Course Outline

Cisco Cloud Training
Course SECCLD: 4 days Instructor Led

All Cisco courses are delivered by a Cisco Authorized Platinum Learning Partner

About this course

The Securing Cloud Deployments with Cisco Technologies (SECCLD) 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 expert instruction 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.

Audience profile

- Engineers, administrators, and security-minded users of public, private, and hybrid cloud infrastructures responsible for implementing security in cloud environments
- Security architects
- Cloud architects
- Security engineers
- Cloud engineers
- System engineers
- Cisco integrators and partners

At course completion

After completing this course, students will 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 AWS environments.
- Explain how to protect the cloud management infrastructure by using specific examples, defined best practices, and AWS reporting capabilities.

Course Outline

SHI | TRAINING & ADOPTION

Course Outline

Module 1: Introducing the Cloud and Cloud Security

- Describe the Evolution of Cloud Computing
- Explain the Cloud Service Models
- Explore the Security Responsibilities Within the Infrastructure as a Service (IaaS) Service Model
- Explore the Security Responsibilities Within the Platform as a Service (PaaS) Service Model
- Explore the Security Responsibilities Within the SaaS Service Model
- Describe Cloud Deployment Models
- Describe Cloud Security Basics

Module 2: Implementing the Cisco Security Solution for SaaS Access Control

- Explore Security Challenges for Customers Using SaaS
- Describe User and Entity Behavior Analytics, Data Loss Prevention (DLP), and Apps Firewall
- Describe Cloud Access Security Broker (CASB)
- Describe Cisco CloudLock as the CASB
- Describe OAuth and OAuth Attacks

Module 3: Deploying Cisco Cloud-Based Security Solutions for Endpoints and Content Security

- Describe Cisco Cloud Security Solutions for Endpoints
- Describe AMP for Endpoints Architecture
- Describe Cisco Umbrella
- Describe Cisco Cloud Email Security
- Design Comprehensive Endpoint Security

Module 4: Introducing Cisco Security Solutions for Cloud Protection and Visibility

- Describe Network Function Virtualization (NFV)
- Describe Cisco Secure Architectures for Enterprises (Cisco SAFE)
- Describe Cisco NGFWv/Cisco Firepower Management Center Virtual
- Describe Cisco ASAv
- Describe Cisco Services Router 1000V
- Describe Cisco Stealthwatch Cloud
- Describe Cisco Tetration Cloud Zero-Trust Model

Module 5: Describing the Network as the Sensor and Enforcer

- Describe Cisco Stealthwatch Enterprise
- Describe Cisco ISE Functions and Personas
- Describe Cisco TrustSec
- Describe Cisco Stealthwatch and Cisco ISE Integration
- Describe Cisco Encrypted Traffic Analytics (ETA)

Module 6: Implementing Cisco Security Solutions in AWS

- Explain AWS Security Offerings
- Describe AWS Elastic Compute Cloud (EC2) and Virtual Private Cloud (VPC)

Course Outline

- Discover Cisco Security Solutions in AWS
- Explain Cisco Stealthwatch Cloud in AWS

Module 7: Describing Cloud Security Management

- Describe Cloud Management and APIs
- Explain API Protection
- Illustrate an API Example: Integrate to ISE Using pxGrid
- Identify SecDevOps Best Practices
- Illustrate a Cisco Cloud Security Management Tool Example: Cisco Defense Orchestrator
- Illustrate a Cisco Cloud Security Management Tool Example: Cisco CloudCenter™
- Describe Cisco Application Centric Infrastructure (ACI)
- Describe AWS Reporting Tools

Lab Outline

- Explore the Cisco Cloudlock Dashboard and User Security
- Explore Cisco Cloudlock Application and Data Security
- Explore Cisco AMP Endpoints
- Perform Endpoint Anaylsis Using the AMP Endpoint Console
- Examine the Umbrella Dashboard
- Examine Cisco Umbrella Investigate
- Explore Email Ransomware Protection by Cisco Cloud Email Security
- DNS Ransomware Protection by Cisco Umbrella
- Explore File Ransomware Protection by Cisco AMP for Endpoints
- Explore a Ransomware Execution Example
- Implement Cisco ASAv in ESXi
- Configure and Test Basic Cisco ASAv Network Address Translation (NAT)/Access Control List (ACL) Functions
- Explore Cisco Stealthwatch Cloud
- Explore Stealthwatch Cloud Alerts Settings, Watchlists, and Sensors
- Explore the Network as the Sensor and Enforcer
- Explore Cisco Stealthwatch Enterprise
- Deploy NGFWv and FMCv in AWS
- Troubleshoot FTD and FMC in AWS – Scenario 1
- Troubleshoot FTD and FMC in AWS – Scenario 2
- Troubleshoot FTD and FMC in AWS – Scenario 3
- Explore AWS Reporting Capabilities