



Пресс-релиз
27 августа 2015 г.

Группа QIWI

Пресс-служба

+7 (495) 980-06-83

karimov@bondstone.ru

pressa@qiwi.ru

www.qiwi.ru

www.facebook.com/QiwiRussia

Компания «Инфосистемы Джет»

Отдел PR

+7 (495) 411-76-01

pr@jet.msk.su

www.jet.msk.su

www.facebook.com/jetinfosystems.online

Компания «Инфосистемы Джет» внедрила систему контроля и мониторинга инцидентов информационной безопасности для Группы QIWI

27 августа 2015 г., Москва – Группа QIWI и компания «Инфосистемы Джет» запустили в эксплуатацию автоматизированную систему контроля и мониторинга инцидентов информационной безопасности в инфраструктуре платежного сервиса QIWI.

Система контроля и мониторинга инцидентов ИБ осуществляет централизованный сбор, корреляцию и анализ событий информационной безопасности со множества источников, а также автоматизирует процессы защиты баз данных. Система реализована на базе решений IBM Security QRadar SIEM и IBM Guardium. Ее внедрение позволило сократить время на поиск и анализ событий ИБ в распределенной инфраструктуре QIWI, осуществлять мониторинг запросов к базам данных и регистрацию событий информационной безопасности в СУБД, а также существенно повысить общий уровень защищенности корпоративной информационной инфраструктуры. Система также помогает обеспечивать соответствие международным стандартам, таким как PCI DSS и SOX.

«Внедрение системы контроля и мониторинга инцидентов ИБ стало серьезным шагом в развитии комплекса безопасности QIWI. Эта система позволяет в кратчайшие сроки реагировать на инциденты и отслеживать всю активность в нашей инфраструктуре. В совокупности с системой мониторинга баз данных комплекс позволяет обнаружить несанкционированную активность на самой ранней стадии», – сообщил директор по информационной безопасности Группы QIWI Кирилл Ермаков.

Проект охватил три московские площадки заказчика – два дата-центра и центральный офис. Специалисты компании «Инфосистемы Джет» провели предпроектное обследование инфраструктуры платежного сервиса QIWI, спроектировали и внедрили решения. К системе контроля и мониторинга инцидентов ИБ были подключены более 1800 источников событий свыше 20 различных типов. Согласно статистике, в день обрабатывается примерно 100 ГБ событий и 50 ГБ сетевого трафика.

Агенты IBM Guardium установлены на основные продуктивные и тестовые базы данных, реализован функционал маскирования (частичного сокрытия при отображении) выводимых критичных данных клиентов сервиса QIWI.

«Яркая особенность проекта с QIWI – большое количество подключенных источников. Часть из них являлись нестандартными, и потребовалась разработка специальных парсеров, – отмечает Евгений Акимов, директор по развитию бизнеса Центра информационной безопасности компании «Инфосистемы Джет». – Эта работа выполнялась в тесном взаимодействии с ИТ-администраторами и разработчиками, некоторые из систем QIWI были дополнительно оптимизированы под этот проект».

Единая консоль IBM QRadar позволяет в режиме, близком к реальному времени, анализировать информационные потоки, проходящие через систему контроля и мониторинга инцидентов ИБ, формировать отчеты, оповещения об инцидентах безопасности.

С целью оценки эффективности созданной системы Группой QIWI были организованы независимые работы по проведению внешнего и внутреннего анализа защищенности (pentest). По результатам проведенных тестов специалисты Группы QIWI высоко оценили возможности внедренной системы по обнаружению угроз ИБ и подозрительной активности в инфраструктурных системах.

Инфраструктура Группы QIWI очень динамична, постоянно расширяется – по мере появления новых систем они подключаются к системе контроля и мониторинга инцидентов информационной безопасности.

О компании QIWI plc.

QIWI – ведущий платежный сервис нового поколения в России и странах СНГ, которому принадлежит интегрированная платежная сеть, позволяющая производить платежи по физическим, интернет- и мобильным каналам связи. Она включает свыше 17,3 млн виртуальных кошельков и более 177 000 терминалов и точек приема платежей. С помощью QIWI торговые компании принимают платежи (в денежной и электронной форме) на сумму свыше 50 млрд руб. от более чем 70 млн клиентов, которые пользуются услугами сети не реже одного раза в месяц. Клиенты QIWI могут использовать наличные, предоплаченные карты и другие способы безналичных расчетов для заказа и оплаты товаров и услуг, используя физические и электронные платежные инструменты попеременно.

О компании «Инфосистемы Джет»

Компания «Инфосистемы Джет» – один из крупнейших российских системных интеграторов – образована в 1991 году. Основные направления деятельности компании: бизнес-решения и программные разработки, ИТ- и телекоммуникационная инфраструктура, информационная безопасность, ИТ-аутсорсинг и техническая поддержка, управление комплексными проектами и др. Компания располагает 10 региональными офисами в России и СНГ, ведет ряд проектов в других странах.

Дополнительная информация доступна на www.jet.su, www.facebook.com/jetinfosystems.online, www.twitter.com/JetInfosystems.