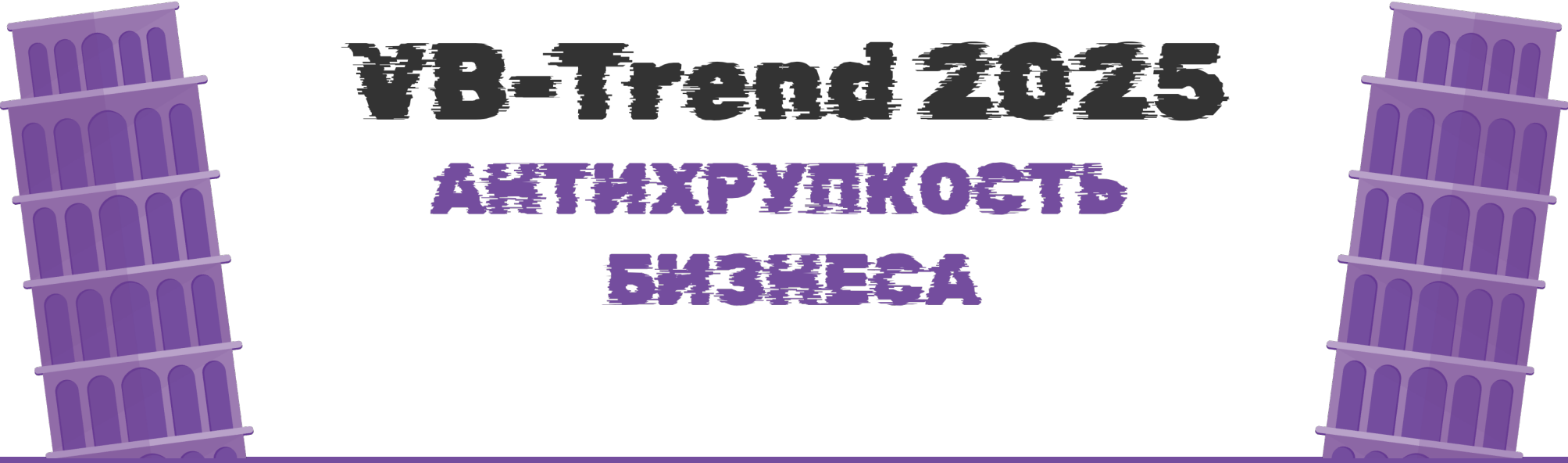




VB-Trend 2025

АНТИХРУПКОСТЬ

БИЗНЕСА

Smart Monitor: обзор изменений

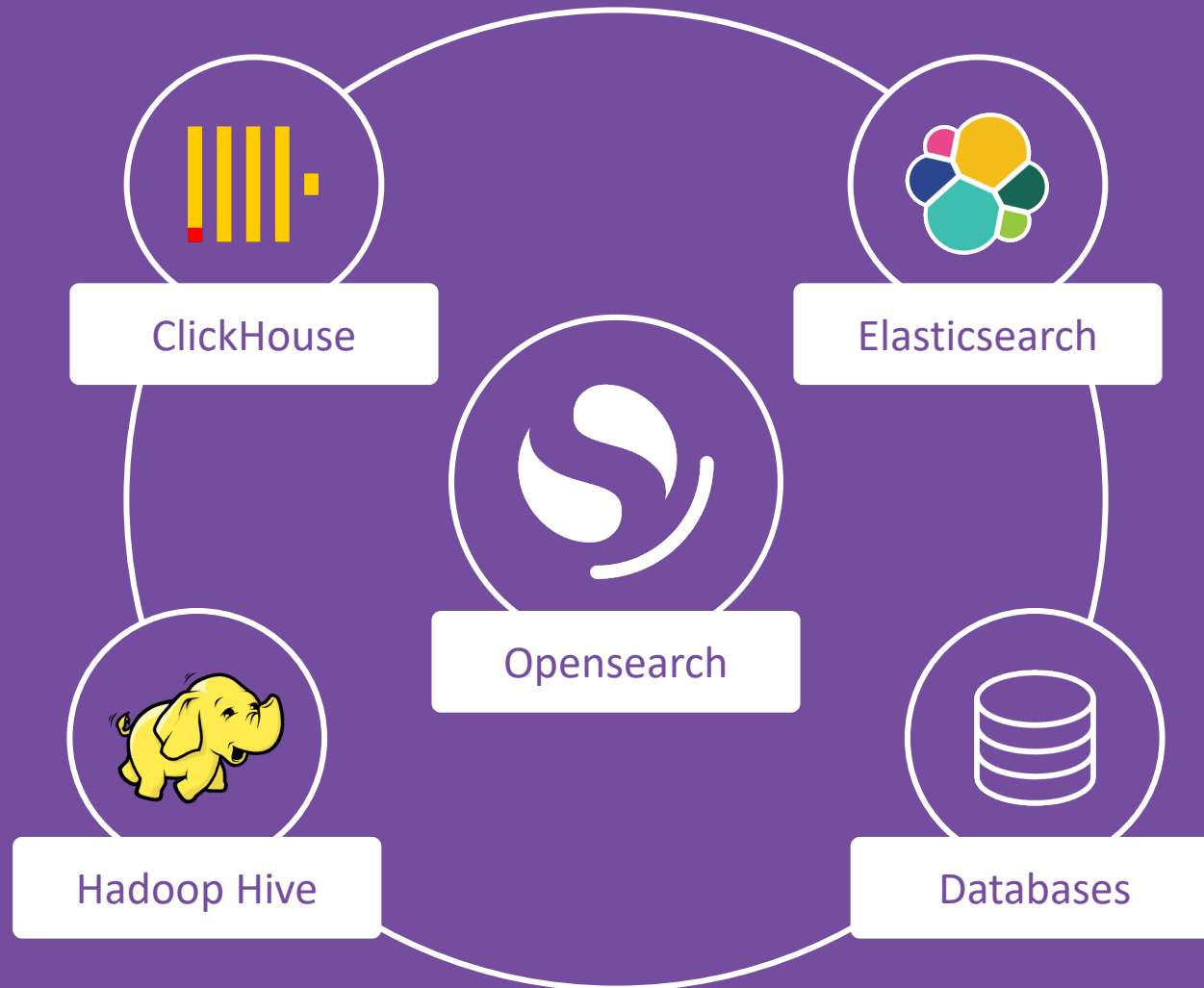


Максим Кириенко
VolgaBlob

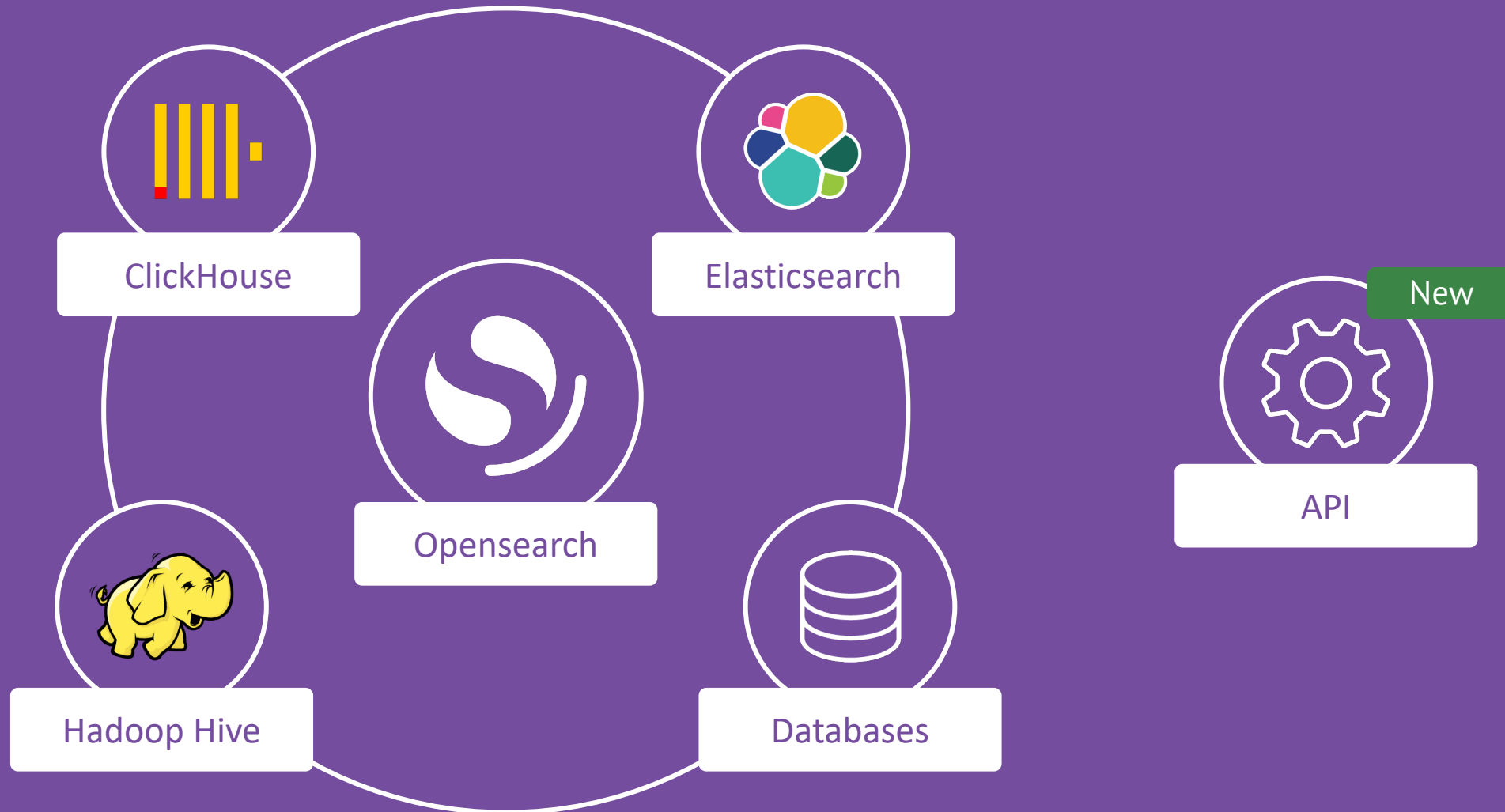


Новый источник Search Anywhere

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.

The screenshot shows the 'Smart Monitor' web interface. The top navigation bar includes a menu icon, the 'Smart Monitor' logo, and tabs for 'Настройки', 'Список конфигу...', and 'amtip'. The left sidebar lists various settings categories: 'ОСНОВНОЕ' (Themes, PDF export, Menu settings, Grok Debugger, Localization, Scoring types, Content management, Painless-scripts, Limits, Tags), 'JOB SCHEDULER' (Scheduler settings, Group settings), 'SEARCH ANYWHERE' (Config list, JDBC queries, API queries), 'UBA' (Initialization), and 'МЕНЕДЖЕР ИНЦИДЕНТОВ' (Incident card, Workflow). The main content area is titled 'Редактирование конфигурации' and 'Выберите тип конфигурации'. It features five selectable options: OpenSearch, Elastic, Hadoop, Clickhouse, and DB, with 'API' being the selected option. Below this, the 'Введите информацию о конфигурации' section contains form fields for 'Имя конфигурации' (filled with 'amtip'), 'URL сервера' (filled with 'https://amtip.ru'), and 'URL прокси сервера'. The 'Выберите тип авторизации' section has three buttons: 'Basic' (selected), 'API key', and 'Bearer'. The 'Пользователь' and 'Пароль' fields are also present, with the password field having a visibility toggle icon.

Поиск через команду source

 Smart Monitor

Поиск



a admin

Новый поиск

1

☐ Отправить в фон



 24 часа назад

Даты

Обновить



Поиск

Поиск по данным и фильтрация

История поиска

История

Избранное (1)

Поиск...

Запрос	Дата запуска ↓	Действия
> source api:nvd:cves mvexpand vulnerabilities eval vulnerabilities.cve.descriptions = tostring(vulnerabilities.cve.descriptions) table vulnerabilities.cve.sourceIdentifier,...	2025-04-09 00:27:05	...
> source api:nvd:cves mvexpand vulnerabilities eval vulnerabilities.cve.descriptions = tostring(vulnerabilities.cve.descriptions) spath input= table vulnerabilities.cve.s...	2025-04-09 00:22:02	  ...
> source api:nvd:cves mvexpand vulnerabilities	2025-04-09 00:18:10	...

Команда api и режимы

Smart Monitor

Поиск

a admin

Новый поиск

1

Отправить в фон

24 часа назад

Даты

Обновить

Поиск

Поиск по данным и фильтрация

История поиска

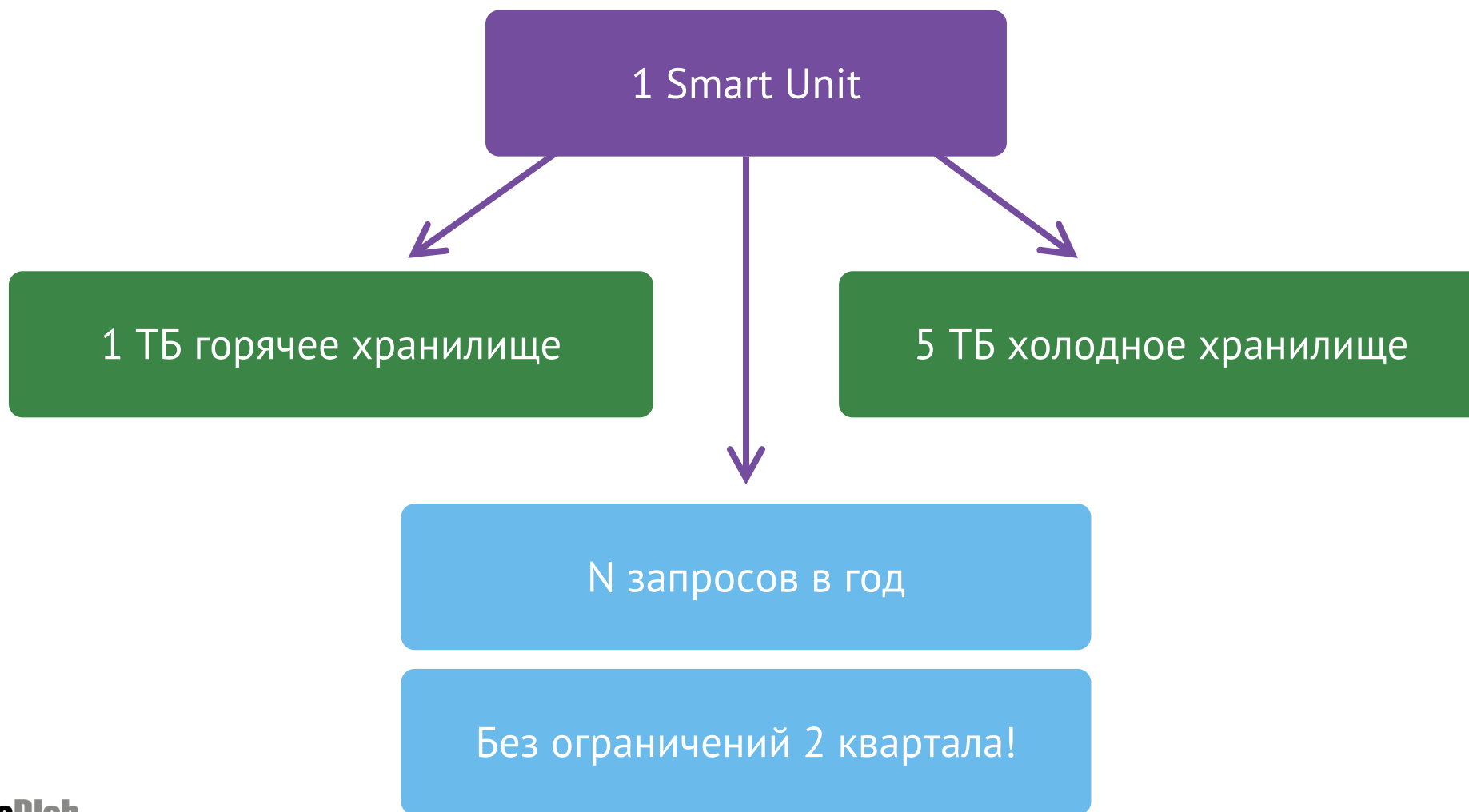
История

Избранное (11)

Поиск...

Запрос	Дата запуска	Действия
> source ti_index qsize=1 timefield="" fields ip eval ioc="{\\\\"ioc\\\\": \\\\", quota = \\\\"} eval ioc_ip = ioc + ip + quota map [api connection=amtip query=create...	2025-04-09 00:45:42	...
> source ti_index qsize=1 timefield="" fields ip eval ioc="{\\\\"ioc\\\\": \\\\", quota = \\\\"} eval ioc_ip = ioc + ip + quota map [api connection=amtip query=create...	2025-04-09 00:45:18	...
> source ti_index qsize=1 timefield="" fields ip eval ioc="{\\\\"ioc\\\\": \\\\", quota = \\\\"} eval ioc_ip = ioc + ip + quota map [api connection=amtip query=create...	2025-04-09 00:45:00	...

Лицензирование





Smart Notebooks

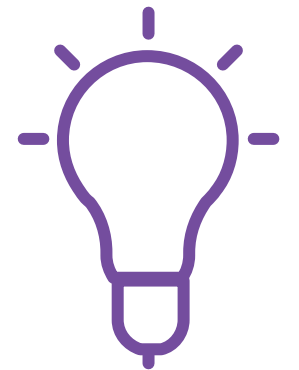
Доступность знаний одно из важных частей

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!

Smart Monitor

Knowledge Center

Все заметки

a admin

Все заметки (4)

Поиск...

С инцидентами

Теги

Создать

Редактировать выбранное

Импорт

Мои заметки

Системные

Все

☐	Заголовок	Дата создания	Дата обновления	Владелец	
☐	Расследование инцидента с пользователем SEAN Инфраструктура	2025-03-27 19:17:20	2025-04-04 13:49:31	admin	...
☐	Информация об устройствах Доступность IT-сервисов	2025-03-26 18:23:25	2025-04-07 22:03:19	admin	...
☐	Обзор инфраструктуры Инфраструктура Веб-сервер	2025-04-06 16:23:22	2025-04-07 22:02:31	admin	...
☐	Информация по коммутаторам Доступность IT-сервисов	2025-03-27 13:09:19	2025-04-07 22:03:06	admin	...

Строк на странице: 10

< 1 >

Пример расследования

Smart Monitor

Knowledge Center

Все заметки

а admin

С инцидентами

Теги

Создать

Все заметки (4)

Поиск...

Редактировать выбранное

Импорт

Мои заметки

Системные

Все

☐	Заголовок	Дата создания	Дата обновления	Владелец	
☐	Расследование инцидента с пользователем SEAN Инфраструктура	2025-03-27 19:17:20	2025-04-07 22:21:53	admin	...
☐	Информация об устройствах Доступность ИТ-сервисов	2025-03-26 18:23:25	2025-04-07 22:03:19	admin	...
☐	Обзор инфраструктуры Инфраструктура Веб-сервер	2025-04-06 16:23:22	2025-04-07 22:02:31	admin	...
☐	Информация по коммутаторам Доступность ИТ-сервисов	2025-03-27 13:09:19	2025-04-07 22:03:06	admin	...

Строк на странице: 10

<

1

>

Все заметки

Различные блоки: инцидент

Smart Monitor

Knowledge Center

Все заметки

Расследование инцидента с пользователем VereschaginaAD

a

admin

4. потенциальные последствия:

- На момент расследования утечки учетных данных не зафиксировано.
- Действия пользователя можно классифицировать как потенциально рискованные, но не имеющие явных признаков вредоносного намерения.

Рекомендации:

- Провести дополнительное обучение сотрудников по безопасному хранению учетных данных.
- Усилить мониторинг действий пользователей с доступом к критическим данным.
- Внедрить автоматизированные механизмы обнаружения и предупреждения попыток поиска учетных данных в файловых системах.

Статус инцидента: Закрыт, нарушений не выявлено.

Вложение (1 файл)

exported_job.zip

2.84 КБ

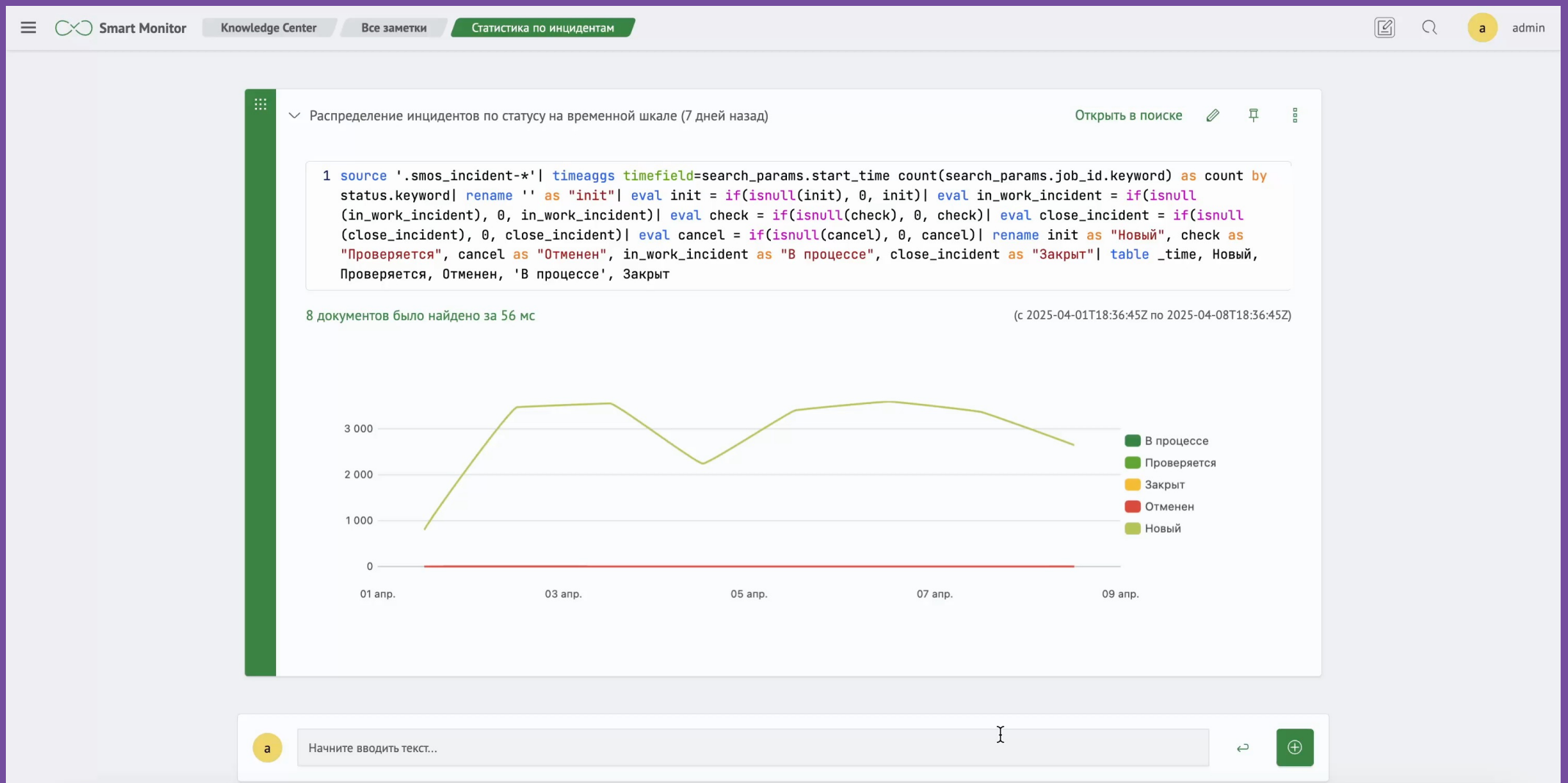
Скачать все (*.zip)

> Устройства / Switch 1 - WS-C3850-48P - FAN 2 (1012)

a

Начните вводить текст...

Различные блоки: поиск



Различные блоки: текст

☰

Smart Monitor

Knowledge Center

Все заметки

Расследование инцидента с пользователем SEAN

📄

🔍

a

admin

- Проверены журналы доступа к хранилищам паролей и секретам – несанкционированного чтения не выявлено.

4. Потенциальные последствия:

- На момент расследования утечки учетных данных не зафиксировано.
- Действия пользователя можно классифицировать как потенциально рискованные, но не имеющие явных признаков вредоносного намерения.

Рекомендации:

- Провести дополнительное обучение сотрудников по безопасному хранению учетных данных.
- Усилить мониторинг действий пользователей с доступом к критическим данным.
- Внедрить автоматизированные механизмы обнаружения и предупреждения попыток поиска учетных данных в файловых системах.

Статус инцидента: **Закрыт, нарушений не выявлено.**

> Диаграмма действия пользователей (день назад)

Открыть в поиске

✎

📌

⋮

> ● Пользователь SEAN осуществляет поиск файлов с небезопасно хранимыми учетными данными на хосте NSK-WS140

НОВЫЙ

👤

Не задан

✎

📌

⋮

a

Начните вводить текст...

↩

+

Различные блоки: файлы и изображения

The screenshot displays the 'Smart Monitor' interface with a top navigation bar. The main content area is titled 'Расследование инцидента с пользователем VereschaginaAD'. It contains a list of findings, recommendations, and the incident status. Below this, a detailed incident entry is shown, including a description, additional fields, and a list of details like 'Детали инцидента' and 'MITRE ATT&CK'. A search bar is visible at the bottom.

Smart Monitor Knowledge Center Все заметки Расследование инцидента с пользователем VereschaginaAD

На момент расследования утечки учетных данных не зафиксировано.

Действия пользователя можно классифицировать как потенциально рискованные, но не имеющие явных признаков вредоносного намерения.

Рекомендации:

- Провести дополнительное обучение сотрудников по безопасному хранению учетных данных.
- Усилить мониторинг действий пользователей с доступом к критическим данным.
- Внедрить автоматизированные механизмы обнаружения и предупреждения попыток поиска учетных данных в файловых системах.

Статус инцидента: Закрыт, нарушений не выявлено.

Пользователь (VereschaginaAD) произвел попытку получения доступа к учетным данным на хосте (NSK-WS715) **НОВЫЙ** Не задан

Описание

Обнаружена попытка доступа к учетным данным для извлечения логинов учетных записей пользователем: (VereschaginaAD) на хосте: (NSK-WS715)

Additional fields

Детали инцидента

MITRE ATT&CK

ID: ZmeMFpYB-Fw0xdL4ahFf

Начните вводить текст...

Различные блоки: актив

Smart Monitor

Knowledge Center

Все заметки

Расследование инцидента с пользователем VereschaginaAD

a

admin

- Действия пользователя можно классифицировать как потенциально рискованные, но не имеющие явных признаков вредоносного намерения.

Рекомендации:

- Провести дополнительное обучение сотрудников по безопасному хранению учетных данных.
- Усилить мониторинг действий пользователей с доступом к критическим данным.
- Внедрить автоматизированные механизмы обнаружения и предупреждения попыток поиска учетных данных в файловых системах.

Статус инцидента: **Закрит, нарушений не выявлено.**

✓

Пользователь (VereschaginaAD) произвел попытку получения доступа к учетным данным на хосте (NSK-WS715)

НОВЫЙ

Не задан

Описание

Обнаружена попытка доступа к учетным данным для извлечения логинов учетных записей пользователем: (VereschaginaAD) на хосте: (NSK-WS715)

Additional fields

Детали инцидента

MITRE ATT&CK

ID: ZmeMFpYB-Fw0xdL4ahFf

Вложение (1 файл)

a

Начните вводить текст...

 VolgaBlob

18

Статический режим

Smart Monitor

Knowledge Center

Все заметки

Расследование инцидента с пользователем VereschaginaAD

a

admin

Расследование инцидента с пользователем VereschaginaAD

Фильтр блоков 6

Действия

Просмотр

Документ

Резюме по результатам расследования

Вложение (1 файл)

Устройства / Switch 1 - WS-C3850-48P - FAN 2 (1012)

exported_job.zip

2.84 КБ

Скачать все (*.zip)

Базовые поля

Хост: 192.168.20.20

Индекс устройства: 1012

Дополнительные поля

ID: 89265146-9797-4f72-9523-48952aa377c2

a

Начните вводить текст...

↩

+

Создание быстрой заметки:

Smart Monitor

Менеджер инцидентов

24 часа назад

Даты

Обновить

Показать теги

Группировать инциденты

Показать пользовательские фильтры

Поиск...

Severity

Workflow

Status

Ответственный

Теги

638

НОРМА

898

ПРЕДУПРЕЖДЕНИЕ

748

ТРЕВОГА

1138

ИНФОРМАЦИЯ

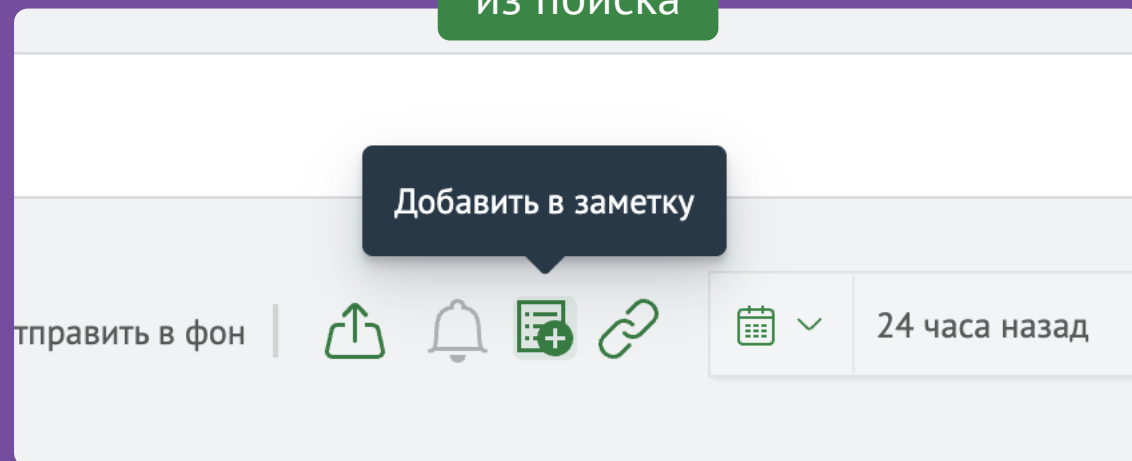
+ Создание инцидента

Настройки

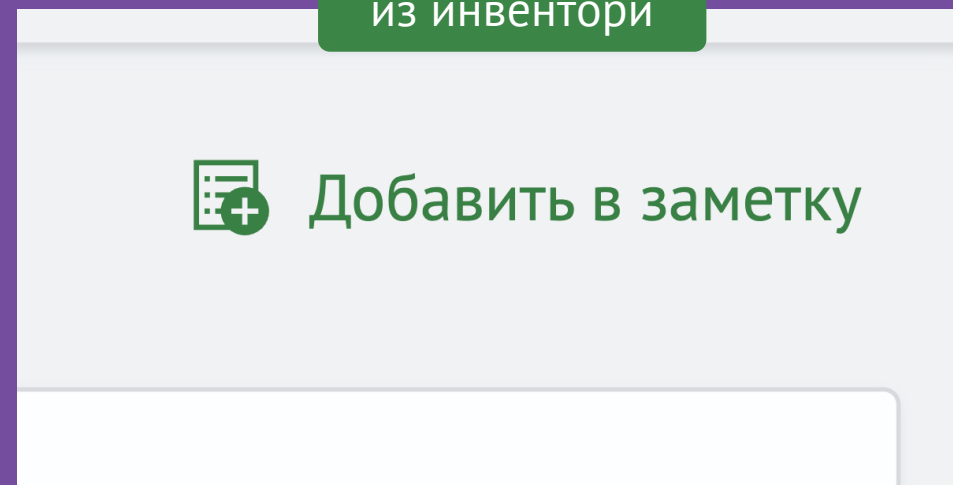
	Дата и время	Инцидент	Статус	Reviewer	
☐	▼ 2025-04-08 21:53:00 +03:00	Обнаружено потенциально вредоносное использование командной оболочки Windows пользователем FominaEM на хосте VLG-WS444 T1059.003 T1059.003	НОВЫЙ	unassigned	
☐	▼ 2025-04-08 21:53:00 +03:00	Пользователь SorokinaKL осуществляет поиск файлов с небезопасно хранимыми учетными данными на хосте KZN-WS804 T1552.001	НОВЫЙ	unassigned	
☐	▼ 2025-04-08 21:53:00 +03:00	Пользователь MorozovGA осуществляет поиск файлов с небезопасно хранимыми учетными данными на хосте EKB-WS925 T1552.001	НОВЫЙ	unassigned	
☐	▼ 2025-04-08 21:52:00 +03:00	Пользователь (DemidovNA) произвел попытку получения доступа к учетным данным на хосте (NSK-WS715) T1003	НОВЫЙ	unassigned	
☐	▼ 2025-04-08 21:52:00 +03:00	Пользователь (ErmolovaZM) произвел попытку получения доступа к учетным данным на хосте (NN-WS863) T1003	НОВЫЙ	unassigned	
☐	▼ 2025-04-08 21:52:00 +03:00	Пользователь (DobryninaVN) выполнил перебор файлов и каталогов или поиск информации на хосте (NSK-WS749) T1083 T1083	НОВЫЙ	unassigned	
☐	▼ 2025-04-08 21:52:00 +03:00	Пользователь (KudrjavitsevaKA) выполнил перебор файлов и каталогов или поиск информации на хосте (NSK-WS968) T1083 T1083	НОВЫЙ	unassigned	

Создание из разных мест интерфейса

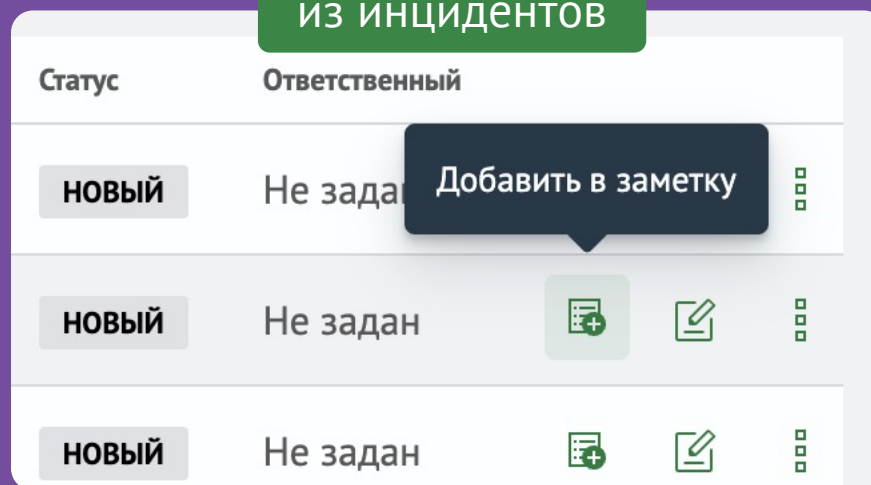
из поиска



из инвентори



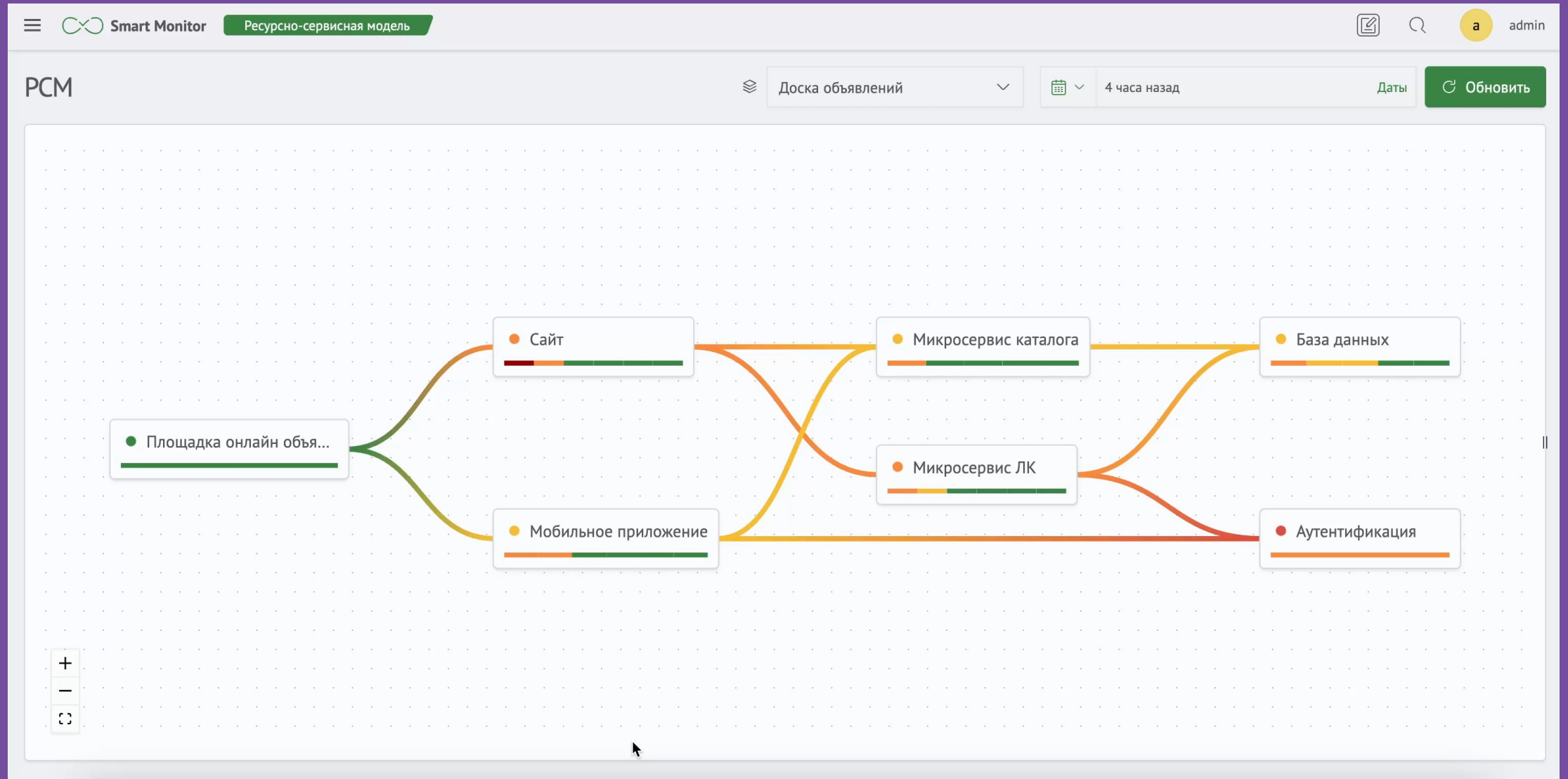
из инцидентов



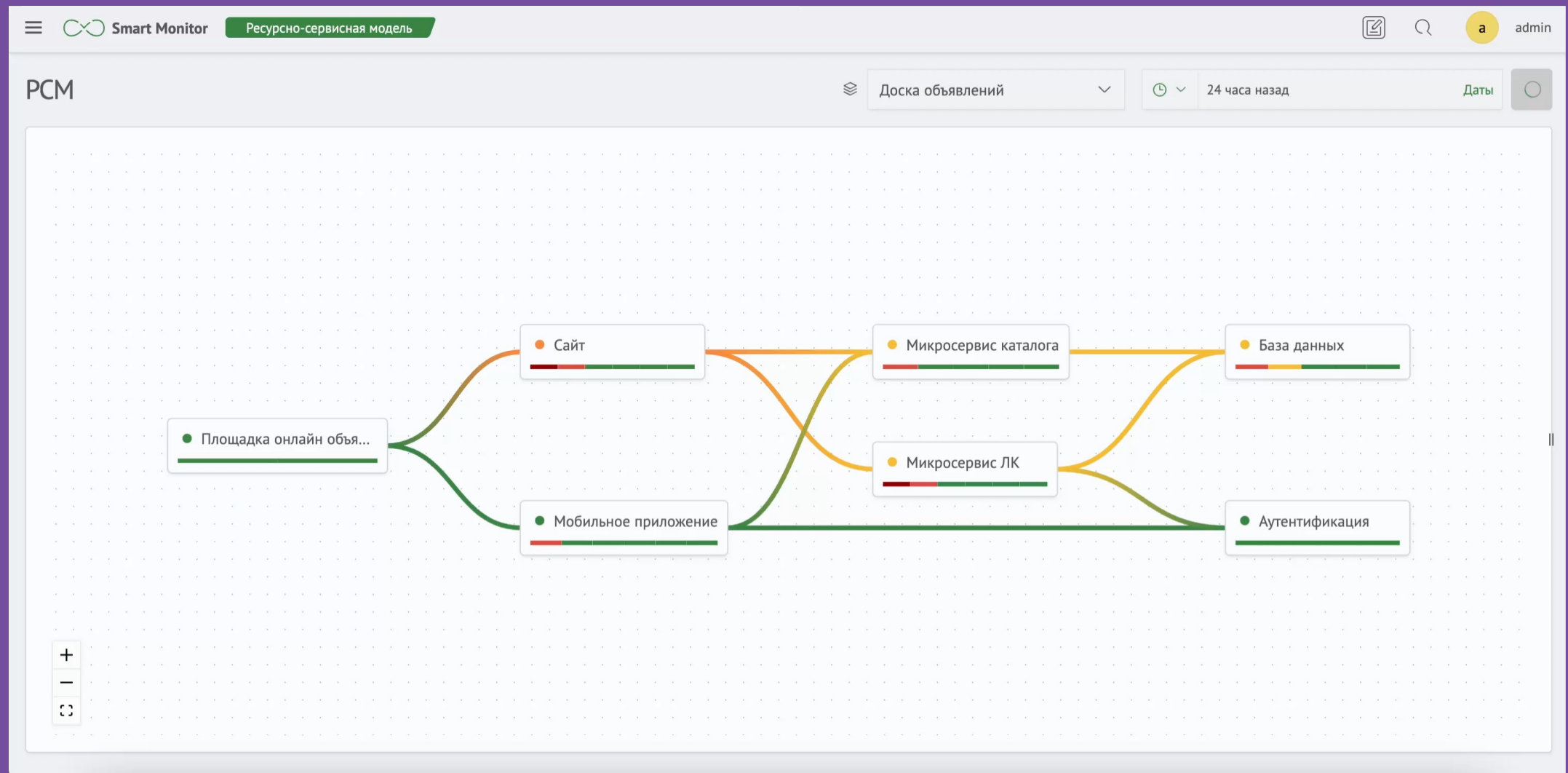


Ресурсно-сервисная модель 2.0

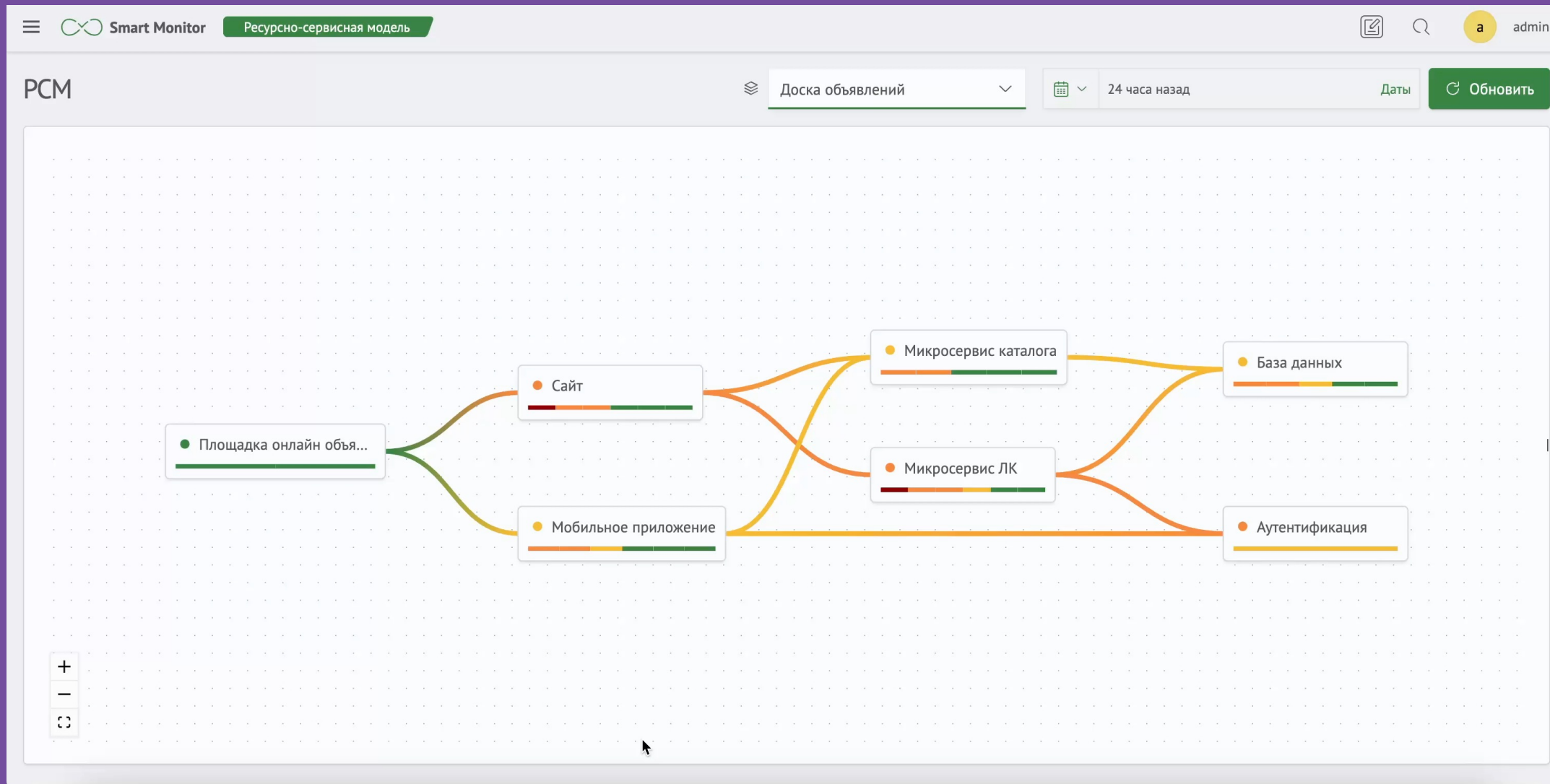
Новое представление графа



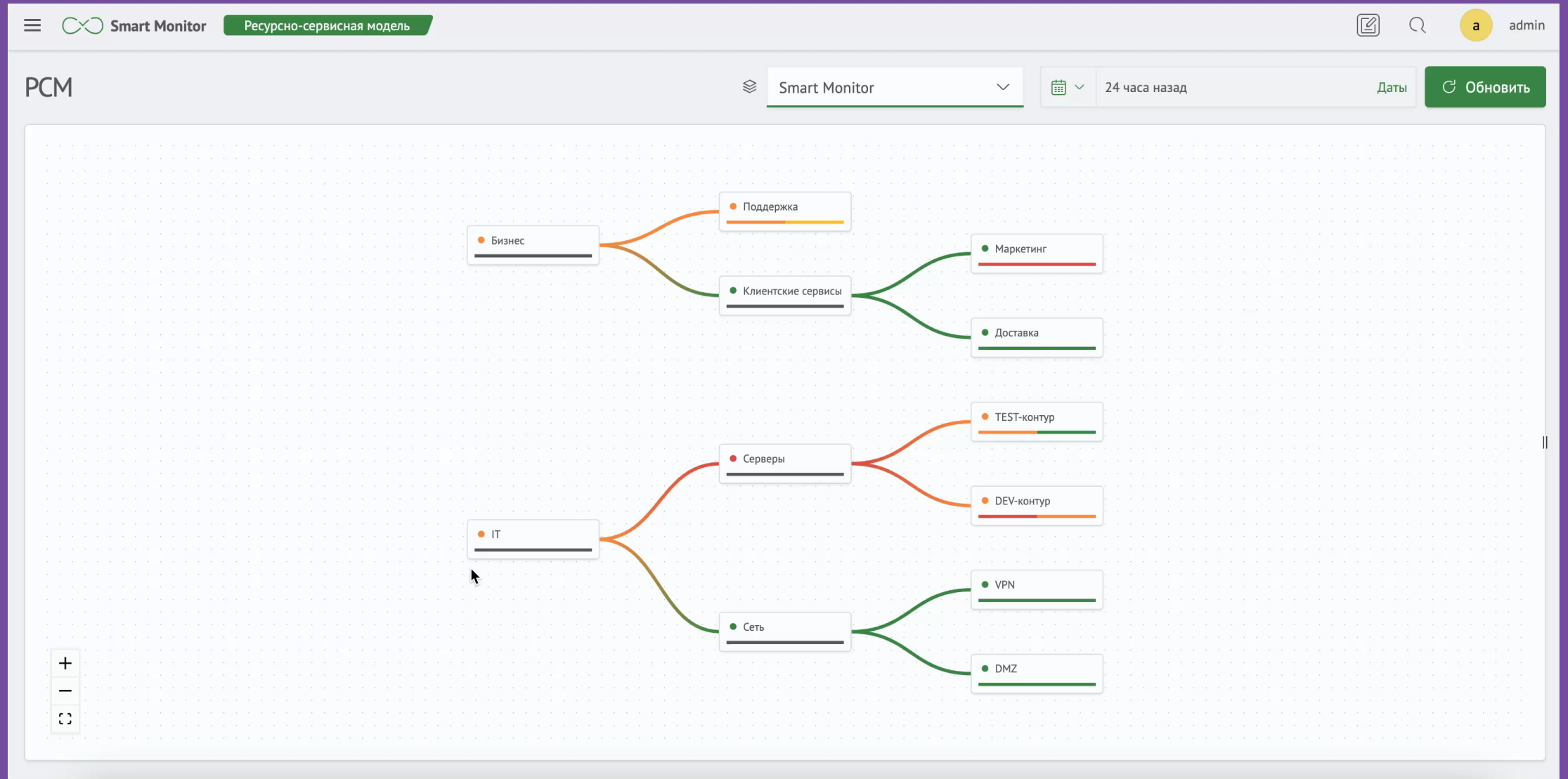
Автообновление



Несколько компонент связанности, слои



Представление блоками



PCM 2.0 – это начало бОльшего модуля

ITSM

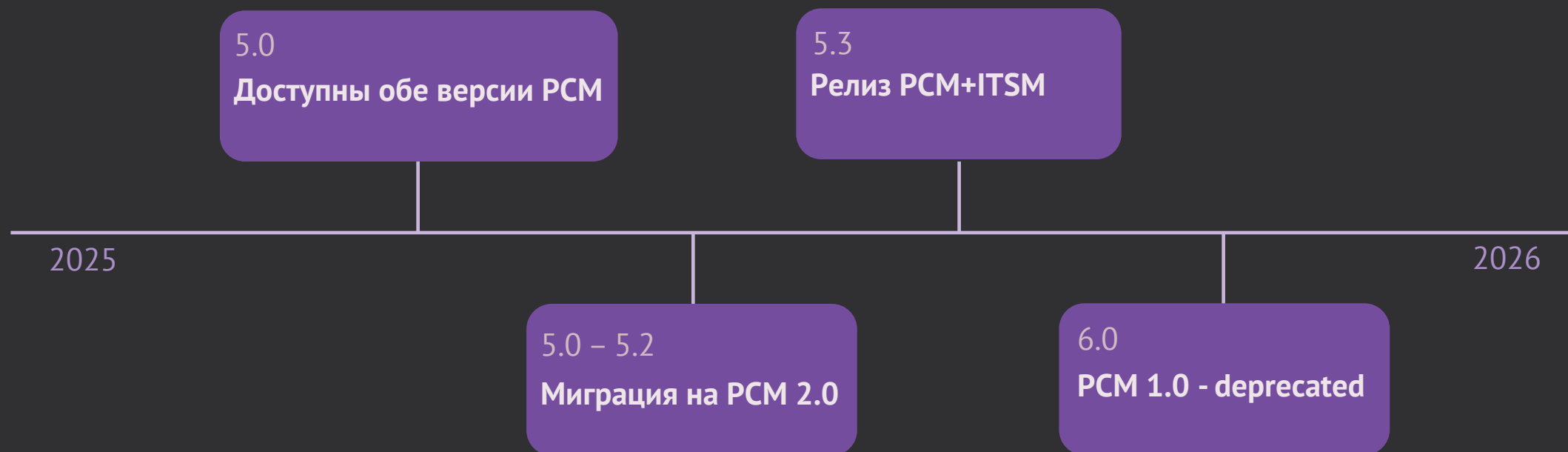
PCM (CORE)

- 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 РСМ 1.0 и 2.0





Smart Beat: Vector

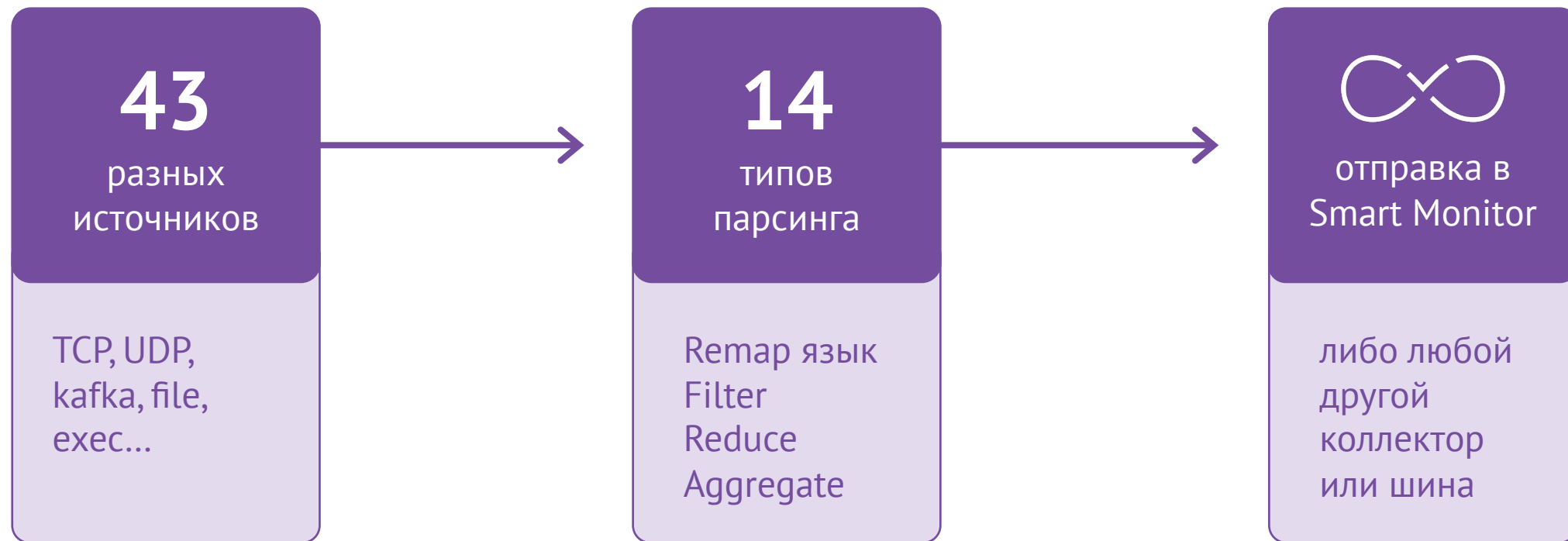
Vector

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

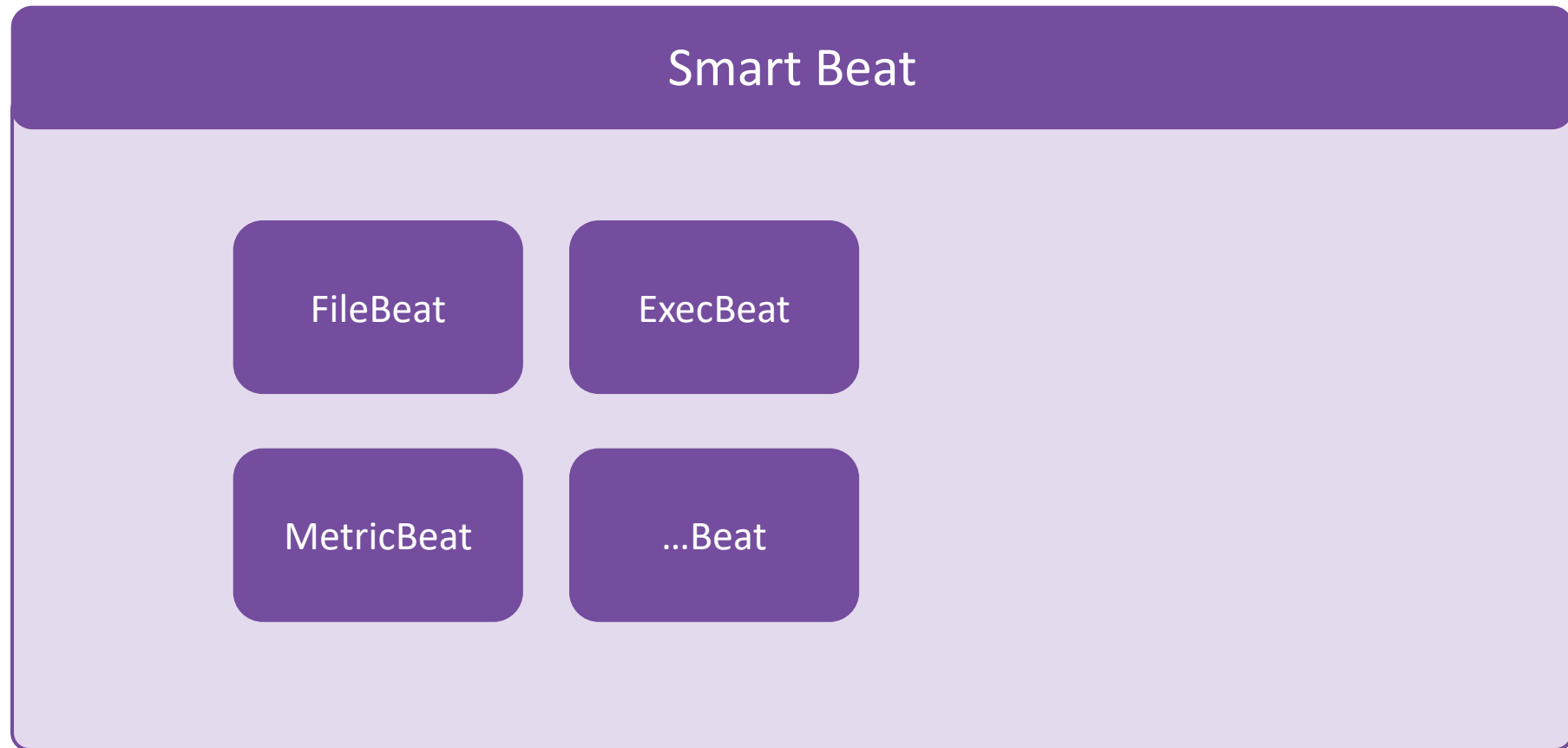
- > Потребляет минимальное количество ресурсов благодаря эффективному управлению памятью
- > Может обрабатывать до 30ТБ в сутки
- > От 10 до 30 раз быстрее конкурентов (beats, logstash, fluentbit) в отдельных случаях



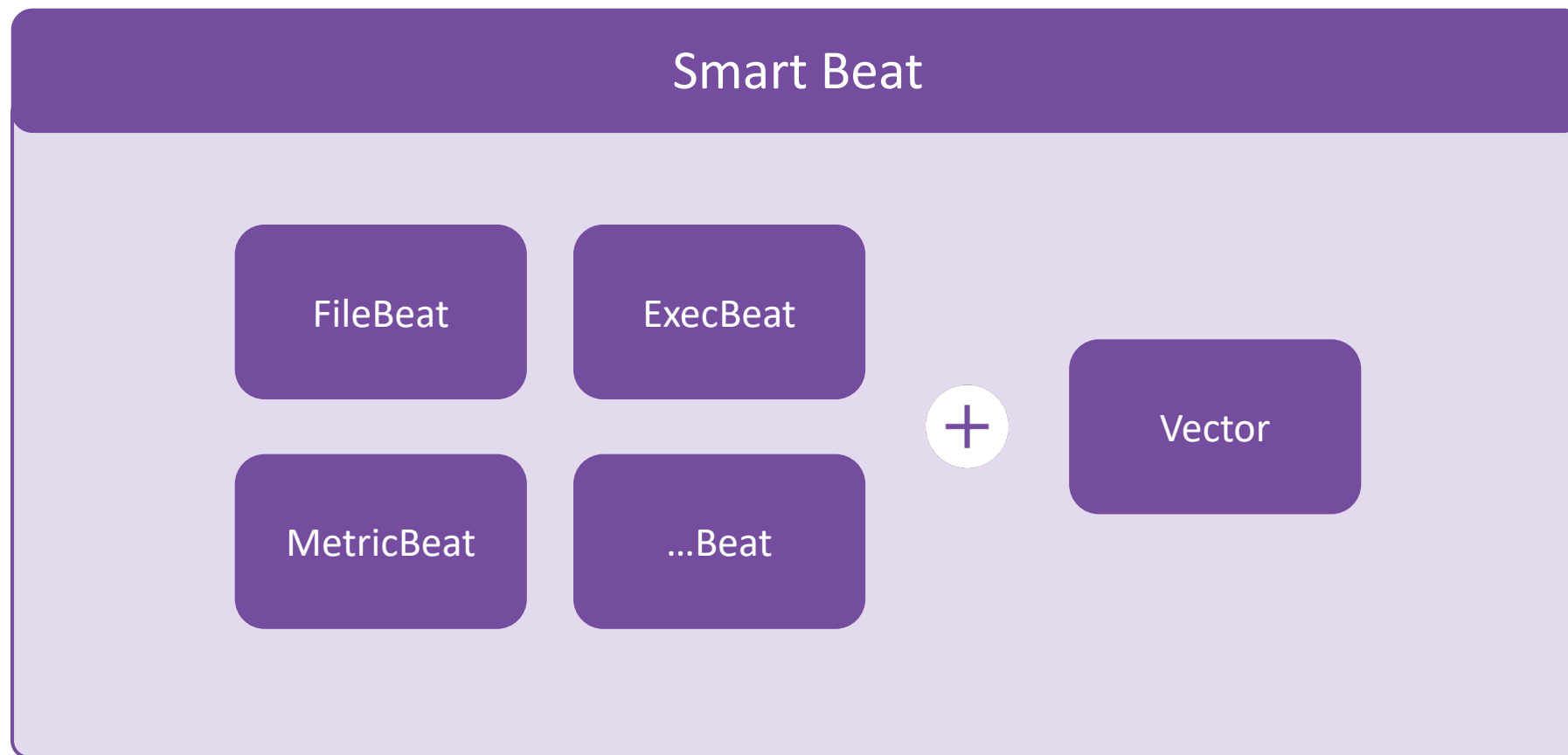
Vector



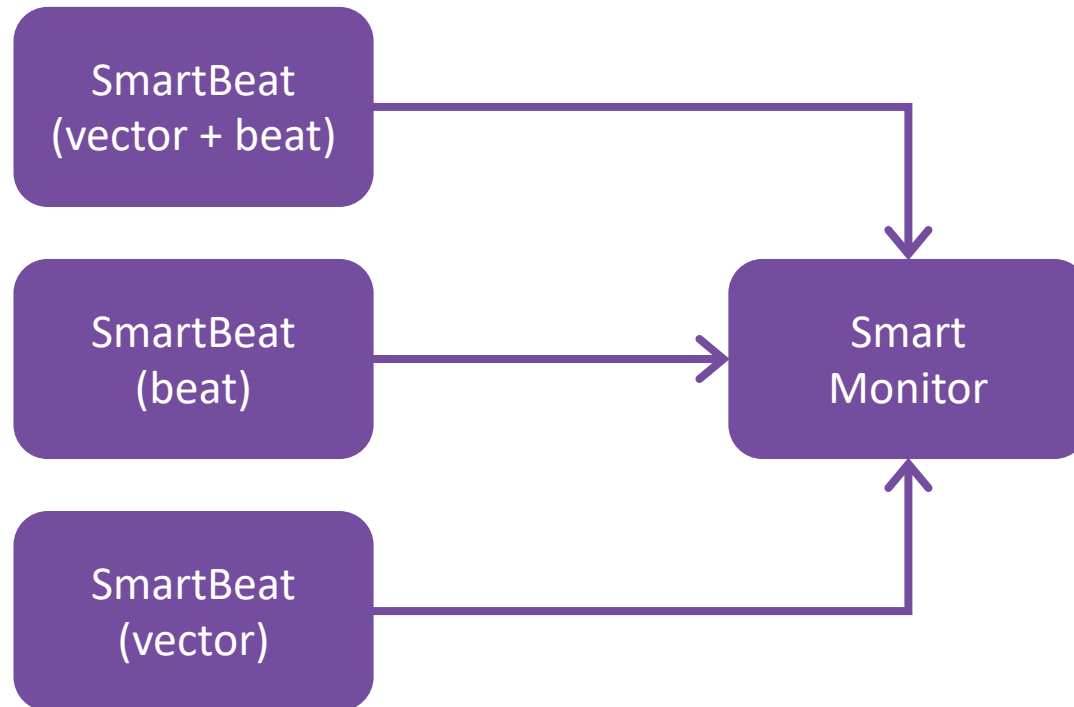
Smart Beat как агрегатор



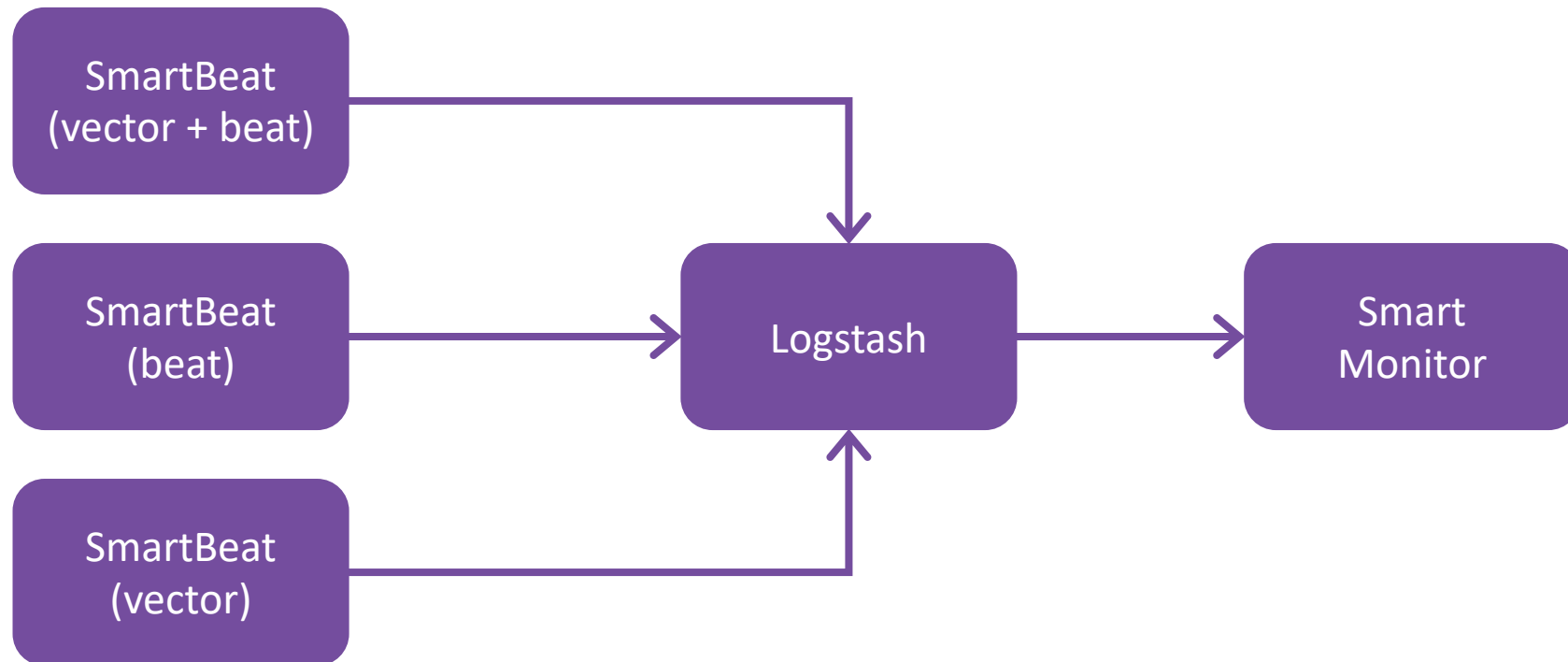
Smart Beat как агрегатор



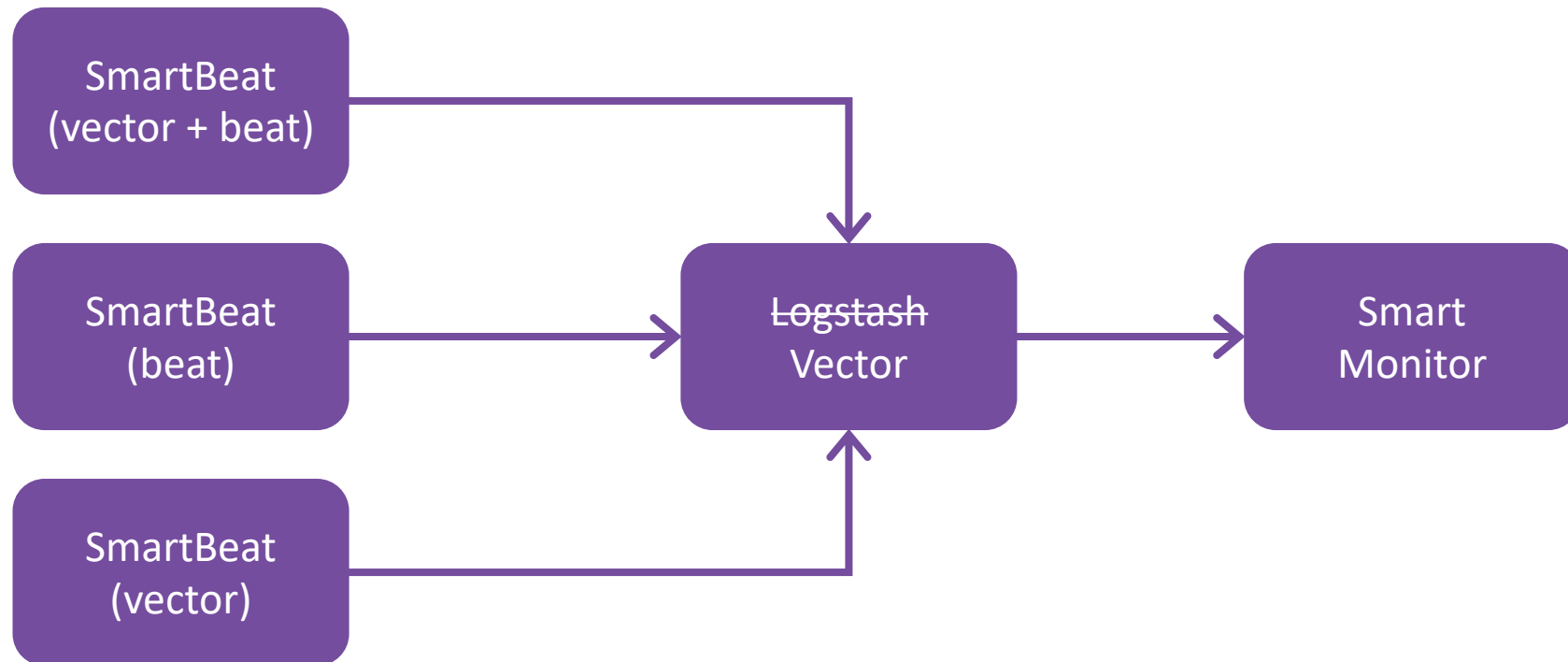
Архитектура сбора



Архитектура сбора



Архитектура сбора



Возможность управления всеми конфигами в интерфейсе

Smart Monitor

Управление Smart...

Файлы

a admin

Управление Smart Beat

ВСЕГО КЛИЕНТОВ
3 563
①

ПОДКЛЮЧЕННЫХ КЛИЕНТОВ
3 563
✓

КЛИЕНТЫ С ОШИБКОЙ
0
⚠

КЛИЕНТЫ НЕ В СЕТИ
0
🚫

Клиенты (3 563)

Группы (5)

Приложения (6)

Файлы (11)

Файлы

Пожалуйста, выберите или перетащите сюда zip/tar.gz архив с файлом

Поиск...

Название ↑	Тип файла	Подключенные клиенты	Валидный дистрибутив	
filebeat-oss-7.10.2-linux-x86_64.tar.gz	Beat	0	Да	
filebeat-oss-7.12.1-linux-x86_64.tar.gz	Beat	12	Да	
filebeat-oss-7.13.2-windows-x86.zip	Beat	0	Да	
filebeat-oss-8.8.1-linux-x86_64.tar.gz	Beat	0	Да	

Выбор решения



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



Новые визуализации

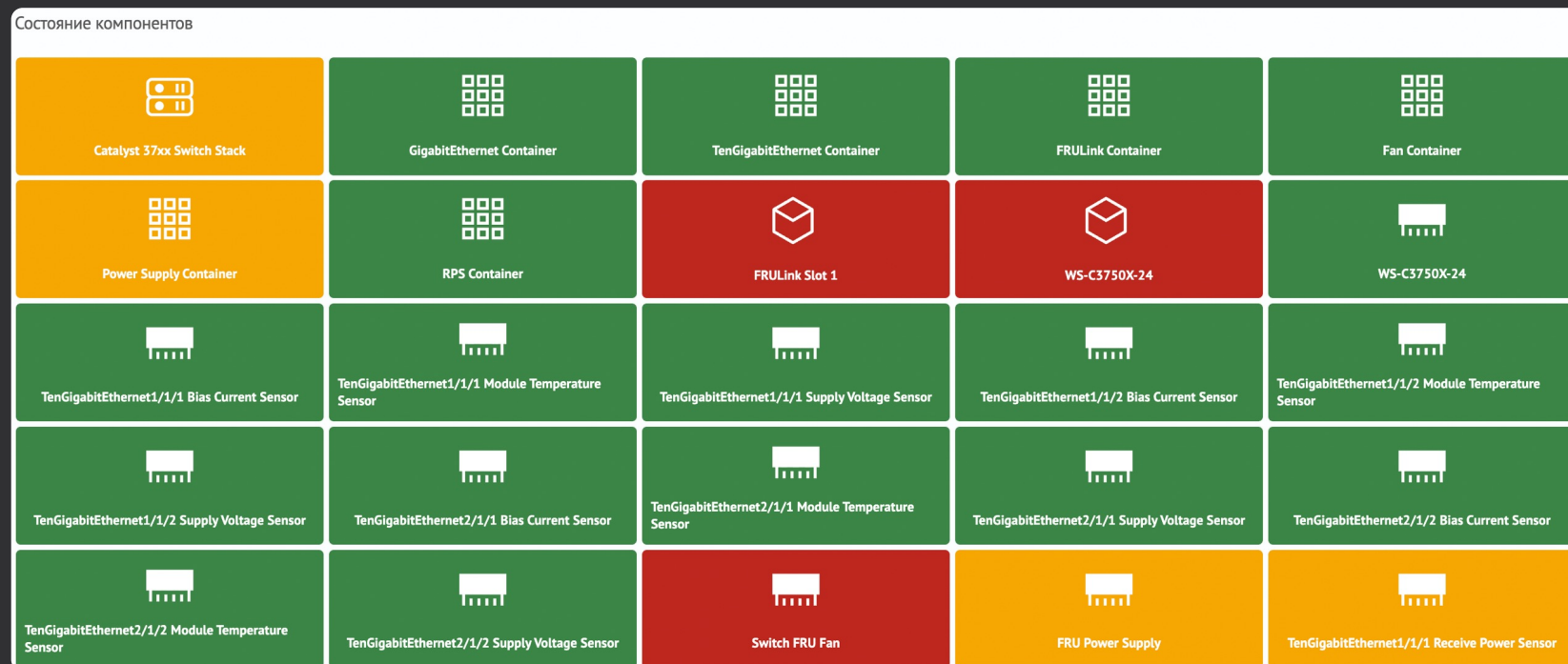
Визуализация Quick State

Feature Request от заказчика

Запрос один – метрик много!

Можно настроить:

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

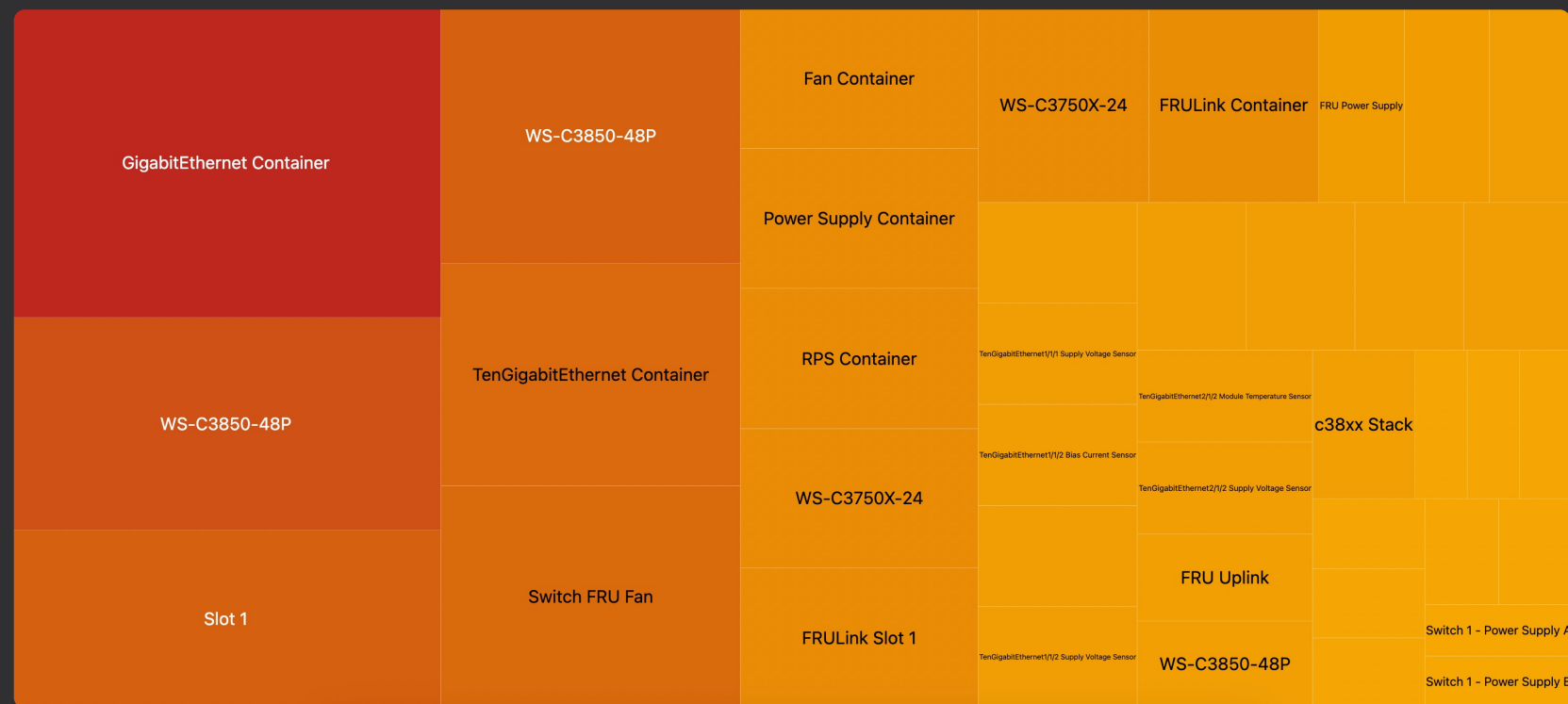


Визуализация TreeMap

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;



Localization;



Linear Regression;



Logistic Regression;



RFC;



Metrics Correlation.



RFC Summarize;

Интеграция ML в модуль Менеджер инцидентов

2025-04-09 09:27:00 +03:00

Пользователь (IvanovaAM) произвел попытку получения доступа к учетным данным на хосте (NSK-WS139)

NOVЫЙ

unassigned

T1003

Пользователь (IvanovaAM) произвел попытку получения доступа к учетным данным на хосте (NSK-WS139)

Взять в работу

Отменить

Ложное срабатывание

Отправить на почту

> История

ML

Предположение	Значение
False Positive	97%

Description

Обнаружена попытка доступа к учетным данным для извлечения логинов учетных записей пользователем: (IvanovaAM) на хосте: (NSK-WS139)

Additional Fields

Время:

2025-04-09T06:26:48.022515+0000

Пользователь:

IvanovaAM

Хост:

NSK-WS139

Образ:

C:\Windows\System32\findstr.exe

IP-адрес:

172.17.25.43

PID процесса:

647498

Действие:

Process Create (rule: ProcessCreate)

GUID процесса:

('43D6865D-0A13-645A-96EA-220000002B00')

Детали инцидента

Офис:

2001-01-01 00:00:00 +03:00

Потенциальный ущерб:

100

Подразделение:

IT

Текстовое поле:

-

Пользователь:

*

MITRE ATT&CK

Правила:

RULE - MA - Sysmon - OS Credential Dumping

Техники:

OS Credential Dumping (T1003)

Тактики:

-

ID:

uSY7GZYB5-9IN6szE1Yt

Посмотреть дополнительную информацию



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

```
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

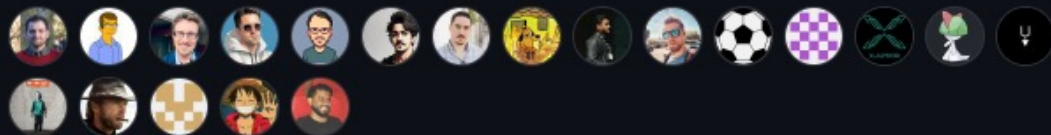
Emerging Threat

Конкретные угрозы, APT кампании, Zero-day, конкретное вредоносное ПО

Sigma

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

Contributors



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

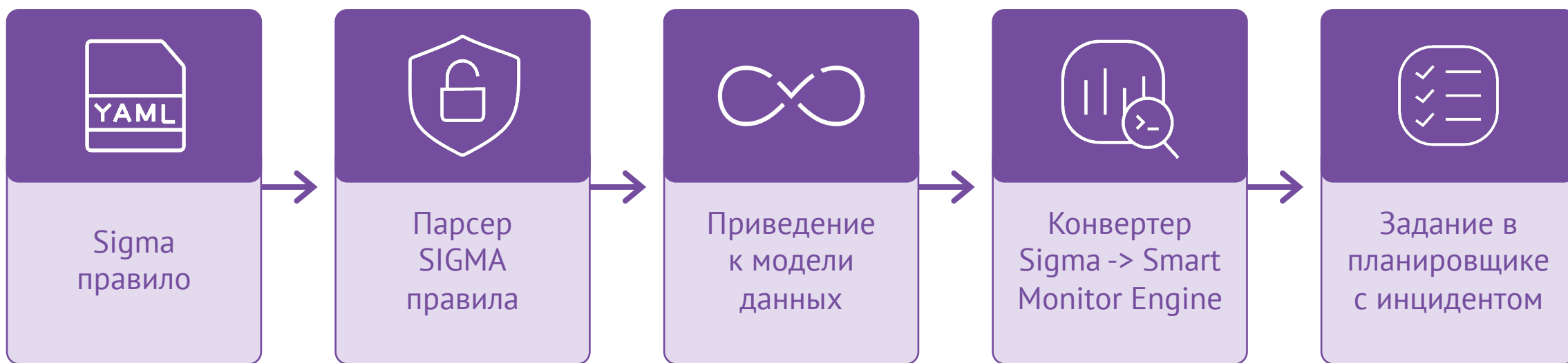
Fixed Rules

- 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

Smart Monitor

Правила Sigma

a admin

Правила Sigma (2883)

Поиск...

Критичность

Теги

Импортировать

Редактировать выбранное

☐	Название правила ↑	Критичность	Источник	Описание	Действия
☐	AWS Attached Malicious Lambda Layer Cisco ISE	medium	aws	Detects when an user attached a Lambda layer to an existing function to override a library that i...	...
☐	AWS S3 Data Management Tampering Cisco ISE INNOSMOS T1072 T1486 T1110.002 Изолированная среда (sandbox) T1552.004	low	aws	Detects when a user tampers with S3 data management in Amazon Web Services.	...
☐	Activity Performed by Terminated User Cisco ISE	medium	m365	Detects when a Microsoft Cloud App Security reported for users whose account were terminated...	...
☐	Activity from Anonymous IP Addresses	medium	m365	Detects when a Microsoft Cloud App Security reported when users were active from an IP addres...	...
☐	Azure Login Bypassing Conditional Access Policies Аутентификация SMB	high	m365	Detects a successful login to the Microsoft Intune Company Portal which could allow bypassing ...	...
☐	Disabling Multi Factor Authentication	high	m365	Detects disabling of Multi Factor Authentication.	...
☐	Github Delete Action Invoked T1486 T1110.002 T1057 Изолированная среда (sandbox) SAML SBERMSMOS Check Point NGFW Gitlab	medium	github	Detects delete action in the Github audit logs for codespaces, environment, project and repo.	...
☐	Github Fork Private Repositories Setting Enabled/Cleared Gitlab	medium	github	Detects when the policy allowing forks of private and internal repositories is changed (enabled ...	...
☐	Github High Risk Configuration Disabled INNOSMOS fields Splunk	high	github	Detects when a user disables a critical security feature for an organization.	...
☐	Github New Secret Created INNOSMOS fields Splunk	low	github	Detects when a user creates action secret for the organization, environment, codespaces or repo...	...
☐	Github Outside Collaborator Detected INNOSMOS fields Splunk	medium	github	Detects when an organization member or an outside collaborator is added to or removed from a...	...
☐	Github Push Protection Disabled				



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

Smart Monitor

Инвентаризация

Связи

admin

Связи (13)

Поиск...

Активы

Связи

Список связей

Актив	Связанный актив	
Контейнеры	Модули	...
Модули	Контейнеры	...
Модули	Порты	...
Модули	Устройства	...
Коммутаторы	Шасси	...
Шасси	Контейнеры	...
Контейнеры	Порты	...
Порты	Устройства	...
Контейнеры	Устройства	...
Шасси	Устройства	...
Шасси	Модули	...
АПКШ Континент	Парные связи	...
Парные связи	АПКШ Континент	...

Карта связей

Скрыть узлы без связей

The diagram illustrates a network topology. At the top left, 'АПКШ Континент' (green box) is connected to 'Парные связи' (purple box). Below them, 'Пользователи' (grey box) is shown. In the center, 'Коммутаторы' (blue box) is connected to 'Шасси' (green box). 'Шасси' is further connected to 'Контейнеры' (grey box), 'Модули' (orange box), and 'Порты' (purple box). 'Контейнеры' and 'Модули' are also connected to 'Порты'. Finally, 'Порты' is connected to 'Устройства' (red box) at the bottom right. A legend on the left shows icons for adding, removing, and zooming the map.

Связи актива

Smart Monitor

Инвентаризация

Коммутаторы

192.168.20.1 (Catalyst 37xx Switch Stack)

a admin

192.168.20.1 (Catalyst 37xx Switch Stack)

Поля

Базовые

Поле	Значение
Хост	192.168.20.1
Индекс устройства	1
Имя устройства	Catalyst 37xx Switch Stack

Дополнительные

Изменить дополнительные поля

Поле	Значение
Идентификатор модели	-
Название модели	Cat37xx Stacking

Связи

Показать карту связей

192.168.20.1 (Catalyst 37xx Switch Stack)

Связанные активы

Поиск

Исходящие

Входящие

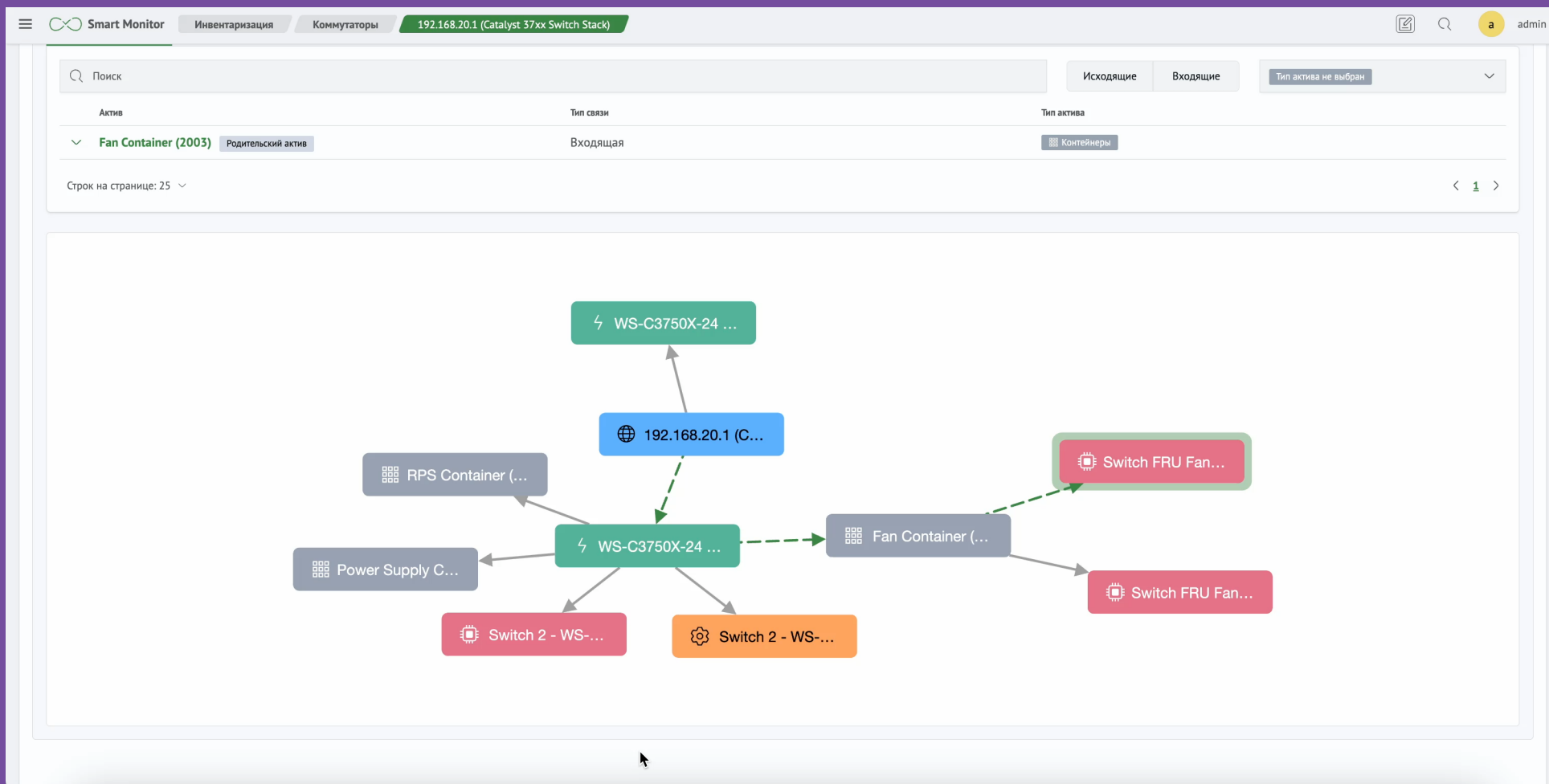
Тип актива не выбран

Актив	Тип связи	Тип актива
WS-C3750X-24 (FDO1650R2GE)	Исходящая	Шасси
WS-C3750X-24 (FDO1642P0YB)	Исходящая	Шасси

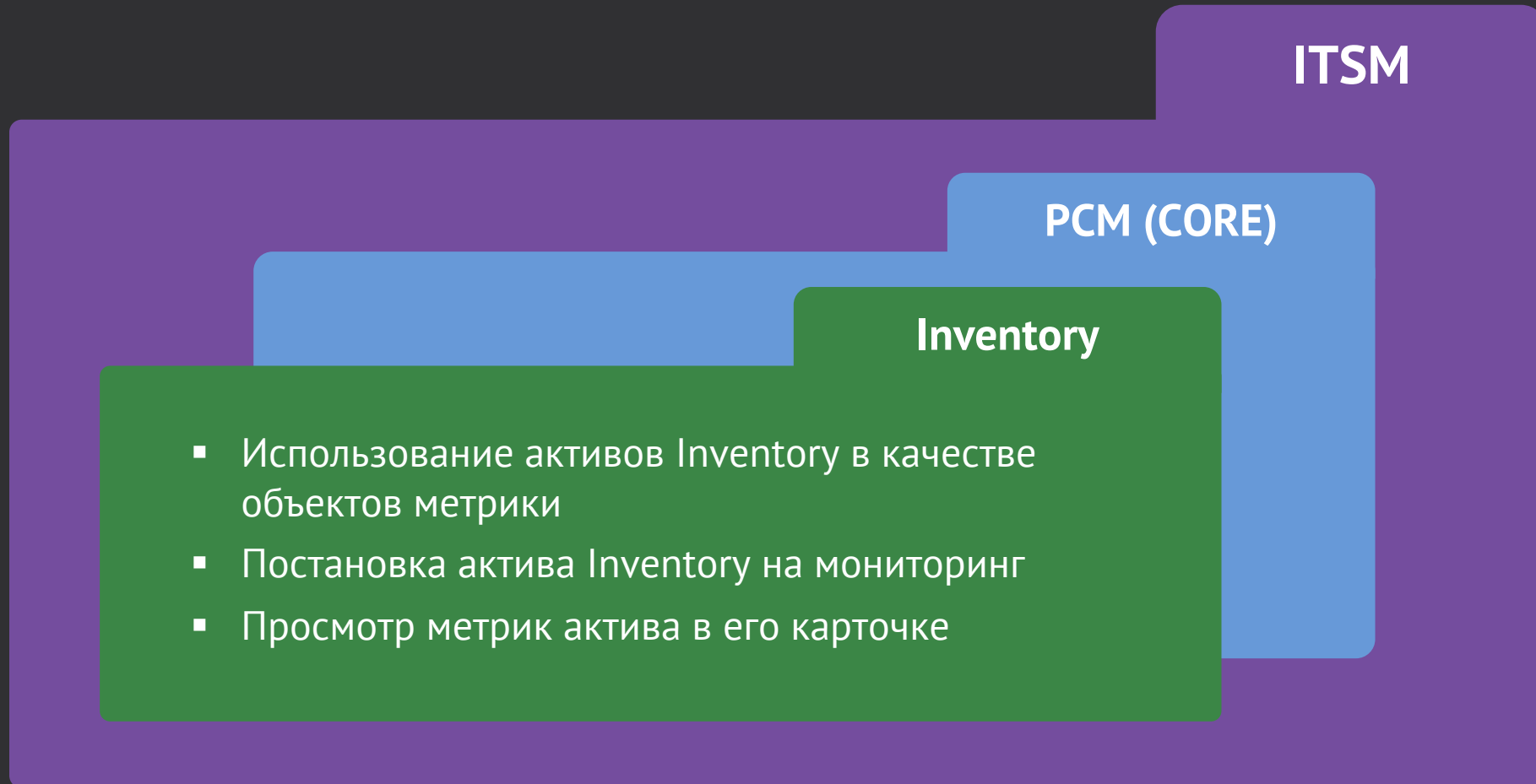
Строк на странице: 25

1

Все связи актива



Экосистема с другими модулями



NetMap

5.0 будет доступна с 1 мая

Спасибо за внимание!

Еще много изменений,

можно посмотреть
changelog и демо зоны

