

Новый поиск

```
1 source 'win_events-*'  
2 | timechart timefield="timestamp" span=15m count by agent.hostname
```

97 документов было найдено за 3434 мс (с 22-12-2021 08:05 по 23-12-2021 08:41)

Документы (97) Визуализация

Line

Добавить на дашборд

Изменить настройки

General Ось X Ось Y Легенда Цветовая схема

Серия

SM-S-WIN-TS02

Цвет #55828A

+ Добавить значение

Отправить в фон 24 часа назад Показать даты

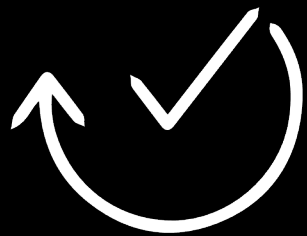
TM

# Smart Monitor

## Search @nywhere

### Обзор платформы v3.0





# Smart Monitor

Search @nywhere

## Комплексная платформа мониторинга



### Сценарии

Решение прикладных задач бизнеса, ИТ и ИБ



### Аналитика

Визуальный конструктор метрик мониторинга



### Реакция

Управление инцидентами и активное реагирование



### Данные

Доверенная картина на основе исходных данных



# Наши клиенты\*



The Central Bank  
of the Russian  
Federation



SOCIETE GENERALE GROUP



\* представлены реализованные VolgaBlob проекты в области поставки/интеграции решений информационной безопасности и мониторинга данных

# Два уровня Smart Monitor

Платформа, как инструмент решения практических задач



# Позиционирование Smart Monitor

	Smart Monitor	Splunk	Elastic/OS Stack	Типичный SIEM
Универсальный поиск по различным хранилищам данных	 Поиск без необходимости переиндексации	 Дополнительные инструменты и переиндексация	 Только в собственном хранилище данных	 Только в собственном хранилище данных
Возможности модификации языка поисковых запросов	 В рамках roadmap и по запросу клиента	 Минорные изменения в рамках релизов	 В рамках roadmap незначительные изменения	 Как правило, отсутствует
Возможность подключения любых источников данных	 Универсальная платформа	 Универсальная платформа	 Универсальная платформа	 Ориентация на средства защиты информации
Аналитические возможности при работе с данными	 Динамично развивающийся язык SML	 Зрелый язык поисковых запросов SPL	 Ограниченный набор команд над данными	 Ограниченный набор команд над данными
Собственная база корреляционных правил для кибербезопасности	 В рамках модуля Cybersecurity + проектная работа	 В рамках приложения Enterprise Security	 Контент решения Elastic SIEM	 Большое число правил «из коробки»

# Практические сферы применения



# Smart Monitor

## Мониторинг бизнес-процессов

Оценка соответствия бизнес-процессов заданным SLA/KPI, выявление аномалий в процессах и сервисах

Профилирование действий пользователей в рамках бизнес-процессов, трудовая дисциплина, скоринг

## Мониторинг кибербезопасности

Smart Code - решение для комплексного мониторинга средств защиты Кода Безопасности

Управление инцидентами информационной безопасности. Автоматизация для SOC

## Мониторинг ИТ-инфраструктуры

Мониторинг сред контейнеризации (Kubernetes, Docker), виртуальных сред

Мониторинг сетевой, серверной инфраструктуры, инвентаризация, диагностика и оценка здоровья ИТ

# Архитектура решения

Ресурсно-сервисная модель  
Visualization Framework  
Job Scheduler для планировки запросов

## Smart Monitor Core

Базовый модуль, осуществляющий хранение и аналитику по данным. Возможность одновременной работы с несколькими хранилищами данных:  
Elasticsearch  
OpenSearch  
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 Beats

## Безагентный сбор

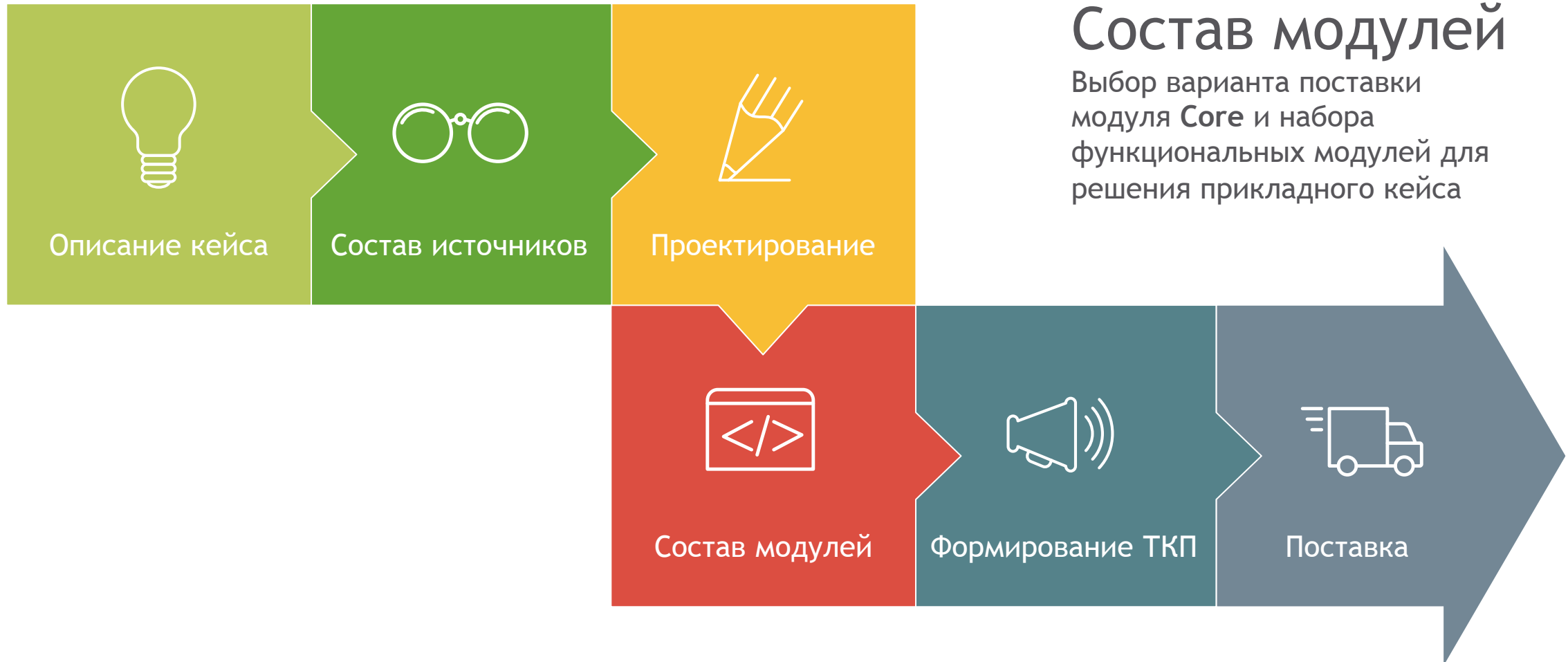
Возможность сбора данных без установки агента с применением Logstash

# Лицензирование

Принципы ценообразования Smart Monitor



# Процесс формирования цены



# Варианты поставки модуля Core



# Модули Smart Monitor

Свой набор модулей для реализации практических задач

# Core

Аналитическое ядро Smart Monitor

# Core: Smart Monitor Engine



Аналитический движок для обработки данных

**Search Anywhere** - хранение и поиск данных в Elasticsearch и не только

Собственный язык запросов Smart Monitor Language, поддержка pipeline-обработки

Многопоточная обработка данных при выполнении команд

# Концепция Search Anywhere

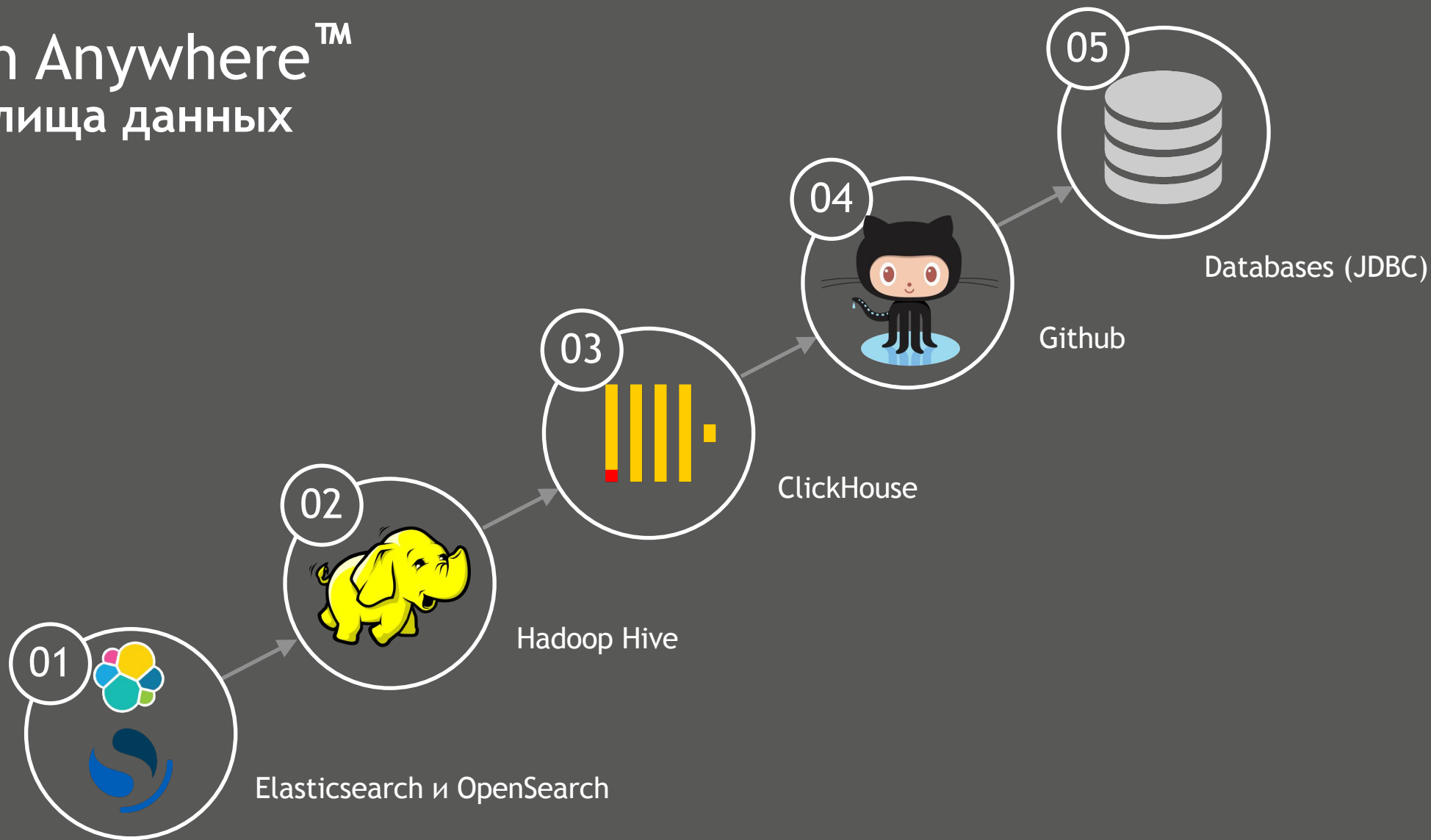


Поиск по данным в любом подключенном хранилище с единым синтаксисом

Исходные данные остаются нетронутыми, переиндексация не происходит

Можно «положить» результаты рядом в любое хранилище

# Search Anywhere™ Хранилища данных



## Как использовать?

```
source win_events:1000, clk:events.nix_events qsize=5000
```

1000 событий из индекса win\_events в  
OpenSearch

5000 событий из таблицы nix\_events в  
Clickhouse



## Как использовать?

```
source win_events:1000, clk:events.nix_events qsize=5000
```

**clk: / had: / db:**

префикс для указания конкретного хранилища

## Как использовать?

```
source win_events:1000, clk:events.nix_events qsize=5000
```

**win\_events: / events.nix\_events:**

индекс Opensearch / база данных или иное хранилище

## Как использовать?

```
source win_events:1000, clk:events.nix_events qsize=5000
```

`:1000`

лимит по числу событий от выбранного хранилища

`qsize=5000`

лимит числа событий по умолчанию

## Поиск по всем данным!

```
source windows  
| search "192.168.10.16"
```

```
source nginx  
| search "*ERROR*"
```

Можно найти по любому фрагменту в данных, даже если не знаете в каком поле искать!

## Пример запроса

```
source win_events:1000, clk:events.nix_events, db:postgre:pg_query  
| eval sourcetype = _type  
| stats count by sourcetype
```

db

```
| db connection=mysql query="SELECT * FROM user_info.user;"
```

Выполнение SQL во время запроса

```
source 'win_events-*
```

```
| append [| db connection=hadoop query="SELECT * FROM  
default.servers LIMIT 10"]
```

```
| stats count by name
```

Комбинирование существующих команд с db

# db конфигурации

## Список конфигураций

[Создать](#)

Название соединения	Строка соединения	Действия
click	jdbc:clickhouse://172.17.0.181:8123	Разрешения <a href="#">Удалить</a>
mysql	jdbc:mysql://localhost/test	Разрешения <a href="#">Удалить</a>
clickhouse_prod	jdbc:clickhouse://172.17.0.181:8123	Разрешения <a href="#">Удалить</a>
<a href="#">mysql</a>	mysql://160.150:156	Разрешения <a href="#">Удалить</a>

Строк на странице: 50 ▾

< [1](#) >

## JDBC-запросы

[Создать](#)

Название	↑ Запрос	Действия
click_query	SELECT * FROM events.nix_events LIMIT 30	Разрешения <a href="#">Удалить</a>
my_sql_macros	SELECT Orders.OrderID, Customers.CustomerName, Orders.OrderDate FROM Orders INNER JOIN Customers ON Orders.Custom...	Разрешения <a href="#">Удалить</a>
test_macr	SELECT * FROM Customers WHERE Country = 'Mexico';	Разрешения <a href="#">Удалить</a>

Строк на странице: 50 ▾

< [1](#) >

## Как использовать?

```
source db:mysql:my_had_query, db:postgre:pg_query
```

```
mysql  
postgre
```

Указываем сохраненные JDBC конфигурации



## Как использовать?

`source db:mysql:my_had_query, db:postgres:pg_query`

my\_had\_query  
pg\_query

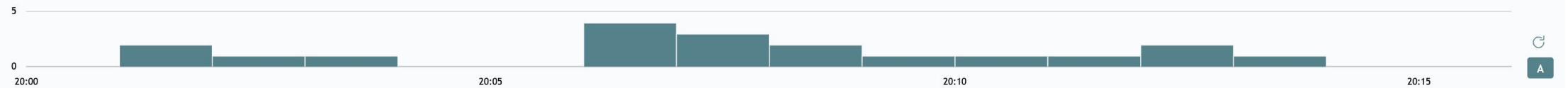
Сохраненные SQL запросы

# Smart Monitor Language

```
1 source win_events-*  
2 | search user.name="bogdanov.t" OR user.name = "ivanov.d"
```

19 документов было найдено за 636 мс (с 13-12-2022 20:00:48 по 13-12-2022 20:15:48)

Отправить в фон | 15 минут назад Даты Обновить



Документы (19) [Статистика](#) [Визуализация](#)

История поиска

Введите поле	Количество
@timestamp	19
@version	1
agent.ephemeral_id	2
agent.hostname	5
agent.id	2
agent.type	1
agent.version	1
ecs.version	1
event.action	4
event.category	1
# event.code	5
event.created	4
event.kind	1

Дата и время	События
> 13-12-2022 20:13:01.267	@timestamp: 2022-12-13T17:13:01.267Z agent.ephemeral_id: 12938567-60c3-4d3a-a227-eae69cab4da3 agent.hostname: SM-S-WIN-MAIL01 agent.id: 03156ce0-1514-4397-9dbb-e310454f583a agent.type: winlogbeat agent.version: 7.3.2 ecs.version: 1.0.1 event.action: Управление учетными записями event.code: 4724 event.created: 2020-10-20T11:08:48.249Z event.kind: event host.ip: 172.16.0.5 host.name: SM-S-WIN-MAIL01 log.level: сведения message: Выполнена попытка сброса пароля учетной записи. Субъект: Идентификатор безопасности: S-1-5-21-253205355-2861714916-1882192604-1338 Имя учетной записи: bogdanov.t Домен учетной записи: VB Идентификатор входа: 0x1504acd3f3 Целевая учетная запись: Идентификатор безопасности: S-1-5-21-253205355-2861714916-1882192604-1481 Имя учетной записи: bogdanov.t Домен учетной записи: VB source.host: SM-NB-B0GDANOV source.ip: 192.168.0.3 source.port: 2269 tags: [ "beats_input_codec_plain_applied" ]
> 13-12-2022 20:12:01.270	@timestamp: 2022-12-13T17:12:01.270Z agent.ephemeral_id: 12938567-60c3-4d3a-a227-eae69cab4da3 agent.hostname: SM-S-WIN-MAIL02 agent.id: 03156ce0-1514-4397-9dbb-e310454f583a agent.type: winlogbeat agent.version: 7.3.2 ecs.version: 1.0.1 event.action: Управление учетными записями event.code: 4724 event.created: 2020-10-20T11:08:48.249Z event.kind: event host.ip: 172.16.0.6 host.name: SM-S-WIN-MAIL02 log.level: сведения message: Выполнена попытка сброса пароля учетной записи. Субъект: Идентификатор безопасности: S-1-5-21-253205355-2861714916-1882192604-1338 Имя учетной записи: bogdanov.t Домен учетной записи: VB Идентификатор входа: 0x1504acd3f3 Целевая учетная запись: Идентификатор безопасности: S-1-5-21-253205355-2861714916-1882192604-1481 Имя учетной записи: bogdanov.t Домен учетной записи: VB

# Smart Monitor Language

## Подсказки команд и описание к ним

```
1 source win_events-*  
2 | stat
```

**stats**

**Stats** ×  
Выполняет статистические операции с данными  
[Смотреть документацию](#)

19 документов было найдено за 636 мс (с 13-12-2022 20:00:48 по ...)

## Подсветка синтаксиса

### Новый поиск

```
1 source win_events-*  
2 | fields user.name  
3 | rename user.name as user  
4 | stats count by user
```

# Smart Monitor Language


## Timeline

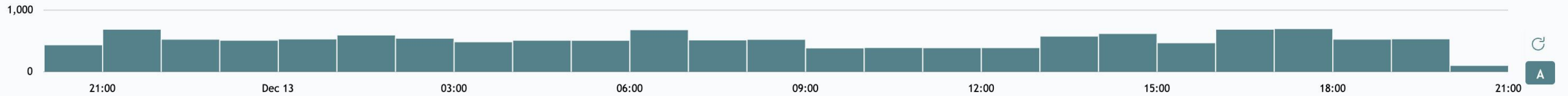
13104 документа было найдено за 1749 мс (с 12-12-2022 20:18:07 по 13-12-2022 20:18:07)

Отправить в фон |  

 24 часа назад

Даты

 Обновить



t agent.hostname	6	<b>source.host</b>
t agent.id	2	
t agent.type	1	
t agent.version	1	
t ecs.version	1	
t event.action	4	
t event.category	1	
# event.code	5	
t event.created	4	
t event.kind	1	
t event.type	1	
t host.ip	6	
t host.name	6	
t log.level	2	
t message	1648	
t process.executable	1	
t process.name	1	
# process.pid	1	
t source.host	13	
t source.ip	13	
# source.port	2866	
t tags	1	

**source.host**

13 значения, в 100.00 % событий  
Количество событий: 13104

Быстрый поиск

[Часто встречаемые](#) Часто встречаемые по времени Редко встречаемые

Все события с этим полем

Значения	Количество	%
SM-WS-IVANOV	1057	8.07 %
SM-NB-KOZLOV	1043	7.96 %
SM-WS-LEBEDEV	1042	7.95 %
SM-WS-VOLKOV	1033	7.88 %
SM-WS-GOLUBEV	1032	7.88 %
SM-WS-VASILIEV	1015	7.75 %
SM-NB-VINOGRADOV	1011	7.72 %

## Field Bar

# Dashboard Framework



Набор базовых визуализаций (table, line chart, column chart, bar chart, ...)

Запуск поискового запроса и отображение его результатов

Возможность настройки Drilldown к дашбордам или произвольной ссылке

Поддержка различных цветовых тем

# Dashboard Framework

```
1 source win_events-*  
2 | timeaggs span=15m count by agent.hostname
```

97 документов было найдено за 383 мс (с 12-12-2022 20:23:00 по 13-12-2022 20:23:00)

Отправить в фон |  

 24 часа назад

Даты

 Обновить

Документы [Статистика \(97\)](#) [Визуализация](#)

 История поиска

 Line

 Добавить на дашборд

Применить настройки

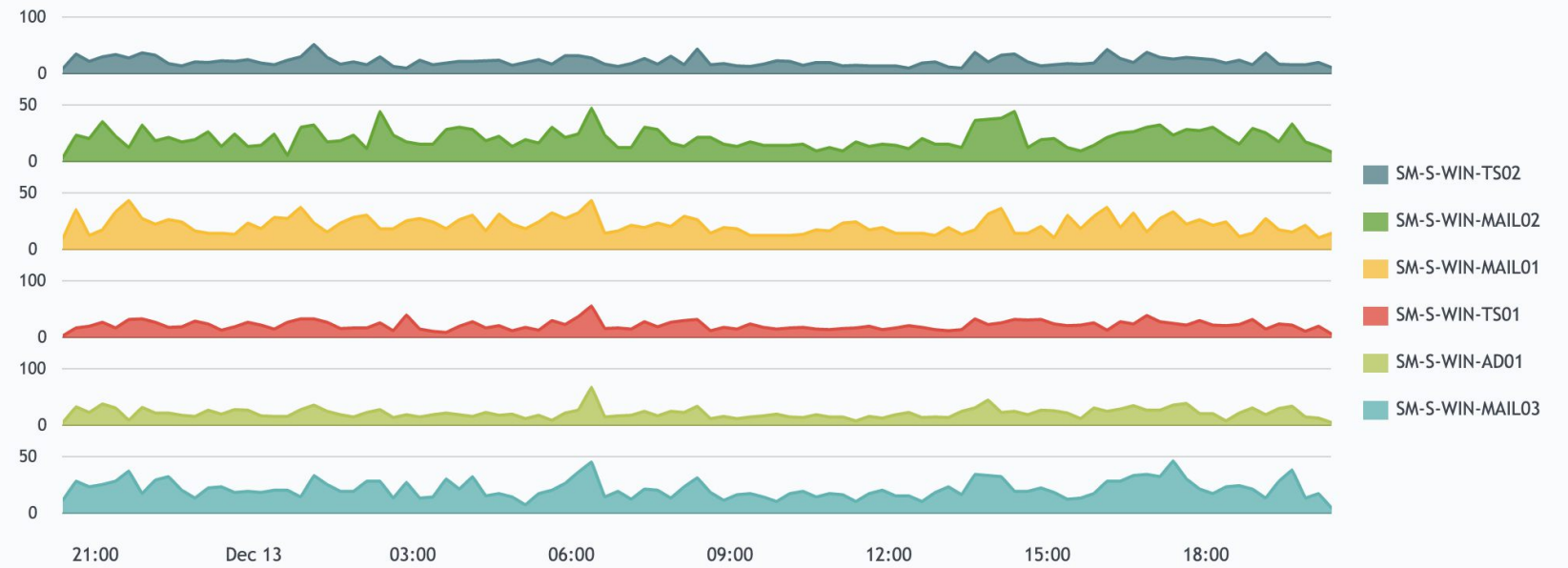
[Главная](#) [Ось X](#) [Ось Y](#) [Легенда](#) [Цветовая схема](#)

Шкала предпросмотра

Группировка

Закраска площади

Разбить по сериям



# Dashboard Framework



Бесшовная интеграция со страницей создания визуализаций

Ресайзинг визуализации по размеру контента

Возможность настройки дашборда с помощью JSON

Выравнивание панелей по сетке

Возможность использования гибкой фильтрации

# Dashboard Framework

SNS: COB

Экспорт

Редактировать

Time

24 часа назад Даты

АРМ

Все ×

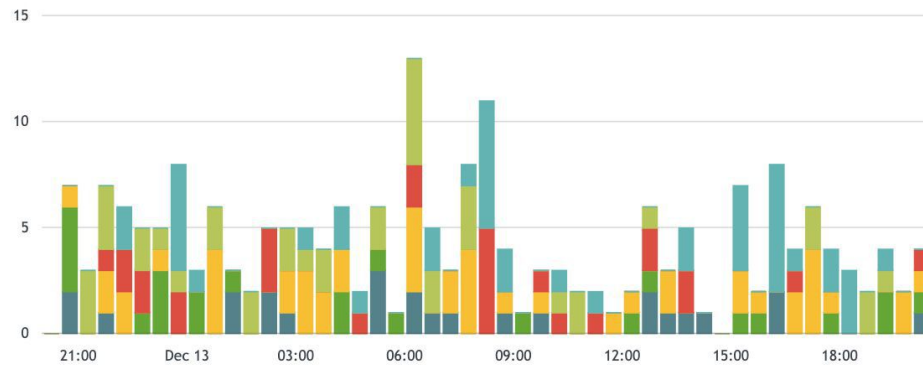
IP-адрес назначения

172.10.0.1 ×  
172.10.0.3 ×  
172.10.0.5 ×  
172.10.0.4 ×

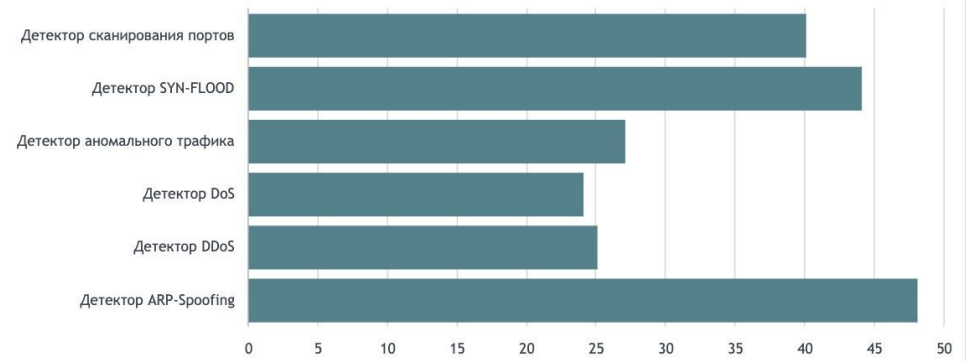
IP-адрес источника

Все ×

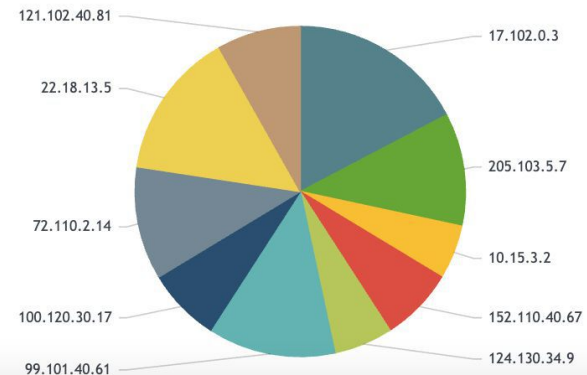
Распределение сетевых атак по подсистемам во времени



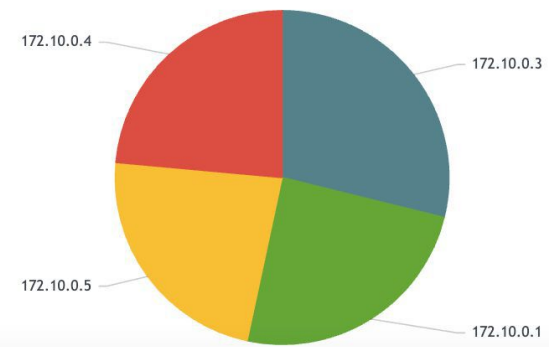
Статистика защитных подсистем



Статистика COB по источнику



Статистика COB по назначению



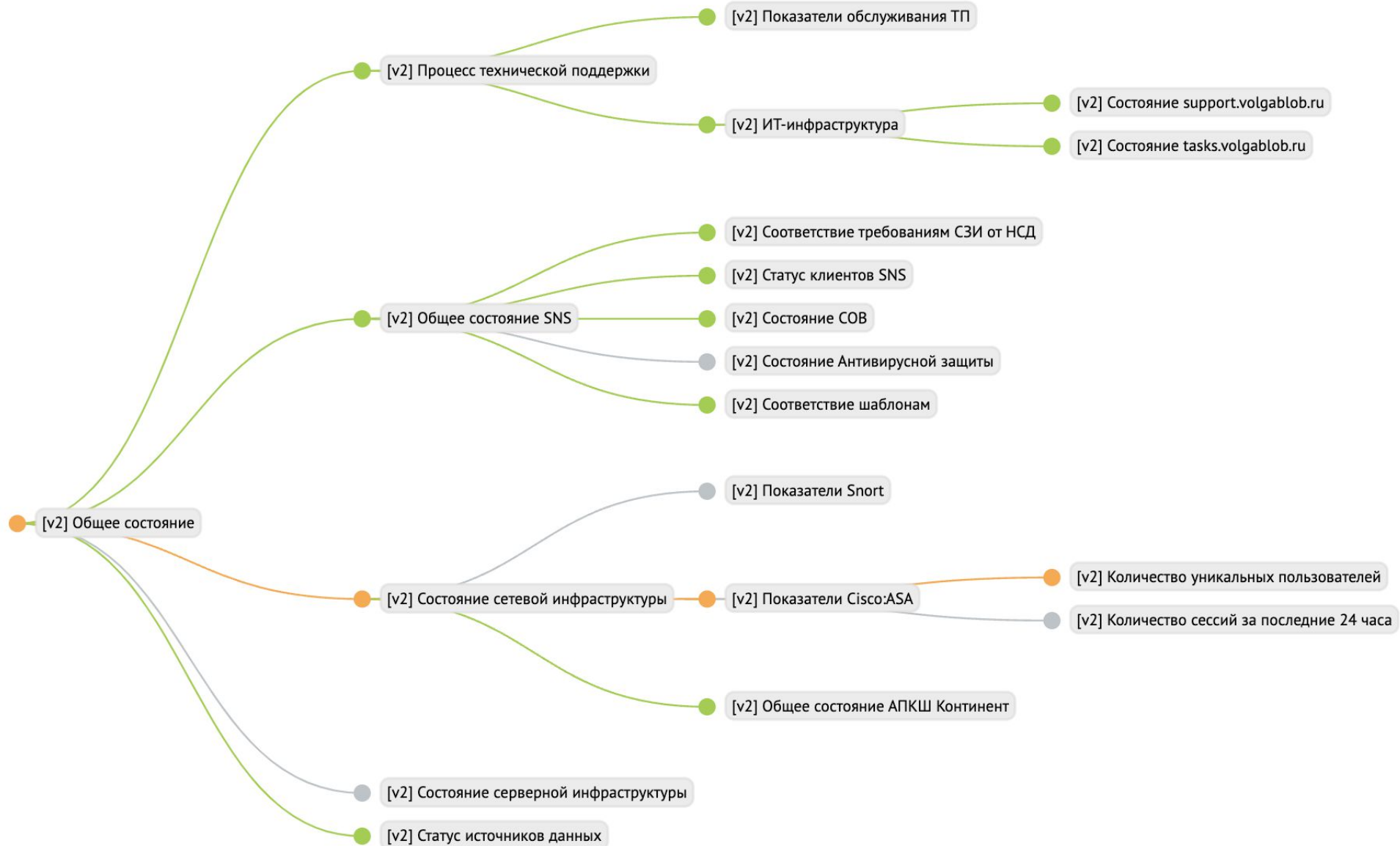


# SDK для создания визуализаций на Smart Monitor

Возможности для разработчиков по внедрению своих вариантов визуализации



# Ресурсно-сервисная модель



# Ресурсно-сервисная модель



# Ресурсно-сервисная модель

Метрика может быть рассчитана с помощью доверительных интервалов

Добавить диапазон

servers\*

По умолчанию 0 75 100

Объекты для диапазона

servers\* x

Укажите объекты для диапазона

Состояние по умолчанию

● Норма

Добавить интервал

Пользовательские интервалы

Состояние	Интервал
● Норма	0 x
● Предупреждение	75 x
● Тревога	100 x

Доверительные интервалы рассчитываются в поисковых запросах.  
Например, с помощью функций avg, stdev

# Ресурсно-сервисная модель

Имя индикатора \*

[v2] Данные sns

Описание индикатора

Настройка зависимостей

Разбивать по объектам

Развернуть все зависимости

Добавить зависимость

sns\_data

1 2 3 4 5 6 7 8 9 10

Отмена Сохранить

# Job Scheduler

<ul style="list-style-type: none"> <li>T1003.004: OS Credential Dumping: LSA Secrets LSA Secrets.</li> </ul>	<ul style="list-style-type: none"> <li>Incident Action</li> <li>Risk Scoring</li> </ul>	<ul style="list-style-type: none"> <li>MITRE ATT&amp;CK®</li> </ul>	<ul style="list-style-type: none"> <li>1-59/15 *****</li> <li>Каждые 15 минут, минуты с 1 по 59</li> </ul>	<ul style="list-style-type: none"> <li>2022-09-21 17:07:35</li> </ul>	<ul style="list-style-type: none"> <li>...</li> </ul>
<ul style="list-style-type: none"> <li>T1016: System Network Configuration Discovery System Network Configuration Discovery</li> </ul>	<ul style="list-style-type: none"> <li>Incident Action</li> <li>Risk Scoring</li> </ul>	<ul style="list-style-type: none"> <li>MITRE ATT&amp;CK®</li> </ul>	<ul style="list-style-type: none"> <li>1-59/15 *****</li> <li>Каждые 15 минут, минуты с 1 по 59</li> </ul>	<ul style="list-style-type: none"> <li>2022-09-21 17:07:38</li> </ul>	<ul style="list-style-type: none"> <li>...</li> </ul>
<ul style="list-style-type: none"> <li>T1049: System Network Connections Discovery Utilities and commands that acquire this information include netstat, "net use," and "net session" with Net. In Mac and</li> </ul>	<ul style="list-style-type: none"> <li>Incident Action</li> <li>Risk Scoring</li> </ul>	<ul style="list-style-type: none"> <li>MITRE ATT&amp;CK®</li> </ul>	<ul style="list-style-type: none"> <li>1-59/15 *****</li> <li>Каждые 15 минут, минуты с 1 по 59</li> </ul>	<ul style="list-style-type: none"> <li>2022-09-21 17:07:53</li> </ul>	<ul style="list-style-type: none"> <li>...</li> </ul>
<ul style="list-style-type: none"> <li>T1057: Process Discovery Process Discovery detected (running tasklist or Get-Process).</li> </ul>	<ul style="list-style-type: none"> <li>Incident Action</li> <li>Risk Scoring</li> </ul>	<ul style="list-style-type: none"> <li>MITRE ATT&amp;CK®</li> </ul>	<ul style="list-style-type: none"> <li>1-59/15 *****</li> <li>Каждые 15 минут, минуты с 1 по 59</li> </ul>	<ul style="list-style-type: none"> <li>2022-09-21 17:07:56</li> </ul>	<ul style="list-style-type: none"> <li>...</li> </ul>
<ul style="list-style-type: none"> <li>T1059.003: Command and Scripting Interpreter: Windows Command Shell Windows Command Shell</li> </ul>	<ul style="list-style-type: none"> <li>Incident Action</li> <li>Risk Scoring</li> </ul>	<ul style="list-style-type: none"> <li>MITRE ATT&amp;CK®</li> </ul>	<ul style="list-style-type: none"> <li>1-59/15 *****</li> <li>Каждые 15 минут, минуты с 1 по 59</li> </ul>	<ul style="list-style-type: none"> <li>2022-09-21 17:08:02</li> </ul>	<ul style="list-style-type: none"> <li>...</li> </ul>
<ul style="list-style-type: none"> <li>T1069.002: Permission Groups Discovery: Domain Groups Domain Groups Discovery</li> </ul>	<ul style="list-style-type: none"> <li>Incident Action</li> <li>Risk Scoring</li> </ul>	<ul style="list-style-type: none"> <li>MITRE ATT&amp;CK®</li> </ul>	<ul style="list-style-type: none"> <li>1-59/15 *****</li> <li>Каждые 15 минут, минуты с 1 по 59</li> </ul>	<ul style="list-style-type: none"> <li>2022-09-21 17:08:12</li> </ul>	<ul style="list-style-type: none"> <li>...</li> </ul>
<ul style="list-style-type: none"> <li>T1087.002: Account Discovery: Domain Account Domain Account Discovery</li> </ul>	<ul style="list-style-type: none"> <li>Incident Action</li> <li>Risk Scoring</li> </ul>	<ul style="list-style-type: none"> <li>MITRE ATT&amp;CK®</li> </ul>	<ul style="list-style-type: none"> <li>1-59/15 *****</li> <li>Каждые 15 минут, минуты с 1 по 59</li> </ul>	<ul style="list-style-type: none"> <li>2022-09-21 17:08:14</li> </ul>	<ul style="list-style-type: none"> <li>...</li> </ul>
<ul style="list-style-type: none"> <li>T1489: Service stop - by net or sc commands Service Stop detected</li> </ul>	<ul style="list-style-type: none"> <li>Incident Action</li> <li>Risk Scoring</li> </ul>	<ul style="list-style-type: none"> <li>MITRE ATT&amp;CK®</li> </ul>	<ul style="list-style-type: none"> <li>1-59/15 *****</li> <li>Каждые 15 минут, минуты с 1 по 59</li> </ul>	<ul style="list-style-type: none"> <li>2022-09-21 17:08:18</li> </ul>	<ul style="list-style-type: none"> <li>...</li> </ul>
<ul style="list-style-type: none"> <li>T1562.001: Impair Defenses: Disable or Modify Tools . Registry change Detect disable or modify security tools (sysmon, win defender, windows security center and etc.). Detect change list of</li> </ul>	<ul style="list-style-type: none"> <li>Incident Action</li> <li>Risk Scoring</li> </ul>	<ul style="list-style-type: none"> <li>MITRE ATT&amp;CK®</li> </ul>	<ul style="list-style-type: none"> <li>1-59/15 *****</li> <li>Каждые 15 минут, минуты с 1 по 59</li> </ul>	<ul style="list-style-type: none"> <li>2022-09-21 17:08:21</li> </ul>	<ul style="list-style-type: none"> <li>...</li> </ul>

# Job Scheduler

## Выполнение запросов по заданному расписанию

Планировщик заданий T1087.002: Account Discovery: Domain Account

Поисковый запрос \*

```
1 source 'sysmon_operational-*' qsize=10000
2 | search (event.code=1 AND (image="*adfind.exe*" OR (( image="*net.exe*" AND command_line="*user*" AND command_line="*domain*") OR
command_line="*get-localuser*" OR command_line="*get-aduser*" OR (command_line="*query*" AND command_line="*user*" AND command_line="*SERVER*") )))
3 | eval mitre_technique_id="T1087.002"
4 | eval eventaction = event.action
5 | table @timestamp, mitre_technique_id, eventaction, host.name, host.ip, user, original_file_name, image, parent_image, command_line, parent_command_line,
process_id, parent_process_id, process_guid, parent_process_guid
6
```

Временной интервал: 15 минут назад Даты

Временное поле \*: @timestamp Поле, содержащее временную метку, например: @timestamp

Длительность блокировки (сек.): 15 Период времени, в течение которого не будут происходить повторные запросы если предыдущий запрос еще не завершился

Расписание Каждые 5 минут, минуты с 2 по 59  
Периодичность и подавление запуска

Периодичность

Тип расписания: Интервал **Срон-выражение**

Срон: 2-59/5 \* \* \* \* \*  
Каждые 5 минут, минуты с 2 по 59

Подавление

Длительность: 15 Ед. Минуты

Поля для подавления: user × host.name × process\_id ×

Активные действия по  
результаты выполнения

(E-mail, SMS, Messenger,  
заведение инцидентов,  
агрегация результатов  
индекс и др.)

# Job Scheduler

**T1057: Process Discovery** Отменить Сохранить

Главное Действия **3**

Развернуть все Системные **3** Добавить

**1** Incident Action ✕

Название: T1057: Process Discovery. User: {{\_soi}}    Критичность: Предупреждение    Workflow: Default workflow

Описание: Detect running tasklist for user {{\_source.user}} and host {{\_source.host.name}}.

Тип детализации: Поиск    Детализация: source ...

**Дополнительные поля**  
Заполнение полей из карточки инцидента

**Поля из результатов поиска**

**Локальные параметры** incident\_id

**2** > MITRE ATT&CK® ✕

**3** > Risk Scoring ✕

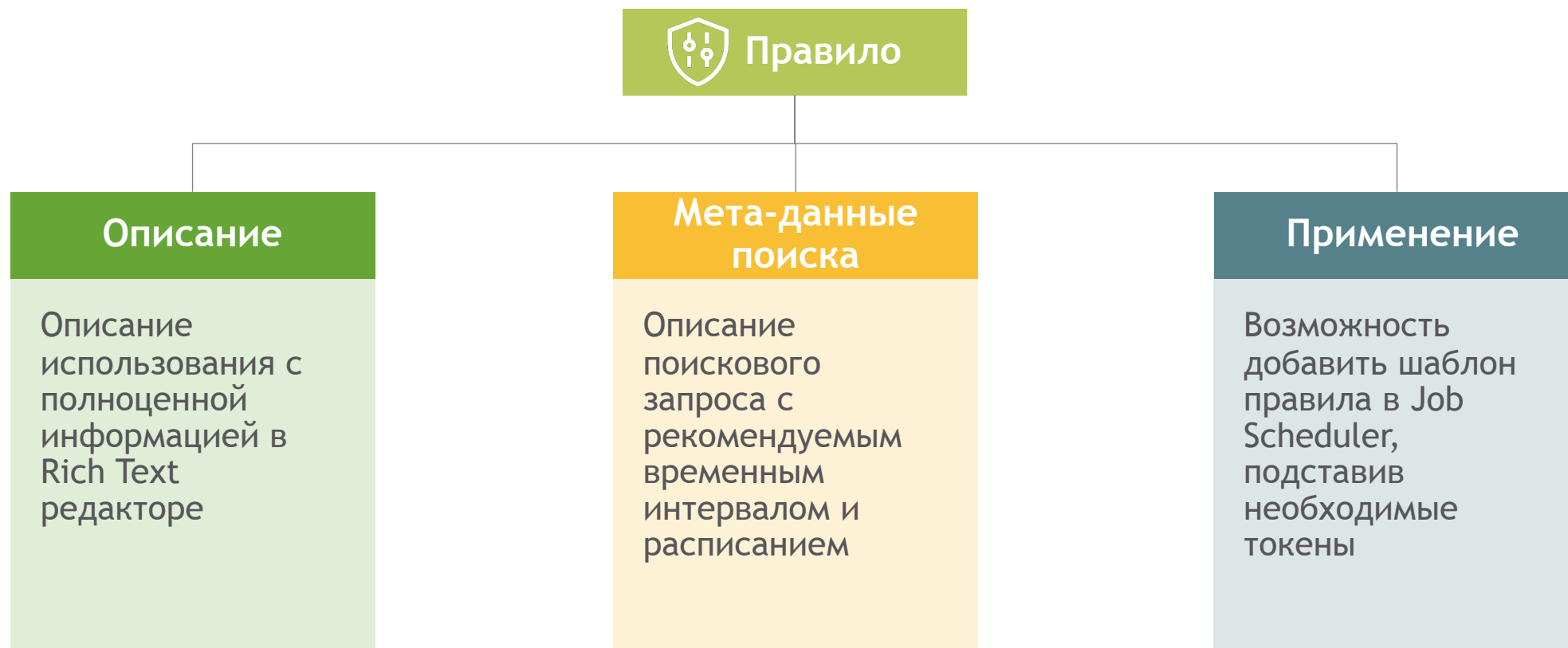


# Knowledge Center - теперь в Core!



# Правила

Корреляционные правила, которые можно использовать для реализации



# Правила

Корреляционные правила, которые можно использовать для реализации

## Список правил

Критичность ▾

Теги ▾

Создать

Наименование правила	Краткое описание	Критичность	Теги	Дата обновления	
SM:RULE:Windows:CreateOrChangeLocalAccounts	Обнаружение событий создания/изменения локальных УЗ на хостах Windows	● Средняя	Операционная система Microsoft Windows	2022-07-06 11:48	☐☐☐
SM:RULE:ChangeAuditor:IrregularDomainReplication	Обнаружение попытки несанкционированной/некорректной репликации домена	● Высокая	Change Auditor	2022-07-06 11:08	☐☐☐
SM:RULE:ChangeAuditor:SetUserNeverExpired	Изменен срок действия учетной записи, активирована опция Never Expired	● Средняя	T1098 Change Auditor	2022-07-06 11:58	☐☐☐
SM:RULE:DataFlow:NoEventsInIndex	Отсутствуют события в контролируемых индексах за последний час	● Высокая	T1562 SM Data Flow	2022-07-06 12:14	☐☐☐
SM:RULE:WEB:ExchangeExploitation	Обнаружена потенциальная попытка эксплуатации уязвимости CVE-2021-28480 на Exchange	● Средняя	Веб-сервер Nginx Microsoft Exchange T1190 IIS CVE-2021-28480	2022-07-06 18:01	☐☐☐
SM:RULE:F5:VulnerabilityExploitationAttempt	Обнаружена потенциальная попытка эксплуатации уязвимости CVE-2020-5902 на F5 BIG-IP	● Высокая	T1190 F5 BIG IP CVE-2020-5902	2022-07-06 16:56	☐☐☐

# Правила

## Корреляционные правила, которые можно использовать для реализации

### SM:RULE:Sysmon:PermissionGroupsDiscovery

[Разрешения](#)[Редактировать](#)

#### Описание правила

Злоумышленник может попытаться определить состав групп, пользователей и разрешений. Эта информация может помочь злоумышленникам определить, какие существуют учетные записи и группы пользователей, членство пользователей в определенных группах, какие пользователи и группы имеют повышенные разрешения.

Поисковый запрос позволяет получить информацию о выполнении любых команд в *Командной строке* (cmd) или консоли *PowerShell*, содержащих сочетания **net**, **localgroup**, **group**, **domain**, **get-localgroupmember**.

Данные команды позволяют получить различные сведения о локальных и доменных группах: **перечень**, **состав** и т.д.

#### Время создания

2021-11-09 15:05:53

#### Последнее обновление

2022-12-13 19:45:56

#### Название запроса

Sysmon: Пользователь {{\_source.user}} выполнил команду для получения информации о локальных или доменных группах безопасности на хосте {{source.host.name}}

#### Описание запроса

Пользователь {{\_source.user}} выполнил команду для получения информации о локальных или доменных группах безопасности на хосте {{source.host.name}}

"fields" : { "@timestamp" : "Время события", "eventaction" : "Действие", "event\_type" : "Тип события", "host.name" : "Хост", "host.ip" : "IP-адрес хоста", "image" : "Исполняемый файл", "target\_object" : "Целевой объект", "details" : "Детали", "process\_id" : "ID процесса", "process\_guid" : "GUID процесса" }

#### Критичность

● Низкая

#### Расписание запуска

2-59/5 \* \* \* \* \* 

#### Временной интервал

now+15m

now

```
1 source {{sysmon_index}}
2 | search (event.code=1 AND ((command_line="*net*" AND
   command_line="*localgroup*") OR (command_line="*net*" AND
   command_line="*group*" AND command_line="*domain*") OR
   command_line="*get-localgroupmember*" ))
3 | eval mitre_technique_id = "T1069.002"
4 | lookup {{sysmon_process_create_exceptions}} mitre_technique_id host.name
   user image parent_image command_line parent_command_line output reason
5 | where isnull(reason)
6 | eval eventaction = event.action
7 | table @timestamp, mitre_technique_id, eventaction, host.name, host.ip,
   user, original_file_name, image, parent_image, command_line,
   parent_command_line, process_id, parent_process_id, process_guid,
   parent_process_guid
```

[Добавить в Job Scheduler](#)

# Wikilogs - динамические статьи!

## Демо страница

× Закрыть

Сохранить



Редакция от 2022-12-13 20:04:47 ▾

+

 Прикрепите или перетащите файлы (макс. размер файла - 100 МБ)

# Глобальная строка поиска

## Spotlight

Search bar: WS579

Active tasks: Активные задачи

User: admin

Search results for WS579:

- [dns: NSK-WS579.it.volga.wave | hostname: NSK-WS579 | ip: 172.216.70.75...](#)
- Актив • Inventory • category: workstation | cpu\_num: 6 | disk\_capacity: 800 |...

[Посмотреть другие результаты](#)

Сквозной поиск по  
объектам **Smart Monitor!**

Search bar: LSA

Active tasks: Активные задачи

User: admin

Search results for LSA:

- [Попытка получения доступа к данным процесса LSASS](#)  
Правило • Knowledge Center • Выявление попыток доступа к данным процесса LSASS п
- [Дамп учетных данных ОС - LSA Secrets](#)  
Правило • Knowledge Center • Злоумышленник может попытаться сделать дамп учетн
- [Попытка получения доступа к учетным данным в ОС](#)  
Сценарий • Knowledge Center • Когда злоумышленник пытается получить доступ к ата
- [Дамп учетных данных ОС - LSASS](#)  
Правило • Knowledge Center • Злоумышленник может попытаться создать дамп учетн
- [Изменения в системном реестре](#)  
Статья • Knowledge Center • 1. Открытие инцидента В Менеджере инцидентов фиксир

[Посмотреть другие результаты](#)

RM-1Y, SM-IM-TERM-1Y, SM-CYBER-SC-TERM-1Y, SM-CONT-TERM-1Y, SM-CYBER-SC-TERM-1Y

# Smart Beat



Управление агентами Beats

Поддержка централизованного управления конфигурацией агентов

Автоматический запуск нескольких Beats без необходимости установки

Простой процесс управления агентами и их обновление

# Smart Beat Manager



- Входит в Smart Monitor Core

- Сервер управления для Smart Beat

- Возможность распространения конфигураций для агентов Beats

- Возможность удаленного обновления версий самих Beats

- Веб-интерфейс для просмотра текущей конфигурации и активных Smart Beat



# Smart Beat Manager

## Управление Smart Beat

ВСЕГО КЛИЕНТОВ

15



ПОДКЛЮЧЕННЫХ КЛИЕНТОВ

8



КЛИЕНТЫ С ОШИБКОЙ

7



Файлы (14) Приложения (47) Группы (14) Клиенты (15)

## Клиенты

Поиск...

Система ▾

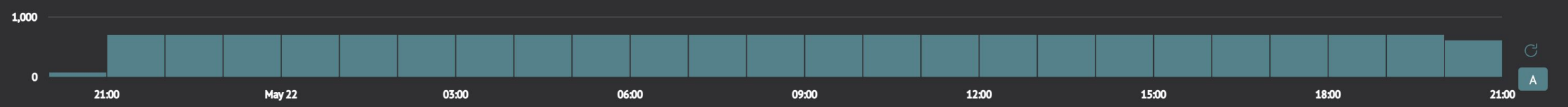
Статус ▾

Имя хоста	GUID	IP-адрес	DNS	Система	Версия	Статус
> ad	af28f439-35a3-4a5f-9346-0bb6bb523e33	192.168.0.1	ad.demo	windows	2.2.0.0	● Ошибка
> AD2	149a70a4-4130-4b34-82a8-c4fd3adb7874	192.168.0.2	ad2.demo	windows	2.2.0.0	● Ошибка
> linux-demo	ca5e000a91777ddcf297d872ecf096ea3443ca65a4a2197a22f9f24ad93e2950	192.168.0.3	null	linux-amd64	2.2.4.0	● Запущен
> exchange-demo	3a95167c-4efe-480f-8209-603f98fb4974	192.168.0.4	exchange-demo	windows	2.2.0.0	● Ошибка
> demo	93064bdc-8901-4a79-ad3b-043800df4d57	192.168.0.5	null	GNU/Linux	-	● Запущен

# Темная тема

1 source 'sysmon\_operational-\*

🕒 17 267 документов было найдено за 230 мс (21-05-2023 20:52:22 to 22-05-2023 20:52:22) 🗑 Отправить в фон | 📁 📧 🔗 📅 24 часа назад Даты 🔄 Обновить



Документы (17 267) [Статистика](#) [Визуализация](#) ☰ История поиска

Введите поле

- t @timestamp
- t @version
- t agent.ephemeral\_id
- t agent.hostname
- t agent.id
- t agent.name
- t agent.type
- t agent.version
- t command\_line
- t details
- t ecs.version
- t event.action
- # event.code
- t event.created


Дата и время	События
> 22-05-2023 20:52:21.000	<pre>@timestamp: 2023-05-22T17:52:21.000000Z agent.ephemeral_id: ff48b083-4f49-4915-a6c2-09e8b7b19273 agent.hostname: Client1win10 agent.id: ac4299c3-3b05-4a9f-8d65-4020d6da22f7 agent.name: Client1win10 agent.type: winlogbeat agent.version: 7.10.2 command_line: C:\AtomicRedTeam\atomics\T1003.001\bin\procdump.exe -accepteula -ma lsass.exe C:\Windows\Temp\lsass_dump.dmp details: Binary Data ecs.version: 1.5.0 event.action: Process Create (rule: ProcessCreate) event.code: 1 event.created: 2023-05-22T17:52:21.000000Z event.kind: event event.provider: Microsoft-Windows-Sysmon event_type: - host.architecture: x86_64 host.hostname: Client1win10 host.id: 43d6865d-6fbf-4c36-aa35-61741f45b378</pre>
> 22-05-2023 20:52:16.000	<pre>@timestamp: 2023-05-22T17:52:16.000000Z agent.ephemeral_id: 62e50066-40c8-404b-ad6e-787833c232ce agent.hostname: DC01 agent.id: c1794ce2-673a-4288-8b45-2380b22c7fd8 agent.name: DC01 agent.type: winlogbeat agent.version: 7.10.2 details: Binary Data ecs.version: 1.5.0 event.action: File created (rule: FileCreate) event.code: 11 event.created: 2023-05-22T17:52:16.000000Z event.kind: event event.provider: Microsoft-Windows-Sysmon event_type: - host.architecture: x86_64 host.hostname: DC01 host.id: 43d6865d-6fbf-4c36-aa35-61741f45b378 host.ip: 169.254.183.199</pre>

# Темная тема

## Новый поиск

```
1 source 'sysmon_operational-*'  
2 | timeaggs count
```

🕒 17 266 документов было найдено за 59 мс (21-05-2023 20:53:43 to 22-05-2023 20:53:43)

Отправить в фон |   

📅 24 часа назад

Даты

 Обновить

Документы [Статистика \(49\)](#) Визуализация

 История поиска

 Line ▾

 Добавить на дашборд

Применить настройки

Главная [Ось X](#) [Ось Y](#) [Легенда](#) [Цветовая схема](#)

Шкала предпросмотра

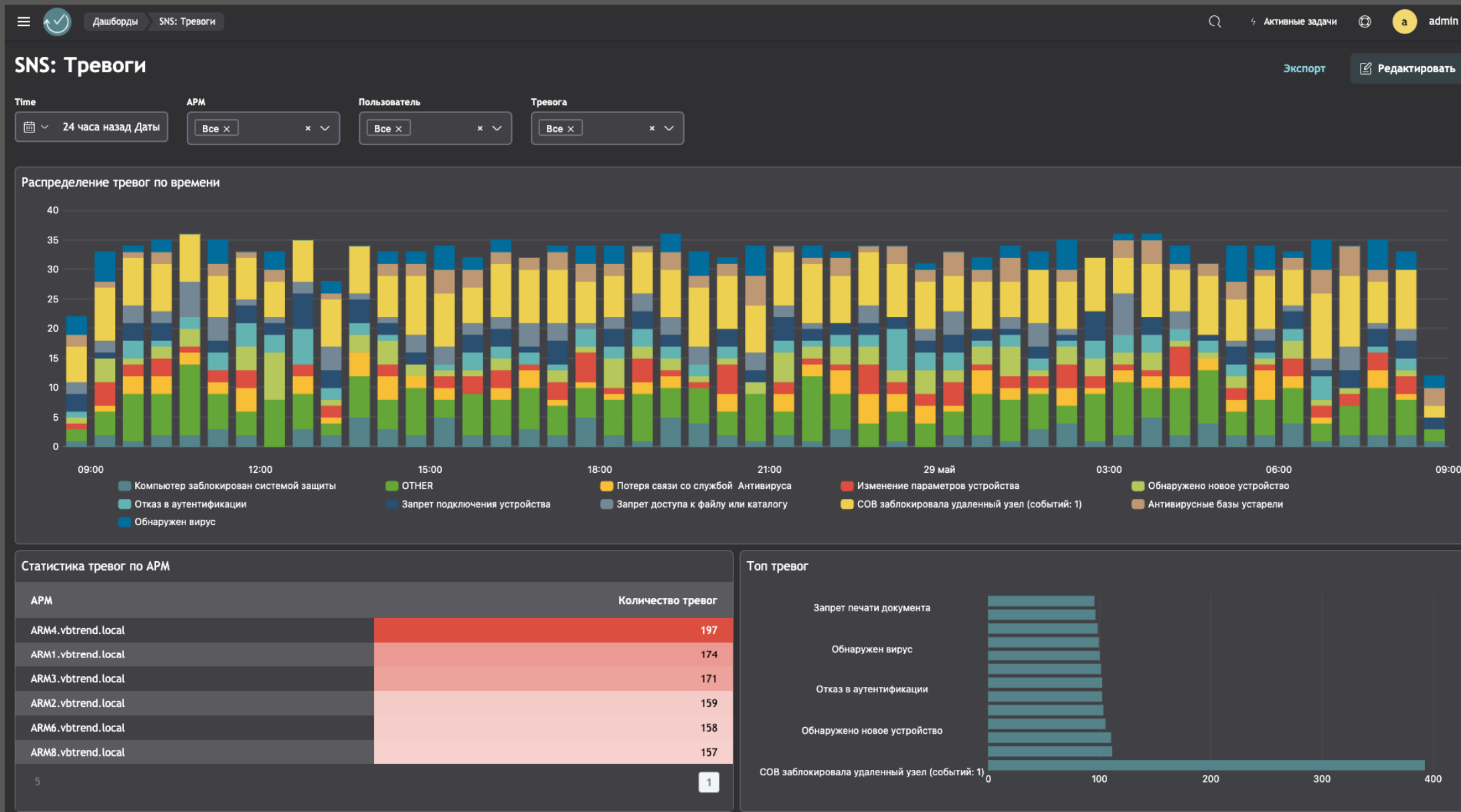
Группировка

Закраска площади

Разбить по сериям



# Темная тема



# Производительность системы



## Варианты поставки модуля Core

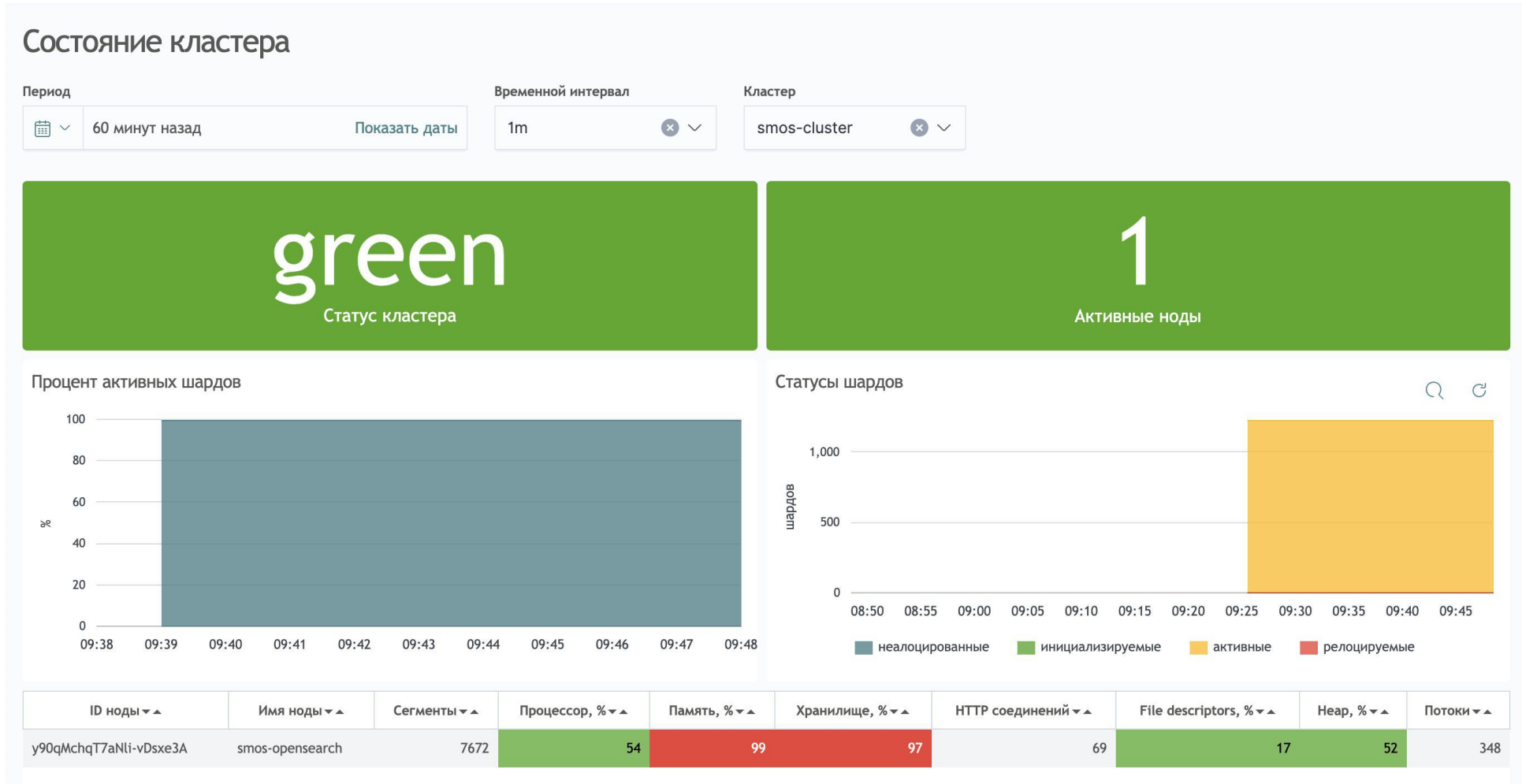
Вариант Core	Максимальный объем хранилища (Гб) Объем дискового хранилища, в рамках которого происходит ротация данных	Ограничения по EPS лимит по числу событий в секунду	Ограничения по Гб/д лимит по объему индексируемого трафика	Кластер Возможность настройки репликации данных	Data Collecting Nodes* далее с до закупкой дополнительных нод
Core Lite 150	До 150 Гб	10000 EPS	250 Гб/д	Нет	1
Core Lite 300	До 300 Гб	10000 EPS	250 Гб/д	Нет	1
Core	Без ограничений	10000 EPS	250 Гб/д	Нет	1
Core Cluster	Без ограничений	Без ограничений	Без ограничений	Да	7
Core Cluster +	Без ограничений	Без ограничений	Без ограничений	Да	70

\* - Data Collecting Node - это сервер с эталонной конфигурацией (16 CPU/64 RAM), который осуществляет прием, первичную обработку, индексирование и фазу "горячего" хранения событий

# Self Monitoring



# Состояние кластера





# Ресурсы узла

41

Загрузка процессора, %

99

Загрузка памяти, %

97.135

Заполненность хранилищ, %

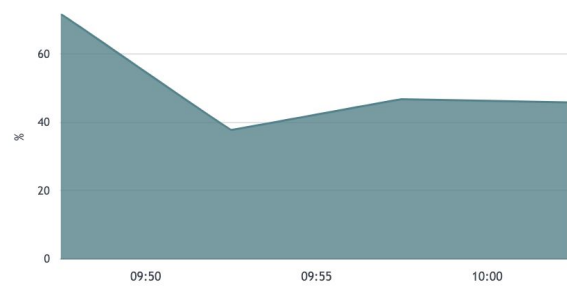
11,050

Открытых file descriptor

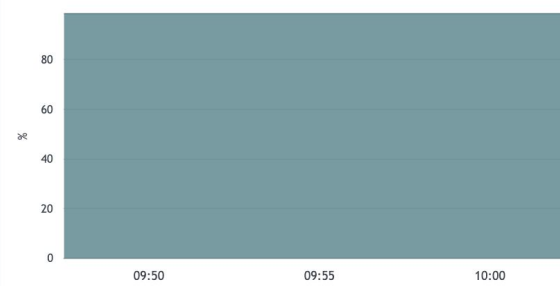
68

Открытых HTTP соединений

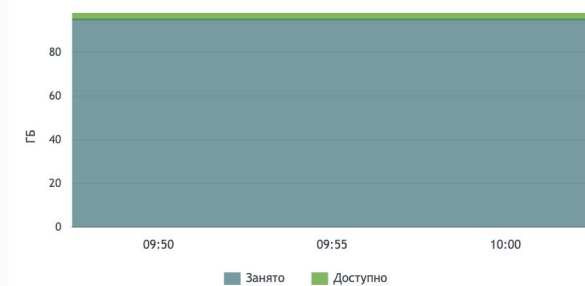
Загрузка процессора



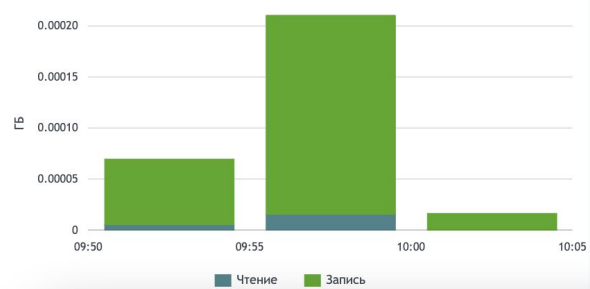
Загрузка памяти



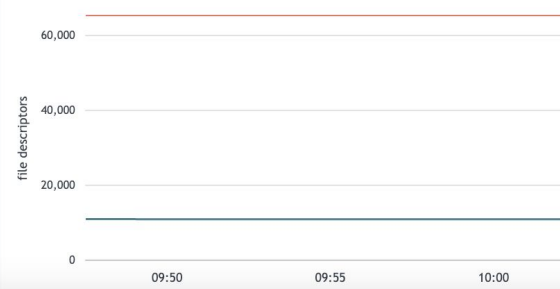
Состояние хранилища



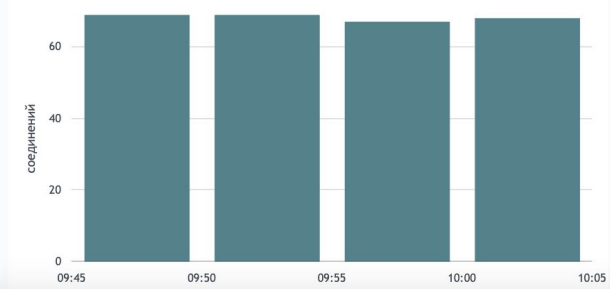
Объем чтения/записи



Открытые file descriptor



Открытые HTTP соединения

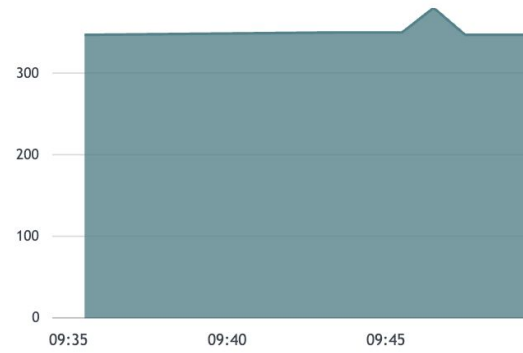


# Мониторинг JVM

348

Кол-во Поток

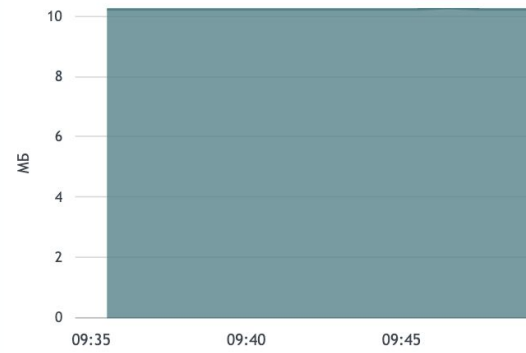
Кол-во потоков



10.25

Размер Direct Buffer, МБ

Размер Direct Buffer



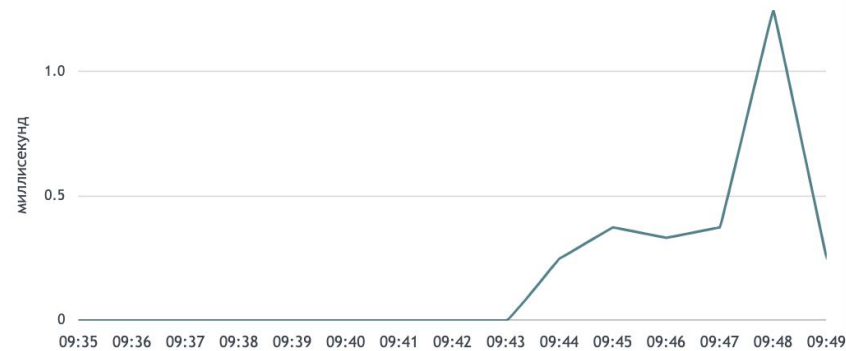
70

Использование Heap, %

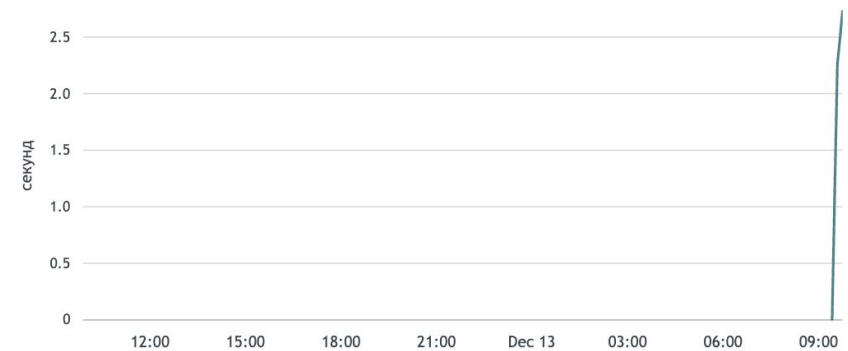
Состояние памяти JVM



Среднее время паузы GC



Среднее время цикла GC



# Поиск и индексация

0

Неудавшиеся индексации

0

Индексация в давлении, секунд

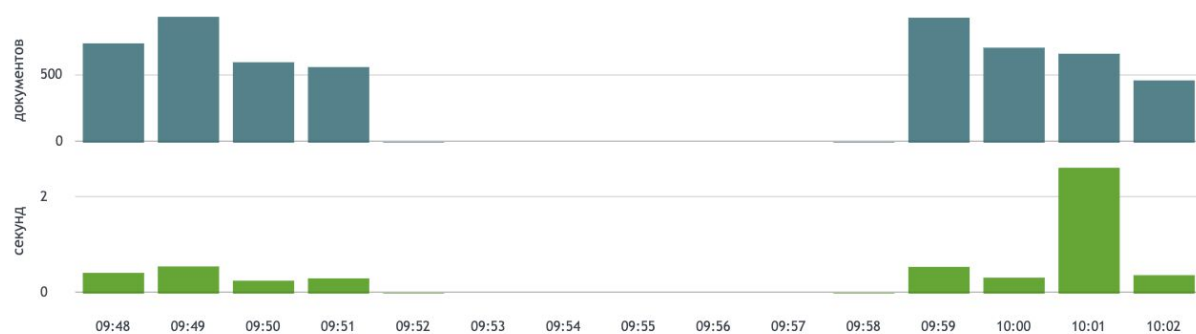
0

Активных merge

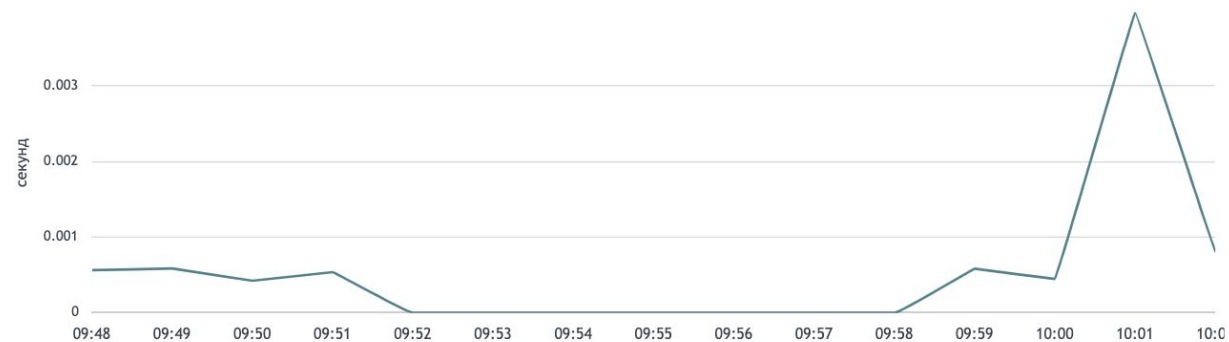
0

Merge использует памяти, МБ

Количество индексаций



Среднее время индексации документа



# Поиск и индексация



# Режим Service Provider



# Режим Service Provider

Настройки Подключенные клиенты

Активные задачи admin

## ОСНОВНОЕ

- Стили
- Настройки экспорта в PDF
- Настройки планировщика
- Настройки меню
- Grok Debugger
- Локализация
- Painless-скрипты
- JDBC-запросы
- JDBC-соединения

## SERVICE PROVIDER

- Управление
- Подключенные клиенты

## INCIDENT MANAGEMENT

- Карточка инцидента
- Рабочий процесс

## OPENSEARCH

- Шаблоны индексов

## Подключенные клиенты

Поиск...

Префикс клиента	Состояние клиента	Количество серверов	Хранилище
smos-cluster-24	yellow	1	smos-node-24: 29.1 GB / 43.39 GB

> Информация о кластере > Информация о серверах

Индексы

Поиск...

Состояние	Индексы	Количество документов	Количество удаленных докуме...	Размер хранилища	Дата создания
yellow	.smos_search_history	0	0	208	2022-10-03T17:58:52.554Z
yellow	.smos_diagrams	0	0	208	2022-10-03T17:58:46.378Z
yellow	.smos_jobs	0	0	208	2022-10-03T17:58:52.978Z
yellow	.smos_wiki_template	1	0	10962	2022-10-03T17:58:46.248Z
yellow	.smos_models	0	0	208	2022-10-03T17:58:53.069Z
yellow	.smos_metrics	0	0	208	2022-10-03T17:58:52.913Z
yellow	internal_audit-2022.10	86921	0	11474284	2022-10-03T17:53:17.257Z
yellow	.smos_search_favorite	0	0	208	2022-10-03T17:58:52.635Z
green	.opendistro_security	9	0	50706	2022-10-03T17:53:12.531Z
green	.kibana_1	0	0	208	2022-10-03T17:58:45.963Z
yellow	.smart_monitor	9	0	176887	2022-10-03T17:53:17.293Z
yellow	.smos_permissions	0	0	208	2022-10-03T17:58:52.784Z

# Режим Service Provider

**Список заданий**

Включено Выключено Действия ▾ Мета-задания Все задания Создать

Клиент	Описание	↑ Активные реакции	Расписание	Последнее обновление	Действия
smos-node-23 smos-node-24	<span>●</span> Отсутствие событий от Windows-сервера Генерирует предупреждение о количестве событий	<span>Incident Action</span>	***** Каждую минуту	2022-12-05 10:39:26	...

Строк на странице: 50 ▾ < 1 >

# Режим Service Provider

## Отсутствие событий от Windows-сервера

✕ Отменить Сохранить

Главное Действия 1

**Основное**  
Название, поисковый запрос smos-node-23 smos-node-24

**Имя \***  
Отсутствие событий от Windows-сервера

**Клиент**  
smos-node-23 ✕ smos-node-24 ✕ ✕ ▾

**Описание**  
Генерирует предупреждение о количестве событий

**Поисковый запрос \***  
1 source win\_events-\* qsize=10  
2 | aggs count

**Временной интервал**  
📅 ▾ 60 минут назад Даты

**Временное поле \***  
@timestamp  
Поле, содержащее временную метку, например: @timestamp

**Длительность блокировки (сек.) \***  
10  
Период времени, в течение которого не будут происходить повторные запросы если предыдущий запрос еще не завершился

**Расписание**  
Периодичность и подавление запуска Каждую минуту



# Incident Manager

Регистрация и процесс обработки инцидентов

# Incident Manager

**Фиксация важных  
событий**

Статусы  
инцидентов

Назначение  
ответственных

Создание  
инцидентов  
вручную

История  
изменений и  
комментарии

**Уровни критичности**

# Incident Manager

Фиксация важных  
событий

**+ Workflow**

Создание  
инцидентов  
вручную

История  
изменений и  
комментарии

Уровни критичности

# Incident Manager

## Менеджер инцидентов

Последние 120 дней Обновить Настройки

102	20	12
ТРЕВОГА	ПРЕДУПРЕЖДЕНИЕ	ИНФОРМАЦИЯ

Поиск... Критичность Workflow Статус Ответственный Создать инцидент

Дата и время	Инцидент	Статус	Ответственный
2022-12-13 09:00:39.526	SmartCode: [SNS] Потеряно соединение с антивирусной службой	IN PROGRESS	demo_test
2022-12-13 08:45:26.805	SmartCode: [SNS] Потеряно соединение с антивирусной службой	NEW	Не задан
2022-12-13 08:43:11.944	SmartCode: [SNS] Обнаружено отключение службы антивируса на хосте ARM01.vbtrend.local	NEW	Не задан

Уровни критичности

Трекинг статусов

Комментарии

История изменений

2022-09-12 14:23:02.565 T1016: System Network Conf Discovery. User: (SM\silkin.i). Host: (client2winsrv.sm.local) NEW demo\_user

**T1016: System Network Conf Discovery. User: (SM\silkin.i). Host: (client2winsrv.sm.local)**

Описание  
Detect system network configuration discovery for user SM\silkin.i and host client2winsrv.sm.local.

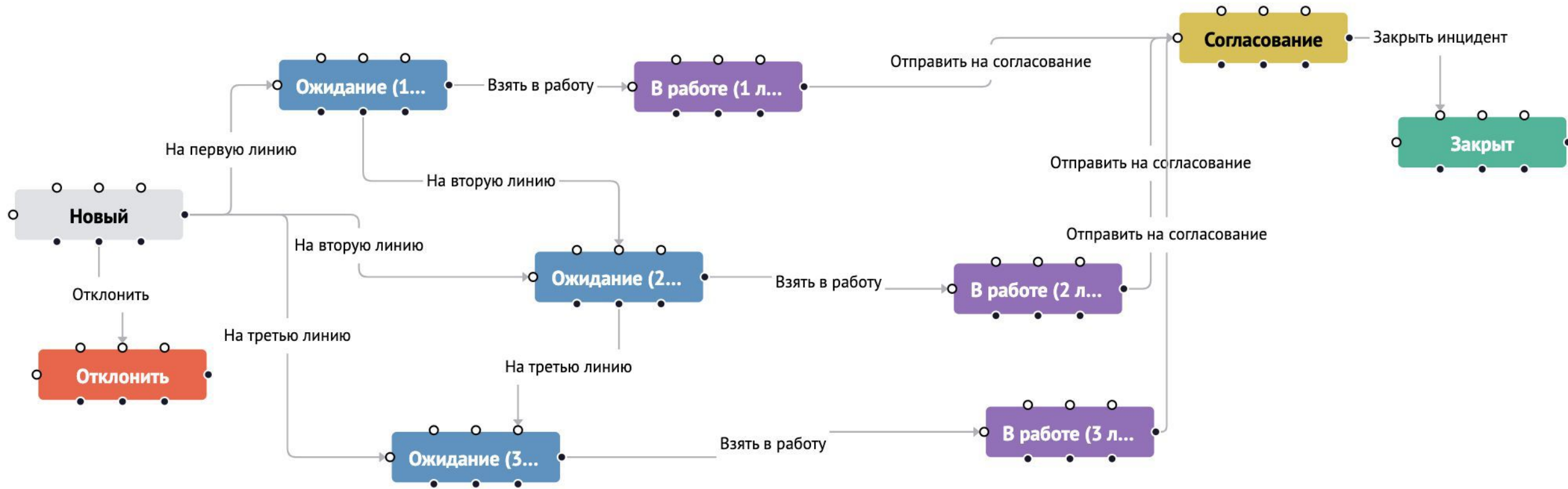
Дополнительные поля

parent_process_id:	4216
image:	C:\Windows\System32\ipconfig.exe
process_id:	4928
parent_command_line:	"C:\Windows\system32\WindowsPowerShell\v1.0\PowerShell_ISE.exe"
eventaction:	Process Create (rule: ProcessCreate)
host.ip:	fe80::a1a7:fca2:9adc:ca7 169.254.12.167 172.16.0.104
@timestamp:	2022-09-12T11:20:27.425Z
process_guid:	43D6865D-15FB-631F-E407-000000002B00
mitre_technique_id:	T1016
parent_image:	C:\Windows\System32\WindowsPowerShell\v1.0\powershell_ise.exe
original_file_name:	ipconfig.exe
parent_process_guid:	43D6865D-9505-6318-F200-000000002B00
host.name:	client2winsrv.sm.local
user:	SM\silkin.i
command_line:	C:\Windows\system32\ipconfig.exe

История

- admin добавил комментарий - 2022-09-13 14:29:42  
Инцидент отправлен на проверку
- admin изменил поле Ответственный с Не задан на demo\_user - 2022-09-13 14:29:42
- admin изменил поле Статус с IN PROGRESS на check - 2022-09-13 14:29:22
- admin изменил поле Статус с NEW на IN PROGRESS - 2022-09-13 14:29:19

# Пример рабочего процесса



# Workflow — активные действия

- Первичные действия могут **влиять** на параметры инцидента
- Разделяются на системные и **пользовательские**
- Пользовательские действия могут быть реализованы на NodeJS / Python

## Первичные действия

- Автоматическое назначение ответственного
- Регистрация времени изменения статуса
- Проверка времени изменения статуса (**соответствие SLA**)

## Другие действия

- Отправка оповещения на почту
- Отправка оповещения в мессенджер
- Интеграция с **Service Desk** (передача информации об инциденте)

# Inventory

Инструмент формирования и управления активами

# Inventory: Назначение

Модуль обеспечивает:

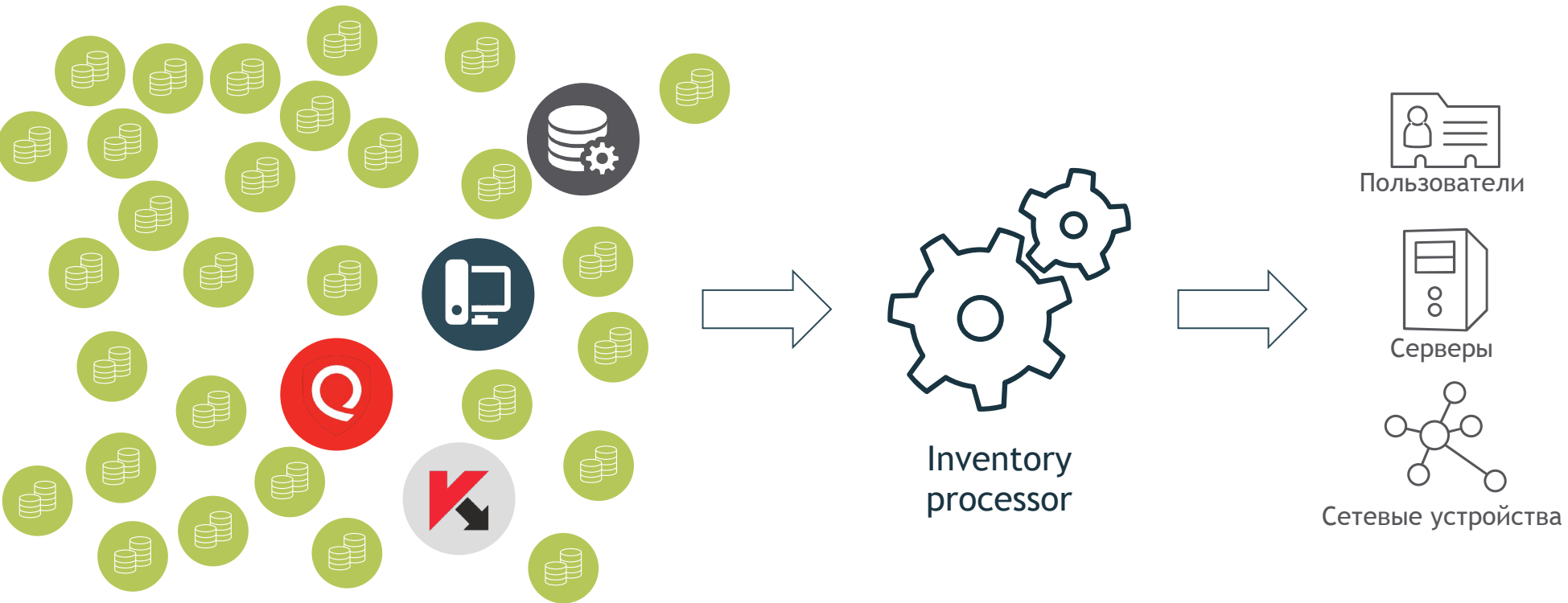
- Формирование единой базы активов
- Поддержку данной базы в актуальном состоянии





# Inventory

⊕ Автоматизированный сбор и обновление базы активов от различных источников



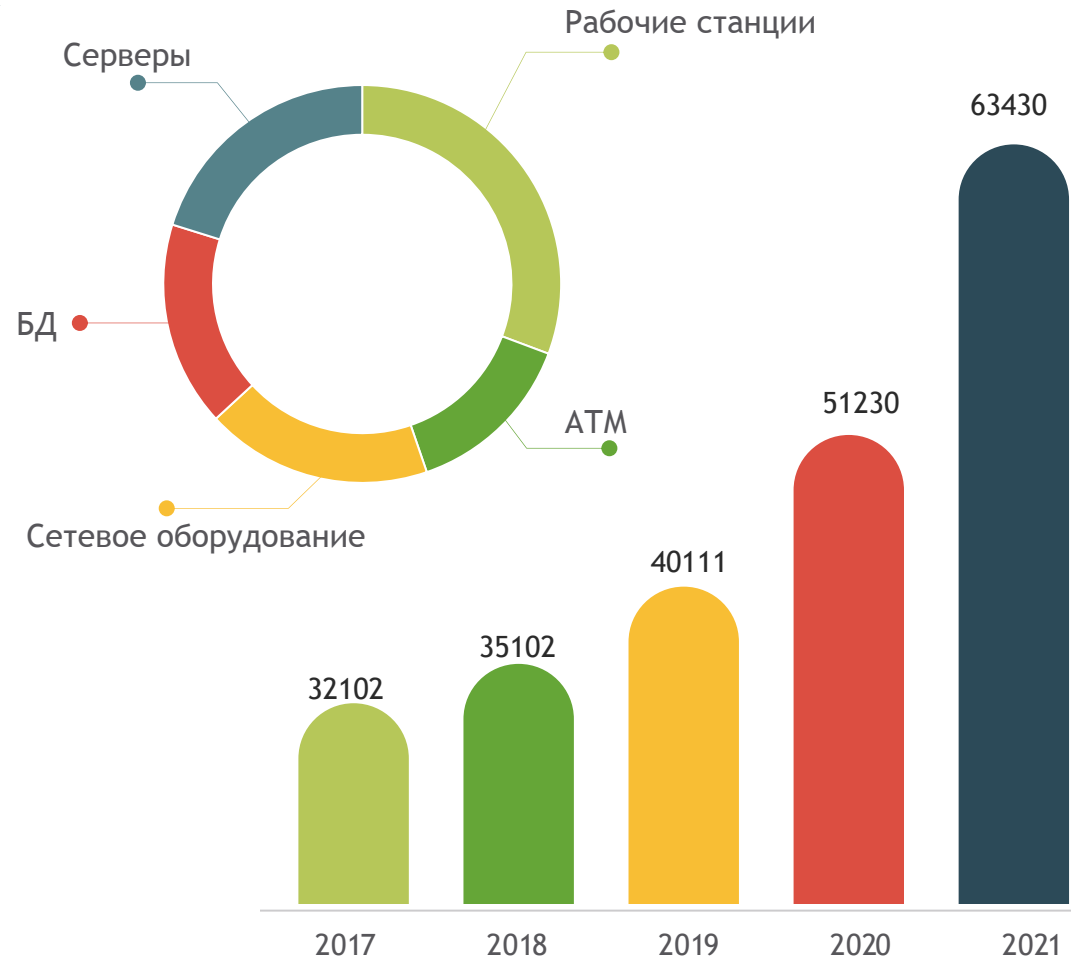
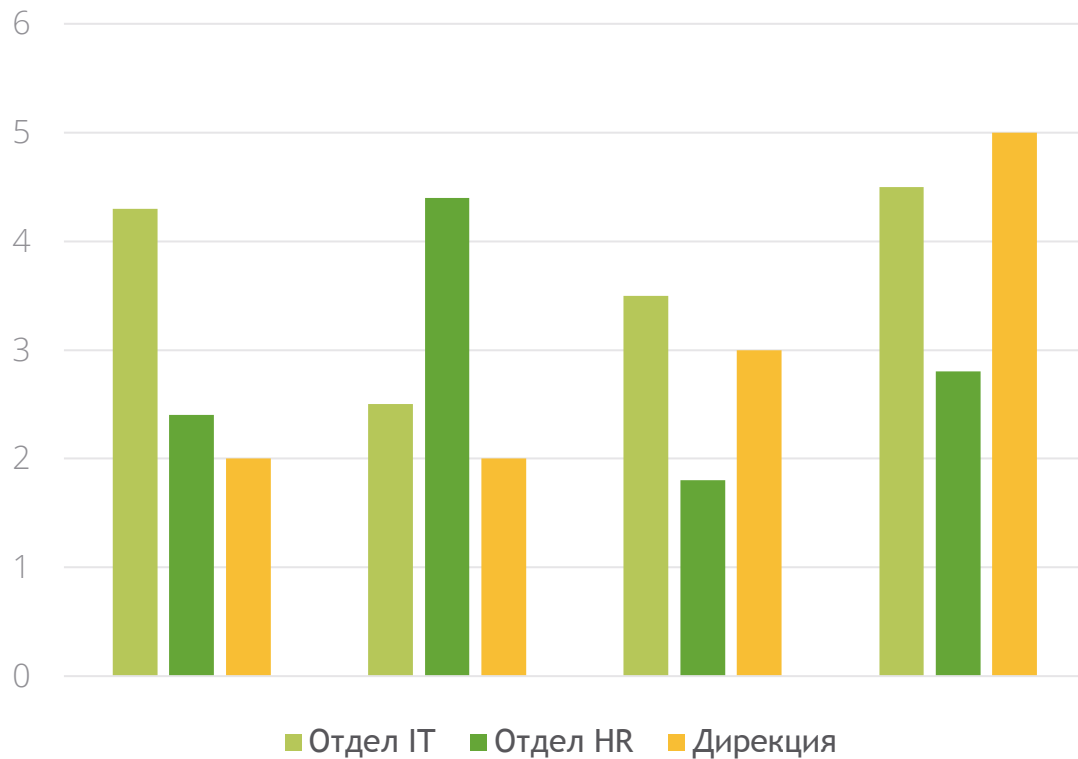
# Актив - объект инвентаризации

## Составные компоненты актива



# Inventory

Использование атрибутов Inventory для фильтрации поиска, анализа и построения статистических отчетов в различных срезах



# SDK для создания приложений на Smart Monitor

Возможности для разработчиков по созданию прикладной логики приложений





Smart Monitor<sup>TM</sup>

Search @nywhere



Пора запросить  
демо-версию,  
как нам кажется 😊