Implementing Automation for Cisco Security Solutions

Durée: 3 Jours **Réf de cours: SAUI** **Version: 1.0**

Résumé:

Le cours Implémentation de l'automatisation pour les solutions de sécurité Cisco (SAUI) vous apprend à concevoir des solutions de sécurité automatisées avancées pour votre réseau. Grâce à une combinaison de leçons et de laboratoires pratiques, vous maîtriserez l'utilisation des concepts de programmation modernes, des interfaces de programme d'application RESTful (API), des modèles de données, des protocoles, des pare-feu, du Web, du système de noms de domaine (DNS), du cloud, de la sécurité de la messagerie, et Cisco® Identity Services Engine (ISE) pour renforcer la cybersécurité de vos services Web, de votre réseau et de vos appareils. Vous apprendrez à travailler au sein des plates-formes suivantes : 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 grille et les appliances de gestion de la sécurité Cisco.
La formation vous permettra de savoir quand utiliser l'API pour chaque solution de sécurité Cisco afin d'améliorer l'efficacité du réseau et de réduire la complexité.

Le suivi de cette formation permet de valider un total de 24 crédits dans le cadre du programme d'Education Continue Cisco (CCE) pour les professionnels qui souhaitent renouveler leur titre de certification.

Public visé:

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

Objectifs pédagogiques:

- **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

Pré-requis:

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
- DEVCOR - Developing Applications Using Cisco Platforms and APIs
- SCOR - Mettre en oeuvre et gérer les solutions de sécurité Cisco

Test et 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.

Contenu:

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

Autres moyens pédagogiques et de suivi:

• Compétence du formateur : Les experts qui animent la formation sont des spécialistes des matières abordées et ont au minimum cinq ans d'expérience d'animation. Nos équipes ont validé à la fois leurs connaissances techniques (certifications le cas échéant) ainsi que leur compétence pédagogique.
• Suivi d'exécution : Une feuille d'émargement par demi-journée de présence est signée par tous les participants et le formateur.
• Modalités d'évaluation : le participant est invité à s'auto-évaluer par rapport aux objectifs énoncés.
• Chaque participant, à l'issue de la formation, répond à un questionnaire de satisfaction qui est ensuite étudié par nos équipes pédagogiques en vue de maintenir et d'améliorer la qualité de nos prestations.

Délais d'inscription :

•Vous pouvez vous inscrire sur l'une de nos sessions planifiées en inter-entreprises jusqu'à 5 jours ouvrés avant le début de la formation sous réserve de disponibilité de places et de labs le cas échéant.
•Votre place sera confirmée à la réception d'un devis ou ""booking form"" signé. Vous recevrez ensuite la convocation et les modalités d'accès en présentiel ou distanciel.
•Attention, si vous utilisez votre Compte Personnel de Formation pour financer votre inscription, vous devrez respecter un délai minimum et non négociable fixé à 11 jours ouvrés.