PENTESTERRA

OSINT INTELLIGENCE

Conosci il Tuo Bersaglio Prima di un Attaccante?

Intelligence OSINT su aziende e persone - raccolta passiva, riutilizzata in phishing, pentest e reporting, non un report fine a sé stesso.

COS'È, IN BREVE

È la raccolta passiva di informazioni pubblicamente disponibili su un'azienda e le persone che ci lavorano - dominio, stack tecnologico, superficie esposta, ruoli, interessi pubblici (opt-in) - senza bisogno di permesso per scansionare. Alimenta direttamente phishing simulation, scope del pentest e il contesto di business-impact nel report finale.

Passivo

Nessuna scansione attiva, nessun permesso richiesto

Azienda + Persone

Fino al profilo approfondito per singola persona

Bulk

Migliaia di aziende caricabili e monitorate

LA SITUAZIONE OGGI

CHI SEI

Sei il responsabile sicurezza, OSINT o pentest di un'azienda che deve raccogliere il contesto pubblico su un bersaglio - proprio o di terzi - prima di un pentest, un'acquisizione o una revisione fornitori.

COSA È SUCCESSO

Un pentest, un'acquisizione o una revisione fornitori è in arrivo, e nessuno ha ancora raccolto ciò che è pubblicamente noto sul bersaglio.

PERCHÉ FA MALE

Gli attaccanti assemblano già questo quadro a mano. Se il tuo team non lo fa per primo, il sottodominio esposto o la credenziale trapelata emergono in un incident report, non in una valutazione preventiva.

DOVE VUOI ARRIVARE

STATO DESIDERATO

Vuoi un profilo unico e riutilizzabile - non informazioni sparse tra tool diversi che nessuno mette mai insieme.

LA SOLUZIONE

Un servizio di OSINT Intelligence: profilo aziendale (stack tecnologico, superficie esposta, contesto business) e intelligence sulle persone (ruoli, contesto professionale, interessi pubblici opt-in), raccolti passivamente e riutilizzati nel resto della valutazione.

PERCHÉ È DIVERSO

Non stai comprando l'ennesimo tool OSINT che genera una lista di domini. 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 gli interessi personali e le attività pubbliche raccolte qui non sono un dettaglio laterale - sono la leva più efficace per il realismo di una simulazione di phishing: un pretesto costruito su un intervento a una conferenza o un progetto personale converte in modo molto diverso da un'email generica.

PROVA CONCRETA

Il risultato è un report PDF completo con il profilo aziendale e delle persone raccolto, riutilizzabile per il resto della valutazione. Se emergono gap più ampi, ti proponiamo le misure aggiuntive: phishing simulation, vulnerability assessment, penetration test.

Riutilizzabile

Alimenta phishing, pentest e reporting

Bulk + Monitoraggio

Ricontrollo automatico a ogni aggiornamento KB

Opt-in

Interessi personali raccolti solo con consenso

COSA INCLUDE DAVVERO

Non una lista di domini - un profilo aziendale e personale riutilizzabile in tutta la piattaforma.

Intelligence a livello aziendale

Un profilo per organizzazione: cosa fa, stack tecnologico probabile, infrastruttura e superficie d'attacco, contesto business/regolatorio.

- Contesto business, prodotti, stack tecnologico probabile
- Domini, sottodomini, range CIDR, footprint cloud
- Segnali pubblici: leak, menzioni dark-web, interesse di threat actor
- Un record aziendale deduplicato, aggiornato a ogni ciclo

Intelligence sulle persone

Chi sono le persone, che ruoli ricoprono, e il contesto professionale pubblico intorno a loro.

- Ruoli, anzianità, struttura organizzativa
- Contesto professionale, interessi personali e footprint social pubblico (opt-in)
- Email e dati identitari collegati al record aziendale
- Profilazione approfondita on-demand per individui di alto valore nominati

Riutilizzabile, non un report fine a sé stesso

La stessa intelligence alimenta phishing, pentest e reporting.

- Alimenta direttamente la progettazione degli scenari di phishing
- Informa lo scope del pentest, lo stack probabile, i percorsi d'attacco
- Aggiunge contesto di business-impact ai finding
- Condivisa tra moduli, non isolata per singola valutazione

Scoperta e monitoraggio su scala

Aggiungi aziende in blocco, scopri entità collegate, tienile monitorate.

- Caricamento in blocco e scoperta aziende
- Ricontrollo quasi in tempo reale a ogni aggiornamento intelligence
- Monitoraggio e alert per le organizzazioni tracciate
- Adatto a due-diligence fornitori, portafoglio e M&A

PENTESTERRA

OSINT INTELLIGENCE

COSA RICEVI

- ✓ Un report PDF completo con il profilo aziendale e delle persone raccolto
- ✓ Superficie d'attacco, stack tecnologico e contesto business dell'azienda
- ✓ Contesto professionale e interessi pubblici (opt-in) delle persone chiave
- ✓ Intelligence riutilizzabile per phishing simulation, pentest e reporting
- ✓ Monitoraggio continuo con alert su nuova esposizione

COME FUNZIONA

1

Definiamo il perimetro

Un'azienda, un fornitore, o un intero portafoglio - stabiliamo insieme lo scope.

2

Raccogliamo passivamente

Nessuna scansione attiva, nessun permesso richiesto per iniziare.

3

Costruiamo il profilo

Azienda e persone chiave, con interessi pubblici raccolti solo con consenso.

4

Ti consegniamo il report

Un PDF completo, riutilizzabile nel resto della tua valutazione.

Scopri cosa è già pubblicamente noto sul tuo bersaglio

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

Richiedi la tua OSINT Intelligence →

info@pentesterra.com · pentesterra.com/osint