Senior Cybersecurity Engineer

Cybersecurity Department

Summary:

The Senior Cybersecurity Engineer is responsible for ensuring that the Firm designs and implements appropriate security controls for critical cloud and on-premises infrastructure. The Senior Cybersecurity Engineer operates a focused, thematic risk and control program that sets expectations for securing core platform and cloud computing solutions. This is a highly technical role that requires hands-on, collaborative work with stakeholders and IT implementers.

Apply

Qualifications:

- Bachelor's degree in cyber security or engineering; advanced degree and CISSP certification preferred.
- Requires 12+ years' experience in cybersecurity, with 5+ years' experience executing security advisory or oversight programs.
- 7+ years on premise enterprise Active Directory and 5+ years working in Microsoft Azure and Microsoft Entra.
- 5+ years enterprise experience in Hybrid Identity Platforms with deep understanding of Cloud Identity and Security with at least 5 years hands on experience working with production workloads in a public or government cloud environment.
- Expert working knowledge of Microsoft Active Directory Domain Services (ADDS), Microsoft Azure, Microsoft Entra, and Microsoft 365.

Duties and Responsibilities:

- Lead, coordinate, and conduct both on-premises and cloud-based security assessments.
- Advise and assist process and asset owners with designing and implementing architecture enhancements and security configuration modifications to defend against identified threats and attacker techniques.
- Provide subject-matter expertise with Active Directory identity protection, hybrid infrastructures, data loss prevention.
- Create and document detailed guides and tracking documents for Business and IT SMEs to leverage as part of Active Directory hardening and overall infrastructure enhancements.
- Work across the IT teams to analyze and define security best practice requirements for solutions.
- Regularly reports on program progress to the Cybersecurity leadership and other senior stakeholders as appropriate, using defined Key Performance Indicators (KPIs) and Key Risk Indicators (KRIs) to highlight control adoption gaps, identify areas of strong or weak performance, or quantify risks, respectively.
- Perform other duties as assigned.
- 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.

Qualifications (continued):

- Expert working knowledge of Microsoft Purview, specifically Data Security Posture Management.
- Experience conducting security assessments, attack path planning and password auditing tools.
- Experience with managing Privileged Access Management Systems.
- Thorough understanding of enterprise security controls in Microsoft Active Directory and cloud-based environments – including scalable architectures and risk reduction strategies.
- Exceptional interpersonal skills; success in the role requires the ability to influence and persuade.
- Effective written and oral communications skills.
- Ability to work independently and drive initiatives with minimal supervision.
- Preferred Certifications:
  - Microsoft Certified: Cybersecurity Architect Expert
  - Microsoft Certified: Cloud and AI Security Engineer Associate
  - Microsoft AZ-305 - Azure Architect
  - Microsoft SC-300 - IAM Administrator

Status: Exempt
Reports To: Cybersecurity Architecture & Engineering Manager
Workplace Type: Remote DC

Salary range of $155,000 - $193,500 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

Qualifications (continued):

- 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.