

Sécurité des équipements IoT – Niveau avancé

2 jours (14 heures)

Perfectionnement

Présentiel ou classe à distance

à partir de

1950 € HT par personne (TVA en vigueur) Repas inclus en présentiel

Contenu mis à jour le 25/09/2026. Document téléchargé le 07/10/2026.

Objectifs

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

- Décrire les mécanismes avancés d'analyse de vulnérabilité des composants IoT
- Identifier des points de faiblesses dans l'architecture de communication inter-composants
- Analyser des binaires compilés et y détecter des anomalies de sécurité
- Expliquer les mécanismes d'injection de code dans des binaires compilés et dans des applications Android
- Analyser le matériel physique à des fins d'exploitation.

Les compétences visées par cette formation font l'objet d'une évaluation.

À qui s'adresse cette formation ?

Pentesters, professionnels de la sécurité et développeurs d'équipements IoT.

Prérequis

Avoir suivi la formation SEC-IOT "Sécurité des équipements IoT – Les fondamentaux" ou avoir les connaissances équivalentes. Avoir une connaissance de base de fonctionnement d'un binaire et des couches Hardwares.

Programme

1 Pendant votre formation

Sécurité des équipements IoT – Niveau avancé

Jour 1

Rappels

- Récapitulatif des concepts de base de sécurité IoT
- Méthodologie d'analyse et de test de sécurité IoT

Vulnérabilités physiques

- Port de débogage
- Exploitation physique (UART, JTAG...)
- Extraction de Firmware

Exemple de travaux pratiques (à titre indicatif)

- *Extraction et analyse d'un Firmware*

Patching de Firmware

- Patching statique d'un Firmware
- Injection d'un Firmware malveillant dans un périphérique
- Patching de vulnérabilité

Exemple de travaux pratiques (à titre indicatif)

- *Mise à jour d'un Firmware vulnérable et réinjection*

Jour 2

Sécurité du microcode

- Rétro-ingénierie de binaires compilés
- Exploitation de binaires (débogage, émulation...)
- Patching statique de binaire

Exemples de travaux pratiques (à titre indicatif)

- *Découverte de vulnérabilité dans un équipement temps réel*
- *Patching statique d'un binaire*

Sécurité des applications Android

- Interception d'appel système
- Recompilement d'applications
- Injection de code à l'exécution

Exemple de travaux pratiques (à titre indicatif)

- Contournement de mécanismes de sécurité avec Frida

Financement

Plusieurs dispositifs de financement sont accessibles via les OPCO (Opérateurs de Compétences), organismes agréés par le ministère du Travail dont le rôle est d'accompagner, collecter et gérer les contributions des entreprises au titre du financement de la formation professionnelle.

Pour plus d'information, une équipe de gestionnaires SKOLAE Formation spécialisée vous accompagne dans le choix de vos formations et la gestion administrative.

[Nous contacter pour en savoir plus →](#)

Modalités 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*

Accessibilité aux personnes en situation de handicap

Détails de la session

Du 5 janvier 2027 au 6 janvier 2027 (2 jours / 14 heures)

À distance

Du 5 janvier 2027 au 6 janvier 2027 **À distance**

- 5 janvier 2027 9h00 – 16h30
- 6 janvier 2027 9h00 – 16h30