



## AUTOMATED SECURITY VALIDATION MIT INDEVIS PENTEST AS A SERVICE

indevis Pentest as a Service (PtaaS) auf Basis der Automated Security Validation (ASV) Plattform von Pentera ermöglicht es Ihnen, Sicherheitslücken in Ihrem Netzwerk zu entdecken und zu beheben, bevor sie von Hackern ausgenutzt werden können. Mit indevis Pentest as a Service lässt sich die interne und externe Angriffsfläche ihrer IT-Infrastruktur kontinuierlich auf Sicherheitslücken überprüfen und auf sichere Weise deren Widerstandsfähigkeit gegen neueste Bedrohungen validieren. PtaaS bietet eine effektive Möglichkeit, die IT-Sicherheit spürbar zu erhöhen und Kosten zu optimieren.

### MIT AUTOMATISierter SICHERHEITSVAlIDIERUNG NICHTS DEM ZUFALL ÜBERLASSEN

Angreifer sind mit gängigen Abwehrtechniken sehr gut vertraut und nutzen Sicherheitslücken gnadenlos aus. Um sicherzustellen, dass Sicherheitssysteme tatsächlich das tun, was sie sollen, können Unternehmen Ihre IT-Infrastruktur und -Systeme nur kontinuierlich testen und validieren. Ergreifen Sie die Initiative bei der Behebung von Schwachstellen, Fehlkonfigurationen, abgeflossenen Anmeldeinformationen und Zugangsrechten, bevor diese ausgenutzt werden können. Eine automatisierte Sicherheitsvalidierung hilft dabei zu entscheiden, worauf Sicherheitsteams ihre Bemühungen als Nächstes konzentrieren sollen.

### SO ERHÖHT INDEVIS PENTEST AS A SERVICE IHRE IT-SICHERHEIT

#### Erkennung von echten Risiken:

Durch das Nachahmen realer Angriffe entdecken Unternehmen ihre ausnutzbare Angriffsfläche und decken angreifbare Sicherheitslücken auf.

#### Zeit- und Kostenersparnis:

Automatisierte Tests laufen schneller und können häufiger durchgeführt werden als manuelle Prüfungen. Das senkt die Gesamtkosten für Sicherheitsprüfungen.

#### Stets auf dem neuesten Stand der Bedrohungen durch regelmäßige Updates:

Automatisierte Systeme können schnell aktualisiert werden, um neue Bedrohungen und Schwachstellen zu erkennen und darauf zu reagieren.

#### Abdeckung der gesamten Angriffsfläche:

Mit einer automatisierten Sicherheitsvalidierung lassen sich sowohl interne als auch externe Angriffsflächen erkennen und bewerten, um echte Sicherheitslücken zu ermitteln.

#### Konsistenz und Genauigkeit:

Automatisierung reduziert menschliche Fehler und stellt sicher, dass Sicherheitsprüfungen stets nach denselben Standards durchgeführt werden.

#### Einfacher Betrieb und Skalierbarkeit:

indevis PtaaS arbeitet ohne Agenten oder Playbooks und kann problemlos auf große und komplexe IT-Umgebungen angewendet werden, was mit manuellen Methoden kaum möglich wäre.

#### Besseres Risikomanagement:

Durch kontinuierliche Bewertung der Sicherheitslage können Risiken besser erkannt und gemindert werden.

#### Effizienzsteigerung:

Sicherheitsteams können sich auf strategische Aufgaben konzentrieren, da Routineprüfungen automatisiert sind.

### IHRE VORTEILE

- + Automatisierte Pentests und Security-Validierung
- + Erkennung von echten Risiken und Sicherheitslücken
- + Erhöhung des Sicherheitsniveaus ohne zusätzliche Belastung interner Ressourcen
- + Erfüllung von Compliance-Vorgaben
- + Detailliertes Reporting mit Handlungsempfehlungen für SecOps Team und Management



### SIE WOLLEN MEHR ERFAHREN?

Ihr persönlicher Ansprechpartner berät Sie gerne und findet mit Ihnen heraus, welches Konzept am besten zu Ihnen passt.

+49 (89) 45 24 24-100  
sales@indevis.de  
www.indevis.de



## ÜBER DIE INDEVIS GMBH

Die ISO 27001 zertifizierte indevis GmbH mit Sitz in München bietet seit 1999 IT-Sicherheits-, Datacenter- und Netzwerklösungen, flankiert von professionellen Consulting-, Management- und Support-Dienstleistungen. Dabei erfüllt indevis sowohl die Anforderungen der Wirtschaft als auch die von öffentlichen Behörden und Hochschulen.

Als einer von Deutschlands führenden Managed Security Service Providern ist indevis der Partner für IT Security und Netzwerktechnik für Unternehmen jeder Größe und Branche – denn IT-Sicherheit muss strategisch geplant werden.

Dabei ist indevis nicht nur in München und Umgebung vertreten: Unsere Mitarbeiterinnen und Mitarbeiter sind an Standorten in ganz Deutschland aktiv.



indevis GmbH  
Koppstraße 14  
81379 München

Tel. +49 (89) 45 24 24-100  
Fax +49 (89) 45 24 24-199

sales@indevis.de  
www.indevis.de

## MANUELLES PENTESTING VERSUS PENTEST AS A SERVICE

Pentesting ist aufwändig und teuer. Bisher konnten sich daher meist nur große Unternehmen solche Cybersecurity-Tests leisten, oder aber Unternehmen mit einem besonders hohen Sicherheitsbedarf, die strengen Compliance-Vorgaben unterliegen. Häufig werden Pentests nur einmal jährlich oder sogar noch seltener durchgeführt. Zudem unterliegen die Tests den individuellen Fähigkeiten des Pentesters, sind nicht unbegrenzt skalierbar und folgen keiner standardisierten Test-Methodik. Glücklicherweise hat sich Pentesting weiterentwickelt: Die autonome Plattform für Cybersicherheitsvalidierung von Pentera bietet eine kontinuierliche Sicherheitsüberprüfung, die auch für mittelständische Unternehmen erschwinglich ist. Gänzlich komfortabel und skalierbar wird Automated Security Validation als indevis Pentest as a Service. Dieser beinhaltet außerdem regelmäßige Servicemeetings inkl. Besprechung der Reports, Anpassung der Szenarien und Beratung.

Manuelles Pentesting	indevis Pentest as a Service
Qualität ist abhängig von Kompetenz und Erfahrung des Pentesters.	Konsistente Testverfahren und keine Abhängigkeit von individuellem Know-how von Drittanbietern.
Manuelle Durchführung ist nach einiger Zeit wieder überholt.	Kontinuierliche Anpassung an aktuelle Angriffstechniken und neue Schwachstellen.
Einmalige sowie zeit- und kostenintensive Durchführung und Auswertung.	Automatisiertes und wiederholbares Pentesting mit präziser Darstellung der Attack-Chain und der Auswirkungen.
Die Umsetzung von Gegenmaßnahmen erfordert ein hohes Skill-Level.	Die Umsetzung von Gegenmaßnahmen kann schnell und ohne hohes Skill-Level erfolgen – bei Bedarf auch mit der Unterstützung von indevis.
Manuell erstellte Berichte mit befristeter Aussagekraft.	Automatisiertes Reporting mit konkreten Handlungsempfehlungen.

## PRIORISIERTE HANDLUNGSEMPFEHLUNGEN FÜR SECURITY-TEAMS

Mit indevis Pentest as a Service können die Ursachen von Angriffspfaden ermittelt und kritischen Sicherheitslücken präzise Prioritäten zugewiesen werden. Das Besondere daran: Die Priorisierung der Handlungsempfehlungen erfolgt nicht rein auf Basis des CVE-Scores, sondern gemäß einer speziellen „Remediation Priority“. Anhand einer Attack-Chain wird aufgezeigt, wie verschiedene Schwachstellen in der Unternehmensinfrastruktur miteinander verbunden sind, was bei ihrer Behebung die Fokussierung auf wirklich ausnutzbare, geschäftsschädigende Sicherheitslücken sowie effektive Gegenmaßnahmen ermöglicht. Mit indevis PtaaS können Unternehmen ihre Sicherheitslage somit automatisiert, regelmäßig und wiederkehrend validieren, ihre Fortschritte mithilfe anschaulicher Reports nachverfolgen und den Sicherheitsstatus ihrer IT-Infrastruktur mithilfe wichtiger Kennzahlen und eines umfassenden Security-Dashboards jederzeit im Blick behalten.

## COMPLIANCE-ANFORDERUNGEN ERFÜLLEN

KRITIS, NIS-2, DORA, TIBER, TISAX & Co erfordern alle eine Sicherheitsvalidierung oder Penetrationstests zur Einhaltung der jeweiligen Regularien. Bewerten Sie das IKT-Risiko (IKT=Informations- und Kommunikationstechnologien) präzise gemäß Ihrer Compliance-Anforderungen mit automatisierten Tests realer Cyberangriffe in Ihren Produktivsystemen.

## INDEVIS PENTEST AS A SERVICE – DEMO ODER PROOF OF VALUE

Gerne führen wir Ihnen indevis PtaaS in einer ausführlichen Demo-Session vor oder demonstrieren Ihnen die Mehrwerte in einem PoV.