

SECCLD - SECURING CLOUD DEPLOYMENTS WITH CISCO TECHNOLOGIES V1.0

Course Code: 5130

Learn to deploy and troubleshoot Cisco cloud security solutions.

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 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

SECCLD - SECURING CLOUD DEPLOYMENTS WITH CISCO TECHNOLOGIES V1.0

Course Code: 5130

VIRTUAL CLASSROOM LIVE

\$4,913 CAD

4 Day

Virtual Classroom Live Outline

- User and Entity Behavior Analytics, Data Loss Prevention (DLP), and Apps Firewall
- Cloud Access Security Broker (CASB)
- Cisco CloudLock as the CASB
- OAuth and OAuth Attacks
- Deploying Cisco Cloud-Based Security Solutions for Endpoints and Content Security
- Cisco Cloud Security Solutions for Endpoints
- AMP for Endpoints Architecture
- Cisco Umbrella
- Cisco Cloud Email Security
- Design Comprehensive Endpoint Security
- Introducing Cisco Security Solutions for Cloud Protection and Visibility
- Network Function Virtualization (NFV)
- Cisco Secure Architectures for Enterprises (Cisco SAFE)
- Cisco NGFWv/Cisco Firepower Management Center Virtual
- Cisco ASAv
- Cisco Services Router 1000V
- Cisco Stealthwatch Cloud
- Cisco Tetration Cloud Zero-Trust Model
- The Network as the Sensor and Enforcer
- Cisco Stealthwatch Enterprise
- Cisco ISE Functions and Personas
- Cisco TrustSec
- Cisco Stealthwatch and Cisco ISE Integration

- Cisco Encrypted Traffic Analytics (ETA)
- Implementing Cisco Security Solutions in AWS
- Explain AWS Security Offerings
- AWS Elastic Compute Cloud (EC2) and Virtual Private Cloud (VPC)
- Discover Cisco Security Solutions in AWS
- Cisco Stealthwatch Cloud in AWS
- Cloud Security Management
- Cloud Management and APIs
- API Protection
- An API Example: Integrate to ISE Using pxGrid
- Identify SecDevOps Best Practices
- Cisco Cloud Security Management Tool Example: Cisco Defense Orchestrator
- Cisco Cloud Security Management Tool Example: Cisco CloudCenter
- Cisco Application Centric Infrastructure (ACI)
- AWS Reporting Tools

Virtual Classroom Live Labs

- Explore the Cisco Cloudlock Dashboard and User Security
- Explore Cisco Cloudlock Application and Data Security
- Explore Cisco AMP Endpoints
- Perform Endpoint Analysis Using the AMP Endpoint Console
- Examine the Umbrella Dashboard
- Examine Cisco Umbrella Investigate
- Explore Email Ransomware Protection by Cisco Cloud Email Security
- DNS Ransomware Protection by Cisco Umbrella
- Explore File Ransomware Protection by Cisco AMP for Endpoints
- Explore a Ransomware Execution Example
- Implement Cisco ASAv in ESXi
- Configure and Test Basic Cisco ASAv Network Address Translation (NAT)/Access Control List (ACL) Functions
- Explore Cisco Stealthwatch Cloud
- Explore Stealthwatch Cloud Alerts Settings, Watchlists, and Sensors
- Explore the Network as the Sensor and Enforcer
- Explore Cisco Stealthwatch Enterprise
- Deploy NGFWv and FMCv in AWS
- Troubleshoot FTD and FMC in AWS - Scenario 1
- Troubleshoot FTD and FMC in AWS - Scenario 2
- Troubleshoot FTD and FMC in AWS - Scenario 3
- Explore AWS Reporting Capabilities

Aug 11 - 14, 2025 | 8:30 AM - 4:30 PM EDT

Jan 26 - 29, 2026 | 8:30 AM - 4:30 PM EST

SECCLD - SECURING CLOUD DEPLOYMENTS WITH CISCO TECHNOLOGIES V1.0

Course Code: 5130

ON-DEMAND

\$1,997 CAD

On-Demand Outline

- User and Entity Behavior Analytics, Data Loss Prevention (DLP), and Apps Firewall
- Cloud Access Security Broker (CASB)
- Cisco CloudLock as the CASB
- OAuth and OAuth Attacks
- Deploying Cisco Cloud-Based Security Solutions for Endpoints and Content Security
- Cisco Cloud Security Solutions for Endpoints
- AMP for Endpoints Architecture
- Cisco Umbrella
- Cisco Cloud Email Security
- Design Comprehensive Endpoint Security
- Introducing Cisco Security Solutions for Cloud Protection and Visibility
- Network Function Virtualization (NFV)
- Cisco Secure Architectures for Enterprises (Cisco SAFE)
- Cisco NGFWv/Cisco Firepower Management Center Virtual
- Cisco ASAv
- Cisco Services Router 1000V
- Cisco Stealthwatch Cloud
- Cisco Tetration Cloud Zero-Trust Model
- The Network as the Sensor and Enforcer
- Cisco Stealthwatch Enterprise
- Cisco ISE Functions and Personas
- Cisco TrustSec
- Cisco Stealthwatch and Cisco ISE Integration

- Cisco Encrypted Traffic Analytics (ETA)
- Implementing Cisco Security Solutions in AWS
- Explain AWS Security Offerings
- AWS Elastic Compute Cloud (EC2) and Virtual Private Cloud (VPC)
- Discover Cisco Security Solutions in AWS
- Cisco Stealthwatch Cloud in AWS
- Cloud Security Management
- Cloud Management and APIs
- API Protection
- An API Example: Integrate to ISE Using pxGrid
- Identify SecDevOps Best Practices
- Cisco Cloud Security Management Tool Example: Cisco Defense Orchestrator
- Cisco Cloud Security Management Tool Example: Cisco CloudCenter
- Cisco Application Centric Infrastructure (ACI)
- AWS Reporting Tools

On-Demand Labs

- Explore the Cisco Cloudlock Dashboard and User Security
- Explore Cisco Cloudlock Application and Data Security
- Explore Cisco AMP Endpoints
- Perform Endpoint Analysis Using the AMP Endpoint Console
- Examine the Umbrella Dashboard
- Examine Cisco Umbrella Investigate
- Explore Email Ransomware Protection by Cisco Cloud Email Security
- DNS Ransomware Protection by Cisco Umbrella
- Explore File Ransomware Protection by Cisco AMP for Endpoints
- Explore a Ransomware Execution Example
- Implement Cisco ASAv in ESXi
- Configure and Test Basic Cisco ASAv Network Address Translation (NAT)/Access Control List (ACL) Functions
- Explore Cisco Stealthwatch Cloud
- Explore Stealthwatch Cloud Alerts Settings, Watchlists, and Sensors
- Explore the Network as the Sensor and Enforcer
- Explore Cisco Stealthwatch Enterprise
- Deploy NGFWv and FMCv in AWS
- Troubleshoot FTD and FMC in AWS - Scenario 1
- Troubleshoot FTD and FMC in AWS - Scenario 2
- Troubleshoot FTD and FMC in AWS - Scenario 3
- Explore AWS Reporting Capabilities



SECCLD - SECURING CLOUD DEPLOYMENTS WITH CISCO TECHNOLOGIES V1.0

Course Code: 5130

PRIVATE GROUP TRAINING

4 Day

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

Date created: 5/9/2025 5:06:08 AM

Copyright © 2025 Global Knowledge Training LLC. All Rights Reserved.