SAUI (IMPLEMENTING AUTOMATION FOR CISCO SECURITY SOLUTIONS) 1.0

Objetivo

After taking this course, you should be able to: â¢ Describe the overall architecture of the Cisco security solutions and how APIs help enable security; â¢ Know how to use Cisco Firepower APIs; â¢ Explain how pxGrid APIs function and their benefits; â¢ Demonstrate what capabilities the Cisco Stealthwatch APIs offer and construct API requests to them for configuration changes and auditing purposes; â¢ Describe the features and benefits of using Cisco Stealthwatch Cloud APIs; â¢ Learn how to use the Cisco Umbrella Investigate API; â¢ Explain the functionality provided by Cisco AMP and its APIs; â¢ Describe how to use Cisco Threat Grid APIs to analyze, search, and dispose of threats.

PÃºblico Alvo

This course is designed primarily for professionals in job roles such as: â¢ Security or network professionals seeking knowledge to design, install, configure, operate, and to design advanced automated security solutions for network; â¢ Professionals who need to prepare for the Cisco 300-735 certification exam.

PrÃ©-Requisitos

Before taking this course, you should have: â¢ Basic programming language concepts; â¢ Basic understanding of virtualization; â¢ Ability to use Linux and Command Line Interface (CLI) tools, such as Secure Shell (SSH) and bash; â¢ CCNP level core networking knowledge; â¢ CCNP level security networking knowledge. For your reference, the following Cisco courses can help you gain the knowledge you need to prepare for this course: â¢ Introducing Automation for Cisco Solutions (CSAU); â¢ Implementing and Administering Cisco Solutions (CCNAÂ®); â¢ Programming Use Cases for Cisco Digital Network Architecture (DNAPUC); â¢ Introducing Cisco Network Programmability (NPICNP); â¢ Implementing and Operating Cisco Security Technologies (SCOR).

Carga HorÃ¡ria

24 horas (3 dias).

ConteÃºdo ProgramÃ¡tico

Course Introduction
Course Outline
Course Goals & Objectives

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
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