Implementing Network Security (IANS)

ID IANS **Prix** 4 950,– € (Hors Taxe) **Durée** 5 jours

A qui s'adresse cette formation

Les candidats typiques pour ce cours sont des ingénieurs réseau responsables de la mise en œuvre des contrôles de sécurité sur les réseaux d'entreprise. Les apprenants peuvent décrire la pile de sécurité réseau (pare-feu, proxy, accès à distance, IDS/IPS, contrôle d'accès, NTA, UEBA).

Cette formation prépare à la/aux certifications

HPE Aruba Networking Certified Professional - Network Security (ACP-NS)

Pré-requis

Les connaissances suivantes sont recommandées pour ce séminaire :

Aruba recommande que le candidat ait assisté au cours Network Security Fundamentals (ANSF) avant de suivre ce cours de niveau professionnel. Ou avoir une expérience et des connaissances équivalentes en matière de fondamentaux de la sécurité réseau.

Nous constatons que de nombreux apprenants sautent la formation de base/de niveau associé et ont des difficultés à suivre les cours de niveaux supérieurs. Nous vous invitons à effectuer cette courte Auto-évaluation pour vérifier si le cours est fait pour vous.

Objectifs

Après avoir suivi ce cours, vous serez en mesure de :

1. Protéger et défendre

- Définir les terminologies de sécurité
- PKI
- Sécurité Zero Trust
- WIPS & WIDS
- Renforcer les appareils
- Sécuriser l'infrastructure réseau
- Sécuriser les protocoles L2 & L3
- Sécuriser un WLAN
- Déployer AAA avec CPPM
- Sécuriser un LAN câblé
- Déployer AAA avec CPPM
- Déployer 802.1x
- Déployer une authentification basée sur des certificats pour les utilisateurs et les appareils
- Sécuriser le WAN
- Comprendre le SD-Branch d'Aruba pour automatiser le déploiement VPN
- Concevoir et déployer un VPN avec le client VIA d'Aruba
- Classifier les points de terminaison
- Déployer la classification des points de terminaison sur les appareils
- Intégrer ClearPass et CPDI

2. Analyser

- Détection des menaces
- Enquêter sur les alertes centrales
- Interpréter les captures de paquets
- Évaluer les postures des points de terminaison
- Dépannage
- Déployer et analyser les résultats des scripts NAE
- Classification des points de terminaison
- Analyser les données de classification des points de terminaison pour identifier les risques
- Analyser les données de classification des points de terminaison sur CPDI

3. Enquêter

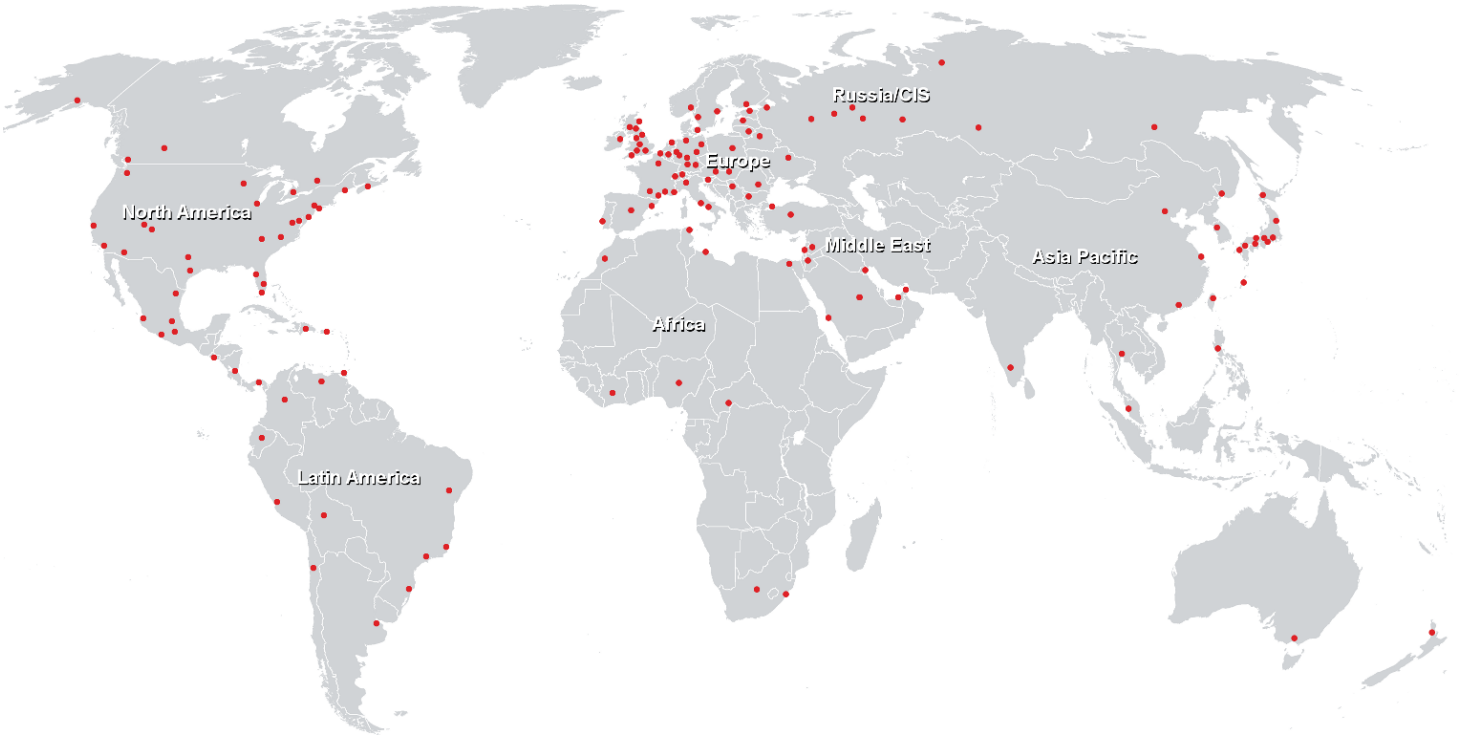
- Criminalistique
- Expliquer les capacités de CPDI pour afficher les conversations réseau sur les appareils Aruba pris en charge

Contenu

- Stratégie de sécurité HPE Aruba Networking et principes fondamentaux de ClearPass
- Déployer des certificats de confiance
- Implémenter l'authentification 802.1X basée sur des certificats
- Implémenter des politiques avancées sur le pare-feu AOS basé sur les rôles

- Évaluer la posture des points de terminaison
- Implémenter une infrastructure réseau de confiance
- Implémenter 802.1X et le contrôle d'accès basé sur les rôles sur AOS-CX
- Implémenter la segmentation dynamique sur les commutateurs AOS-CX
- Surveiller avec le moteur d'analytique réseau (NAE)
- Implémenter WIDS/WIPS
- Utiliser CPPM et l'intégration de tiers pour atténuer les menaces
- Implémenter le profilage des appareils avec CPPM
- Profilage des appareils avec HPE Aruba Networking
- Déployer ClearPass Device Insight
- Intégrer Device Insight avec CPPM
- Utiliser les captures de paquets pour enquêter sur les problèmes de sécurité
- Sécuriser l'accès à distance et aux agences
- Configurer IDS/IPS de la passerelle HPE Aruba Networking
- Utiliser les alertes HPE Aruba Networking Central

Centres de formation dans le monde entier





Fast Lane Institute for Knowledge Transfer (Switzerland) AG

Husacherstrasse 3
CH-8304 Wallisellen
Tel. +41 44 832 50 80

info@flane.ch, https://www.flane.ch