Subject: Security Alert Summary – Multiple Threats Detected on Internal Host

Dear Security Manager,

As part of my Security Operations Center (SOC) internship tasks, I monitored recent system activity using Splunk and identified multiple suspicious events that require immediate attention.

Summary of Findings:

Between 07:45 AM and 09:10 AM on July 3, 2025, several key alerts were detected, including:

- Ransomware behavior on internal host DESKTOP-QC8GMS3 (IP: 172.16.0.3)
- Rootkit and Trojan malware signatures on hosts 172.16.0.3 and 10.0.0.5
- Suspicious internal connection attempts originating from the compromised hosts

Simulated Actions Taken:

- Virtual isolation of host 172.16.0.3 and 10.0.0.5
- Initiation of antivirus scans and malware removal procedures
- Recommendation for full system reimaging and further endpoint investigation
- Incident logged and escalated for review

Recommended Next Steps:

- Deployment of Endpoint Detection and Response (EDR) tools for active threat mitigation
- Enforcement of stricter login policies such as Multi-Factor Authentication (MFA)
- Conduct a comprehensive internal threat sweep
- Enhance employee awareness regarding phishing and malware threats

Please find attached the full Incident Response Report for your review. Should you require any clarifications or further information, feel free to contact me.

Best regards,

Tshiamo Mantswe

tshiamomantswe2@gmail.com

SOC Intern