Обзор решения: Управление безопасностью и соблюдением нормативных требований

Symantec™ Security Information Manager

Реализация документально описанного, воспроизводимого процесса обработки угроз безопасности и соблюдения нормативных требований IT-политики.

Обзор

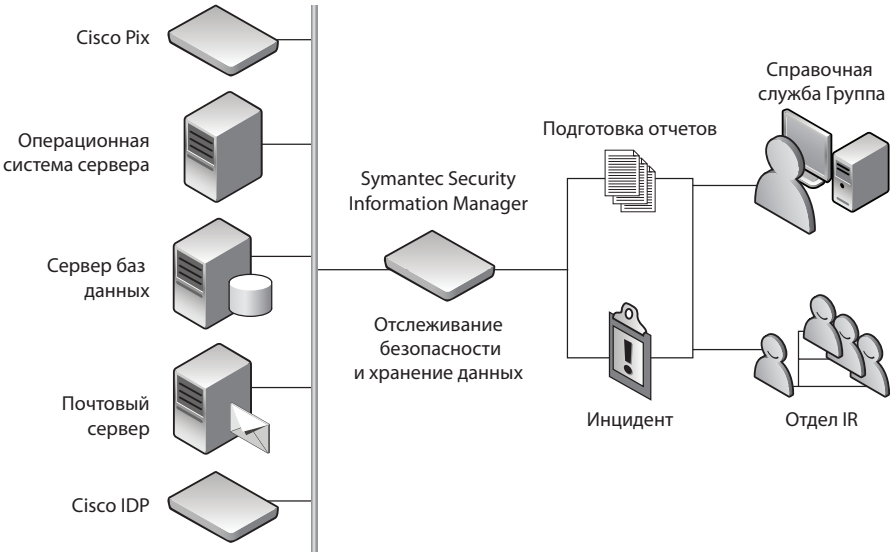
Международные организации помимо защиты критически важных бизнес-ресурсов должны обеспечивать соответствие различным официальным требованиям. Соответствие официальным требованиям - это одна из основных задач информационной безопасности, однако процесс соблюдения требований, таких как акт Сарбанеса-Оксли или HIPAA, на уровне организации связан со значительными трудностями. Эффективные решения должны не только защищать корпоративные бизнес-ресурсы, но и обеспечивать соответствие политикам организации.

Необходимо определить все события системы обеспечения безопасности, имеющие отношение к организации, вне зависимости от уровня серьезности, проанализировать их для расстановки приоритетов и занести в каталог. В управлении каждым этапом этого процесса могут принимать участие разные сотрудники IT-организации, начиная с аналитика в области безопасности, который из тысяч различных событий выбирает разумное число критически важных. Критически важные события передаются менеджеру IT-операций, который отвечает за разработку ответных действий. Для завершения процесса требуется показать, что было предпринято наиболее подходящее и эффективное действие. Этот ресурсоемкий процесс выполняется вручную и, как правило, мало эффективен.

Задачи эффективного управления информацией о безопасности имеют важное значение для каждого CISO:

- Получение понятной и актуальной информации о безопасности
- Точная оценка уровня безопасности IT-среды
- Наглядные отчеты о выполнении подходящих и эффективных действий
- Соблюдение требований без наращивания численности персонала

Продукт Symantec Security Information Manager помогает IT-организациям выявлять угрозы безопасности, направленные на наиболее важные бизнес-приложения, определять их приоритеты, анализировать и устранять эти угрозы. Он выполняет роль системы управления журналами с целью мониторинга управления идентификационными данными, обеспечения соответствия нормативным требованиям, а также сбора доказательств преступной деятельности. Сопоставление недостатков защиты сети и хостов в режиме реального времени с помощью доказавшей свою эффективность службы Symantec Global Intelligence Network - это одно из ключевых преимуществ продукта Symantec Security Information Manager, делающее его системой оперативного реагирования на происшествия мирового класса с акцентом на обеспечение целостности наиболее важных для бизнеса информационных ресурсов.



Продукт Symantec Security Information Manager собирает и хранит данные журналов из нескольких источников в центральном хранилище данных о происшествиях. После нормализации сведений из журналов расставляются приоритеты происшествий с учетом ресурсов и значений CIA. Сопоставление с данными, собранными в глобальной сети, позволяет выделить десятки из тысяч происшествий.

Функции

- Создание отчетов о соблюдении нормативных требований и аудите
- Механизм анализа угроз в режиме реального времени
- Хранилище событий
- Определение приоритетов происшествий
- Процесс исправления происшествий
- Средства хранения и извлечения журналов
- Интегрированная справочная служба

Преимущества

- Обеспечение защиты и соблюдения требований в IT-операциях
- Выявление проблем безопасности, относящихся к среде, с помощью журналов событий
- Выполнение внутренних и официальных требований к хранению данных
- Повышение производительности работы за счет привлечения специалистов по безопасности к работе над наиболее серьезными происшествиями
- Выявление и устранение угроз в соответствии с подробными инструкциями по исправлению
- Комплексное и понятное представление системы безопасности на сводной панели защиты
- Долгосрочное хранение журналов событий в области безопасности для определения тенденций и анализа происшествий
- Расширенная техническая процедура для синхронизации безопасности и IT-операций с целью оперативного решения проблем

Приложения

- Обработка угроз
- Создание отчетов о соблюдении требований
- Ответная реакция на происшествия
- Управление журналами
- Анализ происшествий

Средства хранения и извлечения журналов

Сегодня компании во всем мире должны соблюдать официальные требования, сохраняя журналы событий в течение определенного времени и обеспечивая надлежащую работу средств хранения и извлечения данных. Продукт Symantec Security Information Manager превосходит стандартные продукты контроля информации о безопасности на основе реляционных баз данных, для которых характерны дополнительные начальные затраты и необходимость длительного администрирования баз данных. С продуктом Symantec Security Information Manager не требуется администрирование базы данных.

Продукт Symantec Security Information Manager сохраняет события в архивных файлах в указанном месте. Архив реализован в виде самостоятельного модуля. Он отслеживает использование диска и срок хранения отдельных архивных файлов. При достижении указанного ограничения дисковой памяти или даты истечения срока действия файла система удаляет старые архивные файлы, чтобы освободить место для новых файлов. Для хранения файлов можно выбрать программно-аппаратный комплекс, напрямую подключенный диск (DAS), сетевое устройство хранения (NAS) или сеть хранения данных (SAN).

Архивы Symantec Security Information Manager работают быстрее обычных баз данных, поскольку в отличие от нескольких сотен функций базы данных они оптимизированы для выполнения одной задачи - сохранения большого объема событий. Коэффициент сжатия в продукте Symantec Security Information Manager достигает 30:1. Нормализованные данные вместе с исходной информацией о событиях фиксируются и сохраняются для анализа происшествий. Такая функциа доступна только в Symantec Security Information Manager.

Анализ безопасности в режиме реального времени

Продукт Symantec Security Information Manager использует внешний стандарт выявления угроз безопасности - процесс, описанный в открытых стандартах Distributed Management Task Force (DMTF). Данный метод предусматривает классификацию угроз и проблем безопасности с учетом степени воздействия события на среду, способа атаки и целевых ресурсов. Такая классификация, называемая «Эффекты, механизмы и ресурсы» (EMR), лежит в основе модуля анализа данных Symantec Security Information Manager.

Благодаря гибкости интеллектуальных правил на основе шаблонов, отдельное правило может занять место нескольких более конкретных правил, применяемых в стандартных подходах. В результате значительно упрощается процедура обслуживания и создания правил, которые могут охватывать множество условий. Помимо правил условных действий Security Information Manager поддерживает правила модулей, для активации которых можно выбрать произвольные условия и аномалии статистики. В качестве примера можно привести правило отрицательного условия, которое запускается в случае отсутствия события в течение заданного времени.

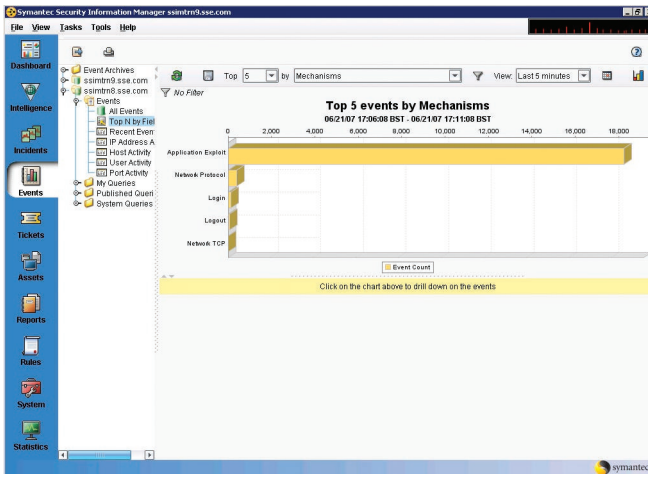
Правила можно присвоить группам с разными правами доступа, разрешив тем самым администраторам передавать права доступа. Продукт Symantec Security Information Manager собирает и анализирует события в реальном масштабе времени путем сопоставления потока нормализованных событий с учетом правил. В результате активации правила создается заключение, содержащее сокращенные идентификаторы связанных событий, а также ссылки на подробную информацию о событиях в хранилище событий. Впоследствии заключения сопоставляются с происшествиями, для которых создано одно или несколько заключений.

Происшествия можно присвоить группам с разными правами доступа, разрешив тем самым администраторам передавать права доступа.

Угрозы безопасности

Два раза в год Symantec публикует отчет *Internet Security Threat Report*. Ниже перечислены некоторые угрозы из последнего отчета, противодействовать которым помогает Symantec Security Information Manager:

- 88 процентов уязвимостей допускают удаленное использование
- 50 процентов уязвимостей позволяют злоумышленникам получить доступ к хосту
- 25 процентов всех краж идентификационных данных происходят в государственных учреждениях
- Компании из США наиболее подвержены фишингу
- 51 процент нелегальных серверов в США заражены вирусами
- 86 процентов пластиковых карт, продающихся на нелегальных серверах, были выпущены банками США
- В 2006 году в мире было зарегистрировано шесть миллионов компьютеров, зараженных ботами
- Права доступа бывшего сотрудника аннулируются с задержкой до четырех месяцев
- 69 процентов организаций сообщили о серьезных утечках данных в результате действий сотрудников



Продукт Symantec Security Information Manager выявляет наиболее опасные для вас угрозы и позволяет устранять их в режиме реального времени.

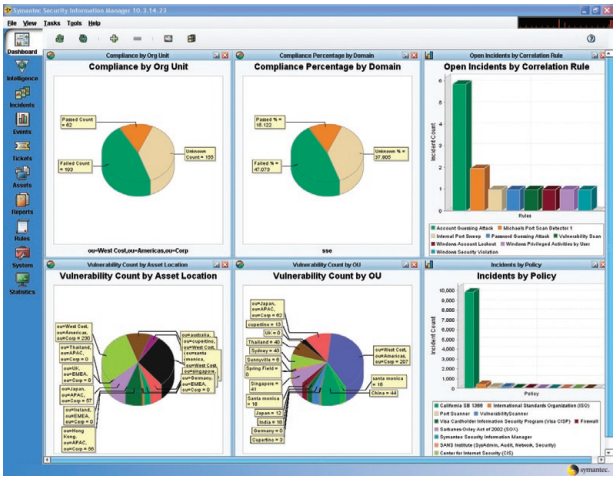
Создание отчетов о соблюдении нормативных требований и рисках

Продукт Symantec Security Information Manager позволяет создавать отчеты для руководителей, технические отчеты и отчеты о контроле, содержащие наглядное представление уровней серьезности угроз и состояния безопасности сети. Предусмотрено более 350 готовых запросов - от соблюдения требований до различных аспектов защиты. При необходимости с помощью мастера запросов можно создать собственные запросы.

В состав Symantec Security Information Manager входят стандартные шаблоны оценки соблюдения требований

для создания отчетов о контроле, такие как SOX, HIPAA, FISMA и PCI. Шаблоны обновляются в режиме реального времени с учетом событий из источников (Windows®, VPN, брандмауэр, операционная система и т.д.), поставляющих события в систему. Продукт Symantec Security Information Manager содержит встроенные отчеты для поддержки средств управления политиками, таких как Symantec Control Compliance Suite.

Запросы можно настроить для обновления сводной панели безопасности или размещения в отчетах с помощью простого в использовании интерактивного редактора. Шаблоны отчетов можно создавать, сохранять и совместно использовать аналогично запросам. Отчеты можно сгруппировать с целью организации или настройки доступа на основе ролей.



Продукт Symantec Security Information Manager позволяет создавать отчеты для руководителей, технические отчеты и отчеты об аудите, содержащие наглядное представление уровней серьезности угроз и состояния безопасности организации. На основе более 300 готовых запросов можно создавать пользовательские отчеты Symantec Security Information Manager.

Symantec Security Information Manager и официальные требования

Продукт Symantec Security Information Manager помогает компаниям соблюдать различные требования.

В частности, для соблюдения требований Symantec Security Information Manager использует следующие средства:

HIPAA

- Обзор активности в системе
- Отслеживание входов в систему
- Выявление и обработка подозрительных и неизвестных происшествий
- Регистрация и проверка событий в системах

GLBA

- «Управление доступом к приложениям путем регистрации попыток доступа и событий безопасности»
- «Безопасный доступ к операционным системам всех компонентов путем регистрации и мониторинга доступа пользователей и программ к важным ресурсам и выдача предупреждений о событиях безопасности»

SOX

- Мониторинг действий администраторов баз данных и привилегированных пользователей
- Интеграция с корпоративными системами контроля изменений, гарантирующая внесение только утвержденных изменений
- Регулярное создание отчетов о всех операциях с данными

California Act 1386

- Мониторинг несанкционированного доступа к личной информации

PCI

- Регистрация всех обращений к информации о способе оплаты
- Мониторинг учетных записей пользователей

Отслеживание происшествий

Продукт Symantec Security Information Manager помогает подготовиться к потенциальным угрозам, направленным на среду компании. Система раннего оповещения обнаруживает угрозы на глобальном уровне и предоставляет подробную информацию о них. Кроме того, она выдает рекомендации относительно мер по обеспечению защиты компании.

На этапе обнаружения для происшествия создается одно или несколько заключений, указывающих на угрозу безопасности. При создании происшествие можно присвоить отдельному сотруднику или группе. Происшествие создает техническую процедуру, облегчающую процесс хранения, уничтожения и восстановления. Техническую процедуру можно создать в виде запроса, отправляемого для обработки во внешнюю службу поддержки и возвращаемого по двустороннему соединению.

База знаний, применяемая Security Information Manager для создания технической процедуры, оперативно обновляется службой Symantec Global Intelligence Network. Специалистам по обработке происшествий предоставляются стратегии устранения угроз в соответствии с типом созданного происшествия. На основе этой информации можно проанализировать полученные знания и выполнить опережающее планирование.

Физические характеристики устройства

Основной программно-аппаратный комплекс содержит встроенное средство сбора и средство сбора без применения агентов; однако, он используется в основном для сопоставления данных. Symantec Security Information Manager позволяет установить дополнительный комплекс меньшего масштаба, повышающий эффективность