KASPERSKY lab

Kaspersky Threat Hunting

www.kaspersky.com
#truecybersecurity

Kaspersky Threat Hunting

Security teams across all industries are working hard building systems to provide comprehensive protection against rapidly evolving cyber threats. But most of these take an "alert" driven approach to cybersecurity incidents, reacting only after an incident has already taken place.

According to recent research, a large proportion of security incidents still goes undetected. These threats move in under the radar, giving businesses, quite literally, a false sense of security. As a result, organizations are increasingly recognizing the need to proactively hunt out threats that are lying undiscovered but still active within their infrastructures. Kaspersky Threat Hunting Services help to uncover advanced threats hiding within the organization, using proactive threat hunting techniques carried out by highly qualified and experienced security professionals.

Kaspersky Cybersecurity Services

- **Kaspersky Threat Intelligence**
- **Kaspersky Threat Hunting**
  Kaspersky Managed Protection
  Targeted Attack Discovery
- **Kaspersky Security Training**
- **Kaspersky Incident Response**
- **Kaspersky Security Assessment**

Kaspersky Managed Protection

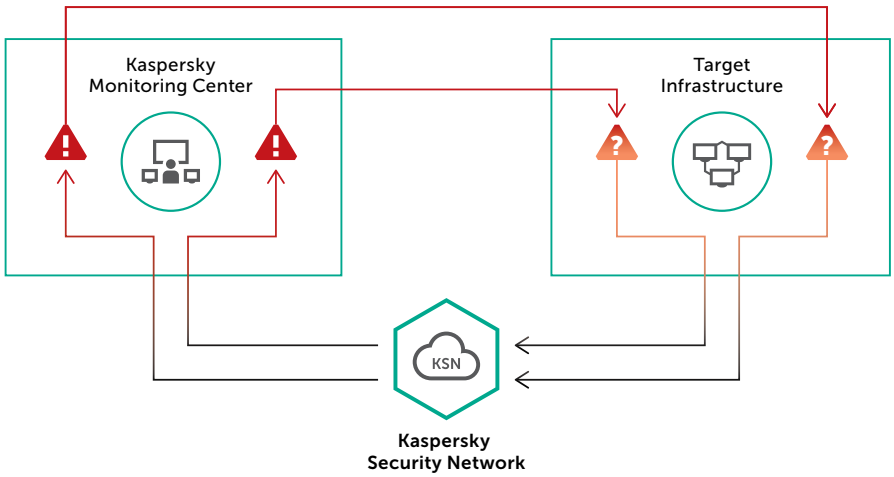
The Kaspersky Managed Protection service offers Kaspersky Endpoint Security and Kaspersky Anti Targeted Attack Platform users a fully managed service, deploying a unique range of advanced technical measures to detect and prevent targeted attacks on your organization. The service includes round-the-clock monitoring by Kaspersky Lab experts and the continuous analysis of cyberthreat data, ensuring the real-time detection of both known and new cyberespionage and cybercriminal campaigns targeting critical information systems.

Service highlights

- A continuously high level of protection against targeted attacks and malware, with 24x7 monitoring and support from your own 'crack team' of Kaspersky Lab experts, drawing on a deep pool of specialist skills and ongoing threat intelligence.
- The timely and accurate detection of non-malware attacks, attacks involving previously unknown tools and attacks exploiting zero-day vulnerabilities.
- Immediate protection against any detected threat through automatic antivirus database updates.
- Retrospective analysis of incidents and threat hunting, including the methods and technologies used by threat actors against your organization.
- An integrated approach - The Kaspersky Lab portfolio includes all the technologies and services you need to implement a complete cycle of protection against targeted attacks: Preparation – Detection-Investigation – Data Analysis – Automated Protection.

Service benefits

- Fast, efficient detection, enabling faster and more effective mitigation and remediation.
- No time-wasting false positives, thanks to the clear, immediate identification and classification of any suspicious activity.
- Reduced overall security costs. No need to employ and train a range of different in-house specialists you may need.
- The reassurance of knowing that you are continuously protected against even the most complex and innovative non-malware threats.
- Insights into attackers, their motivation, their methods and tools, and the potential damage they could inflict, supporting the development of your fully informed, effective protection strategy.



Targeted Attack Discovery

Kaspersky Lab experts provide proactive Targeted Attack Discovery service to ensure the true security of your business assets.

Targeted Attack Discovery results will let you identify current cybercriminal and cyberespionage activity in your network, understand the reasons behind and possible sources of these incidents, and effectively plan mitigation activities that will help avoid similar attacks in future. 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:

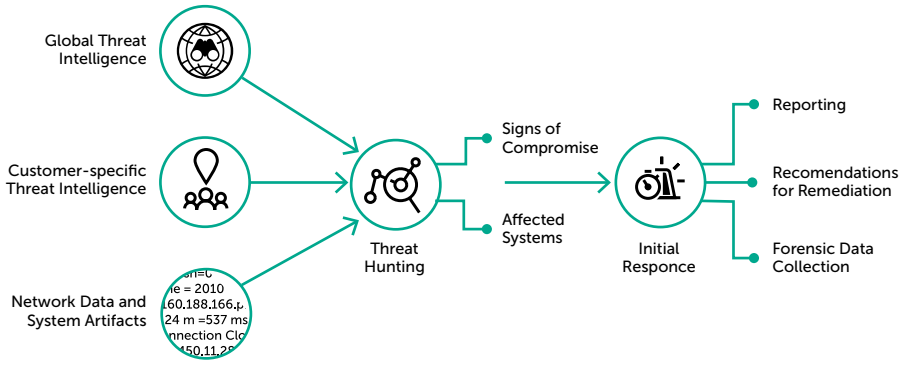
- Whether you are currently under attack, how, and by whom
- How this attack is affecting your systems, and what you can do about it
- How best to prevent further attacks

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:

- **General information** confirming your network is compromised or signs that it may be;
- **Analysis of the intelligence** gathered about threats and indicators of compromise (IOC);
- **Description of possible attack sources** and compromised network components;
- **Remediation recommendations** to mitigate the impact of an incident and protect your resources from similar attacks in future.

The service in more detail

Kaspersky Targeted Attack Discovery includes the following activities:

Gathering and analyzing data on attacks from external sources. The aim at this stage is to obtain a snapshot of the attack surface of a company whose assets are, or were, being targeted by intruders. We tap into a variety of intelligence sources, including underground cybercriminal communities, as well as internal Kaspersky Lab monitoring systems. Analyzing this intelligence allows us to identify weaknesses in a company's infrastructure that are of interest to cybercriminals, compromised accounts, stolen data and much more.

Onsite data collection. This stage sees data collected from workstations, servers, SIEM systems and other equipment in the customer's infrastructure. Some of the data is collected using software provided to the customer within the framework of the service.

Data analysis. Kaspersky Lab experts use the data collected at the previous stage to identify incidents in the corporate network. The main purpose of this stage is to determine the type of incident and assess its impact on the infrastructure, which allows the appropriate remediation measures to be implemented. At this stage, data from workstation logs, network activity data, and other contextual and historical intelligence is used; no additional data is collected directly from compromised systems.

Early incident response. At this stage we provide interim recommendations for initial incident response. In some cases, to confirm and classify an incident, Kaspersky Lab experts may require additional data, such as various files from operating systems, applications and network equipment, network traffic dumps, hard disk images, memory dumps or other types of data. The customer may be asked to provide additional data (via email or various network resources, depending on the type and amount of data requested).

Report preparation. The work carried out within the framework of the service culminates in a final report. It contains the results of data analysis from external sources, as well as descriptions of detected attacks based on analysis of the data collected in the customer's infrastructure. The report also contains remediation recommendations for the detected attacks.

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.

Kaspersky Lab
Find a partner near you: **www.kaspersky.com/buyoffline**
Kaspersky for Business: **www.kaspersky.com/business**
IT Security News: **business.kaspersky.com/**
Our unique approach: **www.kaspersky.com/true-cybersecurity**

#truecybersecurity
#HuMachine

www.kaspersky.com