Malwarebytes Breach Remediation

Расширенный алгоритм удаления угроз

ТЕХНИЧЕСКИЕ ХАРАКТЕРИСТИКИ

- Расширенный алгоритм удаления вредоносного ПО и проверки на наличие руткитов
- Ядро интеллектуального эвристического анализа и поиска на основе сигнатур вирусов
- Автоматическое удаленное выявление и нейтрализация вредоносного ПО
- Представление опасных событий в виде временной шкалы
- Настраиваемые индикаторы угроз OpenIOC (формат XML)
- Четыре типа проверки системы (полная проверка, проверка на наличие угроз, быстрая проверка, проверка по указанному пути)
- Выбор нужного режима: поиск и устранение угроз или только поиск
- Помещение обнаруженных угроз на карантин
- Ведение журнала событий и его сохранение в централизованной базе данных (формат CEF)
- Без продолжительного использования дискового пространства компьютера в сети
- Специальное ядро поиска вредоносного и рекламного ПО на компьютерах Mac
- Расширенный набор средств предоставляет множество вариантов установки

В настоящее время традиционные средства обнаружения угроз только мешают нормальной работе специалистов по реагированию на компьютерные инциденты, поскольку ежедневно генерируют тысячи уведомлений об атаках, но не могут ни полностью удалить вредоносное ПО, ни предотвратить его повторное появление или распространение по сети. Используемый в таких программах подход является реактивным, поскольку пользователь вынужден самостоятельно искать ту или иную угрозу, в результате чего проникшие в систему вредоносные объекты остаются незамеченными в среднем от 205 до 229 дней*. Когда вредоносное ПО наконец обнаружено на ноутбуке или сервере, IT-администратору может потребоваться до шести часов рабочего времени, чтобы переустановить из образа систему каждого зараженного компьютера.

Malwarebytes Breach Remediation – это совершенная утилита нового поколения, призванная выявлять и устранять угрозы на компьютерах в сети предприятий малого, среднего и крупного бизнеса. Malwarebytes Breach Remediation обеспечивает проактивную защиту предприятий от вредоносного ПО и устраняет проблемы в удаленном режиме, так что специалистам уже не приходится идти к зараженному компьютеру и переустанавливать его систему из образа. Это полностью самодостаточная утилита, которая легко интегрируется с уже установленными средствами обеспечения кибербезопасности предприятий и инструментами управления. Malwarebytes Breach Remediation обладает уникальной способностью одновременно обнаруживать и устранять вредоносное ПО, что значительно снижает вероятность возникновения устойчивых угроз.

Ключевые преимущества

Полностью нейтрализует вредоносное ПО

Программа удаляет все следы вирусов и связанных с ними артефактов, не ограничиваясь основной вредоносной нагрузкой или телом вируса. Это решение позволяет исключить риск распространения угроз или новых атак, которые используют следы, оставшиеся после прежних вредоносных объектов. Malwarebytes является лидером в области борьбы с вредоносным ПО, что подтверждается доверием миллионов пользователей и результатами независимой оценки, проведенной организацией AV-Test.org.

Существенно сокращает время простоя

Данное программное решение позволит Вам сконцентрироваться на реализации прибыльных проектов, а не тратить бесконечные часы, вручную устраняя ущерб от атак вредоносного ПО и переустанавливая из образа систему каждого зараженного компьютера на предприятии.

** По материалам доклада Питера Ферстбрука «О защите компьютеров в сети от систематических атак», представленного на конференции «Gartner Security & Risk Management Summit» (8–11 июня 2015 г.).*

По результатам исследования института Ponemon Institute 2016 года «Оценка стоимости утечки информации» (июнь 2016 г.).

Работает проактивно, а не реактивно

Использует средство автоматической нейтрализации угроз, которое обеспечивает проактивную защиту и одновременно устраняет возможные проблемы. Принцип работы этой программы похож на систему предупреждения пожара, в которой спринклеры тушат небольшие возгорания, не давая им разрастись и выйти из-под контроля. Проблема будет решена, Вы станете героем дня и забудете о том, как Вам каждый день досаждали тысячи уведомлений об атаках.

Эффективно обнаруживает вредоносное ПО

Данное решение обнаруживает новые, еще не изученные угрозы и вредоносные объекты и оперативно нейтрализует их. Оно изучает поведение приложений и проводит эвристический анализ на основе технологий Malwarebytes, а также использует индикаторы компрометации (IOC) сторонних средств обнаружения и архивов данных.

Регистрирует опасные события

Программа осуществляет анализ опасных событий с помощью запатентованной функции Forensic Timeliner, которая позволяет Вашей команде своевременно устранять бреши в защите и реагировать на небезопасное поведение пользователей. Кроме того, она собирает информацию о системных событиях, которые происходили до и во время попытки заражения компьютера вирусом, а затем представляет эти данные в виде удобной временной шкалы, помогая Вам определить направление и алгоритм вирусной атаки. В числе регистрируемых событий – модификации файлов и реестра, выполнение файлов и посещение веб-сайтов.

Улучшает эффективность установленных антивирусных средств

Предлагаемое решение легко взаимодействует с существующими инструментами управления событиями и информационной безопасностью (Splunk, ArcSight, QRadar и др.), с системами обнаружения угроз (Lastline, Mandiant, Fidelis и др.), а также с платформами управления компьютерами в сети (Tanium, ForeScout, Microsoft SCCM и др.). Данная особенность позволяет Вам устанавливать и активировать средства защиты с помощью платформы управления компьютерами в сети, основываясь на сообщениях системы SIEM, а также автоматически загружать в систему SIEM данные о решении соответствующих проблем.

Закрывает брешь в защите компьютеров Apple

Программа быстро удаляет вредоносное и рекламное ПО с сетевых компьютеров Mac. Чтобы выполнить очистку системы OS X, Вам потребуется менее минуты. Раздельные решения, основанные на графическом интерфейсе пользователя и интерфейсе командной строки, предоставляют множество вариантов установки с помощью популярных систем управления компьютерами Mac (например, Apple Remote Desktop, Casper Suite, Munki и др.). В данной программе также предусмотрена возможность удаленной автоматизированной работы посредством команд оболочки или команд сценария AppleScript. Системные администраторы и специалисты по реагированию на компьютерные инциденты могут собирать информацию о системе с помощью удобной команды Snapshot.

СИСТЕМНЫЕ ТРЕБОВАНИЯ

Чтобы ознакомиться со всеми техническими характеристиками и системными требованиями, пожалуйста, посетите веб-страницу malwarebytes.com/business/breachremediation.

Компоненты:
Программа Windows CLI
Программа Windows Forensic Timeliner
Программа Mac GUI
Программа Mac CLI

Компьютеры в сети
Поддерживаемые операционные системы:
Windows 10, 8.1, 8, 7, Vista, XP
Windows Server 2012, 2008, 2003
Mac OS X (10.8 и более поздних версий)

malwarebytes.com/business corporate-sales@malwarebytes.com 1 800 520 2796

Malwarebytes защищает частных пользователей и целые компании от опасных угроз, в числе которых вредоносное ПО, программы-вымогатели и эксплойты, постоянно ускользающие от обычных антивирусных средств. Malwarebytes Anti-Malware, флагманский продукт компании, обладает совершенным ядром эвристического поиска, благодаря которому с компьютеров пользователей во всем мире было удалено уже более пяти миллиардов вредоносных объектов. Более 10 000 предприятий малого, среднего и крупного бизнеса в различных регионах мира доверяют Malwarebytes защиту своих данных. Компания ведет свою историю с 2008 года, ее главный офис расположен в Калифорнии. На сегодняшний день она располагает не только рядом представительств в Европе, но и международной командой исследователей и специалистов.