

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.

Kursinhalt

- 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
- Describing Cloud Security Management

E-Book Sie erhalten die englischen Original-Unterlagen als Cisco E-Book. Bei der Cisco Digital Learning Version sind die Inhalte der Kursunterlage stattdessen in die Lernoberfläche integriert.

Zielgruppe

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.

Voraussetzungen

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

Bearbeitungszeit

ca. 24 Stunden

Dieser Kurs im Web



Alle tagesaktuellen Informationen und Möglichkeiten zur Bestellung finden Sie unter dem folgenden Link: www.experteach.ch/go/SCLD

Vormerkung

Sie können auf unserer Website einen Platz kostenlos und unverbindlich für 7 Tage reservieren. Dies geht auch telefonisch unter 06074 4868-0.

Garantierte Kurstermine

Für Ihre Planungssicherheit bieten wir stets eine große Auswahl garantierter Kurstermine an.

Ihr Kurs maßgeschneidert

Diesen Kurs können wir für Ihr Projekt exakt an Ihre Anforderungen anpassen.

Cisco Digital Learning & Cisco U.

Die multimodalen Schulungen der Cisco Digital Learning Library beinhalten referenzgeführte HD-Videos mit hinterlegtem durchsuchbarem Text und Untertiteln, Übungen, Labs und erklärenden Text sowie Grafiken. Das Angebot stellen wir Ihnen über unser Lernportal myExperTeach zur Verfügung. Der Zugriff auf die Kurse steht ab der Freischaltung für einen Zeitraum von sechs Monaten zur Verfügung. Bei Paketen (Cisco U.) beträgt dieser Zeitraum zwölf Monate.

Cisco Digital Learning & Cisco U. Preise zzgl. MwSt.

6 Monate Freischaltung **CHF 1.655,-**

Training Preise zzgl. MwSt.

Termine in der Schweiz 4 Tage

Online Training 4 Tage CHF 5.055,-

Termine auf Anfrage



Inhaltsverzeichnis

SECCLD – Securing Cloud Deployments with Cisco Technologies

Course Outline	Describe Cisco NGFWv/Cisco Firepower Management Center Virtual	Lab Outline
Introducing the Cloud and Cloud Security: Describe the Evolution of Cloud Computing	Describe Cisco ASA	Explore the Cisco Cloudlock Dashboard and User Security
Explain the Cloud Service Models	Describe Cisco Services Router 1000V	Explore Cisco Cloudlock Application and Data Security
Explore the Security Responsibilities Within the Infrastructure as a Service (IaaS) Service Model	Describe Cisco Stealthwatch Cloud	Explore Cisco AMP Endpoints
Explore the Security Responsibilities Within the Platform as a Service (PaaS) Service Model	Describe Cisco Tetration Cloud Zero-Trust Model	Perform Endpoint Analysis Using the AMP Endpoint Console
Explore the Security Responsibilities Within the SaaS Service Model	Describing the Network as the Sensor and Enforcer: Describe Cisco Stealthwatch Enterprise	Examine the Umbrella Dashboard
Describe Cloud Deployment Models	Describe Cisco ISE Functions and Personas	Examine Cisco Umbrella Investigate
Describe Cloud Security Basics	Describe Cisco TrustSec	Explore Email Ransomware Protection by Cisco Cloud Email Security
Implementing the Cisco Security Solution for SaaS Access Control: Explore Security Challenges for Customers Using SaaS	Describe Cisco Stealthwatch and Cisco ISE Integration	DNS Ransomware Protection by Cisco Umbrella
Describe User and Entity Behavior Analytics, Data Loss Prevention (DLP), and Apps Firewall	Describe Cisco Encrypted Traffic Analytics (ETA)	Explore File Ransomware Protection by Cisco AMP for Endpoints
Describe Cloud Access Security Broker (CASB)	Implementing Cisco Security Solutions in AWS: Explain AWS Security Offerings	Explore a Ransomware Execution Example
Describe Cisco CloudLock as the CASB	Describe AWS Elastic Compute Cloud (EC2) and Virtual Private Cloud (VPC)	Implement Cisco ASA in ESXi
Describe OAuth and OAuth Attacks	Discover Cisco Security Solutions in AWS	Configure and Test Basic Cisco ASA Network Address Translation (NAT)/Access Control List (ACL) Functions
Deploying Cisco Cloud-Based Security Solutions for Endpoints and Content Security: Describe Cisco Cloud Security Solutions for Endpoints	Explain Cisco Stealthwatch Cloud in AWS	Explore Cisco Stealthwatch Cloud
Describe AMP for Endpoints Architecture	Describing Cloud Security Management: Describe Cloud Management and APIs	Explore Stealthwatch Cloud Alerts Settings, Watchlists, and Sensors
Describe Cisco Umbrella	Explain API Protection	Explore the Network as the Sensor and Enforcer
Describe Cisco Cloud Email Security	Illustrate an API Example: Integrate to ISE Using pxGrid	Explore Cisco Stealthwatch Enterprise
Design Comprehensive Endpoint Security	Identify SecDevOps Best Practices	Deploy NGFWv and FMCv in AWS
Introducing Cisco Security Solutions for Cloud Protection and Visibility: Describe Network Function Virtualization (NFV)	Illustrate a Cisco Cloud Security Management Tool Example: Cisco Defense Orchestrator	Troubleshoot FTD and FMC in AWS – Scenario 1
Describe Cisco Secure Architectures for Enterprises (Cisco SAFE)	Illustrate a Cisco Cloud Security Management Tool Example: Cisco CloudCenter™	Troubleshoot FTD and FMC in AWS – Scenario 2
	Describe Cisco Application Centric Infrastructure (ACI)	Troubleshoot FTD and FMC in AWS – Scenario 3
	Describe AWS Reporting Tools	Explore AWS Reporting Capabilities

