Senior Cybersecurity Vulnerability Analyst

Cybersecurity Department

Summary:

The Senior Cybersecurity Operations Vulnerability Analyst is responsible for configuring, executing, analyzing, and reporting all aspects of the firm's Vulnerability Management program. Reporting to the Director of Cybersecurity Operations, this role will be responsible for the daily execution of vulnerability scans on premise and in the cloud, consolidation of scanning results, and coordination with functional stakeholders to remediate findings. This role will serve as the analytical focal point for the firm's vulnerability management program.

Apply

Qualifications:

- Minimum of 5 years' experience as a Vulnerability Analyst OR minimum of 3 years' experience in Penetration /Offensive testing, and 2 years of core Vulnerability Management responsibilities.
- Communicates clearly and professionally in both written and verbal contexts and shows intellectual curiosity by identifying knowledge gaps and pursuing deeper understanding.
- Demonstrates critical thinking and analytical skills, with the ability to independently assess situations, apply investigative methods, and draw reasonable conclusions.
- Exhibits strong attention to detail when working with tickets and complex or technical information, paired with effective time management and task prioritization.
- Works collaboratively within a team environment, contributes to shared problem solving and knowledge sharing, and demonstrates flexibility.
- Deep knowledge of common vulnerability types such as CVEs, End-of-life/Support,

Duties and Responsibilities:

- Leverage threat intelligence feeds and vulnerability management tools to identify vulnerabilities across endpoints, servers, and applications and triage assessments based on likelihood and impact of vulnerability information on the Covington environment
- Collaborate with internal business units throughout the vulnerability management lifecycle.
- Apply foundational cybersecurity and networking knowledge to analyze risk and support security operations, including understanding common vulnerability types, attack lifecycles and tactics, and core networking concepts such as protocols, services, and attack techniques. Leverage awareness of compensating controls, layered defenses, and the broader threat landscape to contextualize vulnerabilities, assess potential impact, and support informed remediation.
- Apply foundational risk management concepts to assess and contextualize security issues, including understanding risk terminology, risk appetite, attack surface, and risk treatment options. Evaluate vulnerabilities using likelihood and impact considerations, apply threat modeling concepts to understand potential attack paths, and support informed risk based decision making across security operations and remediation efforts.
- Leverage internal ticketing and communication systems to manage and track security related work, ensuring accurate documentation, clear timelines, and adherence to remediation SLAs, while maintaining situational awareness, applying appropriate follow up cadence, and escalating emerging risks or threats to leadership with clear articulation of impact and urgency through professional and timely communication.
- Apply sound judgment and attention to detail to assess security issues, prioritize work, communicate clearly and professionally, maintain situational awareness of threat activity, and contribute collaboratively while demonstrating initiative and flexibility.

misconfiguration, design flaws, supply chain and dependencies, architectural, administrative, and human vulnerability.

- Hands-on experience with vulnerability scanners.
- Experience automating tasks with connective technologies such as API integrations and hookups into custom scripts and platforms.
- Knowledge of common vulnerability types such as CVEs, End-of-life/Support, misconfiguration, design flaws, supply chain and dependencies, architectural, administrative, and human vulnerability.
- Hands-on experience with vulnerability scanners.
- Knowledge and use of risk assessment frameworks such as OCTAVE preferred.
- Bachelor's degree in computer science, information systems, cybersecurity or related field optional.
- GIAC, ISACA, CompTIA, and/or ISC2 technical certifications are preferred.
- 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.

Duties and Responsibilities (continued)

- Develop and maintain documented procedures, stay current on policies and tooling, identify and document process gaps, contribute to VM program documentation, and support operations through accurate metric reporting as needed.
- Evaluate opportunities for automation and work with leadership to create a roadmap for design and implementation of automated solutions. Develop automated solutions for vulnerability management workflows.
- Follow change management and patch management lifecycles.
- Perform additional duties as appropriate to support the CISO-org.

Status: Exempt
Reports To: Director of Cybersecurity Operations
Workplace Type: Remote
Hours: Ability to work U.S. East Coast (ET) hours 9am - 5:30pm ET

Salary range is $98,000 – $157,000 dependent on experience level and varies based on geography/candidate location.

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

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.