Senior Red Team Operator

Cybersecurity Department

Apply

Qualifications:

- Minimum of 6–10 years' experience in offensive security, penetration testing, red teaming, exposure management, and/or advanced vulnerability management roles.
- Demonstrated hands-on experience conducting penetration tests, red team exercises, attack simulations, or adversary emulation, either internally or via consulting, MSSP, or internal security teams.
- Expertise in manual penetration testing of web, API, cloud (AWS/Azure/GCP), infrastructure, thick-client, and/or mobile applications (android/iOS), including the use of industry-standard tools (e.g., Burp Suite, Nmap, Metasploit, etc.).
- Be capable of leveraging AI-powered toolsets for day-to-day functions such as modernized exploitation and reporting tasks.
- Strong understanding of modern attack chains, including initial access, privilege escalation, lateral movement, persistence, command and control, and data exfiltration.
- Deep knowledge of common vulnerability types and exposure classes, including CVEs, misconfigurations, identity weaknesses, end-of-life software, insecure architectures, supply chain dependencies, and cloud control gaps.

Duties and Responsibilities:

- Conduct penetration testing, red team activities, and adversary emulation across enterprise environments, including endpoints, servers, identity platforms, applications, and cloud services.
- Leverage AI-powered resources to conduct red team, pentesting, and vulnerability management activities.
- Validate vulnerabilities identified through automated scanning, CTI, or third-party reporting to determine exploitability, attack paths, and real-world impact.
- Identify chained vulnerabilities, misconfigurations, or systemic weaknesses that increase exposure beyond individual CVE severity scores.
- Contribute to purple team engagements by collaborating with detection and incident response teams to evaluate monitoring coverage and response effectiveness.
- Act as a senior contributor within the vulnerability management lifecycle, enhancing triage accuracy by providing exploit validation and technical depth.
- Support risk-based prioritization by mapping vulnerabilities to likely attack paths, asset criticality, and existing compensating controls.
- Collaborate with VM analysts to improve assessment quality, reduce false positives, and identify high-risk exposures that warrant immediate action or leadership escalation.
- Stay current on cyber threat intelligence trends, exploit development, and active threat actor campaigns relevant to enterprise and legal services environments.

Qualifications (continued):

- Proven ability to validate vulnerabilities in real-world conditions, distinguish theoretical findings from exploitable risk, and communicate impact clearly to technical and non-technical stakeholders.
- Strong written and verbal communication skills, with the ability to translate technical findings into risk-informed narratives that support prioritization and remediation.
- Demonstrates intellectual curiosity and maintains awareness of current threat actor behaviors, CTI reporting, exploit trends, and emerging attack techniques.
- Experience working collaboratively with vulnerability management, SOC, engineering, IT operations, and risk teams.
- Experience working with offensive artificial intelligence solutions/tools preferred.
- Bachelor's degree in computer science, cybersecurity, or related field preferred but not required.
- Offensive and/or technical certifications preferred (e.g., OSCP, OSCE, CRTO, GXPN, GPEN, GWAPT, or equivalent experience).

Duties and Responsibilities (continued):

- Apply CTI insights to vulnerability assessment, helping identify which vulnerabilities are actively weaponized versus low-risk background noise.
- Partner with IT and security teams to clearly explain findings, recommend solutions, and validate remediation effectiveness.
- Document findings clearly in internal ticketing and reporting systems, articulating technical detail, business impact, recommended remediation, and residual risk.
- Contribute to the evolution of exposure management practices, including documentation, validation workflows, metrics, and continuous improvement of the VM program.
- Apply sound judgment, prioritize work effectively, and communicate emerging risks with appropriate urgency and professionalism.
- Perform additional duties as appropriate to support the CISO-org.
- Uphold high standards of confidentiality, discretion, and integrity, particularly with respect to all sensitive and/or confidential firm and client information to which this position will have access.

Status: Exempt
Reports To: Director of Cybersecurity Operations
Workplace Type: Remote (candidates must be located within DC, NY, or Boston area and commutable to one of 3 offices)

Salary range of $120,000-$189,000 dependent on candidate experience.

We welcome applications from candidates who are authorized to work in the United States for any employer. Please note that the firm is not able to provide or assume employment visa sponsorship for this position.

Candidates hired for staff positions with a minimum work schedule of 30 hours per week are eligible for a comprehensive benefits package, including healthcare insurance. Learn more about benefits at Covington.

https://www.cov.com/en/careers/staff/benefits

View Covington job applicant privacy notice here:

https://www.cov.com/en/job-applicant-privacy-notice

- Position requires access to equipment, software, or technology that is subject to U.S. export controls. To be granted access pursuant to US Export Control laws, candidate must be either (a) a United States citizen or national; (b) a person lawfully admitted for permanent residence of the United States (i.e., “Green Card” holder); or (c) an INS-approved refugee or asylum holder who has applied for naturalization within six months of the date the individual first became eligible; and if not yet naturalized, is still actively pursuing naturalization if 2 years have passed since the date of application to be granted access pursuant to US Export Control laws. Candidates will be required to submit appropriate documentation to determine whether access can be granted before proceeding further through the application process.

Covington & Burling LLP is an equal opportunity employer and does not discriminate in any aspect of employment, including hiring, salary, promotion, discipline, termination, and benefits, on the basis of race, color, ethnicity, religion, national origin, gender, gender identity or expression, age, marital status, sexual orientation, family responsibility, disability (including physical handicap), or any other improper criterion.

Covington will consider qualified applicants with arrest or conviction records for employment in accordance with applicable laws, including the California Fair Chance Act, the Los Angeles Fair Chance Initiative for Hiring Fair Chance Ordinance, the Los Angeles County Fair Chance Ordinance, and the San Francisco Fair Chance Ordinance.