JOB DESCRIPTION
Puyallup School District
Professional Technical - Level 18

Cyber Security Engineer

Purpose Statement

The Cyber Security Engineer is responsible to help plan, design, implement and carry out the district's security strategy and recommend security enhancements to leadership with the goal of protecting computer systems and networks. As sensitive data is more frequently stored on computer systems, and hacking and cyber-attacks grow more frequent, the district relies on the Security Team to develop strategies to prevent, detect, respond to, and recover from Cyber Security incidents. Also, the Cyber Security Engineer has basic to advanced familiarity and skills in network operations and collaborates with all facets of department and their teams to ensure network-wide security. The Cyber Security Engineer should have a sense of urgency, be able to prioritize workload, communicate with professionalism and follow through to ensure that service levels are met and exceeded to meet the core mission of the district.

Essential Functions

- Works with department teams and various other departments to ensure coordination of team and resources to accomplish the needs and support of the district.
- Works with department staff and leadership to help plan, organize and align work priorities to meet and exceed service level objectives.
- Communicates proactively and clearly with various teams within the department and the district to ensure follow-through.
- Manages tasks, timelines, and deadlines with assurance to customers.
- Drives the success of the team and department constantly pushing the limits of what can be accomplished.
- Contributes knowledge and expertise of area to department leadership to help guide decision making.
- Maintains strict confidentiality of accessible district information resources.
- Assures network security, availability, and integrity.
- Collaborates with all department teams and leadership as well as other district staff, teams, and/or departments.
- Follows direction of team lead.

Cyber Security Engineer Focused Functions

- Assists with security tickets and requests submitted via ticketing system, phone calls, emails, messages, etc.
- Utilizes monitoring solutions for indications of compromise, issues, audit, anomalies, trends, and intrusions.
- Assists in performing forensic reviews using technology tools and log aggregators such as public records requests, digital investigations, etc.
- Monitors, reviews, and collaborates with teams around patching of various systems and performing vulnerability scans.
- Develops policies, procedures, and playbooks for frequent security workflows (documentation) leveraging defense-in-depth methodology.
- Actively follows and engages with cyber security industry professionals' blogs, industry news, and forums of other cyber security professionals for latest strategies and emerging threats.
- Creates, analyzes, establishes, maintains, and update security requirements for our systems/network.
- Actively defends network systems against unauthorized access, modification and/or destruction from both internal and external threats.
- Ensures that the district complies with statutory and regulatory requirements regarding information access, security, and privacy.
- Configures and supports security tools such as Microsoft Defender ATP, Security and Compliance, etc.
- Trains fellow department staff in security awareness, policies, and procedures.
- Designs and conducts security audits to ensure operational security and make policy recommendations.
- Responds immediately to security incidents and provide post-incident analysis.
- Creates, updates, and maintains system and security documentation and configuration data for regulatory and audit purposes.

Other Functions

- Leads small teams to accomplish tasks, projects, and goals of department.
- Collaborates with department leadership to periodically revise technology standards to best meet the needs of the district's students and staff.
- Evaluates and responds to special requests for technology and/or support as will arise from time to time.
- Assists other personnel as may be required for the purpose of supporting them in the completion of their work activities.
- Attends meetings as assigned for the purpose of conveying and/or gathering information required to perform functions.

Job Requirements: Minimum Qualifications

Skills, Knowledge, and Abilities

SKILLS include analyzing and documenting existing security controls and review and update documentation; analyze security systems/controls and seek improvements on a continuous basis; evidence and chain-of-custody experience; an understanding of best practices and how to implement them at an enterprise level; help educate the workforce on common threats through cyber security training and awareness; critical thinking skills and the ability to solve problems as they arise; planning, researching and developing security policies, standards, and procedures; experience with scripting (PowerShell, Bash, Python, etc.); perform multiple tasks with the need to upgrade skills to meet changing job requirements.

KNOWLEDGE of different frameworks such as NIST SP-800 (or NIST CSF) and the MITRE ATT&CK Framework; disaster recovery strategies and incident response plans; computer forensic tools; the CIA Triad, what it means, and how to apply it using security controls; risk assessment/management tools, technologies, and methods; anti-virus software, intrusion detection, firewalls, content filtering; digital forensic tools.

ABILITY to communicate effectively with people at all levels of experience and responsibility throughout the district is required. Assist staff with computer operations and software problems; learn and develop new operations, procedures, processes and use of new equipment; articulate technical information to non-technical audiences in person, via written communication and telephone; organize, set priorities and work effectively under pressure; exercise sound judgement, including appropriate handling of confidential matters; learn continually and keep abreast of technological changes in the field; work independently with minimum supervision.

Responsibility

Responsibilities include working under limited supervision following standardized practices and/or methods; providing information and/or advising others; and utilizing resources from other work units may be required to perform the job's functions. There is a continual opportunity to significantly impact the organization's services. Maintain regular and punctual attendance.

Working Environment

The usual and customary methods of performing the job's functions require the following physical demands: generally performed in an indoor office/school environment with frequent interruptions and noise associated with computer equipment, staff and students, and some exposure to risk of injury and/or illness; sitting/standing for prolonged periods; daily walking and moving between work areas; exposure to visual display terminal for prolonged periods; arm, wrist, elbow and hand movements associated with prolonged keyboarding; hand and finger dexterity.

Experience

Minimum two (2) years of experience working in an enterprise network environment required.
Minimum two (2) year of experience with current network security protocols, hardware and software preferred.

Education

Bachelor’s degree in technology field or completion of equivalent training required.
Holding one of the following professional certifications is preferred: CISSP, CISM, GSEC, CEH, Security+.

Other experience and/or education may be substituted for required experience and/or education.

Required Testing

Pre-Employment Proficiency Test is required

Certificates/Licenses

CISSP, CISM, GSEC, CEH, Security+

Clearances

Valid Driver's License and Evidence of Insurability
Criminal Justice Fingerprint/Background Clearance