

# Incident response report

## Introduction

This report documents the analysis of simulated security logs to identify suspicious activities as part of a SOC internship task.

## Tools & Data Used

- Splunk SIEM (for log ingestion and analysis)
- Simulated system and network logs (TXT format)

## Incident Summary

The analysis identified multiple high-risk security incidents, including malware infections, suspicious login behaviour, and repeated connection attempts.

## Alert classification logs

Alert ID	Date & Time	User	IP Address	Alert Type	Description	Severity	Action Taken
A1	2025-07-03 04:19	Alice	198.51.100.42	Malware Detection	Rootkit signature detected	High	System isolation recommended
A2	2025-07-03 05:06	Bob	203.0.113.77	Malware Detection	Worm infection attempt	High	Antivirus scan & password reset
A3	2025-07-03 05:48	Bob	10.0.0.5	Malware Detection	Trojan detected	High	Block IP and investigate
A4	2025-07-03 07:45	Charlie	172.16.0.3	Malware Detection	Trojan detected	High	Endpoint monitoring
A5	2025-07-03 09:10	Bob	172.16.0.3	Malware Detection	Ransomware behavior detected	High	Immediate incident escalation

## Incident Analysis

## Steps taken to upload and analyse the logs in Splunk:

**Add Data**

Selected Source    Input Settings    Review    Done    < Back    **Next >**

**Local Event Logs**  
Collect event logs from this machine.

**Remote Event Logs**  
Collect event logs from remote hosts. Note: this uses WMI and requires a domain account.

**Files & Directories**  
Upload a file, index a local file, or monitor an entire directory.

**HTTP Event Collector**  
Configure tokens that clients can use to send data over HTTP or HTTPS.

**TCP / UDP**  
Configure the Splunk platform to listen on a network port.

**Local Performance Monitoring**  
Collect performance data from this machine.

**Remote Performance Monitoring**  
Collect performance and event information from remote hosts. Requires domain credentials.

**Registry monitoring**  
Have the Splunk platform index the local Windows Registry, and monitor it for changes.

**Active Directory monitoring**

**FAQ**

- What kinds of files can the Splunk platform index?
- I can't access the file that I want to index. Why?
- How do I get remote data onto my Splunk platform instance?
- Can I monitor changes to files in addition to their content?
- What is a source type?
- How do I specify an includelist or excludelist for a directory?

**Input Settings**  
Optionally set additional input parameters for this data input as follows:

**Source type**  
This setting is one of the default fields that the Splunk platform assigns to all incoming data. It tells the Splunk platform what kind of data you've got, so that the Splunk platform can format the data intelligently during indexing. And it's a way to categorize your data, so that you can search it easily.

**App context**  
Application contexts are folders within a Splunk platform instance that contain configurations for a specific use case or domain of data. App contexts improve manageability of input and source type definitions. The Splunk platform loads all app contexts based on precedence rules. Learn More [Learn More](#)

**Host**  
When the Splunk platform indexes data, each event receives a "host" value. The host value should be the name of the machine from which the event originates. The type of input you choose determines the available configuration options. Learn More [Learn More](#)

**Input Settings**

Source type: Automatic    Select    New

App context: App Context (app\$browser)

Host field value: SSPL-051-HARSHA

Constant value  Regular expression on path  Segment in path

**Review**

Input Type: Directory Monitor  
 Source Path: C:\SOC\_Logs  
 Includes: N/A  
 Excludes: N/A  
 Source Type: Automatic  
 App Context: launcher  
 Host: SSPL-051-HARSHA  
 Index: main

**New Search**

source="C:\SOC\_Logs\\*" host="SSPL-051-HARSHA" index="main"

50 events (before 12/16/25 10:29:41:000 PM) No Event Sampling

Events (50) Patterns Statistics Visualization

Time range: All time

Time	Event
7/3/25 9:10:14:000 AM	2025-07-03 09:10:14   user=bob   ip=172.16.0.3   action=malware detected   threat=Ransomware Behavior host = SSPL-051-HARSHA   source = C:\SOC_Logs\SOC_Task2_Sample_Logs.txt sourcetype = SOC_Task2_Sample_Logs-too_small
7/3/25 9:10:14:000 AM	2025-07-03 09:10:14   user=bob   ip=198.51.100.42   action=file accessed host = SSPL-051-HARSHA   source = C:\SOC_Logs\SOC_Task2_Sample_Logs.txt sourcetype = SOC_Task2_Sample_Logs-too_small
7/3/25 9:07:14:000 AM	2025-07-03 09:07:14   user=rene   ip=203.0.113.77   action=login success host = SSPL-051-HARSHA   source = C:\SOC_Logs\SOC_Task2_Sample_Logs.txt sourcetype = SOC_Task2_Sample_Logs-too_small
7/3/25 9:02:14:000 AM	2025-07-03 09:02:14   user=david   ip=203.0.113.77   action=login failed host = SSPL-051-HARSHA   source = C:\SOC_Logs\SOC_Task2_Sample_Logs.txt sourcetype = SOC_Task2_Sample_Logs-too_small
7/3/25 8:42:14:000 AM	2025-07-03 08:42:14   user=rene   ip=172.16.0.3   action=file accessed host = SSPL-051-HARSHA   source = C:\SOC_Logs\SOC_Task2_Sample_Logs.txt sourcetype = SOC_Task2_Sample_Logs-too_small
7/3/25	2025-07-03 08:42:14   user=charlie   ip=203.0.113.77   action=file accessed

## Incident 1: Malware Infection

**New Search**

source="C:\SOC\_Logs\\*" host="SSPL-051-HARSHA" index="main" "action=malware"

11 events (before 12/16/25 10:27:52.000 PM) No Event Sampling

Events (11) Patterns Statistics Visualization

Time range: All time

Time	Event
7/3/25 9:10:14:000 AM	2025-07-03 09:10:14   user=bob   ip=172.16.0.3   action=malware detected   threat=Ransomware Behavior host = SSPL-051-HARSHA   source = C:\SOC_Logs\SOC_Task2_Sample_Logs.txt sourcetype = SOC_Task2_Sample_Logs-too_small
7/3/25 7:51:14:000 AM	2025-07-03 07:51:14   user=eve   ip=10.0.0.5   action=malware detected   threat=Rootkit Signature host = SSPL-051-HARSHA   source = C:\SOC_Logs\SOC_Task2_Sample_Logs.txt sourcetype = SOC_Task2_Sample_Logs-too_small
7/3/25 7:45:14:000 AM	2025-07-03 07:45:14   user=charlie   ip=172.16.0.3   action=malware detected   threat=Trojan Detected host = SSPL-051-HARSHA   source = C:\SOC_Logs\SOC_Task2_Sample_Logs.txt sourcetype = SOC_Task2_Sample_Logs-too_small
5:48:14:000 AM	2025-07-03 05:48:14   user=bob   ip=10.0.0.5   action=malware detected   threat=Trojan Detected host = SSPL-051-HARSHA   source = C:\SOC_Logs\SOC_Task2_Sample_Logs.txt sourcetype = SOC_Task2_Sample_Logs-too_small
5:45:14:000 AM	2025-07-03 05:45:14   user=david   ip=172.16.0.3   action=malware detected   threat=Trojan Detected host = SSPL-051-HARSHA   source = C:\SOC_Logs\SOC_Task2_Sample_Logs.txt sourcetype = SOC_Task2_Sample_Logs-too_small
7/3/25	2025-07-03 05:42:14   user=rene   ip=203.0.113.77   action=malware detected   threat=Trojan Detected

Figure 1: Splunk SIEM showing malware detection alerts

New Search

source="C:\\SOC\_Logs\\\* host=\"SSPL-051-HARSHA\" index=\"main\" \"threat=Ransomware\"

1 event (before 12/16/25 10:28:41 PM) No Event Sampling

Events (1) Patterns Statistics Visualization

Timeline format - Zoom Out + Zoom to Selection X Deselect

Time range: All time Job Save As Create Table View Close

1 millisecond per column

Time	Event
7/3/25 9:10:14 AM	2025-07-03 09:10:14   user=bob   ip=172.16.0.3   action=malware detected   threat=Ransomware Behavior host = SSPL-051-HARSHA   source = C:\SOC_Logs\SOC_Task2_Sample_Logs.txt   sourcetype = SOC_Task2_Sample_Logs-too_small

Format Show: 20 Per Page View: List

Selected Fields: host 1, source 1, sourcetype 1

Interesting Fields: action 1, date\_hour 1, date\_mday 1, date\_minute 1, date\_month 1, date\_second 1, date\_wday 1, date\_zone 1

Figure 2: Splunk SIEM showing Ransomware detection alerts

New Search

source="C:\\SOC\_Logs\\\* host=\"SSPL-051-HARSHA\" index=\"main\" \"threat=Trojan\"

6 events (before 12/16/25 10:31:14.000 PM) No Event Sampling

Events (6) Patterns Statistics Visualization

Timeline format - Zoom Out + Zoom to Selection X Deselect

Jul 3, 2025 4:00 AM 0 events at 6 AM on Thursday, July 3, 2025 Jul 3, 2025 8:00 AM

Time range: All time Job Save As Create Table View Close

1 hour per column

Time	Event
7/3/25 05:45:14 AM	2025-07-03 05:45:14   user=charlie   ip=172.16.0.3   action=malware detected   threat=Trojan Detected host = SSPL-051-HARSHA   source = C:\SOC_Logs\SOC_Task2_Sample_Logs.txt   sourcetype = SOC_Task2_Sample_Logs-too_small
7/3/25 05:48:14 AM	2025-07-03 05:48:14   user=bob   ip=10.0.0.5   action=malware detected   threat=Trojan Detected host = SSPL-051-HARSHA   source = C:\SOC_Logs\SOC_Task2_Sample_Logs.txt   sourcetype = SOC_Task2_Sample_Logs-too_small
7/3/25 05:45:14 AM	2025-07-03 05:45:14   user=david   ip=172.16.0.3   action=malware detected   threat=Trojan Detected host = SSPL-051-HARSHA   source = C:\SOC_Logs\SOC_Task2_Sample_Logs.txt   sourcetype = SOC_Task2_Sample_Logs-too_small
7/3/25 05:42:14 AM	2025-07-03 05:42:14   user=eve   ip=203.0.113.77   action=malware detected   threat=Trojan Detected host = SSPL-051-HARSHA   source = C:\SOC_Logs\SOC_Task2_Sample_Logs.txt   sourcetype = SOC_Task2_Sample_Logs-too_small
7/3/25 05:30:14 AM	2025-07-03 05:30:14   user=alice   ip=192.168.1.101   action=malware detected   threat=Trojan Detected host = SSPL-051-HARSHA   source = C:\SOC_Logs\SOC_Task2_Sample_Logs.txt   sourcetype = SOC_Task2_Sample_Logs-too_small
7/3/25	2025-07-03 04:29:14   user=alice   ip=192.168.1.101   action=malware detected   threat=Trojan Detected

Format Show: 20 Per Page View: List

Selected Fields: host 1, source 1, sourcetype 1

Interesting Fields: action 1, date\_hour 3, date\_mday 1, date\_minute 5, date\_month 1, date\_second 1, date\_wday 1, date\_year 1, date\_zone 1

Figure 3: Splunk SIEM showing Trojan malware detection alerts

New Search

source="C:\\SOC\_Logs\\\* host=\"SSPL-051-HARSHA\" index=\"main\" \"threat=Rootkit\"

2 events (before 12/16/25 10:31:43.000 PM) No Event Sampling

Events (2) Patterns Statistics Visualization

Timeline format - Zoom Out + Zoom to Selection X Deselect

Time range: All time Job Save As Create Table View Close

1 hour per column

Time	Event
7/3/25 07:51:14 AM	2025-07-03 07:51:14   user=eve   ip=10.0.0.5   action=malware detected   threat=Rootkit Signature host = SSPL-051-HARSHA   source = C:\SOC_Logs\SOC_Task2_Sample_Logs.txt   sourcetype = SOC_Task2_Sample_Logs-too_small
7/3/25 04:19:14 AM	2025-07-03 04:19:14   user=alice   ip=198.51.100.42   action=malware detected   threat=Rootkit Signature host = SSPL-051-HARSHA   source = C:\SOC_Logs\SOC_Task2_Sample_Logs.txt   sourcetype = SOC_Task2_Sample_Logs-too_small

Format Show: 20 Per Page View: List

Selected Fields: host 1, source 1, sourcetype 1

Interesting Fields: action 1, date\_hour 2, date\_mday 1, date\_minute 2, date\_month 1, date\_second 1, date\_wday 1, date\_year 1, date\_zone 1

Figure 4: Splunk SIEM showing Rootkit signature alerts

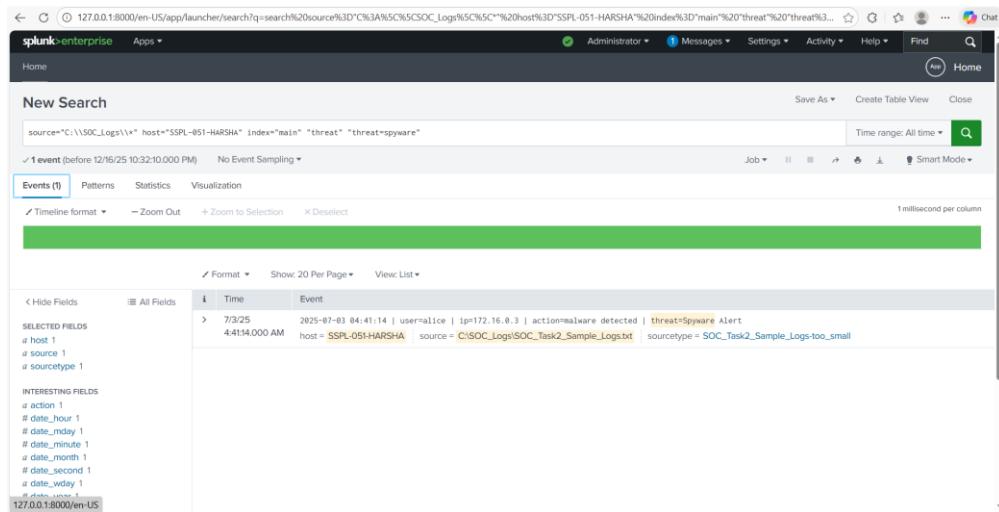


Figure 5: Splunk SIEM showing spyware detection alerts

- Severity:** High
- Impact:** Risk of system compromise, data loss, and ransomware spread.
- Malware detected:** Ransomware, Trojan, Rootkit, Spyware, Worm.
- Affected Users:** Bob, Alice, David
- Recommended Action:** Isolate infected systems, run antivirus scans, reset credentials.

## Incident 2: Unauthorised Access Risk

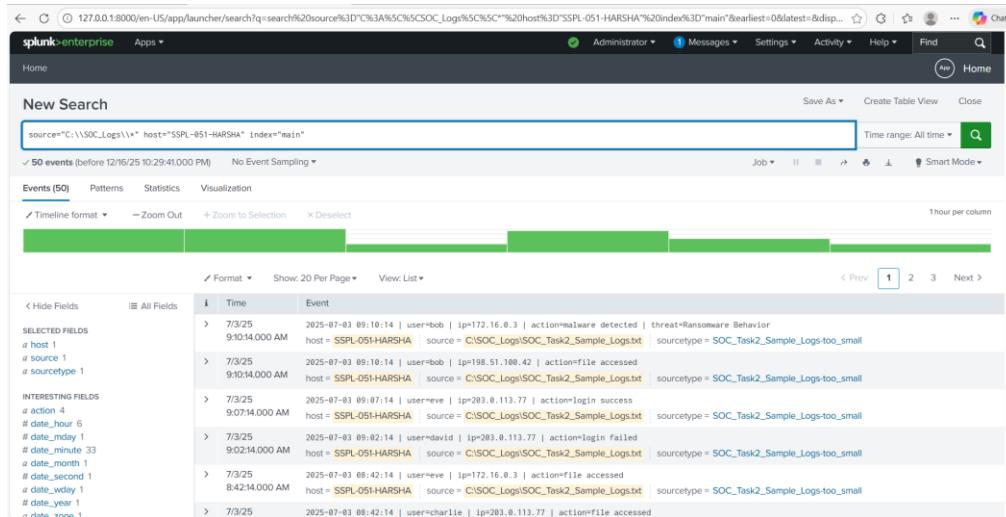


Figure 6: Splunk SIEM showing login after malware detected

- Severity:** High
- Description:** Login success detected after malware alerts.
- Impact:** Potential account takeover.
- Recommended Action:** Force password resets, enable MFA (Multifactor Authentication).

## Incident 3: Suspicious Connection Attempts

The screenshot shows a Splunk search interface with the following details:

- Search Query:** source="C:\SOC\_Logs\\* host=""SSPL-051-HARSHA"" index="main"
- Events Found:** 50 events before 12/16/25 10:29:41.000 PM (No Event Sampling)
- Event List:**

Time	Event
2025-07-03 09:10:14   user=bob   ip=172.16.0.3   action=malware detected   threat=Ransomware Behavior	
2025-07-03 09:10:14   user=bob   ip=198.51.100.42   action=file accessed	
2025-07-03 09:10:14   user=bob   ip=203.0.113.77   action=login success	
2025-07-03 09:42:14   user=david   ip=203.0.113.77   action=login failed	
2025-07-03 08:42:14   user=alice   ip=203.0.113.77   action=login failed	
2025-07-03 08:42:14   user=charlie   ip=198.51.100.42   action=login failed	
2025-07-03 08:42:14   user=charlie   ip=203.0.113.77   action=file accessed	

Figure 7: Splunk SIEM showing multiple connection attempts

- Severity:** Medium
- Description:** Repeated connection attempts by users.
- Impact:** Possible reconnaissance activity.
- Recommended Action:** Monitor IPs, apply firewall rules.

## Incident 4: Multiple failed login attempts

The screenshot shows a Splunk search interface with the following details:

- Search Query:** source="C:\SOC\_Logs\\* host=""SSPL-051-HARSHA"" index="main" failed
- Events Found:** 5 events (before 12/16/25 10:30:38.000 PM) (No Event Sampling)
- Event List:**

Time	Event
2025-07-03 09:02:14   user=david   ip=203.0.113.77   action=login failed	
2025-07-03 07:02:14   user=alice   ip=203.0.113.77   action=login failed	
2025-07-03 04:47:14   user=bob   ip=0.0.0.5   action=login failed	
2025-07-03 04:23:14   user=bob   ip=172.16.0.3   action=login failed	
2025-07-03 04:23:14   user=charlie   ip=198.51.100.42   action=login failed	

Figure 8: Splunk SIEM showing failed login attempts

- Severity:** Low
- Description:** Repeated failed connection attempts by users.
- Impact:** Possible brute force or DoS attack.
- Recommended Action:** Monitor IPs.

## Splunk Dashboard

i	Time	Event
>	7/3/2025 9:10:14:000 AM	2025-07-03 09:10:14   user=bob   ip=172.16.0.3   action=malware detected   threat=Ransomware Behavior
>	7/3/2025 9:10:14:000 AM	2025-07-03 09:10:14   user=bob   ip=198.51.100.42   action=file accessed
>	7/3/2025 9:07:14:000 AM	2025-07-03 09:07:14   user=eve   ip=203.0.113.77   action=login success
>	7/3/2025 9:02:14:000 AM	2025-07-03 09:02:14   user=david   ip=203.0.113.77   action=login failed
>	7/3/2025 8:42:14:000 AM	2025-07-03 08:42:14   user=eve   ip=172.16.0.3   action=file accessed
>	7/3/2025 8:42:14:000 AM	2025-07-03 08:42:14   user=charlie   ip=203.0.113.77   action=file accessed
>	7/3/2025 8:31:14:000 AM	2025-07-03 08:31:14   user=eve   ip=203.0.113.77   action=file accessed
>	7/3/2025 8:30:14:000 AM	2025-07-03 08:30:14   user=eve   ip=172.16.0.3   action=login success
>	7/3/2025 8:21:14:000 AM	2025-07-03 08:21:14   user=david   ip=172.16.0.3   action=connection attempt
>	7/3/2025 8:20:14:000 AM	2025-07-03 08:20:14   user=charlie   ip=192.168.1.101   action=connection attempt

Figure 9: Splunk SIEM dashboard

### Timeline of Events

#### Time (2025-07-03) Event Description

- 04:18            Login success detected for user *bob* from IP 198.51.100.42
- 04:19            Malware detected on *alice*'s system (Rootkit Signature)
- 04:27            Repeated connection attempts observed from user *david*
- 05:06            Malware detected on *bob*'s system (Worm Infection Attempt)
- 05:48            Trojan detected on *bob*'s system from IP 10.0.0.5
- 07:45            Trojan detected on *charlie*'s system
- 09:10            Ransomware behaviour detected on *bob*'s system

---

### Conclusion

The detected incidents indicate active security threats that require immediate containment, monitoring, and remediation.

**Email to Management**

**Subject:** SOC Alert – Multiple Malware & Suspicious Activities Detected

Dear Management Team,

During SOC monitoring, multiple malware infections and suspicious login activities were detected across systems.

Immediate containment and remediation actions are recommended to prevent further impact.

Regards,

SOC Analyst (Intern)