LES FONDAMENTAUX DE LA CYBERSECURITE EMBARQUE

Formation

1 jour
750 € HT

Kereval propose des formations Inter et en Intra-entreprise dispensées par des formateurs certifiés et experts en test logiciel. Selon les besoins spécifiques, Kereval est en mesure de dispenser des formations sur-mesure, dont le contenu et la durée sont adaptés à votre contexte.

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.

Objectifs pédagogiques

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

Pré-requis

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

Public formé

Fabricants de dispositifs électroniques

Et après ?

Formation niveau technique

Contenu

Les fondamentaux de la cybersécurité

- Définitions et termes techniques (risque, vulnérabilité, exploit, etc.)
- Relations entre risques, menaces et vulnérabilités (ISO 27000)
- Qu'est-ce qu'un exploit ? Exemples pratiques

Tour d'horizon de la menace embarquée

- 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
- La modélisation de la menace dans l'embarqué
  - Catégorisation de la menace (STRIDE)
  - Classement de la menace (DREAD)
  - Outils d'aide à la modélisation
- La méthode de test pour la sécurité embarquée
  - Méthode d'analyse de la sécurité d'un firmware
  - Analyse des protocoles et attaques des services
  - Test de pénétration des applications (web, mobiles)

Hardware hacking

- Analyse des composants d'un circuit imprimé
- Exploitation UART, JTAG et SWD
  - Présentation de l'UART, outils pour communiquer en UART, identification des ports UART et la vitesse de transmission
  - Présentation du JTAG et SWD, identification des pins, matériels utilisés
- Exploitation des bus de communications (SPI, I²C)
  - Matériels nécessaires
  - Fonctionnement du SPI
  - Lecture de mémoire à l'aide du SPI
  - Fonctionnement de l'I²C
  - Attaques pratiques sur l'I²C (sniffing)
- Firmware Hacking
  - Comment obtenir un firmware ?
  - Analyse statique d'un firmware (extraction des fichiers, analyse automatique)
  - Analyse dynamique (émulation de firmware)
- Les attaques par canaux auxiliaires
  - Définition et concept
- Mise en pratique sur un système grand publique
  - Fingerprinting
  - Dump mémoire
  - Analyse de firmware

Méthodes pédagogiques

- Formation en présentiel
- Support ppt

Modalités d'accès et délais

Modalités d'inscription : nous contacter

Délais d'accès : de 1 à 6 mois

Les délais d'accès sont dépendants de la disponibilité de nos formateurs.

Accessible aux personnes en situation de handicap. Nous contacter pour tout aménagement spécifique.

Modalités d'évaluation

Le participant complète un test de positionnement en amont et en aval pour valider les compétences acquises.

Durée

7h sur 1 jour

Prix intra – entreprise	Prix inter – entreprise
Nous contacter pour obtenir un devis.	750 € HT / stagiaire.

Chiffres clés*

*Nous ne possédons pas encore d'indicateurs sur cette formation.