AWS SECURITY MANAGEMENT

WHAT IS AWS SECURITY MANAGEMENT?

AWS security management refers to the practices, tools, and services used to protect amazon web services (AWS) environments. it includes identity and access management (), network security, data protection, monitoring and logging, compliance, and incident response. key services include AWS IAM, AWS shield, AWS WAF, amazon GUARDDUTY, AWS config, and AWS CloudTrail.

SECURITY PRACTICES FOR CLOUD DEPLOYMENT: -

identity and access management (IAM): implement the principle of least privilege, use multi-factor authentication (MFA), and regularly review and audit access policies.

data encryption: encrypt data at rest and in transit using strong encryption methods.

network security: use firewalls, security groups, and network access control lists (ACLS) to restrict and control network traffic.

regular monitoring and logging: implement logging and monitoring to detect and respond to security incidents. use tools like AWS CLOUDTRAIL, AWS CLOUDWATCH, and security information and event management (SIEM) systems.

patch management: regularly update and patch systems, applications, and libraries to address vulnerabilities.

backup and disaster recovery: implement regular data backups and test disaster recovery plans to ensure data integrity and availability.

secure configuration: follow security best practices and frameworks like the cis benchmarks to configure cloud resources securely.

incident response planning: develop and test incident response plans to quickly mitigate and recover from security incidents.

compliance and auditing: ensure compliance with relevant regulations and standards. regularly audit cloud environments to identify and remediate security gaps.

CLOUD INSTITUTION

employee training and awareness: educate employees about security best practices, social engineering attacks, and how to recognize and report security threats.

AWS RESPONSIBILITIES: -

Physical Security: protecting the physical infrastructure that runs AWS services (e.g., data centers).
Network Security: ensuring the security of the network that supports the AWS cloud infrastructure.
Hardware and Software: securing the hardware and software that AWS uses to deliver its cloud services.
Global Infrastructure: managing and maintaining the facilities, physical security, and environmental safeguards.
Operational Security: ensuring the integrity and safety of AWS operations, including patches and security updates to the underlying infrastructure.

AWS SECURITIES: -

Data Protection: protecting data at rest and in transit using encryption and data masking.
Identity and Access management (IAM): managing IAM, including user accounts, roles, permissions, and policies.
Application Security: ensuring that applications are secure and free from vulnerabilities, following best practices for secure coding.
Network Configuration: configuring network security, including security groups, network ACLS, and VPNS.
Operating System and Application Patches: applying patches and updates to operating systems, applications, and middleware.

AWS CLOUD TRAIL: -

AWS CloudTrail is an AWS service that helps you enable operational and risk auditing, governance, and compliance of your AWS account. actions taken by a user, role, or an AWS service are recorded as events in CloudTrail. events include actions taken in the AWS management console, AWS command line interface, and AWS SDKS and APIS.

AWS TRUST ADVISOR: -

AWS Trusted Advisor is an online resource that helps you reduce cost, increase performance, improve security, and monitor service limits by providing real-time guidance based on AWS best practices. Trusted Advisor inspects your AWS environment and makes recommendations for improving it.

CLOUD INSTITUTION