

CYBERSECURITY ANALYST I**DEFINITION**

The Cybersecurity Analyst I monitors, analyzes, and responds to security incidents and threats to protect the organization's information systems. This role involves working with various security tools and technologies to identify vulnerabilities and implement measures to mitigate risks. The Cybersecurity Analyst I collaborates with other IT teams to maintain and elevate the organization's security posture.

SUPERVISION RECEIVED AND EXERCISED

The Cybersecurity Analyst I reports to the Chief Information Security Officer and may provide guidance to IT staff across different divisions, end-users, and student workers.

ESSENTIAL DUTIES

- **Security Monitoring and Incident Response:**
 - Monitor security alerts and incidents using various security tools. Analyze and respond to security incidents to mitigate risks.
- **Vulnerability Management:**
 - Conduct regular vulnerability assessments and scans. Identify and prioritize vulnerabilities and work with IT teams to remediate them.
- **Threat Analysis:**
 - Analyze threat intelligence and security data to identify potential threats and vulnerabilities. Provide recommendations for improving security measures.
- **Security Policies and Procedures:**
 - Assist in developing and implementing security policies, plans, procedures, and guidelines. Ensure compliance with relevant regulations and standards.
- **User Training and Awareness:**
 - Conduct security awareness training for employees. Promote best practices for information security within the organization.
- **Documentation and Reporting:**
 - Maintain detailed documentation of security incidents, vulnerabilities, and remediation efforts. Prepare reports for management on security posture and incidents.
- **Security Operations:**
 - Continuously monitor, maintain and operate various cybersecurity systems, including but not limited to perimeter firewalls, antivirus/EDR/XDR, communications security platforms, and SEIM/SOAR systems.
- **Other Duties as Assigned:**
 - May be tasked with various Information Technology, Information Security, or general office-related duties outside those defined in this document

MINIMUM QUALIFICATIONS

To perform this job successfully, an individual must be able to perform each essential duty satisfactorily. The Education/Experience, Knowledge and Ability requirements are representative of essential duties.

Education and Experience:

- **Education:** Possession of an earned Associate's degree from an accredited College or University in Computer Science, Information Technology, Cybersecurity, or a related field.
- **Experience:** Zero to two years of experience in cybersecurity or related roles. Candidates meeting the educational requirements with no prior professional experience will be considered.
- One or more certifications relating to cybersecurity preferred (e.g., CompTIA Security+, Cisco CCNA Security, Palo Alto Networks PCNSA, EC-Council CEH, or ISC2 CISSP Associate)

Knowledge of:

- Basic principles of cybersecurity and information security.
- Standard security tools and technologies (e.g., SIEM, IDS/IPS, EDR/XDR, firewalls).
- Vulnerability assessment and management.

Ability to:

- Analyze and respond to security incidents effectively.
- Communicate security concepts and best practices to non-technical staff.
- Work collaboratively with IT teams and other stakeholders.

Licenses and Certificates:

- Possession of a valid California Motor Vehicle Operator's License

Physical and Mental Standards*:

- **Mobility:** ability to sit for long periods, move about an office, stand occasionally, reach above and below desk level.
- **Dexterity:** fine manipulation sufficient to operate a keyboard, handle individual papers, write and take notes.
- **Lifting:** occasional lifting of papers, files, equipment and material weighing up to 50 pounds.
- **Visual Requirements:** close vision sufficient to read files, documents, and computer screens and do close-up work; ability to adjust focus frequently.
- **Hearing/Talking:** ability to hear normal speech, speak and hear on the telephone, and speak in person.
- **Emotional/Psychological Factors:** ability to make decisions and concentrate; frequent contact with others including some public contact; frequent deadlines and time-limited assignments.

**Reasonable accommodation may be made to enable individuals with disabilities to perform the essential functions of the position.*

TYPICAL WORKING CONDITIONS

- Work is generally performed in a standard office environment.
- May require occasional evening and weekend hours.

Class Adopted: December 2025

Class Amended: