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 leads the Identity and Access Management team within the Security 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

- Leading the Identity and Access Management (IAM) team, supervising one or more Security Operations Analysts.
- Contributing to design, development and/or review of work products and deliverables including:
    - Application Architecture Designs
    - Technical Infrastructure Designs
    - Identity and Access Management Designs
    - Cloud Architecture and Service Designs
    - System Risk Assessments
    - CalSAWS System Operations and Support Plan (SOSP) Review Results
    - Business Continuity Planning (BCP)
    - Disaster Recovery Planning (DRP)
- Designing, building, and supporting AWS account and service architectures, including key responsibilities for Identity and Access Management.
- Design and govern multi-account AWS environments using AWS Organizations, Organizational Units, and Service Control Policies to enforce least privilege and security guardrails at scale.
- Define and manage IAM roles for cross-account access, ensuring secure delegation through tightly scoped IAM trust policies and standardized role assumptions.
- Lead security best practices with identity and access management strategies, implementing role-based access controls (RBAC) and attribute-based access controls (ABAC).
- Partner with platform and application teams to integrate IAM roles into CI/CD pipelines, workloads, and AWS services using temporary credentials and least-privileged access models.
- Assisting security incidents related to suspected intrusion related events;
- Compiling and validating security-related metric data for management review;
- Documenting technical security processes and procedures;
- Assisting in security 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.
- Other duties as assigned by the Security Operations Manager.

DESIRABLE SKILLS AND CAPABILITIES

Ideal candidates for this position should have applicable experience, skills, and capabilities to perform the following functions and activities:

- Have a broad base of technical experience, with specific expertise in the following areas:
  - Identity and Access Management
  - Cloud Infrastructure Security Management
- Prior experience designing and implementing access control models
- Experience with cloud services, including supporting requirements gathering, design, and implementation of enterprise scale cloud architectures.
- Strong analytical and problem-solving skills; and
- Strong organizational and leadership abilities.
- Any of the following certifications:
  - AWS Certified Security – Specialty
  - AWS Certified CloudOps Engineer – Associate
  - Google Cloud Engineer
  - Google Professional Cloud Security Engineer
  - Azure Identity and Access Administrator Associate
  - Azure Administrator Associate
  - Azure Security Engineer Associate

QUALIFICATIONS AND REQUIREMENTS:

MINIMUM REQUIREMENTS:

TRAINING AND EXPERIENCE:

A bachelor's degree in computer science or 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:

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.