McAfee Advanced Correlation Engine

Обнаружение угроз для тех активов, которые для вас важны

Современные изощренные угрозы безопасности не под силу стандартным средствам обнаружения угроз на основе правил. Развернув наряду с McAfee Enterprise Security Manager решение McAfee® Advanced Correlation Engine, вы сможете в режиме реального времени обнаруживать угрожающие вашей безопасности события и присваивать им рейтинги как на основе правил, так и на основе анализа риска. Укажите интересующие вас активы (пользователей или группы пользователей, приложения, конкретные серверы или подсети), и McAfee Advanced Correlation Engine уведомит вас в случае возникновения угрозы для этих активов. Наличие журналов аудита и возможности воспроизведения трафика за прошлые периоды облегчает задачу проведения компьютерно-технических экспертиз, обеспечения нормативно-правового соответствия и настройки правил.

McAfee Advanced Correlation Engine дополняет имеющуюся в McAfee Enterprise Security Manager функцию сопоставления событий двумя отдельными корреляционными модулями, работающими с требуемым уровнем быстродействия:

- модулем для обнаружения риска, генерирующим рейтинг риска на основе сопоставления рейтингов риска без использования правил;
- модулем для обнаружения угроз безопасности, обнаруживающим угрозы безопасности путем традиционного сопоставления событий на основе правил.

Решение McAfee Advanced Correlation Engine развертывается отдельно от других решений и имеет вычислительную мощность, достаточную для выполнения вышеуказанных операций по сопоставлению событий в масштабах всей вашей компании. Используемый в нем модуль обработки данных способен работать даже с самыми крупными сетями.

Обнаружение угроз в режиме реального времени и на основе журнальных данных

Решение McAfee Advanced Correlation Engine может быть развернуто либо в режиме реального времени, либо в журнальном режиме. В режиме

Ключевые преимущества

- Упрощенный запуск: не требуется ни обновления правил, ни настройки сигнатур, ни прочих затратных процедур
- Получение уведомлений в случае возникновения угроз для приоритетных пользователей, активов, приложений и действий
- Точный рейтинг благодаря одновременному сопоставлению событий как на основе правил, так и без использования правил
- Возможность обнаружения событий в прошлом путем сопоставления новых атак и уязвимостей с журнальными данными
- Расширение функциональности McAfee Enterprise Security Manager за счет добавления специализированных ресурсов для сопоставления и обработки событий
- Возможность развертывания как в виде аппаратного устройства, так и в виде виртуальной системы

реального времени McAfee Advanced Correlation Engine выполняет анализ событий по мере их сбора, что позволяет немедленно обнаруживать угрозы и риски.

- Обнаружение угроз по мере их появления путем сопоставления поступающих в реальном времени данных о событиях — на основе правил
- Обнаружение угроз по мере их развития путем сопоставления поступающих в реальном времени данных о событиях — без использования правил

В журнальном режиме любые собранные данные можно «воспроизвести» с помощью обоих корреляционных модулей, что позволяет обнаруживать повторяющиеся угрозы и риски. При обнаружении атак «нулевого дня» решение McAfee Advanced Correlation Engine может выполнить анализ журнальных данных и определить, не подвергалась ли ваша организация подобным атакам в прошлом. Это можно назвать обнаружением угроз безопасности «донулевого дня».

Обеспечения быстродействия именно там, где оно необходимо

Поскольку решение McAfee Advanced Correlation Engine поставляется в виде самодостаточного аппаратного устройства или виртуальной системы, оно не оказывает никакого влияния на быстродействие McAfee Enterprise Security Manager в том, что касается сбора событий и управления событиями. Вы можете использовать весь потенциал McAfee Advanced Correlation Engine без каких-либо ограничений, максимизируя при этом уровень производительности утилиты McAfee Enterprise Security Manager.

Сопоставление событий на основе правил

Сопоставление событий на основе правил производится путем анализа собранной информации в режиме реального времени с использованием традиционных корреляционных алгоритмов. Все журналы, события и сетевые потоки (наряду с контекстной информацией, такой как идентификационные данные, роли, уязвимости и т. д.) сопоставляются между собой с целью обнаружения признаков наличия более крупных угроз. Хотя сопоставление событий на основе правил в масштабах целой сети уже поддерживается всеми решениями McAfee Enterprise Security Manager напрямую, решение McAfee Advanced Correlation Engine располагает выделенной процессорной мощностью, позволяющей проводить сопоставление еще большего объема данных либо дополнительно к уже выполняемым процессам сопоставления данных, либо полностью заменяя их.

Сопоставление рейтингов риска без использования правил

Хотя корреляция на основе правил является необходимой и ценной функцией любой системы управления информацией о безопасности и событиями безопасности (security information and event management — SIEM), такие системы способны обнаруживать лишь уже известные признаки угроз, а для поддержания их эффективности требуется непрерывная настройка сигнатур и установка обновлений. Новые возможности открывает сочетание традиционных средств сопоставления данных с технологией сопоставления данных без использования правил. В системах сопоставления данных без использования правил установка сигнатур

заменяется простой настройкой, выполняемой лишь один раз: просто сообщите решению McAfee Advanced Correlation Engine, какие объекты имеют особую важность для вашей компании. Это может быть определенная служба или приложение, группа пользователей или некоторые типы данных.

Отслеживание и оповещение в реальном времени

После такой настройки решение McAfee Advanced Correlation Engine начинает отслеживание всех действий, связанных с указанными объектами, создавая динамический рейтинг риска, увеличивающийся или уменьшающийся в зависимости от действий в реальном времени. Если рейтинг риска превышает определенное пороговое значение, решение McAfee Advanced Correlation Engine генерирует событие. Такое событие может служить оповещением для аналитика безопасности о растущих угрозах или может быть использовано традиционным корреляционным модулем на основе правил в качестве признака наличия более крупного инцидента. Решение McAfee Advanced Correlation Engine ведет подробный журнал аудита со всеми рейтингами риска, что позволяет выполнять полный ретроспективный анализ и расследование факторов угроз.

Примеры использования

Моделирование корпоративного риска

Решение McAfee Advanced Correlation Engine является платформой для эффективного моделирования корпоративного риска. Доступ к особо секретным документам, получаемый сотрудниками с высоким уровнем допуска, может представлять опасность для оборонной организации, а утечка информации из историй болезни знаменитости, страдающей серьезным заболеванием, может угрожать репутации лечащей клиники. Решение McAfee Advanced Correlation Engine обеспечивает безупречное моделирование рисков вашей организации благодаря определению рейтинга важных для вашей организации параметров, что позволяет определить базовые показатели рисков и рассылать уведомления при превышении пороговых значений.

Упреждающая оценка риска для критически важных данных

Во время мониторинга данных в режиме реального времени McAfee Advanced Correlation Engine позволяет одновременно использовать оба корреляционных модуля для обнаружения рисков и угроз до их возникновения. Рейтинги рисков можно использовать в традиционных системах сопоставления событий. Например, имеется следующая традиционная сигнатура для обнаружения угроз на основе правил: «событие „вредоносная программа“, обнаруживаемое после события „вход в систему путем полного перебора пароля“». Как правило, при срабатывании этой сигнатуры событие уже произошло. Использование же решения McAfee Advanced Correlation Engine позволяет учитывать фактор риска в виде 20-процентного увеличения рейтинга риска после события «вход в систему путем полного перебора пароля». При регистрации такого события решение McAfee Advanced Correlation Engine может выдать упреждающее уведомление, что позволит своевременно вмешаться и предотвратить ущерб.

Оценка повторяющегося риска

Нередко бывает так, что после обнаружения угрозы или взлома возникает подозрение, что данная проблема существует уже давно. Развертывание решения McAfee Advanced Correlation Engine в журнальном режиме позволяет выполнять анализ всех журнальных данных как с помощью традиционного корреляционного модуля, так и с помощью корреляционного модуля «без правил».

Определение времени первого появления только что обнаруженной угрозы значительно повышает вероятность обнаружения основной причины данной проблемы.

Режимы работы

Сопоставление событий в режиме реального времени

- Обнаружение угроз по мере их появления путем сопоставления поступающих в реальном времени данных о событиях — на основе правил
- Обнаружение угроз по мере их развития путем сопоставления поступающих в реальном времени данных о событиях — без использования правил

Сопоставление событий в журнальном режиме

- Обнаружение повторяющихся угроз путем сопоставления журнальных данных о событиях — на основе правил
- Оценка повторяющихся угроз путем сопоставления журнальных данных о событиях — без использования правил

Функция сопоставления событий

- Сопоставление событий одновременно как на основе правил, так и без использования правил
- Сопоставление данных из любого поддерживаемого источника данных
- Сопоставление данных из всех распределенных сетей и устройств сбора данных
- Наличие сотен готовых правил сопоставления событий
- Наличие редактора конфигураций для корреляционного модуля «без правил»
- Наличие простого в использовании редактора правил сопоставления событий с графическим пользовательским интерфейсом для настройки существующих правил под конкретного пользователя и для создания новых правил

Рис. 1. Сопоставление событий на основе рисков помогает обнаруживать надвигающиеся опасности, угрожающие приоритетным активам.

Дополнительная информация

Для получения более подробных сведений посетите наш сайт **www.mcafee.com/ru/products/siem/index.aspx**.

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