Job Description:

The Associate Security Engineer will join our Information Security team to help safeguard our organization's systems. This individual will be responsible for providing on-going support of information security solutions and improving our security posture by aiding in the development of security plans and policies, testing for vulnerabilities, and monitoring and investing security breaches. The ideal candidate has a passion and desire for security, solving challenging problems, while staying up to date with the latest security trends and best practices. Conduct penetration testing and vulnerability assessment projects

• Identify security risks and operational needs.

• Assist in the investigation and analysis of possible security incidents.

• Support of threat detection and response program.

• Aid in creating phishing campaigns for continued security awareness for internal employees to recognize, avoid, and report potential threats that can compromise critical data and systems.

• Partner with Senior Engineers to analyze audits, security, and monitoring logs for potential threats (internal/external) and intrusions.

• Monitor environments for security breaches and attempted attacks.

• Provide ongoing cyber security focused KRI/KPI metrics.

• Research, recommend, and implement new technologies or processes for enhancement of security posture.

• Perform other duties as assigned.

Job Requirement: Must-Have

• Diploma in Engineering or bachelor's degree in engineering / IT related field.

• 1~2 years of Information Security related experience.

• Understanding of network protection technologies and best practices.

• Broad knowledge of computer networking, log analysis, information security principles, policies and adversarial tools and techniques.

• Strong understanding of operating systems architecture and security features.

• Good knowledge of software vulnerabilities, exploits, and mitigation

• Strong understanding of attack vectors and remediations.

• Strong understanding of attack methods, protection, detection, and response.

• Strong understanding of networking protocol, application protocols, and cryptography.

• Proficient in both Linux/Unix and Windows environment.

Good to Have

• Understanding of Security concepts.

• Ability to understand and act on risk-based assessments and regulatory compliance evaluations.

• Familiarity with operating systems (Linux, Embedded Linux, Windows, etc.).

• Hands on experience with scripting languages such as PowerShell and or Python.

• 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 services such as AWS, Azure, M365, G Suites.

• Good understanding of cyber security controls and framework such CIS Controls, NIST CSF.

• Ability to explain complex technical concepts to a non-technical audience.

• Have or willing to take information security certifications such as CompTIA Security+, GIAC, ISACA, ISC2, and Offensive Security