Die Pentera Plattform

Sicherheitslücken reduzieren mit Automated Security Validation™

Testen Sie kontinuierlich Ihre Cyber-Resilienz in allen internen und externen, sowie Cloud-Oberflächen.
Starten Sie sichere Echtzeit-Angriffe auf Ihre produktive IT-Umgebung, um zu ermitteln, wo Sie wirklich verwundbar sind.
Beheben Sie die relevantesten Sicherheitslücken basierend auf den echten Auswirkungen.

So optimieren Sie Ihre Security Readiness.

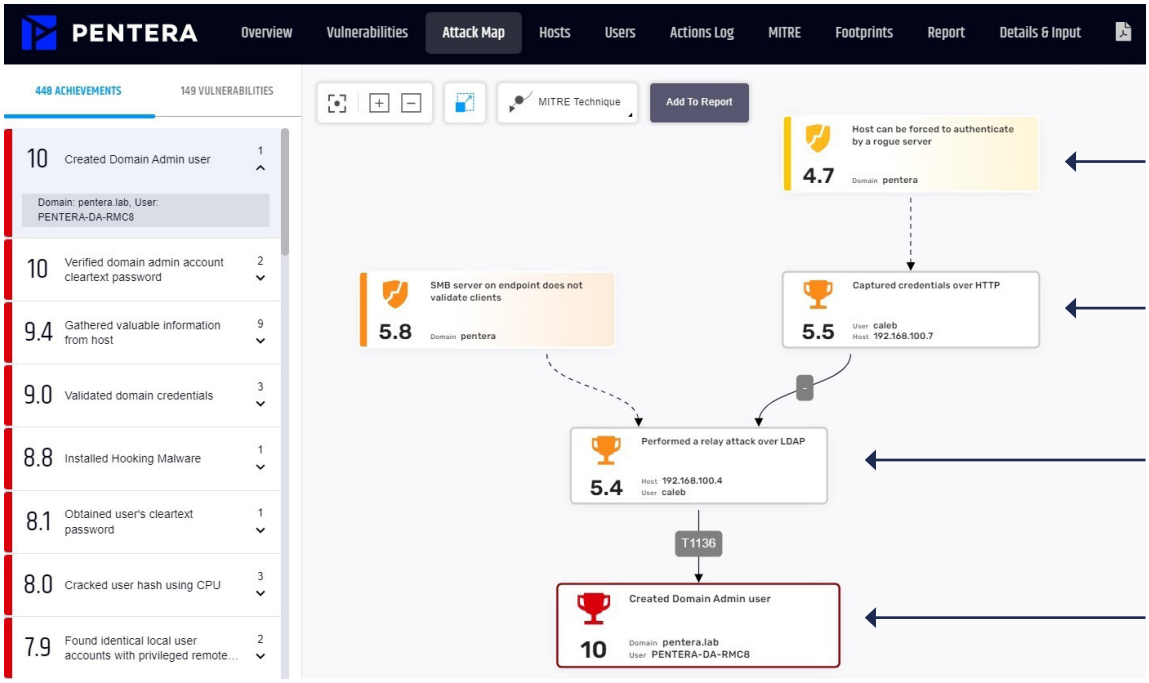
Jede Angriffsoberfläche testen
Identifizieren Sie ausnutzbare Schwachstellen, Fehlkonfigurationen, Anmeldeinformationen und Berechtigungen in Ihrer gesamten IT-Umgebung.

Schwachstellen ausnutzen wie ein Angreifer
Automatisieren Sie Testläufe realistischer Angriffsszenarien in der Produktivumgebung mit dem größten Archiv an Techniken und Taktiken Cyberkrimineller.

Abhilfemaßnahmen präzise steuern
Beheben Sie die Lücken, die Ihr Geschäft am meisten bedrohen und zeigen Sie laufend Verbesserungen Ihrer Security-Umgebung.

Individuelle Testhäufigkeit
Tägliche, wöchentliche oder benutzerdefinierte Testläufe, um Schwachstellen zu ermitteln und zu beheben, bevor Kriminelle sie entdecken.

Beseitigen Sie die Angriffspfade mit dem höchsten Risiko



Root cause:
Misconfiguration

Credentials captured

Authentication via credential relay

Risk impact:
Domain admin access

So sieht Ihre Sicherheit mit uns aus

+ Geringere Gefährdung durch Cyberkriminalität

Ermitteln und beheben Sie chirurgisch kritische Sicherheitslücken mit Algorithmus-basierter, automatischer Sicherheitsvalidierung.

+ Kosten durch Drittanbieter einsparen

Testen Sie Ihr Sicherheitslage nach Bedarf, ohne von manuellen Prüfungen und externen Dienstleistern abhängig zu sein.

+ Mehr Teamproduktivität

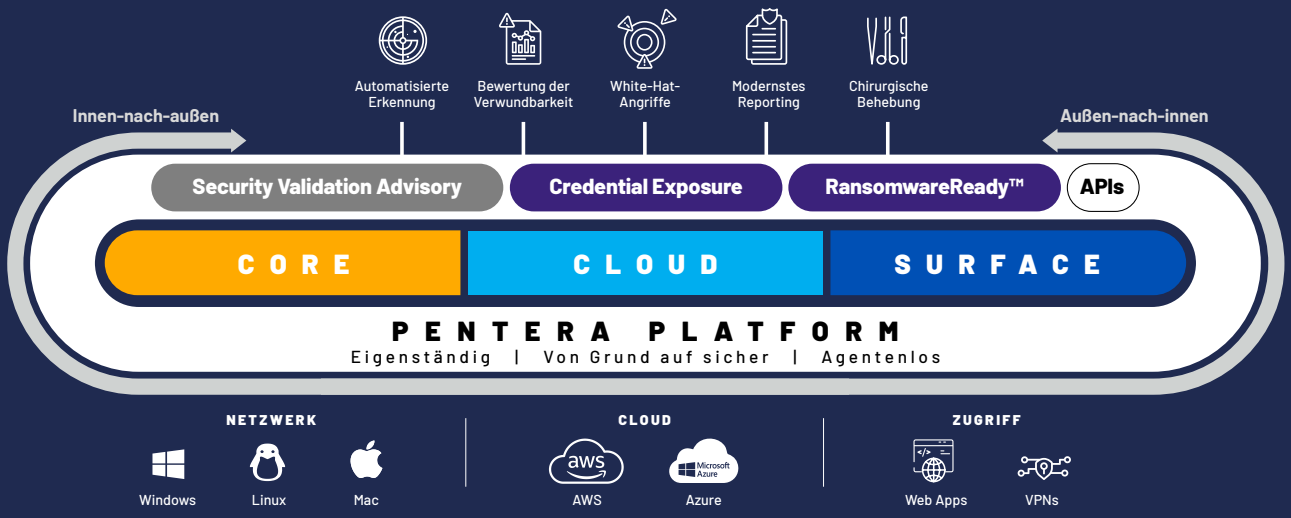
Bieten Sie Ihrem Team einen klaren, nach geschäftlichen Auswirkungen geordneten Fahrplan zur Behebung von Schwachstellen.

Über Pentera

Pentera ist Marktführer im Bereich Automated Security ValidationTM und versetzt jedes Unternehmen in die Lage, ganz leicht die Integrität aller Cybersecurity-Ebenen zu testen und jederzeit und unabhängig von der Größe genaue Informationen zu tatsächlichen Sicherheitslücken zu erhalten.
Tausende von Experten in der IT-Sicherheitsbranche sowie Dienstleister auf der ganzen Welt vertrauen auf Pentera, um anschauliche Anleitung zu erhalten und Sicherheitslücken zu schließen, bevor sie ausgenutzt werden können.

PENTERA | DATA SHEET

Alle Ihre Angriffsoberflächen, kontinuierlich getestet



+ Eigenständig

Penteras Algorithmen-basierte Angriffs-Engine imitiert die Taktiken von Cyberkriminellen und testet tausende von Angriffsvektoren in Computergeschwindigkeit.

+ Von Grund auf sicher

Pentera stellt mit eingebauten Sicherheitskontrollen und einem strengen Zulassungsverfahren für neue Funktionen sicher, dass Ihr Geschäftsablauf und Ihre Assets nicht beeinträchtigt werden.

+ Agentenlos

Pentera operiert in Ihrer IT-Umgebung ohne Installation von Agenten, was Installation und Wartung erleichtert.

Pentera Core

Validieren Sie Ihr Internes Netzwerk, indem Sie Ihre Sicherheitskontrollen stresstesten

Pentera Cloud

Validieren Sie Ihre Cloud-Umgebung mit automatisierten Tests Cloud-nativer Attacken

Pentera Surface

Kontinuierliche Validierung von externen Angriffsoberflächen, um echte webbasierte Sicherheitslücken zu ermitteln

RansomwareReady™

Validierung gegen Ransomware-Gruppen durch Ausführung von Ransomware-Attacken

Credential Exposure

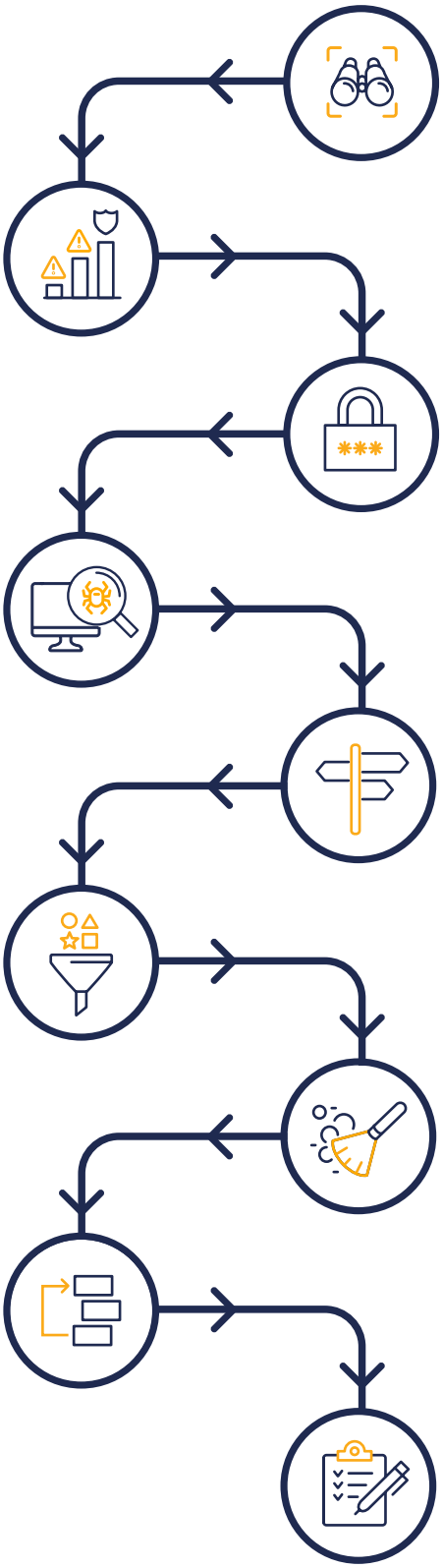
Validierung gegen Identitätsdiebstahl durch Tests von gestohlenen Anmeldeinformationen auf allen Angriffsoberflächen

Security Validation Advisory

Holen Sie das Meiste aus Pentera heraus mit unserem globalen Beraterteam an Ihrer Seite

So funktioniert es:

Pentera führt auf sichere Art und Weiseg alle Aktionen eines potenziellen Angreifers durch



Aufklärung
Automatische Ermittlung und Ausforschung Ihrer internen Netzwerk-, Cloud- und internet-basierten Assets

Bewertung
Ermittlung von Schwachstellen, Konfigurationsfehlern und Lücken in der Sicherheitshygiene

Testen von Anmeldeinformationen
Testen der Passwortstärke und Nutzung schwacher oder gestohlener Zugangsdaten, um Angriffe fortzuführen

Resilienz von Endgeräten
Testen Sie Endgeräte mit sicheren Exploits und Malware-Nachbildungen

Lateralbewegung
Bewegen Sie sich zwischen Assets, über Netzwerksegmente, und von Cloud- zu On-Premise-Strukturen oder umgekehrt

Exfiltration & Impact
Zeigen Sie das Ergebnis eines erfolgreichen Angriffs ohne Daten oder die Betriebsstabilität zu beeinträchtigen

Aufräumen
Testbezogene Daten und Code werden entfernt, um keine Spuren zu hinterlassen

Anleitung zu Abhilfemaßnahmen
Kritische Angriffspfade werden beseitigt und Sicherheitslücken nach ihren tatsächlichen Auswirkungen bei der Reparatur priorisiert

Berichte
Dokumentieren Sie Funde für die Zwecke interner Kommunikation und Umsetzung von Abhilfemaßnahmen