SOC Fundamentals, Security Monitoring, and Incident Handling

Introduction

SOC is a team of professionals that is centralized and is involved in monitoring, detection, and response to cybersecurity threats within the organization. SOC is constantly working and utilizing tools, processes, and analysts to identify any malicious activities taking place in the networks, systems, and applications of the organization. The most important objective of SOC is to point out security incidents as early as possible before any serious damage is done.

Manual monitoring cannot address such threats. A SOC is necessary as it offers the following benefits:

- Continuous System & Network Monitoring
- Identifying Security Threats
- Faster incident response to minimize impact
- Centralized visibility into security events

The purpose of this study is to learn about the basic principles of operations in a SOC and to provide hands-on experience in the security monitoring and incident response mechanisms.

SOC Fundamentals and Operations

The main aim of a SOC is to offer security to the organization in the following ways:

- Detecting the threats before they are exploited
- Handling security events effectively in a timely manner
- Real-Time Viewing of System Logs and Alerts
- Decreasing cyber-attack effects via organized response strategies.

SOC Roles and Responsibilities

SOC teams have distinct roles to allow efficient handling of the incidents:

- Tier 1 (L1) Analyst
  It monitors the alerts produced by the SIEM system, carries out the primary analysis, and filters out the false positives.
- Tier 2 (L2) Analyst
  Examines confirmed alerts, relationships between logs, and determines incident root cause.
- Tier 3 (L3) Analyst
  Deals with difficult cases, high-level threat analysis, and malware analysis.
- Threat Hunter
  Actively looks for hidden dangers that might not generate alerts.
- SOC Manager
  Manages SOC operations, escalations, reporting, management, SOC performance management.

Core Functions of a SOC

- Analysis of log data from various sources, including servers, endpoints, or firewalls.
- Enable alert triage to assign priorities and types to events related to security.
- Investigation and escalation of incident cases.
- Integrating threat intelligence for correlation of alerts to attack indicators.
- Recording and reporting incidents.

SOC Frameworks

NIST Framework (Incident Response Focus)

The NIST Incident Response guide (SP 800-61) gives a systematic method to deal with incidents. The following phases are outlined:

- Preparation – Develop policies and response strategies
- Identification – Detect and confirm security incidents
- Containment – Limit the spread of the Incident
- Eradication – Erase the source of the threat
- Recovery - Restore systems to normal operation
- Lessons Learned – Improve processes based on findings

MITRE ATT&CK Framework

MITRE ATT&CK is a knowledge base of real-world attacker techniques. There are tactics such as:

- Initial Access
- Execution
- Persistence
- Privilege Escalation
- Lateral Movement
- Exfiltration

SOC analysts utilize MITRE ATT&CK for the following purposes

- Understand the attack behavior
- Correspond alerts to particular means of attacking
- Enhance methods for detection and response

Security Monitoring Basics

Monitoring is one of the primary operations of a Security Operations Center. Monitoring includes the continuous observation of systems, networks, and users for signs of malicious activity and potential security events. Monitoring enables the quick detection and mitigation of attacks.

Objectives of Security Monitoring

- Identify abnormalities or irregularities in system or user activities.
- Detect unauthorized access, like brute-force login attempts or remote access.

- Identify policy violations such as credential misuse and unauthorized execution of software.
- Security monitoring enables the SOC analyst to detect threats before they become an incident.

Tools Used For Security Monitoring

Security Information & Event Management (SIEM)

Tools such as Elastic SIEM or Splunk use logs from numerous sources, correlating the data to produce an alert. Such tools assist security analysts in identifying patterns consistent with potential attacks.

The following are the functions of SIEM tools.

- Centralized log collection
- Correlation of events
- Alert generation
- Data visualization

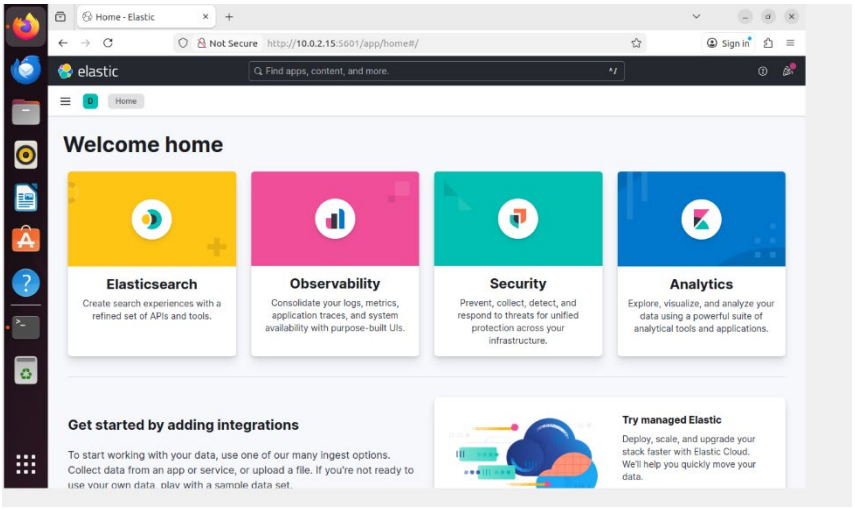

Fig1: Elastic SIEM dashboard

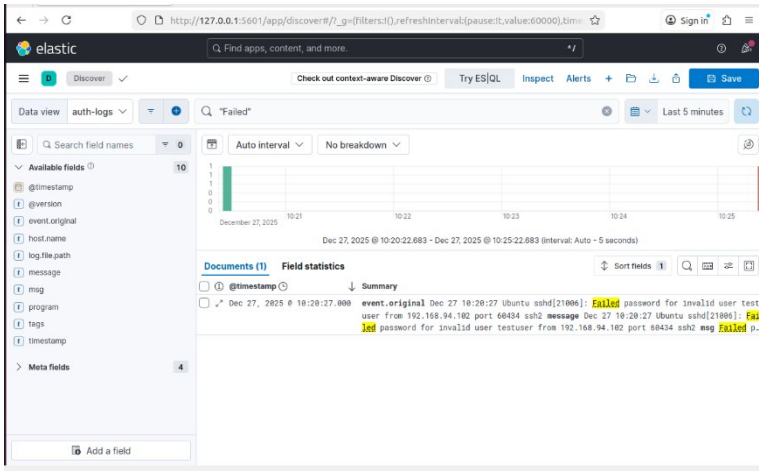

Fig2: Applying filters in SIEM to identify failed login attempts

Network Traffic Analyzers

Tools such as Wireshark enable the analysis of network traffic at a packet level, the identification of:

- Suspicious connections
- Unusual protocols or ports
- Signs of data exfiltration or scanning activity

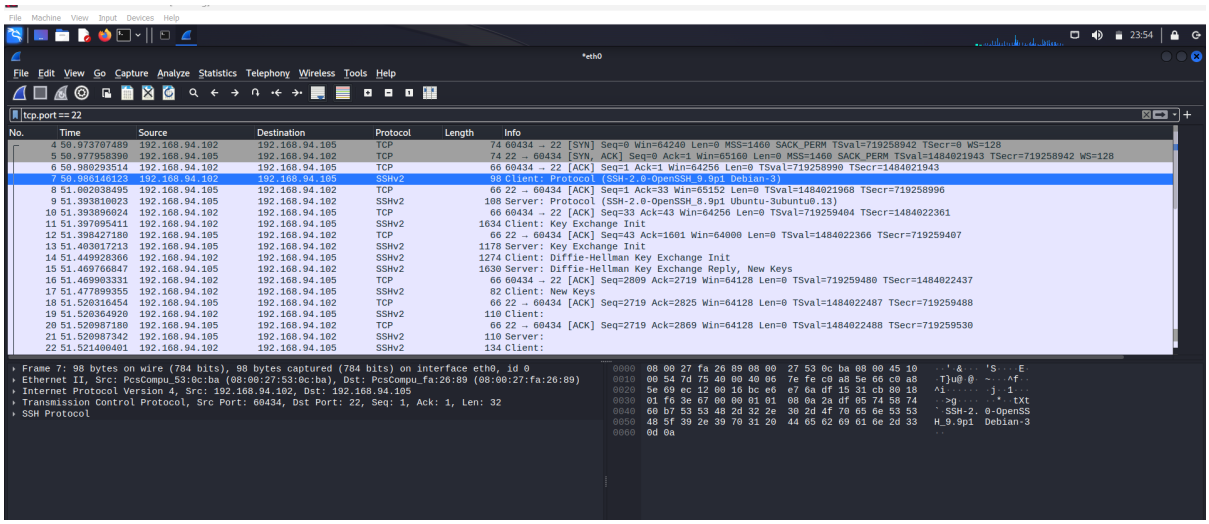

Fig3: Wireshark used to analyze network traffic

Security Monitoring Key Metrics

There are some metrics that SOC teams use to gauge the effectiveness of monitoring:

- ***False Positives***: Alerts that appear malicious but actually are not
- ***False Negatives:*** Real threats not detected
- ***MTTD - Mean Time to Detect***: Average time it takes to detect a security incident. It improves SOC efficiency and analyst productivity by reducing false positives and MTTD.

Log Management Fundamentals

Log management is one of the key functions in Security Operations. Logs give insight into activity in the system, user behavior, and potential security incidents. Effective log management, therefore, needs to ensure that security events are collected, stored, and analyzed in such a structured way that SOC analysts can effectively detect and investigate threats.

Log Lifecycle

- ***Log Collection:***
  Logs are part of a security information and event management system, and mainly logs are collected from servers, endpoints, applications, and network devices.
- ***Log Normalization:*** Collected logs are transformed into a standard format for sure consistency and readability of the logs.
- ***Log Storage:*** Events are securely stored in centralized systems like SIEM platforms for future reference.
- ***Log Retention:*** Logs are kept for a period of time to support compliance, auditing, and forensic investigations.
- ***Log Analysis:*** It does this by looking for anomalies, security incidents, and suspicious behavior within stored logs.

This lifecycle aids the SOC analyst in understanding how to manage logs effectively and maintain system visibility.

Common Log Types

Windows Event Logs: Events related to authentication, system changes, and security relevant activity.

Syslog: Logs generated by Linux systems, network devices and security appliances.

HTTP Server Logs: Web server access and error logs used for detecting suspicious web activities.

Log Collection Using Logstash

In order to comprehend the concept of log collection, there was a lab setting whereby log ingestion was simulated.

- The syslog logs were created on Ubuntu machine by using the "logger" command.
- The command was logger “Test message from SOC log management”.
- The logging forwarding was done by using Logstash.
- The logs were sent to the Elastic SIEM system.
- The exercise showed the procedure involved in acquiring the log data from the endpoints and transferring the data to a SIEM system.

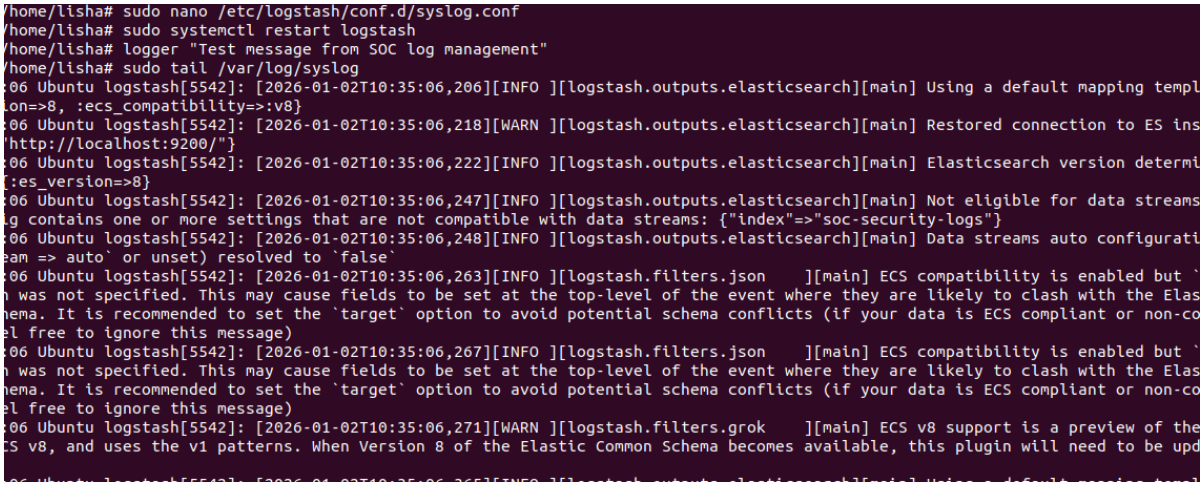

Fig4: Generating test Syslog messages on Ubuntu terminal

Log Analysis & Querying

Once the logs are gathered and standardized, log queries are conducted to seek security events.

- The queries were formulated using KQL (Kibana Query Language).
- Attempts to log in incorrectly were searched with Event ID 4625 to identify any brute-force actions.
- The results of the queries were sorted based on the source IP.
- This assisted in understanding how the SOC analysts work in investigating incidents related to authentication.

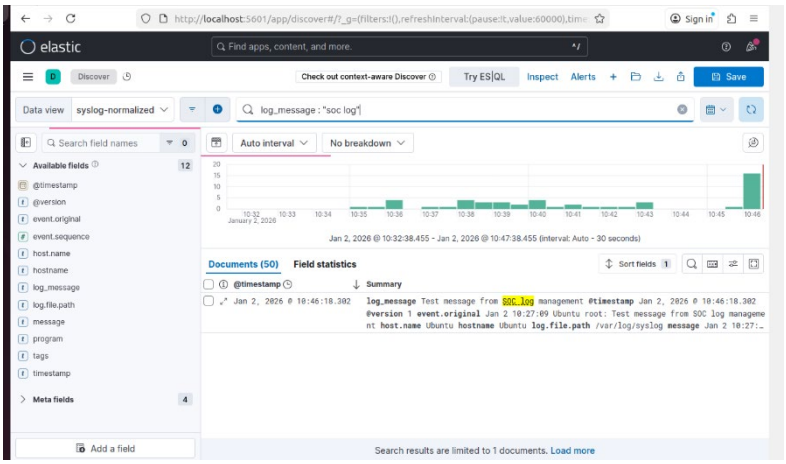

Fig 5: Collected logs visible in Elastic SIEM for analysis

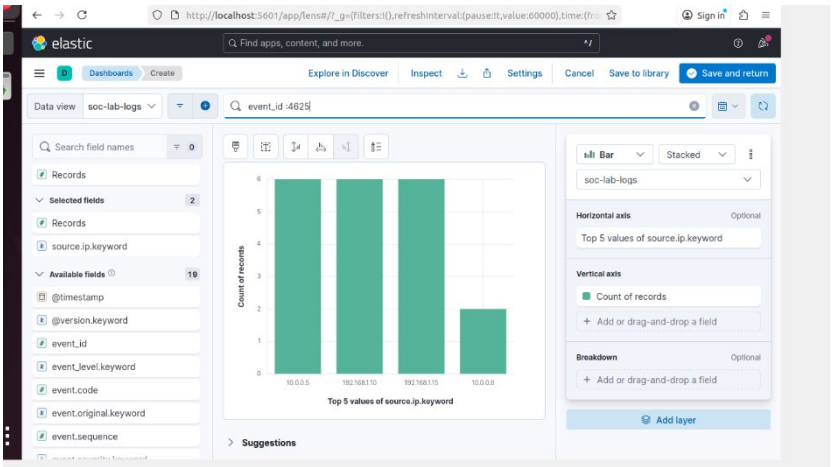

Fig 6: KQL query used to identify failed login attempts

Security Tools Overview

Security tools form the backbone of SOC operations by ensuring that we can monitor, detect, investigate, and respond to security incidents. Different tools are used for different purposes, such as log correlation, endpoint monitoring, intrusion detection, and vulnerability assessment. Understanding the functionality of these various tools will support an SOC analyst in choosing the right tool for a given security scenario.

1.SIEM- Security Information and Event Management

- Security information and event management tools, such as Splunk and IBM QRadar, unify logs across an organization for collection, correlation, and analysis. These tools enhance the central enterprise visibility of security incidents and send alerts against suspicious activities.
- In this learning exercise, open-source and free-tier SIEM platforms such as Wazuh and Elastic SIEM were explored to understand SOC monitoring workflows.

2.Endpoint Detection and Response

- EDR tools, such as CrowdStrike, monitor processes running on the endpoint, including process execution, file changes, and network connections.
- They provide security teams with the capability to detect malicious behaviors right at the endpoint level and enable quick investigation and response.

3. Intrusion Detection and Prevention Systems (IDS/IPS)

- Network activity detection or prevention tools, such as Snort, can be utilized to find or filter malicious network traffic according to specific rules.
- These tools monitor network traffic and trigger alerts as soon as suspicious traffic patterns are detected.
- Snort rules assist us in identifying known threats such as malicious domains, scanning, and protocol violations.

Fig 7: Custom Snort rule created to detect malicious domain access

Fig 8: Testing Snort rule using simulated HTTP request

4.Vulnerability Scanning Tools

- Vulnerability scanners, such as Nessus, are designed to scan target systems for security-related weaknesses in applications, services, or systems. The scanning results in the form of identified vulnerabilities, along with their respective security levels, are provided in the form of a CVSS score.
- Nessus Essentials was utilized to scan the Metasploitable machine(192.168.94.101) to see how vulnerabilities are identified and prioritized.

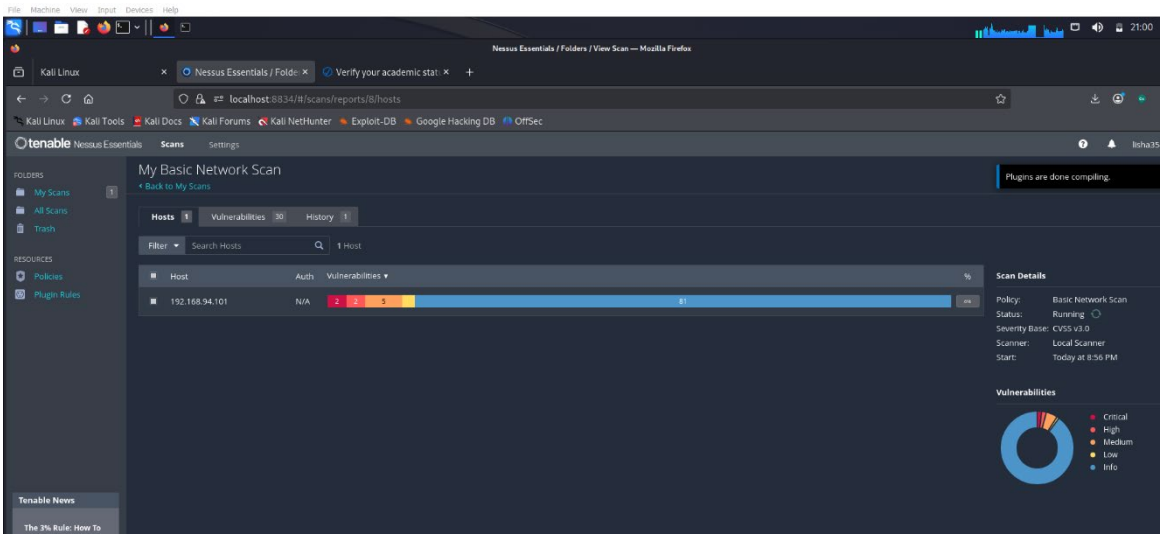

Fig 9: Nessus Essentials configured for vulnerability scanning.

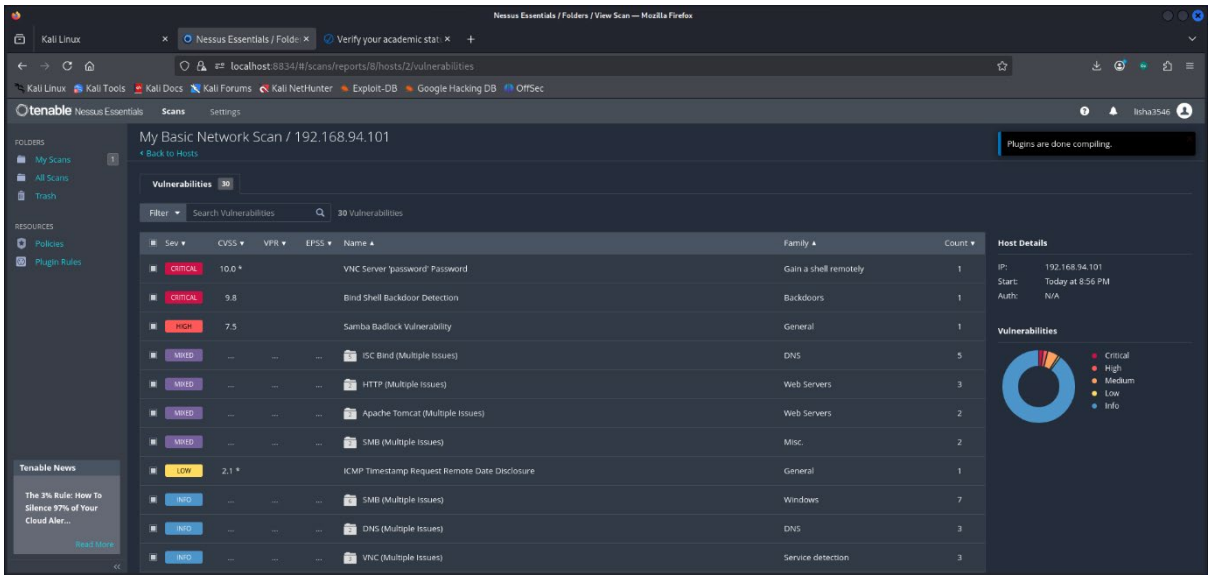

Fig 10: Vulnerability scan results showing identified security weaknesses.

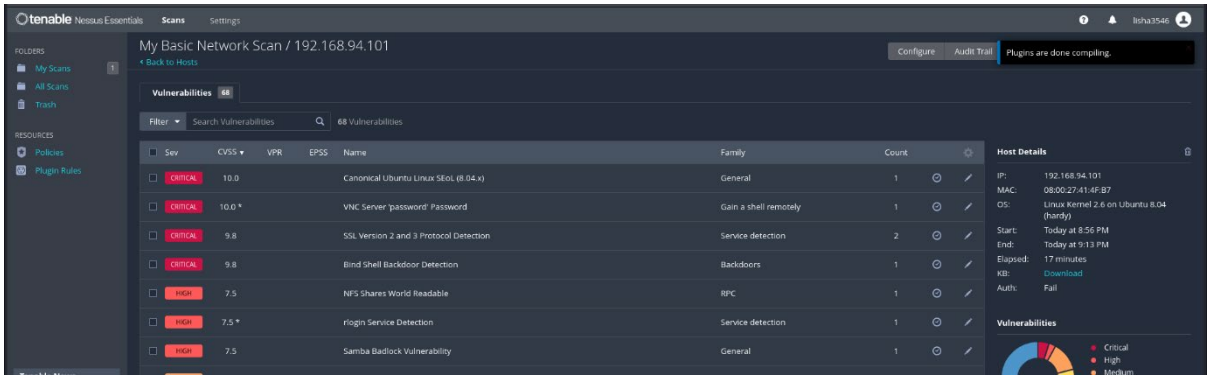

Fig 11: High-severity vulnerabilities identified during Nessus scan.

5. Osquery Monitoring

Osquery querying was done to search processes running on a Windows machine. A harmless batch file was also developed to test a malicious process. The above operation proved the relevance of endpoint monitoring solutions in monitoring system events and even malicious processes.

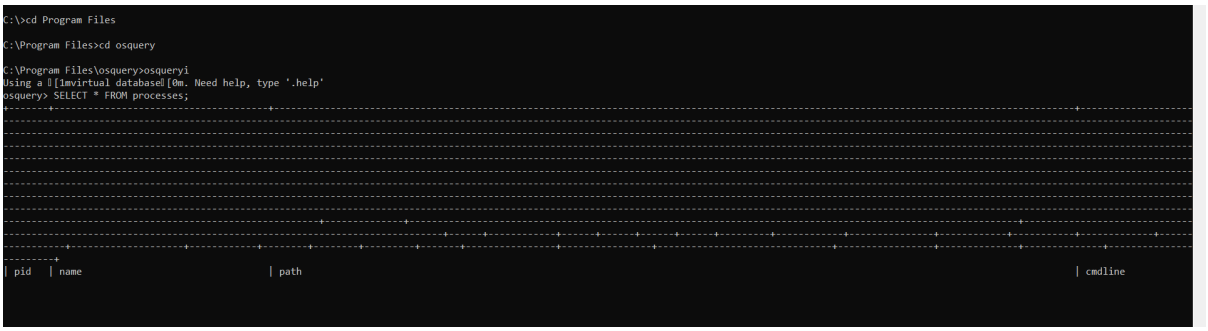

Fig 12: Osquery used to monitor running processes on endpoint

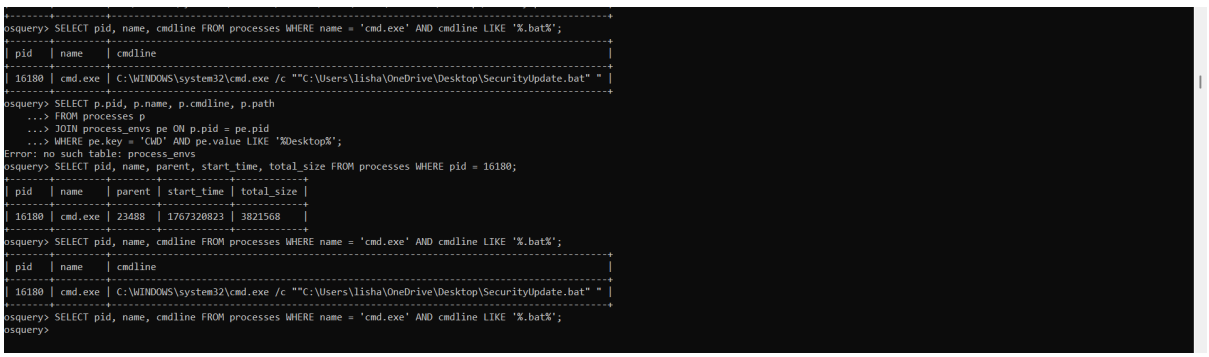

Fig 13: Simulated suspicious process observed through Osquery

Basic Security Concepts

Fundamentals of security are the basis of information security and the operations of a SOC. The knowledge of security concepts enables a security professional to understand threats, manage risks, and employ the relevant security measures.

This report covers the fundamental concepts of the CIA triad, the distinction between threats and vulnerabilities, and new models of security, including defense-in-depth and zero trust.

CIA Triad

The CIA triad encapsulates the three core aims of information security, which are:

- ***Confidentiality***: Confidentiality guarantees that only authorized persons can view sensitive data. This is done through control measures such as authentication, authorization, encryption.

  Example: Controlling access to customer data through role-based access control (RBAC).
- ***Integrity***: Integrity ensures that information is accurate and has not been tampered with during storage and transmission. Methods such as checksum and digital signatures are used.

  Example: Verification of the integrity of files by using hash values to identify unauthorized modifications.
- ***Availability***: Availability also ensures that the system data can be accessed whenever they are required. It entails concepts such as backup, redundancy, or denial-of-service attack.

  Example: Load balancers and system backup to provide system availability during system failure.

Threat, Vulnerability, and Risk

Threat: A threat is anything which might potentially cause damage, which exploits a vulnerability in a system. Threats might be natural, accidental, or deliberate.

Example: A hacker targeting a web app.

Vulnerability: A vulnerability refers to the weakness or defect present in the system, which can be acted upon by a threat.

Example: An unsupported software version with known vulnerabilities.

Risk: A function of the likelihood and potential impact of a threat exploiting a vulnerability.

Example: High-risk will be incurred when there is a vulnerability in the critical system that is internet exposed.

Defense-in-Depth

Defense-in-depth refers to a security concept that involves the use of diverse security measures. When one security measure fails, the next provides the needed security.

Common layers include:

- Firewalls in networks
- Intrusion Detection/Prevention Systems
- Endpoint protection
- Access control policies
- Security monitoring and logging

Zero Trust model

The Zero Trust model functions with the method of “never trust, always verify.” It does not trust any user or device irrespective of whether they are inside the network perimeter or not.

Key principles of Zero Trust include:

- Continuous Authentication and Authorization
- Authentication and Authorization
- Least privilege access
- Continuous monitoring

Security Operations workflow

A Security Operations workflow outlines the procedures involved as the SOC responds to a security event or alert that has been identified. In an orderly workflow, security incidents will be addressed effectively, with as little disruption as possible to the business, and on a consistent basis.

Stages of Security Operations Workflow

1. Detection: The very first step under this subcategory is Detection which refers to the identification of a potential security incident. An alert is produced by other security applications such as SIEM, EDR solutions, IDS systems, and email security gateways.

Examples of detection sources:

- SIEM alerting on suspicious login activity
- EDR alerts on malware activities
- Anti-phishing notifications in email security

An alert/security incident or event is generated for further analysis.

2. Triage: Triage is a process whereby the alert is evaluated for its severity, trustworthiness, and urgency. The analysts determine whether it is a true positive or a false positive alert.

Triage factors would include:

- The severity level (Low/Medium/High)
- Asset Criticality
- User impact
- Known threat indicators

Alerts are prioritized, either escalated or closed.

3. Investigation:

During this phase, the analysts go for in-depth analysis to comprehend the scope and impact of the incident. In addition, several data sources are also correlated.

Investigation activities include the following:

- Log correlation across SIEM data
- IOC hunting - IP, domain, hash
- E-mail header analysis (phishing)
- Checking Activity of an endpoint

The root cause of the incident and its impact are identified.

4. Response

Response actions are taken to stop and remediate the incident.

Common response actions:

- Containment of the affected systems.
- Blocking malicious IPs or domains
- Reset compromised credentials
- Malware removal

The threat has been neutralized and systems have gone into secure mode.

Phishing Email Incident Workflow

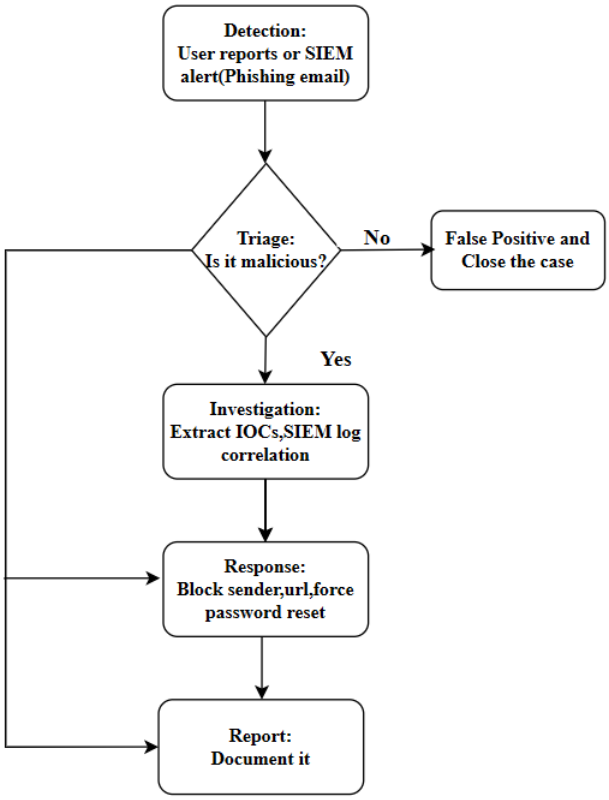

Fig14: Flowchart for phishing email incident

1. Detection (Trigger Stage)

The workflow starts when there is identification of a potential phishing incident. This can be via:

A user reporting a suspicious email via a "Report Phish" option

Automated detection via SIEM, which would involve malicious link identification or anomalous login behavior.

2. Triage (Decision Stage)

This is the most important stage in triaging for workflow.Thus, the objective is to check whether it is a true or false positive.

If the email is confirmed to be safe, the incident will be closed to avoid unnecessary investigation. In case the email is malicious, the incident is escalated for further analysis.

3. Investigation - Analysis Stage

Once identified to be malicious, the analyst proceeds with a deep investigation to determine the impact:

Uniform Resource Locator, sender IP, file hash

Log correlation in order to find other users that may have been affected

4. Response (Mitigation Stage)

Response actions are undertaken to prevent the attack and limit the impact:

Malicious emails are quarantined or deleted from all the mailboxes.

Malicious domains are blocked and affected user credentials are reset.

5. Reporting (Documentation Phase)

All actions and findings are documented into the incident management system. Example: TheHive. This information is afterwards used for incident post-analysis and improvement of detection rules in the future.

Incident Response Basics

Incident Response (IR) is the systematic approach that organizations use to identify, deal with, and recover from information security-related events, commonly known as cybersecurity threats. An effective IR procedure can mitigate the effects of an incident, restore business operations quickly, and prevent a possible future occurrence.

1. Preparation

Preparation is considered the key to incident response preparedness and readiness. It is at this stage that organizations set policies and processes for dealing with incidents.

Key activities are:

- Developing Response Planning and Playbooks
- Role Definition/Roles & Responsibilities
- Use of security technology like SIEM and EDR solutions
- Engaging employees in awareness training

The organization is prepared to detect and respond to any incident efficiently.

2.Identification

Identification of a security incident and verification that it has happened. In the Alert phase, true alerts are distinguished from False Positives.

Common Identification Sources:

- SIEM notifications
- User Reports
- IDS & IPS detections
- Endpoint security alerts

A validated incident is recorded and classified according to severity level or type.

3. Containment

Containment aims at controlling the effects of the incident. The incident is isolated by containing the affected system.

Containment strategies are characterized by :

- Disconnecting the Infected Systems from the Network
- Disabling compromised user accounts
- Blocking malicious IPs or domains

The incident is controlled and prevented from causing further damage.

4. Eradication

In the process of eradicating the problem, the root cause is eliminated from the environment or system.

Examples of Eradication actions:

- Removing Malware
- Closing vulnerabilities
- Deleting Malicious Files/Mechanisms of Persistence

The danger has been completely removed from the system.

5. Recovery

Recovery ensures that systems that have been affected are returned to a normal operation status in a secure way.

Recovery operations encompass:

- Restoration of Systems Using Clean Backups
- Systems for monitoring abnormal behaviors
- Reestablishing System Connections to the Network

All business activities continue uninterrupted.

6. Lessons Learned

This is the last phase that aims at optimizing incident response.

Key actions include:

Recording the timeline of the event and the reaction to it.

Determining gaps in detection or response.

Updating policies and security controls.

Documentation Standards

Documentation plays an integral role as part of Security Operations. Documentation helps ensure incidents are consistently addressed, and there is learned experience, so subsequent incidents can be addressed more quickly. Typical examples of security operation center documentation include incident reports, runbooks, Standard Operating Procedures, and post-incident reviews.

Types of SOC Documentation

- Incident Reports
  They are used for documenting security events from detection through to resolution. They contain information like the time the incident happened, its impact, actions, and the final resolution.
- Runbooks
  Detailed step-by-step procedures to determine how particular incidents should be responded to, such as phishing, malware, and DDoS attacks.
- Standard Operating Procedures (SOPs)
  Formal processes that outline normal SOC activities, roles, and escalation routes.
- Post Documents made after completion of events to determine what happened wrong, what happened right, and what needs to improve.

Practical Application

Log Analysis Practice

- Analyze Windows security logs to detect brute-force login attempts.
- Identify failed login events using specific Event IDs.
- Perform browser history analysis to identify potentially malicious URLs using forensic tools.
- Gain hands-on experience with log analysis tools used in SOC environments.

Steps performed:

- Opened Windows Event Viewer
- Navigated to Windows Logs → Security
- Applied filters for:
- Event ID 4625 – Failed login attempts

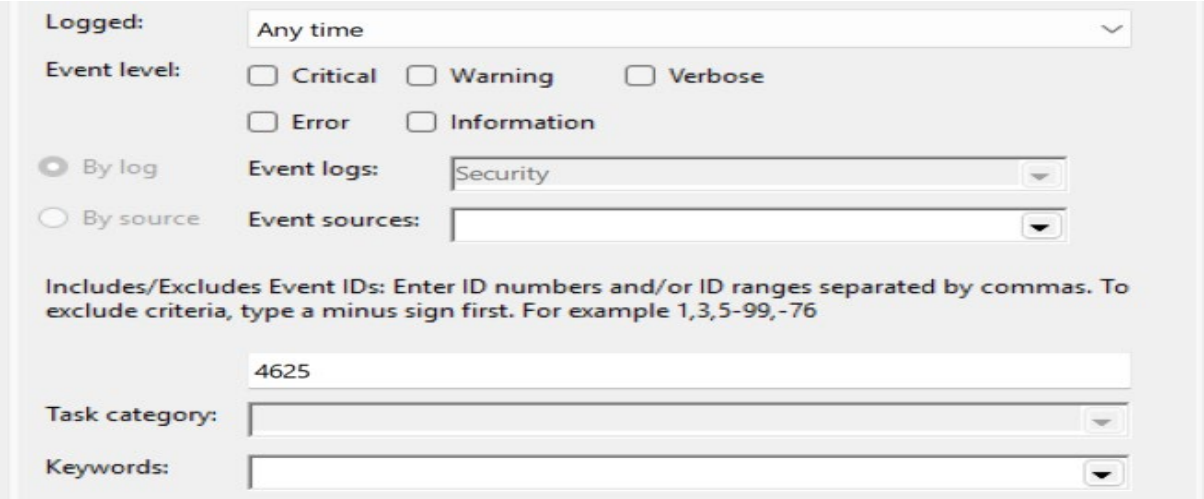

Fig 15: Filter 4625 applied

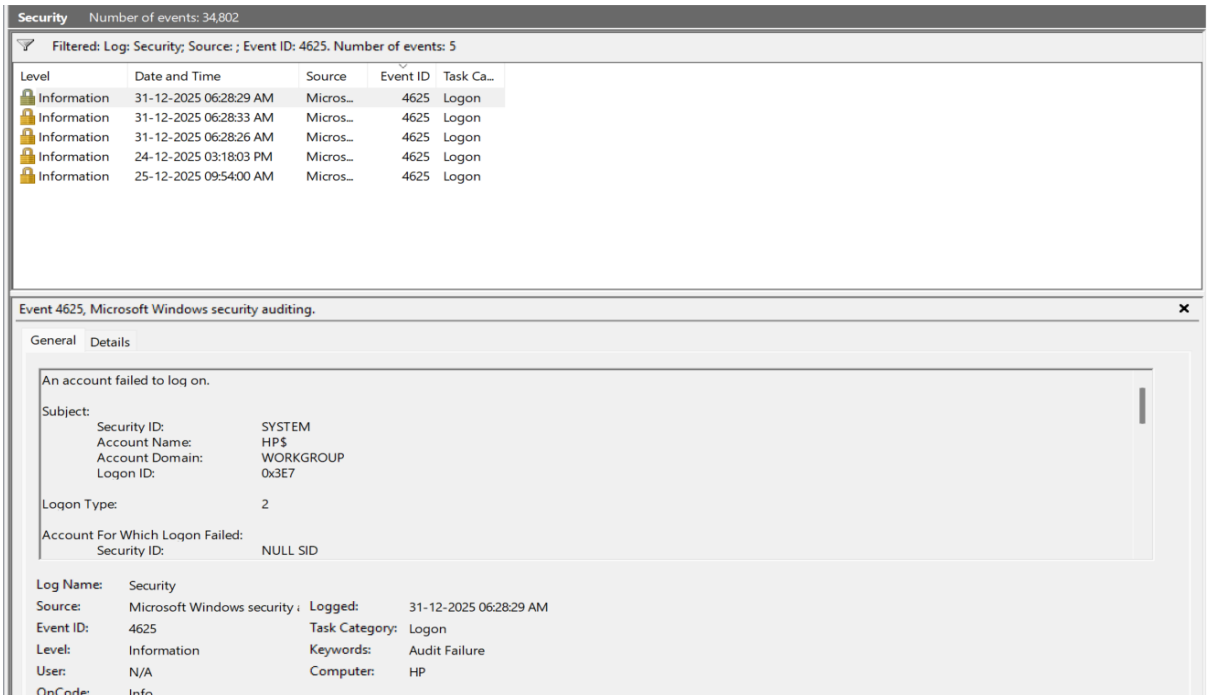

Fig 16: Filter 4625 applied

Multiple incorrect password attempts were generated intentionally in the Windows VM to simulate a brute-force attack. These failed login attempts generated Event ID 4625 entries. Repeated failed login attempts from the same account/IP indicate a potential brute-force attack. Event ID 4625 logs contained:

- Account name
- Logon type
- Source
- Event id

Document Security Events

Date and time	Source IP	Event ID	Description	Action taken
28-12-2025 10:02 AM	192.168.1.15	4625	There were several failed login attempts that occurred from the same IP address; this may be a brute force attack on a user account	IP was monitored for further events, and login attempts were analyzed. The account holder was notified to validate their login details.
28-12-2025 10:05 AM	192.168.1.20	4624	A successful login was detected after previous failed attempts, which could indicate a compromised account.	The login activity was confirmed to ensure it was a genuine user. No malicious activity was detected once logged in.

28-12-2025 10:10 AM	192.168.1.25	7045	A new service was installed on this system. This could represent unauthorized persistence if it is not authorized.	Details of the service were checked. They confirmed the legitimacy of the system update, and no further action was necessary.

Set Up Monitoring Dashboards

To visualize security data and quickly identify suspicious behavior using dashboards in Kibana.

Steps Performed

- Created a data view for ingested security logs in Kibana.
- Built visualizations using parsed log fields.
- Used aggregation-based charts to monitor security trends.
- Verified that dashboards updated automatically as new logs were ingested.

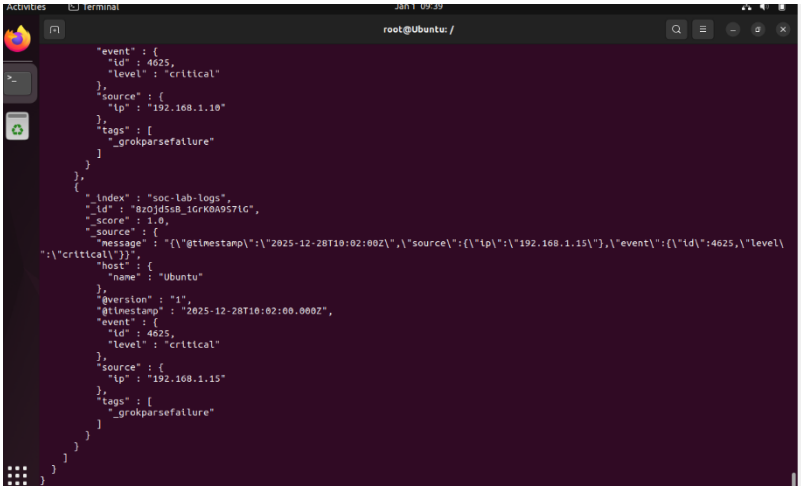

Fig 17: Log shown in json format

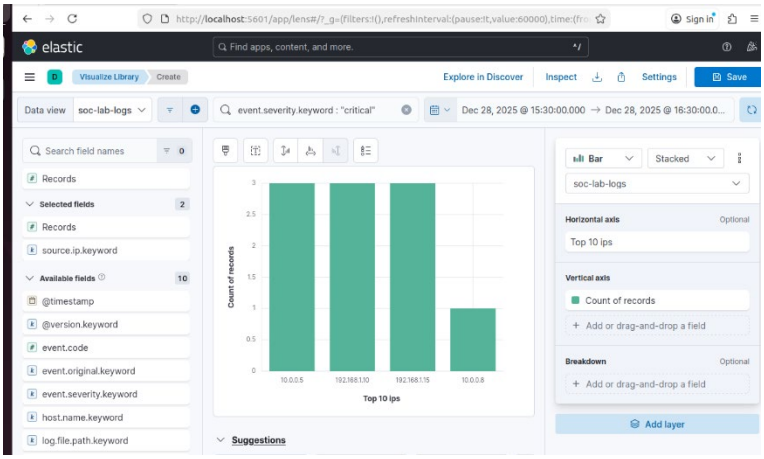

Fig 18: Chart showing Top 10 Source IPs Generating Alerts

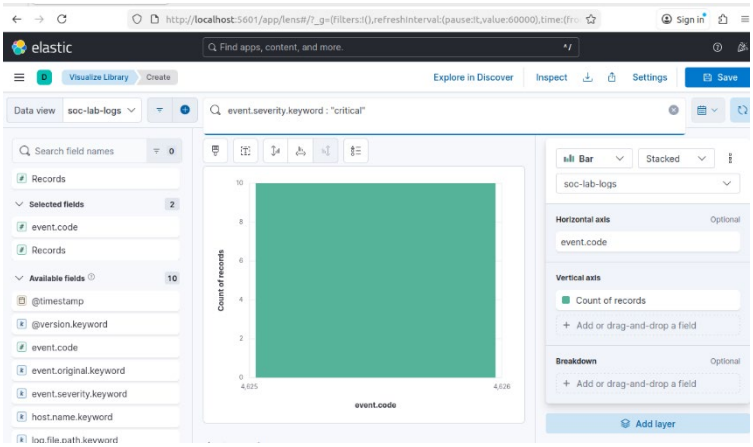

Fig 19: Chart showing frequency of critical event ids

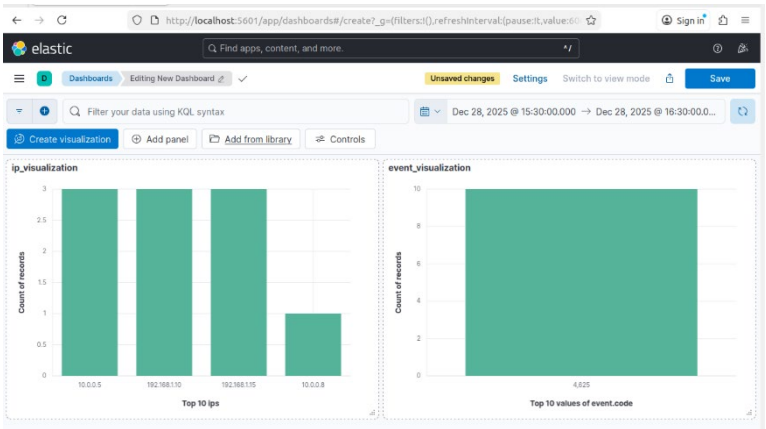

Fig 20: Dashboard showing both charts

Configure Alert Rules

The focus was to create an alert rule that would detect multiple failed login attempts within a small window of time. Conceptually, the Elastic SIEM rule logic was grasped and set up. The problem arose with the advanced task, as communications issues between the Wazuh agent and manager did not allow successful agent enrollment or testing of the alerts.
Rule logic: Find logins of 5+ failed logins within 5 minutes
Condition: count > 5
Index pattern: security-related login logs
Use case: Brute force detection

In an attempt to configure a custom Wazuh alert to alert on more than 3 failed login attempts within 2 minutes, the Wazuh agent failed to connect with the manager. This was attributed to configuration problems on the Wazuh agent. Consequently, Wazuh alert validation on the Wazuh dashboard failed.
However, despite this limitation, there was no misunderstanding regarding the logic of this rule, use case of detection, or expected behaviors.

Learnings

- Learned about the usage of failed login events (Event ID 4625) in detecting brute-force attacks.
- Understood the value of well-structured event reporting in incident handling.
- Acquired Windows Event Viewer filtering and log analysis skills.
- Understood the role of the Elastic SIEM dashboard in the overall security architecture.
- Gained understanding of how alert rules can be constructed using thresholds.
- It involves working with SOC-related tools, not just the results or outputs. Realized
- Better comprehension of log pipes (Logstash -> Elasticsearch -> Kibana).