

Course Outline

Cisco Secure Workload Firewall Enforcement Agents, Data Flow Mapping, and Advanced Policy Deployment Course CSWADV: 5 days Instructor Led

About this course

Cisco Secure Workload Firewall Enforcement Agents, Data Flow Mapping, and Advanced Policy Deployment, CSWADV, is a 5-day course exploring telemetry data, the flows corpus, and how Cisco Secure Workload Firewall Agent provides enforcement. This course will provide the details and hands-on activities necessary to successfully deploy, manage, and troubleshoot policies in Cisco Secure Workload.

At course completion

After completing this course, students will be able to:

- Describe how the Cisco Secure Workload Agents work to enforce security policy
- Describe how to deploy the Cisco Secure Workload Firewall Agent
- Describe how to Manage and Troubleshoot Cisco Secure Workload Firewall Agent policies
- Review administrative and management tasks necessary to operate, support and manage Cisco Secure Workload
- Describe how Cisco Secure Workload telemetry data is utilized in the Flows Corpus
- Construct effective policies based on discovered flows and Application Dependency Mapping (ADM)

Course Outline

Module 1: Cisco Secure Workload Firewall Agent

- How the Cisco Secure Workload Firewall Agent Enforces Firewall Rules
- Deploying and Managing Linux Enforcement Agents
- Deploying and Managing Windows Enforcement Agents
- Deploying and Managing AIX Enforcement Agents

Module 2: Cisco Secure Workload Enforcement Agent Components, Messaging, and Interaction

- Enforcement Front End
- Firewall and Catch-all Rules
- The Preserve Rules Option
- Agent Config Intents
- Stateful Enforcement

Module 3: Enforcement Agent UI Configurations and Troubleshooting

- Agent UI Configuration
- Monitoring Agents
- Platform Specific Enforcement Features and Requirements
- Known Limitations
- Troubleshooting Inbound and Outbound Firewall Rules

Module 4: Secure Connector, Edge and Ingest Appliances

Course Outline

- Secure Connector Overview
- Secure Connector features and configuration
- Edge Appliance Overview
- Edge Appliance configuration
- Ingest Appliance Overview
- Ingest appliance features and configurations

Module 5: Application Dependency Mapping

- Application Management Workflow Cycle
- Application Insight
- ADM Process
- ADM Run Results
- Cluster Confidence

Module 6: Cisco Secure Workload Policy Analysis

- Enable Policy Analysis
- Live Policy Analysis
- Backdated Policy Experiments
- Quick Policy Analysis
- Diagnosis Using Policy Analysis

Module 7: Cisco Secure Workload Analytics Policy Enforcement Overview

- Policy Global Ordering & Conflict Resolution
- Scope Priorities
- Troubleshooting Policy Enforcement

Module 8: Cisco Secure Workload Flow Search

- Understanding the Flow Corpus
- Using Scopes to Filter Results
- Searching with Conjunctions
- Correlating Flow Data with Hosts and Processes
- Leveraging Annotations

Module 9: Using Secure Workload Forensics

- Forensic Signals
- Configuring Forensics
- Forensics Visualization and Alerts
- Forensics Scoring
- Network and Process Hash Anomaly Detection

Module 10: Cisco Secure Workload Apps and API

- App Store

Course Outline

- User Apps
- Visualize Data Sources
- Bring your own Data
- OpenAPI

Lab Outline

Labs are designed to assure learners a whole practical experience, through the following practical activities:

Lab 1: Cisco Secure Workload GUI Familiarization

- Task 1: Log in to Cisco Secure Workload and Explore the Security Dashboard
- Task 2: Explore the Visibility Dashboard
- Task 3: Explore the Visibility Flow Search Options
- Task 4: Explore the Visibility Inventory Search Options

Lab 2: Software Agent Installation

- Task 1: Configure Agent Intents
- Task 2: Install the Enforcement Agent for Linux
- Task 3: Install the Enforcement Agent for Windows
- Task 4: Monitor Enforcement Agent Status

Lab 3: Importing Context Data

- Task 1: Upload User-Defined Annotations
- Task 2: View User-Defined Annotations
- Task 3: Search by User-Defined Annotations

Lab 4: Scopes

- Task 1: Navigate Scopes
- Task 2: Create a Scope
- Task 3: Edit a Scope

Lab 5: Application Dependency Mapping with Agents

- Task 1: Create an Application Workspace
- Task 2: Examine Conversations
- Task 3: Examine Endpoint Clusters
- Task 4: Create an Application View

Lab 6: Implementing Policy

- Task 1: Gather IP Address Information
- Task 2: Create the Server Load Balancing Information File
- Task 3: Create an Application Workspace
- Task 4: Review Day 0 and Automated Policies

Course Outline

Lab 7: Policy Enforcement and Compliance

- Task 1: Enable Policy Enforcement and Compliance
- Task 2: Test Policy Enforcement and Compliance
- Task 3: Monitor and Troubleshoot Policy Enforcement Status and Compliance

Lab 8: Workload Security

- Task 1: Review Packages and CVE Reports
- Task 2: Review Policy Enforcement
- Task 3: Review Rule Order and Efficiency

Lab 9: Secure Connector, Edge and Ingest Appliances

- Task 1: Review Secure Connector deployment and configurations
- Task 2: Review Edge and Ingest Appliance deployment and configurations