Dallas County
Community College District

Job Description

Job Title: Cyber Security Analyst **JTC: TTT**

Salary Range: N07 **FLSA: Exempt**

Since 1965, we have served more than 3 million students. Dallas County Community College District (DCCCD) is one of the largest community college systems in the state of Texas, which includes seven independently accredited colleges located around the Dallas/Fort Worth area.

POSITION SUMMARY

Position plays a vital role in keeping DCCCD's proprietary and sensitive information secure. Responsible for monitoring DCCCD's computer networks and cloud infrastructure for security issues and identifying/correcting flaws while recommending specific measures to improve the DCCCD's overall security posture.

REQUIRED KNOWLEDGE, SKILLS AND ABILITIES

Must have working knowledge and understanding of information security law with a strong technical background in information technology and the ability to test networks, computers, web-based applications and other systems to detect exploitable vulnerabilities. Must be able to continually adapt to stay a step ahead of cyber attackers and stay up-to-date on the latest methods attackers are using to infiltrate computer systems and on IT security.

Ability to effectively analyze all relevant cyber security data and other information sources for suspicious network traffic, attack indicators and potential security breaches; produce reports, and assist in coordination efforts during incidents. Requires a high degree of diplomacy, customer service, planning, accountability, problem solving and the ability to work autonomously, independently and as part of a team. Ability to act ethically and independently in case of investigations, while maintaining strict confidentiality and compliant with district policies, local, state and federal laws, rules and regulations.

Ability to partner with diverse internal/external stakeholders and constituents to assist with defining strategy and roadmaps for technology products, service standards, and governance routines that impact the district's security. Partners with leadership across the district to design controls and service alternatives that improve the district defenses against cyber-attacks.

Working knowledge of anti-virus, firewall, security information and event management (SIEM), intrusion detection/prevention systems (IDPS), and other web security technologies. Ability to identify potential impact to customers by analysis of forensic reports and examination of malware to determine associated indicators of compromise. Able to distribute countermeasures to detect and prevent identified threats. Must have ethical hacking skills to expose weak points and identify potential threats so that DCCCD is protected from hackers.

Must have excellent interpersonal skills and be able to provide clear and concise communication effectively via various media including presentations, oral and written communication to be able to interact effectively with diverse, multi-cultural individuals within the DCCCD community network. Must have excellent time management, planning and organizational skills and be able to adapt to changing work environments, work priorities and organizational needs to meet business objectives. Must have excellent customer service skills.

PHYSICAL REQUIREMENTS

Normal physical job functions performed within a standard office environment. Reasonable accommodations may be made to individuals with physical challenges to perform the essential duties and responsibilities.

MINIMUM KNOWLEDGE AND EXPERIENCE

Bachelor's degree or higher in related field plus three (3) to four (4) years of experience supporting the safety and security of a computing environment or other relevant experience. Due to the nature of cyber security, this position may be required to work outside normal business hours and, at times, be on call to respond to security incidents as they occur. The following certifications or progress toward are preferred but not required… Certified Information Systems Security Professional (CISSP), Certified Information Systems Auditor (CISA), Center of Digital Forensics Academic Excellence (CDFAE). Ability to program at a basic level in multiple languages is a plus. Official transcripts required. May require current and valid driver's license if traveling on behalf of DCCCD. ***Will be subject to a criminal background check. Some positions may be subject to a fingerprint check. ***

ESSENTIAL DUTIES AND RESPONSIBILITIES

Responsible for security, analysis and consultation in support of DCCCD's information privacy and cyber security program, information services, and supporting systems. Manages and operates various security applications and tools following strict guidelines and procedures to minimize and respond to cyber security compromises for DCCCD. Protect digital files and information systems against unauthorized access, modification or destruction.

Monitors computer networks and cloud infrastructure for security breaches and other cyber security incidents, investigates threats and vulnerability alerts, determines current impact, and coordinates remediation actions as necessary. Conducts penetration testing towards networks, computers web-based applications and other systems to detect exploitable vulnerabilities. Designs, recommends, and implements new equipment, tools, configurations and procedures to extend the security of the district's information services and supporting systems.

Consults with information privacy and security officers at district and campus levels in proactive response to emerging threats and reactive response to security incidents. Assists technical staff in implementing technology in a secure manner and documents secure configuration standards.

Participate and attends meetings and consults on cyber security issues and concerns. Researches new security technology to determine what will most effectively protect the organization.

Acquires and analyzes computer based forensic information, as necessary, for response to cyber security compromises, potential fraud and violations of district policies and procedures. Writes concise and legally admissible forensic reports on findings. Installs security measures and software to protect systems and information infrastructure, including firewalls and data encryption programs. Coordinates security plans with outside vendors.

Prevents and mitigates the potential impact of cyber-attacks by developing, distributing and sharing countermeasures that may impact networks and information systems. Exercises judgment within broadly defined cyber practices and policies in selecting methods, techniques, and evaluation criterion for obtaining results and increasing productivity. Train employees in security awareness, preparedness and procedures. Regularly communicate with leadership new methods and procedures related to cyber risks. Must complete required DCCCD Professional Development training hours per academic year. Must have excellent communication skills and the ability to interact with diverse internal/external stakeholders and constituents within the DCCCD community network.

Performs other duties as assigned.

The intent of this job description is to provide a representative summary of the major duties and responsibilities performed by incumbents of this job and shall not be construed as a declaration of the total of the specific duties and responsibilities of any particular position. Incumbents may be directed to perform job-related tasks other than those specifically presented in this description. Position requires regular and predictable attendance.