Информзащита
IZ:SOC

Знай свой SIEM,
углублённые и неочевидные метрики работоспособности высоконагруженных инсталляций

Кирилл Дёмин

Измерение SIEM

Очереди

Задержки

CPU

Количество активов

Average Load

IN

OUT

EPS

Коллектор / Агенты

Единичные источники

RAM

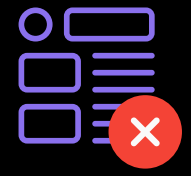
Disk Space

Errors

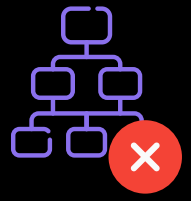
Buffers Size

Network BPS

Проблематика метрик SIEM



Недостаточная детализация

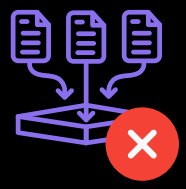


Отсутствие разбивки по компонентам и потокам данным

Ограниченные возможности задания трешхолдов (пороговых значений) и алертов на отклонения каждой метрики

Ограниченные возможности для долгосрочного анализа и прогнозирования

Отсутствие единого окна просмотра и управления всеми метриками



Ограниченный функционал визуализации пайплайнов и потоков данных

Единая платформа для отслеживания метрик на базе Grafana Mimir

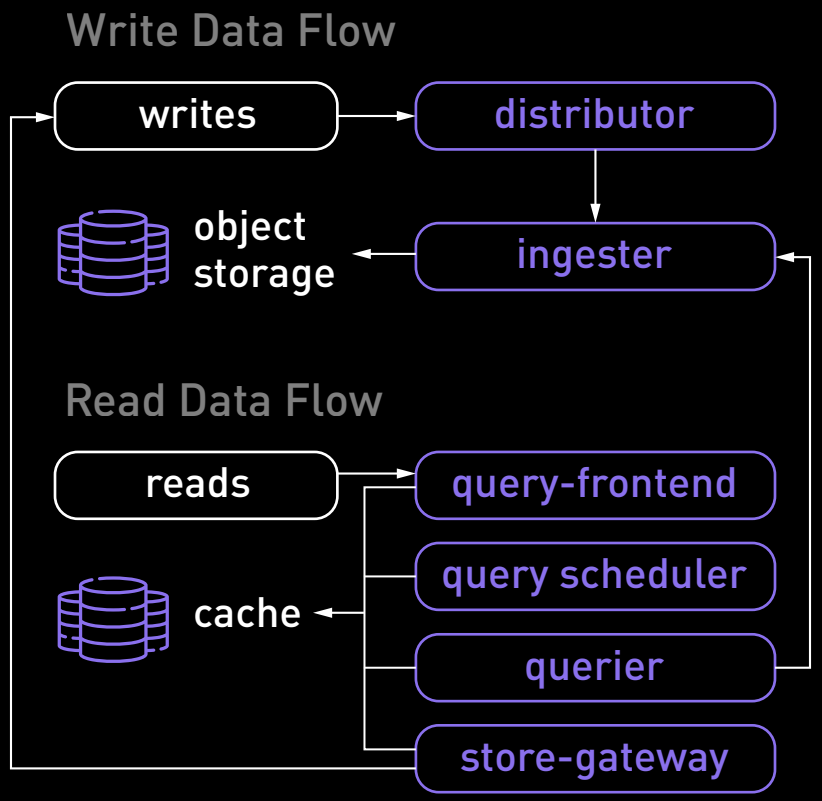
- Масштабируемость и производительность
- Интеграция с другие системами мониторинга, в том числе со встроенными в SIEM (Grafana, RabbitMQ, etc.)
- Гибкость и кастомизация с упором на более глубокую аналитику
- Поддержка высокодоступных архитектур

Prometheus

Zabbix

Based on **cortex**

Как работает Mimir



Архитектура

All-in-one

Один хост, локальное хранилище

Scalable All-in-one

Балансир + Несколько AIO + Локальное хранилище

Microservices

Отдельные компоненты + Удалённое хранилище

Separate Read-Write

Отдельные компоненты Write + Отдельные компоненты Read + Удалённое хранилище

Расширенные метрики для мониторинга компонентов SIEM

ОС

us
Загрузка CPU выполнением процессов в пространстве пользователя

sy
Загрузка CPU выполнением процессов в пространстве ядра

wa
Ожидание процессором ответа от дисковой подсистемы

Коллекторы SIEM

- Алерт на поступление событий с коллектора
- Алерт на резкие скачки input EPS
- Алерт на изменение input EPS на промежутке времени
- Алерт на рост output буфера
- Алерт на рост буфера обогащения

Корреляторы SIEM

- Алерт на отключение правил
- Алерт на всплески сработок отдельных правил корреляции
- Статистика количества бакетов к количеству сработок
- Алерт на размер активных листов

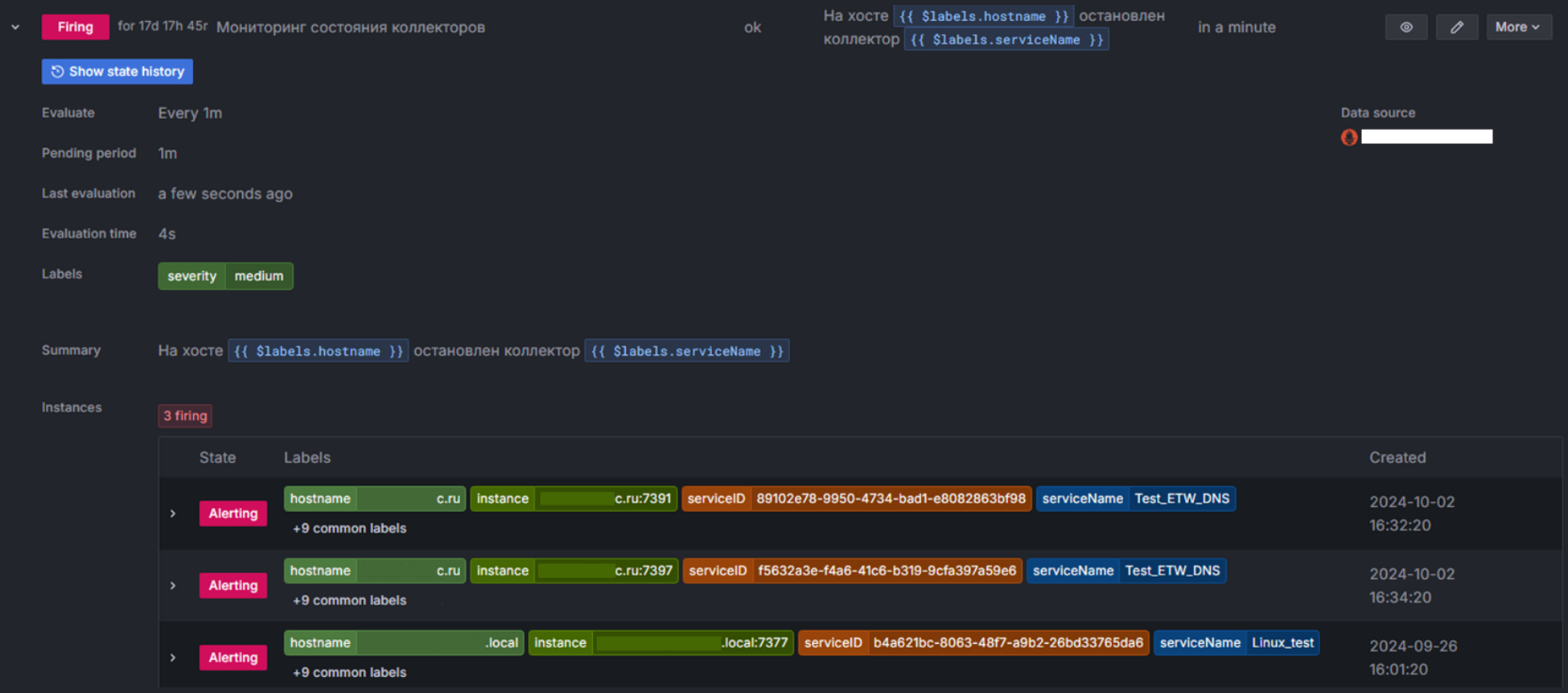
Ядро

- Доступность веб-интерфейса
- Успешность создания бэкапов

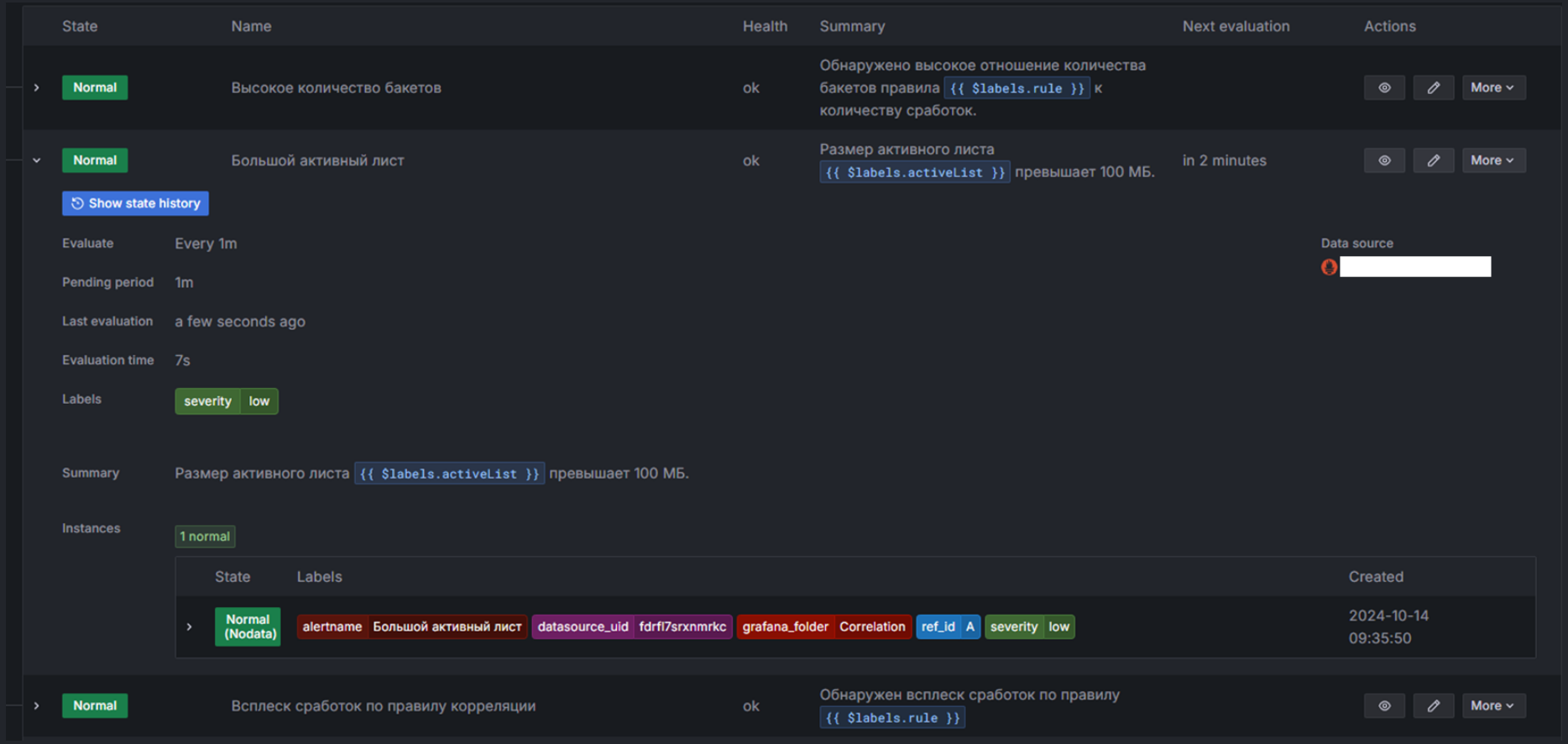
Хранилище SIEM

- Алерт на disk free space
- Алерт на select queries
- Алерт на задержки
- Алерт ошибки в работе хранилища

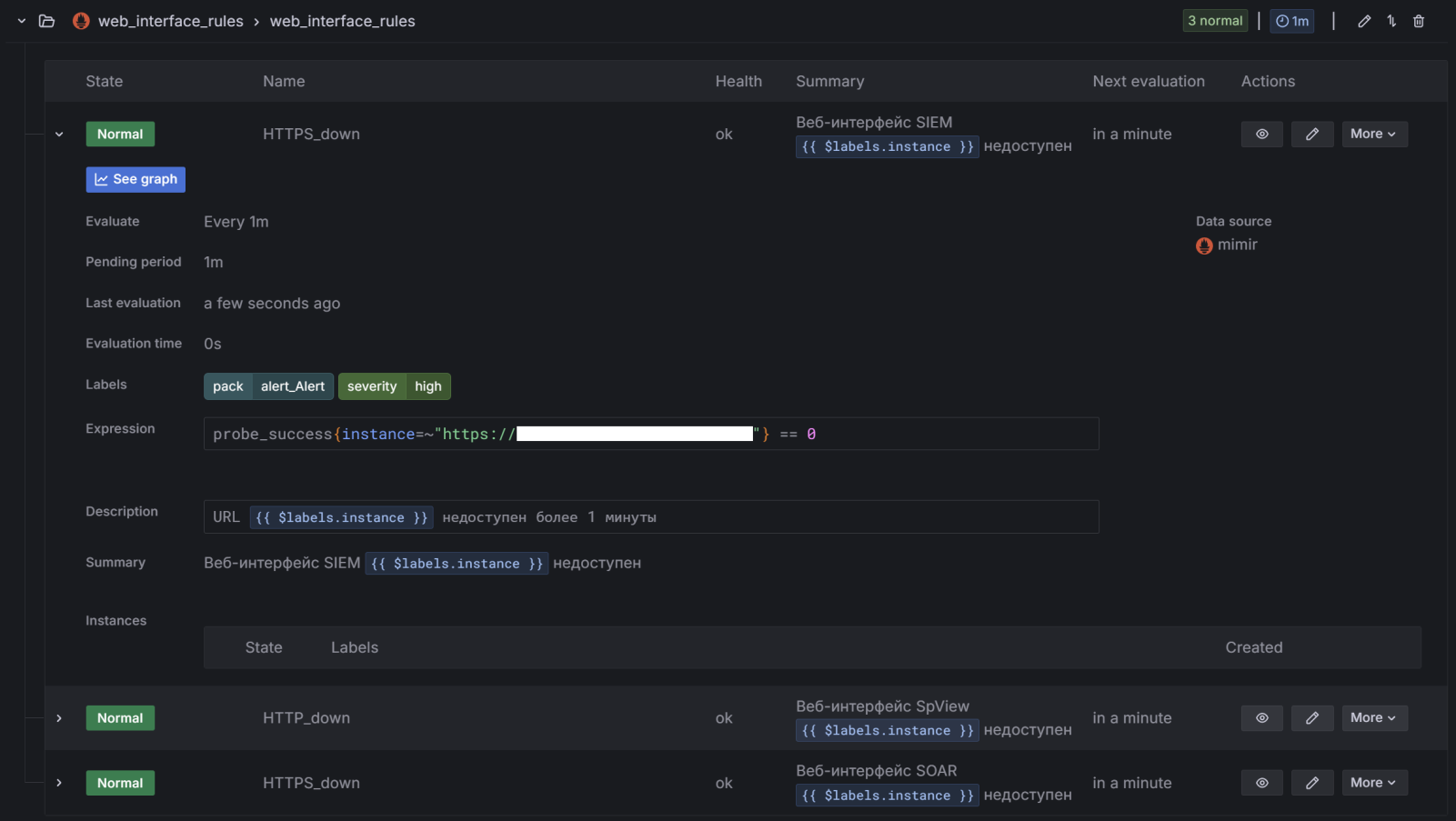
Примеры метрик 1 – сбор событий



Примеры метрик 2 – корреляция



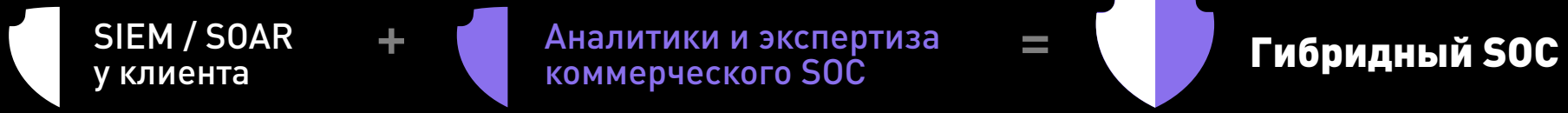
Примеры метрик 3 – веб-интерфейс



Примеры метрик 3 – работа хранилища

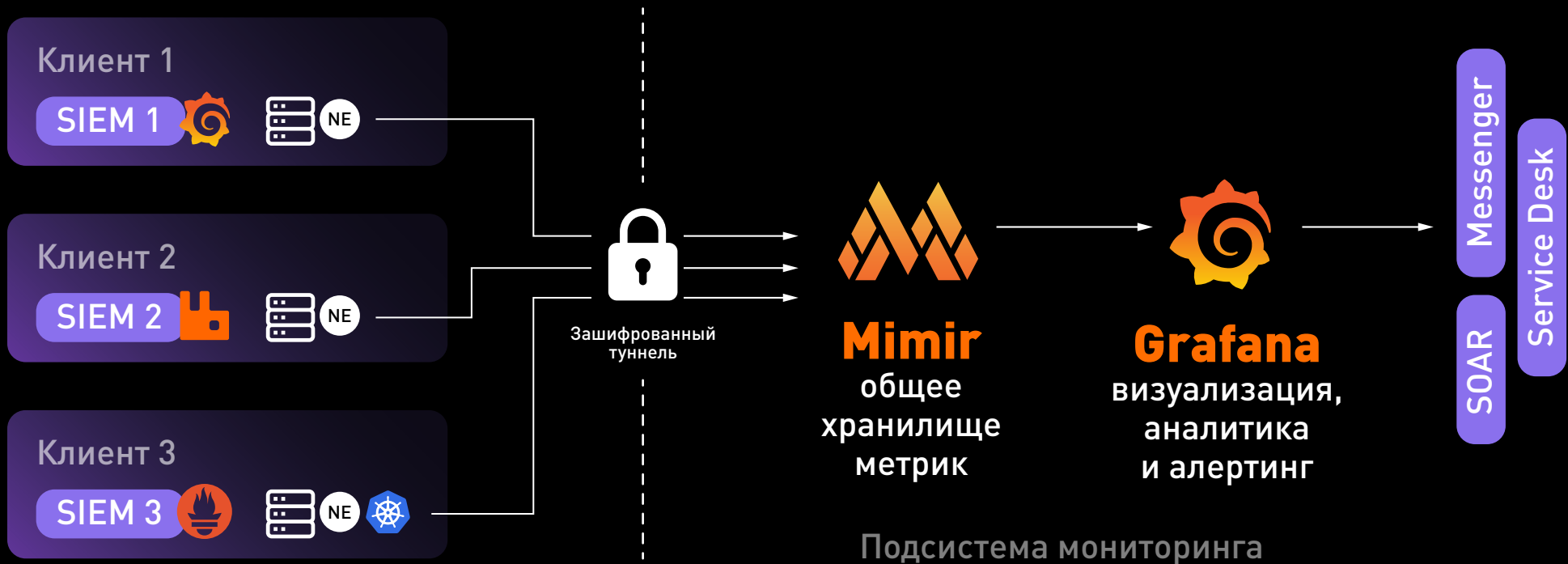
Примеры метрик 4 – ОС

Централизованный мониторинг нескольких инсталляций SIEM (гибридные SOC)



- У клиента не выстроен мониторинг работоспособности технологического стека SOC и серверов или его недостаточно
- SLA сервисного провайдера привязан к оборудованию и системам клиента
- Большое количество клиентов, нужна унификация и «единое окно»
- Нужна маршрутизация тикетов в группу инфраструктуры и/или в ИТ-подразделение клиента

Агрегация метрик на базе Grafana Mimir



Подсистема мониторинга работоспособности MSSP-поставщика

Общий дашборд

	Состояние SIEM	Серверы SIEM	Состояние SOAR	Серверы SOAR
Core + Coll(5) + Corr(2) + Stor(S2R2) AstraLinux 1.7.3 All VM 3 Tenants	No alerts matching filters	No alerts matching filters	— — —	— — —
Core + (Coll + Corr) + Stor(S1R2) AstraLinux 1.7.5 (core 5.15) All VM 1 Tenant	No alerts matching filters	No alerts matching filters	No alerts matching filters	LINUX_HostOutOfM... Firing for 3h 17m 35s › 1 instance Мониторинг состо... Firing for 1h 6m 41s
TestDev SOC All-in-one Ubuntu 22.04 LTS All VM 1 Tenant	Отсутствие событий ... Firing for 1h 29m 41s › 1 instance	No alerts matching filters	No alerts matching filters	No alerts matching filters

Метрики работоспособности инсталляций SOAR

Уже собираем:

- Метрики ОС
- Метрики по статусу контейнеров
- Метрики по статусу сервисов SOAR

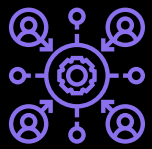
В планах:

- Проработка интеграции с RabbitMQ
- Метрики выполнения плейбуков
- Статусы работоспособности интеграций

Summary

Функционал мониторинга работоспособности в различных SIEM-системах зачастую ограничен в тех или иных аспектах.

В работе SOC важно иметь разнообразные алерты на прямые и косвенные метрики работы компонентов SIEM.



Поставщики MSSP и коммерческие SOC не могут оставлять без внимания поддержку работоспособности SIEM, нужны централизованные решения с развитой мультитенантностью.

Grafana Mimir – хорошее решение для сбора метрик с разнообразных SIEM и SOAR, особенно использующих Prometheus, Grafana и Victoria Metrics.

Спасибо

Информзащита
IZ:SOC

Информационная безопасность

24x7x365

Центр противодействия кибератакам IZ:SOC

+7 495 980 23 45
izsoc@infosec.ru
www.izsoc.ru

Системный интегратор

+7 495 980 23 45
market@infosec.ru
www.infosec.ru

Центр противодействия мошенничеству

antifraud@infosec.ru

Пресс-служба

pr@infosec.ru

Сервисный центр

+7 495 981 92 22
support@itsoc.ru
www.itsoc.ru