



COMMONWEALTH OF PENNSYLVANIA

TREASURY DEPARTMENT

Job Posting – Information Security Specialist I

Class Title: Information Security Specialist I
Class Code: T1517
Office: Bureau of Information Technology
Pay Range: 08: Starting Salary \$57,741
Apply By Date: 11/04/2020
Work Hours: 8:00am – 4:30pm
Work Location: Finance Building, Harrisburg, PA 17120

THE POSITION

This position performs a broad range of security duties in support of information security. The primary responsibility of this position is the day to day operation and monitoring of security systems and the analysis of security events. This position assists in incident research as well as research and evidence gathering. This position also manages the monitoring and troubleshooting for access governance processes to ensure effectiveness and alignment with requirements for compliance with Treasury's policies. This position will assist in the overall management of the work queue to ensure effective and timely execution of requests. Secondary responsibilities may include coordinating tasks that involve multiple teams to meet one end goal and to assist with other projects related to security.

Work at this level is distinguished from lower level information technology (IT) jobs performing information security duties by the independent performance of security duties in a centralized information security unit and the broad range and scope of security duties performed. Work may include lead work over lower level IT staff performing technical information technology work.

DESCRIPTION OF WORK

- Ensures the identification of required security related issues, and that they are alerted upon by configuring and establishing monitoring, correlation, and alerting solutions.
- Performs incident triage to determine scope, urgency, and potential impact of incidents and reports incidents based on set escalation procedures to relevant parties to ensure immediate actions will be taken.
- Correlates all reported events from various multiple systems and network areas where potential security incident is identified; ensures the situation is handled promptly and effectively by starting the process of security incident response.
- Participates in the investigations being performed by the Information Security team.
- Participates in maintaining a DLP solution to effectively give notice of violations to affected parties, and to reduce incidences of false positives.
- Determines nature of data requiring protection by considering its location to support implementation of the appropriate encryption technologies and ensuring compliance with data privacy best practices and regulations.

The Pennsylvania Treasury Department is proud to be an Equal Opportunity Employer and is committed to strengthening diversity & inclusion within our agency.

- Ensures that all solutions set up for security and monitoring can effectively monitor and report upon security events happening within the environment by assigning security solution agents to devices and systems.
- Makes recommendations for changes to the environment that can help in the removal of vulnerabilities and reduction in the risk of exploitation that may result in potential incidents.
- Creates and manages service accounts and security groups in Active Directory as well as, resource accounts and distribution groups for Microsoft Exchange.
- Assists in the review of physical controls to ensure sufficient protection of organization facilities and assets.
- Participates in ensuring team processes and documentation are effectively documented and maintained.
- Assists in the identification and documentation of exceptions to security policies and procedures to ensure proper escalation and follow-up.
- Recommends and executes ideas to improve processes based on lessons learned over time in performing assigned duties.
- Performs as an escalation point for all potential incidents relating to security.
- Provides support by carrying out other enterprise security and duties as assigned by management.

REQUIRED KNOWLEDGE, SKILLS AND ABILITIES

- Knowledge of server and workstation platforms.
- Knowledge of industry standards and best practices of information security.
- Experience with Active Directory user and group administration.
- Some working experience with SIEM solutions.
- Knowledge and understanding of the various ways attacks are carried out against a system or network and how to effectively detect them.
- Possess advanced analytical skills and strong ability to maintain calmness and being diplomatic under highly stressful situations.
- Strong multitasking skills to be able to effectively manage multiple activities, including cross-team dependent activities simultaneously.
- Strong ability to work effectively in collaboration with other members of a team or/and other professionals with minimal supervision.
- Strong ability to quickly learn new processes and technologies, and to adapt to changes in sequences and timelines.
- Strong communication skills, including written and verbal, and ability to work off hours when needed.

MINIMUM EXPERIENCE AND TRAINING

- One year of Information Security experience.
- Possession of professional cybersecurity certification such as, Security+, CEH, CISSP, GIAC, etc., is preferred.

The Pennsylvania Treasury Department is proud to be an Equal Opportunity Employer and is committed to strengthening diversity & inclusion within our agency.