AI-Native Cybersecurity for Enterprises, Governments & Intelligence

01 DEFENSE. OFFENSE. INTELLIGENCE.

02 ADVERSARY EMULATION & RED TEAMING

03 AI-NATIVE SECURITY OPERATIONS

04 SOVEREIGN BY DESIGN

05 RECONNAISSANCE & OSINT

06 ATTACK PATH MAPPING

07 TECHNICAL SOVEREIGNTY



SecNinjaz Technologies LLP

sales@secninjaz.com | +91-9289962965

www.secninjaz.com

secninjaz

1

CORE OFFENSIVE SECURITY

Assess, exploit, validate, retest seven service lines under one scope

Vulnerability Assessment & Penetration Testing (VAPT)

Identify, Exploit and re-validate security risks before attackers do. Combine vulnerability scanning and penetration testing across internal and external environments safely, without disrupting operations.

- Vulnerability identification across systems and applications
- Internal and external environment assessment
- Risk prioritisation by severity and business impact
- Penetration testing that simulates real-world attacks
- Exploit validation confirming real impact
- Detailed reporting with remediation guidance

150+
VAPT assessments delivered

95%
critical issues found pre-exploitation

<72 hrs
report turnaround at close

Seven Offensive Service Lines

1. **Vulnerability Assessment (VA)** FLAGSHIP
2. **Penetration Testing (PT)** FLAGSHIP
3. **Red Teaming**
4. **Purple Teaming**
5. **Breach & Attack Simulation (BAS)**
6. **Social Engineering**



VAPT Engagement Flow

1 **Scope Definition** — boundaries agreed in writing
2 **Reconnaissance** — attack surface and entry points
3 **Vulnerability Scanning** — automated detection & filter false positive
4 **Penetration Testing** — Manual exploitation & revalidation
5 **Reporting** — risk ratings and remediation
6 **Retesting** — fixes verified, closure confirmed

ASSETS WE TEST

- Web applications and portals
- Android and iOS apps
- REST and GraphQL APIs
- Internal and external network
- Cloud infrastructure and workloads

SCOPED TO YOUR SECTOR

Government & PSU | Banking, NBFC, Insurance & Fintech | Healthcare | Telecom & Data Centers | Energy & Utilities | Transportation & Smart Cities | E-commerce & Retail | Logistics & Supply Chain | Manufacturing | Startups & MSMEs | Defence & Corporate Security

2

AI & EMERGING SECURITY

Test the model, red team the misuse, automate the SOC three service lines

HOW WE WORK

Scope and threat model agreed against your actual architecture, adversarial testing run against the live system, findings rated by exploitability and business impact, remediation guidance written for your environment, then retested.

Three AI Service Lines

1. **AI / LLM Security Testing**
   Test AI systems for prompt injection, model theft, poisoning, privacy risks and pipeline weaknesses, with PoC attacks.

2. **AI Red Teaming**
   Identify jailbreaks, safety bypasses, harmful outputs, bias and adversarial weaknesses, aligned to NIST AI RMF.

3. **AI SOC Automation**
   Automate alert triage, enrichment, response and reporting, with human approval for high-impact actions.



AI Engagement Flow

1. **Model & Objective Scoping** — models, pipelines, agents
2. **Threat Modeling** — misuse paths for your architecture
3. **Adversarial Testing** — against the live system
4. **Safety & Bias Evaluation** — varied-input robustness
5. **Risk Analysis** — exploitability and business impact
6. **Reporting & Remediation** — evidence, then retest

STANDARDS WE TEST AGAINST

- MITRE ATT&CK
- OWASP
- CVSS scoring
- NIST AI RMF
- ISO/IEC 42001:2023
- ISO/IEC 27001:2022
- Responsible-AI best practice

WHAT EVERY ENGAGEMENT SHIPS WITH

Scope agreed in writing | Testing windows fixed with your team | Proof-of-concept evidence per finding | CVSS-scored severity | Business-impact rating | Prioritized remediation guidance | Retest and closure confirmation | Audit-ready report | NDA by default

3

QUICKSCAN & WHY SECNINJAZ

Start free, then scope the engagement certified people, audit-ready delivery

Founded in 2018 and headquartered in Delhi, India. Offence and defence sit under one roof, so red team and blue team work the same engagement no coordination gaps and no handoff failures.

Start with QuickScan. Free, no signup.

A free AI-powered vulnerability assessment for websites. Enter a URL and get an instant security check findings mapped to compliance and paired with remediation guidance, before you commit to a scoped engagement.

- Known vulnerabilities and exposed services
- Misconfigurations and exposed ports
- Compliance mapping
- SSL/TLS configuration issues
- CVSS-scored findings, OWASP-aligned
- Remediation guidance per finding



Get in Touch

+91-9289991542

www.secninjaz.com

sales@secninjaz.com

SCAN FOR SERVICES

REGISTERED OFFICE

512–514 Best Business Park, Plot No.: P2, Netaji Subhash Place, Delhi 110034

FOLLOW

/company/secninjaz
@Secninjaz_tech
@secninjaztechnologies

CERTIFICATIONS & MEMBERSHIPS

CMMI Level 3 · ISO 9001:2015 · ISO 27001:2022 · ISO 27701:2025 · ISO 20000-1:2018 · ISO 42001:2023

CERTIFICATES COMPLETED

STQC

CERTIFICATES IN PROGRESS

NCSRC · DPIIT · MSME · MAKE IN INDIA · #startupindia · DSCI PROMOTING DATA PROTECTION

MEMBERS

OEM & TECHNICAL PARTNERS

emudhra Trust Delivered · sslstore · CISCO · INGRAM MICRO · Redington · NxtGen · sslstore · FACTION · HPE

One Partner.
Complete Cyber Resilience.