Vulnerability Platform Specialist

Montreal - Full-time - 744000036141206

Apply Now:
https://jobs.smartrecruiters.com/Ubisoft2/744000036141206-vulnerability-platform-specialist-?oga=true

Join our team as a Vulnerability Platform Specialist and help shape the future of cybersecurity at Ubisoft!

We're looking for someone passionate about uncovering and addressing IT security vulnerabilities to safeguard our digital ecosystem. Your expertise in managing vulnerability platforms (e.g., Tenable) will focus on network scanning, prioritizing and contextualizing critical vulnerabilities, integrating tools, automating processes, and orchestrating seamless workflows. Experience with LLMs for vulnerability triage is an exciting plus!

As part of the Vulnerability Management Program team, you'll play a pivotal role in building Ubisoft's Vulnerability Operations Center, focusing on:

- **Driving Vulnerability Treatment:** Lead operational processes, establish patching strategies, and implement metrics-driven remediation.
- **Enhancing Vulnerability Platforms:** Improve tooling, enable system integrations, automate workflows, customize features, and advance scanning capabilities.

By joining Ubisoft's global Security & Risk Management (SRM) team, you'll contribute to protecting our games, cloud environments, and employee systems. Your efforts will strengthen our security posture and create a safer digital world.

Responsabilities

1. Monitor Ubisoft's environments using industry-standard scanning tools continuously.
2. Identify and prioritize vulnerabilities through automated scanners (e.g., Tenable) and authenticated methods.
3. Optimize scan schedules, enhance configurations, and ensure accuracy.
4. Create or leverage scripts (Python, Bash, etc.) to detect threats and simplify patching.
5. Integrate scanning tools with ticketing systems (e.g., Jira, ServiceNow) to streamline remediation tracking.
6. Collaborate with teams to expedite patching and improve emergency responses.
7. Analyze metrics to drive improvements, track remediation progress, and anticipate vulnerabilities.
8. Enforce patching standards, best practices, and proactive security measures across the organization.

- **Technical Expertise**: Proficient with Tenable (required), scripting (Python, Perl, Bash, PowerShell), and familiar with Qualys/Rapid7.
- **Security Foundations**: Strong understanding of networking, Windows/Linux OS, web security, and frameworks like OWASP, CVE, CVSS.
- **Integration & Optimization**: Experienced in integrating scanners with ticketing systems and optimizing patching pipelines.
- **AI & Analytics**: Skilled in using AI/LLMs to enhance vulnerability triage, prioritization, and assessment accuracy; excellent problem-solving and communication skills.
- **Adaptability**: Capable of managing multiple tasks, producing clear documentation, and thriving in fast-paced environments.

Prior Experience: Solid professional experience in a similar role is necessary to be effective in this position. This experience should be demonstrated through concrete achievements, such as the implementation of automated processes for vulnerability triage and remediation, or through degrees and certifications that showcase expertise (e.g., CISSP, CISM, ISO 27001, NIST, PCI-DSS).

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 is why we strongly encourage you to apply even though you may not have all the requirements listed above.

At Ubisoft, we embrace diversity in all its forms. We're committed to fostering an inclusive and respectful work environment for all. We know the importance of providing a pleasant interview experience, therefore if you need any accommodation, please let us know if there is anything we can do to facilitate the interview process.