Titre d’emploi: Coordonnateur SOC

OFFRE D'EMPLOI

Demande N°: 10849

Titre: Coordonnateur, SOC (Security Operation Center)
Supérieur: Directeur, Sécurité de l'information et transformation TI
Lieu de travail: Siège social
Statut: Indéterminé, temps plein
Groupe d'employés: assujeti à la convention collective des employés administratifs, professionnels et du soutien administratif
Échelle salariale: classe 10
Date d'affichage du 7 mai 2024
Motif de l'affichage: Nouveau poste

SOMMAIRE

Relevant du Directeur, sécurité de l’information et transformation TI, le Gestionnaire de Centre Opérationnel de Sécurité (SOC Manager) est responsable des processus de surveillance des événements de sécurité, de la supervision du traitement des incidents de sécurité, dans les sphères des Technologies de l’Information (TI) et des Technologies Opérationnelles (TO).

RÔLE ET RESPONSABILITÉS

- Définir la stratégie, la gouvernance et les processus de supervision de sécurité TI et TO;
- Définir la stratégie, la gouvernance et les processus de gestion des incidents de sécurité TI et TO;
- Surveiller le niveau de service du Centre Opérationnel de sécurité (SOC), confié à un partenaire spécialisé;
- Gérer les requis de maintenance et d’évolution de la plateforme SIEM (Security information and event management);
- Superviser et contribuer à la définition et la mise à jour des cas d’usage (use cases) et plans de traitement (workbooks) du SOC;
- Proposer des améliorations aux outils et processus de sécurité d’ADM afin d’accroitre la posture de sécurité et limiter le nombre d’événements de sécurité;
- Contribuer au suivi et à la gestion des risques TI et TO au sein d’ADM;
- Effectuer une surveillance du partenaire en charge des opérations de sécurité : contrôles par échantillonnage des incidents traités, surveillance des plateformes de sécurité, tests de vigilance de l’infogérant...;
- Effectuer une surveillance ciblée des outils de sécurité afin de détecter des tentatives d’attaques avancées (threat hunting);
- Contribuer aux spécifications des attentes pour les évolutions de nos solutions de sécurité (DLP, VPN, pare-feu, etc.);
- Aider à la résolution des incidents de sécurité « complexes » et gestion des partenaires pour la résolution et la clôture de ces incidents;
- Synthétiser les informations pertinentes relatives aux activités de cybersécurité pour communication aux Vice-Présidents, Président et au Conseil d’Administration;
- Contribuer à l’élaboration de la stratégie de cybersécurité, de la feuille de route et des encadrements de sécurité d’Aéroports de Montréal (directives, politiques, standards, etc.);
- Apporter une contribution à d’autres chantiers, projets et processus relatifs à la cybersécurité;
- Peut être appelé à représenter ADM dans le cadre de différents forums;
- Effectue toutes autres tâches connexes à la fonction.

EXIGENCES

- Détenir un baccalauréat en technologies de l’information ou dans une discipline connexe;
- Psséder un minimum de six (6) ans d’expérience dans le domaine de la cybersécurité;
- Détenir une certification en matière de sécurité (ISO 2700X, CISSP, PCI DSS...) pourrait être considéré comme un atout important;
- Expérience en sécurité des Technologies Opérationnelles (automates, systèmes industriels, IoT, etc);
- Avoir une bonne aptitude aux travaux conceptuels : définition de processus, principes de gestion des risques, etc.
- Avoir de bonnes aptitudes à l’apprentissage et à l’acquisition de nouveaux savoir-faire;
- Avoir de bonnes aptitudes de gestion du stress et des priorités et avoir de bonnes compétences en matière d’analyse et de résolution de problèmes.
- Bonnes capacités de communication, de synthèse et de vulgarisation des concepts complexes;
- Expérience significative en centre de sécurité opérationnelle;
- Excellentes capacités d’analyse/habiletés en résolutions de problèmes;
- Capacité à comprendre la réalité d’affaires des différentes entités d’ADM;
- Maîtrise du français (parlé et écrit);
- Bonnes aptitudes en anglais (parlé et écrit);
- Esprit d’équipe;
- Capacité de planification, d’organisation et de priorisation;
- Passer avec succès la cote d’enquête pour l’obtention du laisser-passer pour zones réglementées.

Ce concours est ouvert simultanément à l'interne et à l'externe; cependant, les candidatures provenant de l'interne seront traitées en priorité.

Nous vous remercions de l'intérêt porté envers ADM.