LOS ANGELES UNIFIED SCHOOL DISTRICT
PERSONNEL COMMISSION

CLASS DESCRIPTION
CLASS CODE 4886
Confidential

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

- Analyzes, monitors, and correlates security event information from logs, endpoints, networks, and cloud environments, across multiple systems, applications, and users to detect and mitigate external and internal threats.
- Regularly monitors network security devices and systems to identify false positives and perform tuning to collect the right cyber security-related events
- Monitors, installs, and upgrades security devices and controls, that manage the flow of information between networks of different trust levels in order to prevent attackers from exploiting District information assets.
- Researches IT security issues and industry trends to make recommendations for internal improvement.
- Implements, maintains, and applies cryptographic protocols, keys, and credentials to secure information in transit and at rest, authenticate machines and users, and sign data.
- Monitors, troubleshoots and maintains messaging systems to identify malicious email attacks and correlate email telemetry with wider security events, behavior analytics, and other threat information to determine if a cyber attack has occurred, is occurring, or will occur.
- Participates in incident response activities and provides security threat analytics in support of Computer Incident Response Team (CIRT).
- Configures, maintains, and monitors endpoint protection controls such as auto-sandboxing, web filtering, and antivirus to prevent, detect, and remove malware.
- 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.
- Monitors the ongoing operational use of ports, protocols, and services on networked devices in order to prevent potential security risks and vulnerabilities.
- Monitors signs of data exfiltration and escalates for mitigation to ensure the privacy and integrity of sensitive District information.
- 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, analyzes, and correlates cyber security events and logs to identify and mitigate network cyber security incidents and escalates or assists with more complex cyber security incidents or tasks.

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 IT Infrastructure Security Manager 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
- SEIM tool or other similar correlational tools

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 or equivalent certification such as Cisco Cybersecurity Operations Fundamentals or Cisco Certified Network Associate (Security) 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.

Revised
07-16-20
PJO