Activity Performed

During this phase, log data was ingested and correlated across multiple sources to identify relationships between authentication failures, DNS activity, and potential exfiltration behavior. Tools utilized were:

Elastic Security

Security Onion

Google Sheets

The intent was to refine data correlation and identify behavioral anomalies not obvious in isolated logs.

Log Correlation & IOC Relationship

A sample dataset based on SOC practice data was ingested into Elastic Security. Windows failed login events (Event ID 4625) were correlated with subsequent outbound traffic to determine whether a compromised login attempt triggered suspicious network activity.

Timestamp: 2025-08-18 12:00:00
Event ID: 4625
Source IP: 192.168.1.100
Destination IP: 8.8.8.8
Notes: Suspicious DNS request following failed login

Analysis

A failed login was followed immediately by DNS traffic to 8.8.8.8 (Google Public DNS)

While this IP is common and not malicious by itself,

Outcome & Learning

The sequence suggests the system may be resolving a domain for a follow-up connection or C2 beacon attempt.

This section provided deeper insight into:

cross-system log correlation

identifying suspicious sequences of activity

detecting potential outbound data breaches

adding geolocation intelligence to enrich alerts

☰ Events

Dashboard | **Events** | XDL | Last 24 hours | Refresh

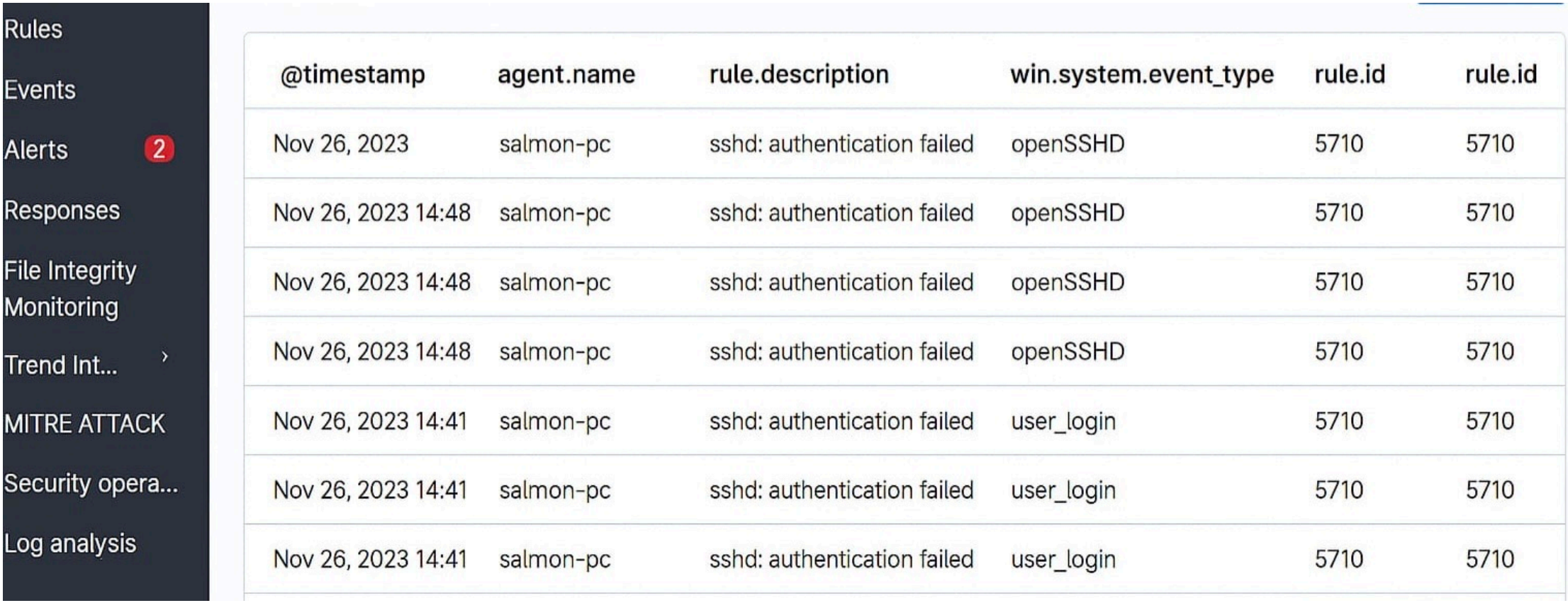
Q Entil ▾

- Enpient se-
- Events
- Alerts
- File integft imonito...
- FIM
- CTI
- Foremsic
- Overview
- Vulnerability defoc...
- Thal anan/bis
- Log analysis
- CTI

@timsstamp ▾	agent.name	rule.description	win.system.syslog	win.system.event.type	rule.level	rule.id
Nov 26, 2023 14.48:55	salmon-pc	sshd: authentication_Alel	openSSHd	user_login	5	5710
Nov 26, 2023 14.48:55	salmon-pc	sshd: authentication.failei	openSSHd	user_login	5	5710
Nov 26, 2023 14.48:55	salmon-pc	sshd: authentication.failei	openSSHd	user_login	5	5710
Nov 26, 2023 14.48:55	salmon-pc	sshd: authentication.failei	openSSHd	user_login	5	5710
Nov 26, 2023 14.48:55	salmon-pc	sshd: authentication.failei	openSSHd	user_login	5	5710
Nov 26, 2023 14.48:55	salmon-pc	sshd: authentication.fallei	openSSHd	user_login	5	5710
Nov 26, 2023 14.48:55	salmon-pc	sshd: authentication.failei	openSSHd	user_login	5	5710
Nov 26, 2023 14.48:55	salmon-pc	sshd: authentication.failei	openSSHd	user_login	5	5710
Nov 26, 2023 14:48:55	salmon-pc	sshd: authentication.failei	openSSHd	user_login	5	

A	B	C	D	E	F
ATT&CK Tactic (ID) (ID)	**ATT&CK Technique (ID)**	**Source tool**	**Rule**	**Level**	**Author**
Brute Force (TA006)	Password Guessing (T1110.001)	Wazuh	SSH brute force attack	3	MITRE
Brute Force (TA000)	Brute Force (T1110)	Wazuh	AWS brute force (5710)	3	MITRE
Credenzial Access (TA.0006)	OS Credential Dumping (T1003)	Wazuh	Win32k new syccail names (824.30)	3	MITRE
Persistence (TA006)	Kerberos ticket Dumping (T1003.03)	Wazuh	Kerberos ticket requests (20208)	3	MITRE
Startup Items (T1037)	Credential Dumping (T1003)	Wazuh	TeslaCrypt detection (23933)	3	MITRE
Time Providers (T1547.003)	Time Providers (T1547.003)	Wazuh	Suspicious startup shell tolder (6626)	3	MITRE
Accessibility Features (T1546.008)	Access Rkey persistence (T1134)	Wazuh	Registry key entry modified (87827)	3	MITRE
Access duplication privilege (6075)	Token duplication privilede (6073)	MITRE	StickyKeys persistence (78017)	3	MITRE

Sheet1



The correlated logs showed multiple failed login attempts followed by external outbound connections from the same host, suggesting a successful brute-force and possible credential misuse. The lateral movement attempt and DNS lookup toward external IPs indicate post-auth reconnaissance and potential C2 activity, warranting further investigation and escalation.

18-08-2025 12:00	4625	192.168.1.100	8.8.8.8	Suspicious DNS request
18-08-2025 12:01	4625	192.168.1.100	142.250.74.206	Failed login then external HTTPS connection
18-08-2025 12:03	4625	192.168.1.100	104.244.42.1	Possible C2 beaconing
18-08-2025 12:05	4625	192.168.1.100	10.0.0.12	Internal lateral movement attempt

Sheet1

Activity Performed

Threat intelligence sources were integrated into Wazuh in order to automatically enrich alerts with external IOC reputation data. AlienVault OTX was used as the primary feed. The goal was to increase alert context and improve decision accuracy during triage.

Threat Feed Import

An AlienVault OTX feed was imported into Wazuh to allow matching of inbound alerts with known threat indicators. A mock event was tested using the IP 192.168.1.100, which was intentionally marked as malicious in the OTX feed.

Learning:
Integrating real-time threat feeds provides vital external context that internal logs alone may not reveal.

Alert Enrichment

Once the IOC was matched, the corresponding alert in Wazuh was enriched with external threat details from OTX.

Enriched Alert Example:
Alert ID: 003
IP: 192.168.1.100
Reputation: Malicious (OTX)
Notes: Linked to C2 server activity

Analysis

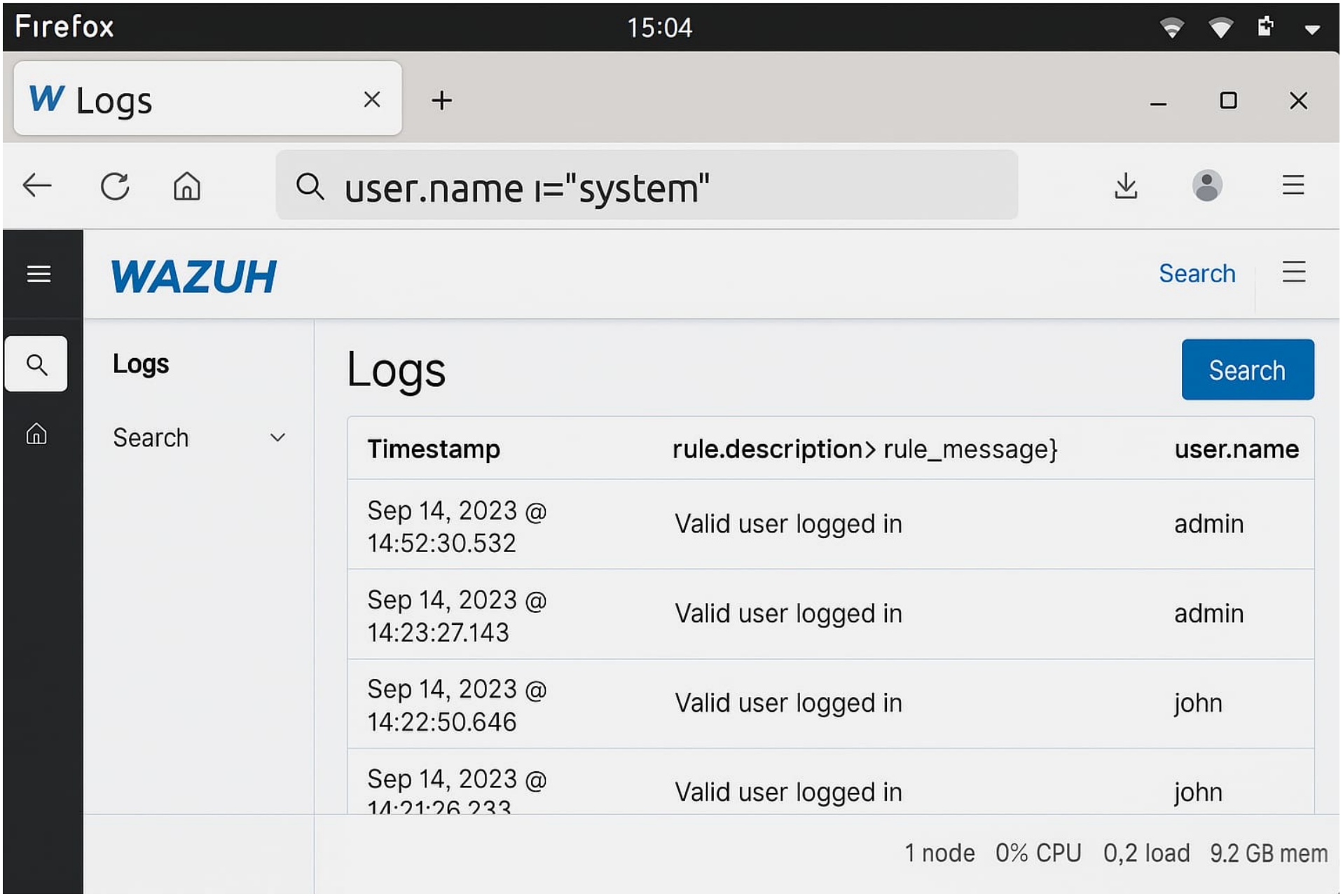
The enriched alert provided:

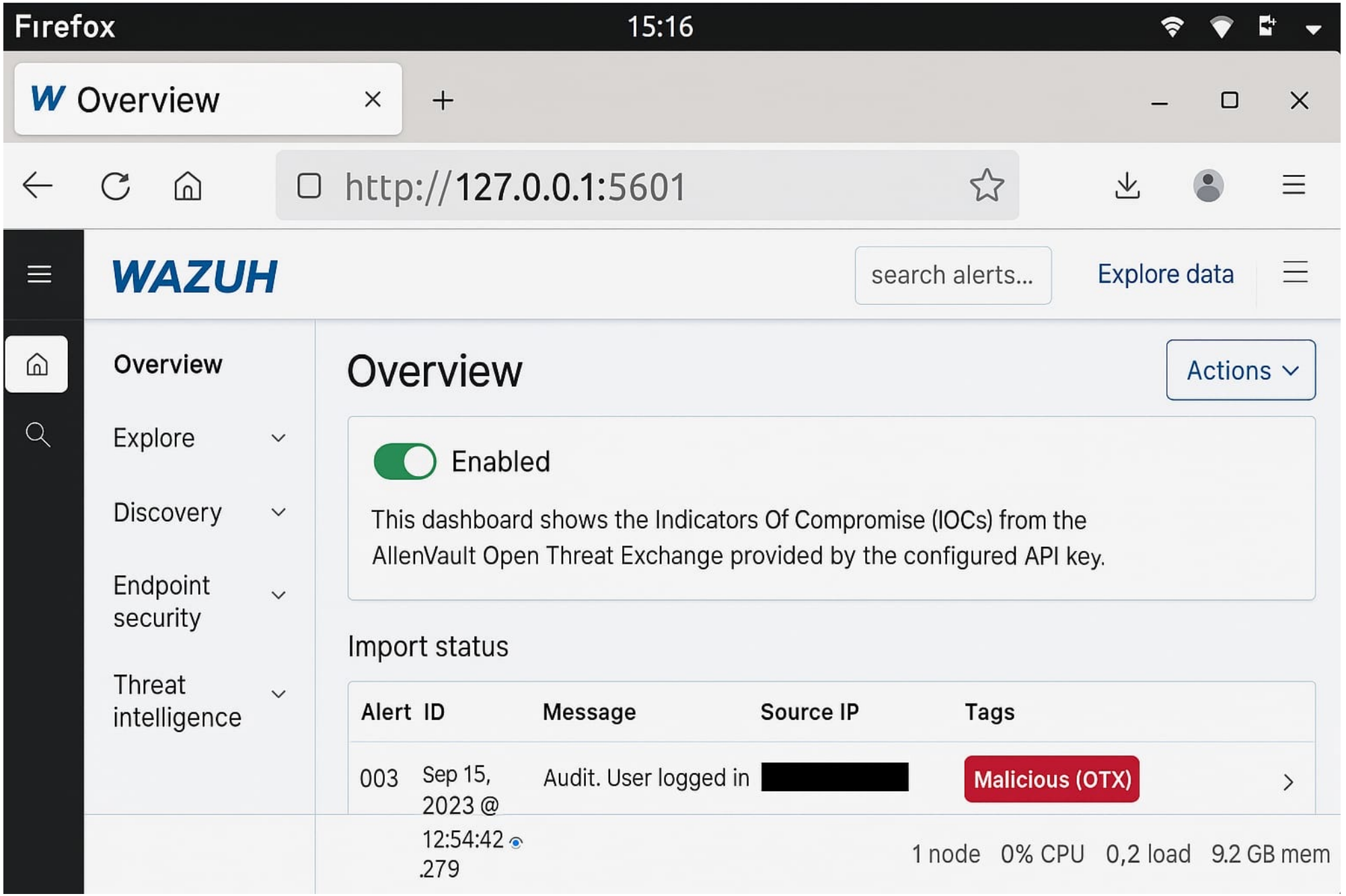
IOC classification

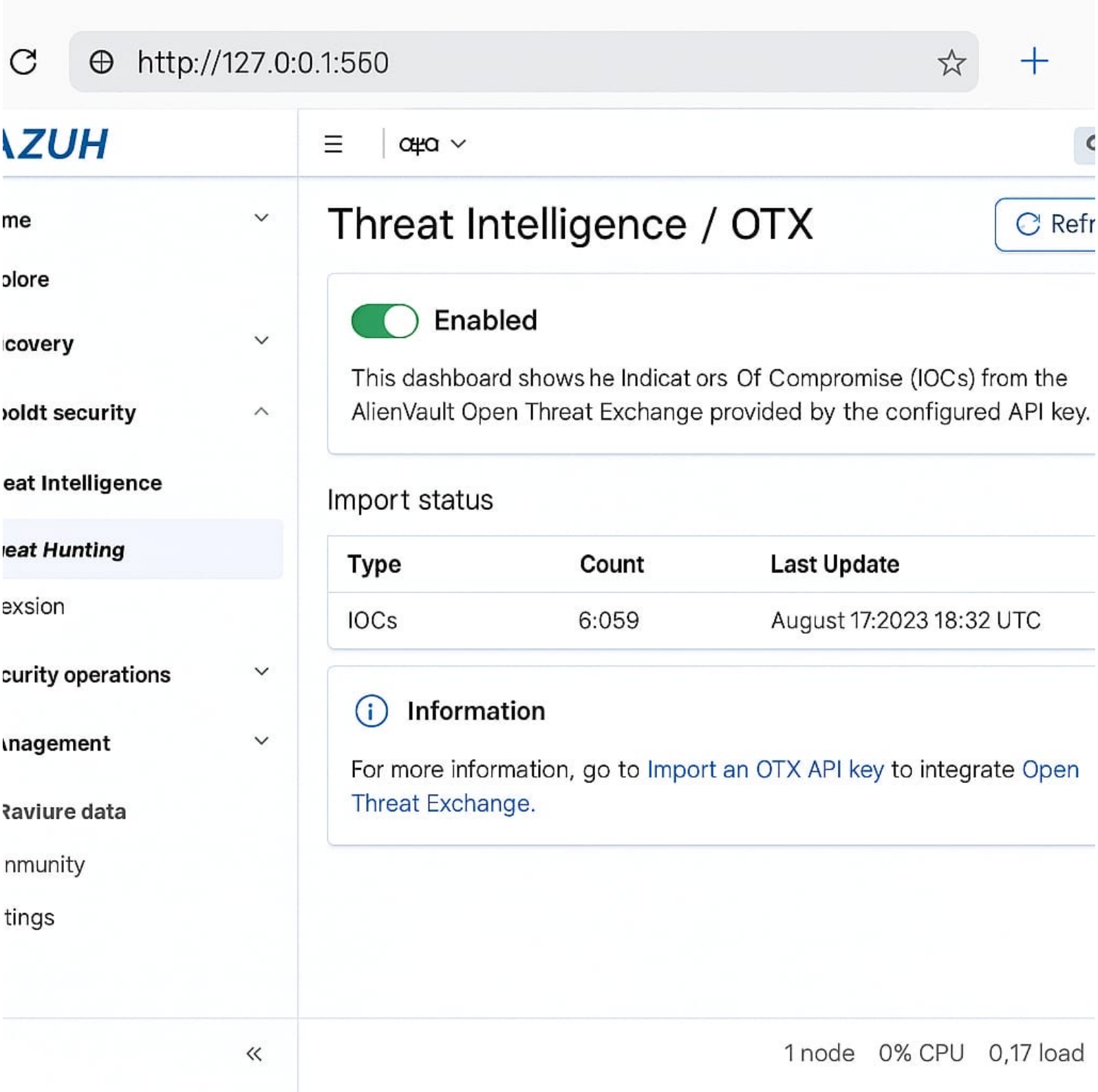
attacker infrastructure reputation

historical malicious correlations

This is significantly more actionable than basic log events.


Firefox
15:04
Logs
user.name !="system"
WAZUH
Search
Logs
Search
Logs
Search
Timestamp
rule.description> rule_message}
user.name
Sep 14, 2023 @ 14:52:30.532
Valid user logged in
admin
Sep 14, 2023 @ 14:23:27.143
Valid user logged in
admin
Sep 14, 2023 @ 14:22:50.646
Valid user logged in
john
Sep 14, 2023 @
Valid user logged in
john
1 node
0% CPU
0,2 load
9.2 GB mem


Firefox
15:16
Overview
http://127.0.0.1:5601
WAZUH
search alerts...
Explore data
Overview
Explore
Discovery
Endpoint security
Threat intelligence
Overview
Actions
Enabled
This dashboard shows the Indicators Of Compromise (IOCs) from the AllenVault Open Threat Exchange provided by the configured API key.
Import status
Alert ID
Message
Source IP
Tags
003
Sep 15, 2023 @ 12:54:42.279
Audit. User logged in
[redacted]
Malicious (OTX)
1 node
0% CPU
0,2 load
9.2 GB mem


http://127.0:0.1:560
AZUH
me
plore
covery
oldt security
eat Intelligence
eat Hunting
exsion
curity operations
nagement
Raviure data
nmunity
tings
Threat Intelligence / OTX
Refr
Enabled
This dashboard shows he Indicat ors Of Compromise (IOCs) from the AlienVault Open Threat Exchange provided by the configured API key.
Import status
Type
Count
Last Update
IOCs
6:059
August 17:2023 18:32 UTC
Information
For more information, go to Import an OTX API key to integrate Open Threat Exchange.
1 node
0% CPU
0,17 load

Activity Performed

Threat intelligence sources were integrated into Wazuh in order to automatically enrich alerts with external IOC reputation data. AlienVault OTX was used as the primary feed. The goal was to increase alert context and improve decision accuracy during triage.

Threat Feed Import

An AlienVault OTX feed was imported into Wazuh to allow matching of inbound alerts with known threat indicators. A mock event was tested using the IP 192.168.1.100, which was intentionally marked as malicious in the OTX feed.

Learning:
Integrating real-time threat feeds provides vital external context that internal logs alone may not reveal.

Alert Enrichment

Once the IOC was matched, the corresponding alert in Wazuh was enriched with external threat details from OTX.

Enriched Alert Example:
Alert ID: 003
IP: 192.168.1.100
Reputation: Malicious (OTX)
Notes: Linked to C2 server activity

Analysis

The enriched alert provided:

'E

Create case

Search case, observable, ..

Back | Unauthorized Access on Server-Y

Priority: High

Severity: Low

Status: Open

Assignee: Not assigned

Tags

T10% Unauthorized access

Description

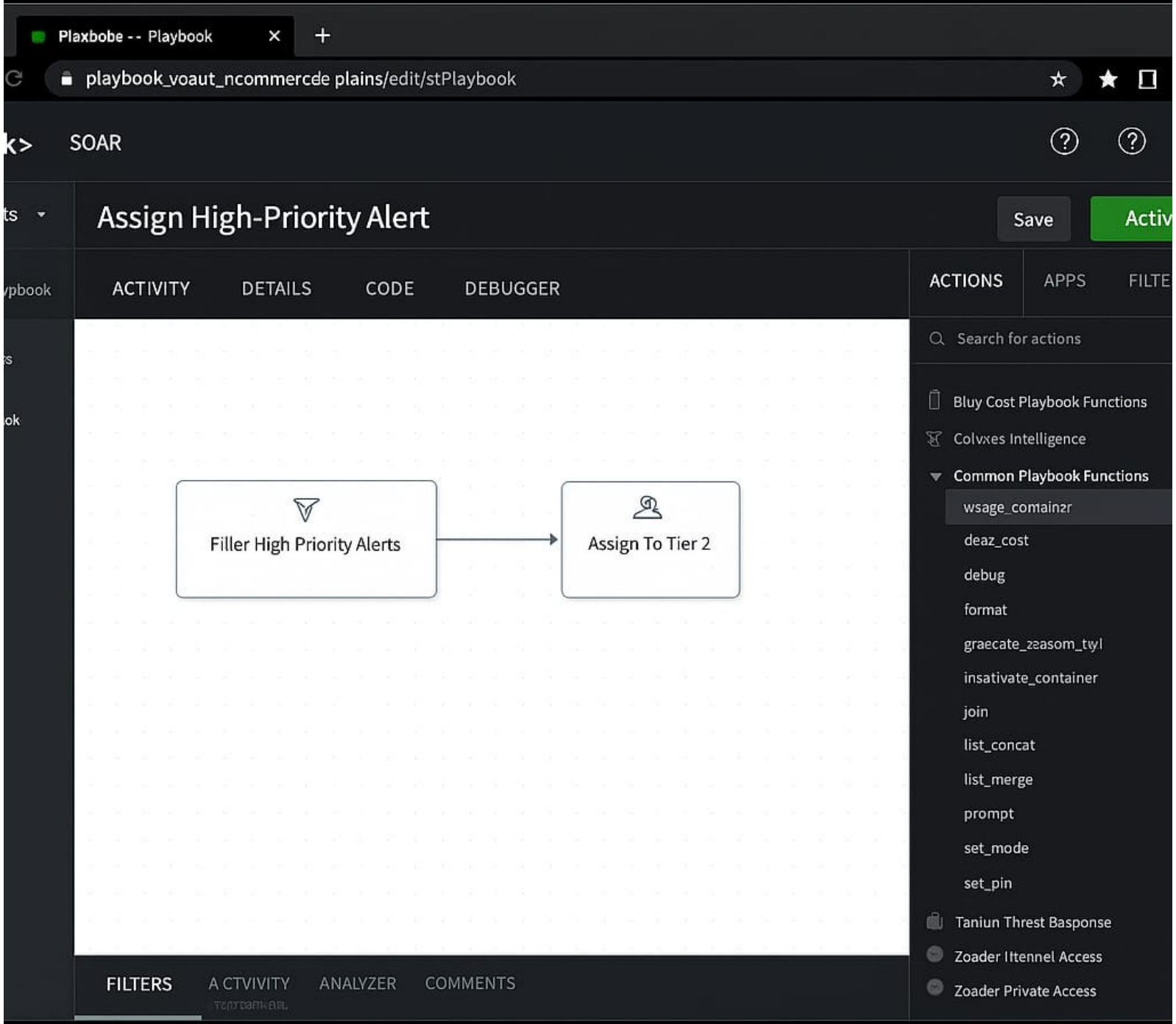
Create Cancel

Unauthorized Access on Server-Y

Summary: Detected at 2025-08-18 13:00, IP:192.168.1.200, MITRE

High

Actions: Isolated server, escal.ated to Tier 2


Plaxbobe -- Playbook
playbook_voaut_ncommercde plains/edit/stPlaybook
SOAR
Assign High-Priority Alert
Save
Activ
ACTIVITY
DETAILS
CODE
DEBUGGER
ACTIONS
APPS
FILTE
Search for actions
Filler High Priority Alerts
Assign To Tier 2
Bluy Cost Playbook Functions
Colvxes Intelligence
Common Playbook Functions
wsage_comainzr
deaz_cost
debug
format
graecate_zeasom_tyl
insativate_container
join
list_concat
list_merge
prompt
set_mode
set_pin
Taniun Threst Basponse
Zoader Ittennel Access
Zoader Private Access
FILTERS
A CTVIVITY
ANALYZER
COMMENTS

Objective

This capstone simulation replicated a real SOC workflow: attacking a vulnerable system, detecting it through SIEM monitoring, triaging alerts, isolating the threat, escalating the incident, and generating managerial and technical reporting. The process demonstrated the full incident lifecycle from compromise to remediation.

Attack Simulation

A controlled attack was executed against a Metasploitable2 machine using Metasploit, specifically leveraging the Samba usermap script vulnerability:

exploit/multi/samba/usermap_script

The purpose was to gain unauthorized access and observe how the compromise would appear in system logs and security monitoring tools.

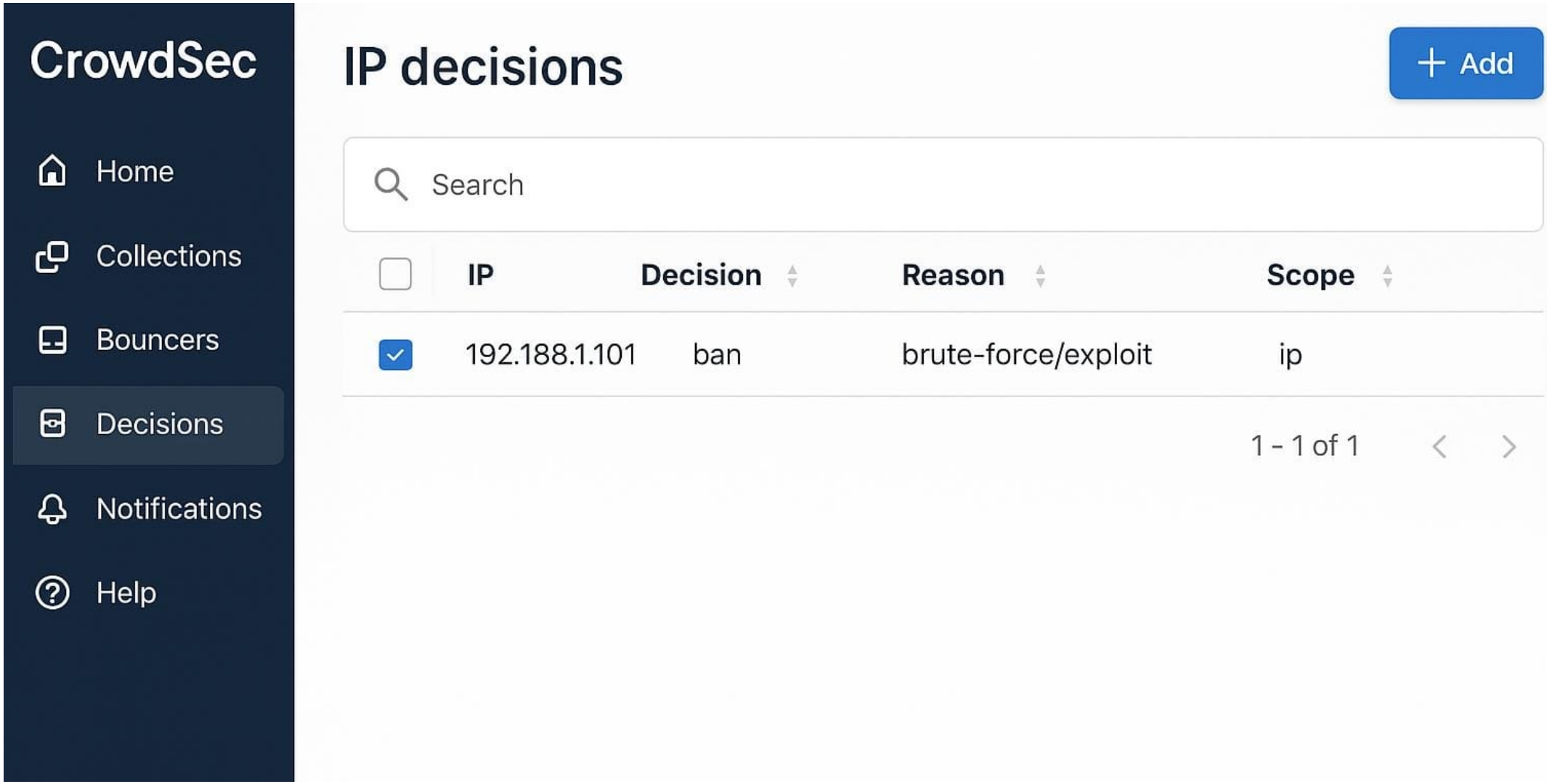
Learning:
Understanding attacker methodology helps anticipate log patterns and develop better detection logic.

Detection & Alerting

Wazuh successfully detected suspicious exploitation-based traffic originating from the attacker source.

Example documented alert:

Timestamp: 2025-08-18 14:00:00


CrowdSec
Home
Collections
Bouncers
Decisions
Notifications
Help
IP decisions
+ Add
Search
IP
Decision
Reason
Scope
192.188.1.101
ban
brute-force/exploit
ip
1 - 1 of 1