# Conseiller principal ou conseillère principale, Sécurité offensive et Bug Bounty

| | |
|---|---|
| **Référence** | R2613869 |
| **Lieux** | Montréal, 200, rue des Commandeurs Lévis |
| **Province** | Québec |
| **Publication** | 23 novembre 2026 |
| **Statut** | Permanent · Temps plein |
| **Mode de travail** | Télétravail |
| **Fin d’affichage** | 18 décembre 2026 |
| **Famille d’emplois** | Sécurité |

## Le poste

Dans votre rôle, vous ferez partie de la Direction des opérations de sécurité offensive, qui est chargée de protéger le Mouvement Desjardins en vous appuyant sur une expertise offensive reconnue. Votre expertise dans le domaine sera utilisée pour mener des campagnes de « chasse aux chiens » avec des examens de codes afin de cerner les menaces et les vulnérabilités sur les surfaces externes du Mouvement Desjardins et de guider leur remise en état.

## Responsabilités

- Utiliser une meilleure maîtrise des techniques d'intrusion, une expertise avancée pour ce qui touche sécurité des réseaux et des applications, des compétences en rétroingénierie, une capacité d'examen du code source et un niveau élevé de connaissance des contrôles ministériels pour découvrir les vulnérabilités imprévues afin d'identifier et d'exploiter les vulnérabilités ou les faiblesses des systèmes de manière rigoureuse et éthique.
- Agir en tant qu'expert offensif pour accompagner, conseiller et agir comme catalyseur du changement, afin de renforcer la protection du Mouvement contre les cyberattaques du point de vue d'un attaquant externe.
- Concevoir, élaborer, mettre en oeuvre et documenter des méthodes et des outils efficaces, appropriés et précis, tout en atténuant les risques associés à leur mise en œuvre.
- Faire preuve d'autonomie et d'initiative pour actualiser les compétences techniques et les connaissances liées à son domaine de compétence offensive, en fonction des besoins émergents, afin de guider et d'influencer activement le changement. Assurer un suivi stratégique des menaces dans son domaine de compétence afin de faciliter l'identification proactive des nouveaux problèmes de sécurité.
- Communiquer clairement et précisément les résultats des activités offensives de sécurité, en mettant à disposition des informations afin que toutes les parties concernées comprennent les risques et prennent les mesures nécessaires.
- Contribuer au soutien, au développement et au mentorat de tous vos collègues et intervenants, tant sur le plan technique qu'en termes de compréhension et de sensibilisation aux menaces contre lesquelles le Mouvement souhaite se protéger.

© 1996-2026 Fédération des caisses Desjardins du Québec. Tous droits réservés - Tous droits réservés © 2026 - optimisé par novijob™

novijob.com novijob.com novijob.com novijob.com novijob.com novijob.com novijob.com novijob.com

## Profil recherché

- Baccalauréat dans une discipline appropriée.
- Expérience requise : au moins huit ans d’expérience pertinente, dont cinq ans dans la réalisation de tests d’intrusion principalement axé sur les applications web, cloud, et mobile.
- Une autre combinaison pertinente d’études et d’expérience peut également être considérée.
- Expérience démontrée dans diverses plates-formes de primes de bugs (p. ex. HackerOne, Buggrowd, YWH, etc.).
- Expérience de travail avec les modèles IA et l'utilisation d'agents dans un contexte de sécurité offensive.
- Certification de sécurité offensive reconnue comme CTPS, OSCP, OSWE ou OSCE.
- Le poste exige le français.
- Compétences avancées en anglais, tant orale qu'écrite en raison de la nature des tâches, des outils de travail ou des interactions avec les partenaires ou les membres anglophones et les clients.
- Expertise en identification, analyse et hiérarchisation des vulnérabilités en matière de sécurité.
- Maîtrise des outils de tests de sécurité, tels que Burp, Caido, etc.
- Connaissance de la sécurité des systèmes d'exploitation Windows et Linux (durcissements et attaques).
- Connaissance approfondie des vulnérabilités du Web, y compris le Top 10 OWASP : injections SQL, CSRF, XSS, etc.
- Connaissance des bonnes pratiques de sécurité en matière de développement web et d'expertise dans l'une des langues suivantes : JavaScript, ASP, C#, Go, etc.
- Connaissances avec des méthodes de modélisation des menaces ou une expérience comparable représentant visuellement les flux de données et de processus dans un environnement commercial.

Être stratégique, maîtriser les relations interpersonnelles.

## Avantages

- Rémunération concurrentielle avec prime versée annuellement.
- Dès la première année, 4 semaines de vacances à prendre avec souplesse.
- Un régime à prestations déterminées procure un revenu stable et prévisible pendant la retraite.
- Couverture d’assurance collective avec accès à la télémédecine.
- Frais admissibles remboursés pour la santé, le bien-être et le matériel de travail à distance.

Les conditions d’admissibilité déterminent les avantages offerts.

## Conditions

Les dispositions syndicales s’appliquent selon l’admissibilité.

## Équité et accessibilité

Desjardins veut offrir un milieu de travail inclusif où chaque personne est reconnue et valorisée. L’employeur pratique la tolérance zéro envers toute discrimination et souhaite que les équipes représentent la diversité de ses membres, de sa clientèle et des collectivités desservies.

Les personnes qui ont besoin d’adaptations pour le recrutement ou pour le poste peuvent en aviser Desjardins. Des mesures peuvent être demandées à toutes les étapes du recrutement.

Pour postuler, recherchez la réquisition R2613869 dans le portail Carrières de Desjardins.

novijob.com novijob.com novijob.com novijob.com novijob.com novijob.com novijob.com novijob.com

© 1996-2026 Fédération des caisses Desjardins du Québec. Tous droits réservés - Tous droits réservés © 2026 - optimisé par novijob™