Exercise 2: Configuring Detection RulesLab 3: Detection Capabilities

Exercise 2: Configuring Detection Rules

In this exercise, you will work with FortiAnalyzer custom handlers to detect and trigger events for specific aspects of the adversary Group ABC behaviors.

Configure Custom Handlers

You will configure a data selector and some custom event handlers on FortiAnalyzer. These custom event handlers cover the following aspects of Group ABC behaviors:

- Reconnaissance using the **Gather Victim Identity Information** subtechnique
- Initial access using the **Spearphishing Attachment** subtechnique

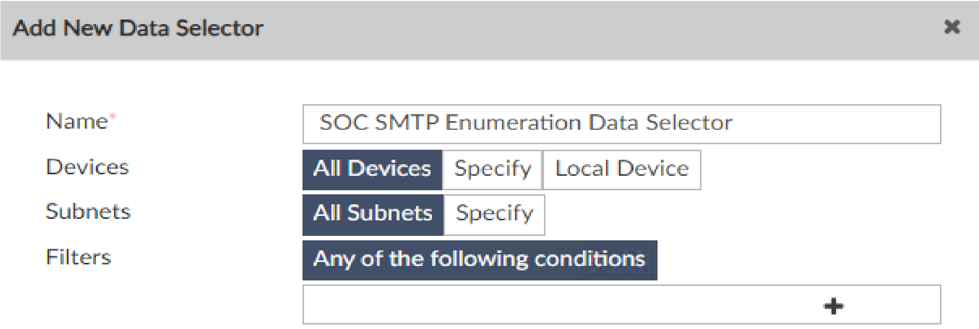
To configure the data selector

1. On the bastion host, in Chrome, log in to the FAZ-SiteB GUI (10.200.4.238) with the following credentials:

- Username: admin
- Password: Fortinet1!

2. Click **Incidents & Events** > **Handlers**.
3. On the **Data Selectors** tab, click **Create New**.
4. In the **Add New Data Selector** window, configure the following settings:

Field	Value
Name	SOC SMTP Enumeration Data Selector
Devices	All Devices
Subnets	All Subnets
Filters	Any of the following conditions



Add New Data Selector

Name* SOC SMTP Enumeration Data Selector

Devices: All Devices | Specify | Local Device

Subnets: All Subnets | Specify

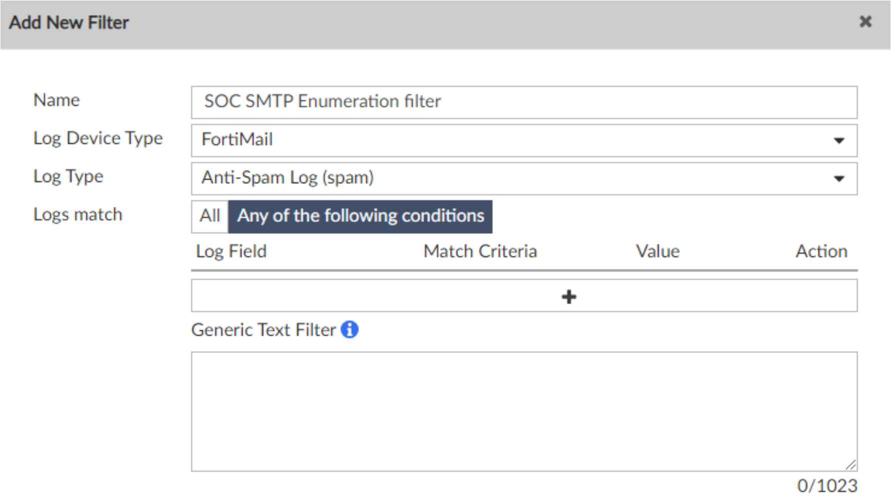
Filters: Any of the following conditions

5. Click **+** to add a new filter.
6. In the **Add New Filter** window, configure the following settings:

Field	Value
Name	SOC SMTP Enumeration filter
Log Device Type	FortiMail
Log Type	Anti-Spam Log (spam)
Logs match	Any of the following conditions

7. Click **x** to remove the default **Logs match** conditions.

Your configuration should match the following example:



Add New Filter

Name: SOC SMTP Enumeration filter

Log Device Type: FortiMail

Log Type: Anti-Spam Log (spam)

Logs match: All | Any of the following conditions

Log Field	Match Criteria	Value	Action

Generic Text Filter

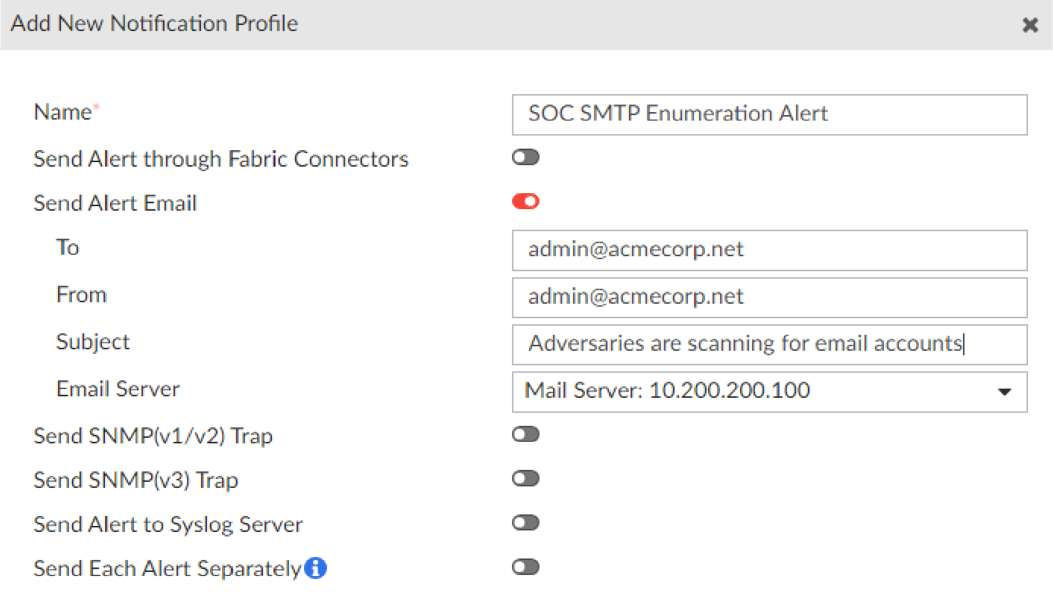
0/1023

8. Click **OK**.
9. Click **OK**.

To configure the notification profile

1. Continuing on the FAZ-SiteB GUI, click the **Notification Profile** tab.
2. Click **Create New**.
3. Configure the following settings:

Field	Value
Name	SOC SMTP Enumeration Alert
Send Alert Email	Enabled
To	admin@acmecorp.net
From	admin@acmecorp.net
Subject	Adversaries are scanning for email accounts
Email Server	Mail Server: 10.200.200.100



Add New Notification Profile

Name*: SOC SMTP Enumeration Alert

Send Alert through Fabric Connectors: ○

Send Alert Email: ●

To: admin@acmecorp.net

From: admin@acmecorp.net

Subject: Adversaries are scanning for email accounts

Email Server: Mail Server: 10.200.200.100

Send SNMP(v1/v2) Trap: ○

Send SNMP(v3) Trap: ○

Send Alert to Syslog Server: ○

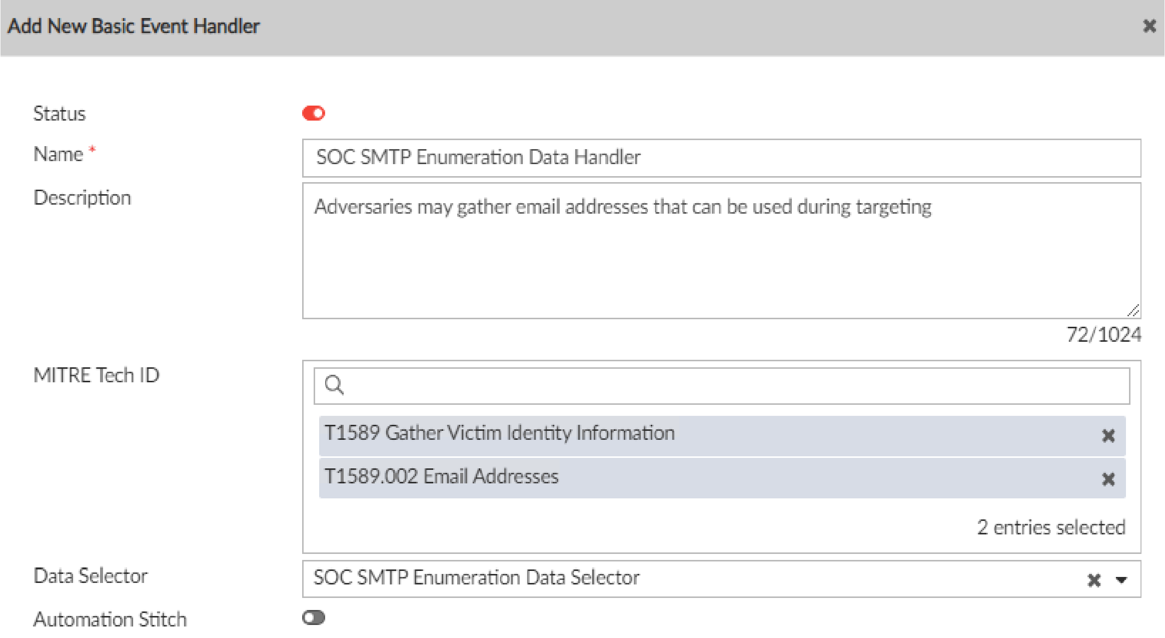
Send Each Alert Separately: ○

4. Click **OK**.

To configure custom event handlers to detect SMTP enumeration

1. Continuing on the FAZ-SiteB GUI, click the **Basic Handlers** tab.
2. Click **Create New**.
3. Configure the following settings:

Field	Value
Status	Enabled
Name	SOC SMTP Enumeration Data Handler
Description	Adversaries may gather email addresses that can be used during targeting
MITRE Tech ID	T1589 Gather Victim Identity Information T1589.002 Email Addresses
Data Selector	SOC SMTP Enumeration Data Selector



Add New Basic Event Handler ✖

Status ●

Name * SOC SMTP Enumeration Data Handler

Description Adversaries may gather email addresses that can be used during targeting

72/1024

MITRE Tech ID

T1589 Gather Victim Identity Information ✖

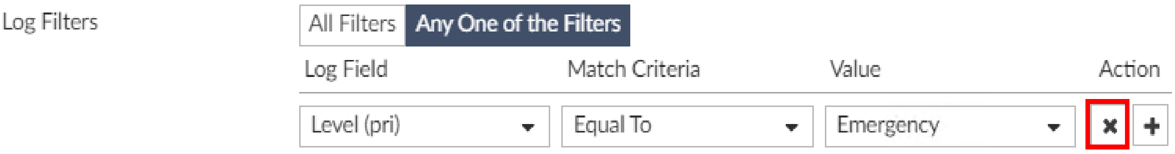
T1589.002 Email Addresses ✖

2 entries selected

Data Selector SOC SMTP Enumeration Data Selector ✖ ▾

Automation Stitch ○

4. In the **Rules** section, click **Add New Rule**.
5. Click **x** to remove the default values in the **Log Field**, **Match Criteria**, **Value**, and **Action** fields.

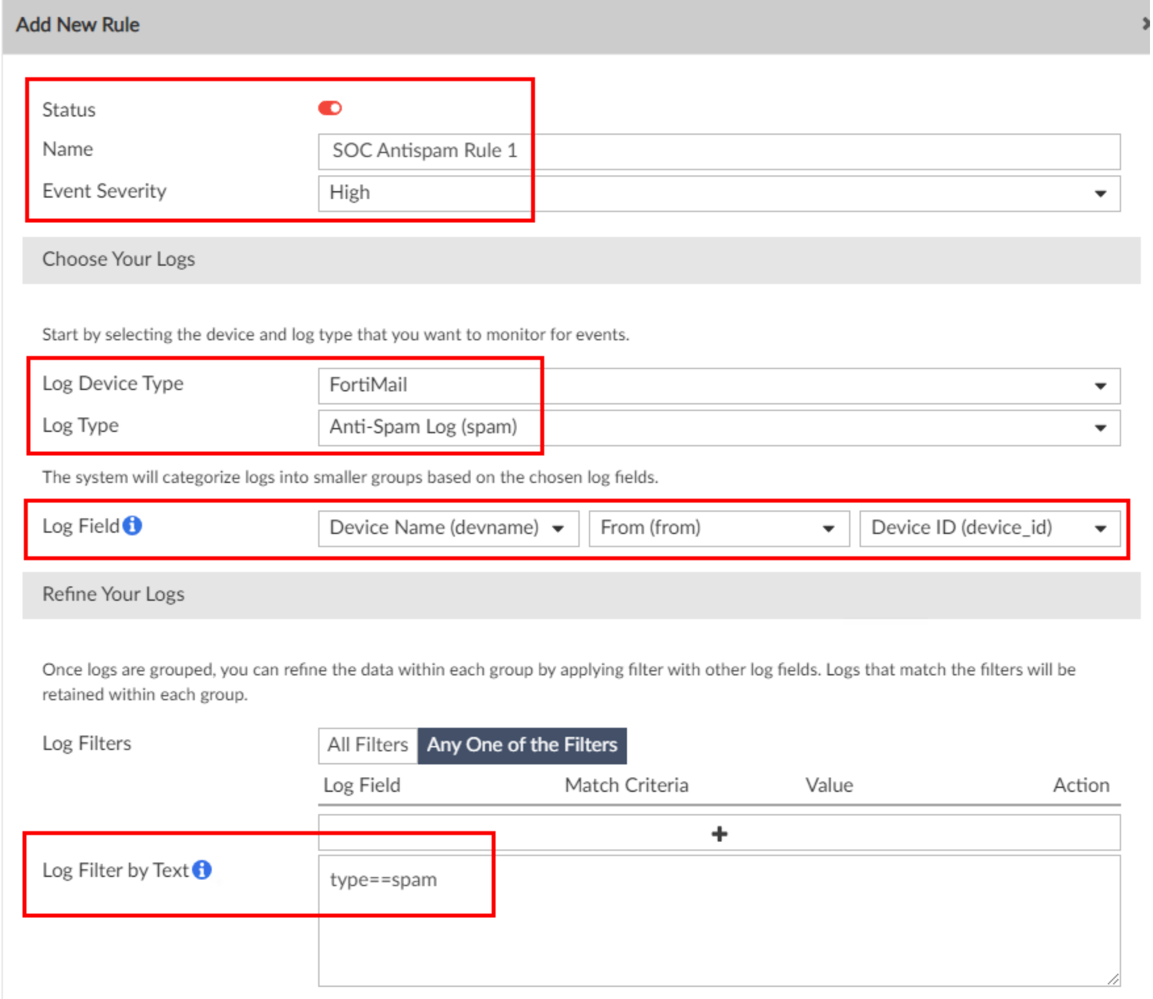


Log Filters All Filters | Any One of the Filters

Log Field	Match Criteria	Value	Action
Level (pri) ▾	Equal To ▾	Emergency ▾	✖ ✚

6. In the **Add New Rule** window, configure the following settings:

Field	Value
Status	Enabled
Name	SOC Antispam Rule 1
Event Severity	High
Log Device Type	FortiMail
Log Type	Anti-Spam Log (spam)
Log Field	Device Name (devname) | From (from) | Device ID (device_id)
Log Filters	Any One of the Filters
Log Filter by Text	type==spam
Trigger an event when	A group contains 10 or more log occurrences



Add New Rule

Status ●

Name: SOC Antispam Rule 1

Event Severity: High

Choose Your Logs

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

Log Device Type: FortiMail

Log Type: Anti-Spam Log (spam)

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

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

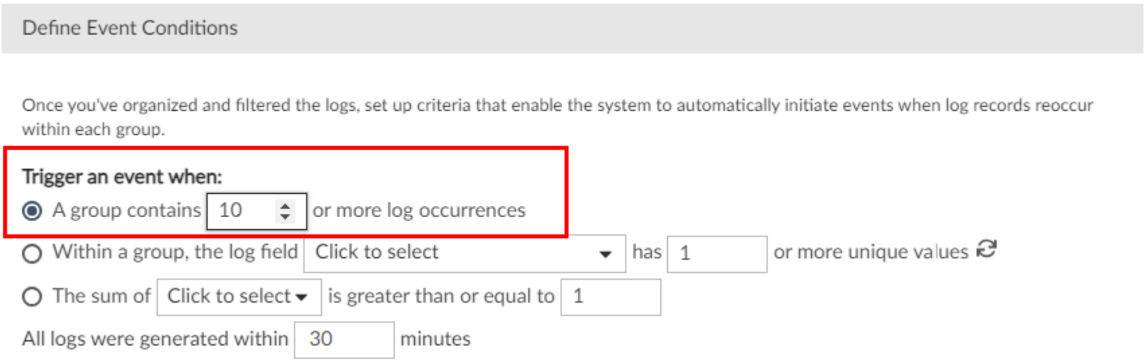
Refine Your Logs

Once logs are grouped, you can refine the data within each group by applying filter with other log fields. Logs that match the filters will be retained within each group.

Log Filters: All Filters | **Any One of the Filters**

Log Field	Match Criteria	Value	Action
+			

Log Filter by Text: type==spam



Define Event Conditions

Once you've organized and filtered the logs, set up criteria that enable the system to automatically initiate events when log records reoccur within each group.

Trigger an event when:

● A group contains 10 or more log occurrences

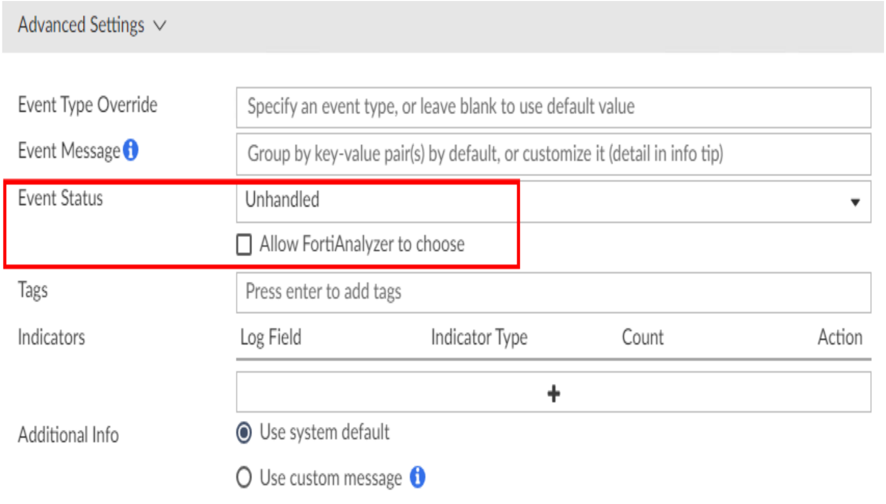
○ Within a group, the log field Click to select has 1 or more unique values

○ The sum of Click to select is greater than or equal to 1

All logs were generated within 30 minutes

7. Click **Advanced Settings**.
8. Configure the following settings:

Field	Value
Allow FortiAnalyzer to choose	Clear the checkbox.
Event Status	Unhandled



Advanced Settings ∨

Event Type Override: Specify an event type, or leave blank to use default value

Event Message: Group by key-value pair(s) by default, or customize it (detail in info tip)

Event Status: Unhandled

□ Allow FortiAnalyzer to choose

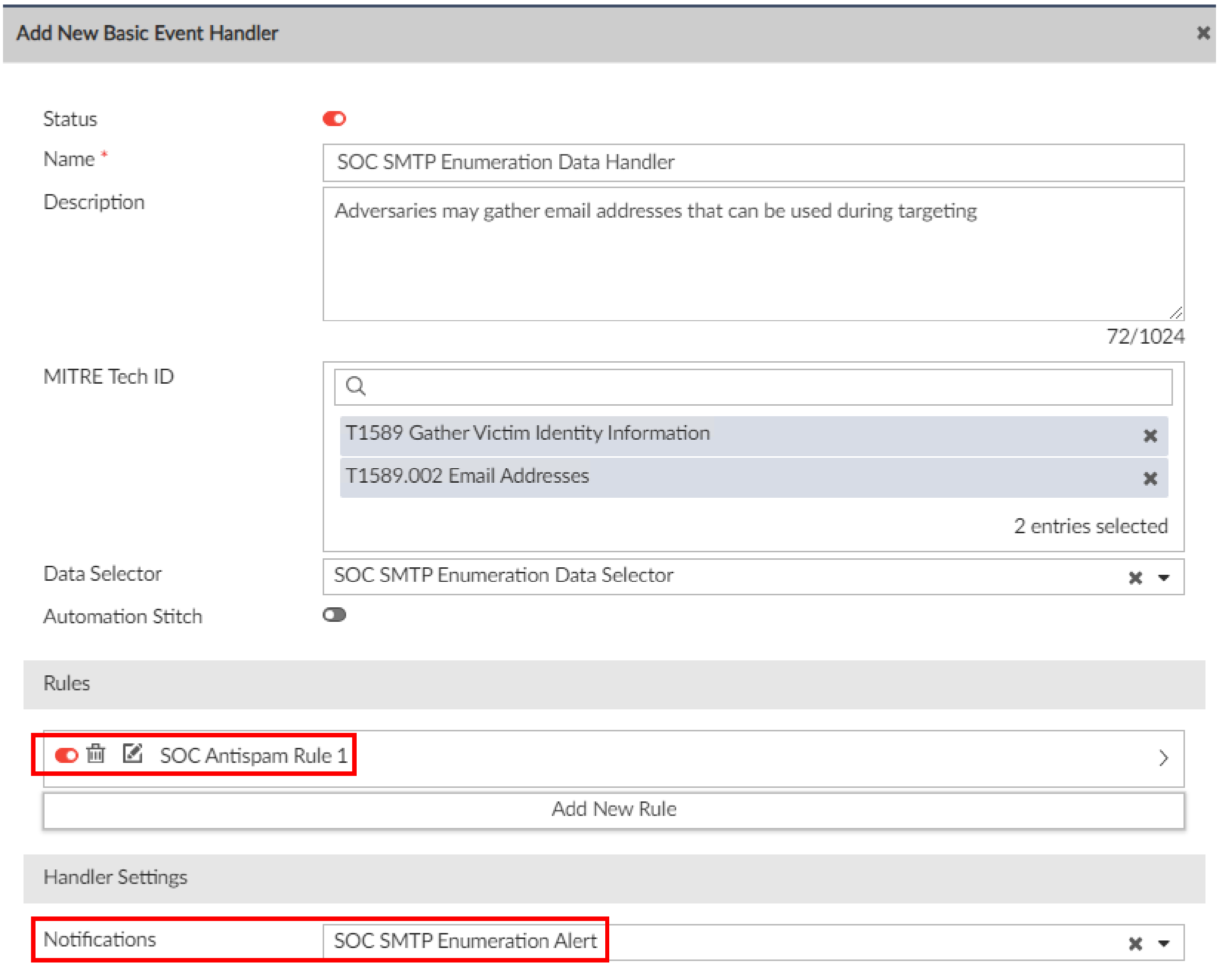
Tags: Press enter to add tags

Indicators:

Log Field	Indicator Type	Count	Action
+			

Additional Info: ● Use system default ○ Use custom message

9. Click **OK**.
10. In the **Notifications** field, select **SOC SMTP Enumeration Alert**.



Add New Basic Event Handler

Status	●
Name *	SOC SMTP Enumeration Data Handler
Description	Adversaries may gather email addresses that can be used during targeting
	72/1024
MITRE Tech ID	T1589 Gather Victim Identity Information T1589.002 Email Addresses 2 entries selected
Data Selector	SOC SMTP Enumeration Data Selector
Automation Stitch	○

Rules

SOC Antispam Rule 1

Add New Rule

Handler Settings

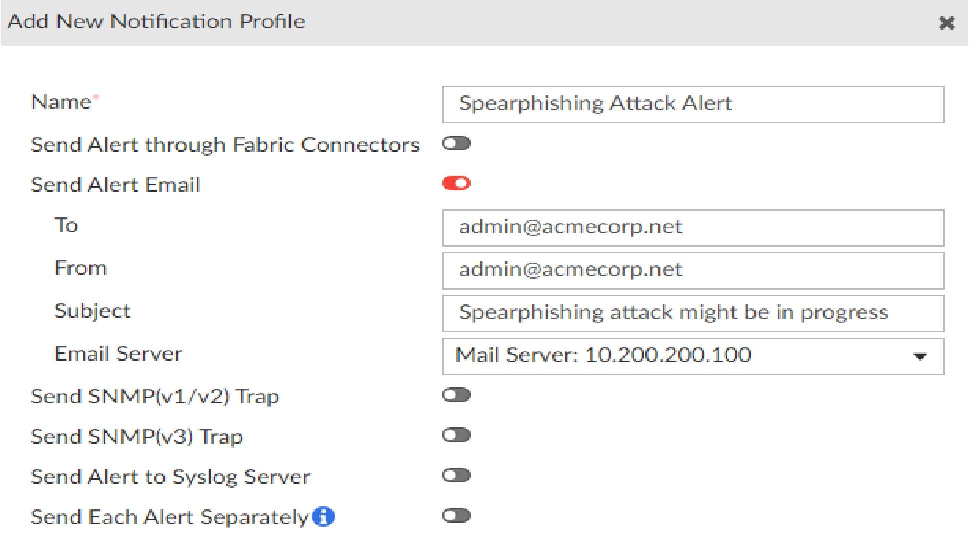
Notifications	SOC SMTP Enumeration Alert

11. Click **OK**.

To configure a notification profile for a spearphishing attack

1. Continuing on the FAZ-SiteB GUI, click the **Notification Profile** tab.
2. Click **Create New**.
3. Configure the following settings:

Field	Value
Name	Spearphishing Attack Alert
Send Alert Email	Enabled
To	admin@acmecorp.net
From	admin@acmecorp.net
Subject	Spearphishing attack might be in progress
Email Server	Mail Server: 10.200.200.100



Add New Notification Profile ✖

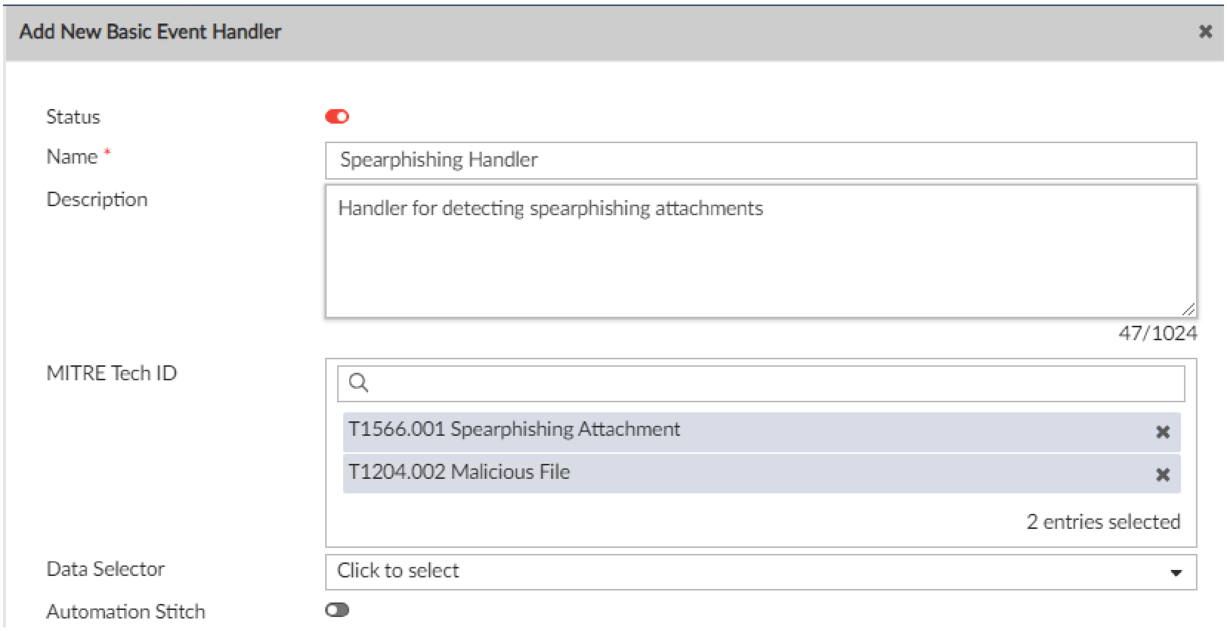
Name*	Spearphishing Attack Alert
Send Alert through Fabric Connectors	○
Send Alert Email	●
To	admin@acmecorp.net
From	admin@acmecorp.net
Subject	Spearphishing attack might be in progress
Email Server	Mail Server: 10.200.200.100 ▾
Send SNMP(v1/v2) Trap	○
Send SNMP(v3) Trap	○
Send Alert to Syslog Server	○
Send Each Alert Separately ℹ	○

4. Click **OK**.

To configure custom event handlers to detect a spearphishing attachment

1. Continuing on the FAZ-SiteB GUI, click **Basic Handlers**.
2. Click **Create New**.
3. In the **Add New Basic Event Handler** window, configure the following settings:

Field	Value
Status	Enabled
Name	Spearphishing Handler
Description	Handler for detecting spearphishing attachments
MITRE Tech ID	T1566.001 Spearphishing Attachment T1204.002 Malicious File



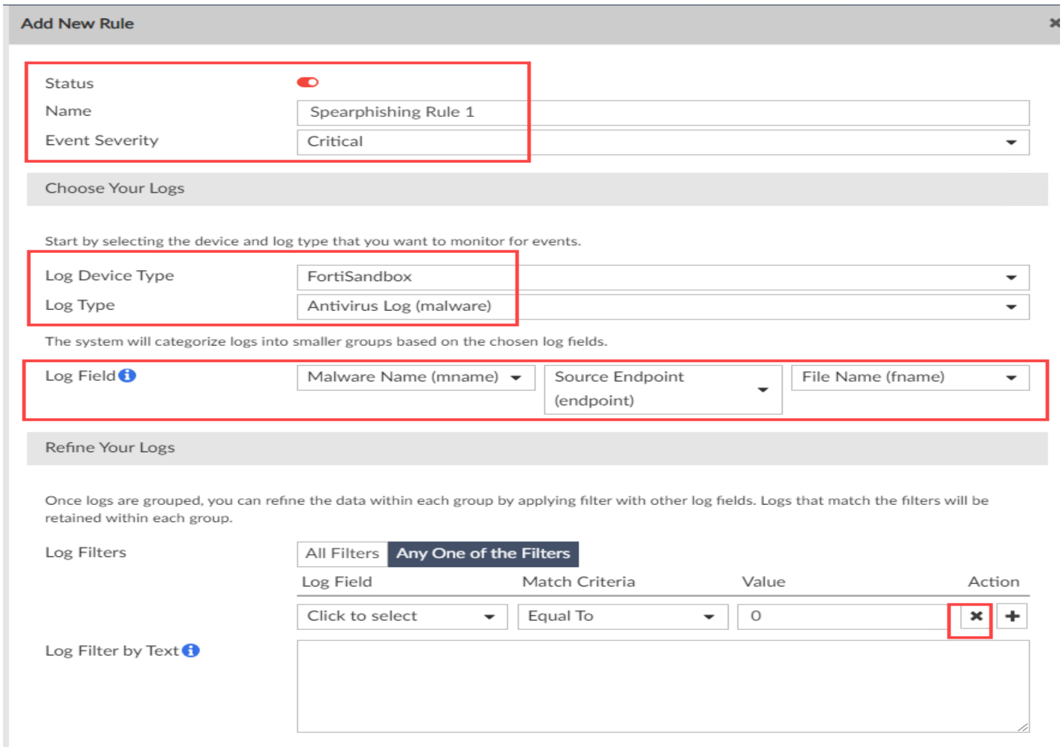
Add New Basic Event Handler ✖

Status	●
Name *	Spearphishing Handler
Description	Handler for detecting spearphishing attachments 47/1024
MITRE Tech ID	T1566.001 Spearphishing Attachment ✖ T1204.002 Malicious File ✖ 2 entries selected
Data Selector	Click to select ▾
Automation Stitch	○

4. Click **Add New Rule**.
5. In the **Add New Rule** window, configure the following settings:

Field	Value
Status	Enabled
Name	Spearphishing Rule 1
Event Severity	Critical

Field	Value
Log Device Type	FortiSandbox
Log Type	Antivirus Log (malware)
Log Field	Malware Name (mname) | Source Endpoint (endpoint) | File Name (fname)
Log Filters	Any One of the Filters
Click **x** to remove the default values in the **Log Field**, **Match Criteria**, **Value**, and **Action** fields.	
Trigger an event when	A group contains 1 or more log occurrences
All logs were generated within	10 minutes



Add New Rule ✖

Status ●
Name: Spearphishing Rule 1
Event Severity: Critical

Choose Your Logs

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

Log Device Type: FortiSandbox
Log Type: Antivirus Log (malware)

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

Log Field: Malware Name (mname) | Source Endpoint (endpoint) | File Name (fname)

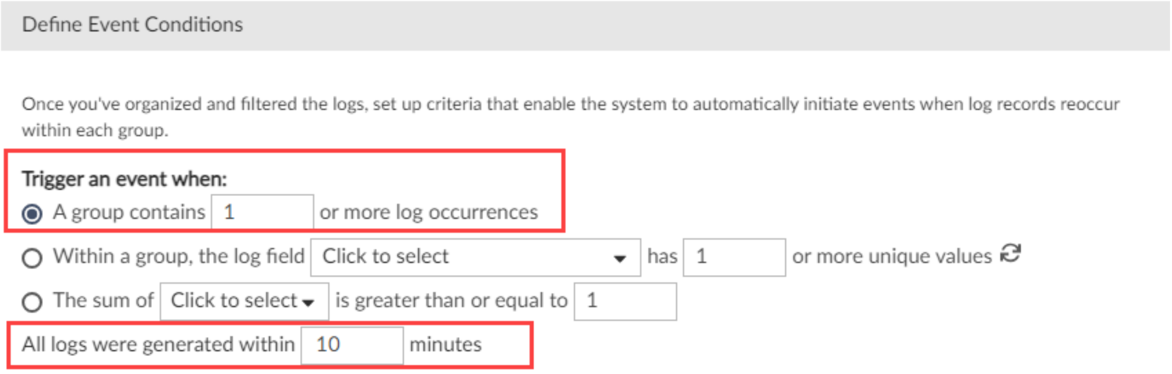
Refine Your Logs

Once logs are grouped, you can refine the data within each group by applying filter with other log fields. Logs that match the filters will be retained within each group.

Log Filters: All Filters | **Any One of the Filters**

Log Field	Match Criteria	Value	Action
Click to select	Equal To	0	✖ +

Log Filter by Text



Define Event Conditions

Once you've organized and filtered the logs, set up criteria that enable the system to automatically initiate events when log records reoccur within each group.

Trigger an event when:

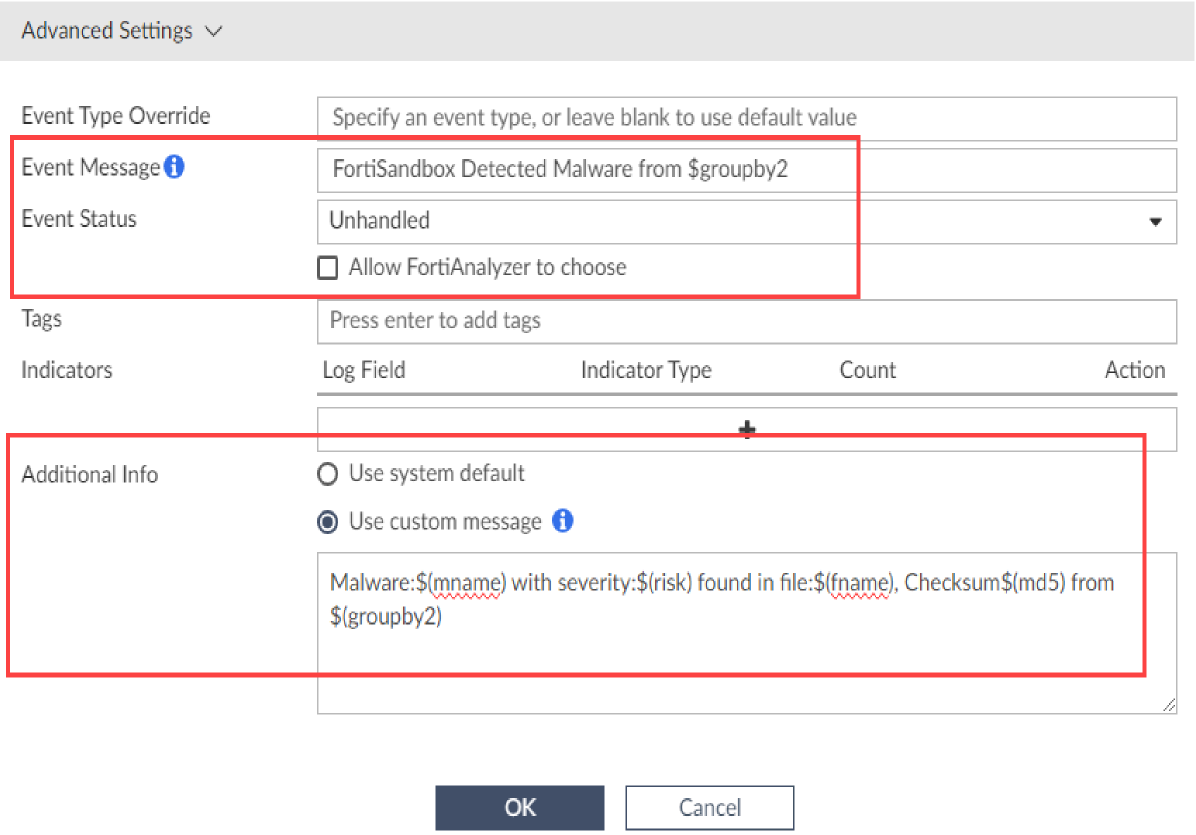
● A group contains 1 or more log occurrences

○ Within a group, the log field Click to select has 1 or more unique values

○ The sum of Click to select is greater than or equal to 1

All logs were generated within 10 minutes

6. Click **Advanced Settings** to view more settings.
7. In the **Event Message** field, type FortiSandbox Detected Malware from $groupby2.
8. Clear the **Allow FortiAnalyzer to choose** checkbox.
9. In the **Event Status** field, select **Unhandled**.
10. In the **Additional Info** field, select **Use custom message**, and then in the text box, type Malware:$(mname) with severity:$(risk) found in file:$(fname), Checksum$(md5) from $(groupby2).



Advanced Settings

Event Type Override: Specify an event type, or leave blank to use default value

Event Message: FortiSandbox Detected Malware from $groupby2

Event Status: Unhandled

□ Allow FortiAnalyzer to choose

Tags: Press enter to add tags

Indicators	Log Field	Indicator Type	Count	Action

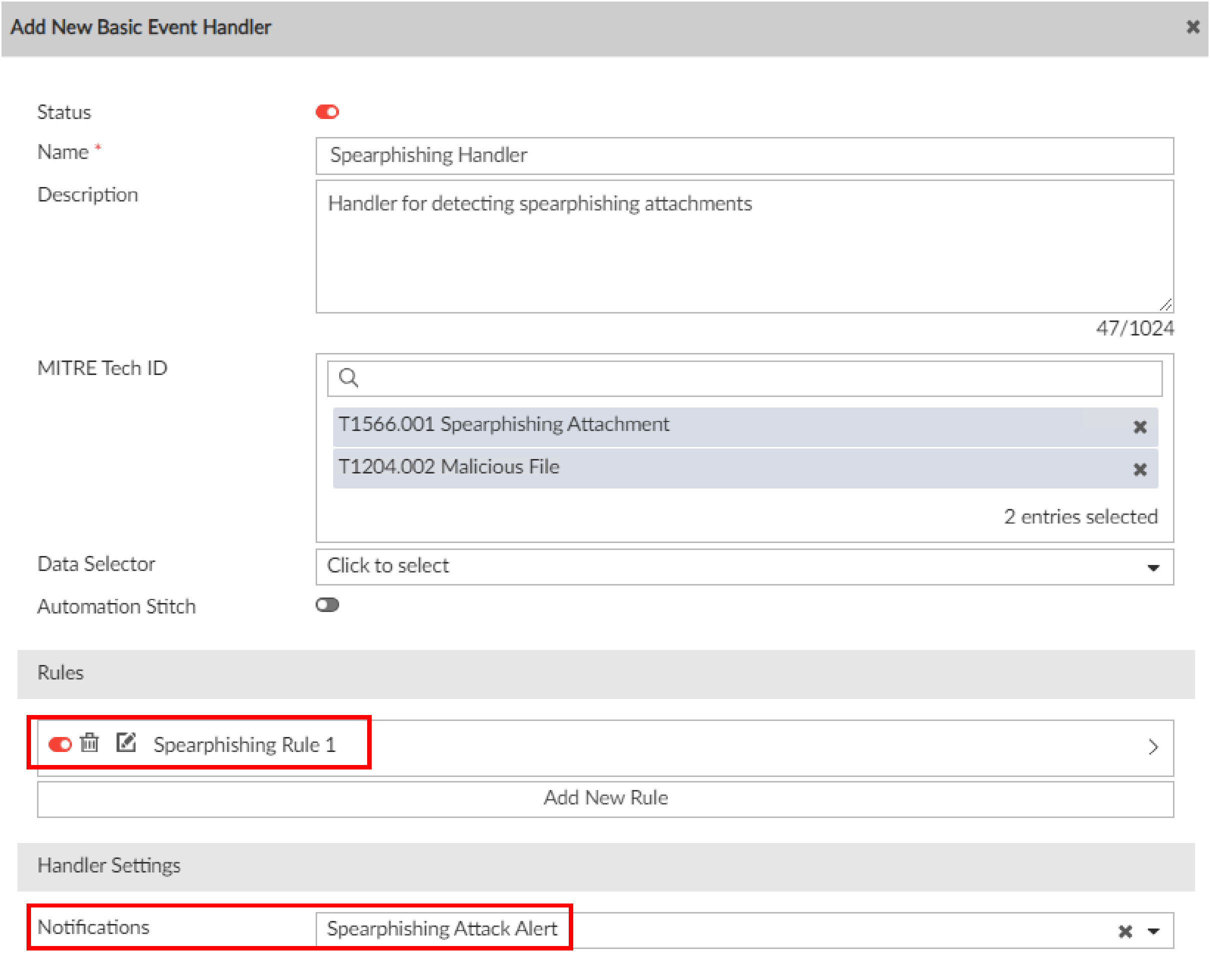
Additional Info:

○ Use system default

● Use custom message

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

11. Click **OK**.
12. In the **Notifications** field, select **Spearphishing Attack Alert**.



Add New Basic Event Handler

Status: ●

Name *: Spearphishing Handler

Description: Handler for detecting spearphishing attachments

47/1024

MITRE Tech ID:

T1566.001 Spearphishing Attachment

T1204.002 Malicious File

2 entries selected

Data Selector: Click to select

Automation Stitch

Rules

Spearphishing Rule 1

Handler Settings

Notifications: Spearphishing Attack Alert

13. Click **OK**.

Due to time constraints, there are additional custom event handlers, which will be used in this lab guide, that have been preconfigured for you.

The goal of this lab is for you to understand the concepts of configuring different elements of event handlers using the examples above.

LAB-3 > Configuring Detection Rules
Outline
preview

-