Kaspersky
Security Day
2021

Мощь синергии CyberTrace и KUMA

Артем Карасев,
старший менеджер
по продуктовому маркетингу

kaspersky

Польза от использования потоков данных очевидна, но...

Несколько источников данных
Данные из различных источников должны дополнять друг друга

Нерелевантная информация
Сложно определить наиболее подходящие источники данных

Ложные срабатывания
Сортировка ложных срабатываний увеличивает время реагирования

Половина всех оповещений вообще не обрабатывается

Отсутствие единого формата
JSON, STIX 1.x, STIX 2.x, CSV, XML и так далее

Огромное количество индикаторов
Существующие системы безопасности не могут обработать такие объемы данных «из коробки»

Платформы threat intelligence решают эти проблемы, но...

Новые проблемы

Медленный API для импорта и экспорта данных

Обновление ~1млн индикаторов может занять несколько часов

Не адаптированы к обработке большого количества информации

Если есть необходимость просканировать большой объем логов или поискать по историческим данным

Ограниченный контроль времени жизни индикатора

Ведет к увеличению количества ложных срабатываний и пропусков

Использование встроенных в SIEM механизмов сопоставления

Перегрузка SIEM-системы
SIEM-системы не предназначены для обработки такого количества индикаторов и контекста

Ложноотрицательные результаты
Из-за ограниченной логики сопоставления и отсутствия нормализации поступающих данных

github.com@520966948 — это обфусцированный **www.facebook.com** или **http://31.13.83.36/**

Kaspersky CyberTrace — Threat Intelligence платформа

SIEM-система собирает журналы с различных устройств и IT-систем и отправляет данные о событиях с URL и IP-адресами и хэшами в CyberTrace на анализ

CyberTrace быстро сопоставляет поступающие события с потоками данных об угрозах и отправляет данные об обнаруженных угрозах в SIEM и CyberTrace Web

- Получает оповещения об обнаруженных угрозах с дополнительным контекстом
- Проводит первоначальное расследование и инициирует процесс реагирования на основе контекста

Функциональность CyberTrace 3.0

Выделенная команда, которая занимается разработкой продукта уже несколько лет для обеспечения эффективной интеграции наших потоков данных об угрозах

CyberTrace интегрируется с любым потоком данных и позволяет использовать различные потоки одновременно

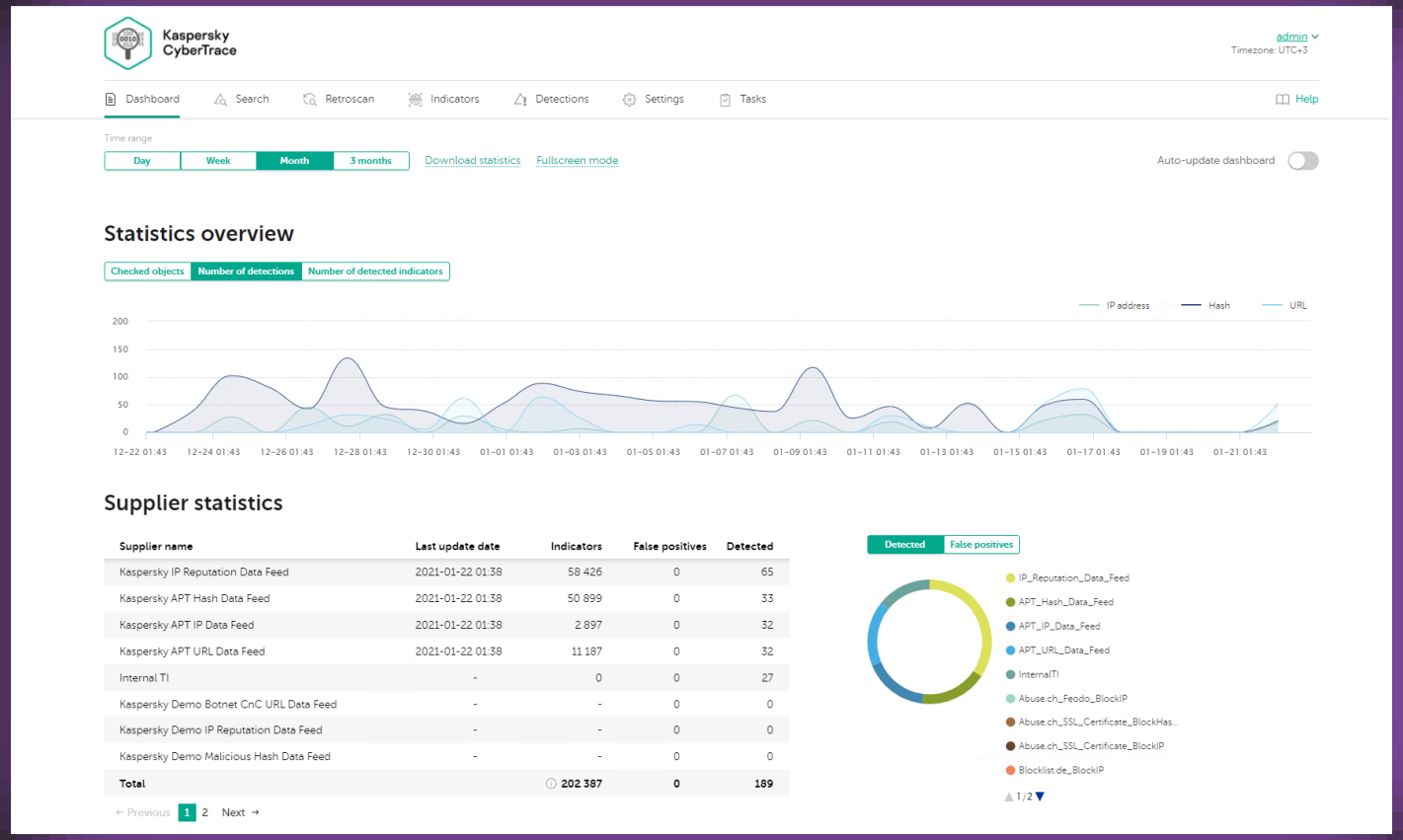
CyberTrace обеспечивает прямую интеграцию с любой системой безопасности (файерволлы, прокси и т.д.), а также с SIEM-системами и системами управления логами

CyberTrace снижает нагрузку на SIEM-системы с помощью встроенных механизмом парсинга и «матчинга»

Встроенные механизмы сопоставления эффективно выявляют техники оббфускации, используемые для скрытия вредоносной активности в логах

CyberTrace позволяет сравнить эффективность интегрированных потоков данных с помощью статистики по их обнаружениям

CyberTrace 4.0



База данных для хранения и поиска по данным (+ retroscan)

Агрегация, дедупликация, нормализация и обмен данными

Статистика обнаружений и матрица пересечений по потокам даных

Публичный API (для интеграции и актоматизации)

Мультитенантность для MSSP
и крупных предприятий

Синергия KUMA и CyberTrace

CyberTrace и сторонний SIEM

Парсинг событий

Необходимо отдельно настраивать парсинг для SIEM и для CyberTrace

Расследование

Для расследования детекта CyberTrace нужно будет найти исходное событие

Логика обнаружения

Повышение сложности корреляции за счёт дополнительного критерия в виде детекта CyberTrace

Парсинг событий

Для CyberTrace не нужно отдельно настраивать регулярные выражения

Расследование

Результаты enrichment пишутся сразу в исходное событие

Логика обнаружения

Создание кастомного индикатора из инцидента и добавление его в базу CyberTrace в едином интрефейсе

Интеграция с KUMA

Основные преимущества

Повышает эффективность обнаружения угроз

Позволяет оптимизировать трудозатраты аналитиков

Существенно снижает время реагирования на инциденты

Спасибо!

kaspersky