Implementing Automation for Cisco Security Solutions (SAUI)

Description

The **Implementing Automation for Cisco Security Solutions (SAUI)** training teaches you how to design advanced automated security solutions for your network. Through a combination of lessons and hands-on labs, you will learn the use of modern programming concepts, RESTful Application Program 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 learn to work within the following platforms: Cisco Firepower® Management Center, Cisco Firepower Threat Defense, Cisco ISE, Cisco pxGrid, Cisco Stealthwatch® Enterprise, Cisco Stealthwatch Cloud, Cisco Umbrella®, Cisco Advanced Malware Protection (AMP), Cisco Threat grid, and Cisco Security Management Appliances. This training will teach you when to use the API for each Cisco security solution to drive network efficiency and reduce complexity.

This training prepares you for Automating and Programming Cisco Security Solutions (300-735 SAUTO) v1.1 certification exam. If passed, you earn the Cisco Certified DevNet Specialist – Security Automation Programmability certification and satisfy the concentration exam requirements for the Cisco Certified Network Professional (CCNP) Security and Cisco Certified DevNet Professional certifications. Introducing Automation for Cisco Solutions (CSAU) training is recommended prior to enrolling in this training because it provides crucial foundational knowledge essential to success. This training also earns you 24 Continuing Education (CE) credits toward recertification.

How you'll benefit

This training will help you:

- Gain the knowledge and skills to use automation and programmability to design more efficient networks, increase scalability, and protect against cyberattacks
- Learn how to create APIs to streamline cloud-based, network security solutions for your organization
- Prepare for the 300-735 SAUTO v1.1 exam
- Earn 24 CE credits toward recertification

Who should enroll

- Network Engineers
- Systems Engineers
- Wireless Engineers
- Consulting Systems Engineers
- Technical Solutions Architects
- Network Administrators
- Wireless Design Engineers
- Network Managers
- Sales Engineers
- Account Managers

Technology areas

- Network Automation
- Security

Objectives

- Describe the overall architecture of the Cisco security solutions and how APIs help enable security
- Know how to use Cisco Firepower APIs
- 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
- 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

Prerequisites

There are no prerequisites for this training. However, the knowledge and skills you are recommended to have before attending this training are:

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

These skills can be found in the following Cisco Learning Offerings:

- Introducing Automation for Cisco Solutions (CSAU)
- Implementing and Administering Cisco Solutions (CCNA)
- Implementing and Operating Cisco Security Core Technologies (SCOR)

Outline

- Introducing Cisco Security APIs

- Consuming Cisco Advanced Malware Protection APIs
- Using Cisco ISE
- Using Cisco pxGrid APIs
- Using Cisco Threat Grid APIs
- Investigating Cisco Umbrella Security Data Programmatically
- Exploring Cisco Umbrella Reporting and Enforcement APIs
- Automating Security with Cisco Firepower APIs
- Operationalizing Cisco Stealthwatch and the API Capabilities
- Using Cisco Stealthwatch Cloud APIs
- Describing Cisco Security Management Appliance APIs

Lab Outline

- Query Cisco AMP Endpoint APIs for Verifying Compliance
- Use the REST API and Cisco pxGrid with Cisco Identity Services Engine
- Construct a Python Script Using the Cisco Threat Grid API
- Generate Reports Using the Cisco Umbrella Reporting API
- Explore the Cisco Firepower Management Center API
- Use Ansible to Automate Cisco Firepower Threat Defense Configuration
- Automate Firewall Policies Using the Cisco Firepower Device Manager API
- Automate Alarm Policies and Create Reports Using the Cisco Stealthwatch APIs
- Construct a Report Using Cisco Stealthwatch Cloud APIs

What to expect on the exam

Automating Cisco Security Solutions (300-735 SAUTO) v1.1 is a 90-minute exam associated with the Cisco Certified DevNet Specialist – Security Automation and Programmability certification and satisfies the concentration exam requirements for the CCNP Security and Cisco Certified DevNet Professional certifications.

This exam tests your knowledge of implementing security automated solutions, including:

- Programming concepts
- RESTful APIs
- Data models
- Protocols
- Firewalls
- Web
- DNS
- Cloud and email security
- ISE

Links

- Cisco U. Learning Path
- Cisco Learning Network Store
- Cisco Learning Locator