Flex-Protection Bullet Point Briefing: AWS Security

Review of Cloud Concepts

- AWS offers public, private, or mixed public/private (hybrid) OWNERSHIP models. Focus is on public cloud solutions here.
- Three DEPLOYMENT models are available, depending on the customer needs and capabilities: IaaS, PaaS, and SaaS.
- Infrastructure as a service (IaaS): offers essential compute, storage, and networking resources on demand, on a pay-as-you-go basis (Ex: hardware).
- Platform as a service (PaaS): provides a complete development and deployment environment in the cloud (Ex: Add Operating System and Web server).
- Software as a service (SaaS): allows users to connect to and use cloud-based applications over the Internet. Common examples are email and calendaring.
- Amazon AWS is one choice among many, including Microsoft Azure, Google Cloud, Oracle Cloud, IBM Cloud and others.
- The AWS overall security model is clear: they secure the cloud itself, and you secure what's in the cloud.
- HOWEVER, AWS provides many tools and systems to help you secure your systems and data, beyond securing the cloud itself.

AWS High-level Overview

- AWS is global in nature: uses many instances (ex: virtual computers) within "Availability Zones", within defined geographic Regions.
- Instances may be your servers, which are also virtual and based on templates.
- You can use existing templates or create your own as a basis for creating instances (virtual machines).
- Other virtual devices/components include software firewalls, sub-nets, and routers. You will create and configure these.
- You will need to review the storage options for your data when you create an instance. There are various ways to allocate your storage space.
- AWS has a free tier, with many limitations, as you might expect.

Identity and Access Management (IAM)

- IAM is the fundamental concept that governs all user accounts, roles, and permissions.
- When you launch your AWS service, you will establish a "root" account, which has total authority and permissions.
- Use the root account to establish user IAM User Groups, and add one or more users to each group. Ex: Administrators, Developers, etc.
- Assign permissions at the group level, and easily add users later. Use the "least privilege" best practice for every user group

Security tools and benefits provided by AWS

- Most security tools may be activated or disabled as you wish
- Your existing security strategies that you use on your in-house servers and applications (ex: database table with users & passwords), may be utilized on your AWS virtual machines
- AWS keeps your data safe – AWS infrastructure is robust, with multiple physical and electronic safeguards in place
- Privacy – your data is stored in secure data centers

- Compliance Requirements – several compliance programs are provided within the AWS infrastructure
- Includes attestations, regulations, alignments, frameworks

Partial List of AWS-Specific Security Features

- AWS Config – compliance auditing, security analysis, resource changes, deployment troubleshooting.
- AWS Service Catalog – organizes resources into Catalogs, including virtual machine (VM) images, servers, software and databases
- Amazon Guard Duty – threat detection and security monitoring
- AWS WAF – Amazon's configurable Web Application Firewall
- AWS Shield – specific protection from DOS/DDOS (Denial of Service) attacks
- AWS KMS – a key management service useful in managing encryption keys
- AWS Artifact – tools for compliance management and security reports
- AWS Inspector – designed to access, scan and troubleshoot security issues for applications you have deployed in your AWS account
- AWS Trusted Advisor – helps improve performance and cost-effectiveness by optimizing your AWS environment