

**Document Generated:** 11/15/2024

**Learning Style:** On Demand

**Provider:** Cisco

**Difficulty:** Intermediate

**Course Duration:** 40 Hours

## Securing Cloud Deployments with Cisco Technologies (SECCLD) v1.0 - On Demand



### About this course:

The Securing Cloud Deployments with Cisco Technologies (SECCLD) v1.0 e-learning course shows you how to implement Cisco® cloud security solutions to secure access to the cloud, workloads in the cloud, and Software as a Service

(SaaS) user accounts, applications, and data.

Through instructor video, text, and hands-on labs, you'll learn a comprehensive set of skills and technologies including how to: use key Cisco cloud security solutions; detect suspicious traffic flows, policy violations, and compromised devices; implement security controls for cloud environments; and implement cloud security management. This course covers usage of Cisco Cloudlock, Cisco Umbrella™, Cisco Cloud Email Security, Cisco Advanced Malware Protection (AMP) for Endpoints, Cisco Stealthwatch® Cloud and Enterprise, Cisco Firepower® NGFW (next-generation firewall), and more.

## **Course Objective:**

After taking this course, you should be able to:

- Contrast the various cloud service and deployment models
- Implement the Cisco Security Solution for SaaS using Cisco Cloudlock Micro Services
- Deploy cloud security solutions using Cisco AMP for Endpoints, Cisco Umbrella, and Cisco Cloud Email Security
- Define Cisco cloud security solutions for protection and visibility using Cisco virtual appliances and Cisco Stealthwatch Cloud
- Describe the network as a sensor and enforcer using Cisco Identity Services Engine (ISE), Cisco Stealthwatch Enterprise, and Cisco TrustSec®
- Implement Cisco Firepower NGFW Virtual (NGFWv) and Cisco Stealthwatch Cloud to provide protection and visibility in Amazon Web Services (AWS) environments
- Explain how to protect the cloud management infrastructure by using specific examples, defined best practices, and AWS reporting capabilities

## **Audience:**

- Security architects
- Cloud architects
- Security engineers
- Cloud engineers
- System engineers
- Cisco integrators and partners

## **Prerequisite:**

To fully benefit from this course, you should have completed the following course or obtained the equivalent knowledge and skills:

- Knowledge of cloud computing and virtualization software basics
- Ability to perform basic UNIX-like OS commands
- Cisco CCNP® Security level of knowledge

## **Course Outline:**

- **User and Entity Behavior Analytics, Data Loss Prevention (DLP), and Apps Firewall**
- **Cloud Access Security Broker (CASB)**
- **Cisco CloudLock as the CASB**
- **OAuth and OAuth Attacks**
- **Deploying Cisco Cloud-Based Security Solutions for Endpoints and Content Security**
- **Cisco Cloud Security Solutions for Endpoints**
- **AMP for Endpoints Architecture**
- **Cisco Umbrella**
- **Cisco Cloud Email Security**
- **Design Comprehensive Endpoint Security**
- **Introducing Cisco Security Solutions for Cloud Protection and Visibility**
- **Network Function Virtualization (NFV)**
- **Cisco Secure Architectures for Enterprises (Cisco SAFE)**
- **Cisco NGFWv/Cisco Firepower Management Center Virtual**
- **Cisco ASAv**
- **Cisco Services Router 1000V**
- **Cisco Stealthwatch Cloud**
- **Cisco Tetration Cloud Zero-Trust Model**
- **The Network as the Sensor and Enforcer**
- **Cisco Stealthwatch Enterprise**
- **Cisco ISE Functions and Personas**
- **Cisco TrustSec**
- **Cisco Stealthwatch and Cisco ISE Integration**
- **Cisco Encrypted Traffic Analytics (ETA)**
- **Implementing Cisco Security Solutions in AWS**
- **Explain AWS Security Offerings**
- **AWS Elastic Compute Cloud (EC2) and Virtual Private Cloud (VPC)**
- **Discover Cisco Security Solutions in AWS**
- **Cisco Stealthwatch Cloud in AWS**
- **Cloud Security Management**
- **Cloud Management and APIs**
- **API Protection**
- **An API Example: Integrate to ISE Using pxGrid**
- **Identify SecDevOps Best Practices**
- **Cisco Cloud Security Management Tool Example: Cisco Defense Orchestrator**
- **Cisco Cloud Security Management Tool Example: Cisco CloudCenter**
- **Cisco Application Centric Infrastructure (ACI)**
- **AWS Reporting Tools**

**Credly Badge:**

**Display your Completion Badge And Get The**



## Recognition You Deserve.

Add a completion and readiness badge to your LinkedIn profile, Facebook page, or Twitter account to validate your professional and technical expertise. With badges issued and validated by Credly, you can:

- Let anyone verify your completion and achievement by clicking on the badge
- Display your hard work and validate your expertise
- Display each badge's details about specific skills you developed.

Badges are issued by QuickStart and verified through Credly.

[Find Out More](#) or [See List Of Badges](#)