

SOC INCIDENT RESPONSE REPORT

Prepared by: Murtaza Sukhsarwala
Cybersecurity Internship Project

Executive Summary

- This report summarizes key suspicious alerts detected using Splunk SIEM.
- High severity malware, failed logins, and unusual file access indicate attempted compromise.

Top Suspicious Alerts

- Ransomware Behavior – High
- Rootkit Detection – High
- Trojan Detection – High
- Failed Login Attempts – Medium
- Suspicious File Access – High

Incident Timeline

- 04:19 – Rootkit detected
- 05:48 – Trojan detected
- 07:02 – Failed logins
- 08:42 – Suspicious file access
- 09:10 – Ransomware detected

Impact & Risk

- • Multiple high-risk malware infections detected.
- • Signs of credential theft and brute-force attempts.
- • Possible lateral movement inside the network.

Recommended Actions

- Immediate: Isolate hosts, block malicious IPs.
- Short-Term: Reset passwords, analyze logs.
- Long-Term: Implement SIEM rules, deploy EDR.

SIEM Dashboard Screenshot

The screenshot displays the Splunk Cloud SIEM dashboard. The top navigation bar includes links for Apps, Messages, Settings, Activity, and a search bar. The main content area shows a search for threat events, with 50 results found. The search criteria are: source="SOC_Task2_Sample_Logs.txt" host="si-1-09025a8f64475aef4.prd-p-29yt2.splunkcloud.com" sourcetype="sample". The search results are displayed in a table format, showing the threat type, count, and percentage. The sidebar on the left lists various fields for selection, including action, date, host, ip, and user.

New Search

source="SOC_Task2_Sample_Logs.txt" host="si-1-09025a8f64475aef4.prd-p-29yt2.splunkcloud.com" sourcetype="sample"

Time range: All time

50 events (before 11/22/25 5:57:24.000 AM) No Event Sampling

Jobs | Visualization | Policy-Based Pool | Smart Mode

threat

5 Values, 22% of events

Selected Yes No

Reports

Top values Top values by time Rare values

Events with this field

Values	Count	%
Trojan	6	54.545%
Rootkit	2	18.182%
Ransomware	1	9.091%
Spyware	1	9.091%
Worm	1	9.091%

7/3/25 8:42:14.000 AM 2025-07-03 08:42:14 | user=eve | ip=172.16.0.3 | action=file accessed

> 7/3/25 8:42:14.000 AM 2025-07-03 08:42:14 | user=charlie | ip=203.0.113.77 | action=file accessed

> 7/3/25 8:31:14.000 AM 2025-07-03 08:31:14 | user=eve | ip=203.0.113.77 | action=file accessed

> 7/3/25 8:30:14.000 AM 2025-07-03 08:30:14 | user=eve | ip=172.16.0.3 | action=login success

> 7/3/25 8:21:14.000 AM 2025-07-03 08:21:14 | user=david | ip=172.16.0.3 | action=connection attempt

> 7/3/25 8:20:14.000 AM 2025-07-03 08:20:14 | user=charlie | ip=192.168.1.101 | action=connection attempt

7/3/25 8:42:14.000 AM 2025-07-03 08:42:14 | user=eve | ip=172.16.0.3 | action=file accessed

7/3/25 8:42:14.000 AM 2025-07-03 08:42:14 | user=charlie | ip=203.0.113.77 | action=file accessed

7/3/25 8:31:14.000 AM 2025-07-03 08:31:14 | user=eve | ip=203.0.113.77 | action=file accessed

7/3/25 8:30:14.000 AM 2025-07-03 08:30:14 | user=eve | ip=172.16.0.3 | action=login success

7/3/25 8:21:14.000 AM 2025-07-03 08:21:14 | user=david | ip=172.16.0.3 | action=connection attempt

7/3/25 8:20:14.000 AM 2025-07-03 08:20:14 | user=charlie | ip=192.168.1.101 | action=connection attempt

SIEM Dashboard Screenshot

splunk-cloud Apps Messages Settings Activity login

Search Analytics Datasets Reports Alerts Dashboards

Search & Reporting

New Search

Save As Create Table View Close

file accessed

Time range: All time

11 events (before 11/22/25 5:59:33.000 AM) No Event Sampling

Job Policy-Based Pool Smart Mode

Events (11) Patterns Statistics Visualization

Timeline format Zoom Out Zoom to Selection Deselect 1 hour per column

Show Fields Format Show: 20 Per Page View List

#	Time	Event
>	7/3/25 9:10:14.000 AM	2025-07-03 09:10:14 user=bob ip=198.51.100.42 action= file accessed action = file date_hour = 9 date_minute = 10 date_month = July date_second = 14 date_wday = thursday date_year = 2025 date_zone = local host = si-09025a8f64475ae4.prd-p-29y2.splunkcloud.com index = main ip = 198.51.100.42 linecount = 1 punct = _-_-_-_-_-_-_-_-_-_- source = SOC_Task2_Sample_Logs.bt sourcetype = sample splunk_server = si-09025a8f64475ae4.prd-p-29y2.splunkcloud.com timeendpos = 20 timestartpos = 0 user = bob
>	7/3/25 8:42:14.000 AM	2025-07-03 08:42:14 user=eve ip=172.16.0.3 action= file accessed action = file date_hour = 8 date_minute = 42 date_month = July date_second = 14 date_wday = thursday date_year = 2025 date_zone = local host = si-09025a8f64475ae4.prd-p-29y2.splunkcloud.com index = main ip = 172.16.0.3 linecount = 1 punct = _-_-_-_-_-_-_-_-_-_- source = SOC_Task2_Sample_Logs.bt sourcetype = sample splunk_server = si-09025a8f64475ae4.prd-p-29y2.splunkcloud.com timeendpos = 20 timestartpos = 0 user = eve
>	7/3/25 8:42:14.000 AM	2025-07-03 08:42:14 user=charlie ip=203.0.113.77 action= file accessed action = file date_hour = 8 date_minute = 42 date_month = July date_second = 14 date_wday = thursday date_year = 2025 date_zone = local host = si-09025a8f64475ae4.prd-p-29y2.splunkcloud.com index = main ip = 203.0.113.77 linecount = 1 punct = _-_-_-_-_-_-_-_-_-_- source = SOC_Task2_Sample_Logs.bt sourcetype = sample splunk_server = si-09025a8f64475ae4.prd-p-29y2.splunkcloud.com timeendpos = 20 timestartpos = 0 user = charlie
>	7/3/25 8:31:14.000 AM	2025-07-03 08:31:14 user=eve ip=203.0.113.77 action= file accessed action = file date_hour = 8 date_minute = 31 date_month = July date_second = 14 date_wday = thursday date_year = 2025 date_zone = local host = si-09025a8f64475ae4.prd-p-29y2.splunkcloud.com index = main ip = 203.0.113.77 linecount = 1 punct = _-_-_-_-_-_-_-_-_-_- source = SOC_Task2_Sample_Logs.bt sourcetype = sample splunk_server = si-09025a8f64475ae4.prd-p-29y2.splunkcloud.com timeendpos = 20 timestartpos = 0 user = eve
>	7/3/25 7:57:14.000 AM	2025-07-03 07:57:14 user=david ip=10.0.0.5 action= file accessed action = file date_hour = 7 date_minute = 57 date_month = July date_second = 14 date_wday = thursday date_year = 2025 date_zone = local host = si-09025a8f64475ae4.prd-p-29y2.splunkcloud.com index = main ip = 10.0.0.5 linecount = 1 punct = _-_-_-_-_-_-_-_-_-_- source = SOC_Task2_Sample_Logs.bt sourcetype = sample splunk_server = si-09025a8f64475ae4.prd-p-29y2.splunkcloud.com timeendpos = 20 timestartpos = 0 user = david
>	7/3/25 7:18:14.000 AM	2025-07-03 07:18:14 user=bob ip=203.0.113.77 action= file accessed action = file date_hour = 7 date_minute = 18 date_month = July date_second = 14 date_wday = thursday date_year = 2025 date_zone = local host = si-09025a8f64475ae4.prd-p-29y2.splunkcloud.com index = main ip = 203.0.113.77 linecount = 1 punct = _-_-_-_-_-_-_-_-_-_- source = SOC_Task2_Sample_Logs.bt sourcetype = sample splunk_server = si-09025a8f64475ae4.prd-p-29y2.splunkcloud.com timeendpos = 20 timestartpos = 0 user = bob
>	7/3/25 6:10:14.000 AM	2025-07-03 06:10:14 user=david ip=203.0.113.77 action= file accessed action = file date_hour = 6 date_minute = 10 date_month = July date_second = 14 date_wday = thursday date_year = 2025 date_zone = local host = si-09025a8f64475ae4.prd-p-29y2.splunkcloud.com index = main ip = 203.0.113.77 linecount = 1 punct = _-_-_-_-_-_-_-_-_-_- source = SOC_Task2_Sample_Logs.bt sourcetype = sample splunk_server = si-09025a8f64475ae4.prd-p-29y2.splunkcloud.com timeendpos = 20 timestartpos = 0 user = david
>	7/3/25 6:01:14.000 AM	2025-07-03 06:01:14 user=bob ip=172.16.0.3 action= file accessed action = file date_hour = 6 date_minute = 1 date_month = July date_second = 14 date_wday = thursday date_year = 2025 date_zone = local host = si-09025a8f64475ae4.prd-p-29y2.splunkcloud.com index = main ip = 172.16.0.3 linecount = 1 punct = _-_-_-_-_-_-_-_-_-_- source = SOC_Task2_Sample_Logs.bt sourcetype = sample splunk_server = si-09025a8f64475ae4.prd-p-29y2.splunkcloud.com timeendpos = 20 timestartpos = 0 user = bob
>	7/3/25 5:44:14.000 AM	2025-07-03 05:44:14 user=bob ip=198.51.100.42 action= file accessed action = file date_hour = 5 date_minute = 44 date_month = July date_second = 14 date_wday = thursday date_year = 2025 date_zone = local host = si-09025a8f64475ae4.prd-p-29y2.splunkcloud.com index = main ip = 198.51.100.42 linecount = 1 punct = _-_-_-_-_-_-_-_-_-_- source = SOC_Task2_Sample_Logs.bt sourcetype = sample splunk_server = si-09025a8f64475ae4.prd-p-29y2.splunkcloud.com timeendpos = 20 timestartpos = 0 user = bob
>	7/3/25 5:33:14.000 AM	2025-07-03 05:33:14 user=david ip=198.51.100.42 action= file accessed action = file date_hour = 5 date_minute = 33 date_month = July date_second = 14 date_wday = thursday date_year = 2025 date_zone = local host = si-09025a8f64475ae4.prd-p-29y2.splunkcloud.com index = main ip = 198.51.100.42 linecount = 1 punct = _-_-_-_-_-_-_-_-_-_- source = SOC_Task2_Sample_Logs.bt sourcetype = sample splunk_server = si-09025a8f64475ae4.prd-p-29y2.splunkcloud.com timeendpos = 20 timestartpos = 0 user = david
>	7/3/25 4:53:14.000 AM	2025-07-03 04:53:14 user=alice ip=203.0.113.77 action= file accessed action = file date_hour = 4 date_minute = 53 date_month = July date_second = 14 date_wday = thursday date_year = 2025 date_zone = local host = si-09025a8f64475ae4.prd-p-29y2.splunkcloud.com index = main ip = 203.0.113.77 linecount = 1 punct = _-_-_-_-_-_-_-_-_-_- source = SOC_Task2_Sample_Logs.bt sourcetype = sample splunk_server = si-09025a8f64475ae4.prd-p-29y2.splunkcloud.com timeendpos = 20 timestartpos = 0 user = alice