

Aruba Network Security – Les fondamentaux

4 jours (28 heures)

Initiation

à partir de

2 880 € HT par personne (TVA en vigueur)

Contenu mis à jour le 30/09/2026. Document téléchargé le 02/10/2026.

Objectifs

A l'issue de cette formation, vous serez capable de :

- Définir la terminologie de la sécurité
- Durcir les devices
- Sécuriser un WLAN (Wireless Local Area Network)
- Sécuriser un réseau local câblé (LAN)
- Sécuriser le WAN
- Classifier les terminaux
- Détecter les menaces
- Analyser les dépannages
- Classifier les terminaux
- Effectuer des recherches Forensics.

Les compétences visées par cette formation font l'objet d'une évaluation.

À qui s'adresse cette formation ?

Ingénieurs réseau / du service d'assistance.

Prérequis

Avoir une expérience dans le domaine de la mise en réseau dans des environnements câblés et sans fils.

Programme

1 Pendant votre formation

Aruba Network Security – Les fondamentaux

Menaces pour la sécurité et stratégie de sécurité d'Aruba

- Aperçu des menaces
- Etapes de l'attaque
- Stratégie de sécurité d'Aruba

Technologies de sécurité

- Conformité réglementaire
- Communications sécurisées :
 - Cryptage symétrique et authentification par hachage
 - Cryptage asymétrique et certificats numériques
 - TLS
- Authentification, autorisation, comptabilité (AAA)

Durcir les commutateurs d'Aruba

- Aperçu du durcissement
- Mettre en place une gestion hors bande
- Authentifier les gestionnaires en toute sécurité
- Assurer la sécurité physique et autres mesures de renforcement

Durcir les dispositifs sans fil ArubaOS

- Blocage de l'accès administratif
- Services de verrouillage
- Utiliser CPSec

Renforcer la sécurité des réseaux locaux

- Protections Spanning Tree
- Snooping DHCP et protection ARP
- Technologies de routage sécurisé

Technologies d'authentification des réseaux

- Authentification des réseaux
- Sécurité WLAN – Cryptage + Authentification

Renforcer la sécurité Edge grâce à une infrastructure Aruba

- Appliquer WPA3-Enterprise
- Appliquer 802.1X sur le réseau câblé

Mettre en place un système d'authentification et de contrôle d'accès basé sur les rôles

- Politiques Aruba de pare-feu basées sur les rôles
- Segmentation dynamique

Identifier et classer les terminaux

- Introduction à la classification des terminaux
- DHCP Fingerprinting avec les devices ArubaOS Mobility
- Aruba ClearPass Policy Manager Device Profiler
- ClearPass Device Insight

Sécurité de la Branch

- Introduction aux solutions Aruba SD-Branch

Mettre en oeuvre la détection des menaces et les Forensics

- Comprendre les Forensics
- Analyser les événements ArubaOS WIP

Dépannage et surveillance

- Introduction au dépannage des problèmes d'authentification
- Utilisation des outils ClearPass pour résoudre certains problèmes courants
- Packet Capture
- Monitoring

Certification (en option)

- Prévoir l'achat de la certification en supplément
- Le passage de l'examen se fera (ultérieurement) dans un centre agréé Pearson Vue
- L'examen (en anglais) s'effectue en ligne, et durera en moyenne 1h30

Financement

Plusieurs dispositifs de financement sont accessibles via les OPCO (Opérateurs de Compétences), organismes agréés par le ministère du Travail dont le rôle est d'accompagner, collecter et gérer les contributions des entreprises au titre du financement de la formation professionnelle.

Pour plus d'information, une équipe de gestionnaires SKOLAE Formation spécialisée vous accompagne dans le choix de vos formations et la gestion administrative.

[Nous contacter pour en savoir plus →](#)

Modalités pédagogiques

Formation délivrée en présentiel ou distanciel* (blended-learning, e-learning, classe virtuelle, présentiel à distance).

Le formateur alterne entre méthode** démonstrative, interrogative et active (via des travaux pratiques et/ou des mises en situation).

Variables suivant les formations, les moyens pédagogiques mis en oeuvre sont :

- Ordinateurs Mac ou PC (sauf pour certains cours de l'offre Management), connexion internet fibre, tableau blanc ou paperboard, vidéoprojecteur ou écran tactile interactif (pour le distanciel)
- Environnements de formation installés sur les postes de travail ou en ligne
- Supports de cours et exercices

En cas de formation intra sur site externe à M2I, le client s'assure et s'engage également à avoir toutes les ressources matérielles pédagogiques nécessaires (équipements informatiques...) au bon déroulement de l'action de formation visée conformément aux prérequis indiqués dans le programme de formation communiqué.

* nous consulter pour la faisabilité en distanciel

** ratio variable selon le cours suivi

Accessibilité aux personnes en situation de handicap