

## ► QU'EST-CE QUE C'EST ?

Une approche étape par étape du pentesting des produits comportant des éléments numériques (PDE), conforme à la loi sur la cyber-résilience (CRA).

## ► À QUI S'ADRESSE-T-IL ?

Petites et moyennes entreprises (PME) fabriquant des produits comportant des éléments numériques.

# MÉTHODOLOGIE DE TEST D'INTRUSION CONFORME AUX NORMES CRA



## CONFIRMATE

Le projet financé dans le cadre de la convention de subvention n° 101190193 bénéficie du soutien du Centre européen de compétences en matière de cybersécurité.



Co-funded by  
the European Union



► POINTS D'ATTENTION !!!

La CRA n'exige pas de tests de pénétration en soi, mais impose des « examens et tests efficaces et réguliers » de la sécurité des produits. Les tests peuvent renforcer les preuves à l'appui d'une déclaration de conformité aux exigences essentielles de la CRA en matière de cybersécurité.

## ► TOUT EST PRÊT ?

Non, il est basé sur les normes industrielles : OSSTMM3, ETSI EN 303 645 et TS 103 701, OWASP Testing Guide, PTES et NIST SP 800-115.

## ► ÉTAPE PAR ÉTAPE



### 1. Pré-engagement et planification

Définir la portée, les exigences de l'ARC, les environnements de test, les autorisations et harmoniser les parties prenantes.

**Résultat :** plan de test, documents juridiques, évaluation initiale des risques.



### 2. Collecte de renseignements et reconnaissance

Cartographier la surface d'attaque, collecter des renseignements OSINT et définir des scénarios d'attaque réalistes.

**Résultat :** profil de l'adversaire, informations initiales sur les vulnérabilités.



### 3. Exécution et exploitation

Test des vulnérabilités à l'aide d'outils et de vérifications manuelles, simulation d'attaques en laboratoire.

**Résultat :** rapport complet sur les vulnérabilités.



### 4. Analyse d'impact et rapports

Évaluer la gravité, établir une correspondance avec la CRA, définir les mesures correctives.

**Résultat :** conclusions établies en fonction de la CRA, stratégie corrective.



### 5. Après l'engagement et suivi

Vérifier les corrections, refaire les tests, recueillir les commentaires et préparer les divulgations si nécessaire.

**Résultat :** rapport final de test d'intrusion pour la conformité CRA.

## À PROPOS DE CONFIRIMATE

Rationalisez et automatisez la conformité à la loi sur la cyber-résilience (CRA). Grâce au développement d'outils open source, de méthodologies standardisées et de ressources de formation, nous donnons aux PME les moyens de répondre facilement et efficacement aux exigences en matière de cybersécurité. Notre objectif est de créer un écosystème dynamique où les parties prenantes peuvent échanger leurs meilleures pratiques, se tenir informées des évolutions réglementaires et contribuer à l'avancement de produits numériques sécurisés.

### VOIR PLUS



[CONFIRIMATE](#)



[www.confirmate-project.eu](http://www.confirmate-project.eu)



[confirmate.project@gmail.com](mailto:confirmate.project@gmail.com)



[cyen-cybersecurity](#)