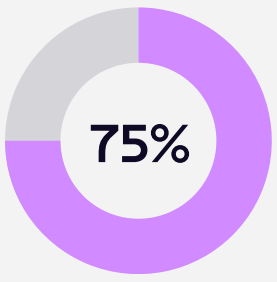
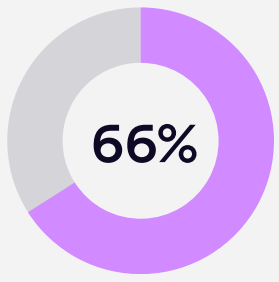
HADRIAN

Der ROI-Leitfaden für Offensive Sicherheit

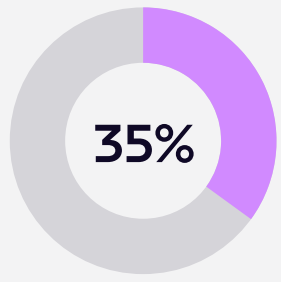
Offensive Sicherheit ergänzt und validiert bestehende Cybersicherheit Investitionen, indem sie Lücken in bestehenden Kontrollmechanismen identifiziert. Analysen zeigen, dass Führungskräfte zunehmend in offensive Sicherheit investieren, um Risiken proaktiv zu identifizieren und zu beheben.



Unbekanntes Risiko veranlasst **75,2%** der Organisationen, ihre Praktiken der offensiven Sicherheit zu erhöhen.[1]



Fernzugriff und internetbasierte Anwendungen machen 39% bzw. 27% der initialen Zugriffsvektoren in der ersten Hälfte des Jahres 2023 aus.[2]



Nach einem erfolgreichen Angriff investieren **35%** der Organisationen in offensive Sicherheit, die somit viert-häufigste Investition.[3]

Traditionelle Methoden der offensiven Sicherheit, wie manuelle Penetrationstests, Schwachstellen-Scans und das Management der Angriffsfläche, können Risiken unentdeckt und ungelöst lassen. Abbildung 1 zeigt die wichtigsten Bedenken, die befragte Sicherheitsfachleute hinsichtlich ihrer externen Bedrohungen hatten.

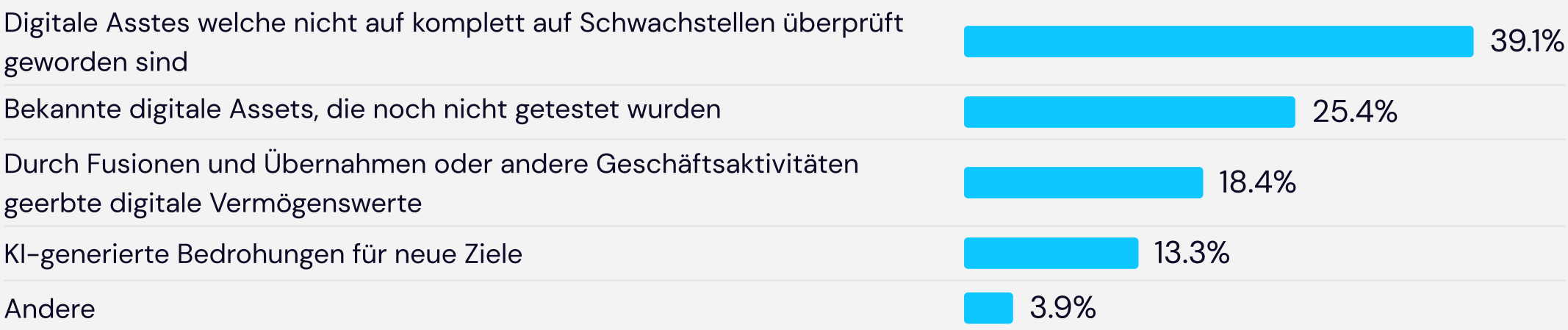


Figure 1 - Principales préoccupations concernant l'exposition aux menaces1

Herausforderungen traditioneller offensiver Sicherheitsmethoden:

Unentdeckte Schwachstellen

Legacy-Tools wie ASM oder Schwachstellenscanner erfassen nur wenige Risiken. Umfassende manuelle Tests sind zu unflexibel, um moderne Angriffsflächen vollständig zu sichern.

Nicht umsetzbare Ergebnisse

Die Effizienz der Behebung wird durch Werkzeuge und Berichte verringert, die unvalidierte Risiken und False-Positive enthalten. Eine Priorisierung ohne Kontext führt zu schlechter Fokussierung und langsamer Lösung.

Ressourcenintensiv

Manuelle Prozesse sind erforderlich, um Tests zu koordinieren oder Werkzeuge zu konfigurieren. Zusätzliche Forschung ist notwendig, um die Risiken zu verstehen und die optimalen Schritte zur Behebung zu identifizieren.

Hadrian Security bietet erstklassige offensive Sicherheit, damit Organisationen Bedrohungen proaktiv mindern und Risiken minimieren können. Die kontinuierliche und autonome Plattform bietet umfassende Abdeckung und macht Hadrian zu einer zukunftssicheren Lösung, die für eine breite Palette von Anwendungsfällen eingesetzt werden kann.

Quantifizierbare Vorteile

Herausforderung	Lösung
Überlastete Sicherheitsteams Cybersicherheitsteams stehen einer Flut von Alarmen gegenüber, die Ressourcen und Aufmerksamkeit von strategischen Sicherheitsaufgaben ablenken. Die Untersuchung von Sicherheitswarnungen ist ressourcenintensiv, wobei Teams durchschnittlich über 25 Minuten pro Alarm beschäftigt sind. Drittanbieter-Tools, wie Sicherheitsbewertungsdienste und das Management der Angriffsfläche, haben diese Situation durch eine Fehlklassifizierung der Schwere von Schwachstellen verschärft. Dies belastete die Ressourcen und behinderte die Konzentration auf entscheidende Sicherheitsbestrebungen.	**Intelligenzgesteuerte Priorisierung** Hadrians eigene Risikobewertungsalgorithmen durchbrechen das Rauschen und ermöglichen es Sicherheitsteams, sich auf die wichtigsten Risiken zu konzentrieren. Das Security Operations Centre (SOC) kann sich auf wichtige Vorfälle konzentrieren, die Prozesse des Vulnerability Managements können das Patching besser priorisieren, und DevSecOps-Teams können sich auf kritische Probleme konzentrieren. Die Priorisierung wird von Hadrians Orchestrator AI durchgeführt, die eine Reihe von Faktoren berücksichtigt, einschließlich der Wahrscheinlichkeit der Ausnutzung und der potenziellen Geschäftsauswirkungen. Die eigenen Bewertungsalgorithmen lernen aus dem Nutzerfeedback, um genauer zu werden.
Teure Drittanbieter-Tests Drittanbieter-Penetrationstests sind teuer und werden oft auf jährlicher Basis durchgeführt. Die periodische Natur der Tests bedeutet, dass Organisationen zwischen den Bewertungen eine eingeschränkte Sichtbarkeit haben. Zusätzlich haben diese Tests einen begrenzten Umfang, was bedeutet, dass nur ein Teil der exponierten Assets bewertet wird. Der typische Tagespreis für manuelle Penetrationstests kann zwischen 1000 und 3000 Dollar pro Tag liegen.	**Automatisierte Penetrationstests** Hadrians automatisierte Penetrationstests emulieren das Verhalten von Angreifern in der realen Welt zu einem Bruchteil der Kosten. Berichte in menschenlesbarer Form ermöglichen es, dass Abhilfemaßnahmen sofort umgesetzt werden und automatische Rescans überprüfen, ob die Lösung erfolgreich war. Hadrians Plattform führt Bedrohungsanalysen kontinuierlich durch, es ist nicht notwendig, auf den nächsten manuellen Test zu warten. Die automatisierten Penetrationstests untersuchen Sicherheitslücken rund um die Uhr, das ganze Jahr über.
Legacy-Sicherheitslizenzen Ineffektive oder isolierte Sicherheitswerkzeuge führen zu begrenzten Einblicken. Zusätzlich dienen Punkt-Lösungen, wie Schwachstellenscanner oder Sicherheitsbewertungsdienste, oft sehr begrenzten Anwendungsfälle. Viele Organisationen stehen vor Herausforderungen, die Wirksamkeit ihrer bestehenden Sicherheitswerkzeuge zu verstehen und Bereiche für Verfeinerungen zu identifizieren.	**KI-basierte Next-Gen-Lösung** Hadrians umfassende offensive Sicherheitsfähigkeiten ermöglichen es, bestehende Werkzeuge vollständig oder teilweise zu ersetzen, wodurch jährlich Zehntausende gespart werden. Hadrian kann auch Infrastruktur- und Edge-Geräte identifizieren, die stillgelegt werden können, um die Kosten weiter zu reduzieren.

Nicht quantifizierbare Vorteile

Herausforderung	Lösung
Langsame Sicherheitsprozesse Wesentliche Bestandteile des Exposure Managements, einschließlich des Prozesses der Planung und Durchführung von Tests, der Validierung der Ergebnisse und der Erforschung von Abhilfemaßnahmen. Sicherheitsteams folgen diesem Prozess, um Angriffspfade zu verstehen und Leitlinien für die Remediation Teams zu bieten. Wenn diese Prozesse jedoch manuell durchgeführt werden, sind sie extrem zeitaufwändig. Dies führt dazu, dass Sicherheitsressourcen dünn gesät sind und Probleme nicht effektiv vollständig untersucht werden können.	**Kontinuierliche Risikominderung** Hadrian automatisiert vollständig die Entdeckung, Validierung, Priorisierung und Abhilfeprozesse. Die Plattform verifiziert kontinuierlich die Sicherheitslage der Organisation und ermöglicht es Sicherheitsteams, ausnutzbare Schwachstellen proaktiv anzugehen. Orchestrator AI vereinfacht die Abhilfe, indem es den relevanten Geschäftseinheiten klare, schrittweise Anweisungen zur Lösung ausnutzbarer Risiken bereitstellt. Zusätzlich führt die Plattform automatisch Regressionstests durch, um die Wirksamkeit der Abhilfemaßnahmen zu bestätigen.
M&A- und Partnerbewertungen Während Fusionen und Übernahmen (M&A) ist das Verständnis und Management der Angriffsfläche neu integrierter Einheiten oft ein Kampf, was zu unbekannten Vermögenswerten und mit den IT-Abteilungen erworbener Tochtergesellschaften verbundenen Risiken führt, die nicht vollständig mit der IT-Abteilung der Mutterorganisation integriert waren. Ohne Einblick in die Sicherheitslage sind Organisationen nicht in der Lage, Maßnahmen zur Minderung ihres Risikoexposures zu ergreifen. Einige Organisationen beauftragen Drittanbieter zur Unterstützung, was pro Übernahme 250.000 kosten kann.	**Automatisierte Risikoeinsichten** Hadrian eliminiert die Notwendigkeit für Spezialprojekte, um ein umfassendes Inventar aller Tochtergesellschaften und Geschäftspartner-Angriffsflächen und ausgesetzten Risiken zu erhalten. Hadrians Plattform identifiziert effizient unbekannte Vermögenswerte und bietet Organisationen vollständige Sichtbarkeit und reduziert den Arbeitsaufwand für interne Teams. Echtzeit-Risikobewertungen bieten Einblicke zum Fußabdruck der erworbenen Firma. Orchestrator AI nutzt sein neuronales Netzwerkdiagramm des Internets, um alle extern ausgerichteten Vermögenswerte zu entdecken und sie umfassend zu testen.
Compliance-Kosten Die Durchführung von Penetrationstests ist ein häufiger Bestandteil von Compliance-Standards, einschließlich ISO 27001, SOC2, NIS2, DORA, HIPAA und PCI-DSS. Für Organisationen, die die Vorschriften einhalten müssen, können diese Bewertungen teure zusätzliche Kosten sein. Darüber hinaus können Organisationen Wochen damit verbringen, Berichte zu erstellen, um die Einhaltung der Compliance zu demonstrieren. Wenn dies vierteljährlich durchgeführt wird, kann dies zu einer Vollzeitfunktion werden.	**Bedarfsorientierte Berichterstattung** Hadrian hilft Organisationen, die Anforderungen an Penetrationstests, Schwachstellen- und Risikomanagement zu erfüllen. Die Plattform führt kontinuierlich Bewertungen durch und reduziert die zusätzlichen Tests, die koordiniert werden müssen. Das Dashboard von Hadrian ermöglicht es Sicherheitsteams, die Wirksamkeit ihrer Prozesse zu überwachen und zu demonstrieren. Berichte können bedarfsorientiert generiert und leicht mit internen und externen Stakeholdern geteilt werden.

Manuelle Asset-Inventur

Organisationen sind von zeitaufwändigen manuellen Prozessen abhängig, die Tabellenkalkulationen und manuelle Skripte umfassen, um ihre digitalen Vermögenswerte zu inventarisieren. Teams verbringen Zeit mit der Wartung der Skripte und der Reduplizierung der Ergebnisse, die sie produzieren.

Es wird geschätzt, dass pro Vermögenswert 10 Minuten Ingenieurzeit benötigt werden, um Vermögenswerte manuell zu inventarisieren. Diese Arbeitsbelastung und die begrenzte Datenpräzision behindern die Überwachung der Angriffsfläche aufgrund des Mangels an Automatisierung und seltenen Aktualisierungen.

Kontinuierliche automatisierte Inventarisierung

Hadrians Plattform findet und katalogisiert rund um die Uhr Vermögenswerte, um ein genaues und immer aktuelles Inventar zu erstellen. Die Ergebnisse können leicht in mehreren tabellenbasierten und grafischen Formaten überprüft oder für externe Analysen exportiert werden.

Die von Hadrian verwendeten Algorithmen zur Vermögensfindung nutzen bewährte Praktiken und eigene Techniken. Das hauseigene Entwicklungsteam aktualisiert die Technologie kontinuierlich, um neue Vermögensklassen zu identifizieren und die Automatisierung zu verbessern.

Hohe Kosten für Cyber-Versicherungen

Bei der Verhandlung von Prämienanpassungen mit einer Organisation berücksichtigen Cybersecurity-Versicherungsanbieter zahlreiche Faktoren. Allerdings fehlt es den Organisationen an Einblick in die tatsächliche Sicherheitslage.

Ohne Zugang zu glaubwürdigen Beweisen über die Stärke der Sicherheitslage der Organisation oder des Branchenbenchmarks wird geschätzt, dass die Cyber-Versicherungsprämien 1.500 Dollar pro Jahr pro 1 Million Dollar Schäden betragen.

Niedrigere Versicherungsprämien

Hadrian ermöglicht Organisationen, Einsparungen durch bevorzugte Bedingungen für ihre Cyber-Versicherung zu realisieren. Indem messbare Beweise für das reduzierte Risiko eines Breaches vorgelegt werden, sind Organisationen in der Lage, mit Versicherungsanbietern zu verhandeln.

Die Plattform ermöglicht es auch Organisationen, ihre Sicherheit mit ihren Kollegen zu vergleichen, sodass sie ihre relative Sicherheitslage und Reaktionsfähigkeit auf Bedrohungen verstehen können.

Verlorene Umsätze und Schäden

Ein Bruch oder eine Dienstunterbrechung kann einen materiellen Einfluss auf die Bilanz einer Organisation haben. Die nachfolgenden Kosten umfassen Sanierung, Ausfallzeiten, Produktivitätsverlust, rechtliche Strafen und Markenschäden.

Regulatorische Strafen, wie GDPR-Bußgelder, können schwerwiegend sein und Organisationen potenziell erhebliche finanzielle Belastungen auferlegen. Zusätzlich können Organisationen auch einer verstärkten Prüfung durch Regulierungsbehörden gegenüberstehen.

Erhöhte Resilienz

Hadrian ermöglicht es Organisationen, das Risikoexposure mit klaren, umsetzbaren Schritten zu reduzieren. Dies reduziert nicht nur die Wahrscheinlichkeit eines Verstoßes, sondern auch die potenziellen Auswirkungen, die ein solcher haben könnte.

Laut eines Berichts der IBM über die Kosten eines Datenleaks investieren 35% der Organisationen nach einem Verstoß in offensive Sicherheitstests. Durch frühzeitige Investitionen können Organisationen die Wahrscheinlichkeit eines Datenlecks erheblich reduzieren.

Abgeschottete Sicherheitsteams

Langsame Sicherheitstestpraktiken sind für die heutigen schnellen Entwicklungszyklen nicht geeignet. Penetrationstests können einen Monat zur Planung, weitere zwei Monate zur Durchführung benötigen und dann mehrere Wochen, bis der Bericht zusammengestellt ist. Dies ist unvereinbar mit Entwicklungsteams, die in 2-Wochen-Sprints arbeiten.

Bestehende Werkzeuge zur Durchführung von Sicherheitsbewertungen sind komplex. Sie sind nicht nur schwierig zu konfigurieren und zu verwenden, sondern die Ergebnisse enthalten oft Falschmeldungen und sind für Nicht-Sicherheitsfachleute schwer zu verstehen, um darauf angemessen zu reagieren.

Kollaborative & gestraffte Arbeitsabläufe

Hadrian rationalisiert den Prozess des Angriffsflächenmanagements und ermöglicht es Sicherheitsteams, eine sichere Cyberumgebung aufrechtzuerhalten. Die automatisierten Penetrationstestfähigkeiten der Plattform identifizieren in Echtzeit ausnutzbare Risiken und bieten Entwicklungsteams nahezu sofortiges Feedback.

Der Orchestrator AI ist darauf ausgelegt, offensive Sicherheits-Arbeitsabläufe zu vereinfachen, indem er Ergebnisse autonom validiert, um Falschmeldungen zu entfernen. Hadrian bietet auch eine Schritt-für-Schritt-Anweisungen, um den behebenden Teams zu ermöglichen, sofort Maßnahmen zu ergreifen.

Drittanbieter- und vergessene Anwendungen

Das Entdecken von Schwachstellen in Software von Drittanbietern wird für Organisationen ohne eine aktualisierte und genaue Inventarliste herausfordernd.

Das Fehlen von Sichtbarkeit stellt ein bedeutendes Problem dar. Zum Beispiel könnte eine Vorproduktionsumgebung erstellt worden sein, um die Funktionalität für ein neues Feature zu testen, wurde aber nicht stillgelegt. Solche übersehenen Anwendungen erfüllen oft nicht die Sicherheitsstandards.

Sichtbarkeit der Lieferkette

Hadrians Sonden sind in der Lage, über 10.000 SaaS-Anwendungen sowie Tausende von Softwarepaketen und Versionen zu identifizieren, was eine umfassende Anwendungserkennung gewährleistet.

Durch das kontinuierliche Scannen des Internets untersucht Hadrians Plattform Technologie, Versionen und Konfigurationen, um potenzielle Sicherheitsbedrohungen zu identifizieren.

Markenmissbrauch und Phishing

Die umfangreiche Anzahl von Subdomains und die dynamische Natur der DNS-Infrastruktur stellen Herausforderungen beim Monitoring dar. Subdomains können leicht übersehen werden, was sie für Übernahmeversuche und Kompromittierung der Infrastruktur anfällig macht.

Unbeanspruchte oder schlecht verwaltete Subdomains können als Eintrittspunkt für Hacker dienen, was zu potenziellen Markenschaden, Verlust des Kundenvertrauens und Datenverletzungen führen kann. Angreifer könnten beispielsweise eine Subdomain ausnutzen, um Authentifizierungscookies zu stehlen.

Eine vertrauenswürdige Marke aufbauen

Hadrian verhindert Markenschäden, indem es Subdomain-Schwachstellen überwacht, die für Übernahmen anfällig sind. Die Plattform scannt kontinuierlich die DNS-Infrastruktur, um aufkommende Risiken zu identifizieren.

Die Plattform alarmiert Sicherheitsteams sofort, ermöglicht proaktive Behebung und verhindert, dass Subdomains für eine Phishing-Kampagne übernommen werden. Schnelle Behebung eliminiert das Risiko, dass Kunden, Mitarbeiter und Partner auf bösartige Phishing-Seiten stoßen.

Über Hadrian

Defensive Sicherheit sollte durch offensive Sicherheit validiert werden. Hadrian bietet die Hacker Perspektive und enthüllt die Ziele und Methoden, die bei einem realen Datenbreach verwendet werden könnten. Hadrians kontinuierliches und umfassendes Testen entdeckt und validiert Risiken vollständig autonom.

Unsere Lösung

Hadrians Plattform vereint die Entdeckung von Angriffsflächen, automatisiertes Penetrationstesting und das Management von Bedrohungslagen in einer cloud-basierten und agentenlosen Plattform. Die Plattform wird vom Orchestrator AI angetrieben, der die Techniken und Verhaltensweisen eines realen Hackers emuliert, um kontinuierlich 24x7 die Erkennung von Bedrohungen, die sich an das Internet richten, zu ermöglichen und Falschmeldungen autonom zu entfernen.

Orchestrator AI nutzt sein Wissen über Ihre Umgebung, um auf ausnutzbare OWASP Top Ten Risiken, bekannte und Zero-Day-Schwachstellen sowie exponierte und falsch konfigurierte Dienste zu testen. Scans werden verknüpft, um komplexe multidimensionale Angriffe zu simulieren. Die Spitzentechnologie wird ständig von Hadrians Hackerteam aktualisiert und verbessert.

+200	+1.2m	40%
Geschützte Unternehmen	Gesicherte Vermögenswerte	Schnellere durchschnittliche Zeit bis zur Lösung

Vertrauenswürdig von

ABN·AMRO · SHV ENERGY · macmillan education · WeatherTech · LEROY MERLIN · LOTTOMATICA · RITUALS · BIOLANDES · nedap

> "Was an dem, was Hadrian tut, spannend ist, ist, dass sie ein scheinbar unmögliches Rätsel gelöst haben: Schwachstellen in einem komplexen Netzwerk mit menschenähnlicher Detailgenauigkeit, im großen Maßstab, von außen und kontinuierlich zu finden. "Was normalerweise ein spezialisiertes Team von Sicherheitsingenieuren in einigen Wochen erledigt, können sie in Minuten für Tausende von Systemen tun."
>
> **Tiago Teles, Security Lead - ABN AMRO**