KASPERSKYⁱᵃᵇ

KASPERSKY SECURITY INTELLIGENCE SERVICES. EXPERT SERVICES

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 Investigation
- Penetration Testing
- Application Security Assessment

EXPERT SERVICES

Incident Investigation
Penetration Testing
Application Security
Assessment

INCIDENT INVESTIGATION

Digital forensics | malware analysis

Personalized incident investigation support to help your organization identify and resolve IT security incidents.

Cyberattacks are an increasing danger for enterprise networks. Tailor-made to exploit the unique vulnerabilities of the criminal's chosen target, these attacks are often designed to steal or destroy sensitive information or intellectual property, undermine operations, damage industrial facilities or steal money.

Protecting an enterprise against these sophisticated, well-planned attacks has become increasingly complicated. It can even be difficult to establish for certain whether your organization is in fact under attack.

Kaspersky Lab's Incident Investigation Services can help organizations formulate their defense strategies through providing in-depth threat analysis and advising on appropriate steps toward resolution of the incident.

SERVICE BENEFITS

Kaspersky Lab Incident Investigation Services help you to resolve live security issues and understand malware behavior and its consequences, providing guidance on remediation. This approach indirectly helps to:

- Reduce the costs of resolving issues arising from a cyber-infection
- Stop the leakage of confidential information that can potentially flow from infected PCs
- Reduce reputational risk caused by the infection harming operational processes
- Restore the normal work of PCs that were damaged by infection

Kaspersky Lab's investigations are carried out by highly experienced analysts with practical expertise in digital forensics and malware analysis. On completion of the investigation, you are provided with a detailed report, giving the full results of the cyber investigation and proposing remediation steps.

DIGITAL FORENSICS

Digital Forensics is an investigation service aimed at producing a detailed picture of an incident. 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 is going on, including the use of HDD images, memory dumps and network traces. The result is a detailed explanation of the incident.

You as the customer initiate the process by gathering evidence and 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.

MALWARE ANALYSIS

Malware Analysis offers a complete understanding of the behavior and objectives of specific malware files that are targeting your organization.

Kaspersky Lab's experts carry out a thorough analysis of the malware sample provided by your organization, 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

DELIVERY OPTIONS

Kaspersky Lab Investigation Services are available:

- by subscription, based on an agreed number of incidents
- in response to a single incident

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.

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§