Защита организации
от сложных и целевых атак

Kaspersky Anti Targeted Attack

с модулем NDR

kaspersky активируй будущее

Kaspersky Anti Targeted Attack

Непревзойденный уровень кибербезопасности

Платформа для защиты от сложных угроз и целевых атак состоит из трех модулей:

Kaspersky Anti Targeted Attack — решение, которое обеспечивает анализ сетевого трафика, позволяя контролировать точки входа потенциальных угроз: сеть, веб-трафик, электронная почта, а также предоставляет возможность проверять потенциально вредоносные объекты в песочнице.

Network Detection & Response (NDR) — модуль, позволяющий проводить глубокий анализ сетевого трафика, выявлять атаки с помощью правил детектирования, индикаторов компрометации и ретроспективного анализа. Позволяет строить карту сети и таблицу сетевых сессий, производить определение и разбор протоколов, осуществлять проактивный поиск угроз по сырому трафику и реагировать на сетевых устройствах и Firewall.

Kaspersky Endpoint Detection & Response Expert — система, которая предоставляет специалистам ИБ полную картину событий в инфраструктуре рабочих мест и серверов и обеспечивает ее эффективную защиту от сложных угроз и APT-атак.

400 млн ₽

средний ущерб от успешной кибератаки в корпоративном сегменте

23 дня

среднее время простоя бизнеса из-за атак программ-вымогателей

25%

всех атак относится к APT

Комплексное решение

Контролируйте все распространенные точки входа для угроз: сеть, веб-трафик, электронную почту, рабочие места, серверы и виртуальные машины, которые будут надежно защищены нашими технологиями. Контролируйте все, что происходит внутри сети.

Единая платформа для централизованного управления защитой всей инфраструктуры

Kaspersky Anti Targeted Attack

с модулем NDR

Комплексная защита от сложных угроз, APT и целевых атак

Kaspersky EDR Expert

Защита рабочих мест от сложных угроз, APT и целевых атак

Network Detection & Response — новый уровень безопасности

Расширьте возможности KATA в части сетевого обнаружение и реагирования при помощи модуля NDR.

Какие задачи решает NDR?

- Анализ внутрисетевого трафика
- Выявление точных первопричин появления алерта
- Исследование сетевых аномалий
- Тестирование гипотез
- Ретроспективный анализ ранее записанной копии трафика
- Повышение видимости во всех сегментах сети

Уникальные преимущества KATA с модулем NDR

- Использование сработок на узлах для формирования комплексных инцидентов, включающих сетевые и узловые алерты
- Выявление имени процесса, порождающего сетевую активность для более быстрого процесса проактивного поиска угроз
- Коннекторы для настраиваемого реагирования на сетевых устройствах
- Использование антивируса Kaspersky в качестве сенсора для NDR
- Единая консоль управления для KATA, KEDR, NDR
- Построение карты сети во всех сегментах сети (даже там, где нет SPAN)
- Возможность автоматического реагирования через KSMG, KWTS, NGFW, KEDR Expert по обнаружениям от KATA Sandbox
- Обогащение информации по ассетам, сетевым коммуникациям и событиям
- Интеграция антивируса Kaspersky и KATA Sandbox

Гибкий подход к вашим задачам

Используйте комбинацию возможностей платформы для необходимого уровня защиты

	KATA	KATA с модулем NDR	KATA с модулем NDR и EDR Expert
Sandbox			
Проверка объектов на предустановленных образах операционных систем Windows 7, Windows 10, CentOS 7.8, Astra 1.7	●	●	●
Проверка объектов на собственных образах Windows XP, Windows 7, Windows 10 с возможностью настраивать логику детектирования объектов	●	●	●
Central Node			
IDS-правила для Suricata	●	●	●
Проверка ссылок (URL reputation)	●	●	●
Проверка антивирусным движком (Antimalware Engine)	●	●	●
Проверка файлов мобильных приложений (APK-файлы)	●	●	●
Проверка цифровой подписи файлов	●	●	●
Получение репутации объекта из KSN	●	●	●
Проверка при помощи YARA правил	●	●	●
Выявление угроз в шифрованном трафике без его расшифровки (TLS Fingerprinting)	●	●	●
Сетевые аномалии и риски		●	●
Определение и разбор протоколов		●	●
Хранение сырого трафика		●	●
Проактивный поиск угроз в ранее записанном трафике (Threat Hunting по SPAN)		●	●
Инвентаризация сети и поиск неавторизованных устройств		●	●
Построение карты сети и отображение сетевой активности устройств		●	●
Таблица сетевых сессий		●	●
Интеграция с KES Win / KES Linux*		●	●
Модуль для выявления аномального поведения в сетевой телеметрии с endpoint (Targeted Attack Analyzer)			●
Проверка сетевой телеметрии на индикаторы компрометации (IOC)			●
Threat hunting по сетевой телеметрии с endpoint			●
EDR			
Агент EDR для Windows, Linux и MAC			●

(i) Решение KATA с модулями NDR и KEDR Expert покрывает более 460 TTP матрицы MitreATTACK

* KES «Расширенный» и KES«Total» (Windows и Linux) могут быть подключены к KATA NDR в качестве дополнительных источников для сбора сетевой статистики. Эта опция недоступна для KES «Стандартный».

Сертификаты и соответствие стандартам

Федеральный закон N187

Решения «Лаборатории Касперского» помогают организациям соответствовать требованиям законодательства РФ в области безопасности КИИ, в том числе требованиям к построению центров ГосСОПКА.

Реестр российского ПО

Продукты Kaspersky Anti Targeted Attack и Kaspersky EDR Expert входят в реестр российского ПО (рег. номер ПО №8350 от 30.12.2020 и рег. номер ПО №8352 от 30.12.2020).

ФСТЭК России

Платформа Kaspersky Anti Targeted Attack имеет сертификат ФСТЭК России, который удостоверяет, что решение соответствует требованиям безопасности информации, устанавливающим уровни доверия к средствам технической защиты информации и средствам обеспечения безопасности информационных технологий по 4 уровню доверия и требованиям к СОВ (профиль защиты СОВ уровня сети четвертого класса защиты — ИТ.СОВ.С4.ПЗ).

ФСБ России

Платформа Kaspersky Anti Targeted Attack имеет сертификат ФСБ России на соответствие требованиям, предъявляемым к средствам обнаружения компьютерных атак класса «АП», и может использоваться в автоматизированных информационных системах, обрабатывающих информацию, не содержащую сведений, составляющих государственную тайну. Решение соответствует требованиям ФСБ России к антивирусным средствам класса «Д» и может использоваться для защиты информации, содержащей сведения, составляющие государственную тайну.

Наши клиенты — российские и зарубежные компании по всему миру

Промышленность

КУМТОР KUMTOR
Подробнее

ФОСАГРО
Подробнее

НОВОСТАЛЬ-М
Подробнее

РН-БашНИПИнефть
Подробнее

Kin Yat Holding
Подробнее

Финансы

МКБ
Подробнее

KICB KYRGYZ INVESTMENT AND CREDIT BANK
Подробнее

OptimaBank
Подробнее

Розничная торговля

МАГНИТ
Подробнее

Государственные структуры

Правительство Ростовской области
Подробнее

Kaspersky
Anti Targeted
Attack

Подробнее

www.kaspersky.ru

© 2025 АО «Лаборатория Касперского».
Зарегистрированные товарные знаки и знаки обслуживания являются собственностью их правообладателей.

#kaspersky
#активируйбудущее