Title: Advanced Log Analysis, Threat Intelligence Integration and Incident

Submitted By: Anjali Shetty

Report Overview:

This report provides a structured overview of Security Operations Center (SOC) activities combining theoretical knowledge with practical application. It covers core security operations center concepts such as advanced log analysis threat intelligence integration and incident escalation workflows followed by hands-on exercises using industry-standard tools.

The theoretical part explains the principles necessary to understand the detection analysis and escalation of security incidents. The hands-on section demonstrates real-world application through log correlation threat hunting alert classification evidence preservation and full SOC workflow simulation.

Overall, this report aims to improve conceptual understanding and practical skills reflecting the responsibilities of real-world security operations center analysts and incident response operations.

Theoretical Knowledge

1. Advanced Log Analysis

Overview

Advanced log analysis is an important Security Operations Center (SOC) skill used to detect, investigate, and respond to security incidents by analyzing logs generated from multiple systems such as firewalls, servers, endpoints, applications, and cloud services. Effective log analysis helps uncover hidden attack patterns and reduce false positives.

Core Concepts

1] Log Correlation

Log correlation involves combining logs from different sources and analyzing them to identify relationships that may indicate malicious activity.

Example:

- Multiple failed login attempts recorded in Windows security logs (Event ID 4625)
- Followed by successful login (event ID 4624)
- Then suspicious outgoing traffic is detected in the firewall or proxy logs

Correlating these events helps identify brute force attacks or credential attacks.

2] Anomaly Detection

Anomaly detection focuses on identifying deviations from normal behavior.

Common anomalies include:

- Logins outside normal business hours
- Logins from unusual geographic locations
- Sudden spikes in data transfer volume
- Unusual process execution or privilege escalation

Detection methods include:

- Rule-based detection (thresholds, known patterns)
- Statistical analysis (baseline vs deviation)

3] Log Enrichment

Log enrichment adds additional context to raw logs to make analysis more efficient.

Examples of enrichment:

- IP address - Geolocation ISP Reputation Score
- Username - Role Department Privilege Level
- Hash - Malware reputation from threat information feeds

Enrichment improves analyst decision-making and alert accuracy.

Key Objectives

- Correlate logs from multiple sources to detect complex attacks
- Fast and accurate identification of anomalies
- Reducing false positives with context-aware analysis

How to Learn

- Studying log analysis techniques from the SANS reading room (e.g. efficient log analysis)
- Explore the Elastic documentation (ELK Stack) about correlation and anomaly detection
- Review real-life case studies such as the Equifax breach through CISA reports

2. Threat Intelligence Integration

Overview

Threat Intelligence Integration improves Security Operations Center (SOC) detection and response by using external and internal intelligence to identify known threats and predict attacker behavior.

Core Concepts

1] Types of intelligence threats

Indicators of Compromise (IOCs):

- Malicious IP addresses
- File hashes
- Domains and URLs

Tactics Techniques and Procedures (TTPs):

- Attacker Behavior and Techniques (Mapped with MITER ATT&CK)

Threat summaries:

- Structured intelligence has been shared through formats such as STIX/TAXII

2] Integration in SOC Operations

Threat intelligence is integrated into SIEM platforms to automatically enrich alerts.

Examples:

- The SIEM detects traffic from a suspicious IP address
- The threat intelligence feed identifies this server as a known command and control server (C2).
- The severity of the alarm is automatically increased

3] Threat Hunting Using Intelligence

Threat intelligence supports proactive threat hunting.

Examples:

- Search for MITER ATT&CK T1078 Technology (valid accounts)
- Search the logs for unusual login patterns or credential abuse

Key Objectives

- Increase detection accuracy with real-world threat data
- Enable proactive threat scanning
- Improving SOC responsiveness

How to Learn

- Explore the MITER ATT&CK framework and its use in SOC processes
- Study STIX/TAXII standards with OASIS Cyber Threat Intelligence
- Review AlienVault OTX for examples of real-world threat intelligence

3. Incident Escalation Workflows

Overview

Incident escalation workflows define how security incidents are managed, investigated and reported at the Security Operations Center (SOC) and stakeholder levels.

Core Concepts

1] SOC Escalation Tiers

- Tier 1 (Triage): Initial alert review, validation, and basic investigation
- Tier 2 (Investigation): In-depth analysis, log correlation, and isolation procedures
- Tier 3 (advanced analysis): Threat analysis, malware analysis, and root cause analysis

Escalation depends on its severity, impact and complexity.

2] Communication Protocols

Clear communication is essential during escalation.

Common methods:

- SITREP (Situation Report)
- Summary reports of events
- Stakeholder briefings

Reports typically include:

- Description of the event
- Impact assessment
- Measures taken
- Recommended next steps

3] Automation in Escalation

SOAR (Security, Orchestration, Automation and Response) tools automate repetitive tasks.

Examples:

- Automatically create and assign tickets

- Augment the alert with threat information
- Notify SOC teams and management

Key Objectives

- Escalate incidents efficiently and accurately
- Maintaining clear communication with stakeholders
- Improve response time with automation

How to Learn

- Incident Management Workflow Study in NIST SP 800-61
- Review the SANS Incident Handler Guide for escalation templates
- Explore Splunk's SOAR documentation to understand automation concepts

Practical Application

1. Advanced Log Analysis

1.1] Log Correlation

Log correlation was performed by analyzing Windows security logs within Elastic Security. Unsuccessful login attempts were identified with event ID 4625. Multiple failed authentication events from the same host within a short period of time were linked using timestamps and event metadata. This pattern may indicate unauthorized access attempts or brute force activity.

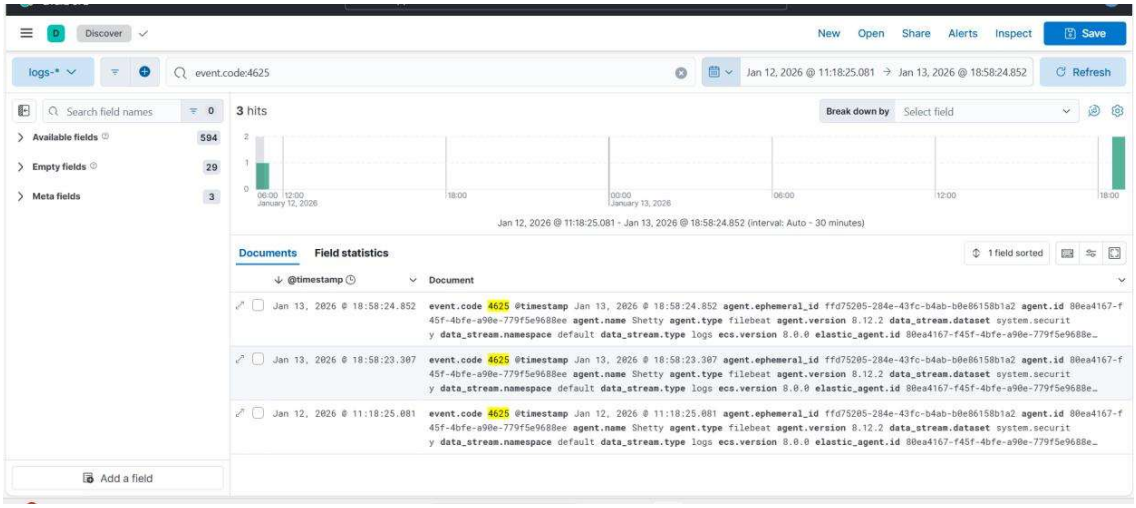

Figure 1: Correlated failed login attempts (Event ID 4625) observed in Elastic Discover

Documentation Table

Since only authentication logs were ingested, correlation was limited to login activity.

Timestamp	Event ID	Source Host	Notes
Jan 13, 2026	4625	Windows-VM	Multiple failed login attempts

1.2] Anomaly Detection

An anomaly detection rule has been created in Elastic Security to detect large outbound data transfers. The rule is set to be activated when the data transfer exceeds a predetermined limit within a short period of time. Successful execution of the rule confirms that resilience can detect anomalous traffic patterns.

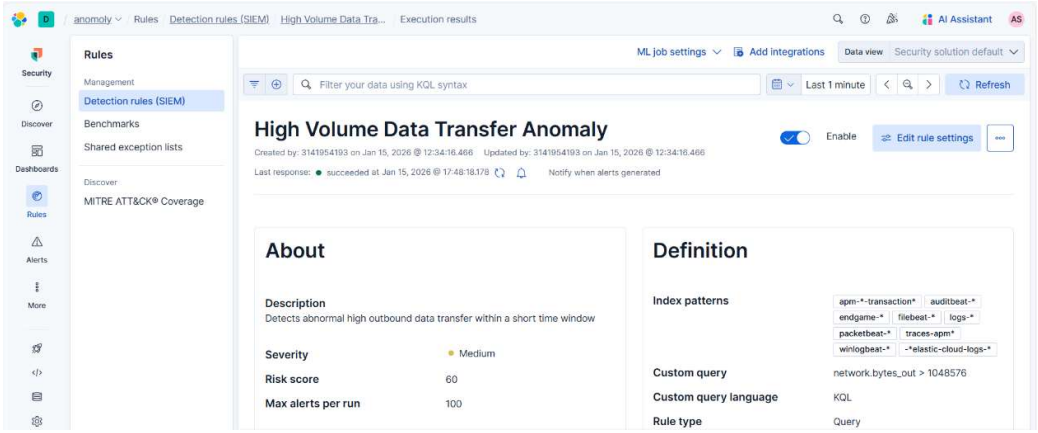

Figure 2: Configuration of high-volume data transfer anomaly detection rule

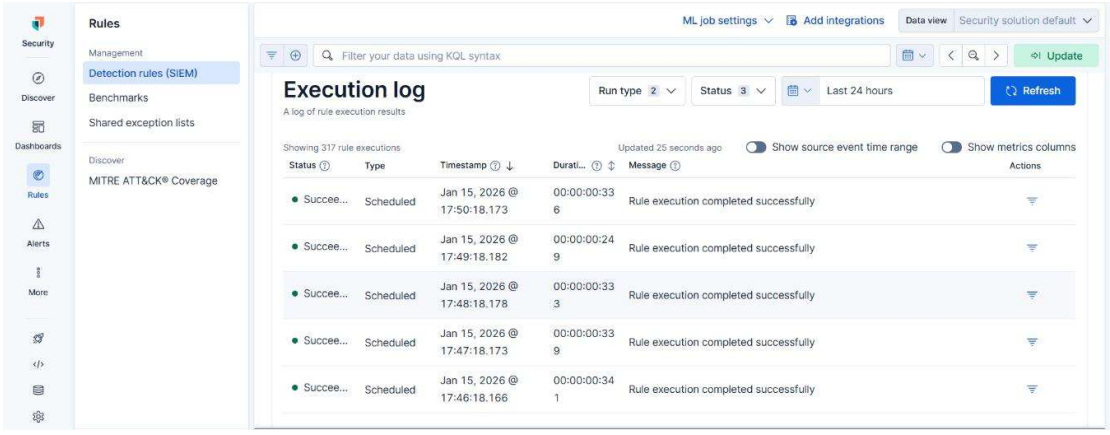

Figure 3: Successful execution of anomaly detection rule

1.3] Log Enrichment

Log enrichment was done using Elastic's built-in metadata fields such as hostname, agent details, timestamps and event categories. These rich attributes provide additional context to security events enabling analysts to better understand the source and nature of suspicious activity and improve investigative effectiveness.

Outbound traffic logs were not available; correlation was limited to authentication events only.

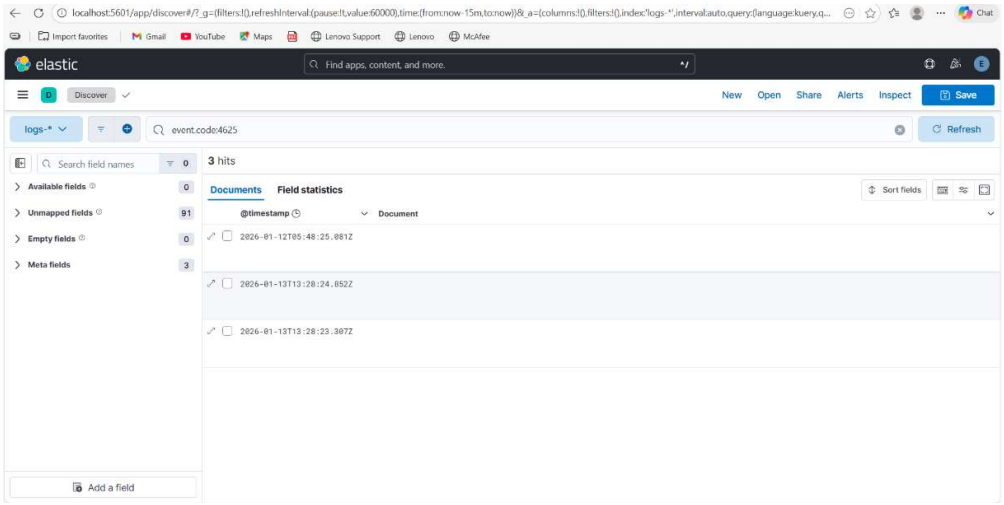

Figure 4: Enriched log data with host and agent metadata

2. Threat Intelligence Integration

2.1] Threat Feed & IOC Enrichment

Threat intelligence enrichment was performed using AlienVault OTX to analyze External Indicators of Compromise (IOC). The IP address model (8.8.8.8) was chosen to demonstrate IOC validation and enrichment.

The IP address was first looked up in Wazuh logs to check if it was observed in the monitored environment. We found no matching events or alarms in Wazuh, indicating that the IOC was not present in internal telemetry during the analysis period.

The IP address was then analyzed using AlienVault OTX, that classified it as suspicious based on previous telemetry, high DNA resolution activity, and association with multiple domains.

It describes the Security Operations Center (SOC) workflow for connecting external threat information with internal security logs.

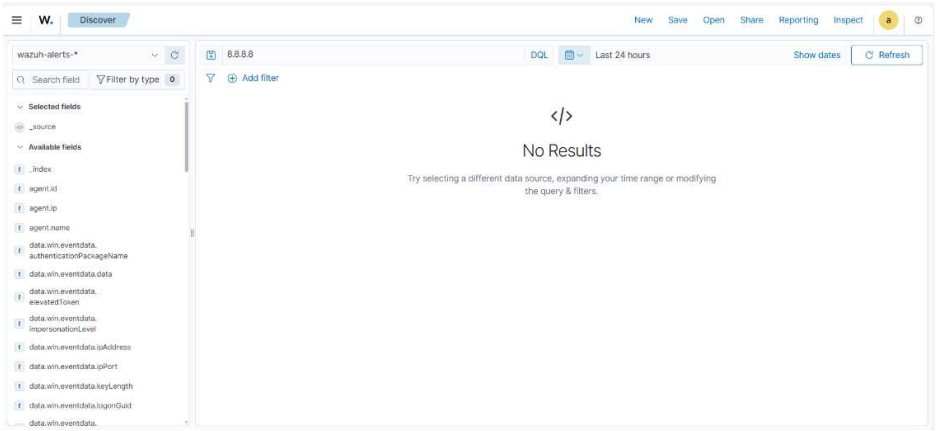

Figure 5: Wazuh Discover view showing no matching events for IOC IP address 8.8.8.8, confirming the IP was not observed in internal logs.

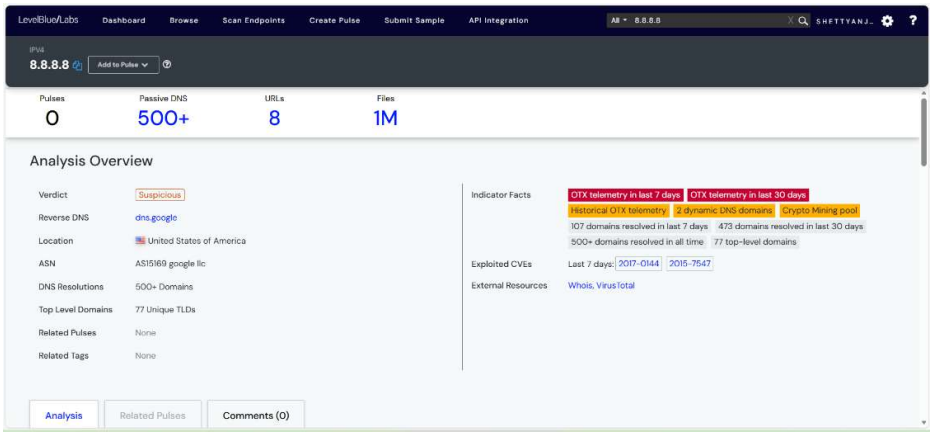

Figure 6: AlienVault OTX Intelligence Report showing historical reputation and threat data for IP address 8.8.8.8.

2.2] Alert Enrichment Summary

Although no active Wazuh alert was generated for the analyzed IP address the enrichment results were documented to demonstrate validation of the threat information. AlienVault OTX external threat intelligence was used to assess IP reputation and correlate with internal log visibility.

Alert Enrichment Table:

Alert ID	IP	Reputation	Notes
003	8.8.8.8	Suspicious (OTX)	IP not observed in Wazuh logs; Validated via OTX

2.3] Threat Hunting - MITRE ATT&CK T1078 (Valid Accounts)

A threat hunt was conducted in Wazuh to detect activity related to MITER ATT&CK T1078 technology (valid accounts). Windows security logs were analyzed to identify successful authentication events generated by external user accounts.

The analysis focused on Event ID 4624 to detect legitimate or suspicious use of the account.

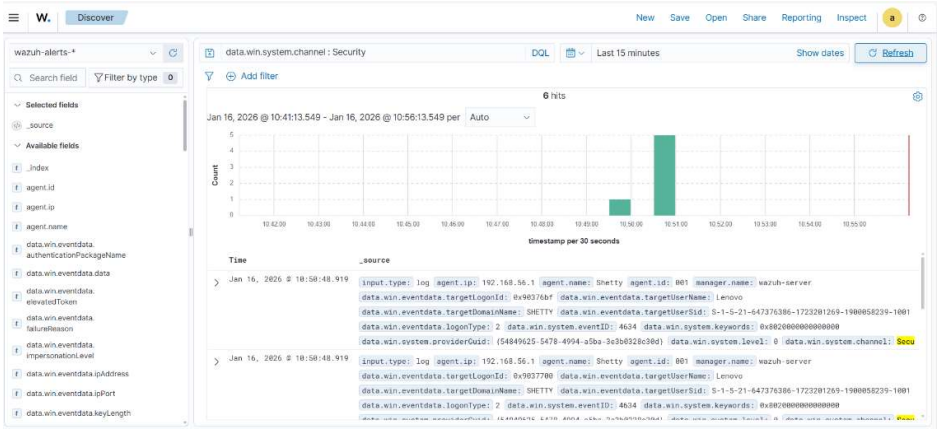

Figure 7: Windows Security log details analyzed in Wazuh to review user authentication activity during threat hunting.

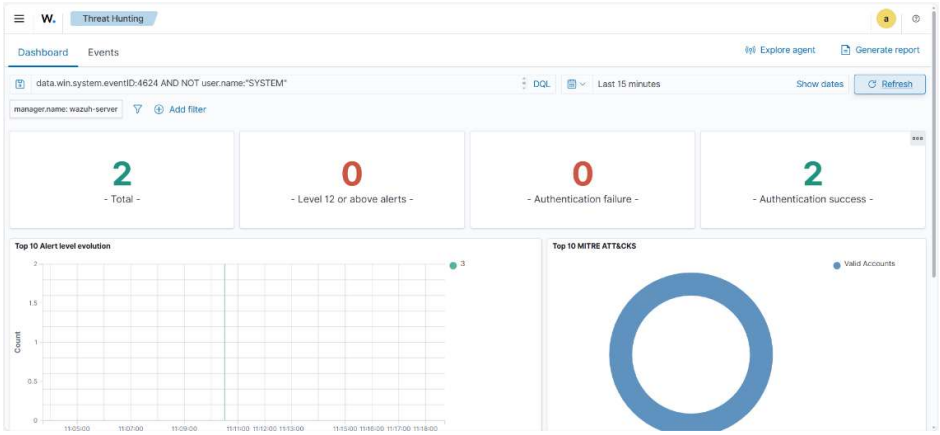

Figure 8: Wazuh Threat Hunting dashboard displaying authentication-related log activity used to investigate MITRE ATT&CK T1078 (Valid Accounts).

2.4] Incident Case Management (TheHive)

TheHive was used for incident documentation and case management.

Created a manual case to record threat hunting results and enrich threat information. Status includes details of analyzed IP address MITER ATT&CK mapping and AlienVault OTX findings. This demonstrates the proper workflow of the Security Operations Center (SOC) by monitoring security scans even when no confirmed attack has been detected.

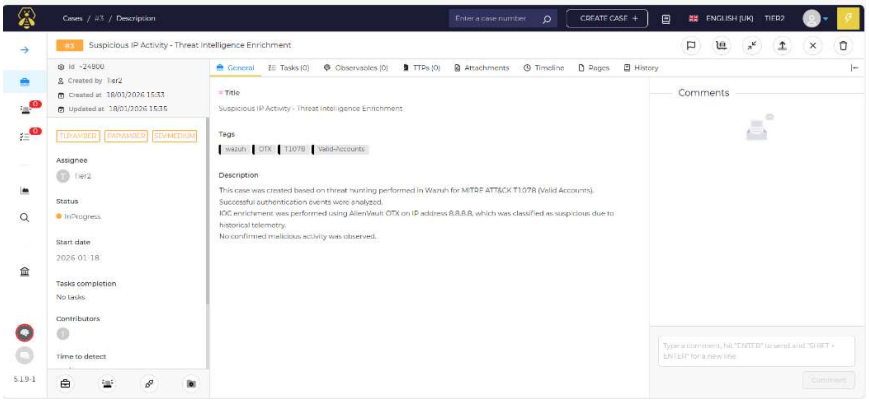

Figure 9: Manual incident case created in TheHive to document threat hunting and threat intelligence enrichment findings.

2.5] Threat Hunting Summary

MITER ATT&CK T1078 threat scan identified failed non-system authentication events in Windows security logs. No unusual login behavior was observed during the analysis. Enrichment of threat intelligence confirmed that the analyzed IOC was not present in internal records, demonstrating effective control of external indicators.

3. Incident Escalation Practice

3.1] Incident Overview

During routine security monitoring a high-priority alert representing unauthorized access on server Y was simulated. A case is created in TheHive to document and manage the incident. The alert contained suspicious access from the IP address 192.168.1.200 indicating possible compromise of credentials assigned to the MITER ATT&CK T1078 technology (valid accounts). The incident was classified as extremely serious to reflect its potential impact.

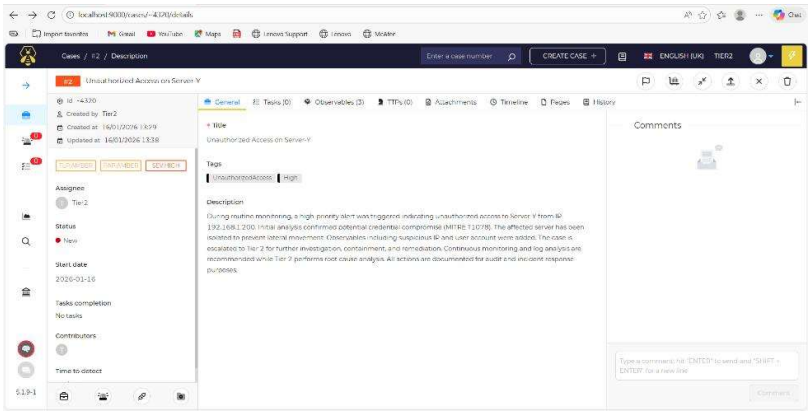

Figure 10: High-severity unauthorized access incident created in TheHive for Server-Y.

3.2] Incident Triage and Observables

As part of the initial screening, case notes are attached to support investigation and escalation. These observations included a suspicious IP address (192.168.1.200), a potentially compromised user account, and a suspicious file (malware.exe). The addition of observable data enables structured analysis, correlation, and future enrichment for Level 2 analysts.

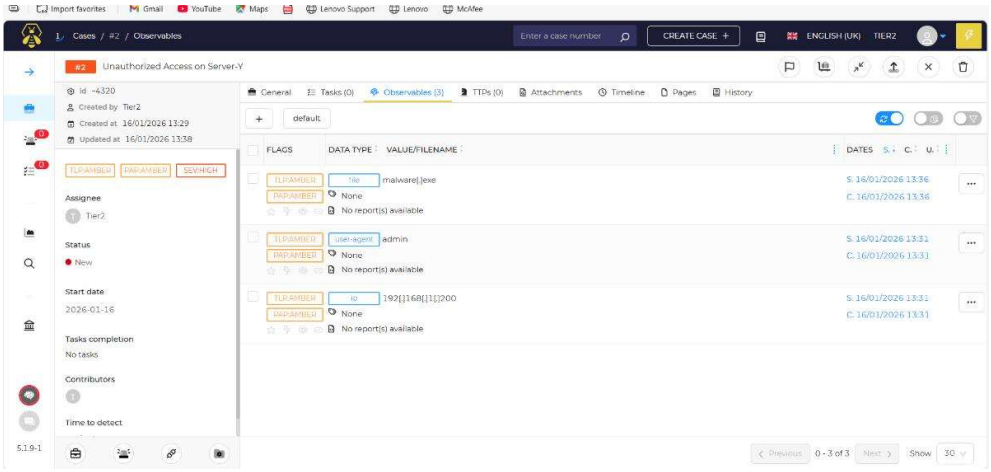

Figure 11: Observables added to the case, including suspicious IP address, user account, and file artifact.

3.3] Incident Escalation to Tier 2

After the initial analysis and documentation was completed, the incident was escalated to Tier 2 for further investigation and response. A detailed escalation summary has been added to the case notes detailing the detection method the devices involved specific indicators and immediate containment measures. Escalation ensures advanced analysts can perform advanced analysis such as root cause identification and remediation planning.

3.4] Situation Report (SITREP)

Incident name:

Unauthorized Access on Server-Y

Severity:

High

Summary:

Unauthorized access activity has been detected on server Y from IP address 192.168.1.200. Initial investigation indicates possible misuse of valid credentials in accordance with MITER ATT&CK T1078. The incident was documented in TheHive, relevant comments were added, and the incident was elevated to Tier 2 for further investigation and closure.

Actions taken:

- A high severity incident state has been created in TheHive
- Observables added (IP address, user account, suspicious file)
- The incident was raised to Tier 2 with a documented summary

3.5] Splunk Phantom Playbook

Splunk Phantom playbook automation was not performed as part of this exercise. However, the escalation process was performed manually within TheHive to demonstrate understanding of the SOC workflow. Automation using SOAR tools such as Splunk Phantom can be integrated into real-world environments to reduce response time and simplify incident management.

4. Alert Triage with Threat Intelligence

4.1] Wazuh Investigation

The Wazuh Discover scan searched for PowerShell-related events within the wazuh-alerts-* index. No matching results were found within the specified time range. This indicates that no suspicious PowerShell activity is actually occurring on the monitored endpoint. The lack of records confirms that the alert is a simulated scenario of a triage exercise.

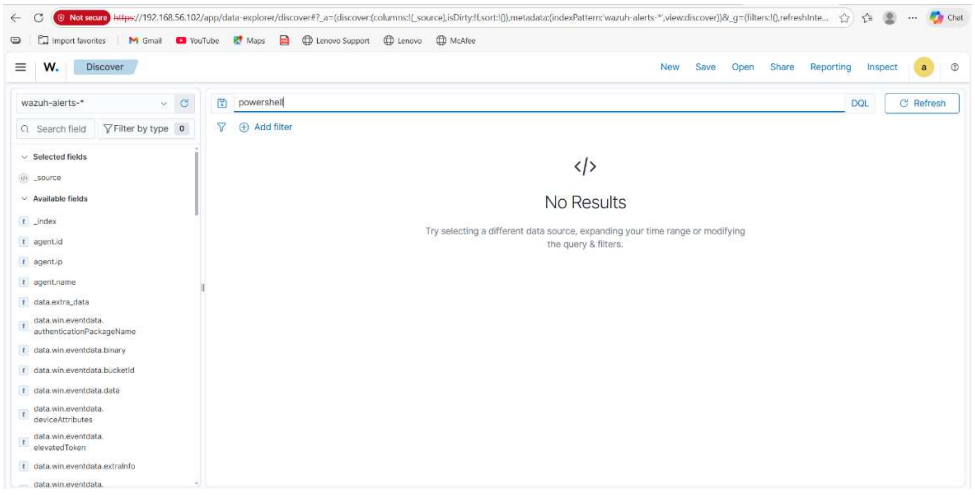

Figure 12: Wazuh Discover showing no PowerShell-related alerts, confirming absence of suspicious PowerShell activity.

4.2] IOC Identification

The IOC selected for validation is the IP address 192.168.56.102. This IP address belongs to the private IP address range (RFC 1918), that is typically used on internal networks and is not directly accessible from the public Internet.

4.3] VirusTotal Analysis

VirusTotal's analysis of the IP address 192.168.56.102 did not detect any security providers with a combined score of 0/93. The IP address is classified as private that indicates that it has no public threat reputation. No malicious activity has been linked to this IOC.

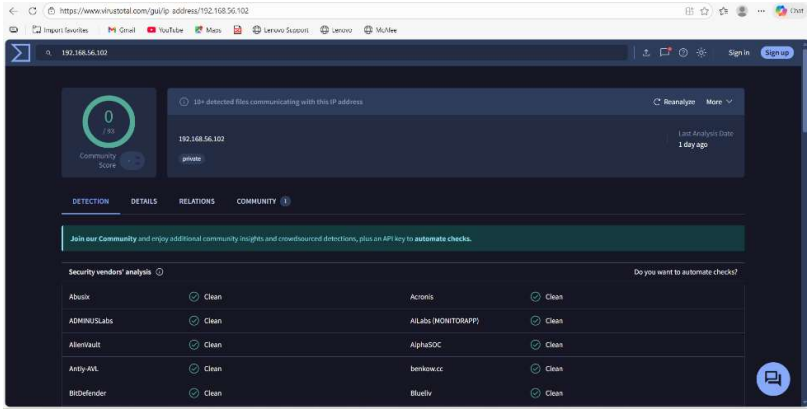

Figure 13: VirusTotal analysis indicating no detections for IP address 192.168.56.102 and classification as a private IP.

4.4] AlienVault OTX Analysis

An AlienVault OTX search returned pulse references for the IP address 192.168.56.102. However further analysis shows that this IP address is part of a private network domain. Impulse links appear to be contextual or related to a dataset and don't demonstrate confirmed malicious activity. No active threats or hostile associations have been identified.

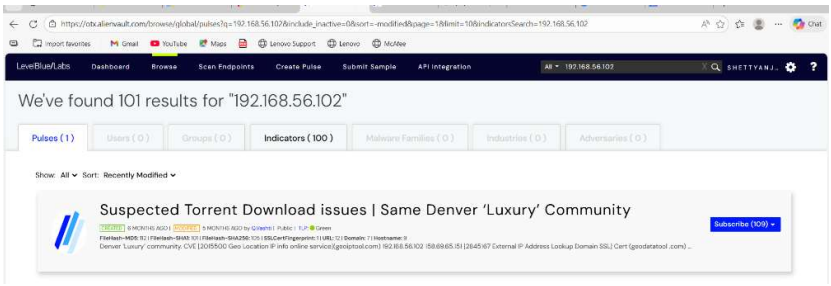

Figure 14: AlienVault OTX search results showing contextual pulse references without confirmed malicious activity.

5. Evidence Preservation and Analysis

5.1] Volatile Network Data Collection (Netstat)

Using Velociraptor the Windows.Network.Netstat tool was implemented on a Windows client to gather active network connections. This artifact retrieves current TCP/UDP connections listening ports and associated processes. The search process was created and scheduled successfully but no active network connection was returned during execution that is acceptable in a clean or passive system.

The results were exported and saved in CSV format for forensic documentation and future analysis.

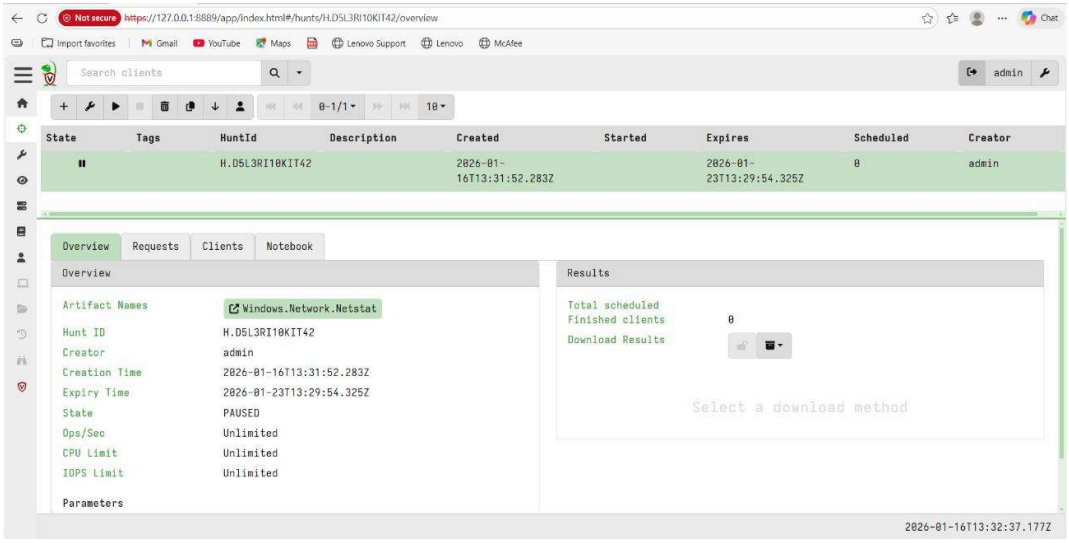

Figure 15: Velociraptor hunt showing execution of Windows.Network.Netstat artifact for collecting active network connections.

5.2] Physical Memory Acquisition

To preserve volatile memory libraries, the Windows.Memory.Acquisition tool is implemented by Velociraptor.

This tool collected a physical memory dump file (PhysicalMemory.dd) from Windows. The search process has completed successfully and the memory image has been downloaded for offline forensic analysis.

Obtaining physical memory is crucial because it can contain running processes, network artifacts, credentials, and traces of malware that cannot be accessed on disk.

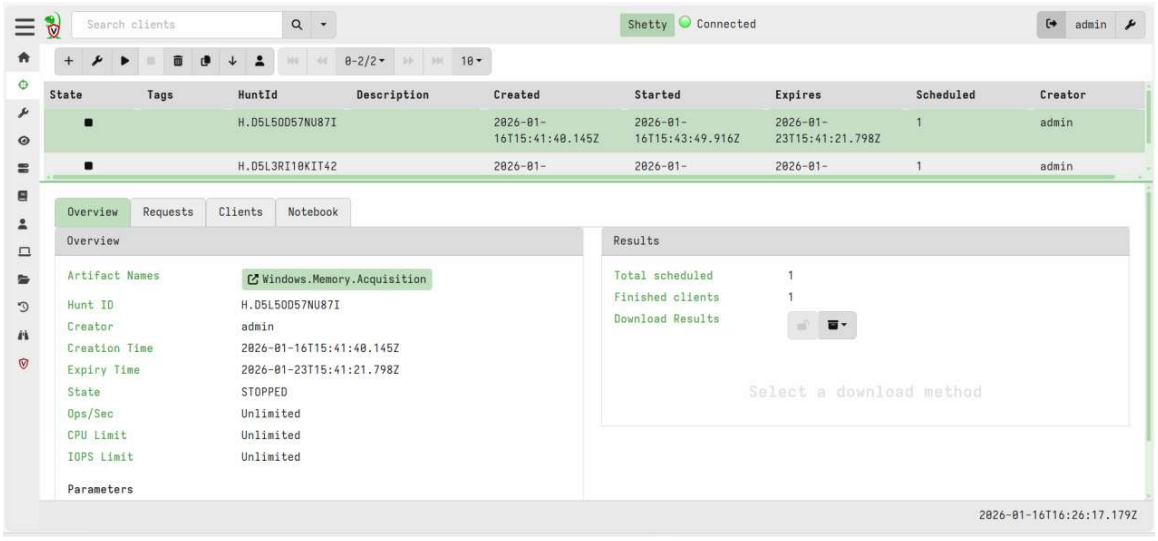

Figure 16: Velociraptor hunt overview showing successful execution of Windows.Memory.Acquisition artifact.

5.3] Evidence Integrity Verification (SHA-256 Hashing)

After the memory dump file was downloaded, PowerShell was used to calculate the file's SHA-256 HASH using the Get-FileHash command.

The hash is generated twice and matched both times, ensuring that the memory image does not change after translation. This ensures the integrity of evidence and supports chain of custody requirements.

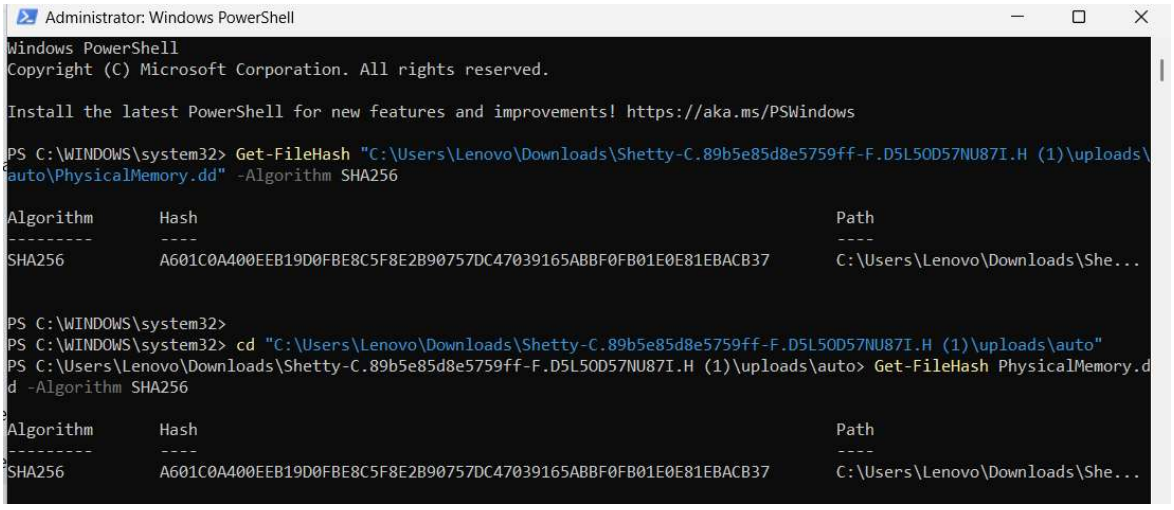

Figure 17: SHA-256 hash calculation of the physical memory dump using PowerShell to verify evidence integrity.

Evidence Documentation Table

Item	Description	Collected By	Date	Hash Value (SHA-256)
Memory Dump	PhysicalMemory.dd (VM)	SOC Analyst	2026-01-16	A601C0A400EEB19D0FBE8C5F8E2B90757DC47039165ABBF0FB01E0E81EBACB37

6. Capstone Project: Full SOC Workflow Simulation

6.1] Environment & Endpoint Status

The Wazuh dashboard is first reviewed to ensure that the endpoint is active and properly connected to the Wazuh Manager. This ensures that security logs and events are collected during the attack simulation.

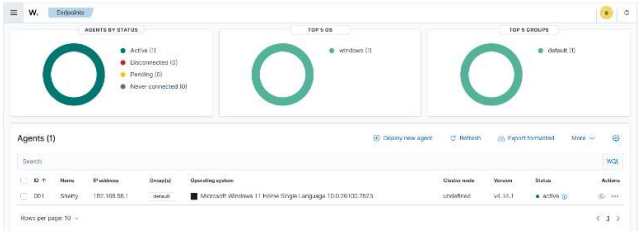

Figure 18: Wazuh dashboard showing the endpoint in active status before the attack simulation.

6.2] Attack Simulation

An attack was simulated from a Kali Linux machine exploiting the Samba usermap_script vulnerability on a Metasploitable2 system using Metasploit. This vulnerability successfully opens a reverse shell confirming unauthorized remote access to the target system.

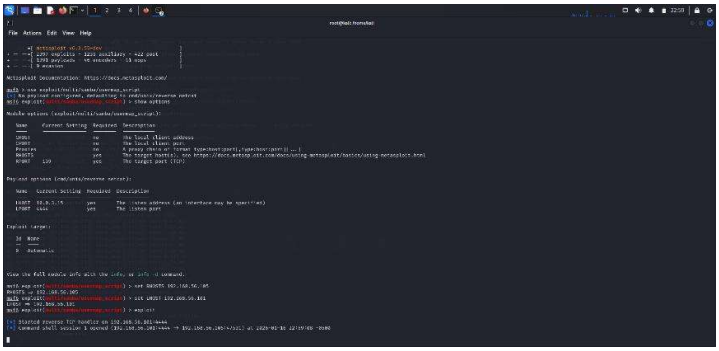

Figure 19: Metasploit exploitation of the Samba usermap_script vulnerability from Kali Linux.

6.3] Detection & Log Review

Following the attack, Wazuh's files were reviewed by the Discovery Division. The Agent Name field confirmed that the logs came from the monitored endpoint. No live Samba exploit alerts were generated; However, system and authentication logs were available for investigation during the attack.

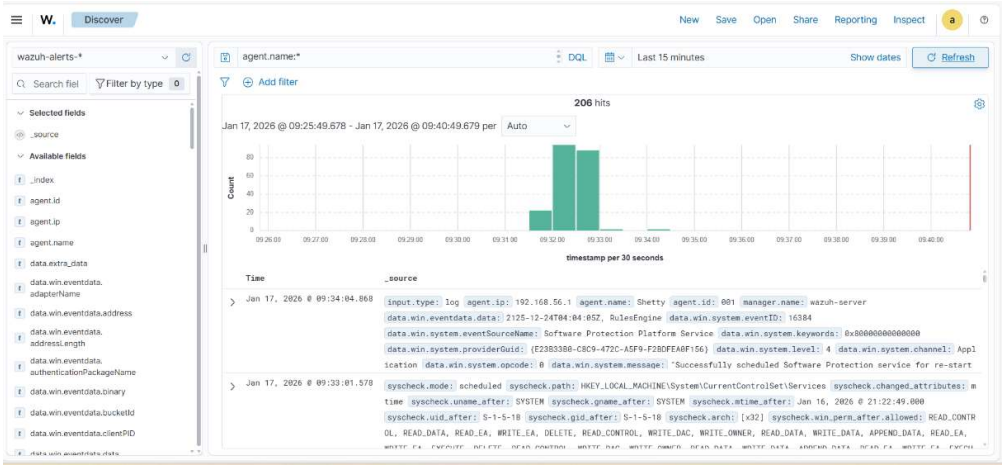

Figure 20: Wazuh Discover view showing logs collected from the agent during the attack period.

6.4] Authentication Rules Review

Reviewed the detection rules for Wazuh authentication to understand how failed or suspicious login attempts are detected. This step helped verify that Wazuh enabled the relevant rules although no high-risk authentication alerts were received during the attack.

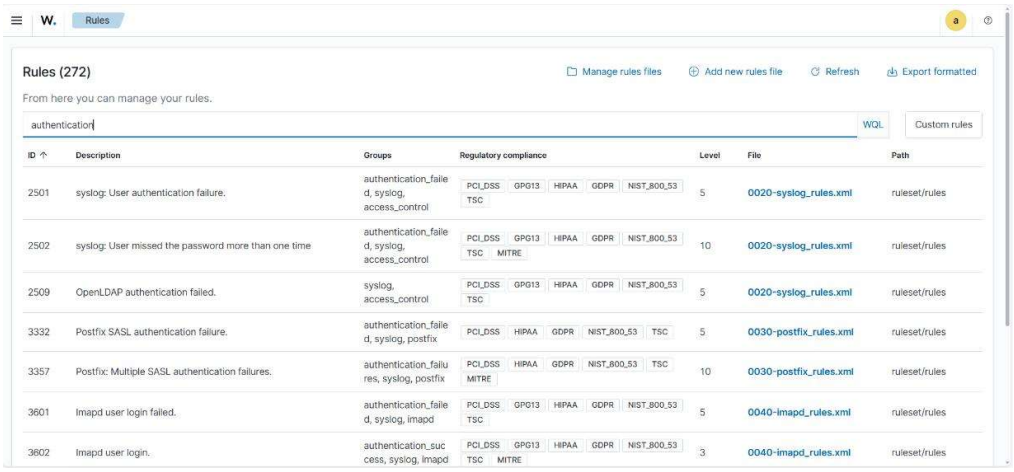

Figure 21: Wazuh authentication-related rules reviewed during alert triage.

6.5] Response & Containment

Blocking Action

As an immediate defensive measure, the attacker's IP address was manually blocked using CrowdSec by adding a ban decision. This measure was taken to prevent further malicious access to the attacker's system.

Block Verification

The CrowdSec decisions list was checked to verify that the attacker IP was successfully banned and that the blocking action was active.

Figure 22: CrowdSec command used to manually block the attacker IP address and decisions list confirming the attacker IP is blocked.

Enforcement Confirmation

The CrowdSec service status was reviewed to confirm that the CrowdSec agent was running and actively enforcing the blocking decision against the attacker IP.

Figure 23: CrowdSec service status on the Kali Linux system confirming active enforcement of the attacker IP ban.

6.6] Escalation - TheHive Case Management

After the containment, the incident was escalated to Tier 2 using TheHive case management platform. A new case is created to document the details of the attack, the response and supporting evidence. The case included a summary of the Samba exploit, a review of Wazuh's log, and CrowdSec's ban actions. Escalation provides deeper forensic analysis, follow-up and formal incident management.

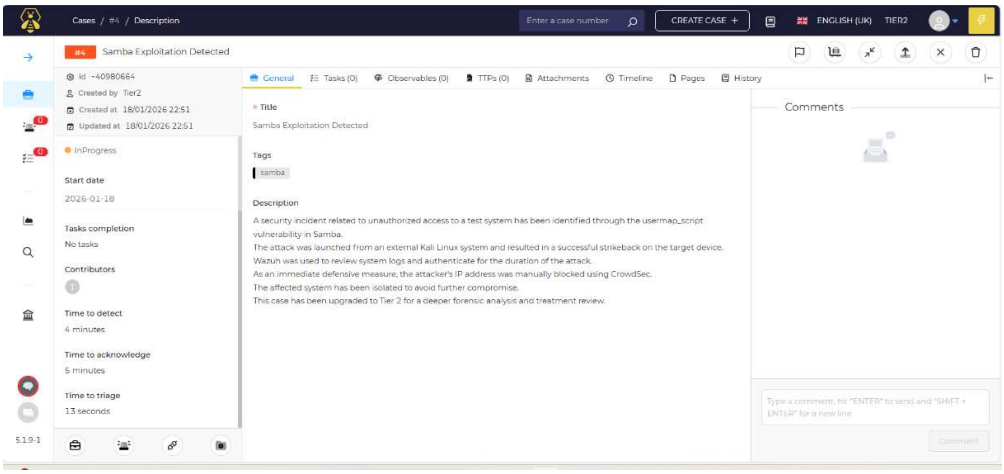

Figure 24: TheHive case created and escalated to Tier-2 for further investigation.

6.7] Reporting

Executive Summary

An event involving unauthorized access was detected in a supervised test environment. An attacker running Kali Linux exploited a known vulnerability in Samba on the targeted machine that resulted in a successful return. Security monitoring was performed using Wazuh that captured system and authentication-related logs during the attack. Although no high confidence alerts were generated a review of the log confirmed suspicious activity. As an immediate defensive measure, the attacker's IP address was manually blocked using CrowdSec preventing further communication. The incident was documented and forwarded for further investigation. No signs of lateral displacement or data leakage were detected. This report summarizes the incident actions taken and recommended improvements to improve detection and response capabilities.

Timeline

- The attack was launched from Kali Linux, using Metasploit to exploit a Samba vulnerability.
- Reverse shell has been successfully installed on the target system.

- Wazuh logs have been checked for authentication and system activity.
- No critical alerts were issued, but relevant logs were identified.
- The attacker's IP address was manually blocked using CrowdSec.
- CrowdSec blocking has been verified and implementation has been confirmed.
- The incident is documented and forwarded for further analysis.

Recommendations

We recommend enabling stricter Wazuh alert rules to extend privileges and perform suspicious operations. Threat intelligence feeds must be fully integrated to improve IOC-based detection. Automatic response actions, such as IP blocking should be configured to reduce response time. In order to prevent the exploitation of known vulnerabilities, regular vulnerability checks and patch management must be carried out. Additional log sources should be added to improve visibility.

6.8] Briefing

A security incident was identified where an external system exploited a known vulnerability in the software to gain unauthorized access to a managed test server. Activity is detected by log monitoring and investigated immediately. Although sensitive data was not affected, immediate steps were taken to block the attacker and prevent further access. The system has been revised for stability and security. The incident was documented and forwarded for further investigation. The proposed improvements focus on improved monitoring and faster automated response to reduce future risks. So, depending on the task, the appropriate writing and approach to the task is correct.