105318 г. Москва, ул. Ибрагимова, д.31
тел./факс+7 (495) 663-95-16
http://www.ntc-vulkan.ru
info@ntc-vulkan.ru

# Результаты подключения АПКШ «Континент» к SIEM-решению RSA Security Analytics

## Введение

Аппаратно-программный комплекс шифрования (АПКШ) «Континент» производства ООО «Код Безопасности»[1] является штатно неподдерживаемым источником событий для большинства существующих на рынке решений класса Security Information and Event Management (SIEM), в том числе продукта RSA Security Analytics производства RSA, The Security Division of EMC[2].

Команда НТЦ «Вулкан», являющегося авторизованным партнером обоих производителей, произвела интеграцию данных решений между собой, результаты которой представлены в настоящем документе.

## Подготовка данных

Примеры событий от АПКШ «Континент», записанные в базу данных, обслуживаемую с использованием СУБД Microsoft SQL Server, представлены на рисунке ниже (см. Рисунок 1).

| | CG_NAME | SL_CATEGORY | SL_TIMEGENERATED | SL_DATASHORT |
|---|---|---|---|---|
| 1 | ЦУС | 40 | 2016-02-12 07:10:13.000 | 0x540000000100000000000000000000000200000080D0C028... |
| 2 | ЦУС | 40 | 2016-02-12 07:38:56.000 | 0x5E00000000000000C2F1F2F0EEE5EDEDFBE920E0E4ECE8E... |
| 3 | КШ с ЦУСом | 35 | 2016-02-12 07:40:35.000 | 0x6D000000C2F1F2F0EEE5EDEDFBE920E0E4ECE8EDE8F1F2... |
| 4 | ЦУС | 40 | 2016-02-12 07:42:55.000 | 0x540000000100000000000000000000000200000090E0C028... |
| 5 | КШ с ЦУСом | 40 | 2016-02-12 07:42:13.000 | 0x540000000100000000000000000000000525649534F52000000... |
| 6 | ЦУС | 35 | 2016-02-12 07:45:27.000 | 0xD0000000C2F1F2F0EEE5EDEDFBE920E0E4ECE8EDE8F1F2... |
| 7 | ЦУС | 40 | 2016-02-12 07:58:00.000 | 0x5F00000000000000C2F1F2F0EEE5EDEDFBE920E0E4ECE8E... |
| 8 | ЦУС | 40 | 2016-02-12 08:15:26.000 | 0x5E00000000000000C2F1F2F0EEE5EDEDFBE920E0E4ECE8E... |
| 9 | КШ с ЦУСом | 35 | 2016-02-12 08:19:08.000 | 0x74000000C2F1F2F0EEE5EDEDFBE920E0E4ECE8EDE8F1F2F... |
| 10 | КШ с ЦУСом | 35 | 2016-02-12 08:19:08.000 | 0x9C000000C2F1F2F0EEE5EDEDFBE920E0E4ECE8EDE8F1F2F... |
| 11 | КШ с ЦУСом | 35 | 2016-02-12 08:19:08.000 | 0x53000000C2F1F2F0EEE5EDEDFBE920E0E4ECE8EDE8F1F2F... |

Рисунок 1 – Исходный вид событий от АПКШ «Континент»

Особенностью ведения сертифицированным по требованиям безопасности информации крипто-шлюзом журналов аудита является кодирование значений ряда полей события.

Примеры событий от АПКШ «Континент», выгруженных с использованием СУБД Microsoft SQL Server и раскодированных силами команды НТЦ «Вулкан», представлены на рисунке ниже (см. Рисунок 2).

В данном представлении события по протоколу Syslog были направлены в RSA Security Analytics.

[1] Подробнее: http://www.securitycode.ru/products/group_kontinent/
[2] Подробнее: http://www.ntc-vulkan.ru/tsentr-kompetentsii/siem#rsa-security-analytics

```
continent;40;2016-02-12 07:10:13;ЦУС;Сеть Континент;Включение КШ;1;0.0.0.0;
continent;40;2016-02-12 07:38:56;ЦУС;Сеть Континент;Подключение администратора ПУ ЦУС к ЦУС;Встроенный администратор;
continent;35;2016-02-12 07:40:35;КШ с ЦУСом;Управляющая команда;Встроенный администратор;Перезагрузить КШ;Успешно;
continent;40;2016-02-12 07:42:55;ЦУС;Сеть Континент;Включение КШ;1;0.0.0.0;
continent;40;2016-02-12 07:42:13;КШ с ЦУСом;Сеть Континент;Включение КШ;1;0.0.0.0;
continent;35;2016-02-12 07:45:27;ЦУС;Управляющая команда;Встроенный администратор;Добавление лицензии;Успешно;
continent;40;2016-02-12 07:58:00;ЦУС;Сеть Континент;Отключение администратора ПУ ЦУС от ЦУС;Встроенный администратор;
continent;40;2016-02-12 08:15:26;ЦУС;Сеть Континент;Подключение администратора ПУ ЦУС к ЦУС;Встроенный администратор;
continent;35;2016-02-12 08:19:08;КШ с ЦУСом;Управляющая команда;Встроенный администратор;Установить режим работы интерфейса
continent;35;2016-02-12 08:19:08;КШ с ЦУСом;Управляющая команда;Встроенный администратор;Установить тип интерфейса;Успешно
continent;35;2016-02-12 08:19:08;КШ с ЦУСом;Управляющая команда;Встроенный администратор;Добавить адрес на интерфейс;Успеш
continent;35;2016-02-12 08:40:20;ЦУС;Управляющая команда;Встроенный администратор;Создание сетевого объекта;Успешно;
continent;40;2016-02-12 10:44:42;ЦУС;Сеть Континент;Отключение администратора ПУ ЦУС от ЦУС;Встроенный администратор;
continent;40;2016-02-15 09:15:15;ЦУС;Сеть Континент;Включение КШ;1;0.0.0.0;
continent;40;2016-02-15 09:14:33;КШ с ЦУСом;Сеть Континент;Включение КШ;1;0.0.0.0;
continent;40;2016-02-15 09:17:05;ЦУС;Сеть Континент;Подключение администратора ПУ ЦУС к ЦУС;Встроенный администратор;
continent;35;2016-02-15 09:17:51;КШ с ЦУСом;Управляющая команда;Встроенный администратор;Установить режим работы интерфейса
continent;35;2016-02-15 09:17:51;КШ с ЦУСом;Управляющая команда;Встроенный администратор;Добавить адрес на интерфейс;Успеш
continent;35;2016-02-15 09:18:52;КШ с ЦУСом;Управляющая команда;Встроенный администратор;Установить режим работы интерфейса
continent;35;2016-02-15 09:18:52;КШ с ЦУСом;Управляющая команда;Встроенный администратор;Удалить адрес с интерфейса;Успешно
continent;35;2016-02-15 09:21:23;ЦУС;Управляющая команда;Встроенный администратор;Изменение сетевого объекта;Успешно;
continent;35;2016-02-15 09:25:07;ЦУС;Управляющая команда;Встроенный администратор;Создание сетевого объекта;Успешно;
continent;35;2016-02-15 09:29:41;ЦУС;Управляющая команда;Встроенный администратор;Создание сетевого объекта;Успешно;
continent;35;2016-02-15 09:30:47;ЦУС;Управляющая команда;Встроенный администратор;Создание сетевого объекта;Успешно;
```

Рисунок 2 – Выгруженные и раскодированные события от АПКШ «Континент»

**Обработка данных**

Пример разбора событий на основе мета-данных в консоли RSA Security Analytics в разделе *Investigation* представлены на рисунках ниже (см. Рисунок 3 и Рисунок 4).

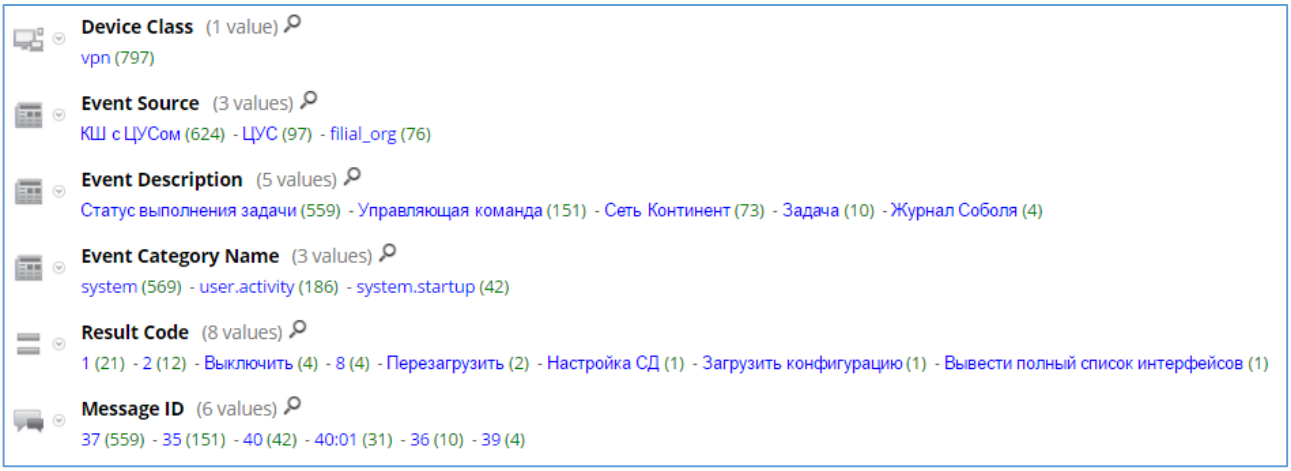


Рисунок 3 – Мета-данные в RSA Security Analytics в разделе *Investigation* – 1

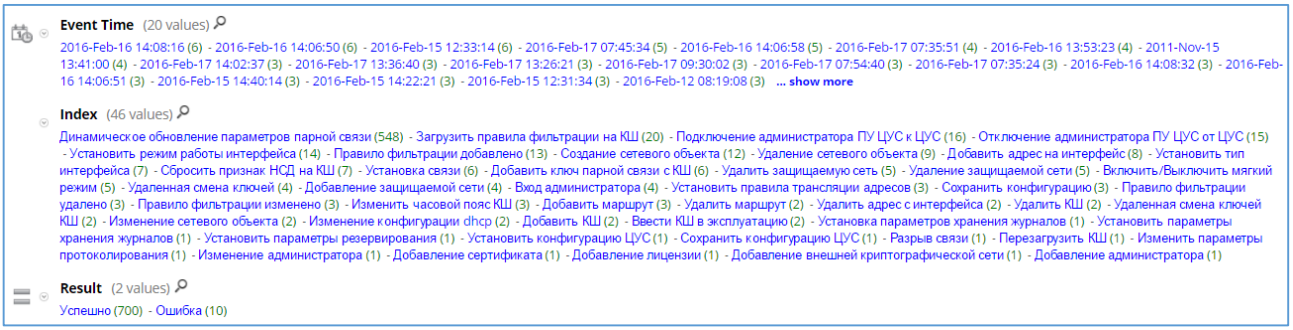


Рисунок 4 – Мета-данные в RSA Security Analytics в разделе *Investigation* – 2

Пример просмотра нормализованного события от АПКШ «Континент» представлен на рисунке ниже (см. Рисунок 5).

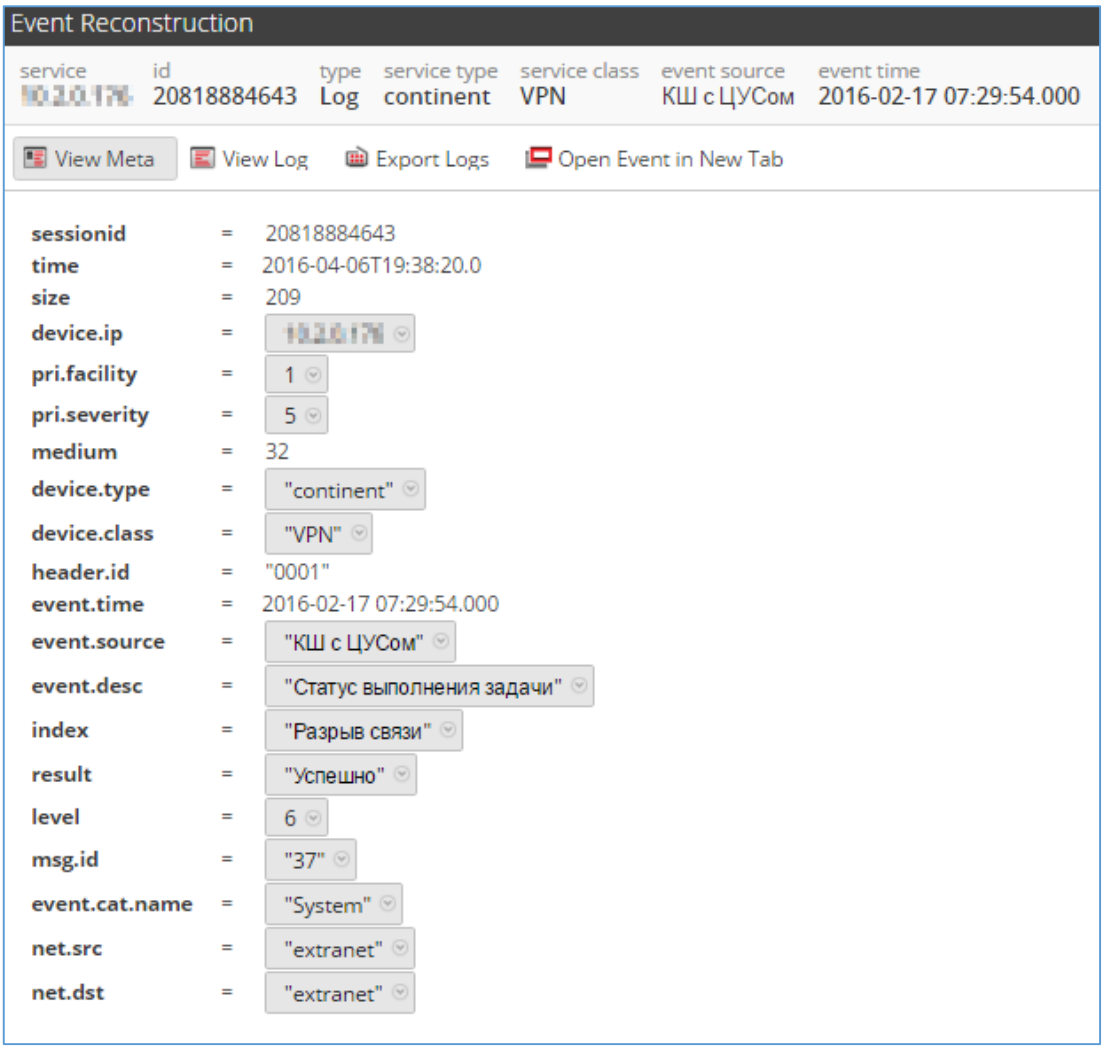


Рисунок 5 – Нормализованное событие от АПКШ «Континент»

Проведенная нормализация позволяет использовать функционал поиска, фильтрации, корреляции и построения отчетности на базе стандартизированных полей сообщения, тем самым обеспечивает унифицированные процедуры работы специалистов по защите информации с событиями, полученными от различных источников событий. При этом сохраняется возможность просмотра события в исходном виде (RAW-формате), см. Рисунок 6.

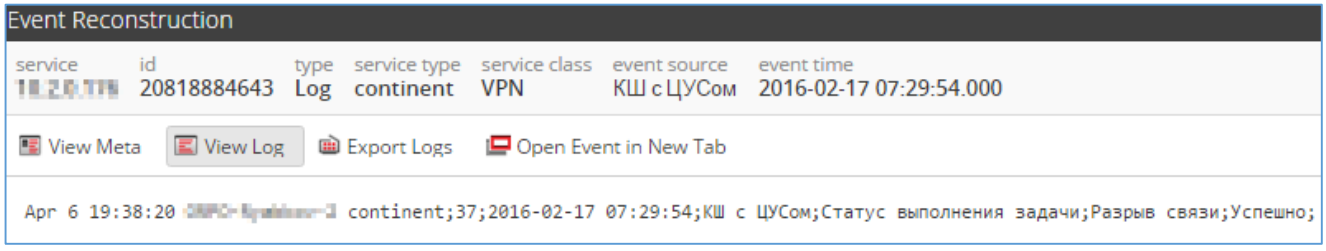


Рисунок 6 – Событие в исходном виде

Примеры различных форм отчетов в RSA Security Analytics приведены на рисунках ниже:

– табличный отчет – «Выключение АПКШ «Континент» (см. Рисунок 7);

– гистограмма – «Вход администратора, сгруппированный по устройствам» (см. Рисунок 8);

– табличный отчет – «Результат выполнения операции – ошибка» (см. Рисунок 9);

– круговая диаграмма – «Результат выполнения операции – ошибка» (см. Рисунок 10).

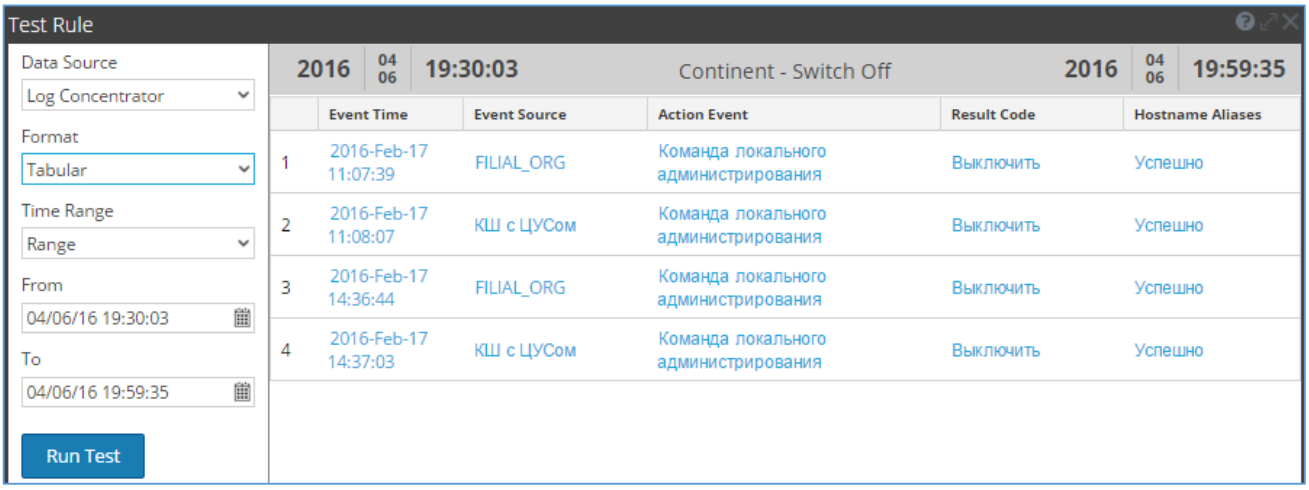


Рисунок 7 – Отчет – «Выключение АПКШ «Континент»

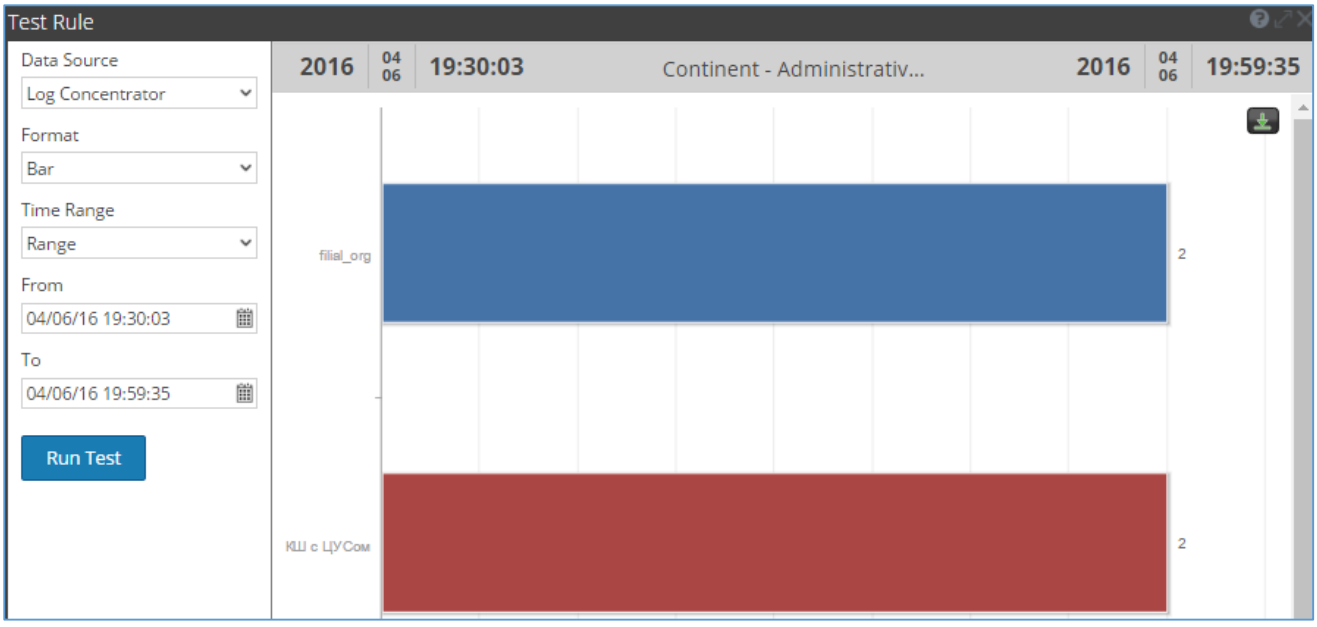


Рисунок 8 – Отчет – «Вход администратора, сгруппированный по устройствам»

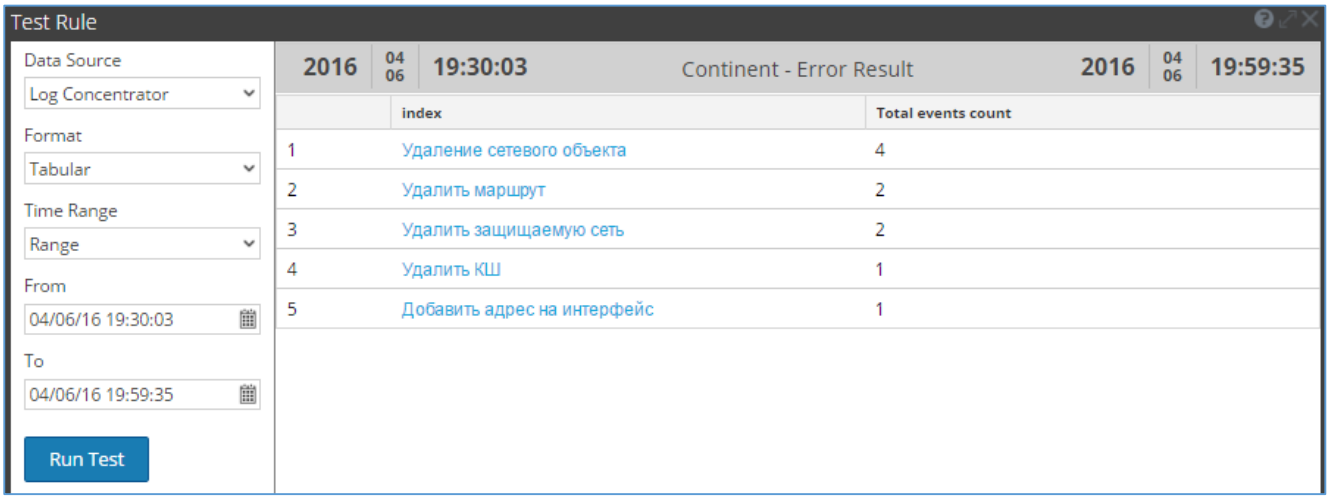


Рисунок 9 – Отчет – «Результат выполнения операции – ошибка»

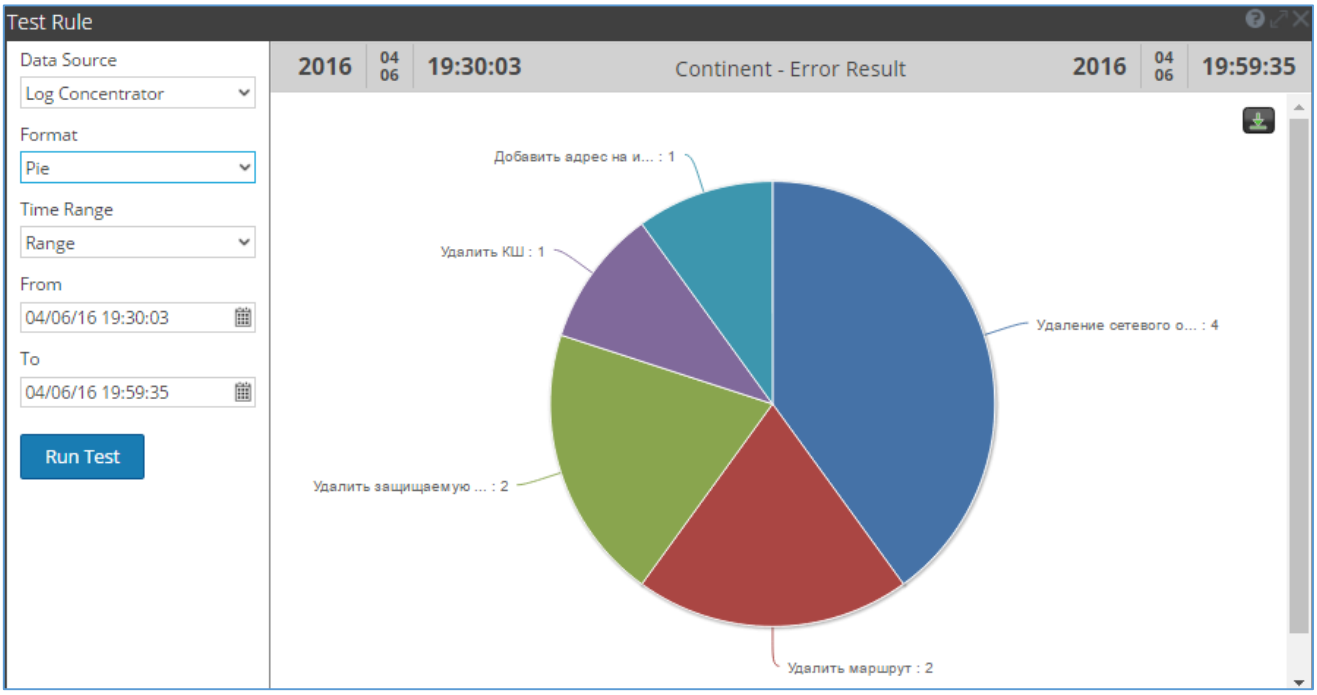


Рисунок 10 – Отчет – «Результат выполнения операции – ошибка»

Ниже приведены результаты использования корреляционного движка RSA Security Analytics для выявления «аномальных» событий от АПКШ «Континент». В качестве «аномального» события рассматривается добавление и/или удаление правила фильтрации в течение 5 минут. Ниже отображены примеры срабатывания данного правила и варианты его отображения в интерфейсе RSA Security Analytics (см. Рисунок 11 – Рисунок 13).

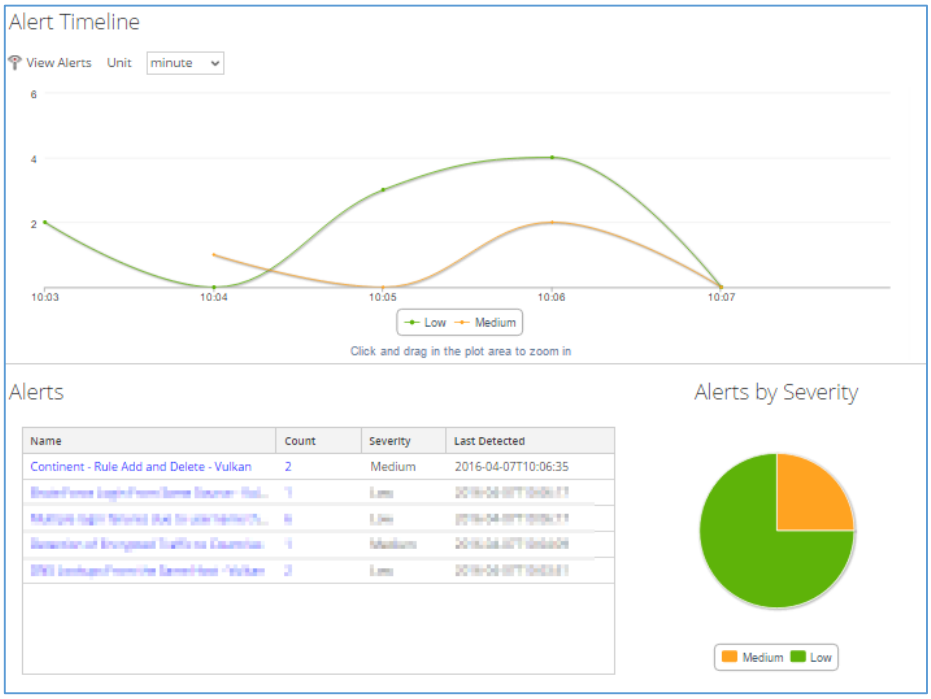


Рисунок 11 – Общая статистика по корреляционному правилу

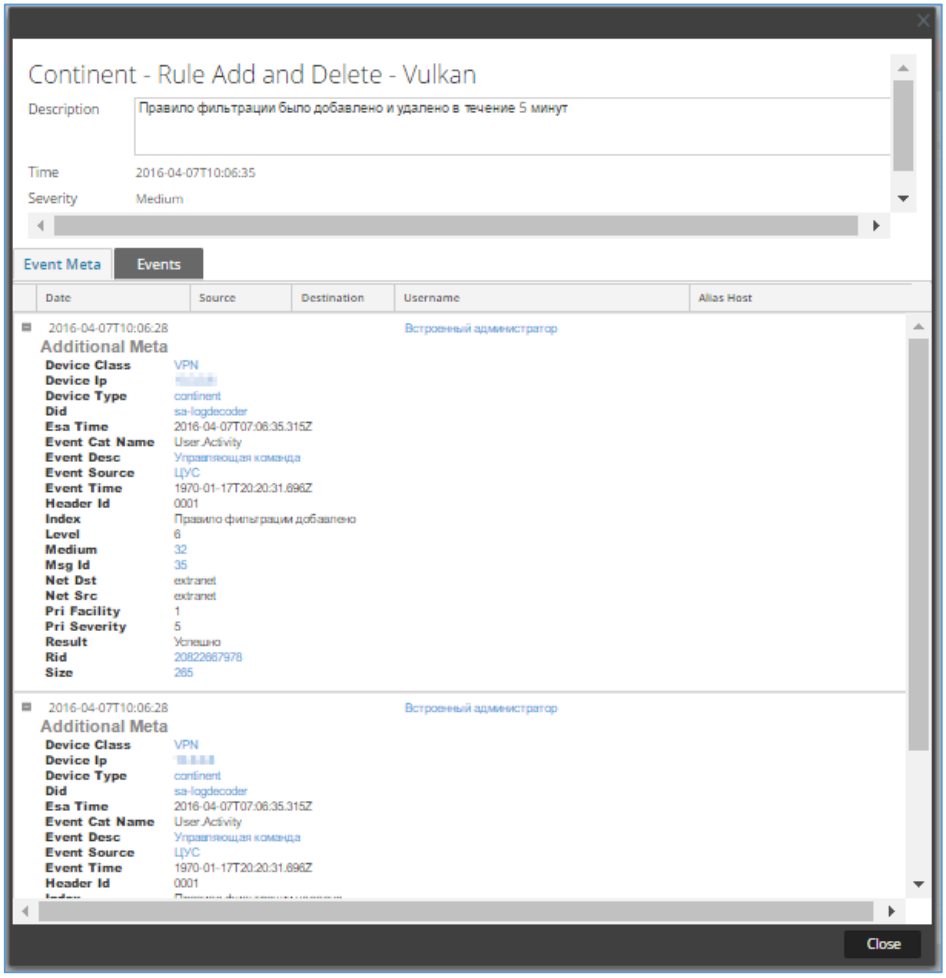


Рисунок 12 – Просмотр мета-данных событий

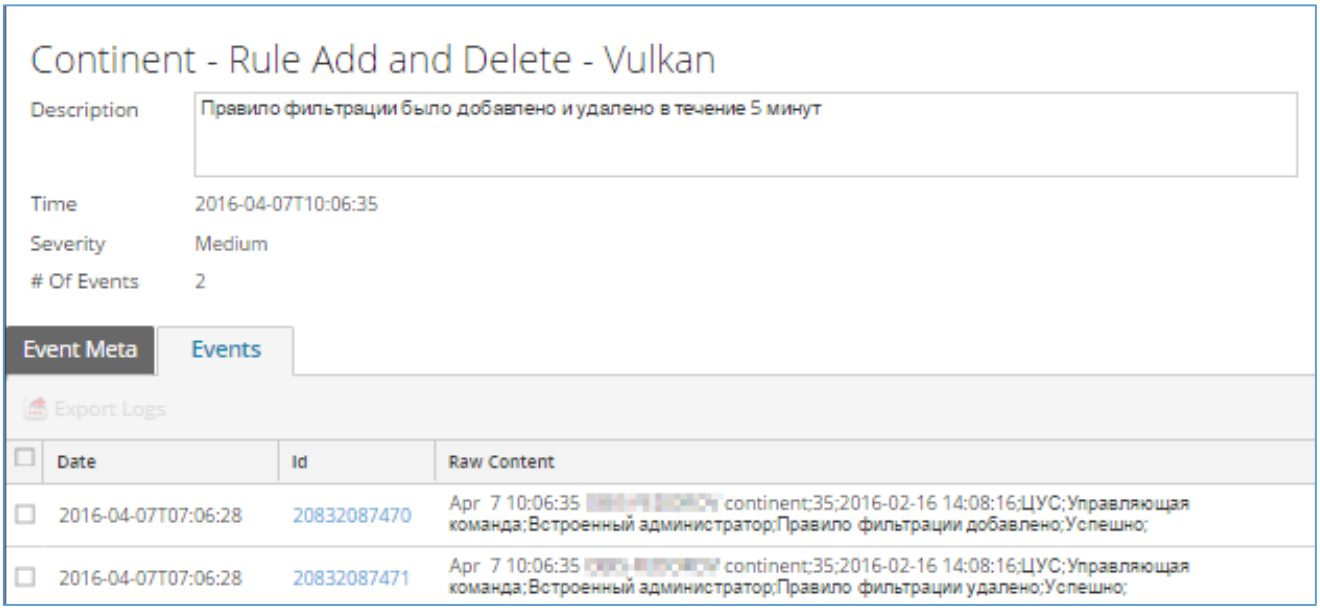


Рисунок 13 – Просмотр исходных событий

На рисунке ниже приведен пример уведомления на электронную почту заинтересованных лиц о срабатывании соответствующего корреляционного правила (см. Рисунок 14).

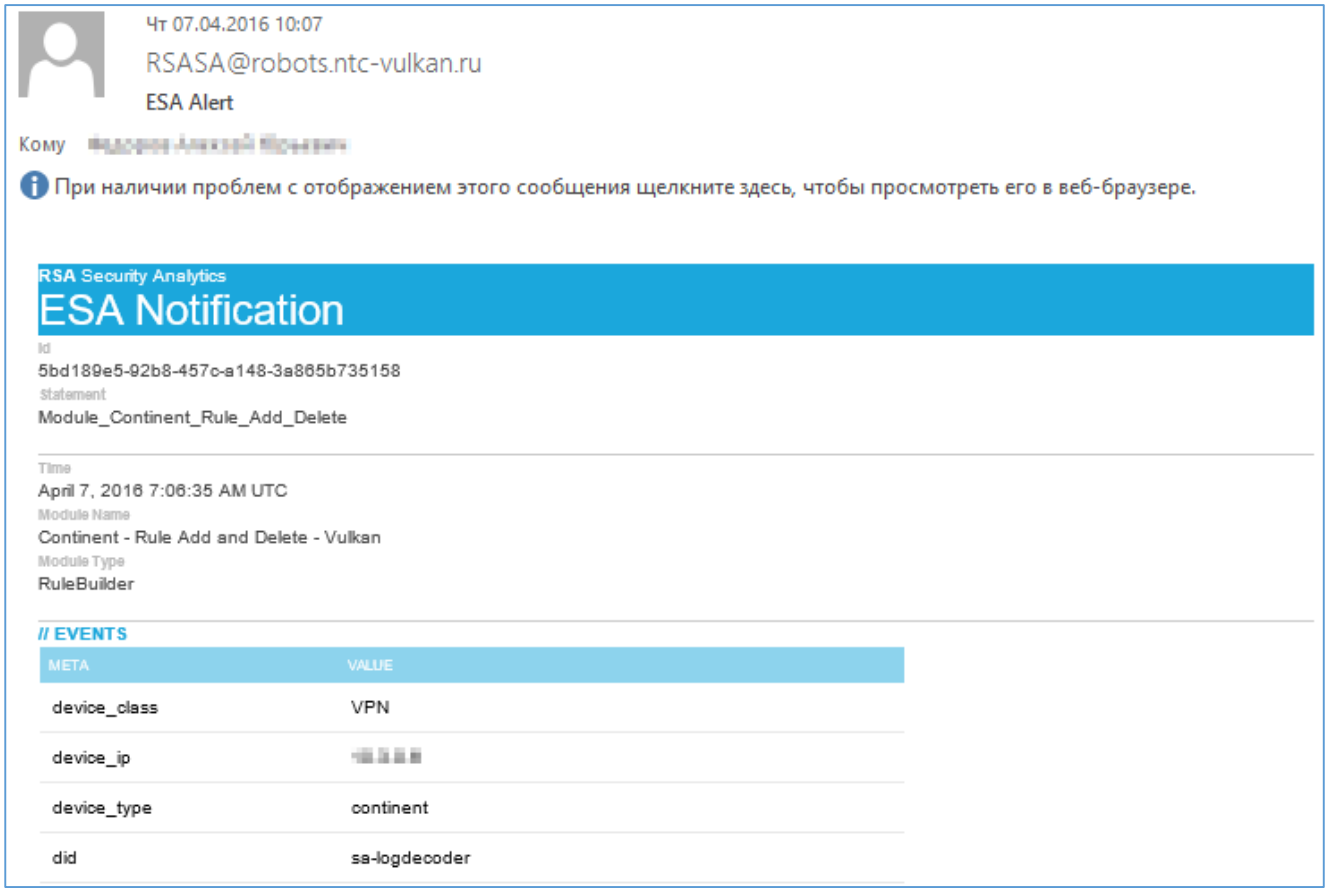


Рисунок 14 – Пример уведомления