Cloud Secuity Analyst

Responsibilities:-

A cloud security analyst is a professional responsible for ensuring the security of cloud computing environments within an organization. Their primary role is to identify and address security risks, vulnerabilities, and threats related to cloud-based systems, applications, and data.

- Conduct security assessments of cloud-based infrastructure, platforms, and applications to identify vulnerabilities, risks, and compliance issues.
- Develop and implement security measures, policies, and procedures to protect cloud-based assets and data from unauthorized access, data breaches, and other security threats.
- Monitor and analyze security events and incidents in cloud environments, and respond promptly to mitigate risks and minimize potential damages.
- Collaborate with cross-functional teams, including system administrators, network engineers, and software developers, to ensure cloud security best practices are followed throughout the organization.
- Perform regular security audits, vulnerability assessments, and penetration testing to evaluate the effectiveness of existing security controls and recommend improvements.
- Stay up-to-date with the latest industry trends, emerging threats, and best practices in cloud security, and provide recommendations for enhancing the organization's cloud security posture.
- Investigate and resolve security incidents, including analyzing logs, conducting forensic investigations, and documenting findings.
- Assist in the development and delivery of cloud security awareness and training programs for employees to promote a culture of security awareness within the organization.
- Participate in the design and implementation of secure cloud architectures, including identity and access management, encryption, network security, and data protection mechanisms.
- Collaborate with external auditors and regulatory bodies to ensure compliance with relevant security standards and regulations (e.g., GDPR, HIPAA, PCI-DSS).

Requirements:

- Bachelor’s degree in Computer Science/Engineering, Electrical Engineering, or related domain certifications such as Certified cloud security professional (CCSP), Certified Information Systems security professional (CISSP), Or cloud - specific certification (AWS certified security speciality, Axure Security Engineer Associate), CEH, OSCP are highly desirable.
- 2+ years of experience with cloud services (AWS, Azure, GCP)

- Experience in cyber security/IT highly preferred.
- Excellent leadership, communication (written and oral) and interpersonal skills.

About Us: - Kratikal Tech Private Limited is a leading cyber security firm that provides cyber security solutions to 145+ Enterprise customers and 1825+ SMEs, belonging to different industries including E-commerce, Fintech, BFSI, NBFC, Telecom, Consumer Internet, Cloud Service Platforms, Manufacturing, and Healthcare. The company was founded with the aim of helping enterprises at a global level combat cybercriminals using new-age technology-based cyber security solutions.

As of today, Kratikal has been awarded as the Top Cyber Security Startup at the 12th Top 100 CISO Awards. Kratikal has launched four products, TSAT, TDMARC, TPIR, and TLMS including VAPT services. Apart from the products receiving several recognitions and awards, Kratikal has also partnered with numerous renowned organizations worldwide...*for more details visit our* *https://kratikal.com/client*