Senior IT Security Engineer (Endpoints & Monitoring)

ITS Department

Summary:

The **Senior IT Security Engineer** is part of a team of engineers who architect, design, build, maintain, and support the Firm's portfolio of security technologies and solutions, inclusive of Perimeter Defense, Monitoring & Logging, and Identity, Access, and Authorization Management.

This role leads the lifecycle management of the Monitoring & Logging portfolio, with focus on technologies that identify threats to operational stability. The senior engineer manages the necessary balance of delivering solutions that provide an optimal experience for our lawyers, staff, practice groups, and clients, without making concessions that add unacceptable risks to the Firm.

To accomplish this objective, the Senior IT Security Engineer partners closely with functional IT leadership and staff, along with Information Security, Compliance, and other cross-functional stakeholders to continuously adapt solutions to meet the evolving needs of the Firm. The role requires an individual with the skills to think both strategically and tactically to handle the operational needs of the Firm, all with the objective of delivering gold-standard services.

Click Here to Apply

Qualifications:

- College degree is strongly preferred, ideally in Computer Science, Information Systems, or a related technical discipline. Master's degree is preferred.

- Appropriate technical certification(s) are preferred.

Duties and Responsibilities:

- Owns the Endpoint & Monitoring solutions portfolio to protect the Firm's technology estate, including but not limited to technologies that evaluate, identify, and track vulnerabilities, activities, and other potential threats.

- Partners closely with the Cyber organization and other IT Security Solutions engineers to establish common standards and objectives for the Firm's security solutions, supports broader IT Security functional objectives as needed.

- Actively rationalizes the Firm's legacy suite of endpoint security agents & environment monitoring solutions against marketplace solutions to optimize the portfolio.

- Implements, integrates, and upgrades the portfolio of solutions for endpoint, monitoring & logging.

- Partners closely with Information Security, Compliance, and IT leadership to architect solutions that uphold the Firm's policies, standards, and requirements.

- Works closely with IT technical teams to evaluate, design, and uphold security standards for Firm information, computer, network, and processing systems, with particular focus on scanning, monitoring, and logging solutions (e.g., thresholds for logging and alerts, reporting and notifications, vulnerability handling).

- Partners with Information Security to conduct regular security assessments for vulnerabilities and potential threats, supporting the development of action plans to remediate findings.

- Calibrates solution settings, configuration, reporting, and visualization to optimize Information Security's ongoing monitoring and analysis of system logs, network traffic, and other data surrounding security incidents.

Qualifications (continued):

- 5+ years of relevant industry experience (exclusive of degree requirements), ideally in regulated and/or compliance focused organizations such as a large Law Firm setting, a comparable professional services organization, or a legal information services provider.

- Demonstrated experience with monitoring and logging concepts, principles, and leading industry practices, including but not limited to: security information event management (SIEM), attack surface management, threat intelligence, incident response, vulnerability management, and log management.

- Demonstrated experience in deploying and managing global monitoring and logging solutions across a variety of platforms, tenants, and environments, including on-premises and cloud-based systems.

- Demonstrated experience in configuring and maintaining various monitoring and logging technologies (e.g., Splunk, Tenable, Panaseer).

- Demonstrated experience with vulnerability assessments, penetration tests, and security audits.

- Experience with of SIEM, MDR, E/XDR tools, Windows desktop and server security tools and topics, Azure security, Windows Event logging, syslog, and related telematics topics.

- Experience with driving continuous improvement and cohesive insights across logging solutions (e.g., enriching data visualization, threat intelligence, automation, machine learning, advanced analytics).

- Knowledge in vulnerability assessment and penetration tools for systems and web security.

- Proven experience working in a fast-paced environment.

Duties and Responsibilities (continued):

- Leads continuous process development, improvement, and automation of monitoring and logging related solutions and support activities (e.g., threat intelligence, data visualization, advanced analytics, machine learning).

- Participates in the design and implementation of recommended information security controls associated with new project application/system deployments.

- Contributes to the design and supports the execution of vulnerability assessments, penetration tests, and security audits.

- Collaborates well with cross-functional stakeholders and third-party providers.

- Recommends policies, standards, procedures, and training programs for lawyers and staff to make effective use of technology.

- Delivers technology solutions for the Firm's security related projects.

- Stays current on trends and issues in the security industry, including current and emerging technologies.

- Stays current on applicable compliance and regulatory requirements for information security controls.

- Assists with the design and implementation of disaster recovery and business continuity plans, procedures, audits, and enhancements.

Status: Exempt
Reports To: IT Security Solutions Director
Workplace Type: Hybrid

- Demonstrated ability to serve as a change agent, leading and inspiring others to act, especially under circumstances when change is unpopular.

- Ability to establish rapport and elicit cooperation from personnel across all levels, including executive management, and cross-functional leadership.

- Ability to develop and motivate technology teams, inclusive of staff, and 3rd party vendors/consultants.

- Skilled in communications to all levels in the organization in writing, speaking, and presentation skills for work with the Firm leadership, the user community, and clients.

- Excellent problem solving and debugging skills required.

- Ability to manage complex information systems and technical personnel.

- Must be able to reliably deal with multiple competing priorities and remain calm under pressure.

- Ability to fulfill on-call duties for IT emergencies outside of Firm business hours.

- 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.

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.