Titre : Chef(-fe) d’équipe, Centre de sécurité opérationnelle

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/R04966?utm_source=Centre+des+femmes+de+Montr%C3%A9al&source=Centre+des+femmes+de+Montr%C3%A9al

NOC ID : 21220

Titre NOC : chef de projet en technologies de l'information (TI) - cybersécurité

Au sein de l’équipe, Centre de sécurité opérationnelle et gestion des identités, la personne titulaire joue un rôle de premier plan dans la protection des capacités d'affaires essentielles de La Caisse et la performance des opérations de sécurité.

Elle agit à titre de responsable de l’équipe du SOC en assurant la coordination, la planification et le pilotage des activités quotidiennes, tout en étant le point de référence technique et opérationnel et en collaborant étroitement avec le directeur principal.

Ce que vous ferez

- Planifier, organiser et diriger les activités et les tâches courantes de l'équipe du SOC, en assurant une répartition efficace de la charge de travail et le respect des priorités opérationnelles;
- Assurer la gestion et le développement de l’équipe en réalisant les évaluations de performance, en offrant du coaching et du mentorat et en favorisant l’engagement et la progression des talents;
- Concevoir, produire et suivre les indicateurs de performance clés (KPI) liés à la sécurité opérationnelle, en produisant des tableaux de bord et des rapports périodiques;
- Gérer les demandes de services émanant des clients internes et externes, en établissant les priorités opérationnelles et en assurant le respect des niveaux de service convenus;
- Gérer la performance et la relation avec les fournisseurs de services de sécurité gérés, incluant la revue des livrables et l'évaluation continue de la qualité des services rendus;
- Agir comme point d'escalade technique pour les incidents complexes et les situations nécessitant une prise de décision rapide;
- Contribuer à la veille technologique quant à l'évolution des outils, des menaces et des meilleures pratiques en matière de cyberdéfense, et formuler des recommandations d'adoption ou d'évolution;
- Fournir une vision ainsi que des recommandations tactiques et stratégiques sur les capacités de sécurité de l'organisation, en identifiant les lacunes, les opportunités d'amélioration et les tendances émergentes;
- Accélérer la transformation des opérations grâce à l’automatisation, l’analytique avancée, l’intelligence artificielle et l’intégration des renseignements de sécurité;
- Participer activement au déploiement de nouvelles initiatives, solutions et fonctionnalités de cybersécurité dans l'écosystème technologique du SOC;

- Animer les rencontres d'équipe et favoriser un environnement de collaboration, de rigueur et d'amélioration continue.

Ce qui vous distingue

- Leadership mobilisateur favorisant l’autonomie, l’engagement et la performance de l’équipe;
- Intérêt marqué pour la cybersécurité, les risques émergents et l'actualité qui y est liée;
- Rigueur, autonomie et capacité à prendre des décisions éclairées sous pression;
- Capacité à gérer simultanément plusieurs initiatives tout en maintenant un haut niveau de qualité;
- Excellentes habiletés de communication permettant de vulgariser des concepts techniques auprès de différents publics;
- Esprit de collaboration, sens du mentorat et contribution active au développement des collègues;
- Orientation client et compréhension des enjeux d’affaires liés aux demandes de sécurité.

Ce que vous apportez

- Diplôme universitaire en cybersécurité, informatique ou domaine connexe;
- Minimum de dix (10) années d'expérience technique en cyberdéfense, incluant la surveillance, la détection, l'investigation, la réponse aux incidents, la chasse aux menaces et le renseignement de sécurité dans des environnements SOC, dont au moins trois (3) années dans un rôle de coordination, de leadership technique ou de gestion d'équipe;
- Expérience démontrée en gestion de fournisseurs de services de sécurité et en suivi de la performance;
- Expérience des solutions Microsoft Sentinel et Microsoft Defender (MDO, MDE, MDI), sur les environnements infonuagiques AWS et Azure et expertise en sécurité réseau, notamment sur les solutions Palo Alto;
- Maitrise du français et de l’anglais, tant à l’oral qu’à l’écrit;
- Certifications en sécurité informatique : CISSP, CISM, GIAC (GCIH, GCIA, GSOM), CSA;
- Certifications Microsoft : Azure Security Engineer, Microsoft Certified: Security Operations Analyst;
- Certifications AWS : AWS Certified Security – Specialty, AWS Certified Cloud Practitioner;
- Expérience avec des cadres de référence tels que NIST CSF, MITRE ATT&CK;, ISO 27001;
- Connaissance du secteur financier et de ses exigences réglementaires en matière 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!

Nous consultons avec attention chaque candidature et nous contacterons directement les personnes retenues pour une entrevue.

La Caisse offre des chances d’emploi égales à tous et toutes. Elle invite les femmes, les membres des minorités visibles et ethniques, les personnes autochtones et les personnes handicapées à présenter leur candidature. Si cette offre d’emploi vous motive, mais que vous ne correspondez pas à tous les critères, contactez-nous quand même!

La Caisse s’engage à promouvoir l’équité, la diversité et l’inclusion comme valeur clé et en fait une source d’enrichissement pour tous les membres de l’organisation. Veuillez nous informer si votre condition nécessite des mesures d’adaptation pendant le processus de recrutement.

La Caisse représente la Caisse de dépôt et placement du Québec et ses filiales.