



Implementing Automation for Cisco Security Solutions (SAUI) V1.1

***WHERE GREAT TRAINING
HAPPENS EVERYDAY!***



Implementing Automation for Cisco Security Solutions (SAUI) V1.1

Course Duration

3 Days

Course Price

\$2,895.00

29 CLCs

Methods of Delivery

In-Person ILT

Virtual ILT

Onsite ILT

About this Class

The Implementing Automation for Cisco Security Solutions (SAUI) course 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 course will teach you when to use the API for each Cisco security solution to drive network efficiency and reduce complexity.



Implementing Automation for Cisco Security Solutions (SAUI) V1.1

How you will benefit

This class 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
- Earn 24 CE credits toward recertification
- Prepares you for the 300-735 SAUTO exam

Why Attend with Current Technologies CLC

- Our Instructors are the top 10% rated by Cisco
- Our Lab has a dedicated 1 Gig Fiber Connection for our Labs
- Our Labs run up to Date Code for all our courses

Who Should Attend

The job roles best suited to the material in this course are:

- Network Engineer
- Network Administrator
- Network Manager
- Systems Engineer
- Wireless Engineer
- Wireless Design Engineer
- Consulting Systems Engineer
- Sales Engineer
- Technical Solutions Architect
- Account Manager

Implementing Automation for Cisco Security Solutions (SAUI) V1.1

Objectives

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 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

Implementing Automation for Cisco Security Solutions (SAUI) V1.1

Course Outline

Module 1: Introducing Cisco Security APIs

Module 2: Consuming Cisco Advanced Malware Protection APIs

Module 3: Using Cisco ISE

Module 4: Using Cisco pxGrid APIs

Module 5: Using Cisco Threat Grid APIs

Module 6: Investigating Cisco Umbrella Security Data Programmatically

Module 7: Exploring Cisco Umbrella Reporting and Enforcement APIs

Module 8: Automating Security with Cisco Firepower APIs

Module 9: Operationalizing Cisco Stealthwatch and the API Capabilities

Module 10: Using Cisco Stealthwatch Cloud APIs

Module 11: Describing Cisco Security Management Appliance APIs

Implementing Automation for Cisco Security Solutions (SAUI) V1.1

Lab Outline

- **Lab 1: Query Cisco AMP Endpoint APIs for Verifying Compliance**
- **Lab 2: Use the REST API and Cisco pxGrid with Cisco Identity Services Engine**
- **Lab 3: Construct a Python Script Using the Cisco Threat Grid API**
- **Lab 4: Generate Reports Using the Cisco Umbrella Reporting API**
- **Lab 5: Explore the Cisco Firepower Management Center API**
- **Lab 6: Use Ansible to Automate Cisco Firepower Threat Defense Configuration**
- **Lab 7: Automate Firewall Policies Using the Cisco Firepower Device Manager API**
- **Lab 8: Automate Alarm Policies and Create Reports Using the Cisco Stealthwatch APIs**
- **Lab 9: Construct a Report Using Cisco Stealthwatch Cloud APIs**