Investigations and Incidents Manager

Cybersecurity Department

Summary: The Investigations and Incidents Manager is responsible for ensuring that the Firm promptly, thoroughly, and lawfully investigates security, privacy, and workplace incidents affecting the Firm's assets, information or people. This role develops and implements digital forensics and incident response capabilities with a mix of internal and external resources. 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 preferred; advanced degree and CISSP certification preferred.
- Requires 10+ years' experience in cybersecurity, with 5+ years' experience running hands-on digital forensics and incident response programs.
- Expert working knowledge of desktop security, forensics data capture, chain of custody concepts, open-source intelligence, and investigative methods. Experience with tools such as EnCase, Axiom and Basis Tech is required.
- Exceptional ability to rapidly assimilate and synthesize information under pressure and during compressed timeframes.
- Cogent and effective written and oral communications skills, combined with a newspaper-reporter's knack for swiftly summarizing situations, including what is known and unknown.

Duties and Responsibilities:

- Defines, documents, and manages the Investigations and Incidents programs. These include developing bodies of practice related to triage and initial assessment of severity, investigations of suspected incidents, evidence capture and preservation, support for law enforcement interactions, and upward reporting as necessary.
- Maintains the Firm's investigations processes, incident response playbooks, and related workflows as implemented in systems of record.
- Works with stakeholders and affected parties to assess likelihood or severity of suspected incidents, identify appropriate follow-ups, conduct investigations, commission third-party assistance, regularly communicate status, and coordinate internal communications. This role will work closely with the CISO, Firm General Counsels, senior lawyers, and other business stakeholders.
- Manages relationships with third-party investigators and incident-response entities the Firm may have relationships with, as necessary.
- Perform other duties as assigned.

Status: Exempt
Reports To: Director of Security Operations

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 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.