

Nouveau Sessions garanties disponibles

Formation Directive RED et Cyber Resilience Act : conformité et cybersécurité des systèmes embarqués

Réf. SF34394

Anticipez les obligations réglementaires et renforcez la cybersécurité de vos systèmes embarqués dès leur conception !

2 j Durée	1 800 € HT Inter / participant	4 000 € HT Intra (≤12 pers.)	28 Sessions à venir
--------------	-----------------------------------	---------------------------------	------------------------

Objectifs pédagogiques

- ✓ Identifier les obligations réglementaires issues de la Directive RED en matière de cybersécurité.
- ✓ Comprendre les principales exigences de la norme EN 18031 pour les objets connectés.
- ✓ Appréhender les impacts du Cyber Resilience Act sur la chaîne de fabrication et de distribution.
- ✓ Définir une stratégie de conformité réglementaire adaptée à leurs produits.
- ✓ Intégrer les principes du Secure by Design dans leur processus de développement.
- ✓ Réaliser une évaluation rapide d'un firmware embarqué selon des critères de sécurité.
- ✓ Élaborer un plan d'action cybersécurité tenant compte des obligations à venir.

Public visé & prérequis

Public visé Chefs de projet, Responsables qualité

Prérequis Connaissances de base en architecture de systèmes embarqués et/ou IoT. Une sensibilité aux enjeux de cybersécurité est un plus.

Programme détaillé

Accueil et introduction

Présentation des objectifs de la journée
Tour de table des participants
Enjeux actuels de la cybersécurité dans les systèmes embarqués

Directive RED (Radio Equipment Directive) – Focus cybersécurité

Présentation générale de la Directive RED (2014/53/EU)
Focus sur l'article 3(3)(d), (e), (f) :
Protection des données personnelles et de la vie privée
Protection contre la fraude
Protection du réseau et de son intégrité
Impact de la mise en application des exigences cyber (obligatoires depuis août 2025)
Exemples de types d'équipements concernés
Atelier : Étude de cas sur un produit connecté – quelles exigences RED appliquer ?

Norme EN 18031 – Sécurité pour l'IoT

Contexte et statut de la norme EN 18031
Structure et exigences principales :
Contrôle d'accès, authentification et gestion des mots de passe
Mise à jour logicielle sécurisée
Communications sécurisées
Réduction de la surface d'attaque
Journalisation et surveillance

Cyber Resilience Act (CRA) – Comprendre et anticiper

Présentation du règlement CRA et son calendrier de mise en œuvre
Obligations applicables aux fabricants, importateurs et distributeurs
Champ d'application et catégorisation des produits (classe I, II, produits critiques)
Exigences techniques et organisationnelles
Aspects légaux et sanctions
Discussion : Comment aligner sa roadmap produit avec les échéances du CRA ?

Stratégie de conformité intégrée

Mettre en place un processus Secure by Design
Outils et méthodes d'analyse de risque
Gestion des vulnérabilités (SBOM, CVE, VEX)
Bonnes pratiques documentaires
Atelier : Créer un plan d'action cybersécurité pour un produit embarqué

Retours d'expérience – Conclusion

Questions ouvertes des participants
Ressources à suivre (ANSSI, ENISA, CENELEC, etc.)

Prochaines sessions

DATE	LIEU	STATUT
04/03/2027	Grenoble	Sur confirmation
04/03/2027	Paris	Sur confirmation
04/03/2027	Toulouse	Sur confirmation
04/03/2027	à distance	Sur confirmation
04/03/2027	Lyon	Sur confirmation
22/04/2027	Paris	Sur confirmation

Pourquoi choisir Sparks Formation ?

20 ans d'expertise IT, des formateurs experts et des sessions garanties contre l'annulation.

20 ans
d'expertise

1 068+
formations

11 178
apprenants formés/an

+67
Net Promoter Score

Avis des participants

4,9/5 — 735 avis

Berenice P. — formatrice agréable à l'écoute bonne pédagogie j'ai beaucoup apprécié nos échanges

Anne-Lise C. — Très bonne adaptation du formateur au public et au niveau d'attente.

Votre formateur

Michael G. — Formateur Cybersécurité

Michael intervient sur des formations portant sur la sécurité défensive et l'architecture de sécurité (Blue Team). Les sujets abordés incluent notamment la cybersécurité. Son activité de formation remonte à 2023.

Ils nous font confiance

Cette année notre filière Systèmes Embarqués & IoT a accompagné plus de 23 entreprises dont :

ACTIA AUTOMOTIVE AMCS TECHNOLOGIES ANSYS FRANCE SAS ASTEK FRANCE ERAS EXAIL AEROSPACE FLANDRIN IT GERFLOR PROVENCE
SNC KNAUF INDUSTRIES GESTION LABORATOIRES CLARINS +13 autres

Financement & certifications

Cette formation est éligible aux financements OPCO et FNE-Formation. Nos équipes vous accompagnent dans le montage de votre dossier.



Réservez votre place dès maintenant

20 ans d'expertise · 1 000+ formations · NPS +67 · réponse sous 24h ouvrées

0 805 950 800

demande@sparks-formation.com