Well Architected Framework: Security

Security Design Principles

1. Apply security at all layers. E.g. Subnet, ACL's Ports that are open on the Load Balancer.
2. Enable tractability. E.g. ability to audit changes using load
3. Automate responses to security events E.g. if you detect someone trying to brute force port 22 then it triggers an SNS notification for someone to look at.
4. Focus on securing your system E.g. you are responsible for securing your data, your application, and your OS.
5. Automate security best practices E.g. look into "center for internet security" to understand how to harden images for Bastion jump boxes.

Security in the cloud consists of 4 areas

1. Data Protection
2. Privilege Management
3. Infrastructure Protection
4. Detective Controls

Best Practices – Data Protection

1. Encrypt data at rest
2. Encrypt data in motion
3. Regular key rotation
4. Detailed logging of changes and access to files
5. Versioning to protect against accidental overwrite deletes

Best Practices – Privilege Management

Ensures that only authorized and authenticated users are able to access the

resources: Privilege Management can be done using:

1. Access Control Lists (ACLs)
2. Role Based Access Controls
3. Password Management (password rotation)