CITY OF MERCED

CYBERSECURITY SPECIALIST I/II

*Class specifications are intended to present a descriptive list of the range of duties performed by employees in the class. Specifications are **not** intended to reflect all duties performed within the job.*

SUMMARY DESCRIPTION

Under general supervision, the Cybersecurity Specialist I/II is responsible for designing, implementing, monitoring, and managing security solutions to protect against unauthorized access, cyberattacks, and data breaches. This position focuses on building and maintaining cybersecurity tools and systems while ensuring compliance with regulatory and organizational security standards.

DISTINGUISHING CHARACTERISTICS

The Cybersecurity Specialist I and II classifications are both professional-level roles responsible for cybersecurity engineering and infrastructure.

The Cybersecurity Specialist I performs complex technical work and contributes to the development and maintenance of cybersecurity systems and tools.

The Cybersecurity Specialist II operates at a strategic and senior level, providing technical leadership across complex initiatives, guiding cross-functional teams, and serving as a key contributor in cybersecurity architecture, threat mitigation, and operational resilience.

REPORTS TO

Information Technology Manager, or designee.

CLASSIFICATIONS SUPERVISED

This is not a supervisory classification. Cybersecurity Specialist II may provide lead direction and mentorship to other staff.

REPRESENTATIVE DUTIES

The following duties are typical for this classification. Incumbents may not perform all of the listed duties and/or may be required to perform additional or different duties from those set forth below to address business needs and changing business practices.

Cybersecurity Specialist I

1. Design, implement, and manage cybersecurity systems to protect critical assets, including networks, servers, and cloud platforms.
2. Build and maintain tools for threat detection and incident response, including SIEM systems, firewalls, and intrusion detection/prevention systems.
3. Ensure the reliability and availability of cybersecurity systems through performance tuning and troubleshooting.
4. Collaborate with internal IT staff and external managed SOC teams to integrate and optimize tools for threat detection and response.
5. Develop and enforce security standards and procedures in compliance with frameworks such as CJIS, HIPAA, PCI-DSS, and NIST.
6. Conduct vulnerability assessments and provide guidance on remediation.
7. Stay informed on emerging cybersecurity threats and recommend upgrades or new tools.

8. Document system configurations, security protocols, and operational processes.

Cybersecurity Specialist II (in addition to above):

1. Provide technical leadership in the development of secure IT infrastructure.
2. Lead complex incident response efforts in coordination with internal IT teams and external managed SOC providers; serve as the escalation point for advanced threat investigations and remediation.
3. Provide lead direction and mentorship to staff or project teams.
4. Evaluate and implement advanced security technologies and automation strategies.

QUALIFICATIONS

The following generally describes the knowledge and ability required to enter the job and/or be learned within a short period of time in order to successfully perform the assigned duties.

Knowledge of:

Cybersecurity systems and best practices for IT infrastructure protection.
SIEM tools.
Create Runbooks and Playbooks.
Network security protocols and tools (e.g., firewalls, VPNs, endpoint protection).
Cloud security practices
Regulatory compliance frameworks (NIST,CJIS, ISO 27001, SOC 2, PCI-DSS).

Ability to:

Design and maintain robust cybersecurity systems tailored to organizational needs.
Collaborate with IT and external SOC teams to ensure tools are optimized for real-time threat detection and incident response.
Implement and manage cybersecurity tools, ensuring their functionality and reliability.
Automate processes using scripting languages to enhance efficiency.
Demonstrate strong interpersonal skills, including active listening, conflict resolution, and the ability to work collaboratively in cross-functional teams.
Communicate technical information clearly and effectively to both technical and non-technical audiences, including through written documentation, in-person meetings, and formal presentations.
Deliver in-person sessions to staff on cybersecurity awareness, tools, and procedures.
Facilitate and participate in cross-departmental meetings to align cybersecurity practices with organizational goals.
Conduct risk assessments and implement measures to mitigate potential threats.

Education and Experience Guidelines - *Any combination of education and experience that would likely provide the required knowledge and abilities is qualifying. A typical way to obtain the knowledge and abilities would be:*

Cybersecurity Specialist I

Candidates must meet **one** of the following qualification paths:

Option 1:

Bachelor's degree in Cybersecurity, Information Technology, Computer Science, or a related field; **and**

Two (2) years of professional experience in a cybersecurity or infrastructure-focused role.

Option 2:

High school diploma or equivalent; **and**

Four (4) years of professional experience in a cybersecurity or infrastructure-focused role.

License or Certificate:
Possession of an appropriate California Driver License.

Special Requirements:
Ability to pass a P.O.S.T. level background investigation.

Cybersecurity Specialist II

Bachelor's degree in Cybersecurity, Information Technology, Computer Science, or a related field; **and**

Five (5) years of progressively responsible experience in a cybersecurity, engineering, or infrastructure-focused role.

License or Certificate:
Possession of an appropriate California Driver License.

Special Requirements:
Ability to pass a P.O.S.T. level background investigation.

DESIRED QUALIFICATIONS: (BOTH LEVELS):

CISSP, CEH, CompTIA Security+/CySA+.

PHYSICAL DEMANDS AND WORKING ENVIRONMENT

The conditions herein are representative of those that must be met by an employee to successfully perform the essential functions of this job. Reasonable accommodations may be made to enable individuals with disabilities to perform these essential job functions.

Environment: Work is typically performed in both an office and field environment with occasional travel to different sites; possible assignment to public safety locations; and position may require working evenings, weekends and holidays.

Physical: Primary functions require sufficient physical ability and mobility to work in an office setting; to sit, stand, climb, bend, and stoop for prolonged periods of time; to see in the normal range with or without correction; to hear in the normal range with or without correction; to operate various office equipment including a computer screen and keyboard; to lift and move objects weighing up to 50 pounds; and to verbally communicate to exchange information.