CITY OF ROSEVILLE

SECURITY ANALYST I
SECURITY ANALYST II

DEFINITION

To perform a variety of professional level work including the design, implementation, evaluation, and daily management of security systems and solutions; and to perform duties related to threat detection and prevention, education, risk assessment, compliance, governance, business recovery, forensics, and incident response.

DISTINGUISHING CHARACTERISTICS

Security Analyst I – This is the entry level class in the Security Analyst series. This class is distinguished from the journey level by the performance of the more routine tasks and duties assigned to positions within this series. Employees at this level are not expected to perform with the same independence of direction and judgment on matters allocated to the journey level. Since this class is typically used as a training class, employees may have only limited or no directly related work experience. Employees work under general supervision while learning job tasks.

Security Analyst II – This is the journey level class within the Security Analyst series and is distinguished from the I level by the assignment of the full range of duties. Employees at this level receive only occasional instruction or assistance as new, unusual or unique situations arise and are fully aware of the operating procedures and policies within the work unit. Positions in this class are flexibly staffed and are normally filled by advancement from the I level.

SUPERVISION RECEIVED AND EXERCISED

Security Analyst I

Receives general supervision from an assigned Security Administrator.

May exercise technical and functional supervision over technical and administrative support personnel.

Security Analyst II

Receives direction from an Security Administrator.

May exercise technical and functional supervision over lower level professional, technical and administrative support personnel.

EXAMPLES OF ESSENTIAL DUTIES - Duties may include, but are not limited to, the following:

Architect, implement, monitor, maintain, and troubleshoot various security systems that protect the City's networks, systems, applications and critical infrastructure.

Design, organize, modify, install, secure and support security infrastructure; provide technical support for network and security issues associated with enterprise applications.

Implement timely solutions to security issues adversely affecting confidentiality, integrity and/or availability of City systems and data.

Analyze both raw and processed security alerts and event data to identify potential security incidents, threats, mitigations, and vulnerabilities.

Ensure all system changes are tested, documented and submitted to the Change Advisory Board prior to implementation.

Facilitate administrator and end-user cyber security training and security awareness programs.

Architect, implement, maintain, and troubleshoot the City's business continuity plan as it relates to redundant, secure infrastructure.

Coordinate with Data Center SMEs to provide secure, fault tolerant and highly available systems and networking infrastructure.

Investigate, analyze, produce reports, and remediate security incidents that occur on City systems and applications, both on-premise as well as in the cloud.

Develop and maintain security-related policies, procedures, design documents, diagrams, drawings, and related documentation.

Serve as subject matter expert for electronic messaging and confidential litigation/eDiscovery requests.

Prepare technical and administrative reports; review, prepare and update internal system documentation and end user training instructional materials; conduct cross-training and end user training on group or individual basis as needed.

Perform risk assessments and execute tests of network and information systems to ensure technology processes are secure

Confer with users to discuss issues such as computer data access needs, security violations, and system changes.

Review violations of computer and network security protocols and discuss procedures with violators to ensure violations are not repeated.

Stay up to date on evolving security threats and trends; regularly review security alerts and reports from Federal, State and commercial security sources.

Review concept papers and proposals and provide input regarding security aspects of proposed projects, applications, and systems

Ensure systems and procedures are compliant with relevant industry requirements and government regulations, e.g. PCI-DSS, CJIS, NERC CIP, etc.

Build and maintain positive working relationships with co-workers, other City employees, vendors, other public agencies and the public using principles of good customer service.

Perform related duties as assigned.

MINIMUM QUALIFICATIONS

Security Analyst I

Knowledge of:

Basic concepts of management, configuration, and deployment of next-generation firewalls.

Basic concepts of network security intrusion detection and prevention.

Methods for system administration, supporting multiple platforms and applications.

Client to site and site to site VPN technologies and protocols

Security appliance, server, and network hardware configuration, installation, maintenance, and troubleshooting.

Basic concepts of cyber security incident response.

Information security standards, compliance mandates, and regulations.

Application and System Vulnerability Scanning and Mitigation.

Principles and practices of authenticating users and devices including Active Directory authentication protocols

Public Key Infrastructure (PKI) and secure web server architectures

Server and network virtualization technologies including, but not limited to VMWare, Hyper-V, and Software-defined Networking.

Networking protocols, services and operating systems, to include but not limited to, OSI Model, TCP/IP, LDAP, RADIUS, IPSec, HTTP, HTTPS, SSL, SSH, SFTP, SMTP, SMB, SNMP, Windows and Linux.

Design techniques, tools, and principles involved in the production of precision technical plans, blueprints, drawings, and models.

Ability to:

Perform professional work involving the evaluation, implementation, and daily management of security systems.

On a continuous basis, know and understand all aspects of the job. Intermittently analyze work papers, reports and special projects; identify and interpret technical and numerical information; observe and problem solve operational and technical policy and procedures.

On a continuous basis, sit at desk for long periods of time. Intermittently twist to reach equipment surrounding desk; perform simple grasping and fine manipulation; intermittently climb stairs and/or ladders to rooftops and walk rooftops perimeter; use telephone, and write or use a keyboard to communicate through written means; and lift or carry weight of 50 pounds or less.

Create accurate network diagrams and detailed technical documentation and reports for designing, planning, and supporting security systems.

Understand and administer security and separation of duty requirements for enterprise applications and systems.

Analyze and diagnose security-related issues with networks and systems.

Maintain and administer security systems and procedures.

Train or instruct stakeholders in the proper use of security-related applications and procedures.

Assist with the building and maintenance of security systems and applications.

Prepare a variety of reports and maintain accurate records and files.

Maintain confidentiality as necessary.

Work weekends, evenings or standby, as required.

Communicate clearly and concisely, both orally and in writing.

Establish and maintain effective working relationships with those contacted in the course of work.

Experience and Training

Experience:

No professional experience is required.

AND

Training:

A Bachelor's degree from an accredited college or university, preferably with major course work in computer science, information systems, business management, business information systems, or a related field.

License or Certificate:

Possession of a valid California driver's license by date of appointment

Security Analyst II

In addition to the qualifications for the Security Analyst I:

Knowledge of:

NIST 800-series cyber security standards, CIS Top-20 Critical Security Controls, Payment Card Industry Data Security Standards (PCI-DSS), and Criminal Justice Information Security (CJIS) requirements.

Principles and practices of securing cloud-hosted systems and applications.

Principles and practices of complex operating system design, analysis, and documentation.

Current hacker techniques, exploits, active defense detection and prevention measures, penetration testing tools, tactics, techniques, and procedures (TTPs).

Unified threat management (UTM) firewalls and associated components including, but not limited to, URL/Content filtering, file scanning and blocking, DNS sinkholing, and data leakage prevention,

Endpoint detection and response (EDR) platform deployment, monitoring and management,

Business continuity planning, documentation, and testing best practices.

Computer and network forensic tools, techniques and analysis including root cause and comprehensive cause and effect analysis of cyber attacks and breaches.

One or more scripting languages, e.g. PowerShell, Python, BASH, etc., at an expert level.

Single sign-on, Multi-factor Authentication and SAML concepts and applications.

eDiscovery processes and techniques for messaging and other social media platforms

Network monitoring tools and techniques used to perform security troubleshooting including packet capture and protocol analysis tools.

Network routing and switching protocols (BGP, EIGRP, OSPF, RIP, VLANs, STP, VTP, IOS, NX-OS, HSRP, CDP, LLDP).

Principles and practices of project management.

File storage technologies, file structures, and file systems.

Methods of application integration.

Ability to:

Independently manage security-related projects, investigations, operations, and incident response.

Independently perform professional work involving the evaluation, implementation, and daily management of information security systems.

Implement and maintain compliance with all required information security rules, regulations, mandates, standards, and best practices.

Design, document, and implement secure network, system, and application architectures.

On an ongoing basis, identify and declare observed risks, threats and vulnerabilities and propose practical steps to minimize or mitigate them.

Participate in, or lead, cross functional teams and meetings.

Perform and/or work with professional service providers to conduct risk assessments and/or ethical hacking/penetration testing against city systems to determine and mitigate vulnerabilities and other security issues

Perform governance tasks, including research, analysis and evaluation, and provide recommendations regarding proposed security, network, and user systems and applications.

Conduct various security awareness programs such as citywide cyber security training campaigns, phishing testing, and periodic targeted training initiatives.

Experience and Training

Experience:

Two years of responsible experience performing duties similar to that of a Security Analyst I with the City of Roseville.

AND

Training:

A Bachelor's degree from an accredited college or university, preferably with major course work in computer science, information systems, business management, business information systems, or a related field.

License or Certificate

Possession of a valid California driver's license by date of appointment.