VIRTUAL & ONSITE

AWS CRYPTO TRAINING

Class Audience > Beginners | Intermediate | Advanced

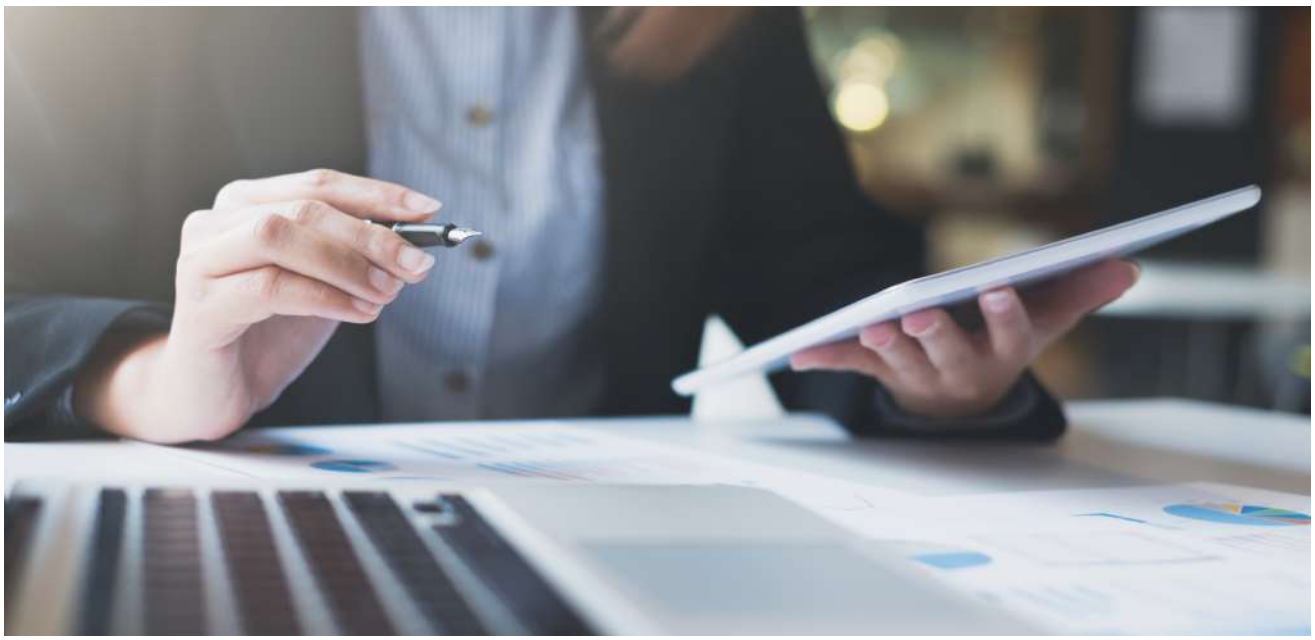
Upgrade Your
Amazon Web Services (AWS)
Crypto Services
Skills With A Training From
Encryption Consulting LLC

ENCRYPTION CONSULTING

About Course

This course demonstrates how to efficiently use AWS Cloud Crypto services to stay secure in the AWS Cloud. The course focuses on the data security best practices as per AWS and industry standards for enhancing the security of Cloud data and complementing Cloud Data governance.
The course highlights the security features of AWS Cryptographic and PKI services, including AWS ACM Private CA, AWS KMS, AWS CloudHSM, and data encryption methods. You will also learn how to leverage AWS services and tools for automation using Third party tools like Terraform, continuous monitoring and logging, and responding to security incidents.

Syllabus



DAY 01

Module 01

- Introduction to Cryptography
- Symmetric Encryption and Asymmetric Encryption
- Hash Functions and Digital Signatures
- Security design principles and Shared responsibility model in AWS
- DevOps integration of Terraform with AWS
- Introduction to PKI environment – On-Premises, Cloud, and Hybrid
- Introduction to AWS Crypto Services and tools (KMS, CloudHSM, and ACM Private CA)

Module 02 : Deep dive into AWS KMS

- Pre-requisites and Custom-built application integration
- Data Protection and Industry compliance (FIPS, SOC, PCI, HIPPA etc.) standard
- Functionality, Architecture and Design Considerations for Key Management as-a-service in AWS
- Understanding the Client-side and Server-side encryption techniques
- Understanding Customer Managed Keys, AWS Managed Keys, and Key Rotation Policies
  - Lab 01: Creation of AWS Managed CMKs and Customer Managed CMKs in AWS environment
- Understanding Symmetric and Asymmetric keys
  - Lab 02: Creation of Symmetric and Asymmetric Customer Managed Key (CMK)
- Understanding the concept of BYOK (Bring Your Own Key), and integration of KMS with HSM
- Management of Keys (AWS Managed CMKs and Customer Managed CMKs) as per FIPS 140-2 L2/L3 compliances
  - Lab 03: Integration of Customer Managed Key with FIPS 140-2 Level3 compliant HSM
- Integration of authentication and access control policy with various policies (Key, IAM, and grants)

AWS KMS use cases

- Lab 04: Encryption of S3 buckets using CMK
- Lab 05: Integration of AWS S3 bucket encryption with CMK using CloudHSM as a key storage
- Lab 06: Integration of Amazon EBS (Elastic Block Store) with CMK
- Lab 07: Digital Signing and verification of contents using CMK-Asymmetric feature
- Troubleshooting for CloudTrail logs, S3 permissions and HSM audit logs

DAY 02

Module 03: Deep dive into AWS CloudHSM

AWS CloudHSM

- Pre-requisites and Multi-Service Integration
- Data Protection, FIPS, and PCI-DSS Compliance
- Software Vs Hardware based HSMs
- Various CloudHSM Models
- Functionality, Architecture and Design Considerations for HSM as-a-service in AWS
- Application integration using Software Libraries to HSM
- CloudHSM prerequisite environment
  - Lab 01: Setting up a prerequisite for CloudHSM environment
- CloudHSM Cluster provisioning and management
  - Lab 02: Deploying CloudHSM cluster in Multi-AZ environment
- Install CloudHSM client Software
  - Lab 03: Installing CloudHSM client Software on Windows and Linux
- Provisioning HSMs (Hardware Security Modules) in the Cluster
  - Lab 04: Deploying HSMs in the CloudHSM cluster
- Learn with hands-on exercise on CloudHSM management and Key management command line tools
  - Lab 05: Activate the CloudHSM cluster using CloudHSM management CLI tool and crypto key operations using Key management CLI tool

CloudHSM use cases

- Lab 06: To provide private key protection of a Windows CA server with AWS CloudHSM service
- Lab 07: Bring your own key (BYOK) use case with CloudHSM
- Troubleshooting for CloudHSM client logs, CloudTrail logs and HSM audit logs

DAY 03

Module 04: Deep dive into AWS PKI Service (ACM Private CA)

AWS ACM Private CA

- Pre-requisites and Multi-Service Integration
- Cloud Security and Data protection
- Certificate Verification and Certificate Chaining
- Simple Storage Service (S3) as-a-CRL-Service Provider
- Various Cloud PKI Models in AWS
- Key factors in development of CP/CPS document to architect the PKI infra including Certificates and their attributes
- Key considerations to outline the Key ceremony document for Root CA
- Functionality, Architecture and Design Considerations for PKI as-a-service

ACM-PCA use case:

- Lab 01: Deploying 2 tier PKI architecture hands-on lab in AWS environment
- Troubleshooting of CloudTrail logs, Windows CA Server logs, S3 permissions

Certificate of Completion

Every student that attends and completes the full training scoring 70% in the AWS exam will receive a certificate of completion. The certificate will allow student to qualify for ISC2 continuing education credit for annual CPE commitments.

Why Encryption Consulting LLC?

ENCRYPTION CONSULTING
www.encryptionconsulting.com

Encryption Advisory Services

Encryption is used for securely protecting data from unauthorized access. Data encrypted can only be seen by those that possess the key to change the data back to plain text. Encryption is now one of the oldest yet still most effective technology solutions able to have data security

Public Key Infrastructure

PKI is a security ecosystem that has stood the test of time for achieving secure Internet-based transactions by the use of digital certificates. Digital certificates have provided security to servers and routers from the very early stages of the Internet through Public Key Infrastructure

Hardware Security Module – HSM

Hardware Security Modules provides protection and strong authentication with cryptographic processing by the use of digital keys inside a physical computing device. This device offers an isolated tamperproof environment which can create and secure cryptographic keys, protecting critical cryptographic operations, all while enforcing self-implemented policies over the keys.

Certificate Lifecycle

Certificates typically have a 4-phase lifecycle - Discovery, Enrollment, Provisioning, and End-of-life. To make your PKI mature and reliable, you must have more control over all the phases

Enterprise Encryption Platforms

Does your business have the need to encrypt large amounts of data-at-rest found in structured databases or in unstructured files across physical, cloud, or both types of environments? Do you want to protect data without disruptive changes to applications or business practices?

Cloud Data Protection Services

The transition towards uploading data on the public cloud is now becoming the normal standard. With relying on the cloud for data storage, cloud security must now become the number one priority for organizations

Encryption Consulting LLC.
130 N Preston Rd, Prosper, TX 75078, USA |
+1- 469-815-4136 | info@encryptionconsulting.com
www.encryptionconsulting.com

Find us:
"EncryptionConsulting" on

CONFIDENTIALITY. INTEGRITY. AVAILABILITY.