AWS Cloud Practitioner Eseentials (4 AWS Security)

- (0) General
  - Approach to Security
    - Keep your data safe
      - Resilient infrastructure
      - High security
      - Strong safeguards
    - Continual Improvement
      - Rapid innovation
      - Constantly evolving security services
    - Pay for what you need
      - Advanced security services
      - Address real-tiem emerging risks
      - Meeting needs at a lower operational cost
    - Meet Compliance Requirements
      - Governance-enabled features: Additional oversight; Security control; Central automation
    - AWS Shared Responsibility Model
      - Inherit AWS Security Controls
      - Layer your controls
  - AWS Environment Controls
  - AWS Offerings and Features
    - Network Security
      - Built-in Firewalls
      - Encryption in transit
      - Private/dedicated connections
      - Distributed denial of service (DDoS) mitigation
    - Inventory and Configuration Mgmt
      - Deployment tools
      - Inventory and configuration tools
      - Template definition and management tools
    - Data Encryption
      - Encryption capabilities
      - Kay mgmt options: AWS Key Mgmt Service
      - Hardware-based cryptographic key strorage option: AWS CloudHSM
    - Access control and mgmt
      - Identity and Access Mgmt (IAM)
      - Multi-Factor Authentication (MFA)
      - Integration and Federation with Corporate Directories
      - Amazon Cognito
      - AWS SSO
    - Monitoring and Logging, to reduce risk profile
      - Deep visibility into API calls
      - Log aggregation and options
      - Alert notifications
- (1) The Shared Responsibility Model (Security is of the utmost importance to AWS)
  - AWS 100%
    - Physical
    - Network
    - Zen based Hypervisor
  - Customer 100%
    - If EC2
      - Guest OS
      - User Data
- (2) Identity and Access Management
  - User: a permanent named operator
  - Group: a collection of users
  - Role: a role is not the permission, it's the authentication method
  - Policy Documents (JSON): authorization
- (3) Amazon Inspector
  - IT Security Challenges
    - Complex
    - Expensive
    - Time Consuming - Build / Configure / Maintain
    - Difficult to track all the changes in IT environment
    - Hard to do effectively
  - Amazon Inspector is an automated security assessment service
    - Assesses applications for Vulnerabilities and Deviations from best practices
    - Produces a detail report with Security findings and Prioritized steps for remediation
  - Amazon does not guarantee that following the provied recommendations will resolve every potnetial security issue. The findings generated by Amazon Inspector depending on your choice of rules packages including in each assessment template, the presense of non-AWS components in your system, and other factors. You are responsible for the security of applications, processes, and tools that run on AWS services
  - Benefits
    - Identify application security issues
      - Agent based, API Driven
    - Integrate security into DevOps
    - Increase development agility
    - Leverage AWS security expertise
    - Streamline security compliance
    - Enforce seucrity standards
  - How to access
    - Amazon Inspector Console
    - AWS software development kits (SDKs)
    - Amazon Inspector HTTPS API
    - AWS command line tools
  - Built-in rules
    - Includes a knowledge base with hundreds of rules that are mapped to common security compliance standards, and vulnerability definitions
    - Regularly updated by AWS security researchers
- (4) Amazon Shield
- (5) Security Compliance