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

Overview

This course demonstrates the tools and the benefits of leveraging programmability and automation in Cisco Security Solutions, including Cisco Firepower Management Center, Cisco Firepower Threat Defense, Cisco ISE, Cisco pxGrid, Cisco Stealthwatch Enterprise, Cisco Stealthwatch Cloud, Cisco Umbrella, Cisco AMP, Cisco Threat grid, and Cisco Security Management Appliances. Students will learn how to use the API for each Cisco security solution and specific applications of when the API benefits IT security content.

Prerequisite Comments

The knowledge and skills you are expected to have before attending this course are:
Basic programming language concepts
Basic understanding of virtualization
Ability to use Linux and CLI tools, such as SSH and bash
CCNP level core networking knowledge
CCNP level security networking knowledge
Here are recommended offerings that may help you meet these prerequisites:
Implementing and Administrating Cisco Solutions v1.0 (CCNA)
Implementing and Operating Cisco Security Technologies v1.0 (SCOR)

Target Audience

Channel and Customer
Engineers
Network Engineer
System Engineer
Wireless Engineer
Consulting Systems Engineer
Technical Solutions Architect
Network Admisnistrator
Wireless Design Engineer
Network Manager
Channel SEs
Sales Engineer
Channel AMs
Account Manager

Course Objectives

Upon completing this course, students will be able to meet these objectives:
Understand the overall architecture of the Cisco security solutions and how APIs help enable security
Understand how to use Cisco Firepower APIs
Understand how pxGrid APIs function and their benefits
Understand what capabilities the Cisco Stealthwatch APIs offer and construct API requests to them for configuration changes and auditing purposes
Understand the features and benefits of using Cisco Stealthwatch Cloud APIs

Learn how to use the Cisco Umbrella Investigate API
Understand the Functionality provided by Cisco AMP and its APIs
Learn how to use Cisco Threat Grid APIs to analyze, search, and dispose of threats

Course Outline

1 - 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

2 - Consuming Cisco Advanced Malware Protection APIs

Cisco AMP overview
Cisco AMP endpoint API
Cisco AMP use cases and workflows
Discovery 1: Query Cisco AMP endpoint APIs for verifying compliance

3 - Using Cisco ISE

Introducing Cisco Identity services engine
Cisco ISE use cases
Cisco ISE APIs

4 - Using Cisco pxGrid APIs

Cisco pxGrid overview
WebSockets and STOMP messaging protocol
Discovery 2: Use the REST API and Cisco pxGrid with Cisco Identity services engine

5 - Using Cisco Threat Grid APIs

Cisco threat grid overview
Cisco threat grid API
Cisco threat grid use cases and workflows
Discovery 3: Construct a Python script using the Cisco threat grid API

6 - Investigating Cisco Umbrella Security Data Programmatically

Cisco Umbrella investigate API overview
Cisco Umbrella investigate API: Details
Discovery 4: Query security data with the Cisco Umbrella investigate API

New Horizons Estonia
+372 555 11 819
A.Weizenbergi 10-3
Tallinn, 10132

Contact Us
info.estonia@newhorizons.com
estonia.newhorizons.com

7 - Exploring Cisco Umbrella Reporting and Enforcement APIs

Cisco Umbrella reporting and enforcement APIs: Overview
Cisco Umbrella reporting and enforcement APIs: Deep dive
Discovery 5: Generate reports using the Cisco Umbrella reporting API

8 - Automating Security with Cisco Firepower APIs

Review basic constructs of Firewall policy management
Design policies for automation
Cisco FMC APIs in depth
Discovery 6: Explore the Cisco Firepower management center API
Cisco FTD automation with ansible
Discovery 7: Use ansible to automate Cisco Firepower threat defense configuration
Cisco FDM API in depth
Discovery 8: Automate Firewall policies using the Cisco Firepower device manager API

9 - Operationalizing Cisco Stealthwatch and Its API Capabilities

Cisco Stealthwatch overview
Cisco Stealthwatch APIs: Details
Discovery 9: Automate alarm policies and create reports using the Cisco Stealthwatch APIs

10 - Using Cisco Stealthwatch Cloud APIs

Cisco Stealthwatch Cloud overview
Cisco Stealthwatch Cloud APIs: Deep dive
Discovery 10: Construct a report using Cisco stealthwatch Cloud APIs

11 - Describing Cisco Security Management Appliance APIs

Cisco SMA APIs overview
Cisco SMA API
Discovery 11: Construct reports using Cisco SMA APIs

Related Courses, Certifications, Exams

- Cisco® Implementing and Administering Cisco® Solutions v1.0 (CCNA)
- Cisco® Implementing and Operating Cisco® Security Core Technologies v1.0 (SCOR)