

Security Audit & Black Box Pentesting

Don't wait for an attacker to discover your weaknesses.

Most organizations only discover they are vulnerable after sensitive data appears on the Dark Web. A single undetected flaw — a misconfigured server, an unmonitored access point — can expose client records, financial data, and business secrets. We systematically identify and eliminate these risks, giving your organization a clear, honest picture of its real security posture and a concrete path to improve it.

83%**OF BREACHES**

exploit known, unpatched vulnerabilities that could have been fixed

287**DAYS AVG**

to detect an active intrusion without active monitoring in place

\$4.9M**AVG BREACH COST**

global average total cost of a data breach in 2024 (IBM Report)

100%**FIND RATE**

of our audits reveal at least one critical or high-severity finding

Our Testing Services

1

Cybersecurity Audit (AS4)

General and sector-specific audits giving leadership a frank, readable assessment of current protection level — ranked findings with a prioritized remediation roadmap.

3

Whitebox Code Audit

In-depth source code review to find logical vulnerabilities, insecure data handling, and hidden backdoors that automated scanning tools simply cannot detect.

5

Public Asset Monitoring

Continuous scanning of domains, subdomains, and mail servers for SSL/TLS integrity, DNS configuration security, and accidental external data exposure.

2

Black Box Pentesting

We simulate a real external attacker with zero insider knowledge — probing web apps, APIs, and login portals exactly as a threat actor operating today would.

4

Infrastructure Pentesting

Network and Active Directory penetration testing to verify segmentation — ensuring no attacker can move laterally or escalate privileges across your environment.

6

OWASP Top 10 Coverage

Full coverage of SQL Injection, XSS, Remote Code Execution, File Inclusion, Command Injection, and DNS poisoning — techniques actively used in current campaigns.

Why It Matters

Known Flaws, Real Risk

Most breaches exploit patchable vulnerabilities. An untested system is an assumed-safe system — and that assumption is consistently and expensively proven wrong.

Detection Takes Months

Without active testing an attacker can operate inside your environment for nearly a year. Every day of dwell time increases the scope and cost of the damage.

Compliance Requires It

NIS2, GDPR, and sector frameworks increasingly mandate regular penetration testing. A documented audit history is your proof of due diligence to regulators and clients.

What You Gain

A

Clear Risk Picture

A prioritized map of every weakness written in plain language your board can read. No jargon — just clear risk and clear action for your team.

B

Stronger Protection

We close the gaps we find and build a resilient foundation so the same weaknesses cannot return and future threats become significantly harder to exploit.

C

Business Confidence

Pass partner due diligence, win enterprise clients, and satisfy regulatory requirements with documented proof your security posture is taken seriously.

"

We identified 14 exploitable vulnerabilities in 72 hours — three of which would have allowed full database extraction. The report paid for itself before we even started remediation.

— CTO, logistics group — Security Audit client

Ready to discover your vulnerabilities? Schedule a free consultation — no commitment required. secureintel.ro