Kaspersky Security Assessment

kaspersky

Kaspersky Security Assessment

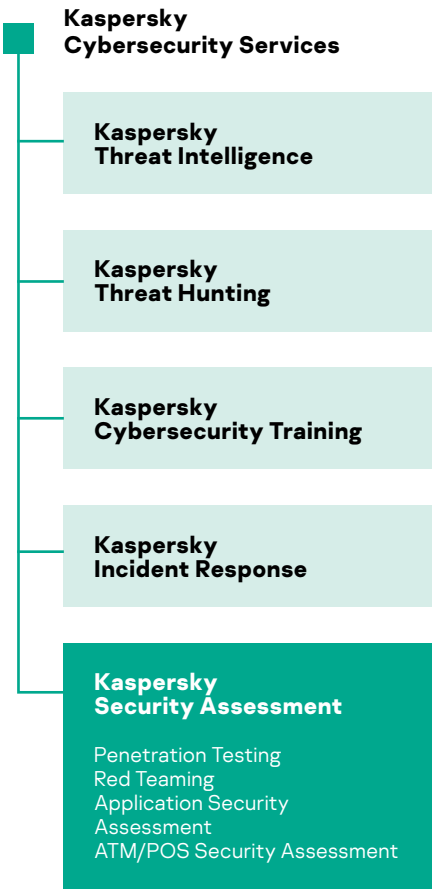
Security Assessment Services from Kaspersky are the services of our in-house experts, many of them global authorities in their own right, whose knowledge and experience is fundamental to our reputation as world leaders in security intelligence.

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.

Kaspersky Security Assessment Services include:

- Penetration Testing
- Red Teaming
- Application Security Assessment
- ATM/POS 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 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 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 cyber-attacks** 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.

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.

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's approach to penetration testing

While penetration testing emulates genuine hacker attacks, these tests are tightly controlled; performed by Kaspersky 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.

Red Teaming

The service includes the following:

- **Threat Intelligence.** The service starts with a discussion of the customer's known threats and Blue Team's experience. The aim is to identify highly critical business assets and understand how project deliverables can be tailored towards TTPs used by the company's defense. However, during these discussions, Kaspersky will not request any information about the target resources, as the Red Team will also conduct independent information gathering activities like real adversaries would do. The information gathering phase will include both analysis of publically available information (open-source intelligence), and analysis of data available in underground communities.
- **Adversary Simulation.** This stage starts with preparation of attack scenarios and tools based on the results of the Threat Intelligence stage. Preparation may include deep research into the systems used in the customer's environment to reveal new vulnerabilities, developing custom tools aimed at bypassing the customer's security systems, or readying spear-phishing attacks. When the preparation is complete, Kaspersky will perform the active phase of Adversary Simulation. These tests may include the following:

  – Passive information gathering
  – Active information gathering (network discovery), including port scanning, identifying available services and manual requests to certain services (DNS, mail),
  – External vulnerability scanning, and analyzing
  – Web application security (using both automated and manual approaches) to identify the following types of vulnerabilities:

- Code injection (SQL Injection, OS Commanding, etc.)
- Client-side vulnerabilities (Cross-Site Scripting, Cross-Site Request Forgery, etc.)
- Flaws in authentication and authorization
- Insecure data storage
- Other web application vulnerabilities leading to the threats listed in WASC Threat Classification v2.0 and OWASP Top Ten

– Manual vulnerability analysis, including identification of resources without authentication, important publically available information, insufficient access control
– Guessing credentials
– Social engineering testing
– Exploitation of one or more of the vulnerabilities found and privilege escalation (if possible)
– Develop an attack using the obtained privileges and techniques listed above until the Service Provider can access the LAN or important network resources (e.g. Active Directory domain controller, business systems, DBMSes, etc.) or until all attack methods available during testing have been exhausted.

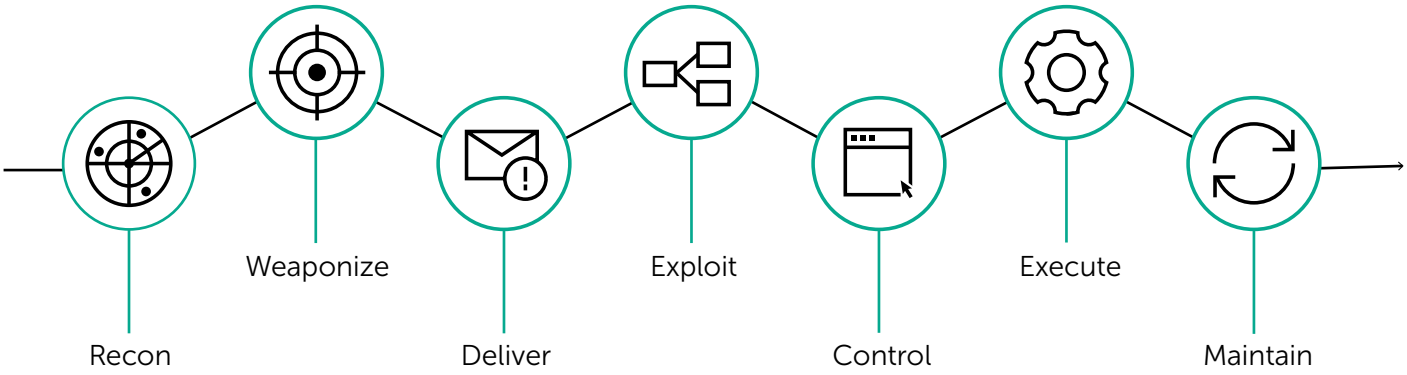


Figure 1:
Adversary simulation

The above tests are carried out according to the prepared customer-specific scenarios, using special techniques to evade detection from the Blue Team. Once the Red Team has accomplished all its objectives, activities that trigger incident detection and response are carried out to ensure Blue Team involvement in the exercise.

- **Report Preparation.** During this stage, Kaspersky will analyze the Adversary Simulation results, prepare a report with detailed description of the attacks (including timestamps and indicators of compromise) and recommendations.

- **Testing Results Overview.** A post-assessment workshop with the company's Blue Team can be arranged to discuss the project results, reasons for anything not detected or prevented, and possible further defense improvements.

Approach and Methodology

Red Teaming has much in common with a real hacker attack and makes it possible to assess the effectiveness of the protection measuresin practice. However, unlike a hacker attack, the service is performed by experienced security experts from Kaspersky who take special care of system confidentiality, integrity and availability in strict adherence to the following international standards and best practices:

- 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)
- And other standards, depending on your organization's business and location

The analysis is performed using automated tools as well as manually by experts. The following security assessment tools can be used:

- Information gathering tools (Maltego, theHarvester and others)
- Various general-purpose and specialized scanners (NMap, MaxPatrol, Nessus, Acunetics WVS, nbtscan and others)
- Complex security assessment solutions (Kali Linux)
- Credentials guessing tools (Hydra, ncrack, Bruter, and others)

- Specialized solutions for web application security assessment (OWASP dirbuster, BurpSuite, ProxyStrike, various plug-ins for Mozilla Firefox)
- Network traffic analyzers (Wireshark, Cain and Abel)
- Credentials extraction and management tools (Mimikatz, WCE, pwdump and others)
- Specialized tools for various types of attacks (Yersinia, Loki, Responder, SIPVicious and others)
- Disassembling and debugging tools (IDA Pro, OllyDbg)
- And others, including limited access exploits and custom exploitation tools developed by the Service Provider.

For Red Teaming to be legal and safe, the customer must provide a point of contact (a representative) for all project communications, including scope negotiations and, resolving access issues, as well as giving confirmation for active works. The representative must be an official employee of the customers with an e-mail address belonging to the customer's domain name (not a third-party intermediary).

The confidentiality, integrity and availability of your IR resources are our top priority. Kaspersky's experts will take all necessary precautions to avoid any harm to your environment. All sensitive technical information related to the project (important data, credentials, assessment results, etc.) will be stored and transferred using strong encryption, and can be deleted on your request after the project has been completed.

Our expert team members are experienced professionals in security assessment with deep knowledge of this field, constantly improving their skills. They have been acknowledged for their security research by such industry leaders as Oracle, Google, Apple, Microsoft, Facebook, PayPal, Siemens, SAP, and others. You can find resumes of the project team members in the attachment to this proposal.

Outcome

Following the service, customers receive a report containing the following:

- High-level conclusions on the identified defensive capabilities, and recommendations to improve them;
- A detailed description of detected vulnerabilities, including severity level, exploitation complexity, possible impact on the vulnerable system, and evidence of the existence of vulnerabilities (where possible);
- A detailed description of activities (including timestamps and indicators of compromise) for analysis and improvement of the defensive team;
- Recommendations for eliminating vulnerabilities;
- Recommendations on improving the incident response processes;
- Recommendations on mitigating the identified prevention and detection issues.

The Red Teaming Testing Service from Kaspersky will help you evaluate the effectiveness of your monitoring capabilities and incident response procedures.

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 Application Security Assessment uncover vulnerabilities in appli-cations 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.

Results
Vulnerabilities which may be identified by Kaspersky 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 implica-tions. Videos and presentations for your technical team or top management can also be provided if required.

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.

Service benefits

Kaspersky 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's Approach To Application Security Assessment

Security assessments of applications are performed by Kaspersky 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

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.

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 help you to recognize the security flaws in your ATM/POS devices, and to mitigate the risk of being compromised.

There is no single solution that offers comprehensive protection. As a business man-ager, it`s your responsibility to protect your organization against today's threats, and to anticipate the dangers that lie ahead in the coming years. This needs more than just smart operational protection against known threats; it demands a level of strategic security intelligence that very few companies have the resources to develop in-house.

Security Assessment Services from Kaspersky – 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.

ATM/POS Security Assessment

Comprehensive analysis of ATMs and POS devices, designed to identify vulnerabilities that can be used by attackers:

- unauthorized cash withdrawal
- performing unauthorized transactions
- obtaining your clients' payment card data
- initiating denial of service

What happens when fraudsters goes in?
Each ATM machine consist of 4 cassettes with up to 3000 banknotes in each cassette. In worst case scenario criminals can obtain up to 255000$. ATM cash-out scheme happened in May, 2016 showed, that criminals are ready to coordinate their actions to access 1400 ATM machines in couple hours frame. Taiwan incident in July, 2016 with malicious software installed on multiple ATMs given criminals possibility to withdraw 2 million $ from twenty ATMs. Criminals are ready to attack ATMs. Don't be a victim.

Who we are
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 re-sults of our ATM/POS security researches at leading information security conferences, including Black Hat, Hack in Paris, Positive Hack Days, Security Analyst Summit, Nuit Du Hack, HITB GSEC, DefCamp, ATMIA events, Chaos Communication Congress and many others.

Follow our experts at www.securelist.com
Call us for help 1337@kaspersky.com

Why you should do this

ATM/POS Security Assessment by Kaspersky 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 whichattackers could exploit.
- Comply with government, industry or internal corporate standards, which include the carrying out of security assessments, e.g. PCI DSS (Payment Card Industry Data Security Standard).

What we are testing

The service includes comprehensive ATM/POS analysis including assessment of software components, hardware devices and network communications. Service can be conducted 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.

How we do this

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.

Threats for Financial Industry

As banks, stock markets, and other financial institutions are under persistent interest of cybercriminals due to the very nature of the financial business, to avoid financial and reputational losses they have to stay ahead of the curve in the field of cybersecurity. Kaspersky offers a set of proactive threat intelligence services for financial institutions that are looking to enhance their security operations and take a proactive approach against advanced threats:

- Security Assessment Services (Penetration Testing, Application Security Assessment, ATM and POS Security Assessment)
- Threat Intelligence Reports (APT Intelligence Reports, Customer-Specific Threat Intelligence Reports)
- Cyber-Attack Readiness Testing
- Botnet Threat Tracking
- Threat Data Feeds
- Malware Analysis and Digital Forensic
- Training: Threat Analysis, Forensic and Investigation

See more at www.kaspersky.com/enterprise

Cyber Threats News: www.securelist.com
IT Security News: business.kaspersky.com

www.kaspersky.com