Proven
Intelligence.
Guided Defense.

Kaspersky for Security Operations Center

kaspersky

Barriers to an effective Security Operations Center

As businesses learn to better protect themselves, criminals are simultaneously devising increasingly sophisticated techniques to penetrate their security barriers. Attracted by the unprecedented financial rewards that cyberattacks can deliver, growing numbers of threat actors are actively seeking and targeting undiscovered security flaws. In this environment, many organizations are establishing Security Operations Centers (SOCs) to combat security issues as they arise, providing a swift response and a decisive resolution.

Key findings according the Kaspersky Corporate IT Security Risks Survey in 2018:

- The cost of data breaches jumped by over a fifth. The average financial impact of a data breach now stands at $1.23 million for enterprises, a 24% increase on 2017.
- Making infrastructure improvements after a breach now sets enterprises back $193k on average, a more than 46% increase on the $132k it cost them in 2017.
- The good news is that average security budgets have increased across businesses of all sizes. Enterprises now spend an average of $8.9m on cybersecurity.
- Compared with previous years, the incidence of global threats experienced continues to grow:

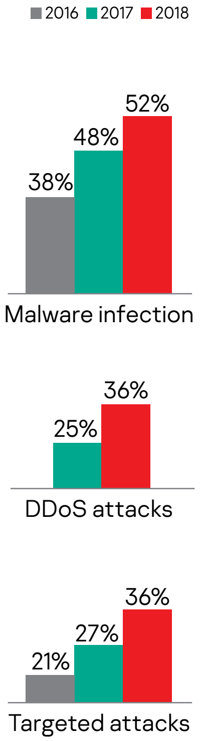


Figure 1:
Global threats experienced

The SOC is a centralized function for continuous threat monitoring and analysis, and for the mitigation and prevention of cybersecurity incidents

The ever-growing volume, complexity, and severity of today's cyberthreats means that documenting processes, implementing basic technologies and building a team of monitoring and response specialists is just the beginning. Without the ability to continuously adapt and advance, in response to ongoing changes in the threat landscape, the effectiveness of the SOC may be compromised.

According to Gartner's Adaptive Security Architecture model, if an organization is to successfully fight cybercrime in the current threat environment, its SOC Team must be able to predict, prevent, detect, and respond effectively to threats.

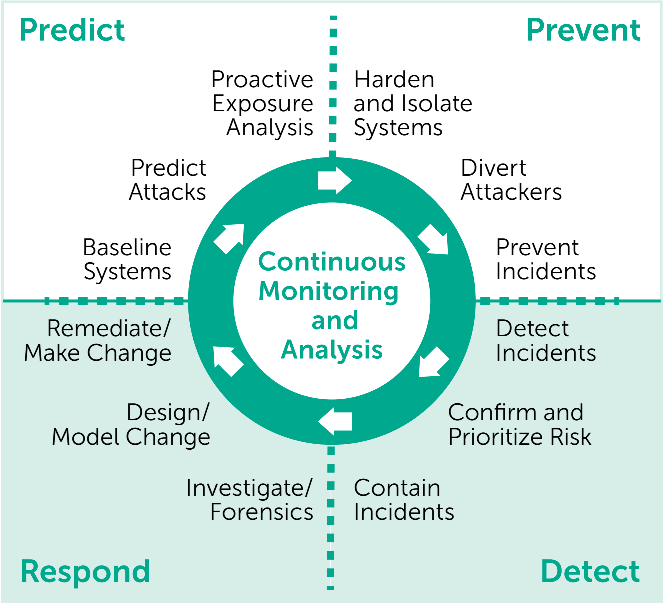
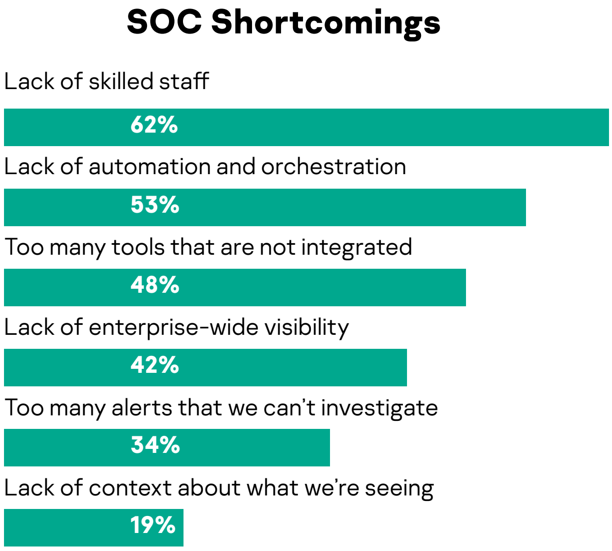


Figure 2:
Gartner, Designing an Adaptive Security Architecture for Protection From Advanced Attacks, February 2014

> **"Security Operations Centers must be architected for intelligence, embracing an adaptive security architecture to become context-aware and intelligence-driven. Security leaders should understand how intelligence-driven SOCs use tools, processes and strategies to protect against modern threats"**
>
> Gartner, The Five Characteristics of an Intelligence-Driven Security Operations Center, November 2015

The ‘SANS 2018 Security Operations Center’ survey of organizations who have created their own SOCs indicates that businesses encounter a number of barriers on the way to achieving an effective, well-run SOC.



Source: SANS2018 Security Operations Center Survey

Figure 3:
SOC shortcomings

Lack of skilled staff

In the face of overall IT security staff shortages, SOCs face a particular problem in terms of shortfalls in suitable skills and experience. The SOC team requires highly qualified niche specialists, with knowledge and experience in the fields of malware analysis, digital forensics, incident response, etc. These professionals should be able to correctly interpret data from the SIEM (Security Information and Event Management) system, identify and extract important information from the general data stream, fine-tune correlation rules and enrich the received information with additional context. Insufficient analyst expertise in dealing with complex threats, together with a lack of knowledge in how to use contextual data to correctly scope and investigate incidents, makes determining the most appropriate response to a specific threat much more difficult, and this can be very damaging to the business.

Lack of Automation

Another issue which can reduce the effectiveness of the SOC is lack of automation. Today, many analysts spend much their time on routine operations which are necessary and important, but which can be automated. Automating these manual tasks saves expensive analyst labor hours, and the resultant workload reduction frees more time to focus on analyzing and responding to really complex incidents.

Lack of integration

Running too many point tools, which don’t integrate with one other, is a concern for 48% of survey respondents. This forces analysts to switch between different tools and consoles, which wastes time, and provides opportunities for error. When introducing additional protection and automation tools, it’s important to take into account how these will integrate with existing solutions, and with one another.

Too many alerts

Information security tools, together with critical business applications connected to SIEM systems, generate a stream of alerts that should be reviewed daily. But this super-abundance of information means that many alerts remain unprocessed - around 50% of all alerts are never investigated. Meanwhile, levels of false positives experienced can be as high as 60-80%. All this means that trying to identify genuine potential threats can feel to the analyst like searching for needles in a haystack. Inevitably, serious incidents can get missed.

Overwhelmed by data, SOCs often understandably try to restrict their scope by monitoring a limited range of systems, but the problem with this approach is that they then don’t have a complete view of their entire infrastructure. This leads to another challenge – a lack of enterprise-wide visibility.

Lack of enterprise-wide visibility

For example, endpoints are rarely used as log sources in SIEM systems, partly because it’s expensive to do so, and partly due to the high number of false positives this generates. But endpoints are a key target for attackers – workstations and servers are the most common attack entry point into corporate IT infrastructures – and their data is key to investigating incidents (processes, programs, modules, files, autoruns, network connections, etc.). Add to this the new TLS 1.3 protocol, which further increases the value of telemetry analysis found on endpoints, and it becomes clear why accessing this data is important.

Lack of contextual data

A lack of understanding of the motivation, tactics, techniques and procedures employed by attackers can prevent SOC specialists from prioritizing incidents for investigation appropriately, leading to the specialist trying to do everything at once, or becoming paralyzed with indecision. Without appropriate and informed incident prioritization, there may be too many alerts to handle, increasing the stress on the overloaded SOC team and resulting in inefficiencies and increased response times. As a result, significant alerts suffer, while the percentage of inaccurate investigative results increases. Comparing information obtained by the SOC with threat intelligence data, provides the contextual information needed for appropriate incident prioritization and effective investigation.

Key Elements

The following key elements, together with clearly defined processes and relevant technologies, must be in place to sustain this industry-recognized approach:

- **Knowledge management.** People (SOC team members) must be well-trained in digital forensics, malware analysis and incident response in order to prevent and successfully respond to increasingly sophisticated attacks.
- **Advanced detection and response technologies** oriented towards complex threats and targeted attacks enabling deeper analysis and faster incident response.
- **Threat intelligence,** collected from relevant, trusted and reliable sources is essential to detect emerging threats quickly:
  - Internal threat data
  - Intelligence from open sources (OSINT)
  - Industry-specific communities (e.g. FS-ISAC)
  - Industry CERTs
  - Private communities
  - Global anti-malware vendors
  - Pure threat intelligence providers
- **Threat hunting** to proactively search for threats not detected by traditional security systems like firewall, IPS/IDS, SIEM, etc.
- **Incident investigation and response capability** to limit damage and reduce remediation costs.
- **Penetration testing & red teaming** to quickly identify weak spots where improvements are critical.

Each of these elements is equally important and warrants separate consideration

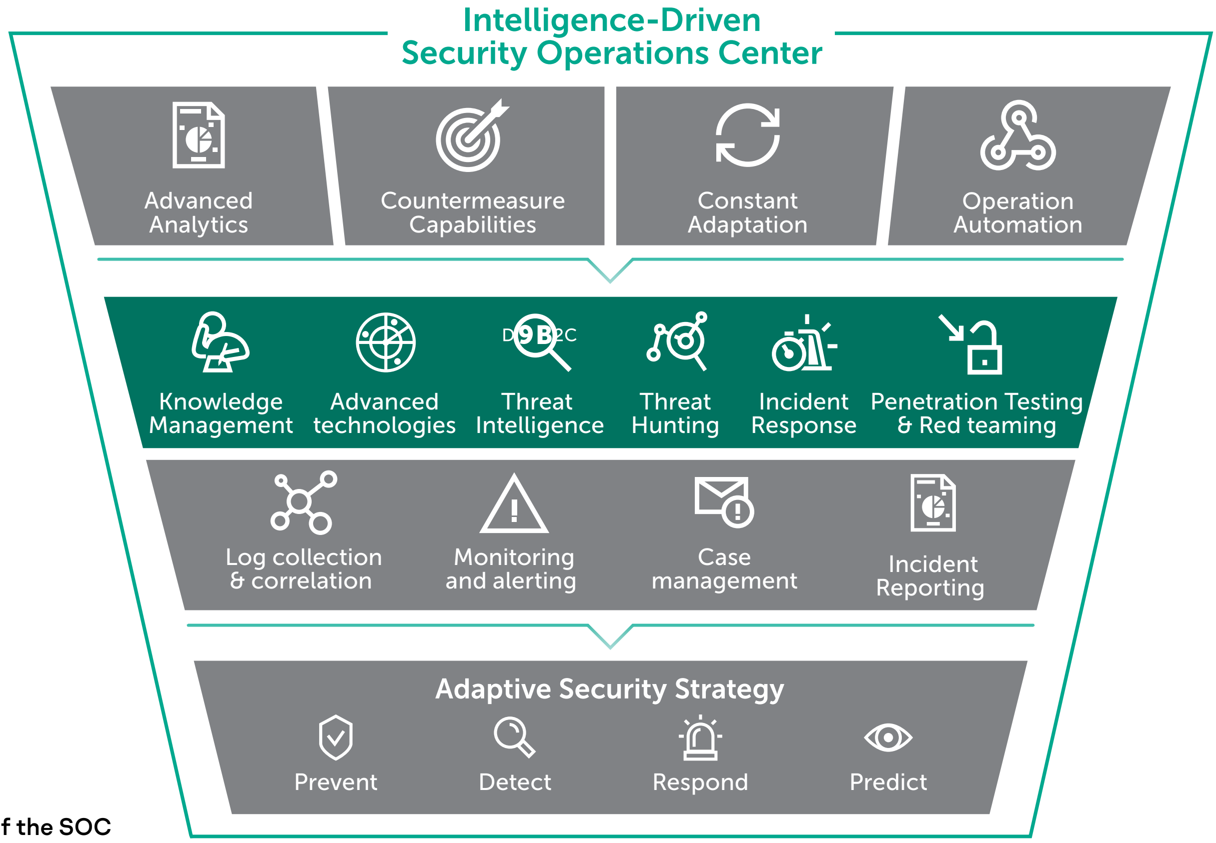


Figure 4:
The key elements of the SOC

Knowledge Management

The SOC must provide a resource pool of practical knowledge and expertise capable of analyzing a vast amount of data and identifying where further investigation is required.

Limited budgets make staffing the SOC a challenge. The market is currently experiencing a shortage of well-trained cybersecurity professionals, resulting in increased recruitment and employment costs.

An effective SOC team member must have:

- An inquisitive mind, able to construct an integrated overall picture from scattered data fragments;
- The ability to maintain a continuous focus while withstanding high stress levels;
- A good general knowledge of IT and cybersecurity, preferably with plenty of practical experience.

Whether you look to fill SOC roles through external recruitment or internal promotion, finding team members with the desired skills 'out of the box' is not easy. Ongoing training will be needed, not just to fill the gaps between current and required skillsets, but to equip team members to deal with ever-changing security technologies and a continuously evolving threat environment.

The table below contains example descriptions of the most common SOC roles and their responsibilities. Relevant roles and staff numbers for your SOC will depend on your service portfolio and scope.

In a small SOC, several roles may be held by one person, while in a large SOC team, more than one person for each role may be more appropriate.

Role	Description	Description
	Core	
Tier1 Analyst	Triage specialist	· Incident registration and assignment · Classification, verification, prioritization of security incidents · Security sensors health monitoring (if applicable) · Collecting data needed for Tier2 analyst work
Tier2 Analyst	Incident handler	· Incident analysis and response · Advice on containment and remediation actions · Incident response coordination and support · Tier1 analyst work periodical review
Malware Analyst	Incident response to highly sophisticated threats requires reverse engineering on malware samples or/and advanced forensic analysis on artifacts. It's the primary responsibility of the Malware Analyst to perform malware reverse engineering and produce valuable results for incident response activity.	· Static and dynamic in-depth malware analysis · Malware samples reverse-engineering · Participation in investigation of computer incidents and targeted attacks · IOCs acquisition
Digital Forensics Analyst	Incident response to highly sophisticated threats requires reverse engineering on malware samples or/and advanced forensic analysis on artifacts. When needed, forensic evidence must be collected and analyzed in a legally sound manner. It's the primary responsibility of the Digital Forensics Analyst to collect and analyze forensic evidence during incident response activity.	· Digital evidence collection and analysis · Participation in investigation of computer incidents and targeted attacks · OS, application, memory, network forensics analysis · IOCs acquisition
Threat Intelligence Analyst	When a SOC scales enough, it becomes reasonable to allocate internal threat intelligence functions to a dedicated role. The Threat Intelligence expert is responsible for analyzing threat intelligence from various sources (analytic reports, OSINT, past experience, etc.) and producing valuable results to the SOC team (TTPs, IOCs, analytics)	· Open source threat intelligence gathering and analysis · Vendor threat intelligence analytic reports analysis and parsing · TTPs and IOCs acquisition from TI-sources · Threat Data Feeds categorization, prioritization and verification · Threat Intelligence analytic reports creation for various stakeholders · Produce relevant analytics for SOC team and external partners · Threat feeds and IOCs sharing with customers
SOC System Admin	The SOC System Administrator is responsible for operation and maintenance (O&M) of the SOC enclave.	· SOC IT-infrastructure O&M · SOC infrastructure health monitoring · Scripting & automation · SOC infrastructure and tools documentation

Role	Description	Description
SOC Manager	The SOC Manager is responsible for overseeing operations overall and team management.	· People management. · Strategic management · SOC roadmap and strategy development · Reporting to higher management, stakeholders, etc. · SOC performance and KPI management
	Optional[1]	
Tier3 Analyst (Threat Hunter)	The Tier3 Analyst is a highly qualified expert who is primarily responsible for proactive threat hunting and high-level detection logic development. S/he may also be involved in incident response activity to address highly sophisticated threats and/or high-priority incidents.	· Threat hunting · Incident analysis and response (Tier3) · Detection logic development and tuning · Security monitoring system development · Tier2 Analyst work review
Vulnerability Assessment Expert	When a SOC scales enough, it becomes reasonable to allocate vulnerability assessment functions to a dedicated role. Also, it becomes essential to have an offensive security expert to organize red team exercises, to conduct attack simulations, etc. It's also very important for TTPs analysis and detection logic development.	· Vulnerability analysis, prioritizing and reporting · Penetration testing, red team exercises · Participation in detection logic testing (attack simulation)
SOC Security Engineer	The SOC Security engineer is responsible for engineering, integration, and deployment of SOC tools. Depending on the size, composition, and needs of the SOC, you may have a variety of security engineers in your team, who specialize in SIEM, endpoint security, and other specific areas of security engineering.	· Create and develop correlation rules, dashboards and reports (if applicable) · Sensor tuning and maintenances · Security monitoring system maintenance and development · Scripting & automation · Custom tools development
Legal Officer	The Legal Officer is responsible for the SOC's activities and processes from a compliance perspective.	· Provide advice on specific legal issues regarding SOC operations · Provide legal advice for stakeholders · Any other legal support for SOC team

Kaspersky offers: Cybersecurity Training Services

For more than 20 years, Kaspersky's cybersecurity expertise – including threat detection, malware research, reverse engineering and digital forensics – has been continuously evolving and advancing. Our experts understand how best to handle the threats posed by the 325,000 malware samples we encounter every day, and how to impart that knowledge and hands-on experience to organizations dealing with today's challenging, changeable cybersecurity environment.

Our Security Training Program has been designed and developed by the security authorities who helped build Kaspersky's anti-virus labs, and who now inspire and mentor the next generation of global experts.

Courses are designed to include both theoretical classes and practical labs. On completion of each course, students are invited to validate their knowledge through an evaluation.

Training courses are suitable for IT-related professionals possessing general or advanced system administration and programming skills. All courses are available either in-class on customer premises or at local or regional Kaspersky offices, as applicable.

Topics	Duration	Skills gained
Windows Digital Forensics		
Through a real-life simulated cyber targeted attack incident, the course covers the following topics: · Introducing digital forensics · Live response and evidence acquisition · Post-mortem analysis of Windows machines · Windows OS registry internals · Windows OS events · Windows OS artifacts analysis · Browsers artifacts forensics · Email analysis · Forensics challenges with SSD disks · Recommendations when building a digital forensics lab · Testing the newly gained skills with a practical challenge using different Windows artifacts	5 days	· Acquiring various digital evidence and dealing with it in forensically sound environment · Find traces of incident-related malicious activities from the Windows OS artifacts · Utilizing time stamps from different Windows artifacts to reconstruct an incident scenario · Finding and analyzing browser and email history · Be able be apply the tools and instruments of digital forensics · Understating the process of creating a digital forensics lab

[1] These roles relevance are highly dependent on a SOC's service portfolio and goals. For example, if the SOC is not responsible for threat hunting or vulnerability management, some team roles like "Tier 3 Analyst (Threat Hunter)" or "Vulnerability Assessment Expert" may be irrelevant.

Topics	Duration	Skills gained
Malware Analysis & Reverse Engineering		
• Basic analysis using IDA Pro • Dynamic analysis using popular virtualization solutions and debuggers • Malicious documents analysis • Unpacking • Decryption • Shellcodes analysis • Exploit analysis • Reversing tips and tricks	5 days	• Get preliminary knowledge about OS and assembly language • Conduct static and dynamic malware analysis obtaining full understanding of its behavior and functionality • Deal with malware anti-analysis tricks, self-protective techniques and protection software bypasses • Identify and reverse engineer standalone and embedded shellcodes • Be able to analyze PDF exploits from scratch
Advanced Windows Digital Forensics		
Through a real-life simulated targeted cyberattack incident, the course will cover the following topics: • Numerical systems • FAT file system • NTFS file system • Deep Windows forensics • Data and file recovery from file system, shadow copies and using file carving • Forensics challenges in Cloud computing • Memory forensics • Network forensics • Timeline vs SuperTimeline analysis • Testing the newly gained skills with a practical challenge with acquired digital evidence	5 days	• Conducting deep file system analysis • Identifying and recovering deleted files using different techniques • Analyzing network traffic with different tools • Identifying and tracking malicious activities in memory dump • Identifying and dumping interesting parts from memory for further analysis • Reconstructing the incident timeline using file system timestamps • Creating one timeline for all Windows OS artifacts for a better understating of the incident scenario
Advanced Malware Analysis & Reverse Engineering		
• Unpacking • Decryption • Developing own decryptors for common scenarios • Byte code decompilation • Code decomposition • Disassembly • Reconstruction of modern APT architectures • Recognizing typical code constructs • Identification of cryptographic and compression algorithms • Classification and attribution based on code and data • Class and structure reconstruction • APT plugin architectures (based on recent APT samples)	5 days	• Be able to analyze a modern APT toolkit, from receiving the initial sample, all the way to producing a technical description of the attacker's TTPs with IOCs • Producing static decryptors for real-life scenarios and then continuing with in-depth analysis of the malicious code • Be able to analyze malicious documents that are typically used to deliver initial payloads and know how to extract them • Ensuring damage assessment and incident response efforts are accurate and effective
Windows Incident Response		
In a real-life simulated environment, an incident will take place and the course will cover the following topics on that scenario: • Introducing the incident response process and its workflow • Explaining the difference between normal threats and APTs • Explaining APT Cyber Kill Chain • Applying the incident response process to different incident scenarios • Applying Cyber Kill Chain on the simulated environment • Applying live analysis on victim machines for first responders • Forensically sound evidence-acquisition techniques • Introducing post-mortem analysis and digital forensics • Introducing memory forensics • Log file analysis with regular expressions and ELK • Introducing cyber threat intelligence • Creating IoCs (Indicators of Compromise), with YARA and SNORT • Introducing malware analysis and sandboxing • Introducing network traffic forensics • Discussing incident analysis reporting and recommendations on building CSIRT • Testing the newly gained skills with a practical challenge in another simulated scenario	5 days	• Understanding the phases of incident response • What to consider while responding to a cyber incident • Understanding various attack techniques and targeted attack anatomy through the Cyber Kill Chain • Responding to different incidents with appropriate actions • The ability to differentiate APTs from other threats • Confirming cyber incidents using live analysis tools • Understanding the difference between live analysis and post-mortem - and when to apply each of them • Identifying digital evidence; HDD, memory and network traffic with an introduction on their forensics analysis • Writing YARA and SNORT IOCs for the detected attack • Log file analysis • Understanding the process involved in building an IR team
Efficient Threat Detection with Yara		
• Brief intro into Yara syntax • Tips & tricks to create fast and effective rules • Yara-generators • Testing Yara rules for false positives • Hunting new undetected samples on VT • Using external modules within Yara for effective hunting • Anomaly search • Lots (!) of real-life examples • A set of exercises for improving your Yara skills	2 days	• Create effective Yara rules • Test Yara rules • Improve them to the point where they find threats that nobody else does

Advanced Detection and Response Technologies

Today's advanced threat protection solutions are oriented towards working with the SIEM system, to help organizations build effective new SOCs and to enrich those already in place. This can be achieved in a number of ways.

First, this can be done by automating, where possible, the detection, analysis and response of manual tasks gives analysts doing alert triage the tools, the time and the head-space they need to apply their analytical skills effectively to things like working with threat data streams. For senior incident response and threat hunting teams, this time can be redirected into proactive threat hunting, the in-depth analysis of incidents and the development plans for an effective response to complex incidents.

Other ways are by ensuring that analysts have a full 360 degree view of the entire infrastructure, and by providing relevant logs to the SIEM, as well fast access to consolidated metadata, objects and verdicts. These last also help analysts work effectively even when compromised workstations are inaccessible, or when data has been encrypted by hackers.

All this enables the SOC team to better understand the complete sequence of intruder actions, while reducing the number of false positive alerts that analysts must deal with, and the time spent on prioritizing alerts.

Kaspersky Offers: Kaspersky Sandbox

Kaspersky's portfolio includes advanced anti-APT technologies with the highest detection rates in the industry – as proven by numerous independent tests. However, to effectively utilize these solutions, companies need to have a fully-fledged IT security department with the appropriate experience and expertise. This is not always the case in companies with geographically distributed infrastructure.

These companies usually have a central office with an integrated IT infrastructure containing a large number of workstations, servers, and other auxiliary elements. Regional offices are often heterogeneous, and may include large branches and small regional offices with poor local network and/or Internet access speed.

Kaspersky Anti Targeted Attack and Kaspersky EDR can be used to protect a central or large regional office. In the hands of experts from the Security Operations Center, these tools allow organizations to fully and promptly identify and defeat complex threats. However, medium-size branches and remote offices are not always able to use these solutions, due to a lack of resources and expertise. Budget constraints and the global shortage of specialists trained to deal with complex threats (making them expensive hires), are often the main factors that prevent companies from using these types of solutions in remote offices.

In this case, the most accessible and effective approach is to counter complex threats using Kaspersky Endpoint Security for Business with Kaspersky Sandbox.

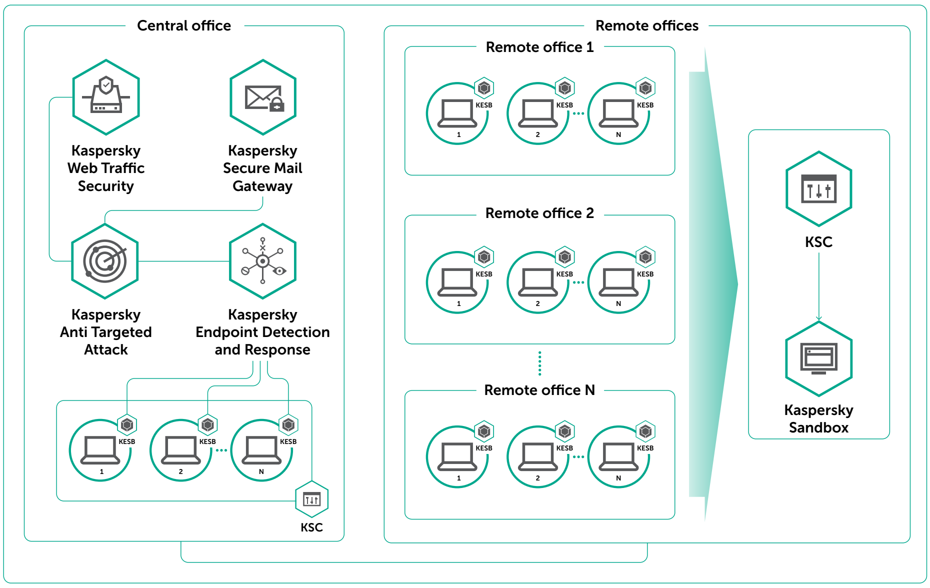

Central office
Kaspersky Web Traffic Security
Kaspersky Secure Mail Gateway
Kaspersky Anti Targeted Attack
Kaspersky Endpoint Detection and Response
KESB
1
2
N
KSC
Remote offices
Remote office 1
Remote office 2
Remote office N
KSC
Kaspersky Sandbox

Figure 5:
Kaspersky Sandbox in a large organization with a distributed network

Kaspersky Sandbox helps organizations combat the growing number and complexity of modern threats that can bypass existing endpoint protection. Complementing the functionality of Kaspersky Endpoint Security for Business, Kaspersky Sandbox allows organizations to significantly increase the level of protection for workstations and servers against previously unknown malware, new viruses and ransomware, zero-day exploits, and others – without the need for highly specialized information security analysts.

How it works

Kaspersky Sandbox harnesses our expert best practices in combating complex threats and APT-level attacks, and is tightly integrated with Kaspersky Endpoint Security for Business. It's managed from Kaspersky Security Center, our unified policy-based management console.

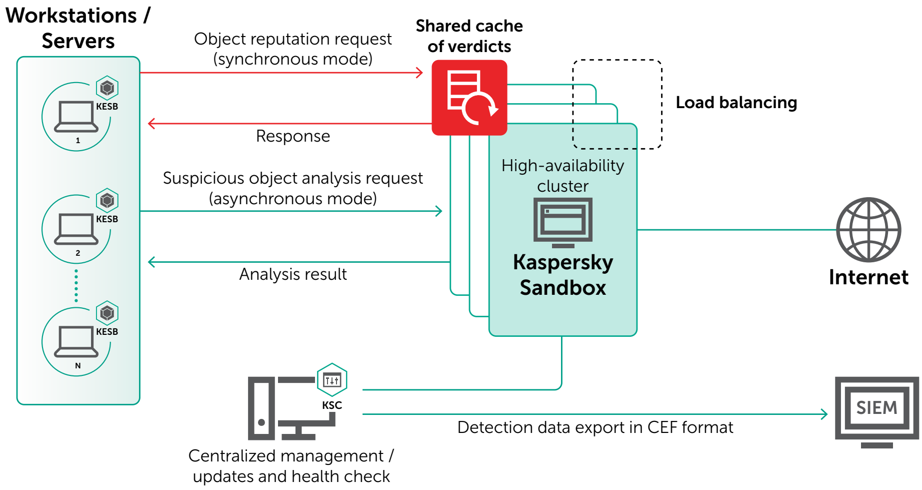

Workstations / Servers
KESB
1
2
N
Object reputation request (synchronous mode)
Shared cache of verdicts
Load balancing
Response
Suspicious object analysis request (asynchronous mode)
High-availability cluster
Kaspersky Sandbox
Internet
Analysis result
KSC
SIEM
Detection data export in CEF format
Centralized management / updates and health check

Figure 6: Kaspersky Sandbox

The Kaspersky Endpoint Security for Business agent requests data about a suspicious object from the shared operational cache of verdicts, located on the Kaspersky Sandbox server. If the object has already been scanned, Kaspersky Endpoint Security for Business receives the verdict and applies one or more remediation options:

- Remove and quarantine;
- Notify user;
- Start a critical areas scan;
- Search detected object on other machines within the managed network.

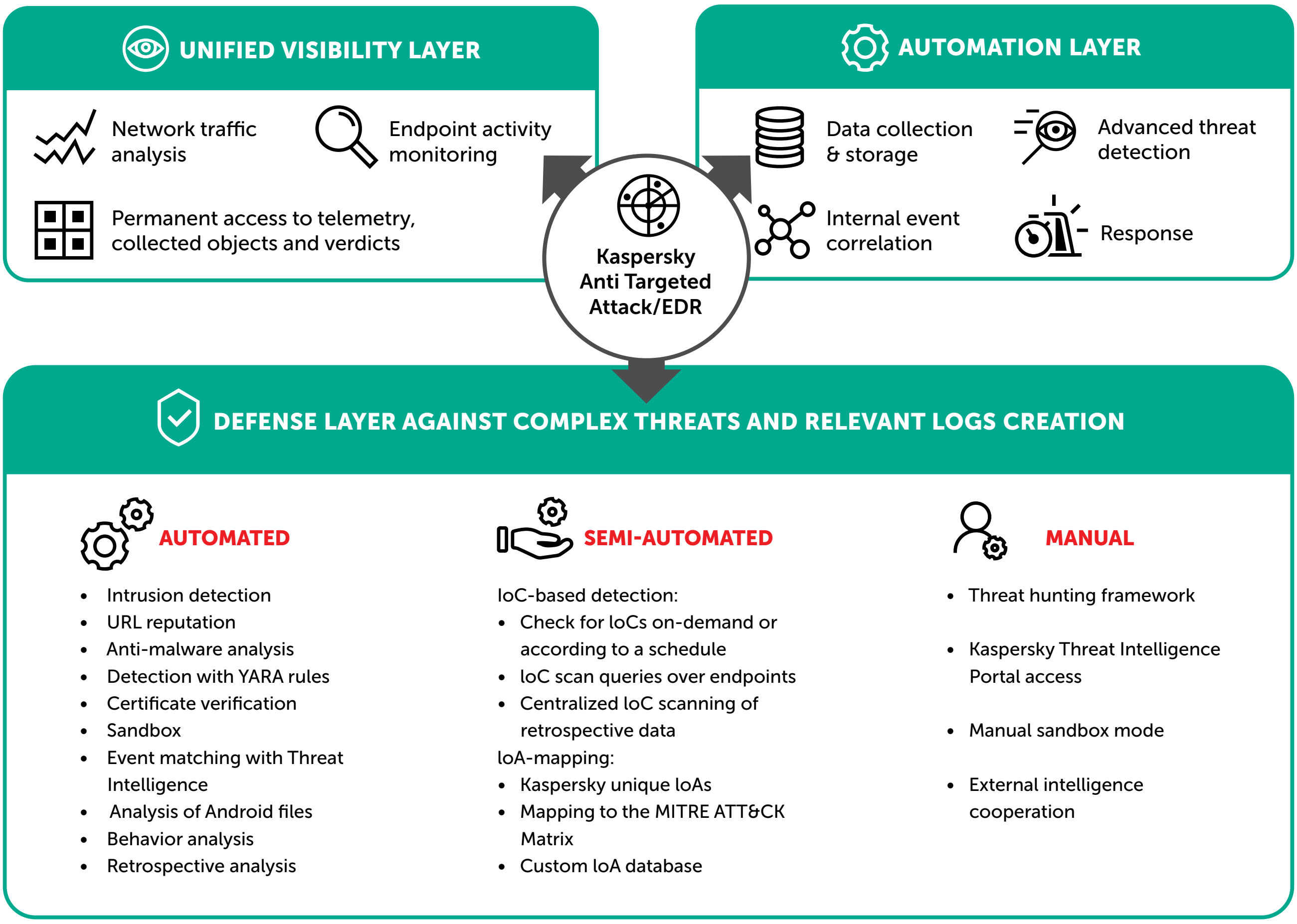
If the verdict on an object's reputation can't be obtained from cache, the Kaspersky Endpoint Security for Business agent sends the suspicious file to the Sandbox and waits for a response. The Sandbox receives a request to scan the object, at which point the test object is run in an environment isolated from the real infrastructure. File scanning is performed in virtual machines equipped with tools that emulate a typical working environment (operating systems/installed applications).To detect the malicious intent of an object, behavioral analysis is carried out, artifacts are collected and analyzed, and if the object performs malicious actions, the Sandbox recognizes it as malware. During sandbox analysis, a verdict is assigned to the object.

Once the object emulation process is complete, the resulting verdict is sent in real-time to the shared operational cache of verdicts, allowing other hosts with Kaspersky Endpoint Security for Business installed to quickly obtain data on the reputation of the scanned object without having to analyze the same file again. This approach ensures rapid processing of suspicious objects, reduces the load on Kaspersky Sandbox servers, and improves the speed and efficiency of the response to threats.

Kaspersky Sandbox allows organizations to significantly reduce outlay on IT security experts and associated costs by automating most of the tasks relating to advanced threat prevention. It automatically blocks advanced, unknown and complex threats without the need for additional resources, and frees up an organization's IT security analysts to focus on other tasks.

Kaspersky offers: Kaspersky Anti Targeted Attack and Kaspersky Endpoint Detection and Response

Kaspersky Anti Targeted Attack for network traffic analysis and Kaspersky Endpoint Detection and Response for endpoint level are based on one technological platform comprising a multi-dimensional, all-in-one solution that fully automates time-consuming evidence collection and routine manual tasks related to the processes of detecting threat traces, analyzing and responding to complex incidents.



UNIFIED VISIBILITY LAYER

- Network traffic analysis
- Endpoint activity monitoring
- Permanent access to telemetry, collected objects and verdicts

AUTOMATION LAYER

- Data collection & storage
- Advanced threat detection
- Internal event correlation
- Response

Kaspersky Anti Targeted Attack/EDR

DEFENSE LAYER AGAINST COMPLEX THREATS AND RELEVANT LOGS CREATION

AUTOMATED

- Intrusion detection
- URL reputation
- Anti-malware analysis
- Detection with YARA rules
- Certificate verification
- Sandbox
- Event matching with Threat Intelligence
- Analysis of Android files
- Behavior analysis
- Retrospective analysis

SEMI-AUTOMATED

IoC-based detection:

- Check for IoCs on-demand or according to a schedule
- IoC scan queries over endpoints
- Centralized IoC scanning of retrospective data

IoA-mapping:

- Kaspersky unique IoAs
- Mapping to the MITRE ATT&CK Matrix
- Custom IoA database

MANUAL

- Threat hunting framework
- Kaspersky Threat Intelligence Portal access
- Manual sandbox mode
- External intelligence cooperation

Figure 7:
Kaspersky Anti Targeted Attack and Kaspersky EDR

Our technologies serve as an invaluable data source for the SIEM, while providing powerful automated detection and threat hunting capabilities. Kaspersky Anti Targeted Attack and Kaspersky EDR include the following detection mechanisms: centralized NGAV, IoC scanning, IoA mapping, YARA rules, sandboxing, cloud-based ML-APK analysis, behavior analysis, certification checking, retrospective analysis, threat hunting framework, a built-in automated Threat Intelligence module and Threat Intelligence Portal access.

As a result, even sophisticated threats designed to bypass traditional security measures are detected, while your SOC is able to perform daily tasks more effectively and efficiently, without wasting time on routine tasks or flipping between multiple consoles. The costs involved in analyzing irrelevant logs are avoided, and the time needed for incident response can be significantly reduced.

Employing Kaspersky Anti Targeted Attack and Kaspersky Endpoint Detection and Response:

- Notably reduces the number of analyst hours wasted on tedious but necessary manual tasks around data collection and detection and response processes
- Contributes significantly to risk mitigation by boosting efficiency in the incident handling process
- Enriches the SIEM with new sources of relevant logs for correlation with logs provided by other systems, resulting in better control and effective investigation as well as significantly improved visibility, and minimizing time-to-action
- Provides a wider long-term approach to building the maturity of the SOC.

Product highlights:

- On-premises deployment makes sure no data is exposed outside the organization.
- Supports the analysis of more than a hundred file types.
- Advanced anti-evasion techniques
- User activity emulation.
- Custom images allowing to analyze threats across a range of operating systems and applications and only those that apply to real environments
- Separate analysis of each process to detect suspicious activities with associated network connections
- Detailed analysis reports, including all system activities, extracted files, network activities (PCAP) and visual graphs.
- Data export in STIX, JSON and CSV.
- Supports integration with Kaspersky Private Security Network.
- Manual file submission and RESTful API for seamless integration and automation of your security operations.

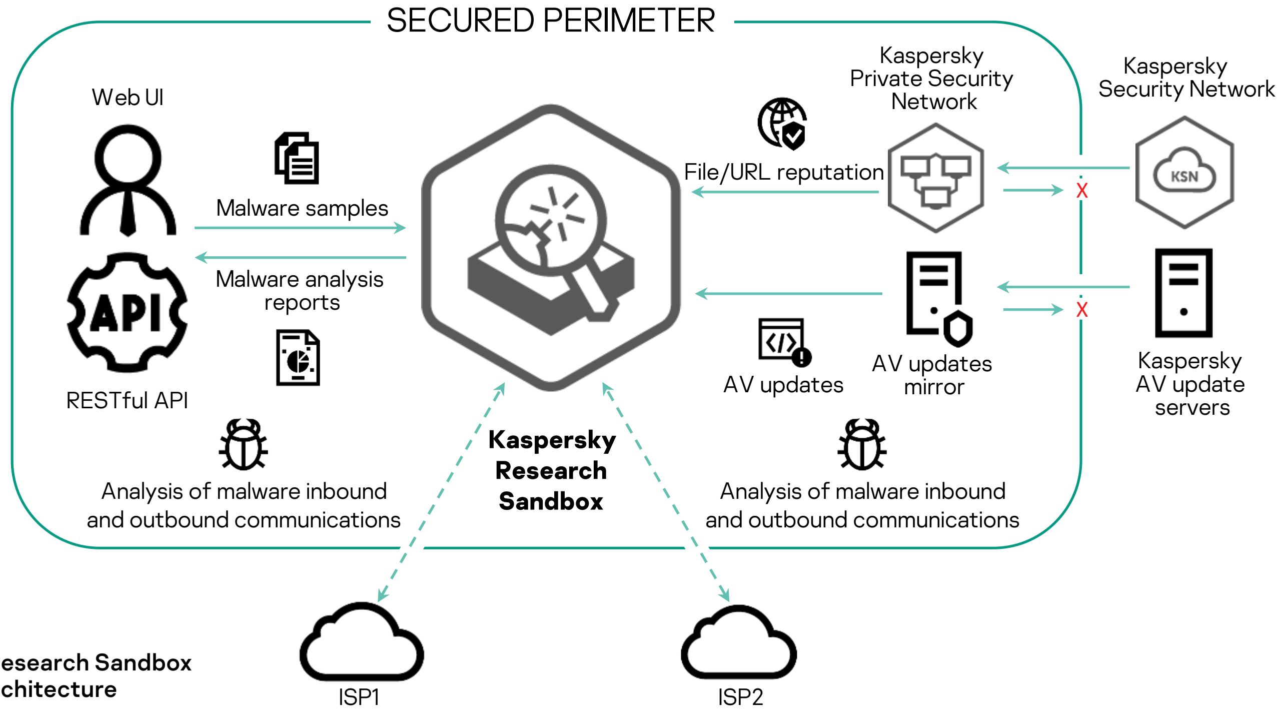
Kaspersky Offers: Research Sandbox

Making an intelligent decision based on a file's behavior while simultaneously analyzing the process memory, network activity, etc., is the optimal approach to understanding current sophisticated targeted and tailored threats. Sandboxing technologies are powerful tools that allow investigation of file sample origins, collection of IOCs based on behavioral analysis and detection of malicious objects not previously seen.

Today's malware uses a whole variety of methods to avoid executing its code if this could lead to exposing its malicious activity. If the system does not meet the required parameters, the malicious program will almost certainly destroy itself, leaving no traces. For the malicious code to execute, the sandboxing environment must therefore be capable of accurately mimicking normal end-user behavior.

Kaspersky Research Sandbox has been developed directly out of our in-lab sandboxing complex, a technology that's been evolving for over a decade. It incorporates all the knowledge about malware behaviors acquired by Kaspersky throughout our continuous threat research, allowing us to detect 350 000+ new malicious objects every day. Deployed on-premises, this powerful technology also prevents exposure of data outside the organization.

The diagram below describes the high-level architecture of Kaspersky Research Sandbox.



SECURED PERIMETER
Web UI
Malware samples
Malware analysis reports
RESTful API
Analysis of malware inbound and outbound communications
Kaspersky Research Sandbox
Kaspersky Private Security Network
File/URL reputation
Kaspersky Security Network
KSN
X
AV updates
AV updates mirror
X
Kaspersky AV update servers
Analysis of malware inbound and outbound communications
ISP1
ISP2

Figure 8:
Kaspersky Research Sandbox high-level architecture

It offers a hybrid approach, combining threat intelligence gleaned from petabytes of statistical data, behavioral analysis, and rock-solid anti-evasion, with human-simulating technologies. Kaspresky Research Sandbox also allows to customize images of the systems for analysis tailoring them to real environments, which increases the accuracy of threat detection and the speed of investigation.

Once that analysis is complete, Research Sandbox provides a detailed report on the behavior and functionality of the analyzed sample, allowing you to define the appropriate response procedures:

- **Summary** — general information about a file's execution results.
- **Sandbox detection names** — a list of detects (both AV and behavioral) that were registered during the file execution.
- **Triggered network rules** — a list of network SNORT rules that were triggered during analysis of traffic from the executed object.
- **Execution map** — a graphically represented sequence of object activities (actions taken on files, processes and the registry, and network activity) and the relationship between them. The root node of the tree represents the executed object.
- **Suspicious activities** — a list of registered suspicious activities.

- **Screenshots** — a set of screenshots that were taken during the file execution.
- **Loaded PE images** — a list of loaded PE images that were detected during the file execution.
- **File operations** — a list of file operations that were registered during the file execution.
- **Registry operations** — a list of operations performed on the OS registry that were detected during the file execution.
- **Process operations** — a list of interactions of the file with various processes that were registered during the file execution.
- **Synchronize operations** — a list of operations of created synchronization objects (mutex, event, semaphore) that were registered during the file execution.
- **Downloaded files** — a list of files that were extracted from network traffic during the file execution.
- **Dropped files** — a list of files that were saved (created or modified) by the executed file.
- **HTTPS/HTTP/DNS requests** — lists of HTTPS/HTTP/DNS requests that were registered during file execution.
- **Network traffic dump (PCAP)** — Network activity can be exported in PCAP format.

Kaspersky Research Sandbox is the instrument of choice for detecting unknown threats. It's more mature and more focused on advanced threats than any other solution.

Product highlights:

- Provides instant access to a repository of curated data about hundreds of APT actors and samples.
- Allows efficient automated or manual threat prioritization and alert triage.
- Functionality to add private actors and objects.
- Manual sample upload and open API for integration with automated workflows.
- Out-of-the-box integration with the Kaspersky Reserach Sandbox
- ESXi-ready.
- Supports fully on-premises deployment option.
- Maintains absolute privacy and confidentiality of all submissions to avoid exposing sensitive information.

Kaspersky Offers: Threat Attribution Engine[1]

The scale of cyberattacks continues to grow worldwide. Nation-sponsored cyberattacks and targeted attacks have reached a level of intensity never previously witnessed. Professional cybercrime organizations, political "hacktivists" and state-sponsored groups have become more technologically advanced, in many cases outpacing the skills and resources of security teams.

However, attackers often reuse code and techniques from previous attacks. Both by recognizing the reused elements from previous attacks and by detecting patterns in the types of modification and reuse observed, we can more rapidly develop defenses, make hypotheses about the source of the malware, and predict and prepare to defend against future attacks.

Kaspersky Threat Attribution Engine is an unrivaled malware analysis tool for security teams based on the biggest repository of APT threats investigated by our Global Research and Analysis Team. It can quickly link a new attack to known APT malware, previous targeted attacks and hacker groups. The tool helps to see the high-risk threat among less serious incidents and take timely protective measures to prevent an attacker from gaining a foothold in the system.

[1] Will be released in Q2 2020

How it works

Kaspersky Threat Attribution Engine analyzes the "genetics" of malware (i.e. reverse engineered representations of the original file) looking for code similarity with previously investigated APT samples and linked actors in an automated way. It compares the "genes", i.e. extracted code strings, of file analyzed with the APT malware samples database and provides a report on malware origin, threat actors and file similarity with known APT samples. Moreover, the product allows security teams to add private actors and objects to its database. The automation of reverse engineering analysis dramatically improves malware analysis and incident response times and allows timely prioritization of threats.

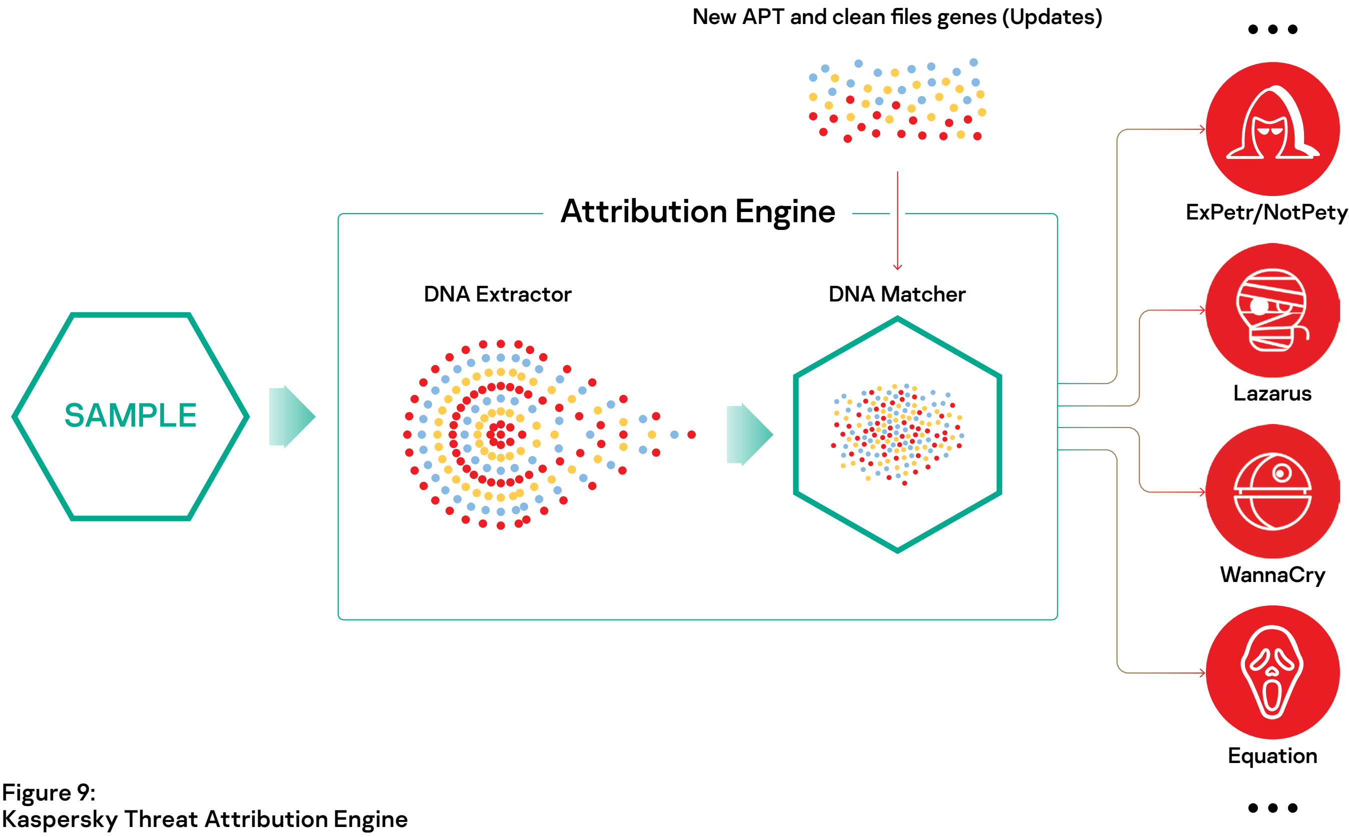


Figure 9:
Kaspersky Threat Attribution Engine

First, the Kaspersky Threat Attribution Engine extracts relevant code strings ("genes") that meet certain criteria. It's important to note that the final genome database contains more than 10 000 genes. Then it calculates the reputation score out of over 3 billion samples collected over more than 20 years of Kaspersky research, and shows all bad and good "genotypes" (group of distinctive genes). Finally, it reveals the sample's genotype and code attribution, providing the customer with insights into the malware's origin and its possible authors.

Kaspersky Attribution Engine improves security operations helping to:

- Rapidly attribute files to known APT actors to reveal motivations, methods and tools behind cyber incidents;
- Quickly evaluate if you are the target of attack or a side victim to setup proper containment and response procedures;
- Ensure effective and timely threat mitigation according to actionable threat intelligence on the APT family provided in Kaspersky APT Intelligence Reporting.[2]

[2] A subscription to Kaspersky APT Intelligence Reporting needs to be purchased separately

Threat Intelligence

SOCs were traditionally built to provide:

- Security device management, perimeter maintenance and preventive security technologies such as IPS/IDS, firewalls, proxies etc.;
- Security event monitoring through a Security Information and Event Management (SIEM) system;
- Incident response and remediation;
- Internal or regulatory compliance (e.g. PCI-DSS).

Many organizations are now seeking to gain greater threat visibility by establishing their own SOCs. However, some organizations that already have a SOC still face many of the same problems as before. There are a number of reasons for this:

- Poor prioritization, meaning that real threats get buried among the thousands of insignificant security alerts received and analyzed each day;
- Incident remediation without a proper understanding of the TTPs (Tactics, Techniques and Procedures) of associated threat actors, resulting in advanced attacks being overlooked;
- A reactive incident approach, rather than proactively 'hunting out' threats lying undiscovered but active within the organization;
- No strategic overview of the existing threat landscape, or awareness of attacks on similar enterprises and the countermeasures available;
- Problems attracting adequate internal investment into specific security technologies, due to difficulties communicating the risks to business processes associated with security breaches to non-technical board level executives.

Based on these considerations, security leaders are advised to follow an intelligence-driven SOC approach. For the SOC to be effective, it must continuously accommodate new technologies and controls in line with sweeping changes in the threat environment.

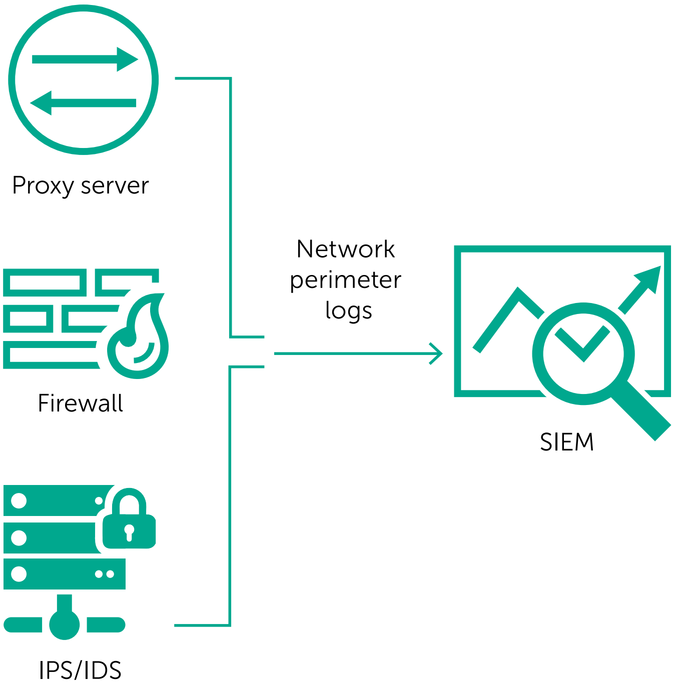
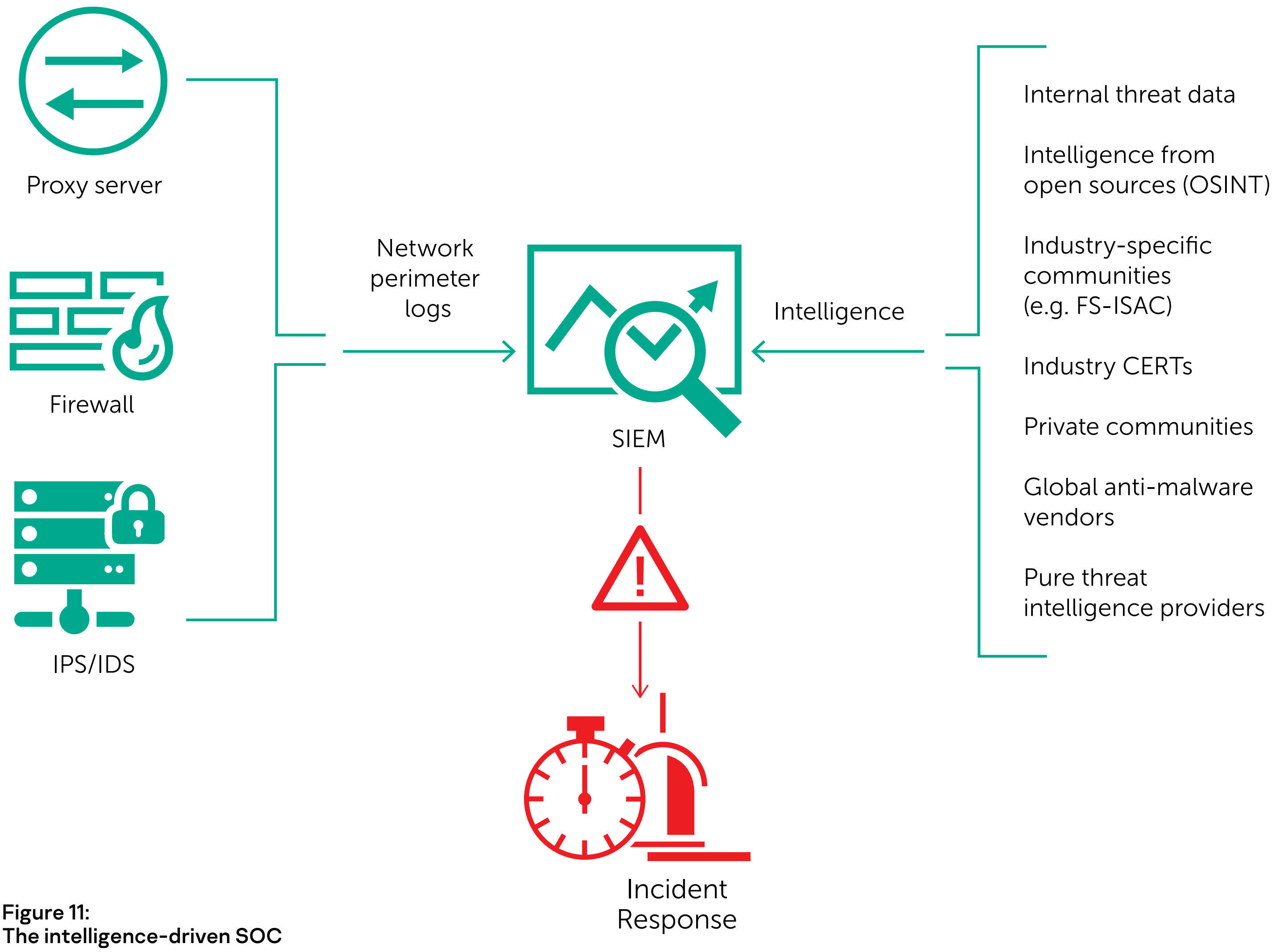


Figure 10:
A Conventional SOC

Gartner defines Threat Intelligence as: "Evidence-based knowledge, including context, mechanisms, indicators, implications and actionable advice about an existing or emerging menace or hazard to assets, that can be used to inform decisions regarding the subject's response to that menace or hazard."

Gartner, How Gartner Defines Threat Intelligence.

Combining internal threat data with information gathered from external, trusted and reliable sources (e.g. OSINT or global anti-malware vendors) provides an understanding of attack techniques and their potential indicators. This is turn allows organizations to develop efficient defensive strategies against commodity and advanced attacks targeting specific organizations.



Proxy server
Firewall
IPS/IDS
Network perimeter logs
SIEM
Intelligence
Internal threat data
Intelligence from open sources (OSINT)
Industry-specific communities (e.g. FS-ISAC)
Industry CERTs
Private communities
Global anti-malware vendors
Pure threat intelligence providers
Incident Response

Figure 11:
The intelligence-driven SOC

Intelligence sources should be carefully selected.

There's a direct correlation between the quality of intelligence used and the effectiveness of decisions made on the basis of this intelligence.

If you rely on intelligence that's irrelevant, inaccurate or not aligned with your industry or business goals, or if threat information is not received promptly, the quality of your organization's decision-making may be seriously compromised.

Raw data without context will not provide the relevance needed for SOC teams to be fully effective. For example, knowing that a specific URL is malicious is very different from also knowing that it's used to host an exploit or a specific type of malware. This additional layer of intelligence tells your security experts what to look out for as they investigate an incident.

There are still no common criteria for evaluating various commercial threat intelligence offerings, but here are some things to bear in mind when doing so:

- Look for intelligence with global reach. Attacks have no borders - an attack targeting a company in Latin America can be initiated from Europe and vice versa. Does the vendor source information globally and collate seeming disjoined activities into cohesive campaigns? This kind of intelligence will help you to take appropriate action.

- If you are looking for more strategic content to inform your long-term security planning, like:
  - High-level view of attack trends
  - Techniques and methods used by attackers
  - Motivations
  - Attributions, etc,

  then look for a threat intelligence provider with a proven track record of continuously uncovering and investigating complex threats in your region or industry. The ability of the provider to tailor its research capabilities to the specifics of your company is also critical.
- Context makes intelligence from data. Threat indicators without context are of no value - you should look for providers that help you to answer the important 'why does this matter?' questions. Relationship context (e.g. domains associated with the detected IP addresses or URLs where the specific file was downloaded from) provides additional value, boosting incident investigation and supporting better incident 'scoping' through uncovering newly acquired related Indicators of Compromise in the network.
- It's assumed that your company already has some security controls in place, with the associated processes defined, and that it's important for you to use threat intelligence with the tools you already use and know. So look for delivery methods, integration mechanisms and formats that support smooth integration of threat intelligence into your existing security operations.

Kaspersky offers: Threat Data Feeds

Kaspersky offers continuously updated Threat Data Feeds to inform your SOC team about risks and implications associated with cyberthreats, helping you to mitigate threats more effectively and to defend against attacks even before they are launched.

Feed description

- **IP Reputation Feed** — a set of IP addresses with context covering suspicious and malicious hosts.

- **Malicious URLs** — a set of URLs covering malicious links and websites. Masked and non-masked records are available.

- **Phishing URLs** — a set of URLs identified by Kaspersky as phishing sites. Masked and non-masked records are available.

- **Botnet C&C URLs** — a set of URLs of botnet command and control (C&C) servers and related malicious objects.

- **Ransomware URL Feed** — covering links that host ransomware objects or that are accessed by them.

- **Vulnerability Data Feed** – a set of security vulnerabilities with related threat intelligence (hashes of vulnerable apps/exploits, timestamps, CVEs, patches etc.).

- **APT IoC Feeds** — covering malicious domains, hosts, malicious IP addresses, malicious files used by adversaries to commit APT attacks.

- **Passive DNS (pDNS) Feed** — a set of records that contain the results of DNS resolutions for domains into corresponding IP addresses.

- **IoT URL Feed** — covering websites that were used to download malware that infects IoT devices.

- **Whitelisting Data Feed** — a set of file hashes providing third-party solutions and services with a systematic knowledge of legitimate software.

- **Malicious Hash Feed** — covering the most dangerous, prevalent and emerging malware.

- **Mobile Malicious Hash Feed** — a set of file hashes for detecting malicious objects that infect mobile platforms.

- **P-SMS Trojan Feed** — a set of Trojan hashes with corresponding context for detecting SMS Trojans ringing up premium charges for mobile users as well as enabling an attacker to steal, delete and respond to SMS messages.

- **Mobile Botnet C&C URLs** — a set of URLs with context covering mobile botnet C&C servers.

Service highlights

- Data Feeds are automatically generated in real time, based on findings across the globe (Kaspersky Security Network provides visibility to a significant percentage of all internet traffic, covering tens of millions of end-users in more than 200 countries) providing high detection rates and accuracy.
- Every record in each Data Feed is enriched with actionable context (threat names, timestamps, geolocation, resolved IPs addresses of infected web resources, hashes, popularity etc.). Contextual data helps reveal the 'bigger picture', further validating and supporting wide-ranging use of the data. Set in context, the data can more readily be used to answer the who, what, where, when questions which lead to identifying your adversaries, helping you to make timely decisions and take the actions which will specifically safeguard your organization.
- Simple lightweight dissemination formats (JSON, CSV, OpenIoC, STIX) via HTTPS or ad-hoc delivery mechanisms support the easy integration of feeds into security solutions.
- Threat Intelligence is generated and monitored by a highly fault-tolerant infrastructure, ensuring continuous availability and consistent performance.
- Out-of-the-box integration with HP ArcSight, IBM QRadar, Splunk and more.

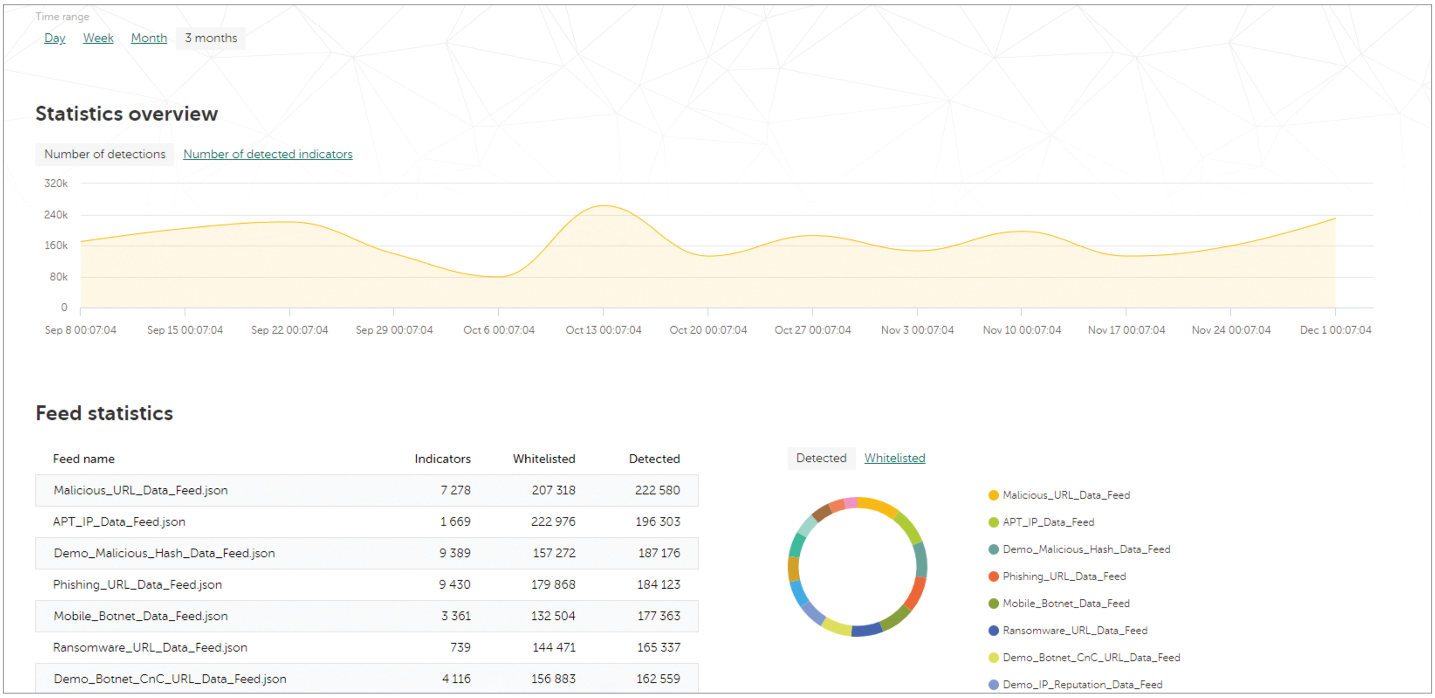
Kaspersky offers: Kaspersky CyberTrace

The number of security alerts processed by Security Operations Center's Tier 1 analysts every day is growing exponentially. With this amount of data being analyzed, effective alert prioritization, triage and validation becomes nearly impossible. There are too many blinking lights coming from numerous security products, leading to a significant number of alerts getting buried in the noise, and analyst burnout. SIEMs, log management and security analytics tools aggregating security data and correlating related alarms all help to reduce the number of alerts warranting additional examination, but Tier 1 specialists remain extremely overloaded.

Enabling effective alert triage and analysis

By integrating up-to-the-minute machine-readable threat intelligence into existing security controls, like SIEM systems, Security Operation Centers can automate the initial triage process while providing their Tier 1 specialists with enough context to immediately identify alerts that need to be investigated or escalated to Incident Response (IR) teams for further investigation and response. However, the continuing growth in the number of threat data feeds and available threat intelligence sources makes it difficult for organizations to determine what information is relevant for them. Threat intelligence is provided in different formats and includes a huge number of Indicators of Compromise (IoCs), making it hard for SIEMs or network security controls to digest them.

Kaspersky CyberTrace is a threat intelligence fusion and analysis tool enabling seamless integration of threat data feeds with SIEM solutions to help analysts leverage threat intelligence in their existing security operations workflow more effectively. It integrates with any threat intelligence feed (in JSON, STIX, XML and CSV formats) you might want to use (threat intelligence feeds from Kaspersky, other vendors, OSINT or your custom feeds), supporting out-of-the-box integration with numerous SIEM solutions and log sources. By automatically matching the logs against threat intelligence feeds, the Kaspersky CyberTrace provides real-time 'situational awareness', allowing Tier 1 analysts to make timely and better informed decisions.



Feed name	Indicators	Whitelisted	Detected
Malicious_URL_Data_Feed.json	7 278	207 318	222 580
APT_IP_Data_Feed.json	1 669	222 976	196 303
Demo_Malicious_Hash_Data_Feed.json	9 389	157 272	187 176
Phishing_URL_Data_Feed.json	9 430	179 868	184 123
Mobile_Botnet_Data_Feed.json	3 361	132 504	177 363
Ransomware_URL_Data_Feed.json	739	144 471	165 337
Demo_Botnet_CnC_URL_Data_Feed.json	4 116	156 883	162 559

Figure 12:
Kaspersky CyberTrace statistics

Kaspersky CyberTrace provides a set of instruments to operationalize threat intelligence for conducting effective alert triage and initial response:

- Demo threat data feeds from Kaspersky and OSINT feeds are available out-of-the-box;
- SIEM connectors for a wide range of SIEM solutions to visualize and manage data about threat detections;
- Feed usage statistics for measuring the effectiveness of the integrated feeds.
- On-demand lookup of indicators (hashes, IP addresses, domains, URLs) for in-depth threat investigation
- A web user interface providing data visualization, access to configuration, feed management, log parsing rules, blacklists and whitelists

- Advanced filtering for feeds (based on the context provided with each of the indicators, including threat type, geolocation, popularity, time stamps and more) and log events (based on custom conditions)
- Export of lookup results matching data feeds to CSV format for integration with other systems (firewalls, network and host IDS, custom tools)
- Bulk scanning of logs and files
- Command-line interface for Windows and Linux platforms
- Stand-alone mode, where Kaspersky CyberTrace is not integrated with a SIEM but receives and parses the logs from various sources such as networking devices
- Installation in DMZ-supporting scenarios where it needs to be isolated from the Internet.

The tool uses an internalized process of parsing and matching incoming data, which significantly reduces SIEM workload. Kaspersky CyberTrace parses incoming logs and events, rapidly matches the resulting data to feeds, and generates its own alerts on threat detection. A high-level architecture of the solution integration is shown in the Figure below:

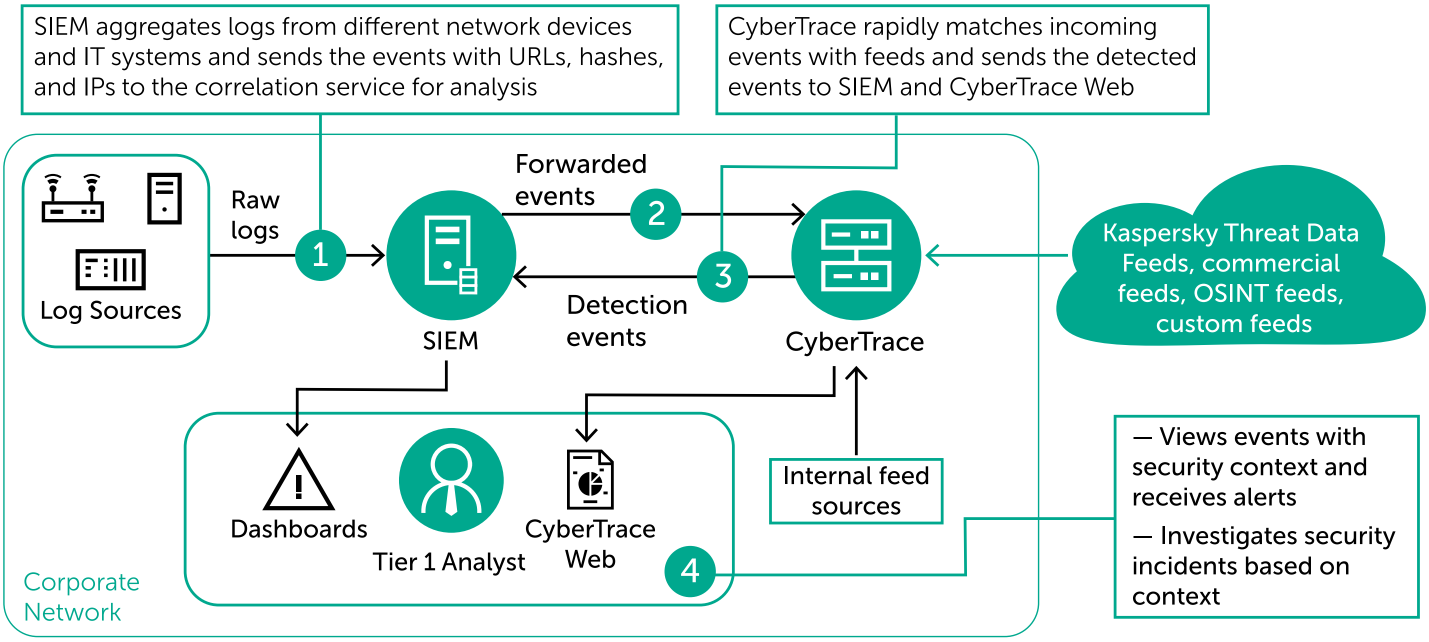

SIEM aggregates logs from different network devices and IT systems and sends the events with URLs, hashes, and IPs to the correlation service for analysis
CyberTrace rapidly matches incoming events with feeds and sends the detected events to SIEM and CyberTrace Web
Log Sources
Raw logs
1
SIEM
Forwarded events
2
3
Detection events
CyberTrace
Kaspersky Threat Data Feeds, commercial feeds, OSINT feeds, custom feeds
Dashboards
Tier 1 Analyst
CyberTrace Web
4
Internal feed sources
— Views events with security context and receives alerts
— Investigates security incidents based on context
Corporate Network

Figure 13:
Kaspersky CyberTrace integration scheme

Kaspersky also offers a set of continuously updated threat data feeds that can be integrated with the Kaspersky CyberTrace, enabling global threat visibility, timely detection of cyberthreats, prioritization of security alerts and effective response to information security incidents:

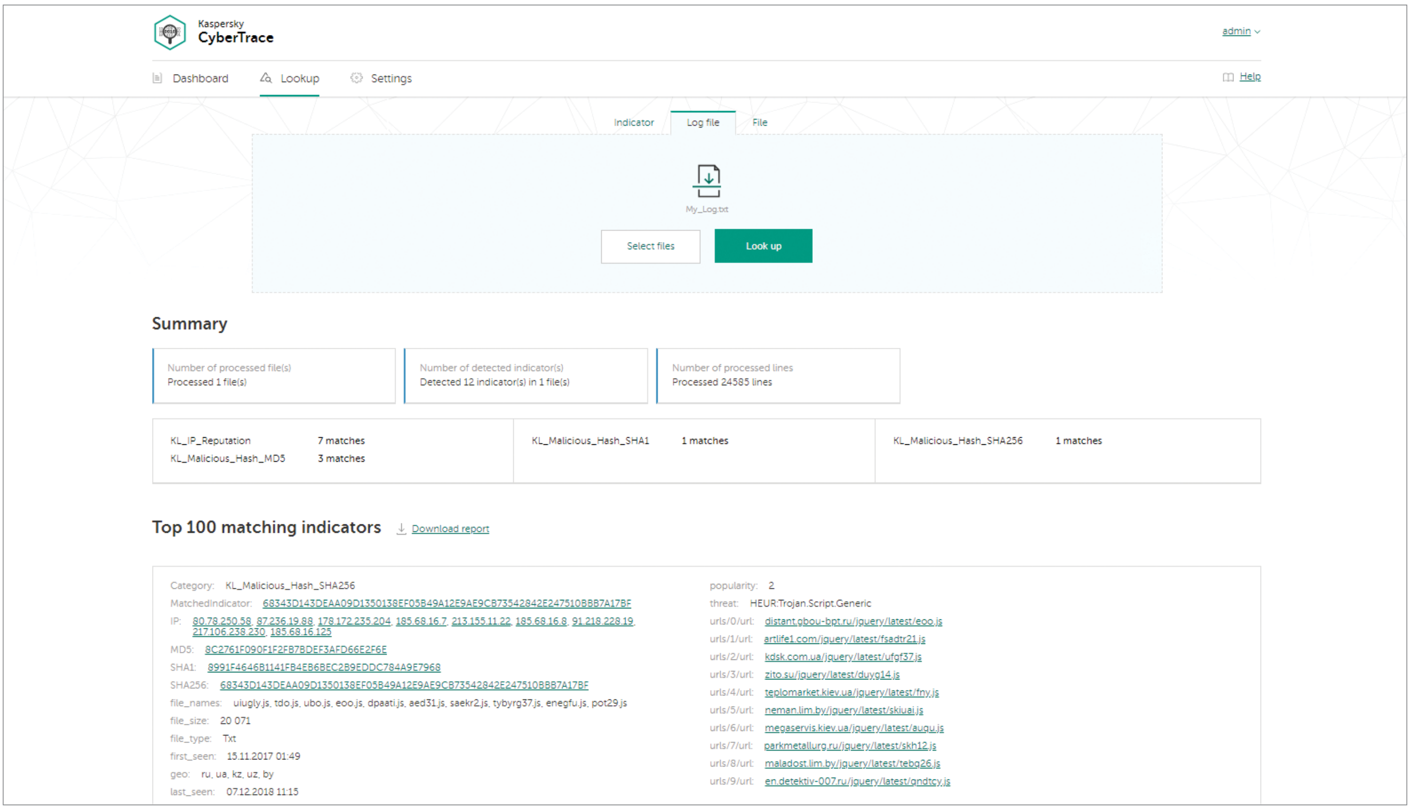
- IP reputation feed – a set of IP addresses with context covering different categories of suspicious and malicious hosts;
- Malicious and phishing URL feed – covering malicious and phishing links and websites;
- Botnet C&C URL feed – covering desktop botnet C&C servers and related malicious objects;
- Mobile botnet C&C URL feed – covering mobile botnet C&C servers;
- Ransomware URL feed – covering links that host ransomware objects or that are accessed by them;
- APT IoC feeds – covering malicious domains, hosts, malicious IP addresses, malicious files used by adversaries to commit APT attacks;
- Passive DNS (pDNS) feed – a set of records that contain the results of DNS resolutions for domains into corresponding IP addresses[3];
- IoT URL feed – covering websites that were used to download malware that infects IoT devices[4];
- Malicious hash feed – covering the most dangerous, prevalent and emerging malware;
- Mobile malicious hash feed – covering malicious objects that infect Android and iOS mobile platforms;
- P-SMS Trojan feed – covering SMS Trojans that enable attackers to steal, delete and respond to SMS messages, as well as clocking-up premium charges for mobile users;
- Whitelisting data feed – providing third-party solutions and services with a systematic knowledge of legitimate software.

[3] Integration will be supported in 2019
[4] Integration will be supported in 2019

Data feeds are aggregated from a combination of fused, heterogeneous and highly reliable sources, including Kaspersky Security Network and its 100+ million global users who voluntarily share their data on cyberthreats with us, our own web crawlers, botnet monitoring system (24/7/365 monitoring of all known botnets, their targets and activities), spam traps, threat research teams and trusted partners.

Then, in real-time, all this aggregated data is carefully inspected and refined using multiple preprocessing techniques, such as statistical criteria, Kaspersky Expert Systems (sandboxes, heuristics engines, multi-scanners, similarity tools, behavior profiling, etc.), analyst validation and whitelisting verification.

Every record in each data feed is supplied with rich actionable context (threat scoring, geolocation, threat names, timestamps, resolved IPs addresses of infected web resources, hashes, popularity, etc.).



Summary

Number of processed file(s)
Processed 1 file(s)

Number of detected indicator(s)
Detected 12 indicator(s) in 1 file(s)

Number of processed lines
Processed 24585 lines

KL_IP_Reputation	7 matches	KL_Malicious_Hash_SHA1	1 matches	KL_Malicious_Hash_SHA256	1 matches
KL_Malicious_Hash_MD5	3 matches				

Top 100 matching indicators Download report

Category: KL_Malicious_Hash_SHA256
MatchedIndicator: 68343D143DEAA09D1350138EF05B49A12E9AE9CB73542842E247510BBB7A17BF
IP: 80.78.250.58, 87.236.19.88, 178.172.235.204, 185.68.16.7, 213.155.11.22, 185.68.16.8, 91.218.228.19, 217.106.238.230, 185.68.16.125
MD5: 8C2761F090F1F2FB7BDEF3AFD66E2F6E
SHA1: 8991F4646B1141FB4EB6BEC2B9EDDC784A9E7968
SHA256: 68343D143DEAA09D1350138EF05B49A12E9AE9CB73542842E247510BBB7A17BF
file_names: uiugly.js, tdo.js, ubo.js, eoo.js, dpaati.js, aed31.js, saekr2.js, tybyrg37.js, enegfu.js, pot29.js
file_size: 20 071
file_type: Txt
first_seen: 15.11.2017 01:49
geo: ru, ua, kz, uz, by
last_seen: 07.12.2018 11:15

popularity: 2
threat: HEUR:Trojan.Script.Generic
urls/0/url: distant.gbou-bpt.ru/jquery/latest/eoo.js
urls/1/url: artlife1.com/jquery/latest/fsadtr21.js
urls/2/url: kdsk.com.ua/jquery/latest/ufgf37.js
urls/3/url: zito.su/jquery/latest/duyg14.js
urls/4/url: teplomarket.kiev.ua/jquery/latest/fny.js
urls/5/url: neman.lim.by/jquery/latest/skiuai.js
urls/6/url: megaservis.kiev.ua/jquery/latest/augu.js
urls/7/url: parkmetallurg.ru/jquery/latest/skh12.js
urls/8/url: maladost.lim.by/jquery/latest/tebg26.js
urls/9/url: en.detektiv-007.ru/jquery/latest/gndtcy.js

Figure 14:
Kaspersky Threat Data Feeds context

This contextual data helps reveal the 'bigger picture', further validating and supporting the wide-ranging use of the data. Set in context, the data can be more readily used to answer the 'who, what, where and when' questions which lead to identifying your adversaries and helping you make good decisions.

Although Kaspersky CyberTrace and Kaspersky Threat Data Feeds can be used separately, when used together they significantly strengthen your threat detection capabilities, empowering your security operations with global visibility into cyberthreats. With Kaspersky CyberTrace and Kaspersky Threat Data Feeds, Security Operations Center's analysts are able to:

- Effectively distill and prioritize sweeping amounts of security alerts
- Improve and accelerate triage and initial response processes
- Immediately identify alerts critical for the enterprise and make more informed decisions about which should be escalated to IR teams
- Form a proactive and intelligence-driven defense.

Kaspersky offers: Kaspersky Threat Intelligence Portal (Threat Lookup & Cloud Sandbox)

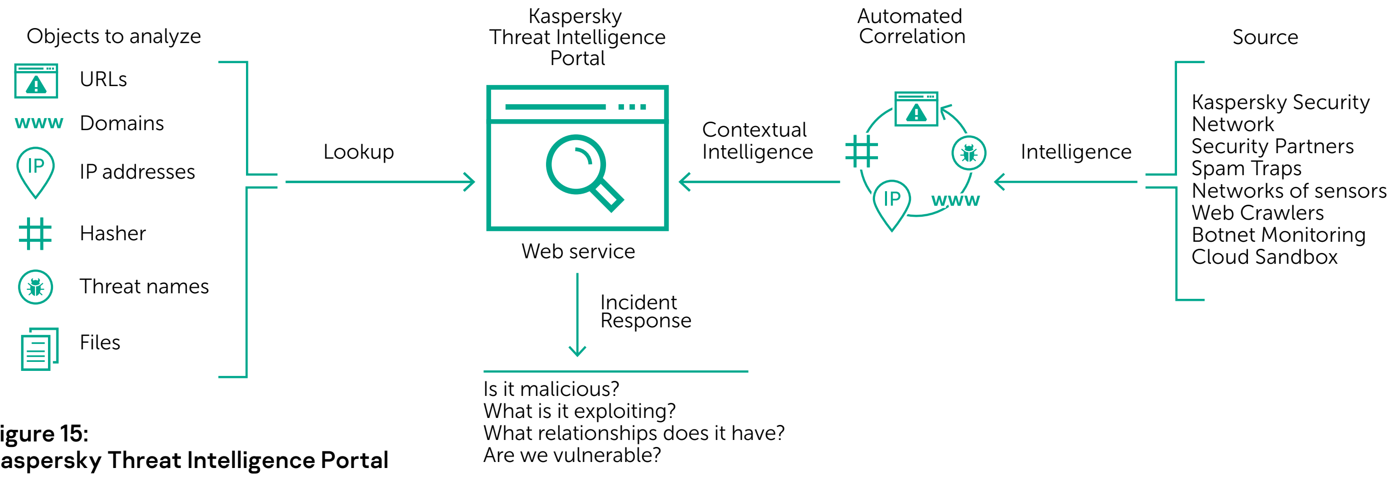


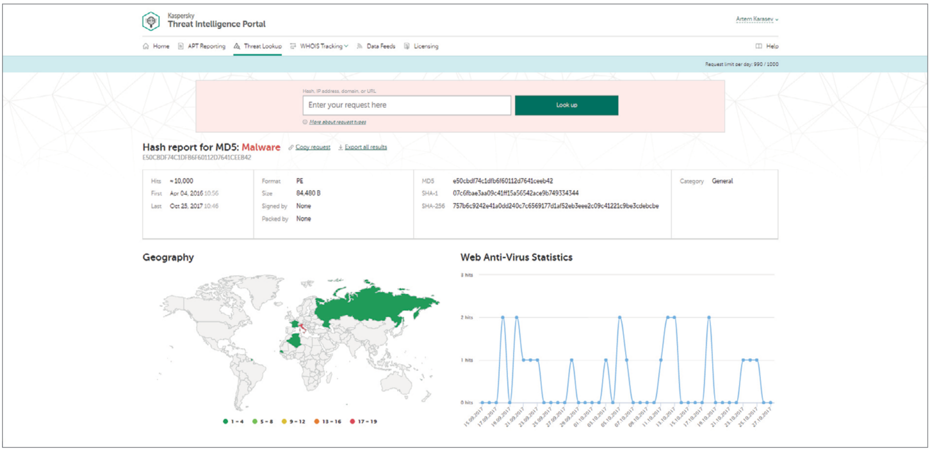
Figure 15:
Kaspersky Threat Intelligence Portal

Service highlights

- **Trusted Intelligence:** A key attribute of Kaspersky Threat Intelligence Portal is the reliability of our threat intelligence data, enriched with actionable context. Kaspersky products lead the field in anti-malware tests3, demonstrating the unequalled quality of our security intelligence by delivering the highest detection rates, with near-zero false positives.
- **Threat Hunting:** Be proactive in preventing, detecting and responding to attacks, to minimize their impact and frequency. Track and aggressively eliminate attacks as early as possible. The earlier you can discover a threat – the less damage is caused, the faster repairs take place and the sooner network operations can get back to normal.
- **Sandbox Analysis:** Detect unknown threats by running suspicious objects in a secure environment, and review the full scope of threat behavior and artifacts through easy-to-read reports.
- **Wide Range of Export Formats:** Export IOCs (Indicators of Compromise) or actionable context into widely used and more organized machine-readable sharing formats, such as STIX, OpenIOC, JSON, Yara, Snort or even CSV, to enjoy the full benefits of Threat Intelligence, automate operations workflow, or integrate into security controls such as SIEMs.
- **Easy-to-use Web Interface or RESTful API:** Use the service in manual mode through a web interface (via a web browser) or access via a simple RESTful API.

Kaspersky Threat Intelligence Portal delivers all the knowledge acquired by Kaspersky about cyberthreats and their relationships, brought together into a single, powerful web service. The goal is to provide your SOC teams with as much data as possible, preventing cyberattacks before they impact your organization. The Portal retrieves the latest detailed threat Intelligence about URLs, domains, IP addresses, file hashes, threat names, statistical/behavior data, WHOIS/DNS data, file attributes, geolocation data, download chains, timestamps, while the Cloud Sandbox allows that knowledge to be linked to the IOCs generated by the analyzed sample. The result is global visibility of new and emerging threats, helping you secure your organization and boosting incident response.

Threat intelligence delivered by Kaspersky Threat Intelligence Portal is generated and monitored in real time by a highly fault-tolerant infrastructure, ensuring continuous availability and consistent performance. Hundreds of experts, including security analysts from across the globe, world-famous security experts from our GReAT team and leading-edge R&D teams, all contribute to generating valuable real-world threat intelligence.



Request limit per day: 990 / 1000

Hash report for MD5: Malware
E50CBDF74C1DFB6F60112D7641CEEB42

Hits ≈ 10,000
First Apr 04, 2016 10:56
Last Oct 25, 2017 10:46

Format PE
Size 84,480 B
Signed by None
Packed by None

MD5 e50cbdf74c1dfb6f60112d7641ceeb42
SHA-1 07c6fbae3aa09c41ff15a56542ace9b749334344
SHA-256 757b6c9242e41a0dd240c7c6569177d1af52eb3eee2c09c41221c9be3cdebcbe

Category General

Figure 16:
Kaspersky Threat Intelligence Portal

5 http://www.kaspersky.com/top3

Kaspersky offers: APT Intelligence Reporting

Not all Advanced Persistent Threat discoveries are reported immediately, and many are never publicly announced. Be the first to receive our latest research with our exclusive, in-depth, actionable intelligence reporting on APTs.

Our Research

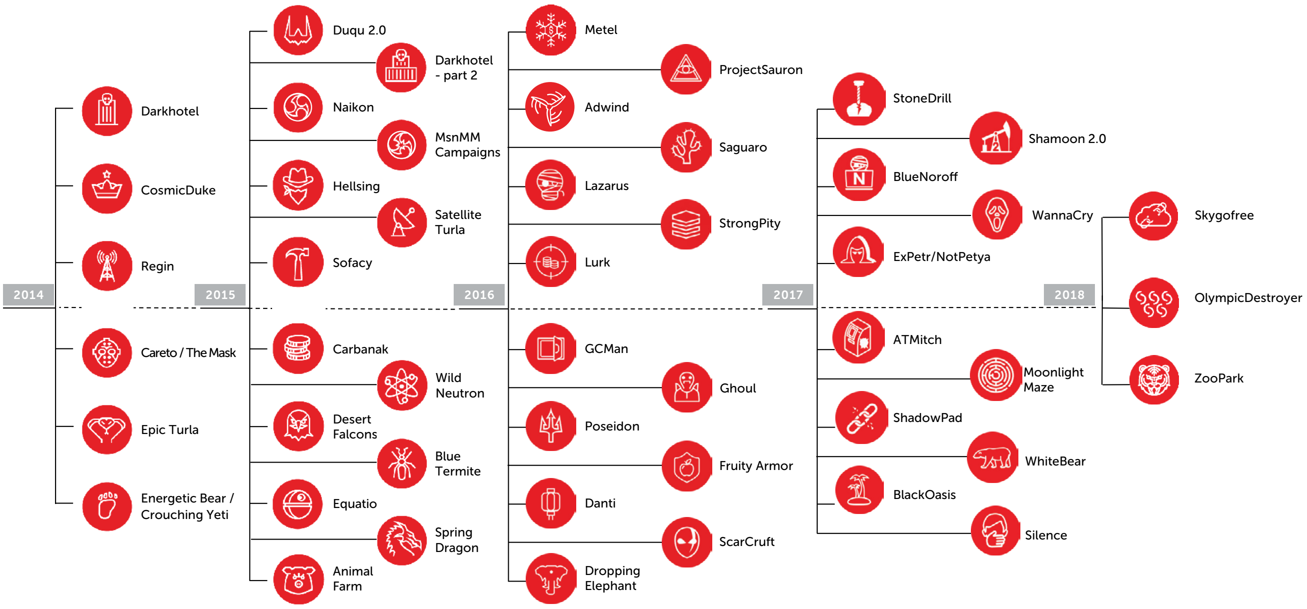


Figure 17:
Kaspersky's publicly announced APT investigations

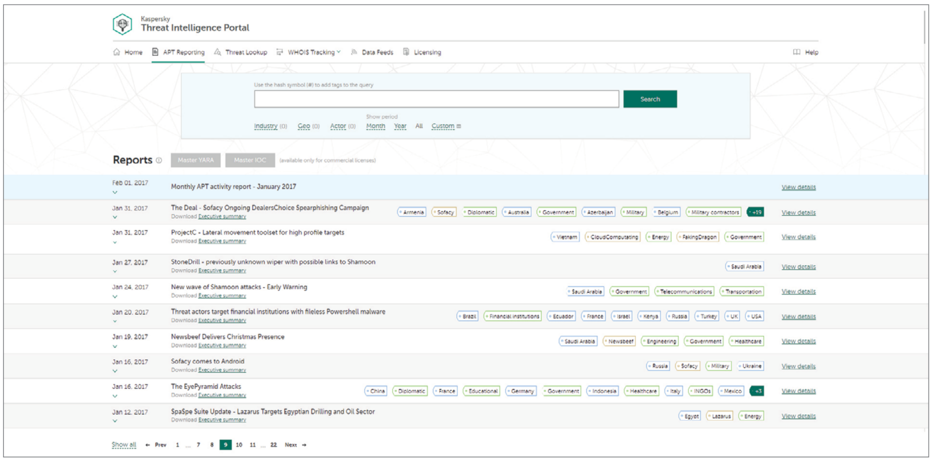
Service highlights

- Exclusive access to technical descriptions of cutting-edge threats during the ongoing investigation, before public release. More than 100 APT reports were issued in 2017.
- Insight into non-public APTs. Not all high profile threats are subject to public notification. Some, due to the victims who are impacted, the sensitivity of the data, the nature of the vulnerability fixing process or associated law enforcement activity, are never made public. But all are reported to our customers.
- Detailed supporting technical data, including an extended list of Indicators of Compromise (IOCs), available in openIOC format, and access to our Yara Rules.
- Continuous APT campaign monitoring. Access to actionable intelligence during the investigation (information on APT distribution, IOCs, C&C infrastructure).
- Retrospective analysis – access to all previously issued private reports is provided throughout the period of your subscription.

As a subscriber to Kaspersky APT Intelligence Reporting, you are provided with unique ongoing access to our investigations and discoveries, including full technical data supplied in a range of formats, on each APT revealed, including all those threats that will never be made public. Our experts, the most skilled and successful APT hunters in the industry, will also alert you immediately to any changes they detect in the tactics of cybercriminal groups. Furthermore, you will have access to Kaspersky's complete APT reports database – another powerful research and analysis component of your corporate security armory.

From a practical perspective, Indicators of Compromise are the most actionable part of the report for SOC experts. This structured information is provided for subsequent use with specific automated tools that help check your infrastructure for signs of infection.

All reports are available via the web interface or can be accessed via RESTful API.



Feb 01, 2017	Monthly APT activity report - January 2017		View details
Jan 31, 2017	The Deal - Sofacy Ongoing DealersChoice Spearphishing Campaign Download Executive summary	Armenia, Sofacy, Diplomatic, Australia, Government, Azerbaijan, Military, Belgium, Military contractors, +19	View details
Jan 31, 2017	ProjectC - Lateral movement toolset for high profile targets Download Executive summary	Vietnam, CloudComputating, Energy, FakingDragon, Government	View details
Jan 27, 2017	StoneDrill - previously unknown wiper with possible links to Shamoon Download Executive summary	Saudi Arabia	View details
Jan 24, 2017	New wave of Shamoon attacks - Early Warning Download Executive summary	Saudi Arabia, Government, Telecommunications, Transportation	View details
Jan 20, 2017	Threat actors target financial institutions with fileless Powershell malware Download Executive summary	Brazil, Financial institutions, Ecuador, France, Israel, Kenya, Russia, Turkey, UK, USA	View details
Jan 19, 2017	Newsbeef Delivers Christmas Presence Download Executive summary	Saudi Arabia, Newsbeef, Engineering, Government, Healthcare	View details
Jan 16, 2017	Sofacy comes to Android Download Executive summary	Russia, Sofacy, Military, Ukraine	View details
Jan 16, 2017	The EyePyramid Attacks Download Executive summary	China, Diplomatic, France, Educational, Germany, Government, Indonesia, Healthcare, Italy, INGOs, Mexico, +3	View details
Jan 12, 2017	SpaSpe Suite Update - Lazarus Targets Egyptian Drilling and Oil Sector Download Executive summary	Egypt, Lazarus, Energy	View details

Figure 18:
APT Intelligence Reporting

Kaspersky offers: Tailored Threat Intelligence Reporting

Customer-specific Threat Intelligence Reporting

What's the best way to mount an attack against your organization? Which routes, and what information, are available to an attacker specifically targeting you? Has an attack already been mounted, or are you about to come under threat?

Kaspersky Customer-specific Threat Reporting answers these questions and more, as our experts piece together a comprehensive picture of your current attack status, identifying weak spots ripe for exploitation and revealing evidence of past, present and planned attacks.

Empowered by these unique insights, you can focus your defense strategy on areas pinpointed as cybercriminals' prime targets, acting quickly and with precision to repel intruders and minimize the risk of a successful attack.

Developed using open source intelligence (OSINT), deep analysis of Kaspersky expert systems and databases and our knowledge of underground cybercriminal networks, these reports cover areas including:

- Identification of threat vectors: Identification and status analysis of externally available critical components of your network –including ATMs, video surveillance and other systems using mobile technologies, employee social network profiles and personal email accounts – that are potential targets for attack;

- Malware and cyberattack tracking analysis: Identification, monitoring and analysis of any active or inactive malware samples targeting your organization, any past or present botnet activity and any suspicious network based activity;

- Third-party attacks: Evidence of threats and botnet activity specifically targeting your customers, partners and subscribers, whose infected systems could then be used to attack you;

- Information leakage: through discreet monitoring of underground online forums and communities, we discover whether hackers are discussing attack plans with you in mind or, for example, if an unscrupulous employee is trading information;

- Current attack status: APT attacks can continue undetected for many years. If we detect a current attack affecting your infrastructure, we provide advice on effective remediation.

Quick start – easy to use – no resources needed

Once parameters (for customer-specific reports) and preferred data formats are established, no additional infrastructure is needed to start using this Kaspersky service.

Kaspersky Threat Intelligence Reporting has no impact on the integrity and availability of resources,including network resources.

Country-specific Threat Intelligence Reporting

The cybersecurity of a country includes protection of all its major institutions and organizations. Advanced persistent threats (APTs) against government authorities can affect national security; possible cyberattacks against manufacturing, transportation, telecommunication, banking and other pivotal industries can lead to significant damage on the state level, like financial losses, production accidents, blockage of network communications, and popular discontent.

Having an overview of the current attack surface and the current trends in malware and hacker attacks targeting your country, you can focus your defense strategy on areas pinpointed as cybercriminals' prime targets, acting fast and with precision to repel intruders and minimize the risk of successful attacks.

Created using approaches ranging from Open Source Intelligence (OSINT) to deep analysis of Kaspersky expert systems and databases, and our knowledge of the underground cybercriminal networks, country-specific threat reports cover areas including:

- **Identification of threat vectors:** identification and status analysis of externally available critical IT resources of the country – including vulnerable government applications, telecommunication equipment, industrial control systems' components (such as SCADA, PLCs, etc.), ATMs, etc.

- **Malware and cyberattack tracking analysis:** identification and analysis of APT campaigns, active or inactive malware samples, past or present botnet activity, and other notable threats targeting your country, based on data available in our unique internal monitoring resources.
- **Information leakages:** through clandestine monitoring of underground forums and online communities, we discover whether hackers are discussing attack plans with certain organizations in mind. We also reveal notable compromised accounts, which could pose risks to suffered organizations and institutions (for instance, accounts belonging to government agencies' employees available in the Ashley Madison breach, which could be used for blackmailing).

Kaspersky Threat Intelligence Reporting has no impact on the integrity and availability of the network resources being inspected. The service is based on non-intrusive network reconnaissance methods, and analysis of information available in open sources and resources of limited access.

At the conclusion of the service you will be provided with a report containing a description of notable threats for different state industries and institutions, as well as additional information on detailed technical analysis results. Reports are delivered via encrypted email messages.

The service can be provided as a one-time project or periodically under subscription (for example, quarterly).

More about Kaspersky Threat Intelligence Sources

Threat Intelligence is aggregated from a fusion of heterogeneous and highly reliable sources, including the Kaspersky Security Network (KSN) and our own web crawlers, our Botnet Monitoring service (24/7/365 monitoring of botnets and their targets and activities), spam traps, research teams, partners and other historical data about malicious objects collected by Kaspersky over almost two decades. Then, in real time, all aggregated data is carefully inspected and refined using multiple preprocessing techniques, such as statistical criteria, Kaspersky Expert Systems (sandboxes, heuristics engines, similarity tools, behavior profiling etc.), analyst validation and whitelisting verification.

With appropriately skilled and trained people in place, and Threat Intelligence acquired from reliable sources and implemented into existing security controls, it's time to consider your Incident Response.

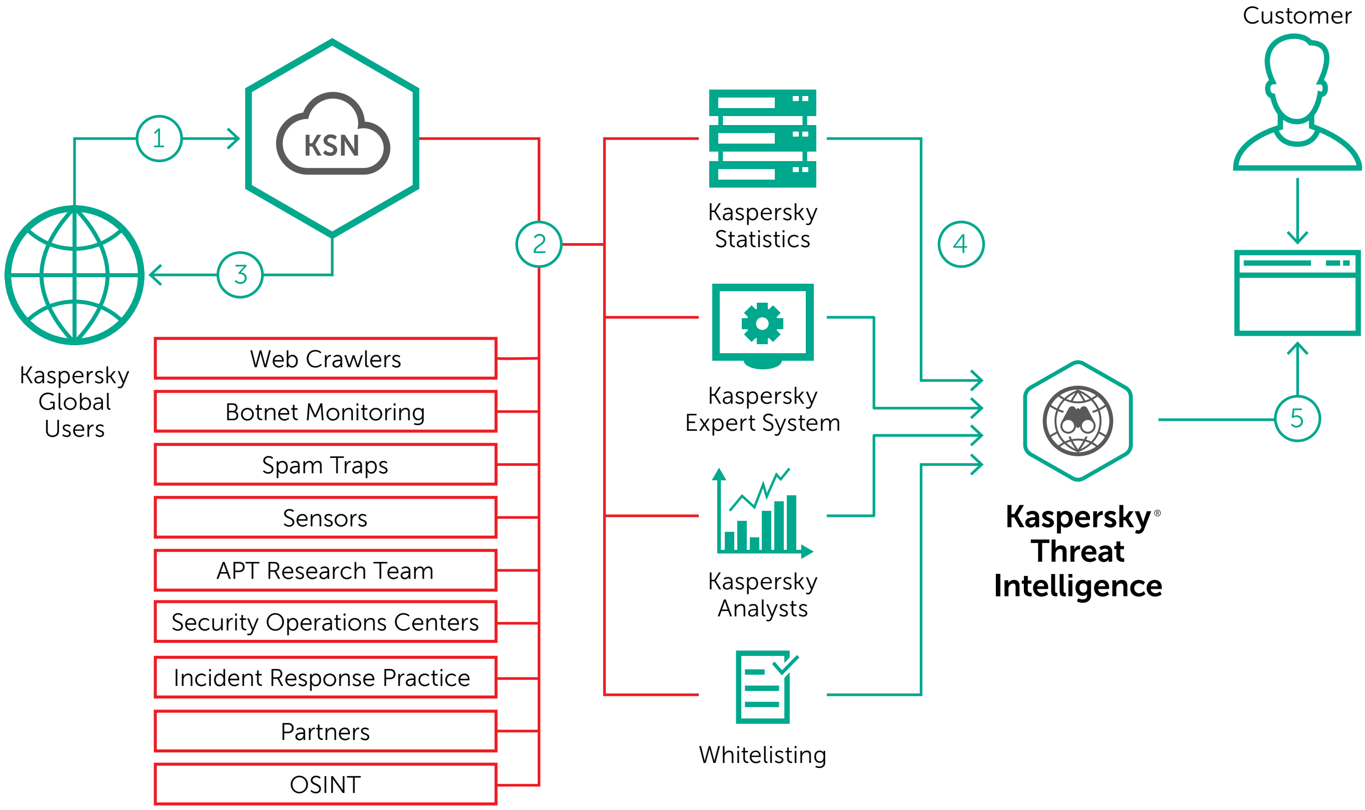


Figure 19:
Kaspersky's Threat Intelligence Sources

Threat Hunting

Threat hunting is also an important element of everyday SOC operations. This is not a new concept. The detection of unknown and advanced threats relies on the painstaking, hands-on efforts of security analysts, rather than automated rules or signature-based detection mechanisms.

Modern attacks 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 modern-day attacks:

- The use of tools to hamper digital forensics, e.g. by securely deleting artifacts 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. Threat hunting can 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.

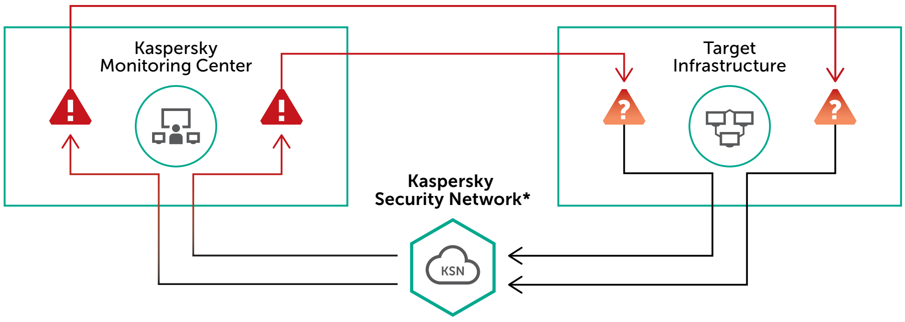
But neither automated threat detection and prevention tools nor cyberthreat hunting alone is a silver bullet for the entire modern spectrum of threats. A combination of traditional detection and prevention tools active before a compromise occurs, plus a post-compromise iterative process of searching for new threats missed by automated tools, can be effective.

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 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 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.

Kaspersky offers: 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 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.



*Kaspersky Private Security Network for isolated Infrastructures

Figure 20:
Kaspersky Managed 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.

Incident Investigation and Response

Forensics and incident response requires the allocation of considerable internal resources at little or no notice. Knowledgeable specialists, armed with extensive practical experience of fighting cyberthreats, will need to act quickly to identify, isolate and block malicious activity. Speed is of the essence, if consequences and remediation costs are to be minimized.

Mastering this level of expertise at short notice can be challenging, even for a well-established SOC team – few organizations have sufficient in-house resources on hand to stop an advanced attack in its tracks. Additionally, there may be cases, e.g. complex state-sponsored threats or APTs, where the SOC Team lacks expert knowledge of the specific approaches and tactics used by the APT actors involved.

In cases like these, it may be more cost-effective and productive to collaborate with a third-party Incident Response vendor or consultancy, who will be geared up to applying a rapid, fully-informed response.

A comprehensive Incident Response Framework should include:

- **Incident Identification**
  Initial incident analysis and isolation of the infected systems
- **Evidence acquisition**
  Depending on the type of the incident, different sources will need to be inspected to obtain the necessary evidence
- **Forensic Analysis (if required)**
  At this stage, a detailed picture of the incident can be established
- **Malware Analysis (if required)**
  To gain an understanding of given malware capabilities
- **Remediation Plan**
  Development of a plan to eradicate both the root cause of the problem and all traces of the malicious code
- **Lessons learned**
  Existing security controls review and update to prevent similar incidents

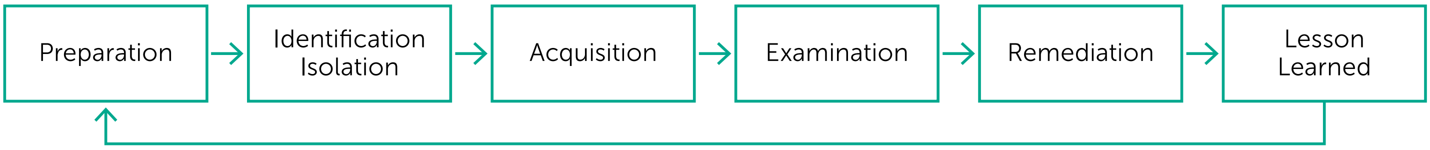


Figure 21:
Incident Response Framework

Kaspersky offers: Incident Response Services

Incident Response is our premium service, covering the entire incident investigation cycle, from the onsite acquisition of evidence to the identification of additional indications of compromise, preparing a remediation plan and completely eliminating the threat to your organization. Kaspersky's investigations are carried out by highly experienced Cyber-Intrusion Detection Analysts and Investigators. The full weight of our global expertise in Digital Forensics and Malware Analysis can be brought to bear on the resolution of your security incident.

The following objectives are to be achieved during execution of the service:

- Identifying compromised resources;
- Isolating the threat;
- Preventing the attack from spreading;
- Finding and gathering evidence;
- Analyzing the evidence and reconstructing the incident's chronology and logic;
- Analyzing the malware used in the attack (if any malware is found);
- Uncovering the sources of the attack and other potentially compromised systems (if possible);
- Conducting tool-aided scans of your IT infrastructure to reveal possible signs of compromise;
- Analyzing outgoing connections between your network and external resources to detect anything suspicious (such as possible command and control servers);
- Eliminating the threat;
- Recommending further remedial action you can take.

Depending on whether or not you have your own incident response team, you can ask our experts to execute the complete investigation cycle, to simply identify and isolate compromised machines and prevent dissemination of the threat, or to conduct Malware Analysis or Digital Forensics.

Malware Analysis

Malware Analysis offers a complete understanding of the behavior and objectives of the specific malware files that are targeting your organization. Kaspersky's experts carry out a thorough analysis of the malware sample you provide, creating a detailed report that includes:

- Sample properties: A short description of the sample and a verdict on its malware classification;
- Detailed malware description: An in-depth analysis of your malware sample's functions, threat behavior and objectives – including IOCs – arming you with the information required to neutralize its activities;
- Remediation scenario: The report will suggest steps to fully secure your organization against this type of threat.

Digital Forensics

Digital Forensics can include malware analysis as above, if any malware was discovered during the investigation. Kaspersky experts piece together the evidence to understand exactly what's going on, including the use of HDD images, memory dumps and network traces. The result is a detailed explanation of the incident. You as the customer initiate the process by gathering evidence and providing an outline of the incident. Kaspersky experts analyze the incident symptoms, identify the malware binary (if any) and conduct the malware analysis in order to provide a detailed report including remediation steps.

Delivery options

Kaspersky's Incident Response Services are available:

- By subscription
- In response to a single incident

Both options are based on the amount of time our experts spend to resolving the incident. This is negotiated with the customer prior signing the contract. Customer may flexibly include as much working hours as he thinks are necessary or follow our experts' recommendations tailored to each specific case.

Penetration Testing and Red Teaming

Ensuring that your IT infrastructure is fully secured against cyberattacks is an ongoing challenge for any organization, but even more so for large enterprises with thousands of employees, hundreds of IT systems, and multiple locations worldwide. To improve your security stance, experts recommend paying special attention to web application security, timely updates of vulnerable software, password protection and firewalling rules. It's also very important to run regular security assessments for your IT infrastructure (including applications).

Completely preventing information resources being compromised can be extremely difficult in large networks or even impossible when attacks are launched using zero-day vulnerabilities. For this reason, it's critical to do everything you can to ensure that information security incidents are detected as early as possible. Timely detection of threat actor activities at the early stages of an attack and a prompt response may help prevent any damage from being caused - or substantially mitigate it. Mature organizations with well-established processes in place for security assessments, vulnerability management and detection of information security incidents should consider running Red Teaming-type 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 attacks and react to them in real-world conditions.

Kaspersky offers: Penetration Testing

Kaspersky's Penetration Testing gives you a greater understanding of the security flaws in your infrastructure, revealing vulnerabilities, analyzing the possible consequences of different forms of attack, evaluating the effectiveness of your current security measures and suggesting remedial actions and improvements.

Penetration Testing from Kaspersky helps you and your organization to:

- Identify the weakest points in your network, so you can make fully informed decisions about where best to focus your attention and budget to mitigate future risk.
- Avoid financial, operational and reputational losses caused by cyberattacks by preventing these attacks from happening, through proactively detecting and fixing vulnerabilities.
- Comply with government, industry or internal corporate standards that require this form of security assessment (for example, Payment Card Industry Data Security Standard (PCI DSS)).

Service scope and options

Depending on your needs and your IT infrastructure, you may choose any or all of these services:

- External penetration testing: A security assessment conducted through the Internet by an 'attacker' with no preliminary knowledge of your system.
- Internal penetration testing: Scenarios based on an internal attacker, such as a visitor with only physical access to your offices or a contractor with limited systems access.
- Social engineering testing: An assessment of security awareness among your personnel by emulating social engineering attacks such as phishing, pseudo-malicious links in emails, suspicious attachments, etc.
- Wireless networks security assessment: Our experts visit your site and analyze your WiFi security controls.

You can include any part of your IT infrastructure in the scope of penetration testing, although we strongly recommend you include the whole network or at least its largest segments, as test results are always more worthwhile when our experts are working under the same conditions as a potential intruder.

Service highlights

The Service is designed to reveal security shortcomings which could be exploited to gain unauthorized access to critical network components. These may include:

- Vulnerable network architecture, insufficient network protection
- Vulnerabilities leading to network traffic interception and redirection
- Insufficient authentication and authorization in different services
- Weak user credentials
- Configuration flaws, including excessive user privileges
- Vulnerabilities caused by errors in application code (code injections, path traversal, client-side vulnerabilities, etc.)
- Vulnerabilities caused by using outdated hardware and software versions without the latest security updates
- Information disclosure

Results are provided in a final report that includes detailed technical information on the testing process, results, vulnerabilities revealed and recommendations for remediation, as well as an executive summary outlining test results and illustrating attack vectors. Videos and presentations for your technical team or top management can also be provided if required.

About Kaspersky's approach to penetration testing

Penetration testing emulates genuine hacker attacks, but you can rest assured that these tests are tightly controlled; performed by Kaspersky security experts with full regard of your systems' confidentiality, integrity and availability, and in strict adherence to international standards and best practices, including:

- Penetration Testing Execution Standard (PTES)
- NIST Special Publications 800-115 Technical Guide to Information Security Testing and Assessment
- Open Source Security Testing Methodology Manual (OSSTMM)
- Information Systems Security Assessment Framework (ISSAF)
- Web Application Security Consortium (WASC) Threat Classification
- Open Web Application Security Project (OWASP) Testing Guide
- Common Vulnerability Scoring System (CVSS)

Project team members are experienced professionals with deep, up-to-date practical knowledge of this field, acknowledged as expert security advisors by industry leaders including Oracle, Google, Apple, Microsoft, Facebook, PayPal, Siemens and SAP.

Delivery options

Depending on the type of security assessment service, your systems specifics and working practices, security assessment services can be provided remotely or onsite. Most services can be performed remotely, and internal penetration testing can even be performed through VPN access, while some services (like wireless networks security assessment) require an onsite presence.

Kaspersky offers: Red Teaming

The service includes the following:

- **Threat Intelligence.** The service starts with a discussion of the customer's known threats and Blue Team's experience. The aim is to identify highly critical business assets and understand how project deliverables can be tailored towards TTPs used by the company's defense. However, during these discussions, Kaspersky will not request any information about the target resources, as the Red Team will also conduct independent information gathering activities like real adversaries would do. The information gathering phase will include both analysis of publically available information (open-source intelligence), and analysis of data available in underground communities.

- **Adversary Simulation.** This stage starts with preparation of attack scenarios and tools based on the results of the Threat Intelligence stage. Preparation may include deep research into the systems used in the customer's environment to reveal new vulnerabilities, developing custom tools aimed at bypassing the customer's security systems, or readying spear-phishing attacks. When the preparation is complete, Kaspersky will perform the active phase of Adversary Simulation. These tests may include the following:

  - Passive information gathering,
  - Active information gathering (network discovery), including port scanning, identifying available services and manual requests to certain services (DNS, mail),
  - External vulnerability scanning, and analyzing
  - Web application security (using both automated and manual approaches) to identify the following types of vulnerabilities:

    - Code injection (SQL Injection, OS Commanding, etc.)
    - Client-side vulnerabilities (Cross-Site Scripting, Cross-Site Request Forgery, etc.)
    - Flaws in authentication and authorization
    - Insecure data storage
    - Other web application vulnerabilities leading to the threats listed in WASC Threat Classification v2.0 and OWASP Top Ten

- Manual vulnerability analysis, including identification of resources without authentication, important publically available information, insufficient access control
- Guessing credentials
- Social engineering testing
- Exploitation of one or more of the vulnerabilities found and privilege escalation (if possible)

- Develop an attack using the obtained privileges and techniques listed above until the Service Provider can access the LAN or important network resources (e.g. Active Directory domain controller, business systems, DBMSes, etc.) or until all attack methods available during testing have been exhausted.

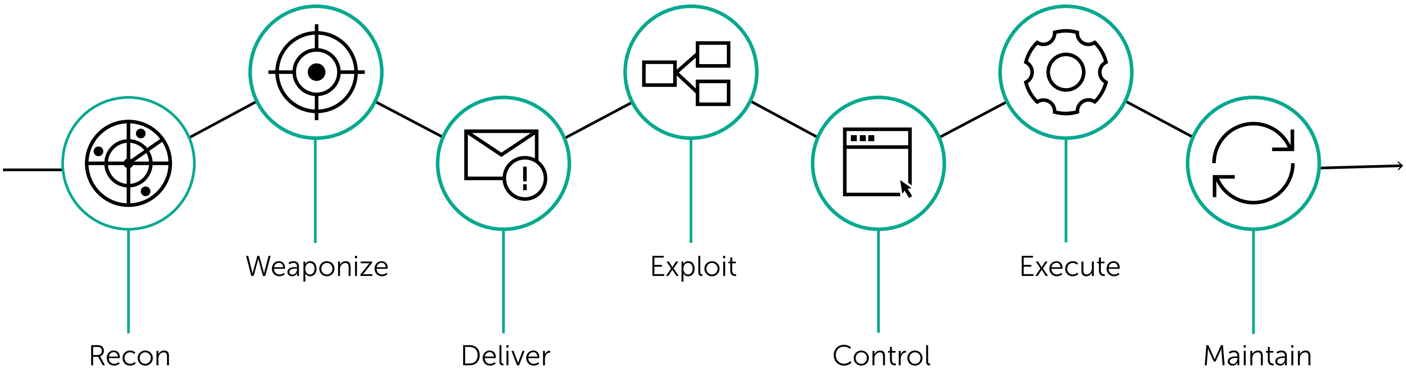


Figure 22:
Adversary simulation

The above tests are carried out according to the prepared customer-specific scenarios, using special techniques to evade detection from the Blue Team. Once the Red Team has accomplished all its objectives, activities that trigger incident detection and response are carried out to ensure Blue Team involvement in the exercise.

- **Report Preparation.** During this stage, Kaspersky will analyze the Adversary Simulation results, prepare a report with detailed description of the attacks (including timestamps and indicators of compromise) and recommendations.
- **Testing Results Overview.** A post-assessment workshop with the company's Blue Team can be arranged to discuss the project results, reasons for anything not detected or prevented, and possible further defense improvements.

Approach and Methodology

Red Teaming has much in common with a real hacker attack and makes it possible to assess the effectiveness of the protection measuresin practice. However, unlike a hacker attack, the service is performed by experienced security experts from Kaspersky who take special care of system confidentiality, integrity and availability in strict adherence to the following **international standards and best practices**:

- Penetration Testing Execution Standard (PTES)
- NIST Special Publications 800-115 Technical Guide to Information Security Testing and Assessment
- Open Source Security Testing Methodology Manual (OSSTMM)
- Information Systems Security Assessment Framework (ISSAF)
- Web Application Security Consortium (WASC)
- Threat Classification Open Web Application Security Project (OWASP)
- Testing Guide Common Vulnerability Scoring System (CVSS)
- And other standards, depending on your organization's business and location

The analysis is performed using automated tools as well as manually by experts. The following security assessment tools can be used:

- Information gathering tools (Maltego, theHarvester and others)
- Various general-purpose and specialized scanners (NMap, MaxPatrol, Nessus, Acunetics WVS, nbtscan and others)
- Complex security assessment solutions (Kali Linux)
- Credentials guessing tools (Hydra, ncrack, Bruter, and others)
- Specialized solutions for web application security assessment (OWASP dirbuster, 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.

For Red Teaming to be legal and safe, the customer must provide a point of contact (a representative) for all project communications, including scope negotiations and, resolving access issues, as well as giving confirmation for active works. The representative must be an official employee of the customers with an e-mail address belonging to the customer's domain name (not a third-party intermediary).

The confidentiality, integrity and availability of your IR resources are our top priority. Kaspersky's experts will take all necessary precautions to avoid any harm to your environment. All sensitive technical information related to the project (important data, credentials, assessment results, etc.) will be stored and transferred using strong encryption, and can be deleted on your request after the project has been completed.

Our expert team members are experienced professionals in security assessment with deep knowledge of this field, constantly improving their skills. They have been acknowledged for their security research by such industry leaders as Oracle, Google, Apple, Microsoft, Facebook, PayPal, Siemens, SAP, and others (see section 7 for description of the project team). You can find resumes of the project team members in the attachment to this proposal.

Outcome

Following the service, customers receive a report containing the following:

- High-level conclusions on the identified defensive capabilities, and recommendations to improve them;
- A detailed description of detected vulnerabilities, including severity level, exploitation complexity, possible impact on the vulnerable system, and evidence of the existence of vulnerabilities (where possible);
- A detailed description of activities (including timestamps and indicators of compromise) for analysis and improvement of the defensive team;
- Recommendations for eliminating vulnerabilities;
- Recommendations on improving the incident response processes;
- Recommendations on mitigating the identified prevention and detection issues.

The Red Teaming Testing Service from Kaspersky will help you evaluate the effectiveness of your monitoring capabilities and incident response procedures.

Why Kaspersky?

Because we have:

- Partnerships with global law enforcement agencies such as Interpol and CERTs;
- Cloud-based tools monitoring millions of cyberthreats across the globe in real-time;
- Global teams analyzing and understanding internet threats of all kinds.

Because we are:

- The world's largest independent security software company, focused on Threat Intelligence and technology leadership;
- The undisputed leader in more independent malware detection tests than any other vendor;
- Identified as Leader by Gartner, Forrester and IDC.

About Kaspersky

Kaspersky is the world's largest privately held vendor of endpoint protection solutions. The company is ranked among the world's top four vendors of security solutions for endpoint users. Throughout its more than 21-year history, Kaspersky has remained an innovator in IT security and provides effective digital security solutions for enterprises, SMBs and consumers. With its holding company registered in the United Kingdom, Kaspersky operates in almost 200 countries and territories worldwide, providing protection for over 400 million users across the globe.

Disclaimer.

This document is not a public offer and is intended for introductory purposes only.

The scope of the service can vary depending on it's availability in the specific geographical region. Some services described in the document require additional agreement with Kaspersky.

For additional details, please contact Kaspersky's regional representative or send your request to intelligence@kaspersky.com.

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

www.kaspersky.com

kaspersky **BRING ON THE FUTURE**