Implementing Automation for Cisco Security Solutions (SAUI) v1.0 - On Demand

Modality: On Demand

Duration: 40 Hours

CLC: 7 Units

Course Information

About this course:

This course equips you with skills to design advanced automated security solutions for your network. A combination of theoretical lessons and hands-on labs will help you master the use of modern programming concepts, RESTful application programming interfaces (APIs), data models, protocols, firewalls, web, Domain Name System (DNS), cloud, email security, and Cisco Identity Services Engine (ISE) to strengthen cybersecurity for your web services, network, and devices.

You will also learn to work within the following platforms: Cisco Advanced Malware Protection (AMP), Cisco Threat grid, Cisco Firepower Threat Defense, Cisco ISE, Cisco Firepower® Management Center, Cisco pxGrid, Cisco Stealthwatch® Enterprise, Cisco Stealthwatch Cloud, Cisco Umbrella®, and Cisco Security Management Appliances. You will also learn when to use the API for each Cisco security solution to drive network efficiency and reduce complexity.

Upon completing this course, you will be fully prepared for the Automating and Programming Cisco Security Solutions (300-735 SAUTO) certification exam.

Course Objective:

After taking this course, you should be able to:

- Describe the overall architecture of the Cisco security solutions and how APIs help enable security
- Know how to use Cisco Firepower APIs
- Explain the functionality provided by Cisco AMP and its APIs
- Describe how to use Cisco Threat Grid APIs to analyze, search, and dispose of threats
- Explain how pxGrid APIs function and their benefits
- Demonstrate what capabilities the Cisco Stealthwatch APIs offer and construct API requests to them for configuration changes and auditing purposes
- Describe the features and benefits of using Cisco Stealthwatch Cloud APIs
- Learn how to use the Cisco Umbrella Investigate API

Audience:

This course is designed primarily for professionals in job roles such as:

- Network administrator
- Wireless design engineer
- Network manager
- Sales engineer
- Account manager
- Network engineer
- Systems engineer
- Wireless engineer
- Consulting systems engineer
- Technical solutions architect

Prerequisite:

You should have the following knowledge and skills before taking this course:

- Basic programming language concepts
- CCNP-level core networking knowledge
- CCNP-level security networking knowledge
- Basic understanding of virtualization
- Ability to use Linux and CLI tools, such as Secure Shell (SSH) and Bash

The following Cisco courses can help you gain the knowledge you need to prepare for this course:

- Implementing and Administering Cisco Solutions (CCNA)
- Introducing Automation for Cisco Solutions (CSAU)
- Programming Use Cases for Cisco Digital Network Architecture (DNAPUC)
- Introducing Cisco Network Programmability (NPICNP)
- Implementing and Operating Cisco Security Technologies (SCOR)

Course Outline:

Introducing Cisco Security APIs

Role of APIs in Cisco Security Solutions
Cisco Firepower, Cisco ISE, Cisco pxGrid and Cisco Stealthwatch APIs
Use Cases and Security Workflow

Consuming Cisco Advanced Malware Protection APIs

Cisco AMP Overview
Cisco AMP Endpoint API
Cisco AMP Use Cases and Workflows

Using Cisco ISE

Introducing Cisco Identity Services Engine
Cisco ISE Use Cases
Cisco ISE APIs

Using Cisco pxGrid APIs

- Cisco pxGrid Overview
- WebSockets and STOMP Messaging Protocol

Using Cisco Threat Grid APIs

- Cisco Threat Grid Overview
- Cisco Threat Grid API
- Cisco Threat Grid Use Cases and Workflows

Investigating Cisco Umbrella Security Data Programmatically

- Cisco Umbrella Investigate API Overview
- Cisco Umbrella Investigate API: Details

Exploring Cisco Umbrella Reporting and Enforcement APIs

- Cisco Umbrella Reporting and Enforcement APIs Overview
- Cisco Umbrella Reporting and Enforcement APIs: Deep Dive

Automating Security with Cisco Firepower APIs

- Review Basic Constructs of Firewall Policy Management
- Design Policies for Automation
- Cisco FMC APIs in Depth
- Cisco FTD Automation with Ansible
- Cisco FDM API In Depth

Operationalizing Cisco Stealthwatch and the API Capabilities

- Cisco Stealthwatch Overview
- Cisco Stealthwatch APIs: Details

Using Cisco Stealthwatch Cloud APIs

- Cisco Stealthwatch Cloud Overview
- Cisco Stealthwatch Cloud APIs Deep Dive

Describing Cisco Security Management Appliance APIs

- Cisco SMA APIs Overview
- Csico SMA API