PROGRAMME DE FORMATION

-

Cyber Resilience Act (CRA) - Niveau 1

Comprendre en pratique les exigences du CRA européen

Version	V1.0
Date	Mars 2026
Organisme	DVID SAS
Modalité	100% FOAD asynchrone (e-learning autonome)
Contact	contact@dvid.eu

Table des matières

1 Informations générales

Intitulé	CRA — Niveau 1 : Comprendre en pratique le Cyber Resilience Act
Référentiel couvert	Règlement (UE) 2024/2847 — Cyber Resilience Act (Annexe I, Parties I et II)
Modalité	100% FOAD asynchrone — e-learning autonome (experience.dvid.eu)
Durée estimée	12 heures en autonomie
Délai d'accès	Sous 48h après validation de l'inscription
Tarif	3 000 € HT par apprenant (licence annuelle nominative)
Contact	contact@dvid.eu
Référent pédagogique	Arnaud COURTY
Référent handicap	Lionel CAUBET
NDA	75170346017
Catégorie Qualiopi	Actions de Formation (L. 6313-1, 1°)

2 Analyse du besoin

Avant toute inscription, un questionnaire d'analyse du besoin est transmis au bénéficiaire et/ou à l'entreprise commanditaire. Ce questionnaire permet d'identifier le contexte réglementaire de l'entreprise (produits concernés par le CRA, échéances de mise en conformité, niveau de maturité cybersécurité) et l'adéquation de la formation avec le projet du bénéficiaire.

Sur la base de cette analyse, le référent pédagogique valide l'inscription ou oriente vers un parcours plus adapté.

3 Objectifs opérationnels / Compétences acquises

À l'issue de la formation, l'apprenant sera capable de :

- **Analyser** les exigences essentielles de cybersécurité du CRA et **évaluer leur impact** sur un produit connecté.
- **Identifier** les obligations de gestion des vulnérabilités imposées aux fabricants.
- **Évaluer** la conformité d'un produit vis-à-vis de chaque exigence CRA.
- **Appliquer** les exigences CRA dans des démonstrations contrôlées sur la plateforme DVID.
- **Construire** un plan d'action de mise en conformité CRA pour un produit IoT.

4 Positionnement à l'entrée

Un test automatisé (10 questions) évalue :

- connaissances cybersécurité,
- compréhension IoT,
- maturité réglementaire.

5 Public visé et prérequis

5.1 Public visé

- Responsables conformité / réglementaire produit
- Chefs de projet IoT / embarqué
- RSSI et responsables sécurité produit
- Ingénieurs qualité et certification

5.2 Prérequis

- Culture générale en cybersécurité (pas d'expertise technique requise)
- Connaissance de base des produits connectés / IoT

6 Contenu pédagogique

Le parcours couvre les 22 exigences de l'Annexe I du CRA, réparties en deux parties :

Partie I — Exigences essentielles de cybersécurité (14 modules)

1. CRA (ANNEXE I) : 1 — Un niveau de cybersécurité approprié aux risques
2. CRA (ANNEXE I) : 2a — Aucune vulnérabilité exploitable connue lors de la mise sur le marché
3. CRA (ANNEXE I) : 2b — Configuration de sécurité par défaut + réinitialisation
4. CRA (ANNEXE I) : 2c — Mises à jour de sécurité et correction des vulnérabilités
5. CRA (ANNEXE I) : 2d — Protection contre les accès non autorisés
6. CRA (ANNEXE I) : 2e — Protection de la confidentialité des données
7. CRA (ANNEXE I) : 2f — Protection de l'intégrité
8. CRA (ANNEXE I) : 2g — Minimisation des données
9. CRA (ANNEXE I) : 2h — Protection de la disponibilité des fonctions essentielles
10. CRA (ANNEXE I) : 2i — Réduction des répercussions sur la disponibilité
11. CRA (ANNEXE I) : 2j — Limitation des surfaces d'attaque
12. CRA (ANNEXE I) : 2k — Réduction des répercussions d'un incident
13. CRA (ANNEXE I) : 2l — Enregistrement et surveillance des activités internes
14. CRA (ANNEXE I) : 2m — Suppression et transfert sécurisés des données

Partie II — Gestion des vulnérabilités (8 modules)

15. CRA (ANNEXE I) : II 1 — Recensement des vulnérabilités et composants (SBOM)
16. CRA (ANNEXE I) : II 2 — Gestion et correction rapide des vulnérabilités
17. CRA (ANNEXE I) : II 3 — Tests et examens de sécurité réguliers
18. CRA (ANNEXE I) : II 4 — Communication sur les vulnérabilités corrigées
19. CRA (ANNEXE I) : II 5 — Politique de divulgation coordonnée (CVD)
20. CRA (ANNEXE I) : II 6 — Partage d'informations sur les vulnérabilités potentielles
21. CRA (ANNEXE I) : II 7 — Distribution sécurisée des mises à jour + automatisation
22. CRA (ANNEXE I) : II 8 — Diffusion rapide et gratuite des correctifs de sécurité

7 Moyens pédagogiques

- Plateforme SaaS DVID (experience.dvid.eu) :
  - modules théoriques
  - mises en situation pratiques
- Chaque module illustre l'exigence CRA par une démonstration concrète sur la plateforme
- Documentation de référence : texte officiel CRA annoté
- Ressources téléchargeables

8 Modalités d'évaluation

- Attestation de fin de formation délivrée automatiquement par la plateforme
- Cas pratique final :
  - évaluation de la conformité CRA d'un dispositif IoT fictif — l'apprenant doit identifier les exigences non respectées et produire un plan d'action de mise en conformité.
  - Seuil de réussite : 70% au QCM + validation du cas pratique final.

9 Suivi et prévention des abandons

Suivi automatisé de la progression

Alertes d'inactivité à 7 / 14 / 21 jours

Relance par le référent pédagogique

Assistance technique par email (contact@dvid.eu) et Discord (délai < 48h ouvrées)

10 Accessibilité

Adaptations possibles : temps majoré, supports alternatifs, assistance personnalisée.
Référent handicap : contact@dvid.eu

11 Indicateurs de résultats

Collecte trimestrielle via la plateforme (complétion, satisfaction, réussite).
Publication sur dvid.eu dès la première cohorte terminée.