Kaspersky Enterprise Cybersecurity

Kaspersky Security Assessment Services

www.kaspersky.com
#truecybersecurity

Kaspersky Security Assessment Services

Security Assessment Services from Kaspersky Lab are the services of our in-house experts, many of them global authorities in their own right, whose knowledge and experience is fundamental to our reputation as world leaders in security intelligence.

Because no two IT infrastructures are exactly the same, and because the most powerful cyberthreats are tailor-made to exploit the specific vulnerabilities of the individual organization, our expert services are also tailor-made. The services described on the following pages form a part of our professional toolkit – some or all of these services, in part or in full, may be applied as we work with you.

Our objective, above all, is to work with you, one on one, as your expert advisors, helping to evaluate your risk, harden your security and mitigate against future threats.

Security Assessment Services include:

- Penetration testing
- Application security Assessment
- ATM/POS Security Assessment
- Telecommunication Networks Security Assessment

Kaspersky Cybersecurity Services

- **Kaspersky Threat Intelligence Services**
- **Kaspersky Threat Hunting Services**
- **Kaspersky Security Trainings**
- **Kaspersky Incident Response Services**
- **Kaspersky Security Assessment Services**

  Penetration Testing
  Application Security Assessment
  ATM/POS Security Assessment
  Telecommunication Networks Security Assessment

Penetration Testing

Ensuring that your IT infrastructure is fully secured against potential cyberattack is an ongoing challenge for any organization, but even more so for large enterprises with perhaps thousands of employees, hundreds of information systems, and multiple locations worldwide.

Penetration testing is a practical demonstration of possible attack scenarios where a malicious actor may attempt to bypass security controls in your corporate network to obtain high privileges in important systems.

Kaspersky Lab's Penetration Testing gives you a greater understanding of security flaws in your infrastructure, revealing vulnerabilities, analyzing the possible consequences of different forms of attack, evaluating the effectiveness of your current security measures and suggesting remedial actions and improvements.

Penetration Testing from Kaspersky Lab helps you and your organization to:

- **Identify the weakest points in your network,** so you can make fully informed decisions about where best to focus your attention and budget in order to mitigate future risk.
- **Avoid financial, operational and reputational losses caused by cyberattacks** by preventing these attacks from ever happening through proactively detecting and fixing vulnerabilities.
- **Comply with government, industry or internal corporate standards** that require this form of security assessment (for example Payment Card Industry Data Security Standard (PCI DSS)).

Penetration testing results

The Service is designed to reveal security shortcomings which could be exploited to gain unauthorized access to critical network components. These could include:

- Vulnerable network architecture, insufficient network protection
- Vulnerabilities leading to network traffic interception and redirection
- Insufficient authentication and authorization in different services
- Weak user credentials
- Configuration flaws, including excessive user privileges
- Vulnerabilities caused by errors in application code (code injections, path traversal, client-side vulnerabilities, etc.)
- Vulnerabilities caused by usage of outdated hardware and software versions without latest security updates
- Information disclosure

Results are given in a final report including detailed technical information on the testing process, results, vulnerabilities revealed and recommendations for remediation, as well as an executive summary outlining test results and illustrating attack vectors. Videos and presentations for your technical team or top management can also be provided if required.

Service scope and options

Depending on your needs and your IT infrastructure, you may choose to employ any or all of these Services:

- **External penetration testing:** Security assessment conducted through the Internet by an 'attacker' with no preliminary knowledge of your system.

- **Internal penetration testing:** Scenarios based on an internal attacker, such as a visitor with only physical access to your offices or a contractor with limited systems access.

- **Social engineering testing:** An assessment of security awareness among your personnel by emulating social engineering attacks, such as phishing, pseudo-malicious links in emails, suspicious attachments, etc.

- **Wireless networks security assessment:** Our experts will visit your site and analyze WiFi security controls.

You can include any part of your IT infrastructure into the scope of penetration testing, but we strongly recommend you consider the whole network or its largest segments, as test results are always more worthwhile when our experts are working under the same conditions as a potential intruder.

About Kaspersky Lab's approach to penetration testing

While penetration testing emulates genuine hacker attacks, these tests are tightly controlled; performed by Kaspersky Lab security experts with full regard to your systems' confidentiality, integrity and availability, and in strict adherence to international standards and best practices including:

- Penetration Testing Execution Standard (PTES)
- NIST Special Publications 800-115 Technical Guide to Information Security Testing and Assessment
- Open Source Security Testing Methodology Manual (OSSTMM)
- Information Systems Security Assessment Framework (ISSAF)
- Web Application Security Consortium (WASC) Threat Classification
- Open Web Application Security Project (OWASP) Testing Guide
- Common Vulnerability Scoring System (CVSS)

Project team members are experienced professionals with a deep, current practical knowledge of this field, acknowledged as security advisors by industry leaders including Oracle, Google, Apple, Microsoft, Facebook, PayPal, Siemens and SAP.

Delivery options

Depending on the type of security assessment service, your systems specifics and working practices, security assessment services can be provided remotely or onsite. Most services can be performed remotely, and internal penetration testing can even be performed through VPN access, while some services (like wireless networks security assessment) require an onsite presence.

Application Security Assessment

Whether you develop corporate applications internally, or purchase them from third parties, you'll know that a single coding error can create a vulnerability exposing you to attacks resulting in considerable financial or reputational damage. New vulnerabilities can also be generated during an application's lifecycle, through software updates or insecure component configuration, or can arise through new attack methods.

Kaspersky Lab's Application Security Assessment uncover vulnerabilities in applications of any kind, from large cloud-based solutions, ERP systems, online banking and other specific business applications, to embedded and mobile applications on different platforms (iOS, Android and others).

Combining practical knowledge and experience with international best practices, our experts detect security flaws which could expose your organization to threats including:

- Syphoning off confidential data
- Infiltrating and modifying data and systems
- Initiating denial of service attacks
- Undertaking fraudulent activities

Following our recommendations, vulnerabilities revealed in applications can be fixed, and such attacks prevented.

Service benefits

Kaspersky Lab Application Security Assessment Services help application owners and developers to:

- **Avoid financial, operational and reputational loss**, by proactively detecting and fixing the vulnerabilities used in attacks against applications

- **Save remediation costs** by tracking down vulnerabilities in applications still in development and test, before they reach the user environment where fixing them may involve considerable disruption and expense.

- **Support a secure software development lifecycle** (S-SDLC) committed to creating and maintaining secure applications.

- **Comply with government, industry or internal corporate standards** covering application security, such as PCI DSS or HIPAA

Service scope and options

Applications assessed can include official web sites and business applications, standard or cloud based, including embedded and mobile applications.

The services are tailored to your needs and application specifics, and may involve:

- **Black-box testing** – emulating an external attacker

- **Grey-box testing** – emulating legitimate users with a range of profiles

- **White-box testing** – analysis with full access to the application, including source codes; this approach is the most effective in terms of revealing numbers of vulnerabilities

- **Application firewall effectiveness assessment** – applications are tested with and without firewall protection enabled, to find vulnerabilities and verify whether potential exploits are blocked

About Kaspersky Lab’s Approach To Application Security Assessment

Security assessments of applications are performed by Kaspersky Lab security experts both manually and through applying automated tools, with full regard to your systems’ confidentiality, integrity and availability and in strict adherence to international standards and best practices, such as:

- Web Application Security Consortium (WASC) Threat Classification
- Open Web Application Security Project (OWASP) Testing Guide
- OWASP Mobile Security Testing Guide
- Other standards, depending on your organization’s business and location

Results

Vulnerabilities which may be identified by Kaspersky Lab Application Security Assessment services include:

- Flaws in authentication and authorization, including multi-factor authentication
- Code injection (SQL Injection, OS Commanding, etc.)
- Logical vulnerabilities leading to fraud
- Client-side vulnerabilities (Cross-Site Scripting, Cross-Site Request Forgery, etc.)
- Use of weak cryptography
- Vulnerabilities in client-server communications
- Insecure data storage or transferring, for instance lack of PAN masking in payment systems
- Configuration flaws, including ones leading to session attacks
- Sensitive information disclosure
- Other web application vulnerabilities leading to the threats listed in WASC Threat Classification v2.0 and the OWASP Top Ten.

Results are given in a final report including detailed technical information on the assessment processes, results, vulnerabilities revealed and recommendations for remediation, together with an executive summary outlining management implications. Videos and presentations for your technical team or top management can also be provided if required.

Project team members are experienced professionals with a deep, current practical knowledge of the field, including different platforms, programming languages, frameworks, vulnerabilities and attack methods. They speak at leading international conferences, and provide security advisory services to major vendors of applications and cloud services, including Oracle, Google, Apple, Facebook and PayPal.

Delivery options

Depending on a type of security assessment service, specifics of systems in the scope, and your requirements to work conditions, security assessment services can be provided remotely or onsite. Most of these services can be performed remotely.

ATM/POS Security Assessment

ATMs and POS devices are no longer vulnerable only to physical attacks like ATM burglary or card skimming. As protection measures applied by banks and ATM/POS vendors evolve, so attacks against these devices also shift up a gear, becoming ever more sophisticated. Hackers are exploiting vulnerabilities in ATM/POS infrastructure architecture and applications, and are creating malware specifically tailored to ATM/POS. ATM/POS Security Assessment services from Kaspersky Lab help you to recognize the security flaws in your ATM/POS devices, and to mitigate the risk of being compromised.

ATM/POS Security Assessment is comprehensive analysis of your ATMs and/or POS devices, designed to identify vulnerabilities that can be used by attackers for activities like unauthorized cash withdrawal, performing unauthorized transactions, obtaining your clients' payment card data, or initiating denial of service. This service will uncover any vulnerabilities in your ATM/POS infrastructure that are exploitable by different forms of attack, outline the possible consequences of exploitation, evaluate the effectiveness of your existing security measures, and help you plan further actions to fix detected flaws and improve your security.

Service benefits

ATM/POS Security Assessment by Kaspersky Lab helps vendors and financial organizations to:

- **Understand the vulnerabilities** in their ATM/POS devices and improve your corresponding security processes

- **Avoid the financial, operational and reputational losses** that can result from an attack, through proactively detecting and fixing the vulnerabilities which attackers could exploit.

- **Comply with government, industry or internal corporate standards**, which stipulate the carrying out of security assessments, e.g. PCI DSS (Payment Card Industry Data Security Standard).

Service scope

The service includes comprehensive ATM/POS analysis, including fuzzing and attack demonstrations in a test environment. This can be provided on a single ATM/POS device or on a network of devices. We recommend you to choose for assessment the type of ATMs/POS device in most common use within your organization, or those that are most critical (which have, for instance, already suffered from incidents) in their typical configurations.

ATM/POS Security Assessment Results

The ATM/POS Security Assessment service may be expected to identify a range of vulnerabilities, including:

- Vulnerabilities in network architecture and insufficient network protection.
- Vulnerabilities which enable an attacker to escape kiosk-mode and obtain unauthorized access to the OS.
- Vulnerabilities in third-party security software, allowing potential attackers to bypass security controls.
- Insufficient input and output device protection (card reader, dispenser unit, etc.) including vulnerabilities in device communications, which can allow the interception and modification of transferred data.
- Vulnerabilities caused by errors in application code or resulting from using outdated hardware and software versions (buffer overflows, code injections, etc.)
- Information disclosure.

Once the assessment is concluded, you will receive a report containing both detailed technical information on the testing process, results, vulnerabilities and recommendations, and a straightforward executive summary outlining our conclusions based on the testing results and illustrating the various attack vectors. Additionally, videos of attack demonstrations and presentations for your technical team or top management can be provided if required.

Kaspersky Lab's Approach To ATM/POS Security Assessment

During analysis, our experts will not just seek out and identify configuration flaws and vulnerabilities in obsolete software versions, but will deeply analyze the logic behind the processes performed by your ATMs/POS devices, undertaking security research aimed at identifying any new (0-day) vulnerabilities at component level. If we uncover vulnerabilities which could profit an attacker (resulting, for example, in unauthorized cash withdrawal), our experts can provide demonstrations of possible attack scenarios using specially crafted automation tools or devices.

Though an ATM/POS Security Assessment involves emulating the attack behavior of a genuine hacker in order to practically assess the effectiveness of your defenses, it is entirely safe and non-invasive. The service is performed by experienced Kaspersky Lab security experts who will pay particular attention to the confidentiality, integrity and availability of your systems, in strict adherence with international law and best practices. If we discover a new vulnerability in a customer ATM/POS, we are committed to following a responsible disclosure policy, notifying the vendor and providing consultative help to prepare a fix.

Kaspersky Lab provides ATM/POS Security Assessments in accordance with the following international standards and best practices:

- Payment Card Industry standards
  - Data Security Standard
  - Payment Application Data Security Standard
  - PIN Transaction Security
- Open Source Security Testing Methodology Manual (OSSTMM)
- Information Systems Security Assessment Framework (ISSAF)
- Common Vulnerability Scoring System (CVSS)
- Other standards applicable to specific business models and geographical locations, as required.

Project team members are professionals highly experienced in practical security, who have a deep knowledge in the field and are constantly improving their skills; they regularly provide security consultancy to ATM/POS vendors and present the results of our ATM/POS security researches at leading information security conferences (like Black Hat).

Telecommunication Networks Security Assessment

Services Overview

IT infrastructure of a telecommunication company comprises a number of interconnected networks based on various functions and technologies. These typically include a corporate network including management elements, a core radio network (GSM/UMTS/LTE), providing broadband Internet Access to subscribers, dedicated high-speed trunk channels, hosting and cloud services. Each part of this infrastructure is critical to the business, and should be well protected from hacker attacks if financial, operational and reputational risk is to be minimized. Kaspersky Lab's services for telecommunication networks allow you reduce these risks by recognizing the vulnerabilities in your systems and either removing them or remediating their effects through introducing controls.

Kaspersky Lab offers the following security assessment services for telecommunication networks:

- IT Infrastructure Penetration Testing
- IT Infrastructure Configuration Security Assessment
- Security Assessment for GSM/UMTS/LTE Networks
- Application Security Assessment (for applications providing various services: IP-TV, client self-service portals etc.)

- VoIP Security Assessment
- Telecommunications Equipment Security Assessment

Services Outcome

As a result of each security assessment, you will receive both technical and high-level views of security flaws in your telecommunication networks, as well as conclusions on the effectiveness of your security controls. These results can be used to enhance the security of the network, and this mitigate the financial, operational and reputational risks associated with information security threats.

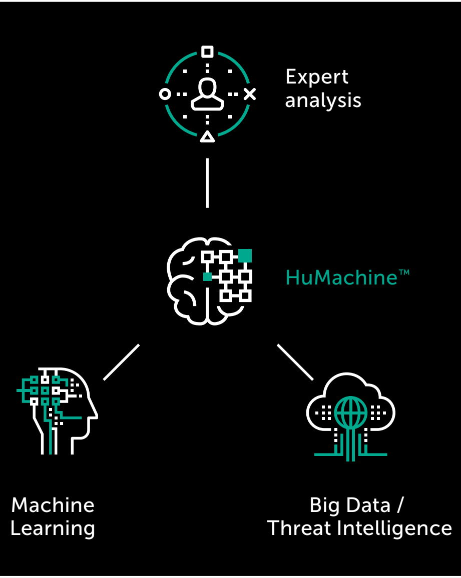
The report will contain the following information:

- High-level conclusions on the current security levels of your telecommunication networks
- Descriptions of the service methodology and process.
- Detailed descriptions of detected vulnerabilities, including the severity level, exploitation complexity, possible impact on the vulnerable system, and evidence of the vulnerability existence (where possible).
- Recommendations on vulnerability elimination, including changes in configuration, updates, changing source codes, or implementing compensatory controls where elimination of the vulnerability is impossible

Kaspersky Lab
Enterprise Cybersecurity: **www.kaspersky.com/enterprise**
Cyber Threats News: **www.securelist.com**
IT Security News: **business.kaspersky.com/**

#truecybersecurity
#HuMachine

www.kaspersky.com


Expert
analysis
HuMachine™
Machine
Learning
Big Data /
Threat Intelligence