Formation Sécurité des réseaux & Architectures sécurisées

Informations

Durée : 2 jours (14h.)

Tarif* : Nous consulter

Réf : SRAS

Niveau : Moyen

intra

Mise à jour le 30/12/25

*tarif valable jusqu'au 31/12/2026

Prochaines sessions

Contactez-nous pour connaitre nos futures sessions.

Pré-requis

- Connaissances de base en réseaux (TCP/IP, routage, VLAN)
- Compréhension générale des systèmes d'information
- Notions de cybersécurité recommandées

Objectifs

Objectifs pédagogiques :

- Comprendre les menaces ciblant les réseaux
- Connaître les principes fondamentaux de la sécurité réseau
- Comprendre les mécanismes de protection réseau
- Identifier les bonnes pratiques d'architecture sécurisée
- Appréhender les concepts de segmentation et de contrôle des flux

Objectifs opérationnels :

- Analyser la sécurité d'une architecture réseau existante
- Mettre en place des règles de segmentation réseau
- Sécuriser les flux réseau internes et externes
- Appliquer les principes d'architectures sécurisées
- Contribuer à la conception de réseaux plus résilients

Programme

Jour 1 – Fondamentaux de la sécurité réseau

Menaces et attaques réseau

Panorama des attaques réseau (scan, sniffing, spoofing, DoS)
Attaques internes et externes
Mouvement latéral et propagation
Importance de la visibilité réseau

Principes de la sécurité réseau

Défense en profondeur
Filtrage et contrôle des flux
Principe du moindre privilège réseau
Segmentation et cloisonnement

Mécanismes de protection réseau

Pare-feu et filtrage
NAT et zones de sécurité
IDS / IPS (principes)
Sécurisation des accès distants

Atelier pratique

Analyse d'une architecture réseau existante
Identification des faiblesses de sécurité
Proposition d'améliorations

Jour 2 – Architectures sécurisées et bonnes pratiques

Segmentation et architectures sécurisées

VLAN, sous-réseaux et zones de confiance
DMZ et réseaux exposés
Micro-segmentation (principes)

Formation Sécurité des réseaux & Architectures sécurisées

Isolation des environnements

Architectures modernes et Zero Trust

Limites des architectures périmétriques
Principes du Zero Trust
Contrôle des identités et des accès réseau
Sécurisation des flux applicatifs

Sécurité réseau et environnements hybrides

Réseaux on-premise et cloud
Interconnexions sécurisées
Sécurisation des accès aux ressources cloud
Bonnes pratiques multi-environnements

Atelier pratique

Conception d’une architecture réseau sécurisée
Définition des zones, flux et contrôles
Présentation et validation collective