Positive Technologies и Qlik: технологическое партнерство в сфере информационной безопасности

«Платформа QlikView позволила нам создать гибкую, эффективную и удобную для пользователей систему бизнес-анализа событий безопасности — Positive Technologies Reporting Portal, предназначенную для обработки и визуализации результатов анализа защищённости информационных активов»,

– говорит Максим Филиппов, директор по развитию бизнеса Positive Technologies в России

– Максим Филиппов, директор по развитию бизнеса Positive Technologies в России

Компания Positive Technologies работает на рынке систем анализа защищенности с 2002 года. Согласно исследованиям IDC, в 2013 году компания заняла третье место на российском рынке ПО для безопасности, а также стала лидером по темпам роста на международном рынке систем управления уязвимостями. На сегодняшний день более 1000 организаций из 30 стран мира используют решения Positive Technologies для оценки защищенности своих сетей и приложений, для проверки соответствия стандартам безопасности, а также для выявления и блокирования атак в режиме реального времени. В середине 2015 года компания Positive Technologies был назван «визионером» в рейтинге Gartner Magic Quadrant по безопасности веб-приложений.

В помощь флагману

Флагманским продуктом Positive Technologies является MaxPatrol 8. Это система контроля защищенности и соответствия стандартам, которая позволяет получать объективную оценку состояния защищенности как всей информационной системы, так и отдельных подразделений, узлов и приложений. Работа системы базируется на механизмах тестирования на проникновение (Pentest), системных проверках (Audit) и контроле соответствия стандартам (Compliance) в сочетании с поддержкой анализа различных операционных систем, СУБД и веб-приложений. Такой комплексный анализ позволяет MaxPatrol 8 обеспечивать непрерывный

Компания
Positive Technologies

Индустрия
IT

Функции
Выявление и анализ событий безопасности

География
Россия

Задачи
Создание простого и функционального инструмента для анализа больших объемов данных по событиям безопасности

Решение
Компания Positive Technologies создала на платформе QlikView систему бизнес-анализа событий безопасности Positive Technologies Reporting Portal, интегрированную с PT MaxPatrol 8 и MaxPatrol SIEM.

Преимущества

- Широкие возможности интеграции с любыми источниками данных и мощные инструменты обработки этих данных
- Высокоинтерактивный пользовательский интерфейс в сочетании с принципом in-memory
- Удобные механизмы расширения функциональности позволяют строить нестандартные визуализации данных, подстраиваясь под особенности конкретных клиентов
- Мобильный и веб-доступ к дашбордам
- Возможность формирования отторгаемой отчетности

Источники данных

- Данные PT MaxPatrol 8 в СУБД Microsoft SQL
- Конфигурационные файлы

технический аудит безопасности на всем жизненном цикле информационной системы.

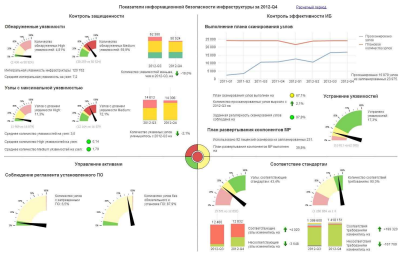
«В процессе работы MaxPatrol на каждом сетевом узле информационной системы клиента нередко обнаруживается больше десятка уязвимостей или настроек, не соответствующих стандартам безопасности. Таким образом, в организациях с большим количеством узлов пользователь MaxPatrol может получать тысячи сообщений о проблемах безопасности, найденных в результате каждого сканирования, – рассказывает Михаил Башлыков, заместитель генерального директора Positive Technologies по развитию продуктов. – Чтобы мгновенно обрабатывать такое количество сообщений, делать необходимые выборки, менять уровень детализации, нужен был удобный и функциональный инструмент. Требования к нему были достаточно высокими. Мы понимали, что система должна сохранять высокую производительность при постоянном увеличении объемов данных, обеспечивать высокую гибкость для адаптации под индивидуальные требования заказчика и иметь удобный интерфейс для интеграции с продуктами Positive Technologies».

Кроме того, продукт должен было генерировать графические представления для оценки динамики изменений системы между сканированиями, а также для сравнения уровня защищенности между организационными или географически распределёнными подразделениями компании.

Инструмент для Big Data

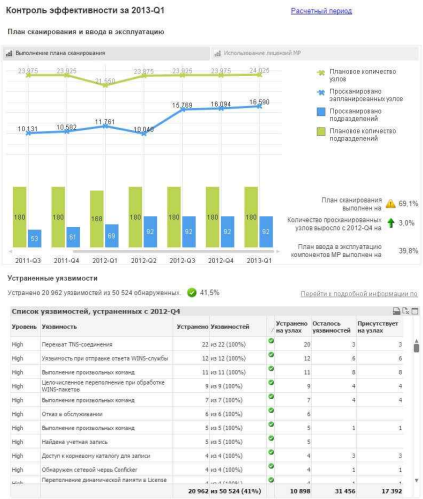
Удовлетворить все требования к новой системе могло только решение класса Business Intelligence. Анализ представленных на рынке BI-решений показал, что заданным требованиям оптимально соответствует платформа QlikView. Именно она и стала основой для системы бизнес-анализа Positive Technologies Reporting Portal (PT Reporting Portal).

«Оперативный анализ больших потоков данных становится критической задачей для современных средств безопасности, – рассказывает Борис Симис, заместитель генерального директора Positive Technologies по развитию бизнеса. – Многие из них собирают данные от тысяч



« Оперативный анализ больших потоков данных становится критической задачей для современных средств безопасности. Многие из них собирают данные от тысяч устройств и приложений, но без инструмента для анализа и наглядного представления данных практически невозможно обеспечить своевременное реагирование на обнаруженные угрозы ... »

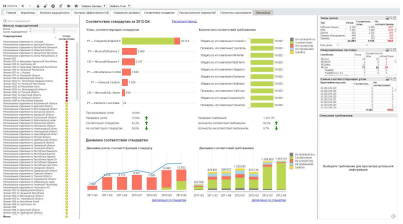
– Борис Симис, заместитель генерального директора Positive Technologies по развитию бизнеса



устройств и приложений, но без инструмента для анализа и наглядного представления данных практически невозможно обеспечить своевременное реагирование на обнаруженные угрозы. Именно поэтому мы выбрали технологию QlikView для создания системы бизнес-анализа событий безопасности PT Reporting Portal».

Одним из важнейших преимуществ платформы QlikView стали широкие возможности интеграции с любыми источниками данных и мощные инструменты обработки этих данных. Кроме того, сделать выбор в пользу данной платформы позволил и высокий уровень интерактивности пользовательского интерфейса в сочетании с принципом in-memory, при котором все данные хранятся в оперативной памяти. Это сочетание позволяет легко переходить с презентационных уровней отчетности к детальной информации по каждому факту, моментально проводить анализ «что если», изменяя условия расчетов ключевых показателей и мгновенно получая ожидаемые результаты.

Также платформа QlikView предоставляет инструменты для самостоятельного формирования выборок по большому числу различных измерений и быстрого получения данных по текущему состоянию или историческим трендам, и проведения расчётов ключевых показателей. Удобные механизмы расширения функциональности QlikView позволяют строить нестандартные визуализации данных, подстраиваясь под особенности конкретных клиентов. Плюсами платформы стали наличие как веб-интерфейса, так и мобильного доступа к построенным дашбордам, а также возможность формирования отторгаемой отчетности.

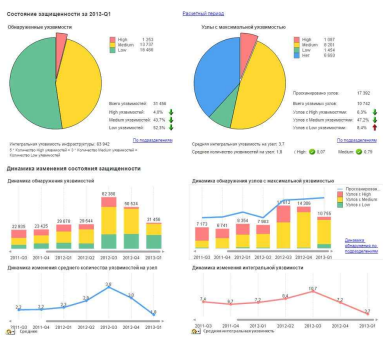


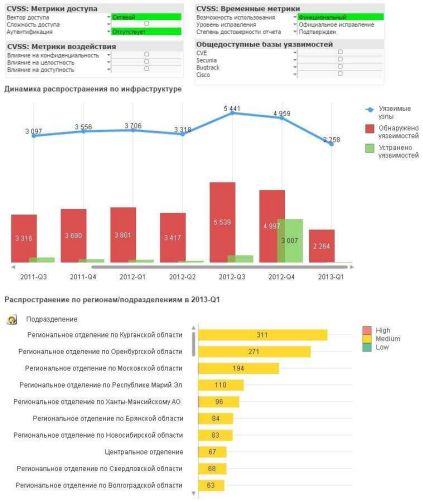
Дорога длиною в год

«Система бизнес-анализа событий безопасности PT Reporting Portal создавалось силами сотрудников Positive Technologies в течение одного года. Для создания концепции продукта нами использовалась версия QlikView Personal Edition, а уже после завершения этой работы мы обратились в компанию Qlik с предложением технологического партнёрства, – вспоминает Олег Матыков, руководитель отдела проектных решений Positive Technologies. – В процессе организации технологического партнёрства наши сотрудники прошли обучение на авторизованных курсах QlikView, а сотрудники Qlik проконсультировали по всем организационным, коммерческим и техническим вопросам по формированию совместного продукта. На время проведения первых пилотных проектов сотрудники Qlik оперативно предоставляли демонстрационные лицензии, что помогло в успешном завершении этих проектов».

В результате сотрудничества Positive Technologies и QlikView была создана система Positive Technologies Reporting Portal. Одна из ее ключевых особенностей — сочетание скорости и универсальность технологии обработки данных QlikView с одной стороны, а с другой — многолетнего опыта экспертов Positive Technologies.

В продукте PT Reporting Portal платформа QlikView интегрирована с СУБД Microsoft SQL, куда информация выгружается из PT MaxPatrol 8 в соответствии с установленным расписанием. Кроме того, к QlikView подключено некоторые количество конфигурационных файлов. В результате интеграции MaxPatrol и BI-системы пользователи PT Reporting Portal могут практически моментально получать информацию о защищённости своих информационных активов в





различных представлениях, подготовленных экспертами Positive Technologies. Возможности QlikView позволяют при необходимости адаптировать представления информации под требования заказчика.

Выход в люди

Впервые система бизнес-анализа событий безопасности PT Reporting Portal была представлена экспертному сообществу весной 2013 года на форуме по практической безопасности Positive Hack Days III.

«В результате выбора QlikView как технологической платформы для PT Reporting Portal нам удалось добиться необходимой даже самым требовательным заказчикам гибкости, отзывчивости интерфейса и удобства многопользовательского вывода информации о защищённости информационных активов», – резюмирует Максим Филиппов.

На данный момент ряд клиентов Positive Technologies активно используют PT Reporting Portal для оперативного получения аналитической информации обо всех аспектах защищённости своих информационных систем. Среди пользователей системы – ведущие российские банки, крупные госструктуры, предприятия энергетического сектора.

Positive Technologies планирует и дальше развивать сотрудничество с компанией Qlik и интегрировать систему PT Reporting Portal со своими новыми продуктами. В частности, уже закончена интеграция с системой мониторинга событий безопасности MaxPatrol SIEM, которая вышла на рынок в мае 2015 года.

«В результате выбора QlikView как технологической платформы для PT Reporting Portal нам удалось добиться необходимой даже самым требовательным заказчикам гибкости, отзывчивости интерфейса и удобства многопользовательского вывода информации о защищённости информационных активов»

– Максим Филиппов, директор по развитию бизнеса Positive Technologies в России.