Incident Response Report

Task 2 – SECURITY ALERT MONITORING & INCIDENT RESPONSE

Prepared by: Nitish Patil

Date: September 17, 2025

Contents

Introduction

This Incident Response Report summarizes the analysis of simulated security logs using Splunk Cloud as part of the Cyber Security Internship Task 02 by Future Interns. The objective was to detect suspicious activities, classify incidents, and generate alerts to simulate the workflow of a SOC analyst.

The dataset used was `SOC_Task2_Sample_Logs.txt`, containing log entries such as authentication attempts, IP activity, and malware detections.

—

Chapter 1

Methodology

The following methodology was followed during the project:

1. Ingested the provided sample log dataset into Splunk Cloud.
2. Extracted fields (timestamp, user, IP, action, threat) using regex.
3. Built SPL queries to detect malware (Trojan, Rootkit, Ransomware).
4. Created alerts for each detection with automated email notification actions.
5. Constructed a SOC dashboard with a 2x2 layout to visualize detections.
6. Exported classification and results into CSVs for documentation.

—

Chapter 2

Key Findings

During analysis of the logs, the following suspicious activities were identified:

- Multiple **malware detections**, including Trojan, Rootkit, Worm, Spyware, and Ransomware.
- **Ransomware Behavior** detected for user `bob` from IP `172.16.0.3`.
- **Rootkit Signature** events for users `alice` (`198.51.100.42`) and `eve` (`10.0.0.5`).
- **Trojan Detected** on user `david` (`198.51.100.42`).

—

Chapter 3

Alert Classification

Alert ID	Alert Title	Severity	SPL Query (simplified)	Trigger Condition	Action
A-001	Malware Detected (General)	High	index=internship_logs sourcetype=TXT_logs host=SOC_TASK2 action="malware detected" | stats count by threat, user, ip	Number of results > 0	Send Email (SOC Team)
A-002	Ransomware Behavior Detected	High	index=internship_logs sourcetype=TXT_logs host=SOC_TASK2 action="malware detected" | search "Ransomware Behavior" | table _time user ip threat	Number of results > 0	Send Email (SOC Team)
A-003	Rootkit Signature Detected	High	index=internship_logs sourcetype=TXT_logs host=SOC_TASK2 action="malware detected" | search "Rootkit Signature" | table _time user ip threat	Number of results > 0	Send Email (SOC Team)
A-004	Trojan Detected	Medium-High	index=internship_logs sourcetype=TXT_logs host=SOC_TASK2 action="malware detected" | search "Trojan Detected" | table _time user ip threat	Number of results > 0	Send Email (SOC Team)

—

Chapter 4

Timeline of Events

The following timeline highlights key suspicious events detected:

Table 4.1: Malware General Detection Results (A-001)

Threat	User	IP Address	Count
Ransomware	bob	172.16.0.3	1
Rootkit	alice	198.51.100.42	1
Rootkit	eve	10.0.0.5	1
Spyware	alice	172.16.0.3	1
Trojan	alice	192.168.1.101	1
Trojan	bob	10.0.0.5	1
Trojan	charlie	172.16.0.3	1
Trojan	david	172.16.0.3	1
Trojan	eve	192.168.1.101	1
Trojan	eve	203.0.113.77	1
Worm	bob	203.0.113.77	1

Table 4.2: Ransomware Detection Results (A-002)

Time	User	IP Address	Threat
2025-07-03T09:10:14.000+0000	bob	172.16.0.3	Ransomware

Table 4.3: Rootkit Detection Results (A-003)

Time	User	IP Address	Threat
2025-07-03T04:19:14.000+0000	alice	198.51.100.42	Rootkit
2025-07-03T07:51:14.000+0000	eve	10.0.0.5	Rootkit

—

Table 4.4: Trojan Detection Results (A-004)

Time	User	IP Address	Threat
2025-07-03T04:29:14.000+0000	alice	192.168.1.101	Trojan
2025-07-03T05:42:14.000+0000	eve	203.0.113.77	Trojan
2025-07-03T05:30:14.000+0000	eve	192.168.1.101	Trojan
2025-07-03T05:45:14.000+0000	david	172.16.0.3	Trojan
2025-07-03T05:48:14.000+0000	bob	10.0.0.5	Trojan
2025-07-03T07:45:14.000+0000	charlie	172.16.0.3	Trojan

Chapter 5

Dashboard Overview

A Splunk dashboard was developed to visualize detections with the following panels:

- Malware by Type (Pie Chart)
- Ransomware Events (Table)
- Rootkit Events (Table)
- Trojan Detections (Bar Chart)

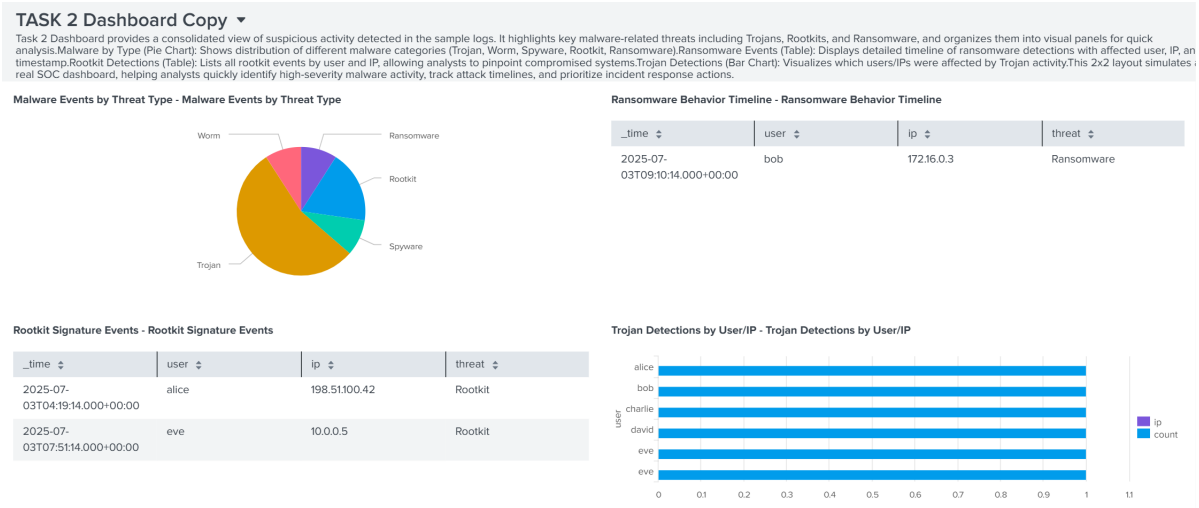

Figure 5.1: Task 2 Dashboard

Chapter 6

Incident Classification

- **A-001: Malware Detected (General)** – High Severity
- **A-002: Ransomware Behavior Detected** – High Severity
- **A-003: Rootkit Signature Detected** – High Severity
- **A-004: Trojan Detected** – Medium–High Severity

—

Chapter 7

Impact Assessment and Recommendations

Impact:

- At least four users (alice, bob, david, eve) showed malware infections.
- Multiple malware families were present, including ransomware and rootkits.
- Risk of credential compromise, lateral movement, and persistence mechanisms.

Recommendations:

1. Immediately isolate affected endpoints.
2. Reset passwords for impacted users.
3. Conduct forensic scans for persistence.
4. Apply security patches and update EDR signatures.
5. Continue monitoring for repeated infection attempts.

—

Conclusion

This simulated SOC task successfully demonstrated end-to-end monitoring, detection, and reporting using Splunk Cloud. The results confirmed the analyst's ability to identify, classify, and escalate high-impact incidents such as ransomware and rootkits, along with supporting documentation via dashboards and alerts.