VB-Trend 2025

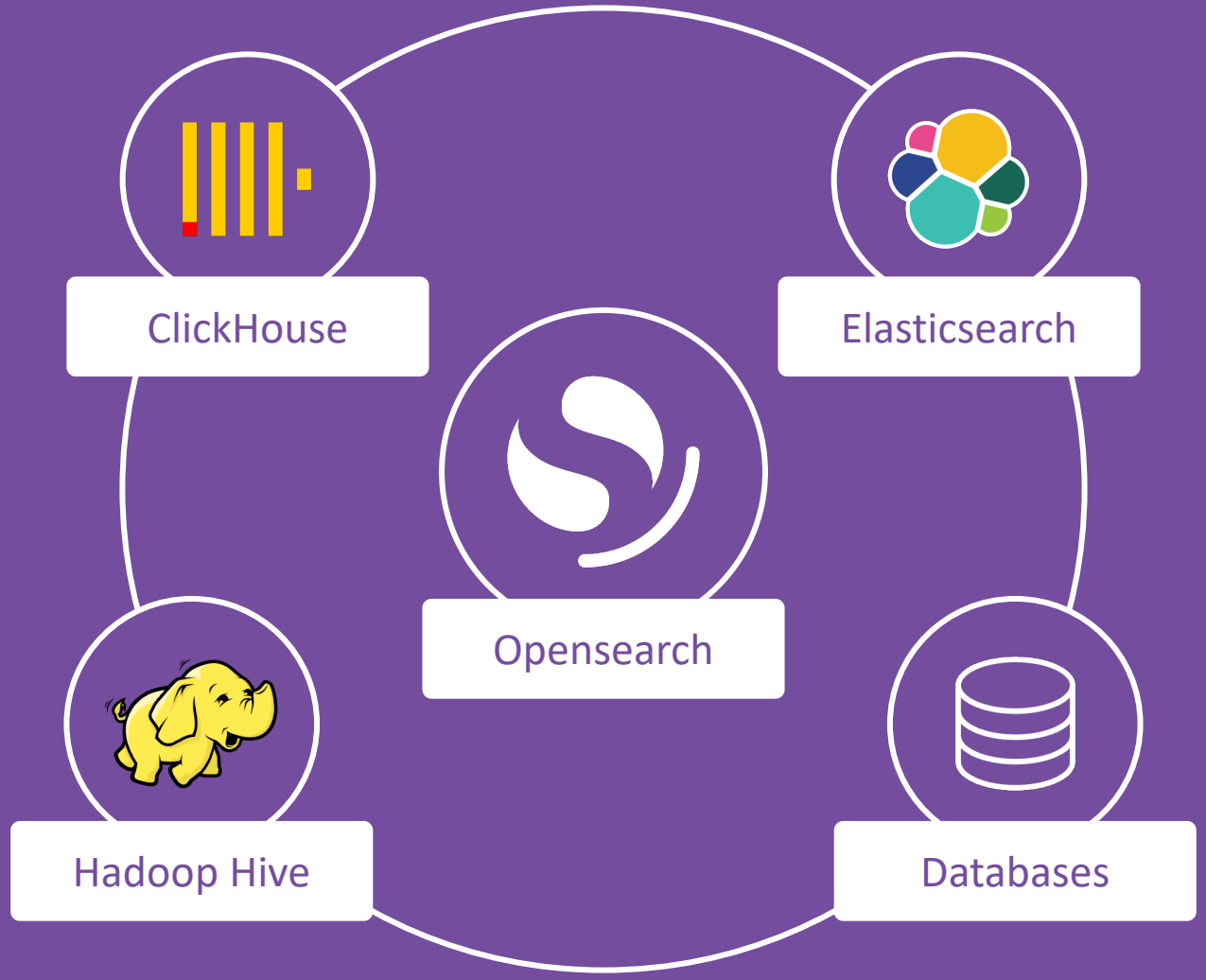
АНТИХРУПКОСТЬ БИЗНЕСА

Smart Monitor: обзор изменений

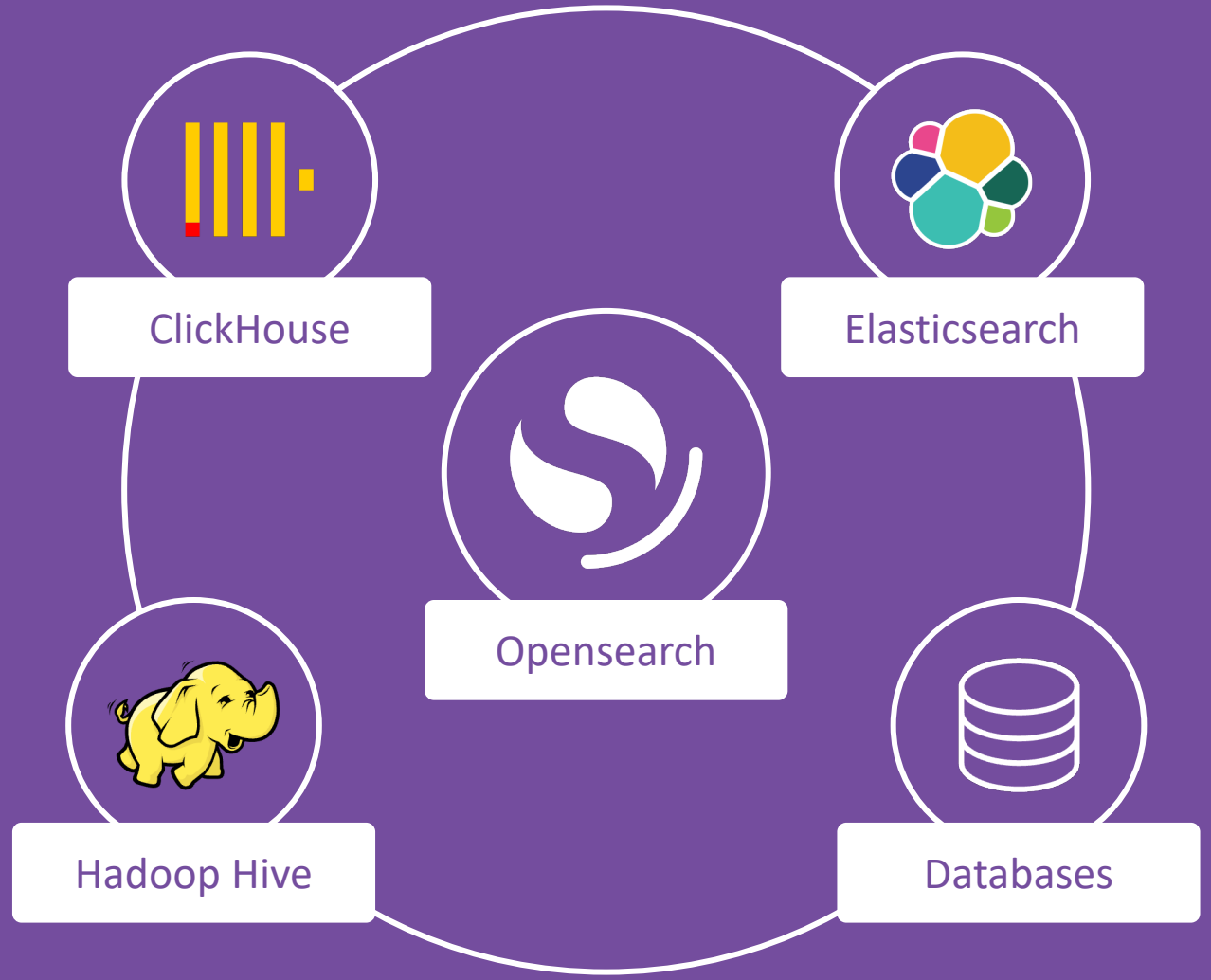
Максим Кириенко
VolgaBlob

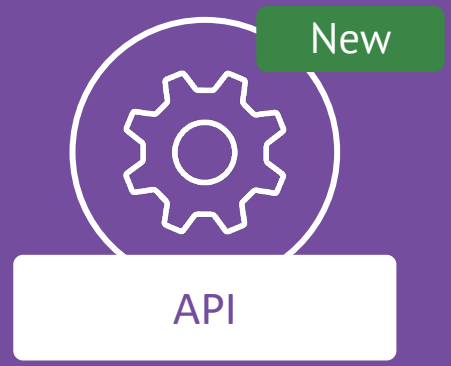
Новый источник Search Anywhere

Развитие Search Anywhere



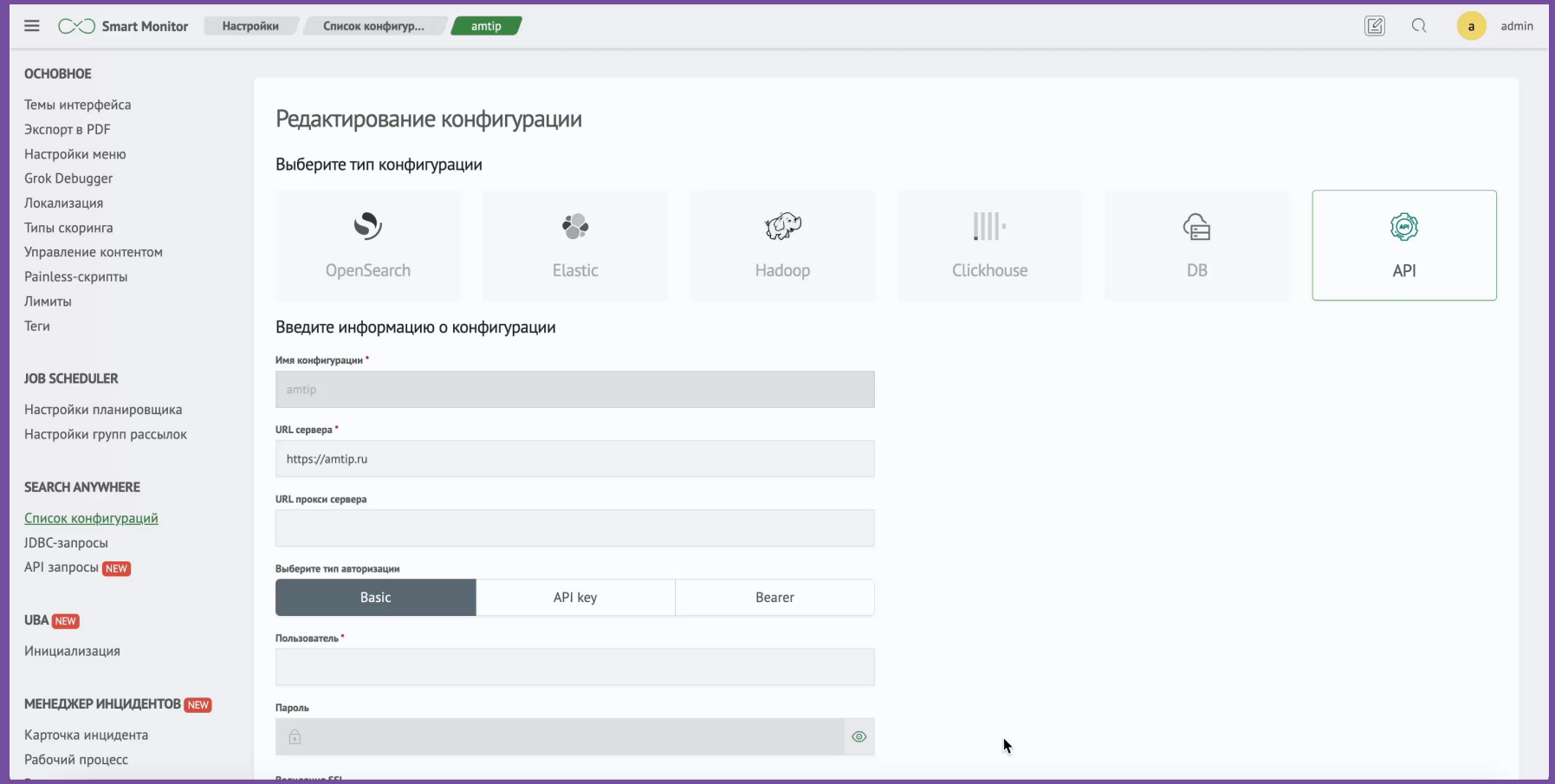
Развитие Search Anywhere





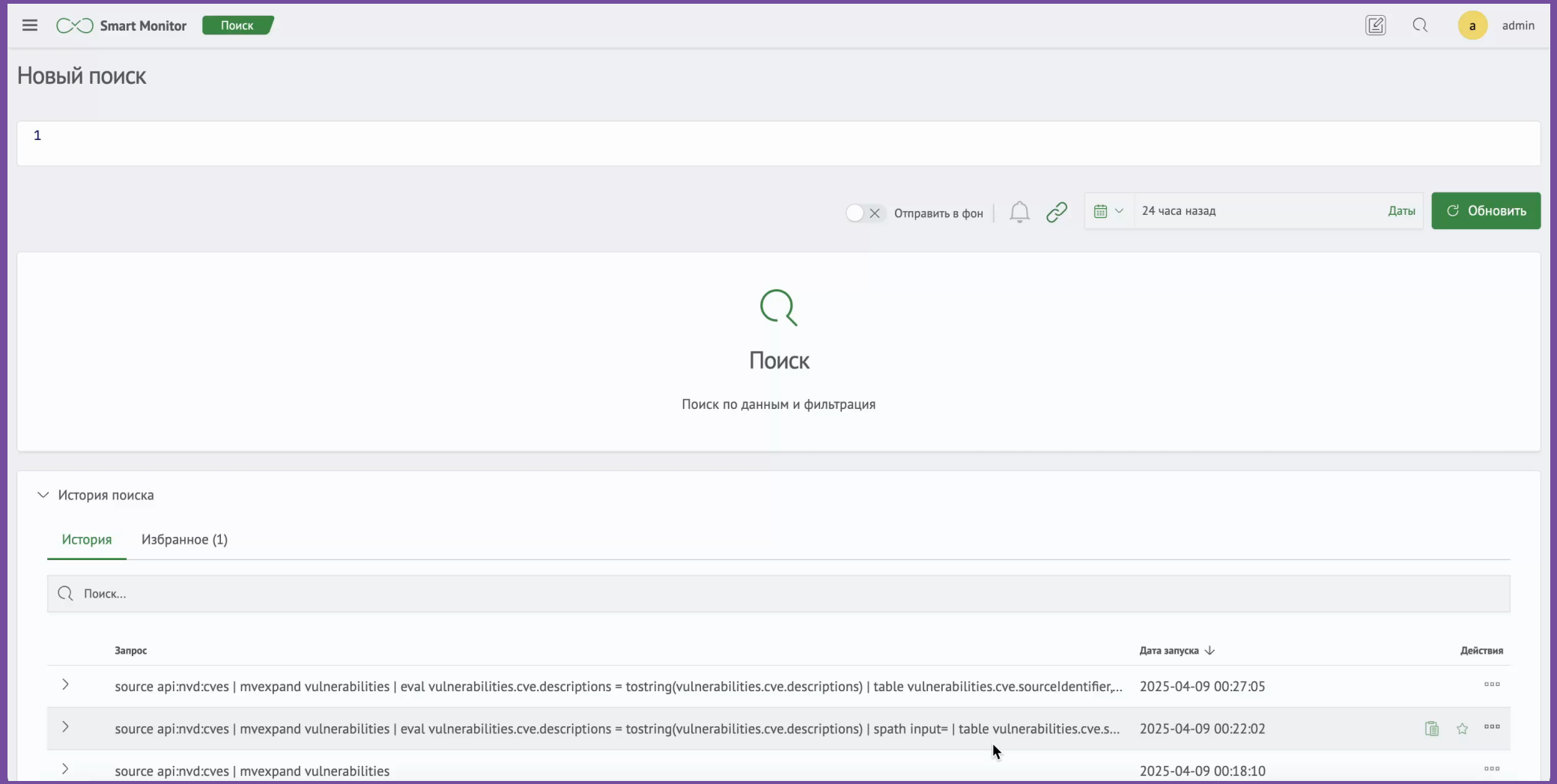
Возможности конфигурации

- Предоставлены все необходимые настройки для подключению по REST API к различным источникам
- Можно настроить подключение и запрос, которые в дальнейшем могут быть использованы в команде.

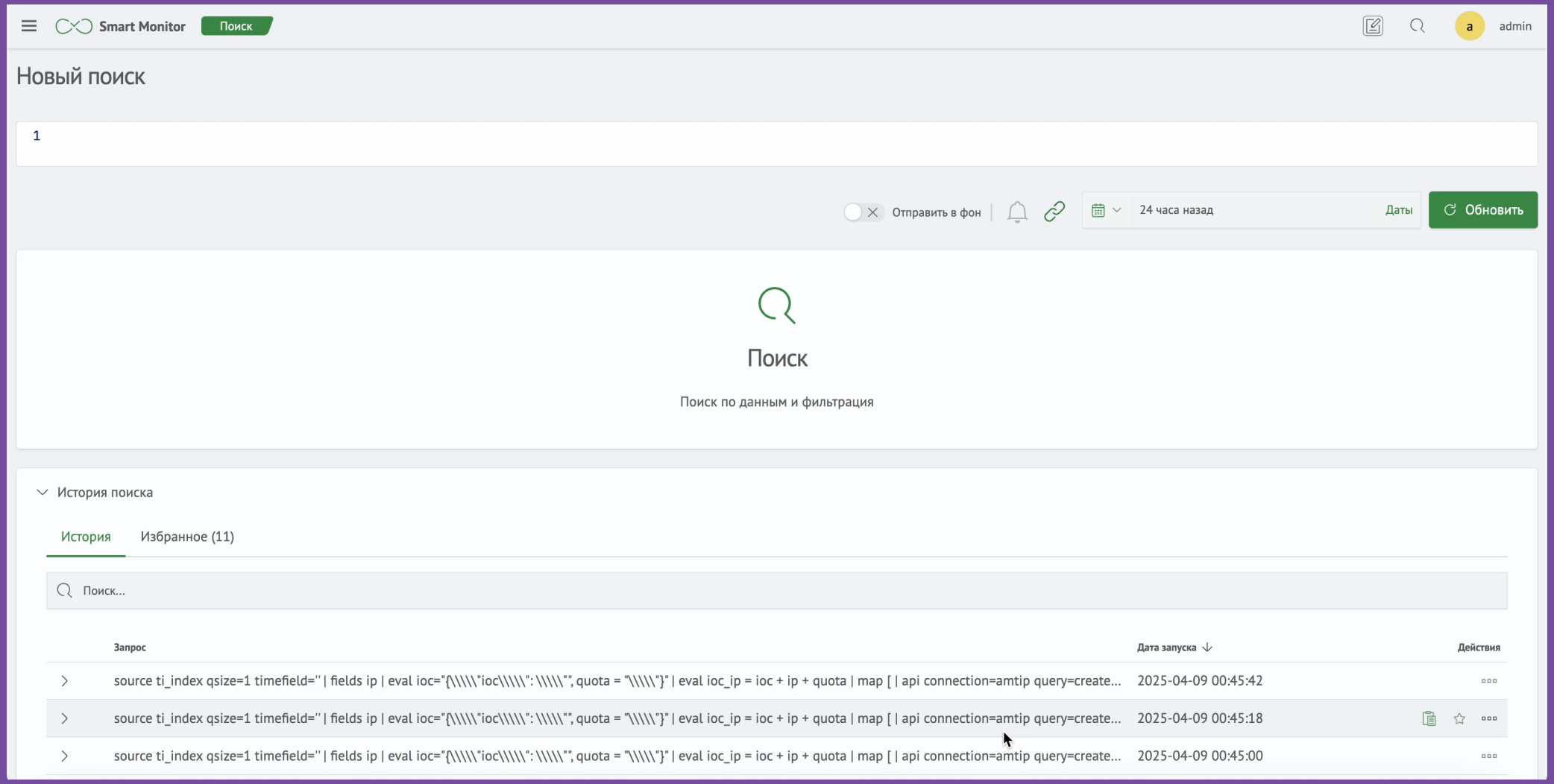


VolgaBlob

Поиск через команду source

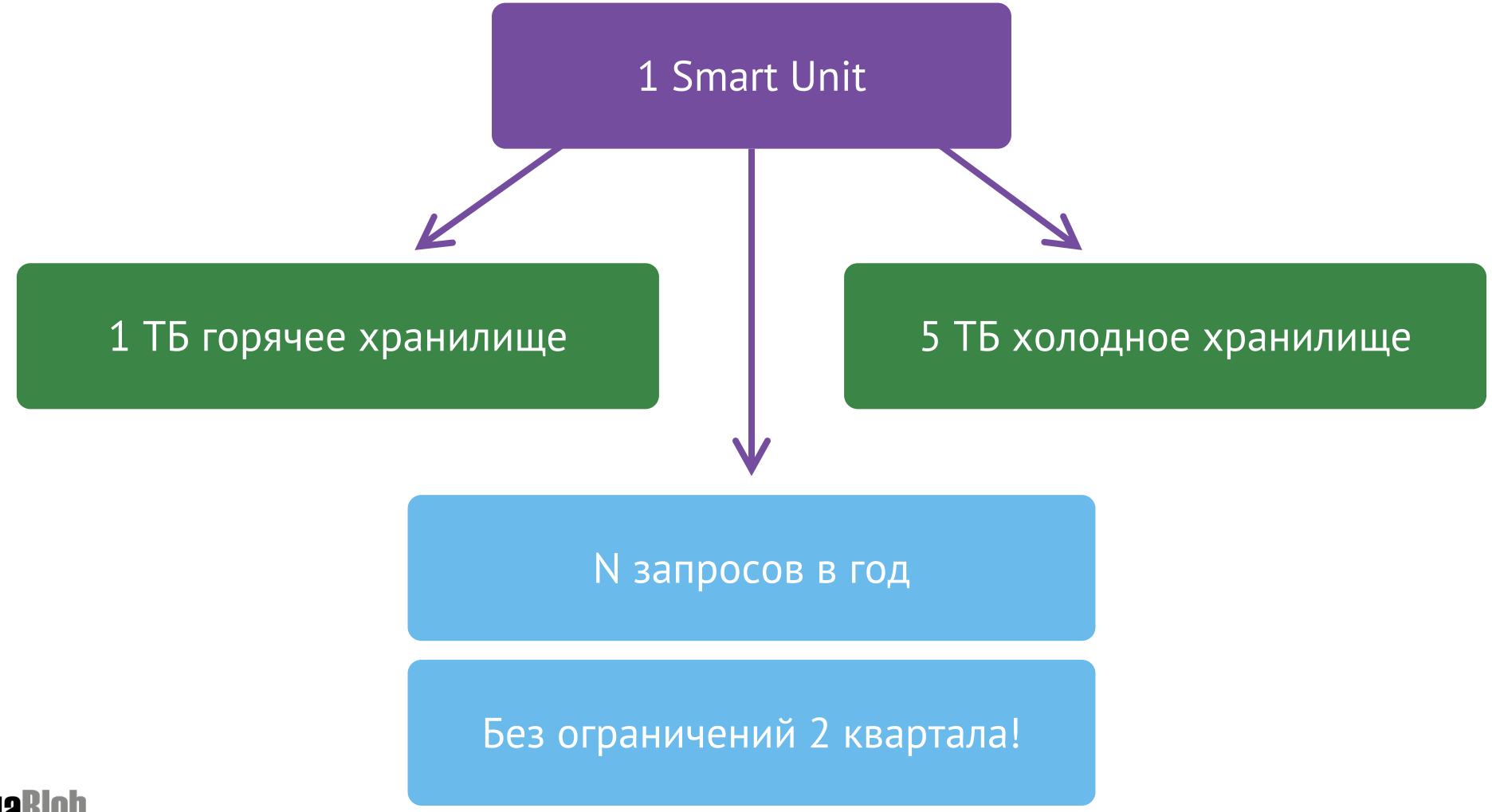


Команда api и режимы



VolgaBlob

Лицензирование



Smart Notebooks

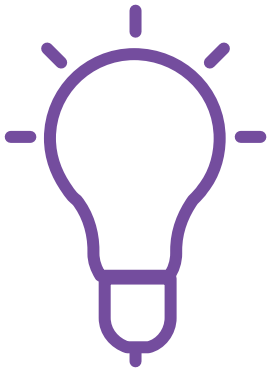
Доступность знаний одно из важных частей

Какие плюсы дает накопление знаний

- Переиспользование опыта и знаний
- Ускорение работы
- Предотвращение потерь данных и «bus factor»

Последствия отсутствия базы знаний

- Повторяющиеся ошибки
- Медленные процессы
- Упущенная выгода



Кейсы применения

Расследование

Сохранять все необходимые данные об инциденте

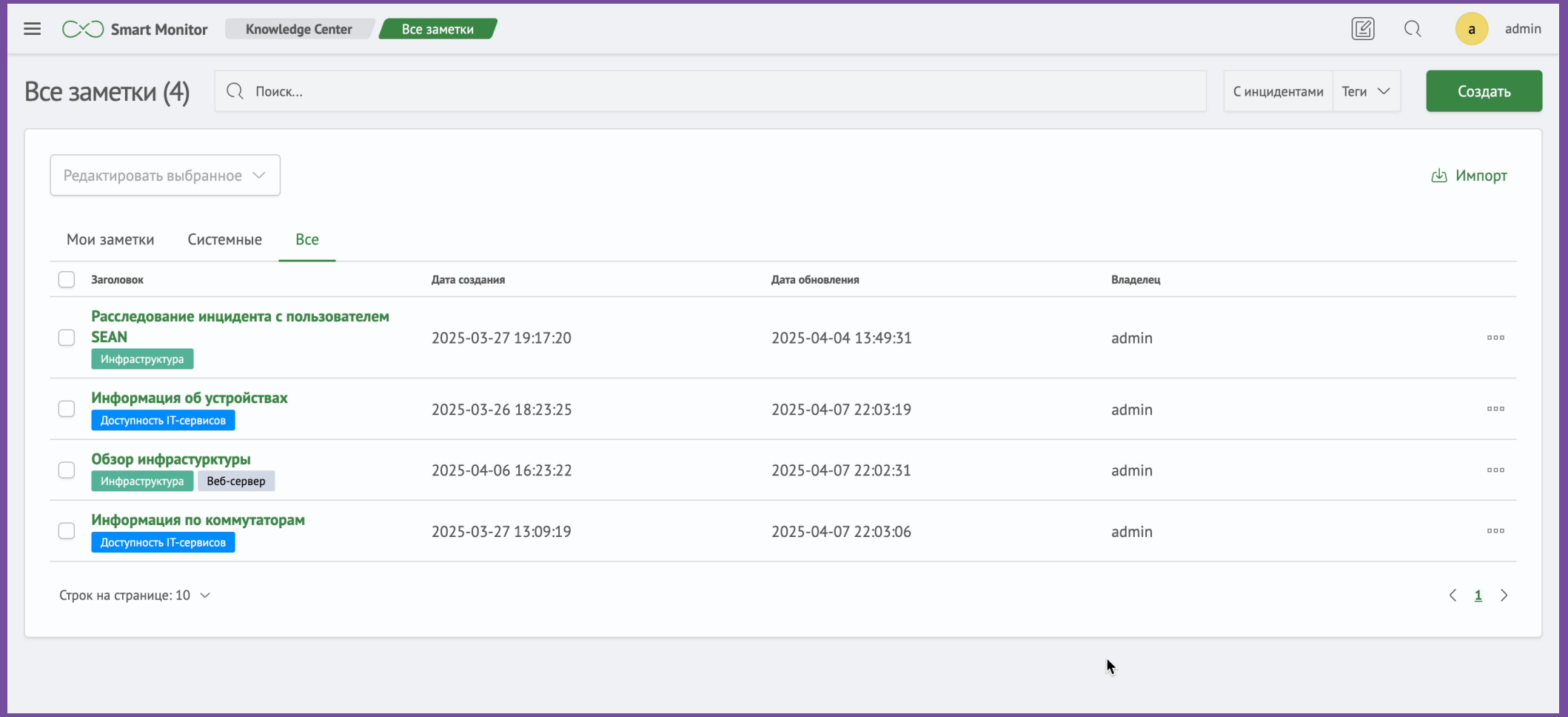
Отчетность

Динамические отчеты на основе данных
в реальном времени

Полезные заметки

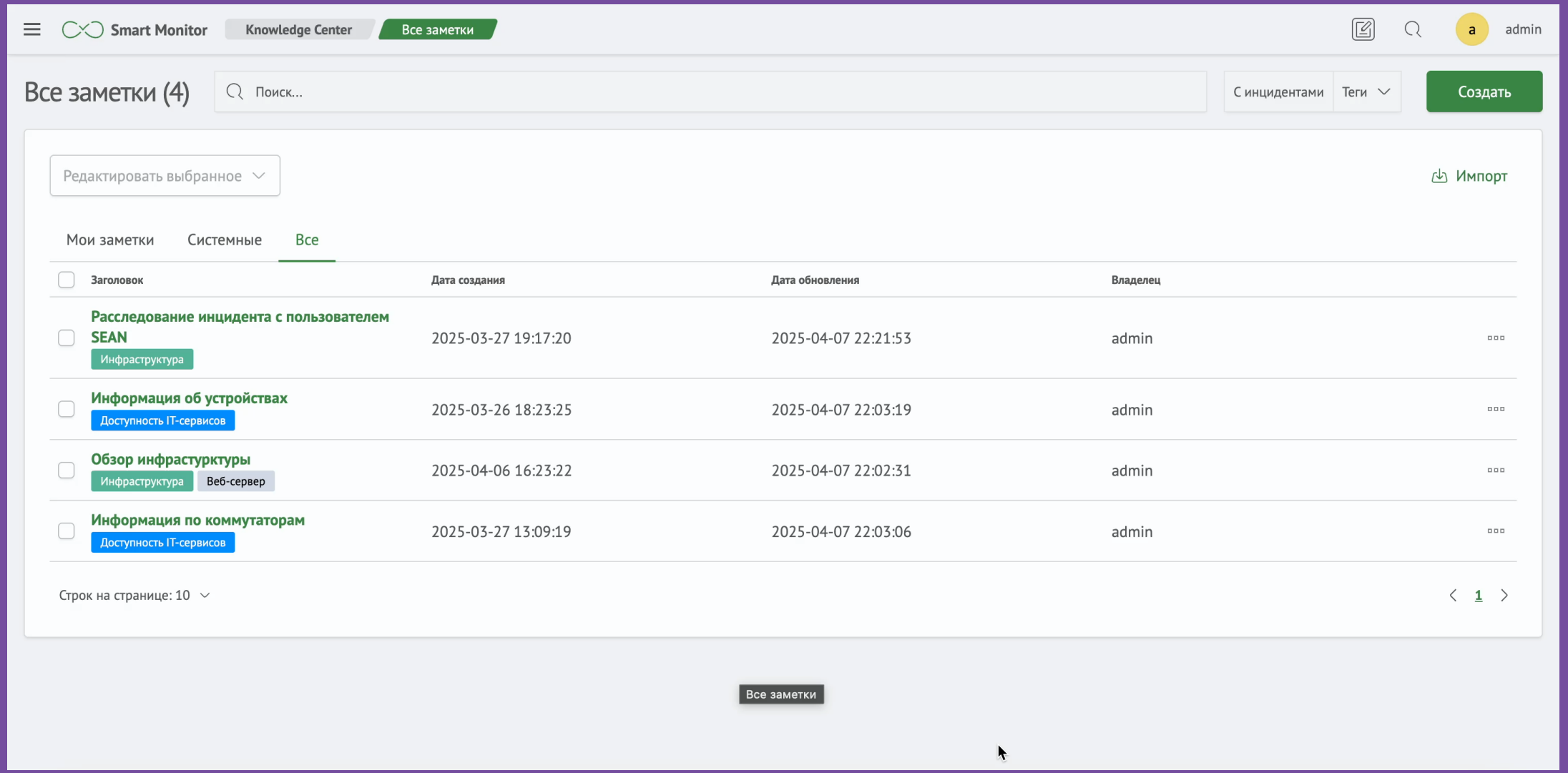
Сохранить знания, полезные для себя и для других

Заметки в Smart Monitor!

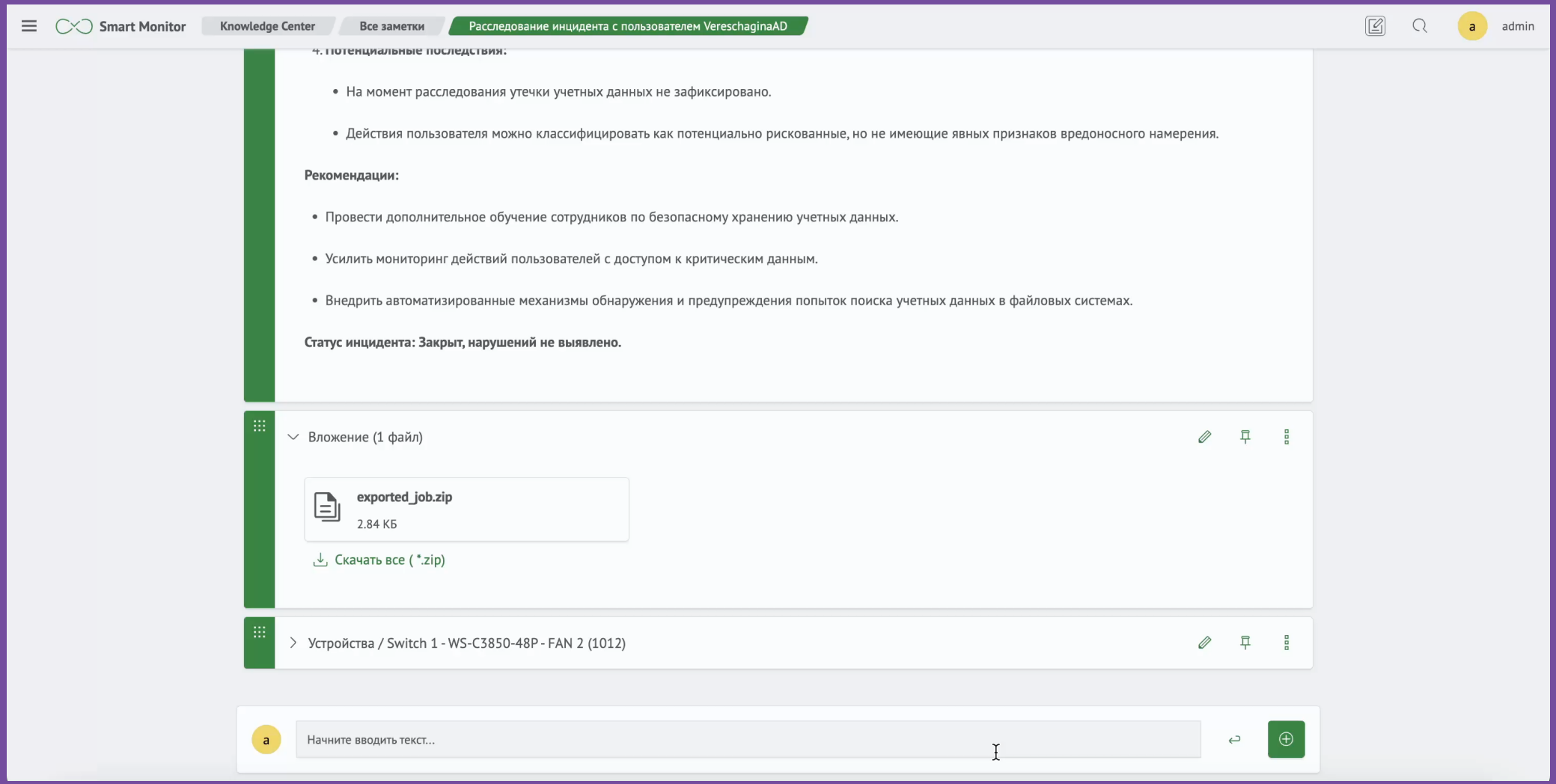


VolgaBlob

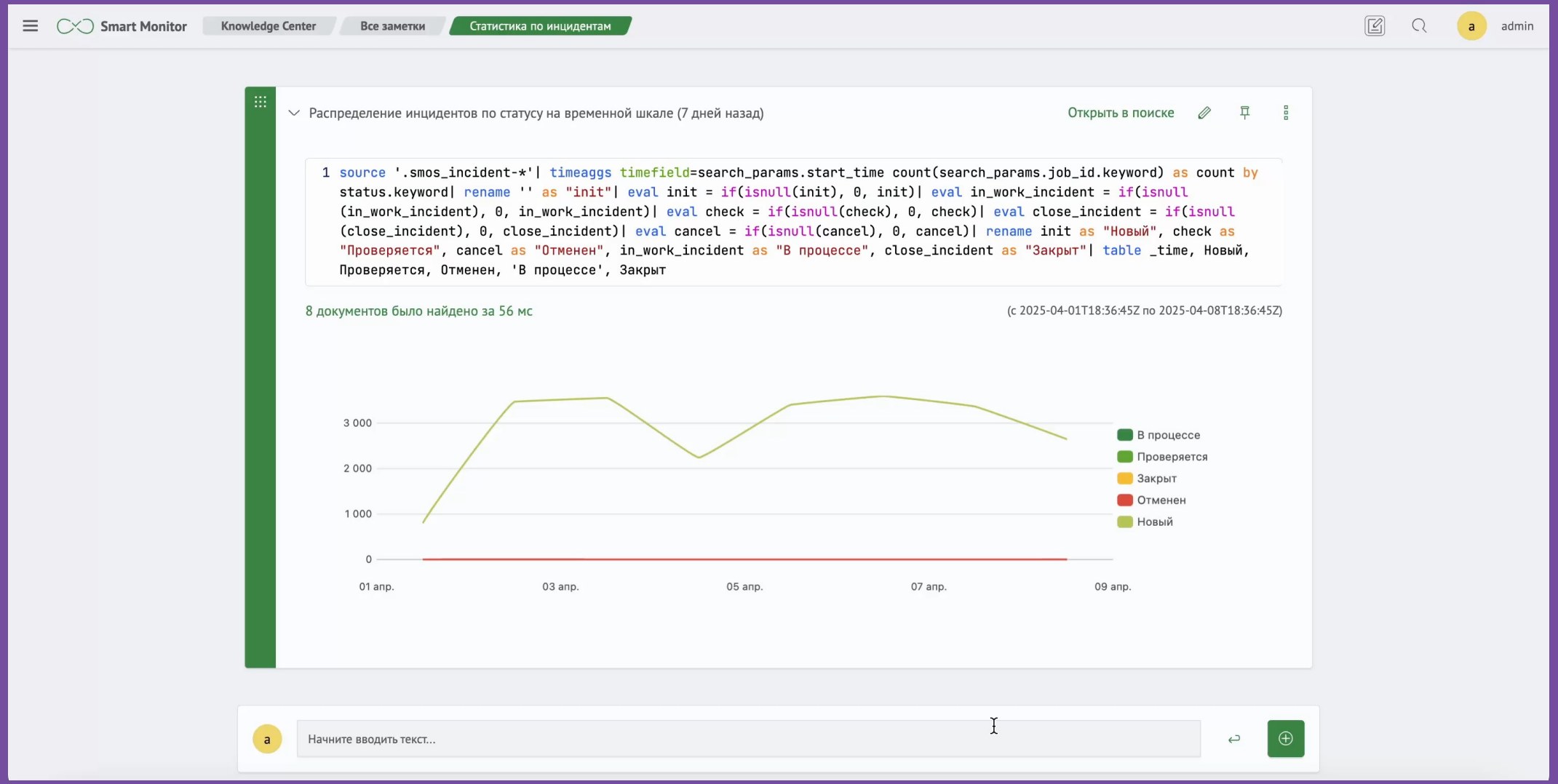
Пример расследования



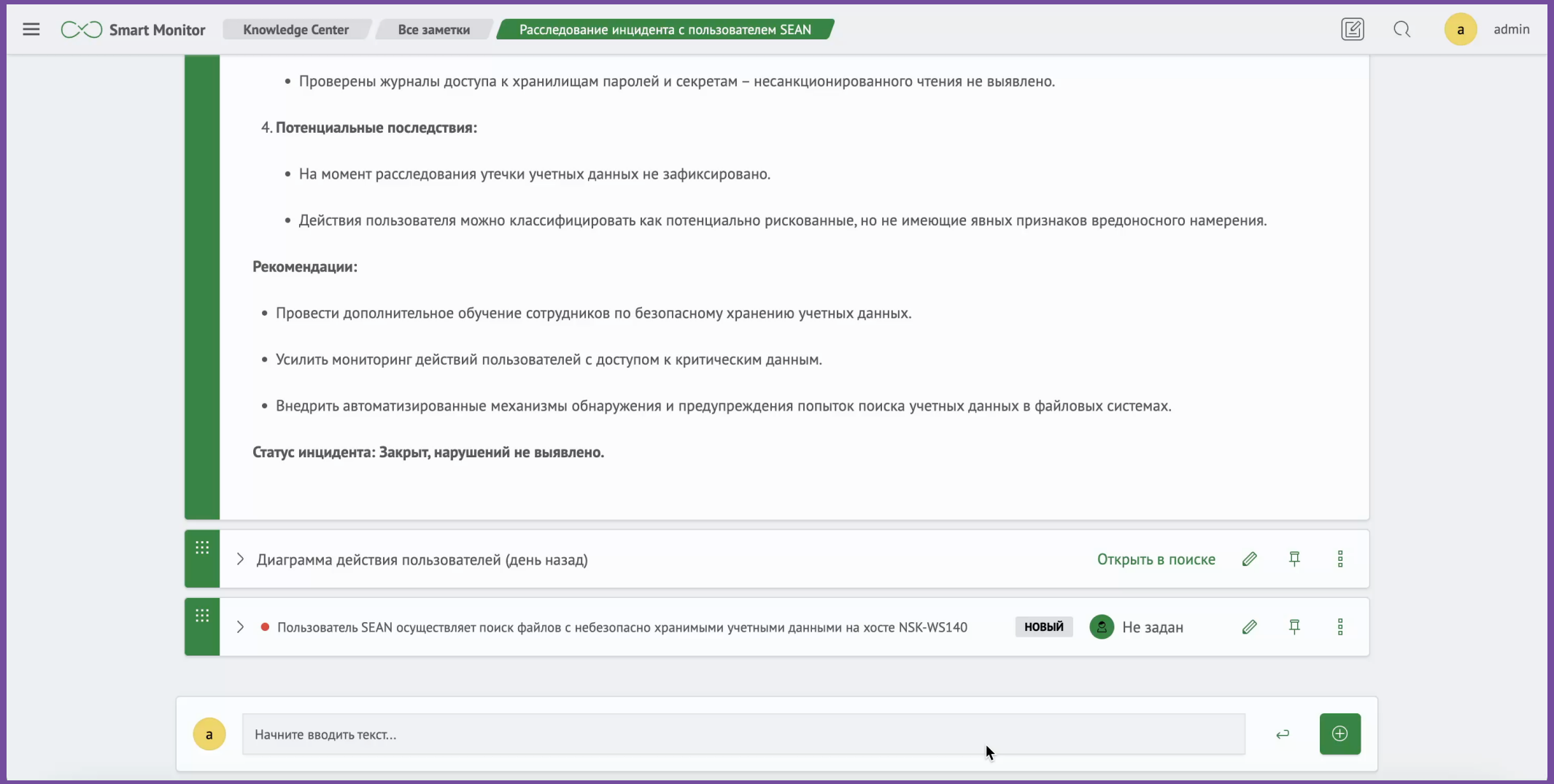
Различные блоки: инцидент



Различные блоки: поиск

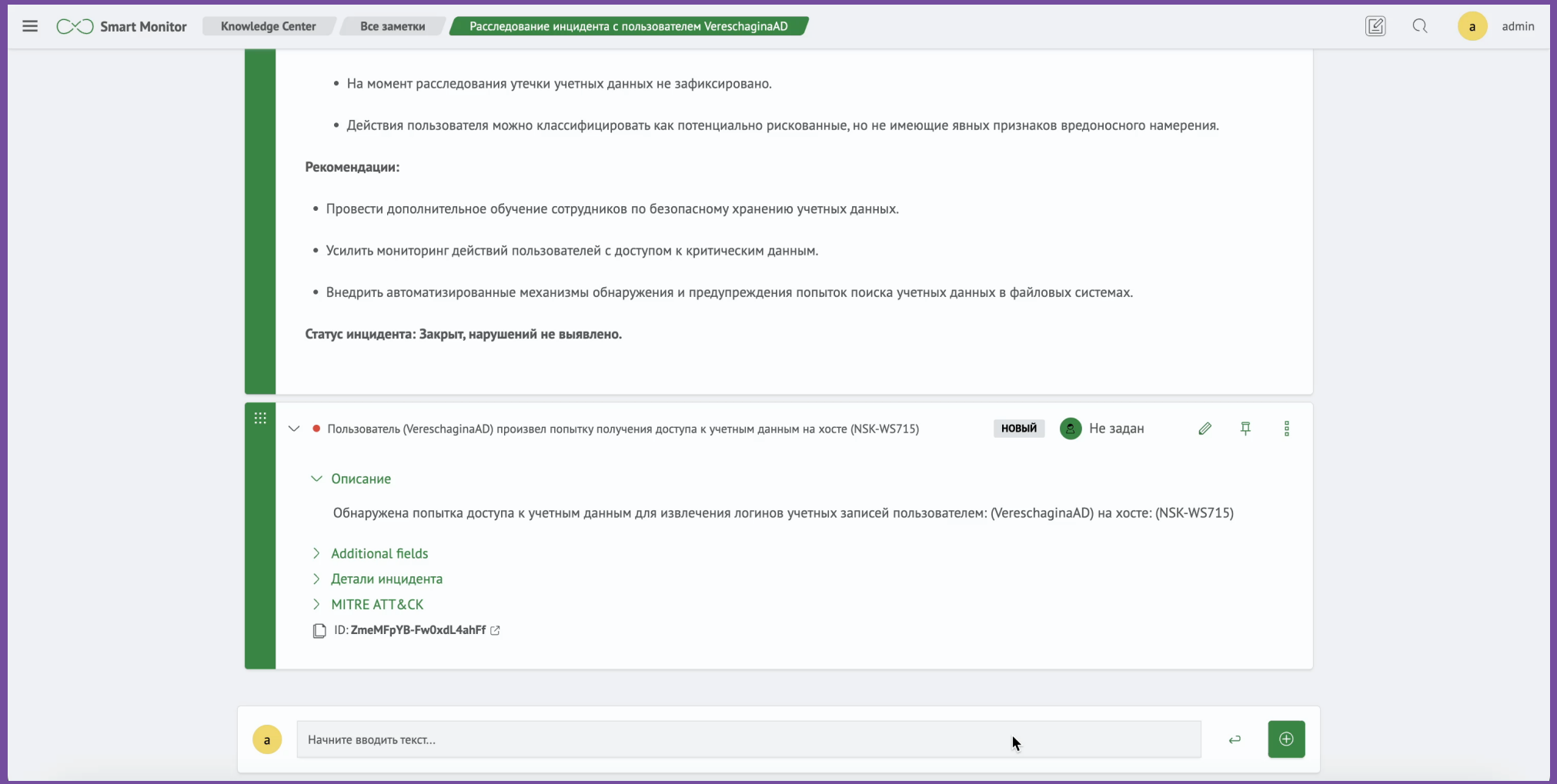


Различные блоки: текст

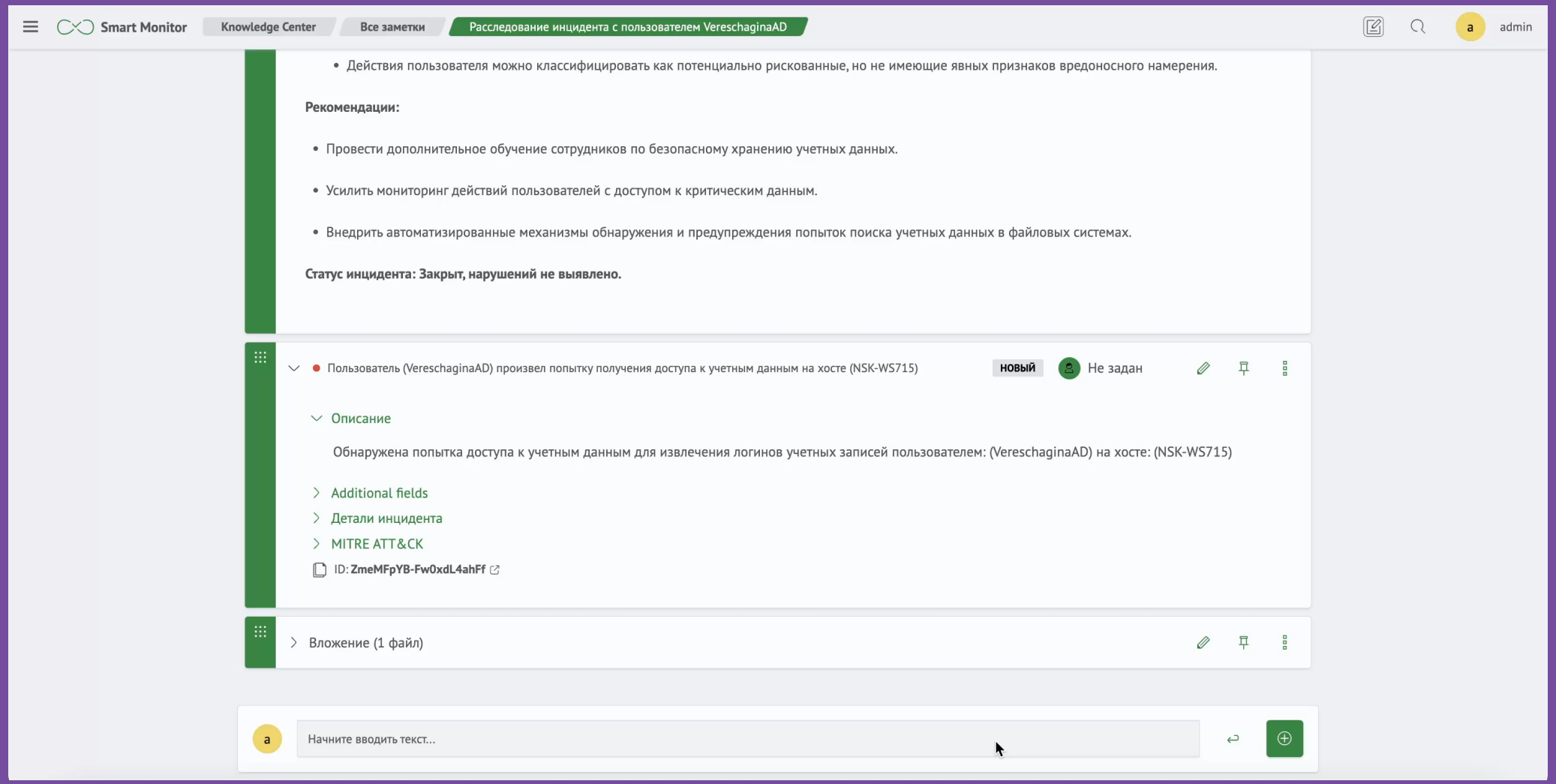


VolgaBlob

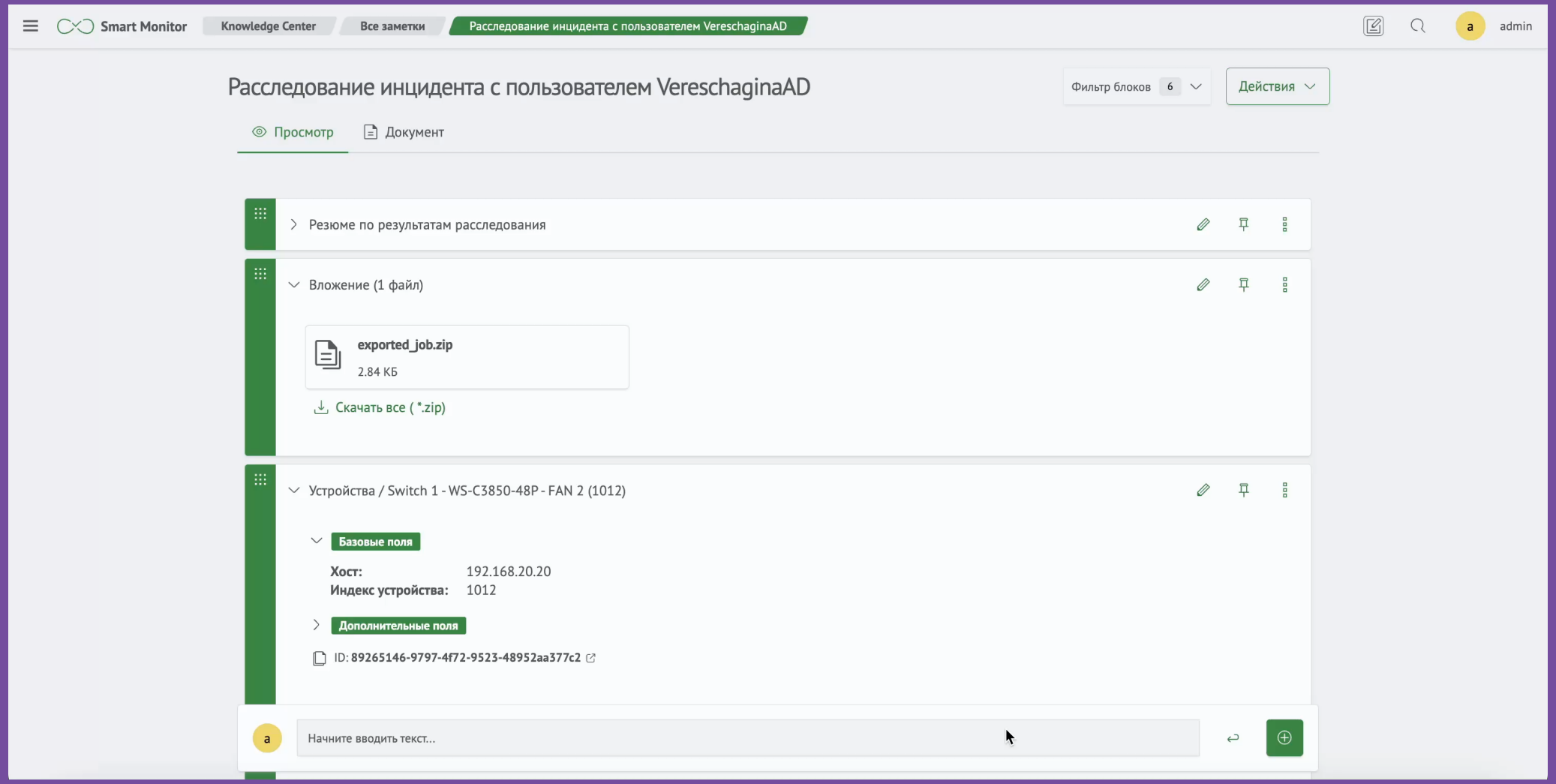
Различные блоки: файлы и изображения



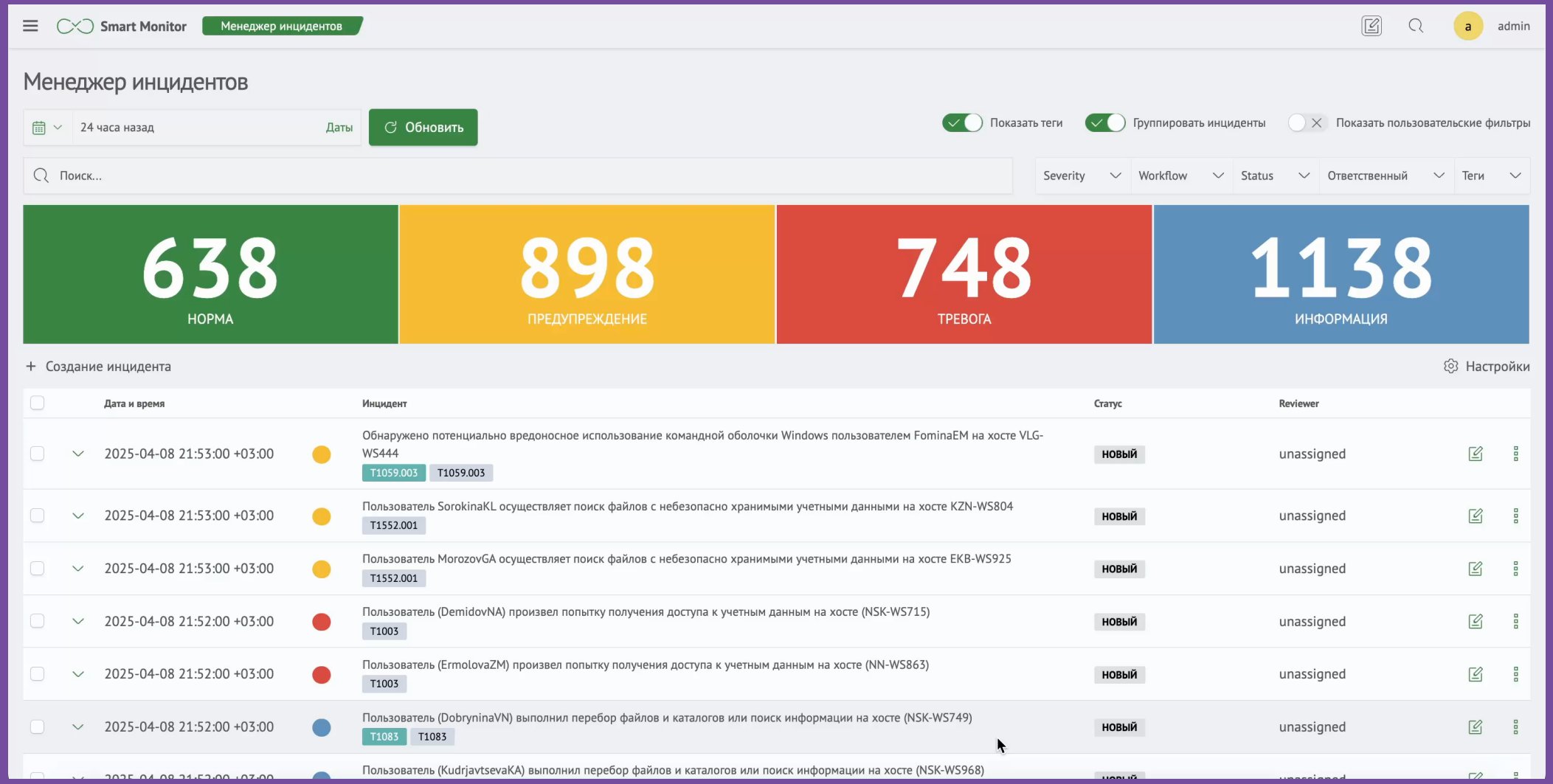
Различные блоки: актив



Статический режим

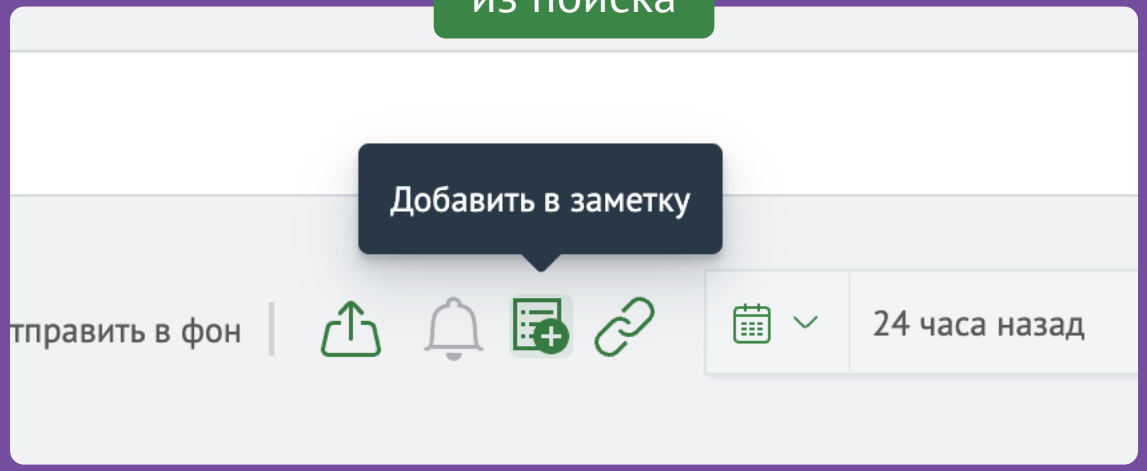


Создание быстрой заметки:

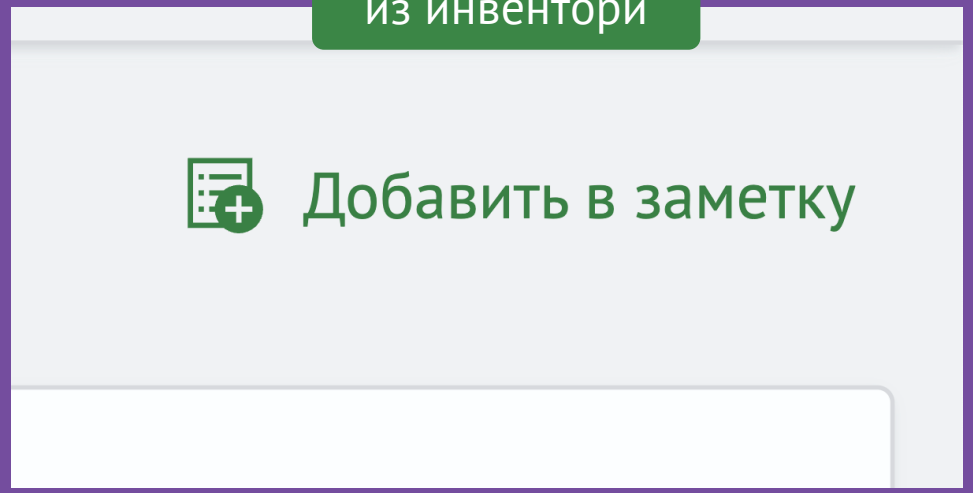


Создание из разных мест интерфейса

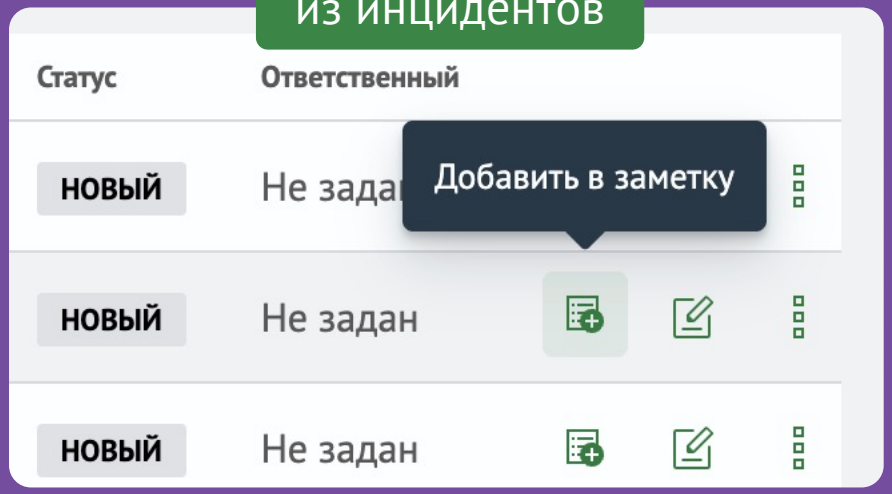
из поиска



из инвентори



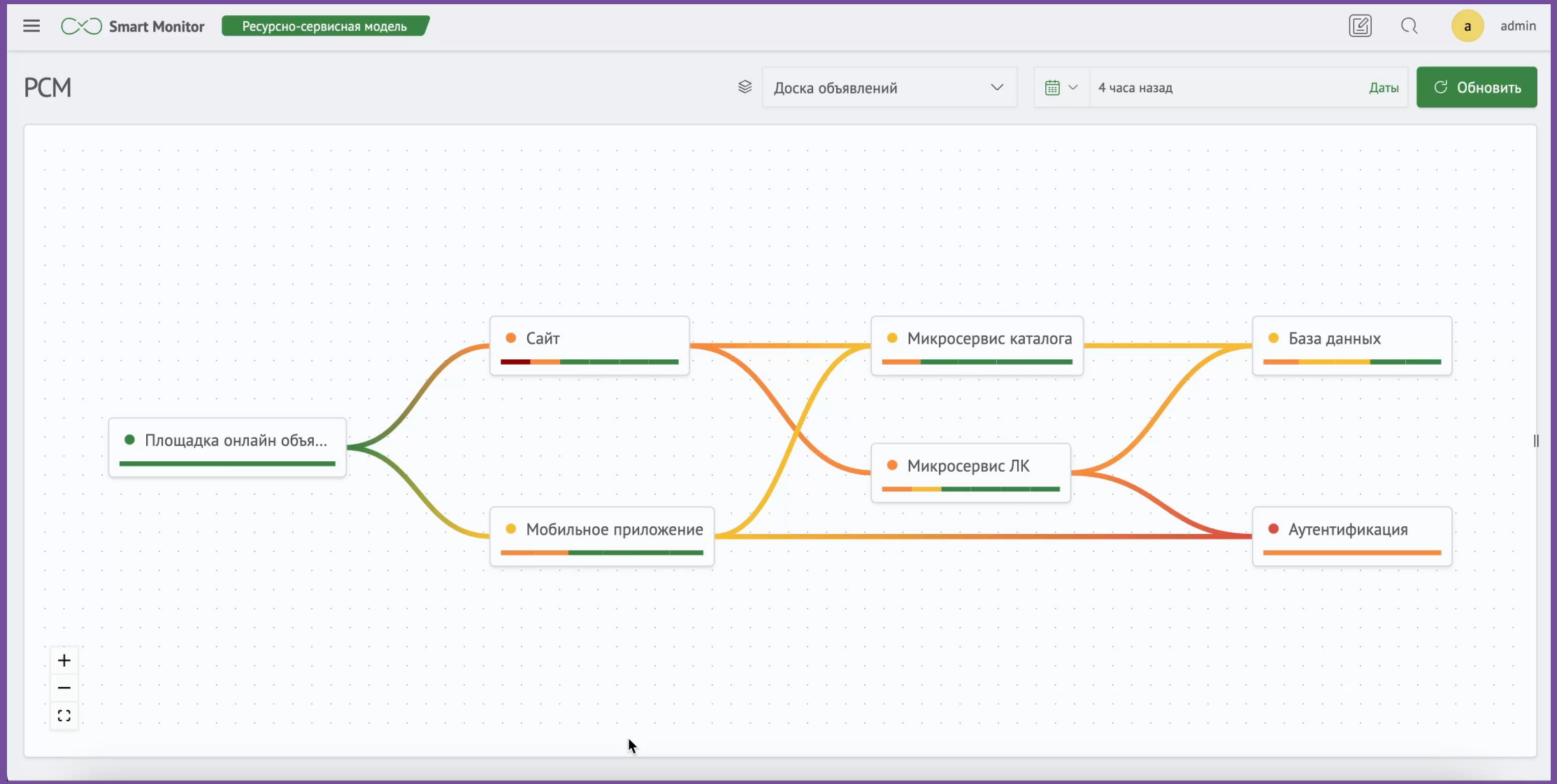
из инцидентов



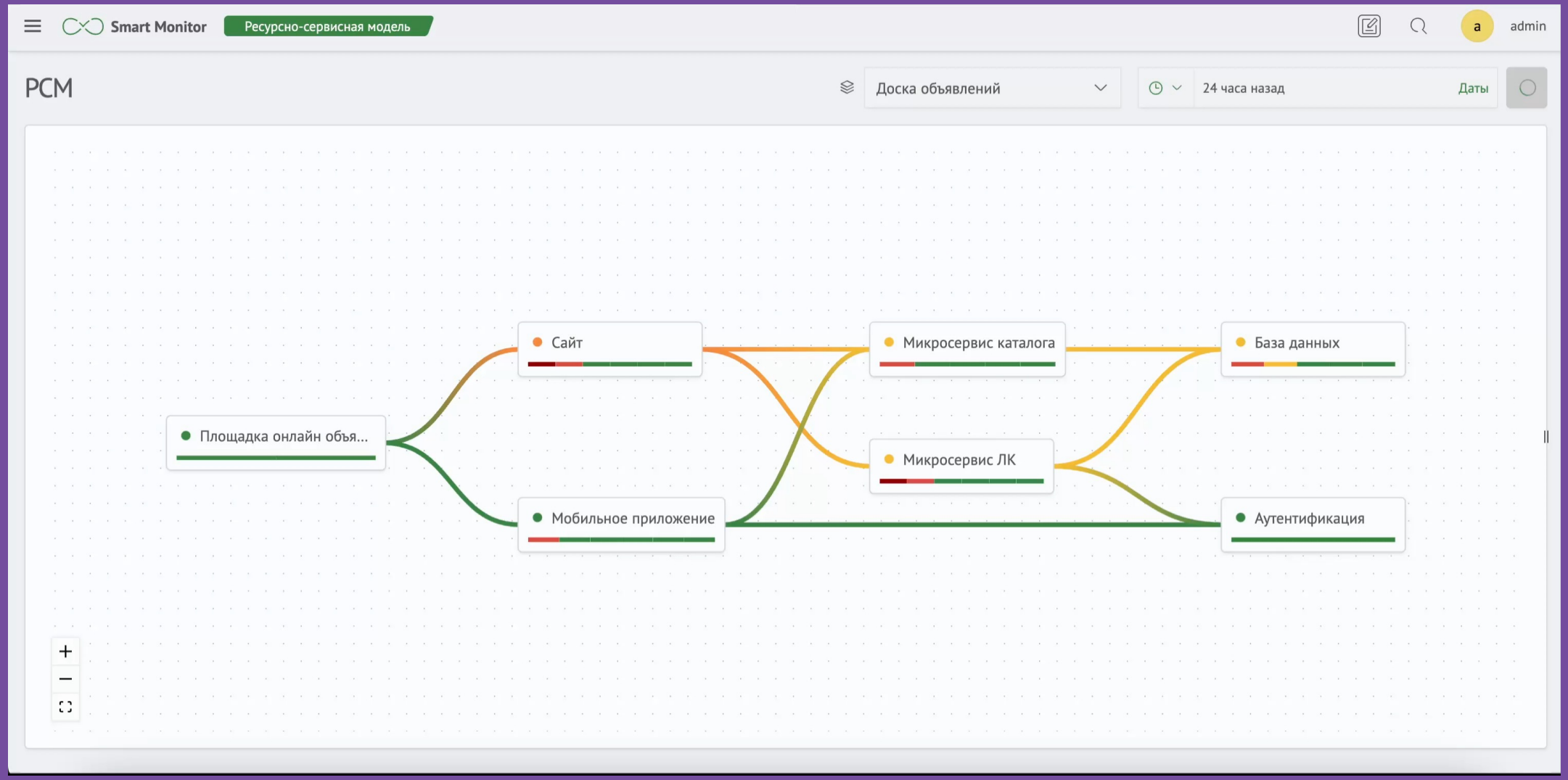
VolgaBlob

Ресурсно-сервисная модель 2.0

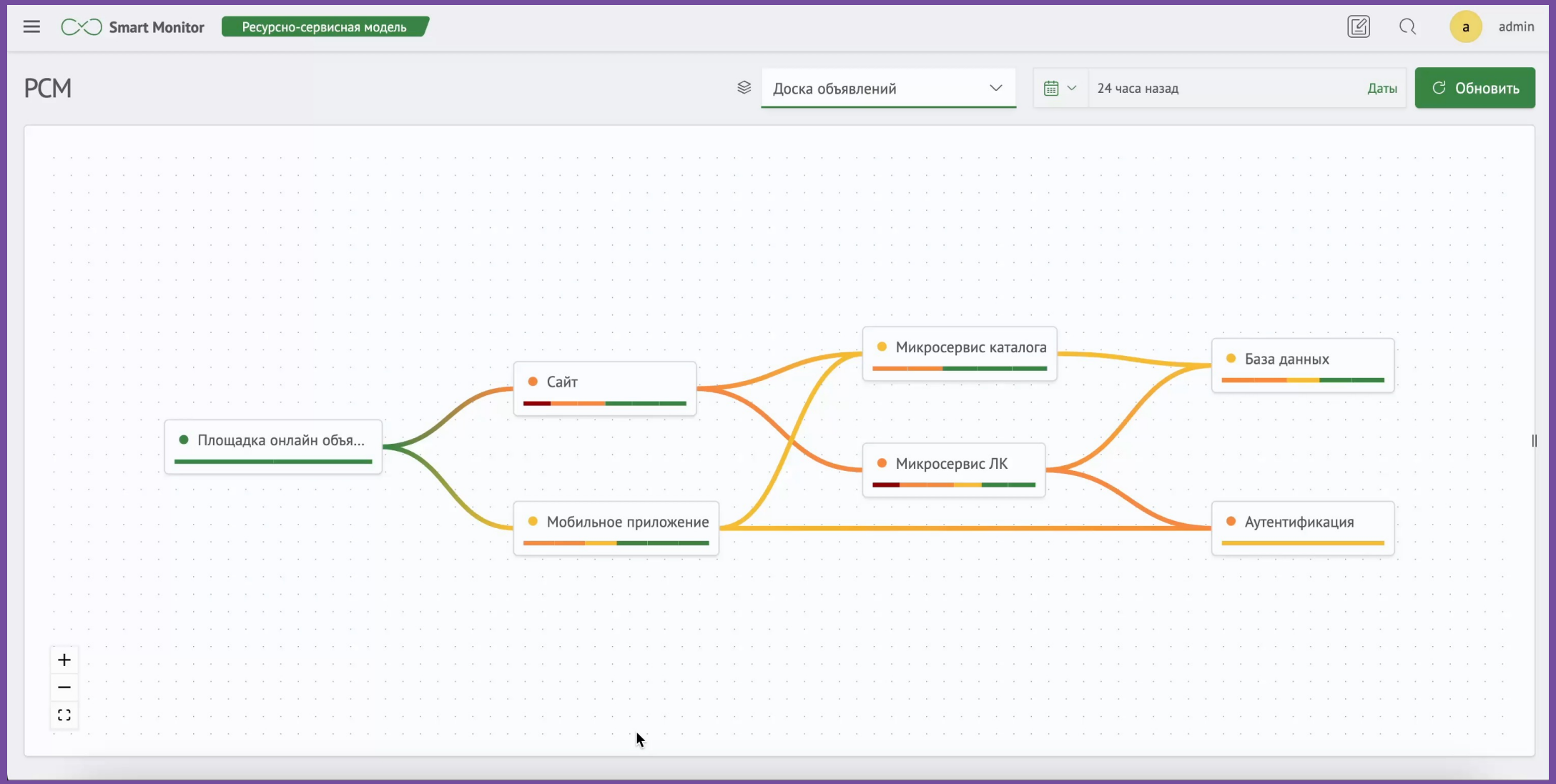
Новое представление графа



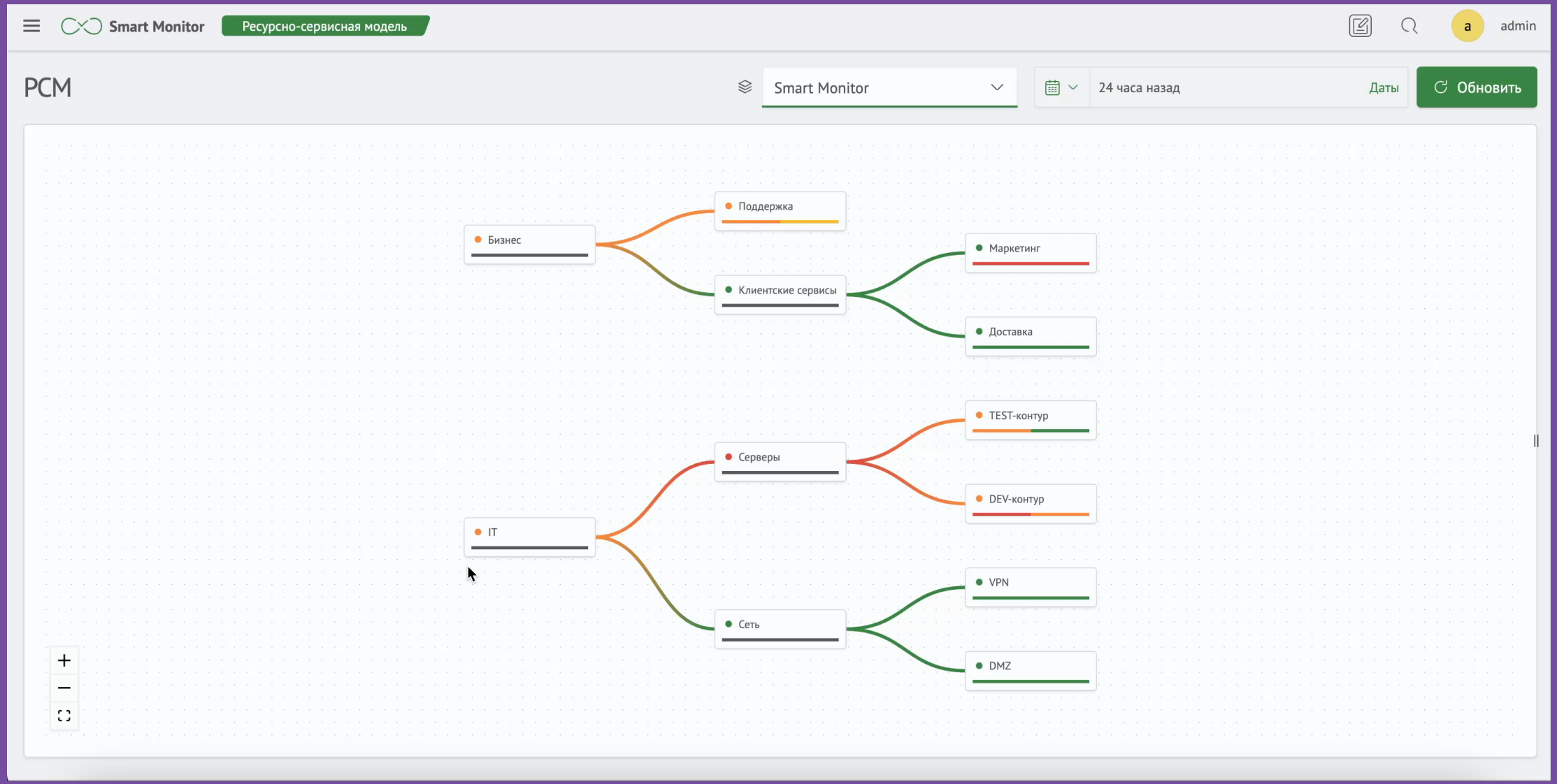
Автообновление



Несколько компонент связанности, слои



Представление блоками



PCM 2.0 – это начало бОльшего модуля

ITSM

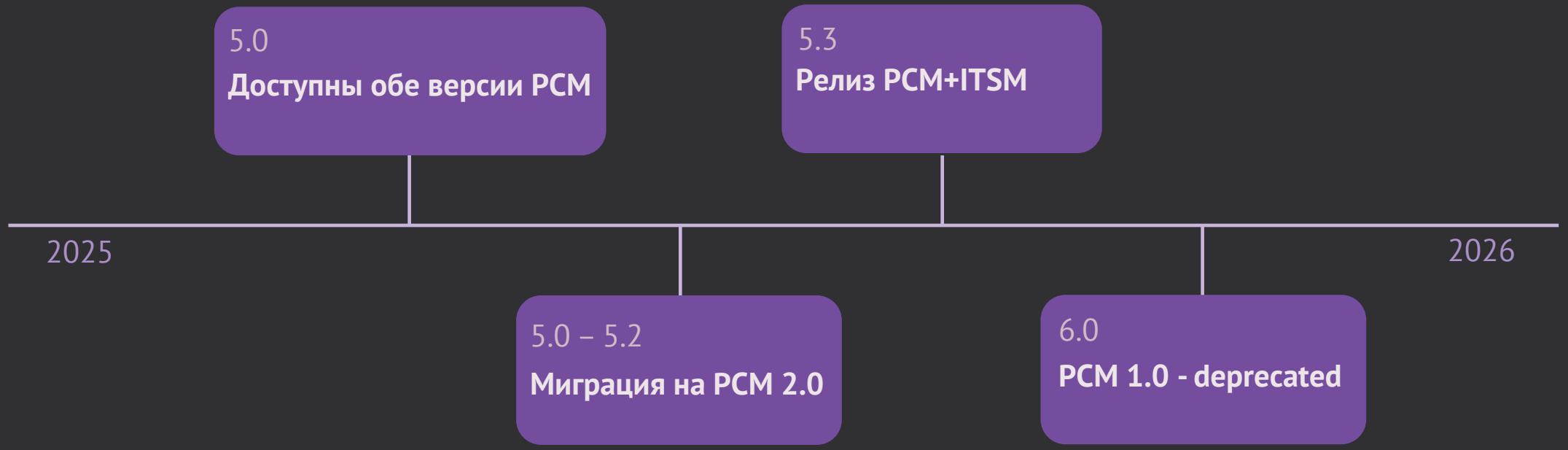
PCM (CORE)

- Полностью новый интерфейс
- Возможность построения графа
- Слои
- Несколько компонент связанности
- Аналитика сервисов, метрик

- Автогенерируемые деревья/графы
- Определение здоровья сервиса на основе ML
- Готовые шаблоны сервисов и метрик
- Интеграция с модулем Inventory
- Интеграция с модулем Incident Manager

И многое другое...

Одновременная работа PCM 1.0 и 2.0



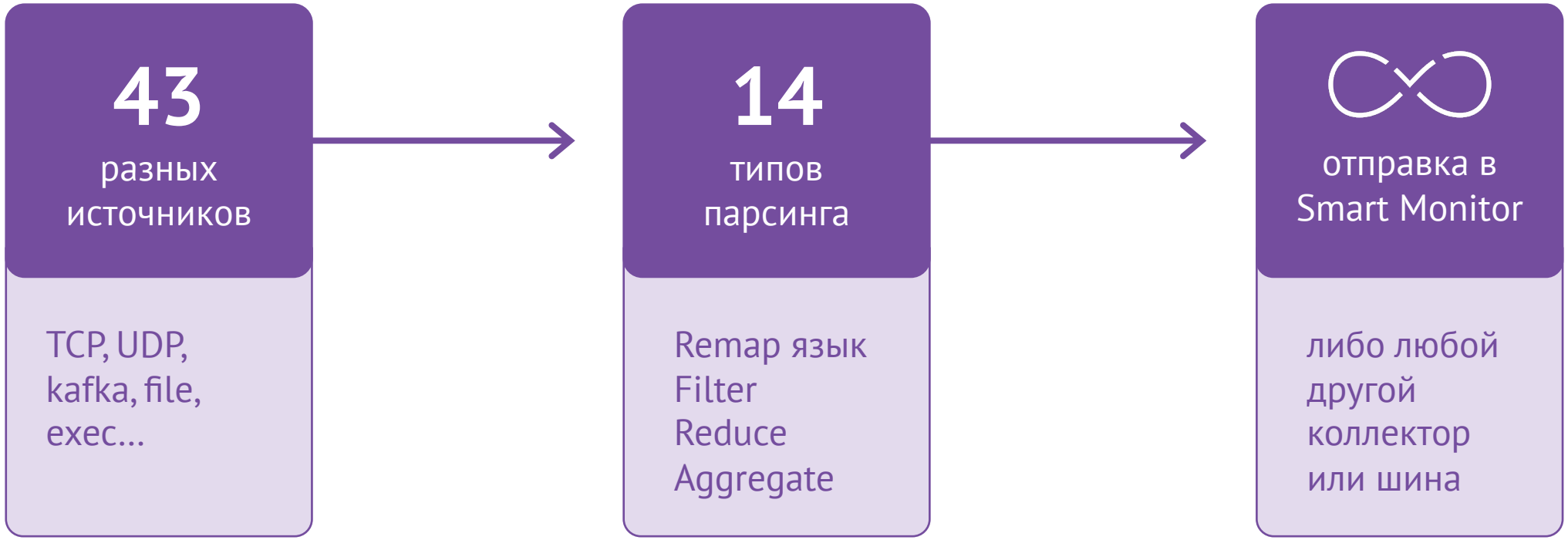
Smart Beat: Vector

Vector

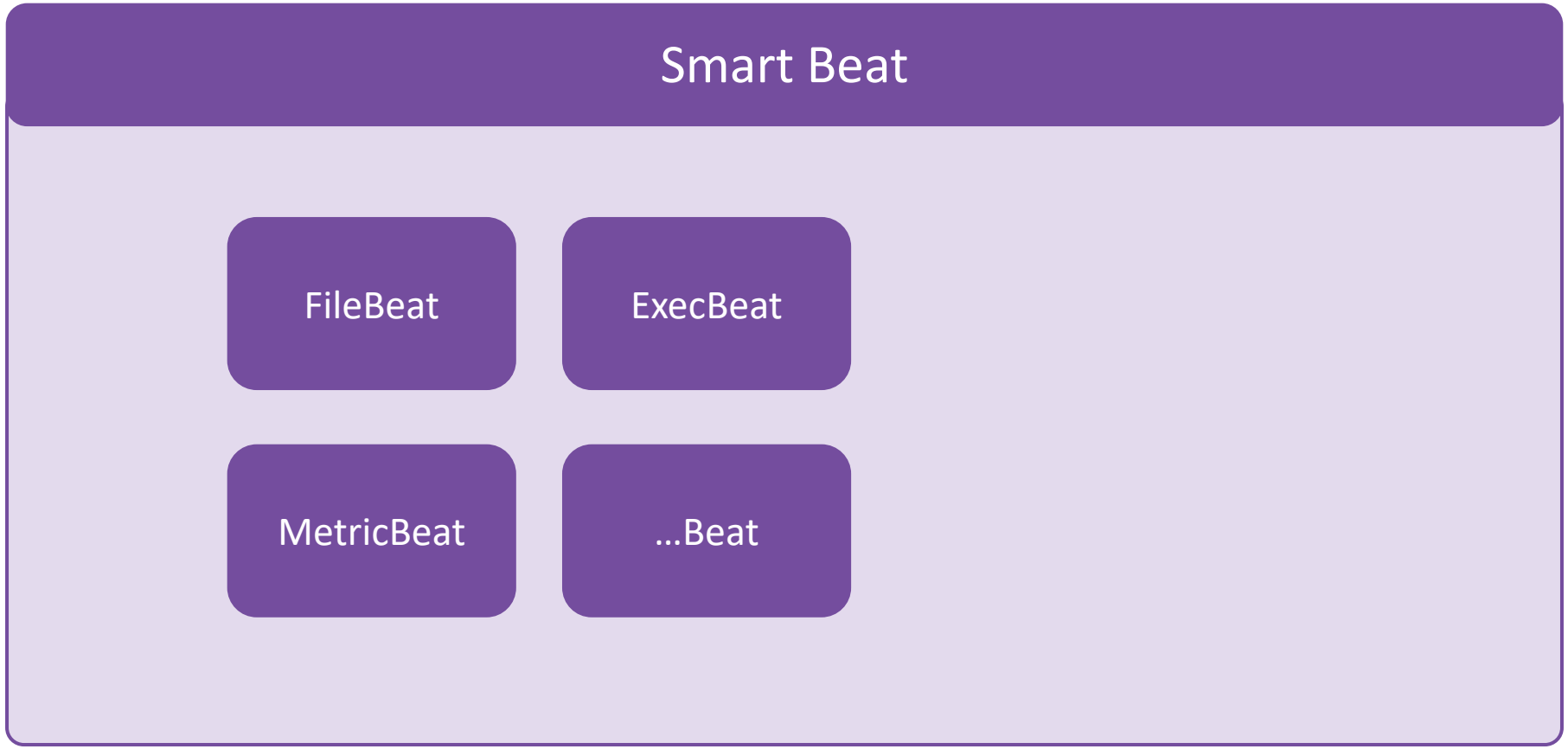
Vector – инструмент для сбора, преобразования и отправки данных логов, метрик и событий

- Потребляет минимальное количество ресурсов благодаря эффективному управлению памятью
- Может обрабатывать до 30ТБ в сутки
- От 10 до 30 раз быстрее конкурентов (beats, logstash, fluentbit) в отдельных случаях

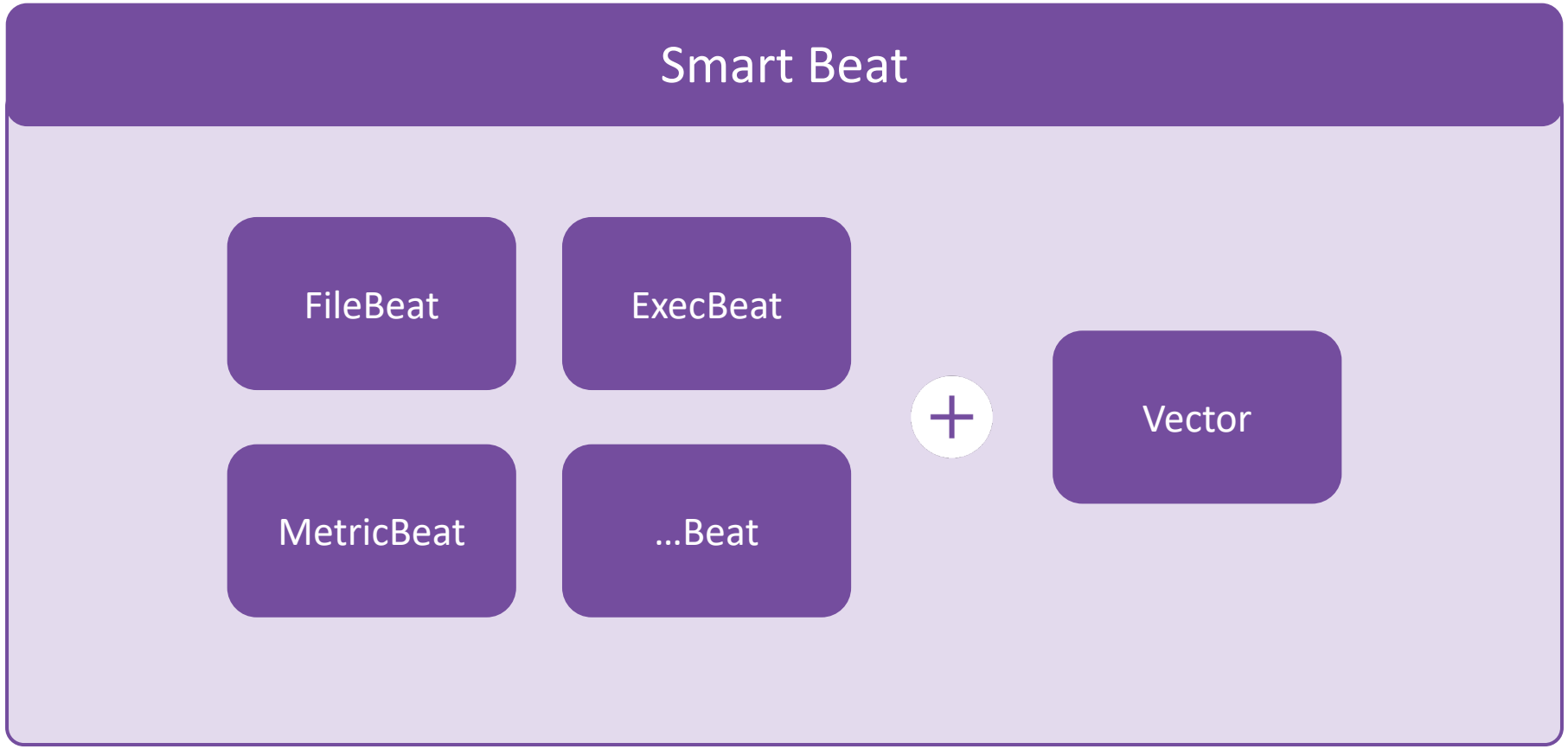
Vector


43
разных
источников
TCP, UDP,
kafka, file,
exec...
14
типов
парсинга
Remap язык
Filter
Reduce
Aggregate
отправка в
Smart Monitor
либо любой
другой
коллектор
или шина

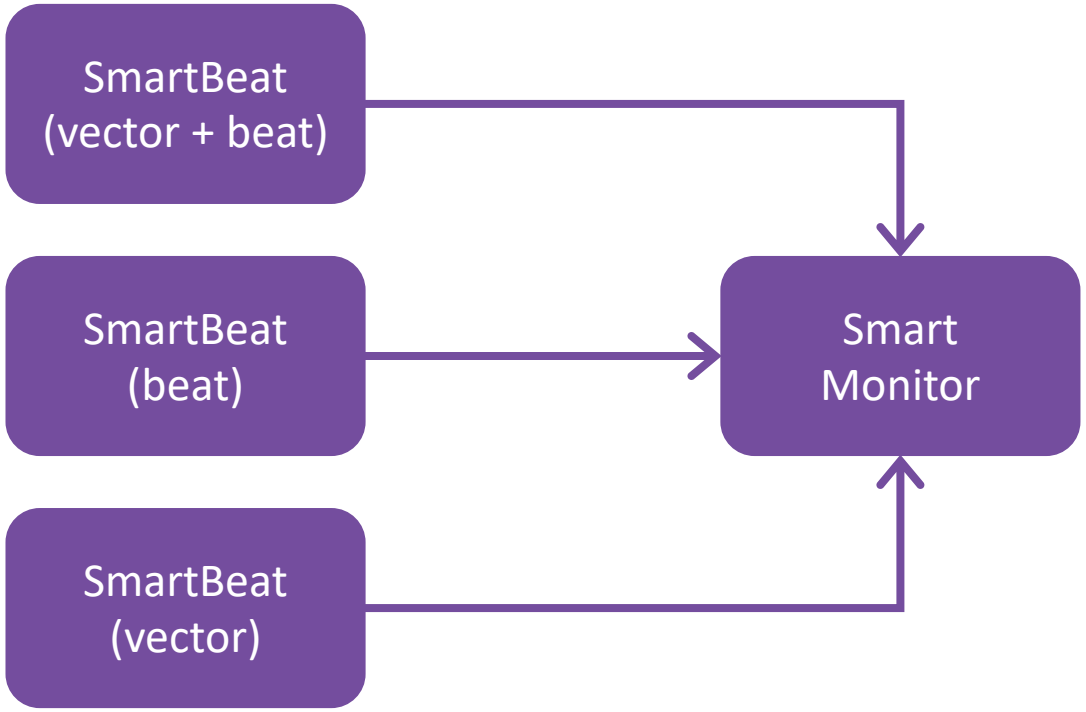
Smart Beat как агрегатор



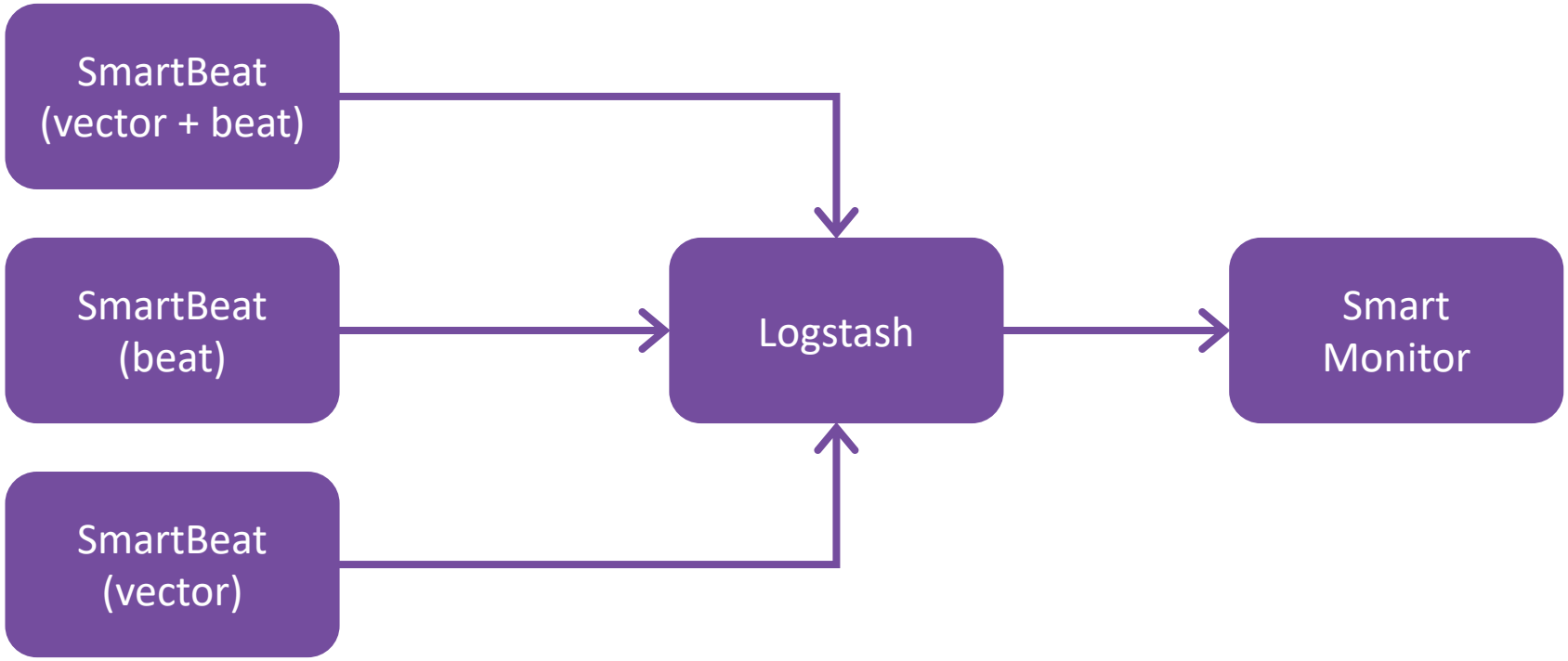
Smart Beat как агрегатор



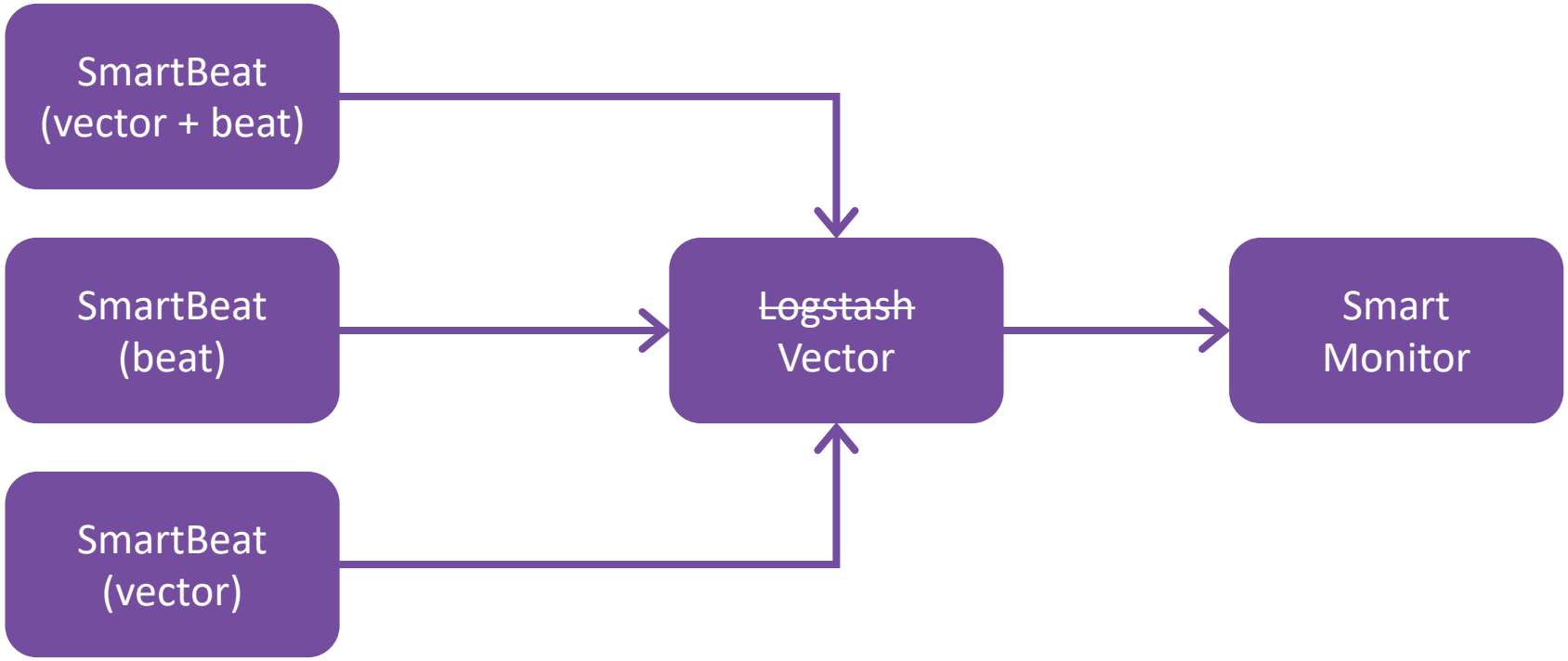
Архитектура сбора



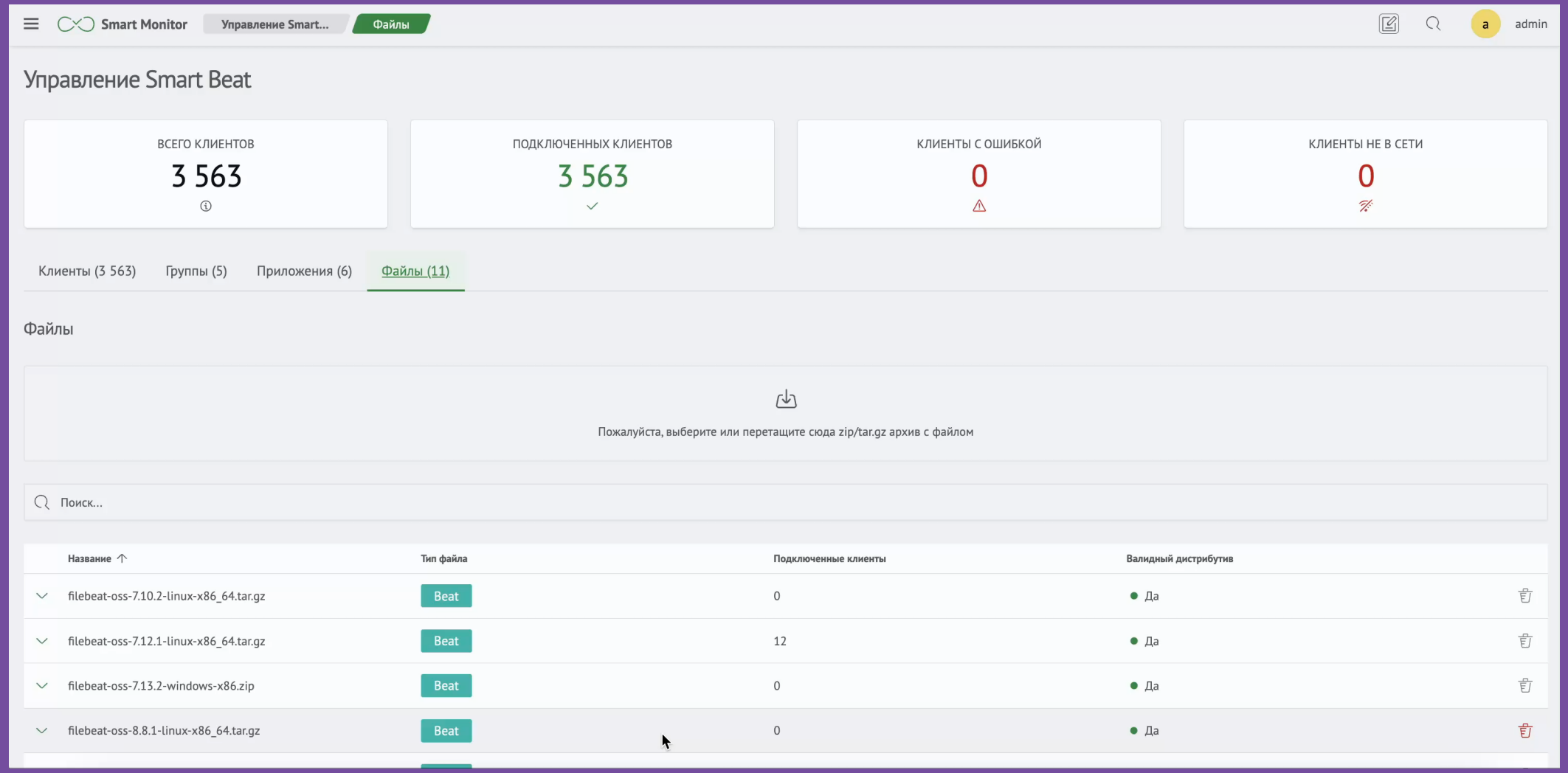
Архитектура сбора



Архитектура сбора



Возможность управления всеми конфигами в интерфейсе



VolgaBlob

Выбор решения

- \+ High Perfomance
- \+ Трансформация логов прямо на агенте
- \+ Ограниченное количество ресурсов RAM < 1ГБ
- \+ Мониторинг Docker, Kubernetes
- \+ Нужен только один инструмент в инфраструктуре
- — Сбор Windows Event Logs
- — Нужно большое количество интеграций (inputs, sink)
- — Простота конфигурации на агенте, готовые модули
- — Сложные и «условные» пайплайны
- — Сбор БД, API, LDAP

Новые визуализации

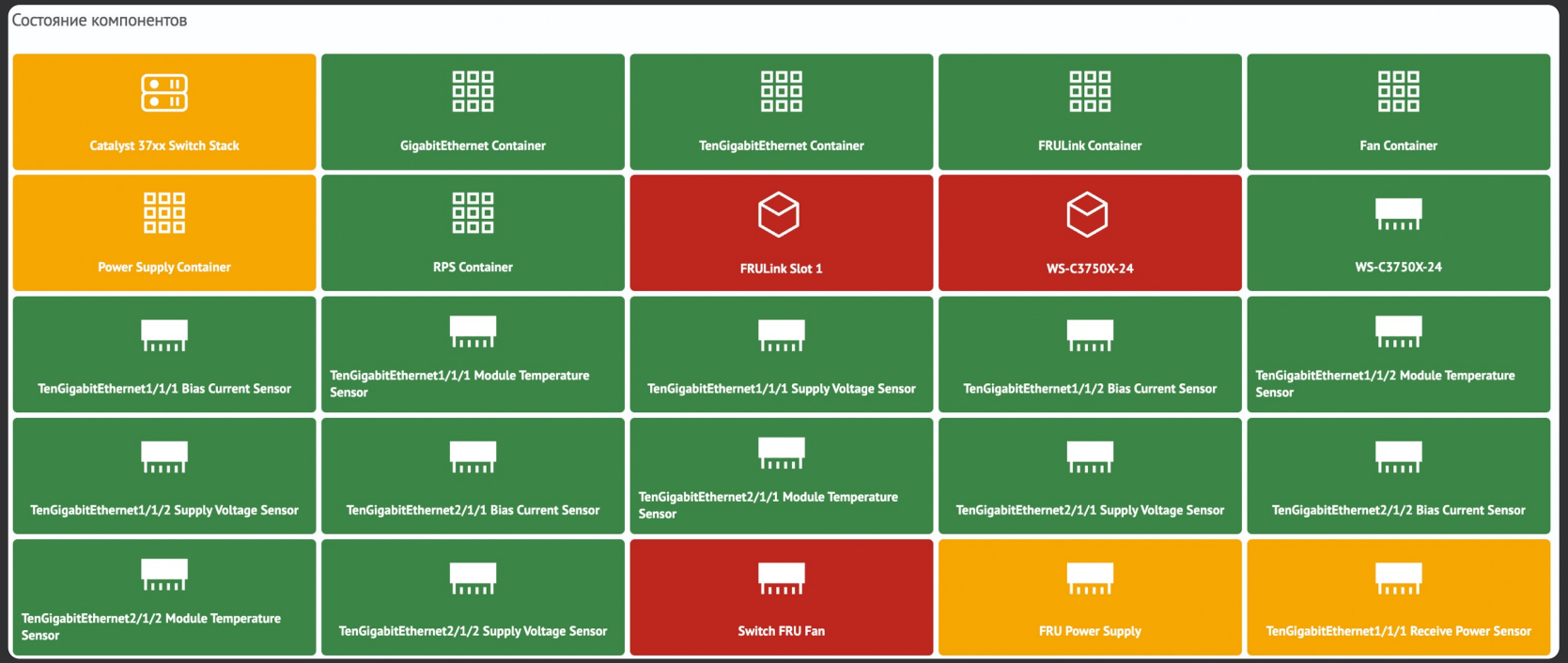
Визуализация Quick State

Feature Request от заказчика

Запрос один – метрик много!

Можно настроить:

- Иконки
- Цвет
- Размер сетки
- Высоту ячейки
- Drilldown по клику



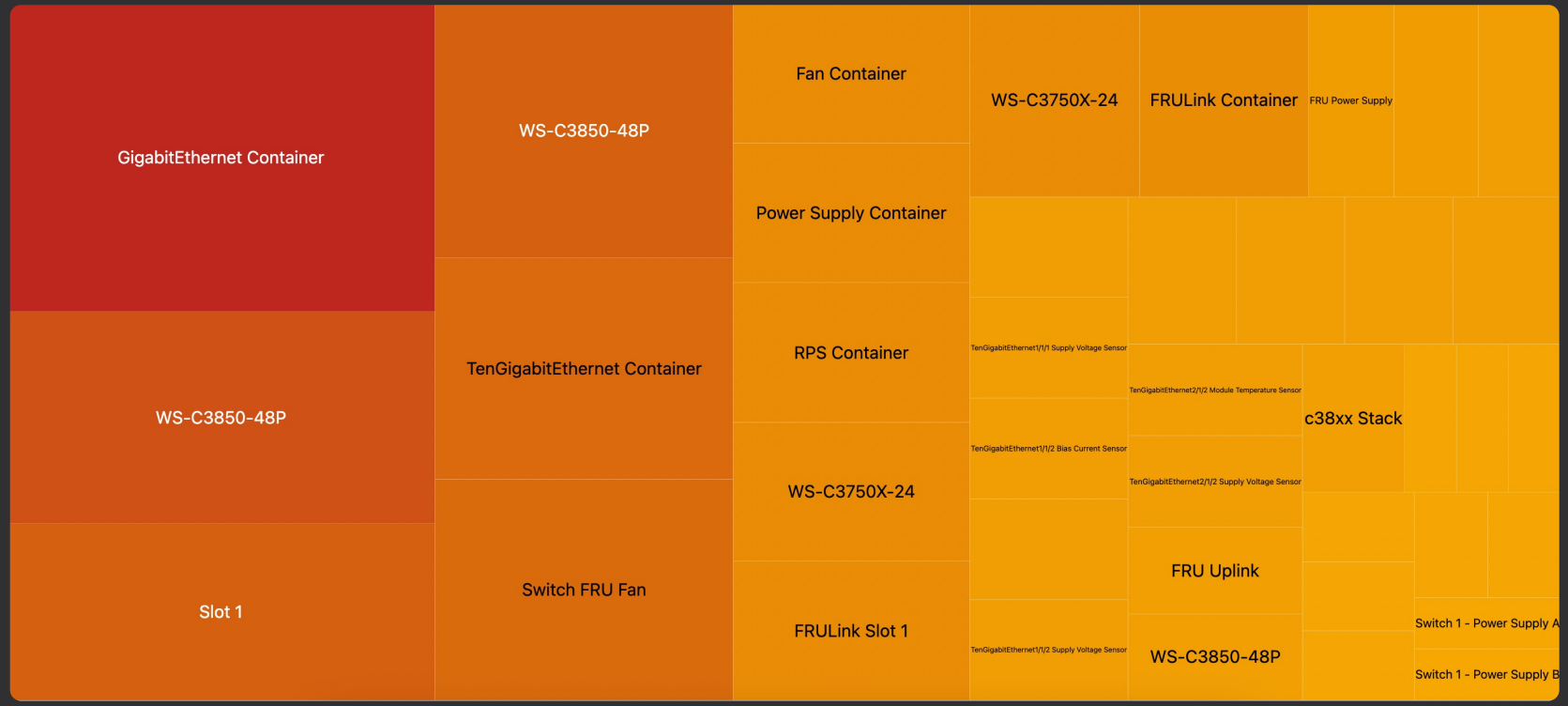
VolgaBlob

Визуализация TreeMap

Feature Request от заказчика

Можно настроить:

- цвет «от» и «до»
- алгоритмы расположения
- отступы
- сортировка



Machine Learning в поисковом движке

Команды Machine Learning в поисковом движке

Реализованы команды train и predict для обучения моделей и их использования

Команда train

Выполняет обучение модели на входных данных. Результатом команды является идентификатор модели, который можно использовать в команде predict.

SML Syntax

```
| train <algorithm> [<params>]
<input_fields>
```

Команда predict

Выполняет предсказание на основе обученной модели и входных данных.

SML Syntax

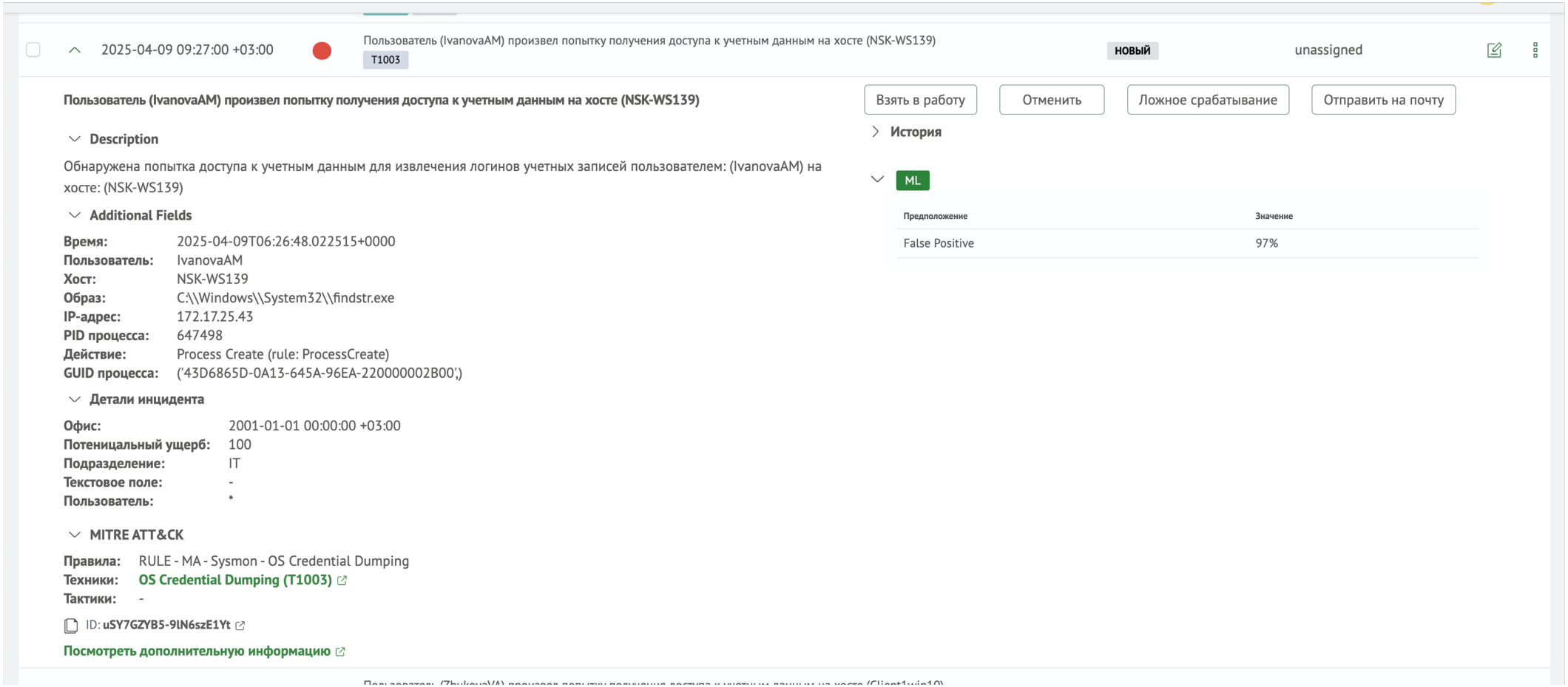
```
| predict <algorithm> <model_id>
<input_fields>
```

Доступные алгоритмы Machine Learning

На данный момент Smart Monitor поддерживает следующие алгоритмы обучения:

- Kmeans;
- Linear Regression;
- RFC;
- RFC Summarize;
- Localization;
- Logistic Regression;
- Metrics Correlation.

Интеграция ML в модуль Менеджер инцидентов



Улучшения в поиске

Небольшие, но полезные изменения

Подсветка

При выделении строки в запросе, подсвечиваются другие совпадающие строки

Сайдбар

Отображение наиболее используемых полей

search in

Функция in упрощает написание запросов с поиском по нескольким значениям

search, кавычки, AND

Кавычки для значений можно опустить
Оператор AND по умолчанию

Макросы

Большие части запроса теперь могут быть вызваны аналогично функции с аргументами

Cyber Security: SIGMA правила

Что такое Sigma?

Sigma – это унифицированный формат описания правил детектирования, основанных на данных из логов.

Правила хранятся в отдельных YAML-файлах

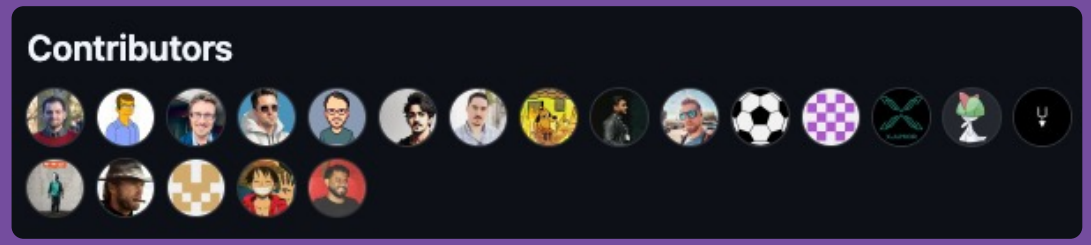
```yaml
title: Suspicious PowerShell Execution
description: Detects PowerShell with encoded commands
logsource:
  product: windows
  category: process_creation
detection:
  selection:
    Image: "*\powershell.exe"
    CommandLine: "* -EncodedCommand *"
  condition: selection
falsepositives:
  - Legitimate administrative scripts
level: high
tags:
  - attack.execution
  - attack.t1059.001
```

Sigma


> 3000 правил
Generic
Общие правила, для обнаружения техники или процедуры
Threat Hunting
Потенциальные подозрительные или вредоносные действия
Emerging Threat
Конкретные угрозы, APT кампании, Zero-day, конкретное вредоносное ПО

Sigma

Sigma репозиторий постоянно
наполняется и обновляется,
не смотря на то что это Open Source



Release r2025-02-03 Latest

New Rules

- new: Azure Login Bypassing Conditional Access Policies
- new: CVE-2024-49113 Exploitation Attempt - LDAP Nightmare
- new: Suspicious Binaries and Scripts in Public Folder
- new: Suspicious Invocation of Shell via Rsync
- new: Windows Event Log Access Tampering Via Registry

Updated Rules

- update: Exploit Framework User Agent - Add default Havoc C2 UA
- update: Renamed Powershell Under Powershell Channel - Update regex to use `\s+` to account for different parsers
- update: Shell Execution via Rsync - Linux - Rework logic to make it more generic and include additional shells.
- update: Suspicious Non PowerShell WSMAN COM Provider - Update regex to use `\s+` to account for different parsers
- update: Suspicious Windows Service Tampering - Add additional services

Removed / Deprecated Rules

- remove: Windows Defender Exclusion Deleted

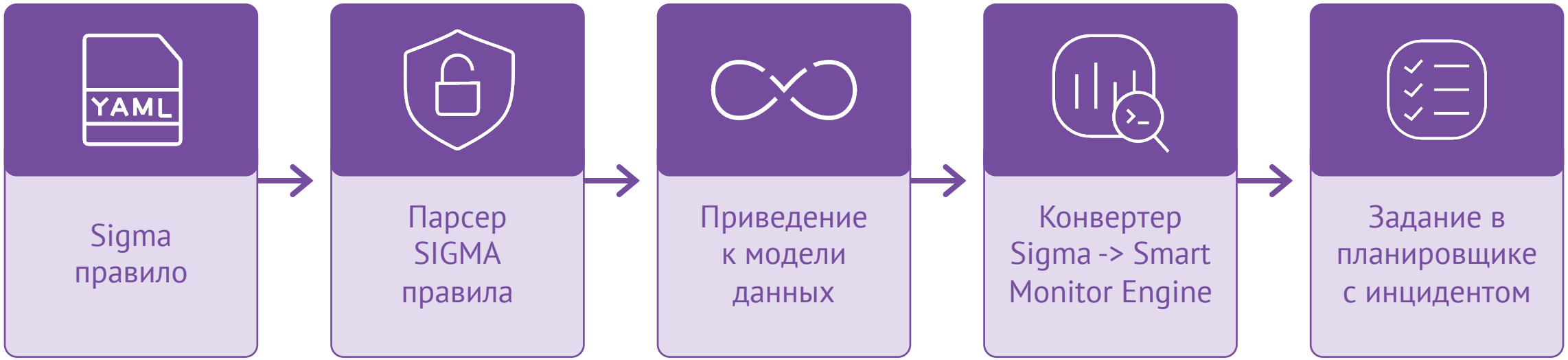
Fixed Rules

- fix: BITS Transfer Job With Uncommon Or Suspicious Remote TLD - Add `dn.onenote.net/` and `cdn.office.net/`
- fix: CodeIntegrity - Unmet Signing Level Requirements By File Under Validation - Add filter for `Kaspersky` and `mDNS Responder`
- fix: Failed Code Integrity Checks - Add filters for `CrowdStrike`.

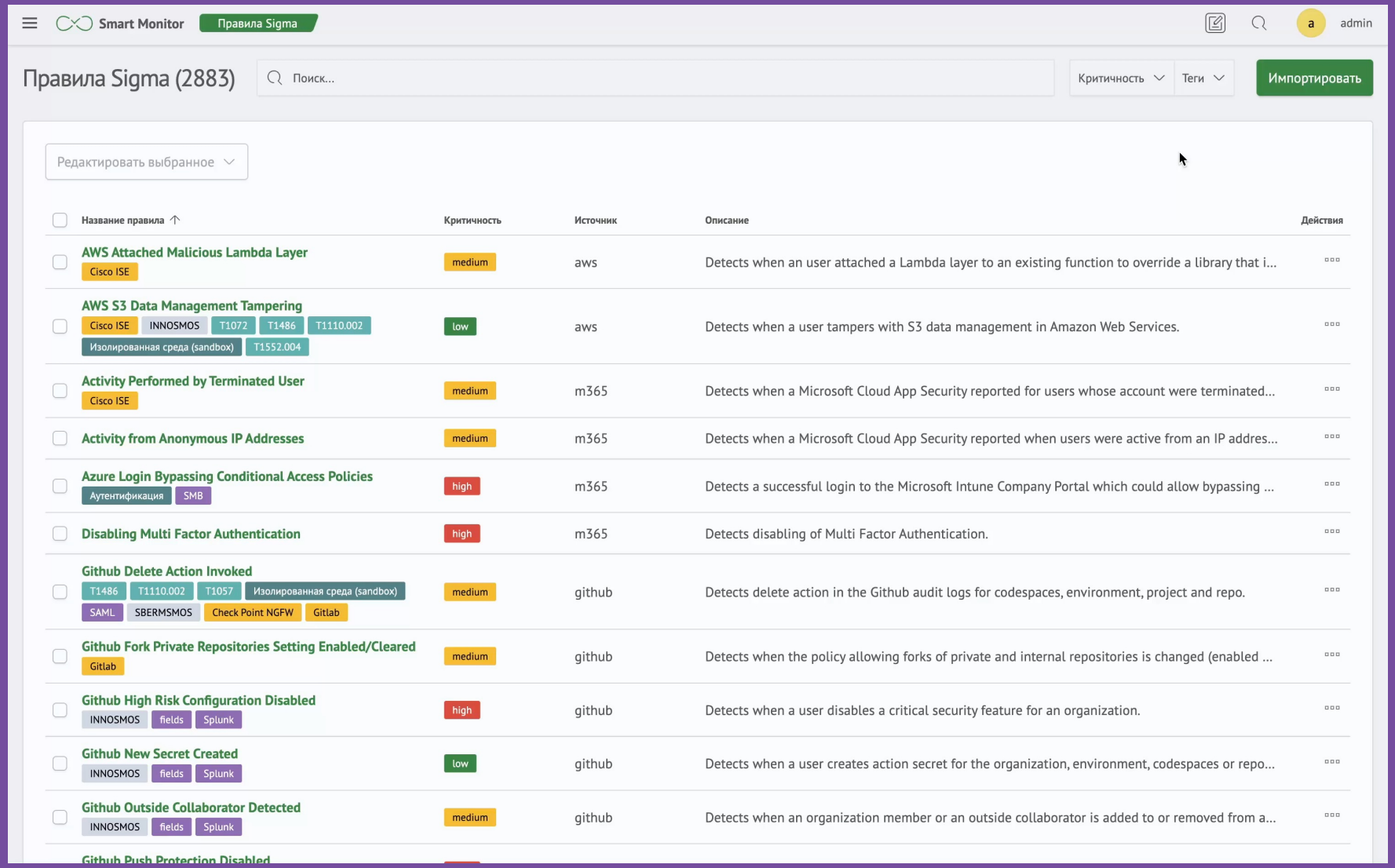
Теперь в Cyber Security **на 3000+ правил больше!**

Но мы пошли дальше...

Cyber Security: мастер импорта Sigma



Cyber Security: мастер импорта Sigma



Inventory

Важность связей

Наглядность

Визуальное представление взаимодействия активов друг с другом

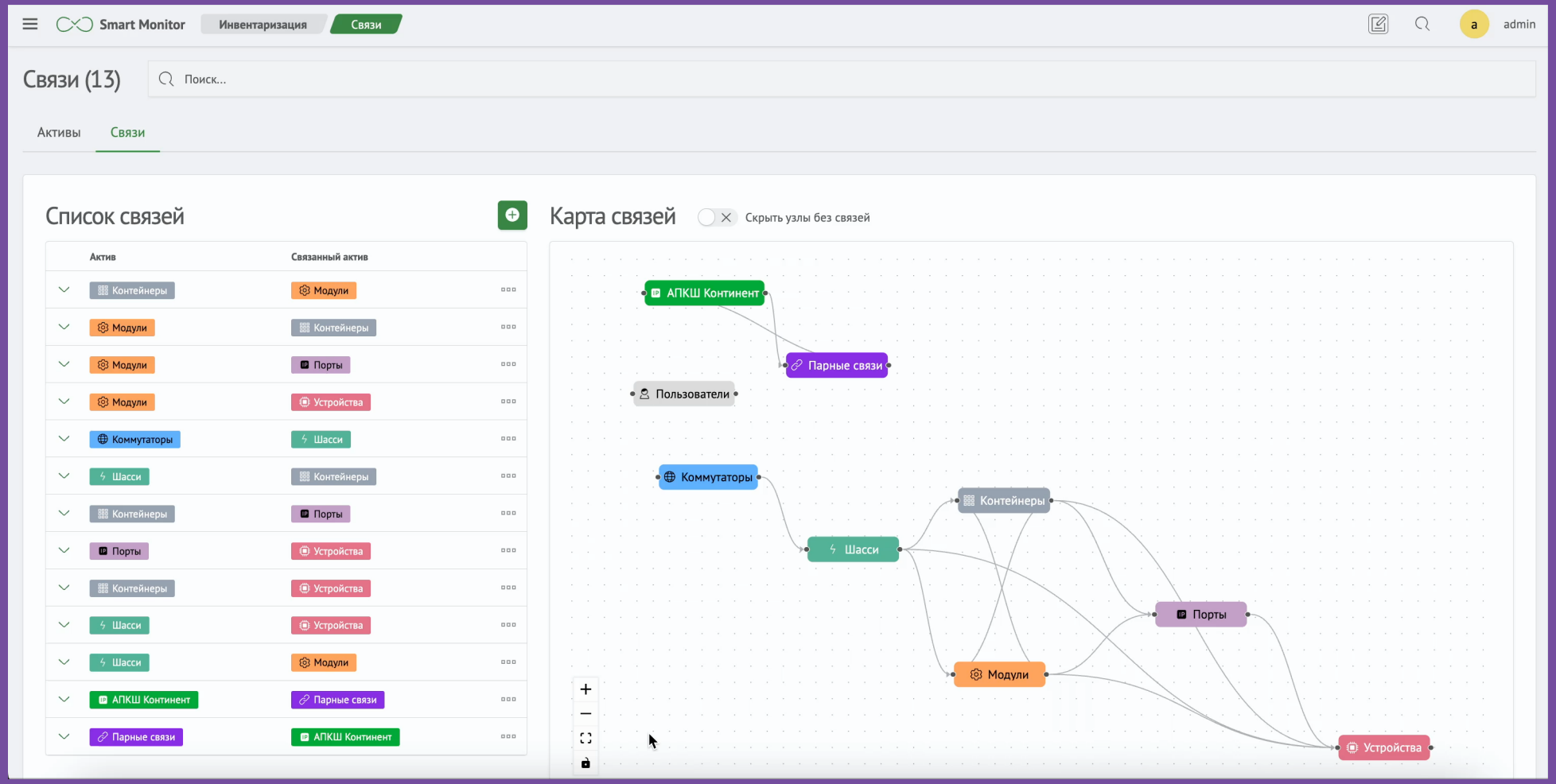
Прогноз

Выявление уязвимых активов при потенциальных связанных сбоях

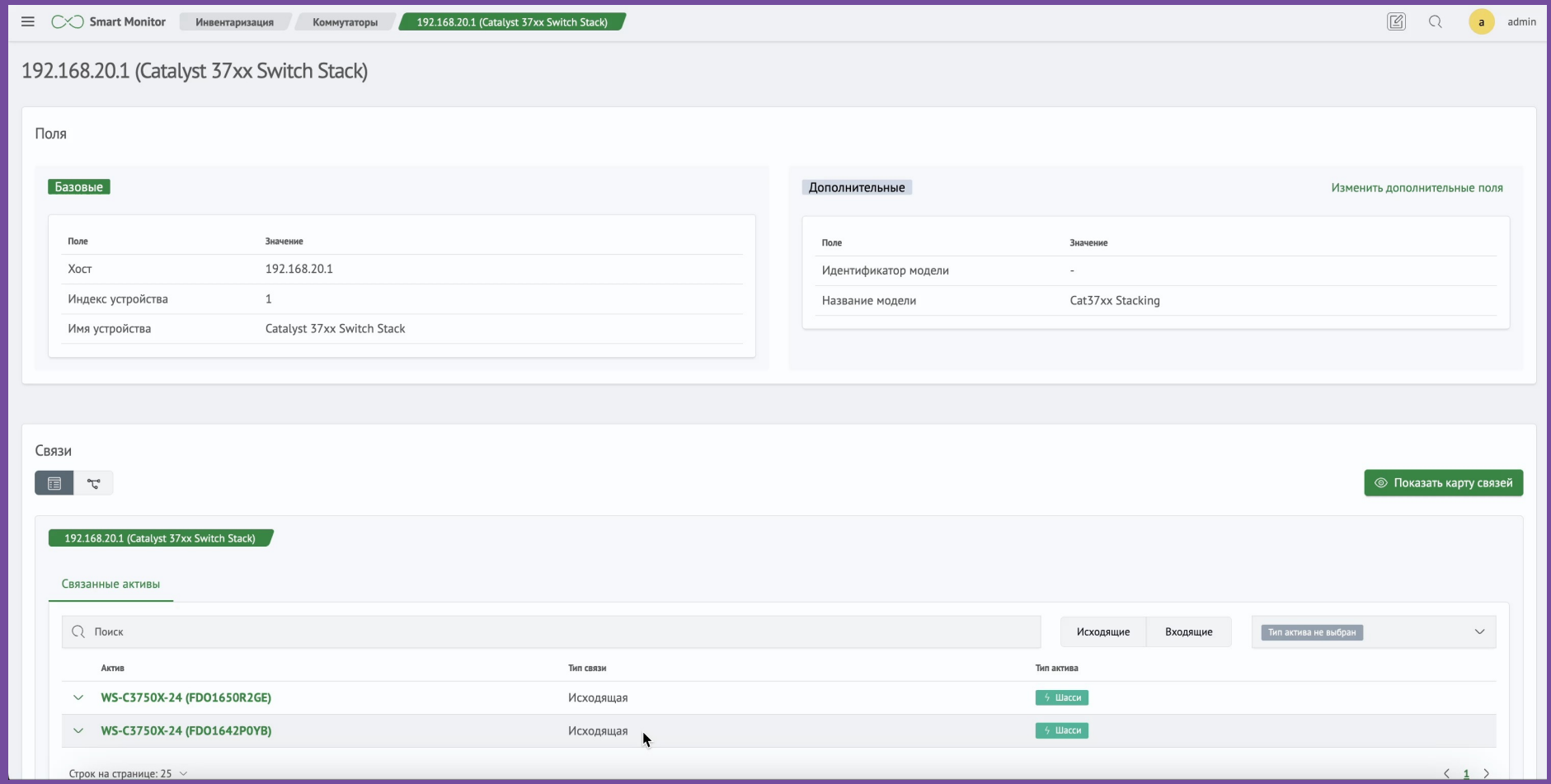
Оценка

Обнаружение узких мест системы для масштабирования/ оптимизации

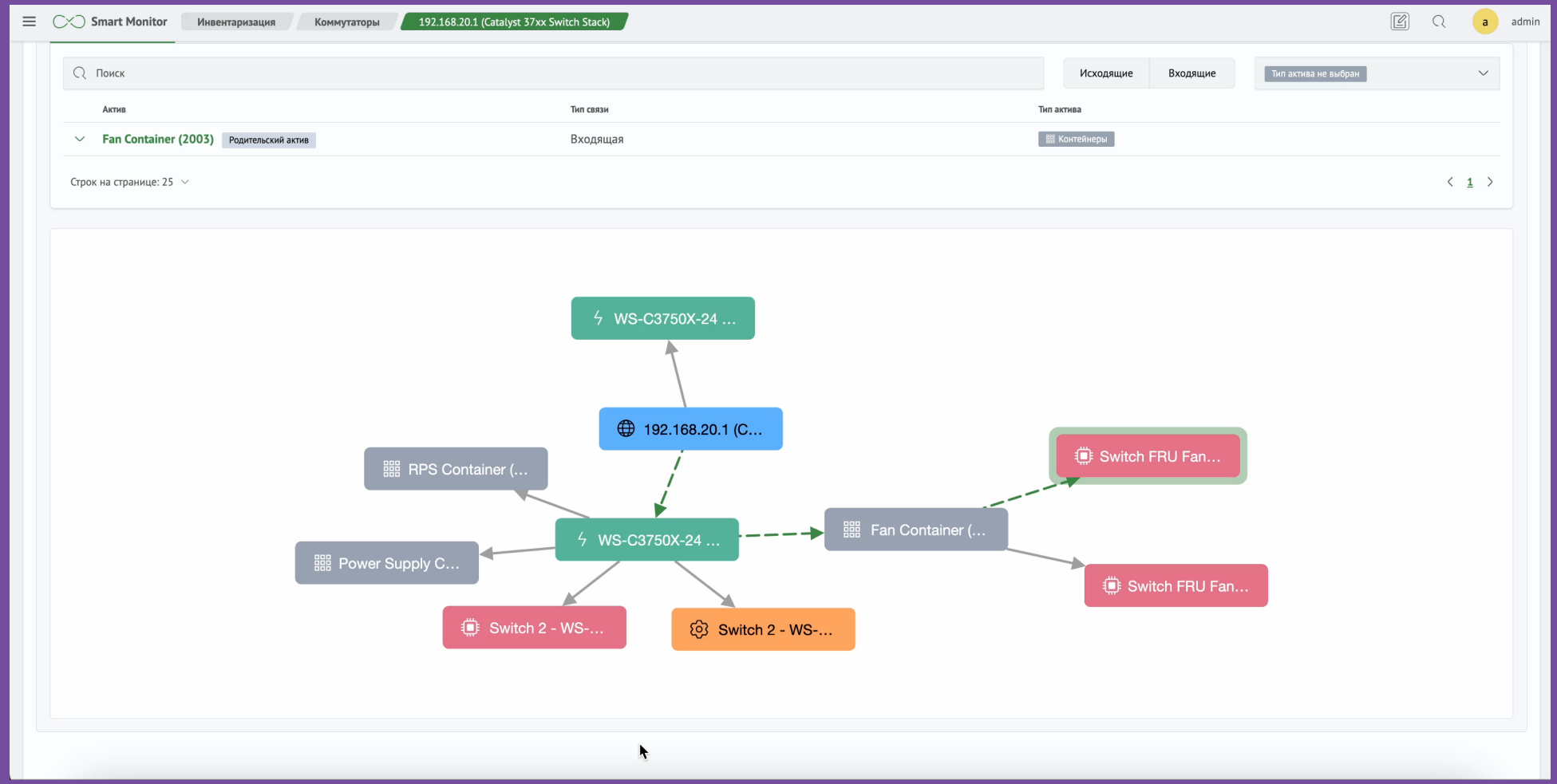
Настройка связывания



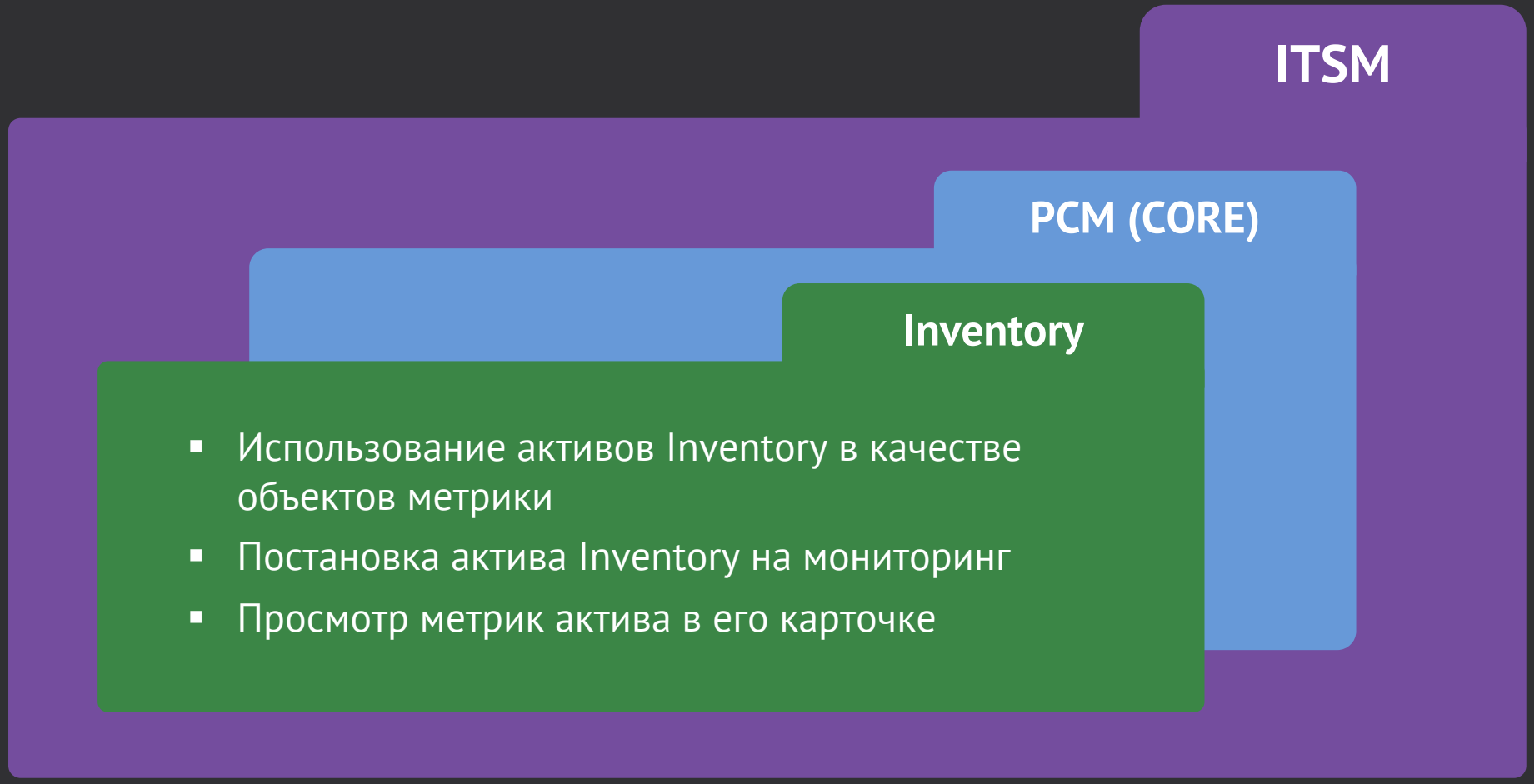
Связи актива



Все связи актива



Экосистема с другими модулями



NetMap

5.0 будет доступна с 1 мая

Спасибо за внимание!

Еще много изменений,

можно смотреть

changelog и демо зоны