SOC Operations Report

Analyst: Samuel Jemal
Date: 30 October 2025
Role: SOC Analyst (Intern)

1. Executive Summary

This report summarizes daily SOC operations conducted on 30 October 2025. Activities included monitoring alerts, validating threat intelligence feeds, analyzing endpoint logs, and maintaining incident response documentation. The focus was on improving correlation rule accuracy and developing playbooks for phishing and malware triage.

2. Tools Used

- Splunk / ELK Stack – Log monitoring
- Wireshark – Network traffic inspection
- Sysmon – Endpoint event tracking
- MITRE ATT&CK; – Threat mapping

3. Findings

Observation	Impact	Resolution
High false positives from IDS	Reduced analyst efficiency	Optimized detection rules
Missing endpoint logs	Limited visibility	Enabled centralized Sysmon logging
Delayed phishing alert response	Increased dwell time	Automated email sandboxing

4. Recommendations

- Implement continuous monitoring dashboards for real-time visibility.
- Improve rule tuning for false positive reduction.
- Regularly train analysts on new detection methods.
- Adopt automation (SOAR) for faster alert triage.

5. Analyst Signature

Name: Samuel Jemal
Date: 30 October 2025
Role: SOC Analyst (Intern)