AWS101 - DEFENDING AWS

Course Learning Objectives

This course is part of the line of defending against threats to cloud. Defending AWS builds on the foundations of cloud security in the context of Amazon Web Services.

In six modules, we'll explore user identity management, using AWS Security Hub for ensuring safe cloud deployments, managing cloud resources, protecting network traffic, using AWS Inspector and AWS GuardDuty for monitoring cloud deployments, and protecting sensitive data at rest in the cloud.

Description

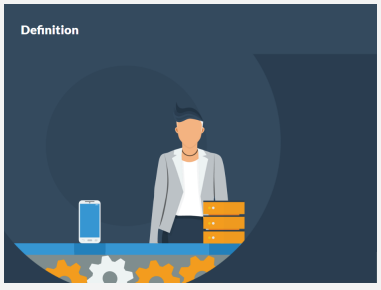
Defending AWS was created for DevOps and Ops Engineers who have some familiarity with application security. This course focuses on configuring AWS to defend against the most common security threats using best practices.

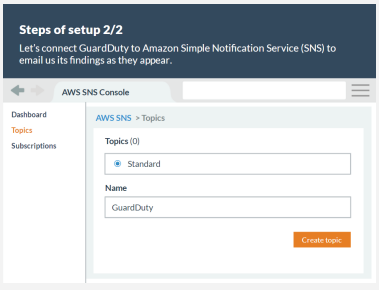
Audience

DevOps/Ops Engineers

Time Required

Tailored learning - 60 minutes total





AWS101 - DEFENDING AWS

Course Outline

1. Identity Management

- About Amazon Cognito
- Components
- Access protection
- MFA
- Data protection
- Logging and monitoring
- About AWS IAM
- ABAC

2. Security Hub

- Overview
- Enable AWS Security Hub
- Insights in AWS Security Hub
- Automate response and remediation

3. Layered Security Architecture

- Virtual Private Cloud
- Security Groups for VPC
- VPC Flow Logs
- VPN Connection

4. Infrastructure Protection

- AWS Network Firewall
- About the Network Firewall
- Network Firewall Setup
- AWS Web Application Firewall
- Application Firewall Setup

5. Security Detection

- Introduction
- AWS Inspector definition
- Setup
- AWS GuardDuty definition
- Setup

6. Data Protection

- AWS Macie
- Setup
- AWS Cloud HSM
- AWS Key Management Service
- AWS Secrets Manager

SecurityCompass