Partners in defense,
experts in offense

Kaspersky Security Assessment

kaspersky cybersecurity
true to business

Practical cybersecurity exercises

Kaspersky Security Assessment

Our experts in practical cybersecurity simulate adversary behavior, showing how real attackers could exploit your applications, networks, and devices – providing clear visibility into your true exposure. We don't just list weaknesses; we prove impact and show exactly what an adversary could achieve.

Security assessment portfolio

Kaspersky offers a range of Security Assessment Services that can be tailored or combined to match the attacker models most relevant to each industry.

Kaspersky Penetration Testing

Maps real attack paths – from external perimeter to critical internal assets – by chaining exploitable flaws into real vectors.

Kaspersky Red Teaming

Simulates goal-driven, scenario-based adversary attacks to validate detection and response capabilities and strengthen resilience against real threats.

Kaspersky Application Security Assessment

Uncovers vulnerabilities and business logic flaws through in-depth technical testing and analysis of application workflows.

Kaspersky Security Assessment Services

Kaspersky Appliance Security Assessment

Provides in-depth analysis of hardware, software, and wired/wireless interfaces to identify weaknesses, assess protection mechanisms and reduce threats in IoT and embedded devices.

Kaspersky ICS Security Assessment

Assesses the attack surface and evaluates the security of OT environment from Level 4 to Level 0 of the Purdue Model, including network equipment, DCS, SCADA, PLC, IED, and mission-critical systems to identify cyberthreats.

Kaspersky ATM Security Assessment

Comprehensive analysis of ATMs and POS devices to reveal attack surface and uncover exploitable flaws, showing how attackers could steal funds, capture card data, or disrupt services.

Offensive expertise across industries

Our experts apply hands-on offensive security expertise to reveal vulnerabilities and threat patterns unique to each business. Beyond the services listed here, we can assess any environment with computer systems and networks – adapting to your objectives and attacker models to demonstrate real attacker capabilities and hidden risks.

Manufacturing & industrial automation

Identify and validate attack vectors across OT networks, DCS, CNC machinery and other cell/area zone devices to help CISOs prioritize remediation and strengthen the security of production and supply-chain operations.

Building & smart facilities

Identify and remediate vulnerabilities in building automation systems, BMS controllers, HVAC, elevators, access control and fire and gas systems, helping CISOs prevent operational disruptions, unauthorized access, and safety incidents.

Energy & utilities infrastructure

Identify and remediate vulnerabilities across power plants and wind turbines, including grid management, substation controls, and remote monitoring systems, preventing operational disruptions, sabotage, and safety incidents.

Banking & payment systems

Identify exploitable flaws across ATMs, PoS infrastructure, core banking, digital channels and interbank payment rails, addressing risks from sophisticated fraud schemes, targeted intrusions to safeguard sensitive financial data and maintain transaction integrity.

Retail & supply chain

Detect and mitigate flaws in e-commerce platforms, WMS, PDT/barcode scanners, AGV robots, automated conveyor and robotic picking systems, protecting customer data, ensuring supply chain continuity, and preventing fraud or operational downtime.

Transportation & automotive

Expose weaknesses in ground infrastructure, onboard telematics, V2X communications and transportation control systems to strengthen operational continuity and protect passenger and cargo safety.

Approach

Our team applies real-world attack techniques with expert guidance to uncover non-obvious vulnerabilities, test defenses beyond automated scans, and provide actionable insights tailored to each organization's threat environment – ethically and safely.

Real world TTPs to simulate attacker behavior and validate your security defenses

Expert-driven deep assessments beyond automated scans

Deliver more than just a list of discovered vulnerabilities

Experts selected per project by domain, threat, and scope

Legal and ethical boundaries, ensuring no real harm is done

Go the extra mile proactively uncovering nonobvious attack paths

Offensive security experts

Industry insights

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

Collaborative intelligence

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

Proven research leadership

Our experts regularly publish research and discovered vulnerabilities (CVEs).

Deliverables

Whichever service you choose, we don't just reveal what we find – we explain how we discovered it. By sharing our expertise, we enable your team to build a sustainable, adaptable methodology that evolves with the threat landscape, rather than delivering a one-time fix.

Kaspersky Security Assessment

Contact us

Powered by Security Services

www.kaspersky.com

#kaspersky
#truetobusiness