Правда или вымысел? 5 самых распространенных мифов об MDR

К 2025 году объем рынка решений управляемого обнаружения угроз и реагирования на инциденты (Managed Detection and Response, MDR) превысит 2 млрд долларов, что более чем в 2 раза превышает показатели 2021 года. MDR-решения помогают бизнесу делегировать внешним специалистам различные критически важные задачи по идентификации угроз и реагированию на них. Этот продукт не просто так заслужил столько внимания: у него много преимуществ. Однако вокруг MDR также появилось несколько популярных мифов, которые пришла пора развеять.

Миф № 1

MDR – это такой же управляемый сервис безопасности, как и все остальные

Миф

MDR ничем не отличается от других управляемых сервисов безопасности (MSS). Вы точно так же передаете управление своей IT-инфраструктурой сторонней организации.

Реальность

Как правило, поставщики MSS оказывают ряд базовых услуг в сфере кибербезопасности, например выполняют оценку соответствия требованиям, настраивают VPN-соединение и сетевые экраны или проводят консультации. MDR – это сервис с упором на эффективное обнаружение и быстрое реагирование на новые, неизвестные и скрытые угрозы, способные обходить автоматизированную защиту рабочих мест. Для этого используются технологии активного поиска угроз на базе информации о тактиках, методах и процедурах, которыми пользуются злоумышленники.

Миф № 2

MDR подходит только крупным компаниям

Миф

В MDR используются сложные технологии активного поиска угроз и обнаружения по индикаторам атаки (IoA) – сервис предназначен только для крупных инфраструктур.

Реальность

MDR – это не универсальное решение. Однако оно может расширить возможности любой компании. Например, компаниям, которые испытывают недостаток ресурсов в области ИБ, MDR-решение поможет быстро укрепить безопасность IT-инфраструктуры и защититься от сложных угроз. Предприятия со зрелым подходом к безопасности смогут передать задачи по приоритизации и расследованию инцидентов внешним экспертам, разгрузив своих ИБ-специалистов и позволив им сосредоточиться на других важных задачах.

Миф № 3

MDR на базе ИИ-технологий не требует вмешательства человека

Миф

Искусственный интеллект (ИИ) и машинное обучение достигли такого уровня развития, что MDR скоро сможет работать без вмешательства человека.

Реальность

ИИ, машинное обучение и проприетарные индикаторы атаки позволяют обрабатывать в среднем 30–40% оповещений автоматически, в том числе автоматически приоритизировать инциденты. Это существенно увеличивает пропускную способность сервиса и максимально сокращает среднее время обнаружения и реагирования, обеспечивая непрерывную защиту даже от новейших угроз, не использующих вредоносное ПО. Но в случаях, когда злоумышленник использует неизвестные ранее методы, которые невозможно обнаружить с помощью автоматизированных инструментов, управляемый активный поиск угроз предполагает кропотливую ручную работу опытных экспертов, которые проактивно ищут угрозы и анализируют их.

Миф № 4

MDR стоит дорого, а внедрить это решение сложно

Миф

MDR часто позиционируется как решение, обеспечивающее круглосуточную защиту на уровне центра мониторинга и реагирования (SOC). Наверняка оно очень сложное и дорогое решение.

Реальность

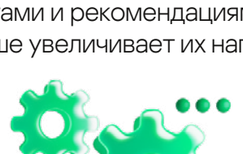
Развенчивая миф № 2, мы отметили, что MDR может служить разным целям – от блокирования сложных угроз, способных обойти корпоративную систему защиты, до высвобождения времени ИБ-специалистов, которое они смогут уделять более важным задачам. Сразу же после внедрения решения (что не потребует много усилий) компания сможет существенно сократить среднее время обнаружения угроз и реагирования на них. А чем раньше определена и заблокирована атака, тем меньше пострадают бизнес-процессы и тем меньше будут убытки. MDR-решения также помогают исключить капитальные затраты и не требуют приобретения дополнительного оборудования. Это гораздо дешевле, чем развернуть собственный SOC.

Миф № 5

MDR не поможет разгрузить специалистов

Миф

Функции MDR ограничиваются расследованием инцидентов. После завершения расследования IT-специалистам клиента приходится разбираться с техническими отчетами и рекомендациями, что еще больше увеличивает их нагрузку.



Реальность

Раньше все действительно так и было. Но сейчас вы можете делегировать поставщику MDR-решения автоматическое реагирование на инциденты от вашего имени. Он будет самостоятельно принимать рекомендованные меры реагирования (например, изолировать хост, отправить файлы на карантин или удалить их, завершить процессы, запросить файлы с хоста или запустить программу на хосте, выполнить поиск индикаторов компрометации и т. д.) либо будет следовать управляемым сценариям восстановления, которые можно согласовать заранее или утверждать вручную при обработке каждого оповещения.

О решении Kaspersky MDR

Kaspersky Managed Detection and Response – это полностью управляемая защита от растущего числа угроз, способных обходить системы автоматизированного обнаружения и реагирования. Это решение позволяет компаниям сразу же развернуть зрелые функции IT-безопасности и разгрузить собственные ресурсы за счет быстрой приоритизации оповещений, классификации, проверки и эскалации инцидентов, отсутствия ложных срабатываний, а также за счет использования протоколов автоматизированного, полуавтоматизированного реагирования и реагирования по инструкциям.
Kaspersky MDR Optimum входит в уровень Kaspersky Optimum Security.

Подробнее о Kaspersky Optimum Security

Узнать больше о Kaspersky MDR

kaspersky