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

Duration: 3 Days

Prerequisites:

Before taking this training, you should have:

- 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

The following Cisco trainings can help you gain the knowledge you need to prepare for this training:

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

Course Description:

The Implementing Automation for Cisco Security Solutions (SAUI) v1.0 training teaches you how to design advanced automated security solutions for your network. Through a combination of lessons and hands-on labs, you will master 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 300-735 Automating and Programming Cisco Security Solutions (SAUTO) certification exam. Introducing Automation for Cisco Solutions (CSAU) is required prior to enrolling in Implementing Automation for Cisco Security Solutions (SAUI) because it provides crucial foundational knowledge essential to success. This training also earns you 24 Continuing Education (CE) credits towards recertification.

Course 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

Intended Audience:

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

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

Course Outlines:

- 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 Reports Using Cisco Security Management Appliance (SMA) APIs

REGISTER NOW!
training@trends.com.ph
(+632) 8863-2123
www.trendsacademy.com.ph