Cybersécurité des dispositifs médicaux connectés

Public visé

Professionnels du dispositif médical ou du diagnostic in vitro :

- Ingénieurs en systèmes embarqués
- Responsables cybersécurité
- Développeurs de logiciels embarqués pour les dispositifs médicaux

Pourquoi participer ?

La cybersécurité des dispositifs médicaux intégrant du logiciel est devenue une préoccupation majeure en raison de l'augmentation des cyberattaques ciblant les établissements de santé. Ces dispositifs, souvent connectés à des réseaux et contenant des données sensibles, présentent des vulnérabilités qui peuvent être exploitées par des hackers malveillants. Il est donc essentiel de comprendre les risques et de les prendre en compte dès la conception du produit afin d'assurer la sécurité des patients.

Prérequis

Il est recommandé de posséder, avant l'entrée en formation, de compétences en informatique et électronique.

Objectifs pédagogiques

Acquérir une compréhension technique approfondie et des compétences pratiques en matière de cybersécurité des dispositifs médicaux connectés.

Contenu de la formation

- **Les fondamentaux de la cybersécurité**
  - Définitions et termes techniques (risque, vulnérabilité, exploit, etc.)
  - La sécurité d'un dispositif médical numérique versus la sécurité IT traditionnelle ?

- **Conception Sécurisée des dispositifs médicaux connectés**
  - Principes de sécurité dans la conception des dispositifs médicaux
  - Gestion des vulnérabilités dans les systèmes embarqués (ex : vulnérabilités logicielles, failles matérielles)
  - Architecture de sécurité des dispositifs médicaux connectés et segmentation des composants critiques

- **Sécurité des Interfaces et Protocoles de Communication**
  - Protocoles de communication (Bluetooth, Wi-Fi, Zigbee, etc.)
  - Sécurité des interfaces des dispositifs médicaux (ports USB, UART, JTAG et SWD)
  - Techniques de défense contre les attaques sur les protocoles de communication (ex : attaques de type man-in-the-middle)

- **Sécurité du matériel et du logiciel**
  - Attaque sur le firmware et extraction (dump) de la mémoire
  - Analyse statique d'un firmware (extraction des fichiers, analyse automatique)
  - Analyse dynamique (émulation de firmware)
  - Attaque par canaux auxiliaires

Gestion des mises à jour et des patches de Sécurité

- Méthodologies de gestion des mises à jour sécurisées
- Stratégies de déploiement des correctifssans interruption des soins
- Protection contre les mises à jour malveillantes (vérification d'intégrité)
- Utilisation de mécanismes de récupération sécurisée après un échec de mise à jour

- **Cryptographie et Protection des Données dans les dispositifs médicaux connectés**
  - Introduction aux concepts cryptographiques appliqués aux systèmes embarqués (AES, RSA, ECC)
  - Sécurisation des données échangées et des communications entre dispositifs (ex : chiffrement des données en transit et au repos)
  - Gestion des clés de chiffrement dans les systèmes embarqués

- **Audit de suivi**
  - Niveau de risque des vulnérabilité et plan d'actions
  - Mise en place de mesures correctives et évaluation de leur pertinence et de leur efficacité
  - Rejeu des tests de sécurité initiaux et vérification que les mesures correctives n'entrainent pas de nouvelles vulnérabilités

- **Démonstration d'une mise en pratique de tests de sécurité : méthodologie de pentest**

Modalités pédagogiques

Techniques : ordinateur.
Encadrement : Formateur titulaire d'un diplôme d'ingénieur ou équivalent ; expérience professionnelle de plus de 5 ans dans le domaine des dispositifs médicaux.

Moyens et supports pédagogiques

Un espace extranet dédié sera mis à la disposition de chaque stagiaire.
Support de cours et exercices.

Modalités d'évaluation et de suivi

Suivi : Feuilles de présence à la demi-journée, signées par les stagiaires et contresignées par le formateur, attestations de fin de formation remises à chaque stagiaire.
Évaluation : QCM et Questionnaires de satisfaction remplis par les stagiaires en fin de formation.

Informations pratiques

Durée : 7 heures
Modalité d'accès : Formation sur site client ou à distance
Nombre de participants maximum : 12
Délai d'accès : formation réalisable sous 2 à 4 mois.
Tarif : 3900,00 € HT
Accessibilité : Accès possible aux personnes à mobilité réduite et adaptation possible selon handicap : nous contacter
Contact : bonjour@md101.io

« *Investir dans la formation c'est conjuguer au présent mais aussi au futur le souci des hommes et le souci des résultats.* »