CalSAWS Job Description

SECURITY ANALYST II

Salary Determined by Employer
RGS Salary Range:
$8,560.62- $11,851.88 Monthly

JOB DESCRIPTION

The Security Analyst II works within the Technical and Operations team to protect critical assets and personally identifying data through technology controls to prevent intrusion as well as monitoring, research, assessment, and analysis on notable security events. This includes developing, implementing, and monitoring systems security standards, best practices and protocols.

RESPONSIBILITIES

- Contributing to design, development and/or review of work products and deliverables including:
    - Application Architecture Designs;
    - Technical Infrastructure Designs;
    - Network Infrastructure Designs;
    - Environment, server and workstation security;
    - Identity and access management;
    - System Risk Assessments,
    - CalSAWS System Operations and Support Plan (SOSP) Review Results,
    - Business Continuity Planning (BCP)
    - Disaster Recovery Planning (DRP)
- Coordinating and supporting IT project security audits;
- Analyzing security incidents related to suspected intrusion related events and ensuring incident reporting processes are followed;
- Ensuring that the enterprise system security is maintained via upgrades, patches and security updates;
- Compiling and validating security-related statistical data for management review;
- Documenting technical security processes and procedures;
- Assisting in the risk and issue identification, resolution, escalation and tracking;
- Maintaining confidential information in accordance with legal standards and regulations.
- Assisting with development of compliance strategies for IT security programs;
- Assessing risks of non-compliance with IT security policies, procedures, standards and guidelines based on state and federal regulations and best practices, and reporting findings to appropriate management.

DESIRABLE SKILLS AND CAPABILITIES

Candidates of this position should have applicable experience, skills, and capabilities to perform the following functions and activities:

- Have a broad base of technical experience in at least four (4) of the following areas:
    - Network Security Management;
    - Application Security Management;
    - Identity and Access Management;
    - Incident Response Management;

  - Security Policy and Compliance Management;
  - Server and Workstation Security Management;
  - Cloud Infrastructure Security Management;
- Working knowledge of IT security policies as it relates to state and federal policies, standards, procedures and guidelines;
- Strong analytical and problem-solving skills; and
- Strong organizational and leadership abilities.

QUALIFICATIONS AND REQUIREMENTS:

MINIMUM REQUIREMENTS:

TRAINING AND EXPERIENCE:

A bachelor's degree in computer science or a related discipline and three (3) years of recent, highly responsible experience in supporting the security of multiple platforms, operating systems, software, and network protocols in a large information technology organization

-OR-

Two (2) years of experience administering an IT security program at the level of a Departmental Information Security Officer I

-OR-

Five (5) years of recent, progressively responsible experience in implementing information systems or managing/assisting in the management of an information technology organization, three (3) years of which must have been leading an IT-related security and/or privacy program on a full-time basis.

IDENTIFICATION:

A valid California Class C Driver License or the ability to utilize an alternative method of transportation when needed to carry out job-related essential functions.

PHYSICAL CLASS:

2-Light.

OTHER REQUIREMENTS:

N/A

SPECIALTY REQUIREMENTS:

Specialized examinations may include one or more of the following:

*Specialty / *Add*

Application Security management (ASM): Experience in application development using standard IT systems development methodology and techniques for resolving business problems. Includes systems design, database management, development of online data entry and data inquiry capabilities, and defining techniques; communications, network analysis, design, planning and performance tuning.

Identity and Access Management (IAM): Experience assisting with defining, testing, and implementing IT user provisioning and identity management technologies. Includes developing IAM policies, standards, and

procedures; identifying appropriate access control techniques; analyzing and selecting IAM solutions; and familiarity with security and system development life cycles (SDLC) processes.

Incident Response Management (IRM): Experience in an IT organization providing technical assistance in computer incident response for potential or actual information-security breaches or attacks. Includes detecting, analyzing, responding to, and reporting information security incidents; and familiarity with the chain-of-custody process.

Network Security Management (NSM): Experience in IT network planning, design, and analysis. Includes assisting in implementing security tools and controls such as intrusion detection/prevention systems, sniffers, and firewalls.

Physical / Environmental Security (PES): Experience assisting with managing physical and environmental IT security methodologies to prohibit unauthorized physical access and prevent damage to IT resources. Includes physical and environmental security planning, design, and analysis.

Policy and Compliance Management (PCM): Experience assisting with developing and implementing IT security policies and standards. Includes assisting in monitoring for compliance.

Risk Assessment Management (RAM): Experience performing IT security risk assessments. Includes assisting in developing and implementing business continuity and disaster recovery plans and in developing risk assessment reports of findings and recommendations for remediation.

Security Awareness Training (SAT): Experience assisting in developing, implementing, and evaluating IT security awareness training programs and related materials. Includes assisting in reporting of training compliance.

Server Security Management (SSM): Experience in IT server (e.g., email, web, application, and database) security management comprised of implementing upgrades, patches, and updates to operating systems, software applications, and security protection software. Includes configuring server environment to protect the integrity of the system, for example by limiting user rights, disabling unnecessary services, and establishing group policies where applicable.

Workstation Security Management (WSM): Experience managing the security of workstation (e.g., desktops, laptops and tablets) and portable devices (e.g., thumb drives and personal digital assistants). Includes implementing upgrades, patches, and updates to operating systems, software applications, and security protection software; establishing group policies and user rights; and disabling unnecessary services where applicable.