PENTESTERRA

NIST CSF 2.0 GAP ASSESSMENT

Le Tue 6 Funzioni di Cybersicurezza Sono Davvero Coperte?

Gap assessment sulle 106 sottocategorie del NIST Cybersecurity Framework 2.0, lungo le 6 funzioni Govern, Identify, Protect, Detect, Respond, Recover.

COS'È, IN BREVE

Copre tutte le 106 sottocategorie del NIST CSF 2.0 nelle 6 funzioni (GV Govern, ID Identify, PR Protect, DE Detect, RS Respond, RC Recover) e 22 categorie. Le sottocategorie tecniche sono auto-compilate dall'evidenza delle tue scansioni.

106

Sottocategorie NIST CSF 2.0 coperte

6

Funzioni: Govern, Identify, Protect, Detect, Respond, Recover

Volontario

Framework di riferimento richiesto sempre più spesso da clienti e assicuratori

LA SITUAZIONE OGGI

CHI SEI

Sei il CISO di un'azienda che usa (o vuole adottare) il NIST CSF come framework di riferimento per la propria postura di cybersicurezza - volontario, ma sempre più richiesto come baseline.

COSA È SUCCESSO

Un board, un assicuratore cyber o un cliente enterprise chiede una mappatura della tua postura rispetto al NIST CSF, non solo una lista di strumenti installati.

PERCHÉ FA MALE

Senza una mappatura reale, 'seguiamo il NIST CSF' resta un'affermazione, non una prova - e un assicuratore o un cliente lo nota.

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 NIST CSF 2.0 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 NIST CSF 2.0, raggruppati come li vedrai nella piattaforma.

Govern e Identify

Le due funzioni che stabiliscono strategia e visibilità sul rischio.

- Strategia di gestione del rischio di cybersicurezza
- Inventario di asset, dati e fornitori
- Ruoli, responsabilità e politiche

Protect

Le salvaguardie per limitare o contenere un evento di cybersicurezza.

- Gestione identità e controllo accessi
- Formazione e consapevolezza
- Sicurezza dei dati e della piattaforma

Detect

Le attività per scoprire tempestivamente eventi anomali.

- Monitoraggio continuo della sicurezza
- Analisi degli eventi avversi

Respond e Recover

Cosa fare durante e dopo un incidente.

- Gestione e comunicazione degli incidenti
- Pianificazione ed esecuzione del ripristino

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 NIST CSF 2.0

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

Richiedi il tuo NIST CSF 2.0 Gap Assessment →

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