CONFIRMATE

Évaluation de la Conformité, métriques et automatisation de la conformité pour la loi sur la cyber-résilience

Méthodologie des tests d'intrusion

Date de sortie : 2025-08-05

Statut : Révisé

Le projet financé dans le cadre de la convention de subvention **n° 101190193** est soutenu par le Centre européen de compétences en matière de cybersécurité. Les opinions exprimées sont toutefois celles des auteurs et ne reflètent pas nécessairement celles de l'Union européenne ou du Centre européen de compétences en matière de cybersécurité. Ni l'Union européenne ni l'autorité qui octroie la subvention ne peuvent en être tenues responsables.

Version: 0.3

Co-funded by the European Union
ECCC EUROPEAN CYBERSECURITY COMPETENCE CENTRE

Liste des modifications

Version	Date	Description	Auteur(s)
0.1	21/03/25	Première ébauche de la méthodologie partagée avec les partenaires pour examen et commentaires	Cyen
0.2	08/04/25	Révisions intégrées sur la base des commentaires reçus des partenaires.	Cyen
0.3	05/08/25	Révisions intégrées sur la base des commentaires reçus de nos pairs.	Cyen

Nous remercions sincèrement les pairs évaluateurs, en particulier Krasen Parvanov (QRTECH), Stijn Horemans (Refracted), Ayman Khalil et Romain Muguet (Red Alert Labs), Peter Kuzmin (Kikimora) et Dominik Holzapfel (Nviso), pour leurs commentaires critiques et leurs remarques pertinentes, qui ont considérablement contribué à améliorer la précision et la clarté de cette méthodologie.

Méthodologie de test de pénétration de conformité CRA pour les PME

Contenu

1. Références

- Règlement (UE) 2024/2847 du Parlement européen et du Conseil du 23 octobre 2024 relatif aux exigences horizontales en matière de cybersécurité applicables aux produits comportant des éléments numériques et modifiant les règlements (UE) n° 168/2013 et (UE) n° 2019/1020 et la directive (UE) 2020/1828 (loi sur la cyberrésilience), disponible ici : https://eur-lex.europa.eu/eli/reg/2024/2847/oj/eng
- Institut pour la sécurité et les méthodologies ouvertes (ISECOM). (2010). Manuel de méthodologie de test de sécurité open source (OSSTMM) version 3.0, disponible ici : https://www.isecom.org/OSSTMM.3.pdf
- Norme d'exécution des tests d'intrusion (PTES) Organisation PTES. (n.d.). Norme d'exécution des tests d'intrusion (PTES), disponible ici : https://www.pentest-standard.org/index.php/Main_Page
- Scarfone, K., & Mell, P. (2008). Technical Guide to Information Security Testing and Assessment (NIST SP 800-115), disponible ici : https://csrc.nist.gov/pubs/sp/800/115/final
- Fondation OWASP. (n.d.). Guide de test de sécurité Web OWASP (WSTG), disponible ici : https://owasp.org/www-project-web-security-testing-guide/
- MITRE Corporation. (n.d.). Cadre MITRE ATT&CK®, disponible ici : https://attack.mitre.org/
- Open Information Systems Security Group (OISSG). (2005). Information Systems Security Assessment Framework (ISSAF) Draft 0.2, disponible ici : https://untrustednetwork.net/files/issaf0.2.1.pdf
- Threat Intelligence-Based Ethical Red Teaming (TIBER-EU) Banque centrale européenne. (2023). Cadre TIBER-EU : Threat Intelligence-Based Ethical Red Teaming, disponible ici : https://www.ecb.europa.eu/pub/pdf/other/ecb.tiber_eu_framework.en.pdf
- ETSI TS 103 701 V1.1.1 (2021-08) : Cybersécurité pour l'Internet des objets grand public : évaluation de la conformité aux exigences de base. Available here: https://www.etsi.org/deliver/etsi_ts/103700_103799/103701/01.01.01_60/ts_103701v010101p.pdf

2. Glossaire : Acronymes, Termes et Abréviations

Acronymes

OSSTMM:	**Manuel de méthodologie de test de sécurité open source**
OWASP:	**Projet de sécurité des applications Web ouvertes**
PTES:	**Norme d'exécution des tests d'intrusion**
NIST:	**Institut national des normes et technologies**
SIEM:	**Gestion des informations et des événements de sécurité**
IAM:	**Gestion des identités et des accès (déduite du contexte)**
API:	**Interface de programmation d'application**
VPN:	**Réseau privé virtuel**
SSO:	**Authentification unique**
IoT:	**Internet des objets**
GDPR:	**Règlement général sur la protection des données**
ISO:	**Organisation internationale de normalisation**
IEC:	**Commission électrotechnique internationale**
CIS:	**Centre pour la sécurité Internet**
CMMC:	**Certification du modèle de maturité en matière de cybersécurité**
PSD2:	**Directive révisée sur les services de paiement**
SWIFT CSP:	**Société pour la sécurité des communications interbancaires mondiales Programme de sécurité client**

Termes

Test d'intrusion (ou test d'infiltration):	Exercice de sécurité au cours duquel un expert en cybersécurité tente de trouver et d'exploiter les vulnérabilités d'un produit et de son environnement, y compris le matériel, les logiciels, les interfaces et les surfaces d'interaction avec l'utilisateur.
Vulnérabilité:	Une faiblesse ou une faille dans un système, une application ou un réseau qui peut être exploitée pour compromettre la sécurité.

Exploit:	Un morceau de code, une technique ou un processus qui exploite une vulnérabilité pour provoquer un comportement indésirable dans un système.
Acteur malveillant:	Une personne ou un groupe qui représente un risque potentiel pour la cybersécurité d'une organisation peut être un pirate informatique, un employé ou un concurrent.
Évaluation des risques:	Processus consistant à identifier les risques susceptibles d'avoir un impact négatif sur la capacité d'une organisation à mener ses activités.
Audit de sécurité:	Évaluation systématique du niveau de sécurité d'un produit comportant des éléments numériques, mesurant sa conformité avec des exigences techniques et réglementaires prédéfinies, telles que la CRA.
Plan d'intervention en cas d'incident:	Ensemble d'instructions destinées à aider les organisations à détecter les incidents liés à la sécurité des réseaux informatiques, à y répondre et à s'en remettre.
Cryptage:	Méthode consistant à convertir des informations en un code secret qui en cache le véritable sens.
Fabricant:	Une personne physique ou morale qui développe ou fabrique des produits comportant des éléments numériques ou qui fait concevoir, développer ou fabriquer des produits comportant des éléments numériques, et qui les commercialise sous son nom ou sa marque, que ce soit à titre onéreux, à des fins de monétisation ou gratuitement.
Authentification multifactorielle (MFA):	Méthode d'authentification qui exige que l'utilisateur fournisse au moins deux facteurs de vérification pour accéder à une ressource, telle qu'une application, un compte en ligne ou un VPN.
Ingénierie Sociale:	La tactique consistant à manipuler, influencer ou tromper une victime afin de prendre le contrôle d'un système informatique ou de voler des informations personnelles et financières.
Tactiques, techniques et procédures (TTP) :	Décrit le comportement d'un acteur malveillant et un cadre structuré pour l'exécution d'une cyberattaque.

Triade CIA (confidentialité, intégrité, disponibilité) :	Modèle de sécurité de l'information conçu pour protéger les informations sensibles contre les violations de données.
Produit avec éléments numériques (PDE):	Produit qui contient ou est interconnecté avec un logiciel ou un micrologiciel et qui est capable de collecter, transmettre ou traiter des données. Les PDE comprennent à la fois les dispositifs physiques et les produits définis par logiciel qui sont mis sur le marché ou mis en service.

3. Introduction

3.1 But et objectifs

Ce document décrit comment gérer et réaliser des tests d'intrusion sur des produits comportant des éléments numériques (PDEs) afin de vérifier leur conformité avec la loi sur la cyber-résilience (CRA). Cette méthodologie comble une lacune pratique en définissant un processus de test d'intrusion conforme à la CRA et adapté au niveau d'exposition au risque des produits, en mettant l'accent sur la manière dont ces tests permettent d'étayer une déclaration de conformité. Bien que la CRA ne fasse pas référence aux tests d'intrusion et ne les rende pas obligatoires, ceux-ci restent l'une des techniques les plus efficaces pour déterminer dans quelle mesure les vulnérabilités potentielles peuvent être exploitées par un attaquant. Par conséquent, un exercice de test d'intrusion réussi peut renforcer les preuves à l'appui d'une déclaration de conformité.

Tout au long de l'élaboration de cette méthodologie, une attention particulière a été accordée à un ensemble de produits identifiés à l'annexe A. Ces produits couvrent différents niveaux de criticité définis dans la loi sur la cyberrésilience (CRA). Ils ont été sélectionnés afin de garantir que la méthodologie soit applicable et pratique dans différents cas d'utilisation, et ils constituent un point positif pour tous les outils Confirmate.

L'approche est basée sur une méthodologie reconnue (OSSTMM3), qui a été développée dans le cadre d'une communauté ouverte et soumise à un examen par des pairs et interdisciplinaire. L'OSSTMM3 offre une approche structurée pour identifier les vulnérabilités et les mettre en correspondance avec des cyberattaques possibles, ce qui permet une évaluation plus précise des risques potentiels pour la sécurité.

Les objectifs de l'approche proposée sont les suivants :

- Fournir une méthode structurée pour tester la pénétration des produits comportant des éléments numériques, tout en offrant une certaine souplesse dans les techniques utilisées.
- Définir un ensemble standard de résultats pouvant être utilisés pour étayer la déclaration de conformité du fabricant à la CRA.
- Illustrer l'utilisation de l'approche en expliquant comment elle pourrait être appliquée à plusieurs produits issus des produits importants (classe I et classe II) et des produits critiques tels que définis par la CRA.
- Cette méthodologie ne couvre pas les évaluations informatiques génériques des entreprises ni les tests d'intrusion d'applications web autonomes qui ne constituent pas un PDE tel que défini par la CRA. Les actifs exclusivement web sont souvent couverts par les méthodologies OWASP, mais ne correspondent pas au champ d'application réglementaire centré sur les produits requis ici.

3.2 Public Cible

Le public cible de ce document est constitué des fabricants de produits comportant des éléments numériques tels que définis par la CRA.

4. Portée

4.1 Applicabilité aux PME

L'approche des tests d'intrusion proposée dans ce document a été conçue pour être utilisée par les petites et moyennes entreprises (PME). En particulier, tout a été mis en œuvre pour que cette approche reste simple et facile à comprendre et pour réduire au minimum le jargon inutile, afin que les méthodes proposées soient à la portée des petites entreprises.

Cette méthodologie est applicable aux produits numériques autonomes et intégrés relevant du champ d'application de la CRA, y compris les appareils grand public, les contrôleurs industriels, les passerelles intelligentes et les composants critiques pour la sécurité. Bien qu'elle soit principalement conçue pour les tests avant la mise sur le marché et pendant l'exploitation, elle peut également être appliquée à des phases de développement antérieures afin d'identifier les faiblesses en matière de sécurité avant le déploiement sur le marché.

4.2 Limites et restrictions

Ce document décrit comment gérer et exécuter des tests d'intrusion dans le but d'étayer une déclaration de conformité aux exigences de l'ARC. Il ne traite pas des stratégies de remédiation, des contrôles d'atténuation ou des mesures de sécurité correctives qui pourraient s'avérer nécessaires à la suite de la découverte de faiblesses lors des tests.

De plus, contrairement aux tests d'intrusion classiques, qui ciblent un environnement, les tests décrits dans le présent document ciblent un produit. Cela dit, cela n'a de sens que si le produit est hébergé dans un environnement approprié. En ce sens, l'environnement utilisé pour héberger un produit tout au long des tests jouera un rôle dans la détermination de la validité des résultats finaux. Dans ce contexte, les tests d'intrusion se déroulent généralement dans un laboratoire contrôlé. L'équipe chargée des tests doit soit fournir, soit approuver le banc d'essai, en s'assurant qu'il reflète des conditions d'exploitation réalistes sans affaiblir les hypothèses de sécurité.

4.3 Hypothèses et contraintes

Les principales hypothèses retenues dans l'approche présentée sont les suivantes :

Le produit sera testé dans un « environnement de laboratoire » plutôt que sur le terrain.

L'environnement dans lequel le produit sera testé sera très proche de l'environnement cible (c'est-à-dire l'environnement dans lequel le produit sera utilisé).

Bien que des exemples de scénarios de test soient proposés dans cette approche, il est supposé que les fabricants adapteront ces scénarios afin de refléter la nature du produit qu'ils testent.

Les contraintes relatives au processus seront identifiées dans le cadre des activités de la phase 1. La principale contrainte est que les tests doivent être conçus de manière à ne pas avoir d'impact négatif sur les activités de l'entité chargée des tests.

5. Normes industrielles pour les essais

5.1 ETSI EN 303 645

La norme est accompagnée d'une spécification d'essai (TS 103 701) et d'un guide de mise en œuvre (TR 103 621)
https://www.etsi.org/deliver/etsi_ts/103700_103799/103701/01.01.01_60/ts_103701v010101p.pdf

La norme ETSI TS 103 701 fournit des groupes de tests structurés et des évaluations de conformité adaptés aux appareils IoT grand public. Les cas de test couvrent les exigences fonctionnelles, de résilience, d'interface et de protection des données. Dans cette méthodologie, les groupes de tests pertinents de la norme TS 103 701 sont appliqués de manière sélective aux catégories de produits décrites à l'annexe A.

La norme ETSI EN 303 645 est la norme européenne de base en matière de cybersécurité pour les appareils IoT grand public. Elle établit des dispositions visant à lutter contre les vecteurs d'attaque les plus courants et les plus impactants. Cette norme vise à garantir un niveau de sécurité minimum et sert de référence pour les réglementations nationales et les évaluations de conformité.

5.2 OSSTMM3

Un audit OSSTMM est une mesure précise de la sécurité au niveau opérationnel, sans hypothèses ni preuves anecdotiques. En tant que méthodologie, il est conçu pour être cohérent et reproductible. En tant que projet open source, il permet à tout testeur de sécurité de contribuer à l'amélioration des tests de sécurité afin de les rendre plus précis, plus exploitables et plus efficaces. De plus, il permet la libre diffusion des informations et de la propriété intellectuelle.

Par rapport aux normes basées sur la conformité, OSSTMM 3 se concentre sur la validation de la sécurité dans le monde réel dans plusieurs domaines, notamment :

- **Réseaux de données:** routeurs, pare-feu, SIEM, compteurs intelligents et appareils IoT.
- **Télécommunications:** sécurité de l'accès à distance, configurations VPN.
- **Sécurité sans fil:** vulnérabilités Wi-Fi, normes de cryptage**.**

Il a également introduit les valeurs d'évaluation des risques (RAV), qui permettent aux équipes de sécurité de quantifier l'exposition aux risques et de suivre les vulnérabilités au fil du temps, améliorant ainsi la gestion des risques et la prise de décision.

5.3 Guide de test OWASP

Le guide de test OWASP est développé dans le cadre du projet de test OWASP de l'Open Web Application Security Project (OWASP). Il ne s'agit pas d'une méthodologie complète couvrant un test d'intrusion complet, mais uniquement des phases essentielles du test de sécurité des applications web.

Le guide fournit une analyse détaillée de l'évaluation de la sécurité des applications Web ainsi que de leur pile de déploiement, y compris la configuration du serveur Web. Il suit une approche de test d'intrusion de type « boîte noire » et couvre de manière exhaustive le « quoi » et le « quand ». Il contient également quelques conseils sur le « comment », principalement sous la forme d'une liste des outils pouvant être utilisés à chaque étape ou tâche.

5.4 PTES

La norme PTES (Penetration Testing Execution Standard) est la méthodologie de test d'intrusion la plus récente à ce jour. Elle a été développée par une équipe de professionnels de la sécurité de l'information dans le but de répondre au besoin d'une norme complète et actualisée en matière de tests d'intrusion.

En plus de guider les professionnels de la sécurité, elle vise également à informer les entreprises sur ce qu'elles peuvent attendre d'un test d'intrusion et à les aider à définir la portée et à négocier des projets fructueux. Elle couvre le « quoi » et le « quand », mais va beaucoup plus loin dans le « comment ».

La PTES se compose de deux parties principales qui se complètent. Les lignes directrices Pentest décrivent les principales sections et étapes d'un test d'intrusion, tandis que les lignes directrices techniques traitent des outils et techniques spécifiques à utiliser à chaque étape.

5.5 NIST SP 800-15

La norme NIST 800-115, intitulée « Guide technique pour les tests et l'évaluation de la sécurité de l'information » (Guide technique pour les tests et l'évaluation de la sécurité de l'information), est une publication élaborée afin de fournir des lignes directrices et des recommandations pour la réalisation d'évaluations de la sécurité de l'information visant à évaluer le niveau de sécurité des systèmes et des réseaux d'information.

Il vise à aider les organisations à comprendre les différents types d'évaluations de sécurité, à sélectionner les techniques d'évaluation appropriées et à concevoir des programmes d'évaluation complets. Ces lignes directrices peuvent être appliquées à de nombreuses organisations, notamment les agences fédérales, les organisations du secteur privé et les établissements d'enseignement.

De plus amples informations sur les méthodologies de test d'intrusion les plus courantes et leur comparaison sont disponibles à l'annexe D : Comparaison des méthodologies. En outre, les lignes directrices et les meilleures pratiques en matière de sécurité les plus courantes sont répertoriées à l'annexe E.

6. Méthodologie de pointe

Le manuel OSSTMM 3 (Manuel sur la méthodologie des tests de sécurité open source) est la principale méthodologie utilisée dans cette approche de test d'intrusion. Il fournit une méthodologie pour un test de sécurité approfondi, appelé ici audit OSSTMM.

Bien que l'OSSTMM 3 soit la méthodologie principale, ce cadre de test d'intrusion intègre également des éléments provenant de:

- **ETSI TS 103 701 –** Les cas de test pertinents issus de cette norme de test de conformité sont intégrés à notre processus d'exécution des tests, en particulier pour l'IoT et les PDE grand public.
- **Guide de test OWASP –** Nous avons intégré les cas de test OWASP aux phases de reconnaissance et d'exploitation pour les applications Web et les API. Cela implique de suivre les directives OWASP afin d'identifier les vulnérabilités telles que l'injection SQL, le cross-site scripting et la gestion non sécurisée des sessions.
- **PTES (Norme d'exécution des tests d'intrusion) –** PTES définit un cycle de vie structuré que nous avons intégré à notre méthodologie. Afin de garantir que chaque phase dispose d'objectifs, de résultats et de protocoles de communication clairs, nous avons aligné les phases OSSTMM3 sur PTES, ce qui a permis d'obtenir un processus de test cohérent et reproductible.
- **NIST SP 800-115 –** La norme NIST SP 800-115 fournit un cadre solide pour les tests de sécurité basés sur les risques. Les phases d'exploitation et d'analyse d'impact ont été alignées sur ses directives afin de garantir une identification systématique des vulnérabilités, une évaluation complète des risques et des rapports détaillés.

7. Préparation à un test d'intrusion

Pourquoi tester ? La CRA exige que les PDE « procèdent à des tests et à des examens efficaces et réguliers de la sécurité du produit comportant des éléments numériques » (annexe I, partie II, point 3). La planification d'évaluations régulières de la sécurité garantit une surveillance continue et une identification proactive des vulnérabilités, ce qui permet de maintenir la résilience face aux menaces émergentes.

Qui effectuera les tests ? Dans le cadre des évaluations alignées sur la CRA, le choix d'un testeur (ou d'un fournisseur) de pénétration a un impact direct sur la fiabilité, la reproductibilité et la pertinence réglementaire des résultats. Les PME peuvent sélectionner des testeurs de pénétration qui démontrent les qualités suivantes :

- *Compétences techniques* : expertise avérée en matière de sécurité des produits, de systèmes embarqués, de tests de micrologiciels et d'analyse des vulnérabilités logicielles. Les fournisseurs doivent comprendre les différences entre les tests de produits et les évaluations traditionnelles de l'environnement d'entreprise.
- *Connaissance de la CRA* : connaissance démontrable de la loi sur la cyber-résilience, y compris les exigences de l'annexe I, parties I et II, et capacité à produire des résultats qui soutiennent les déclarations de conformité CRA.
- *Expérience spécifique au secteur* : le cas échéant, choisissez des fournisseurs ayant une expérience dans le domaine du produit.
- *Garantie juridique et éthique* : vérifiez que les testeurs respectent des directives éthiques claires, fournissent une couverture d'assurance et concluent des contrats juridiques bien définis, comprenant des clauses de responsabilité et de traitement des données.

***Certifications et accréditations* :** les certifications telles que OSCP, OSCE, CREST ou des certifications nationales équivalentes au niveau européen sont utiles. Pour les produits à haut risque ou critiques, envisagez une certification TIBER-EU ou Red Team.

-

Combien de temps cela prendra-t-il ? Les délais peuvent varier en fonction de la complexité du produit, du niveau de connaissance (boîte noire/grise/blanche) et de la classification CRA (par défaut, importante ou critique), mais une estimation générique du temps nécessaire pour chaque phase peut être résumée comme suit :

1. Préparation (5 à 10 jours ouvrables, *en collaboration avec le testeur et le fabricant*), comprenant :

- Définition de la portée, des objectifs et des limites des tests
- Cartographie des exigences de l'annexe I de la CRA
- Accords juridiques et alignement des parties prenantes
- Le client fournit la documentation technique

2. Exécution des tests et rapport (3 à 10 jours ouvrables, *dirigée par le testeur*), comprenant :

- Collecte de renseignements, exploitation et analyse d'impact
- Test du micrologiciel, des interfaces, des API et des contrôles de sécurité du produit
- Préparation et communication du rapport

3. Remédiation (12 à 4 semaines, *dirigée par le fabricant*)

- Développement de correctifs, corrections de configuration, assurance qualité interne
- Acceptation facultative des risques et mise à jour de la documentation

4. Nouveau test (1 à 2 jours ouvrables, *en collaboration avec le testeur et le fabricant*)

- Revalidation des problèmes résolus
- Confirmations techniques finales et collecte de preuves

8. Méthodologie des tests d'intrusion

8.1 Pré-engagement et planification

La première étape consiste à définir le type de test le plus approprié, en tenant compte de la maturité du produit, des risques de sécurité identifiés pour le produit (internes/externes), de la documentation disponible et des vecteurs d'attaque possibles (comment un produit peut-il être exploité). Les tests peuvent être :

- **Boîte noire** : les testeurs n'ont aucune connaissance interne ; simule un attaquant externe.
- **Boîte grise** : les testeurs ont une connaissance partielle. Souvent guidés par un accès partiel.
- **Boîte blanche** : connaissance interne complète (code source, architecture) ; permet des tests approfondis.

Notez que les tests en laboratoire supposent une connaissance partielle ou complète (boîte blanche).

Entrées :

- *Identification du produit*. Pour les tests en boîte blanche et en boîte grise : une documentation technique sera nécessaire, comprenant : des cas d'utilisation opérationnelle, des schémas d'architecture, la version du micrologiciel/logiciel, la liste des interfaces internes et externes (par exemple, USB, BLE, API, interface utilisateur web, ports, protocoles) ou tout autre élément/composant connu pertinent pour les tests, le modèle de menace (si disponible). En outre, les détails des évaluations ou audits précédents (si disponibles), y compris les tickets de bogues ouverts ou les résultats de tests non résolus, pourraient être utiles.
- Cadres industriels (par exemple, OSSTMM3, PTES, NIST SP 800-115, OWASP)
- Exigences réglementaires et documentation de conformité, y compris les exigences de l'annexe I, parties I et II de la CRA (voir l'annexe B : Exigences de la CRA)
- Points de contact et protocoles d'urgence, y compris une procédure d'urgence (que faire en cas d'événements imprévus, tels que des interruptions de service) pendant les tests.
- Documentation contractuelle (si vous faites appel à des testeurs externes) : contrats de service, accords de confidentialité, autorisation de test et décharges de responsabilité.

Activités :

- *Définition des objectifs et établissement de la portée* : cette phase commence par la définition claire des objectifs et de la portée. L'accent est mis sur la vérification des fonctionnalités propres à chaque système. La définition de la portée est essentielle pour aligner les tests d'intrusion sur les objectifs de l'ARC et les caractéristiques propres au produit testé. La définition de la portée comprend :
    - *Définition des limites du produit* : définir le périmètre technique (logiciels, matériel, API, interfaces) du produit avec des éléments numériques (PDE).
    - *Cartographie CRA* : identifier les exigences de l'annexe I de la CRA qui s'appliquent, en fonction de la classe de risque du produit.
    - *Modélisation des menaces* : intégrer les acteurs malveillants connus, les surfaces d'attaque et le contexte du produit.

- *Profondeur des tests : la profondeur des tests de pénétration correspondrait à la classification de criticité du produit selon la loi sur la cyberrésilience (CRA).*
    - *Les tests par défaut et importants des produits de classe I* se concentrent généralement sur les services et interfaces exposés à l'extérieur, les mécanismes de contrôle d'accès, la protection des données en transit et l'identification des vulnérabilités connues.
    - *Un produit de classe II important* nécessite une inspection plus approfondie du micrologiciel, des mécanismes de mise à jour, de la communication entre les appareils et le cloud, des flux d'authentification et des scénarios d'utilisation abusive des protocoles.
    - Les tests sur les *produits critiques* comprennent la validation de la sécurité au niveau matériel, telle que la détection des altérations, la résistance à l'injection de défauts et la vérification du démarrage sécurisé.

- *Considérations juridiques, réglementaires et éthiques* : Les tests sont effectués dans le respect des exigences légales et réglementaires (par exemple, confidentialité, protection des données, lois sur la propriété intellectuelle) et des politiques internes. Toutes les autorisations requises sont obtenues et les contraintes sont documentées afin que l'environnement de test n'ait aucune incidence sur les opérations de production. (voir annexe B : Exigences de l'ARC,

annexe I de l'ARC, partie I, points 1, 2(b), 2(g) et 2(j) ; et annexe I, partie II, point 1).
- *Mise en place d'un laboratoire d'essai* qui reproduit l'environnement opérationnel du PDE.

Résultats pour les phases suivantes :

- Document méthodologique de haut niveau
- Formulaires d'autorisation légale
- Définition du champ d'application
- Directives d'engagement
- Rapport d'évaluation des risques liés au produit
- Briefing des parties prenantes

Résultats finaux :

- Document de planification et d'exigences (D1) : un plan détaillé du projet de test d'intrusion décrivant la portée, les rôles, les objectifs, les autorisations, le calendrier et la configuration du laboratoire.

Évaluation des risques avant le test et alignement des parties prenantes (D2) :

- Avant de commencer les tests, une évaluation des risques spécifiques au produit doit être effectuée afin d'identifier tout risque potentiel que le test d'intrusion pourrait poser pour la fonctionnalité, l'intégrité ou la disponibilité du produit. Cela comprend l'évaluation de l'impact que le test pourrait avoir sur les interfaces, les services et les données critiques traités par le produit. Les parties prenantes sont informées et le plan de test d'intrusion doit être aligné sur leurs exigences en matière de sécurité (y compris l'annexe B : Exigences de l'ARC, annexe I, partie I de l'ARC) et leur tolérance au risque.

8.2 Collecte de renseignements et reconnaissance

Entrées :

- Définition du périmètre
- Rapport d'évaluation des risques liés au produit

Activités :

- Renseignement open source et découverte des actifs : le renseignement open source est utilisé dans cette phase pour recueillir autant d'informations que

possible. Cela comprend la cartographie de l'empreinte numérique de chaque produit et élément.
- Profilage des cibles et analyse du paysage des menaces : une analyse de chaque actif est nécessaire pour déterminer les vulnérabilités potentielles. Le paysage des menaces est également examiné afin de s'assurer que des scénarios réalistes sont utilisés pour les tests d'intrusion et que les tactiques des adversaires sont reflétées dans les attaques simulées pendant les tests.
- Élaboration de scénarios basés sur le comportement des adversaires : des scénarios d'attaque spécifiques sont formulés à partir des renseignements et des données collectées.

Résultats pour les phases suivantes :

- Scénarios de comportement des adversaires et profils cibles
- Première version du rapport sur les vulnérabilités (D3) : conclusions détaillées issues des évaluations externes et internes du produit, y compris les évaluations des risques, la faisabilité de l'exploitation et les suggestions de remédiation, qui fournissent une vue d'ensemble des vulnérabilités affectant le produit lui-même.

Résultats finaux :

- Aucun résultat finalisé au cours de cette phase.

8.3 Exécution et exploitation des tests

Entrées :

- Première version du rapport sur les vulnérabilités (D3) : conclusions détaillées issues des évaluations externes et internes du produit, y compris les évaluations des risques, la faisabilité de l'exploitation et les suggestions de remédiation qui fournissent une vue d'ensemble des vulnérabilités affectant le produit lui-même.
- Scénarios de comportement des adversaires et profils cibles
- Outils de test (par exemple, Nessus, Metasploit, Wireshark). Des exemples d'outils de test et de cadres sont répertoriés à l'annexe E.
- (si disponible) code source du logiciel.

Activités:

- Identification des vulnérabilités et simulation d'attaques : les vulnérabilités sont identifiées à l'aide de techniques telles que l'analyse statique (SAST) et l'analyse dynamique de la sécurité des applications (DAST) ou la révision manuelle du code, le cas échéant. L'intelligence artificielle peut être utilisée pour améliorer l'efficacité de la détection des vulnérabilités. Chaque produit est testé conformément aux normes établies. Les activités d'évaluation des vulnérabilités sont effectuées de manière itérative tout au long de l'exécution des tests et alimentent directement la génération du rapport sur les vulnérabilités D4. Elles servent de base principale pour l'évaluation ultérieure des risques. Les scénarios de test sélectionnés, issus de la norme ETSI TS 103701, sont énumérés à l'annexe C, car ils pourraient être exécutés dans le cadre des tests d'intrusion qui, outre la sécurité, permettraient de vérifier la conformité avec la CRA. Les activités menées au cours de cette phase permettent également de valider la conception sécurisée et les exigences de protection conformes à la CRA. Voir l'annexe B : CRA, annexe I, partie I, points 2(a), 2(b), 2(d), 2(e), 2(j), 2(k) ; et annexe I, partie II, point 3.
- Techniques d'exploitation et d'émulation d'adversaires : valider les failles en tentant de les exploiter dans un environnement contrôlé. Un scan assisté par IA peut être utilisé si des outils sont disponibles. Les PME qui ne disposent pas de tels outils peuvent s'appuyer sur une inspection manuelle ou une automatisation plus simple. Il peut s'agir, par exemple, de la détection d'anomalies dans les journaux ou du fuzzing basé sur l'apprentissage automatique. Il convient également d'évaluer les situations dans lesquelles des adversaires pourraient contourner les mesures de sécurité et obtenir un accès non autorisé.
- Analyse post-exploitation : évaluer l'impact d'une attaque réussie, y compris l'escalade des privilèges dans le système et les mouvements latéraux potentiels vers d'autres utilisateurs, composants ou systèmes connectés. Il s'agit notamment de déterminer si un attaquant peut accéder à des données sensibles, se déplacer entre les modules d'application ou les segments d'infrastructure, ou compromettre des services critiques. Les détails de l'impact fonctionnel sont recueillis en analysant les conséquences potentielles de chaque vulnérabilité exploitée.
- Les résultats des cas de test sont intégrés dans les résultats finaux de cette phase afin d'assurer la traçabilité des activités de test par rapport aux comportements attendus.

Résultats pour les phases suivantes :

- Liste des vulnérabilités
- Preuves d'exploitation (preuve de concept)
- Évaluations préliminaires des risques
- Rapport sur la faisabilité de l'exploitation
- Rapport sur la simulation des tactiques adverses

Résultats finaux :

- Rapport sur les vulnérabilités (D3) : conclusions détaillées issues des évaluations externes et internes du produit, y compris les évaluations des risques, la faisabilité de l'exploitation et les suggestions de remédiation, qui fournissent une vue d'ensemble des vulnérabilités affectant le produit lui-même.

8.4 Analyse d'impact et rapports

Entrées :

- Liste des vulnérabilités
- Preuves d'exploitation (preuve de concept)
- Évaluations préliminaires des risques
- Normes d'évaluation des risques spécifiques à l'industrie
- Politiques de classification des données.

Activités :

Évaluation des risques et analyse de l'impact fonctionnel : analyse de la gravité des vulnérabilités identifiées, mesure de leur impact sur la CIA (confidentialité, intégrité ou disponibilité). Attribution d'une note de risque afin de hiérarchiser les efforts de remédiation.

- En outre, des modèles de notation des risques basés sur l'IA peuvent être utilisés pour améliorer la phase d'évaluation globale en attribuant des niveaux de risque basés sur des informations en temps réel sur les menaces et les données d'exploitabilité. Cela comprend l'évaluation, conformément à la CRA, de l'intégrité des données, de la résilience et de la réponse aux vulnérabilités. Voir l'annexe B : CRA Annexe I, partie I, points 2(e), 2(f), 2(i) ; Annexe I, partie II, points 1, 2.

- Documentation des conclusions et collecte de preuves : Compiler des rapports détaillés contenant des descriptions des vulnérabilités, des preuves techniques et des preuves d'exploitation. Veiller à ce que les parties prenantes aient une compréhension claire des lacunes en matière de sécurité.
- Indicateur de conformité réglementaire : Traduire les résultats des tests en termes de conformité réglementaire en signalant les conclusions liées aux exigences des annexes I et II de la CRA énumérées à l'annexe B. Contribuer ainsi à un rapport d'alignement sur la conformité réglementaire, qui peut être utilisé pour justifier la déclaration de conformité d'un fabricant.
- Recommandations et stratégies de remédiation concrètes : fournir des conseils détaillés pour atténuer les risques identifiés. Suggérer des contrôles de sécurité, des modifications de configuration et des stratégies de correction pour rendre le système plus résilient. Voir l'annexe B : Exigences CRA

Résultats pour les phases suivantes :

- Rapport d'évaluation des risques
- Document complet des résultats
- Détails de l'impact fonctionnel
- Recommandations de remédiation
- Plan d'action de remédiation priorisé
- Rapport d'alignement sur la conformité réglementaire

Résultats finaux :

- Recommandations et feuille de route de remédiation (D5) : recommandations priorisées accompagnées d'une feuille de route de remédiation claire, comprenant des actions à court, moyen et long terme.

8.5 Suivi post-engagement

Entrées :

- Rapports de correction
- Configurations système mises à jour et résultats des nouveaux tests.

Activités :

- Vérification des mesures correctives et nouveaux tests : effectuer de nouveaux tests pour vérifier que les failles de sécurité ont été corrigées. S'assurer que les

mesures correctives éliminent efficacement les vulnérabilités. Les activités post-test confirment la conformité avec les attentes de CRA en matière de mises à jour de sécurité et de divulgation. Voir l'annexe B : Annexe I de la CRA, partie I, points 2(h) et 2(m) ; et annexe I, partie II, points 2, 4, 7 et 8.

- Amélioration continue et intégration des enseignements tirés : mise à jour des méthodologies de test et des politiques de sécurité sur la base des conclusions. L'analyse basée sur l'IA contribue à améliorer les évaluations de sécurité futures en tirant parti des enseignements tirés des tests précédents. (voir : Annexe : Exigences de la CRA, Annexe I, Partie I)
- Divulgation et communication des vulnérabilités : dès que les mises à jour de sécurité sont disponibles, les fabricants doivent préparer et divulguer publiquement les détails des vulnérabilités résolues. Dans les cas où la divulgation entraînerait un risque excessif, la publication peut être reportée de manière justifiée jusqu'à ce que les correctifs soient largement déployés (Annexe I, Partie II, Point 4).

Résultats finaux :

- Rapport de test d'intrusion (D5) : un rapport de test d'intrusion type comprend un résumé (aperçu général, évaluation globale des risques, résultats des tests et recommandations prioritaires), la portée et la méthode des tests (D1), les activités, les conclusions (avec des détails supplémentaires, y compris les vulnérabilités (D2) et les preuves d'exploitation) et les recommandations (D4). Ce document pourrait être considéré comme un « examen de la sécurité du produit comportant des éléments numériques » aux fins de l'exigence de l'ARC figurant à l'annexe I, partie II, point 3 (Appliquer des tests et des examens efficaces et réguliers de la sécurité du produit comportant des éléments numériques).

8.6 Résultats

- Chaque mission donnera lieu à un ensemble complet de résultats destinés à répondre à la fois aux besoins techniques et stratégiques. Pour chaque phase de la méthodologie, les résultats seront de deux types : (a) les résultats utilisés comme intrants pour une phase ultérieure et (b) les résultats de l'ensemble de l'exercice. Les résultats de l'ensemble de l'exercice sont énumérés ci-dessous ;

- Document de planification et d'exigences (D1) : un plan détaillé du projet de test d'intrusion décrivant les objectifs, la portée, les rôles, les procédures d'urgence, les autorisations, le calendrier et la configuration du laboratoire.

-

- Évaluation des risques avant le test et alignement des parties prenantes (D2) : une analyse approfondie des risques potentiels avant le début des tests, garantissant l'alignement avec les parties prenantes en ce qui concerne la portée, les priorités et les objectifs.
- Rapport sur les vulnérabilités (D3) : conclusions détaillées des évaluations externes et internes du produit, y compris les niveaux de risque, la faisabilité de l'exploitation et les suggestions de remédiation, qui fournissent une vue d'ensemble des vulnérabilités affectant le produit lui-même.
- Recommandations et feuille de route pour la correction (D4) : recommandations classées par ordre de priorité, accompagnées d'une feuille de route claire pour la correction, comprenant des mesures à court, moyen et long terme.
- Rapport de test d'intrusion (D5) : aperçu général destiné aux parties prenantes non techniques, résumant les principales conclusions et recommandations stratégiques.

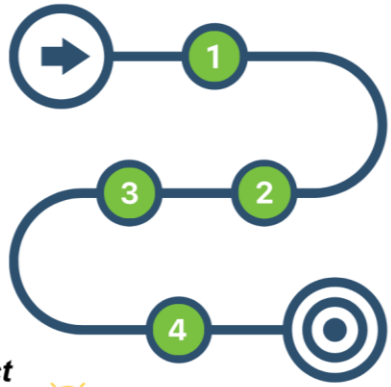
8.7 Exemples de Scénarios

Cette section a pour objectif de fournir des exemples illustratifs de scénarios de tests d'intrusion, y compris les ressources approximatives requises et le calendrier probable. Ces scénarios sont uniquement fournis à titre indicatif et peuvent varier considérablement d'un exercice à l'autre.

Scénario 1 : Gestion des identités et des accès (produit important de CRA : classe I)

Approche de Test

- **Type de test :** Grey Box (les informations d'identification de base ont été fournies. Le pentester doit énumérer les fonctions et privilèges IAM internes).
- **Complexité :** Moyenne (5 à 15 fonctions/modules IAM).
- **Estimation de l'effort :** 8 à 12 jours de travail (~15 à 20 jours écoulés).



Chemin d'attaque

1. **Reconnaissance:** énumérer les points de terminaison de connexion IAM, les mécanismes MFA et la logique de gestion des sessions.
2. **Exploitation des vulnérabilités:** contourner la MFA de secours via la récupération sociale. Détourner la session administrateur grâce à la collecte de jetons.
3. **Analyse d'impact et rapports:** identifier les risques d'accès non autorisé au portail d'administration et aux configurations internes.
4. **Suivi:** corriger la logique de secours MFA et reconfigurer la gestion des sessions.

Conclusions et Impact

- Une gestion incorrecte des sessions exposait les jetons de session à des utilisateurs non autorisés.
- La logique de secours de l'authentification multifacteur (MFA) pouvait être contournée à l'aide de méthodes de récupération via les réseaux sociaux.
- Les journaux IAM ne signalaient pas les élévations de privilèges obtenues par la manipulation des rôles.

Recommandations

- Mettez en place des jetons de session sécurisés avec les attributs HttpOnly, Secure et SameSite.
- Appliquez des flux d'authentification multifactorielle stricts sans repli non vérifié.
- Activez la journalisation et les alertes en cas de tentatives d'élévation de privilèges et de changements de rôle.

Impact sur la conformité CRA

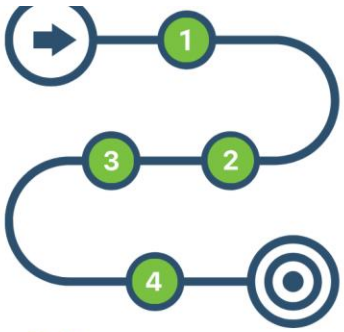
Une solution de secours MFA non sécurisée enfreint l'annexe I, partie I, point 2(d) de la CRA : « Assurer la protection contre tout accès non autorisé au moyen de mécanismes de contrôle appropriés. »

L'absence d'enregistrement des élévations de privilèges enfreint l'annexe I, partie I, point 2(l) de la CRA : « Fournir des informations relatives à la sécurité en enregistrant et en surveillant les activités internes pertinentes. »

Scénario 2 : Gestion des informations et des événements de sécurité (SIEM) (Produit important de la CRA : Classe II)

Approche de Test

- **Type de test :** Grey Box (identifiants SIEM fournis ; le pentester simule des entrées hostiles et la falsification des journaux).
- **Complexité :** élevée (15 à 30 sources de journaux, ensembles de règles et intégrations).
- **Estimation de l'effort:** 12 à 15 jours de travail (environ 20 à 25 jours écoulés).



Chemin d'attaque

1. **Reconnaissance:** examinez les points d'ingestion SIEM, les règles de corrélation et les seuils d'alerte.
2. **Exploitation des vulnérabilités:** injectez des journaux spécialement conçus pour masquer les attaques réelles. Exploitez l'absence de corrélation des événements lors des échecs de connexion.
3. **Analyse d'impact et reporting:** évaluez comment la suppression des alertes permet un accès persistant.
4. **Suivi :** renforcez la logique d'analyse et les ensembles de règles d'audit.

Conclusions et Impact

- *Le SIEM n'a pas déclenché d'alertes lors de tentatives de connexion répétées infructueuses.*
- *L'injection de syslog a permis de masquer les journaux d'intrusion.*
- *Les contrôles d'intégrité des journaux pouvaient être contournés via l'évasion de charge utile.*

Recommandations

- *Configurez des règles de détection des anomalies pour les seuils basés sur l'authentification.*
- *Nettoyez les entrées du journal pour empêcher l'injection de journaux.*
- *Utilisez la signature et la validation cryptographiques des journaux pour garantir leur intégrité.*

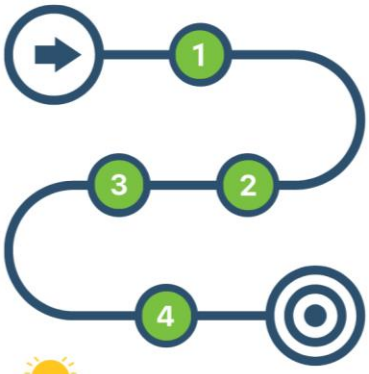
Impact sur la conformité CRA

La falsification des journaux sans détection enfreint l'annexe I, partie I, point 2(l) de la CRA : « Enregistrement et surveillance des activités internes pertinentes ».
Le contournement des alertes en cas d'échecs répétés de connexion enfreint l'annexe I, partie I, point 2(h) de la CRA : « Protéger la disponibilité des fonctions essentielles et de base... y compris l'atténuation des attaques par déni de service ».

Scénario 3 : Passerelle de compteur intelligent (produit essentiel pour les CRA)

Approche de Test

- **Type de test :** Grey Box (spécifications du micrologiciel et de l'interface fournies ; le pentester effectue les tests de protocole et les tests intégrés).
- **Complexité :** élevée (systèmes intégrés complexes et protocoles propriétaires).
- **Estimation de l'effort :** 15 à 20 jours de travail (environ 25 à 30 jours écoulés).



Chemin d'attaque

1. **Reconnaissance :** Identification des points de terminaison de mise à jour du micrologiciel et des modèles de communication.
2. **Exploitation des vulnérabilités :** Réutilisation du trafic de mise à jour du micrologiciel capturé. Déploiement d'un micrologiciel malveillant.
3. **Analyse d'impact et rapport :** Démonstration de la prise de contrôle totale de la logique de la passerelle du compteur intelligent.
4. **Suivi :** Refonte du démarrage sécurisé avec une chaîne cryptographique et une protection contre la relecture des correctifs.

Conclusions et Impact

- *Le processus de mise à jour du micrologiciel acceptait des images non signées.*
- *La validation du démarrage sécurisé était contournée via des failles du chargeur d'amorçage.*
- *Les attaques par rejeu capturaient et renvoyaient des communications cryptées valides.*

Recommandations

- *Appliquez des vérifications de signature numérique lors de l'installation du micrologiciel.*
- *Renforcez le chargeur d'amorçage afin de valider les chaînes de confiance cryptographiques.*
- *Incluez des nonces et des vérifications de fraîcheur afin d'atténuer les attaques par rejeu.*

Impact sur la conformité CRA

L'absence de validation du micrologiciel enfreint l'annexe I, partie I, point 2(k) de la CRA : « Réduire l'impact d'un incident à l'aide de techniques d'atténuation des exploits appropriées. »
Les attaques par rejeu exploitant les communications du micrologiciel enfreignent l'annexe I, partie I, point 2(e) de la CRA : « Protéger la confidentialité des données stockées ou transmises à l'aide de mécanismes de pointe. »

Annexe A : Sélection des PDE pris en considération

Important : Classe I

- *Systèmes de gestion des identités*
- *Navigateurs*
- *Gestionnaires de mots de passe*
- *Logiciels de délivrance de certificats numériques*
- *Routeurs*
- *Produits pour la maison intelligente*
- *Appareils portables de surveillance de la santé*
- *Systèmes SIEM*

Important : Classe II

- *Pare-feu*

Produits critiques

- *Passerelle pour compteurs intelligents*

Annexe B: Exigences de l'ARC

1. Annexe I Partie I – Exigences essentielles en matière de cybersécurité

Exigence de l'ARC	Référence à l'exigence de l'ARC
Les produits comportant des éléments numériques doivent être conçus, développés et fabriqués de manière à garantir un niveau de cybersécurité approprié en fonction des risques.	Annexe I, Partie I, Point 1
(a) être mis à disposition sur le marché avec une configuration sécurisée par défaut, sauf accord contraire entre le fabricant et l'utilisateur professionnel concernant un produit sur mesure comportant des éléments numériques, y compris la possibilité de réinitialiser le produit à son état d'origine	Annexe I, Partie I, Point 2 (a)
(b) Être mis à disposition sur le marché avec une configuration sécurisée par défaut, y compris la possibilité de rétablir l'état d'origine.	Annexe I, Partie I, Point 2 (b)
c) Veiller à ce que les vulnérabilités puissent être corrigées au moyen de mises à jour de sécurité, y compris, le cas échéant, au moyen de mises à jour de sécurité automatiques installées dans un délai approprié, activées par défaut et assorties d'un mécanisme de désactivation clair et facile à utiliser, en informant les utilisateurs de la disponibilité des mises à jour et en leur offrant la possibilité de les reporter temporairement.	Annexe I, Partie I, Point 2 (c)

(d) Assurer la protection contre tout accès non autorisé au moyen de mécanismes de contrôle appropriés, y compris, mais sans s'y limiter, des systèmes d'authentification, de gestion des identités ou des accès, et signaler tout accès non autorisé éventuel.	Annexe I, Partie I, Point 2 (d)
(e) Protéger la confidentialité des données stockées, transmises ou traitées de toute autre manière, qu'elles soient personnelles ou autres, par exemple en cryptant les données pertinentes au repos ou en transit à l'aide de mécanismes de pointe et en utilisant d'autres moyens techniques.	Annexe I, Partie I, Point 2 (e)
(f) Protéger l'intégrité des données stockées, transmises ou traitées de toute autre manière, qu'elles soient personnelles ou autres, ainsi que les commandes, programmes et configurations contre toute manipulation ou modification non autorisée par l'utilisateur, et signaler toute corruption.	Annexe I, Partie I, Point 2 (f)
(g) Traiter uniquement les données, personnelles ou autres, qui sont adéquates, pertinentes et limitées à ce qui est nécessaire au regard des finalités pour lesquelles le produit comportant des éléments numériques est destiné (minimisation des données)	Annexe I, Partie I, Point 2 (g)
h) Protéger la disponibilité des fonctions essentielles et fondamentales, y compris après un incident, notamment par des mesures de résilience et d'atténuation contre les attaques par déni de service.	Annexe I, Partie I, Point 2 (h)
(i) Minimiser l'impact négatif des produits eux-mêmes ou des appareils connectés sur la disponibilité des services fournis par d'autres appareils ou réseaux.	Annexe I, Partie I, Point 2 (i)
(j) Conçu, développé et produit pour limiter les surfaces d'attaque, y compris les interfaces externes.	Annexe I, Partie I, Point 2 (j)
(k) Être conçu, développé et produit de manière à réduire l'impact d'un incident à l'aide de mécanismes et de techniques d'atténuation des risques appropriés.	Annexe I, Partie I, Point 2(k)

(l) Fournir des informations relatives à la sécurité en enregistrant et en surveillant les activités internes pertinentes, y compris l'accès ou la modification des données, des services ou des fonctions, avec un mécanisme de désactivation pour l'utilisateur.	Annex I, Partie I, Point 2(l)
(m) Offrir aux utilisateurs la possibilité de supprimer de manière sécurisée et définitive toutes les données et tous les paramètres, et, lorsque ces données peuvent être transférées vers d'autres produits ou systèmes, veiller à ce que cela soit fait de manière sécurisée.	Annex I, Partie I, Point 2(m)

2. Annexe I, Partie II – Exigences Relatives à la Gestion de la Vulnérabilité

Exigence de l'ARC	Référence CRA
Identifier et documenter les vulnérabilités et les composants contenus dans les produits comportant des éléments numériques, notamment en établissant une liste des composants logiciels dans un format couramment utilisé et lisible par machine, couvrant au minimum les dépendances de haut niveau des produits.	Annex I, Partie II, Point 1
En ce qui concerne les risques liés aux produits comportant des éléments numériques, remédiez sans délai aux vulnérabilités, notamment en fournissant des mises à jour de sécurité ; lorsque cela est techniquement possible, les nouvelles mises à jour de sécurité doivent être fournies séparément des mises à jour fonctionnelles.	Annex I, Partie II, Point 2
Appliquer des tests et des contrôles efficaces et réguliers de la sécurité du produit comportant des éléments numériques.	Annex I, Partie II, Point 3

Une fois qu'une mise à jour de sécurité a été mise à disposition, partager et divulguer publiquement les informations relatives aux vulnérabilités corrigées, y compris une description des vulnérabilités, les informations permettant aux utilisateurs d'identifier le produit contenant les éléments numériques concernés, les conséquences des vulnérabilités, leur gravité et des informations claires et accessibles aidant les utilisateurs à remédier aux vulnérabilités ; dans des cas dûment justifiés, lorsque les fabricants estiment que les risques liés à la publication l'emportent sur les avantages en matière de sécurité, ils peuvent reporter la publication des informations relatives à une vulnérabilité corrigée jusqu'à ce que les utilisateurs aient eu la possibilité d'appliquer le correctif approprié.	Annex I, Partie II, Point 4
Mettre en place et appliquer une politique de divulgation coordonnée des vulnérabilités.	Annex I, Partie II, Point 5
Prendre des mesures pour faciliter le partage d'informations sur les vulnérabilités potentielles de leurs produits comportant des éléments numériques, ainsi que des composants tiers contenus dans ces produits, notamment en fournissant une adresse de contact pour signaler les vulnérabilités découvertes dans les produits comportant des éléments numériques.	Annex I, Partie II, Point 6
Prévoir des mécanismes permettant de distribuer en toute sécurité les mises à jour des produits comportant des éléments numériques afin de garantir que les vulnérabilités sont corrigées ou atténuées en temps utile et, le cas échéant, les mises à jour de sécurité, de manière automatique.	Annex I, Partie II, Point 7
Veiller à ce que, lorsque des mises à jour de sécurité sont disponibles pour remédier à des problèmes de sécurité identifiés, elles soient diffusées sans délai et, sauf accord contraire entre un fabricant et un utilisateur professionnel concernant un produit sur mesure comportant des éléments numériques, gratuitement, accompagnées de messages d'avertissement fournissant aux utilisateurs les informations	Annex I, Partiet II, Point 8

pertinentes, y compris sur les mesures à prendre éventuellement.	

Annexe C : Sélection des groupes de tests ETSI TS 103701 et des cas de test avec correspondance aux exigences CRA

ID du groupe de test	Cas test (conceptuel)	Référence à l'exigence CRA liée.
TSO 5.1 : Pas de mots de passe par défaut universels	(5.1-1) L'objectif de ce cas test est l'évaluation conceptuelle des mécanismes d'authentification par mot de passe.	Annex I, Partie I, Point 2(d)
	(5.1-2) L'objectif de ce cas de test est l'évaluation conceptuelle des mécanismes de génération des mots de passe préinstallés.	Annex I, Partie I, Point 2(d)
TSO 5.2 : Mettre en place un moyen de gérer les rapports de vulnérabilité.	(5.2-1) L'objectif de ce cas test est l'évaluation conceptuelle de la publication de la politique de divulgation des vulnérabilités.	Annex I, Partie II, Point 5
	(5.2-2) L'objectif de ce cas test est l'évaluation conceptuelle de la manière dont les vulnérabilités sont traitées, a), et la confirmation que les conditions préalables à la mise en œuvre sont remplies, b).	Annex I, Partie II, Point 2
TSO 5.3 : Maintenir les logiciels à jour	(5.3-1) L'objectif de ce cas test est l'évaluation conceptuelle de la mise à jour des composants logiciels en l'absence de mises à jour logicielles, a) et des mécanismes de mise à jour b).	Annex I, Partie II, Point 7
	(5.3-2) L'objectif de ce cas de test est l'évaluation conceptuelle du mécanisme d'installation des mises à jour concernant les mesures adéquates pour empêcher un attaquant d'utiliser de manière abusive l'installation des mises à jour sur le DUT.	Annex I, Partie II, Point 7
	(5.3-3) L'objectif de ce cas de test est l'évaluation conceptuelle des mécanismes de mise à jour en termes de simplicité pour l'utilisateur.	Annex I, Partie I, Point 2(c)

		Annex I, Partie II, Point 8
TSO 5.4 : Stocker de manière sécurisée les paramètres de sécurité sensibles	(5.4-1) L'objectif de ce cas de test est l'évaluation conceptuelle du stockage sécurisé des paramètres de sécurité sensibles concernant les déclarations de sécurité (a-c) et l'exhaustivité de la documentation IXIT (d).	Annex I, Partie I, Point 2(e)
	(5.4-2) L'objectif de ce cas de test est l'évaluation conceptuelle du stockage inviolable des identités codées en dur.	Annex I, Partie I, Point 2(e)
TSO 5.5 : Communiquer en toute sécurité	(5.5-1) L'objectif de ce cas de test est l'évaluation conceptuelle de la cryptographie utilisée pour les mécanismes de communication concernant l'utilisation des meilleures pratiques en matière de cryptographie (a-c) et la vulnérabilité à une attaque réalisable (d).	Annex I, Partie I, Point 2(e)
	(5.5-4) L'objectif de ce cas de test est l'évaluation conceptuelle de la fonctionnalité du dispositif via une interface réseau à l'état initialisé, en ce qui concerne l'authentification et l'autorisation.	Annex I, Partie I, Point 2(d)
TSO 5.7 : Garantir l'intégrité des logiciels	(5.7-1) L'objectif de ce cas de test est l'évaluation conceptuelle des mécanismes de démarrage sécurisé du DUT.	Annex I, Partie I, Point 2(f)
	(5.7-2) Le but de ce cas de test est l'évaluation conceptuelle des mécanismes d'alerte, a), et des mécanismes de restriction de la communication, b), en cas de détection d'une modification non autorisée du logiciel.	Annex I, Partie I, Point 2(f)
TSO 5.8 : Veiller à la sécurité des données à caractère personnel	(5.8-1) L'objectif de ce cas de test est l'évaluation conceptuelle de la cryptographie utilisée pour la communication de données à caractère personnel entre un appareil et un service.	Annex I, Partie I, Point 2(e)

TSO 5.9 : Rendre les systèmes résilients aux pannes	(5.9-1) L'objectif de ce cas de test est l'évaluation conceptuelle des mécanismes de résilience concernant les pannes du réseau et de l'alimentation électrique.	Annex I, Partie I, Point 2(h)
	(5.9-3) L'objectif de ce cas de test est l'évaluation conceptuelle des mesures de résilience pour les mécanismes de communication.	Annex I, Partie I, Point 2(h)

Annexe D : Comparaison des méthodologies

Méthodologies de test d'intrusion largement reconnues dans le secteur	
Portée	**Rôle dans ce guide**

	Major	Moyen	Aucun
Groupes de test et procédures spécifiques aux produits, conformes à l'annexe I du CRA.	**ETSI TS 103 701**		
Définit les exigences de base en matière de cybersécurité pour les appareils IoT grand public. Dans cette méthodologie, elle complète la norme TS 103 701 en définissant la posture de sécurité attendue dès la conception, qui est vérifiée par des tests.	**ETSI EN 303 645**		
Fournit une méthode structurée pour mesurer le niveau de sécurité à l'aide d'indicateurs définis (par exemple, les scores RAV). L'application des indicateurs OSSTMM3 peut faciliter le suivi de la maturité interne et être mentionnée dans la documentation CRA lorsque cela est justifié.	**OSSTMM3**		
Largement applicable aux systèmes informatiques, aux réseaux et aux applications. Il s'agit également du modèle le plus détaillé, avec des phases explicites pour l'analyse post-exploitation et l'analyse de l'impact sur l'activité.		**PTES**	
Moins normatif quant aux étapes préalables et postérieures à l'engagement, en mettant l'accent sur l'exécution technique.		**NIST SP 800-115**	
Axé sur les applications, avec des conseils spécifiques à l'IoT limités.		**Guide de test OWASP**	
Se concentre sur la cartographie des comportements des adversaires et des TTP. Il ne fournit pas de méthodologie de test structurée, mais améliore les simulations d'attaques et les opérations de sécurité.			**Cadre MITRE ATT&CK**
Concentrez-vous sur les aspects techniques, procéduraux et de conformité des évaluations de sécurité.			**ISSAF**
Équipe rouge axée sur le renseignement, adaptée aux secteurs critiques, mettant l'accent sur des simulations d'attaques réalistes basées sur les menaces émergentes.			**TIBER-EU**

Annexe E : Outils et cadres de test

Catégorie	Outils
Directives réglementaires et de conformité	CRA (loi sur la cyber-résilience), PSD2 (directive révisée sur les services de paiement), SWIFT CSP (programme de sécurité client)
Collecte de renseignements	recon-ng (cadre de reconnaissance), Maltego (exploration de données et analyse de liens), Shodan (analyse Internet à la recherche d'appareils connectés), theHarvester (outil de collecte d'informations), SpiderFoot (collecte automatisée d'informations OSINT)
Sécurité du réseau	Nmap (analyse réseau), Wireshark (analyse de paquets), Nessus (analyse des vulnérabilités), OpenVAS (analyse des vulnérabilités open source)
Sécurité Web et API	Burp Suite (tests de sécurité Web), Checkmarx ZAP (analyse automatisée des vulnérabilités Web), Bruno (tests de sécurité API), Caido
Exploitation et équipe rouge	Metasploit (cadre d'exploitation), BloodHound (analyse des chemins d'attaque Active Directory), Cobalt Strike (outil de red teaming)
Sécurité dans le cloud	ScoutSuite (audit de sécurité multi-cloud), Prowler (évaluation de la sécurité AWS), CloudMapper (visualisation de l'architecture AWS et contrôles de sécurité)
Sécurité de la fabrication	FactorySecure (surveillance de la sécurité des systèmes de fabrication), OTORIO RAM2 (plateforme de sécurité des technologies opérationnelles), Claroty (tests de cybersécurité industrielle)
IA et automatisation	Darktrace (détection des anomalies par apprentissage automatique), Vectra AI (détection des menaces par intelligence artificielle), MITRE CALDERA (émulation

	automatisée des adversaires), SnapAttack (outil automatisé de red teaming)
Analyse du micrologiciel	binwalk (rétro-ingénierie de micrologiciels), Ghidra (suite logicielle de rétro-ingénierie)
Numérisation IoT	Shodan (détection de périphériques et recherche de vulnérabilités), Firmwalker (scanner de configuration de micrologiciels), JTAGulator (identification d'interfaces matérielles)
Interfaces matérielles	USBlyzer (analyse du protocole USB), analyseurs logiques (inspection des signaux numériques), outils UART/série (débogage d'interface série)
Test du protocole	Scapy (outil de manipulation de paquets), Wireshark (analyse de protocoles), CAN-utils (test du protocole Controller Area Network)

Annexe E : Directives de sécurité et meilleures pratiques

Alors que le chapitre 5 décrit les normes et méthodologies de test intégrées à cette méthodologie de test d'intrusion, cette annexe fournit les meilleures pratiques en matière de sécurité et des conseils de mise en œuvre classés par catégorie de produits.

Catégorie de produit	**Normes et directives pertinentes**
Systèmes de gestion des identités, navigateurs, gestionnaires de mots de passe, logiciels de certificats numériques, systèmes SIEM	Norme OWASP ASVS relative à la vérification de la sécurité des applications Norme ISO/IEC 27001 relative à la gestion de la sécurité de l'information Directives CIS relatives à la configuration sécurisée Norme ISVS relative à la vérification de la sécurité de l'Internet des objets
Appareils IoT grand public : routeurs, appareils domestiques intelligents, appareils portables de surveillance de la santé,	ETSI EN 303 701 Cybersécurité pour l'Internet des objets grand public : évaluation de la conformité aux exigences de base ISO/IEC 27400:2022, Cybersécurité. Sécurité et confidentialité de l'Internet des objets. Lignes directrices Guide de bonnes pratiques de l'ENISA pour la sécurité de l'IoT, Cycle de vie sécurisé du développement logiciel RGPD (Règlement général sur la protection des données), ISO/IEC 27701 (Gestion des informations confidentielles), Lignes directrices de la Fondation pour la sécurité de l'IoT
Pare-feu, passerelles de compteurs intelligents	Guide NIST SP 800-82 sur la sécurité des systèmes de contrôle industriels, IEC 62443 Réseaux de communication industriels – Sécurité des réseaux et des systèmes
Secteur manufacturier	ISA/IEC 62443 Sécurité des systèmes d'automatisation et de contrôle industriels ISO 9001 Systèmes de management de la qualité CMMC Certification du modèle de maturité en matière de cybersécurité