

# Information Security Analyst

## Cybersecurity Department

### Summary:

The Information Security Analyst will be part of the Cybersecurity Operations Group and will report to the Director of Information Security & Assurance. This position will be responsible for maintaining continuous monitoring of the networking environment for malicious activities, threat detection and response.

[Email Resume Here to Apply](#)

### Qualifications:

- Minimum of 3 years' experience in an Information Security and/or Cybersecurity professional role.
- Knowledge of cyber defense practices and cyber-attack techniques across computing platforms.
- Knowledge of information security policy, standards and industry recognized best practices.
- Strong written and verbal communication skills.
- Bachelor's degree in computer science, information systems, cybersecurity or related field preferred, not required.
- CISSP, CISA, CISM, CEH are preferred certifications

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

### Duties and Responsibilities:

- Use cyber defense tools for continual monitoring of systems to identify malicious activity.
- Analyze identified malicious activity to determine weaknesses that can be exploited, exploitation methods, and the potential effects on systems and information if compromised.
- Analyze suspicious email to determine threats with possible malicious intent.
- Monitor various cyber threat consoles, and receive threat alerts and event notifications upon detection of malicious/suspicious activity.
- Detonate suspicious files and URL's in malware sandboxes and analyze results for actionable tasks.
- Monitor email content filtering appliances for quarantined messages and files that need to be analyzed for possible threats.
- Analyzes audit logs for exceptions to policy, and data loss prevention events.
- Monitor firewall intrusion detection and prevention solutions for threat identification.
- Perform event correlation using information gathered from a variety of sources within the network to gain situational awareness and determine the effectiveness of an observed threat or attack.
- Perform cyber defense trend analysis and reporting.
- Triage SIEM notables by investigating various network logs to identify potential threats to systems, applications, infrastructure and operational processes.

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.

### **Duties & Responsibilities (Continued):**

- Characterize and analyze network traffic to identify anomalous activity and potential threats to network resources.
- Assists with cybersecurity incident response activities.
- Successfully sets priorities, performs tasks in an orderly fashion, and meet time deadlines.
- 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.

**Status:** Exempt

**Reports To:** Director of Information Security

**Workplace Type:** Hybrid

Salary range of \$86,000- \$121,000.

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.