# Senior Cybersecurity Analyst – Incident Response

Cybersecurity Department


**Summary:**
The Senior Cybersecurity Analyst is an experienced, hands-on cybersecurity professional capable of independently handling complex security incidents and investigations with minimal oversight. The role performs advanced threat hunting, log analysis, and digital forensics while maintaining and testing incident response playbooks, automation, and response procedures. The analyst also supports day-to-day Cybersecurity Operations and helps strengthen the organization's overall incident response readiness.


**Apply**

## Qualifications:

- Minimum of 5-8 years' experience in an Information Security and/or Cybersecurity professional role with significant hands-on experience in cybersecurity incident response and investigation.
- Strong knowledge of incident response practices, including detection, triage, investigation, containment, eradication, recovery, and post-incident analysis.
- Ability to independently lead and coordinate technical investigations from initial identification through resolution.
- Strong knowledge of cyber defense practices, attacker techniques, and investigative methodologies across endpoint, identity, email, network, and cloud environments.

## Duties and Responsibilities:

- Be capable of working independently during investigations and major incidents with little-to-no oversight.
- Perform advanced log analysis, threat hunting, and investigative analysis across endpoint, identity, email, network, cloud, and other available security telemetry to reconstruct attacker activity and determine incident scope.
- Perform digital forensic analysis and evidence collection necessary to support cybersecurity investigations.
- Develop and maintain clear incident timelines, investigative findings, evidence, response actions, and supporting documentation throughout the incident lifecycle.
- Own the development, maintenance, validation, and continuous improvement of cybersecurity incident response playbooks and supporting procedures.
- Regularly exercise and test incident response playbooks to identify gaps in technical capabilities, processes, escalation paths, documentation, and response readiness.
- Perform essential monitoring, triage, investigation, and resolution of security alerts, tickets, suspicious emails, and other Cybersecurity Operations activities when not actively engaged in incident response or preparedness activities.
- Assist in the development and refinement of detection and mitigation techniques based on findings from investigations, threat hunting, and observed attacker techniques.
- Plan, coordinate, and facilitate cybersecurity tabletop exercises designed to validate incident response readiness, playbooks, stakeholder

- Experience with SOAR technologies, playbook automation, and AI-enabled solutions for alert handling and incident response (containment, evidence collection, etc.) strongly preferred.
- Strong written and verbal communication skills, including the ability to clearly document investigative findings, response actions, timelines, and technical conclusions.
- Demonstrated experience performing log analysis and threat hunting across large or complex datasets using SIEM, EDR, and other technologies.
- Experience developing, maintaining, testing, and improving cybersecurity incident response procedures, and playbooks.
- Experience collecting, preserving, and analyzing digital evidence and performing host and network-based forensic analysis in support of cybersecurity investigations
- Ability to correlate evidence across multiple data sources to determine incident scope, attack progression, root cause, and potential impact.
- Experience planning and facilitating cybersecurity tabletop exercises preferred.
- Competencies in the following areas: vulnerability analysis, security alert analysis, email threat analysis, 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.

responsibilities, escalation processes, and technical response capabilities.

- Own SOAR, playbook automation, and other automated solutions for rapid response during incidents and day-to-day security operations.
- Provide mentorship to other Cybersecurity Operations personnel on incident investigation, threat hunting, digital forensics, and response practices.
- Participate in an on-call roster and be prepared to support cybersecurity incident response activities and urgent security operations during off hours as needed.
- Perform additional duties as appropriate to support the CISO-org.
- 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
**Workplace Type:** Remote
**Reports To:** Director of Cybersecurity Operations

Salary range is $120,000 – $157,000 depending on candidate experience.

We welcome applications from candidates who are authorized to work in the United States for any employer. Please note that the firm is not able to provide or assume employment visa sponsorship for this position.

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

View Covington job applicant privacy notice here:

https://www.cov.com/en/job-applicant-privacy-notice

- GIAC, ISACA, and/or ISC2 technical certifications preferred.

- 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.

**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.**