), Folder (dropdown), More (dropdown), Import (highlighted with a red box), and Export.

A modal window titled 'Import Report' is open on the right. It contains the following fields:

- File: Drag & Drop your files or Browse
- Save to Folder: All Reports
- Action in Case of Conflict: Keep Current Settings (selected), Reject with Error, Overwrite

FORTINET
 Training Institute

© Fortinet Inc. All Rights Reserved. 36

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.

DO NOT REPRINT

© FORTINET

Attach Reports to Incidents

- Attach a report to add historical data to an incident
- There are three ways to attach a report:
 - Manually, from an existing report
 - Manually, from an existing incident
 - Automatically, through playbook automation

The screenshot shows a list of generated reports. For 'Today (2)', there are two entries: 'HTML PDF XML CSV JSON Daily Summary Report-2023-10-14' and 'HTML PDF XML CSV JSON Daily Summary Report-2023'. For 'Earlier This Week (28)', there are 28 entries. A context menu is open over the second report in the 'Today' section, with options: Delete, Retrieve Diagnostic, Create New Incident, and Add to Existing Incident. The 'Add to Existing Incident' option is highlighted with a red box.

Right-click on a generated report

The screenshot shows the 'Reports' tab for an incident. The incident details are at the top: High priority, IN00001463, DDoS attempt on firewall, Denial of Service (DoS), Assigned to:admin, Analysis. Below are sections for 'Affected Endpoint/User' (No related user available) and 'Executed Playbooks'. A button 'Execute Playbook' is visible. At the bottom, there's a search bar and filter options for 'Report Name', 'Format', 'Time Range', 'Devices', and 'Status'. A red box highlights the 'Reports' tab in the navigation bar.

Or add a report to an existing incident

FORTINET
Training Institute

© Fortinet Inc. All Rights Reserved. 37

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.

DO NOT REPRINT
© FORTINET

Viewing Scheduled Reports Through Calendar

- Graphic view of scheduled (generated and pending) reports

Reports > Advanced Settings > Report Calendar

November 2023

W Sun Mon Tue Wed Thu Fri

44 29 30 1 2 3 4

45 6 7 8 9 10 11

Report: Daily Summary Report
Status: Pending
Device Type: FortiGate
Start Time in US/Pacific: 2023-11-08 03:00:00 -08:00

46 12 13 14 15 16 17 18

47 19 20 21 22 23 24 25

48 26 27 28 29 30 1 2

FORTINET Training Institute © Fortinet Inc. All Rights Reserved. 38

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.

DO NOT REPRINT

© FORTINET

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

DO NOT REPRINT

© FORTINET

Lesson Progress



Report Concepts



Generating and Customizing Reports



Customizing Charts and Datasets



Managing Reports



Troubleshooting Reports

Good job! You now understand how to manage reports.

Now, you will learn about report troubleshooting.

DO NOT REPRINT

© FORTINET

Troubleshooting Reports

Objectives

- Troubleshoot reports



© Fortinet Inc. All Rights Reserved. 41

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.

DO NOT REPRINT
© FORTINET

Troubleshooting Report Generation Run Time

- Retrieve report diagnostics
 - Check the **Report Summary** for details, including hcache building time
 - If hcache not precompiled, the report generation time increases
- Check log rates (see *Gathering Log Rate and Device Usage Statistics* slide)
- Check insert rate and receive rate
- Check log insert lag
- Enable auto-cache on report settings →

Enable Schedule	<input type="checkbox"/>
Enable Notification	<input type="checkbox"/>
Enable Auto-cache	<input checked="" type="checkbox"/>

The screenshot shows a list of reports for 'Today (2)'. The first report has its checkbox checked. A context menu is open over this report, with the 'Retrieve Diagnostic' option highlighted by a red box and a red arrow pointing to the 'Report Summary' window on the right.

Report Summary
Sat Oct 14 09:39:07 2023

Number of charts: 9
Number of tables: 4
Number of hcaches requested: 20

HCACHE building time: 1.89s
Rendering time: 1.28s
Total time: 3.17s

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.

DO NOT REPRINT**© FORTINET**

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

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

DO NOT REPRINT

© FORTINET

Empty Reports

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

Name	App-Risk-High-Risk-Application
Log Type	Traffic
Query	<pre>1 select risk as d_risk, behavior as d_behavior, t2.id, t2.name, t2.app_cat, t2.technology, sum(coalesce(senbyte, 0)+coalesce(rcvbyte, 0)) as bandwidth, count(*) as sessions from \$log t1 inner join app_mdata t2 on t1.appid=t2.id where \$filter and (Logflag&1<0) and behavior is not null group by t2.id order by risk desc, sessions desc</pre>

Go Stop				
Time Period		Previous 7 Days		
Devices		All Devices		
d_risk	d_behavior	id	name	app_cat
4	Evasive,Excessive-Bandwidth	6	BitTorrent	P2P
3	Excessive-Bandwidth,Cloud	35421	Dropbox_File.Download	Storage.Backup
3	Excessive-Rawbandwidth,Cloud	38473	Vimeo_Video.Play	Video/Audio

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

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.

DO NOT REPRINT

© FORTINET

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

DO NOT REPRINT

© FORTINET

Lesson Progress



Report Concepts



Generating and Customizing Reports



Customizing Charts and Datasets



Managing Reports



Troubleshooting Reports

Congratulations! You have completed this lesson.

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

DO NOT REPRINT**© FORTINET**

Review

- ✓ Describe the elements that constitute a report
- ✓ Describe how charts extract data from the database
- ✓ Describe how reports function within ADOMs
- ✓ Run and fine-tune predefined reports
- ✓ Customize reports
- ✓ Use macros in reports
- ✓ Customize and create charts and datasets
- ✓ Configure external storage for reports
- ✓ Enable auto-cache
- ✓ Group reports
- ✓ Import and export reports and charts
- ✓ Attach reports to incidents
- ✓ Manage scheduled reports
- ✓ Troubleshoot reports



© Fortinet Inc. All Rights Reserved. 47

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.

DO NOT REPRINT

© FORTINET

FORTINET
Training Institute



FortiAnalyzer Analyst

Playbooks

 FortiAnalyzer 7.4.1

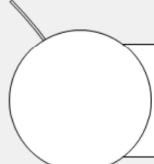
Last Modified: 21 December 2023

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

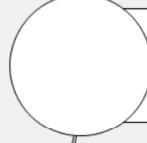
DO NOT REPRINT

© FORTINET

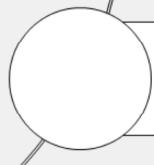
Lesson Overview



Playbook Components



Creating Playbooks



Managing Playbooks

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

DO NOT REPRINT**© FORTINET**

Playbook Components

Objectives

- Understand FortiAnalyzer automation capabilities
- Understand playbook concepts
- Understand trigger types and characteristics
- Understand connector types
- Understand playbook tasks



© Fortinet Inc. All Rights Reserved.

© Fortinet Inc. All Rights Reserved.

3

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

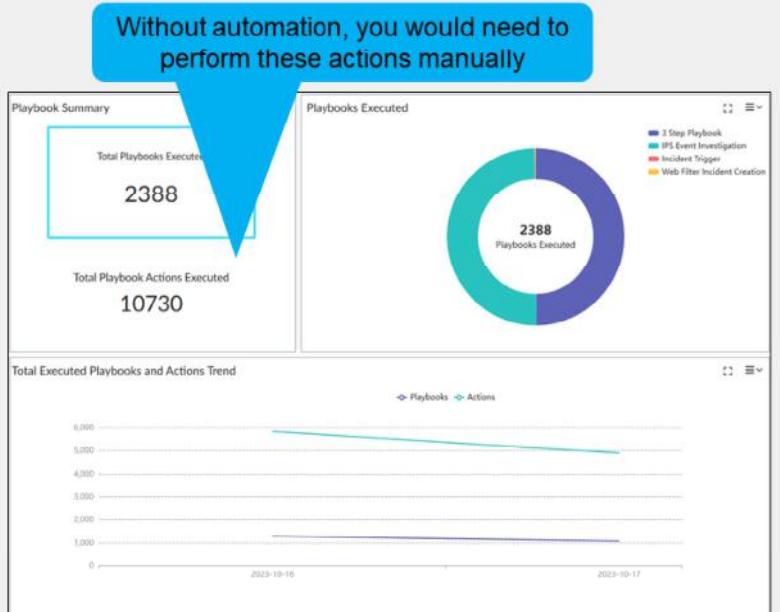
By demonstrating competence in understanding the purpose of playbooks and their components, you will be able to use playbooks effectively.

DO NOT REPRINT

© FORTINET

Why Automation?

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



FORTINET
Training Institute

© Fortinet Inc. All Rights Reserved.

© Fortinet Inc. All Rights Reserved.

4

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.

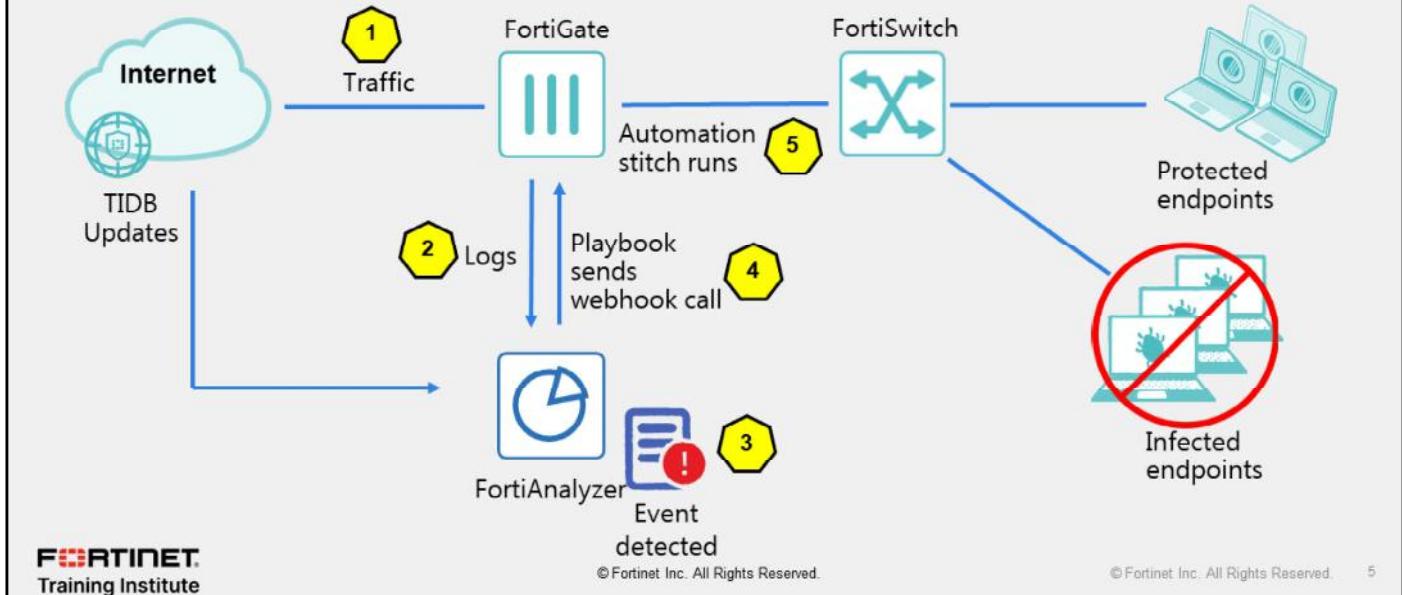
FortiAnalyzer works with standalone devices, but it is also integrated with the Security Fabric. This integration allows FortiAnalyzer to communicate with other devices in the Security Fabric to detect security events, and trigger corrective or preventive actions automatically, by running automated playbooks.

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.

DO NOT REPRINT
© FORTINET

An Example of Automation With a Playbook



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.

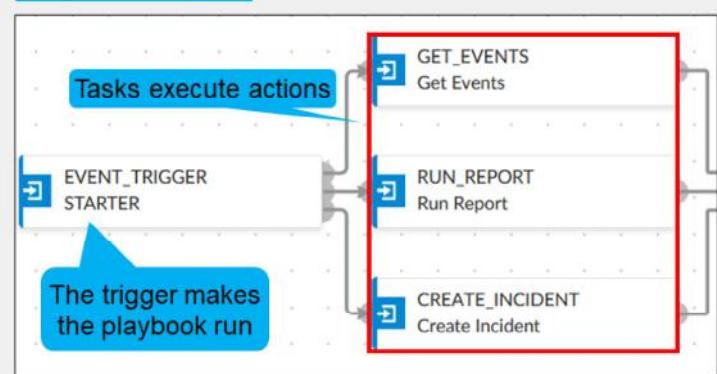
DO NOT REPRINT

© FORTINET

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

Playbook Designer



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



© Fortinet Inc. All Rights Reserved.

© 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.

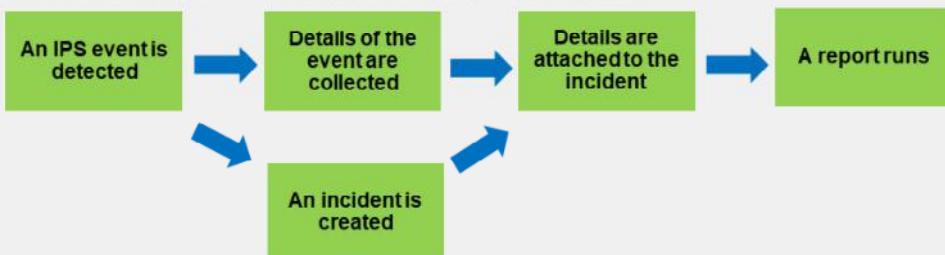
DO NOT REPRINT
© FORTINET

Playbook Concepts (Contd)

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



- Multiple tasks can be triggered
- Tasks can be sequential, or run in parallel
 - The second step has two tasks that run at the same time



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.

DO NOT REPRINT

© FORTINET

Triggers

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



© Fortinet Inc. All Rights Reserved.

© Fortinet Inc. All Rights Reserved.

8

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.

DO NOT REPRINT

© FORTINET

Triggers (Contd)

- A wide variety of categories can be used as filters for the event and incident triggers
 - You can use more than one condition to narrow down when the playbook will run
 - AND (all conditions must match) and OR logic (any condition must match) are supported
- ON_SCHEDULE** triggers parameters are all based on timeframes
- ON_DEMAND** triggers have no extra configurable parameters

The screenshot shows the FortiAnalyzer configuration interface for triggers. It includes three main sections:

- EVENT_TRIGGER**: Filters include Basic Handler Name, Event Time, Threat Type, Device ID, Severity, Endpoint ID, Endpoint Name, Endpoint MAC, and Endpoint IP.
- INCIDENT_TRIGGER**: Filters include Change Types (New), All of the following conditions (MITRE Tech ID), Reporter, Endpoint ID, End User ID, and Endpoint.
- ON_SCHEDULE**: Parameters include The start time of the schedule (10/17/2023), The end time of the schedule (04/30/2024), The interval of the schedule (N-MINUTES), and The frequency of the interval (60).

A blue callout bubble with the text "Available filters depend on the chosen trigger type" points to the filters section of the EVENT_TRIGGER tab.

Example

EVENT_TRIGGER

All of the following conditions

Severity	Equal To	Critical	Remove
Device ID	Equal To	FGVM0123456789	Remove

Add Condition Group | Add Condition

© Fortinet Inc. All Rights Reserved. © Fortinet Inc. All Rights Reserved. 9

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.

DO NOT REPRINT

© FORTINET

Connectors

- Allow playbooks to interact with devices in the Security Fabric and standalone devices
- Determine which actions can be performed by playbook tasks
- Many connector types are available:
 - EMS
 - FortiOS
 - FortiGuard
 - FortiMail
 - FortiCASB
 - Local (FortiAnalyzer)
 - And more
- Only the local connector is ready to be used by default
- The status of each connector is shown:
 - Green: connection successful
 - Black: connection unknown
 - Red: connection down

Fabric View > Automation > Connectors

Automation Rule	Automation Action(s)	Parameters
Lab5 webhook disable FW policy	Lab 5 disable firewall policy	policyid
Lab5 webhook enable FW policy	Lab 5 enable firewall policy	policyid

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.

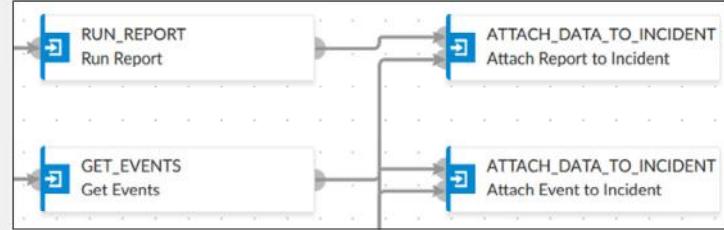
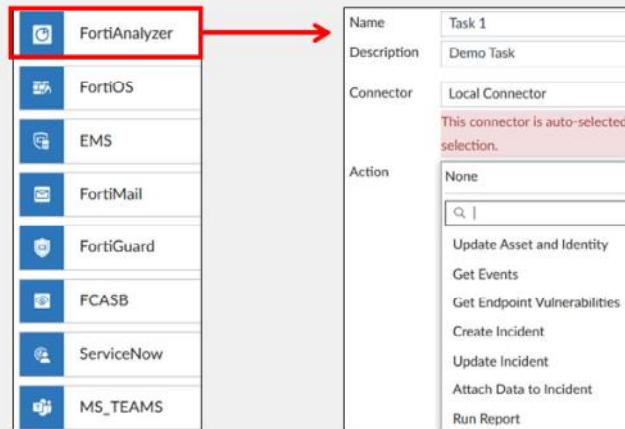
For example, the FortiOS connector will be listed as soon as the first FortiGate device is added to FortiAnalyzer. However, in order to see the actions related to that FortiOS connector, you must enable an automation rule using the **Incoming Webhook Call** trigger on the FortiGate side.

DO NOT REPRINT

© FORTINET

Tasks

- Tasks are the actions that are executed when the playbook runs
- The available actions depend on the connector chosen
- You can chain one task to another task in order to execute a sequence of actions
- The output of a task can be used as the input of the next task in the sequence



FORTINET
Training Institute

© Fortinet Inc. All Rights Reserved.

© Fortinet Inc. All Rights Reserved.

11

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.

DO NOT REPRINT

© FORTINET

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 Inc. All Rights Reserved.

© Fortinet Inc. All Rights Reserved. 12

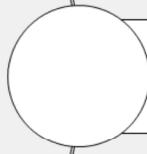
DO NOT REPRINT

© FORTINET

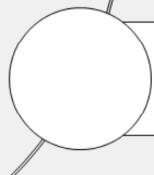
Lesson Overview



Playbook Components



Creating Playbooks



Managing Playbooks

FORTINET
Training Institute

© Fortinet Inc. All Rights Reserved.

© Fortinet Inc. All Rights Reserved.

13

Good job! You now understand playbook components.

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

DO NOT REPRINT**© FORTINET**

Creating Playbooks

Objectives

- Create new playbooks from a template
- Customize playbooks settings
- Create new playbooks from scratch
- Understand the use of variables in tasks



© Fortinet Inc. All Rights Reserved.

© Fortinet Inc. All Rights Reserved.

14

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.

DO NOT REPRINT
© FORTINET

Creating Playbooks From a Template

- FortiAnalyzer includes several playbook templates
- Playbooks created from these templates can be customized to fit your needs

Summary		Connectors	Playbook	Playbook Monitor	
		<input type="button" value="Run"/>	<input checked="" type="button" value="Edit"/>	<input type="button" value="Delete"/>	<input checked="" type="button" value="Enable"/>
<input type="checkbox"/>	Name				
<input type="checkbox"/>	Incident Trigger				
<input type="checkbox"/>	Sample Playbook				

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

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

FORTINET
 Training Institute

© Fortinet Inc. All Rights Reserved.

© Fortinet Inc. All Rights Reserved.

15

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.

DO NOT REPRINT
© FORTINET

Customizing Playbook Settings

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



© Fortinet Inc. All Rights Reserved.

© Fortinet Inc. All Rights Reserved.

16

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.

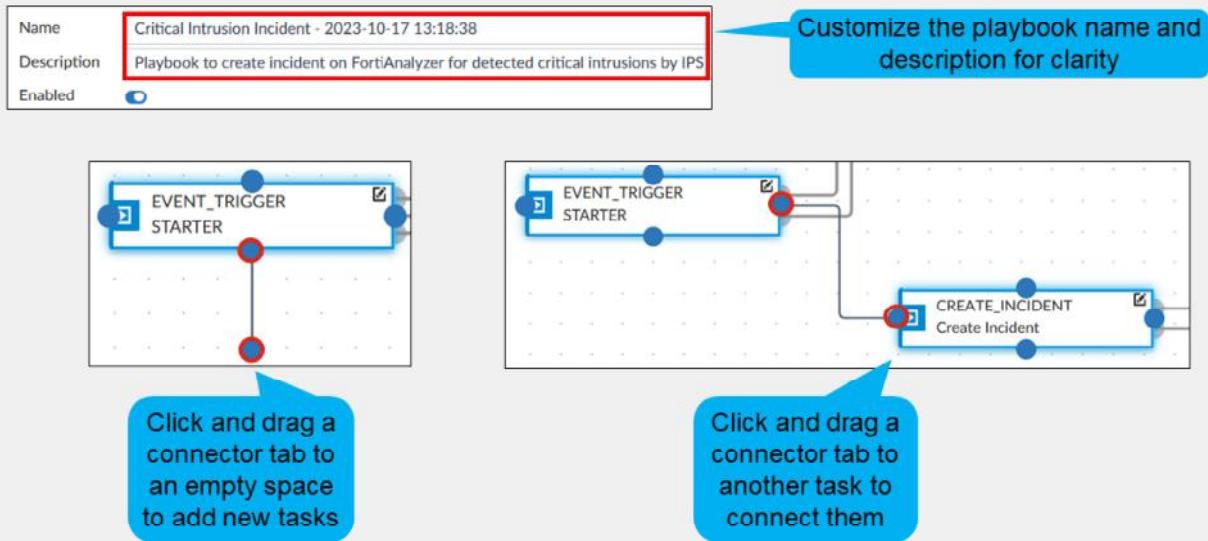
Note that to be able to run a report as a task, that report must already exist, and it must have both auto-cache and extended log filtering enabled.

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.

DO NOT REPRINT
© FORTINET

Customizing Playbook Settings (Contd)



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.

DO NOT REPRINT
© FORTINET

Creating a New Playbook From Scratch

The screenshot shows the FortiAnalyzer interface for creating a new playbook. At the top, there's a navigation bar with tabs: Summary, Connectors, Playbook (which is selected), and Playbook Monitor. Below the navigation bar is a button labeled '+ Create New'.

A modal window titled 'Choose from Playbook Templates' is open, showing two options:

- New Playbook created from scratch**: Described as a 'Custom build playbook to get started'.
- Attach Endpoint Vulnerability list to incident**: Described as a 'Playbook to collect the list of endpoint vulnerab'.

An arrow points from the 'New Playbook created from scratch' option to the 'Edit Playbook' section below.

The 'Edit Playbook' section has fields for Name (set to 'New Playbook created from scratch'), Description (set to 'Custom build playbook to get started'), and Enabled (checkbox checked). It also includes a note: 'FortiAnalyzer needs a few minutes to parse a newly created playbook'.

In the 'Edit Playbook' section, there's a placeholder box labeled 'ON_DEMAND Select a Step'.

On the right side of the interface, under 'TRIGGERS', there are four options: EVENT_TRIGGER, INCIDENT_TRIGGER, ON_SCHEDULE, and ON_DEMAND.

At the bottom of the interface, a red error message box states: 'Server error: FAZ is parsing the recent created playbook: 301f8fc9-7831. Please wait for about 5 minutes.'

At the bottom left is the Fortinet Training Institute logo. At the bottom right are copyright notices: '© Fortinet Inc. All Rights Reserved.' and '18'.

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.

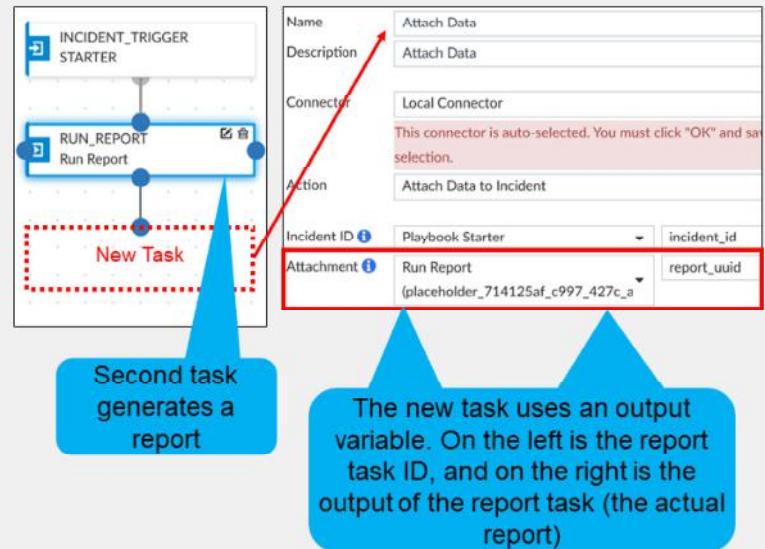
Also, keep in mind that after you create a new playbook, FortiAnalyzer will need a few minutes to parse it. For example, if you try to run a newly created playbook configured with an ON_DEMAND trigger before it is parsed, you will see an error, like the one shown on the slide, telling you why the playbook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

DO NOT REPRINT

© FORTINET

Using Variables in Tasks

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



FORTINET
Training Institute

© Fortinet Inc. All Rights Reserved.

© Fortinet Inc. All Rights Reserved.

19

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.

DO NOT REPRINT**© FORTINET**

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 Inc. All Rights Reserved.

© Fortinet Inc. All Rights Reserved. 20

DO NOT REPRINT

© FORTINET

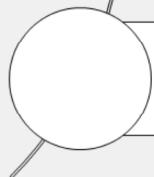
Lesson Overview



Playbook Components



Creating Playbooks



Managing Playbooks

FORTINET
Training Institute

© Fortinet Inc. All Rights Reserved.

© Fortinet Inc. All Rights Reserved.

21

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

Now, you will learn how to manage playbooks.

DO NOT REPRINT

© FORTINET

Managing Playbooks

Objectives

- Monitor playbooks
- Export and import playbooks



© Fortinet Inc. All Rights Reserved.

© Fortinet Inc. All Rights Reserved.

22

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.

DO NOT REPRINT

© FORTINET

Monitoring Playbooks

- To see the details of a playbook job, click **Details** and then **View Log**

Fabric View > Automation > Playback Monitor

Playbook	Trigger	Start Time	Status	Details
Create 2 Incidents	user(admin)	2023-10-17 15:07	failed(Scheduled:0/Running:0/Success:1/Failed:1)	
placeholder_7a3688b5_fca3_4bad	Create Incident 1	2023-10-17 15:07:14-0700	2023-10-17 15:07:15-0700	failed
placeholder_9ad9c67b_7957_48a	Create Incident 2	2023-10-17 15:07:14-0700	2023-10-17 15:07:15-0700	success

[2023-10-17T15:07:15.076-0700] {taskinstance.py:1824} ERROR - Task failed with exception
 Traceback (most recent call last):
 File "/drive0/private/airflow/plugins/incident_operator.py", line 223, in execute
 self.euid = int(FAZUtilSOoperator.parse input(context, self.euid, context dict))
 TypeError: int() argument must be a string, a bytes-like object or a number, not 'NoneType'
[2023-10-17T15:07:15.158-0700] {standard_task_runner.py:104} ERROR - Failed to execute job 16119 for task placeholder_7a3688b5_fca3_4bad_88cf_b448da08cde2 (int()) argument must be a string, a bytes-like object or a number, not 'NoneType'; 21500

This playbook has two tasks:
 one task ran successfully but the other one failed

This playbook failed because one task was expecting a value for the euid field, but it received nothing

Training Institute

© Fortinet Inc. All Rights Reserved.

© Fortinet Inc. All Rights Reserved. 23

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 **Playback 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 **Playback Monitor**. A failed status, however, does not mean that all tasks failed. Some individual actions may have completed successfully.

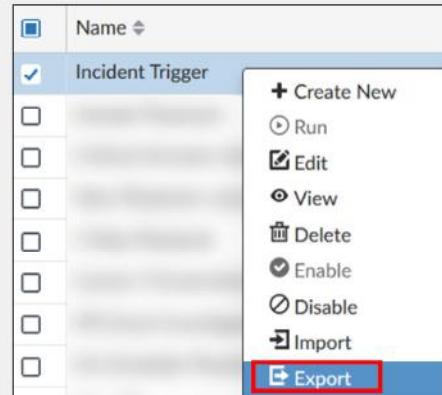
In the example shown on the slide, the playbook has two tasks configured and only the task named `Create incident 1` failed to run. Therefore, the playbook job is considered to have failed. The specific reason for the failure in the example is that the end user ID field expects a value; however, none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

DO NOT REPRINT

© FORTINET

Exporting Playbooks

- Playbooks are defined per ADOM
- Export the playbooks that are to be used in a different ADOM or device
- The connectors can be included in the exported file
- The resulting file uses a JSON format
 - You can choose to compress the file



Including the
connectors ensures all
required components
are exported

Playbooks are defined per ADOM. If you want to use an existing playbook 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.

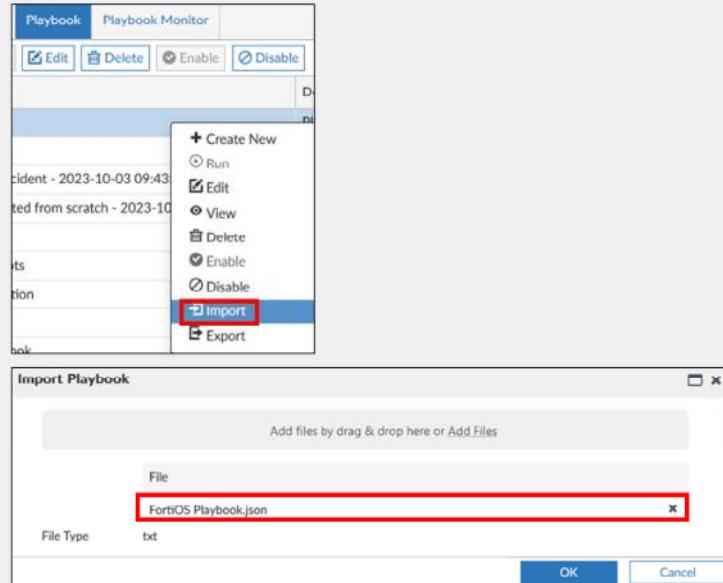
If you need to be able to read the contents of the JSON file in plain text, you must choose the text version during the export process.

DO NOT REPRINT

© FORTINET

Importing Playbooks

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



FORTINET
Training Institute

© Fortinet Inc. All Rights Reserved.

© Fortinet Inc. All Rights Reserved.

25

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.

DO NOT REPRINT
© FORTINET

Playbooks Dashboard

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



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.

DO NOT REPRINT

© FORTINET

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 Inc. All Rights Reserved.

© Fortinet Inc. All Rights Reserved. 27

DO NOT REPRINT

© FORTINET

Lesson Overview



Playbook Components



Creating Playbooks



Managing Playbooks

FORTINET
Training Institute

© Fortinet Inc. All Rights Reserved.

© Fortinet Inc. All Rights Reserved.

28

Congratulations! You have completed this lesson.

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

DO NOT REPRINT**© FORTINET**

Review

- ✓ Understand FortiAnalyzer automation capabilities
- ✓ Understand playbooks concepts
- ✓ Understand trigger types and characteristics
- ✓ Understand connector types
- ✓ Create new playbooks
- ✓ Understand the use of variables in tasks
- ✓ Monitor playbooks
- ✓ Export and import playbooks



© Fortinet Inc. All Rights Reserved.

© Fortinet Inc. All Rights Reserved. 29

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 to create them to automate tasks in FortiAnalyzer. You also learned how to monitor and manage playbooks.

DO NOT REPRINT
© FORTINET



FORTINET®



No part of this publication may be reproduced in any form or by any means or used to make any derivative such as translation, transformation, or adaptation without permission from Fortinet Inc., as stipulated by the United States Copyright Act of 1976.

Copyright© 2023 Fortinet, Inc. All rights reserved. Fortinet®, FortiGate®, FortiCare® and FortiGuard®, and certain other marks are registered trademarks of Fortinet, Inc., in the U.S. and other jurisdictions, and other Fortinet names herein may also be registered and/or common law trademarks of Fortinet. All other product or company names may be trademarks of their respective owners. Performance and other metrics contained herein were attained in internal lab tests under ideal conditions, and actual performance and other results may vary. Network variables, different network environments and other conditions may affect performance results. Nothing herein represents any binding commitment by Fortinet, and Fortinet disclaims all warranties, whether express or implied, except to the extent Fortinet enters a binding written contract, signed by Fortinet's General Counsel, with a purchaser that expressly warrants that the identified product will perform according to certain expressly-identified performance metrics and, in such event, only the specific performance metrics expressly identified in such binding written contract shall be binding on Fortinet. For absolute clarity, any such warranty will be limited to performance in the same ideal conditions as in Fortinet's internal lab tests. In no event does Fortinet make any commitment related to future deliverables, features, or development, and circumstances may change such that any forward-looking statements herein are not accurate. Fortinet disclaims in full any covenants, representations, and guarantees pursuant hereto, whether express or implied. Fortinet reserves the right to change, modify, transfer, or otherwise revise this publication without notice, and the most current version of the publication shall be applicable.

<https://t.me/learningnets>