Description

Securing Cloud Workloads with DevOps Automation is designed to teach security engineers, developers, solutions architects, and other technical security practitioners how to use a DevSecOps approach to design and build robust security controls at cloud scale for next-generation workloads. This bootcamp walks through the design considerations of operating high-assurance workloads on top of the AWS platform and provides hands-on labs on governance, configuration management, trust-decision automation, audit artifact generation, and native integration of these tasks into custom software workloads.

Course Objectives

This course teaches you how to:

- Design your organizational security controls to employ the features of the AWS platform for robust security operations at scale that oversee different workloads, networks, and accounts.
- Assemble custom configuration pipelines and workflows using AWS CloudFormation, Amazon Simple Workflow Service (SWF), and Jenkins to streamline your ongoing security and compliance operations.
- Build security into your software through native integrations to AWS services such as AWS Identity and Access Management and AWS Key Management Service (KMS).
- Capture and preserve audit artifacts such as application logs, execution environments, and human approvals.

Intended Audience

This course is intended for:

- Security engineers
- Developers and DevOps engineers
- Solutions architects
- Other hands-on security practitioners

Prerequisites

We recommend that attendees of this course have the following prerequisites:

- Good understanding of information security techniques such as defining and implementing security controls, maintaining roles and responsibilities, generating artifacts, and performing audits
- Good understanding of the AWS security model, including shared responsibility, compliance reports, and security best practices
- Working knowledge of core AWS services and features, including Amazon Elastic Compute Cloud (EC2), Auto Scaling, Amazon Virtual Private Cloud, Amazon Elastic Block Store, and Amazon Simple Storage Service (S3)
- Fundamental understanding of software development paradigms such as encryption, logging, version control systems, workflow engines, pub/sub notifications, and making AWS API calls

- Basic understanding of system administration activities such as identity and access management, configuration management, remote administration, and automation frameworks

Delivery Method

This course is delivered through a mix of:

- Instructor-Led Training (ILT)
- Hands-On Labs

Duration

One day

Course Outline

This course covers the following concepts:

- Assembling a configuration inventory and change-management pipeline using AWS CloudFormation and Jenkins
- Securing ongoing Amazon EC2 scaling operations through Amazon SWF and Amazon EC2 Container Service (ECS)
- Building application micro-segmentation and leveraging it for network intrusion prevention and robust centralized logging
- Building tailored identity and access management logic into the application architecture for code-driven authorization decisions
- Integrating AWS KMS into a custom application for record-level double-redundant data access control