

JD Number: 745

Title

data security analyst

Description

Our client is looking for a Security Analyst for a permanent opportunity in Folsom, CA. SUMMARY The Security Analyst II position is responsible for managing and maintaining the information security systems to ensure member data confidentiality, integrity, availability, and compliance with established security policies, procedures and standards. Monitors, manages and analyzes malicious activities on a daily basis to ensure the security infrastructure is free from malicious code and/or misuse Assists in the development and maintenance of Information Technology Security Program, to include: policies, standards, procedures, and security awareness training. The Security Analyst II, at times works under the direction of the Senior Security Analyst. ESSENTIAL DUTIES AND RESPONSIBILITIES Manage, monitor, analyze and maintain the security infrastructure (50%) Maintain IT Security helpdesk ticketing queue and track issues through resolution Manage network firewalls, intrusion prevention systems (IPS), data loss prevention (DLP) systems, and antivirus suite to detect and prevent malicious activity Conduct vulnerability scanning and develop prioritized remediation plans Assist in incident response activities Actively promote system security awareness programs internally II. Audit and Compliance 25% Identify information security risks and recommend security controls to reduce and/or mitigate those risks. Audit security information and event management logs for anomalies and unauthorized activity Audit systems configuration and access to ensure compliance with regulatory guidance and security policies Assist internal and external auditors as required Work with IT teams and vendors regarding disaster recovery and business continuity Documentation 25% Produce project plan and design documentation, and business justification documents. Follow Change Management processes and procedures Assists in development of information security standards, policies, and procedures Assist in development and maintenance for information security awareness training Evaluate proposed technologies additions and/or changes and make recommendations Completes other duties as assigned. QUALIFICATIONS To perform this job successfully, an individual must be able to perform each essential duty satisfactorily. The

requirements listed below are representative of the knowledge, skill, and/or ability required. Reasonable accommodations may be made to enable individuals with disabilities to perform the essential functions.

EDUCATION AND/OR EXPERIENCE Four year college or university program degree; or 3 to 5 years related experience and/or training; or equivalent combination of education and experience.

CERTIFICATES, LICENSES, REGISTRATIONS Candidate must hold one or more of the following industry certifications: CompTIA Security+GIAC Information Security CertificationCertified Information Systems Security Professional (CISSP)

TECHNICAL SKILLS Strong Knowledge and experience with:IDS/IPS TechnologiesFirewall management and maintenanceAnti-Virus / Anti-Malware softwareNetwork protocols (BGP, OSPF etc.)SIEM/LEM Technology Data Loss Prevention hardware and software technologiesPatch Management hardware/software Data ForensicsVulnerability scanning and patchingPenetration testing techniques and tools

OTHER SKILLS AND ABILITIES Must be a self-starter, able to work without constant supervisionStrong written and verbal communication skillsStrong investigation, remediation, and reporting intuitionDemonstrated ability to work in a team environment

Skills

Full Time