CYBER SECURITY ENGINEER I

DEFINITION

Analyzes, installs, operates, and maintains a variety of cyber security controls and tools and performs cyber security operational tasks such as managing security incidents, functional reviews, validating findings, and recommending remediation processes.

TYPICAL DUTIES

- Coordinates and carries out the activities of the secure file transfer application to ensure files are securely maintained and transferred.
- Analyzes security investigations and monitors security analytics by leveraging the security information event management (SIEM) tool to identify and correct any anomalies.
- Analyzes, installs, upgrades, and monitors security controls, focusing on firewall systems, Virtual Private Network systems, content filtering hardware and software, and intrusion detection devices.
- Researches IT security issues and industry trends to make recommendations for internal improvement.
- Reviews security logs to facilitate auditing activities.
- Collaborates with various IT units in organizing, writing, and editing technical instructions, operational procedures, and related materials, as appropriate.
- Maintains, generates, and applies internal and/or external SSL certificates on servers by coordinating with other IT departments to ensure the certificates are appropriate and up-to-date.
- Troubleshoots, monitors, and maintains the security hygiene messaging gateway to prevent or resolve any issues, threats, or inappropriate content that may be received.
- Performs regular system administration, installs software patches, reviews logs, and resolves security events.
- Diagnoses and corrects security-related network issues.
- Participates in incident response activities with affected business units and applicable IT personnel.
- May assist with web filters by reviewing dashboard for actionable items and processing requests to ensure the functionality of the system.
- May assist higher level engineers with the configuration and validation of Domain Name Server (DNS) requests by creating internal and external A records, internal and external C name aliases, and creating external TXT records.
- May assist with network security device and appliance testing by performing functional reviews, validating findings and implementing remediation processes.
- Performs related duties as assigned.

DISTINGUISHING CHARACTERISTICS AMONG RELATED CLASSES

A Cyber Security Engineer I monitors, troubleshoots, and maintains network security incidents and escalates or assists with more complex cyber security tasks such as monitoring of content filtering hardware and software, intrusion detection devices, managed/secure file transfer and associated systems.

A Cyber Security Engineer II configures and maintains network security controls and appliances and is responsible for the maintenance tasks associated with their operation.

A Cyber Security Engineer III is responsible for the overall design, administration, and installation, upgrades, and management of the security infrastructure and security controls.

SUPERVISION

General supervision is received from the Cyber Security Engineer III or other higher level cyber security administrator. Technical direction may be exercised over lower-level staff engaged in cyber security activities.

CLASS QUALIFICATIONS

Knowledge of:

- Current firewall, VPN, content filtering, and intrusion detection methodologies
- TCP/IP protocols including IP addressing, subnetting and well known ports
- Industry standards for encryption including but not limited to FTP, SFTP and SSH
- Basic networking concepts and services such as DNS, SMTP, HTTP, and HTTPS
- Risk and threat assessment processes and practices
- Malware such as worms, viruses and Trojans
- Unsecure protocols ports and services
- Incident response procedures and processes
- Windows and Linux security processes

Ability to:

- Develop, analyze, and maintain tools that support and automate processes for software product release
- Install, configure and monitor network security devices, including firewalls, VPN, content filtering, and Intrusion Detection Systems
- Analyze and diagnose malfunctions and perform required changes
- Learn characteristics of new security threats, vulnerabilities, and countermeasure techniques and technology
- Effectively communicate technical information to all levels of staff
- Maintain effective working relationships
- Identify and analyze trends related to threats
- Conduct WireShark captures
- Maintain up-to-date detailed knowledge of the IT Security industry including awareness of new or revised security solutions, improved security processes, and the deployment of new attacks and threat vectors

ENTRANCE QUALIFICATIONS

Education:

Graduation from a recognized college or university with a bachelor's degree in computer science or a related field. Qualifying experience in addition to that required may be substituted on a year-for-year basis provided that the requirement of a high school diploma or equivalent is met.

Experience:

Two years of recent experience in the engineering, installation, configuration, and maintenance of security devices for a large organization; such as next-generation firewalls, Virtual Private Networks, intrusion detection/prevention systems, multi-factor authentication, next-generation endpoint security, and Security Information Event Management systems.

Special:

Cisco Certified Network Associate is required and must be kept valid during the term of employment
Information Technology Infrastructure Library (ITIL) Foundation level certification is preferable
A valid California Driver License
Use of an automobile

SPECIAL NOTES

Employees in this class may be subject to call at any hour.

This class description is not a complete statement of essential functions, responsibilities, or requirements. Entrance requirements are representative of the minimum level of knowledge, skill, and /or abilities. To the extent permitted by law, management retains the discretion to add or change typical duties of a position at any time, as long as such addition or change is reasonably related to existing duties.

New Class
05-14-18
PJO