JOB DESCRIPTION

San Diego County Office of Education

CYBERSECURITY SPECIALIST

Purpose Statement:
Under general supervision, the Cybersecurity Specialist is responsible for leading, coordinating, and overseeing advanced cybersecurity functions for SDCOE and supported local educational agencies, provides program-level leadership in incident response, vulnerability management, cybersecurity training, and enterprise phishing simulation services (Red Herring), exercises independent judgment, strategic coordination, and professional discretion.

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:

- Oversees and manages Red Herring phishing simulation campaigns for SDCOE and participating districts, serving as the primary technical liaison for campaign management, troubleshooting, training and continuous improvement based on district feedback.
- Responds to significant cybersecurity risks and planned operations, providing strategic guidance and coordination.
- Continuously monitors systems, applications, networks, and logs for security incidents using SDCOE approved tools (e.g., Microsoft Sentinel, Defender and other security applications)
- Leads and coordinates complex incident response activities, ensuring timely containment, escalation, and resolution of threats.
- Guides and coordinates vulnerability management activities across SDCOE departments and participating local educational agencies, ensuring alignment with CIS Controls and organizational cybersecurity policies and standards.
- Develops, maintains, and leads incident response plans and conduct investigations of cybersecurity incidents and breaches.
- Collaborates with network, application, infrastructure, and other Information Technology Services (ITS) teams to support the secure design, implementation, and operation of systems and services.

- Provides oversight and delivery of cybersecurity training and awareness programs for staff, students, and partner agencies, including phishing awareness, threat recognition, and safe technology practices.
- Prepares and presents comprehensive reports on cybersecurity operations, risks, and outcomes of key initiatives.
- Serves as the lead point of contact and technical liaison for local educational agencies during cybersecurity investigations and incidents.
- Mentors and coaches students participating in internship programs, to support workforce development initiatives.
- Participates in on-call rotations to ensure timely response to after-hours and high-impact cybersecurity incidents.
- Monitors and evaluates AI-driven applications and platforms for emerging threats and collaborate to develop robust defense strategies for AI workloads.

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;
Advanced network security concepts;
Phishing simulation platforms (e.g., Red Herring), and cyber defense methodologies;
Incident response frameworks and vulnerability management practices;
Cybersecurity training development and program implementation;
Applicable laws, regulations, and industry standards related to information security.

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;
Lead technical initiatives and mentor others;
Analyze complex security threats and respond swiftly and effectively;
Develop and oversee cybersecurity training programs;
Exercise sound judgment, maintain confidentiality, and communicate technical information clearly to varied audiences.

Working Environment:

ENVIRONMENT:
Duties are typically performed in an office setting environment; may require occasional travel or off-hour response.

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; and

Experience: Three (3) years of progressively responsible experience in cybersecurity is required. Including work within complex technical environments in the area of network security, application development, computer system support, or related areas; or

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 closely related field and three (3) years of progressively responsible experience in cybersecurity is required. Including work within complex technical environments in the area of network security, application development, computer system support, or related areas

Required Testing	Certificates, Licenses, Credentials
N/A	GSOC, GCIH, CEH certifications in areas of Security Essentials or incident handling are highly desirable. Valid California Driver's License
Continuing Educ./Training	**Clearances**
N/A	Criminal Justice Fingerprint/Background Clearance Physical Exam including drug screen Tuberculosis Clearance

FLSA Status: Exempt
Salary Grade: Classified Management, Grade 033

Personnel Commission Approval: April 15, 2026

Revised: N/A