Advanced SOC Operations

Name: Shah Devam

Email: shahdevam48@gmail.com

---

1. Theoretical Knowledge

1.1 Advanced Log Analysis

Core Concepts

Log Correlation

Log correlation involves combining and analyzing logs from multiple sources—such as firewalls, endpoints, and application logs—to identify attack patterns that may not be visible in isolation.
Example: Correlating repeated failed login attempts (Windows Event ID 4625) with suspicious outbound network traffic to detect potential credential misuse or data exfiltration.

Anomaly Detection

Anomaly detection focuses on identifying unusual behaviors that deviate from normal baselines. This includes abnormal login times, excessive data transfers, or unexpected user activity, using statistical thresholds or rule-based detection methods.

Log Enrichment

Log enrichment enhances raw logs by adding contextual information such as IP geolocation, user roles, asset tags, or threat intelligence data. This improves investigation accuracy and reduces analyst effort.

Key Objectives

- Develop the ability to analyze and correlate logs from multiple sources
- Detect complex threats while minimizing false positives

Learning Resources

- SANS Reading Room – *Effective Log Analysis*
- Elastic Anomaly Detection Documentation
- Public breach case studies (e.g., Equifax)

1.2 Threat Intelligence Integration

Core Concepts

Indicators of Compromise (IOCs)

Includes malicious IP addresses, file hashes, domains, tactics, techniques, and procedures (TTPs).

SOC Integration

Threat intelligence feeds are integrated into SIEM platforms to automatically enrich alerts with reputation and context.

Threat Hunting

Proactively searching for adversary behavior mapped to MITRE ATT&CK techniques such as T1078 (Valid Accounts).

Learning Resources

- MITRE ATT&CK Framework
- STIX/TAXII Standards
- AlienVault OTX Practical Use Cases

1.3 Incident Escalation Workflows

Core Concepts

SOC Tier Model

- Tier 1: Alert triage
- Tier 2: Investigation and validation
- Tier 3: Advanced threat analysis and response

Communication

Use of SITREP templates and stakeholder briefings to ensure clear escalation.

Automation

Use of SOAR platforms to automate ticketing, enrichment, and response workflows.

Learning Resources

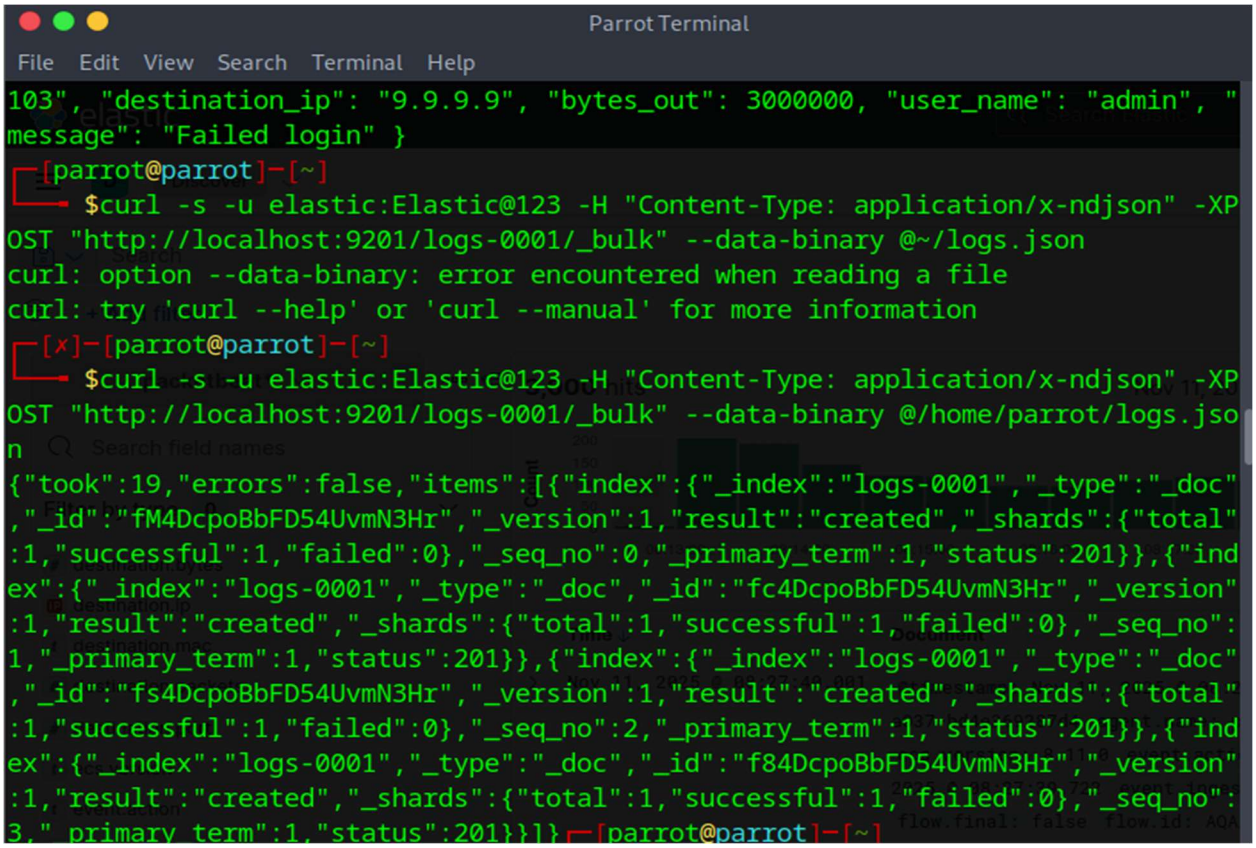
- NIST SP 800-61 Incident Handling Guide
- SANS Incident Handler's Handbook
- Splunk SOAR Documentation

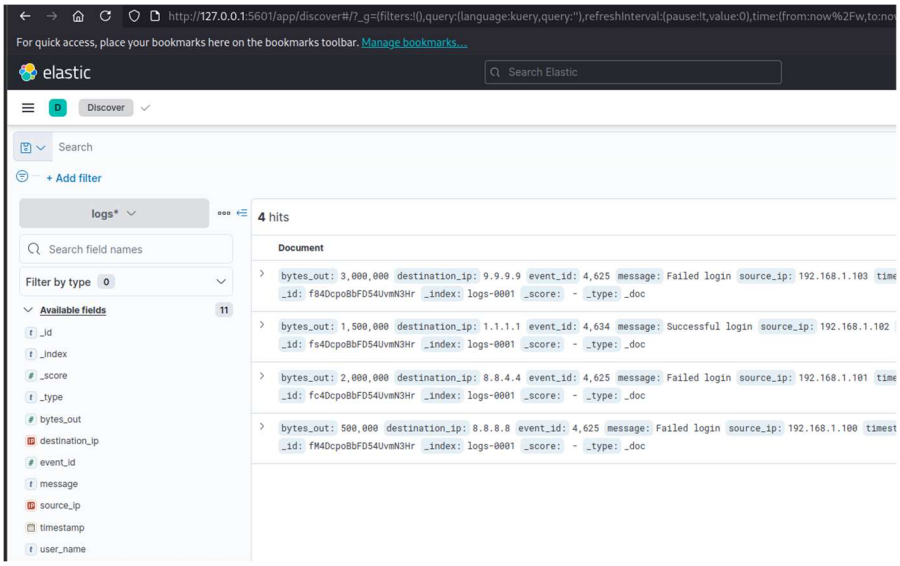
---

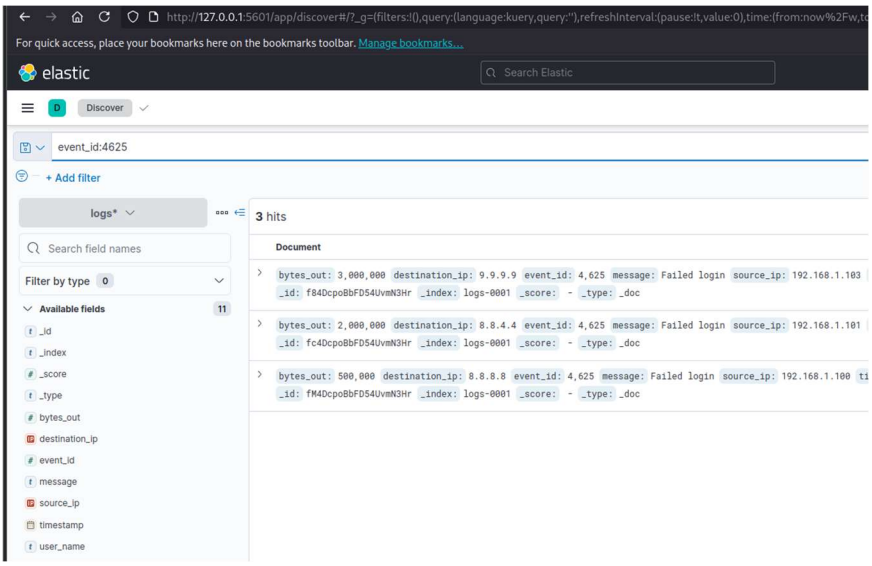
2. Practical Application

2.1 Advanced Log Analysis

Activity: Log Ingestion and Verification







Sample Correlated Log Data

Timestamp	Event ID	Source IP	Destination IP	Notes
January, 2026, 12:03:00	4625	192.168.1.103	9.9.9.9	High outbound traffic

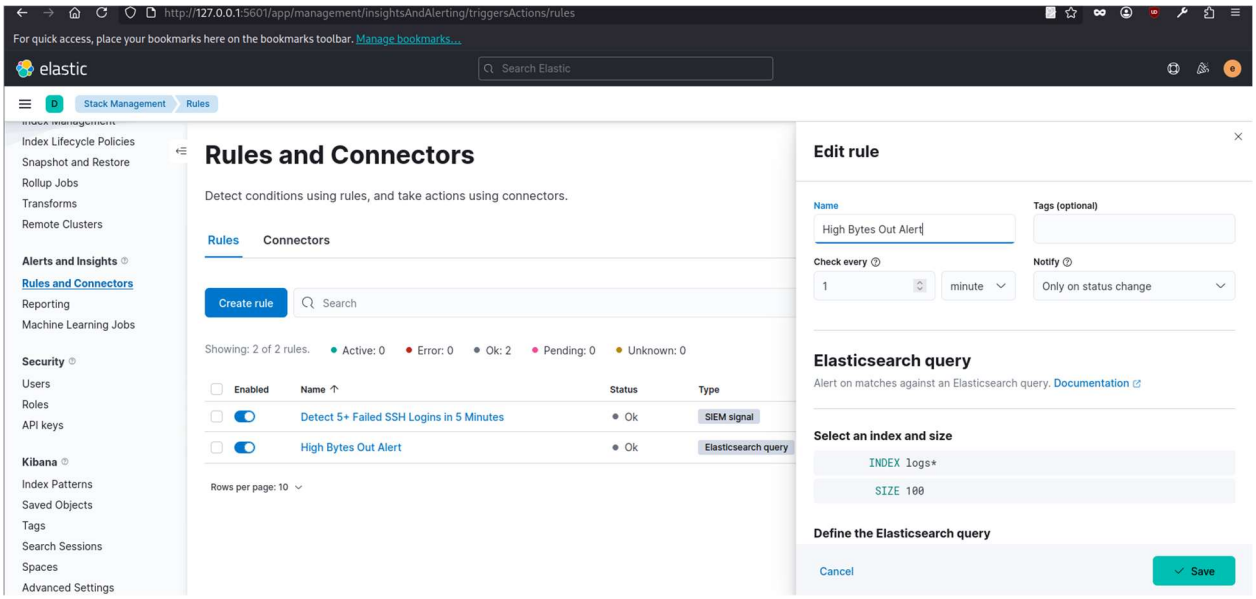
Timestamp	Event ID	Source IP	Destination IP	Notes
January, 2026 12:01:00	4625	192.168.1.101	9.9.9.9	High outbound traffic

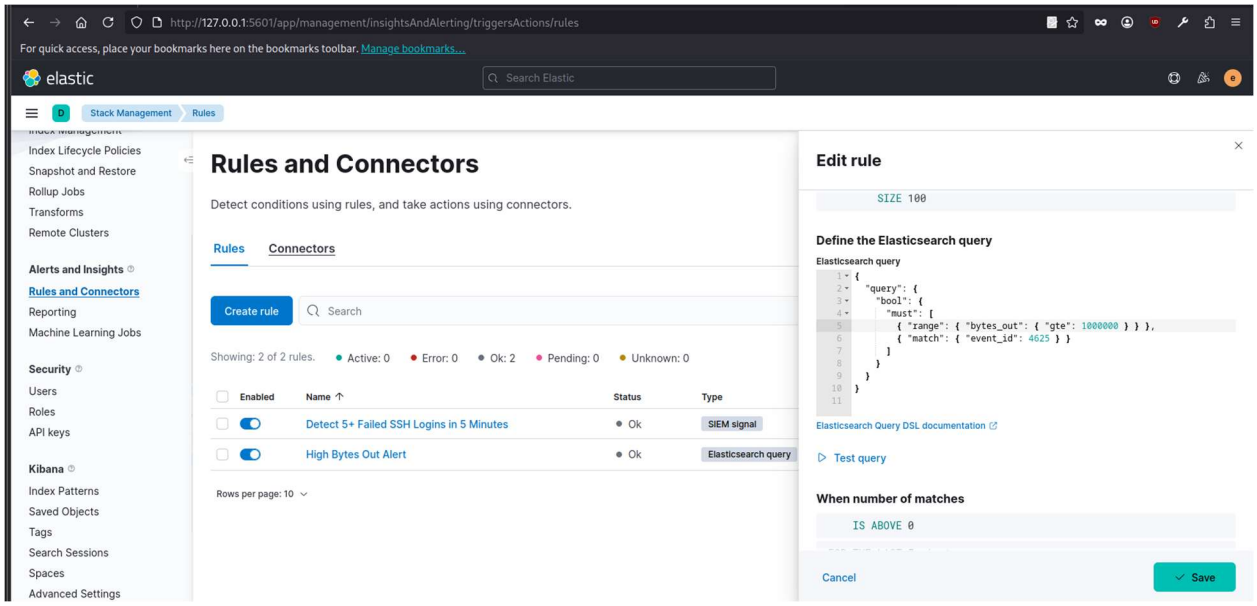
---

Anomaly Detection

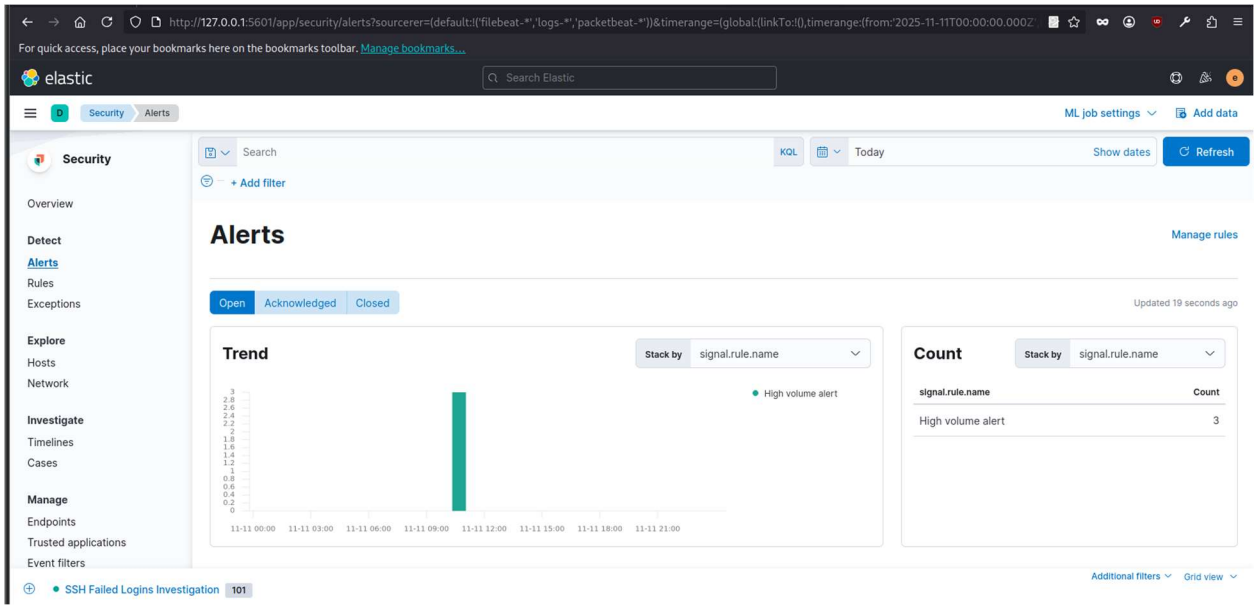
Task:

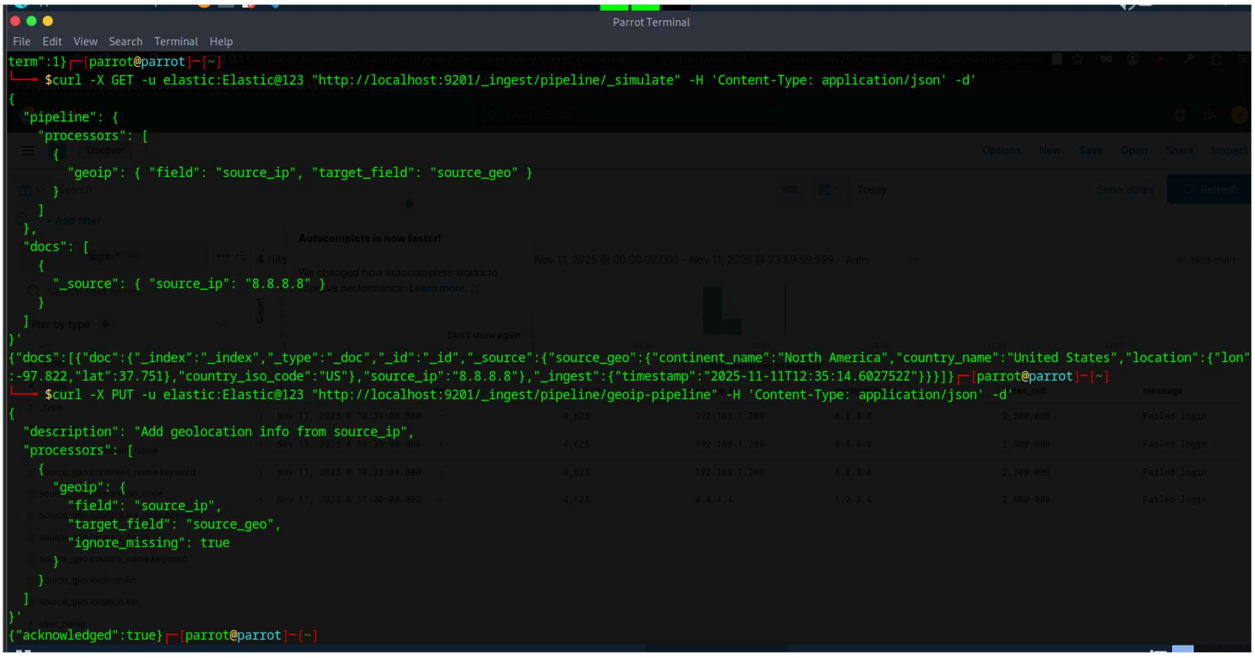
Create an Elastic rule to detect high-volume data transfers where bytes_out > 1MB within 1 minute.





Log Enrichment





Summary

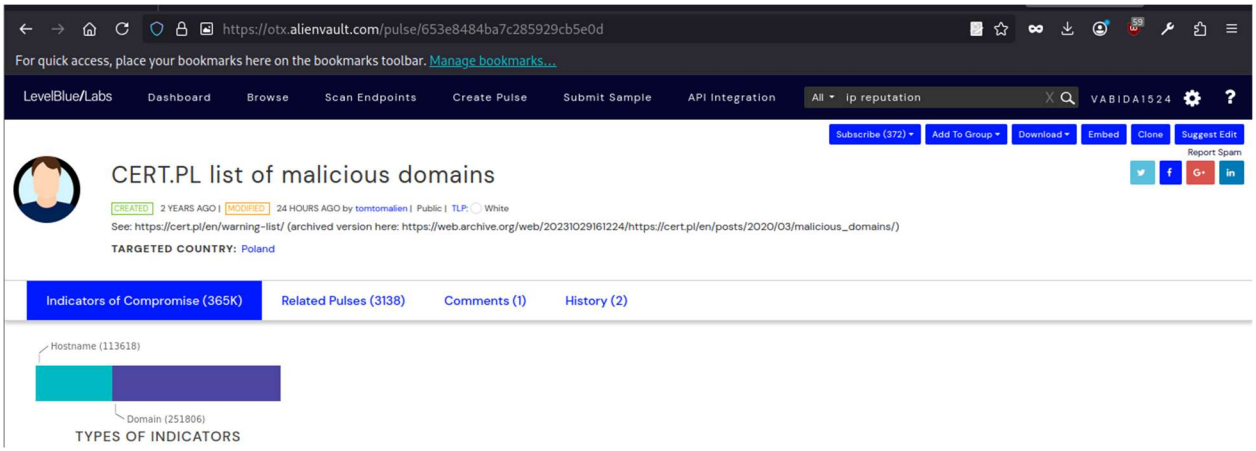
Network logs were ingested into Elasticsearch, timestamp issues were corrected, and anomaly rules were created to detect high-volume data transfers. GeoIP enrichment was applied to source IPs, enabling improved correlation of failed logins and suspicious data exfiltration attempts.

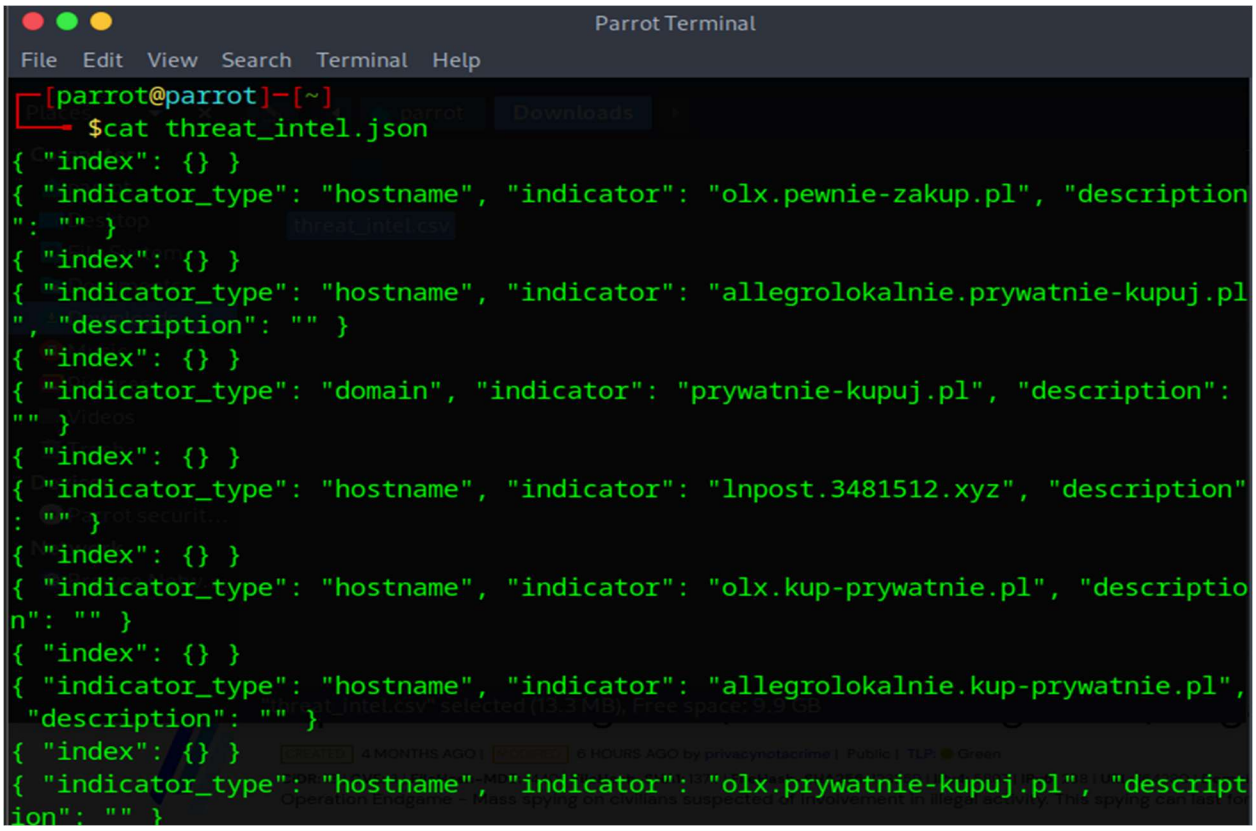
---

3. Threat Intelligence Integration

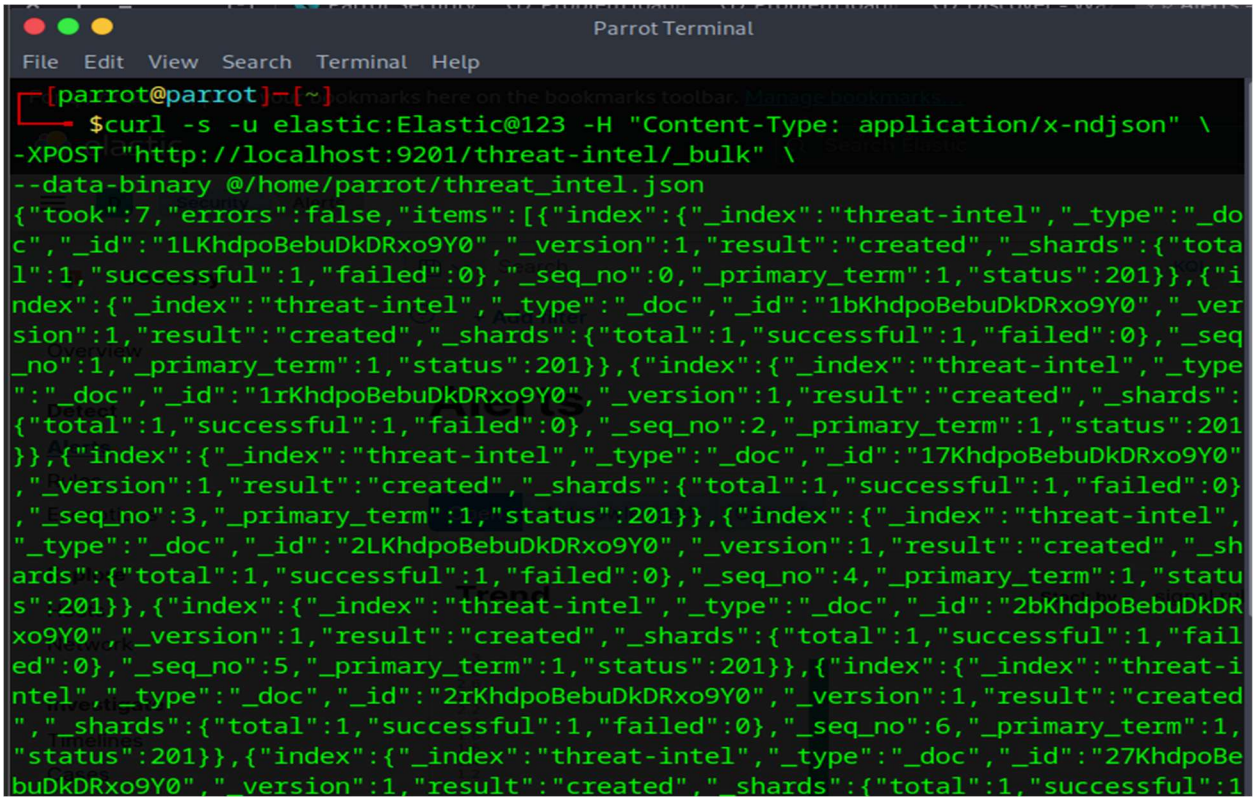
Activities

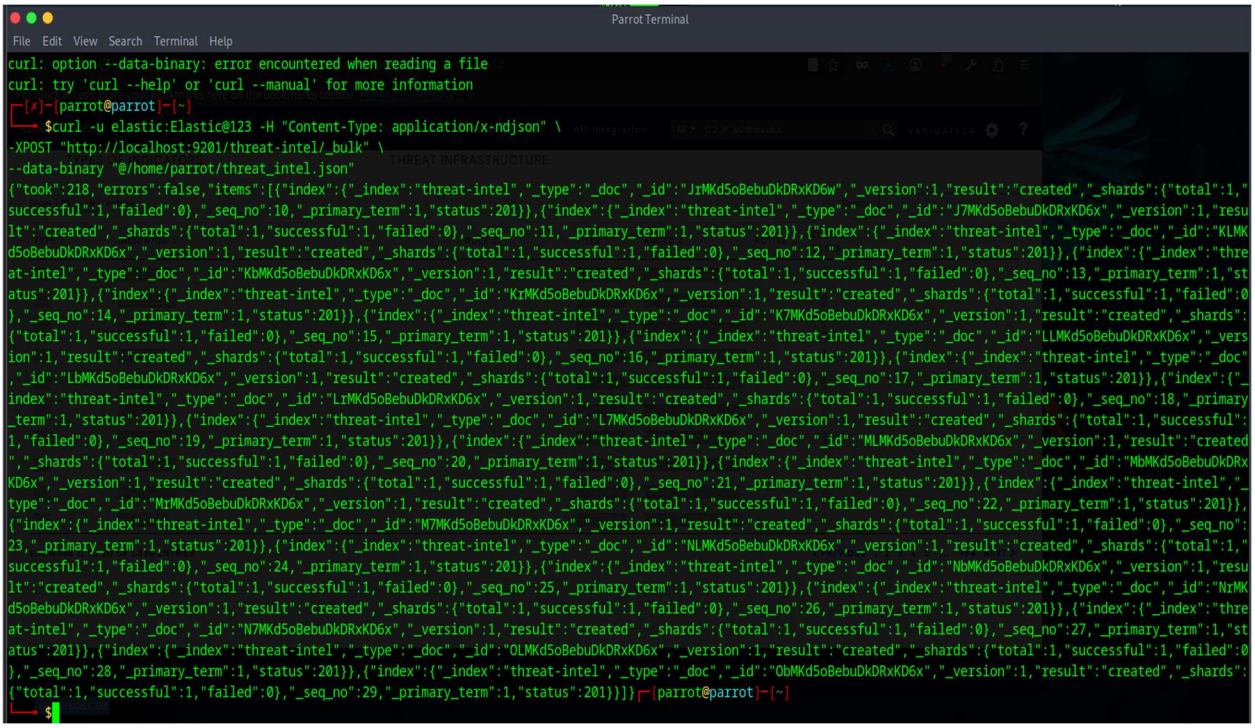
- Import threat intelligence feeds
- Enrich alerts
- Perform threat hunting





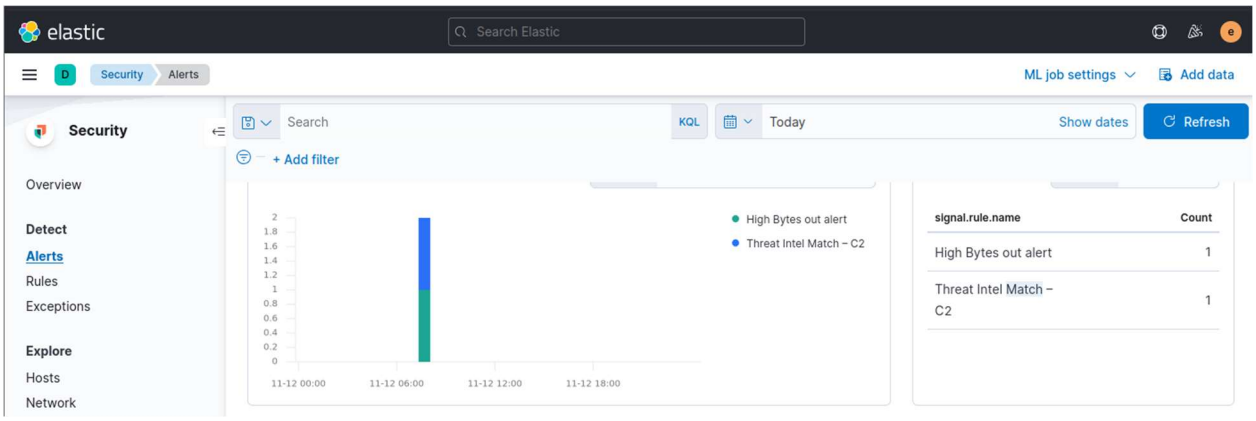
Convert data to the json format.





Correlation Rule Creation

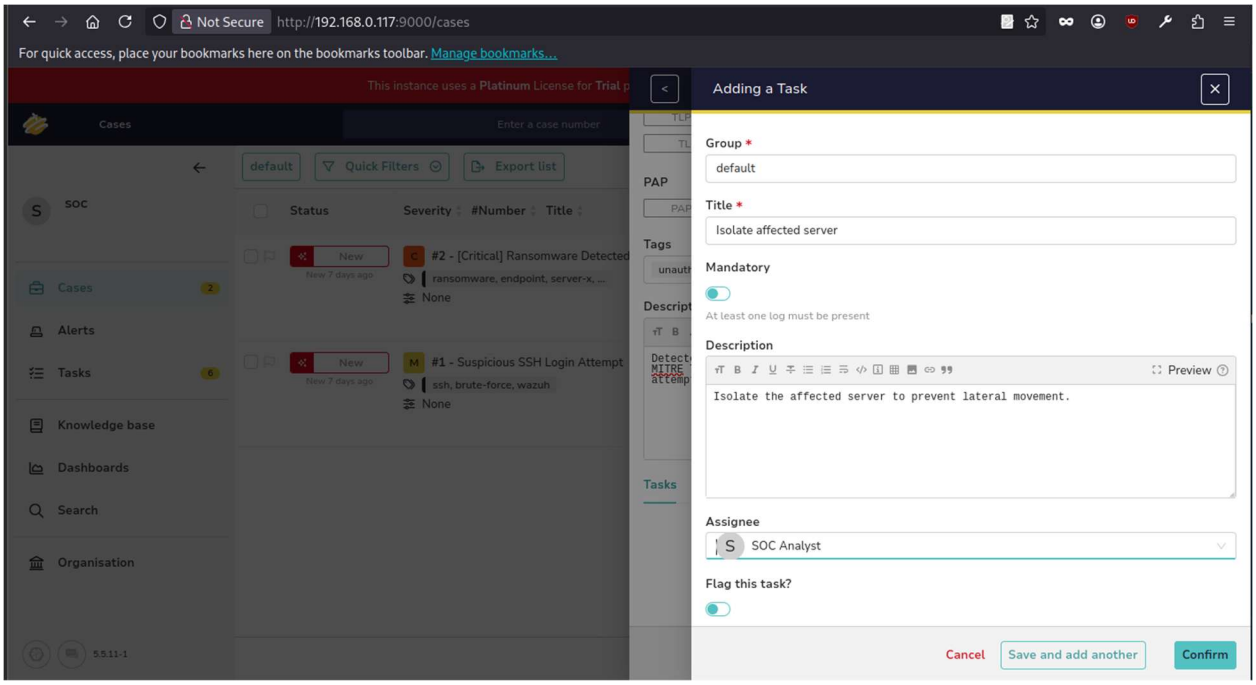
Rule created for the malicious IP from AlienVault feed.

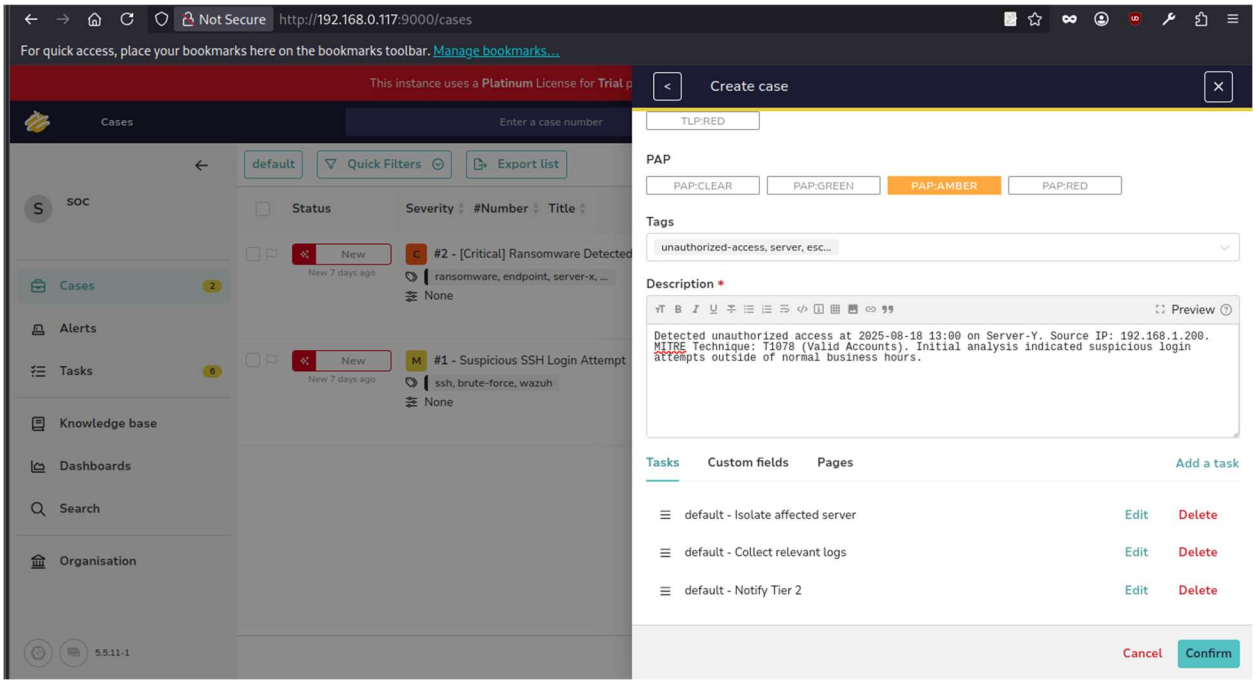


Alert Example

Alert ID	IP	Reputation	Notes
001	185.244.172.155	Malicious (OTX)	Matched DarkComet C2

MITRE T1078 Hunt (Valid Accounts)





Summary

A hunt for MITRE technique T1078 identified 12 successful logins from non-system accounts. These events indicate valid authentication activity that may represent legitimate access or potential credential misuse requiring further validation.

4. Incident Escalation Practice

Activities

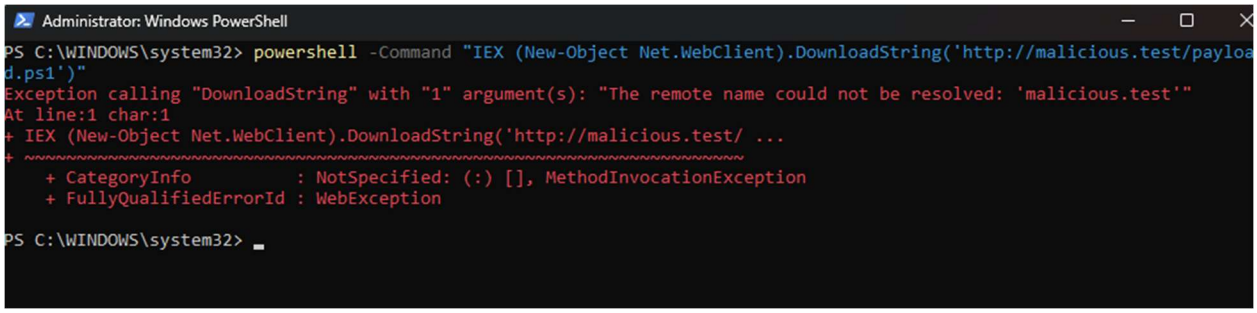
- Simulate escalation
- Create TheHive case
- Draft SITREP

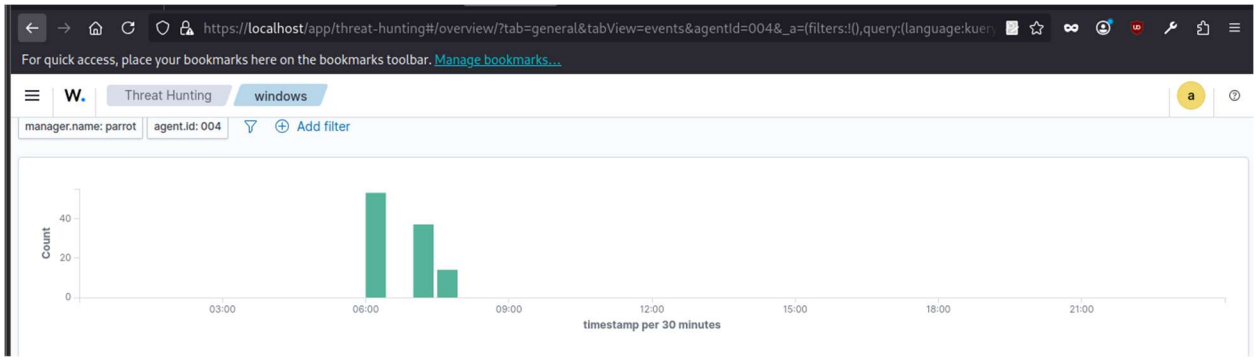
SITREP Summary (Mock Incident)

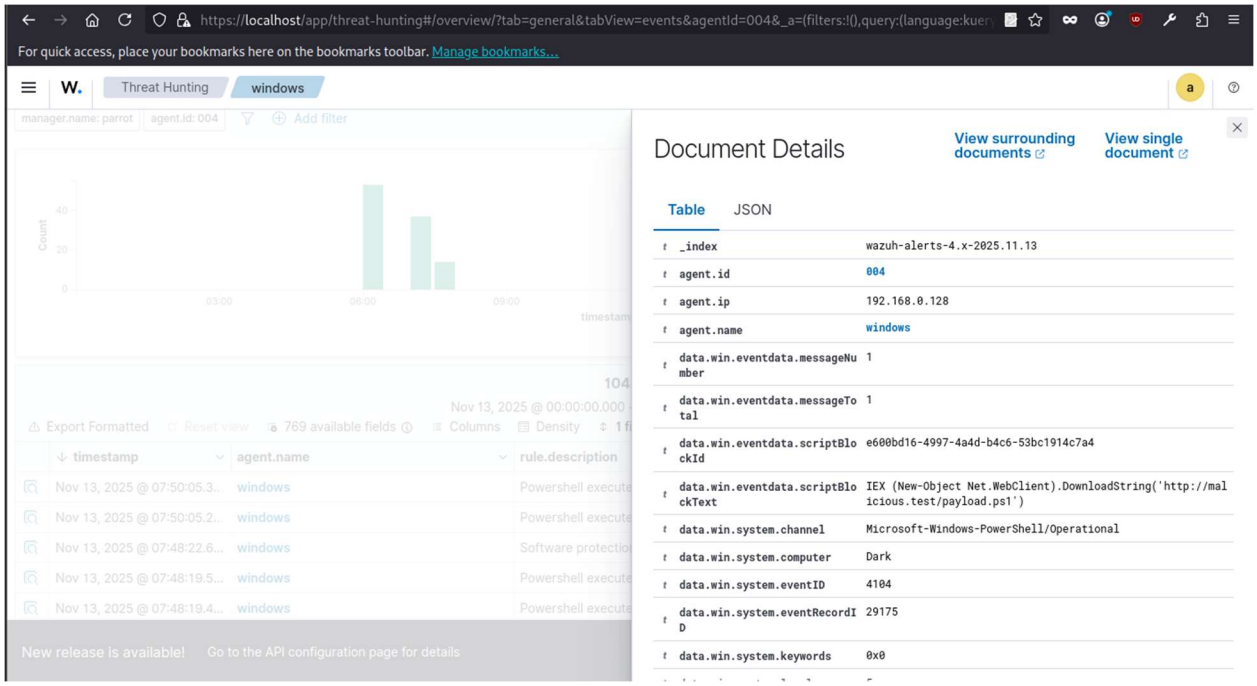
Section	Details
Summary	Unauthorized access detected
Actions Taken	Server isolated, escalated to Tier 2
Next Steps	Log review and user verification
Prepared By	SOC Analyst
Date	2026-01-13

---

5. Alert Triage with Threat Intelligence

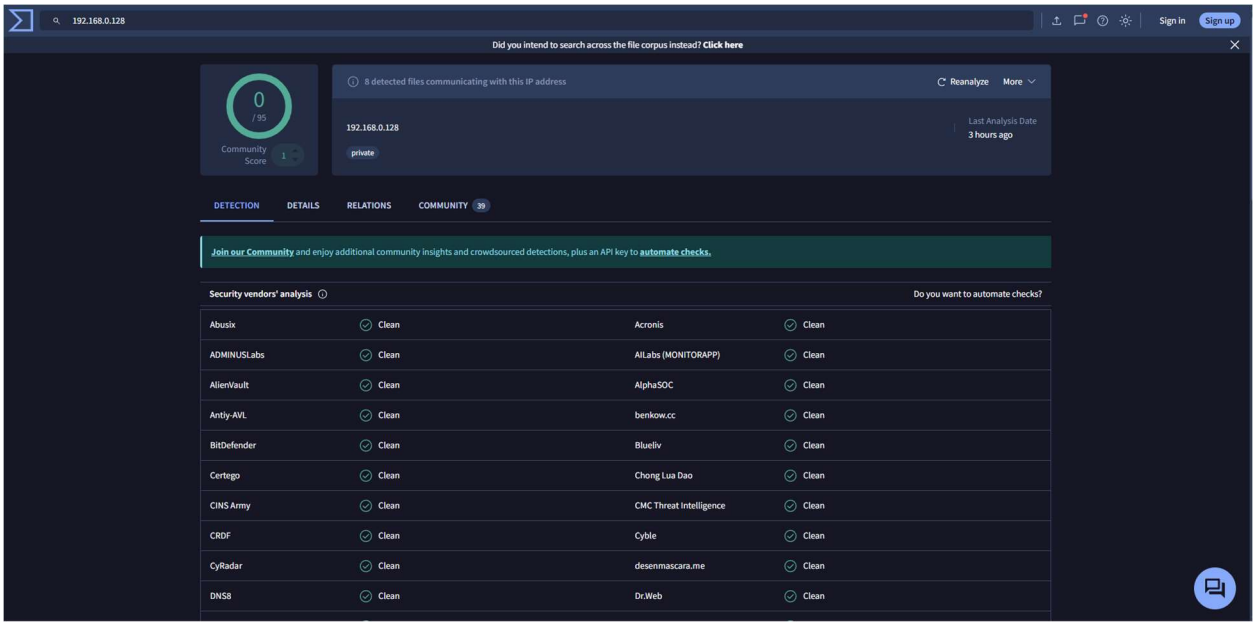


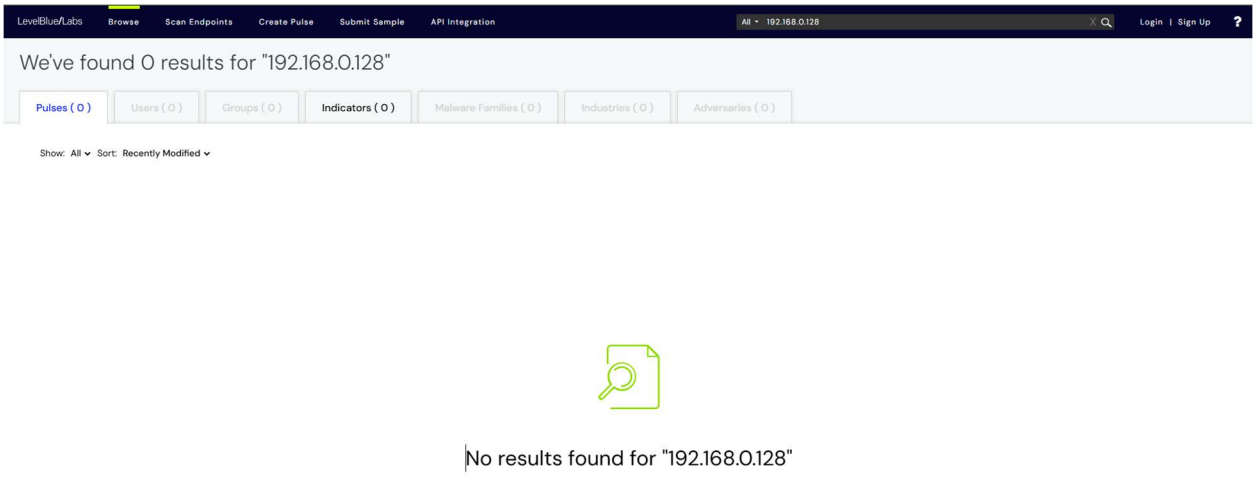




Alert Details

Alert ID	Description	Source IP	Priority	Status
004	PowerShell ScriptBlock Execution	192.168.0.128	Medium	Open





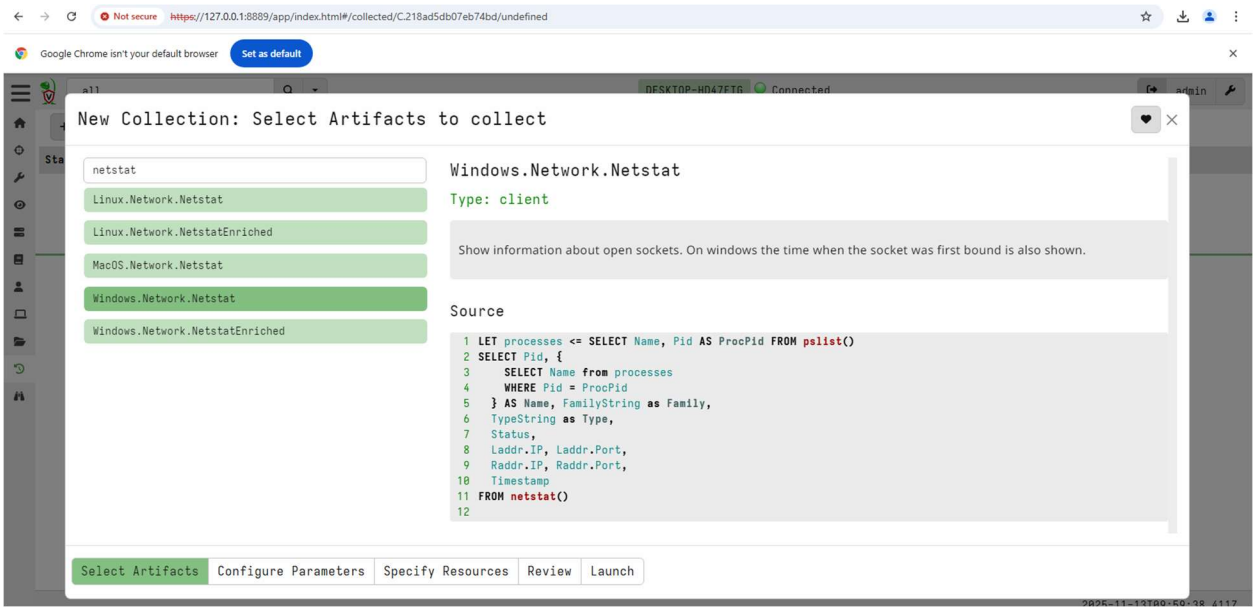
Summary

The PowerShell alert was analyzed, and IOC validation showed no malicious reputation. The source IP was identified as an internal lab system, confirming a benign event.

---

6. Evidence Preservation and Analysis

Volatile Data Collection



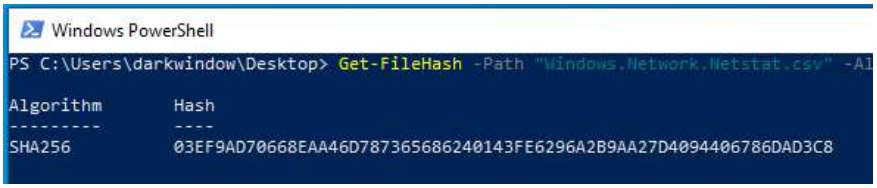
Chain of Custody

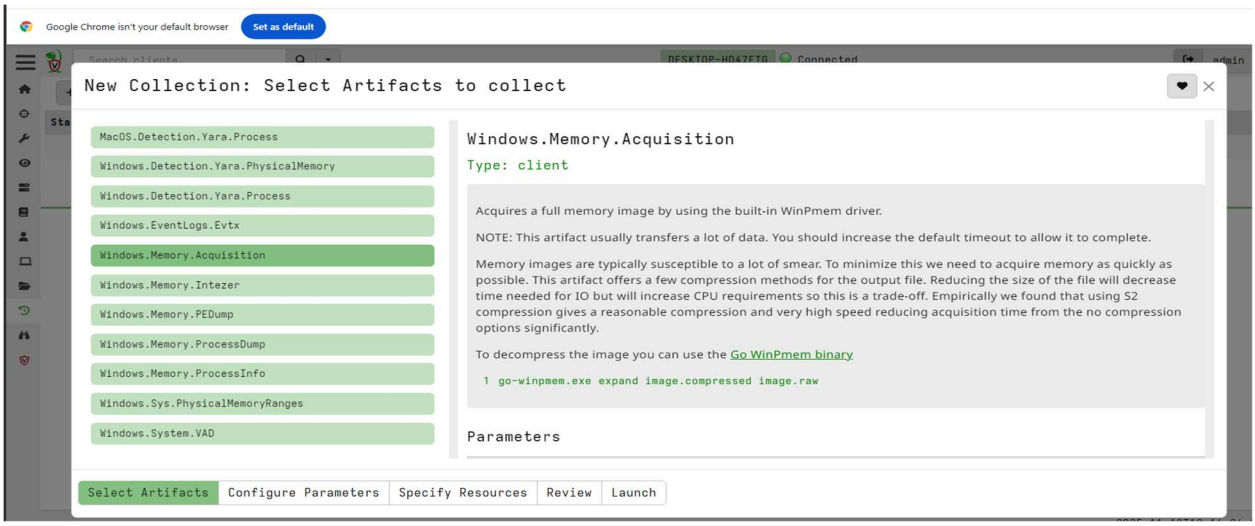
Item	Description	Collected By	Date	Hash
Netstat CSV	Network connections	SOC Analyst	2026-01-13	SHA-256
Memory Dump	Server-Y dump	SOC Analyst	2026-01-13	SHA-256

---

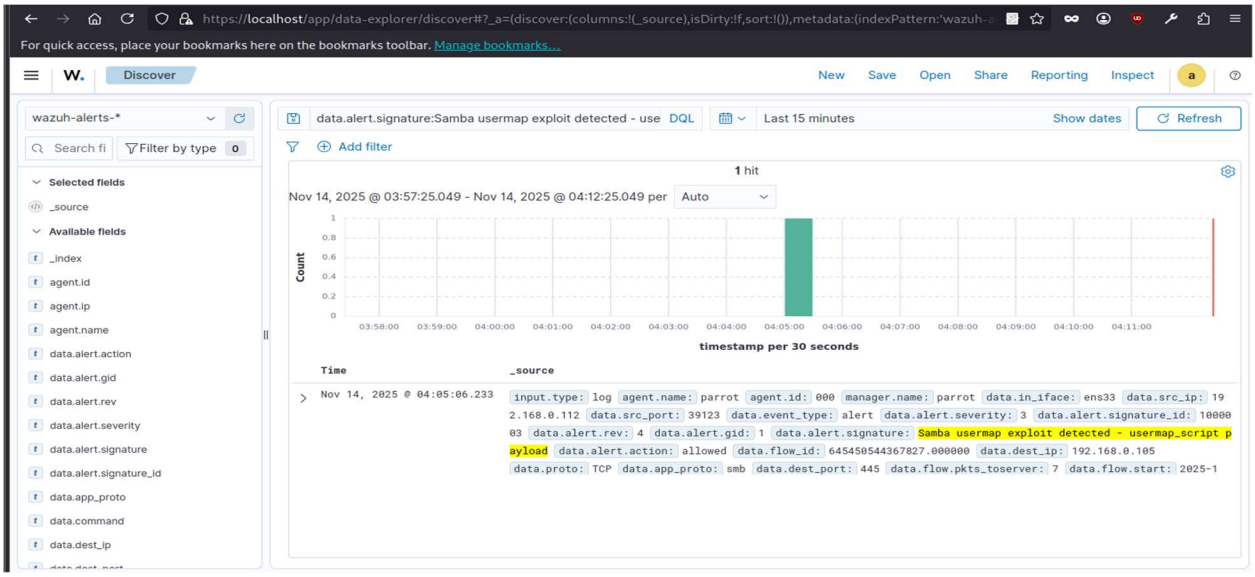
7. Capstone Project – Full SOC Workflow Simulation

7.1 Attack Simulation

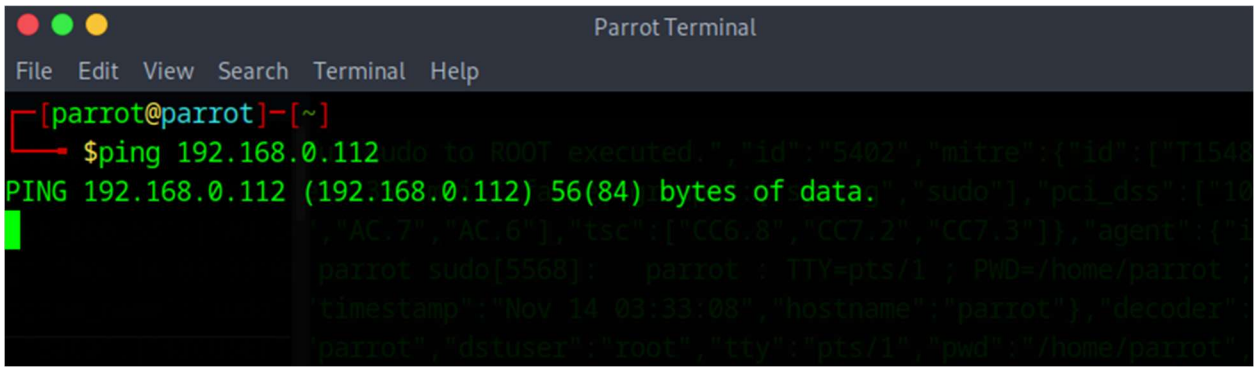


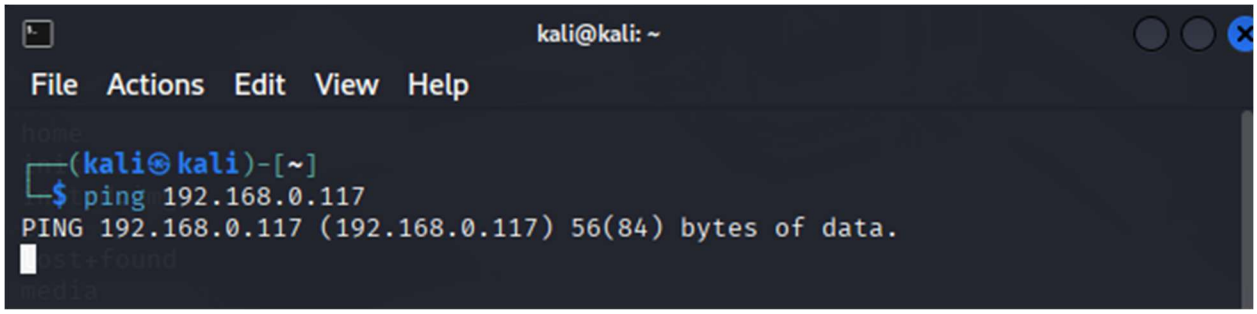


7.2 Detection and Triage

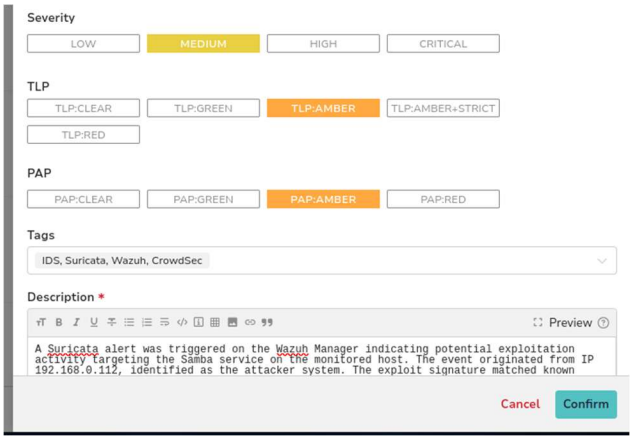


7.3 Response and Containment





7.4 Escalation



7.5 Reporting & Management Brief

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
2. https://attack.mitre.org/
3. https://docs.suricata.io/
4. https://documentation.wazuh.com/current/index.html
5. https://docs.crowdsec.net/
6. https://nvlpubs.nist.gov/nistpubs/specialpublications/nist.sp.800-61r2.pdf