

Exercise 8: Creating a Report

In this exercise, you will create a report to summarize your findings in this lab. While this exercise includes specific steps to create, customize, and generate a report, you are encouraged to try and make it your own. The following table contains some general steps that you can follow if you decide to create your own report:

Topic	Content
Introduction	Write at least a paragraph to summarize what the report is about. You can focus on one element of the lab exercises, such as discovered software vulnerabilities, attack vectors, network misconfigurations, or have a broader focus.
Scope	Be mindful of the scope and length of the report. For the purposes of this exercise, you should limit it to fewer than four pages. Add at least one chart to the report. You can create your own, use an existing one, or customize one.
Charts	You can use the chart builder function on FortiAnalyzer to help you build a chart and a dataset together, or manually create both separately. Select charts that are logical for the data you want to present.
Macros	Add at least one macro to the report. You can create your own, use an existing one, or customize one. Select macro units (for example, bandwidth) that are logical for the data you want to present.
Customization	Try to customize the report, such as by applying a different title page, adjusting the headers, and more.
Schedule	Configure a schedule to generate the report based on a set interval. You can still generate the report on-demand.

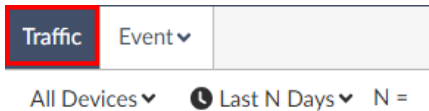
Create a Report

In this sample report, you will focus on one aspect of the attack against ACME Corp. You will review the SSH connection attempts to the DMZ, and then include your findings in the report, including listing suspicious traffic flows, network misconfiguration, and recommendations to improve security. By creating a report, you will get hands-on experience with creating a dataset, a chart, and a macro, and organizing them in the layout editor of your report.

Then, you will schedule this report to run daily.

To confirm the logs are present

- On the bastion host, in Chrome, log in to the FAZ-SiteB (10.200.4.238) GUI with the following credentials:
 - Username: admin
 - Password: Fortinet1!
- Click **Log View > FortiGate**.
- Click the **Traffic** tab.



- Click **More Columns** to customize which columns to display.

To create a dataset

1. Click **Reports > Report Definitions**.
2. Click the **Datasets** tab.
3. Click **Create New**.
4. Configure the following settings:

Field	Value
Name	SSH Attempts
Log Type	Traffic (under FortiGate)
Query	<pre>SELECT `dstip` AS `Target`, `srcip` AS `Source`, count(*) AS `SSH Connection Attempts` FROM \$log WHERE \$filter AND (lower(`service`) = lower('ssh')) AND (`srcip` = inet('10.200.3.1')) AND (`dstip` << inet('10.200.200.0/24')) GROUP BY `dstip`, `srcip` ORDER BY `Target` ASC</pre>

On the bastion host, in the **Desktop > Resources > SQL Queries** folder, there is an SSH Attempt Dataset.sql file with the query above saved. If you prefer, you can open that file in Notepad++, and then copy and paste the text into the **Query** field.



To break down the query, it is looking for SSH traffic sourced from 10.200.3.1 to any destination in the 10.200.200.0/24 subnet. Note also that the column names are changed by using the AS keyword in the SELECT clause.

5. Click **Validate** to ensure the query is correct.

Validate Result

No Validation Issues Found

6. In the **Time Period** field, select an appropriate time range.

For the purposes of report generation, time periods starting with **Previous** *do not* include logs from the current day. Instead, select periods such as **Today** or **This Week** to include the current day.



You also have the option to specify a custom time range.

7. Click **Go** to test the query.

Go

Stop

Time Period

This Month

Devices

All Devices ▼

Target	Source	SSH Connection Attempts
10.200.200.12	10.200.3.1	37
10.200.200.100	10.200.3.1	6
10.200.200.213	10.200.3.1	6
10.200.200.238	10.200.3.1	6

You should see results.

8. Click **OK** to save the dataset.

To create a chart

- 1. Click **Reports > Report Definitions**.
- 2. Click the **Chart Library** tab.
- 3. Click **Create New**.
- 4. Configure the following settings:

Section	Field	Value
Commo n	Name	SSH Attempts
	Dataset	SSH Attempts
	Type	Pie
Categor y	Data	Target
	Bindings	
Series	Data	SSH Connection
	Bindings	Attempts
	Format	Counter (K/M/G)

Common

Name

SSH Attempts

Description

Dataset

SSH Attempts

Resolve Hostname

Inherit

Type

Pie

Bundle rest into "Others"

☒

Category

Data Bindings

Target

Show Top (0 for all)

5

Label

Series

Data Bindings

SSH Connection Attempts

Format

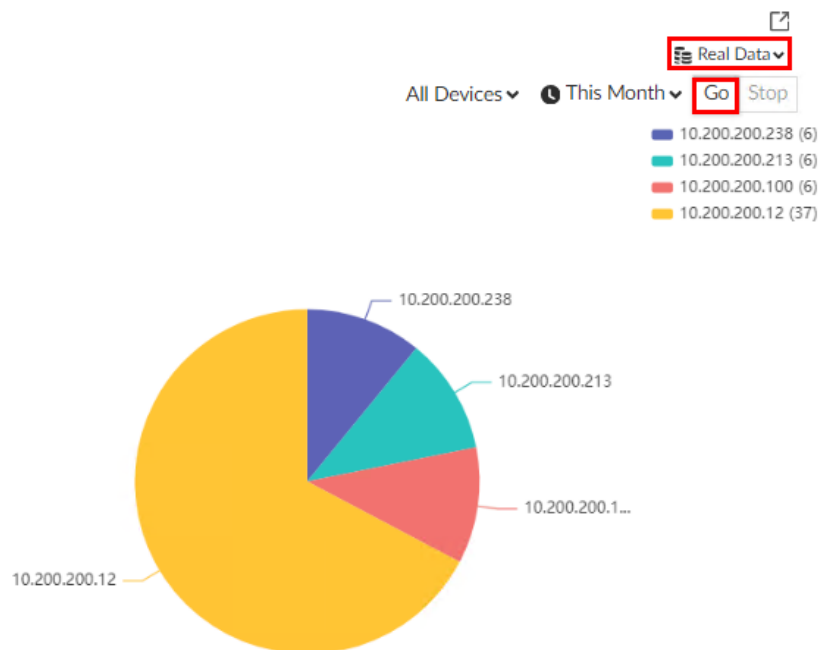
Counter (K/M/G)

Label

5. Change the data type to **Real Data**, and then in the **Time Period** drop-down list, select an appropriate time range.

If you are expecting matching logs on the same day, do not select a time range starting with **Previous**.

6. Click **Go**.



You should see a pie chart.

7. Click **OK** to save the chart.

To create a macro

1. Click **Reports > Report Definitions**.
2. Click the **Macro Library** tab.
3. Click **Create New**.
4. Configure the following settings:

Field	Value
Name	SSH Bandwidth
Dataset	SSH-Bandwidth-Domain-Controller
Data Binding	Total Bandwidth
Display	Bandwidth (KB/MB/GB)

Name	SSH Bandwidth
Description	
Dataset	SSH-Bandwidth-Domain-Controller
Query	<pre> select app_group_name(app) as Application, sum(bandwidth) as `Total Bandwidth` from (select app, sum(coalesce(rcvddelta, rcvdbyte, 0) + coalesce(sentdelta, sentbyte, 0)) as bandwidth from \$log-traffic where \$filter AND (`srcip` = inet('10.200.3.1')) -- Filter for specific source IP AND (lower(`service`) = lower('ssh')) -- Filter for SSH service group by app) base group by app_group_name(app), app </pre>
Data Binding	Total Bandwidth
Display	Bandwidth (KB/MB/GB)

 The **SSH-Bandwidth-Domain-Controller** dataset is cloned and modified from the default **Top-App-By-Bandwidth** dataset.

5. Click **OK** to save the macro.

To create a new report

- 1. Click **Report Definitions > All Reports**.
- 2. Click **Report > Create New**.
- 3. Configure the following settings:

Field	Value
Name	SOC Analyst Report
Create from	Blank
Save to Folder	All Reports

4. Click **OK**.

Format and Configure the Report

After you have created the different elements, such as a dataset, a chart, a macro, and a blank report, it is time to put all of them together. You will use the editor to format the report and insert the elements that you created in the previous steps. Then, you will customize the report to your needs before creating a schedule and generating the report.

To format the report using the editor

- 1. Click the **Editor** tab.
- 2. Click **Normal** to change the style to **Heading 1**.

3. Type Summary, and then press Enter.
4. Change the style back to **Normal**.
5. Type the following text:

The SOC team, as part of the company's mandated security audit, was able to establish unauthorized SSH connections to the DMZ, sourced from the domain controller WIN-AD. This matter requires urgent remediation detailed in this report.

The red team was able to compromise a user machine using an infected document file. After gaining access to the user machine, the attacker proceeded to move to the domain controller, where it probed the network for accessible resources. Upon further review, it was determined that the ISFW is misconfigured, with the web server not included in the list of destination of traffic to be blocked.

There is a separate report for the initial access exploit. This report focuses on the SSH security issue.

You can change the summary in any way you prefer, including shortening the summary.



Optionally, you can also take screenshots of identified security misconfigurations, and then insert them using the editor.

Summary

The SOC team, as part of the company's mandated security audit, was able to establish unauthorized SSH connections to the DMZ, sourced from the domain controller WIN-AD. This matter requires urgent remediation detailed in this report.

The red team was able to compromise a user machine using an infected document file. After gaining access to the user machine, the attacker proceeded to move to the domain controller, where it probed the network for accessible resources. Upon further review, it was determined that the ISFW is misconfigured, with the web server not included in the list of destination of traffic to be blocked.

There is a separate report for the initial access exploit. This report focuses on the SSH security issue.]

Misconfigured Policy

Edit Policy

Name ⓘ

LAN to DMZ

Incoming interface

port1

+

×

Outgoing interface

port3

+

×

6. Change the style back to **Heading 1**.
7. Type Findings, and then press Enter.
8. Change the style back to **Normal**.
9. Type the following text:

The SOC team could see many SSH connection attempts initiated by the domain controller:

10. Click **Insert Chart**.
11. In the second field, search for SSH Attempts.

Chart

All

SSH Attempts

Edit Chart

Clone Chart

Title

{default}

Width (px / %)

100%

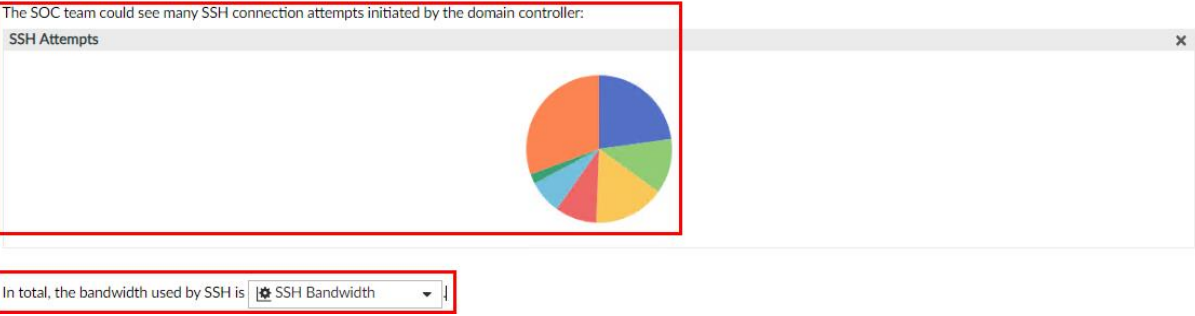
Filters

12. Click **OK**.
13. Type the following text:

In total, the bandwidth used by SSH is

14. Click **Insert Macro**.
15. Select **SSH Bandwidth**.

Findings



16. Change the style back to **Heading 1**.
17. Type Remediation, and then press Enter.
18. Change the style back to **Normal**.
19. Type the following text:
- The domain controller should be segmented from the LAN network
 - Properly restrict SSH access from the LAN to the DMZ
 - Disable SSH TCP forwarding on all network devices unless explicitly required

Remediation

- The domain controller should be segmented from the LAN network
- Properly restrict SSH access from the LAN to the DMZ
- Disable SSH TCP forwarding on all network devices unless explicitly required

20. Click **Apply** to save the report.

To customize the report settings

1. Click the **Settings** tab.
2. In the **Time Period** field, select an appropriate time range.

Generated Reports **Settings** Editor

Path All Reports

Name SOC Analyst Report

Time Zone Default

Time Period **This Month**

07/01/2024 00:00:00 - 07/31/2024 23:59:59 (for example)

Devices ☒ All Devices ☐ Specify

Subnets ☒ All Subnets ☐ Specify

☐ Generate separate report per-device/VDOM

Again, if you want to include today's data, do not select time periods that start with **Previous**.

3. Select the **Enable Schedule** checkbox.
4. Configure the following settings:

Field	Value
Generate Report Every	1 Weeks
Start Time	The current date and time
End Time	Never

Enable Schedule

☒

Generate Report Every

1

Weeks

Start Time

2024-07-29


09:50:13 PM

End Time

☒ Never

☐ Specify

5. Click **Advanced Settings**.

 You do not have to follow these steps for customizing the report. You are encouraged to try different combinations to see what they do.

6. Select the **Layout Header** checkbox.

7. In the **Header Text** field, type ACME Corp.

Chart Heading Level

Heading 2

Default Font

Open Sans

Hide # Column

☐

Layout Header

☒

Header Text

ACME Corp

Header Image

Select Image fortinet_logo.png

Layout Footer

☐

Print Cover Page

☒ Edit Cover Page

Print Table of Contents

☒

Print Device List

☒ Compact

Display Device Name

By Device Name

Print Report Filters

☒

Obfuscate User

☐

Resolve Hostname

☐

Date Format

Default


Allow save maximum

99

8. In the **Print Cover Page** field, click **Edit Cover Page**.

9. In the **Custom Text 1** field, type SSH Incident.

Edit Cover Page



Background Image

Select Image def_cover_bgimg_defv2.png

Top Image

Select Image

Top Image Position

Center

Text Color

Black

☒ Show Creation Time

☒ Show Data Range

Report Title

{default}

Custom Text 1

SSH Incident

Custom Text 2

Bottom Image

Select Image

Footer Left Text

Footer Right Text

Footer Background Color

Transparent

Reset to Default

OK

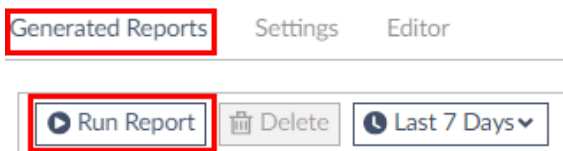
Cancel

10. Click **OK**.


11. Click **Apply**.

To generate a report on demand

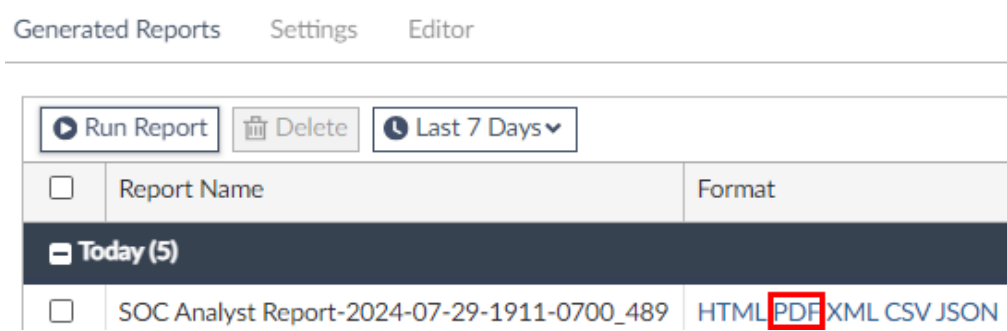
1. Click the **Generated Reports** tab.
2. Click **Run Report**.



3. Wait for the report to generate.

 Even though you scheduled a weekly report, you will generate an on-demand report to save time.

4. In the **Format** field, click **PDF** to open the report.



5. Review the report.



Table of Contents

Summary	2
Findings	2
SSH Attempts	3
Remediation	3
Appendix A	4
Devices (6)	4

Summary

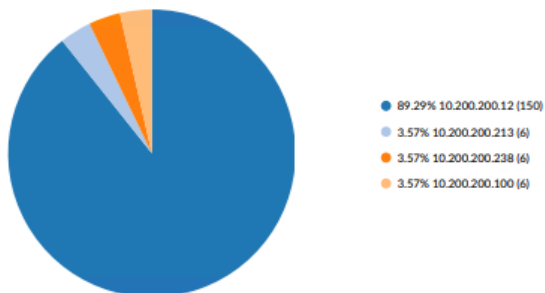
The SOC team has identified unauthorized SSH connections to the DMZ, sourced from the domain controller WIN-AD. This matter requires urgent attention.

The attacker compromised a user machine using an infected word file. After gaining access to the user machine, the attacker proceeded to move to the domain controller, where it probed the network for accessible resources. Upon further review, it was determined that the ISFW is misconfigured, with the web server not included in the list of destination of traffic to be blocked.

Edit Policy

Name <i>i</i>	LAN to DMZ
Incoming interface	port1 + ×
Outgoing interface	port3 + ×
Source	SiteB-LAN + ×
Security posture tag <i>i</i>	+
Destination	<div> FortiMail ×</div> <div> FortiSandbox ×</div> <div> FortiAnalyzer ×</div> <div>+</div>
Schedule	always ▼
Service	<div> SSH ×</div> <div> HTTPS ×</div>

SSH Attempts



The total bandwidth used by SSH is 4.28 MB .

Your report may look different, but it should contain at least some of these elements.

LAB-CHALLENGE > Creating a Report