Titre du poste : **Analyste principal, Sécurité informatique**
Lieu de travail : **Montréal**
Type d'emploi : **Permanent**

Otéra Capital est un chef de file en financement immobilier commercial, réputé pour son expertise, son professionnalisme et sa fiabilité. Nous rassemblons des spécialistes du financement immobilier commercial qui allient une expertise de pointe en matière de financement hypothécaire à une connaissance approfondie des marchés immobiliers où nous investissons.

Nous sommes une filiale de la Caisse de dépôt et placement du Québec, l'un des plus importants gestionnaires de fonds institutionnels au Canada.

Le succès d'Otéra repose en grande partie sur le talent de son capital humain. Voilà pourquoi l'accent est mis sur le développement et l'autonomie de tous ses employés en leur proposant de nombreuses occasions d'apprentissage et de croissance. Grâce à une rémunération et des avantages sociaux compétitifs, ainsi qu'à des programmes axés sur la santé et le bien-être, nos employés arrivent à concilier travail et vie personnelle. Nous offrons un environnement à la fois stimulant et dynamique fondé sur l'ouverture, la poursuite de l'excellence, le travail d'équipe et l'engagement. Nous accordons également une grande importance à la responsabilité sociale de l'organisation et nos employés ont fréquemment la chance d'y participer.

VOTRE RÔLE

Vous avez un sens de l'analyse développé? vous êtes reconnu pour votre souci du détail? Voici une excellente occasion de mettre de l'avant votre expertise en sécurité informatique en vous joignant à une équipe dynamique qui joue un rôle important dans le succès de notre organisation.

Relevant de la directrice principale, Systèmes d'information, l'analyste principal, Sécurité informatique, a pour mandat d'identifier et étudier les failles du système informatique et d'apporter des solutions de protection afin de sécuriser les données. Le titulaire du poste est responsable de la gestion des mots de passe, des antivirus, de la cryptologie, des pare-feu, des limitations aux accès d'information et autres. L'analyste principal doit s'assurer de la pérennité des dispositifs, et les actualiser en fonction des dernières technologies et des réglementations. En collaboration avec d'autres directions, il participera à la formation du personnel de l'entreprise et à la sensibilisation au respect des processus en matière de protection des données.

VOS PRINCIPALES RESPONSABILITÉS

- Développer une vision globale du système d'information;
- Identifier, analyser et prioriser les vulnérabilités et les non-conformités de l'infrastructure technologique et assurer une veille permanente et une vigie continue sur l'évolution des cybermenaces et de leurs contre-mesures;
- Supporter les équipes de gestion de risque et de conformité dans leurs travaux;
- Assurer le suivi et la mise en œuvre des politiques et normes organisationnelles et des processus SI relativement à la sécurité des systèmes d'information et au plan de continuité des affaires (PCA);
- Piloter les projets de mise en œuvre de la sécurité (infrastructures internes/ hébergées/infonuagiques, réseau, systèmes, plans d'action correctifs des recommandations d'audit interne);
- Participer à la conception et la définition des architectures de sécurité (réseau, téléphonie et Datacenters) et des processus d'exploitation, afin de décliner opérationnellement la politique de sécurité SI Client sur les infrastructures internes et externalisées;
- Participer aux activités du plan de relève informatique et du PCA et contribuer aux activités de sensibilisation auprès des équipes dans le domaine de la sécurité;
- Installer, tenir à jour et gérer les outils et technologies de sécurité de l'information (y compris les systèmes d'information de sécurité/gestion d'événement [SIEM] les systèmes de prévention d'intrusion [IPS] ou systèmes de détection d'intrusion [IDS] les logiciels anti-programme malveillants les scanneurs de gestion de la vulnérabilité, les pare-feu, DLP etc.);
- Gérer les éventuels incidents qui surviendraient, traiter et mettre en place des solutions autour des incidents de sécurité pour éviter leur répétition;
- Participer à l'identification et la gestion des impacts que les changements de processus et de systèmes amènent dans l'organisation.

VOTRE PROFIL

- Baccalauréat en informatique ou équivalent avec une spécialisation en sécurité informatique;
- Certification CISSP, CISA ou CISM, un atout;
- Minimum de 10 années d'expérience dans le domaine des TI dont un minimum de 5 années dans le domaine de la sécurité TI;

- Excellente maîtrise du français et de l'anglais, oral et écrit;
- Solides connaissances des pratiques ISO 27001, NIST, COBIT 5 etc.;
- Excellentes connaissances techniques dans le développement des systèmes, l'administration des réseaux et les normes de sécurité;
- Capacité à avoir une vision synthétique et globale du système d'information, des processus de l'entreprise et des profils utilisateurs, externes ou internes;
- Esprit de synthèse et sens analytique développés;
- Capacité à travailler de manière autonome;
- Excellent esprit d'équipe et de collaboration,
- Sens de l'organisation, de la planification et de l'établissement des priorités et des échéanciers;
- Capacité à prendre des initiatives et proposer des solutions novatrices et créatives;

- Fortes habiletés d’adaptation au changement;
- Souci du travail bien fait.

L’utilisation du genre masculin est adoptée afin d’alléger la structure du texte et n’a aucune intention discriminatoire. Otéra Capital souscrit au principe d’équité en matière d’emploi et encourage la diversité et l’inclusion. Nous encourageons tous les candidats qualifiés à postuler. Seuls les candidats sélectionnés pour une entrevue seront contactés.

Veuillez faire parvenir votre curriculum vitæ à :

Otéra Capital
cvrh@oteracapital.com
Centre de commerce mondial
413, rue Saint-Jacques - Bureau 700 Montréal (Québec) H2Y 1N9