

CyberProof Penetration Testing

Validate risk before attackers exploit it.

Verification

NOT JUST
ASSURANCE

50+ Experts

ACROSS DIVERSE
REGIONS

OWASP · CREST

SUB-COMMITTEE
MEMBERS

CTEM-powered

THREAT-LED
PRIORITIZATION

Modern enterprise environments change constantly. Cloud services, SaaS platforms, identities, APIs, mobile applications, OT and IoT assets, and third-party integrations expand the attack surface faster than many security teams can validate it. Traditional penetration testing often confirms that a test was performed, but it may not show whether critical systems will behave securely under real-world pressure.

CyberProof's **Penetration Testing** service helps organizations **proactively identify, validate, and prioritize** security weaknesses before they can be exploited. Our ethical hackers safely simulate the tactics, techniques, and procedures used by malicious actors to uncover **vulnerabilities, configuration weaknesses, control gaps, and staff awareness issues** across applications, networks, infrastructure, mobile environments, IoT, OT, and red team scenarios.

WHAT CYBERPROOF DELIVERS

Clear outcomes for every audience.

After each assessment, CyberProof delivers a **comprehensive report** detailing the tests performed, vulnerabilities identified, business risk, and recommended mitigation steps. The report includes an **executive summary for leadership**, a **step-by-step technical breakdown** for security teams, and actionable remediation guidance across code, configuration, people, and process.

For CyberProof **MDR/MXDR customers**, penetration testing insights can also inform **detection improvements**, helping security teams strengthen coverage based on validated findings.

TESTING MODELS

What CyberProof tests – aligned to your objectives, risk profile, and environment.

01

**Infrastructure
penetration
testing**

02

**Web & mobile
application
assessments**

03

**Social
engineering &
phishing**

04

**Wireless & Wi-Fi
assessments**

05

**Red team
simulation
testing**

CTEM POWERED

Penetration testing is enhanced by **CDC Reveal360 Continuous Threat Exposure Management** (powered by Interpres) – keeping an up-to-date view of exposed vulnerabilities so testing focuses where it matters most: **crown-jewel assets, high-risk identities**, exposed applications, and critical business processes.

01 Built for adversarial reality – verification, not just assurance

THE CYBERPROOF VIEW

Assurance confirms activity. Verification proves that systems behave as intended under stress, error conditions, and realistic attack paths – uncovering how access, trust, and exposure connect across the enterprise.

Our methodology combines **structured manual analysis**, contextual understanding, and engineering discipline to move beyond checklist testing. CyberProof’s ethical hackers safely simulate the tactics, techniques, and procedures used by real adversaries to surface vulnerabilities, configuration weaknesses, control gaps, and staff awareness issues.

CyberProof’s testers bring global experience across **telecom, finance, banking, and healthcare**. The team includes **OWASP and CREST Penetration Testing sub-committee members**, CVE authors, and more than **50 experts** supporting diverse regions.

02 Customer outcomes

Penetration testing engagements typically deliver:

01

Mapped attack surface weaknesses

A clearer view of how access, trust, and exposure connect across the enterprise.

02

Hardened Active Directory

Improved configuration that reduces lateral movement and privilege escalation risk.

03

Discovery of unpatched assets

Surfacing systems, services, and applications that fall outside vulnerability management.

04

Stronger training priorities

End-user awareness focus areas grounded in real phishing and social engineering results.

05

Smarter security spend

Improved investment decisions and reduced reliance on ineffective tools.

06

Regulatory mandate support

Evidence and documentation that helps meet compliance and audit requirements.

WHY CYBERPROOF

Global expertise, threat-led focus.

CyberProof’s testers bring deep experience across telecom, finance, banking, and healthcare, with **OWASP and CREST sub-committee members, CVE authors, and 50+ experts** supporting diverse regions.

We turn one-off testing into a **focused offensive security program** – combining verification methodology, CTEM-driven prioritization, and clear reporting to improve resilience and reduce business risk.

NEXT STEPS

Start with a Pen Testing strategy workshop.

Review your current risk landscape, critical business processes, crown-jewel assets, testing cadence, and likely attack paths. CyberProof practitioners will help identify gaps across people, process, and technology, then define a prioritized action plan for the testing methods that best fit your environment.

[SCHEDULE YOUR WORKSHOP →](#)