Titre : Premier(-ère) conseiller(-ère), Analytique et intelligence de sécurité

Organisation : La Caisse (Caisse de dépôt et placement du Québec)

Localisation : 1000, place Jean-Paul-Riopelle Montréal (Québec) H2Z 2B3

Méthode de postulation : https://cdpq.mediarh.ca/R05087?utm_source=Centre+des+femmes+de+Montr%C3%A9al&source=Centre+des+femmes+de+Montr%C3%A9al

NOC ID : 21221

NOC JOB TITLE : analyste de l'intelligence d'affaires – Technologie de l'information

Le niveau de poste peut varier en fonction du profil de la personne retenue.

Au sein de l'équipe de cybersécurité, la personne titulaire du poste est responsable de la conception, de la mise en œuvre et de l'évolution des pipelines de détection et de télémétrie de sécurité, ainsi que des flux de renseignements de cybermenaces soutenant les opérations de sécurité.

Elle joue un rôle central dans l'ingénierie et la normalisation des données de sécurité et contribue directement à l'efficacité des capacités de détection en traduisant les besoins opérationnels du centre de sécurité opérationnelle (SOC) en cas d'usage et en logique de détection exploitables.

Ce rôle s'adresse à une personne rigoureuse, collaborative et orientée vers la qualité des données, qui souhaite faire progresser la maturité de la pratique de détection à La Caisse.

Ce que vous ferez

- Traduire les besoins de détection exprimés par le centre de sécurité opérationnelle et l'équipe de gestion des vulnérabilités en pipelines, règles et logique de détection exploitables par les analystes;
- Accompagner les équipes du SOC dans l'ingestion, l'organisation et l'exploitation des données nécessaires à la détection, à l'investigation, à la chasse aux menaces et à la gestion des incidents;
- Valider et ajuster en continu les règles de détection avec le SOC afin de réduire les faux positifs et d'améliorer la couverture ainsi que la fidélité des alertes;
- Assurer la fiabilité des pipelines de détection en s'appuyant sur des principes rigoureux d'ingénierie de données, notamment les flux ETL/ELT, la qualité, la fraîcheur et l'intégrité des données;
- Normaliser des sources de données hétérogènes vers des schémas communs exploitables par les outils et les cas d'usage de détection;
- Concevoir, mettre en œuvre, configurer et faire évoluer les pipelines de télémétrie de sécurité, incluant les journaux, les événements et les métriques;
- Mettre en place et maintenir les intégrations nécessaires à l'ingestion et au routage des données vers les systèmes appropriés, notamment les plateformes MDR, SIEM, les lacs de données, les moteurs analytiques et les outils de détection;
- Assurer la qualité, l'intégrité, l'immuabilité et la gouvernance des données de sécurité tout au long de leur cycle de vie;

- Déployer, configurer et maintenir les agrégateurs, les plateformes et les intégrations de renseignements de cybermenaces;
- Travailler de concert avec le responsable de la pratique AIS et les architectes de sécurité afin d'aligner les solutions sur la vision analytique et les orientations technologiques de l'organisation;
- Contribuer à la maturation de la pratique de détection en définissant et en suivant des indicateurs de performance tels que le taux de couverture, la qualité des détections, le taux de faux positifs et le délai de mise en production des cas d'usage.

Ce qui vous distingue

- Capacité à traduire les besoins opérationnels du SOC en cas d'usage et en logique de détection concrets et exploitables;
- Aptitude à travailler de façon transversale avec le SOC, les équipes de gestion des vulnérabilités et les architectes de sécurité tout en maintenant une rigueur d'ingénierie;
- Sens de la priorisation basé sur le risque, notamment pour orienter la couverture de détection en fonction des vulnérabilités critiques;
- Rigueur et souci constant de la qualité des données comme fondement des capacités de détection;
- Leadership mobilisateur permettant de faire progresser la maturité et la performance de la pratique de détection.

Ce que vous apportez

- Diplôme universitaire en informatique, cybersécurité, génie logiciel, science des données ou dans un domaine connexe;
- Minimum de dix (10) années d'expérience en sécurité de l'information;
- Minimum de cinq (5) années d'expérience en gestion des vulnérabilités, journalisation et surveillance, ainsi qu'en gestion des menaces;
- Expérience démontrée en ingénierie de détection, incluant la conception de règles ou de cas d'usage et la collaboration directe avec un centre de sécurité opérationnelle (SOC);
- Minimum de deux (2) années d'expérience pertinente en ingénierie de données, en télémétrie de sécurité, en plateformes analytiques ou en architecture de pipelines;
- Connaissance démontrée des concepts de gouvernance des données, d'ETL/ELT, de qualité des données et de normalisation;
- Expérience avec des solutions de collecte et d'agrégation de journaux, des plateformes de renseignements sur les cybermenaces (CTI), des lacs de données ou des environnements analytiques tels que Databricks, Snowflake ou Cribl;
- Bonne compréhension des cadres de détection, notamment MITRE ATT&CK;, ainsi que des pratiques de gestion des vulnérabilités;
- Excellentes habiletés de communication, de vulgarisation et de collaboration auprès d'équipes multidisciplinaires;
- Expérience de travail dans un environnement Agile;
- Maîtrise du français et de l'anglais*, tant à l'oral qu'à l'écrit;

* Interactions fréquentes en anglais à l’oral et à l’écrit avec des partenaires externes basés à l’extérieur du Québec tels que des fournisseurs de services, des cabinets avocats, des pairs, des banquiers, firmes de courtage, firmes d’analyse de crédit et agences de crédit, etc.