

Security Assessment Report -2

Project Title:

Security Alert Monitoring & Incident Response Simulation (Project 2)

Prepared By:

Shashanka U N
Cybersecurity Intern
Future interns

Prepared For:

Future interns

Contents

- 1. Introduction**
- 2. Background and need**
- 3. Scope and objective**
- 4. Methodology**
- 5. Tools and technology**
- 6. Project preparation**
- 7. Results and analysis**
- 8. Vulnerability report**
- 9. Conclusion**

1. Introduction

The Security Operations Center (SOC) Task 2 project focuses on simulating real-world SOC operations through monitoring and responding to security alerts using a SIEM tool (Splunk). The logs analyzed include Linux system events, Windows event logs, and malware alerts, representing common security challenges.

The task involved detecting suspicious activities such as failed logins, unusual connections, file access anomalies, and malware detections. These events were reviewed, classified by severity, and documented in an incident response report. This exercise provided hands-on experience in log analysis, alert triage, and incident handling, helping to build essential SOC analyst skills. It highlights the importance of proactive monitoring and structured response in maintaining organizational security.

2. Background and Need

With the rise of advanced cyberattacks, organizations face constant threats such as account compromise, malware infections, and unauthorized access. Security Operations Centers (SOCs) play a crucial role in detecting, analyzing, and responding to these incidents in real time.

This project simulates SOC activities by using a SIEM (Splunk) to monitor and analyze simulated security logs. The primary need for this exercise is to understand how alerts are generated, identify suspicious behavior, and classify incidents by severity. By performing this hands-on analysis, I aim to strengthen my skills in log analysis, incident classification, and response planning — skills that are vital for any SOC analyst.

3. Scope & Objectives

Scope

This report focuses on analyzing and classifying simulated security logs within a SIEM environment. The scope is limited to:

- Linux system logs (authentication, file access, malware detections).
- Windows security logs (logon events, access attempts, anomalies).
- Malware detection alerts (rootkit, trojan, ransomware, worm infections).
- Incident reporting and response recommendations.

Objectives

- The main objectives of this project are:
- To gain practical experience in **SIEM monitoring and log analysis**.
- To detect and classify **suspicious events** from Linux, Windows, and malware logs.
- To document findings with evidence from the SIEM dashboard.

4. Methodology

This assessment was conducted using a structured SOC investigation methodology aligned with industry best practices. The process included the following phases:

1. Log Collection

- Uploaded simulated Linux, Windows, and malware logs into Splunk.
- Configured appropriate source types for accurate parsing.

2. Alert Analysis

- Queried logs for failed logins, unusual IP activity, file access anomalies, and malware alerts.
- Grouped alerts into categories (Authentication, Malware, Connections, File Access).

3. Incident Classification

- Classified alerts into **High, Medium, and Low severity** based on risk and impact.
- Identified patterns of potential attacks such as brute force attempts and malware infections.

4. Incident Response

- Assessed the impact of suspicious activities on system security.
- Suggested remediation actions such as account lockouts, malware cleanup, and monitoring.

5. Documentation & Reporting

- Consolidated findings with evidence from Splunk queries and screenshots.
- Drafted an **Incident Response Report** with a timeline, severity ratings, and recommendations.

5. Tools and Technologies

- **Splunk (Free Trial):** SIEM platform used for ingesting, parsing, and analyzing logs.
- **Sample SOC Logs:** Provided datasets containing Linux, Windows, and malware events.

6. Project Setup

6.1 Installing and Configuring Splunk SIEM

Splunk, a Security Information and Event Management (SIEM) platform, was used to ingest and analyze simulated logs in a controlled environment. This setup ensured centralized log management and streamlined alert investigation.

- The **Splunk Enterprise Free Trial** was installed on the host system (Windows/Linux).
- Installation was verified by accessing the Splunk web interface at:

`http://localhost:8000`

- An **admin account** was created during the setup to allow access to the Splunk dashboard and configuration features.
- Splunk services were confirmed to be running using the command:
Bash: ./splunk status

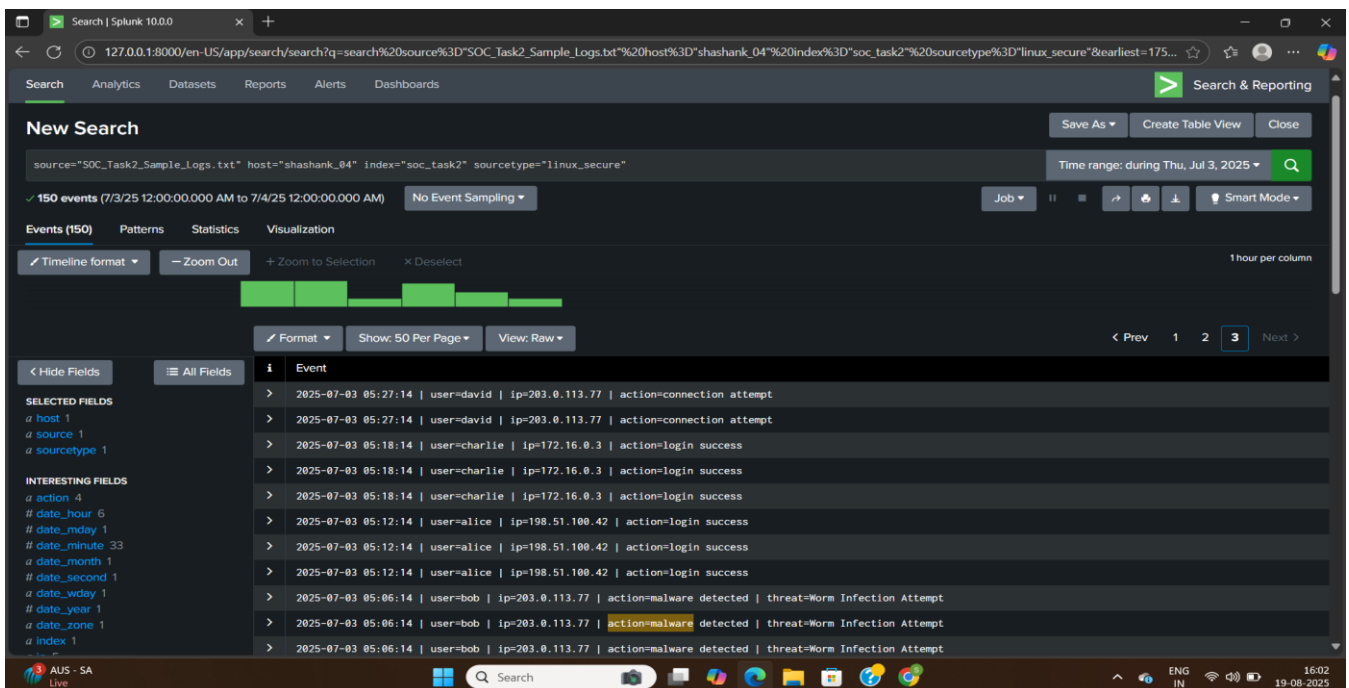
6.2 Ingesting Security Logs into Splunk

- To simulate SOC activities, sample log datasets were ingested into Splunk for monitoring and analysis.
- Security logs included Linux system logs, Windows event logs, and malware detection alerts.
- Logs were uploaded in .txt format using Splunk's Upload Data feature.
- Appropriate sourcetypes were configured (syslog for Linux, WinEventLog for Windows, custom for malware alerts) to ensure proper parsing.
- Indexes were created for each log type (linux_index, windows_index, malware_index) to separate data for analysis.

7. Results & Analysis

7.1 Linux Logs Analysis

- Multiple **failed login attempts** from external IPs (possible brute-force attempt).
- Successful logins from unusual IPs (possible compromised credentials).
- Malware alerts such as **Trojan Detected** and **Rootkit Signature** found in system activity.



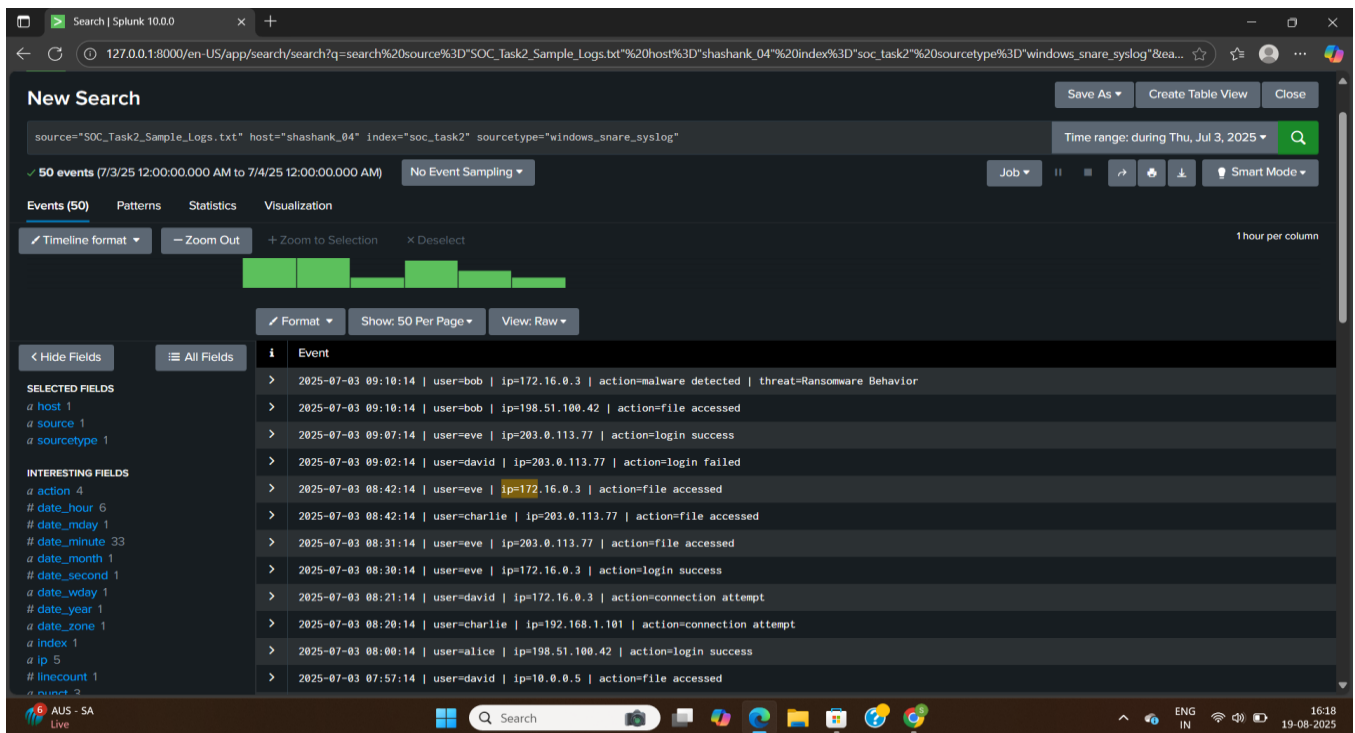
The screenshot shows the Splunk Search interface with the following details:

- Search Bar:** Contains the search query: `source="SOC_Task2_Sample_Logs.txt" host="shashank_04" index="soc_task2" sourcetype="linux_secure"`.
- Results Summary:** 150 events (7/3/25 12:00:00 AM to 7/4/25 12:00:00 AM). No Event Sampling.
- Visualizations:** A bar chart showing event counts over time.
- Event List:**

_type	_source	_sourcetype	_index	_date	_time	_host	_user	_ip	_action	_threat
linux_secure	/var/log/auth.log	linux_secure	soc_task2	2025-07-03	05:27:14	shashank_04	david	203.0.113.77	connection attempt	
linux_secure	/var/log/auth.log	linux_secure	soc_task2	2025-07-03	05:27:14	shashank_04	david	203.0.113.77	connection attempt	
linux_secure	/var/log/auth.log	linux_secure	soc_task2	2025-07-03	05:18:14	shashank_04	charlie	172.16.0.3	login success	
linux_secure	/var/log/auth.log	linux_secure	soc_task2	2025-07-03	05:18:14	shashank_04	charlie	172.16.0.3	login success	
linux_secure	/var/log/auth.log	linux_secure	soc_task2	2025-07-03	05:18:14	shashank_04	charlie	172.16.0.3	login success	
linux_secure	/var/log/auth.log	linux_secure	soc_task2	2025-07-03	05:12:14	shashank_04	alice	198.51.100.42	login success	
linux_secure	/var/log/auth.log	linux_secure	soc_task2	2025-07-03	05:12:14	shashank_04	alice	198.51.100.42	login success	
linux_secure	/var/log/auth.log	linux_secure	soc_task2	2025-07-03	05:12:14	shashank_04	alice	198.51.100.42	login success	
linux_secure	/var/log/auth.log	linux_secure	soc_task2	2025-07-03	05:06:14	shashank_04	bob	203.0.113.77	malware detected	Worm Infection Attempt
linux_secure	/var/log/auth.log	linux_secure	soc_task2	2025-07-03	05:06:14	shashank_04	bob	203.0.113.77	malware detected	Worm Infection Attempt
linux_secure	/var/log/auth.log	linux_secure	soc_task2	2025-07-03	05:06:14	shashank_04	bob	203.0.113.77	malware detected	Worm Infection Attempt

7.2 Windows Logs Analysis

- Repeated login failures on critical accounts.
- Malware-related events such as Worm Infection Attempt and Spyware Alerts.
- Abnormal file access patterns by users outside of normal business hours.
- Evidence of connection attempts from suspicious IPs.



7.3 Malware Detection Logs

- Alerts for **Trojan, Worm, Spyware, and Ransomware** activities were observed.
- Repeated detections across different hosts indicate a **coordinated attack** rather than isolated incidents.
- High-severity malware events corresponded with login anomalies, strengthening the incident case.

7.4 Alert Prioritization

- **High Severity:** Malware detections (Trojan, Ransomware, Rootkit), repeated failed logins from the same IP.
- **Medium Severity:** Multiple connection attempts from unusual IPs.
- **Low Severity:** Single failed login attempts or routine file access.

8. Incident Response Report

Timestamp	User	IP	Event	Severity
04:19	alice	198.51.100.42	Malware detected (Rootkit Signature)	High
04:23	bob, charlie	172.16.0.3 / 198.51.100.42	Login failed	Medium
08:21	david	172.16.0.3	Multiple connection attempts	Medium
08:30	eve	172.16.0.3	Login success from unusual IP	High
09:10	bob	172.16.0.3	Malware detected(Ransom ware Behaviour)	High

9. Conclusion

This project gave me hands-on experience in SOC operations, especially log monitoring and incident response. By analyzing Linux and Windows logs, I detected suspicious activities such as failed logins, unusual file access, and malware alerts like Ransomware, Trojans, Rootkits, and Worms.

The exercise showed how attackers attempt unauthorized access and spread malware, highlighting the need for continuous monitoring. I also practiced classifying alerts, assessing impact, and suggesting remediation steps.