

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 services including Active Directory Domain Services (ADDS), Active Directory Certificate Services (ADCS), Azure AD (AAD), and Active Directory Federation Services (ADFS). This is a highly technical role that requires hands-on, collaborative work with stakeholders and IT implementers.

[Email Resume Here to Apply](#)

Qualifications:

- Bachelor's degree in computer science or engineering strongly preferred; 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 Azure Active Directory experience.
- 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), Active Directory Certificate Services (ADCS), Azure Active Directory, Microsoft 365, and/or Office 365.

Duties and Responsibilities:

- Lead, coordinate, and conduct both on-premises Active Directory security assessments and cloud-based security assessments focused on Microsoft Azure.
- 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, Active Directory Certificate Services (ADCS), synchronization, and hybrid infrastructures.
- 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 Active Directory and Azure Active Directory integrations.
- 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.

Status: Exempt

Reports To: Cybersecurity Architecture & Engineering Manager

Workplace Type: Remote

Salary range is \$134,000 - \$188,500 depending on years of experience and location.

Qualifications (continued):

- Expert working knowledge of Privileged Access Management (PAM), Justin Time Access (JIT) and other identity best practices.
- Experience conducting Azure and Active Directory security assessments, attack path planning and password auditing tools.
- Thorough understanding of enterprise security controls in Microsoft Active Directory 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.
- Preferred Certifications:
 - Microsoft AZ-500 - Azure Security
 - Microsoft Certified: Cybersecurity Architect Expert
 - Microsoft AZ-305 - Azure Architect
 - Microsoft SC-300 - IAM Administrator
- 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.