Technology Division

Data Center & Infrastructure Department

Position: Security Engineer (Assistant Manager)

Key Responsibilities:

Security Engineering and Architecture

- **Design, deploy, and manage critical security infrastructure components (e.g., Firewalls, IDS/IPS, WAF, SIEM, EDR/XDR, IAM/PAM, DLP)**
- **Serve as the Subject Matter Expert (SME) for one or more key security domains (e.g., Network Security, Endpoint Security, Application Security, Cloud Security, Identity & Access Management).**
- **Lead technical security reviews of new projects and infrastructure changes, ensuring adherence to security standards and policies from the design phase.**

Threat & Vulnerability Management

- **Execute and optimize the bank's Vulnerability Management program, including advanced scanning, false-positive tuning, and prioritization of remediation efforts.**
- **Conduct routine security assessments and penetration testing (or manage external tests) and lead the technical remediation of identified vulnerabilities.**
- **Develop and maintain advanced correlation rules and use cases within the SIEM (Security Information and Event Management) platform to enhance threat detection capabilities.**

Incident Response and Automation

- **Act the subject matter expert during security incidents, performing deep-dive analysis, malware analysis, and advanced containment actions.**
- **Develop and maintain security automation scripts and workflows (e.g., using SOAR tools or custom scripting) to streamline security operations and incident response activities.**
- **Provide technical mentorship and guidance to security analysts.**

Compliance and Documentation

- **Ensure all security configurations and operations meet the compliance requirements of local regulators and industry standards (e.g., Central Bank of Myanmar guidelines, PCI-DSS, ISO 27001).**
- **Create and maintain detailed technical documentation, architectural diagrams, and standard operating procedures (SOPs) for security controls.**

Job Requirement:

Must-Have

- **Bachelor's degree in computer science, Information Technology, Diploma in Engineering or IT related field.**
- **5+ years of hands-on experience as a Security Engineer in an enterprise environment, with 3+ years working specifically in the Banking/Financial Services sector or a similarly regulated industry.**
- **Proven expertise with at least three core security technologies (e.g., Next-Gen Firewall, EDR/XDR, SIEM, WAF, IAM/PAM and DLP).**
- **Deep understanding of common attacker Tactics, Techniques, and Procedures (TTPs) using frameworks like MITRE ATT&CK, focusing on attacks relevant to the financial sector.**
- **Expertise in scripting/automation (e.g., Python, PowerShell) for API integration and task automation.**
- **Expert proficiency in SIEM/Logging platforms (e.g., Elastic, Sentinel, Wazuh) for threat hunting and developing automated SOAR workflows.**
- **Strong understanding of network protection technologies and best practices.**
- **Strong analytical and problem-solving skills for complex security issues.**
- **Strong understanding of operating systems security architecture (Windows, Linux) and knowledge of application security vulnerabilities, exploits, and mitigation techniques.**
- **Deep practical expertise in TCP/IP, network segmentation, cryptography, and securing modern architectures (e.g., Zero Trust, microservices).**
- **Excellent communication skills to articulate technical risks to both technical teams and management.**
- **Ability to work independently and lead technical projects to completion.**
- **Broad knowledge of computer networking, log analysis, information security principles, policies and adversarial tools and techniques.**
- **CISSP, CISM, GCIA, ITIL certification or strong relevant certification domains knowledge and proven experiences.**

Good to Have

- **Ability to understand and act on risk-based assessments and regulatory compliance evaluations.**
- **Experience in managing a Security Operations Center (SOC) or equivalent tiered response function.**
- **Knowledge of Threat Modeling techniques (e.g., STRIDE).**
- **Familiarity with operating systems (Linux, Embedded Linux, Windows, etc.).**
- **Familiarity with web related technologies (Web applications, Web Services, Service Oriented Architectures).**
- **Experience in fuzzing frameworks, reverse engineering and exploit development.**
- **Assist in the investigation and analysis of possible security incidents.**
- **Proficient in implementing and managing cloud security such as AWS, Azure and Huawei.**
- **Ability to explain complex technical concepts to a non-technical audience.**

- **Experience creating technical standards documentation.**
- **Good understanding of cyber security controls, framework and international standard such CIS Controls Version 8.1, NIST CSF 2.0, NIST SP 800-53, ISO 27002.**
- **Strong understanding of incident response and cyber security risk standard such NIST SP 800-61 Rev.3 and CISA Cyber Incident & Vulnerabilities Response Playbook.**
- **Good understanding of local regulatory and international standard such Central Bank Of Myanmar guidelines, ISO 27001, ISO 9001, PCI DSS.**