Security Specialist

Montreal - Full-time - 744000163906029

Apply Now:
https://jobs.smartrecruiters.com/Ubisoft2/744000163906029-security-specialist?oga=true

As an Application Security Specialist at Ubisoft Montréal, you will join our Application and Platform Security team within the Security Risk Management (SRM) department.

Working within engineering teams across Ubisoft, you'll partner with developers, infrastructure specialists, and technical stakeholders to strengthen the security of applications, services, platforms, and development environments. You'll address systemic security weaknesses, improve existing technical architecture, and help teams adopt secure-by-default practices.

This hands-on role combines technical expertise with self-directed work and collaboration. You'll help shape engineering priorities and deliver lasting security improvements across teams without direct organizational authority.

What you'll do

- Partner with engineering teams as an embedded security specialist, trusted technical partner, and primary security contact for assigned environments and services.
- Identify, investigate, and remediate systemic security weaknesses across applications, services, infrastructure, and development environments.
- Implement structural security improvements to address recurring vulnerabilities, reduce technical risks, and strengthen existing systems by design.
- Improve secure development and delivery workflows, including continuous integration (CI) and continuous delivery (CD) pipelines, build processes, authentication, authorization, secrets management, and infrastructure configurations.
- Coordinate with Vulnerability Management to report deficiencies, support remediation, and escalate structural security issues that require cross-team intervention.
- Collaborate with engineering teams to document and hand over security improvements so the appropriate system owners can maintain them.
- Build collaborative relationships with technical stakeholders, influence engineering priorities, and advance security improvements across teams without direct organizational authority.

- Substantial experience in application security, platform security, infrastructure security, or secure software development.
- Hands-on experience investigating and remediating vulnerabilities in existing applications, services, or infrastructure.
- Sound understanding of application security principles, secure architecture, common vulnerability classes, and Open Worldwide Application Security Project (OWASP) guidance.
- Experience with modern development environments, CI and CD pipelines, DevOps practices, and security testing tools such as static application security testing (SAST), software

composition analysis (SCA), or dynamic application security testing (DAST).
- Practical knowledge of authentication, authorization, identity management, secrets management, and software supply chain security.
- Proficiency in one or more programming or scripting languages, such as C#, Go, Python, or JavaScript, and the ability to modify and secure existing systems.
- Effective communication skills, a self-directed approach, and the ability to balance security requirements with engineering priorities and operational constraints.