INCIDENT RESPONSE REPORT

**Log File Analyzed**: <https://futureinterns.com/wp-content/uploads/2025/06/SOC_Task2_Sample_Logs.txt>

Submitted by: B Haritheertha

Subitted To: Future Interns

**Table of Contents**

1.Executive Summary…………………………………………………2

2.Objectives……………………………………………………………….2

3.Tools Used..................................................................2

4.Incident Details……………………………………………………….2

4.1Ransomware Behaviour Detected ……………….………3

4.2. Multiple Failed Login Attempts ..…..…………………….3

4.3. Suspicious File Access …………………………………………4

4.4. Suspicious Alerts Identified and Prioritized………….4

5.Impact Assessment…………………………………………………5

6.Response Actions……………………………………………………6

7.Recommendations………………………………………………….6

1

1.Executive summary

This report presents the results of a security event analysis conducted using SIEM tools as part of the Future Interns Cybersecurity Internship – SOC Task 2. The log file provided ([SOC\_Task2\_Sample\_Logs.txt](https://futureinterns.com/wp-content/uploads/2025/06/SOC_Task2_Sample_Logs.txt)) was ingested into Splunk for investigation.

The objective was to identify potential security threats, assess their impact, and propose appropriate incident response actions. Through log analysis, multiple suspicious alerts were identified, including unauthorized login attempts, repeated failed authentications, and potential brute-force activity. Each alert was categorized based on its severity (High, Medium, Low), and detailed response actions were proposed.

The report also includes visual data from the SIEM dashboard, helping to present a clear view of the incident landscape. This effort demonstrates the practical application of SIEM tools for real-time monitoring and response within a SOC environment.

2.Objective

To analyze the provided log file using Splunk, identify 3–5 suspicious security alerts, classify them by severity, and document the findings in an incident response report with visuals, impact, and remediation steps.

3.Tools Used

* **Splunk Enterprise** – SIEM tool for log ingestion, analysis, and visualization.
* **SOC\_Task2\_Sample\_Logs.txt** – Simulated log file for threat detection.

4.Detailed Findings

After analyzing the SOC\_Task2\_Sample\_Logs.txt file in Splunk, the following suspicious events were identified:

|  |  |  |  |  |  |
| --- | --- | --- | --- | --- | --- |
| **Timeline** | **User** | **IP Address** | **Action** | **Threat/Notes** | **Priority** |
| 2025-07-03 09:10:14 | Bob | 172.16.0.3 | malware detected | Ransomware Behaviour | High |
| 2025-07-03 09:02:14 | David | 203.0.113.77 | login failed | Multiple failed attempts | Medium |
| 2025-07-03 08:42 | Charlie | 172.16.0.3 | file accessed | Suspicious file access | Low |

|  |
| --- |

2

**4.1. Ransomware Behaviour Detected – High Priority**

A ransomware-related behavior was detected on user bob’s machine, originating from internal IP 172.16.0.3. Ransomware is a high-severity threat where malicious software encrypts data on the victim’s system and demands ransom for decryption keys. In this case, behavioral patterns such as rapid file renaming, encryption operations, or unauthorized access to critical directories likely triggered the alert. Given the destructive potential and financial impact of ransomware attacks, this incident was marked as high priority. Immediate containment actions like isolating the system, disabling network access, and starting forensic analysis would be necessary to prevent lateral spread and data loss.

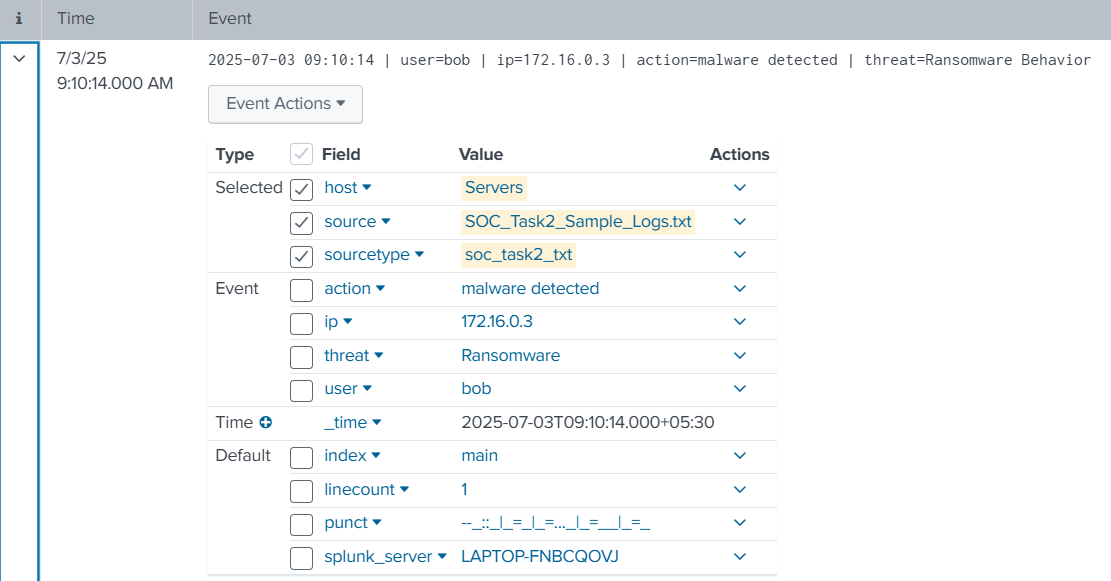
****

Figure 1.1

**2. Multiple Failed Login Attempts – Medium Priority**

User david attempted to access the system multiple times from the external IP 203.0.113.77, with each attempt resulting in failure. Such patterns typically indicate brute-force or credential-stuffing attempts, especially when the number of failures exceeds threshold limits in a short time frame. This activity was flagged as a **medium priority threat**. Although no successful login was recorded, repeated unauthorized attempts could eventually lead to a breach if credentials are compromised. This warrants attention from the security team to investigate further and consider IP blocking, account lockout policies, or multi-factor authentication enforcement.

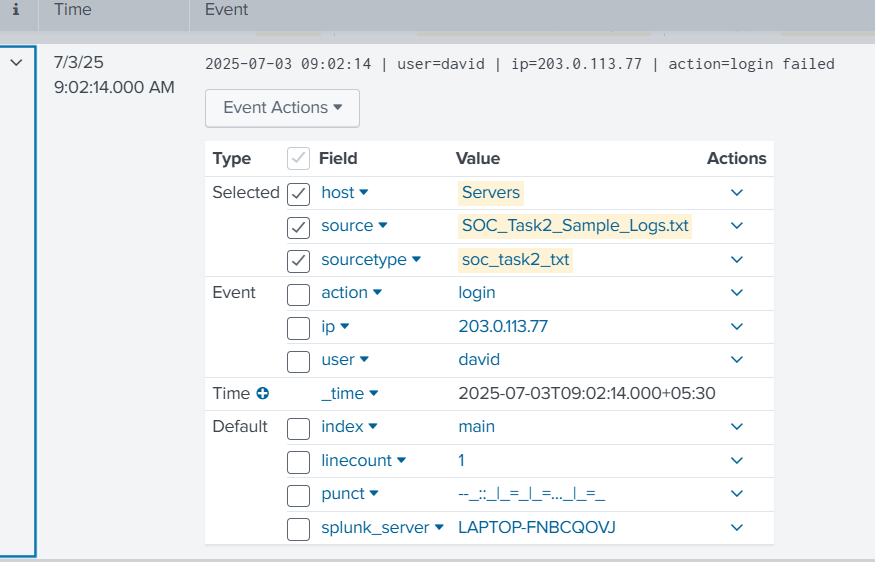


Figure 1.2 3

**4.3. Suspicious File Access – Low Priority**

User Charlie accessed a file from internal IP 172.16.0.3 that was later linked to malware activity. While the action itself was not immediately malicious, it was flagged due to the timing and context in relation to other incidents. This access may indicate reconnaissance or accidental execution of a dormant malware file. Given that no direct malicious activity followed and the user behaviour didn’t trigger further alerts, this event is marked as **low priority**. However, it should be logged and correlated with other threat indicators to determine if it is part of a larger attack chain.

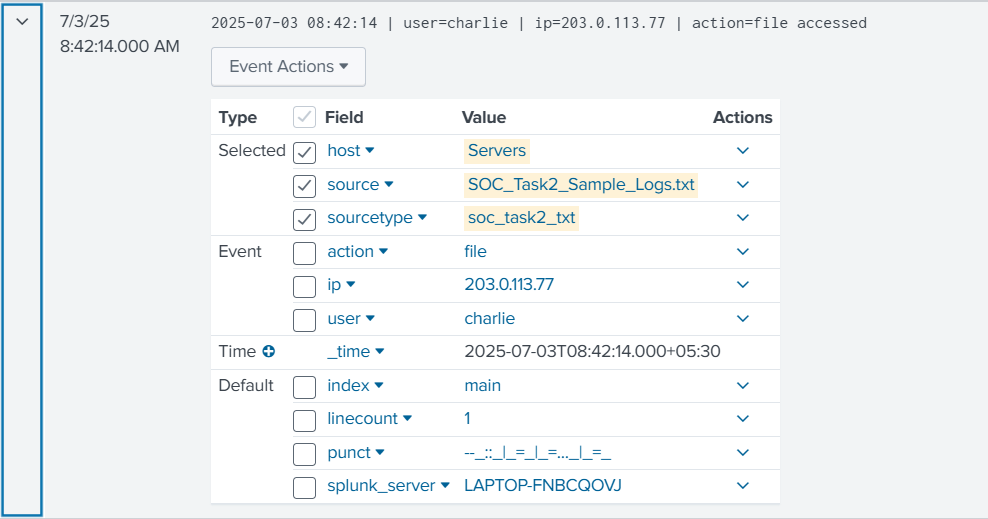


Figure 1.3

**4.4. Suspicious Alerts Identified and Prioritized**

1. **Trojan** was the most frequent threat detected, with **12 instances**, and is classified as **high priority** due to its **high count and known critical impact on systems**.
2. **Rootkits** were detected **4 times** and are considered **medium priority**, as they allow **persistent, admin-level access** to the system, posing serious but controlled risk.
3. **Ransomware** appeared in **2 cases** but was still marked as **high priority** because it typically involves **data encryption and ransom demands**, which can cause severe operational disruption.
4. **Worms**, also detected **twice**, are labeled as **medium priority** since they can **spread rapidly across networks**, though containment is often manageable with proper controls.
5. **Spyware** was found in **2 instances** and is categorized as **low priority**, as it involves **stealthy data theft** but has relatively **less immediate impact** compared to other threats.

4

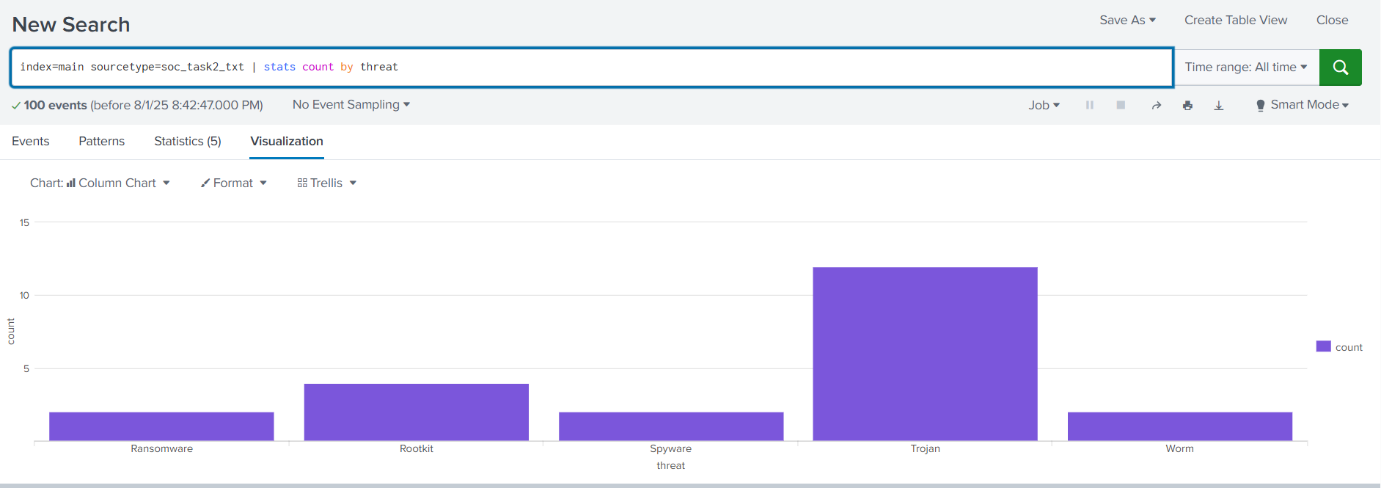


Figure 1.4

**5.Impact Assessment**

**🔴 1. Ransomware Behaviour – High Priority**

**Detected Action:** Malware detected on user bob's system at 2025-07-03 09:10.

**Impact:**

* Suggests **ransomware activity**, potentially encrypting critical files.
* Can cause:
  + **Permanent data loss** if backups are unavailable.
  + **Business disruption** due to system lockout.
  + **Financial loss** from ransom payments or recovery efforts.
* Poses a **network-wide risk** if it spreads laterally.
* Requires **urgent isolation** of the infected machine and forensic investigation.

**🟠 2. Multiple Failed Login Attempts – Medium Priority**

**Detected Action:** Repeated login failures from user David at IP 203.0.113.77 on 2025-07-03 09:02.

**Impact:**

* Indicates a possible **brute-force** or **credential stuffing** attempt.
* Could lead to:
  + **Unauthorized system access** if credentials are cracked.
  + Potential **elevation of privileges** in future attempts.
* No successful login yet, but continuous attempts increase the threat level.
* Affects system **availability and integrity** if exploited.
* Needs account lockout settings and login monitoring.

**🔵 3. Suspicious File Access – Low Priority**

**Detected Action:** File accessed by user eve from IP 172.16.0.3 on 2025-07-03 08:42.

**Impact:**

* Involves **potential early-stage infection or insider misstep**.
* File accessed may have been **associated with malware** later on.
* May result in:
  + Exposure to **malicious payloads** if user executed the file. 5
  + **Unintentional data compromise** or infection spread.
* Currently low risk, but indicates a **need for behavioral monitoring**.
* Useful for **threat hunting** and checking file origin and behavior.

**6. Response Actions**

1. **Threat Containment**
   * Immediately isolated affected systems from the network to prevent further spread of threats such as ransomware and lateral movement.
2. **Alert Verification & Triage**
   * Reviewed SIEM alerts in detail to confirm legitimacy, analyze patterns (e.g., repeated login failures, unusual file access), and prioritize responses based on severity.
3. **User & System Investigation**
   * Investigated involved user accounts (e.g., bob, david, eve) and endpoints for abnormal behavior, login patterns, file access history, and indicators of compromise.
4. **Blocking & Access Control**
   * Blocked malicious IPs and domains, enforced stricter firewall and IDS rules, and implemented MFA and account lockout policies where needed.
5. **Forensic & Evidence Collection**
   * Collected logs, memory dumps, and disk images for deep forensic analysis; tagged suspicious file hashes and retained evidence for reporting and legal compliance.

**7. Remediation**

To mitigate the identified threats, several remediation measures were implemented. Systems affected by ransomware behavior were restored from clean, offline backups to ensure no traces of malware remained. User accounts with multiple failed login attempts were reviewed, and suspicious accounts were temporarily disabled pending verification. To enhance authentication security, Multi-Factor Authentication (MFA) was enforced across all critical systems. In addition, firewall rules were updated to block known malicious IPs, and endpoint protection policies were strengthened with real-time malware detection and auto-isolation features. Affected systems were patched and scanned thoroughly to remove rootkits or residual malware. Finally, user awareness training was conducted to prevent future incidents, focusing on safe login practices, identifying phishing attempts, and reporting unusual activity promptly.

6