Securing Cloud Deployments with Cisco Technologies (SECCLD)

ID SECCLD   **Price** CHF 4,600.—(excl. VAT)   **Duration** 4 days

Who should attend

This course is open to 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

Prerequisites

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 knowledge or understanding of the following topic areas:

Course Objectives

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 AWS environments
- Explain how to protect the cloud management infrastructure by using specific examples, defined best practices, and AWS reporting capabilities

Course Content

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

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

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

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 (FMCv)/Cisco AMP for Networks
- Describe Cisco ASAv

- Describe Cisco Services Router 1000V (CSR1Kv)
- Describe Cisco Stealthwatch Cloud
- Describe Cisco Tetration Cloud Zero-Trust Model

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)

Implementing Cisco Security Solutions in AWS

- Explain AWS Security Offerings
- Describe AWS Elastic Compute Cloud (EC2) and Virtual Private Cloud (VPC)
- Discover Cisco Security Solutions in AWS
- Explain Cisco Stealthwatch Cloud in AWS

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

Training Centres worldwide

Fast Lane Institute for Knowledge Transfer (Switzerland) AG

Husacherstrasse 3
CH-8304 Wallisellen
Tel. +41 44 832 50 80

info@flane.ch, https://www.flane.ch