Security Team Lead

Montreal - Full-time - 744000112134542

Apply Now:

As a **Security Team Lead** at Ubisoft Montréal, you will lead our **Security Operations Center (SOC)** and **Digital Forensics and Incident Response (DFIR)** team within the Security Risk Management group. In this Security Team Lead role, you will guide incident response efforts, strengthen security monitoring, and ensure effective coordination across teams and leadership. As a Security Team Lead, you will support a distributed team of security analysts by combining technical expertise, strategic thinking, and people leadership.

What you'll do

- Lead **incident response** and **internal investigations** through their full lifecycle, acting as a central point of coordination
- Coordinate **Digital Forensics and Incident Response (DFIR)** activities with security teams, leadership, and external authorities when required
- Aggregate and analyze **security logs** from multiple sources, producing clear and actionable reports for stakeholders
- Develop and evolve the team vision aligned with company strategy for **incident detection and response**
- Manage team capacity and priorities to ensure effective use of resources and timely resolution of incidents
- Represent the SOC and DFIR team with internal partners across **Security Operations** and **Security Risk Management**
- Foster a culture of **trust**, open communication, and collaborative problem-solving
- Support team growth by identifying skill gaps, anticipating future needs, and proposing relevant training

- Experience leading a **distributed or remote security team** with a focus on collaboration and accountability
- Strong **investigative mindset** with attention to detail and persistence during complex security cases
- Hands-on expertise in **cyber incident response** and **digital forensics**
- Ability to collect, correlate, and explain **technical logs** to non-technical audiences such as executives, legal, or HR teams
- Proficiency with **SIEM tools** such as **Splunk** and **ELK Stack**
- Working knowledge of **endpoint protection**, **EDR**, **IDS**, **DLP**, and forensic tools
- Basic capability in **malware analysis** and **script de-obfuscation** using tools like CyberChef or automated sandboxes
- Relevant **cybersecurity or incident response certifications** considered an asset

Just a heads up: If you require a work permit, your eligibility may depend on your education and years of relevant work experience, as required by the government.

Skills and competencies show up in different forms and can be based on different experiences, that's why we strongly encourage you to apply even though you may not have all the requirements listed above.

At Ubisoft, you can come as you are. We embrace diversity in all its forms. We're committed to fostering a work environment that is inclusive and respectful of all differences.