Principal Cybersecurity Architect

Cybersecurity Department

Summary:

The **Principal Cybersecurity Architect** is a senior-level security leader responsible for defining the organization's cybersecurity architecture, security standards, and long-term security strategy. The role serves as the bridge between executive security leadership, technology teams, and business stakeholders to ensure security is embedded into the design of systems and platforms from the outset rather than added later.

This position focuses heavily on enterprise architecture, risk reduction, and governance. The architect establishes consistent security patterns, translates regulatory and risk requirements into technical controls, and ensures solutions align with Zero Trust principles, access governance requirements, and evolving cyber threats. Success is measured not by the number of activities performed, but by tangible improvements in security posture, reduced risk exposure, faster remediation, and adoption of secure design practices across the organization.

Apply

Qualifications:

- Bachelor’s degree in cybersecurity or engineering preferred; advanced degree and CISSP certification strongly preferred.
- Requires 15+ years' progressive experience in IT, with 7+ years progressive experience in Cybersecurity.

Duties and Responsibilities:

- Define and maintain the enterprise cybersecurity architecture and security roadmap.
- Establish security standards, reference architectures, and approved design patterns.
- Partner with cybersecurity leadership, IT teams, and business stakeholders to design secure and scalable solutions.
- Translate risk, compliance, and regulatory requirements into practical technical controls.
- Ensure security is embedded throughout the system development and implementation lifecycle.
- Drive adoption of Zero Trust, least-privilege access, and identity-centric security practices.
- Evaluate existing environments to identify architectural weaknesses and opportunities for risk reduction.
- Provide architectural guidance for cloud, identity, access management, and legacy technology modernization initiatives.
- Influence enterprise technology decisions and long-term security investments.
- Support audit readiness and compliance requirements while minimizing operational friction.
- 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):

- Demonstrated experience designing and implementing enterprise-scale security architectures across on-premises, cloud, and hybrid environments.
- Deep expertise in Identity and Access Management (IAM), Zero Trust Architecture, Privileged Access Management (PAM), and Access Governance.
- Experience securing AI, automation, and cloud-native platforms.
- Familiarity with DevSecOps, Infrastructure as Code (IaC), and secure software development practices.
- Experience conducting security assessments, attack path planning and password auditing tools.
- 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.
- Hands-on and legal experience a plus.

Status: Non-Exempt
Reports To: Director of Cybersecurity Architecture & Engineering
Workplace Type: Remote (must be local to DC office)

Salary range of $200,000 - $250,000 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

Qualifications (continued):

- Preferred Certifications:
  - CISSP, CSSP
  - Microsoft Certified: Cybersecurity Architect Expert
  - Microsoft Certified: Cloud and AI Security Engineer Associate
  - Microsoft AZ-305 - Azure Architect
- 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.