

Security Analyst (Contingent)

Description

The Security Engineer/Analyst employs experience as a seasoned professional and uses extensive knowledge of industry best practices, policies and good judgment in selecting methods and techniques for designing, defining, developing, testing, purchasing, implementing, and analyzing of technical products and systems of diverse scope. This position performs engineering design evaluations and applies extensive analytical skills to recommend performance enhancements. The Security Engineer/Analyst proposes standards that will be followed by engineering, and operations groups. This position will design subsystems and integrate systems for a range of products. The Security Engineer/Analyst interacts with business partners and providers who are dependent on Engineering.

Responsibilities include:

Implementation of security solutions (risk management, intrusion detection, antivirus, vulnerability scanning, event correlation, etc.).

Helping establish security standards, requirements and processes.

Monitoring and responding to security events.

Helping ensure technical solutions leverage industry best practices.

Conducting web application security testing, network penetration testing, and risk assessments.

Staying current on technologies, technology trends and directions, and best practices.

Evaluation of potential technologies for use within the enterprise.

Qualifications

Requires a Bachelor's degree in computer science or related field, or equivalent work experience

Five years of information technology experience with two years in an information security-related role

CISSP, GIAC and/or Cisco certification preferred

Must be able to adapt and learn new concepts and new products as well as possessing strong troubleshooting skills

Demonstrated ability to develop, refine, and follow repeatable processes

Experience implementing Open Web Application Security Project (OWASP) tools and methodologies

Working knowledge of securing and administering network devices and operating systems

Experience in risk management, auditing, incident handling, computer forensics, intrusion detection systems, firewalls, antivirus, syslog, etc.

Demonstrated understanding of telecommunications, network and internet security

Knowledge of UNIX, Windows, TCP/IP, VPN, e-mail and DNS standards

Knowledge of ISO 27000, National Institute of Standards and Technology, and Center for Internet Security

Advanced knowledge and experience in firewall administration and security principles and network architectures

<http://www.slc-staffing.com>