Kaspersky CyberTrace

kaspersky АКТИВИРУЙ БУДУЩЕЕ

Kaspersky CyberTrace Платформа для управления данными о киберугрозах

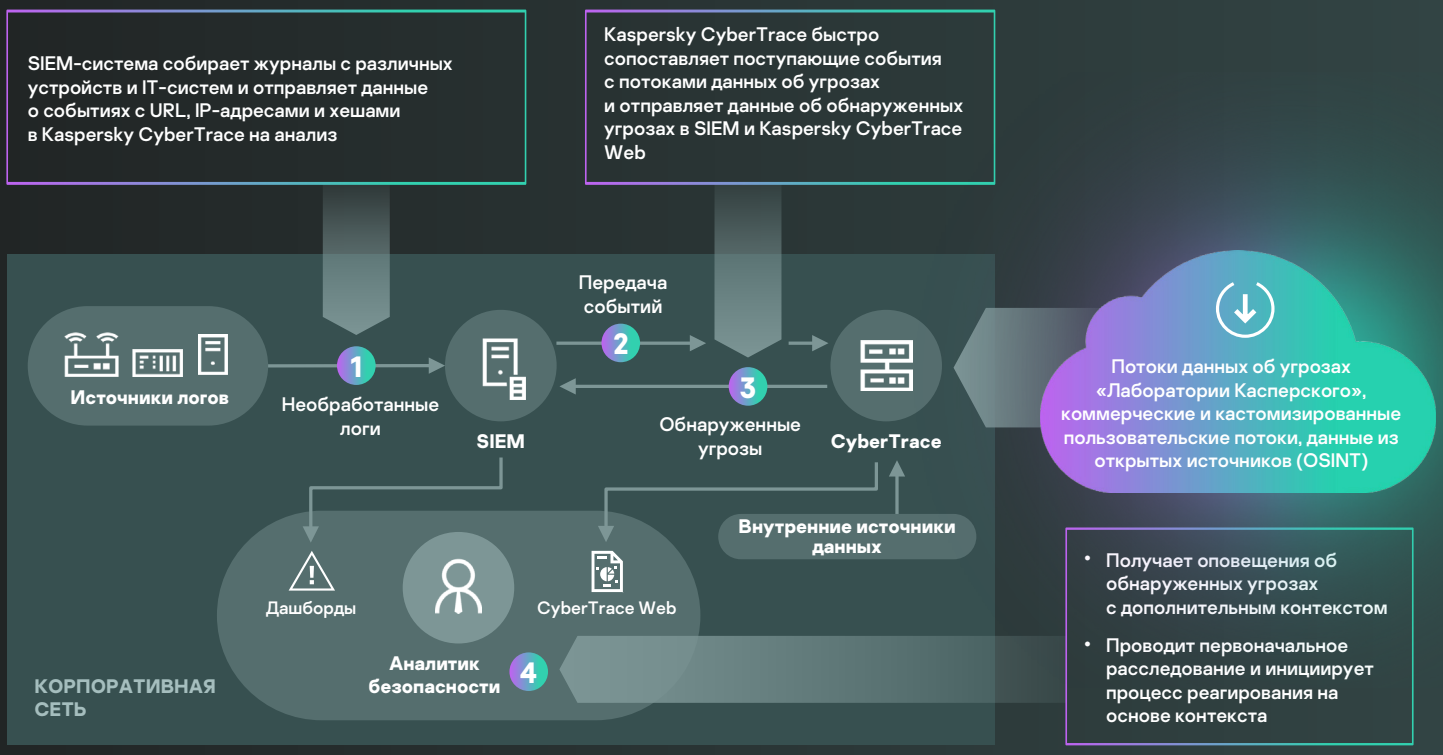
Интеграция актуальных машиночитаемых аналитических данных об угрозах в существующие средства управления безопасностью, такие как SIEM-системы, позволяет автоматизировать процесс первоначальной приоритизации и классификации. Но постоянный рост числа доступных для интеграции потоков данных об угрозах мешает определить источники информации, подходящие для конкретной организации. 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.

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.
- 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.
- 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.
- 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.
- Ретроспективная проверка позволяет анализировать объекты в ранее проверенных событиях с использованием последних потоков данных для поиска не обнаруженных ранее угроз.
- Фильтрация событий обнаружения для дальнейшей отправки в SIEM-системы снижает нагрузку как на сами системы, так и на аналитиков.
- 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.
- Для поставщиков управляемых услуг безопасности, а также для использования на крупных предприятиях реализована поддержка мультитенантности.
- REST API позволяет выполнять поиск и управлять аналитическими данными об угрозах, а также интегрировать Kaspersky CyberTrace в сложные среды для автоматизации и управления.

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. На схеме ниже показана высокоуровневая архитектура решения.



Kaspersky CyberTrace и потоки данных «Лаборатории Касперского» об угрозах позволяют аналитикам безопасности:

- эффективно фильтровать и приоритизировать огромное количество оповещений систем безопасности;
- оптимизировать и ускорять процессы классификации и сдерживания угроз;
- быстро определять наиболее критичные из оповещений и принимать более взвешенные решения об их дальнейшей передаче группам реагирования;
- создавать проактивную систему защиты на основе глобальных аналитических данных.

Kaspersky Threat Intelligence

FORRESTER®

«Лаборатория Касперского» признана лидером по результатам исследования внешних сервисов анализа угроз (Forrester Wave™: External Threat Intelligence Services, Q1 2021)

«Лаборатория Касперского» предлагает сервисы информирования об угрозах, которые открывают доступ к различной информации, полученной нашими аналитиками и исследователями мирового класса. Эти данные помогут любой организации эффективно противостоять современным киберугрозам.

Наша компания обладает глубокими знаниями, богатым опытом исследования киберугроз и уникальными сведениями обо всех аспектах IT-безопасности. Благодаря этому «Лаборатория Касперского» стала доверенным партнером правоохранительных и государственных организаций по всему миру, в том числе Интерпола и различных подразделений CERT. Kaspersky Threat Intelligence предоставляет актуальные технические, тактические, операционные и стратегические данные об угрозах.

Kaspersky Threat Intelligence

Подробнее

www.kaspersky.ru