INGÉNIEUR(E) EN CYBERSÉCURITÉ

Vous souhaitez rejoindre une organisation qui?

- Joue un rôle important dans la sécurité de l'espace aérien mondial ?
- Possède plus de 35 ans d'expérience dans la fourniture de systèmes de formation par simulation au contrôle de la circulation aérienne (ATC) de premier plan et de solutions de gestion du trafic aérien (ATM) à la fine pointe de la technologie ?
- Offre un programme de remboursement des frais de formation liés à l'emploi ainsi que l'accès à diverses possibilités de perfectionnement professionnel ?
- Propose des programmes favorisant l'équilibre travail-vie personnelle ainsi qu'un régime complet d'avantages sociaux entièrement personnalisable selon vos besoins particuliers ?

Si cela vous semble intéressant, continuez à lire notre offre d'emploi ci-dessous.

Résumé du poste:

L'ingénieur(e) en cybersécurité ATM contribue à la conception, à l'évaluation, à l'intégration et à l'assurance tout au long du cycle de vie de systèmes de gestion du trafic aérien sécurisés et résilients, des environnements d'ingénierie et des plateformes opérationnelles déployées chez les clients. Le rôle combine l'analyse pratique des vulnérabilités, l'architecture de sécurité et l'ingénierie des systèmes conformément aux réglementations de cybersécurité ATM. L'ingénieur(e) identifie et valide les vulnérabilités, évalue les risques liés à la sécurité de l'information dans le contexte de la continuité opérationnelle et de la sûreté des systèmes, traduit les obligations de sécurité de l'information en exigences techniques vérifiables et collabore avec les équipes de logiciels, systèmes, réseaux, infrastructure, sûreté, qualité, projets et TI/TO afin d'élaborer des mesures concrètes de correction et d'atténuation. Le poste contribue à toutes les étapes, de l'analyse des propositions et des exigences à l'architecture, la mise en œuvre, l'intégration, la vérification, le déploiement, la maintenance et la gestion contrôlée des changements.

Tâches et responsabilités essentielles:

- Évaluation des vulnérabilités et validation autorisée:

- Identifier, valider et évaluer la criticité des vulnérabilités dans les plateformes et applications ATM.
- Évaluer l'exposition, la criticité des actifs, les mesures compensatoires, la continuité opérationnelle, la reprise et les répercussions potentielles sur la sûreté.

- **Évaluation des exigences de sécurité et de l'architecture:**
  - Traduire les obligations de sécurité de l'information et de cybersécurité des clients, des produits, des contrats, des règlements et de l'organisation en exigences claires, testables et traçables.
- **Conception sécurisée et ingénierie de remédiation:**
  - En collaboration avec les ingénieurs systèmes et l'architecte de solutions, élaborer des contrôles de sécurité et des mesures de remédiation pour les logiciels, systèmes, réseaux, infrastructures et sites clients.
  - Traiter les causes profondes au moyen de mesures proportionnées telles que la segmentation, les communications sécurisées, le contrôle des accès privilégiés, le renforcement des systèmes, la journalisation et la surveillance, la sauvegarde et la reprise, la résilience et le principe du moindre privilège, tout en maintenant les performances, la disponibilité, l'interopérabilité, la maintenabilité et la sûreté des systèmes ATM.
- **Vérification, clôture et traçabilité:**
  - Définir et valider les preuves de clôture des mesures correctives.
  - Vérifier la mise en œuvre au moyen d'activités de vérification appropriées.
  - Maintenir la traçabilité entre les exigences, les constats, les mesures correctives, les configurations de référence et les dossiers de vérification.
  - Consigner les mesures compensatoires et les risques résiduels acceptés.
- **Rapports techniques et communication avec les parties prenantes:**
  - Produire des évaluations concises et exploitables à l'intention des parties prenantes techniques et non techniques.
- **Soutien aux propositions:**
  - Collaborer avec les équipes d'ingénierie, de produits et de sûreté afin d'élaborer des propositions concurrentielles et conformes.
- **Co-ingénierie de la cybersécurité et de la sûreté ATM:**
  - Collaborer avec les spécialistes de la sûreté des systèmes et de l'ingénierie afin d'identifier les conditions cyber susceptibles d'affecter la sûreté, l'intégrité, la disponibilité, la synchronisation, la redondance ou le service opérationnel.

Compétences:

Analyse conceptuelle: Prend en compte divers facteurs; s'intéresse à différents domaines; cherche à comprendre plusieurs champs d'activité; apprécie autant la théorie

que les sujets conceptuels et abstraits.

Pensée systémique: Pense à long terme; élabore des stratégies tenant compte d'un large éventail de facteurs, notamment l'évolution de l'organisation et du marché; sait prendre du recul et considérer la situation dans son ensemble.

Communication: Explique clairement des enjeux techniques complexes et adapte le niveau de détail aux responsables de la mise en œuvre, aux dirigeants de l'ingénierie, aux équipes de projet et à la direction.

Consultation de l'équipe: Accepte que ses opinions soient remises en question; consulte les membres de l'équipe lors de décisions qui les concernent; reconnaît la valeur de leurs points de vue et sollicite leur contribution.

Gestion des conflits: Gère les désaccords qui surviennent; défend ses positions; sait faire des concessions lorsque cela est approprié; recherche un compromis acceptable et, idéalement, des solutions gagnant-gagnant.

Qualifications:

Requises:

- Baccalauréat en cybersécurité, sécurité de l'information, informatique, génie informatique, génie des systèmes, génie logiciel ou dans une discipline technique connexe, ou expérience pertinente équivalente.
- De 3 à 6 ans d'expérience en ingénierie de la cybersécurité, évaluation des vulnérabilités, architecture de sécurité, sécurité des réseaux, ingénierie des systèmes ou dans un domaine connexe.
- Expérience des processus de gestion des risques, notamment l'analyse, l'évaluation et le traitement des risques.
- Solides aptitudes en analyse, collaboration, communication et rédaction de rapports, avec la capacité de travailler de façon autonome et de soumettre à un niveau supérieur les décisions complexes liées à l'architecture, à l'exploitation ou à l'acceptation des risques.
- Capacité à évaluer les changements en matière de sécurité de l'information et de cybersécurité en fonction des contraintes de disponibilité, de redondance, de performance, d'interopérabilité, de maintenabilité et de sûreté des systèmes, tant dans les environnements produits que dans ceux déployés chez les clients.
- Capacité à examiner les architectures système et réseau, les interfaces, les flux de données et les exigences techniques, et à traduire les risques identifiés en mesures concrètes de remédiation.

- Connaissance pratique de la gestion des vulnérabilités, de l'architecture sécurisée, de la modélisation des menaces, de la configuration sécurisée, de la sécurité des réseaux, de l'authentification et de l'autorisation, des principes fondamentaux de la cryptographie et de la prise de décision fondée sur les risques.
- Expérience pratique de l'évaluation des vulnérabilités, des revues de configuration et de sécurité, de l'analyse des éléments de preuve et de la validation des constats techniques.

Désirées:

- Expérience de la sécurisation d'environnements mixtes Windows et Linux, d'infrastructures virtualisées, d'équipements réseau et de systèmes tiers intégrés.
- Une expérience dans l'aviation, l'ATM, le contrôle industriel, le transport, la défense ou un autre domaine opérationnel à haute disponibilité est fortement valorisée.
- Expérience des technologies opérationnelles (TO), du contrôle industriel, des systèmes en temps réel, de l'aérospatiale, des services de navigation aérienne, de la gestion du trafic aérien ou d'autres environnements critiques pour la mission ou la sûreté.
- Connaissance des cadres et lignes directrices de sécurité tels que le NIST Cybersecurity Framework, le NIST Risk Management Framework, le NIST Secure Software Development Framework, ISO/IEC 27001, ISO/IEC 27005 ou toute méthodologie de gestion des risques, IEC 62443, MITRE ATT&CK, OWASP, Part-IS (UE 2022/1645 et UE 2023/203), ainsi que des pratiques reconnues d'architecture sécurisée.
- Expérience du suivi du cycle de vie des vulnérabilités, des registres de risques, des preuves de vérification de sécurité et de la documentation des exceptions ou des risques résiduels.
- Certifications pertinentes telles que Security+, CySA+, CISSCP, GSEC, certifications GIAC en évaluation des vulnérabilités ou tests d'intrusion, OSCP, ou formation pratique équivalente.

Autres qualifications:

- Capacité à respecter la politique d'Adacel relative à un milieu de travail sans drogue.
- Capacité à satisfaire aux vérifications d'antécédents d'Adacel pendant la durée de l'emploi.

Exigences physiques:

- Soulèvement occasionnel de charges allant jusqu'à 50 lb.
- Mouvements répétitifs du poignet, de la main et des doigts.

Environnement de travail:

- Lieu : Montréal.
- Statut d'emploi : permanent, à temps plein.
- Environnement de télétravail hybride.
- Horaire de travail alternatif (9/80 avec un vendredi sur deux de congé).
- Travail généralement effectué en position assise à un bureau.

Avantages:

- Jusqu'à 26 fins de semaine de trois jours par année grâce à l'horaire 9/80.
- Quatre semaines de vacances.
- REER de l'entreprise, RPDB (cotisation de l'employeur) et CELI.
- Programme d'assurance complet payé à 100 % par l'employeur dès le premier jour d'emploi.

Comment postuler:

- Vous pouvez postuler en envoyant votre curriculum vitæ par courriel à careers@adacel.com.careers@adacel.com
- Indiquez le titre du poste dans l'objet de votre message.

Clause de non-responsabilité:

Adacel souscrit au principe de l'égalité d'accès à l'emploi et à l'action positive. Toutes les personnes qualifiées seront considérées pour un emploi sans égard à la race, à la couleur, à la religion, au sexe, à l'orientation sexuelle, à l'identité de genre, à l'origine nationale, au handicap ou au statut d'ancien combattant protégé.

La présente description de poste reflète l'attribution par la direction des tâches et responsabilités essentielles. Elle ne limite pas les tâches et responsabilités qui peuvent être assignées. Des mesures d'adaptation raisonnables peuvent être mises en place afin de permettre aux personnes en situation de handicap d'accomplir les tâches et responsabilités essentielles. Si ce poste exige des déplacements, veuillez noter que leur fréquence peut augmenter à tout moment en fonction de l'évolution des besoins opérationnels d'Adacel.