Job Title:	Senior Security Engineer – Incident Response	**Job Category:**	Information Security Incident Response
Department/Group:	Blue Team Alpha		
Location:	St. Paul, MN	**Travel Required:**	Up to 25% travel Required
Level/Salary Range:	DOE	**Position Type:**	Full-time

Job Description

ROLE AND RESPONSIBILITIES

The Senior Incident Response Security Engineer is responsible for incident response and investigation including preparation, documentation, and coordination with other teammates and teams, assisting with eradication and recovery, and any necessary post-incident activities. Additional duties include security technology management/design, boundary and network defense, endpoint defense, supporting information security incident response, and vulnerability/threat remediation and advising counterparts in the creation of or updating existing policies, standards, and practices.

The Incident Response Security Engineer is responsible for providing technical analysis and remediation of assets on a client's network during active incident response engagement. Must be able to provide forensic collection and analysis of infrastructure device logging information, as well as threat hunting tooling during active incident response engagements. Incident Response personnel are also tasked with Vulnerability Scanning and Penetration Testing duties as required. IR SE's are prepared to design, implement, and maintain complex security technologies and projects that support the underlying security policies and procedures to protect information assets. Provide input to the creation of new and updates to existing policies, standards and practices as necessary.

60% Incident Response:

- Triaging, recovering, and rebuilding Infrastructure devices during incidents while collecting forensic evidence for later analysis
- Maintain skillset on security and vulnerability trends. Remediate systems based on supplied threat intelligence information.
- Conduct Cyber Incident Forensic Investigations
- Recommend and remediate information systems based on incident attack vectors witnessed and exploited
- Provide support in the resolution and response to suspected and actual information security incidents, breaches, abuse or system failures. Analyze highly visible and complex security incidents to determine root cause and identify process or system changes to prevent reoccurrence. Recommend and perform fixes, security patches, disaster recovery procedures, and other required measures. Assure the preservation of cyber-attack evidence as appropriate.

25% Compromise Assessing

- Deploy IDS/EDR tooling and analyzing the results to determine if a company has been compromised, and to what extent

5% Red/Purple/Blue Event Participation

5% Penetration Testing/Vulnerability Scanning

5% Other Duties as Assigned

- Serve as a security resource on application development, database design, network and/or platform (operating system) projects, helping project teams comply with enterprise and Technology security procedures and capabilities.
- Participate in complex projects related to information security regulatory compliance and the implementation and maintenance of all information security programs, processes, and technologies. Assure the implementation of appropriate security configurations or re-configurations and work with appropriate teams to execute them as required.

QUALIFICATIONS AND EDUCATION REQUIREMENTS

- Bachelor's degree or equivalent work experience
- 7 years' experience installing, monitoring, and maintaining Information Security solutions
- 5 years' information system forensics experience
- 5 years' previous Incident Response Investigation Experience (as an Incident Responder)

PREFERRED REQUIREMENTS

- SANS GCIH or equivalent security certification
- SANS GIAH or equivalent security certification
- SANS GPEN or equivalent security certification
- Offensive Security Certified Professional or equivalent security certification
- SANS GIAC Certified Forensic Examiner (GCFE)

REQUIRED SKILLS

- Demonstrated understanding and working mastery of security-related technologies and practices, including: authentication and authorization systems, endpoint protection, encryption, segmentation strategies, vulnerability management, secure remote access, hyperconverged technologies, virtualization technologies, and a wide variety of firewalls
- Strong/diverse technical background in enterprise networking, firewall, storage options, server infrastructure, operating systems, database technologies, and desktop operating systems and security
- Strong understanding of Cloud Technologies (Azure, AWS, Google Cloud, etc.)
- Intimate knowledge of Virtualization Technology is a must (Hyper-V and VMware ESX)

PREFERRED SKILLS

- Demonstrated experience contributing and collaborating effectively as an informal leader in a high-functioning team
- Effective organizational, analytical, and independent problem-solving skills
- Successful experience coordinating and completing multiple tasks within established and changing deadlines
- Strong presentation skills with experience addressing and interfacing with executives and technical staff
- Experience working in DoD ecosystem, financial services, healthcare services, or other highly regulated/compliance-oriented environments
- Experience with regulatory compliance issues
- An enthusiasm for staying up to date with the very latest updates about security threats and solutions
- Strong time management and organizational skills
- Self-motivated and naturally problem-solving skills required

BENEFITS

We offer our employees a robust compensation package! Our comprehensive benefits include: medical, dental, and vision insurance coverage; 100% company-paid life and disability coverage, unlimited PTO after the first 100 days of employment, and much more. Blue Team Alpha proudly promotes from within as part of a strong commitment to providing career growth opportunities for employees of all levels. Our diverse business portfolio allows employees broad career options with the advantage of staying with the same organization.

The company is an equal opportunity employer and will not tolerate discrimination in employment on the basis of race, color, age, sex, sexual orientation, gender identity or expression, religion, disability, ethnicity, national origin, marital status, protected veteran status, genetic information, or any other legally protected classification or status.