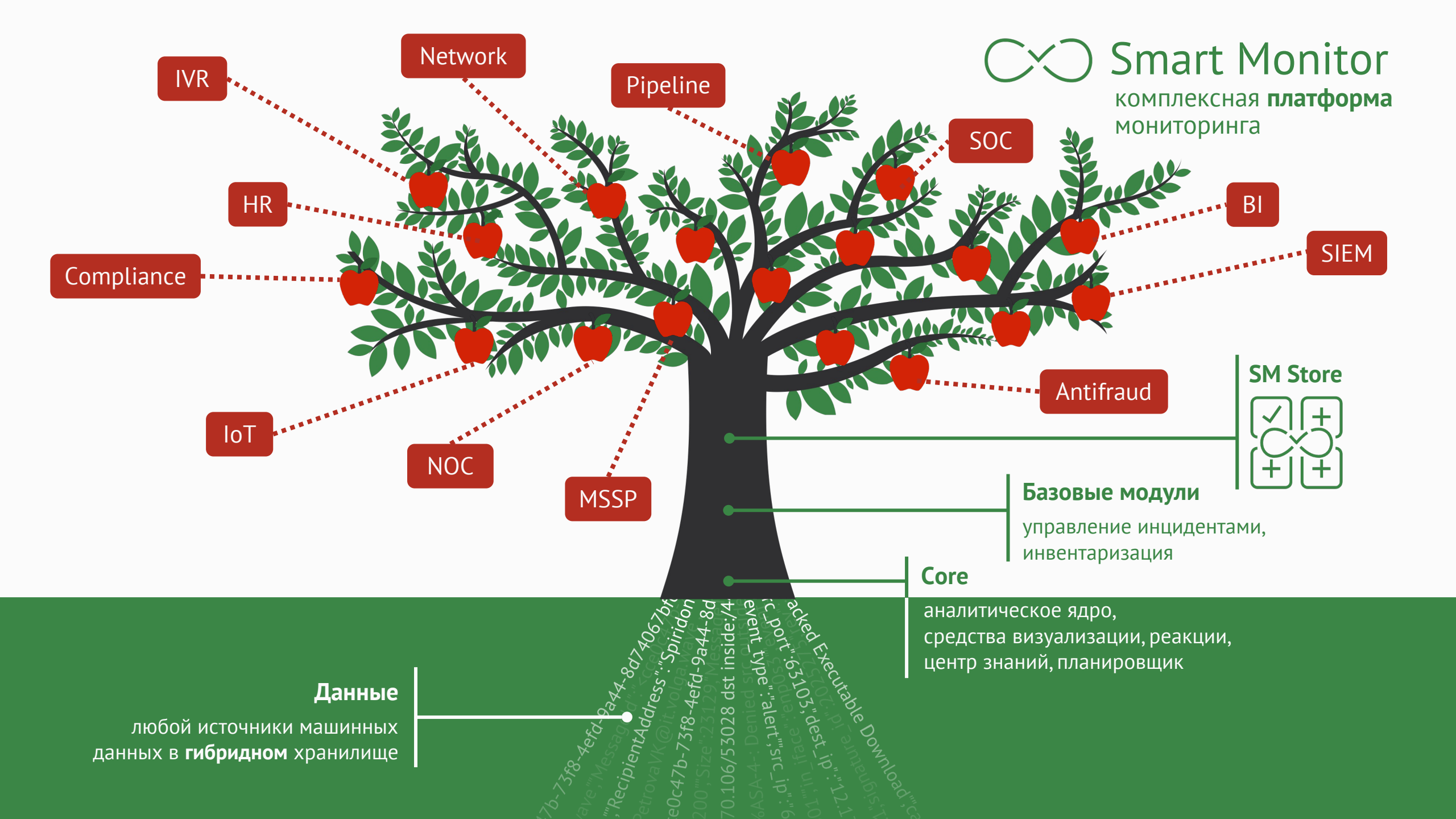
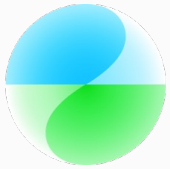
Smart Monitor

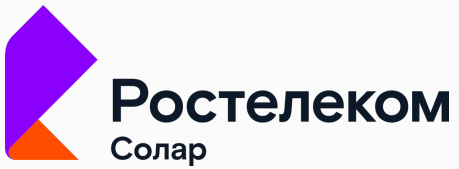
Обзор платформы


Smart Monitor
комплексная **платформа** мониторинга
IVR
Network
Pipeline
SOC
HR
BI
Compliance
SIEM
Antifraud
IoT
NOC
MSSP
SM Store
Базовые модули
управление инцидентами, инвентаризация
Core
аналитическое ядро, средства визуализации, реакции, центр знаний, планировщик
Данные
любой источники машинных данных в **гибридном** хранилище

Наши клиенты



ЕАБР



ДИТ

ПЕРСПЕКТИВНЫЙ
МОНИТОРИНГ

VolgaBlob

Smart Monitor

Меньше кликов до ответа
SM делает поиск доступнее

05 **>500% скорость**
в переходе от данных к ответам

04 **В 3х раза ниже TCO**
за счет Search Anywhere

03 **Более чем 700%**
оптимизация времени на поиск

02 **Корпоративные знания**
трансформация данных в знания и совместное использование

01 **10х вовлечение**
ИТ, ИБ и бизнес-пользователей в поиск, анализ, гипотезы по данным

Позиционирование Smart Monitor

	SM	MP SIEM	KUMA	RUSIEM
Ключевые функции				
Универсальный поиск по различным хранилищам данных	●	○	○	○
Применение в других областях (IT, бизнес-аналитика, compliance)	●	○	○	○
Корреляция на основе исторических данных	●	◔	◔	◔
Возможность интеграции с источниками	●	◕	◑	◕
Поисковый движок	●	◑	◕	◔
Модификация поискового движка	●	○	○	○
Кастомизируемая база знаний	●	◔	○	○
База корреляционных правил	◕	●	◕	◕
Ценообразование				
Сравнение стоимости	◕	◔	◔	●

Два уровня Smart Monitor

Платформа, как инструмент решения практических задач

01

Platform [Core]

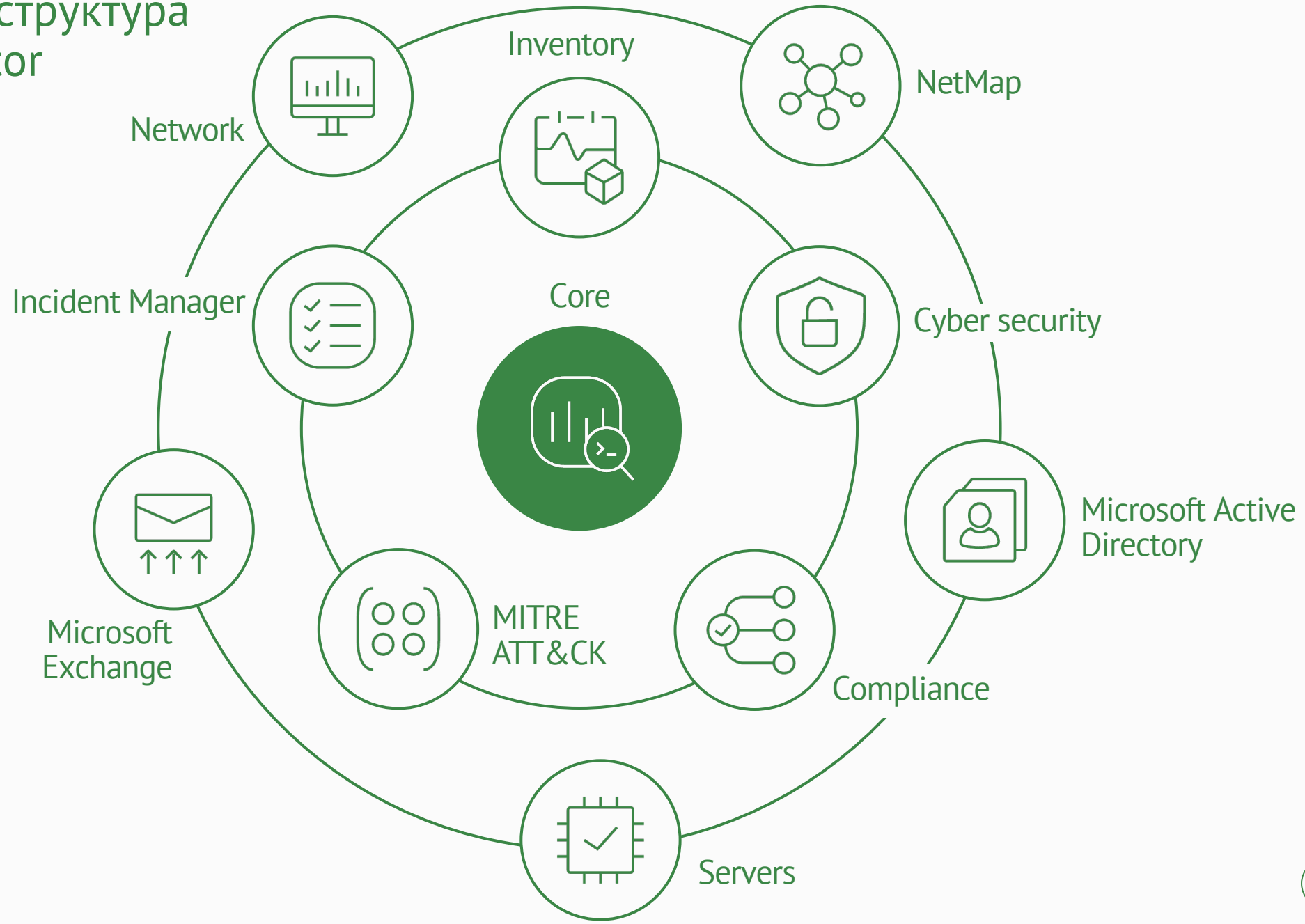
Универсальная платформа полного жизненного цикла управления машинными данными: сбор → хранение → анализ → визуализация → реакция.

02

Use Case [набор модулей]

Кейсы, решающие конкретные практические задачи клиентов: анализ операционной эффективности сотрудников, мониторинг ИТ-инфраструктуры, SIEM, анализ бизнес-процесса, мониторинг среды контейнеризации и пр.

Модульная структура Smart Monitor



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

SM 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**

VolgaBlob

Модули Smart Monitor

Набор модулей для реализации практических задач

Модуль Core

Аналитическое ядро Smart Monitor

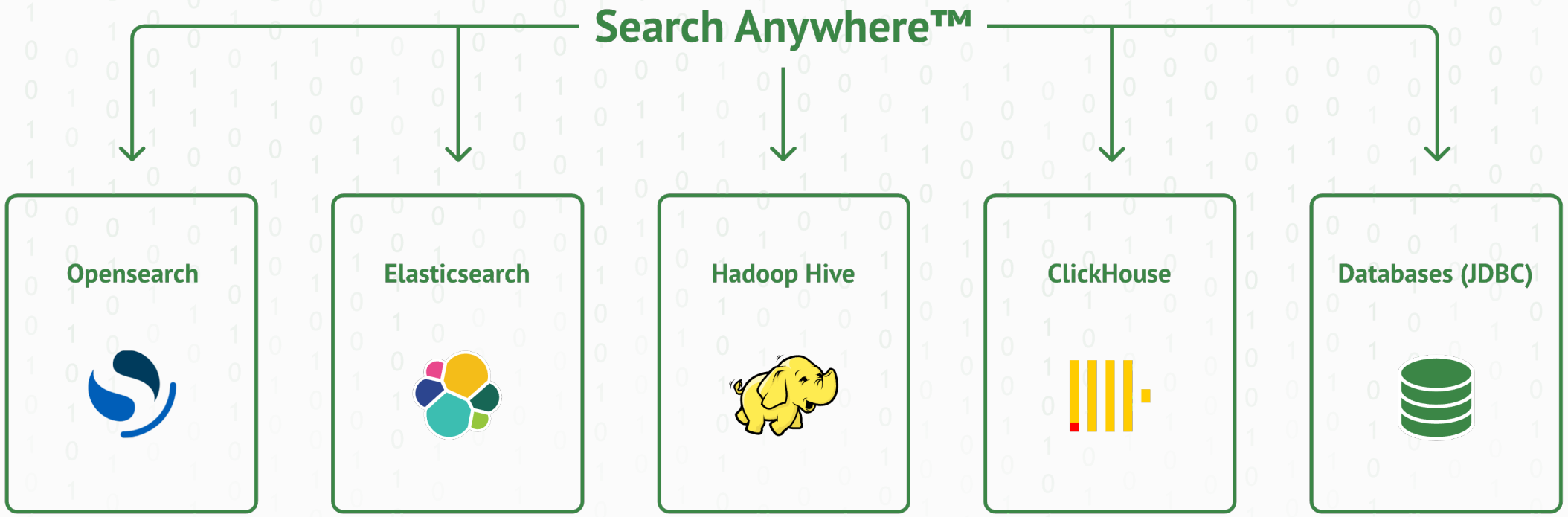
Core: Smart Monitor Engine

- 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

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

Поиск...

Создать

Назавние соединения	Строка соединения	Действия
click	jdbc:clickhouse://172.17.0.181:8123	Разрешения Удалить
mysql	jdbc:mysql://localhost/test	Разрешения Удалить
clickhouse_prod	jdbc:clickhouse://172.17.0.181:8123	Разрешения Удалить
mysql	mysql://160.150:156	Разрешения Удалить

Строк на странице: 50

1

JDBC-запросы

Поиск...

Создать

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

Строк на странице: 50

1

VolgaBlob

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:postgre:pg_query
```

my_had_query, pg_query

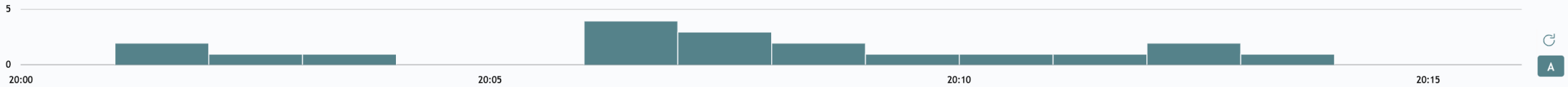
Сохраненные SQL запросы

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

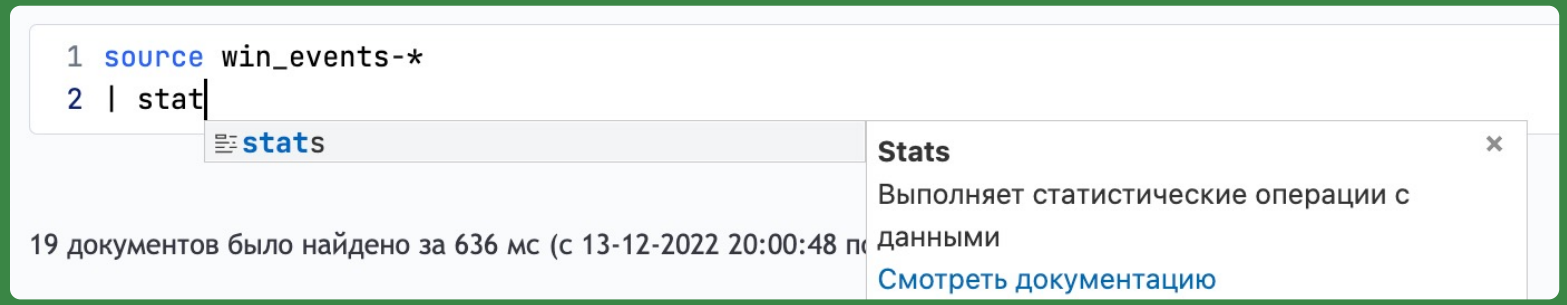
Введите поле

t	@timestamp	19
t	@version	1
t	agent.ephemeral_id	2
t	agent.hostname	5
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

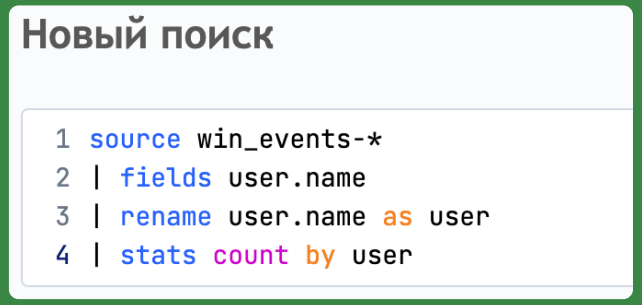
Дата и время	События
13-12-2022 20:13:01.267	@timestamp: 2022-12-13T17:13:01.267Z agent.ephemeral_id: 12938567-60c3-4d3a-a227-eae69cab4da3 agent.hostname: SM-S-WIN-MAIL01 agent.id: 03156ce0-1514-4397-9dbb-e310454f583a agent.type: winlogbeat agent.version: 7.3.2 ecs.version: 1.0.1 event.action: Управление 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: 0x1504acdcf3 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-BOGDANOV 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: 0x1504acdcf3 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

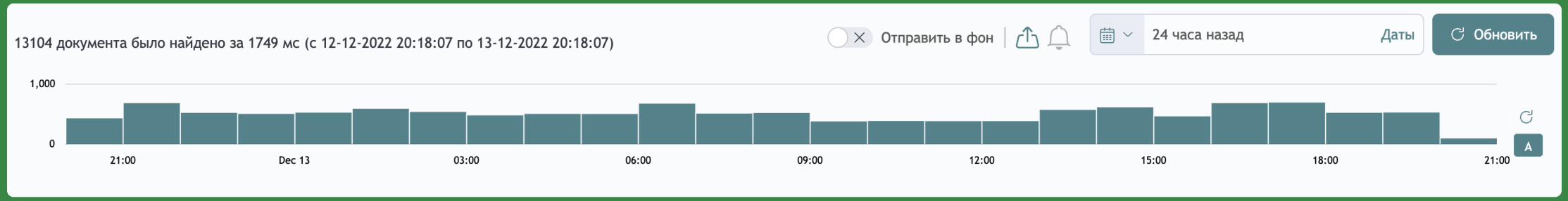
Подсказки команд и описание к ним



Подсветка синтаксиса



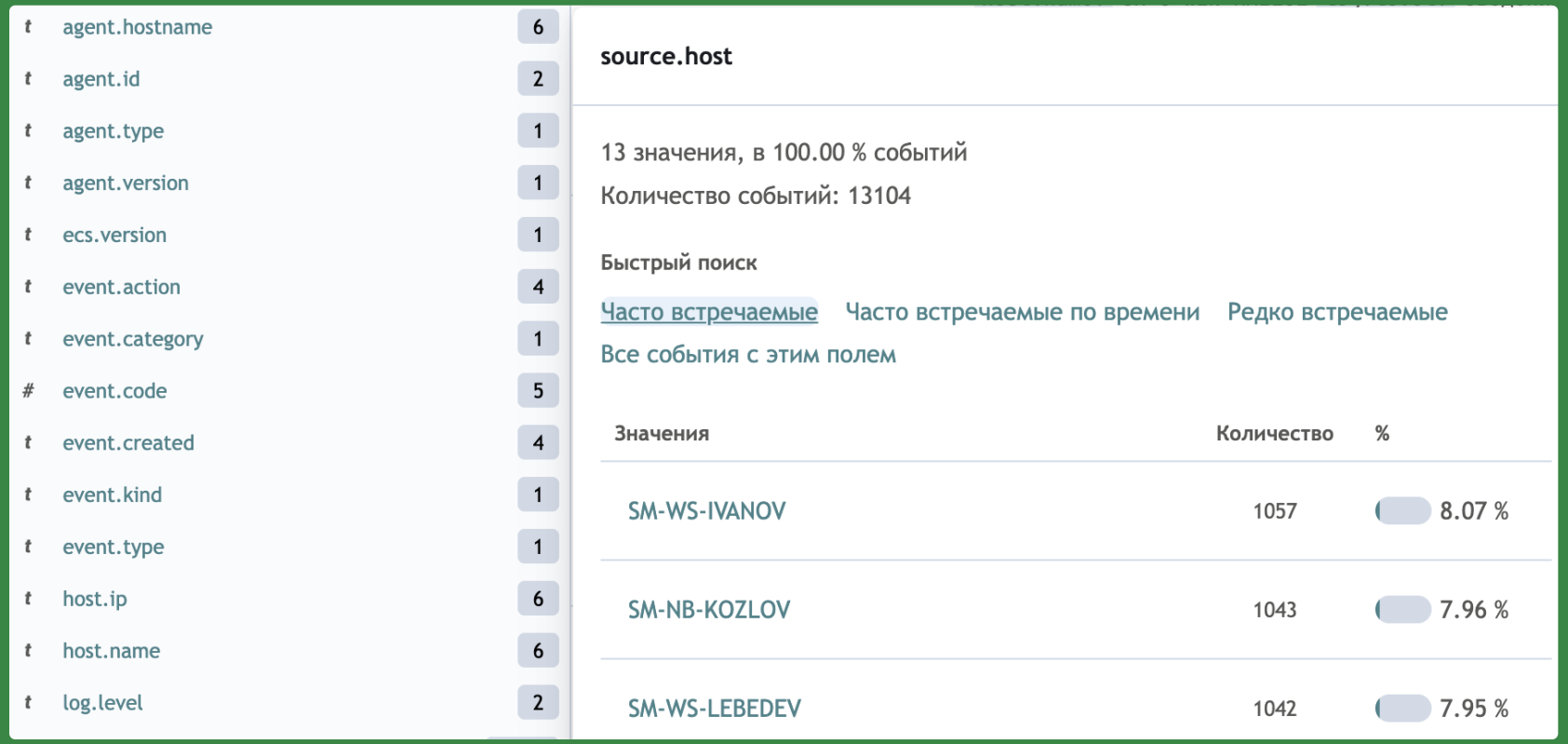
Timeline



VolgaBlob

Smart Monitor Language

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

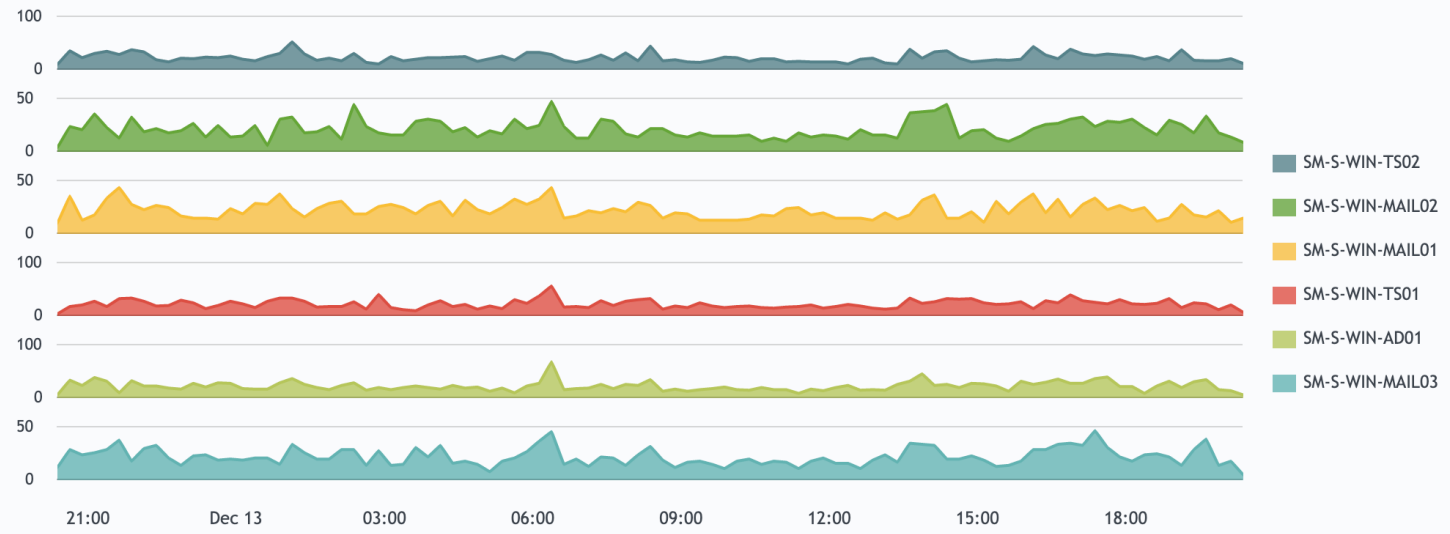
Документы | Статистика (97) | Визуализация | История поиска

Line | Добавить на дашборд

Применить настройки

Главная | Ось X | Ось Y | Легенда | Цветовая схема

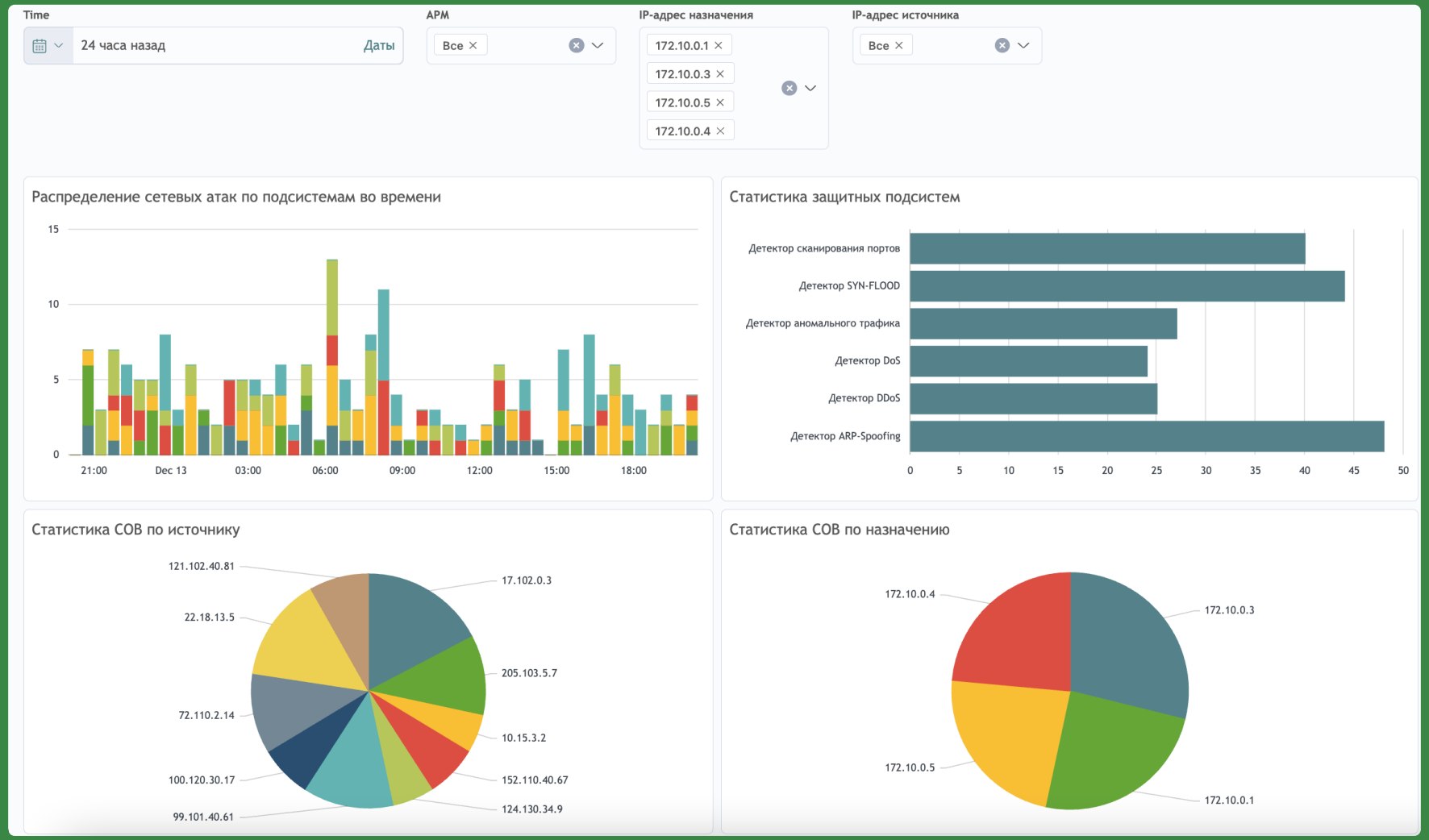
- Шкала предпросмотра
- Группировка
- Закраска площади
- Разбить по сериям



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



SDK для создания визуализаций на Smart Monitor

Возможности для разработчиков по внедрению своих вариантов визуализации

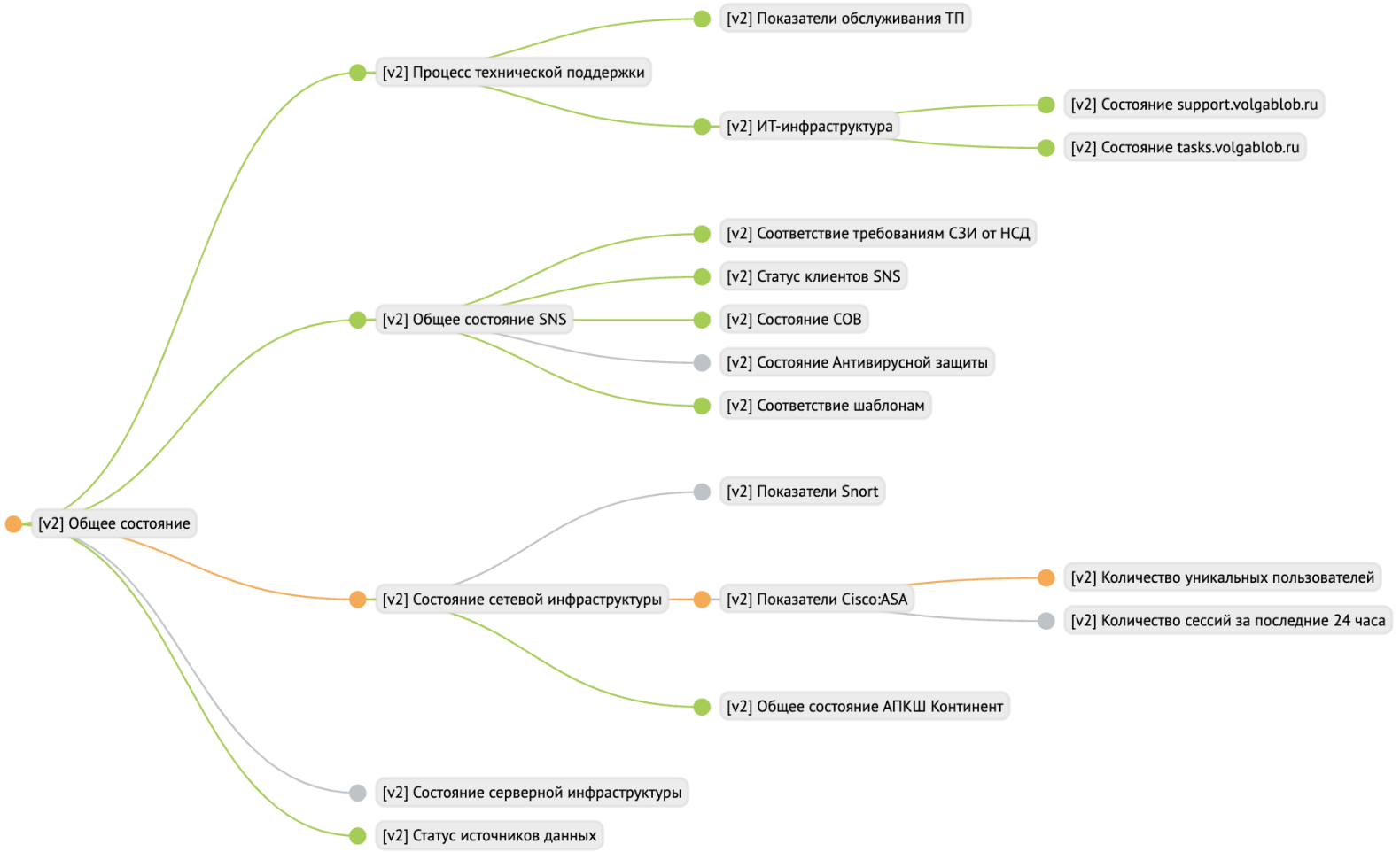
Визуализация
Пользовательская визуализация, отправляющая запрос на регистрацию своих React-компонентов

SDK
Набор методов и компонентов для интеграции в Smart Monitor

Core
Приложение Smart Monitor

VolgaBlob

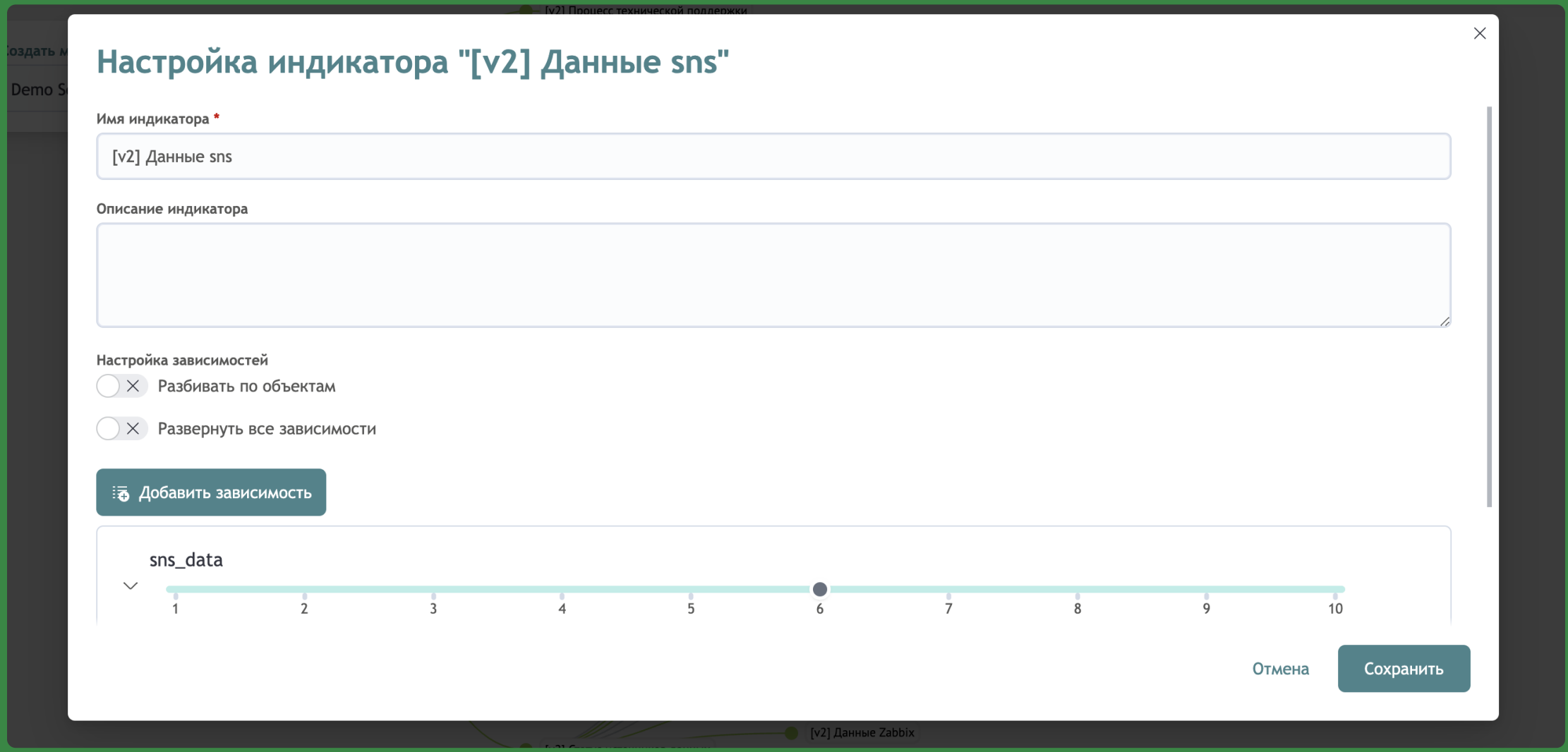
Ресурсно-сервисная модель



VolgaBlob

Ресурсно-сервисная модель

Ресурсно-сервисная модель

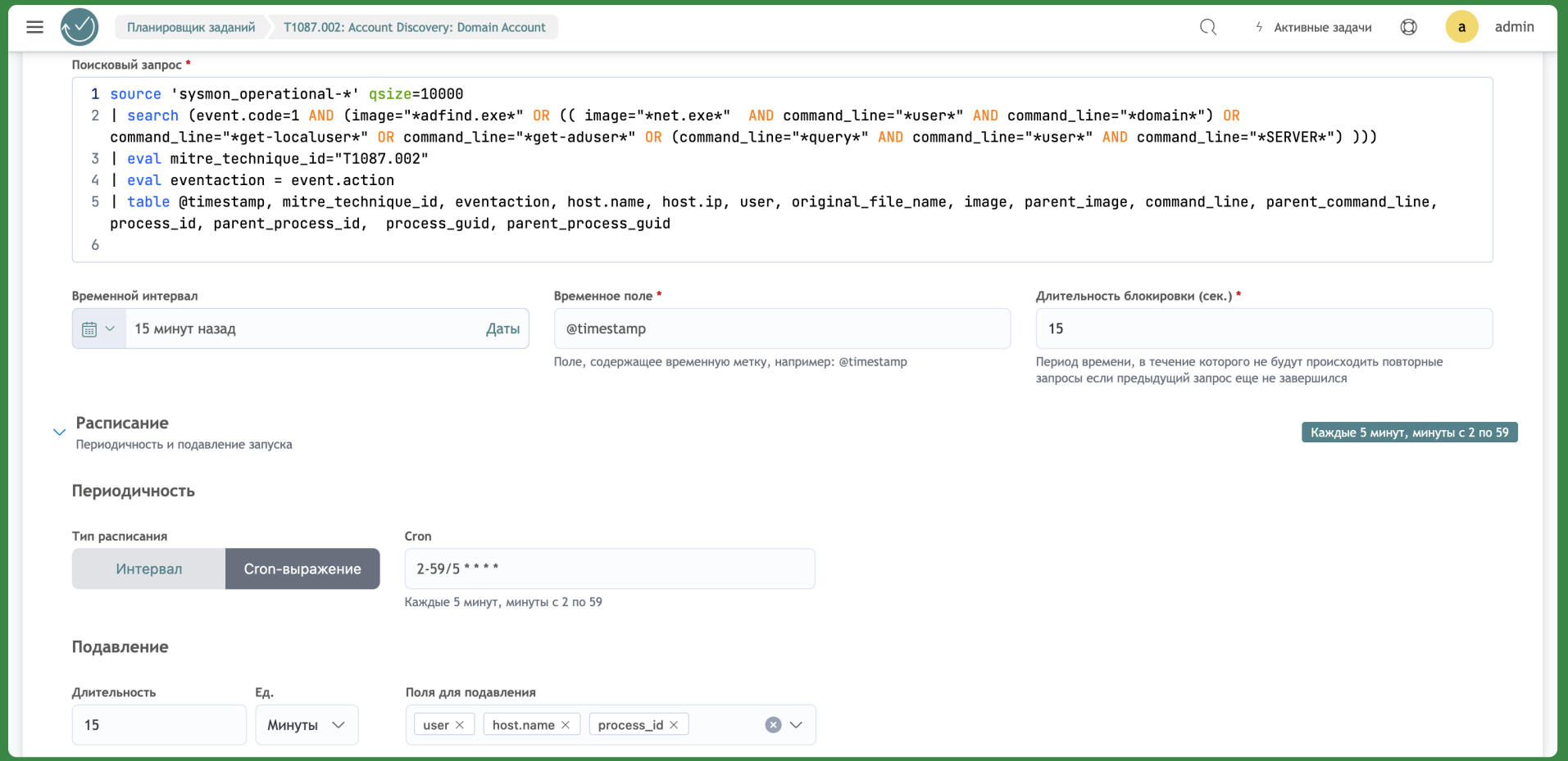


Job Scheduler

●	T1003.004: OS Credential Dumping: LSA Secrets LSA Secrets.	Incident Action MITRE ATT&CK® Risk Scoring	1-59/15 * * * * Каждые 15 минут, минуты с 1 по 59	2022-09-21 17:07:35
●	T1016: System Network Configuration Discovery System Network Configuration Discovery	Incident Action MITRE ATT&CK® Risk Scoring	1-59/15 * * * * Каждые 15 минут, минуты с 1 по 59	2022-09-21 17:07:38
●	T1049: System Network Connections Discovery Utilities and commands that acquire this information include netstat, "net use," and "net session" with Net. In Mac and	Incident Action MITRE ATT&CK® Risk Scoring	1-59/15 * * * * Каждые 15 минут, минуты с 1 по 59	2022-09-21 17:07:53
●	T1057: Process Discovery Process Discovery detected (running tasklist or Get-Process).	Incident Action MITRE ATT&CK® Risk Scoring	1-59/15 * * * * Каждые 15 минут, минуты с 1 по 59	2022-09-21 17:07:56
●	T1059.003: Command and Scripting Interpreter: Windows Command Shell Windows Command Shell	Incident Action MITRE ATT&CK® Risk Scoring	1-59/15 * * * * Каждые 15 минут, минуты с 1 по 59	2022-09-21 17:08:02
●	T1069.002: Permission Groups Discovery: Domain Groups Domain Groups Discovery	Incident Action MITRE ATT&CK® Risk Scoring	1-59/15 * * * * Каждые 15 минут, минуты с 1 по 59	2022-09-21 17:08:12
●	T1087.002: Account Discovery: Domain Account Domain Account Discovery	Incident Action MITRE ATT&CK® Risk Scoring	1-59/15 * * * * Каждые 15 минут, минуты с 1 по 59	2022-09-21 17:08:14
●	T1489: Service stop - by net or sc commands Service Stop detected	Incident Action MITRE ATT&CK® Risk Scoring	1-59/15 * * * * Каждые 15 минут, минуты с 1 по 59	2022-09-21 17:08:18

Job Scheduler

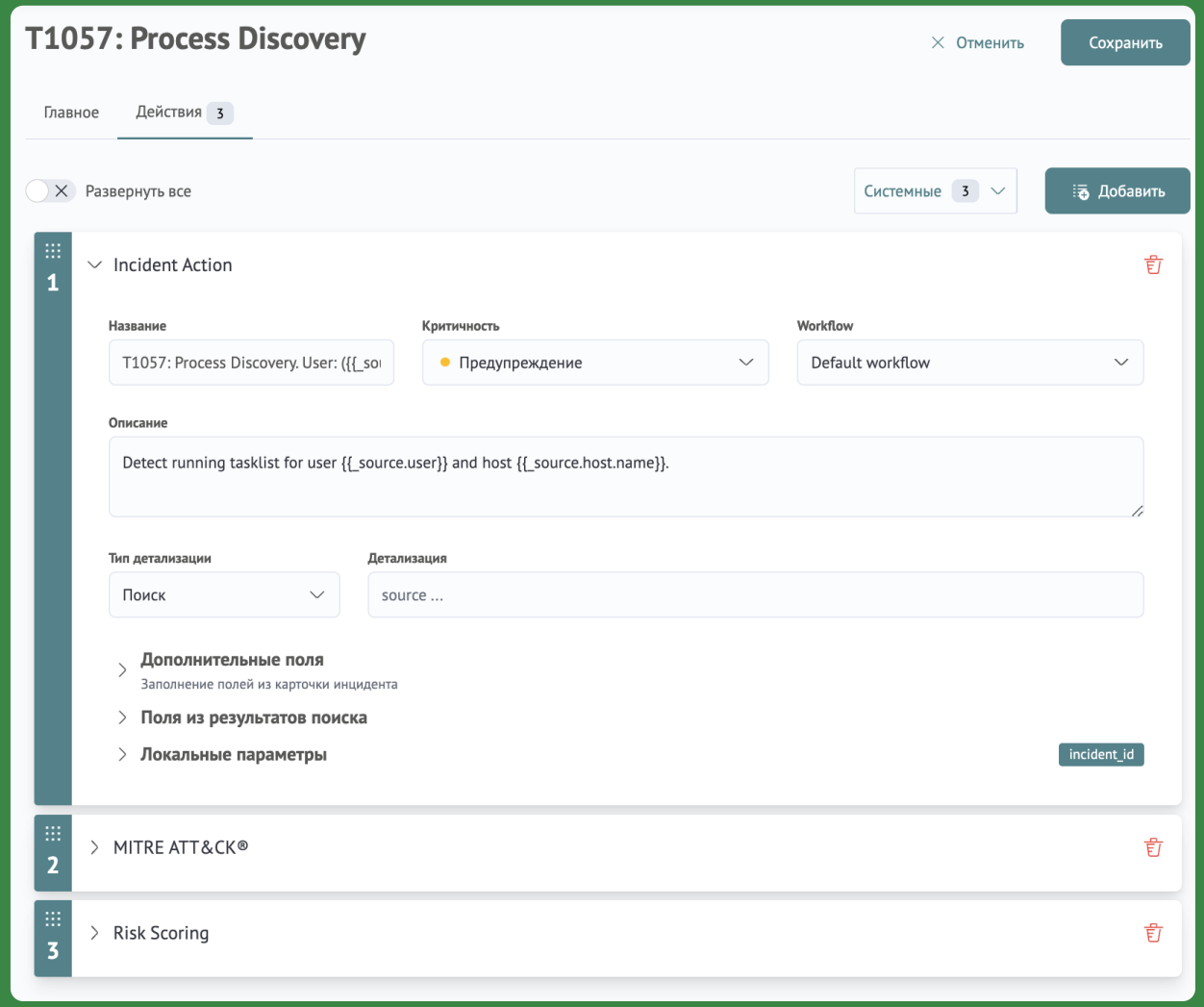
Выполнение запросов по заданному расписанию



Job Scheduler

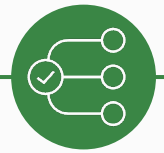
Активные действия по результаты выполнения

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



VolgaBlob

Knowledge Center – теперь в Core!

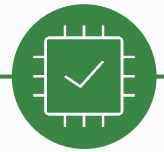


Сценарии

Сценарии использования правил

Правила

Набор корреляционных правил

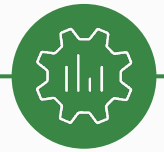


Playbooks

Последовательность действий для закрытия инцидента

Wikilogs

Статьи с детальным описанием

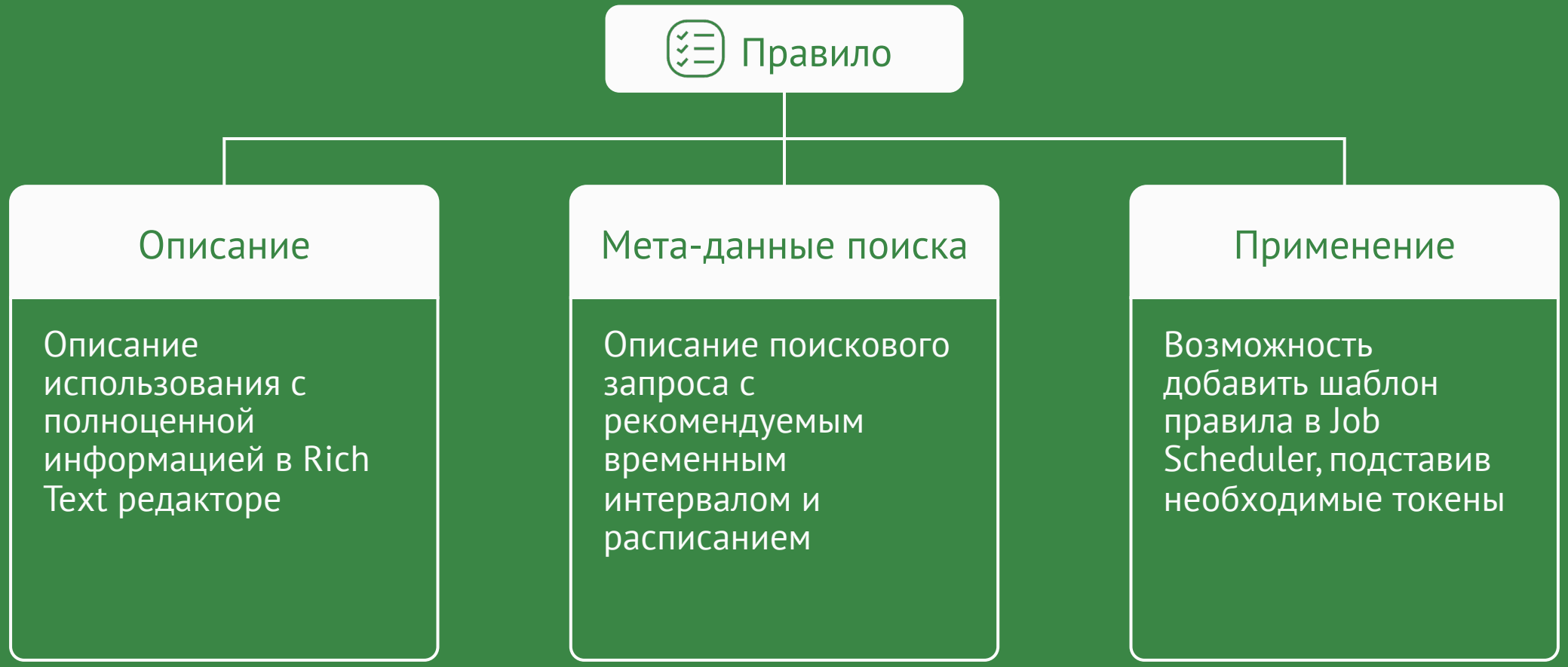


Источники

Эталонные конфигурации для сбора данных

Правила

Корреляционные правила, которые можно использовать для реализации



Правила

Корреляционные правила, которые можно использовать для реализации

Список правил

Поиск...

Критичность | Тег | 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

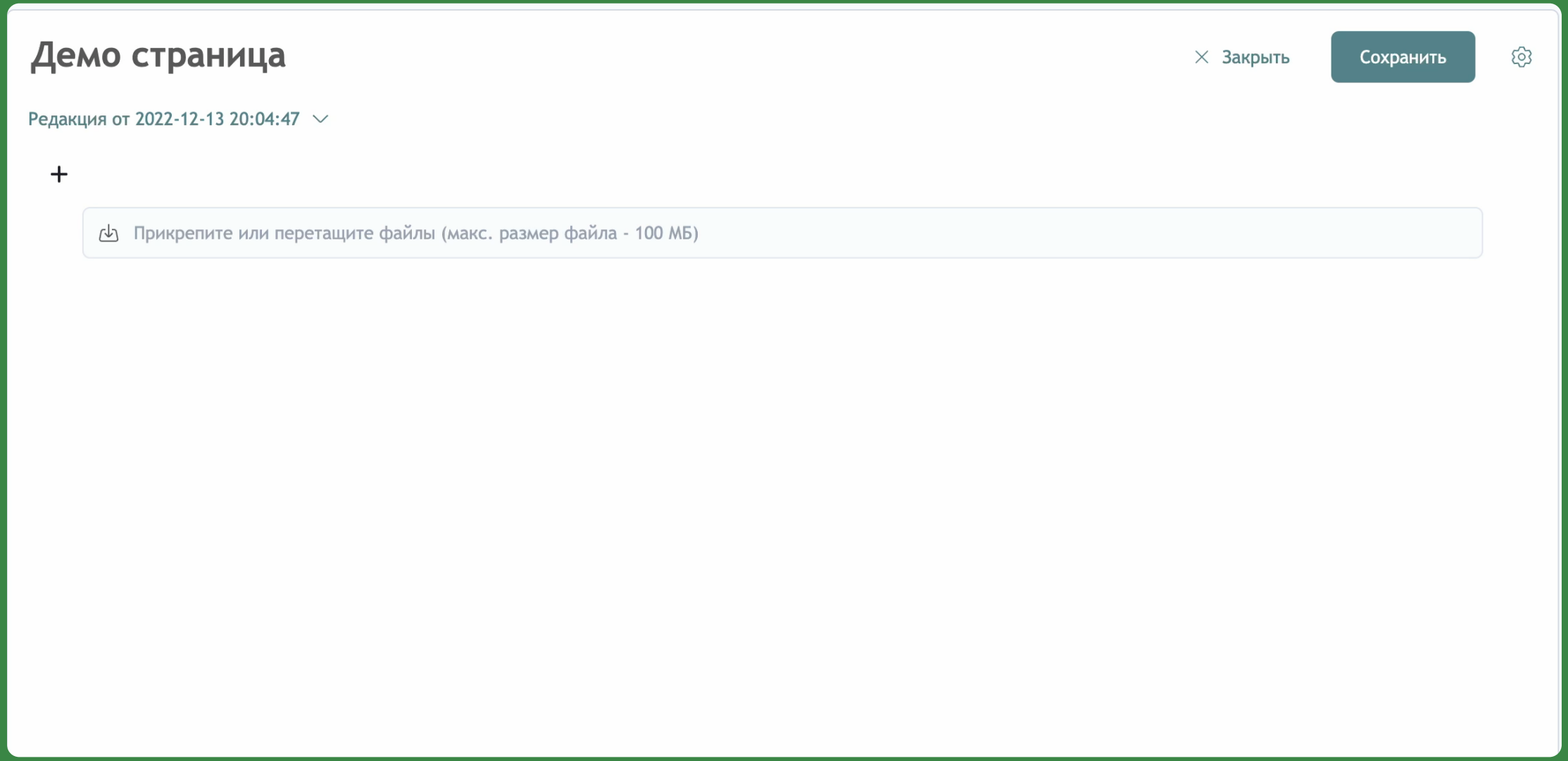
`now+15m` `now`

```
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

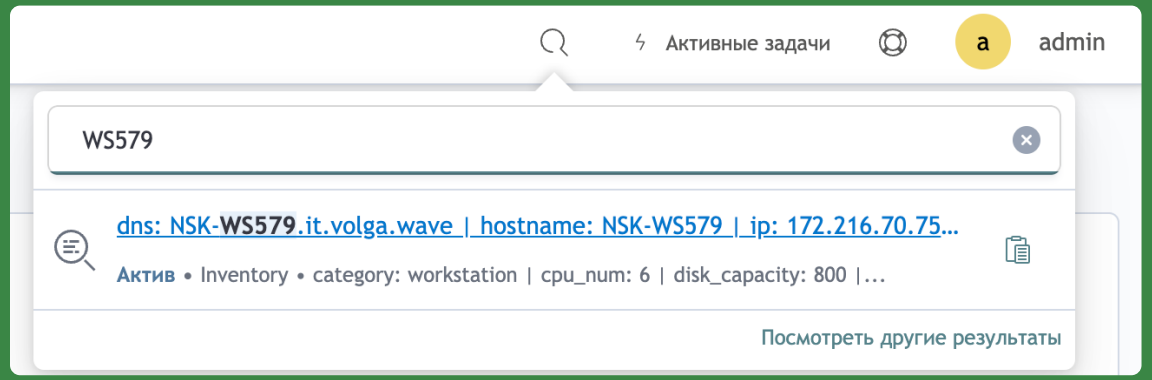
VolgaBlob

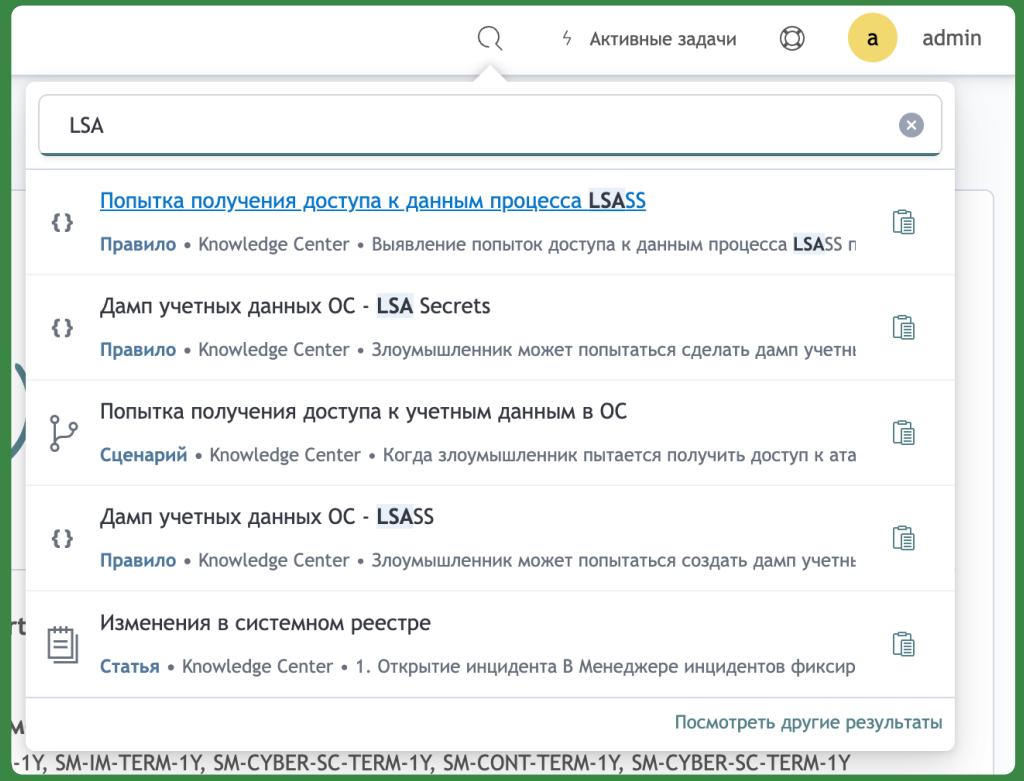
Wikilogs – динамические статьи!



Глобальная строка поиска

Spotlight





Сквозной поиск по объектам
Smart Monitor!

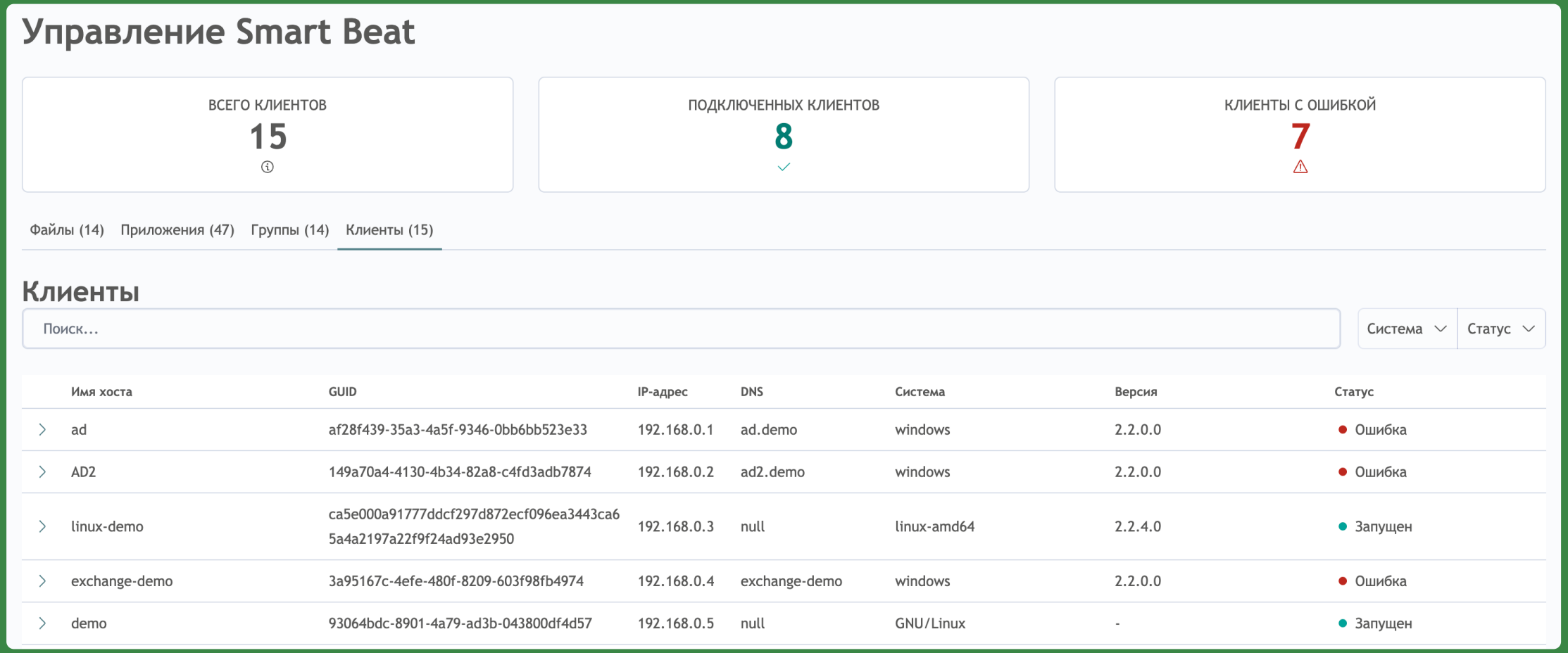
Smart Beat

- Управление агентами Beats
- Поддержка централизованного управления конфигурацией агентов
- Автоматический запуск нескольких Beats без необходимости установки
- Простой процесс управления агентами и их обновление

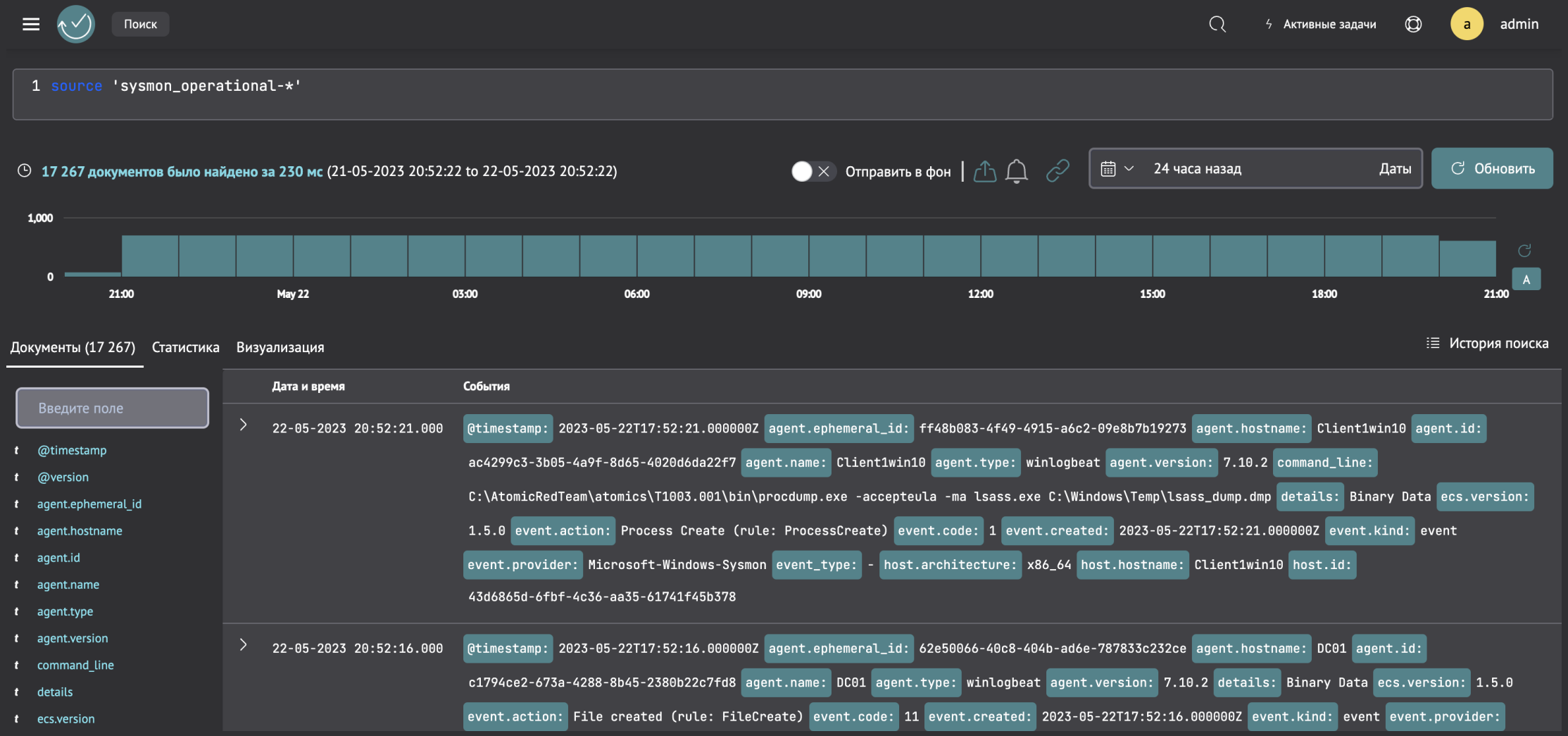
Smart Beat Manager

- 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

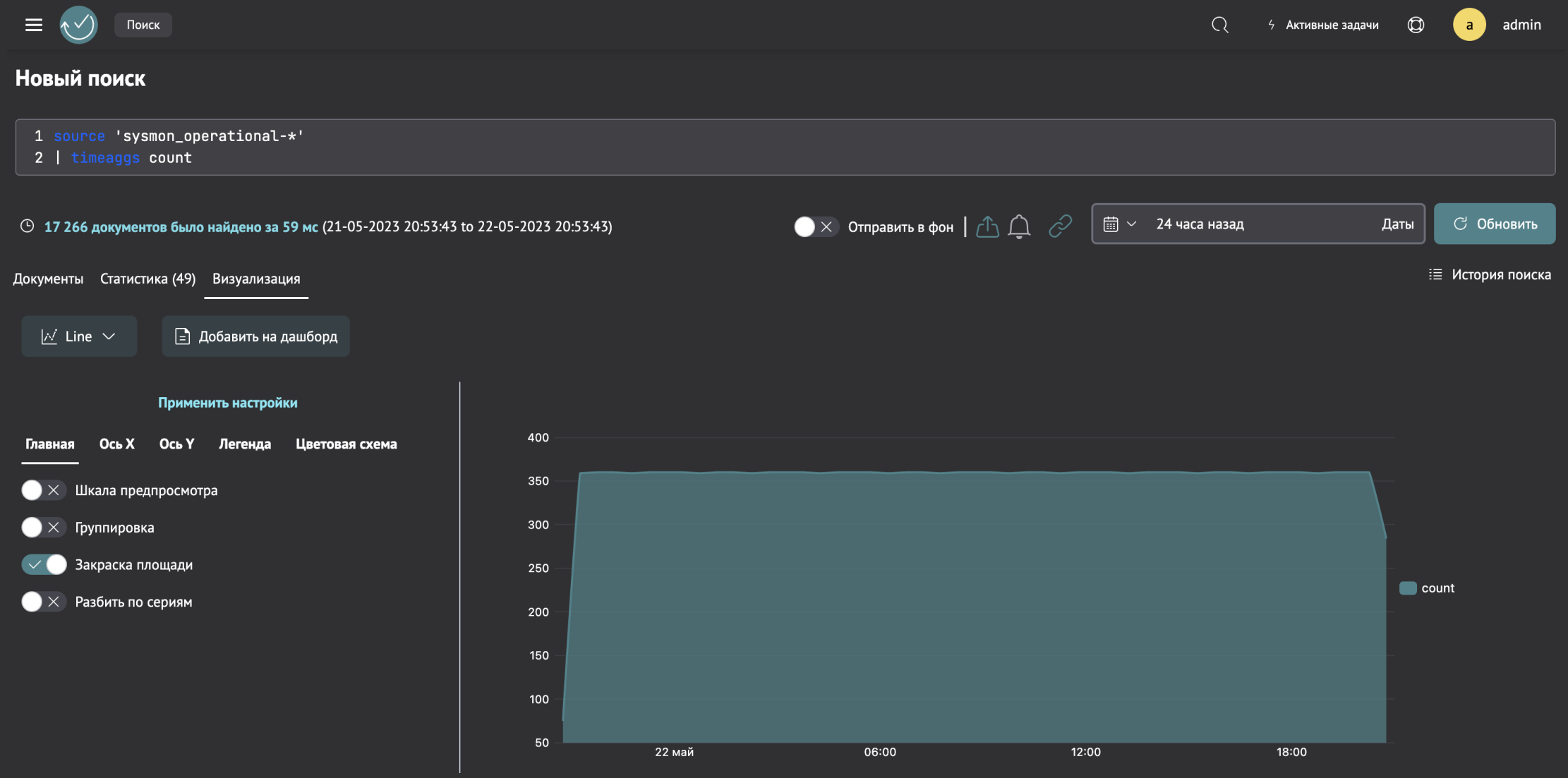


Темная тема



VolgaBlob

Темная тема


Поиск
Активные задачи
admin
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
400
350
300
250
200
150
100
50
22 май
06:00
12:00
18:00
count

Темная тема

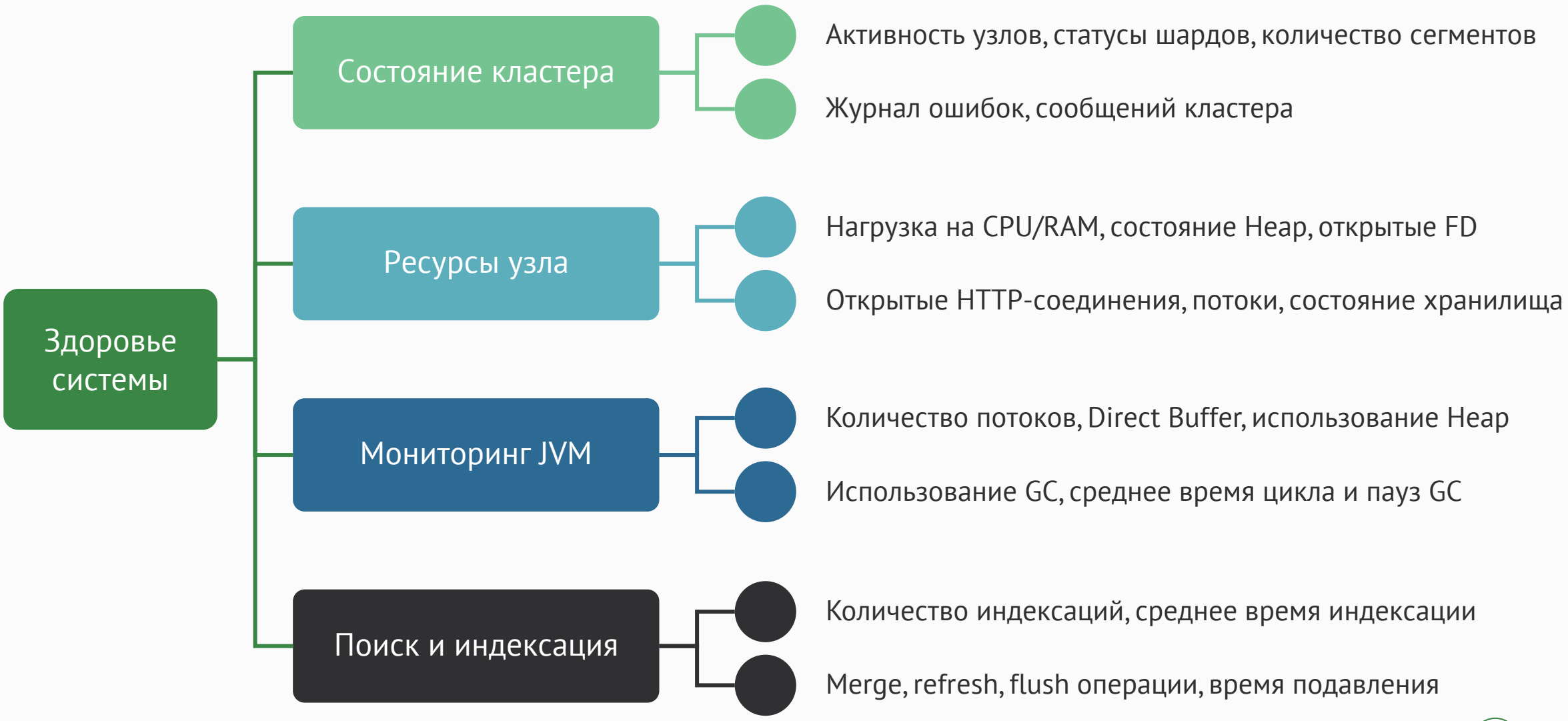

SNS: Тревоги
Экспорт
Редактировать
Time
24 часа назад Даты
APM
Все
Пользователь
Все
Тревога
Все
Распределение тревог по времени
40
35
30
25
20
15
10
5
0
09:00
12:00
15:00
18:00
21:00
29 май
03:00
06:00
09:00
Компьютер заблокирован системой защиты
OTHER
Потеря связи со службой Антивируса
Изменение параметров устройства
Обнаружено новое устройство
Отказ в аутентификации
Запрет подключения устройства
Запрет доступа к файлу или каталогу
СОВ заблокировала удаленный узел (событий: 1)
Антивирусные базы устарели
Обнаружен вирус
Статистика тревог по APM
APM
Количество тревог
ARM4.vbtrend.local 197
ARM1.vbtrend.local 174
ARM3.vbtrend.local 171
ARM2.vbtrend.local 159
ARM6.vbtrend.local 158
ARM8.vbtrend.local 157
Топ тревог
Запрет печати документа
Обнаружен вирус
Отказ в аутентификации
Обнаружено новое устройство
СОВ заблокировала удаленный узел (событий: 1)
0
100
200
300
400

Производительность системы

SBER CLOUD

VolgaBlob

Self Monitoring



Состояние кластера

Состояние кластера

Период: 60 минут назад — Показать даты

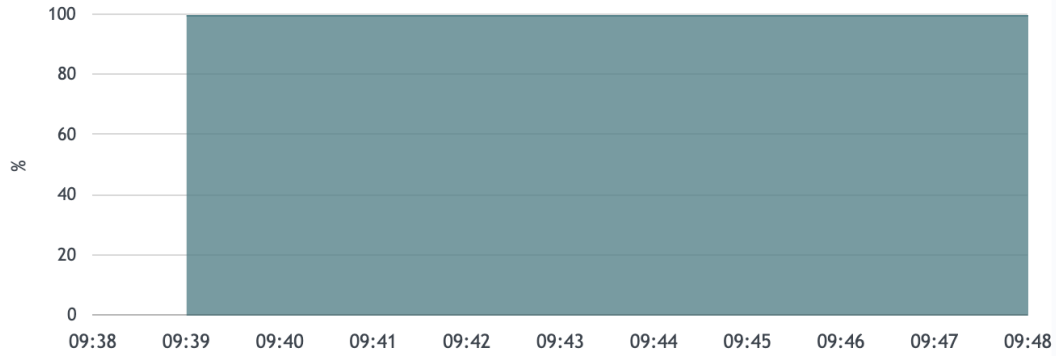
Временной интервал: 1m

Кластер: smos-cluster

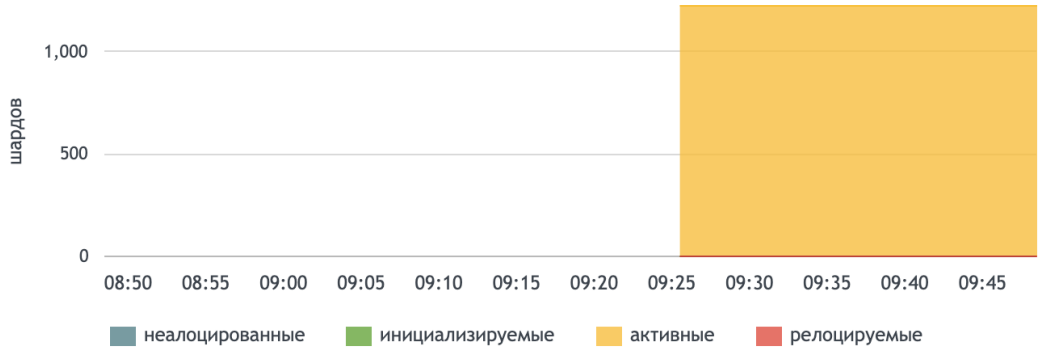
green
Статус кластера

1
Активные ноды

Процент активных шардов



Статусы шардов



ID ноды	Имя ноды	Сегменты	Процессор, %	Память, %	Хранилище, %	HTTP соединений	File descriptors, %	Heap, %	Потоки
y90qMchqT7aNli-vDsxe3A	smos-opensearch	7672	54	99	97	69	17	52	348

Ресурсы узла

41
Загрузка процессора, %

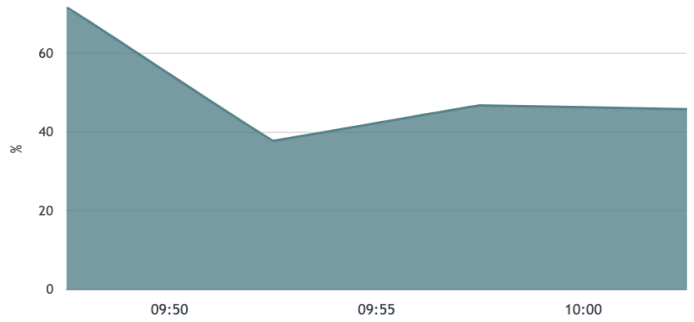
99
Загрузка памяти, %

97.135
Заполненность хранилищ, %

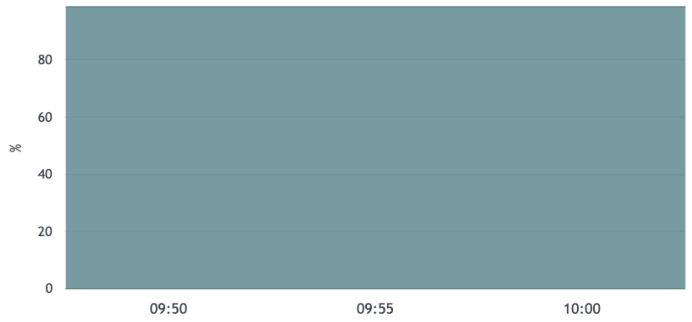
11,050
Открытых file descriptor

68
Открытых HTTP соединений

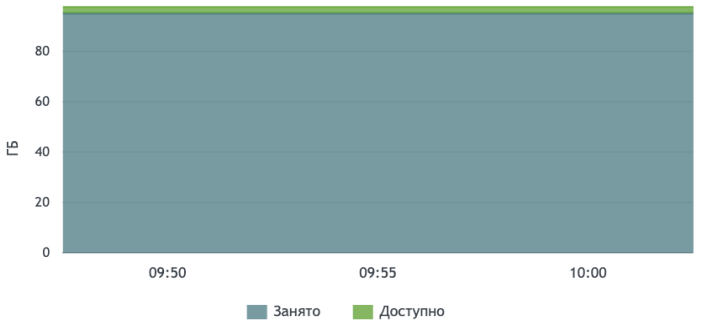
Загрузка процессора



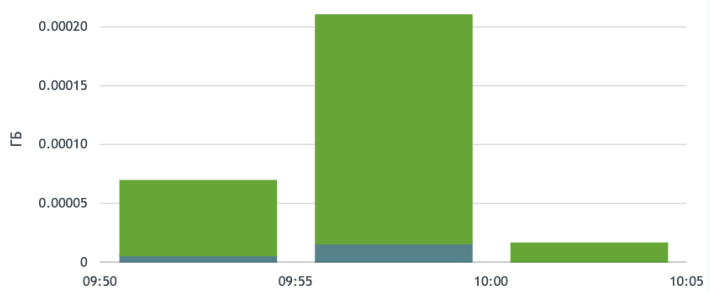
Загрузка памяти



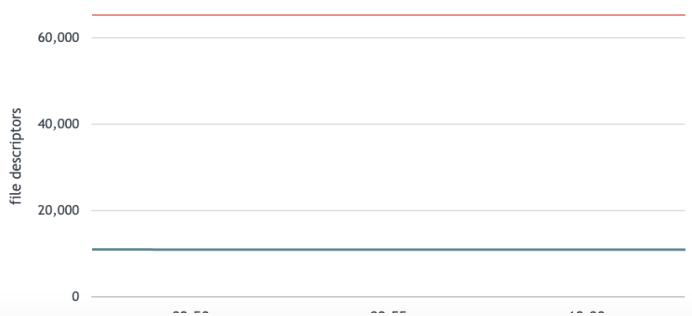
Состояние хранилища



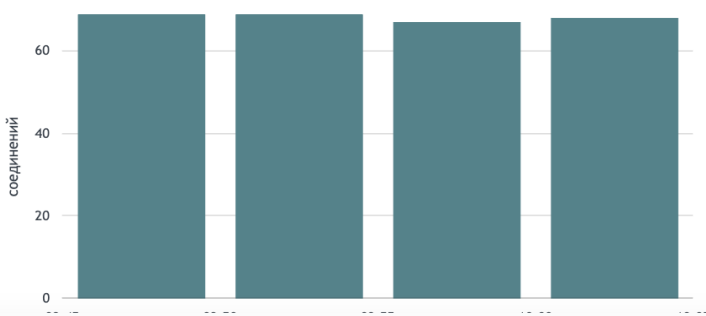
Объем чтения/записи



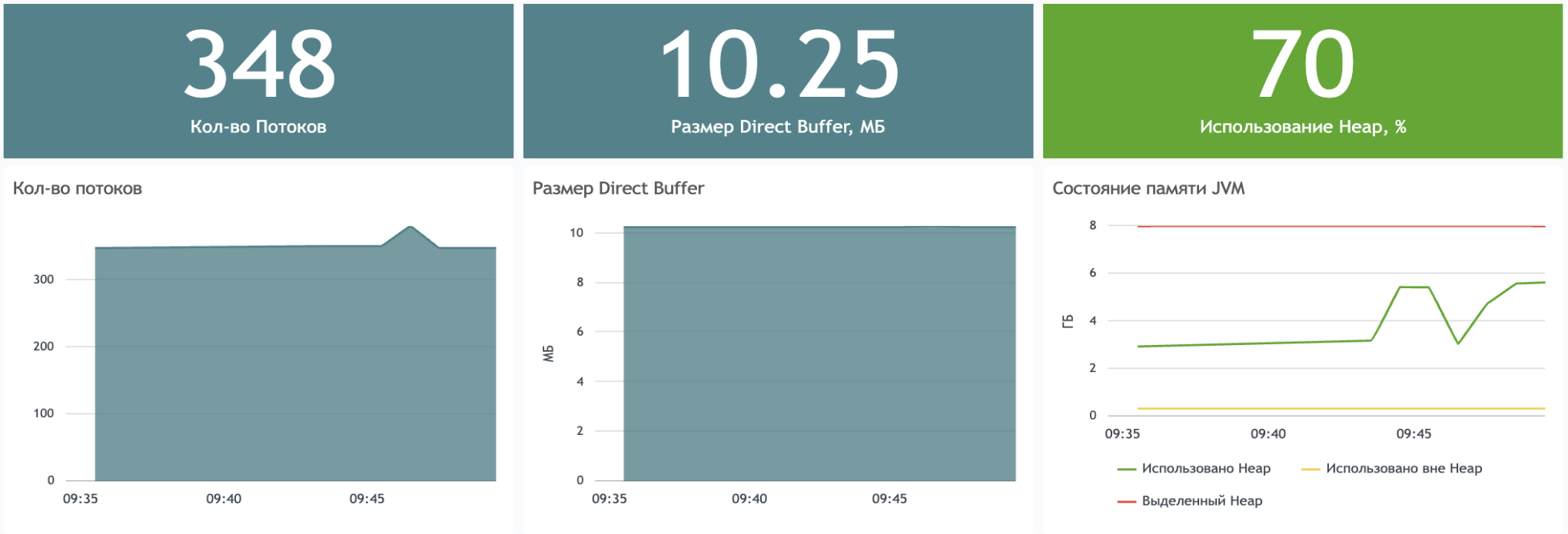
Открытые file descriptor



Открытые HTTP соединения



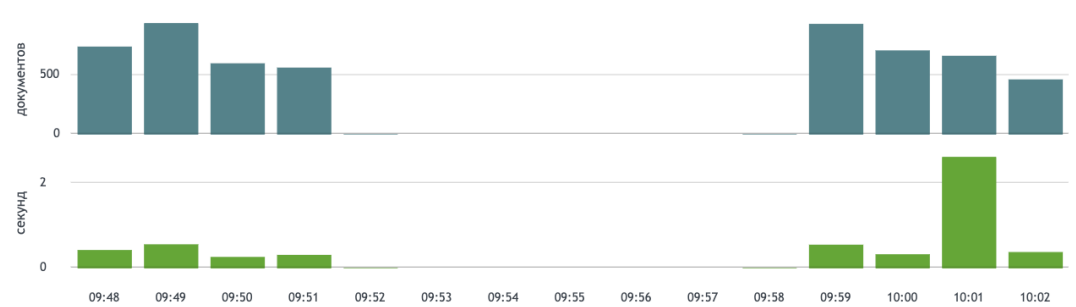
Мониторинг JVM



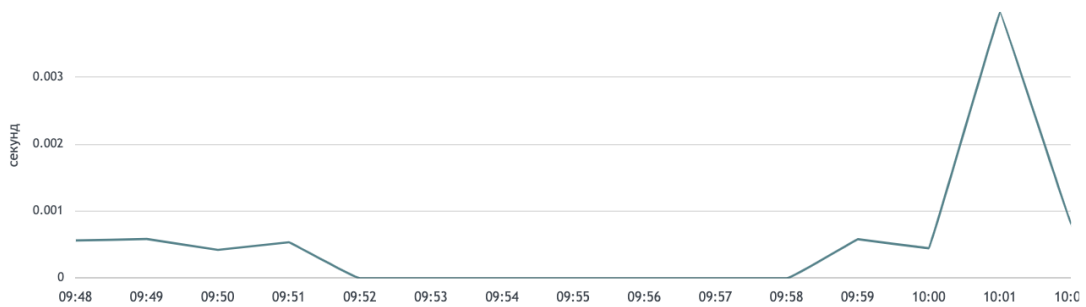
Поиск и индексация

0	0	0	0
Неудавшиеся индексации	Индексация в подавлении, секунд	Активных merge	Merge использует памяти, МБ

Количество индексаций

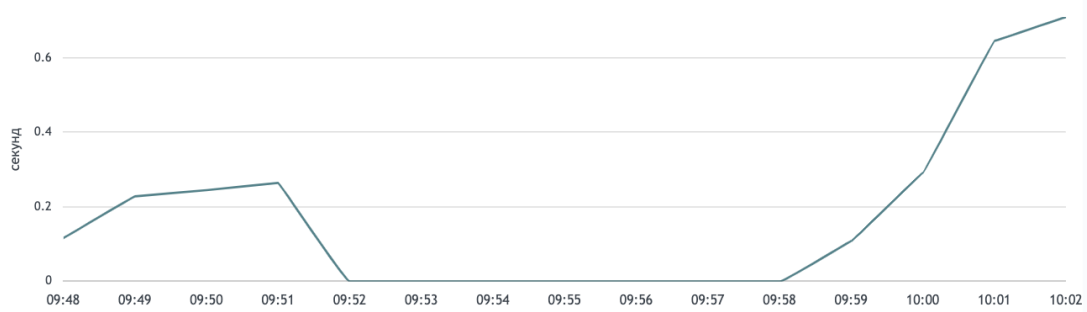


Среднее время индексации документа



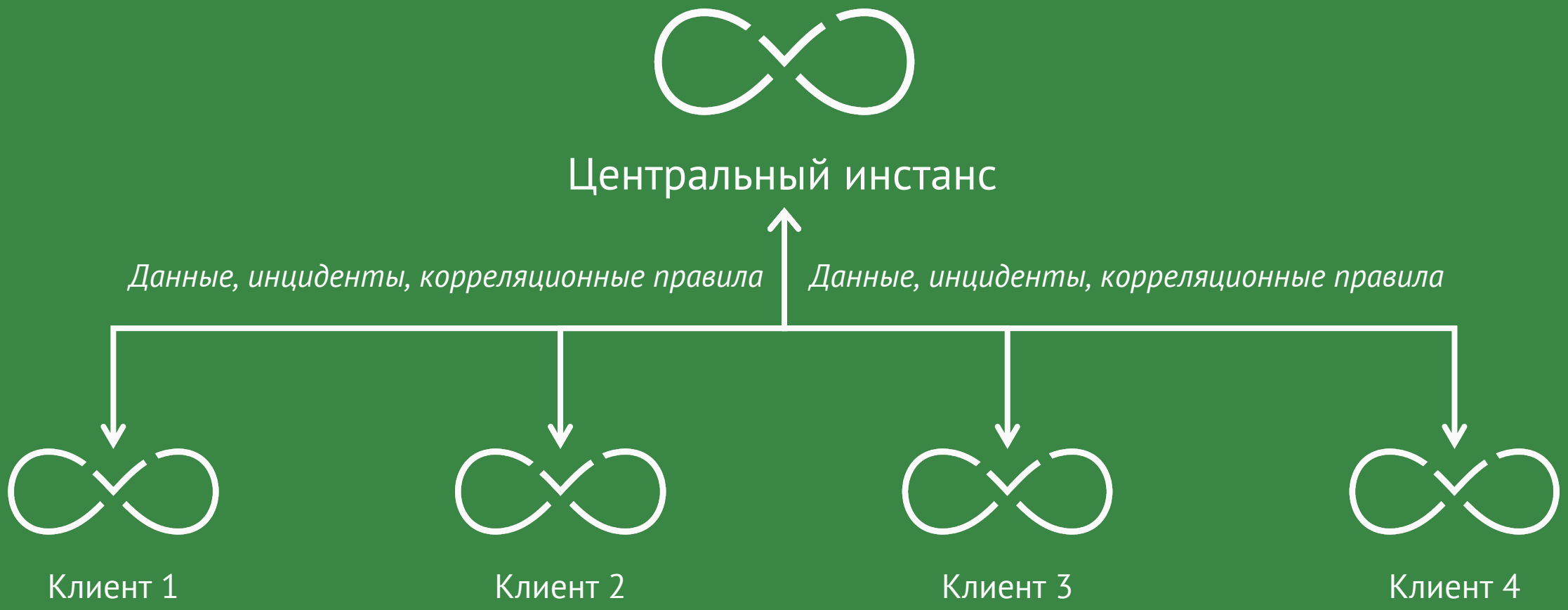
Merge операции

Среднее время merge операций

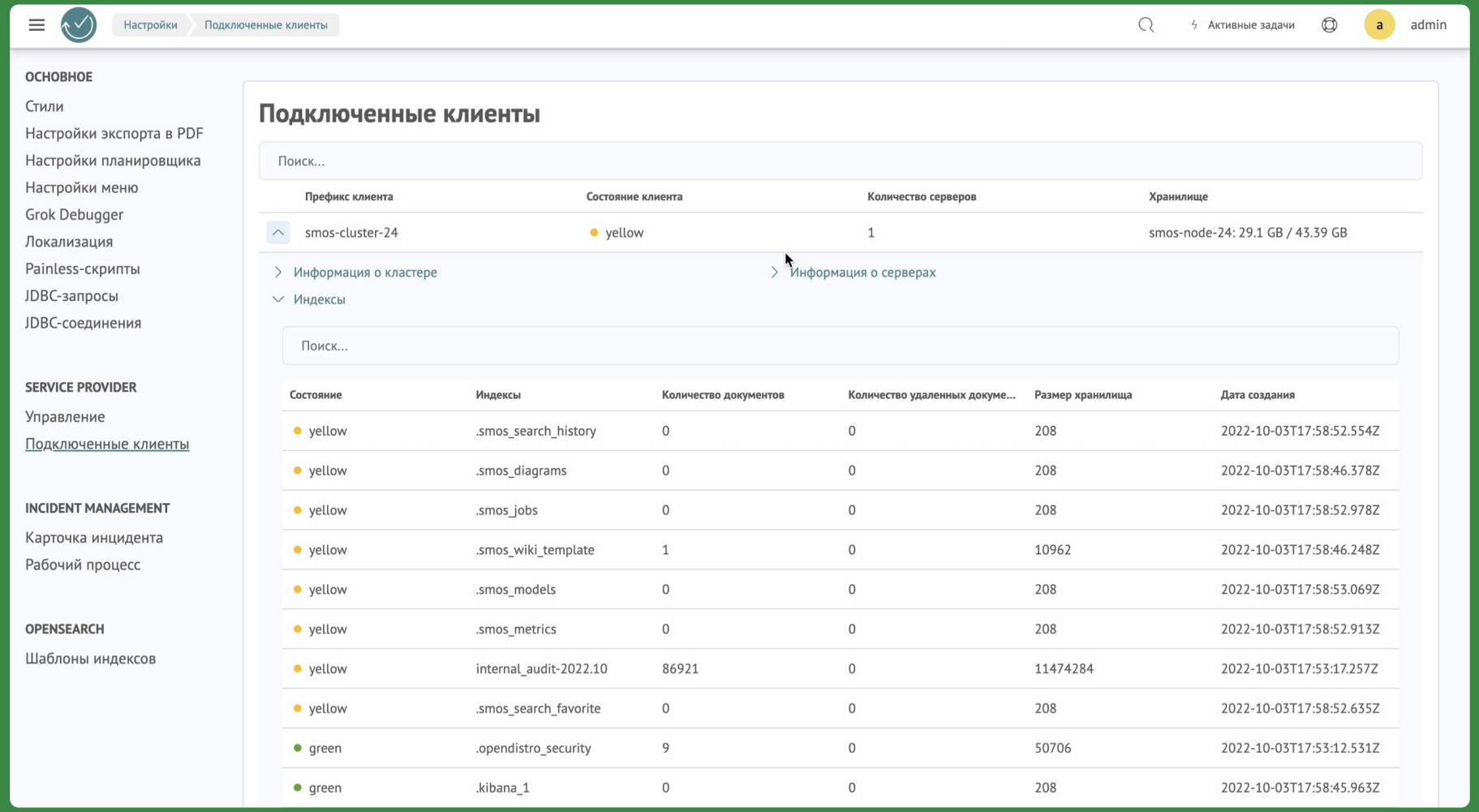


VolgaBlob

Режим Service Provider

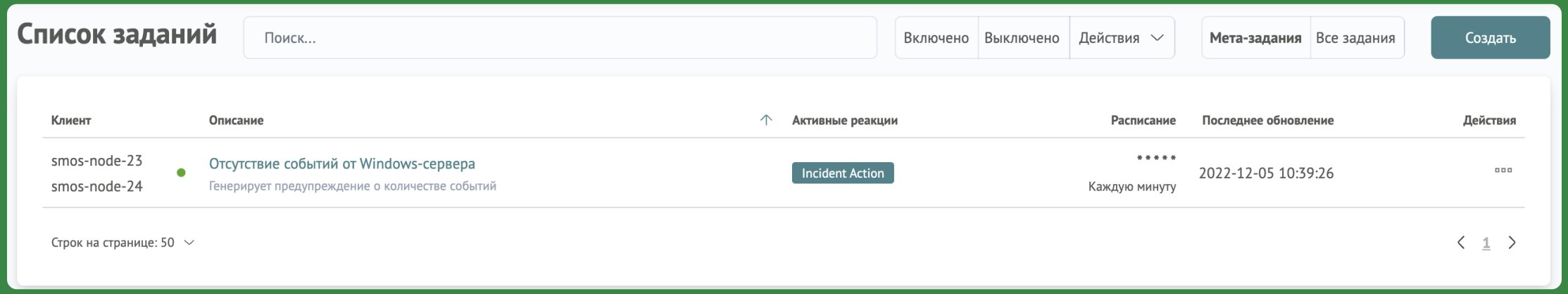


Режим Service Provider

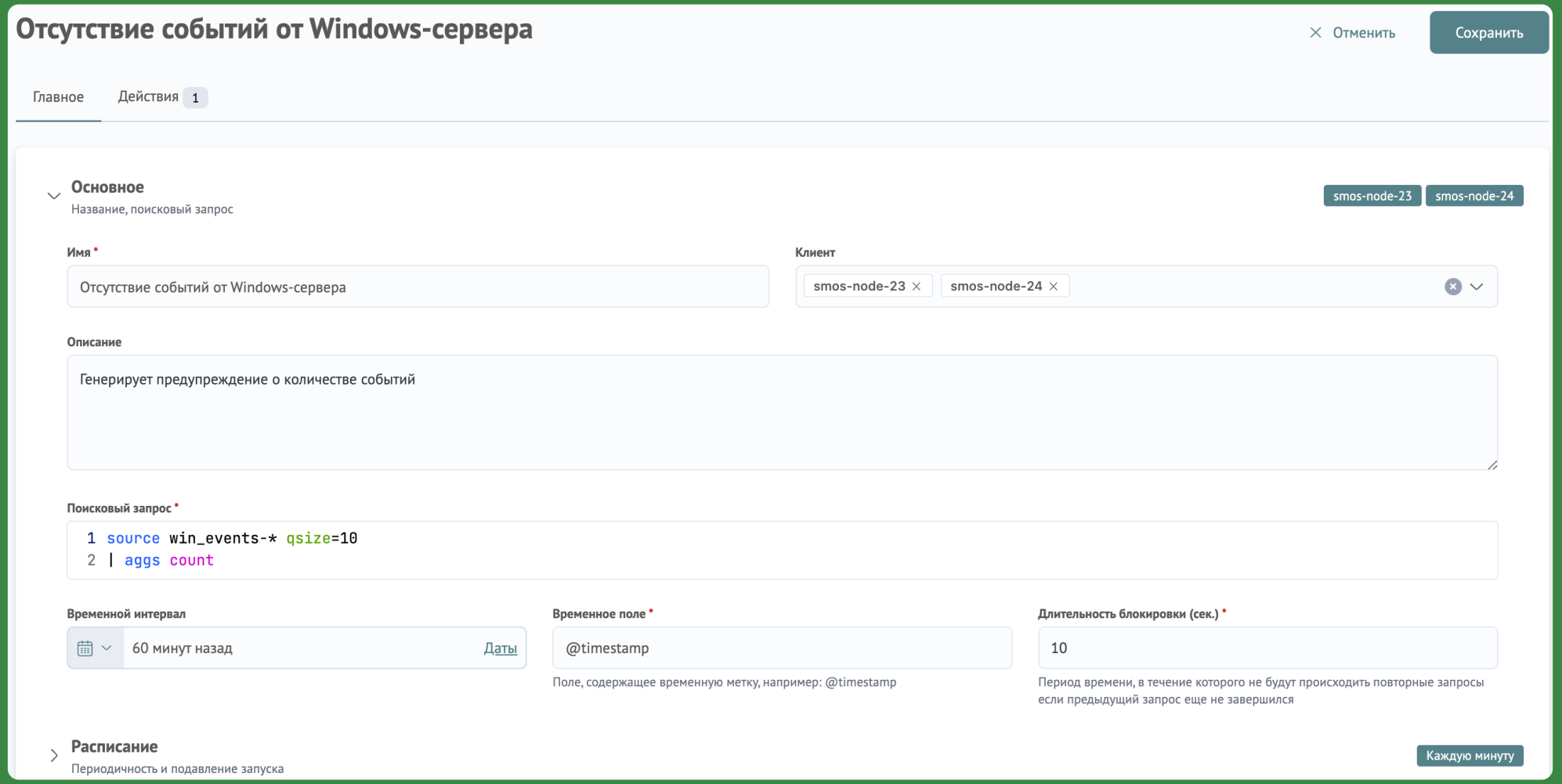


VolgaBlob

Режим Service Provider



Режим Service Provider



Модуль 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

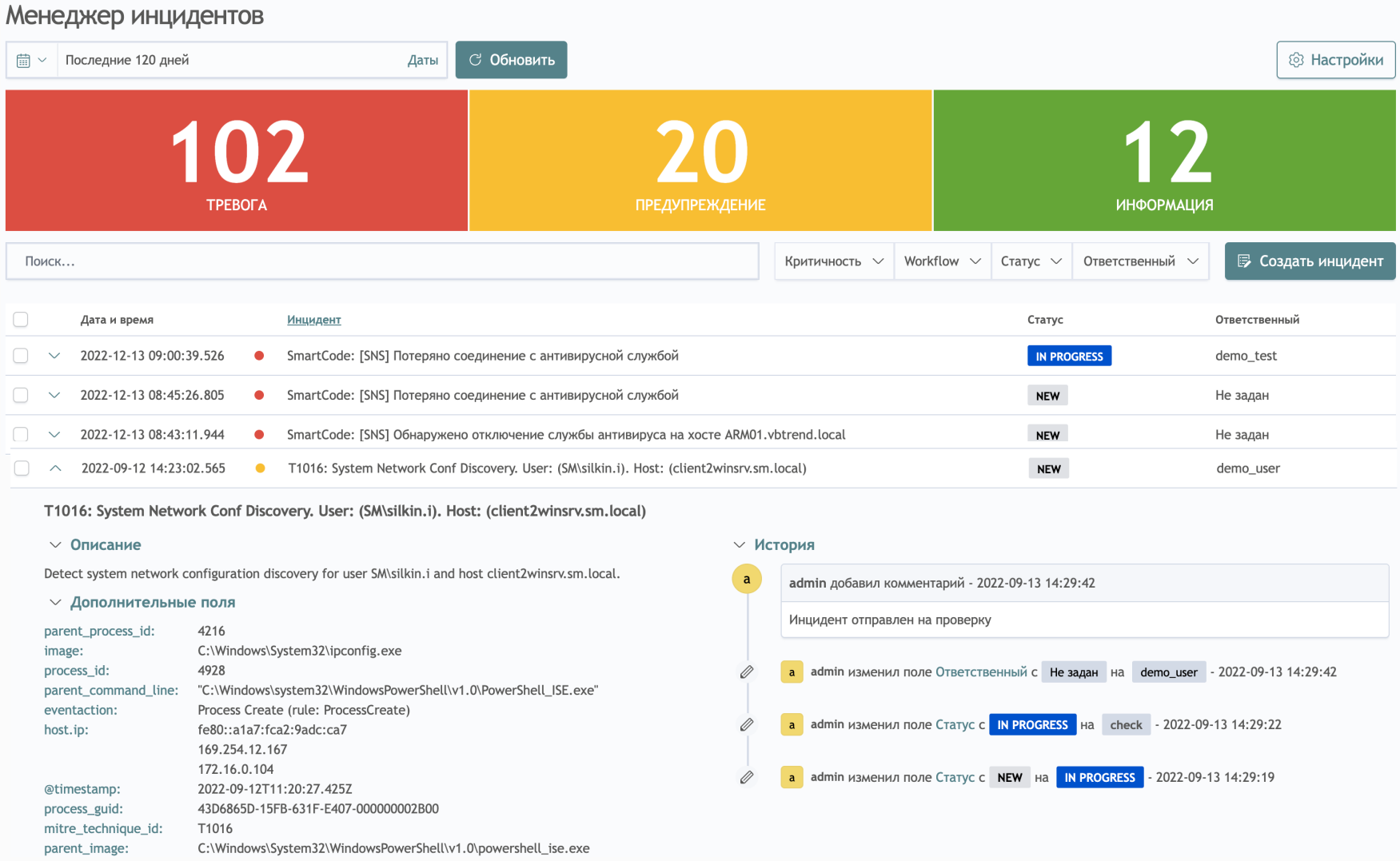
+ Workflow

Создание инцидентов вручную

История изменений и комментарии

Уровни критичности

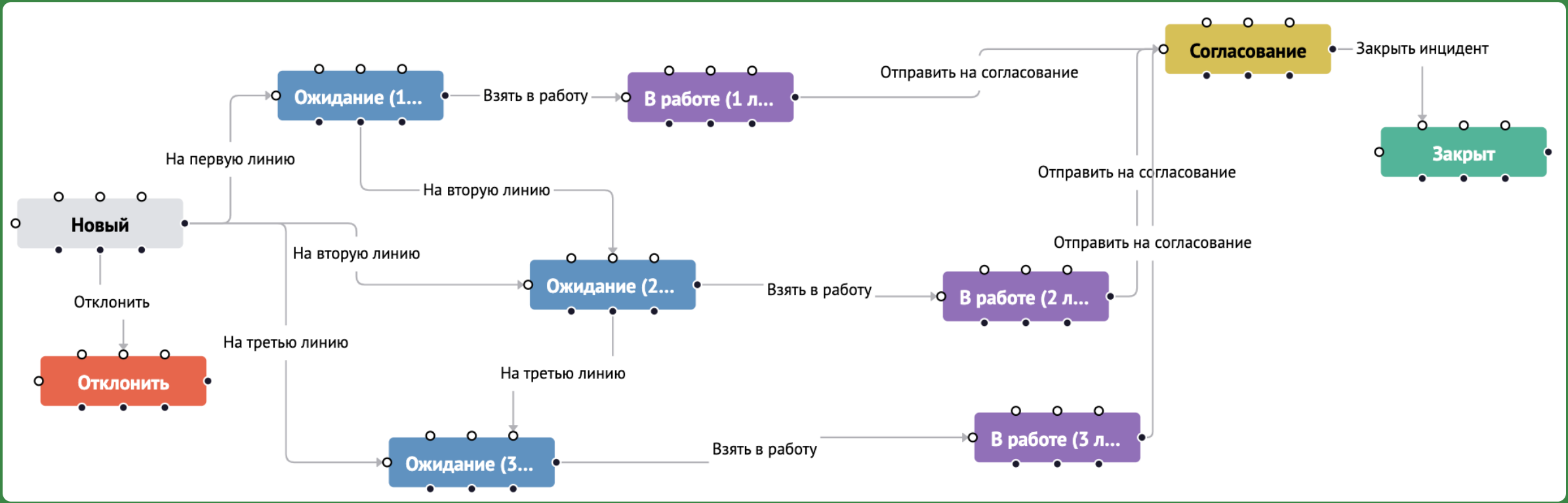
Incident Manager



- Уровни критичности
- Трекинг статусов
- Комментарии
- История изменений

VolgaBlob

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)

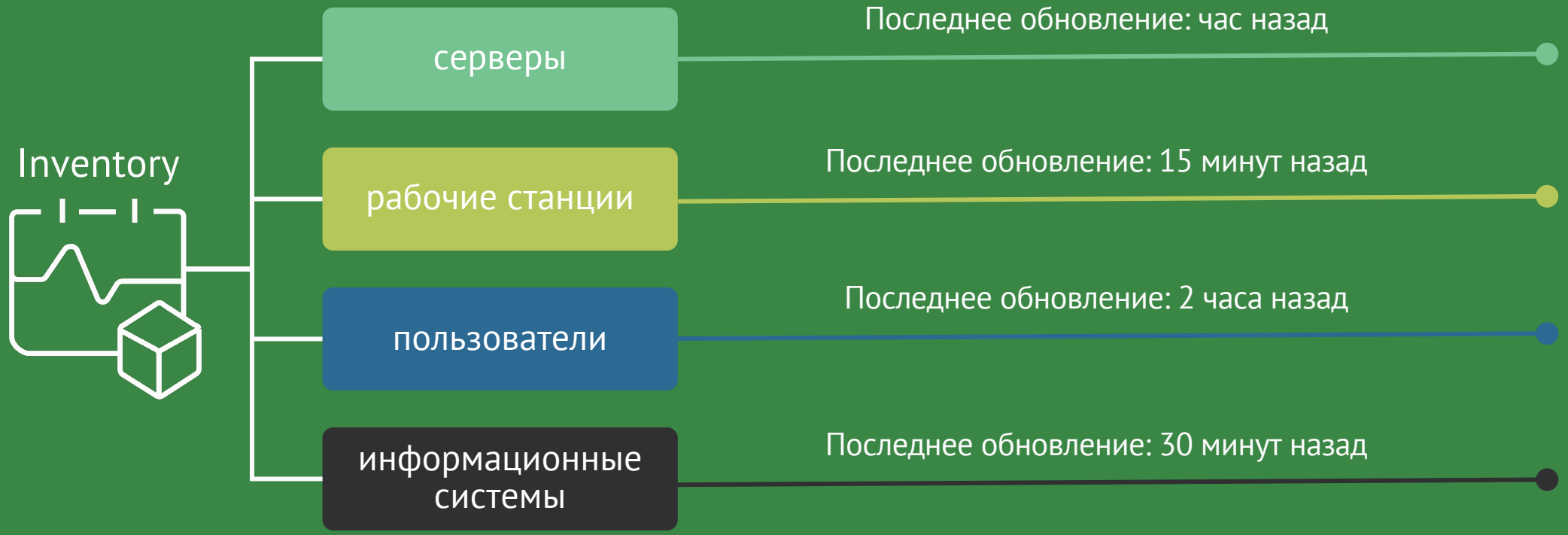
Модуль Inventory

Инструмент формирования и управления активами

Inventory: Назначение

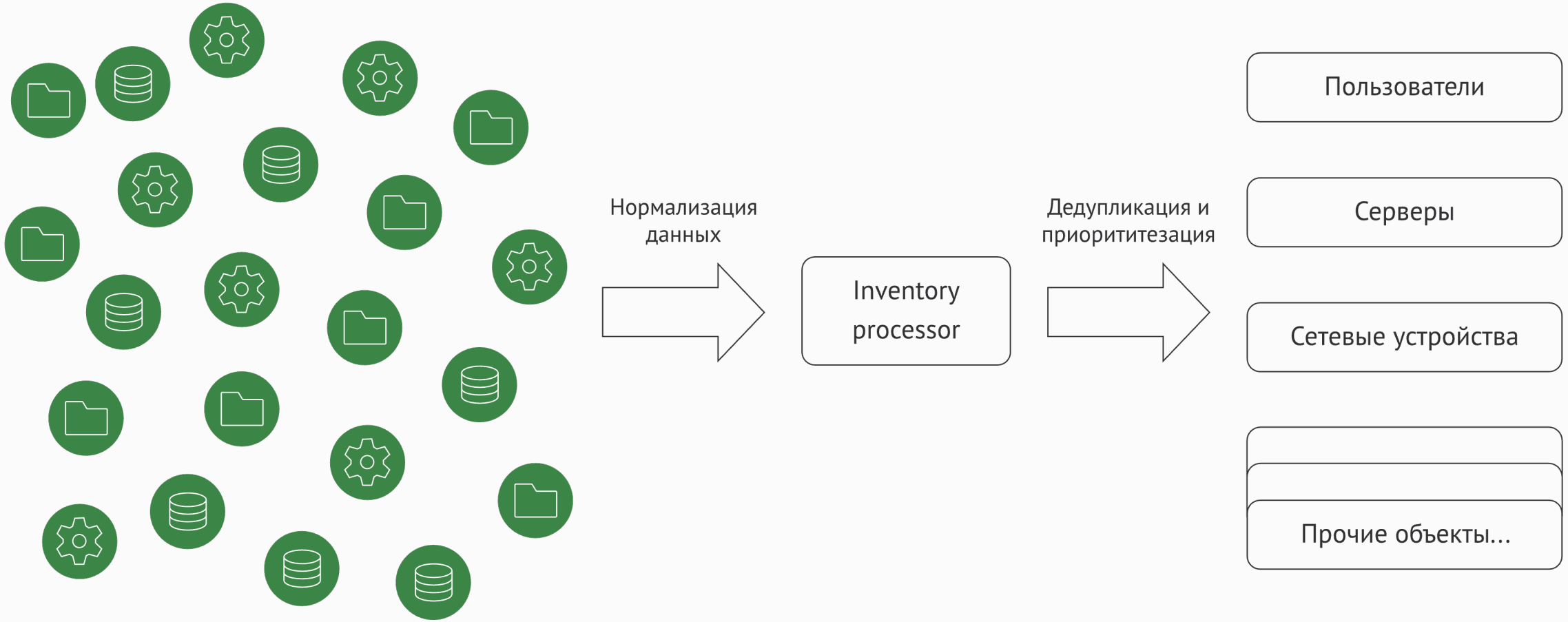
Модуль обеспечивает:

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



Inventory

Автоматизированный сбор и обновление базы активов от различных источников

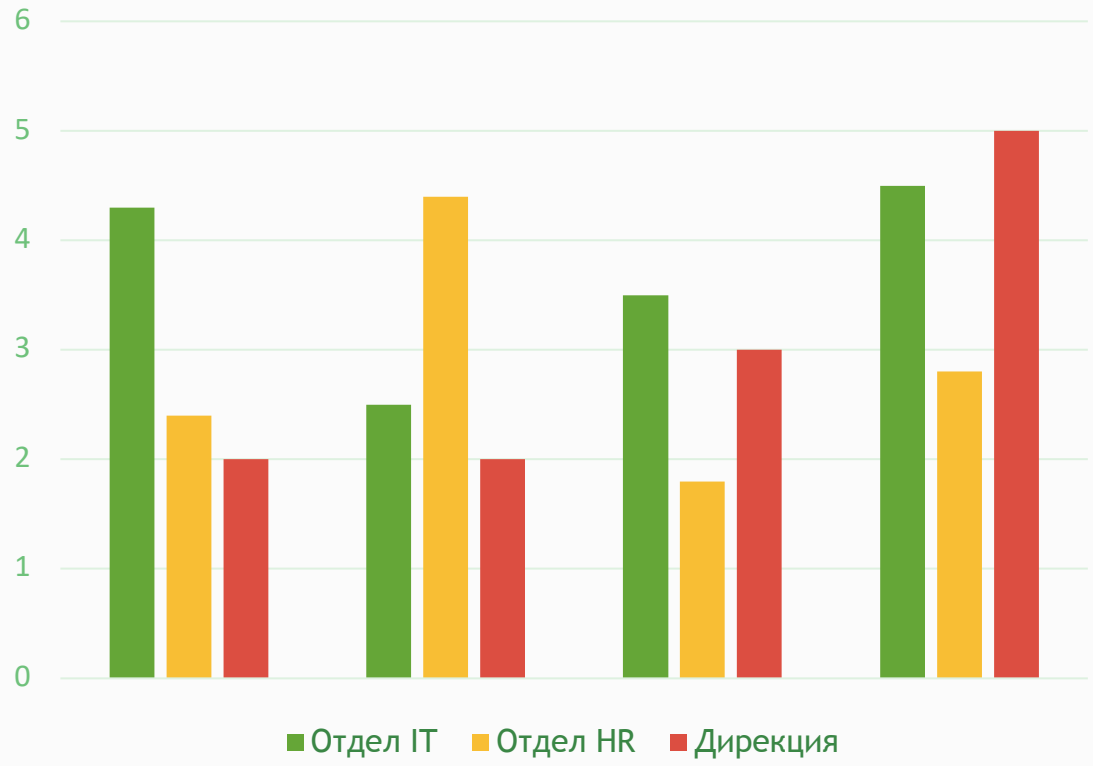


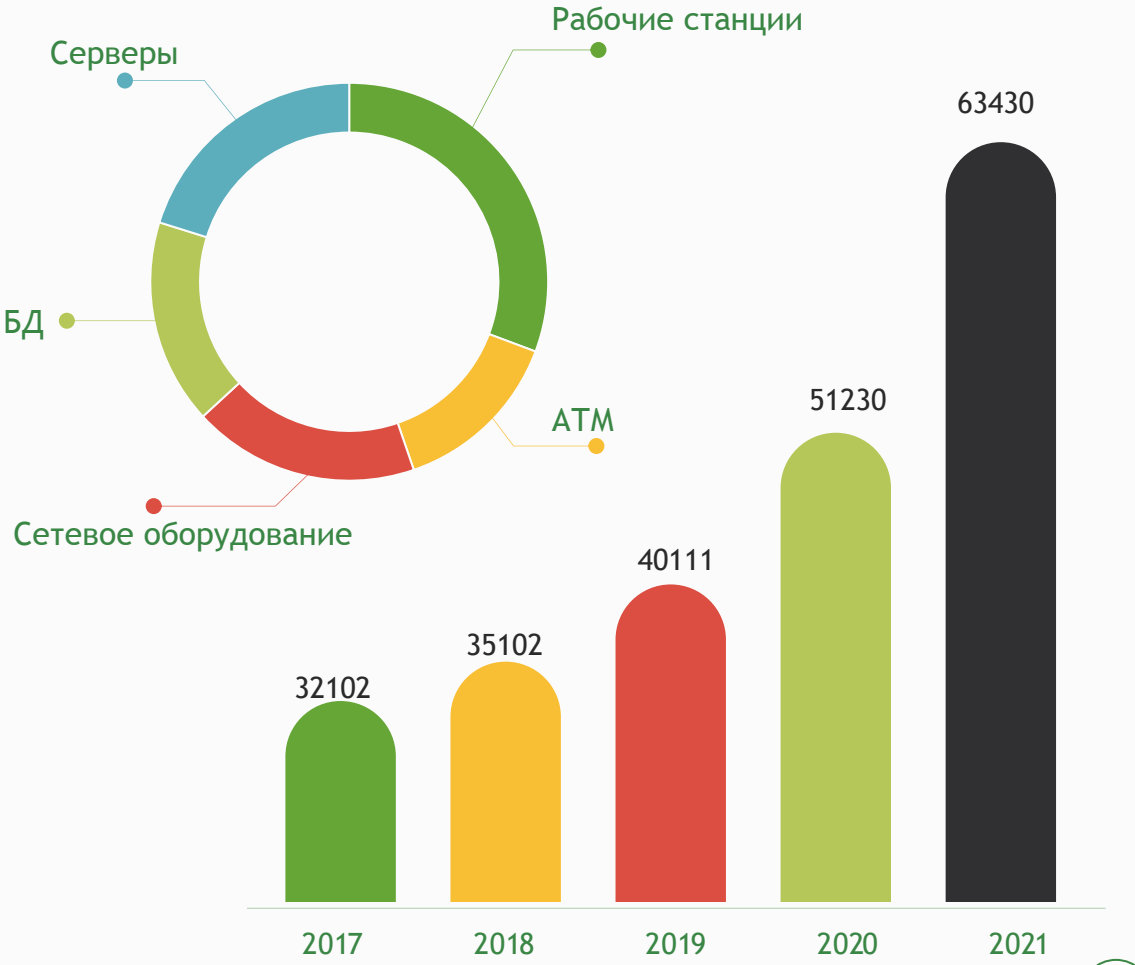
Актив – объект инвентаризации

Составные компоненты актива

Inventory

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

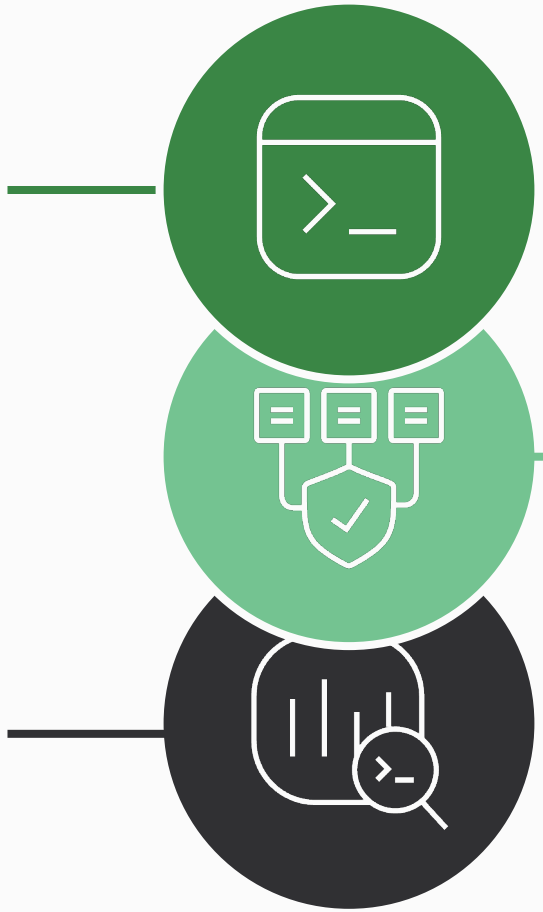




SDK для создания приложений на Smart Monitor

Возможности для разработчиков по созданию прикладной логики приложений

Приложение
Предоставление пользовательскому приложению возможности «встраивания» в Smart Monitor



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

Core
Приложение Smart Monitor

VolgaBlob

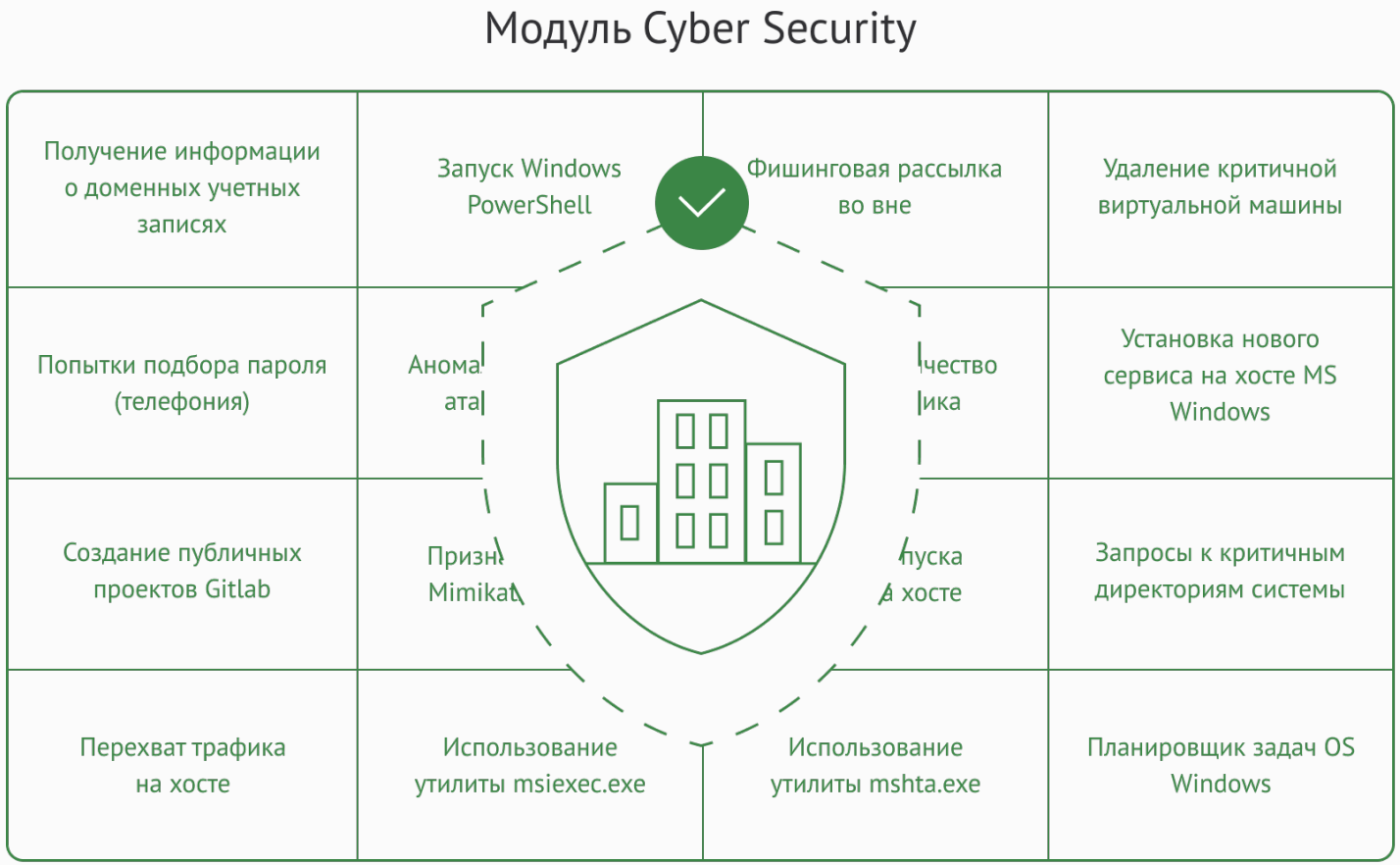
Модуль Cyber Security

Отслеживание событий информационной безопасности

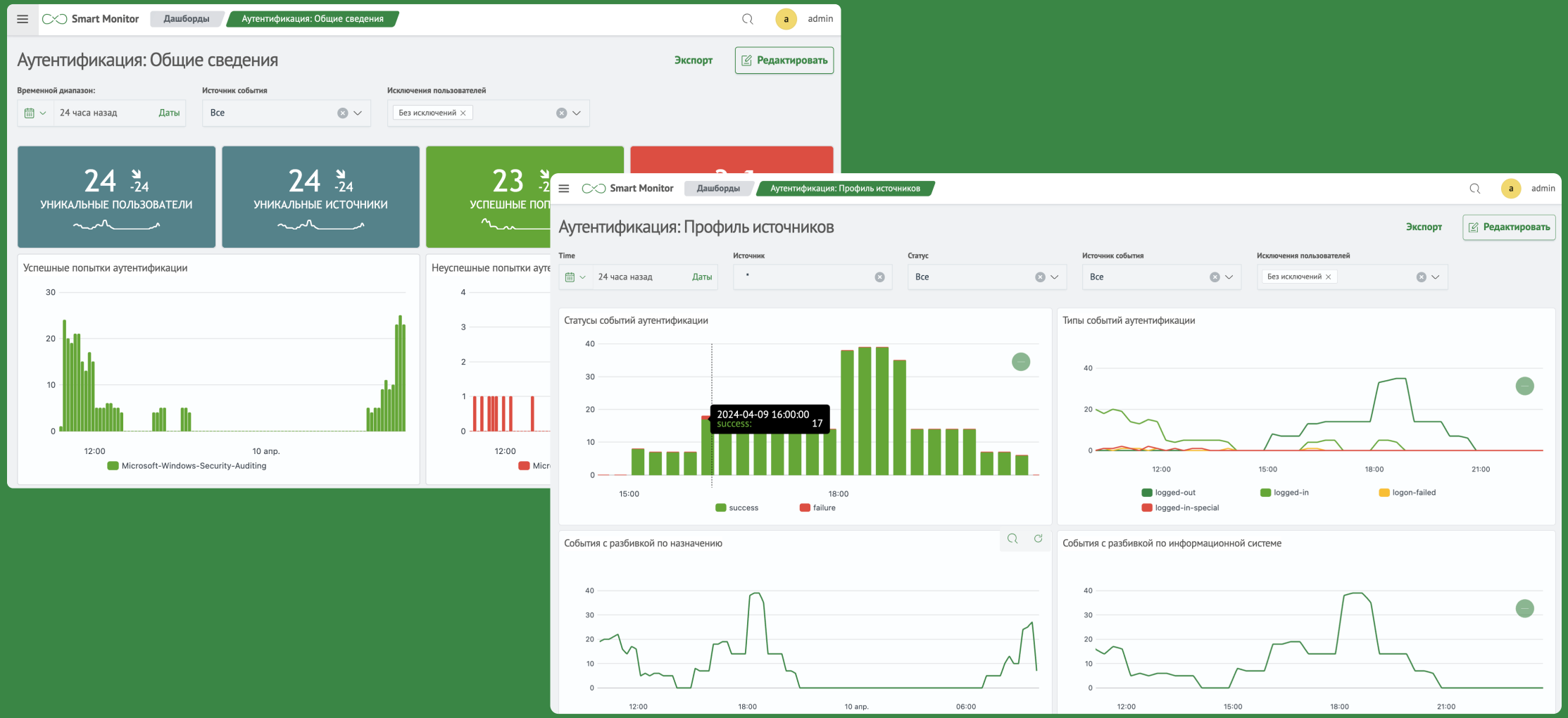
Cyber Security

Содержимым модуля является набор дашбордов и правил, которые структурно разделены на разделы.

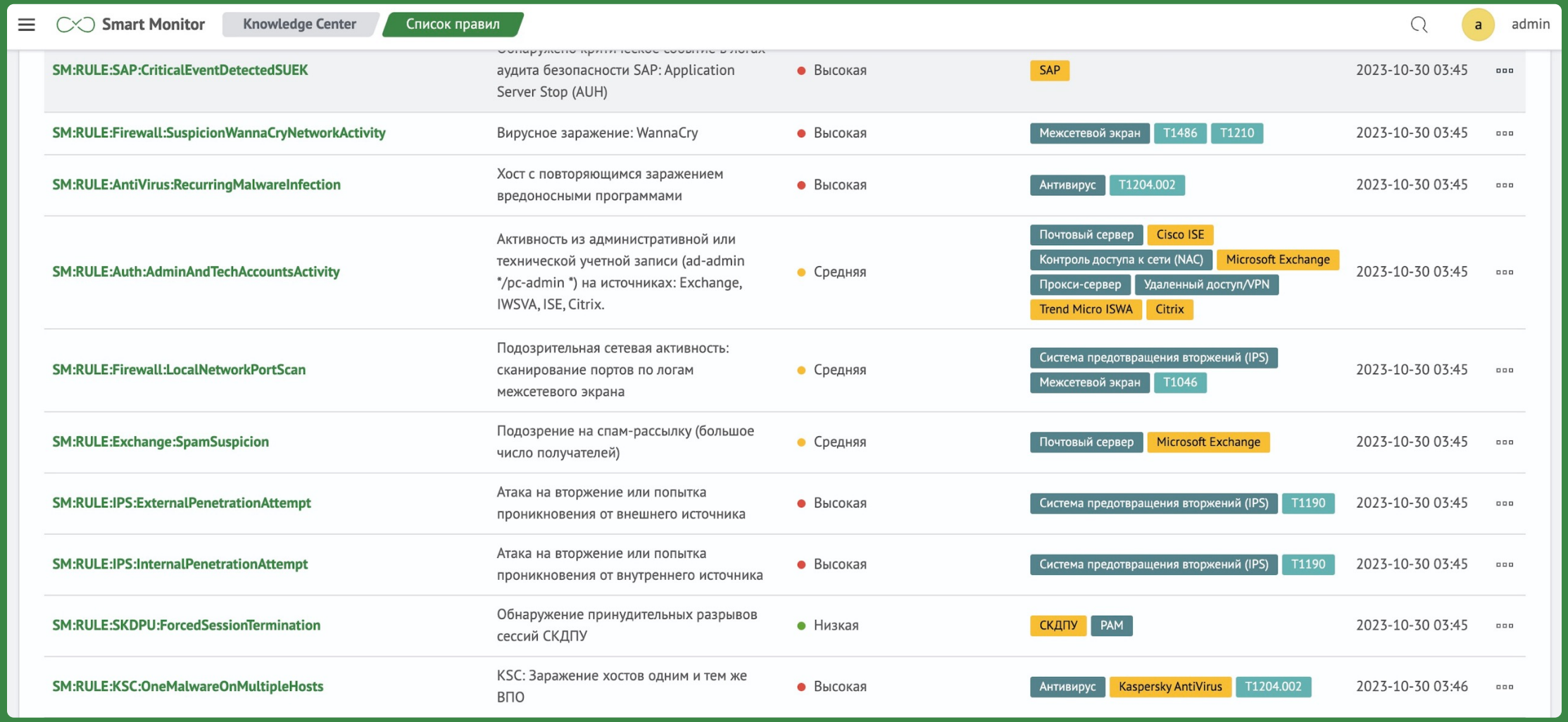
- Обновление базы корреляционных правил
- Обновление базы дашбордов
- Актуальная информация о новых инцидентах ИБ



Cyber Security: набор функциональных дашбордов

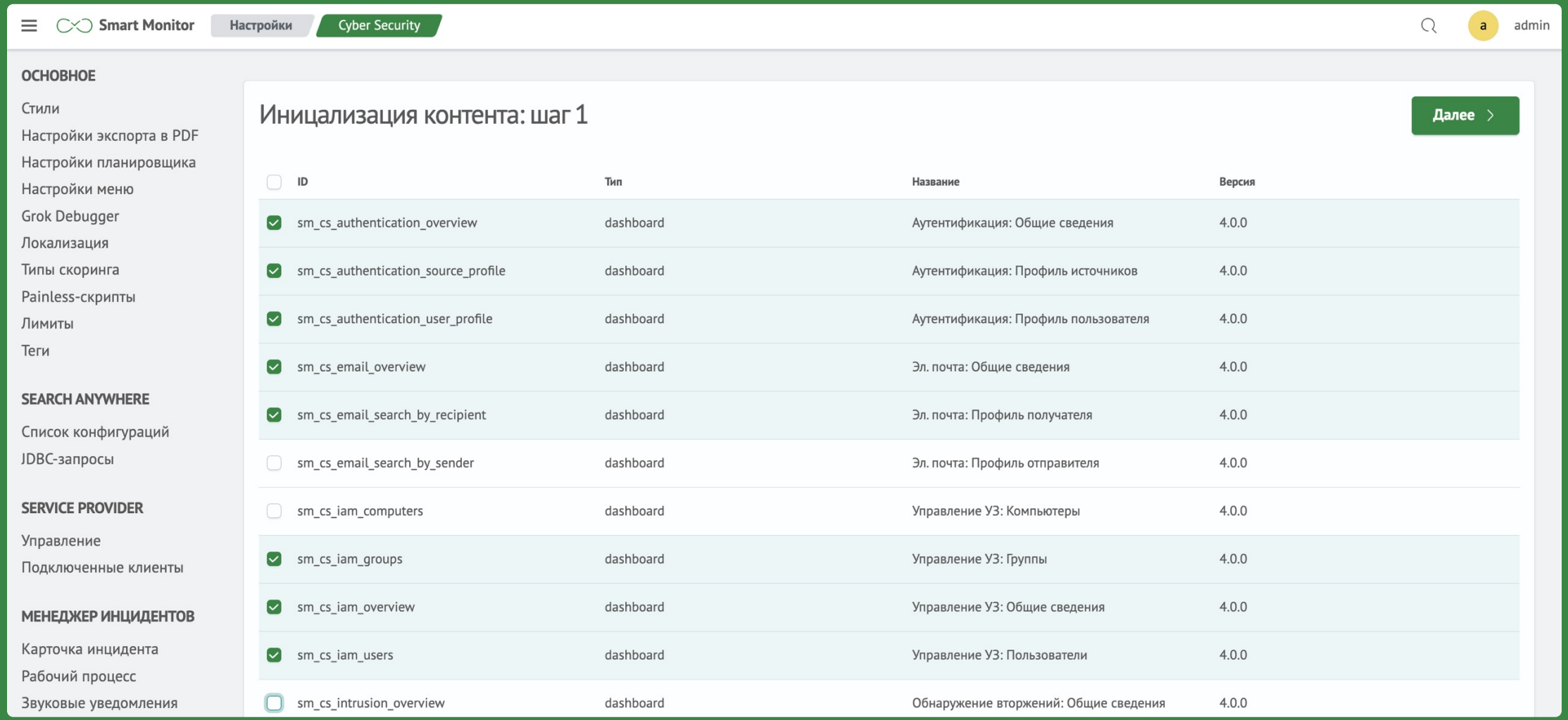


Cyber Security: правила детектирования инцидентов



SM:RULE:SAP:CriticalEventDetectedSUEK	Обнаружено критическое событие в логах аудита безопасности SAP: Application Server Stop (AUH)	Высокая	SAP	2023-10-30 03:45
SM:RULE:Firewall:SuspicionWannaCryNetworkActivity	Вирусное заражение: WannaCry	Высокая	Межсетевой экран, T1486, T1210	2023-10-30 03:45
SM:RULE:AntiVirus:RecurringMalwareInfection	Хост с повторяющимся заражением вредоносными программами	Высокая	Антивирус, T1204.002	2023-10-30 03:45
SM:RULE:Auth:AdminAndTechAccountsActivity	Активность из административной или технической учетной записи (ad-admin */pc-admin *) на источниках: Exchange, IWSVA, ISE, Citrix.	Средняя	Почтовый сервер, Cisco ISE, Контроль доступа к сети (NAC), Microsoft Exchange, Прокси-сервер, Удаленный доступ/VPN, Trend Micro ISWA, Citrix	2023-10-30 03:45
SM:RULE:Firewall:LocalNetworkPortScan	Подозрительная сетевая активность: сканирование портов по логам межсетевого экрана	Средняя	Система предотвращения вторжений (IPS), Межсетевой экран, T1046	2023-10-30 03:45
SM:RULE:Exchange:SpamSuspicion	Подозрение на спам-рассылку (большое число получателей)	Средняя	Почтовый сервер, Microsoft Exchange	2023-10-30 03:45
SM:RULE:IPS:ExternalPenetrationAttempt	Атака на вторжение или попытка проникновения от внешнего источника	Высокая	Система предотвращения вторжений (IPS), T1190	2023-10-30 03:45
SM:RULE:IPS:InternalPenetrationAttempt	Атака на вторжение или попытка проникновения от внутреннего источника	Высокая	Система предотвращения вторжений (IPS), T1190	2023-10-30 03:45
SM:RULE:SKDPU:ForcedSessionTermination	Обнаружение принудительных разрывов сессий СКДПУ	Низкая	СКДПУ, PAM	2023-10-30 03:45
SM:RULE:KSC:OneMalwareOnMultipleHosts	KSC: Заражение хостов одним и тем же ВПО	Высокая	Антивирус, Kaspersky AntiVirus, T1204.002	2023-10-30 03:46

Cyber Security: управление контентом

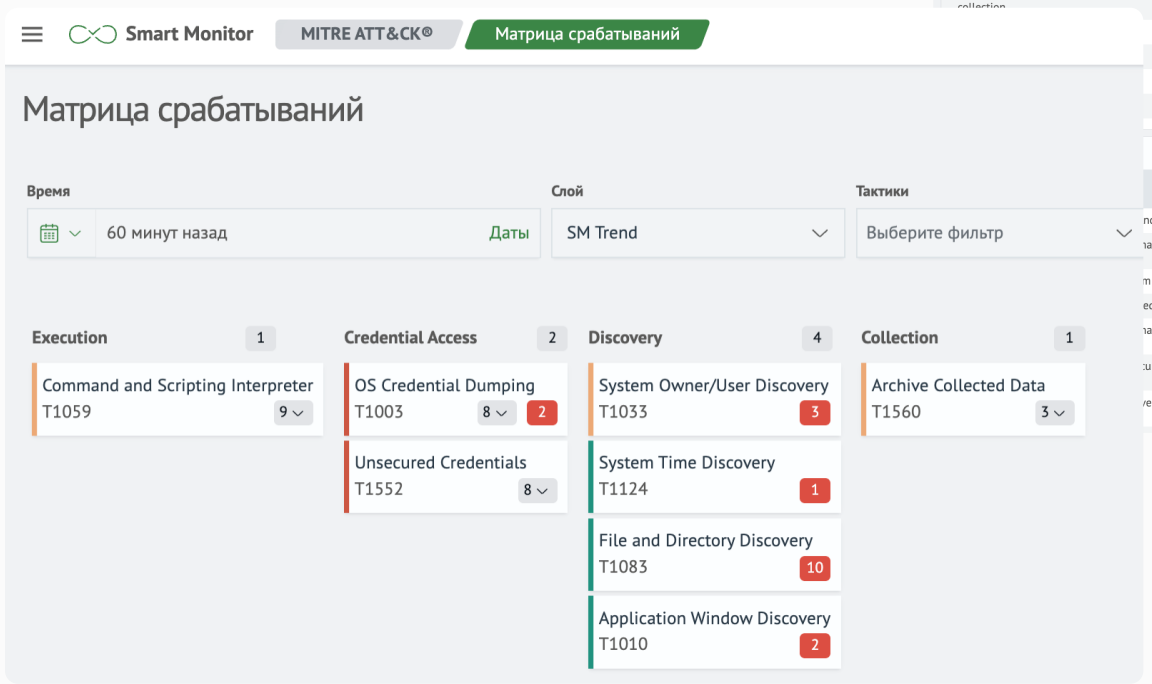


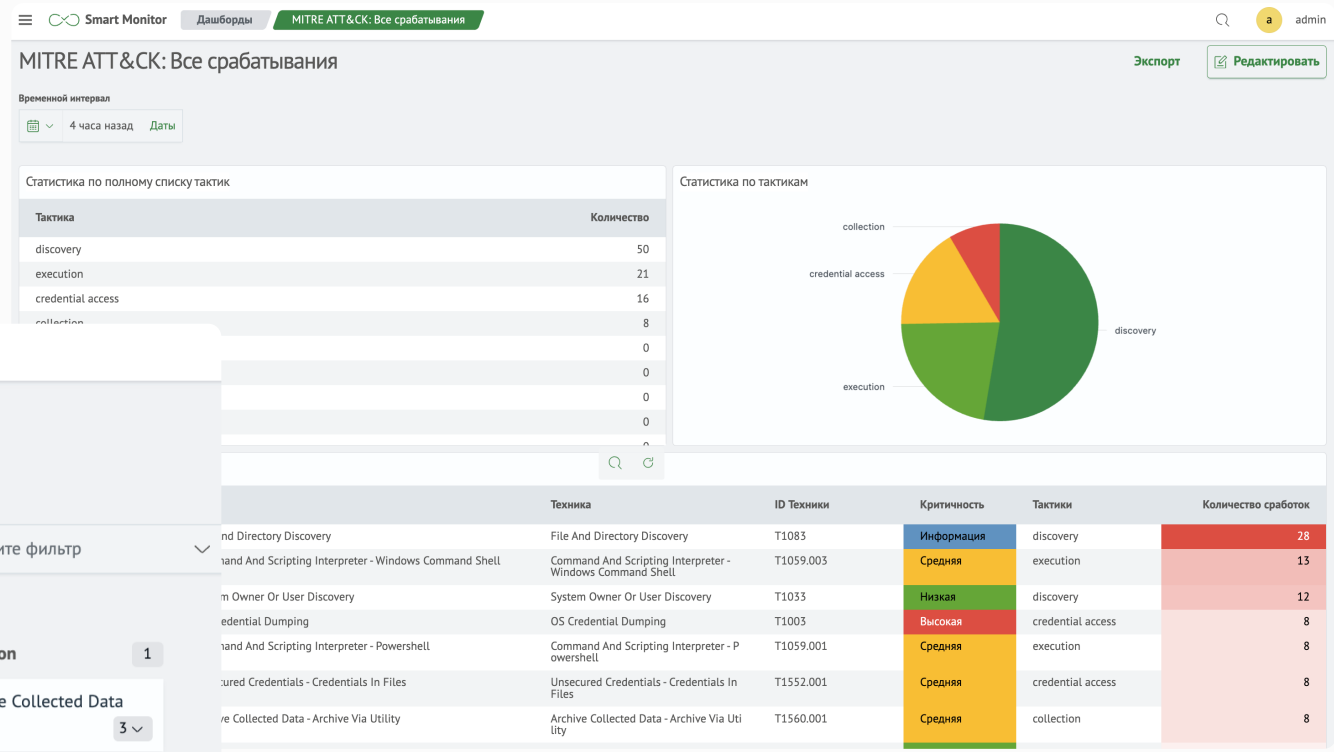
Модуль MITRE ATT&CK

Применение сценариев использования MITRE ATT&CK

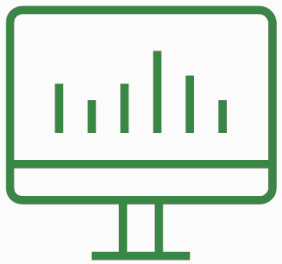
Модуль MITRE ATT&CK позволяет:

- оценить покрытие техник инструментальными контролями
- сформировать специализированные модели угроз и применить их к компонентам ИТ-ландшафта





- детектировать потенциальное использование техник на основе событий от источников данных

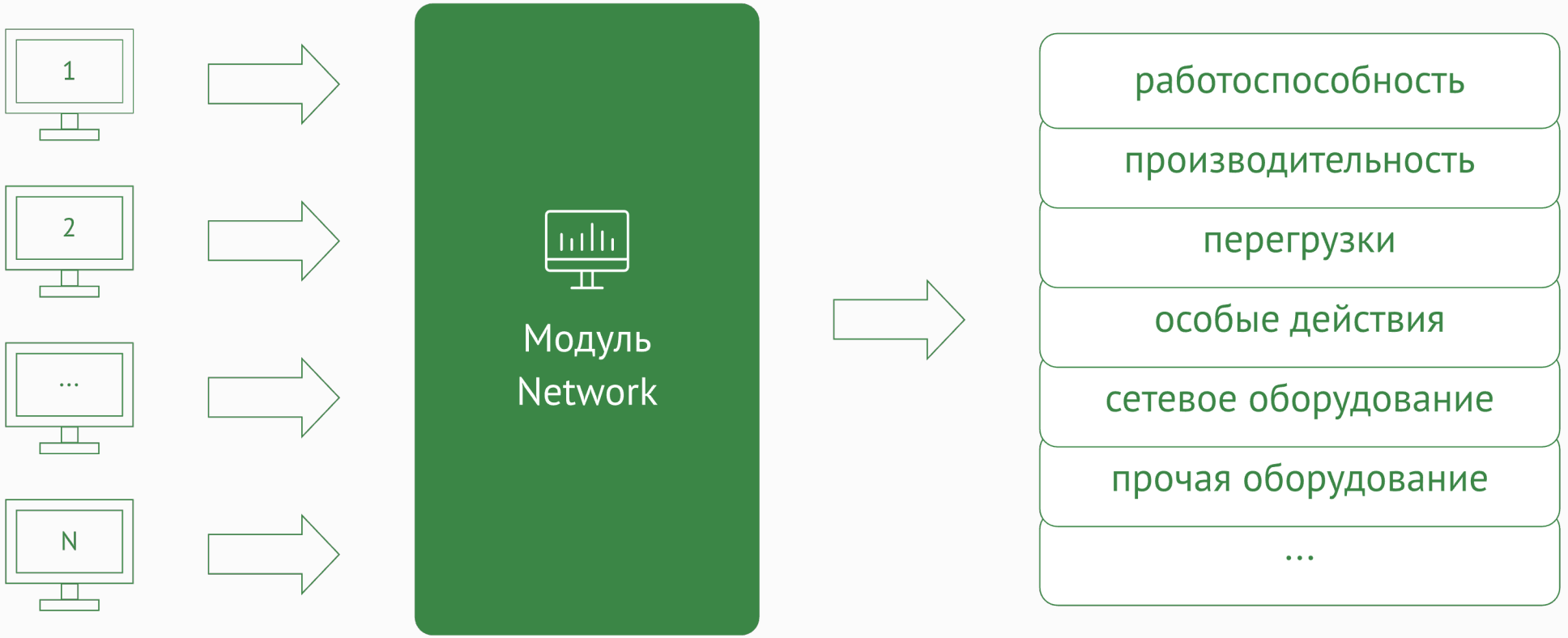


Модуль Network

Мониторинг сетевого оборудования

Network: функциональные характеристики

Модуль предназначен для тщательного мониторинга сетевого оборудования
и реагирования на возможные изменения в его сети и конфигурациях



Network: функциональные характеристики

Контроль за использованием ресурсов оборудования

- оптимизация работы устройств (процессор, память, сетевые интерфейсы, порты, вентиляторы, температуру)
- снижение затрат на техническое обслуживание и повышение производительность сети

Контроль за изменениями конфигурации оборудования

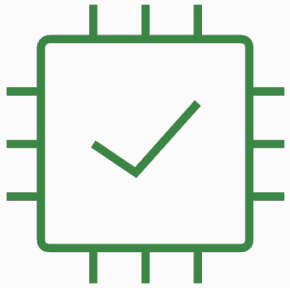
- отслеживание любых изменений в настройках сетевого оборудования
- контроль изменений в сети и управление ими
- предотвращение возможных нарушений безопасности или неправильных конфигураций

Автоматизация

- автоматический сбор и анализ информации о состоянии сетевого оборудования, каналов связи и подключенных устройств
- мгновенное уведомление пользователя о работоспособности и производительности сети

История контроля и доступа к оборудованию

- отслеживание, кто и когда получал доступ к сетевому оборудованию
- предотвращение несанкционированного доступа или использование оборудования

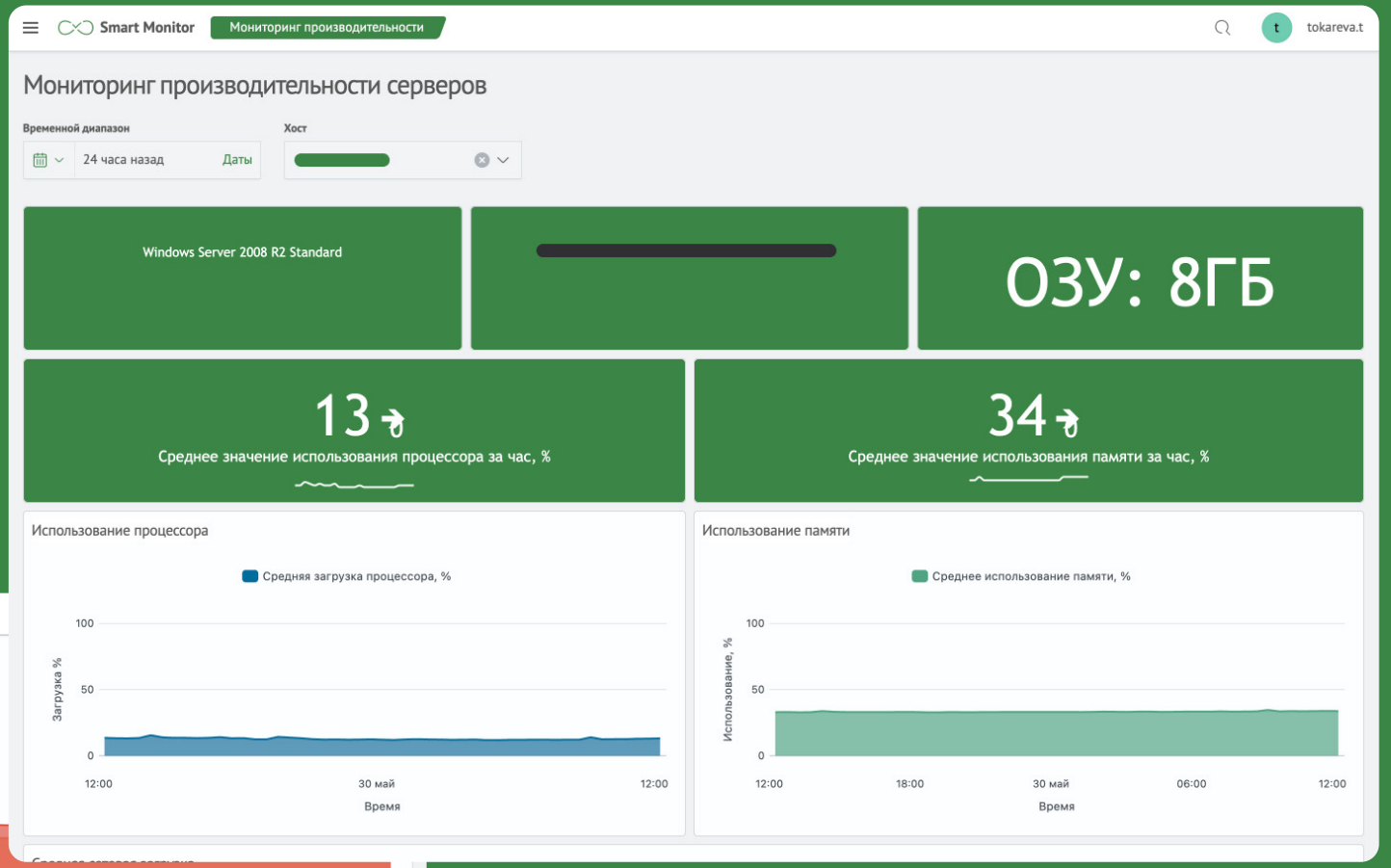


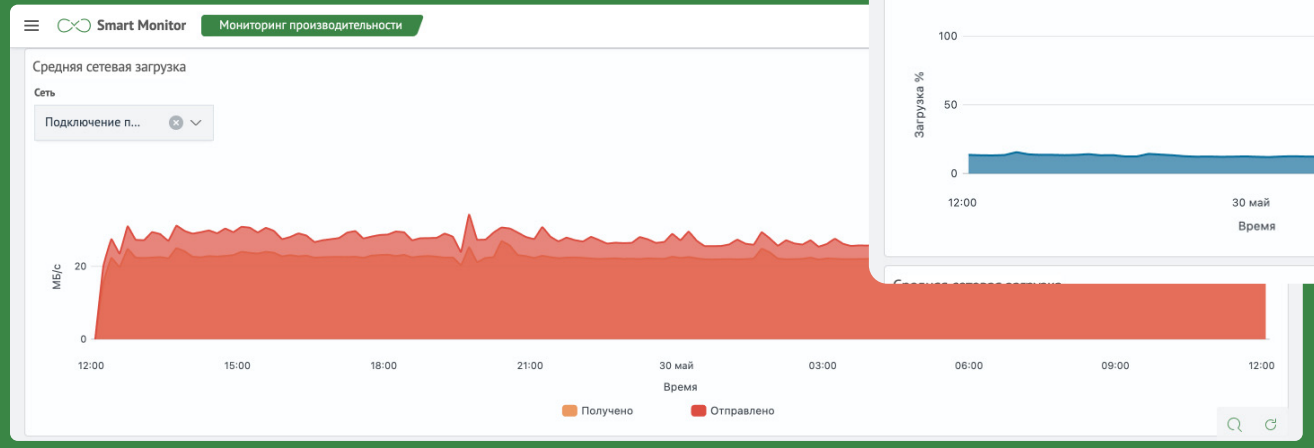
Модуль Servers

оптимизация ресурсов и контроль эффективности

Servers

Модуль отслеживает и анализирует серверные процессы, использование ресурсов (в том числе, активность процессора, памяти и диска).





VolgaBlob

Демонстрация

Smart Monitor

Пора запросить

демо-версию,

как нам кажется ☺