



VB-Trend 2025

АНТИХРУПКОСТЬ

БИЗНЕСА

Импортозамещение SIEM

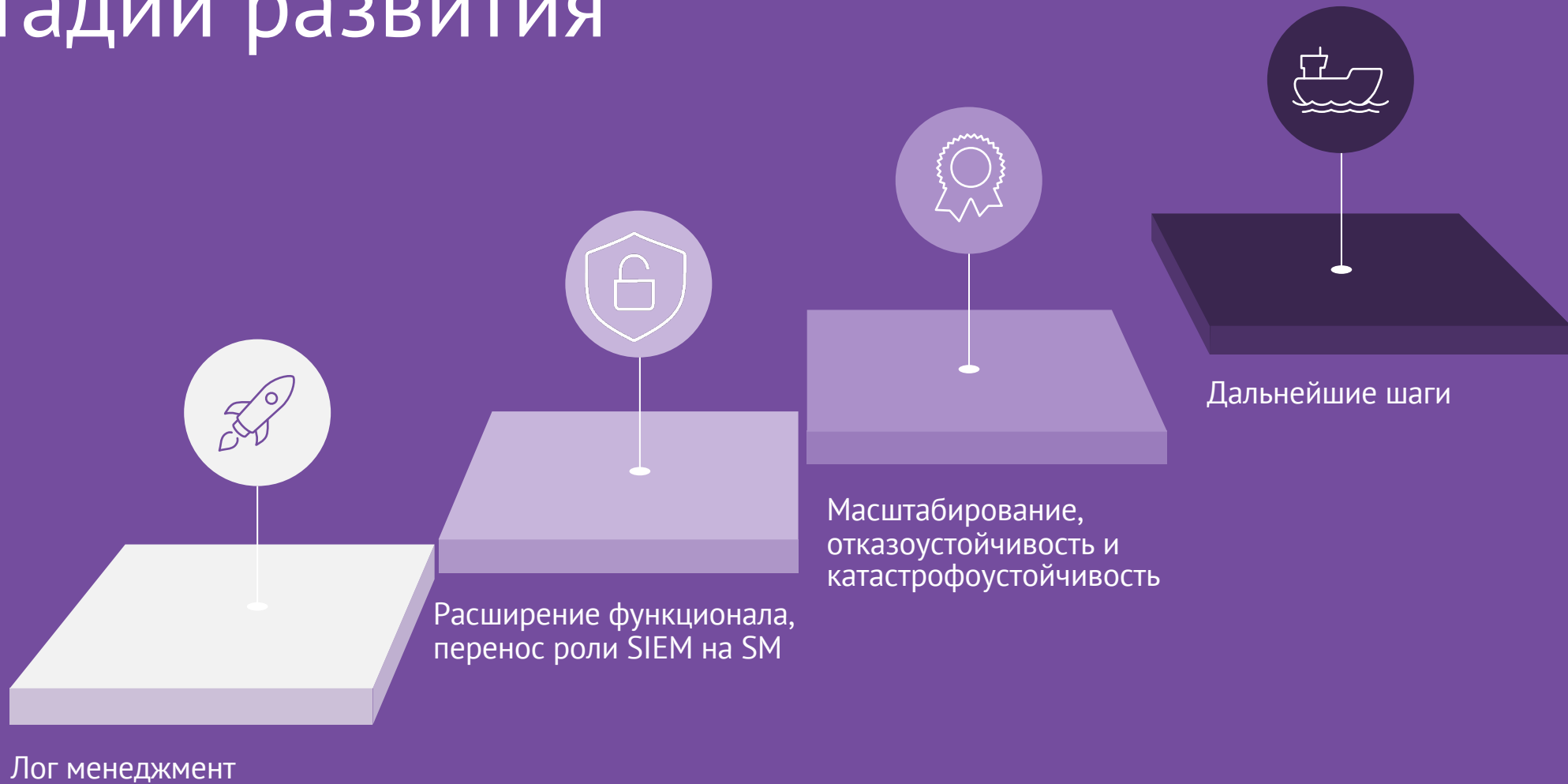
Внушительный Такой Банк



Мельников Илья
VolgaBlob



Стадии развития



Лог менеджмент

Долгосрочное хранение

Долгосрочное хранение информации, до 3 лет, при умеренных финансовых затратах

Ретроспективный поиск

Язык запросов должен предоставлять широкие возможности для поиска и построения корреляций по ретроспективным данным

Интеграционные возможности

Возможности интеграции с имеющимися источниками данных, включая сбор данных с действующего SIEM

Лог менеджмент, результат

- > Выполнена интеграция с действующим **SIEM** и **основными источниками** данных
- > Настроены **активы** инвентаризации
- > Предоставлены возможности для **ретроспективного** поиска и анализа данных

Потребность и выбор SIEM

Возможности поиска
Многофункциональный язык запросов

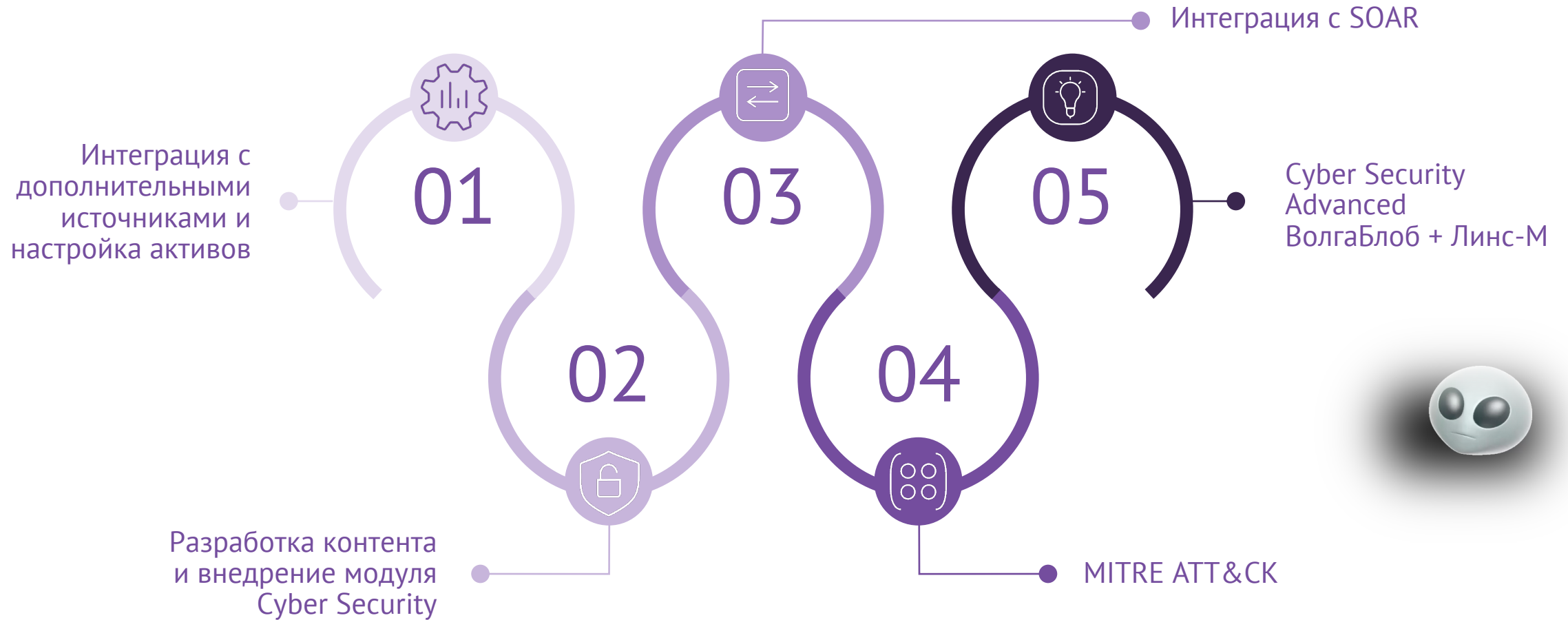
Вендорская поддержка
Помощь с запуском решения и обработка возникающих Feature Request

Работа с инцидентами
Понятный интерфейс, кастомизируемые рабочие процессы

Интеграции
Поиск во внешних хранилищах без переиндексации (Hadoop, Elasticsearch).

Интеграция с SOAR для передачи инцидентов

Построение SIEM



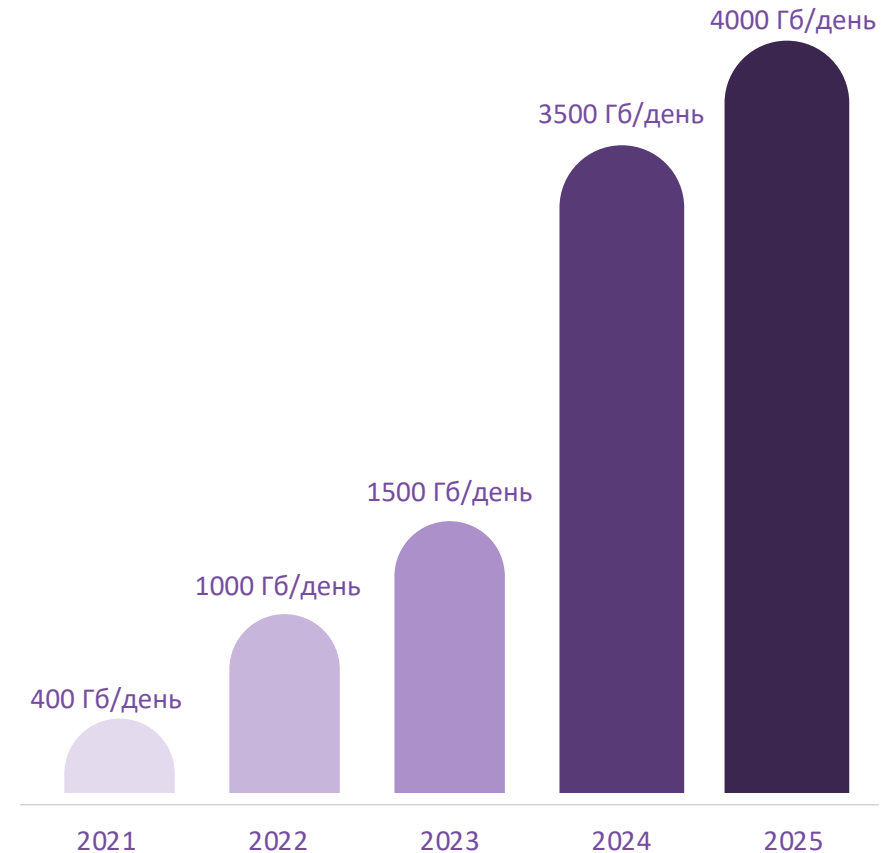
Задачи замещения SIEM

Интеграции с источниками

В процессе развития системы планомерно развивается набор источников данных для Smart Monitor.

В настоящий момент насчитывается более **100** типов источников данных с общим потоком данных ~ **4 ТБ** в сутки.

Насчитывается более **400** тысяч активов инвентаризации в системе

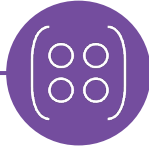


Покрытие корреляционной
логикой

300+
правил

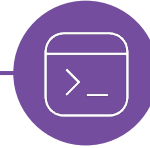


MITRE ATT&CK



Приоритезация

Приоритезация техник для покрытия в SIEM



Детектирование

Сопоставление техник с действующими правилами



Срабатывания

Фиксация срабатываний техник



Аналитика

Дополнительная аналитика по метаданным MITRE



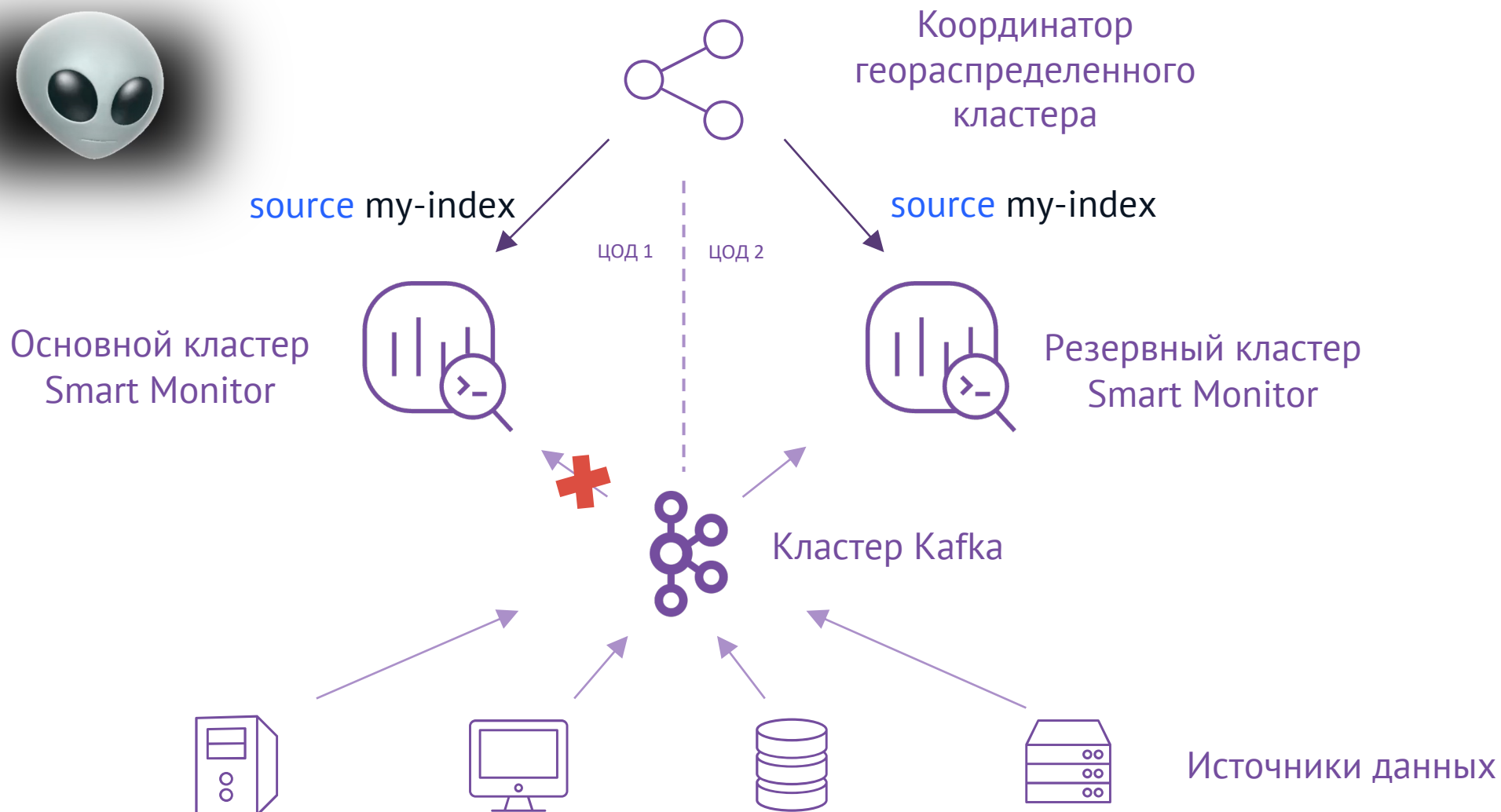
Инциденты

Фиксация инцидентов на основании метаданных

Масштабирование и отказоустойчивость



Масштабирование и отказоустойчивость



Планы

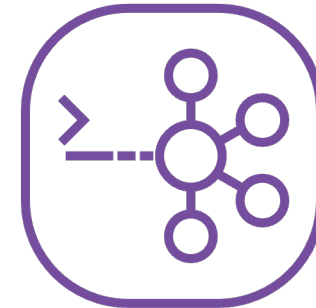


User Behavior Analytics

Пилотный проект по внедрению модуля.

Kafka Manager

Ввод в эксплуатацию партнерского модуля для контроля за состоянием Kafka



Спасибо
за внимание!

Буду рад ответить на ваши вопросы

