Senior Cybersecurity Analyst

Cybersecurity Department

Email Resume Here to Apply

Qualifications:

- Minimum of 7-8 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 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 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 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.
- Conduct proactive threat hunting activities to identify and mitigate emerging threats before they impact the organization.
- Leverage threat intelligence feeds and vulnerability management tools to identify and patch vulnerabilities across endpoints, servers, and applications.
- Develop and execute custom detection and mitigation techniques to prevent exploitation of vulnerabilities.
- Assist in the development and enforcement of security policies, procedures, and best practices across the organization.
- Conduct purple team exercises in order to identify potential security weaknesses and policy/procedure gaps.
- Successfully sets priorities, performs tasks in an orderly fashion, and meet time deadlines.
- Participate in an on call roster to provide incident response support during off hours as needed.

Status: Exempt
Reports To: Director of Cybersecurity Operations
Workplace Type: Remote- NY
Salary range is $117,000 - $165,500.