Kaspersky
Security Day
2021

Что означает быть в курсе современных угроз? Threat Intelligence от лидера рынка

Булат Сираев,
Deputy Head of Global Enterprise Sales

kaspersky

Определение

> Threat intelligence - это основанные на фактических данных **знания, включая контекст, механизмы, индикаторы,** последствия и действенные рекомендации, о существующей или возникающей угрозе или угрозе активам, которые могут использоваться для **принятия решений** относительно реакции субъекта на эту угрозу или опасность.

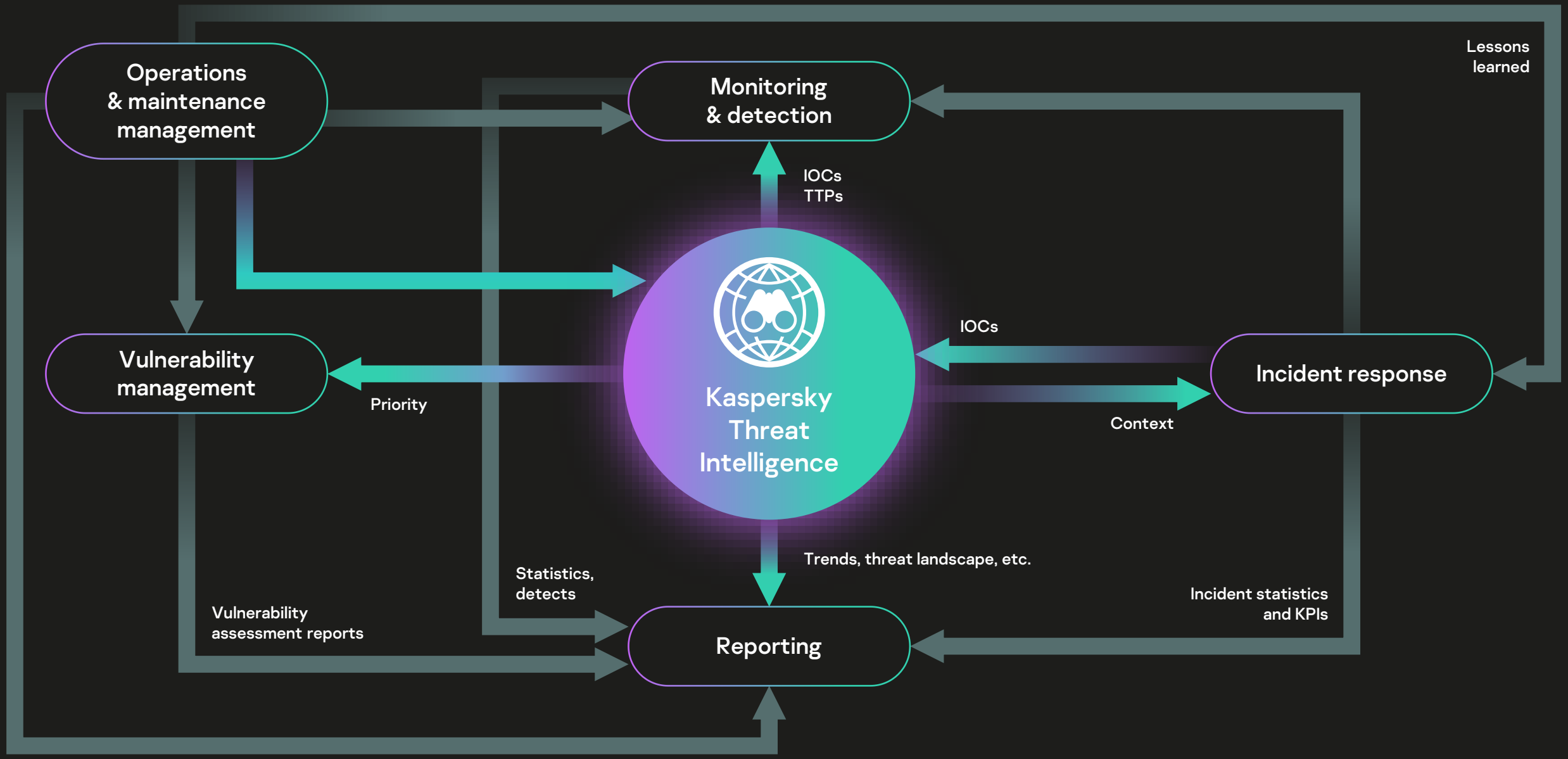
Gartner

История рынка

2021


Акции S
обвалил
May 19, 2021
1:02 AM MSK
В сеть стратегически важного поставщика IT-решений для американских правительственных организаций SolarWinds хакеры ходят как к себе домой.
Вскоре после публикации FireEye материалов в отношении выявленной компрометации
https://www.cnbc.com/2021/05/13/colonial-pipeline-paid-ransom-to-hackers-source-says.html
CNBC
Colonial Pipeline paid $5 million ransom to hackers
Ransomware attacks involve malware that encrypts files on a device or network that results in the system becoming inoperable.
INSTANT VIEW
Side ransom
een them?
remote access
12,8K 12:22
Фото: Sashkin / Shutterstock

Роль в security operations



Типы данных об угрозах: Threat Intelligence

Технические

#Feeds
#MRTI
#Correlation

Операционные

#Расследования
#Исследования

Тактические

#TTPs
#Actors

Стратегические

#Тренды
#Целевая информация

Почему Threat Intelligence это важно?

Принятие решений за счет понимания действий злоумышленников

Детектирование угроз, выявление техник, тактик и процедур (TTP’s)

Управление рисками

Сценарии использования

Расследование

- Инструменты для ускорения расследований
- Threat Hunting

Реагирование

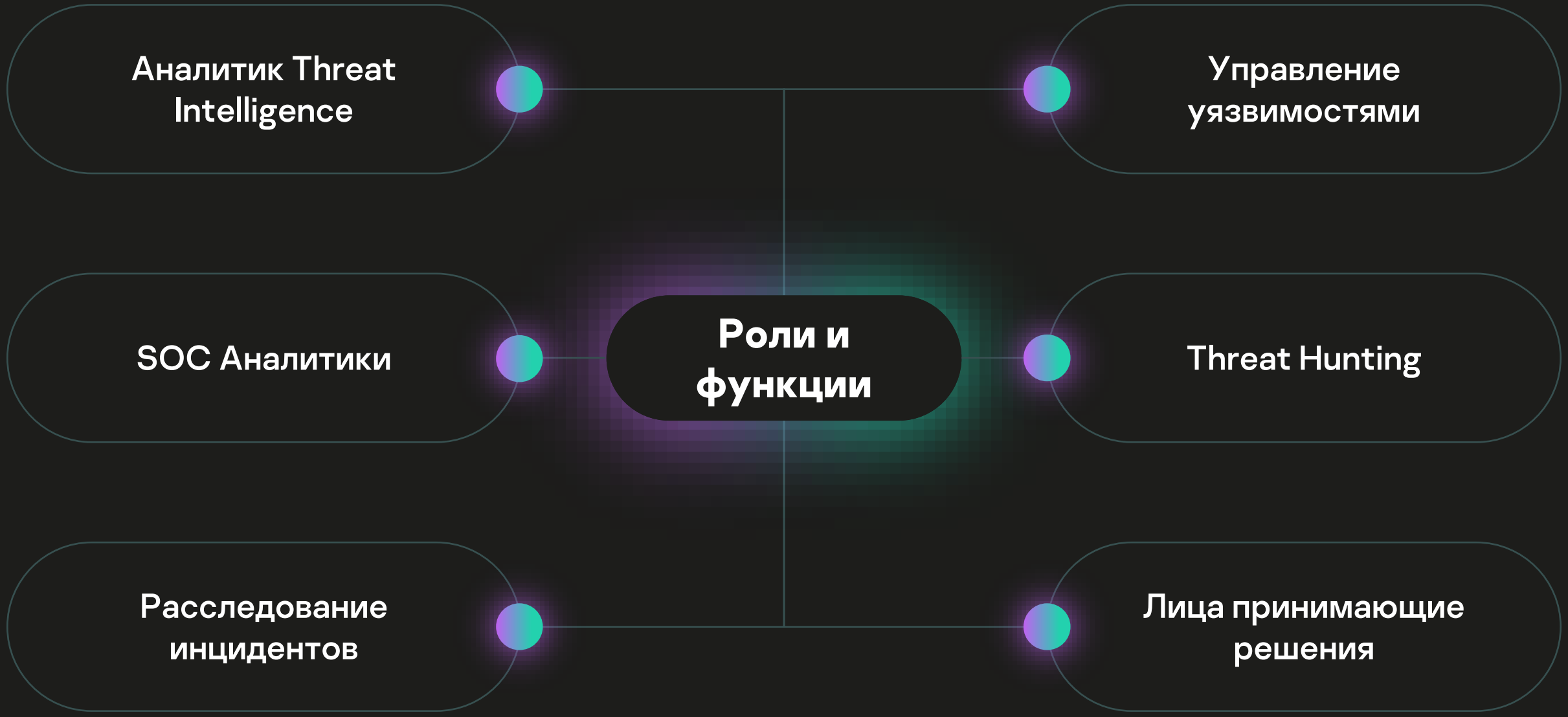
- Валидация событий и обогащение
- Приотиризация уязвимостей

Устранение

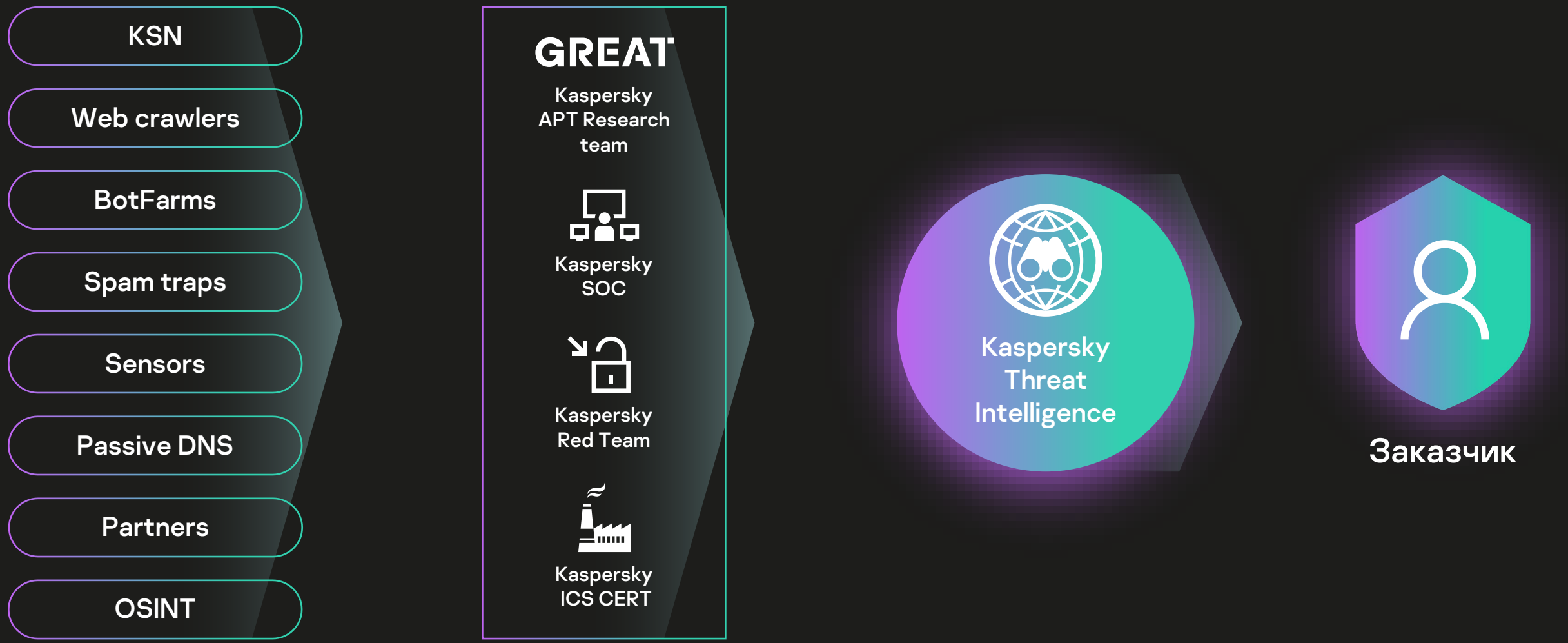
- Мониторинг бренда
- Takedown и блокировка ресурсов

Детектирование

- Обнаружение инцидентов
- Отслеживание источников
- Security Enrichment


Аналитик Threat Intelligence
Управление уязвимостями
SOC Аналитики
Роли и функции
Threat Hunting
Расследование инцидентов
Лица принимающие решения

Threat intelligence - источники



Исследования – публичные анонсы ЛК

2016

- Metel
- Saguaro
- Adwind
- StrongPity
- Lazarus
- Ghoul
- Lurk
- Fruity Armor
- GCMan
- ScarCruft
- Poseidon
- Danti
- Dropping Elephant
- ProjectSauron

2017

- StoneDrill
- WhiteBear
- BlueNoroff
- Silence
- ExPetr/ NotPetya
- ATMitch
- ShadowPad
- BlackOasis
- Shamoon 2.0
- WannaCry
- Moonlight Maze

2018

- Zebrocy
- DarkTequila
- MuddyWater
- Skygofree
- Olympic Destroyer
- ZooPark
- Hades
- Octopus
- AppleJeus

2019

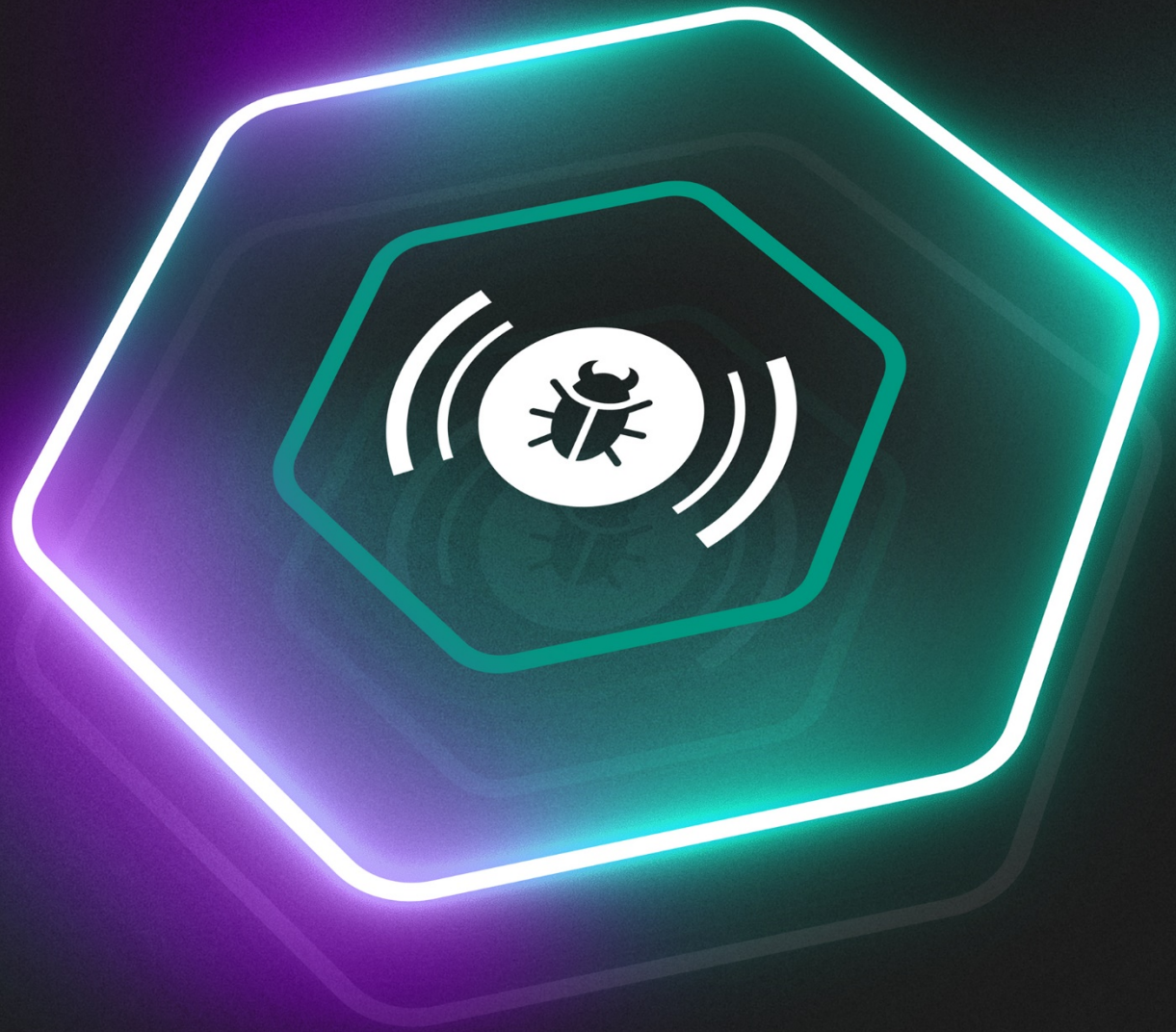
- Topinambour
- ShadowHammer
- SneakyPastes
- FinSpy
- DarkUniverse
- COMpfun
- Titanium

2020

- Cycldek
- MosaicRegressor
- SixLittle Monkeys (aka Microcin)
- VHD Ransomware
- CactusPete
- WildPressure
- DeathStalker
- PhantomLance
- MATA
- TransparentTribe
- WellMess
- TwoSail Junk
- MontysThree

Портфолио Kaspersky Threat Intelligence

Kaspersky Threat Data Feeds



Потоки данных об угрозах

Постоянное обновление данных об угрозах минимизирует число ложноположительных срабатываний

Информативный контекст позволяет оперативно реагировать на угрозы

Разнообразные форматы и механизмы предоставления сведений упрощают интеграцию с существующими средствами защиты

Потоки данных об угрозах

- IP REPUTATION FEED
- HASH FEED (WIN / *nix / MacOS / AndroidOS / iOS)
- URL FEEDS (Malicious, Phishing and C&C)
- RANSOMWARE URL FEED
- APT IOC FEEDS
- VULNERABILITY FEED
- PASSIVE DNS (pDNS) FEED
- IoT URL FEED
- WHITELISTING FEED
- ICS HASH FEED
- И ДРУГОЕ

Kaspersky Threat Data Feeds

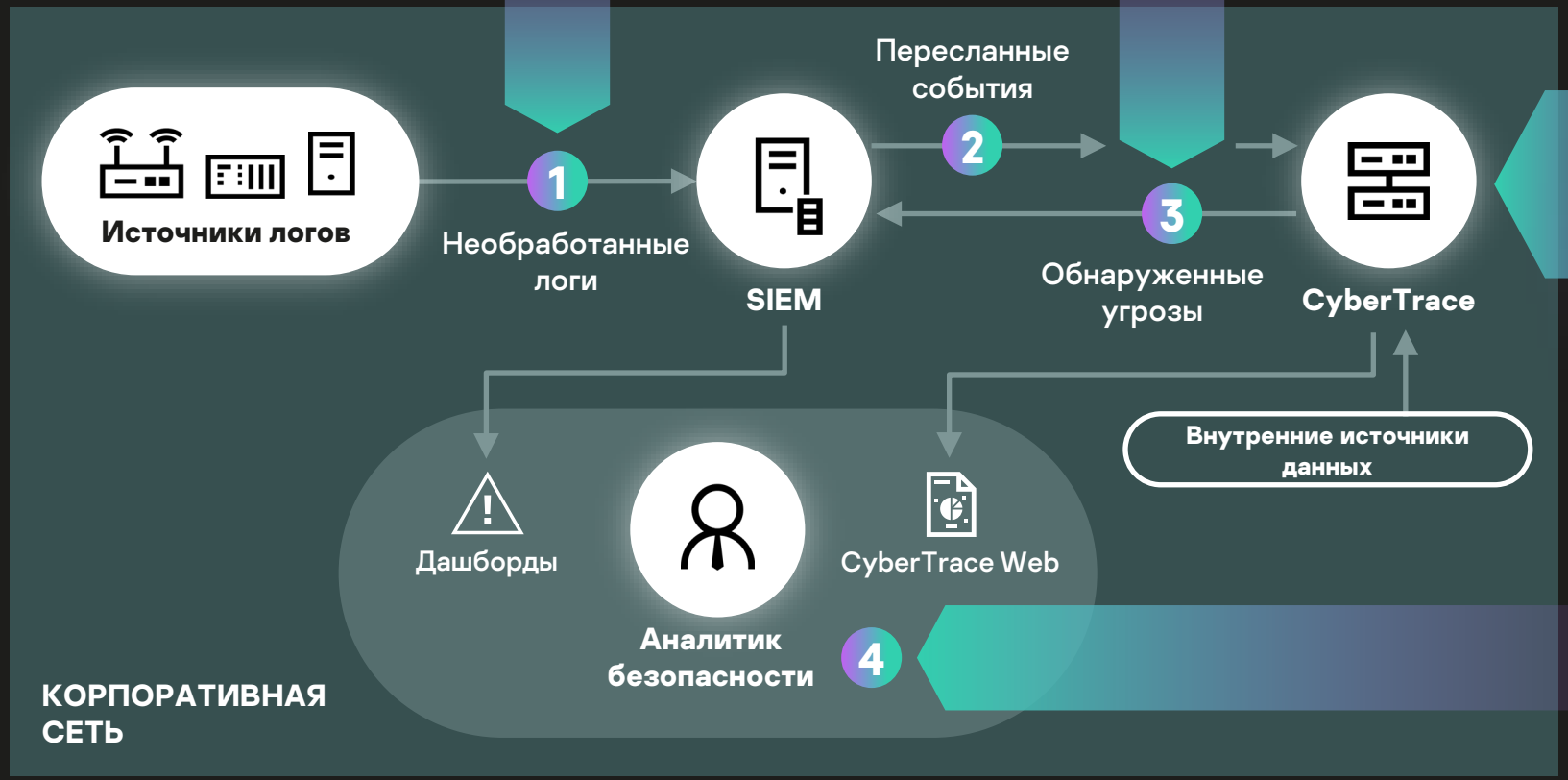
Kaspersky CyberTrace

Kaspersky CyberTrace объединяет аналитические данные из разных источников с решениями для обнаружения угроз и защиты от них. В результате пользователь может оперативно использовать аналитику угроз для мониторинга безопасности, защиты и реагирования на инциденты в рамках привычных процессов.

Kaspersky CyberTrace — платформа для управления данными о киберугрозах

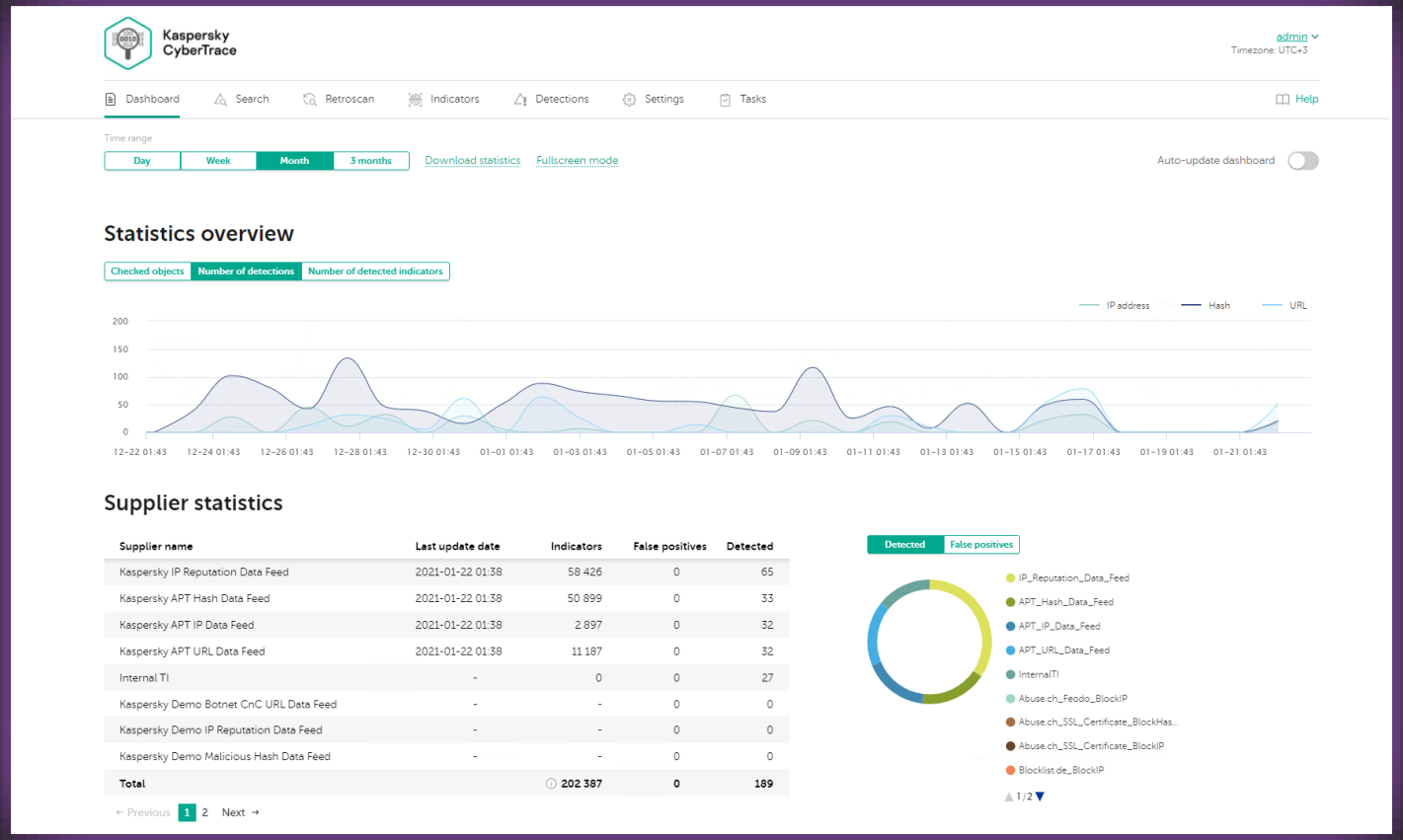
SIEM-система собирает журналы с различных устройств и IT-систем и отправляет данные о событиях с URL и IP-адресами и хэшами в CyberTrace на анализ

CyberTrace быстро сопоставляет поступающие события с потоками данных об угрозах и отправляет данные об обнаруженных угрозах в SIEM и CyberTrace Web



- Получает оповещения об обнаруженных угрозах с дополнительным контекстом
- Проводит первоначальное расследование и инициирует процесс реагирования на основе контекста

CyberTrace



База данных для хранения и поиска по данным (+ retroscan)

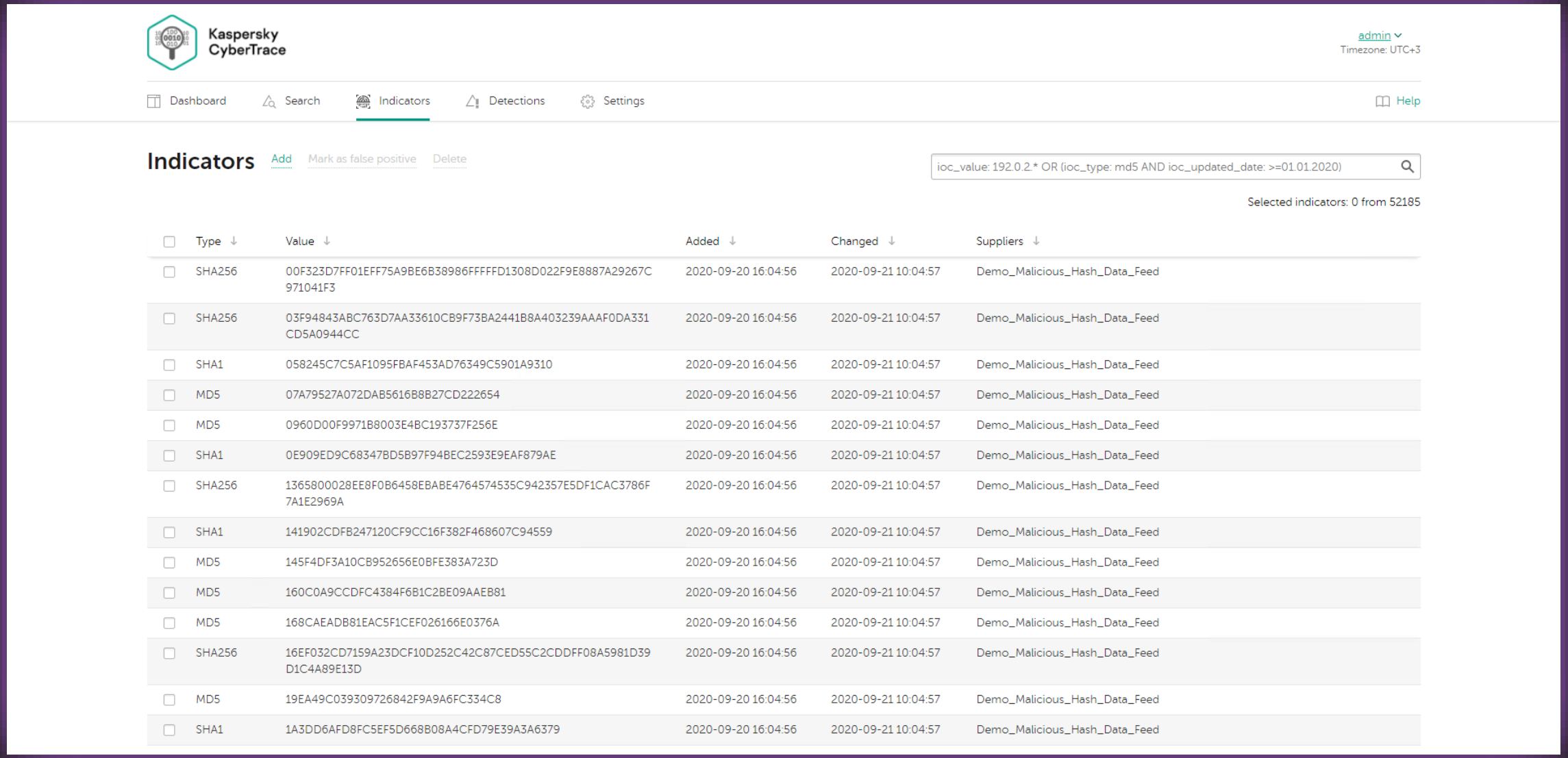
Агрегация, дедупликация, нормализация и обмен данными

Статистика обнаружений и матрица пересечений по потокам даных

Публичный API (для интеграции и автоматизации)

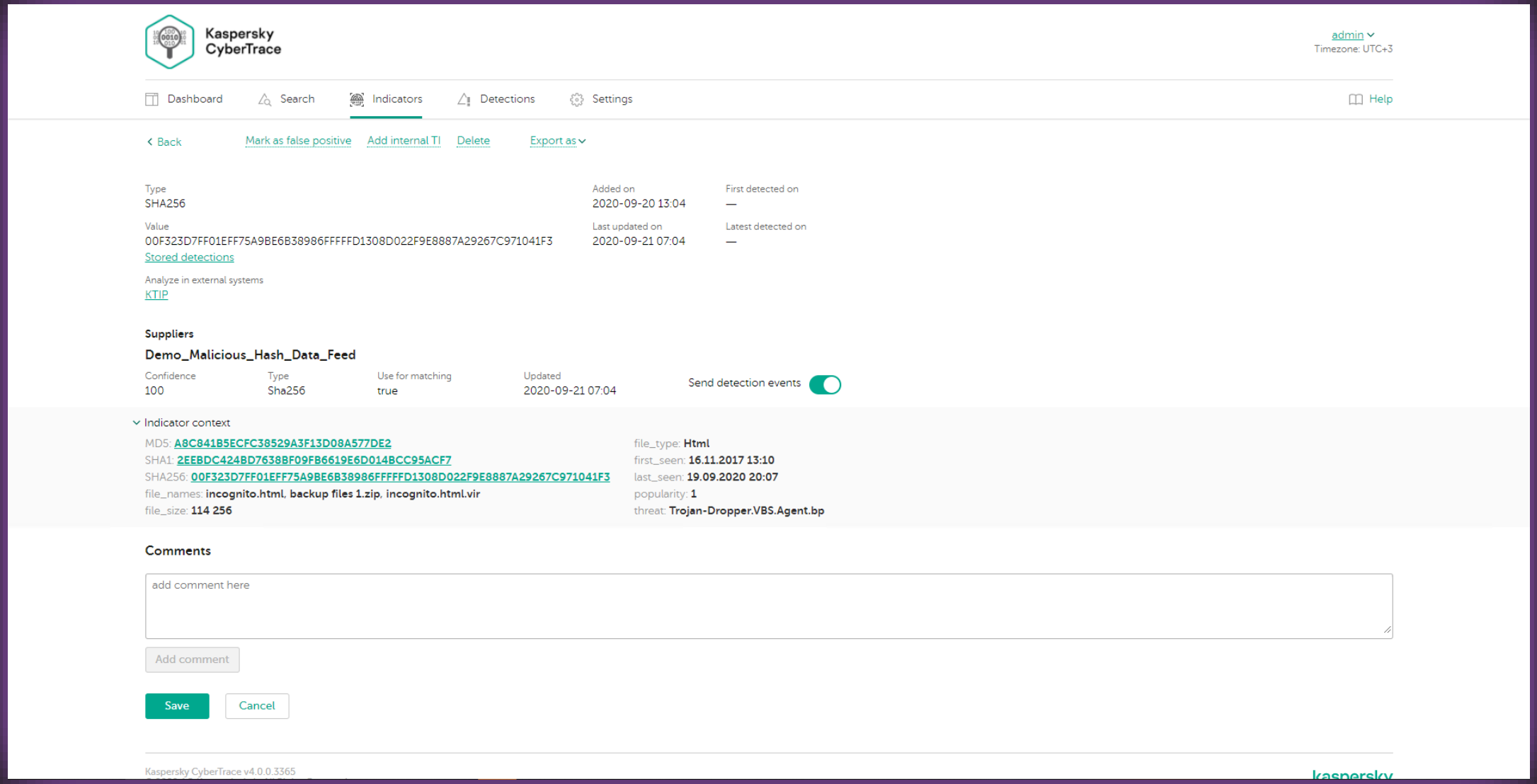
Мультитенантность для MSSP и крупных предприятий

База данных об индикаторах с полнотекстовым поиском

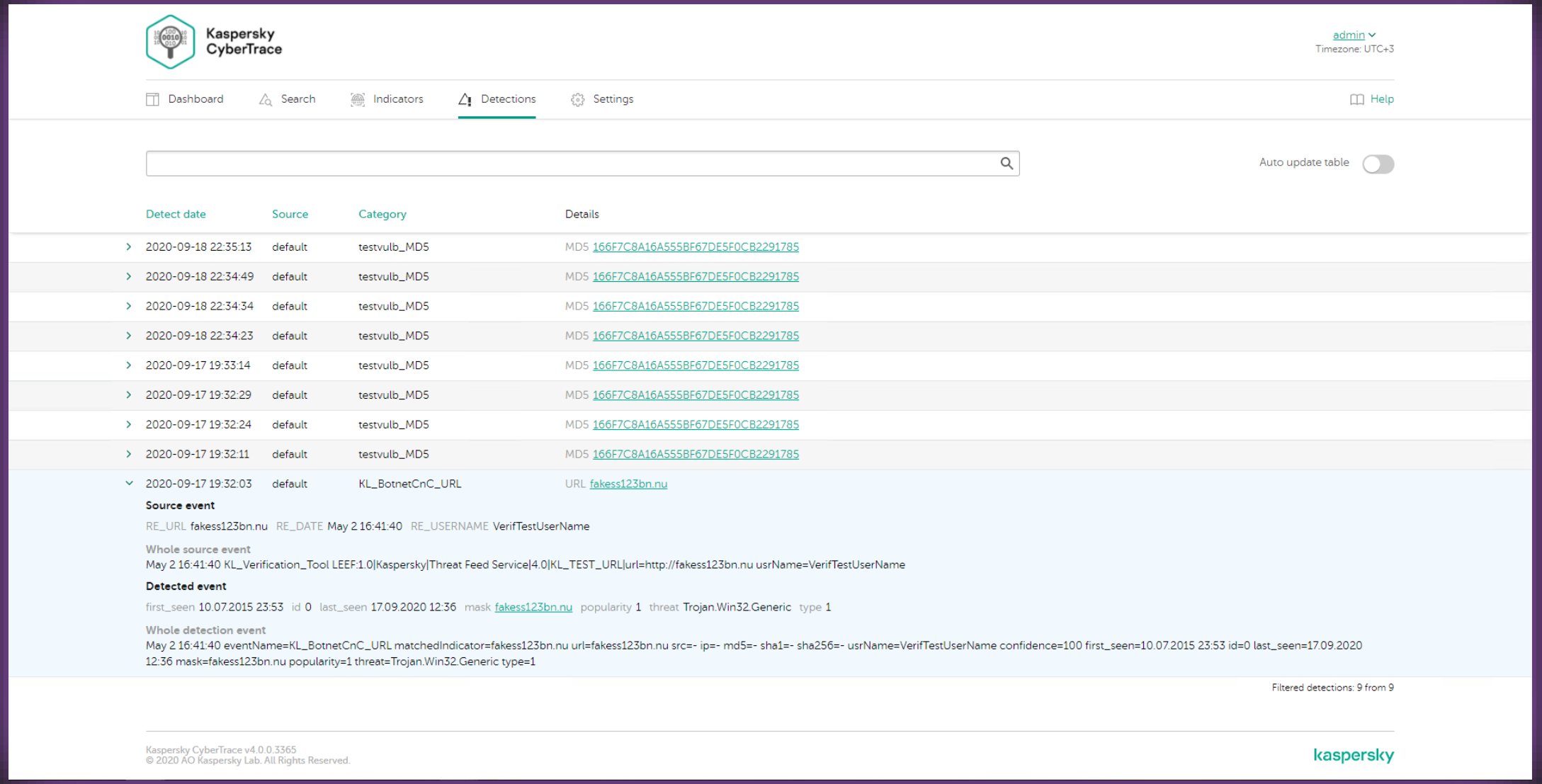


Type	Value	Added	Changed	Suppliers
SHA256	00F323D7FF01EFF75A9BE6B38986FFFFFD1308D022F9E8887A29267C971041F3	2020-09-20 16:04:56	2020-09-21 10:04:57	Demo_Malicious_Hash_Data_Feed
SHA256	03F94843ABC763D7AA33610CB9F73BA2441B8A403239AAAF0DA331CD5A0944CC	2020-09-20 16:04:56	2020-09-21 10:04:57	Demo_Malicious_Hash_Data_Feed
SHA1	058245C7C5AF1095FBAF453AD76349C5901A9310	2020-09-20 16:04:56	2020-09-21 10:04:57	Demo_Malicious_Hash_Data_Feed
MD5	07A79527A072DAB5616B8B27CD222654	2020-09-20 16:04:56	2020-09-21 10:04:57	Demo_Malicious_Hash_Data_Feed
MD5	0960D00F9971B8003E4BC193737F256E	2020-09-20 16:04:56	2020-09-21 10:04:57	Demo_Malicious_Hash_Data_Feed
SHA1	0E909ED9C68347BD5B97F94BEC2593E9EAF879AE	2020-09-20 16:04:56	2020-09-21 10:04:57	Demo_Malicious_Hash_Data_Feed
SHA256	1365800028EE8F0B6458EBABE4764574535C942357E5DF1CAC3786F7A1E2969A	2020-09-20 16:04:56	2020-09-21 10:04:57	Demo_Malicious_Hash_Data_Feed
SHA1	141902CDFB247120CF9CC16F382F468607C94559	2020-09-20 16:04:56	2020-09-21 10:04:57	Demo_Malicious_Hash_Data_Feed
MD5	145F4DF3A10CB952656E0BFE383A723D	2020-09-20 16:04:56	2020-09-21 10:04:57	Demo_Malicious_Hash_Data_Feed
MD5	160C0A9CCDFC4384F6B1C2BE09AAEB81	2020-09-20 16:04:56	2020-09-21 10:04:57	Demo_Malicious_Hash_Data_Feed
MD5	168CAEADB81EAC5F1CEF026166E0376A	2020-09-20 16:04:56	2020-09-21 10:04:57	Demo_Malicious_Hash_Data_Feed
SHA256	16EF032CD7159A23DCF10D252C42C87CED55C2CDDFF08A5981D39D1C4A89E13D	2020-09-20 16:04:56	2020-09-21 10:04:57	Demo_Malicious_Hash_Data_Feed
MD5	19EA49C039309726842F9A9A6FC334C8	2020-09-20 16:04:56	2020-09-21 10:04:57	Demo_Malicious_Hash_Data_Feed
SHA1	1A3DD6AFD8FC5EF5D668B08A4CFD79E39A3A6379	2020-09-20 16:04:56	2020-09-21 10:04:57	Demo_Malicious_Hash_Data_Feed

Подробная информация о каждом добавленном индикаторе для более глубокого анализа



Хранилище данных об обнаружении: упрощает мониторинг безопасности и приоритизацию оповещений



Kaspersky Threat Lookup

Kaspersky Threat Lookup

Объекты для анализа

- Файлы
- URL-адреса
- Домены
- IP-адреса
- Хеши

Поиск информации

Kaspersky Threat Lookup

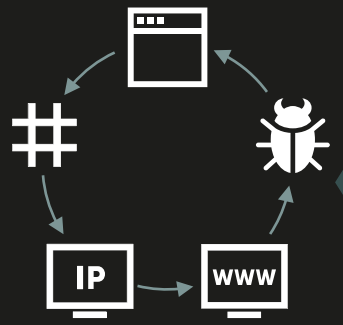
поиска угроз

РЕАГИРОВАНИЕ НА ИНЦИДЕНТ

- Объект вредоносный?
- Компания под угрозой?
- Какова цель угрозы?
- Какие есть взаимосвязи?

Контекстуальная аналитика

Автоматическое сопоставление

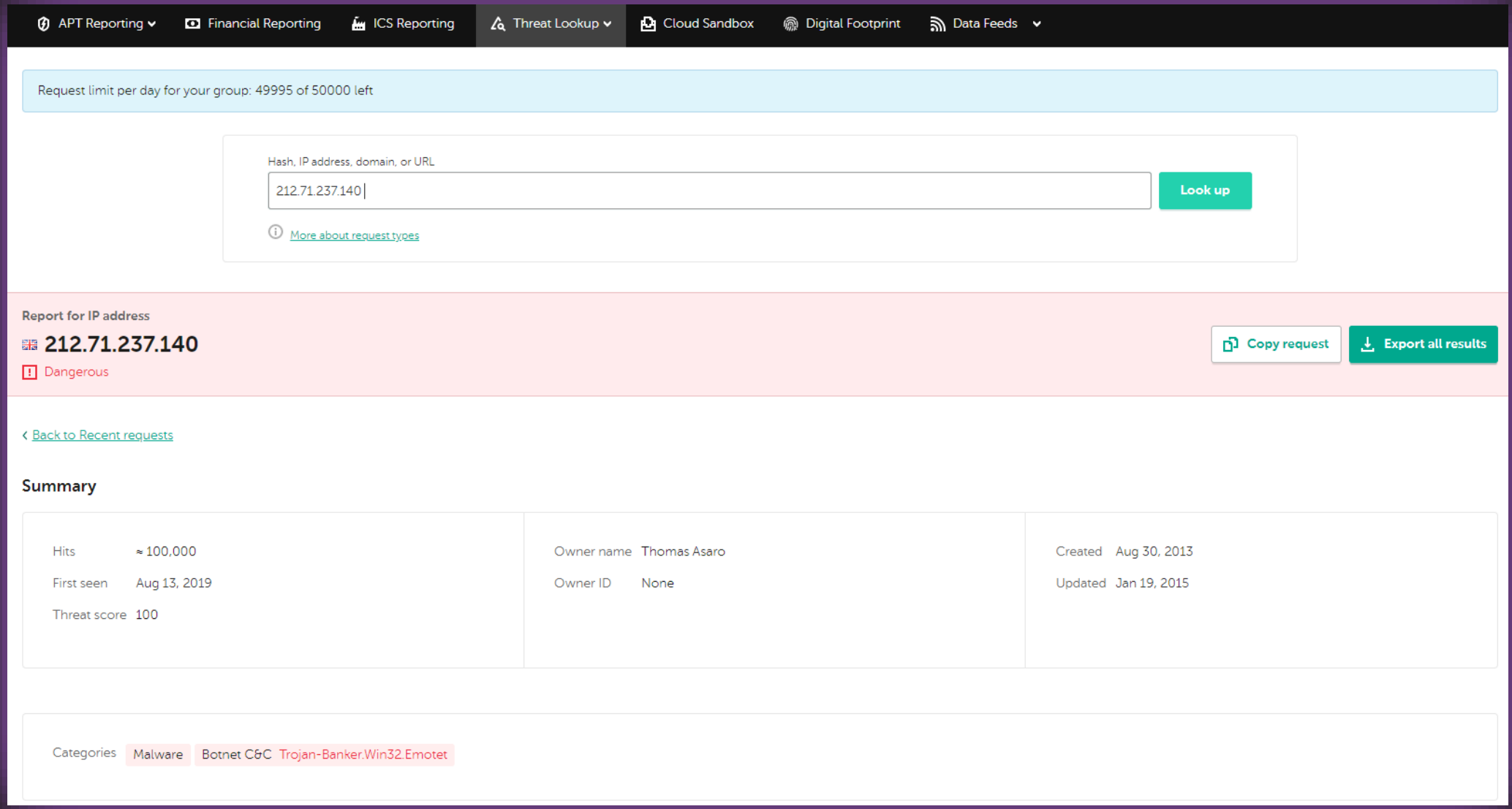


Данные

Источники

- Kaspersky Security Network
- Поисковые роботы
- Ловушки для спама
- Мониторинг ботнет-угроз
- Пассивная репликация DNS
- Сенсоры
- Партнеры

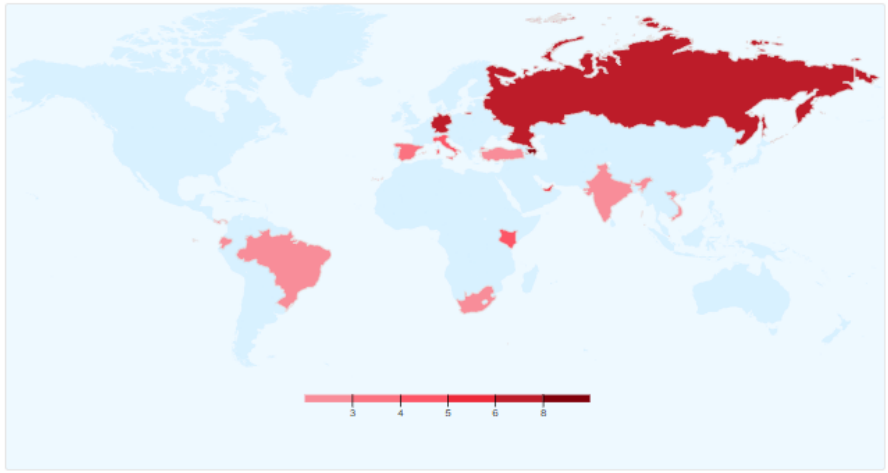
Kaspersky Threat Lookup: результат по запросу



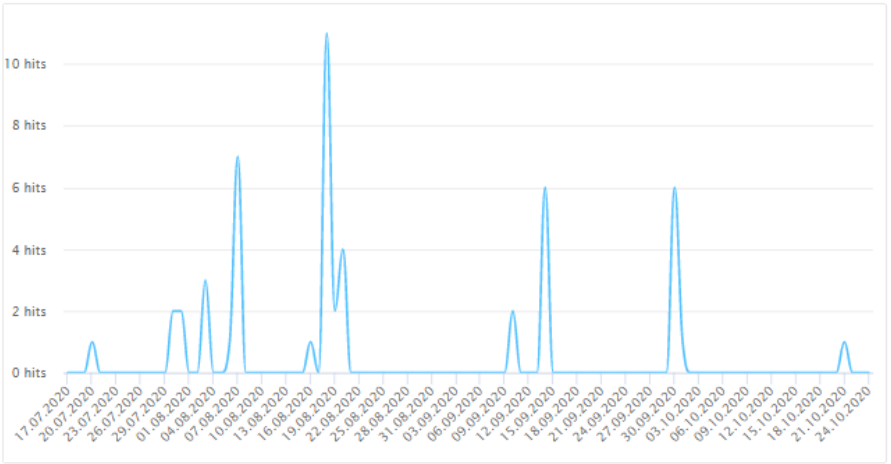
Kaspersky Threat Lookup: контекстная информация

APT Reporting | Financial Reporting | ICS Reporting | Threat Lookup | Cloud Sandbox | Digital Footprint | Data Feeds

Geography



Anti-Virus Statistics

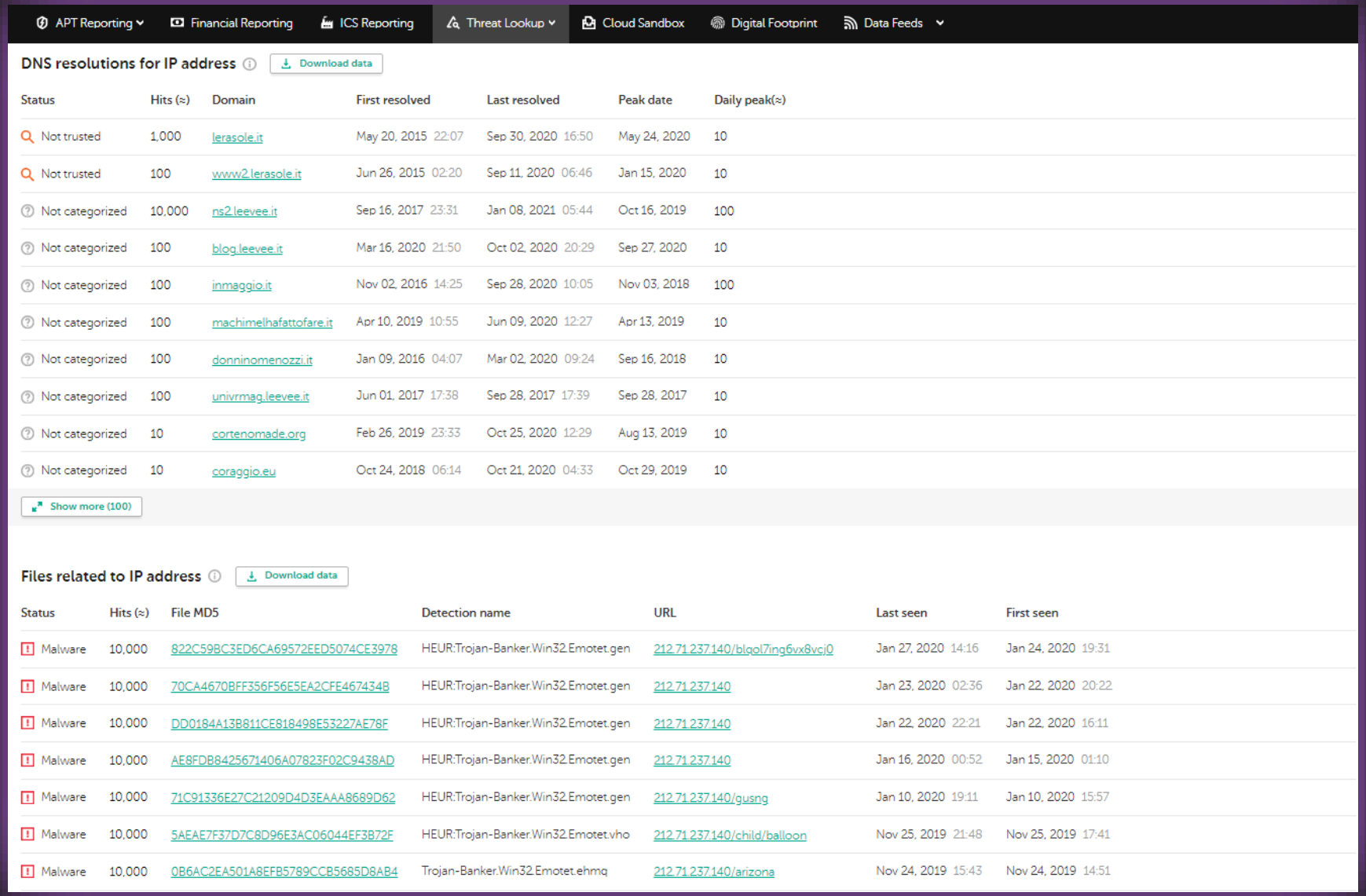


WHOIS

IP range	212.71.236.0-212.71.239.255	Created	Aug 30, 2013
Net name	LINODE-UK	Changed	Jan 19, 2015
Net description	Linode, LLC	AS description	Linode
		ASN	15830

Contact	Name	Role	Address	Phone / Fax	Email
person	Thomas Asaro	tech	329 E. Jimmie Leeds Road, Suite A, Galloway, NJ 08205, USA	+16093807504 Phone	–
person	Thomas Asaro	admin	329 E. Jimmie Leeds Road, Suite A, Galloway, NJ 08205, USA	+16093807504 Phone	–
person	Linode Abuse Support	tech	329 E. Jimmie Leeds Road, Suite A, Galloway, NJ 08205, USA	+16093807100 Phone	–

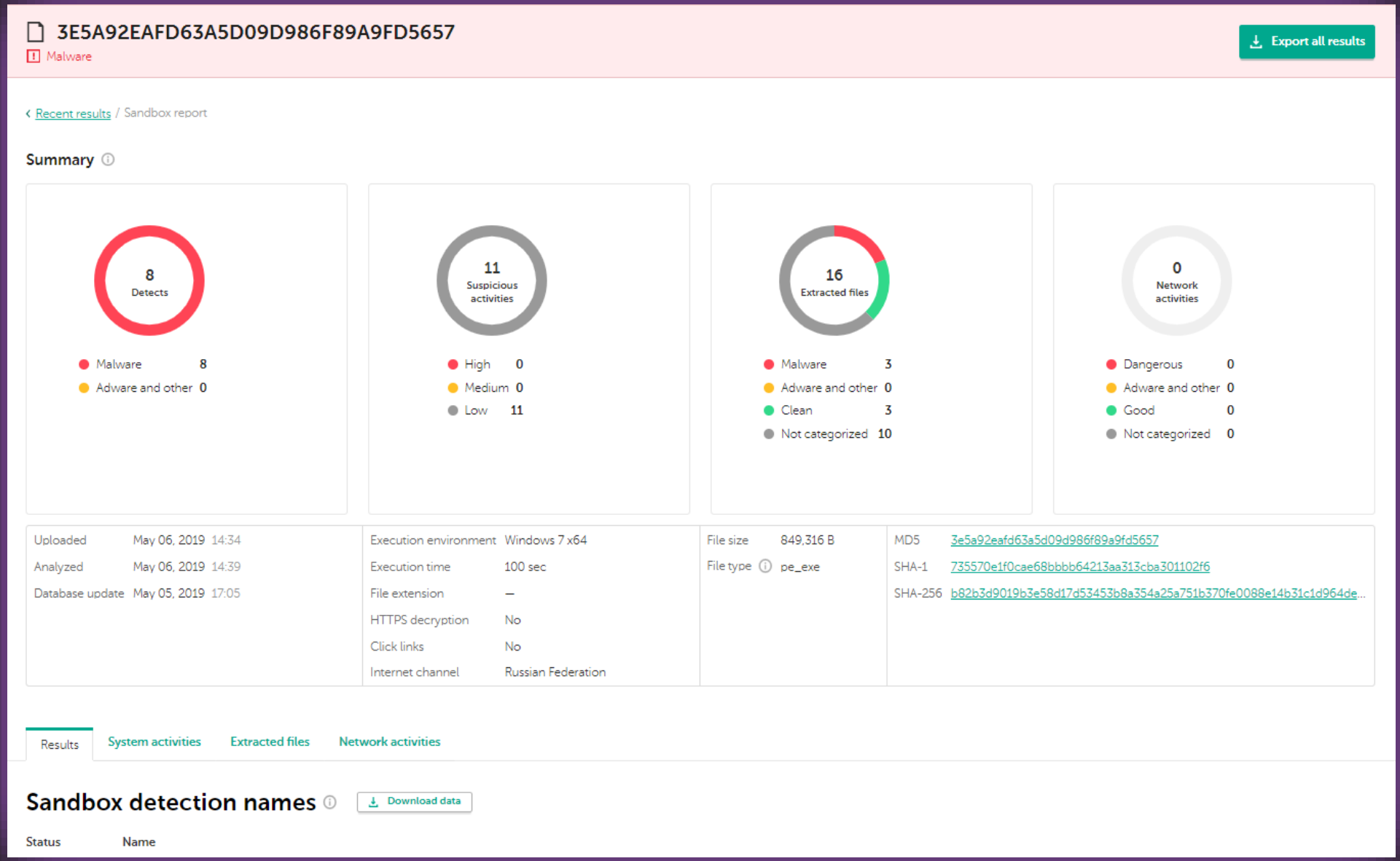
Kaspersky Threat Lookup: взаимосвязанные индикаторы



Kaspersky Cloud Sandbox

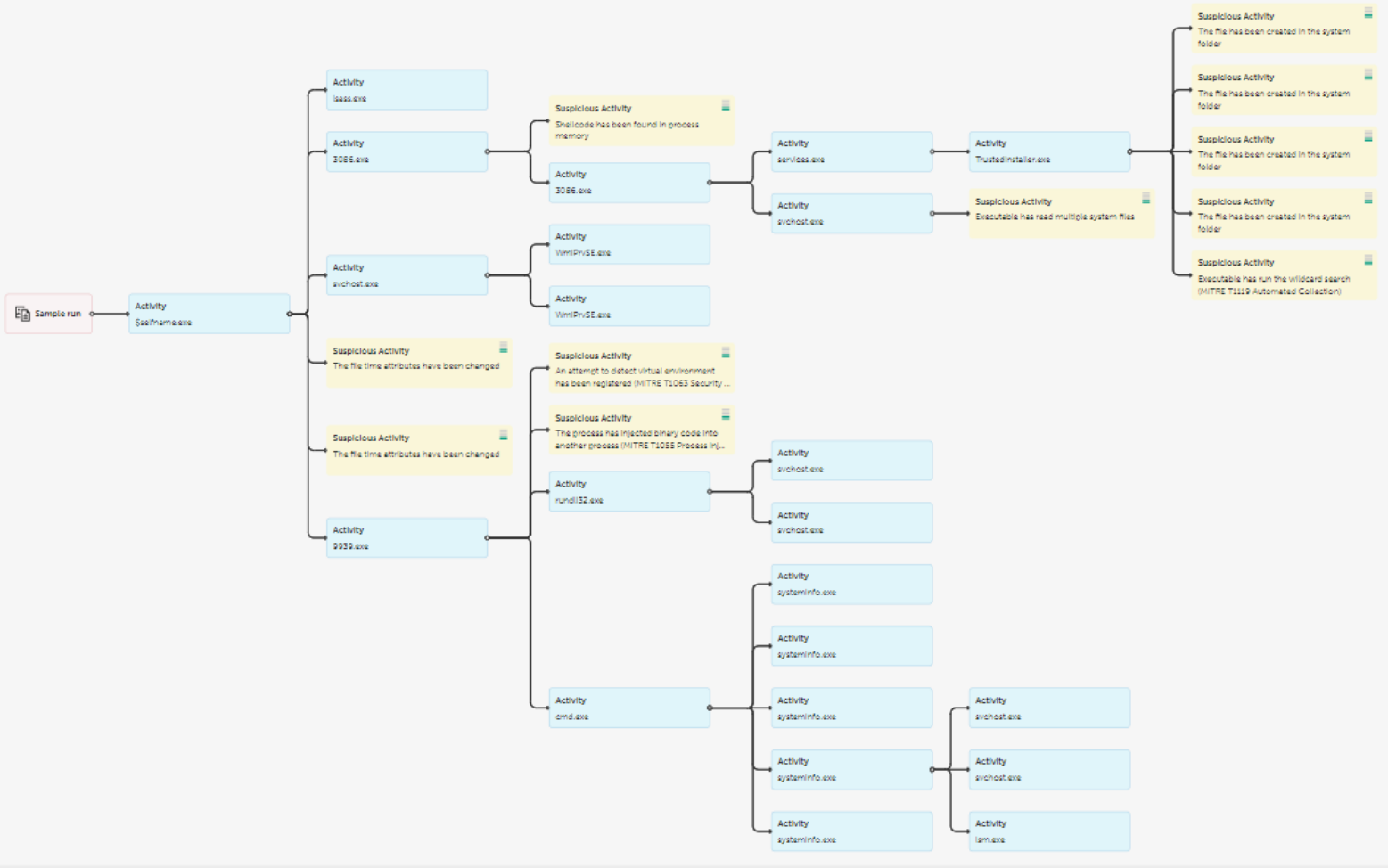
Kaspersky Cloud Sandbox

Kaspersky Cloud Sandbox: информационная панель



Kaspersky Cloud Sandbox: карта выполнения

Execution map



Kaspersky Cloud Sandbox: отслеживание подозрительного поведения и снимки экрана

Suspicious activities

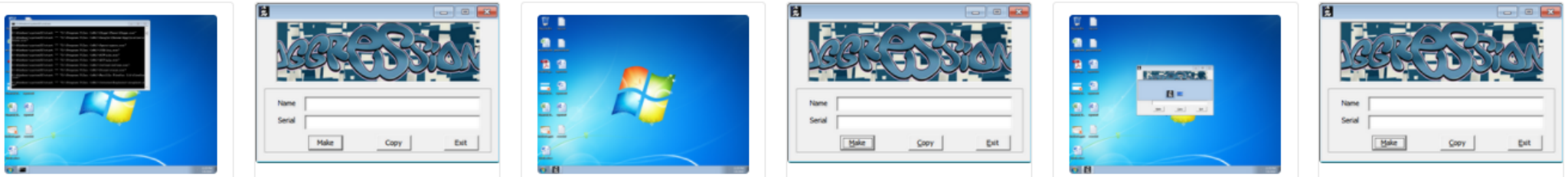
Download data

Status	Severity	Description
Low	290	The process $windir\servicing\TrustedInstaller.exe has created the file in the system folder: $windir\$system32\config\COMPONENTS{016888b8-6c6f-11de-8d1d-001e0bcde3ec}.TxR.blf.
Low	290	The process $windir\servicing\TrustedInstaller.exe has created the file in the system folder: $windir\$system32\config\COMPONENTS{016888b8-6c6f-11de-8d1d-001e0bcde3ec}.TxR.0.regtrans-ms.
Low	290	Shellcode has been found in the memory of the process $user\$temp\RarSFX0\3086.exe.
Low	290	The process $user\$temp\RarSFX0\9939.exe has attempted to detect a virtual environment (MITRE: T1063 Security Software Discovery).
Low	290	The process $user\$temp\RarSFX0\9939.exe has injected the binary code into the process $windir\$system32\rundll32.exe (MITRE: T1055 Process Injection).
Low	290	The process $windir\$system32\svchost.exe has read multiple system files.
Low	290	The process $windir\servicing\TrustedInstaller.exe has created the file in the system folder: $windir\$system32\config\COMPONENTS{016888b8-6c6f-11de-8d1d-001e0bcde3ec}.TxR.1.regtrans-ms.
Low	290	The process $windir\servicing\TrustedInstaller.exe has created the file in the system folder: $windir\$system32\config\COMPONENTS{016888b8-6c6f-11de-8d1d-001e0bcde3ec}.TxR.2.regtrans-ms.
Low	200	The process $windir\servicing\TrustedInstaller.exe has run the wildcard search: $windir\servicing\sqm*.sqm (MITRE: T1119 Automated Collection).
Low	100	The process $selfpath\$selfname.exe has modified the time attributes of the file $user\$temp\RarSFX0\3086.exe.

Show more (100)

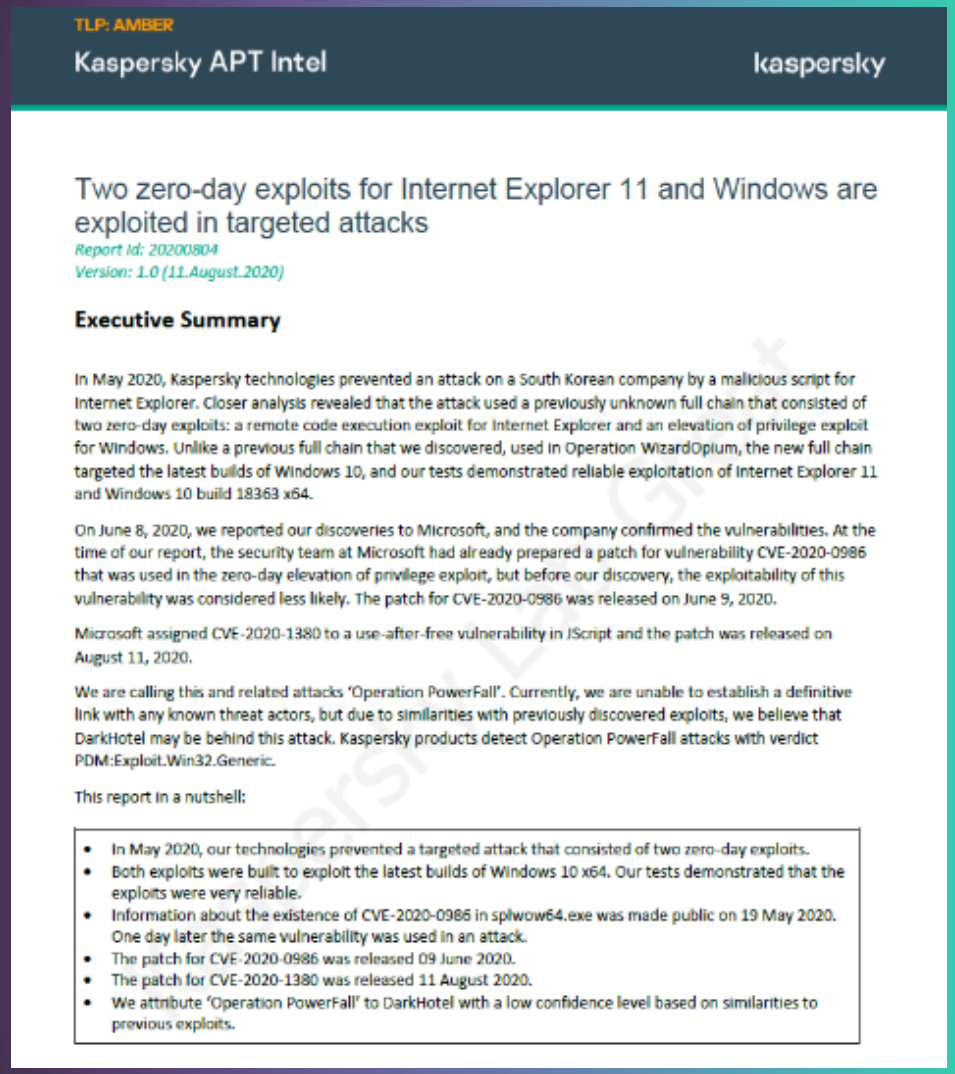
Screenshots (19)

Download data



Аналитические отчеты об APT-угрозах

Аналитические отчеты об APT-угрозах



TLP: AMBER

Kaspersky APT Intel

kaspersky

Two zero-day exploits for Internet Explorer 11 and Windows are exploited in targeted attacks

Report Id: 20200804
Version: 1.0 (11.August.2020)

Executive Summary

In May 2020, Kaspersky technologies prevented an attack on a South Korean company by a malicious script for Internet Explorer. Closer analysis revealed that the attack used a previously unknown full chain that consisted of two zero-day exploits: a remote code execution exploit for Internet Explorer and an elevation of privilege exploit for Windows. Unlike a previous full chain that we discovered, used in Operation WizardOpium, the new full chain targeted the latest builds of Windows 10, and our tests demonstrated reliable exploitation of Internet Explorer 11 and Windows 10 build 18363 x64.

On June 8, 2020, we reported our discoveries to Microsoft, and the company confirmed the vulnerabilities. At the time of our report, the security team at Microsoft had already prepared a patch for vulnerability CVE-2020-0986 that was used in the zero-day elevation of privilege exploit, but before our discovery, the exploitability of this vulnerability was considered less likely. The patch for CVE-2020-0986 was released on June 9, 2020.

Microsoft assigned CVE-2020-1380 to a use-after-free vulnerability in JScript and the patch was released on August 11, 2020.

We are calling this and related attacks 'Operation PowerFall'. Currently, we are unable to establish a definitive link with any known threat actors, but due to similarities with previously discovered exploits, we believe that DarkHotel may be behind this attack. Kaspersky products detect Operation PowerFall attacks with verdict PDM:Exploit.Win32.Generic.

This report in a nutshell:

- In May 2020, our technologies prevented a targeted attack that consisted of two zero-day exploits.
- Both exploits were built to exploit the latest builds of Windows 10 x64. Our tests demonstrated that the exploits were very reliable.
- Information about the existence of CVE-2020-0986 in splwow64.exe was made public on 19 May 2020. One day later the same vulnerability was used in an attack.
- The patch for CVE-2020-0986 was released 09 June 2020.
- The patch for CVE-2020-1380 was released 11 August 2020.
- We attribute 'Operation PowerFall' to DarkHotel with a low confidence level based on similarities to previous exploits.

Профили злоумышленников

Сопоставление с базой знаний ATT&CK

Общие сведения

- Информация, предназначенная для высшего руководства

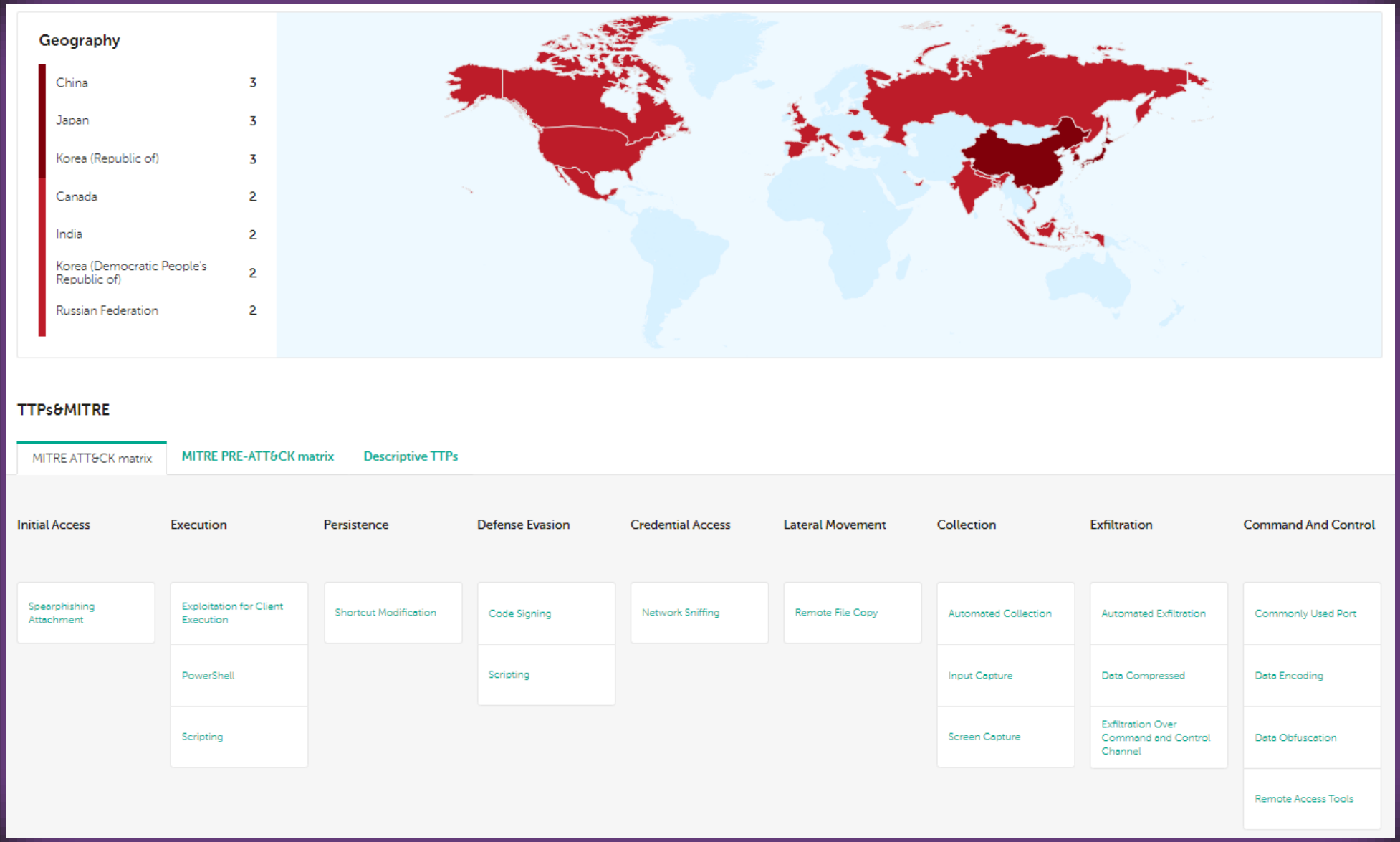
Подробный технический анализ

- Методы проведения атак
- Используемые эксплойты
- Описание вредоносного ПО
- Инфраструктура командных серверов и описание протоколов
- Анализ жертв атак
- Анализ эксфильтрации данных
- Атрибуция кибератак

Выводы и рекомендации

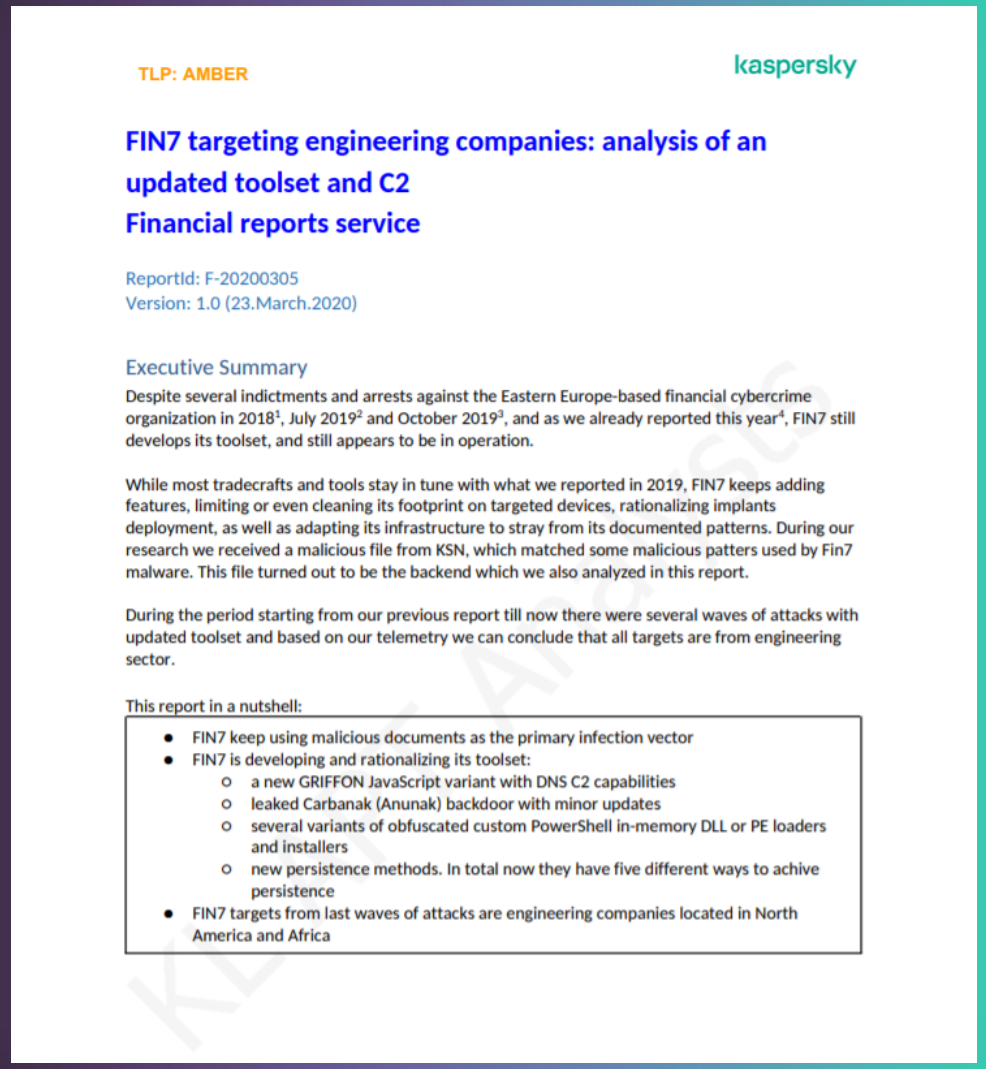
Индикаторы компрометации и YARA-правила

Сопоставление с базой знаний MITRE ATT&CK в аналитических отчетах об APT-угрозах



Отчеты об угрозах для финансовых организаций

Отчеты об угрозах для финансовых организаций



TLP: AMBER

kaspersky

FIN7 targeting engineering companies: analysis of an updated toolset and C2
Financial reports service

ReportId: F-20200305
Version: 1.0 (23.March.2020)

Executive Summary

Despite several indictments and arrests against the Eastern Europe-based financial cybercrime organization in 2018[1], July 2019[2] and October 2019[3], and as we already reported this year[4], FIN7 still develops its toolset, and still appears to be in operation.

While most tradecrafts and tools stay in tune with what we reported in 2019, FIN7 keeps adding features, limiting or even cleaning its footprint on targeted devices, rationalizing implants deployment, as well as adapting its infrastructure to stray from its documented patterns. During our research we received a malicious file from KSN, which matched some malicious patters used by Fin7 malware. This file turned out to be the backend which we also analyzed in this report.

During the period starting from our previous report till now there were several waves of attacks with updated toolset and based on our telemetry we can conclude that all targets are from engineering sector.

This report in a nutshell:

- FIN7 keep using malicious documents as the primary infection vector
- FIN7 is developing and rationalizing its toolset:
  - a new GRIFFON JavaScript variant with DNS C2 capabilities
  - leaked Carbanak (Anunak) backdoor with minor updates
  - several variants of obfuscated custom PowerShell in-memory DLL or PE loaders and installers
  - new persistence methods. In total now they have five different ways to achive persistence
- FIN7 targets from last waves of attacks are engineering companies located in North America and Africa

Профили злоумышленников

Сопоставление с базой знаний ATT&CK

Общие сведения

- Информация, предназначенная для высшего руководства

Подробный технический анализ

- Методы проведения атак
- Используемые эксплойты
- Описание вредоносного ПО
- Инфраструктура командных серверов и описание протоколов
- Анализ жертв атак
- Анализ эксфильтрации данных
- Атрибуция кибератак

Выводы и рекомендации

Индикаторы компрометации и YARA-правила

Кибератаки, наносящие финансовый ущерб

Prilex, Silence, Fin7, Deathstalker, HydraPOS – это преступные группировки, которые фокусируются на финансовых организациях и их крупных клиентах, таких как государственные структуры, а также на компаниях, участвующих в сделках слияния и поглощения. Кибернаемники и вымогатели также выбирают эти цели.

Массовые атаки проводятся с использованием вредоносного ПО для мобильного банкинга, банкоматов и платежных терминалов.

Что может помочь:

- Отчеты об угрозах для финансовых организаций
- Потоки данных об угрозах
- Kaspersky Digital Footprint Intelligence

Kaspersky Digital Footprint Intelligence

Kaspersky Digital Footprint Intelligence

Источники

Инвентаризация периметра сети

- Цифровые отпечатки в сервисах
- Выявление уязвимостей
- Анализ эксплойтов
- Оценка и анализ рисков

Поверхностный, глубокий и даркнет

- Активность киберпреступников
- Утечки информации и учетных данных
- Инсайдеры
- Поведение сотрудников в социальных сетях
- Утечки метаданных

База знаний «Лаборатории Касперского»

- Анализ экземпляров вредоносных программ
- Отслеживание ботнетов и фишинга
- Sinkhole-серверы и серверы с ВПО
- Аналитические отчеты об APT-угрозах
- Потоки данных об угрозах

Отчеты об угрозах для АСУ ТП

Kaspersky ICS CERT: Аналитика угроз для АСУ ТП

Отчеты об угрозах для АСУ ТП

Доступ по подписке к порталу с регулярными отчетами об атаках, угрозах и уязвимостях, характерных для АСУ ТП

Потоки данных о ВПО для АСУ ТП

Индикаторы компрометации (IoC) и метаданные для интеграции со сторонними SIEM-системами

Персонализированные отчеты

Персонализированные аналитические отчеты (квартал, год) для конкретного региона или отрасли

Потоки данных об уязвимостях АСУ ТП

Точная и актуальная информация для выявления уязвимостей в сетях АСУ ТП

Все исследования, связанные с аналитикой угроз для АСУ ТП, проводятся командой Kaspersky ICS CERT

- Подразделение основано в 2016 году
- Первая команда CERT создавалась для обслуживания коммерческой организации
- Порядка 20 высококвалифицированных экспертов по угрозам для АСУ ТП, поиску уязвимостей в таких системах, реагированию на инциденты и анализу защищенности

Возможности, доступные подписчикам сервиса

Исследование уязвимостей

Отчеты об анализе уязвимостей самых популярных продуктов, используемых в АСУ ТП, интернета вещей и инфраструктур в разных отраслях промышленности

Ландшафт угроз

Отчеты о важных изменениях в ландшафте угроз для АСУ ТП, критических факторах, влияющих на безопасность и уязвимость систем

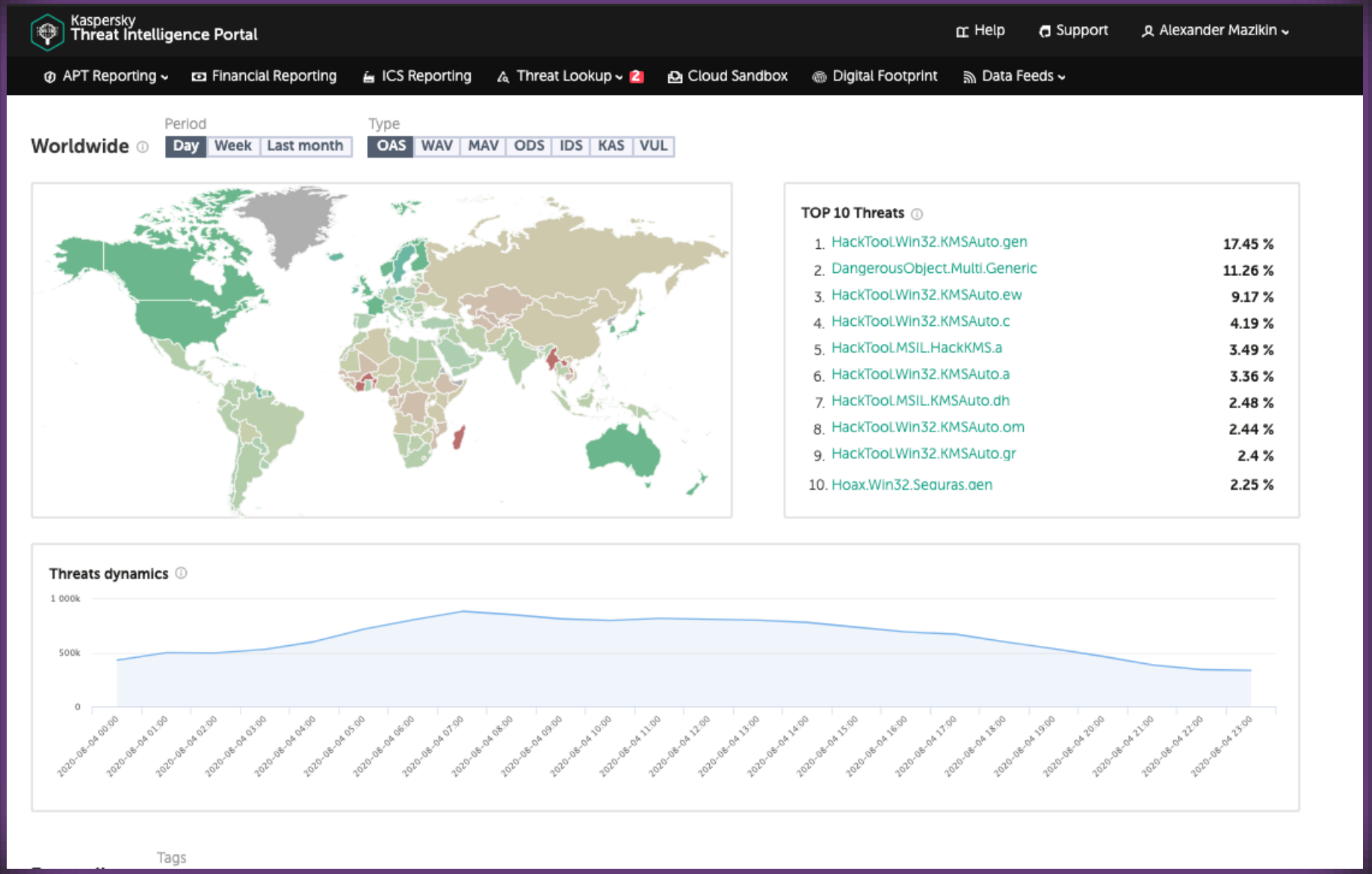
Отчеты об APT-атаках

Отчеты о новых APT-атаках и масштабных кампаниях против промышленных организаций и обновленные данные об активных угрозах

Помощь экспертов

Эксперты «Лаборатории Касперского» дают обоснованные практические советы по выявлению и минимизации уязвимостей в IT-инфраструктуре предприятия

Threat Intelligence Portal



Дорожная карта

Объединение технологий

- Threat Analysis Lab

Унификация

- Эволюция экосистемы, единая строка поиска

Развитие решений

- Новые продукты и развитие текущих

Защита бренда

- Усиление позиций Digital Risk Management

Технологические партнеры

SIEM/SOAR/IRP

Radar, McAfee, ArcSight An HP Company, RSA, splunk>, ALIEN VAULT, DFLABS CYBER INCIDENTS UNDER CONTROL, FORTINET, elastic, resilient an IBM Company, Phantom, LogRhythm

Платформы Threat Intelligence

THREATQ, THREATCONNECT, ANOMALI, eclectic iq, Arctic Security, MISP Threat Sharing

Средства управления сетевой безопасностью

paloalto networks, McAfee, SURICATA, CISCO FirePower

Стратегические партнеры

> 100

каналов продаж и партнеров – системных интеграторов

> 20

технологических партнёров

> 10

MSSP-партнеров в Европе, на Ближнем Востоке и в Азиатско-Тихоокеанском регионе

69

промышленных, государственных, национальных групп CERT и CSIRT и правоохрани-тельных структур

Доказанная эффективность Kaspersky Threat Intelligence

INTERPOL

«Лаборатория Касперского» помогает Интерполу эффективнее бороться с киберпреступностью

Gartner peerinsights™

«Лаборатория Касперского» имеет самый высокий рейтинг и наибольшее число рекомендаций среди поставщиков продуктов и сервисов для аналитики угроз

GREAT GLOBAL RESEARCH & ANALYSIS TEAM

Сервисы Kaspersky Threat Intelligence работают при поддержке команды экспертов мирового уровня – Kaspersky GREAT. На их счету множество успешных расследований по раннему обнаружению APT- угроз

MITRE | ATT&CK®

«Лаборатория Касперского» предоставила информацию о CozyDuke и Carbanak для тестов MITRE в рауде 2 и 3. Это помогло улучшить базу знаний MITRE ATT&CK

MOST TESTED*
MOST AWARDED*
KASPERSKY PROTECTION
*kaspersky.com/top3

Качество нашей аналитики подкрепляют технологии защиты, прошедшие множество испытаний и удостоенные множества наград

FORRESTER®

«Лаборатория Касперского» признана лидером по результатам исследования Forrester New Wave: External Threat Intelligence Services (Внешние услуги по анализу угроз), 2021 г.

Лидер рынка Threat Intelligence

FORRESTER®

The Forrester Wave™: External Threat Intelligence Services Q1, 2021.

«Лаборатория Касперского» признана лидером в области сервисов оперативного информирования о киберугрозах.

> The biggest intelligence bodies in the cyberworld are private entities – FireEye and Kaspersky have more information than any state intelligence body.

Dr. Mohamed al-Kuwaiti, Head of Cyber Security, UAE Government

Спасибо!

kaspersky