

Kaspersky EDR Expert

Актуальные проблемы ИТ-безопасности:

- Необходимость ручного разбора и анализа большого числа инцидентов
- Эксплуатация средств ИБ, которые не взаимодействуют друг с другом и управляются из разных консолей
- Принятие решений без использования средств для наглядного централизованного представления информации
- Выполнение сложных задач в условиях нехватки квалифицированных кадров и экспертизы
- Несоответствие требованиям регулирующих органов и действующего законодательства

Экспертное решение для защиты вашей инфраструктуры

Рабочие места по-прежнему остаются основной мишенью злоумышленников и удобными точками входа при проведении кибератак. Чтобы защитить рабочие места и не дать преступникам использовать их для проникновения в инфраструктуру, ИБ-специалистам необходимо осваивать новые способы усиления существующей системы безопасности. Полный цикл защиты рабочих мест, от автоматического блокирования распространенных угроз до быстрого реагирования на сложные инциденты, предполагает использование превентивных технологий наряду с расширенными возможностями защиты.

Kaspersky EDR Expert — это мощная система информационной безопасности, которая предоставляет специалистам ИБ полную картину событий в инфраструктуре рабочих мест и серверов и обеспечивает их эффективную защиту от сложных угроз и АPT-атак.

1

Kaspersky EDR Expert дополняет платформу для защиты рабочих мест — **Kaspersky Security для бизнеса**, предлагая мощные функции обнаружения, расследования и реагирования, которые значительно повышают уровень безопасности.

2

Kaspersky EDR Expert предоставляет детализированный анализ угроз и поддерживает как автоматическое сравнение результатов внутренних расследований с глобальной репутационной базой **Kaspersky Security Network**, так и получение дополнительного контекста от **Kaspersky Threat Intelligence**.

3

Kaspersky EDR Expert может входить в состав платформы **Kaspersky Anti Targeted Attack**, благодаря чему возможности EDR совмещаются с функциями обнаружения продвинутой угрозы на уровне сети, создавая решение класса XDR нативного типа. Также, эта технология EDR лежит в основе гибридного типа XDR от «Лаборатории Касперского» — **Kaspersky Symphony XDR**.



Ваш выбор защиты для устойчивого развития бизнеса

Решения XDR от «Лаборатории Касперского» помогают отражать продвинутые атаки значительно быстрее и с меньшими усилиями благодаря оптимально настроенной автоматизации защитных действий на уровне сети и рабочих мест, доступу к актуальной информации об угрозах и централизованному управлению.

Kaspersky Symphony XDR обеспечивает надежную защиту от кибератак, легко встраивается в текущую систему ИБ благодаря гибриднему типу XDR и помогает соответствовать требованиям законодательства, в том числе за счет встроенного модуля ГосСОПКА.

Kaspersky EDR Expert поможет вашей организации:

- Повысить эффективность защиты с помощью мощного корпоративного решения по обнаружению инцидентов и реагированию на них
- Усилить контроль инфраструктуры рабочих мест и повысить качество обнаружения сложных угроз с помощью продвинутых технологий
- Автоматизировать выявление угроз и реагирование на них, не нарушая работу бизнеса
- Наладить процессы обнаружения угроз, управления инцидентами и реагирования на них, оптимально распределяя ресурсы
- Повысить эффективность внутреннего SOC
- Соответствовать требованиям действующего законодательства

Быстрое обнаружение и устранение сложных угроз

Kaspersky EDR Expert надежно защищает рабочие места и повышает эффективность вашего SOC. Решение обеспечивает сбор, запись и централизованное хранение информации о событиях безопасности на всех рабочих местах, что позволяет обеспечить оперативный доступ к ретроспективным данным при расследовании продолжительных атак, даже в условиях недоступности рабочих мест, а также вредоносного шифрования или уничтожения данных злоумышленниками.

Расширенные функции обнаружения и расследования на основе уникальных индикаторов атак (IoA), сопоставление с базой знаний тактик и техник злоумышленников MITRE ATT&CK, гибкий инструмент создания запросов и доступ к порталу Kaspersky Threat Intelligence – все это обеспечивает эффективное выявление угроз и быстрое реагирование на инциденты до нанесения ущерба.

Анализ данных и расследование угроз

ХРАНЕНИЕ ДАННЫХ



Вердикты



Объекты



Телеметрия

СБОР ДАННЫХ



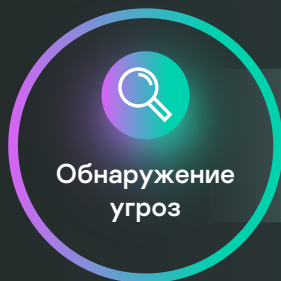
Сервер



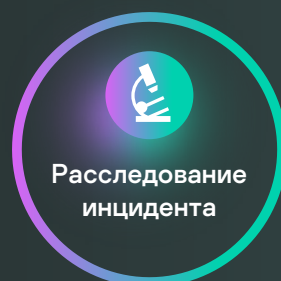
ПК



Ноутбук



Обнаружение
угроз



Расследование
инцидента



Мониторинг
и визуализация



Передовое автоматическое
детектирование угроз



Детектирование
на основе IoC и IoA



Проактивный
поиск угроз



Анализ
первопричин



Ретроспективный
анализ



Доступ к аналитическим
данным об угрозах



Обогащение данными
матрицы MITRE ATT&CK



Реагирование
на инцидент



Победитель Gartner Peer Insights Customers' Choice в категории EDR-решения, 2020 год

«Лаборатория Касперского» получила высокую награду Gartner Peer Insights Customers' Choice в категории EDR-решений. Всего 6 производителей в мире стали обладателями этой награды.

MITRE | ATT&CK®

Качество обнаружения подтверждено оценкой MITRE ATT&CK

Решение Kaspersky EDR Expert прошло тестирование MITRE ATT&CK (Раунд 2), показав высокую эффективность обнаружения ключевых техник, применяемых на основных этапах проведения современных целевых атак.

[Подробнее](#)



Решение Kaspersky EDR Expert было признано технологическим лидером на рынке EDR-решений

По результатам исследования 2020 SPARK Matrix от Quadrant Knowledge Solutions.

www.kaspersky.ru

© 2022 АО «Лаборатория Касперского». Зарегистрированные товарные знаки и знаки обслуживания являются собственностью их правообладателей.

Ценность Kaspersky EDR Expert для вашего бизнеса



Устранение брешей в системе безопасности и быстрое обнаружение атак



Автоматизация рутинных задач по обнаружению угроз и принятию ответных мер



Освобождение ресурсов ИТ и ИБ для решения более важных задач



Ускорение выявления угроз и принятия ответных мер



Повышение эффективности анализа угроз и реагирования на инциденты



Обеспечение соответствия требованиям регулирующих органов



[Подробнее](#)