Schwachstellen finden, bevor Angreifer es tun. Penetration Testing von Argos.

Realitätsnahe Angriffssimulationen decken ausnutzbare Lücken in Netzwerken, Anwendungen und Systemen auf. Zertifizierte Tester verifizieren jedes Finding manuell und liefern einen nach CVSS priorisierten Bericht mit konkreten Maßnahmen.

>600	100+	24/7	seit 1999	ISO 27001	NIS-2
Kunden	Security-Experten	Cyber Defense Center	Managed Security	TÜV-SÜD-zertifiziert	DSGVO- & ISO-27001-Nachweise unterstützt

Das leistet der Service für Sie.

Angriffssimulation

Externe und interne Angriffssimulation prüft Ihre Angriffsfläche, wie ein echter Angreifer vorgehen würde – kontrolliert, dokumentiert, ohne Betriebsrisiko.

Web- & API-Tests

Gezielte Tests von Webanwendungen, APIs und Cloud-Diensten auf Logik-, Authentifizierungs- und Injection-Schwachstellen – vor Releases und größeren Changes.

Manuelle Verifikation

Jede Schwachstelle wird manuell verifiziert und kontrolliert ausgenutzt – kein reiner Scan: nur real belegte Risiken, keine Fehlalarme im Bericht.

Priorisierter Bericht

Management-Zusammenfassung und technische Details je Finding, nach CVSS bewertet und nach realem Risiko geordnet – mit konkreten Maßnahmenempfehlungen.

Für wen: Für Organisationen, die ihre reale Angreifbarkeit belastbar kennen müssen – von Software- und SaaS-Anbietern über KRITIS-, NIS-2- und DORA-regulierte Unternehmen bis zum wachsenden Mittelstand nach Cloud-Migration.

Automatisierte Scans listen potenzielle Schwachstellen – mit Fehlalarmen und ohne Blick auf reale Angriffspfade. Argos-Tester verifizieren jede Schwachstelle manuell, nutzen sie kontrolliert aus und verketten sie zu realen Angriffspfaden – so fließt Ihr Budget in die Risiken, die wirklich ausnutzbar sind.

Auf Seite 2: der direkte Vergleich mit dem klassischen Ansatz →

Ihr direkter Draht: +49 89 45 24 24-100 · kontakt@argos.security

Argos Penetration Testing vs. klassischer Ansatz

der Vergleich auf einen Blick

Kriterium	Klassischer Ansatz	Argos Penetration Testing
Methode	Automatisierter Scan, potenzielle Findings	**100 % manuell verifiziert** kontrollierte Ausnutzung realer Angriffspfade
Perspektiven	Eine Sicht, oft nur von außen	**Black-, Grey- und White-Box** extern und intern, Beratung im Scoping
Ergebnis	Scanner-Score, viele Fehlalarme	**CVSS-priorisiert nach realem Risiko** Management- und Technik-Report getrennt
Betrieb	Testrisiko für laufende Systeme	**Rules of Engagement vorab** auf Wunsch außerhalb der Geschäftszeiten
Nachhaltigkeit	Bericht abgelegt, Lücken bleiben offen	**Re-Test der behobenen Findings** wiederholbar als jährlicher Programmbaustein

Ihr Leistungsumfang im Überblick

- Scoping und Zieldefinition mit Rules of Engagement
- Externe und interne Angriffssimulation
- Web-, API- und Cloud-Anwendungstests
- Priorisierter Bericht mit CVSS-Bewertung je Finding
- Management-Zusammenfassung und technische Details
- Re-Test der behobenen Findings

> **Für Ihre Geschäftsleitung:** Auswahlsorgfalt belegbar (ISO/IEC 27001 TÜV SÜD, seit 1999, >600 Kunden) · Überwachung erfüllbar (Reporting an die Geschäftsleitung) · Leistungsumfang vertraglich klar definiert.
>
> **Ihr Part:** benannte Ansprechpartner und Dokumentenzugang – Rollen, Zuständigkeiten und Berichtswege werden gemeinsam festgelegt. Details (Leistungsbeschreibung, AVV/TOM) im Erstgespräch.

Souverän. Deutsch. Nachweisbar.

- Deutscher Anbieter – seit 1999, Sitz in München
- 100+ Security-Expertinnen und -Experten
- ISO/IEC 27001 zertifiziert (TÜV SÜD)
- Unterstützt NIS-2-, DORA- und ISO-27001-Nachweise
- DSGVO-konforme Verarbeitung – AVV (Art. 28) & TOM auf Anfrage
- Angebunden an das 24/7 Cyber Defense Center

So starten Sie mit dem Service

01
Scoping

Ziele, Umfang und Rules of Engagement werden gemeinsam festgelegt – inklusive Beratung, ob Black-, Grey- oder White-Box zu Ihrem Ziel passt.

02
Test & Exploitation

Tester kartieren die Angriffsfläche, nutzen Schwachstellen kontrolliert aus und verketten sie zu realen Angriffspfaden – ohne Betriebsrisiko.

03
Bericht & Re-Test

Sie erhalten den CVSS-priorisierten Bericht mit konkreten Maßnahmen; nach der Behebung bestätigt ein Re-Test die Wirksamkeit der Umsetzung.

Sprechen Sie mit uns, bevor es der Angreifer tut.

Vereinbaren Sie ein kostenloses 30-Minuten-Erstgespräch – Sie erfahren, wie Penetration Testing auf Ihre Organisation und Ihre Anforderungen zugeschnitten wird.

Dr. Nils Kaufmann
Chief Sales Officer

+49 89 45 24 24-100
kontakt@argos.security · www.argos.security

Mehr zur Leistung: argos.security/leistungen/penetration-testing →

Termin buchen