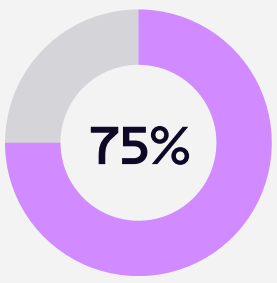
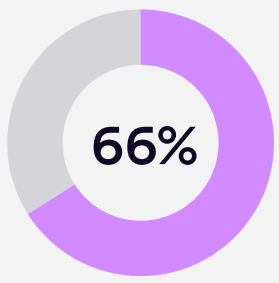
HADRIAN

Guida al ROI sulla Sicurezza Offensiva

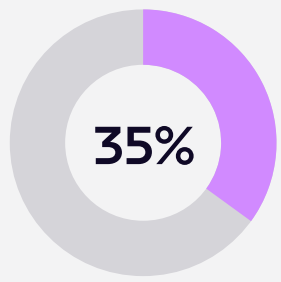
La sicurezza offensiva integra e valida gli investimenti esistenti in cybersicurezza identificando eventuali lacune nei controlli esistenti. Le analisi dimostrano che i cybersecurity manager stanno investendo sempre più in questo tipo di approccio per identificare prontamente i rischi e rimediarvi proattivamente.



L'aumento dei rischi sconosciuti sta spingendo il **75,2%** delle organizzazioni a migliorare le proprie pratiche di sicurezza offensiva.[1]



Gli accessi da remoto e le applicazioni connesse a internet hanno rappresentato rispettivamente il 39% e il 27% dei vettori di accesso iniziale nella prima metà del 2023.[2]



Il **35%** delle organizzazioni, a seguito di una violazione, investe in sicurezza offensiva, rendendola il quarto investimento più comune.[3]

I metodi tradizionali di sicurezza offensiva, come i penetration test manuali, la scansione delle vulnerabilità e la gestione della superficie di attacco, possono rivelarsi inefficaci, lasciando inosservati e irrisolti potenziali rischi. La Figura 1 illustra le principali preoccupazioni dei professionisti della sicurezza in merito all'esposizione a minacce esterne:

Figura 1 - Principali preoccupazioni sull'esposizione alle minacce1

Le principali sfide che i metodi tradizionali di sicurezza offensiva incontrano sono:

Punti ciechi

Gli strumenti tradizionali, come ASM o scanner di vulnerabilità, testano solo una frazione dei potenziali rischi. I test manuali approfonditi non sono sufficientemente scalabili per coprire l'estensione delle moderne superfici di

Risultati non affidabili

L'efficacia dei rimedi è limitata da strumenti e report che includono rischi non validati e falsi positivi. La prioritarizzazione senza contesto causa una scarsa focalizzazione e soluzioni tardive.

Uso intensivo di risorse

La coordinazione dei test o la configurazione degli strumenti richiede processi manuali. Per comprendere i rischi e identificare i passi ottimali di prevenzione sono necessarie ricerche aggiuntive.

Hadrian Security offre un servizio di sicurezza offensiva di primo livello per permettere alle organizzazioni di mitigare proattivamente le minacce e minimizzare i rischi. La piattaforma, operando in modo continuo e autonomo, offre una copertura completa, rendendo Hadrian una soluzione a prova di

Benefici quantificabili

Sfida	Soluzione
Team di sicurezza sopraffatti I team di cybersicurezza ricevono una raffica di alert, che li obbligano a spostare risorse e attenzione dai compiti di sicurezza strategici. Approfondire ciascun allarme sulla sicurezza è un processo intensivo, al quale i team dedicano in media oltre 25 minuti per avviso. Gli strumenti di terze parti, come i servizi di valutazione della sicurezza e di gestione della superficie di attacco, hanno esacerbato questa situazione classificando erroneamente la gravità delle vulnerabilità. Ciò ha messo sotto pressione le risorse e ostacolato la concentrazione su imprese di sicurezza cruciali.	**Prioritizzazione basata sull'IA** Gli algoritmi proprietari di valutazione del rischio di Hadrian isolano le minacce prioritarie, liberando i team di sicurezza dal rumore di fondo. In questo modo, il Centro Operazioni di Sicurezza (SOC) può concentrarsi sugli incidenti più importanti, i processi di gestione delle vulnerabilità possono ottimizzare la priorità delle patch e i team DevSecOps possono focalizzarsi sulle questioni critiche. L'Orchestrator AI di Hadrian è il motore di questa prioritarizzazione. L'analisi si basa su una serie di fattori, tra cui la probabilità di sfruttamento e l'impatto potenziale sul business. Inoltre, gli algoritmi di punteggio proprietari apprendono e si affinano continuamente grazie al feedback degli utenti.
Test di terze parti costosi I test di penetrazione condotti da terze parti sono costosi e spesso eseguiti solo una volta all'anno. La loro natura periodica comporta una mancanza di visibilità sulla sicurezza informatica tra le diverse valutazioni. Inoltre, questi test hanno un'ampiezza limitata, focalizzandosi solo su un sottoinsieme degli asset esposti. Il costo giornaliero per tali test manuali varia tipicamente da 1000 a 3000 dollari.	**Test di penetrazione automatizzati** Il test di penetrazione automatizzato di Hadrian simula il comportamento di veri attaccanti a una frazione del costo. La reportistica, comprensibile e chiaro, permette di intervenire tempestivamente per porre rimedio alle vulnerabilità identificate. Le scansioni di follow-up automatiche verificano l'efficacia delle azioni correttive intraprese. La piattaforma di Hadrian conduce valutazioni delle minacce in modo continuo, eliminando la necessità di attendere il prossimo test manuale. Il test di penetrazione automatizzato è in grado di esaminare le falle di sicurezza 24 ore su 24, 365 giorni all'anno.
Licenze di sicurezza legacy Strumenti di sicurezza inefficaci o isolati offrono intuizioni limitate. Soluzioni puntuali come scanner di vulnerabilità o servizi di valutazione della sicurezza spesso si concentrano su casi d'uso molto ristretti. Di conseguenza, molte organizzazioni faticano a comprendere l'efficacia dei loro strumenti di sicurezza esistenti e a identificare aree di miglioramento.	**Soluzione AI di nuova generazione** Le complete capacità di sicurezza offensiva di Hadrian permettono di sostituire, completamente o parzialmente, gli strumenti esistenti, con un risparmio di decine di migliaia di euro all'anno. Inoltre, Hadrian è in grado di identificare infrastrutture e dispositivi periferici superflui, consentendo una riduzione ulteriore dei costi. La reportistica integrata nella piattaforma fornisce all'organizzazione la possibilità di misurare in modo

Benefici non quantificabili

Sfida	Soluzione
Processi di sicurezza lenti La gestione dell'esposizione si basa su componenti essenziali quali la pianificazione e l'esecuzione di test, la validazione dei risultati e la ricerca di rimedi. I team di sicurezza seguono questo processo per acquisire una comprensione dei percorsi di attacco e fornire indicazioni ai team di remediation. Tuttavia, l'esecuzione manuale di questi processi comporta un dispendio di tempo considerevole. Di conseguenza, le risorse dedicate alla sicurezza si ritrovano disperse e non possono condurre un'analisi efficace di tutte le problematiche.	**Mitigazione continua del rischio** Hadrian automatizza integralmente i processi di scoperta, validazione, prioritarizzazione e remediation. La piattaforma verifica costantemente la cybersecurity posture dell'organizzazione e permette ai team di sicurezza di affrontare le vulnerabilità in modo proattivo. L'Orchestrator AI facilita la remediation fornendo alle unità aziendali istruzioni chiare e passo-passo per i rischi potenziali. In aggiunta la piattaforma esegue automaticamente test di regressione per confermare l'efficacia dei rimedi posti in essere.
Valutazioni in caso di M&A e partner Nelle operazioni di fusione e acquisizione (M&A), la comprensione e la gestione della superficie di attacco delle entità appena integrate risulta spesso ardua. Tale criticità si traduce in asset sconosciuti e rischi associati ai dipartimenti IT delle filiali acquisite, i quali non sono stati completamente integrati nel sistema informatico dell'organizzazione madre. In assenza di una puntuale valutazione della posizione di sicurezza, le organizzazioni non sono in grado di adottare misure per mitigare la loro esposizione al rischio. Alcune scelgono di affidarsi a supporti esterni, con costi che possono raggiungere i 250.000 dollari per ogni acquisizione.	**Approfondimenti automatici sui rischi** Hadrian elimina la necessità di avviare progetti speciali per ottenere un inventario completo della superficie di attacco e dei rischi esposti di tutte le filiali e i partner commerciali. La piattaforma di Hadrian identifica con efficacia gli asset sconosciuti, offrendo alle organizzazioni una visibilità completa e riducendo il carico di lavoro per i team interni. Le valutazioni del rischio in tempo reale forniscono approfondimenti sull'intera impronta digitale dell'azienda acquisita. L'Orchestrator AI, grazie al suo grafico neurale di internet, scopre tutti gli asset rivolti verso l'esterno e li testa approfonditamente per identificarne i rischi.
Spese per la conformità I test di penetrazione sono un elemento comune degli standard di conformità quali ISO 27001, SOC2, NIS2, DORA, HIPAA e PCI-DSS. Per le organizzazioni che necessitano di conformità normativa, la conduzione di tali valutazioni può rappresentare un costo aggiuntivo significativo. Inoltre la compilazione di report per la dimostrazione della conformità può richiedere alle organizzazioni settimane di lavoro. Se condotti trimestralmente, questi adempimenti possono assumere le caratteristiche di un impegno a tempo pieno.	**Rapporti su richiesta** Hadrian supporta le organizzazioni nel soddisfare i requisiti dei test di penetrazione, gestione delle vulnerabilità e dei rischi. La piattaforma esegue valutazioni in maniera continua, riducendo la necessità di coordinare test supplementari. La dashboard di Hadrian permette ai team di sicurezza di monitorare e comprovare l'efficacia dei propri processi. La generazione di report è possibile su richiesta e la loro condivisione con stakeholder interni ed esterni risulta semplice e immediata.

Inventario manuale degli asset

Le organizzazioni si affidano a processi manuali che richiedono tempo e fatica, basati su fogli di calcolo e script creati ad hoc, per inventariare i propri asset digitali. I team dedicano tempo prezioso alla manutenzione di questi script e alla rimozione dei duplicati nei risultati ottenuti.

Si stima che siano necessari 10 minuti di lavoro ingegneristico per ogni singolo asset per un inventario manuale completo. Questo carico di lavoro, unito alla limitata accuratezza dei dati, ostacola il monitoraggio efficace della superficie di attacco a causa della mancanza di automazione e dell'infrequenza degli aggiornamenti.

Scoperta automatizzata e continua

La piattaforma di Hadrian implementa una scoperta automatizzata e continua degli asset, costruendo un inventario accurato e costantemente aggiornato. I risultati sono facilmente fruibili in diversi formati, sia tabellari che grafici, e possono essere esportati per analisi esterne.

Gli algoritmi di ricerca degli asset di Hadrian si basano sulle migliori pratiche e su tecniche proprietarie. Il team di sviluppo interno aggiorna continuamente la tecnologia per identificare nuove classi di asset e perfezionare l'automazione.

Costi elevati delle cyber insurance

Durante la negoziazione dei premi con le organizzazioni, i fornitori di assicurazioni cyber tengono conto di molteplici fattori. Tuttavia, le aziende lamentano una mancanza di informazioni sulla propria posizione di sicurezza e su quella dei loro pari.

L'assenza di dati affidabili sulla robustezza della sicurezza aziendale e di benchmark di settore determina un'ampia variabilità nei premi delle polizze cyber, che possono oscillare da 1.500 dollari all'anno per 1 milione di dollari di copertura.

Riduzione dei premi assicurativi

Hadrian permette alle organizzazioni di ottenere risparmi grazie a termini e condizioni preferenziali per la loro assicurazione cyber. Le organizzazioni, fornendo prove misurabili della riduzione del rischio di una violazione, sono in grado di negoziare con i fornitori di assicurazioni per ottenere condizioni migliori.

La piattaforma consente inoltre alle organizzazioni di confrontare la propria sicurezza con quella di aziende simili, permettendo loro di comprendere la propria posizione di sicurezza relativa e la reattività alle minacce.

Perdita di ricavi e danni

Una violazione o un'interruzione del servizio possono avere un impatto significativo sul margine di profitto di un'organizzazione. I costi a valle includono la rimozione della minaccia, il tempo di inattività, la perdita di produttività, le sanzioni pecuniarie e il danno alla reputazione del marchio.

Le sanzioni normative, come quelle previste dal GDPR, possono essere severe e imporre oneri finanziari considerevoli alle organizzazioni. Inoltre, queste possono essere soggette a un maggiore controllo da parte degli enti regolatori.

Aumento della resilienza

Hadrian aiuta le organizzazioni a ridurre la loro esposizione al rischio fornendo passi chiari e concreti da seguire. Questo approccio non solo riduce la probabilità di una violazione, ma ne limita anche l'impatto potenziale.

Come evidenziato dal rapporto IBM sul Costo di una Violazione dei Dati, il 35% delle organizzazioni decide di investire in test di sicurezza offensivi solo dopo aver subito una violazione. Tuttavia, investendo in anticipo in misure di sicurezza adeguate, le organizzazioni possono ridurre significativamente la probabilità di subire un attacco informatico.

Team di sicurezza rallentati

Le lente pratiche di test di sicurezza risultano inadeguate ai rapidi cicli di sviluppo odierni. I test di penetrazione possono richiedere un mese per la pianificazione, due per l'esecuzione e diverse settimane aggiuntive per la stesura del rapporto. Tale tempistica si scontra con le metodologie di sviluppo basate su sprint di due settimane.

Gli strumenti attualmente disponibili per le valutazioni di sicurezza si dimostrano complessi. Non solo la loro configurazione e utilizzo risultano onerosi, ma i risultati generati spesso includono falsi positivi e si presentano difficili da interpretare e gestire per il personale non specializzato in sicurezza.

Flussi di lavoro collaborativi e semplificati

Hadrian semplifica il processo di gestione della superficie di attacco, supportando le operazioni di sicurezza nel mantenimento di un ambiente cibernetico sicuro. Le capacità di test di penetrazione automatizzate della piattaforma identificano in tempo reale i rischi sfruttabili, fornendo ai team di sviluppo un feedback quasi istantaneo.

L'Orchestrator AI è progettato per ottimizzare i flussi di lavoro di sicurezza offensiva, validando autonomamente i risultati per eliminare i falsi positivi. Hadrian fornisce inoltre istruzioni passo-passo per consentire ai team di remediation di intervenire tempestivamente.

Applicazioni di terze parti dimenticate

La scoperta di vulnerabilità in software di terze parti rappresenta una sfida per le organizzazioni che non dispongono di un inventario aggiornato e accurato. L'assenza di visibilità sulle superfici di attacco esterne e sulle lacune di sicurezza amplifica il problema.

Un esempio emblematico è rappresentato da ambienti di pre-produzione creati per testare nuove funzionalità e poi dimenticati. Questi ambienti, spesso trascurati, non rispecchiano gli standard di sicurezza necessari, esponendo l'organizzazione a rischi significativi.

Visibilità della catena di fornitura

Le sonde di Hadrian sono in grado di identificare oltre 10.000 applicazioni SaaS e migliaia di pacchetti software e versioni, garantendo un'identificazione completa degli strumenti in uso.

Attraverso una scansione continua di internet, la piattaforma di Hadrian esamina tecnologie, versioni e configurazioni, con l'obiettivo di individuare potenziali minacce alla sicurezza. Tale processo consente a Hadrian di svelare la postura di sicurezza della vostra organizzazione e di valutare l'impatto che un compromesso del software di terze parti potrebbe avere.

Abuso del marchio e phishing

Il panorama digitale odierno è caratterizzato da un'ampia diffusione di sottodomini, la cui natura dinamica rende complesso il monitoraggio. I sottodomini possono facilmente passare inosservati, rendendoli suscettibili a tentativi di takeover e compromissioni dell'infrastruttura.

I sottodomini non reclamati o mal gestiti possono fungere da porta d'ingresso per i malintenzionati, con possibili danni al marchio, perdita di fiducia dei clienti e violazioni dei dati. Per esempio, gli aggressori potrebbero sfruttare un sottodominio per rubare cookie di autenticazione.

Mantenere la fiducia nel marchio

Hadrian previene danni al marchio mediante il monitoraggio continuo delle vulnerabilità nei sottodomini a rischio di takeover. La piattaforma esegue scansioni ricorrenti dell'infrastruttura DNS per identificare tempestivamente eventuali rischi emergenti.

In caso di minacce, la piattaforma allerta immediatamente i team di sicurezza, consentendo l'adozione di misure proattive e prevenendo l'acquisizione dei sottodomini. Una rapida remediation elimina il rischio che clienti, dipendenti e partner si imbattano in siti di phishing dannosi.

Riguardo Hadrian

La sicurezza difensiva necessita di convalida tramite simulazioni di attacchi reali. Hadrian offre una prospettiva hacker, svelando obiettivi e metodi impiegabili in una violazione informatica realistica. I test di Hadrian, continui e completi, scoprono e validano i rischi in maniera autonoma.

La nostra soluzione

La piattaforma Hadrian combina scoperta della superficie di attacco, test di penetrazione automatizzati e tecnologie di gestione dell'esposizione alle minacce in un sistema basato su cloud e senza agenti. L'Orchestrator AI alimenta la piattaforma, emulando le tecniche e i comportamenti di un vero attore malevolo. Questo permette un rilevamento continuo 24/7 delle minacce rivolte a Internet e la rimozione automatica di falsi positivi.

L'Orchestrator AI sfrutta la conoscenza del tuo ambiente per testare rischi sfruttabili OWASP Top Ten, vulnerabilità note e zero-day, oltre a servizi esposti e configurati erroneamente. Le scansioni si integrano per simulare attacchi complessi multidimensionali. Inoltre questa tecnologia all'avanguardia è costantemente aggiornata e migliorata dal team interno di hacker di Hadrian.

+200
Di aziende protette

+1.2m
Di asset messi in sicurezza

40%
La riduzione media di tempo per risoluzione

Scelto da

ABN·AMRO · SHV ENERGY · macmillan education
WeatherTech · LEROY MERLIN · LOTTOMatica
RITUALS... · BIOLANDES · nedap

> "Ciò che entusiasma di Hadrian è la sua capacità di risolvere una sfida apparentemente impossibile: individuare debolezze in reti complesse con una granularità simile a quella umana, su larga scala, dall'esterno e in modo continuo. In pratica, Hadrian compie in pochi minuti per migliaia di sistemi un'analisi che di solito richiederebbe a un team dedicato di ingegneri della sicurezza diverse settimane per un singolo sistema."
>
> **Tiago Teles, Responsabile della Sicurezza presso ABN AMRO**