MD101
CONNECTIONS FOR CARE

Date de publication : Novembre 2023

FORMATION

INTER-ENTREPRISES

ASSURANCE QUALITÉ

Les fondamentaux de la cybersécurité des dispositifs médicaux IoT

7h

INFORMATIONS PRATIQUES

Date : 20 février 2024
Durée totale : 7h00
Horaires : 9h00-12h30 / 13h30-17h00
Nombre de participants : 10 personnes maximum
Modalités d'accès : formation inter-entreprise à distance
Tarif : 750€ HT par personne
Accessibilité : accès possible aux personnes à mobilité réduite et adaptation possible selon handicap (nous contacter)
Contact : bonjour@md101.io

OBJECTIFS PÉDAGOGIQUES

- Comprendre les fondamentaux de la sécurité dans un dispositif embarqué
- Acquérir une compréhension des compétences d'un attaquant dans un environnement embarqué

A QUI S'ADRESSE LA FORMATION ?

Fabricants de dispositifs médicaux

PRÉREQUIS

Il est recommandé de posséder, avant l'entrée en formation, de compétences en informatique et électronique et connaitre les normes applicables à la cybersécurité des dispositifs médicaux

POURQUOI PARTICIPER ?

L'électronique et les logiciels embarqués des dispositifs médicaux gagnent en complexité. Les normes cybersécurité applicables permettent de garantir la qualité et la sécurité de ces dispositifs. Cette formation vous permet de comprendre la spécificité du risque cyber des systèmes embarqués dans les applications médicales, et d'ainsi améliorer votre produit.

Les fondamentaux de la cybersécurité des dispositifs médicaux IoT

DISTANCIEL

CONTENU DE LA FORMATION

1. Définitions et termes techniques (risque, vulnérabilité, exploit, etc.)
   - Relations entre risques, menaces et vulnérabilités (ISO 27000)
   - Qu'est-ce qu'un exploit ? Exemples pratiques
2. La sécurité embarquée
   - Pourquoi la sécurité de l'IoT est-elle importante?
   - Comment diffère-t-elle de la sécurité IT traditionnelle ?
   - Frameworks, standards et guides
3. La modélisation de la menace dans l'embarqué
   - Framework pour la modélisation de la menace (STRIDE)
   - Utilisation d'« attack tree » pour préciser la menace
   - Comment classer vos menaces à l'aide du système DREAD ?
   - Autres types de modélisation
   - Menaces communes dans l'IoT
4. La méthode de test pour la sécurité embarquée
   - Reconnaissance passive (OSINT)
   - Couche matérielle (périphérique, interface de debug, attaques par canaux auxiliaires…)
   - Couche réseau (scan, détection de service, écoute réseau)
   - Analyse des protocoles et attaques des services
   - Test de pénétration des applications (web, mobiles)

MOYENS PÉDAGOGIQUES

- **Pédagogiques :** support de cours et exercices.
- **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 DE SUIVI ET D'ÉVALUATION DE LA FORMATION

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

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

MD101
CONNECTIONS FOR CARE

MD101 Consulting, 276 avenue du Douard - 13400 AUBAGNE
SIRET : 79033094800023 - Email : bonjour@md101.io

ORGANISME DE FORMATION
Déclaration d'activité enregistrée sous le N° 93131913913 auprès du préfet de région Provence-Alpes-Côte d'Azur