Warkena Abay

CSOC Analyst

warkenahabay19@gmail.com | +251917797974 | Addis Ababa, Ethiopia

Summary

I'm a dedicated cyber security professional with more than 3 years of experience at Safaricom Telecommunications Ethiopia in the cyber security operation center analyst (CSOC). I'm good at communication, demonstrated through my ability to effectively collaborate with teams and respectful relationships with colleagues. This has resulted in the delivery of the project on time both as an individual and as team members, supporting the company to reach its mission.

Education

Bachelor of Science in Electrical and Computer Engineering, Jimma University Institute of Technology (2018 - 2022).

Work Experience

CSOC Analyst at Safaricom Telecommunications Ethiopia PLC January 2023 - present

Monitoring Security Alerts:

- Continuously monitor security alerts and notifications from various security tools and systems.
- Analyze alerts to identify potential security incidents.

Incident Detection and Response:

- Identify, investigate, and respond to security incidents.
- Perform initial triage to determine the severity and impact of incidents.
- Escalate significant incidents to higher-level analysts or incident response teams.

Log Analysis:

- Collect and analyze logs from various sources like firewalls, IDS, IPS, EDR, DLP and Anti DDOS.
- Correlate log data to identify suspicious activities and potential threats.

Documentation and Reporting:

- Prepare documentation of incidents, findings, and actions taken in detailed reports.
- Provide regular daily shift reports and updates to the management and cyber security team.

Splunk Engineering & Administration Responsibilities

Deployment & Configuration

- Install, configure, and maintain **Splunk Enterprise**, including Indexer Clusters, Search Head Clusters, Deployment Server, Heavy Forwarders, and Universal Forwarders.
- Perform upgrades, patching, and configuration management across distributed Splunk environments.

Data Onboarding & Field Extraction

- Create and manage data inputs such as **syslog, API integrations, HF and UF.**
- Implement parsing, timestamp correction, line-breaking, and data normalization.

Monitoring, Performance & Maintenance

- Perform daily Splunk health checks: indexing status, cluster replication, disk usage, CPU/memory consumption, and license usage.
- Optimize search performance through search tuning, summary indexing, acceleration, and knowledge object governance.

Indexing, Storage & Retention

- Manage index lifecycle policies, data retention schedules, SmartStore configurations, and volume definitions.
- Monitor hot/warm/cold bucket transitions and maintain efficient storage utilization.
- Implement **RBAC (roles and capabilities)** and enforce least-privilege access.

Backup, Recovery & High Availability

- Develop and test backup and restore procedures for **indexes, KVStore, and configuration bundles**.

Integrations & Ecosystem Support

- Integrate Splunk with third-party tools including **Cribl Stream, syslog-ng, syslog, EDR** and other telemetry sources.
- Troubleshoot ingestion failures, replication issues, parsing errors, and search performance bottlenecks.

Technical Skills

- Integrating and onboarding of assets with Splunk SIEM and made strong relationships with stakeholders and node owners.
- Develop, optimize, fine-tune and customize use-case
- Prepare dashboards and widget on Splunk based on requirements
- SOAR playbook development and tuning
- Expert with Windows, Linux and Unix operating systems.
- Knowledge of MITRE ATT&CK
- Threat hunting using Splunk SPL etc.
- Basic scripting python, and VBA
- Automate the process of managing asset lists to separate for onboarded, not-onboarded and not send logs using Splunk SPL.
- Skilled in data analysis on Excel specifical by using VBA scripts.

Internship Experience

Jimma University ICT Development Directorate Office

December 2021 - March 2022

- Provided solutions to enhance cybersecurity and deployed these solutions for the organization.
- Assisted in improving the overall security posture of the ICT infrastructure.
- Implemented best practices for health monitoring of servers for us.

Certification and Awards

- Palo Alto Network Certified Security Automation Engineer (PCSAE)
- Splunk Enterprise Security Certified Admin (I have voucher and will take exam after a month)
- Safaricom Star Award
  Issued by: Safaricom Human Resource Officer
  April 2024
- Big Data Analyst

Issued by: Vodacom and Safaricom Telecommunication Ethiopia

January 3, 2025

- Cisco Certified Network Associate (CCNAv7)

  Issued by: Jimma University

  February 2022

- Building Electrical Installation & Computer Maintenance

  Issued by: Jimma University

  May 2022

- Sightline/TMS DDOS User/Admin/System Admin

  Issued by: NETSCOUT

  July 2023

- Design of Server Resource Metrics Management System

  Issued by: Jimma University

  February 2022