New

Zero Trust Security – Implémenter une architecture moderne de sécurité

Renforcer la protection des identités et des ressources

Présentiel ou en classe à distance

3 jours (21 h)

Prix inter : 2.890,00 € HT
Forfait intra : 7.690,00 € HT

Réf.: SR107

La formation **Zero Trust Security** Implémenter une architecture moderne de sécurité apporte une compréhension complète et opérationnelle du modèle Zero Trust, devenu une référence pour faire face à l'évolution des menaces et à la disparition progressive des périmètres traditionnels. Elle permet d'appréhender les principes fondamentaux du « Never trust, always verify », d'identifier les piliers clés d'une architecture Zero Trust (identité, appareils, réseau, applications, données, supervision) et de comprendre l'apport des référentiels tels que **NIST 800-207** et **Cloud Security Alliance**. Les participants acquièrent une vision claire des mécanismes essentiels : IAM, MFA, ZTNA, micro-segmentation, contrôle d'accès contextuel, supervision continue et UEBA.
Au-delà des concepts, la formation met l'accent sur la **conception et la mise en oeuvre concrète** d'une architecture Zero Trust adaptée à un système d'information existant. Grâce aux ateliers pratiques, les apprenants apprennent à cartographier leur SI, définir des politiques d'accès, concevoir des stratégies de micro-segmentation, analyser des signaux de sécurité et élaborer une roadmap Zero Trust réaliste.

A qui s'adresse cette formation ?

Pour qui

- Responsables et ingénieurs cybersécurité
- RSSI / adjoints RSSI Architectes systèmes, réseaux ou cloud Ingénieurs infrastructure / DevSecOps / SecOps
- Administrateurs systèmes et réseaux confirmés
- Chefs de projet sécurité ou transformation SI Consultants IT / cybersécurité

Prérequis

- Connaissances en systèmes, réseaux et sécurité
- Disposez-vous des connaissances nécessaires pour suivre cette formation ? Testez-vous !

Programme

1 - Introduction au Zero Trust

- Contexte et limites des modèles de sécurité périmétriques
- Définition : Never trust, always verify
- Menaces internes et externes
- Principes clés : moindre privilège, vérification continue, accès contextuel
  Atelier

  Étude de cas : comparaison sécurité périmétrique vs Zero Trust (risques / bénéfices)

2 - Référentiels, cadres et piliers du Zero Trust

- Référentiels et standards (NIST 800-207, CSA)
- Modèles de maturité Zero Trust

- Piliers du Zero Trust : Identités et utilisateurs, Appareils (device posture, endpoint trust), réseau et environnement, applications et workloads, données
- Software-Defined Perimeter (SDP)
  Atelier

  Positionner un SI sur un modèle de maturité Zero Trust

  Identifier les piliers prioritaires à sécuriser

3 - Identity et Access Management dans une approche Zero Trust

- Rôle central de l'identité dans Zero Trust
- MFA, SSO, RBAC, ABAC, politiques adaptatives
- ZTNA vs VPN
- Gestion des identités, des sessions et des privilèges
  Atelier

  Concevoir des politiques d'accès Zero Trust pour différents profils (utilisateur, admin, prestataire)

4 - Réseau, appareils et micro-segmentation

- Micro-segmentation : principes et cas d'usage
- Flux Nord-Sud vs Est-Ouest
- Sécurisation des appareils et posture de confiance
- Outils et approches de segmentation logique
  Atelier

  Définir une stratégie de micro-segmentation et de contrôle des flux sur un cas donné

5 - Supervision, validation continue et sécurité des données

- Supervision continue dans un modèle Zero Trust
- Logs, SIEM, UEBA
- Détection d'anomalies et réponse aux incidents
- Protection et contrôle d'accès aux données
  Atelier

  Analyse de scénarios de sécurité à partir de signaux de supervision

  Décisions d'accès et de réponse dans un modèle Zero Trust

6 - Conception et gouvernance d'une architecture Zero Trust

- Principes de conception d'une architecture Zero Trust
- Démarche de conception par étapes
- Gouvernance SSI et intégration Zero Trust
- Gestion des risques et conformité (ISO, RGPD)
  Atelier

  Concevoir une architecture Zero Trust cible à partir d'un SI existant

7 - Mise en oeuvre et plan d'adoption Zero Trust

- Phases d'implémentation et priorisation
- Roadmap Zero Trust
- Mesure de maturité et indicateurs de pilotage
- Conduite du changement
  Atelier

  Élaborer une roadmap Zero Trust réaliste et priorisée

8 - Projet d'intégration global

- Étude de cas complète (inspirée d'incidents réels)
- Synthèse des concepts, architecture et gouvernance
  Atelier

  Projet final : conception d'un plan Zero Trust complet : analyse, architecture cible, plan d'adoption

Les objectifs de la formation

- Comprendre les principes fondamentaux du Zero Trust
- Identifier les composants clés d’une architecture Zero Trust (IAM, ZTNA, micro-segmentation, supervision, ...)
- Savoir concevoir et planifier une implémentation Zero Trust adaptée à un contexte réel
- Réaliser des mises en pratique concrètes (cartographie, scénarios d’accès, micro-segmentation)

Evaluation

- Pendant la formation, le formateur évalue la progression pédagogique des participants via des QCM, des mises en situation et des travaux pratiques. Les participants passent un test de positionnement avant et après la formation pour valider leurs compétences acquises.

Les points forts de la formation

- L'apprentissage par la pratique : les phases théoriques sont complétées d'ateliers favorisant un ancrage durable des acquis
- Une formation animée par des formateurs experts en cybersécurité et architectures Zero Trust

Dates et villes 2026 - Référence SR107

Dernières places disponibles Session garantie

A distance

du 2 mars au 4 mars	du 15 juin au 17 juin	du 19 oct. au 21 oct.
du 27 avr. au 29 avr.	du 7 sept. au 9 sept.	du 30 nov. au 2 déc.

Paris

du 2 mars au 4 mars	du 15 juin au 17 juin	du 19 oct. au 21 oct.
du 27 avr. au 29 avr.	du 7 sept. au 9 sept.	du 30 nov. au 2 déc.