CYBER SECURITY INTERNSHIP

TASK 2 REPORT	
Task Title	SIEM-BASED INCIDENT MONITORING AND ANALYSIS
Track_code	FUTURE_CS_02
Intern Name	FENIL THUMMAR

Aim:

To monitor and analyze simulated security alerts using a SIEM (Splunk) to identify suspicious activities, classify incidents, and recommend mitigation strategies based on log analysis from simulated brute force and account compromise scenarios.

Tools Used:

• SIEM Tool: Splunk Free Trial

• Environment: Custom Log Dataset simulating brute force attempts, malware alerts, and file access — uploaded and analyzed within Splunk Free Trial.

• File: SOC_Task2_Sample_Logs.txt

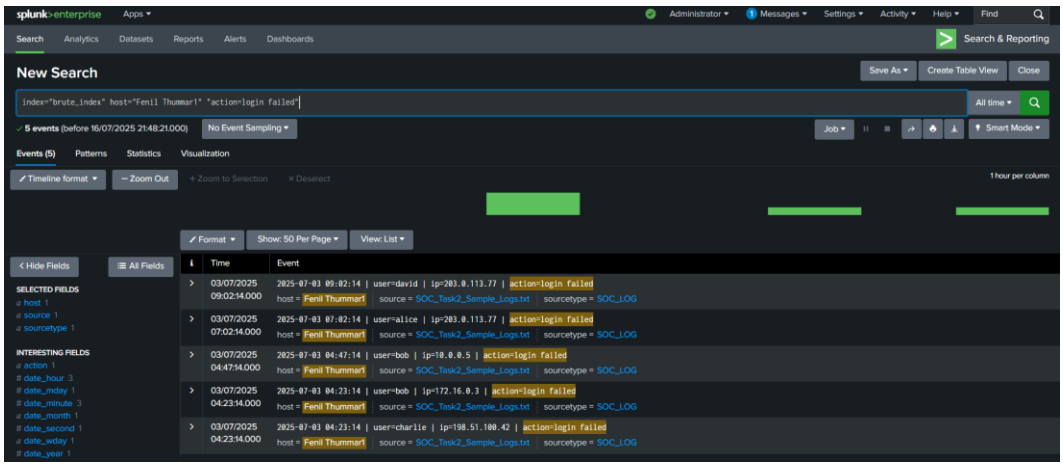
Procedure & Findings:

A custom Windows log file containing simulated security events was uploaded into Splunk. Log analysis was conducted focusing on key event types such as login failures, malware alerts, and suspicious file access. The queries were used to identify brute force attempts, malware detection, and user activity related to file access.

1.Login Failure Events were analyzed using the following query:

index="brute_index" host="Fenil Thummar1" "action=login failed"

Findings: Multiple failed login attempts were noticed from users like david, alice, bob, and charlie.



2.Malware activity was investigated using the following query:

> ***index="brute_index" host="Fenil Thummar1" "action=malware detected"***

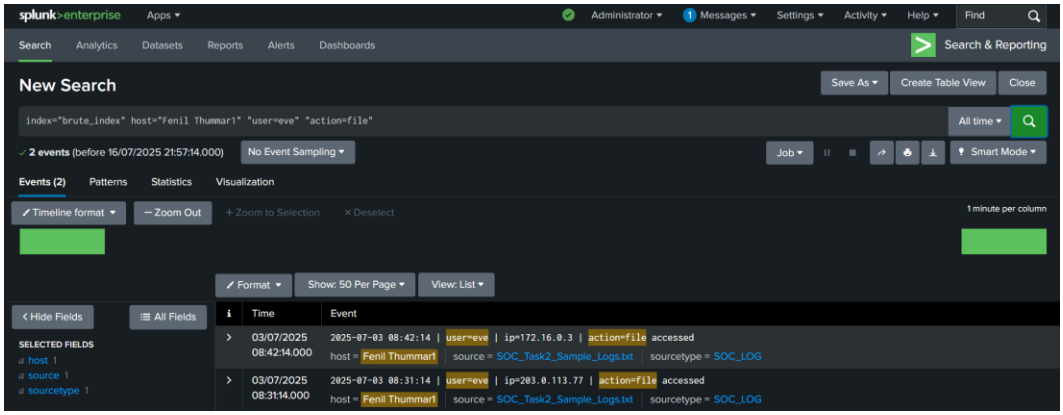
Findings: Several malware types including ransomware, trojans, rootkits, worms, and spyware were detected.

i	Time	Event
>	03/07/2025 09:10:14.000	2025-07-03 09:10:14 | user=bob | ip=172.16.0.3 | action=malware detected | threat=Ransomware Behavior host = Fenil Thummar1 | source = SOC_Task2_Sample_Logs.txt | sourcetype = SOC_LOG
>	03/07/2025 07:51:14.000	2025-07-03 07:51:14 | user=eve | ip=10.0.0.5 | action=malware detected | threat=Rootkit Signature host = Fenil Thummar1 | source = SOC_Task2_Sample_Logs.txt | sourcetype = SOC_LOG
>	03/07/2025 07:45:14.000	2025-07-03 07:45:14 | user=charlie | ip=172.16.0.3 | action=malware detected | threat=Trojan Detected host = Fenil Thummar1 | source = SOC_Task2_Sample_Logs.txt | sourcetype = SOC_LOG
>	03/07/2025 05:48:14.000	2025-07-03 05:48:14 | user=bob | ip=10.0.0.5 | action=malware detected | threat=Trojan Detected host = Fenil Thummar1 | source = SOC_Task2_Sample_Logs.txt | sourcetype = SOC_LOG
>	03/07/2025 05:45:14.000	2025-07-03 05:45:14 | user=david | ip=172.16.0.3 | action=malware detected | threat=Trojan Detected host = Fenil Thummar1 | source = SOC_Task2_Sample_Logs.txt | sourcetype = SOC_LOG
>	03/07/2025 05:42:14.000	2025-07-03 05:42:14 | user=eve | ip=203.0.113.77 | action=malware detected | threat=Trojan Detected host = Fenil Thummar1 | source = SOC_Task2_Sample_Logs.txt | sourcetype = SOC_LOG
>	03/07/2025 05:30:14.000	2025-07-03 05:30:14 | user=eve | ip=192.168.1.101 | action=malware detected | threat=Trojan Detected host = Fenil Thummar1 | source = SOC_Task2_Sample_Logs.txt | sourcetype = SOC_LOG
>	03/07/2025 05:06:14.000	2025-07-03 05:06:14 | user=bob | ip=203.0.113.77 | action=malware detected | threat=Worm Infection Attempt host = Fenil Thummar1 | source = SOC_Task2_Sample_Logs.txt | sourcetype = SOC_LOG
>	03/07/2025 04:41:14.000	2025-07-03 04:41:14 | user=alice | ip=172.16.0.3 | action=malware detected | threat=Spyware Alert host = Fenil Thummar1 | source = SOC_Task2_Sample_Logs.txt | sourcetype = SOC_LOG
>	03/07/2025 04:29:14.000	2025-07-03 04:29:14 | user=alice | ip=192.168.1.101 | action=malware detected | threat=Trojan Detected host = Fenil Thummar1 | source = SOC_Task2_Sample_Logs.txt | sourcetype = SOC_LOG
>	03/07/2025 04:19:14.000	2025-07-03 04:19:14 | user=alice | ip=198.51.100.42 | action=malware detected | threat=Rootkit Signature host = Fenil Thummar1 | source = SOC_Task2_Sample_Logs.txt | sourcetype = SOC_LOG

3.Suspicious file access was tracked using:

> ***index="brute_index" host="Fenil Thummar1" user="eve" "action=file"***

Findings: User eve accessed files from multiple IPs, indicating potential unauthorized activity.



Incident Classification:

Type	Description	Severity
Brute Force Attack	Multiple failed login attempts from same IP	High
Malware Infection	Logs show detections activity affecting users	Critical
Suspicious File Access	Indicating possible account misuse or unauthorized access.	Medium

Security Recommendations:

Immediate:

- Block or monitor IPs
- Reset affected user passwords
- Enforce MFA for admin users

Preventive:

- Implement account lockout policies
- Enable CAPTCHA and login rate limiting

• Use detection rules for excessive login failures

Review:

• Audit administrator logon patterns

• Improve Splunk alert logic

• Conduct user awareness training

Learning Outcomes:

• Understood Windows Event Log types and formats

• Detected and investigated brute force and malware patterns using Splunk

• Gained hands-on experience with search queries, dashboards, and alerts

Ethical Note:

All analysis was done in a virtual lab with simulated logs. No real systems were harmed.

Conclusion:

This exercise demonstrated effective use of Splunk for monitoring and identifying security threats. The incidents detected using query-based searches reflect real-world attack scenarios and emphasize the importance of log analysis in incident response.

Prepared by: Fenil Thummar