Testia Canada – Consultant(e) intermédiaire en Cybersécurité GRC (H/F) – Mirabel

TESTIA GmbH

Région de Montréal (Québec), Canada

Temps plein · Permanent

Publié le 16 octobre 2026 · JR10451461

Aperçu du poste

Testia Canada - Consultante intermédiaire en cybersécurité (H/F) - Mirabel

Testia est une société internationale spécialisée dans l'intégrité et les inspections des aérostructures et du contrôle aéronautique non destructif.

Avec un réseau mondial, des bureaux en Europe, en Amérique du Nord et en Asie, Testia peut fournir ses services à l'échelle internationale et fournir des solutions globales aux besoins de l'industrie.

Avec un catalogue unique de services et de produits CND, Testia est votre partenaire complet pour la CND aéronautique. Nous proposons une large gamme d'équipements et de produits pour une analyse rapide et efficace des structures, des composants et des assemblages. Testia est également un centre de formation dans toutes les méthodes CND, tous niveaux, et offre également des services d'inspection, de conseil et d'ingénierie.

Nous recherchons actuellement un :

Consultant(e) en Cybersécurité GRC (H/F) - Mirabel

Contexte de la mission :

Vous rejoindrez nos équipes Cybersécurité en tant que Consultant Senior Gouvernance, Risques et Conformité (GRC) pour accompagner nos différents clients et partenaires (aéronautique, transport, énergie...) dans la définition, la gestion et la mise en œuvre des aspects de gouvernance, de risque et de conformité autour des problématiques de cybersécurité. Ce soutien se concentrera sur leurs entreprises, leurs environnements, leurs SI, mais aussi sur leurs produits.

Détails de la mission :

En tant que membre d'équipes multidisciplinaires, vos principales tâches seront :

Mise en œuvre des politiques et procédures de sécurité :

- Élaborer et mettre en œuvre des politiques et des procédures de sécurité pour l'ensemble de l'organisation.
- Veiller à ce que les politiques et procédures soient conformes aux réglementations et aux meilleures pratiques en matière de cybersécurité.
- Sensibiliser les employés aux politiques de sécurité et les former aux bonnes pratiques.

Conformité réglementaire :

- Veiller à la conformité de l'organisation aux réglementations de cybersécurité.

- Fournir une expertise sur les règlements et les normes (par exemple NIST, LPCE, CMMC, CIRCIA, projet de loi C-26, loi 25, ISO 27001).
- Effectuer des audits internes pour vérifier la conformité et recommander des améliorations.

Évaluation des risques et élaboration de stratégies de sécurité :

- Effectuer régulièrement des évaluations des risques (EBIOS RM, ISO 27005) pour fournir une vision claire des menaces et orienter les choix d'investissement.
- Participer à l'élaboration de stratégies de sécurité avec les équipes internes et les parties prenantes, et proposer des mesures correctives.

Gestion des incidents de sécurité :

- Participer à l'élaboration des plans de gestion des incidents et coordonner les activités d'intervention.
- Mener des enquêtes sur les incidents de sécurité et fournir des rapports détaillés.

Architecture de sécurité :

- Participer à la stratégie des architectures de sécurité des produits et appliquer des modèles de référence pour les systèmes embarqués ou critiques.
- Accompagner les projets en conception architecturale, préciser les paramètres et définir les exigences techniques de sécurité.
- Conseiller sur le choix des solutions techniques, plaider pour des architectures sécurisées et décliner les exigences tout au long du cycle de vie du produit.

Profil recherché :

- Diplôme universitaire ou d'école d'ingénieur avec une majeure en informatique / cybersécurité, OU expérience significative équivalente en cybersécurité.
- Minimum de 5 ans d'expérience en gestion des risques, gouvernance et/ou audit.
- Connaissance approfondie des cybermenaces, des attaques (TTP) et des vulnérabilités.
- Bonne connaissance des normes et réglementations applicables (notamment en Amérique du Nord : NIST, LPCE, CMMC, CIRCIA, projet de loi C-26, ISO 27001).
- Maîtrise des principes de sécurité défensive (architectures de produits, systèmes, informatique) et solide connaissance globale de la sécurité de l'information (PKI, cryptographie, durcissement, protocoles réseau, cycle de vie des produits).
- Autonomie globale, capacité à gérer plusieurs projets simultanément, à arbitrer les conflits et à prendre des décisions.
- Un esprit d'organisation analytique, synthétique et rigoureux.
- Excellente communication et pédagogie pour jouer un rôle de facilitateur avec les équipes techniques et la direction.
- Niveau avancé requis en français et en anglais (écrit et oral).

Informations sur l'offre:

- Contrat : CDI
- Date de début : Dès que possible
- Lieu : Mirabel
- Rémunération : selon le profil et/ou l'expérience et les avantages Testia ci-dessous

Le poste demande de reconnaître les risques de conformité et d’agir avec intégrité. Airbus considère ces exigences comme essentielles à sa réussite, à sa réputation et à sa croissance durable.

Entité juridique

TESTIA GmbH

Type de contrat:

Permanent

Niveau d’expérience

Professionnel

Famille d’emplois

La soumission d’un CV ou d’une candidature autorise Airbus à utiliser et à conserver les renseignements de la personne pour le suivi de sa candidature ou d’un emploi futur. Airbus est le seul utilisateur de ces renseignements.

Airbus favorise un milieu de travail inclusif et diversifié. L’entreprise accueille les candidatures sans distinction de milieu social ou culturel, d’âge, de sexe, de handicap, d’orientation sexuelle ou de croyances religieuses.

Airbus applique l’égalité des chances et ne demande aucun paiement pendant le recrutement. L’entreprise invite à signaler toute usurpation de son identité.

Airbus facilite le travail et la collaboration. L’entreprise privilégie des modalités souples lorsque les activités le permettent afin d’encourager l’innovation.