CCSD
CLARK COUNTY
SCHOOL DISTRICT

Cybersecurity Engineer Technical Specialist

Position Details

Class Code: 1440
Job Family: Information System
Classification: Support Professional
Terms of Employment: Pay Grade 62 on the Support Professional Salary Schedule
FLSA STATUS: NON-EXEMPT

Position Summary

Under general supervision, is responsible for designing, implementing, and maintaining advanced security solutions to protect the organization's information technology (IT) infrastructure and data. This role involves working with cross-functional teams to ensure the effectiveness of security measures, responding to security incidents, and enhancing the overall cybersecurity posture of the organization.

Essential Duties and Responsibilities

The list of Essential Duties and Responsibilities is not exhaustive and may be supplemented.

1. Develops and implements security architectures and solutions tailored to the Clark County School District (CCSD)'s needs, including firewalls, intrusion detection systems, and encryption technologies.
2. Assesses and selects security tools and technologies that align with business objectives and compliance requirements.
3. Configures, deploys, and maintains security systems and software, ensuring they operate effectively and securely.
4. Conducts regular updates and patches to security applications to mitigate vulnerabilities.

5. Leads incident response efforts for security breaches, investigating and analyzing incidents to identify root causes and impacts.
6. Documents incident response procedures and lessons learned to improve future responses.
7. Performs regular vulnerability assessments and penetration testing to identify and address potential weaknesses in the organization's systems.
8. Collaborates with IT and development teams to remediate identified vulnerabilities and enhance security controls.
9. Monitors security alerts and logs from various security tools and platforms, responding promptly to potential threats.
10. Utilizes security information and event management (SIEM) tools to analyze data and detect security incidents.
11. Assists in the development and implementation of security policies, standards, and procedures to ensure compliance with industry regulations.
12. Provides technical input for security training and awareness programs to educate staff on cybersecurity best practices.
13. Works closely with IT, compliance, and other departments to ensure a unified approach to security across the organization.
14. Communicates effectively with stakeholders, providing updates on security initiatives, incidents, and risk assessments.
15. Stays updated on the latest cybersecurity trends, threats, and technologies to continually enhance CCSD's security posture.
16. Participates in ongoing training and certification opportunities to develop skills and knowledge in cybersecurity.
17. Conforms to safety standards, as prescribed.
18. Performs other tasks related to the position, as assigned.

Distinguishing Characteristics

Responsible for the development and implementation of computer network security protocols. Participates in the analysis, installation, configuration, and ongoing monitoring of security infrastructure, including firewall systems, virtual private network (VPN) solutions, content filtering hardware and software, intrusion detection and prevention systems, and related security technologies. Collaborates with IT and security teams to ensure a robust security posture, proactively identifies vulnerabilities, and conducts regular assessments to maintain and improve network defenses.

Knowledge, Skills, and Abilities (Position Expectations)

1. Strong knowledge of cybersecurity frameworks, standards, and best practices (e.g., NIST, ISO 27001).
2. Proficiency in configuring and managing security technologies, including firewalls, intrusion detection system/intrusion prevention system (IDS/IPS), and SIEM systems.
3. Excellent analytical and problem-solving skills, with the ability to evaluate complex security issues and develop effective solutions.
4. Strong communication skills, with the ability to convey technical information to both technical and non-technical stakeholders.
5. Possess physical and mental stamina commensurate with the responsibilities of the position.

Position Requirements

Education, Training, and Experience

1. High school graduation or other equivalent (General Educational Development [GED], foreign equivalency, etc.).
2. Two (2) years of college courses in computer science or information security from an accredited college or university; plus, three (3) years of experience supporting/operating telecommunications and networking security, application and systems security, application development security, user authentication and authorization management, information systems vulnerability assessment, and physical data security, with supervision of technical staff; or,
3. Bachelor's degree from an accredited college or university in Computer Science, Information Technology, Cybersecurity, or a related field; plus, one (1) year of experience in cybersecurity engineering, with a focus on technical implementation and security solutions.

Licenses and Certifications

1. A valid driver's license that allows the applicant/employee to legally operate a motor vehicle in Nevada. License must be maintained for the duration of the assignment.
2. Current driving history (dated within six [6] months from the date printed) issued by the Department of Motor Vehicles (DMV) at the time of application or Qualified

Selection Pool (QSP) placement and at the time of interview prior to final selection.
3. Safe driving record. Safe driving record must be maintained for the duration of the assignment.

Preferred Qualifications

1. Relevant certifications (e.g., Certified Information Systems Security Professional [CISSP], Certified Ethical Hacker [CEH], Global Information Assurance Certification [GIAC]).
2. Four (4) to six (6) years of experience in cybersecurity engineering, with a focus on technical implementation and security solutions.
3. Proven experience in incident response, vulnerability management, and security monitoring.
4. Experience with cloud security practices and technologies (e.g., Amazon Web Services [AWS], Azure).
5. Familiarity with DevSecOps practices and secure coding principles.
6. Prior experience in a regulated industry (e.g., finance, healthcare) with knowledge of relevant compliance requirements.

Document(s) Required at Time of Application

1. High school transcript or other equivalent (GED, foreign equivalency, etc.).
2. College transcripts from an accredited college or university.
3. Copy of a valid driver's license that allows the applicant/employee to legally operate a motor vehicle in Nevada.
4. Copy of current driving history (dated within six [6] months from the date printed) issued by the DMV.
5. Safe driving record.
6. Specific documented evidence of training and experience to satisfy qualifications.

Examples of Assigned Work Areas

Enterprise Information Security Department, and travel to and from schools and other CCSD office settings.

Work Environment

Strength

Sedentary/light - exert force up to 20 lbs., occasionally; 10 lbs., frequently; negligible force, constantly.

Physical Demand

Frequent sitting, standing, walking, pushing, pulling, stooping, kneeling, crouching, reaching, handling, and repetitive fine motor activities. Hearing and speech to communicate in person, via video conference and computers, or over the telephone. Mobility to work in a typical office setting and use standard office equipment. Stamina to remain seated and maintain concentration for an extended period of time. Vision: Frequent near acuity, occasional far acuity, and color vision. Vision to read printed and online materials, Video Display Terminal screens, or other monitoring devices.

Environmental Conditions

Climate-controlled office setting with temperatures ranging from mild to moderate cold/heat. Exposure to noise levels ranging from moderate to loud for occasional to frequent time periods.

Hazards

Furniture, office equipment, communicable diseases, chemicals and fumes (as related to specific assignment), and power/hand-operated equipment and machinery (as related to specific assignment).

Examples of Equipment/Supplies Used to Perform Tasks

CCSD-issued/personal vehicles, various computers, printers, copiers, calculators, fax machines, telephones, filing cabinets/equipment, etc.

AA/EOE Statement

The Clark County School District is proud to be an equal opportunity employer. The Clark County School District is committed to providing all applicants and employees equal employment opportunities without regard to race, color, religion, sex, gender identity or expression, sexual orientation, national origin, genetics, disability, age, military status, or other characteristics protected by applicable law. Here at Clark County School District, we are a diverse group of people who honor the differences that drive innovative

solutions to meet the needs of our students and employees. We believe that through a culture of inclusivity, we have the power to reflect the community we serve.

Job Revision Information

- Created: 02/19/25