# Senior Cybersecurity Analyst

Information Security Department

**Summary:**
The Senior Cybersecurity Analyst will support the firms efforts in monitoring and analyzing security events and alerts across the organization. This position requires someone that is motivated, detail-oriented, and eager to provide mentorship and take ownership over assigned tasks.

**Click Here to Apply**

## Qualifications:

- Minimum of 5-8 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 standards and industry recognized best practices.
- Strong written and verbal communication skills.
- Dedication to staying aware of current threat landscape and ongoing threat campaigns.
- Competencies in the following areas: vulnerability analysis, security alert analysis, email threat analysis, incident response, ability to read and understand essential scripting and database languages (PowerShell, python, SQL, KQL, etc)
- Bachelor's degree in computer science, information systems, cybersecurity or related field optional.

## Duties and Responsibilities:

- Lead the monitoring and analysis of security events and alerts across the organization's networks, endpoints, and cloud infrastructure using SIEM, EDR, and other security tools.
- Investigate, respond to, and resolve security incidents, ensuring timely detection, containment, and mitigation.
- Perform triage and root cause analysis of security incidents and collaborate with IT and other teams to identify and address underlying vulnerabilities.
- Actively contribute to the Vulnerability Management program and participate in the CTI program to identify and mitigate emerging threats before they impact the organization.
- Leverage threat intelligence feeds and vulnerability management tools to identify vulnerabilities across endpoints, servers, and applications and provide recommendations in alignment with best practices. Support business units in response efforts.
- Assist in the development of custom detection and mitigation techniques to detect or prevent malicious activity.
- Assist in the development and enforcement of program procedures and best practices for cybersecurity operations programs refinement and maintenance.
- Provide mentorship and technical guidance to junior and mid-level analysts, fostering skill development through knowledge sharing, hands-on training, and collaborative incident response activities.
- Demonstrates effective prioritization and consistently meets established

- GIAC, ISACA, and/or ISC2 technical certifications preferred.
- Possess the highest level of integrity and good judgment, with the ability to effectively handle highly sensitive and confidentiality.
- 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.

deadlines.

- Participate in an on-call roster to provide incident response support during off hours as needed.
- Perform additional duties as appropriate to support the CISO-org.

**Status:** Exempt
**Reports To:** Director of Cybersecurity Operations
**Workplace Type:** Remote (hours 9:00 AM – 5:30 PM Pacific Time)
Salary range of $86,000 – $138,000 dependent on candidate experience and candidate location.

Candidates hired for staff positions with a minimum work schedule of 30 hours per week are eligible for a comprehensive benefits package, including healthcare insurance. Learn more about benefits at Covington.

https://www.cov.com/en/careers/staff/benefits