Course : Amazon Web Services (AWS) - Security engineering on AWS

Official course, Security Engineering on AWS

Practical course - 3d - 21h00 - Ref. AWJ
Price : 2570 € E.T.

4,4 / 5

ActionCo | Nouvelle édition

Formation éligible au financement Atlas

With this course, you'll discover the security challenges facing cloud users and those considering cloud adoption. With cyber-attacks and data leaks on the rise, this Security Engineering on AWS course will help you understand how to work securely with AWS. You'll learn how to manage identities, roles and accounts, monitor API activity, protect data on AWS, and analyze logs to detect and investigate security incidents.

Teaching objectives

At the end of the training, the participant will be able to:

- Explaining AWS cloud security using the CIA model
- Create and analyze authentications and authorizations with IAM
- Manage and provision AWS accounts with appropriate AWS services
- Identify how to manage secrets using AWS services
- Monitor sensitive information and protect data with encryption and access controls
- Identify AWS services that respond to attacks from external sources
- Monitor, generate and collect logs
- Identify indicators of security incidents
- Identify how to investigate and mitigate threats using AWS services

Intended audience

Security engineers, security architects, cloud architects, cloud operators.

Prerequisites

Completion of AWS "Security Essential" or "Security Fundamentals" or "Architecting on AWS" training courses. Knowledge of IT security infrastructure concepts and practices.

PARTICIPANTS

Security engineers, security architects, cloud architects, cloud operators.

PREREQUISITES

Completion of AWS "Security Essential" or "Security Fundamentals" or "Architecting on AWS" training courses. Knowledge of IT security infrastructure concepts and practices.

TRAINER QUALIFICATIONS

The experts who lead the training courses are specialists in the subjects covered. They are approved by the publisher and certified for the course. They have also been validated by our teaching teams in terms of both professional knowledge and teaching skills for each course they teach. They have at least three to ten years of experience in their field and hold or have held positions of responsibility in companies.

ASSESSMENT TERMS

Assessment of targeted skills prior to training.
Assessment by the participant, at the end of the training course, of the skills acquired during the training course.
Validation by the trainer of the participant's learning outcomes, specifying the tools used: multiple-choice questions, role-playing exercises, etc.
At the end of each training course, ITTCERT provides participants with a course evaluation questionnaire, which is then analysed by our teaching teams. Participants also complete an official evaluation of the publisher.
An attendance sheet for each half-day of attendance is provided at the end of the training course, along with a certificate of completion if the participant has attended the entire session.

Practical details

Teaching methods

Training in French. Official course material in English and digital format. Good understanding of written English.

Course schedule

1 Security on AWS

- Explain security in the AWS cloud.
- Explain the AWS Shared Responsibility Model.
- Summarize IAM, data protection, threat detection and response.
- Show the different ways of interacting with AWS using the console, CLI and SDKs.
- Describe how to use multi-factor authentication (MFA) for additional protection.
- Indicate how to protect the root user account and access.

2 Securing entry points to AWS

- Describe how to use multi-factor authentication (MFA) for additional protection.
- Describe how to protect the root user account and access keys.
- Describe IAM policies, roles, policy components and permission limits.
- Securing entry points to AWS: MFA, root account protection, access keys and IAM policy management.
- Use AWS CloudTrail to record and view API requests, and analyze access history.

Hands-on work

Use of identity- and resource-based policies.

3 Account management and provisioning on AWS

- Explain how to manage multiple AWS accounts using AWS Organizations and AWS Control Tower.
- Explain how to set up multi-account environments with AWS Control Tower.
- Demonstrate the ability to use identity providers and brokers to access AWS services...
- Explain the use of AWS IAM Identity Center (successor to AWS Single Sign-On) and AWS Directory Service.
- Demonstrate the ability to manage domain user access with Directory Service and IAM Identity Center.

Hands-on work

Manage domain user access with AWS Directory Service.

TEACHING AIDS AND TECHNICAL RESOURCES

The teaching resources used are the publisher's official materials and practical exercises.

TERMS AND DEADLINES

Registration must be completed 24 hours before the start of the training course.

ACCESSIBILITY FOR PEOPLE WITH DISABILITIES

Do you have specific accessibility requirements? Contact Ms FOSSE, disability advisor, at the following address: psh-accueil@orsys.fr so that we can assess your request and its feasibility.

4 Managing secrets on AWS

- Describe and list the features of AWS KMS, CloudHSM, AWS Certificate Manager (ACM) and AWS Secrets Manager.
- Demonstrate how to create a multi-region AWS KMS key.
- Demonstrate how to encrypt a Secrets Manager secret with an AWS KMS key.
- Use an encrypted secret to connect to an Amazon RDS database in several AWS regions.

Hands-on work
Using AWS KMS to encrypt secrets in Secrets Manager.

5 Data security

- Monitor data for sensitive information with Amazon Macie.
- Explain how to protect data at rest with encryption and access controls.
- Identify AWS services used to replicate data for protection.
- Determine how to protect data once archived.

Hands-on work
Data security in Amazon S3.

6 Edge infrastructure protection

- Describe the AWS features used to build a secure infrastructure.
- Describe the AWS services used to create resilience in the event of an attack.
- Identify the AWS services used to protect workloads against external threats.
- Compare the features of AWS Shield and AWS Shield Advanced.
- Explain how centralized deployment via AWS Firewall Manager can improve security.

Hands-on work
Use AWS WAF to mitigate malicious traffic.

7 Monitoring and logging on AWS

- Identify the importance of generating and collecting logs.
- Use Amazon Virtual Private Cloud (Amazon VPC) flow logs to monitor security events.
- Explain how to monitor deviations from the baseline.
- Describe Amazon EventBridge events.
- Describe Amazon CloudWatch metrics and alarms.
- List log analysis options and available techniques.
- Identify the use cases for traffic mirroring in a virtual private cloud (VPC).

Hands-on work
Monitoring and responding to security incidents.

8 Responding to threats

- Classify incident types in incident response.
- Understand incident response workflows.
- Discover information sources for incident response using AWS services.
- Understand how to prepare for incidents.
- Detect threats using AWS services.
- Analyze and respond to safety findings.

Hands-on work
Incident response

Options

Certification : 360 € HT

La réussite de l'examen permet d'obtenir la certification AWS Certified Security - Specialty. (Prérequis - avoir suivi les formations : AWS Technical Essentials ou AWS Security Essentials, Architecting on AWS et Security Engineering on AWS).
Comment passer votre examen ?

The certification option comes in the form of a voucher or invitation that will allow you to take the exam at the end of the training course.

Dates and locations

REMOTE CLASS
2026 : 16 June, 29 Sep., 8 Dec.

PARIS LA DÉFENSE
2026 : 16 June, 29 Sep., 8 Dec.