SECCLD (SECURING CLOUD DEPLOYMENTS WITH CISCO TECHNOLOGIES) 1.0

Objetivo

This class will help you: â¢ Learn how to deploy and troubleshoot Cisco cloud security solutions to protect your cloud, users, data, and applications; â¢ Prevent breaches and quickly detect and mitigate attacks; improve security and incident response, and more; â¢ Learn skills that can be applied to both public and private solutions including Amazon Web Services (AWS), Google Cloud Platform (GCP), IBM Cloud, Microsoft Azure, Dimension Data Cloud, Alibaba Cloud, VMware Cloud, and other cloud solutions; â¢ Gain leading-edge skills for high-demand jobs focused on enterprise security. After taking this course, you should be able to: â¢ Contrast the various cloud service and deployment models â¢ Implement the Cisco Security Solution for SaaS using Cisco Cloudlock Micro Services â¢ Deploy cloud security solutions using Cisco AMP for Endpoints, Cisco Umbrella, and Cisco Cloud Email Security â¢ Define Cisco cloud security solutions for protection and visibility using Cisco virtual appliances and Cisco Stealthwatch Cloud â¢ Describe the network as a sensor and enforcer using Cisco Identity Services Engine (ISE), Cisco Stealthwatch Enterprise, and Cisco TrustSecÂ® â¢ Implement Cisco Firepower NGFW Virtual (NGFWv) and Cisco Stealthwatch Cloud to provide protection and visibility in AWS environments â¢ Explain how to protect the cloud management infrastructure by using specific examples, defined best practices, and AWS reporting capabilities

PÃºblico Alvo

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.

PrÃ©-Requisitos

To fully benefit from this course, you should have completed the following course or obtained the equivalent knowledge and skills: â¢ Knowledge of cloud computing and virtualization software basics; â¢ Ability to perform basic UNIX-like OS commands; Cisco CCNPÂ® security knowledge or understanding of the following topic areas: â¢ Cisco Adaptive Security Appliance (ASA) and Adaptive Security Virtual Appliance (ASAv) deployment, and Cisco IOSÂ® Flexible NetFlow operations â¢ Cisco NGFW (Cisco Firepower Threat Defense [FTD]), Cisco Firepower, and Cisco Firepower Management Center (FMC) deployment â¢ Cisco Content Security operations including Cisco Web Security Appliance (WSA)/ Cisco Email Security Appliance (ESA)/Cisco Cloud Web Security (CWS) â¢ Cisco AMP for network and endpoints deployment â¢ Cisco ISE operations and Cisco TrustSec architecture â¢ VPN operation

Carga HorÃ¡ria

32 horas (4 dias).

ConteÃºdo ProgramÃitico

Course Introduction
Course Outline
Course Goals & Objectives

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
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 Anaylsis 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 ASAv in ESXi
Lab 12: Configure and Test Basic Cisco ASAv 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 21: Explore AWS Reporting Capabilities