HADRIAN

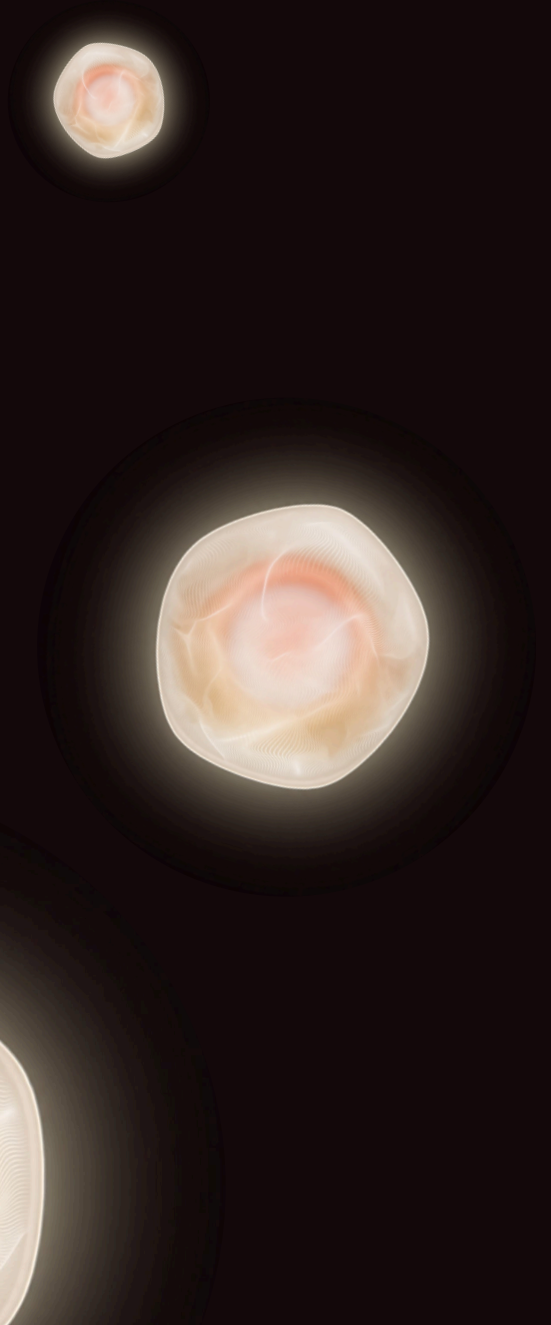
ZUSAMMENFASSUNG FÜR FÜHRUNGSKRÄFTE

Ihr Expositionsprogramm ist nur so stark wie seine schwächste Dimension.

Die meisten CISOs wissen, dass ihr Programm nicht dort steht, wo es stehen sollte. Die schwierigere Frage ist: Welcher Teil hält alles andere zurück – und was würde sich durch die Behebung genau dieses einen Punktes bei Remediation-Geschwindigkeit, Validierungs-Sicherheit und Leadership-Visibilität verändern?

Die Lücke ist selten eine Frage der Ressourcen. Organisationen auf jedem Maturity-Level kennen dieselbe Frustration: Tools sind implementiert, Prozesse definiert – und dennoch wächst der Remediation-Backlog, Findings häufen sich schneller an als sie validiert werden können, und die Führungsebene stellt Fragen, die das Programm noch nicht beantworten kann.

Der Grund ist strukturell. Externes Expositionsmanagement kennt vier verschiedene operative Haltungen. Die meisten Organisationen sind in einigen Dimensionen stärker als in anderen. Die schwächste Dimension setzt die Obergrenze für alles darüber. Solange diese Lücke nicht identifiziert und geschlossen ist, stagniert der Fortschritt – unabhängig davon, was sich sonst ändert.



Was das Modell ist

Das Hadrian Exposure Maturity Model bildet vier Stages des externen Expositionsmanagements ab – von reaktiv und unvollständig erfasst bis kontinuierlich und autonom. Jede Stage ist eine erkennbare operative Haltung, abgeleitet aus realen Programmmustern – kein Aspirationsrahmen. Das Modell nutzt sieben operative Dimensionen, um zu zeigen, wo Sie tatsächlich stehen und welcher operative Engpass Sie zurückhält.

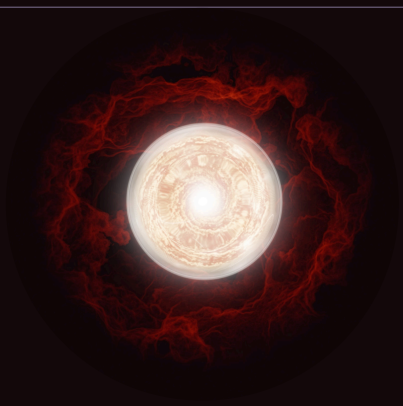
WARUM MATURITY-FORTSCHRITT ZÄHLT

STAGE 1 ZU 2

MTTR sinkt von 90+ Tagen auf 45. Coverage steigt von unter 20 % auf 40–60 %.MTTR sinkt von 90+ Tagen auf 45. Coverage steigt von unter 20 % auf 40–60 %.

STAGE 2 ZU 3

True-Positive-Raten steigen auf 40–60 %. SLA-Compliance erreicht 60–80 %. MTTR sinkt auf 15–45 Tage.



STAGE 3 ZU 4

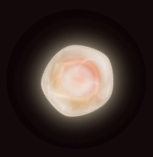
Coverage übersteigt 95 %. Kritische Expositionen werden innerhalb von 48 Stunden geschlossen. Neue Exploits werden in Stunden bestätigt, nicht Tagen.

DIE BEDROHUNGSLAGE WARTET NICHT

Die durchschnittliche Zeit zwischen Schwachstellen-Disclosure und aktiver Ausnutzung ist von 32 Tagen auf 5 gesunken. Nahezu jede dritte Schwachstelle wird am Tag ihrer Offenlegung oder früher ausgenutzt.

Die meisten Security-Programme basieren auf wöchentlichen Triage-Zyklen und quartalsweisem Testing. Die Lücke zwischen Angreifer-Geschwindigkeit und Programm-Maturity ist kein künftiges Risiko. Sie besteht jetzt.

Die vier Stages



STAGE 1

Ohne klare Sicht handeln

Exposition wird reaktiv entdeckt. Ownership ist unklar. Die Remediation-Queue wächst schneller als sie schrumpft. Das Team verwendet den Großteil seiner Kapazität auf Findings, die sich als irrelevant herausstellen.

- Reaktive Discovery
- Kein systematisches Asset-Ownership
- CVSS-getrieben Triage
- Compliance-orientiertes Reporting

STAGE 2

Mehr Überblick, bessere Perspektiven

Das Programm ist strukturiert, die Coverage verbessert sich. Die Einschränkung ist Validierung: Ausnutzbarkeit wird aus Severity-Scores abgeleitet statt bestätigt. MTTR liegt bei 45–90 Tagen.

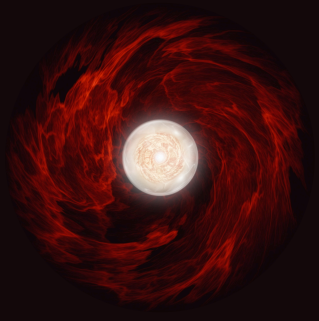
- Geplante Pentests
- Coverage bekannter Assets
- Manuelle Ausnutzbarkeitsuntersuchung
- Aktivitätsbasierte Metriken

STAGE 3

Zusammenhänge herstellen

Findings werden validiert, bevor sie die Queue erreichen. True-Positive-Raten erreichen 40–60 %. MTTR sinkt auf 15–45 Tage. Die Einschränkung: Findings ohne erhebliche manuelle Orchestrierung zu einem vollständigen Attack Picture zusammenzufügen.

- Kontinuierliches Monitoring
- Automatisierte Validierung
- Integriertes Remediation-Routing
- Messung ausnutzbaren Risikos



STAGE 4

Ein klares Gesamtbild gewinnen

Discovery ist kontinuierlich, Validierung autonom, die Führungsebene sieht Live-Posture-Daten. Coverage übersteigt 95 %. Kritische Expositionen werden innerhalb von 48 Stunden geschlossen. Neue Exploits werden in Stunden bestätigt.

- Autonome Emulation
- Echtzeit-Posture-Visibilität
- Prädiktive Priorisierung
- Live-Board-Reporting

DIE MEISTEN PROGRAMME HABEN EINE DIMENSION, DIE ALLES LIMITIERT.

Das interaktive Self-Assessment bewertet Ihr Programm über alle sieben Dimensionen unabhängig, identifiziert Ihren spezifischen Engpass und erstellt einen stage-spezifischen Aktionsplan, den Ihr Team direkt umsetzen kann. Es dauert fünf Minuten.

ASSESSMENT DURCHFÜHREN AUF HADRIAN.IO

ÜBER HADRIAN

Hadrian ist eine Offensive-Security-Plattform, die externe Exposition so erkennt und validiert wie ein Angreifer – ohne vordefinierten Scope, den Attack Paths folgend wohin sie führen, und jedes Finding als real bestätigend, bevor es Ihr Team erreicht. Ausgezeichnet 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

VON 300+ ENTERPRISE-ORGANISATIONEN EINGESETZT

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