FUTURE INTERNS – CYBER SECURITY INTERNSHIP

Incident Response Report

Task 2: Security Alert Monitoring & Incident Response

FUTURE_CS_02_Incident_Response_Report

Prepared by: Shahana

Date: October 4, 2025

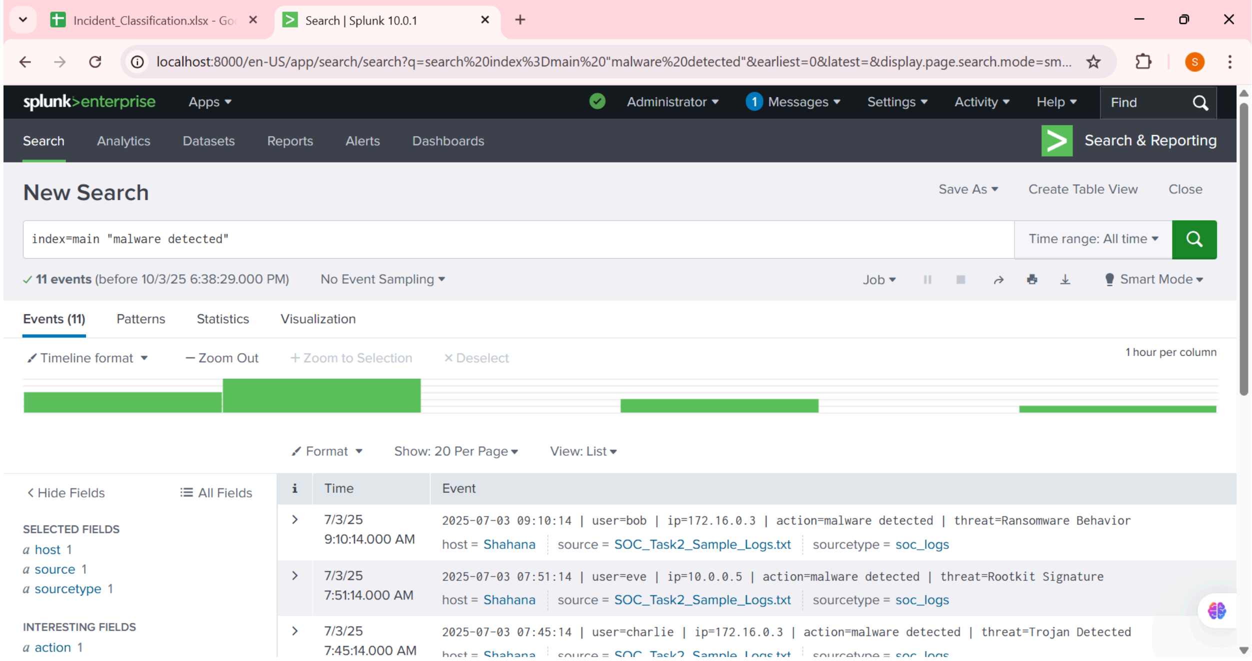
1. Executive Summary

During log monitoring in Splunk, multiple suspicious events were identified, including malware detections, failed login attempts, and external IP activity. Several of these are high-severity incidents suggesting possible system compromise and data exfiltration attempts.

2. Findings & Evidence

a) Malware Detections (High Severity)

- Trojan, Rootkit, Ransomware, Worm, Spyware alerts were detected.



```
index=main "malware detected"
```

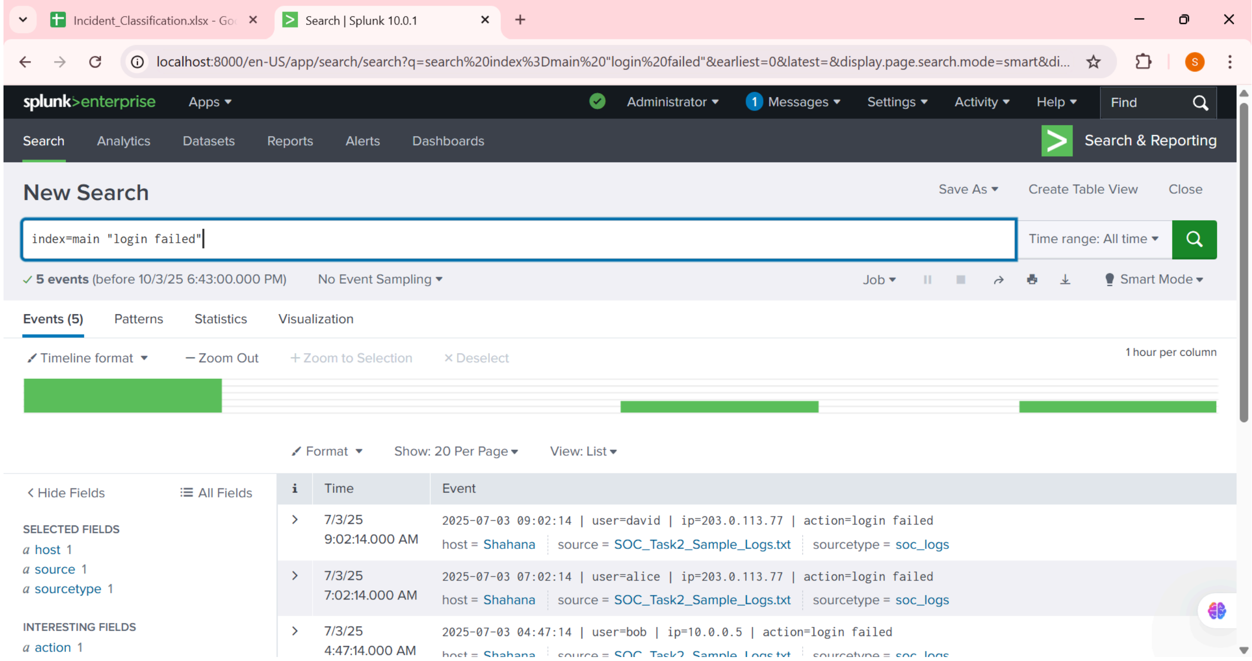
✓ 11 events (before 10/3/25 6:38:29.000 PM)

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 = Shahana source = SOC_Task2_Sample_Logs.txt sourcetype = soc_logs
>	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 = Shahana source = SOC_Task2_Sample_Logs.txt sourcetype = soc_logs
>	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 = Shahana source = SOC_Task2_Sample_Logs.txt sourcetype = soc_logs

malware_detected.png

b) Failed Logins (Medium Severity)

- Multiple users (bob, alice, david) had failed login attempts, some followed by later successes → possible brute force.



localhost:8000/en-US/app/search/search?q=search%20index%3Dmain%20"login%20failed"&earliest=0&latest=&display.page.search.mode=smart&di...

New Search

```
index=main "login failed"
```

Time range: All time

✓ 5 events (before 10/3/25 6:43:00.000 PM)   No Event Sampling

SELECTED FIELDS
a host 1
a source 1
a sourcetype 1

INTERESTING FIELDS
a action 1

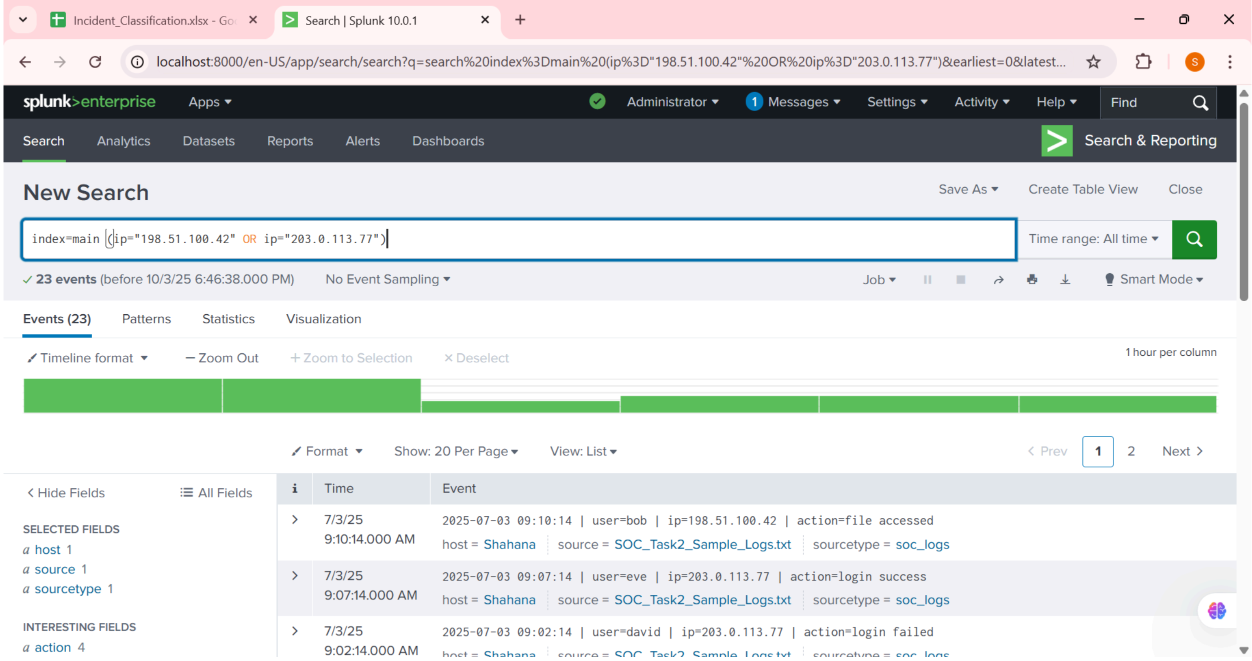
i	Time	Event
>	7/3/25 9:02:14.000 AM	2025-07-03 09:02:14 | user=david | ip=203.0.113.77 | action=login failed host = Shahana | source = SOC_Task2_Sample_Logs.txt | sourcetype = soc_logs
>	7/3/25 7:02:14.000 AM	2025-07-03 07:02:14 | user=alice | ip=203.0.113.77 | action=login failed host = Shahana | source = SOC_Task2_Sample_Logs.txt | sourcetype = soc_logs
>	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 = Shahana | source = SOC_Task2_Sample_Logs.txt | sourcetype = soc_logs

failed_logins.png

c) External IP Activity (High Severity)

- Users logged in or accessed files from public IPs 198.51.100.42 and 203.0.113.77.

- These IPs are outside the internal network and could indicate unauthorized access.



localhost:8000/en-US/app/search/search?q=search%20index%3Dmain%20(ip%3D"198.51.100.42"%20OR%20ip%3D"203.0.113.77")&earliest=0&latest...

```
index=main (ip="198.51.100.42" OR ip="203.0.113.77")
```

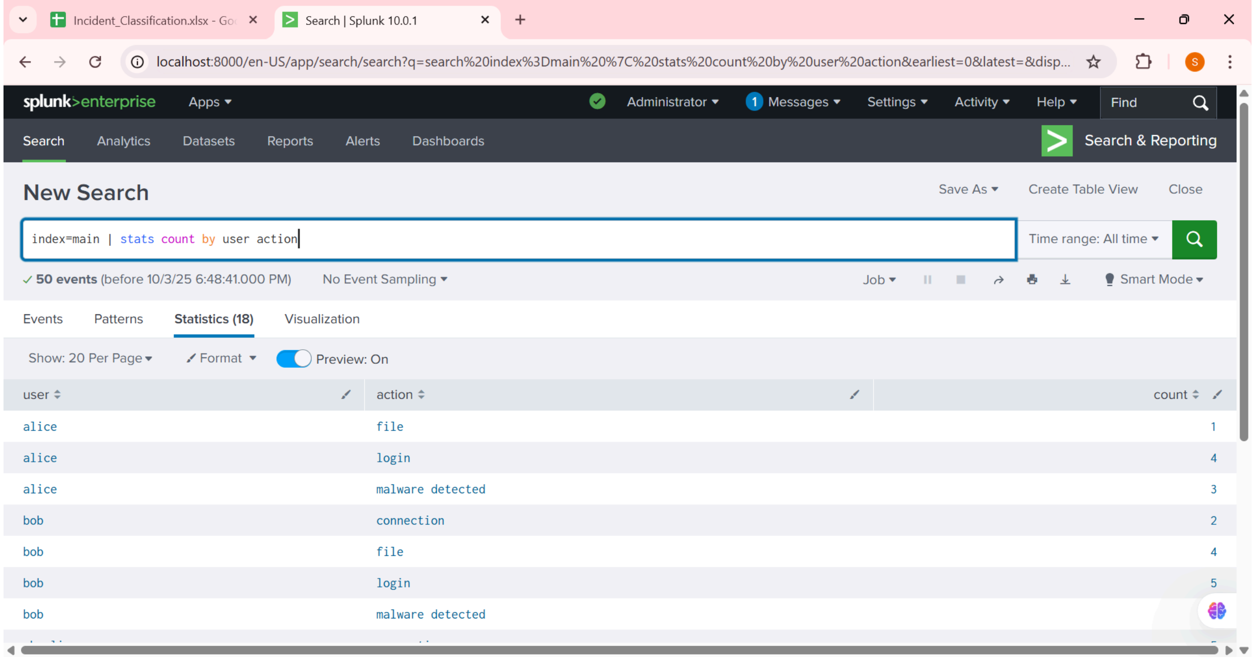
✓ 23 events (before 10/3/25 6:46:38.000 PM)

i	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 host = Shahana source = SOC_Task2_Sample_Logs.txt sourcetype = soc_logs
>	7/3/25 9:07:14.000 AM	2025-07-03 09:07:14 | user=eve | ip=203.0.113.77 | action=login success host = Shahana source = SOC_Task2_Sample_Logs.txt sourcetype = soc_logs
>	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 = Shahana source = SOC_Task2_Sample_Logs.txt sourcetype = soc_logs

external_ip.png

d) User Action Summary

- Stats table shows actions by each user (logins, malware detections, file access).



```
index=main | stats count by user action
```

✓ 50 events (before 10/3/25 6:48:41.000 PM) No Event Sampling

user	action	count
alice	file	1
alice	login	4
alice	malware detected	3
bob	connection	2
bob	file	4
bob	login	5
bob	malware detected	[illegible]

stats_summary.png

3. Impact Assessment

The analysis indicates several serious security issues. There is a high chance of credential compromise due to repeated failed logins followed by successful attempts. Multiple malware detections suggest that infected hosts might already be compromised, creating a risk of system instability and lateral movement within the network. Access from external public IPs indicates potential data exfiltration or unauthorized external control of internal systems.

4. Recommendations

1. Immediately isolate all affected hosts to prevent further spread of malware.

2. Block suspicious external IP addresses (198.51.100.42 and 203.0.113.77) at the firewall.

3. Force password resets for all affected user accounts (bob, alice, david, eve, charlie).

4. Conduct a full malware and antivirus scan on all infected systems.

5. Apply security patches and update endpoint protection software.

6. Enable multi-factor authentication (MFA) for all user logins.

7. Enhance monitoring rules in Splunk to alert on repeated login failures and external IP access.

8. Conduct a post-incident review to strengthen security playbooks.

5. Conclusion

This simulated SOC investigation using Splunk successfully demonstrated the process of detecting, analyzing, and responding to security alerts. The analysis revealed multiple high-severity incidents such as malware detections, failed login attempts, and external IP activity. These findings highlight the importance of proactive monitoring and quick response actions to contain and mitigate threats. Regular log reviews, updated security policies, and continuous SOC training are essential to maintain a strong cybersecurity posture.