

Нейрохирургия от Solar JSOC,
или Как мы меняли SIEM
на непрерывном сервисе

SOC
FORUM
2023



АНДРЕЙ ЕРЕГИН

ОДИН ПЕРЕЕЗД РАВЕН ДВУМ ПОЖАРАМ

ПОСТАНОВКА ЗАДАЧИ

>120

ТИПОВ ИСТОЧНИКОВ

>500

ПРАВИЛ КОРРЕЛЯЦИИ

- МУЛЬТИТЕНАНТНОСТЬ
- ГИБКАЯ НАСТРОЙКА ХРАНЕНИЯ
- ПРОДУМАННЫЙ КОРРЕЛЯТОР
- СБОР СОБЫТИЙ РАЗЛИЧНЫМИ МЕТОДАМИ
- ИНТЕГРАЦИЯ С ВНЕШНИМИ СИСТЕМАМИ
- МОДЕЛЬ АКТИВОВ
- API

- СЕТЕВАЯ МОДЕЛЬ
- КАТЕГОРИЗАЦИЯ

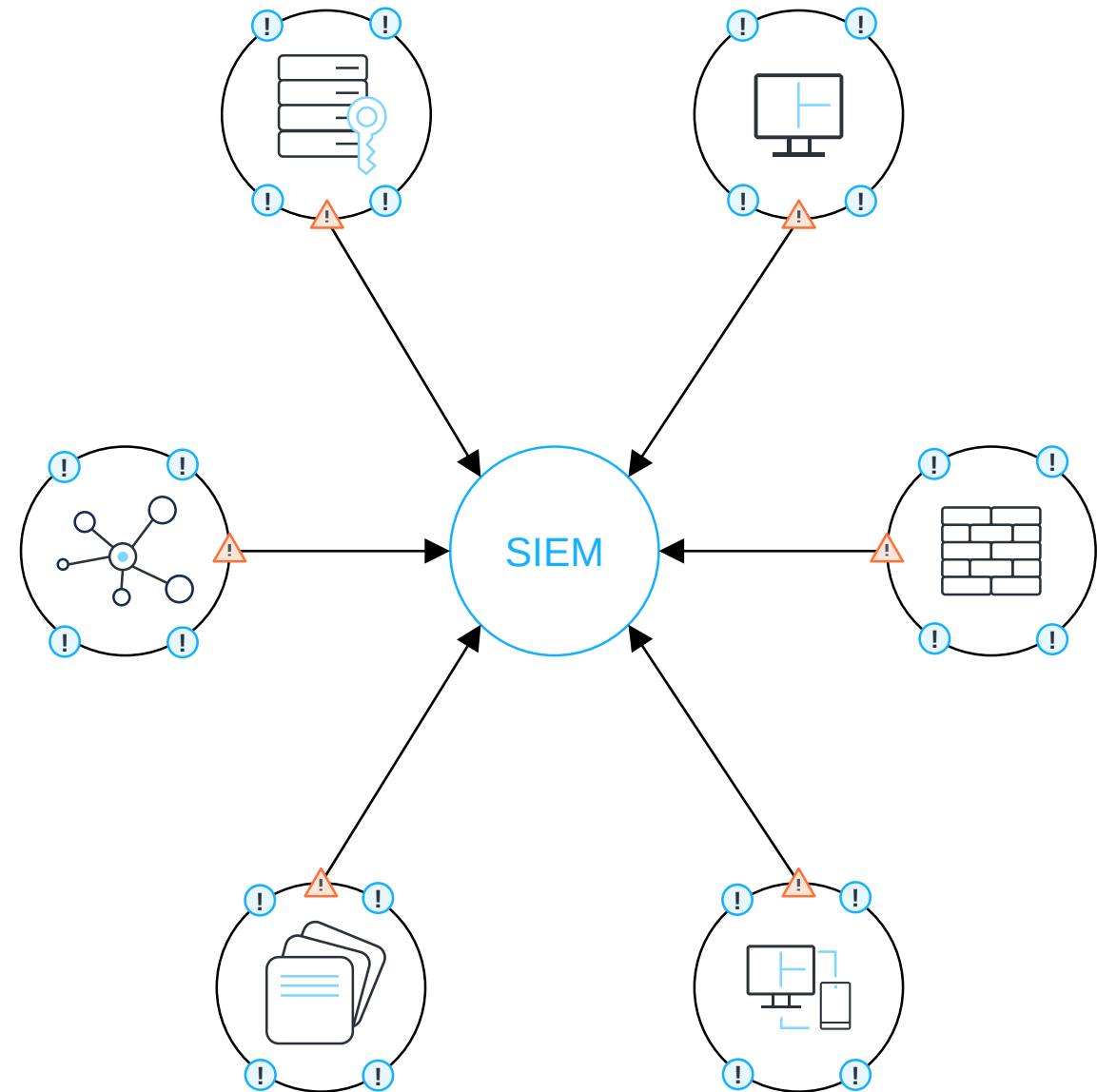
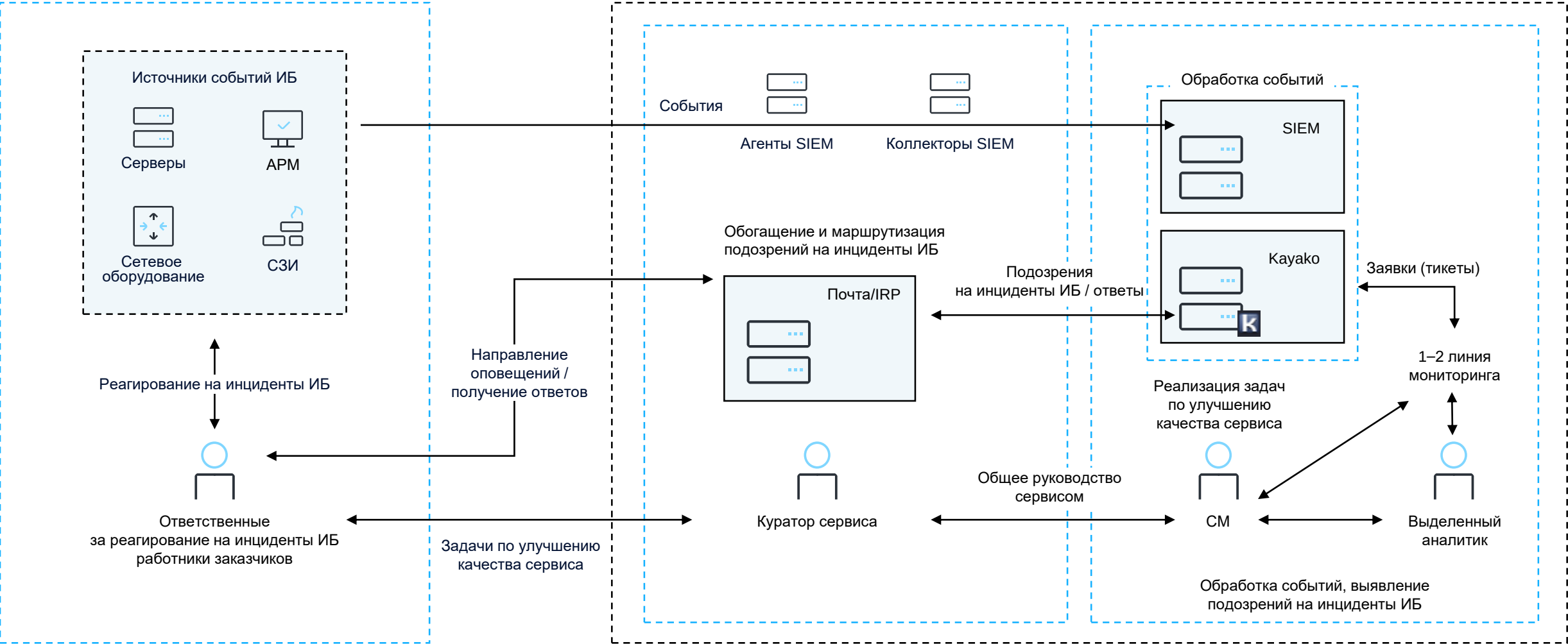


Схема работы Solar JSOC



ОТДЕЛ ОБРАБОТКИ
ИНЦИДЕНТОВ

Расследование инцидентов
Выгрузка отчетов

ОТДЕЛ
АНАЛИТИКИ

Расследование инцидентов
Настройка регулярной отчетности
Создание и тестирование контента
Подключение источников

ОТДЕЛ
АДМИНИСТРИРОВАНИЯ

Мониторинг состояния
инфраструктуры
Взаимодействие с вендором

ОТДЕЛ УПРАВЛЕНИЯ
СЕРВИСАМИ SOC

Проверка полноты оповещений
Анализ отчетности

[01]

Подключение заказчиков

[02]

Обучение взаимодействию
с ClickHouse

[03]

Регламентирование
процесса разработки

[04]

Разработка процесса
тестирования контента

[05]

Описание процесса
подготовки отчетности

[06]

Проработка системы отслеживания
состояния инсталляции

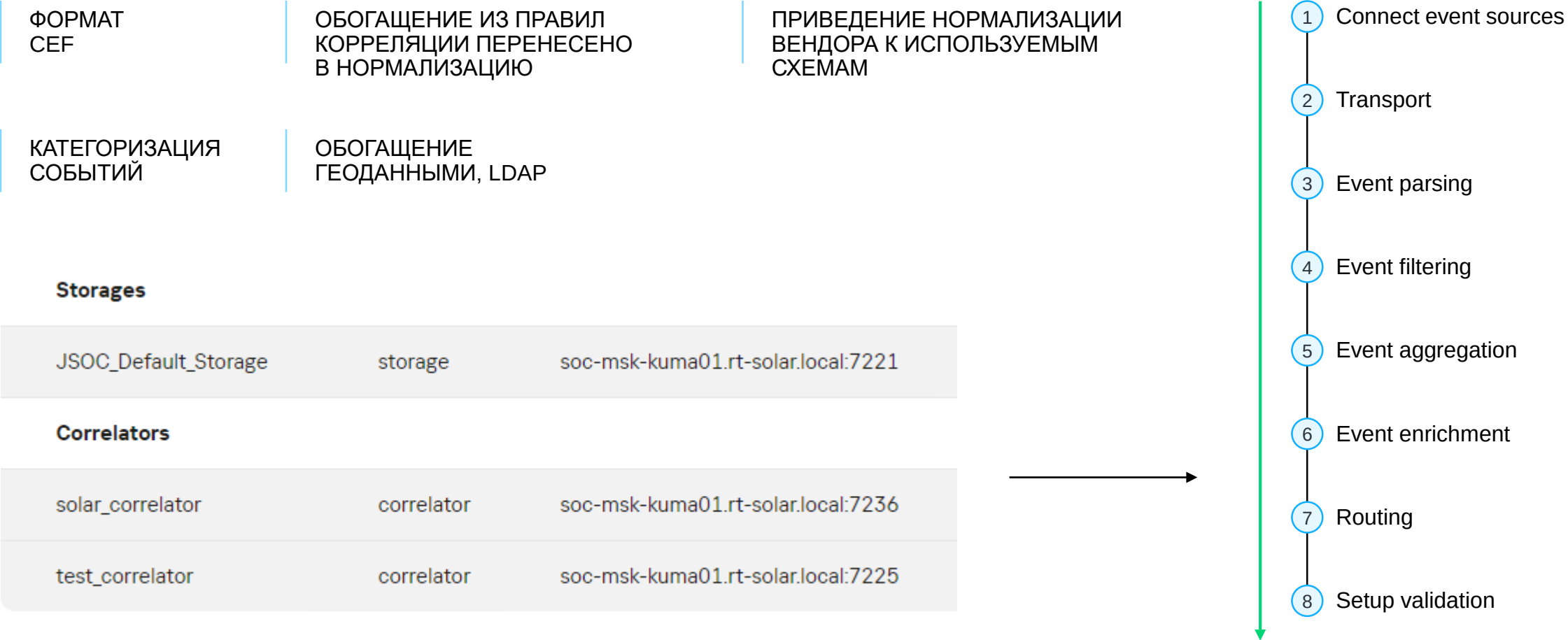
[07]

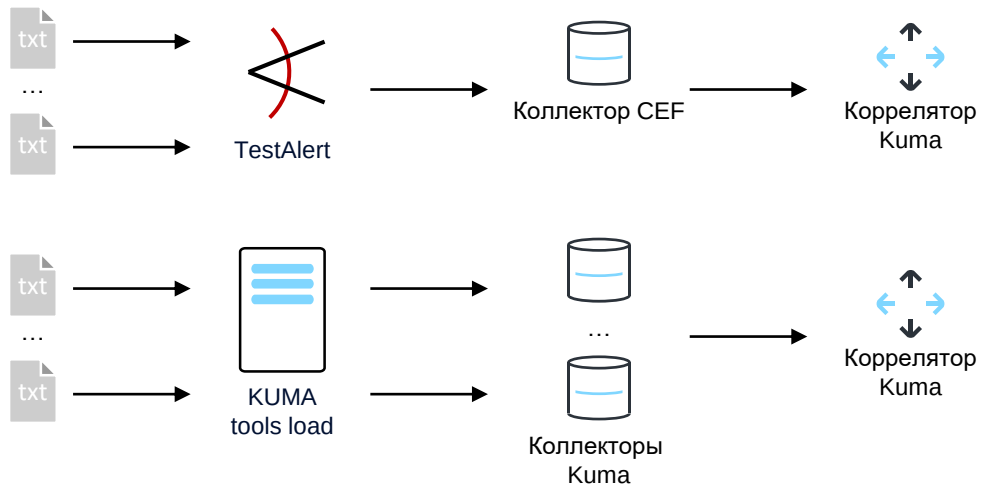
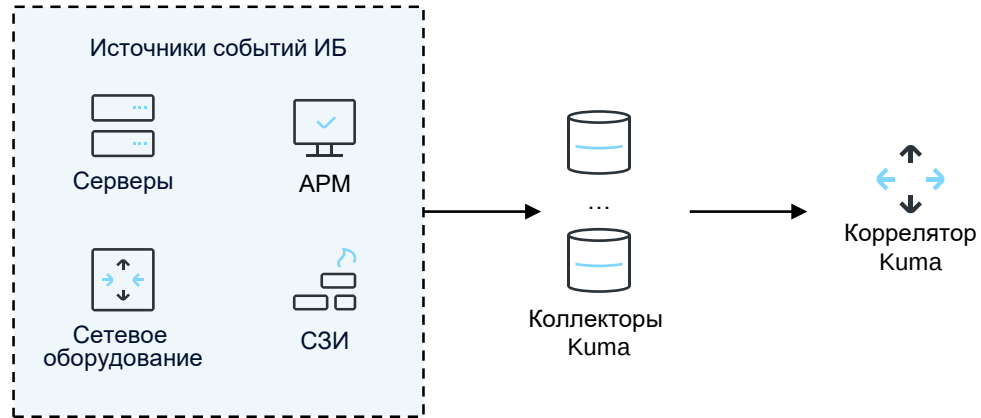
Создание системы мониторинга
состояния источников событий

СТАРТ РАБОТ

КОРРЕЛЯЦИОННЫЕ МЕХАНИЗМЫ
ОПЕРАТОРЫ ПОИСКА
ЛОГИЧЕСКИЕ КОНСТРУКЦИИ
ВЗАИМОДЕЙСТВИЕ С СОБЫТИЯМИ И РЕСУРСАМИ

УСЛОВНЫЙ ОПЕРАТОР [ИСПРАВЛЕНО]
КАТЕГОРИЗАЦИЯ
УСЛОВИЯ НА СЕТЕВУЮ МОДЕЛЬ
ПОДСЧЕТ УНИКАЛЬНЫХ ЗНАЧЕНИЙ [ЗАМЕНА]





ОДНОВРЕМЕННОЕ ТЕСТИРОВАНИЕ
НОРМАЛИЗАЦИИ И КОРРЕЛЯЦИИ

НАГРУЗОЧНОЕ ТЕСТИРОВАНИЕ

ТЕСТИРОВАНИЕ ПО РАСПИСАНИЮ

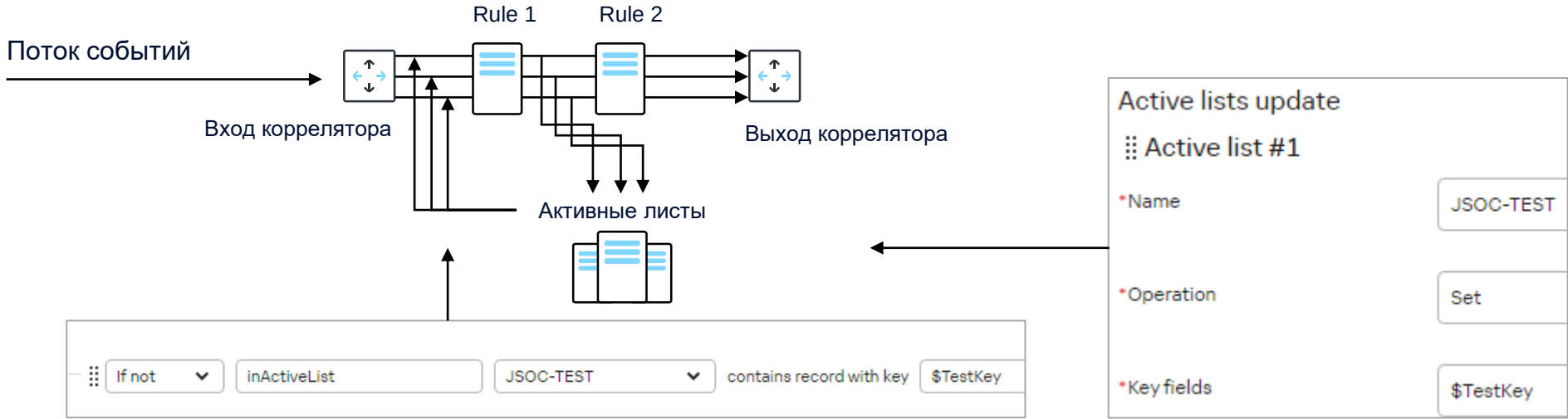
- 1 General
- 2 Global variables
- 3 Correlation
- 4 Enrichment
- 5 Response
- 6 Routing
- 7 Setup validation

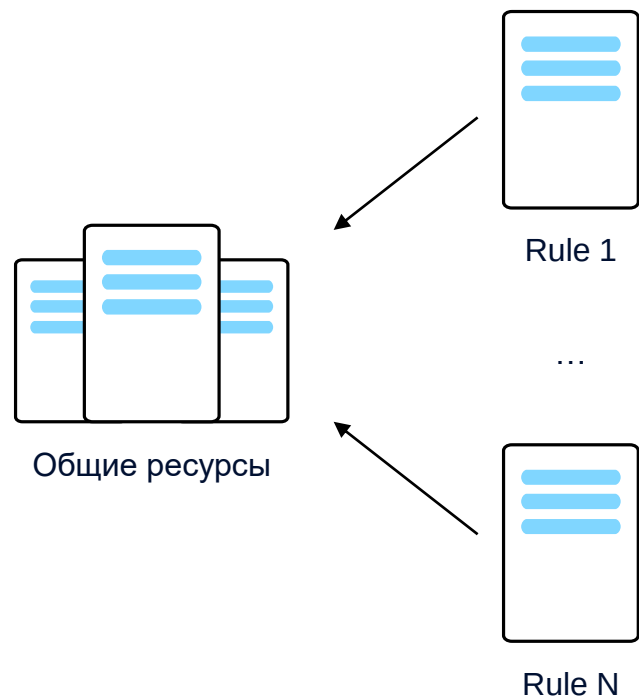
ТЕХНИЧЕСКИЕ
ОТЛИЧИЯ

РЕГЛАМЕНТ
РАЗРАБОТКИ

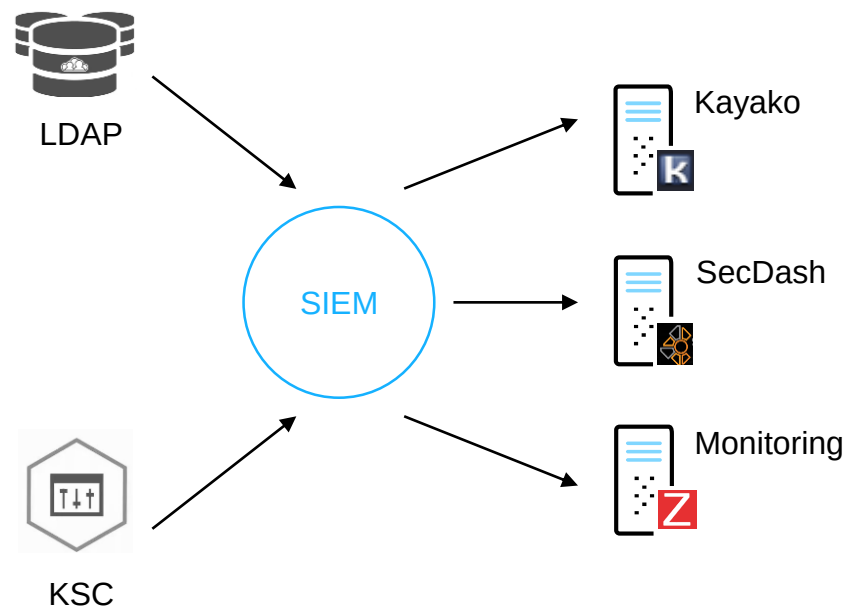
ТЕСТИРОВАНИЕ
ПРАВИЛ КОРРЕЛЯЦИИ

ВЗАИМОДЕЙСТВИЕ
С ВЕНДОРОМ



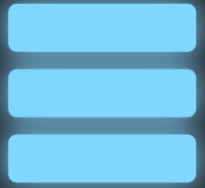


СОЗДАНИЕ ЯДРА
КОНТЕНТА



НАСТРОЙКА
ИНТЕГРАЦИЙ

ЗАПУСК СЕРВИСА



ПРОСТОЙ ПРИНЦИП
РАСПОЛОЖЕНИЯ



ПОНЯТНЫЙ
ПОРЯДОК ЗАПУСКА



СИНХРОНИЗАЦИЯ
ИЗМЕНЕНИЙ

ИМПОРТ СПИСКА ИСКЛЮЧЕНИЙ

СИНХРОНИЗАЦИЯ ПРОФИЛЕЙ

НАСТРОЙКА ПОРОГОВ
И ПАРАМЕТРОВ

ПЕРЕНОС СТАТИСТИКИ СРАБАТЫВАНИЙ



ПРОДОЛЖЕНИЕ
СЛЕДУЕТ

1

Недостатки схемы событий

2

Связность ресурсов и поиск по контенту

3

Сетевая модель

4

Интерфейс

Взаимодействие с вендором

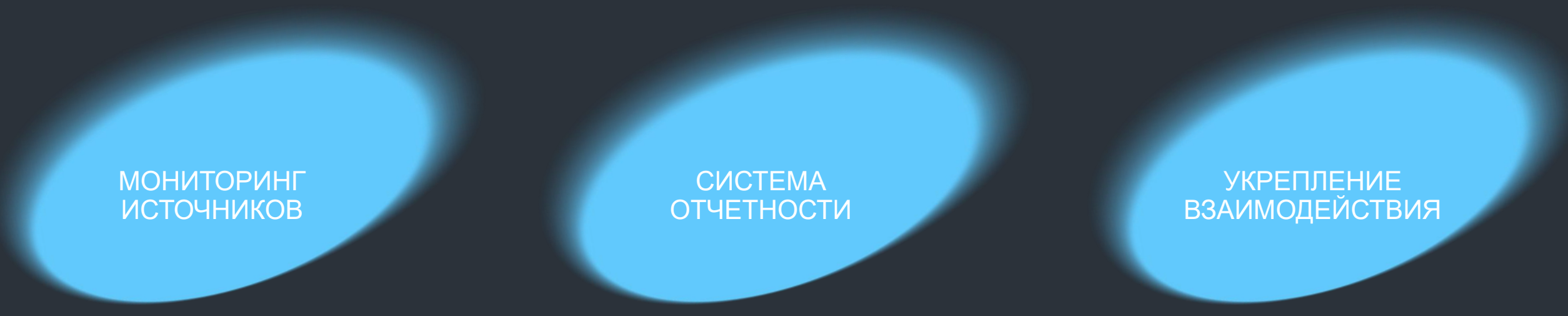
[01] ТЕСНОЕ ВЗАИМОДЕЙСТВИЕ

[02] БЫСТРАЯ РЕАКЦИЯ НА ПРОБЛЕМЫ

[03] ГОТОВНОСТЬ К ИЗМЕНЕНИЯМ В ПРОДУКТЕ

[04] ПОМОЩЬ В НОРМАЛИЗАЦИИ
СОБЫТИЙ ДЛЯ ИСТОЧНИКОВ





МОНИТОРИНГ
ИСТОЧНИКОВ

СИСТЕМА
ОТЧЕТНОСТИ

УКРЕПЛЕНИЕ
ВЗАИМОДЕЙСТВИЯ

SOC FORUM 2023



8 (800) 302-85-23
solar@rt-solar.ru

ГК «Солар»
Никитский переулок, 7, стр. 1,
г. Москва