California's Valued Trust

JOB DESCRIPTION

Position: **Senior Systems Security Analyst**

Reports To: Information Technology Manager

Status: Full Time

Classification: Exempt

Position Summary

Operates under the general direction and supervision of the Information Technology Manager. Position requires professional experience in technical and operational security standards and controls. Position requires a GIAC, OSCP, or CISSP certification. Demonstrates excellence in technical skills and technical knowledge required to perform high level security analysis, maintenance, and incident response.

Essential Duties:

- Responsible for security and security related maintenance, of all systems infrastructure in including:
  - Network Systems(switches, firewall, wireless, etc.)
  - Virtual servers and virtual infrastructure
  - Host systems hardware
  - Hosted services security and maintenance
  - Server operating systems, data storage, and databases
  - Secure email systems
  - All security related applications and tools
  - Threat management system
  - Mobile device security
- Maintain all security and systems documentation
- Responsible for disaster recovery and business continuity maintenance and testing
- Monitors and documents system configuration baselines and activities
- Maintains documentation required for assigned regulatory control standards

- Provides security training for employees and consultants
- Provides scheduled penetration testing and remediation efforts
- Performs scheduled vulnerability scans and remediation coordination
- Review and coordinate secure application development practices and coding standards
- Performs other work as assigned.

Minimum Qualifications

Education and Certification:

- High school diploma or equivalent
- Bachelor's degree or equivalent work experience in field
- GIAC GSEC certification. GSE, CISSP, or OSCP certification preferred

Experience, Skills & Abilities:

- Highly effective communications skills, both oral and written, will be required and will be a major component in the selection of the successful candidate.
- Work experience in network security related position requiring identification and remediation of a wide breadth of vulnerabilities
- System administration experience with Microsoft and Linux, desktop and server environments
- Administration of server virtualization environment
- Administration of SQL databases
- Virtual host hardware maintenance and administration, including network attached storage and fiber channel switching.
- Use multiple information gathering techniques to identify and enumerate targets running various operating systems and services.
- Write basic scripts and tools to aid in the penetration testing process.
- Analyze, correct, modify, cross-compile, and port public exploit code.
- Identify and remediate both remote and client side attacks.
- Identify XSS, SQL injection, and file inclusion vulnerabilities in web applications.
- Identify potential techniques to bypass firewalls.
- Demonstrate creative problem solving and lateral thinking
- Management, deployment, and configuration of unified threat management system
- Wireshark and other vulnerability/threat detection tools

Miscellaneous: Requires flexible schedule to address system administrative needs and maintain an exemplary security posture while providing low user disruption.

Confidentiality: Requires adherence to established policies on confidentiality of records and other information available through employment with the Trust.