

Знай свой SIEM, углублённые и неочевидные метрики работоспособности высоконагруженных инсталляций

Кирилл Дёмин



Измерение SIEM





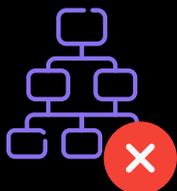
Проблематика метрик SIEM



Недостаточная
детализация



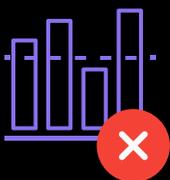
Ограниченные возможности
для долгосрочного анализа
и прогнозирования



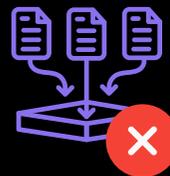
Отсутствие разбивки
по компонентам и потокам
данным



Отсутствие единого окна
просмотра и управления
всеми метриками



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



Ограниченный функционал
визуализации пайплайнов
и потоков данных

Единая платформа для отслеживания метрик на базе Grafana Mimir



- ✓ Масштабируемость и производительность
- ✓ Интеграция с другими 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

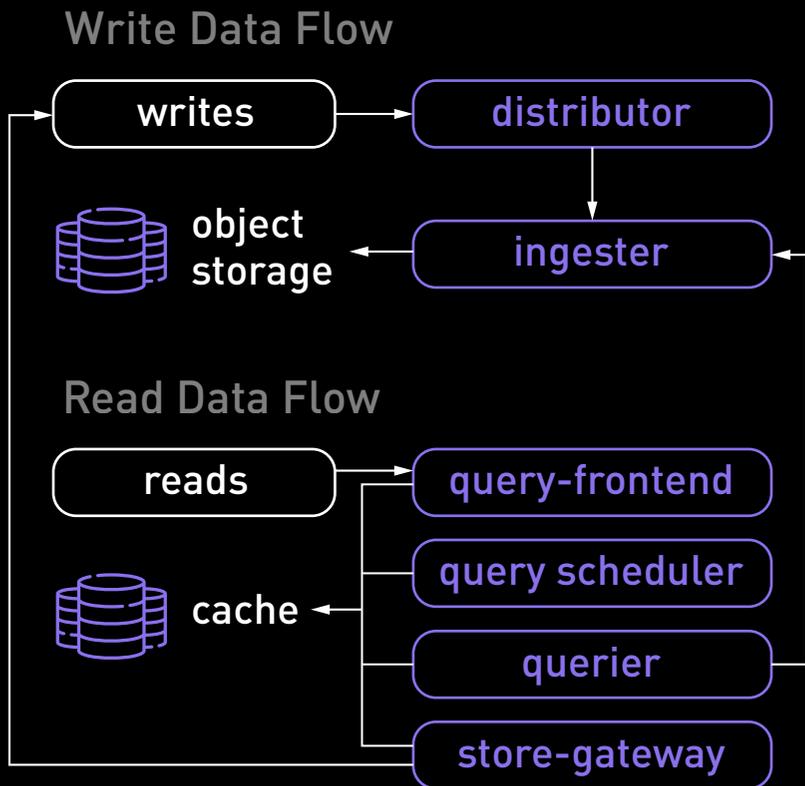
Zabbix



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 задержки
- › Алерт на select queries
- › Алерт ошибки в работе хранилища



Примеры метрик 1 – сбор событий

▼ **Firing** for 17d 17h 45m Мониторинг состояния коллекторов ok На хосте `{{ $labels.hostname }}` остановлен коллектор `{{ $labels.serviceName }}` in a minute 👁 ✎ More ▼

[🕒 Show state history](#)

Evaluate Every 1m
Pending period 1m
Last evaluation a few seconds ago
Evaluation time 4s
Labels **severity** **medium**

Summary На хосте `{{ $labels.hostname }}` остановлен коллектор `{{ $labels.serviceName }}`

Instances **3 firing**

State	Labels	Created
> Alerting	<code>hostname</code> <code>c.ru</code> <code>instance</code> <code>c.ru:7391</code> <code>serviceID</code> <code>89102e78-9950-4734-bad1-e8082863bf98</code> <code>serviceName</code> <code>Test_ETW_DNS</code> +9 common labels	2024-10-02 16:32:20
> Alerting	<code>hostname</code> <code>c.ru</code> <code>instance</code> <code>c.ru:7397</code> <code>serviceID</code> <code>f5632a3e-f4a6-41c6-b319-9cfa397a59e6</code> <code>serviceName</code> <code>Test_ETW_DNS</code> +9 common labels	2024-10-02 16:34:20
> Alerting	<code>hostname</code> <code>.local</code> <code>instance</code> <code>.local:7377</code> <code>serviceID</code> <code>b4a621bc-8063-48f7-a9b2-26bd33765da6</code> <code>serviceName</code> <code>Linux_test</code> +9 common labels	2024-09-26 16:01:20



Примеры метрик 2 – корреляция

State	Name	Health	Summary	Next evaluation	Actions						
> Normal	Высокое количество бакетов	ok	Обнаружено высокое отношение количества бакетов правила <code>{{ \$labels.rule }}</code> к количеству сработок.		More ▾						
▼ Normal	Большой активный лист	ok	Размер активного листа <code>{{ \$labels.activeList }}</code> превышает 100 МБ.	in 2 minutes	More ▾						
Show state history											
Evaluate	Every 1m				Data source <input type="text"/>						
Pending period	1m										
Last evaluation	a few seconds ago										
Evaluation time	7s										
Labels	severity low										
Summary	Размер активного листа <code>{{ \$labels.activeList }}</code> превышает 100 МБ.										
Instances	1 normal										
<table border="1"><thead><tr><th>State</th><th>Labels</th><th>Created</th></tr></thead><tbody><tr><td>> Normal (Nodata)</td><td>alertname Большой активный лист datasource_uid fdrfl7srxnmrkc grafana_folder Correlation ref_id A severity low</td><td>2024-10-14 09:35:50</td></tr></tbody></table>						State	Labels	Created	> Normal (Nodata)	alertname Большой активный лист datasource_uid fdrfl7srxnmrkc grafana_folder Correlation ref_id A severity low	2024-10-14 09:35:50
State	Labels	Created									
> Normal (Nodata)	alertname Большой активный лист datasource_uid fdrfl7srxnmrkc grafana_folder Correlation ref_id A severity low	2024-10-14 09:35:50									
> Normal	Всплеск сработок по правилу корреляции	ok	Обнаружен всплеск сработок по правилу <code>{{ \$labels.rule }}</code>		More ▾						



Примеры метрик 3 – веб-интерфейс

web_interface_rules > web_interface_rules 3 normal | 1m | 🔍 🔄 🗑️

State	Name	Health	Summary	Next evaluation	Actions
Normal	HTTPS_down	ok	Веб-интерфейс SIEM {{ \$labels.instance }} недоступен	in a minute	👁️ ✎ More ▾

[📊 See graph](#)

Evaluate: Every 1m Data source: mimir

Pending period: 1m

Last evaluation: a few seconds ago

Evaluation time: 0s

Labels: pack alert_Alert severity high

Expression: `probe_success{instance=~"https://"} == 0`

Description: URL {{ \$labels.instance }} недоступен более 1 минуты

Summary: Веб-интерфейс SIEM {{ \$labels.instance }} недоступен

Instances

State	Labels	Created
Normal	HTTP_down	
Normal	HTTPS_down	



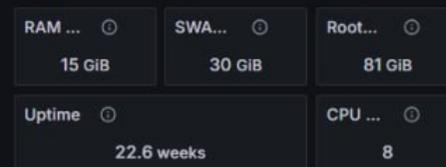
Примеры метрик 3 – работа хранилища

State	Name	Health	Summary	Next evaluation	Actions
Normal	Мониторинг состояния хранилищ SIEM	ok	На хосте <code>{{ \$labels.hostname }}</code> остановлено хранилище <code>{{ \$labels.serviceName }}</code>	in a minute	More ▾
Show state history					
Evaluate	Every 1m				Data source <input type="text"/>
Pending period	1m				
Last evaluation	a few seconds ago				
Evaluation time	6s				
Labels	severity high				
Summary	На хосте <code>{{ \$labels.hostname }}</code> остановлено хранилище <code>{{ \$labels.serviceName }}</code>				

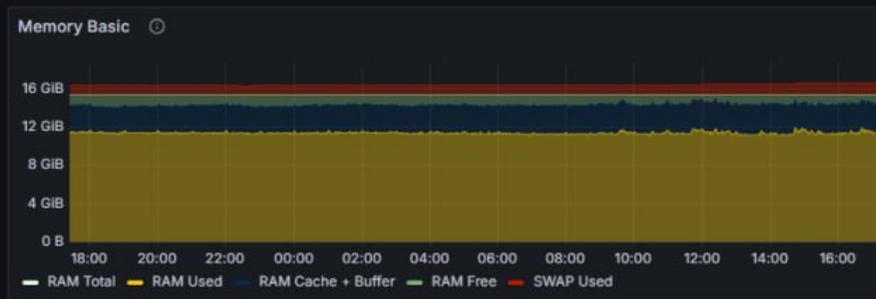


Примеры метрик 4 – ОС

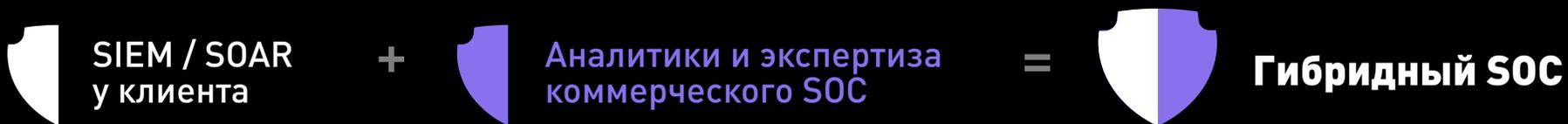
Quick CPU / Mem / Disk



Basic CPU / Mem / Net / Disk



Централизованный мониторинг нескольких инсталляций SIEM (гибридные SOC)



У клиента не выстроен мониторинг работоспособности технологического стека SOC и серверов или его недостаточно



Большое количество клиентов, нужна унификация и «единое окно»



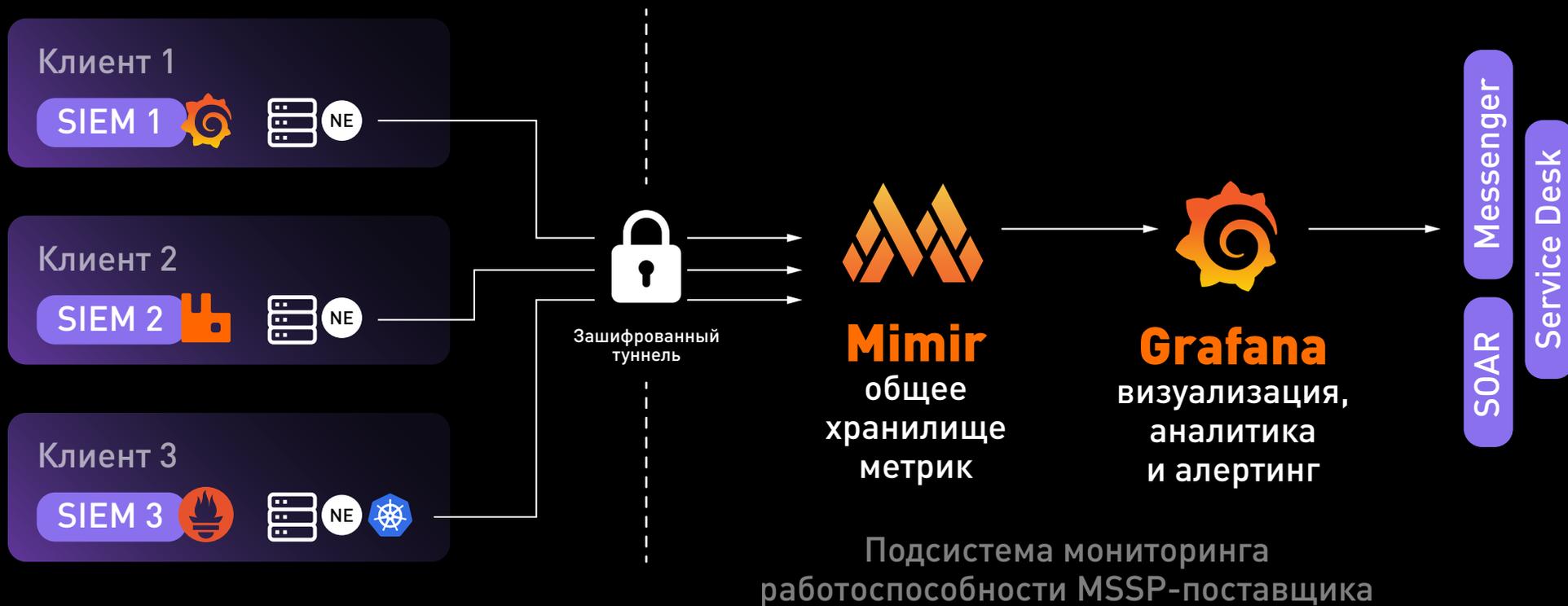
SLA сервисного провайдера привязан к оборудованию и системам клиента



Нужна маршрутизация тикетов в группу инфраструктуры и/или в ИТ-подразделение клиента



Агрегация метрик на базе Grafana Mimir





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	<p>LINUX_HostOutOfM... ↗</p> <p> Firing for 3h 17m 35s > 1 instance</p> <p>Мониторинг состо... ↗</p> <p> Firing for 1h 6m 41s</p>
TestDev SOC All-in-one Ubuntu 22.04 LTS All VM 1 Tenant	<p>Отсутствие событий ... ↗</p> <p> Firing for 1h 29m 41s > 1 instance</p>	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

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

