

# 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 alowing 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:**

<b>Alert Type</b>	<b>Severity</b>	<b>Reason</b>
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

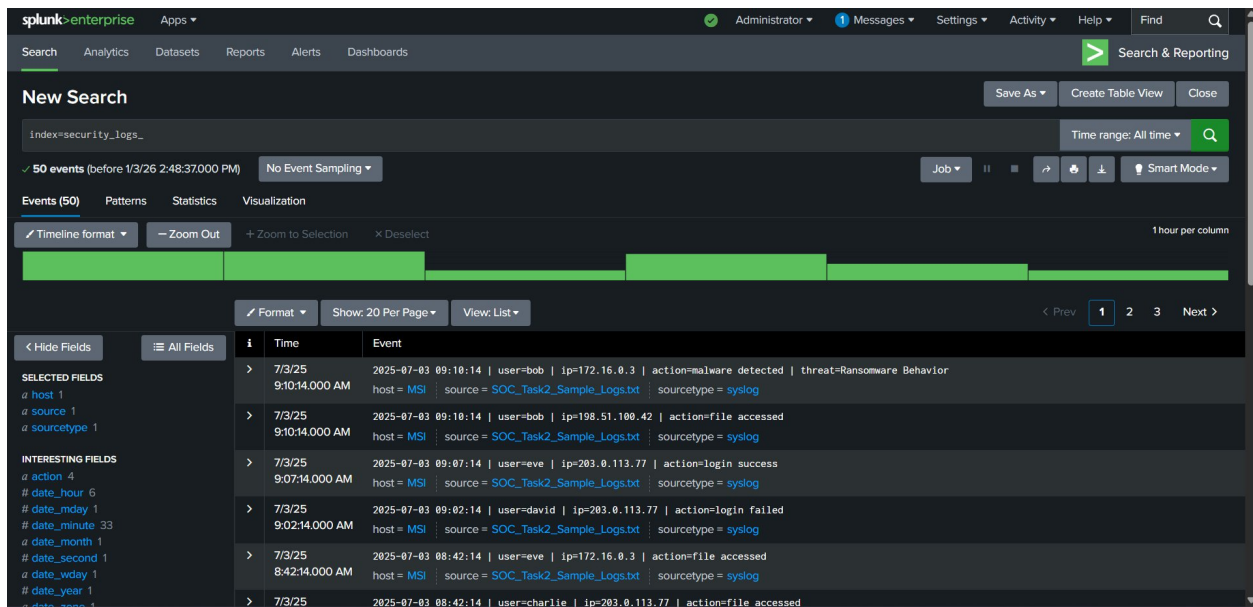
## Impact :-

- 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



**New Search** Save As Create Table View Close

index=security\_logs\_ action="malware detected" Time range: All time Q

✓ 11 events (before 1/3/26 2:51:28.000 PM) No Event Sampling Job || ▢ ↶ ⬇ ⬆ Smart Mode

Events (11) Patterns Statistics Visualization

✓ Timeline format Zoom Out + Zoom to Selection X Deselect 1 hour per column

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  
a date\_month 1  
# date\_second 1  
a 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	2025-07-03 05:42:14   user=eve   ip=203.0.113.77   action=malware detected   threat=Trojan Detected

**New Search** Save As Create Table View Close

index=security\_logs\_ "action-login" failed Time range: All time Q

✓ 5 events (before 1/3/26 2:54:10.000 PM) No Event Sampling Job || ▢ ↶ ⬇ ⬆ Smart Mode

Events (5) Patterns Statistics Visualization

✓ Timeline format Zoom Out + Zoom to Selection X Deselect 1 hour per column

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  
a date\_month 1  
# date\_second 1  
a 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