PENTESTERRA

SUPPLY CHAIN EXPOSURE

I Tuoi Fornitori Sono Già Compromessi?

Vendor risk scorato senza questionari - evidenza esterna osservata, non autovalutazioni. Stesso motore di External Exposure Assessment, applicato alla tua supply chain.

COS'È, IN BREVE

È la valutazione del rischio di fornitori e terze parti basata su evidenza esterna oggettiva - 6 livelli di segnali osservati, dalla superficie d'attacco alla presenza su forum criminali - senza questionari e senza bisogno della cooperazione del fornitore.

0	24/7	NIST CSF+
Questionari inviati - ogni segnale è osservato esternamente	Ricontrollo continuo a ogni aggiornamento della threat intel	Finding mappati sul tuo reporting di rischio e compliance

LA SITUAZIONE OGGI

CHI SEI

Sei il responsabile rischio fornitori, procurement o sicurezza di un'azienda che deve valutare l'esposizione dei propri fornitori e terze parti senza dipendere da questionari auto-dichiarati.

COSA È SUCCESSO

Un questionario fornitore è tornato pulito - ma i questionari sono auto-dichiarati. Un fornitore compromesso senza connessione di rete diretta può comunque costarti la violazione: credenziali condivise, accesso SaaS condiviso, un laptop infetto.

PERCHÉ FA MALE

Il tuo ultimo incidente con un fornitore probabilmente non è iniziato con una risposta 'no' nel questionario - i questionari misurano intenzioni dichiarate, non esposizione reale.

DOVE VUOI ARRIVARE

STATO DESIDERATO

Vuoi sapere, con evidenza oggettiva, quali fornitori sono davvero esposti o già compromessi - non solo quali hanno risposto bene a un questionario.

LA SOLUZIONE

Un servizio di Supply Chain Exposure Assessment: 6 livelli di evidenza esterna osservata - superficie d'attacco, igiene TLS/DNS, sicurezza web/email, monitoraggio darknet, monitoraggio continuo, mappatura compliance - senza cooperazione richiesta dal fornitore.

PERCHÉ È DIVERSO

Non stai comprando l'ennesimo questionario fornitore da far compilare. 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 che è già stato nostro cliente. E ogni fornitore tracciato viene ricontrollato automaticamente a ogni aggiornamento della base di threat intelligence - non solo quando qualcuno ricorda di reinviare un questionario. La stessa base di evidenza si riusa nei tuoi assessment di compliance.

PROVA CONCRETA

Il risultato è un report PDF completo, pronto da consegnare, con l'esposizione di ogni fornitore documentata su 6 livelli di evidenza. Se emergono gap, ti proponiamo le misure aggiuntive: external exposure assessment, vulnerability assessment, penetration test.

6 Livelli

Superficie, TLS/DNS, web/email, darknet, monitoraggio, compliance

Nessuna Cooperazione

Il fornitore non deve fare nulla

Scala

Da un singolo fornitore a un intero portafoglio

COSA INCLUDE DAVVERO

6 livelli di evidenza esterna osservata - non un questionario da far compilare al fornitore.

Mappatura della superficie d'attacco

Domini, IP risolti, range CIDR - rivela cosa espone davvero un fornitore su internet, non solo ciò che dichiara.

- Enumerazione completa di domini e sottodomini
- Scoperta di IP risolti e range CIDR
- Fingerprinting del provider cloud e hosting

Igiene TLS/DNS e sicurezza web/email

Configurazione certificati, autenticazione DNS/email, header di sicurezza, fingerprinting WAF/CDN.

- Rilevamento crittografia debole e certificati scaduti
- Postura SPF/DKIM/DMARC
- Probing di relay di posta aperti
- Verifica presenza WAF/CDN

Monitoraggio darknet e threat-actor

La stessa base di threat intel usata per i tuoi domini, applicata a ogni fornitore tracciato.

- Segnale di menzione su darknet/forum criminali per fornitore
- Correlazione con malware noti e infrastrutture C2
- Correlazione con leak-site ransomware e breach news, verificata da un analista

Monitoraggio continuo e mappatura compliance

Il rischio fornitori non si congela il giorno dell'onboarding.

- Ricontrollo automatico di ogni fornitore a ogni aggiornamento threat feed
- Notifica immediata su nuovo indicatore di compromissione
- Categorie di finding allineate a NIST CSF
- Export dell'evidenza per fornitore in un click

PENTESTERRA

SUPPLY CHAIN EXPOSURE

COSA RICEVI

- ✓ Un report PDF completo con l'esposizione di ogni fornitore su 6 livelli di evidenza
- ✓ Mappatura della superficie d'attacco esterna di ogni fornitore
- ✓ Correlazione con leak-site ransomware, breach news e forum criminali
- ✓ Mappatura delle categorie di finding su NIST CSF
- ✓ Monitoraggio continuo con notifica su nuovi indicatori di compromissione

COME FUNZIONA

1

Carichiamo la lista fornitori

Da un singolo fornitore a un intero portafoglio - nessuna cooperazione richiesta.

2

Raccogliamo l'evidenza

6 livelli di segnali osservati esternamente, in automatico.

3

Verifichiamo i segnali

Ogni indicatore di compromissione è confermato da un analista.

4

Ti consegniamo il report

Un PDF completo con i rischi prioritizzati per fornitore.

Scopri quali fornitori sono già esposti o compromessi

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

Richiedi il tuo Supply Chain Exposure Assessment →

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