skillsoft
global
knowledge™

SECCLD - SECURING CLOUD DEPLOYMENTS WITH CISCO TECHNOLOGIES V1.0

Course Code: 5130

Learn to deploy and troubleshoot Cisco cloud security solutions.

This course includes Cisco Training Exclusives

EXCLUSIVE TO GLOBAL KNOWLEDGE - Enhance your Cisco learning experience with complimentary access to our Introduction to Cybersecurity On-Demand course, course recordings, IT Resource Library, and digital courseware.

Learn more

The *SECCLD - Securing Cloud Deployments with Cisco Technologies 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 the 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.

This course is eligible for 32 Continuing Education Credits (ILT & ELT Modality).

What You'll Learn

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.

Who Needs to 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 courses or obtained the equivalent knowledge and skills listed below:

- Knowledge of cloud computing and virtualization software basics
- Ability to perform basic UNIX-like OS commands

Cisco CCNP Security or 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 Applicance (WSA)/Cisco Email
- Security Applicance (ESA)/Cisco Cloud Web Security (CWS)
- Cisco AMP for network and endpoints deployment
- Cisco ISE operations and Cisco TrustSec architecture VPN operation

Visit us at www.globalknowledge.com or call us at 1-866-716-6688.

Date created: 12/15/2025 1:53:03 PM