Sacramento County Office of Education Job Description
Classification Title: Cybersecurity Engineer

Definition

Under general direction as part of the Computer, Network, and Telecommunications Support (CNTS) team, performs a variety of duties and responsibilities related to the implementation of cybersecurity systems and controls within the Sacramento County Office of Education (SCOE) network; provides cybersecurity-related assistance and consultation to school districts; performs other related duties as assigned.

Directly Responsible To

Appropriate Administrator

Supervision Over

Professional, technical, and clerical personnel as assigned.

Duties and Responsibilities

(Any one position may not include all of the listed duties, nor do all of the listed examples include all tasks which may be found in positions within this classification.)

Manages various cybersecurity systems including but not limited to: firewalls, Office 365 security systems, endpoint protection systems (antivirus), Virtual Private Network (VPN) systems, Intrusion Detection Systems (IDS), and Intrusion Prevention Systems (IPS); develops and maintains centralized security alert logging and reporting systems; assists with updating and maintaining incident response plan; researches and performs security updates and patches; reviews, implements, and maintains Center for Internet Security (CIS) controls; implements Data Loss Prevention (DLP) systems; installs, manages, and updates firewall rules and other security-related devices; investigates security alerts and suspicious network activity; mitigates, remediates, and assists with recovery from security events; investigates suspicious user activity within Microsoft Office 365, Google Workspace, and other systems; creates critical incident reports; identifies phishing and social engineering attacks targeting SCOE and notifies staff of associated security risks; performs vulnerability scans on SCOE and school district networks; interprets scan results and works with staff to remediate security issues; removes network devices that pose security risks; assists with the identification and development of security training content; may present security training to SCOE or district staff; implements new and emerging cybersecurity systems and services; remains up-to-date on current cybersecurity best practices and policies; may work with local, state, and federal agencies related to security incidents; ensures SCOE follows all new and existing state and federals laws, requirements, and guidelines regarding data privacy and security; attends pertinent local, regional, and state conferences, trainings, or workshops.

Minimum Qualifications

Education, Training, and Experience

Any combination of education, training, and experience equivalent to a bachelor’s degree with a technical major such as Computer Science or related field from an accredited institution; five or more years of progressively responsible experience in the technology field; three years related to the duties of this position desirable; trainings or certifications in cybersecurity-related systems or technologies preferred.

Knowledge of

Cybersecurity methodologies and technologies; network security and access control systems such as firewalls, endpoint protection systems (antivirus), Virtual Private Network (VPN) systems, Intrusion Detection Systems (IDS), and Intrusion Prevention Systems (IPS); principles of local and wide-area network design and operation; modern scripting languages such as PowerShell, Bash, Python, or Perl; data security design; modern operating systems including Windows, Mac OS, and Linux; application, server, and storage architecture; cybersecurity laws and regulations; standards, controls, policies, and procedures as defined by CIS, SANS, or NIST

Skill and Ability to

Conduct daily cybersecurity operations and services; install, configure, and maintain firewalls and other cybersecurity systems; perform vulnerability scans, configuration audits and security monitoring; investigate suspicious network and user activity; maintain high level of attention to detail; make cybersecurity-related recommendations; learn new hardware and software systems and adapt to changes in technology; prioritize, organize, and schedule work assignments and projects; work independently with minimal direction; effectively convey technical knowledge to non-technical audiences; lead and manage projects; establish and maintain cooperative working relationships with those contacted during the course of work; accurately document incidents and create reports; communicate effectively in oral and written forms with individuals from various socioeconomic and cultural backgrounds

Other Characteristics:
Possession of a valid California driver's license and willingness to travel locally using own transportation to conduct work assignments.

Approved by the Personnel Commission 11/8/2022