

TTP-First Use Case

In today's environments, security tools are not failing because they lack visibility, they are failing because they lack context.

Organizations are flooded with alerts:

- *A scan detected at the perimeter...*
- *A phishing email flagged by the mail gateway...*
- *A suspicious PowerShell execution on an endpoint...*
- *Internal traffic is not always inspected...*

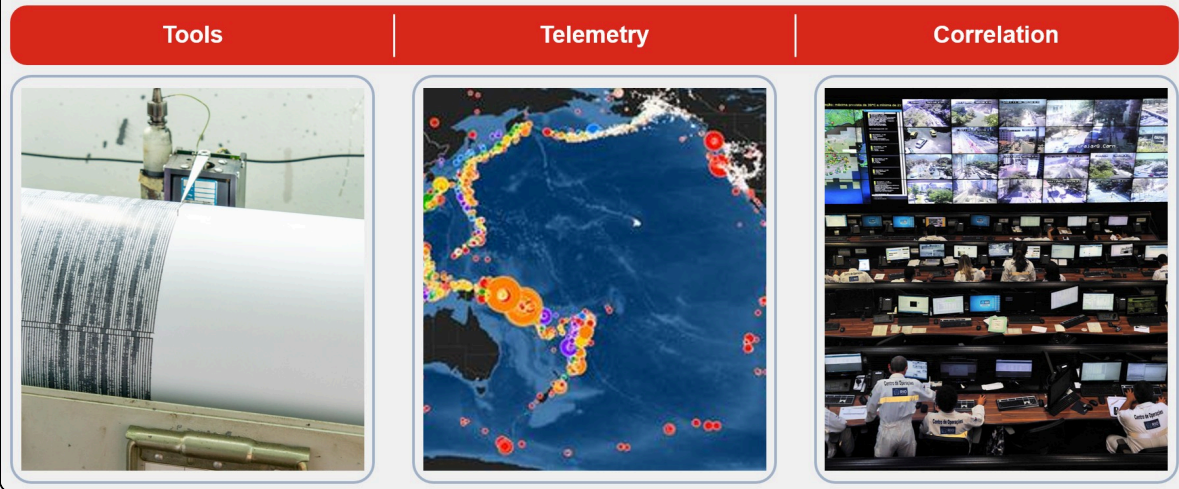
Each control does its job, but none of them tell the full story.

The **purpose** of this use case is to demonstrate how a TTP-First SecOps approach, based on the MITRE ATT&CK framework can help transforming isolated alerts into a connected attack narrative.

Purpose of the labs

1. Demonstrate behavioral correlation through a continuous attack simulation.
2. Link events accross different Fortinet products.
3. Reduction of the investigation time.
4. Align detections to attacker behavior using MITRE ATT&CK framework.

From Tools to Telemetry Architecture



Products Used

All systems share the password:

Fortinet123#

System	Fabric Studio Name	Method	Username	IP Address
FabricStudio	FabricStudio	HTTPS	admin	10.128.111.48
FortiGate	Enterprise_Core	HTTPS	admin	10.20.0.254 (Fortinet Fabric)
FortiMail	FortiMail	HTTPS	admin	10.20.0.7 (Fortinet Fabric)
FortiWeb	FortiWeb	HTTPS	admin	fortirecon.forticloud.com and simulated Domain Threats alerts

FortiSIEM	FortiSIEM	HTTPS	admin	10.128.111.48:13016 or 10.20.0.8
Windows	Alpha	Remote Desktop	fortixperts	10.128.111.48:13016 or 10.20.0.8
Kali Linux	Kali	Desktop	kali	10.128.111.48:13016 or 10.20.0.8
Linux Server	Ubuntu- DVWA	Desktop	user	10.128.111.48:13016 or 10.20.0.8

Labs

No.	Lab Name	Main Objective
1	External Reconnaissance	Detect an <i>early stage attack</i> via FortiAnalyzer (FortiGate + FortiWeb)
2	Initial Access	Configure FortiAnalyzer for detecting some common <i>initial access</i> events from FortiMail
3	Execution, Command & Control	Using FortiEDR, identify some <i>not so innocent</i> behaviors once an attacker is inside the network
4	Lateral Movement	Detect the <i>lateral movement</i> using FortiSIEM
5	Impact	Detect the <i>impact</i> using FortiSIEM

Disclaimer, these labs are simulations intended to demonstrate some useful configurations for SecOps, however, to keep the flow of the exercises, some configurations have been crafted by not following the best practices, maintaining default parameters or simply configured in detect mode

instead of blocking. We strongly advise to evaluate any configuration prior to be productive.

You made it — the final use case. Let's get on it!

Lab 01. External Reconnaissance

Estimated Time to Complete

25 minutes

Lab Access Information

Access Fabric Studio via https://<your_fabric_studio_ip> using the following credentials:

- **Username:** admin
- **Password:** Fortinet123#

System	Fabric Studio Name	Method	Username	Password	IP Address
FortiGate	Enterprise_Core	HTTPS	admin	Fortinet123#	<a href="https://<your_fabric_studio_ip>:13000">https://<your_fabric_studio_ip>:13000
FortiWeb	FortiWeb	HTTPS	admin	Fortinet123#	<a href="https://<your_fabric_studio_ip>:13006">https://<your_fabric_studio_ip>:13006
FortiAnalyzer	FortiAnalyzer	HTTPS	admin	Fortinet123#	<a href="https://<your_fabric_studio_ip>:13001">https://<your_fabric_studio_ip>:13001

```
ic_studio_ip>/console/spice/basi00
```

Introduction

Every attack begins with reconnaissance — the attacker is mapping the environment. In this lab, we detect early scanning activity before exploitation begins.

Using tools like `nmap` and `nikto`, we emulate common reconnaissance techniques (`T1595`, `T1046`) to identify exposed services and vulnerabilities and map them through FortiGate and FortiWeb telemetry in FortiAnalyzer.

Recon the environment

1. Simulating to be an attacker, connect to Kali using the following credentials:
2. **Username:** `kali`
3. **Password:** `Fortinet123#`
4. From a web browser private window, navigate to the webserver using the bookmark.
5. You just found a corporate portal, it is not quite secure though, let's see how far we can get...

Configure FortiGate

Info

Let's begin by adjusting some FortiGate settings so it can detect reconnaissance activity.

Enable Logging in FortiGate

1. Navigate to **Security Fabric** → **Fabric Connectors**
2. Click on **Logging & Analytics** and Authorize the FortiAnalyzer.
3. In the **Security Fabric Connectors** section, click on Authorize for FortiMail and FortiWeb devices.

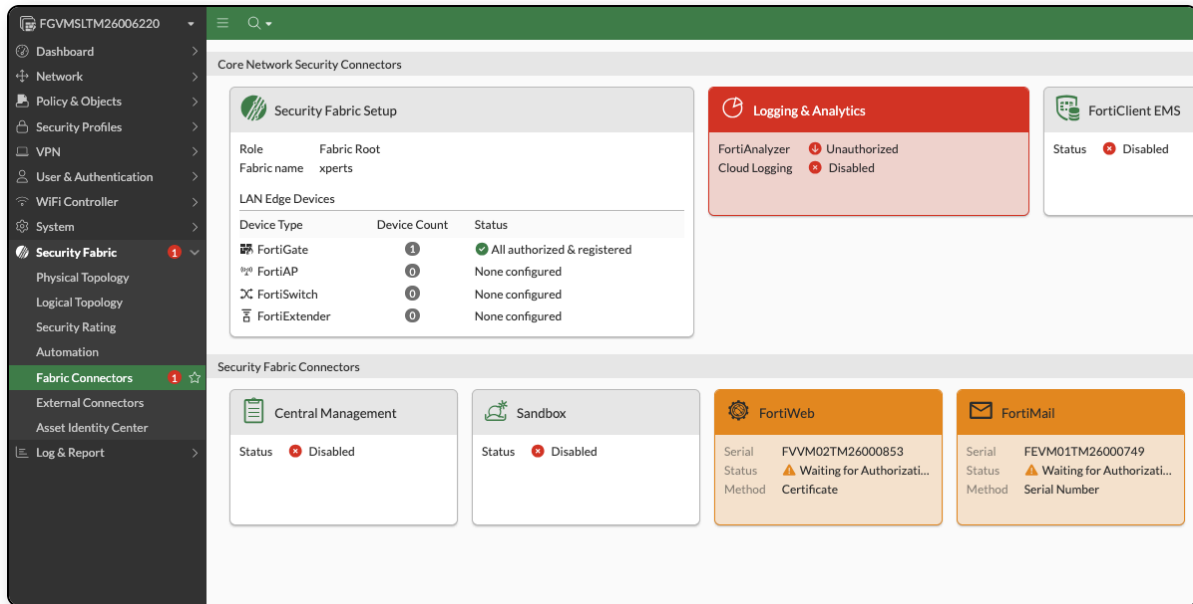


Figure 0: Fabric Connectors

Enable a DoS Policy in FortiGate

1. From Fabric Studio, access the FortiGate via HTTPS.
2. Log in with the following credentials:
3. **Username:** admin
4. **Password:** Fortinet123#
5. Navigate to **Policy & Objects** → **DoS Policy**.
6. Click **Create New** and use the following details for the rule:
7. **Name:** Xperts_DoS_Policy
8. **Incoming Interface:** port6
9. **Source Address:** All
10. **Destination Address:** All
11. **Service:** All
12. In the **L4 Anomalies** section, configure the following:
13. **tcp_port_scan:** enable
14. **Monitor:** enable
15. **Threshold:** 100
16. Click **OK**.

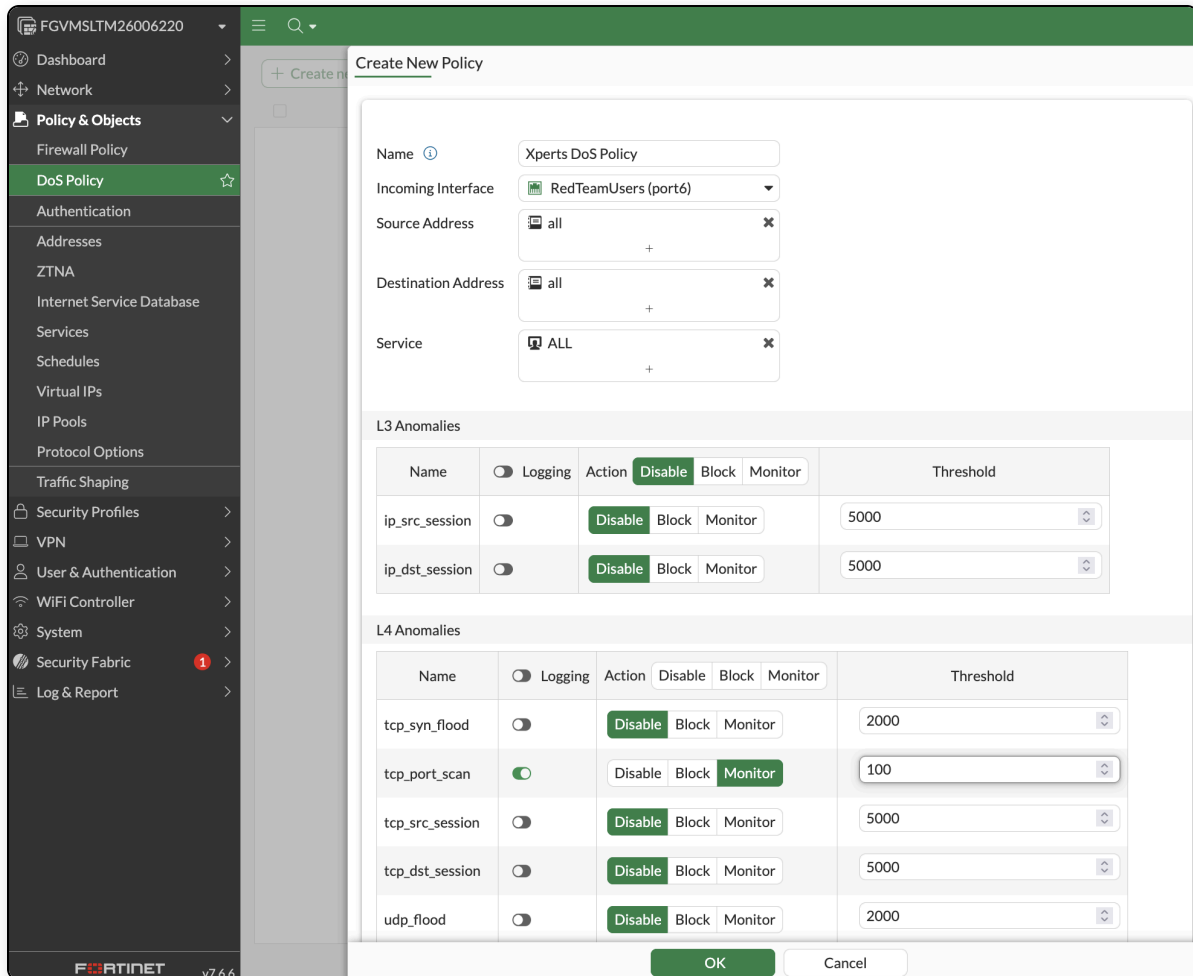


Figure 1: FortiGate DoS Policy Configuration

Configure FortiAnalyzer

Configurations for some devices to send logs to FortiAnalyzer are already in place to save time, however, we need to register those devices into FortiAnalyzer.

Register Devices into FortiAnalyzer

1. From Fabric Studio, access the FortiAnalyzer via HTTPS.
2. Log in with the following credentials:
3. **Username:** admin
4. **Password:** Fortinet123#
5. Navigate to **Device Manager** → **All Logging Devices**

6. Select the *LOGGING DEVICES* and delete them
7. Navigate to **Device Manager** → **Uregistered Devices**
8. Select all the devices and click on **Authorize**
9. Edit the names accordingly for registration **FortiGate**, **FortiWeb** and **FortiMail**.

Create Event Handlers in FortiAnalyzer

Info

FortiAnalyzer Event Handlers are used to detect specific security, system, or network events from incoming logs and trigger immediate automated actions such as alerts, emails, or incident creation. For more information, refer to the FortiAnalyzer Administration Guide:

[FortiAnalyzer Event Handlers Documentation](#)

1. Still in FortiAnalyzer.
2. Go to **Incidents & Events** → **Event Handlers**.
3. Click **Create New**.
4. Toggle **Status** on at the top of the Event Handler editor.
5. Rename the new Event Handler to `xperts_tcp_port_scan`.
6. Toggle **Automatically Create Incident** on.
7. From the **MITRE Tech ID** dropdown, select `T1595.001 Scanning IP Blocks`.
8. From the **MITRE Tech ID** dropdown, select `T1046 Network Service Discovery`.

- **Match Criteria:** Equal To
- **Value:** tcp_port_scan

Add New Rule

Status

☒

Name

TCP_port_scan

Event Severity

Medium

Choose Your Logs

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

Log Device Type

FortiGate

Log Type

IPS (ips)

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

Log Field

Source IP (srcip)

Not in use

Not in use

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
Attack Name (attack)	Equal To	tcp_port_scan	× +

Log Filter by Text

0/2047

Define Event Conditions

Once you have 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

☐ A group contains

1

or more log occurrences

☐ A group contains

1

or more log occurrences

OK

Cancel

Figure 3: TCP Port Scan Rule

1. Click **OK**.
2. Click **OK** at the bottom of the Event Handler editor.

i Info

Additional information about Custom Event Handlers can be found in the FortiAnalyzer Administration Guide: (<https://docs.fortinet.com/document/fortianalyzer/7.6.6/administration-guide/348606/creating-a-custom-event-handler>)

Let's create a second Event Handler, this time to detect FortiWeb events.

1. Back in the **Event Handlers** section, click **Create New**.
2. Configure the handler with the following details:
3. **Status:** ☐ On
4. **Name:**
5. **MITRE Tech ID:**
6. **Automatically Create Incident:** ☐ On

7. **Log Type:** Attack Log

8. **Log Field:** HTTP Host

9. **Filter Configuration**

- **Log Filters:** Any One of the Filters
- **Log Field:** Main Type
- **Match Criteria:** Equal To
- **Value:** Signature Detection

10. Click **OK**

11. Click **OK**

Add New Rule

Status

☒

Name

FortiWeb Vulnerability Scanner

Event Severity

Critical

Choose Your Logs

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

Log Device Type

FortiWeb

Log Type

Attack Log (attack)

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

Log Field

HTTP Host (http_host)

Not in use

Not in use

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
Main Type (main_type)	Equal To	Signature Detection	× +

Log Filter by Text

0/2047

Define Event Conditions

Once you have 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

OK

Cancel

Figure 5: Rule for FortiWeb

1. Verify the handler creation by searching for it in the list using the **Search** field and filtering with the keyword `Xperts`.

Event Handlers						
St...	Name	Rules	Origin	Data Selector	Notification Profile	Automation Stitch
☐	Xperts Default-NMAP-Process-Activity-Detection NMAP Process Activity detected. NMAP is a tool for network scannin...	Rule-1 NMAP Process Activity Detected: srcintrole Equal To LAN AND /	Custom			No
☐	Xperts tcp_port_scan	Rule-1 TCP_port_scan: attack Equal To tcp_port_scan	Custom			No
☒	Xperts Vulnerability Scanner	Rule-1 FortiWeb Vulnerability Scanner: main_type Equal To Signature De	Custom			No

Figure 6: Custom Event Handler

Testing Event Handlers for Reconnaissance

1. Log in to Kali using the following credentials:

2. **Username:** kali

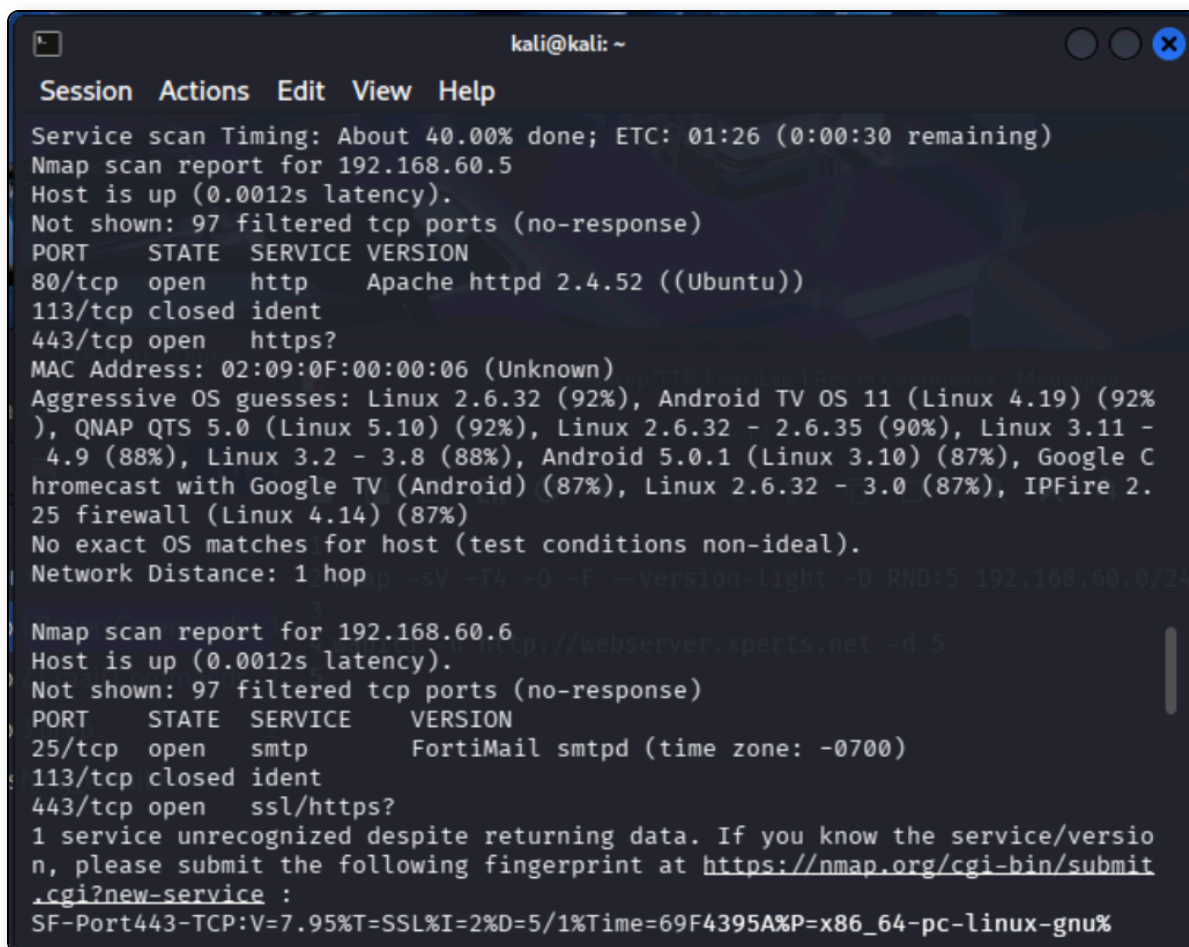
3. **Password:** Fortinet123#

!!! info for easiness of executing commands in Kali, there is a Folder in the Desktop named *TTP-First* with the commands used in the labs, this way you can copy & paste into the console.

1. Open a terminal console and run the following command at least a couple of times:

```
nmap -sV -T4 -O -F --version-light -D RND:5 192.168.60.0/24
```

1. Observe the scan results.



```
kali@kali: ~
Session Actions Edit View Help

Service scan Timing: About 40.00% done; ETC: 01:26 (0:00:30 remaining)
Nmap scan report for 192.168.60.5
Host is up (0.0012s latency).
Not shown: 97 filtered tcp ports (no-response)
PORT      STATE SERVICE VERSION
80/tcp    open  http   Apache httpd 2.4.52 ((Ubuntu))
113/tcp   closed ident
443/tcp   open  https?
MAC Address: 02:09:0F:00:00:06 (Unknown)
Aggressive OS guesses: Linux 2.6.32 (92%), Android TV OS 11 (Linux 4.19) (92%), QNAP QTS 5.0 (Linux 5.10) (92%), Linux 2.6.32 - 2.6.35 (90%), Linux 3.11 - 4.9 (88%), Linux 3.2 - 3.8 (88%), Android 5.0.1 (Linux 3.10) (87%), Google Chromecast with Google TV (Android) (87%), Linux 2.6.32 - 3.0 (87%), IPFire 2.25 firewall (Linux 4.14) (87%)
No exact OS matches for host (test conditions non-ideal).
Network Distance: 1 hop

Nmap scan report for 192.168.60.6
Host is up (0.0012s latency).
Not shown: 97 filtered tcp ports (no-response)
PORT      STATE SERVICE VERSION
25/tcp    open  smtp   FortiMail smtpd (time zone: -0700)
113/tcp   closed ident
443/tcp   open  ssl/https?
1 service unrecognized despite returning data. If you know the service/version, please submit the following fingerprint at https://nmap.org/cgi-bin/submit.cgi?new-service :
SF-Port443-TCP:V=7.95%T=SSL%I=2%D=5/1%Time=69F4395A%P=x86_64-pc-linux-gnu%
```

Figure 7: Kali NMAP

1. Test with a different scanner, this time looking for web vulnerabilities.
2. In the Kali terminal, run the following commands:

```
nikto -h http://webserver.xperts.net/dvwa/login.php
nikto -h http://webserver.xperts.net
```

!!! info Nikto is an open-source, command-line web server vulnerability scanner pre-installed in Kali Linux.

Verifying Results on FortiAnalyzer

1. Go back to the FortiAnalyzer GUI and navigate to **Incidents & Events** → **Incidents** → **MITRE ATT&CK**.
2. Adjust the timeframe to display events from the last 30 minutes.

3. You should see two highlighted blocks one in the **Reconnaissance** tactic and the other under **Discovery**. These were detected by the Event Handlers you just configured.

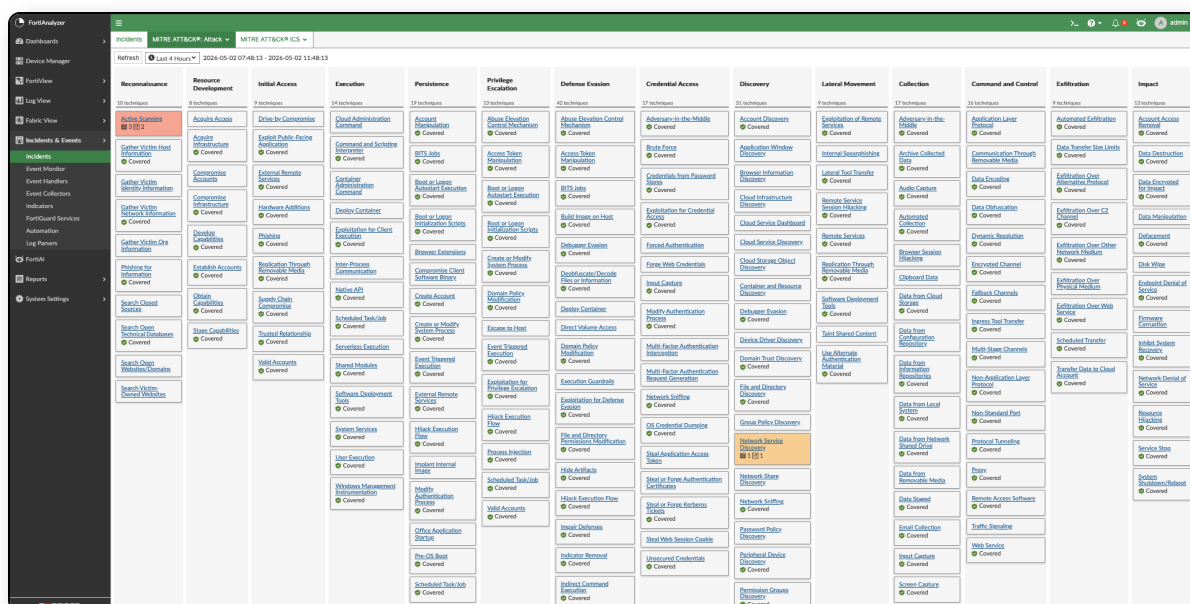


Figure 8: MITRE ATT&CK

1. Hover the mouse over the highlighted tactics to inspect the details, click on them to get further information.
2. Identify the source and destination IP addresses for the events.
3. Identify the detected attacks.
4. Navigate to **Dashboards** → **SOC Dashboard** to get a different view of the detected incidents.

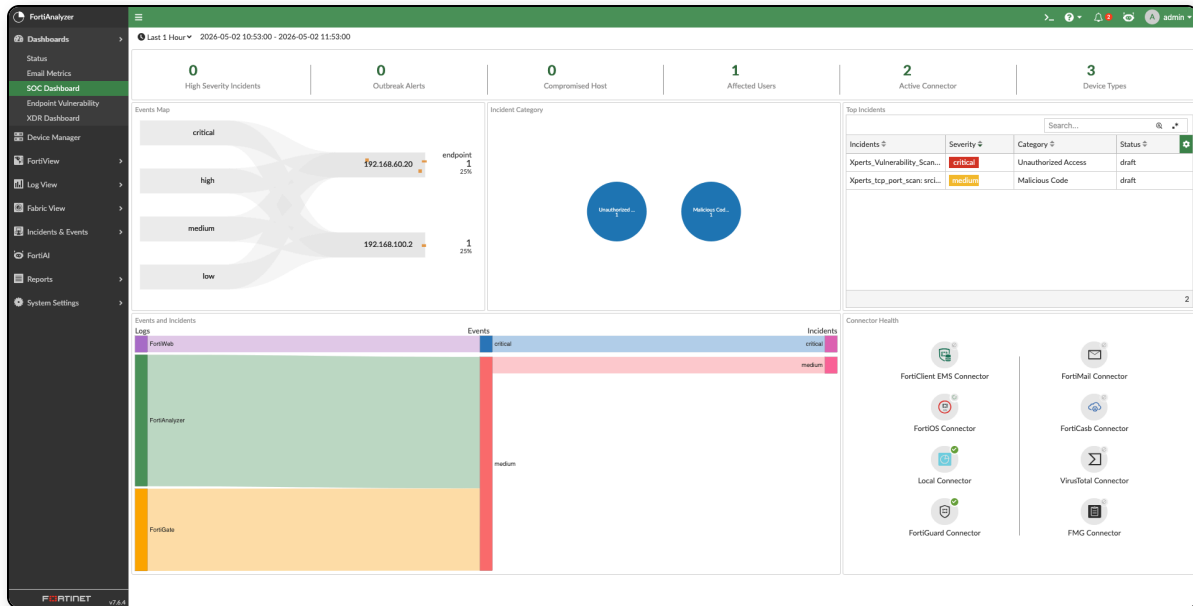


Figure 9: SOC Dashboard

1. Navigate to **Dashboards** → **XDR Dashboard** to get a different view of the alerts. This view was introduced in version 7.6.4 to provide a real-time view of all alerts and incidents detected from different sources.

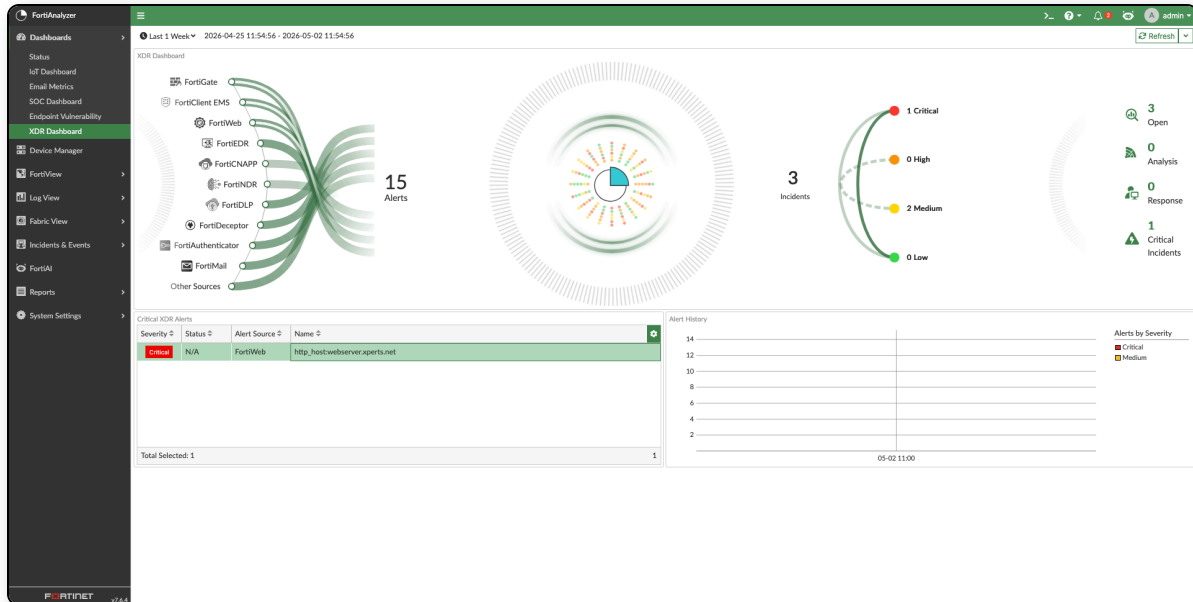


Figure 10: XDR Dashboard

1. Which device helped to contain the attack?
2. Is it a definitive containment?
3. What is the core purpose of **Event Handlers** within FortiAnalyzer?

!!! info Event Handlers "Core Functions" - Detect security incidents - Correlate multiple logs
- Trigger alerts or automation - Generate events mapped to MITRE ATT&CK techniques -
Feed SOC dashboards and incident workflows

Lab 02. Initial Access

Estimated Time to Complete

30 minutes

Lab Access Information

Access Fabric Studio via https://<your_fabric_studio_ip> using the following credentials:

- **Username:** `admin`
- **Password:** `Fortinet123#`

System	Fabric Studio Name	Method	Username	Password	IP Address
FortiMail	FortiMail	HTTPS	<code>admin</code>	<code>Fortinet123#</code>	<a href="https://<your_fabric_studio_ip>:13005">https://<your_fabric_studio_ip>:13005
FortiAnalyzer	FortiAnalyzer	HTTPS	<code>admin</code>	<code>Fortinet123#</code>	<a href="https://<your_fabric_studio_ip>:13001">https://<your_fabric_studio_ip>:13001
Kali Linux	Kali	Display	<code>kali</code>	<code>Fortinet123#</code>	<a href="https://<your_fabric_studio_ip>/console/spice/basi00">https://<your_fabric_studio_ip>/console/spice/basi00

```
t Fortinet123 https://<your_fabric_studio_ip>/console/spice/
s # wind00
```

Introduction

Initial access is the moment an attacker attempts to enter the environment — often through phishing, malicious links, or weaponized attachments. In this lab, we simulate a phishing-based entry point and observe how FortiMail and FortiAnalyzer work together to detect, classify, and map these events to the MITRE ATT&CK framework.

By combining email security controls, subject tagging, and Event Handlers in FortiAnalyzer, this lab demonstrates how early-stage email threats can be identified as *Spearphishing Attachment* and *Spearphishing Link* techniques before the attack progresses further.

FortiMail Configuration

Access FortiMail

1. Connect to FortiMail using the following credentials:
2. **Username:** admin
3. **Password:** Fortinet123#

Configure AntiSpam Profile

1. Navigate to **Profile** → **AntiSpam**
2. Select the profile **AS_Inbound** and click **Clone**

3. Set the name to `AS_Inbound_Xperts` and click **OK**

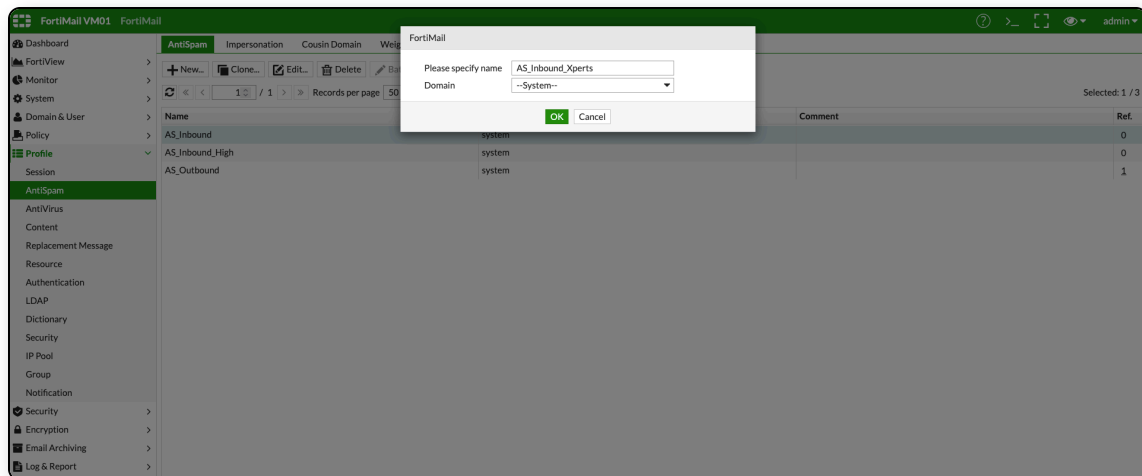


Figure 1: AntiSpam Profile

4. Double-click the newly created profile to edit it
5. Change the **Default action** to `TagSubject`
6. Click the **+** sign next to **FortiGuard**
7. Enable **Secondary URL Category**
8. Set **Spam Outbreak Protection** to `Enable`
9. Disable the following options:
 10. `SPF`
 11. `DMARC`

12. Click **OK**

AntiSpam Profile

Domain: --System--

Name: AS_Inbound_Xperts

Comment:

Default action: TagSubject

Scan Configuration

- ☒ FortiGuard Action: --Default--
- ☒ IP Reputation Action: --Default--
- URL Category
 - ☒ Primary: phishing Action: --Default--
 - ☒ Secondary: unrated Action: TagSubjectSuspiciousURL
- Spam outbreak protection: Enable
- ☐ Greylist
- ☒ SPF Action: --Default--
- ☒ DKIM Action: --Default--
- ☒ DMARC Action: TagSubjectSuspicious
- ☒ ARC Action: --Default--
- ☒ Behavior analysis Action: --Default--
- ☐ Header analysis Action: TagSubjectSuspicious
- ☒ Business email compromise Action: --Default--
- ☒ Heuristic Action: --Default--
- ☐ SURBL [Configuration...] Action: --Default--
- ☐ DNSBL [Configuration...] Action: --Default--
- ☐ Banned word [Configuration...] Action: --Default--
- ☐ Safelist word [Configuration...] Action: --Default--

OK Cancel

Figure 2: AntiSpam Profile Configuration

Configure AntiVirus Profile

1. Navigate to **Profile** → **AntiVirus**
2. Click the **Action** tab

Create Action Profile

1. Click **+New**
2. Configure:

3. **Name:** Deliver_Xperts
4. **Tag Subject:** [*Virus Removed*]
5. Enable:
6. Tag Subject
7. Deliver to original host
8. Replace infected / suspicious body or attachment default
9. Click **Create**

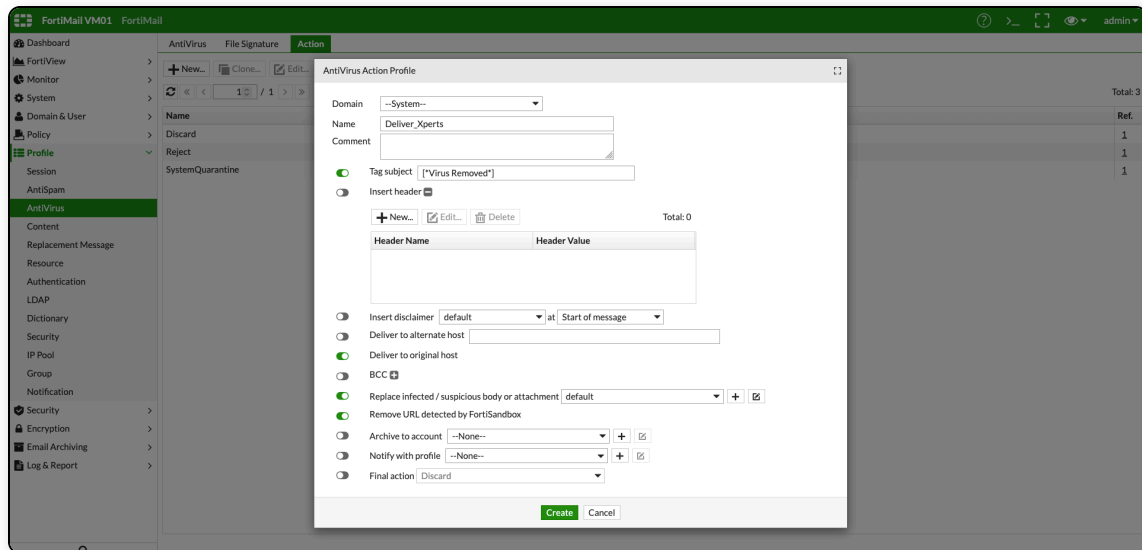


Figure 3: Action Profile Configuration

Create AntiVirus Profile

1. Navigate to the **AntiVirus** tab
2. Click **+New**
3. Configure:
4. **Name:** AV_Removed_Xperts
5. **Default action:** Deliver_Xperts

6. Click **Create**

AntiVirus Profile

Domain: --System--

Name: AV_Removed_Xperts

Comment:

Default action: Deliver_Xperts

☒ AntiVirus

- ☒ Malware/virus outbreak Action: --Default--
- ☒ Heuristic Action: --Default--
- ☐ File signature check Action: --Default--
- ☒ Grayware

☐ FortiNDR

☐ FortiSandbox

Scan mode: **Submit and wait for result** Submit only

☒ Attachment analysis

Malicious/Virus	Action: --Default--
High risk	Action: --Default--
Medium risk	Action: --Default--
Low risk	Action: --Default--
No Result	Action: --None--

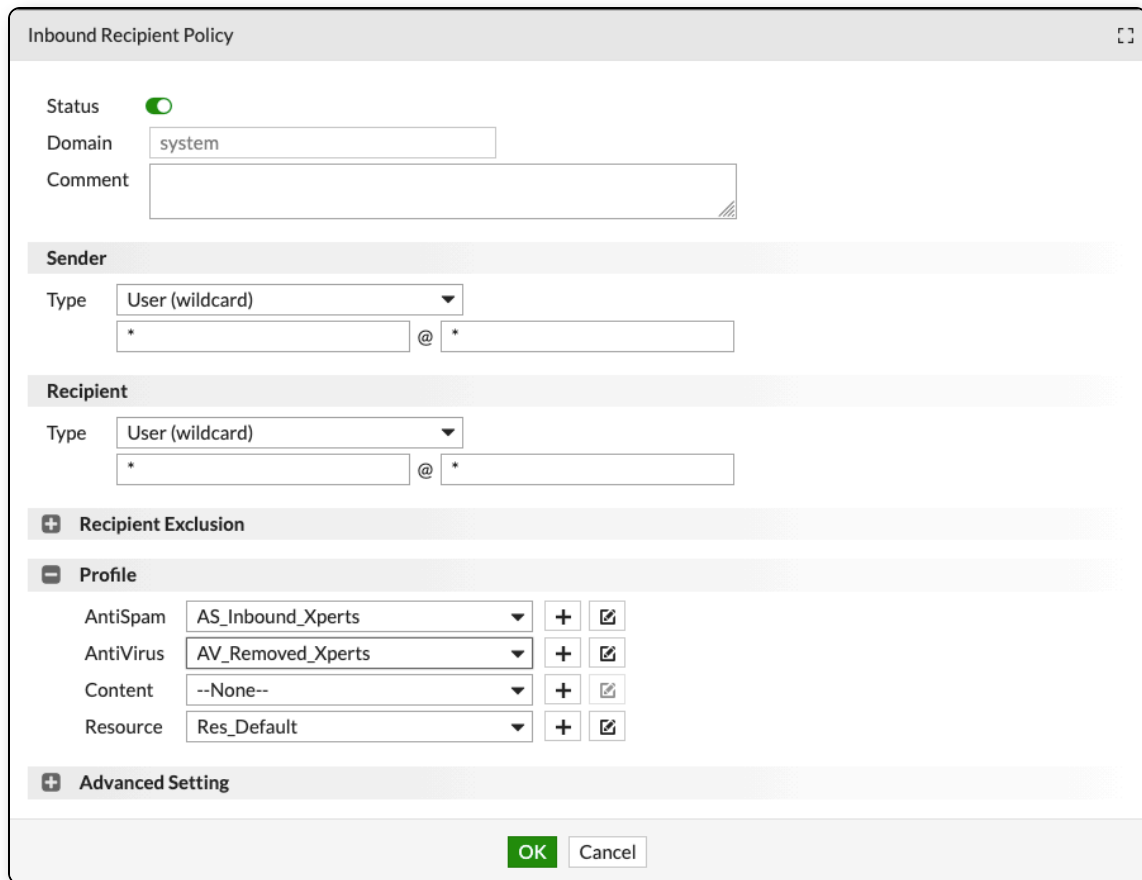
Create Cancel

Figure 4: AntiVirus Profile Configuration

Apply Profiles to Policy

1. Navigate to **Policy** → **Recipient Policy**
2. Edit the existing policy
3. Under **Profile** → **AntiSpam**, select the profile AS_Inbound_Xperts
4. Under **Profile** → **AntiVirus** assign the profile AV_Removed_Xperts

5. Click **OK**



The screenshot shows the 'Inbound Recipient Policy' configuration window. The 'Status' toggle is turned on. The 'Domain' field is set to 'system'. The 'Comment' field is empty. The 'Sender' section has a 'Type' dropdown set to 'User (wildcard)' and two input fields for email addresses, both containing an asterisk (*). The 'Recipient' section also has a 'Type' dropdown set to 'User (wildcard)' and two input fields for email addresses, both containing an asterisk (*). The 'Recipient Exclusion' section is collapsed. The 'Profile' section is expanded, showing four rows: 'AntiSpam' set to 'AS_Inbound_Xperts', 'AntiVirus' set to 'AV_Removed_Xperts', 'Content' set to '--None--', and 'Resource' set to 'Res_Default'. Each row has a '+' button and an edit icon. The 'Advanced Setting' section is collapsed. At the bottom, there are 'OK' and 'Cancel' buttons.

Figure 5: Inbound Policy Configuration

FortiAnalyzer Configuration

Access FortiAnalyzer

1. Login using:
2. **Username:** admin
3. **Password:** Fortinet123#

Enable Event Handler

1. This time we are using a pre-configured *Event Handler*, navigate to **Incidents & Events - > Event Handlers**
2. Search for Default-FML-Threat-Detection-By-Email

3. Right-click and select **Enable**

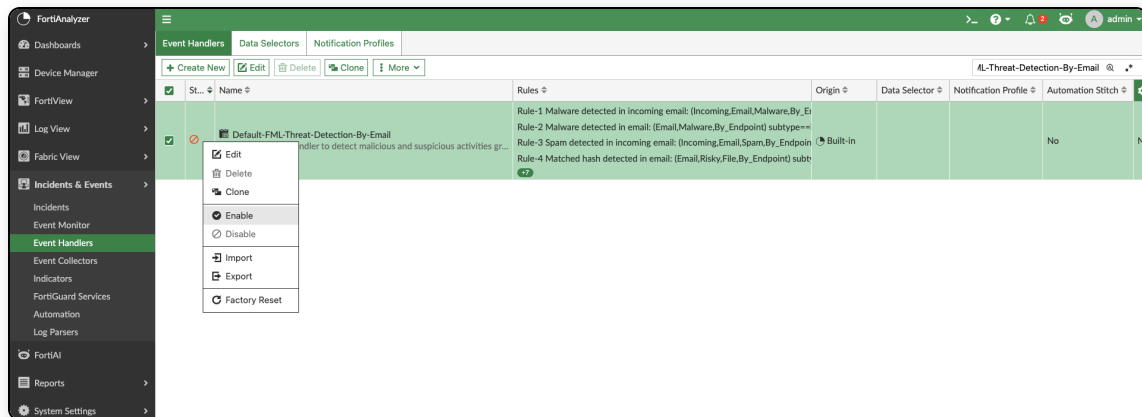


Figure 6: Event Handler

4. Double-click to edit

5. Enable **Automatically Create Incident**

6. Click **OK**

Edit Basic Event Handler

Status: ☒

Name: Default-FML-Threat-Detection-By-Email

Description: Default FortiMail Handler to detect malicious and suspicious activities grouped by user's Email address

MITRE Tech ID: 103/1024

MITRE Tech ID List:

- T1598.002 Spearphishing Attachment
- T1598.003 Spearphishing Link
- T1566.001 Spearphishing Attachment
- T1566.002 Spearphishing Link
- T1204.001 Malicious Link
- T1204.002 Malicious File
- T1204.003 Malicious Image
- T1114 Email Collection

Click to select 8 entries selected

Data Selector: Click to select

Automation Stitch: ☐

Automatically Create Incident: ☒

Rules:

- ☒ Malware detected in incoming email
- ☒ Malware detected in email

Factory Reset OK Cancel

Figure 7: Event Handler Configuration

i Info

This built-in Event Handler provides detection for email-based threats and maps them into actionable incidents.

Testing AntiSpam and Event Handler

Access Kali

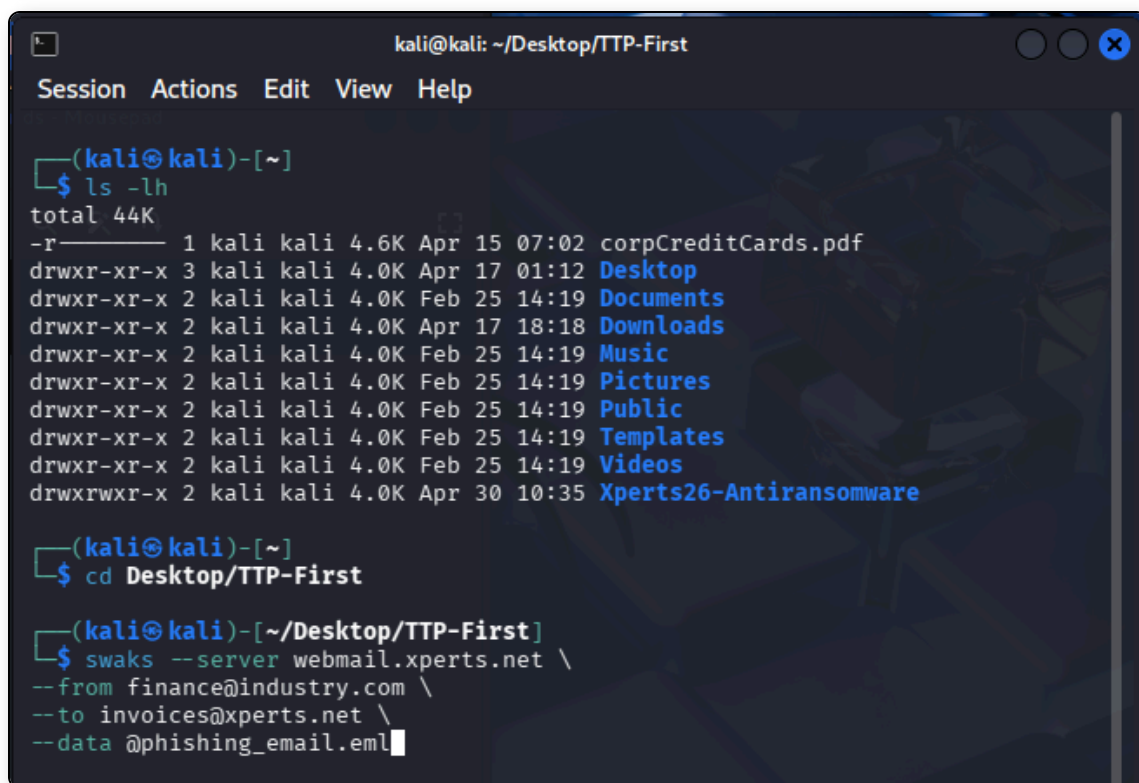
1. Login using:
2. **Username:** kali
3. **Password:** kali

Execute Email Simulation

1. Open the file `Lab 2 Email Commands.txt` from TTP-First folder in Desktop
2. Copy all contents
3. Open a terminal and run:

```
cd Desktop/TTP-First/
```

1. Paste the previously copied commands into the terminal
2. Press **Enter**



```
kali@kali: ~/Desktop/TTP-First
Session Actions Edit View Help

(kali@kali)-[~]
$ ls -lh
total 44K
-r----- 1 kali kali 4.6K Apr 15 07:02 corpCreditCards.pdf
drwxr-xr-x 3 kali kali 4.0K Apr 17 01:12 Desktop
drwxr-xr-x 2 kali kali 4.0K Feb 25 14:19 Documents
drwxr-xr-x 2 kali kali 4.0K Apr 17 18:18 Downloads
drwxr-xr-x 2 kali kali 4.0K Feb 25 14:19 Music
drwxr-xr-x 2 kali kali 4.0K Feb 25 14:19 Pictures
drwxr-xr-x 2 kali kali 4.0K Feb 25 14:19 Public
drwxr-xr-x 2 kali kali 4.0K Feb 25 14:19 Templates
drwxr-xr-x 2 kali kali 4.0K Feb 25 14:19 Videos
drwxrwxr-x 2 kali kali 4.0K Apr 30 10:35 Xperts26-Antiransomware

(kali@kali)-[~]
$ cd Desktop/TTP-First

(kali@kali)-[~/Desktop/TTP-First]
$ swaks --server webmail.xperts.net \
--from finance@industry.com \
--to invoices@xperts.net \
--data @phishing_email.eml
```

Figure 8: Email Simulation

Info

This sends a crafted email containing a malicious attachment and URL.

Verify Email Delivery

1. Login to Windows VM Alpha:
2. **Username:** fortixperts
3. **Password:** Fortinet123#
4. Open **Firefox**
5. Access **webmail** bookmark
6. Login using:
7. **Username:** invoices
8. **Password:** Fortinet123#

Analyze Email

1. Open the recently received email
2. Observe the modified subject and observe the tag: [***Virus Removed***]
3. What else did FortiMail do to the email?

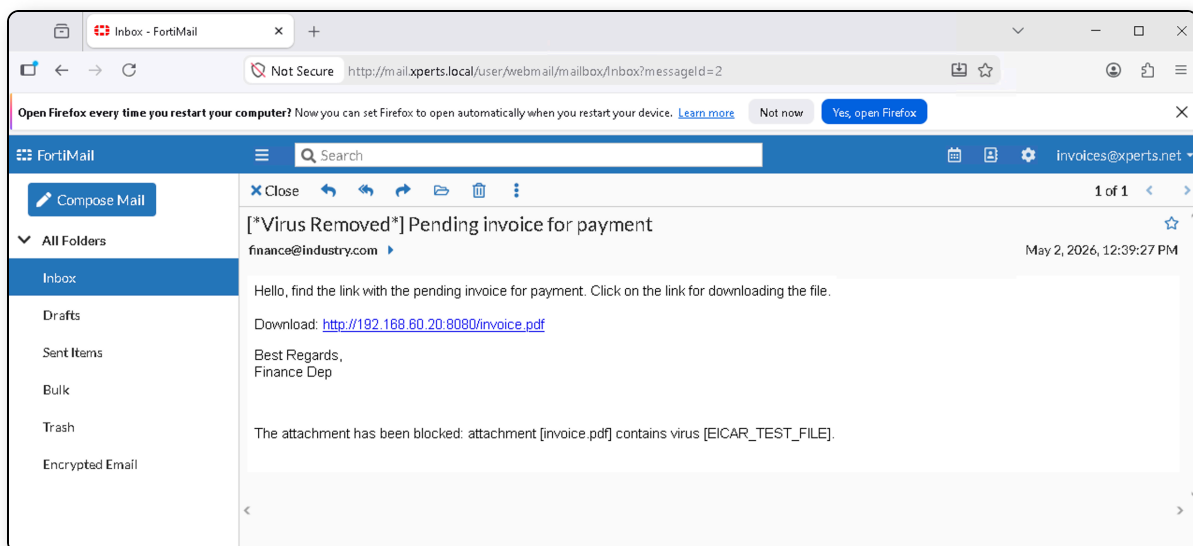


Figure 9: Email Inspection

Review FortiAnalyzer Results

1. Login to FortiAnalyzer GUI.
2. **Username:** admin
3. **Password:** Fortinet123#
4. Navigate to **Incidents & Events** → **Incidents**
5. Identify new incidents:
6. FML-Threat-Detection-By-Email: Malware detected in email
7. FML-Threat-Detection-By-Email: Malware detected in incoming email

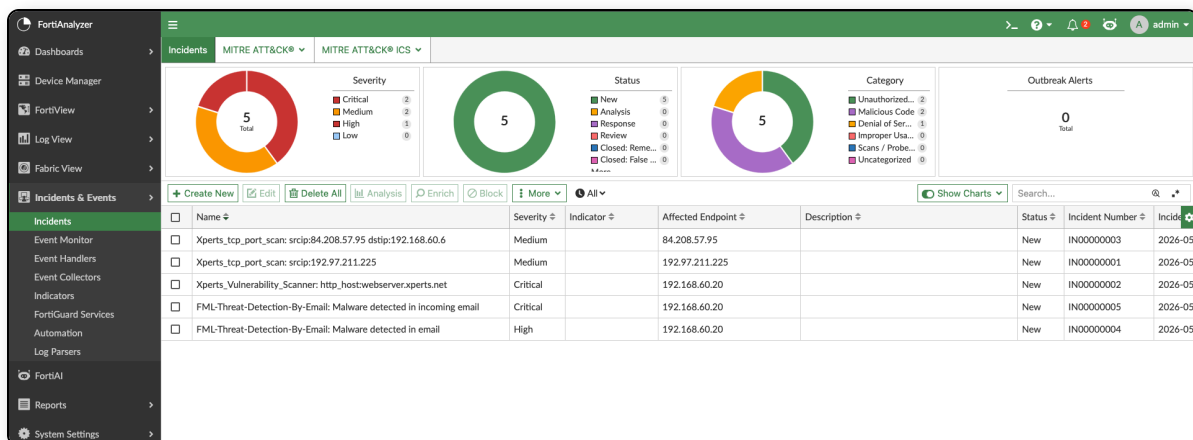


Figure 10: Incidents

Review MITRE ATT&CK Mapping

1. Navigate to **Incidents & Events** → **Incidents** → **MITRE ATT&CK** → **Attack**
2. Adjust timeframe if needed

Identify MITRE Techniques

1. What are the recently highlighted techniques in the matrix?
2. Explore the information they provide.

Answer: - T1566.001 Spearphishing Attachment - T1566.002 Spearphishing Link

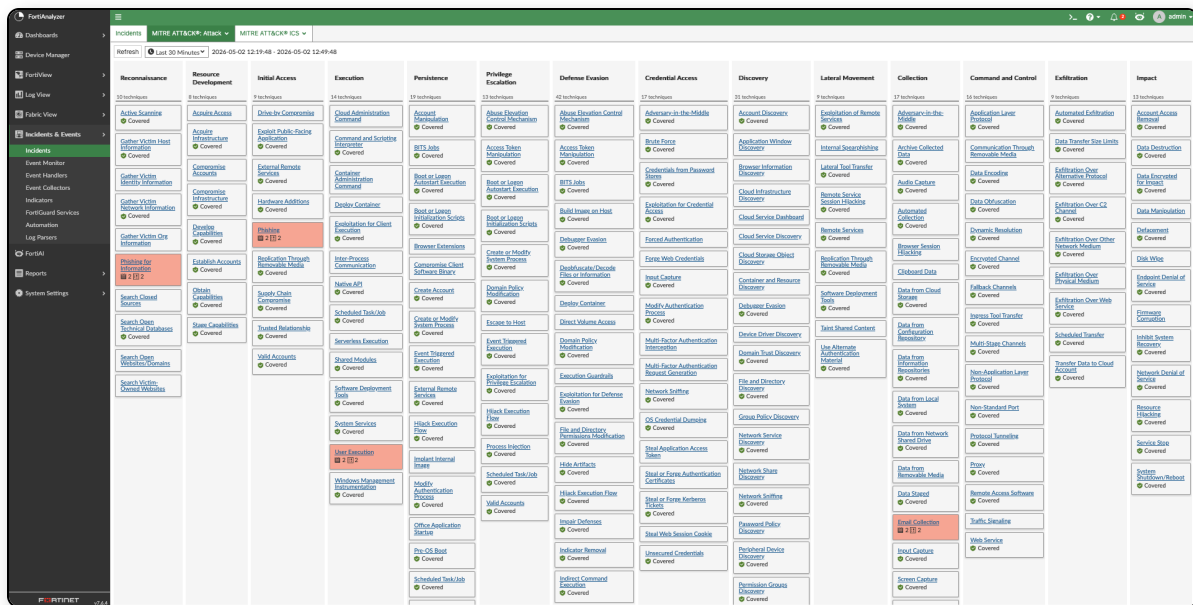


Figure 11: MITRE ATT&CK

Discussion

So, let's pause for a moment... did we prevent the attack?

Not necessarily.

The malicious attachment may have been blocked, but the email still contains a download URL. If the user clicks it, the attack could continue outside the original email control.

Prevention at one layer does not always mean the attack is over.

Now, let's move forward in the story...

The internal user *somehow* trusts the email and clicks the link.

This is where the attack evolves — transitioning from **Initial Access** into **Execution and beyond**, mapping new attacker behaviors.

Optional Exercise

How would you prevent the attack?

 Tip

By default, only a system administrator in FortiMail can release a System Quarantine element.

Lab 03. Execution and Command & Control

Estimated Time to Complete

40 minutes

Lab Access Information

Access Fabric Studio via https://<your_fabric_studio_ip> using the following credentials:

- **Username:** `admin`
- **Password:** `Fortinet123#`

System	Fabric Studio Name	Method	Username	Password	IP Address
FortiEDR Cloud	FortiEDR	HTTPS	<code>student-specific</code>	<code>student-specific</code>	<code>https://x pertsldata m.fortied r.com/</code>
FortiAnalyzer	FortiAnalyzer	HTTPS	<code>admin</code>	<code>Fortinet1 23#</code>	<code>https://< your_fabr ic_studio _ip>:1300 1</code>
Kali Linux	Kali	Display	<code>kali</code>	<code>Fortinet1 23#</code>	<code>https://< your_fabr ic_studio _ip>/cons ole/spice /basi00</code>

```
ic_studio_ip>/console/spice/wind00
```

Introduction

The attack has already entered the environment. In the previous lab, the user interacted with a phishing email. In this lab, the attacker moves one step forward by executing code on the endpoint and establishing outbound communications.

Using FortiEDR and FortiAnalyzer, this lab demonstrates how suspicious PowerShell behavior and repeated outbound connections can be detected, forwarded, and correlated into a broader attack narrative mapped to the MITRE ATT&CK framework.

FortiAnalyzer Preparation

Before reviewing FortiEDR logs in FortiAnalyzer, it is required to enable support for third-party log ingestion into FortiAnalyzer.

1. Access the FortiAnalyzer CLI via HTTPS using the following credentials:
2. **Username:** admin
3. **Password:** Fortinet123#

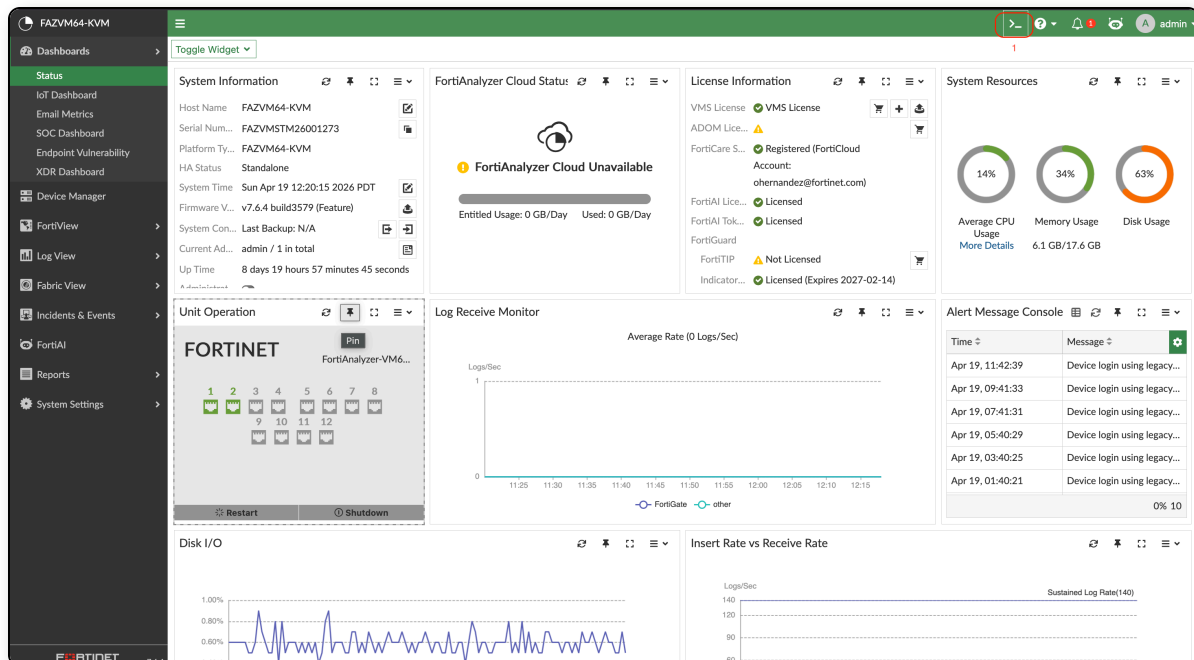


Figure 1: FortiAnalyzer CLI Access

1. Run the following commands:

```
config system log settings
    set unencrypted-logging-tcp enable
end
```

end

```
Connected
FAZVM64-KVM # config system log settings

(settings)# set unencrypted-logging-tcp enable

(settings)# end

FAZVM64-KVM # █
```

Figure 2: FortiAnalyzer CLI Commands

1. Verify the configuration is applied successfully.

i Info

This setting allows FortiAnalyzer to receive third-party logs over TCP when required by the integration method. It is off by default, so be aware to enable it in order to extend FortiAnalyzer capabilities. <https://community.fortinet.com/t5/FortiAnalyzer/Technical-Tip-How-to-add-a-third-party-device-to-FortiAnalyzer/ta-p/192587>

i Info

It is also important to enable the 3rd party log parser if required, additional information can be found at docs.fortinet.com <https://docs.fortinet.com/document/fortianalyzer/7.4.0/new-features/751895/support-parsing-and-addition-of-third-party-application-logs-to-the-siem-db>

FortiEDR Configuration

Install the Collector on Windows Alpha

Info

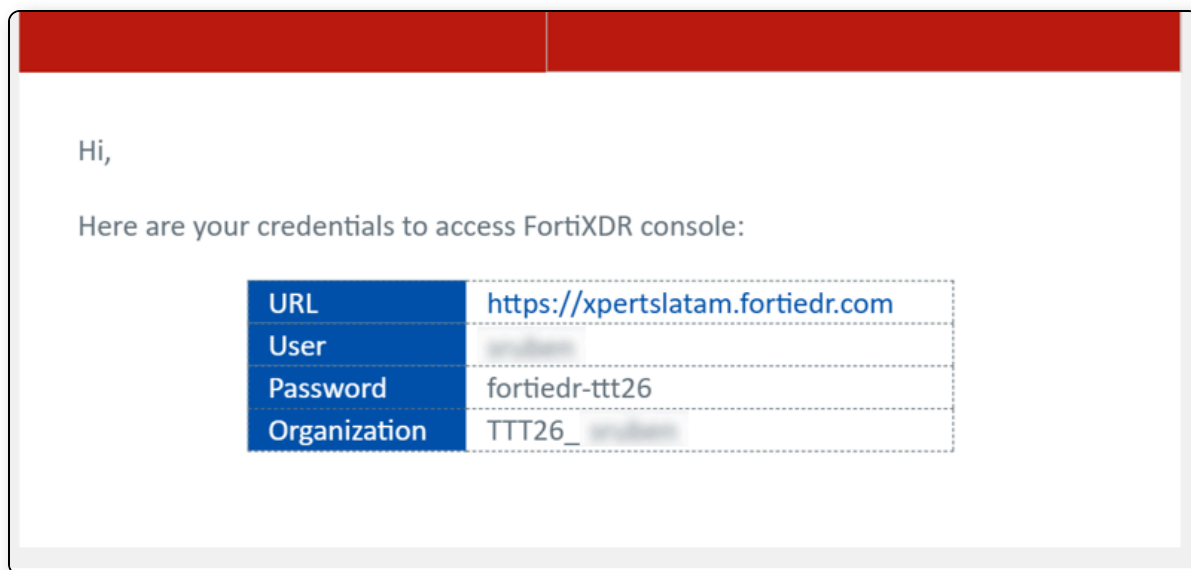
This step should be done already as part of a previous activity. If for any reason you need to re-deploy the EDR Collector here you can find the steps, otherwise jump to the next section "Assign the Collector to a Group"

1. Log in to **Windows VM Alpha**.
2. **Username:** fortixperts
3. **Password:** Fortinet123#

Accessing Your Organization

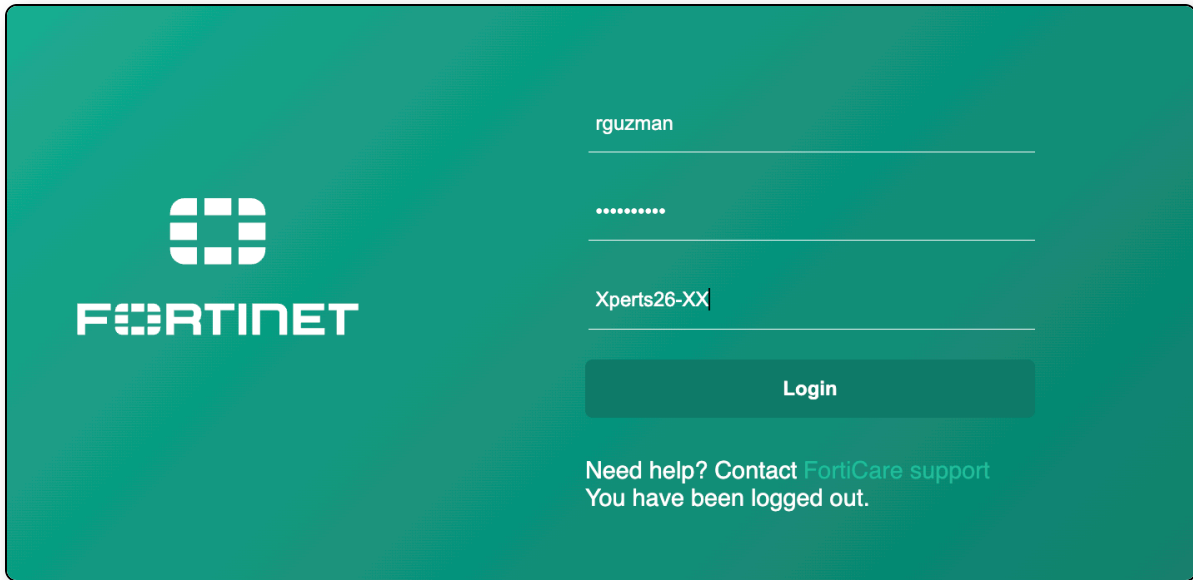
Access the FortiEDR Central Manager: <https://xpertslatam.fortiedr.com/>.

You will receive an email with your FortiEDR credentials, like this:



- **Username:** username
- Replace xxx with your assigned username received by email.
- **Password:** fortiedr-ttt26
- You will be prompted to change this password upon first login.

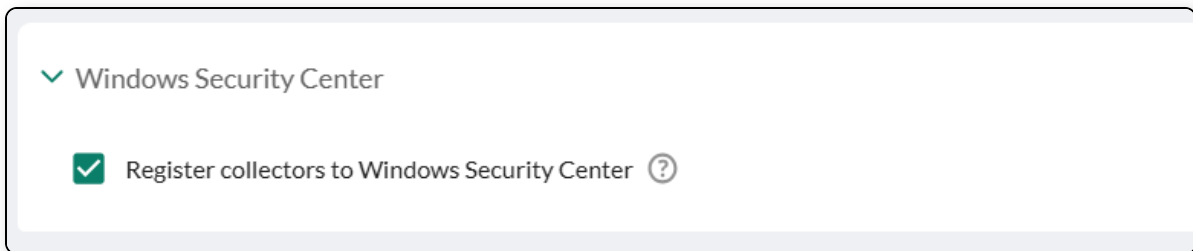
- **Organization Name:** TTT26_XX
- Replace **XX** with your organization suffix received by email.

The image shows the Fortinet login interface. On the left is the Fortinet logo. On the right, there are three input fields: the first contains 'rguzman', the second contains a masked password '.....', and the third contains 'Xperts26-XX'. Below these fields is a 'Login' button. At the bottom right, there is a message: 'Need help? Contact FortiCare support' and 'You have been logged out.'

 Danger

Before move on installing FortiEDR, we need to make sure it's integrated to Windows Security Center so Windows Defender does not conflict with our FortiEDR installation.

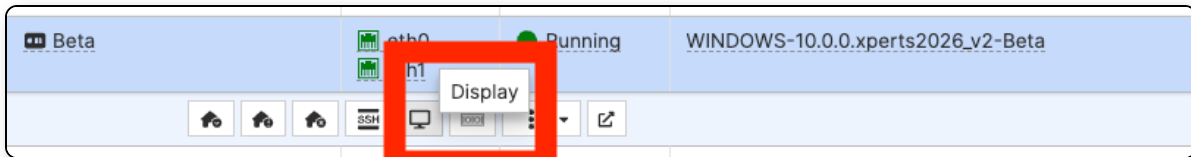
To enable this option, in your FortiEDR Manager console, go to `Administration > Settings` and search for the `Windows Security Center` section. Enable the option `Register collectors to Windows Security Center` by clicking in the checkbox.

The image shows a settings panel for 'Windows Security Center'. It has a green checkmark icon to the left of the title. Below the title, there is a checkbox labeled 'Register collectors to Windows Security Center' which is checked, followed by a help icon (a circle with a question mark).

Windows VM Login and FortiEDR Client Installation

Accessing the Windows VM

1. Log in to the FortiPOC VM Environment:
2. Locate the Windows VM and access it via **DISPLAY**.



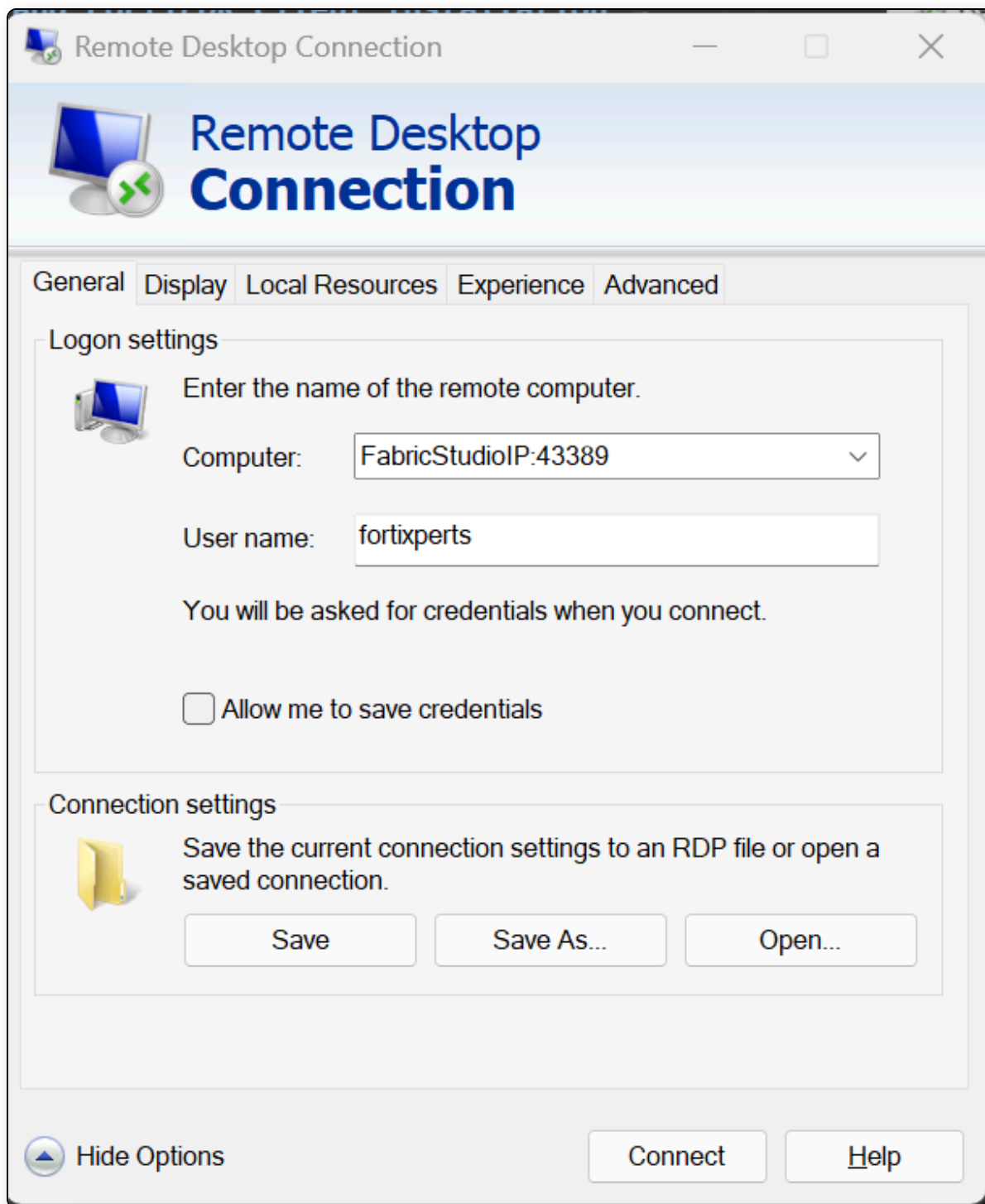
1. Use Remote Desktop Protocol (RDP):
2. It is recommended to use RDP.
3. Use the FortiPOC public IP (visible in your browser URL).
4. Connect via RDP (port 43389):
5. Username: `fortixperts`
6. Password: `Fortinet123#`

Important: Save the RDP file for reuse.

1. Copy the FortiPOC IP address from your browser.

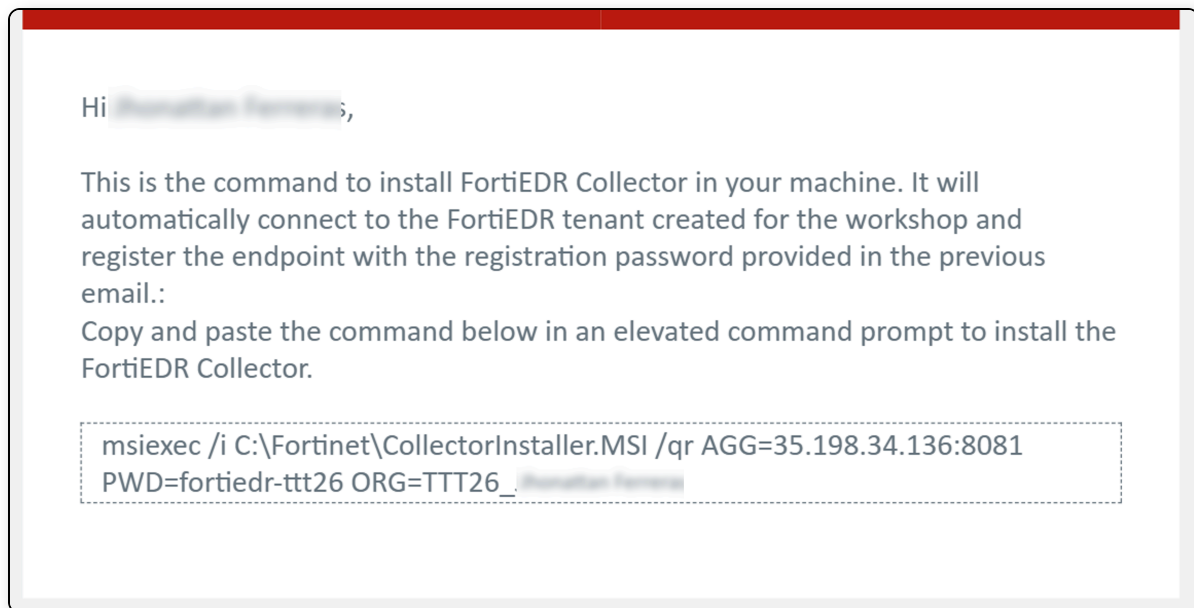


1. Open your RDP client and connect using the IP and port.



Deploying FortiEDR Collector

You might have received an email with your own `customized` installation command line, like this:



We did this way to make things easier for you to just copy and paste the command line.

 Warning

If you haven't received it, you can run it manually, replacing the {VARIABLES} with the your own.

```
msiexec /i C:\Fortinet\CollectorInstaller.MSI /qr AGG=35.198.34.136:8081 PWD={FORTIEDR_PASSWORD_ON_THE_EMAIL} ORG={YOUR_ORGANIZATION_NAME}
```

 Note

Do not forget: the registration password is the same one you have received on your email with the other FortiEDR credentials, even if you have changed it, it will keep the same registration password!

On your windows machine (Alpha), open the command prompt as an Administrator and run your FortiEDR installation command, like this:

```
Administrator: Command Prompt
Microsoft Windows [Version 10.0.26100.8246]
(c) Microsoft Corporation. All rights reserved.

C:\Windows\System32>msiexec /i C:\Fortinet\CollectorInstaller.MSI /qr AGG=35.198.34.136:8081
PWD=fortiedr-ttt26 ORG=TTT26_MY_ORGANIZATION_NAME
```

Verify the Collector is Reporting

1. Open the FortiEDR Cloud console.
2. Log in using the credentials provided by the instructor.
3. Confirm the correct organization is selected before continuing.

Info

FortiEDR credentials are unique per student. Use the credentials assigned to your lab instance.

1. Navigate to **Assets** → **Inventory**.
2. Confirm the collector for **Windows Alpha** is visible and reporting properly, by default it should appear into the **Default Collector Group** with the hostname *AnomalyDetection*.

Info

Do not continue until the collector appears as active in inventory.

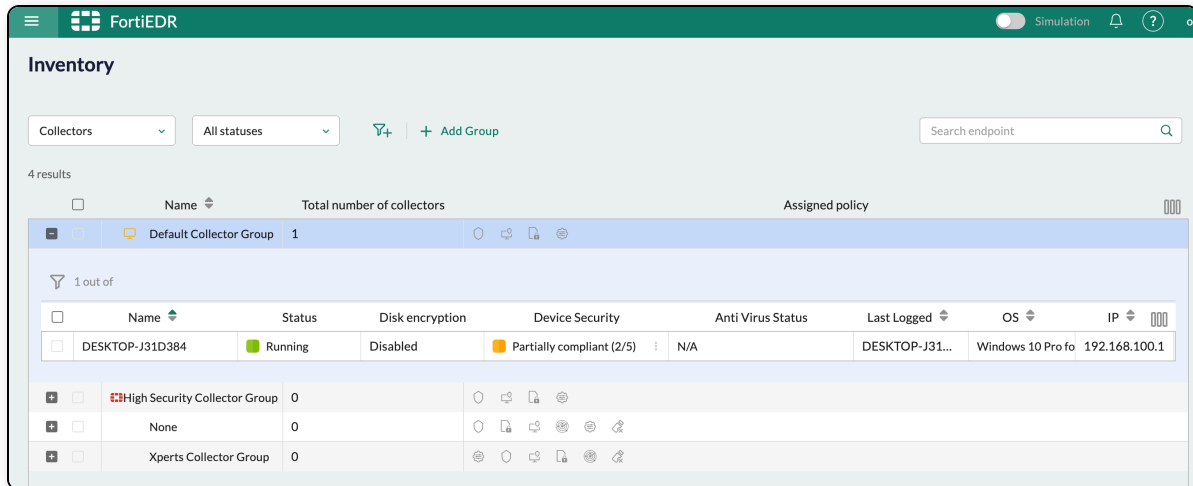


Figure 4: FortiEDR Inventory

Assign the Collector to a Group

1. Identify or create the group `Xperts Collector Group`, remember you can use groups in order to apply different FEDR policies per group.

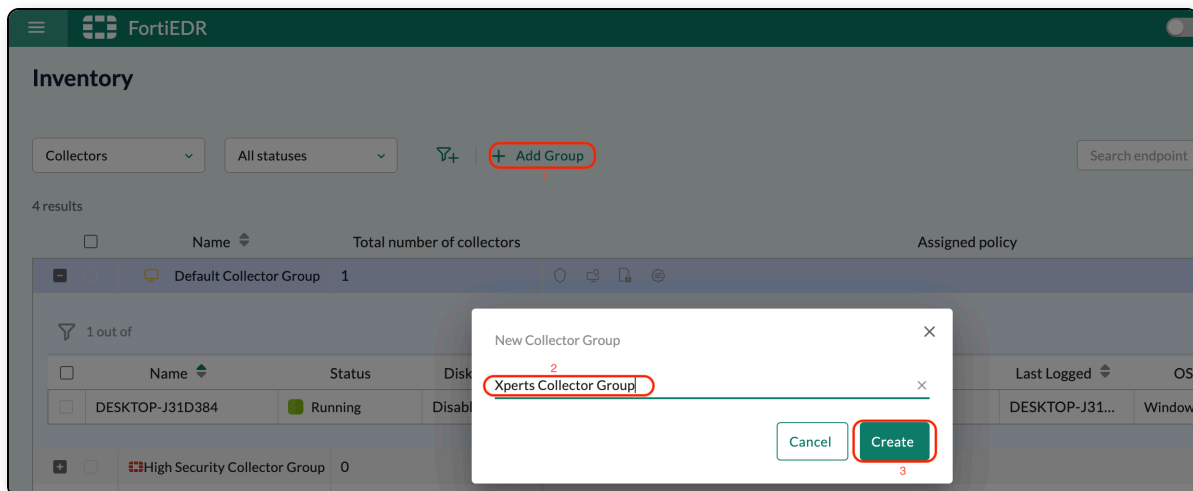


Figure 5: FortiEDR Group Creation

1. Select the collector for the Windows VM.
2. Move it to `Xperts Collector Group`.
3. Click **Move** to confirm.

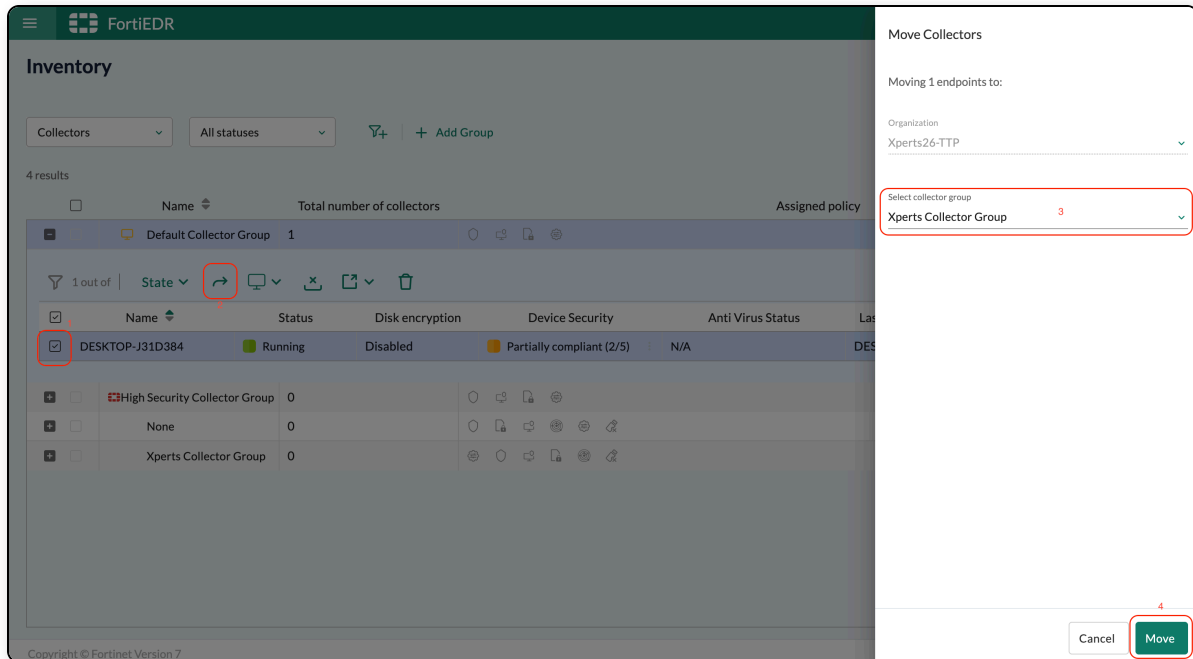


Figure 6: FortiEDR Group Assignment

Clone and Assign Security Policies

1. Navigate to **Profiles** → **Security** → **Policies**.
2. Select all the available policies but the one named "Mobile Devices", as we DO NOT have mobile devices in the lab.
3. Click **Clone Policy**.
4. Add the prefix `xperts_` to the **Name** field of cloned policies.

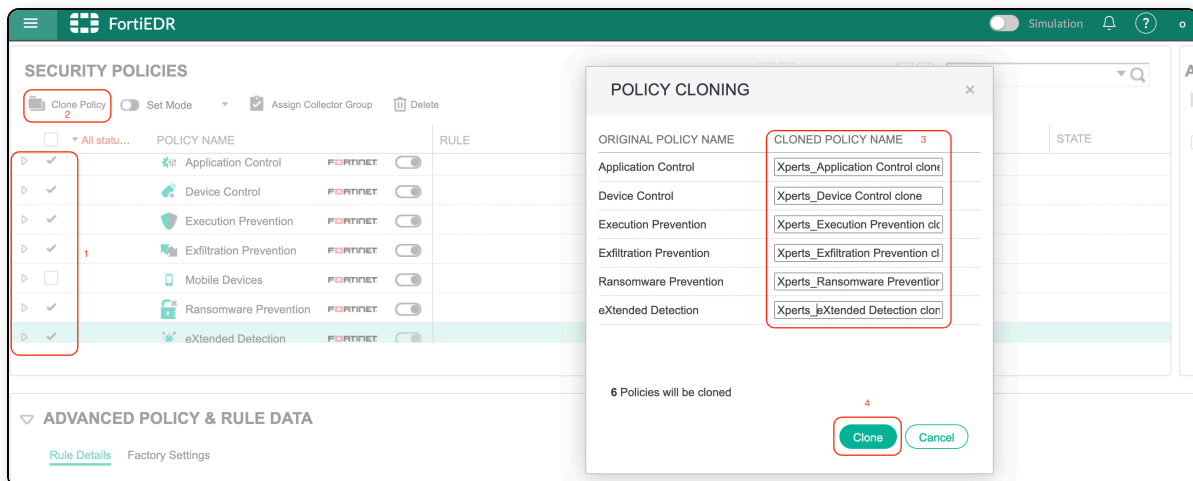


Figure 7: FortiEDR Policy Cloning

1. Use the search field to filter with the keyword `Xperts`.
2. Select all the policies containing the prefix keyword `Xperts`.
3. Assign the cloned policies to the group `Xperts Collector Group`.
4. Click the **Assign Collector Group** button.
5. Click the **Assign** button, there's a pop-up window asking for confirmation, click **Assign**.
6. Another pop-up confirming the assignment, click **Close**.

Info

This allows the collector group to use a dedicated policy set for the lab without modifying the default profiles.

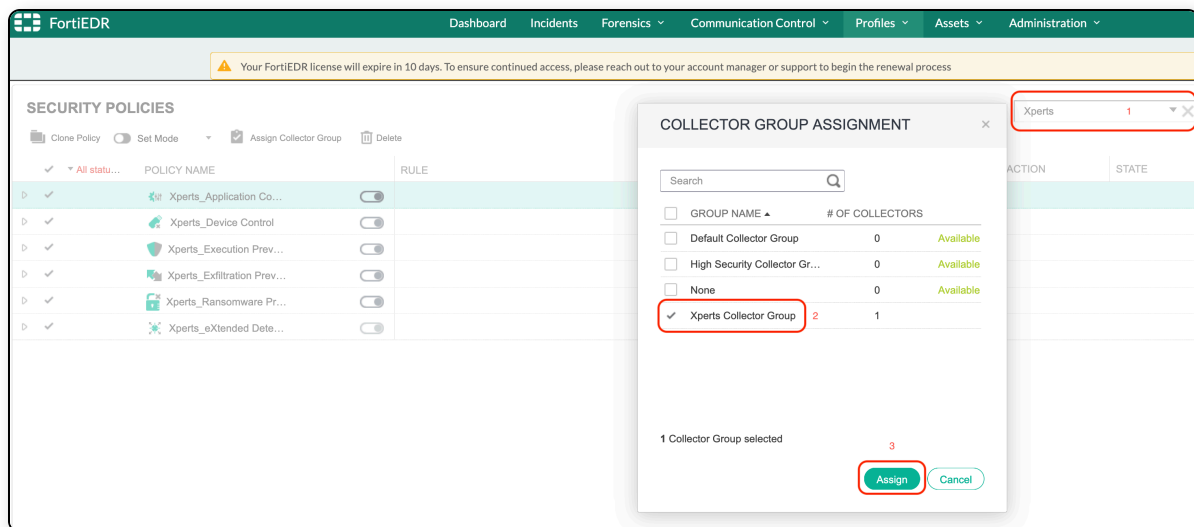


Figure 8: FortiEDR Policies Assignment

Info

Before proceeding, ensure that the Policies Mode is set to **Simulation**. Remember, the goal here is only to detect behavior; however, in a production environment, using **Prevention** mode is strongly recommended.

Define a Syslog Server for FortiEDR

1. Navigate to **Profiles** → **Export Settings**

2. Click on **Define New Syslog**
3. Fill up the fields with the following settings:
4. **Name:** FAZ_Xperts
5. **Host:** <your_fabric_studio_ip>
6. **Port:** 514
7. **Protocol:** TCP
8. **TLS:** unchecked
9. **Format:** FAZ
10. **RFC:** 5424
11. Click on **Test**.
12. If test was successful, then click on the **Save** icon to the right of the entry.

 **Info**

This test should display a check mark if successful, otherwise, verify your settings or ask your instructor.

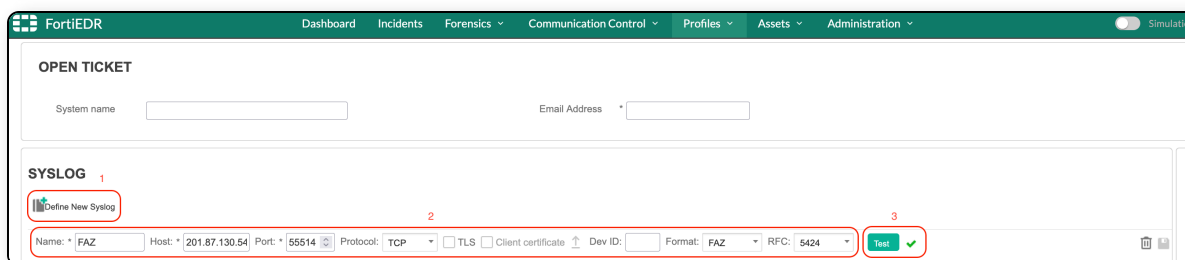


Figure 9: FortiEDR Syslog Configuration

FortiAnalyzer Configuration

Create a Correlation Event Handler for FortiEDR Logs

1. Access the FortiAnalyzer CLI via HTTPS using the following credentials:
2. **Username:** admin
3. **Password:** Fortinet123#
4. Navigate to **Incidents & Events** → **Event Handlers**. Click **Create New**.

5. Configure the handler with the following details:
6. **Name:** Xperts_FortiEDR_Correlation
7. **Event Handler Type:** Correlation
8. **MITRE Tech ID:** T1059.001 PowerShell
9. **MITRE Tech ID:** T1027.010 Command Obfuscation
10. **MITRE Tech ID:** T1543.003 Windows Service
11. **Automatically Create Incident:** On
12. **Threshold Duration:** 3m

Add New Correlation Event Handler

Status: ☒

Name: FortiEDR Correlation

Description:
0/1024

Event Handler Type: Basic **Correlation**

MITRE Tech ID:

 T1059.001 PowerShell ☒
 T1543.003 Windows Service ☒
 T1543.003 Windows Service ☒
 Click to select 3 entries selected

Automation Stitch: ☐

Automatically Create Incident: ☒

Data Selector: Click to select

Threshold Duration: 3m

Figure 12: FortiEDR Correlation Event Handler

1. Within the **Correlation Sequence** section Click + this is the **Add New Rule** button and configure the rule with the following details:
2. **Name:** Encoded Commands
3. **Log Device Type:** FortiEDR
4. **Log Type:** Event Log (event)
5. **Log Field 1:** Device_name

6. In the **Refine Your Logs** section, configure:

7. **Log Filters:** Any One of the Filters

8. **Remove the predefined Log Filter**

9. **Log Filter by Text:** threat_name==generic.powershell.fileless and command_line ~ '-EncodedCommand'

10. Click **OK**.

Edit Rule

Name

Encoded Commands

Choose Your Logs

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

Log Device Type

FortiEDR

Log Type

Event Log (event)

Log Field

Device Name (device_na...

Not in use

Not in use

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 FiltersAny One of the Filters

Log Field	Match Criteria	Value	Action
+			
Generic Text Filter threat_name==generic.powershell.fileless and command_line ~ '-EncodedCommand'			

77/2047

Define Event Conditions

Once you have 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

☐ Safeguard Risk Score is more than 0.5

☐ Advanced Mode COUNT(*)>=1

OK

Cancel

Figure 13: FortiEDR Rule 1

1. Repeat the creation of a new rule to be correlated with the previous one with the following details:
2. Click **+**
3. **Name:** `svchost Abuse Indicator`
4. **Log Device Type:** `FortiEDR`
5. **Log Type:** `Event Log (event)`
6. **Log Field 1:** `Device_name`
7. In the **Refine Your Logs** section, configure:
8. **Log Filters:** `Any One of the Filters`
9. **Log Field:** `Command Line`
10. **Match Criteria:** `Contains`
11. **Value:** `-k netsvcs -p -s`
12. Click **OK**.

Edit Rule

Name

svchost Abuse Indicator

Choose Your Logs

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

Log Device Type

FortiEDR

Log Type

Event Log (event)

Log Field

Device Name (device_na...

Not in use

Not in use

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
Command Line (com...	Contains	-k netsvcs -p -s	✕ +

Generic Text Filter

0/2047

Define Event Conditions

Once you have 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

☐
Safeguard Risk Score is more than
0.5

☐
Advanced Mode
COUNT(*)>=1

OK

Cancel

Figure 14: FortiEDR Rule 2

- Once you have created both rules, there's a new field activated for correlation, select the **AND** option.
- Below, in the **Correlation Criteria** we need to match a common field in both rules to be used as correlation so:
- Rule 1:** Encoded Commands
- Field 1:** device_name

5. Match Criteria: =

6. Rule 2: svchost Abuse Indicator

7. Field 2: `device_name`

8. Below, in the **Event Severity** field, select **High**

9. Click **OK** to save the Event Handler.

Edit Correlation Event Handler

Threshold Duration

3m

Correlation Sequence

Encoded Commands

AND

svchost Abuse Indicator

Show Raw Config

Correlation Criteria

Rule	Field	Match Criteria	Rule	Field	Action
Encoded Comma...	device_name	=	svchost Abuse In...	device_name	

Handler Settings

Event Type Override

Specify an event type, or leave blank to use default value

Event Message

Event Status

Click to select

Allow FortiAnalyzer to choose

Event Severity

High

Tags

Indicators

Log Field	Indicator Type	Count	Action

Additional Info

Use system default

Use custom message

Notifications

Click to select

OK

Cancel

Figure 15: FortiEDR Correlation Rule

i Info

This Event Handler is intended to correlate 2 different log types from FortiEDR and create a single Incident into FortiAnalyzer while highlighting the corresponding MITRE techniques.

Create a Custom Event Handler for Beaconsing Detection

1. Navigate to **Incidents & Events** → **Event Handlers**. Click **Create New**.
2. Configure the handler with the following details:
3. **Name:** Xperts_FortiGate_Beaconsing_Detected
4. **MITRE Tech ID:** T1071.001 Web Protocols
5. **Automatically Create Incident:** On

Add New Basic Event Handler

Status
Name *
Description

☒
FortiGate Beaconing Detected
0/1024

Event Handler Type
MITRE Tech ID

BasicCorrelation

T1071.001 Web Protocols

Click to select1 entry selected

Data Selector
Automation Stitch
Automatically Create Incident

Click to select
☐
☒

Rules

Add New Rule

Handler Settings

Notifications
Click to select

OKCancel

Figure 16: FortiGate Custom Event Handler

1. Click **Add New Rule** and configure the rule with the following details:
2. **Name:** FortiGate Possible Beaconing Detected
3. **Event Severity:** High
4. **Log Device Type:** FortiGate
5. **Log Type:** Traffic Log
6. **Log Subtype:** Any
7. **Log Field 1:** Source IP
8. **Log Field 2:** Destination IP

9. **Log Field 3:** Destination Port

10. In the **Refine Your Logs** section, configure:

11. **Log Filters:** All Filters

12. **Log Filter by Text:** dstport!='80' and dstport!='443' and dstport!='53'

13. Eliminate the default filter

14. In the **Define Event Conditions** section, configure:

15. **A group contains 3 or more log occurrences**

16. **All logs were generated within a duration of 1m**

17. Click **OK**.

18. Click **OK** again to save the Event Handler.

Add New Rule

Status

Name

FortiGate Possible Beaconing Detected

Event Severity

High

Choose Your Logs

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

Log Device Type

FortiGate

Log Type

Traffic Log (traffic)

Log Subtype

Any

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

Log Field

Source IP (srcip)

Destination IP (dstip)

Destination Port (dstport)

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
Level (pri)	Equal To	Emergency	× +

Log Filter by Text

dstport!='80' and dstport!='443'

32/2047

Define Event Conditions

OK

Cancel

Figure 17: FortiEDR Custom Event Rule

Define Event Conditions

Once you have 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 or more log occurrences

☐ Within a group, the log field has or more unique values

☐ The sum of is greater than or equal to

☐ Safeguard Risk Score is more than

☐ Advanced Mode

All logs were generated within a duration of

Advanced Settings >

OK

Cancel

Figure 18: FortiEDR Custom Event Rule

Configure FortiAnalyzer for FortiEDR Log Reception

1. Navigate to **Device Manager** → **Unauthorized Devices**.
2. You will see a Generic SYSLOG Server at first, this is the source of the TEST, however, once you get the first FortiEDR logs, you will see a new device to be *Authorized* it is important to authorize it, as it contains the FortiEDR Security Events.
3. Identify the **FortiEDR-VM** device and select it.
4. Click the **Authorize** button.

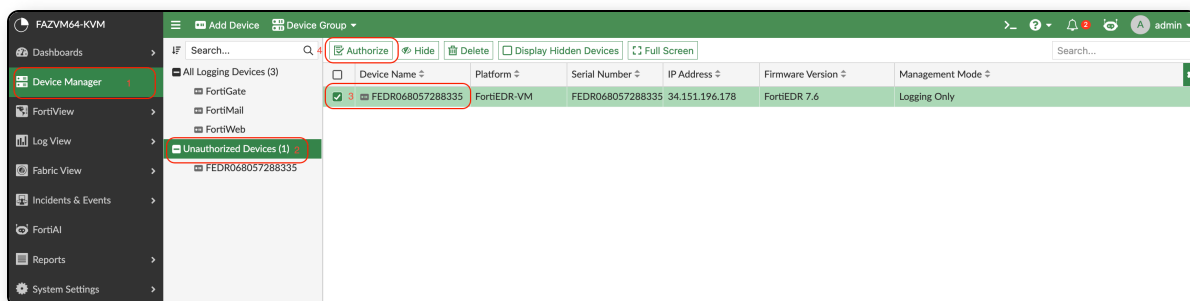


Figure 10: FortiEDR Syslog Authorization

1. Assign the name **FortiEDR**.
2. Click **OK**.
3. Click **Close**

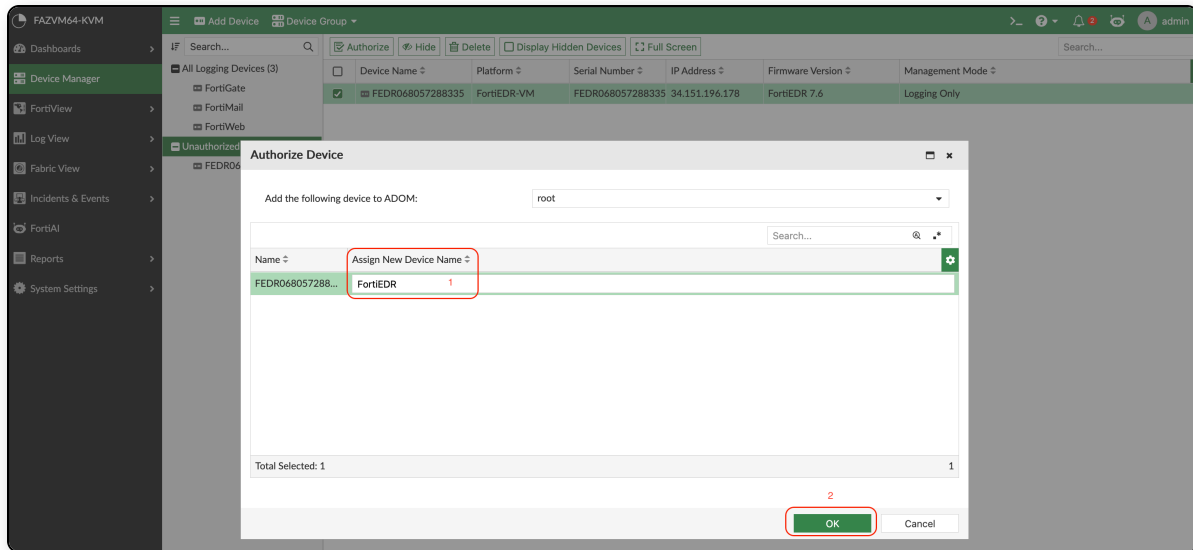


Figure 11: FortiEDR Syslog Authorization 2

Prepare for testing

Info

In this lab, Kali acts as a simple web server and a destination for outbound beaconing traffic generated by the script.

Verify the PowerShell Script is Present

1. Log in to **Windows VM Alpha** using the following credentials:
2. **Username:** fortixperts
3. **Password:** Fortinet123#
4. Open **File Explorer**.
5. Navigate to `C:\AtomicRedTeam\`.
6. Confirm the file `lab3_fortiedr.ps1` exists.

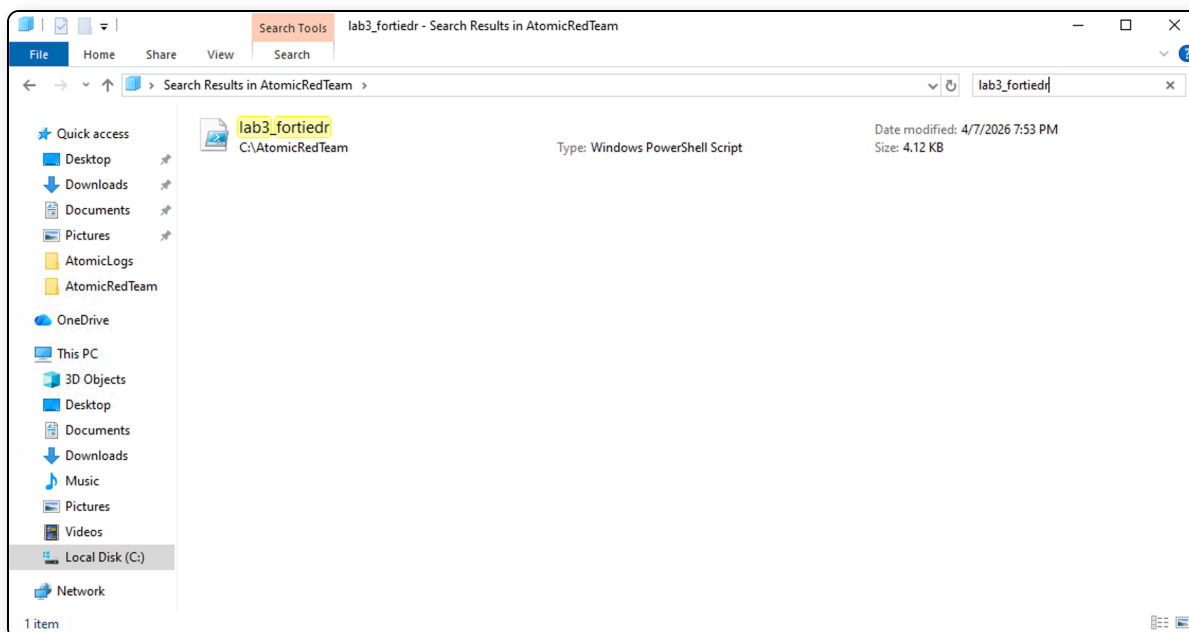


Figure 20: PowerShell Script Location

Info

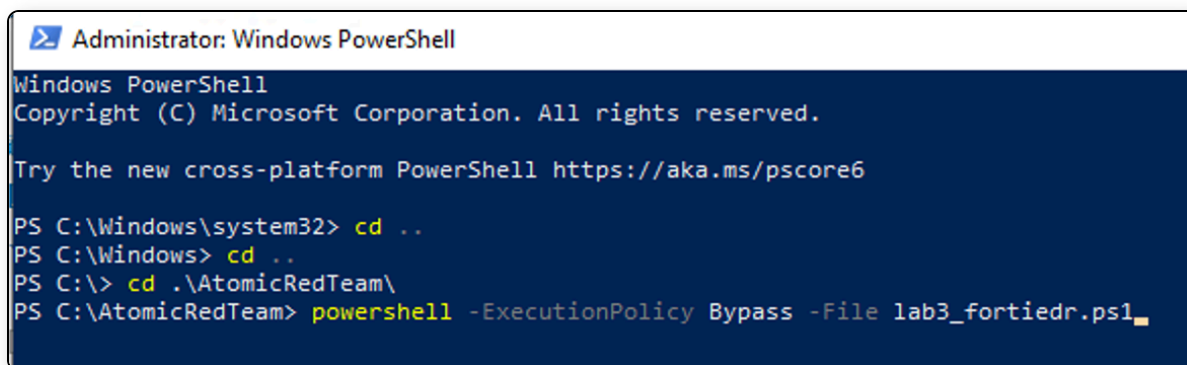
For this version of the lab, disable the Windows Antivirus so FortiEDR can detect the behaviors.

Execute the Attack Simulation

1. From the Windows ALPHA VM, open **PowerShell**.
2. Run the following command:

```
powershell -ExecutionPolicy Bypass -File C:\AtomicRedTeam\lab3_fortiedr.ps1
```

1. Wait for the script to complete.



```
Administrator: Windows PowerShell
Windows PowerShell
Copyright (C) Microsoft Corporation. All rights reserved.

Try the new cross-platform PowerShell https://aka.ms/pscore6

PS C:\Windows\system32> cd ..
PS C:\Windows> cd ..
PS C:\> cd .\AtomicRedTeam\
PS C:\AtomicRedTeam> powershell -ExecutionPolicy Bypass -File lab3_fortiedr.ps1
```

Figure 21: PowerShell Script Execution

What the Script Simulates

During execution, the script performs multiple common actions to emulate attacker behavior, including:

- Encoded PowerShell execution
- Scheduled task creation
- Basic host discovery activity
- Repeated HTTP beaconing to Kali
- Cleanup at the end of the test

Info

The script is configured to send 10 beacons with 2 seconds of delay between requests for testing purposes.

Info

Do you remember FortiEDR needs to be authorized in FortiAnalyzer in order to receive logs? If you have not Authorized it yet, do it now.

Review Results in FortiEDR

1. Return to the **FortiEDR** console.
2. Navigate to **Incidents** and adjust the time frame accordingly.

- Review the recent alerts or events associated with **Windows Alpha / AnomalyDetection**.
- Confirm the endpoint generated telemetry during the test window.

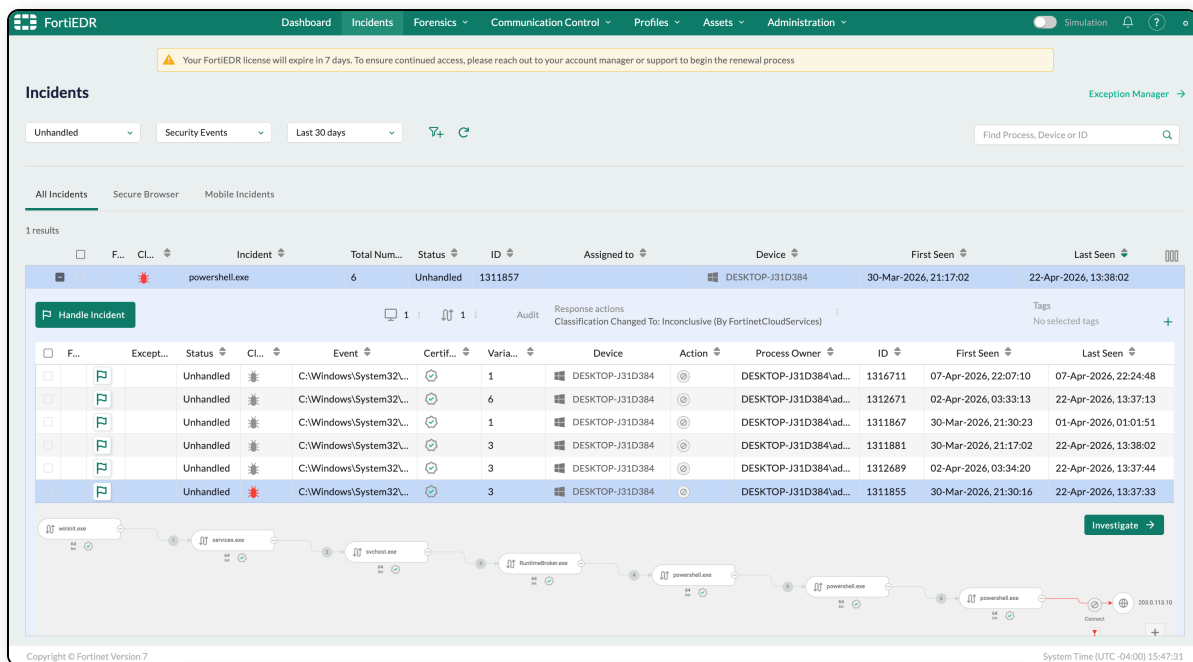


Figure 22: FortiEDR Console

Info

If no relevant FortiEDR detection appears, confirm the collector is active, the endpoint belongs to the correct group, and the cloned policies are assigned.

- From FortiEDR console you can start an investigation by selecting the incident and clicking the **Investigate** button.
- In the **Overview** section you will find details about *MITRE Techniques* by hovering the mouse over the corresponding *Violated Policies*.
- Explore the info FortiEDR provides.

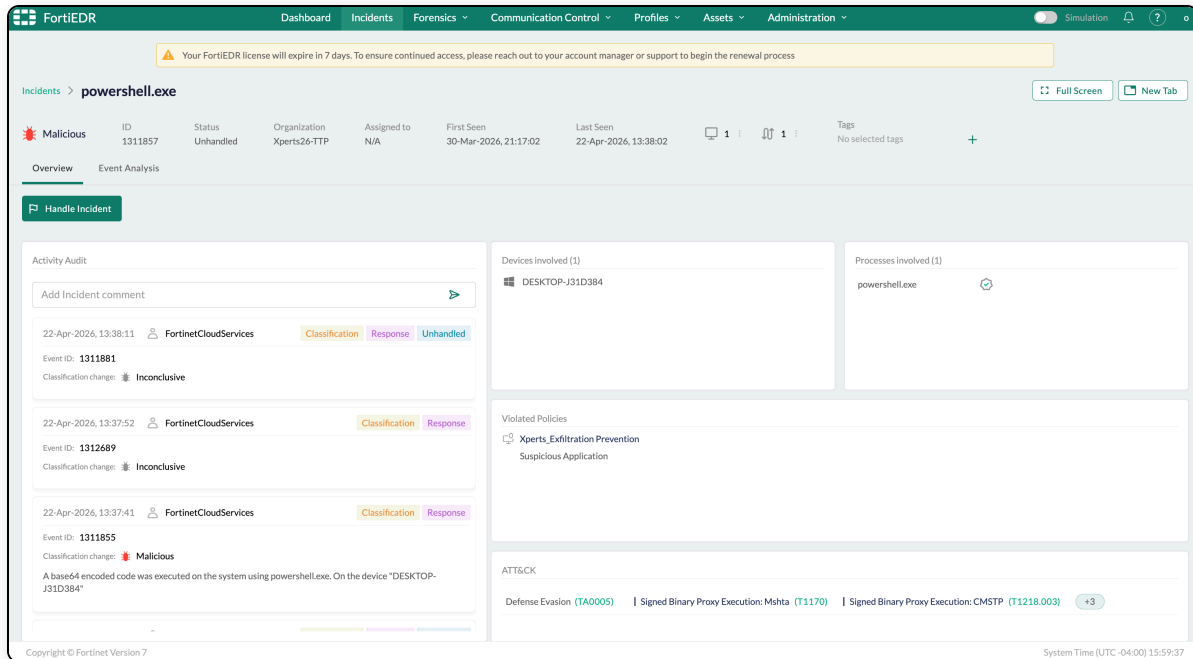


Figure 23: FortiEDR Console

Review Results in FortiAnalyzer

Review Incidents

1. In **FortiAnalyzer**, navigate to **Incidents & Events** → **Incidents**.
2. Identify the incidents generated from FortiEDR telemetry.

i Info

If no relevant FortiAnalyzer incidents appear, confirm the FortiEDR is Authorized in FortiAnalyzer. Execute the PowerShell script 2 or 3 times more.

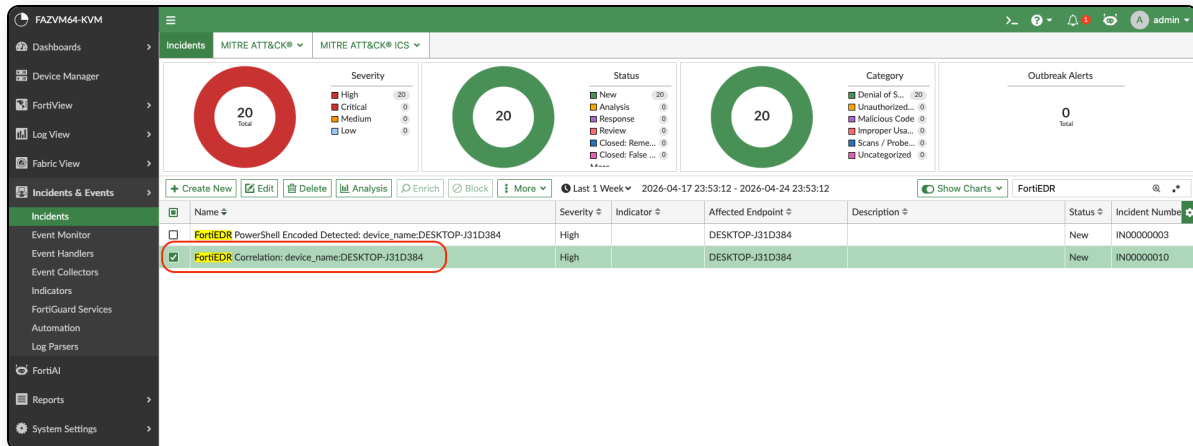


Figure 24: FortiAnalyzer Incidents

Review MITRE ATT&CK Mapping

1. Navigate to **Incidents & Events** → **MITRE ATT&CK**.
2. Adjust the timeframe if needed.
3. Look for the newly highlighted tactics and techniques associated with the lab execution.

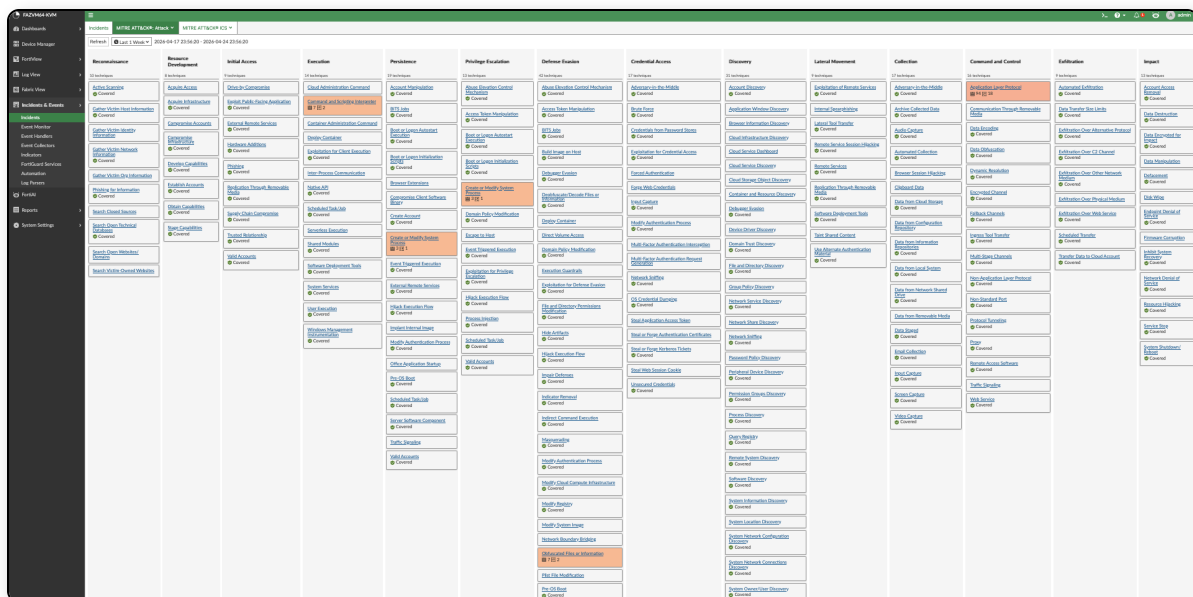


Figure 25: MITRE ATT&CK View

Identify the Detected Techniques

What are the behaviors identified by FortiAnalyzer while detecting the following MITRE techniques.

Answer: - T1059 Command and Scripting Interpreter: PowerShell - T1027 Obfuscated Files or Information - T1543 Windows Service - T1071 Web Protocols

Info

Depending on policy behavior and telemetry timing, additional techniques may appear. For this lab, focus first on the ones detected by the FortiEDR Event Handler.

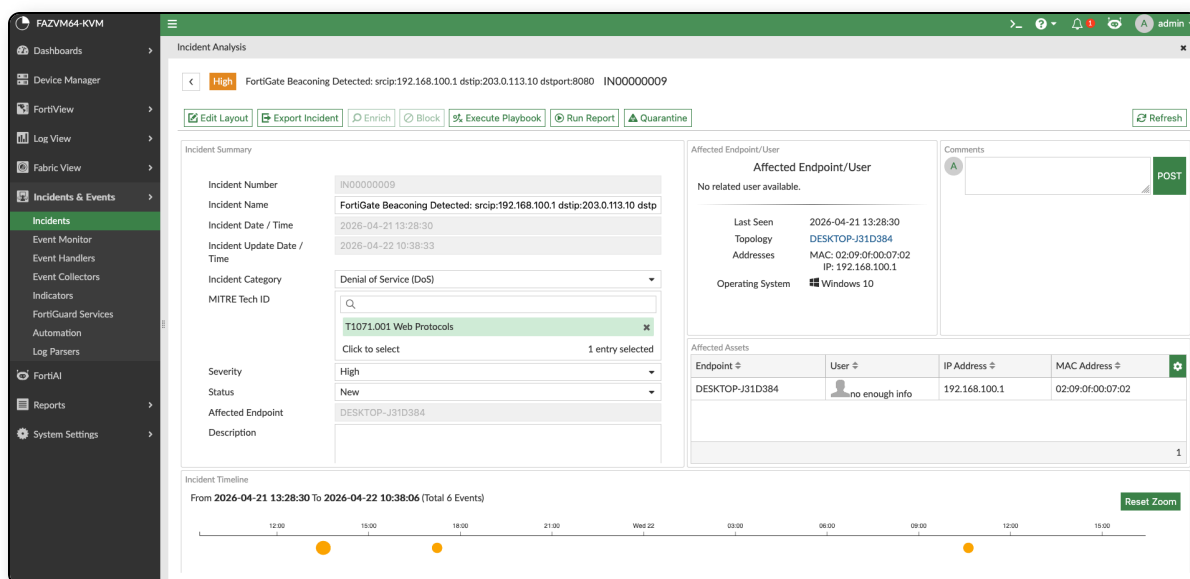


Figure 26: Beaconing Traffic Observed on Kali

Discussion

At this point, the attack is no longer limited to email delivery. The endpoint is now executing suspicious commands and generating outbound communications that resemble attacker-controlled activity.

This is where endpoint telemetry becomes critical.

Perimeter controls may detect the initial delivery attempt, but once the user interacts with the content and execution begins locally, products such as **FortiEDR** provide the visibility needed to identify suspicious behavior from the inside out.

By forwarding this telemetry into **FortiAnalyzer**, the SOC gains additional context and can connect isolated events into a broader attack narrative.

!!! info Remember it is possible to receive third-party logs into FortiAnalyzer by enabling the feature and parsers from version 7.4.X, this feature was enhanced in 7.6.0.

Optional Questions

1. Which FortiEDR detection provided the clearest signal of suspicious PowerShell activity?
2. What evidence in Kali suggests that outbound beaconing took place?
3. Why is endpoint visibility important after a phishing email is delivered?
4. How does FortiAnalyzer help transform endpoint alerts into MITRE-aligned incidents?
5. Identify other EDR solutions whose logs can be ingested into FortiAnalyzer for correlation and analysis.

Lab 04. Lateral Movement

Estimated Time to Complete

15 minutes

Lab Access Information

Access Fabric Studio via https://<your_fabric_studio_ip> using the following credentials:

- **Username:** `admin`
- **Password:** `Fortinet123#`

System	Fabric Studio Name	Method	Username	Password	IP Address
FortiGate	Enterprise_Core	HTTPS	<code>admin</code>	<code>Fortinet123#</code>	<a href="https://<your_fabric_studio_ip>:13000">https://<your_fabric_studio_ip>:13000
FortiSIEM	FortiSIEM	HTTPS	<code>admin</code>	<code>Fortinet123#</code>	<a href="https://<your_fabric_studio_ip>:13008">https://<your_fabric_studio_ip>:13008
Collector	Collector	Display	<code>root</code>	<code>Fortinet123#</code>	<a href="https://<your_fabric_studio_ip>/console/spice/fsm002">https://<your_fabric_studio_ip>/console/spice/fsm002
Ubuntu-					

DVWA	Ubuntu-DVWA	Display	user	Forti net12 3#	<a href="https://<your_fabric_studio_ip>/console/spice/basi01">https://<your_fabric_studio_ip>/console/spice/basi01
Windows VM	Alpha	Display	forti xpert s	Forti net12 3#	<a href="https://<your_fabric_studio_ip>/console/spice/wind00">https://<your_fabric_studio_ip>/console/spice/wind00

Introduction

After achieving execution and beaconing activity in Lab 3, the attacker leverages internal network trust to pivot into a Linux-based web server located in the DMZ.

Unlike external access, internal communications are often less restricted, making lateral movement significantly easier once an endpoint is compromised.

In this lab, we introduce FortiSIEM as a visibility and detection layer to identify this internal movement using network and system logs.

FortiSIEM Preparation

Let's start for preparing the FortiSIEM in order to receive some logs from *FortiGate* and *Web Server*.

!!! info FortiSIEM architecture relies on Collectors in order to receive logs from different sources, most of the times located in remote locaitons or representing a high log volume, for time constraints we have already deployed and register one collector to be used during the lab. This is required for certain operations, like File Integrity Monitoring (to be used in the next lab).

Configure Linux Web Server Syslog Forwarding

1. Connect to Ubuntu-DVWA server with the following credentials:
2. **Username:** user
3. **Password:** Fortinet123#
4. Open a terminal console

5. Using vi, edit **/etc/rsyslog.conf** `sudo nano /etc/rsyslog.conf`
6. Add the following line to define the Supervisor IP as syslog server. `*.* @10.20.0.19:514`
7. The shortcut to save using nano is *Ctrl+O* then *Enter*, for exit *Ctrl+X*.

```
GNU nano 6.2 /etc/rsyslog.conf *
# /etc/rsyslog.conf configuration file for rsyslog
#
# For more information install rsyslog-doc and see
# /usr/share/doc/rsyslog-doc/html/configuration/index.html
#
# Default logging rules can be found in /etc/rsyslog.d/50-default.conf

*.* @10.20.0.19:514

#####
#### MODULES ####
#####

module(load="imuxsock") # provides support for local system logging
#module(load="immark") # provides --MARK-- message capability

# provides UDP syslog reception
#module(load="imudp")
#input(type="imudp" port="514")

# provides TCP syslog reception
#module(load="imtcp")
#input(type="imtcp" port="514")

# provides kernel logging support and enable non-kernel klog messages
module(load="imklog" permitnonkernelfacility="on")

#####
#### GLOBAL DIRECTIVES ####
#####

#
# Use traditional timestamp format.
# To enable high precision timestamps, comment out the following line.
#
$ActionFileDefaultTemplate RSYSLOG_TraditionalFileFormat

# Filter duplicated messages
$RepeatedMsgReduction on

#
# Set the default permissions for all log files.
#
$FileOwner syslog
File Name to Write: /etc/rsyslog.conf
^G Help      M-D DOS Format  M-A Append    M-B Backup File
^C Cancel    M-M Mac Format  M-P Prepend    ^T Browse
```

Figure 1: Linux rsyslog config

1. Restart rsyslog service `sudo systemctl restart rsyslog`

2. Validate FortiGate Log Reception in FortiSIEM GUI:
3. Go to **Analytics** → **Search**
4. Filter by: `Reporting IP = 192.168.50.30` and click **Apply & Run**
5. Confirm log reception.

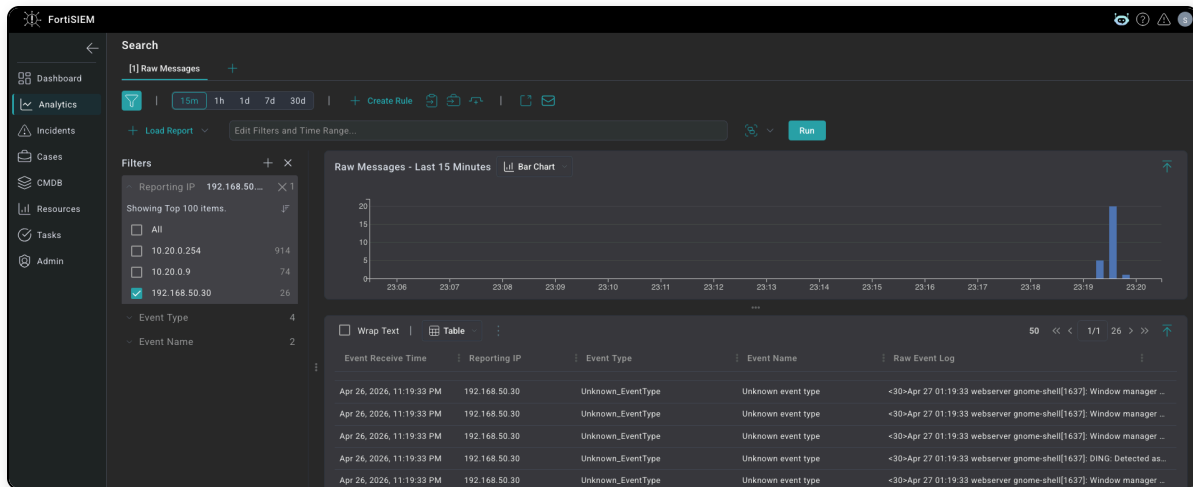


Figure 2: FortiSIEM Logs View

Forward FortiGate logs to FortiSIEM

1. Login to FortiGate GUI and open up CLI, copy and paste the following commands to define the syslog forwarding to FSIEM through Collector:

```
config log syslogd setting
set status enable
set server "10.20.0.19"
set mode udp
set port 514
set facility local7
set format default
end
```



Tip

Ensure policies have logging enabled (Log Allowed Traffic = All Sessions) to capture lateral movement later.

1. Validate FortiGate Log Reception in FortiSIEM GUI:

2. Go to **Analytics** → **Search**

3. Filter by: `Reporting IP = 10.20.0.254` and click **Apply & Run**

4. Confirm logs.

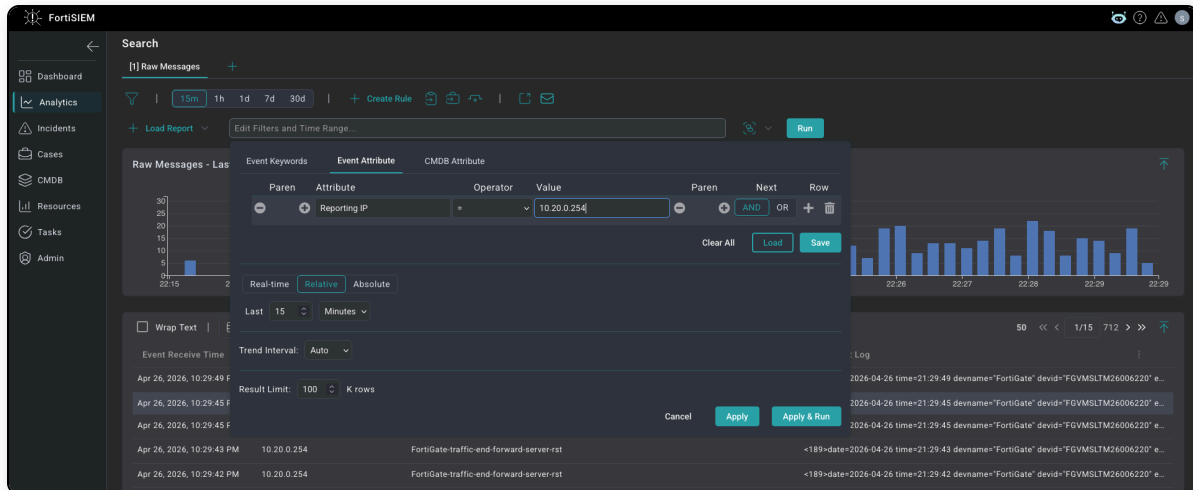


Figure 3: FortiSIEM Logs View

Create a Custom Correlation Rule

1. Into FortiSIEM Supervisor, navigate to **Resources** → **Rules**.

2. Click on **+** to create a new rule.

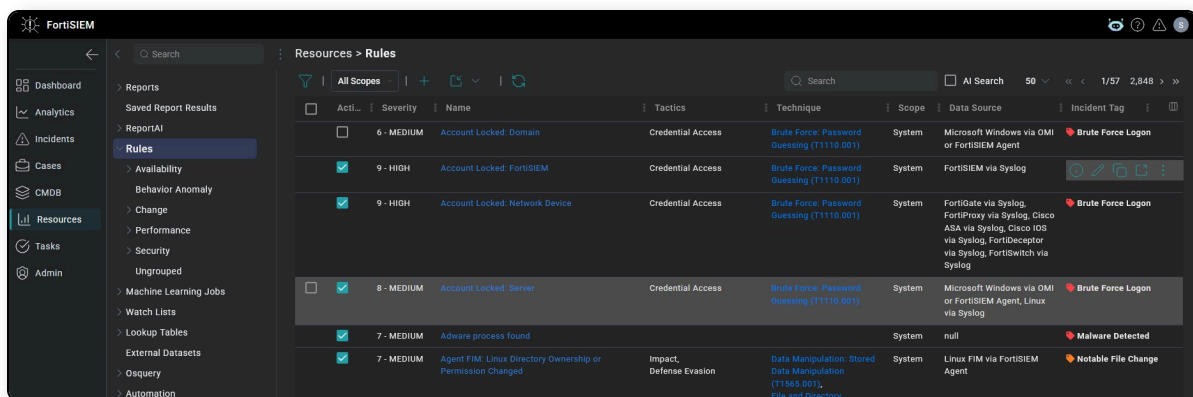


Figure 4: FortiSIEM Create Rule

1. Fill the details for the 3 different steps.

Step 1: General

1. Fill up the fields with the following settings:

2. **Gourp:** Security
3. **Rule Name:** Xperts-Suspicious-SSH-Connection-Correlation
4. **Detection Technology:** Correlation
5. **Evaluation Mode:** Streaming

Step 2: Define Condition

1. Create **filter_0** and fill up the fields with the following settings:
2. **Attribute 1:** Event Type
3. **Operator 1:** =
4. **Value 1:** Generic_Unix_Successful_SSH_Login
5. **Next:** AND
6. **Attribute 2:** Source IP
7. **Operator 2:** IN
8. **Value 2:** 192.168.100.0/24
9. **Next:** AND
10. Into the **Aggregate** section:
11. **Attribute:** COUNT(Matched Events)
12. **Operator:** >=
13. **Value:** 1
14. Into the **Group By** section:
15. **Attribute:** Source IP
16. Click **Save**

Edit SubPattern

Name:

Filters:	Paren	Attribute	Operator	Value	Paren	Next	Row
[-] [+] Event Type		=	Generic_Unix_Successful_SSH	[-] [+] AND	OR	[+] [X]	
[-] [+] Source IP		IN	192.168.100.0/24	[-] [+] AND	OR	[+] [X]	

Aggregate:	Paren	Attribute	Operator	Value	Paren	Next	Row
[-] [+] COUNT(Matched Events)		>=	1	[-] [+] AND	OR	[+] [X]	

Group By: **Attribute**

Attribute	Row	Move
Source IP	[+] [-]	[↑] [↓]

Run as Query Save as Report Cancel Save

Figure 5: SubPattern 0

1. Create **filter_1** and fill up the fields with the following settings:
2. **Attribute 1:** `Destination IP`
3. **Operator 1:** `=`
4. **Value 1:** `192.168.50.30`
5. **Next:** `AND`
6. **Attribute 2:** `Service Name`
7. **Operator 2:** `=`
8. **Value 2:** `SSH`
9. **Next:** `AND`
10. **Attribute 3:** `Firewall Action`
11. **Operator 3:** `=`
12. **Value 3:** `accept`
13. **Next:** `AND`
14. **Attribute 4:** `Event Type`
15. **Operator 4:** `=`
16. **Value 4:** `FortiGate-traffic-forward`
17. **Next:** `AND`
18. Into the **Aggregate** section:

19. **Attribute:** COUNT(Matched Events)

20. **Operator:** >=

21. **Value:** 1

22. Into the **Group By** section:

23. **Attribute:** Source IP

24. Click **Save**

Edit SubPattern

Name: filter_1

Filters:	Paren	Attribute	Operator	Value	Paren	Next	Row
-	+	Destination IP	=	192.168.50.30	-	+	AND OR +
-	+	Service Name	=	SSH	-	+	AND OR +
-	+	Firewall Action	=	accept	-	+	AND OR +
-	+	Event Type	=	FortiGate-traffic-forward	-	+	AND OR +

Aggregate:	Paren	Attribute	Operator	Value	Paren	Next	Row
-	+	COUNT(Matched Events)	>=	1	-	+	AND OR +

Group By:	Attribute	Row	Move
	Source IP		+ - ↑ ↓

Run as Query Save as Report Cancel Save

Figure 6: SubPattern 1

1. Select **AND** as logical operator between SubPatterns

2. In the section **Given these Subpattern relationships:**

3. **Subpattern 1:** filter_0

4. **Attribute 1:** Source IP

5. **Operator:** =

6. **Subpattern 2:** filter_1

7. **Attribute 2:** Source IP

Suspicious SSH Connection Correlation - Edit Details

Step 1: General > **Step 2: Define Condition** > Step 3: Define Action

Condition: If this Pattern occurs within any 300 second time window

Paren	Subpattern	Paren	Next	Row
+	filter_1	+	AND	+
+	filter_2	+		+

Given these Subpattern relationships:

Subpattern	Attribute	Operator	Subpattern	Attribute	Next	Row
filter_1	Source IP	=	filter_2	Source IP	AND	+

Figure 7: Step 2 Conditions

Step 3: Define Action

1. Use the following settings:
2. **Severity:** 9 - HIGH
3. **Category:** Security
4. **Subcategory:** Lateral Movement
5. **Technique:** T1021.004 Remote Services: SSH
6. **Tactics:** Lateral Movement
7. **Tag:** Lateral Movement
8. **Update Status on Summary Dashboard:** Check

Suspicious SSH Connection Correlation - Edit Details

Step 1: General > Step 2: Define Condition > **Step 3: Define Action**

Severity: 9 - HIGH Update Status on Summary Dashboard: ☒

Category: Security Notification: 1 Hour

Subcategory: Lateral Movement Impacts: Other

Technique: [T1021.004] Remote Services: SSH

Tactics: Lateral Movement

Action: Defined

Exception: Undefined

Tag: Lateral Movement

Watch List: Defined

Clear: Undefined

Figure 8: Step 3 Define Action

1. For **Action** click on the **pencil icon** to edit:
2. **Event Attribute:** Source IP
3. **Subpattern:** filter_1

4. **Filter Attribute:** Source IP

5. **Incident Title:** Suspicious SSH Connection

6. For **Triggered Attributes** make sure you have the following selections:

- Event Receive Time
- Event Type
- Reporting IP
- Raw Event Log
- Source IP
- Destination IP

7. Click **Save**.

The screenshot shows a dark-themed dialog box titled "Generate Incident for: Suspicious SSH Connection Correlation". It contains the following sections:

- Incident Attributes:** A table with four columns: "Event Attribute", "Subpattern", "Filter Attribute", and "Row". The first row shows "Source IP" under "Event Attribute", "=" under "Subpattern", "filter_1" under "Filter Attribute", and a dropdown menu under "Row".
- Incident Title:** A text field containing "Suspicious SSH Connection".
- Insert Attribute:** A dropdown menu with a plus icon.
- Triggered Attributes:** A section with a search bar and a list of attributes. The list is divided into two columns. The left column contains: "Connection Use Time", "WLAN Max Host Txmit Rate Mbps", "Peak Connections", "WLAN AP Association Uptime", "Closed Connections", and "WLAN Protocol". The right column contains: "Event Receive Time", "Event Type", "Reporting IP", "Raw Event Log", "Source IP", and "Destination IP".
- Buttons:** "Cancel" and "Save" buttons at the bottom right.

Figure 9: Step 3 Action

1. For **Watch List** click on the **pencil icon** to edit:

2. **Incident Attribute:** Source IP

3. **Watch List:** Policy Violators

4. Click **Save**.

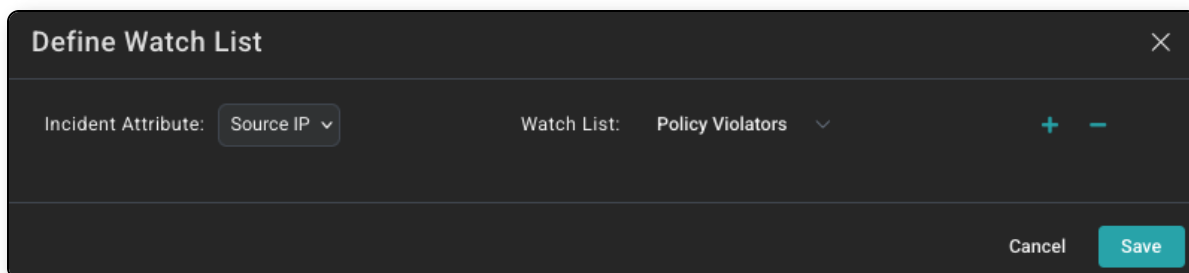


Figure 10: Step 3 Watch List

1. Click **Save** for the entire Rule.
2. Finally, find the recently created rule and enable it.

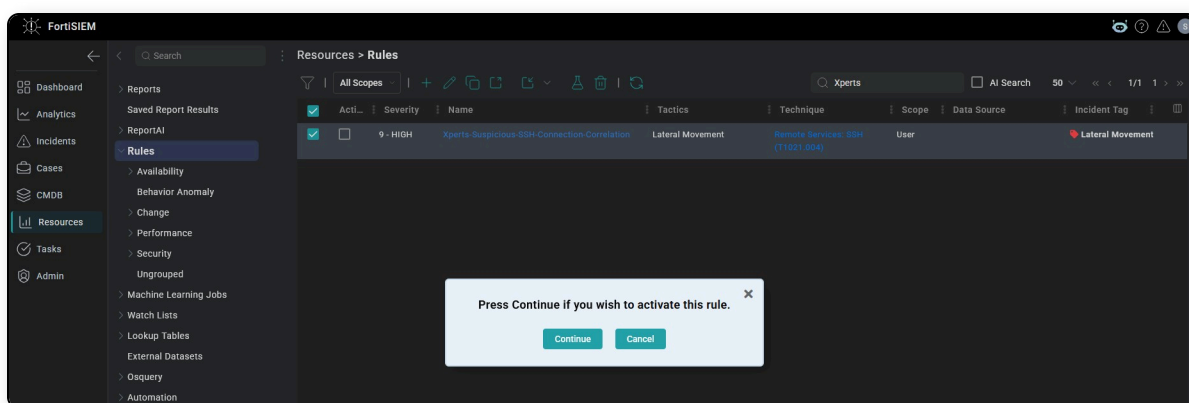


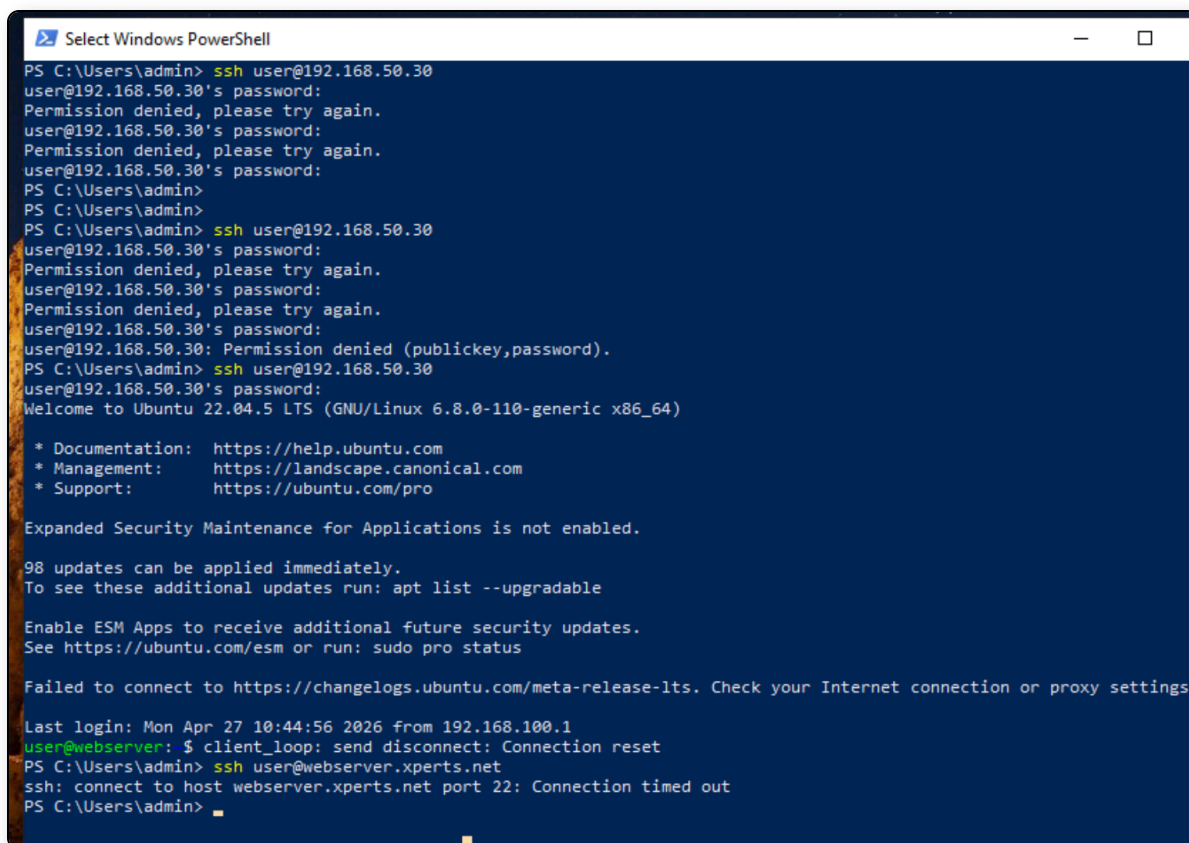
Figure 11: Enable the rule

Test the Correlation Rule

1. Connect to Windows VM Alpha.
2. **Username:** fortixperts
3. **Password:** Fortinet123#
4. Open a PowerShell terminal.
5. Execute a SSH connection directly to the Ubuntu-DVWA with wrong password.
Remember, internal access is often more relaxed, in this case, there is direct access to the webserver without considering the FortiWeb due to a misplaced firewall policy.
`ssh user@192.168.50.30`

!!! info Try at least 6 times to SSH with a wrong password, then try using the correct password.

1. You should be able to login successfully.



```
PS C:\Users\admin> ssh user@192.168.50.30
user@192.168.50.30's password:
Permission denied, please try again.
user@192.168.50.30's password:
Permission denied, please try again.
user@192.168.50.30's password:
PS C:\Users\admin>
PS C:\Users\admin>
PS C:\Users\admin> ssh user@192.168.50.30
user@192.168.50.30's password:
Permission denied, please try again.
user@192.168.50.30's password:
Permission denied, please try again.
user@192.168.50.30's password:
user@192.168.50.30: Permission denied (publickey,password).
PS C:\Users\admin> ssh user@192.168.50.30
user@192.168.50.30's password:
Welcome to Ubuntu 22.04.5 LTS (GNU/Linux 6.8.0-110-generic x86_64)

 * Documentation:  https://help.ubuntu.com
 * Management:    https://landscape.canonical.com
 * Support:       https://ubuntu.com/pro

Expanded Security Maintenance for Applications is not enabled.

98 updates can be applied immediately.
To see these additional updates run: apt list --upgradable

Enable ESM Apps to receive additional future security updates.
See https://ubuntu.com/esm or run: sudo pro status

Failed to connect to https://changelogs.ubuntu.com/meta-release-lts. Check your Internet connection or proxy settings

Last login: Mon Apr 27 10:44:56 2026 from 192.168.100.1
user@webserver:~$ client_loop: send disconnect: Connection reset
PS C:\Users\admin> ssh user@webserver.xperts.net
ssh: connect to host webserver.xperts.net port 22: Connection timed out
PS C:\Users\admin>
```

Figure 12: SSH login

Verify results in FortiSIEM

1. Navigate to **Incidents** → **Overview** to verify incidents creation.
2. Navigate to **Incidents** → **MITRE ATT&CK®IT** explore the panels **Rule Coverage**, **Incident Coverage** and **Incident Explorer**, make sure to adjust the timeframe accordingly.
3. Answer these questions:
4. What are the tactics and techniques detected?
5. Why are there some other incidents created?

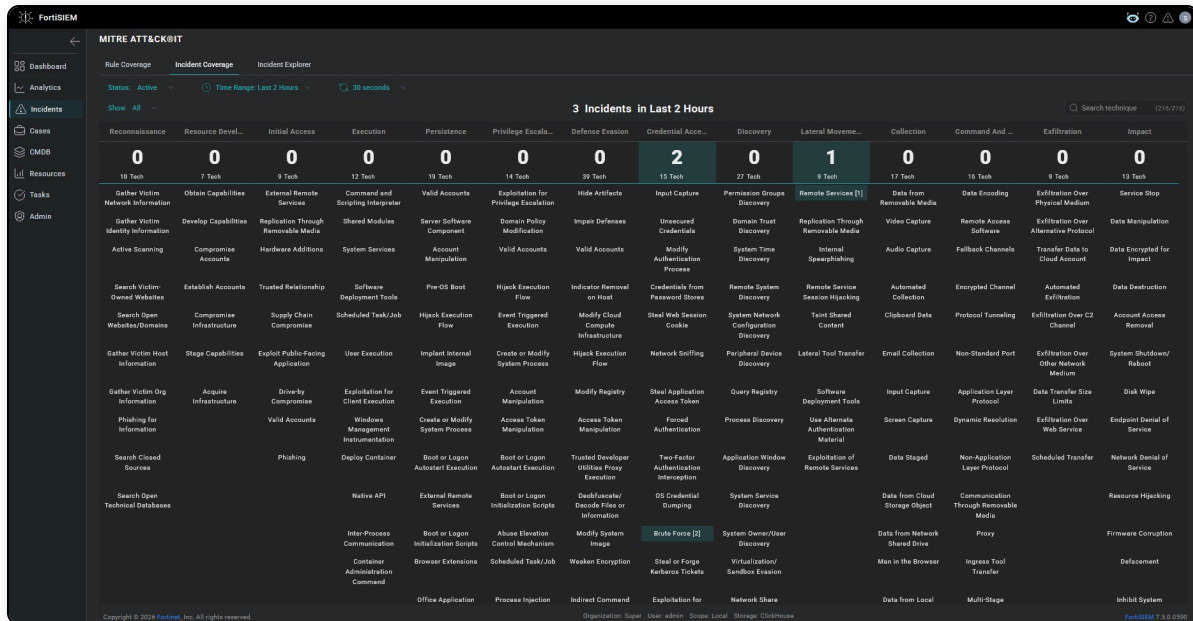


Figure 13: Incidents MITRE

Optional

1. How could you prevent the lateral movement based on the "Brute Force Attack" detected in FortiSIEM?

Lab 05. Impact

Estimated Time to Complete

20 minutes

Lab Access Information

Access Fabric Studio via https://<your_fabric_studio_ip> using the following credentials:

- **Username:** `admin`
- **Password:** `Fortinet123#`

System	Fabric Studio Name	Method	Username	Password	IP Address
FortiGate	Enterprise_Core	HTTPS	<code>admin</code>	<code>Fortinet123#</code>	<a href="https://<your_fabric_studio_ip>:13000">https://<your_fabric_studio_ip>:13000
FortiSIEM	FortiSIEM	HTTPS	<code>admin</code>	<code>Fortinet123#</code>	<a href="https://<your_fabric_studio_ip>:13008">https://<your_fabric_studio_ip>:13008
Collector	Collector	Display	<code>root</code>	<code>Fortinet123#</code>	<a href="https://<your_fabric_studio_ip>/console/spice/fsm002">https://<your_fabric_studio_ip>/console/spice/fsm002
Ubuntu-					

DVWA	Ubuntu-DVWA	Display	user	Forti net12 3#	<a href="https://<your_fabric_studio_ip>/console/spice/basi01">https://<your_fabric_studio_ip>/console/spice/basi01
Windows VM	Alpha	Display	forti xpert s	Forti net12 3#	<a href="https://<your_fabric_studio_ip>/console/spice/wind00">https://<your_fabric_studio_ip>/console/spice/wind00

Introduction

Every attack ultimately aims to create impact — whether by disrupting operations, altering critical data, or destroying system integrity.

In this lab, we simulate the final stage of an attack lifecycle by triggering unauthorized file modifications on a Linux Webserver and detecting them using File Integrity Monitoring (FIM) capabilities from FortiSIEM.

By leveraging the FortiSIEM Linux Advanced Agent, we gain deep visibility into logs, performance and file-level changes, allowing a SOC to detect behaviors aligned with MITRE ATT&CK Impact techniques such as:

T1565 – Data Manipulation T1485 – Data Destruction T1491 – Defacement

This lab demonstrates how endpoint-level telemetry complements network and behavioral detection from previous labs, providing high-confidence detection of real impact events.

FortiSIEM Advaced Agent for Linux Installation

FortiSIEM Configuration

1. Login to FortiSIEM Supervisor.
2. **Username:** user
3. **Password:** Fortinet123#
4. Navigate to **CMDB** → **Users** → **FortiSIEM Users** to create a new user for Agents Registration.
5. Click the + button.

6. Fill the **User Name:** `agent_user` .

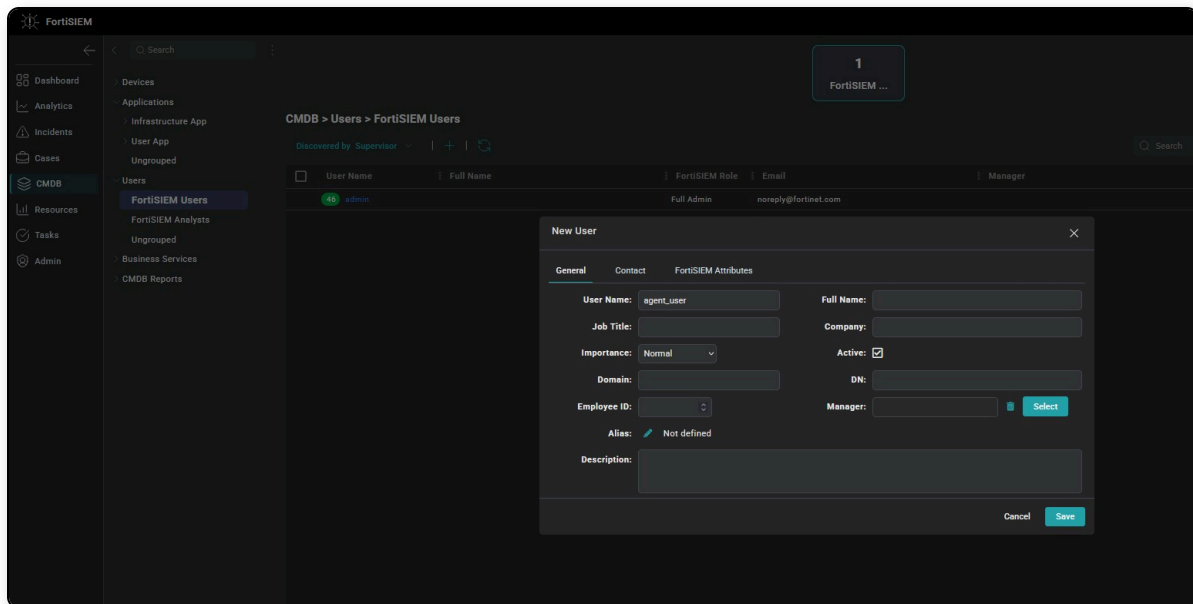


Figure 1: Agent Admin User

1. Move to **FortiSIEM Attributes** tab and check the **FortiSIEM Role** option, this will open a the **New User** creation window.
2. Check the option **Agent Admin** and fill the password `Fortinet123#` .
3. Click **Save**.

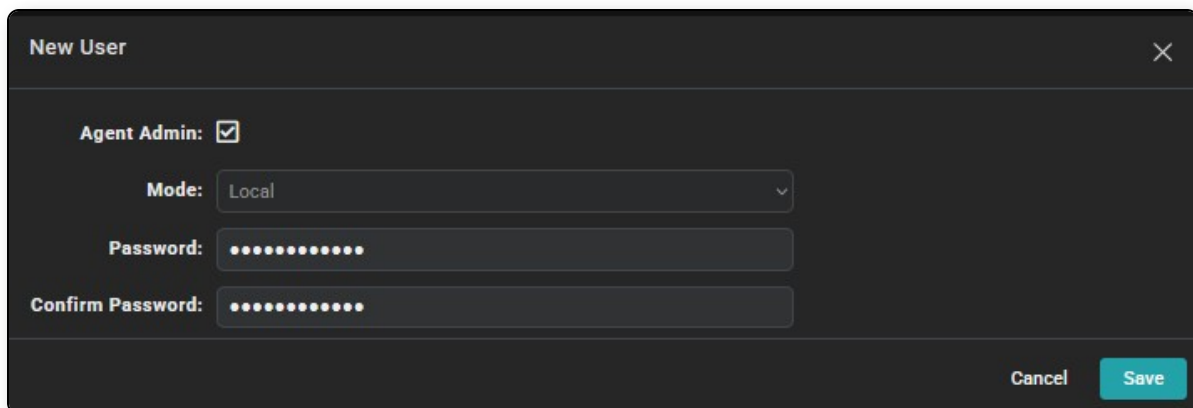


Figure 2: Agent Admin User Properties

1. Click **Save** again.
2. Navigate to **Admin** → **Setup** → **Linux Agent** tab to define *Host to template associations*.
3. Click the **+** sign to create a new template, fill the options as indicated:
 - **Name:** `Xperts-Webserver-Template`

4. Navigate to the **Monitor** tab, select all the available options to monitor, keep the time defaults.
5. Go to the **FIM** tab into the template and add the following items to be monitored by clicking the **+** sign, make sure to select the options **Create, Modify** and **Delete**
6. `/var/www/html/dvwa`
7. `/etc/apache2/`
8. `/etc/shadow`
9. Select from the **Actions** for each one:
10. Create
11. Modify
12. Delete
13. Push Files
14. Go to **Process Monitoring** tab, check the option `Process Monitoring`
15. Click **Save**

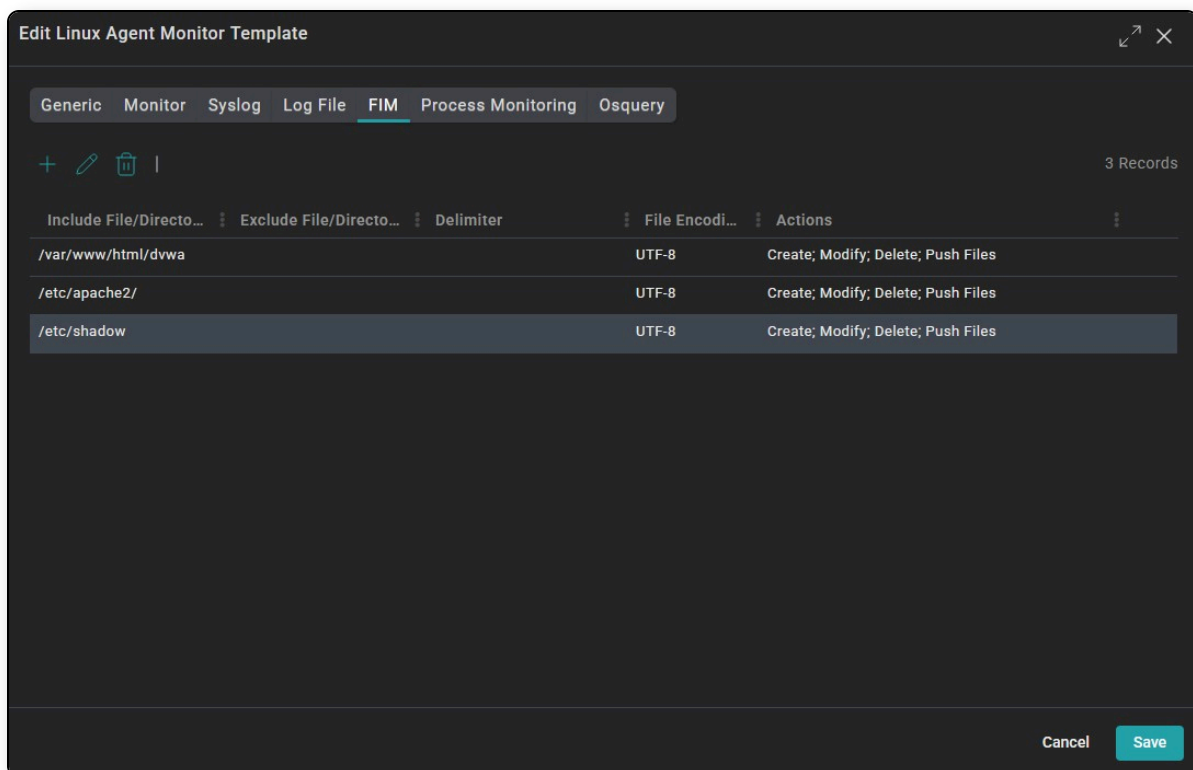
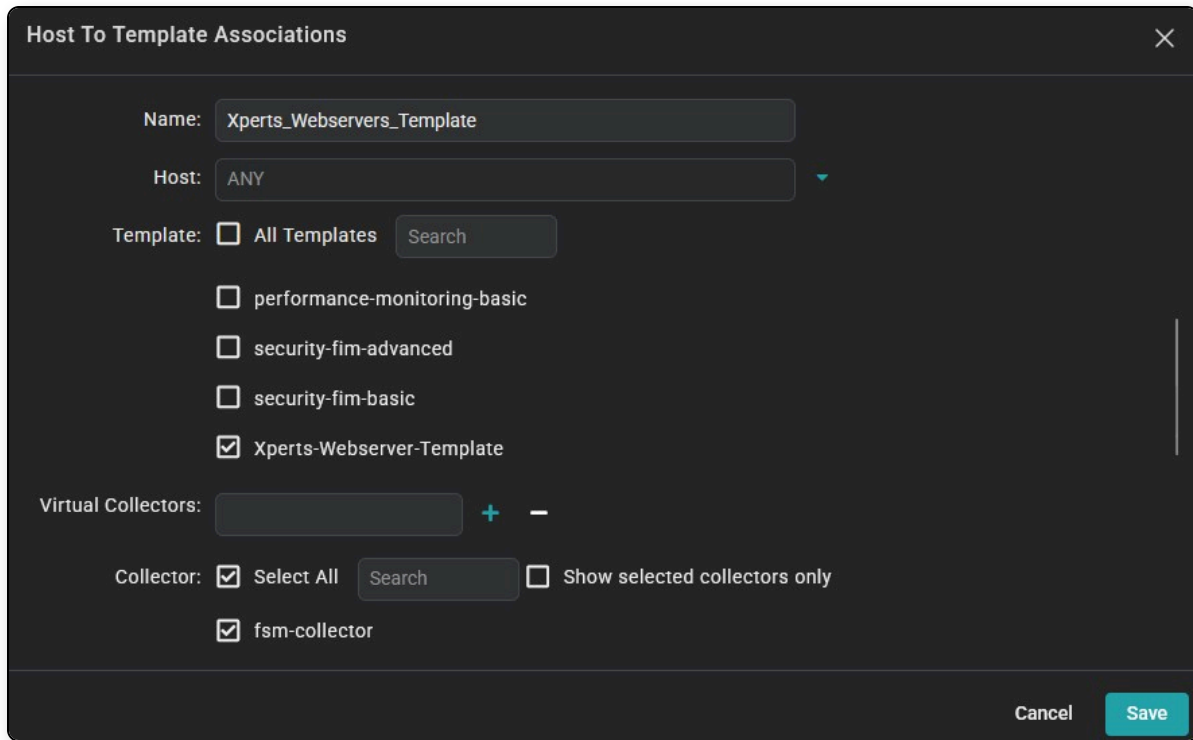


Figure 3: Agent Template

1. Click the **+** sign from **Host To Template Associations** section.

2. **Name:** Xperts_Webservers_Template
3. **Template:** Check Xperts-Webserver-Template
4. **Collector:** Check Select All
5. Click **Save**



The image shows a 'Host To Template Associations' dialog box with a dark theme. It contains several sections: 'Name' with a text field containing 'Xperts_Webservers_Template'; 'Host' with a dropdown menu showing 'ANY'; 'Template' with a list of templates where 'Xperts-Webserver-Template' is selected; 'Virtual Collectors' with a search bar and '+' '-' buttons; and 'Collector' with a list of collectors where 'Select All' and 'fsm-collector' are checked. There are 'Cancel' and 'Save' buttons at the bottom right.

Host To Template Associations

Name: Xperts_Webservers_Template

Host: ANY

Template: ☐ All Templates Search

- ☐ performance-monitoring-basic
- ☐ security-fim-advanced
- ☐ security-fim-basic
- ☒ Xperts-Webserver-Template

Virtual Collectors: + -

Collector: ☒ Select All Search ☐ Show selected collectors only

- ☒ fsm-collector

Cancel Save

Figure 4: Host to Template

Linux Agent Installation

!!! info FortiSIEM Advanced Agent for Linux is already present into Ubuntu-DVWA server.

1. Login into Ubuntu-DVWA via SSH through port 20022 using .
2. **Username:** user
3. **Password:** Fortinet123#
4. Open a terminal and navigate to the installer location `cd /home/user/Downloads`
5. Execute the following command for installation `sudo ./fortisiem-linux-agent-installer-7.5.0.0590.sh -s 10.20.0.19 -i 1 -o Super -u agent_user -p 'Fortinet123#' -n webserver`

```
user@webserver: ~/Downloads

1 additional security update can be applied with ESM Apps.
Learn more about enabling ESM Apps service at https://ubuntu.com/esm

New release '24.04.4 LTS' available.
Run 'do-release-upgrade' to upgrade to it.

Last login: Tue May  5 02:31:59 2026 from 10.254.1.254
user@webserver:~$
user@webserver:~$
user@webserver:~$ cd /home/user/Downloads/
user@webserver:~/Downloads$ pwd
/home/user/Downloads
user@webserver:~/Downloads$ sudo ./fortisiem-linux-agent-installer-7.5.0.0590.sh -s 10.20.0.19 -i 1 -o Super -u agent_user -p 'Fortinet123#' -n webserver
[sudo] password for user:
Install Fortisiem Linux Agent in /opt
Checking Connectivity to Server ... 10.20.0.19
Supervisor at 10.20.0.19 is reachable. Continuing with installation...
Agent parameters validated successfully
SUPER_IP:10.20.0.19
CUSTOMER_ID:1
CUSTOMER_NAME:Super
AGENT_REG_USERNAME:agent_user
AGENT_REG_PASSWORD:Fortinet123#
PROXY_SERVER_IP:
PROXY_SERVER_PORT:
SSL_VERIFY_PEER:false
SSL_CA_CERT_FILE:/etc/ssl/certs/ca-certificates.crt
HOST_NAME:webserver
SSL_CA_CERT_PATH:
Adding user `fsmadmin' ...
Adding new group `fsmadmin' (1001) ...
Adding new user `fsmadmin' (1001) with group `fsmadmin' ...
Creating home directory `/home/fsmadmin' ...
Copying files from `/etc/skel' ...
fapolicyd.service is not active - no need to config.
Executing command systemctl start fortisiem-linux-agent.service
Executing command systemctl enable fortisiem-linux-agent.service
Created symlink /etc/systemd/system/multi-user.target.wants/fortisiem-linux-agent.service - /etc/systemd/system/fortisiem-linux-agent.service.
Executing command systemctl daemon-reload
service fortisiem-linux-agent status...
● fortisiem-linux-agent.service - FortiSIEM Linux Agent daemon
   Loaded: loaded (/etc/systemd/system/fortisiem-linux-agent.service; enabled; vendor preset: enabled)
   Active: active (running) since Tue 2026-05-05 02:47:05 EDT; 402ms ago
     Main PID: 3872 (phLinuxAgent)
        Tasks: 3 (limit: 9427)
       Memory: 10.0M
          CPU: 162ms
      CGroup: /system.slice/fortisiem-linux-agent.service
              └─3872 /opt/fortinet/fortisiem/linux-agent/bin/phLinuxAgent
                 └─3947 sh -c "/usr/sbin/service auditd restart"
                   └─3950 systemctl restart auditd.service

May 05 02:47:05 webserver systemd[1]: Started FortiSIEM Linux Agent daemon.
May 05 02:47:06 webserver systemd[1]: /etc/systemd/system/fortisiem-linux-agent.service:13: PIDFile= references a path below legacy directory /var/run/, update:
update the unit file accordingly.
May 05 02:47:06 webserver "fortisiem-linux-agent"[3872]: 2026-05-05T02:47:06.6478-00:00 (null) phLinuxAgent[3872]: [PH_MODULE_LOG_LEVEL_CHANGE]:[eventSeverity]:
, [oldLogLevel]=2047, [newLogLevel]=424, [phLogDetail]=Module received log level change
May 05 02:47:06 webserver "fortisiem-linux-agent"[3920]: /bin/sed: can't read /etc/audit/rules.d/fsm-process.rules: No such file or directory
May 05 02:47:06 webserver "fortisiem-linux-agent"[3937]: /bin/grep: /usr/libexec/initscripts/legacy-actions/auditd/stop: No such file or directory
May 05 02:47:06 webserver systemd[1]: /etc/systemd/system/fortisiem-linux-agent.service:13: PIDFile= references a path below legacy directory /var/run/, update:
update the unit file accordingly.
INSTALLATION SUCCESS
INSTALL PATH:/opt/fortinet/fortisiem/linux-agent
user@webserver:~/Downloads$
```

Figure 5: FSIEM Linux Agent Install

Explore the CMDB

Now that we have installed the FortiSIEM Advanced Agent into the webserver, let's take a look at the properties discovered.

1. Navigate to **CMDB** → **Devices** and click on the *webserver*. A side window with useful information is open, explore the different options.

!!! info FortiSIEM can also discover devices automatically via SNMP, or populating the credentials and ip ranges to scan. This is useful for network devices such as Firewalls, Routers and Switches which can be also backed up into FortiSIEM CMDB.

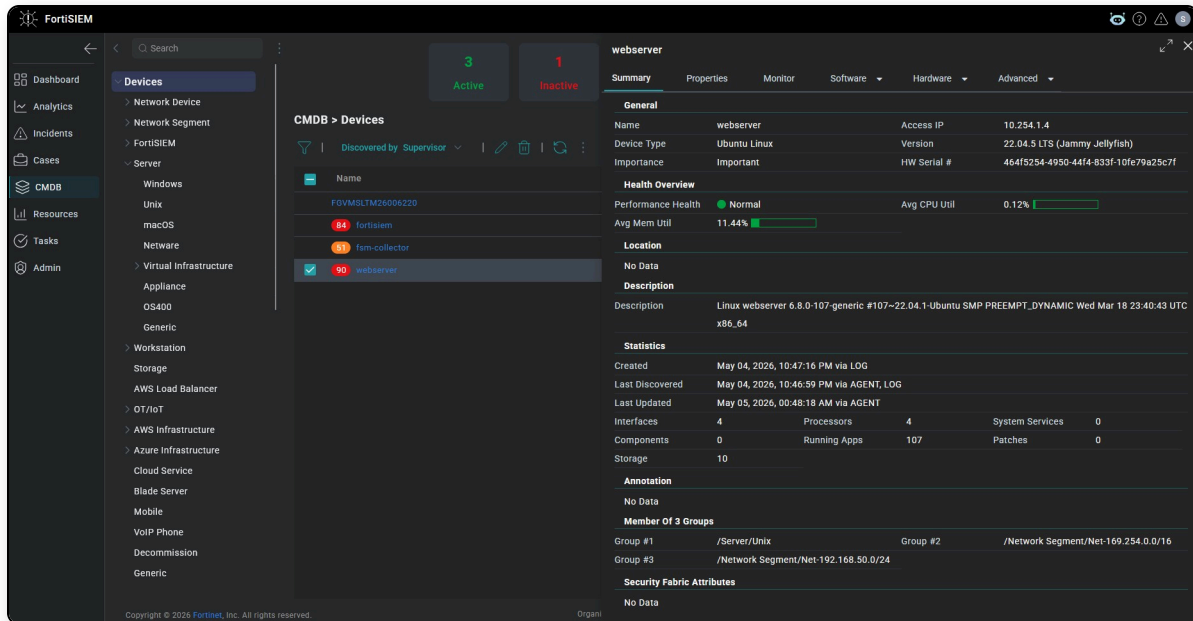


Figure 6: CMDB Devices

For Further info visit: <https://docs.fortinet.com/document/fortisiem/7.5.0/user-guide/635270/viewing-device-information>

Custom Correlation Rule

Correlation Rule Configuration for Webservers and FIM

Considering a webserver to be critical part of most businesses, we will create a correlation rule capable to detect a web file change into a webserver when the remote session comes from a "potentially compromised" source.

1. Into FortiSIEM Supervisor, navigate to **Resources** → **Rules**.
2. Using the search bar, find the rule **Agent FIM: Linux File Content Modified**, select it and *Clone it*
3. Change the name to **Xperts Agent FIM: Linux File Content Modified**
4. Edit the fields accordingly.

Step 1: General

Xperts Agent FIM: Linux File Content Modified - Edit Details

Step 1: General > **Step 2: Define Condition >** **Step 3: Define Action**

Rule Name: Xperts Agent FIM: Linux File Content Modified

Description: Detects that a user modified either the content or the attributes of a file or directory

Data Source: Any Device Agentless FIM via SSH

Detection Technology: Correlation

Event Type: Xperts_Agent_FIM_Linux_File_Content_Modified

Evaluation Mode: Streaming

Remediation Note: Make sure it is an authorized change

Prompt:

Cancel Save

Figure 7: Rule Edition

Step 2: Define Condition

1. Click to edit the existent subpattern **FileChange**, preserve the current configuration, just add a 4th filter:
2. **Attribute:** Source IP
3. **Operator:** IN
4. **Value:** (Click on Select from CMDB) and search for WatchList Policy Violators and move it to the right using the arrows >>

Edit SubPattern

Name: FileChange

Filters:

	Paren	Attribute	Operator	Value	Paren	Next	Row
-	+	Event Type	=	FSM_LINUX_FILE_MODIFY	-	+	AND OR +
-	(	Event Type	=	FSM_LINUX_FILE_DELETE_SEI	-	+	AND OR +
-	+	Target Object Name	=	/etc/passwd	-	)	AND OR +
-	+	Source IP	IN	DyWatchLists: Policy Violators	-	+	AND OR +

Aggregate:

	Paren	Attribute	Operator	Value	Paren	Next	Row
-	+	COUNT(Matched Events)	>=	1	-	+	AND OR +

Group By:

Attribute	Row	Move
Reporting Device	+	-
User	+	-
Target Object Name	+	-
Hash Algorithm	+	-

Run as Query

Save as Report

Cancel

Save

Figure 8: SubPattern FileChange

Step 3: Define Action

1. Verify and change accordingly
2. **Severity:** 10 - HIGH
3. **Catergory:** Change
4. **Subcatergory:** Impact
5. **Technique:** T1565.001, T1070.004, T1491.002, T1491.001
6. **Tactics:** Defense Evation, Impact
7. **Tag:** Notable File Changed
8. **Update Status on Summary Dashboard:** Check
9. **Notification:** 1 Hour
10. **Impacts:** Server

Xperts Agent FIM: Linux File Content Modified - Edit Details

Step 1: General > Step 2: Define Condition > Step 3: Define Action

Severity: 10 - HIGH Update Status on Summary Dashboard: ☒

Category: Change Notification: 1 Hour

Subcategory: Impact Impacts: Server

Technique: 4 Selected

Tactics: Defense Evasion, Impact

Action: Defined

Exception: Undefined

Tag: Notable File Change

Watch List: Undefined

Clear: Undefined

Cancel Save

Figure 9: Step 3 Define Action

1. Click **Save** for the entire Rule.
2. Finally, find the recently created rule and enable it.

Testing

1. From the *compromised* Alpha Windows VM, start a SSH session to Ubuntu-DVWA and try to modify some files.
2. **user:** user
3. **Password:** Fortinet123#
4. Using PowerShell execute the following commands:
5. **Command 1:**

```
echo "owned" | sudo tee /var/www/html/dvwa/probe.txt
```

6. **Command 2:**

```
echo "pwned" | sudo tee /var/www/html/dvwa/probe.txt
```

7. Command 3:

```
echo "<h1 style='color:red;'>HACKED BY XPERTS LAB</h1>" | sudo tee  
/var/www/html/dvwa/login.php
```

8. Command 3:

```
sudo rm /var/www/html/dvwa/probe.txt
```

9. Connect to FortiSIEM GUI and navigate to **Incidents** → **Overview**, explore the new incidents. Adjust the time accordingly.

10. What is the information we can obtain from the incidents created by the rule *Xperts Agent FIM: Linux File Content Modified*?

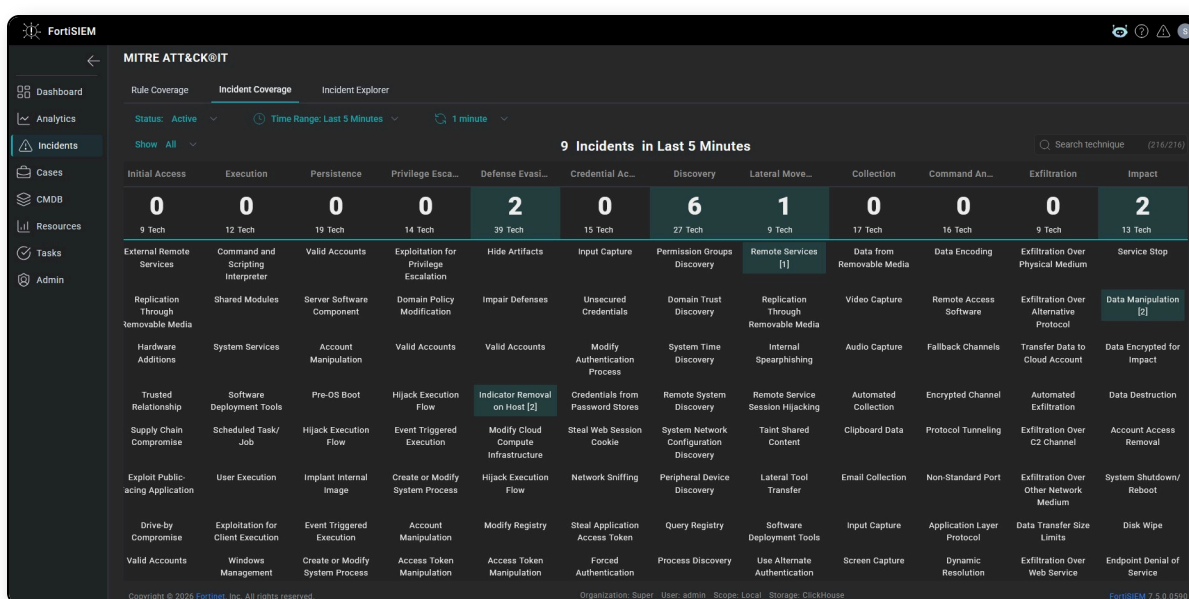


Figure 10: FIM Correlation

1. Finally, connect to the Kali VM, open Firefox and using the bookmark, navigate to the webserver...

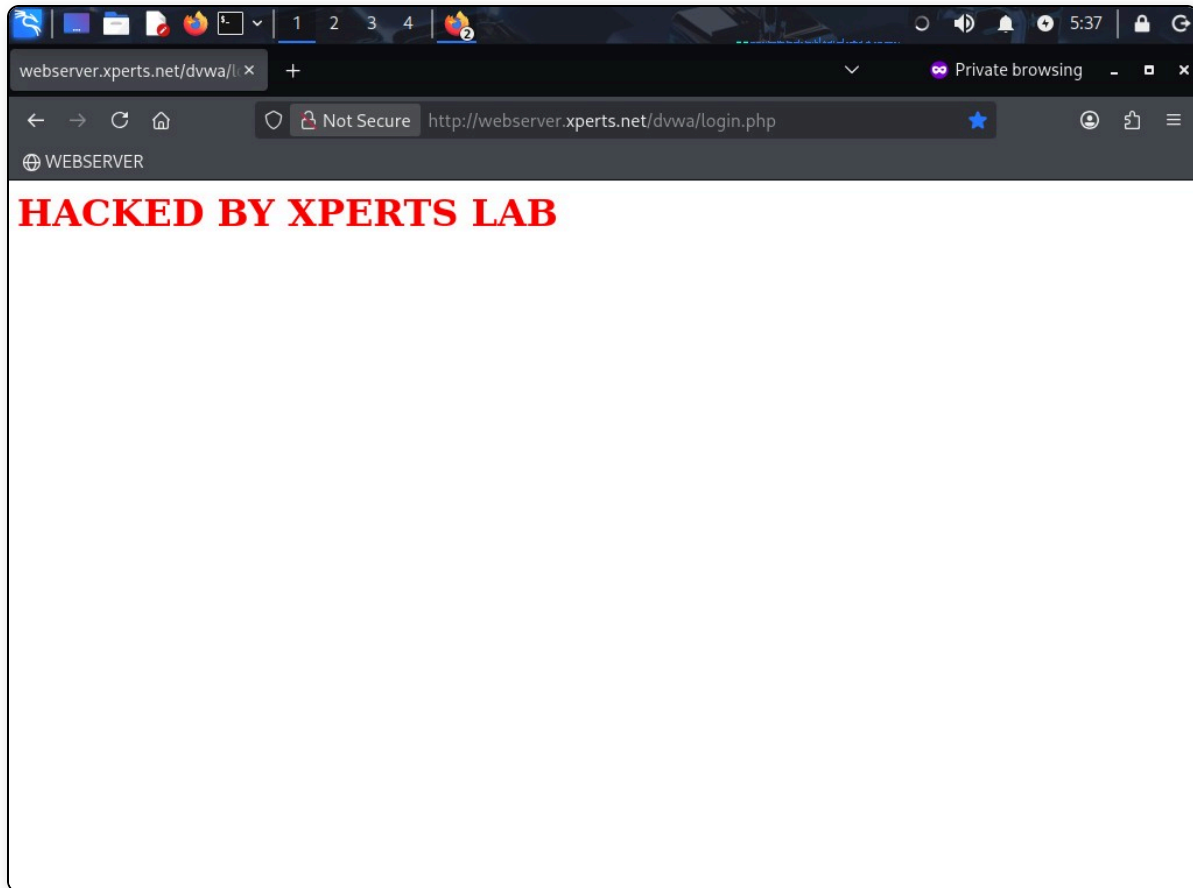


Figure 11: Hacked by Xperts Lab

You made it!!!

As a reminder, these labs were intended to demonstrate behavioral correlation through a continuous attack simulation by linking different Fortinet products by aligning to the MITRE ATT&CK framework.

This is the end of the SecOps Track 2026.