Платформа для управления данными о киберугрозах

Kaspersky CyberTrace

kaspersky активируй будущее

Kaspersky CyberTrace

Обеспечивает ситуационную осведомленность в реальном времени и позволяет аналитикам по безопасности принимать своевременные и взвешенные решения.

Kaspersky CyberTrace

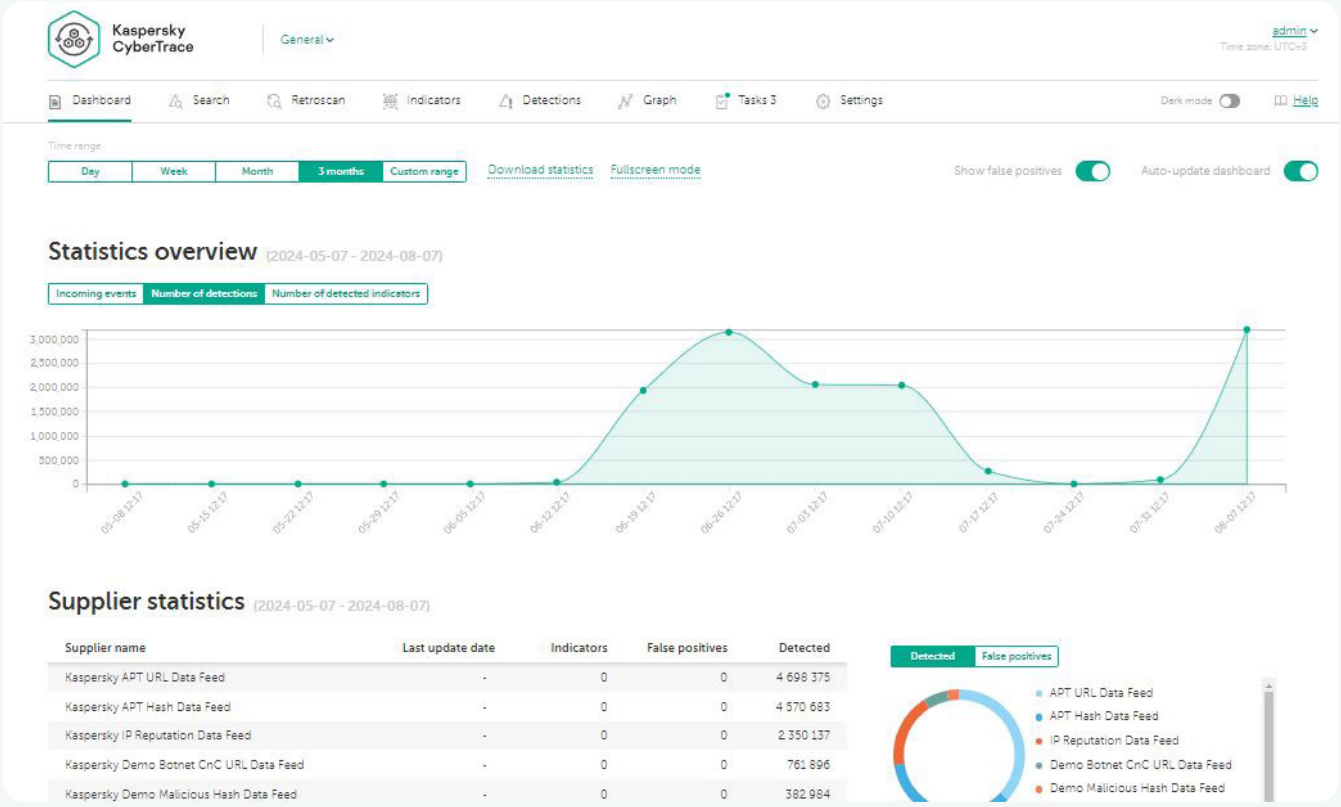
Платформа для управления данными о киберугрозах

Интеграция актуальных машиночитаемых аналитических данных об угрозах в существующие средства управления безопасностью, такие как SIEM-системы, позволяет автоматизировать процесс первоначальной приоритизации и классификации.

Аналитические данные предоставляются в различных форматах и включают большое количество индикаторов компрометации (IoCs), что сильно усложняет их обработку SIEM-системами или другими средствами управления сетевой безопасностью.

Kaspersky CyberTrace — это решение класса Threat Intelligence Platform, которое позволяет упростить интеграцию потоков данных с SIEM-системой для дальнейшего использования аналитики угроз в повседневной работе ИБ-служб. Платформа взаимодействует с любыми типами потоков аналитических данных об угрозах («Лаборатории Касперского», других поставщиков, из открытых источников или иных каналов) в форматах JSON, STIX, XML и CSV и поддерживает настроенную интеграцию со многими SIEM и источниками журналов.

Благодаря автоматическому сопоставлению журналов с потоками аналитических данных об угрозах, Kaspersky CyberTrace обеспечивает ситуационную осведомленность в реальном времени и позволяет аналитикам по безопасности принимать своевременные и взвешенные решения.



Состав

Kaspersky CyberTrace содержит набор инструментов для эффективной классификации событий ИБ и первоначального реагирования:

База данных индикаторов с полнотекстовым поиском и возможностью поиска с использованием расширенных запросов позволяет выполнять сложный поиск по всем полям индикаторов

Статистика использования потоков данных помогает выбрать наиболее ценных поставщиков аналитической информации об угрозах посредством измерения эффективности интегрированных потоков данных и построения матрицы пересечения потоков данных

Назначение тегов индикаторам компрометации упрощает управление ими. Можно создать любой тег, указать его значимость и присваивать его индикаторам компрометации вручную. Можно выполнять сортировку и фильтрацию индикаторов по тегам и их значимости

Research Graph позволяет визуально изучать хранящиеся в CyberTrace сведения и обнаружения и выявлять общие черты угроз

Функция экспорта индикаторов позволяет экспортировать наборы индикаторов и передавать данные об угрозах между экземплярами Kaspersky CyberTrace или другими платформами анализа угроз

Ретроспективная проверка позволяет анализировать объекты в ранее проверенных событиях с использованием новых поступивших данных для поиска не обнаруженных ранее угроз

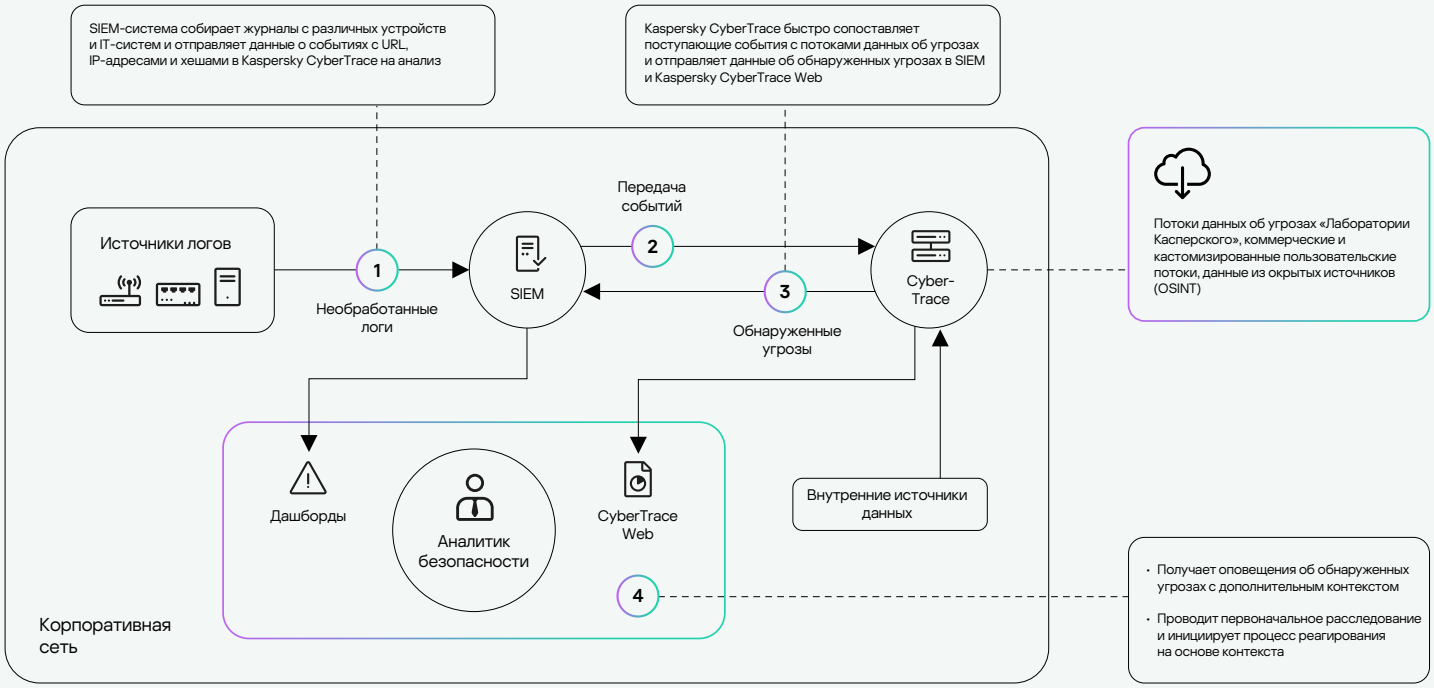
Для поставщиков управляемых услуг безопасности, а также для использования на крупных предприятиях реализована поддержка мультитенантности

Фильтрация событий обнаружения для дальнейшей отправки в SIEM-системы снижает нагрузку как на сами системы, так и на аналитиков

REST API позволяет выполнять поиск и управлять аналитическими данными об угрозах, а также интегрировать Kaspersky CyberTrace в сложные среды для автоматизации и управления

Страницы с подробной информацией о каждом индикаторе обеспечивают более глубокий анализ. Полная информация об индикаторе от всех поставщиков аналитических данных об угрозах (с исключением дублирующихся данных) позволяет аналитикам обсуждать угрозы в комментариях и добавлять внутренние данные к индикатору

Схема работы



Решение использует внутренний процесс анализа и сопоставления поступающих данных, что существенно снижает рабочую нагрузку на SIEM-систему. Kaspersky CyberTrace анализирует поступающие данные, быстро сопоставляет их с потоками и генерирует собственные оповещения при обнаружении угроз.

Преимущества

Эффективная фильтрация и приоритизация огромного количества оповещений систем безопасности

Оптимизация и ускорение процессов классификации и сдерживания угроз

Создание проактивной системы защиты на основе глобальных аналитических данных

Быстрое определение наиболее критичных из оповещений и принятие более взвешенных решений об их дальнейшей передаче группам реагирования

Kaspersky CyberTrace

Подробнее

www.kaspersky.ru

#kaspersky
#активируйбудущее