CITY OF BELLINGHAM

JOB DESCRIPTION

JOB TITLE: **Senior Information Security Analyst** **UNION:231**
SG:7
DEPARTMENT: **Information Technology Services** **CS:N**
FLSA:N
EEO4CODE:TE

JOB SUMMARY:

Oversees and serves as primary resource for administrative, operational, and technical aspects of the City's security information event and vulnerability management systems. Prioritizes the availability, operation, maintenance, and security of the City's computer systems, networks and data. The City's networks are a mission critical part of the City's operation and provide services to over 30 staffed worksites and to numerous non-staffed locations.

Conducts risk assessments, evaluates security vulnerabilities, and monitors and analyzes City systems to identify priority mitigations. Provides direction, coordination, assistance and training support to City staff to correct identified security vulnerabilities and implement priority security controls. Prepares, plans and leads tabletop exercises for City staff based on City policies and procedures. Coordinates or supports ad-hoc information security projects. Participates in the selection of consultants to conduct outside risk assessments and/or pen tests. Reviews, drafts and improves incident response plans and procedures. Maintains detailed and accurate technical and administrative records. Serves as a member of the IT Security Team. Leads and/or assists with internal technical investigations.

Assists the Director and Network Operations Manager in developing programs to ensure City compliance with regulatory, security, and privacy standards such as Criminal Justice Information Services (CJIS), Health Insurance Portability and Accountability Act (HIPAA) and Payment Card Industry Data Security Standard (PCI DSS), along with security and privacy standards adopted by the City.

SUPERVISORY RELATIONSHIP:

Reports directly to the Information Technology Network Operations Manager. Work is performed under general supervision and the guidance of applicable departmental, City, state, and federal regulations, policies, guidelines, and standards. Directs and assists technical staff from all departments to correct priority security vulnerabilities and confirm completion. Provides education, training and guidance to staff at all levels of the organization related to security policies, standards and vulnerabilities. Supervises contractors, consultants, project teams and vendors performing security analysis and auditing work.

ESSENTIAL FUNCTIONS OF THE JOB:

1. Monitors the availability, operation, maintenance and security of the City's computer systems, networks and data. Using a variety of enterprise monitoring tools, reviews anomalies, bulletins, and alerts as they may apply to the enterprise network. Advises other staff and enterprise clients of steps to take to mitigate security threats. If threat is imminent, determines risk of waiting to apply known fixes/patches as opposed to immediate implementation.

2. Oversees and serves as primary resource responsible for administrative, operational, and technical aspects of the City's Security Information and Event Management (SIEM) and multiple vulnerability management platforms. Provides leadership, direction, coordination and training to technical staff to correct high priority vulnerabilities. Resolves problems through internal resources or through consultation with vendor technical support staff.

3. Monitors the security of the City's technology systems using best practices and security standards. Develops dashboards or reports to provide awareness, training and status information to other staff. Researches and maintains knowledge of current network security and network infrastructure technologies and best practices.

4. Serves as a member of the IT Security Team responsible for supporting security initiatives in area of responsibility. Reviews and maintains required security metrics and documentation on City systems, ensuring compliance with security standards. Responds to incidents, providing guidance to all levels of the organization; may serve as technical lead on incidents consistent with City policies and procedures.

5. Plans, coordinates and conducts cybersecurity tabletop exercises based on existing policies and procedures. Selects appropriate exercises from partner agencies (i.e. Washington State Office of Cybersecurity) and modifies to represent the City's needs. Creates presentation material, schedules and leads exercises.

6. Plans and conducts internal risk assessments and audits. Serves as project manager for risk assessments and pen tests. Responsible for project development, planning, implementation, communication and training. Develops requests for information (RFIs) and requests for proposals (RFPs); reviews bids to ensure vendors meet minimum requirements; participates in selection of vendors. Works closely with department administrative staff to maintain accurate billing, budget and related project records. Supports external technical audits and assessments by collecting and distributing relevant data and documentation.

7. Serves as lead for certificate management. Acquires, manages, inspects and applies certificates to internal and external systems.

8. Supports Department Director and Network Operations Manager in the development and monitoring of budgets for security systems and outside professional services. Recommends products and services and provides budget estimates to management.

9. Maintains accurate and up-to-date technical and administrative records including documentation of the enterprise network and critical security configurations, risk registers, vendor contacts, network diagrams and Knowledge Base articles.

10. Contributes to the development of City policies, standards, and procedures related to technology and security. Provides training and communications related to policies, procedures, and standards to City staff and outside contractors. Advises department leaders and managers of system vulnerabilities.

ADDITIONAL WORK PERFORMED:

1. Performs other related work of a similar nature and level.

PERFORMANCE REQUIREMENTS (Knowledge, Skills, and Abilities):

TECHNICAL

Knowledge of:

- Thorough knowledge of Information Security including Vulnerability Management, Risk Assessment, Auditing, Response, and Compliance.
- Extensive knowledge of network applications and protocols, configuration, routers, logging, monitoring, administration.
- Extensive knowledge of Syslog and SIEM principles, operations, configuration, and usage.
- Extensive knowledge of operating systems such as Microsoft Windows, VMware and Cisco IOS Syslog.
- Extensive knowledge of browsers, i.e., Chrome, Edge, etc.
- Extensive knowledge of a multitude of monitoring and investigative tools such as Nessus Vulnerability Scanner, Wireshark Packet Analyzer, forensic drive imaging tools and Security Orchestration, Automation and Response (SOAR) packages.
- Extensive knowledge of a wide variety of computer language skills, including PowerShell and Python.
- Extensive knowledge of Command Line Interface syntax and use.
- Thorough knowledge and awareness of regulatory and security standards and requirements including CJIS, HIPPA, PCI, and CIS.
- Encryption technology, tools, and techniques.

Skill in:

- Extensive skills using, administering, configuring, and interpreting SIEM and Vulnerability management tools.
- Extensive skills in auditing network services and systems - administering, monitoring, tuning, and modifying network equipment including appliances, routers, switches, firewalls, telephony equipment, servers, virtual environments, and associated software.
- Extensive skills with network connectivity for all workplace devices.
- Extensive skills in network and desktop operations Extensive skills with use of Command Line Interfaces (MS-DOS, Unix/Linux Shells, PowerShell).
- Extensive skills with TCP/IP protocol stack and associated applications including Telnet / SSH / FTP (CRT), TFTP, DNS, DHCP.
- Extensive skills with Microsoft Windows domain networks; firewall management; active directory federation services; multi-factor authentication and VPN.
- Extensive skills with wired and Wi-Fi networking both on-site and remote; integration with and use of cloud-based resources including Azure and OneDrive and secure connections including SaaS and hosted application environments.
- Data storage, backup and recovery management, procedures and concepts; data center security requirements.
- Thorough skills in security incident response and management.
- Thorough skills with Regular Expression (Regex) parsing.
- Thorough skills in communications protocols and file system structures.

Ability to:

- Maintain absolute confidentiality of sensitive files, data and materials accessed, discussed, or observed while working with City staff, and while adhering to security policies and procedures.
- Maintain high degree of familiarity with City security policies, standards, and procedures.
- Lead and coordinate security projects and tasks.
- Understand and comply with City procurement policies.
- Extensive abilities with operating and monitoring complex and technical network and communications equipment.

- Thorough ability to read and interpret instruction manuals and troubleshoot and solve hardware and software problems.
- Thorough ability to maintain detailed and accurate documentation using appropriate tools.

COMMUNICATIONS

Skill in:
- Thorough written communication skills for preparing reports, composing documentation, and corresponding with City employees and vendors.
- Thorough communication and interpersonal skills for interactions with co-workers, supervisors, managers, other City employees, vendors, consultants and the general public.

Ability to:
- Understand, follow, and train others on regulatory requirements, security standards, and City policies, standards, procedures, and vulnerabilities related to technology and security.

OTHER

Skill in:
- Extensive organization, time management, problem solving, technical troubleshooting, and planning skills. Ability to work on several projects concurrently.
- Thorough skills and abilities to establish and maintain effective working relationships with other employees, City officials, representatives of other government agencies and community groups and the general public.
- Ability and willingness to demonstrate the Public Service Competencies of Service Orientation, Results Orientation, and Teamwork and Cooperation.
- Maintain consistent and punctual attendance.
- Physical ability to perform the essential functions of the job including:
  - Dexterity of hands and fingers to operate a computer keyboard;
  - May need to sit or stand for long periods of time;
  - Near distance visual acuity to assure proper operation of computers and software;
  - Ability to exchange verbal information in person and by telephone;
  - Occasionally transports components weighing up to 25 pounds.

WORKING ENVIRONMENT:

The work performed is in an office setting at a computer workstation with long periods of sitting or standing. Work environment incudes a normal range of noise and other distractions with low everyday risks working around standard office equipment. Work requires periodic visits to customer worksites. Work requires providing on-call support which may include evenings and weekends. The work involves occasionally inspecting equipment in ceilings to identify and solve problems, which can require ascending/descending ladders, entering tunnels, using lifts, standing on roofs to access equipment and cabling. Works with a variety of hand tools and computer diagnostic equipment to identify, repair and solve problems. Some travel to professional meetings is expected.

EXPERIENCE AND TRAINING REQUIREMENTS:

- Bachelor’s degree in information security/cybersecurity, information technology, computer science or related field required.

- Technical:
  - Four (4) years of experience in Information Security, including vulnerability management, SIEM administration, and/or incident response responsibilities.
  - Two (2) years of experience in network administration and support in a complex multi-site enterprise environment.
- One of the following certifications strongly preferred: GSEC, Security+, CISM, CISSP.
- An equivalent combination of education and experience sufficient to provide the applicant with the knowledge, skill and ability to successfully perform the essential functions of the job will be considered.

NECESSARY SPECIAL REQUIREMENTS:

- Agreement to and signature of a Privileged Access Confidentiality Agreement is required.
- Employment contingent upon passing a criminal convictions check, local background check and fingerprinting. Subject to re-check every five years.
- Valid Washington State driver's license and good driving record. Must provide a three-year driving abstract prior to hire.
- Willingness and ability to work extra hours or change hours as needed and to respond to evening and weekend callouts for incidents, emergencies, or when special circumstances require.

PREPARED BY: M Mulholland
I. Stewart
E. Weinberg
A. Sullivan
5/21

REVIEWED BY: _____
Marty Mulholland, Director
Information Technology
Services