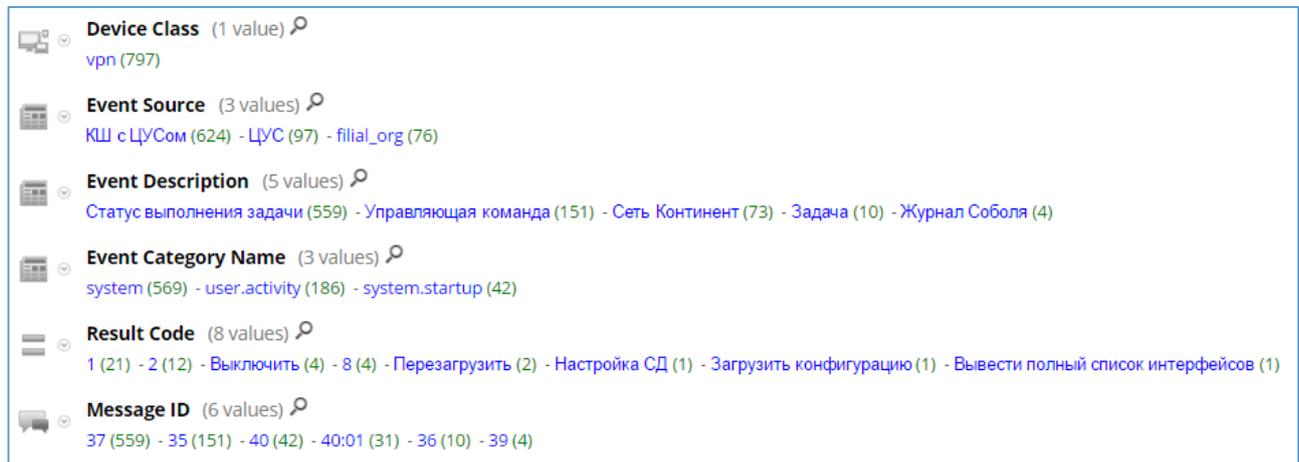



```
continent;40;2016-02-12 07:10:13;ЦУС;Сеть Континент;Включение КШ;1;0.0.0.0;
continent;40;2016-02-12 07:38:56;ЦУС;Сеть Континент;Подключение администратора ПУ ЦУС к ЦУС;Встроенный администратор;
continent;35;2016-02-12 07:40:35;КШ с ЦУСом;Управляющая команда;Встроенный администратор;Перезагрузить 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;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;Успешно;
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).



Device Class (1 value)  vpn (797)

Event Source (3 values)  КШ с ЦУСом (624) - ЦУС (97) - filial_org (76)

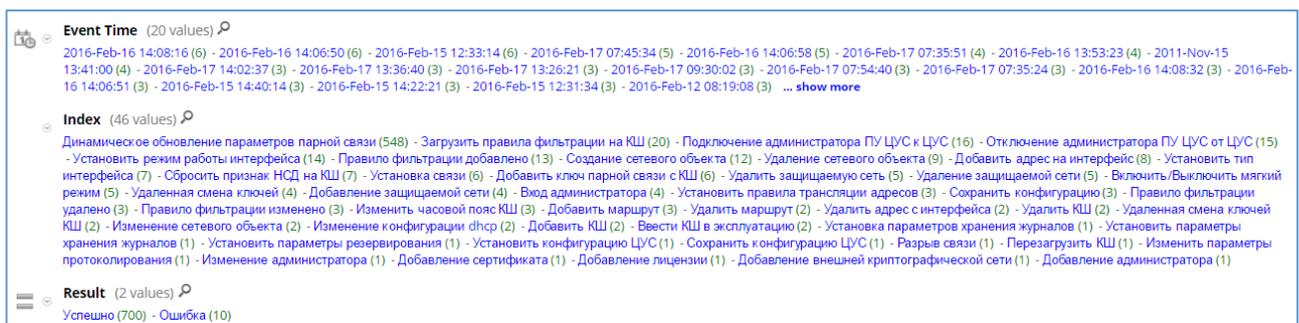
Event Description (5 values)  Статус выполнения задачи (559) - Управляющая команда (151) - Сеть Континент (73) - Задача (10) - Журнал Соболя (4)

Event Category Name (3 values)  system (569) - user.activity (186) - system.startup (42)

Result Code (8 values)  1 (21) - 2 (12) - Выключить (4) - 8 (4) - Перезагрузить (2) - Настройка СД (1) - Загрузить конфигурацию (1) - Вывести полный список интерфейсов (1)

Message ID (6 values)  37 (559) - 35 (151) - 40 (42) - 40:01 (31) - 36 (10) - 39 (4)

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



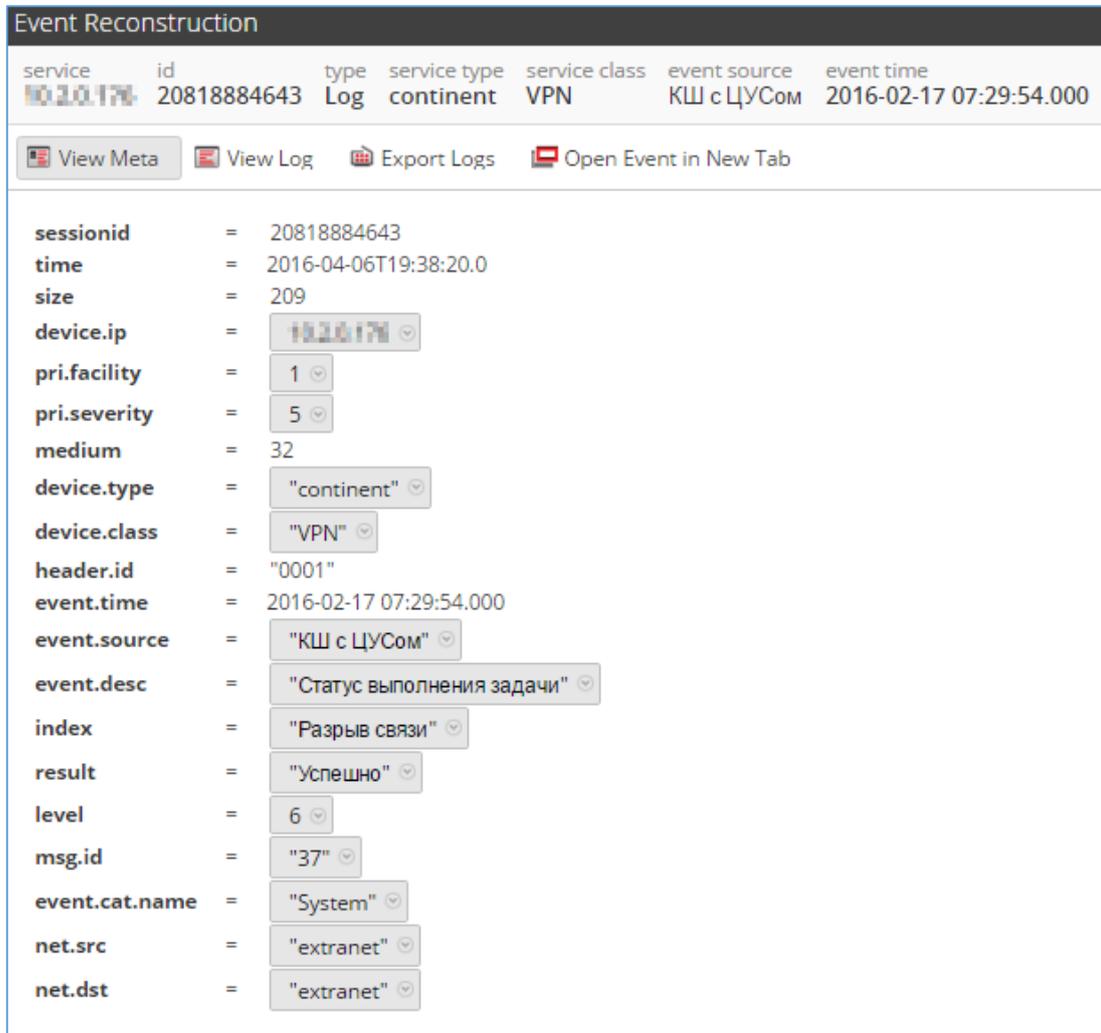
Event Time (20 values)  2016-Feb-16 14:08:16 (6) - 2016-Feb-16 14:06:50 (6) - 2016-Feb-15 12:33:14 (6) - 2016-Feb-17 07:45:34 (5) - 2016-Feb-16 14:06:58 (5) - 2016-Feb-17 07:35:51 (4) - 2016-Feb-16 13:53:23 (4) - 2011-Nov-15 13:41:00 (4) - 2016-Feb-17 14:02:37 (3) - 2016-Feb-17 13:36:40 (3) - 2016-Feb-17 13:26:21 (3) - 2016-Feb-17 09:30:02 (3) - 2016-Feb-17 07:54:40 (3) - 2016-Feb-17 07:35:24 (3) - 2016-Feb-16 14:08:32 (3) - 2016-Feb-16 14:06:51 (3) - 2016-Feb-15 14:40:14 (3) - 2016-Feb-15 14:22:21 (3) - 2016-Feb-15 12:31:34 (3) - 2016-Feb-12 08:19:08 (3) - ... [show more](#)

Index (46 values)  Динамическое обновление параметров парной связи (548) - Загрузить правила фильтрации на КШ (20) - Подключение администратора ПУ ЦУС к ЦУС (16) - Отключение администратора ПУ ЦУС от ЦУС (15) - Установить режим работы интерфейса (14) - Правило фильтрации добавлено (13) - Создание сетевого объекта (12) - Удаление сетевого объекта (9) - Добавить адрес на интерфейс (8) - Установить тип интерфейса (7) - Сбросить признак НСД на КШ (7) - Установка связи (6) - Добавить ключ парной связи с КШ (6) - Удалить защищаемую сеть (5) - Включить/Выключить маячки режим (5) - Удаленная смена ключей (4) - Добавление защищаемой сети (4) - Вход администратора (4) - Установить правила трансляции адресов (3) - Сохранить конфигурацию (3) - Правило фильтрации удалено (3) - Правило фильтрации изменено (3) - Изменить часовой пояс КШ (3) - Добавить маршрут (3) - Удалить маршрут (2) - Удалить адрес с интерфейса (2) - Удаленная смена ключей КШ (2) - Изменение сетевого объекта (2) - Изменение конфигурации dhcp (2) - Добавить КШ (2) - Вести КШ в эксплуатацию (2) - Установка параметров хранения журналов (1) - Установить параметры хранения журналов (1) - Установить параметры резервирования (1) - Установить конфигурацию ЦУС (1) - Сохранить конфигурацию ЦУС (1) - Разрыв связи (1) - Перезагрузить КШ (1) - Изменить параметры протоколирования (1) - Изменение администратора (1) - Добавление сертификата (1) - Добавление лицензии (1) - Добавление внешней криптографической сети (1) - Добавление администратора (1)

Result (2 values)  Успешно (700) - Ошибка (10)

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).



service	id	type	service type	service class	event source	event time
10.20.170	20818884643	Log	continent	VPN	КШ с ЦУСом	2016-02-17 07:29:54.000

[View Meta](#)
[View Log](#)
[Export Logs](#)
[Open Event in New Tab](#)

```

sessionid = 20818884643
time = 2016-04-06T19:38:20.0
size = 209
device.ip = 10.20.170
pri.facility = 1
pri.severity = 5
medium = 32
device.type = "continent"
device.class = "VPN"
header.id = "0001"
event.time = 2016-02-17 07:29:54.000
event.source = "КШ с ЦУСом"
event.desc = "Статус выполнения задачи"
index = "Разрыв связи"
result = "Успешно"
level = 6
msg.id = "37"
event.cat.name = "System"
net.src = "extranet"
net.dst = "extranet"
    
```

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.



service	id	type	service type	service class	event source	event time
10.20.170	20818884643	Log	continent	VPN	КШ с ЦУСом	2016-02-17 07:29:54.000

[View Meta](#)
[View Log](#)
[Export Logs](#)
[Open Event in New Tab](#)

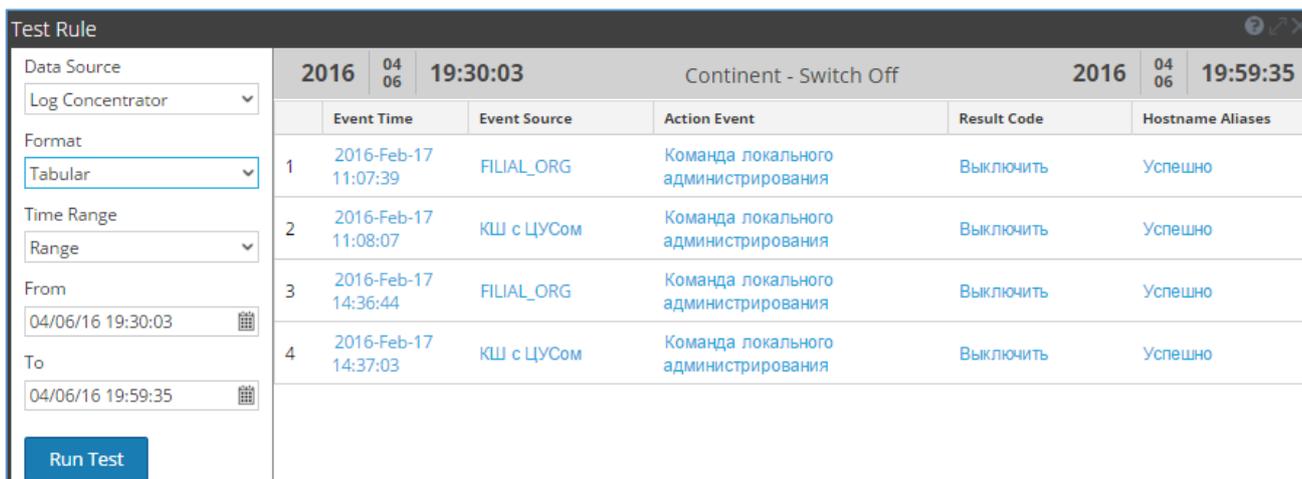
```

Apr 6 19:38:20 2016-04-06T19:38:20.0 continent;37;2016-02-17 07:29:54;КШ с ЦУСом;Статус выполнения задачи;Разрыв связи;Успешно;
    
```

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).



2016 04 06 19:30:03		Continent - Switch Off		2016 04 06 19:59:35	
	Event Time	Event Source	Action Event	Result Code	Hostname Aliases
1	2016-Feb-17 11:07:39	FILIAL_ORG	Команда локального администрирования	Выключить	Успешно
2	2016-Feb-17 11:08:07	КШ с ЦУСом	Команда локального администрирования	Выключить	Успешно
3	2016-Feb-17 14:36:44	FILIAL_ORG	Команда локального администрирования	Выключить	Успешно
4	2016-Feb-17 14:37:03	КШ с ЦУСом	Команда локального администрирования	Выключить	Успешно

Рисунок 7 – Отчет – «Выключение АПКШ «Континент»

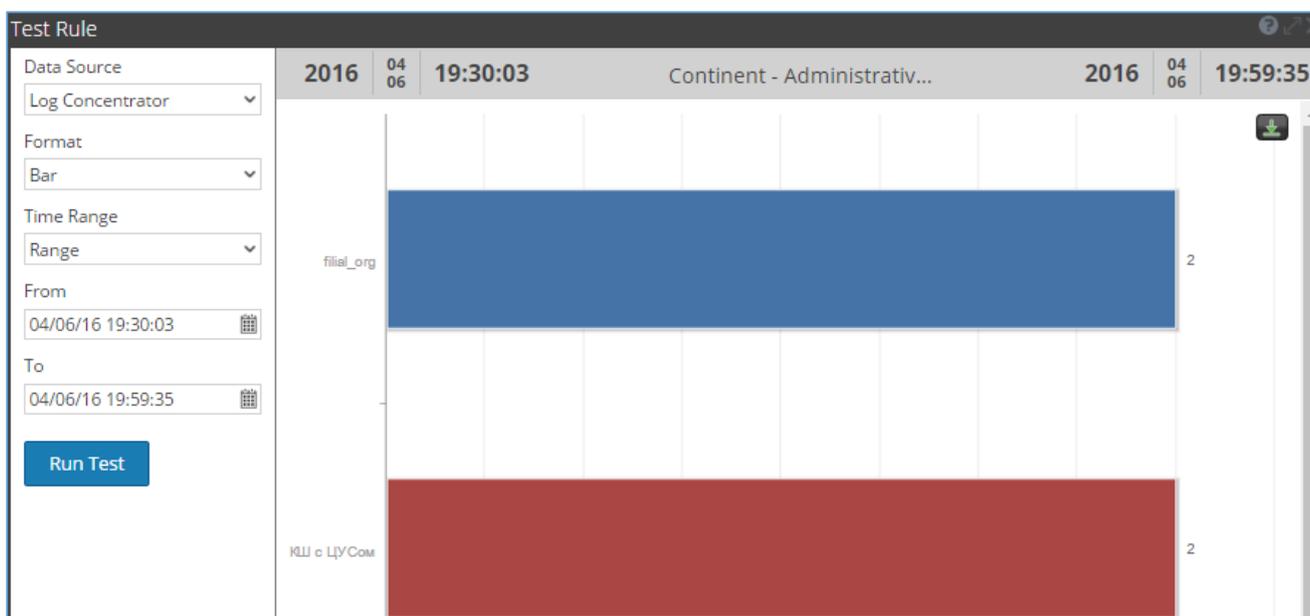


Рисунок 8 – Отчет – «Вход администратора, сгруппированный по устройствам»

Test Rule

Data Source: Log Concentrator

Format: Tabular

Time Range: Range

From: 04/06/16 19:30:03

To: 04/06/16 19:59:35

Run Test

2016 04 06 19:30:03		Continent - Error Result		2016 04 06 19:59:35	
	index		Total events count		
1	Удаление сетевого объекта		4		
2	Удалить маршрут		2		
3	Удалить защищаемую сеть		2		
4	Удалить КШ		1		
5	Добавить адрес на интерфейс		1		

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

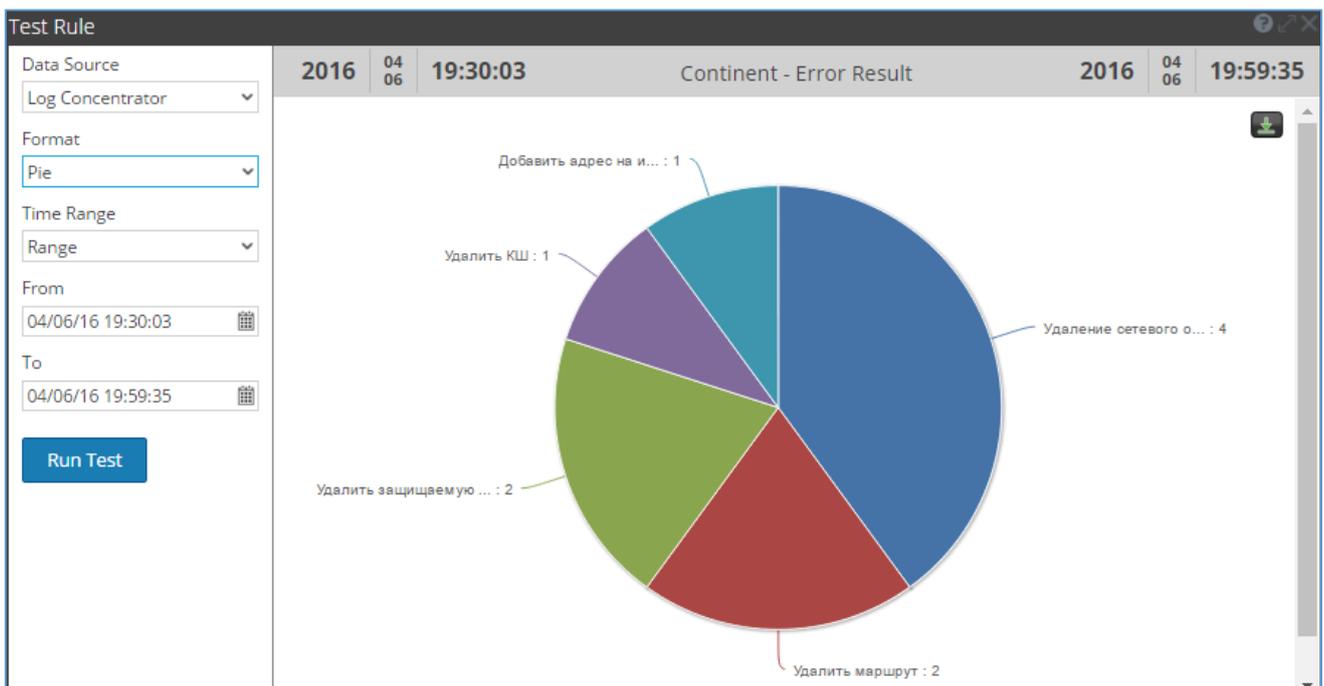


Рисунок 10 – Отчет – «Результат выполнения операции – ошибка»

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).

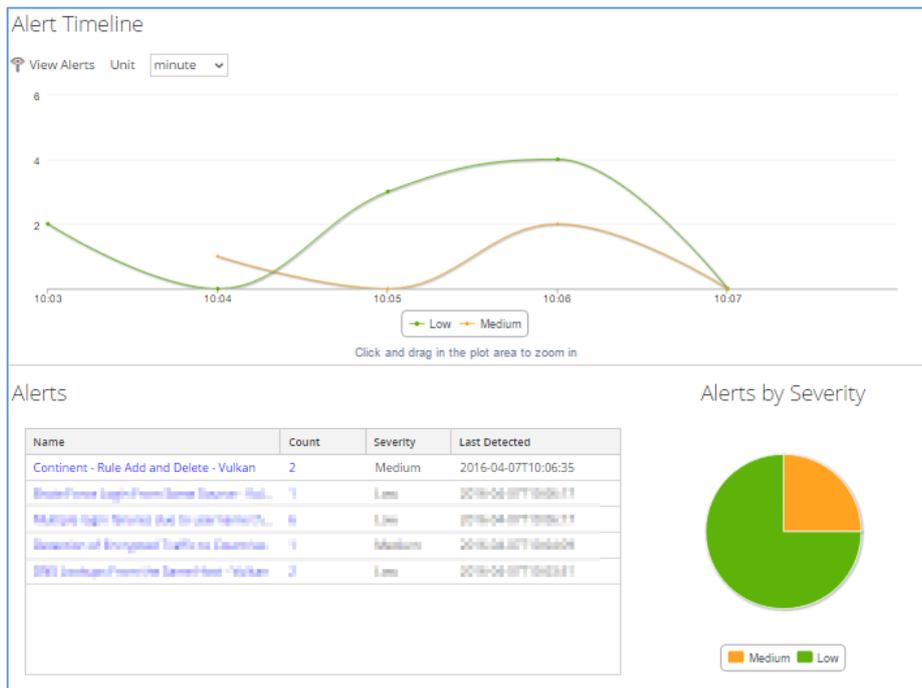
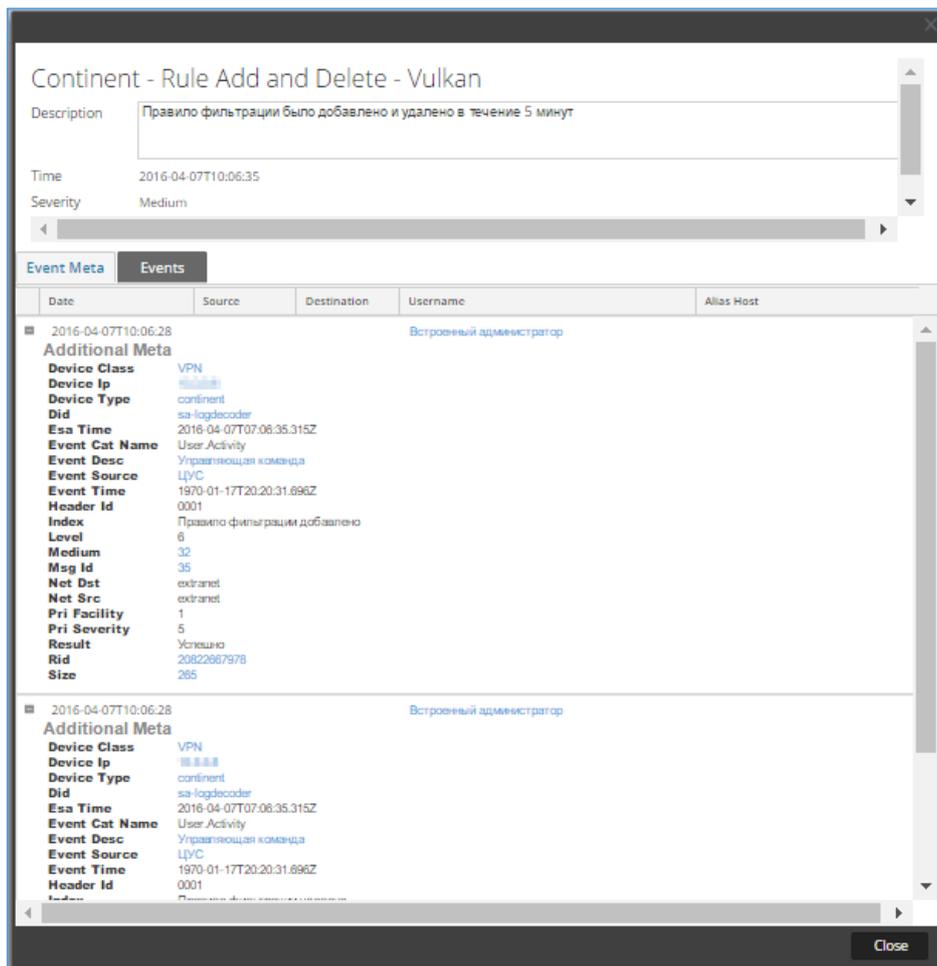


Рисунок 11 – Общая статистика по корреляционному правилу



Continent - Rule Add and Delete - Vulkan

Description: Правило фильтрации было добавлено и удалено в течение 5 минут

Time: 2016-04-07T10:06:35

Severity: Medium

Event Meta

Date	Source	Destination	Username	Alias Host
2016-04-07T10:06:28			Встроенный администратор	

Additional Meta

- Device Class: VPN
- Device Ip: 192.168.1.1
- Device Type: continent
- Did: sa-logdecoder
- Esa Time: 2016-04-07T07:06:35.315Z
- Event Cat Name: User Activity
- Event Desc: Управляющая команда
- Event Source: LXC
- Event Time: 1970-01-17T20:20:31.696Z
- Header Id: 0001
- Index: Правило фильтрации добавлено
- Level: 6
- Medium: 32
- Msg Id: 35
- Net Dst: extranet
- Net Src: extranet
- Pri Facility: 1
- Pri Severity: 5
- Result: Успешно
- Rid: 20822657978
- Size: 265

Рисунок 12 – Просмотр мета-данных событий

Continent - Rule Add and Delete - Vulkan

Description: Правило фильтрации было добавлено и удалено в течение 5 минут

Time: 2016-04-07T10:06:35
Severity: Medium
Of Events: 2

Event Meta | Events

Export Logs

<input type="checkbox"/>	Date	Id	Raw Content
<input type="checkbox"/>	2016-04-07T07:06:28	20832087470	Apr 7 10:06:35 [REDACTED] continent;35;2016-02-16 14:08:16;ЦУС;Управляющая команда;Встроенный администратор;Правило фильтрации добавлено;Успешно;
<input type="checkbox"/>	2016-04-07T07:06:28	20832087471	Apr 7 10:06:35 [REDACTED] continent;35;2016-02-16 14:08:16;ЦУС;Управляющая команда;Встроенный администратор;Правило фильтрации удалено;Успешно;

Рисунок 13 – Просмотр исходных событий

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

Чт 07.04.2016 10:07
RSASA@robots.ntc-vulkan.ru
ESA Alert

Кому: Александр Александрович

При наличии проблем с отображением этого сообщения щелкните здесь, чтобы просмотреть его в веб-браузере.

RSA Security Analytics
ESA Notification

Id
5bd189e5-92b8-457c-a148-3a885b735158
Statement
Module_Continent_Rule_Add_Delete

Time
April 7, 2016 7:06:35 AM UTC
Module Name
Continent - Rule Add and Delete - Vulkan
Module Type
RuleBuilder

// EVENTS

META	VALUE
device_class	VPN
device_ip	[REDACTED]
device_type	continent
did	sa-logdecoder

Рисунок 14 – Пример уведомления