kaspersky АКТИВИРУЙ БУДУЩЕЕ

Kaspersky CyberTrace

Количество оповещений от различных систем информационной безопасности, ежедневно обрабатываемых аналитиками в центрах мониторинга и реагирования на инциденты ИБ (SOC), растет в геометрической прогрессии. Такой объем анализируемых данных практически исключает возможность их эффективной приоритизации и классификации для дальнейшего анализа и реагирования. SIEM-системы, средства управления журналами и другие аналитические системы, уменьшают количество событий, требующих дополнительной проверки, но ИБ-специалисты все равно остаются перегружены.

Потоки данных об угрозах предоставляются в различных форматах и включают огромное количество индикаторов компрометации (IoC), что сильно усложняет их обработку SIEM-системами или средствами управления сетевой безопасностью.

Эффективные классификация, анализ и реагирование на события ИБ

Благодаря интеграции актуальных машиночитаемых аналитических данных об угрозах в существующие средства управления событиями ИБ, такие как SIEM-системы, центры мониторинга могут автоматизировать процесс первоначальной приоритизации и классификации. При этом аналитики безопасности получают достаточно контекста, чтобы сразу выявлять события, которые требуют более пристального изучения или эскалации группам реагирования на инциденты для проведения детального расследования. Однако, постоянный рост числа доступных для интеграции потоков данных об угрозах мешает определить источники информации, релевантные конкретной организации. Потоки данных предоставляются в различных форматах и включают огромное количество индикаторов компрометации (IoC), что сильно усложняет их обработку SIEM-системами или средствами управления сетевой безопасностью.

Kaspersky CyberTrace позволяет организациям упростить и существенно повысить эффективность использования аналитических данных об угрозах. Он представляет из себя комплексную Threat Intelligence платформу и дает возможность интегрировать потоки данных об угрозах с различными системами безопасности для их дальнейшего более эффективного использования. Продукт позволяет работать с любым потоком аналитических данных в форматах JSON, STIX, XML и CSV. CyberTrace также поддерживает интеграцию “из коробки” с различными SIEM-системами и источниками логов.

CyberTrace использует внутренний процесс анализа и сопоставления поступающих данных, что существенно снижает рабочую нагрузку на SIEM- систему. Он анализирует поступающие данные, быстро сопоставляет их с потоками и генерирует собственные оповещения при обнаружении угроз. На рисунке ниже показана высокоуровневая архитектура интеграции решения.

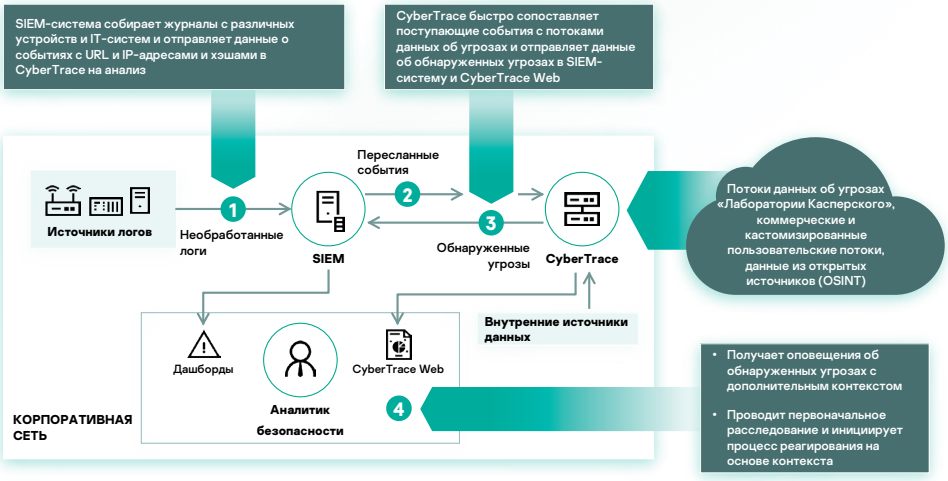

Рисунок 1. Верхнеуровневая схема работы Kaspersky CyberTrace

Богатый функционал для проведения всестороннего анализа

Kaspersky CyberTrace предоставляет набор инструментов для эффективной работы с потоками данных об угрозах:

- База данных со всеми индикаторами с возможностью полнотекстового поиска, а также поддержкой сложных поисковых запросов для поиска по всем полям индикатора, включая поля, содержащие контекст. Результаты поиска могут быть отфильтрованы по поставщику данных для упрощения дальнейшего анализа.
- Страницы с детальной информацией по каждому индикатору для более подробного анализа. На каждой странице представлена сводная дедуплицированная информация по индикатору, полученная от всех подключенных поставщиков данных. Аналитики могут обсуждать связанные угрозы в комментариях, а также добавлять собственную информацию об индикаторе. Если индикатор был ранее обнаружен в логах, то тут же будет доступна информация о дате обнаружения со ссылкой на список всех соответствующих событий.

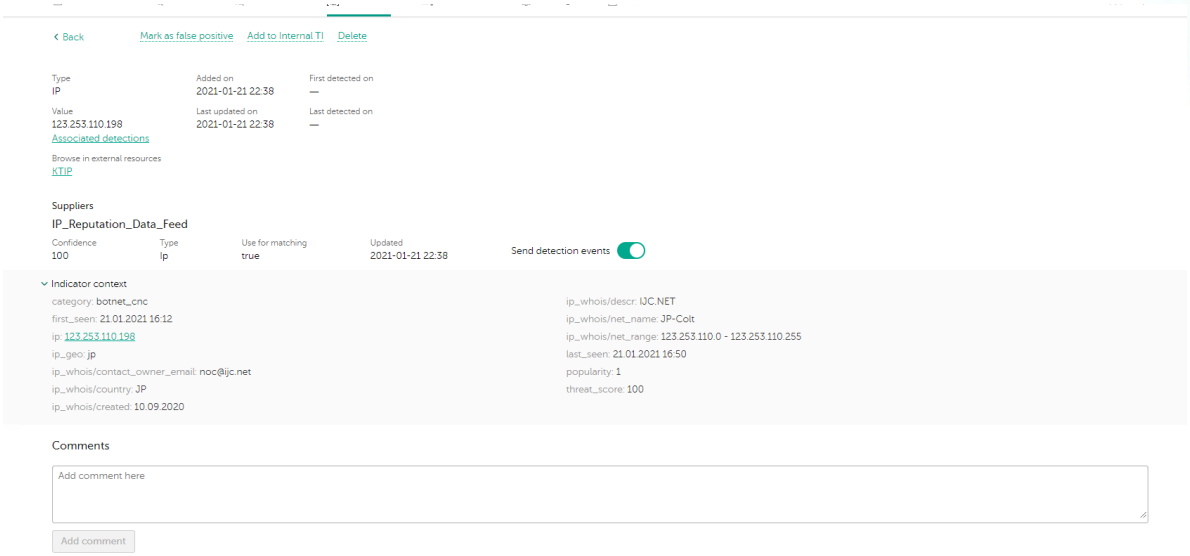

Рисунок 2. Страница со сводной информацией по индикатору

- Хранилище событий обнаружения позволяет упростить процессы мониторинга и приоритизации оповещений безопасности. Необработанное событие, полученное из источника, и вся связанная информация сохраняются в базе для дальнейшего анализа. Список событий обнаружения поддерживает поиск по любым полям, включая тип угрозы, IP адрес источника события, имя пользователя и т.д.
- Возможность выгрузить индикаторы позволяет экспортировать их в используемые системы безопасности в качестве стоп-листов, а также использовать их в других экземплярах Kaspersky CyberTrace или с другими Threat Intelligence платформами.

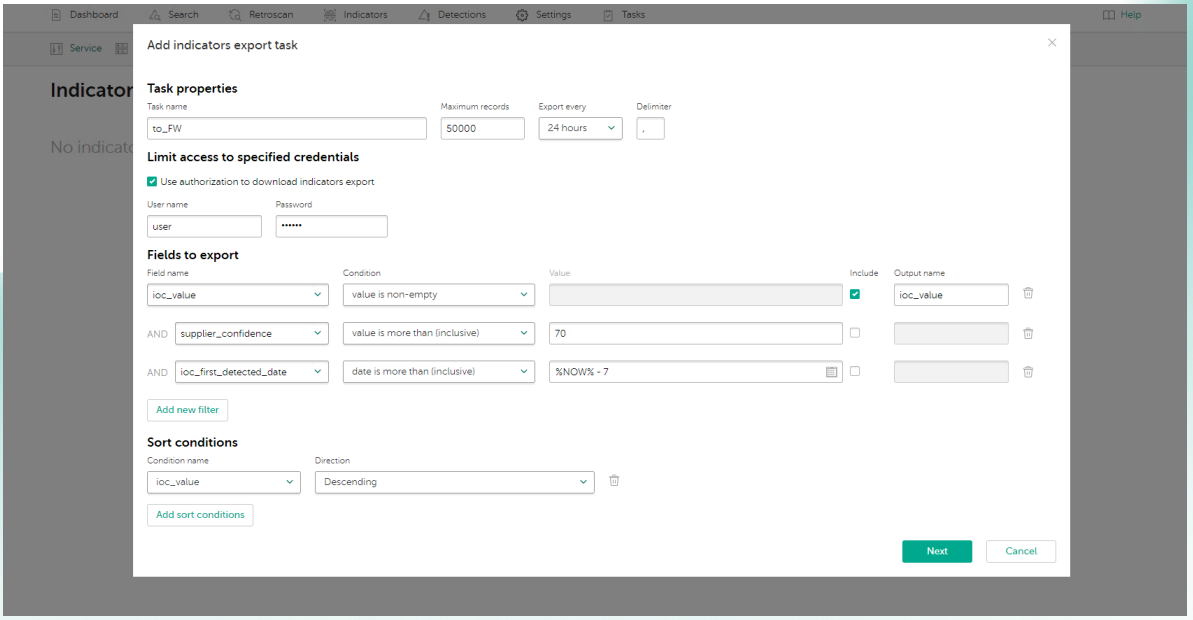

Рисунок 3. Создание задачи на экспорт индикаторов

- Возможность проверки уже проанализированных событий с использованием самых последних данных об угрозах позволяет выявить ранее необнаруженные инциденты для проведения дальнейших расследований.
- Фильтрация отправляемых в SIEM событий обнаружения дает возможность снизить нагрузку на эту систему, а также упросить дальнейшую работу аналитиков. CyberTrace позволяет отправлять в SIEM только наиболее опасные события, а также события с высоким коэффициентом доверия, которые однозначно требуют дальнейшего расследования. Все остальные события сохраняются в базе данных и могут использоваться в процессе анализа причин инцидентов или в процессе проактивного поиска угроз (threat hunting).
- Поддержка мультитенантной архитектуры позволяет реализовать сценарии использования поставщиков сервисов безопасности (MSSP) или крупных компаний, когда есть необходимость анализировать события различных клиентов или дочерних отделений по отдельности. Данный функционал позволяет подключить один экземпляр Kaspersky CyberTrace ко многим SIEM-системам, установленным в дочерних или обслуживаемых организациях, и отдельно настроить потоки данных, которые должны быть использованы для каждой их них.

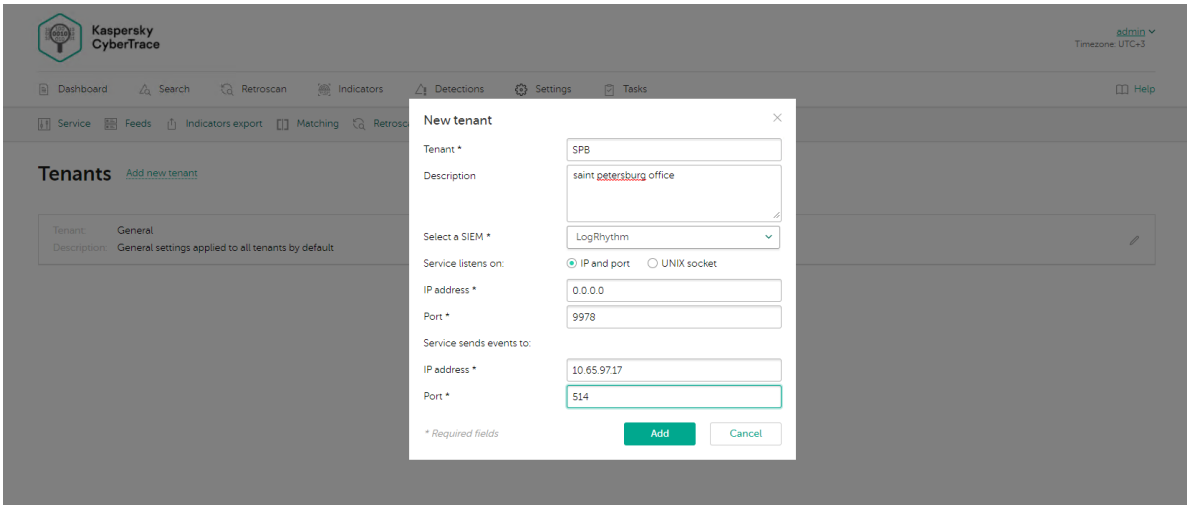

Рисунок 4. Заведение нового тенанта

- Статистика детектов по подключённым потокам данных позволяет сравнить их эффективность для конкретной инфраструктуры, определить, какое количество индикаторов из одного потока есть также в потоке из другого используемого источника, и, соответственно, выбрать те потоки, которые больше всего подходят компании.

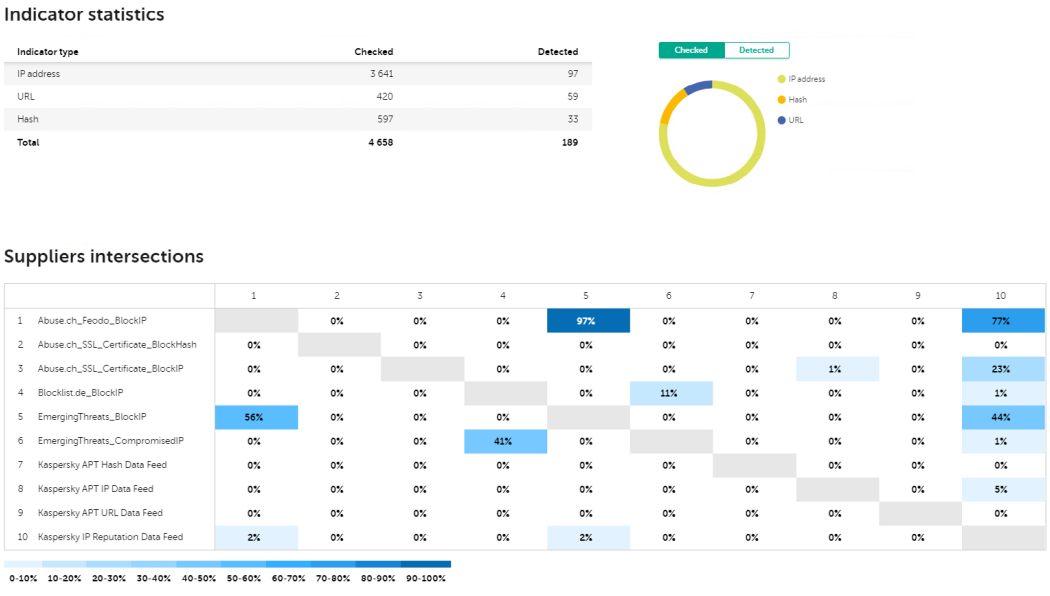

Рисунок 5. Наглядное представление различной эффективности используемых источников данных

Другие возможности Kaspersky CyberTrace:

- SIEM-коннекторы для визуализации данных об обнаружении угроз и управления ими;
- Расширенная фильтрация потоков
- Массовое сканирование логов и файлов;
- Интерфейс командной строки для платформ Windows и Linux;
- Автономный режим, в котором Kaspersky CyberTrace получает и анализирует логи различных систем, например, логи сетевых устройств;
- И многое другое

- С помощью HTTP RestAPI, Kaspersky CyberTrace может быть просто интегрирован в комплексную инфраструктуру для автоматизации и оркестрации работы с данными threat intelligence.
- Поддержка интеграции с Kaspersky Unified Monitoring and Analysis Platform (KUMA), включая единый веб-интерфейс.

Хотя Kaspersky CyberTrace и потоки данных «Лаборатории Касперского» об угрозах можно использовать по отдельности, при совместном использовании они существенно расширяют возможности обнаружения угроз, предоставляя специалистам по обеспечению безопасности их полную картину. Kaspersky CyberTrace и потоки данных «Лаборатории Касперского» об угрозах позволяют:

- Оперативно выявлять критичные оповещения систем безопасности для принятия взвешенных решений об их дальнейшей передаче группам реагирования на инциденты
- Снизить нагрузку на аналитиков безопасности и предотвратить их «выгорание»
- Более эффективно использовать имеющиеся ресурсы и сконцентрировать усилия на работе с серьезными инцидентами
- Создать проактивную систему защиты на основе глобальных аналитических данных.

Cyber Threats News: www.securelist.com
IT Security News: business.kaspersky.com
IT Security for SMB: kaspersky.com/business
IT Security for Enterprise: kaspersky.com/enterprise
Threat Intelligence Portal: opentip.kaspersky.com

www.kaspersky.com

We are proven. We are independent. We are transparent. We are committed to building a safer world, where technology improves our lives. This is why we secure it, so everyone everywhere has the endless opportunities it brings. Bring on cybersecurity for a safer tomorrow.

Find out more at kaspersky.com/transparency

Proven.
Transparent.
Independent.