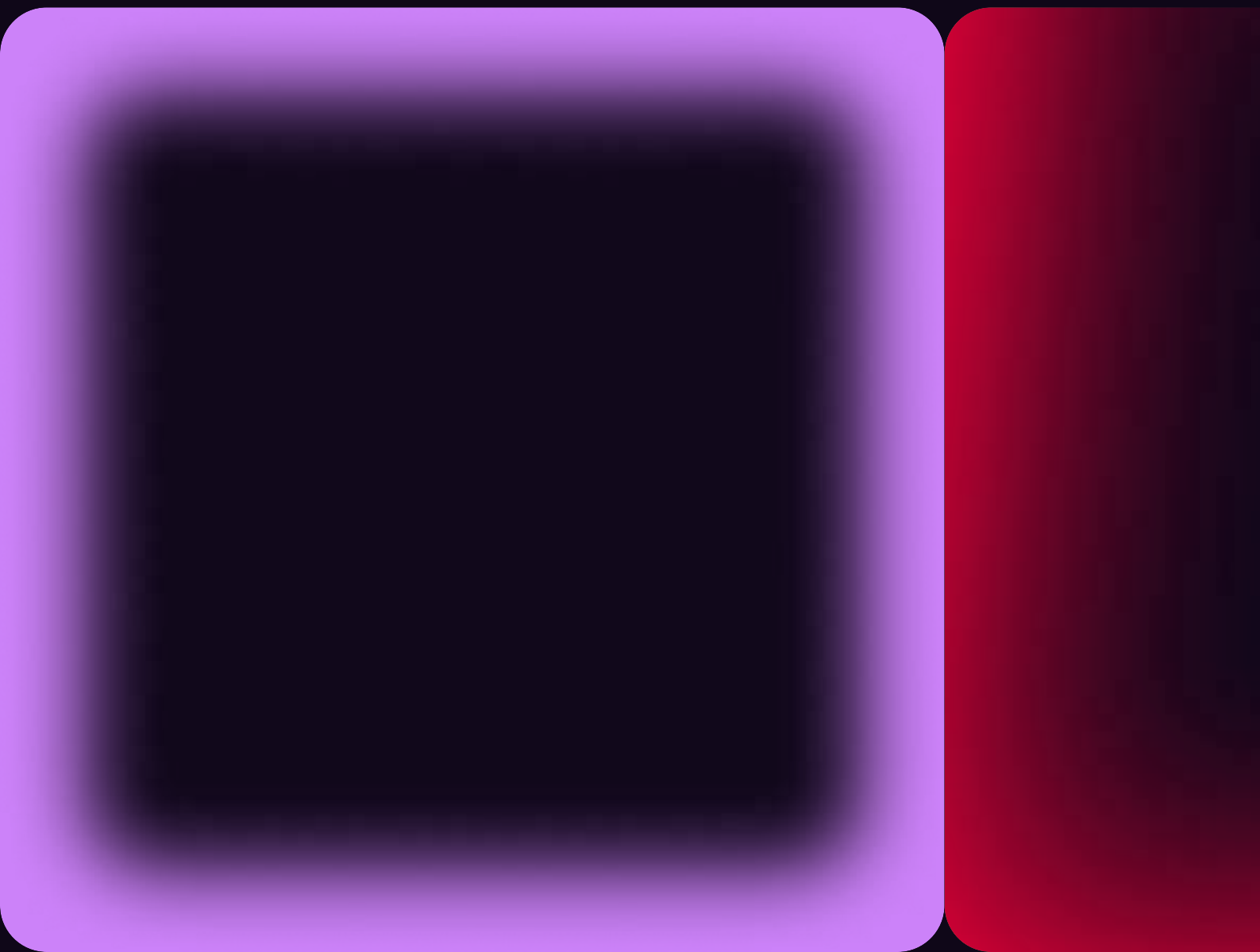
HADRIAN

WHITEPAPER

Wie Adversarial Exposure Validation Sicherheitsvorfälle durch Automatisierung verhindert



Inhaltsverzeichnis

Zusammenfassung

Zusammenfassung

Cyberbedrohungen entwickeln sich heute mit einer Geschwindigkeit, die alles Bisherige übertrifft. Bereits 2022 begannen Angreifer, nur 15 Minuten nach einer Offenlegung damit, nach Schwachstellen zu suchen. Und das war vor drei Jahren – noch vor dem Einsatz KI-gestützter Hacking-Tools. Heute ist künstliche Intelligenz einer der Haupttreiber dieser Beschleunigung. KI-generierte Angriffe ermöglichen es Cyberkriminellen, ihre Informationsbeschaffung zu automatisieren, Schwachstellen sofort auszunutzen und ihre Attacken in einem Tempo hochzufahren, mit dem menschliche Verteidiger kaum Schritt halten können.

Laut dem Verizon 2025 Data Breach Incident Report sind Verstöße durch Ausnutzung von Schwachstellen in den letzten zwei Jahren um 275 % gestiegen – befeuert durch Zero-Day-Exploits und eine schnellere Ausrichtung auf Edge-Geräte. In der Zwischenzeit beträgt die mittlere Zeit zur Behebung von internet-exponierten Schwachstellen 32 Tage, wobei fast ein Drittel überhaupt nie behoben wird. Im Jahr 2025 meldete CrowdStrike eine durchschnittliche Breakout-Zeit von nur 48 Minuten – der schnellste Fall lag bei 51 Sekunden. Gegen KI-gestützte Angreifer ist eine reine Detektion nicht mehr schnell genug – Organisationen müssen Prävention zur Priorität machen.

Hier kommt die Adversarial Exposure Validation (AEV) ins Spiel. Indem sie kontinuierlich das Verhalten von Angreifern von außen nach innen emuliert, validiert AEV in Echtzeit, welche Expositionen tatsächlich verwertbar sind. Sie durchbricht Alarmmüdigkeit, eliminiert Vermutungen und befähigt Sicherheitsteams, zu handeln, bevor ein Vorfall eintritt – nicht danach.

Die Angreifer warten nicht. Ihr könnt es euch auch nicht leisten.

1. Geschwindigkeit tötet

In der Cybersicherheitsbranche ist seit Langem bekannt, dass Geschwindigkeit der entscheidende Faktor ist, um Sicherheitsverletzungen zu verhindern oder zumindest einzudämmen. Doch die „Time to Compromise“ hat sich schneller verkürzt, als viele erwartet haben. Die sogenannte Breakout-Zeit – also der Zeitraum zwischen dem ersten Zugriff eines Angreifers und seiner lateralen Bewegung innerhalb eines Netzwerks – wird heute nicht mehr in Tagen, Stunden oder auch nur Minuten gemessen. Es geht zunehmend um Sekunden.

Der CrowdStrike Global Threat Report 2025 zeichnet ein alarmierendes Bild: Über Tausende untersuchter Vorfälle hinweg lag die durchschnittliche Breakout-Zeit bei nur 48 Minuten. Besonders besorgniserregend: Einige Angriffe zeigten Breakout-Geschwindigkeiten von weniger als einer Minute. In einem prominenten Fall, der einer finanziell motivierten eCrime-Gruppe zugeschrieben wird, erfolgte die vollständige laterale Bewegung in einer hybriden Cloud-Umgebung innerhalb von 51 Sekunden.

Schon im Jahr 2022 begannen Hacker, innerhalb von 15 Minuten nach einer Offenlegung nach Schwachstellen zu scannen. Doch 2022 markierte erst den Anfang des Zeitalters generativer KI. Heute, drei Jahre später, nutzen Angreifer KI-gestützte Tools effektiv, um ihre Arbeit schneller, effizienter und gefährlicher zu machen. Dieses 15-Minuten-Fenster dürfte sich mittlerweile auf wenige Sekunden reduziert haben.

01 Diese Geschwindigkeit stellt Verteidiger vor tiefgreifende operative Herausforderungen.

02 Große Sprachmodelle werden inzwischen dazu eingesetzt, die Entdeckung von Schwachstellen zu automatisieren, Low-Severity-Probleme zu echten Exploits zu koppeln und exponierte Assets in einem zuvor nie dagewesenen Umfang und Tempo anzugreifen.

03 Dies zeigt, dass Verteidigung ihrer Natur nach bereits zu spät ist.

Historische Maßstäbe greifen zu kurz

Hinzu kommt: Patch-Management ist im Vergleich zur Geschwindigkeit heutiger Angreifer erschreckend langsam. Laut dem Verizon DBIR 2025 beträgt die durchschnittliche Zeit zur Behebung von Schwachstellen auf internetzugänglichen Systemen 32 Tage. Noch gravierender: Etwa 30 % der Schwachstellen auf Edge-Geräten werden überhaupt nicht behoben. Angesichts der Tatsache, dass die Ausnutzung neu entdeckter Schwachstellen oft innerhalb von fünf Tagen beginnt – bei Edge-Geräten sogar am Tag der Offenlegung – ist klar, dass rein patchbasierte Abwehrstrategien nicht ausreichen, um modernen Bedrohungsakteuren standzuhalten.

HACKER SCANNEN NACH SCHWACHSTELLEN KURZ NACH DEREN VERÖFFENTLICHUNG

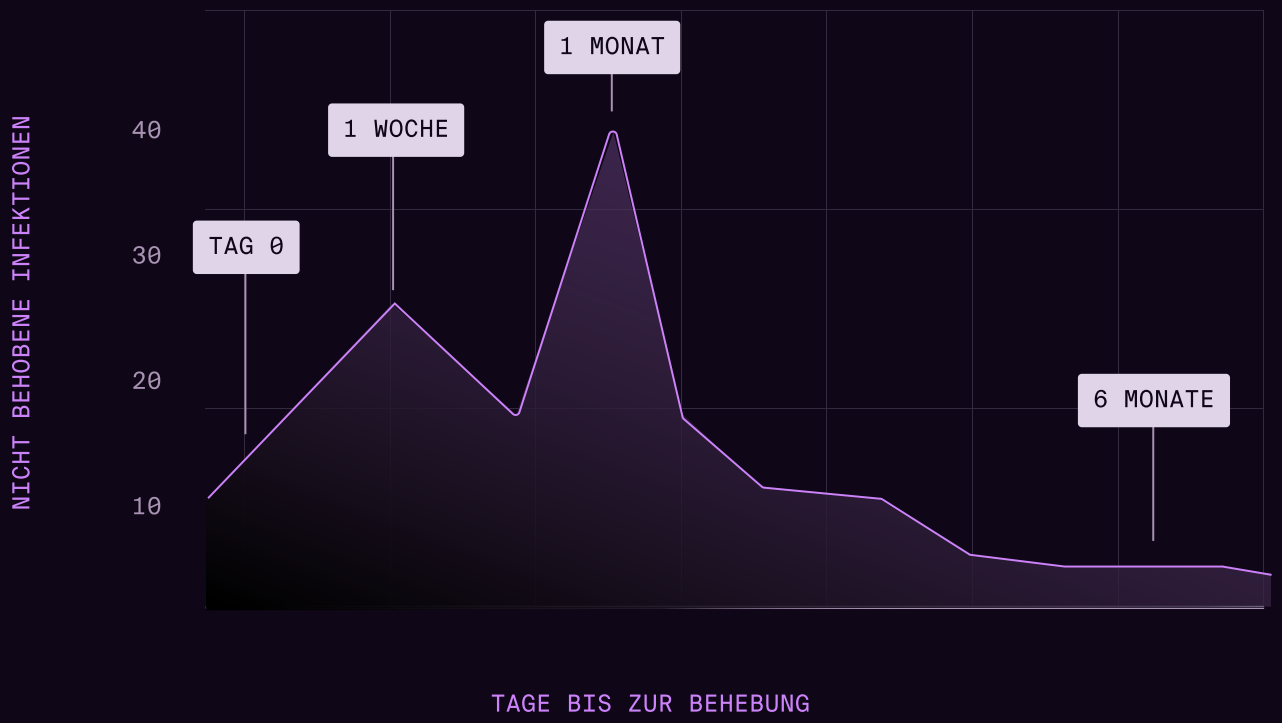
<15 MINUTES

ANSTIEG DER SCHWACHSTELLEN-AUSNUTZUNG SEIT 2023

UP 275%

DURCHSCHNITTLICHE BREAKOUT-ZEIT IM JAHR 2025

48 MINUTES



Operative Altlasten bremsen Sie aus

Ein weiterer massiver Druckfaktor für CISOs sind begrenzte Ressourcen. Noch nie mussten CISOs so viele Tools managen – bei gleichbleibender oder sogar schrumpfender Teamgröße. Budgets stehen unter genauer Beobachtung. Sicherheitsteams versinken in Warnmeldungen und sind gezwungen, Risiken ohne ausreichenden Kontext zu priorisieren. Viele Organisationen haben schlichtweg nicht das Personal, um jede Meldung zu prüfen, jede Bedrohung zu validieren oder jedem Fehlalarm nachzugehen. Das sind nur einige der operativen Zwänge, mit denen SOC-Teams täglich kämpfen:

01 Eine Vielzahl an Sicherheitstools, deren Pflege Zeit und Ressourcen bindet.

02 Sicherheitsteams leiden unter Alarmmüdigkeit und einem stetig wachsenden Backlog.

03 Compliance-Berichte lenken vom operativen Tagesgeschäft ab.

Eine der tückischsten Herausforderungen für Sicherheitsteams ist fragmentierte Sichtbarkeit. Alles, was Sie nicht sehen, verschafft Angreifern zusätzliche Angriffsmöglichkeiten – und Munition für den nächsten Exploit.

Vor allem bei Übernahmen und Fusionen entstehen Risiken: Unternehmen übernehmen dabei nicht nur Infrastruktur, sondern auch unbekannte Subdomains und Legacy-Systeme, die nie mit einem zentralen Sicherheitsansatz entwickelt wurden. Gleichzeitig starten Marketing-Teams immer wieder Microsites, registrieren neue Domains oder binden Drittanbieter-Tools ein – meist ohne Rücksprache mit der IT-Sicherheit.

In Summe führen solche Silos zu einer fragmentierten Sicht auf die Angriffsfläche – und damit zu Lücken, die Angreifer gezielt und mit enormer Geschwindigkeit ausnutzen, gegen die Sie sich kaum verteidigen können. Shadow IT gedeiht in diesen blinden Flecken und schafft Schwachstellen, von denen das Sicherheitsteam oft erst dann erfährt, wenn es zu spät ist. Auch hier gilt: Nur ein präventiver Sicherheitsansatz ermöglicht durchgehende Transparenz über alle potenziellen Angriffsflächen hinweg.

Statische Verteidigung reicht nicht mehr aus

Vor diesem Hintergrund sind traditionelle Sicherheitsmodelle – etwa punktuelle Scans, Compliance-Checklisten oder jährliche Penetrationstests – den heutigen, extrem schnellen Angriffsmethoden nicht mehr gewachsen. Eine manuelle Patch-Prüfung kann mit Gegnern, die im KI-Tempo agieren, nicht mithalten. Red-Team-Übungen pro Quartal sind zwar wertvoll, liefern aber immer nur eine Momentaufnahme – und decken nur den jeweils definierten Bereich ab.

In einer Umgebung, in der jede Sekunde zählt, brauchen Verteidiger kontinuierliche Sichtbarkeit, laufende Validierung und eine fortlaufende Priorisierung realer Risiken.

Die Metriken, die wirklich zählen

Im Zeitalter von 48-Minuten-Breakouts muss auch die Leistung von Sicherheitsteams mit neuen Kennzahlen gemessen werden – darunter:

- **Mean Time to Prevent (MTTP):** Wie schnell lassen sich Risiken erkennen, validieren und beheben, bevor eine Schwachstelle ausgenutzt wird?
- **Mean Time to Validate (MTTV):** Wie zügig können potenzielle Risiken als tatsächlich ausnutzbar bestätigt werden?
- **Mean Time to Remediate (MTTR):** Wie rasch werden kritische Schwachstellen beseitigt oder neutralisiert?

Organisationen, die keine ambitionierten Ziele für diese Kennzahlen verfolgen, gelten heute nicht mehr nur als Nachzügler – sie bewegen sich auf extrem gefährlichem Terrain.

2025 und darüber hinaus gilt: Sicherheitsteams müssen mit der Haltung arbeiten, dass jede Minute zählt. Ob gegen Ransomware-Banden, APTs oder opportunistische Angreifer – der entscheidende Unterschied wird künftig darin liegen, wie schnell echte Risiken erkannt, validiert und priorisiert werden können. Das wird darüber entscheiden, wer sich schützt – und wer zum Ziel wird.

2. Andere Tools bringen Sie weit – aber nicht weit genug

In der Cybersicherheit ist es üblich, ein ganzes Portfolio an Tools einzusetzen, um Bedrohungen einen Schritt voraus zu sein. Doch nicht alle Werkzeuge sind gleichwertig.

Punktuelle Sicherheitslösungen, regelmäßige Penetrationstests und statische Asset-Inventare sind typisch für ein reaktives Sicherheitsmodell. Diese Tools haben in bestimmten Kontexten durchaus ihre Berechtigung – doch in einer Welt, in der sich Bedrohungen in Echtzeit entwickeln und sich externe Angriffsflächen stündlich verändern, reichen sie nicht mehr aus.

Wenn der Alarm zur Routine wird

Ein Übermaß an Warnmeldungen führt unweigerlich zur Alarmmüdigkeit. Sicherheitsteams werden mit Schwachstellenberichten und Asset-Listen überschwemmt, die keinerlei Priorisierung enthalten. Ohne Validierung verschwenden sie wertvolle Zeit mit der Einschätzung von Meldungen, die sich später als Fehlalarme oder kaum relevante Risiken herausstellen. Gleichzeitig gehen tatsächlich ausnutzbare Angriffsvektoren in der Masse unter – oder bleiben gänzlich unentdeckt. Typische Beispiele für Warnungen, die Lärm verursachen, aber wenig Nutzen bringen:

NIEDRIG
EINGESTUFTE CVES:

Meldungen zu veralteten Bibliotheken oder geringfügigen Schwachstellen, die kein realistisches Risiko darstellen – insbesondere wenn es keine funktionierenden Exploits gibt oder kompensierende Schutzmaßnahmen greifen.

REIN INTERNE ASSETS:

Funde auf nicht öffentlich zugänglichen Assets – etwa Entwicklungsumgebungen oder Backend-Diensten – die dennoch markiert werden, obwohl sie von außen gar nicht erreichbar sind.

Willkommen im „Theaterstück der Sicherheit“

Regelmäßige Penetrationstests sind kein gleichwertiger Ersatz für echte, kontinuierliche Angriffsvalidierung. Selbst erstklassige, manuelle Pentests finden meist nur quartalsweise oder jährlich statt. Das Ergebnis: ein trügerisches Gefühl von Sicherheit – ein „Theaterstück der Sicherheit“. Sie fühlen sich geschützt, weil erst kürzlich ein Test durchgeführt wurde. Doch Ihre Angriffsfläche hat sich in der Zwischenzeit längst verändert.

Statische Asset-Inventare verschärfen das Problem. In hybriden und Cloud-nativen Umgebungen ist Asset-Wildwuchs nicht die Ausnahme, sondern der Normalzustand. Wer sich auf manuell gepflegte Bestandslisten verlässt, baut seine Sicherheitsstrategie auf einer unvollständigen Grundlage auf – und testet schlimmstenfalls nur einen kleinen Teil der tatsächlichen Infrastruktur. Die gefährlichsten Warnungen sind oft jene, die Sie gar nicht erst erhalten – weil das zugrunde liegende Asset nie erfasst oder in den Prüfbereich aufgenommen wurde.

Hinzu kommt: Keiner dieser Ansätze bildet das Verhalten echter Angreifer realistisch ab. Weder spiegeln sie die TTPs (Tactics, Techniques and Procedures) aus Frameworks wie MITRE ATT&CK wider, noch bewerten sie die Wirksamkeit Ihrer Detection- und Response-Fähigkeiten. Sie berücksichtigen auch nicht die Fähigkeit von Angreifern, mehrere scheinbar harmlose Schwachstellen zu einer kritischen Angriffskette zu kombinieren.

Sicherheitsverantwortliche wissen das. CISOs sind sich sehr bewusst, dass ihre Teams überlastet, unterbesetzt und in einem reaktiven Dauermodus gefangen sind. Die entscheidende Frage ist dabei nicht, ob es Schwachstellen gibt – denn die hat jedes Unternehmen. Sondern: Sind diese Schwachstellen ausnutzbar? Und können sie behoben werden, bevor Angreifer aktiv werden?

Genau hier beginnt Adversarial Exposure Validation, diese Lücke zu schließen. Doch bevor wir betrachten, wie das funktioniert, müssen wir zunächst klären, was genau AEV eigentlich ist.

3. Das fehlende Puzzleteil: Adversarial Exposure Validation (AEV)

Adversarial Exposure Validation (AEV) ist ein neues Paradigma im Bereich der Sicherheitsvalidierung – eines, das die Denkweise von Angreifern in Ihr tägliches Exposure Management integriert. Es handelt sich nicht einfach um eine weitere Testmethode. Es ist eine operative Fähigkeit, die darauf ausgelegt ist, das Verhalten realer Angreifer kontinuierlich und präzise zu emulieren.

Im Kern ist AEV die fortlaufende Nachbildung externer Angreiferaktivitäten, mit dem Ziel, herauszufinden, welche Schwachstellen tatsächlich ausnutzbar sind. In einer Welt, in der KI-generierte Bedrohungen Aufklärung und Exploit-Ausführung automatisieren, beantwortet AEV die entscheidendere Frage: Wie steht es aktuell um meine gesamte Angriffsfläche?

Nehmen Sie die Perspektive Ihrer Angreifer ein

AEV arbeitet von außen nach innen. Es betrachtet Ihre Umgebung aus demselben Blickwinkel wie ein echter Angreifer: von einem unautorisierten, externen Standpunkt aus. Das ist entscheidend – denn es durchbricht die trügerische Annahme, dass interne Sichtbarkeit automatisch Sicherheit bedeutet. Viele Organisationen verfügen über gut dokumentierte Inventare und Patch-Richtlinien – doch das heißt nicht, dass ihre Perimeter auch wirklich sicher sind. AEV deckt unbekannte, nicht verwaltete oder fehlerhaft konfigurierte Assets auf, die andere Tools oft übersehen.

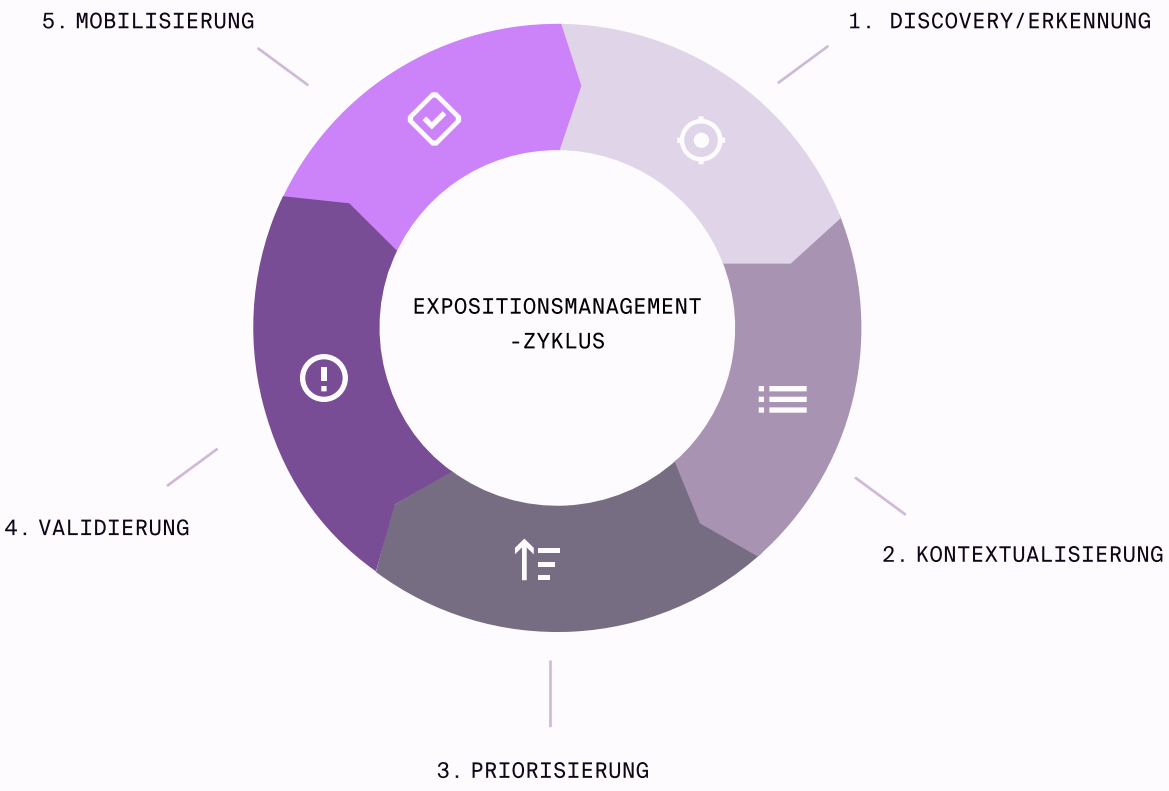
AEV unterscheidet sich klar von Red-Teaming, Breach and Attack Simulation (BAS) oder klassischen Schwachstellenanalysen. Im Gegensatz zu Red Teams ist AEV kontinuierlich und autonom im Einsatz. Und anders als viele BAS-Tools, die in Laborumgebungen vordefinierte Angriffsketten abspielen, fokussiert sich AEV auf Ihre reale, live erreichbare Angriffsfläche. Dabei bleibt es nicht bei der Identifikation einer CVE stehen – AEV prüft, ob die Schwachstelle erreichbar, ausnutzbar und mit einem konkreten geschäftlichen Risiko verbunden ist.

AEV ergänzt das External Attack Surface Management (EASM). Während EASM darauf abzielt, öffentlich erreichbare Systeme zu entdecken und zu inventarisieren, geht AEV einen Schritt weiter und stellt die entscheidende Frage: Und was bedeutet das jetzt konkret? Es durchforstet Ihr Asset-Inventar und identifiziert jene Komponenten, die tatsächlich ein Risiko darstellen – insbesondere solche, die sich mithilfe automatisierter oder KI-gestützter Taktiken besonders schnell ausnutzen lassen.

Die ganzheitliche Philosophie von CTEM

Was AEV operativ so leistungsfähig macht, ist seine Einbettung in umfassendere Frameworks wie das Continuous Threat Exposure Management (CTEM). CTEM ist ein strukturierter Ansatz zur Risikoreduzierung, der darauf abzielt, Bedrohungspotenziale kontinuierlich zu identifizieren, zu bewerten, zu priorisieren, zu validieren und zu beheben – noch bevor sie ausgenutzt werden können. Damit synchronisiert CTEM sicherheitsrelevante Prozesse mit dem Tempo und der Dynamik moderner Bedrohungen – insbesondere solcher, die durch KI-gestützte Automatisierung vorangetrieben werden.

CTEM gliedert sich in fünf zentrale Phasen:



AEV wirkt vor allem in den Phasen Priorisierung und Validierung. Es liefert belastbare Echtzeitdaten, auf deren Basis Risiken sinnvoll eingeordnet und gezielte Maßnahmen abgeleitet werden können. Damit ergänzt AEV die vorangehenden Phasen der Erkennung und Kontextualisierung durch EASM – und ermöglicht es Sicherheitsteams, sich auf das Wesentliche zu konzentrieren: die wirksame Behebung tatsächlicher Risiken.

AEV-Simulationen enden bewusst beim ersten Zugriff. Das ist entscheidend für Sicherheit und Compliance: Ziel ist es nicht, in ein Netzwerk einzudringen oder Daten zu exfiltrieren – sondern festzustellen, ob ein Zugriff überhaupt möglich wäre. Diese bewusste Designentscheidung ermöglicht den sicheren Einsatz von AEV in Production-Umgebungen, ohne den laufenden Betrieb zu stören oder den Datenschutz zu verletzen.

Aus technologischer Sicht basieren AEV-Plattformen typischerweise auf koordiniert eingesetzter Automatisierung. Sie nutzen Scan-Engines, Exploit-Simulationsframeworks und die Emulation von Angreiferverhalten. Oft werden sie durch Threat Intelligence ergänzt, um die neuesten in freier Wildbahn beobachteten TTPs realitätsnah nachzubilden. Die fortschrittlichsten Plattformen integrieren zusätzlich KI-basierte Entscheidungslogik, um Ziele auf Basis von Ausnutzbarkeit und geschäftlicher Relevanz zu priorisieren.

Für CISOs und Sicherheitsverantwortliche liegt der Mehrwert von AEV vor allem in Präzision und Effizienz. Durch die kontinuierliche Validierung werden ausschließlich relevante Schwachstellen identifiziert – also solche, die tatsächlich ausgenutzt werden könnten. Das reduziert die Alarmmüdigkeit, optimiert die Behebungsprozesse und verschafft Sicherheitsteams den nötigen Freiraum, sich auf strategische Maßnahmen statt auf operatives Klein-Klein zu konzentrieren.

Kurz gesagt: AEV zeigt Ihnen nicht nur, wo potenzielle Schwachstellen liegen – sondern was Angreifer als Nächstes ausnutzen könnten. Und zwar jetzt gerade.

4. Warum AEV Geschwindigkeit eine neue Bedeutung gibt

Einer der überzeugendsten Aspekte von Adversarial Exposure Validation ist ihre Geschwindigkeit. Gemeint ist dabei nicht nur, wie schnell Bedrohungen erkannt werden – sondern vor allem, wie schnell auf diese Erkenntnisse zielgerichtet reagiert werden kann. In einer Bedrohungslandschaft, in der Angreifer sich innerhalb von Minuten lateral im Netzwerk bewegen können, ist Geschwindigkeit kein Luxus – sondern eine Grundvoraussetzung.

AEV-Plattformen sind darauf ausgelegt, kontinuierlich zu arbeiten. Anders als periodische Scans oder geplante Tests validiert AEV in Echtzeit, sobald neue Schwachstellen auftauchen. Das bedeutet: Sobald ein fehlkonfiguriertes Asset öffentlich zugänglich ist oder eine neue CVE für Ihre Perimeter-Infrastruktur relevant wird, kann AEV innerhalb von Minuten die potenzielle Ausnutzung erkennen und simulieren.

Schließen Sie das „Risikofenster”

Diese Unmittelbarkeit ist entscheidend. Zum Vergleich: Ein herkömmlicher Scanner läuft einmal pro Woche – in dieser Zeit hat ein Angreifer dieselbe Schwachstelle entdeckt und sich vom Erstzugriff bis zur vollständigen Domänenübernahme vorgearbeitet. Der Zeitraum zwischen Entdeckung und Reaktion – das sogenannte „Risikofenster“ – muss so stark wie möglich minimiert werden. AEV wurde genau dafür konzipiert.

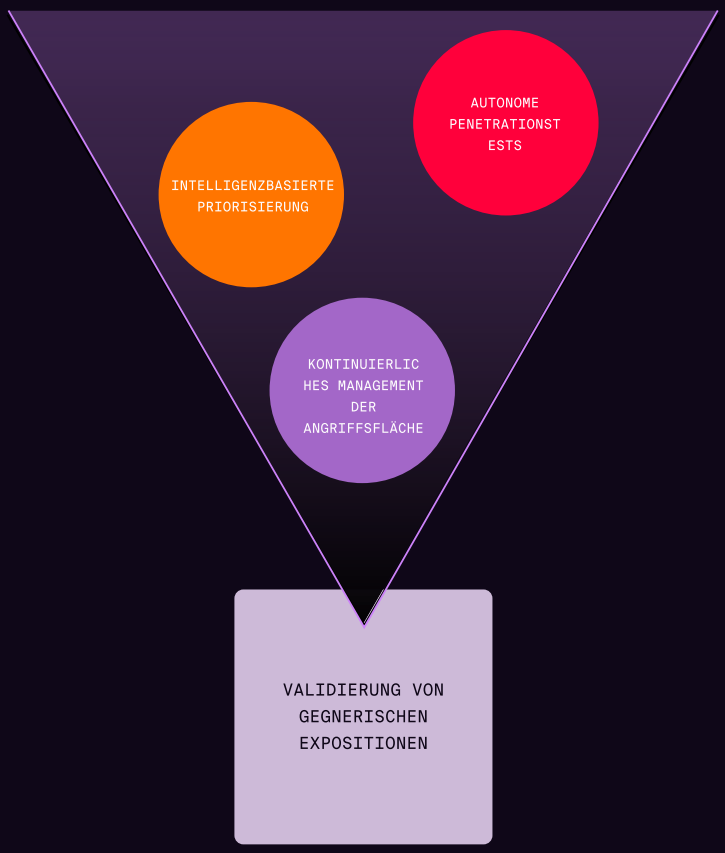
Ein Grund für die hohe Geschwindigkeit liegt im Aufbau moderner AEV-Plattformen. Sie werden typischerweise als SaaS-Lösungen bereitgestellt, was skalierbare, bedarfsgerechte Analysen ohne den Aufwand von lokalem Deployment ermöglicht. Laut Gartner setzen führende Anbieter auf Automatisierung und cloud-native Infrastruktur, um Angreiferverhalten über externe Assets hinweg realitätsnah und mit minimaler Beeinträchtigung zu simulieren.

Die Geschwindigkeit ergibt sich außerdem durch umfassende Automatisierung. AEV-Plattformen wie Hadrian nutzen Orchestrierungs-Engines, die bestimmen, welche Schwachstellen getestet werden, wie sie getestet werden und welche Schritte sich aus den Ergebnissen ergeben. Dadurch entfällt die Notwendigkeit manueller Eingriffe in jeder Phase – und die Zeit bis zur Validierung wird massiv reduziert.

Besonders wichtig: AEV beseitigt die typischen Verzögerungen durch manuelle Priorisierung. Klassische Scanner produzieren Tausende Findings, die zunächst manuell sortiert und bewertet werden müssen. AEV hingegen identifiziert validierte, ausnutzbare Schwachstellen. Keine theoretischen Risiken, sondern evidenzbasierte, priorisierte Bedrohungen. Das heißt: Ihre Sicherheitsteams verlieren keine Zeit mit Diskussionen über Schweregrade – sie können sofort mit der Behebung beginnen.

Teil eines ausgewogenen Security-Workflows

AEV fügt sich außerdem nahtlos in Ihre bestehenden Workflows ein. Validierte Schwachstellen lassen sich direkt in SIEM- oder SOAR-Plattformen integrieren – oder über Tools wie Jira als Tickets weiterverarbeiten. Und: Die Geschwindigkeit von AEV ermöglicht strategischere Sicherheitsentscheidungen. Schnelle Validierung führt zu schnellerer Behebung – und schafft kürzere Feedback-Zyklen. Mit der Zeit steigern Organisationen, die AEV einsetzen, ihre operative Reife: Sie senken ihre durchschnittliche MTTR, machen unter Druck weniger Fehler – und beginnen, Angreiferverhalten zu antizipieren, statt nur darauf zu reagieren.



5. Geschwindigkeitsszenarien in der Praxis

CISOs, die eine Investition in Adversarial Exposure Validation (AEV) rechtfertigen möchten, brauchen handfeste Belege dafür, wie AEV präventives Handeln in realen Situationen ermöglicht. Im Folgenden zeigen wir Ihnen, wie sich AEV in zeitkritischen Bedrohungsszenarien bewährt – und wie schnell und präzise es im Vergleich zu anderen Sicherheitstools reagiert.

Szenario: Eine fehlkonfigurierte Admin-Oberfläche wird öffentlich

Ein Unternehmen bringt eine neue SaaS-Anwendung auf den Markt – bereitgestellt über Infrastructure-as-Code. Im Endspurt vor dem Release wird versehentlich eine Entwicklungsumgebung samt Admin-Login-Oberfläche öffentlich zugänglich gemacht. Intern weiß niemand von dieser offenen Angriffsfläche.

Ein klassischer Schwachstellenscanner könnte dieses Asset bei der nächsten geplanten Prüfung erkennen – also erst in einigen Tagen oder sogar Wochen. In der Zwischenzeit ist das exponierte Asset für jeden sichtbar, der breite Scans mit Tools wie Nmap durchführt.

Mit AEV im Einsatz erkennen Sie die Fehlkonfiguration innerhalb von Minuten. Das AEV-System simuliert das Verhalten eines Angreifers, scannt den IP-Bereich, identifiziert die Admin-Oberfläche, bestätigt deren Erreichbarkeit und das Fehlen grundlegender Schutzmechanismen – und validiert die Schwachstelle unmittelbar als ausnutzbar. Da das System über den geschäftlichen Kontext informiert ist – etwa, dass die Anwendung auf eine Datenbank mit Kundendaten zugreift – wird der Vorfall automatisch als hochprioritär eingestuft.

Eine Warnung wird generiert und direkt an die zuständige Sicherheitsfachkraft weitergeleitet – inklusive konkreter Handlungsempfehlungen zur Behebung. All das geschieht schneller, als ein Angreifer überhaupt reagieren kann.

ZEIT VON DER OFFENLEGUNG BIS ZUR VALIDIERUNG

12 MINUTEN

ZEIT BIS ZUR PRÄVENTIVEN BEHEBUNG

<90 MINUTEN

Szenario: Eine neue Zero-Day-Schwachstelle wird bekannt

Eine Zero-Day-Schwachstelle in einer weit verbreiteten Webserver-Anwendung wird öffentlich gemacht – inklusive Proof-of-Concept-Code. Innerhalb weniger Stunden sind erste internetweite Exploit-Versuche im Gange.

Einige Sicherheitsteams beginnen nun hektisch, die neue CVE manuell mit ihren Asset-Inventaren abzugleichen – oft unter Zeitdruck und mit lückenhaften Informationen.

Mit AEV hingegen beginnt die Plattform sofort nach Veröffentlichung der CVE damit, alle bekannten extern erreichbaren Assets zu scannen – und den möglichen Exploitpfad automatisiert gegen diese Systeme zu simulieren. Von insgesamt 50 Servern, die die verwundbare Version verwenden, werden 3 als extern erreichbar und ungepatcht identifiziert. Die Schwachstelle wird in Echtzeit validiert, und es werden automatisch Aufgaben für das IT-Operations-Team erstellt.

Dieser Prozess spart nicht nur Zeit – er verhindert blinde Flecken. **Statt einer überhasteten, organisationsweiten Krisenreaktion entsteht ein zielgerichteter, proaktiver Ablauf.**

6.
Bauen Sie ein schlagkräftiges Sicherheitsteam mit AEV auf

Die Einführung von AEV ist mehr als nur eine Tool-Entscheidung – sie bedeutet einen Wandel in Ihrem operativen Sicherheitsmodell. In diesem Abschnitt zeigen wir, wie Sie ein Programm aufbauen, das AEV nutzt, um Risikofenster zu minimieren und Ihr Exposure Management auf das nächste Level zu heben.

Drei Auslöser für AEV-gestützte Tests

AEV-Systeme entfalten ihre volle Wirkung, wenn sie direkt an konkrete Ereignisse im Kontext von Angriffsflächen gekoppelt sind. Die Plattform von Hadrian startet automatisierte Validierungen bei folgenden Auslösern:

01 **Neue externe Angriffsfläche –** z. B. eine neue öffentlich erreichbare IP-Adresse, ein Dienst oder eine Domain.

02 **Änderungen an bestehenden Assets –** etwa modifizierte Konfigurationen, veränderte Access Control Lists (ACLs) oder DNS-Änderungen, die das Risikoprofil verändern.

03 **Neue Exploits oder TTPs durch Bedrohungsakteure –** bezogen auf Informationen aus Threat-Intelligence-Feeds oder durch Monitoring von Darknet-Quellen.

Dieses ereignisbasierte Modell sorgt dafür, dass AEV nicht einfach nach Zeitplan, sondern kontextbezogen arbeitet.

Relevante Metriken für den operativen Erfolg

Einige dieser Kennzahlen haben wir bereits erwähnt – hier zur Erinnerung. Um den Impact von AEV messbar zu machen, sollten Sicherheitsteams folgende KPIs im Blick behalten:

- **MTTP (Mean Time to Prevent):** Wie schnell können Assets erkannt, validiert und behoben werden, bevor sie ausnutzbar sind?
- **MTTV (Mean Time to Validate):** Wie lange dauert es, bis klar ist, ob eine Angriffsfläche tatsächlich ausnutzbar ist?
- **MTTR (Mean Time to Remediate):** Wie viel Zeit vergeht von der Validierung bis zur Behebung oder Eindämmung?

AEV reduziert insbesondere den MTTV drastisch – von mehreren Tagen auf wenige Minuten. Und dank sauber validierter Daten sinkt auch der MTTR deutlich. Addiert man MTTV, MTTR und MTTD (Mean Time to Detect), ergibt sich der MTTP. Wenn Findings nicht hypothetisch sind, stoßen sie auf weniger Widerstand im IT-Bereich – und werden von Dev- und Ops-Teams schneller umgesetzt.

Rollenbasierte Remediation-Wege

Der Wert von AEV vervielfacht sich, wenn es in ein übergeordnetes Verantwortlichkeitsmodell eingebunden ist. Gleichzeitig ist AEV auch für kleinere, ressourcenschwache Teams äußerst effektiv – denn viele Prozesse laufen automatisiert ab.

Darüber hinaus fließen AEV-Findings in Risikoregister, Berichte auf Vorstandsebene sowie in kontinuierliche Kontrolltests ein – und verbinden so Ihren technischen Sicherheitsstatus direkt mit Ihrer strategischen Unternehmenssteuerung.

7. Geschwindigkeit heilt

In einer Zeit, in der Angreifer innerhalb von 15 Minuten nach Veröffentlichung damit beginnen, Schwachstellen zu testen – und mit KI-gestützten Tools womöglich noch schneller – zählt buchstäblich jede Sekunde. Die einzige Möglichkeit, dieses Tempo zu schlagen, ist, Ihre eigene Geschwindigkeit in der Prävention zu steigern.

Im Gegensatz zu vielen anderen Tools, die Teams mit Datenfluten überfordern, liefert AEV klare Ergebnisse. Im Gegensatz zu Red Teams, die nur gelegentlich und im begrenzten Umfang validieren, arbeitet AEV kontinuierlich. Und im Gegensatz zu rein hypothetischen Risikomodellen beweist AEV die Ausnutzbarkeit von Schwachstellen in der realen Welt.

Für CISOs und SOC-Teams bedeutet das: mehr Kontrolle, bessere Priorisierung und eine messbare Reduktion des operativen Risikos. AEV verkürzt Entscheidungs- und Reaktionszeiten, verbindet technische Befunde mit geschäftlicher Relevanz und hilft Teams, sich von reaktivem Krisenmanagement hin zu proaktiver, resilienzbasierter Echtzeitabwehr zu entwickeln.

> Sie können Angreifer nicht verlangsamen. Aber mit AEV sind Sie ihnen immer einen Schritt voraus.