JOB PROFILE

TITLE: Cyber Threat Intelligence Analyst

ORGANIZATIONAL CONTEXT

The Ministry of Technology and Innovation's Cybersecurity division is responsible for overseeing all aspects of information and technology security for the Government of Alberta (GoA). The division collaborates with ministries, public agencies, and external partners to strengthen Alberta's overall cybersecurity posture, thereby safeguarding Albertans and promoting the province's economic and social well-being.

To manage and deliver its services effectively, the division operates through two distinct programs. The first, the GoA Cybersecurity Program, is dedicated to protecting the digital assets of the GoA as an organization. This program ensures that the government's digital infrastructure remains secure and resilient against cyber threats.

The second program, CyberAlberta, focuses on fostering collaboration among Alberta's public and private organizations. By leading these collaborative efforts, CyberAlberta aims to enhance the cybersecurity defenses of various entities across the province, thereby providing a unified front against cyber threats.

JOB OVERVIEW

As part of the CyberAlberta branch, the CTI analyst operates within the framework of relevant government and Ministry legislation, policies, and guidelines to provide comprehensive threat intelligence services to the Cybersecurity division and the province. Reporting to the Director, this role is responsible for all stages of the intelligence life cycle. Key responsibilities include identification of intelligence requirements, performing intelligence collection, data exploitation, analysis and synthesis, and the dissemination of written reports, verbal briefings, and presentations to various target audiences.

This position emphasizes team collaboration, analytical rigor, technical expertise, and excellent communication skills.

ACCOUNTABILITIES

- **Profile Threats Accurately**
  - Assess threats for their intent to cause harm to the organization.
  - Assess threats for their capability to cause harm to the organization.
  - Assess the opportunities presented to threats enabling them to cause harm to the organization.
  - Assess the willingness and capacity of a threat to cause harm to the organization.
  - Clearly articulate the level of risk presented by a threat and why.
- **Satisfy Intelligence Requirements and Requests for Information**
  - Work with stakeholders to develop intelligence requirements.
  - Accurately extract from stakeholder engagement the intelligence requirement.
  - Predict future intelligence requirements.
  - Complete requests for information.
- **Perform Intrusion Analysis**
  - Accurately extract and analyze intrusion events according to industry frameworks.
  - Cluster intrusion events according to standard and pre-defined analytical models.
  - Interpret from intrusion data, the Tactic and Technique being exercised by the adversary.
  - Interpret from intrusion data, the phase of the kill chain the adversary is in.
  - Interpret from intrusion data, the diamond model vertices most appropriate.
  - Interpret from intrusion data, the “human fingerprints” that enable attribution and tracking.
- **Develop Open-Source Intelligence**
  - Proficiently pivot from an initial data point to other data points using open sources.
  - Manage the collection and organization of mass amounts of opensource data.
  - Manage indicators throughout their lifecycle, and be able to accurately identify the stage a current indicator is in.
  - Exploit data to make sense of it and derive actionable insights.
- **Perform Intelligence Activities Safely**
  - Handle malware according to standard and safely, avoiding accidental detonation.
  - Operate, maintain, and ensure the integrity of an investigatory environment.
  - Apply the appropriate operational security during investigations.
  - Rapidly calculate intelligence cost-benefit analysis during on-going investigations.
  - Correctly select between active and passive collection.
- **Develop Code as Required**
  - Rapidly develop one-time use code for the purpose of solving a problem that may be intractable manually.
  - Develop automations which transform data into something useable and interpretable.
  - Develop analytical tools which aid in the various forms of data analysis.
  - Develop data visualizations for reporting or analysis purposes.
- **Communicate Intelligence to Consumers**
  - Understand the requirements and frame of reference of the target audience.
  - Create and disseminate strategic, operational, and tactical intelligence reports.
  - Provide briefings and status updates on urgent issues.
  - Provide rapid responses and advice to urgent requests.
  - Deliver presentations on technical and non-technical topics to strategic, operational, and tactical audiences.

- **Apply Analytical Rigor**
  - Identify and combat bias, analytical fallacies, and fallacies to form in yourself and others.
  - Utilize estimative language and subjective probability to convey analytical judgements.
  - Clearly distinguish between fact and assessment, both when receiving an assessment or delivering one.
  - Proficiently apply structured analytic techniques.

Optional Ministry Specific Accountabilities:

- Monthly Division Operational Reporting
- Assigned project work

JOB REQUIREMENTS (EDUCATION AND TECHNICAL EXPERIENCE)

- A university degree in Computer Science, Information Technology or related field, supplemented by at least two (2) years of related experience is required. See below for equivalencies.
- Related experience may include experience in an information technology or related role with an emphasis in threat intelligence, threat hunting, vulnerability management, security risk management, or security operation centre.
- Two (2) years of related progressively responsible experience

Equivalencies:

- A related two-year diploma in a related field from a recognized postsecondary institution and four (4) years related experience; or
- A related one-year certificate from a recognized post-secondary institution and five (5) years related experience.

Assets:

- Experience conducting research using open sources.
- Knowledge of network protocols and how adversaries utilize them to facilitate intrusions.
- Experience attributing malicious activity to known threat actors and uncovering their motivations, affiliations, and any further context.
- Proficient in one or more programming language (e.g., Python, C, C++), and one or more query language (e.g., KQL, SQL).
- Strong critical thinking, analytical and problem-solving skills, including the ability to deal with large amounts of information in a limited time
- Excellent communication skills, both written and verbal. Ability to communicate technical information to diverse audiences – both technical and non-technical – in a clear and concise manner.
- Familiarity with Microsoft PowerBI and the Azure suite of products, including Microsoft Sentinel and Microsoft 365 Defender.
- Possession of a cybersecurity certification, such as CISSP, CISM, CISA, CEH, GPEN, or equivalent.

BEHAVIOURAL COMPETENCIES

Agility: Ability to anticipate, assess, and readily adapt to changing priorities, manage resilience in times of uncertainty and effectively work in a changing environment.

Drive for Results: Knowing what outcomes are important and maximizing resources to achieve results that are aligned with the goals of the organization, while maintaining accountability to each other and external stakeholders.

Develop self and others: A commitment to lifelong learning and the desire to invest in the development of the long-term capability of yourself and others.

Build Collaborative Environments: Leads and contributes to the conditions and environments that allow people to work collaboratively and productively to achieve outcomes.

Develop Networks: Proactively building networks, connecting, and building trust in relationships with different stakeholders.

Systems Thinking: The work done within the APS is part of a larger integrated and inter-related

environment. It is important to know that work done in one part of the APS impacts a variety of other groups/projects inside and outside the APS. Systems thinking allows us to keep broader impacts and connections in mind.

Creative Problem Solving: Ability to assess options and implications in new ways to achieve outcomes and solutions.