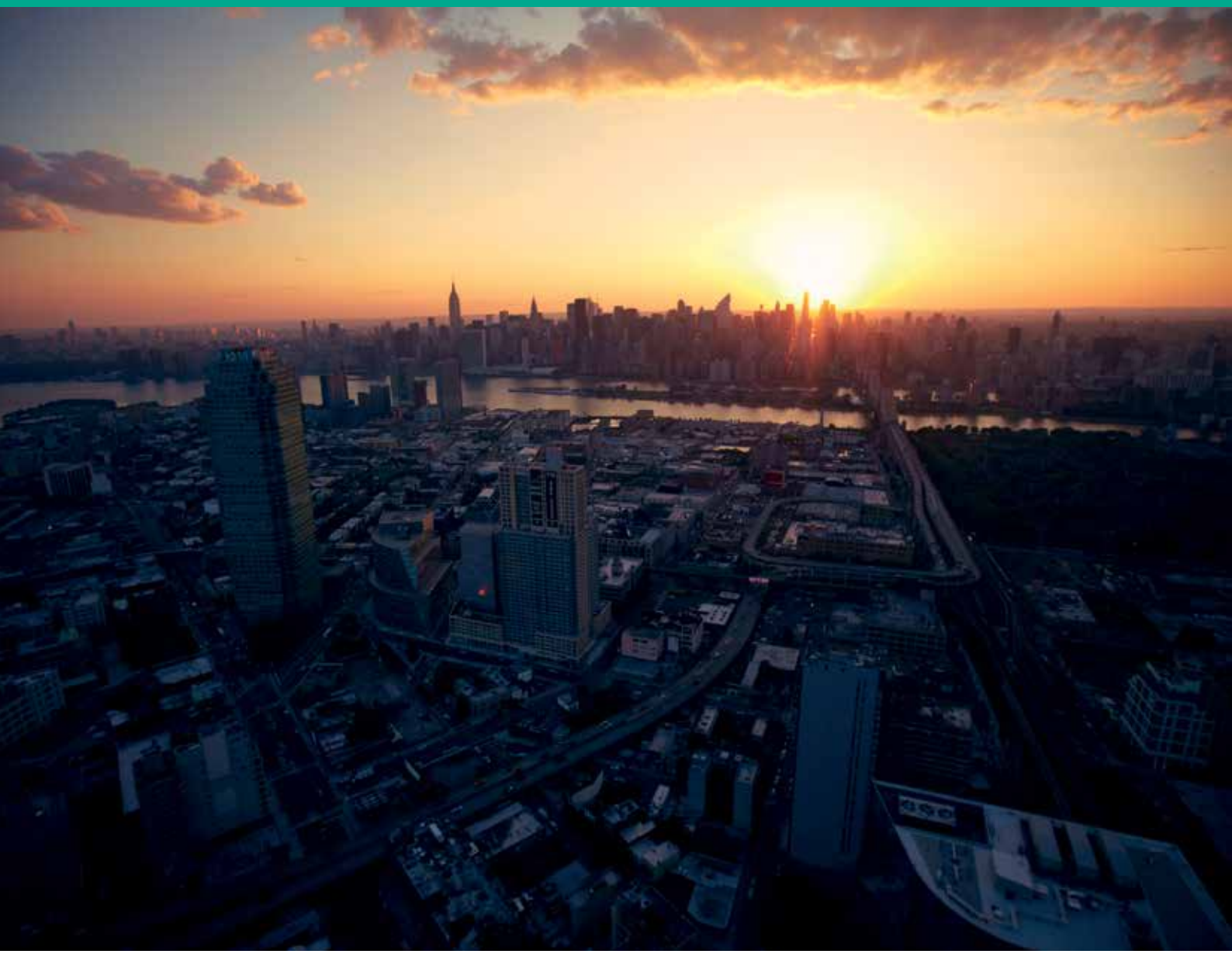


Kaspersky Threat Hunting Services

www.kaspersky.com
#truecybersecurity

Kaspersky Threat Hunting Services

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.

Service benefits

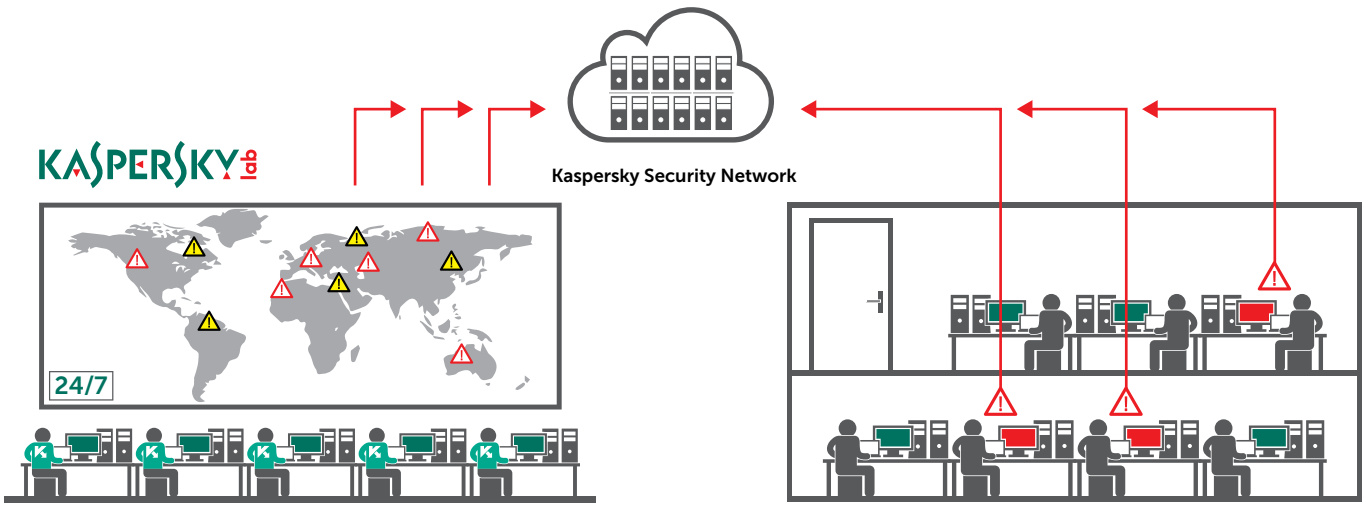
- Fast, efficient detection, enabling faster and more effective mitigation and remediation.
- No time-wasting false positives, thanks to the clear, immediate identification and classification of any suspicious activity.
- Reduced overall security costs. No need to employ and train a range of different 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.

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.



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:

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.

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.

The service in more detail

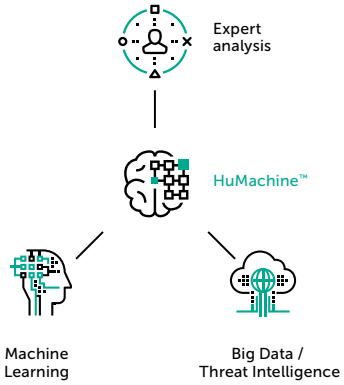
Kaspersky Targeted Attack Discovery includes the following activities:

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. Analyzing 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.



Kaspersky Lab
Enterprise Cybersecurity: **www.kaspersky.com/enterprise**
Cyber Threats News: **www.securelist.com**
IT Security News: **business.kaspersky.com/**

#truecybersecurity
#HuMachine

www.kaspersky.com