Security, Identity & Compliance

This part of the course goes into the various ways of managing the AWS Security Framework and the tools that can be used.

Security, Identity, and Compliance:

Security, Identity, and Compliance are the three primary pillars of operating on AWS in a safe and secure way. Let's look into what each of these pillars brings to the table.

IAM (Identity and Access Management): allows you to manage users and their levels of access to the AWS resources.

Cognition: is used for device authentication / O Auth service, this service provides end users temporary access to AWS resources. Imagine you have an app that lets users upload pictures on to your S3. You can do this by using cognito.

Guard Duty: is used to monitor for malicious activity on your AWS account.

Inspector: is an agent installed on your virtual machine and you can run tests for security vulnerabilities etc.

Macie: is used to check your entire suite of application for personally identifiable information. Think PCI compliances.

It is a security service that uses machine learning to automatically discover

classify, and protect sensitive data in AWS.

Amazon Macie recognizes sensitive data such as personally identifiable information (PII) or intellectual property and provides you with dashboards and alerts that give visibility into how this data is being accessed or moved.

This fully managed service continuously monitors data access activity for anomalies and generates detailed alerts when it detects the risk of unauthorized access or inadvertent data leaks.

Certificate Manager: is used to give any domain you have registered via AWS/Routes S3 a certificate. This also helps in maintaining and updating certificates that are about to expire.

Cloud HSMHardware Security Module: is a dedicated Hardware to store your Hardware Private and Public key, that are used to securely access your application/EC2 instances. You can also store a variety of exception keys.

Directory Services: is used for integrating your Microsoft active directory services with AWS services.

WAF – Web Application Firewall:

WAF sits in front of your web server and it mitigates against injection, cross

scripting.

WAF primarily protects your application layer from any malicious attacks

Shield:

You get this as a default for your load balancers, cloud front, as well as Route 53. This is basically a DDoS mitigation service. Preventing DDoS Attacks.

Advance Shield:is an AWS team that is in standby mode in the case of a DDOS attack. If you have advance shield protection, then AWS will not charge you for any auto-scaling or added utilization of the AWS services during the attack.

Artifact: Is used for compliance and audit. It can be utilized for all the compliance and audit type of use cases.

Artifact gives access to AWS SOC 1, 2, 3, PCI reports, etc. Is a central resource for compliance-related information that matters to you. It provides on-demand access to AWS' security posture.