



Game Security Specialist - Rainbow Six Siege

Montreal - Full-time - 744000109993826

Apply Now:

<https://jobs.smartrecruiters.com/Ubisoft2/744000109993826-game-security-specialist-rainbow-six-siege?oga=true>

What you will do

As a member of the Game Security Team, the incumbent helps managing and reducing security risks by providing technical security expertise and best practices, focusing on games related projects.

- Lead the implementation and maintenance of a comprehensive local security program to analyze and remedy the risks surrounding the game in question.
- Building, supporting and evolving the mapping of the game's current and potential security risks.
- Develop and manage game security guidelines, evaluate and participate in the implementation of security protections with Ubisoft developer teams.
- In collaboration with the associate director, you will oversee the technical vision of the team.
- Set up collaboration objectives and plans with service partner teams (SRM, Online platforms, IT, anti-cheat provider, etc.) to increase game protection.
- Ensure prevention and good management of game risks caused by Ubisoft production or service partner activity. More specifically, ensure reviews and propose improvements to security procedures, guidelines and standards with a focus on the game needs and service integration.
- Communicate with efficiency while delivering security needs and validating with project owners/stakeholders that those security needs are in place.
- Define and monitor key security performance indicators to measure the health of the game after its launch.
- Use their expertise and experience to promote safety awareness and education among members of the production team.

What you bring

Training:

- Bachelors' Degree in Computer Sciences or any related discipline.
- Master's Degree in Computer Sciences is a plus.
- Experience in cyber security (specifically network, API, and encryption / obfuscation best practices).
- Cyber security certificates such as OSCP, OTH, OSDA, or PT1 are a plus.

Relevant experience:

- 3 to 5+ years in game development or IT security, with experiences in API exploitation and scripting (Powershell, Python, etc.).

Skills:

- Security savvy.
- Strong analytical and organizational skills.
- Autonomous and result-oriented.
- Ability to understand and adapt solutions to business requirements.
- Pragmatic and curious.
- Adapt quickly to change.
- Bring a positive, team-oriented attitude.

Knowledge:

- Proficiency in English is required for effective communication with our colleagues and partners around the world who do not speak French.
- Knowledge of game protection technologies, gaming technologies and game design, code obfuscation, debugging, virtualization technologies, tamper proofing and watermarking.
- Well-versed in finding potential security issues with all aspects of a game, from its architecture to its core features (virtual economy, sessions, etc.).
- Knowledge of cryptography and binary protections (ideally related to game security).
- Knowledge of breaking and/or bypassing protection systems methodologies.