Kaspersky Threat Intelligence

Всегда на ход впереди

kaspersky

Источники данных Kaspersky Threat Intelligence

- KSN
- Поисковые роботы
- Бот-фермы
- Ловушки для спама
- Сенсоры
- Записи Passive DNS
- Репозитории файлов
- Партнеры
- Открытые источники (OSINT)
- И многие другие...

Исследовательские и экспертные ресурсы «Лаборатории Касперского»

Kaspersky Threat Intelligence

Клиент

Kaspersky Threat Intelligence предоставляет доступ к широкому спектру данных, собранных нашими аналитиками и исследователями, чтобы помочь вашей организации эффективно противостоять современным киберугрозам.

Аналитика угроз на основе уникального опыта и знаний с глобальным охватом

Каждый из центров вносит свой вклад в развитие и поддержку решений и сервисов «Лаборатории Касперского»

- Исследование угроз
- Расследование инцидентов

Глобальный центр исследования и анализа угроз (GReAT)

- Исследование самых сложных угроз: APT, кампаний кибершпионажа, глобальных киберэпидемий и т. д.
- Безопасность для технологий, ориентированных на будущее
- Расследование сложных финансовых киберпреступлений

Kaspersky Threat Research

- Исследование вредоносного ПО
- Исследования в области контентной фильтрации
- Методики безопасной разработки ПО и оборудования

Kaspersky AI Technology Research

- Кибербезопасность в сфере ИИ
- Исследования генеративного ИИ
- Обнаружение угроз и другие решения с использованием ИИ

Kaspersky Security Services

- MDR
- Анализ защищенности
- Анализ цифровых ресурсов организаций
- Реагирование на инциденты
- Консультирование по вопросам SOC

Kaspersky ICS CERT

- Анализ угроз для критической инфраструктуры
- Исследование и оценка уязвимостей АСУ ТП
- Технологические ассоциации, аналитика и стандарты

Кратко о "Лаборатории Касперского"

Благодаря глубоким знаниям, большому опыту изучения киберугроз и уникальному пониманию всех аспектов кибербезопасности «Лаборатория Касперского» стала доверенным партнером компаний во всем мире и ценным союзником правоохранительных и правительственных организаций, включая Интерпол и подразделения CERT.

Глобальный охват и многолетний опыт изучения угроз в регионах, откуда исходит большинство атак

Непрерывный вклад экспертов «Лаборатории Касперского»

Анализ угроз для IT- и OT-сред

Кратко о Kaspersky Threat Intelligence

Мы отслеживаем:

300+

группировок

500+

кампаний

200+

приватных отчетов выходит в год

170 000+

индикаторов компрометации, связанных с отчетами

2500+

правил YARA, связанных с отчетами

Уровни аналитических данных об угрозах

Тактический

Детализированная, но быстро устаревающая информация для поддержки операций по обеспечению безопасности и реагирования на инциденты. Например, индикаторы компрометации, получаемые при обнаружении новой атаки.

Роль:

- Аналитик SOC

Системы:

- SIEM
- IPS
- IDS
- SOAR
- NGFW

Процессы:

- Активный поиск угроз
- Мониторинг

Операционный

Этот уровень обычно включает данные о кампаниях и TTP (тактиках, техниках и процедурах) более общего характера. Это может быть информация по атрибуции, а также о возможностях и намерениях злоумышленников.

Роли:

- Аналитик SOC 3-й линии
- Аналитик DFIR
- Аналитик IR

Системы:

- SIEM
- NTA
- EDR/XDR
- TIP

Процессы:

- Реагирование на инциденты
- Активный поиск угроз

Стратегический

Этот уровень помогает руководителям высшего звена и советам директоров принимать важные решения, касающиеся оценки рисков, распределения ресурсов и стратегии организации. Сюда входят тенденции в поведении киберпреступных групп, их мотивация и классификация.

Роли:

- CISO
- CTO
- CIO
- CEO

Процессы:

- Разработка стратегии ИБ
- Информирование об угрозах

Форматы предоставления аналитических данных об угрозах

Машиночитаемые аналитические данные об угрозах

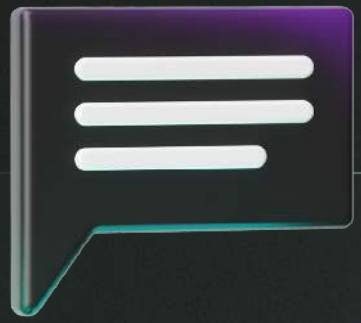
Kaspersky Threat Data Feeds

Более 30 потоков данных об угрозах, охватывающих различные потребности в области IT и OT, и платформа аналитики угроз

Человекочитаемые аналитические данные об угрозах

Kaspersky Threat Intelligence Portal

Основное портфолио Kaspersky Threat Intelligence для IT- и OT-сред с единым доступом через портал Kaspersky Threat Intelligence



Поддержка экспертов по борьбе с угрозами

Kaspersky Takedown Service

Kaspersky Ask the Analyst

Экспертные рекомендации профессионалов

Kaspersky Threat Intelligence

Машиночитаемые аналитические данные об угрозах

- Потоки данных об угрозах
- Kaspersky CyberTrace

Поддержка экспертов по борьбе с угрозами

- Kaspersky Takedown
- Kaspersky Ask the Analyst

Человекочитаемые аналитические данные об угрозах

- Kaspersky Threat Lookup
- Kaspersky Digital Footprint Intelligence
- Kaspersky Threat Analysis
  - Sandbox
  - Attribution
  - Similarity
- Отчеты Kaspersky Threat Intelligence
  - APT
  - Crimeware
  - ICS
- Kaspersky Threat Infrastructure Tracking

Kaspersky Threat Intelligence

- Тактический уровень
- Операционный уровень
- Стратегический уровень

○ доступно через

Kaspersky Threat Intelligence Portal

Потоки данных об угрозах

Более 30 готовых потоков данных об угрозах для различных задач.

Возможно создание потоков данных, адаптированных под задачи вашей организации.

- Тактический уровень
- Операционный уровень

Общие потоки данных об угрозах

- Malicious URL
- Ransomware URL
- Phishing URL
- Botnet C&C URL
- Mobile Botnet C&C URL
- Malicious Hashes
- Mobile Malicious Hashes
- IP Reputation
- IoT URL
- ICS Hashes
- APT Hashes
- APT IP
- APT URL
- Crimeware Hashes
- Crimeware URL

Потоки данных об угрозах → SIEM, SOAR/IRP, TIP, EDR/XDR

Платформа TI

Быстрый анализ множества потоков данных об угрозах поможет вам извлечь из них пользу и снизит нагрузку на SIEM-системы.

Kaspersky CyberTrace

Специализированные потоки данных об угрозах

Network Security Data Feeds	**Suricata Rules Feed**	**Sigma Rules Data Feed**	**Yara Rules Data Feeds**	**Vulnerability Feed**	**Open Source Software Threats Data Feed**
NGFW	IDS/IPS	SIEM/EDR	YARA-сканер	SBOM/CMDB	OSA/CSA/ASOC

Kaspersky Threat Intelligence Portal

Kaspersky Threat Intelligence Portal предоставляет доступ ко всем человекочитаемым аналитическим данным об угрозах через единый веб-интерфейс, где сервисы работают взаимосвязанно, усиливая друг друга. Сводя воедино все знания и опыт в области киберугроз, накопленные "Лабораторией Касперского", и используя проприетарные технологии обработки и нормализации данных, портал позволяет отслеживать и исследовать угрозы, актуальные для конкретной организации

- Тактический уровень
- Операционный уровень
- Стратегический уровень

Kaspersky Threat Intelligence Portal (бесплатная версия)

Ландшафт угроз на портале Kaspersky Threat Intelligence

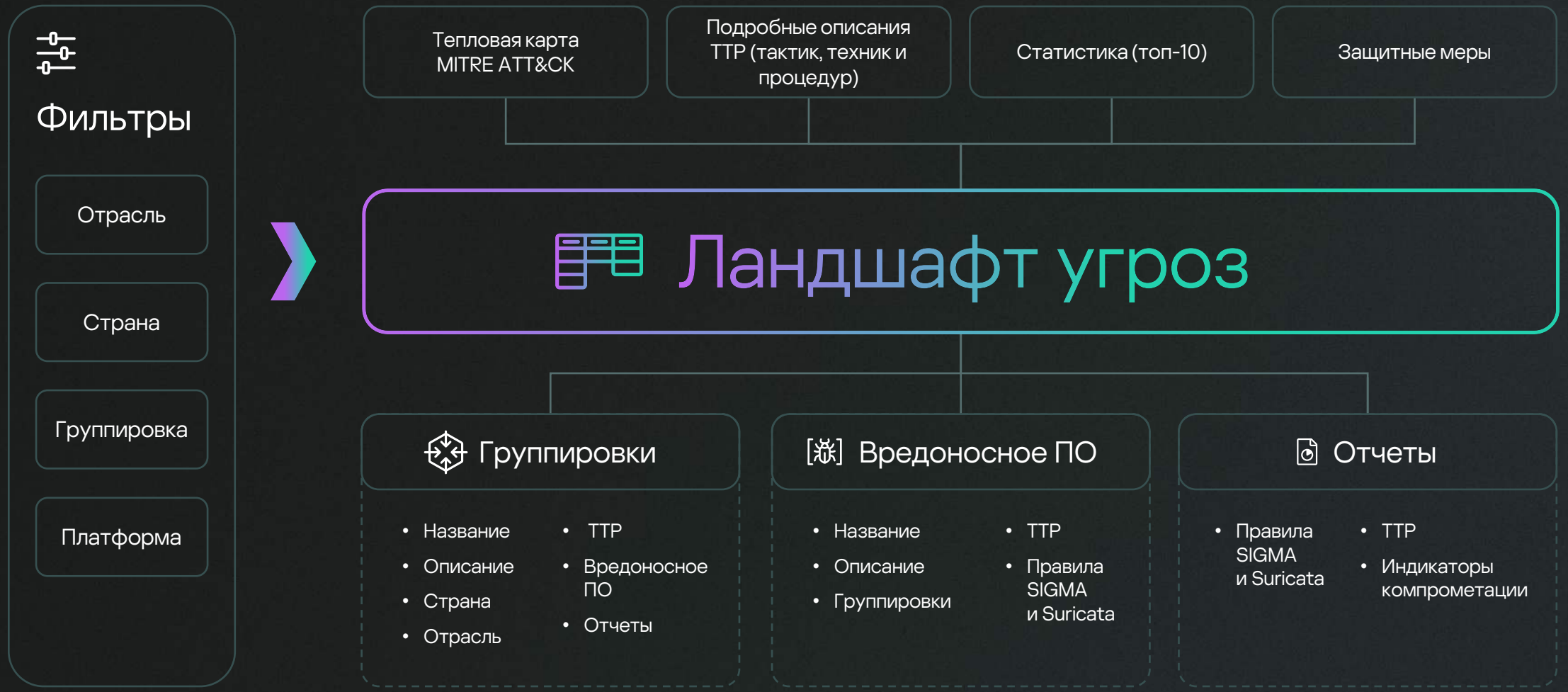
Актуальный для вашей организации ландшафт угроз с учетом специфики региона и отрасли

- Карта угроз на основе матрицы MITRE ATT&CK
- Обновления по результатам текущих исследований «Лаборатории Касперского» в режиме реального времени
- Автоматическое заполнение профилей злоумышленников и ВПО
- Релевантные детектирующие правила

400 000+

вредоносных файлов, выявляемых ежедневно, являются источником этих данных

Ландшафт угроз: как это работает



Экспертная поддержка Kaspersky Threat Intelligence

Kaspersky Ask the Analyst

- Операционный уровень
- Стратегический уровень

Сервис Kaspersky Ask the Analyst дополняет наш портфель решений для анализа угроз. Он позволяет вам обращаться к экспертам за рекомендациями и другой полезной информацией по конкретным угрозам, с которыми вы столкнулись или которые вас интересуют.

Вы сможете обсуждать конкретные инциденты с основной командой исследователей «Лаборатории Касперского». Наши эксперты готовы поделиться с вашими специалистами уникальными знаниями и ресурсами.

Kaspersky Takedown Service

- Операционный уровень

Сервис Kaspersky Takedown быстро нейтрализует угрозы вредоносных и фишинговых доменов, прежде чем они нанесут ущерб вашему бизнесу и репутации. За годы работы мы проанализировали большое количество доменов и знаем, как собирать доказательства их вредоносности. Мы возьмем на себя управление блокированием.

Данный сервис предоставляется во всем мире в сотрудничестве с международными организациями, национальными и региональными правоохранительными органами.

Kaspersky Threat Intelligence для промышленности

Машиночитаемые аналитические данные об угрозах

Kaspersky Threat Data Feeds

Машиночитаемые данные об угрозах и уязвимостях в области промышленной кибербезопасности:

Поток данных с хэшами угроз для АСУ ТП
Поток данных с уязвимостями АСУ ТП
Поток данных с уязвимостями АСУ ТП в формате OVAL

Человекочитаемые аналитические данные об угрозах

Kaspersky ICS Intelligence Reporting

Доступ к регулярным публикациям об угрозах и уязвимостях в сфере промышленной кибербезопасности через Kaspersky Threat Intelligence Portal

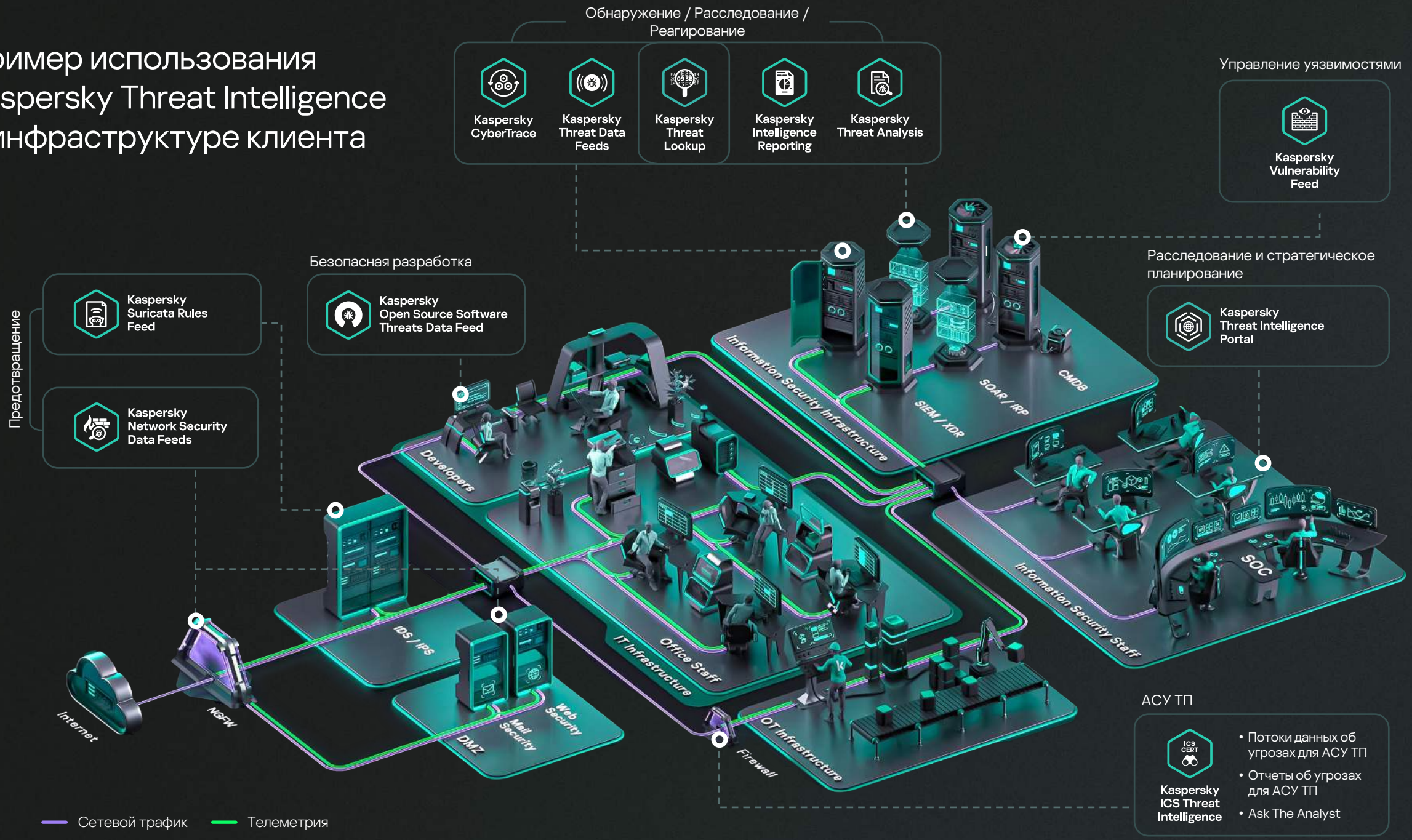
Поддержка экспертов по борьбе с угрозами

Kaspersky Ask the Analyst

Индивидуальные консультации с экспертами ICS CERT «Лаборатории Касперского» по угрозам и уязвимостям в области промышленной кибербезопасности, статистике угроз, ландшафту угроз, отраслевым стандартам и множеству других тем.

Тактический уровень
Операционный уровень
Стратегический уровень

Пример использования Kaspersky Threat Intelligence в инфраструктуре клиента



Почему стоит выбрать Kaspersky Threat Intelligence?

Передовое TI портфолио, признанное отраслевыми аналитиками	Подтверждено аналитиками глобальных исследовательских компаний, включая Frost & Sullivan, Quadrant Knowledge Solutions, Forrester и IDC.
Множество уникальных и достоверных источников данных об угрозах	Инфраструктура Kaspersky Security Network включает более 100 млн сенсоров в 200 странах. Мы обладаем крупнейшими репозиториями вредоносных и легитимных файлов, получаем данные в процессе постоянного активного поиска угроз и реагирования на инциденты, а также используем источники в даркнете, поисковые роботы, ловушки для спама и др.
Опыт признанных экспертов в области IT и OT	Наши эксперты работают по всему миру и говорят более чем на 20 языках – это более 200 сертифицированных специалистов из 5 экспертных центров, включая команды GReAT и ICS CERT. При появлении новых масштабных угроз – от Stuxnet и WannaCry до операции «Триангуляция» – эксперты «Лаборатории Касперского» всегда одними из первых обнаруживали их.
Глобальный охват угроз	Широкое присутствие в регионах, откуда исходит большинство атак (страны СНГ, Китай и др.), дает нам уникальную возможность собирать, анализировать и распространять достоверные аналитические данные об угрозах для организаций в любой стране.
Уникальный опыт обнаружения вредоносного ПО	Как крупнейший поставщик антивирусных решений, отмеченных многочисленными наградами, мы ежедневно обрабатываем миллионы новых образцов вредоносного ПО с помощью проприетарных технологий обнаружения угроз.
Обширный опыт исследований APT-угроз	Мы отслеживаем несколько сотен APT-группировок и кампаний, ежегодно выпуская более 200 подробных отчетов со стратегическим анализом угроз. Наша коллекция файлов APT-угроз, в которой собрано более 70 тыс. образцов, – крупнейшая в отрасли.
Данные об угрозах с применением ИИ	Технологии искусственного интеллекта и машинного обучения помогают извлекать полезные сведения из данных, создавать специализированные отчеты и автоматизировать процесс анализа, что значительно экономит время и ресурсы.
Надежный поставщик решений	Наша прозрачная отказоустойчивая инфраструктура с высоким качеством обслуживания и широкими возможностями мониторинга построена по методике SDLC и регулярно проходит независимую внешнюю оценку (аудит SOC 2 второго типа или сертификацию по ISO 27001).

Истории успешного сотрудничества

Теперь мы лучше понимаем угрозы, с которыми сталкиваются наши клиенты. Когда приходит уведомление об угрозе, хорошо иметь надежный источник дополнительных данных о ней, на который можно опереться. Это позволяет сформировать полную картину инцидента и понять, какой урок мы можем из него извлечь.

Пол Колвелл
CyberGuard Technologies

CyberGuard Technologies

Читать историю

«Лаборатория Касперского» часто выявляет новые угрозы до того, как производители ПО узнают о них.

Экспертные знания и опыт позволяют «Лаборатории Касперского» рассказывать о новых скрытых угрозах, с которыми мы еще не сталкивались. Это полезнее, чем поток вторичных новостей, из которых не узнаешь ничего нового.

Хуан Андрес Герреро Сааде
исследователь, Chronicle Security

chronicle

Читать историю

Возможности, которые предлагает «Лаборатория Касперского», и готовность прислушаться к нашим пожеланиям превзошли мои ожидания. Убедившись в надежности продукта и людей, которые за ним стоят, мы смогли повысить безопасность своей сети.

Рашид Аль-Нахлави
консультант по IT-безопасности, Олимпийский комитет Катара

قطر
QATAR

Читать историю

Kaspersky Threat Intelligence делает вас сильнее

Проактивно выявляйте и предотвращайте угрозы

Kaspersky Threat Intelligence предоставляет информацию о новейших угрозах и уязвимостях, помогая вам действовать на опережение – защищать свои системы до того, как произойдет атака.

Усильте свои средства обнаружения угроз

Kaspersky Threat Intelligence дополняет имеющиеся у вас решения безопасности новейшими данными об угрозах, существенно повышая эффективность обнаружения и блокирования продвинутых угроз.

Эффективнее реагируйте на инциденты

Kaspersky Threat Intelligence в режиме реального времени предоставляет информацию о новых угрозах и индикаторах компрометации, чтобы вы могли реагировать на инциденты быстро и эффективно.

Получите полное представление о своих цифровых активах

Kaspersky Threat Intelligence создает полную картину всех ваших цифровых ресурсов и указывает, какие из них могут стать мишенью для атаки или компрометации.

Получите ценные знания в области кибербезопасности

Эксперты «Лаборатории Касперского» – одни из самых опытных и уважаемых исследователей в отрасли – готовы поделиться своими обширными знаниями и опытом с вашей командой специалистов по информационной безопасности.

Соблюдайте регламенты и стандарты

Каждая компания обязана соблюдать различные нормы и отраслевые стандарты. Kaspersky Threat Intelligence помогает обеспечить выполнение таких требований.

Спасибо за внимание!

Kaspersky Threat Intelligence Portal – центр знаний о кибербезопасности

Kaspersky Threat Intelligence Portal

Узнать больше

Заказать демонстрацию