CSBS SINCE 1902

CONFERENCE OF STATE BANK SUPERVISORS

Conference of State Bank Supervisors (CSBS)
Job Description

Job Title	Senior Information Security Analyst
Reports To	Chief Information Security Officer
Department	IT
FLSA Status	Exempt
Date	August 2017
Position Number	209
Grade	8

Job Summary

The Senior Information Security Analyst is responsible for maintaining the security and integrity of CSBS and SRR data. The security analyst has to have knowledge of every aspect of information security within the company. Their main job is to analyze the security measures of a company and to support the planning, deployment, implementation, operations and maintenance of security tools, processes, procedures. The Senior Information Security Analyst plays a critical role in maintaining and administering the security of CSBS's diverse IT environment, that includes desktop services, on-site and Cloud (IaaS/PaaS) hosted solutions, Software-as-a-Service (SaaS) solutions and on-site hosted applications and mobile solutions. They are responsible for implementing any training required including instructing staff on proper security measures both in the office and online. The security analyst must work with business administrators as well as IT professionals in communicating flaws in security systems. They recommend changes that will improve every aspect of company security. The security analyst is also responsible for creating documentation to help the company in case there are any breaches.

Essential Functions

To perform this job successfully, an individual must be able to perform each essential duty and responsibility satisfactorily. Reasonable accommodations may be made to enable individual with disabilities to perform the essential functions. Other duties may be assigned to meet business needs.

- The Senior Information Security Analyst should be familiar with the NIST Cyber Security Framework.
- The Senior Information Security Analyst is responsible for protecting all sensitive information within the company. Experience planning, deploying, configuring and implementing technologies such as Disk Encryption, Data Masking, Data Obfuscation, etc.
- Responsible for insuring all networks have adequate security to prevent unauthorized access. Experience in configuring firewalls, access control list (ACLs), Network IDS/IP, Host IDS/IPS, DLP, etc.
- Produce compliance reports using the tools that would satisfy FISMA, CJIS and PCI compliance requirements.
- Provide technical guidance in the outsourced MSSP operation of firewalls, intrusion detection systems, enterprise anti-virus and log monitoring tools (SIEM).
- In conjunction with the outsourced MSSP, perform investigation of network intrusions and other cyber security breaches to determine the cause and extent of the breach.

- Develop reports to share with administrators about the efficiency of security policies and recommend any changes. Assist in developing and maintaining security program metrics to measure program effectiveness.
- They must plan and document all security information in the company including physical and network security.

Additional Responsibilities:

- Monitor industry trends for changes in physical and cyber security challenges and implement planning, policy and procedure changes in response.
- Contribute to industry and government forums that develop industry guidance and regulations regarding security practices.

Minimum Qualifications

To perform this job successfully, an individual should possess the knowledge, skills, and abilities listed and meet the amount of education, training and/or work experience required.

Education & Certification

- Bachelor's degree or equivalent experience in an information technology or information security discipline.
- Certifications: CISSP, GIAC, CISA, CISM, SANS or equivalent certification required

Experience

- 7+ years of experience in information security with Expertise using and managing firewalls, Network & Host IDS/IPS systems, Network & Host DLP, VPN, web application firewalls (WAFs), OS hardening, multi-factor authentication, encryption key management, database security controls, and network segmentation. Experience with security on Windows and RHEL Linux systems preferred.

Additional Experience:

- Experience with security controls for an Infrastructure as a Service (IaaS), Platform as a Service (PaaS) and Software as a Service (SaaS) cloud paradigms.

Knowledge, Skills and Abilities

- Experience working with leading firewall (such as Juniper ScreenOS Firewalls, Cisco ASA, Sophos UTM**),** intrusion detection technologies (SourceFire/Snort, Sophos UTM).
- Experience working with log monitoring and SEIM tools (McAfee Nitro, Splunk) and file integrity monitoring tools.
- Experience working with data loss prevention technologies and tools.
- Knowledge of securing servers (Linux and Windows); desktop systems (Win10) and networks (Cisco, Juniper, Netscreen).
- Experience applying security to virtual platforms.
- Knowledge of mobile security and MDM.
- Cloud security concepts and protection. Experience with AWS Security and IDM is a huge plus.
- Knowledge of common application vulnerabilities, current threat vectors and mitigations.
- Participate in the enterprise Incident Response Plan and lead incident response activities.

- Ability to work in a team environment. Effective working with matrix teams across organizational structure.
- Ability to work with external service providers.
- Ability to work calmly during stressful circumstances.
- Strong interpersonal and communication skills.
- Ability to work in fast paced environment managing multiple tasks driven by multiple deadlines.
- Must be dependable due to operational nature of work. Occasional, but infrequent off-hours work may be needed to respond to critical operational issues.

Additional

- Must be able to obtain or currently possess a U.S. Government clearance at the Public Trust Moderate (MBI) level or higher
- Must be a United States Citizen or a Legal Permanent Resident (LPR) with at least three (3) years of consecutive residence in the United States as indicated on the United States Citizenship and Immigration services (USCIS) LPR issued card

Working Conditions

- General office
- Some Travel required

This job description should not be construed to imply that these requirements are the only standards for the position. Incumbents will follow any other instructions and perform any other related duties as may be required. CSBS has the right to revise this job description at any time. CSBS is an "at will" employer and as such, neither this job description nor your signature constitutes any form of contractual arrangement between you and CSBS.

Employee's Signature:	Date:
Manager's Signature:	Date: