COMMISSIONNAIRES
FIABLE · EN TOUT TEMPS · EN TOUT LIEU

OPERATEUR– CENTRE DES OPÉRATIONS DE SÉCURITÉ DU CCC MTL

SOMMAIRE

En tant qu'opérateur de niveau 1, vous serez intégré à une équipe au sein du Centre des opérations de sécurité (SOC) du Corps canadien des commissionnaires de Montréal (CCC Mtl) afin de fournir une surveillance 24h/24 et 7jours/7 des réseaux d'un ou plusieurs de ses clients.

Date d'entrée en fonction : 1 novembre 2017

ATTRIBUTIONS ET RESPONSABILITES

- Surveiller les alertes, événements et incidents identifiés grâce aux outils de détection.
- Utiliser des outils de support standards afin d'effectuer un premier triage des comportements détectés.
- Différencier les faux-positifs des tentatives réelles d'intrusion ou de comportements dangereux ou suspicieux.
- Collecter les informations en support des analystes niveau 2.
- Mettre à jour les procédures et la base de connaissances suite aux premières investigations effectuées.
- Escalader les alertes aux analystes niveau 2 si besoin.
- Ouvrir, tracer et clôturer les tickets d'incident résultant du triage et des investigations dans l'outil de gestion des incidents.
- Communiquer par téléphone ou par email et agir en accord avec les procédures de gestion des incidents de sécurité.
- Enregistrer les demandes lorsque le SOC reçoit des appels de la part des clients.
- Produire les rapports quotidiens et ponctuels.
- Investiguer activement sur les récentes vulnérabilités de sécurité, les conseils, les incidents et les intrusions.
- Fournir des retours pour le développement des futurs buts et objectifs pour le département et les services proposés.
- Participer à l'amélioration des processus afin d'optimiser les opérations du SOC.
- Participer à l'amélioration et au développement des manuels de procédure et à la documentation du SOC.
- Suivre scrupuleusement les procédures du département.
- Participer au partage de connaissance avec les autres membres de l'équipe.
- Coordonner ou participer à des projets individuels ou en équipe.
- Écrire des articles techniques pour la base de données de connaissance interne.
- Suivre le plan d'assurance qualité du département.

Nous contacter

Commissionnaires du Québec
201 Avenue Laurier E, Montréal,
QC, H2T 3E6 (Jusqu'au 20 octobre)

1001 Sherbrooke Est, Montreal,
QC, H2L 1L3 (À partir du 20 octobre)

(514) 273-8578 poste 250
Recrutement@cccmtl.ca

QUALITES REQUISES

Études :

- Diplôme d'études secondaires.
- Formation ITIL foundations serait un avantage.
- Une certification Cisco CCNA serait un avantage.
- Une certification CISSP serait un avantge

Expérience :

- Expérience dans un environnement de Services Informatiques ou de supervision d'équipements réseau.

Souhaitable

- Connaissance des équipements typiques de protection d'un réseau tel que :
  SIEM, Firewalls, Security Gateway/Web Proxy, NIDS/NIPS, HIDS/HIPS, etc.
- Compréhension des protocols de réseau et et d'application commun tel que :
  TCP/IP, UDP, HTTP/HTTPS, FTP, ICMP, SMTP
- Connaissance de base d'une architecture de sécurité incluant l'encryption, l'encodage, les partages réseau, les serveurs Web, etc.
- Être capable d'interpréter les différents journaux de Windows (événements, applications, services. etc).
- Être capable de communique efficacement avec ses pairs et produire des rapports pour les différents niveaux.
- Avoir un esprit analytique développé, être capable de porter attention au détail et être un fervent de la sécurité cybernétique.
- Expérience de travail dans un environnement TI et préférablement dans le domaine de la sécurité.
- Capable de travailler de façon autonome.
- Avoir une attestation de sécurité de niv II ou être disposé à suivre les procédures pour obtenir une attestation de sécurité niv II.

CONDITIONS D'EMPLOI

Statut de l'emploi : Contrat

Horaire : Temps plein

Quarts de travail : Jour au début, quart de travail par la suite

Nombre d'heures par semaine : 40

*La forme masculine est utilisée sans discrimination uniquement dans le but d'alléger le texte