Security Engineers, protect your serverless applications!

AWS Classroom Training

Course description

This course gives security engineers an exposure to and practice with best practices for securing serverless applications using AWS Lambda and other services in the AWS serverless platform. You will implement security measures to ensure the protection of serverless resources and data to avoid application outages. The hands-on exercises challenge you to ensure how to apply security at all layers, and safe guard your serverless applications from security threats.

- Course level: Intermediate
- Duration: 4 hours

Activities

This course includes presentations, demonstrations, and lab exercises.

Course objectives

In this course, you will learn to:

- Apply security best practices to serverless applications at all layers
- Compare and contrast how AWS security shared responsibility model differs between serverless and server-based infrastructure
- Identify potential security threats to a serverless application and how AWS services protect from DDoS attacks
- Implement identify and access controls to secure API endpoints and backend integrations
- Safe guard your applications limiting the access rate and filtering traffic through API Gateway
- Apply the principle of least privilege when granting permissions to your resources
- Protect the data at rest and in transit while accessing through Amazon DynamoDB, Amazon S3, and Amazon CloudFront
- Protect and control how secrets are handled in applications using AWS KMS, Systems Manager Parameter store, and Secrets Manager
- Compare and contrast different ways of accessing key data using AWS SDKs that is secured with KMS, Parameter Store, and Secrets Manager using AWS SDKs
- Review AWS services and features available to implement auditing and security automations

Intended audience

This course is intended for:

- Security Engineers
- Cloud Developers

Security Engineers, protect your serverless applications!

AWS Classroom Training

- Solutions Architects

Prerequisites

We recommend that attendees of this course have:

- Familiarity with the basics of AWS Cloud architecture and network controls
- Basic understanding of Identity and Access Management (IAM), encryption, and developing aspects using AWS SDKs
- Basic knowledge of serverless applications and AWS services such as AWS Lambda, Amazon API Gateway, Amazon DynamoDB, etc.

Bootcamp outline

Module 0: Introduction

- Introduction to bootcamp
- Access to resources (Hands-on lab interface, instructions)

Module 1: Understanding Serverless Security Model

- AWS security shared responsibility model for serverless applications
- Common security threats to modern applications
- Best practices for securing serverless applications

Module 2: Securing applications from bad actors

- Control web traffic before reaching to serverless resources using AWS Shield, Amazon CloudFront, and AWS Web Application Firewall (WAF).
- Protect your web applications from common web exploits using AWS Web Application Firewall (WAF).
- Control access to APIs using throttling and request filtering.
- Mitigate security risks to lambda functions from SQL injections, dependency vulnerabilities, and, untrusted code packages.
- Hands-on exercise: Securing applications with AWS WAF ACLs.

Module 3: Controlling access to serverless resources

- Identify permissions for Lambda functions
- Options for authenticating to APIs using API Gateway
- Controlling access to APIs using resource policies
- Hands-on exercise: Securing applications using API Gateway resource policies

Security Engineers, protect your serverless applications!

AWS Classroom Training

Module 4: Protecting data accessed in serverless resources

- How encryption works with API Gateway, Amazon S3, and Amazon DynamoDB
- Protect data passed to Lambda functions using AWS KMS, Parameter Store, and Secrets Manager.
- Control access using S3 bucket policies and Origin Access Identifiers.
- Hands-on exercise: Secure data passed to AWS Lambda functions

Module 5: Monitoring activity

- Review AWS services that help automating security solutions.
- Compare and contrast how AWS Config and Amazon CloudTrail handle auditability.
- Hands-on exercise: Troubleshoot and resolve security issues to reinstate application functionality.