Leul Tadele

SOC Analyst

Addis Ababa, Ethiopia | +251707955027 | leultadele123@gmail.com

Professional Summary

SOC Analyst with hands-on experience in monitoring, detecting, and responding to cyber threats in real time. Proficient in operating within high-pressure SOC environments and leveraging tools such as Splunk, Wazuh, Microsoft Defender for Endpoint, and CrowdStrike Falcon for threat detection and incident response. Experienced in developing playbooks and using Cortex XSOAR to automate and orchestrate security workflows. Strong knowledge of network security, vulnerability assessment, and penetration testing, with proven ability to triage alerts, analyze security events, and support timely mitigation to reduce risk.

SKILLS

- SIEM – Splunk Enterprise Security (ES), Use-case development, dashboarding, SPL optimization
- SOAR – Cortex XSOAR (playbook development, automation, tuning)
- Endpoint Security – Microsoft Defender, CrowdStrike
- IDS/IPS – Suricata, Snort
- Log Analysis & Forensics – Splunk SPL, Wireshark
- Scripting – Python, Bash
- Threat Hunting – Splunk, MITRE ATT&CK–aligned techniques
- Asset Onboarding & Log Integration – Automation of asset tracking and log-status management
- Vulnerability & Penetration Testing – Nessus, Burp Suite, Metasploit
- Operating Systems – Windows, Linux

Work History

SOC Analyst at Safaricom Telecommunications Ethiopia PLC *January 2025 - Current*

Addis Ababa, Ethiopia

- Monitor and analyze security alerts in a 24/7 environment using SIEM platforms such as Splunk ES.
- Detect, investigate, and respond to security incidents, performing initial triage, impact analysis, and escalation when required.
- Conduct comprehensive log analysis from firewalls, IDS/IPS, EDR, servers, telecom network nodes, DLP, and Anti-DDoS systems to identify suspicious activity.
- Execute endpoint investigations and response actions using EDR tools including Microsoft Defender for Endpoint and CrowdStrike Falcon.
- Tune and optimize Splunk correlation searches and detection rules to improve accuracy and reduce false positives.
- Develop, automate, and maintain SOAR playbooks in Cortex XSOAR to streamline incident response and enhance SOC efficiency.
- Create and customize Splunk dashboards and visualizations for threat monitoring, alert summaries, and operational reporting.
- Document security incidents, investigation findings, and response actions in detailed reports, and provide daily shift updates to security management teams.

Intrusion Analyst at Information Network Security Administration (INSA) *Sep 2022 – Dec 2024*

Addis Ababa, Ethiopia

- Monitored and analyzed security events using SIEM platforms to ensure timely detection and proactive response to emerging threats.
- Investigated security incidents in collaboration with the incident response team, ensuring effective containment, mitigation, and root-cause analysis.
- Performed comprehensive log analysis on different critical systems to identify anomalies and indicators of compromise (IOCs).
- Integrated diverse log sources into the SIEM environment and fine-tuned detection rules and correlation searches to improve accuracy and reduce false positives.
- Conducted penetration testing and vulnerability assessments, contributing to a measurable reduction in overall system and network security risks.
- Configured and maintained IDS/IPS and SIEM systems to improve threat detection and prevention capabilities against evolving attack vectors.

EDUCATION

Bachelor of Science: Electrical Engineering and Computing, 06/2022

Adama Science and Technology University (ASTU) - Adama, Ethiopia

GPA: 3.70 / 4.00

CERTIFICATIONS

- Palo Alto Networks Certified Security Automation Engineer (PCSAE)
- CompTIA Cyber security analyst (CySA+)
- Ethical Hacker Essentials (EHE)
- Fortinet Certified Association in Cybersecurity