PROFESSIONAL EMAIL COMMUNICATION DRAFT
REPORTING THE INCIDENT

Subject: URGENT: Security Incident Report (IR-2025-07-03-001) – High Severity Malware Detection

To: CISO; IT Management Team **Cc:** SOC Lead; Incident Response Team **From:** Zannu Opeyemi Emmanuel (SOC Analyst Intern) **Date:** July 3, 2025 **Importance:** High

Dear Management Team,

This email serves as an immediate notification regarding a **High-Severity Security Incident** detected by the SOC team this morning.

1. Incident Overview Between **04:19 AM and 09:10 AM**, our SIEM (Splunk) detected a coordinated malware outbreak affecting multiple workstations. The investigation has confirmed the presence of **Ransomware behavior** and **Rootkit signatures**, indicating a critical threat to data integrity and system security.

2. Key Findings

- **Critical Threat:** Active Ransomware behavior was detected on the workstation associated with user **Bob** (IP: 172.16.0.3) at 09:10 AM.
- **Persistence:** Rootkit signatures were identified on endpoints belonging to users **Alice** and **Eve**, suggesting deep system compromise.
- **Lateral Movement:** Evidence of Worm infection attempts indicates the malware is trying to propagate across the network.

3. Immediate Actions Taken (Containment) To prevent further data loss and network propagation, the SOC team has initiated the following containment measures:

- **Isolation:** The affected IP addresses (172.16.0.3, 10.0.0.5, 203.0.113.77, 198.51.100.42) have been logically disconnected from the corporate network.
- **Blocking:** Firewall rules have been updated to block traffic to/from the external command-and-control IPs identified.
- **Account Lockout:** Active sessions for users Bob, Alice, Eve, and Charlie have been terminated, and accounts are temporarily locked.

4. Recommendations & Next Steps We request approval to proceed with the following remediation steps:

- Full forensic imaging of the affected machines for analysis.
- Re-imaging of systems infected with Rootkits.
- Restoration of data from backups for the ransomware-affected endpoint (User: Bob).

A detailed **Incident Response Report** is attached to this email providing a full timeline and technical analysis.

We will provide an update within the next hour regarding the containment status.

Best regards,

Zannu Opeyemi Emmanuel SOC Analyst Intern | Future Interns

Attachment(s):

- SOC_Task2_Incident_Response_Report.pdf
- SOC_Task2_Alert_Logs.xlsx