Job Title: Cloud Security Engineer

Location: Sleepy Hollow, NY / Basking Ridge, NJ

Responsibilities

- Ensures applications and infrastructure are breach-resistant.
- Data Loss Prevention event triage and operationalization.
- Develop, promote and enforce security policies, rules and technologies throughout the entire cloud system.
- Leads investigations and takes corrective/preventive actions working closely with Information Security team.
- Review and enhance Service Control Policies and IAM by assessing, developing, implementing, optimizing and documenting a comprehensive and broad set of security technology solutions.
- Coding experience using AWS CLI, Terraform, Cloudformation to build automation scripts for bulk updates and reporting.
- Develop standard operating procedures and trainings for each Cloud technology.
- Expert on authentication paradigms: IAM policy management and Cloud KMS solutions.
- Develop and implement system hardening standards conforming to CIS benchmarks.
- Develop a Well Architected framework for Security, issues identification and remediations.
- Develop, evolve, and manage monitoring and alerting solutions to create a deep understanding of trends, anomalies, and incidents.
- Support cloud WAF solutions.
- Build, Review and investigate alerts generated from Cloud security tools and escalate as appropriate.
- Partner across the Security Operations team to respond to cybersecurity incidents.
- Develop and report Cloud security coverage metrics and remediation plans.
- Define procedures to validate the effectiveness of the design, deployment, and management of security controlsto maintain confidentiality, integrity, and availability of Cloud networks and technology platforms.
- Promote and drive adoption of Cloud security tooling across the enterprise.
- Architect and continuously improve security technology stack, process and procedures, support model and cross-function interactions.

Basic Qualifications:

- Familiarity with source code management tools (e.g., Github, Bitbucket)
- Certifications and understanding of Cloud (AWS, Microsoft Azure), IT Security (ISO 27001, PCI-DSS, CISSP, CCSP), and DevSecOps Working knowledge of code hardening techniques.
- Strong Programing/Scripting Skills Experience (eg: Python, Java etc.)
- Experience implementing and maintaining Zero-Trust environments
- Deep knowledge of network security in IaaS, PaaS and SaaS multi-cloud environments and data in transit security mechanisms Deep knowledge of common and industry standard cloud-native/cloud-friendly authentication mechanisms (OAuth, OpenID, SAML, etc.), as well as traditional methods such as Directory Services, Identity and Access Management (IAM), Single Sign-On (SSO), etc.
- Deep knowledge of IT security monitoring, detection and protection methods (Network Segregation, Firewalls, IDS, IPS, NAC, SIEM, etc.) Experience with IT security in service-oriented and microservices for cloud-based services Experience working with cloud security and governance tools, cloud access security brokers (CASBs) and virtualization technologies.