Spécialiste de la sécurité - Responsable de la gestion des incidents de cybersécurité (analyse forensique)

Montreal - Full-time - 744000141448927

Apply Now:
https://jobs.smartrecruiters.com/Ubisoft2/744000141448927-specialiste-de-la-securite-responsable-de-la-gestion-des-incidents-de-cybersecurite-analyse-forensique-?oga=true

En tant que Spécialiste de la sécurité - Responsable de la gestion des incidents de cybersécurité à Ubisoft Montréal, vous dirigerez la réponse aux incidents de cybersécurité complexes touchant notre infrastructure mondiale, nos environnements de production de jeux et nos services destinés aux joueurs. Vous rejoindrez l'équipe Gestion de la sécurité et des risques et contribuerez au renforcement de nos capacités de détection, d'enquête et d'intervention.

Ce que vous ferez

- Diriger la réponse aux incidents de cybersécurité critiques impliquant plusieurs équipes, notamment les opérations de sécurité, les technologies de l'information, les équipes juridiques et les équipes de production
- Coordonner les activités de gestion des incidents et agir comme personne-ressource principale durant les enquêtes actives
- Analyser les risques de sécurité liés aux environnements de production de jeux, aux services en ligne, aux chaînes de développement et aux données des joueurs
- Améliorer les processus d'intervention, les procédures d'enquête et les outils internes de sécurité
- Réaliser des activités proactives de recherche de menaces dans les environnements de l'entreprise
- Effectuer des enquêtes judiciaires numériques portant sur la mémoire, les disques et les réseaux à l'aide d'outils comme Velociraptor, Autopsy et d'autres solutions comparables
- Collaborer avec des intervenants techniques et non techniques afin de communiquer les résultats des enquêtes et les plans d'intervention
- Accompagner les membres de l'équipe et favoriser le partage des connaissances au sein du centre des opérations de sécurité
- Animer des exercices de simulation et contribuer aux initiatives d'amélioration continue
- Rédiger des rapports après incident destinés aux équipes techniques, à la direction, aux équipes juridiques et aux responsables de la protection des renseignements personnels

Ce que vous apportez à l'équipe

- Expérience dans la gestion et la coordination d'incidents de cybersécurité complexes, de la détection jusqu'à la résolution

- Capacité démontrée à travailler de façon autonome, à repérer les améliorations possibles et à mettre en œuvre des solutions
- Bonne connaissance des plateformes de gestion des événements et des informations de sécurité ainsi que des outils de détection et de réponse sur les terminaux comme Splunk, CrowdStrike, Defender ou des technologies équivalentes
- Expérience avec des plateformes d'automatisation et d'orchestration des opérations de sécurité
- Expérience pratique en enquêtes judiciaires numériques à l'aide d'outils comme Velociraptor, Autopsy, Axiom ou des solutions similaires
- Connaissance des méthodes de recherche de menaces et des techniques d'enquête dans des environnements complexes
- Excellentes aptitudes en communication et capacité à adapter l'information technique à différents publics
- Expérience dans les environnements de jeux vidéo, les systèmes anti-triche ou les infrastructures infonuagiques à grande échelle constitue un atout

- Votre CV mettant en valeur vos compétences
- Projets, publications ou présentations techniques pertinents liés à la cybersécurité ou à la gestion des incidents