Architecture Zero Trust : conception et déploiement selon le framework NIST SP 800-207

Lien : https://innov-systems.com/formation/architecture-zero-trust-conception-et-deploiement-selon-le-framework-nist-sp-800-207

DURÉE
5 jours (35h)

RÉFÉRENCE
SI121

CATÉGORIE
Identité, Gestion des Accès (IAM) et Zero Trust

Innov Systems

OBJECTIFS DE LA FORMATION

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

- Comprendre les principes fondamentaux du Zero Trust
- Maîtriser le framework NIST SP 800-207
- Concevoir une architecture Zero Trust en entreprise
- Mettre en œuvre des politiques d’accès conditionnel
- Sécuriser les identités, endpoints et réseaux
- Réduire la surface d’attaque des systèmes d’information
- Implémenter la micro-segmentation réseau
- Intégrer les outils SIEM, IAM et EDR dans une architecture Zero Trust
- Piloter la transformation sécurité d’un SI traditionnel vers Zero Trust
- Améliorer la posture globale de cybersécurité
- Déployer des stratégies de sécurité adaptatives
- Étudier des cas concrets de mise en œuvre Zero Trust

POUR QUI ?

- Architectes cybersécurité
- RSSI / CISO
- Ingénieurs sécurité
- Cloud security engineers
- Network security engineers
- DevSecOps engineers
- Administrateurs systèmes et réseaux
- Consultants cybersécurité
- SOC analysts
- Identity & Access management specialists
- Risk and compliance officers
- Toute personne impliquée dans la conception et la mise en œuvre de architectures sécurisées Zero Trust

Innov Systems

Programme détaillé

1 / Introduction au Zero Trust

- Principes fondamentaux du modèle Zero Trust
- Évolution des architectures périmétriques vers Zero Trust
- Enjeux de sécurité dans les environnements cloud et hybrides

2 / Référentiel NIST SP 800-207

- Présentation du framework NIST Zero Trust Architecture
- Concepts clés : Policy Engine, Policy Administrator, Policy Enforcement Point
- Application du modèle en entreprise

3 / Principes fondamentaux du Zero Trust

- “Never trust, always verify”
- Micro-segmentation des réseaux
- Moindre privilège et contrôle continu

4 / Gestion des identités et des accès (IAM)

- Identity-first security
- MFA et authentification forte
- Federation d’identités et SSO

5 / Micro-segmentation et sécurité réseau

- Segmentation dynamique des réseaux
- Contrôle des flux est-ouest et nord-sud
- SDN et politiques réseau contextuelles

Innov Systems

6 / Sécurisation des endpoints et workloads

- EDR/XDR et protection des terminaux
- Sécurisation des workloads cloud et containers
- Attestation et posture de sécurité des devices

7 / Accès conditionnel et contrôle contextuel

- Politiques basées sur le contexte (device, localisation, risque)
- Adaptive access control
- Risk-based authentication

8 / Monitoring, logging et détection des menaces

- Centralisation des logs et SIEM
- Analyse comportementale et détection d’anomalies
- Threat intelligence intégrée

9 / Déploiement et transformation Zero Trust

- Étapes de migration depuis une architecture legacy
- Stratégie progressive d’adoption
- Intégration avec cloud et environnements hybrides

10 / Cas pratiques et architecture cible

- Design d’une architecture Zero Trust complète
- Mise en œuvre dans un environnement entreprise
- Retours d’expérience et bonnes pratiques

Innov Systems

Approche pédagogique

- Support Ecrit et Projection
- Exposés Interactifs, Podcasts et Vidéos
- Brainstorming et Jeux de Rôle
- Cas Pratiques et Labs inclus pour leur impact opérationnel
- Test de Validation des Acquis des Connaissances

Prochaines dates programmées

01 au 05 Fév. 2027	Présentiel - Casablanca
29 Mars au 02 Avr. 2027	Présentiel - Casablanca
24 au 28 Mai 2027	Présentiel - Casablanca
19 au 23 Juil. 2027	Présentiel - Casablanca
13 au 17 Sep. 2027	Présentiel - Casablanca

Autres dates possibles sur demande. Contactez-nous pour organiser une session intra-entreprise.

Réservation & Renseignements

Téléphone : +212 522 247 210
Email : contact@innov-systems.com
Web : https//www.innov-systems.com

Innov Systems — Tous droits réservés