Cybersecurity Engineer

Purpose Statement:

Under administrative supervision, the Cybersecurity Engineer is responsible for conducting comprehensive cybersecurity assessments in various K-12 information technology environments, identifying vulnerabilities, and simulating real-world attack scenarios; monitoring and assessing information systems to mitigate vulnerabilities and implement information technology security solutions and programs by utilizing security tools and techniques.

Diversity Statement:

Because each person is born with inherent worth and dignity, and because equitable access and opportunity are essential to a just, educated society, SDCOE employee commitments include being respectful of differences and diverse perspectives, and being accountable for one's actions and the resulting impact.

Representative Duties:

This position description is intended to describe the general nature and level of work being performed by the employee assigned to the position. This description is not an exhaustive list of all duties, responsibilities, knowledge, skills, abilities, and working conditions associated with the position. Incumbents may be required to perform any combination of these duties.

Essential Functions

- Performs security assessments, including security program reviews, penetration testing, vulnerability testing, risk analysis to identify and address potential threats, and provides recommendations related to findings.
- Analyzes security data from computing and network devices to identify potential threats, risks, and vulnerabilities and cause of security incidents.
- Analyzes system outages, alerts, and reports of abnormal system behavior due to suspected security-related events and incidents, including impact of damages.
- Designs and implements robust security measures for cloud environments, such as AWS, Azure, Google Cloud, or other similar platforms.
- Maintains current knowledge of information security trends and research relevant to the K-12 sector.
- Responds proactively to security incidents, performs root cause analyses, and enacts preventive security measures to safeguard the digital infrastructure.
- Compiles detailed reports on cybersecurity findings, complete with recommendations for remediation.
- Assists with the development and delivery of training and presentations on penetration testing and vulnerability management.
- Designs, builds, implements, and supports enterprise-class information security systems.
- Serves as a resource and provides Tier-2 support to cybersecurity staff in response to security-related incidents.
- Communicates cybersecurity-related vital information, security needs and priorities to senior management on a regular basis.
- Reviews and analyzes system logs, SIEM tools, and network traffic with a focus on continuous improvement; for unusual or suspicious activity and makes recommendations to restore secure operations.

- Conducts ongoing interviews and assessments with client groups for the purpose of learning how employees interact with technology and to integrate cybersecurity measures.
- Compiles and reports metrics and key performance indicators to senior management in all areas of responsibility.
- Identifies and validates security compliance and best practices for securing data, including encryption technologies and key management processes.
- Regularly attends CITE Regional meetings and other events assigned by management.

Other Functions

- Performs other related duties as assigned for the purpose of ensuring the efficient and effective functioning of the work unit.

Job Requirements: Minimum Qualifications:

Knowledge and Abilities:

KNOWLEDGE of:
Human centered and socially conscious leadership;
Performing penetration testing across multiple domains (network, cloud, application, and mobile);
Cybersecurity policies and procedures;
Industry cyber security regulations and standards (e.g., OWASP, SANS, CIS, NIST etc.);
Current security vulnerabilities and exposures (CVEs);
Industry-standard tools and frameworks used in penetration testing, such as Metasploit, Burp Suite, Nmap, Kali Linux, and other tools;
SDCOE technology and information systems;
Technical aspects of field of technical support and information technology;
Cloud computing environments, system and network security, authentication and security protocols, and cryptography.

ABILITY to:
Promote a human-centered culture that elevates the strengths of others creating a sense of belongingness;
Practice cultural competency while working collaboratively with diverse groups and individuals;
Conduct daily cybersecurity operations and services;
Create reports that are both accessible to, and easily utilized by, audiences with varying levels of technical expertise;
Develop and present training materials;
Effectively articulate and demonstrate current security vulnerabilities and exposures and their impact;
Identify abnormalities to recognize potential problems and conducting periodic audits to detect violations and report any findings;
Use current scripting languages and technologies to administer and automate information security systems;
Interpret laws, regulations, policies, and procedures and apply to cybersecurity-related incidents;
Work with a wide diversity of individuals;
Work with similar types of data and utilize job-related equipment;
Proficiently assess and address issues, utilizing data-driven problem-solving skills, and exhibiting a keen attention to detail;
Establish and maintain effective working relationships;
Communicate with persons with diverse technical knowledge and skills;
Maintain confidentiality;

Work with frequent interruptions;
Work both independently and as a member of a team to meet established goals, objectives, and vision of the unit.

Working Environment

ENVIRONMENT:
Duties are typically performed in an office setting.
May be designated in an alternate work setting using computer-based equipment to perform duties.

PHYSICAL ABILITIES:
Must be able to hear and speak to exchange information; see to perform assigned duties; sit or stand for extended periods of time; possess dexterity of hands and fingers to operate computer and other office equipment; kneel, bend at the waist, and reach overhead, above the shoulders and horizontally, to retrieve and store files; lift light objects. All requirements are subject to possible modification to reasonably accommodate individuals with a disability.

Education and Experience:

Education: A bachelor's degree from a regionally accredited college or university in Information Technology, Computer Science, or closely related field of study.

Experience: Three (3) years of work experience in implementing and monitoring information security technology, specifically with penetration testing, intrusion detection, incident response, or digital forensics. Successful experience in a school/educational environment is highly desirable.

Equivalency: A combination of education and experience equivalent to a bachelor's degree from a regionally accredited college or university in information technology, computer science, or related field of study, and three (3) years of experience in implementing and monitoring information security technology, specifically with penetration testing, intrusion detection, incident response, or digital forensics.

Required Testing	Certificates
N/A	Valid CA Driver's License CEH (Certified Ethical Hacker), or OSCP (Offensive Security Certified Professional), or GPEN (GIAC Penetration Tester)
Continuing Educ./Training	Clearances
As needed to maintain certificates	Criminal Justice Fingerprint/Background Clearance Physical Exam including drug screen Tuberculosis Clearance

FLSA State: Exempt

Salary Range: Classified Management Salary Schedule Grade 040

Personnel Commission Approved: Oct. 18, 2023