**SOC Internship Task  
*Prepared by: Yehya Hamdy Sayed-Ahmed Mohammed*  
*Date: October 20, 2025*  
*Submitted to: Future Interns Task Two***

**Executive Summary**

**On July 3, 2025, between 07:45 AM and 09:10 AM, the Security Operations Center (SOC) identified five critical security incidents, including three malware detections (Ransomware, Rootkit, and Trojan) and a failed login attempt from an external IP address. These incidents pose a severe threat to system integrity, data confidentiality, and operational continuity. Immediate containment actions have been executed, and this report delivers a detailed analysis, remediation plan, and strategic recommendations.**

**Incident Details**

**Timeline of Events**

* **07:45:14 AM: Trojan malware detected on user *charlie* (IP: 172.16.0.3).**
* **07:51:14 AM: Rootkit signature detected on user *eve* (IP: 10.0.0.5).**
* **09:02:14 AM: Failed login attempt for user *david* (IP: 203.0.113.77).**
* **09:10:14 AM: Ransomware behavior detected on user *bob* (IP: 172.16.0.3).**
* **07:44:14 AM - 08:21:14 AM: Multiple connection attempts observed from various IP addresses.**

**Impact Assessment**

**The identified malware variants (Ransomware, Rootkit, Trojan) present significant risks, including data encryption, unauthorized remote access, and persistent system compromise. The failed login attempt suggests a potential brute force attack, while recurring connection attempts indicate reconnaissance activities by a malicious actor. These incidents could result in substantial data loss, financial repercussions, and operational downtime if not addressed effectively.**

**A screenshot of a computer

AI-generated content may be incorrect.**

**A screenshot of a computer program

AI-generated content may be incorrect.**

**A screenshot of a computer

AI-generated content may be incorrect.**

**Root Cause Analysis**

**The malware infections are likely the result of a successful exploit, potentially delivered through phishing emails or malicious attachments. The failed login attempt from an external IP (203.0.113.77) aligns with patterns of a brute force attack. Multiple connection attempts across different IPs suggest a reconnaissance phase, possibly preceding a larger-scale attack.**

**Remediation Steps**

**Immediate Actions**

* **Block malicious IPs: 172.16.0.3, 10.0.0.5, and 203.0.113.77.**
* **Isolate affected systems associated with users *bob*, *eve*, and *charlie*.**
* **Initiate comprehensive antivirus scans to eradicate malware.**

**Long-Term Measures**

* **Update antivirus software with the latest threat definitions.**
* **Enforce multi-factor authentication (2FA) across all user accounts.**
* **Enhance SIEM monitoring with custom rules to detect similar anomalies.**

**Recommendations**

* **Implement mandatory phishing awareness training for all employees.**
* **Strengthen SIEM detection rules to identify failed login attempts and unusual connection patterns.**
* **Review and tighten network access controls to restrict external IP activity.**
* **Conduct a thorough post-incident review to assess vulnerabilities and enhance security posture.**

**Alert Classification Log**

| **Alert ID** | **Timestamp** | **Type** | **Source IP** | **User/Target** | **Severity** |
| --- | --- | --- | --- | --- | --- |
| **1** | **2025-07-03 09:10:14** | **Malware** | **172.16.0.3** | **bob** | **High** |
| **2** | **2025-07-03 07:51:14** | **Malware** | **10.0.0.5** | **eve** | **High** |
| **3** | **2025-07-03 07:45:14** | **Malware** | **172.16.0.3** | **charlie** | **High** |
| **4** | **2025-07-03 09:02:14** | **Failed Login** | **203.0.113.77** | **david** | **Medium** |
| **5** | **2025-07-03 07:44:14** | **Connection Attempt** | **203.0.113.77** | **bob** | **Medium** |