PENTESTERRA

CYBER RESILIENCE ACT GAP ASSESSMENT

I Tuoi Prodotti Digitali Sono Pronti per il CRA?

Gap assessment sui 24 controlli del Cyber Resilience Act - requisiti di sicurezza by-design e gestione delle vulnerabilità - per produttori di hardware e software venduti nell'UE.

COS'È, IN BREVE

Copre i requisiti essenziali di cybersicurezza e gestione delle vulnerabilità dell'Annex I del CRA. Gli obblighi di segnalazione a ENISA/CSIRT si applicano dall'11 settembre 2026, i requisiti essenziali dall'11 dicembre 2027 - il lavoro di design e processo (SBOM, policy CVD, meccanismo di update) richiede tempo reale.

24
Controlli CRA coperti (Annex I)

2027
Scadenza dei requisiti essenziali di cybersicurezza

UE
Produttori di prodotti con elementi digitali

LA SITUAZIONE OGGI

CHI SEI

Sei il responsabile prodotto o sicurezza di un'azienda che produce hardware o software con elementi digitali destinati al mercato UE, e deve prepararsi agli obblighi del Cyber Resilience Act.

COSA È SUCCESSO

Le scadenze del CRA si avvicinano (2026 per la segnalazione, 2027 per i requisiti essenziali), e SBOM, policy di divulgazione delle vulnerabilità e meccanismo di aggiornamento non sono ancora strutturati.

PERCHÉ FA MALE

I requisiti CRA richiedono lavoro di design e processo che non si improvvisa a ridosso della scadenza - SBOM e gestione delle vulnerabilità vanno costruiti nel prodotto, non aggiunti dopo.

DOVE VUOI ARRIVARE

STATO DESIDERATO

Vuoi sapere, controllo per controllo, cosa è soddisfatto, cosa è parziale e cosa manca - con un'evidenza tecnica reale allegata a ogni risposta, non una dichiarazione ottimistica che nessuno ha verificato.

LA SOLUZIONE

Il Cyber Resilience Act Gap Assessment di Pentesterra: una valutazione strutturata su tutti i controlli, con compilazione automatica dei controlli tecnici a partire da scansioni di vulnerabilità, penetration test, OSINT e monitoraggio dell'esposizione esterna, dove l'evidenza esiste.

PERCHÉ È DIVERSO

Non stai comprando l'ennesimo questionario di autovalutazione, e non stiamo parlando di un parere legale. Stai lavorando con [NOME AZIENDA] - fornitore certificato, italiano, con quasi 20 anni di storia nel settore della sicurezza informatica. Probabilmente ci conosci già, o conosci qualcuno - un collega, un fornitore, un concorrente - che è già stato nostro cliente. E il gap assessment non si ferma a una checklist cartacea: i controlli tecnici vengono auto-compilati dall'evidenza già raccolta, con mappatura cross-standard verso gli altri 12 framework supportati dalla piattaforma, così un secondo audit non riparte da zero.

PROVA CONCRETA

Il risultato è un report PDF completo, pronto da consegnare, con copertura di tutti i controlli e riferimento diretto alla base normativa. Se emergono gap, ti proponiamo le misure aggiuntive per colmarli: vulnerability assessment, penetration test di rete o applicativo, formazione e simulazioni di phishing.

COSA INCLUDE DAVVERO

Non una checklist generica - i controlli reali di Cyber Resilience Act, raggruppati come li vedrai nella piattaforma.

Annex I Parte I: Sicurezza by-design

I requisiti essenziali di cybersicurezza del prodotto.

- Assenza di vulnerabilità sfruttabili conosciute alla consegna
- Configurazione sicura di default
- Protezione dei dati trattati dal prodotto

Annex I Parte II: Gestione delle vulnerabilità

Il processo che continua dopo il rilascio del prodotto.

- Identificazione e documentazione dei componenti (SBOM)
- Gestione e correzione delle vulnerabilità
- Meccanismo di aggiornamento sicuro

Art. 11 Segnalazione e Art. 13 Documentazione

Gli obblighi verso ENISA/CSIRT e la documentazione tecnica.

- Segnalazione di vulnerabilità sfruttate attivamente
- Segnalazione di incidenti con impatto sulla sicurezza
- Documentazione tecnica del prodotto

Preparazione per le scadenze 2026-2027

Il lavoro di design richiede tempo reale, non si improvvisa.

- Roadmap verso la conformità entro dicembre 2027
- Gap assessment su SBOM e policy CVD esistenti
- Priorità sui componenti a rischio più alto

COSA RICEVI

- ✓ Una matrice di controllo esportabile in XLSX, con lo stato di ogni singolo controllo
- ✓ Un gap report editabile in DOCX, pronto per il tuo auditor o il tuo consiglio
- ✓ Compilazione automatica dei controlli tecnici dall'evidenza già raccolta dalla piattaforma
- ✓ Verifica di applicabilità guidata per settore, paese e dimensione aziendale
- ✓ Mappatura cross-standard verso gli altri 12 framework supportati - una risposta, riusata su più standard
- ✓ Un pacchetto per l'auditor in un click: questionario, evidenza tecnica e gap report insieme
- ✓ Raccomandazioni di remediation prioritizzate per i gap trovati

COME FUNZIONA

1

Definiamo il perimetro

Ambito dell'assessment, sistemi e processi coinvolti - stabiliamo insieme lo scope.

2

Raccogliamo l'evidenza

Compiliamo automaticamente i controlli tecnici dall'evidenza già raccolta dalla piattaforma.

3

Completiamo il questionario

I controlli non tecnici vengono verificati con il tuo team.

4

Ti consegniamo il report

Un PDF completo con i gap trovati e le azioni da intraprendere.

Scopri quanto sei pronto per Cyber Resilience Act

Un report completo, pronto da presentare a clienti, auditor o al tuo consiglio di amministrazione.

Richiedi il tuo Cyber Resilience Act Gap Assessment →

info@pentesterra.com · pentesterra.com/solutions/compliance