Incident Response Report - SOC Task 2

Summary

During log analysis on 03 July 2025, the SOC team detected multiple high-severity security events. These include malware infections, login failures, and unusual access patterns. The incidents point to potential internal compromise and active threats within the network.

Key Incidents

- Malware Detected: Trojan, Rootkit, Ransomware on multiple IPs

- Repeated login failures for user 'alice'

- Suspicious activity from users: bob, alice, charlie, david, eve

- Affected IPs: 10.0.0.5, 198.51.100.42, 203.0.113.77, 172.16.0.3

Recommended Actions

1. Quarantine affected systems immediately

2. Force password reset for affected users

3. Run malware scans across suspected systems

4. Enable real-time login and access monitoring

5. Prepare for further forensic analysis

SIEM Dashboard Screenshot