JOB DESCRIPTION
San Diego County Office of Education

DIRECTOR, SECURITY OPERATIONS CENTER

Purpose Statement:

The Director, Security Operations Center (SOC) is responsible for directing, planning, developing, and maintaining a comprehensive, enterprise-wide cybersecurity program to protect SDCOE electronic data and network infrastructure from external and internal security breaches, data loss, and privacy violations. The Director, Security Operations Center is also tasked with providing cybersecurity services to San Diego County local education agencies (LEAs) as well as other statewide LEAs, as directed.

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:

- Ensures cybersecurity measures taken follow statutory and regulatory requirements regarding information access, security, and privacy.
- Reviews alerts, alarms, dashboards, and reports to determine relevancy and urgency of cybersecurity threats, vulnerabilities, and incidents.
- Implements standards and procedures to ensure alerts are addressed with relevancy, accuracy, and in a timely manner.
- Directs appropriate threat escalation responses and prepares clear and concise communications to ITS leadership and other partners during major incidents.
- Defines protocols and ongoing development of 'playbooks' for operational response to cyber threats.
- Serves as the incident response primary coordinator and leads SOC staff during incident response actions, advise and coordinate with ITS leadership during active incidents.
- Supervises the implementation of new technologies and business processes to improve SOC value and efficiency.
- Serves as technical expert related to monitoring and response of partner LEA operations and provides input to ITS senior management on recommendations for supporting partner LEAs.

- Oversees the communication of alerts to LEAs regarding intrusions and compromises to their networks, applications, and operating systems.
- Collaborates with vendor partners and consultants to ensure technical solutions, workflows, and processes for the SDCOE SOC are thoughtful, innovative, and forward-looking.
- Collaborates with outside law enforcement agencies for the purpose of investigating electronic security breaches, as needed.
- Coordinates cybersecurity business continuity and data recovery policies with appropriate units across the organization division for the purpose of supporting organization goals
- Creates audit and security reports to identify needed responses to unusual or suspicious activity, exceptions, and abnormalities in the SDCOE digital environments.
- Develops, implements, and monitors an ongoing risk assessment program and information security management system for the purpose of targeting electronic information, and infrastructure security, and security breach prevention, detection, and remediation.
- Directs and maintains configuration management of electronic security systems, applications, and data encryption for the purpose of providing total data security including policy assessment and compliance tools, network security appliances, and host-based systems.
- Establishes information and infrastructure security controls, including log monitoring procedures, identification of unnecessary services/applications, redundant accounts, risky applications, etc. for the purpose of identifying unnecessary services/applications, redundant accounts, risky applications, etc. to support system hardening and policy and procedure alignment.
- Implements practices and standards for user access, operating systems, applications, network security devices, appliance, server patching, etc. for the purpose of incorporating changes to policies, standards, and procedures of the SDCOE and industry best practices.
- Leads the development, maintenance and dissemination of electronic information security, policies, standards, procedures, and other SOC documentation activities.
- Provides relevant and ongoing training opportunities for SOC staff.

Other Functions:

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

Job Requirements:

Knowledge and Abilities:

KNOWLEDGE of:

Human centered and socially conscious leadership;
Established cybersecurity frameworks and standards such as NIST, Cybersecurity Framework, CIS Controls and their application to develop and maintain effective security programs;
Current cybersecurity threats, attack vectors, and evolving trends;
Complex IT Systems, cybersecurity policies and privacy standards;
ITIL V4 Service Management principles and procedures;

Thread intelligence and vulnerability management;
Risk management and risk assessment methodologies;
Security Operations Center (SOC) processes or procedures;
Information security governance principles and practices and understanding of policies, procedures and controls required to maintain a secure and compliant environment;
California Student Privacy Alliance (CSPA) and its resources, which provide support to LEAs in addressing student data privacy requirements and promoting responsible data stewardship.

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;
Promote a culture where employee wellness and professional development are essential to maintaining a skilled and motivated workforce;
Promote an environment of positive customer service (internal and external) and continuous improvement to meet SDCOE and ITS goals and objectives;
Establish strong team and individual SOC staff objectives to be measured against Key Performance Indicators;
Think strategically and develop long term cybersecurity plans;
Stay up to date with the latest threat intelligence and K-12 education specify risks to ensure proactive security measures.
Identify security risks, proposing innovative solutions, and driving continuous improvement;
Strong analytical and problem-solving skills to assess complex security issues, analyze data, and make informed decisions.
Troubleshoot and resolve security incidents efficiently;
Adapt to rapidly changing security threats and technologies.
Demonstrates flexibility in managing priorities, resources, and stakeholder expectations in a dynamic environment;
Demonstrates a commitment to ongoing learning and professional development in the field of cybersecurity.
Actively seek out new information, certifications, and training opportunities to stay updated with the evolving security landscape;
Collaborate and establish strong partnerships with local educational agencies to share best practices, provide guidance on cybersecurity measures, and facilitate information sharing to enhance the overall security posture of the K-12 educational community.

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 in computer science or a closely related field from an college or university accredited by a regional accrediting organization. Master's degree in computer science or closely related field is highly desirable.

Experience: Five (5) years working in a technical capacity in one or more of the following areas: database, programming, networking and at least one (1) year supervisory experience managing technical IT staff in a cybersecurity environment.

Equivalency: A bachelor's degree in computer science or a closely related field from an institution of higher learning accredited by a regional accrediting organization and five (5) years working in a technical capacity in one or more of the following areas: database, programming, networking and at least one (1) year supervisory experience managing technical IT staff in a cybersecurity environment. Master's degree in computer science or closely related field is highly desirable.

Required Testing	Certificates, Licenses, Credentials
N/A	Valid California Driver's License Professional certification from GAIC or CISSP in one or more of the following areas: Incident Handling, Secure Programming, Security Leadership desirable.
Continuing Educ./Training	**Clearances**
N/A	Criminal Justice Fingerprint/Background Clearance Physical Exam including drug screen Tuberculosis Clearance

FLSA State: Exempt

Salary Range: Classified Management Salary Schedule Grade 50

Personnel Commission Approved: Oct. 18, 2023