McAfee Threat Intelligence Exchange

Обмен информацией об угрозах между разными защитными решениями

McAfee® Threat Intelligence Exchange действует в качестве агента по оценке репутации, позволяя использовать адаптивные механизмы обнаружения угроз и реагирования на них. Решение сводит воедино локальную информацию, получаемую от установленных в вашей организации средств защиты, с глобальной информацией об угрозах и мгновенно рассылает такие объединенные данные во все точки вашей комплексной экосистемы безопасности, давая всем защитным решениям возможность действовать на базе общей информации.

Создание экосистемы сбора данных об угрозах, построенной на взаимодействии

Агент по оценке репутации McAfee Threat Intelligence Exchange комбинирует информацию об угрозах, импортируемую из глобальных источников, таких как McAfee Global Threat Intelligence (McAfee GTI) и сторонних источников (таких как VirusTotal) с информацией, получаемой из локальных источников, включая конечные точки, шлюзы и решения для анализа угроз повышенной сложности. Используя уровень обмена данными Data Exchange Layer (DXL), он мгновенно рассылает эти объединенные данные во все точки вашей комплексной экосистемы безопасности, позволяя защитным решениям действовать как единое целое для обеспечения надежной защиты в масштабе всей организации.

Простая интеграция, полученная за счет использования уровня обмена данными DXL позволяет существенно сократить расходы на развертывание и эксплуатацию многочисленных интегрированных интерфейсов прикладного программирования (API) и обеспечивает наивысший уровень безопасности, оперативности и эффективности. Уровень обмена данными DXL представляет собой открытый стандарт, дающий всем защитным решениям (в том числе продуктам сторонних производителей) возможность динамически подключаться к экосистеме McAfee Threat Intelligence Exchange.

Ключевые преимущества

- Система адаптивной защиты от угроз сокращает период между обнаружением сложной направленной атаки и ее нейтрализацией с нескольких дней, недель или месяцев до миллисекунд.
- Коллективная информация об угрозах составляется на основе данных, полученных из глобальных источников, которые дополняются локальными данными об угрозах.
- Обмен важной информацией об угрозах между решениями для защиты конечных точек, шлюзов, сетей и центров обработки данных осуществляется в режиме реального времени.
- Вы получаете возможность принимать решения по ранее не встречавшимся файлам на основе контекстных характеристик конечных точек (атрибутов файла, процесса и среды выполнения), дополненных коллективно собираемой информацией об угрозах.

Адаптация к новым угрозам и создание механизмов устойчивости против них

Все сведения, собираемые во всех точках сети организации и рассылаемые на все используемые в организации средства защиты, ведут к повышению уровня осведомленности организации в борьбе с целенаправленными атаками. Поскольку такие угрозы по определению являются узконаправленными, требуется локальная система наблюдения, позволяющая фиксировать тенденции и учитывать все уникальные атаки, с которыми сталкиваются организации. Такие локальные контекстные данные, собираемые при столкновениях с атаками и дополненные глобальными данными об угрозах, дают возможность принимать более точные решения по ранее не встречавшимся файлам, что ведет к повышению скорости обеспечения защиты и обнаружения угроз.

В случае обнаружения неопознанного файла в любой точке вашей сети, в McAfee Threat Intelligence Exchange поступает обращение за информацией о репутации этого файла. Описательные метаданные, такие как масштаб распространения в рамках организации и возраст, также сохраняются и отражаются в объединенных информационных данных. Кроме направления запросов о репутации интегрированные защитные решения также могут вносить обновления по репутации файлов в McAfee Threat Intelligence Exchange на основании локальных решений о признании их вредоносными. Затем обновленные данные о репутациях рассылаются на все ваши системы в режиме реального времени.

Полученная таким образом локальная информация об угрозах сохраняется на будущее, т. е. в случае повторного обнаружения этого файла на другом устройстве или сервере он больше не будет помечен как неизвестный, а будет немедленно распознан.

McAfee Threat Intelligence Exchange позволяет администраторам легко настраивать систему сбора информации об угрозах. Администраторы систем безопасности могут создавать, аннулировать, дорабатывать и настраивать элементы комплексной информации об угрозах в соответствии с индивидуальными потребностями защиты своей среды и организации. Наличие такой локально приоритизированной и скорректированной информации об угрозах обеспечивает мгновенное реагирование на любые будущие инциденты.

Укрепленные конечные точки усиливают защиту

Интегрированные решения, охватывающие всю сеть — от конечных точек до периферии сети, — применяются на основе политик с учетом имеющейся информации о репутации и метаданных или же на основе комбинации информационных точек. Единое глубоко интегрированное решение — McAfee Endpoint Security — выполняет тщательных анализ комплекса локальной информации (метаданных файла, таких как масштаб распространения в масштабе организации и возраст, в сочетании с локальной информацией о репутации, полученной от других компонентов системы безопасности) и доступной на текущий момент глобальной информации

Ключевые преимущества (продолжение)

- Простая интеграция благодаря уровню обмена данными DXL: объединение решений McAfee и других поставщиков в единую систему, позволяющую в режиме реального времени принимать меры на основе информации об угрозах, дает возможность сократить расходы на внедрение и эксплуатацию защитных решений.

для принятия точных решений. Например, пользовательское приложение, не имеющее глобальной репутации, но распространенное в организации не вызовет формирования сводной репутации вредоносной угрозы и, скорее всего, не будет заблокировано. С другой стороны, файл, еще не разу не встречавшийся в организации, не имеющий ни глобальной, ни локальной репутации, к тому же подозрительно упакованный скорее всего, получит низкий уровень доверия и, возможно, будет блокирован или потребует дальнейшего расследования с помощью других механизмов McAfee Endpoint Security или анализа «в песочнице» с помощью McAfee Advanced Threat Defense или McAfee Cloud Threat Detection.

Real Protect, технология машинного обучения McAfee Endpoint Security, и функция динамического сдерживания приложений улучшают процессы обнаружения и защиты конечных точек. Real Protect выполняет поиск актуальной информации об угрозах в облаке и анализ до и после выполнения вредоносной программы, в то время как функция динамического сдерживания приложений предотвращает вредоносную активность на конечной точке, защищая первую машину, подвергшуюся новой угрозе, в то время как выполняется дополнительный анализ.

Преимущества совместной работы

Расширенный анализ угроз

Если требуется больше информации о файле, McAfee Threat Intelligence Exchange может автоматически направлять соответствующий запрос решениям McAfee для анализа угроз повышенной сложности — таким как McAfee Advanced Threat Defense или McAfee Cloud Threat Detection, — чтобы незамедлительно получить дополнительные данные о потенциальных новых угрозах и определить репутацию рассматриваемого файла. Весь процесс автоматизирован, а полученные данные протоколируются и пересылаются через уровень обмена данными DXL на все другие средства защиты в экосистеме безопасности организации.

Управление событиями безопасности

McAfee Enterprise Security Manager позволяет вам выполнять углубленный анализ признаков взлома, выявленных с помощью McAfee Threat Intelligence Exchange. Доступ к журналам событий безопасности и возможности создавать списки автоматически отслеживаемых действий повышаеют эффективность системы безопасности в организации.

Сложные направленные атаки — это реальная проблема

Сложные целенаправленные атаки, разработанные с целью избежать обнаружения и надолго закрепиться в сети организации, продолжают наносить ущерб организациям и помогают похищать ценнейшие данные. Согласно данным, опубликованным в недавно опубликованном отчете компании Verizon о расследовании утечек данных за 2015 год (2015 Data Breach Investigations Report), от 70 до 90 процентов образцов вредоносных программ являются уникальными, т. е. они были обнаружены только в одной организации. Это свидетельствует о том, что обнаружение признаков уникальных угроз является одной из сложнейших задач сегодняшнего дня.[1]

За дополнительной информацией обращайтесь по адресу **www.mcafee.com/ru/products/threat-intelligence-exchange.aspx**.

1. http://www.verizonenterprise.com/DBIR/2015/

McAfee Together is power.

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