KASPERSKY lab

SOC powered by Kaspersky Lab

www.kaspersky.com

While businesses learn to better protect themselves, criminals are simultaneously devising ever more sophisticated techniques to penetrate their security walls. Attracted by the unprecedented earning opportunities cyber-attacks can deliver, increasing numbers of threat actors are actively seeking and targeting unspotted security flaws.

Increasingly, Security Operations Centers (SOCs) are now being established to combat security issues as they arise, and to provide a swift response and resolution.

"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

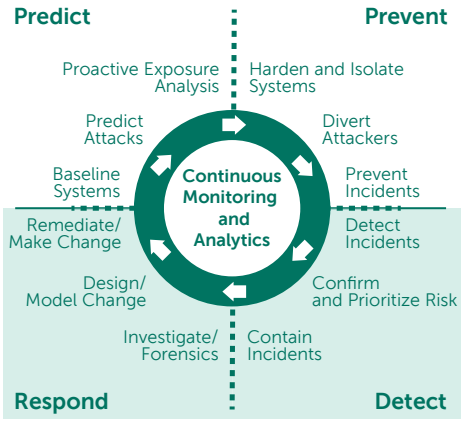
THE SOC IS A CENTRALIZED FUNCTION FOR CONSTANT THREAT MONITORING AND ANALYSIS, AND THE MITIGATION AND PREVENTION OF CYBERSECURITY INCIDENTS

A survey recently conducted by B2B International (to be published in the end of 2016), involving over 4000 businesses in 25 countries, found that:

- **38%** of respondents had experienced severe **issues with viruses and malware** over the previous 12 months, resulting in a loss of productivity.
- **21%** had experienced **data loss/exposure due to targeted attacks**.
- Around 40% or respondents highlighted these challenges as a specific concern.
- **17%** of businesses had suffered a **DDoS attack** in the previous 12 months, often more than once.
- **42%** of all respondents who experienced **phishing attacks** were enterprises.
- **26%** of all security events **went undetected** for weeks or more, being revealed only through external security audits.
- For an enterprise business suffering at least one data breach, **the average financial impact** was **$891k** (this includes additional internal staff wages, damage to credit ratings/insurance premiums, lost business, extra PR to repair brand damage and employing external consultants).
- These **impact** figures for enterprises **ranged from $393k to $1.1m**, depending on when the breach was detected – rapid detection resulting in lower costs to the business.
- The total number of sensitive customer/employee records compromised was also time-dependent – ranging from 9K with virtually instant detection (detection system in place), to 240K when the breach had remained undetected for over a year.

According to Gartner's Adaptive Security Architecture model, if they are to successfully fight cybercrime in the current threat environment, SOC Teams must be able to:

- PREDICT
- DETECT
- PREVENT
- RESPOND



Gartner, Designing an Adaptive Security Architecture for Protection From Advanced Attacks, February 2014, Foundational January 2016

FOUR KEY ELEMENTS

Four key elements, together with clearly defined processes and relevant technologies, must be in place to sustain this industry-recognized approach. They are:

- **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.
- **THREAT INTELLIGENCE**, collected from many different sources (the more the better) is essential to timely detect emerged threats:
  1. Internal threat data
  2. Intelligence from open sources (OSINT)
  3. Industry CERTs
  4. Global anti-malware vendors
- **THREAT HUNTING** to proactively search for threats being undetected by traditional security systems like firewall, IPS/IDS, SIEM etc.
- **AN INCIDENT RESPONSE FRAMEWORK** implemented to limit damage and reduce remediation costs.

Each of these elements is equaly important and warrant separate consideration.

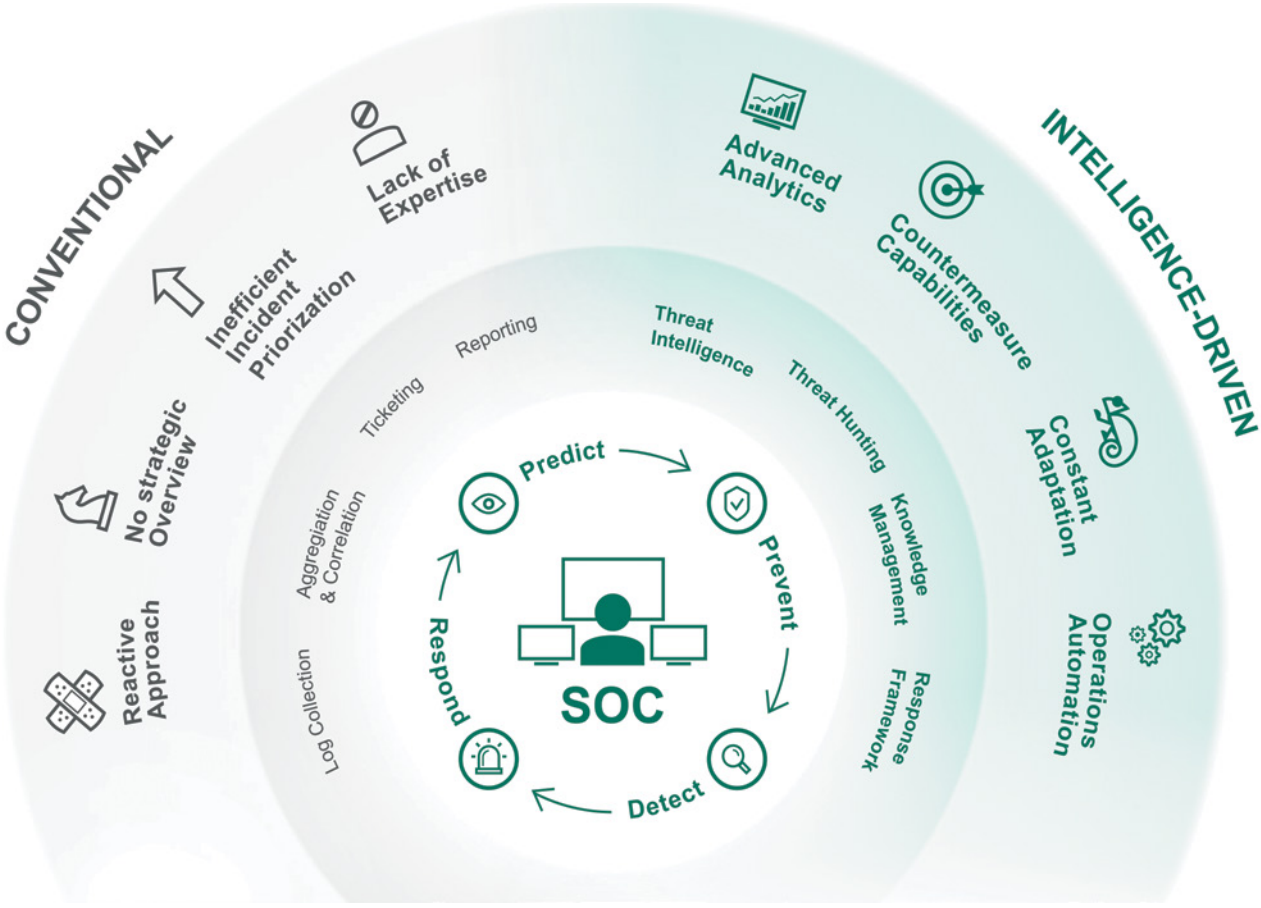


Figure 1:
The four key elements of the SOC

KNOWLEDGE MANAGEMENT

The SOC must provide a resource-pool of practical knowledge and expertise sufficient to analyze a vast amount of data and to identify 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 including 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.

Incident response, digital forensics and malware analysis are indispensable competencies.

INCIDENT RESPONSE & DIGITAL FORENSICS	MALWARE ANALYSIS
• Timely and accurately responding to the incident • Analysing evidence (hdd images, memory dumps, network activity traces) and reconstructing the incident history and logic • Revealing the presumed sources of the attack and other likely compromised systems (if possible) • Understanding the root cause of the incident to prevent any similar incident arising	• Gaining an understanding of the suspicious software sample and its capabilities • Defining whether it is in fact malware • Determining the potential impact the sample might have on compromized systems within the organization • Building a comprehensive a remediation plan based on the malware behavior revealed

Kaspersky Lab offers:
Cybersecurity Training Services

For more than 17 years, Kaspersky Lab'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 confronted with the new dangers of contemporary cyber-reality.

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 Lab offices, as applicable.

PROGRAM DESCRIPTION

TOPICS	DURATION	SKILLS GAINED
DIGITAL FORENSICS		
• Introduction to Digital Forensics • Live response and evidence acquisition • Windows registry internals • Windows artifacts analysis • Browsers forensics • Email analysis	5 days	• Build a Digital Forensics lab • Collect digital evidence and deal with it properly • Reconstruct an incident and use time stamps • Find traces of intrusion based on artifacts in Windows OS • Find and analyze browser and email history • Confidently apply digital forensics tools and techniques
MALWARE ANALYSIS & REVERSE ENGINEERING		
• Malware Analysis & Reverse Engineering goals and techniques • Windows internals, executable files, x86 assembler • Basic static analysis techniques (string extraction, import analysis, PE entry points at a glance, automatic unpacking, etc.) • Basic dynamic analysis techniques (debugging, monitoring tools, traffic interception, etc.) • .NET, Visual Basic, Win64 files analysis • Script and non-PE analysis techniques (Batch files; AutoIt; Python; JScript; JavaScript; VBS)	5 days	• Build a secure environment for malware analysis: deploy sandbox and all necessary tools • Understand principles of Windows program execution • Unpack, debug and analyze a malicious object, identify its functions • Detect malicious sites through script malware analysis • Conduct express malware analysis

TOPICS	DURATION	SKILLS GAINED
ADVANCED DIGITAL FORENSICS		
• Deep Windows forensics • Data recovery • Network and cloud forensics • Memory forensics • Timeline analysis • Real world targeted attack forensics practice	5 days	• Be able to perform deep file system analysis • Be able to recover deleted files • Be able to analyze network traffic • Reveal malicious activities from dumps • Reconstruct the incident timeline
ADVANCED MALWARE ANALYISIS & REVERSE ENGINEERING		
• Advanced static analysis techniques (analyzing shellcode statically, parsing PE header, TEB, PEB, loading functions by different hash algorithms) • Advanced dynamic analysis techniques (PE structure, manual and advanced unpacking, unpacking malicious packers that store the full executable in an encrypted form) • APT reverse engineering (cover an APT attack scenario, starting from phishing email and going as in-depth as possible) • Protocol analysis (analyse encrypted C2 communication protocol, how to decrypt traffic) • Rootkits and Bootkits analysis (debugging the boot sector using Ida and VMWare, Kernel debugging using 2 virtual machines, analyzing Rootkit samples)	5 days	• Be able to follow best practices in reverse engineering while recognizing anti-reverse engineering tricks(obfuscation, antidebugging) • Be able to apply advanced malware analysis for Rootkits/ Bootkits dissection • Be able to analyze exploit shellcode embedded in the different file types and non-Windows malware
INCIDENT RESPONSE		
• Introduction to Incident Response • Detection and primary analysis • Digital analysis • Creating of detection rules (YARA, Snort, Bro)	5 days	• Differentiate APTs from other threats • Understand various attackers' techniques and targeted attack anatomy • Apply specific methods of monitoring and detection • Follow incident response workflow • Reconstruct incident chronology and logic • Create detection rules and reporting

Tools change with time, but basics and methods of work remain consistent. Participants will receive, not just a set of tools and instructions, but an understanding of fundamental principles and functionality. All practical tasks are based on real cases, wherever this is possible without breaching customer confidentiality.

THREAT INTELLIGENCE AND THREAT HUNTING

The SOC was 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 system (SIEM).
- Incident forensics and remediation.
- Internal or regulatory compliance (e.g. PCI-DSS).

Many organizations are now planning to gain greater threat visibility by establishing their own SOCs. However, some organizations who already have an SOC find they still face many of the same problems.
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.
- False negatives due to the lack of corresponding threat data
- 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.

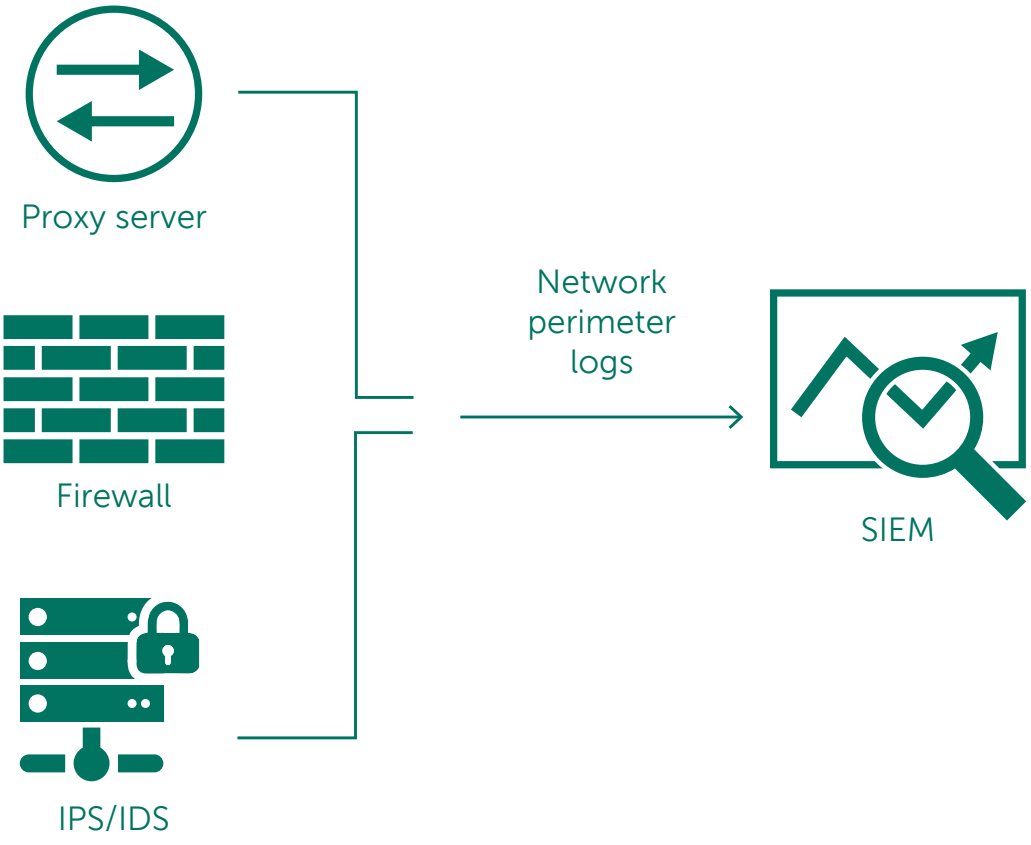


Figure 2:
A Conventional SOC

- 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.

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, February 2016

Based on these considerations, security leaders would be well-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 ongoing threat environment.

Combining internal threat data with information gathered from various different 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.

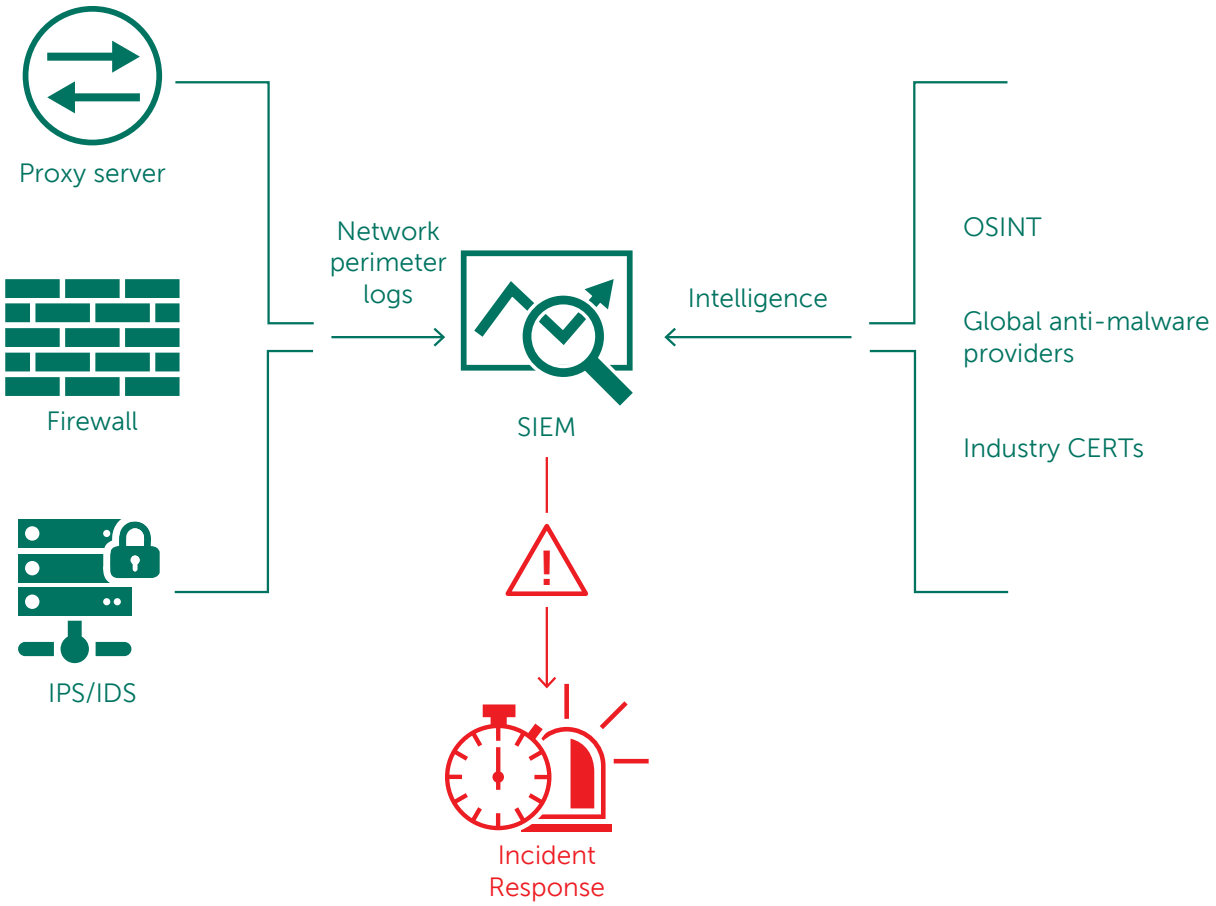


Figure 3:
The intelligence-driven SOC

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 explore an infected machine.

What to look for in external Threat Intelligence sources:

- Intelligence with a global reach, providing the broadest attack visibility
- A provider with a track record in spotting new threat indicators early
- Context-rich, immediately actionable intelligence
- Delivery formats and mechanisms that allow easy integration into existing security controls

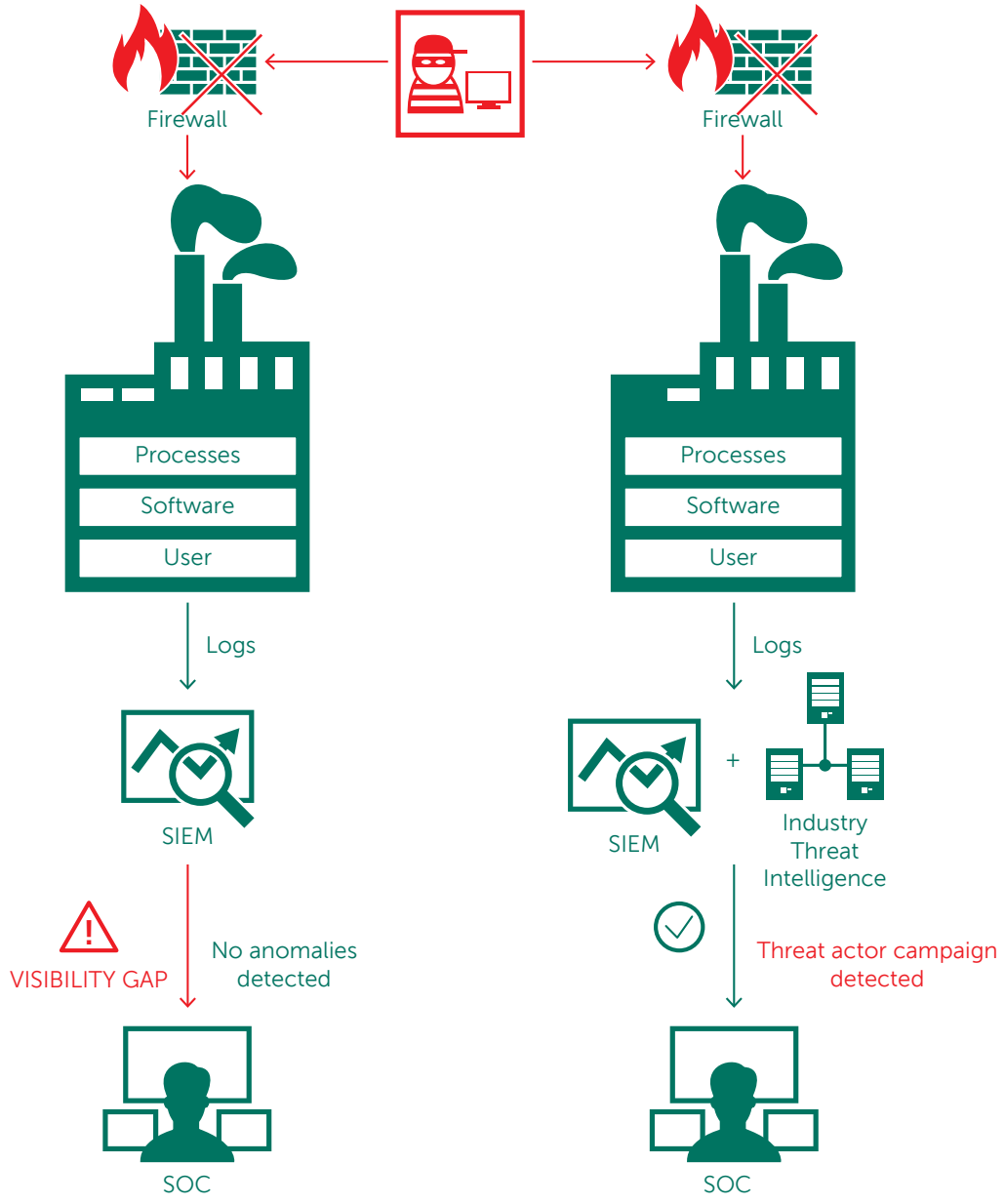


Figure 4:
Threat Intelligence Model

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.

This process involves gathering and applying different techniques (such as statistical analysis, machine learning and visualization) to all available data obtained from endpoints, networks, implemented security controls, authentication systems etc. The objective is to confirm an existing hypothesis regarding the potential breach. Threat-hunting technologies the analyst may employ include those already mentioned — SIEM solutions, OSINT, Threat Intelligence Platforms and other data sources.

The threat-hunting analyst will consult externally obtained IOCs (Indicators of Compromise), and apply specialized tools to search for these artefacts (in the form of IP addresses, file hashes, URLs etc.) inside the organization's hosts. Where a clear sign of compromised security is unearthed, incident response procedures can be initiated.

Trawling through huge volumes of data to identify artefacts that automated measures have failed to detect is a task for highly qualified and experienced professionals.

Kaspersky Lab offers:
Threat Intelligence Data Feeds

Kaspersky Lab offers continuously updated Threat Intelligence 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 Feeds — 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 Lab 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.
Whitelisting Data Feeds — a set of file hashes providing third-party solutions and services with a systematic knowledge of legitimate software.
Malicious Hash Feeds — overing the most dangerous, prevalent and emerging malware.
Mobile Malicious Hash Feeds — a set of file hashes for detecting malicious objects that infect mobile platforms.
P-SMS Trojan Feeds — 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 Threat Lookup

Kaspersky Threat Lookup delivers all the knowledge acquired by Kaspersky Lab 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 cyber-attacks before they impact your organization. The platform retrieves the latest detailed Threat Intelligence about URLs, domains, IP addresses, file hashes, threat names, statistical/behavior data, WHOIS/DNS data, etc. The result is global visibility of new and emerging threats, helping you secure your organization and boosting incident response.

SERVICE HIGHLIGHTS

- Trusted Intelligence: A key attribute of Kaspersky Threat Lookup is the reliability of our threat intelligence data, enriched with actionable context. Kaspersky Lab products lead the field in anti-malware tests[1], demonstrating the unequalled quality of our security intelligence by delivering the highest detection rates, with near-zero false positives.
- High levels of Real Time Coverage: Threat Intelligence is automatically generated in Real Time, based on findings throughout the world, supported by the Kaspersky Security Network.
- 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.
- Rich Data: Threat Intelligence delivered by Kaspersky Threat Lookup covers a huge range of different data types including hashes, URLs, IPs, whois, pDNS, GeoIP, file attributes, statistical and behavior data, download chains, timestamps and much more. Empowered with this data, you can survey the diverse landscape of security threats you're facing.
- Continuous Availability: Threat Intelligence is generated and monitored by a highly fault-tolerant infrastructure, ensuring continuous availability and consistent performance.
- Continuous Review by Security Experts: 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.

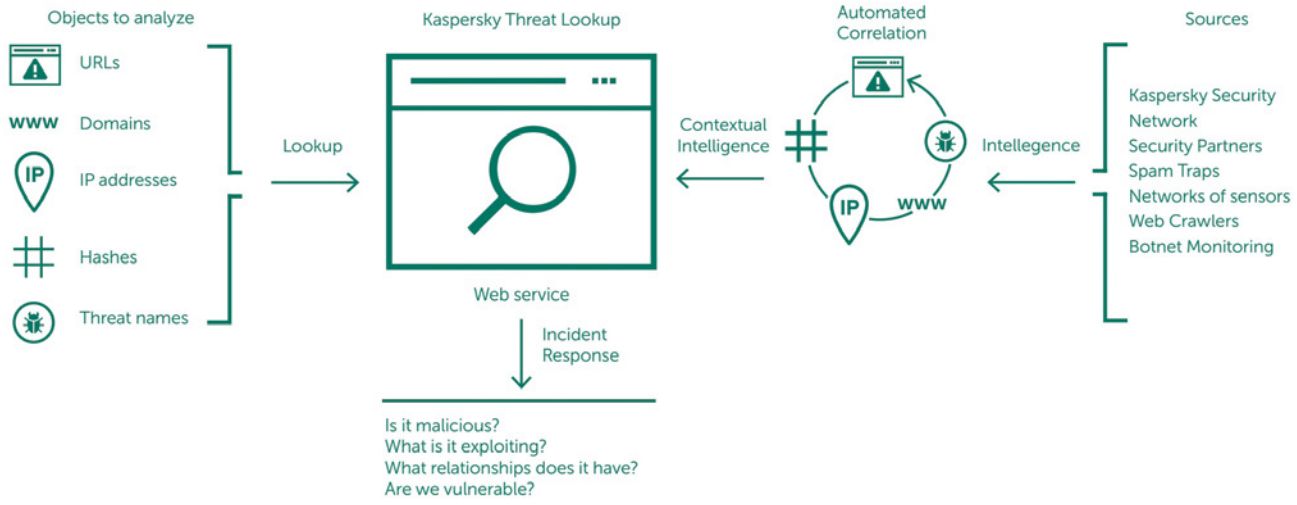
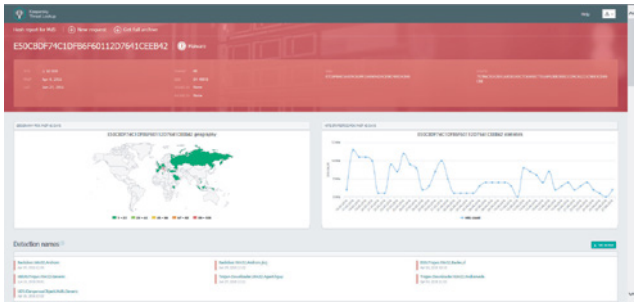
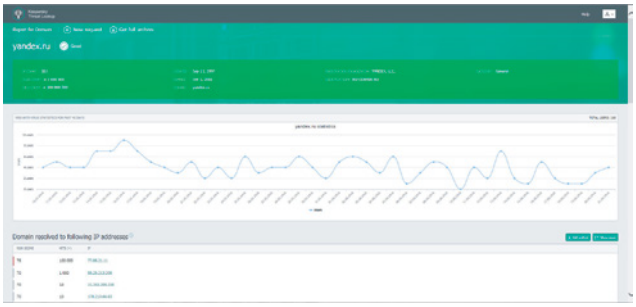


Figure 5:
Kaspersky Threat Lookup

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

- 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 as you prefer.





APT Intelligence Reporting

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

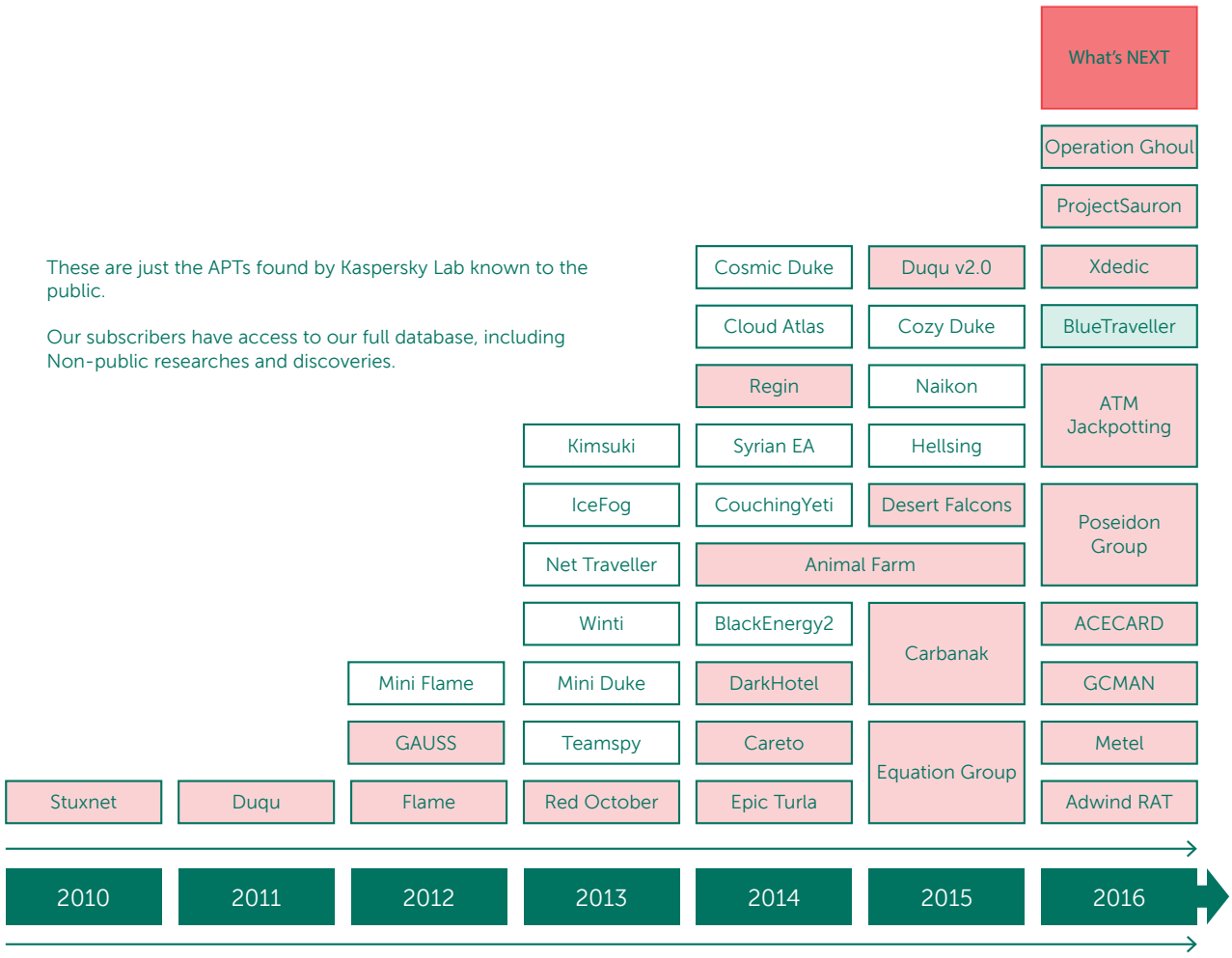


Figure 6:
APTs found by Kaspersky Lab

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 and cyberterrorist groups. Furthermore, you will have access to Kaspersky Lab's complete APT reports database – a further powerful research and analysis component of your corporate security armory.

SERVICE HIGHLIGHTS

- Exclusive access to technical descriptions of cutting edge threats during the ongoing investigation, before public release.
- 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, samples and tools, 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.

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 delivered via the APT Intelligence Portal, as illustrated below.

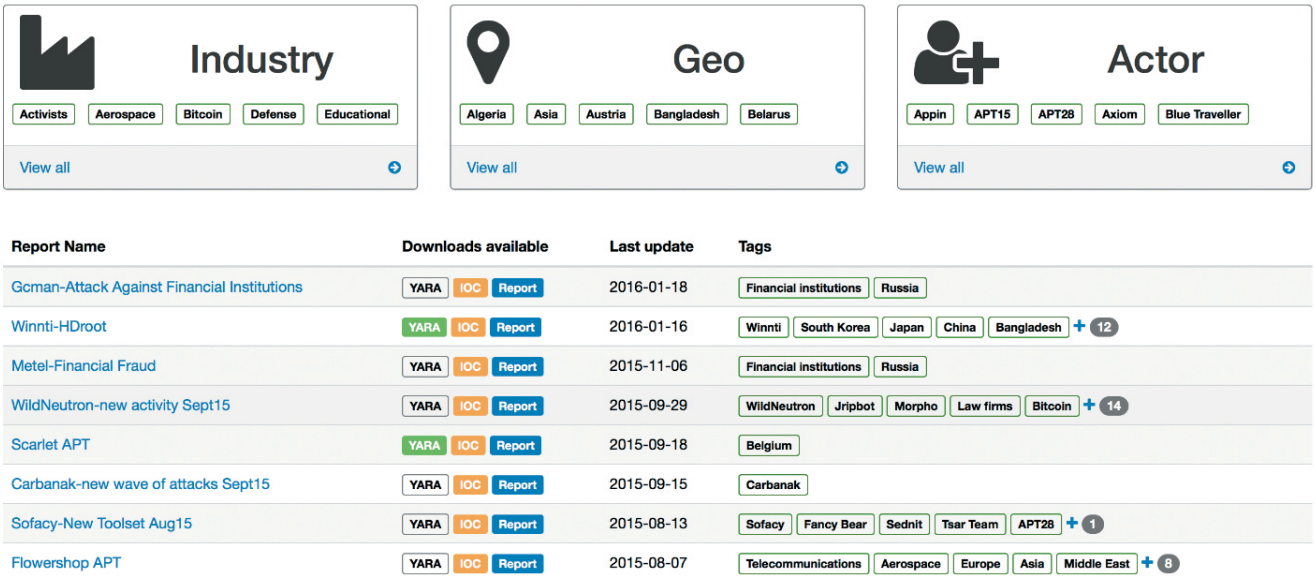


Figure 7:
APT Intelligence Portal

Tailored Threat Reporting

Customer-specific Threat Reporting

What's the best way to mount an attack against your organization? Which routes and what information is 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 this unique insight, 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 Lab 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 cyber-attack 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 Lab service.

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

Country-specific Threat Reporting

Cybersecurity of a country comprises protection of all its major institutions and organizations. Advanced persistent threats (APT) against government authorities can affect national security; possible cyberattacks against manufacturing, transportation, telecommunication, banking and other pivotal industries potentially 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 Lab 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 cyber-attack 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.

As the conclusion of the service you will be provided with a report containing 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 a subscription (for example, quarterly).

Kaspersky Managed Protection

The Kaspersky Managed Protection service offers Kaspersky Security for Business and Kaspersky Anti Targeted Attack Platform users a unique combination of advanced technical measures to detect and prevent targeted attacks. The service includes round-the-clock monitoring by Kaspersky Lab experts and the continuous analysis of cyberthreat data (Cyber-Threat Intelligence), ensuring real-time detection of both known and new cyber-espionage and cybercriminal campaigns targeting critical information systems.

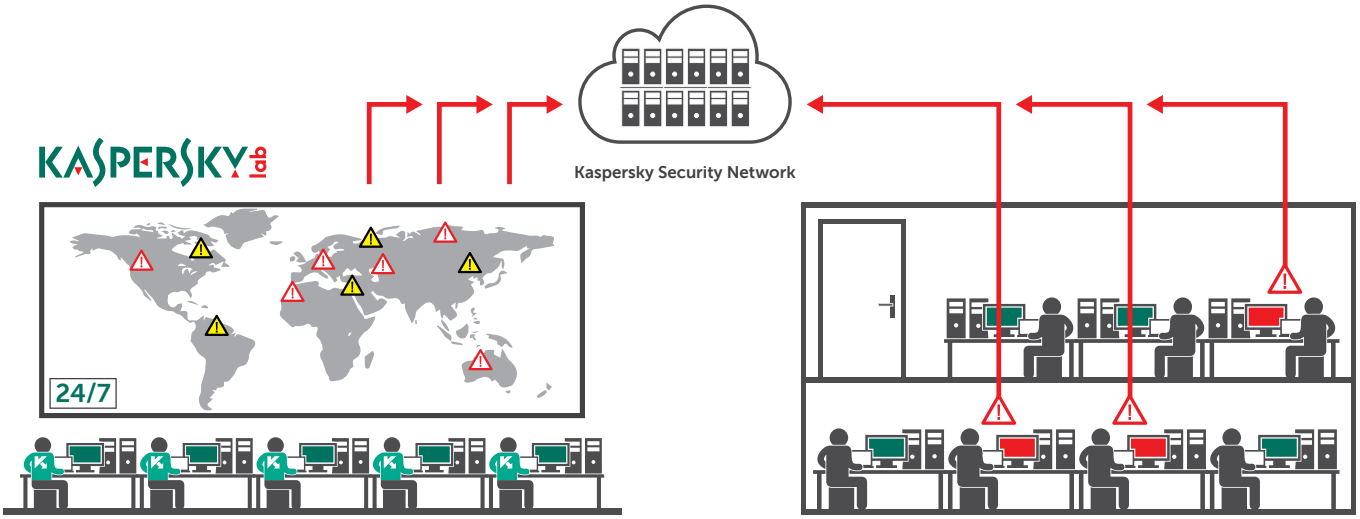


Figure 8:
Kaspersky Managed Protection

SERVICE HIGHLIGHTS

- A high level of protection against targeted attacks and malware with 24x7 support from Kaspersky Lab analysts.
- Insights into attackers, their motivation, their methods and tools, and the potential damage they could inflict, supporting the development of a fully informed, effective protection strategy.
- Detection of non-malware attacks, attacks involving previously unknown tools and attacks exploiting zero-day vulnerabilities.
- Retrospective analysis of incidents and threat hunting.
- Reduction in overall security costs while simultaneously enhancing the quality of protection. This is a highly professional service offered by the world leader in cyber-attack analysis, including the analysis of the methods and technologies used by threat actors. Obtaining this level of information through an outside service is far more economical than employing narrowly focused specialists.
- Integrated approach — our extensive range of integrated Kaspersky Security for Business solutions means Kaspersky Lab offers all the technologies and services needed to implement a complete cycle of protection against targeted attacks: Preparation — Detection — Investigation — Data Analysis — Automated Protection.

SERVICE BENEFITS

- Quickly detects incidents.
- Collects sufficient information to enable classification (into false positive or correct detection).
- Identifies how common the collected artifacts are, determining how unique the attack is.
- Initiates the process of responding to an information security incident.
- Initiates any necessary updates to antivirus databases, to block the spread of threats.

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 Lab 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 Lab 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, its time to consider your Incident Response.

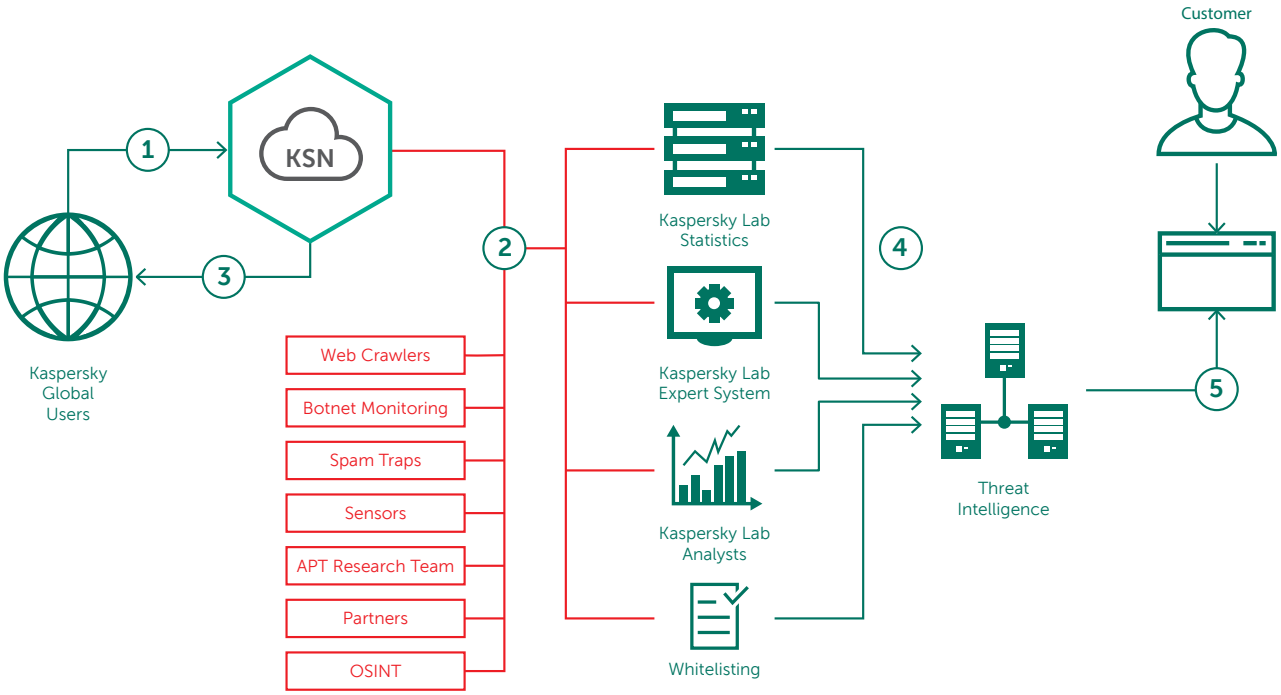


Figure 9:
Kaspersky Lab's Threat Intelligence Sources

INCIDENT RESPONSE FRAMEWORK

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 an 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

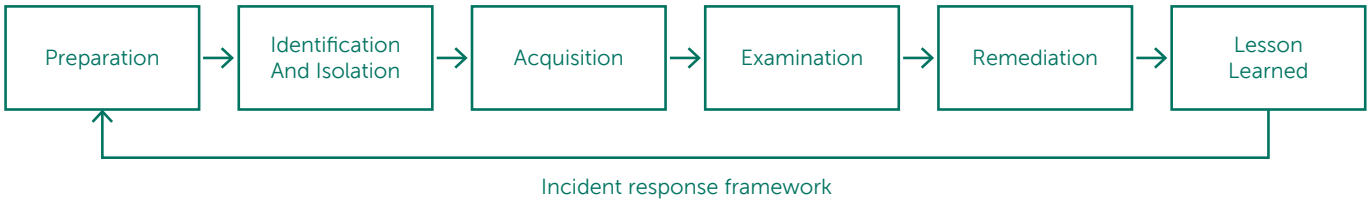


Figure 10:
Incident Response Framework

Kaspersky Lab 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 Lab'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 Lab'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 Lab 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 elucidation of the incident. You as the customer initiate the process by gathering evidence and providing an outline of the incident. Kaspersky Lab 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 Lab'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.

WHY KASPERSKY LAB?

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 Lab

Kaspersky Lab 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 18-year history, Kaspersky Lab 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 Lab operates in almost 200 countries and territories worldwide, providing protection for over 350 million users across the globe.


Twitter.com/
Kaspersky


Facebook.com/
Kaspersky


Youtube.com/
Kaspersky

Kaspersky Lab, Moscow, Russia
www.kaspersky.com

All about Internet security:
www.securelist.com

Find a partner near you:
www.kaspersky.com/buyoffline

KASPERSKY lab