SOC Alert Management, Incident Response, and Threat Analysis

Kanchi Kakkad
SOC task - 2

Summary

This week’s assignment focused on developing both theoretical understanding and practical skills required for a Tier-1 Security Operations Center (SOC) analyst**.**

From a theoretical perspective, the assignment covered alert priority levels, emphasizing how alerts are classified as Critical, High, Medium, or Low based on impact, exploitability, and business risk. Concepts such as CVSS scoring, asset criticality, and incident severity classification were studied to understand how SOC teams prioritize alerts effectively. The assignment also introduced incident classification frameworks, including MITRE ATT&CK, to standardize how security incidents are categorized and analyzed. In addition, the incident response lifecycle—preparation, identification, containment, eradication, recovery, and lessons learned—was reviewed to understand structured response workflows.

The practical component was implemented using a two-VM SOC lab, consisting of a Wazuh Manager VM and a Wazuh Agent VM. Security events were generated on the agent system through simulated SSH authentication failures and were successfully detected and analyzed on the manager system. Alerts were reviewed in the Wazuh dashboard, classified by severity, and mapped to MITRE ATT&CK techniques.

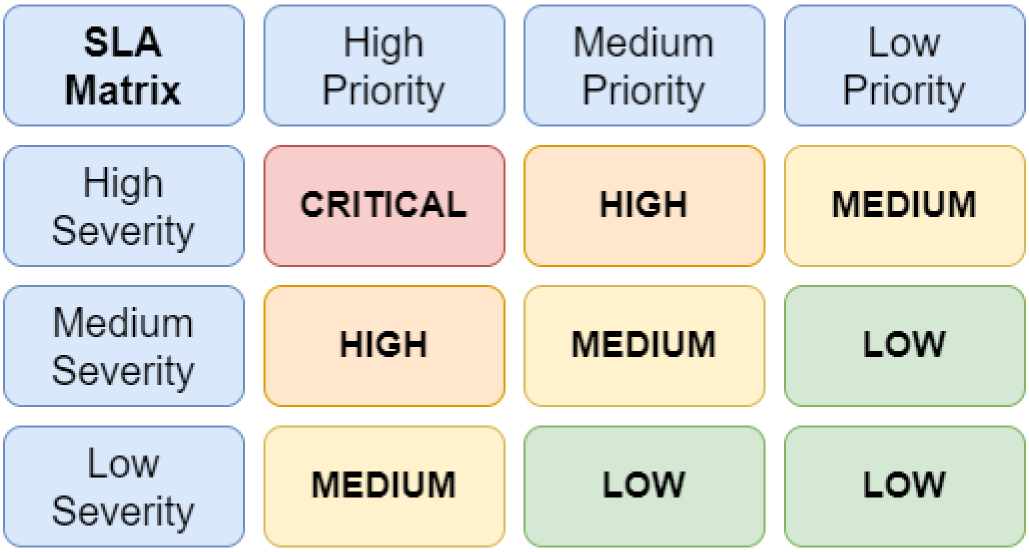
Detected alerts were converted into formal incident tickets, documenting key details such as affected assets, indicators of compromise, severity, and recommended actions. Alerts were then triaged to determine true positives, and indicators were validated using external threat intelligence platforms. A structured incident response report was created to document timelines, impact analysis, response actions, and lessons learned.

The assignment also included evidence preservation and chain of custody, where system log files were hashed and documented to ensure integrity. Finally, a capstone exercise demonstrated the complete SOC workflow from attack simulation to detection, response, reporting, and management briefing.

Overall, this week’s assignment provided a balanced understanding of SOC theory and hands-on practice, closely reflecting real-world SOC analyst operations and responsibilities.

Theoretical Knowledge

1. Alert Priority Levels

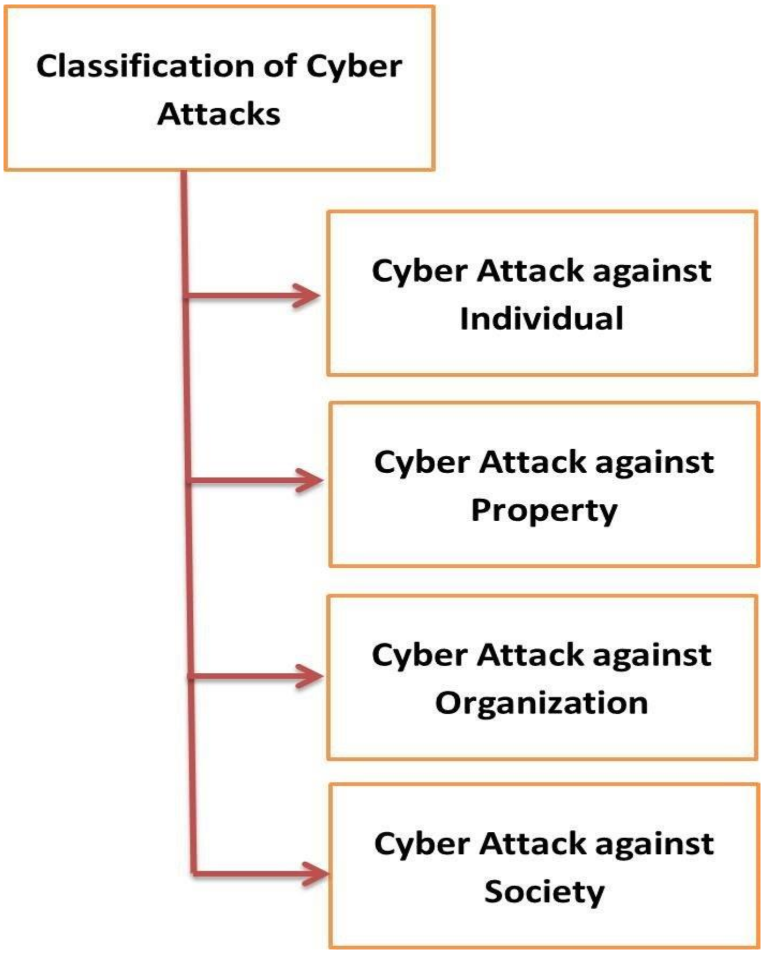


SLA Matrix	High Priority	Medium Priority	Low Priority
High Severity	CRITICAL	HIGH	MEDIUM
Medium Severity	HIGH	MEDIUM	LOW
Low Severity	MEDIUM	LOW	LOW

Alert priority levels are used in a Security Operations Center (SOC) to decide how quickly a security alert should be handled. Alerts are usually divided into four categories: Critical, High, Medium, and Low. This classification is based on the potential impact of the incident and how urgent the situation is. Critical alerts indicate serious threats such as ransomware attacks or active data breaches and require immediate response. High-priority alerts involve severe issues like unauthorized administrative access, while Medium alerts include suspicious activities such as repeated login failures. Low-priority alerts are mostly informational and include events like basic port scans or minor policy violations.

SOC analysts assign alert priority by considering factors such as the importance of the affected system, the likelihood of exploitation, and the possible business impact. For example, a vulnerability on a production server is treated as more serious than one on a test system. The Common Vulnerability Scoring System (CVSS) helps analysts measure the severity of vulnerabilities using standardized metrics. A well-known example is the Log4Shell vulnerability (CVE-2021-44228), which received a high CVSS score of 9.8 and was therefore classified as Critical. Proper alert prioritization helps SOC teams respond efficiently and focus on the most serious threats first.

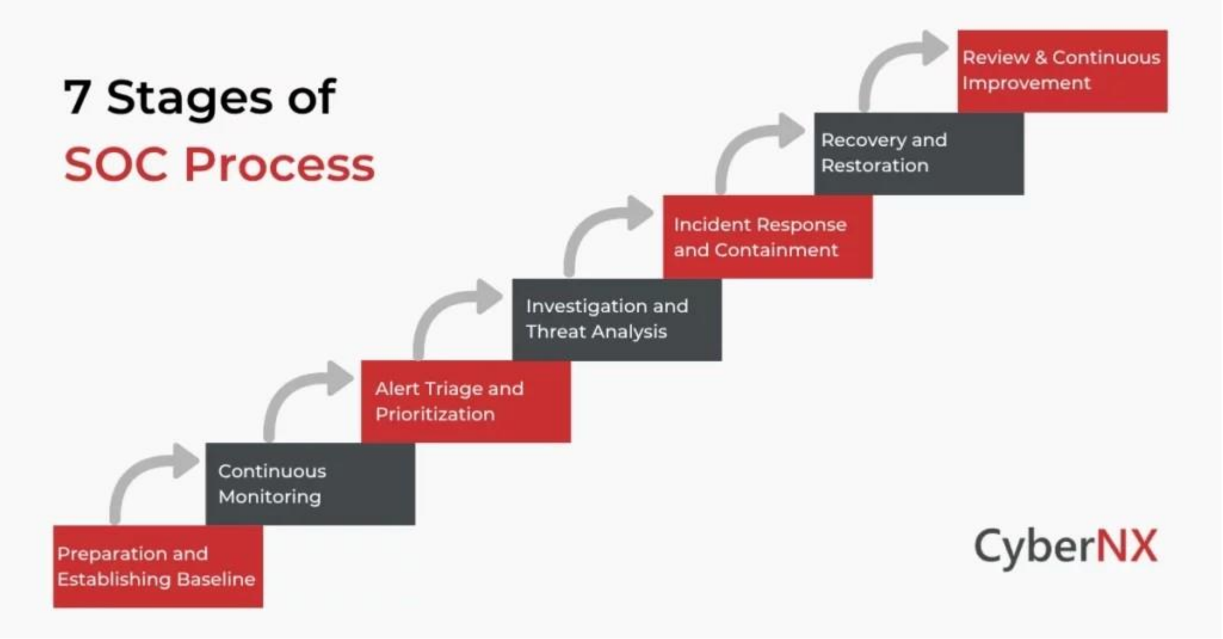
2. Incident Classification


Classification of Cyber Attacks
Cyber Attack against Individual
Cyber Attack against Property
Cyber Attack against Organization
Cyber Attack against Society

Incident classification is the process of categorizing security events into specific types so that they can be handled in an organized and consistent way. Common types of security incidents include malware infections, phishing attacks, denial-of-service attacks, insider threats, and data theft. Correct classification allows SOC analysts to quickly understand what kind of incident has occurred and choose the appropriate response. For example, an incident involving unauthorized data access by an employee is classified as an insider threat, which requires different handling than an external cyberattack.

To ensure consistency, SOC teams use standard frameworks for incident classification. The MITRE ATT&CK framework is widely used to map incidents to attacker tactics and techniques, such as T1566 for phishing attacks. Other frameworks, such as ENISA and VERIS, provide structured methods for recording and sharing incident information. In addition to classification, incidents are enriched with details like affected systems, timestamps, source IP addresses, and indicators of compromise (IOCs). This additional information helps analysts investigate incidents more effectively and improves overall incident management.

3. Basic Incident Response

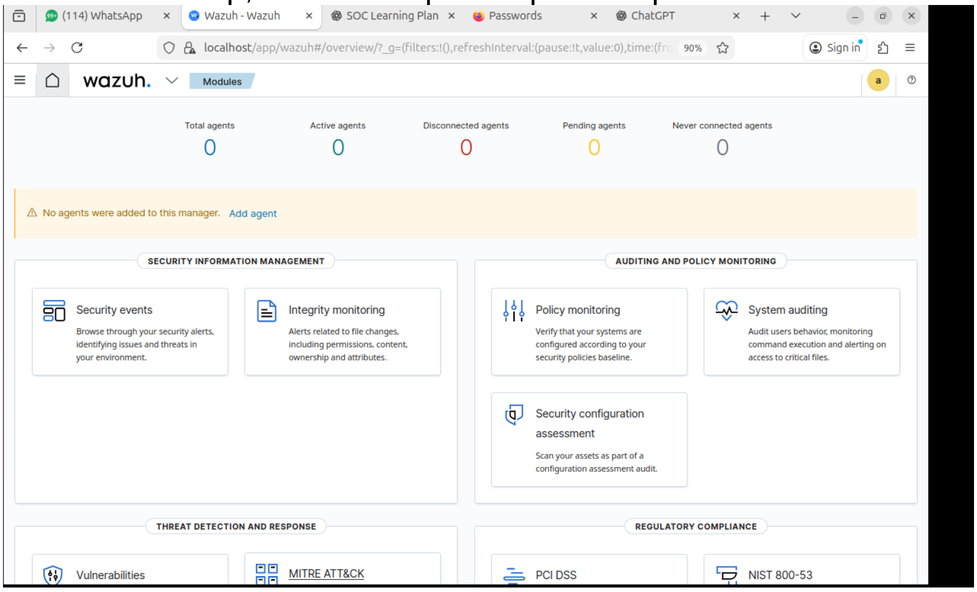

7 Stages of
SOC Process
Preparation and Establishing Baseline
Continuous Monitoring
Alert Triage and Prioritization
Investigation and Threat Analysis
Incident Response and Containment
Recovery and Restoration
Review & Continuous Improvement
CyberNX

Incident response refers to the structured process used by SOC teams to manage and resolve security incidents. The incident response lifecycle includes several stages: preparation, identification, containment, eradication, recovery, and lessons learned. Preparation involves setting up policies, tools, and response plans. Identification focuses on detecting and confirming security incidents through alert analysis. During containment, affected systems are isolated to prevent further damage, while eradication removes the root cause of the incident. Recovery ensures that systems are restored to normal operation.

Proper incident response also involves following standard procedures such as preserving evidence and maintaining clear communication. Evidence preservation includes collecting logs, creating memory dumps, and calculating file hashes to maintain data integrity. Industry standards like NIST SP 800-61 and the SANS Incident Handler’s Handbook provide guidelines and best practices for handling incidents effectively. By following a structured incident response process, SOC analysts can reduce the impact of incidents, improve response efficiency, and strengthen security measures through lessons learned after each incident.

3. SOC Lab Environment

The practical tasks were performed using a simulated SOC lab consisting of two virtual machines. The Manager Virtual Machine (VM1**)** hosted the SIEM platform and was responsible for centralized log collection, alert detection, and analysis. The Agent Virtual Machine (VM2) acted as an endpoint system, generating system logs and security events that were forwarded to the manager. This architecture reflects a real-world SOC setup, where multiple endpoints report to a centralized monitoring system.


(114) WhatsApp
Wazuh - Wazuh
SOC Learning Plan
Passwords
ChatGPT
localhost/app/wazuh#/overview/?_g=(filters:!(),refreshInterval:(pause:!t,value:0),time:(fro
90%
Sign in
wazuh.
Modules
a

Total agents 0

Active agents 0

Disconnected agents 0

Pending agents 0

Never connected agents 0

⚠ No agents were added to this manager. Add agent

SECURITY INFORMATION MANAGEMENT

Security events
Browse through your security alerts, identifying issues and threats in your environment.

Integrity monitoring
Alerts related to file changes, including permissions, content, ownership and attributes.

AUDITING AND POLICY MONITORING

Policy monitoring
Verify that your systems are configured according to your security policies baseline.

System auditing
Audit users behavior, monitoring command execution and alerting on access to critical files.

Security configuration assessment
Scan your assets as part of a configuration assessment audit.

THREAT DETECTION AND RESPONSE

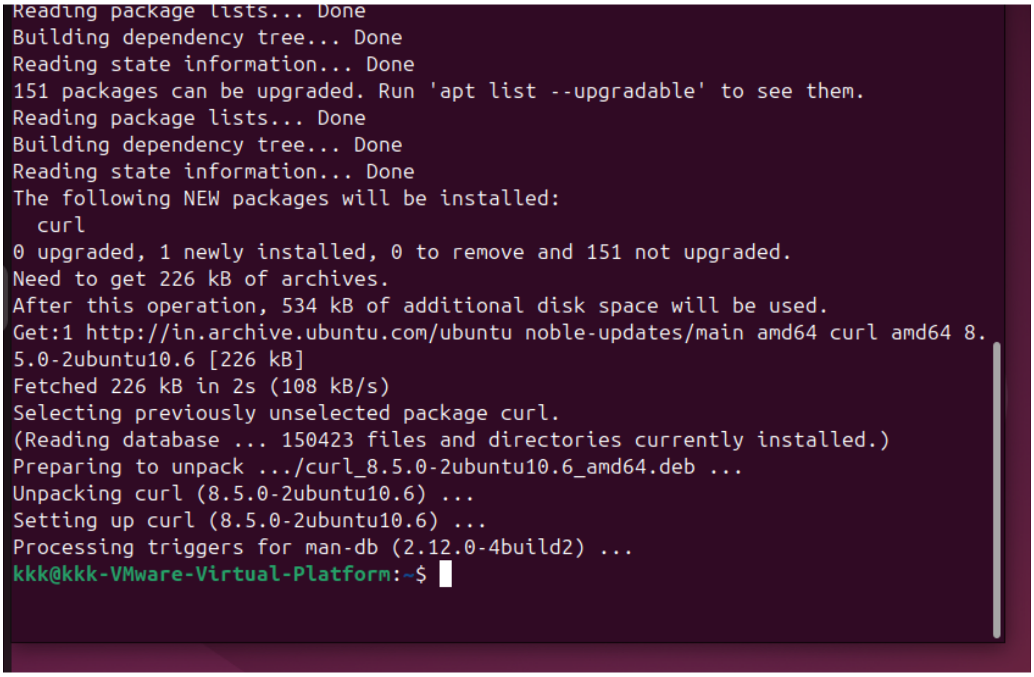
Vulnerabilities

MITRE ATT&CK

REGULATORY COMPLIANCE

PCI DSS

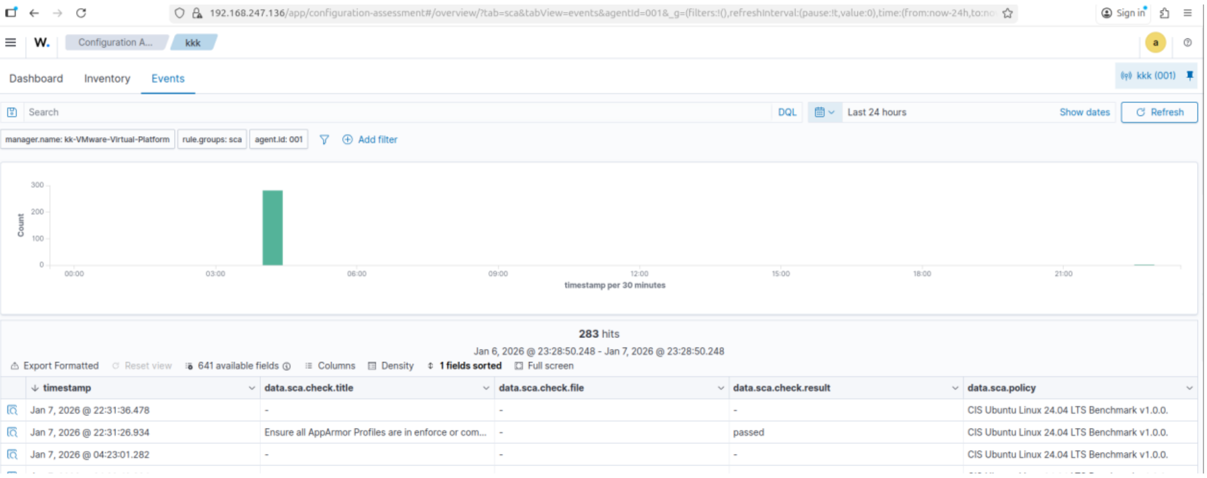
NIST 800-53



```
Reading package lists... Done
Building dependency tree... Done
Reading state information... Done
151 packages can be upgraded. Run 'apt list --upgradable' to see them.
Reading package lists... Done
Building dependency tree... Done
Reading state information... Done
The following NEW packages will be installed:
  curl
0 upgraded, 1 newly installed, 0 to remove and 151 not upgraded.
Need to get 226 kB of archives.
After this operation, 534 kB of additional disk space will be used.
Get:1 http://in.archive.ubuntu.com/ubuntu noble-updates/main amd64 curl amd64 8.
5.0-2ubuntu10.6 [226 kB]
Fetched 226 kB in 2s (108 kB/s)
Selecting previously unselected package curl.
(Reading database ... 150423 files and directories currently installed.)
Preparing to unpack .../curl_8.5.0-2ubuntu10.6_amd64.deb ...
Unpacking curl (8.5.0-2ubuntu10.6) ...
Setting up curl (8.5.0-2ubuntu10.6) ...
Processing triggers for man-db (2.12.0-4build2) ...
kkk@kkk-VMware-Virtual-Platform:~$ 
```

4. Alert Generation and Detection

Security events were generated on the agent system by simulating repeated SSH authentication failures. These events were forwarded to the manager system and detected by the SIEM platform. Alerts were reviewed in the Security Events dashboard, where details such as alert description, severity level, timestamp, and affected asset were analyzed. This task demonstrated how endpoint activity is transformed into actionable security alerts in a SOC environment.

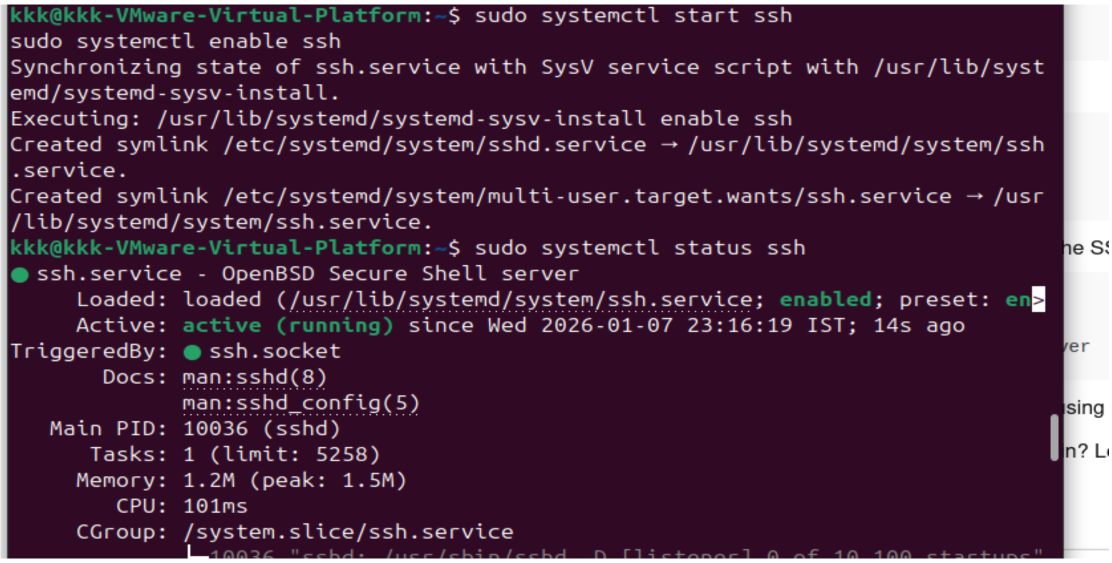


283 hits

Jan 6, 2026 @ 23:28:50.248 - Jan 7, 2026 @ 23:28:50.248

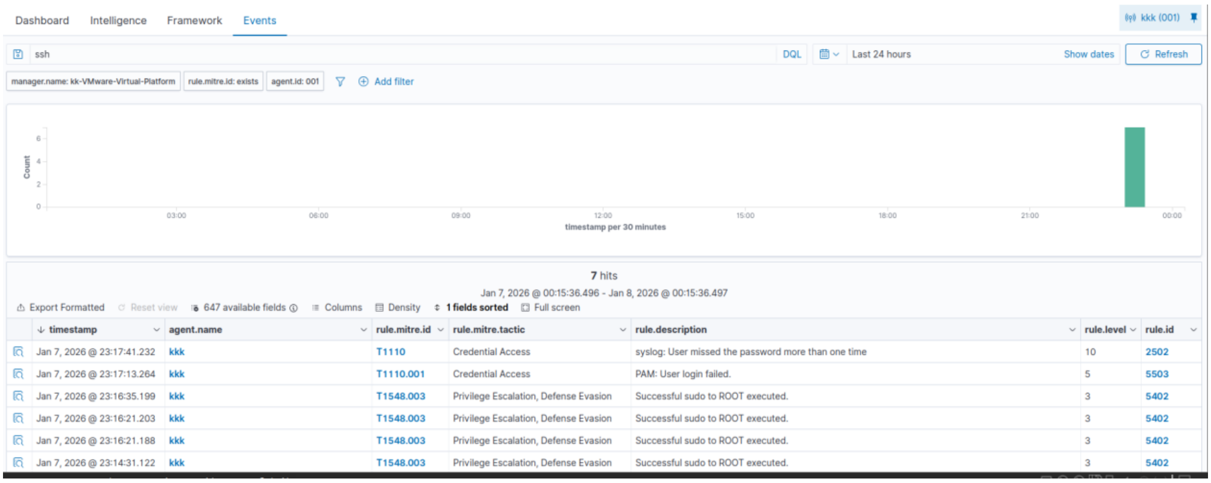
timestamp	data.sca.check.title	data.sca.check.file	data.sca.check.result	data.sca.policy
Jan 7, 2026 @ 22:31:36.478	-	-	-	CIS Ubuntu Linux 24.04 LTS Benchmark v1.0.0.
Jan 7, 2026 @ 22:31:26.934	Ensure all AppArmor Profiles are in enforce or com...	-	passed	CIS Ubuntu Linux 24.04 LTS Benchmark v1.0.0.
Jan 7, 2026 @ 04:23:01.282	-	-	-	CIS Ubuntu Linux 24.04 LTS Benchmark v1.0.0.

This image shows Security Configuration Assessment (SCA) events collected by Wazuh based on the CIS Ubuntu Linux benchmark, indicating the system’s compliance status



```
kkk@kkk-VMware-Virtual-Platform:~$ sudo systemctl start ssh
sudo systemctl enable ssh
Synchronizing state of ssh.service with SysV service script with /usr/lib/syst
emd/systemd-sysv-install.
Executing: /usr/lib/systemd/systemd-sysv-install enable ssh
Created symlink /etc/systemd/system/sshd.service → /usr/lib/systemd/system/ssh
.service.
Created symlink /etc/systemd/system/multi-user.target.wants/ssh.service → /usr
/lib/systemd/system/ssh.service.
kkk@kkk-VMware-Virtual-Platform:~$ sudo systemctl status ssh
● ssh.service - OpenBSD Secure Shell server
     Loaded: loaded (/usr/lib/systemd/system/ssh.service; enabled; preset: en>
     Active: active (running) since Wed 2026-01-07 23:16:19 IST; 14s ago
TriggeredBy: ● ssh.socket
       Docs: man:sshd(8)
             man:sshd_config(5)
   Main PID: 10036 (sshd)
      Tasks: 1 (limit: 5258)
     Memory: 1.2M (peak: 1.5M)
        CPU: 101ms
     CGroup: /system.slice/ssh.service
             └─10036 "sshd: /usr/sbin/sshd -D [listener] 0 of 10-100 startups"
```

the SSH service is enabled and actively running on the agent system, which is required for generating and monitoring SSH-related authentication events.



7 hits

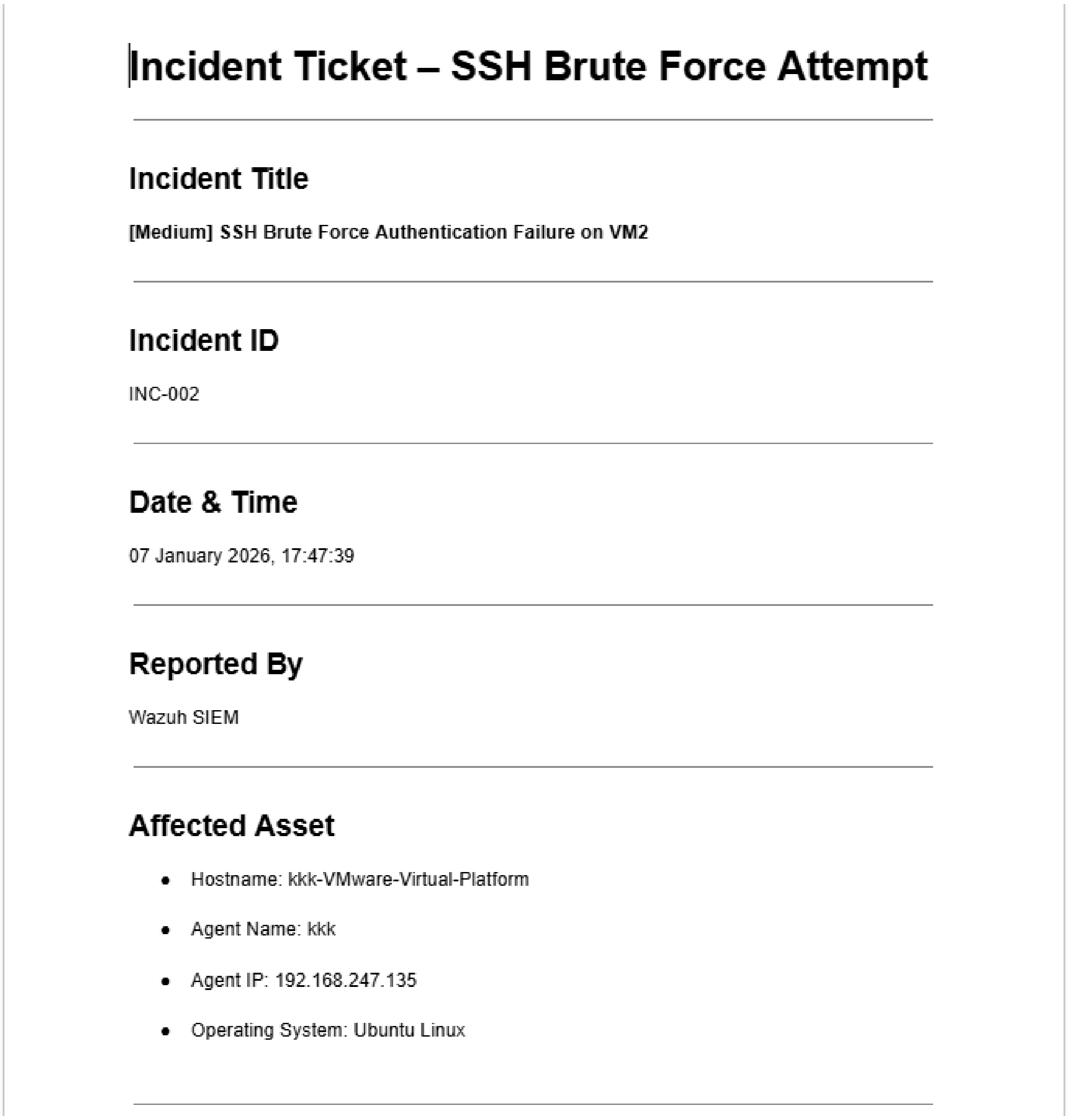
Jan 7, 2026 @ 00:15:36.496 - Jan 8, 2026 @ 00:15:36.497

timestamp	agent.name	rule.mitre.id	rule.mitre.tactic	rule.description	rule.level	rule.id
Jan 7, 2026 @ 23:17:41.232	kkk	T1110	Credential Access	syslog: User missed the password more than one time	10	2502
Jan 7, 2026 @ 23:17:13.264	kkk	T1110.001	Credential Access	PAM: User login failed.	5	5503
Jan 7, 2026 @ 23:16:35.199	kkk	T1548.003	Privilege Escalation, Defense Evasion	Successful sudo to ROOT executed.	3	5402
Jan 7, 2026 @ 23:16:21.203	kkk	T1548.003	Privilege Escalation, Defense Evasion	Successful sudo to ROOT executed.	3	5402
Jan 7, 2026 @ 23:16:21.188	kkk	T1548.003	Privilege Escalation, Defense Evasion	Successful sudo to ROOT executed.	3	5402
Jan 7, 2026 @ 23:14:31.122	kkk	T1548.003	Privilege Escalation, Defense Evasion	Successful sudo to ROOT executed.	3	5402

displays SSH-related security alerts detected by Wazuh, including brute-force authentication failures

5. Incident Ticket Creation

Detected alerts were converted into formal incident tickets to document and track security incidents. Each incident ticket included details such as incident title, severity, affected asset, indicators of compromise, and an initial assessment. Proper incident documentation supports accountability, escalation, and coordination between different SOC tiers and ensures traceability throughout the incident lifecycle.



Incident Ticket – SSH Brute Force Attempt

Incident Title

[Medium] SSH Brute Force Authentication Failure on VM2

Incident ID

INC-002

Date & Time

07 January 2026, 17:47:39

Reported By

Wazuh SIEM

Affected Asset

- Hostname: kkk-VMware-Virtual-Platform
- Agent Name: kkk
- Agent IP: 192.168.247.135
- Operating System: Ubuntu Linux

Incident Category

Unauthorized Access Attempt / Brute Force Attack

Severity

Medium
(Rule Level: 10)

Status

Open

Incident Description

Multiple failed SSH authentication attempts were detected on the endpoint system (VM2). The Wazuh agent identified repeated password failures through the SSH daemon, indicating a potential brute-force attack targeting the SSH service. The event was generated from system logs monitored via journald and decoded by the SSHD decoder.

No successful authentication was observed during this activity.

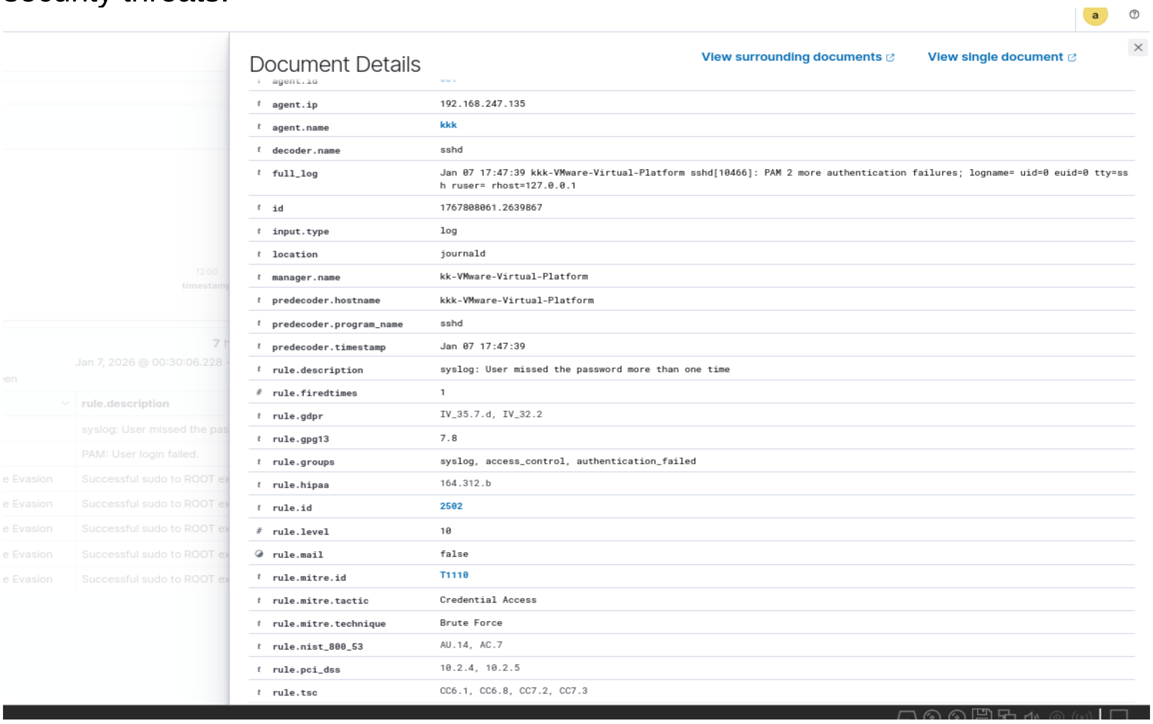
Detection Details

- Detection Source: Wazuh Agent
- Decoder Name: sshd
- Log Source: journald
- Rule ID: 2502
- Rule Description: User missed the password more than one time

6. Alert Triage and IOC Validation

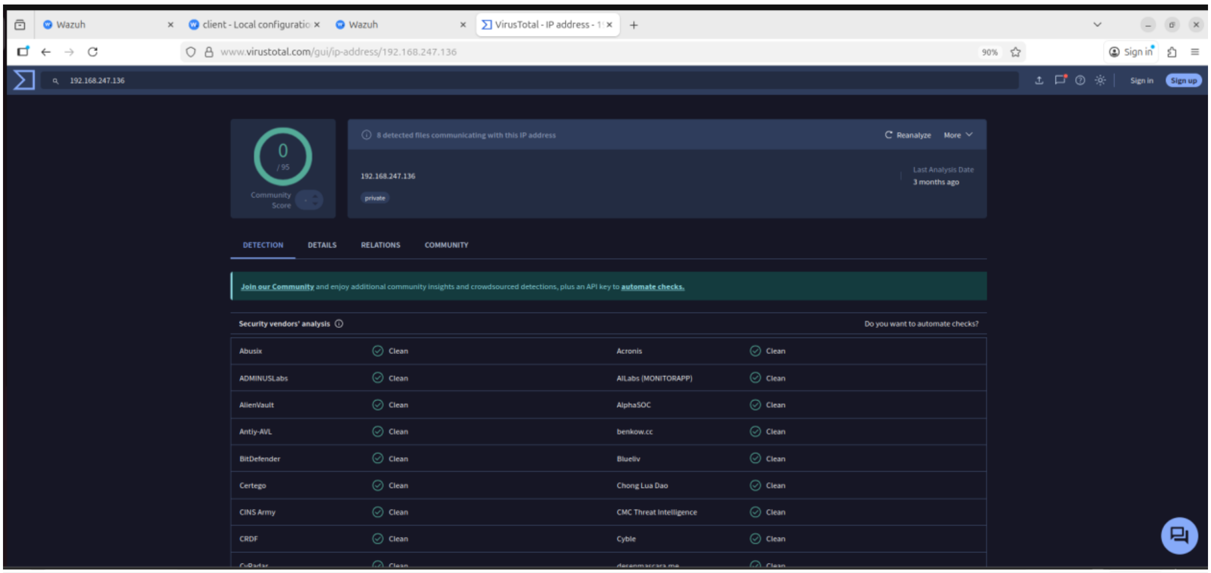
Alert triage was conducted to evaluate detected security alerts and determine whether they represented true security incidents or false positives. During this process, alert attributes such as frequency, severity level, affected assets, and contextual log information were carefully analyzed. The SSH brute-force alert was classified as a true positive due to the presence of multiple consecutive authentication failures, which indicated intentional and unauthorized access attempts rather than normal user behavior.

Following triage, indicators of compromise (IOCs) associated with the alert were identified and validated using external threat intelligence platforms. Key IOCs, including source IP addresses and authentication-related artifacts, were cross-referenced to assess their reputation and potential malicious associations. This validation step helped confirm the nature of the alert and rule out benign activity. The triage and IOC validation process highlights the importance of analyst judgment combined with threat intelligence in reducing false positives, improving alert accuracy, and ensuring that SOC efforts are focused on genuine and higher-risk security threats.



agent.id	[illegible]
agent.ip	192.168.247.135
agent.name	kkk
decoder.name	sshd
full_log	Jan 07 17:47:39 kkk-VMware-Virtual-Platform sshd[10466]: PAM 2 more authentication failures; logname= uid=0 euid=0 tty=ssh ruser= rhost=127.0.0.1
id	1767808061.2639867
input.type	log
location	journald
manager.name	kk-VMware-Virtual-Platform
predecoder.hostname	kkk-VMware-Virtual-Platform
predecoder.program_name	sshd
predecoder.timestamp	Jan 07 17:47:39
rule.description	syslog: User missed the password more than one time
rule.firedtimes	1
rule.gdpr	IV_35.7.d, IV_32.2
rule.gpg13	7.8
rule.groups	syslog, access_control, authentication_failed
rule.hipaa	164.312.b
rule.id	2502
rule.level	10
rule.mail	false
rule.mitre.id	T1110
rule.mitre.tactic	Credential Access
rule.mitre.technique	Brute Force
rule.nist_800_53	AU.14, AC.7
rule.pci_dss	10.2.4, 10.2.5
rule.tsc	CC6.1, CC6.8, CC7.2, CC7.3

Detailed Wazuh alert information for SSH brute-force detection used during alert triage and analysis



Wazuh
client - Local configuratio
Wazuh
VirusTotal - IP address - 1
www.virustotal.com/gui/ip-address/192.168.247.136
90%
Sign in
192.168.247.136
Sign in
Sign up

0 / 95 Community Score

8 detected files communicating with this IP address

Reanalyze More

192.168.247.136

private

Last Analysis Date
3 months ago

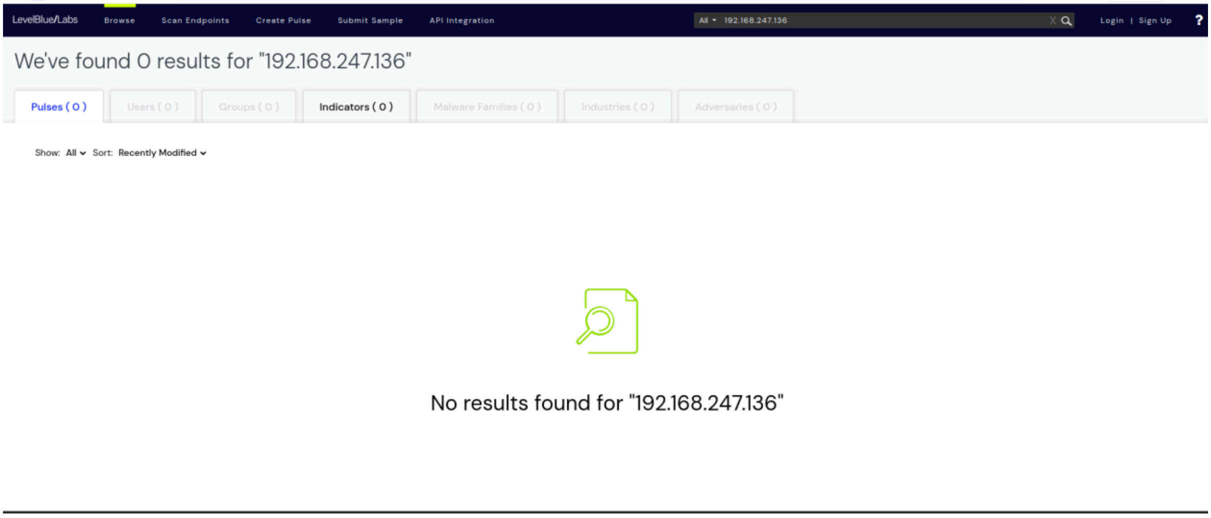
DETECTION
DETAILS
RELATIONS
COMMUNITY

Join our Community and enjoy additional community insights and crowdsourced detections, plus an API key to automate checks.

Security vendors' analysis

Do you want to automate checks?

Abusix	✓ Clean	Acronis	✓ Clean
ADMINUSLabs	✓ Clean	AILabs (MONITORAPP)	✓ Clean
AlienVault	✓ Clean	AlphaSOC	✓ Clean
Antiy-AVL	✓ Clean	benkow.cc	✓ Clean
BitDefender	✓ Clean	Blueliv	✓ Clean
Certego	✓ Clean	Chong Lua Dao	✓ Clean
CINS Army	✓ Clean	CMC Threat Intelligence	✓ Clean
CRDF	✓ Clean	Cyble	✓ Clean
CyRadar	✓ Clean	desenmascara.me	✓ Clean

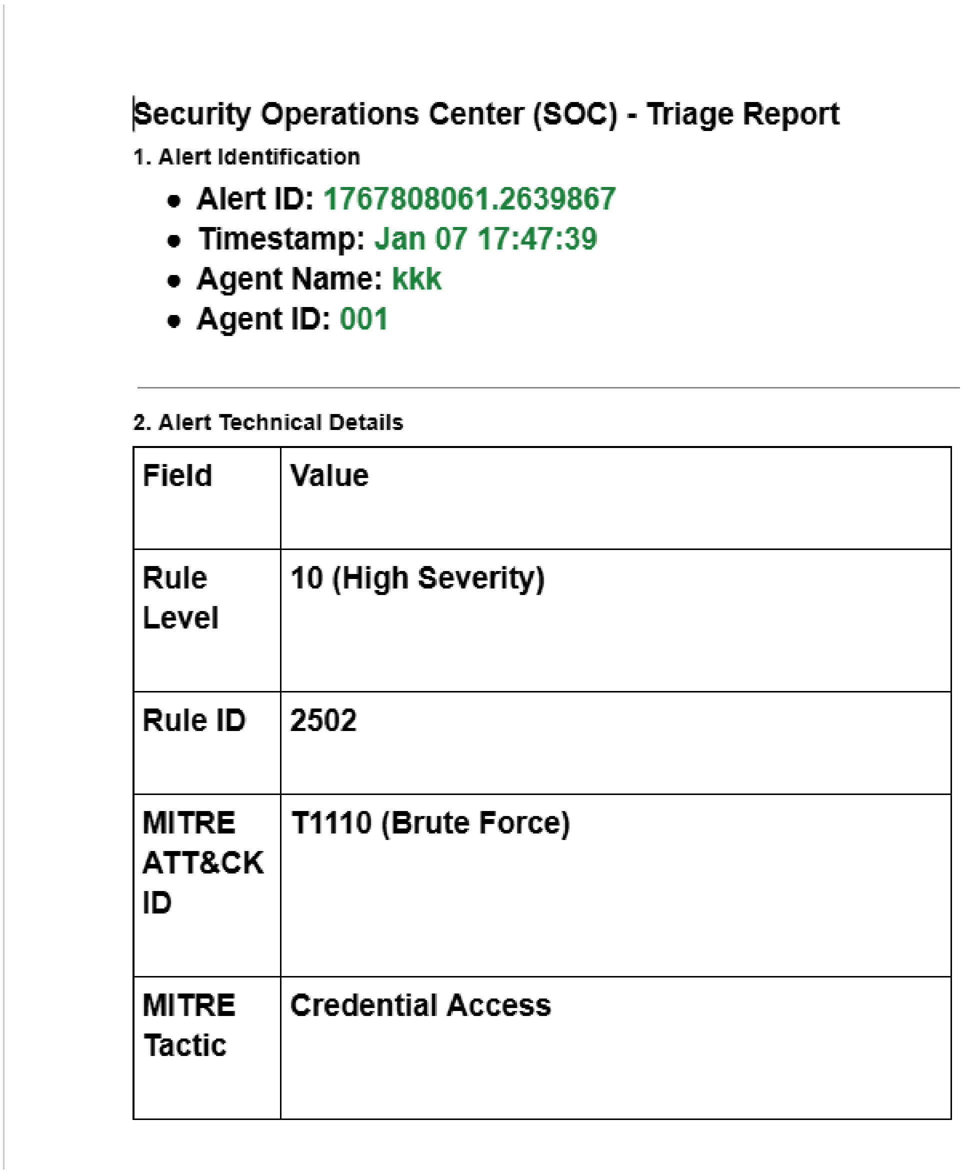


We've found 0 results for "192.168.247.136"

No results found for "192.168.247.136"

7. Incident Response and Documentation

Based on the triage results, appropriate response actions were documented. As no successful system compromise was identified, the response focused on monitoring and recommending security hardening measures. A structured incident response report was prepared, including an executive summary, incident timeline, impact analysis, response actions, and lessons learned.



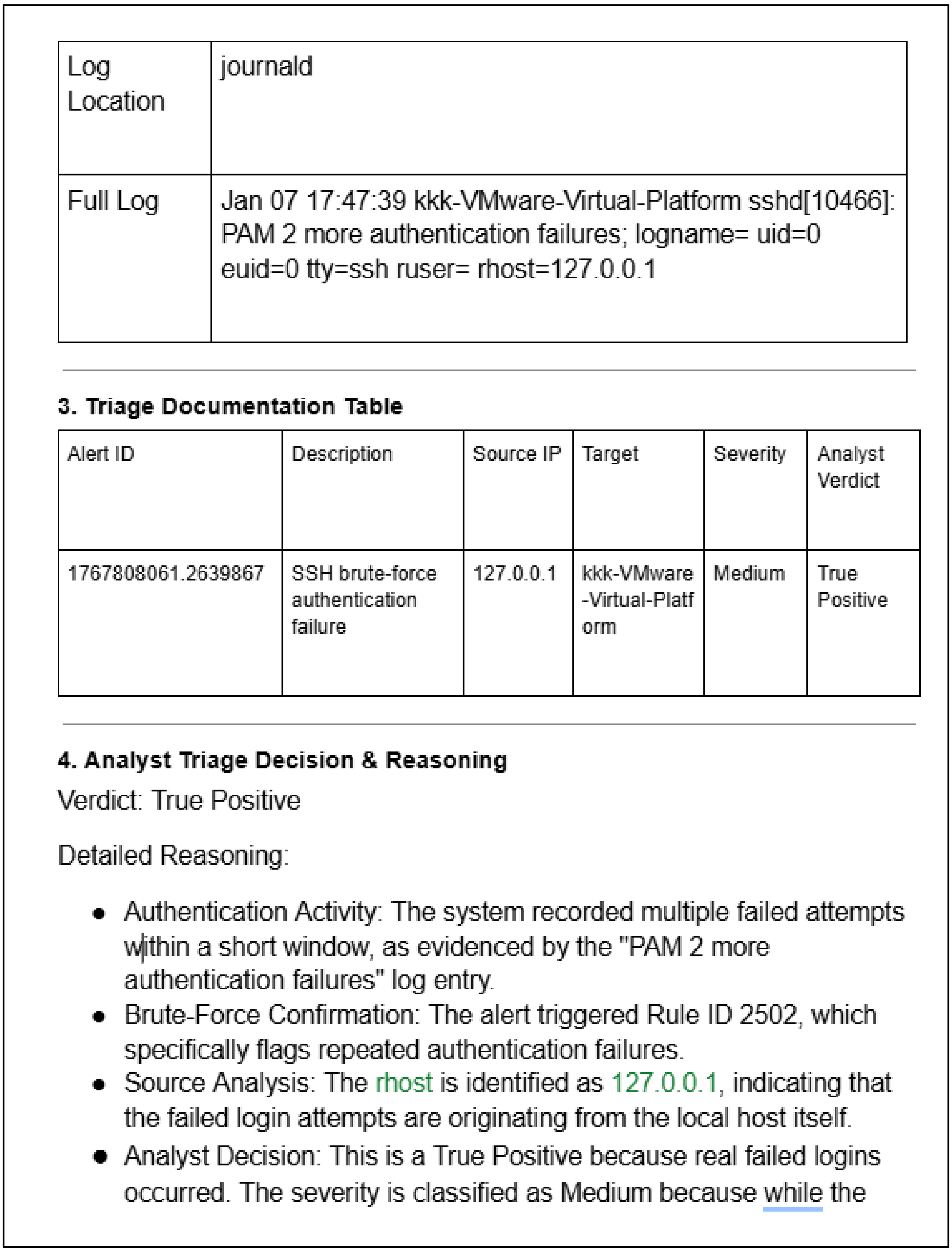
Security Operations Center (SOC) - Triage Report

1. Alert Identification

- **Alert ID:** 1767808061.2639867
- **Timestamp:** Jan 07 17:47:39
- **Agent Name:** kkk
- **Agent ID:** 001

2. Alert Technical Details

Field	Value
Rule Level	10 (High Severity)
Rule ID	2502
MITRE ATT&CK ID	T1110 (Brute Force)
MITRE Tactic	Credential Access



Log Location	journald
Full Log	Jan 07 17:47:39 kkk-VMware-Virtual-Platform sshd[10466]: PAM 2 more authentication failures; logname= uid=0 euid=0 tty=ssh ruser= rhost=127.0.0.1

3. Triage Documentation Table

Alert ID	Description	Source IP	Target	Severity	Analyst Verdict
1767808061.2639867	SSH brute-force authentication failure	127.0.0.1	kkk-VMware-Virtual-Platform	Medium	True Positive

4. Analyst Triage Decision & Reasoning

Verdict: True Positive

Detailed Reasoning:

- Authentication Activity: The system recorded multiple failed attempts within a short window, as evidenced by the "PAM 2 more authentication failures" log entry.
- Brute-Force Confirmation: The alert triggered Rule ID 2502, which specifically flags repeated authentication failures.
- Source Analysis: The rhost is identified as 127.0.0.1, indicating that the failed login attempts are originating from the local host itself.
- Analyst Decision: This is a True Positive because real failed logins occurred. The severity is classified as Medium because while the

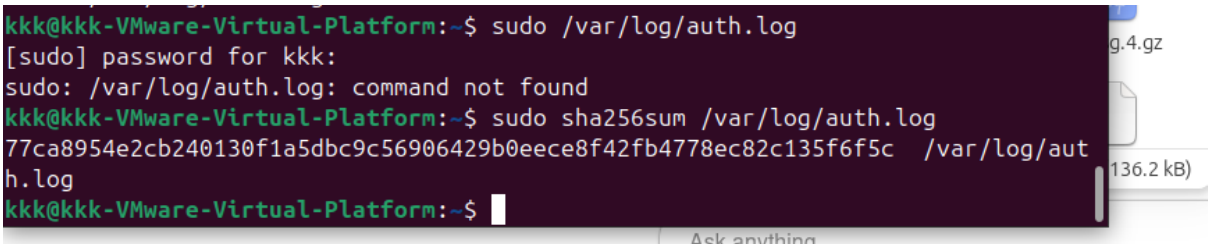
Analyst triage documentation for SSH brute-force alert

8. Evidence Preservation and Chain of Custody

Evidence preservation is a critical component of incident response, as it ensures that digital artifacts related to a security incident remain reliable, verifiable, and legally admissible if required. During this task, relevant system artifacts associated with the incident were identified and preserved, including authentication log files containing records of suspicious SSH activity. Preserving such evidence allows security teams to perform further forensic analysis and supports compliance, auditing, and potential legal investigations.

To maintain the integrity of the collected evidence, cryptographic hashing techniques were applied. A SHA-256 hash value was generated at the time of collection to create a unique digital fingerprint of the evidence file. This hash value serves as a mechanism to verify that the evidence has not been altered or tampered with after collection. Any modification to the file would result in a mismatch in the hash value, thereby indicating a loss of integrity. The use of hashing is a standard practice in digital forensics to ensure evidence authenticity.

In addition to evidence preservation, a formal chain of custody record was maintained to document the handling of the evidence throughout its lifecycle. The chain of custody recorded details such as the date and time of collection, the individual responsible for collecting the evidence, the method of acquisition, and the storage location. Maintaining a clear and complete chain of custody ensures accountability and transparency, demonstrating that the evidence was handled in a controlled and secure manner. This process reinforces best practices in digital forensics and incident response, emphasizing the importance of evidence integrity and proper documentation in SOC operations.



```
kkk@kkk-VMware-Virtual-Platform:~$ sudo /var/log/auth.log
[sudo] password for kkk:
sudo: /var/log/auth.log: command not found
kkk@kkk-VMware-Virtual-Platform:~$ sudo sha256sum /var/log/auth.log
77ca8954e2cb240130f1a5dbc9c56906429b0eece8f42fb4778ec82c135f6f5c  /var/log/aut
h.log
kkk@kkk-VMware-Virtual-Platform:~$
```

SHA-256 hash calculation of authentication log file to preserve evidence integrity

9. Capstone Project: End-to-End SOC Workflow

The capstone task demonstrated the complete SOC workflow from attack simulation to final reporting. A security event was generated, detected, triaged, responded to, and documented end-to-end. A detailed incident report and a non-technical management briefing were prepared, highlighting both technical analysis and professional communication skills required in SOC operations.

This week’s tasks successfully demonstrated how to manage a security incident from start to finish using a professional SOC workflow. By moving from the theory of alert priority and CVSS scoring to the practical use of Wazuh, I learned how to identify real threats among many logs. The lab environment allowed me to see how a manager and agent work together to detect suspicious activity, like the brute-force attack analyzed in this report.

Beyond just detecting the attack, this project emphasized the importance of proper documentation and evidence preservation. Learning how to create incident reports and maintain a chain of custody ensures that the work of a SOC analyst is accurate and useful for future security improvements. Overall, this task provided the hands-on experience needed to understand the daily responsibilities and technical skills required in a modern Security Operations Center.

Conclusion

This week’s assignment provided a comprehensive understanding of core Security Operations Center (SOC) concepts through a balanced integration of theoretical study and practical implementation. Key areas such as alert prioritization, incident classification, alert triage, incident response, and evidence preservation were systematically explored using a simulated SOC laboratory environment. Theoretical frameworks, including alert severity models, MITRE ATT&CK mappings, and structured incident response lifecycles, were reinforced through hands-on analysis of real security events.

The practical tasks demonstrated the complete SOC workflow, beginning with alert generation and detection, followed by triage and IOC validation, formal incident ticket creation, response documentation, and evidence integrity verification. Emphasis was placed on accurate documentation, analytical decision-making, and adherence to industry best practices such as hashing and chain-of-custody maintenance. Overall, this assignment strengthened foundational SOC analyst skills and enhanced readiness for real-world security operations by closely replicating professional SOC processes and responsibilities.