Domain 3: Secure Applications

Secure resource access

Security should be considered at every level, stage, and architecture.

The biggest security decision you make early is how the people tool and applications you build will access the necessary AWS resources. It will tell you how to manage the access that is given.

Identity and access management is how you will be giving access. How you create them, what kind of strength they have. Users and groups.

Least privilege.

Never hard code credentials into your application!

Learn about policy statement.

How does the IAM use policy statement.

Secure application tiers

Network ACLs and security groups provide security for the network traffics. It lets you control the incoming and outgoing traffics. You will have to add rules to control the traffic based on the protocol and port numbers.

For example: You can specify for TCP over port 443 to allow it or disallow it for say a EC2 instances.

You can use security groups along with VPC to control traffic that is allowed to leave the resource in a VPC. By default VPC have a default security group that allows all incoming and outgoing traffic for the resources in the VPC if you don't specify one.

External threat

What services can be used to protect against external attack against your applications?

What controls do they provide.

Data security options

How are the data protected during transit or when it is at rest?

How does the data storage services handle data protection? Are they encrypted?

Encryption options

How does the storage services handle encryption? How will the key be handled?

Does encryption affect performance?

AWS Key management service will help you generate, store, and control cryptographic keys.

Revision #2
Created 2023-01-06 19:28:31 UTC by Tamarine
Updated 2023-02-06 18:24:02 UTC by Tamarine