

McAfee Global Threat Intelligence for Enterprise Security Manager

Обеспечение ситуационной осведомленности с помощью ресурсов McAfee® Labs

McAfee® Global Threat Intelligence for Enterprise Security Manager позволяет воспользоваться ресурсами McAfee Labs для обеспечения мониторинга корпоративных систем безопасности. Благодаря выпуску этого продукта впервые появилась возможность использовать в системе управления информацией о безопасности и событиями безопасности (SIEM) данные о репутации IP-адресов, поступающие от расположенных по всему миру датчиков, общее число которых превышает 100 миллионов. Использование McAfee Enterprise Security Manager в сочетании с этим постоянно обновляемым каналом, поставляющим подробные сведения об угрозах, ведет к повышению уровня ситуационной осведомленности, поскольку дает возможность быстро обнаруживать события, в рамках которых происходит обмен данными с подозрительными или вредоносными IP-адресами. Благодаря этому администраторы безопасности могут определять, какие узлы обменивались или в настоящее время обмениваются данными с источниками риска, и быстро выявлять условия, при которых угроза исходила от известного источника риска.

Потребность во внешнем контексте

События безопасности несут в себе информацию о важной с точки зрения безопасности активности на тот или иной момент времени. И хотя SIEM может сопоставлять эти события, у оператора все равно остается ряд нерешенных вопросов: Приемлема ли данная активность? Как мне понять, что требует первостепенного внимания? Как обнаруживать

изоциранные атаки, которые не создают много шума? Умножьте количество этих вопросов на количество ежедневных событий в обычной крупной компании — более четверти миллиарда — и вы поймете, что при проведении мониторинга безопасности задача обнаружения известных шаблонов, которой уделяли основное внимание прежние решения SIEM, является лишь верхушкой

Ключевые преимущества

- Доступ к ресурсам McAfee Labs из системы SIEM.
- Точный анализ риска, связанного с событиями.
- Использование объемного канала данных McAfee GTI для получения информации об угрозах без снижения быстродействия.
- Автоматическое получение и обработка новых сведений о репутации источников в McAfee Enterprise Security Manager.
- Более точно распознавайте угрозы, одновременно сокращая время реагирования.

айсберга. Одним из важнейших контекстуальных элементов, необходимых для ответа на эти вопросы, является информация о репутации внешних систем. До сих пор получить такое четкое представление о событиях безопасности было невозможно.

Прямой доступ к ресурсам McAfee Labs из системы SIEM

Технология McAfee Global Threat Intelligence for Enterprise Security Manager, предназначенная для работы с большими объемами данных безопасности, позволяет использовать результаты работы McAfee Labs непосредственно для мониторинга безопасности с помощью высокоскоростной и высокоинтеллектуальной системы управления информацией о безопасности и событиями безопасности (SIEM), разработанной McAfee. Этот сервис (требующий дополнительной подписки) непрерывно предоставляет и корректирует информацию о репутации источников для более чем 140 млн IP-адресов, что позволяет использовать репутационный контекст внешних систем непосредственно в работе с потоком событий безопасности и тем самым быстро выявлять случаи взаимодействия с известными источниками риска в прошлом и в настоящем. Информация о репутации IP-адресов, поступающая из McAfee Global Threat Intelligence (GTI), создается путем сопоставления данных об угрозах по всем основным векторам. Эти данные собираются с более чем 100 миллионов датчиков по всему миру и анализируются более чем 500 специалистами.

Преимущества McAfee Global Threat Intelligence for Enterprise Security Manager

- **Повышенный уровень защиты для всей сети.** Благодаря McAfee Global Threat Intelligence for Enterprise Security Manager вы сможете мгновенно выявлять случаи взаимодействия любого узла вашей сети с предполагаемыми или известными источниками риска и быстро определять путь распространения угрозы.
- **Приоритизация на основе риска.** Информация о репутации IP-адресов автоматически встраивается в используемый в McAfee Enterprise Security Manager алгоритм количественной оценки риска без использования правил, позволяя точно определять, где необходимо вмешательство.
- **Непрерывный мониторинг угроз.** McAfee Labs непрерывно анализирует информацию об угрозах с целью обнаружения недавно зараженных и вредоносных систем и (после полного удаления вирусов из этих систем) предоставляет организациям точные и актуальные сведения о глобальной ситуации с угрозами безопасности.

Точное обнаружение вредоносных действий в режиме реального времени

Благодаря McAfee Global Threat Intelligence for Enterprise Security Manager у организаций теперь есть возможность получать сведения о репутации IP-адресов для любого события, которое фиксируется различными брандмауэрами, системами предотвращения вторжений, маршрутизаторами

Ключевые преимущества (продолжение)

- Быстрое выявление путей атак и прошлых случаев взаимодействия с известными источниками риска, связанными с бот-сетями и атаками типа «распределенный отказ в обслуживании» (DDoS), с вредоносными программами для рассылки электронной почты и спама, с серверами, на которых размещены программы для зондирования сети, с присутствием вредоносных программ, с DNS-хостингом и активностью, порождаемой вторжениями злоумышленников.

или конечными точками. Имеющаяся в McAfee Enterprise Security Manager функция динамических списков наблюдения позволяет автоматически связывать события с оценкой репутации источника и корректировать риск. При изменении характера глобальных угроз безопасности McAfee GTI снабжает McAfee Enterprise Security Manager актуальной информацией, благодаря которой присвоенные серверам и системам оценки репутации являются неизменно точными. Эта функция помогает организациям не только получать картину рисков, но и в режиме реального времени выявлять неотложные проблемы, тем самым сокращая временной интервал, необходимый для реагирования на инциденты, а также обеспечивает точный анализ рисков.

Обнаружение неизвестного

Основным преимуществом McAfee Enterprise Security Manager является наличие архива, позволяющего сохранять, извлекать и сопоставлять данные за много лет. Благодаря McAfee GTI теперь у аналитиков безопасности есть возможность обращаться к накопленным за многие годы объемам данных и анализировать прошлые случаи взаимодействия с источниками риска. Это имеет критически важное значение с точки зрения обнаружения «медленных и незаметных» атак, повторной активности бот-сетей, атак с использованием межсайтовых сценариев и попыток внедрения SQL-кода.

Сокращение времени реагирования

Служба McAfee GTI напрямую интегрирована с используемыми в McAfee Enterprise Security Manager механизмами рассылки предупреждений и оповещений: это дает возможность не оставлять без должного внимания случаи взаимодействия с известными вредоносными системами.

Доступ к базе данных McAfee, работа с большими объемами данных безопасности

Как известно, объемы обрабатываемой информации постоянно растут. Растет и объем базы знаний McAfee Labs, доступный теперь через системы SIEM. McAfee Enterprise Security Manager обладает уникальной способностью хранить, сопоставлять и обновлять предоставляемые службой McAfee GTI данные о репутации IP-адресов, не снижая при этом быстродействие систем до неприемлемого уровня. McAfee Enterprise Security Manager имеет проприетарную базу данных, которая позволяет не только отказаться от трудоемкого администрирования баз данных для SIEM, но и принимать и обрабатывать огромное количество событий и реляционных данных на чрезвычайно высоких скоростях. Благодаря McAfee Global Threat Intelligence for Enterprise Security Manager клиенты могут быть уверены в том, что информация McAfee GTI будет поступать в режиме реального времени.

Спецификации

Поддерживаемые версии

McAfee Enterprise Security Manager 9.4 и McAfee Event Reporter Appliance 9.4

- Сеть McAfee Labs для сбора информации об угрозах: более 100 миллионов узлов в более чем 120 странах
- Среднее количество сведений о репутации IP-адресов: зависит от картины угроз



McAfee Ireland Ltd.
Building 2000, City Gate
Mahon, Cork, Ireland
www.mcafee.com/ru

McAfee и логотип McAfee являются товарными знаками или зарегистрированными товарными знаками компании McAfee, LLC или ее филиалов в США и других странах. Другие названия и фирменная символика являются собственностью соответствующих владельцев.
Copyright © 2017 McAfee, LLC. 61318_0914
Сентябрь 2014 г.