
Job Requirement
Cloud Security Engineer

Job Description:
As a Cloud Security Engineer, you will be responsible for designing, implementing, and maintaining security solutions to protect our organization's cloud-based infrastructure, applications, and data. You will work closely with cross-functional teams to identify security risks, develop security policies and procedures, and implement security controls to mitigate threats and vulnerabilities. Your role will be critical in ensuring the confidentiality, integrity, and availability of our cloud resources while enabling secure and compliant operations in the cloud.

Key Responsibilities:

1. Design and implement security architecture for cloud environments, including infrastructure security, network security, identity and access management (IAM), encryption, and data protection.
2. Ensure compliance with industry regulations and standards (e.g., GDPR, HIPAA, PCI DSS) as well as cloud service provider security requirements.
3. Conduct security assessments, vulnerability scans, and penetration testing of cloud infrastructure and applications to identify security weaknesses and risks.
4. Develop incident response plans and procedures for cloud security incidents. Lead incident response efforts to investigate and mitigate security breaches or incidents.
5. Implement security automation using tools and technologies such as AWS Security Hub, Azure Security Center, or Google Cloud Security Command Center to automate security monitoring, compliance checks, and incident response.
6. Design and implement IAM policies, roles, and permissions to enforce least privilege access controls and ensure secure authentication and authorization in cloud environments.
7. Implement encryption mechanisms and key management solutions to protect data at rest and in transit in the cloud.
8. Configure and manage security monitoring tools, SIEM (Security Information and Event Management) solutions, and log management systems to detect and respond to security threats and anomalies.
9. Provide security training and awareness programs for employees, contractors, and partners to promote security best practices and compliance.
10. Create documentation, reports, and dashboards to communicate security posture, incidents, and remediation efforts to stakeholders and management.

Preferred Qualifications:

Job Requirement
Cloud Security Engineer

- Bachelor's degree in Computer Science, Information Security, or a related field. Advanced degree or relevant certifications (e.g., CISSP, CCSP, AWS Certified Security – Specialty, Azure Security Engineer) is a plus.
- 5+ years of proven experience as a security engineer, cybersecurity analyst, or similar role, with a focus on cloud security.
- Strong understanding of cloud computing concepts and architectures, as well as cloud service models (IaaS, PaaS, SaaS) and deployment models (public, private, hybrid).
- Hands-on experience with cloud security technologies and services offered by major cloud service providers (e.g., AWS, Azure, GCP), such as AWS Identity and Access Management (IAM), Azure Active Directory, or Google Cloud IAM.
- Experience with security assessment tools and methodologies, including vulnerability scanning, penetration testing, and security auditing.
- Knowledge of security compliance frameworks and standards (e.g., NIST, CIS, ISO 27001) and their application to cloud environments.
- Familiarity with security automation and scripting languages (e.g., Python, PowerShell) for security automation tasks.
- Strong analytical and problem-solving skills with the ability to analyze security incidents, assess risks, and recommend mitigating actions.
- Excellent communication and collaboration skills with the ability to work effectively in cross-functional teams and communicate security concepts to technical and non-technical stakeholders.
- Continuous learning mindset with a passion for staying updated on emerging cloud security threats, vulnerabilities, and best practices.