Cybersécurité des systèmes de santé : protection des DMP, imagerie médicale et dispositifs connectés

Lien : https://innov-systems.com/formation/cybersecurite-des-systemes-de-sante-protection-des-dmp-imagerie-medicale-et-dispositifs-connectes

DURÉE
8 jours (56h)

RÉFÉRENCE
SI91

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 établissements de santé
- Identifier les risques pesant sur les dossiers médicaux, l'imagerie et les dispositifs connectés
- Concevoir une architecture de sécurité adaptée aux systèmes d'information de santé
- Mettre en œuvre des mécanismes de protection des données médicales
- Sécuriser les infrastructures d'imagerie médicale et les dispositifs IoMT
- Déployer des solutions de détection, de supervision et de réponse aux incidents
- Assurer la continuité des soins grâce à des stratégies de résilience cyber
- Renforcer la gouvernance et la conformité des systèmes de santé
- Sécuriser les accès, les identités et les échanges de données médicales
- Intégrer les bonnes pratiques de cybersécurité dans les projets de santé numérique
- Réduire les risques liés aux fournisseurs et aux logiciels médicaux
- Étudier des cas concrets de sécurisation d'établissements de santé

POUR QUI ?

- RSSI / CISO des établissements de santé
- Responsables des systèmes d'information hospitaliers
- Architectes cybersécurité
- Ingénieurs cybersécurité
- Administrateurs systèmes et réseaux
- Responsables biomédicaux
- Responsables de la sécurité des dispositifs médicaux
- Professionnels de l'informatique de santé
- Consultants en cybersécurité et e-santé
- Responsables conformité et protection des données de santé
- Chefs de projet en transformation numérique de la santé
- Toute personne impliquée dans la sécurisation des systèmes d'information et des infrastructures de santé

Innov Systems

Programme détaillé

1 / Introduction à la cybersécurité des systèmes de santé

- Enjeux de la transformation numérique en santé
- Panorama des menaces ciblant les établissements de santé
- Impacts des cyberattaques sur les soins et la continuité des activités

2 / Architecture des systèmes d'information de santé

- Dossier Médical Patient (DMP/DPI) et systèmes d'information hospitaliers
- Interconnexion des applications cliniques et administratives
- Flux de données entre établissements, laboratoires et plateformes de santé

3 / Protection des dossiers médicaux électroniques

- Classification et protection des données de santé
- Contrôle d'accès, gestion des identités (IAM) et moindre privilège
- Chiffrement des données au repos et en transit

4 / Sécurisation des systèmes d'imagerie médicale

- Architectures PACS, RIS et modalités d'imagerie
- Sécurisation des protocoles DICOM et des échanges d'images
- Protection des serveurs d'archivage et des postes de diagnostic

5 / Cybersécurité des dispositifs médicaux connectés (IoMT)

- Inventaire et gestion des équipements biomédicaux
- Analyse des risques des dispositifs connectés
- Segmentation réseau et sécurisation des communications

Innov Systems

6 / Sécurité des infrastructures hospitalières

- Protection des serveurs, postes de travail et réseaux
- Microsegmentation et architecture Zero Trust
- Sécurisation des accès distants et des environnements cloud

7 / Détection des menaces et réponse aux incidents

- Supervision des événements de sécurité (SIEM)
- Détection des comportements anormaux et des ransomwares
- Réponse aux incidents et gestion de crise hospitalière

8 / Gouvernance, conformité et protection des données de santé

- Politiques de sécurité des établissements de santé
- Conformité aux réglementations sur les données de santé
- Audit, traçabilité et gestion des preuves numériques

9 / Continuité d'activité et résilience cyber

- Sauvegarde sécurisée des données médicales
- Plans de continuité (PCA) et de reprise d'activité (PRA)
- Exercices de simulation et amélioration continue

10 / Intelligence artificielle et cybersécurité en santé

- Détection assistée des anomalies de sécurité
- Protection des applications de santé utilisant l'IA
- Analyse prédictive des risques cyber

11 / Sécurité de la chaîne d'approvisionnement numérique

- Gestion des risques liés aux fournisseurs et prestataires
- Sécurisation des logiciels médicaux et des mises à jour

Inov Systems

- Évaluation des tiers et des dispositifs connectés

12 / Cas pratiques et stratégie de sécurisation d'un établissement de santé

- Analyse d'incidents cyber dans le secteur de la santé
- Élaboration d'une feuille de route de cybersécurité
- Bonnes pratiques de protection des systèmes hospitaliers

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 10 Fév. 2027	Présentiel - Casablanca
29 Mars au 07 Avr. 2027	Présentiel - Casablanca
24 Mai au 02 Juin 2027	Présentiel - Casablanca
19 au 28 Juil. 2027	Présentiel - Casablanca
13 au 22 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