YOSEMITE COMMUNITY COLLEGE DISTRICT *Range: 36*

CYBERSECURITY ANALYST II

DEFINITION

The Cybersecurity Analyst II is responsible for leading the analysis and responding to complex security incidents and threats. This role involves advanced threat analysis, vulnerability management, and the development of security policies and procedures. The Cybersecurity Analyst II collaborates with various IT teams and stakeholders to enhance the organization's security posture and ensure compliance with relevant regulations.

DISTINGUISHING CHARACTERISTICS

The Cybersecurity Analyst II focuses on complex incidents, advanced threat analysis, and leadership responsibilities. This classification works independently, develops and enforces security policies, leads forensic investigations, and provides guidance to Analyst I and other IT staff. Analyst II serves as a subject matter expert, collaborating across teams to strengthen the organization’s security posture and ensure compliance with regulations and best practices.

SUPERVISION RECEIVED AND EXERCISED

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

ESSENTIAL DUTIES

- **Advanced Security Monitoring and Incident Response:**
  - Lead the monitoring and response to complex security incidents. Perform detailed analysis and forensic investigations to identify root causes and mitigate risks.
- **Vulnerability Management:**
  - Conduct in-depth vulnerability assessments and scans. Develop and implement remediation plans for identified vulnerabilities.
- **Threat Intelligence and Analysis:**
  - Analyze advanced threat intelligence and security data. Identify emerging threats and vulnerabilities and provide strategic recommendations.
- **Security Policies and Procedures:**
  - Develop and implement comprehensive security policies, plans, procedures, and guidelines. Ensure compliance with relevant regulations and standards.
- **User Training and Awareness:**
  - Lead security awareness training programs for employees. Promote a culture of security within the organization.
- **Documentation and Reporting:**
  - Maintain detailed documentation of security incidents, vulnerabilities, and remediation efforts. Prepare comprehensive reports for management on security posture and incidents.
- **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 a Bachelor's degree from an accredited College or University in Computer Science, Information Technology, Cybersecurity, or a related field.
- **Experience**: Three to five years of experience in cybersecurity or related roles.
- 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:

- Advanced principles of cybersecurity and information security.
- Advanced security tools and technologies (e.g., SIEM, IDS/IPS, EDR/XDR, firewalls).
- In-depth vulnerability assessment and management.

Ability to:

- Lead the analysis and response to complex security incidents.
- Develop and implement comprehensive security policies and procedures.
- Communicate advanced security concepts and best practices to technical and 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: