Security Specialist - Incident Commander (DFIR)

Montreal - Full-time - 744000141446434

Apply Now:
https://jobs.smartrecruiters.com/Ubisoft2/744000141446434-security-specialist-incident-commander-dfir-?oga=true

As a Security Specialist - Incident Commander (DFIR) at Ubisoft Montréal, you will lead the response to complex cybersecurity incidents affecting our global infrastructure, game production environments, and player-facing services. You'll join the Security and Risk Management team and help strengthen our detection, investigation, and response capabilities across the organization.

What you'll do

- Lead the response to high-severity cybersecurity incidents across multiple teams including security operations, information technology, legal, and production teams
- Coordinate incident management activities and serve as a central point of contact during active investigations
- Analyze security risks affecting game production environments, live services, development pipelines, and player data
- Improve incident response processes, investigation procedures, and internal security tools
- Conduct proactive threat hunting activities across enterprise environments
- Perform digital forensic investigations involving memory, disk, and network analysis using tools such as Velociraptor, Autopsy, and similar platforms
- Collaborate with technical and non-technical stakeholders to communicate investigation findings and response plans
- Mentor team members and support knowledge sharing activities across the security operations center
- Lead simulation exercises and contribute to continuous improvement initiatives
- Prepare post-incident reports for technical teams, leadership, legal, and privacy stakeholders

What you bring to the team

- Experience responding to and coordinating complex cybersecurity incidents from detection through resolution
- Demonstrated ability to work independently, identify gaps, recommend improvements, and implement solutions
- Strong knowledge of security information and event management platforms and endpoint detection and response tools such as Splunk, CrowdStrike, Defender, or equivalent technologies
- Experience working with security automation and orchestration platforms
- Hands-on experience conducting digital forensic investigations using tools such as

Velociraptor, Autopsy, Axiom, or similar solutions
- Knowledge of threat hunting methodologies and investigation techniques in complex environments
- Strong communication skills with the ability to adapt technical information for different audiences
- Experience working with gaming environments, anti-cheat systems, or large-scale cloud services is an asset

- Your CV highlighting relevant skills and experiences

- Relevant project links, publications, or technical presentations related to cybersecurity or incident response