Employee Job Description

stewart®

Senior Security Engineer

Employee Information

Department:	**IT**	Date:	**20/10/2016**
Job Category:	**First/Mid-Level Officials and Managers**	Job Title:	**Senior Security Engineer**
# Hrs. Per Week:	**40**	Reports to:	**IT Manager**
Work Days:	**Monday - Friday**	Exempt/Non-Exempt:	**Non-Exempt**
Employment Status:	**Regular Full-Time**		
Work Hours:	**40 Weekly - 9 daily**		

Job Summary

The Senior Information Security Engineer provides technical support to the enterprise as the principal technical expert on the company's cyber security tools and cyber defense technologies. This individual will track escalated incidents for end-user support and provide resolution and root cause analyses for issues that may be of moderate-to-high complexity to closure. He or she will work with the various teams to maintain up-to-date baselines for the secure configuration and operations of all in-place devices, security tools, workstations, servers, and network devices, etc. He or she will conduct analysis of security vulnerabilities and proactively monitor remediation and/or mitigation. This individual may be called upon to assist with the deployment, integration and initial configuration of new security solutions or enhancements to existing security solutions; including network and systems to improve overall security.

The Senior Information Security Engineer will work either onsite at the company's office in San José, or remotely with hiring manager approval. A candidate for this position must be a HS graduate eligible to work full-time in Costa Rica and must be able to pass a personal background check of past employment and criminal history.

Essential Job Functions

Position requires financial responsibility: □ Yes ☒ No

An ideal candidate for this position will possess the following attributes and qualifications:

- Strong background in the principles, theories, techniques, practices, and policies and procedures of information security and technical security safeguards
- Extensive knowledge and practical work experience in implementing the Center for Internet Security (CIS) Critical Security Controls in a corporate IT environment
- Has recent experience working with the following technologies:
  - McAfee E-Policy Orchestrator and Enterprise Endpoint Protection
  - McAfee Web Gateway
  - Proofpoint email security
  - Rapid7 Nexpose
  - Splunk Enterprise
- Seeks ongoing improvements to the organization's information security processes and procedures.
- Prioritizes daily tasks to ensure that emerging, urgent issues are resolved without losing sight of longer-term projects.
- Sets standards, timelines, priorities and approaches to help team complete and deliver assignments on time.
- Takes advantage of available resources to complete work efficiently; coordinates with internal and external partners.
- Allocates appropriate amounts of time for completing one's own and others' work; develops timelines and milestones.
- Demonstrates effective techniques in holding meetings, planning time, setting priorities, setting timelines and deadlines, and making effective use of time.

- Performs independently; informs managers or senior leaders of projects' progress and issues encountered; recommends solution.
- Oversees project completion of less experienced team members; provides guidance to senior level team members on highly complex assignments or projects with a major impact.
- Thorough understanding of the concepts, theories, and practices of enterprise IT
- Excellent communication, interpersonal and presentation skills
- Demonstrated analytical and problem-solving skills
- Evaluates risk, assesses controls, and identifies improvements to mitigate risk.
- Ability to mentor, guide and coach

Job Specifications

- • Proven knowledge and practical application of network security, firewalls, access and perimeter control, vulnerability Computer Science degree or equivalent
- Proven experience in design and configuration of network security devices
- Deep understanding of different threats, how they propagate through the network and how to configure network devices to protect against them
- Ability to work on multiple projects, sometimes under pressure
- Ability to adapt within a small, highly diversified team is a must. Self-starter who can work independently with minimum supervision
- Experience working in a complex, multi-tenant environment in insurance or financial sector is HIGHLY DESIRABLE
- "Big Data" analysis experience is HIGHLY DESIRABLE (ability to understand, process and analyze raw data)
- Flexible hours, possible after hours and weekend work may be required

Preferred Skills:

- 7+ years of experience in supporting networking infrastructure in highly available, high transaction volume and high security production operations
- 7+ years of networking experience. Deep understanding of network topologies, protocols and devices. Experience configuring and supporting Cisco ASA, Catalyst and Nexus switches, and routers. Solid understanding of network segregation and traffic analysis, VLAN, NetFlow, QoS
- 7+ years of network logs monitoring and log analysis for security threats.
- Deep understanding of security events, ability to correlate the events to attack vectors
- Deep understanding of network topologies and security
- Understanding of securing Web Applications
- Ability to document environment, create diagrams, create processes and procedures
- Excellent analytical and troubleshooting skills
- Experience with configuring, managing and tuning IDS/IPS systems is a PLUS
- Experience with security technologies that are closely related to the networking (IDS/IPS, NAC, WAF) is a plus
- LAN and WAN optimization technologies
- Networking and infrastructure monitoring tools
- Packet capturing, analysis and troubleshooting
- Netflow and other analytics tools
- SIEM
- Load balancers
- Threat Analytics
- Penetration testing

Training

Minimum training required per year as assigned by the company

Physical Demands

This job requires the employee to occasionally stand; walk; sit; use hands; climb stairs; balance; stoop; kneel; read; talk or hear. The employee must occasionally lift and/or move up to 25 pounds. Specific vision abilities include close vision and the ability to adjust focus. Reasonable accommodations may be made to enable individuals with disabilities to perform the essential functions.

Work Environment

Work is primarily light; exerting up to 20 pounds of force occasionally and/or 10 pounds of force frequently or constantly to lift, carry, push, pull or otherwise move objects. The noise level in the work environment is moderate.