Malwarebytes

ОБЗОР РЕШЕНИЯ

Malwarebytes Incident Response

Комплексная всеобъемлющая защита, которой доверяют во всем мире

КЛЮЧЕВЫЕ ПРЕИМУЩЕСТВА

- В автоматическом режиме точно и тщательно устраняет последствия атаки
- Объединяет разрозненные технологии защиты в единую инфраструктуру
- Сокращает время обнаружения вредоносного ПО на компьютере
- Решает проблему нехватки кадров и восполняет недостатки квалификации специалистов
- Снижает стоимость и трудоемкость устранения последствий атак

НАГРАДЫ

Forbes — Самая многообещающая компания США

CRN — Продукт года

V3 — Инновация года в области безопасности

Количество киберугроз, с которыми сталкиваются группы реагирования на инциденты в области компьютерной безопасности (CIRT), неуклонно растет, множатся типы компьютерных вирусов, а значит – увеличивается стоимость и трудоемкость устранения последствий атак.

Более чем в 60 % случаев на устранение последствий атаки организациям требуется более девяти часов.[1] Поэтому сегодня, будучи ограниченными в ресурсах и находясь под постоянным прессингом со стороны совершенных угроз, организации сталкиваются с необходимостью сменить приоритеты и перейти от реактивных действий к использованию автоматизированных средств нейтрализации атак.

Malwarebytes Incident Response – это именно то решение, которое способно создать для Вас надежную всеобъемлющую защиту и оптимизировать эффективность реагирования на инциденты. Работая в автоматическом режиме, оно укрепляет безопасность Вашей системы и объединяет разрозненные технологии защиты в единую инфраструктуру.

Основные функции

Автоматическая нейтрализация угроз

Благодаря технологии автоматической нейтрализации угроз Ваша группа реагирования на инциденты в области компьютерной безопасности (CIRT) уже не должна в каждом отдельном случае вручную выполнять очистку и восстановление пользовательских устройств после заражения вредоносным ПО, что экономит время и высвобождает столь ценные ресурсы. Автоматическое выполнение задач осуществляется быстрее и с большей точностью – в результате сокращается время от проникновения угрозы на компьютер до ее обнаружения и блокировки.

Всеобъемлющая защита

Большинство решений нейтрализуют только активные компоненты вредоносного ПО, однако не удаляют из системы все его следы. Malwarebytes Linking Engine использует специальный метод поиска, позволяющий выявлять и удалять динамические компоненты и другие артефакты. Затем ядро программы выполняет виртуализацию, чтобы окончательно удалить механизмы устойчивости вредоносного ПО и исключить возможность повторного заражения. Мы создали совершенную технологию противодействия атакам вредоносного ПО, которая предоставляет организациям превосходное средство выявления и тщательного удаления угроз.

Совершенная телеметрия

Обширные сведения о киберугрозах позволяют нам безошибочно идентифицировать «плохие данные» и выявлять атаки, в результате которых злоумышленникам удается выполнить программный код на корпоративных устройствах. Используя мощные системы анализа данных и специальные исследовательские методы, мы ежедневно обрабатываем более 3 миллионов операций по нейтрализации вредоносных объектов на компьютерах в корпоративных сетях. Благодаря полученным данным телеметрии мы больше узнаем о вредоносном ПО нулевого дня и продолжаем совершенствовать свою технологию, стремясь более оперативно реагировать на новейшие угрозы и предугадывать пути распространения вредоносного ПО в будущем.

Проактивный поиск

Возможно, некоторые угрозы уже проникли в Вашу корпоративную среду. Заразив один компьютер, злоумышленники часто инициируют экстенсивное распространение вируса, чтобы проникнуть и на другие компьютеры в сети. Благодаря Malwarebytes специалисты по реагированию на компьютерные инциденты получили эффективное средство противодействия вирусам: в ходе запланированных проверок наше программное решение проактивно действует в отношении недавно зарегистрированных индикаторов компрометации (IOC). Этот метод поиска направлен на выявление подозрительных объектов, которые могли быть скомпрометированы вирусом, что значительно повышает безопасность корпоративной среды.

Гибкая установка и широкие возможности интеграции

Malwarebytes дает возможность осуществлять установку именно так, как нужно Вам: для компьютеров в сети Вы можете выбрать постоянный облачный агент или непостоянный агент (Breach Remediation). Непостоянный агент существенно упрощает интеграцию с существующей инфраструктурой SIEM и системой управления компьютерами в сети. Наше решение может в реальном времени предпринимать необходимые действия в отношении индикаторов компрометации (IOC), обнаруженных системой SIEM. Например, Malwarebytes может оперативно отреагировать на инцидент, предупреждение о котором выдал продукт Splunk или ForeScout.

Веб-ресурсы

С дополнительной информацией о продукте Malwarebytes Incident Response Вы можете ознакомиться на веб-странице: malwarebytes.com/business/incidentresponse/

Последние новости: blog.malwarebytes.com/

Чтобы запросить ознакомительную версию, пожалуйста, посетите веб-страницу: malwarebytes.com/business/licensing

Источник

[1] *Распространение программ-вымогателей в мире: важность и глубина проблемы*, Osterman Research

Santa Clara, CA | malwarebytes.com | corporate-sales@malwarebytes.com | 1.800.520.2796

Компания Malwarebytes предлагает новые технологии киберзащиты, которым доверяют миллионы пользователей во всем мире. Malwarebytes проактивно защищает частных пользователей и целые компании от опасных угроз, в числе которых вредоносное ПО, программы-вымогатели и эксплойты, постоянно ускользающие от обычных антивирусных средств. Флагманский продукт компании сочетает в себе совершенные средства эвристического анализа и бессигнатурные технологии выявления угроз, что позволяет блокировать кибератаку до того, как системе будет нанесен ущерб. Продуктами Malwarebytes пользуются более 10 000 компаний по всему миру – они доверяют нашим программам и рекомендуют их всем пользователям. Компания Malwarebytes была основана в 2008 году, ее главный офис расположен в Калифорнии. На сегодняшний день компания располагает не только рядом представительств в Европе и Азии, но и международной командой профессионалов, в которую входят исследователи киберугроз и специалисты в области компьютерной безопасности.