McAfee Enterprise Security Manager

Приоритизация. Расследование. Реагирование.

Самая эффективная защита начинается с получения точной картины всего происходящего в системах, сетях, базах данных и приложениях. Фундаментом эффективной системы безопасности является управление информацией о безопасности и событиями безопасности (SIEM). McAfee® Enterprise Security Manager, являющийся центральным элементом разработанного McAfee решения SIEM, обеспечивает высокий уровень быстродействия, сбор данных для принятия конкретных мер реагирования и интеграцию решений с той скоростью и на том уровне масштабирования, которые необходимы подразделениям информационной безопасности. Решение дает возможность быстро приоритизировать, изучать и устранять скрытые угрозы, а также выполнять нормативно-правовые требования.

McAfee Enterprise Security Manager дает возможность в режиме реального времени получать информацию о происходящем за пределами компании (в виде данных об угрозах и репутации), а также обеспечивает представление сведений о системах, данных, рисках и действиях внутри компании. Он дает вашим ИТ-специалистам полный доступ к сопоставленным данным об угрозах и контексте, необходимым для быстрого анализа рисков и принятия решений, чтобы в условиях динамично меняющихся угроз и эксплуатационных требований вы могли использовать имеющиеся ресурсы с максимальной эффективностью. Такая функция служит важной предпосылкой для успешного расследования атак затяжного и скрытого характера, для поиска признаков взлома и для устранения отклонений, выявляемых в ходе аудитов. Стремясь сделать управление угрозами и нормативно-правовым соответствием неотъемлемой частью операций по обеспечению информационной безопасности, мы включили в McAfee Enterprise Security Manager интегрированные друг с другом средства управления конфигурациями и изменениями, управления ситуациями и централизованного управления политиками — всё, что необходимо для оптимизации рабочих процессов и повышения производительности труда специалистов по обеспечению ИБ. Кроме того, пользователям McAfee Enterprise Security Manager

Ключевые преимущества

- **Интеллектуальный продукт.** Обнаруживает и приоритизирует угрозы при помощи передовых функций анализа, используя большой объем контекстной информации.
- **Эффективные меры реагирования.** Необходимые вам данные выводятся в динамических представлениях, позволяющих, среди прочего, при получении важных предупреждений и обнаружении важных признаков принимать меры по расследованию, сдерживанию и устранению угроз и адаптации защиты.

Подписаться

предлагаются пакеты контента (англ. Content Packs), т. е. готовые конфигурации для сложных сценариев использования, помогающие упростить операции по обеспечению информационной безопасности.

Решение корпоративного масштаба

Перед подразделениями информационной безопасности, вынужденными собирать и быстро анализировать постоянно растущие объемы неструктурированных и структурированных данных в современных динамичных и распределенных корпоративных архитектурах, всё более остро встает вопрос повышения производительности труда. Для решения этой проблемы в McAfee Enterprise Security Manager используется открытая и масштабируемая шина данных, предназначенная именно для обработки больших объемов данных. Кроме того, все операции с данными осуществляются с использованием высокомасштабируемой архитектуры обработки данных во избежание нарушений в процессе сбора, использования и хранения данных. Такие нарушения могут поставить под угрозу проведение расследований, например, в случае утери критически важных данных, в случае слишком медленной обработки запросов или в случае невозможности проведения полноценного поиска из-за недостаточного быстродействия.

Сбор критически важных фактов за минуты, а не за часы

Возможность быстрого доступа к устройствам долгосрочного хранения данных о событиях является важной предпосылкой для успешного расследования инцидентов, для поиска признаков сложных атак и для исправления ошибок, обнаруживаемых в ходе аудитов нормативно-правового соответствия — для всего этого необходимо иметь возможность анализа архивных данных и полный доступ ко всей информации по каждому конкретному событию.

Высокопроизводительные аппаратные устройства собирают и обрабатывают накопленные на протяжении многих лет журнальные события и сопоставляют их с другими потоками данных (в том числе в формате STIX) на необходимой вам скорости. McAfee Enterprise Security Manager в состоянии хранить миллиарды событий и потоков, предоставляя, с одной стороны, постоянную возможность доступа ко всей информации для спонтанных запросов, а с другой стороны, обеспечивая долгосрочную сохранность данных для проведения компьютерно-технических экспертиз, проверки правил и обеспечения нормативно-правового соответствия. Более того, обеспечивается мгновенная репликация данных с сохранением их в различные места хранения, что гарантирует непрерывность работы бизнеса.

Анализ контекста и содержимого

При наличии контекстной информации (включая информацию об угрозах и репутации, о системах управления идентификационными данными и доступом, о решениях для обеспечения конфиденциальности данных и других поддерживаемых системах), данные о каждом событии обогащаются соответствующей контекстной информацией. Контекст помогает разобраться в том, как сетевые события и события

Ключевые преимущества (продолжение)

- **Интегрированный подход.** Решение отслеживает и анализирует данные, получаемые из обширной, разнородной инфраструктуры безопасности, и обеспечивает двустороннюю интеграцию благодаря открытым интерфейсам. Кроме того, оно позволяет автоматизировать большое количество первоначальных мер реагирования.

безопасности соотносятся с атрибутами активов и с реальными бизнес-процессами и политиками, что в свою очередь позволяет оптимизировать процессы анализа и приоритизации угроз.

Благодаря своей масштабируемости и быстродействию McAfee Enterprise Security Manager позволяет собирать большее количество информации из большего количества источников (включая используемые в разных приложениях данные: документы, транзакции, сообщения и т. п.), что значительно облегчает задачу проведения компьютерно-технических экспертиз. Эти данные тщательно индексируются, нормализуются и сопоставляются между собой с целью обнаружения большего количества рисков и угроз безопасности.

Расширенная трактовка угроз

Любое отклонение от нормы, обнаруженное в сетевом трафике, действиях пользователей или поведении приложений может свидетельствовать о наличии угрозы и о том, что ваши данные или ваша инфраструктура подвержены риску. McAfee Enterprise Security Manager рассчитывает базовый уровень активности для всей собираемой информации. Это решение заблаговременно создает приоритизированные уведомления о потенциальных угрозах и параллельно анализирует собранные данные на наличие признаков более крупных угроз. Кроме того, чтобы облегчить понимание взаимосвязи событий безопасности с реальными бизнес-процессами, McAfee Enterprise Security Manager снабжает каждое событие контекстной информацией.

Имеющиеся в McAfee Enterprise Security Manager панели Cyber Threat Manager позволяют оптимизировать процессы мониторинга и анализа новых угроз в режиме реального времени. Агрегирование информации об известных и потенциальных угрозах, поступающей через STIX/TAXII, из McAfee Advanced Threat Defense и/или со сторонних URL-адресов, и последующее ее сопоставление с данными событий либо в режиме почти реального времени, либо в журнальном режиме (с помощью функции обратного отслеживания), дает подразделениям ИБ возможность глубже анализировать распространение угроз в пределах той или иной среды. Такая информация помогает организациям предоставлять необходимые данные соответствующим специалистам для принятия рациональных решений и оперативных мер в режиме почти реального времени.

Оптимизация операций по обеспечению безопасности

Ориентированность McAfee Enterprise Security Manager на удобство работы пользователей дает аналитикам бóльшую свободу выбора, облегчает индивидуальную настройку операций и позволяет быстрее реагировать на результаты расследований. Благодаря упорядоченности рабочих процессов управление инцидентами осуществляется более оперативно и эффективно. Наличие быстрого и интеллектуального доступа к информации об угрозах дает аналитикам любого уровня

(т. е. как новичкам, так и опытным специалистам) возможность легче определять приоритеты угроз, расследовать угрозы и реагировать на них.

McAfee Enterprise Security Manager обеспечивает удобство в использовании без дополнительных усилий: в распоряжении специалистов немедленно оказываются сотни отчетов, представлений, правил и предупреждений, которые можно легко настраивать. Например, пользователи панели мониторинга McAfee Enterprise Security Manager могут настроить базовый уровень для оценки типичного использования сети или задать индивидуальные параметры предупреждений. Эта панель позволяет легко визуализировать важнейшие сведения о безопасности, исследовать их и составлять отчеты на их основе. В результате организации получают долгожданную возможность полного доступа к содержимому и контекстным данным, сопоставление которых необходимо для принятия быстрых и рациональных решений.

Кроме того, для упрощения операций по обеспечению безопасности пользователям McAfee Enterprise Security Manager предлагаются «пакеты контента» (Content Packs), включающие в себя готовые конфигурации для распространенных сценариев использования, позволяющие быстро брать на вооружение сложные функции обнаружения угроз и управления нормативно-правовым соответствием. В состав пакетов контента входят готовые конфигурации для осуществления практических операций по обеспечению безопасности, включая наборы правил, оповещений, представлений, отчетов, переменных и списков наблюдения. Многие пакеты контента включают в себя готовые триггеры для моделей поведения, требующих дополнительного анализа или автоматического устранения угроз.

Упрощение процесса обеспечения нормативно-правового соответствия

Благодаря централизации и автоматизации мониторинга нормативно-правового соответствия и формирования соответствующих отчетов McAfee Enterprise Security Manager позволяет отказаться от трудоемких ручных процессов. Кроме того, интеграция с Unified Compliance Framework (UCF) дает возможность повторно использовать однажды собранные данные для демонстрации соответствия различным нормативно-правовым требованиям и свести к минимуму финансовые и трудовые затраты на проведение аудитов. Поддержка UCF повышает эффективность процесса обеспечения нормативно-правового соответствия путем нормализации требований всех стандартов, что позволяет легко сопоставлять единый набор сведений о событиях с множеством отдельных нормативов.

Включенные в McAfee Enterprise Security Manager сотни готовых панелей мониторинга, всеобъемлющие журналы аудита и отчеты, отвечающие требованиям более чем 240 мировых стандартов и регламентирующих систем, в том числе PCI DSS, HIPAA, NERC-CIP, FISMA, GLBA, GPG13, JSOX и SOX упрощают и ускоряют процесс управления нормативно-правовым соответствием.

Помимо обширных встроенных возможностей, все отчеты, правила и панели мониторинга McAfee Enterprise Security Manager поддерживают полную индивидуальную настройку.

Объединение вашей ИТ-инфраструктуры

Интеграция в масштабе всей инфраструктуры ИБ дает возможность в режиме реального времени получать беспрецедентно подробную информацию об уровне защищенности организации. McAfee Enterprise Security Manager может получать ценные данные как с защитных устройств сотен различных производителей, так и из каналов информации об угрозах. Интеграция с McAfee Global Threat Intelligence (McAfee GTI) позволяет получать данные с более чем 100 миллионов расположенных по всему миру датчиков McAfee Labs, формирующих постоянно обновляемый канал информации об известных вредоносных IP-адресах. McAfee Enterprise Security Manager может также принимать информацию об угрозах, поступающую через STIX/TAXII и/или со сторонних URL-адресов, и принимать меры на основе результатов анализа.

Кроме того, McAfee Enterprise Security Manager поддерживает активную интеграцию с десятками дополнительных решений для управления инцидентами и анализа угроз, включая решения McAfee и партнеров по McAfee Security Innovation Alliance.

Так, например, McAfee Threat Intelligence Exchange анализирует результаты мониторинга конечных точек и собирает сведения о малораспространенных атаках, используя для этого информацию об угрозах, получаемую из глобальных, сторонних и локальных источников. Для дальнейшего анализа и классификации файлов McAfee Threat Intelligence Exchange может также использовать другие интегрированные продукты, например, McAfee Advanced Threat Defense.

Для аналитиков дополнительное преимущество заключается в интеграции с McAfee Behavioral Analytics — отдельным решением для анализа поведения пользователей и организаций, позволяющим свести миллиарды событий безопасности к нескольким сотням аномалий и на выходе получить несколько приоритизированных указаний на возможные угрозы, а также дающим аналитикам возможность обнаруживать необычные и крайне опасные угрозы безопасности, зачастую не определяемые другими решениями. Аналогичным образом, интеграция McAfee Enterprise Security Manager с McAfee Investigator помогает превратить аналитиков в специалистов по расследованию угроз и дает им возможность повысить скорость разрешения проблем и быть более уверенными в том, что им удалось определить действительную причину того или иного инцидента.

Для проверки систем на наличие временно бездействующих вредоносных файлов «нулевого дня» и для поиска активных процессов в памяти специалисты по реагированию на инциденты и администраторы могут использовать McAfee Active Response. Кроме того, McAfee Active Response использует постоянно работающие коллекторы, позволяющие осуществлять непрерывный мониторинг конечных точек на наличие определенных признаков взлома и автоматически рассылать предупреждения в случае обнаружения того или иного признака взлома в какой-либо точке среды. В отличие от стандартных подходов к обеспечению безопасности, это сочетание позволяет организациям использовать преимущества замкнутого рабочего процесса, охватывающего все этапы от обнаружения до нейтрализации и устранения угроз.

McAfee предлагает комплексную систему обеспечения безопасности, дающую организациям возможность предотвращать атаки и реагировать на новые угрозы. Мы поможем вам устранять угрозы быстрее и эффективнее, задействуя при этом меньше ресурсов. Наша объединенная архитектура и централизованное управление системой защиты позволяют снизить сложность и повысить эффективность работы в масштабах всей инфраструктуры безопасности. McAfee прилагает все усилия к тому, чтобы быть вашим главным партнером в вопросах безопасности, предоставляя вам полный набор интегрированных друг с другом средств защиты.

Дополнительная информация

Дополнительную информацию о McAfee Enterprise Security Manager можно получить по адресу **https://www.mcafee.com/ru/products/siem/index.aspx**.

Дополнительную информацию об интегрированных решениях можно получить по адресу **www.mcafee.com/secops**.

McAfee Together is power.

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