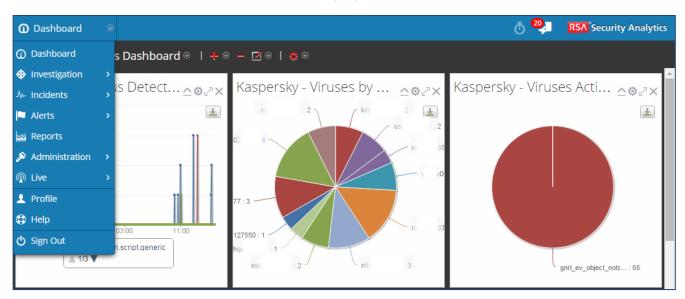


# Сбор, хранение и обработка событий информационной безопасности с помощью RSA Security Analytics

Заказчик: российский дочерний банк одной из крупнейших банковских групп в еврозоне.

**Назначение проекта:** автоматизация процессов централизованного сбора, накопления и обработки событий от компонентов ИТ-инфраструктуры Заказчика и сетевых пакетов.



#### Цели выполнения проекта:

- создание единого центра сбора событий
- возможность ретроспективного анализа состояния ИТ-инфраструктуры с точки зрения событий
- своевременное выявление инцидентов ИБ, построенных на основе полученных событий
- сокращение времени реакции на события / инциденты
- обеспечение информационно-аналитической поддержки деятельности по управлению ИБ
- оптимизация функционирования ИТ-инфраструктуры по результатам анализа событий

## Масштаб проекта: компоненты ИТ-инфраструктуры, включенные в процесс управления событиями

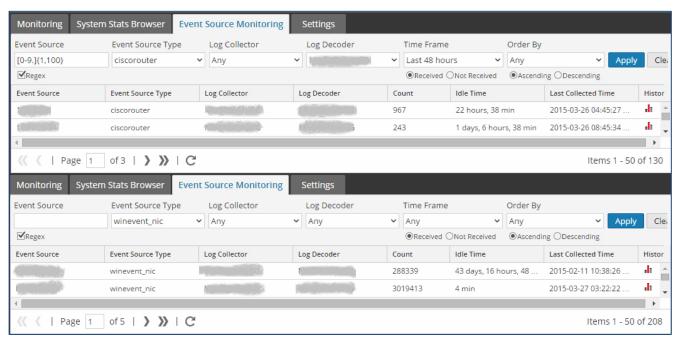
- активное сетевое оборудование (коммутаторы, маршрутизаторы) более 200 единиц
- серверы с ОС Microsoft Windows более 200 единиц
- система предотвращения утечек конфиденциальной информации Symantec DLP
- средство виртуализации VMware ESXi
- средство централизованного управления антивирусом Kaspersky Security Center

### Способы и методы сбора событий

- Windows Event Log посредством WMI
- протокол Syslog
- протокол JDBC







#### В рамках проекта проведены следующие работы:

- установка компонентов в серверные стойки, коммутация, инициализация компонентов (в составе системы используются три аппаратных сервера)
- обновление программного обеспечения до последней версии
- создание пользователей, разграничение прав доступа пользователей
- консультирование персонала Заказчика по администрированию и настройке системы
- формирование информационных панелей с учетом требований Заказчика
- разработка инструкций по подключению и контроль подключения источников событий с выявлением ошибок в настройках
- разработка фильтров для событий и сетевых пакетов для экономии объемов жесткого диска
- разработка отчетов, правил, уведомлений под требования заказчика
- подготовка проектной документации

#### В результате внедрения системы заказчик получил:

- видимость событий со средств защиты информации в «одном окне»
- уведомление о наиболее критичных событиях ИТ-инфраструктуры на электронную почту
- формирование ретроспективных выборок (отчетов) по критичным категориям событий
- отслеживание действий определенных категорий пользователей
- отслеживание действий над определенными объектами в ИТ-инфраструктуре
- сокращение времени реакции на события в ИТ-инфраструктуре
- понимание структуры сетевого трафика и дополнительный канал визуализации действий сотрудников и/или внешних нарушителей

