Formation Implementing Automation for Cisco Security Solutions

Implementing Automation for Cisco Security Solutions

N° ACTIVITÉ : 11 92 18558 92 | TÉLÉPHONE : 01 85 77 07 07 | E-MAIL : inscription@hubformation.com

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.

Référence	SAUI
Durée	3 jours (21h)
Tarif	2 790 €HT
Repas	60 €HT(en option)

SESSIONS PROGRAMMÉES

A DISTANCE (ENG)

du 23 au 25 septembre 2024
du 4 au 6 décembre 2024

VOIR TOUTES LES DATES

Objectifs

| Décrire l'architecture globale des solutions de sécurité Cisco et comment les API contribuent à activer la sécurité
| Savoir utiliser les API Cisco Firepower
| Expliquer le fonctionnement des API pxGrid et leurs avantages
| Démontrer les fonctionnalités offertes par les API Cisco Stealthwatch et créer des demandes d'API pour les modifications de configuration et à des fins d'audit
| Décrire les fonctionnalités et les avantages de l'utilisation des API Cisco Stealthwatch Cloud
| Apprendre à utiliser l'API Cisco Umbrella Investigate
| Expliquer les fonctionnalités fournies par Cisco AMP et ses API
| Décrire comment utiliser les API Cisco Threat Grid pour analyser, rechercher et éliminer les menaces

Public

| Les personnes qui cherchent à utiliser l'automatisation et la programmabilité pour concevoir des réseaux plus efficaces, augmenter l'évolutivité et se protéger contre les cyberattaques.

Prérequis

| Concepts de base du langage de programmation
| Compréhension de base de la virtualisation
| Capacité à utiliser Linux et les outils d'interface de ligne de commande (CLI), tels que Secure Shell (SSH) et bash
| Connaissances réseau de base de niveau CCNP
| Connaissance des réseaux de sécurité de niveau CCNP

Programme de la formation

Présentation des API de sécurité Cisco
- Rôle des API dans les solutions de sécurité Cisco
- API Cisco Firepower, Cisco ISE, Cisco pxGrid et Cisco Stealthwatch
- Cas d'utilisation et workflow de sécurité

Utilisation des API Cisco Advanced Malware Protection
- Présentation de CiscoAMP
- API de point de terminaison Cisco AMP
- Cas d'utilisation et workflows de Cisco AMP

Utilisation de Cisco ISE
- Présentation du moteur de services d'identité Cisco
- Cas d'utilisation Cisco ISE
- API Cisco ISE

Utilisation des API Cisco pxGrid
- Présentation de Cisco pxGrid
- WebSockets et protocole de messagerie STOMP

Utilisation des API Cisco Threat Grid
- Présentation de Cisco Threat Grid
- API Cisco Threat Grid
- Cas d'utilisation et workflows de Cisco Threat Grid

Examen des données de sécurité de Cisco Umbrella par programmation
- Présentation de l'API Cisco Umbrella Investigate
- API Cisco Umbrella Investigate : Détails

Explorer les API Cisco Umbrella Reporting and Enforcement
- Présentation des API Cisco Umbrella Reporting and Enforcement
- API Cisco Umbrella Reporting and Enforcement : analyse approfondie

Automatisation de la sécurité avec les API Cisco Firepower
- Passez en revue les constructions de base de la gestion des politiques de pare-feu
- Politiques de conception pour l'automatisation
- API Cisco FMC en détail
- Automatisation Cisco FTD avec Ansible
- API Cisco FDM en détail

Opérationnalisation de Cisco Stealthwatch et des capacités de l'API
- Présentation de Cisco Stealthwatch
- API Cisco Stealthwatch : détails

Utilisation des API Cisco Stealthwatch Cloud
- Présentation de Cisco Stealthwatch Cloud
- Analyse approfondie des API Cisco Stealthwatch Cloud

Description des API de Cisco Security Management Appliance
- Présentation des API Cisco SMA
- API SMA Csico

Laboratoires
- Interroger les API Cisco AMP Endpoint pour vérifier la conformité
- Utiliser l'API REST et Cisco pxGrid avec Cisco Identity Services Engine
- Construire un script Python à l'aide de l'API Cisco Threat Grid
- Interroger les données de sécurité avec l'API Cisco Umbrella Investigate
- Générer des rapports à l'aide de l'API Cisco Umbrella Reporting
- Explorer l'API Cisco Firepower Management Center
- Utiliser Ansible pour automatiser la configuration de Cisco Firepower Threat Defense
- Automatiser les politiques de pare-feu à l'aide de l'API Cisco Firepower Device Manager
- Automatiser les politiques d'alarme et créez des rapports à l'aide des API Cisco Stalthwatch
- Créer un rapport à l'aide des API Cisco Stealthwatch Cloud

Méthode pédagogique

Chaque participant travaille sur un poste informatique qui lui est dédié. Un support de cours lui est remis soit en début soit en fin de cours. La théorie est complétée par des cas pratiques ou exercices corrigés et discutés avec le formateur. Le formateur projette une présentation pour animer la formation et reste disponible pour répondre à toutes les questions.

Méthode d'évaluation

Tout au long de la formation, les exercices et mises en situation permettent de valider et contrôler les acquis du stagiaire. En fin de formation, le stagiaire complète un QCM d'auto-évaluation.

Suivre cette formation à distance

Voici les prérequis techniques pour pouvoir suivre le cours à distance :

| Un ordinateur avec webcam, micro, haut-parleur et un navigateur (de préférence Chrome ou Firefox). Un casque n'est pas nécessaire suivant l'environnement.
| Une connexion Internet de type ADSL ou supérieure. Attention, une connexion Internet ne permettant pas, par exemple, de recevoir la télévision par Internet, ne sera pas suffisante, cela engendrera des déconnexions intempestives du stagiaire et dérangera toute la classe.
| Privilégier une connexion filaire plutôt que le Wifi.
| Avoir accès au poste depuis lequel vous suivrez le cours à distance au moins 2 jours avant la formation pour effectuer les tests de connexion préalables.
| Votre numéro de téléphone portable (pour l'envoi du mot de passe d'accès aux supports de cours et pour une messagerie instantanée autre que celle intégrée à la classe virtuelle).
| Selon la formation, une configuration spécifique de votre machine peut être attendue, merci de nous contacter.
| Pour les formations incluant le passage d'une certification la dernière journée, un voucher vous est fourni pour passer l'examen en ligne.
| Pour les formations logiciel (Adobe, Microsoft Office...), il est nécessaire d'avoir le logiciel installé sur votre machine, nous ne fournissons pas de licence ou de version test.
| Horaires identiques au présentiel.

Accessibilité

Les sessions de formation se déroulent sur des sites différents selon les villes ou les dates, merci de nous contacter pour vérifier l'accessibilité aux personnes à mobilité réduite.
Pour tout besoin spécifique (vue, audition...), veuillez nous contacter au 01 85 77 07 07.

HUB Formation - 1-7, Cours Valmy - 92923 Paris - La Defense
01 85 77 07 07 - www.hubformation.com - SIREN 525 287 785