

Sécurité physique et logique des composants

5 jours (35 heures)

Expertise

Présentiel ou classe à distance

à partir de

5 625 € HT par personne (TVA en vigueur) **Repas inclus en présentiel**

Contenu mis à jour le 25/09/2026. Document téléchargé le 02/10/2026.

Objectifs

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

- Reconnaître les menaces qui pèsent sur les implantations matérielles telles que les cartes à puce, microcontrôleurs, systèmes embarqués...
- Suivre l'état de l'art des protections et contre-mesures disponibles et connaître les outils pour évaluer leur efficacité.

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

À qui s'adresse cette formation ?

Spécialistes en électronique, en cryptographie, intégrateurs, architectes ou spécialistes d'une maîtrise d'ouvrage devant prendre en compte les questions de sécurité des implantations matérielles.

Prérequis

Connaître la cryptographie.

Programme

1 Pendant votre formation

Sécurité physique et logique des composants

Jour 1 – Introduction aux composants et sécurisation des interfaces

Matin

Types de composants et architecture matérielle

- Découverte des microcontrôleurs, FPGA, SoC et processeurs sécurisés (TPM, enclaves Intel SGX, RISC-V)
- Introduction à Secureboot et TEE
- Reconnaissance d'une cible hardware

Exemple de travaux pratiques (à titre indicatif)

- *Lecture et interprétation de datasheet*

Après-midi

Attaque sur les canaux de communications internes

- Présentation et attaque sur bus internes (SPI, I2C)

Exemple de travaux pratiques (à titre indicatif)

- *Utilisation et conception d'outils pour observer les bus de communications*

Jour 2 – Interagir avec le code

Matin

Introduction au ports de débogage

- Boundary scan et JTAG, les ports de débogages
- Présentation SWD et ICSP, des approches modernes ou propriétaires

Exemple de travaux pratiques (à titre indicatif)

- *Bruteforce PIN JTAG, extraction Firmware*

Après-midi

Analyse de code

- Présentation ASM pour ARM
- Rétro-conception avec Ghidra et SVDLoader

Exemple de travaux pratiques (à titre indicatif)

- *Ecriture d'un script simple en ASM*

Jour 3 – Analyse matérielle et applicative

Matin

Attaque micro-architecturale

- Analyse d'inférence de données, types d'attaques (analyse de consommation et d'émission électromagnétique)
- Vulnérabilités Spectre et Meltdown, introduction aux contre-mesures comme le partitionnement de cache

Exemple de travaux pratiques (à titre indicatif)

- *Simulation d'une attaque Spectre*

Après-midi

Attaques sur le code

- Analyse pratique de firmware
- Introduction aux vulnérabilités applicative

Exemple de travaux pratiques (à titre indicatif)

- *Exploitation d'un buffer overflow*

Jour 4 – Attaques par injection de faute

Matin

Mécanismes d'injection de faute

- Présentation des techniques de voltage glitching et laser fault injection

Exemple de travaux pratiques (à titre indicatif)

- *Simulation d'une injection de faute sur microcontrôleur*

Après-midi

Démonstration d'attaque par injection de faute

- Conception d'outils pour injection de faute

Jour 5 – Rétro-conception de cible hardware

Matin

Attaques invasives et certification matérielle

- Techniques de décapsulations
- Rétro conception de standards cell

Exemple de travaux pratiques (à titre indicatif)

- *Utilisation de libreCell et analyse de standard cell, comprendre un ordinateur 8 bit*

Après-midi

CTF

- Mise en situation sur une cible IOT complète

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 19 octobre 2026 au 23 octobre 2026 (5 jours / 35 heures)

Angers

Du 19 octobre 2026 au 23 octobre 2026

Angers

- 19 octobre 2026 9h00 – 15h00
- 20 octobre 2026 9h00 – 15h00
- 21 octobre 2026 9h00 – 15h00
- 22 octobre 2026 9h00 – 15h00
- 23 octobre 2026 9h00 – 15h00