Security Operations Centre (SOC)

Submitted By:

Kanishka Mishra

CIN ID:

FIT/DEC25/CS5207

Domain:

Cyber Security / SOC Operations

Project Title:

Security Alert Monitoring & Incident Response Simulation

Tools Used:

Sample SOC Logs, Manual Log Analysis

Submission Date:

26th December 2025

INTRODUCTION

A Security Operations Centre (SOC) plays a critical role in monitoring, detecting, and responding to cybersecurity threats in real time. SOC analysts continuously analyse security alerts and system logs to identify suspicious activities that may indicate cyberattacks such as malware infections, unauthorized access attempts, or network intrusions.

This project focuses on simulating the responsibilities of a SOC analyst by analysing provided sample security logs. The objective is to identify malware-related alerts, assess their severity, and document appropriate incident response actions. Through this task, practical exposure to alert triage, threat identification, and incident reporting is achieved, reflecting real-world SOC operations.

Objective

The primary objectives of this task are:

- To understand how SOC analysts monitor and analyse security alerts
- To identify malware-related alerts from system logs
- To classify incidents based on severity and risk
- To document an incident response with impact and remediation steps
- To gain hands-on experience in alert analysis and SOC reporting

TOOLS & TECHNOLOGIES USED

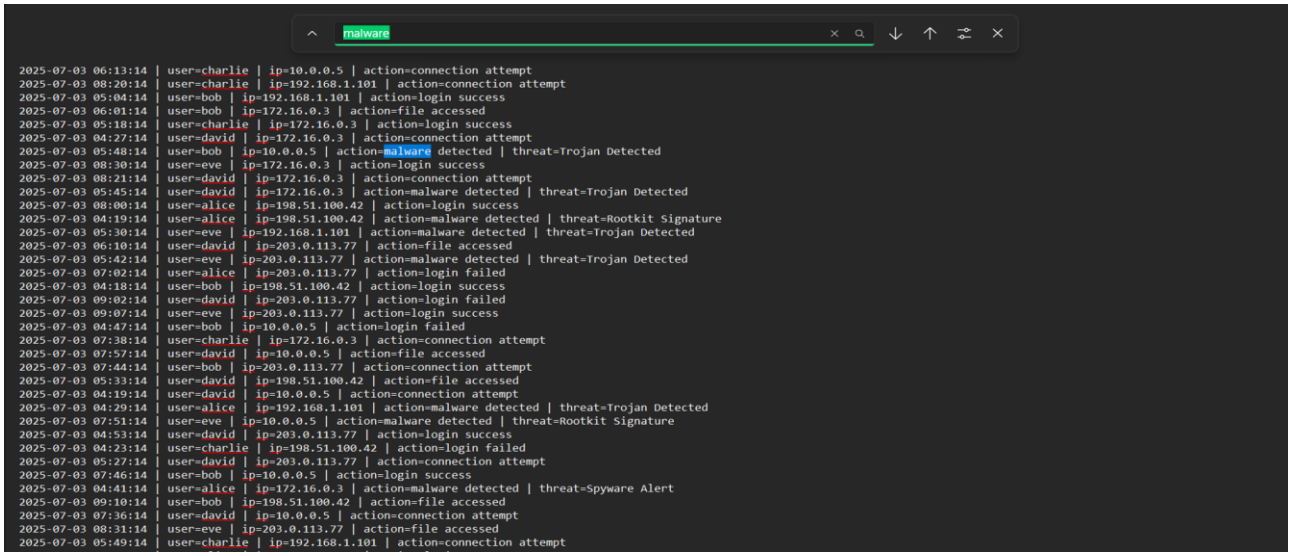
The following tools and resources were used to complete this task:

- **Sample SOC Logs:** Provided simulated logs containing malware alerts and system events
- **Notepad:** Used for manual log analysis and keyword searching
- **Operating System:** Windows
- **Documentation Tools:** Google Docs / Microsoft Word for report preparation

Identified Security Alerts

During the analysis of the provided SOC sample logs, multiple malware-related security alerts were identified. These alerts indicate the presence of malicious activity such as Trojan infections, Rootkit signatures, and Spyware detection.

A total of four malware alerts were observed. Each alert was analysed based on event timestamp, affected user account, IP address, and action performed. Screenshots of the malware detection logs were captured as evidence of the identified threats.



```
malware

2025-07-03 06:13:14 | user=charlie | ip=10.0.0.5 | action=connection attempt
2025-07-03 08:20:14 | user=charlie | ip=192.168.1.101 | action=connection attempt
2025-07-03 05:04:14 | user=bob | ip=192.168.1.101 | action=login success
2025-07-03 06:01:14 | user=bob | ip=172.16.0.3 | action=file accessed
2025-07-03 05:18:14 | user=charlie | ip=172.16.0.3 | action=login success
2025-07-03 04:27:14 | user=david | ip=172.16.0.3 | action=connection attempt
2025-07-03 05:48:14 | user=bob | ip=10.0.0.5 | action=malware detected | threat=Trojan Detected
2025-07-03 08:30:14 | user=eve | ip=172.16.0.3 | action=login success
2025-07-03 08:21:14 | user=david | ip=172.16.0.3 | action=connection attempt
2025-07-03 05:45:14 | user=david | ip=172.16.0.3 | action=malware detected | threat=Trojan Detected
2025-07-03 08:00:14 | user=alice | ip=198.51.100.42 | action=login success
2025-07-03 04:19:14 | user=alice | ip=198.51.100.42 | action=malware detected | threat=Rootkit Signature
2025-07-03 05:30:14 | user=eve | ip=192.168.1.101 | action=malware detected | threat=Trojan Detected
2025-07-03 06:10:14 | user=david | ip=203.0.113.77 | action=file accessed
2025-07-03 05:42:14 | user=eve | ip=203.0.113.77 | action=malware detected | threat=Trojan Detected
2025-07-03 07:02:14 | user=alice | ip=203.0.113.77 | action=login failed
2025-07-03 04:18:14 | user=bob | ip=198.51.100.42 | action=login success
2025-07-03 09:02:14 | user=david | ip=203.0.113.77 | action=login failed
2025-07-03 09:07:14 | user=eve | ip=203.0.113.77 | action=login success
2025-07-03 04:47:14 | user=bob | ip=10.0.0.5 | action=login failed
2025-07-03 07:38:14 | user=charlie | ip=172.16.0.3 | action=connection attempt
2025-07-03 07:57:14 | user=david | ip=10.0.0.5 | action=file accessed
2025-07-03 07:44:14 | user=bob | ip=203.0.113.77 | action=connection attempt
2025-07-03 05:33:14 | user=david | ip=198.51.100.42 | action=file accessed
2025-07-03 04:19:14 | user=david | ip=10.0.0.5 | action=connection attempt
2025-07-03 04:29:14 | user=alice | ip=192.168.1.101 | action=malware detected | threat=Trojan Detected
2025-07-03 07:51:14 | user=eve | ip=10.0.0.5 | action=malware detected | threat=Rootkit Signature
2025-07-03 04:53:14 | user=david | ip=203.0.113.77 | action=login success
2025-07-03 04:23:14 | user=charlie | ip=198.51.100.42 | action=login failed
2025-07-03 05:27:14 | user=david | ip=203.0.113.77 | action=connection attempt
2025-07-03 07:46:14 | user=bob | ip=10.0.0.5 | action=login success
2025-07-03 04:41:14 | user=alice | ip=172.16.0.3 | action=malware detected | threat=Spyware Alert
2025-07-03 09:10:14 | user=bob | ip=198.51.100.42 | action=file accessed
2025-07-03 07:36:14 | user=david | ip=10.0.0.5 | action=connection attempt
2025-07-03 08:31:14 | user=eve | ip=203.0.113.77 | action=file accessed
2025-07-03 05:49:14 | user=charlie | ip=192.168.1.101 | action=connection attempt
```

Figure 1: Malware Detection Alert – Trojan

```
malware
2025-07-03 06:13:14 | user=charlie | ip=10.0.0.5 | action=connection attempt
2025-07-03 08:20:14 | user=charlie | ip=192.168.1.101 | action=connection attempt
2025-07-03 05:04:14 | user=bob | ip=192.168.1.101 | action=login success
2025-07-03 06:01:14 | user=bob | ip=172.16.0.3 | action=file accessed
2025-07-03 05:18:14 | user=charlie | ip=172.16.0.3 | action=login success
2025-07-03 04:27:14 | user=david | ip=172.16.0.3 | action=connection attempt
2025-07-03 05:48:14 | user=bob | ip=10.0.0.5 | action=malware detected | threat=Trojan Detected
2025-07-03 08:30:14 | user=eve | ip=172.16.0.3 | action=login success
2025-07-03 08:21:14 | user=david | ip=172.16.0.3 | action=connection attempt
2025-07-03 05:45:14 | user=david | ip=172.16.0.3 | action=malware detected | threat=Trojan Detected
2025-07-03 08:00:14 | user=alice | ip=198.51.100.42 | action=login success
2025-07-03 04:19:14 | user=alice | ip=198.51.100.42 | action=malware detected | threat=Rootkit Signature
2025-07-03 05:30:14 | user=eve | ip=192.168.1.101 | action=malware detected | threat=Trojan Detected
2025-07-03 06:10:14 | user=david | ip=203.0.113.77 | action=file accessed
2025-07-03 05:42:14 | user=eve | ip=203.0.113.77 | action=malware detected | threat=Trojan Detected
2025-07-03 07:02:14 | user=alice | ip=203.0.113.77 | action=login failed
2025-07-03 04:18:14 | user=bob | ip=198.51.100.42 | action=login success
2025-07-03 09:02:14 | user=david | ip=203.0.113.77 | action=login failed
2025-07-03 09:07:14 | user=eve | ip=203.0.113.77 | action=login success
2025-07-03 04:47:14 | user=bob | ip=10.0.0.5 | action=login failed
2025-07-03 07:38:14 | user=charlie | ip=172.16.0.3 | action=connection attempt
2025-07-03 07:57:14 | user=david | ip=10.0.0.5 | action=file accessed
2025-07-03 07:44:14 | user=bob | ip=203.0.113.77 | action=connection attempt
2025-07-03 05:33:14 | user=david | ip=198.51.100.42 | action=file accessed
2025-07-03 04:19:14 | user=david | ip=10.0.0.5 | action=connection attempt
2025-07-03 04:29:14 | user=alice | ip=192.168.1.101 | action=malware detected | threat=Trojan Detected
2025-07-03 07:51:14 | user=eve | ip=10.0.0.5 | action=malware detected | threat=Rootkit Signature
2025-07-03 04:53:14 | user=david | ip=203.0.113.77 | action=login success
2025-07-03 04:23:14 | user=charlie | ip=198.51.100.42 | action=login failed
2025-07-03 05:27:14 | user=david | ip=203.0.113.77 | action=connection attempt
2025-07-03 07:46:14 | user=bob | ip=10.0.0.5 | action=login success
2025-07-03 04:41:14 | user=alice | ip=172.16.0.3 | action=malware detected | threat=Spyware Alert
```

Figure 2: Malware Detection Alert – Rootkit

```
2025-07-03 05:27:14 | user=david | ip=203.0.113.77 | action=connection attempt
2025-07-03 07:46:14 | user=bob | ip=10.0.0.5 | action=login success
2025-07-03 04:41:14 | user=alice | ip=172.16.0.3 | action=malware detected | threat=Spyware Alert
2025-07-03 09:10:14 | user=bob | ip=198.51.100.42 | action=file accessed
2025-07-03 07:36:14 | user=david | ip=10.0.0.5 | action=connection attempt
2025-07-03 08:31:14 | user=eve | ip=203.0.113.77 | action=file accessed
2025-07-03 05:49:14 | user=charlie | ip=192.168.1.101 | action=connection attempt
```

Figure 3: Malware Detection Alert – Spyware

```
2025-07-03 05:06:14 | user=bob | ip=203.0.113.77 | action=malware detected | threat=Worm Infection Attempt
2025-07-03 08:42:14 | user=charlie | ip=203.0.113.77 | action=file accessed
2025-07-03 09:10:14 | user=bob | ip=172.16.0.3 | action=malware detected | threat=Ransomware Behavior
2025-07-03 04:46:14 | user=david | ip=203.0.113.77 | action=login success
2025-07-03 08:42:14 | user=eve | ip=172.16.0.3 | action=file accessed
2025-07-03 07:22:14 | user=charlie | ip=192.168.1.101 | action=connection attempt
```

Figure 4: Malware Detection Alert – Worm Infection Attempt

```
2025-07-03 09:10:14 | user=bob | ip=172.16.0.3 | action=malware detected | threat=Ransomware Behavior
2025-07-03 04:46:14 | user=david | ip=203.0.113.77 | action=login success
2025-07-03 08:42:14 | user=eve | ip=172.16.0.3 | action=file accessed
2025-07-03 07:22:14 | user=charlie | ip=192.168.1.101 | action=connection attempt
2025-07-03 04:53:14 | user=alice | ip=203.0.113.77 | action=file accessed
2025-07-03 07:45:14 | user=charlie | ip=172.16.0.3 | action=malware detected | threat=Trojan Detected
2025-07-03 05:44:14 | user=bob | ip=198.51.100.42 | action=file accessed
Ln 44, Col 64   7 of 4,010 characters   Plain text
```

Figure 5: Malware Detection Alert – Ransomware Behaviour

INCIDENT IDENTIFICATION & ANALYSIS

During log analysis, multiple malware-related alerts were identified by searching for the keyword “Malware” in the log file. These alerts indicate malicious activity detected on the system and require immediate attention.

Alert id	Alert type	Threat name	Severity
1	Malware	Trojan Detected	High
2	Malware	Rootkit Signature	High
3	Malware	Spyware Alert	Medium
4	Malware	Ransomware Behavior	Critical
5	Malware	Worm Infection	High

Incident Response Actions & Recommendations

1. Containment Actions
   - Immediately isolate affected systems from the network
   - Disable suspicious user accounts temporarily
   - Block malicious IP addresses detected in the logs
   - Stop execution of any identified malware processes
2. Eradication Steps
   - Perform a full malware scan on impacted machines
   - Remove Trojan, Worm, or Rootkit components if detected
   - Patch vulnerable applications and update antivirus signatures

- Reset passwords for potentially compromised users

3. Recovery Plan

- Restore clean system backups if required
- Re-enable user accounts after verification
- Monitor systems for recurring suspicious activity
- Validate normal business operations before closure

4. Preventive Measures

- Enable Multi-Factor Authentication (MFA)
- Apply regular security patching
- Conduct user awareness training
- Implement network-level threat monitoring
- Restrict administrative privileges
- Incident Response Summary & Communication Plan

Incident Response Summary

- During the SOC monitoring activity, multiple malware-related alerts were detected in the sample system logs. These alerts indicated the presence of malicious files and potentially compromised systems. The alerts were analyzed and categorized based on severity to understand the level of threat.
- High-severity alerts were treated as priority because they indicate active malware presence. Medium-level alerts indicated suspicious activity requiring follow-up monitoring. No confirmed system shutdown or data breach was detected during the analysis, but the alerts suggested that immediate security action would be required in a real-world environment.
- Incident Response Summary & Communication Plan

Incident Response Summary

- During the SOC monitoring activity, multiple malware-related alerts were detected in the sample system logs. These alerts indicated the presence of malicious files and potentially compromised systems. The alerts were analyzed and categorized based on severity to understand the level of threat.
- High-severity alerts were treated as priority because they indicate active malware presence. Medium-level alerts indicated suspicious activity requiring follow-up monitoring. No confirmed system shutdown or data breach was detected during the analysis, but the alerts suggested that immediate security action would be required in a real-world environment.

References & Tools Used

- • Sample SOC Log File – Provided by Internship Mentor
- • Security Operations Concepts – SOC Best Practices
- • OWASP Security Learning Resources
- • Cybersecurity Log Analysis Fundamentals

- Skills Gained:
  - • Log Analysis
  - • Alert Triage
  - • Incident Documentation
  - • SOC Operations Awareness
- Tools Referred:
  - • SIEM Concepts
  - • Elastic Stack (ELK) – Reference
  - • Splunk Free Trial – Reference
  - • Text Log Review Tools