Classification: Computer Information Technology Specialist (CITS) II - Logscan

Title Code: V08005

Pay Range: 33

POSITION SUMMARY: This position provides advanced professional, technical, and consultative position in the support and coordination of computer information technology (IT) services and activities, as related to information security. An employee in this class provides technical security monitoring functions within the Security Audit and Compliance Unit (SACU). An employee will perform analysis and hands on investigation, within a dynamic environment, extending across event monitoring, security intelligence, threat analysis, and usage of advanced threat detection technologies. An employee in this class will also provide information security expertise and guidance in all areas and platforms listed above. Work is generally focused on performing log file management and searches using customized and commercial software. Work includes conducting feasibility and impact studies of technology direction, as well as providing recommendations. Duties may also include implementation of recommendations, project management, and/or provision of technical consultative services. This position will also perform security-related audits, testing, and evaluations of information systems. Work is performed under general supervision; however, the employee is expected to exercise independence in the performance of assigned responsibilities. This position may be required to work after normal business hours, and may be on call.

DESCRIPTION OF DUTIES PERFORMED: (Any one position may not include all of the duties listed nor do the listed examples include all tasks which may be found in positions of this class.)

Monitors log event collection and reviews it against security intelligence and emerging threat information sources, to include: Security Event and Incident Management (SEIM), vendors, researchers, websites, newsfeeds, and other sources.

Performs logscans and log file analysis for Missouri Uniform Law Enforcement System (MULES), email, file servers, web applications, and other system log files.

Performs electronic discovery for legal reviews and sunshine law requests.

Performs video log analysis and retrieval for Patrol security video systems, as needed.

Performs analysis of all threat/vulnerability sources, assessing any impacts to infrastructure and systems, as well as provides an assessment, recommendations, and potential actions correlative to the security threat posture, to include maturing the current vulnerability and scanning/assessment capabilities.

Coordinates responses, triage, and escalation activities for security events affecting information assets.

Identifies and creates use cases within the SIEM tool.

Develops, implements, and maintains an IT security policy for the criminal justice domain.

Leads and conducts ongoing IT audits and/or assessments, in accordance with various regulatory requirements, specifically the current Federal Bureau of Investigation's (FBI) Criminal Justice Information Services (CJIS) Security Policy.

Develops audit processes and procedures, as well as documents test results with recommendations.

Assists in leading the an annual risk assessment of the Patrol and MULES systems.

Collaborates with the IT functional teams, and other stakeholders, to review, analyze, and develop enhanced IT controls from a compliance and security perspective, as well as to ensure action plans are effectively designed and successfully implemented.

Provides guidance and expertise on IT risk management matters, to include infrastructure, security, and industry standards.

Ensures proper policies, procedures, risk mitigation activities, and operating controls are followed.

Performs security testing and evaluations on information systems and products.

Develops communication channels with technology owners, and the business, to evangelize the evolving threat landscape.

Gives structured presentations to different audiences such as business, technical, or management.

Establishes and maintains business relationships with individual contributors as well as management.

Leads efforts in the improvement and development of process/procedure manuals and documentation for the escalation of threat intelligence; advanced persistent threat detection; vulnerability analysis; and incident response handling.

Maintains a continuous process improvement work environment for security monitoring, security configuration standards, and threat analysis, to include recommending and implementing new/improved process in accordance with existing policy, industry standards, and best practices.

Provides policy expertise in computer systems analysis and design; database and/or network administration; systems programming; and/or other computer IT specialties.

Reviews and updates cybersecurity policies; participates in the development of plans for emergencies; prepares and/or conducts cybersecurity awareness and training; reports, investigates, and takes corrective action for security audit findings; as well as administers and oversees security systems such as access control, encryption, anti-virus, firewalls, etc.

Serves as one of the technical experts on the SACU team, as well as provides mentoring to junior staff in complex technical functions and best practices.

Participates in computer systems disaster recovery plan maintenance and implementation, as well as in computer systems management plan development, maintenance, and implementation.

Researches, reviews, recommends, and prepares requests for proposals and/or bid specifications for hardware and/or software purchases.

Designs, writes, maintains, documents, and tests complex computer programs and clearly defined segments of highly complex programs.

Designs procedures for preserving data integrity.

Performs other related work as assigned.

REQUIRED KNOWLEDGE, SKILLS, AND ABILITIES: Thorough knowledge of the general operating principles and capabilities of computer hardware and software.

Thorough knowledge of log files, log file analysis, and reporting

Thorough knowledge of, or ability to learn the CJIS Security Policy.

Through knowledge of, or ability to learn the MULES system as it relates to the technical connectivity and CJIS requirements.

Thorough knowledge of computer security systems and procedures.

Thorough knowledge of computer networking and telecommunications.

Thorough knowledge of the principles of cost benefit analysis.

Thorough knowledge of the principles of project management.

Thorough knowledge of the procurement process.

Thorough knowledge of the information strategic planning process.

Thorough knowledge of the systems management process.

Considerable knowledge of software reference libraries and related utility programs.

Considerable knowledge of computer operating systems.

Considerable knowledge of database management systems.

Working knowledge of, or ability to learn the agency's automated information systems.

Working knowledge of, or ability to learn the agency's functions and their interrelationships.

Working knowledge of the principles of disaster recovery.

Working knowledge of continuing trends and developments in computer hardware and software.

Working knowledge of various computer platforms.

Working knowledge of the principals of information system audits and security testing.

Possess good organizational skills.

Possess research and analysis skills.

Ability to utilize project management tools.

Ability to prepare and interpret computer program documentation.

Ability to prepare and maintain standards, policies, procedures, guidelines and technical manuals.

Ability to troubleshoot and resolve hardware and/or software problems.

Ability to train and assist less experienced personnel.

Ability to create and present materials for training programs.

Ability to operate basic office equipment as detailed in the description of duties.

Ability to handle restricted and confidential information in a professional manner and maintain the information as such.

Ability to communicate in English clearly and concisely, both orally and in writing.

Ability to establish and maintain harmonious working relations with others.

Ability to work with material that may be of a sexual nature relating to criminal activity (e.g., written material, photographs, and/or verbal language, etc.).

Ability to work hours as assigned.

MINIMUM EXPERIENCE AND EDUCATION REQUIRED: (The following represents the minimum qualifications used to accept applicants, provided that equivalent substitution will be permitted in case of deficiencies in either experience or education.)

Possess a bachelor's degree in Information Security, Cybersecurity, Information Assurance, Information systems, Business Administration, Criminal Justice, or related field; AND five years of experience in the areas of information security; cybersecurity; information assurance; or in a business, financial, or academic environment, compiling data, analyzing findings, and writing comprehensive reports.

Preference may be given to those possessing current certification(s) in Information Security or Information Technology and/or work experience and knowledge in all areas of information security, to include: security best practices, standards, legal requirements, privacy policy, networking, servers, end user support, databases, web and application development, and the concepts vital to ensuring confidentiality, integrity and availability of protected data and systems.

NECESSARY SPECIAL REQUIREMENTS: Must be a United States Citizen, or a legal resident of a country participating in the Visa Waiver Program (VWP).

Must possess and maintain a MULES Certification within one year of hire.

FLSA STATUS: Exempt

WORK SCHEDULE: An employee in this position works an eight-hour shift as directed; however, working hours are subject to change at the discretion of the commanding authority.