Cybersécurité des administrations publiques et de l'e-gouvernement

Lien : https://innov-systems.com/formation/cybersecurite-des-administrations-publiques-et-de-le-gouvernement

DURÉE
8 jours (56h)

RÉFÉRENCE
SI88

CATÉGORIE
Cybersécurité Sectorielle

Innov Systems

OBJECTIFS DE LA FORMATION

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

- Comprendre les enjeux de la cybersécurité dans les administrations publiques
- Concevoir des architectures sécurisées pour les plateformes d’e-gouvernement
- Mettre en œuvre une gouvernance cybersécurité adaptée au secteur public
- Sécuriser les identités numériques et les accès aux services publics
- Protéger les données sensibles et les informations des citoyens
- Renforcer la sécurité des infrastructures, applications et API gouvernementales
- Développer des capacités de détection et de réponse aux incidents
- Assurer la continuité et la résilience des services publics numériques
- Intégrer les exigences réglementaires et les bonnes pratiques internationales
- Déployer une stratégie de sensibilisation et de culture cybersécurité
- Exploiter les technologies émergentes pour renforcer la sécurité publique
- Élaborer une feuille de route de cybersécurité pour une administration numérique

POUR QUI ?

- RSSI / CISO des administrations publiques
- DSI et responsables informatiques du secteur public
- Responsables de la transformation numérique
- Architectes cybersécurité
- Ingénieurs cybersécurité
- Administrateurs systèmes et réseaux
- Responsables des plateformes d’e-gouvernement
- Auditeurs SSI et responsables conformité
- Analystes SOC et équipes CERT/CSIRT
- Décideurs publics et hauts fonctionnaires
- Consultants en cybersécurité du secteur public
- Toute personne impliquée dans la sécurisation des services publics numériques et des plateformes d’e-gouvernement

Innov Systems

Programme détaillé

1 / Introduction à la cybersécurité des administrations publiques

- Enjeux de la transformation numérique du secteur public
- Menaces ciblant les administrations et services publics
- Principes de la gouvernance de la cybersécurité publique

2 / Architecture de sécurité des plateformes d’e-gouvernement

- Portails citoyens et services numériques
- Interconnexion des systèmes d'information publics
- Architectures cloud, hybrides et souveraines

3 / Gouvernance, gestion des risques et conformité

- Cadres de gouvernance SSI
- Gestion des risques cyber dans le secteur public
- Conformité réglementaire et politiques nationales

4 / Gestion des identités numériques et des accès

- Identity and Access Management (IAM)
- Authentification forte (MFA) et Single Sign-On (SSO)
- Gestion des identités des citoyens, agents et partenaires

5 / Protection des données publiques et confidentialité

- Classification et protection des données sensibles
- Chiffrement des données en transit et au repos
- Protection des données personnelles et respect de la vie privée

Innov Systems

6 / Sécurité des infrastructures et des réseaux

- Sécurisation des centres de données et réseaux gouvernementaux
- Segmentation, pare-feu et architectures Zero Trust
- Sécurité des environnements cloud gouvernementaux

7 / Sécurité des applications et des API gouvernementales

- Développement sécurisé des applications publiques
- Sécurisation des API et services numériques
- Gestion des vulnérabilités et correctifs

8 / Détection des menaces et réponse aux incidents

- Supervision SOC et surveillance continue
- Gestion des incidents de cybersécurité
- Plans de réponse, continuité d’activité (PCA) et reprise (PRA)

9 / Cybersécurité des services numériques critiques

- État civil, fiscalité, santé et justice numériques
- Protection des infrastructures critiques gouvernementales
- Résilience des services essentiels

10 / Sensibilisation, gouvernance et culture cybersécurité

- Formation des agents publics
- Sensibilisation des décideurs et des utilisateurs
- Gestion des risques humains et de l’ingénierie sociale

11 / Technologies émergentes et cybersécurité publique

- Intelligence artificielle pour la cyberdéfense
- Sécurité des objets connectés (IoT) et des Smart Cities

Inov Systems

- Blockchain et identité numérique souveraine

12 / Cas pratiques et feuille de route de sécurisation

- Audit d’une plateforme d’e-gouvernement
- Élaboration d’un plan directeur de cybersécurité
- Retours d’expérience et bonnes pratiques internationales

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

12 au 21 Jan. 2027	Présentiel - Casablanca
08 au 17 Mars 2027	Présentiel - Casablanca
03 au 12 Mai 2027	Présentiel - Casablanca
28 Juin au 07 Juil. 2027	Présentiel - Casablanca
23 Août au 01 Sep. 2027	Présentiel - Casablanca

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

Innov Systems

Réservation & Renseignements

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

Innov Systems — Tous droits réservés