Mariam Kimbisa

Georgetown, TX
-Email me on Indeed: http://www.indeed.com/r/Mariam-Kimbisa/9eb791e0d85b965f

A trained professional with hands on experience in the cyber dynamic. The ability to review the current environment, assess potential risks and convey valuable solutions and recommendations. Adept in cyber security processes, procedures and mitigation. Expert experience in vulnerability management, log review, security assessment, software security and management etc. Hands on with various cyber tools that support the detection process such as Cisco Esa, Tufin, Burpsuite, Acunetix, Solarwinds, ESET EDR,
Palo Alto and more

Work Experience

AG Cybersecurity Manager
CRDB BANK PLC - DAR-ES-SALAAM, TANZANIA
July 2022 to Present

Operational:
o Taking lead on assessing all critical projects within the bank and analyzing the security gaps, as well as making sure all gaps are closed in order to fit the bank's environment.
o Oversee and reporting of remediation activities such as vulnerability management, patching, network security etc.
o Asset explorer system owner, responsible for inventorying of all IT assets within the banks infrastructure, classifying, segmenting and the overall monitoring of EOL and EOS of assets, e.g. routers, switches, servers etc.
o Championing roll-out of security control tasks in the infrastructure such as MFA, migration of production servers to DR, implementing antivirus solutions in the ATM's, system hardening
o Closure of reported vulnerabilities, developing schemes that would minimize the number of vulnerabilities in the infrastructure
o Responsible for ascertaining all vulnerabilities are within SLA. Closure of vulnerabilities from web, servers and pentest
o Championing the closure of audit queries, e.g. critical, high and medium systems to have a recovery plan and have DR, EOL and EOS monitoring and implementing remediation etc.
o Develop API policy and enhance the security assessment baseline
o Review of the security policies in place and applying my recommendations for updates
o Developing initiatives and work plans that would support cyber forensics and cyber threat analytics activities, such as dark web, sandboxing etc.
o Working with the developer's team on ways to successfully incorporate security measures in the SDLC. This includes the API's and APK's and how to ensure a more secured file sharing/transfer process on route to public deployment.
o Fine-tuning and enhancing the Asset Management tool to improve visibility of the banks infrastructure

Cybersecurity Specialist
CRDB BANK PLC - DAR-ES-SALAAM, TANZANIA
January 2021 to June 2022

Operational:
o Responsible for the daily monitoring of security systems in the SOC
o Share daily reporting and tracking of security threats/incidents
o Lead projects and ascertain key deliverables are attained within the stated time frame and with the allocated budget
o Responsible for the planning, monitoring and execution of security projects
o Responsible for developing project milestones, achievements to achiever project objectives and goals
o Ability to work collaboratively yet independently to achieve set targets
Technical
o Deployed new security systems to advance the bank's security posture
o Performed vulnerability assessments for all web and mobile applications within the bank.
o Conducted threat detection, mitigation and remediation of security events
o Conducted daily assessment of end points detection, logs review, applications security, email security server management, network security through Solarwinds SIEM, Acunetix, EDR, Tenable,
Palo Alto, Checkmarx etc.
o Assess the banks application and cloud security and incorporate effective controls to mitigate risks
o Execute security assessment on application source code, API and integration process review to ascertain they meet the bank's security standard.
o Review of set firewall rules and advancing security controls
o Implementing of HTTPS on all sites within the bank
o Daily review of VPN logs and taking initiative to resolve threats detected
o Review of unauthorized software in the bank's network and perform software blocking
o Executed security assessment on new incoming projects within the bank such as core banking systems, switches etc.
Strategic
o Champion the security awareness initiative within the bank
o Developed the SOC and NOC strategy for the bank and conveyed the overall mission and vision
o Established the cloud security and application security processes
o Shared recommendations within different departments in the bank, on how to incorporate new business functions in the daily monitoring in security systems such as SIEM and log feeds
o Advanced the security operation center through championing new facilities, tools, trainings and developing the charter
o Managed effective implementation of ICT security projects.
o Represent the security team in both internal and external meetings
Eliminated the ICT security department from the unresolved audit query of unauthorized software. Reduced the number from 1700 to 0 unauthorized software in the network.
Championed and implemented the SOC activation initiative, whereby this involved the implementation of tools, facilities system solutions, play books etc. Executed HTTPS on all web application within the bank and eliminated the unsecured and unencrypted connection vulnerability.

Financial Inclusion Digital Specialist
FUNDACION CAPITAL - DAR-ES-SALAAM, TANZANIA
January 2019 to December 2020

o Provided technical assistance within and outside the organization
o Coordinated and manage projects with various partners such as UNCDF, Mercy Corps, TASAF, Bill and Melinda Gates, DFID etc.
o Developed digital solutions, tablet based learning applications that are human centered and interactive.

o Ensured effective coordination of the project within teams and/or partners; timely delivery, project status, field visit, timely reporting, efficient data collection and budget tracking
o Conducted qualitative and quantitative data collection, including liaising with external stakeholders as necessary.
o Conducted research and built insights on preferences and preparedness of the low-income population in engaging with digital services;
o Coordinated the creation of financial digital solutions that suits the low-income population;
o Manage the development of JIJENGE application- a digital solution with an objective of building financial capabilities for the low-income population and JIFUNZE BIASHARA application- a livelihood tablet-based learning app that aims at training beneficiaries to acquire basic life skills, entrepreneurship and business development skills
o Assisted in the development of project proposal
o Project report writing to highlight projects deliverables, scope, findings, analysis etc.
Success Examples:
Developed the creation of financial literacy digital solutions that were used by refugees, farmers and people living in rural geographical locations. Due to the success, users requested more topics that initially advanced their business skills, financial management etc.

Cybersecurity Analyst
Century, FL
August 2017 to December 2018

o Performed daily threat assessments
o Developed web application vulnerability trends
o Communicate and follow up with system administrators to resolve vulnerabilities within the SLA
o Developed daily reports of incidents and security posture
o Executed incidents analysis, investigation and closing of incidents
o Take lead of security projects, from the initiation phase to the implementation
o Coordinated the daily monitoring activities of SOC
o Manage the administration of systems; system deployment, hardening, configuration
o Analyze security events and suggest preventative methods
o Assisted with the daily monitoring and reporting of incidents
o Contribute to the process improvement and efficiency

Education

CERTIFICATE in CYBERECURITY
HARVARD UNIVERSITY
August 2021

CERTIFICATE in THREAT DETECTION
WEBSTER UNIVERSITY
December 2018

MASTER OF SCIENCE in CYBERECURITY
WEBSTER UNIVERSITY
December 2018

BACHELOR OF BUSINESS ADMINISTRATION in Desktop Decision Support and Technology
UNIVERSITY OF CENTRAL ARKANSAS
December 2018

Skills

• Threat Detection
• Web and Mobile Application Security
• Compliance
• Security Infrastructure and Architecture
• Security Assessment
• Incidence Response Management
• Vulnerability Assessment/Management
• Endpoint Security
• Security Logging
• Cloud Security
• Network Traffic Review
• DLP
• Project Management