CalSAWS Job Description

SECURITY ANALYST III

Security and Operations Team

Salary Determined by Employer

RGS Salary Range:

$8,731 - $12,088 Monthly

JOB DESCRIPTION

The Security Analyst III is responsible for leading a team to ensure the operational delivery of critical security services that provide protection for the CalSAWS services, data, and information assets that serve all 58 counties in California. Reporting directly to the Security and Operations Manager, this position works closely with contracted security teams, third party vendors, and other CalSAWS Consortium staff. This role requires a combination of excellent communication skills and broad technical subject matter expertise across security and related technical disciplines. Primary areas of responsibility include security incident response, vulnerability management, and software development security.

RESPONSIBILITIES

- Provide leadership and participate in the operation and oversight of the security incident response process, including preparing for incidents, conducting incident response activities, and identifying lessons learned. Owns the overall security incident response process.
- Oversee the process for identification, triage, and remediation of vulnerabilities within CalSAWS infrastructure across all systems. Provides approval and leadership in the vulnerability management process.
- Lead the Security Operations team’s review and approval of contract vendors’ application security testing and defect resolution processes. Acts as an approver and subject matter expert within this process.
- Reviews and approves technical and system change requests on behalf of security.
- Participates in user access reviews for Security Operations staff.
- Development and maintenance of detailed process documentation to support security operations activities.
- Understanding and ensuring CalSAWS security policies are implemented.
- Developing, measuring, and improving security operations key performance indicators (KPIs).
- Organizing and coordinating regular cross team penetration testing activities.
- Developing and leading recurring incident response exercises.
- Lead and mentor a team of analysts to support all areas of responsibility.
- Respond to audits for the scope of responsible activities.
- Ensure effective and professional communication with State and County government counterparts.
- Other responsibilities as required by the Security and Operations Manager.

QUALIFICATIONS AND REQUIREMENTS

MINIMUM QUALIFICATIONS

Have a bachelor's degree in Cyber Security, Computer Science, Information Systems, or a closely related field from an accredited college or university -OR- possess relevant cyber security certifications, such as Certified Information Systems Security Professional, CompTIA+, or Certified Information Systems Manager.

- A minimum of three (3) years of recent, full-time, paid experience in delivery or management of the following security domains and related tooling:
    - Security incident response
    - Vulnerability management
    - Software development security
- Demonstrated ability to lead and mentor security operations delivery teams.
- Experience with cloud security controls and architecture, AWS preferred.
- Broad understanding of technical concepts across security and non-security domains.
- Excellent critical thinking skills.
- Have good oral and written communication.

WORK LOCATION REQUIREMENT

Applicants must reside and work within the State of California or be willing to relocate to the greater Sacramento, California area. This position may require travel on a limited basis for specific work assignments. This position is a hybrid work location position, which may include remote and onsite office work.

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

N/A