Offensive Security Specialist

Montreal - Full-time - 744000080868705

Apply Now:
https://jobs.smartrecruiters.com/Ubisoft2/744000080868705-offensive-security-specialist?oga=true

Ubisoft is seeking a skilled and motivated **Offensive Security Specialist** to join our cybersecurity team and strengthen Ubisoft's ability to identify, assess, and mitigate security vulnerabilities across its diverse environments, ranging from IT and corporate systems to games and online services.

You will contribute to our vulnerability management program by validating CVEs, developing exploit proofs-of-concept, collaborating with our Red Team, and supporting remediation and triage through actionable insights. Your expertise in offensive techniques will play a critical role in reducing risk exposure across the organization.

Responsibilities

- Validate the exploitation of third-party CVEs identified by vulnerability scanners (e.g., Tenable.io).
- Triage and validate first-party vulnerabilities discovered through responsible disclosure programs (e.g., Bug Bounty).
- Collaborate with the Red Team to build exploit chains and simulate real-world attack scenarios.
- Retest vulnerabilities identified by internal security teams to confirm remediation effectiveness.
- Contribute to the development and deployment of internal security tools and workflows aligned with industry best practices.
- Continuously research emerging offensive techniques and integrate findings into testing methodologies and tooling.
- Document validated vulnerabilities, and communicate detailed findings and remediation recommendations to internal stakeholders.
- Remediate vulnerabilities by following up with asset and application owners to ensure timely resolution.

- **Practical Experience**: Demonstrated track record in penetration testing or offensive security within large-scale, complex infrastructures, suited for an intermediate-level professional with a with a strong commitment to keeping skills current in offensive security with certifications such as OSCP.
- **Vulnerability Assessment Expertise**: Strong knowledge of vulnerability scoring, attack vectors, triage, and assessments, including the ability to exploit common flaws such as: Web vulnerabilities (XSS, IDOR, CSRF), Server-side issues (SQLi, XXE, SSRF, RCE), Authentication and access control weaknesses
- **Exploit Development**: Proven ability to build or adapt CVE exploitation proofs of concept (PoCs) tailored to organizational environments.

- **Tool Proficiency**: Skilled in vulnerability assessment and penetration testing tools, including vulnerability scanners (Tenable, Qualys) and network analysis utilities (Wireshark, tcpdump, Scapy); Reverse engineering & debugging tools (IDA Pro, Ghidra, x64dbg, WinDbg) is a plus.
- **Security Frameworks & Practices**: Familiarity with OWASP, MITRE ATT&CK, remediation techniques, and system hardening.

We embrace a hybrid work model helping you stay connected with your team and aligned with business priorities, while giving you the opportunity to maintain your work-life balance. Note, that some roles are fully office-based and are not eligible for hybrid work.

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.