Anti-Cheat Programmer (March of Giant)

Montreal - Full-time - 744000129250807

Apply Now:
https://jobs.smartrecruiters.com/Ubisoft2/744000129250807-anti-cheat-programmer-march-of-giant-?oga=true

The incumbent is responsible for contributing to the mission of the March of Giant anti-cheat team, ensuring a fair and competitive environment for the community. This role focuses on both the prevention and detection of cheating through a dual approach: code hardening and advanced detection.

The incumbent will make the game client more resilient against manipulation by implementing encryption, obfuscation, and platform-level security features. They will also help enhance robust detection systems, including in-game metrics, machine learning, and AI-based methods.

To succeed in this position, the incumbent must combine the skills of a security professional with the mindset of an engine programmer, implementing complex security features directly into the game engine and ensuring seamless integration with the client’s UI and Ubisoft’s online services.

What you'll do

- Develop and implement core anti-cheat technologies directly within the game engine, focusing on code hardening and client security, and integrating with March of Giant's and Ubisoft online systems.
- Integrate and maintain platform security features to strengthen the game's defense against cheats.
- Analyze existing cheats in partnership with Security Researchers to understand their functionality and use this knowledge to develop new protections and detection methods.
- Apply your knowledge of Windows internals and operating system security to identify and mitigate vulnerabilities.
- Collaborate with the broader development team to ensure our anti-cheat solutions are effective, performant, and do not negatively impact the player experience.
- Debug complex issues related to game security and performance and propose optimal solutions.
- Stay up to date with the latest trends in game security, reverse engineering, and cheat development to proactively counter emerging threats.

What you bring

- A degree in Computer Science or Software Engineering (or other relevant training)
- A Hacker Mindset: You're naturally curious and enjoy digging into how things work, and more importantly, how they can be broken.
- Security Expertise: Proven experience in cybersecurity, vulnerability analysis, or a similar

field. Knowledge of game protection technologies, including obfuscation, anti-tamper measures, and various forms of detection is highly valued.
- Strong C++ Skills: Proven experience in C++ programming, with a solid understanding of low-level systems, multi-threading, and memory management.
- Windows Internals Knowledge: A deep understanding of Windows operating system architecture, APIs, and security mechanisms.
- Problem-Solving Skills: The ability to solve complex technical challenges and a knack for anticipating potential security vulnerabilities.
- Communication & Collaboration: A collaborative spirit and excellent communication skills to work effectively with various teams and stakeholders.