Cyber Security Analyst

Job Summary

The Cyber Security Analyst serves as the security subject matter expert by developing and interpreting security policies and procedures to mitigate security risks.

Job level: Individual Contributor

Competencies

Cyber Security (Level 3)

Developing and implementing policies, tools, and safeguards to protect the organization's network, systems, applications, and data from attack, damage, and unauthorized access.

Applies the competency in the full range of typical situations, requiring guidance in only the most complex or new situations.

- Performs complete threat and risk and privacy impact assessments on new and upgraded systems.
- Provides guidance to others on cyber security policies and best practices, including delivering training and awareness programs to non-technical staff.
- Reviews existing controls and countermeasures to assess vulnerabilities and risks.
- Investigates security incidents, recommending improvements in security controls.
- Produces regular status reports on cyber security compliance.
- Identifies metrics and tools used to measure compliance with the cyber security strategy.

Telecommunications Network (Level 3)

Implementing the methods, practices and policies governing the design, analysis, development, management and use of the hardware and software used to transfer information such as data, voice, images and video.

Applies the competency in the full range of typical situations, requiring guidance in only the most complex or new situations.

- Explains how data communications integrate with other environments such as mainframe, distributed, e-commerce, firewalls and external networks, at a component level.
- Translates multiple client network connectivity requirements and limitations into technical specifications.
- Designs building environments using existing standards.
- Resolves typical hardware and software problems such as connectivity and congestion.
- Conducts certification testing.
- Implements new standards, or changes to existing standards, within the technical environment.
- Secures and manages access to systems and environment.

Infrastructure (Level 3)

Supporting the enterprise computing infrastructure (e.g., enterprise servers, client server, storage devices and systems, hardware and software) in the provision, management, storage, operation, scheduling, support and maintenance of the infrastructure.

Applies the competency in the full range of typical situations, requiring guidance in only the most complex or new situations.

- Describes how a specific infrastructure component integrates with other enterprise elements.
- Uses performance data collection tools and techniques to mitigate down-time and improve performance.
- Manages a specific infrastructure component, including hardware/software/firmware installation, patching, and updating.
- Solves routine problems, documenting new problems and their solution for future reference.
- Uses appropriate diagnostic tools to solve complex problems.
- Executes standards without supervision, suggesting modifications to these standards.

Fostering Communication (Level 2)

Listening and communicating openly, honestly, and respectfully with different audiences, promoting dialogue and building consensus.

Fosters two-way communication

- Recalls others' main points, taking them into account in own communication.
- Checks own understanding of others' communication (e.g., paraphrases, asks questions).
- Elicits comments or feedback on what has been said.
- Maintains continuous, open and consistent communication with others.

Collaborating with Others (Level 2)

Working together with others in a cooperative and supportive manner to achieve shared goals.

Proactively assists and involves others

- Initiates collaboration with others.
- Assumes additional responsibilities to facilitate the achievement of team goals.
- Seeks input from others on matters that affect them.
- Anticipates when others might require assistance, providing it before they ask for it.

Attention to Detail (Level 3)

Working in a conscientious, consistent and thorough manner.

Monitors and verifies the work of others for accuracy and completeness

- Identifies multiple sources/approaches of information to ensure that details are addressed.
- Reviews the work of others for accuracy and thoroughness.
- Follows up to ensure tasks are completed and commitments are met by others.
- Verifies that work has been done according to procedures and standards.

Resilience (Level 3)

Staying energized, productive and focused in the face of challenges, ambiguity, change or strenuous demands, creating a supportive environment that helps others become more resilient and productive.

Adapts to ongoing, or regular strenuous work demands

- Remains focused and productive in the face of difficult or demanding situations such as pervasive ambiguity, frequent change, or high workloads.
- Describes disruptions as challenges that can be overcome rather than threats.
- Adjusts personal coping mechanisms to deal with disruptions.

Project Risk Management (Level 2)

Identifying, assessing, prioritizing, documenting and managing risk and its impact.

Applies the competency in common situations that present limited difficulties, working with a moderate level of guidance.

- Identifies risks within own project.
- Completes risk tracking tools such as risk register and risk breakdown structure.
- Evaluates risk consequences, probability and impact.
- Develops solutions to address barriers in project and monitors results.
- Recommends corrective action regarding risk for a small project or component of a large project.
- Communicates the risks associated with budget, schedules and scope to stakeholders and project team members.
- Updates risk response plan when risk is realized, avoided, transferred or mitigated.

Responsibilities

Cyber Security

- Participate in security compliance efforts
- Observe strict security protocols associated with all security management practices
- Recommend additional security solutions or process enhancements to existing security solutions to improve overall enterprise security
- Provide security awareness training to the organization
- Assists with analysis to detect and respond to IT security incidents
- Develop and interpret security policies and procedures
- Assist other teams as a security liaison, providing security advisory services, ensuring security risks are identified
- Define and implement network solutions to mitigate security risks
- Perform advanced hands on analysis of security incidents
- Monitor all in place security solutions for efficient and appropriate operations

Knowledge Areas

- Appsider (Intermediate)
- Bash (Intermediate)
- Encryption Technologies (Intermediate)
- Firewalls (Intermediate)
- Git (Intermediate)
- Identity Management (Intermediate)
- Metaspolit Project (Intermediate)
- National Institute of Standards and Technology (NIST) Standards (Intermediate)
- Penetration Testing Principles (Intermediate)
- Rapid7 Nexpose (Intermediate)
- Remote Access Trojans (Intermediate)
- Server Hardening (Intermediate)
- Version Control Systems (Intermediate)