**ROLE DESCRIPTION**

**Role title: M365 Security Engineer IV**

**Date updated: 4/9/24**

**About M365 Security Engineer:**

**Role summary:**

The M365 security engineer is responsible for enabling the secure use of Microsoft products at Capital Group. They will be instrumental in the design and implementation of products by providing security requirements, risk assessments, and continuous monitoring security effectiveness, particularly in Microsoft 365 environments. Staying updated on Microsoft’s security features is also a key part of their role to effectively protect against evolving cybersecurity challenges.

**Primary responsibilities/essential functions**:

* **Tactical focus:** 
  + Create information security POVs and initial build requirements for new Microsoft products
  + Assess application integration points from a security perspective and provide risk recommendations
  + Support incident response efforts. Provide the technical depth to aid in investigations
* **Domain Knowledge Focus:**
  + Research and evaluate emerging services from Microsoft, as they become available
  + Contribute security best practices for the M365 suite of products, including copilot
  + Serve as tools and product SME for new and existing technology toolset to provide the best-in-class protection to CG
* **Consultative / Business Acumen Focus:**
  + Work closely with Microsoft and internal teams to secure the changing landscape of the M365 suite
  + Drive high-quality Microsoft product related project delivery by establishing relationships with customer stakeholders and understanding their requirements.
  + Work with Information Technology on enabling new services and establishing secure configurations and governance.
  + Partnership with Information Technology on full lifecycle of a product in M365 from initial exploration to deployment and operationalization of the platform (Copilot, Fabric, Purview features ... etc)

**Required Skills/Abilities**:

* Minimum 5-7 years in Information Technology with at least 5 in Information Security
* A Bachelor’s degree in Computer Science, Information Security, or a related field (or equivalent work experience).
* Expert knowledge of Microsoft products such as Windows operating systems, M365 applications, and Azure
* Strong background in security technical engineering and architecture, such as infrastructure/cloud engineering or software development.
* Information Security certifications (CISSP, SANS GIAC, CISA, etc.) is a plus.
* Microsoft security certifications (Azure Security Engineer Associate, Cybersecurity Architect Expert) is desired
* Proven ability to build partnerships and collaboration between stakeholder teams.
* Strong communication skills and ability to outline security risks to senior leadership.
* Experience managing vendor partnerships

**Reporting Location**: Any major CG hubs such as IRV, SNO, and NYO

**Job Posting**: Bring your passion and expertise and we will provide the opportunities that will challenge you to apply your knowledge and creativity to solve complex business problems. You will work in a collaborative environment with clearly defined strategic objectives and management support to provide the necessary resources to be successful. The ideal candidate needs to possess a high level of proficiency with Microsoft 365 security products and services. Additionally, the candidate must understand the delineation of responsibilities between the cloud service provider and the cloud service consumer particularly for Software-as-a-Service (SaaS) applications. M365 will be the initial focus for the role but the role will later expand to cover other critical SaaS application deployed within Capital Group.

Interview panel first round

* Hani Kaldas (HQXK)
* Rajat Swarup (RQXS)
* Michael Hanzich (MADH)
* Wilson Gonzalez (WQG)

Interview panel second round

* Mike Antico (MCLA)
* Lauren Silverman (LQYS)

Competencies

* **Drives results with minimal supervision** – Need someone who takes ownership in following tasks through completion and who takes pride in getting things done regardless of how difficult or trivial the work is.
* **Manages complexity** – Need someone who is not overwhelmed by complex challenges and who is adept at breaking down problems into smaller digestible chunks and can formulate a plan of action with the right sequencing/priority.
* **Tech Savvy** – looking for someone who loves cutting edge technology, understand cloud technology/challenges, but also understands core security principles and knows how to strike the right balance between usability and security.
* **Persuasion and partnership building** – Looking for someone who understands the importance of building rapport with partner organizations and who can negotiate/advocate for stronger security.
* **Great communication and workload management** – Need to be able to adjust the messaging for technical and non-technical audiences and need to be adept with prioritizing the work with a fair amount of multi-tasking and context switching.