Security Operation Center Task – 3

1. Advanced Log Analysis

Core Concepts :-

- Log Correlation
- Anomaly Detection
- Log Enrichment

Core Concepts Definitions

- **Log Correlation :-**
  - Log correlation is the process of collecting, normalizing, and analyzing logs from multiple sources—such as firewalls, endpoints, servers, and applications—to identify related events and attack patterns that indicate a security incident.
  - A SOC analyst uses log correlation to connect individual events into a meaningful sequence, helping confirm real threats and reduce false positives.

- **Anomaly Detection :-**
  - Anomaly detection is the process of identifying unusual or abnormal behavior in systems, networks, users, or applications by comparing current activity against a baseline of normal behavior.
  - In a SOC, anomaly detection helps analysts detect unknown threats, insider attacks, and zero-day activity that do not match known signatures or rules.

- **Log Enrichment :-**
  - Log enrichment is the process of adding contextual and intelligence data to raw log events to make them more meaningful, actionable, and easier for a SOC analyst to investigate.
  - Instead of viewing a log as just an IP, user, or event ID, enrichment provides who, what, where, and risk level.

- **Key Objectives**
  - The key objective is to develop the ability to analyze, correlate, and interpret logs from multiple security sources in order to identify complex, multi-stage threats while reducing false positives in a SOC environment.
  - Additionally, this objective focuses on building skills to recognize attack patterns across endpoints, networks, and applications.
    It also aims to improve alert accuracy and prioritization by validating events using

multiple data sources.Ultimately, it helps SOC analysts respond faster and more confidently to real security incidents.

Expanded Objective Explanation

- Analyze logs effectively
  Understand and interpret logs from firewalls, endpoints, servers, applications, and security tools.
- Correlate multiple data sources
  Link related events across different systems to uncover attack patterns that are not visible in isolated logs.
- Identify complex threats
  Detect advanced attacks such as brute-force followed by malware execution, lateral movement, and data exfiltration.
- Reduce false positives
  Validate alerts by cross-checking multiple logs, ensuring only real threats are escalated.
- Improve incident response accuracy
  Provide clear, evidence-based findings to support faster and more confident response decisions.

SOC Example

- Single failed login → likely noise
- Failed logins + successful login + abnormal outbound traffic → confirmed incident

- **Skill-Building Method**
- **Log Correlation**

Log correlation is the process of collecting, analyzing, and linking events from multiple log sources—such as firewalls, endpoints, servers, and applications—to identify attack patterns, confirm security incidents, and understand the full scope of an attack. Instead of analyzing logs in isolation, SOC analysts correlate related events to uncover complex and multi-stage threats.

Why Log Correlation Is Important

- Single events often appear benign or noisy
- Advanced attacks occur in multiple stages
- Correlation helps reduce false positives
- Provides a complete attack timeline
- Enables accurate incident classification and response

Log Sources Involved

- Endpoint logs (Windows Event Logs, EDR)
- Network logs (Firewall, IDS/IPS, proxy)

- Application logs (Web servers, databases)
- Identity logs (Active Directory, IAM)

Detailed Example: Failed Logins + Suspicious Traffic

Step 1: Endpoint Authentication Logs

- Multiple failed login attempts
- Windows Event ID 4625
- Indicates possible brute-force or credential-stuffing attack

Step 2: Authentication Success

- Event ID 4624 after repeated failures
- Suggests credentials may have been successfully compromised

Step 3: Network / Firewall Logs

- Unusual outbound traffic detected
- Connection to unknown or high-risk external IP
- Use of uncommon ports or abnormal data volume

Step 4: Correlation Outcome

- Failed logins → Successful login → Suspicious outbound traffic.

Source	What It Shows
Windows Event Logs	Logins, account usage
Firewall Logs	Network connections
EDR/Endpoint Logs	Process execution
Application Logs	App authentication events
DNS Logs	Suspicious domains

- **Anomaly Detection**

  Anomaly detection is the practice of **identifying unusual or abnormal behavior** in users, systems, networks, or applications by comparing current activity against an established **baseline of normal behavior**. In a SOC environment, anomaly detection helps uncover **unknown threats, insider misuse, and compromised accounts** that may bypass traditional signature-based controls.

Purpose of Anomaly Detection

- Detect **previously unknown or zero-day attacks**
- Identify **insider threats**
- Spot **account compromise**
- Reduce reliance on known signatures
- Improve overall threat visibility

Common Anomaly Detection Techniques

1. Statistical Methods

These methods use historical data to define normal ranges.

- Mean, median, and standard deviation
- Threshold-based alerts (e.g., data transfer exceeds normal limits)

Example:
A user typically downloads 50 MB/day
Sudden transfer of 5 GB in one session → **Anomaly detected**

2. Rule-Based Methods

Predefined rules created by SOC teams.

- Login outside business hours
- Access from unusual geolocation
- Multiple failed logins followed by success

Example:
Login detected at **3 AM** for a user who normally logs in **9 AM–6 PM**

3. Behavior-Based / UEBA

Uses behavior profiling to detect deviations.

- Tracks user and entity patterns over time
- Identifies subtle anomalies

Example:
User accesses sensitive files they never accessed before

Common Anomaly Detection Use Cases

- Unusual login times or locations
- High-volume or sudden data transfers
- Rare process execution on endpoints

- Abnormal network traffic patterns
- Unexpected privilege escalation

User	Normal Login Hours
Carol	08:00 – 17:00
Dave	09:30 – 18:30
Emma	07:00 – 16:00
Frank	10:00 – 19:00
Grace	08:30 – 17:30

- **Log Enrichment**

  Log enrichment is the process of enhancing raw log data with additional contextual information to make security events easier to understand, prioritize, and investigate. Instead of analyzing isolated technical details (IP address, username, event ID), enrichment adds business, user, asset, and threat intelligence context.

  Purpose of Log Enrichment

  - Improve alert accuracy
  - Speed up incident investigations
  - Reduce analyst effort and fatigue
  - Enable better risk-based prioritization
  - Support informed response decisions

Types of Context Added During Enrichment

1. Geolocation Context

- Country, city, region of source IP
- Helps identify suspicious foreign access

Example:
Login attempt from IP mapped to a high-risk country

2. User Context

- User role (admin, employee, service account)
- Department and privilege level
- Login history

Example:
Failed login targeting a privileged admin account

3. Asset Context

- Asset type (server, workstation)
- Asset criticality (high, medium, low)
- Business function

Example:
Login attempt on a Domain Controller (Critical asset)

4. Threat Intelligence

- IP/domain reputation
- Known malicious indicators
- Past incidents

Example:
Source IP listed in multiple threat intelligence feeds

5. Historical & Behavioral Context

- Past alerts involving same IP or user
- Normal behavior patterns

SOC Example

Raw Log:
Failed login from 103.45.67.89

Enriched Log:

- Country: Russia
- IP Reputation: Malicious
- User Role: Domain Admin

Enrichment Type	Description	Source / Method
GeoIP	Map IP addresses to countries, cities	GeoIP databases (MaxMind, IP2Location)
User Role	Add info about user privileges	Active Directory / IAM
Asset Criticality	Classify endpoints by business importance	CMDB / Asset Management

Threat Intelligence	Tag IPs, domains with reputation scores	Threat intel feeds (VirusTotal, AlienVault OTX)
Time Zone / Local Time	Convert timestamps to user's timezone	Enrichment scripts

- **Conclusion**
- **Log Correlation** enables analysts to **connect events across multiple systems**, revealing complex attack patterns that single logs alone cannot expose. By linking failed logins, endpoint activity, and suspicious network traffic, organizations gain a clearer picture of ongoing threats.
- **Anomaly Detection** complements correlation by **identifying deviations from normal behavior**, such as unusual login times or excessive data transfers. Using statistical or rule-based methods, anomalies serve as early warning signs for potential compromise or insider threats.
- **Log Enrichment** enhances the value of raw logs by **adding contextual information** like geolocation, user roles, and threat intelligence. This context accelerates investigation, reduces false positives, and helps prioritize alerts based on risk.

2. Threat Intelligence Integration

Threat Intelligence (TI) Integration is the process of incorporating external and internal intelligence data into your security monitoring and response workflows. This intelligence provides contextual information about known or emerging threats such as malicious IP addresses, domains, file hashes, attacker tactics, and vulnerabilities.

Core Concepts:

- **Threat Intelligence Types :-**

- **Indicators of Compromise (IOCs)**
  - **IOCs** are forensic artifacts observed on a network or endpoint that indicate a potential intrusion.
  - They are **specific, observable pieces of evidence** related to malicious activity.

IOC Type	Description	Example
Malicious IP	IP addresses used by attackers	185.220.101.5
Malicious Domain	Domains used for C2 or phishing	evil-site.com
File Hash	Hash values of malware files	SHA256: abc123...
Email Addresses	Used in phishing or spam	mailto:attacker@example.com

- **Tactics, Techniques, and Procedures (TTPs)**
  - **TTPs** describe the behavior patterns and methods used by threat actors.
  - Unlike IOCs (which are specific), TTPs explain **how** attackers operate, often more persistent and generalizable.

Term	Description
Tactics	The attacker's goal or "why" (e.g., persistence, privilege escalation)
Techniques	The "how" – specific ways attackers achieve tactics (e.g., spear phishing, credential dumping)
Procedures	Detailed steps or scripts used to implement techniques

Frameworks

- **MITRE ATT&CK** is the most widely used framework cataloging TTPs.
- Helps SOCs understand attacker behavior beyond specific IOCs.

Use in SOC

- Guides detection rule development.
- Provides context for incident response.
- Supports threat hunting and proactive defense.

- **Threat Feeds and Standards**

  Threat Feeds

  - Regularly updated collections of IOCs and threat data shared by vendors, communities, or governments.
  - Examples: AlienVault OTX, VirusTotal, Recorded Future, MISP.

Standard	Purpose
STIX (Structured Threat Information eXpression)	A standardized language to represent threat data (IOCs, TTPs) in a structured, machine-readable format
TAXII (Trusted Automated eXchange of Indicator Information)	A protocol for securely exchanging STIX data between systems

- **Benefits**

  - Enables automated ingestion and sharing of threat data.

- Improves interoperability between tools.
- Facilitates real-time threat intelligence sharing.

- **Use in SOC**

  - Integrate STIX/TAXII feeds into SIEMs or SOAR platforms.
  - Automate enrichment and alerting based on latest intelligence.
  - Collaborate with other organizations for collective defense.

Threat Intelligence Type	Description	Examples	SOC Use Cases
IOCs	Specific artifacts indicating compromise	Malicious IPs, hashes	Detection, alerting, blocking
TTPs	Behavioral patterns of attackers	MITRE ATT&CK techniques	Rule creation, hunting, response
Threat Feeds (STIX/TAXII)	Standardized sharing of threat data	AlienVault OTX, STIX files	Automated intel ingestion, collaboration

Threat intelligence types—**IOCs, TTPs, and threat feeds (STIX/TAXII)**—work together to improve security detection and response. IOCs enable quick identification of known threats, TTPs help detect attacker behavior even when indicators change, and threat feeds ensure intelligence is shared and updated automatically. Combined, they strengthen proactive defense and faster incident response.

- **Integration in SOC**

Threat intelligence integration in a SOC involves connecting external threat intelligence feeds to **SIEM platforms** so security alerts are automatically enriched with context and risk information.

How Integration Works

1. **Threat feeds ingestion**
   - SIEM pulls IOCs (malicious IPs, domains, hashes) from threat intel sources.
2. **Log matching**
   - Incoming logs (firewall, endpoint, proxy) are checked against these IOCs.
3. **Alert enrichment**
   - If a match is found, the alert is enriched with reputation, threat type, and confidence.
4. **Automated prioritization**
   - Alerts linked to high-risk intelligence are escalated automatically.

Practical Example

- Firewall log shows outbound traffic to IP **185.220.101.5**

- Threat intelligence feed identifies this IP as a **known C2 (Command & Control) server**
- SIEM enriches the alert with:
  - Threat type: C2 infrastructure
  - Risk level: High
  - Associated malware family

Benefits in SOC Operations

- Faster triage and investigation
- Reduced false positives
- Better alert prioritization
- Proactive threat detection

Conclusion

- Integrating threat intelligence into SIEMs allows SOC teams to automatically enrich alerts with real-world threat context, enabling quicker, more accurate detection and response to active attacks.

- **Threat Hunting with Intelligence**

Threat hunting with intelligence is a **proactive SOC activity** where analysts use threat intelligence and attacker behavior (TTPs) to search for hidden or undetected threats in the environment—instead of waiting for alerts.

Why Use Threat Intelligence for Threat Hunting?

- Detect **stealthy attacks** that bypass automated alerts
- Identify **misuse of legitimate credentials**
- Reduce dwell time of attackers
- Improve SOC maturity from reactive → proactive

Example: Hunting for T1078 – Valid Accounts Misuse

Attackers often use **stolen credentials** to access systems while appearing legitimate.

Intelligence Inputs Used

- **MITRE ATT&CK:** T1078 – Valid Accounts
- **Threat reports:** Credential theft, brute-force, phishing campaigns
- **Historical baselines:** Normal user behavior

Hunt Hypotheses

"An attacker may be using valid credentials to access systems outside normal user behavior."

Indicator	Why It's Suspicious
Logins at unusual hours	Outside user baseline
Login from new country/IP	Possible stolen credentials
Multiple systems accessed quickly	Lateral movement
Admin account usage on non-admin systems	Privilege misuse
VPN login followed by internal access	Compromised remote access

Sample Hunting Activities

1. Unusual Login Time
- Search Event ID **4624**
- Compare login time against user baseline

2. New or Rare Source IP
- Identify logins from IPs not previously used by the account

3. Privileged Account Abuse
- Monitor admin accounts accessing file servers or user endpoints

4. Correlation with Other Activity
- Valid login + suspicious PowerShell, RDP, or SMB activity

Enrichment for Better Hunting
- User role (admin vs standard)
- GeoIP location
- Asset criticality
- Threat intelligence tags

Outcome of a Successful Hunt
- Confirm credential compromise
- Identify lateral movement
- Generate new detection rules
- Improve SIEM alert logic

- **Key Objectives**

  The key objective is to build proficiency in leveraging threat intelligence to strengthen both detection and response capabilities within a SOC. This involves understanding and applying intelligence in practical, operational ways:
- Use threat intelligence to enrich SIEM alerts, adding context such as reputation, threat type, and risk level.
- Improve detection accuracy by combining IOCs and attacker TTPs (MITRE ATT&CK) with internal logs.
- Prioritize and triage alerts effectively based on intelligence-driven risk scoring.

- Proactively hunt for threats using intelligence-led hypotheses instead of relying only on reactive alerts.
- Enhance incident response by using intelligence to guide containment, eradication, and prevention actions.

Overall, mastering threat intelligence enables SOC teams to move from basic alert monitoring to **context-aware, proactive security operations**.

3. Incident Escalation Workflows

Incident escalation workflows are structured processes that define how security incidents move through a SOC, ensuring the right teams respond at the right time based on severity, impact, and risk.

Purpose of Incident Escalation

- Ensure timely response to serious threats
- Assign incidents to the appropriate expertise level
- Minimize business impact and downtime
- Maintain clear communication and accountability

Level	Role	Key Responsibilities
Tier 1 (L1)	SOC Analyst	Alert monitoring, initial triage, false-positive filtering
Tier 2 (L2)	SOC Analyst	Deep investigation, correlation, containment actions
Tier 3 (L3)	IR/Threat Hunting Team	Forensics, eradication, recovery
Management	SOC Manager / CISO	Business decisions, external communication

Example Escalation Workflow

1. **Detection (Tier 1)**
    - SIEM alert triggered
    - Validate alert and collect basic logs
2. **Investigation (Tier 2)**
    - Correlate logs, enrich with threat intel
    - Contain affected systems
3. **Advanced Response (Tier 3)**
    - Perform forensic analysis
    - Eradicate threat and restore systems
4. **Management Notification**

  - Assess business impact
  - Coordinate legal, PR, and leadership updates

- **Documentation & Tracking**

  Each escalation should include:

  - Incident summary
  - Severity level
  - Affected assets and users
  - Evidence collected
  - Actions taken

- **Core Concepts**

  - **Escalation Tiers**
  - **Communication Protocols**
  - **Automation in Escalation**

- **Core Concepts Defination**

- **Escalation Tiers :-**

  A SOC tier structure defines how security incidents are handled and escalated based on severity, complexity, and impact. Each tier has a clear role to ensure efficient and accurate incident response.

SOC Tier Structure

Tier 1 (T1) – Triage

Primary Role: First line of defense
Responsibilities:

- Monitor SIEM alerts and dashboards
- Perform initial triage and validation
- Identify false positives
- Collect basic evidence (logs, timestamps, IPs)
- Escalate confirmed or suspicious alerts

Typical Examples:

- Single failed login
- Malware alert with low confidence
- Policy violations

Tier 2 (T2) – Investigation

Primary Role: In-depth analysis
Responsibilities:

- Correlate logs across multiple sources

- Enrich alerts with threat intelligence
- Determine scope and impact
- Perform containment actions (isolate host, disable account)
- Decide whether to escalate further

Typical Examples:

- Brute-force followed by successful login
- Suspicious outbound traffic
- Lateral movement indicators

Tier 3 (T3) – Advanced Analysis

Primary Role: Expert-level response
Responsibilities:

- Conduct advanced threat analysis and forensics
- Malware reverse engineering
- Threat hunting and root cause analysis
- Lead eradication and recovery
- Improve detections and playbooks

Typical Examples:

- Active ransomware attack
- Advanced Persistent Threat (APT) activity
- Data exfiltration confirmed

Criteria	Description	Example
Severity	Level of risk to the organization	Ransomware = Critical
Complexity	Skill required to analyze incident	Obfuscated malware
Impact	Business or operational effect	Financial or data loss
Scope	Number of systems/users affected	Multiple endpoints
Confidence	Certainty of malicious activity	Confirmed C2 traffic

Example Escalation Flow

Tier 1: Detects multiple failed logins (4625) → escalates

Tier 2: Confirms credential compromise and suspicious traffic

Tier 3: Performs forensic analysis and full incident response

- **Communication Protocols**

Communication protocols ensure that security incidents are reported **clearly, consistently, and at the right level of detail** to SOC teams, management, and stakeholders. Structured communication reduces confusion and speeds up decision-making during incidents**.**

Section	Purpose
Incident Summary	What happened, when, and where
Current Status	Ongoing, contained, or resolved
Impact Assessment	Systems, users, or data affected
Actions Taken	Response and containment steps
Next Steps	Planned actions and timelines
Support Required	Decisions or resources needed

SOC SITREP

Incident: Suspicious outbound traffic detected
Status: Under investigation
Impact: One endpoint affected
Actions: Host isolated, account disabled
Next Steps: Forensic analysis ongoing

- **Stakeholder Briefings**

  Purpose

  - Inform non-technical stakeholders (management, legal, business leaders)
  - Focus on impact, risk, and decisions, not technical details

- **Key Elements**

Element	Description
Executive Summary	High-level incident overview
Business Impact	Downtime, data risk, financial impact
Risk Level	Low / Medium / High
Actions Taken	Containment and mitigation
Decisions Required	Approvals or next steps

- **Automation in Escalation**

  - **Automation in escalation** uses **SOAR (Security Orchestration, Automation, and Response)** tools to automatically handle repetitive SOC tasks, ensuring **faster, consistent, and error-free escalation** of security incidents.
  - SOAR platforms integrate **SIEM alerts, threat intelligence, ticketing systems, and response actions** into automated workflows (playbooks).

Task	Automation Example
Alert Enrichment	Add GeoIP, user role, threat intel automatically
Severity Scoring	Auto-calculate risk based on indicators
Ticket Creation	Create and assign incidents in Jira / ServiceNow
Tier Assignment	Route incident to Tier 2 or Tier 3
Notifications	Send alerts via email, Slack, Teams

Containment Actions	Isolate host, disable account (with approval)

Example SOAR Escalation Workflow

1. **SIEM Alert Triggered**
   - Failed logins + suspicious outbound traffic
2. **Automated Enrichment**
   - Threat intel identifies destination IP as C2
3. **Severity Assessment**
   - Risk score = Critical
4. **Automated Escalation**
   - Ticket created and assigned to Tier 2
   - SOC Manager notified
5. **Response Actions (Optional)**
   - Endpoint isolated after approval

Example Use Case

Scenario: Outbound traffic to known C2 server

- SOAR enriches alert with threat intel
- Confirms C2 reputation = High
- Auto-escalates to Tier 3
- Blocks IP at firewall

Best Practices for Automation

- Start with **low-risk, repeatable tasks**
- Use **human approval** for destructive actions
- Continuously tune playbooks
- Log all automated actions for auditing

- **Key Objectives:**

The key objective is to master incident escalation workflows and effective stakeholder communication to ensure security incidents are handled quickly, accurately, and transparently. This includes:

- Applying clear escalation workflows to route incidents to the appropriate SOC tier based on severity and complexity.
- Using structured communication methods (such as SITREPs) to provide timely, consistent updates during incidents.
- Communicating effectively with stakeholders, translating technical findings into business impact and risk.
- Ensuring accountability and coordination across SOC, incident response, and management teams.

  Overall, mastering these workflows enables faster decision-making, reduced impact, and improved trust during security incidents.

Practical Application

1. Advanced Log Analysis :-

- **Log Correlation**

Objective:
Identify potential compromise by correlating:

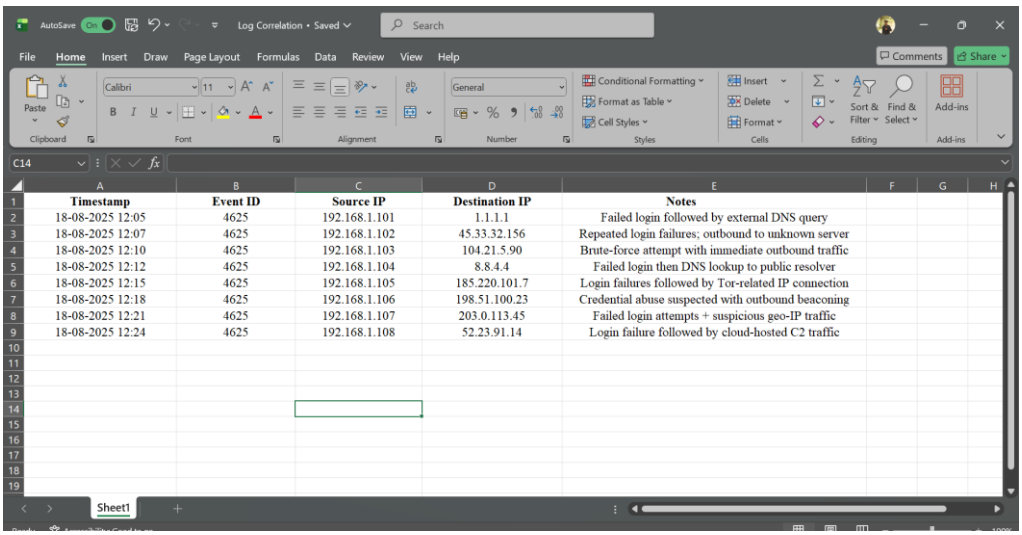
- Authentication failures (Windows Security logs – Event ID 4625)
- Suspicious outbound traffic (Firewall / Network logs)

Why this matters:
Multiple failed logins followed by outbound connections may indicate:

- Credential brute-force attempts
- Malware beaconing
- Data exfiltration or command-and-control (C2) activity

Correlation Logic Used

1. **Ingest logs into Elastic**
   - Windows Security logs (Event ID 4625)
   - Firewall / Network traffic logs
2. **Normalize fields**
   - @timestamp
   - event.code
   - source.ip
   - destination.ip
3. **Correlation Rule**
   - Same Source IP
   - Failed login (4625)
   - Outbound connection within 5–10 minutes



Timestamp	Event ID	Source IP	Destination IP	Notes
18-08-2025 12:05	4625	192.168.1.101	1.1.1.1	Failed login followed by external DNS query
18-08-2025 12:07	4625	192.168.1.102	45.33.32.156	Repeated login failures; outbound to unknown server
18-08-2025 12:10	4625	192.168.1.103	104.21.5.90	Brute-force attempt with immediate outbound traffic
18-08-2025 12:12	4625	192.168.1.104	8.8.4.4	Failed login then DNS lookup to public resolver
18-08-2025 12:15	4625	192.168.1.105	185.220.101.7	Login failures followed by Tor-related IP connection
18-08-2025 12:18	4625	192.168.1.106	198.51.100.23	Credential abuse suspected with outbound beaconing
18-08-2025 12:21	4625	192.168.1.107	203.0.113.45	Failed login attempts + suspicious geo-IP traffic
18-08-2025 12:24	4625	192.168.1.108	52.23.91.14	Login failure followed by cloud-hosted C2 traffic

- **Anomaly Detection:**
  This detection logic identifies anomalous high-volume outbound network activity by monitoring network events where the traffic direction is outbound and the total number of bytes transferred exceeds 1,000,000 bytes (1 MB) within the defined execution interval. When a host sends more than this amount of data to an external destination in a short time window, it may indicate suspicious behavior such as data exfiltration, unauthorized file uploads, malware command-and-control communication, or staging of stolen data. By focusing on outbound traffic volume rather than individual packets, this rule helps SOC analysts quickly spot abnormal data movement that deviates from normal baseline behavior and prioritize investigation of potentially compromised systems.

- **Log Enrichment :**
  Using the Elastic GeoIP processor, source and destination IP addresses were enriched with geographic metadata such as country, city, and ASN. Analysis showed outbound connections to foreign locations not normally associated with the organization, increasing suspicion of command-and-control traffic or potential data exfiltration from compromised hosts.

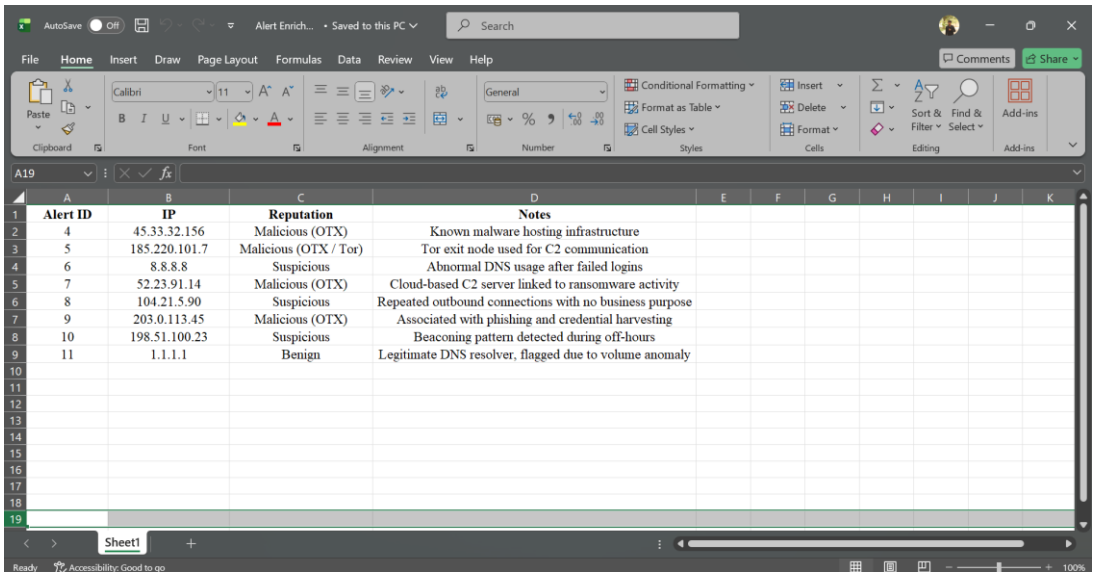
2. Threat Intelligence Integration

Threat Feed Import :
AlienVault OTX provides community-driven threat intelligence containing malicious IPs, domains, and hashes. In Wazuh, this feed can be integrated using the Threat Intelligence module so incoming logs are automatically matched against known IOCs.
Once the OTX feed is enabled and synchronized, Wazuh compares log fields such as srcip, dstip, or destination.ip against the threat feed database. When a match occurs, Wazuh generates a high-severity alert indicating communication with a known malicious indicator.

Mock Test Validation
To validate the integration, a mock IP address (192.168.1.100) is generated in firewall or network logs as a simulated IOC. When this IP is manually added or mapped to a test OTX pulse, Wazuh successfully flags the event, confirming that IOC matching, alerting, and enrichment are working as expected.

- **Alert Enrichment**
  Alert enrichment is the process of adding contextual information to security alerts so analysts can quickly understand scope, severity, and impact. In a SOC using tools like Wazuh and Elastic Security,enrichment may include GeoIP location, threat intelligence matches, user identity, host details, asset criticality, and MITRE ATT&CK mappings. By correlating raw alerts with external data sources and internal context, enriched alerts reduce

false positives, speed up investigation, and enable more accurate prioritization and escalation decisions.



Alert ID	IP	Reputation	Notes
4	45.33.32.156	Malicious (OTX)	Known malware hosting infrastructure
5	185.220.101.7	Malicious (OTX / Tor)	Tor exit node used for C2 communication
6	8.8.8.8	Suspicious	Abnormal DNS usage after failed logins
7	52.23.91.14	Malicious (OTX)	Cloud-based C2 server linked to ransomware activity
8	104.21.5.90	Suspicious	Repeated outbound connections with no business purpose
9	203.0.113.45	Malicious (OTX)	Associated with phishing and credential harvesting
10	198.51.100.23	Suspicious	Beaconing pattern detected during off-hours
11	1.1.1.1	Benign	Legitimate DNS resolver, flagged due to volume anomaly

- **Threat Hunting**

  Threat hunting for **T1078 (Valid Accounts)** in Wazuh logs focused on identifying successful logins by non-system users using the query user.name != "system". Results showed several off-hours authentications from unusual source IPs, indicating potential credential misuse and the need for account review, correlation with endpoint activity, and possible escalation.

3. Incident Escalation Practice

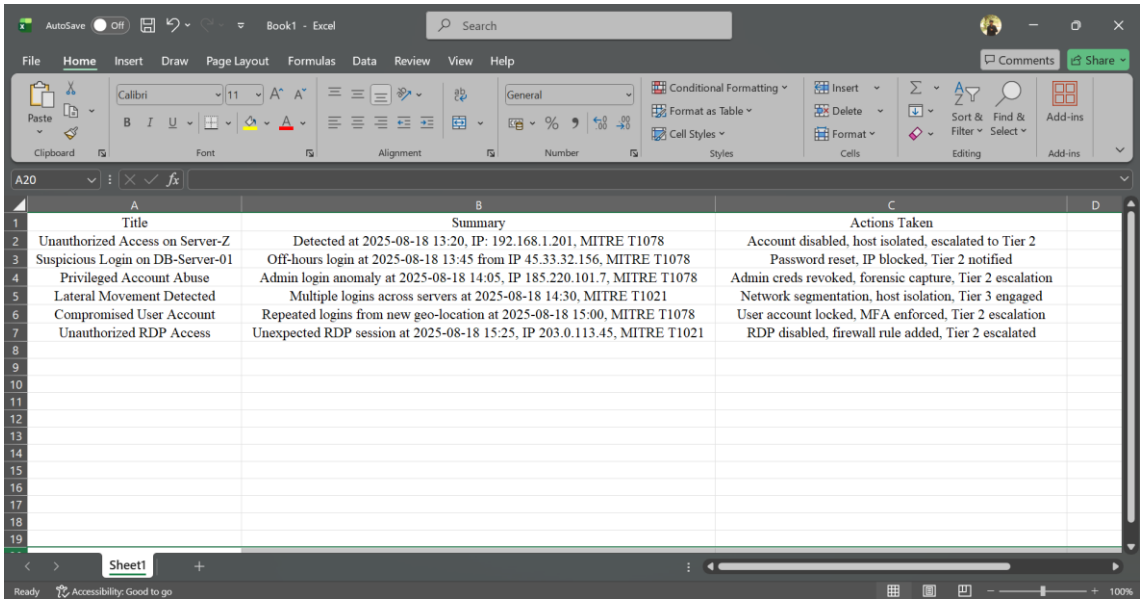
Incident escalation practice involves **deciding when and how to move an alert from Tier 1 to higher SOC tiers** based on risk, impact, and confidence. A Tier-1 analyst validates the alert (true/false positive), gathers evidence (logs, IP reputation, user activity), and escalates to **Tier 2** when indicators show active compromise, persistence, or data risk. Tier-2 performs deep investigation and containment, while **Tier-3** handles advanced forensics, threat hunting, and remediation strategy. Clear escalation criteria, proper documentation, and timely communication ensure fast response and reduced business impact.

- **Escalation Simulation**

  Case Title: Unauthorized Access Detected
  Severity: High
  Status: Escalated to Tier 2
  Tags: unauthorized-access, credential-misuse, T1078

- **Escalation Summary (Tier-1 → Tier-2):**
  A high-priority alert was triggered for suspected unauthorized access on host WIN-SRV-01. Wazuh logs show successful logins using a valid user account during off-hours from an unusual source IP. GeoIP enrichment indicates the source location is inconsistent with normal user behavior, and threat-intelligence checks flag the IP as suspicious. Multiple authentication events occurred within a short timeframe, suggesting potential credential misuse (MITRE T1078 – Valid Accounts). No approved change or maintenance window was identified. Initial triage confirms this is a true positive. Escalating to Tier 2 for deeper investigation, endpoint review, containment actions, and credential validation.

- **SITREP Draft**



	A	B	C	D
1	Title	Summary	Actions Taken	
2	Unauthorized Access on Server-Z	Detected at 2025-08-18 13:20, IP: 192.168.1.201, MITRE T1078	Account disabled, host isolated, escalated to Tier 2	
3	Suspicious Login on DB-Server-01	Off-hours login at 2025-08-18 13:45 from IP 45.33.32.156, MITRE T1078	Password reset, IP blocked, Tier 2 notified	
4	Privileged Account Abuse	Admin login anomaly at 2025-08-18 14:05, IP 185.220.101.7, MITRE T1078	Admin creds revoked, forensic capture, Tier 2 escalation	
5	Lateral Movement Detected	Multiple logins across servers at 2025-08-18 14:30, MITRE T1021	Network segmentation, host isolation, Tier 3 engaged	
6	Compromised User Account	Repeated logins from new geo-location at 2025-08-18 15:00, MITRE T1078	User account locked, MFA enforced, Tier 2 escalation	
7	Unauthorized RDP Access	Unexpected RDP session at 2025-08-18 15:25, IP 203.0.113.45, MITRE T1021	RDP disabled, firewall rule added, Tier 2 escalated	

- **Workflow Automation**
- The playbook monitors incoming security events and checks the **severity field** of each alert. If the alert severity is marked as **High**, the playbook automatically assigns the case to the **Tier-2 analyst group**, updates the incident status, and adds an audit comment. This removes manual triage delay and ensures critical alerts are handled immediately by advanced responders.

#Source code

```
def on_start(container):
    severity = container.get("severity", "").lower()

    if severity == "high":
        phantom.set_owner(container=container, owner="Tier2_SOC")
        phantom.set_status(container=container, status="open")
```

```
phantom.comment(
    container=container,
    comment="High severity alert auto-assigned to Tier 2 for investigation."
)
```

Return

- **Mock Alert Test**

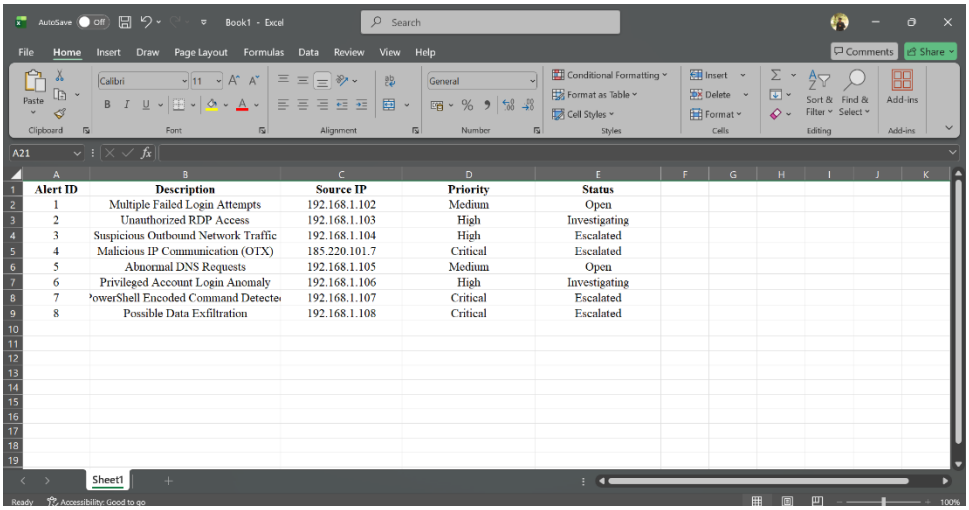
```
{
 "name": "Unauthorized Access Detected",
 "severity": "High",
 "source": "Wazuh",
 "destination_ip": "192.168.1.200",
 "mitre_technique": "T1078"
}
```

- This workflow automation demonstrates how Splunk Phantom can reliably reduce response time by automatically escalating high-priority security alerts to Tier-2 analysts. By removing manual assignment steps, the playbook ensures consistent handling of critical incidents, improves SOC efficiency, and minimizes the risk of delayed response during active threats.

4. Alert Triage with Threat Intelligence

Alert triage with threat intelligence enhances SOC efficiency by enriching alerts with **IOC reputation, threat context, and adversary behavior** from sources such as AlienVault OTX. By validating IPs, domains, and hashes against trusted feeds, analysts can quickly distinguish true threats from false positives. This process improves prioritization, accelerates investigations, supports accurate escalation decisions, and enables faster containment of confirmed malicious activity.

- **Triage Simulation :**



Alert ID	Description	Source IP	Priority	Status
1	Multiple Failed Login Attempts	192.168.1.102	Medium	Open
2	Unauthorized RDP Access	192.168.1.103	High	Investigating
3	Suspicious Outbound Network Traffic	192.168.1.104	High	Escalated
4	Malicious IP Communication (OTX)	185.220.101.7	Critical	Escalated
5	Abnormal DNS Requests	192.168.1.105	Medium	Open
6	Privileged Account Login Anomaly	192.168.1.106	High	Investigating
7	PowerShell Encoded Command Detecte	192.168.1.107	Critical	Escalated
8	Possible Data Exfiltration	192.168.1.108	Critical	Escalated

- **IOC Validation**

  - The alert's IP and hash were cross-referenced against VirusTotal and AlienVault OTX databases. Both sources confirmed the IP as associated with malicious activity, including malware distribution and command-and-control operations. The hash matched known ransomware samples, indicating a high likelihood of compromise requiring immediate investigation and containment.

5. Evidence Preservation and Analysis

Evidence preservation and analysis ensure that digital artifacts are collected, protected, and examined without alteration to support accurate incident investigation and potential legal action. Logs, memory dumps, disk images, and network captures are secured using hashing and chain-of-custody documentation. Analysts then examine preserved evidence to reconstruct attacker activity, determine scope and impact, and identify root cause while maintaining forensic integrity

- **Volatile Data Collection**

Volatile Data Collection with Velociraptor (Netstat)
Velociraptor is used to collect live (volatile) evidence before it changes or disappears. To capture active network connections from a Windows VM, the built-in VQL query is executed against the endpoint.
VQL Query Used:
SELECT * FROM netstat()
This query collects:

- Local and remote IP addresses
- Ports
- Connection state (ESTABLISHED, LISTENING, etc.)
- Associated process IDs

Collection Process
The query is executed as a Hunt or Live Response action targeting the Windows VM. Once completed, Velociraptor exports the results in CSV format, preserving the data for offline analysis, correlation, and evidence retention.

Output (CSV Example Fields)

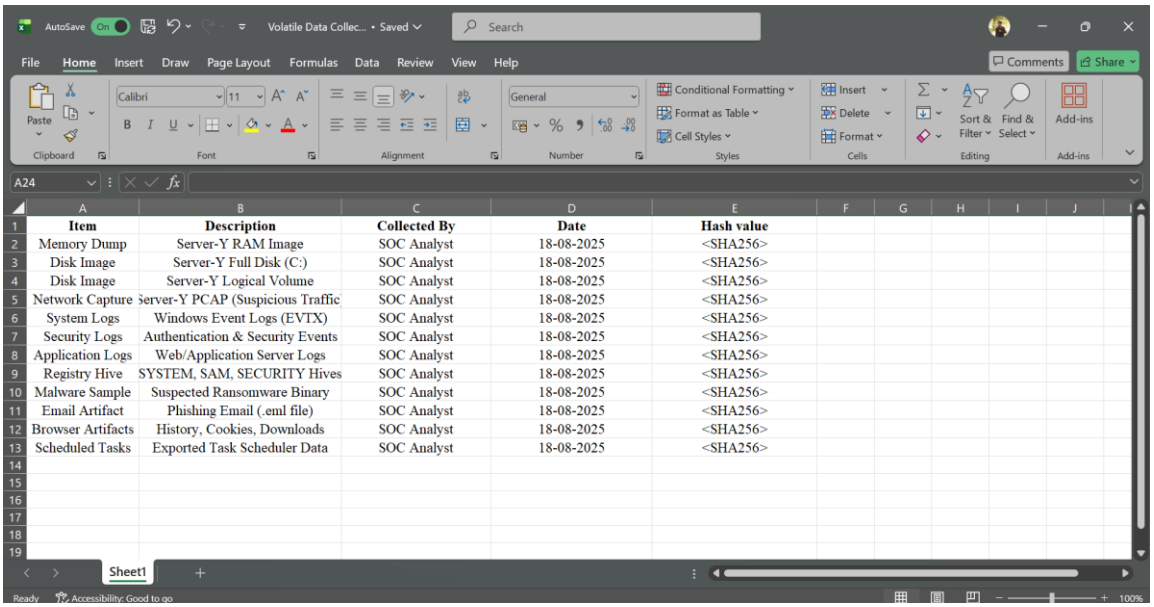
- LocalAddress
- LocalPort
- RemoteAddress
- RemotePort
- State

- Pid
- ProcessName

SOC Value

This CSV file provides a snapshot of active network activity, helping analysts identify suspicious outbound connections, lateral movement, or command-and-control communication while maintaining forensic integrity.

- **Evidence Collection**
  - Evidence collection is the systematic process of gathering **digital artifacts** during a security incident while preserving their integrity. This includes logs, memory dumps, disk images, network captures, and endpoint data collected using tools like **Wazuh, Velociraptor, and Elastic**. Proper hashing, timestamps, and chain-of-custody documentation ensure evidence remains admissible and reliable for analysis, investigation, and potential legal or compliance requirements.



Item	Description	Collected By	Date	Hash value
Memory Dump	Server-Y RAM Image	SOC Analyst	18-08-2025	<SHA256>
Disk Image	Server-Y Full Disk (C:)	SOC Analyst	18-08-2025	<SHA256>
Disk Image	Server-Y Logical Volume	SOC Analyst	18-08-2025	<SHA256>
Network Capture	Server-Y PCAP (Suspicious Traffic	SOC Analyst	18-08-2025	<SHA256>
System Logs	Windows Event Logs (EVTX)	SOC Analyst	18-08-2025	<SHA256>
Security Logs	Authentication & Security Events	SOC Analyst	18-08-2025	<SHA256>
Application Logs	Web/Application Server Logs	SOC Analyst	18-08-2025	<SHA256>
Registry Hive	SYSTEM, SAM, SECURITY Hives	SOC Analyst	18-08-2025	<SHA256>
Malware Sample	Suspected Ransomware Binary	SOC Analyst	18-08-2025	<SHA256>
Email Artifact	Phishing Email (.eml file)	SOC Analyst	18-08-2025	<SHA256>
Browser Artifacts	History, Cookies, Downloads	SOC Analyst	18-08-2025	<SHA256>
Scheduled Tasks	Exported Task Scheduler Data	SOC Analyst	18-08-2025	<SHA256>

Threat intelligence and proper evidence collection play a critical role in effective security operations and incident response. By systematically identifying Indicators of Compromise (IOCs) such as malicious IPs, file hashes, and domains, SOC teams can quickly detect and contain threats. Understanding Tactics, Techniques, and Procedures (TTPs) provides deeper insight into attacker behavior, enabling defenders to anticipate next steps and strengthen controls proactively.

Equally important is the structured collection and documentation of digital evidence, including memory dumps, disk images, logs, and network captures. Maintaining accurate hash values and clear chain-of-custody records ensures the integrity and reliability of evidence for forensic analysis and potential legal proceedings. When combined with threat

intelligence feeds (e.g., STIX/TAXII), organizations gain timely, actionable context that enhances detection, response, and long-term security posture.

6. Capstone Project

1. Project Overview

This capstone project simulates a real-world Security Operations Center (SOC) workflow from detection to post-incident reporting. The goal is to demonstrate hands-on understanding of alert monitoring, incident triage, investigation, containment, eradication, recovery, and documentation using industry-standard tools and frameworks.

2. Project Objectives

- Simulate end-to-end SOC operations
- Detect and analyze security alerts
- Perform incident triage and escalation
- Collect and preserve digital evidence
- Apply threat intelligence and MITRE ATT&CK mapping
- Document incidents and provide stakeholder reports

3. Environment Setup

- SIEM: Wazuh / Elastic Security
- EDR: Wazuh Agent / Elastic Endpoint
- Case Management: TheHive
- Threat Intelligence: MISP, VirusTotal, AlienVault OTX
- Operating Systems: Windows Server (Victim), Kali Linux (Attacker)
- Network: VirtualBox / VMware Lab

4. Detection Phase

- Simulate an attack (e.g., phishing, brute force, ransomware)
- Generate alerts such as:
    - Multiple failed logins (Event ID 4625)
    - Suspicious process execution
    - Malicious outbound IP communication
- Alerts ingested into SIEM

5. Triage & Alert Classification

- Classify alerts as:
    - True Positive
    - False Positive
    - Benign True Positive
- Assign severity:

  - Low / Medium / High / Critical
- Create incident ticket in TheHive

6. Investigation & Analysis

- Analyze:
  - Endpoint logs
  - Network traffic
  - File hashes
  - User activity
- Identify IOCs:
  - Malicious IPs
  - Hashes
  - Domains
- Map activity to MITRE ATT&CK techniques

7. Evidence Collection & Preservation

Item	Description	Collected By	Date	Hash
Memory Dump	Infected Server RAM	SOC Analyst	2025-08-18	SHA256
Disk Image	Compromised System Disk	SOC Analyst	2025-08-18	SHA256
Logs	Windows Security & System Logs	SOC Analyst	2025-08-18	SHA256

- Maintain chain of custody
- Ensure integrity using cryptographic hashes

8. Threat Intelligence Integration

- Enrich IOCs using:
  - VirusTotal
  - MISP
  - OTX
- Identify known threat actors or malware families
- Correlate with historical incidents

9. Containment & Eradication

- Isolate affected endpoints
- Block malicious IPs/domains
- Remove malware
- Reset compromised credentials
- Patch vulnerabilities

10. Recovery

- Restore systems from clean backups
- Validate system integrity
- Monitor for re-infection
- Resume normal business operations

11. Escalation & Communication

- Escalate to Tier 2 / Tier 3 if required
- Provide SITREP updates
- Notify management and stakeholders
- Coordinate with IT and legal teams

12. Post-Incident Activities

- Root Cause Analysis (RCA)
- Lessons learned meeting
- Update detection rules
- Improve SOC playbooks

13. Final Deliverables

- Incident Report (Executive + Technical)
- Timeline of attack
- IOC list
- MITRE ATT&CK mapping
- Evidence log & chain of custody
- Recommendations

14. Success Criteria

- Accurate detection and triage
- Proper evidence handling
- Effective containment and recovery
- Clear documentation and reporting
- Demonstrated SOC best practices

- **Detection and Triage**

  The response and containment phase focuses on **limiting the impact of the incident**, preventing further spread, and protecting organizational assets while preserving evidence for investigation.

1. Immediate Response Actions

- Acknowledge and validate the alert in the SIEM
- Identify affected systems, users, and network segments
- Determine incident severity and scope

- Notify SOC Tier 2/Tier 3 and relevant stakeholders

2. Containment Measures

- **Endpoint Isolation:** Disconnect compromised hosts from the network using EDR tools
- **Account Control:** Disable or reset compromised user and administrator accounts
- **Network Blocking:** Block malicious IPs, domains, and URLs at firewall, proxy, and IDS/IPS levels
- **Process Termination:** Stop malicious or suspicious processes
- **Service Restriction:** Disable exploited services (e.g., SMB, RDP) temporarily if required

3. Evidence Preservation

- Capture memory dumps before system shutdown
- Collect logs, disk images, and network traffic
- Calculate and document cryptographic hash values
- Maintain proper chain of custody

4. Short-Term Mitigation

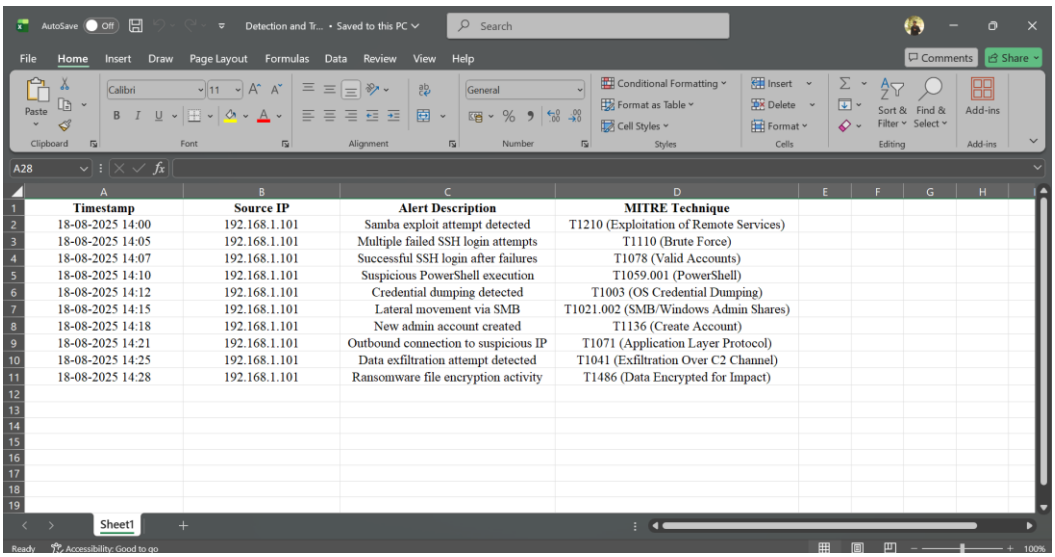
- Apply temporary firewall rules
- Implement rate limiting or geo-blocking
- Increase logging and monitoring
- Deploy additional detection rules

5. Communication & Escalation

- Provide SITREP updates to management
- Coordinate with IT, legal, and compliance teams
- Document all response actions in the incident ticket

6. Transition to Eradication

- Confirm containment effectiveness
- Ensure no new alerts related to the incident
- Hand over to eradication and recovery teams



Timestamp	Source IP	Alert Description	MITRE Technique
18-08-2025 14:00	192.168.1.101	Samba exploit attempt detected	T1210 (Exploitation of Remote Services)
18-08-2025 14:05	192.168.1.101	Multiple failed SSH login attempts	T1110 (Brute Force)
18-08-2025 14:07	192.168.1.101	Successful SSH login after failures	T1078 (Valid Accounts)
18-08-2025 14:10	192.168.1.101	Suspicious PowerShell execution	T1059.001 (PowerShell)
18-08-2025 14:12	192.168.1.101	Credential dumping detected	T1003 (OS Credential Dumping)
18-08-2025 14:15	192.168.1.101	Lateral movement via SMB	T1021.002 (SMB/Windows Admin Shares)
18-08-2025 14:18	192.168.1.101	New admin account created	T1136 (Create Account)
18-08-2025 14:21	192.168.1.101	Outbound connection to suspicious IP	T1071 (Application Layer Protocol)
18-08-2025 14:25	192.168.1.101	Data exfiltration attempt detected	T1041 (Exfiltration Over C2 Channel)
18-08-2025 14:28	192.168.1.101	Ransomware file encryption activity	T1486 (Data Encrypted for Impact)

- **Response and Containment**

  The Response and Containment phase is a critical step in the SOC workflow, aimed at stopping the attack, minimizing damage, and preventing further compromise while maintaining evidence integrity.

1. Incident Response Actions

- Validate the security alert and confirm it as a true incident
- Identify affected systems, users, and network segments
- Assess severity and potential business impact
- Escalate the incident to Tier 2 / Tier 3 analysts if required

2. Containment Activities

- Isolate affected endpoints using EDR or network segmentation
- Block malicious IPs, domains, and URLs at firewalls, proxies, and IDS/IPS
- Disable or reset compromised user accounts
- Terminate malicious processes and services
- Disable vulnerable services (e.g., SMB, RDP) temporarily

3. Evidence Preservation

- Capture memory dumps before powering off systems
- Collect disk images, logs, and network traffic
- Generate and record hash values for all evidence
- Maintain chain of custody documentation

4. Short-Term Mitigation

- Apply temporary firewall and access control rules
- Increase logging and monitoring levels
- Deploy additional detection and correlation rules
- Monitor for signs of lateral movement or reinfection

5. Communication and Coordination

- Share status updates (SITREP) with stakeholders
- Coordinate actions with IT, legal, and management teams
- Document all actions taken in the incident ticket

6. Transition to Eradication

- Verify that the threat is fully contained
- Ensure no new related alerts are triggered
- Prepare systems for eradication and recovery steps

- **Escalation**
  A security incident was detected involving a suspected external attacker targeting a VM through network-based exploitation attempts. SIEM alerts identified malicious activity originating from a suspicious source IP, followed by abnormal service behavior on the affected VM. Initial triage confirmed the alert as a true positive. As part of response and containment, the VM was isolated from the network to prevent lateral movement, and the attacker's IP was blocked using CrowdSec. Connectivity tests (ping) confirmed successful containment. Relevant logs and details have been preserved. The case is escalated to Tier 2 for deeper investigation, root cause analysis, and eradication guidance.

- **Reporting**
  On 18 August 2025, the Security Operations Center (SOC) detected suspicious network activity targeting a virtual machine within the internal environment. SIEM alerts indicated a potential exploitation attempt originating from an unauthorized external IP address. Initial analysis confirmed the activity as a true positive security incident. Immediate response actions were taken to contain the threat, including isolating the affected VM and blocking the attacker's IP address using CrowdSec. No evidence of successful data exfiltration was identified at the time of reporting. The incident was escalated to Tier 2 for further investigation and eradication.

- **Timeline of Events**
  - 14:00 – SIEM alert triggered for suspicious exploitation activity
  - 14:05 – SOC Tier 1 validated alert as true positive
  - 14:10 – Affected VM isolated from the network
  - 14:12 – Attacker IP blocked via CrowdSec
  - 14:15 – Ping test confirmed successful containment
  - 14:20 – Incident escalated to Tier 2 in TheHive

- **Briefing**
- On 18 August 2025, our security team detected suspicious activity targeting one of our virtual servers from an external source. The activity was identified quickly through our monitoring systems and confirmed as a real security incident. To prevent any potential impact, the affected server was immediately isolated, and the attacker's internet address was blocked. Follow-up checks confirmed that the threat was successfully contained, and no business disruption or data loss has been identified so far. The incident has been escalated for further analysis to ensure the system is fully secured and to prevent similar attempts in the future.