FUTURE_CS_02

Intern Name: Vaibhav Gulati

Domain: Cyber Security

Task Title: Security Alert Monitoring & Incident Response

Date: August 2025

Tools Used: Splunk Cloud Free Trial

🎯 Objective of the Report

To analyze and document suspicious security events identified during log monitoring in Splunk, including malware alerts and unauthorized access attempts. This report aims to assess potential risks, determine impact on system integrity and user accounts, and recommend appropriate incident response actions to safeguard organizational assets and prevent further compromise.

Log Source:

- Log File Name: sample_logs.txt
- Description: Simulated logs containing login attempts, usernames, IP addresses, system access events
- Upload Platform: Splunk Cloud Free Trial

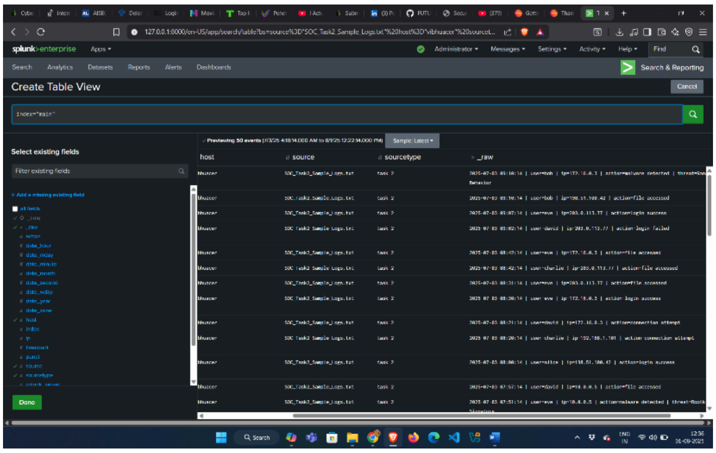
Queries Executed:

- Query 1 –

Show All Logs

index="main"

#Verified that logs were uploaded successfully and viewable in the Splunk console.



Create Table View

index="main"

✓ Previewing 50 events (7/3/25 4:18:14.000 AM to 8/1/25 12:22:14.000 PM)

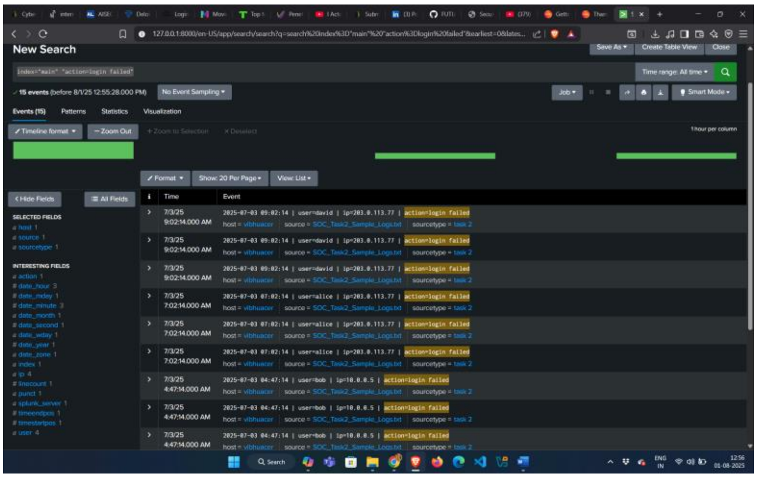
host	source	sourcetype	_raw
bhuacer	SOC_Task2_Sample_Logs.txt	task 2	2025-07-03 09:10:14 | user=bob | ip=172.16.0.3 | action=malware detected | threat=Sus Behavior
bhuacer	SOC_Task2_Sample_Logs.txt	task 2	2025-07-03 09:10:14 | user=bob | ip=198.51.100.42 | action=file accessed
bhuacer	SOC_Task2_Sample_Logs.txt	task 2	2025-07-03 09:07:14 | user=eve | ip=203.0.113.77 | action=login success
bhuacer	SOC_Task2_Sample_Logs.txt	task 2	2025-07-03 09:02:14 | user=david | ip=203.0.113.77 | action=login failed
bhuacer	SOC_Task2_Sample_Logs.txt	task 2	2025-07-03 08:42:14 | user=eve | ip=172.16.0.3 | action=file accessed
bhuacer	SOC_Task2_Sample_Logs.txt	task 2	2025-07-03 08:42:14 | user=charlie | ip=203.0.113.77 | action=file accessed
bhuacer	SOC_Task2_Sample_Logs.txt	task 2	2025-07-03 08:31:14 | user=eve | ip=203.0.113.77 | action=file accessed
bhuacer	SOC_Task2_Sample_Logs.txt	task 2	2025-07-03 08:30:14 | user=eve | ip=172.16.0.3 | action=login success
bhuacer	SOC_Task2_Sample_Logs.txt	task 2	2025-07-03 08:21:14 | user=david | ip=172.16.0.3 | action=connection attempt
bhuacer	SOC_Task2_Sample_Logs.txt	task 2	2025-07-03 08:20:14 | user=charlie | ip=192.168.1.101 | action=connection attempt
bhuacer	SOC_Task2_Sample_Logs.txt	task 2	2025-07-03 08:00:14 | user=alice | ip=198.51.100.42 | action=login success
bhuacer	SOC_Task2_Sample_Logs.txt	task 2	2025-07-03 07:57:14 | user=david | ip=10.0.0.5 | action=file accessed
bhuacer	SOC_Task2_Sample_Logs.txt	task 2	2025-07-03 07:51:14 | user=eve | ip=10.0.0.5 | action=malware detected | threat=Rootk Signature

- Query 2 –

Failed Login Attempts

index="main" "action=login failed"

#Displayed all events where login attempts failed.



New Search

index="main" "action=login failed"

Time range: All time

✓ 15 events (before 8/1/25 12:55:28.000 PM)

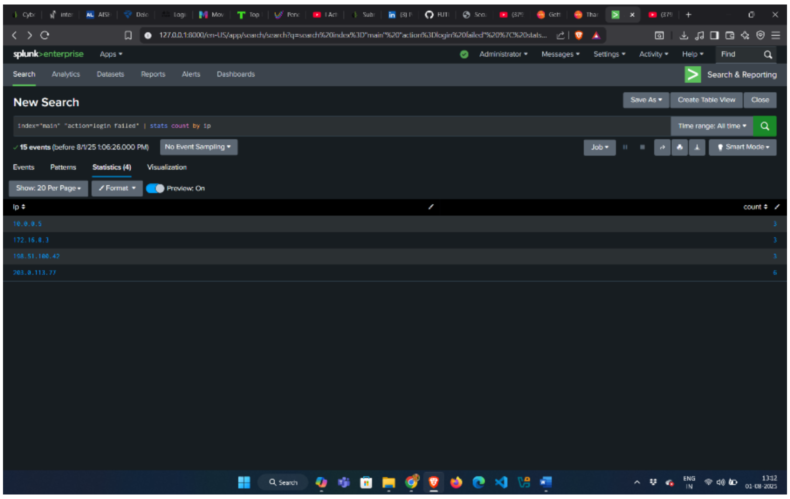
```
7/3/25 9:02:14.000 AM   2025-07-03 09:02:14 | user=david | ip=203.0.113.77 | action=login failed
                        host = vibhuacer   source = SOC_Task2_Sample_Logs.txt   sourcetype = task 2
7/3/25 9:02:14.000 AM   2025-07-03 09:02:14 | user=david | ip=203.0.113.77 | action=login failed
                        host = vibhuacer   source = SOC_Task2_Sample_Logs.txt   sourcetype = task 2
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 = vibhuacer   source = SOC_Task2_Sample_Logs.txt   sourcetype = task 2
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 = vibhuacer   source = SOC_Task2_Sample_Logs.txt   sourcetype = task 2
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 = vibhuacer   source = SOC_Task2_Sample_Logs.txt   sourcetype = task 2
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 = vibhuacer   source = SOC_Task2_Sample_Logs.txt   sourcetype = task 2
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 = vibhuacer   source = SOC_Task2_Sample_Logs.txt   sourcetype = task 2
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 = vibhuacer   source = SOC_Task2_Sample_Logs.txt   sourcetype = task 2
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 = vibhuacer   source = SOC_Task2_Sample_Logs.txt   sourcetype = task 2
```

- Query 3 –

Repeated Failed Logins (Potential Brute Force)

index="main" "action=login failed" | stats count by ip

#Grouped failed login attempts per IP address. Further investigation shows that the user that are getting attacked by different ip’s where Bob (10.0.0.5, 172.16.0.3), Charlie (198.51.100.42), David (203.0.113.77), Alice (203.0.113.77). All the attempts were failed.



```
index="main" "action=login failed" | stats count by ip
```

✓ 15 events (before 8/1/25 1:06:26.000 PM)

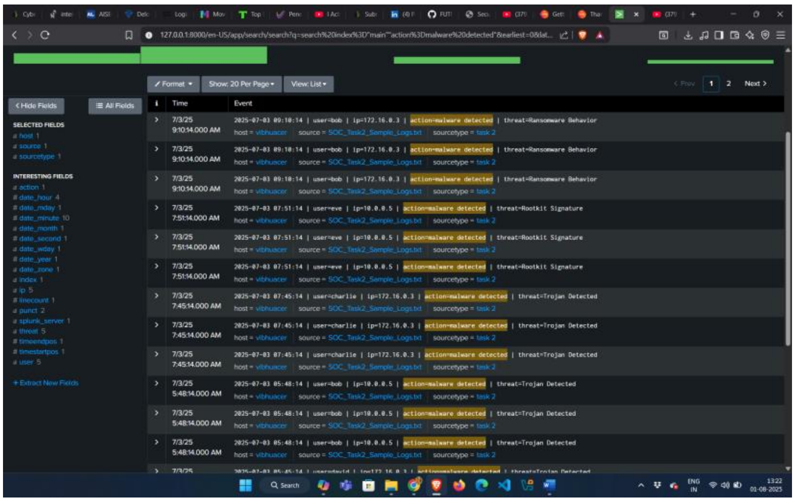
ip	count
10.0.0.5	3
172.16.0.3	3
198.51.100.42	3
203.0.113.77	6

- Query 4 –

Malware Action’s

index="main" "action=malware detected"

#Many threats are detected and there Ip’s such as Trojan (192.168.1.101,172.16.0.3,10.0.0.5), Rootkit (19851.100.42,10.0.0.5), Ransomware (172.16.0.3), Spyware (172.16.0.3), Worm(203.0.113.77)



```
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 = vibhuacer   source = SOC_Task2_Sample_Logs.txt   sourcetype = task 2
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 = vibhuacer   source = SOC_Task2_Sample_Logs.txt   sourcetype = task 2
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 = vibhuacer   source = SOC_Task2_Sample_Logs.txt   sourcetype = task 2
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 = vibhuacer   source = SOC_Task2_Sample_Logs.txt   sourcetype = task 2
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 = vibhuacer   source = SOC_Task2_Sample_Logs.txt   sourcetype = task 2
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 = vibhuacer   source = SOC_Task2_Sample_Logs.txt   sourcetype = task 2
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 = vibhuacer   source = SOC_Task2_Sample_Logs.txt   sourcetype = task 2
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 = vibhuacer   source = SOC_Task2_Sample_Logs.txt   sourcetype = task 2
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 = vibhuacer   source = SOC_Task2_Sample_Logs.txt   sourcetype = task 2
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 = vibhuacer   source = SOC_Task2_Sample_Logs.txt   sourcetype = task 2
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 = vibhuacer   source = SOC_Task2_Sample_Logs.txt   sourcetype = task 2
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 = vibhuacer   source = SOC_Task2_Sample_Logs.txt   sourcetype = task 2
7/3/25                2025-07-03 05:45:14 | user=david | ip=172.16.0.3 | action=malware detected | threat=Trojan Detected
```

- Query 5 –

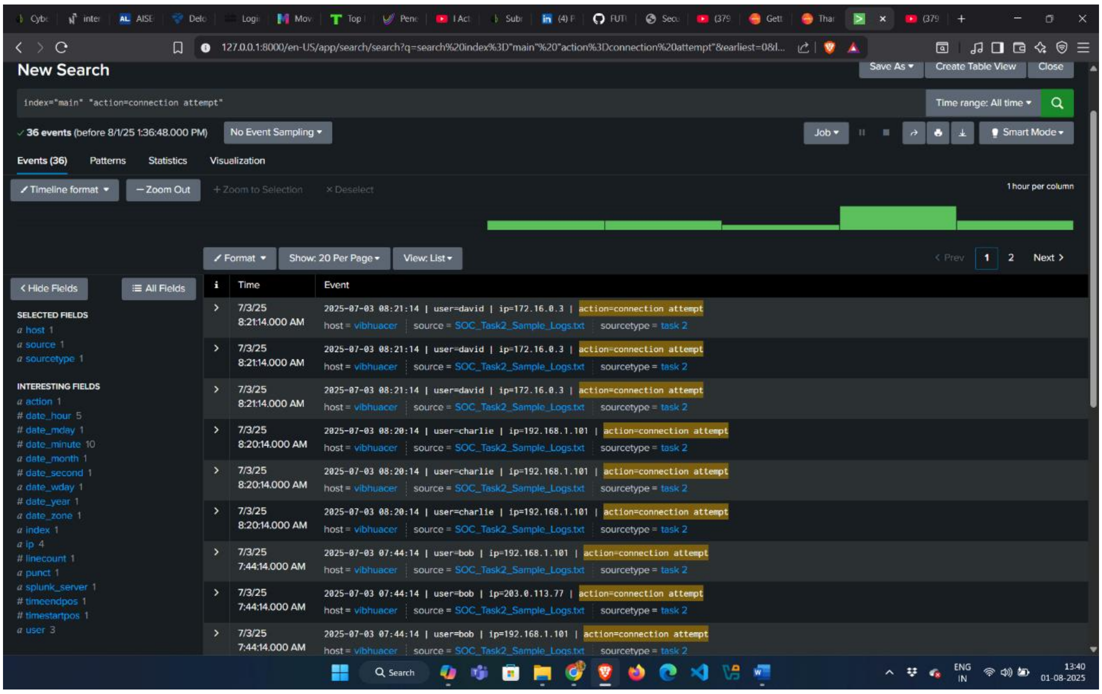
Sensitive File Access Attempt

index="main" “action=connection attempt”

#There is seen that some ip’s tried to attempt connection to many users. And it is also observed earlier that these ip’s also tried to do malware attack.

Ip’s that forced connection for malware attack:

Malware Detected	IP responsible for	User Targeted
Trojan	172.16.0.3, 192.168.1.101, 10.0.0.5	David, Charlie, Bob
Worm	203.0.113.77	Bob, David
Spyware	172.16.0.3	David
Rootkit	192.168.1.101, 10.0.0.5	David, Charlie, Bob
Ransomware	172.16.0.3	David



```
index="main" "action=connection attempt"
```

✓ 36 events (before 8/1/25 1:36:48.000 PM)

```
Time                  Event
7/3/25 8:21:14.000 AM  2025-07-03 08:21:14 | user=david | ip=172.16.0.3 | action=connection attempt
                       host = vibhuacer | source = SOC_Task2_Sample_Logs.txt | sourcetype = task 2
7/3/25 8:21:14.000 AM  2025-07-03 08:21:14 | user=david | ip=172.16.0.3 | action=connection attempt
                       host = vibhuacer | source = SOC_Task2_Sample_Logs.txt | sourcetype = task 2
7/3/25 8:21:14.000 AM  2025-07-03 08:21:14 | user=david | ip=172.16.0.3 | action=connection attempt
                       host = vibhuacer | source = SOC_Task2_Sample_Logs.txt | sourcetype = task 2
7/3/25 8:20:14.000 AM  2025-07-03 08:20:14 | user=charlie | ip=192.168.1.101 | action=connection attempt
                       host = vibhuacer | source = SOC_Task2_Sample_Logs.txt | sourcetype = task 2
7/3/25 8:20:14.000 AM  2025-07-03 08:20:14 | user=charlie | ip=192.168.1.101 | action=connection attempt
                       host = vibhuacer | source = SOC_Task2_Sample_Logs.txt | sourcetype = task 2
7/3/25 8:20:14.000 AM  2025-07-03 08:20:14 | user=charlie | ip=192.168.1.101 | action=connection attempt
                       host = vibhuacer | source = SOC_Task2_Sample_Logs.txt | sourcetype = task 2
7/3/25 7:44:14.000 AM  2025-07-03 07:44:14 | user=bob | ip=192.168.1.101 | action=connection attempt
                       host = vibhuacer | source = SOC_Task2_Sample_Logs.txt | sourcetype = task 2
7/3/25 7:44:14.000 AM  2025-07-03 07:44:14 | user=bob | ip=203.0.113.77 | action=connection attempt
                       host = vibhuacer | source = SOC_Task2_Sample_Logs.txt | sourcetype = task 2
7/3/25 7:44:14.000 AM  2025-07-03 07:44:14 | user=bob | ip=192.168.1.101 | action=connection attempt
                       host = vibhuacer | source = SOC_Task2_Sample_Logs.txt | sourcetype = task 2
```

Impact Assessment:

- Potential data exposure via unauthorized file access
- Credential guessing attempts on admin-level accounts
- High likelihood of lateral movement by attacker IPs

Recommended Response:

- Block or restrict IP 203.0.113.77 and 198.51.100.42
- Force password reset for impacted accounts (Bob, David)
- Scan endpoints for residual malware activity

📄 Summary

This incident response report investigates a series of security alerts detected via Splunk, including high-severity malware activity and unauthorized access attempts. Key events involve suspicious IP addresses linked to ransomware behaviour, credential brute-forcing, and potential account compromise. Through detailed log analysis and correlation of IP patterns, several user accounts were identified as impacted or at risk. The report outlines investigative findings, assesses system integrity, and provides actionable mitigation steps to contain the threat and prevent further incidents.

🏵Thing I learned from this assignment:

"This exercise deepened my understanding of log analysis and reinforced the importance of timely, ethical response in cybersecurity. Going forward, I'm motivated to apply this learning to real-world systems where protecting users means protecting trust. This assignment made the foundation of what real-world Security Operations Centre (SOC) teams do for live incident monitoring and response"