

PENETRATION TESTING AND OFFENSIVE SECURITY

See your network the way an attacker does.

We watch your environment every hour of every day. Now we'll show you exactly how an attacker would break in.

Book a scoping call

Delivered with NaviSec,
Vijilan Elite Partner.



The problem

Scanners list vulnerabilities; attackers chain them together. Compliance frameworks and cyber insurers increasingly expect independent testing. And most reports land as a PDF nobody walks you through.

Two core services



Network Penetration Test

External and Internal

Full scope, starting where attackers start: what anyone can find about you online.

- › Passive and active recon: OSINT, DNS, exposed shares and cloud storage
- › Exploitation: web attacks, password spraying, social engineering
- › Grey-box post-exploitation: lateral movement, Active Directory mapping
- › Internal testing via a lightweight virtual appliance on your VM or cloud

Includes 90-day retest



Web Application Penetration Test

Apps, portals and APIs

We learn how your app works, then how it breaks.

- › Analysis of your app's logic and intended functions
- › Exploitation methodology based on the OWASP Top 10
- › Authentication, sessions, access control, input validation, APIs, file upload
- › Unauthenticated or per user role, with optional source code review

Includes 90-day retest

Also available: vulnerability assessment, red team operations and purple team operations.

Why it's different



TTP-driven, not tool-centric

We emulate real-world attackers, not scanner output. Engineers often build custom tooling for your scenario.



Hand-crafted, QA reviewed reports

Every finding is triaged and written by the engineer, with proof-of-concept evidence, then formally QA reviewed.



Direct access to your engineer

Reach the engineer running your test by email or instant message throughout the testing window.



Critical findings escalated immediately

An extremely critical vulnerability, active breach or insider threat goes to your technical contact right away.



Clean attribution

Each assessment runs from a freshly built, dedicated cloud environment, so your SOC can answer "is this you?" with certainty.



90-day AfterGuard retest

One free retest of all findings at once, when scheduled within 90 days of report delivery.

How an engagement runs



Find. Fix. Prove. Protect.

Find it. Fix it. Prove it's fixed. Then we keep watching.

Once the retest confirms your fixes, ThreatRespond™, ThreatDefend™ or NextDefend™ keeps watching the environment you just hardened, 24/7 from our U.S.-based SOC.

When Vijilan is your SOC, test windows are coordinated with our analysts, and findings feed straight into the environment we monitor.

Vijilan Security

Aventura Onyx Tower, 1010 S Federal Hwy, Suite 1205, Hallandale Beach, FL 33009
Phone: +1 954.334.9988
Email: sales@vijilan.com
Web: vijilan.com

Three ways to buy

- Through your MSP or MSSP
- Through your VAR or distributor
- Direct from Vijilan

Book a scoping call