Cyber Security Analyst - Job Description

Description

The Cyber Security Analyst (CSA) is responsible for assisting with the day-to-day operations of securing the firm's various information systems. Reporting to the Information Security Manager, the CSA is tasked with providing technical expertise in all areas of network, system, and application security. The CSA works closely with the various teams in the Information Technology department to ensure that systems and networks are always designed, developed, deployed, and managed with an emphasis on strong, effective security and risk management controls. The CSA leads the firm's vulnerability management program, manages the annual cybersecurity assessments and penetration tests, and researches and reports on emerging threats, to help the firm take pre-emptive risk mitigation steps. The CSA effectively correlates and analyzes security events within the context of AEW's unique environment to proactively detect threats and mitigate attacks before they occur.

Key Responsibilities

- Proactively monitor the environment to detect and implement steps to mitigate cyber-attacks before they occur.
- Provides technical expertise regarding security-related concepts to operational teams within the Information Technology Department and the business.
- Review, investigate, and respond to real-time alerts within the environment.
- Review real-time and historical reports for security and/or compliance violations.
- Monitor online security-related resources for new and emerging cyber threats.
- Assesses new security technologies to determine potential value for the enterprise.
- Conducts vulnerability assessments of firm systems and networks.
- Manage systems owned by the Information Security Team.

Demonstrable Requirements

- A four-year college degree or equivalent industry training and certifications.
- Three to five years of experience in a security analyst or related position.
- Technical knowledge of enterprise-class technologies such as firewalls, routers, switches, wireless access points, VPNs, and desktop and server operating systems.
- Thorough understanding of Microsoft's enterprise technology platform, including Azure, Active Directory, SQL, Office365, and the Windows server and desktop operating systems.
- Proficiency with Windows PowerShell.
- Working experience with the following technology vendors and products: Splunk Cloud, Rapid7 Nexpose Vulnerability Scanner, Sophos Antivirus, Varonis DatAlert, ForeScout CounterACT.
- Strong writing skills, as well as the ability to articulate security-related concepts to a broad range of technical and non-technical staff.
- Working experience with creating, implementing, and managing a threat hunting program within a corporate environment.
- Demonstrated experience implementing and/or enforcing security and compliance frameworks such as NIST, Cobit, and ISO.
- Be a proficient problem-solver that is able to work autonomously.

Desired Qualifications

- One or more of the following certifications: CEH, CISM, CompTIA Security+, CISSP, GSEC
- Experience with managing and securing both on-premise and hosted systems and applications.
- Experience with application and database security.