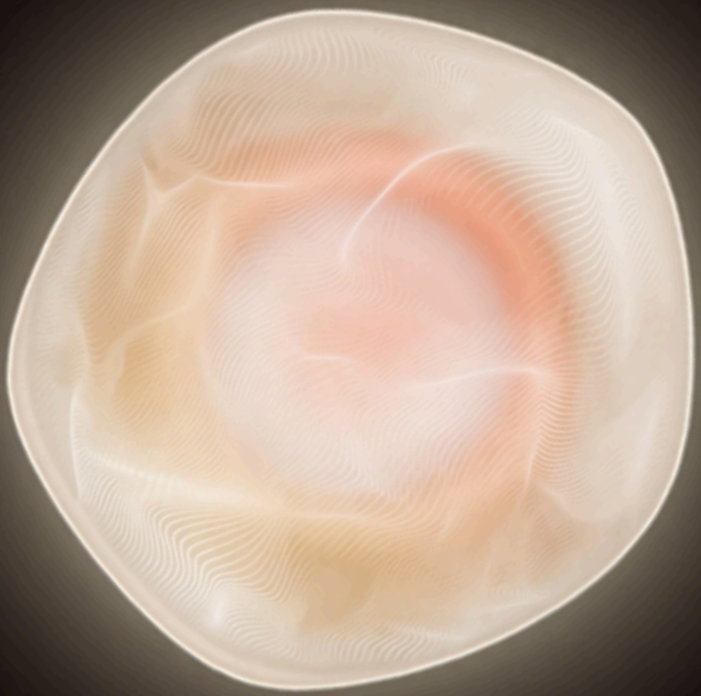
HADRIAN

EXTERNES REIFEGRADMODELL FÜR EXPOSITION



Wo steht Ihr Exposure-Management-Programm heute, und wie sieht echter Fortschritt aus?

DAS EXPOSITIONSPROBLEM, DAS PROGRAMME NICHT LÖSEN

Die meisten Organisationen haben erheblich in Security-Tooling investiert. Sie betreiben Vulnerability-Scanner, nutzen SIEM-Plattformen, führen jährliche oder quartalsweise Penetrationstests durch und pflegen ein Vulnerability-Management-Programm mit definierten Ownern und SLAs. Dennoch wiederholt sich dasselbe Muster: Ausnutzbare Exposition bleibt bestehen, Remediations-Queues wachsen schneller als sie schrumpfen, und wenn etwas schiefläuft, lag der entsprechende Fund meist monatelang in einem Report.

Das Problem ist nicht fehlende Security-Aktivität, sondern eine fehlende Programmstruktur, die Aktivitäten mit Ergebnissen verknüpft. Scanning erzeugt Findings, Findings erzeugen Tickets. Tickets werden geschlossen – oder auch nicht. Die entscheidende Frage, ob die ausnutzbare Exposition der Organisation tatsächlich sinkt, bleibt oft unbeantwortet.

Genau diese Lücke adressiert das External Exposure Maturity Model. Es beschreibt vier erkennbare operative Haltungen – definiert nicht durch vorhandene Tools, sondern durch die Struktur, mit der die Organisation Exposition erkennt, ihre Ausnutzbarkeit bestätigt und sie schließt, bevor ein Angreifer handeln kann. Das Modell gibt Security-Verantwortlichen eine präzise Sprache dafür, wo ihr Programm heute steht, was es strukturell dort festhält und was sich ändern muss, um voranzukommen.

Bezug zu CTEM

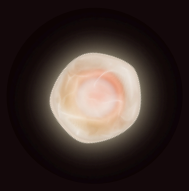
Continuous Threat Exposure Management (CTEM) ist ein fünfphasiges Framework von Gartner, das den Übergang von reaktivem Vulnerability Management zu kontinuierlicher, ergebnisorientierter Expositionsreduktion strukturiert. Die Phasen lauten: Scope, Discover, Prioritise, Validate und Mobilise. Dieses Modell bildet direkt auf CTEM-Maturity ab: Stage-1- und Stage-2-Organisationen führen üblicherweise die frühen Phasen aus, während Stage-3- und Stage-4-Organisationen den Loop durch Validierung und Mobilisierung geschlossen haben. Die Phase, bei der die meisten Organisationen ins Stocken geraten, ist Validation: die Bestätigung, dass Findings tatsächlich ausnutzbare Risiken darstellen – und nicht lediglich theoretische Schweregrade. Das ist der strukturelle Inflection Point, auf dem dieses Modell aufbaut.

WARUM FORTSCHRITT ZÄHLT

Der Unterschied zwischen Stage 1 und Stage 4 ist keine Frage der Ressourcen, sondern der Struktur: wie eine Organisation Exposition erkennt, ihre Ausnutzbarkeit bestätigt und sie schließt, bevor ein Angreifer handeln kann.

Was Fortschritt tatsächlich bringt

The gap between Stage 1 and Stage 4 is not a matter of resources. It is a matter of structure: how an organisation discovers exposure, confirms it is real, and closes it before an attacker can act.



STAGE 1 → STAGE 2

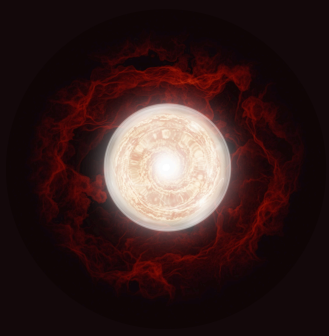
Vom Blindflug zu Klarheit und Hoffnung

Die Attack-Surface-Monitoring-Coverage steigt von 20 % auf 40–60 %. Die True-Positive-Raten verbessern sich von unter 10 % auf 15–25 %. Statt weniger als 1 in 10 Alerts erfordert nun 1 von 4 bis 6 eine Untersuchung. Die Mean Time to Remediation sinkt von 90+ Tagen auf 40–90 Tage. Der praktische Effekt: Das Security-Team verbringt weniger Zeit mit Findings, die sich als irrelevant erweisen.

STAGE 2 → STAGE 3

Von besserer Übersicht und mehr Hoffnung zum Erkennen von Zusammenhängen

Coverage erreicht 75–90 % der Angriffsfläche. Die True-Positive-Rate steigt auf 40–60 %: Nahezu die Hälfte aller Findings ist als ausnutzbar bestätigt, bevor jemand nachforscht. Die MTTR sinkt auf 15–45 Tage. SLA-Compliance erreicht 60–80 %. Die Remediation-Queue wird kürzer und präziser: weniger Findings insgesamt, höheres Vertrauen in jeden einzelnen und eine messbare Reduktion ausnutzbarer Exposition statt bloß geschlossener Tickets.



STAGE 3 → STAGE 4

Vom Verbinden der Punkte zum klaren Gesamtbild

Coverage übersteigt 95 %. Die True-Positive-Rate steigt über 70 %. MTTR fällt unter 7 Tage, kritische Expositionen werden innerhalb von 48 Stunden geschlossen. SLA-Compliance über 90 %. Der wichtigste Benchmark: Bei einem neu bekannt gewordenen Exploit bestätigt die Organisation innerhalb von Stunden, ob sie betroffen ist – nicht innerhalb von Tagen. In Stage 3 erforderte diese Antwort ein Team-Meeting und eine manuelle Untersuchung. In Stage 4 beantwortet das Programm dies automatisch.

Nutzen Sie es als Diagnose, Roadmap oder gemeinsame Sprache mit der Führungsebene. Es schreibt weder ein Toolset noch einen Zeitplan vor. Keine Organisation muss Stage 4 für alle Assets erreichen. Die richtige Frage lautet nicht: Wie weit sind wir? Sondern: Entspricht das Programm dem erforderlichen Risikoniveau?

DAS MODELL AUF EINEN BLICK

Zu verstehen, wo Ihr Programm steht, bildet die Grundlage für eine gezielte Weiterentwicklung. Dieser Abschnitt bietet Ihnen einen klaren Überblick über die spezifischen Fähigkeitslücken und messbaren Ergebnisse, die jede Stufe kennzeichnen.

Die Lens-Tabelle

Markieren Sie für jede Lens eine Spalte, die Ihr Programm am ehrlichsten beschreibt. Liegen Ihre Antworten konstant in einer Spalte, ist das Ihre aktuelle Stage. Verteilen sich die Antworten über mehrere Spalten, entspricht Ihr Floor der am weitesten links markierten Spalte.

BETRACHTUNGSEBENE	STAGE 1: IM BLINDFLUG	STAGE 2: BESSERE ÜBERSICHT, MEHR HOFFNUNG	STAGE 3: ZUSAMMENHÄNGE ERKENNEN	STAGE 4: KLARES GESAMTBILD
Arbeitsrhythmus Wie häufig befasst sich Ihr Programm mit Exposition?	REAKTIV	PERIODISCH	KONTINUIERLICH	AUTONOM
Umgang mit Risiken Wie gut verstehen Sie, was tatsächlich ausnutzbar exponiert ist?	EXPONIERT	BEWUSST	VALIDIERT	PROAKTIV
Sicherheitsausrichtung Wie positioniert sich Ihr Programm gegenüber Angreifern?	REAKTIV	STRUKTURIERT	PROAKTIV	PRÄDIKATIV
Validierungsansatz Wie geht Ihr Programm mit der Frage um: Funktionieren unsere Kontrollen wirklich?	ANGENOMMEN	GETESTET	VALIDIERT	KONTINUIERLICH

Die Capability Matrix

Fünf operative Dimensionen, 4 Stages.
Identifizieren Sie damit Ihre fehlende Dimension.

FÄHIGKEIT	STAGE 1: IM BLINDFLUG	STAGE 2: BESSERE ÜBERSICHT, MEHR HOFFNUNG	STAGE 3: ZUSAMMENHÄNGE ERKENNEN	STAGE 4: KLARES GESAMTBILD
Betriebsmodell	Event-getrieben; Exposition wird über Incidents oder Audits entdeckt	Strukturiertes Programm; definierte Ownership; CTEM-Phasen eingeführt	Closed-Loop; Validierungsergebnis steuert die Remediation	Standardmäßig offensive; adaptiv; minimale manuelle Orchestrierung
Erkundung	Unvollständiges Inventar; periodisches Scanning bekannter Assets	EASM implementiert; Cloud, SaaS, APIs, Third-Party im Scope	Kontinuierliches Monitoring; nahezu Echtzeit-Drift-Erkennung	Adaptiv; korreliert Identität, Infrastruktur, SaaS automatisch
Priorisierung	CVSS- und Vendor-Scores; eingeschränkter Business-Kontext	Risikobasiert unter Einbeziehung der Business-Kritikalität	Ausnutzbarkeit und Attack-Path-Kontext; weniger, aber belastbare Findings	Prädikativ und kontextbewusst; Prioritäten verschieben sich mechanisch
Validierung	Jährliche Pentests oder ad hoc; Ausnutzbarkeit angenommen, nicht bestätigt	Szenariobasiertes periodisches Testing innerhalb definierter Scopes	Kontinuierliche automatisierte Validation; Blind Windows eliminiert	Autonome Adversarial Emulation; Attack Chains passen sich Änderungen an
Automatisierung	Manuell, ticket-getrieben; isolierte Tools	Integrierte Workflows; standardisierte Handoffs	Validierung löst Remediation aus; SOC/IT-Integrationen aktiv	Weitgehend autonom; Menschen konzentrieren sich auf strategische Entscheidungen

Quantitative Vergleichswerte

Diese Zahlen basieren auf der Analyse von Exposure-Management-Programmen durch Hadrian in über 300 Organisationen. Sie stellen beobachtete Bandbreiten dar, keine Zielwerte – Ihr Programm kann je nach Komplexität der Umgebung, Branche und Ausgangssituation darüber oder darunter liegen.

METRIC	STAGE 1: IM BLINDFLUG	STAGE 2: BESSERE ÜBERSICHT, MEHR HOFFNUNG	STAGE 3: ZUSAMMENHÄNGE ERKENNEN	STAGE 4: KLARES GESAMTBILD
Angriffsfläche unter ständigem Monitoring	< 20%	40–60%	75–90%	> 95%
Alert True-Positiv-Rate	< 10%	15–25%	40–60%	> 70%
Mean Time to Remediation (MTTR)	> 90 Tage	45–90 Tage	15–45 Tage	< 7 Tage (kritisch: < 48 Std.)
SLA-Compliance	< 20%	< 40%	60–80%	> 90%
Findings vor Eskalation als ausnutzbar validiert	Selten	Selektiv	Konsistent	Kontinuierlich und automatisch

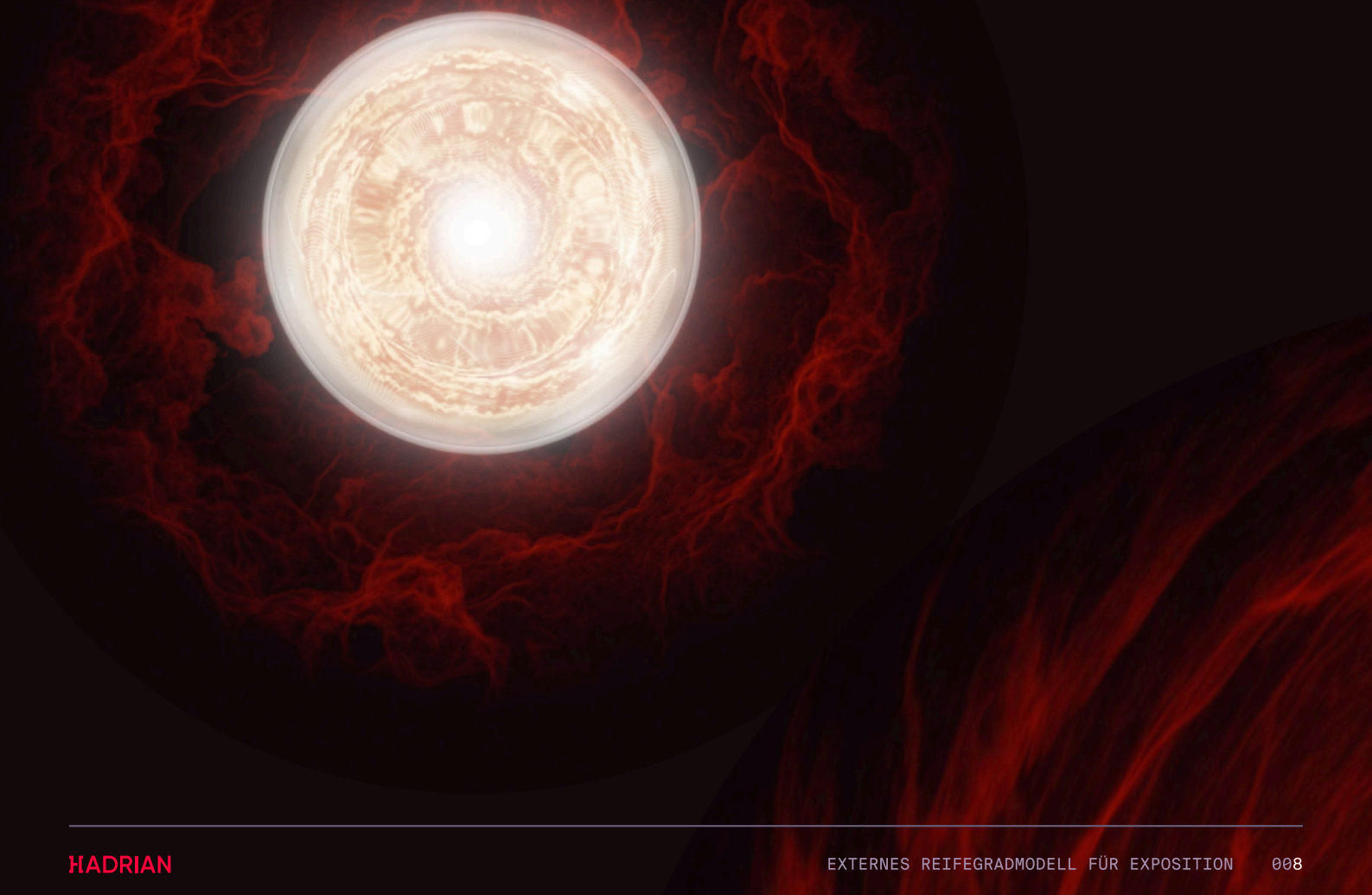
SELBSTEINSCHÄTZUNG:

Zum interaktiven Self-Assessment

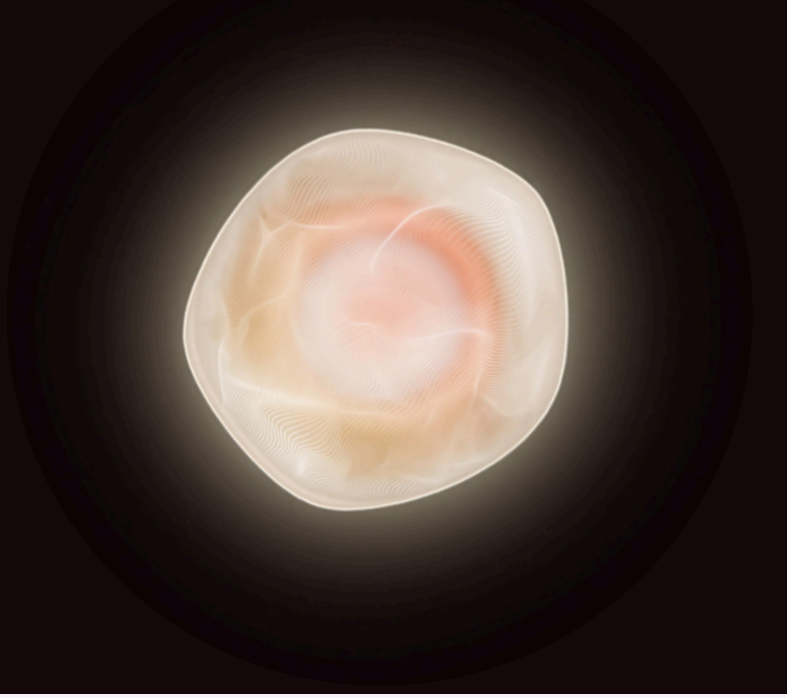
ENTDECKEN SIE IHREN REIFEGRAD

DIE 4 STAGES

Jede Stage ist eine erkennbare operative Haltung – kein Score, keine Note. Lesen Sie diese als Porträts davon, wie Organisationen tatsächlich arbeiten. Wenn eine Beschreibung unangenehm ist, ist sie wahrscheinlich die richtige.



STAGE 1



IM BLINDFLUG

„Wir erfahren von Exposition, wenn etwas schiefläuft."

Der Name ist nüchtern, weil die Erfahrung nüchtern ist. Die Organisation hat kein verlässliches Bild ihrer externen Angriffsfläche. Assets tauchen in Gesprächen nach Incidents auf – nicht davor. Das Security-Team weiß, dass es Lücken gibt, aber nicht wo, was oder wie gravierend. Scanning findet statt, doch das Ergebnis ist eine Liste von Severities, der niemand vollständig vertraut und die schneller wächst, als sie abgearbeitet werden kann.

Was Stage 1 von Stage 2 unterscheidet, ist nicht das Tooling. Viele Organisationen in dieser Stage haben Scanner, SIEMs und Ticketing-Workflows. Was fehlt, ist Struktur: kein systematischer Discovery-Rhythmus, kein definiertes Ownership-Modell, keine konsistente Methode zur Bestätigung, ob Findings ein reales Risiko darstellen. Die Aktivität ist vorhanden. Das Programm nicht.

So beschreiben es Teams

„Wir bekämpfen ständig Brände. Wir kommen den Dingen nie zuvor."

„Der Pentest-Report kommt an, und die Hälfte des letzten Jahres ist noch offen."

„Ich weiß nicht, wie viele Internet-Facing-Assets wir haben. Niemand weiß es."

Wie sieht es organisatorisch aus

Security-Meetings werden vom letzten Incident oder Audit-Finding dominiert. Das Board-Update des CISO dreht sich um den Compliance-Status, nicht um Exposition. Bei einem neuen kritischen CVE lautet die erste Frage: „Haben wir diese Software?" Niemand ist sich der Antwort sicher. Remediation-Gespräche beginnen häufiger mit „Wessen Team ist das?" als mit „Wie ausnutzbar ist das?" Der Pentest-Report von vor acht Monaten ist noch immer in einer Tabelle offen, die nie vollständig abgearbeitet wurde.

Die Beziehung zwischen Security und Engineering ist bestenfalls transaktional. Security meldet Findings; Engineering stellt die Schwere infrage oder priorisiert sie gegenüber Produktarbeit niedriger. Ohne eine konsistente Methode zur Bestätigung der Ausnutzbarkeit kann Security die Dringlichkeit nicht überzeugend begründen. Das Team agiert reaktiv und verbringt unverhältnismäßig viel Zeit damit, auf das zu reagieren, was diese Woche in den Nachrichten ist, statt auf die tatsächliche Exposition der Organisation.

Was Organisationen hier festhält

Der häufigste Grund ist nicht das Budget. Es ist, dass die Organisation Security als Compliance-Funktion statt als Risikomanagement-Funktion definiert. Compliance erfordert kein Wissen darüber, was ausnutzbar ist – nur, was dokumentiert ist. Das schafft eine strukturelle Obergrenze: Das Programm liefert Nachweise für Aktivität, nicht für ein reduziertes Risiko. Die Führungsebene fragt noch nicht nach dem Unterschied.

Der operative Engpass in Stage 1 ist ein Signal-to-Noise-Kollaps. Scanner erzeugen Tausende von Findings ohne Mechanismus zur Unterscheidung von realem Risiko und Hintergrundrauschen. Das Ergebnis: Die gesamte Kapazität des Teams fließt in Triage, keine in Remediation. Volumen erzeugt den Anschein von Arbeit – aber keine Security-Outcomes.

Ownership ist das dritte Hindernis. Exposition liegt an der Schnittstelle von Security, IT und Engineering. Wenn niemand das Gesamtbild verantwortet, wird nichts als dringend behandelt, bis etwas bricht.

Der Moment der Bereitschaft

Organisationen sind bereit voranzukommen, wenn etwas die Lücke unübersehbar macht – typischerweise ein Incident, der ein unbekanntes Asset enthüllt, oder eine Board-Frage, die den Abstand zwischen gemeldeter und tatsächlicher Posture aufdeckt. Der Wandel von Compliance zu Risikoorientierung erfordert meist einen internen Fürsprecher: jemanden, der das Gespräch nicht als „Wir brauchen mehr Tools" rahmt, sondern als „Wir müssen wissen, was wir tatsächlich exponiert haben".

Was sich strukturell ändern muss

Die Voraussetzung für Stage 2 ist kein Tool-Kauf, sondern eine Ownership-Entscheidung. Jemand muss für die Vollständigkeit des externen Asset-Inventars verantwortlich sein – nicht nur für die Security bekannter Assets. Sobald diese Accountability besteht, folgen die unterstützenden Strukturen: kontinuierliche Discovery außerhalb des vordefinierten Scopes, risikobasierte Priorisierung mit Business-Kontext neben Severity-Scores und definierte SLAs, die tatsächlich durchgesetzt werden – nicht nur angestrebt.

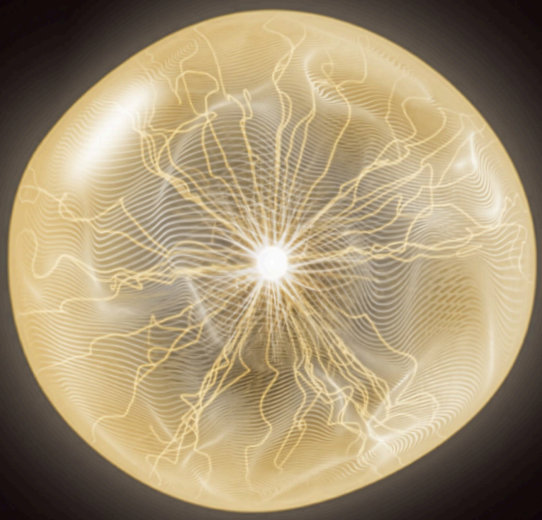
Capabilities, die diesen Übergang ermöglichen

- Attack Surface Management, das Assets außerhalb des vordefinierten Inventars entdeckt: Cloud, SaaS, Tochtergesellschaften, Third Parties
- Risikobasierte Priorisierung unter Einbeziehung von Business-Kritikalität und Reachability – nicht nur CVSS
- Asset-Ownership-Workflows, die entdeckte Assets mit verantwortlichen Teams verbinden

ADVANCEMENT PLAN STAGE 1 ZU 2 HERUNTERLADEN

STAGE 2

BESSERE ÜBERSICHT, MEHR HOFFNUNG



„Wir wissen mehr als früher. Nur nicht, ob es genug ist."

Stage-2-Organisationen haben solide Arbeit geleistet. Es gibt ein formales Vulnerability-Management-Programm. Wichtige Assets sind inventarisiert. Testing erfolgt nach Plan, nicht nur nach Incidents. Security hat einen Platz am Tisch und ein definiertes Mandat. Der CISO kann einen Posture-Report erstellen, ohne hektisch zu werden.

Der Name beschreibt sowohl den Fortschritt als auch die Einschränkung. Der Scope hat sich erweitert: mehr Assets, mehr Testing-Coverage, mehr strukturierte Ownership. Und es gibt echte Hoffnung: die Hoffnung, dass die bekannten Assets die wichtigen sind, dass der Quartals-Pentest das Wesentliche erfasst hat, dass Ausnutzbarkeit grob mit Severity korreliert. Diese Hoffnung ist nicht unvernünftig. Aber es bleibt Hoffnung statt Evidenz. Das Programm ist strukturiert – aber noch nicht validiert.

So sieht es organisatorisch aus

„Findings aus dem letzten Pentest sind bereits veraltet, wenn der nächste Zyklus läuft."

„Wir haben gute Coverage der bekannten Assets. Das Problem sind die unbekannten."

„Theoretisch sind wir risikobasiert. Praktisch arbeiten wir noch CVSS 8 und 10 ab."

So sieht es organisatorisch aus

Das Security-Team hat einen Programmrhythmus: Quartals-Pentests, regelmäßige Vulnerability-Scans, eine Ticket-Queue mit definierten Owners. Das Board-Reporting hat sich von Compliance-Status zu aktueller Vulnerability-Exposition verbessert. Bei einem neuen CVE gibt es einen Prüfprozess – aber er ist manuell und langsamer als gewünscht.

Die Frustration in Stufe 2 ist subtiler als in Stufe 1, da das Programm von außen gesund wirkt: Abdeckungskennzahlen verbessern sich, die Einhaltung von SLAs wird nachverfolgt, und Lageberichte lassen sich ohne Hektik erstellen. Doch das Team spürt, dass etwas nicht stimmt: Findings aus dem letzten Pentest veralten, bevor der nächste Zyklus startet, die Remediation-Queue enthält Einträge, deren tatsächliche Ausnutzbarkeit niemand bestätigt hat, und die Lücke zwischen dem, was das Programm berichtet, und dem, was ein Angreifer tatsächlich tun könnte, bleibt unangenehm groß.

Was Organisationen hier festhält

Das strukturelle Hindernis in Stage 2 ist die Lücke zwischen Testing-Kadenz und Umgebungsgeschwindigkeit. Quartalsweise Penetrationstests wurden für Umgebungen konzipiert, die sich quartalsweise änderten. Die meisten Enterprise-Umgebungen ändern sich heute täglich. Das Programm ist nicht defekt – es passt schlicht nicht zum Tempo des Problems.

Der operative Engpass in Stage 2 ist manuelle Validierung. Die Bestätigung, dass ein Finding tatsächlich ausnutzbar ist, erfordert menschliche Untersuchung. Wenn dieser Schritt nicht skaliert, füllen sich Remediation-Queues mit unvalidierten Findings, und Teams greifen auf informelle Heuristiken zurück: Alles über CVSS 8 gilt als ausnutzbar. Das ist schneller – aber deutlich ungenauer, und es reduziert weder den Backlog noch verbessert es das Vertrauen in die verbleibenden Findings.

Messbarkeit verstärkt beide Probleme. Die meisten Stage-2-Programme verfolgen Coverage und Aktivität: entdeckte Findings, geschlossene Findings, SLA-Compliance. Diese Metriken fühlen sich wie Fortschritt an, beantworten aber nicht die entscheidende Frage der Führungsebene: Sinkt unsere ausnutzbare Exposition?

Der Moment der Bereitschaft

Der Auslöser ist meist ein Finding, das früher hätte erkannt werden sollen: eine ausnutzbare Exposition zwischen Test-Zyklen, bei einem ungeplanten Assessment oder durch externe Forscher. Die folgende Frage – wie lange war das offen? – ist oft der Katalysator dafür, dass periodische Validierung nicht mehr Schritt halten kann. Die Bereitschaftsfrage lautet: Ist die Organisation bereit, von geplanten Tests zu kontinuierlichem Monitoring zu wechseln – und wird die Führungsebene den dafür erforderlichen strukturellen Wandel finanzieren?

Was sich strukturell ändern muss

Der Übergang von Stage 2 zu Stage 3 erfordert das Schließen der Lücke zwischen Testing-Kadenz und Umgebungsgeschwindigkeit: kontinuierliches externes Monitoring, das neue Exposition erkennt, sobald sie entsteht – nicht erst beim nächsten geplanten Scan. Zudem muss Exploitability-Validierung als Workflow-Schritt behandelt werden, nicht als manuelle Untersuchung. Sobald die Bestätigung eines realen Findings automatisiert statt menschenabhängig ist, löst sich der Triage-Engpass auf. Auch die Messung muss sich ändern: Das Programm sollte ausnutzbares Risiko messen, das beseitigt wurde – nicht nur geschlossene Findings.

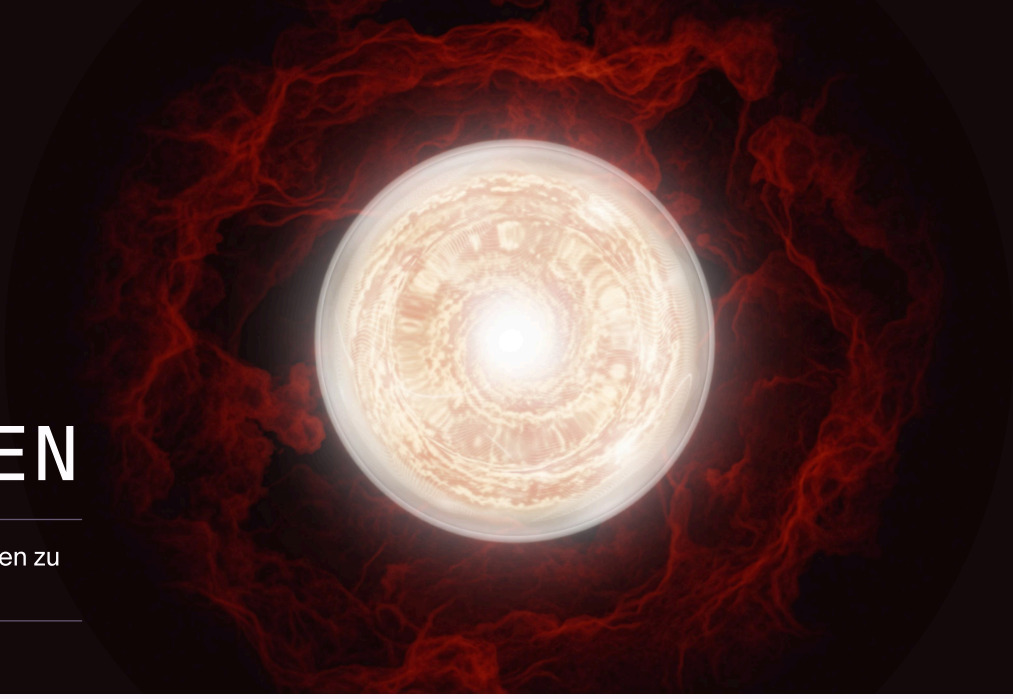
Capabilities, die diesen Übergang ermöglichen

- Kontinuierliches externes Attack-Surface-Monitoring, das neue Assets und Änderungen zwischen Pentest-Zyklen erkennt
- Automatisierte Exploitability-Validierung, die bestätigt, welche Findings tatsächlich erreichbar und testbar sind
- Integriertes Remediation-Routing, damit validierte Findings ohne manuellen Handoff den richtigen Owner erreichen

ADVANCEMENT PLAN STAGE 2 ZU 3 HERUNTERLADEN

STAGE 3

ZUSAMMENHÄNGE ERKENNEN



„Wir wissen, was ausnutzbar ist. Wir beginnen zu sehen, wie es zusammenhängt."

Stage 3 ist ein echter operativer Inflection Point. Validierung ist nicht mehr periodisch, sondern kontinuierlich. Blind Windows zwischen Test-Zyklen sind weitgehend geschlossen. Ausnutzbarkeit wird vor der Eskalation von Findings bestätigt – nicht aus Severity-Scores abgeleitet. Remediation-Workflows sind in Security-Tooling integriert, sodass validierte Findings automatisch geroutet werden, statt in einem gemeinsamen Posteingang zu landen.

Der Name markiert das Neue: Zum ersten Mal katalogisiert das Programm Schwachstellen nicht mehr isoliert, sondern fügt sie zu einem Bild zusammen, wie ein Angreifer tatsächlich vorgehen könnte. Einzelne validierte Findings werden gegen Attack Paths gemappt. Die Priorisierung verschiebt sich von „Was hat den höchsten CVSS?" zu „Was lässt sich verketten, um realen Schaden anzurichten?" Das ist eine fundamental andere Perspektive. Die Einschränkung: Aufbau und Pflege dieses Bildes erfordern noch erhebliche menschliche Orchestrierung. Das Programm sieht die Punkte – sie schnell und in großem Maßstab zu verbinden, bleibt manuell.

So beschreiben es Teams

„Wir wissen, was ausnutzbar ist. Die Herausforderung ist das Tempo der Umgebungsänderungen."

„Unsere Findings sind validiert, bevor sie die Queue erreichen. Das Problem ist, sie zu einem vollständigen Attack Picture zusammenzufügen."

„Wir können dem Board mitteilen, was als ausnutzbar bestätigt ist. Wir können noch nicht sagen, wie ein Angreifer es verketten würde."

So sieht es organisatorisch aus

Der tägliche Rhythmus des Security-Teams sieht anders aus. Findings kommen vorvalidiert an. Tickets werden automatisch an Owners geroutet. Das Triage-Gespräch hat sich verschoben von „Ist das real?" zu „Wie fügt sich das in das übergeordnete Expositionsbild ein?" Die MTTR wird aktiv gemessen, sinkt kontinuierlich und ist durch ausnutzbares, geschlossenes Risiko definiert – nicht durch Ticket-Anzahl.

Reporting, Board-Metriken und KPIs basieren häufig noch auf periodischen Momentaufnahmen, weil dies traditionell von der Führungsebene gefordert wurde. Der Vorstand erwartet weiterhin eine Kennzahl zwischen eins und zehn. KPIs, die in Stufe 2 sinnvoll waren, messen inzwischen die falschen Dinge, doch ihre Anpassung erfordert eine Diskussion, die bislang niemand priorisiert hat. Gleichzeitig arbeitet das Security-Team mit einer Präzision, für die die Governance-Struktur nicht ausgelegt ist. Der CISO kann benennen, was exponiert ist – aber noch nicht schnell genug sagen, was ein Angreifer tatsächlich ausnutzen könnte.

Was Organisationen hier festhält

Die Einschränkung ist der Orchestrierungs-Durchsatz. Die Ausführung eines komplexen Adversarial-Szenarios, das Attack Chains über Systeme hinweg verfolgt, realistische Intrusion Paths testet und sich an Umgebungsänderungen anpasst, erfordert erhebliche Expertenzeit. Einzelne Findings können kontinuierlich validiert werden; zu simulieren, was ein versierter Angreifer damit tun würde, bleibt manuell und ressourcenintensiv. Das Programm sieht die Punkte. Sie schnell zu verbinden, bleibt menschliche Arbeit.

Der operative Engpass in Stage 3 ist Emulations-Skalierung. Das Programm kann einzelne Findings kontinuierlich validieren, aber sie in ein vollständiges Echtzeitbild zu übersetzen, wie diese Findings sich zu ausnutzbaren Attack Paths kombinieren, erfordert noch menschliche Orchestrierung pro Szenario. Mit wachsender Umgebungskomplexität wird die Lücke zwischen dem, was validiert, und dem, was emuliert werden kann, zum limitierenden Faktor.

Es gibt auch einen organisatorischen Rückstand. Der Betrieb läuft kontinuierlich, aber die Governance hat nicht Schritt gehalten. Leadership-Reporting, Board-Metriken und KPIs basieren oft noch auf periodischen Snapshots statt auf Live-Posture-Daten. Das Programm erzeugt mehr Signal, als die Organisation gelernt hat, zu verarbeiten.

Der Moment der Bereitschaft

Stage-3-Organisationen werden bereit voranzukommen, wenn sie eine konkrete Frage nicht schnell beantworten können: Wenn heute eine neue Exploit-Klasse bekannt würde – wie lange würde es dauern, zu bestätigen, ob die gesamte Angriffsfläche betroffen ist? Lautet die ehrliche Antwort „Tage" statt „Stunden", ist die Lücke zwischen Detection- und Emulations-Capability zum limitierenden Faktor geworden. Das Bereitschaftsgespräch dreht sich darum, ob die Führungsebene in das Schließen dieser Lücke investiert – und ob die Programm-Governance autonomen Betrieb ermöglichen kann.

Was sich strukturell ändern muss

Der Übergang zu Stage 4 erfordert, die manuelle Orchestrierung von Adversarial-Szenarien durch automatisierte Emulation zu ersetzen, die sich ohne menschlichen Eingriff pro Szenario an Umgebungsänderungen anpasst. Es erfordert zudem das Schließen der Schleife zwischen Live-Betriebsdaten und Leadership-Visibilität: Echtzeit-Posture-Dashboards, die direkt aus Programm-Output abgeleitet werden – nicht periodisch zusammengestellt. Und es erfordert eine Governance-Entscheidung: Rapid-Response-Protokolle vorab zu autorisieren, damit das Programm bei einem neuen Exploit in Stunden reagiert – nicht erst nach einem Triage-Meeting.

Capabilities, die diesen Übergang ermöglichen

- Automatisierte Adversarial Emulation, die sich ohne manuelle Orchestrierung pro Szenario an Umgebungsänderungen anpasst
- Echtzeit-Posture-Scoring und board-fähige Metriken, direkt aus Live-Programmdaten abgeleitet
- Kontinuierliche Attack-Chain-Analyse, die zeigt, wie validierte Findings sich zu ausnutzbaren Pfaden kombinieren

ADVANCEMENT PLAN STAGE 3 ZU 4 HERUNTERLADEN

STAGE 4

KLARES GESAMTBILD

„Zum ersten Mal sehen wir, was ein Angreifer jederzeit sieht."

Clear Picture ist kein Aspirations-Tier. Es ist, wie Expositionsmanagement aussieht, wenn die strukturellen Einschränkungen der vorherigen Stages alle behoben sind: reaktive Discovery, periodische Validierung, manuelle Orchestrierung und verzögerte Leadership-Visibilität. Das Programm ist kontinuierlich, adaptiv und weitgehend autonom. Die Aufmerksamkeit des Security-Teams gilt strategischen Entscheidungen und Ausnahmebehandlung – nicht der Triage von Rauschen oder dem manuellen Zusammenstellen von Attack Paths.

Der Name ist präzise. Zum ersten Mal hat die Organisation ein vollständiges Echtzeit-Bild ihrer externen Angriffsfläche aus Angreiferperspektive: nicht nur, welche Assets existieren, sondern welche erreichbar und ausnutzbar sind, wie sie sich verketten und wie die wahrscheinlichen Intrusion Paths gerade aussehen. Dieses Bild aktualisiert sich kontinuierlich mit der Umgebung. Es wartet nicht auf den nächsten Scan-Zyklus oder den nächsten Pentest.

Was Clear Picture auszeichnet, ist keine einzelne Capability, sondern das Fehlen der strukturellen Lücken, die jede frühere Stage definieren. Es gibt keine Blind Windows, keinen Triage-Backlog aus unvalidierten Findings, keine Lücke zwischen dem, was das Programm weiß, und dem, was die Führungsebene sieht. Die Organisation reagiert nicht mehr auf Exposition – sie antizipiert sie.

Was gelöst wurde, um hierher zu gelangen

Die Organisation ersetzte die manuelle Orchestrierung von Adversarial-Szenarien durch automatisierte Emulation, die sich kontinuierlich an Umgebungsänderungen anpasst. Sie schloss die Schleife zwischen Live-Betriebsdaten und Leadership-Reporting und traf eine Governance-Entscheidung: Rapid-Response-Protokolle wurden vorab autorisiert und Eskalationspfade für autonomen Betrieb definiert – damit das Programm mit Maschinengeschwindigkeit reagiert, ohne bei jedem Schritt eine menschliche Entscheidung zu benötigen.

Das Team ist im Verhältnis zur abgedeckten Angriffsfläche kleiner als in jeder früheren Stufe – nicht, weil Stellen abgebaut wurden, sondern weil Automatisierung die Arbeit übernommen hat, die zuvor manuelle Triage erforderte. Die Expertise hat sich nach oben verlagert. Das Security-Team arbeitet an Fragestellungen, die Urteilsvermögen erfordern: Threat Modelling, die Entwicklung adversarieller Szenarien und strategische Fragen, die sich nicht automatisieren lassen. Auch die Beziehung des CISO zum Vorstand hat sich verändert. Im Fokus steht nicht mehr, was im letzten Quartal passiert ist, sondern was das Programm aktuell erkennt.

So sieht es organisatorisch aus

Das Posture-Gespräch des Security-Teams hat sich grundlegend verändert. Die Frage lautet nicht mehr „Welcher Exposition sind wir ausgesetzt?" – das beantwortet das Programm kontinuierlich. Die Frage ist: „Wie schnell können wir sie schließen?" und „Woran sollten unsere Mitarbeitenden arbeiten, was Automatisierung noch nicht übernehmen kann?" Das Board-Reporting stammt direkt aus Live-Programmdaten. Engineering-Teams empfangen validierte, geroutete Findings ohne manuellen Handoff durch Security. Bei einem neu bekannt gewordenen Exploit bestätigt das Programm innerhalb von Stunden, ob die Angriffsfläche betroffen ist – nicht innerhalb von Tagen.

Das Security-Team ist in dieser Stage kleiner im Verhältnis zur Surface-Coverage als in jeder früheren Stage, weil Automatisierung die Arbeit übernommen hat, die früher menschliche Triage erforderte. Die Expertise hat sich nach oben verschoben: Das Team arbeitet an Problemen, die Urteilsvermögen erfordern – nicht an solchen, die Volumen erfordern.

So beschreiben es Teams

- „Wir erfahren von einer neuen Exposition, bevor Angreifer sie sondieren können."
- „Die Frage ist nicht mehr, ob wir exponiert sind, sondern wie schnell wir es schließen können."
- „Ich kann dem Board unsere aktuelle Posture auf Basis von Daten der letzten 24 Stunden darlegen. Das war vorher nicht möglich."

Was diese Stage zur Aufrechterhaltung erfordert

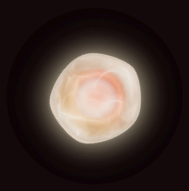
Clear Picture ist kein Ziel, das sich, einmal erreicht, von selbst erhält. Adversarial-Techniken entwickeln sich weiter, und die Emulationsqualität des Programms muss mithalten. Neue Infrastrukturkategorien – darunter KI-Systeme, agentische Workflows und neue SaaS-Integrationen – schaffen Angriffsfläche, die kontinuierliche Aktualisierungen der Discovery- und Validierungsmodelle erfordert.

Die organisatorischen Anforderungen sind ebenso wichtig wie die technischen. Governance-Strukturen müssen autonomen Betrieb unterstützen, ohne zum Hindernis zu werden: vorab autorisierte Response-Protokolle, klar definierte Eskalationsschwellen und Leadership-Alignment darüber, was „Echtzeit-Posture-Visibilität" in der Praxis bedeutet. Programme, die Clear Picture erreichen und dann bürokratische Genehmigungsstufen für automatisierte Responses einführen, werden feststellen, dass ihre Capability in Richtung Stage 3 degradiert.

Der häufigste Weg zurück zu Stage 3 ist ein Führungswechsel: ein neuer CISO, der manuelle Review-Gates wieder einführt, oder ein Board, das nach einem False Positive das Vertrauen in den autonomen Betrieb verliert. Die Aufrechterhaltung von Clear Picture erfordert die aktive Pflege des organisatorischen Mandats – nicht nur der technischen Capability.

Capabilities, die diese Stage definieren

- Autonome Adversarial Emulation, die sich kontinuierlich ohne manuelle Orchestrierung, pro Szenario an Umgebungsänderungen anpasst
- Prädiktive, dynamische Priorisierung, die sich automatisch anpasst, wenn neue Expositionen entstehen und sich der Attack-Chain-Kontext ändert
- Echtzeit-Angriffsflächen-Modell, das Identity-, Infrastruktur-, SaaS- und Third-Party-Änderungen in einem kontinuierlich aktualisierten Bild korreliert
- Vollständige Programmintegration von Expositions-Detection über validierte Findings bis zum Abschluss der Remediation – mit minimalen manuellen Handoffs

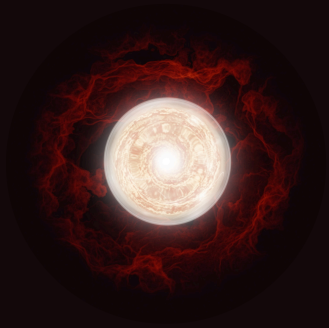


STAGE 1 → STAGE 2

Der Übergang von Stage 1 zu Stage 2 kann mit fokussiertem Einsatz und klarer Ownership in wenigen Monaten erreicht werden.

STAGE 2 → STAGE 3

Stage 2 zu Stage 3 dauert typischerweise sechs bis achtzehn Monate, abhängig von Umgebungskomplexität und Integrationstiefe.

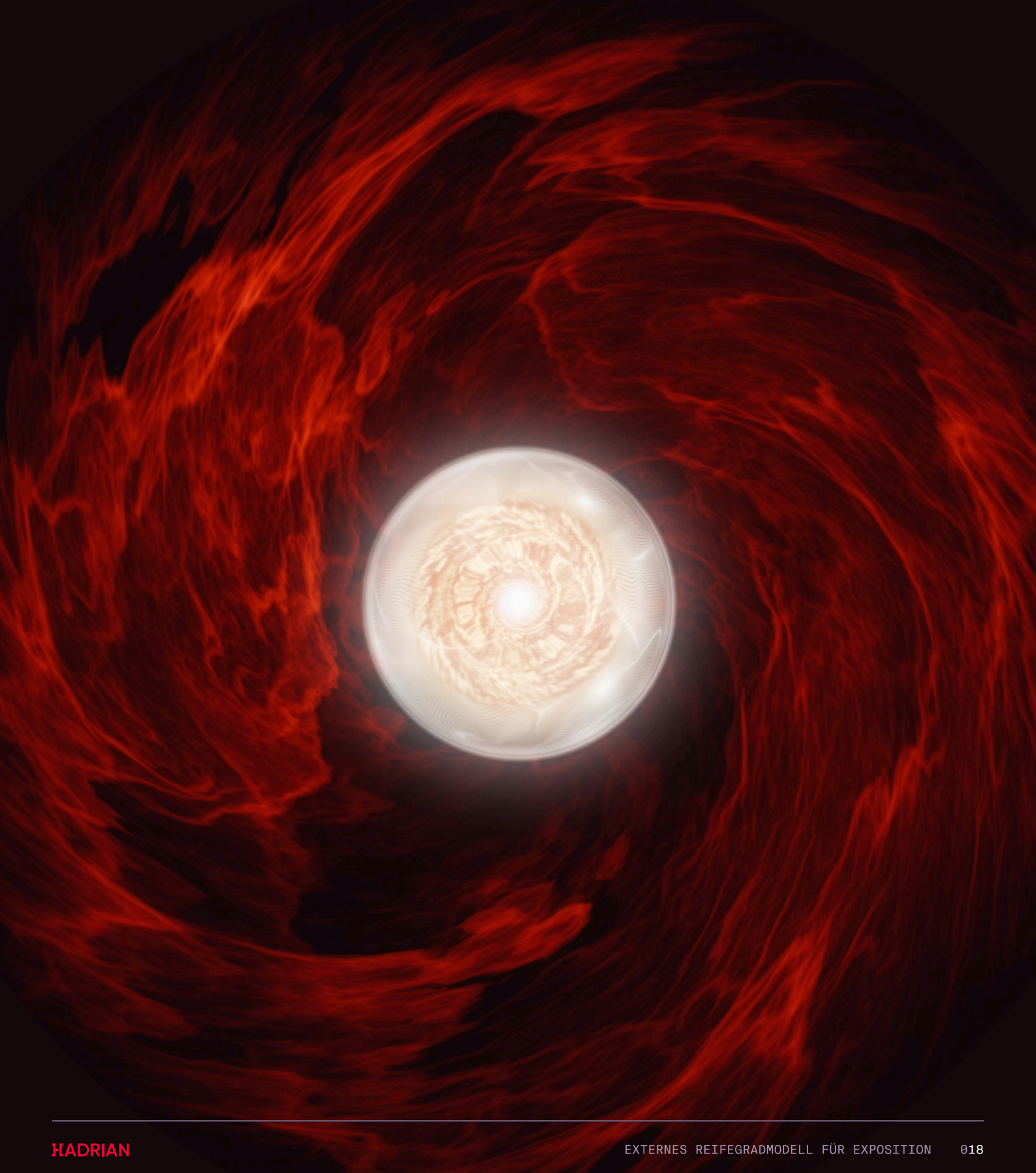


STAGE 3 → STAGE 4

Der Übergang zu Stage 4 ist fortlaufend und erfordert nachhaltiges operatives Investment statt eines definierten Projekts. Was den Fortschritt beschleunigt, ist nicht mehr Tooling – sondern Klarheit: klare Ownership über Exposition, klare Definitionen von „Done" und die Messung ausnutzbaren Risikos, das beseitigt wurde – nicht generierter Aktivität.

ABSCHNITT 4

WO STEHEN SIE?



Die meisten Organisationen, die die vier Stages durcharbeiten, stellen fest, dass ihre ehrliche Antwort zwischen zweien liegt. Discovery ist reifer als Validierung. Validierung ist reifer als Remediation-Routing. Ein Gesamt-Stage-Score kann ungefähr zeigen, wo Sie stehen – aber nicht, welche spezifische Dimension alles andere zurückhält.

Dieser Unterschied ist wichtiger als er klingt. Ein Programm, das im Durchschnitt Stage 3 erreicht, aber Stage-1-Validierung aufweist, ist kein Stage-3-Programm. Es ist ein Programm mit einem Stage-1-Engpass, der die Performance in jeder anderen Dimension unterdrückt. Remediation-SLAs, Board-Reporting, Automatisierungsgrad – all das wird durch das schwächste Glied begrenzt, nicht durch das stärkste. Die meisten internen Assessments übersehen dies, weil sie die Gesamt-Posture bewerten, statt sie nach operativer Dimension aufzuschlüsseln.

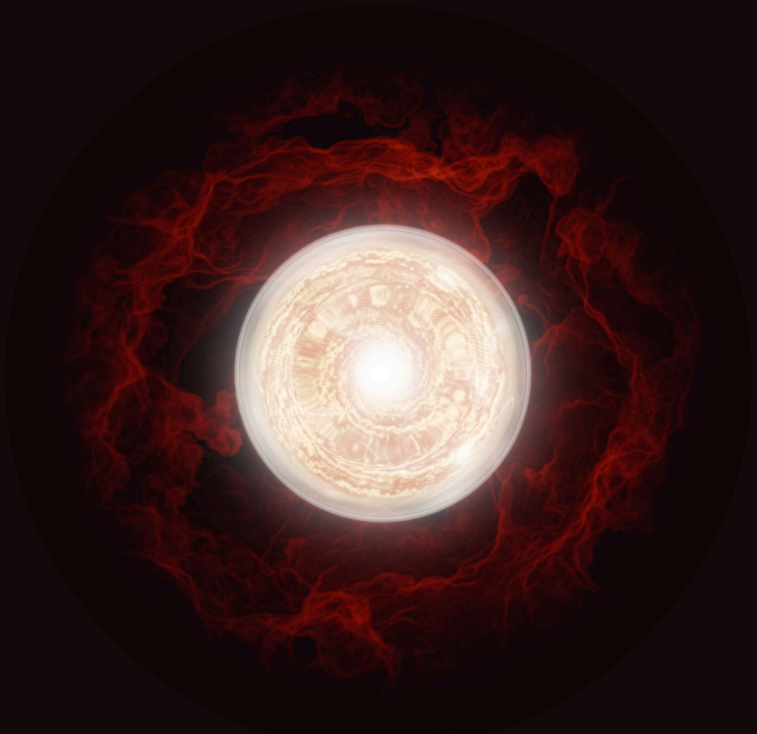
Das interaktive Self-Assessment ist anders aufgebaut. Es bewertet Ihr Programm über sechs Dimensionen unabhängig und gewichtet sie, um zu identifizieren, wo die Lücke zwischen Ihrer aktuellen Posture und Ihrem Risikoprofil am größten ist. Das Ergebnis ist keine Zahl, sondern eine Aufschlüsselung Ihres Stands nach Dimension, ein Callout Ihres wirkungsstärksten Engpasses und ein stage-spezifischer Aktionsplan, den Ihr Team direkt umsetzen kann.

Wenn Sie Ihren Gesamt-Stage bereits kennen, lohnt sich das Assessment dennoch. Das dimensionsspezifische Profil ist es, dass es in einer Leadership-Konversation nützlich macht – nicht „wir sind Stage 2", sondern „wir sind Stage 3 in Discovery und Stage 1 in Validierung, und das bedeutet Folgendes für unsere Remediation-Zeit."

SELBSTEINSCHÄTZUNG:

Zum interaktiven Self-Assessment

ENTDECKEN SIE IHREN REIFEGRAD



Häufig gestellte Fragen

Muss jede Organisation Clear Picture erreichen?

Nein. Clear Picture ist geeignet für Organisationen, bei denen die Folgen einer Kompromittierung kontinuierliche, autonome Validierung rechtfertigen. Für viele Organisationen ist Stage 2 oder Stage 3 das richtige Ziel für den Großteil ihrer Angriffsfläche – mit Stage-4-Praktiken, die den wertvollsten Assets vorbehalten sind. Die richtige Frage lautet nicht, wie man Stage 4 erreicht, sondern welche Assets und Risikoklassen eine Stage-4-Behandlung erfordern.

Wir nutzen viele Tools. Warum bleibt unsere Maturity niedrig?

Tool-Adoption ist nicht gleich Programm-Maturity. 93 % der Organisationen nutzen Vulnerability-Scanner; nur 40 % haben automatisierte Penetrationstests eingeführt. Hohe Tool-Adoption hat bei den meisten Organisationen nicht zu schnellerer Remediation geführt, weil der limitierende Faktor nicht die vorhandenen Tools sind, sondern ob diese Tools in einer Struktur operieren, die Ausnutzbarkeit validiert, mit Remediation integriert und Outcomes statt Aktivität misst.

Unser CTEM-Programm ist aktiv. Warum führt es nicht schneller zur Remediation?

Die meisten CTEM-Programme messen Erfolg auf eine Weise, die keine tatsächliche Risikoreduktion widerspiegelt. 67 % der Organisationen messen CTEM anhand identifizierter Coverage-Lücken; nur 33 % verfolgen Reduktionen ausnutzbarer Exposition über die Zeit. Ohne Exploitability-Validierung als erstklassigen Output und ohne Ownership-Alignment, das validierte Findings mit den zuständigen Personen verbindet, erzeugen CTEM-Programme mehr Findings, ohne die relevanten Outcomes zu verbessern.

Wir haben volle Pipeline-Visibilität. Warum sinkt unsere Exposition nicht?

Discovery und Validierung sind separate Probleme, und die meisten Programme behandeln sie als eines. Die Erweiterung der EASM-Coverage oder die Erhöhung der Scan-Frequenz erzeugt mehr Findings – aber wenn kein automatisierter Mechanismus bestätigt, welche davon tatsächlich ausnutzbar sind, entsteht ein größerer Backlog, keine verbesserte Posture. Mehr Discovery ohne Validierungskapazität erhöht die Last der Analysten, ohne ausnutzbares Risiko zu reduzieren. Der limitierende Faktor ist selten die Anzahl der gefundenen Findings; es ist, wie viele davon als real bestätigt und zur Remediation geleitet werden können, bevor ein Angreifer handelt.

Über Hadrian

Hadrian ist eine Offensive-Security-Plattform, die externe Angriffsflächen so identifiziert und validiert, wie es ein Angreifer tun würde – ohne vordefinierten Scope, entlang realer Angriffspfade und mit der Bestätigung jeder Schwachstelle, bevor sie Ihr Team erreicht. Anerkannt im Gartner Hype Cycle for Security Operations sowie von GigaOm und Frost & Sullivan.

MEHR ERFAHREN: HADRIAN.IO

FROST & SULLIVAN BEST PRACTICES AWARDS

GIGAOM RADAR REPORT LEADER 2025

Gartner Peer Insights 4.9/5 ★

AICPA SOC · ISO 27001

VERTRAUT VON

NBC · amadeus · McKESSON · BLINQX · CRÉDIT AGRICOLE · LEROY MERLIN · SHV

ABN·AMRO · London Business School · RITUALS... · SIEMENS energy · LOTTOMatica · FP FRANCISCO PARTNERS · CHRISTIE'S

BIOLANDES · WeatherTech · BLINQX · DAMEN · jamf · =exact

ICT GROUP · nedap · celio* · Inova · XM Cyber · AROMA360

UND ÜBER 300 WEITERE