CONFIRMATE

Evaluarea CONFormItății, metRici și autoMATizarea conformității cu regulamentul privind reziliEnța cibernetică

Metodologia testelor de penetrare

Data publicării: 2025-08-05

Status: Revizuit

Versiunea: 0.3

Co-funded by the European Union

ECCC EUROPEAN CYBERSECURITY COMPETENCE CENTRE

Proiectul finanțat prin Acordul de finanțare **nr. 101190189** este susținut de Centrul European de Competență în domeniul securității cibernetice. Opiniile și punctele de vedere exprimate sunt însă ale autorului/autorilor și nu le reflectă neapărat pe cele ale Uniunii Europene sau ale Centrului european de competență în domeniul securității cibernetice. Nici Uniunea Europeană, nici autoritatea care acordă finanțarea nu pot fi considerate responsabile pentru acestea.

Lista modificărilor

Versiune	Dată	Descriere	Autor(i)
0.1	21/03/25	Proiectul inițial al metodologiei a fost transmis Parteaenerilor pentru revizuire și feedback.	Cyen
0.2	08/04/25	Revizuiri incorporate pe baza feedback-ului primit de la Parteaeneri	Cyen
0.3	05/08/25	Revizuiri incorporate pe baza feedback-ului primit de la colegi	Cyen

Sincere mulțumiri evaluatorilor, în special Krasen Parvanov (QRTECH), Stijn Horemans (Refracted), Ayman Khalil și Romain Muguet (Red Alert Labs), Peter Kuzmin (Kikimora) și Dominik Holzapfel (Nviso), pentru informațiile esențiale și feedback-ul constructiv, care au contribuit semnificativ la îmbunătățirea acurateței și clarității acestei metodologii.

Metodologia testelor de penetrare privind conformitatea cu CRA a IMM-urilor

Cuprins

1. Referințe bibliografice

- Regulation (EU) 2024/2847 of the European Parliament and of the Council of 23 October 2024 on Horizontal Cybersecurity Requirements for Products with Digital Elements and amending Regulations (EU) No 168/2013 and (EU) No 2019/1020 and Directive (EU) 2020/1828 (Cyber Resilience Act), available here: https://eur-lex.europa.eu/eli/reg/2024/2847/oj/eng
- Institute for Security and Open Methodologies (ISECOM). (2010). Open Source Security Testing Methodology Manual (OSSTMM) Version 3.0, available here: https://www.isecom.org/OSSTMM.3.pdf
- Penetration Testing Execution Standard (PTES) PTES Organization. (n.d.). Penetration Testing Execution Standard (PTES), available here: 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), available here: https://csrc.nist.gov/pubs/sp/800/115/final
- OWASP Foundation. (n.d.). OWASP Web Security Testing Guide (WSTG), available here: https://owasp.org/www-project-web-security-testing-guide/
- MITRE Corporation. (n.d.). MITRE ATT&CK® Framework, available here: https://attack.mitre.org/
- Open Information Systems Security Group (OISSG). (2005). Information Systems Security Assessment Framework (ISSAF) Draft 0.2, available here: https://untrustednetwork.net/files/issaf0.2.1.pdf
- Threat Intelligence-Based Ethical Red Teaming (TIBER-EU) European Central Bank. (2023). TIBER-EU Framework: Threat Intelligence-Based Ethical Red Teaming, available here: https://www.ecb.europa.eu/pub/pdf/other/ecb.tiber_eu_framework.en.pdf
- ETSI TS 103 701 V1.1.1 (2021-08): Cyber Security for Consumer Internet of Things: Conformance Assessment of Baseline Requirements. Available here: https://www.etsi.org/deliver/etsi_ts/103700_103799/103701/01.01.01_60/ts_103701v010101p.pdf

2. Glosar: Acronime, Termeni și Abrevieri

Acronime

OSSTMM:	**Open Source Security Testing Methodology Manual**
OWASP:	**Open Web Application Security Project**
PTES:	**Penetration Testing Execution Standard**
NIST:	**National Institute of Standards and Technology**
SIEM:	**Security Information and Event Management**
IAM:	**Identity and Access Management (contextually inferred)**
API:	**Application Programming Interface**
VPN:	**Virtual Private Network**
SSO:	**Single Sign-On**
IoT:	**Internet of Things**
GDPR:	**General Data Protection Regulation**
ISO:	**International Organization for Standardization**
IEC:	**International Electrotechnical Commission**
CIS:	**Center for Internet Security**
CMMC:	**Cybersecurity Maturity Model Certification**
PSD2:	**Revised Payment Services Directive**
SWIFT CSP:	**Society for Worldwide Interbank Financial Telecommunication Customer Security Programme**

Termeni

Penetration Testing (or pen testing):	Un exercițiu de securitate în care un expert în securitate cibernetică încearcă să găsească și să exploateze vulnerabilitățile unui produs și ale mediului său, inclusiv hardware, software, interfețe și suprafețe de interacțiune cu utilizatorul
Vulnerabilitate:	O slăbiciune sau defect al unui sistem, aplicație sau rețea care poate fi exploatat pentru a compromite securitatea.
Exploit:	O bucată de cod, tehnică sau proces care profită de o vulnerabilitate pentru a provoca un comportament neintenționat într-un sistem.
Threat Actor:	O persoană sau un grup care reprezintă un risc potențial pentru securitatea cibernetică a unei organizații, cum ar fi hackeri, persoane din interior sau concurenți.
Evaluare de risc:	Procesul de identificare a riscurilor care ar putea afecta negativ capacitatea unei organizații de a-și desfășura activitatea.

Audit de securitate:	O evaluare sistematică a nivelului de securitate al unui produs cu elemente digitale, care măsoară conformitatea acestuia cu cerințele tehnice și legislative predefinite, cum ar fi CRA.
Planul de răspuns la incidente:	Un set de instrucțiuni pentru a ajuta organizațiile să detecteze, să răspundă și să se recupereze în urma incidentelor de securitate a rețelelor de calculatoare.
Criptare:	Metoda prin care informațiile sunt convertite într-o reprezentare codificată care ascunde adevăratul sens al informațiilor.
Producător:	O persoană fizică sau juridică care dezvoltă sau fabrică produse cu elemente digitale sau care are produse cu elemente digitale proiectate, dezvoltate sau fabricate și le comercializează sub numele sau marca sa comercială, fie contra cost, fie în scop de monetizare, fie gratuit.
Autentificare multifactor (MFA):	O metodă de autentificare care necesită ca utilizatorul să furnizeze doi sau mai mulți factori de verificare pentru a obține acces la o resursă, cum ar fi o aplicație, un cont online sau o rețea VPN.
Inginerie socială:	Tactica de manipulare, influențare sau înșelare a unei victime pentru a obține controlul asupra unui sistem informatic sau pentru a fura informații personale și financiare
Tactici, tehnici și proceduri (TTP):	Descrie comportamentul unui actor amenințător și un cadru structurat pentru executarea unui atac cibernetic.
Triada CIA (Confidențialitate, Integritate, Disponibilitate):	Un model de securitate a informațiilor conceput pentru a proteja informațiile sensibile împotriva încălcării securității datelor.
Produs cu elemente digitale (PDE):	Un produs care conține sau este interconectat cu software sau firmware și este capabil să colecteze, să transmită sau să prelucreze date. PDE includ atât dispozitive fizice, cât și produse definite de software care sunt introduse pe piață sau puse în funcțiune.

3. Introducere

3.1 Scop și obiective

Acest document descrie modul de gestionare și efectuare a testelor de penetrare asupra produselor cu elemente digitale (PDE) în scopul verificării conformității cu Regulamentul privind reziliența cibernetică (CRA)[1]. Această metodologie completează lacunele practice prin definirea unui flux de lucru pentru testele de penetrare pentru a fi aliniate la cerințele CRA, adaptat la nivelul de risc la care este expus produsul, concentrându-se pe modul în care astfel de teste susțin o declarație de conformitate. Deși CRA nu face referire la testarea de penetrare și nici nu o impune, aceasta rămâne una dintre cele mai puternice tehnici pentru a determina în ce măsură vulnerabilitățile potențiale pot fi exploatate de un atacator. În consecință, un exercițiu de testare de penetrare reușit poate consolida lista de dovezi pentru o declarație de conformitate.

Pe parcursul elaborării acestei metodologii, s-a acordat atenție unui set de produse identificate în anexa A. Aceste produse acoperă diferite niveluri de criticitate definite în Regulamentul privind reziliența cibernetică (CRA). Aceste produse au fost selectate pentru a se asigura că metodologia este aplicabilă și practică în diferite cazuri de utilizare, iar produsele servesc ca un exemplu pozitiv pentru toate instrumentele Confirmate.

Abordarea se bazează pe o metodologie recunoscută (OSSTMM32), care a fost dezvoltată într-o comunitate deschisă și supusă unei evaluări interdisciplinare și inter pares. OSSTMM3 oferă o abordare structurată pentru identificarea vulnerabilităților și corelarea acestora cu posibile atacuri cibernetice, ceea ce permite o evaluare mai precisă a potențialelor riscuri de securitate.

Obiectivele abordării propuse sunt următoarele:

- Să furnizeze o metodă, structurată, de efectuare a testelor de penetrare asupra produselor cu elemente digitale, oferind în același timp flexibilitate în tehnicile utilizate.
- Să definească un set standard de rezultate care pot fi utilizate pentru a susține o cerere de conformitate cu CRA din Parteaea producătorului.
- Să ilustreze utilitatea abordării prin explicarea modului în care aceasta ar putea fi aplicată mai multor produse preluate din Produsele Importante (clasa I și clasa II) și Produsele Critice, astfel cum sunt definite de CRA.

[1] The Cyber Resilience Act, (EU) 2024/2847: https://eur-lex.europa.eu/legal-content/EN/TXT/PDF/?uri=OJ:L_202402847

- Această metodologie nu acoperă evaluările IT generice ale întreprinderilor sau testele de penetrare ale aplicațiilor web independente care nu constituie un PDE, astfel cum este definit de CRA. Metodologiile Web-o și OWASP acoperă adesea active exclusiv web care nu se aliniază cu domeniul de reglementare centrat pe produs cerut aici.

3.2 Public țintă

Publicul țintă al acestui document este reprezentat de producătorii de produse cu elemente digitale, astfel cum sunt definite de CRA.

4. Scop

4.1 Aplicabilitatea pentru IMM-uri

Abordarea propusă în acest document, pentru testele de penetrare, a fost concepută pentru a fi utilizată de întreprinderile mici și mijlocii (IMM-uri). În special, s-au depus toate eforturile pentru a menține o abordare simplă și ușor de înțeles și pentru a reduce la minimum jargonul inutil, astfel încât metodele propuse să fie accesibile întreprinderilor mai mici.

Această metodologie este aplicabilă atât produselor digitale independente, cât și celor integrate, aflate în domeniul de aplicare al CRA, inclusiv dispozitive de consum, controlerelor industriale, gateway-uri inteligente și componentelor critice pentru securitate. Deși este concepută în primul rând pentru testarea înainte de comercializare și în timpul utilizării, ea poate fi aplicată și în fazele incipiente de dezvoltare pentru a identifica punctele slabe din punct de vedere al securității înainte de lansarea pe piață.

4.2 Boundaries and Limitations

Acest document descrie modul de gestionare și executare a testelor de penetrare cu scopul de a susține conformitatea cu cerințele CRA. Acesta nu acoperă strategiile de remediere, controalele de atenuare sau măsurile corective de securitate care pot fi necesare în urma descoperirii unor vulnerabilități în timpul testării.

În plus, spre deosebire de testele de penetrare clasice, care vizează un mediu, testele descrise în acest document vizează un produs. Acestea fiind spuse, acest lucru are sens numai dacă produsul este găzduit într-un mediu adecvat. În acest sens, mediul utilizat pentru găzduirea unui produs pe durata testelor va juca un rol important în determinarea validității rezultatelor finale. Testarea de penetrare în acest context are loc de obicei într-un laborator controlat. Echipa de testare trebuie să furnizeze sau să aprobe mediul de testare, asigurându-se că acesta reflectă condiții de utilizare realiste, fără a slăbi ipotezele de securitate.

4.3 Ipoteze și constrângeri

Principalele ipoteze formulate în abordarea prezentată sunt următoarele:

- Produsul va fi testat într-un „mediu de laborator”, și nu în condiții reale de utilizare.

- Mediul în care este testat produsul va fi cât mai apropiat de mediul țintă (adică mediul în care produsul va fi utilizat).

Deși în această abordare sunt propuse exemple de scenarii de testare, se presupune că producătorii vor adapta aceste scenarii pentru a reflecta natura produsului pe care îl testează.

Constrângerile privind procesul vor fi identificate în cadrul activităților din faza 1. Principala constrângere este că testele trebuie concepute astfel încât să nu aibă un impact negativ asupra operațiunilor entității de testare.

5. Standardele industriei pentru testare

5.1 ETSI EN 303 645

Standardul este însoțit de o specificație de testare (TS 103 701) și un ghid de implementare (TR 103 621) https://www.etsi.org/deliver/etsi_ts/103700_103799/103701/01.01.01_60/ts_103701v010101p.pdf.

ETSI TS 103 701 prevede grupuri de teste structurate și evaluări de conformitate adaptate dispozitivelor IoT destinate consumatorilor. Cazurile de testare acoperă cerințele funcționale, de reziliență, de interfață și de protecție a datelor. În această metodologie, grupurile de teste relevante din TS 103 701 sunt aplicate în mod selectiv categoriilor de produse descrise în anexa A.

ETSI EN 303 645 este standardul european de bază pentru securitatea cibernetică a dispozitivelor IoT destinate consumatorilor. Acesta stabilește prevederi pentru combaterea celor mai frecvente și mai grave vectori de atac. Standardul are ca scop asigurarea unui nivel minim de securitate și servește ca referință pentru reglementările naționale și evaluările de conformitate.

5.2 OSSTMM3

Un audit OSSTMM este o măsurare precisă a securității la nivel operațional, fără presupuneri și dovezi anecdotice. Ca metodologie, este conceput pentru a fi consecvent și repetabil. Fiind un proiect open source, permite oricărui tester de securitate să contribuie cu idei pentru efectuarea de teste de securitate mai precise, mai eficiente și mai ușor de pus în practică. În plus, permite diseminarea liberă a informațiilor și a proprietății intelectuale.

În comparație cu standardele bazate pe conformitate, OSSTMM 3 se concentrează pe validarea securității în lumea reală în mai multe domenii, inclusiv:

- **Rețele de date**: routere, firewall-uri, SIEM, contoare inteligente și dispozitive IoT.
- **Telecomunicații**: securitatea accesului la distanță, configurații VPN
- **Securitate wireless**: vulnerabilități Wi-Fi, standarde de crpitare.

De asemenea, a introdus valorile de evaluare a riscurilor (RAV), care permit echipelor de securitate să cuantifice expunerea la riscuri și să urmărească vulnerabilitățile în timp, îmbunătățind gestionarea riscurilor și luarea deciziilor.

5.3 Ghidul de testare OWASP

Ghidul de testare OWASP este elaborat în cadrul proiectului OWASP Testing Project al Open Web Application Security Project (OWASP). Acesta nu este o metodologie completă care acoperă un test de penetrare integral, ci se concentrează numai pe fazele esențiale ale testării securității aplicațiilor web.

Ghidul oferă o discuție detaliată privind evaluarea securității aplicațiilor web, precum și a stivei de implementare a acestora, inclusiv configurarea serverului web. Acesta urmează o abordare de testare de penetrare de tip black-box și este cuprinzător în ceea ce privește „ce” și „când”. Există, de asemenea, câteva ghiduri privind „cum”, în principal sub forma unei liste de instrumente care pot fi utilizate în fiecare etapă sau sarcină.

5.4 PTES

Standardul de execuție a testelor de penetrare (PTES) este cea mai recentă metodologie de testare a penetrării. A fost dezvoltat de o echipă de specialiști în securitatea informațiilor cu scopul de a răspunde nevoii de a avea un standard complet și actualizat în domeniul testării penetrării.

Pe lângă îndrumarea profesioniștilor din domeniul securității, acesta încearcă să informeze întreprinderile cu privire la ceea ce ar trebui să aștepte de la un test de penetrare și să le ghideze în definirea scopului și negocierea proiectelor de succes. Acesta acoperă „ce” și „când”, dar aprofundează mult mai mult „cum”.

PTES este alcătuit din două părți principale, care se completează reciproc. Liniile directoare Pentest descriu secțiunile și pașii principali ai unui test de penetrare, în timp ce liniile directoare tehnice discută instrumentele și tehnicile specifice care trebuie utilizate în fiecare etapă.

5.5 NIST SP 800-15

NIST 800-115, intitulat „Ghid tehnic pentru testarea și evaluarea securității informațiilor”, este o publicație elaborată pentru a oferi orientări și recomandări pentru efectuarea

evaluărilor de securitate a informațiilor în vederea evaluării nivelului de securitate al sistemelor și rețelelor informatice.

Acesta are scopul de a ajuta organizațiile să înțeleagă diferitele tipuri de evaluări de securitate, să selecteze tehnicile de evaluare adecvate și să conceapă programe de evaluare cuprinzătoare. Liniile directoare pot fi aplicate mai multor organizații, inclusiv agenții federale, organizații din sectorul privat și instituții de învățământ.

Detalii suplimentare privind metodologiile populare de testare penetrantă și compararea acestora sunt disponibile în anexa D: Compararea metodologiilor. În plus, liniile directoare populare în materie de securitate și cele mai bune practici sunt enumerate în anexa E.

6. Metodologie de vârf

Manualul de metodologie pentru testarea securității open source (OSSTMM 3) este metodologia principală utilizată în această abordare de testare a penetrării. Acesta oferă o metodologie pentru un test de securitate aprofundat, denumit în continuare audit OSSTMM.

În timp ce OSSTMM 3 este metodologia a, acest cadru de testare a penetrării integrează și elemente din:

- **ETSI TS 103 701 –** Cazurile de testare relevante din acest standard de testare a conformității sunt încorporate în procesul nostru de execuție a testelor, în special pentru IoT și PDE-urile destinate consumatorilor.
- **OWASP Testing Guide** – Am integrat cazurile de testare OWASP în fazele de recunoaștere și exploatare pentru aplicații web și API-uri. Acest lucru implică respectarea liniilor directoare OWASP pentru identificarea vulnerabilităților, cum ar fi inserarea de comenzi SQL, cross-site scripting și gestionarea nesigură a sesiunilor.
- **PTES** (Penetration Testing Execution Standard) – PTES definește un ciclu de viață structurat al angajamentului, pe care l-am integrat în metodologie. Pentru a ne asigura că fiecare fază are obiective, rezultate și protocoale de comunicare clare, am aliniat fazele OSSTMM3 cu PTES, obținând astfel un proces de testare consistent și repetabil.
- **NIST SP 800-115** – NIST SP 800-115 oferă un cadru solid pentru testarea securității bazate pe riscuri. Fazele de exploatare și analiză a impactului au fost aliniate la liniile directoare ale acestuia pentru a asigura identificarea sistematică a vulnerabilităților, evaluarea cuprinzătoare a riscurilor și raportarea detaliată.

7. Pregătire pentru un test de penetrare

De ce să testați? CRA impune PDE să „aplice teste și revizuiri eficiente și periodice ale securității produsului cu elemente digitale” (anexa I, Parteaea II, punctul 3). Planificarea evaluărilor periodice de securitate asigură monitorizarea continuă și identificarea proactivă a vulnerabilităților, menținând reziliența împotriva amenințărilor emergente.

Cine va efectua testarea? În contextul evaluărilor aliniate la CRA, alegerea unui tester de penetrare (sau a unui furnizor) are un impact direct asupra fiabilității, reproductibilității și relevanței din punct de vedere normativ a rezultatelor. IMM-urile ar putea selecta pentesteri care demonstrează următoarele:

- *Competență tehnică:* Expertiză dovedită în securitatea produselor, sisteme încorporate, testarea firmware-ului și analiza vulnerabilităților software. Furnizorii trebuie să înțeleagă diferențele dintre testarea produselor și evaluările tradiționale ale mediului de întreprindere.
- *Familiaritate cu CRA*: Cunoștințe demonstrabile privind Legea privind reziliența cibernetică, inclusiv cerințele din anexa I Parteaea I și II, și capacitatea de a produce rezultate care să susțină declarațiile de conformitate CRA.
- *Experiență specifică sectorului*: Dacă este relevant, alegeți furnizori cu experiență în domeniul produsului.
- *Garanții legale și etice*: verificați dacă testerii respectă linii directoare etice clare, oferă acoperire de asigurare și execută contracte legale bine definite, inclusiv clauze de răspundere și de prelucrare a datelor.
- *Certificări și acreditări*: sunt utile certificări precum OSCP, OSCE, CREST sau acreditări naționale echivalente la nivel european. Pentru produsele cu risc ridicat sau critice, luați în considerare experiența de certificare TIBER-EU sau Red Team.

Cât timp va dura? Termenele pot varia în funcție de complexitatea produsului, nivelul de cunoștințe (black/grey/white box) și clasificarea CRA (implicită, importantă sau critică), dar o estimare generică a timpului scurs pentru fiecare fază poate fi rezumată după cum urmează:

1. Pregătire (5-10 zile lucrătoare, colaborare între tester și producător), incluzând:
    - Definirea domeniului de aplicare, a obiectivelor și a limitelor testării
    - Corelarea cerințelor din anexa I la CRA
    - Acorduri legale și alinierea părților interesate

- Clientul furnizează documentația tehnică

2. Executarea testării și raportarea (3-10 zile lucrătoare, condusă de tester), incluzând:

- Culegerea de informații, exploatarea și analiza impactului
- Testarea firmware-ului produsului, a interfețelor, a API-urilor și a controalelor de securitate
- Pregătirea raportului și comunicarea

3. Remediere (1-4 săptămâni, condusă de producător)

- Dezvoltarea patch-urilor, remedieri de configurare, control intern al calității
- Acceptarea opțională a riscurilor și actualizarea documentației

4. Retestare (1-2 zile lucrătoare, colaborare între tester și producător)

- Revalidarea problemelor rezolvate
- Confirmări tehnice finale și colectarea probelor

8. Metodologia testelor de penetrare

8.1 Pregătirea și planificarea

Primul pas este definirea tipului de testare cel mai potrivit, luând în considerare maturitatea produsului, riscurile de securitate identificate pentru produs (interne/externe), documentația disponibilă și posibilele vectori de atac (modul în care produsul poate fi exploatat). Testarea poate fi:

- **Black-box**: Testerii nu au cunoștințe interne; simulează un atacator extern.
- **Grey-box**: Testerii au cunoștințe parțiale. Adesea condusă de acces parțial.
- **White-box**: Cunoștințe interne complete (cod sursă, arhitectură); permite testarea aprofundată.

Rețineți că testarea în laborator presupune cunoștințe parțiale sau complete (white-box).

Date de intrare:

- *Identificarea produsului*. Pentru testarea white-box și grey-box: este necesară documentația tehnică, inclusiv: cazuri de utilizare operațională, diagrame de arhitectură, versiunea firmware/software, lista interfețelor - interne și externe (de exemplu, USB, BLE, API-uri, interfață web, porturi, protocoale) sau orice active/componente cunoscute relevante pentru testare, modelul de amenințări (dacă este disponibil). În plus, ar putea fi utile detalii despre evaluările sau auditurile anterioare (dacă sunt disponibile), inclusiv tichetele de erori deschise sau rezultatele testelor nerezolvate.
- Cadre industriale (de exemplu, OSSTMM3, PTES, NIST SP 800-115, OWASP)
- Cerințe de reglementare și documentație de conformitate, inclusiv cerințele din anexa I, Parteaea I și II din CRA (a se vedea anexa B: Cerințe CRA)
- Puncte de contact și protocoale de urgență, inclusiv o procedură de urgență (ce trebuie făcut în cazul unor evenimente neprevăzute, cum ar fi întreruperi ale serviciului) în timpul testării..
- Documentație contractuală (dacă se utilizează testeri externi): contracte de servicii, acorduri de confidențialitate, autorizații de testare și renunțări la răspundere..

Activități:

- *Definirea obiectivelor și stabilirea domeniului de aplicare*: această fază începe cu definirea clară a obiectivelor și a domeniului de aplicare. Accentul se pune pe asigurarea faptului că fiecare sistem este testat pentru funcționalitățile sale unice. Stabilirea domeniului de aplicare este esențială pentru alinierea testării de

penetrare la obiectivele CRA și la atributele unice ale produsului testat. Stabilirea domeniului de aplicare include:

- *Definirea limitelor produsului*: Definiți perimetrul tehnic (software, hardware, API-uri, interfețe) al produsului cu elemente digitale (PDE)..
- *Cartografierea CRA*: Identificați cerințele din anexa I la CRA care se aplică, pe baza clasei de risc a produsului..
- *Informații pentru modelarea amenințărilor*: Incorporarea actorilor de amenințări cunoscuți, a suprafețelor de atac și a contextului produsului.

- *Nivelul de profunzime al testării*: Nivelul de profunzime al testării de penetrare ar corespunde clasificării de criticitate a produsului în conformitate cu Legea privind reziliența cibernetică (CRA).
  - *Testarea produselor de clasă I* implicită și importantă se concentrează, în mod normal, pe serviciile și interfețele expuse extern, mecanismele de control al accesului, protecția datelor în tranzit și identificarea vulnerabilităților cunoscute.
  - *Un produs important din clasa II* necesită o inspecție mai amănunțită a firmware-ului, a mecanismelor de actualizare, a comunicării între dispozitiv și cloud, a fluxurilor de autentificare și a scenariilor de utilizare abuzivă a protocoalelor.
  - Testarea produselor critice ar include validarea securității la nivel de hardware, cum ar fi detectarea manipulării, rezistența la injectarea de erori și verificarea pornirii securizate.
- Considerații juridice, de reglementare și etice: Testarea se efectuează cu respectarea cerințelor legale și de reglementare (de exemplu, confidențialitatea, protecția datelor, legile privind proprietatea intelectuală) și a politicilor interne. Toate autorizațiile necesare sunt obținute, iar restricțiile sunt documentate astfel încât mediul de testare să nu afecteze operațiunile de producție. (a se vedea anexa B: Cerințe CRA, anexa I la CRA, Parteaea I, punctele 1, 2(b), 2(g), 2(j); și anexa I, Parteaea II, punctul 1.)
- Înființarea unui laborator de testare care imită mediul operațional al PDE.

Rezultate pentru fazele ulterioare:

- Document metodologic de nivel înalt
- Formulare de autorizare legală
- Definirea domeniului de aplicare
- Linii directoare privind desfășurarea testării
- Raport de evaluare a riscurilor produsului
- Informarea părților interesate

Rezultate finale:

- Document de planificare și cerințe (D1): Un plan detaliat al proiectului de testare de penetrare, care prezintă domeniul de aplicare, rolurile, obiectivele, autorizarea, calendarul și configurarea laboratorului.
- Evaluarea riscurilor înainte de testare și alinierea părților interesate (D2): Înainte de inițierea testării, trebuie efectuată o evaluare a riscurilor specifice produsului pentru a identifica orice riscuri potențiale pe care testul de penetrare le-ar putea prezenta pentru funcționalitatea, integritatea datelor sau disponibilitatea produsului. Aceasta include evaluarea modului în care testul ar putea afecta interfețele, serviciile și datele critice gestionate de produs. Părțile interesate sunt informate, iar planul de testare de penetrare trebuie să fie aliniat la cerințele lor de securitate (inclusiv anexa B: Cerințe CRA, anexa I Parteaea I CRA) și la toleranța la risc.

8.2 Culegerea de informații și recunoașterea

Date de intrare:

- Definirea domeniului de aplicare
- Raportul de evaluare a riscurilor produsului

Activități:

- Informații din surse deschise și descoperirea activelor: În această fază se utilizează informații din surse deschise pentru a colecta cât mai multe informații posibil. Aceasta include cartografierea amprentei digitale a fiecărui produs și element.
- Profilarea țintelor și analiza peisajului amenințărilor: Este necesară o analiză pentru fiecare activ pentru a determina eventualele vulnerabilități. Peisajul amenințărilor este, de asemenea, analizat pentru a se asigura că scenariile utilizate pentru testarea penetrării sunt realiste și că tacticile adversarilor sunt reflectate în atacurile simulate în timpul testării.
- Elaborarea scenariilor pe baza comportamentului adversarilor: Pe baza informațiilor și datelor colectate, se formulează scenarii de atac specifice.

Rezultate pentru fazele următoare:

- Scenarii de comportament ale adversarilor și profiluri ale țintelor
- Prima versiune a raportului privind vulnerabilitățile (D3): Constatări detaliate din evaluările externe și interne ale produsului, inclusiv evaluări ale riscurilor,

fezabilitatea exploatării și sugestii de remediere, care oferă o imagine cuprinzătoare a vulnerabilităților care afectează produsul în sine.

Rezultate finale:

- Nu există rezultate finalizate în această fază.

8.3 Executarea testelor și exploatarea

Date de intrare:

- Prima versiune a Raportului privind vulnerabilitățile (D3): Constatări detaliate rezultate din evaluările externe și interne ale produsului, inclusiv evaluări ale riscurilor, fezabilitatea exploatării și sugestii de remediere, care oferă o imagine cuprinzătoare a vulnerabilităților care afectează produsul în sine.
- Scenarii de comportament advers și profiluri țintă
- Instrumente de testare (de exemplu, Nessus, Metasploit, Wireshark). Exemple de instrumente și cadre de testare sunt enumerate în anexa E.
- (dacă este disponibil) codul sursă al software-ului.

Activități:

- Identificarea vulnerabilităților și simularea atacurilor: Vulnerabilitățile sunt identificate utilizând tehnici precum analiza statică (SAST) și dinamică (DAST) a securității aplicațiilor sau revizuirea manuală a codului, după caz. Informațiile despre amenințări bazate pe inteligența artificială pot fi utilizate pentru a spori eficiența detectării vulnerabilităților. Fiecare produs este testat în conformitate cu standardele stabilite. Activitățile de evaluare a vulnerabilităților sunt efectuate în mod iterativ pe parcursul executării testelor și sunt utilizate direct pentru generarea raportului D4 privind vulnerabilitățile și servesc ca bază principală pentru evaluarea ulterioară a riscurilor. Scenariile de testare selectate, provenite din ETSI TS 103701, sunt enumerate în anexa C, deoarece acestea ar putea fi executate ca Parteae a testării de penetrare care, pe lângă securitate, ar testa conformitatea cu CRA în conformitate cu alinierea. Activitățile din această fază validează, de asemenea, cerințele de proiectare și protecție securizate aliniate la CRA. A se vedea anexa B: CRA anexa I, Parteaea I, punctele 2(a), 2(b), 2(d), 2(e), 2(j), 2(k); și anexa I, Parteaea II, punctul 3.
- Tehnici de exploatare și emulare a adversarilor: validarea defectelor prin încercarea de a le exploata într-un mediu controlat. Se poate utiliza scanarea asistată de IA, dacă sunt disponibile instrumente. IMM-urile care nu dispun de astfel de instrumente se pot baza pe inspecția manuală sau pe o automatizare

mai simplă. Exemple includ detectarea anomaliilor din jurnalele de înregistrare sau fuzionarea bazată pe învățarea automată. De asemenea, evaluarea situațiilor în care adversarii ar putea ocoli măsurile de securitate și obține acces neautorizat.

- Analiza post-exploatare: evaluarea impactului unui atac reușit, inclusiv escaladarea privilegiilor în sistem și potențiala mișcare laterală către alți utilizatori, componente sau sisteme conectate. Aceasta include determinarea dacă un atacator poate accesa date sensibile, se poate deplasa între module de aplicații sau segmente de infrastructură sau poate compromite servicii critice. Detaliile privind impactul funcțional sunt colectate prin analizarea consecințelor potențiale ale fiecărei vulnerabilități exploatate.
- Rezultatele cazurilor de testare sunt incluse în rezultatele finale ale acestei faze pentru a asigura trasabilitatea activităților de testare în raport cu comportamentele așteptate.

Rezultate pentru fazele următoare:

- Lista vulnerabilităților
- Dovezi de exploatare (proof-of-concept)
- Evaluări preliminare ale riscurilor
- Raport privind fezabilitatea exploatării
- Raport privind simularea tacticii adversarului

Rezultate finale:

- Raport privind vulnerabilitățile (D3): Constatări detaliate din evaluările externe și interne ale produsului, inclusiv evaluări ale riscurilor, fezabilitatea exploatării și sugestii de remediere, care oferă o imagine cuprinzătoare a vulnerabilităților care afectează produsul în sine.

8.4 Analiza impactului și raportarea

Date de intrare:

- Lista vulnerabilităților
- Dovezi de exploatare (proof-of-concept)
- Evaluări preliminare ale riscurilor
- Standarde de evaluare a riscurilor specifice industriei
- Politici de clasificare a datelor.

Activități:

- Evaluarea riscurilor și evaluarea impactului funcțional: Analizarea gravității vulnerabilităților identificate, măsurarea impactului acestora asupra CIA (confidențialitate, integritate sau disponibilitate). Atribuirea unui rating de risc pentru a prioritiza eforturile de remediere. De asemenea, pot fi utilizate modele de evaluare a riscurilor bazate pe IA pentru a îmbunătăți faza de evaluare generală, prin atribuirea de niveluri de risc pe baza informațiilor în timp real privind amenințările și a datelor privind exploatabilitatea. Aceasta include evaluarea conform CRA a integrității datelor, a rezilienței și a răspunsului la vulnerabilități. A se vedea anexa B: CRA anexa I, Parteaea I, punctele 2(e), 2(f), 2(i); anexa I, Parteaea II, punctele 1, 2.
- Documentarea constatărilor și colectarea probelor: Compilarea de rapoarte detaliate care conțin descrieri ale vulnerabilităților, probe tehnice și dovezi de exploatare. Asigurarea faptului că părțile interesate au o înțelegere clară a lacunelor de securitate.
- Indicator de conformitate cu reglementările: Traducerea rezultatelor testelor în termeni de conformitate cu reglementările, prin semnalarea constatărilor legate de cerințele din anexele I și II la CRA enumerate în anexa B. Astfel, se contribuie la un raport de aliniere la conformitatea cu reglementările, care poate fi utilizat pentru a justifica declarația de conformitate a unui producător.
- Recomandări și strategii de remediere aplicabile: Furnizarea de orientări detaliate pentru atenuarea riscurilor identificate. Sugerarea de controale de securitate, modificări de configurare și strategii de remediere pentru a spori reziliența sistemului. A se vedea anexa B: Cerințe CRA

Rezultate pentru fazele următoare:

- Raport de evaluare a riscurilor
- Document cuprinzător cu constatările
- Detalii privind impactul funcțional
- Recomandări de remediere
- Plan de acțiune de remediere prioritizat
- Raport de aliniere la conformitatea cu reglementările

Rezultate finale:

- Recomandări și foaie de parcurs pentru remediere (D5): Recomandări prioritizate cu o foaie de parcurs clară pentru remediere, inclusiv acțiuni pe termen scurt, mediu și lung.

8.5 Urmărirea post-angajament

Date de intrare:

- Rapoarte de remediere
- Configurații actualizate ale sistemului și rezultate ale testelor repetate.

Activități:

- Verificarea eforturilor de remediere și repetarea testelor: Efectuarea de teste repetate pentru a valida remedierea defectelor de securitate. Asigurarea faptului că eforturile de remediere elimină în mod eficient vulnerabilitățile. Activitățile post-test confirmă alinierea la așteptările CRA în ceea ce privește actualizările de securitate și divulgarea informațiilor. A se vedea anexa B: CRA anexa I, Parteaea I, punctele 2(h) și 2(m); și anexa I, Parteaea II, punctele 2, 4, 7 și 8.
- Îmbunătățirea continuă și integrarea lecțiilor învățate: Actualizarea metodologiilor de testare și a politicilor de securitate pe baza constatărilor. Analizele bazate pe inteligența artificială contribuie la îmbunătățirea evaluărilor de securitate viitoare prin utilizarea lecțiilor învățate din testele anterioare. (a se vedea: Anexă: Cerințe CRA, Anexa I la CRA, Parteaea I)
- Dezvăluirea și comunicarea vulnerabilităților: După disponibilitatea actualizărilor de securitate, producătorii trebuie să pregătească și să dezvăluie public detalii despre vulnerabilitățile rezolvate. În cazurile în care dezvăluirea ar introduce un risc nejustificat, publicarea poate fi amânată în mod justificat până la implementarea pe scară largă a patch-urilor (Anexa I la CRA, Parteaea II, punctul 4).

Rezultate finale:

- Raportul testului de penetrare (D5): Un raport tipic de testare de penetrare include un rezumat executiv (prezentare generală la nivel înalt, evaluarea generală a riscurilor, rezultatele testelor și recomandările prioritare), domeniul de aplicare și metoda testării (D1), activitățile, constatările (cu detalii suplimentare, inclusiv vulnerabilitățile (D2) și dovezile de exploatare) și recomandările (D4). Acest document ar putea fi considerat o „revizuire a securității produsului cu elemente digitale” în sensul cerinței CRA din anexa I Parteaea II punctul 3 (Aplicarea unor teste și revizuiri eficiente și periodice ale securității produsului cu elemente digitale).

8.6 Rezultate

Fiecare angajament va produce un set cuprinzător de rezultate concepute pentru a răspunde atât nevoilor tehnice, cât și celor strategice. Pentru orice fază a metodologiei, rezultatele vor fi de două tipuri: (a) rezultate care sunt utilizate ca date de intrare pentru

o fază ulterioară și (b) rezultate ale întregului exercițiu. Rezultatele întregului exercițiu sunt enumerate mai jos;

- Document de planificare și cerințe (D1): un plan detaliat al proiectului de testare penetrantă, care prezintă obiectivele, domeniul de aplicare, rolurile, procedura de urgență, autorizarea, calendarul și configurarea laboratorului.
-
- Evaluarea riscurilor înainte de testare și alinierea părților interesate (D2): o analiză aprofundată a riscurilor potențiale înainte de începerea testării, asigurând alinierea cu părțile interesate în ceea ce privește domeniul de aplicare, prioritățile și obiectivele.
- Raport privind vulnerabilitățile (D3): Constatări detaliate ale evaluărilor externe și interne ale produsului, inclusiv evaluări ale riscurilor, fezabilitatea exploatării și sugestii de remediere, care oferă o imagine cuprinzătoare a vulnerabilităților care afectează produsul în sine.
- Recomandări și plan de remediere (D4): recomandări prioritizate cu un plan clar de remediere, inclusiv acțiuni pe termen scurt, mediu și lung.
- Raport de testare de penetrare (D5): o prezentare generală la nivel înalt pentru părțile interesate fără cunoștințe tehnice, care rezumă principalele constatări și recomandări strategice.

8.7 Exemple de scenarii

Scopul acestei secțiuni este de a oferi exemple ilustrative de scenarii de testare de penetrare, inclusiv cerințele aproximative de resurse și durata probabilă. Aceste scenarii sunt doar orientative și pot varia semnificativ de la un exercițiu la altul.

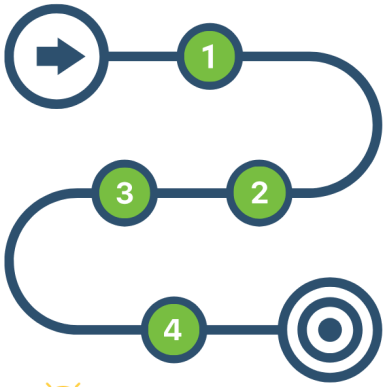
Scenariul 1: Gestionarea identității și a accesului (produs important al CRA: clasa I)

Testing Approach

- **Testing Type:** Grey Box (Basic credentials were provided. Pentester must enumerate internal IAM functions and privileges).
- **Complexity:** Medium (5–15 IAM functions/modules).
- **Effort Estimate:** 8–12 days of work (~15–20 days elapsed).
-

Findings & Impact

- Improper session handling exposed session tokens to unauthorized users.
- Fallback MFA logic allowed bypass using social recovery methods.
- IAM logs did not flag privilege escalation through role manipulation.



Recommendations

- Implement secure session tokens with HttpOnly, Secure and SameSite attributes.
- Enforce strict multi-factor authentication flows with no unverified fallback.
- Enable logging and alerting on privilege elevation attempts and role changes.

Attack Path

1. **Reconnaissance:** Enumerate IAM login endpoints, MFA mechanisms, and session management logic.
2. **Vulnerability Exploitation:** Bypass fallback MFA via social recovery. Hijack admin session through token harvesting.
3. **Impact Analysis & Reporting:** Identify risk of unauthorized access to admin portal and internal configurations.
4. **Follow-Up:** Patch MFA fallback logic and reconfigure session management.

CRA compliance impact

Insecure MFA fallback violates CRA Annex I, Part I, point 2(d): "Ensure protection from unauthorized access by appropriate control mechanisms."

Absence of privilege elevation logging violates CRA Annex I, Part I, point 2(l): "Provide security-related information by recording and monitoring relevant internal activity."

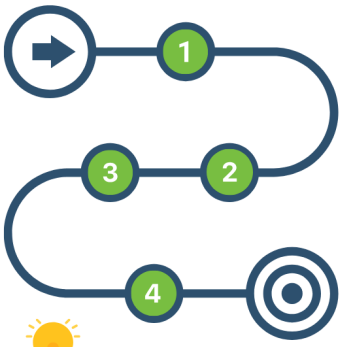
Scenariul 2: Gestionarea informațiilor și evenimentelor de securitate (SIEM) (Produs important al CRA: Clasa II)

Testing Approach

- **Testing Type:** Grey Box (SIEM credentials provided; pentester simulates adversarial inputs and log tampering).
- **Complexity:** High (15–30 log sources, rule sets, and integrations).
- **Effort Estimate:** 12–15 days of work (~20–25 days elapsed).

Findings & Impact

- *SIEM failed to trigger alerts on repeated failed login attempts.*
- *Syslog injection permitted hiding of intrusion logs.*
- *Log integrity checks could be bypassed via payload evasion.*



Recommendations

- *Configure anomaly detection rules for authentication-based thresholds.*
- *Sanitize log inputs to prevent log injection.*
- *Use cryptographic log signing and validation to ensure integrity.*

Attack Path

1. **Reconnaissance:** Review SIEM ingestion points, correlation rules and alert thresholds.
2. **Vulnerability Exploitation:** Inject crafted logs to hide real attacks. Exploit lack of event correlation on failed logins.
3. **Impact Analysis & Reporting:** Evaluate how alert suppression enables persistent access.
4. **Follow-Up:** Harden parsing logic and audit rule sets.

CRA compliance impact

Log tampering without detection violates CRA Annex I, Part I, point 2(l): "Recording and monitoring relevant internal activity."

Alert bypass on repeated login failures breaches CRA Annex I, Part I, point 2(h): "Protect the availability of essential and basic functions… including mitigation against denial-of-service attacks."

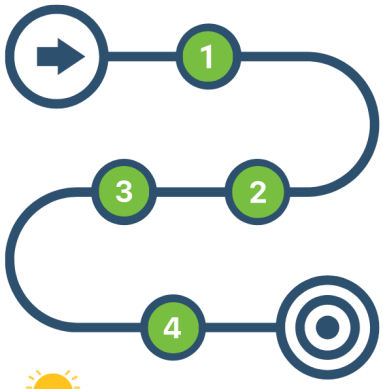
Scenariul 3: Gateway pentru contoare inteligente (produs critic CRA)

Testing Approach

- **Testing Type:** Grey Box (Firmware and interface specs provided; pentester performs protocol and embedded testing).
- **Complexity:** High (Complex embedded systems and proprietary protocols).
- **Effort Estimate:** 15–20 days of work (~25–30 days elapsed).

Findings & Impact

- *Firmware update process accepted unsigned images.*
- *Secure boot validation bypassed via bootloader flaws.*
- *Replay attacks captured and resent valid encrypted communications.*



Recommendations

- *Enforce digital signature checks during firmware installation.*
- *Harden bootloader to validate cryptographic chains of trust.*
- *Include nonces and freshness checks to mitigate replay attacks.*

Attack Path

1. **Reconnaissance:** Identify firmware update endpoints and communication patterns.
2. **Vulnerability Exploitation:** Reuse captured firmware update traffic. Deploy rogue firmware.
3. **Impact Analysis & Reporting:** Demonstrate complete takeover of smart meter gateway logic.
4. **Follow-Up:** Redesign secure boot with cryptographic chain and patch replay exposure.

CRA compliance impact

Missing firmware validation violates CRA Annex I, Part I, point 2(k): "Reduce the impact of an incident using appropriate exploitation mitigation techniques."

Replay attacks exploiting firmware comms breach CRA Annex I, Part I, point 2(e): "Protect the confidentiality of stored or transmitted data by using state-of-the-art mechanisms."

Anexa A: Selecția PDE luată în considerare

Important: Clasa I

- *Sisteme de gestionare a identității*
- *Browsere*
- *Manageri de parole*
- *Software de emitere a certificatelor digitale*
- *Routere*
- *Produse pentru case inteligente*
- *Dispozitive portabile pentru monitorizarea sănătății*
- *SIEM systems Sisteme SIEM*

Important: Clasa II

- *Firewall-uri*

Produse critice

- *Gateway pentru contoare inteligente*

Anexa B: Cerințele CRA

1. Anexa I Partea I – Essential Cybersecurity Requirements

CRA Requirement	CRA Requirement reference
Produsele cu elemente digitale sunt proiectate, dezvoltate și fabricate astfel încât să asigure un nivel adecvat de securitate cibernetică bazat pe riscuri.	Anexa I, Partea I, Punctul 1
(a) Be made available on the market with a secure by default configuration, unless otherwise agreed between manufacturer and business user in relation to a tailor-made product with digital elements, including the possibility to reset the product to its original state	Anexa I, Partea I, Punctul 2 lit. (a)
(b) Be made available on the market with a secure by default configuration, including the ability to reset to the original state.	Anexa I, Partea I, Punctul 2 lit. (b)
(c) să se asigure că vulnerabilitățile pot fi abordate prin actualizări de securitate, inclusiv, după caz, prin actualizări automate de securitate care sunt instalate într-un interval de timp adecvat, activate ca setare implicită, cu un mecanism de neparticipare clar și ușor de utilizat, prin notificarea utilizatorilor cu privire la actualizările disponibile și prin opțiunea de a le amâna temporar;	Anexa I, Partea I, Punctul 2 lit. (c)
(d) să asigure protecția împotriva accesului neautorizat prin mecanisme de control adecvate, inclusiv, dar fără a se limita	Anexa I, Partea I, Punctul 2 lit. (d)

la sistemele de autentificare, de gestionare a identității sau a accesului, și să raporteze privind posibilul acces neautorizat;	
(e) să protejeze confidențialitatea datelor stocate, transmise sau prelucrate în alt mod, cu caracter personal sau de altă natură, de exemplu prin criptarea datelor relevante în repaus sau în tranzit prin mecanisme de ultimă generație și prin utilizarea altor mijloace tehnice;	Anexa I, Partea I, Punctul 2 lit. (e)
(f) să protejeze integritatea datelor stocate, transmise sau prelucrate în alt mod, cu caracter personal sau de altă natură, a comenzilor, a programelor și a configurației împotriva oricărei manipulări sau modificări neautorizate de către utilizator, și să raporteze cu privire la fișierele corupte;	Anexa I, Partea I, Punctul 2 lit. (f)
(g) să prelucreze numai date, cu caracter personal sau de altă natură, care sunt adecvate, relevante și limitate la ceea ce este necesar în legătură cu scopul preconizat al produsului cu elemente digitale (reducerea la minimum a datelor);	Anexa I, Partea I, Punctul 2 lit. (g)
(h) să protejeze disponibilitatea funcțiilor esențiale și de bază, iar după un incident, inclusiv prin reziliență și măsuri de atenuare împotriva atacurilor vizând blocarea accesului la servicii;	Anexa I, Partea I, Punctul 2 lit. (h)
(i) să reducă la minimum impactul negativ al produselor în sine sau al dispozitivelor conectate asupra disponibilității serviciilor furnizate de alte dispozitive sau rețele;	Anexa I, Partea I, Punctul 2 lit. (i)

(j) să fie proiectate, dezvoltate și fabricate de așa manieră încât să se limiteze suprafețele de atac, inclusiv interfețele externe;	Anexa I, Partea I, Punctul 2 lit. (j)
(k) să fie proiectate, dezvoltate și fabricate de așa manieră încât să se reducă impactul unui incident prin utilizarea de mecanisme și tehnici adecvate de prevenire a exploatării vulnerabilităților;	Anexa I, Partea I, Punctul 2 lit. (k)
(l) să furnizeze informații legate de securitate prin înregistrarea și monitorizarea activității interne relevante, inclusiv accesul la date, servicii sau funcții sau modificarea acestora, cu un mecanism de neparticipare pentru utilizator;	Anexa I, Partea I, Punctul 2 lit. (l)
(m) să ofere utilizatorilor posibilitatea de a elimina în mod securizat și cu ușurință, în mod permanent, toate datele și setările și, în cazul în care astfel de date pot fi transferate către alte produse sau sisteme, și să se asigure că acest lucru se realizează în mod securizat.	Anexa I, Partea I, Punctul 2 lit. (m)

2. Anexa I Partea II – Vulnerability Handling Requirements

CRA Requirement	CRA Citation
Să identifice și să documenteze vulnerabilitățile și componentele produselor cu elemente digitale, inclusiv prin întocmirea unei liste a materialelor software într-un format folosit în mod curent și care poate fi citit automat, care să acopere cel puțin dependențele de nivel superior ale produsului;	Anexa I, Partea II, Punctul 1

În ceea ce privește riscurile pe care le prezintă produsele cu elemente digitale, să abordeze și să remedieze fără întârziere vulnerabilitățile, inclusiv prin furnizarea de actualizări de securitate; în cazul în care acest lucru este fezabil din punct de vedere tehnic, noile actualizări de securitate sunt furnizate separat de actualizările de funcționalitate;	Anexa I, Partea II, Punctul 2
Să aplice teste și reexaminări eficace și periodice ale securității produsului cu elemente digitale;	Anexa I, Partea II, Punctul 3
După punerea la dispoziție a unei actualizări de securitate, să partajeze și să publice informații cu privire la vulnerabilitățile remediate, inclusiv o descriere a vulnerabilităților, informații care să permită utilizatorilor să identifice produsul cu elemente digitale afectat, impactul vulnerabilităților, gravitatea acestora și informații clare și accesibile care să ajute utilizatorii să remedieze vulnerabilitățile; în cazuri justificate în mod corespunzător, atunci când producătorii consideră că riscurile de securitate ale publicării depășesc beneficiile în materie de securitate, aceștia pot amâna publicarea informațiilor cu privire la o vulnerabilitate fixă până după ce utilizatorilor li s-a oferit posibilitatea de a aplica corecția relevantă;	Anexa I, Partea II, Punctul 4
Să instituie și să pună în aplicare o politică privind divulgarea coordonată a vulnerabilităților;	Anexa I, Partea II, Punctul 5
Să ia măsuri pentru a facilita schimbul de informații cu privire la potențialele vulnerabilități ale produsului lor cu elemente digitale, precum și cu privire la componentele terților conținute în produsul respectiv, inclusiv prin furnizarea unei adrese de contact pentru raportarea	Anexa I, Partea II, Punctul 6

vulnerabilităților descoperite în produsul cu elemente digitale;	
Să prevadă mecanisme de distribuire securizată a actualizărilor pentru produsele cu elemente digitale, pentru a se asigura că vulnerabilitățile sunt remediate sau atenuate în timp util și, dacă este cazul pentru actualizările de securitate, în mod automat;	Anexa I, Partea II, Punctul 7
Să se asigure că, în cazul în care sunt disponibile actualizări de securitate pentru abordarea problemelor de securitate identificate, acestea sunt difuzate fără întârziere și, cu excepția cazului în care producătorul și furnizorul prin servicii de intermediere online au convenit altfel în legătură cu un produs personalizat cu elemente digitale, gratuit, însoțite de mesaje de consiliere care să ofere utilizatorilor informațiile relevante, inclusiv cu privire la eventualele acțiuni care trebuie întreprinse.	Anexa I, Partea II, Punctul 8

Anexa C: Selectarea grupurilor de testare și a cazurilor de testare ETSI TS 103701 cu corelarea cu cerințele CRA

ID Grup de testare	Test case (conceptual)	Linked CRA requirement ref.
TSO 5.1: Fără parole implicite universale	(5.1-1) Scopul acestui caz de testare este evaluarea conceptuală a mecanismelor de autentificare bazate pe parolă.	Anexa I, Partea I, Punctul 2(d)
	(5.1-2) Scopul acestui caz de testare este evaluarea conceptuală a mecanismelor de generare a parolelor preinstalate.	Anexa I, Partea I, Punctul 2(d)
TSO 5.2: Implementarea unui mijloc de gestionare a rapoartelor privind vulnerabilitățile	(5.2-1) Scopul acestui caz de testare este evaluarea conceptuală a publicării politicii de divulgare a vulnerabilităților.	Anexa I, Partea II, Punctul 5
	(5.2-2) Scopul acestui caz de testare este evaluarea conceptuală a modului în care se acționează asupra vulnerabilităților, a) și confirmarea faptului că sunt asigurate condițiile prealabile pentru implementare, b).	Anexa I, Partea II, Punctul 2
TSO 5.3: Menținerea software-ului actualizat	(5.3-1) Scopul acestui caz de testare este evaluarea conceptuală a posibilității de actualizare a componentelor software în ceea ce privește absența actualizărilor software, a) și a mecanismelor de actualizare b).	Anexa I, Partea II, Punctul 7
	(5.3-2) Scopul acestui caz de testare este evaluarea conceptuală a mecanismului de instalare a actualizărilor în ceea ce privește măsurile adecvate pentru a împiedica un atacator să utilizeze în mod abuziv instalarea actualizărilor pe DUT.	Anexa I, Partea II, Punctul 7

	(5.3-3) Scopul acestui caz de testare este evaluarea conceptuală a mecanismelor de actualizare în ceea ce privește simplitatea pentru utilizator.	Anexa I, Partea I, Punctul 2(c) Anexa I, Partea II, Punctul 8
TSO 5.4: Stocarea în siguranță a parametrilor sensibili de securitate	(5.4-1) Scopul acestui caz de testare este evaluarea conceptuală a stocării sigure a parametrilor sensibili de securitate în ceea ce privește cerințele de securitate (a-c) și completitudinea documentației IXIT (d).	Anexa I, Partea I, Punctul 2(e)
	(5.4-2) Scopul acestui caz de testare este evaluarea conceptuală a stocării rezistente la manipulare a identităților codificate în mod permanent.	Anexa I, Partea I, Punctul 2(e)
TSO 5.5: Comunicarea în siguranță	(5.5-1) Scopul acestui caz de testare este evaluarea conceptuală a criptografiei utilizate pentru mecanismele de comunicare în ceea ce privește utilizarea celor mai bune practici de criptografie (a-c) și vulnerabilitatea la un atac fezabil d).	Anexa I, Partea I, Punctul 2(e)
	(5.5-4) Scopul acestui caz de testare este evaluarea conceptuală a funcționalității dispozitivului prin intermediul unei interfețe de rețea în starea inițializată, în ceea ce privește autentificarea și autorizarea.	Anexa I, Partea I, Punctul 2(d)
TSO 5.7: Asigurarea integrității software-ului	(5.7-1) Scopul acestui caz de testare este evaluarea conceptuală a mecanismelor de pornire securizată ale DUT.	Anexa I, Partea I, Punctul 2(f)
	(5.7-2) Scopul acestui caz de testare este evaluarea conceptuală a mecanismelor de alertă, a) și a mecanismelor de restricționare a comunicării, b) în cazul detectării unei modificări neautorizate a software-ului.	Anexa I, Partea I, Punctul 2(f)
TSO 5.8: Asigurați securitatea datelor cu caracter personal	(5.8-1) Scopul acestui caz de testare este evaluarea conceptuală a criptografiei utilizate pentru comunicarea datelor cu caracter personal între un dispozitiv și un serviciu.	Anexa I, Partea I, Punctul 2(e)

TSO 5.9: Asigurați rezistența sistemelor la întreruperi	(5.9-1) Scopul acestui caz de testare este evaluarea conceptuală a mecanismelor de reziliență în ceea ce privește întreruperile rețelei și ale alimentării cu energie electrică.	Anexa I, Partea I, Punctul 2(h)
	(5.9-3) Scopul acestui caz de testare este evaluarea conceptuală a măsurilor de reziliență pentru mecanismele de comunicare.	Anexa I, Partea I, Punctul 2(h)

Anexa D: Compararea Metodologiilor

Metodologii de testare de penetrare recunoscute pe scară largă în industrie	
Domeniu de aplicare	**Role in this Guide**

	Major	Mediu	Niciunul
Grupuri și proceduri de testare specifice produsului, aliniate la Anexa I a CRA.	**ETSI TS 103 701**		
Prezintă cerințele de bază în materie de securitate cibernetică pentru dispozitivele IoT destinate consumatorilor. În această metodologie, completează TS 103 701 prin definirea poziției de securitate prin proiectare preconizate, care este verificată prin testare.	**ETSI EN 303 645**		
Oferă o metodă structurată de măsurare a nivelului de securitate utilizând indicatori definiți (de exemplu, scoruri RAV). Aplicarea indicatorilor OSSTMM3 poate sprijini urmărirea maturității interne și poate fi menționată în documentația CRA, acolo unde este justificat.	**OSSTMM3**		
Aplicabil pe scară largă la sisteme, rețele și aplicații IT. De asemenea, este cel mai detaliat, cu faze explicite pentru analiza post-exploatare și a impactului asupra activității.		**PTES**	
Mai puțin prescriptiv în ceea ce privește etapele pre/post-testare, concentrându-se pe execuția tehnică.		**NIST SP 800-115**	
Centrat pe aplicații, cu îndrumări specifice IoT limitate.		**OWASP Ghid de testare**	
Se concentrează pe cartografierea comportamentelor adversarilor și a TTP-urilor. Nu oferă o metodologie de testare structurată, dar îmbunătățește simulările de atac și operațiunile de securitate.			**MITRE ATT&CK Framework**
Se concentrează pe aspectele tehnice, procedurale și de conformitate ale evaluărilor de securitate.			**ISSAF**
Red teaming bazate pe informații, adaptate sectoarelor critice, punând accentul pe simulări realiste de atacuri bazate pe amenințări emergente.			**TIBER-EU**

Anexa E: Instrumente și cadre de testare

Categorie	Instrumente
Linii directoare privind reglementarea și conformitatea	CRA (Cyber Resilience Act), PSD2 (Directiva revizuită privind serviciile de plată), SWIFT CSP (Programul de securitate pentru clienți)
Culegerea de informații	recon-ng (cadru de recunoaștere), Maltego (extragerea datelor și analiza legăturilor), Shodan (scanarea internetului pentru dispozitive conectate), theHarvester (instrument de colectare a informațiilor), SpiderFoot (colectare automată OSINT)
Securitatea rețelelor	Nmap (scanare de rețea), Wireshark (analiza pachetelor de trafic), Nessus (scanare a vulnerabilităților), OpenVAS (scanare open-source a vulnerabilităților)
Securitatea web și API	Burp Suite (testare securitate web), Checkmarx ZAP (scanare automată vulnerabilități web), Bruno (testare securitate API), Caido
Exploatarea și Red Teaming	Metasploit (cadru de exploatare), BloodHound (analiză căi de atac Active Directory), Cobalt Strike (instrument red teaming)
Securitate în cloud	ScoutSuite (audit de securitate multi-cloud), Prowler (evaluare de securitate AWS), CloudMapper (vizualizare arhitectură AWS și verificări de securitate)
Securitate în producție	FactorySecure (monitorizare securitate sisteme de producție), OTORIO RAM2 (platformă de securitate tehnologie operațională), Claroty (testare securitate cibernetică industrială)
AI și automatizare	Darktrace (detectarea anomaliilor prin învățare automată), Vectra AI (detectarea amenințărilor bazată pe AI), MITRE CALDERA (emulare automată a adversarilor), SnapAttack (instrument automatizat de red teaming)
Analiza firmware	binwalk (inginerie inversă firmware), Ghidra (suită de inginerie inversă software)

Scanare IoT	Shodan (descoperire dispozitive și căutare vulnerabilități), Firmwalker (scanner configurație firmware), JTAGulator (identificare interfață hardware)
Interfețe hardware	USBlyzer (analiză protocol USB), Logic Analyzers (inspecție semnal digital), instrumente UART/Serial (debugging interfață serială)
Testarea protocoalelor	Scapy (instrument de manipulare a pachetelor), Wireshark (analiza protocoalelor), CAN-utils (testarea protocoalelor rețelei de control)

Anexa E: Linii directoare de securitate și bune practici

În timp ce capitolul 5 descrie standardele și metodologiile de testare integrate în această metodologie de testare a penetrării, prezenta anexă oferă cele mai bune practici în materie de securitate și orientări de implementare organizate pe categorii de produse.

Categorie de produse	**Standarde și linii directoare relevante**
Sisteme de gestionare a identității, browsere, gestionare parole, software pentru certificate digitale, sisteme SIEM	Standardul OWASP ASVS pentru verificarea securității aplicațiilor ISO/IEC 27001 Managementul securității informației Ghidul CIS pentru configurarea securizată Standardul ISVS pentru verificarea securității obiectelor conectate la internet
Dispozitive IoT pentru consumatori: routere, dispozitive inteligente pentru casă, dispozitive portabile pentru monitorizarea sănătății,	ETSI EN 303 701 Securitate cibernetică pentru obiectele conectate la internet destinate consumatorilor: evaluarea conformității cu cerințele de bază ISO/IEC 27400:2022, Securitate cibernetică. Securitatea și confidențialitatea obiectelor conectate la internet. Ghid ENISA Ghid de bune practici pentru securitatea IoT, ciclul de viață al dezvoltării software-ului securizat GDPR (Regulamentul general privind protecția datelor), ISO/IEC 27701 (Gestionarea informațiilor confidențiale), Linii directoare ale fundației pentru securitatea IoT
Ffirewall-uri, gateway-uri pentru contoare inteligente	NIST SP 800-82 Ghid pentru securitatea sistemelor de control industrial, IEC 62443 Rețele de comunicații industriale – Securitatea rețelelor și a sistemelor
Sectorul producției	ISA/IEC 62443 Securitatea sistemelor de automatizare și control industrial ISO 9001 Sisteme de management al calității CMMC Certificarea modelului de maturitate în domeniul securității cibernetice