Платформа IBM QRadar Security Intelligence Platform

Обеспечение аналитики, пригодной для практического применения, для обеспечения информационной безопасности предприятия и соответствия нормативным требованиям

Особенности

- Интегрирует в единое унифицированное решение управление информацией и событиями системы безопасности (SIEM), управление логами, выявление аномалий и управление конфигурациями и устранением уязвимостей
- Использует преимущества единой архитектуры для анализа системных журналов, потоков данных, уязвимостей, данных пользователей и информационных ресурсов
- Использует корреляцию в режиме реального времени и обнаружение аномалий для выявления наиболее изощренных угроз
- Выявляет признаки наиболее критичных инцидентов ИБ среди миллиардов обычных журнальных записей
- Обеспечивает всестороннее наглядное представление графиков сетевой активности, работы приложений и действий пользователей
- Автоматизирует процессы, направленные на соблюдение нормативных требований по ИБ: сбор сведений, их корреляция и создание отчетов.

IBM® QRadar Security Intelligence Platform интегрирует в единое унифицированное решение управление сбором информациии (SIEM), обработку системных журналов, выявление аномалий, управление конфигурациями систем и устранением их уязвимостей. Используя аналитику (интеллектуальную функциональность), интеграцию и автоматизацию для обеспечения всестороннего рассмотрения условий поддержания безопасного состояния защищаемой информационной системы, данное решение обеспечивает превосходное обнаружение угроз, увеличивает простоту использования и снижает общую стоимость владения (TCO).

Предоставляет интеллектуальную функциональность, интеграцию и автоматизацию

Платформа QRadar Security Intelligence Platform обеспечивает преимущества в области безопасности и соответствия регуляторным требованиям, которые становятся бесценными в современном, более интеллектуальном мире, где технически оснащенные, взаимосвязанные и интеллектуальные бизнесы собирают, обрабатывают и хранят больше информации, чем когда бы то ни было ранее.

Обнаруживает угрозы, которые в другом случае могли бы оказаться пропущенными

Сегодня организации подвергаются большему количеству и разновидности атак, чем когда-либо в прошлом. Современные взломщики стали умнее и терпеливее, об их присутствии сообщают лишь едва уловимые шорохи. Платформа QRadar Security Intelligence Platform представляет собой интегрированное семейство продуктов, помогающих обнаружить угрозы и защищаться от них путем применения новой аналитики к увеличенному числу типов рассматриваемых данных. Такая методика помогает выявить первоочередные инциденты, которые в другом случае могли бы затеряться в шуме.

Платформа IBM QRadar Security Intelligence Platform обеспечивает всестороннюю безопасность.

Консолидирует хранилища первичных данных

Несмотря на то, что в регистрационных журналах и системных логах, создаваемых в организации, в ее сетевом потоке и в данных бизнес-процессов существует огромное количество информации, полезной для обеспечения ИБ, эта информация часто остается в хранилищах и игнорируется либо используется в недостаточной степени. QRadar сводит представления сети, безопасности и эксплуатации в единое, унифицированное и гибкое решение. Эта платформа разрушает препятствия между отдельными источниками сведений, выполняя коррелирование логов с потоками сети и множеством других данных и представляя всю релевантную информацию на едином экране. Так обеспечивается отличное обнаружение угроз и более функциональное представление активности предприятия.

Обнаруживает внутренние злоупотребления

Некоторые самые серьезные угрозы безопасности компании происходят изнутри, но организациям часто недостает аналитики и интеллектуальной функциональности, необходимой для обнаружения внутренних злоумышленников и внешних сторон, поставивших под угрозу учетные записи пользователей. Комбинируя мониторинг пользователей и приложений с наглядным представлением сети на уровне приложений, организации смогут лучше находить важные отклонения от нормальной активности, что поможет остановить атаку до того, как она достигнет цели.

Защищает и устраняет риски с помощью управления устранением уязвимостей

Команды, отвечающие за безопасность, сеть и инфраструктуру, стараются лучше справиться с рисками, выявляя уязвимости и вынося в приоритеты исправление этих уязвимостей прежде чем произойдет взлом. QRadar Security Intelligence Platform интегрирует в себе управление конфигурациями и устранением уязвимостей и возможности SIEM, включая коррелирование и аналитику сетевого потока, что позволяет получить лучшее понимание о критических уязвимостях. В результате организации могут устранять риски более эффективно и оперативно.

Соблюдает предписания нормативных требований регуляторов в области обеспечения ИБ

Многие организации бьются над тем, как пройти проверку на соблюдение требований регуляторов, одновременно пытаясь выполнить сбор данных, мониторинг и подготовку отчетов в условиях чрезвычайной ограниченности ресурсов. Чтобы автоматизировать и упростить задачу соответствия регуляторным требованиям, QRadar предлагает функциональность сбора данных, коррелирования и подготовки отчетов для активности, связанной с соблюдением требований регуляторов, подкрепленную многочисленными готовыми шаблонами отчетов.

Использует преимущества более простой в применении и более интеллектуальной аналитики

Платформа QRadar Security Intelligence Platform обеспечивает унифицированную архитектуру для хранения, коррелирования, выполнения запросов и подготовки отчетов по логам, потокам данных, уязвимостям, данным пользователей и ресурсов. Она объединяет в себе изощренную аналитику с готовыми правилами, отчетами и информационными панелями отображения. Будучи достаточно мощной и масштабируемой, пригодной для корпораций, входящих в перечень Fortune 500, и крупных государственных органов, она также достаточно интуитивна и гибка для малых и средних организаций. Пользователи извлекают выгоду за счет сокращения времени получения результата, снижения стоимости владения, роста гибкости и улучшения защиты от рисков, связанных с безопасностью и соблюдением требований регуляторов.

Аналитика

Анализируя больше типов данных и используя больше аналитических методик, QRadar может часто обнаруживать угрозы, пропущенные другими решениями, и обеспечивать наглядное представление сети, какое другие решения не могут обеспечить.

Интеграция

Благодаря общей платформе приложений, базе данных и пользовательскому интерфейсу эта платформа способна обеспечивать значительный масштаб при управлении процессом сбора регистрационной информации ИБ, не ухудшая аналитику в реальном времени и аналитику сетевого поведения. Она обеспечивает общее решение для всех функций поиска, коррелирования, обнаружения аномалий и подготовки отчетов. Единый интуитивный пользовательский интерфейс обеспечивает беспроблемный доступ ко всем функциям управления логами, анализа потока данных, управления инцидентами, управления конфигурациями и устранением уязвимостей, к информационным панелям и функциям подготовки отчетов.

Автоматизация

Платформа QRadar Security Intelligence Platform проста в развертывании и управлении и предлагает обширный выбор готовых интеграционных модулей и аналитики для обеспечения безопасности. Автоматизируя многие функции обнаружения ресурсов, нормализации данных и настройки, а также обеспечивая готовые к использованию шаблоны правил и отчетов, данное решение может существенно уменьшить сложность использования, которая часто портит другие продукты.

Почему IBM?

В распоряжении IBM находится одна из самых больших в мире организаций, занимающихся исследованиями, разработкой и предоставлением решений в области безопасности. Она состоит из 10 операционных центров защиты, девяти исследовательских центров IBM Research, 11 лабораторий разработки ПО для обеспечения безопасности и Института передовой безопасности (Institute for Advanced Security) с отделениями в США, Европе и Юго-Восточной Азии. Решения IBM позволяют организациям уменьшить уязвимости в своей системе обеспечения безопасности и бросить основные силы на обеспечение успеха стратегических инициатив. Такие продукты создаются на основании опыта исследований угроз, накопленного группой IBM X-Force по исследованию и разработке, что позволяет обеспечить предупредительный подход к безопасности. Компания IBM, доверенный партнер в области безопасности, предоставляет решения, позволяющие обеспечить защиту всей инфраструктуры предприятия, включая облако, от самых современных рисков в области безопасности.

Дополнительные сведения

Для получения дополнительных сведений о платформе IBM QRadar Security Intelligence Platform обратитесь к представителю или бизнес-партнеру IBM либо посетите следующий веб-сайт: **ibm.com**/security

IBM Восточная Европа/Азия
123317, Москва
Краснопресненская наб., 18
Тел.: +7 (495) 775-8800, +7 (495) 940-2000
Факс: +7 (495) 940-2070

Домашняя страница IBM находится по адресу **ibm.com**/ru

WGD03023-RURU-00