Implementing Automation for Cisco Security Solutions

Duration: 3 Days **Course Code: SAUI** **Version: 1.1**

Overview:

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.

This course is worth 24 Continuing Education (CE) Credits

Target Audience:

Individuals looking to use automation and programmability to design more efficient networks, increase scalability and protect against cyberattacks.

Objectives:

- **After completing 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

Prerequisites:

Attendees should meet the following 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
- CCNA - Implementing and Administering Cisco Solutions
- SCOR - Implementing and Operating Cisco Security Core Technologies
- CSAU - Introducing Automation for Cisco Solutions

Testing and Certification

Recommended as preparation for the following exams:

- **300-735** - Automating and Programming Cisco Security Solutions (SAUTO) exam

After you pass **300-735 SAUTO** exam, you earn the **Cisco Certified DevNet Specialist - Security Automation and Programmability** certification, and you satisfy the concentration exam requirements for the CCNP Security certification and the Cisco Certified DevNet Professional certification.

Content:

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

Labs

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

Further Information:

For More information, or to book your course, please call us on 00 966 92000 9278

training@globalknowledge.com.sa

www.globalknowledge.com/en-sa/

Global Knowledge - KSA, 393 Al-Uroubah Road, Al Worood, Riyadh 3140, Saudi Arabia