

**Threat Intelligence Platform** 





#### Kaspersky CyberTrace

A Threat Intelligence Platform that enables seamless integration of threat data feeds with SIEM solutions to help analysts leverage threat intelligence in their existing security operations workflows more effectively.

## Enabling effective alert triage and analysis

The number of alerts processed by cybersecurity analysts is growing exponentially. With this amount of data being analyzed, effective alert prioritization, triage and validation is nearly impossible.

There are too many blinking lights coming from numerous security products, leading to important alerts being buried in the noise and analyst burnout. SIEMs and other security analytics tools correlate events and help to reduce the number of alerts, but security analysts remain extremely overloaded.

#### **SIEM** systems

By integrating up-to-the-minute machine-readable threat intelligence into existing security controls, like SIEM systems, security professionals can automate the initial triage process getting enough context to immediately identify alerts that need to be investigated or escalated to incident response teams for further investigation and response.

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 comes 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.

#### Integrations

Kaspersky CyberTrace can be integrated with any threat intelligence data feed in JSON, STIX, XML and CSV formats:

2

Kaspersky threat intelligence data feeds

Other vendors data feeds

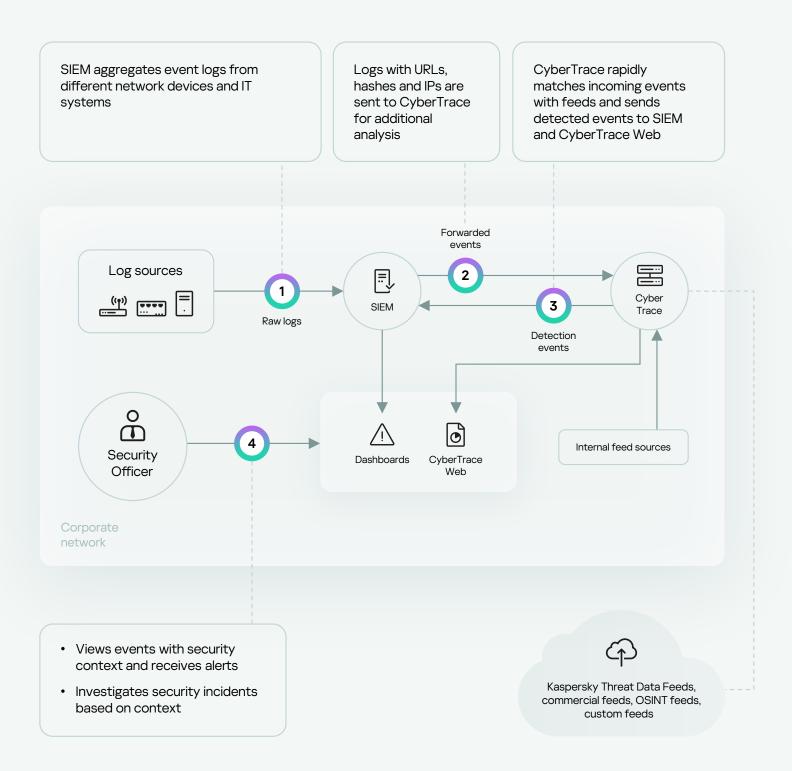
### 3

OSINT or your custom feeds

For customers' convenience CyberTrace supports out-of-the-box integration with numerous SIEM solutions and log sources.

## Kaspersky CyberTrace integration scheme

Kaspersky CyberTrace is able to enhance SIEM capability with additional layer of incoming data parsing and matching, significantly reducing SIEM workload. Matching events with information from data feeds helps to identify threats and provide valuable context to detected incidents. A high-level architecture of the solution integration is shown in the Figure below.



## **Product features**

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

#### **Detailed information**

#### about an indicator from all threat intelligence suppliers

A database of indicators with full text search and the ability to search using advanced search queries enables complex searches across all indicator fields, including context fields. Filtering results by intelligence supplier simplifies the process of analyzing threat intelligence.

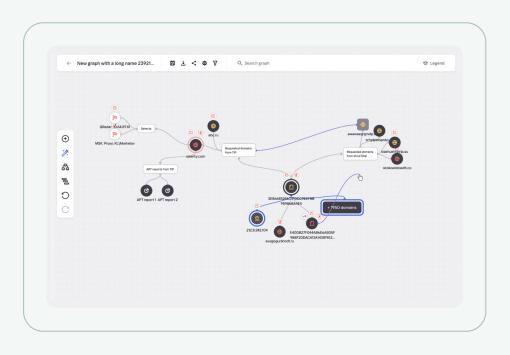
E-mail subscriptions and PDF documents from National/Government/ Financial Computer Emergency Response Teams (CERTs), TI vendors, and communities could be used as a source of IoCs for CyberTrace. Extraction of IOCs is possible from both email body and attachment (XML, CSV, JSON, PDF). IMAP/POP3 servers and local/shared folders with a collection of PDF files could be used as a feed source.

Kaspersky CyberTrace				edmin Timezone: UTC+3
in Dashboard 🔬 Searc	n 🕞 Retroscen 🛔	Indicators	is 💮 Settings 🖸 Tasks	II Help
K Back Mark as failse	positive Add to Internal TI	Delete		
Type IP	Added on First d 2021-01-21 22:38 —	etected on		
Value 123 253 110 198 Associated detections Browse in external resources	Last updated on Last d 2021-01-21 22:38 —	stected on		
KTIP Suppliers				
IP_Reputation_Data_Feed Confidence Type 100 Ip	Use for matching true	Updated 2021-01-21 22:38	Send detection events	
Indicator context category: botnet_cnc			ip_whois/descr: UC.NET	
first_seen: 21.01.2021.16:12 ip: <u>123.253.110.198</u> ip_geo: jp			ip_whois/net_name. JP-Colt ip_whois/net_range: 123 253.110.0 - 123.253.110.255 last_seer: 21.01.2021 16.50	
ip_whois/contact_owner_email	noc@ijc.net		popularity: 1	
ip_whois/country: JP ip_whois/created: 10.09.2020			threat_score: 100	
Comments				
Add comment here				
Add comment				
Kaspersky CyberTrace v4.0.0.6481 © 2021 AO Kaspersky Lab				kaspersky

Pages with detailed information about each indicator provide even deeper analysis. Each page presents all information about an indicator from all threat intelligence suppliers (deduplication) so analysts can discuss threats in the comments and add internal threat intelligence about the indicator. If the indicator was detected, the information about detection dates and links to the detections list will be available.

#### **Research Graph**

A Research Graph allows to visually explore data and detections stored in CyberTrace and discover threat commonalities. It allows graphic visualization of the relationship between URLs, domains, IPs, files, and other contexts encountered during investigations. The graph includes the following features: transformations, mini graph, grouping nodes, manually adding of links, adding indicators and searching for nodes on the graph. IoCs enrichment on Research Graph from VirusTotal is supported.



#### Indicators export task

The indicators export feature supports native integration of exported IoCs with third-party security controls such as policies lists (block lists) as well as the sharing of threat data between Kaspersky CyberTrace instances or with other TI Platforms.

b Dashboard	🛆 Search 🔞 Retroscan	🛞 Indicators 🖉 Detections 🛞 :	iettings 🔄 Tasks				🛄 Help					
11 Service	Add indicators export task					×						
Indicator	Task properties         Meanwin reside         Extern way         Delimar           "San year         (S000)         San year         (San year)											
No indicate	Limit access to specified credentials											
	Unit access to spectrate Creatmans											
	User name Password											
	Fields to export											
	Field name	Output name										
	ioc_value ~	value is non-empty *			ioc_value	Ť						
	AND supplier_confidence v value is more than (inclusive) v 70											
	AND ioc_first_detected_date V	date is more than (inclusive)	%NOW% - 7			0						
	Add new filter											
	Sort conditions Condition name Dir	ection										
		Descending	~ 0									
	Add sort conditions											
					Next	Cancel						

#### loC tags

Tagging loCs simplifies their management. You can create any tag and specify its weight (importance) and use it to tag loCs manually. You can also sort and filter loCs based on these tags and their weights.

# Tags Add tags Create new tag Manage all tags Total tags weight: 13 Image: BFSI Image: Russia Image: R

#### **Restroscan** feature

The historical correlation feature (retroscan) lets you analyze observables from previously checked events using the latest feeds to find previously uncovered threats. All historical detections are included in the report for future investigations.

Kaspersky CyberTrace				admin ∽ Timezone: UTC+3
) Dashboard 💪 See	arch 🕄 Retroscan	∭ Indicators ∠1 Detect	tions N/ Graph 😅 Tasks 1 💮 Settings	III Help
			Sur Letonocum Neur Invesses 124 49 110 2023 Sand ener 9 6440 Sand Letono 1 644 100 Sand Letono 1 644 100 Sand Letono 2 20	
etroscan results period Day Week Show only retroscan result Retroscan result		All time Custom range		
Day Week	s with detection	All time Custom range	Detected indicators	
Day Week Show only retroscan result Retroscan result	s with detection		Detected indicators	
Day Week Show only retroscen result Retroscan resul Status	s with detection JITS Date	Scenned events		
Day Week Show only retroscan result Retroscan result Status Detected	s with desection JLTS Date 2023-01-12.20.18.41	Scanned events 9 216 816	3	
Day Week Show only retroscan result Retroscan result Status Detected V Not detected	s with detection <b>Jlts</b> Date 2023-01-12 20:18:41 2023-01-12 20:06:02	Scanned events 9 216 816 9 216 813	3 0	
Day Week Show only retroscen result Retroscan result Status Detected Viol detected Viol detected	s with detection <b>Jits</b> <b>Date</b> 2023-01-12 20 18 41 2023-01-12 20 06 02 2023-01-12 13 44 47	Scanned events 9 216 816 9 216 813 9 216 813	3 0 0	

#### **Event source filters**

A filter for sending detection events to SIEM solutions reduces the load on them and on the analyst battling alert fatigue. It allows you to send only the most dangerous detections, those that must be treated as incidents, to SIEM. All other detections are saved to the internal database and can be used during root cause analysis or in threat hunting.

🏽 Indicators 🛆 Detections 🔊 Graph 📑 Tasks 2. 🔕 Settings	CD <u>Help</u>
export 🛄 Matching 🗔 Retroscan 🏠 Detections ≫ Events format 🛞 Users 🚊 Tenants 🗊 Logging 🗊 Licensing	
Edit default rules	
7p≈ Hostname ♥ Wile: Iocahost	/ 11
Type: RegEup V Value: cef	/ 8
A solution. For more information, see Help Contain Wile	
value is more than (inclusive) OR field is not present v	Ð
	epor () Marching (), Reinston (), Deections ()e Beins format (e) Users () Tenants (i) Logang (i) Usersing Est ontwinner 7 per Host name V Male (incomposition) 7 per Magibio V Male (incomposition) 7 per Magibio V Male (incomposition) totalison for more information, see <u>Balo</u> Constant View

#### Multitenancy support

Multitenancy supports MSSPs or large enterprise use cases when a service provider (central office) needs to handle events from different branches (tenants) separately. This allows a single Kaspersky CyberTrace instance to be connected with different SIEM solutions from different tenants, and you can configure which feeds are to be used for each tenant.

🗿 Dashboard 💪 Search 🖓 Retroscan 👾 Indicator	s 🖉 Detections 💮	Settings 🕑 Tasks	🖽 Help
👔 Service 🔠 Feeds 📋 Indicators export 🔲 Matching 😪 R	erroso New tenant	×	
	Tenant *	SPB	
Tenants Add new tenant	Description	saint petersburg office	
Tenant: General	Select a SIEM *	LogRhythm ~	
Description: General settings applied to all tenants by default	Service listens on:	IP and port UNIX socket	
	IP address *	0.0.0.0	
	Port *	9978	
	Service sends events to:		
	IP address *	10.65.9717	
	Port *	514	
	* Required fields	Add Cancel	
	required rates	Carcos	

#### Indicator statistics

## and feeds intersection matrix

Feed usage statistics for measuring the effectiveness of the integrated feeds and feeds intersection matrix help choosing the most valuable threat intelligence suppliers.

սրբ	olier intersections																
		1	2	3	4	5	6	7	8	9	10	11	12	13	14	15	16
1	Kaspersky APT Hash Data Feed		0%	0%	0%	0%	0%	0%	0%	0%	0%	8%	0%	0%	0%	0%	0%
2	Kaspersky APT IP Data Feed	0%		0%	3%	0%	0%	0%	0%	3%	0%	0%	2%	0%	0%	0%	0%
3	Kaspersky APT URL Data Feed	0%	0%		5%	0%	0%	0%	0%	0%	0%	0%	1%	0%	0%	0%	0%
4	Kaspersky Botnet CnC URL Data Re	0%	0%	0%		1%	0%	0%	0%	4%	0%	0%	3%	2%	0%	0%	3%
5	Kaspersky Demo Botnet CnC URL	0%	0%	1%	100%		0%	0%	0%	17%	0%	0%	55%	6%	0%	0%	9%
6	Kaspersky Demo IP Reputation Dat	0%	0%	0%	39%	9%		0%	0%	99%	0%	0%	31%	7%	0%	0%	1%
7	Kaspersky Demo Malicious Hash D	0%	0%	0%	0%	0%	0%		25%	0%	0%	100%	0%	0%	0%	0%	0%
8	Kaspersky ICS Hash Data Feed	0%	0%	0%	0%	0%	0%	0%		0%	0%	12%	0%	0%	0%	0%	0%
9	Kaspersky IP Reputation Data Feed	0%	0%	0%	32%	1%	0%	0%	0%		0%	0%	5%	6%	0%	0%	0%
10	Kaspersky IoT URL Data Feed	0%	0%	0%	0%	0%	0%	0%	0%	0%		3%	0%	0%	0%	0%	0%
11	Kaspersky Malicious Hash Data Fee	0%	0%	0%	0%	0%	0%	1%	10%	0%	0%		0%	0%	0%	0%	0%
12	Kaspersky Malicious URL Data Feet	0%	0%	0%	18%	4%	0%	0%	0%	4%	0%	0%		1%	0%	1%	5%
13	Kaspersky Mobile Botnet CnC URL	0%	0%	0%	100%	3%	0%	0%	0%	27%	0%	0%	5%		0%	0%	1%
14	Kaspersky Mobile Malicious Hash [	0%	0%	0%	0%	0%	0%	0%	0%	0%	0%	0%	0%	0%		0%	0%
15	Kaspersky Phishing URL Data Feed	0%	0%	0%	0%	0%	0%	0%	0%	0%	0%	0%	0%	0%	0%		0%
16	Kaspersky Ransomware URL Data	0%	0%	0%	21%	1%	0%	0%	0%	0%	0%	0%	5%	0%	0%	0%	

#### HTTP RestAPI allows you to look up and manage threat intelligence

By using the Rest API, Kaspersky CyberTrace can be easily integrated into complex environments for automation and orchestration. Integration with Kaspersky's incident monitoring, analysis, and response platform.

## Other product features

- SIEM connectors for a wide range of SIEM solutions to visualize and manage data about threat detections
- On-demand lookup of indicators (hashes, IP addresses, domains, URLs) for in-depth threat investigation
- Advanced filtering for feeds
- Bulk scanning of logs and files
- Command-line interface for Windows and Linux platforms
- Stand-alone mode, where Kaspersky CyberTrace receives and parses the logs from various sources such as network devices
- And much more

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, organizations can:

#### (心)

-Δ

Effectively distill and prioritize security alerts.

Immediately identify critical

decisions about escalation to incident response teams.

alerts and make more informed



Reduce analyst workload and prevent burnout.



Build a proactive and intelligence-driven defense.



Learn more

www.kaspersky.com

© 2024 AO Kaspersky Lab. Registered trademarks and service marks are the property of their respective owners. #kaspersky #bringonthefuture