BELOW IS A SAMPLE JOB DESCRIPTION FOR AN ENTRY-LEVEL CYBERSECURITY ROLE:

We are seeking a driven and skilled cybersecurity analyst to join our team. The ideal candidate will possess strong technical expertise in cybersecurity principles, along with a passion for integrating security throughout the software development lifecycle. In this role, you will actively contribute to the protection of our systems, networks, and sensitive data by proactively identifying vulnerabilities, implementing robust security measures, and responding effectively to security incidents.

RESPONSIBILITIES

-Fix detected vulnerabilities to maintain high-security standards
-Research security enhancements and make recommendations to management
-Contribute to all levels of the architecture of proposed and existing software
-Maintain technical documentation of application security, assessments and remediation
-Help colleagues install security software and understand information security management
-Collaborate with cross-functional teams to address security issues and implement best practices
-Work with the security team to monitor and analyze network traffic for potential threats and suspicious activities
-Implement, test and operate security software, tools and techniques in compliance with technical reference architecture
-Provide secure engineering designs for new software solutions to help mitigate security vulnerabilities
-Perform ongoing security testing and code review to uncover vulnerabilities
-Stay up-to-date on information technology trends and security standards
-Investigate security breaches and other cybersecurity incidents
-Consult team members and peers on secure coding practices
-Develop company-wide best practices for IT security
-Document security breaches and assess the impact
-Perform penetration testing on applications

SKILLS AND REQUIREMENTS

-Degree in Computer Science or related field
-Excellent written and verbal communication skills in English
-Basic understanding of cybersecurity principles and practices
-Familiarity with network protocols, firewalls, and security technologies
-Interest in all aspects of security research and development + research emerging cybersecurity trends, threats, and technologies
-Have knowledge of industry standard classification schemes, such as ISO 27000, NIST GDPR, TH PDPA, PCI DSS, Data Loss Prevention etc.
-Detailed technical knowledge of techniques, standards and state-of-the art capabilities for authentication and authorization, applied cryptography, security vulnerabilities and remediation
-Adequate knowledge of web related technologies (web applications, web services and service-oriented architectures) and of network/web related protocols
-Familiarity with one of the following core languages: PHP, Python, Java, Javascript and .NET (C# etc)
-Demonstrable experience working on a software-related project from ideation to implementation
-Review and analyze security policies and procedures to identify areas for improvement
-Experience with cybersecurity tools, such as Wireshark or Metasploit, is a plus
-Stay current on IT security trends and news