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.

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 1-й линии получают достаточно контекста, чтобы сразу выявлять события, которые требуют более пристального изучения или эскалации группам реагирования на инциденты для проведения детального расследования. 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 упростить интеграцию потоков данных с SIEM системами для их дальнейшего более эффективного использования. Это средство позволяет работать с любым потоком аналитических данных об угрозах в форматах JSON, STIX, XML и CSV: open-source, от «Лаборатории Касперского», от других поставщиков, а также собственными кастомизированными потоками. CyberTrace также поддерживает “out-of-the-box” интеграцию с различными SIEM системами и источниками логов. Благодаря автоматическому сопоставлению полученных логов с потоками аналитических данных об угрозах, Kaspersky CyberTrace обеспечивает «ситуационную осведомленность» в режиме реального времени и позволяет аналитикам 1-й линии принимать своевременные и более взвешенные решения.

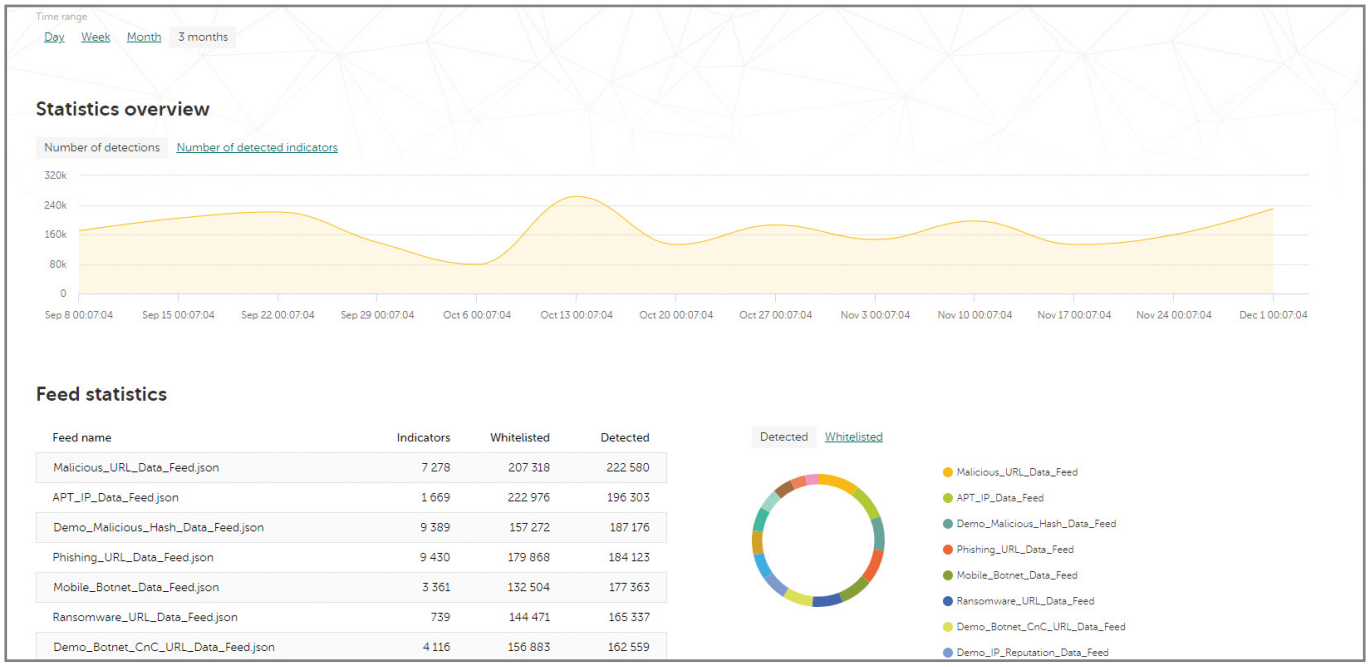


Рисунок 1. Статистика Kaspersky

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

- в стандартной версии доступны демонстрационные потоки данных об угрозах от «Лаборатории Касперского» и потоки из открытых источников (OSINT);
- SIEM-коннекторы для визуализации данных об обнаружении угроз и управления ими;
- статистика использования для измерения эффективности используемых потоков данных;
- поиск индикаторов по запросу (контрольные суммы, IP-адреса, домены, URL-адреса) для углубленного исследования угроз;
- пользовательский веб-интерфейс с визуализацией данных, доступом к конфигурации, управлением потоками, правилами парсинга логов, черными и белыми списками;
- расширенная фильтрация потоков (на основе контекста, предоставляемого каждым из индикаторов, включая тип угрозы, географическое положение, популярность, метки времени и др.) и логов (на основе пользовательских условий);
- экспорт результатов поиска по индикаторам, содержащихся в потоках данных, в формат CSV для интеграции с другими системами (сетевые экраны, системы предотвращения вторжений (IDS) на уровне сети и хоста, другие инструменты);
- массовое сканирование логов и файлов;
- интерфейс командной строки для платформ Windows и Linux;
- автономный режим, в котором Kaspersky CyberTrace не интегрируется с SIEM-системой, а получает и анализирует логи различных систем, например, логи сетевых устройств;
- возможность установки в DMZ, когда требуется изоляция от интернета.

Этот продукт 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 рисунке ниже показана высокоуровневая архитектура интеграции решения.

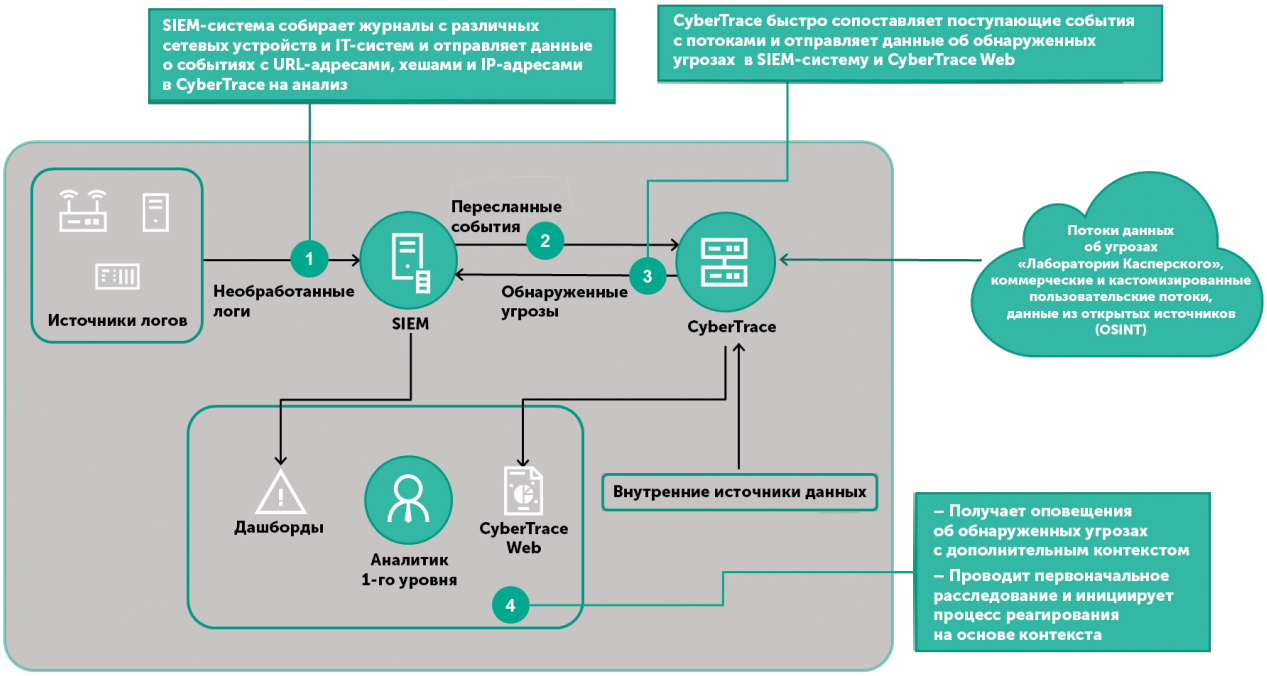


Рисунок 2. Схема интеграции Kaspersky CyberTrace

«Лаборатория Касперского» также предлагает набор постоянно обновляемых потоков данных об угрозах, которые могут интегрироваться с Kaspersky CyberTrace, обеспечивая глобальное представление об угрозах, их своевременное обнаружение, приоритизацию оповещений систем защиты и эффективное реагирование на инциденты:

- **Данные о репутации IP-адресов** – список IP-адресов с контекстной информацией, сообщающий о подозрительных и вредоносных узлах.
- **URL-адреса вредоносных и фишинговых ссылок** — список URL-адресов, соответствующих опасным ссылкам и веб-сайтам. Доступны записи с масками и без масок.
- **URL-адреса командных серверов ботнетов** – список URL-адресов командных серверов ботнетов и связанных с ними вредоносных объектов.
- **URL-адреса командных серверов ботнетов для мобильных устройств** – список URL-адресов командных серверов ботнетов для мобильных устройств. Идентификация зараженных устройств, обменивающихся данными с командными серверами.
- **URL-адреса программ-вымогателей** – ссылки на страницы, где размещены программы-вымогатели (ransomware) или к которым обращаются такие программы.
- **Индикаторы заражения APT** – вредоносные домены, хосты, IP-адреса и файлы, используемые злоумышленниками для осуществления APT-атак.
- **Passive DNS (pDNS)** – набор записей, содержащий результаты DNS разрешений доменов в соответствующие IP-адреса[1];
- **URL-адреса IoT угроз** – веб-сайты, которые использовались для загрузки вредоносного ПО, заражающего устройства интернета вещей[2];
- **Хеши вредоносных объектов** – список файловых хешей, охватывающий наиболее опасные и распространенные, а также самые новые вредоносные программы.
- **Хеши вредоносных объектов для мобильных устройств** – список файловых хэшей для обнаружения вредоносных объектов, заражающих мобильные устройства на базе Android и iOS.
- **Данные о троянцах P-SMS** – список хэшей троянцев с контекстной информацией для обнаружения SMS-троянцев, которые звонят с мобильных телефонов на платные номера, а также позволяют злоумышленнику перехватывать SMS-сообщения, отвечать на них и удалять их.
- **Данные белых списков** – систематизированный список хэшей надежных файлов, доступный для использования решениями и сервисами третьих сторон.

1 Поддержка интеграции будет добавлена в 2019 г.

2 Поддержка интеграции будет добавлена в 2019 г.

Данные собираются из множества разнообразных надежных источников, включая сеть Kaspersky Security Network, наши собственные поисковые роботы, сервис мониторинга ботнет-угроз (круглосуточное слежение за ботнетами и их мишенями), ловушки для спама, данные исследовательских групп и партнеров.

Вся собранная информация тщательно проверяется и очищается в режиме реального времени при помощи различных методов предварительной обработки: статистических методов, инструментов экспертных систем «Лаборатории Касперского» (таких как песочницы и средства эвристического анализа, мультисканеры, определения сходства и профилирования моделей поведения), проверки аналитиками и сопоставления с белыми списками.

Каждая запись в каждом потоке содержит обширные контекстные данные (оценки угроз, географическое положение, имена угроз, метки времени, установленные IP-адреса зараженных веб-ресурсов, хеши, популярность и т. п.).

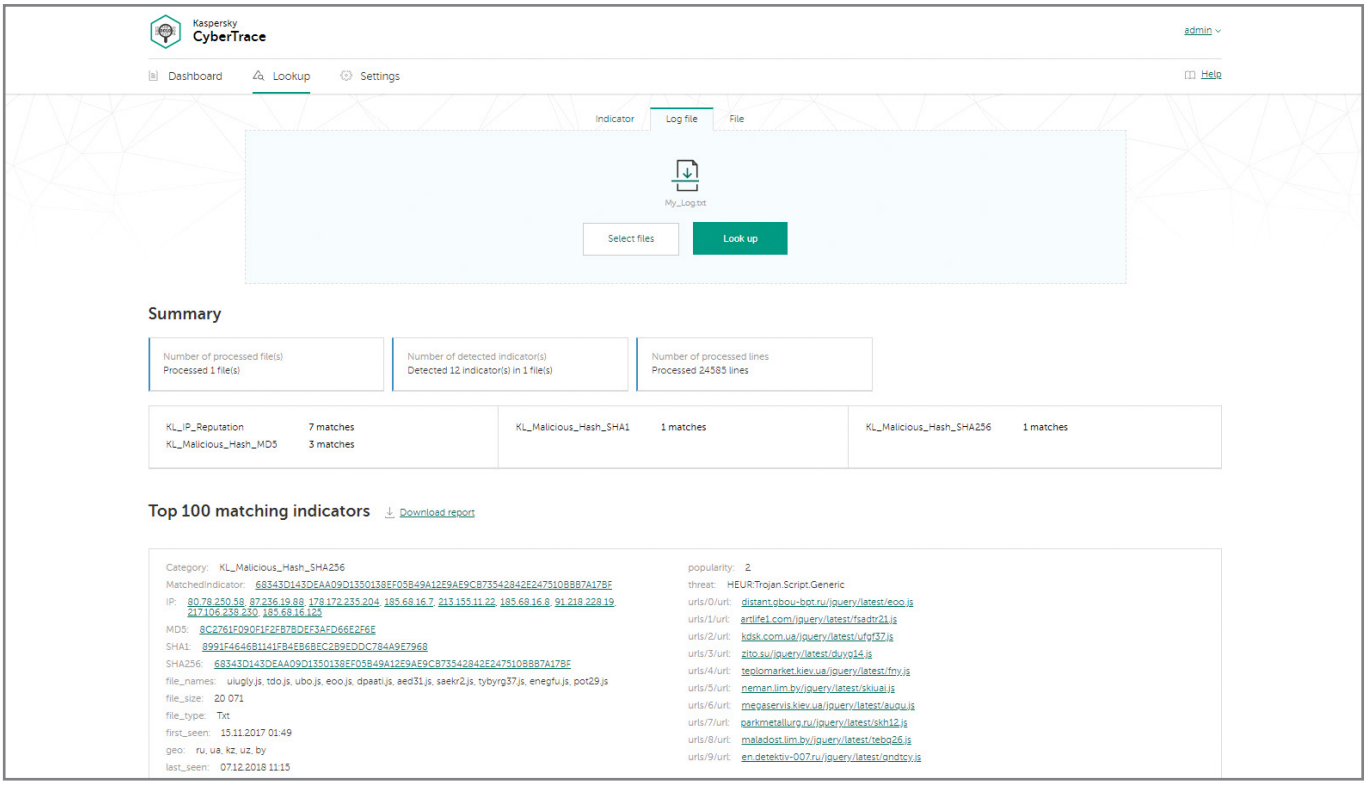
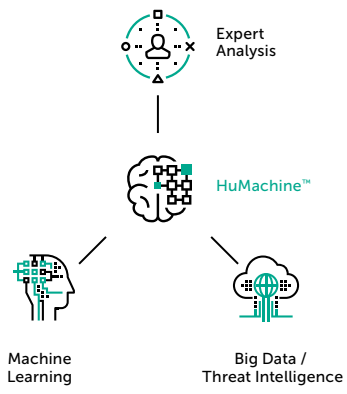


Рисунок 3. Контекст потоков данных об угрозах

Эти данные можно использовать, например, чтобы составить общее представление о ситуации или провести дополнительные проверки. Они помогут найти ответы на вопросы «кто?», «что?», «где?» и «когда?», чтобы выявить источники атак и принять своевременные решения.

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 аналитикам центра обеспечения безопасности:

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



www.kaspersky.ru

#ИстиннаяБезопасность