

Information Security Analyst - Job Description

Description

This position reports to the Information Security and Privacy Office Program Director, Division of Toll Operations - Florida's Turnpike Enterprise. The Information Security Analyst position is a core member of the Information Security and Privacy Office (ISPO).

The Information Security Analyst's main role is to support the threat and vulnerability management program at the Division of Toll Operations. This position is heavily focused on security monitoring in support of this program. The incumbent is expected to become familiar with security operational processes and ensure they are performed efficiently and securely. Furthermore, this position will be responsible for using security monitoring tools to check the integrity and security of the computing environment and produce reports on a regular basis.

Skills and Experience Weighting

A = Candidate must have these attributes
B = Management strongly desires that the candidate have these attributes
C = Management desires the candidate to have these attributes

Skills Needed

B – Working level knowledge of File Integrity Monitoring tools like Tripwire
B – Working level knowledge using Log Management Tools like QRadar
B – Working level knowledge using Security Information and Event Management Tools like QRadar
B – Experience with process lifecycle of the creation, management and compliance of security policies, procedures, standards and guidelines
B – Experience with the processes of identifying appropriate controls to meet compliance to the security policies and regulations
B- Experience with Threat and Vulnerability Management Tools
B- Experience with the process of remediation of vulnerabilities identified by the Threat and Vulnerability Management Tools
C – Familiar with incident response procedures and risk assessments
B – Familiar with Payment Card Industry (PCI) security requirements
C – Familiarity with ISO/IEC 27000 series of security standards
A – Excellent threat and vulnerability analysis skills
A – Experience producing threat and compliance reports for a wide variety of audiences (technical and non-technical)
A - Excellent communication and analytical skills
A - Must work well with others as part of larger team and be able to collaborate on cross functional teams
A - Must be available and willing to work extended and/or alternative hours as needed for issue resolutions, roll-outs, system upgrades, etc.
A- Able to work independently toward goals set at a higher level
A- Good working knowledge of Microsoft Word, Excel, Outlook, PowerPoint, Visio and Project

**Knowledge and
Experience
Needed**

**A - 3 years of Information Security experience or related field
B – 2 years of experience in the areas of compliance, auditing, risk assessment, and vulnerability mitigation and remediation.
B - 2 year of experience of development and management of Information Security Policy**

Responsibilities

- 1. Support the Policy Management Program**
- 2. Support the Threat and Vulnerability Management Program**
- 3. Support of Incident Response Process, Risk Assessments**

**Measures of
Performance**

No metrics yet defined

**Education and
certifications**

**A - Bachelor's degree in Computer Science / Computer Information Systems or related field
B – CISSP, CISM, CISA certifications
C – CoBit and other security related certifications**