HADRIAN

Come la gestione dell'esposizione riduce i rischi ai confini delle organizzazioni

Una soluzione moderna per proteggere gli asset più importanti delle aziende

I confini non sono più ben definiti

Oggi esistono più asset strategici che mai ai confini di sicurezza delle imprese

Nel mondo veloce di oggi, le aziende devono abbracciare la trasformazione digitale per rimanere competitive. I benefici di quest'ultima infatti sono significativi e di vasta portata:

- **Esperienza cliente migliorata** – Sfruttando tecnologie come app mobili, social media e chatbot, le aziende possono creare interazioni personalizzate con i loro clienti.
- **Aumento dell'efficienza e della produttività** – Gli strumenti digitali hanno automatizzato i processi manuali, riducendo gli errori e migliorando l'accuratezza. Questo permette ai dipendenti di liberare il proprio tempo e di concentrarsi su compiti ad alto valore aggiunto, come l'innovazione e lo sviluppo del business.
- **Maggiore agilità e flessibilità** – L'utilizzo di applicazioni cloud su richiesta ha permesso alle organizzazioni di scalare le proprie operazioni in modo rapido e flessibile, in base alle necessità. Inoltre, gli strumenti di lavoro remoto favoriscono una maggiore efficienza lavorativa.

Abbracciare la trasformazione digitale ha permesso alle organizzazioni di adeguarsi ai tempi, adattarsi alle mutevoli condizioni di mercato e cogliere le nuove opportunità. Tuttavia, tale trasformazione ha anche ridisegnato il perimetro di sicurezza, rendendo la gestione del rischio una sfida sempre più complessa. L'aumento di dipendenti, clienti e applicazioni di terze parti che accedono all'infrastruttura aziendale ha ampliato la superficie di attacco e reso più arduo il controllo.

40%

delle aziende, secondo il sondaggio sul Cloud Infrastructure del 2022 di Forrester, prevede di adottare una strategia "cloud-native" prioritaria nel 2023, con l'obiettivo di aumentare l'agilità e l'efficienza riducendo al contempo i costi.

24%

Il numero di lavoratori remoti è aumentato del 24% tra il 2021 e il 2022.

87%

dei dirigenti senior, come riportato da Gartner nel 2021, ha identificato la trasformazione digitale come una priorità chiave per la propria organizzazione.

Gli attori delle minacce stanno sfruttando questi nuovi confini

Gli attacchi stanno prendendo sempre più di mira gli asset esposti ai margini

La trasformazione digitale porta con sé nuovi rischi e sfide per la cybersecurity. Criminali informatici e attori delle minacce sfruttano rapidamente le vulnerabilità dell'infrastruttura digitale, causando violazioni di dati, perdite finanziarie e danni alla reputazione per le organizzazioni.

Nella corsa all'adozione di nuove tecnologie e al mantenimento di un vantaggio competitivo, la sicurezza viene spesso trascurata. Il cloud computing, i dispositivi IoT e le applicazioni mobili hanno ampliato la superficie di attacco che gli attori delle minacce possono sfruttare.

> Si ha la sensazione che le organizzazioni concentrino i loro sforzi di sicurezza unicamente sui propri ambienti "noti" e tradizionali. Tale approccio crea un terreno fertile per gli attori delle minacce, che con maggiore probabilità troveranno un asset esposto online da sfruttare a proprio vantaggio.
>
> **Olivier Beg - Head of Hacking presso Hadrian**

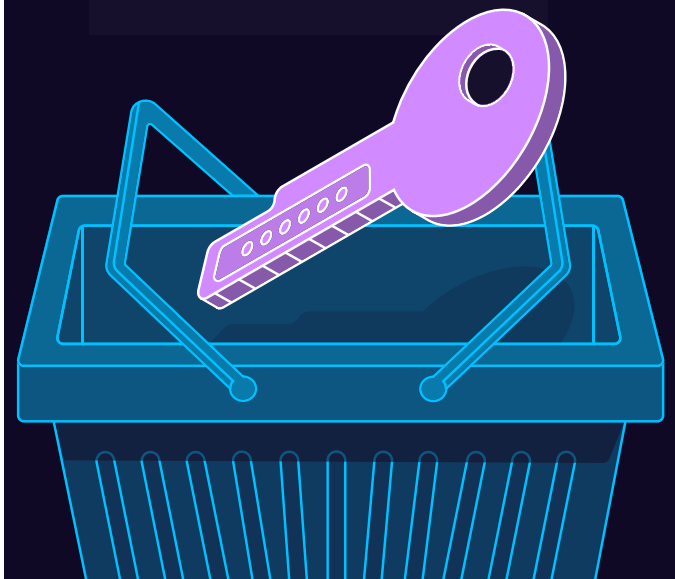
Le organizzazioni devono bilanciare l'adozione della trasformazione digitale con la gestione dei rischi e delle minacce ad essa associate. Gli attori malevoli sfruttano la scarsa attenzione alla sicurezza, prendendo di mira le vulnerabilità delle nuove tecnologie per accedere a dati sensibili.

69%

delle organizzazioni ha subito un attacco mirato a un asset esterno sconosciuto, non gestito o gestito in modo inadeguato.

10/55

Nel 2022, il 10% delle vulnerabilità zero-day sfruttate coinvolgeva dispositivi IoT connessi a internet.



Come il panorama delle minacce si sta ridisegnando

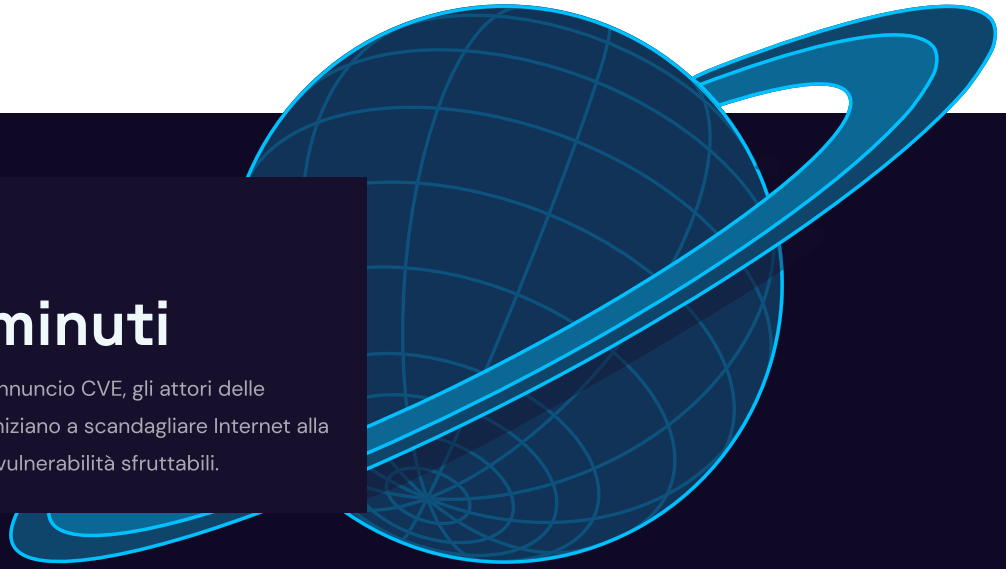
I broker di accesso iniziale (IAB) stanno ridisegnando il panorama delle minacce, introducendo nuovi incentivi e dinamiche nel mondo criminale.

Storicamente, le bande di ransomware e altri attori delle minacce gestivano autonomamente ogni fase di un attacco, dall'ottenimento dell'accesso a una rete alla cifratura dei dati e alla negoziazione dei riscatti. Tuttavia, l'ascesa degli IAB ha modificato questo scenario. Questi aggressori si focalizzano sull'acquisizione di accessi alle reti, per poi venderli ad altri criminali.

Le competenze degli IAB sono spesso limitate. Non sviluppano malware o programmi di ransomware sofisticati, ma traggono profitto dalla vendita di accessi a numerose organizzazioni, che altri cybercriminali sfruttano per i loro attacchi.

Questo modello offre vantaggi a entrambi i lati. Gli IAB ottengono un profitto costante senza dover possedere competenze avanzate, mentre le bande di ransomware e altri gruppi di minaccia persistente avanzata (APT) possono ampliare il loro raggio d'azione, non essendo più limitati dal numero di sistemi che riescono a colpire autonomamente.

Gli attacchi degli IAB sono indiscriminati. Non prendono di mira specifiche industrie oppure organizzazioni, ma sfruttano vulnerabilità note alla ricerca di qualsiasi asset vulnerabile sul perimetro di un'organizzazione. Con la loro crescente stabilizzazione, si prevede un aumento del numero di attacchi da parte delle bande di ransomware.



25,059

record CVE pubblicati nel 2022, con un aumento di circa il 25% rispetto al 2021.

15 minuti

dopo un annuncio CVE, gli attori delle minacce iniziano a scandagliare Internet alla ricerca di vulnerabilità sfruttabili.

I processi esistenti non riescono a stare al passo

I programmi tradizionali di gestione delle vulnerabilità non sono più sufficienti

Il principio alla base della gestione delle vulnerabilità è semplice: identificare e correggere le debolezze nei sistemi e nelle applicazioni prima che possano essere sfruttate dagli hacker. Tuttavia, i programmi tradizionali di gestione delle vulnerabilità si stanno dimostrando inefficaci nel contrastare l'elevato numero di violazioni che sfruttano vulnerabilità note.
Le principali sfide che ostacolano l'efficacia dei programmi di gestione delle vulnerabilità includono:

- **Scarsa visibilità** – Le organizzazioni spesso non hanno una conoscenza completa della loro superficie di attacco, rendendo difficile l'identificazione di tutte le vulnerabilità presenti.
- **Scoperta inefficace** – Identificare le vulnerabilità è un processo complesso che richiede di trovare il maggior numero possibile di vulnerabilità reali, minimizzando al contempo i falsi positivi che possono intasare i team di sicurezza.
- **Prioritizzazione inaccurata** – Molte organizzazioni non riescono a dare la giusta priorità alle vulnerabilità, concentrandosi su quelle più vecchie o con punteggi CVSS elevati, ignorando invece rischi critici che potrebbero portare a violazioni.

56%

delle grandi aziende gestisce oltre 1.000 allarmi di sicurezza ogni giorno.

66%

dei team di sicurezza afferma di avere difficoltà nel proteggere superfici di attacco complesse e in continua evoluzione.

68%

di tutti gli attacchi informatici sfruttano vulnerabilità per le quali era disponibile una patch da oltre un anno.

Un approccio moderno a un problema moderno

Introduzione alla Gestione Continua dell'Esposizione alle Minacce (CTEM)

La Gestione Continua dell'Esposizione alle Minacce (CTEM) rappresenta un metodo all'avanguardia per contrastare le sfide odierne in materia di sicurezza informatica. Si tratta di un processo di monitoraggio costante che permette di identificare in tempo reale minacce, vulnerabilità e rischi, consentendo alle organizzazioni di rispondere tempestivamente e ridurre il rischio di subire un attacco informatico con successo.

> Entro il 2026, le organizzazioni che prioritarizzano gli investimenti in sicurezza basandosi su un programma di CTEM avranno una probabilità tre volte inferiore di subire una violazione.
>
> **Gartner**

Le modalità di riduzione del rischio sono specifiche per ogni organizzazione, ma il CTEM fornisce l'architettura per affrontare le sfide comuni:

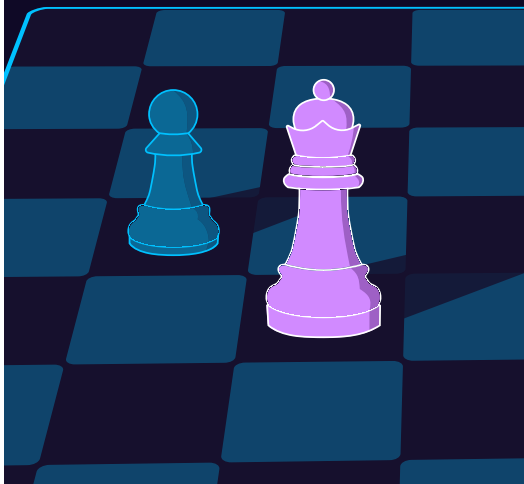
- Minimizzare il numero di incidenti di sicurezza che le organizzazioni attualmente affrontano.
- Creare ambienti sicuri in contesti in costante evoluzione.
- Identificare i punti deboli nella tua cybersecurity posture che un attacco potrebbe sfruttare.
- Ridurre il rischio creato dalla tecnologia che coinvolge i lavoratori remoti.
- Spostare funzioni aziendali critiche verso servizi o piattaforme di terze parti.

87%

percento dei dirigenti senior dà priorità alla trasformazione digitale come priorità organizzativa, secondo il rapporto di Gartner.

85%

Secondo il rapporto di Gartner, i dirigenti di alto livello considerano la trasformazione digitale una priorità per l'organizzazione.



Comprendere la Gestione dell'Esposizione

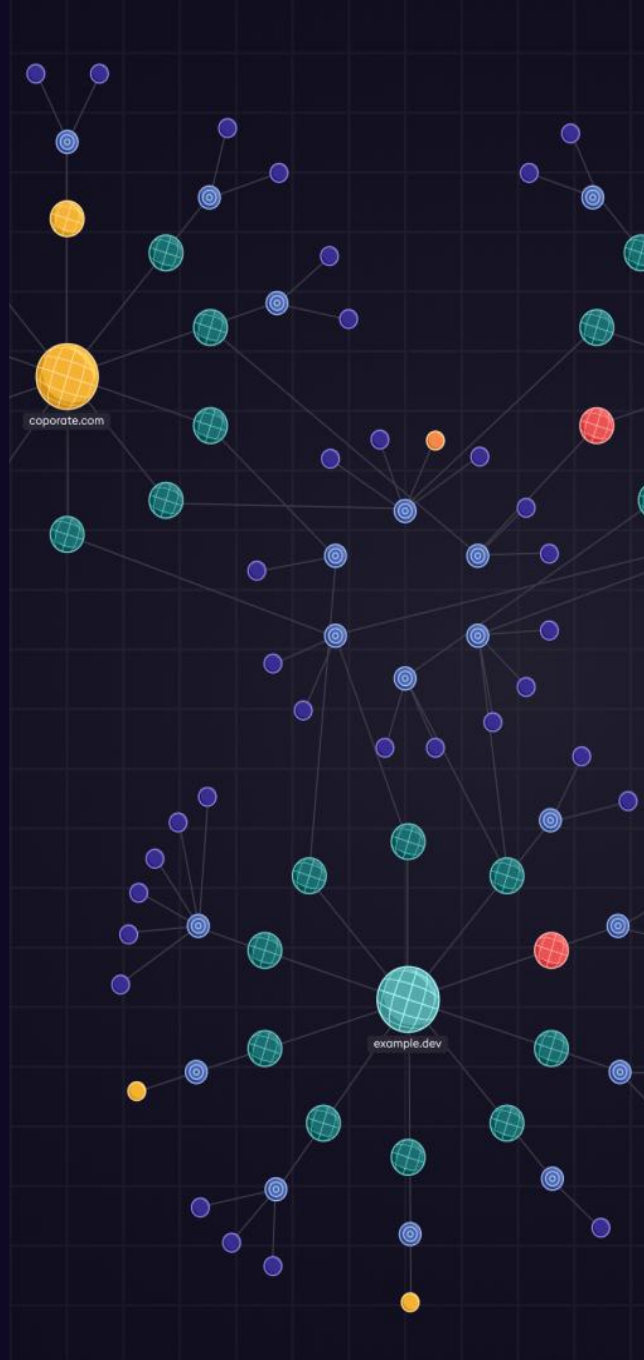
Offrire ciò che la gestione delle vulnerabilità non può garantire

I programmi di gestione dell'esposizione vanno oltre la gestione delle vulnerabilità in diversi modi:

- **Valutazione completa della cybersecurity posture:** L'analisi include l'intera superficie di attacco dell'organizzazione, non solo gli asset conosciuti e catalogati manualmente.
- **Determinazione precisa del rischio:** La probabilità e l'impatto dell'exploit vengono calcolati considerando l'intero ambiente dell'organizzazione, non solo esaminando il rischio in casi isolati.
- **Raccomandazioni di rimedio a livello aziendale:** Le attività di rimedio suggerite sono applicabili all'intera organizzazione, non solo ai team responsabili della patch delle vulnerabilità.

L'implementazione di un programma di gestione dell'esposizione efficace richiede diverse capacità chiave:

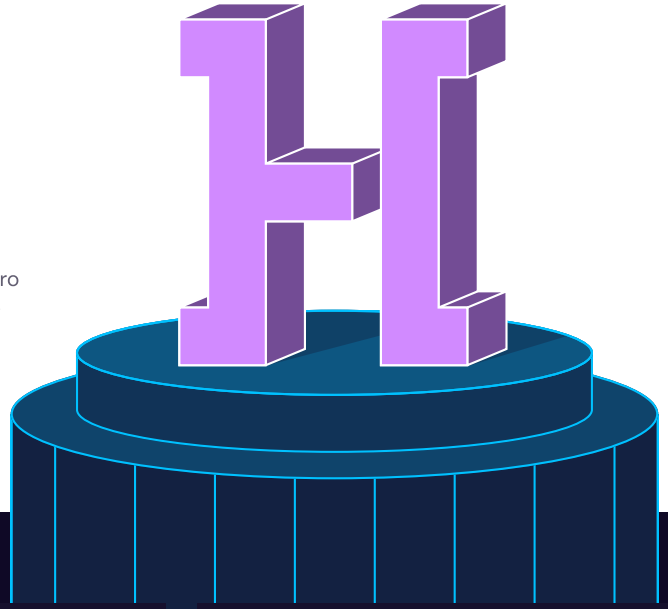
- Identificazione costante di tutti gli asset esposti a internet.
- Individuazione automatica delle vulnerabilità e dei rischi sfruttabili.
- Classificazione precisa dei rischi in base alla loro gravità e urgenza.
- Verifica che le misure di rimedio abbiano effettivamente risolto i rischi identificati.



L'Orchestrator AI di Hadrian

Prevenire le violazioni con la gestione dell'esposizione

Hadrian offre una copertura continua del ciclo di vita della gestione dell'esposizione esterna, riducendo i rischi, migliorando l'efficienza e semplificando la conformità. Al centro della nostra piattaforma si trova l'Orchestrator, che conduce analisi 24 ore su 24, 7 giorni su 7, 365 giorni all'anno, simulando un avversario del mondo reale e concatenando dinamicamente oltre 200 moduli "hacker".



1

Asset

L'Orchestrator scopre asset sconosciuti elaborando 1.1Tb di dati al giorno per scoprire ogni asset appartenente alla tua organizzazione. Per prevenire sorprese indesiderate, l'Orchestrator esegue continuamente scansioni alla ricerca di segni di nuovi asset e cambiamenti.

2

Contesto

La piattaforma di Hadrian contestualizza i tuoi asset per comprendere come un avversario potrebbe condurre un attacco. Durante questa fase, Hadrian rileva informazioni sul sistema operativo, sui moduli, sulle librerie, sui campi di input, sui metodi di autenticazione e molto altro.

3

Rischi

L'Orchestrator utilizza la sua conoscenza del tuo ambiente per sondare le debolezze, imparando e affinando le sue tecniche man mano che procede. Hadrian identifica in modo affidabile rischi precedentemente non scoperti per la tua organizzazione, con un numero ridotto di falsi positivi.

HADRIAN

Hadrian è un fornitore leader di soluzioni di Gestione della Superficie di Attacco Esterna (EASM), Test Continuo Automatizzato di Penetrazione (CART) e Gestione Continua dell'Esposizione alle Minacce (CTEM). La nostra piattaforma cataloga asset noti e sconosciuti ovunque si trovino, indaga sulle vulnerabilità eseguendo exploit come farebbe un attore di minaccia e dà priorità ai rischi per una rapida remediation basata sul tuo ambiente specifico.

Prenota una Demo | Per Saperne di Più

(1) Forrester, Infrastructure Cloud Survey (2022)
(2) Owl Labs, State of Remote Work (2022)
(3) Gartner, Speed Up Your Digital Business Transformation (2019)
(4) ESG, Security Hygiene and Posture Management (2022)
(5) Madiant, Move, Patch, Get Out the Way: 2022 Zero-Day Exploitation Continues at an Elevated Pace (2023)
(6) CVE, Metrics webage (accessed April 2023)
(7) Palo Alto, Incident Response Report (2022)
(8) Sumo Logic, State of SecOps and Automation (2020)
(9) Ponemon, The Cybersecurity Illusion: The Emperor Has No Clothes (2019)
(10) Abdalslam, Patch Management Statistics, Trends And Facts (2023)
(11) Cloud Native Computing Foundation, Cloud Native Security Microsurvey (2021)

Scelto da

BIOLANDES | CTC GLOBAL | beyond. | KCK

KINGSWAY CAPITAL | bank prov. | LEROY MERLIN | London Business School