Titre : Premier(-ère) conseiller(-ère), Cyberdéfense

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/R05114?utm_source=Centre+des+femmes+de+Montr%C3%A9al&source=Centre+des+femmes+de+Montr%C3%A9al

NOC ID : 21220

NOC JOB TITLE : conseiller/conseillère en sécurité des technologies de l'information (TI)

Au sein du Centre de sécurité opérationnelle, la personne titulaire joue un rôle de premier plan dans la protection des capacités d'affaires essentielles de La Caisse et dans l'évolution de ses capacités de cyberdéfense. Relevant du chef, Centre de sécurité opérationnelle, elle agit comme référence technique pour les activités de détection, d'investigation, de chasse aux menaces et de réponse aux incidents.

Elle contribue à faire évoluer le SOC vers un modèle davantage proactif, automatisé et fondé sur le renseignement, les données et une utilisation responsable de l'intelligence artificielle. Elle exerce un leadership d'influence auprès de ses collègues et soutient le développement des pratiques de l'équipe.

- Faire évoluer les capacités de détection en concevant, testant, documentant et optimisant des cas d'usage et des règles de détection, notamment en les alignant sur MITRE ATT&CK; et sur les scénarios de menace pertinents pour La Caisse;
- Mesurer et améliorer la couverture et la qualité des détections, notamment par la validation continue, l'analyse des angles morts, la réduction des faux positifs et l'exploitation des constats découlant des incidents et des exercices;
- Optimiser les processus de réponse aux incidents par l'automatisation, l'orchestration et l'enrichissement contextuel, tout en maintenant une validation humaine appropriée pour les décisions à incidence élevée;
- Exploiter de façon responsable les capacités d'intelligence artificielle et d'analytique avancée afin d'accélérer le triage, la corrélation, la recherche, la création de chronologies et la production de comptes rendus, en tenant compte de la confidentialité, de la traçabilité et du risque d'erreur;
- Agir comme référence technique du SOC et prendre en charge les investigations et incidents de sécurité, de l'analyse initiale jusqu'au confinement, à l'éradication, au rétablissement et au retour d'expérience;
- Orienter et réaliser des activités de chasse aux menaces fondées sur des hypothèses, le renseignement de sécurité, les comportements adverses et la connaissance des actifs critiques;
- Soutenir la préparation et l'exécution d'exercices de simulation, de tests de scénarios et de revues après incident, puis assurer le suivi des améliorations convenues;

Contribuer à l'intégration opérationnelle des nouvelles solutions, sources de télémétrie et capacités de sécurité.

Ce que vous ferez

- Produire une documentation claire et durable, incluant les playbooks, runbooks, procédures d'enquête, rapports techniques, leçons apprises et recommandations de réduction du risque;

- Effectuer une veille structurée sur les menaces, les techniques adverses et l’évolution des pratiques SOC, puis transformer les constats pertinents en améliorations concrètes et priorisées;
- Soutenir la couverture continue des opérations, agir comme point d’escalade technique et contribuer à la coordination des partenaires de services de sécurité lors d’incidents;
- Contribuer à l’intégration opérationnelle des nouvelles solutions, sources de télémétrie et capacités de sécurité;
- Soutenir la préparation et l’exécution d’exercices de simulation, de tests de scénarios et de revues après incident, puis assurer le suivi des améliorations convenues;

Ce qui vous distingue

- Intérêt marqué pour la cybersécurité et l'actualité qui y est liée;
- Rigueur, autonomie, initiative et capacité à exercer un jugement éclairé dans des contextes complexes;
- Intégrité, discrétion et haut niveau d’éthique dans la gestion de dossiers sensibles;
- Capacité à gérer simultanément plusieurs priorités dans un environnement opérationnel en constante évolution;
- Excellentes habiletés de communication et aptitude à vulgariser des concepts techniques auprès de différents publics;
- Esprit d'équipe favorisant la collaboration et le partage de connaissances.

Ce que vous apportez

- Diplôme universitaire en cybersécurité, informatique ou dans un domaine connexe, ou combinaison équivalente de formation et d’expérience pertinente;
- Minimum de sept (7) années d’expérience technique en cyberdéfense, incluant une expérience approfondie en surveillance, détection, investigation, chasse aux menaces et réponse aux incidents dans des environnements SOC;
- Expérience démontrée dans la prise en charge d’incidents complexes et dans l’accompagnement technique de collègues;
- Maîtrise de Microsoft Sentinel et de Microsoft Defender XDR, incluant Defender for Endpoint, Defender for Office 365 et Defender for Identity;
- Très bonne maîtrise de KQL et expérience en conception, optimisation et validation de détections;
- Expérience dans des environnements infonuagiques Azure et AWS ainsi qu’en sécurité réseau, notamment avec des technologies Palo Alto;
- Expérience pratique de l’automatisation des opérations de sécurité à l’aide de capacités SOAR, de scripts ou d’API;
- Connaissance pratique de MITRE ATT&CK;, des méthodes d’analyse d’incidents et des principes de collecte et de préservation des éléments de preuve;
- Maîtrise du français, tant à l'oral qu'à l'écrit.

Exigences souhaitées : certifications en sécurité informatique (CISSP, CISM, GIAC), certifications Microsoft pertinentes, certification AWS Certified Security - Specialty ou expérience équivalente, expérience en forensique, rançongiciels, compromission d’identité, sécurité infonuagique ou investigation de menaces

internes, connaissance du secteur financier et de ses exigences en matière de résilience opérationnelle, de gestion du risque et de cybersécurité.

Sentir que mon rôle est important. Avoir du plaisir au quotidien. Pouvoir évoluer au rythme de mes ambitions. Obtenir une rémunération à la hauteur de ma contribution. C’est l’expérience professionnelle que m’offre La Caisse!