Cloud and Active Directory Specialist

Cybersecurity Department

Summary: The Cloud and Active Directory Specialist is responsible for ensuring that the Firm designs and implements appropriate security controls for critical infrastructure. The Specialist operates a focused, thematic risk and control program that sets expectations for securing core platform services including Active Directory, Azure, and Active Directory Federation Services. This is a highly technical role with requires hands-on, collaborative work with stakeholders and IT implementers.

Click 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.
- 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.
- 7+ years on premise enterprise Active Directory and 5+ years working in Active Azure Active Directory experience.
- Expert working knowledge of Microsoft Active Directory, Azure Active Directory, Microsoft 365, and/or Office 365.
- Experience with Azure and Active Directory security assessment, attack-path planning and/or password auditing tools.

Duties and Responsibilities:

- Lead, coordinate, and conduct both on-premises Active Directory security assessments and cloud-based security assessments focused in 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, synchronization, and hybrid infrastructures.
- Create and document detailed guides and tracking documents for Business and IT SME's 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 Director of Security and Risk Oversight 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: Director of Security and Risk Oversight

Qualifications (continued):

- 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 AZ-305 - Azure Architect
  - Microsoft SC-300 - IAM Administrator
- You must be fully vaccinated against COVID-19 by your hire date to be eligible for starting in the role. Proof of vaccination will be required. Covington will provide reasonable accommodation(s) based on medical or religious grounds for qualified candidates.
- 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.