Partners in defense,
experts in offense

Kaspersky Penetration Testing

kaspersky bring on the future

Offensive security experts

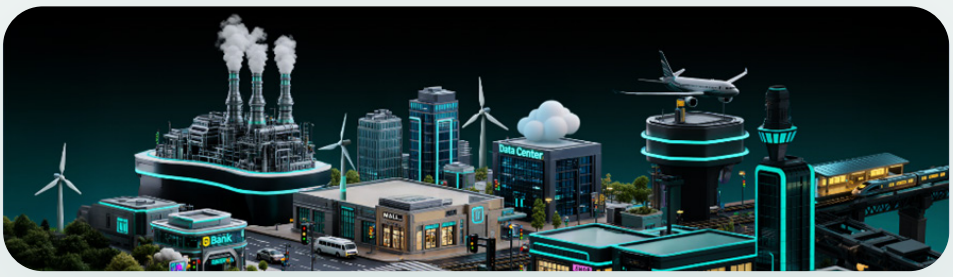
Leveraging our proven approach grounded in deep expertise and industry standards, our team of experts in practical cybersecurity simulates real-world attack techniques to deliver a bespoke assessment — from complex multi-network infrastructures to individual solutions.

What is penetration testing

This service involves proactive identification and exploration of attack vectors targeting your critical assets. By simulating real-world attacker behavior and applying relevant tactics, techniques, and procedures (TTPs), our team demonstrates the potential impact on key business processes — no matter the complexity of your infrastructure — all within a controlled and secure environment.

How it helps:

- Minimize attack surface, reduce vulnerabilities and focus on preventing exploitable security flaws that could lead to significant damage
- Analyze the potential impact attackers could have on critical business processes
- Communicate technical risks in business terms to highlight the importance of security investments



Kaspersky Penetration Testing

Security foundation for business

Key advantages:

Industry insights

Our team provides tailored insights for your unique challenges, backed by hands-on experience in industries

- Power and utilities
- Manufacturing
- Oil and gas
- Transportation
- Banking
- IT

Collaborative intelligence

We collaborate with Kaspersky's Incident Response and Threat Intelligence teams to ensure access to the latest cyber threat data and insights.

Proven research leadership

Our experts regularly publish researches and discovered vulnerabilities (CVEs) in major companies such as Oracle, Google, Apple, and Microsoft.

Attack surface | Critical assets | Business functions | IT risks

External Infrastructure

External penetration testing (including attack development phase) helps analyze risks related to assets and information systems exposed to the Internet. Kaspersky experts proactively identify vulnerabilities by applying real-world attack techniques, enabling you to address security weaknesses before attackers can exploit them to access critical business processes.

Internal Infrastructure

Internal penetration testing provides a clear understanding of the actual risks associated with attacks aimed at gaining access to sensitive data and critical corporate services. During this stage experts demonstrate how attackers can escalate privileges, compromise assets, and employ lateral movement to bypass security controls.

Holistic adversarial testing: the entire attack surface

Key features

Kaspersky Penetration Testing

Identifying real attack vectors and understanding critical security flaws require more than simply running a vulnerability scan of your environment and manually verify the results. A holistic strategy is essential to gain a deep understanding of all industry-specific threats. Kaspersky Penetration Testing utilizes a proven methodology built on years of expertise and industry best practices.

Not a vulnerability scan

Penetration testing conducted by humans, including manual verification of vulnerabilities and demonstration of attack vectors

Real world TTPs

Latest attack TTPs to simulate real-world attacker behavior and validate your security defenses

Do not stop on the first breach

Demonstration of all possible attack vectors

Push the envelope

We go the extra mile to deliver maximum value — proactively uncovering non-obvious attack paths

Overt exercise

All efforts put into attack surface exploration, rather than covert actions

Legal and ethical boundaries

Simulated attacker actions with strictly adherence with legal and ethical standards, ensuring no real harm is done

Comprehensive approach

- External Testing
- Attack Development
- Internal Testing
- Reporting & Tailored Recommendations

Deliverables

- Executive report
- Technical report

Identified vulnerabilities & detailed attack vectors

Lists critical, high, and medium-risk vulnerabilities with PoC evidence and clear step-by-step exploitation paths show how an attacker could breach systems

Real-time attack perspective

Up-to-date security insights from an attacker's viewpoint at the time of testing

Practical recommendations

Provides practical recommendations for: Patching or configuration fixes or implementing compensating controls if immediate remediation isn't possible

Traceability for blue team follow-up

Key IOCs & IOAs are logged & timestamped for proactive threat hunting

43%

High-severity incidents are human-driven attacks according to Kaspersky MDR report; automated tools often miss adversary tradecraft, while security assessments powered by experts reveal critical attack paths for proactive defense

Kaspersky Penetration Testing

Learn more

www.kaspersky.com

#kaspersky
#bringonthefuture