# Security Engineering on AWS

Duration: 3 days
Audience: Professionnel TI

## Who is this training for?

- Security Engineers
- Security Architects
- Security Operations
- Security Information.

## Training objectives

- Assimilate and leverage AWS's shared security model
- Design and integrate application infrastructures that protect against the most common security threats
- Protect data at rest and in transit with encryption
- Apply security controls and analytics in an automated and repeatable manner
- Configure authentication of resources and applications in the AWS Cloud
- Gather event information by capturing, monitoring, processing, and analyzing logs
- Identify and mitigate incoming threats to applications and data
- Conduct security assessments to ensure common vulnerabilities are resolved and security best practices are applied

## Summary

This course explains how to effectively use AWS security services to work securely in AWS Cloud. This course focuses on AWS recommended security practices to improve the security of your data and systems in the cloud. This course highlights the security features built into core AWS services, including compute, storage, networking, and database services. You'll also learn how to leverage AWS services and tools to automate, monitor, and log your activities continuously, and respond to security incidents. Learn how to use common DevOps practices to develop, deploy, and manage applications on AWS securely.

## Course outline

### Module 1: Introduction to AWS Security

- AWS Shared Responsibility Model
- Cloud Security Principles
- Security Governance and Frameworks

### Module 2: Identity and Access Management (IAM)

- AWS IAM (Users, Roles, Policies)
- MFA and Best Practices
- AWS Organizations and Account Control
- Access Management with AWS SSO / IAM Identity Center

### Module 3: Network Infrastructure Protection

- VPC Security (Subnets, Routing)
- Security Groups vs NACL
- AWS Shield and AWS WAF
- AWS Firewall Manager

### Module 4: Data Protection

- Encryption at Rest and in Transit
- AWS KMS and Key Management
-

AWS CloudHSM

- Secrets Management (AWS Secrets
- Manager, Parameter Store)

**Module 5: AWS Service Security**

- Securing EC2, S3, RDS, Lambda
- Secure Service Configuration
- Architecture Best Practices

**Module 6: Monitoring and Logging**

- AWS CloudTrail (Auditing)
- Amazon CloudWatch (Monitoring)
- AWS Config (Compliance)
- Centralizing Logs

**Module 7: Threat Detection and Incident Response**

- Amazon GuardDuty
- AWS Security Hub
- Amazon Inspector
- Incident Response Playbooks

**Module 8: Security Automation**

- Secure Infrastructure-as-Code
- Automating Controls (AWS Config Rules)
- Automatic Remediation

**Module 9: Assessment and Compliance**

- Security Audits
- AWS Artifact Standards (ISO, PCI-DSS, CIS benchmarks)

## Approach and methodology

This course combines theoretical lectures with demonstrations and hands-on labs to immediately apply security concepts on AWS. Participants work on real-world cases, analyze secure architectures, and use AWS services to configure, monitor, and automate security. Interactive exchanges and role-playing complete the learning.

## Prerequisites

- Basic knowledge of AWS services (EC2, S3, VPC, IAM)

## Recommendations

- Hands-on experience with AWS or prior training (e.g. AWS Technical Essentials / Architecting on AWS)
- Understanding of IT security concepts (network, encryption, access management)
- Experience in systems administration or security can be an asset