



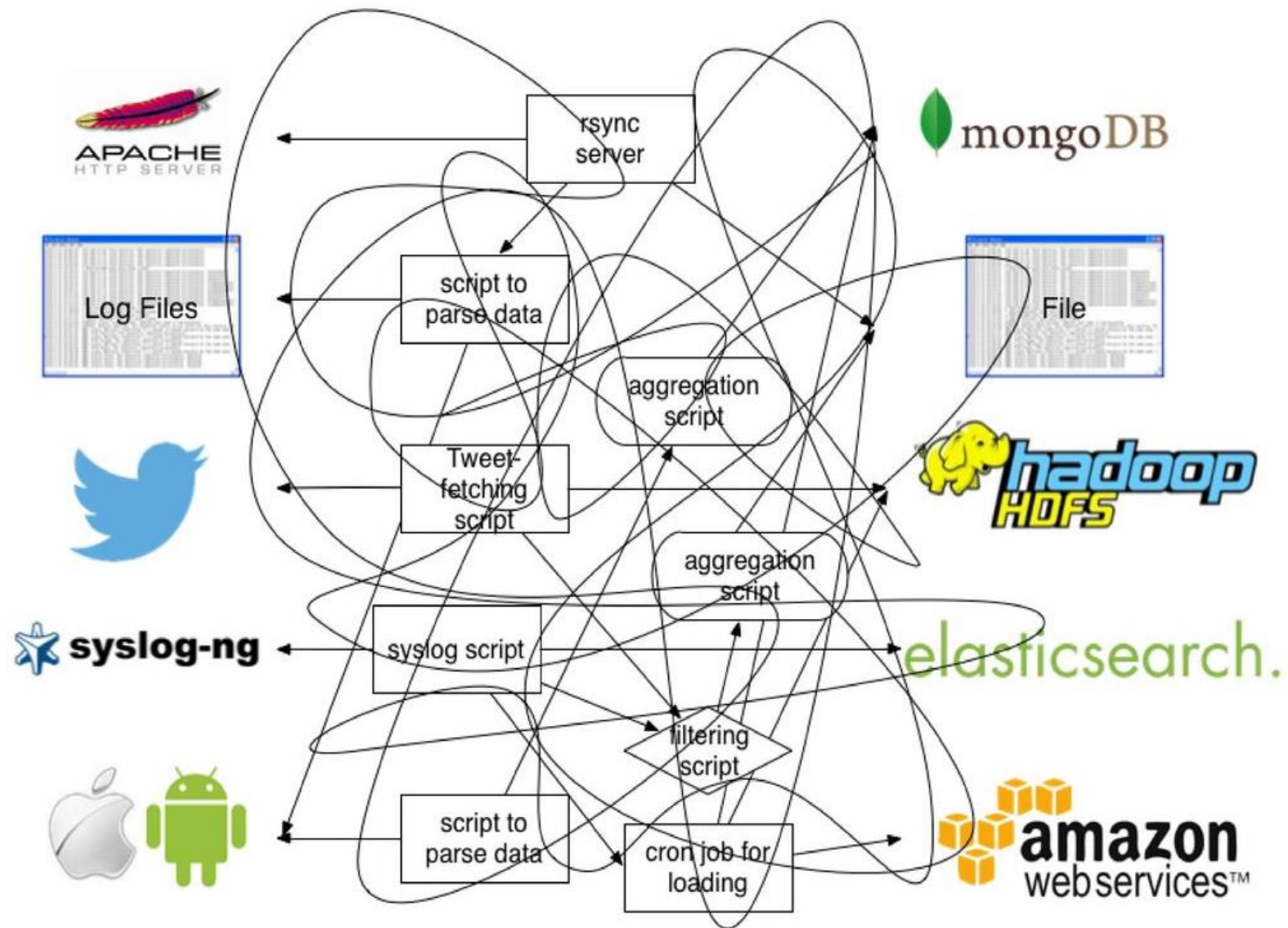
Log Management: Централизация, обнаружение и анализ

Централизованное управление событиями

rvision.ru

О чем сегодня поговорим

- 
- 1 Что такое Log Management
 - 2 Для чего собирать события
 - 3 Сбор и обработка событий
 - 4 Централизация
 - 5 Для кого?

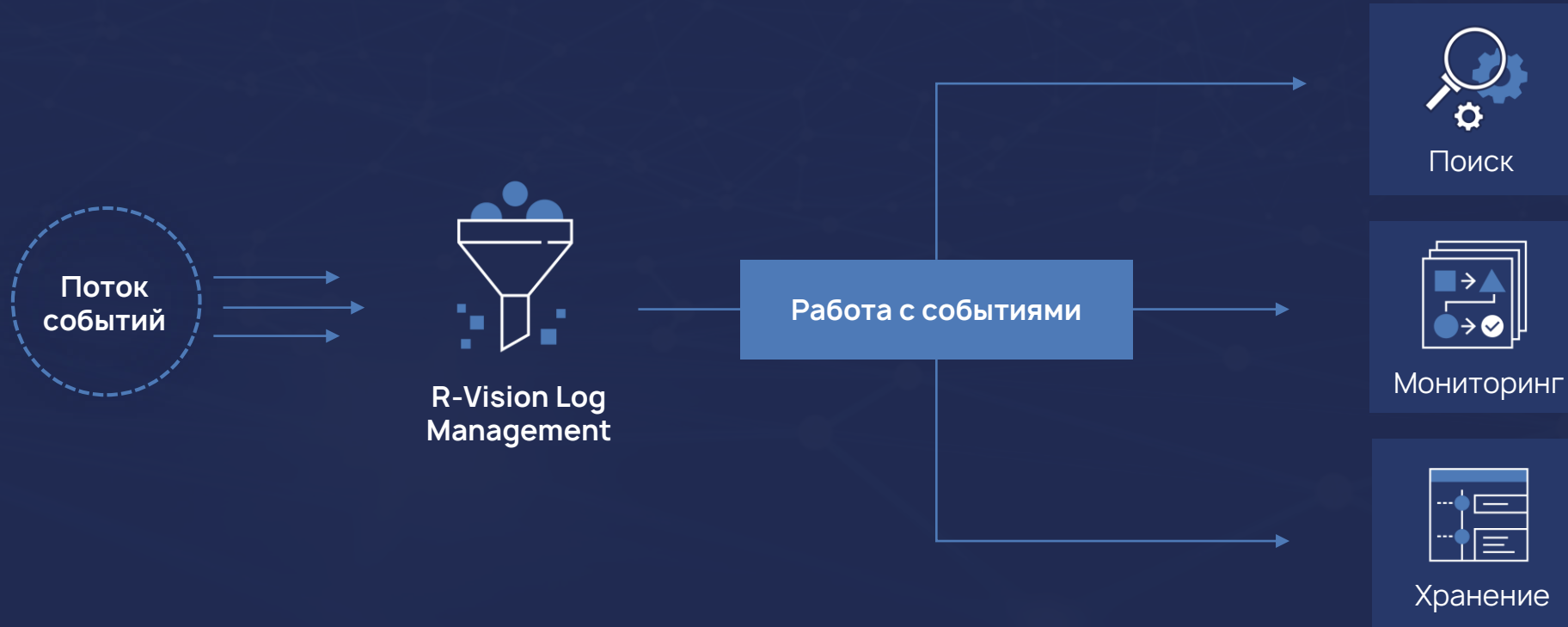




Зачем собирать логи?

Что такое Log Management

Решение, которое позволит **централизованно** управлять потоками событий и работать с ними из единого интерфейса.



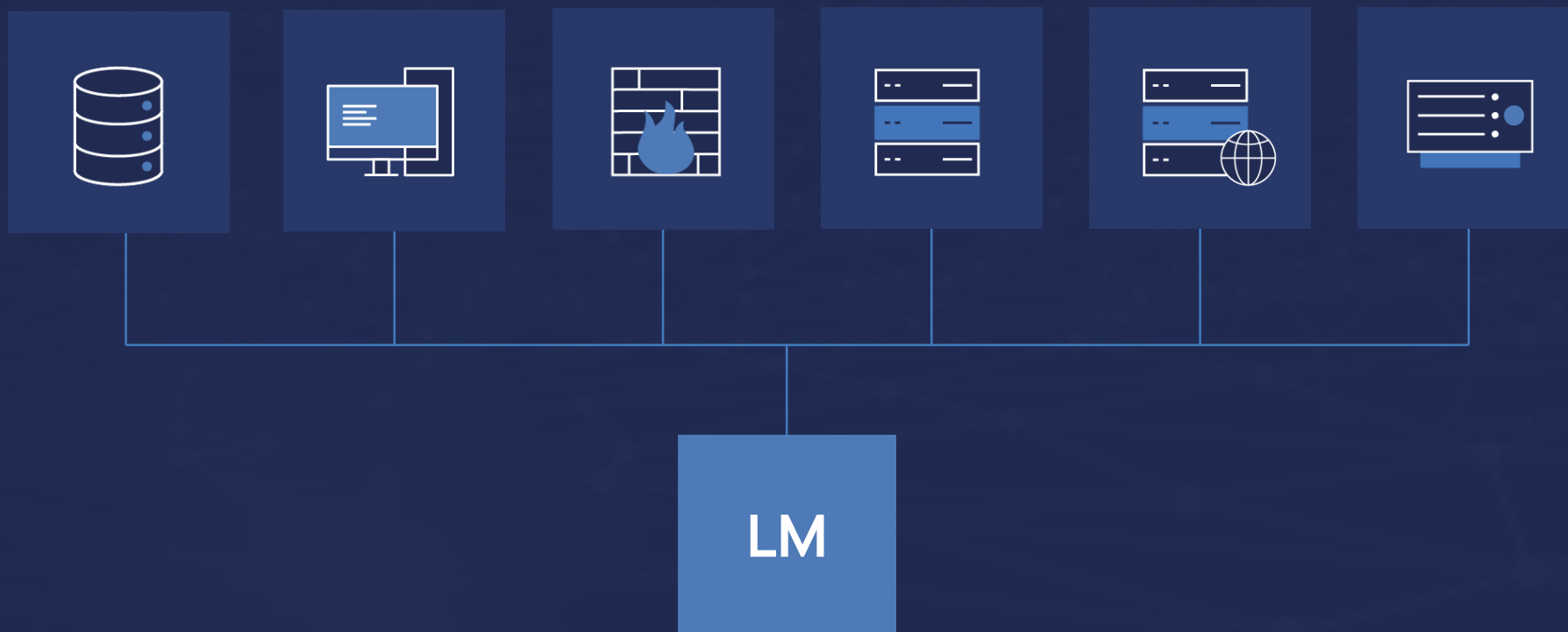
Зачем собирать логи



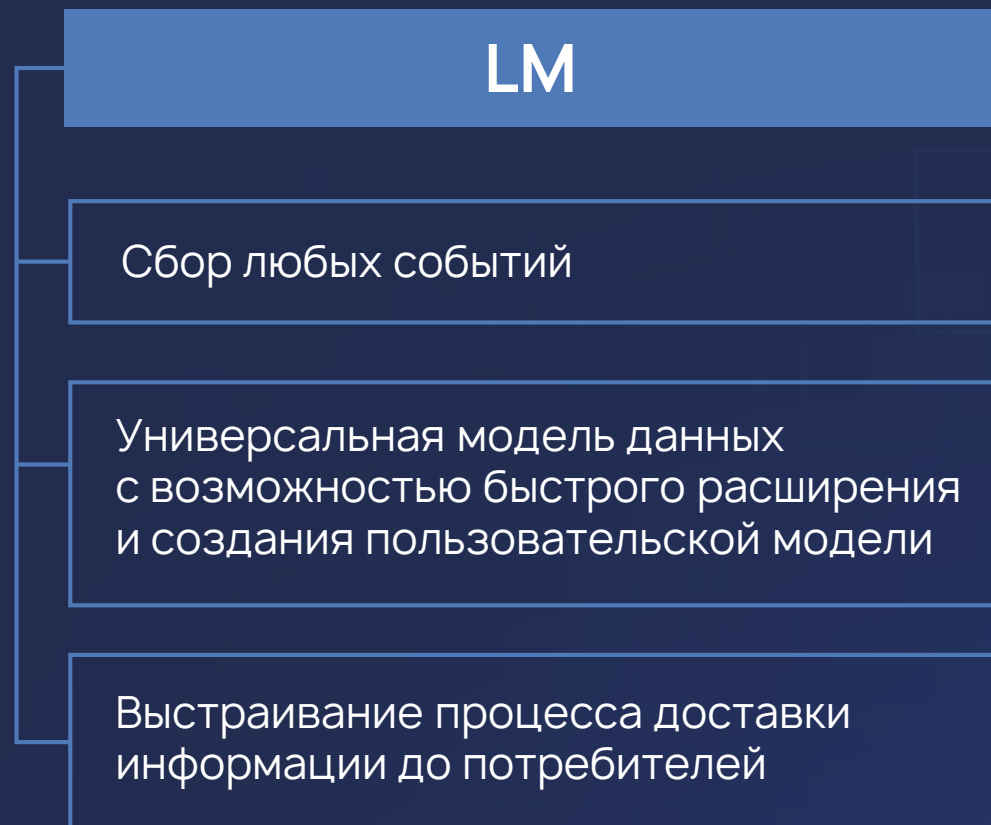
Собрать и обработать



Сбор и обработка событий



Сбор и обработка событий



Подключение новых источников

Решаемые задачи

Большой набор обработчиков
«из коробки»

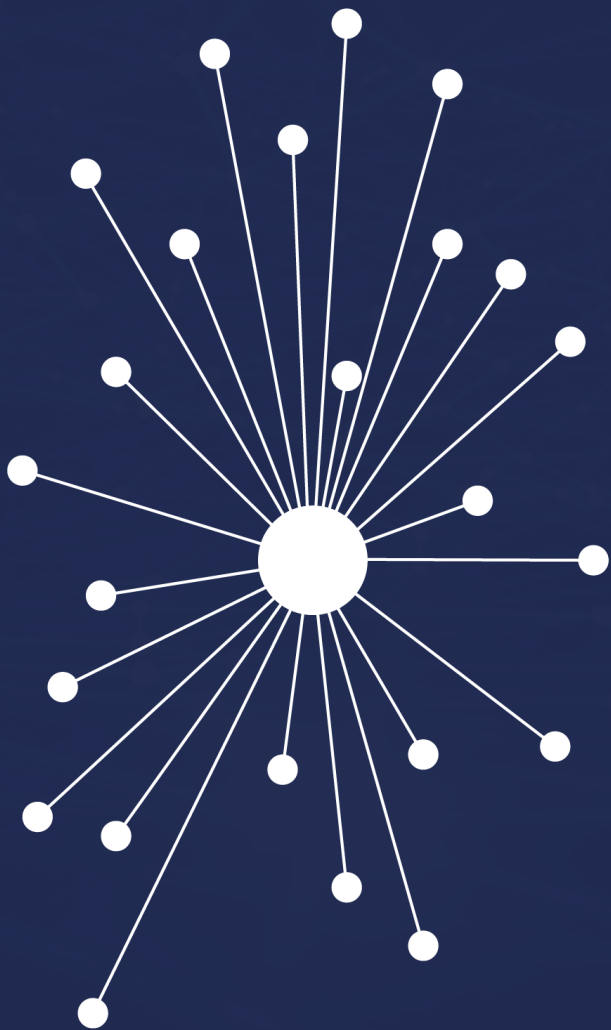
Механизм отладки правил нормализации

Отслеживание метрик на каждом этапе
обработки

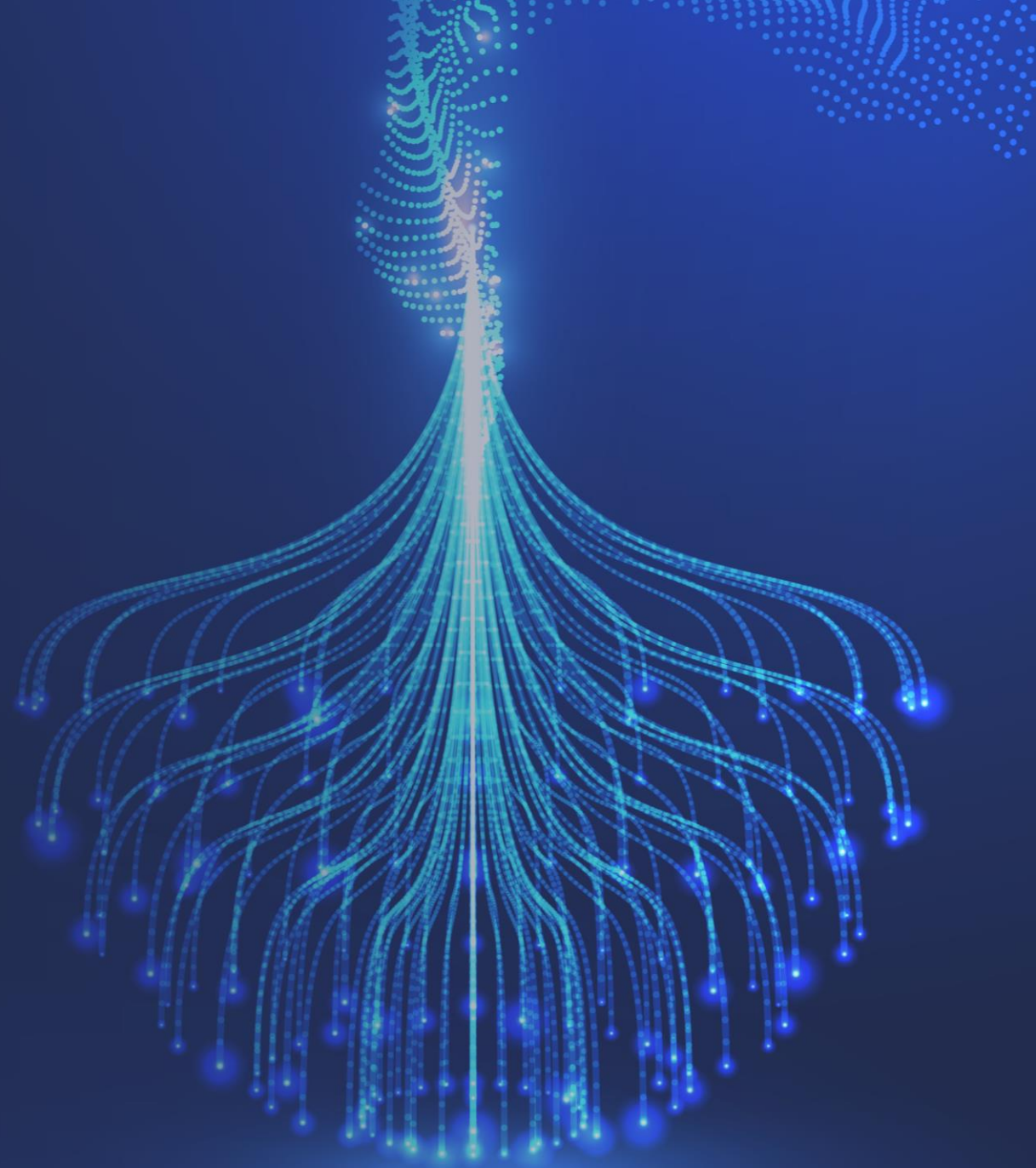
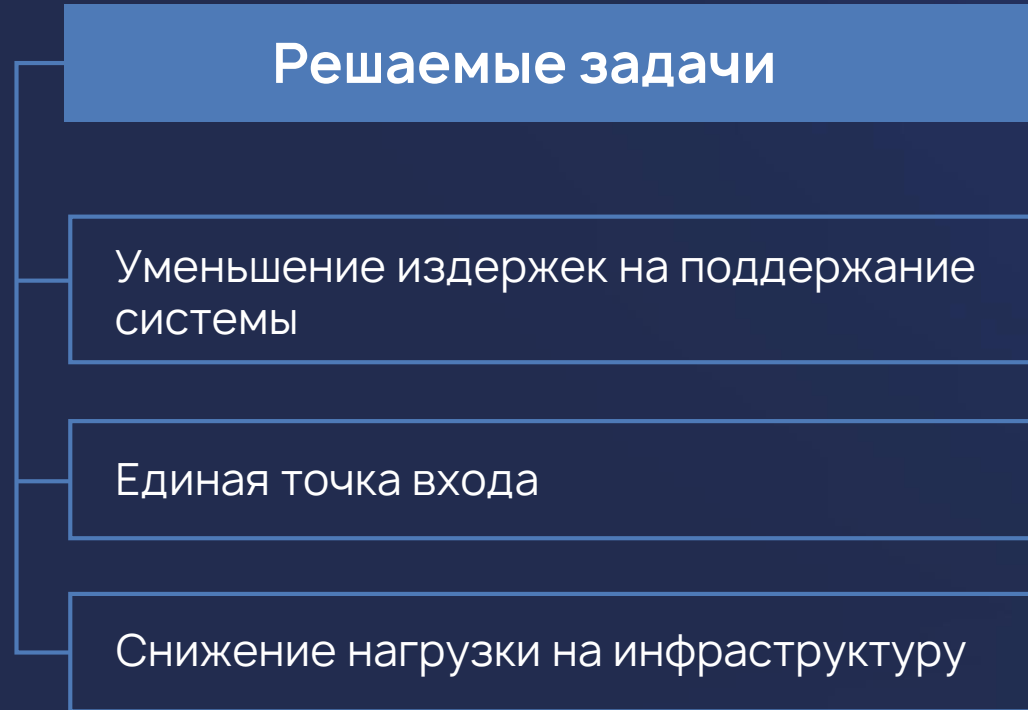
Выстраивание процесса обработки
и передачи событий

```
id: r-vision.ru/10-fall-logging
name: 10-fall-logging
version: 0.0.2111
filter: |
    .act == "login_failed"
group_by:
    - dhost
    - duser
on_event: |
    %state.count = int(%state.
correlate_when: |
    int!(%state.count) >= 10
tests:
    - name: 10 events with noise
```

Централизация



Преимущества





Для кого

Кому нужны журналы событий



IT – мониторинг состояния инфраструктуры, управление ресурсами, устранение неполадок и поиск их причин.



ИБ – SIEM, TI, DPI и другие системы. Мониторинг, расследование, сбор форензики.



Бизнес-юниты – подготовка аналитических отчетов для принятия решений по стратегическому планированию, управлению рисками, повышению эффективности IT-операций.

Задачи LM

Решаемые задачи

«Наблюдаемость»

Анализ данных

Расследование инцидентов

Снижение требуемых ресурсов

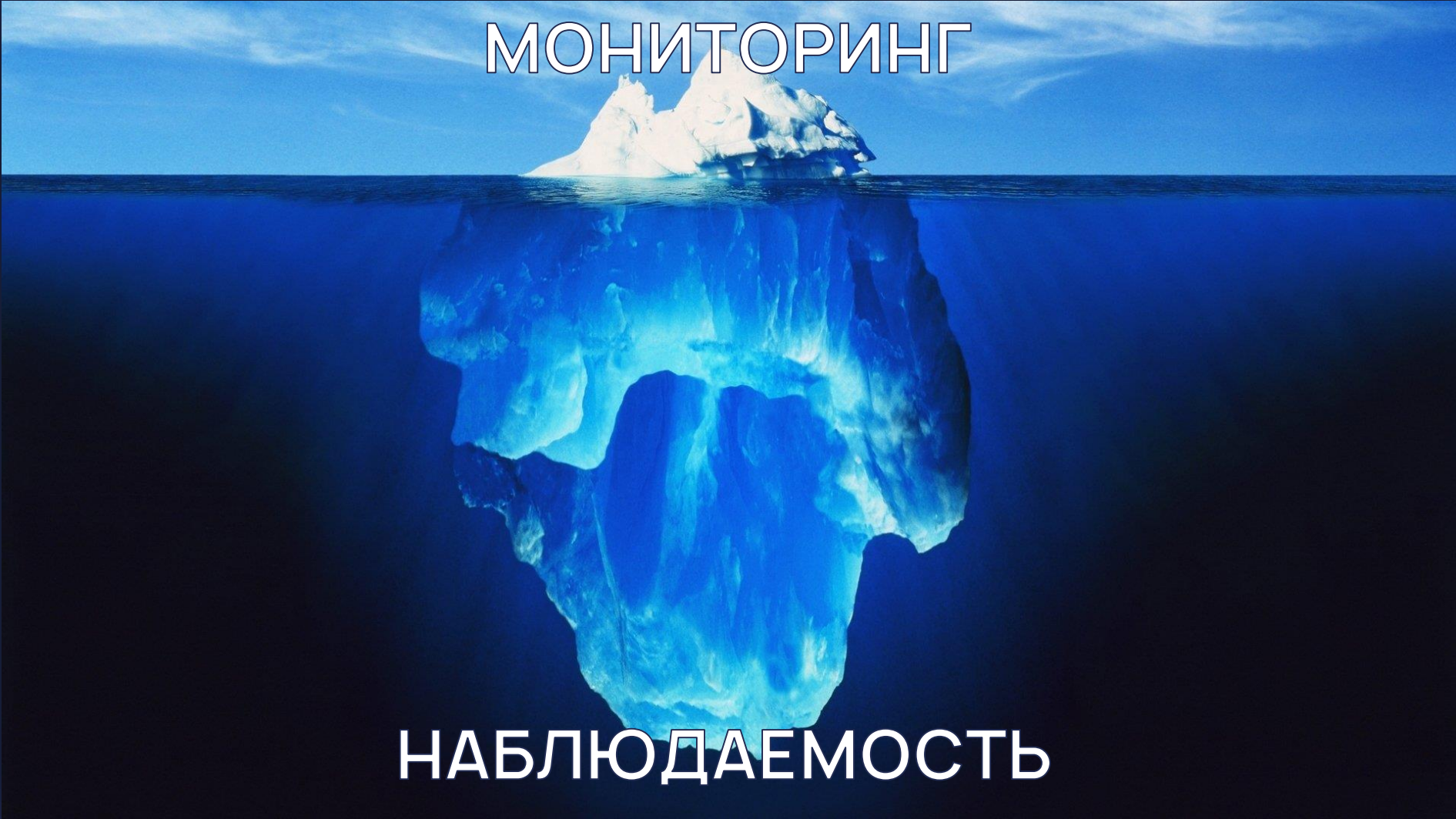
dproduct = "Microsoft Windows" AND "externalid" = 4625 AND outcome = "failure" AND duser != NULL



dproduct = "Microsoft Windows" AND "externalid" = 4625 AND outcome = "failure" AND duser != NULL



dproduct = "Microsoft Windows" AND "externalid" = 4625 AND outcome = "failure" AND duser != NULL

A photograph of an iceberg floating in a deep blue ocean under a clear sky. The small tip of the iceberg is visible above the water line, while the much larger, jagged mass of the iceberg is submerged below the surface. The water is a deep, dark blue, and the sky is a lighter blue with some wispy clouds. The horizon line is clearly visible, separating the water from the sky.

МОНИТОРИНГ

НАБЛЮДАЕМОСТЬ

Наблюдаемость

Задачи LM

Решаемые задачи

«Наблюдаемость»

Анализ данных

Расследование инцидентов

Снижение требуемых ресурсов

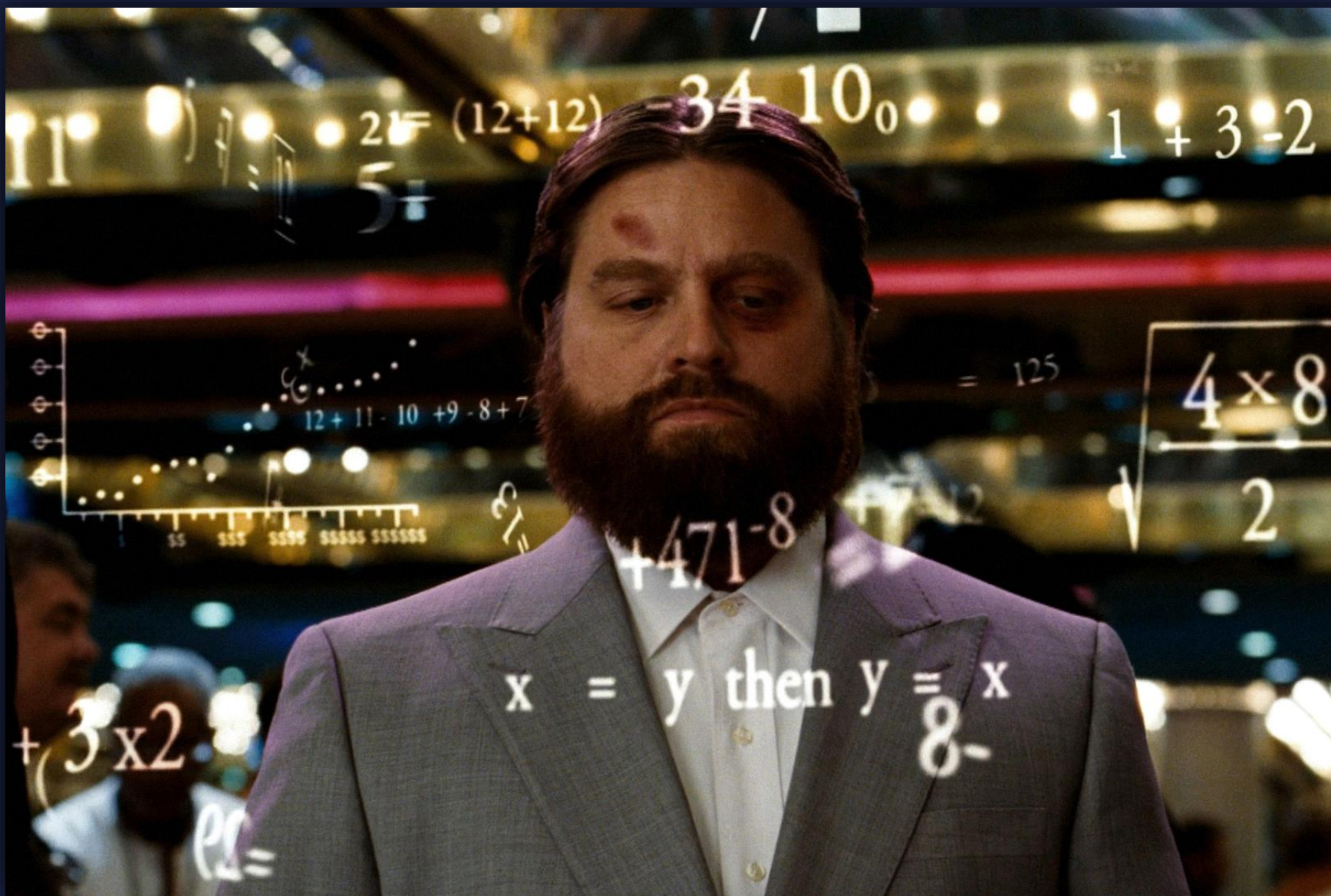
dproduct = "Microsoft Windows" AND "externalid" = 4625 AND outcome = "failure" AND duser != NULL



dproduct = "Microsoft Windows" AND "externalid" = 4625 AND outcome = "failure" AND duser != NULL



dproduct = "Microsoft Windows" AND "externalid" = 4625 AND outcome = "failure" AND duser != NULL



Анализ данных

Задачи LM

Решаемые задачи

«Наблюдаемость»

Анализ данных

Расследование инцидентов

Снижение требуемых ресурсов

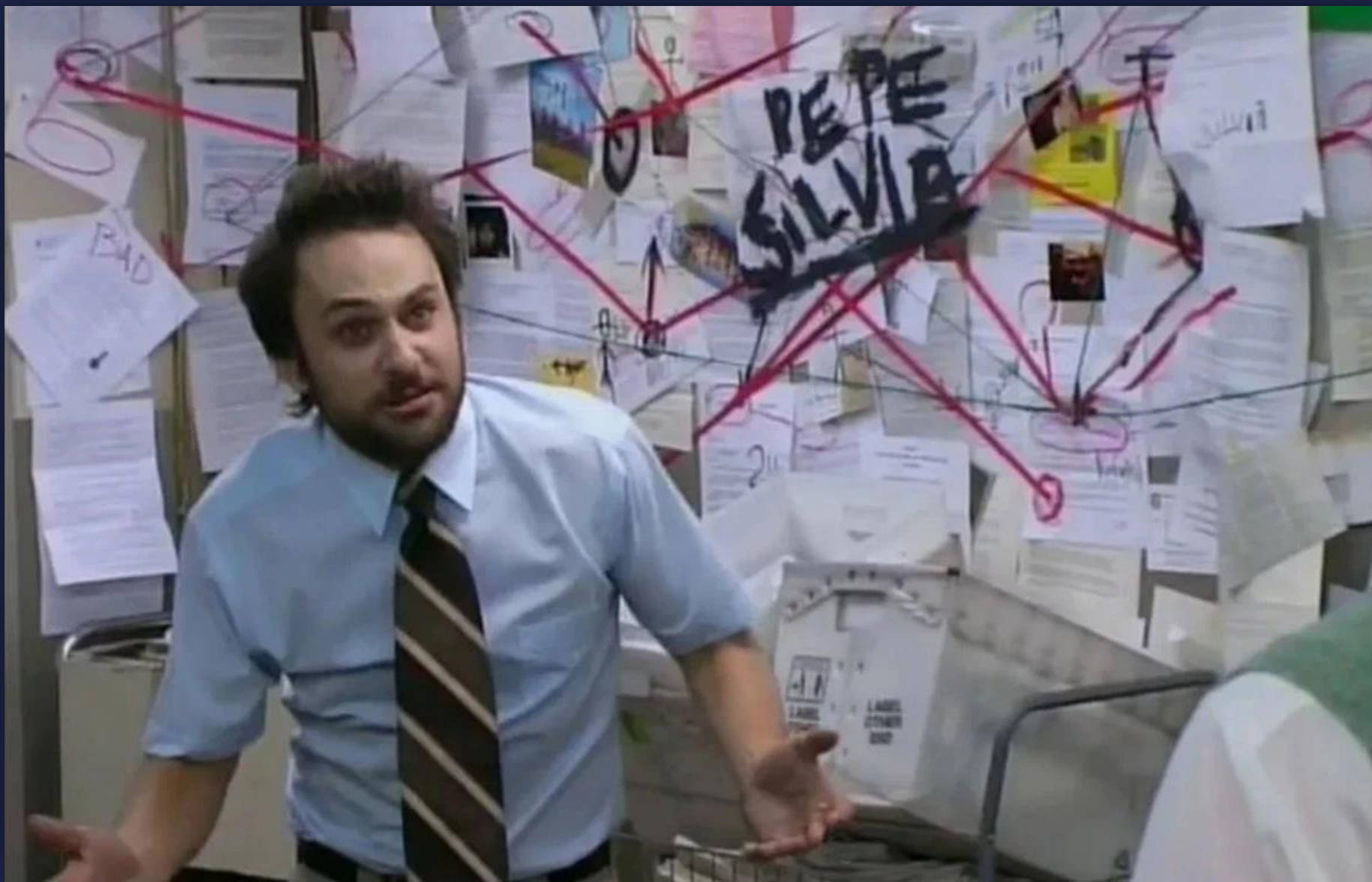
`dproduct = "Microsoft Windows" AND "externalid" = 4625 AND outcome = "failure" AND duser != NULL`



`dproduct = "Microsoft Windows" AND "externalid" = 4625 AND outcome = "failure" AND duser != NULL`



`dproduct = "Microsoft Windows" AND "externalid" = 4625 AND outcome = "failure" AND duser != NULL`



Расследование инцидентов

Задачи LM

Решаемые задачи

«Наблюдаемость»

Анализ данных

Расследование инцидентов

Снижение требуемых ресурсов

dproduct = "Microsoft Windows" AND "externalid" = 4625 AND outcome = "failure" AND duser != NULL



dproduct = "Microsoft Windows" AND "externalid" = 4625 AND outcome = "failure" AND duser != NULL



dproduct = "Microsoft Windows" AND "externalid" = 4625 AND outcome = "failure" AND duser != NULL

Задачи LM

Для пользователей

Удобная работа с системой,
визуализация данных

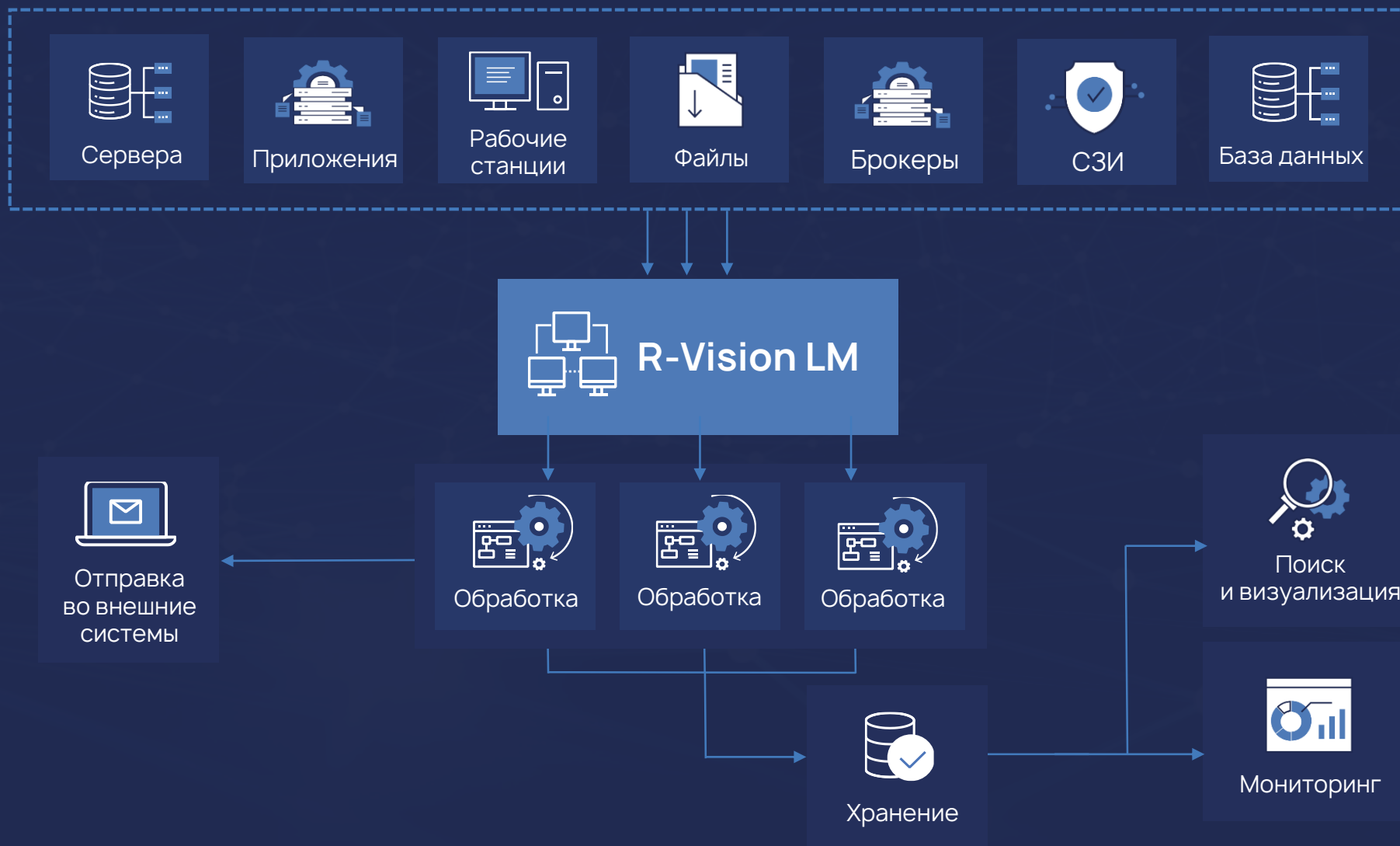
Минимизация затрат на обучение
работе с системой

Централизованное управление
обработкой событий, механизмы отладки

Масштабирование системы и настроек



Задачи, которые решает LM



R-Vision

 + 7 (499) 322 80 40

 sales@rvision.ru

 rvision.ru

 t.me/rvision_pro

 vk.com/rvision_ru

Подписывайтесь на наш
дайджест ИБ: rvision.ru/blog