FORTINET
CERTIFIED
SOLUTION
SPECIALIST
Security
Operations

FORTINET
Training Institute

Security Operations Analyst

SOC Threat Hunting

FortiAnalyzer 7.4

Last Modified: 21 January 2025

Lesson Overview

Threat Hunting

Threat Hunting

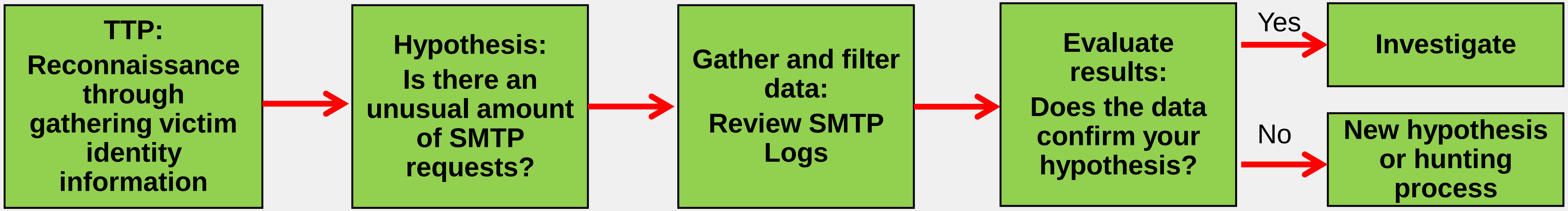
Objectives

- Describe the threat hunting workflow
- Analyze threat hunting dashboards
- Analyze IOC information from compromised hosts
- Manage outbreak alerts

Training Institute

Threat Hunting

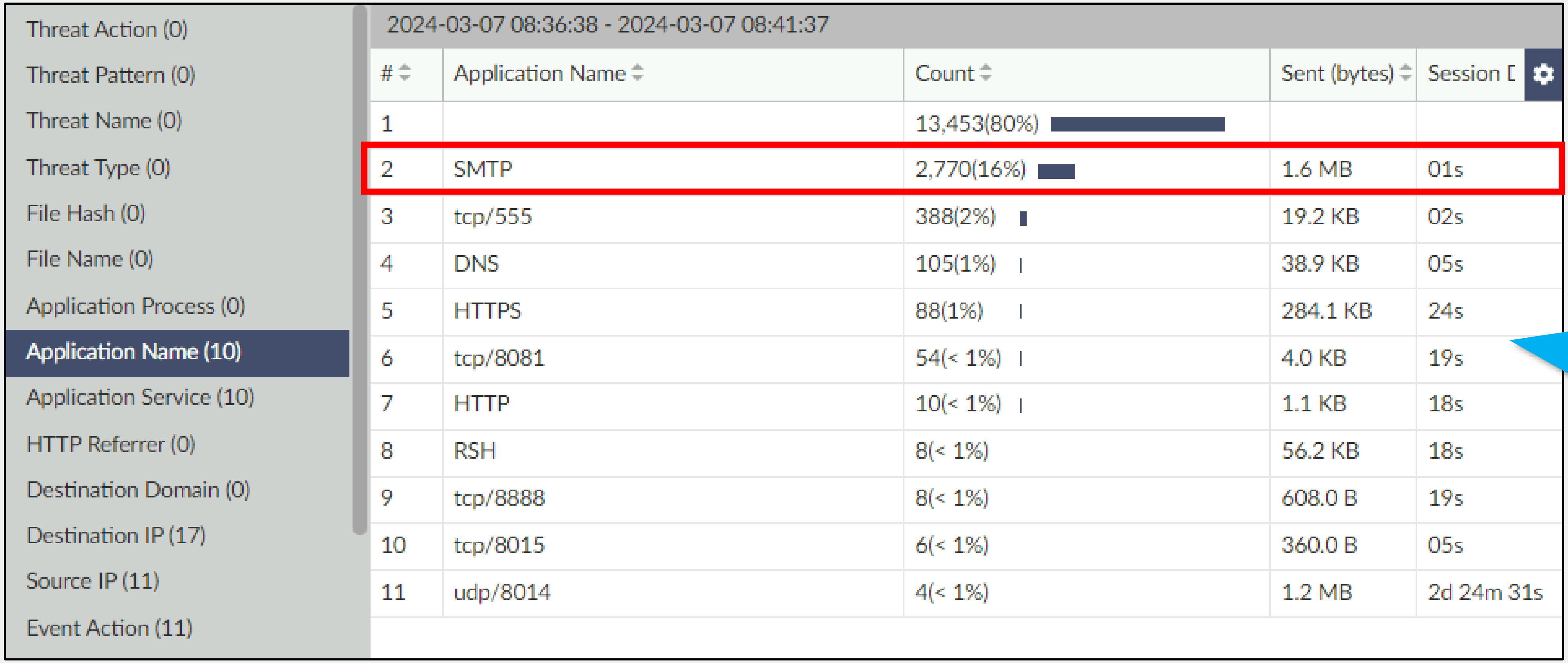
- Proactively search for suspicious or risky network activity that may have gone undetected
- The process usually begins with a question:
  - Are any advanced persistent threats (APTs) currently active in the network?
- The reference to tactics, techniques, and procedures (TTPs), behaviors, and indicators helps to refine your questions further
  - Frequently aligned with the MITRE ATT&CK or the Cyber Kill Chain frameworks
- You can also create an if-then statement, for example:
  - If you suspect reconnaissance activities in the network, then you should see abnormal traffic trends
- A simplified example:


TTP:
Reconnaissance through gathering victim identity information
Hypothesis:
Is there an unusual amount of SMTP requests?
Gather and filter data:
Review SMTP Logs
Evaluate results:
Does the data confirm your hypothesis?
Yes
Investigate
No
New hypothesis or hunting process

Threat Hunting (Contd)

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

Incidents & Events > Threat Hunting



2024-03-07 08:36:38 - 2024-03-07 08:41:37

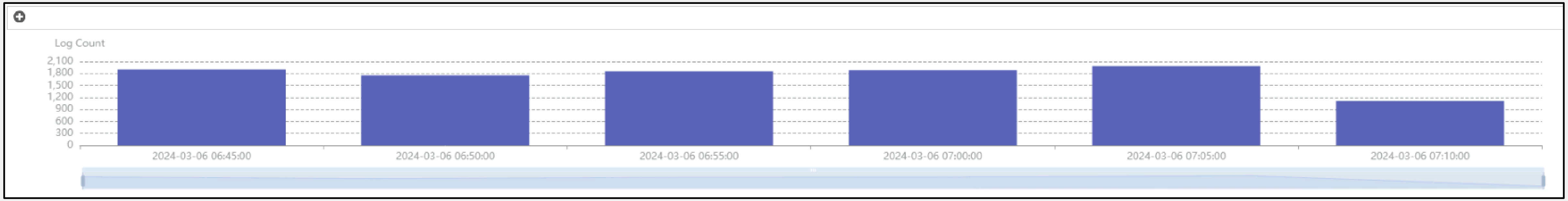
#	Application Name	Count	Sent (bytes)	Session D
1		13,453(80%)		
2	SMTP	2,770(16%)	1.6 MB	01s
3	tcp/555	388(2%)	19.2 KB	02s
4	DNS	105(1%)	38.9 KB	05s
5	HTTPS	88(1%)	284.1 KB	24s
6	tcp/8081	54(< 1%)	4.0 KB	19s
7	HTTP	10(< 1%)	1.1 KB	18s
8	RSH	8(< 1%)	56.2 KB	18s
9	tcp/8888	8(< 1%)	608.0 B	19s
10	tcp/8015	6(< 1%)	360.0 B	05s
11	udp/8014	4(< 1%)	1.2 MB	2d 24m 31s

SOC analytics dashboard using the SIEM database

Log Count Chart

- Use the **Log Count** chart to focus on the logs you must analyze based on a time range
- The details in the SIEM log table auto adjusts to the timeframe you select in this chart

Incidents & Events > Threat Hunting

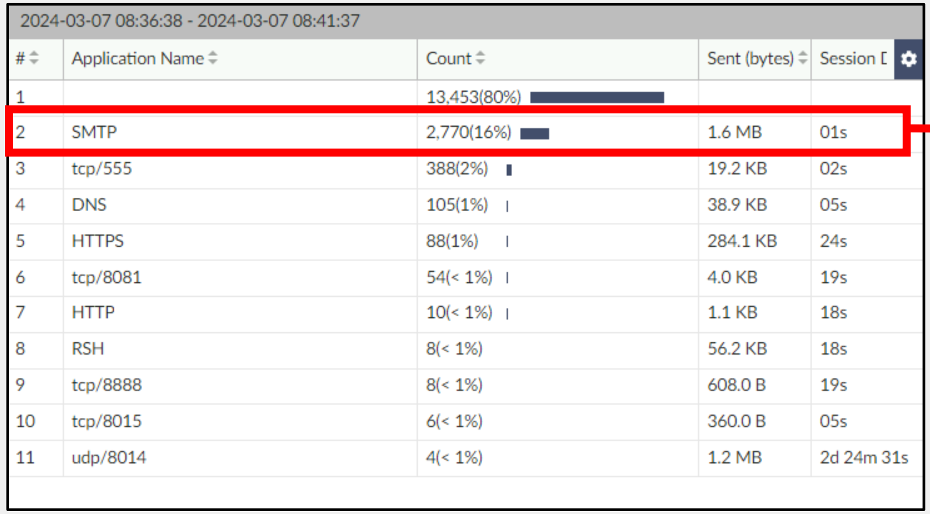


Adjust the time bar to include only the desired time frame

Threat Hunting Example With FortiAnalyzer

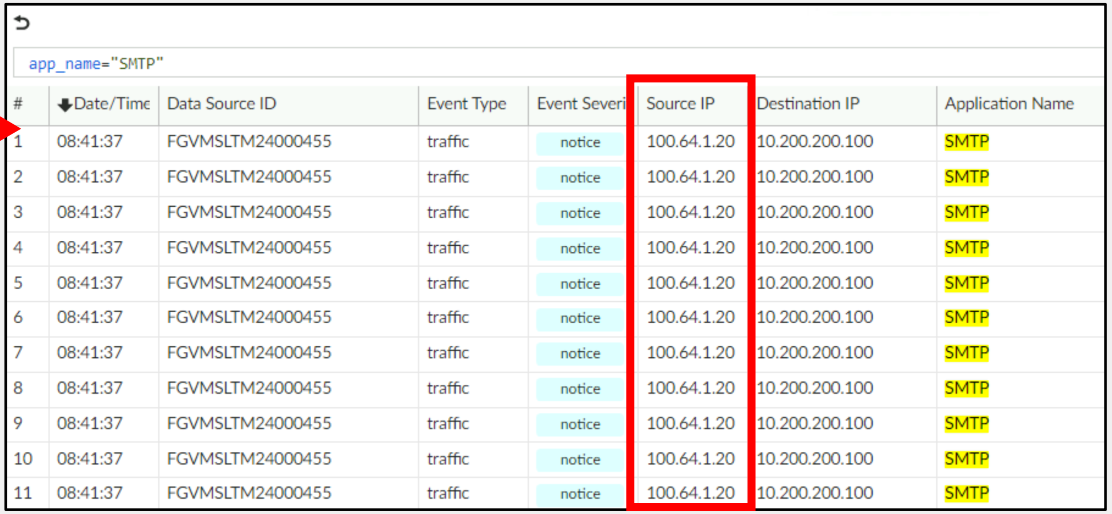
- *Has reconnaissance been used to gather victim identity information from the mail server?*
- In this example, the analyst uses the log chart to discover an unusual number of SMTP requests
- Analysis shows that the IP address `100.64.1.20` is generating lots of queries within a short time period

Incidents & Events > Threat Hunting



2024-03-07 08:36:38 - 2024-03-07 08:41:37

#	Application Name	Count	Sent (bytes)	Session [
1		13,453(80%)		
2	SMTP	2,770(16%)	1.6 MB	01s
3	tcp/555	388(2%)	19.2 KB	02s
4	DNS	105(1%)	38.9 KB	05s
5	HTTPS	88(1%)	284.1 KB	24s
6	tcp/8081	54(< 1%)	4.0 KB	19s
7	HTTP	10(< 1%)	1.1 KB	18s
8	RSH	8(< 1%)	56.2 KB	18s
9	tcp/8888	8(< 1%)	608.0 B	19s
10	tcp/8015	6(< 1%)	360.0 B	05s
11	udp/8014	4(< 1%)	1.2 MB	2d 24m 31s



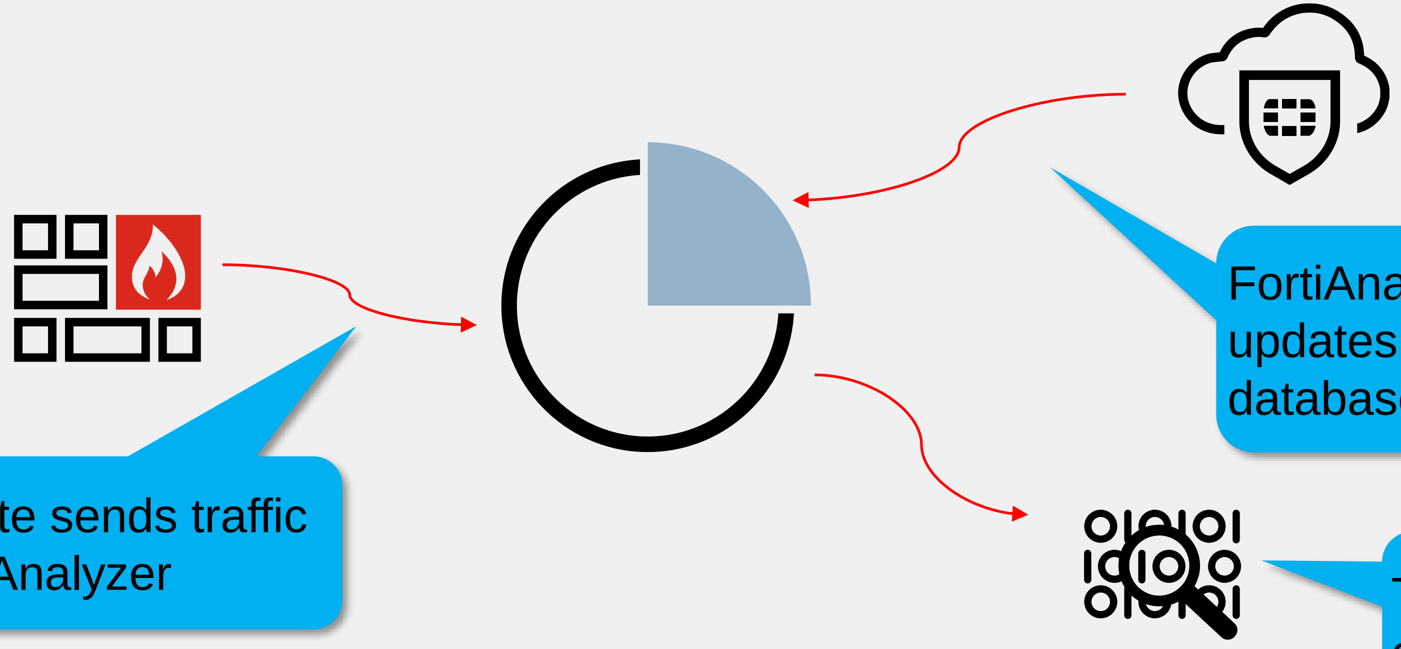
```
app_name="SMTP"
```

#	Date/Time	Data Source ID	Event Type	Event Severi	Source IP	Destination IP	Application Name
1	08:41:37	FGVMSLTM24000455	traffic	notice	100.64.1.20	10.200.200.100	SMTP
2	08:41:37	FGVMSLTM24000455	traffic	notice	100.64.1.20	10.200.200.100	SMTP
3	08:41:37	FGVMSLTM24000455	traffic	notice	100.64.1.20	10.200.200.100	SMTP
4	08:41:37	FGVMSLTM24000455	traffic	notice	100.64.1.20	10.200.200.100	SMTP
5	08:41:37	FGVMSLTM24000455	traffic	notice	100.64.1.20	10.200.200.100	SMTP
6	08:41:37	FGVMSLTM24000455	traffic	notice	100.64.1.20	10.200.200.100	SMTP
7	08:41:37	FGVMSLTM24000455	traffic	notice	100.64.1.20	10.200.200.100	SMTP
8	08:41:37	FGVMSLTM24000455	traffic	notice	100.64.1.20	10.200.200.100	SMTP
9	08:41:37	FGVMSLTM24000455	traffic	notice	100.64.1.20	10.200.200.100	SMTP
10	08:41:37	FGVMSLTM24000455	traffic	notice	100.64.1.20	10.200.200.100	SMTP
11	08:41:37	FGVMSLTM24000455	traffic	notice	100.64.1.20	10.200.200.100	SMTP

- Further investigation determines that the queries are an external attacker gathering victim identity information
- A new incident is created, and the SOC responders can start containment and eradication steps

IOC (Compromised Hosts)

- The IOC engine detects end users with suspicious web usage compromises by checking new and historical logs against IOC signatures
- Uses FortiGuard threat intelligence to provide visibility of emerging threats
- Requires a FortiGuard subscription



FortiGate sends traffic to FortiAnalyzer

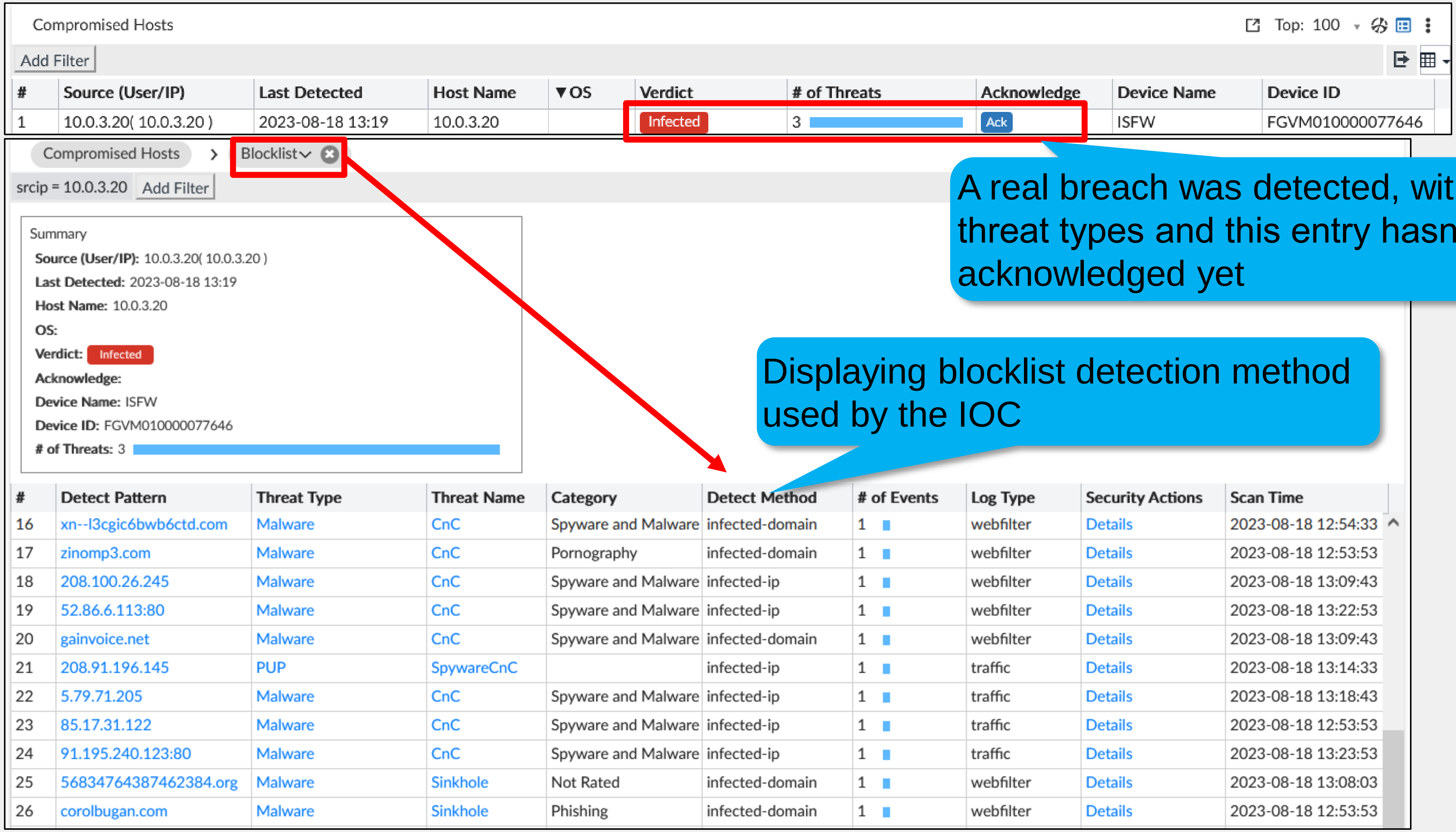
FortiAnalyzer receives updates to its threat database from FortiGuard

The breach detection engine analyzes logs

FORTINET
Training Institute

Compromised Host IOC Example

FortiView > Threat & Events



#	Source (User/IP)	Last Detected	Host Name	▼OS	Verdict	# of Threats	Acknowledge	Device Name	Device ID
1	10.0.3.20(10.0.3.20)	2023-08-18 13:19	10.0.3.20		Infected	3	Ack	ISFW	FGVM010000077646

Summary

Source (User/IP): 10.0.3.20(10.0.3.20)
Last Detected: 2023-08-18 13:19
Host Name: 10.0.3.20
OS:
Verdict: Infected
Acknowledge:
Device Name: ISFW
Device ID: FGVM010000077646
# of Threats: 3

#	Detect Pattern	Threat Type	Threat Name	Category	Detect Method	# of Events	Log Type	Security Actions	Scan Time
16	xn--l3cgic6bwb6ctd.com	Malware	CnC	Spyware and Malware	infected-domain	1	webfilter	Details	2023-08-18 12:54:33
17	zinomp3.com	Malware	CnC	Pornography	infected-domain	1	webfilter	Details	2023-08-18 12:53:53
18	208.100.26.245	Malware	CnC	Spyware and Malware	infected-ip	1	webfilter	Details	2023-08-18 13:09:43
19	52.86.6.113:80	Malware	CnC	Spyware and Malware	infected-ip	1	webfilter	Details	2023-08-18 13:22:53
20	gainvoice.net	Malware	CnC	Spyware and Malware	infected-domain	1	webfilter	Details	2023-08-18 13:09:43
21	208.91.196.145	PUP	SpywareCnC		infected-ip	1	traffic	Details	2023-08-18 13:14:33
22	5.79.71.205	Malware	CnC	Spyware and Malware	infected-ip	1	traffic	Details	2023-08-18 13:18:43
23	85.17.31.122	Malware	CnC	Spyware and Malware	infected-ip	1	traffic	Details	2023-08-18 12:53:53
24	91.195.240.123:80	Malware	CnC	Spyware and Malware	infected-ip	1	traffic	Details	2023-08-18 13:23:53
25	56834764387462384.org	Malware	Sinkhole	Not Rated	infected-domain	1	webfilter	Details	2023-08-18 13:08:03
26	corolbugan.com	Malware	Sinkhole	Phishing	infected-domain	1	webfilter	Details	2023-08-18 12:53:53

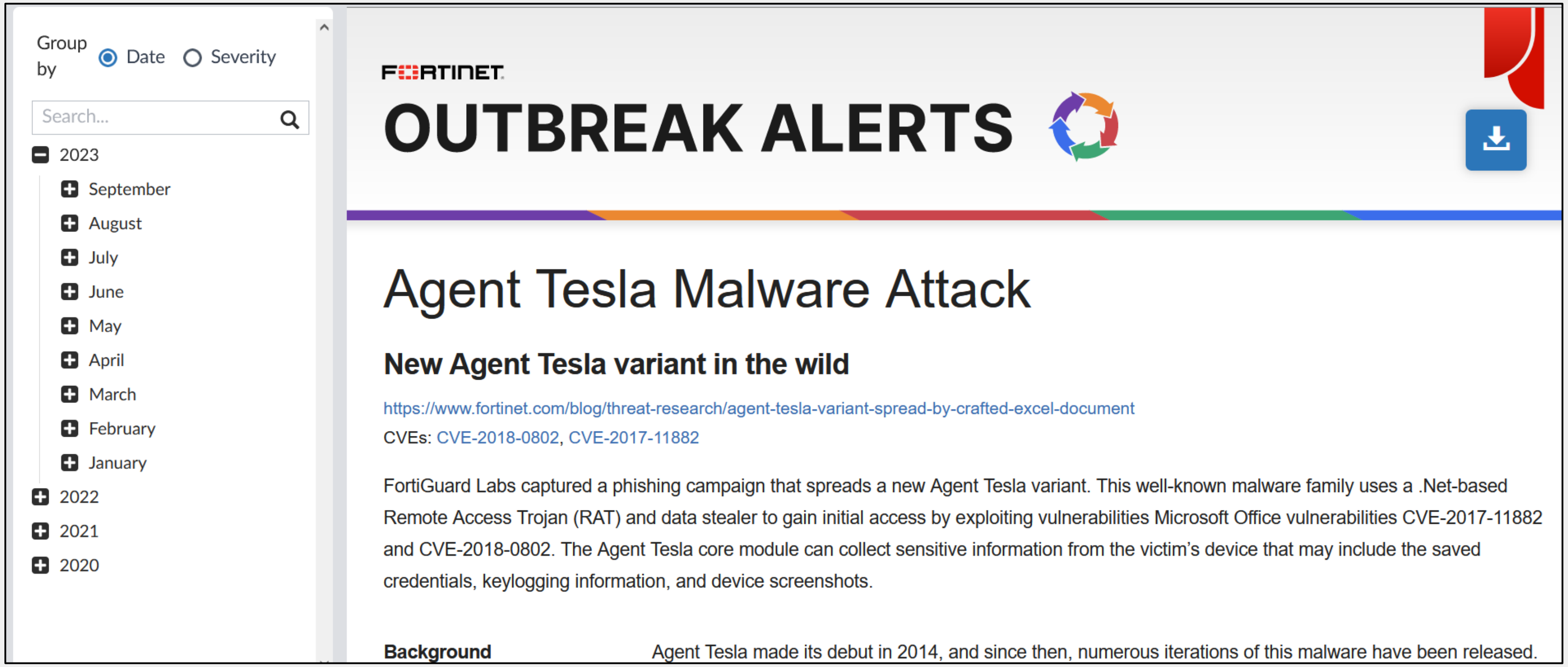
A real breach was detected, with three threat types and this entry hasn’t been acknowledged yet

Displaying blocklist detection method used by the IOC

Outbreak Detection Service Overview

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

Incidents & Events > Outbreak Alerts



Agent Tesla Malware Attack

New Agent Tesla variant in the wild

https://www.fortinet.com/blog/threat-research/agent-tesla-variant-spread-by-crafted-excel-document

CVEs: CVE-2018-0802, CVE-2017-11882

FortiGuard Labs captured a phishing campaign that spreads a new Agent Tesla variant. This well-known malware family uses a .Net-based Remote Access Trojan (RAT) and data stealer to gain initial access by exploiting vulnerabilities Microsoft Office vulnerabilities CVE-2017-11882 and CVE-2018-0802. The Agent Tesla core module can collect sensitive information from the victim's device that may include the saved credentials, keylogging information, and device screenshots.

Background Agent Tesla made its debut in 2014, and since then, numerous iterations of this malware have been released.

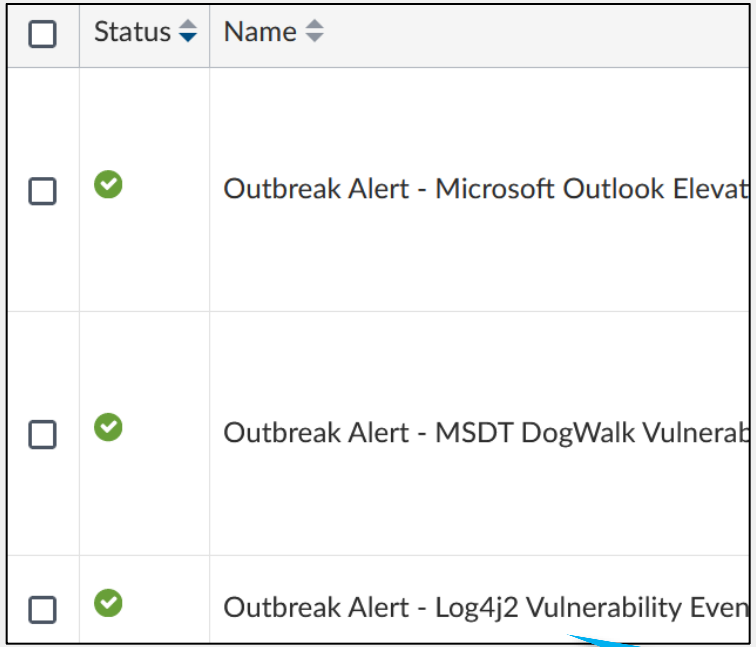
FORTINET Training Institute

Outbreak Alert Handlers and Reports

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

- The same is true for the newly downloaded reports

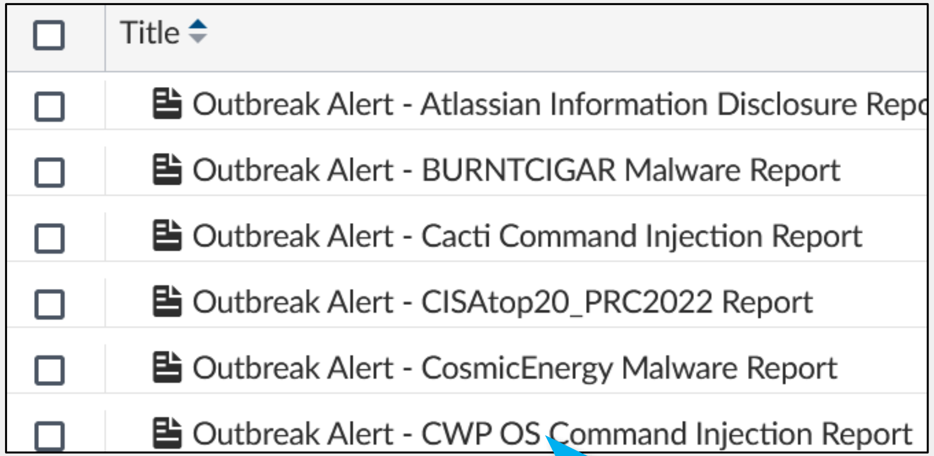
Incidents & Events > Handlers



□	Status	Name
□	✓	Outbreak Alert - Microsoft Outlook Elevat
□	✓	Outbreak Alert - MSDT DogWalk Vulnerab
□	✓	Outbreak Alert - Log4j2 Vulnerability Even

Event handlers downloaded through the outbreak alerts service

Reports > Report Definitions



□	Title
□	Outbreak Alert - Atlassian Information Disclosure Repo
□	Outbreak Alert - BURNTCIGAR Malware Report
□	Outbreak Alert - Cacti Command Injection Report
□	Outbreak Alert - CISAtop20_PRC2022 Report
□	Outbreak Alert - CosmicEnergy Malware Report
□	Outbreak Alert - CWP OS Command Injection Report

Reports downloaded through the outbreak alerts service

Knowledge Check

1. The IOC engine analyzes new and historical logs against IOC signatures for which type of hosts?

✓ A. End users

B. Fabric devices

2. The threat hunting dashboard uses which database?

✓ A. SIEM

B. TIDB

Lesson Overview

✓ Threat Hunting

Review

- ✓ Describe the threat hunting workflow
- ✓ Analyze threat hunting dashboards
- ✓ Analyze IOC information from compromised hosts
- ✓ Manage outbreak alerts