Department of Health Care Access and Information
Duty Statement

Employee Name Vacant	**Organization** Office of Technology Services Infrastructure and Operations Branch Infrastructure and Operations Section Security Operations Group
Position Number 441-610-1401-001	**Telework Option** Hybrid or None
Classification Information Technology Associate	**Working Title** Security Operations Analyst
Supervision Exercised N/A	**Location** Sacramento
Conflict of Interest: Yes ☐ No ☒	**Fingerprint/Live Scan:** Yes ☐ No ☒
Revision Date July 2026	**Effective Date**

Mission and Vision

HCAI is a leader in collecting data and disseminating information about California's healthcare landscape, promoting an equitably distributed health workforce, and publishing valuable information. The Department does this through five areas of program - Affordability, Workforce, Data, Facilities, Financing.

HCAI's mission is to expand access to quality, equitable, affordable health care for all Californians by supporting high value delivery systems, resilient health facilities and workforces, and actionable health information and strategies.

HCAI's vision is a healthier California where all receive equitable, affordable, and quality health care.

General Description

Under the general supervision of Information Technology (IT) Supervisor II, Security Operations Group, incumbent serves as one of the Tier 1 Security Analyst. The IT Associate primarily monitors HCAI security tools and service management system for alerts and incidents. The incumbent evaluates alerts and incidents for criticality and responds accordingly.

The IT Associate will work alongside IT Supervisor II and IT Specialists to enhance security tools and maintain endpoint and security device patching levels. The incumbent will also be responsible for documenting procedures and solutions to incidents.

The IT Associate works primarily in the Business Technology Management, Client Services, and Software Engineering domains.

Essential Job Functions

40% Tier 1 Security Analyst

- Monitor Security Information and Event Management (SIEM) System
- Review alerts daily for relevance and urgency
- Triage security events to ensure a valid security incident is occurring
- Respond to verified incidents to stop threats from spreading
- Monitor the security settings of infrastructure services and alert on any deviations from established controls
- Tune infrastructure and cloud solutions to ensure logs are returned to security monitoring solutions
- Remediate security incidents and events
- Tune security and network appliances to reduce false positive reports

30% Security Tuning and Patch Management

- With the assistance of Security engineers, tune security monitoring tools to reduce false positives
- Leverage vulnerability management tools to deploy patches to affected endpoint systems With the assistance of security engineers, schedule patching and maintenance on network security tools
- Configure security settings on infrastructure solutions to ensure compliance with Department and State standards
- Configure security settings on cloud solutions to ensure compliance with Department and State standards

15% Documentation

- Document standard procedures for evaluating alerts
- Document standard procedures for responding to different incidents
- Document processes followed to maintain the security of the HCAI network and systems

10% Research and Training

- Research new features of existing tools
- Research security industry trends
- Research emerging threats and evaluate options to protect our network

Marginal Job Functions

5% Performs related duties, special assignments, and program support activities consistent with the classification and level of responsibility of the position

Physical Demands

Must possess and maintain sufficient strength, agility, endurance, and sensory ability to perform the duties contained in this duty statement with or without reasonable accommodation.

Working Conditions

Requires use of computing devices and phones, frequent face-to-face contact with management, staff, consultants and the public, verbal, written and digital (e-mail) communication, extensive review, analysis and preparation of electronic and written documents, assessment of practical demonstrations, mobility to various areas of the Department, occasional travel and overnight stays to training/conferences or the Los Angeles field office may also be required, and work hours may deviate from core business hours based on the service requirements of the Department.

Employee Statement

I have reviewed and discussed the duties and responsibilities of this position with my supervisor and have received a copy of this duty statement.

Employee Name	Employee Signature	Date Signed

Supervisor Statement

I have discussed the duties of this position with and have provided a copy of this duty statement to the employee named above.

Supervisor Name	Supervisor Signature	Date Signed