

## Caisse de dépôt et placement du Québec

### Conseiller.ère, Cyberdéfense

Référence : R04038

Durée : Temps plein

Endroit : 1000, place Jean-Paul Riopelle, Montréal

Au sein de l'équipe de Cyberdéfense, la personne titulaire du rôle joue un rôle essentiel dans la protection de l'infrastructure informatique de la CDPQ contre les menaces de sécurité. Elle est responsable de la surveillance, de la détection et de la réponse aux incidents de sécurité, en mettant l'accent sur les environnements technologiques Palo Alto. Elle travaille également en étroite collaboration avec les équipes internes et les partenaires externes pour assurer une réponse rapide et efficace aux incidents de sécurité.

#### Ce que vous ferez

- Surveiller les systèmes de sécurité pour détecter les activités suspectes et les incidents de sécurité;
- Analyser les alertes de sécurité et mener des enquêtes approfondies pour identifier les menaces potentielles;
- Répondre aux incidents de sécurité en suivant les procédures établies, y compris le triage, le confinement, l'éradication et la récupération;
- Collaborer avec les équipes techniques pour résoudre les incidents de sécurité et mettre en œuvre des mesures correctives;
- Participer à la rotation des équipes pour assurer une couverture 24/7 des opérations de sécurité;
- Maintenir à jour les connaissances sur les dernières tendances et techniques en matière de cyberdéfense, en particulier sur les produits Palo Alto;
- Contribuer à l'amélioration continue des processus et des procédures de gestion des incidents.

#### Ce que vous êtes

Vous vous distinguez par votre

- Collaboration, imputabilité, ambition et ouverture;
- Capacité à travailler sous pression et gestion des parties prenantes;
- Gestion des priorités face à des incidents simultanés;
- Rigueur, vigilance et réactivité;
- Sens de l'urgence requis pour évaluer rapidement la gravité des alertes et prendre des mesures appropriées.

#### Ce que vous apportez

- Diplôme en Cybersécurité, Informatique ou domaine connexe;
- Maîtrise des concepts de cybersécurité, centres d'opérations de sécurité (SOC) et des services de détection/réponse aux incidents;
- De trois (3) à cinq (5) ans d'expérience en surveillance, détection et réponse aux incidents de sécurité;
- Expérience pratique avec les technologies de sécurité Palo Alto en relation aux fonctions de Cyberdéfense;
- Certifications en sécurité informatique telles que CompTIA Security+, SSCP, un atout.
- Certifications Palo Alto SecOps, des atouts:
- Palo Alto Networks Certified Security Operations Generalist
- Palo Alto Networks Certified Detection and Remediation Analyst (PCDRA)
- Palo Alto Networks Certified Security Automation Engineer (PCSAE)

SVP Postulez en ligne au : <https://rita.cegid.cloud/go/67cf420bee25f7cf9e666e0e/51fc022158b70066fae49fdc/fr>