Chef·fe d’équipe Sécurité

Montreal - Full-time - 744000112134932

Apply Now:
https://jobs.smartrecruiters.com/Ubisoft2/744000112134932-chef-fe-d-equipe-securite?oga=true

En tant que **Chef·fe d’équipe Sécurité** à Ubisoft Montréal, vous dirigerez notre **Centre des opérations de sécurité (SOC)** ainsi que l’équipe de **forensique numérique et réponse aux incidents (DFIR)** au sein du groupe Gestion des risques de sécurité *(security risk management - SRM)*.

Dans ce rôle de Chef·fe d’équipe Sécurité, vous superviserez la gestion des incidents, l’amélioration de la surveillance de sécurité et la coordination avec les équipes et la direction. Le poste de Chef·fe d’équipe Sécurité implique l’encadrement d’une équipe distribuée d’analystes en sécurité, en combinant expertise technique, vision stratégique et leadership humain.

Ce que vous ferez

- Diriger les **réponses aux incidents** et les **enquêtes internes** sur l’ensemble de leur cycle de vie
- Coordonner les activités de **DFIR** avec les équipes de sécurité, la direction et, au besoin, les autorités locales
- Collecter et analyser des **journaux de sécurité** provenant de multiples sources et produire des rapports clairs
- Définir et faire évoluer la vision de l’équipe en matière de **détection et réponse aux incidents**
- Organiser le travail de l’équipe afin d’optimiser l’utilisation des ressources et la résolution des incidents
- Représenter l’équipe SOC et DFIR auprès des partenaires internes en **Opérations de sécurité** et en **Gestion des risques**
- Créer un environnement fondé sur la **confiance**, la communication ouverte et la collaboration
- Soutenir le développement de l’équipe en anticipant les besoins futurs et en proposant des formations adaptées

- Expérience en gestion d’une **équipe de sécurité distribuée ou à distance**
- Solide **esprit d’enquête** et rigueur dans l’analyse des incidents complexes
- Expertise pratique en **réponse aux incidents cyber** et en **forensique numérique**
- Capacité à corréler et expliquer des **données techniques** à des publics non techniques
- Maîtrise d’outils **SIEM** tels que **Splunk** et **ELK Stack**
- Connaissance des solutions **EDR**, **IDS**, **DLP**, Endpoint AV & EDR, IDS, DLP, & digital forensics
- Notions en **analyse de maliciels** et dé-obfuscation de scripts avec CyberChef ou des bacs à sable automatisés
- **Certifications en cybersécurité ou réponse aux incidents** considérées comme un atout

Pour info : Si vous avez besoin d'un permis de travail, votre admissibilité peut dépendre de votre éducation et de vos années d'expérience de travail pertinentes, comme l'exige le gouvernement.

Les habiletés et les connaissances se présentent sous différentes formes et peuvent être basées sur des expériences pertinentes, c'est pourquoi nous vous encourageons vivement à poser votre candidature, même si vous ne remplissez pas toutes les exigences énumérées ci-dessus.

Chez Ubisoft, nous encourageons la diversité sous toutes ses formes. Nous nous engageons à favoriser un environnement de travail inclusif et respectueux pour tous. Nous savons qu'il est important que l'entretien soit agréable. Par conséquent, si vous avez besoin d'accommodements, veuillez nous faire savoir si nous pouvons faire quoi que ce soit pour faciliter le déroulement de l'entretien.