

Mis à jour le 15/01/2026

S'inscrire

Formation Cybersécurité des systèmes embarqués

1 jour (7 heures)

Présentation

Le Cyber Resilience Act (CRA) impose désormais aux fabricants d'objets connectés de fournir une analyse de risques cybersécurité complète. L'analyse de risques n'est plus une simple formalité : c'est la pierre angulaire du Security by Design et une obligation légale pour le marquage CE.

Notre formation "Cybersécurité & Analyse de Risques Systèmes Embarqués" vous propose de découvrir la méthode de référence EBIOS RM (Risk Manager) et de l'adapter aux contraintes spécifiques du monde de l'embarqué (IoT, IIoT, OT). En une journée intensive, vous apprendrez à identifier vos "Biens Essentiels", à construire des scénarios d'attaques réalistes (incluant les attaques physiques et logiques) et à définir des mesures de sécurité proportionnées aux enjeux.

À l'issue de la formation, vous disposerez des clés méthodologiques pour initier une démarche de conformité CRA et dialoguer efficacement avec les experts sécurité ou l'ANSSI.

Cette formation privilégie une approche pragmatique : nous laissons de côté la théorie lourde pour nous concentrer sur la construction de scénarios concrets applicables à vos produits.

Objectifs

- Comprendre l'obligation d'évaluation des risques imposée par le CRA.
- S'approprier la démarche EBIOS RM et ses 5 ateliers clés.
- Adapter l'analyse de risques aux contraintes de l'embarqué (Accès physique, Safety).
- Savoir construire des Scénarios Opérationnels crédibles (Attaques JTAG, Réseau, Supply Chain).
- Définir un plan de traitement du risque pour la documentation technique.

Public visé

- Architectes systèmes embarqués & IoT
- Chefs de produits (Product Owners)
- Responsables Qualité / Sûreté de fonctionnement
- CISO / RSSI souhaitant appréhender le périmètre industriel

Pré-requis

- Connaissance générale des systèmes informatiques ou électroniques.
- Aucune maîtrise préalable de la méthode EBIOS n'est requise.

Matériel

- Ordinateur portable pour la consultation des supports et la réalisation des ateliers.

Programme de notre Formation Cybersécurité des systèmes embarqués

[Matin]

Contexte Réglementaire et Cadrage (Ateliers 1 & 2)

- Le Cyber Resilience Act (CRA) : pourquoi l'analyse de risque devient obligatoire ?
- Survol de la méthode EBIOS RM : principes et itérations
- Atelier 1 (Le Socle) : Identifier les biens supports spécifiques (Firmware, Clés, Bus de communication)
- Définir le périmètre et les événements redoutés (Impact Sûreté vs Vie Privée)
- Atelier 2 (Sources de risques) : Qui sont les attaquants ? (Cybercriminels, Concurrents, Étatiques)
- Cas pratique fil rouge : Cadrage de l'analyse pour un objet connecté industriel critique.

[Après-midi]

Scénarios d'Attaques et Traitement (Ateliers 3, 4 & 5)

- Atelier 3 (Scénarios Stratégiques) : Risques liés à l'écosystème numérique (Cloud, Supply Chain, Mises à jour OTA)
- Atelier 4 (Scénarios Opérationnels) : Le cœur technique
- Modéliser des chemins d'attaque : Accès physique (JTAG/UART), Réseau (Man-in-the-Middle), Logique (Buffer Overflow)
- Utilisation des bases de connaissances (ATT&CK for ICS, CAPEC)
- Atelier 5 (Traitement) : Choisir les mesures de sécurité (Secure Boot, Chiffrement, Authentification)
- Validation du risque résiduel et intégration au Dossier Technique CRA
- Cas pratique fil rouge : Rédaction complète d'un scénario d'attaque technique et choix des mesures de protection.

Sociétés concernées

Cette formation s'adresse à la fois aux particuliers ainsi qu'aux entreprises, petites ou grandes, souhaitant former ses équipes à une nouvelle technologie informatique avancée ou bien à acquérir des connaissances métiers spécifiques ou des méthodes modernes.

Positionnement à l'entrée en formation

Le positionnement à l'entrée en formation respecte les critères qualité Qualiopi. Dès son inscription définitive, l'apprenant reçoit un questionnaire d'auto-évaluation nous permettant d'apprécier son niveau estimé sur différents types de technologies, ses attentes et objectifs personnels quant à la formation à venir, dans les limites imposées par le format sélectionné. Ce questionnaire nous permet également d'anticiper certaines difficultés de connexion ou de sécurité interne en entreprise (intraentreprise ou classe virtuelle) qui pourraient être problématiques pour le suivi et le bon déroulement de la session de formation.

Méthodes pédagogiques

Stage Pratique : 60% Pratique, 40% Théorie. Support de la formation distribué au format numérique à tous les participants.

Organisation

Le cours alterne les apports théoriques du formateur soutenus par des exemples et des séances de réflexions, et de travail en groupe.

Validation

À la fin de la session, un questionnaire à choix multiples permet de vérifier l'acquisition correcte des compétences.

Sanction

Une attestation sera remise à chaque stagiaire qui aura suivi la totalité de la formation.