Leul Tadele Tegegn

♦ Addis Ababa, Ethiopia ♦ +251 934 235 095 ♦ leultadele123@gmail.com

Professional Summary

Cybersecurity Analyst with hands-on experience in monitoring, detecting, and responding to cyber threats in real-time. Adept at working in high-pressure SOC environments, leveraging tools like Splunk, Wazuh, Microsoft Defender for Endpoint, and CrowdStrike Falcon for threat detection and incident response. Strong understanding of network security, vulnerability assessment and penetration testing, with a proven ability to triage alerts, analyze indicators of compromise (IOCs), and support timely mitigation efforts.

Skills

- Threat Detection - Splunk, Wazuh
- IDS/IPS - Suricate, Snort
- Log Analysis & Forensics - Wireshark
- Vulnerability & Penetration Testing - Nessus, Burp Suite, Metasploit
- Endpoint Security - Microsoft Defender, CrowdStrike
- SOAR platform - Cortex XSOAR
- Scripting - Bash, Python
- Knowledge of MITRE ATT&CK framework

Work History

SOC Analyst, 01/2025 - Current
Safaricom Telecommunications Ethiopia PLC – Addis Ababa, Ethiopia

- Monitoring and analyzing security events (24/7) using SIEM tools such as Splunk.
- Investigate security incidents to identify root causes and mitigate associated risks.
- Conduct log analysis from multiple sources, including firewalls, servers, and telecom nodes.
- Perform incident response using Endpoint Detection and Response (EDR) tools such as Microsoft Defender and CrowdStrike.
- Tune detection rules and correlation searches in monitoring tools (Splunk), optimizing alert quality and significantly reducing false positives.

Intrusion Analyst, 09/2022 - 11/2024
Information Network Security Administration (INSA) – Addis Ababa, Ethiopia

- Monitored and analyzed security events using SIEM tools to ensure timely detection and response to potential threats.
- Investigated security incidents in coordination with the incident response team to effectively contain and mitigate risks.
- Performed log analysis from diverse sources including firewalls, intrusion detection systems (IDS), and servers-to identify anomalies and indicators of compromise (IOCs).
- Conducted penetration testing and vulnerability assessments, resulting in a measurable reduction of system vulnerabilities.
- 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, Electronics and Communication Engineering, 06/2022
Adama Science and Technology University (ASTU) - Adama, Ethiopia
GPA: 3.70 / 4.00

Certifications

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