LOS ANGELES UNIFIED SCHOOL DISTRICT
PERSONNEL COMMISSION

CLASS DESCRIPTION
CLASS CODE 4884
Confidential

CYBER SECURITY ENGINEER II

DEFINITION

Configures, evaluates, operates and maintains a variety of security controls and tools to perform complex Cyber Security operational tasks including developing and evaluating approaches to solving Cyber Security challenges.

TYPICAL DUTIES

- Evaluates and participates in the development of requirements for network and security technologies and devices to ensure the requirements are adequate for the District.
- Performs network security device and appliance testing, implementation, and maintenance via installation, upgrades, patches, and updates with appropriate security controls such as authentication and configuration.
- Collaborates with various IT units in the District's vulnerability management program by performing technical scans, highlighting vulnerabilities and providing remediation to reduce risk.
- Assesses security threats posed by changes in systems architecture and dependencies.
- Collaborates with higher level engineers in the review of security architecture to identify gaps or deficiencies within the District's network in order resolve issues or find solutions.
- Validates and configures Domain Name Server (DNS) requests by creating internal and external A records, internal and external C name aliases, and creating external TXT records.
- Analyzes and corrects security-related connectivity issues utilizing network management systems.
- Configures firewalls by creating and maintaining access list rules, creating object groups and processing network addressing translation requests to maintain access control.
- Configures the District's web access filter by processing requests on dashboard to ensure the functionality of the system and review dashboard for actionable items.
- Fulfills Virtual Private Network (VPN) requests by adding new users to active directory VPN groups, maintaining and configuring access lists, adding IP addresses to access list, assign software token for password generation, and review authentication logs and troubleshoot access issues.
- Recommends security solutions or enhancements to existing security solutions to improve overall enterprise security.
- Collaborates with higher level engineers in the deployment, integration and initial configuration of all new security solutions and of any enhancements to existing security solutions.
- Researches IT security issues and industry trends to make recommendations for internal improvement.
- Performs related duties as assigned

DISTINGUISHING CHARACTERISTICS AMONG RELATED CLASSES

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 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 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
- Knowledge of security tools such as IDS/IPS, SIEM, DLP
- Knowledge of vulnerability assessment tools including but not limited to Nessus, Nmap and Metasploit
- Risk and threat assessment processes and practices
- Malware such as worms, viruses and Trojans
- Proof of Concepts procedures and processes
- Project management techniques

Ability to:

- Install, configure and monitor network security devices, including firewalls, VPN, content filtering, and Intrusion Detection Systems
- Design and implement technical modifications to firewall, VPN, content filtering, and intrusion detection rule sets
- 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
- Train and mentor staff effectively
- 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:

Four 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 Professional (CCNP) Security, Cisco Certified CyberOps Professional or equivalent is required and must be kept valid during the term of employment
Any Global Information Assurance Certification GIAC certification is preferred
Information Technology Infrastructure Library (ITIL) Foundation level certification is preferable
A valid driver's license to legally operate a motor vehicle in the state of California and the use of a motor vehicle.

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
10-20-22
JAP