FIREFLY

Implementing Automation for Cisco Security Solutions

DURATION: 3 DAYS COURSE CODE: SAUI FORMAT: LECTURE/LAB

COURSE DESCRIPTION

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

This course prepares you for 300-735 Automating and Programming Cisco Security Solutions (SAUTO) certification exam.

WHO SHOULD ATTEND

Network engineer

Systems engineer

Wireless engineer

Consulting systems engineer

Technical solutions architect

Network administrator

Wireless design engineer

Network manager

Sales engineer

Account manager

PREREQUISITES

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

LEARNING 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

COURSE OUTLINE

1. Introducing Cisco Security APIs
2. Consuming Cisco Advanced Malware Protection APIs
3. Using Cisco ISE
4. Using Cisco pxGrid APIs
5. Using Cisco Threat Grid APIs
6. Investigating Cisco Umbrella Security Data Programmatically
7. Exploring Cisco Umbrella Reporting and Enforcement APIs
8. Automating Security with Cisco Firepower APIs
9. Operationalizing Cisco Stealthwatch and the API Capabilities
10. Using Cisco Stealthwatch Cloud APIs
11. Describing Cisco Security Management Appliance APIs

DISCOVERY LABS

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