cyfidex

Think offensive. Secure what's next.

Expert-led VAPT and offensive security across established and emerging attack surfaces. Built around real attack paths, clear evidence, and practical next steps.

01 / EXPERT-LED OFFENSIVE SECURITY

Web & API security

Find exploitable weaknesses in your applications, authorization, and business logic.

Web applications · REST & GraphQL APIs · Authentication & authorization · Business logic

Mobile application security

Assess the mobile experience from on-device storage to connected backend services.

iOS · Android · Mobile backends · On-device storage

Network & infrastructure

Uncover attack paths, privilege escalation, and lateral movement across your environment.

Networks · Infrastructure · Internal environments · Identity environments

Cloud & attack surface

Understand external exposure and how cloud permissions and weaknesses can combine.

Cloud infrastructure · External attack surfaces · Cloud identities · Public-facing assets

Red teaming

Challenge your defenses with controlled, objective-led adversary simulations.

Adversary simulation · Detection & response · Internal environments · End-to-end attack paths

AI & agentic security

Test the trust boundaries between models, context, agents, tools, and connected services.

AI & LLM applications · AI agents · Agentic systems · MCP servers · Tool integrations

Authorized testing. Agreed scope. Clear communication.

A clear path from exposure to action.

Cyfidex brings an adversarial mindset and a technology-building perspective to security testing. Our current commercial focus is expert VAPT and offensive security services.

02 / YOUR ENTIRE ATTACK SURFACE

Traditional environments

Web applications · APIs · Mobile applications
Networks · Cloud infrastructure · Infrastructure
External attack surfaces · Internal environments
Red teaming

Emerging attack surfaces

AI security · LLM security · AI applications
AI agents · Agentic systems
MCP · MCP servers · Tool integrations
Emerging technology architectures

03 / YOUR ENGAGEMENT

01 Scope together

Agree on assets, objectives, testing windows, and rules of engagement.

02 Test like an adversary

Investigate exploitable weaknesses and the attack paths that matter.

03 Make risk clear

Receive reproducible evidence and prioritized remediation guidance.

04 Close the loop

Review findings with your team and agree on retesting arrangements.

Reproducible findings. Risk context. Practical remediation. Technical debriefs. Agreed retesting.

Talk to an expert

Discuss your assets, scope, and timeline.