Director of Cybersecurity Operations

Cybersecurity Department

Summary:
The Director, Security Operations is responsible for developing security strategies, incident response protocols, and enhancing proactive measures to ensure strong Cybersecurity practices. This role involves implementing measures to monitor threats, swiftly respond to incidents, and continuously improve data protections against cyber threats.

Email Resume Here to Apply

Qualifications:

- Bachelor's degree required; advanced degree and CISSP certification preferred.
- In-depth knowledge of information security frameworks, best practices, and administrative, physical, and technical safeguards, with experience in common security frameworks such as NIST preferred.
- Minimum of 10+ years of experience developing infrastructure and security programs, implementing and managing security solutions, and leading security teams in incident response.
- Minimum 3+ years of experience working in a Security Operations function in an enterprise environment.
- Strong technical background and expertise in network and systems security, system and network configuration, and application security.

Duties and Responsibilities:

Cybersecurity Operations Strategy:

- Establish enterprise security monitoring program to drive continuous improvements aimed at cyber events and incident detection, containment, and remediation.
- Develop standard operating procedures to improve security operations and response capabilities and meet global compliance standards.
- Integrate threat intelligence sources into security operations to enhance threat detection and response capabilities, leveraging both internal and external sources to stay abreast of evolving cyber threats.
- Drive continuous improvement initiatives within the security operations function, leveraging metrics and data analytics to identify areas for enhancement and optimization.

Incident Response Management:

- Lead incident response team to develop and support 24x7x365 incident response capabilities, including defining response procedures.
- Receive escalations/notifications of cybersecurity and business impacting events and appropriately triage, ensure that leadership is kept informed through regular communication as appropriate, and that necessary personnel for managing an incident respond effectively.
- Conduct regular incident simulation exercises to test the efficacy of incident response procedures and identify areas for improvement, ensuring the organization's readiness to respond effectively to real-world cyber threats.

Qualifications (Continued):

- Proficiency in incident response management, next-generation firewalls, web application firewalls, multi-factor authentication, data loss prevention, and disaster recovery.
- Hands-on experience with Security Incident and Event Management (SIEM) tools, Endpoint Detection and Response (EDR) tools, vulnerability management suites, and various security solutions.
- Demonstrates good written and oral communications skills and communicates effectively.
- Experience working with and implementing NIST, ITIL, and ISO 27001 standards.
- Working knowledge of regulatory data governance obligations, such as EU/UK GDPR, HIPAA/HITECH, ITAR/EAR, and CUI a plus.

This position requires access to equipment, software, or technology that is subject to U.S. export controls. To be granted access in accordance with US Export Control laws, candidates must meet one of the following criteria: (a) be a United States citizen or national; (b) be a person lawfully admitted for permanent residence of the United States (i.e., "Green Card" holder); or (c) be an INS-approved refugee or asylum holder who has applied for naturalization within six months of becoming eligible. If not yet naturalized, the candidate must still be actively pursuing naturalization if two years have passed since the date of application. Candidates will be required to submit appropriate documentation to determine eligibility for access before proceeding further through the application process.

Duties and Responsibilities (Continued):

Proactive Capabilities Enhancement:

- Proactively validate preventative and detective capabilities and lead improvements, especially in cloud environment.
- Build relationships with IT teams to proactively develop and deploy security event detection systems, incident response procedures, and monitoring functions.

Operations Team Management:

- Support and oversee cyber event response activities as the most senior escalation point on the Security Operations team.
- Function as a cybersecurity subject matter expert who can stand on their own to deliver work and represent the team as well as lead their team to success through delegation.
- Lead development and tracking of key performance indicators (KPIs) related to cybersecurity operations, to benchmark and further enhance capabilities.

Status: Exempt
Reports To: Chief Information Security Officer
Workplace Type: Hybrid

Salary range of $226,000- $318,000.