Job Description: Information Security Engineer

Customer Success

Following another year of rapid expansion Kim is looking for an Information Security Engineer with expertise in securing cloud solutions and deployments.

Your Profile

This employee will be a member of the DevOps team and will focus on managing all aspects of cloud security, such as secure creation and management of cloud resources, monitoring and alerting, logging and audit trail, networking, cloud-based IDS/IPS and DLP solutions, etc.

You must understand, design, and implement appropriate safeguards and security controls in various cloud environment to reduce overall risk.

The ideal candidate will be flexible, excel at multi-tasking, and flourish in a fast-paced and challenging environment. This person should be a self-starter, self-motivator and possess the ingenuity to excel in this position.

Responsibilities

To be successful, have fun and become part of the Kim team you need to:

- Be a key player on the DevOps team and lead the expansion of the Cloud Security unit within that.
- Provide expertise on securely deploying, managing, and ongoing maintenance in Azure.
- Create solutions that are scalable, repeatable, maintainable and secure.
- Secure IaaS/PaaS services for major cloud platforms.
- Evaluate, configure and deploy best-in-class cloud-based security solutions.
- Deeply understand cloud-based security solutions, their values and shortcomings, and act as a subject matter expert for their configuration, ongoing maintenance, and integrations.
- Identify and provide technical evaluation of risk in the enterprise, assist in the articulation and documentation of that risk, and solutions that mitigate those risks.
- Analyze and make recommendations for improvements to the cloud environments and associated services and configurations.

Preferred Skills and Experience

- Experience with Terraform, Kubernetes and containerization.
- Experience with Azure Security Center, vulnerability management, Microsoft 365 Security & Compliance, auditing, eDiscovery.
- Ability to diagnose and troubleshoot problems, as well as consult on architectural design and configuration changes.

- Track record of getting things done quickly and with quality.
- Ability to operate in a dynamic, evolving environment.
- Monitor and audit Microsoft Azure system and service changes.
- Lead all security efforts for integration of infrastructure and business solutions with cloud environments.
- Experience with Networking, Firewall, VPN, IPSec, Gateway.

Basic Qualifications

- Bachelor's degree in information technology, information security, computer science or similar technical field of study.
- 8+ years of information security, networking and/or systems administration experience.
- Certified Cyber Security Professional with one or more of the following CISM, CompTIA Security+, CISSP, CEH, CCSP.
- Experience integrating Azure with on-prem services like Active Directory, DNS, firewalls.
- Experience with Cloud Infrastructure Security, Zero Trust, IAM, Networking, and/or Data Security.
- Have previously worked with SaaS, PaaS, and IaaS providers, in which you provided guidance on secure system and service configuration.

Salary Range

The salary range for this role is $90,000 - $105,000.