EXPLOIT LABS

OFFENSIVE SECURITY. REAL-WORLD RESULTS.

HYBRID PENTEST

Menschliche Expertise trifft auf skalierbare Automatisierung — für ISO 27001, NIS2 und DORA.

WER WIR SIND

Exploit Labs (XPLT) ist ein deutsches Offensive-Security-Team mit Standorten in Frankfurt (HQ), Dubai und Reykiavik.

- ENISA-Beiträge 2021–2024 (Threat Landscape WG)
- DORA TLPT 2024: unter den ersten in Deutschland abgeschlossen
- FIRST Red Teaming SIG Mitglied
- OffSec Learning & Channel Partner (DACH, MENA, GCC)
- Arbeit nach ISO 27001 / BSI IT-Grundschutz

DAS PROBLEM

Reine automatisierte Scans und rein manuelle Pentests haben blinde Flecken.

Autonome Scanner finden bekannte Schwachstellen – aber sie denken nicht wie Ihr Gegner.
Kein Kontext. Keine Kreativität. Keine Exploitation-Chains. Viele False Positives.

Rein manuelle Pentests sind tief – aber nicht skalierbar.
Momentaufnahme. Höherer Aufwand. Längere Zyklen. Schwieriger, mit der Release-Geschwindigkeit Schritt zu halten.

UNSERE LÖSUNG: HYBRID PENTEST

Unser 4-Phasen-Modell kombiniert kontinuierliche Automatisierung mit menschlicher Angreifer-Expertise.

1 DISCOVERY
Asset Discovery & Attack Surface Mapping
Technologien: Nmap, Shodan, Chaos, DNSenum, GitLeaks, Subfinder

2 AUTOMATED CONTINUOUS TESTING
Kontinuierliches Scanning & Validierung bekannter Risiken
Technologien: Nuclei, ZAP, Nikto, Trivy, SCA/SAST, Secrets Scanning

3 MANUAL DEEP-DIVE
Angreifer denken wie Ihr Gegner: TTPs, Exploitation, Lateral Movement, Privilege Escalation
Methoden: OWASP WSTG, MITRE ATT&CK, AD Attack Path, Cloud Misconfig

4 REMEDIATION & RE-TEST
Priorisierung, technische Empfehlungen & Validierung
Fix Verification & Regression Testing

3-WEGE-VERGLEICH

	MANUELLER PENTEST	AUTONOMER AI-SCANNER	HYBRID PENTEST (XPLT)
TIEFE	Sehr hoch (punktuell)	Niedrig bis mittel	✓ Sehr hoch (kontinuierlich + tief)
ABDECKUNG	Begrenzt (zeitabhängig)	Hoch (breit, aber oberflächlich)	✓ Sehr hoch (breit & tief)
KONTINUITÄT	Gering (Momentaufnahme)	Sehr hoch (24/7)	✓ Sehr hoch (kontinuierlich)
FALSE POSITIVES	Niedrig	Hoch	✓ Niedrig (validiert)
KONTEXT	Hoch (menschlich)	Niedrig	✓ Sehr hoch (menschlich + Daten)
ANGREIFER-MINDSET	Hoch	Niedrig	✓ Sehr hoch
EFFIZIENZ	Gering (Ressourcenintensiv)	Sehr hoch (skalierbar)	✓ Hoch (effizient & zielgerichtet)
ERGEBNISQUALITÄT	Hoch, aber nicht kontinuierlich	Mittel (viele False Positives)	✓ Sehr hoch (relevant & umsetzbar)

EXPLOIT LABS

COMPLIANCE-MAPPING

ISO/IEC 27001:2022 A.8.8 Technischer Schwachstellen-Check	Regelmäßige Identifikation von Schwachstellen, Bewertung der Exposition und Wirksamkeit von Maßnahmen.
NIS2 Richtlinie Art. 21 (Technische Maßnahmen)	Risikoorientierte Tests, Schwachstellenmanagement, Incident Readiness und sichere Systemkonfiguration.
DORA Verordnung Art. 24 (Operational Resilience)	TLPT-basiertes Testing, Bedrohungsleid, mit Lessons Learned und Nachweisen für Aufsichtsbehörden.

Hybrid Pentest liefert belastbare Evidenz, reduziert Risiko und unterstützt Audits und regulatorische Nachweise.

SOVEREIGNTY-MODELL

Daten bleiben in der EU
Alle Scans, Logs und Reports werden in EU-Rechenzentren verarbeitet und gespeichert.

Kein Cloud-Traffic ins Drittland
Keine Übertragung in unsichere Jurisdiktionen.

Lokale Testinfrastruktur
Dedizierte, mandantengetrennte Infrastruktur in der EU.

DSGVO-konform
Vertragliche und technische Maßnahmen nach DSGVO und BSI IT-Grundschutz.

PROOF POINTS

ENISA-Beiträge 2021–2024
Aktiver Beitrag zur ENISA Threat Landscape Working Group.

DORA TLPT 2024
Unter den ersten in Deutschland abgeschlossenem TLPT-Engagements.

Kunden aus regulierten Branchen
Banken, Zahlungsdienstleister, Energieversorger, Industrie und kritische Infrastrukturen.

Echte Angreifer-Expertise
Operator mit OffSec-Backgrounds, Red Team TIBER-EU Erfahrung. MITRE ATT&CK-aligned.

BOOK A TECHNICAL BRIEFING

Sprechen Sie mit unseren Senior Operatoren über Ihr Umfeld, Ihre Risiken und die passende Teststrategie.

xplt.com/de/hybrid-pentest >

DOWNLOAD ONE-PAGER

Erhalten Sie den vollständigen One-Pager als PDF für Ihr Team oder Ihre Unterlagen.

LEAD-FORMULAR ÖFFNEN >

xplt.com · hello@xplt.com · Exploit Labs GmbH · Schwalbacher Str. 54, 65760 Eschborn