Непрерывный поиск, обнаружение и помощь в устранении киберугроз, направленных на вашу организацию

Kaspersky Managed Detection and Response

kaspersky активируй будущее

Современные вызовы

55%

компаний сообщают, что их корпоративные устройства были заражены вредоносным ПО[1]

20%

компаний сталкиваются с APT-угрозами[2]

18%

респондентов отмечают, что причиной киберинцидентов в компании была нехватка квалифицированных ИБ-специалистов[3]

2,5 млрд $

составил максимальный ущерб в следствии успешной кибератаки[4]

Круглосуточная защита вашего бизнеса

Сегодня компании сталкиваются с целенаправленной киберагрессией и хактивизмом. Как следствие — необходимость в эффективной киберзащите возрастает с каждым днем. Организации могут иметь ограниченные ИБ-ресурсы, или же службы ИБ могут быть перегружены, что оставляет им мало времени для тщательной обработки киберинцидентов. К тому же найти опытных специалистов по обнаружению и реагированию на инциденты — совсем непростая задача.

Kaspersky Managed Detection and Response (MDR) — это решение по круглосуточной управляемой защите от растущего числа киберугроз и сложных атак, обходящих автоматические средства безопасности.

Решение повышает уровень информационной безопасности небольших организаций с невысоким уровнем ИБ-экспертизы за счет быстрого развертывания услуги «под ключ». А для опытных команд с развитой ИБ-экспертизой предоставляет дополнительную гибкость, поскольку они могут передать вопросы обнаружения и классификации инцидентов в «Лабораторию Касперского» или же получить дополнительное мнение по обнаруженным самостоятельно инцидентам.

Kaspersky MDR повышает устойчивость организации к киберугрозам, помогает эффективно использовать имеющиеся ресурсы, а также оптимизировать будущие инвестиции в информационную безопасность.

Ключевые возможности

- Проактивный поиск угроз (Threat Hunting)
- Обзор всех защищаемых ресурсов с их текущим статусом
- Автоматическое и управляемое реагирование на инциденты
- Прямой доступ к аналитикам SOC по вопросам инцидентов
- REST API для интеграции с IRP / SOAR
- Консоль управления с панелями мониторинга и отчетами
- Хранение необработанной телеметрии в течение 3 месяцев
- Возможность самостоятельно зарегистрировать инцидент при подозрении на компрометацию
- Совместимость со сторонними антивирусными решениями

[1] Исследование IT Security Economics, 2022
[2] Аналитический отчет Kaspersky MDR за 2023 год
[3] Kaspersky Human Factor 360 Report, 2023
[4] Global financial stability report. The Last Mile: Financial Vulnerabilities and Risks, 2024

Источники телеметрии и событий безопасности для Kaspersky MDR:

- Kaspersky Endpoint Security for Windows
- Kaspersky Endpoint Security for macOS
- Kaspersky Endpoint Security for Linux
- Kaspersky Virtualization Light Agent
- Kaspersky Anti-Targeted Attack
- Kaspersky Industrial CyberSecurity for Nodes

Как работает решение

1

Команда Kaspersky MDR расследует события безопасности и проактивно анализирует телеметрию, получаемую от установленных в сети клиента продуктов «Лаборатории Касперского», на предмет инцидентов. Эта телеметрия сопоставляется с аналитическими данными «Лаборатории Касперского» о киберугрозах и результатами успешных расследований APT-атак для выявления тактик, техник и процедур, применяемых злоумышленниками против конкретной организации. При этом уникальные индикаторы атак позволяют обнаружить скрытые угрозы, не использующие вредоносное ПО и имитирующие легитимную активность.

2

В рамках процесса обработки событий безопасности в Kaspersky MDR внедрены механизмы искусственного интеллекта. Они способствуют снижению количества ложноположительных срабатываний и ускоряют процесс обработки событий безопасности.

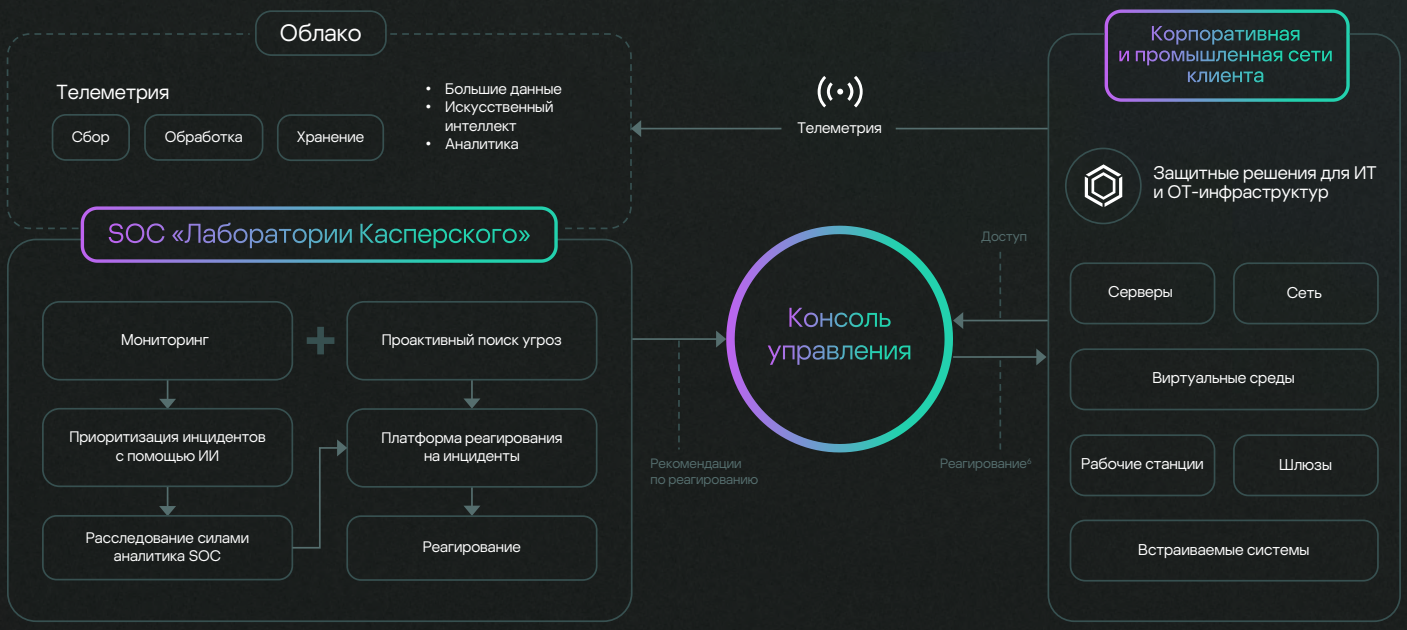
3

При обнаружении потенциальной угрозы решение классифицирует ее по уровню критичности и отправляет уведомление об инциденте на электронную почту и/или в Telegram. А анализ первопричин позволяет выявлять источники и принимать меры для их нейтрализации.

4

В рамках решения клиент может частично или полностью передать возможности по реагированию[5] команде SOC «Лаборатории Касперского». Имеющиеся вопросы в рамках инцидента можно обсудить в интерактивном чате в веб-консоли Kaspersky MDR.

Архитектура решения



Kaspersky MDR совместим со сторонними антивирусными решениями.

[5] Возможно проведение более глубокого анализа и расследования инцидента при наличии активной подписки на Kaspersky Incident Response

[6] Автоматическое реагирование начинается после того, как клиент одобрит его в консоли Kaspersky MDR (если клиент этого не сделает, консоль MDR запросит разрешение до начала автоматического реагирования).

Преимущества

Уверенность в том, вы находитесь под постоянной защитой

Сокращение расходов из-за отсутствия необходимости нанимать новых ИБ-специалистов

Возможность направить внутренние ИБ-ресурсы компании на решение других задач

Возможность пользоваться ключевыми преимуществами центра SOC, не имея его внутри компании

Быстрое подключение и простота использования консоли управления

Подтвержденная эффективность

«Лаборатория Касперского» активно участвует в независимых тестированиях и взаимодействует с ведущими мировыми аналитическими агентствами. Решение Kaspersky MDR признано во всем мире и удостоено многочисленных международных наград. А эффективные функции обнаружения и реагирования в Kaspersky MDR дополнены знаниями одной из самых успешных и опытных в отрасли команд по активному поиску угроз – команды SOC «Лаборатории Касперского», эксперты которой обладают многочисленными сертификатами, подтверждающими их высокий уровень экспертизы и знаний.

Kaspersky Managed Detection and Response

Подробнее

www.kaspersky.ru

#kaspersky
#активируйбудущее