Spécialiste, plateformes de cyberdéfense

Air Canada

Dorval (Québec), Canada

Lieux annoncés · DORVAL, QUÉBEC, CANADA; TORONTO, ONTARIO, CANADA

Temps plein · Solutions numériques et technologie

Publié le 25 novembre 2026 · Poste 40321

Candidatures jusqu’au 29 novembre 2026

Air Canada, un symbole canadien récemment nommé meilleur transporteur aérien en Amérique du Nord, invite les candidats à rejoindre une équipe diversifiée qui innove dans le transport aérien de passagers.

En tant qu’autorité technique reconnue au sein de la fonction Cyber Défense, le spécialiste dirige la conception, le déploiement, l’intégration, l’optimisation et l’évolution de plateformes de sécurité complexes, développe des feuilles de route, des normes et des solutions pour les plateformes et fait preuve d’un jugement indépendant sur des questions techniques et opérationnelles complexes. Le poste assure un leadership technique dans les initiatives de cyberdéfense et influence les décisions sur l’architecture, les investissements technologiques et les risques pour s’assurer que les capacités de cybersécurité restent sécurisées, résilientes, entièrement déployées et opérationnelles pour les experts en cyberdéfense et les équipes d’opérations de sécurité. Les technologies clés comprennent l'écosystème Palo Alto Networks, Koi Security, Microsoft Defender, la sécurité des e-mails, ainsi que les services d'infrastructure à clé publique et de gestion des certificats.

Le poste peut être basé à Montréal ou à Toronto.

Responsabilités du poste

- Assumer la responsabilité du cycle de vie de bout en bout, de la direction technique et de l’efficacité opérationnelle des plateformes de cybersécurité d’entreprise assignées couvrant les terminaux, les identités, les applications, les services cloud et l’infrastructure, afin que les capacités restent sécurisées, résilientes, évolutives et opérationnelles.
- Élaborer et mettre en œuvre des feuilles de route de la plateforme, des plans de cycle de vie et des priorités d’amélioration continue, en tenant compte de l’évolution des cybermenaces, des technologies émergentes, des exigences opérationnelles, des dépendances techniques et des objectifs de cybersécurité de l’entreprise.
- Diriger la conception, la configuration, le déploiement, l’intégration, l’optimisation et l’évolution de plateformes de cybersécurité complexes, en traduisant les exigences opérationnelles et de cybersécurité en architectures, politiques, contrôles, intégrations, sources de données et flux de travail évolutifs.
- Agir en tant qu’autorité technique et point d’escalade pour les plateformes de cyberdéfense attribuées, fournir des conseils d’experts et exercer un jugement indépendant sur des questions complexes liées aux plateformes, à l’architecture, à la configuration, à l’intégration et au fonctionnement.
- Établir et régir les normes de plateforme et les pratiques techniques sécurisées, y compris les configurations de référence, les modèles d'architecture, les procédures de déploiement, les guides d'exploitation, les normes d'intégration et les modèles de support.
- Diriger l'administration et l'évolution continue des capacités de Palo Alto Networks, y compris XSIAM, Cortex XDR, SSPM, Xpanse et la gestion de l'exposition, pour être efficacement intégré et aligné avec les exigences de la cyberdéfense.

- Diriger la migration et l'intégration des capacités d'opérations de sécurité dans XSIAM, y compris l'ingestion de données, l'analyse, l'automatisation, les tableaux de bord, le contenu de détection et les flux de travail connexes, en gérant les dépendances techniques complexes entre les environnements.
- Évaluer l’architecture de la plateforme, la couverture du déploiement, le statut des agents, l’efficacité du contrôle, la cohérence des politiques et la maturité de l’intégration ; identifier les lacunes importantes et identifier les stratégies de correction ou d’optimisation appropriées.
- Concevoir et diriger des intégrations complexes entre les plateformes de cybersécurité et les technologies d’entreprise grâce à des API, des connecteurs, des collecteurs, des agents, des sources de journaux, des webhooks, des comptes de service et des mécanismes d’authentification.
- Établir et maintenir l’intégrité et la disponibilité de la télémétrie de sécurité, de sorte que les données requises par les équipes de cyberdéfense soient complètes, exactes, normalisées, opportunes, sécurisées de manière adéquate et utilisables sur le plan opérationnel.
- Diriger le déploiement et l'intégration opérationnelle de Koi Security, y compris la configuration de la plate-forme, les politiques, la surveillance, les alertes et les flux de réponse, et mener des améliorations en fonction des exigences opérationnelles et de sécurité.
- Assumer la responsabilité technique de l’infrastructure à clé publique de l’entreprise et des capacités de gestion des certificats dans la portée attribuée au poste, y compris la découverte, l’inventaire, la délivrance, le renouvellement, la révocation, la surveillance des délais et les contrôles et intégrations connexes.
- Identifier et surveiller les mesures liées à l’état, à la couverture et au rendement de la plateforme, y compris la disponibilité, la capacité, l’octroi de licences, l’état d’intégration, l’ingestion de données et la couverture du déploiement; identifier les tendances et prendre des mesures correctives ou préventives au besoin.
- Identifier, évaluer et résoudre les risques complexes liés à la plateforme et les lacunes de capacité, y compris les faiblesses de configuration, les échecs d'intégration, les problèmes de qualité des données, les privilèges excessifs, la couverture de sécurité insuffisante et les limitations de visibilité.
- Concevoir et mettre en œuvre des stratégies d'automatisation en utilisant des scripts, des API, des pratiques d'infrastructure comme code et des flux de travail automatisés pour améliorer le déploiement, la validation, la surveillance, l'administration, la fiabilité et l'évolutivité de la plate-forme.
- Mener des activités de changement de cycle de vie et de plateforme, y compris des mises à niveau, des correctifs, des mises à jour de contenu, de la maintenance, de l'activation des fonctionnalités et de l'évolution technologique, en évaluant les dépendances techniques et les impacts potentiels sur la visibilité de la sécurité et la préparation opérationnelle.
- Diriger l'analyse technique et la résolution des problèmes complexes, ambigus et à fort impact sur les plateformes, y compris ceux liés aux points de terminaison, au réseau, aux identités, au cloud computing, à l'intégration des données et à l'ingestion, lorsque les pratiques ou les solutions établies ne répondent pas entièrement à la situation.
- Mener et diriger l’analyse technique des causes profondes des incidents importants sur la plateforme et des problèmes récurrents, et définir des mesures correctives et des améliorations à long terme pour réduire les risques opérationnels et de cybersécurité.
- Démontrer un jugement technique autonome dans l’identification des solutions et la mise en œuvre des changements susceptibles d’avoir un impact sur la visibilité de la sécurité de l’entreprise, la résilience de la plateforme, la préparation opérationnelle ou l’efficacité des contrôles de cybersécurité.
- Fournir des conseils techniques et des recommandations faisant autorité aux dirigeants de Cyber Defence, aux équipes technologiques, aux architectes et aux autres parties prenantes concernant les capacités de la plate-forme, les risques, les solutions techniques, l'orientation architecturale et les priorités d'amélioration.

- Diriger des discussions techniques interfonctionnelles et coordonner des initiatives de plates-formes complexes impliquant la cyberdéfense, l'infrastructure, le cloud, le réseau, les identités, l'architecture, les équipes d'applications et les fournisseurs tiers, en équilibrant les exigences techniques et les dépendances concurrentes.
- Diriger les échanges techniques avec les fournisseurs de services et de cybersécurité, évaluer les solutions, résoudre les problèmes complexes liés aux produits et à l’intégration, évaluer les capacités des plateformes et formuler des recommandations pour des améliorations ou des changements technologiques.
- Évaluer les technologies et les capacités émergentes en matière de cybersécurité, y compris leur valeur potentielle, leurs exigences en matière d’intégration, les risques et l’alignement avec les besoins en matière de cyberdéfense en constante évolution, et formuler des recommandations d’adoption ou d’autres investissements.
- Mettre l'expertise technique à travailler dans les décisions d'investissement technologique, l'analyse de rentabilisation, les besoins en licences et en capacité, et faire des recommandations sur l'expansion, le renouvellement, l'optimisation ou le remplacement des plates-formes, selon la portée du poste.
- Soutenir les activités de gouvernance, d’audit et d’assurance en matière de cybersécurité en tant qu’expert en la matière pour les plateformes, fournir des preuves techniques et une expertise, et traiter les résultats des plateformes grâce à des plans de réparation appropriés.
- Fournir un leadership fonctionnel, des conseils techniques, du mentorat et un transfert de connaissances aux professionnels de la cyberdéfense et aux équipes technologiques, et élaborer de la documentation technique, des approches de dépannage, des procédures opérationnelles et des guides de soutien qui renforcent les capacités des équipes.
- Prioriser et diriger simultanément plusieurs initiatives liées aux plateformes opérationnelles et aux priorités, en équilibrant le déploiement, l’intégration, le cycle de vie, la correction et les exigences de gestion des incidents, tout en gérant les dépendances techniques et les risques de cybersécurité de l’entreprise.
- Identifier et continuellement améliorer la sécurité, la stabilité, la résilience, la couverture, l'automatisation et la valeur opérationnelle de la plateforme, en introduisant de nouvelles approches lorsque les pratiques ou solutions existantes ne répondent pas adéquatement aux exigences changeantes.

Qualifications recherchées

- Diplôme d’études postsecondaires en cybersécurité, en informatique, en technologie de l’information ou dans une discipline connexe, ou combinaison équivalente d’études et d’expérience professionnelle pertinente.
- Au moins cinq ans d’expérience progressive dans la cybersécurité, l’ingénierie de la sécurité, les opérations de sécurité ou les technologies d’entreprise, y compris une expérience significative dans la conception, le déploiement, l’intégration et la gestion du cycle de vie de plates-formes de cybersécurité d’entreprise complexes.
- Une expérience des technologies de sécurité de Palo Alto Networks, y compris XSIAM et Cortex XDR, est hautement souhaitable. Les certifications pertinentes en matière de cybersécurité ou de technologie, telles que les certifications CISSP, CISM, GIAC ou fournisseurs applicables, sont des atouts.
- Expérience approfondie des technologies de cybersécurité d'entreprise, y compris les solutions SIEM et SOAR, la détection et la réponse des terminaux, la gestion de l'exposition et les plateformes de sécurité connexes.
- Expérience avérée en leadership technique et expertise en la matière pour les plateformes de cybersécurité d’entreprise, y compris la capacité d’évaluer de manière indépendante des problèmes techniques complexes, d’identifier des solutions et de formuler des recommandations faisant autorité.
- Expérience dans le développement ou la contribution à des feuilles de route, des normes techniques, des architectures, des plans de cycle de vie et des stratégies d’amélioration continue pour les plateformes de cybersécurité.
- Expérience dans l’intégration de technologies métier complexes via des API, des connecteurs, des sources de journaux, des agents, des collecteurs, des comptes de service et des mécanismes d’authentification, ainsi

qu’une capacité démontrée à diagnostiquer et à résoudre des problèmes complexes d’intégration et d’ingestion de données.

- Connaissance approfondie de l'architecture de sécurité d'entreprise et des domaines connexes, notamment la gestion des identités et des accès, la sécurité des terminaux, la sécurité du cloud, la sécurité du réseau, la gestion des vulnérabilités et des expositions, la surveillance de la sécurité et la résilience opérationnelle.
- Bonne compréhension des infrastructures à clé publique, des certificats numériques, du chiffrement, des autorités de certification, des modèles de confiance et de la gestion du cycle de vie des certificats dans des environnements d'entreprise complexes.
- Expérience dans le développement d'automatisations utilisant Python, PowerShell, les API REST, JSON, YAML, l'infrastructure en tant que code ou des technologies comparables pour améliorer le déploiement, l'intégration, la surveillance et l'administration de la plate-forme.
- Capacité démontrée d’analyser des problèmes techniques complexes ou ambigus, d’évaluer les risques et les solutions de rechange, et d’exercer un jugement indépendant dans l’élaboration de solutions lorsque les approches établies ne répondent pas pleinement à la situation.
- Expérience de la direction ou de la fourniture de conseils techniques pour des initiatives complexes de cybersécurité impliquant plusieurs équipes technologiques, parties prenantes de la cybersécurité, fournisseurs et fournisseurs de services.
- Capacité démontrée à évaluer les technologies de cybersécurité émergentes et les capacités de la plateforme, et à formuler des recommandations concernant l’architecture, l’adoption, l’optimisation, le cycle de vie et les investissements technologiques.
- Capacité à communiquer des concepts techniques, de sécurité et de risque complexes de manière claire et convaincante aux parties prenantes techniques et non techniques, et à influencer les décisions dans de multiples domaines de l'organisation.
- Capacité à préparer et à établir une documentation technique complète, des normes d'architecture et de configuration, des procédures d'exploitation, des directives de mise en œuvre et des documents justificatifs.

Solides compétences analytiques, organisationnelles, de communication, de collaboration et de résolution de problèmes, et capacité à gérer de multiples priorités complexes et dépendances techniques dans un environnement de cybersécurité dynamique.

- Faire preuve de ponctualité et de fiabilité pour soutenir le succès global de l'équipe dans un environnement en évolution rapide.

Conditions d’emploi

Au moment où Air Canada présente une offre, la personne doit avoir le droit de travailler dans le pays concerné. Elle se charge d’obtenir les permis, visas et autres autorisations nécessaires. Elle fournit une preuve de son admissibilité avant son entrée en poste.

Langues de travail

À compétences égales, Air Canada privilégie les candidatures bilingues.

Diversité et inclusion

Air Canada valorise la diversité et l’inclusion. Elle cherche à offrir un milieu de travail sain, accessible et stimulant où chaque personne peut contribuer à la réussite de l’entreprise.

En tant qu’employeur qui garantit l’égalité d’accès à l’emploi, nous encourageons un large éventail d’applications afin que nous puissions avoir une main-d’œuvre diversifiée et représentative de nos clients et des communautés où nous vivons et offrons nos services.

Air Canada remercie les personnes qui postulent et communique avec celles retenues pour une entrevue.