Formation Cyber Resilience Act pour les équipes produit

Les obligations de signalement du Cyber Resilience Act s'appliquent depuis septembre 2026, et toutes les autres à partir de décembre 2027. Ce que les produits et les organisations doivent fournir, en une journée.

1 jour	Tous niveaux, sans programmation	Sur site ou à distance	Français ou anglais
Durée	Niveau	Format	Langue (supports en anglais)

Présentation

Cette formation d'une journée explique ce que le Cyber Resilience Act européen exige des fabricants de produits embarqués connectés, et ce que cela implique pour le produit comme pour l'organisation. Le signalement des vulnérabilités activement exploitées s'applique depuis le 11 septembre 2026, et toutes les autres obligations s'appliquent aux produits mis sur le marché à partir du 11 décembre 2027.

Objectifs

À la fin de la formation, les participants savent :

- savoir si un produit relève du CRA, et dans quelle catégorie ;
- expliquer les exigences essentielles et l'évaluation de la conformité ;
- organiser la gestion des vulnérabilités et le signalement aux autorités ;
- comprendre ce qu'est un SBOM et comment il est produit ;
- planifier le travail technique et organisationnel avant le 11 décembre 2027.

Public

Chefs de produit, responsables qualité et conformité, et responsables techniques d'entreprises qui vendent dans l'Union européenne des produits comportant des éléments numériques.

Prérequis

Aucun. La formation ne comporte pas de programmation.

Programme

La journée va du règlement jusqu'aux processus et aux mesures techniques qu'il implique.

Jour 1

- Pourquoi les produits connectés sont réglementés, et comment fonctionne le droit européen des produits
- Le CRA : périmètre, rôles et catégories de produits
- Les exigences essentielles et l'évaluation de la conformité
- Le signalement aux autorités et les échéances du CRA
- Le SBOM : ce que c'est et comment il est produit
- La gestion des vulnérabilités : CVE, triage, divulgation et équipe de sécurité produit
- Ce que les exigences impliquent pour le produit : secure boot, mises à jour sécurisées, durcissement et durée de support

Format

La formation est un séminaire sans travaux pratiques, donné sur site ou à distance, en français ou en anglais, avec des supports en anglais.

Qui anime cette formation

La formation est conçue et animée par le fondateur de LABCSMART, ingénieur Linux embarqué et noyau Linux avec plus de onze ans d'expérience industrielle. Il contribue au noyau Linux en amont pour les SoC Renesas RZ, dans les sous-systèmes PCIe, audio, Ethernet, thermique, DMA et horloges, et a écrit deux livres publiés chez Packt, *Linux Device Driver Development, Second Edition* (2022) et *Mastering Linux Device Driver Development* (2021), présentés sur notre page de publications.

Organiser une session pour votre équipe. Chaque formation est composée de modules indépendants. Une équipe peut retirer les modules dont elle n'a pas besoin et en ajouter d'autres à la place, et nous construisons aussi des formations sur mesure autour d'un SoC, d'une carte ou d'un projet. Contact : contact@labcsmart.com, https://labcsmart.com/fr/contact/. Page de la formation : https://labcsmart.com/fr/formations/formation-cyber-resilience-act/