

AI-POWERED CYBERSECURITY. SMARTER CYBER DEFENSE.

We find what attackers would, and prove it before they do.

Veiliux yields fast and reliable results with AI-powered cyber security to fortify your business's cyber defenses. One AI engine covers every attack surface at machine speed, and certified testers verify every finding before it reaches you.

3,000+

security audits in the last five years

500+

global companies have credited our team

24/7

autonomous monitoring

10+

years of innovation

ONE AI ENGINE. EVERY ATTACK SURFACE.

Web

API

Mobile

Network & cloud

SCADA / OT

Blockchain

Source code

AI & LLM systems

AI-POWERED CYBER SECURITY SERVICES

Penetration Testing

AI-assisted testing across web, mobile, API, network and cloud, verified by certified testers. Exploit-verified findings, fix-first reporting, free retest included.

Red Teaming

Goal-driven assessments that emulate real adversaries across people, process and technology. Objective-based scenarios, purple team debrief, detection gap report.

Threat Intelligence

Tracking the actors, campaigns and exposures aimed at your organisation. Dark web monitoring, actor profiling, actionable IOC feeds.

Source Code Auditing

Manual review that surfaces the flaws automated scanners miss. Line-by-line review, SAST plus manual analysis, developer-ready fixes.

Also: AI Security · Blockchain Assessment · Compliance (ISO 27001, SOC 2, PCI DSS, HIPAA, GDPR) · Digital Forensics · Incident Response · System Hardening · Cyber Resilience · Defense in Depth · Post-Quantum Cryptography · 24/7 AI-assisted SOC and CERC · Training with EC-Council and Mile2

RECOGNIZED BY INDUSTRY LEADERS

Our research has earned recognition from the world's leading technology companies for discovering and responsibly disclosing critical vulnerabilities. Founder Shahmeer Amir is ranked the world's third most accomplished bug hunter.

Facebook

Microsoft

Google

X

LinkedIn

Yahoo

Uber

Salesforce

Snapchat

Airbnb

Tesla

Apple

...and more than 500 global companies in total.

TRUSTED BY

medical brain

sehat.kahani

TPS



TECHNOLOGICA

K·MICRO

pallo

TERRA VIRTUA

BIG

Also Bayt · RepairDesk · Din Global · iClosed · Relymer · Eocean

Ten engagements. Found before attackers found them.

Healthcare, fintech, government, education, SaaS, logistics, recruitment and blockchain, across the USA, the Gulf and Asia. Clients are described by sector to protect their confidentiality.

HEALTHCARE SAAS · USA
Six apps and 130+ APIs, every fix verified
API testing and source code analysis across desktop, web, iOS and Android, then remediation verification and certification.
242 of 244 items resolved or closed

B2B SAAS · USA
AI-powered red team for an enterprise seller
App, API, network and cloud testing, threat intelligence, vulnerability policies and a SOC 2 roadmap.
89 findings · 20 ATT&CK kill chains broken

TELEMEDICINE · MONTHLY RETAINER
A standing security team for 15 months
Web, Android, source code and the external footprint, tested release after release.
38 findings · all 4 critical closed

EDUCATION · INCIDENT RESPONSE
Answers within days of a breach
Five applications tested, the likely entry point traced through cloud logs, then DevOps and cloud hardened.
23 findings · attack path reconstructed

RETAIL TECHNOLOGY SAAS
A client that came back five years later
Web, code and stress testing in 2020; a grey-box retest of eight assets in 2025 as the platform grew.
22 findings across two engagements

GLOBAL PORT OPERATOR · VIA PARTNER
Partner-delivered, half-yearly testing
Scoped, tested and reported through a UAE technology partner, to OWASP, for an enterprise end client.
14 findings · 2 critical caught early

GOVERNMENT REGULATOR
A national results platform, secured
Readiness review, application and stress testing, then a network assessment over six months.
Data-exposure path closed · stability restored

RECRUITMENT PLATFORM · MIDDLE EAST
Legacy code most auditors won't read
Line-by-line audit of a Tcl codebase plus static analysis of 42 library files.
Every flaw pinned to file and line · certified

FINTECH PAYMENTS · USA
Proof of strength, not padded findings
Android, iOS and API testing, with every attack the platform withstood documented.
7 targeted attacks resisted

BLOCKCHAIN · ERC-20 TOKEN
Smart contract audited before launch
Solidity review plus dynamic tests for reentrancy, access control and front-running.
10 of 11 attack tests passed · certified

EVERY ENGAGEMENT

Scope under NDA → **Recon** with AI-assisted scanning → **Test**, every finding exploit-verified → **Escalate** criticals the moment they are confirmed → **Report** with a fix for every issue → **Retest** and certify.

WAYS TO WORK WITH US

One-off assessment · Test, fix, verify, certify · Periodic retesting · Monthly retainer · Incident response · Multi-month red team · Channel partnership for IT firms and MSPs

Know exactly what your security testing should cost.

Build your scope in two minutes at veiliux.com. We send a detailed estimate and a proposed test plan to your inbox.