Cyber Security Engineer Job Description

Duties and Responsibilities:

- Partake in technical design reviews, integration, testing, and documentation work
- Responsible for technical advisory to research teams
- Update, sustain, and administer a high level of security for in-house security infrastructures
- Run vulnerability valuation and fizzing of protocols, hardware, and software
- Apply system security engineering principles to deliver real solutions premeditated to enhance the security position
- Identify threats and develop suitable defense measures, evaluate system changes for security implications, and recommend enhancements, research, and draft cyber security white papers, and provide first-class support to the cyber security operations staff for resolving difficult cyber security issues
- Write Risk Management Framework (RMF)-based policies and procedures, and develop comprehensive cyber security processes to contain implementation
- Manage and lead security incident response efforts
- Configure Windows and Linux host-based security as well as network and cloud-based security systems
- Support with the installation and configuration of network security architectures, including firewalls, router ACLs (Access Control Lists), web content filters and Demilitarized Zones (DMZ)
- Observe and respond to Intrusion Detection System (IDS) cues and anti-virus alerts.

Cyber Security Engineer Requirements – Skills, Knowledge, and Abilities

- 3 years plus of experience identifying threats and developing appropriate protection measures
- Ability to review system changes for security implications and recommending improvements
- Understanding of cyber security methodologies
- Proficient in Java, Net, C++, Python, bash, power shell
- Good team player, self-confident, motivated, and independent
- Excellent communication skills
- Bachelor's degree or equivalent in Computer engineering/science preferred
- Current knowledge of technology capabilities and trends; types, and techniques of hacking attacks in the wild
- Understanding of the OSI (Open Systems Interconnection) model and renowned ports and services can be an added advantage
- Significant low-level networking experience with the TCP/IP (Transmission Control Protocol/Internet Protocol) stack can be an added advantage
- Ability to multi-task with a calm demeanor and work under pressure in a fast-paced environment
- One of five potential security-related certifications or capacity to acquire a Public Trust security clearance can be an added advantage
- Attention to details and good problem-solving skills
- Veteran enterprise-level security strategic planning experience can be an added advantage
- Knowledge of DoD (Department of Defense) 8500 series Risk Management Framework (RMF) processes can be an added advantage.