PENTESTERRA

EXTERNAL EXPOSURE ASSESSMENT

La Tua Azienda È Già Compromessa?

Una valutazione dell'esposizione esterna (cyber) - superficie d'attacco, indicatori di compromissione e interesse degli attaccanti - senza installare nulla sulla tua infrastruttura.

COS'È UN EXTERNAL EXPOSURE ASSESSMENT, IN BREVE

È l'analisi di tutto ciò che è visibile dall'esterno della tua organizzazione - domini, servizi, credenziali trapelate, menzioni su forum criminali - incrociato in continuo con una base di threat intelligence aggiornata, per capire non solo cosa è esposto, ma se sei già nel mirino o già compromesso.

Agentless
Nulla da installare sulla tua infrastruttura o su quella dei fornitori

24/7
Ricontrollo automatico ad ogni aggiornamento della threat intel

1 Record
Ogni evidenza di ogni modulo, aggregata su una sola azienda

LA SITUAZIONE OGGI

CHI SEI

Sei il CISO, il responsabile rischio fornitori o il CTO di un'azienda che deve sapere se la propria organizzazione - o un fornitore critico - è già esposta o compromessa, prima che diventi una notizia.

COSA È SUCCESSO

Un fornitore ha fatto notizia per una violazione, o un cliente sta chiedendo prova della tua postura di sicurezza prima di firmare. Senza visibilità su cosa sia realmente esposto, un sottodominio dimenticato o una credenziale trapelata può diventare il punto d'ingresso di un ransomware.

IL PROBLEMA

Non sai, con certezza, cosa sia visibile dall'esterno della tua organizzazione oggi - né se qualche indicatore di compromissione sia già emerso su un forum criminale o in un leak-site ransomware. Una revisione manuale o un questionario fornitore arriva sempre troppo tardi.

PERCHÉ FA MALE

Un sottodominio dimenticato, una credenziale di un dipendente trapelata in un infostealer log, una menzione su un forum criminale - questi sono i segnali che un questionario fornitore non cattura mai, ma che un attaccante trova per primo. Un cliente, un assicuratore cyber o un auditor possono chiedere prova di una valutazione recente prima di firmare.

DOVE VUOI ARRIVARE

STATO DESIDERATO

Vuoi sapere, con prova concreta, cosa è visibile ed eventualmente già compromesso della tua organizzazione - o di un fornitore critico - senza aspettare l'autorizzazione per una scansione attiva o un pentest.

LA SOLUZIONE

Un **External Exposure Assessment**: mappatura della superficie d'attacco, correlazione con indicatori di compromissione e leak-site ransomware, segnale di menzione su darknet/forum criminali, e un record unico che aggrega l'evidenza di ogni altro modulo Pentesterra su quella azienda.

PERCHÉ È DIVERSO

Non stai comprando l'ennesimo scanner passivo che elenca porte aperte. 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. Molti dei tuoi concorrenti diretti si stanno già rivolgendo a noi. E puoi importare 50.000+ aziende in un unico batch - un intero settore, un portafoglio fornitori, un paese: ogni azienda tracciata viene ricontrollata automaticamente ogni volta che la base di threat intelligence si aggiorna, non solo quando qualcuno si ricorda di rilanciare una scansione.

PROVA CONCRETA

Il risultato è un report PDF completo, pronto da consegnare, con ogni esposizione e indicatore di compromissione documentato. Se emergono gap più ampi, ti proponiamo le misure aggiuntive per colmarli: vulnerability assessment, penetration test, revisione DevGuard del codice, formazione anti-phishing.

50.000+

Aziende analizzabili in un unico batch, per chi valuta fornitori su scala

Passivo

Nessuna autorizzazione richiesta per iniziare

Verificato

Ogni compromissione confermata da un analista prima di essere mostrata

COSA INCLUDE DAVVERO

Non solo porte aperte - superficie d'attacco, segnali di compromissione e conformità, incrociati in continuo con una threat intelligence viva.

Superficie d’attacco, verificata passivamente

Domini e servizi controllati contro le classi di attacco più comuni, senza scansioni invasive.

- Igiene DNS/email, TLS, header di sicurezza, cookie, fingerprinting WAF/CDN/cloud
- Controlli opzionali semi-attivi in sicurezza (esposizione portali VPN/firewall) - mai attivi di default
- Stesso motore per i tuoi domini e per quelli dei fornitori o prospect

Segnali di compromissione e interesse degli attaccanti

Non solo 'una porta è aperta' - l'azienda è già compromessa, o nel mirino attivo di un attaccante.

- Relay di posta aperto, suscettibilità al phishing, indicatori malware/C2 noti
- Esposizione di credenziali e sessioni dei dipendenti da infostealer log
- Correlazione con leak-site ransomware e breach news, verificata da un analista
- Segnale di menzione su darknet e forum criminali

Un’azienda, le evidenze di ogni modulo

Un'unica scheda aziendale che aggrega l'evidenza raccolta da tutto il resto della piattaforma.

- Copertura per modulo mostrata esplicitamente: valutato, non ancora valutato, mai vuoto in silenzio
- Accesso diretto dal riepilogo azienda all'evidenza del modulo sottostante
- I finding di Web Pentest e Vulnerability Management alimentano il punteggio di esposizione

Monitoraggio continuo, non un report puntuale

Uno scan è una fotografia; la threat intelligence si muove ogni giorno.

- Ricontrollo automatico su ogni azienda tracciata ad ogni aggiornamento della base di threat intel
- Notifica immediata quando un nuovo indicatore di compromissione corrisponde a un'azienda monitorata
- Base compliance generata dall'evidenza raccolta, non da un questionario auto-dichiarato

PENTESTERRA

EXTERNAL EXPOSURE ASSESSMENT

COSA RICEVI

- ✓ Un report PDF completo con ogni esposizione e indicatore di compromissione documentato
- ✓ Mappatura della superficie d'attacco esterna, agentless
- ✓ Correlazione con leak-site ransomware, breach news e forum criminali
- ✓ Base compliance generata dall'evidenza realmente raccolta
- ✓ Executive summary pronto per il tuo consiglio o per un cliente enterprise

COME FUNZIONA

1

Definiamo il perimetro

La tua azienda, un fornitore, o un intero portafoglio - stabiliamo insieme lo scope.

2

Mappiamo l'esposizione

Domini, servizi, credenziali trapelate, presenza su forum criminali.

3

Verifichiamo i segnali

Ogni indicatore di compromissione è confermato da un analista prima di essere mostrato.

4

Ti consegniamo il report

Un PDF completo con i rischi prioritizzati e le azioni da intraprendere.

Scopri cosa è già visibile - o compromesso - della tua azienda

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

Richiedi il tuo External Exposure Assessment →

info@pentesterra.com · pentesterra.com/external-exposure-assessments