CYBER SECURITY ENGINEER III

DEFINITION

Plans, manages and designs the District's security infrastructure and performs the most complex Cyber Security operational tasks to ensure compliance with defined requirements and seamless integration with various technologies

TYPICAL DUTIES

Reviews security architecture to identify gaps or deficiencies within the District's network in order to resolve issues or find solutions.
Administers, designs, and maintains the District's IT security architecture, including the District's secure file transfer system, web application firewall, security analytics application, firewall, District's Virtual Private Network (VPN), and security hygiene messaging gateway.
Performs validation reviews to ensure that network devices are tested, implemented, and maintained via upgrades, patches, and updates with appropriate security controls.
Recommends security solutions or enhancements to existing security solutions to improve overall enterprise security.
Designs, manages and coordinates 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 and implement modifications for internal improvement.
Performs related duties as assigned.

DISTINGUISHING CHARACTERISTICS AMONG RELATED CLASSES

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

An IT Infrastructure Security Manager develops strategies for critical IT Infrastructure security initiatives and leads a team of security engineers to ensure the proper design and implementation of infrastructure security services.

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

SUPERVISION

General supervision is received from the IT Infrastructure Security Manager or other higher level administrator. General supervision is exercised over lower-level personnel.

CLASS QUALIFICATIONS

<u>Knowledge of:</u>

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
Understanding and ability to apply project planning and management concepts

Knowledge of vulnerability assessment tools including but not limited to Nessus, Nmap and Metasploit
Understanding of risk and threat assessment processes and practices
Understanding of malware such as worms, viruses and Trojans
Proof of Concepts procedures and processes
Project management techniques
RFP and other procurement processes

Ability to:

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 independent systems analysis of complex business processes
Develop secure architecture designs and systems
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:

Six 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
Certified Information Systems Security Professional (CISSP) is preferred
Information Technology Infrastructure Library (ITIL) Foundation level certification is preferable
Project Management Professional (PMP) 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