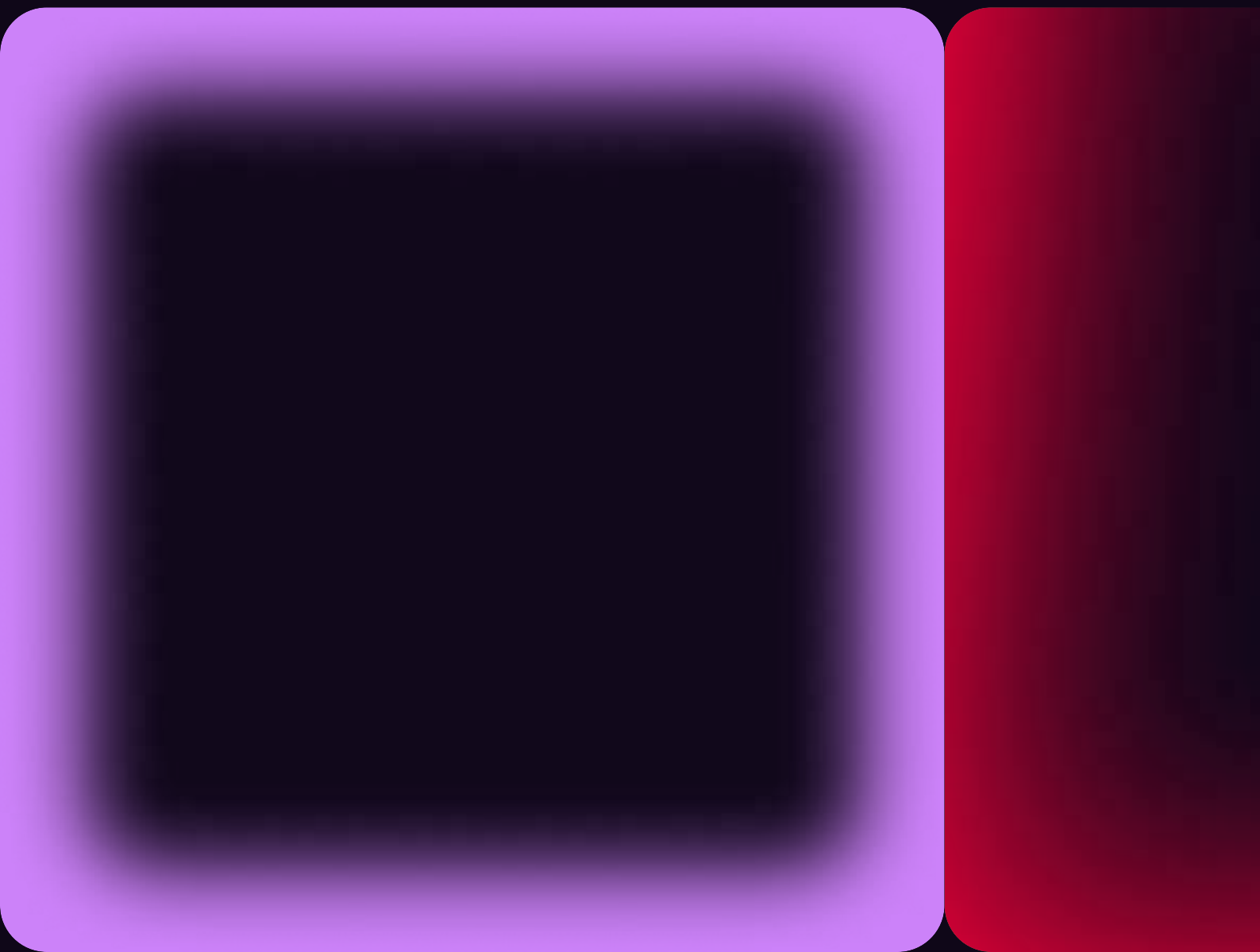
HADRIAN

WHITEPAPER

Come allineare la propria strategia per la sicurezza al ritmo degli aggressori utilizzando l'AEV



Indice

Riepilogo esecutivo

Nel 2022, gli hacker scansionavano le vulnerabilità entro 15 minuti dalla loro rivelazione. Questo accadeva tre anni fa, prima dell'implementazione di strumenti di hacking basati sull'intelligenza artificiale. E l'intelligenza artificiale è un elemento chiave di questa accelerazione. La velocità impressionante con cui emergono le minacce è determinata in parte dalle minacce generate dall'intelligenza artificiale, che consentono agli aggressori di automatizzare la reconnaissance, sfruttare le vulnerabilità e scalare le operazioni più rapidamente di quanto possano fare i professionisti della sicurezza.

Secondo il Verizon 2025 Data Breach Incident Report, le violazioni dovute allo sfruttamento di vulnerabilità sono aumentate del 275% negli ultimi due anni—trainate da exploit zero-day e da una più rapida individuazione dei dispositivi di frontiera. Nel frattempo, il tempo mediano per correggere le vulnerabilità esposte a Internet è di 32 giorni, con quasi un terzo che non viene mai risolto. Nel 2025, CrowdStrike ha riportato un tempo medio di breakout di soli 48 minuti—con il caso più rapido registrato in appena 51 secondi. Contro avversari potenziati dall'intelligenza artificiale, il rilevamento non è più sufficiente—le organizzazioni devono dare priorità alla prevenzione.

È qui che entra in gioco l'Adversarial Exposure Validation (AEV). Emulando costantemente il comportamento degli aggressori dall'esterno verso l'interno, AEV convalida in tempo reale quali esposizioni sono effettivamente sfruttabili. Riduce la stanchezza da allarmi, elimina le supposizioni e dà ai team di sicurezza il potere di agire prima che si verifichi un incidente—non dopo.

Gli aggressori non stanno aspettando. Nemmeno voi potete permettervelo.

1. Più veloci, più pericolosi

Il settore della sicurezza informatica sa da tempo che la velocità è il parametro decisivo per la prevenzione e la mitigazione di una violazione. Ma il "time to compromise" si è ridotto a una velocità che pochi avevano previsto. Il breakout time, ovvero il periodo che intercorre tra l'accesso iniziale di un avversario e il suo movimento laterale all'interno di una rete, non si misura più in giorni, ore o addirittura decine di minuti, ma sempre più spesso in secondi.

Il Global Threat Report 2025 di CrowdStrike traccia un quadro molto chiaro. Su migliaia di indagini sugli incidenti, il breakout time medio è stato di soli 48 minuti. È preoccupante che alcuni set di violazioni abbiano registrato una velocità di breakout inferiore a un minuto. In un caso di alto profilo, attribuito a un'organizzazione eCrime a scopo finanziario, il movimento laterale completo attraverso un ambiente cloud ibrido è avvenuto in 51 secondi.

Nel 2022, gli hacker scansionavano le vulnerabilità entro 15 minuti dalla loro rivelazione. Il 2022 è l'anno della nascita dell'IA generativa. Sono trascorsi tre anni dall'inizio di quest'era e gli hacker hanno efficacemente sfruttato gli strumenti dell'IA per rendere il loro lavoro più veloce, più efficiente e più pericoloso. La finestra di 15 minuti si è probabilmente ridotta a pochi secondi.

01 Questa velocità crea sfide operative profonde per i difensori.

02 I modelli linguistici di grandi dimensioni vengono ormai utilizzati per automatizzare la scoperta delle vulnerabilità, concatenare problemi di bassa gravità in exploit reali e colpire asset esposti con una scala e una velocità mai viste prima.

03 Questo dimostra che la difesa, per sua stessa natura, arriva già troppo tardi.

I benchmark storici sono troppo lunghi

Ad aggravare la sfida, le pratiche relative alla gestione delle patch rimangono eccessivamente lente rispetto alla velocità di sfruttamento da parte degli attori delle minacce. Il DBIR 2025 di Verizon ha rivelato che il tempo medio per rimediare alle vulnerabilità sui sistemi connessi a Internet è di 32 giorni. Inoltre, circa il 30% delle vulnerabilità identificate sui dispositivi edge rimane completamente irrisolto. Dato che lo sfruttamento delle vulnerabilità spesso inizia entro 5 giorni dal rilevamento, o addirittura il giorno stesso del rilevamento nel caso dei dispositivi edge, è chiaro che le strategie di difesa basate sulle patch siano insufficienti per contrastare i moderni attori delle minacce.

GLI HACKER SCANSIONANO LE VULNERABILITÀ SUBITO DOPO LA DIVULGAZIONE

<15 MINUTI

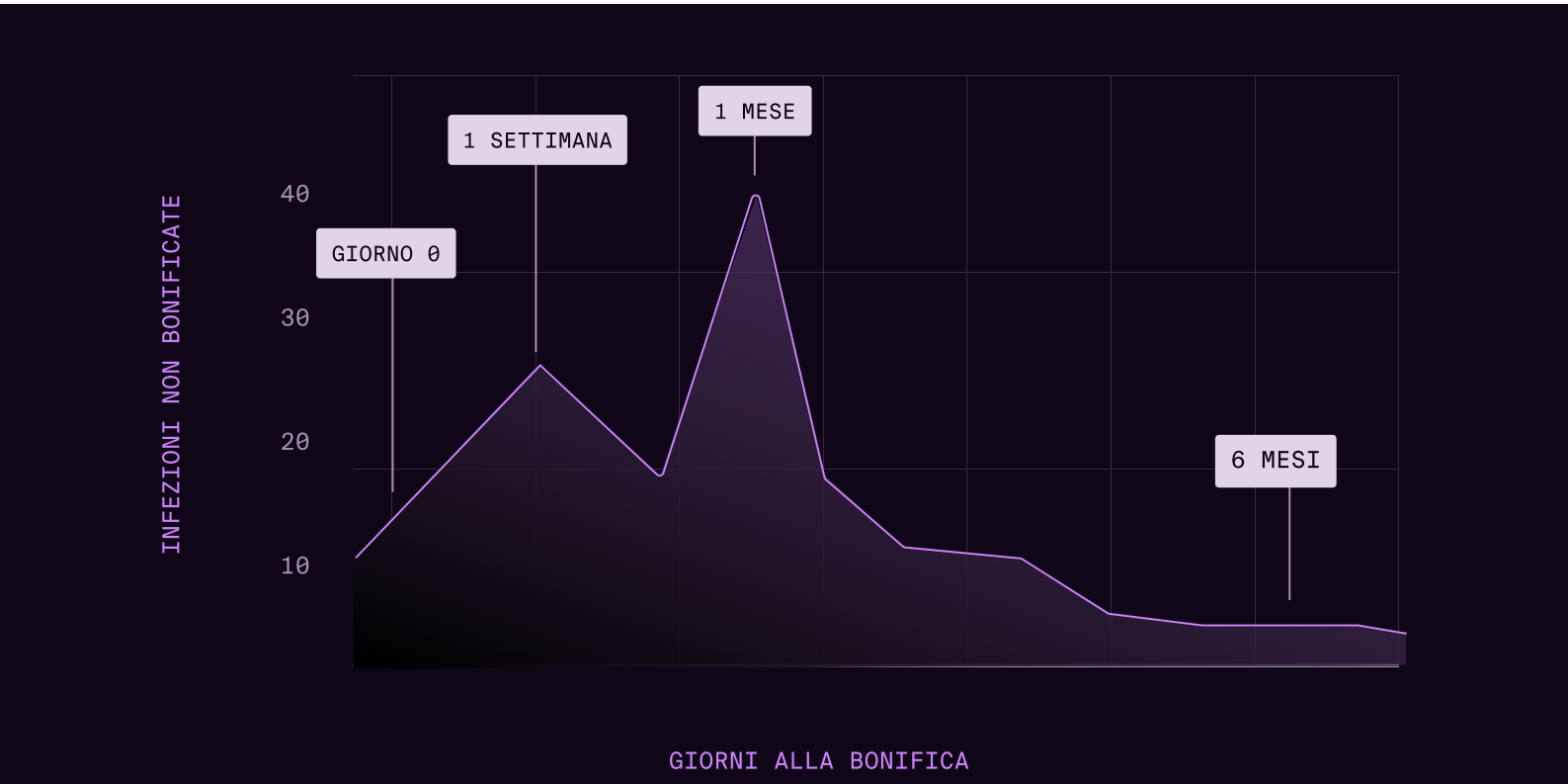
AUMENTO DELLO SFRUTTAMENTO DELLE VULNERABILITÀ DAL 2023

+275%

TEMPO MEDIO DI BREAKOUT NEL 2025

48 MINUTI

TEMPO DI BONIFICA DELLE VULNERABILITÀ NEI SISTEMI ESPOSTI A INTERNET



Il debito operativo ti rallenta

La seconda fonte di pressione che i CISO devono affrontare è la limitazione delle risorse. I CISO si trovano a gestire più strumenti che mai, ma con un organico ridotto all'osso o in calo. I budget sono sottoposti a controlli. I team addetti alla sicurezza sono sommersi dalle segnalazioni e sono costretti a valutare i rischi senza un contesto preciso. Molte organizzazioni semplicemente non hanno il personale necessario per analizzare tutti i problemi segnalati, convalidare tutte le minacce o individuare tutti i falsi positivi. Queste sono solo alcune delle limitazioni operative che i team SOC devono affrontare:

01 Una miriade di strumenti per la sicurezza la cui manutenzione richiede tempo e risorse da parte dei team SOC;

02 I team addetti alla sicurezza risentono dello stress provocato dalle segnalazioni e dall'eccessivo lavoro arretrato;

03 I report di conformità distraggono dalle priorità operative.

La visibilità isolata è una delle sfide più insidiose che gli addetti alla sicurezza devono affrontare. È tutto ciò che non si vede a dare agli aggressori più spazio e opportunità di sfruttare le tue vulnerabilità.

Le attività di fusione e acquisizione spesso si portano dietro infrastrutture preesistenti, sottodomini sconosciuti e sistemi legacy che non sono stati progettati pensando a controlli di sicurezza unificati.

Nel frattempo, i team marketing spesso lanciano micrositi per le campagne, registrano nuovi domini o attivano strumenti di terze parti senza una supervisione da parte dei responsabili della sicurezza. Questi domini possono raccogliere dati sensibili o integrarsi con i sistemi interni, ma raramente sono monitorati dall'IT o coperti da flussi di lavoro per la gestione delle vulnerabilità.

Nel complesso, questi silos frammentano la visibilità e creano lacune che gli aggressori sfruttano a un ritmo difficilmente arginabile. Lo Shadow IT prospera in questi punti ciechi, introducendo esposizioni di cui il team addetto alla sicurezza potrebbe non venire a conoscenza fino a quando non è troppo tardi. Ancora una volta, la sicurezza preventiva è l'unico metodo per avere una visibilità continua sulla superficie di attacco.

La difesa statica ha degli svantaggi

In questo contesto, altri modelli di sicurezza (basati su scansioni point-in-time, liste di controllo della conformità e penetration test annuali) non sono adatti ad attacchi che si muovono a velocità così elevate. La convalida manuale delle patch non può sperare di eguagliare gli avversari che operano alla velocità dell'IA. Gli esercizi trimestrali di red-team, pur essendo validi, forniscono garanzie solo per il momento in cui vengono condotti e solo per l'ambito che viene loro assegnato.
In un ambiente in cui ogni secondo è importante, i difensori hanno bisogno di visibilità, convalida e priorità continue.

Le metriche più importanti

Nell'era delle finestre di breakout di 48 minuti, le performance in materia di sicurezza devono essere misurate in base a nuovi KPI, tra cui:

- **Mean Time to Prevent (MTTP):** la velocità con cui è possibile individuare, convalidare e correggere i rischi in caso di esposizione sfruttabile.
- **Mean Time to Validate (MTTV):** la velocità con cui i rischi potenziali vengono confermati come sfruttabili.
- **Mean Time to Remediate (MTTR):** la rapidità con cui le esposizioni critiche vengono corrette o neutralizzate.

Le organizzazioni che operano senza avere obiettivi ambiziosi su queste metriche non sono più da considerarsi "ritardatarie in materia di best practice", ma sono profondamente a rischio.

In questo contesto, altri modelli di sicurezza — basati su scansioni puntuali, checklist di conformità e test di penetrazione annuali — non sono adatti ad affrontare attacchi che si muovono a velocità così elevate. La validazione manuale delle patch non può competere con avversari che operano alla velocità dell'intelligenza artificiale. Gli esercizi trimestrali di red team, pur essendo utili, forniscono garanzie solo per il momento in cui vengono eseguiti e solo per l'ambito definito.

In un ambiente in cui ogni secondo conta, i difensori hanno bisogno di visibilità continua, validazione continua e una continua capacità di stabilire le priorità.

2. Altri strumenti possono essere d’aiuto, ma non bastano

La natura della sicurezza informatica è tale che spesso si utilizza un portfolio di strumenti per prevenire ogni minaccia informatica. Ma non tutti questi strumenti sono uguali.

Gli strumenti point-in-time, i penetration test periodici e gli inventari degli asset sono indice di un modello di sicurezza reattivo. Questi strumenti, pur essendo ancora utili in determinati contesti, sono divenuti di per sé inadeguati in un mondo definito da minacce in tempo reale e superfici di attacco esterne che cambiano di ora in ora.

Le segnalazioni che gridano al lupo

Un gran numero di segnalazioni conduce direttamente all'alert fatigue. I team addetti alla sicurezza sono inondati di report sulle vulnerabilità e di inventari degli asset che non hanno una priorità. Senza una convalida, i team sprecano cicli preziosi per gestire esposizioni che si rivelano falsi positivi o che rappresentano un rischio minimo.
Nel frattempo, i vettori realmente sfruttabili possono restare nascosti nella confusione o essere del tutto ignorati. Esempi di segnalazioni che causano molto rumore sono:

CVE A BASSA GRAVITÀ:

Segnalazioni relative a librerie obsolete o a vulnerabilità minori che comportano un rischio minimo sul piano concreto, soprattutto quando non dispongono di un percorso di exploit praticabile o sono protette da controlli compensativi.

ASSET ESCLUSIVAMENTE INTERNI:

Segnalazioni su sistemi non visibili su Internet, come ambienti di sviluppo o servizi di backend, che vengono segnalati nonostante non siano raggiungibili da aggressori esterni.

Benvenuti nel “teatrino della sicurezza”

I penetration test periodici non sono un sostituto sufficiente. Anche i migliori pentest manuali sono in genere programmati trimestralmente o annualmente. Il risultato è una sorta di ”teatrino della sicurezza”: ci si sente protetti perché si è eseguito un test il mese scorso, ma la superficie di attacco si è evoluta nel frattempo.

Gli inventari statici degli asset aggravano il problema. Negli ambienti ibridi e cloud-native, la dispersione degli asset non è solo frequente, ma è la norma. Affidarsi a elenchi compilati manualmente fa sì che la postura di sicurezza si basi su un quadro incompleto e, peggio ancora, significa che probabilmente si sta esaminando solo una frazione di quel quadro. Gli avvisi più pericolosi sono spesso quelli che non si ricevono mai, semplicemente perché l'asset non è mai stato riconosciuto o incluso nell'ambito di applicazione.

Inoltre, nessuno di questi approcci riproduce gli attacchi reali. Non replicano le TTP (tattiche, tecniche e procedure) di framework come MITRE ATT&CK. Non valutano l'efficacia delle capacità di rilevamento e risposta. Non tengono conto della capacità dell'attaccante di concatenare più esposizioni in un unico percorso estremamente devastante.

I responsabili della sicurezza lo sanno. I CISO sono perfettamente consapevoli che i loro team sono sovraccarichi di lavoro, privi di risorse e inchiodati a cicli reattivi. Sanno che la questione non è tanto se le aziende siano esposte o meno, perché ogni organizzazione lo è, ma se tali esposizioni siano sfruttabili e se sia possibile prevenirle prima che gli aggressori agiscano.

È qui che la Validazione dell'esposizione avversaria entra in gioco per colmare questo vuoto. Ma prima di capire come funziona, dobbiamo capire di cosa si tratta.

3. Il tassello mancante: la Validazione dell’esposizione avversaria (AEV)

La Validazione dell'esposizione avversaria (AEV) è un nuovo paradigma nella validazione della sicurezza, che introduce la logica dell'aggressore nella gestione quotidiana dell'esposizione. Non si tratta semplicemente di un metodo di testing, ma di una capacità operativa progettata per emulare il comportamento degli aggressori in modo continuo e preciso.

Il fulcro dell'AEV è la replica continua dell'attività di un aggressore esterno per individuare le esposizioni effettivamente sfruttabili. In un mondo in cui le minacce generate dall'IA automatizzano la reconnaissance e la distribuzione degli exploit, l'AEV risponde a una domanda più urgente: in che stato è la mia esposizione nel suo complesso?

Mettiti nei panni dell’aggressore

L'AEV agisce dall'esterno verso l'interno. Esamina l'ambiente nello stesso modo in cui lo farebbe un aggressore: da un punto di vista esterno e non attendibile. Questo aspetto è fondamentale perché elimina il presupposto che la visibilità interna equivalga alla sicurezza. Molte organizzazioni dispongono di inventari e politiche di patch ben documentati, ma ciò non significa che il loro perimetro sia sicuro. L'AEV identifica asset sconosciuti, non gestiti o mal configurati che ad altri strumenti potrebbero sfuggire.

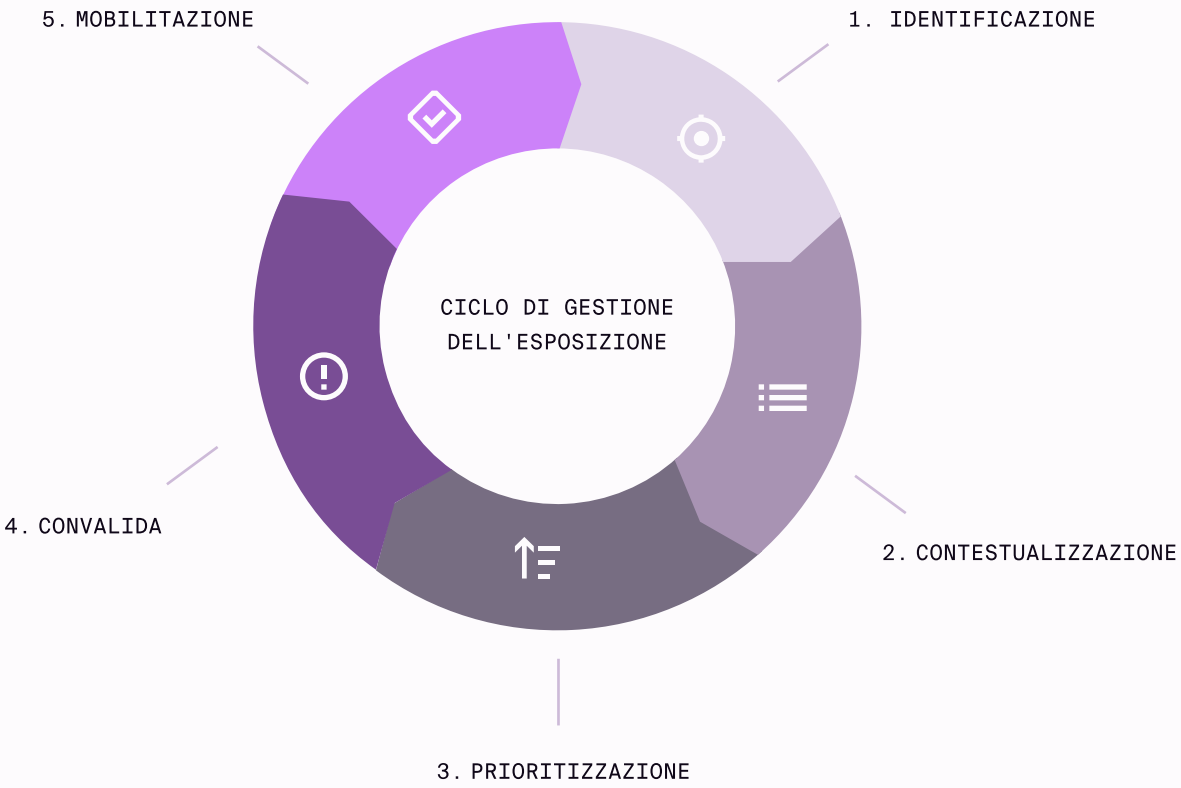
L'AEV si distingue dal red teaming, dalla simulazione di violazioni (BAS) e attacchi e da altre valutazioni sulla vulnerabilità. A differenza dei red team, l'AEV opera in modo continuo e autonomo. A differenza degli strumenti BAS, che spesso replicano sequenze di attacchi predefinite in un ambiente simile a un laboratorio, l'AEV si focalizza sul tuo perimetro effettivo. Inoltre, non si ferma all'identificazione di un CVE, ma verifica se l'esposizione è raggiungibile, sfruttabile come arma e se comporta un rischio aziendale concreto.

È complementare alla gestione della superficie di attacco esterna (Externat Attack Surface Management, EASM). L'EASM si focalizza sul rilevamento e sull'inventario degli asset connessi a Internet. L'AEV amplia l'EASM chiedendo: E quindi? Setaccia l'inventario e identifica gli asset che rappresentano minacce reali, in particolare quelli che potrebbero essere sfruttati in tempi brevi con tattiche automatizzate o potenziate dall'IA.

La filosofia unitaria della CTEM

La potenza operativa dell'AEV risiede nella sua integrazione in quadri più ampi di gestione continua dell'esposizione alle minacce (CTEM). La CTEM è un approccio strutturato alla riduzione dell'esposizione che si concentra sull'identificazione, la valutazione, l' ordinamento, la convalida e la correzione continua del rischio, prima che diventi sfruttabile. Allinea le pratiche di sicurezza alla velocità e alla fluidità delle minacce odierne, in particolare quelle guidate dall'automazione dell'IA.

La CTEM si articola in cinque fasi principali:



L'AEV interviene nelle fasi di definizione delle priorità e di convalida. Fornisce prove concrete che permettono di definire le priorità e di attivare flussi di lavoro intelligenti e mirati per la risoluzione dei problemi. Completa l'identificazione e la contestualizzazione dell'EASM e consente ai team addetti alla sicurezza di concentrarsi sulle procedure risolutive.

Le simulazioni AEV sono concepite per fermarsi all'accesso iniziale. È un aspetto fondamentale per la sicurezza e la conformità. L'obiettivo non è violare la rete o estrarre i dati, ma capire se è possibile accedervi in primo luogo. Questa scelta di progettazione consente all'AEV di operare in sicurezza negli ambienti di produzione, senza interrompere le operazioni o violare i limiti della privacy.

Da un punto di vista tecnologico, in genere le piattaforme AEV utilizzano l'automazione orchestrata, sfruttando motori di analisi, framework di simulazione degli exploit ed emulazione del comportamento. Possono essere integrate con informazioni sulle minacce per imitare i TTP più recenti osservati sul campo. Le piattaforme più avanzate adottano una logica basata sull'IA per definire le priorità degli obiettivi in base alla sfruttabilità e alla criticità aziendale.

Per i CISO e i responsabili della sicurezza, il valore dell'AEV risiede nella sua precisione ed efficienza. Convalidando continuamente le esposizioni, l'AEV fa emergere solo i risultati rilevanti. Ciò riduce l'alert fatigue, ottimizza i flussi di lavoro dedicati all'implementazione delle procedure risolutive e consente ai team addetti alla sicurezza di concentrarsi sui risultati strategici anziché sul caos tattico.

In breve, l'AEV non si limita a mostrare i punti vulnerabili, ma mostra cosa gli aggressori possono sfruttare nell'immediato.

4. Perché l’AEV ha ridefinito il concetto di velocità

Uno degli aspetti più interessanti della Validazione dell'esposizione avversaria è la sua velocità intrinseca. Non solo in termini di rapidità di identificazione delle minacce, ma anche in termini di rapidità di reazione. In un ambiente caratterizzato da minacce in cui gli aggressori possono spostarsi lateralmente in pochi minuti, la velocità non è un lusso, ma un prerequisito.

Le piattaforme AEV sono concepite per operare in modo continuo. A differenza delle scansioni periodiche o dei test programmati, l'AEV agisce in tempo reale, convalidando le esposizioni nel momento in cui emergono. Ciò significa che nel momento in cui un asset mal configurato viene esposto su internet o un nuovo CVE diventa rilevante per il tuo perimetro, l'AEV è in grado di rilevare e replicare il suo sfruttamento in pochi minuti.

Chiudere la “finestra di rischio”

Questa rapidità è fondamentale. Valuta una soluzione alternativa: ogni settimana viene eseguita una scansione e, in quel lasso di tempo, un aggressore ha identificato la stessa vulnerabilità ed è passato dall'accesso iniziale alla compromissione completa del dominio. Il tempo che intercorre tra il rilevamento e l'azione, quello che potremmo definire la “finestra di rischio”, deve essere ridotto al minimo e l'AEV è stata concepita appositamente per ridurre tale finestra.

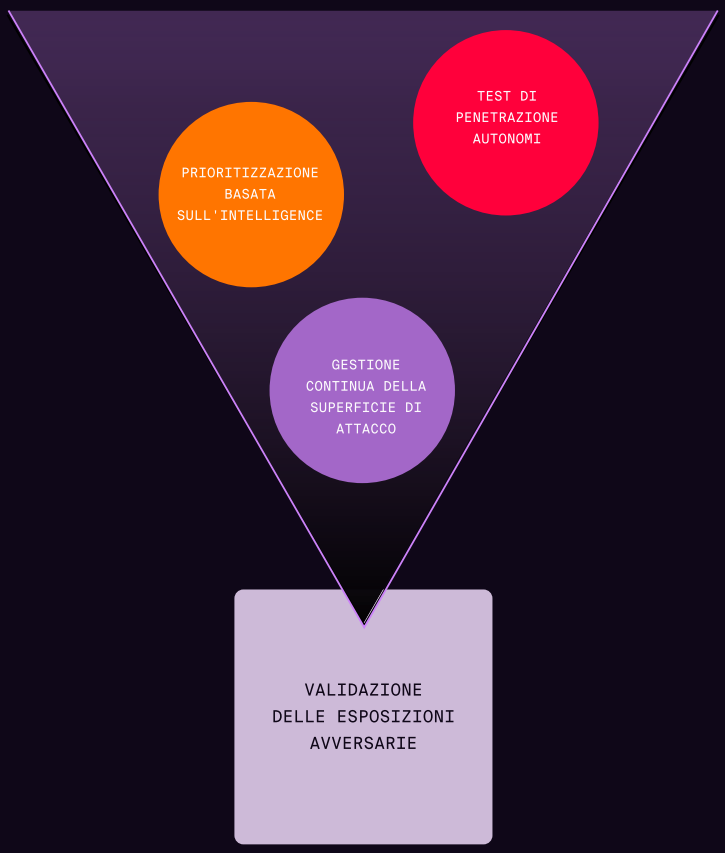
La rapidità dell'AEV è in parte dovuta al suo design architettonico. Le moderne piattaforme di convalida dell'esposizione sono generalmente distribuite in modalità SaaS, in modo da consentire valutazioni scalabili e on-demand senza la necessità di un'implementazione on-premise. Secondo Gartner, le soluzioni leader spesso sfruttano l'automazione e l'infrastruttura cloud-native per simulare il comportamento degli aggressori su asset esterni con un'interferenza minima.

Anche l'automazione consente di guadagnare in rapidità. Le piattaforme AEV come Hadrian utilizzano motori di orchestrazione per stabilire quali esposizioni testare, come testarle e quali azioni intraprendere a seconda dei risultati ottenuti. Ciò elimina la necessità di interventi manuali in ogni fase e accelera drasticamente il time-to-validation.

Inoltre, l'AEV elimina il ritardo nel triage. Altri programmi di rilevamento accumulano migliaia di risultati in una coda che deve essere esaminata manualmente e classificata per ordine di priorità. L'AEV offre risultati convalidati e basati sugli exploit. Non si tratta di rischi teorici, ma di minacce sostenute da prove e classificate per priorità. In questo modo i team addetti alla sicurezza non perdono tempo a discutere sulla gravità dei rischi, ma possono passare direttamente alla loro risoluzione.

Parte di un flusso di lavoro ben equilibrato in materia di sicurezza

L'AEV si integra perfettamente con i flussi di lavoro esistenti. Le esposizioni convalidate possono essere convogliate direttamente nelle piattaforme SIEM e SOAR o nei sistemi di gestione dei ticket come Jira per un intervento immediato. Infine, la rapidità dell'AEV consente di ottenere risultati più strategici in materia di sicurezza. Una convalida rapida comporta una risoluzione più veloce, che si traduce in cicli di feedback più serrati. A lungo andare, le organizzazioni che utilizzano l'AEV riscontrano un miglioramento della maturità operativa. Riducono il loro MTTR medio, commettono meno errori in condizioni di pressione e iniziano ad anticipare il comportamento degli aggressori anziché limitarsi a reagire.



5. Scenari di velocità del mondo reale

I CISO che cercano di giustificare l'investimento nella Validazione dell'esposizione avversaria (AEV), devono capire in che modo questa soluzione consente di intraprendere un'azione preventiva all'interno di uno scenario pratico. Di seguito viene illustrato il modo in cui l'AEV si comporta in scenari di minaccia ad alta pressione e sensibili al fattore temporale, evidenziandone la rapidità e la precisione rispetto ad altri strumenti di sicurezza.

Scenario: esposizione di un’interfaccia del pannello di controllo configurata erroneamente

Un'organizzazione lancia una nuova applicazione SaaS utilizzando l'infrastructure-as-code. Nella fretta di rispettare una scadenza per il rilascio, un ambiente di sviluppo viene inavvertitamente lasciato esposto su Internet, compreso un pannello di login dell'amministratore. Nessuno all'interno dell'organizzazione è a conoscenza dell'esposizione.

Un sistema di rilevamento potrebbe segnalare questo asset nella sua prossima scansione programmata, giorni o addirittura settimane dopo. Nel frattempo, l'asset esposto è rilevabile da chiunque conduca scansioni di rete ad ampio raggio utilizzando strumenti come Nmap.

Con l'AEV, la configurazione errata viene rilevata in pochi minuti. Il sistema AEV replica un attaccante che prende di mira lo spazio IP, individua l'interfaccia del pannello di controllo, conferma che è raggiungibile e che non dispone di controlli di base, e convalida immediatamente l'esposizione come sfruttabile. Poiché il sistema è a conoscenza del contesto aziendale (questa applicazione è collegata a un database con i dati dei clienti), segnala la problematica come altamente prioritaria.

Viene generato un avviso e inviato all'ingegnere di sicurezza appropriato con indicazioni complete per la risoluzione del problema. Tutto questo avviene in tempo reale, senza che gli aggressori abbiano la possibilità di sfruttare l'esposizione.

TEMPO
DALL'ESPOSIZIONE
ALLA CONVALIDA

12 MINUTI

TEMPO PER LA RISOLUZIONE
PREVENTIVA

<90 MINUTI

Scenario: Una nuova vulnerabilità zero-day

Una vulnerabilità zero-day colpisce un'applicazione server web ampiamente utilizzata viene rilevata e viene diffuso il codice POC. Nel giro di poche ore, i tentativi di exploit si diffondono in tutta la rete.

Alcuni team addetti alla sicurezza si affannano a incrociare i dati di questo nuovo CVE con gli inventari degli asset, spesso manualmente.

Con l'AEV, non appena la CVE viene rilevata, la piattaforma esegue la scansione di tutti gli asset esterni noti e replica il percorso di exploit contro di essi. Dei 50 server che utilizzano la versione vulnerabile, 3 sono accessibili dall'esterno e privi di patch. L'esposizione viene convalidata in tempo reale e le attività vengono generate automaticamente dal team operativo IT.

Questo processo non solo fa risparmiare tempo, ma previene i punti ciechi. **Permette di passare da una risposta generalizzata dell'organizzazione a una strategia preventiva e precisa.**

6. Creare un team di specialisti che risponda rapidamente con l'AEV

L'adozione dell'AEV non è solo una decisione riguardante uno strumento, ma anche un cambiamento del modello operativo. Questa sezione illustra come sviluppare un programma che utilizzi l'AEV per ridurre al minimo le finestre di rischio e migliorare la gestione dell'esposizione.

Tre condizioni di attivazione del test con l’AEV

I sistemi AEV sono più potenti quando sono associati direttamente agli eventi di esposizione. La piattaforma di Hadrian, ad esempio, avvia la convalida automatica in risposta a:

01 **Esposizione di nuovi asset:** qualsiasi nuovo IP, servizio o dominio accessibile dall'esterno.

02 **Modifiche agli asset esistenti:** modifiche a configurazioni, liste di controllo degli accessi (ACL) o sistemi di nome di dominio (DNS) che alterano il livello di rischio.

03 **Comparsa di nuovi exploit o TTP di attori pericolosi,** sia che provengano da feed di informazioni sulle minacce sia che vengano scoperti tramite il monitoraggio del dark web.

Questo modello basato sugli eventi garantisce che l'AEV non funzioni solo su una base temporale, ma anche in funzione di un contesto.

Metriche operative fondamentali

Abbiamo menzionato queste statistiche in precedenza, ma ribadiamo la loro importanza. Per valutare l'impatto dell'AEV, i responsabili della sicurezza dovrebbero tenere traccia di:

- **MTTP (Mean Time to Prevent):** la velocità con cui gli asset possono essere rilevati, convalidati e corretti per un'esposizione sfruttabile.
- **MTTV (Mean Time to Validate):** il tempo necessario per capire se l'esposizione è effettivamente sfruttabile.
- **MTTR (Mean Time to Remediate):** il tempo che intercorre tra la convalida e la risoluzione o la mitigazione.

L'AEV riduce in modo significativo l'MTTV (da giorni a minuti) e, fornendo dati chiari e convalidati, accelera anche l'MTTR. Sommando queste due metriche con l'MTTD si ottiene l'MTTP. Quando i risultati non sono ipotetici, c'è meno resistenza da parte dell'IT e un'esecuzione più rapida da parte dei team di sviluppo e operativi.

Strategie risolutive basate sui ruoli

Le minacce convalidate vengono indirizzate a specifici stakeholder, in modo che non ci siano silos informativi. Gli sviluppatori ricevono i risultati relativi alle configurazioni errate a livello di codice. L'IT riceve ticket per le esposizioni dell'infrastruttura. I team responsabili della conformità possono esaminare i dashboard di sola lettura per il monitoraggio e la reportistica. Il valore dell'AEV si moltiplica se collegato a un sistema di responsabilità più ampio. Ma può essere altrettanto efficace per i team più piccoli, in quanto automatizza gran parte del lavoro.

I risultati dell'AEV influenzano anche i registri dei rischi, i report del consiglio di amministrazione e i test di controllo continuo, così da legare la sicurezza alla supervisione strategica.

7. Risoluzione rapida

In un'era in cui gli avversari testano le vulnerabilità entro 15 minuti (forse anche più velocemente se si utilizzano strumenti IA) dalla loro divulgazione, non bisogna perdere nemmeno un secondo. L'unico modo per avere la meglio sulla rapidità degli attacchi è migliorare la rapidità della prevenzione.

A differenza di altri strumenti che possono sovraccaricare i team che si occupano dei dati, l'AEV offre chiarezza. A differenza dei red team che convalidano solo occasionalmente e solo entro un certo ambito, l'AEV effettua una convalida continua. E a differenza dei modelli di rischio che sono speculativi, l'AEV dimostra la sfruttabilità sul campo.

Per i team CISO e SOC, questo significa maggiore controllo, migliore definizione delle priorità e una riduzione misurabile del rischio operativo. L'AEV comprime le tempistiche, allinea i risultati tecnici all'impatto aziendale e fa passare il team da un approccio reattivo a una resilienza proattiva e in tempo reale.

> Non è possibile rallentare i criminali informatici, ma con l'AEV si può stare un passo avanti a loro.