Director of Security Architecture

Cybersecurity Department

Summary: The Director of Security Architecture is responsible for selecting, designing, and implementing critical technologies that enable digital security, physical security, and risk teams to execute their missions efficiently. The Director owns all security-related tools and technologies used by the Firm, ensures that they interoperate coherently, and works with the teams that use them to make sure that they are fit for purpose. The Director also ensures that the computing environment for employees is well-engineered, so that it produces secure outcomes by default, while imposing the smallest possible tax on productivity. This role is highly technical and not operations-oriented.

Click Here to Apply

Qualifications:

- Bachelor's degree required; advanced degree and CISSP certification preferred.
- Requires 15+ years' experience in cybersecurity, with 10+ years' experience running security architecture programs, SIEM rationalization initiatives, endpoint agent collapse programs, or other cyber transformation projects.
- Expert working knowledge of SIEM, MDR, E/XDR tools, Windows desktop and server security tools and topics, Azure security, Windows Event logging, syslog, and related telematics topics.
- Exceptional interpersonal skills; success in the role requires the ability to influence and persuade.
- Excellent written and oral communication skills.

Duties and Responsibilities:

- Selects critical technologies that support the missions of the Digital Security Operations, Physical Security Operations, and Risk Operations teams. These technologies include those used for:
  - building secure computing enclaves to protect highly sensitive data;
  - protecting desktops, servers and infrastructure from attack with appropriate defensive technologies;
  - providing visibility into the security state of servers, desktops, mobile devices, applications, databases, and infrastructure;
  - detecting security events by collecting and analyzing security logs and related telemetry from servers, desktops, mobile devices, applications, databases, and infrastructure;
  - responding to security, privacy, and workplace incidents efficiently; and:
  - recovering from attack with minimal disruption to operations.
- Documents the design and interoperations of the critical security technologies described above to ensure that they are rational; in-depth or deliberately de-conflicted as appropriate to the situation; cost-effective and coherent; and that they work together harmoniously.
- Selects vendors of critical technology, in consultation with security and technology process owners, including the Digital Security Operations, Physical Security Operations, Risk Operations, Information Technology Services, Information Resource Services, and Practice Services and Support teams.

Qualifications (continued):

- 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 INSapproved 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):

- Oversees implementation of critical technologies by Covington technology asset or process owners, cloud vendors, contractors, or managed services providers, as appropriate.

- Maintains the Firm's technical standards for event logging, col-lection, analysis, and alerting.

- Defines and maintains and the Cybersecurity Five-Year Plan for future-proofing the Firm against unknown threats.

- Defines, hires, and retains the talent necessary to ensure that all of the responsibilities described above are suitably staffed.

- Perform other duties as assigned.

Status: Exempt
Reports To: CISO