Senior Specialist Threat Management - Threat Intelligence

Job Title	Senior Specialist Threat Management - Threat Intelligence
Division	Office of the Chief Information Security Officer
Reports To	Manager Threat Intelligence & Fulfillment
Job Location	Metro Hall, 55 John Street
Job Type and Duration	Full Time, Permanent
Shift Information	Monday to Friday, 40 Hours per Week
Affiliation	Non-Union
Max Salary Range	$110,947.20 to $130,353.60
Posting Closing	October 28, 2020
Number of Positions Open	1

JOB SUMMARY:

To support the execution of the Chief Information Security Officer's (CISO) mandate, cyber vision and strategy, providing technical and business advice, support and services on Threat Management cyber programs and initiatives to all City divisions, agencies and corporations.

To define, develop and support Threat Management cyber programs and initiatives, engaging with teams across the organization to build alignment on key projects and develop execution roadmaps.

To provide subject matter expertise, strategic advice, senior level guidance and operational support for Threat Intelligence area within the Threat Management section.

MAJOR RESPONSIBILITIES:

- Leads the development, deployment and management of cyber threat intelligence capabilities and methods and creates models and analytics to detect abnormal activities within the City's infrastructure.
- Provides expertise and understanding of the threat landscape to mitigate risk and understand threats that might impact the City.
- Provides expert knowledge of Threat Intelligence processes and technologies including VM, SIEM, SOC, threat hunting, Incident response, and cloud security.
- Finds new and creative ways to detect new threats as well as existing threats by matching the tactics, techniques and procedures of known threat actors.

- Builds knowledge of and stays current on developments in the cyber threat landscape to adapt investigation techniques and provide recommendations on responding to and remediating related incidents, including the development of proactive analytics use cases.
- Assesses the relevance and usefulness of security data, conducts gap analyses on the data, and specifies configuration requirements for tools and controls to ensure that indicators of attacks/misuses are recorded properly in security data.
- Develops and implements detailed plans and recommends cyber security policies/procedures regarding program specific requirements.
- Supervises, motivates and trains assigned project staff and contract resources, ensuring effective teamwork, high standards of work quality and organizational performance, continuous learning and encourages innovation in others.
- Supervises the day to day operation of all assigned project staff and contract resources, including the scheduling, assigning and reviewing of work. Coordinates vacation and overtime requests. Monitors and assists in evaluating staff performance, hears grievances and recommends disciplinary action when necessary.
- Provides direction, leadership and guidance to project teams, assigned project staff and contract resources. Oversees and reviews their work.
- Provides leadership to influence employee engagement to the organization, to the team, and to their role.
- 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.
- Provides input into assigned project budgets, ensuring that expenditures are controlled and maintained within approved budget limitations.
- Provides subject matter expertise and strategic advice on cyber security issues affecting the organization, identifying potential exposures, and conducting reviews to ensure that undesirable effects are detected, mitigated and/or corrected, and providing pragmatic advice to clients to ensure that cyber risks are managed appropriately.
- Serves as the internal/external point of contact and subject matter expert in their respective function.
- Determines cyber security requirements of business strategies in order to provide appropriate advice, guidance, and technical solutions.
- Develops, reviews, and ensures approvals of security strategies within industry-accepted frameworks.
- Provides leadership in the evaluation, selection and recommendation of technical solutions and professional services. Identifies and evaluates emerging security technologies.
- 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.
- Participates in the development of transformation strategies focused on security, integrating and managing new or existing technology systems to deliver continuous operational improvements and detect, respond, and remediate threats.
- 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.

- 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.
- Provides a confidential assessment of organizational issues and makes recommendations for next steps, including policy, procedural and structural change.
- Takes a proactive approach to identify gaps and opportunities for improvement to mitigate risk.
- 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.
- Provides oversight and monitors cyber risk activities performed by project teams. Reviews and supports the implementation of processes and controls by various teams as outlined in the information risk policy and related operating directives, standards and procedures.
- Provides project coordination and management support, and ensures comprehensive and effective information communication across various functional and project teams.
- Communicates effectively to stakeholders, clients, project managers, 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.
- Provides support in the design, implementation, maintenance, and enforcement of policies, procedures, and controls.
- Plans, prioritizes and coordinates internal and/or external assigned project resources to meet project objectives.
- Prepares and/or supervises the preparation of various formal contractual documents such as Request For Information/ Proposal/Quotation , Statement of Work, Memorandum of Understanding and Service Level Agreements.
- Maintains accurate reporting of key risk metrics and associated measurements in alignment with the cyber risk appetite.
- Prepares regular cyber risk management reports, briefing notes, and presentations as required, leveraging cyber risk subject matter expertise.
- Builds and maintains strong relationships with internal and external stakeholders. Establishes relationships with strategic partners, collaborating on the advancement of cyber programs.
- Participates in meetings with executive leadership and strategic partners to review City's cyber security posture.
- Maintains an up-to-date and in-depth knowledge of cyber security, emerging threats, trends, and associated techniques and technologies as well as key business drivers and opportunities.

QUALIFICATIONS/CERTIFICATIONS:

- Post-secondary degree in Business or Technology or a related discipline.
- Over 6 years experience in Threat Hunting
- In-Depth knowledge of cyber investigation or threat intelligence.

- Extensive experience with intelligence analysis processes, including Open Source Intelligence (OSINT) and closed source intelligence gathering, source verification, data fusion, link analysis, and threat actor, is required.
- Extensive experience working in a Security Operations Centre (SOC) or Computer Emergency Response Team (CERT/CIRT).
- Excellent understanding of the current vulnerabilities, response, and mitigation strategies used in cyber security is required.
- Excellent ability to research and characterize security threats to include identification and classification of threat indicators is required.
- Investigative and analytical problem solving skills demonstrated by previous risk analysis and intelligence development experience are required.
- Excellent current and working knowledge of Information Security best-practices, methodologies, and techniques.
- Strong knowledge of effective security practices in a large, complex environment and awareness of general security-related training requirements within this environment.
- 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.
- Able to work extremely well under pressure while maintaining a high level of professionalism
- Self-motivated person with desire to go above and beyond tasks
- 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.