Sécurisation

Sécurité des équipements IoT - Les fondamentaux

3 jours (21h00) | ★★★★½ 4,6/5 | SEC-IOT | Évaluation qualitative de fin de stage | Formation délivrée en présentiel ou distanciel

Contenu mis à jour le 13/10/2023. Document téléchargé le 21/09/2024.

Objectifs de formation

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

- Décrire les bonnes pratiques de déploiement sécurisé des services d'échange réseaux
- Identifier les menaces courantes sur les équipements embarqués
- Analyser la sécurité des micrologiciels embarqués dans les périphériques
- Examiner le fonctionnement des applications d'interactions avec les périphériques.

Modalités, méthodes et moyens pédagogiques

Formation délivrée en présentiel ou distanciel* (blended-learning, e-learning, classe virtuelle, présentiel à distance).

Le formateur alterne entre méthode** démonstrative, interrogative et active (via des travaux pratiques et/ou des mises en situation).

Variables suivant les formations, les moyens pédagogiques mis en oeuvre sont :

- Ordinateurs Mac ou PC (sauf pour certains cours de l'offre Management), connexion internet fibre, tableau blanc ou paperboard, vidéoprojecteur ou écran tactile interactif (pour le distanciel)
- Environnements de formation installés sur les postes de travail ou en ligne
- Supports de cours et exercices

En cas de formation intra sur site externe à M2i, le client s'assure et s'engage également à avoir toutes les ressources matérielles pédagogiques nécessaires (équipements informatiques...) au bon déroulement de l'action de formation visée conformément aux prérequis indiqués dans le programme de formation communiqué.

* *nous consulter pour la faisabilité en distanciel*

** *ratio variable selon le cours suivi*

Prérequis

Posséder des bases dans la sécurité des systèmes d'information. Avoir une connaissance de base des commandes Linux ainsi qu'une familiarité avec les architectures Web courantes.

Public concerné

Pentesters, professionnels de la sécurité et développeurs d'équipements IoT cherchant à approfondir leurs compétences en sécurité appliquée aux équipements embarqués et à comprendre les vulnérabilités courantes et les corriger.

Cette formation :

- Est animée par un consultant-formateur dont les compétences techniques, professionnelles et pédagogiques ont été validées par des diplômes et/ou testées et approuvées par l'éditeur et/ou par M2i Formation
- Bénéficie d'un suivi de son exécution par une feuille de présence émargée par demi-journée par les stagiaires et le formateur.

Programme

Jour 1

Panorama de la sécurité IoT

- Rappels sur les périphériques embarqués
- La cybersécurité et l'IoT
- Vulnérabilités et attaques les plus courantes
- Méthodologie de test de sécurité IoT

Sécurité des réseaux IoT

- Les protocoles spécifiques pour l'IoT
- Analyse de la surface d'attaque (Edge to Cloud)
- Protocoles de communication sans fil (Zigbee / 5G / LORA...)
- Etude de la sécurité des couches applicatives (MQTT)

Exemples de travaux pratiques (à titre indicatif)

- *Tests d'intrusion sur un broker MQTT*
- *Sécurisation d'un broker MQTT*

Jour 2

Pentest appliqué à l'IoT

- Le Top 10 IoT de l'OWASP
- Analyse des interfaces de l'écosystème
- Tests de sécurité des services réseaux exposés
- Exploitation de mécanismes de communication sans fil

Analyse de Firmware

- Méthodologie d'émulation de Firmware
- Extraction du contenu d'un Firmware
- Découverte d'éléments codés en dur
- Exploitation des services réseaux
- Analyse de code source interne

Exemple de travaux pratiques (à titre indicatif)

- *Analyse de sécurité d'un Firmware vulnérable*

Jour 3

Analyse des contrôleurs

- Etude des communications externes (API, Lambda...)
- Interception et rejeux
- Injection d'évènement

Android

- Architecture et sécurité du système
- Décompilation d'un fichier APK
- Etude des interactions avec les périphériques IoT
- Découverte de vulnérabilités dans les applications

Exemples de travaux pratiques (à titre indicatif)

- *Analyse de sécurité d'une application Android*
- *Exploitation des interactions entre les périphériques et le Cloud*

Le contenu de ce programme peut faire l'objet d'adaptation selon les niveaux, prérequis et besoins des apprenants.

Modalités d’évaluation des acquis

- En cours de formation, par des études de cas ou des travaux pratiques
- Et, en fin de formation, par un questionnaire d'auto-évaluation

Accessibilité de la formation

Le groupe M2i s'engage pour faciliter l'accessibilité de ses formations. Les détails de l'accueil des personnes en situation de handicap sont consultables sur la page Accueil et Handicap.

Modalités et délais d’accès à la formation

Les formations M2i sont disponibles selon les modalités proposées sur la page programme. Les inscriptions sont possibles jusqu'à 48 heures ouvrées avant le début de la formation. Dans le cas d'une formation financée par le CPF, ce délai est porté à 11 jours ouvrés.