GUILFORD COUNTY SCHOOLS JOB DESCRIPTION

JOB TITLE: CYBERSECURITY ANALYST I

TECHNOLOGY SERVICES DEPARTMENT

GENERAL STATEMENT OF JOB

Reporting to the IT Security Supervisor, the CyberSecurity Analyst I is responsible for monitoring, detecting, and responding to security incidents and alerts. This entry-level role focuses on maintaining cybersecurity defenses and supporting the organization's ongoing security efforts through continuous monitoring, documentation, and reporting. The analyst will also assist in performing risk assessments and participating in incident response activities.

SPECIFIC DUTIES AND RESPONSIBILITIES

ESSENTIAL JOB FUNCTIONS

1. **Security Monitoring and Response:**
    a. Monitor security information and event management (SIEM) tools to identify and investigate potential threats.
    b. Respond to security incidents under the guidance of senior staff, documenting all findings and actions.
    c. Perform initial triage of alerts and escalate issues when necessary.
2. **Incident Response:**
    a. Participate in the incident response process, including containment, eradication, and recovery phases.
    b. Assist in maintaining the incident response playbooks and keeping them up-to-date.
    c. Collaborate with the IT Security team to conduct post-incident analysis.
3. **Vulnerability Management:**
    a. Conduct regular vulnerability scans and assist in remediation efforts.
    b. Track and report on vulnerabilities and ensure corrective actions are implemented.
4. **Documentation and Reporting:**
    a. Maintain detailed logs and documentation of security incidents and responses.
    b. Assist in preparing reports on security metrics, including detected threats and system vulnerabilities.
5. **Compliance and Risk Assessments:**
    a. Support compliance with district policies and state regulations.
    b. Assist in performing risk assessments to identify areas of improvement in the security posture.
6. **Training and Awareness:**

a. Contribute to user security awareness training programs by providing input on current threats and best practices.
b. Stay current with emerging security threats and vulnerabilities.

ADDITIONAL JOB FUNCTIONS

Perform other related duties as required by the IT Security team.

MINIMUM TRAINING AND EXPERIENCE

Education: Bachelor's degree in Cybersecurity, Computer Science, Information Systems, or a related field, or relevant certifications (e.g., CompTIA Security+, Certified Ethical Hacker – CEH, Microsoft Certified: Security, Compliance, and Identity Fundamentals).

Experience: Prior experience is not required, but internships or hands-on security project experience is preferred.

KNOWLEDGE, SKILLS, AND ABILITIES

Technical Skills: Understanding of basic networking concepts, operating systems (Windows and Linux), and cybersecurity fundamentals.

Tools and Technologies: Familiarity with SIEM tools, vulnerability scanners, and firewalls.

Analytical Skills: Ability to analyze data and identify patterns indicative of security incidents.

Communication Skills: Strong written and verbal communication skills to report findings and provide recommendations.

Team Collaboration: Ability to work collaboratively with senior security staff and other IT team members.

Attention to Detail: Meticulous in documenting incidents and following security procedures.

MINIMUM QUALIFICATIONS OR STANDARDS REQUIRED TO PERFORM ESSENTIAL JOB FUNCTIONS

Physical Requirements: Must be physically able to operate a van. Must be able to exert up to 50 pounds of force occasionally, and/or up to 25 pounds of force frequently, and/or up to 10 pounds of force constantly to move objects. Physical demand requirements are for Medium Work.

Data Conception: Requires the ability to compare and/or judge the readily observable, functional, structural, or composite characteristics (whether similar to or divergent from obvious standards) of data, people or things.

Interpersonal Communication: Requires the ability of speaking and/or signaling people to convey or exchange information in an effective manner. Includes receiving instructions, assignments and/or directions from superiors, and communicating information and instructions to students and other persons.

Language Ability: Requires the ability to read correspondence, reports, instructions, etc. Requires the ability to prepare correspondence, reports, etc., using proper format. Requires the ability to speak to people with poise, voice control and confidence.

Intelligence: Requires the ability to apply common sense understanding to carry out instructions furnished in written, oral, or diagrammatic form; to deal with problems involving several concrete variables in or from standardized situations.

Verbal Aptitude: Requires the ability to record and deliver information, to explain procedures, to follow oral and written instructions. Must be able to communicate effectively and efficiently in standard English.

Numerical Aptitude: Requires the ability to utilize mathematical formulas; to add and subtract totals.

Form/Spatial Aptitude: Requires the ability to inspect items for proper length, width and shape.

Motor Coordination: Requires the ability to coordinate hands and eyes rapidly and accurately in operating a van.

Manual Dexterity: Requires the ability to handle a variety of items, van equipment, control knobs, switches, etc. Must have minimal levels of eye/hand/foot coordination.

Color Discrimination: Requires the ability to recognize the colors of traffic signals and devices showing standard red, green, and amber.

Interpersonal Temperament: Requires the ability to deal with people beyond giving and receiving instructions. Must be adaptable to performing under stress and when confronted with persons acting under stress.

Physical Communication: Requires the ability to talk and/or hear: (talking: expressing or exchanging ideas by means of spoken words; hearing - perceiving nature of sounds by ear). Requires sufficient hearing ability to distinguish warning sounds made by horns, screeching tires, sirens, grade-crossing alarms or train whistles. Hearing a forced whispered voice in the better ear at a distance of five feet is considered adequate hearing.

.

CYBERSECURITY ANALYST I

DISCLAIMER

This job description outlines the general duties and responsibilities of the position of Cyber Security Analyst I. It is not intended as a comprehensive inventory of all duties, responsibilities, and qualifications required. Employees may be assigned additional tasks as needed.