Architecture Zero Trust : réduire les surfaces d'attaque

Durée: 1 jour
Public cible: Professionnel TI

À qui s'adresse cette formation ?

- Architectes de sécurité
- RSSI
- Directeurs TI.

Objectifs de la formation

- Comprendre les principes et composantes du Zero Trust.
- Concevoir des architectures réduisant les surfaces d'attaque.
- Mettre en place l'authentification et l'autorisation continues.
- Aligner le Zero Trust avec les exigences de conformité.

Description sommaire

Cette formation présente une approche structurée pour concevoir et implanter une architecture Zero Trust. Elle aborde la protection des identités, réseaux et applications afin de réduire les surfaces d'attaque.

Contenu du plan de cours

Module 1 : Fondamentaux du Zero Trust

- De la sécurité périmétrique au Zero Trust.
- Principes : ne jamais faire confiance, toujours vérifier.
- Composantes principales : identité, appareils, réseaux, applications.

Module 2 : Concevoir une architecture Zero Trust

- Sécurité centrée sur l'identité.
- Microsegmentation et contrôles réseau.

- Accès sécurisé aux applications.

Module 3 : Feuille de route de mise en œuvre

- Étapes pour une adoption graduelle.
- Outils et technologies (Okta, Azure AD, Zscaler, etc.).
- Intégration avec l'infrastructure existante.

Module 4 : Étude de cas et gouvernance

- Mise en place d'une ZTA réelle.
- Alignement avec politiques et conformité.
- Monitoring et maintien en condition de sécurité.

Approche et méthode pédagogique

Ce cours privilégie une approche structurée et orientée vers la conception d’architectures de sécurité, combinant des exposés conceptuels à des études de cas concrets. L’apprentissage est centré sur l’application des principes du Zero Trust à des environnements réels, notamment par l’analyse de scénarios et des stratégies de mise en œuvre. La progression permet aux participant.e.s de développer une vision globale et opérationnelle pour sécuriser les systèmes et réduire les surfaces d’attaque.

Prérequis

- Connaissances en gestion des réseaux et identités.
- Familiarité avec les cadres de cybersécurité.

Recommandations

Réviser : les concepts de sécurité réseau la gestion des identités et des accès (IAM)

Se familiariser avec : les principes de la cybersécurité moderne les environnements hybrides (cloud et on premises)

Identifier vos enjeux : protection des accès et des données sensibles réduction des surfaces d’attaque modernisation de l’architecture de sécurité