SIEM: пять требований, позволяющих решить серьезные бизнес-задачи

Решения для управления информацией о безопасности и событиях безопасности (SIEM) используются в производственных средах уже более десяти лет и считаются достигшими зрелого возраста. Такие функции, как сбор сведений о событиях, сопоставление событий, рассылка предупреждений и демонстрация нормативно-правового соответствия, считаются основополагающими и имеются в большинстве решений SIEM. Однако ситуация меняется. Организациям приходится иметь дело с такими новыми угрозами, как направленные и постоянные атаки; с такими новыми тенденциями, как мобильные устройства, облачные службы и виртуализация; а также со сменой бизнес-приоритетов в том, что касается привлечения клиентов, эффективности операций и экономии средств. Поэтому для решения серьезных бизнес-задач системы SIEM должны иметь более совершенный набор функций.

Специалисты McAfee обратились к пользователям SIEM, чтобы узнать об основных проблемах в работе с этими решениями. Пользователи назвали следующие пять первоочередных проблем:

- «большие данные» в сфере безопасности;
- ситуационная осведомленность;
- контекст в режиме реального времени;
- простота управления;
- встроенная безопасность.

Чтобы решения SIEM помогали повышать эффективность стратегий управления безопасностью и рисками (в частности, в том, что касается снижения уровня угроз, следования новым тенденциям и согласования ИТ с приоритетами бизнеса), все эти пять пунктов должны быть учтены. Описание каждой проблемы сопровождается соответствующими примерами из практики.

Пример использования: «большие данные» в сфере безопасности

- Расширение возможностей для сбора данных благодаря увеличению числа каналов и источников информации
- Получение аналитической информации и проведение компьютерно-технических экспертиз с использованием очень больших наборов данных
- Оптимизация скорости и пропускной способности для обработки «больших данных» в сфере безопасности
- Повышение эффективности труда и процессов

1. «Большие данные» в сфере безопасности

«Большие данные» в сфере безопасности могут быть чрезвычайно ценны — если вы можете их использовать. Прежние решения SIEM не предусматривали интеграции с таким большим числом конечных точек, сетей и источников данных. Они не были предназначены ни для обработки событий, происходящих со столь высокой частотой, ни для хранения данных в течение столь длительного периода времени. Поэтому использование реляционных баз данных и другие подобные недостатки прежних решений SIEM, предназначавшихся прежде всего для обработки сетевых событий, просто-напросто не соответствуют тем требованиям к безопасности, которые предъявляются в современных динамичных ИТ-инфраструктурах. Чтобы оставаться эффективными и пригодными к использованию, прежним решениям не хватает скорости, расширяемости и масштабируемости.

Пример из практики: государственное учреждение федерального уровня

Крупному государственному учреждению требовалось подробно анализировать «большие данные» о безопасности, хранящиеся в многопетабайтной реляционной базе данных SIEM. Однако формирование даже простых отчетов занимало несколько часов, а на некоторые отчеты не хватало и дня, из-за чего имеющееся в учреждении решение SIEM было непригодно для проведения компьютерно-технических экспертиз.

Переход на использование McAfee® Enterprise Security Manager позволил учреждению увеличить количество интегрированных устройств разных типов, что дало возможность использовать более широкий контекст данных и пользователей. Частота событий и объем хранимых данных также возросли. Отчеты теперь формируются за несколько минут, что значительно упрощает всю процедуру проведения компьютерно-технических экспертиз.

Пример использования: ситуационная осведомленность

- Повышение ситуационной осведомленности с помощью дополнительных решений для идентификации пользователей
- Ответы на вопросы «кто», «когда», «как», «где» и «что»
- Оценка продолжительности событий и взаимосвязи их с другими событиями и пользователями
- Учет личных устройств сотрудников: ноутбуков, смартфонов и т. п.

2. Ситуационная осведомленность

Когда-то решения SIEM были просто инструментом для сопоставления событий, поступающих со всех межсетевых экранов и систем обнаружения вторжений. Иногда сопоставленные события анализировались с помощью некоторого набора данных для оценки уязвимостей. Даже сегодня существуют решения SIEM, делающие основную ставку на данные о сетевых потоках. Хотя все эти источники важны, их необходимо дополнять информацией о приложениях, контексте данных и пользователях. В противном случае потребуется больше времени и ресурсов на то, чтобы проанализировать события и определить их приоритет, в достаточной мере учитывая особенности ситуации для своевременного принятия необходимых мер.

Пример из практики: медицинское учреждение

Региональное медицинское учреждение взяло на вооружение концепцию использования сотрудниками личных устройств в рабочих целях (bring your own device — BYOD), чтобы повысить динамичность работы персонала путем поддержки личных планшетных компьютеров сотрудников. Однако из-за ряда инцидентов, имевших место в прошлом, учреждение было обеспокоено риском внутренних злоупотреблений. Прежнее решение SIEM, использовавшееся в этой организации, не позволяло идентифицировать пользователей, взаимодействующих с конфиденциальными данными, независимо от устройства (ноутбук, настольный компьютер, планшетный компьютер или виртуальная рабочая станция).

Перейдя на McAfee Enterprise Security Manager, учреждение получило возможность подключаться к системам управления идентификационными данными и мобильными устройствами, каталогу Active Directory и продуктам LDAP для получения информации о пользователях и устройствах. McAfee Enterprise Security Manager интегрируется с хранилищами структурированных и неструктурированных данных (в частности, путем встроенной поддержки баз данных), а также с системами предотвращения утечки данных (DLP) и мониторинга активности баз данных (DAM). Благодаря такой интеграции достигается более полная ситуационная осведомленность и более высокий уровень защиты от внутренних угроз.

Пример использования: контекст в режиме реального времени

- Получение представления о внутренних и внешних угрозах
- Повышение качества собираемой с помощью SIEM информации путем добавления контекста, получаемого в режиме реального времени
- Повышение скорости обнаружения инцидентов и реагирования на них
- Обнаружение угроз и определение их приоритета благодаря сбору дополнительной информации

3. Контекст в режиме реального времени

Одной из первых областей применения SIEM было управление журналами, включавшее в себя сбор, хранение и извлечение информации, а также некоторые дополнительные функции. Журналы по-прежнему остаются основополагающим компонентом SIEM, но сегодняшним решениям SIEM необходим также контекст, получаемый в режиме реального времени.

Примерами обеспечения такого контекста являются McAfee Global Threat Intelligence (McAfee GTI) и McAfee Vulnerability Manager. McAfee GTI представляет собой облачную службу оценки репутации в режиме реального времени, а McAfee Vulnerability Manager собирает информацию об уязвимости активов организации.

Пример из практики: розничная торговая сеть

Розничная торговая сеть из списка Fortune 100, не использовавшая решение SIEM и не имевшая решений McAfee, провела оценку эффективности SIEM на практике. За первую неделю обнаружилось, что более 30 % трафика, пытавшегося попасть в сеть организации, исходило из вредоносных источников и/или содержало вредоносную нагрузку.

Используя McAfee Enterprise Security Manager для сопоставления информации о событиях с McAfee GTI, организация быстро определила, какие активы в ее магазинах и центрах обработки данных стали объектами атак злоумышленников, и получила лучшее представление о типах атак, которым она подвергается. Предложенное компанией McAfee решение SIEM позволило определить крайнюю степень риска и ранжировать ответные меры по приоритетам. Использование SIEM в сочетании с получаемым в режиме реального времени контекстом позволило быстрее обнаруживать, ранжировать и устранять угрозы.

Пример использования: простота управления

- Защита устройств фиксированного назначения путем развертывания SIEM с функцией динамических белых списков и программно-аппаратными средствами защиты
- Упрощение процедуры проведения компьютерно-технических экспертиз благодаря настраиваемым функциям детализации отчетов.
- Повышение скорости реагирования на инциденты благодаря интеграции SIEM с межсетевыми экранами и системами предотвращения вторжений (IPS)
- Продление срока службы устаревших активов благодаря повышению уровня безопасности

4. Простота управления

Устаревшие решения SIEM имеют крайне негибкую архитектуру, и у них нет ряда важных функций. Например, их трудно интегрировать с теми устройствами, которые раньше не поддерживались, что затрудняет доступ к информации на этих устройствах. С другой стороны, SIEM следующего поколения отличается простотой настройки и достаточной гибкостью, что позволяет ему работать в любой среде. Именно поэтому внедрение современного решения SIEM имеет стратегическое значение для такого большого количества организаций.

Пример из практики: коммунальная компания

Крупной коммунальной компании нужно было внедрить такие средства безопасности, которые защитили бы ее инфраструктуру от атак типа Stuxnet, способных привести к отключению электричества у миллионов потребителей. Используя McAfee Enterprise Security Manager со встроенной поддержкой устройств, приложений и протоколов, компания обеспечила себе осведомленность о ситуации во всех корпоративных зонах, связанных с ИТ-инфраструктурой, системами SCADA и системами АСУ.

SIEM компании McAfee предоставило в распоряжение клиента все средства, необходимые для самостоятельного осуществления интеграции с устройствами SCADA и АСУ. А это в свою очередь дало клиенту возможность осуществлять сопоставление событий, обнаружение аномалий и анализ тенденций во всех трех зонах. Клиент смог не только подстроить под себя механизм сбора сведений о событиях, но также

легко и быстро создал свои собственные панели мониторинга, отчеты, правила сопоставления событий и предупреждения. Таким образом, решение SIEM стало незаменимым инструментом для обеспечения безопасности, демонстрации соответствия нормативно-правовым требованиям и обеспечения доступности активов — иными словами, для дальнейшей бесперебойной работы компании.

Пример использования: встроенная безопасность

- Упорядочение процессов обеспечения безопасности и потока операций
- Упрощение работы благодаря автоматизации задач и простоте настроек
- Повышение уровня информированности и ситуационной осведомленности с помощью защитных решений, способных взаимодействовать друг с другом
- Повышение уровня безопасности путем сбора информации и интеграции решений

5. Встроенная безопасность

SIEM — важный, но не единственный компонент любой стратегической инициативы в области безопасности. Решения для обеспечения безопасности и нормативно-правового соответствия более эффективны в совокупности, чем по отдельности, к тому же использование разрозненной архитектуры сильно усложняет работу. Сложность работы — вот причина, по которой обеспечение безопасности зачастую не становится стратегической задачей, а остается по большей части тактической инициативой, недостаточно согласованной с приоритетами бизнеса.

Пример из практики: финансовые услуги

У клиента, занимающегося международными банковскими операциями, было множество разрозненных продуктов от различных поставщиков. Некоторые продукты использовались в производственных системах, но многие использовались нерегулярно или не обслуживались вовремя из-за ограниченности ресурсов. Банк установил, что используя решение SIEM в сочетании с интегрированными средствами защиты конечных точек, сетей и данных, он сможет более эффективно снижать риск и сокращать затраты, повышая при этом соответствие системы безопасности требованиям бизнеса.

Банк сократил количество поставщиков и достиг экономии за счет масштаба. Кроме того, ему удалось понизить расходы на обучение и сократить число агентов, консолей, серверов и т. п. Это привело к сокращению затрат по контрактам и множества сопутствующих расходов. Помимо экономии средств банк получил гарантию полной интеграции всех существующих и будущих решений с McAfee Enterprise Security Manager, что позволяет ему лучше обеспечивать защиту и иметь более полное представление об уровне своей безопасности.

Основные вопросы

- Насколько важна для вас возможность легко справляться с задачами сбора, хранения, использования, обработки и анализа информации, предоставляемая технологиями обработки «больших данных» в сфере безопасности?
- Располагают ли заинтересованные в обеспечении вашей безопасности стороны всей информацией, необходимой для принятия обоснованных решений и совершения своевременных действий?
- Есть ли у ваших специалистов по безопасности собираемая в режиме реального времени информация о контексте, необходимая для обнаружения рисков и атак до того, как они успеют причинить вред?
- Если бы вы стали использовать SIEM с интуитивно понятными средствами детализации и легко настраиваемыми представлениями, то как это сказалось бы на уровне вашей безопасности и эффективности использования ресурсов?
- К каким положительным изменениям с точки зрения безопасности, процессов, оперативности и понимания ситуации привела бы интеграция в масштабах всей вашей инфраструктуры?

Средства, успешно использовавшиеся в прошлом десятилетии устаревшими системами SIEM, уже не отвечают требованиям сегодняшнего дня. Новые требования, касающиеся сбора информации о безопасности, обработки «больших данных», ситуационной осведомленности, быстродействия, удобства использования и интеграции, расширили сферу применения SIEM. Решения SIEM должны упрощать работу, а не усложнять ее. Требуйте большего от своего решения SIEM.

Сегодня решения SIEM должны быть частью более крупной и взаимосвязанной платформы безопасности, согласовывающей приоритеты безопасности с приоритетами бизнеса. SIEM играет важную роль в повышении стратегического значения безопасности и создании реальных преимуществ для бизнеса.

Дополнительную информацию о решениях SIEM компании McAfee см. на странице www.mcafee.com/ru/products/siem/index.aspx.

Security Connected

Платформа Security Connected компании McAfee представляет собой единую структуру, в рамках которой сотни продуктов, услуг и партнеров могут обмениваться друг с другом важными сведениями, в режиме реального времени делиться друг с другом данными о контексте и совместно обеспечивать безопасность информации и сетей. Используя предлагаемые данной платформой инновационные концепции, оптимизированные процессы и практичные способы экономии, любая организация может повысить уровень своей безопасности и минимизировать операционные затраты.

ООО «МакАфи Рус»
Адрес: Москва, Россия, 123317
Пресненская набережная, 10
БЦ «Башни на набережной», Башня «А», 15 этаж
Телефон: +7 (495) 653-85-13
www.McAfee.ru

61099brf_focus-5-siem_0514_fnl_ETMG