EMAIL COMMUNICATION DRAFT

Subject: Security Incident Notification – Immediate Review Required

To: Security Manager / IT Leadership
From: SOC Analyst
Date: 11/12/2025

Dear Team,

This email is to notify you that multiple high-severity alerts were detected during routine SOC monitoring. These include confirmed malware detections (Trojan, Rootkit, Worm, and Ransomware behaviors), repeated connection attempts, failed login attempts from suspicious IPs, and unusual file-access patterns.

A preliminary incident analysis has been completed, and the affected hosts have been flagged for immediate isolation and review. A full incident response report, including screenshots and recommended remediation steps, has been prepared and is attached for your assessment.

Immediate attention is recommended to prevent further spread or compromise.

Please let me know if further investigation or escalation is required.

Regards,
Amit V
SOC Analyst – Future Interns Program