Architecture de la Sécurité Microsoft et Gouvernance Cloud

Lien :
https://innov-systems.com/formation/architecture-de-la-securite-microsoft-et-gouvernance-cloud

DURÉE
5 jours (35h)

RÉFÉRENCE
SEC313

CATÉGORIE
Sécurité des Systèmes, Sécurité des Serveurs

OBJECTIFS DE LA FORMATION

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

- Concevoir une architecture de sécurité Microsoft alignée sur les principes Zero Trust et la gouvernance d’entreprise
- Développer une stratégie complète de protection des identités, des données et des applications dans les environnements hybrides et multi-clouds
- Intégrer les bonnes pratiques de conformité et d’audit avec les outils Microsoft (Defender, Entra ID, Purview, Azure Policy)
- Renforcer la résilience opérationnelle et la surveillance continue à travers des processus de sécurité automatisés
- Déployer des contrôles techniques et organisationnels adaptés aux menaces modernes

POUR QUI ?

- Architectes systèmes et cloud
- Administrateurs sécurité et responsables infrastructure
- Chefs de projet techniques en cybersécurité
- Responsables sécurité des systèmes d’information (RSSI techniques)

Programme détaillé

1 / PRINCIPES DE L'ARCHITECTURE ZERO TRUST

- Comprendre les piliers du modèle Zero Trust appliqué à Microsoft 365 et Azure
- Identifier les composants d'une architecture de sécurité moderne
- Relier les objectifs métier aux exigences de sécurité

2 / MODÉLISATION DES RISQUES ET DE LA GOUVERNANCE

- Cartographier les actifs critiques et les vecteurs de menaces
- Définir une stratégie GRC (Gouvernance, Risques, Conformité) alignée sur les normes ISO et NIST
- Évaluer les indicateurs de maturité de la sécurité

3 / CONSTRUCTION D'UNE STRATÉGIE DE SÉCURITÉ GLOBALE

- Identifier les domaines d'intégration technique : réseau, identités, données
- Élaborer une architecture de défense en profondeur
- Étude de cas : diagnostic et conception d'une stratégie de sécurité d'entreprise

4 / STRATÉGIE D'IDENTITÉ ET AUTHENTIFICATION

- Mettre en œuvre la gestion des identités avec Microsoft Entra ID (ex Azure AD)
- Configurer l'accès conditionnel et l'authentification multifacteur
- Définir une politique de gouvernance des rôles et des accès privilégiés

5 / SÉCURISATION DES IDENTITÉS HYBRIDES ET MULTI-CLOUDS

- Synchroniser les identités on-premise et cloud en toute sécurité
- Gérer les identités de service et les comptes non humains
- Implémenter la délégation et la séparation des privilèges

6 / PROTECTION DES SESSIONS ET DES ACCÈS CLIENT

- Sécuriser les connexions distantes avec Microsoft Defender for Endpoint
- Configurer la supervision des activités suspectes dans le SIEM
- Étude de cas : stratégie d’accès sécurisé pour les utilisateurs distants

7 / CONCEPTION D’UNE STRATÉGIE DE PROTECTION DES DONNÉES

- Identifier, classifier et protéger les données sensibles (Microsoft Purview, DLP)
- Définir les politiques de chiffrement et de gestion des clés
- Appliquer la confidentialité dès la conception (Privacy by Design)

8 / SÉCURISATION DES APPLICATIONS ET DES API

- Intégrer la sécurité dans le cycle DevSecOps
- Configurer la sécurité applicative via Azure App Service et Defender for Cloud Apps
- Appliquer les principes de modélisation des menaces sur les API

9 / GESTION DE LA CONFORMITÉ ET DES AUDITS

- Configurer Azure Policy et Microsoft Defender for Cloud pour la conformité continue
- Suivre et interpréter les scores de conformité
- Rédiger un plan d’action d’amélioration de la sécurité

10 / ARCHITECTURE DES OPÉRATIONS DE SÉCURITÉ

- Construire une stratégie SOC adaptée à Microsoft 365 et Azure
- Définir les processus d’audit et d’investigation
- Déterminer les exigences de journalisation et de conservation des logs

11 / INTÉGRATION DES OUTILS SIEM ET SOAR

- Configurer Microsoft Sentinel pour la détection et la réponse
- Automatiser la réponse aux incidents avec des playbooks et runbooks

- Corréler les alertes entre les environnements hybrides

12 / THREAT INTELLIGENCE ET RÉPONSE AUX INCIDENTS

- Identifier les sources de renseignement sur les menaces
- Élaborer un plan de réponse et d’escalade
- Étude de cas : gestion d’un incident de sécurité sur un environnement Azure

13 / RÉSILIENCE, CONTINUITÉ ET PLAN DE REPRISE

- Définir une stratégie de sauvegarde et de reprise sécurisée dans Azure
- Intégrer la sécurité dans la gestion de la continuité d’activité
- Tester et auditer la résilience du système

14 / SÉCURITÉ DES SERVICES CLOUD (IAAS, PAAS, SAAS)

- Spécifier les lignes de base de sécurité pour les workloads cloud
- Sécuriser les conteneurs, microservices et environnements DevOps
- Évaluer la sécurité des environnements SaaS interconnectés

15 / ÉVOLUTION DE L’ARCHITECTURE DE SÉCURITÉ

- Mettre en place une amélioration continue de la posture de sécurité
- Mesurer et piloter la performance des contrôles de sécurité
- Atelier final : conception d’une architecture de sécurité Microsoft complète et documentée

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

06 au 10 Juil. 2026	Présentiel - Casablanca
31 Août au 04 Sep. 2026	Distanciel
26 au 30 Oct. 2026	Distanciel

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