



1. JOB TITLE: Systems Security Specialist - Applications (1 Position(s))

Job Location :

Head Office, Hq

Job Purpose:

To plan, organize, and deliver cost-effective and efficient IT security controls within developed and acquired systems within the bank.

Main Responsibilities:

- Support the secure application development strategy and roadmap of the bank by ensuring applications are securely designed and developed.
- Support implementation of application security governance by defining, developing, implementing, and maintaining required policies, procedures, standards, and guidelines
- Establish and develop security requirements and designs for all developed and acquired systems.
- Provide security assurance of all applications implemented by validating the implementation of security designs, conducting manual applications code reviews and security assessments to eliminate security vulnerabilities.
- Assist the development team and system vendors in reproducing, triaging, and addressing application security vulnerabilities.
- Conduct periodic security assessments and review of implemented systems to ensure their continued compliance with security standards.
- Establish, maintain, and implement optimal security configurations of all databases, middleware, and applications.
- Conduct research and make recommendations on systems security solutions, services, protocols, standards, and best practices in support of systems security continuous improvements.
- Prepare and maintain systems security documentation including security architecture and designs of systems and applications.
- Implement security improvements by continuously assessing the implemented controls, evaluating security risks, and anticipating requirements.

Knowledge and Skills:

- Knowledge of modern software development trends as well as understanding of software security practices.
- Knowledge of systems security standards and baselines in operating systems, databases, middleware, and applications; Hands-on experience in implementing applications in wide range of Operating Systems is mandatory.
- Knowledge in the best practices of secure mobile application development.
- Experience identifying security issues through manual code review in Java, PHP, JavaScript, Typescript, and other programming languages.

- Hands-on experience in common security libraries and tools (e.g., static and dynamic application security testing tools, proxying / penetration testing tools)
- A basic understanding of network and web related protocols (such as TCP/IP, UDP, HTTP, HTTPS).
- Familiarity with security standards such as OWASP Testing Guide, OWASP ASVS and NIST Security Standards.
- Good interpersonal, written, and oral communication skills in English and Swahili.
- Demonstrable honesty, integrity, and credibility; ability to engender the trust and confidence of internal constituency and external partners.
- Ability to communicate complex security concepts in an easy-to-understand business language.

Qualifications and Experience:

- At least a bachelor's degree in Computer Science or related academic field.
- Professional certifications such as CEH, CISA, CISSP, OSCP, GPEN will be an added advantage.
- At least 2 years of relevant work experience.
- Experience in scripting and automation using PowerShell and Bash/Shell Scripting.
- Solid hands-on experience in Computer Programming in either Java, PHP or Python is mandatory.

NMB Bank Plc is committed to creating a diverse environment and is proud to be an equal opportunity employer

Job opening date : 14-Mar-2023

Job closing date : 28-Mar-2023

2. JOB TITLE: Systems Security Specialist - Penetration Tester (3 Position(s))

Job Location :

Head Office, Hq

Job Purpose:

To plan and implement security tests on NMB systems.

Main Responsibilities:

- Perform manual penetration testing of web applications, mobile applications, APIs, external and internal networks.
- Work closely with cross-functional delivery teams, present security test findings, agree upon remediation response plans, and follow-up implementation of the plans.
- Carry out proof of concept on known risks and discovered vulnerabilities against the bank's environment.
- Recognize and safely utilize penetration testing tools, tactics and procedures.
- Research and develop customized tools and automation scripts to improve the identification of vulnerabilities.
- Develop comprehensive and accurate reports and presentations for both technical staff and management.
- Provide security recommendations in the development and acquisition of the bank's systems.
- Support third-party security test engagements including regulatory tests conducted at the bank.
- Work with system vendors as well as internal teams in verifying the security of the applications/systems implemented within the bank.

Knowledge and Skills:

- Knowledge of the security testing landscape.
- Knowledge of security of various operating system flavors such as Windows, Linux, and Unix.
- Understanding of network security architecture.
- Scripting skills in at least one scripting language including Python, PowerShell or Bash.
- Pen-testing skills in applications and infrastructure domains.
- Good interpersonal, written, and oral communication skills in English and Swahili.
- Demonstrable honesty, integrity, and credibility; ability to engender the trust and confidence of internal constituency and external partners.

Qualifications and Experience:

- Degree in Cyber Security, Computer Science, Information Systems or related.
- The following certifications are a plus OSCP, eJPT, CEH.
- Experience in software/web development and/or source code review in Python, C/C, C#, Java, VB .NET, ASP.NET, PHP, NodeJS.
- Hands-on experience in Linux and Windows environment.
- Actively participate in Capture The Flag (CTF) events, HackTheBox, TryHackMe or similar.

NMB Bank Plc is committed to creating a diverse environment and is proud to be an equal opportunity employer

Job opening date : 14-Mar-2023

Job closing date : 28-Mar-2023

APPLY THROUGH THE LINK BELOW:

https://careers.nmbbank.co.tz/nmb_career/career.aspx