KASPERSKY SECURITY INTELLIGENCE SERVICES. EXPERT SERVICES

www.kaspersky.com

EXPERT SERVICES

Expert Services from Kaspersky Lab are exactly that – 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.

Expert services include:

- Incident Detection and Response Services
- Kaspersky Managed Protection
- Penetration Testing
- ATM/POS Security Assessment
- Telecommunication Networks Security Assessment
- Application Security Assessment Services

EXPERT SERVICES

Incident Detection and Response Services

Kaspersky Managed Protection

Penetration Testing

ATM/POS Security Assessment

Telecommunication Networks Security Assessment

Application Security Assessment Services

INCIDENT DETECTION AND RESPONSE SERVICES

While your IT and security specialists work hard to ensure that every network component is both secure against intruders and fully available to legitimate users, a single vulnerability can offer an open door to any cybercriminal intent on gaining control over your information systems. No one is immune: however effective your security controls, you can become a victim.

Incident Detection and Response Services are designed to discover whether you are currently under cyber-attack and why, to trace possible sources of the attack, to formulate a mitigation action plan and to help you to avoid similar attacks in future.

Kaspersky Lab's experts will work with you to resolve live security issues and understand malware behavior and its consequences, as well as providing guidance on remediation, through two services:

- **Targeted Attack Discovery**
- **Incident Response**
- **Digital Forensics**
- **Malware Analysis**

TARGETED ATTACK DISCOVERY

If you are concerned about attacks directed at your industry, if you have noted possible suspicious behavior in your own systems, or if your organization simply recognizes the benefits of regular preventative inspections, Kaspersky Targeted Attack Discovery services are designed to tell you:

- Whether you are currently under attack, how, and by whom
- How this attack is affecting your systems, and what you can do about it
- How best to prevent further attacks

HOW THE SERVICE WORKS

Our globally-recognized independent experts will reveal, identify and analyze ongoing incidents, advanced persistent threats (APTs), cybercriminal and cyber-espionage activities in your network. They will help you to uncover malicious activities, understand the possible sources of incidents, and to plan the most effective remedial actions.

We do this by:

- Analyzing threat intelligence sources to understand your organization's specific threat landscape
- Conducting in-depth scans of your IT infrastructure and data (such as log files) to uncover possible signs of compromise
- Analyzing your outgoing network connections for any suspicious activity
- Uncovering probable sources of the attack, and other potentially compromised systems

THE RESULTS

Our findings are delivered in a detailed report covering:

Our overall discoveries – confirmation of the presence or absence of compromise signs in your network

In-depth analysis – of threat intelligence data gathered and of the Indicators of Compromise (IoCs) revealed.

Detailed descriptions – of vulnerabilities exploited, possible attack sources, and the network components affected.

Remediation recommendations – suggested steps to mitigate consequences of the incident revealed and to protect your resources from similar attacks in future.

THE SERVICE IN MORE DETAIL

Kaspersky Targeted Attack Discovery includes the following activities:

Threat intelligence gathering and analysis. The goal is to obtain a snapshot in time of your attack surface – the cybercriminal and cyber-espionage threats and attacks potentially or actively targeting your assets. We'll be tapping into internal and external intelligence sources, including underground fraudster communities, as well as internal Kaspersky Lab monitoring systems. Analysing this intelligence allows us to identify, for example, weaknesses in your infrastructure of current interest to cybercriminals, or compromised accounts.

Onsite data collection and early incident response. Alongside threat intelligence activity conducted in our own labs, Kaspersky Lab experts will be on site collecting network and system artefacts, together with any SIEM information available. We may also conduct a brief vulnerability assessment to reveal the most critical security flaws for immediate action. If an incident has already taken place, we'll be collecting evidence for investigation. At this stage, we'll provide you with our interim recommendations for short-term remediation steps.

Data analysis. The network and system artefacts collected will be analyzed back at the lab, using the Kaspersky Lab knowledge base of IoCs, C&C blacklists, sandboxing technology etc. to understand exactly what's been happening in your system. If, for example, new malware is identified at this stage, we'll give you advice and the tools (i.e. YARA rules) to detect it right away. We'll be keeping in close touch with you throughout, working remotely with your systems if appropriate.

Report preparation. Finally, we'll prepare our formal report with targeted attack discovery results and our recommendations for further remediation activity.

ADDITIONAL SERVICES

You can also ask our experts to analyze the symptoms of an incident, perform deep Digital Analysis for certain systems, identify a malware binary (if any) and conduct Malware Analysis. These optional services report separately, with further remediation recommendations.

We can also, on request, deploy the **Kaspersky Anti Targeted Attack (KATA) Platform** onto your network, permanently or as a 'proof of concept' exercise. This platform combines the latest technologies and global analytics in order to detection and respond promptly to targeted attacks, counteracting the attack at all stages of its lifecycle in your system.

INCIDENT RESPONSE

It's becoming increasingly difficult to prevent information security incidents. But while it may not always be possible to halt an attack before it penetrates your security perimeter, it's absolutely in our power to limit the resultant damage and to prevent the attack from spreading.

The overall aim of Incident Response is to reduce the impact of a security breach or an attack on your IT environment. The service covers the entire incident investigation cycle, from the onsite acquisition of evidence to the identification of additional indications of compromise, preparing a remediation plan and completely eliminating the threat to your organization.

We do this by:

- Identifying compromised resources.
- Isolating the threat.
- Preventing the attack from spreading.
- Finding and gathering evidence.
- Analyzing the evidence and reconstructing the incident's chronology and logic.
- Analyzing the malware used in the attack (if any malware is found).
- Uncovering the sources of the attack and other potentially compromised systems (if possible).
- Conducting tool-aided scans of your IT infrastructure to reveal possible signs of compromise.
- Analyzing outgoing connections between your network and external resources to detect anything suspicious (such as possible command and control servers).
- Eliminating the threat.
- Recommending further remedial action you can take.

Depending on whether or not you have your own incident response team, you can ask our experts to execute the complete investigation cycle, to simply identify and isolate compromised machines and prevent dissemination of the threat, or to conduct Malware Analyses or Digital Forensics.

Kaspersky Lab's Incident Response Services are carried out by highly experienced cyber-intrusion detection analysts and investigators. The full weight of our global expertise in Digital Forensics and Malware Analysis can be brought to bear on the resolution of your security incident.

MALWARE ANALYSIS

Malware Analysis offers a complete understanding of the behavior and objectives of the specific malware files that are targeting your organization. Kaspersky Lab's experts carry out a thorough analysis of the malware sample you provide, creating a detailed report that includes:

- *Sample properties*: A short description of the sample and a verdict on its malware classification.
- *Detailed malware description*: An in-depth analysis of your malware sample's functions, threat behavior and objectives – including IOCs – arming you with the information required to neutralize its activities.
- *Remediation scenario*: The report will suggest steps to fully secure your organization against this type of threat.

DIGITAL FORENSICS

Digital Forensics can include malware analysis as above, if any malware was discovered during the investigation. Kaspersky Lab experts piece together the evidence to understand exactly what's going on, including the use of HDD images, memory dumps and network traces. The result is a detailed elucidation of the incident. You as the customer initiate the process by gathering evidence and providing an outline of the incident. Kaspersky Lab experts analyze the incident symptoms, identify the malware binary (if any) and conduct the malware analysis in order to provide a detailed report including remediation steps.

DELIVERY OPTIONS

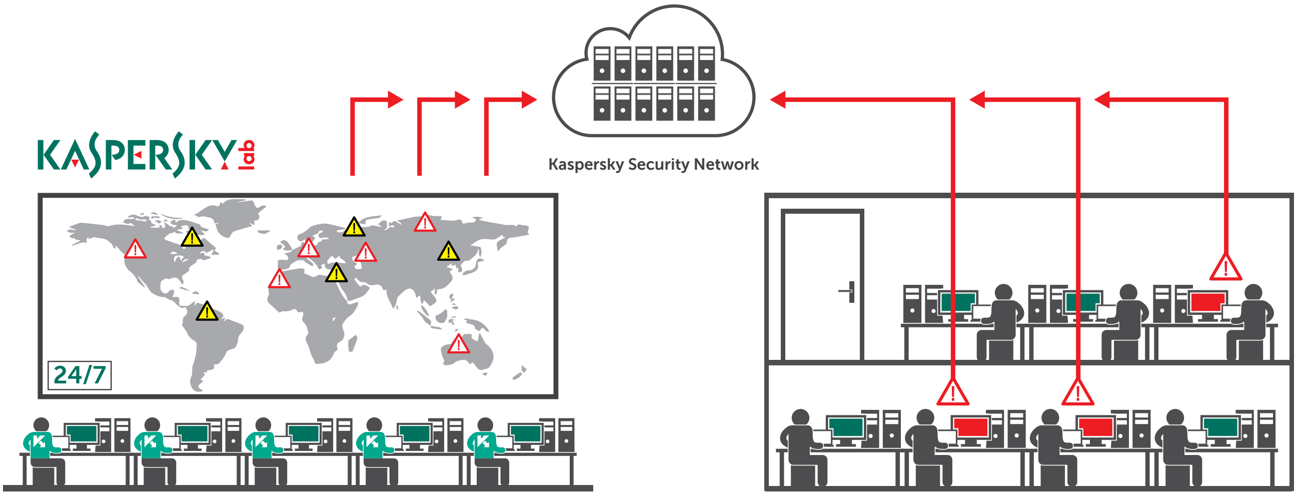
Kaspersky Lab's Incident Response Services are available:

- By subscription
- In response to a single incident

Both options are based on the amount of time our experts spend resolving the incident – this is negotiated with you prior signing the contract. You can specify the number of working hours you wish us to spend, or follow our experts' recommendations based on the specific incident and your individual requirements.

KASPERSKY MANAGED PROTECTION

The Kaspersky Managed Protection service offers Kaspersky Security for Business and Kaspersky Anti Targeted Attack Platform users a unique combination of advanced technical measures to detect and prevent targeted attacks. The service includes round-the-clock monitoring by Kaspersky Lab experts and the continuous analysis of cyberthreat data (Cyber-Threat Intelligence), ensuring real-time detection of both known and new cyber-espionage and cybercriminal campaigns targeting critical information systems.



SERVICE HIGHLIGHTS

- A high level of protection against targeted attacks and malware with 24x7 support from Kaspersky Lab analysts.
- Insights into attackers, their motivation, their methods and tools, and the potential damage they could inflict, supporting the development of a fully informed, effective protection strategy.
- Detection of non-malware attacks, attacks involving previously unknown tools and attacks exploiting zero-day vulnerabilities.
- Retrospective analysis of incidents and threat hunting.
- Reduction in overall security costs while simultaneously enhancing the quality of protection. This is a highly professional service offered by the world leader in cyber-attack analysis, including the analysis of the methods and technologies used by threat actors. Obtaining this level of information through an outside service is far more economical than employing narrowly focused specialists.
- Integrated approach — our extensive range of integrated Kaspersky Security for Business solutions means Kaspersky Lab offers all the technologies and services needed to implement a complete cycle of protection against targeted attacks: Preparation — Detection — Investigation — Data Analysis — Automated Protection.

SERVICE BENEFITS

- Quickly detects incidents.
- Collects sufficient information to enable classification (into false positive or correct detection).
- Identifies how common the collected artifacts are, determining how unique the attack is.
- Initiates the process of responding to an information security incident.
- Initiates any necessary updates to antivirus databases, to block the spread of threats.

PENETRATION TESTING SERVICES

Ensuring that your IT infrastructure is fully secured against potential cyber-attack 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.

While your IT and security specialists work hard to ensure that every network component is both secure against intruders and fully available to legitimate users, a single vulnerability can offer an open door to any cybercriminal intent on gaining control over your information systems.

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 Service 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 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)).

SERVICE SCOPE AND OPTIONS

Depending on your needs and your IT infrastructure, you may choose to employ any or all of these Penetration Testing 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.

PENETRATION TESTING RESULTS

The Penetration Testing 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.

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 rremotely, and internal penetration testing can even be performed through VPN access, while some services (like wireless networks security assessment) require an onsite presence.

ATM/POS SECURITY ASSESSMENT SERVICES

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 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.

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.

TELECOMMUNICATION NETWORKS SECURITY ASSESSMENT SERVICES

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 through 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

Incident response

It's becoming increasingly difficult to prevent information security incidents. But while it may not always be possible to halt an attack before it penetrates your security perimeter, it's absolutely in our power to limit the resultant damage and to prevent the attack from spreading.

The overall aim of Incident Response is to reduce the impact of a security breach or an attack on your IT environment. The service covers the entire incident investigation cycle, from the onsite acquisition of evidence to the identification of additional indications of compromise, preparing a remediation plan and completely eliminating the threat to your organization.

We do this by:

- Identifying compromised resources.
- Isolating the threat.
- Preventing the attack from spreading.
- Finding and gathering evidence.
- Analyzing the evidence and reconstructing the incident's chronology and logic.
- Analyzing the malware used in the attack (if any malware is found).
- Uncovering the sources of the attack and other potentially compromised systems (if possible).
- Conducting tool-aided scans of your IT infrastructure to reveal possible signs of compromise.
- Analyzing outgoing connections between your network and external resources to detect anything suspicious (such as possible command and control servers).
- Eliminating the threat.
- Recommending further remedial action you can take.

Depending on whether or not you have your own incident response team, you can ask our experts to execute the complete investigation cycle, to simply identify and isolate compromised machines and prevent dissemination of the threat, or to conduct Malware Analyses or Digital Forensics.

Kaspersky Lab's Incident Response Services are carried out by highly experienced cyber-intrusion detection analysts and investigators. The full weight of our global expertise in Digital Forensics and Malware Analysis can be brought to bear on the resolution of your security incident.

MALWARE ANALYSIS

Malware Analysis offers a complete understanding of the behavior and objectives of the specific malware files that are targeting your organization. Kaspersky Lab's experts carry out a thorough analysis of the malware sample you provide, creating a detailed report that includes:

- *Sample properties*: A short description of the sample and a verdict on its malware classification.
- *Detailed malware description*: An in-depth analysis of your malware sample's functions, threat behavior and objectives – including IOCs – arming you with the information required to neutralize its activities.
- *Remediation scenario*: The report will suggest steps to fully secure your organization against this type of threat.

DIGITAL FORENSICS

Digital Forensics can include malware analysis as above, if any malware was discovered during the investigation. Kaspersky Lab experts piece together the evidence to understand exactly what's going on, including the use of HDD images, memory dumps and network traces. The result is a detailed elucidation of the incident. You as the customer initiate the process by gathering evidence and providing an outline of the incident. Kaspersky Lab experts analyze the incident symptoms, identify the malware binary (if any) and conduct the malware analysis in order to provide a detailed report including remediation steps.

DELIVERY OPTIONS

Kaspersky Lab's Incident Response Services are available:

- By subscription
- In response to a single incident

Both options are based on the amount of time our experts spend resolving the incident – this is negotiated with you prior signing the contract. You can specify the number of working hours you wish us to spend, or follow our experts' recommendations based on the specific incident and your individual requirements.

APPLICATION SECURITY ASSESSMENT SERVICES

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 Services 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

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.

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 of 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.

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.

KASPERSKY lab