

Incident Response Report – Task 2 (SOC Internship)

Table of Contents

- 1. Introduction
- 2. Incident Summary
- 3. Detection and Analysis
 - 3.1 Failed Login Attempts
 - 3.2 Malware Detection Alerts
 - 3.3 External IP Connections
- 4. Containment, Eradication, and Recovery
- 5. Lessons Learned

1. Introduction

This report documents the findings from Task 2 of the SOC Internship Program, focused on Security Alert Monitoring and Incident Response using Splunk. The goal of this exercise is to analyze simulated log data, detect suspicious activities, and recommend appropriate incident response actions.

2. Incident Summary

During the analysis of provided system logs, several suspicious activities were identified, including repeated failed login attempts, multiple malware detections, and connections from unusual external IP addresses. These findings suggest potential brute-force attempts, malware infections, and possible unauthorized access from outside the network.

3. Detection and Analysis

3.1 Failed Login Attempts

Search Query:
index=* action="login failed" | table _time, user, ip, action

SearchAnalyticsDatasetsReportsAlertsDashboards

Search & Reporting

New Search

Save AsCreate Table ViewClose

index=* action="login failed" | table _time, user, ip, action

Time range: All time

10 events (before 8/19/25 2:02:55.000 PM)No Event SamplingJobPauseRefreshDownloadPolicy-Based PoolSmart Mode

EventsPatternsStatistics (10)Visualization

Show: 20 Per PageFormatPreview: On

_time	user	ip	action
2025-07-03 04:23:14	charlie	198.51.100.42	login failed
2025-07-03 04:47:14	bob	10.0.0.5	login failed
2025-07-03 09:02:14	david	203.0.113.77	login failed
2025-07-03 07:02:14	alice	203.0.113.77	login failed
2025-07-03 04:23:14	bob	172.16.0.3	login failed
2025-07-03 04:23:14	bob	172.16.0.3	login failed
2025-07-03 04:23:14	charlie	198.51.100.42	login failed
2025-07-03 04:47:14	bob	10.0.0.5	login failed
2025-07-03 09:02:14	david	203.0.113.77	login failed
2025-07-03 07:02:14	alice	203.0.113.77	login failed

Analysis: Multiple failed login attempts were detected across different users. This pattern may indicate brute-force attack attempts or unauthorized users trying to guess credentials. Monitoring should be intensified for accounts with repeated failed attempts.

3.2 Malware Detection Alerts

Search Query:
index=* action="malware detected" | table _time, user, ip, threat

splunkcloudAppsMessagesSettingsActivityFind

SearchAnalyticsDatasetsReportsAlertsDashboards

Search & Reporting

New Search

index="malware detected" | table _time, user, ip, action, threatTime range: All time

44 events (before 8/19/25 1:51:30.000 PM)No Event Sampling

Job

EventsPatternsStatistics (44)Visualization

Show: 20 Per PageFormatPreview: On

_time	user	ip	action	threat
2025-07-03 09:10:14	bob	172.16.0.3	malware detected	Ransomware
2025-07-03 05:06:14	bob	203.0.113.77	malware detected	Worm
2025-07-03 04:41:14	alice	172.16.0.3	malware detected	Spyware
2025-07-03 07:51:14	eve	10.0.0.5	malware detected	Rootkit
2025-07-03 04:29:14	alice	192.168.1.101	malware detected	Trojan
2025-07-03 05:42:14	eve	203.0.113.77	malware detected	Trojan
2025-07-03 05:30:14	eve	192.168.1.101	malware detected	Trojan
2025-07-03 04:19:14	alice	198.51.100.42	malware detected	Rootkit
2025-07-03 05:45:14	david	172.16.0.3	malware detected	Trojan
2025-07-03 05:48:14	bob	10.0.0.5	malware detected	Trojan

Analysis: Several malware alerts were triggered, including Trojan, Rootkit, and Ransomware detections. These represent high-severity threats that could compromise system integrity. Immediate containment and system scans are recommended to prevent lateral movement of threats.

3.3 External IP Connections

Search Query:
index=* source="SOC_Task2_Sample_Logs.txt"

NOT (ip="10.*" OR ip="192.168.*" OR ip="172.16.*")

splunkcloudAppsMessagesSettingsActivityFind

SearchAnalyticsDatasetsReportsAlertsDashboards

Search & Reporting

Create Table View

HistorySPL

Selected Data

Previewing 50 events (7/3/25 4:18:14.000 AM to 8/20/25 2:45:24.000 PM)Sample: Latest

	host	source	sourcetype	_raw
2	si-i-0674565ca7204c600.prd-p-gf3r6.splunkcloud.com	SOC_Task2_Sample_Logs.txt	Testing-log	2025-07-03 09:10:14 user=bob ip=198.51.100.42 action=file accessed
2	si-i-0674565ca7204c600.prd-p-gf3r6.splunkcloud.com	SOC_Task2_Sample_Logs.txt	log	2025-07-03 09:10:14 user=bob ip=198.51.100.42 action=file accessed
2	si-i-0674565ca7204c600.prd-p-gf3r6.splunkcloud.com	SOC_Task2_Sample_Logs.txt	testing	2025-07-03 09:10:14 user=bob ip=198.51.100.42 action=file accessed
2	si-i-0674565ca7204c600.prd-p-gf3r6.splunkcloud.com	SOC_Task2_Sample_Logs.txt	log	2025-07-03 09:10:14 user=bob ip=198.51.100.42 action=file accessed
2	si-i-0674565ca7204c600.prd-p-gf3r6.splunkcloud.com	SOC_Task2_Sample_Logs.txt	name	2025-07-03 09:10:14 user=bob ip=198.51.100.42 action=file accessed
2	si-i-0674565ca7204c600.prd-p-gf3r6.splunkcloud.com	SOC_Task2_Sample_Logs.txt	Testing-log	2025-07-03 09:07:14 user=eve ip=203.0.113.77 action=login success
2	si-i-0674565ca7204c600.prd-p-gf3r6.splunkcloud.com	SOC_Task2_Sample_Logs.txt	log	2025-07-03 09:07:14 user=eve ip=203.0.113.77 action=login success

Analysis: Logs show multiple connection attempts from external IP ranges such as 198.51.x.x and 203.0.x.x. These IPs are not part of the internal private ranges, suggesting potential unauthorized external access attempts. Such events should be investigated and blocked if necessary.

4. Containment, Eradication, and Recovery

Based on the detected incidents, the following actions are recommended:

- Block suspicious external IP addresses at the firewall level.
- Reset compromised user accounts and enforce multi-factor authentication.
- Quarantine affected machines and run full malware scans.
- Apply security patches and harden system configurations.

5. Lessons Learned

This task highlights the importance of proactive monitoring using SIEM tools like Splunk. Regular log analysis enables early detection of brute-force attempts, malware infections, and unauthorized access. Clear documentation and communication ensure faster incident response and minimize business impact.