

ZERO TRUST

UNE POSTURE DE SÉCURITÉ RENFORCÉE

FFCNCERCERXCS27

PRIX : 2 580 €

DURÉE : 3 JOURS

Pauses et déjeuners offerts



NOUVEAU



AVANCÉ



ATELIER



RÉALISABLE
EN ANGLAIS



FAISABLE À
DISTANCE

PRÉSENTATION

Le Zero Trust (ou « confiance zéro ») est une approche moderne et innovante de la cybersécurité qui rompt avec le modèle traditionnel et qui repose sur un principe fondamental : ne jamais faire confiance, toujours vérifier.

Cette formation a pour objectif de donner aux participants les clés pour comprendre, mettre en œuvre et porter une stratégie Zero Trust au sein de leur organisation.

OBJECTIFS

- Présenter les principes fondamentaux du Zero Trust et ses avantages
- Évaluer la posture de sécurité d'une organisation
- Concevoir une feuille de route pour implémenter la stratégie Zero Trust
- Identifier et appliquer les axes de mise en œuvre technique et organisationnelle

PROGRAMME

Introduction et enjeux de la cybersécurité moderne

- Les principales cyberattaques et leurs caractéristiques
- Risques, menaces et vulnérabilités
- Objectifs de sécurité
- Domaines d'application en entreprise

Origine du modèle Zero Trust

Comparaison avec les approches traditionnelles

Principes et conception : Architecture à 5 piliers

- Réseaux : Micro-segmentation, ZTNA
- Données : Chiffrement de bout-en-bout
- Applications : Contrôle des transactions
- Identité : MFA continu, authentification forte
- Terminaux : XDR, conformité
- Travaux pratiques

Gouvernance, risques et conformité dans un modèle Zero Trust

- Gouvernance : Vision métier / Vision opérationnelle
- Gestion et analyse de risque
- ISO 27001 et 27005
- Audit de sécurité
- Conformité : NIS2, RGPD, DORA, ZTX, ...

Transition vers le Zero Trust : Mise en place progressive

Zero Trust dans l'ère de l'IA

Synthèse et conclusion

PUBLIC/PRÉREQUIS

Cette formation s'adresse aux professionnels impliqués dans la définition, la mise en œuvre ou la gouvernance de la cybersécurité au sein de leur organisation.

Des connaissances de base des enjeux IT et cybersécurité sont recommandées afin de tirer pleinement profit de cette formation.

RESPONSABLE(S)

Maya BADR

Enseignante et responsable pédagogique en cybersécurité et technologies du numérique à Télécom Paris Executive Education. Elle a obtenu son diplôme de doctorat en communications numériques de Télécom Paris.

MODALITÉS PÉDAGOGIQUES

L'approche pédagogique combine apports théoriques, études de cas et travaux pratiques pour favoriser une appropriation opérationnelle et adaptée aux enjeux réels des entreprises.



CYBERSÉCURITÉ

FORMATIONS INTER-ENTREPRISES