Cyber Security

Cyber Security Job Responsibilities:

- Safeguards information system assets by identifying and solving potential and actual security problems.
- Protects system by defining access privileges, control structures, and resources.
- Recognizes problems by identifying abnormalities; reporting violations.
- Implements security improvements by assessing current situation; evaluating trends; anticipating requirements.
- Determines security violations and inefficiencies by conducting periodic audits.
- Upgrades system by implementing and maintaining security controls.
- Keeps users informed by preparing performance reports; communicating system status.
- Maintains quality service by following organization standards.
- Maintains technical knowledge by attending educational workshops; reviewing publications.
- Contributes to team effort by accomplishing related results as needed.

Cyber Security Qualifications / Skills:

- System administration
- Network security
- Problem solving
- Information security policies
- On-call network troubleshooting
- Firewall administration
- Network protocols
- Routers, hubs, and switches
- Informing others
- Process improvement

Education, Experience, and Licensing Requirements:

- Bachelor’s degree in Computer Science, Information Systems, or equivalent education or work experience
- 4+ years of prior relevant experience
- Advanced certifications such as SANS GIAC/GCIA/GCIH, CISSP or CASP and/or SIEM-specific training and certification
- Hold DoD-8570 IAT Level 2 baseline certification (Security+ CE or equivalent) at start date
- Advanced understanding of TCP/IP, common networking ports and protocols, traffic flow, system administration, OSI model, defense-in-depth and common security elements.
- Hands-on experience analyzing high volumes of logs, network data (e.g. Netflow, FPC), and other attack artifacts in support of incident investigations
- Experience with vulnerability scanning solutions
- Familiarity with the DOD Information Assurance Vulnerability Management program.

- Proficiency with any of the following: Anti-Virus, HIPS, ID/PS, Full Packet Capture, Host-Based Forensics, Network Forensics, and RSA Security
- In-depth knowledge of architecture, engineering, and operations of at least one enterprise SIEM platform (e.g. Nitro/McAfee Enterprise Security Manager, ArcSight, QRadar, LogLogic, Splunk)
- Experience developing and deploying signatures (e.g. YARA, Snort, Suricata, HIPS)
- Understanding of mobile technology and OS (i.e. Android, iOS, Windows), VMware technology, and Unix and basic Unix commands
- Design, build and implement enterprise-class security systems for a production environment
- Align standards, frameworks and security with overall business and technology strategy
- Identify and communicate current and emerging security threats
- Design security architecture elements to mitigate threats as they emerge
- Create solutions that balance business requirements with information and cyber security requirements
- Identify security design gaps in existing and proposed architectures and recommend changes or enhancements
- Use current programming language and technologies to writes code, complete programming and performs testing and debugging of applications
- Train users in implementation or conversion of systems

Cybersecurity Duties and Responsibilities

- Develop unique, effective security strategies for software systems, networks, data centers, and hardware
- Implement/build-in security systems to software, hardware, and components
- Research best ways to secure company-wide IT infrastructure
- Build firewalls to protect network infrastructures
- QA software and hardware for security vulnerabilities and risks
- Monitor software for external intrusions, attacks, and hacks
- Close off security vulnerability in the case of an attack
- Identify cyber attackers, report to upper management, and cooperate with police or other legal forces to detain perpetrator
- Work independently or as part of a team as needed

Cybersecurity Requirements and Qualifications

- Bachelor’s degree in computer science or STEM subject prefered
- Completion of an internship/apprenticeship in cybersecurity a plus
- Strong IT skills including knowledge on hardware, software, networks, and data centers
- Thorough work ethic, attention to detail
- Skills of perception and QA, ability to identify vulnerabilities and overall issues
- Critical thinking skills, problem solving aptitude
- Forensic approach to challenges
- Ability to think like a hacker and anticipate hacker moves
- Desire to self-educate on the ever-changing landscape of cyber hacking tactics
- Experience in professional cybersecurity a plus

Similar Job Titles

- Cybersecurity Manager
- Cybersecurity Analyst
- Cybersecurity Specialist
- Information Systems (IT) Manager
- Information Technology/Software Trainer
- Systems Analyst
- Set and implement user access controls and identity and access management systems
- Monitor network and application performance to identify and irregular activity
- Perform regular audits to ensure security practices are compliant
- Deploy endpoint detection and prevention tools to thwart malicious hacks
- Set up patch management systems to update applications automatically
- Implement comprehensive vulnerability management systems across all assets on-premises and in the cloud
- Work with IT operations to set up a shared disaster recovery/business continuity plan
- Work with HR and/or team leads to educate employees on how to identify suspicious activity
- Set and implement user access controls and identity and access management systems
- Monitor network and application performance to identify and irregular activity
- Perform regular audits to ensure security practices are compliant
- Deploy endpoint detection and prevention tools to thwart malicious hacks
- Set up patch management systems to update applications automatically
- Implement comprehensive vulnerability management systems across all assets on-premises and in the cloud
- Work with IT operations to set up a shared disaster recovery/business continuity plan
- Work with HR and/or team leads to educate employees on how to identify suspicious activity

Responsibilities

As a cyber security analyst, you'll need to:

- keep up to date with the latest security and technology developments
- research/evaluate emerging cyber security threats and ways to manage them
- plan for disaster recovery in the event of any security breaches
- monitor for attacks, intrusions and unusual, unauthorised or illegal activity
- test and evaluate security products
- design new security systems or upgrade existing ones
- use advanced analytic tools to determine emerging threat patterns and vulnerabilities
- engage in 'ethical hacking', for example, simulating security breaches
- identify potential weaknesses and implement measures, such as firewalls and encryption
- investigate security alerts and provide incident response
- monitor identity and access management, including monitoring for abuse of permissions by authorised system users
- liaise with stakeholders in relation to cyber security issues and provide future recommendations
- generate reports for both technical and non-technical staff and stakeholders

- maintain an information security risk register and assist with internal and external audits relating to information security
- monitor and respond to 'phishing' emails and 'pharming' activity
- assist with the creation, maintenance and delivery of cyber security awareness training for colleagues
- give advice and guidance to staff on issues such as spam and unwanted or malicious emails.

Requirements – Skills, Abilities, and Knowledge – for Cyber Security Engineer Role

If you are seeking the job of a cyber security engineer, here are typical requirements and qualifications most recruiters will expect you to have:

- 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.