**AWS Tools(Security):**

Wednesday, January 3, 2024

12:11 PM

* 1. **Identity and Access Management:**
     + **AWS Identity and Access Management (IAM): Manages user access and encryption keys.**
     + **IAM Roles and Policies: The specific use of roles for delegated permissions and policies for defining permissions.**
     + **IAM Groups: To manage sets of users and permissions.**
     + **IAM Access Advisor: To review service permissions.**
     + **Amazon Cognito: Handles user authentication and data synchronization for application access.**
     + **AWS Key Management Service (KMS): Manages cryptographic keys for data encryption.**
     + **Amazon Directory Service: Integration with existing on-premise Active Directory or setting up a new, standalone directory in the AWS Cloud.**
     + **AWS Single Sign-On (SSO): Centrally manage SSO access to multiple AWS accounts and business applications.**

* 1. **Threat Detection and Monitoring and logging:**
     + **Amazon GuardDuty: Offers continuous monitoring for malicious or unauthorized behavior.**
     + **AWS CloudTrail: Records AWS account activity for security monitoring.**
     + **AWS Security Hub: Aggregates security alerts and compliance status.**
     + **Amazon Inspector: Assesses applications for vulnerabilities and deviations from best practices.**
     + **Amazon Macie: Uses machine learning for data classification and protection.**
     + **Amazon Detective: Analyzes and visualizes security data for investigative purposes.**
     + **AWS Trusted Advisor Review: Is a service that review your account for best practices, at an account level it inspects our environments and makes recommendations based on best practice.**
     + **AWS Incident Response: Guides and tools to prepare and manage incidents, including automating the analysis of security events.**
     + **VPC Flow Logs: Captures information about the IP traffic going to and from network interfaces in your VPC.**
     + **Amazon CloudWatch Logs Insights: Enables interactive exploration of your log data, allowing you to find specific information within the logs.**

* 1. **Data Protection and Privacy:**
     + **AWS Secrets Manager: Manages access to secrets needed to access applications and services.**
     + **AWS Certificate Manager: Handles SSL/TLS certificates for secure data transfer.**
     + **Amazon Macie: Protects sensitive data through automatic discovery and classification.**
     + **Amazon KMS: Key Management System. AWS KMS is a managed service that makes it easy to create and control encryption keys used to encrypt data.**
     + **AWS CloudHSM: Offers hardware security modules in the cloud for customers requiring stringent key storage for regulatory or compliance needs.**

* 1. **Networking and Content Delivery:**
     + **AWS Direct Connect: Establishes a dedicated network connection from your premises to AWS, which can increase bandwidth throughput and provide a more consistent network experience than internet-based connections.**
     + **Amazon Route 53: A scalable and highly available Domain Name System (DNS) web service, also providing domain registration and DNS routing along with automated DDoS protection.**
     + **AWS Network Firewall: A managed service that provides network protections for your VPC.**
     + **AWS Transit Gateway: Connects VPCs and on-premises networks through a central hub to simplify network topology and reduce operational overhead.**
     + **Amazon VPC (Virtual Private Cloud): Offers a private, isolated section of the AWS cloud.**
     + **Amazon CloudFront: A content delivery network service.**
     + **AWS PrivateLink: Provides private connectivity between VPCs, AWS services, and on-premises applications, securely on the Amazon network.**
     + **AWS VPN (Virtual Private Network): Establishes a secure and private tunnel from the on-premises network or client to the AWS global network.**

* 1. **Infrastructure Protection:**
     + **AWS WAF (Web Application Firewall): Protects web applications from common web exploits.**
     + **AWS Shield: Provides DDoS protection.**
     + **AWS Firewall Manager: Centralizes firewall rule management across accounts and resources.**
     + **AWS Systems Manager Patch Manager: Automates the process of patching managed instances with both security related and other types of updates.**

* 1. **Compliance and Governance:**
     + **AWS Config: Tracks configurations and changes for compliance auditing.**
     + **AWS Artifact: Accesses security and compliance documentation.**
     + **AWS Well-Architected Tool: Reviews and improves workloads for compliance with AWS best practices.**

* 1. **Application Security:**
     + **AWS AppSync: Manages secure application data synchronization.**
     + **Amazon Cognito Sync: Synchronizes user profile data across mobile devices and the web without requiring your own backend code or database.**

* 1. **Compute Services:**
     + **Amazon EC2 (Elastic Compute Cloud): Provides scalable computing capacity.**
     + **AWS Lambda: Allows running code without managing servers.**
     + **Amazon Lightsail: Offers virtual private servers.**
     + **Amazon EC2 Auto-scaling: Automatically adjusts computing capacity.**
     + **AWS Elastic Beanstalk: Manages and deploys web applications.**

* 1. **Storage Services:**
     + **Amazon S3 (Simple Storage Service): Object storage service.**
     + **Amazon Glacier: Low-cost storage service for data archiving and backup.**
     + **Amazon EBS (Elastic Block Store): Block storage service for EC2 instances.**

* 1. **Database Services:**
     + **Amazon RDS (Relational Database Service): Simplifies setup, operation, and scaling of a relational database.**
     + **Amazon DynamoDB: A NoSQL database service.**
     + **Amazon ElastiCache: In-memory caching service.**

