CYBERSECURITY SPECIALIST

DEFINITION

Under general supervision, the Cybersecurity Specialist 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 the tools and systems that support Cybersecurity Analysts, while ensuring compliance with regulatory and organizational security standards and enhancing the efficiency of the Security Operations Center (SOC).

SUPERVISION RECEIVED/EXERCISED

Receives supervision from a Manager or designee. Exercises no supervision; may provide lead direction and guidance to team members on system tools and configurations.

DISTINGUISHING CHARACTERISTICS

This class differs from the Cybersecurity Analyst and Senior Cybersecurity Analyst classification by emphasizing cybersecurity architecture and system engineering. The Cybersecurity Specialist is responsible for the development and maintenance of technical tools and infrastructure used in monitoring, threat detection, and response and ensures the SOC functions effectively and efficiently while enabling the Manager to focus on operational leadership.

EXAMPLES OF IMPORTANT AND ESSENTIAL DUTIES

May include, but are not limited to, the following:

Designs, implements, and manages advanced cybersecurity systems to protect critical city assets, including networks, servers, and cloud platforms.

Builds and maintains tools used for threat detection and incident response, including Security Information and Event Management (SIEM) systems, firewalls, and intrusion detection/prevention systems.

Ensures the reliability and availability of cybersecurity systems through performance tuning and troubleshooting.

Provides technical leadership in the development of secure IT infrastructure, focusing on proactive measures to mitigate risks.

Collaborates with the SOC team to integrate and optimize tools, enabling swift detection and response to emerging threats.

Develops and enforces security standards and procedures, ensuring compliance with frameworks such as CJIS, HIPAA, PCI-DSS, and NIST.

Conducts vulnerability assessments and provides guidance on remediation to reduce the risk of cyberattacks.

Stays informed on emerging cybersecurity threats and advancements, recommending upgrades or new tools to enhance the city's cybersecurity posture.

Develops comprehensive documentation for system configurations, security protocols, and operational processes.

May provide lead direction and guidance to team members on system tools and configurations.

May lead Tier 3 SOC operations.

Performs related duties as required.

JOB RELATED AND ESSENTIAL QUALIFICATIONS

Knowledge of:

Advanced cybersecurity systems and best practices for IT infrastructure protection.
Security Information and Event Management (SIEM) tools, such as Splunk, QRadar, or Azure Sentinel.

Network security protocols and tools, including firewalls, VPNs, and endpoint protection platforms.

Cloud security practices for AWS, Azure, or Google Cloud environments.
Regulatory compliance frameworks, such as NIST, ISO 27001, and SOC 2.

Skill/Ability to:

Design and maintain robust cybersecurity systems tailored to organizational needs.

Collaborate with IT and SOC teams to ensure tools are optimized for real-time threat detection and incident response.

Communicate technical information clearly to both technical and non-technical audiences.

Analyze complex cybersecurity challenges and develop effective solutions.

Implement and manage cybersecurity tools, ensuring their functionality and reliability.

Automate processes using scripting languages, such as Python or PowerShell, to enhance efficiency.

Conduct risk assessments and implement measures to mitigate potential threats.

MINIMUM QUALIFICATIONS

Option 1:

Possession of a bachelor's degree from an accredited college or university in Cybersecurity, Information Technology, Computer Science, or a related field AND three (3) years of experience equivalent to that gained in a cybersecurity engineering or infrastructure-focused role.

Option 2:

High School Diploma or equivalent AND five (5) years of experience equivalent to that gained in a cybersecurity engineering or infrastructure-focused role.

Preferred Qualifications:

- CISSP, CompTIA Security+, or other relevant credentials.

Special Requirements

Possession and continued maintenance of a valid California Driver's License at time of appointment.

Candidates selected for hiring consideration will be required to pass an extensive pre-employment background investigation.

APPROVED: *(Signature on File)* DATE: 9/3/2025
Director of Personnel Services

NEW: SM:vd 9/8/2025