Описание функций

Kaspersky Managed Detection and Response

kaspersky

kaspersky.ru

Введение

Противостоять изощренным угрозам, способным обходить системы автоматического обнаружения и реагирования, можно, только эффективно используя специализированные решения, такие как Kaspersky Anti Targeted Attack Platform. Для этого необходимы ресурсы и опытные кадры. Однако по всему миру наблюдается нехватка специалистов, способных противостоять сложным угрозам. Поэтому их услуги стоят недешево, из-за чего многие компании не спешат приобретать данный класс решений и сервисов.

Kaspersky Managed Detection and Response обеспечивает непрерывную круглосуточную защиту от растущего числа угроз, способных обходить системы автоматического обнаружения и реагирования. Это решение разработано специально для организаций, которым не хватает ресурсов и квалифицированных специалистов, но которые обладают зрелым подходом к информационной безопасности и понимают важность защиты от сложных и продвинутых угроз.

Архитектура

Продукты «Лаборатории Касперского»

Kaspersky Security для бизнеса, Kaspersky Endpoint Detection and Response и Kaspersky Anti Targeted Attack Platform отправляют метаданные в SOC «Лаборатории Касперского», используя инфраструктуру Kaspersky Security Network, распределенную по различным регионам.

Kaspersky Security Network

Kaspersky Security Network – это облачная репутационная база данных, предоставляющая продуктам «Лаборатории Касперского» аналитические данные об угрозах в режиме реального времени. Ее инфраструктура используется для передачи телеметрических данных клиентов в SOC «Лаборатории Касперского», который сопоставляет их и анализирует.

Security Operations Center «Лаборатории Касперского»

SOC «Лаборатории Касперского» ведет проактивный мониторинг телеметрических данных безопасности, получаемых от продуктов «Лаборатории Касперского». Используя регулярно обновляемые запатентованные индикаторы атаки, адаптированные к среде клиента, он выявляет угрозы, способные обходить системы автоматического предотвращения и обнаружения угроз. Процесс анализа в значительной степени автоматизирован и задействует запатентованные модели машинного обучения.

Портал Kaspersky Managed Detection and Response

Портал Kaspersky Managed Detection and Response дает полный обзор всех инцидентов, обнаруженных сервисом и продуктами «Лаборатории Касперского», оповещает о них и предоставляет подробные рекомендации по реагированию.

Агент EDR

Kaspersky Managed Detection and Response использует тот же агент, что Kaspersky Endpoint Detection and Response и Kaspersky Sandbox, но открывает дополнительные возможности после активации. Агент EDR позволяет изолировать зараженные хосты, завершать несанкционированные процессы, помещать на карантин и удалять вредоносные файлы, и все это – удаленно, в один клик.

Реагирование на инциденты

Пользователи Kaspersky Managed Detection and Response могут использовать агент EDR, чтобы принимать рекомендованные меры реагирования самостоятельно, или предоставить «Лаборатории Касперского» право удаленно осуществлять автоматическое реагирование для тех или иных типов инцидентов.

Возможности

Защита

- Круглосуточный проактивный поиск угроз и расследование
- Мгновенные оповещения об инцидентах
- Ретроспективный анализ инцидентов
- Автоматизированное и управляемое реагирование на инциденты
- Прозрачность активов и проверка работоспособности системы
- Хранение истории инцидентов безопасности в течение 1 года
- Хранение необработанных данных в течение 1-3 мес.

Реагирование

Агент EDR поддерживает следующие сценарии реагирования[1]:

- Изоляция хоста
- Помещение файлов на карантин
- Удаление файлов
- Завершение процессов
- Запрос файлов с хоста
- Запуск программы на хосте

Портал Kaspersky Managed Detection and Response

- Управление доступом на основе ролей
- Управление ролями пользователей
- Карточки инцидентов:
  - Просмотр
  - Отправка вопросов
  - Закрытие инцидентов
  - Рекомендации по реагированию
- Фильтрация по типу инцидента
- Уведомления
- Карточки защищаемых ресурсов
- Отчетность
- Список всех предложенных мер реагирования

Коммуникации

- Уведомления портала
- Мгновенный обмен сообщениями
- Электронная почта

1 Сценарии удаленного автоматического реагирования по предварительной авторизации будут доступны в I кв. 2021 г

Управление

Единая консоль управления Kaspersky Security Center предоставляет следующие возможности:

- Статус обновлений и график их установки:
  - Версия продукта / агента EDR / антивирусной базы
  - Управление графиком обновлений и обновление вручную
- Проверка статуса агента EDR:
  - Хосты, на которых установлены или отсутствуют агенты
  - Хосты, на которых есть проблемы с агентами
  - Хосты, на которых включена или отключена защита Kaspersky Managed Detection and Response
  - Хосты под защитой Kaspersky Managed Detection and Response, которые не отправляют «Лаборатории Касперского» данные телеметрии
- Управление агентом/защитой
  - Установка агента EDR
  - Активация защиты Kaspersky Managed Detection and Response
  - Выбор места для хранения данных

Интеграция

- Портал Kaspersky Managed Detection and Response использует API на основе REST, обеспечивающий загрузку данных для интеграции с существующими ИБ-процессами.

Масштабирование

- Решение предлагает быстрое развертывание и позволяет легко масштабировать защиту, динамически наращивая количество защищаемых активов.

Расположение ЦОД

- AWS в Ирландии, клиентская часть Kaspersky Security Network в Швейцарии
- Москва, Россия

Поддерживаемые операционные системы

- Windows
- Linux
- MacOS[2]

Поддерживаемые версии продуктов

- Kaspersky Endpoint Security для бизнеса для Windows v11.4+ с полной поддержкой: телеметрия и реагирование
- Kaspersky Endpoint Security для бизнеса для Windows v10 SP1 с ограниченной поддержкой: только телеметрия
- Kaspersky Endpoint Security для бизнеса для Mac[3]
- Kaspersky Security для Windows Server v10+
- Kaspersky Endpoint Security для бизнеса для Linux v11 SP1 +
- Kaspersky Anti Targeted Attack / Kaspersky Endpoint Detection and Response 3.7[4]

2 Поддержка планируется на начало 2021 г.

3 Поддержка планируется на начало 2021 г.

4 Поддержка планируется на сентябрь 2020 г.

www.kaspersky.ru

kaspersky АКТИВИРУЙ БУДУЩЕЕ