Security Engineering on AWS – Intensive Training («AWSS04»)

This course prepares you to become a AWS Certified Security (Specialty Level). You will learn AWS-recommended security best practices that you can implement to enhance the security of your data and systems in the cloud.

Duration: 3 days
Price: 2'500.–
Course documents: Digital original AWS courseware
Vendor code: AWSS04

Content

Day 1
Module 1: Security on AWS

- Security in the AWS cloud
- AWS Shared Responsibility Model
- Incident response overview
- DevOps with Security Engineering

Module 2: Identifying Entry Points on AWS

- Identify the different ways to access the AWS platform
- Understanding IAM policies
- IAM Permissions Boundary
- IAM Access Analyzer
- Multi-factor authentication
- AWS CloudTrail
- Lab 01: Cross-account access

Module 3: Security Considerations: Web Application Environments

- Threats in a three-tier architecture
- Common threats: user access
- Common threats: data access
- AWS Trusted Advisor

Module 4: Application Security

- Amazon Machine Images
- Amazon Inspector
- AWS Systems Manager
- Lab 02: Using AWS Systems Manager and Amazon Inspector

Module 5: Data Security

- Data protection strategies
- Encryption on AWS
- Protecting data at rest with Amazon S3, Amazon RDS, Amazon DynamoDB
- Protecting archived data with Amazon S3 Glacier
- Amazon S3 Access Analyzer
- Amazon S3 Access Points

Day 2

Module 6: Securing Network Communications

- Amazon VPC security considerations
- Amazon VPC Traffic Mirroring
- Responding to compromised instances
- Elastic Load Balancing
- AWS Certificate Manager

Module 7: Monitoring and Collecting Logs on AWS

- Amazon CloudWatch and CloudWatch Logs
- AWS Config
- Amazon Macie
- Amazon VPC Flow Logs
- Amazon S3 Server Access Logs
- ELB Access Logs
- Lab 03: Monitor and Respond with AWS Config

Module 8: Processing Logs on AWS

- Amazon Kinesis
- Amazon Athena
- Lab 04: Web Server Log Analysis

Module 9: Security Considerations: Hybrid Environments

- AWS Site-to-Site and Client VPN connections
- AWS Direct Connect
- AWS Transit Gateway

Module 10: Out-Of-Region Protection

- Amazon Route 53
- AWS WAF
- Amazon CloudFront
- AWS Shield
- AWS Firewall Manager
- DDoS mitigation on AWS

Day 3

Module 11: Security Considerations: Serverless Environments

- Amazon Cognito
- Amazon API Gateway
- AWS Lambda

Module 12: Threat Detection and Investigation

- Amazon GuardDuty
- AWS Security Hub
- Amazon Detective

Module 13: Secrets Management on AWS

- AWS KMS
- AWS CloudHSM
- AWS Secrets Manager
- Lab 05: Using AWS KMS

- AWS CloudFormation
- AWS Service Catalog
- Lab 06: Security automation on AWS with AWS Service Catalog

Module 15: Account Management and Provisioning on AWS

- AWS Organizations
- AWS Control Tower
- AWS SSO
- AWS Directory Service
- Lab 07: Federated Access with ADFS

Key Learnings

- Identifying security benefits and responsibilities of using the AWS Cloud
- Building secure application infrastructures
- Protecting applications and data from common security threats
- Performing and automating security checks
- Configuring authentication and permissions for applications and resources
- Monitoring AWS resources and responding to incidents
- Capturing and processing logs
- Creating and configuring automated and repeatable deployments with tools such as AMIs and AWS CloudFormation

Methodology & didactics

These hybrid courses come in 3 instructor-led full day sessions with the instructor supervising the participants live. Each course consits of theory parts with live demos and practical lab exercises. The courses can be attended either on-site at a physical Digicomp location or virtually via Zoom. Please also refer to each course's description for specific details regarding the prerequisites and the covered topics.

Target audience

This course is intended for the following job roles:

- Cyber Security
- Data Analytics

Why should you attend this specific course? What are my benefits from taking this course? The **Voice of the Instructor answers these questions**. We have asked our instructor team to write a short text about WHY this course is very relevant for the respective job roles and what you can expect from attending the course. You can find this section in the course description under the «*Additional Information*» section.

Requirements

We recommend that attendees of this course have attended the following course (or equivalent knowlege):

- AWS Security Essentials – Intensive Training («AWSE04»)
- Architecting on AWS – Intensive Training («AWSA01»)

Additional information

Participating in the «Security Engineering on AWS» course offers several compelling reasons for individuals interested in enhancing their skills and knowledge in AWS security. Here are some key benefits:

1. Comprehensive AWS Security Expertise: The course provides in-depth coverage of AWS security services, tools, and best practices. It equips you with the knowledge required to design, implement, and manage secure applications and infrastructure on AWS.
2. Protecting Data and Assets: AWS offers a robust set of security services and features, and this course helps you understand how to leverage them effectively. You'll learn about encryption, access controls, identity and access management (IAM), network security, and data protection mechanisms, enabling you to safeguard sensitive data and assets on AWS.
3. Compliance and Governance: Understanding compliance requirements and implementing appropriate controls is crucial for many organizations. The course helps you align your AWS deployments with industry standards and best practices.
4. Incident Response and Monitoring: Security incidents can occur despite preventive measures. The course delves into incident response strategies, threat detection, and monitoring techniques using AWS services like AWS CloudTrail, AWS Config, and Amazon GuardDuty. You'll gain insights into identifying and responding to security events promptly.
5. Industry Demand and Career Opportunities: With the increasing adoption of AWS by organizations worldwide, there is a growing demand for skilled professionals who can ensure the security of AWS deployments. By completing this course, you position yourself as a qualified security engineer with expertise in AWS, expanding your career opportunities in the field.
6. Practical Hands-on Experience: The course incorporates hands-on labs and real-world scenarios, allowing you to apply the learned concepts in practice. This hands-on experience gives you the confidence and proficiency to tackle security challenges effectively within an AWS environment.
7. AWS Certification Preparation: The knowledge gained from the course serves as a solid foundation for pursuing the AWS Certified Security - Specialty certification. This professional certification validates your expertise in securing AWS environments and adds credibility to your profile.

Overall, participating in the «Security Engineering on AWS» course equips you with the necessary skills, knowledge, and practical experience to secure AWS deployments effectively. It not only enhances your professional capabilities but also enables you to contribute to the secure and successful implementation of AWS solutions.

Further courses

- Security Engineering on AWS – JAM Day («AWSSJ4»)
- AWS Well-Architected Best Practices – Intensive Training («AWSE08»)

Any questions?

We are happy to advise you on +41 44 447 21 21 or info@digicomp.ch. You can find detailed information about dates on www.digicomp.ch/courses-it-provider/amazon-web-services-aws/aws-cyber-security/course-security-engineering-on-aws-intensive-training-awss04