

SECURITY ALERT MONITORING & INCIDENT RESPONSE

Tool used : Splunk Enterprise

Introduction :

This reports consist of a analysis of security log using Splunk SIEM to detect ,analyze and respond to security incidents .The sample data provided by future interns was analysed on Splunk .

The sample data which was provide by Future interns was ingested to splunk . It was uploaded using add data feature of splunk allowing the system to parse and index the events for analysis.The logs were classified using the syslog source type, which enabled Splunk to automatically recognize and extract key fields such as timestamp, IP address, user, action, and threat type. A dedicated index named “security_logs_”was created to store and organize all ingested events, ensuring separation from default system logs and improving search efficiency.

The ingestion process successfully indexed all events, and data availability was verified by executing search queries within the Splunk Search & Reporting interface. This step confirmed that the

logs were properly parsed and ready for further security analysis, alert generation, and incident response activities.

Identified Suspicious alerts :-

- 1.Ransomware Behaviour
- 2.Rootkit Signature
- 3.Trojan Detected
- 4.Worm Infection Attempt
- 5.Spyware alert

Incident Classification:

Alert Type	Severity	Reason
Ransomware Behaviour	High	Potential data encryption & business impact
Rootkit Signature	High	Stealth malware with persistence
Trojan Detected	High	Known malicious payload
Worm Infection Attempt	Medium	Attempted spread, blocked
Spyware alert	Medium	Data monitoring risk

NOTE : Severity was assigned based on potential impact, persistence, and spread capability.

Detailed Incident Report :-

Time stamp	Event
7/3/25 9:10:14	Ransome Behaviour on 172.16.0.3 User=Bob
7/3/25 7:51:14	Rootkit Signature on 10.0.0.5 User=Eve
7/3/25 7:45:14	Trojan Detected on 172.16.0.3 User=Charlie
7/3/25 5:48:14	Trojan Detected on 10.0.0.5 User=Bob
7/3/25 5:45:14	Trojan Detected on 172.16.0.3 User=David
7/3/25 5:42:14	Trojan Detected on 203.0.113.77 User=Eve
7/3/25 5:30:14	Trojan Detected on 192.168.1.101 User=Eve
7/3/25 5:06:14	Worm Infection Attempt on 203.0.113.77 User=Bob
7/3/25 4:41:14	Spyware Alert on 172.16.0.3 User=Alice
7/3/25 4:29:14	Trojan Detected on 192.168.1.101 User=Alice
7/3/25 4:19:14	Rootkit Signature on 198.51.100.42 User=Alice

Impact :-

- Multiple internal systems showed malware activity
- Risk of data compromise due to ransomware and spyware

- Potential lateral movement within internal network
- No evidence of intentional insider threat

Response/Remediation :-

- Investigated affected IPs and users
- Correlated alerts using Splunk searches
- Identified external suspicious IPs
- Recommended isolating infected endpoints
- Suggested blocking malicious external IPs
- Run full endpoint malware scans
- Patch vulnerable systems
- Reset affected user credentials
- Improve email and endpoint security controls

The screenshot shows the Splunk Enterprise search interface. The top navigation bar includes 'splunk>enterprise' and 'Administrator'. The main search bar contains the query 'index=security_logs_'. Below the search bar, it displays '50 events (before 1/3/26 2:48:37:00 PM)' and 'No Event Sampling'. The time range is set to 'All time'. The search results are presented in a table with columns: 'Time' and 'Event'. The table shows several log entries, such as file access and login attempts, with details like host, source, and action. The interface also includes a timeline visualization at the bottom, showing the progression of events over time.

Time	Event
2025-07-03 09:10:14 host = MSI source = SOC_Task2_Sample_Logs.txt sourcetype = syslog	action=malware detected threat=Ransomware Behavior
2025-07-03 09:10:14 host = MSI source = SOC_Task2_Sample_Logs.txt sourcetype = syslog	user=bob ip=172.16.0.3 action=file accessed
2025-07-03 09:10:14.000 AM	
2025-07-03 09:07:14 host = MSI source = SOC_Task2_Sample_Logs.txt sourcetype = syslog	user=eve ip=203.0.113.77 action=login success
2025-07-03 09:07:14 host = MSI source = SOC_Task2_Sample_Logs.txt sourcetype = syslog	user=david ip=203.0.113.77 action=login failed
2025-07-03 09:02:14 host = MSI source = SOC_Task2_Sample_Logs.txt sourcetype = syslog	
2025-07-03 08:42:14 host = MSI source = SOC_Task2_Sample_Logs.txt sourcetype = syslog	user=eve ip=172.16.0.3 action=file accessed
2025-07-03 08:42:14 host = MSI source = SOC_Task2_Sample_Logs.txt sourcetype = syslog	user=charlie ip=203.0.113.77 action=file accessed

New Search

index=security_logs_ action="malware detected"

11 events (before 1/3/26 2:51:28.000 PM) No Event Sampling ▾

Events (11) Patterns Statistics Visualization

Timeline format ▾ Zoom Out + Zoom to Selection × Deselect

Format Show: 20 Per Page ▾ View: List ▾

< Hide Fields All Fields

SELECTED FIELDS

- a_host_1
- a_source_1
- a_sourcetype_1

INTERESTING FIELDS

- a_action_1
- #date_hour_4
- #date_mday_1
- #date_minute_10
- #date_month_1
- #date_second_1
- #date_wday_1
- #date_year_1

i	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 = MSI source = SOC_Task2_Sample_Logs.txt sourcetype = syslog
>	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 = MSI source = SOC_Task2_Sample_Logs.txt sourcetype = syslog
>	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 = MSI source = SOC_Task2_Sample_Logs.txt sourcetype = syslog
>	7/3/25 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 = MSI source = SOC_Task2_Sample_Logs.txt sourcetype = syslog
>	7/3/25 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 = MSI source = SOC_Task2_Sample_Logs.txt sourcetype = syslog
>	7/3/25 7:02:56-07-03 05:42:14	2025-07-03 05:42:14 user=eve ip=203.0.113.77 action=malware detected threat=Trojan Detected host = MSI source = SOC_Task2_Sample_Logs.txt sourcetype = syslog

New Search

index=security_logs_ "action=login" failed

5 events (before 1/3/26 2:54:10.000 PM) No Event Sampling ▾

Events (5) Patterns Statistics Visualization

Timeline format ▾ Zoom Out + Zoom to Selection × Deselect

Format Show: 20 Per Page ▾ View: List ▾

< Hide Fields All Fields

SELECTED FIELDS

- a_host_1
- a_source_1
- a_sourcetype_1

INTERESTING FIELDS

- a_action_1
- #date_hour_3
- #date_mday_1
- #date_minute_3
- #date_month_1
- #date_second_1
- #date_wday_1
- #date_year_1

i	Time	Event
>	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 = MSI source = SOC_Task2_Sample_Logs.txt sourcetype = syslog
>	7/3/25 7:02:14.000 AM	2025-07-03 07:02:14 user=alice ip=203.0.113.77 action=login failed host = MSI source = SOC_Task2_Sample_Logs.txt sourcetype = syslog
>	7/3/25 4:47:14.000 AM	2025-07-03 04:47:14 user=bob ip=10.0.0.5 action=login failed host = MSI source = SOC_Task2_Sample_Logs.txt sourcetype = syslog
>	7/3/25 4:23:14.000 AM	2025-07-03 04:23:14 user=bob ip=172.16.0.3 action=login failed host = MSI source = SOC_Task2_Sample_Logs.txt sourcetype = syslog
>	7/3/25 4:23:14.000 AM	2025-07-03 04:23:14 user=charlie ip=198.51.100.42 action=login failed host = MSI source = SOC_Task2_Sample_Logs.txt sourcetype = syslog

Note :- All Screenshots are Attached to this report