Classification: Computer Information Technologist (CIT) Trainee - Logscan

Title Code: V08000

Pay Range: 18

POSITION SUMMARY: This is a trainee-level position providing professional, technical, and consultative 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 learn to 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. Work is generally focused on performing log file management and searches using customized and commercial software. Work includes learning to 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 learn to perform security-related audits, testing, and evaluations of information systems. Work is performed under detailed direction and close supervision. 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.)

Learns to monitor 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.

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

Receives direction in performing electronic discovery for legal reviews and sunshine law requests.

Receives direction performing video log analysis and retrieval for Patrol security video systems, as needed.

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

Learns to coordinate responses, triage, and escalation activities for security events affecting information assets.

Learns to identify and create use cases within the SIEM tool.

Receives direction in developing, implementing, and maintaining an IT security policy for the criminal justice domain.

Learns to conduct 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.

Receives direction in developing audit processes and procedures, as well as documenting test results with recommendations.

Learns to assist with an annual risk assessment of the Patrol and MULES systems.

Receives direction in collaborating 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.

Receives direction in ensuring proper policies, procedures, risk mitigation activities, and operating controls are followed.

Learns to perform security testing and evaluations on information systems and products.

Receives direction in developing communication channels with technology owners, and the business, to evangelize the evolving threat landscape.

Receives direction in providing structured presentations to different audiences such as business, technical, or management.

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

Receives direction in leading 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.

Learns to maintain 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.

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

Receives direction in the review and update of 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.

Receives direction in participation of computer systems disaster recovery plan maintenance and implementation, as well as in computer systems management plan development, maintenance, and implementation.

Receives direction in designing, writing, maintaining, documenting, and testing complex computer programs and clearly defined segments of highly complex programs.

Receives direction in designing procedures for preserving data integrity.

Performs other related work as assigned.

REQUIRED KNOWLEDGE, SKILLS, AND ABILITIES: Knowledge of, or ability to learn the general operating principles and capabilities of computer hardware and software.
Knowledge of, or ability to learn the log files, log file analysis, and reporting

Knowledge of, or ability to learn the CJIS Security Policy.

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

Knowledge of, or ability to learn the software reference libraries and related utility programs.

Knowledge of, or ability to learn the computer security systems and procedures.

Knowledge of, or ability to learn the computer networking and telecommunications.

Knowledge of, or ability to learn the computer operating systems.

Knowledge of, or ability to learn the database management systems.

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

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

Knowledge of, or ability to learn the principles of cost benefit analysis.

Knowledge of, or ability to learn the principles of project management.

Knowledge of, or ability to learn the principles of disaster recovery.

Knowledge of, or ability to learn the procurement process.

Knowledge of, or ability to learn the various computer platforms.

Knowledge of, or ability to learn the information strategic planning process.

Knowledge of, or ability to learn the systems management process.

Knowledge of, or ability to learn 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 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.

OR

Successful completion of an Associate Arts program (or at least 60 credit hours) with at least 15 credit hours in in Information Security, Cybersecurity, Information Assurance, Information systems, Business Administration, Criminal Justice, or related field.

OR

Possess a high school diploma or equivalent and four years of experience in the areas of information security; cybersecurity; information assurance; in a business, financial, or academic environment, compiling data, analyzing findings, and writing comprehensive reports; and/or the duties associated with this position.

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: Non-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.