Kaspersky Threat Intelligence Portal: Building a threat intelligence workflow

When talking about an IT security strategy, businesses are interested in one question: What measures are sufficient? For a long time, common wisdom held that a passive strategy — protecting the network perimeter and workstations — sufficed. But with enterprises increasingly falling victim to advanced and targeted attacks, it's now clear that protection requires new methods, based on Threat Intelligence.

Generating this intelligence, revealing the methods and tools used by threat actors and identifying the most effective countermeasures requires constant dedication and high levels of expertise. At Kaspersky Lab we've been focusing on threat research for over two decades. With petabytes of rich threat data to mine and a unique pool of world experts to draw upon, we work to help organizations all over the world maintain immunity against even previously unseen cyber-attacks.

Tactical Intelligence. Threat indicators including IP addresses, domains, and hashes showing what organizations need to focus on when responding to incidents. Provided in machine-readable formats, it allows automated detection by your security controls.

Operational Intelligence. Specialized and technically focused intelligence to guide and support the response to specific incidents by giving an indication to the nature of the attack allowing faster mitigation: for example, by removing attack paths or hardening services.

Strategic Intelligence. A comprehensive picture of the intent and capabilities of malicious actors, including the tools, and TTPs used, with the identification of trends, patterns, emerging threats and risks, in order to inform your security policies and overall information security strategy.

Immediate Access to the Ultimate Threat Intelligence Resource

Subscribers to Kaspersky Lab's Threat Intelligence Portal enjoy a single point of entry to four complementary services: Kaspersky Threat Data Feeds, APT Intelligence Reporting, Financial Threat Intelligence Reporting and Kaspersky Threat Lookup, all available in human and machine-readable formats.
As a subscriber, you gain instant access to both immediate and historic threat intelligence, helping you, your SIEM analyst and your SOC (Security Operations Center) to combat cyber-attacks as they arise, securing your organization before they can do any damage, and to boost incident response.

Threat Data Feeds	Threat Lookup	Threat Intelligence Reporting
Broad coverage	Threat hunting	Exclusive insights
Trusted sources	Link and analysis	TTPs
Rich context	Sandbox	IoCs and Yara rules
Immediately actionable	WHOIS tracking	Retrospective analysis

Web access or RESTful API

Interactive map of top trending threats worldwide

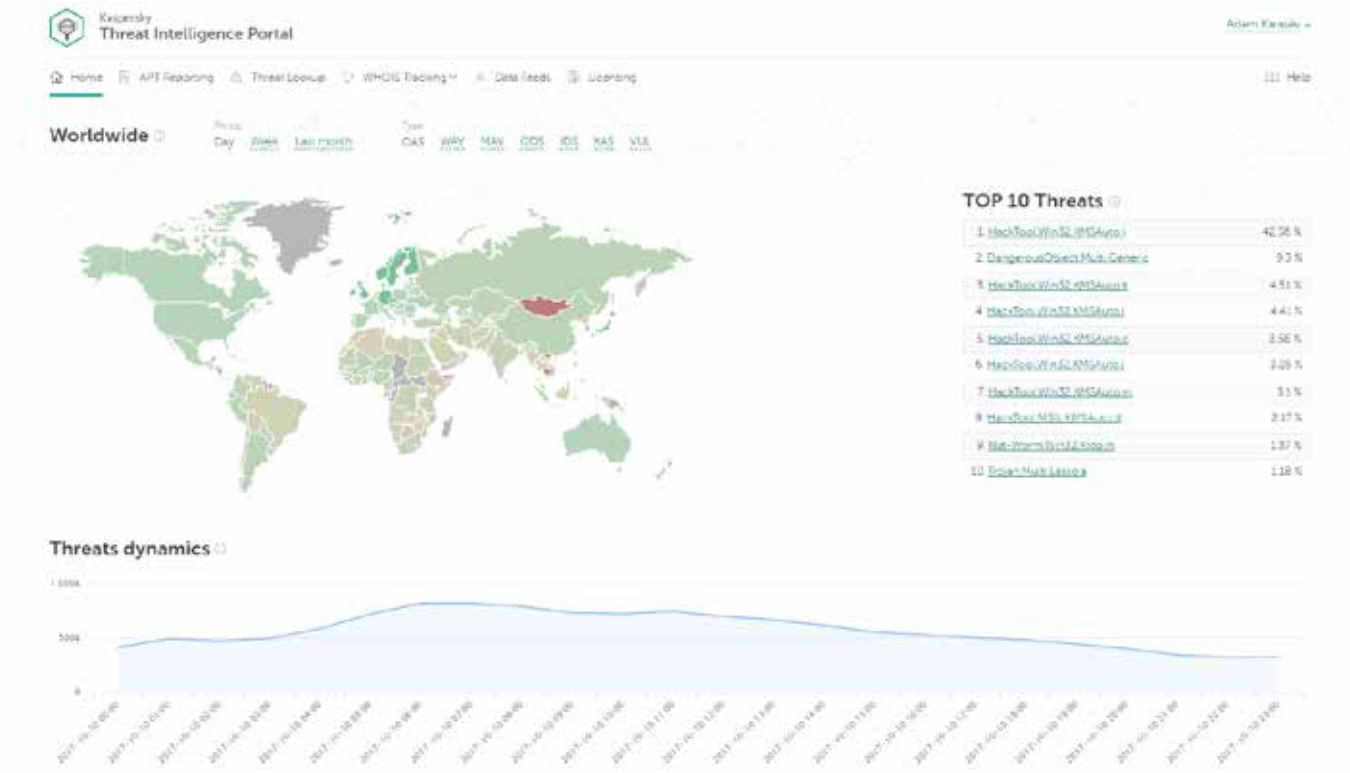
Tactical Intelligence	Operational Intelligence	Strategic Intelligence
Continuously updated Threat Data Feeds contain indicators with additional context for the most dangerous and prevalent threats to inform your business or your clients about risks and implications associated with them, helping you to mitigate those cyberthreats more effectively and defend against attacks even before they are launched.	Kaspersky Threat Lookup provides interactive access to five petabytes of cyberthreat intelligence, collected and categorized by Kaspersky Lab for over more than 20 years. It gives all the ammunition your SOC team needs to drill down, historically and geographically, into your adversaries' activities and malicious behavior across the internet by revealing detailed intelligence on threat indicators and their relationships.	Kaspersky Lab has discovered the most significant APT attacks. But many investigations are never publicly announced. APT and Financial Threat Intelligence Reporting provide you with exclusive ongoing access to our investigations and discoveries, including full technical data, in a range of formats, on each attack as it's revealed, including all those which will never be made public.

A comprehensive threat intelligence workflow

Kaspersky Lab's multi-layered, next generation protection utilizes machine learning methods extensively on all stages of detection pipeline - from scalable clustering methods used for preprocessing incoming file stream in infrastructure to robust and compact deep neural network models for behavioral detection that will work directly on users' machines. Kaspersky Threat Intelligence Portal transforms BigData gathered and processed by Kaspersky Lab into actionable intelligence for your business.

The Kaspersky Threat Intelligence Portal enables SOC and IR teams to build a comprehensive threat intelligence workflow, by providing instruments and tools to automate and extend analytical capabilities for threat detection:

- Kaspersky machine-readable threat intelligence allows integration with existing security controls including leading SIEM systems, firewalls, IDS etc., enabling faster detection times.
- Every detected threat can then be investigated in Kaspersky Threat Lookup. Historical data helps to interlink the information on various files, IPs, URLs, domains, hashes and threat names, revealing detailed intelligence data including whois, pDNS, GeoIP, file attributes, statistical and behavioral data, download chains, timestamps and much more.
- Our reporting capabilities can then be used to enrich existing technical data with descriptions of the associated threat actor TTPs , together with information on customer-specific vulnerabilities that can be exploited to compromise the network.



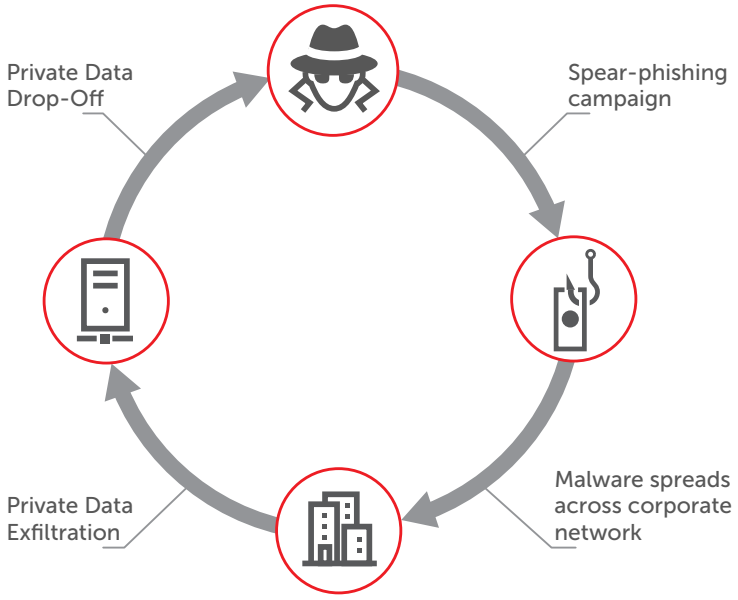
Let's see how this works in practice.

Imagine a SOC team in a typical e-commerce corporation[1] who are becoming concerned about occasional anomalies in network traffic between corporate workstations. The corporate network has in fact already become compromised as the first stage of a targeted attack, but the SOC team is unable to see the full picture, so can't respond appropriately until problems have escalated. Customers start to complain about thefts from their credit cards and web money accounts.

Clearly this organization is experiencing a serious information security breach, which is already beginning to cause reputational damage and revenue losses. So how could the Kaspersky Threat Intelligence Portal help the SOC team identify the causes of this outbreak, and how can they prevent further costly consequences?

1 Kaspersky Threat Intelligence is applicable to a wide range of industries. The described scenario is an example only, and does not imply that application is limited to the e-commerce industry.

Let's assume that the attackers have used the common social engineering tactic of sending to company employees spear phishing emails containing weaponized files as attachments. One of those employees being fooled by the tailored messaging opened an attachment. This has allowed the attackers to spread malware across different hosts throughout the corporate network, infecting every web server on which the e-commerce application is installed. The compromised e-commerce application has then started to transfer cardholder data on to C2 servers for drop-off each time a customer makes a payment.

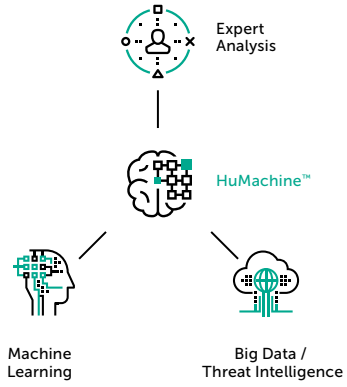


Using the portal, the SOC team can successfully identify and completely eliminate the threat, early enough to prevent catastrophic damage.

How are they able to do this? Here are some examples of steps they could take:

- Using their SIEM in conjunction with the Kaspersky C&C URL feed, the SOC team are able to uncover and pinpoint periodic outbound traffic with hosts pointing to C2 servers.
- Kaspersky Threat Lookup is able to show that the detected URLs are related to the specific threat actor.
- Using WHOIS Tracking and Hunting functionality, all domains registered by the specific threat actor, including those newly registered, can be revealed and added to the corporate blacklist.
- Threat Intelligence Reporting gives the SOC team and CISO an understanding of the TTPs used by the related threat actor together with Indicators of Compromise (IOC) and Yara rules.
- Using IOCs and Yara rules, the SOC team can identify all the infected hosts and take the necessary actions to disinfect them.
- Finally, the SOC team issues a business-wide warning to employees explaining how to recognize and report phishing emails. IT security awareness is assessed throughout the organization, and training initiated for all employees.

We at Kaspersky Lab are focused on providing you with more and more unique insights into the most notorious threats through further developing our Threat Intelligence offerings. Backed by this commitment the Kaspersky Threat Intelligence Portal allows your SOC or IR Team to detect threats early, conduct quick and efficient investigations and build comprehensive security strategies to mitigate the risk that cyberattacks pose to your organization.



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

#truecybersecurity
#HuMachine

www.kaspersky.com