Передовая защита инфраструктуры конечных точек в виртуозном исполнении

Kaspersky Symphony EDR

kaspersky АКТИВИРУЙ БУДУЩЕЕ

Ключевой элемент XDR

Kaspersky Symphony EDR — один из тиров экосистемы решений Kaspersky Symphony и ключевой элемент верхнего тира — комплексной платформы класса XDR (Extended Detection and Response) Kaspersky Symphony XDR

Введение

Рабочие места, где тесно взаимосвязаны данные, пользователи и корпоративные системы, играют важнейшую роль в бизнесе, а также имеют большую значимость в области IT-безопасности. В современном мире конечные точки остаются основной целью злоумышленников. Чтобы обеспечить полный цикл защиты рабочих мест, от автоматического блокирования угроз до мгновенного обнаружения и оперативного реагирования на сложные инциденты, важно применять превентивные технологии вместе с прогрессивными мерами защиты.

Kaspersky Symphony EDR

Kaspersky Symphony EDR — это мощное решение класса EDR (Endpoint Detection and Response), разработанное для экспертов в области ИБ, которое в синергии с включенной базовой защитой конечных точек EPP (Endpoint Protection Platform) Kaspersky Symphony Security позволяет блокировать массовые угрозы, автоматически и проактивно искать сложные киберугрозы, проводить расследования инцидентов и предоставляет ИБ-специалистам обширный инструментарий для реагирования. Все это позволяет обеспечить быстрое и точное сдерживание угроз и эффективное устранение инцидентов в распределенных инфраструктурах, оптимизируя работу ИБ-отдела, а комплексная защита конечных точек на базе единого агента позволяет экономить на обслуживании и поддержке установленных продуктов при минимальном влиянии на производительность.

EDR

2 Обнаружение

Обнаружение на основе IoC, IoA и кастомных правил

Обогащение обнаружений глобальными данными об угрозах

Проактивный поиск угроз и ретроспективный анализ

3 Расследование

Расследование и анализ первопричин

Базовый инструментарий цифровой криминалистики

4 Реагирование

Поддержка различных мер по реагированию

EPP

1 Предотвращение

Передовой антивирусный движок

Различные контроли безопасности и защита данных

Управление уязвимостями и обновлениями

Поведенческий анализ и адаптивный контроль аномалий

Функциональные возможности решения

Kaspersky Symphony EDR, в дополнение к включенным в решение превентивным технологиям и поддержке различных контролей, представляет собой истинный симфонический оркестр безопасности на уровне инфраструктуры конечных точек. Он обеспечивает всесторонний обзор всех рабочих мест в корпоративной сети (физических и виртуальных) и визуализацию каждого этапа расследования. С помощью мощного арсенала детектирующих движков и инструментов анализа первопричин Kaspersky Symphony EDR обеспечивает эффективное обнаружение и расследование угроз. Ретроспективный анализ и сопоставление обнаружений с базой знаний MITRE ATT&CK позволяют идентифицировать тактики и техники злоумышленников. Продукт также предоставляет проактивный поиск угроз и доступ к порталу Kaspersky Threat Intelligence, что позволяет экспертам воссоздать последовательность действий злоумышленников и эффективно противостоять самым изощренным атакам.

EPP

Ведущие превентивные технологии, в том числе на базе машинного обучения

- Защита, поддерживающая все типы конечных точек: мобильные, физические и виртуальные
- Автоматическая блокировка угроз
- Автоматическое восстановление
- Защита от шифровальщиков
- Защита от эксплуатации уязвимостей
- Защита от кражи учетных данных

Контроли безопасности и данных

- Контроль приложений
- Веб-контроль
- Контроль устройств
- Адаптивный контроль аномалий
- Управление шифрованием и политиками
- Шифрование портативных устройств

Оценка уязвимостей и управление исправлениями

- Расширенное управление исправлениями
- Оценка уязвимостей
- Управление лицензиями
- Централизованное развертывание приложений и ОС
- Инструменты удаленного управления
- Инвентаризация

EDR

Автоматическое обнаружение сложных угроз

- Сбор данных и их хранение
- Передовые механизмы обнаружения по IoA-правилам
- Автоматический доступ к TI (KSN)
- Ретроспективный анализ
- Корреляция событий

IoC-поиск и threat hunting

- Полная видимость и контроль
- Приоритизация инцидентов
- IoC-сканирование
- Применение Yara-правил
- Доступ в Threat Lookup
- Гибкий конструктор поисковых запросов

Реагирование

- Инструмент принятия решений по реагированию на инциденты
- Постановка задач по автоматическому реагированию
- Рекомендации по реагированию
- Сдерживание угрозы
- Централизованная локализация инцидентов

Международное признание

Наши технологии регулярно проходят независимые тестирования, признаны ведущими аналитическими агентствами и удостоены многочисленных международных сертификатов и наград.

MITRE | ATT&CK®

Качество обнаружения подтверждено оценкой MITRE ATT&CK

IDC

«Лаборатория Касперского» признана ключевым игроком в области защиты конечных устройств для бизнеса, по версии IDC MarketScape

AV-TEST

Независимая лаборатория AV-Comparatives протестировала технологии EPP и EDR от Kaspersky и присвоила статус стратегического лидера

SE Labs AAA Enterprise Advanced Security EDR Detection Apr–Jun 2023

SE Labs протестировала эффективность технологий EPP и EDR от Kaspersky против широкого спектра кибератак и присвоила решению рейтинг AAA

Ценность для вашего бизнеса

Повышает эффективность защиты с помощью мощного корпоративного решения по обнаружению инцидентов и реагированию на них

Усиливает контроль инфраструктуры рабочих мест и повышает качество обнаружения сложных угроз с помощью продвинутых технологий

Налаживает процессы обнаружения угроз, управления инцидентами и реагирования на них, оптимально распределяя ресурсы

Повышает эффективность внутреннего SOC и экономит время специалистов

Автоматизирует выявление угроз и реагирование на них, не нарушая работу бизнеса

Обеспечивает соответствие требованиям действующего законодательства

Kaspersky Symphony EDR

Подробнее

www.kaspersky.ru

#kaspersky
#активируйбудущее