SOC TASK 2: SECURITY ALERT MONITORING AND INCIDENT RESPONSE

NAME: ONONOGBU DANIELLA IHEOMA

INTERNSHIP: FUTURE INTERN

DATE: 3rd January, 2026.

1. INTRODUCTION

This report documents the monitoring and analysis of simulated security alerts from provided logs using Splunk Enterprise. The objective is to identify suspicious activity, classify incidents, and recommend remediation steps.

2. OBJECTIVES

- Monitor security alerts using a SIEM tool
- Identify suspicious activity and malware
- Classify incidents by severity (High, Medium, Low)
- Draft actionable incident response report
- Provide visual evidence via dashboards and screenshots

3. TOOLS USED

Splunk Enterprise – SIEM platform for log ingestion and analysis

Sample Logs – Provided by Future Intern

Microsoft Word / Google Docs – For report documentation

Microsoft Excel / Google Sheets – For Alert Classification Log

4. METHODOLOGY

1. Uploaded sample logs into Splunk using the Upload feature
2. Analyzed failed logins, suspicious IP activity, and malware alerts
3. Filtered search results per IP to identify affected users and events
4. Saved critical events to dashboard panels for visual summary
5. Classified incidents by severity (High, Medium, Low)
6. Documented incidents in a detailed report, with screenshots and timeline
7. Created an Alert Classification Log for tracking all incidents

5.0 INCIDENT TIMELINE

Incident Timeline – Summary of Security Events

Date	Time (Approx.)	IP Adress	Event Type	Affected Users	Description of Activity	Severity
03-07-2025	04:23 – 09:02	203.0.113.77	Authentication Failure	Alice, David	Multiple failed login attempts from a single public IP targeting different user accounts	Medium
03-07-2025	07:10 – 09:30	203.0.113.77	Malware Detection	Eve, Bob	Trojan and infection attempt alerts detected after repeated authentication activities	High
03-07-2025	04:20 – 06:50	10.0.0.5	Malware Detection	Bob, Eve	Multiple Trojan and rootkit malware alerts detected from same internal IP	High
03-07-2025	03:55 – 06:30	172.16.0.3	Malware Outbreak	Alice, Bob, Charlie, David	Ransomware behavior, spyware alerts, and Trojan detections across multiple users	High
03-07-2025	05:40 – 07:15	192.168.1.101	Network & Malware Activity	Bob, Charlie, Eve, Alice	Repeated connection attempts and Trojan malware alerts from internal IP	Medium
03-07-2025	04:47	198.51.100.42	Malware Detection	Alice	Isolated malware alert detected from a public IP	Low

The incident timeline summarizes key security events observed during log analysis in Splunk. Multiple incidents involving malware detection, repeated authentication failures, and abnormal user activity were identified. Events were prioritized based on severity, frequency, and potential impact on system integrity.

6. INCIDENT ANAIYSYS AND FINDINGS

Alert Triage and Analysis

Prior to detailed incident investigation, all detected security events were recorded and evaluated using an Alert Classification Log. Events were assessed based on severity, repetition, and associated threat indicators. Alerts classified as High or Critical were escalated for incident investigation. The complete alert classification is provided in Appendix A.

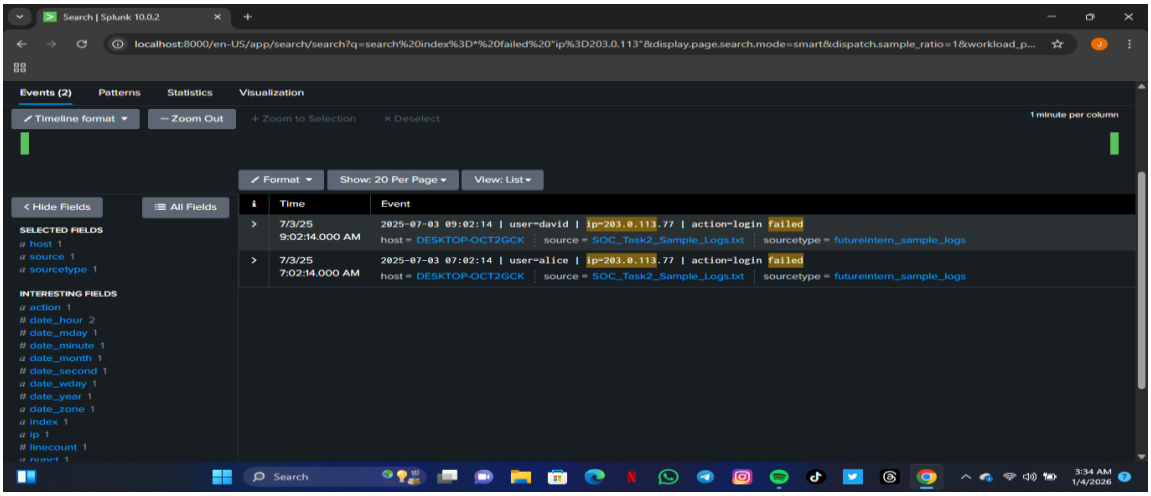
6.1 Failed Login Attempts

Incident Description

Analysis of authentication logs in Splunk revealed multiple failed login attempts involving different user accounts and originating from the same IP address. The pattern observed indicates repeated authentication failures across multiple users within a short time frame, which deviates from normal user behavior and may suggest a brute-force or credential-stuffing attempt.

IP Address	User	Event	Severity	Note
203.0.113.7	David	Login failed	High	External IP, multiple failed logins
203.0.113.7	Alice	Login failed	High	External IP, multiple failed logins
10.9.8.5	Bob	Login failed	Low	Internal IP, likely user error
172.16.0.3	Bob	Login failed	Low	Internal IP
172.16.0.3	Charlie	Login failed	Low	Internal IP

Figure 1: Multiple failed login attempts from a public IP address



This screenshot shows failed authentication attempts originating from IP 203.0.113.77 targeting multiple user accounts, indicating a possible brute-force or credential stuffing attempt.

Observations

- Multiple failed login attempts originated from the same public IP address.

- Different user accounts were targeted within a short time window.
- Single failed attempts from internal IPs were observed and assessed as low risk.
- The repeated nature of failed logins from a public IP suggests intentional probing rather than user error

Recommendations

- Monitor the identified IP address for further authentication attempts.
- Enforce account lockout policies after repeated failed logins.
- Implement multi-factor authentication (MFA) for user accounts.
- Review authentication logs regularly for similar patterns.
- Educate users on strong password practices.

6.2 **Suspicious IP Activity**

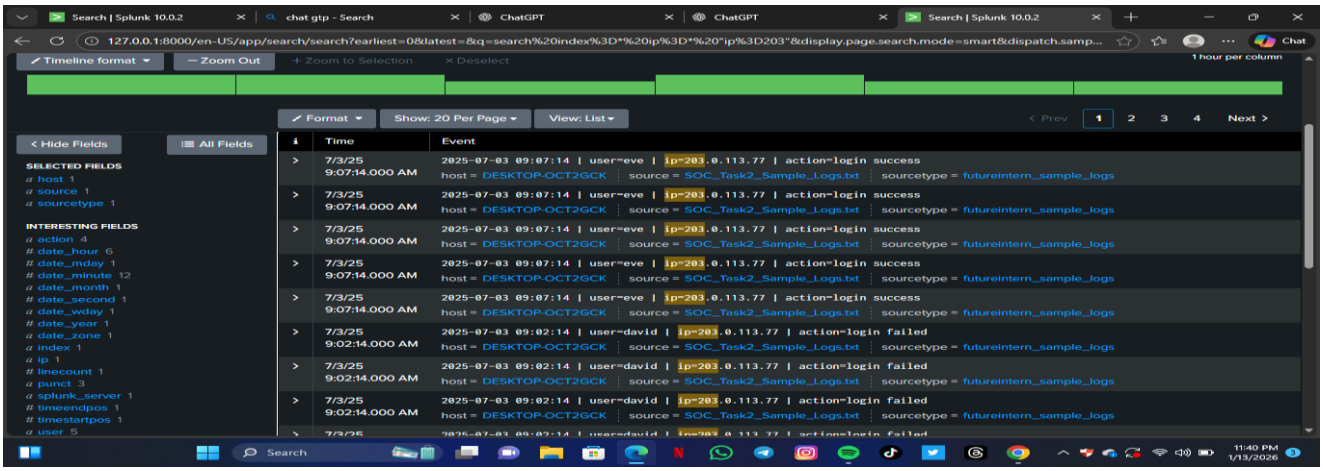
Incident Description

During log analysis in Splunk, multiple security events were observed originating from the same IP address and involving several user accounts. The IP address exhibited repeated authentication attempts, successful logins, and file access activities across different users, which is abnormal and indicative of suspicious behavior.

.

IP Address	Users Affected	Event Type	Severity	Note
203.0.113.7	Alice, Eve, David, Bob and Charlie	Failed and successful logins, file access	High	External public IP
10.0.0.5	Bob, Eve	Failed login, Malware detected	High	Internal IP
172.16.0.3	Bob, Charlie, David and Alice	Failed logins, Malware	Low	Internal Network
192.168.1.101	Bob and Charlie	Connection attempt, Malware detected	Medium	Internal IP

Figure 2: Suspicious IP accessing multiple user accounts



The image shows IP address 203.0.113.77 performing several login attempts (successful and failed) across different user accounts, which suggests abnormal access behavior requiring further investigation.

Observation

- Public IPs with repeated events are classified **High Severity**
- Internal IPs are mostly **Low/Medium Severity** unless malware is detected

Recommendation

- Monitor the IP address for continued suspicious activity.
- Enforce multi-factor authentication (MFA) for affected accounts.
- Review user access permissions and recent activity logs.
- Implement IP reputation checks and block the IP if malicious behavior persists.
- Educate users on secure login practices.

.

6.3 Malware Alert Incident Analysis

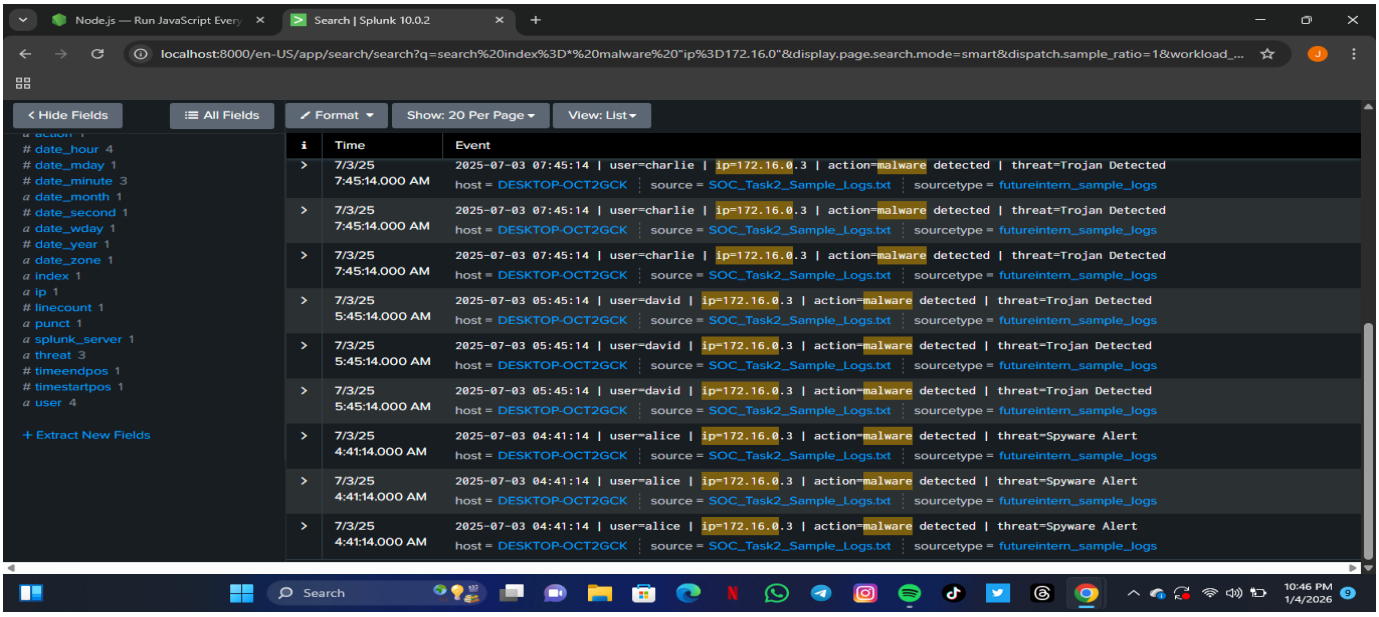
Incident Description

During security monitoring using Splunk SIEM, multiple malware detection alerts were identified across different user accounts and IP addresses. The alerts included various malware types such as Trojan infections, ransomware behavior, spyware alerts, and rootkit signatures. The recurrence and diversity of malware detections indicate compromised endpoints and represent a high-risk security incident.

IP Address	Malware Type Detected	Affected User	Numbers of Alerts	Risk
172.16.0.3	Ransomware behavior, Trojan detected, Spyware alert	Bob, Charlie, David, Alice	Multiple (10)	High

10.0.0.5	Trojan detected	Eve,	Multiple (6)	High
203.0.113.77	Trojan detected, Infection attempt	Eve, Bob	Multiple (6)	High
192.168.1.101	Trojan detected	Eve, Alice.	Multiple (5)	High
198.51.100.42	Malware detected	Alice	2	Medium

Figure 3: Repeated malware detections including ransomware and Trojan activity from IP address 172.16.0.3



This screenshot displays multiple malware alerts, including ransomware behavior and Trojan detections, affecting several user accounts from a single host, indicating a likely compromised system.

Observations

- Multiple malware types were detected, including high-impact threats such as ransomware.
- The same IP address was associated with malware alerts across several user accounts.
- Repeated detections suggest persistence rather than a one-time false positive.
- Malware activity affected both internal and external IP ranges, increasing risk exposure.
- Such behavior strongly indicates endpoint compromise.

Recommendations

- Immediately isolate affected systems from the network.
- Run full antivirus and endpoint detection scans.
- Reset credentials for affected user accounts.
- Block malicious IP addresses and update firewall rules.
- Review security patches and ensure systems are up to date.
- Conduct user awareness training on phishing and malware risks.

'A detailed log of all malware events can be found in Appendix A'.

7.0 SIEM Dashboard Summary

Purpose of the Dashboard

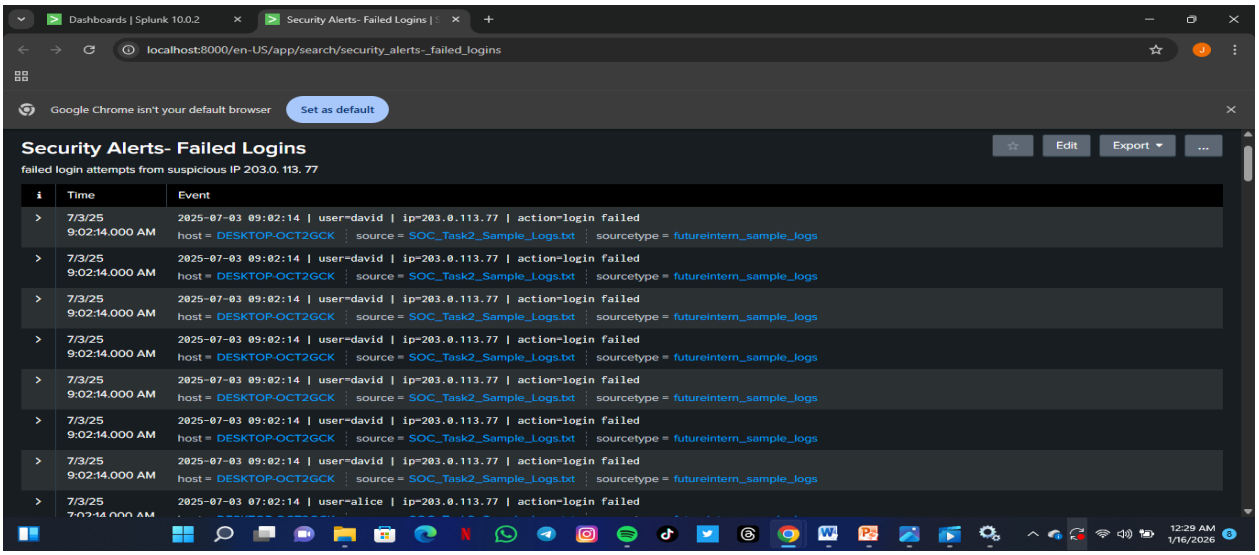
A SIEM dashboard was created in Splunk to provide a centralized view of key security events identified during the investigation. The Splunk dashboard provides visual summaries of the key incidents identified during log analysis. The panels include failed login attempts, suspicious IP activity, and malware alerts. These dashboard panels allow analysts to quickly assess incident trends and prioritize response actions. The figures below show the panels for each incident type.

Dashboard Panels Included

7.1 Failed Login Attempts Panel

- Displays repeated login failures by username and IP address.
- Highlights IPs attempting multiple authentications across user accounts

Figure 1: Failed Login Dashboard

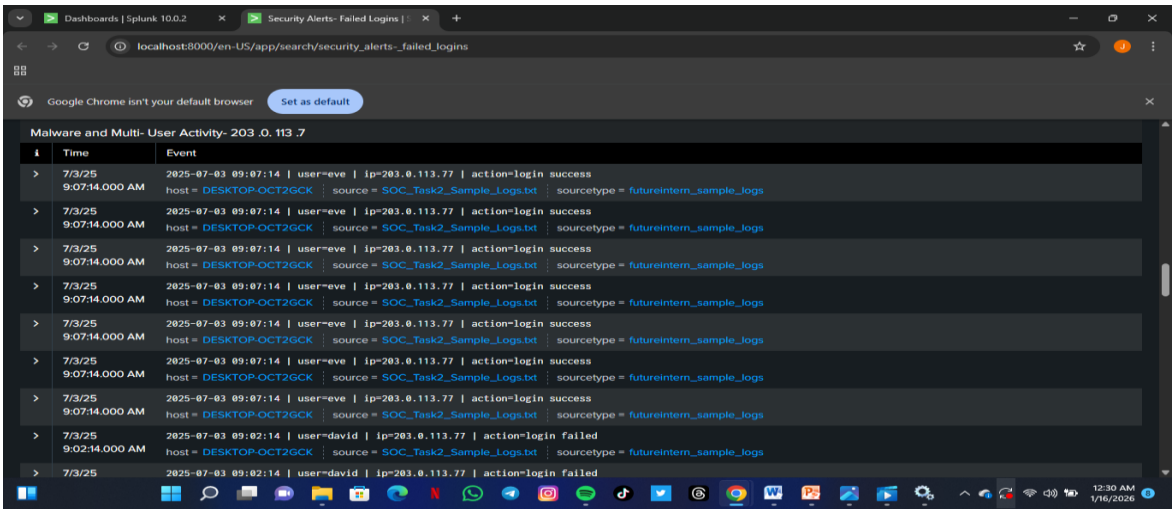


Dashboard panel showing failed login attempts from IP address 203.0.113.77.

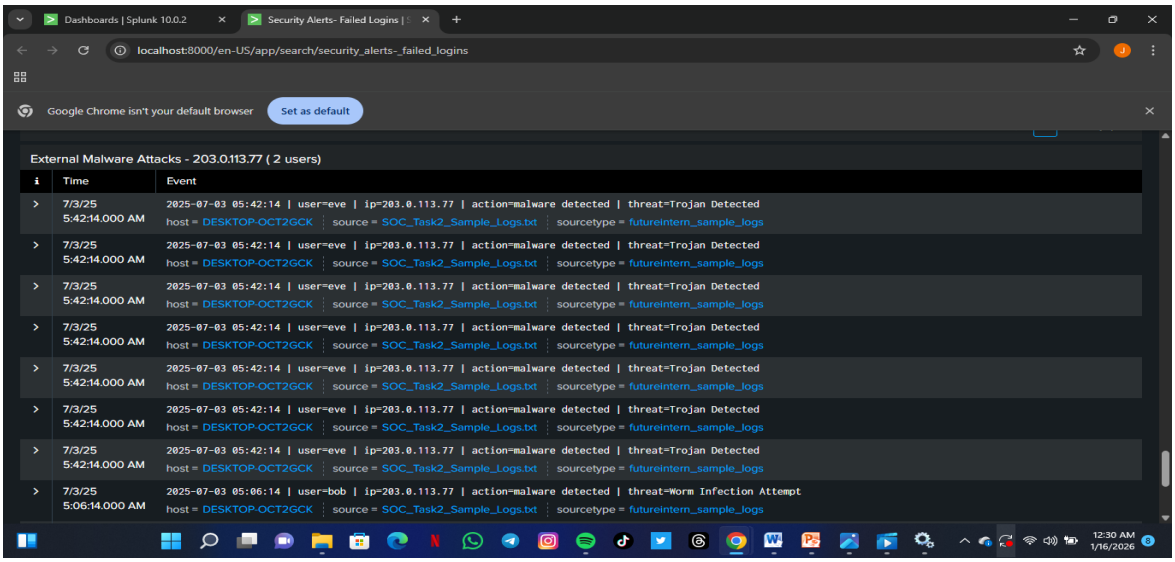
7.2 Suspicious IP Activity Panel

- Summarizes IPs with multiple connections, login attempts, and file access events.
- Helps identify potential brute-force or reconnaissance activity.

Figure 2: Suspicious IP Dashboard



Dashboard panel showing multi-user activity and malware events originating from suspicious IP address 203.0.113.7.



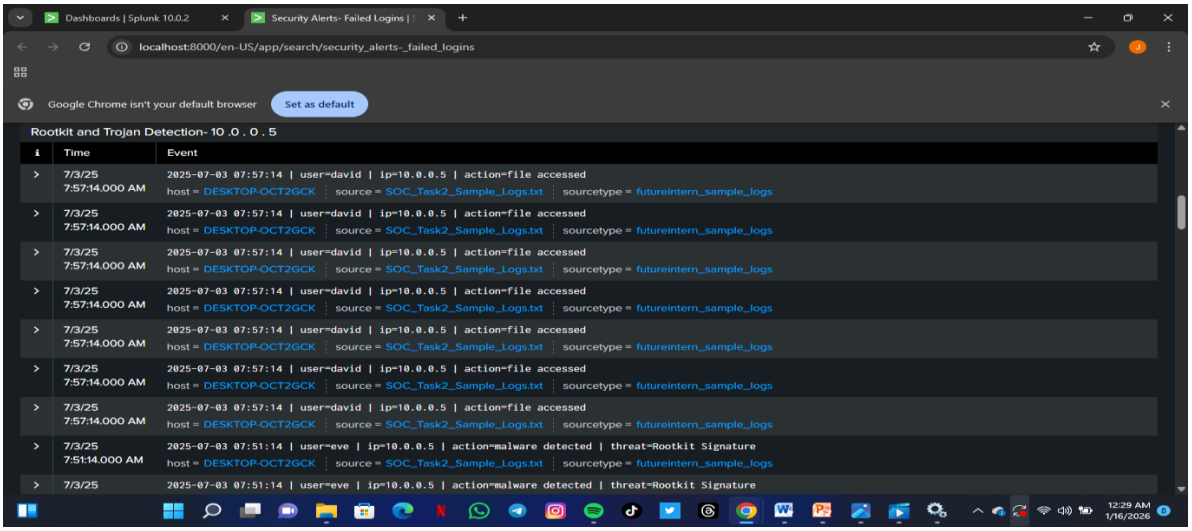
Dashboard panel highlighting external malware attacks and abnormal access patterns from IP address 203.0.113.77.

Filtered IP Search results are sown in Appendix B; Supporting Screenshots.

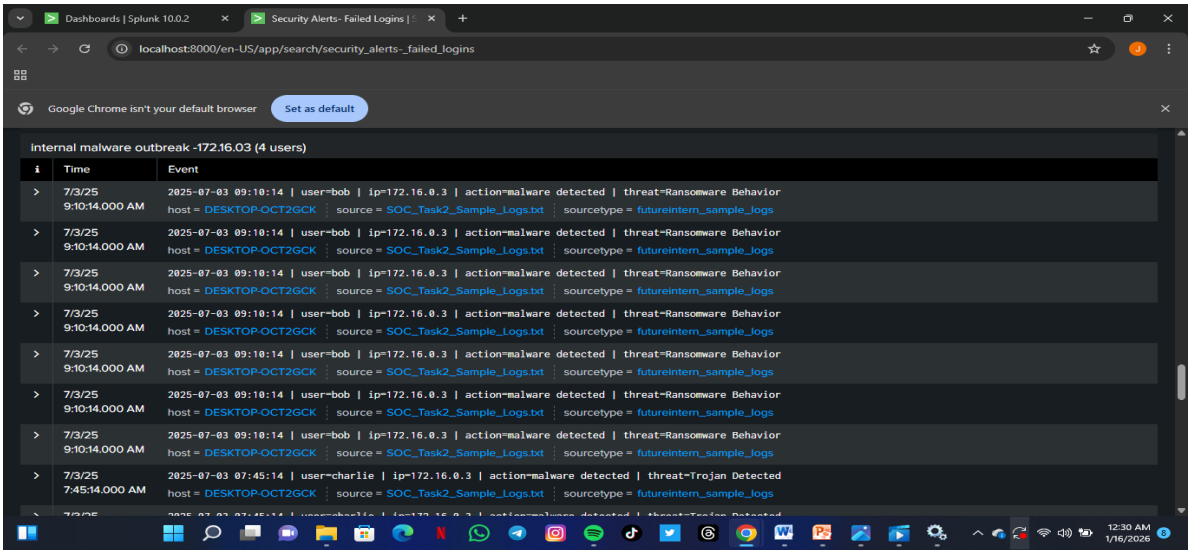
7.3 Malware Alerts Panel

- Displays malware detections (Trojan, ransomware, spyware) grouped by IP and affected users.
- Provides quick visibility of high-risk infections.

Figure 3: **Malware Alerts Panel Dashboard**



Dashboard panel displaying rookit and Trojan detections associated with IP address 10.0.0.5



Dashboard panel showing widespread internal malware activity affecting multiple user from IP address 172.16.0.3

The dashboard panels collectively provide a high-level view of security incidents. Analysts can quickly understand which IPs, users, or malware types are generating the most alerts, allowing prioritization of remediation and monitoring efforts.

8.0 Recommendations and Mitigation Measures

Based on the security incidents identified during log analysis, the following mitigation actions and recommendations are proposed to reduce risk, contain threats, and prevent recurrence.

8.1 Authentication and Access Control

Observed Issue:
Multiple failed login attempts from public IP addresses targeting different user accounts indicate possible brute-force or credential-stuffing attacks.

Recommendations:

- Enforce account lockout policies after repeated failed login attempts.
- Implement Multi-Factor Authentication (MFA) for all user accounts.
- Restrict login access from unknown or suspicious public IP addresses.
- Enable centralized authentication logging and alerting for abnormal login patterns.

8.2 Malware Detection and Response

Observed Issue:
Several malware alerts were detected, including Trojan infections, ransomware behavior, rootkit signatures, and spyware alerts affecting multiple users and systems.

Recommendations:

- Immediately isolate affected hosts from the network to prevent lateral movement.
- Perform full antivirus and endpoint detection scans on infected systems.
- Apply security patches and updates to operating systems and applications.
- Review endpoint security configurations and ensure real-time malware protection is enabled.

8.3 Network Monitoring and IP Reputation Management

Observed Issue:
Repeated malicious activity originating from specific IP addresses suggests targeted attack attempts and internal malware propagation.

Recommendations:

- Block known malicious public IP addresses using firewall or IDS/IPS rules.
- Monitor internal IP addresses exhibiting abnormal behavior for signs of compromise.
- Implement IP reputation filtering to automatically flag high-risk IP addresses.
- Conduct network segmentation to limit the spread of malware within internal networks.

8.4 Security Awareness and User Behavior

Observed Issue:
Malware detections across multiple user accounts may indicate unsafe user actions such as downloading malicious files or clicking phishing links.

Recommendations:

- Conduct regular security awareness training for users.
- Educate users on recognizing phishing attempts and suspicious downloads.
- Enforce least-privilege access to reduce the impact of compromised accounts.
- Periodically review user access rights and remove unnecessary privileges.

8.5 Incident Response Preparedness

Observed Issue:
Multiple incidents highlight the need for a structured response process.

Recommendations:

- Develop and maintain formal Incident Response Playbooks.
- Establish escalation procedures based on incident severity.
- Regularly test incident response processes through tabletop exercises.
- Maintain proper documentation and logging for forensic investigations.

9.0 Conclusion

This incident response exercise demonstrates the ability to monitor, analyze, and respond to security alerts using Splunk Enterprise. Multiple incidents, including failed logins, suspicious IP activity, and malware alerts, were identified and classified. Recommendations for mitigation and improved security posture have been provided. The report highlights practical SOC operations skills, including log analysis, incident classification, and dashboard monitoring.

10. Appendices

Note: All appendices are referenced in the main report for cross-verification of the events and analysis

Appendix A: Detailed Event Logs

Table A1: Detailed Event log summary

Date/Time	IP Address	Username	Event Type	Malware Type	severity	Notes
2025-07-03 04:23	172.16.0.3	Bob	Loin Failed	Ransomware	High	Part of malware detection incident
2025-07-03 04:23.sw	172.16.0.3	Charlie	Loin Failed	Trojan	High	Part of malware detection incident
2025-07-03 07:02	203.0.113.77	Alice	Login Success	_	Medium	Multiple login events from same IP
2025-07-03 07:02	203.0.113.77	David	Login Failed	_	Medium	Suspicious authentication activity
2025-07-03 09:02	10.0.0.5	Bob	Malware Detected	Trojan	High	Internal Malware Outbreak
2025-07-03 09:02	10.0.0.5	Eve	Malware Detected	Trojan	High	Internal Malware Outbreak
2025-07-03 09:02	203.0.113.77	File Access	File Access	_	Medium	External Suspicious IP activity
2025-07-03 09:02	203.0.113.77	File Access	File Access	_	Medium	External Suspicious IP activity

This table contains a comprehensive log of security-related events observed during the analysis. It supports the incident analysis discussed in Sections 4 and 5 of the report and enables cross-verification of detected threats.

Appendix B : Supporting Screenshots

This appendix contains screenshots of filtered Splunk search results and dashboard panels for the identified incidents

Figure B1: Failed login attempts from multiple users and IP addresses in Splunk

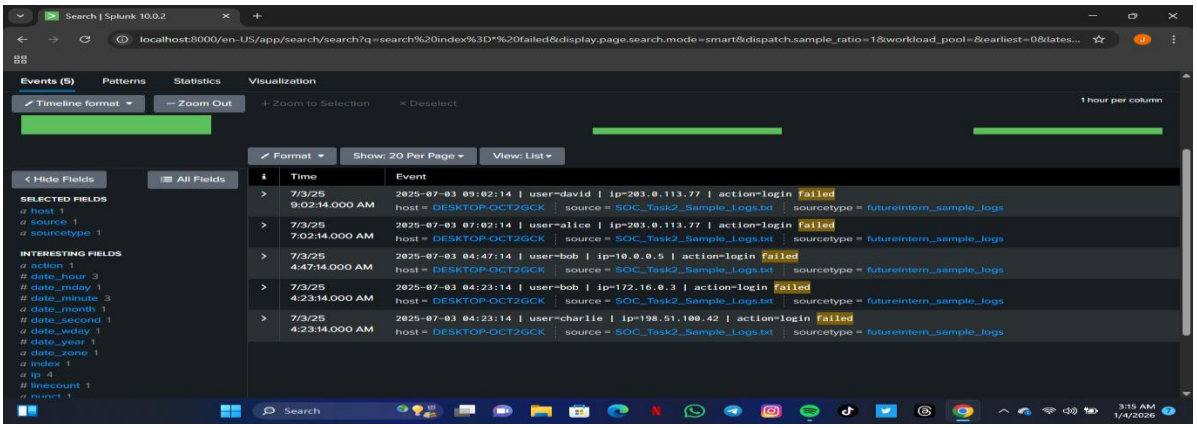
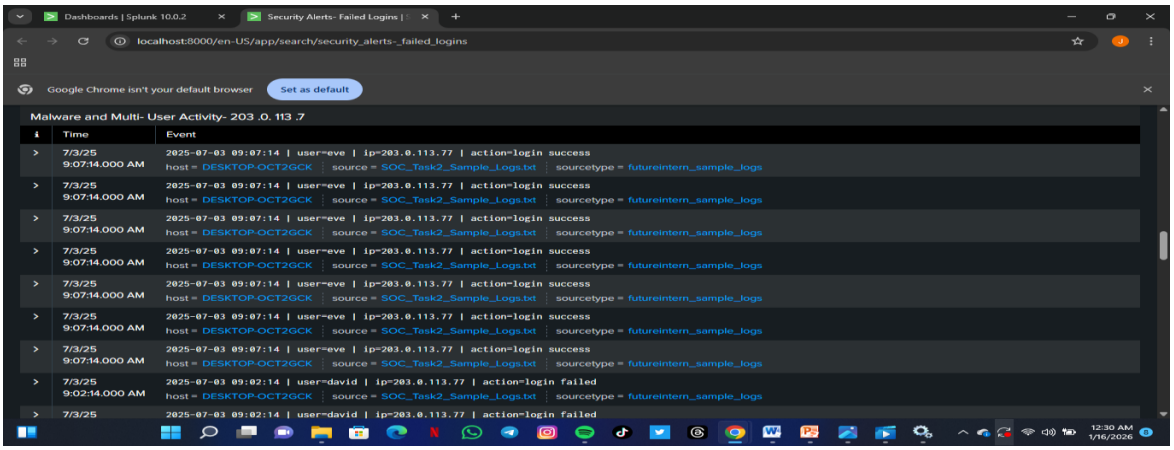
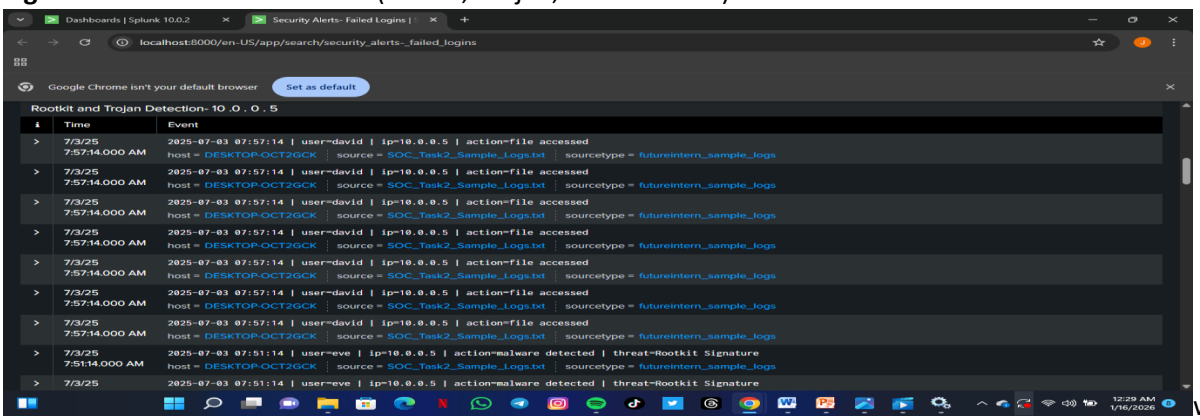


Figure B2: Suspicious IP activity (IP: 203.0.113.77)



Dashboard panel showing multi-user activity and malware events originating from suspicious IP address 203.0.113.7.

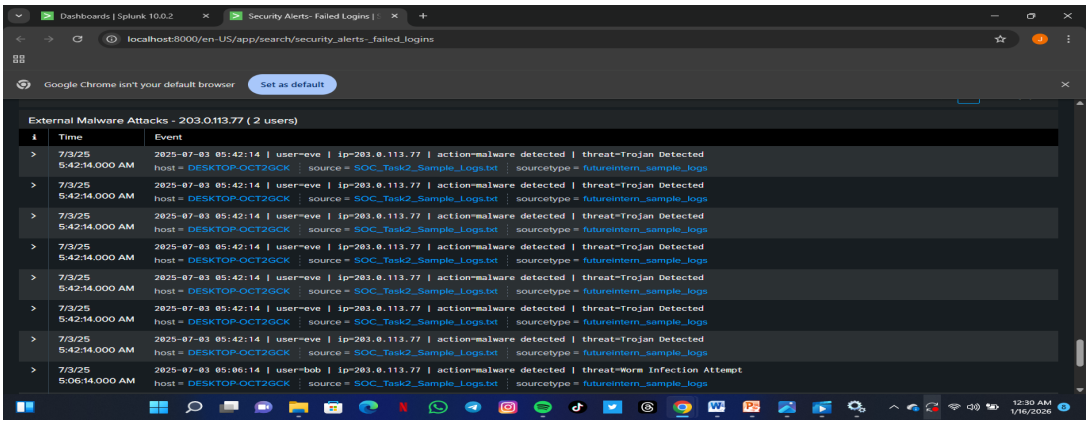
Figure B3: Malware detections (Rookit, Trojan, Ransomware) from IP 10.0.0.5



wa

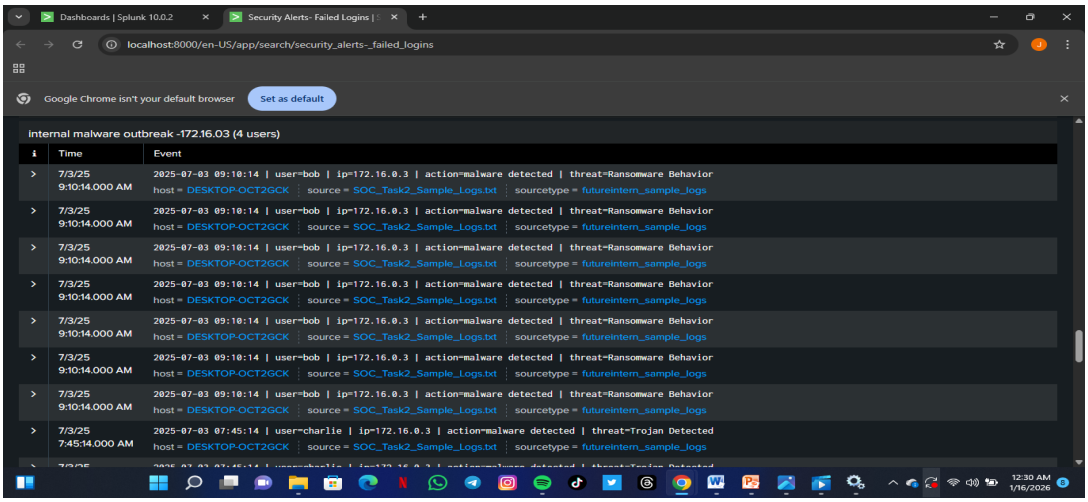
Dashboard panel displaying rookit and Trojan detections associated with IP address 10.0.0.5

Figure B4: Malware and multi-user activity from IP 203.0.113.77



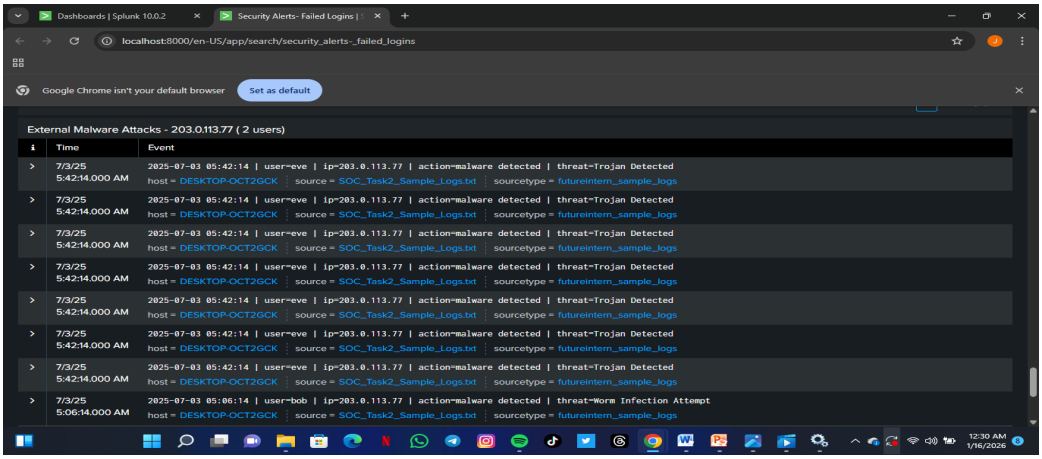
Dashboard panel showing multi-user activity and malware events originating from suspicious IP

Figure B5: Internal malware outbreak from IP 172.16.0.3



Dashboard panel showing widespread internal malware

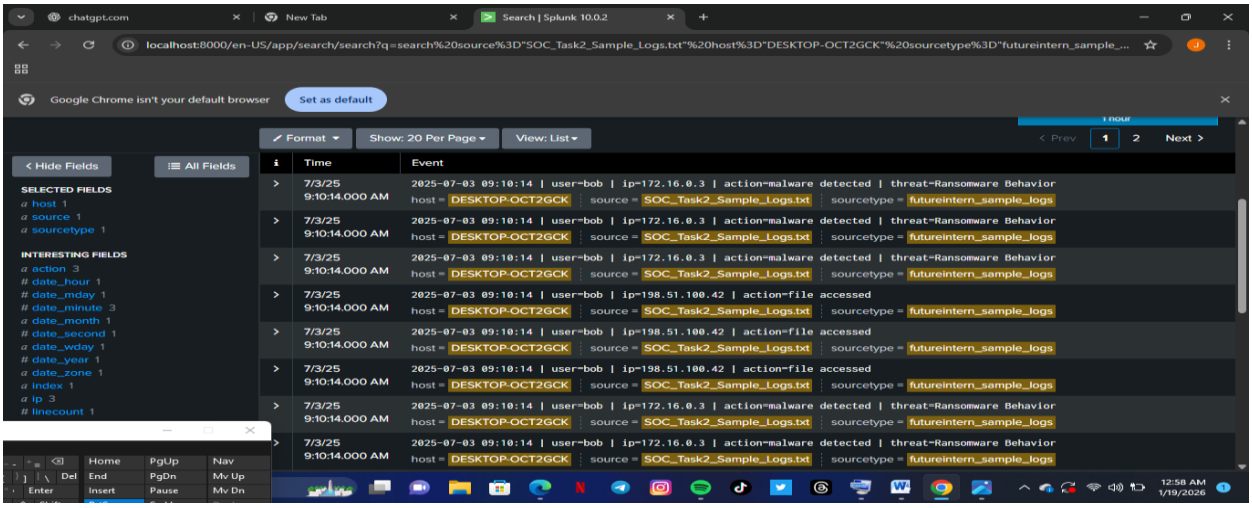
Figure B6: External malware attacks from IP 198.51.100.42



Dashboard panel highlighting external malware attacks and abnormal access

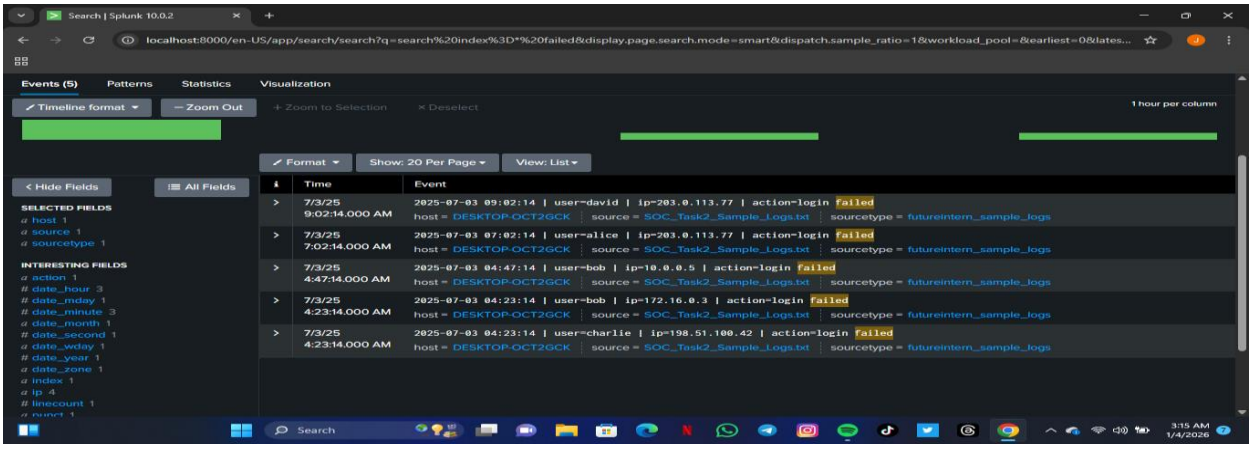
C Appendix C: Raw Sample Logs from SIEM Tool

This appendix includes excerpts from the provided `SOC_Task2_Sample_Logs.txt` file. These raw logs show the original system and network events that were analyzed for incident detection and classification.



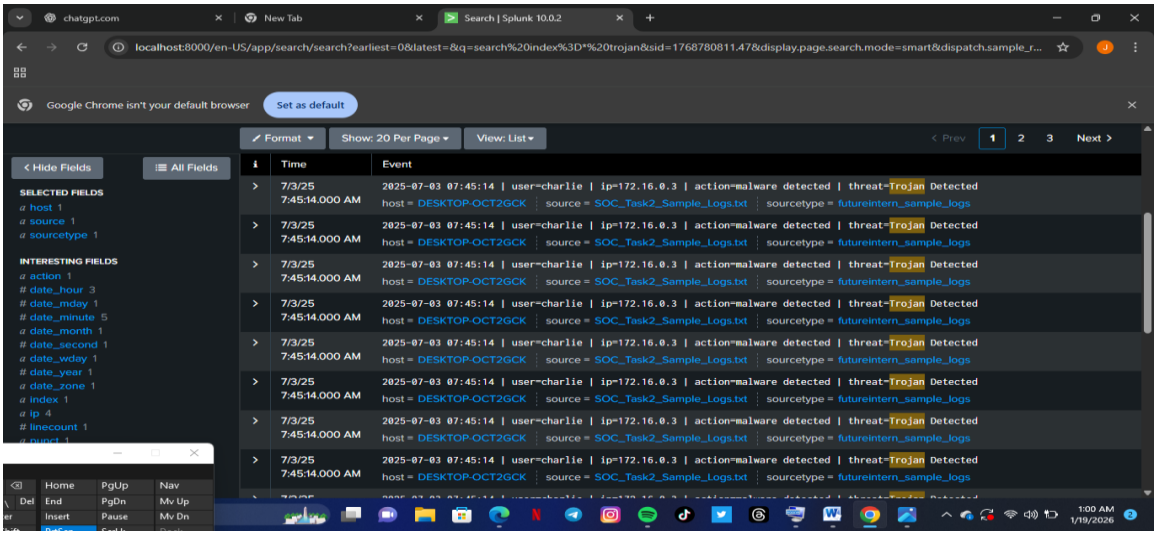
This appendix contains raw log samples obtained directly from the SIEM tool before extensive filtering or analysis. These logs serve as evidence supporting the incident findings discussed in the main report.

Figure C1: Raw authentication log showing failed login event from multiple users and IP addresses



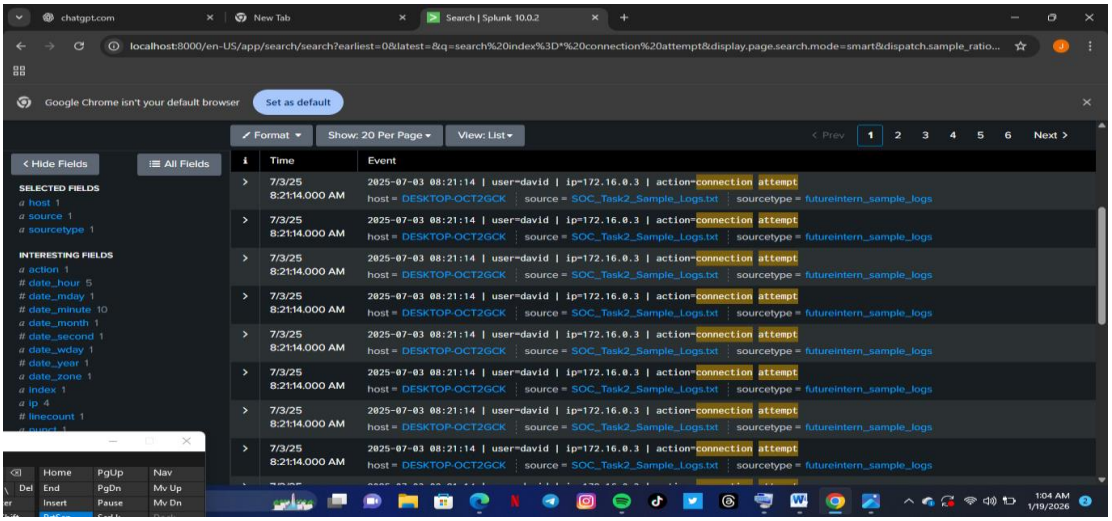
This screenshot presents unfiltered login events to demonstrate the source of failed authentication alerts discussed in Section 6.1: Failed Login Incident Analysis.

Figure C2: Raw malware detection log with Trojan signature



This screenshot captures the original malware detection events, highlighting Trojan threats detected across multiple users and hosts.

Figure C3: Raw connection attempt log from suspicious IP



This screenshot displays unfiltered connection attempt logs to provide evidence of suspicious activity associated with the incident analysis.

References / Acknowledgements

References

1. Splunk Documentation. “Getting Started with Splunk Enterprise.” https://docs.splunk.com
2. Elastic Stack Tutorials, Elastic.co. “Introduction to ELK for Log Analysis.” https://www.elastic.co/
3. Future Interns Internship Materials – Task 2: Security Alert Monitoring & Incident Response

Acknowledgements

I would like to acknowledge the guidance and mentorship of the Future Interns team during this task. Special thanks to the internship mentors for providing the sample logs, instructions, and support throughout the monitoring and incident response exercise.