Automating Cisco Security Solutions (SAUTO)

Référence : **SAUI** Durée : **3 jours** Certification : **Aucune**

CONNAISSANCES PREALABLES

• Pour suivre ce cours, il est recommandé de posséder les compétences et les connaissances suivantes :.
•Compréhension de base de la virtualisation. • Concepts de base du langage de programmation. • Connaissance des réseaux de sécurité de niveau CCNP. • Connaissances de base en réseau de niveau CCNP. • Implementing and Operating Cisco Security Core Technologies (SCOR). • Possibilité d'utiliser Linux et les outils CLI (Command Line Interface), tels que Secure Shell (SSH) et bash.

PROFIL DES STAGIAIRES

• Administrateur réseau. • Architecte de solutions techniques. • Gestionnaire de compte. • Gestionnaire de réseau. • Ingénieur commercial. • Ingénieur conseil en systèmes. • Ingénieur de conception sans fil. • Ingénieur réseau. • Ingénieur sans fil. • Ingénieur Systèmes.

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 comment fonctionnent les API pxGrid et leurs avantages. • Démontrez quelles capacités les API Cisco Stealthwatch offrent et construisez des demandes d'API pour les changements de configuration et à des fins d'audit. • Décrire les fonctionnalités et les avantages de l'utilisation des API Cloud de Cisco Stealthwatch. • Apprenez à utiliser l'API Cisco Umbrella Investigate. • Expliquez les fonctionnalités fournies par Cisco AMP et ses API. • Décrire comment utiliser les API Cisco Threat Grid pour analyser, rechercher et éliminer les menaces.

CERTIFICATION PREPAREE

Aucune

METHODES PEDAGOGIQUES

- Mise à disposition d'un poste de travail par stagiaire
- Remise d'une documentation pédagogique papier ou numérique pendant le stage
- La formation est constituée d'apports théoriques, d'exercices pratiques, de réflexions et de retours d'expérience
- Le suivi de cette formation donne lieu à la signature d'une feuille d'émargement

FORMATEUR

Consultant-Formateur expert Enterprise Infrastructure

METHODE D'EVALUATION DES ACQUIS

- Auto-évaluation des acquis par le stagiaire via un questionnaire
- Attestation des compétences acquises envoyée au stagiaire
- Attestation de fin de stage adressée avec la facture

CONTENU DU COURS

Présentation des API de sécurité Cisco

Consommation des API Cisco Advanced Malware Protection

Utilisation de Cisco ISE

Utilisation des API Cisco pxGrid

Utilisation des API Cisco Threat Grid

Examen des données de sécurité de Cisco Umbrella par programme

Explorer les API Cisco Umbrella Reporting and Enforcement

Automatisation de la sécurité avec les API Cisco Firepower

Opérationnalisation de Cisco Stealthwatch et des capacités de l'API

Utilisation des API Cisco Stealthwatch Cloud

Décrire les API de l'appliance de gestion de la sécurité Cisco

Laboratoire

- Interrogez les API Cisco AMP Endpoint pour vérifier la conformité
- Utilisez l'API REST et Cisco pxGrid avec Cisco Identity Services Engine
- Construisez un script Python à l'aide de l'API Cisco Threat Grid
- Générez des rapports à l'aide de l'API Cisco Umbrella Reporting
- Explorez l'API Cisco Firepower Management Center
- Utilisez Ansible pour automatiser la configuration de Cisco Firepower Threat Defense
- Automatisez les politiques de pare-feu à l'aide de l'API Cisco Firepower Device Manager
- Automatisez les stratégies d'alarme et créez des rapports à l'aide des API Cisco Stealthwatch
- Construisez un rapport en utilisant les API Cloud de Cisco Stealthwatch

*Notre **référent handicap** se tient à votre disposition au 01.71.19.70.30 ou par mail à referent.handicap@edugroupe.com pour recueillir vos éventuels besoins d'aménagements, afin de vous offrir la meilleure expérience possible*