PENTERA PLATFORM

VERWANDELN SIE VALIDIERTE CYBERRISIKEN IN MESSBARE REDUZIERUNG DER ANGRIFFSOBERFLÄCHE

Reduzieren Sie Ihre Cyber-Exposition über interne Netzwerke, externe Assets sowie Cloud- und Hybridumgebungen hinweg durch KI-gestütztes Testen in Produktivumgebungen. Beheben Sie ausnutzbare Sicherheitslücken, priorisiert nach nachgewiesenem Schadenspotenzial und verkürzen Sie die Behebungszeit durch integrierte Remediation-Workflows. Weisen Sie die Reduzierung der Angriffsoberfläche durch kontinuierliche Nachtests mit revisionssicheren Nachweisen für Führungskräfte und Compliance-Teams nach.

Stärken Sie Ihre Sicherheitsresilienz

TESTEN SIE SO DYNAMISCH WIE ANGREIFER

Führen Sie nach Bedarf Tests aus der Angreifersicht durch, die sich der Umgebung anpassen, um ausnutzbare Fehlkonfigurationen, Zugangsdaten und Risiken durch Privilegieneskalation aufzudecken.

PRIORISIEREN SIE AUF BASIS NACHGEWIESENER AUSWIRKUNGEN

Identifizieren Sie Ihr größtes Risiko, indem Sie Daten dynamisch abfragen und Risiken im Kontext von Asset-Kritikalität, Risiko für den Geschäftsbetrieb, Branche und Region bewerten.

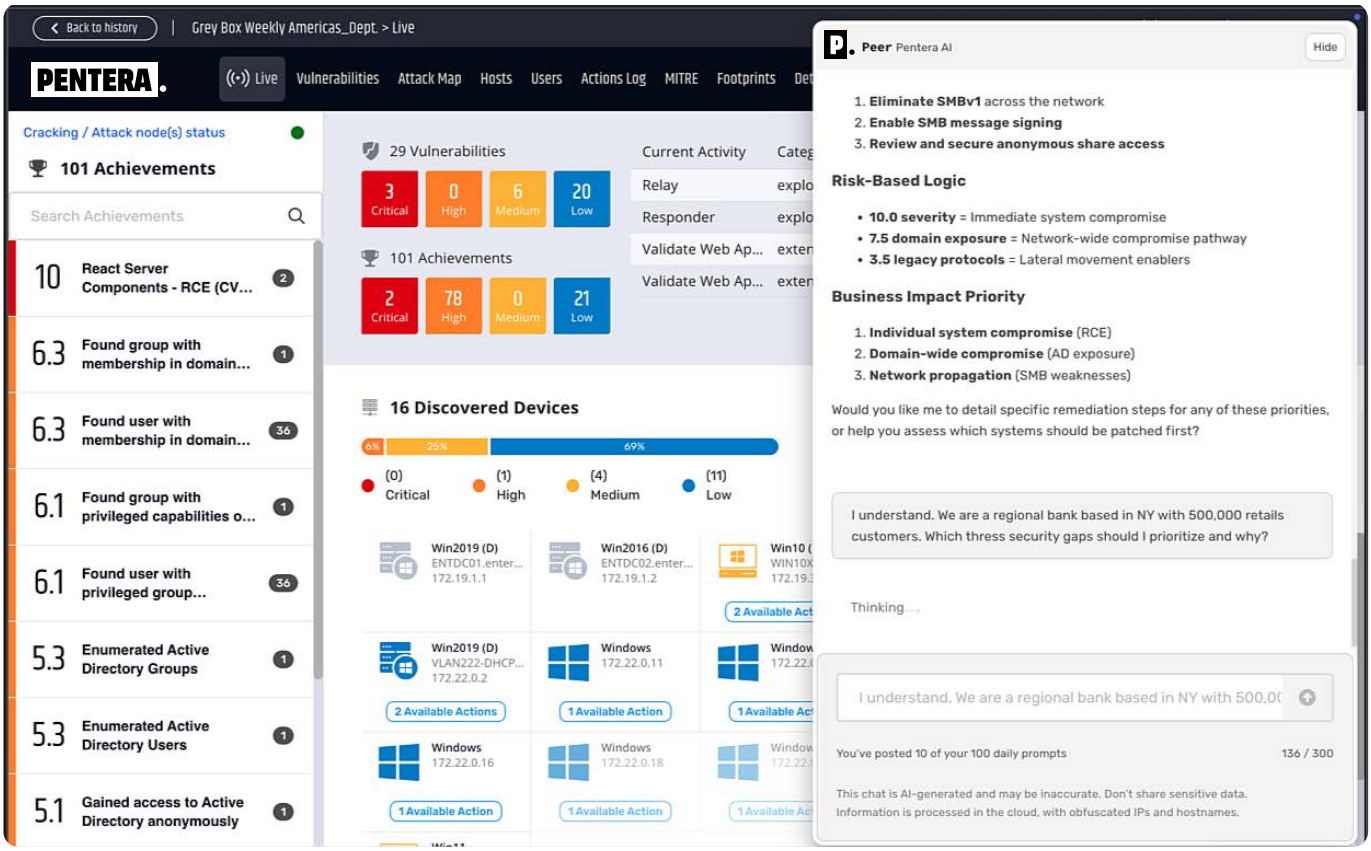
BEHEBEN SIE SCHWACHSTELLEN MIT PRÄZISION

Mobilisieren Sie die Remediation und reduzieren Sie die MTTR (Mean Time To Remediate - die Zeit zwischen Erkennen und Beheben einer Schwachstelle) mit KI-gestützten Workflows, die klare Behebungsschritte direkt in bestehende SecOps-Tools integrieren.

VALIDIEREN SIE DIE RISIKOREDUKTION

Weisen Sie Verbesserungen Ihrer Sicherheitslage im Zeitverlauf nach, indem Sie den Fortschritt der Behebungsmaßnahmen verfolgen und Korrekturen erneut testen, um sicherzustellen, dass Probleme vollständig behoben sind.

Agentengestützte Angriffsemulation



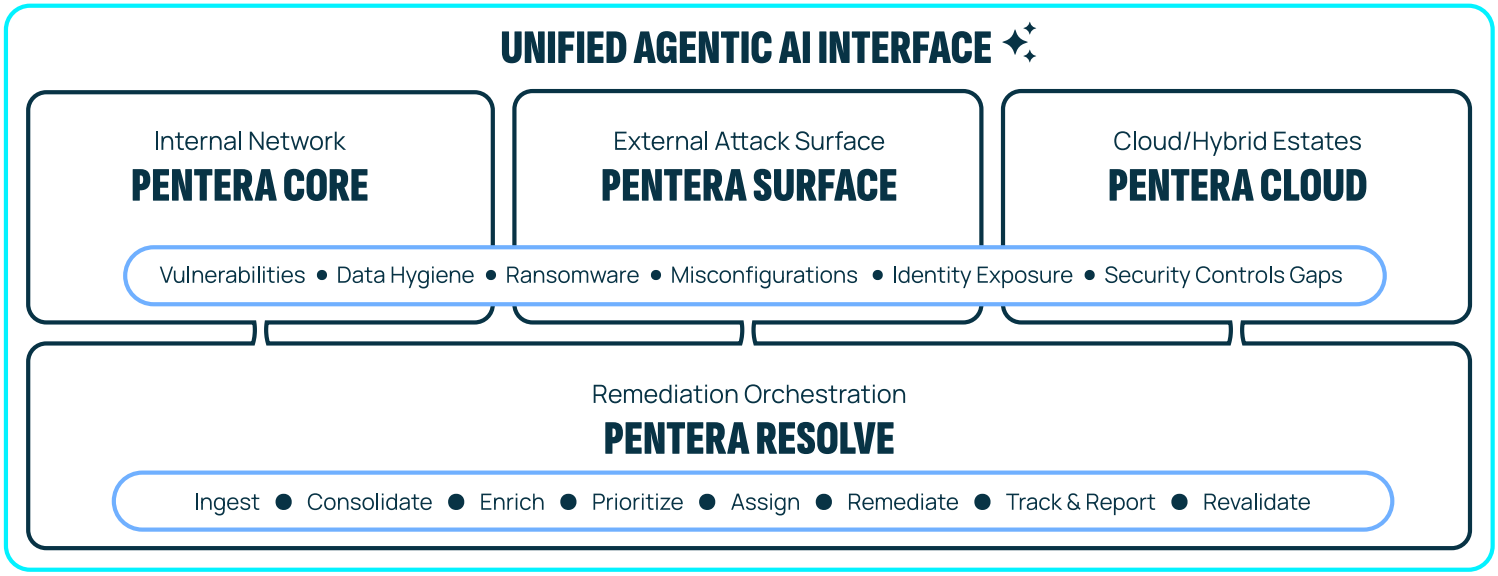
GESCHÄFTSORIENTIERTE ANALYSE
Übersetzen Sie validierte Ergebnisse in klare, geschäftsrelevante Prioritäten – abgestimmt auf Ihre Rolle, Branche und Compliance-Anforderungen.

VERWANDELN SIE AKTUELLE TESTERGEBNISSE IN EINEN SOFORT UMSETZBAREN MASSNAHMENPLAN
abgestimmt auf Ihre Behebungsprioritäten.

ÜBER PENTERA

Pentera ist Marktführer im Bereich KI-gestützter Sicherheitsvalidierung und bietet Unternehmen eine Plattform, mit der sie ihre Cybersicherheitskontrollen proaktiv anhand aktueller Angriffsszenarien testen können. Pentera identifiziert sicherheitsrelevante Risiken über die gesamte Angriffsoberfläche hinweg und steuert automatisiert Maßnahmen zur Behebung, um die Angriffsoberfläche nachhaltig zu reduzieren.
Die Sicherheitsvalidierung ist ein zentraler Bestandteil von Continuous Threat Exposure Management (CTEM). Tausende Sicherheitsexperten weltweit vertrauen auf Pentera, um Schwachstellen zu beheben, bevor Angreifer sie ausnutzen können.

Vereinheitlichte plattform zur exposure-validierung



ANGRIFFSTESTS IM ENTERPRISE-MASSSTAB

- **Echte Angreifer Emulation** - Validieren Sie Ihre Abwehrmaßnahmen gegen reales Angreiferverhalten über vollständige Angriffsketten hinweg, unter Einsatz deterministischer Logik und agentischer Adaptivität.
- **Umfassende Abdeckung der Angriffsoberfläche** - Identifizieren Sie ausnutzbare Schwachstellen und validieren Sie die Leistungsfähigkeit Ihrer Sicherheitskontrollen über die gesamte Enterprise-Angriffsoberfläche hinweg.
- **Tests im Enterprise-Maßstab** - Skalieren und passen Sie Ihre Tests an Threat Intelligence, Compliance-Anforderungen und geschäftliche Auslöser an – ganz ohne zusätzlichen Personalbedarf.

OPERATIONALISIERUNG DER RISIKOREDUKTION

- **Kontextbasierte Priorisierung** - Priorisieren Sie Behebungsmaßnahmen anhand integrierter Daten aus Ihrer gesamten Sicherheitsarchitektur, angereichert mit validierten Angriffspfaden.
- **Automatisierte Einordnung der Behebungsprioritäten** - Verkürzen Sie die Zeit bis zur Lösung mit KI-gestützten Abläufen, integriert in Ihre bestehenden IT-Service-Management-Systeme.
- **Exposure- und Performance-Reporting** - Verkürzen Sie die MTTR und reduzieren Sie Ihre Angriffsoberfläche durch klare, trendbasierte Auswertungen.

Warum Pentera

KI-gestützte Sicherheitsvalidierung vom ersten Angriff bis zur Behebung.

Testing und Governance auf Enterprise-Niveau über hybride und verteilte IT-Umgebungen hinweg.

Remediation, nativ integriert in bestehende SecOps-Workflows.

Sichere Angriffsemulation in Live-Umgebungen – ohne Beeinträchtigung von Verfügbarkeit oder Stabilität.

Agentenlose Bereitstellung ohne Wartungsaufwand oder operative Reibungsverluste.

Operationalisieren Sie das Exposure Management mit Pentera

Testen Sie proaktiv gegen reale Angreifer, identifizieren Sie tatsächlich ausnutzbare Schwachstellen und orchestrieren Sie die Behebung vom Fund bis zur vollständigen Beseitigung.