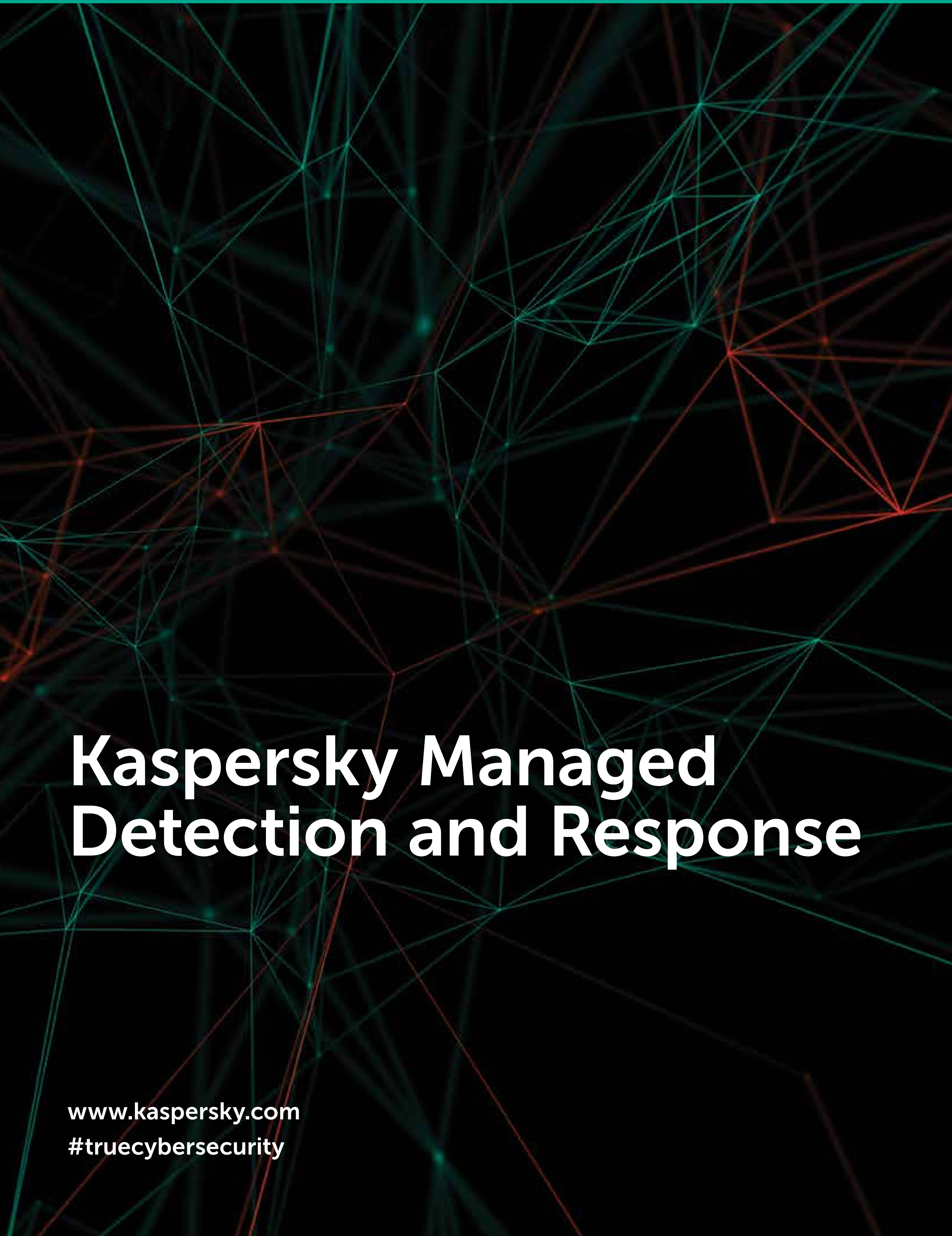
Kaspersky Enterprise Cybersecurity



Kaspersky Managed Detection and Response

www.kaspersky.com
#truecybersecurity

Kaspersky Managed Detection and Response

Problem Statement

As corporate processes undergo extensive, across-the-board automation, businesses are becoming increasingly dependent on information technologies. This, in turn, means the risks associated with disruption to core business processes are steadily shifting to the IT field. The developers of automation tools are aware of this and, in an attempt to address possible risks, are increasingly investing in IT security – a key characteristic of an IT system along with reliability, flexibility and cost. The last couple of decades have seen a dramatic improvement in the security of software products; virtually all global software manufacturers now publish documents dedicated to safety configurations and secure use of their products, while the information security market has been flooded with offers to ensure protection in one form or another.

On the flipside, the more a company's business is dependent on IT, the more attractive the idea of hacking its information systems. The aforementioned increase in software security levels has resulted in more resources being required to successfully carry out hacking attacks.

The increased minimum costs of a successful attack, in combination with cybercriminals having to establish a long-standing presence within the target infrastructure to overcome the multiple layers of defense and ensure a maximum return on their investments, have led to the emergence of targeted attacks. Such attacks are carefully planned and implemented; along with automatic tools, they require the direct and deep involvement of professional attackers whose work is not dissimilar to that of penetration testing teams. Counteracting these professional attackers takes professionals that are no less qualified and equipped with the latest tools for detecting and preventing computer attacks.

Professional publications often advance the theory that an organization's security goals can be considered achieved when the cost of compromise exceeds the value of the protected information assets. However, this premise has had to be substantially reevaluated in light of recent publications on CIA and NSA cyber weapons. Practice has shown that the developers of cyber weapons don't care that much about keeping their creations secret, meaning there is a good chance those creations will end up in the hands of potential threat actors whose research resources are far more modest. Given that the resources of intelligence services are virtually unlimited, it becomes clear that the possibility of using their creations dramatically cuts the cost of hacking. The only way to counter such threat actors is to adopt a systemic approach to protection. This implies prompt detection if a threat is impossible to prevent, and if detection is impossible, then having an effective response and restoration capabilities to mitigate the damage from attacks. This is especially important given that these attacks can be activated at various stages, via various vectors and in various environments, using a wide range of tactics, procedures and technologies.

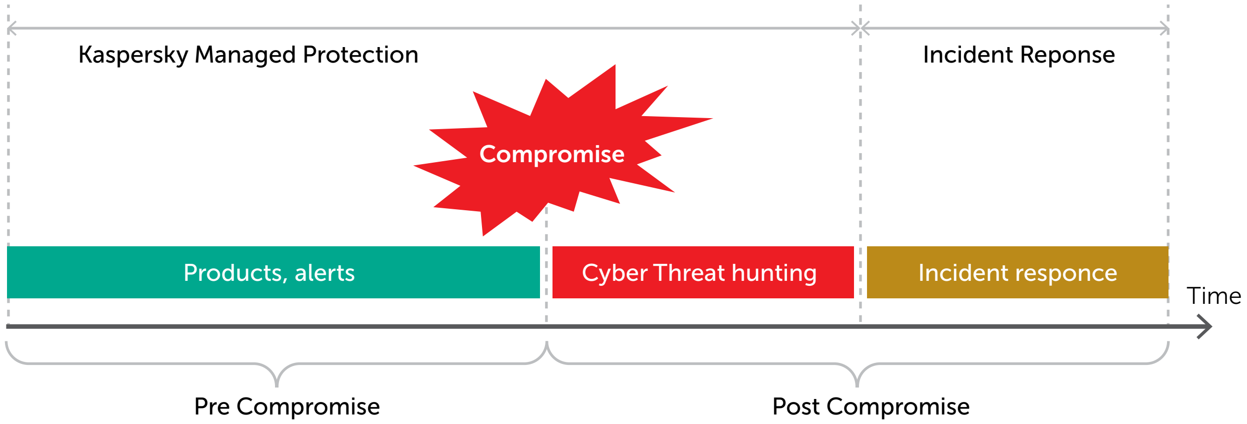
Kaspersky Managed Protection and Incident Response

Kaspersky Lab has been researching and preventing computer attacks for over 20 years. We can say with a degree of confidence that the list of threat detection and prevention technologies that we've developed over the years, including the latest research on big data and machine learning, means Kaspersky Lab's security products can stop any attack that can be detected and neutralized in automated mode.

Targeted attacks, however, take the protection tools available to their victims into consideration and are developed accordingly, bypassing automatic detection and prevention systems. These kinds of attacks are often carried out without any software being used, and the attackers' actions are barely distinguishable from those that IT or information security officers would perform.
The following are just some of the techniques used in modernday attacks:

- the use of tools to hamper digital forensics, e.g. by securely deleting artefacts on the hard drive or by implementing attacks solely within a computer's memory;
- the use of legitimate tools that IT and information security departments routinely use;
- multi-stage attacks, when traces of preceding stages are securely deleted;
- interactive work by a professional team (similar to that used during penetration testing).

This sort of attack can only be detected after the target asset has been compromised, as only then can suspicious behavior indicative of malicious activity be detected.
An approach called cyber threat hunting is used to detect attacks after the initial breach has taken place; a key element is the involvement of a professional analyst at the final stage of decision making. A human presence within the event analysis chain helps compensate for the weaknesses of automatic threat detection logic. Moreover, when pentest-like attacks involve a human on the attacking side, that human undoubtedly has an advantage when it comes to bypassing automatic technologies, so the presence of a human analyst is the only way to withstand such attacks. Neither automated threat detection and prevention tools nor cyber threat hunting alone is a silver bullet for the entire modern spectrum of threats. However, a combination of traditional detection and prevention tools active before a compromise occurs, plus a post-compromise iterative process of searching for new threats missed by automated tools can be effective.



Kaspersky Managed Protection (KMP) implements all the latest approaches to cyber threat hunting, improving the overall quality of threat detection by Kaspersky Lab products by supplementing multiple automated detection technologies with the skills of professional analysts. KMP's key advantage is that it detects attacks that automated detection and prevention tools have missed, including:

- detection of new malware that products failed to detect in automated mode; • detection of persistent attacks whose activities are below the detection thresholds of automated logic;
- detection of attacks launched without the use of malware;
- detection of fileless malware whose activities are executed exclusively in RAM memory;
- detection of pentest-like attacks carried out by professional attackers.

As well as detection, KMP also offers the following benefits:

- the ability to reproduce the sequence of attack stages if the attackers use techniques to hinder an investigation (secure deletion tools, multiple stages, etc.);
- 100% relevance for customers, because attacks are detected as part of an analysis of their IT infrastructure;
- if technically feasible, real-time protection can be provided with Kaspersky Lab's prevention products (Kaspersky Endpoint Security, Kaspersky Security for Mail Gateway, etc.), with subsequent supervision of treatment to ensure its effectiveness.

However, not all attacks can be stopped solely by adding neutralization components to an automated protection tool: if an attacker notices that they have been detected, they will change their tools and tactics and fall off the radar until detected again by an analyst within the framework of cyber threat hunting. Repeating this cycle is obviously not an effective way to solve the problem, so the additional Incident Response service comes into play here – it includes research on new malware samples and digital forensics.

As part of the Incident Response service, each security incident undergoes in-depth analysis, which results in the creation of new, more effective attack handling procedures, and measures are taken to prevent similar attacks in the future.

The KMP and Incident Response services complement each other nicely, because a more effective response than that provided by automated detection via the protection service can be determined through incident investigation procedures. At the same time, any investigation requires facts that can be established by analyzing events within the framework of Kaspersky Managed Protection.

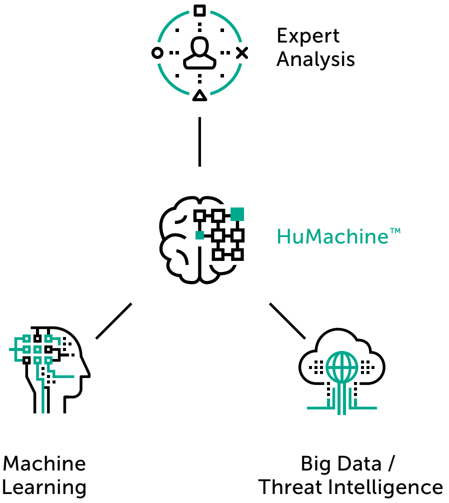
Despite the close connection and benefits of integration, Kaspersky Managed Protection and Incident Response are implemented as two separate services within the Kaspersky Lab services portfolio – this provides the client with extra flexibility when choosing which better suits their needs.

Unique Experience of Researching Targeted Attacks

Kaspersky Lab has a proven track record of effective targeted attack research, with the company's experts detecting the most advanced targeted attacks on a global scale, including Duqu, Project Sauron, Lambert, Equation and many more, as well as providing protection tools for them. For a chronology of the most notorious attacks, see https://apt.securelist.com/#!/threats/.

www.kaspersky.com

#truecybersecurity


Expert Analysis
HuMachine™
Machine Learning
Big Data / Threat Intelligence