VB-Trend 2021

Wikilogs

Knowledge Center

VB-Trend

2021

Program

Telegram

Knowledge Center

VB-Trend 2021

Wikilogs

Knowledge Center

Архитектурные изменения Smart Monitor

VolgaBlot

Smart Monitor – единая консоль мониторинга

01 Диагностика инфраструктуры и бизнес-процессов

02 Визуальный конструктор метрик мониторинга

03 Управление инцидентами и активными реакциями

04 Панели мониторинга всего оборудования и бизнес-отчеты о realtime статусе систем

Архитектура решения

Ресурсно-сервисная модель
Visualization Framework поверх **Kibana**
Job Scheduler для планировки запросов

Smart Monitor Core

Базовый модуль, осуществляющий хранение и аналитику по данным. Возможность одновременной работы с несколькими хранилищами данных:
Elasticsearch
ClickHouse
Hadoop
…

Modules

Набор прикладных модулей, которые реализуют клиентские use cases:
Incident Manager
Cyber Security
Network
Servers
UBA
…

Smart Beat

Универсальный агент по сбору данных, использует **Elastic Beats**

Безагентный сбор

Возможность сбора данных без установки агента с применением **Logstash**

VolgaBlob

Что нового ?

Background запросы

Background запросы

Позволяют запустить запрос в фоне

Формируем запрос 01

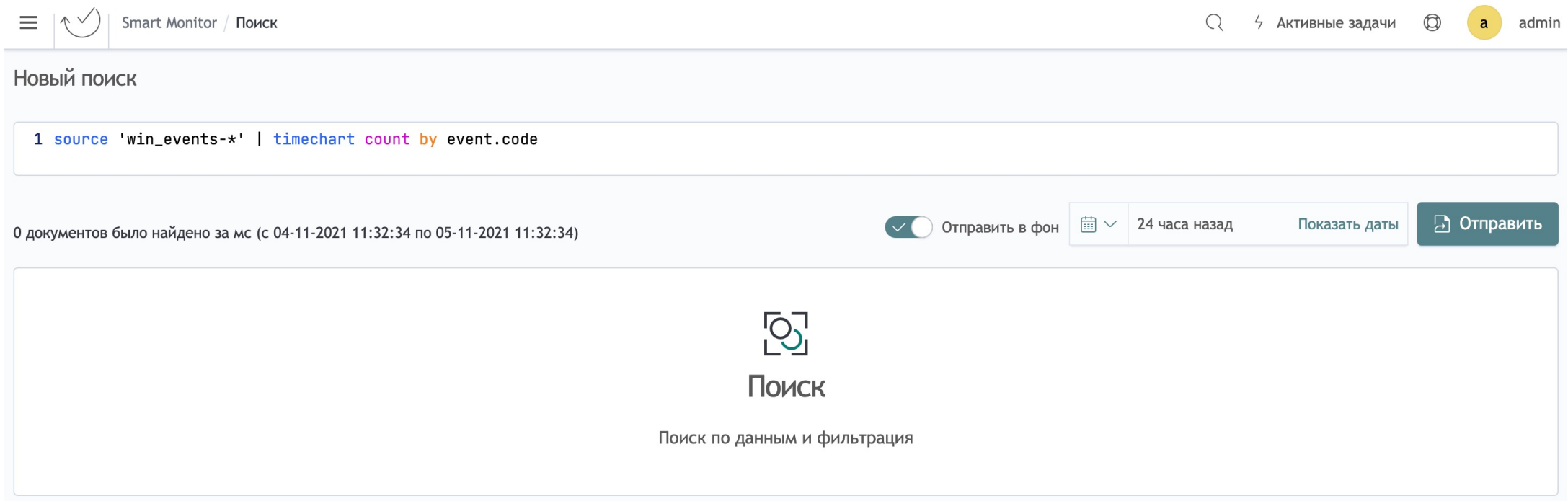
Отправляем в SME 02

SME обрабатывает запрос 03

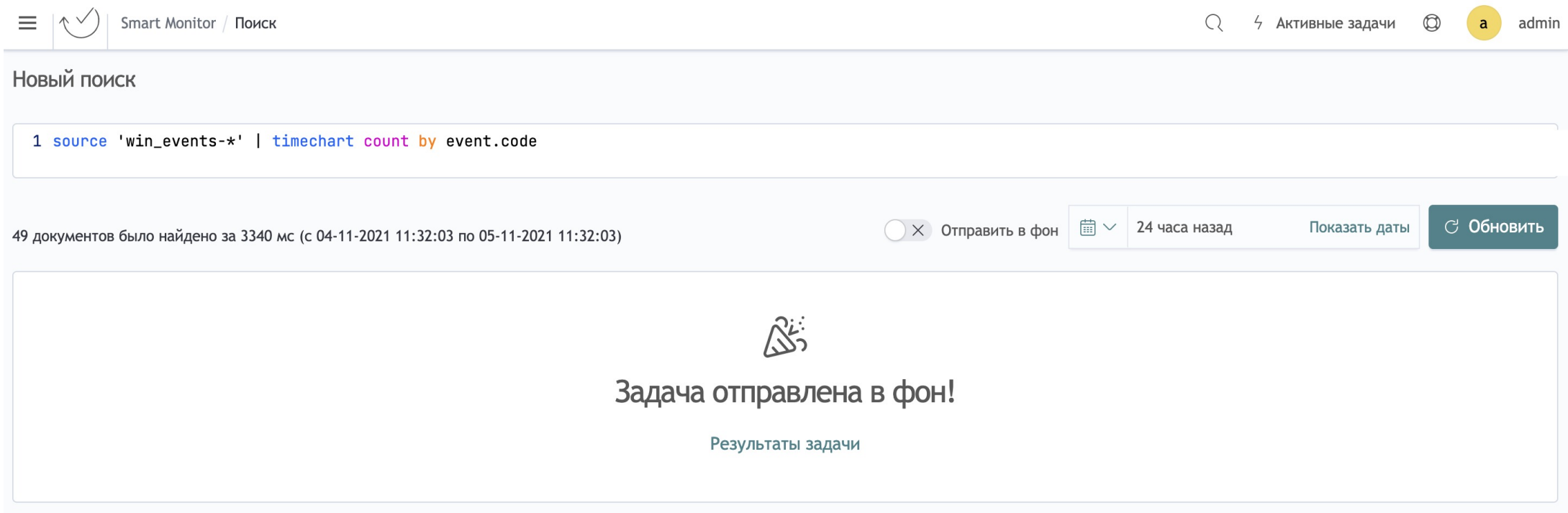
Моментально получаем результат 04

VolgaBlob

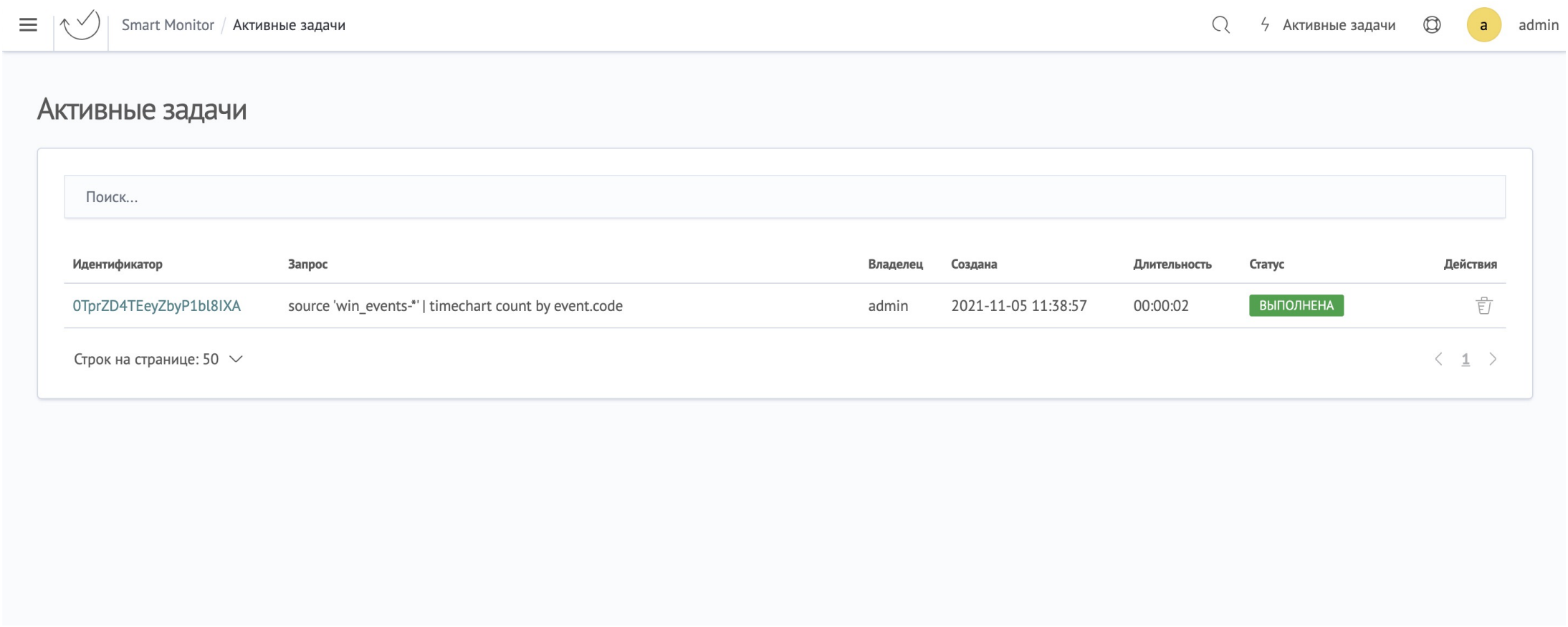
Background запросы



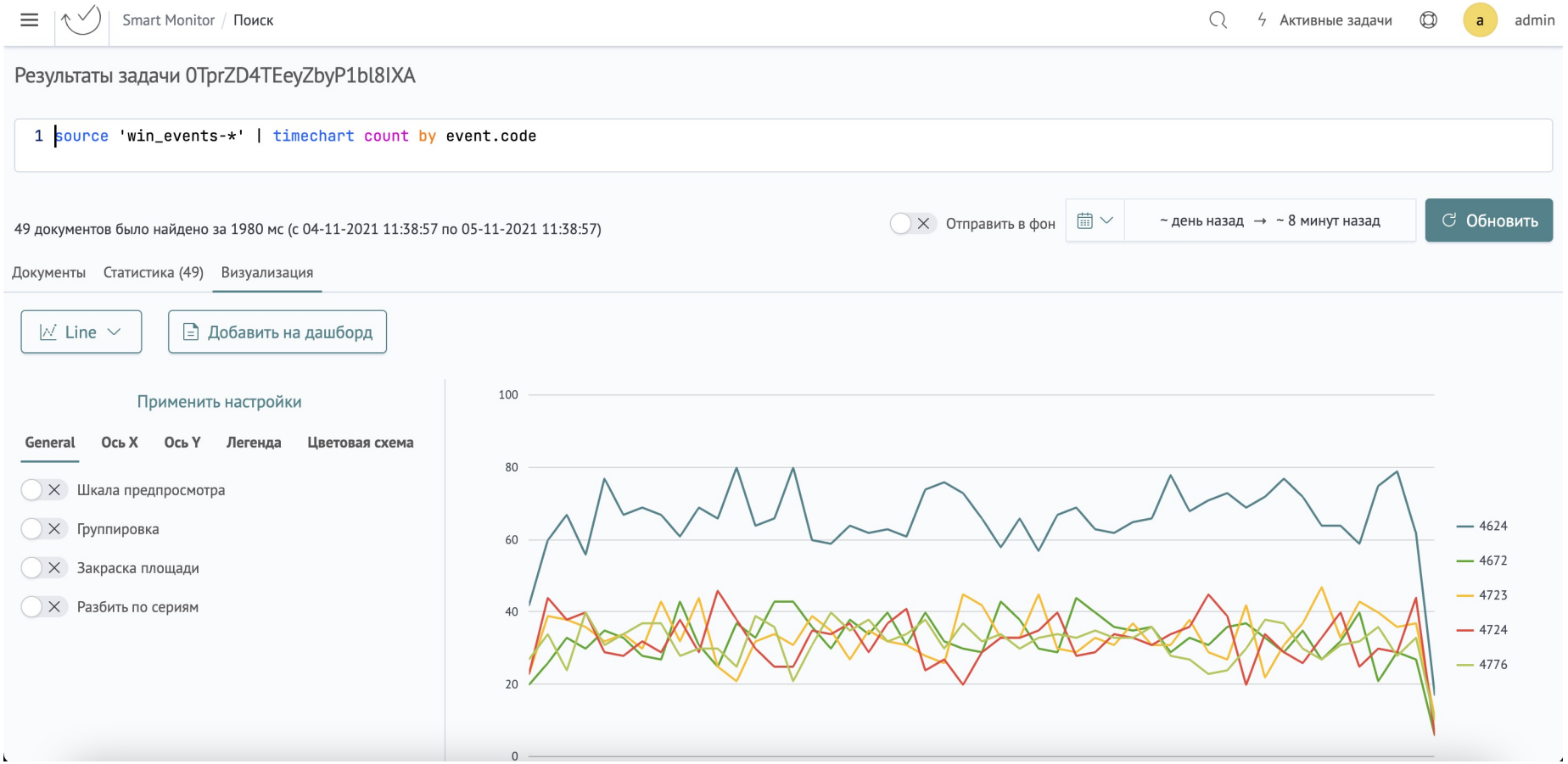
Background запросы



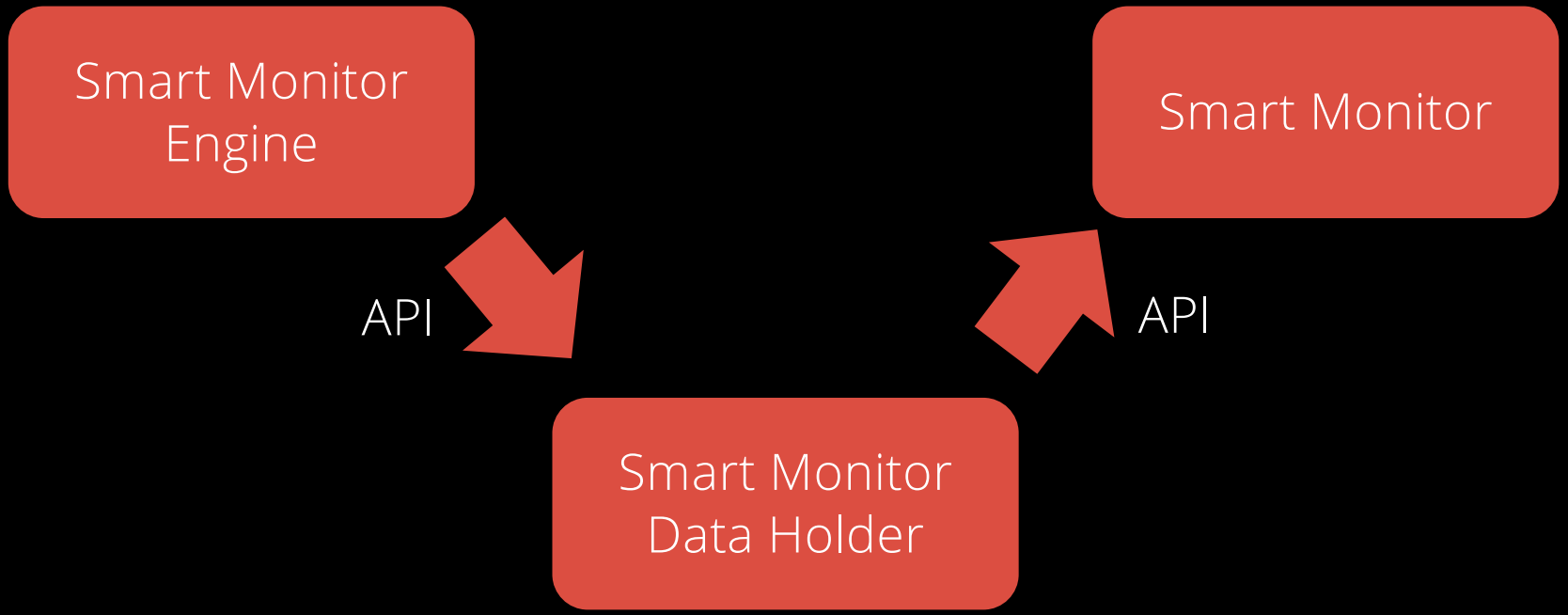
Background запросы



Background запросы



Background запросы. Как это работает?



Background запросы. Возможности

- Отправка запросов на обработку
- Получение результатов
- Хранение промежуточных результатов на диске
- Удаление результатов с диска по истечению времени хранения
- Ручное удаление результатов с диска
- Остановка запроса «налету»

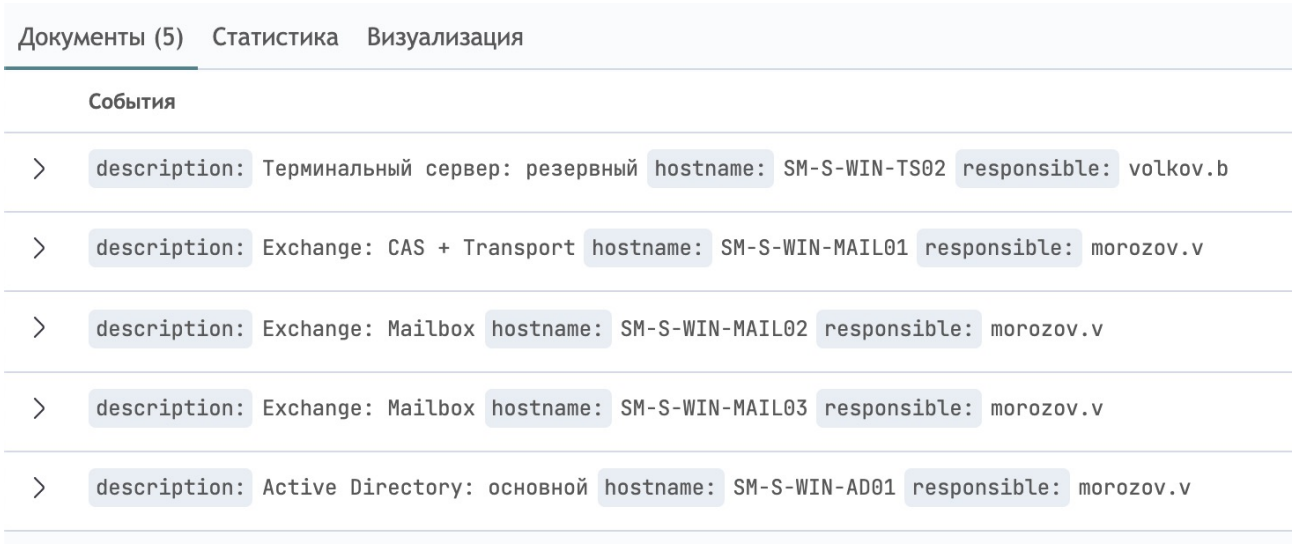
Новые команды

Команда inputlookup

- Команда inputlookup позволяет выгрузить данные из справочника (lookup)

- Параметр start позволяет указать номер стартовой записи из справочника
- Параметр max позволяет указать максимальное количество записей для выгрузки
- Параметр append указывает, добавлять документы или нет

```
| inputlookup e_servers_info  start=1 max=5 append=true
```



Команда outputlookup

- Команда outputlookup записывает результаты запроса в справочник

- Параметр start позволяет указать номер стартовой записи из справочника
- Параметр max позволяет указать максимальное количество записей для выгрузки
- Параметр append указывает, добавлять документы или записать полностью заново

```
source win_events-*
| inputlookup e_servers_info append=true
| stats count by host.name
| outputlookup e_servers_info
```

Команда iplocation

- Команда iplocation определяет IP адрес и добавляет в результаты дополнительные поля

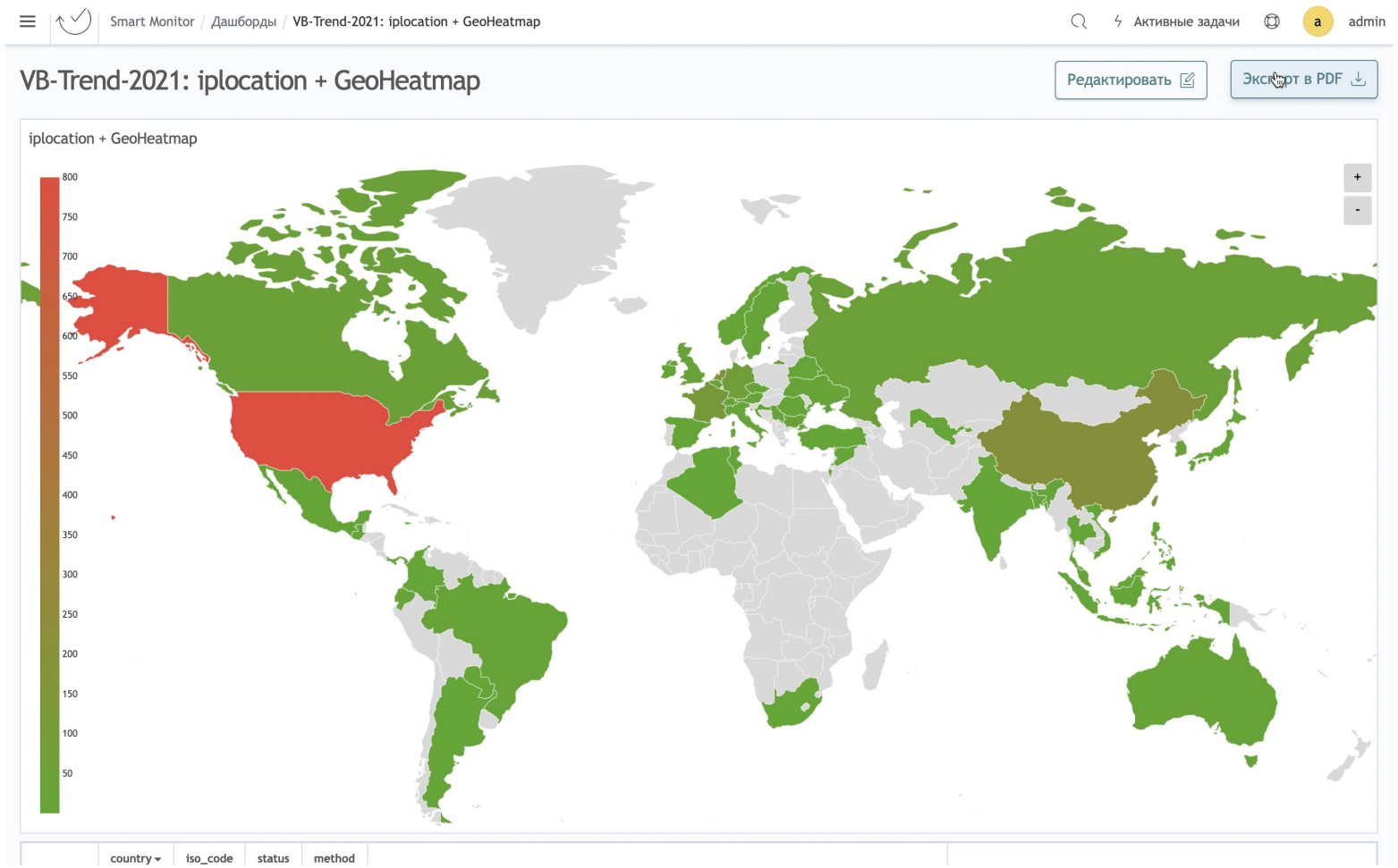
```
source 'sm_demo_geo'
| search status="4*"
| iplocation clientip
| table clientip, country, iso_code, status, method,
uri, useragent
```

clientip	country	iso_code	subdivision	city	latitude	longitude
46.172.244.149	Andorra	AD	Andorra la Vella	Andorra la Vella	42.5015	1.5144
60.173.10.8	China	CN	Anhui	Tongling	30.9309	117.8146
86.125.217.197	Romania	RO	Arad	Arad	46.184	21.3225
86.125.217.197	Romania	RO	Arad	Arad	46.184	21.3225

Команда iplocation

clientip	country	iso_code	status	method	uri	useragent
100.43.83.129	Russia	RU	404	GET	/comments/feed	Mozilla/5.0 (compatible; YandexBot/3.0; +http://yandex.com/bots)
66.249.71.214	United States	US	404	GET	/yxiysovfcnnnn.html	Mozilla/5.0 (compatible; Googlebot/2.1; +http://www.google.com/bot.html)
195.50.124.162	United Kingdom	GB	404	GET	/forum/	Mozilla/5.0 (Windows NT 6.1; rv:16.0) Gecko/20100101 Firefox/16.0
195.50.124.162	United Kingdom	GB	404	GET	/ipb/	Mozilla/5.0 (Windows NT 6.1; rv:16.0) Gecko/20100101 Firefox/16.0
195.50.124.162	United Kingdom	GB	404	GET	/oscommerce/	Mozilla/5.0 (Windows NT 6.1; rv:16.0) Gecko/20100101 Firefox/16.0
195.50.124.162	United Kingdom	GB	404	GET	/shop	Mozilla/5.0 (Windows NT 6.1; rv:16.0) Gecko/20100101 Firefox/16.0
195.50.124.162	United Kingdom	GB	404	GET	/catalog/	Mozilla/5.0 (Windows NT 6.1; rv:16.0) Gecko/20100101 Firefox/16.0
37.1.207.22	Netherlands	NL	404	GET	/wp-content/themes/diarise/thumb.php	Mozilla/5.0 (Macintosh; Intel Mac OS X 10_6_8) AppleWebKit/535.7 (KHTML, like Gecko) Chrome/16.0.912.77 Safari/535.7

Команда iplocation



Команда rest

| rest "_cluster/health"

Документы | Статистика (1) | Визуализация

cluster_name	active_shards	status
vbtrend-cluster	350	green

| rest "_cat/indices"

win_events-2021.44	25.2mb	open	green
kwc_tag_object_ru	29.6kb	open	green
win_events-2021.45	10.3mb	open	green
kwb_object	180.6kb	open	green

Первые шаги к дашбордам самодиагностики

| rest "_cluster/..."

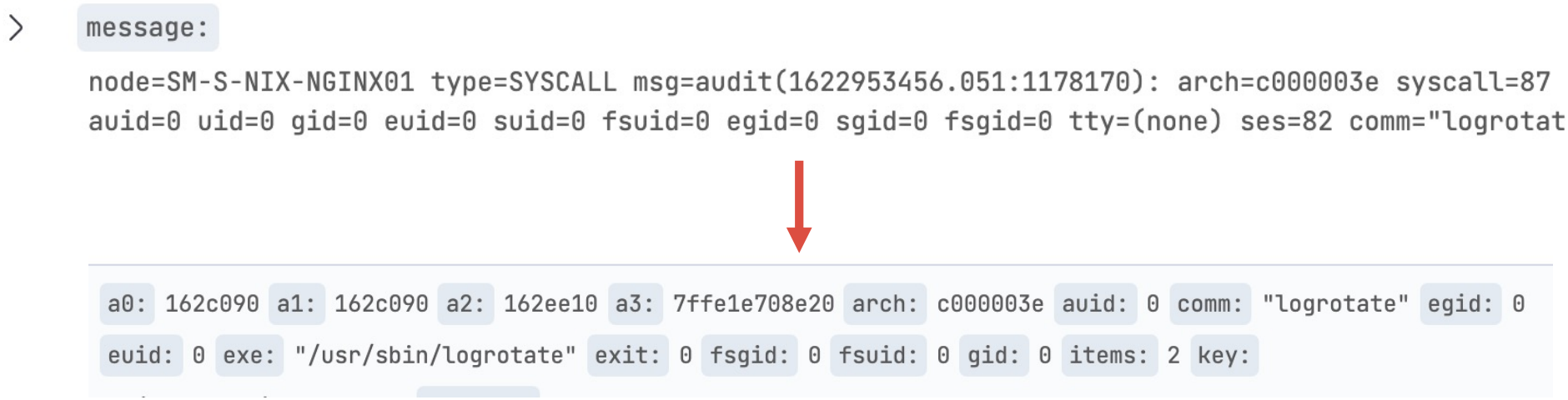
| rest "_cat/..."

VolgaBlob

Команда rex

- Команда rex позволяет во время поиска, «на лету» извлечь нужные значения с помощью регулярных выражений

```
source audisp-2021.11
| rex field=message max_match=0
"(?<_KEY_field>\w+)=(?<_VAL_field>\S+)"
```



И еще команды!

```
| makeresults count=2 shownumbers=true
```

События

@timestamp:	2021-11-09T08:14:34.686Z	number:	1
@timestamp:	2021-11-09T08:14:34.686Z	number:	2

```
source 'win_events-*'
| addinfo
| table *
```

host.ip	info_min_time	info_max_time	info_sid	info_search_time
172.16.0.8	2021-11-08T08:18:14Z	2021-11-09T08:18:14Z	95b2fc82-4135-11ec-b971-fbfc6228997e	2021-11-09T08:18:14.263Z
172.16.0.8	2021-11-08T08:18:14Z	2021-11-09T08:18:14Z	95b2fc82-4135-11ec-b971-fbfc6228997e	2021-11-09T08:18:14.263Z
172.16.0.4	2021-11-08T08:18:14Z	2021-11-09T08:18:14Z	95b2fc82-4135-11ec-b971-fbfc6228997e	2021-11-09T08:18:14.263Z

One more command…

transaction

Что такое транзакция?

- Транзакция – это любая группа связанных событий в определенном промежутке времени
- События могут поступать из нескольких приложений или хостов
  - События, связанные с одной покупкой в интернет-магазине, могут охватывать сервер приложений, базы данных и др.
  - Одно сообщение об ошибке может создавать несколько событий
  - Несколько событий в журналах сетевого трафика представляют одного пользователя, который сгенерировал один HTTP-запрос
  - Посещение одного web-сайта обычно генерирует несколько HTTP- запросов
    - HTML, JavaScript, файлы CSS
    - Flash, Изображения

Команда transaction

- В индексе apache находятся события access log веб-сервера, в нескольких событиях имеются одни и те же JSESSIONID
- Однако группу событий в выводе поиска сложно воспринимать как единое целое

source 'apache-*'

Дата и время	События
11-08-2021 03:35:17.000	@timestamp: 2021-08-11T00:35:17.000Z JSESSIONID: SD9SL2FF7ADFF42192 action: addtocart bytes: 748 clientip: 175.44.1.122 host: localhost.localdomain method: POST other: 156 path: /etc/logstash/conf.d/data_test_transaction/transaction.json referer: http://www.buttercupgames.com/product.screen?productId=SC-MG-G10 status: 200 uri: /cart.do?action=addtocart&itemId=EST-19&productId=SC-MG-G10&JSESSIONID=SD9SL2FF7ADFF42192 useragent: Mozilla/5.0 (Windows NT 6.1; WOW64) AppleWebKit/536.5 (KHTML, like Gecko) Chrome/19.0.1084.52 Safari/536.5
11-08-2021 03:35:17.000	@timestamp: 2021-08-11T00:35:17.000Z JSESSIONID: SD9SL2FF7ADFF42192 action: - bytes: 1644 clientip: 175.44.1.122 host: localhost.localdomain method: GET other: 263 path: /etc/logstash/conf.d/data_test_transaction/transaction.json referer: http://www.buttercupgames.com/category.screen?categoryId=SIMULATION status: 200 uri: /product.screen?productId=SC-MG-G10&JSESSIONID=SD9SL2FF7ADFF42192 useragent: Mozilla/5.0 (Windows NT 6.1; WOW64) AppleWebKit/536.5 (KHTML, like Gecko) Chrome/19.0.1084.52 Safari/536.5
11-08-2021 03:32:59.000	@timestamp: 2021-08-11T00:32:59.000Z JSESSIONID: SD0SL4FF1ADFF42170 action: purchase bytes: 1998 clientip: 50.23.124.50 host: localhost.localdomain method: POST other: 913 path: /etc/logstash/conf.d/data_test_transaction/transaction.json referer: http://www.buttercupgames.com/cart.do?action=addtocart&itemId=EST-18&categoryId=STRATEGY&productId=FS-SG-G03 status: 200 uri: /cart.do?action=purchase&itemId=EST-18&JSESSIONID=SD0SL4FF1ADFF42170 useragent: Mozilla/5.0 (Windows; U; Windows NT 5.1; en-US; rv:1.9.2.28) Gecko/20120306 YFF3 Firefox/3.6.28 (.NET CLR 3.5.30729; .NET4.0C)
11-08-2021 03:32:58.000	@timestamp: 2021-08-11T00:32:58.000Z JSESSIONID: SD0SL4FF1ADFF42170 action: - bytes: 644 clientip: 50.23.124.50 host: localhost.localdomain method: GET other: 737 path: /etc/logstash/conf.d/data_test_transaction/transaction.json referer: http://www.buttercupgames.com/product.screen?productId=SF-BVS-G01 status: 503 uri: /oldlink?itemId=EST-17&JSESSIONID=SD0SL4FF1ADFF42170 useragent: Mozilla/5.0 (Windows; U; Windows NT 5.1; en-US; rv:1.9.2.28) Gecko/20120306 YFF3 Firefox/3.6.28 (.NET CLR 3.5.30729; .NET4.0C)

Команда transaction

- Используйте команду transaction для создания одного события из группы событий, которые имеют одно и то же значение в заданном поле

- Транзакция может связывать события нескольких уровней (т.е. веб-сервер, сервер приложений), использую общие поля, в этом примере JSESSIONID

```
source 'apache-*'
| transaction JSESSIONID
```

Команда transaction

transaction добавляет дополнительные поля в результаты поиска

+ eventcount

+ duration

Команда transaction

- Вы также можете определить максимальный общий временной интервал и максимальный разрыв между событиями

```
source 'apache-*'
| transaction clientip maxspan=10m maxpause=1m
```

```
> 01-10-2021 02:56:56.000 @timestamp: 2021-09-30T23:56:56.000Z JSESSIONID: [ "SD1SL2FF9ADFF7375" ] action: [ "-", "view", "addtocart", "purchase" ] bytes:
[ "1880", "1248", "1544", "2069", "1682", "2280", "3427" ] clientip: 76.89.103.115 duration: 6 eventcount: 7 host:
[ "localhost.localdomain" ] method: [ "GET", "POST" ] other: [ "381", "645", "668", "180", "813", "972", "274" ] path:
[ "/etc/logstash/conf.d/data_test_transaction/transaction.json" ] referer:
[ "http://www.buttercupgames.com", "http://www.buttercupgames.com/oldlink?itemId=EST-17",
"http://www.buttercupgames.com/category.screen?categoryId=STRATEGY", "http://www.buttercupgames.com/cart.do?action=view&itemId=EST-
6&productId=WC-SH-A01", "http://www.buttercupgames.com/category.screen?categoryId=ARCADE",
"http://www.buttercupgames.com/product.screen?productId=FI-AG-G08", "http://www.buttercupgames.com/cart.do?
action=addtocart&itemId=EST-17&categoryId=ARCADE&productId=FI-AG...
status: [ "200", "503" ] uri:
[ "/oldlink?itemId=EST-11&JSESSIONID=SD1SL2FF9ADFF7375", "/oldlink?itemId=EST-17&JSESSIONID=SD1SL2FF9ADFF7375", "/product.screen?
productId=DB-SG-G01&JSESSIONID=SD1SL2FF9ADFF7375", "/category.screen?categoryId=ACCESSORIES&JSESSIONID=SD1SL2FF9ADFF7375",
"/product.screen?productId=FI-AG-G08&JSESSIONID=SD1SL2FF9ADFF7375", "/cart.do?action=addtocart&itemId=EST-17&productId=FI-AG-
G08&JSESSIONID=SD1SL2FF9ADFF7375", "/cart.do?action=purchase&itemId=EST-17&JSESSIONID=SD1SL2FF9ADFF7375" ]
useragent: [ "Mozilla/4.0 (compatible; MSIE 7.0; Windows NT 5.1; Trident/4.0; .NET CLR 2.0.50727; MS-RTC LM 8; InfoPath.2)" ]
```

Команда transaction

- Для формирования транзакции на основе терминов или значений полей используйте опции startswith и endswith

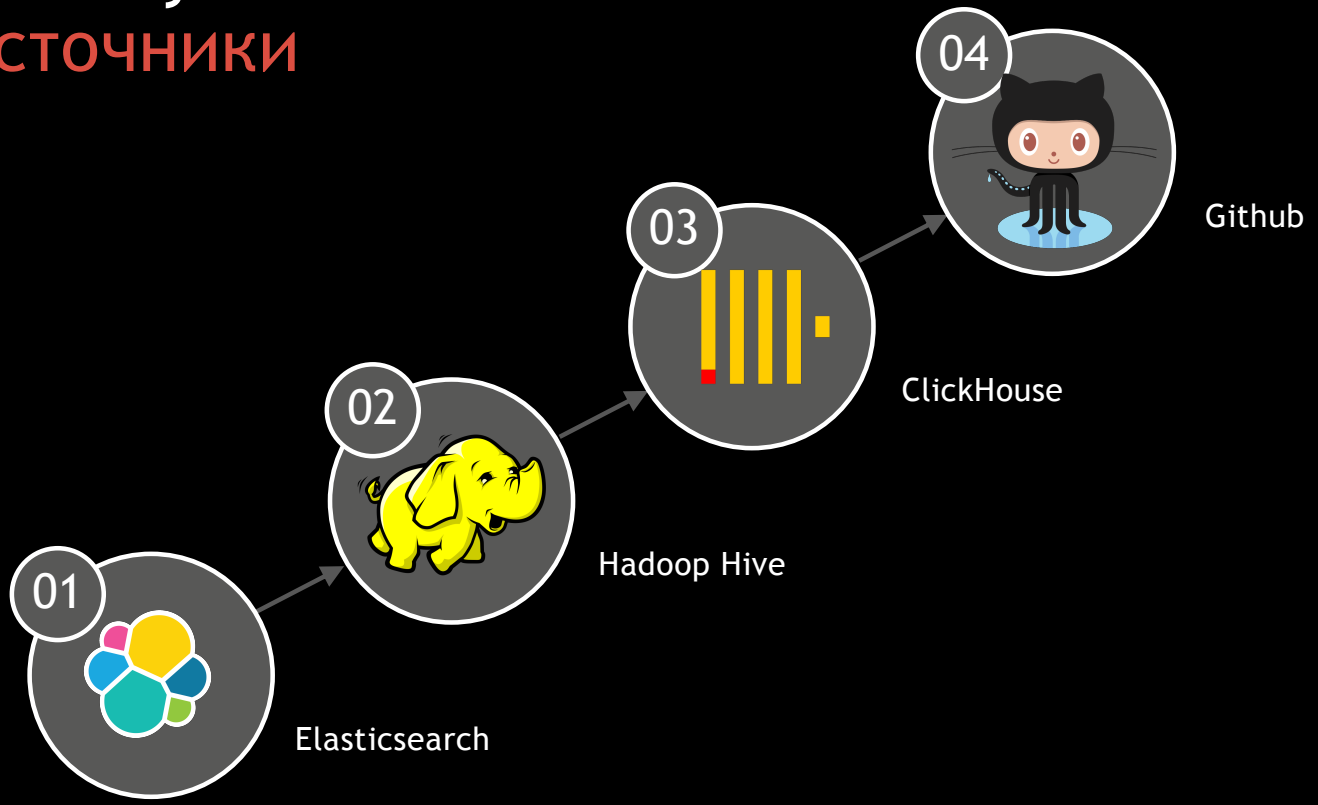
```
source 'apache-*'
| transaction clientip, JSESSIONID maxspan=10m
maxpause=1m startswith=(action="addtocard")
endswith=(action="purchase")
| table clientip, JSESSIONID, duration, eventcount
```

clientip	JSESSIONID	duration	eventcount
92.1.170.135	SD5SL1FF7ADFF40870	5	8
178.19.3.199	SD0SL6FF10ADFF40884	5	13
109.169.32.135	SD4SL6FF7ADFF40900	9	12
49.212.64.138	SD7SL5FF2ADFF40913	4	8
110.138.30.229	SD2SL7FF9ADFF40916	5	10
69.72.161.186	SD9SL1FF8ADFF40929	8	12

Smart Monitor™

Search @nywhere

Search Anywhere
Источники



Команда gitsource

- Команда gitsource выполняет поиск по github.

```
gitsource searchType="code" query="@volgablob.ru"
```

- Можно указать несколько типов поиска:
  - code
  - issues
  - commits

Документы (81) Статистика Визуализация

События

git_url: https://api.github.com/repositories/90011526/git/blobs/a86a194b18a91d2a5acf2eec2eb505e4c4683482 html_url:
https://github.com/akilbekov/blog/blob/d642be6ddaadb42d0799b04817ee341a9dd87465/src/pages/articles/2018-08-20---Learning-splunk/index.md name: index.md path:
src/pages/articles/2018-08-20---Learning-splunk/index.md repository:
{ "tags_url": "https://api.github.com/repos/akilbekov/blog/tags", "contributors_url": "https://api.github.com/repos/akilbekov/blog/contributors", "private": "false", "notifications_url": "https://api.github.com/repos/akilbekov/blog/notifications{?since,all,participating}", "description": "null", "subscription_url": "https://api.github.com/repos/akilbekov/blog/subscription", "branches_url": "https://api.github.com/repos/akilbekov/blog/branches{/branch}", "deployments_url": "htt...
score: 1.0 sha: a86a194b18a91d2a5acf2eec2eb505e4c4683482 text_matches: ["/splunk\\n- https://www.aplura.com/resources\\n- https://www.hurricanelabs.com/blog\\n- https://www.volgablob.ru"]
url: https://api.github.com/repositories/90011526/contents/src/pages/articles/2018-08-20---Learning-splunk/index.md?ref=d642be6ddaadb42d0799b04817ee341a9dd87465

Демонстрация Gitsource

VB-Trend 2021

Wikilogs

Knowledge Center

Функциональные изменения Smart Monitor

VolgaBlot

SDK для создания приложений на SM

SDK

API для регистрации приложений, шаринг конфигураций, полезных свойств и компонентов Smart Monitor

Приложение

Предоставление пользовательскому приложению возможности «встраивания» в Smart Monitor

Core

Приложение Smart Monitor

VolgaBlob

SDK для создания визуализаций на SM

SDK

Набор методов и компонентов для интеграции в Smart Monitor

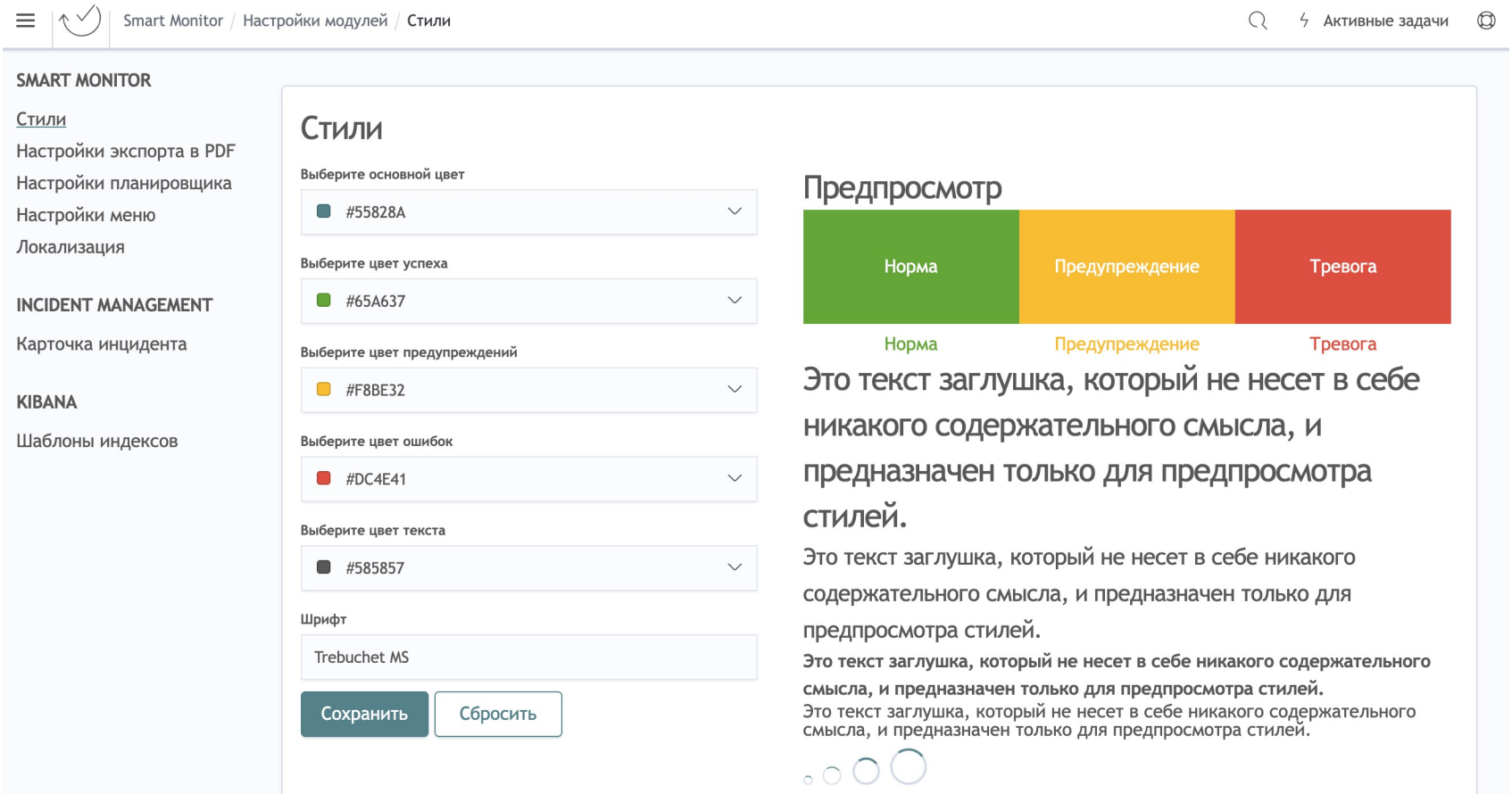
Визуализация

Пользовательская визуализация, отправляющая запрос на регистрацию своих React-компонентов

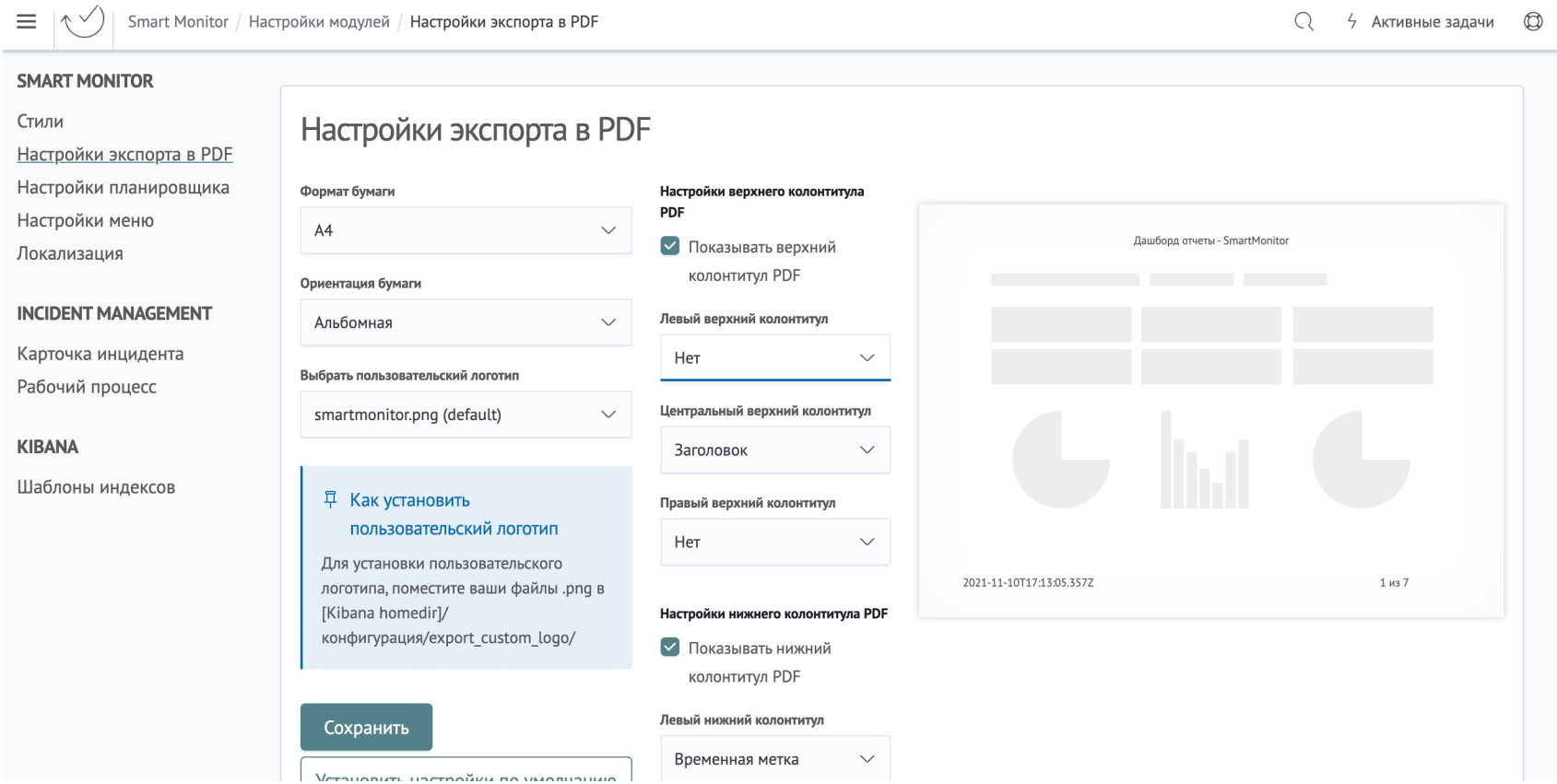
Core

Приложение Smart Monitor

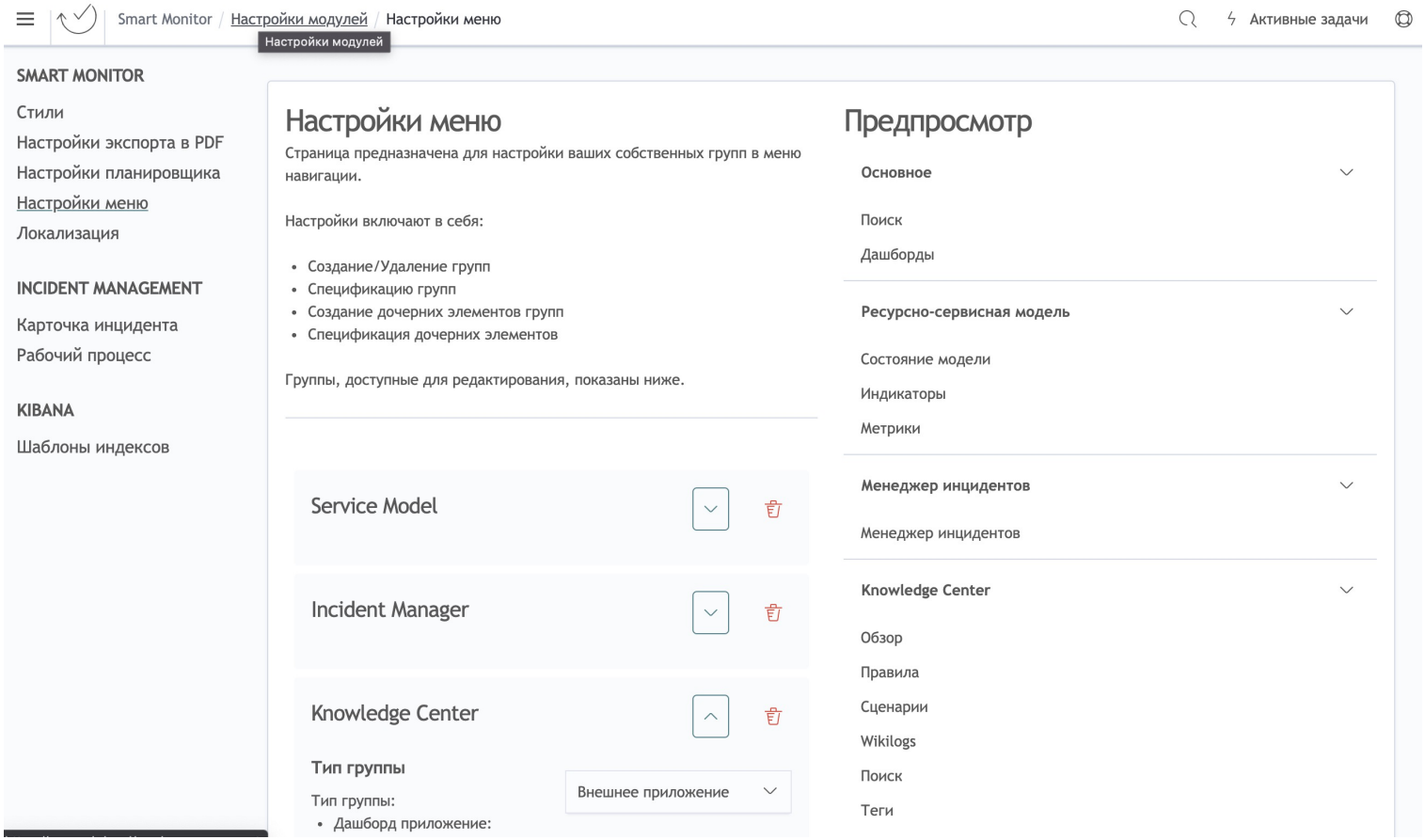
Интерфейс настроек системы



Интерфейс настроек системы

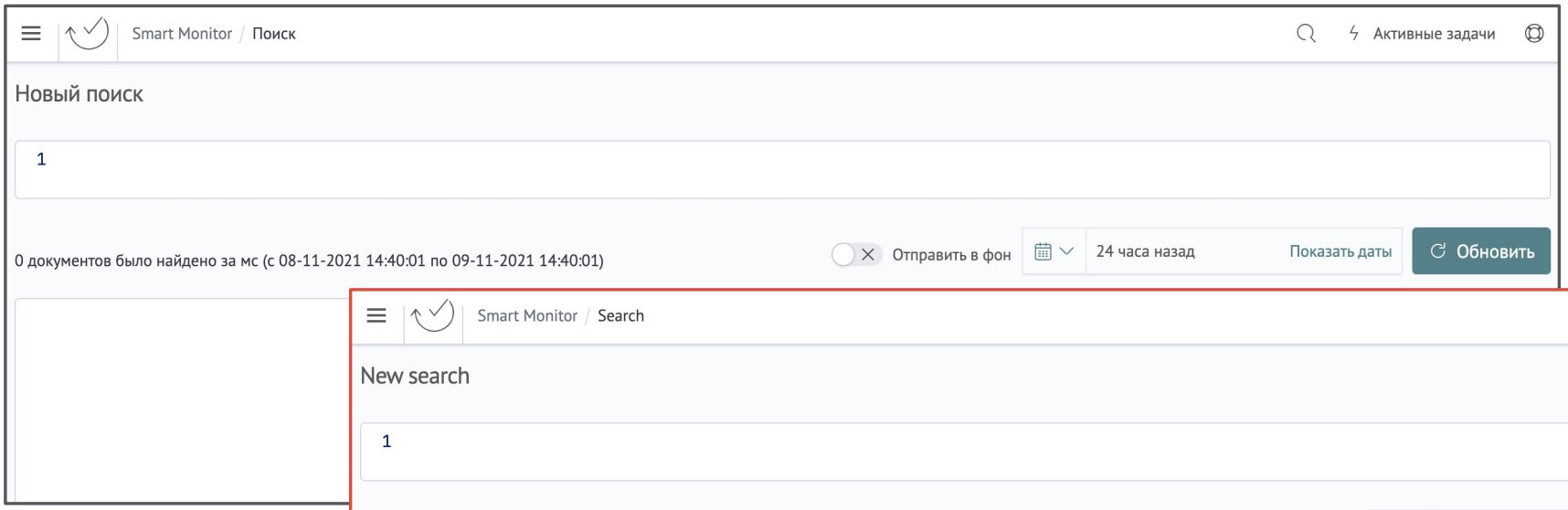


Интерфейс настроек системы

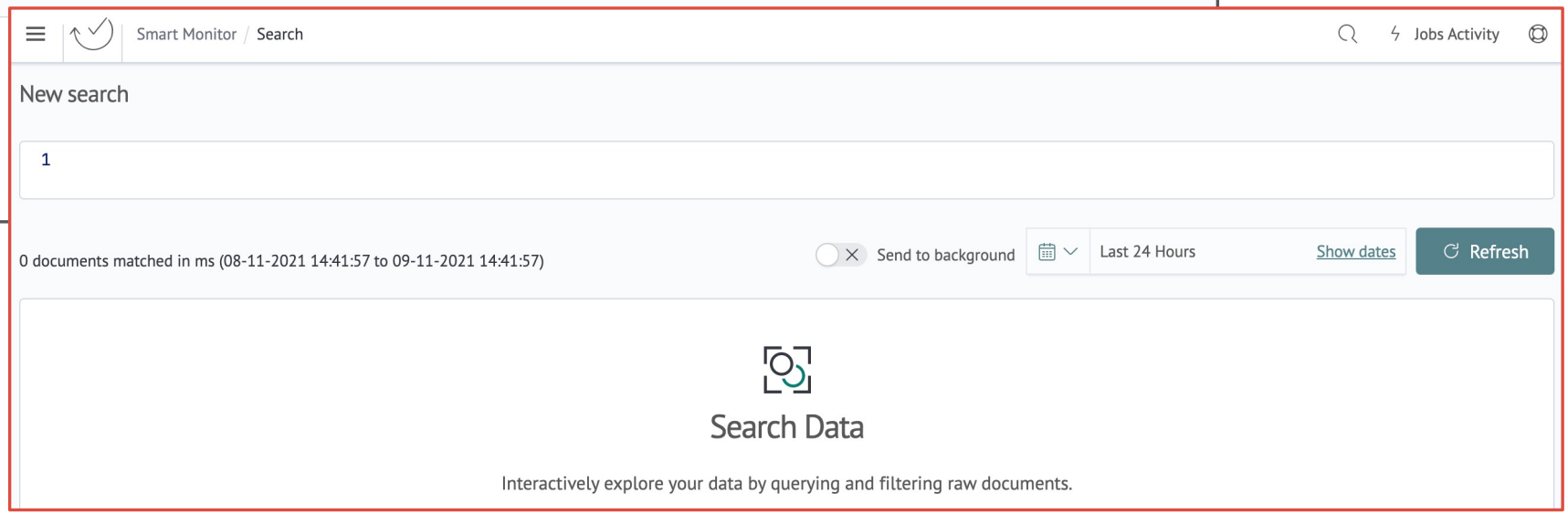


Локализация интерфейса

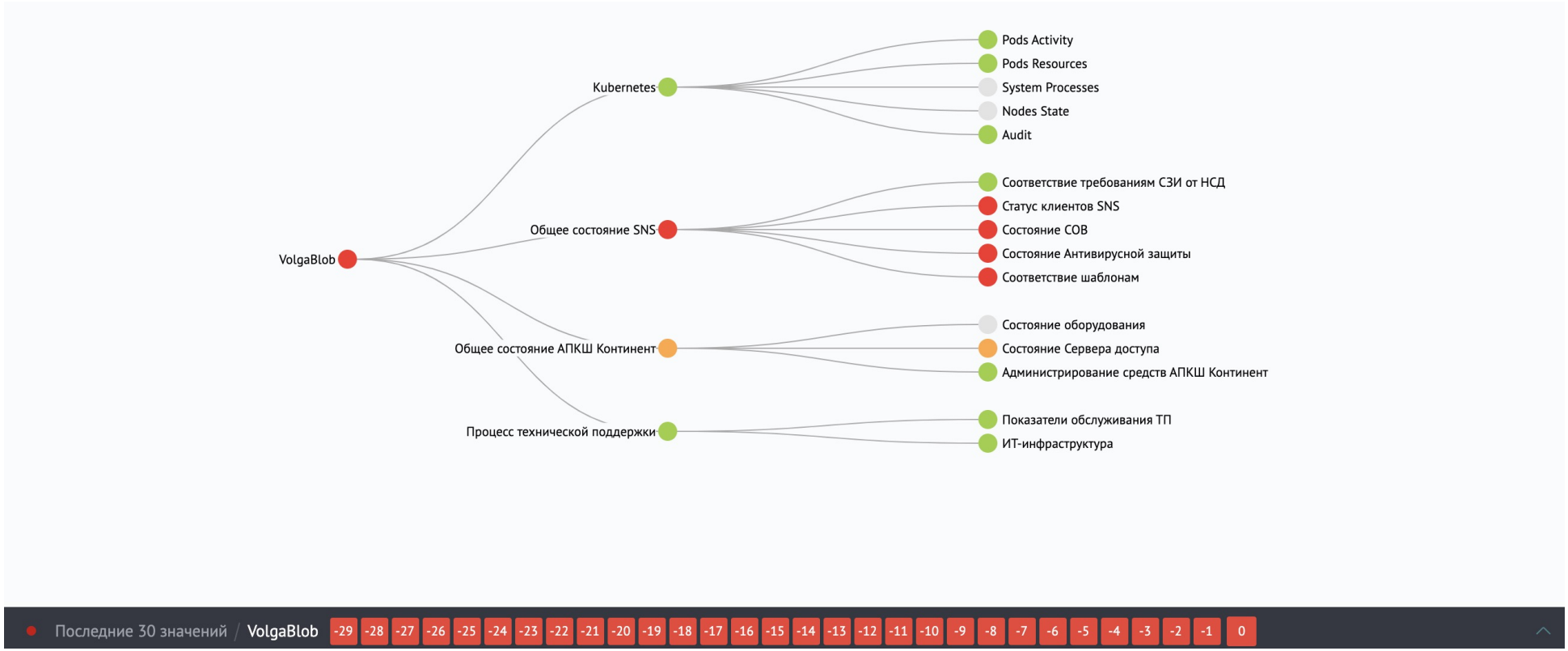
Русская



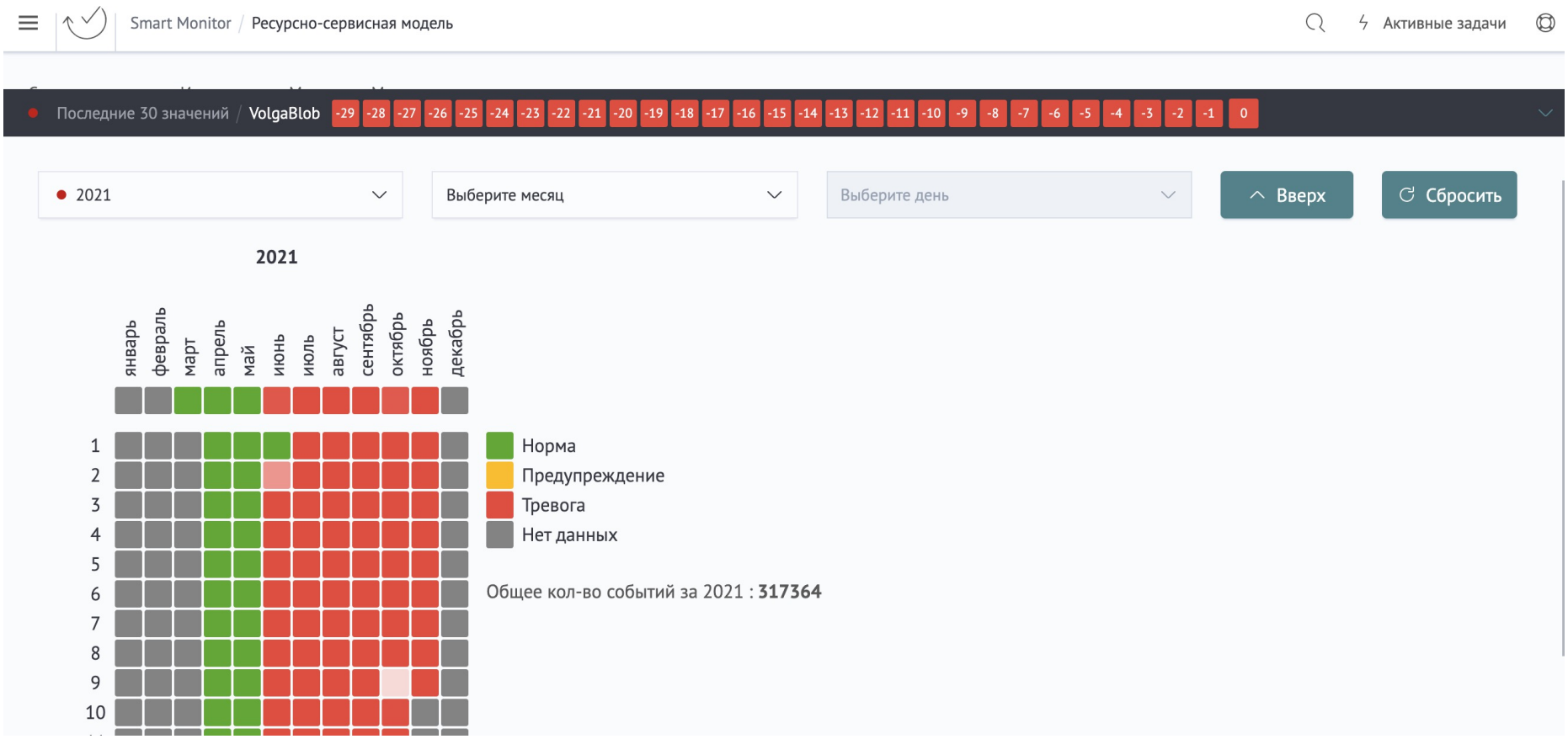
Английская



Новое в PCM - история

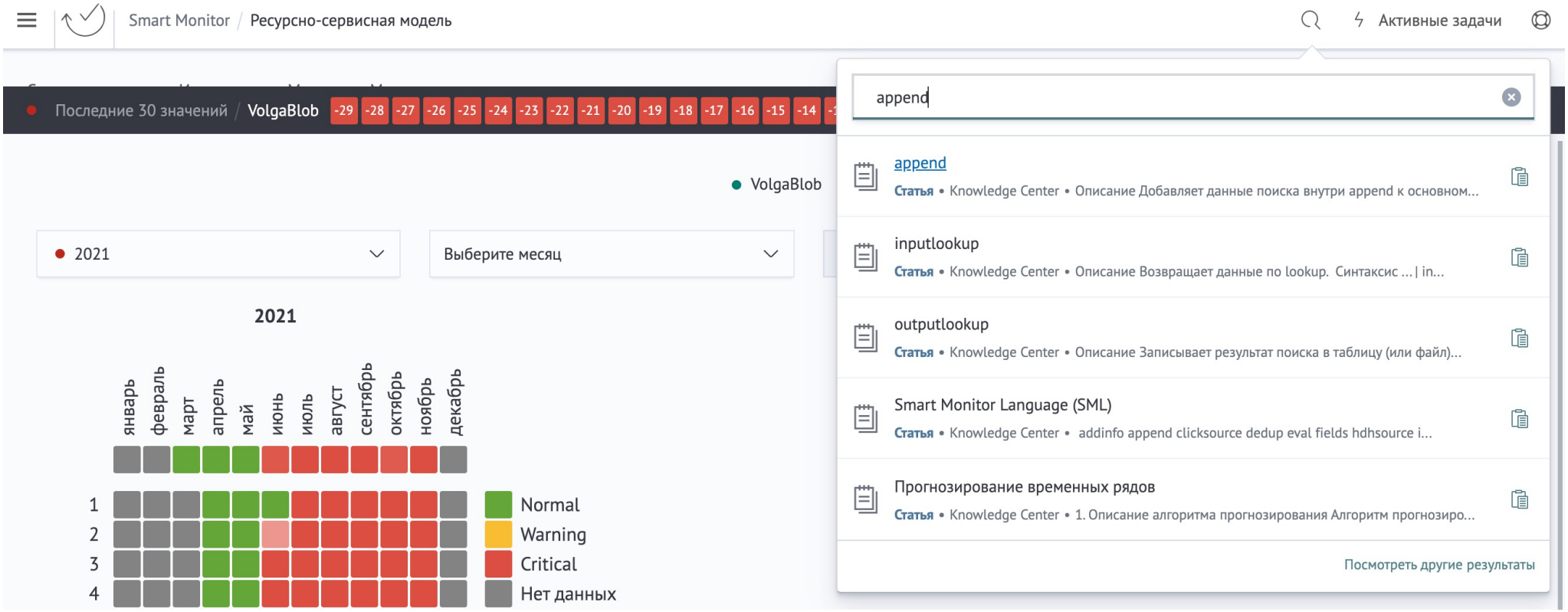


Новое в РСМ – «тепловая» карта



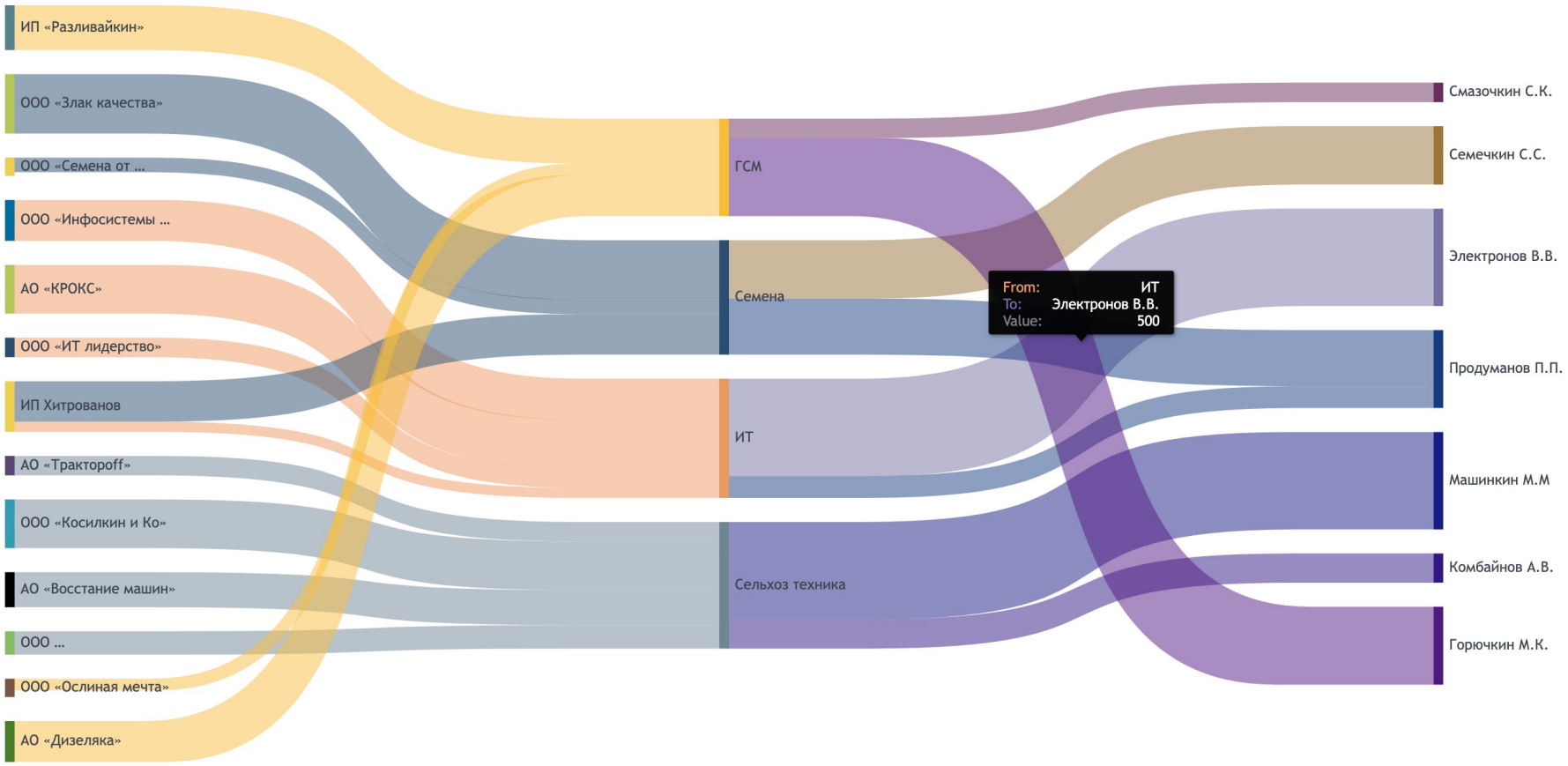
Глобальная строка поиска

Spotlight



Дополнительные визуализации

Radar | Sankey | Geomap



VolgaBlob

Развитие Smart Monitor

Векторы развития Smart Monitor

Разработчикам

Framework для пользовательских **команд**

Framework для создания пользовательских **действий** (Actions)

Plugin Builder: модуль для разработки собственных плагинов с SM SDK

Векторы развития Smart Monitor

Администраторам

Модуль **самодиагностики** и **мониторинга**

Lookup Manager
удобная работа со справочниками

JDBC Manager
удобная работа источниками-БД через UI

Компонент централизованного управления **инсталляциями**

VolgaBlob

Векторы развития: Функциональные модули

Пользователям
ИБ, ИТ, Бизнес

MITRE ATT&CK

Smart Monitor for MITRE ATT&CK

Применение на практике основных сценариев использования MITRE ATT&CK - публичной базы знаний, содержащей набор тактик и техник **поведения злоумышленников** во внутренней сети организации.

Модуль содержит инструменты для:

- анализа применимости угроз/техник
- детектирования поведения злоумышленников
- Risk-скоринга пользователей и хостов
- анализа покрытия техник

Векторы развития: Функциональные модули

Пользователям
ИБ, ИТ, Бизнес

UBA

Smart Monitor User Behavior Analytics

Модуль предназначен для анализа действий пользователей и обнаружения случаев отклонений от типового поведения

NetMap

Smart Monitor NetMap

Автоматическое построение карты сети на основе получаемой с сетевого оборудования информации

MLE

SM Machine Learning Engine

Применение алгоритмов машинного обучения при анализе данных внутри Smart Monitor

VolgaBlob

Векторы развития Smart Monitor

Пользователям
ИБ, ИТ, Бизнес

Search Anywhere

Развитие концепции Search Anywhere

Файлы и поиск по ним: использование инструментов «краулинга» для поиска в общедоступных сетевых хранилищах

Векторы развития Smart Monitor

Партнерам