

Securing Cloud Deployments with Cisco Technologies

Durée: 4 Jours Réf de cours: SECCLD Version: 1.0

Résumé:

The Securing Cloud Deployments with Cisco Technologies 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.

Public visé:

Engineers and administrators responsible for implementing security in a cloud environment whether that be a public, private or hybrid cloud infrastructure.

Objectifs pédagogiques:

- **After completing 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.

Pré-requis:

Attendees should meet the following prerequisites:

- Knowledge of cloud computing and virtualization software basics
 - Ability to perform basic UNIX-like OS commands
- Cisco CCNP security knowledge or an understanding of the following topic areas:**
- Cisco Adaptive Security Appliance (ASA) and Adaptive Security Virtual Appliance (ASAv) deployment
 - Cisco IOS Flexible NetFlow operations
 - Cisco NGFW (Cisco Firepower Threat Defense [FTD]), Cisco Firepower, and Cisco Firepower Management Center (FMC) deployment
 - Cisco Content Security operations including Cisco Web Security Appliance (WSA)/Cisco Email Security Appliance (ESA)/Cisco Cloud Web Security(CWS)
 - Cisco AMP for network and endpoints deployment
 - Cisco ISE operations and Cisco TrustSec architecture
 - VPN operation

Test et certification

Recommended as preparation for the following exams:

- There are currently no exams linked to this course

- SENSS - Mettre en oeuvre les solutions Cisco pour sécuriser son réseau d'entreprise (Cisco Edge Network)
 - SIMOS - Mettre en oeuvre la sécurité pour la mobilité avec les produits Cisco
 - SISAS - Mettre en oeuvre les solutions Cisco Secure Access
 - SITCS - Gestion des menaces avec les produits de sécurité Cisco Threat Control Systems
-

Contenu:

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
- Describe Cisco ASA v
- Describe Cisco Services Router 1000V
- 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

Labs

- Lab 1: Explore the Cisco Cloudlock Dashboard and User Security
- Lab 2: Explore Cisco Cloudlock Application and Data Security
- Lab 3: Explore Cisco AMP Endpoints
- Lab 4: Perform Endpoint Analysis Using the AMP Endpoint Console
- Lab 5: Examine the Umbrella Dashboard
- Lab 6: Examine Cisco Umbrella Investigate
- Lab 7: Explore Email Ransomware Protection by Cisco Cloud Email Security
- Lab 8: DNS Ransomware Protection by Cisco Umbrella
- Lab 9: Explore File Ransomware Protection by Cisco AMP for Endpoints
- Lab 10: Explore a Ransomware Execution Example
- Lab 11: Implement Cisco ASA v in ESXi
- Lab 12: Configure and Test Basic Cisco ASA v Network Address Translation (NAT)/Access Control List (ACL) Functions
- Lab 13: Explore Cisco Stealthwatch Cloud
- Lab 14: Explore Stealthwatch Cloud Alerts Settings, Watchlists, and Sensors
- Lab 15: Explore the Network as the Sensor and Enforcer
- Lab 16: Explore Cisco Stealthwatch Enterprise
- Lab 17: Deploy NGFWv and FMCv in AWS
- Lab 18: Troubleshoot FTD and FMC in AWS – Scenario 1
- Lab 19: Troubleshoot FTD and FMC in AWS – Scenario 2
- Lab 20: Troubleshoot FTD and FMC in AWS – Scenario 3
- Lab 30: Explore AWS Reporting Capabilities

Autres moyens pédagogiques et de suivi:

• Compétence du formateur : Les experts qui animent la formation sont des spécialistes des matières abordées et ont au minimum cinq ans d'expérience d'animation. Nos équipes ont validé à la fois leurs connaissances techniques (certifications le cas échéant) ainsi que leur