



VB-Trend 2025

АНТИХРУПКОСТЬ

БИЗНЕСА

MSSP на SM

Опыт T1 Холдинг



Мельников Илья
VolgaBlob



Шляпин Алексей
T1 Холдинг

Предпосылки к реализации проекта



Внутренние

Внутренняя
потребность группы
компаний в **SIEM** и
SOC

Внешние

Запросы партнеров
на **экспертизу** по
мониторингу и
реагированию

Критерии выбора решения



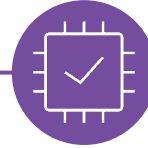
Мультитенантность

Возможность работы с несколькими клиентами



Язык запросов

Функциональный язык запросов, возможность реализации сложной корреляционной логики



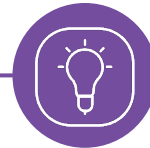
Ролевая модель

Полноценная поддержка разграничения доступов для клиентов и операторов SOC



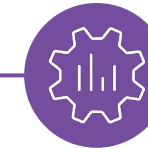
Импортозамещение

Решение в реестре отечественного ПО



Компетенции

Наличие необходимых хард-скиллов в команде



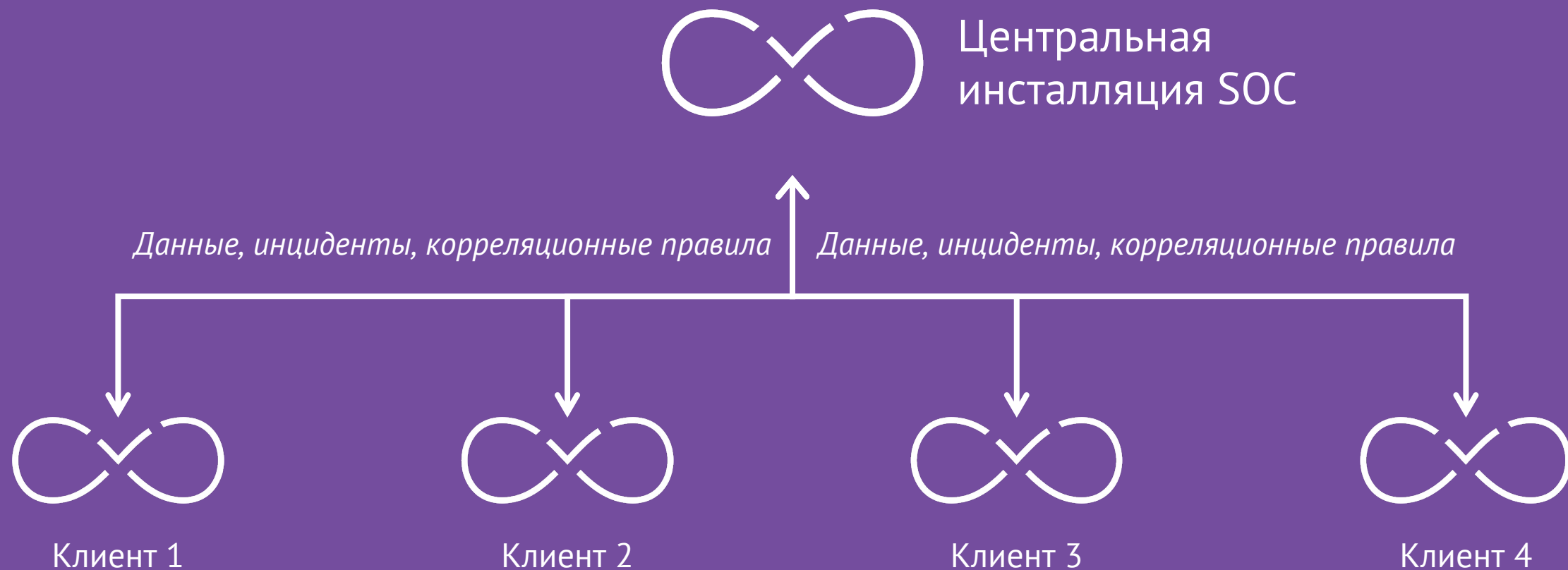
Ресурсы

Минимизация ресурсов на внедрение и дальнейшее сопровождение

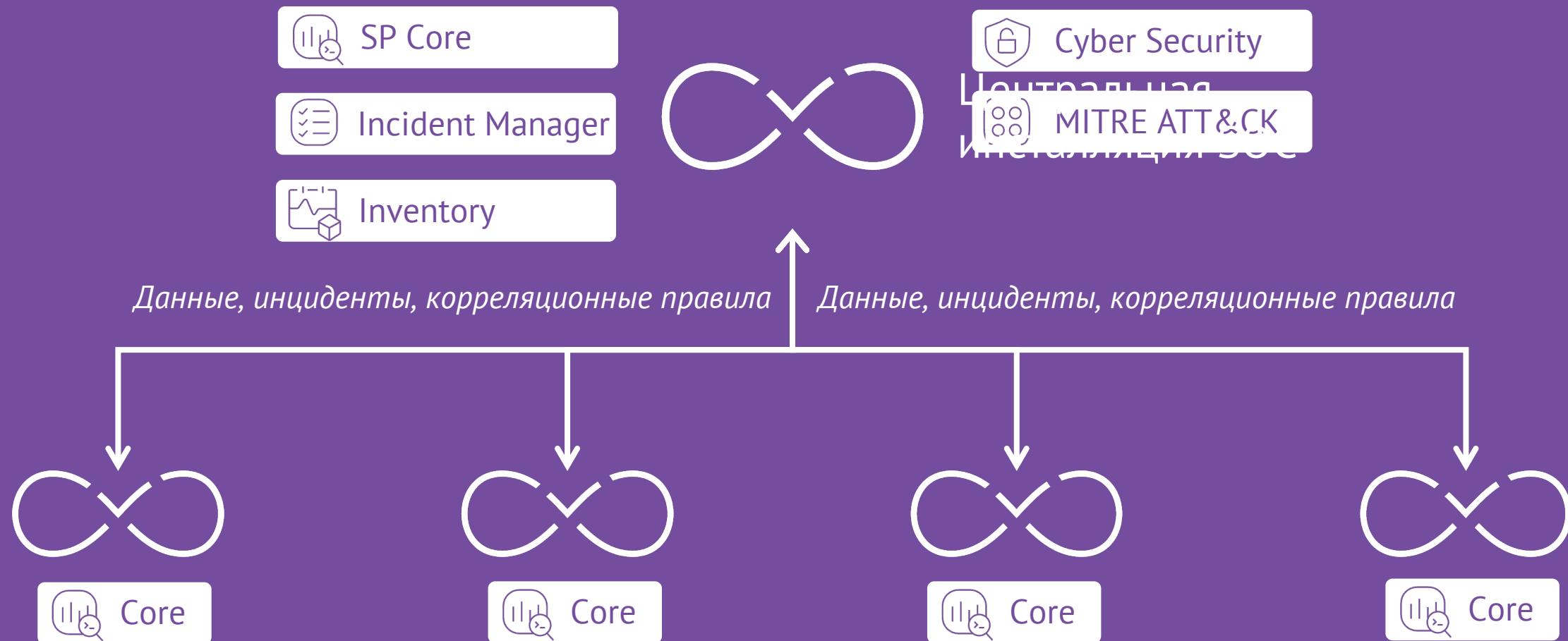
Цели проекта

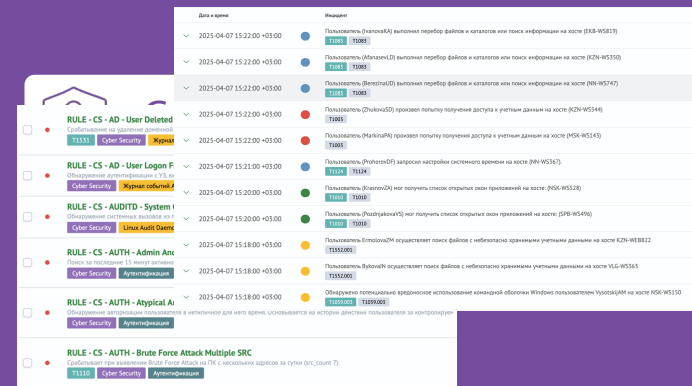


Режим Service Provider



Режим Service Provider





Данные, инциденты, корреляционные правила



ПРЕИМУЩЕСТВА

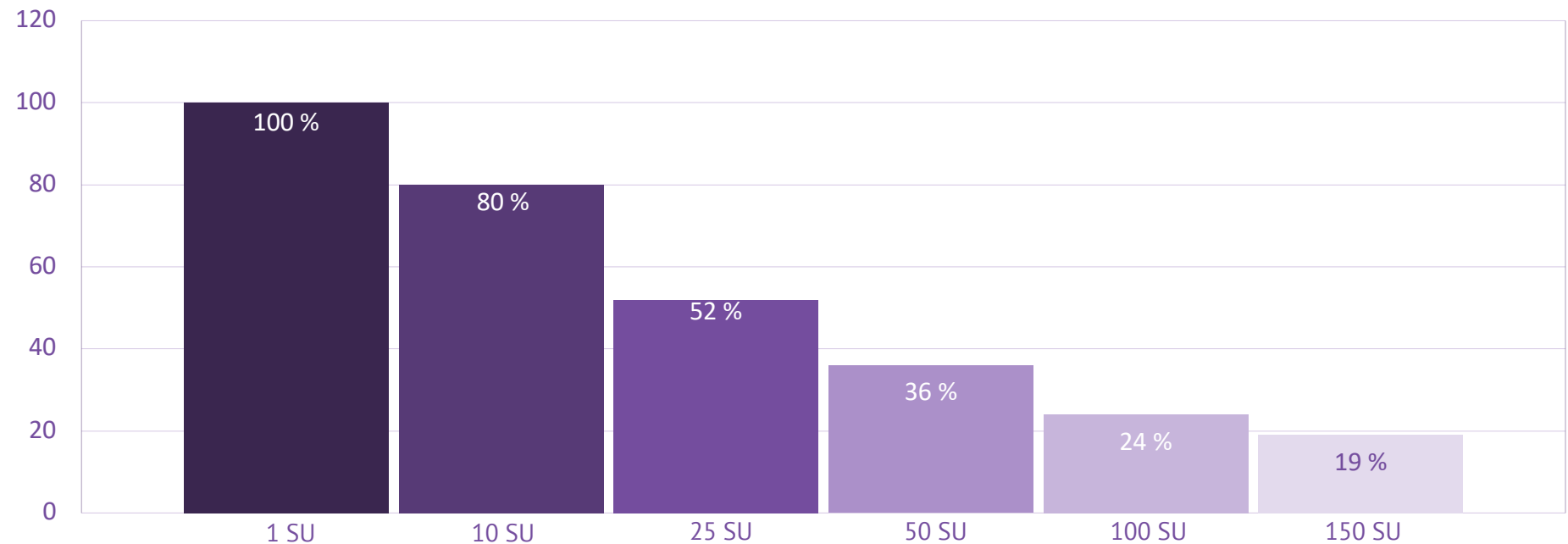
Технические

- **унификация решения**, включая коннекторы и контентную часть
- **архитектурная гибкость**, различные схемы подключения
- контроль за состоянием компонентов системы из **единой консоли** Самомониторинга

ПРЕИМУЩЕСТВА

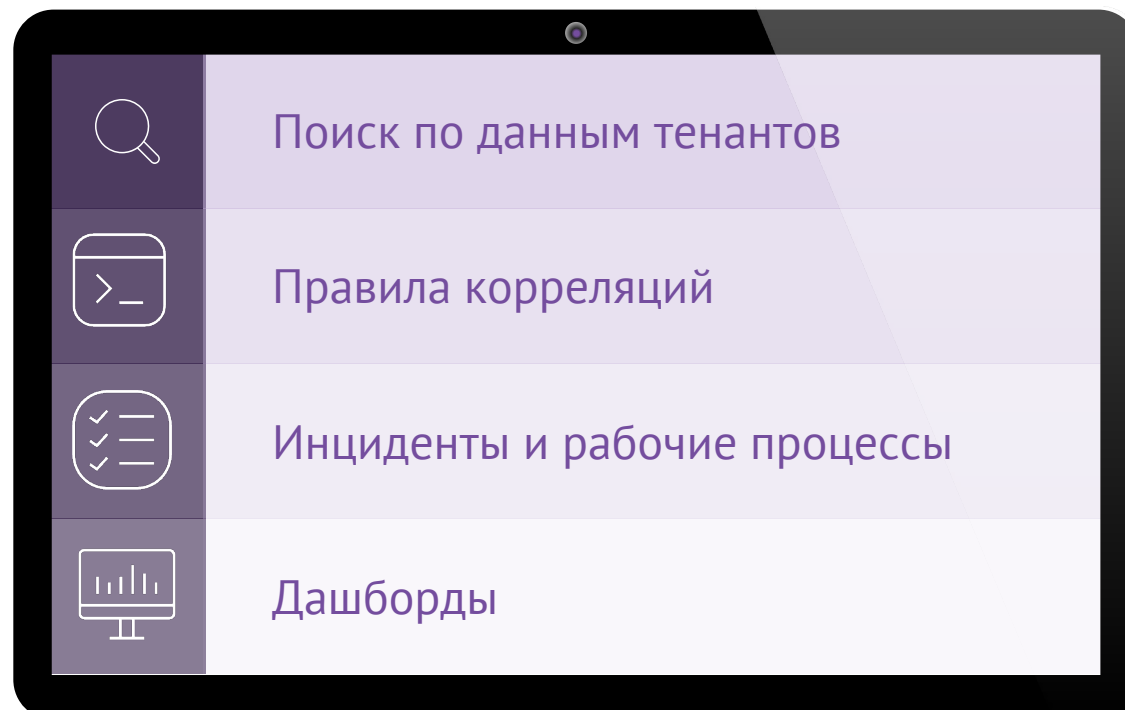
Экономические

Стоимость Smart Unit с учетом объема закупки

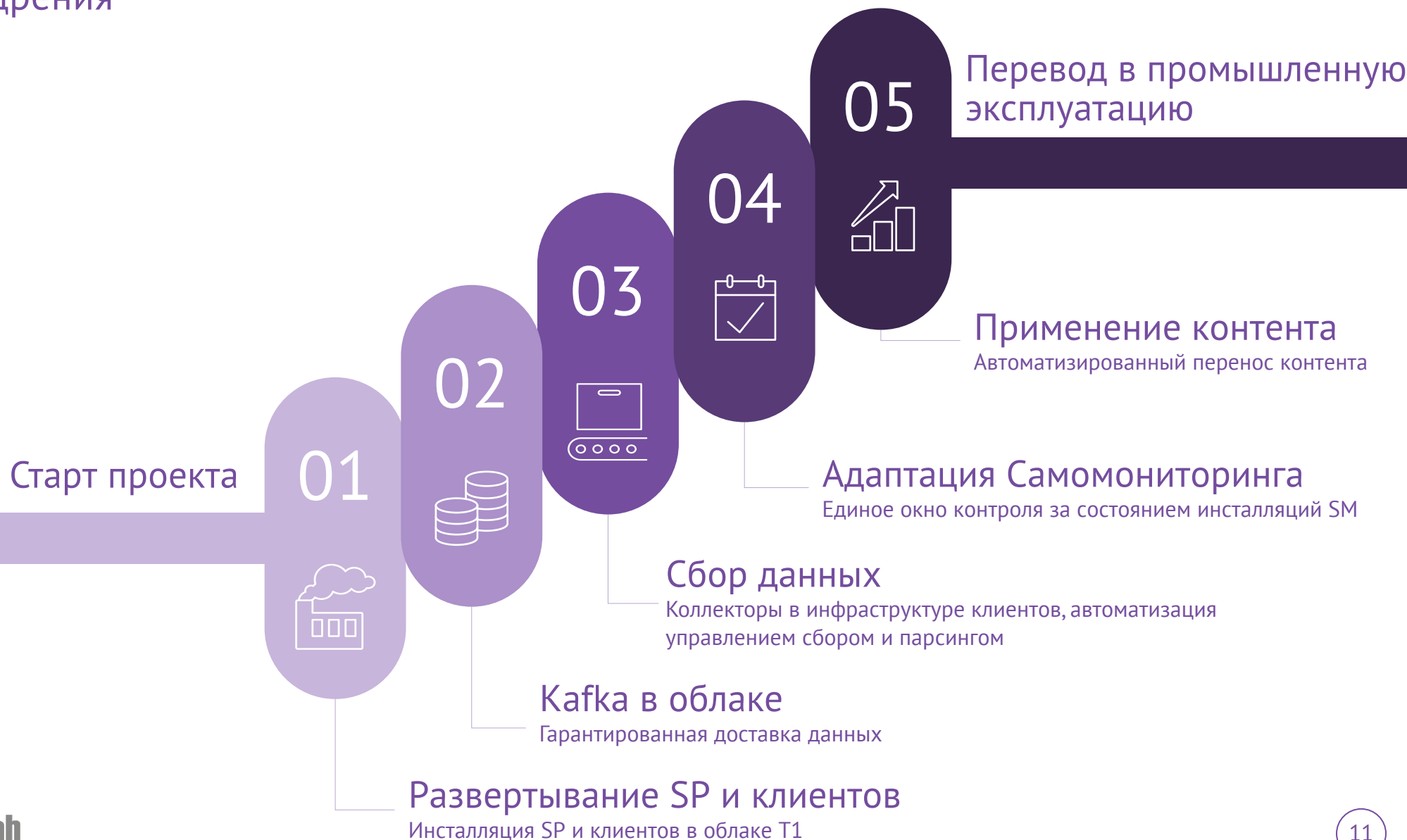


ПРЕИМУЩЕСТВА

Организационные



Шаги внедрения





Развертывание



Smart Monitor

Клиент 1
SM Core



Центральная инсталляция SOC
Контентные и функциональные модули



Клиент 2
SM Core



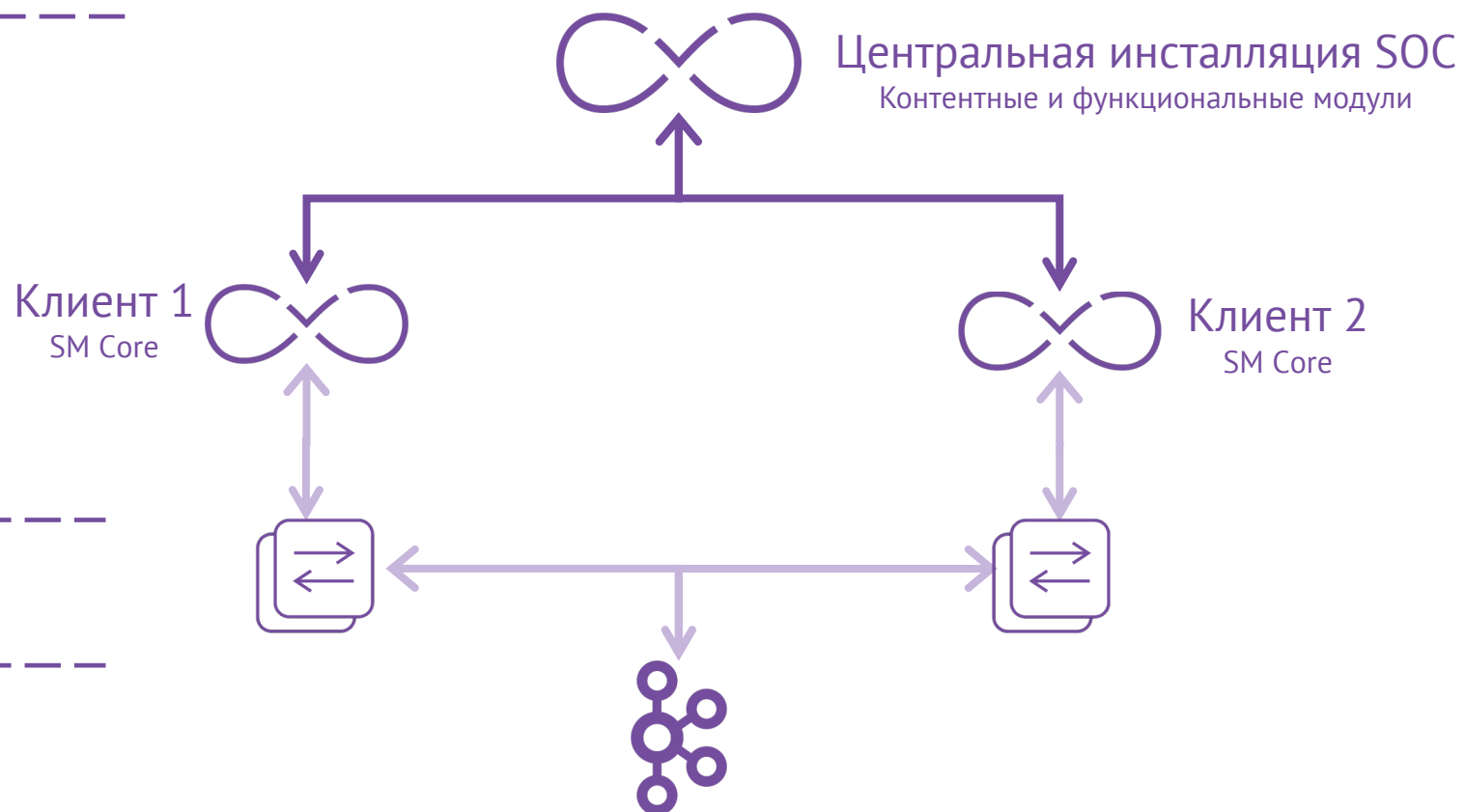
Kafka



Smart Monitor

Слой парсинга и
нормализации данных

Kafka



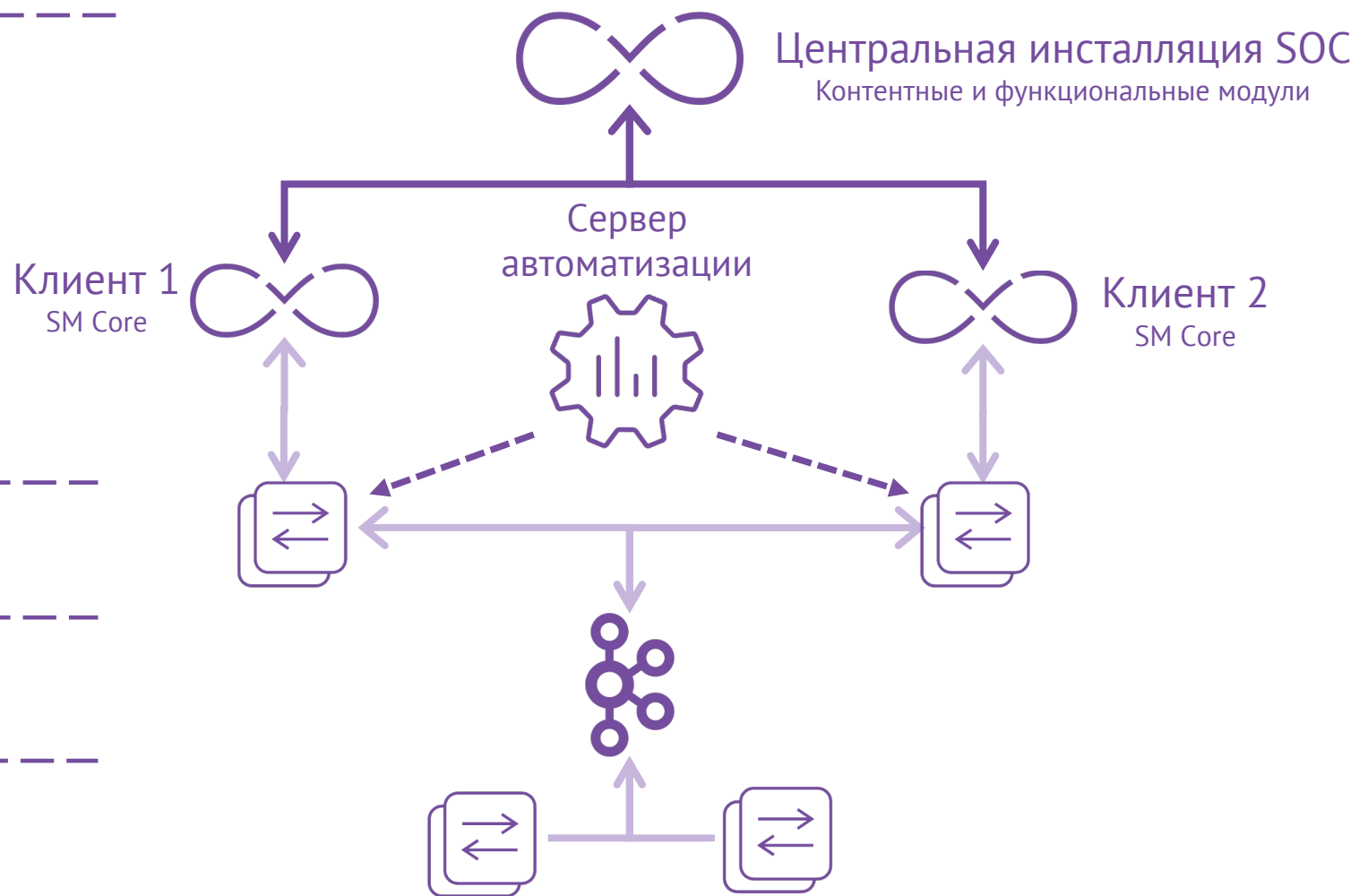
Сбор данных

Smart Monitor

Слой парсинга и
нормализации данных

Kafka

Слой сбора данных



Самомониторинг

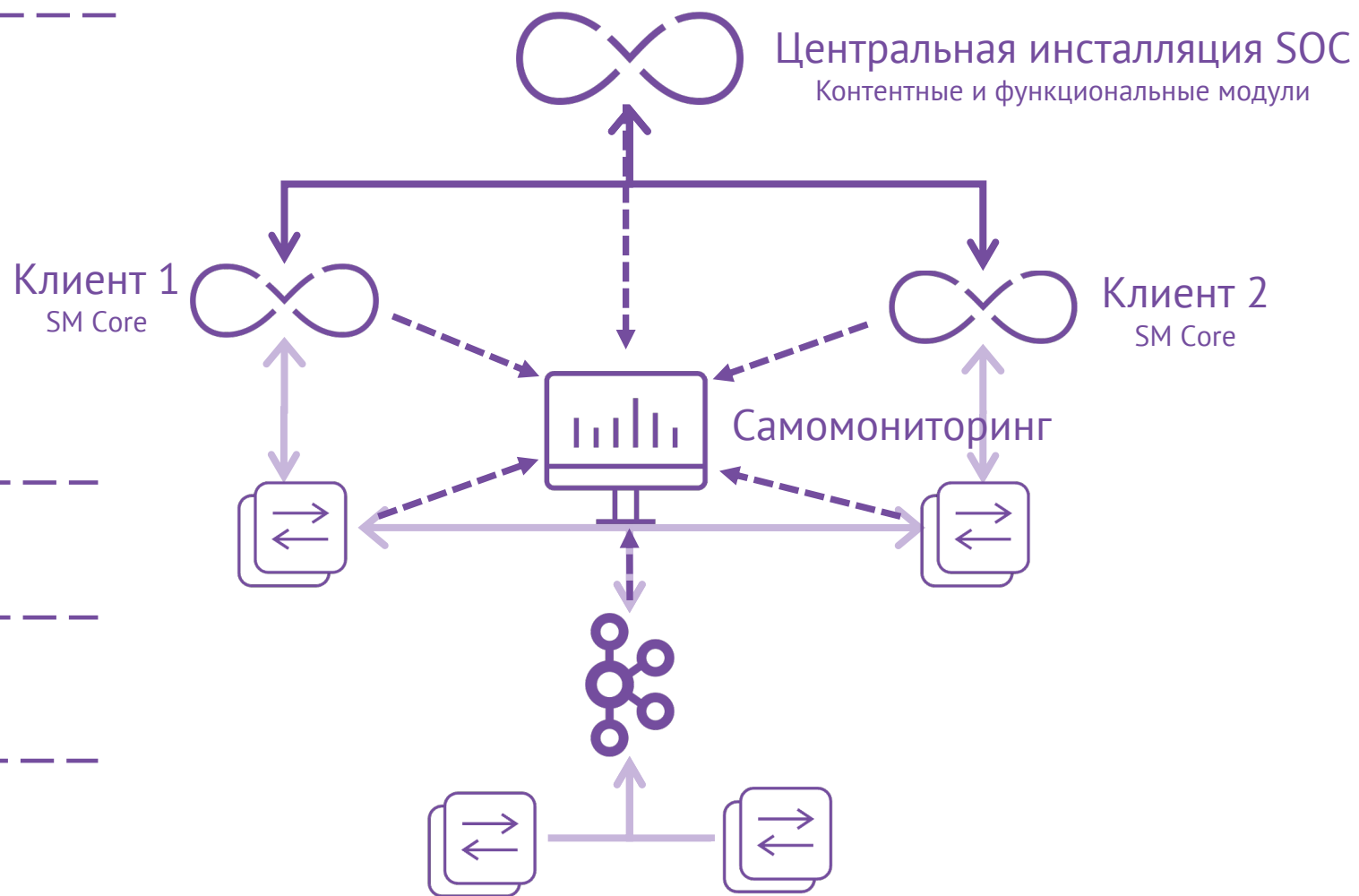


Smart Monitor

Слой парсинга и
нормализации данных

Kafka

Слой сбора данных





- переиспользование имеющихся правил на уровне Сервис провайдера
- автоматизированная настройка Активных действий Smart Monitor
- добавление метаданных в модуль MITRE ATT&CK на основании поисковых запросов

Промежуточные итоги



Подключение клиентов

Подключение пилотной группы клиентов



Доступ для всех бизнес-единиц

Гранулярная ролевая модель



Единое окно реагирования

Для клиентов и операторов SOC



Модель масштабирования

Подключения новых клиентов



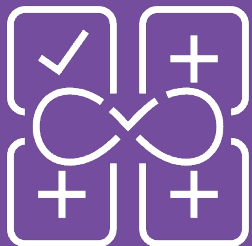
Архитектурная гибкость

Отработаны разные схемы подключения



Промышленная эксплуатация

Дальнейшие перспективы

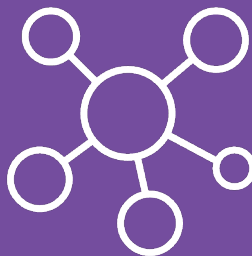


Автоматизация развертывания тенантов

Сокращение трудозатрат на подключение к SOC

Развитие контентной базы

Внутренняя экспертиза для клиентов, применение
>500 правил



Масштабирование

Подключение к сервису новых клиентов

Спасибо за внимание!

Будем рады ответить на ваши
вопросы

