TIP: PoC

Kaspersky Threat Intelligence

Threat Intelligence от Kaspersky – это доступ к аналитике, необходимой для снижения киберрисков, предоставляемой командой мировых исследователей и аналитиков.

Основные типы Threat Intelligence:

Тип	Описание
Тактическая	Краткосрочная, быстро устаревающая информация, поддерживающая операции SOC и реагирование на инциденты (например, IOCs новых атак).
Оперативная	Данные о кампаниях, TTP, атрибуции актёров, их возможностях и намерениях.
Стратегическая	Информация для C-уровня и совета директоров: тренды, мотивации актёров, классификации.

??????? ???????????? PoC Threat Intelligence

Вы получаете доступ к **Kaspersky Threat Intelligence Portal**: https://tip.kaspersky.com. Ниже перечислены доступные функции и их ограничения в рамках PoC.

Threat Landscape

Функция	Доступ	Ограничения
Hunt Hub	Ограниченный доступ, детали правил скрыты	—
TTPs	Полный доступ, правила Suricata и Sigma не доступны для скачивания	—
Actors	Полный доступ	—
Software	Полный доступ	—

Функция	Доступ	Ограничения
Mitigations	Полный доступ	—
Vulnerabilities	Полный доступ	—

Threat Lookup – 100 ???????? ? ????

Возможность	Квота
WHOIS Hunting Rule (Normal)	1 правило
WHOIS Hunting Rule (High)	1 правило
Saved Search	10 правил
Research Graph	100 графов

Reporting

Возможность	Квота
APT Intelligence Reporting	10 отчётов (Master Yara и Master IoC отключены)
Crimeware Intelligence Reporting	10 отчётов (Master Yara и Master IoC отключены)

Threat Analysis

Возможность	Квота
Cloud Sandbox	10 запросов в день
Threat Attribution Engine	10 запросов в день
Similarity	10 запросов в день

?????? ???????

- **Digital Footprint Intelligence** – лишь демонстрационные уведомления.
- **Threat Infrastructure Tracking** – уровень страны.
- **Data Feeds** – только демонстрационные фиды.

Kaspersky Threat Landscape

?????????????? ??????

Глобальная картина угроз постоянно меняется: появляются новые методы атак, а известные становятся более изощрёнными. Пользователям необходимо быстро приоритизировать те угрозы, которые требуют незамедлительного реагирования.

Раздел «Threat Landscape» предоставляет информацию о злоумышленниках, нацеленных на конкретную отрасль и регионы, связывает технологии обнаружения с глобальной разведкой, даёт полную и актуальную контекстную информацию о тактиках, техниках и процедурах (TTP) атакующих.

???? ???????

Пользователи портала могут **самостоятельно сформировать свою Threat Landscape** в соответствии с матрицей MITRE ATT&CK, получая:

- актуальные техники, тактики и процедуры, которые могут быть использованы против них;
- детальные описания актёров, вредоносного ПО и используемых TTP;
- отчёты с подробным описанием атак;
- рекомендации-смягчения (mitigations) – конкретные меры для предотвращения выполнения техники.

????????? ???????????

Threat Landscape предлагает данные по:

- географии;
- отрасли;
- типам угроз и актёрам;
- их TTP;
- используемому вредоносному ПО;
- релевантным IOC.

??? ???????? ??????? MITRE ATT&CK

- **Такт** – цель, которую преследует злоумышленник.
- **Техника** – действие, реализующее цель.
- **Подтехника** – конкретный метод выполнения техники.

Пользователь может:

- просматривать всё TTP или фильтровать их;
- скрывать/показывать тактики/техники;
- раскрывать/сворачивать все подтехники;

- использовать полноэкранный режим;
- видеть список подтехник с количеством связанных подпунктов;
- получать имена и ID TTP;
- переходить к детальному описанию каждой записи.

?????????? ? Threat Landscape

- **Top Techniques** – наиболее часто используемые техники.
- **Attacks by Industry** – отрасли, получающие наибольшее количество атак.
- **Related Rules and Reports** – количество использованных правил и соответствующих отчётов.
- **Top Software** – часто используемое вредоносное ПО.
- **Top Tactics** – популярные тактики.
- **Related Actors** – активные актёры.

Фильтры автоматически обновляют статистику и графики.

???? ????????????

Тестировать возможность **Threat Landscape** выполнять следующие задачи:

1. **Создать heat-map MITRE ATT&CK**, релевантную компании.
2. **Предоставить практичную информацию о TTP**, релевантных компании.
3. **Определить актёров-угроз и инструменты**, используемые ими.

?????1 – ???????? MITRE ATT&CK heat?map, ???????????? ????????

Портал позволяет сохранять наборы фильтров, которые затем применяются к матрице ATT&CK.

????????? ???????

Фильтр	Описание
Actor	Актёры/группы, использующие техники ATT&CK (включая алиасы).
Industry	Отраслевой фильтр.
Affected countries	Страны/регионы.
Platform	Семейства ОС, к которым применимы техники.

??? ????????? ???????

1. На странице **Threat Landscape** выберите нужные фильтры и нажмите **Apply**.
2. При необходимости нажмите **Reset to default** для сброса.

??? ????????? ????? ????????

1. Выберите фильтры → **Save**.
2. В боковой панели введите **имя** (до 255 симв.) и **описание** (до 2048 симв.).
3. Нажмите **Save** – набор появится в коллекции.

?????? ? ??????????? ????????

- **Filter collection** – список всех наборов, созданных пользователями организации (видно имя, описание, дату создания/изменения, автора).
- Можно искать по имени, применять, редактировать (Edit) или удалять (Delete) набор.

????????? ???????? ????????

№	Действие	Ожидаемый результат
1	Выбрать **Affected countries** → *Россия и СНГ*.	Heat-map подсветит TTP, актуальные для выбранных стран.
2	Добавить **Industry** → *Государственный сектор*.	Heat-map уточнит подсветку в соответствии с выбранной отраслью.
3	Нажать **Hide** (правый-верхний угол).	Появятся только релевантные TTP.
4	Прокрутить вниз к **Top Techniques / Top Tactics / Top Software** и другим дашбордам.	Дашборды отразят данные, соответствующие выбранным фильтрам.

??????2 – ????????????? ?????????? ?????????? ? TTP, ???????????? ????????

???????

Страница **Tactics** содержит список тактик и общую информацию:

Поле	Описание
ID	Идентификатор тактики в MITRE ATT&CK.
Name	Наименование тактики (кликабельно, ведёт к детальному описанию).
Adversary action	Действие, которое злоумышленник стремится выполнить.
Created / Updated	Даты создания и последнего обновления.

???????

Поле	Описание
Description	Подробное описание техники.
ID	Идентификатор техники.
Sub-techniques	Список подтехник (кликабельно).
Tactics	Связанная тактика (кликабельно).
Platforms	ОС/приложения, в которых техника реализуется.
Permissions required	Требуемые привилегии.
Created / Updated / Version	Дата создания, последнего обновления, версия.

??????????

Поле	Описание
Description	Подробное описание подтехники.
ID	Идентификатор подтехники.
Sub-technique of	Родительская техника (кликабельно).
Tactics / Platforms / Permissions required	Как у техники.
Created / Updated / Version	Даты и версия.

??????? ????????

Раздел **Procedure examples** показывает хеши, связанные с подтехникой.

Поле	Описание
ID	ID актёра/программы, если привязан.
Name	Наименование актёра/программы/детекции.

Поле	Описание
Hash	MD5-хеш.

??????? (Rules)

Раздел **Rules** перечисляет правила, покрывающие подтехнику. Возможна загрузка полного списка правил (Sigma, Suricata) при наличии коммерческой лицензии.

Sigma????????

Поле	Описание
ID	Идентификатор правила.
Title	Название.
Description	Описание.
Severity	Уровень серьёзности.
Actions	Кнопка загрузки полного файла правила.

Suricata????????

Поле	Описание
ID	Идентификатор.
Content	Текст правила (первые 100 символов).
Actions	Кнопка загрузки.

?????? (Reports)

Список отчётов, относящихся к подтехнике. Клик по строке раскрывает детали.

Поле	Описание
Date	Дата публикации.
Group	Группа отчёта – **APT**, **Crimeware**, **Industrial**.
Report ID	Идентификатор отчёта (кликабельно открывает полное описание).
Report	Название, краткое резюме, ссылки на загрузку в разных форматах.
Tags	Теги отчёта.

????????? ????????

№	Действие	Ожидаемый результат
1	Открыть релевантную **Technique** из heat-map (например, *Boot or Logon Autostart Execution*).	Переход к странице техники.
2	Перейти к подтехнике (например, *Registry Run Keys / Startup Folder*).	Переход к странице подтехники.
3	Прокрутить до **Procedure examples** и нажать **Export**.	Файл JSON с примерами процедур скачан.
4	Прокрутить до **Rules**.	Виден список доступных Sigma/Suricata/EDR-правил, их можно экспортировать.

?????3 – ????????????? ?????????? ??? ???????? ????????????? ? ?? ?????????????

??????

На странице **Threat Landscape → Actors** отображается список профилей актёров. Каждый профиль содержит:

- общий обзор, поражённые страны, алиасы, жертвы, кампании, наборы инструментов, внешние ссылки.

Поле	Описание
ID	Идентификатор актёра.
Name	Основное имя (кликабельно → профиль).
Description	Краткое описание.
Aliases	Список алиасов.
Industries	Целевые отрасли.
Countries	Страны/регионы, где происходили атаки.
Updated	Дата последнего обновления.

??????? ??????

- **General information** – имя, группа (APT/Crimeware), иконка, алиасы.

- **CVEs** – уязвимости, которые актёр использует.
- **Software** – инструменты/вредоносное ПО, применяемое актёром (кликабельно → профиль ПО).
- **TTPs Details** – таблица MITRE ATT&CK TTP, используемых актёром (можно экспортировать в JSON).
- **Reports** – список относящихся к актёру отчётов (с датой, группой, ID, названием, тегами).

?????? ????????

№	Действие	Ожидаемый результат
1	Открыть вкладку **Actors**, отфильтровать **Affected Countries** → *Россия* и **Industries** → *Государственный сектор*.	Список актёров, соответствующих фильтрам.
2	Выбрать актёра (пример – *Angry Likho*).	Откроется профиль с описанием, TTP, отчётами.
3	В разделе **TTPs Details** нажать **Download JSON**.	Скачан JSON-файл со всеми TTP.
4	В секции **Reports** просмотреть последние отчёты.	Список доступных отчётов.
5	Перейти к связанному **Software** (пример – *Lumma Stealer*).	Появится профиль ПО с описанием, возможностями детекции и TTP.
6	В **Procedure examples** нажать **Download JSON**.	Скачан JSON со списком хешей.
7	**Дополнительно**: сформировать heat-map, выбрав страну, актёра, отрасль и платформу (например, *Windows*).	Получена кастомизированная матрица ATT&CK.

??????????? ??????????? (Software)

На странице **Threat Landscape → Software** перечисляются инструменты, используемые в APT-кампаниях.

Поле	Описание
ID	Идентификатор ПО.
Name	Наименование (кликабельно → профиль).
Aliases	Альтернативные имена.
Platforms affected	Уязвимые/затронутые платформы.
Related threat actors	Актёры, использующие ПО.

Поле	Описание
Updated	Дата последнего обновления.

??????? ???????????? ???????????

- **Description** – цель и функции.
- **Exploited vulnerabilities** – уязвимости, которые ПО использует.
- **TTPs Details** – таблица MITRE ATT&CK TTP (экспорт в JSON).
- **Procedure examples** – хеши, примеры файлов.

?????? ???????? (??. ??????? ????)

Mitigations (??????????)

Раздел **Mitigations** предоставляет сведения о мерах и технологиях, которые могут предотвратить успешное выполнение техники или подтехники.

Поле	Описание
ID	Идентификатор смягчения.
Name	Наименование (кликабельно → подробный профиль).
Updated	Дата/время последнего обновления.

Поиск возможен по имени или ID.

????????? ???????????? ??????

№	Критерий успеха	Достигнуто (да/нет)	Комментарий
1. Создать heat-map MITRE ATT&CK			
1.1	После выбора отрасли – heat-map обновилась в реальном времени.	**Да**	
1.2	После выбора географии – heat-map обновилась в реальном времени.	**Да**	

№	Критерий успеха	Достигнуто (да/нет)	Комментарий
1.3	Фильтры легко фокусируют информацию о релевантных TTP.	**Да**	
1.4	Threat Landscape предоставляет сводку по топ-TTP и ПО.	**Да**	
2. Предоставить практичную информацию о TTP			
2.1	Лёгкий доступ к детальной информации о тактиках/техниках/подтехниках.	**Да**	
2.2	Возможность собрать **procedure examples**.	**Да**	
2.3	Экспорт примеров процедур в нужном формате (JSON).	**Да**	
2.4	Предоставляются Sigma-правила.	**Да**	
2.5	Предоставляются Suricata-правила.	**Да**	
2.6	Предоставляются EDR-правила (при наличии лицензии).	**Да**	
3. Идентифицировать актёров и их инструменты			
3.1	Лёгкий поиск актёров, релевантных компании.	**Да**	
3.2	Экспорт TTP актёров в другие системы.	**Да**	
3.3	Быстрый доступ к TI-отчётам по актёрам.	**Да**	
3.4	Возможность найти ПО, используемое актёрами.	**Да**	
3.5	Экспорт примеров процедур, использованных актёрами.	**Да**	

??????????

?????????????? ??????

Совместный обмен разведданными – ключ к стратегии безопасности любой организации. Проблема большинства компаний – смешивание **информации** и **разведки**: без контекста «терабайты» данных мало что значат.

Наша позиция – предоставлять **глубокую аналитическую разведку** (APT-кампании, финансово-мотивированные группы, такие как Duqu, Carbanak, The Flame, Careto, Equation Group) и одновременно сохранять практический контекст для оперативного использования.

???? ???????

Kaspersky APT Intelligence Reporting – надёжный аналитический сервис, дающий:

- сведения о текущих APT-кампаниях, тактиках, техниках, инструментах и IOC;
- рекомендации по обнаружению и смягчению;
- executive-summary для руководства;
- техническую детализацию для аналитиков.

Kaspersky Crimeware Intelligence Reporting – информирует о кампаниях, направленных на финансовый сектор, банковские системы и платежные шлюзы.

????????? ???????????

Сервис предоставляет четыре типа отчётов:

1. **APT-отчёты** (конкретные атаки) – executive-summary, детальное описание, выводы и рекомендации, приложения (технический анализ, IOC, C2, хеши, маппинг MITRE ATT&CK).
2. **Crimeware-отчёты** (анализ криминального ПО).
3. **Researcher notes** – дополнительные заметки от аналитиков.
4. **Monthly APT activity report** – обзор активности за месяц.

Фильтрация по **Tags** (Industry, Geolocation, Threat Actor). С помощью колонки **Group** можно отделить APT-отчёты от Crimeware-отчётов.

?????4 – ?????? ? ???????? ? ??

№	Действие	Ожидаемый результат

1	Открыть вкладку **Reporting**, отфильтровать по тегу **Geo → Россия** и **Industry → Government**.	Показаны отчёты, соответствующие выбранным тегам.
2	Найти нужный отчёт и кликнуть по **Report ID** (пример – *Awaken Likho*).	Открыт детальный отчёт.
3	Скачать **Report (En)** (PDF).	PDF-файл скачан и открывается.
4	Скачать **IoC** (OpenIOC) и открыть в текстовом редакторе.	Список IOC получен.
5	Скачать **Yara**-правила и открыть в редакторе.	Правила Yara получены.

Kaspersky Threat Lookup

?????????????? ??????

Threat Lookup предлагает единый веб-сервис, собирающий всю накопленную Kaspersky информацию о киберугрозах и их взаимосвязях. Цель – дать команде безопасности максимум данных для предотвращения атак до их возникновения.

Ключевые возможности

- **Надёжная разведка** – проверенные данные, низкий уровень ложных срабатываний.
- **Реальное время** – автоматическая генерация данных по всему миру.
- **Threat hunting** – проактивный поиск, раннее обнаружение.
- **Широкий спектр данных** – хеши, URL, IP, WHOIS/DNS, pDNS, GeoIP, атрибуты файлов, цепочки загрузок, timestamps и пр.
- **Непрерывная доступность** – отказоустойчивая инфраструктура.
- **Экспорт в STIX, OpenIOC, JSON, Yara, Snort, CSV**.
- **Web-интерфейс и REST-API**.

????????? ???????????

- Поиск индикаторов (IP, домен, хеш, URL) через веб-интерфейс или API.
- Оценка статуса (malicious, clean, unknown и т.п.).
- Просмотр подробностей (WHOIS, DNS, связанные файлы, URL-маски, спам-/фишинг-атаки).
- Кнопки **Open in research graph**, **Copy request**, **Export all results** (CSV, OpenIOC, STIX).

?????? ??????? ????

Поле	Описание
Status	Малисийный/чистый/неизвестный.
Hits	Популярность (сколько раз обнаружен).
First/Last seen	Дата первого/последнего появления.
Format	Формат файла.
Size	Размер (байт).
Signed by / Packed by	Подписант / упаковщик.
MD5 / SHA-1 / SHA-256	Хеши.
Category	Принадлежность к APT.
Reports	Ссылка на связанные отчёты (при наличии лицензии).
Data Feeds	Список фидов, содержащих объект.
Industries	Отрасли, где объект встречался.

?????? ??????? IP???????

Поле	Описание
Status	Рискованность.
Hits	Популярность.
First/Last seen	Даты появления.
Threat scope	Оценка (0-100).
Owner name / ID	Владелец.
Created / Updated	Даты регистрации/обновления.
Category	Категория.
Reports / Data Feeds / Industries	Аналогично хешам.

?????? ??????? ??????/URL

Поле	Описание
Status, **IPv4 count**, **Files count**, **Created**, **Expires**, **Domain**, **Registrar**, **Owner**, **Category**, **Reports**, **Data Feeds**, **Industries**	Как в таблицах выше.

?????5 – ?????? ? Threat Lookup

№	Действие	Ожидаемый результат

1	Ввести IP *81.0.236.93* в **Master search**. Проверить Overview, WHOIS, Timeline, Files related.	Показаны результаты поиска.
2	В секции **Files related to IP address** нажать **Download data**.	CSV-файл со списком файлов скачан.
3	Поиск в системе по одному из хешей (пример *093B946FD1C80071AA0AE912D7362FAA*). Перейти к **Files downloaded from web address** и открыть URL.	Показаны результаты по выбранному хешу и URL.
4	В **Files that accessed the requested web address** кликнуть хеш → открывается страница хеша.	Показан список хешей.
5	Прокрутить к **TTPs details** для данного хеша.	Видны детали TTP.

AI OSINT IoCs

Раздел **AI OSINT IoCs** автоматически генерирует резюме из открытых источников (соцсети, блоги, форумы) по запрошенному индикатору.

- Возможные поля в AI-резюме: **Observed**, **Threat actors**, **Affected areas**, **Affected industries**, **Associated software**, **Exploited vulnerabilities**, **Exploited weaknesses**, **General threat information**, **Highlights**.

?????6 – ?????? ? AI OSINT IoC

№	Действие	Ожидаемый результат
1	На главной странице кликнуть по индикатору (пример *346C29015AFE9380B6499F5A88CDDBB7*), открыть вкладку **OSINT IoCs**.	Переход к Look-up-tab.
2	Проверить AI-генерированную карточку.	Карточка отображается сверху.

???????????? ?????? (Saved Searches)

Позволяют задать периодические запросы (ежедневно) для отслеживания изменений индикаторов.

?????7 – ?????? ?? Saved Searches ? Research Graph

№	Действие	Ожидаемый результат

1	В **Saved Searches** создать запрос, отслеживающий файлы, обращающиеся к вашему домену (пример: `Request → kaspersky.com`, `Service → Lookup`, `Section → Files accessing domain`, `Name → test`).	Открыта страница создания поискового запроса.
2	Через 24 ч проверить результаты.	Появится AI-карточка с новыми данными.
3	Ввести IP в **Master search**, нажать **Open in research graph**.	Откроется страница графа.
4	Правой кнопкой мыши по группе объектов → **Show grouped nodes**, найти нужный хеш, перетащить в граф.	Хеш добавлен в граф.

Kaspersky Threat Analysis

?????????????? ??????

Традиционные антивирусы способны остановить лишь известные угрозы. Сегодня необходимы **аналитика поведения, атрибуция и технологии сходства**, позволяющие обнаруживать ранее невидимый малвер. Kaspersky Threat Analysis объединяет:

- **Cloud Sandbox** – динамический анализ поведения.
- **Attribution Engine** – определение источника/автора APT-образцов.
- **Similarity** – поиск файлов, схожих по поведению и структуре.

Эти инструменты позволяют ускорить приоритизацию инцидентов и автоматизировать рутинные задачи.

Kaspersky Research Sandbox (???????? ??????)

- Гибридный подход: эмуляция поведения + анти-эвейшн-техники.
- Патент US10339301.
- Автоматическое ускорение времени внутри ВМ, когда малвер пытается «замедлиться» в VM.

??? ????????? ? ???????????????? ????

1. **Upload and execute file** – выбрать файл (или drag-and-drop). Максимальный размер – 256 МБ.

2. Выбрать нужные технологии: **Sandbox**, **Attribution**, **Similarity** (по умолчанию только Sandbox).
3. При необходимости указать **Archive password**, **Document password**, **Internet channel** (Any, Tor, Tarpit, отдельные страны).
4. Выбрать **File execution environment** (Windows XP, 7 x86/64, 10 x64, Android x86/ARM).
5. При желании задать **Execution time**, **Decrypt HTTPS**, **Click links**, **Command line parameters**.
6. Нажать **Start analysis** → ожидать завершения (в **Recent results** статус *Completed*).

?????? Sandbox

- **Summary** – карта активности, скриншоты, сетевые запросы.
- **Results** – обнаруженные угрозы, правила, сетевые активности.
- **Static analysis** – только для Android.
- **System activities**, **Extracted files**, **Network activities** – детальная информация.
- Для каждой секции доступна кнопка **Download data** (CSV, JSON, STIX, ZIP).

?????8 – ?????? ?????????????? ????? ? Cloud Sandbox

№	Действие	Ожидаемый результат
1	Скачать образец по ссылке `https://support.kaspersky.com/common/diagnostics/7399`, загрузить в **Threat Analysis**, нажать **Start file analysis**, после завершения открыть **Sandbox**.	Появятся результаты анализа, summary в верхней части.
2	Кликнуть **Malware** в разделе **Detects**.	Показаны названия детекций.
3	Прокрутить до **Execution map**.	Отображаются действия файла в системе.
4	Прокрутить до **Screenshots**.	Показаны скриншоты выполнения.
5	Нажать **Export Results → Debug report**.	Скачан zip-архив (пароль *infected*) со всеми API-вызовами.

Kaspersky Attribution Engine (???????? ??????)

- Сравнивает загруженный файл с базой более **80 000** APT-образцов и 25-летней коллекцией «чистых» файлов.
- Выдаёт **Summary**, **Sample & Content**, **Similar samples**, **Matched genotypes**, **Matched strings**.
- Экспорт в **JSON, STIX, CSV**.

Kaspersky Similarity

- Ищет файлы с похожими хешами (50+ типов similarity-hashes).
- Отображает **Summary**, **Sample & Content**, **Similar files**, **Confidence** (8-11), **Statistics**, **Detection names**, **Status summary**.

Threat Infrastructure Tracking

?????????????? ??????

Сервис **Threat Infrastructure Tracking** выдаёт IP-адреса инфраструктуры, связанной с продвинутыми угрозами (C2-серверы, хостинг-провайдеры и пр.). Обновляется ежедневно, содержит:

- IP, дата первого/последнего появления, домен, страна, тип IP, теги, краткое описание.

IP-адреса доступны в машинно-читаемом виде (JSON/CSV) для интеграции в существующие решения.

????????? ?????????????

- Доступен в **Threat Intelligence Portal** → вкладка **Active feed** (список IP) и **History** (история активности).
- Фильтрация по стране.

?????9 – ?????? ? ???????? Threat Infrastructure

№	Действие	Ожидаемый результат
1	Открыть **Threat Infrastructure**.	Показан список IP-адресов, принадлежащих C2.
2	Нажать **Download data** → выбрать JSON или CSV. При нажатии на IP перейти в **Threat Lookup** для детального просмотра.	Скачан файл, пригодный для использования в виде Data Feed.

??????

- https://www.kaspersky.com/
- https://www.securelist.com

Примечание: Некоторые разделы (например, таблицы с нумерацией «0», «1», «2») содержат placeholder-значения в оригинальном документе; в переводе они оставлены без изменения. При необходимости уточните их контекст у поставщика услуги.

Revision #4
Created 6 April 2026 12:54:30 by Administrator
Updated 6 April 2026 14:09:54 by Administrator