McAfee Threat Intelligence Exchange

Обмен информацией об угрозах для борьбы с целенаправленными атаками

McAfee® Threat Intelligence Exchange — адаптивная система обнаружения угроз и реагирования на них с помощью мер на основе информации, получаемой от всех имеющихся в организации средств защиты конечных точек, шлюзов, сетей и центров обработки данных в режиме реального времени. Благодаря локальному сбору информации об угрозах, дополненному импортированной глобальной информацией, и мгновенной рассылке этой информации на другие защитные решения все компоненты системы безопасности способны действовать согласованно. Решение McAfee Threat Intelligence Exchange позволяет сократить период между обнаружением угрозы и ее нейтрализацией с нескольких дней, недель или месяцев до миллисекунд.

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.
- Предоставляет сборную информацию об угрозах, полученную из глобальных источников данных в сочетании с локальными сведениями об угрозах.
- Моментально оповещает о появлении в вашей организации сложных направленных атак.
- Обмен важной информацией об угрозах между решениями для защиты конечных точек, шлюзов, сетей и центров обработки данных осуществляется в режиме реального времени.

Создание экосистемы сбора данных об угрозах, построенной на взаимодействии

Для обмена данными и создания комплексной системы обеспечения безопасности McAfee Threat Intelligence Exchange использует уровень обмена данными McAfee Data Exchange Layer. Информация об угрозах, получаемая из разных источников, мгновенно рассылается на все связанные между собой защитные решения, в том числе сторонние.

Когда компоненты системы безопасности работают как единое целое, данные об угрозах, необходимые для обнаружения угроз и защиты от них, моментально передаются на все средства защиты, размещенные на конечных точках, на шлюзах, в центрах обработки данных, в облаке и в других точках ИТ-среды, подлежащих защите. Простота интеграции, достигаемая благодаря использованию уровня обмена данными McAfee Data Exchange Layer, позволяет сократить издержки на внедрение и эксплуатацию и обеспечить непревзойденный уровень безопасности и высокую эффективность работы.

Уровень обмена данными McAfee Data Exchange Layer представляет собой открытый стандарт, дающий всем защитным решениям (в том числе продуктам сторонних производителей) возможность динамически подключаться к экосистеме McAfee Threat Intelligence Exchange. Создание такой системы безопасности, в которой все компоненты могут обмениваться друг с другом всей необходимой информацией, снижает совокупную стоимость владения защитными продуктами и дает организации возможность более эффективно использовать имеющиеся у нее защитные продукты и решения.

intel Security

Ключевые преимущества (продолжение)

- Вы получаете возможность принимать решения по ранее не встречавшимся файлам на основании контекстных характеристик конечных точек (атрибутов файла, процесса и среды выполнения), дополненных коллективно собираемой информацией об угрозах.
- Использование уровня обмена данными McAfee Data Exchange Layer упрощает процесс интеграции. Объединение решений Intel Security и других поставщиков в единую систему, позволяющую в режиме реального времени принимать меры на основании информации об угрозах, дает возможность сократить расходы на внедрение и эксплуатацию защитных решений.

Предотвращение угроз с помощью такой взаимодействующей и адаптивной системы представляет собой радикально новый подход к обеспечению информационной безопасности предприятий, поскольку создает эффективную согласованную работу разрозненных систем. Если сотрудники отделов безопасности хотят преодолеть границы между организациями и бюджетные ограничения, то им необходимо иметь возможность автоматически обмениваться информацией об угрозах и в упреждающем режиме применять превентивные политики и средства защиты ко всем точкам сетей.

Преобразуя инфраструктуру безопасности в координированную систему, администраторы системы безопасности получают возможность выявлять угрозы, обмениваться информацией о них и делать свою среду невосприимчивой к этим угрозам. McAfee Threat Intelligence Exchange позволяет существенно повысить отказоустойчивость и уровень осведомленности в борьбе с новыми и направленными атаками.

Адаптация к новым угрозам и создание устойчивости к ним

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 сети организации он направляется в McAfee Threat Intelligence Exchange для проведения локальной оценки. Результаты оценки в режиме реального времени рассылаются на все имеющиеся в организации системы. 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.

Так, например, в случае обнаружения на шлюзе вредоносного файла информация о нем через уровень обмена данными McAfee Data Exchange Layer направляется в McAfee Threat Intelligence Exchange и за несколько миллисекунд доходит до всех конечных точек и центра обработки данных, что дает им возможность вовремя обезопасить себя от этой угрозы. Сведения о попытке атаки на конечную точку и заблокированной при этом вредоносной программе будут мгновенно переданы на шлюзы и другие компоненты системы безопасности, и периметр сети будет защищен от этой угрозы.

Мгновенное принятие мер реагирования на основе информации об угрозах

Теперь у наших клиентов есть возможность комбинировать данные об угрозах, получаемые из импортируемых глобальных источников, таких как McAfee Global Threat Intelligence (McAfee GTI), источники сторонних производителей и признаки взлома (indicators of compromise — IoC), рассылаемые другими организациями, например, в виде файлов в формате STIX (Structured Threat Information eXpression). McAfee Global Threat Intelligence обеспечивает сбор локальных данных за текущий и прошлые периоды, предоставляемых конечными точками, центром обработки данных, шлюзами, сетью организации и «песочницей» McAfee Advanced Threat Defense. Все эти данные об угрозах, собранные из глобальных и локальных источников, служат основой для принятия мер реагирования и в режиме реального времени рассылаются на все компоненты экосистемы безопасности, созданной в организации.

McAfee Threat Intelligence Exchange дает администраторам возможность создать собственную комплексную систему сбора информации об угрозах на основе глобальных источников данных, таких

Сложные направленные атаки — это реальная проблема

Сложные направленные атаки являются актуальной проблемой: они специально разрабатываются для преодоления систем безопасности и нацелены на получение постоянного доступа к особо ценным данным в организации и скрытой пересылки этих данных. Согласно данным, опубликованным в недавно вышедшем 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**.

как McAfee GTI, источники сторонних производителей и импортируемые файлы STIX. Полученная таким образом информация дополняется локальной информацией об угрозах, получаемой в результате анализа данных о текущих и прошлых событиях на конечных точках, шлюзах, в «песочницах» и других компонентах системы безопасности. Администраторы системы безопасности могут дополнять и корректировать собираемую информацию так, как это необходимо для обеспечения защиты их среды и организации (например, при создании черных и белых списков файлов или сертификатов, используемых организацией).

Наличие такой локально приоритизированной и скорректированной информации об угрозах позволяет обеспечить мгновенное реагирование на любые будущие инциденты. Все основные объекты описываются с помощью метаданных, которые включаются в общий объем собираемой информации. Используя собранную информацию, администраторы и системы управления информацией о безопасности и событиями безопасности (SIEM) могут совместными усилиями анализировать прошлые вредоносные действия и мгновенно выявлять системы с высоким уровнем риска.

Передовое средство защиты конечных точек

McAfee Threat Intelligence Exchange обеспечивает передовую защиту конечных точек при помощи модуля VirusScan® Enterprise решения McAfee Threat Intelligence Exchange. Для принятия решений о запрете или разрешении выполнения файла этот модуль использует настраиваемые правила, информацию из контекста конкретной конечной точки (атрибуты файла, процесса и среды выполнения) и имеющуюся совокупную информацию об угрозах на уровне организации (например, распространенность файла в организации, дата его создания и репутация).

При настройке модуля VirusScan Enterprise решения McAfee Threat Intelligence Exchange в соответствии с допустимым уровнем риска для конечных точек администраторы имеют возможность задавать условия выполнения файлов согласно политике организации. Эти условия могут быть жесткими, например полный запрет доступа к неизвестным файлам и файлам в «серой зоне». При этом правила настраиваются таким образом, что в доступе к любому файлу будет отказано, если он не имеет положительной репутации.

Управление конечными точками в любое время и в любом месте

McAfee Threat Intelligence Exchange обеспечивает адаптивную защиту от угроз и возможность управления системой безопасности в любой точке мира. Решение имеет доступ к конечным точкам вне зависимости от их расположения и позволяет управлять политиками обнаружения угроз, принимать решения по обнаруженным угрозам, устанавливать обновления средств защиты и выполнять удаленное расследование инцидентов. Все компоненты системы безопасности работают как единое целое вне зависимости от их физического расположения. Они моментально передают информацию об угрозах конечным точкам, шлюзам и другим элементам системы безопасности вне зависимости от их расположения, формируя тем самым комплекс адаптивного предотвращения угроз.

Другие решения для управления безопасностью не имеют функций моментального обновления политик, содержимого и программного обеспечения на конечных точках. Это создает брешь в защите, как только организации сталкиваются с повышенным уровнем риска. Благодаря использованию McAfee Data Exchange Layer решение McAfee Threat Intelligence Exchange имеет возможность постоянно поддерживать связь с другими компонентами системы несмотря на возможные проблемы в сети. Это позволяет закрыть брешь в системе безопасности и обеспечивает контроль над всеми конечными точками.

Преимущества совместной работы

Запрос репутации одним щелчком мыши
McAfee Threat Intelligence Exchange позволяет легко определить репутацию неизвестного файла, обнаруженного на любом компоненте системы безопасности в организации — на шлюзе, конечной точке или в сети — на основе атрибутов и собранных сведений об угрозах.

Расширенный анализ угроз
При необходимости получить дополнительную информацию о файле он автоматически пересылается из McAfee Threat Intelligence Exchange в McAfee Advanced Threat Defense и мгновенно анализируется на наличие потенциальных новых угроз. Совместное использование этих двух технологий позволяет определять репутацию файла на основе результатов динамического и статического анализа кода. Весь процесс автоматизирован, а полученные данные протоколируются и пересылаются через уровень обмена данными McAfee Data Exchange Layer на все другие средства защиты в экосистеме безопасности организации.

Управление событиями безопасности
Для углубленного анализа признаков взлома, выявляемых с помощью McAfee Threat Intelligence Exchange, используется McAfee Enterprise Security Manager. Наличие доступа к журналам событий безопасности и возможности создавать списки автоматически отслеживаемых действий повышает эффективность системы безопасности в организации.

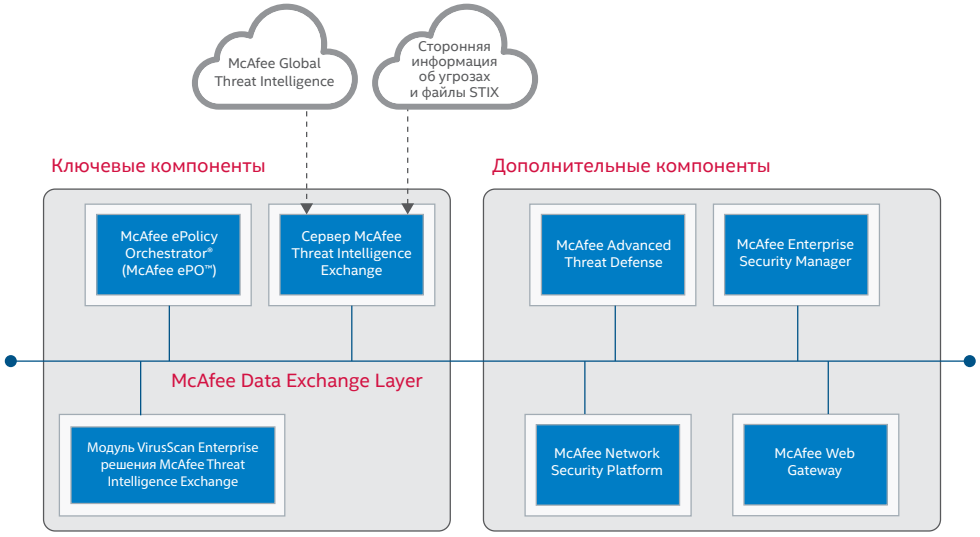

Рис. 1. Простота интеграции через McAfee Data Exchange Layer позволяет сократить издержки на внедрение и эксплуатацию и обеспечить непревзойденную эффективность работы. Это новый этап развития платформы Security Connected.

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

McAfee. Part of Intel Security.
Адрес: Москва, Россия, 123317
Пресненская набережная, 10
БЦ «Башни на набережной»,
Башня «А», 15 этаж
Телефон: +7 (495) 653-85-13
www.intelsecurity.com