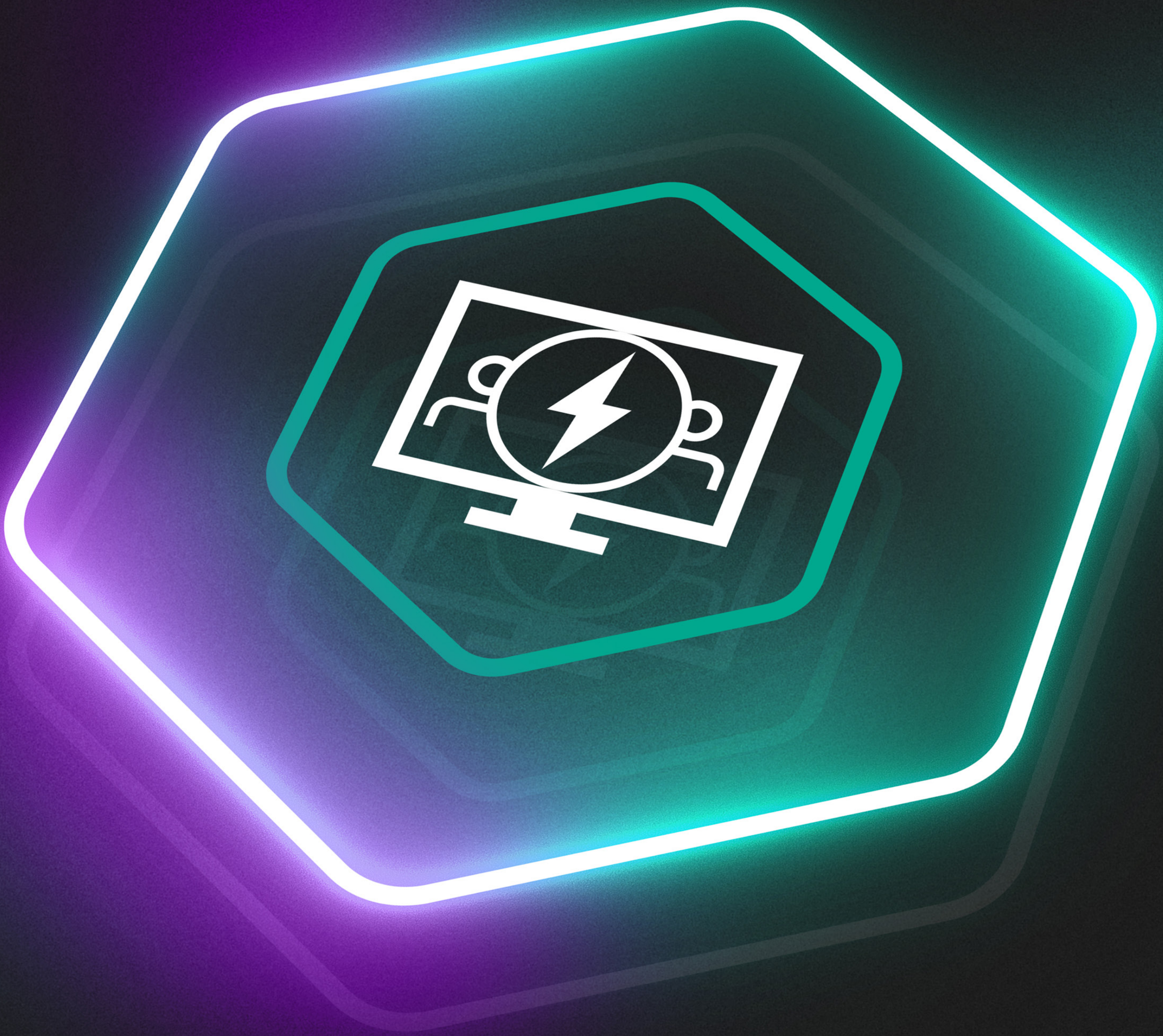

Kaspersky Red Teaming

kaspersky bring on the future

Kaspersky
Red Teaming

Overview

Completely preventing information assets from being compromised can be extremely difficult in large networks, or even impossible when attacks are launched using zero-day vulnerabilities.

That's why it's critical to do everything you can to ensure that information security incidents are detected as early as possible. Mature organizations with well-established processes for security assessments, vulnerability management, and information security incident detection should conduct Red Teaming tests.

These tests determine how well infrastructures are protected against highly skilled attackers operating with maximum stealth, and help train the IT security team to identify and respond to attacks under real-world conditions.

How Kaspersky Red Teaming works?

Threat Intelligence

The service begins with a discussion of the customer's known threats and Blue Team experience. The goal is to identify the most critical business assets and understand how the project deliverables can be tailored to the TTPs used by the company's defense. However, during these discussions Kaspersky will not request any information about the target assets, as the Red Team will also conduct independent information gathering activities, just as real adversaries would. The information gathering phase includes both the analysis of publicly available information (open source intelligence) and the analysis of data available in underground communities.

Adversary Simulation

This phase begins with the preparation of attack scenarios and tools based on the results of the threat intelligence phase.

Preparation may include in-depth research of systems used in the client's environment to identify new vulnerabilities, development of custom tools to bypass the client's security systems, or preparation of spear-phishing attacks. Once the preparation is complete, Kaspersky performs the active phase of adversary simulation.

The tests are performed based on customer-specific scenarios using special techniques to avoid detection by the Blue Team. After the Red Team completes its objectives, activities that trigger incident detection and response are carried out to involve the Blue Team in the exercise.

Adversary simulation tests may include:

- Adversary simulation tests may include:
- Passive information gathering
- Active information gathering (network discovery)
- including port scanning, identification of available services, and manual requests to specific services (DNS, mail)
- Web application security (using both automated and manual approaches) to identify the various types of vulnerabilities
- Web application security (using both automated and manual approaches) to identify the various types of vulnerabilities
- Manual vulnerability analysis, including identification of resources without authentication, important publicly available information, insufficient access control
- Credential guessing
- Social engineering tests
- Exploiting one or more of the vulnerabilities found and escalating privileges (if possible)
- Developing an attack using the privileges gained and the techniques listed above until the service provider is able to can access the LAN or critical network resources (e.g., Active Directory domain controllers, business systems, DBMSs, etc.) or until all attack methods available during the available during the test have been exhausted.

Report Preparation

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

Overview of Testing Results

A post-assessment workshop can be arranged with the company's Blue Team to discuss project results, reasons for any undetected or unprevented issues, and potential defense improvements.

Kaspersky Red Teaming methodology

The following security assessment tools can be used:

- Information gathering tools (Maltego, theHarvester and others)
- Various general-purpose and specialized scanners (NMap, MaxPatrol, Nessus, AcuneticsWVS, nbtscan and others)
- Complex security assessment solutions (KaliLinux)
- Credentials guessing tools (Hydra, ncrack, Bruter, andothers)
- Specialized solutions for web application security assessment (OWASPdirbuster, 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.

Red Teaming is similar to a real hacker attack and allows for the evaluation of protection measures in practice. However, unlike a hacker attack, this service is performed by experienced security experts from Kaspersky who prioritize system confidentiality, integrity, and availability while strictly adhering to international standards and best practices, such as:

1. Penetration Testing Execution Standard (PTES)
2. NIST Special Publications 800-115 Technical Guide to Information Security Testing and Assessment
3. Open Source Security Testing Methodology Manual (OSSTMM)
4. Information Systems Security Assessment Framework (ISSAF)
5. Web Application Security Consortium (WASC)
6. Threat Classification Open Web Application Security Project (OWASP)
7. Testing Guide Common Vulnerability Scoring System (CVSS)
8. And other applicable standards based on your organization's business and location

To ensure the legality and safety of Red Teaming, the customer must provide an official employee as a point of contact for all project communications, including scope negotiations, resolving access issues, and confirming active works. The representative must have an email address belonging to the customer's domain name and not be a third-party intermediary.

Kaspersky Red Teaming outcome

Executive summary	After the service, customers will receive a report that includes high-level conclusions on the identified defensive capabilities and recommendations to improve them.
Vulnerability details	In addition, the report includes a detailed description of the vulnerabilities found, including severity level, complexity of exploitation, potential impact on the vulnerable system, and evidence of the existence of the vulnerabilities (where possible).
Activity details	A detailed description of activities, including timestamps and indicators of compromise, is provided for the analysis and improvement of the defensive team.
Recommendations	For eliminating vulnerabilities, improving incident response processes, and mitigating identified prevention and detection issues are also included.

Why Kaspersky?

Prioritizing Security

Our top priority is ensuring the confidentiality, integrity, and availability of your resources. Kaspersky's experts will take all necessary precautions to prevent any harm to your environment.

Protecting Your Data

We will store and transfer all sensitive technical information related to the project, including important data, credentials, and assessment results, using strong encryption. If requested, this information can be deleted after the project is completed.

Providing Expertise

Our team of security assessment experts are highly experienced professionals with deep knowledge of the field. They constantly develop and hone their skills. They have been recognized for their security research by industry leaders such as Oracle, Google, Apple, Microsoft, Facebook, PayPal, Siemens, SAP, and others

www.kaspersky.com

#kaspersky
#bringonthefuture