Specialist Offensive Security

Job Title	Specialist Offensive Security
Division	Office of the Chief Information Security Officer
Reports To	Manager Offensive Security
Job Location	Metro Hall, 55 John Street
Job Tyle & Duration	Full time, Permanent
Shift Information	Monday to Friday, 40 hours per week
Affiliation	Non-Union
Max Salary Range	$103,303.20 to $121,368.40
Posting Closing	October 28, 2020
Number of Positions	2

JOB SUMMARY:

To provide expertise, guidance, advice, and operational support for the development, deployment and management of Threat Management programs to ensure the City is adequately protected from cyber security threats and to support the execution of the Chief Information Security Officer's (CISO) mandate, cyber vision and strategy.

To design and implement security systems to protect the City's computer networks from cyber attacks, and set and maintain security standards.

MAJOR RESPONSIBILITIES:

- Delivers expert capabilities and direction to conduct offensive security services.
- Conducts authorized assessment of infrastructure and applications to proactively identify security weaknesses.
- Verifies weaknesses by leveraging attacker techniques to evaluate the difficulty and effectiveness of potential attack from various threat actors.
- Provides comprehensive and actionable recommendations to counter the threat posed by identified security weaknesses, given the applicable threat landscape.
- Contributes to the continuous improvement of security processes, tools and techniques to counter threats faced by the organization. Researches and develops testing tools, techniques and processes.
- Leads and delivers reporting and metrics including Key Risk Indicators (KRIs).
- Develops and reports enterprise-level metrics for vulnerabilities and remediation progress.
- Understands, demonstrates, and educates stakeholders on the real-world impact of threats and vulnerability exploitation in a given environment.
- Develops and implements detailed plans and recommends cyber security policies/procedures regarding program specific requirements.

- Leads, coordinates, and executes assigned projects, ensuring effective teamwork and communication, high standards of work quality and organizational performance and continuous learning.
- Supervises the day to day operation of all assigned project staff and contract resources including the scheduling, assigning and reviewing of work. Motivates and trains assigned staff. Coordinates vacation and overtime requests. Monitors and assists in evaluating staff performance, hears grievances and recommends disciplinary action when necessary.
- Provides guidance, advice, and direction to assigned project teams and contract resources to meet objectives.
- Works with Senior Specialists on large, complex projects, providing project coordination support, technical advice and guidance.
- Conducts research into assigned area ensuring that such research takes into account developments within the field, corporate policies and practices, legislation and initiatives by other levels of government.
- Ensures that project expenditures are controlled and maintained within approved budget limitations.
- Provides expertise in identification, analysis, testing, and remediation of cyber threats.
- Monitors, identifies, and analyzes events to ensure cyber threats are reported and remediated
- Assesses cyber security requirements of business strategies in order to provide appropriate advice, guidance, and technical solutions.
- Reviews, and facilitates approvals of security strategies within industry-accepted frameworks.
- Provides guidance in the evaluation, selection and recommendation of technical solutions and professional services. Identifies and evaluates emerging security technologies.
- Resolves cyber risk issues. Escalates significant cyber risk matters to senior management when required.
- Deals with confidential information affecting the organization and its resources. Prepares and presents reports to management supporting recommendations on changes/improvements in business processes, training and services standards that impact appropriate staffing levels and resource allocation. Makes recommendations based on investigation results which could lead to the discipline or dismissal of staff.
- Provides a confidential assessment of organizational issues and makes recommendations for next steps, including policy, procedural and structural change.
- Participates in the development, implementation, administration, monitoring and maintenance of security tools collecting confidential information on infrastructure and application weaknesses Maintains up to date knowledge of City's confidential cyber infrastructure.
- Works with senior management within the division to address active internal/external cyber threats to the City. Attends senior management meetings, makes recommendations to mitigate the threats, and takes appropriate urgent action as needed.
- Maintains an up-to-date and in-depth knowledge of cyber security, current and emerging application security threats, trends, and associated techniques and technologies as well as key business drivers and opportunities. Identifies, manages, and mitigates cyber security risks in applications.
- Participates in the preparation of various formal contractual documents such as Request For Information/ Proposal/Quotation , Statement of Work, Memorandum of Understanding and Service Level Agreements.

- Anticipates, analyzes and identifies organizational impacts of emerging requirements; recommends and coordinates innovative solutions using conflict resolution and negotiation skills to successfully manage sensitive and controversial matters.
- Provides project coordination and management support, and ensures comprehensive and effective information communication across various functional and project team.
- Organizes and works with multidisciplinary business and technical teams from across the organization to formulate and execute project plans and tasks according to established project management principles and methodologies.
- Maintains accurate reporting of key risk metrics and associated measurements in alignment with the cyber risk appetite.
- Prepares regular cyber management reports leveraging cyber analytics subject matter expertise.
- Communicates effectively to stakeholders, clients, project managers, supervisors and team members regarding any business and technical decisions and actions that may impact solution delivery, staff performance, business processes, management workflow and technical support of public services.

QUALIFICATIONS/CERTIFICATIONS:

- Post-secondary degree in Business or Technology or a related discipline.
- Over 5 years experience in penetration testing.
- Extensive penetration testing experience with operating systems, web applications and network infrastructure.
- Strong experience with using Penetration Testing Tools. e.g. NMap, Nessus, Metasploit, BurpSuite, Nikto, Tcpdump.
- Administrator level knowledge of Server Operating Systems specifically Unix and Windows
- Intricate technical knowledge of TCP/IP Networking/Routing, Intranet / Internet Architectures and Segregation Technologies/VLANs, Firewalls, Intrusion Detection, Intrusion Prevention, SQL Databases
- Ability to test web technologies e.g. web applications, containers, container managers
- Programming ability to create, read and modify exploit code to achieve system penetration. C, C++, Java, C#, scripting knowledge is an asset.
- Experience scaling security testing capabilities
- Demonstrate a current and working knowledge of Information Security best-practices, methodologies, and techniques.
- Preferred Certifications (any in the list): CISSP, CRISC, OSCP, CEH, GPEN

SKILLS:

- Ability to work in transformative programs
- Ability to lead efficient communication between all project stakeholders, including internal teams and clients.
- Ability to achieve business objectives through influencing and effectively working with key stakeholders.
- Excellent written & verbal communication skills (comfortable & confident communicating at all levels including business partners, leadership and vendors.
- Excellent problem-solving skills with capability to identify solutions to unusual and complex problems.

- Keen attention to detail and strong organizational skills.
- Highly organized, proactive, self-motivated team player who takes initiative and is able to work independently.
- Ability to work in a fast-paced environment managing multiple priorities with proven time management skills.
- Strong analytical skills and ability to prioritise and multitask.
- Ability to prioritize and effectively manage competing priorities and projects.
- Ability to manage multiple initiatives while adhering to strict deadlines.
- Transferable skills, like communication and decision-making, are equally important.
- Being able to think on your feet and show good judgment are especially valuable in this field. “Security pros should always be ready to react to cyber-related incidents quickly.

ADDITIONAL COMMENTS/INFORMATION:

A normal work week is 40 hours, however, unforeseen situation may require extended hours of work with little or no prior notice.
In case of a cyber incident or breach, rotation shift, continuous extended hours may be required with little or no prior notice.

*Subject to a police check, background check, psychological assessment and/or any other checks on a regular basis as the Office of the CISO handles highly sensitive and confidential information.