SOC Incident Response Report

Date: 03 July 2025
Log Source: SOC_Task2_Sample_Logs.txt
Sourcetype: custom_logs
Host: si-i-01b109feba6dfc063.prd-p-uon6d.splunkcloud.com
Investigator: Anoop Dev
Email: anoopdev012@gmail.com
LinkedIn: https://www.linkedin.com/in/anoop-dev-592089245/

Executive Summary

This report provides a comprehensive analysis of security alerts detected by the Security Operations Center (SOC) on 03 July 2025. Multiple malware alerts were identified, affecting several users and endpoints. The report details the types of threats, affected users and IPs, and provides actionable recommendations for containment, remediation, and future prevention. The investigation aims to ensure organizational systems remain secure and compliant with cybersecurity best practices.

Key Findings

- 11 malware detected alerts: Trojan, Rootkit, Ransomware, Spyware, Worm
- Affected users: bob, eve, charlie, david, alice
- Multiple endpoints identified as infected
- Immediate isolation of affected endpoints recommended to prevent lateral movement of threats
- Alert patterns suggest potential targeted attacks and possible privilege escalation attempts

Malware Detections

Threat	User	IP Address
Ransomware	bob	172.16.0.3
Rootkit	alice	198.51.100.42
Rootkit	eve	10.0.0.5
Spyware	alice	172.16.0.3
Trojan	alice	192.168.1.101
Trojan	bob	10.0.0.5
Trojan	charlie	172.16.0.3
Trojan	david	172.16.0.3
Trojan	eve	192.168.1.101
Trojan	eve	203.0.113.77
Worm	bob	203.0.113.77

Response & Recommendations

- Immediately isolate affected machines based on user/IP to prevent further spread of malware.
- Perform thorough endpoint scans for malware signatures and remove any detected threats.
- Update firewall rules, antivirus signatures, and overall security policies.
- Notify SOC stakeholders and affected users with clear instructions on required actions.
- Conduct a root cause analysis to understand attack vectors and improve future detection.
- Review user access privileges and apply principle of least privilege where necessary.

Evidence

Please refer to the attached screenshots for Splunk search queries, detected events, and table statistics as documented from the investigation. The evidence supports the analysis and ensures transparency of the incident handling process.