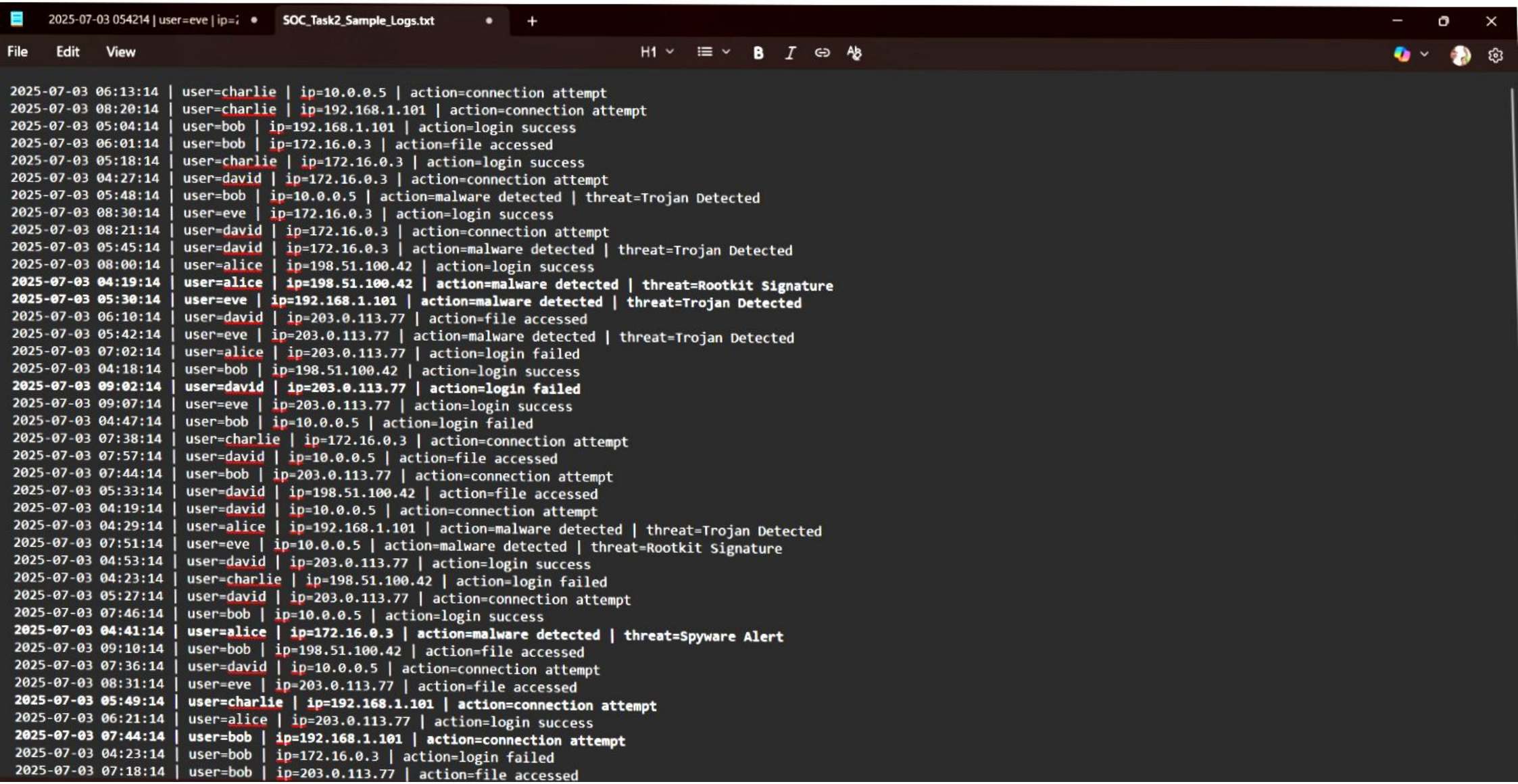
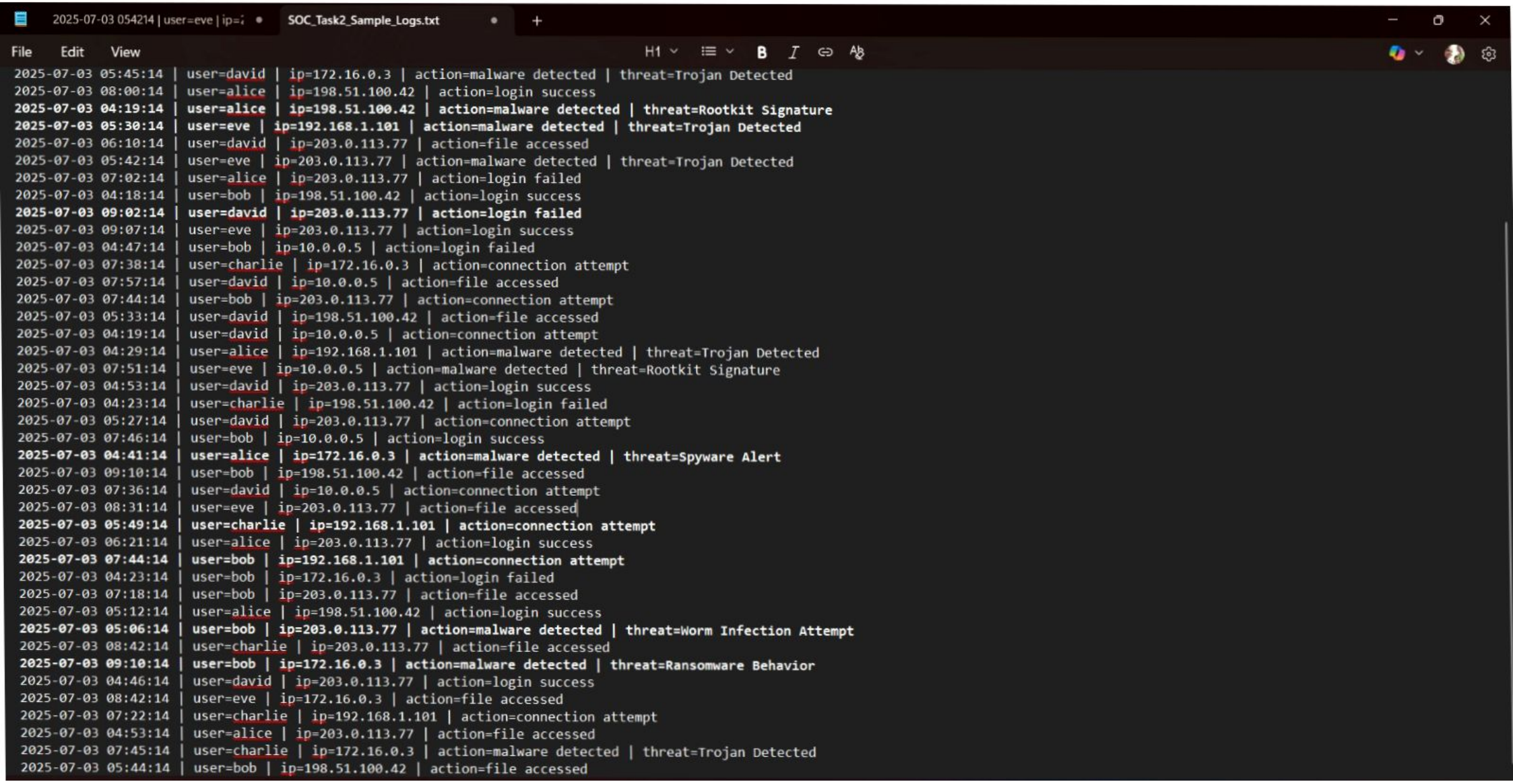
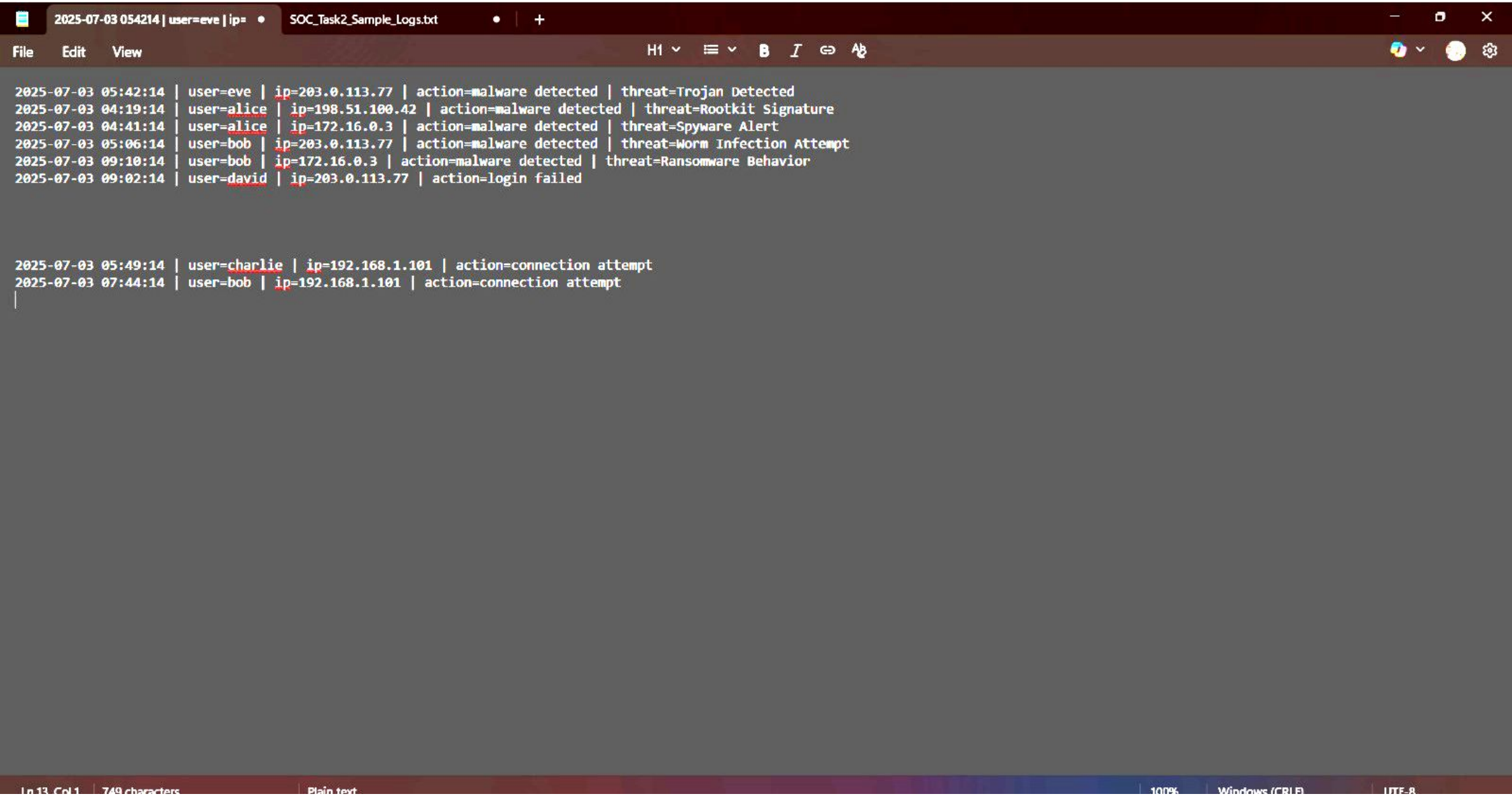

2025-07-03 054214 | user=eve | ip=
SOC_Task2_Sample_Logs.txt
File
Edit
View
H1
2025-07-03 06:13:14 | user=charlie | ip=10.0.0.5 | action=connection attempt
2025-07-03 08:20:14 | user=charlie | ip=192.168.1.101 | action=connection attempt
2025-07-03 05:04:14 | user=bob | ip=192.168.1.101 | action=login success
2025-07-03 06:01:14 | user=bob | ip=172.16.0.3 | action=file accessed
2025-07-03 05:18:14 | user=charlie | ip=172.16.0.3 | action=login success
2025-07-03 04:27:14 | user=david | ip=172.16.0.3 | action=connection attempt
2025-07-03 05:48:14 | user=bob | ip=10.0.0.5 | action=malware detected | threat=Trojan Detected
2025-07-03 08:30:14 | user=eve | ip=172.16.0.3 | action=login success
2025-07-03 08:21:14 | user=david | ip=172.16.0.3 | action=connection attempt
2025-07-03 05:45:14 | user=david | ip=172.16.0.3 | action=malware detected | threat=Trojan Detected
2025-07-03 08:00:14 | user=alice | ip=198.51.100.42 | action=login success
2025-07-03 04:19:14 | user=alice | ip=198.51.100.42 | action=malware detected | threat=Rootkit Signature
2025-07-03 05:30:14 | user=eve | ip=192.168.1.101 | action=malware detected | threat=Trojan Detected
2025-07-03 06:10:14 | user=david | ip=203.0.113.77 | action=file accessed
2025-07-03 05:42:14 | user=eve | ip=203.0.113.77 | action=malware detected | threat=Trojan Detected
2025-07-03 07:02:14 | user=alice | ip=203.0.113.77 | action=login failed
2025-07-03 04:18:14 | user=bob | ip=198.51.100.42 | action=login success
2025-07-03 09:02:14 | user=david | ip=203.0.113.77 | action=login failed
2025-07-03 09:07:14 | user=eve | ip=203.0.113.77 | action=login success
2025-07-03 04:47:14 | user=bob | ip=10.0.0.5 | action=login failed
2025-07-03 07:38:14 | user=charlie | ip=172.16.0.3 | action=connection attempt
2025-07-03 07:57:14 | user=david | ip=10.0.0.5 | action=file accessed
2025-07-03 07:44:14 | user=bob | ip=203.0.113.77 | action=connection attempt
2025-07-03 05:33:14 | user=david | ip=198.51.100.42 | action=file accessed
2025-07-03 04:19:14 | user=david | ip=10.0.0.5 | action=connection attempt
2025-07-03 04:29:14 | user=alice | ip=192.168.1.101 | action=malware detected | threat=Trojan Detected
2025-07-03 07:51:14 | user=eve | ip=10.0.0.5 | action=malware detected | threat=Rootkit Signature
2025-07-03 04:53:14 | user=david | ip=203.0.113.77 | action=login success
2025-07-03 04:23:14 | user=charlie | ip=198.51.100.42 | action=login failed
2025-07-03 05:27:14 | user=david | ip=203.0.113.77 | action=connection attempt
2025-07-03 07:46:14 | user=bob | ip=10.0.0.5 | action=login success
2025-07-03 04:41:14 | user=alice | ip=172.16.0.3 | action=malware detected | threat=Spyware Alert
2025-07-03 09:10:14 | user=bob | ip=198.51.100.42 | action=file accessed
2025-07-03 07:36:14 | user=david | ip=10.0.0.5 | action=connection attempt
2025-07-03 08:31:14 | user=eve | ip=203.0.113.77 | action=file accessed
2025-07-03 05:49:14 | user=charlie | ip=192.168.1.101 | action=connection attempt
2025-07-03 06:21:14 | user=alice | ip=203.0.113.77 | action=login success
2025-07-03 07:44:14 | user=bob | ip=192.168.1.101 | action=connection attempt
2025-07-03 04:23:14 | user=bob | ip=172.16.0.3 | action=login failed
2025-07-03 07:18:14 | user=bob | ip=203.0.113.77 | action=file accessed


2025-07-03 054214 | user=eve | ip=
SOC_Task2_Sample_Logs.txt
File
Edit
View
H1
2025-07-03 05:45:14 | user=david | ip=172.16.0.3 | action=malware detected | threat=Trojan Detected
2025-07-03 08:00:14 | user=alice | ip=198.51.100.42 | action=login success
2025-07-03 04:19:14 | user=alice | ip=198.51.100.42 | action=malware detected | threat=Rootkit Signature
2025-07-03 05:30:14 | user=eve | ip=192.168.1.101 | action=malware detected | threat=Trojan Detected
2025-07-03 06:10:14 | user=david | ip=203.0.113.77 | action=file accessed
2025-07-03 05:42:14 | user=eve | ip=203.0.113.77 | action=malware detected | threat=Trojan Detected
2025-07-03 07:02:14 | user=alice | ip=203.0.113.77 | action=login failed
2025-07-03 04:18:14 | user=bob | ip=198.51.100.42 | action=login success
2025-07-03 09:02:14 | user=david | ip=203.0.113.77 | action=login failed
2025-07-03 09:07:14 | user=eve | ip=203.0.113.77 | action=login success
2025-07-03 04:47:14 | user=bob | ip=10.0.0.5 | action=login failed
2025-07-03 07:38:14 | user=charlie | ip=172.16.0.3 | action=connection attempt
2025-07-03 07:57:14 | user=david | ip=10.0.0.5 | action=file accessed
2025-07-03 07:44:14 | user=bob | ip=203.0.113.77 | action=connection attempt
2025-07-03 05:33:14 | user=david | ip=198.51.100.42 | action=file accessed
2025-07-03 04:19:14 | user=david | ip=10.0.0.5 | action=connection attempt
2025-07-03 04:29:14 | user=alice | ip=192.168.1.101 | action=malware detected | threat=Trojan Detected
2025-07-03 07:51:14 | user=eve | ip=10.0.0.5 | action=malware detected | threat=Rootkit Signature
2025-07-03 04:53:14 | user=david | ip=203.0.113.77 | action=login success
2025-07-03 04:23:14 | user=charlie | ip=198.51.100.42 | action=login failed
2025-07-03 05:27:14 | user=david | ip=203.0.113.77 | action=connection attempt
2025-07-03 07:46:14 | user=bob | ip=10.0.0.5 | action=login success
2025-07-03 04:41:14 | user=alice | ip=172.16.0.3 | action=malware detected | threat=Spyware Alert
2025-07-03 09:10:14 | user=bob | ip=198.51.100.42 | action=file accessed
2025-07-03 07:36:14 | user=david | ip=10.0.0.5 | action=connection attempt
2025-07-03 08:31:14 | user=eve | ip=203.0.113.77 | action=file accessed
2025-07-03 05:49:14 | user=charlie | ip=192.168.1.101 | action=connection attempt
2025-07-03 06:21:14 | user=alice | ip=203.0.113.77 | action=login success
2025-07-03 07:44:14 | user=bob | ip=192.168.1.101 | action=connection attempt
2025-07-03 04:23:14 | user=bob | ip=172.16.0.3 | action=login failed
2025-07-03 07:18:14 | user=bob | ip=203.0.113.77 | action=file accessed
2025-07-03 05:12:14 | user=alice | ip=198.51.100.42 | action=login success
2025-07-03 05:06:14 | user=bob | ip=203.0.113.77 | action=malware detected | threat=Worm Infection Attempt
2025-07-03 08:42:14 | user=charlie | ip=203.0.113.77 | action=file accessed
2025-07-03 09:10:14 | user=bob | ip=172.16.0.3 | action=malware detected | threat=Ransomware Behavior
2025-07-03 04:46:14 | user=david | ip=203.0.113.77 | action=login success
2025-07-03 08:42:14 | user=eve | ip=172.16.0.3 | action=file accessed
2025-07-03 07:22:14 | user=charlie | ip=192.168.1.101 | action=connection attempt
2025-07-03 04:53:14 | user=alice | ip=203.0.113.77 | action=file accessed
2025-07-03 07:45:14 | user=charlie | ip=172.16.0.3 | action=malware detected | threat=Trojan Detected
2025-07-03 05:44:14 | user=bob | ip=198.51.100.42 | action=file accessed


2025-07-03 054214 | user=eve | ip=
SOC_Task2_Sample_Logs.txt
File
Edit
View
H1
2025-07-03 05:42:14 | user=eve | ip=203.0.113.77 | action=malware detected | threat=Trojan Detected
2025-07-03 04:19:14 | user=alice | ip=198.51.100.42 | action=malware detected | threat=Rootkit Signature
2025-07-03 04:41:14 | user=alice | ip=172.16.0.3 | action=malware detected | threat=Spyware Alert
2025-07-03 05:06:14 | user=bob | ip=203.0.113.77 | action=malware detected | threat=Worm Infection Attempt
2025-07-03 09:10:14 | user=bob | ip=172.16.0.3 | action=malware detected | threat=Ransomware Behavior
2025-07-03 09:02:14 | user=david | ip=203.0.113.77 | action=login failed
2025-07-03 05:49:14 | user=charlie | ip=192.168.1.101 | action=connection attempt
2025-07-03 07:44:14 | user=bob | ip=192.168.1.101 | action=connection attempt
Ln 13, Col 1
749 characters
Plain text
100%
Windows (CRLF)
UTF-8

🛡 INCIDENT RESPONSE REPORT
SOC Analysis – Malware & Suspicious Activity

---

1 Executive Summary
This report presents the analysis of security logs collected on **03 July 2025**. Multiple high-risk malware infections and suspicious authentication activities were identified during log review. The incidents indicate potential system compromise and unauthorized access attempts, requiring immediate security response.

---

2 Scope of Analysis
- Log Source: System & Network Logs (TXT format)
- Date Analyzed: 03-07-2025
- Objective: Identify suspicious activities, classify alerts, and recommend mitigation steps

---

3 Identified Security Incidents

🔴 Incident 1: Trojan Malware Detection
- **User**: eve
- **IP Address**: 203.0.113.77
- **Threat**: Trojan Detected
- **Severity**: High

Description:
A Trojan malware was detected on the system associated with user *eve*. Trojans are capable of providing unauthorized access to attackers and may lead to data breaches.

🔴 Incident 2: Rootkit Infection
- **User**: alice
- **IP Address**: 198.51.100.42
- **Threat**: Rootkit Signature
- **Severity**: High

Description:
Rootkit detection indicates a deep system compromise. Such malware hides its presence and allows persistent unauthorized access.

🔴 Incident 3: Ransomware Behavior Detected
- **User**: bob
- **IP Address**: 172.16.0.3
- **Threat**: Ransomware Behavior
- **Severity**: Critical

Description:
Ransomware-like behavior was observed, which may lead to data encryption and loss. Immediate containment is required.

🟡 Incident 4: Failed Login Attempt
- **User**: david
- **IP Address**: 203.0.113.77
- **Action**: Login Failed
- **Severity**: Medium

Description:
A failed login attempt was detected from the same IP involved in malware activity, indicating possible credential misuse.

🟡 **Incident: Suspicious Connection Attempt**

- **Users:** charlie, bob
- **IP Address:** 192.168.1.101
- **Action:** Connection Attempt
- **Severity:** Medium

Description:
Multiple connection attempts were observed from the same IP address involving different user accounts. This behavior is suspicious and may indicate unauthorized access attempts or the use of shared or compromised credentials. Continuous monitoring is recommended.

---

4 Impact Assessment

- Possible data theft
- Risk of malware spread within the network
- Potential ransomware attack leading to system downtime

---

5 Incident Response Actions Recommended

1. Isolate infected systems immediately
2. Run full antivirus and malware scans
3. Reset compromised user credentials
4. Block malicious IP addresses
5. Monitor network traffic continuously

---

6 SIEM Tool Usage Explanation

• This task was performed using manual log analysis instead of an automated SIEM tool.
• The provided logs were in TXT format, which allowed direct inspection without SIEM ingestion.
• Manual analysis helped in understanding log structure, alert patterns, and incident identification clearly.
• Alerts such as malware detection, failed login attempts, and suspicious connections were successfully identified and classified.
• In real-time environments, a SIEM tool is recommended for automation, correlation, and faster response.

---

7 Conclusion

The log analysis confirms multiple high-risk malware incidents and suspicious access attempts. Immediate remediation and continuous monitoring are necessary to prevent further security breaches.
