

SECCLD

Securing Cloud Deployments with Cisco Technologies

The Securing Cloud Deployments with Cisco Technologies (SECCLD) v1.0 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.

Course Contents

- Introducing the Cloud and Cloud Security
- Implementing the Cisco Security Solution for SaaS Access Control
- Deploying Cisco Cloud-Based Security Solutions for Endpoints and Content Security
- Introducing Cisco Security Solutions for Cloud Protection and Visibility
- Describing the Network as the Sensor and Enforcer
- Implementing Cisco Security Solutions in AWS

E-Book You will receive the original course documentation from Cisco in English language as a Cisco E-Book. In the Cisco Digital Learning Version, the content of the courseware is integrated into the learning interface instead.

Target Group

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:

Processing time
approx. 24 hours

This Course in the Web



You can find the up-to-date information and options for ordering under the following link:

www.expertech-training.com/go/SCLD

Reservation

On our Website, you can reserve a course seat for 7 days free of charge and in a non-committal manner. This can also be done by phone under +49 6074/4868-0.

Guaranteed Course Dates

To ensure reliable planning, we are continuously offering a wide range of guaranteed course dates.

Your Tailor-Made Course!

We can precisely customize this course to your project and the corresponding requirements.

Cisco Digital Learning

This course is available in the Cisco Digital Learning Library. These recently developed, multi-modal training events include HD videos moderated by lecturers with stored searchable text and subtitles, as well as exercises, labs, and explanatory text and graphics. We provide this offer to you via our myExpertech learning portal. Effective of the activation of the account, access to the courses will be granted for a duration of 6 months. In the case of packet solutions (Cisco Digital Learning Subscriptions), this time period will amount to 12 months.

Cisco Digital Learning	Prices, excl. of V.A.T.
12 Monate Freischaltung	€ 1,500

Training	Prices, excl. of V.A.T.
Classes in Germany	4 Days € 4,595
Online Training	4 Days € 4,595
Dates upon request	

Status 05/07/2024

SECCLD

Security



EXPERTech



Table of Contents

SECCLD – Securing Cloud Deployments with Cisco Technologies

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

