



Поисковый сервис  
о киберугрозах  
и их взаимосвязях

# Kaspersky Threat Lookup

**kaspersky** активируй  
будущее



## Kaspersky Threat Lookup

Сервис «Лаборатории Касперского», предоставляющий компаниям информацию об угрозах для защиты их инфраструктуры. В рамках данного сервиса предоставляется информация об известных вредоносных программах, фишинговых веб-сайтах, последних уязвимостях и эксплойтах, а также других типах киберугроз.

# Kaspersky Threat Lookup

## Поисковый сервис о киберугрозах и их взаимосвязях

Киберпреступность не знает границ, а ее техническая база быстро совершенствуется. Попытки взломать защиту предпринимаются все чаще, при этом сложность и скрытность киберугроз растет. Для компаний, направленных на нарушение рабочих процессов, кражу активов и нанесение ущерба, злоумышленники используют сложные цепочки поражения, а также специально подобранные тактики, техники и процедуры.

**Kaspersky Threat Lookup** — это мощная единая онлайн-платформа, открывающая доступ ко всем накопленным «Лабораторией Касперского» знаниям о киберугрозах и их взаимосвязях. Сервис предоставляет специалистам по безопасности максимум информации для предотвращения кибератак до того, как организации будет нанесен вред. Сервис предоставляет самые последние данные по веб-адресам, доменам, IP-адресам, хешам файлов, названиям угроз, статистическим и поведенческим данным, данным WHOIS / DNS, атрибутам файлов, данным геолокации, цепочкам загрузки, временным меткам и прочему. Результатом является глобальная видимость новых и возникающих угроз, что помогает защитить организацию и ускоряет реагирование на инциденты.

## Основные возможности



Найдет информацию об индикаторах угроз с помощью веб-интерфейса или REST API



Выяснит, является ли обнаруженный объект распространенным или уникальным

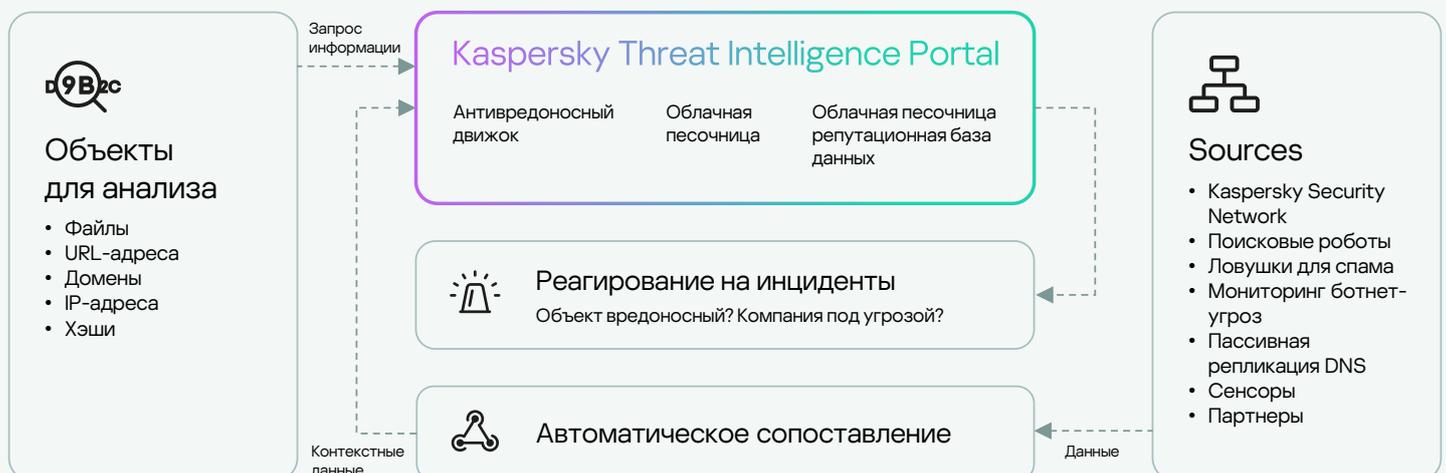


Поймет, почему объект считается вредоносным



Получит подробные сведения об объекте, включая сертификаты, распространенные названия, пути файлов и веб-адреса, для выявления новых подозрительных объектов

## Схема работы



# Преимущества



## Надежные данные об угрозах

«Лаборатория Касперского» предоставляет надежные данные об угрозах детальной контекстной информацией. Продукты «Лаборатории Касперского» демонстрируют наилучшие результаты при тестировании решений для защиты от вредоносных программ. Непревзойденное качество аналитических данных подтверждается высоким уровнем обнаружения с минимальным уровнем ложных срабатываний.



## Разнообразие форматов экспорта

Поддерживается экспорт индикаторов компрометации и контекстных данных в популярные машиночитаемые форматы, такие как STIX, OpenIOC, JSON, YARA, Snort и CSV. Это позволяет применять данные об угрозах с максимальной пользой, автоматизируя рабочие процессы и интегрируя эти сведения в системы управления безопасностью, такие как SIEM.



## Расследование инцидентов

Research Graph ускоряет расследование инцидентов, позволяя визуально изучать хранящиеся в Threat Lookup данные и обнаружения; дает графическое представление связей между веб-адресами, доменами, IP-адресами, файлами и другими данными для иллюстрации полного масштаба инцидента и выявления его основной причины.



## Поиск угроз

Проактивный подход к предотвращению и обнаружению атак и реагированию на них позволяет минимизировать частоту инцидентов и ущерб. Вы сможете отслеживать и устранять атаки на самых ранних этапах. Чем раньше будет обнаружена угроза, тем меньший будет нанесен ущерб и тем быстрее будет восстановлена работоспособность ресурсов и сети.



## Простота использования через веб-интерфейс или REST API

Сервисом можно пользоваться в ручном режиме через веб-интерфейс (в браузере) или через REST API.



## Мастер-поиск

Поиск информации с использованием всех активных сервисов анализа угроз и внешних источников (включая индикаторы компрометации из открытых источников, а также поиск в теневом и поверхностном интернете) в едином и мощном интерфейсе.



## Глубокий анализ индикаторов угроз

с помощью проверенной контекстной информации позволяет приоритезировать атаки и сосредоточиться на устранении угроз, представляющих наибольший риск для бизнеса.



## Эффективная и результативная диагностика

и анализ инцидентов безопасности на узлах и в сети. Приоритизация сигналов о неизвестных угрозах от внутренних систем.



## Улучшение процесса реагирования на инциденты

и расширение возможностей поиска угроз, позволяющее прервать цепочку развития угрозы до момента компрометации критически важных систем и данных.



# Kaspersky Threat Lookup

[Подробнее](#)

[www.kaspersky.ru](http://www.kaspersky.ru)

© 2024 АО «Лаборатория Касперского». Зарегистрированные товарные знаки и знаки обслуживания являются собственностью их правообладателей.

[#kaspersky](#)  
[#активируйбудущее](#)