

# Простые инструменты для улучшения incident response: опыт Туту

# Обо мне

Борзов Андрей

В Туту с 2012 года,

С 2015 года руковожу эксплуатацией сайта

Сервис путешествий Туту.ру:

~1 млн уникальных посетителей в день,

20 команд разработки,

Более 500 микросервисов на 4х языках  
(и монолит)



# Наш бэкграунд

- Монолит и в нем самописный мониторинг
- Nagios для серверов
- Эксплуатация отвечает за сайт, админы – за инфраструктуру



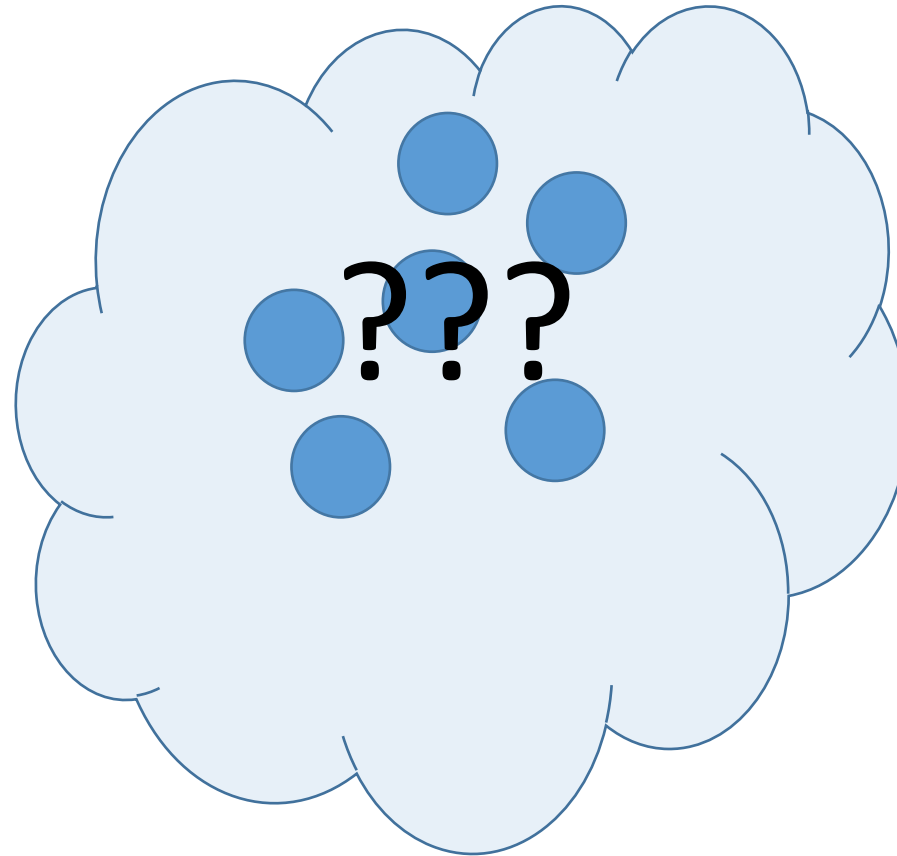
- Grafana (Graphite, ELK, Prometheus)
- Больше микросервисов, продуктов и команд
- «You Build It – You Run It»



Самописный  
мониторинг

**Nagios**

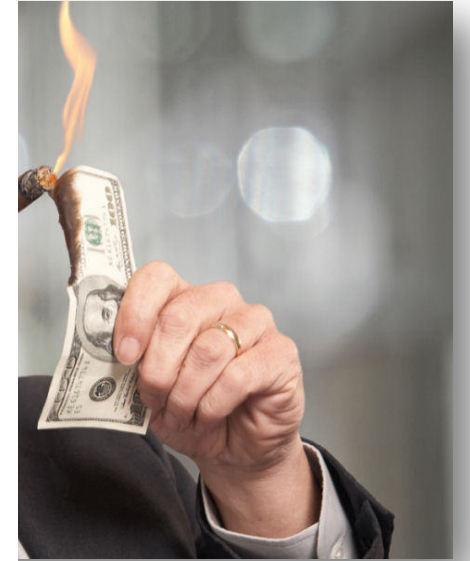
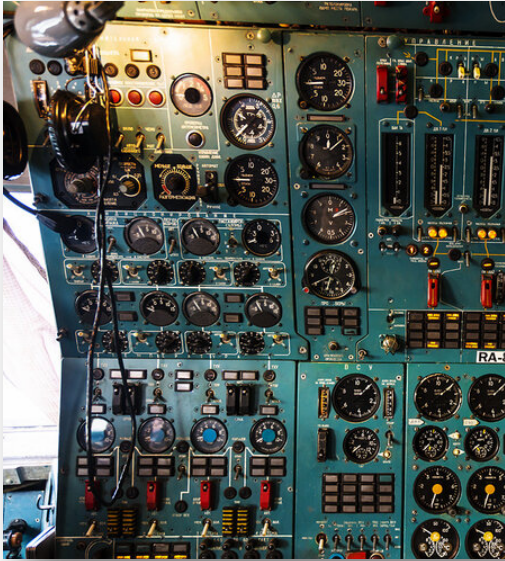
 **Grafana**



Команды



# Выбор решения



# Шаг 1: Проблемы

- Нет инфы о потоках сообщений
- Нет уверенности, что люди получают свои алерты
- Команды подключаются к мониторингу сами, кто как СМОГ

# Шаг 1: Контроль


- Создаем well-known точки для алертов команды (tg chat)
- Пишем сервис, который принимает алерты от всех систем и доставляет в эти точки
- Нотификации делаем полезнее доступных «из коробки» (хотя бы чуть-чуть)



Chats

TeddyBot

bot



**[Alerting] 50X ошибки на всем сайте alert**

State: 50X ошибки на всем сайте alert

Message:

[sli\_name=test\_overall\_error\_count]

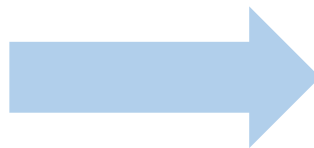
URL: <https://grafana.monitoring.tutu.ru/d/9sFJM2qik/sli-samples?fullscreen&edit&tab=alert&panelId=2&orgId=1>

Image: <https://grafana.monitoring.tutu.ru/public/img/attachments/5IWSSLxUnr1EVd9zYiBA.png>

*Metrics:*

50X: 10.000


16:52




Chats

TeddyBot

bot

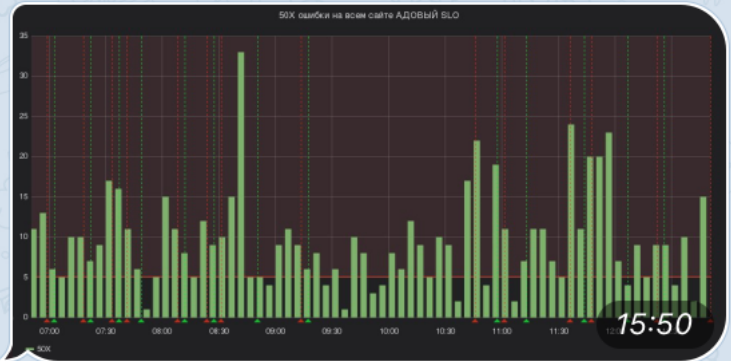


 **[Alerting] 50X ошибки на всем сайте alert**

[sli\_name=test\_overall\_error\_count] <https://grafana.monitoring.tutu.ru/d/9sFJM2qik/sli-samples?fullscreen&edit&tab=alert&panelId=2&orgId=1>

**50X = 15.**

15:50





# Шаг 1: Результаты

- Можно анализировать потоки сообщений
- Команды не тратят время на самостоятельную интеграцию
- Нотификации стали полезнее
- Знаем, что люди получают свои алерты

## Шаг 2: Проблемы

- Типовую диагностику проводим «далеко» от чата
- Дублируем действия друг друга
- Чтобы поделиться результатами, нужны усилия

## Шаг 2: Интерактив

- Учим бота понимать, когда ему отдают команды
- Реализуем команды с типовыми действиями (у нас – в bash стиле)





Andrey Borzov

#run errors\_info -minutes 15



TeddyBot

 Статистика ошибок за последние 15 минут. 

- К алертам прикручиваем кнопки с действиями, которые хочется «в один клик»

# Алерт с кнопками



TeddyBot



**[Alerting] 50X ошибки на всем сайте alert**

[sli\_name=test\_overall\_error\_count] <https://grafana.monitoring.tutu.ru/d/9sFJM2qik/sli-samples?fullscreen&edit&tab=alert&panelId=2&orgId=1>

**50X = 9.**

Позвонить Пете

А чо там с базулей?

Поставить тикет админам

# Примеры команд

- Перезапустить сервис
- Рестарт apache в монолите
- Mysql: проверить slave status, показать медленные запросы в processlist
- Сводная информация об ошибках на сайте
- Лог изменений на production
- Создать тикет

## Шаг 2: Результаты

- В 90% случаев за секунды понимаем, у кого проблемы
- Прямо из чата: производим отладку, оповещаем заинтересованных или прикладываем подорожник
- Проще координироваться: все видят результаты диагностических команд

Но!

## Шаг 3: Всё еще проблемы

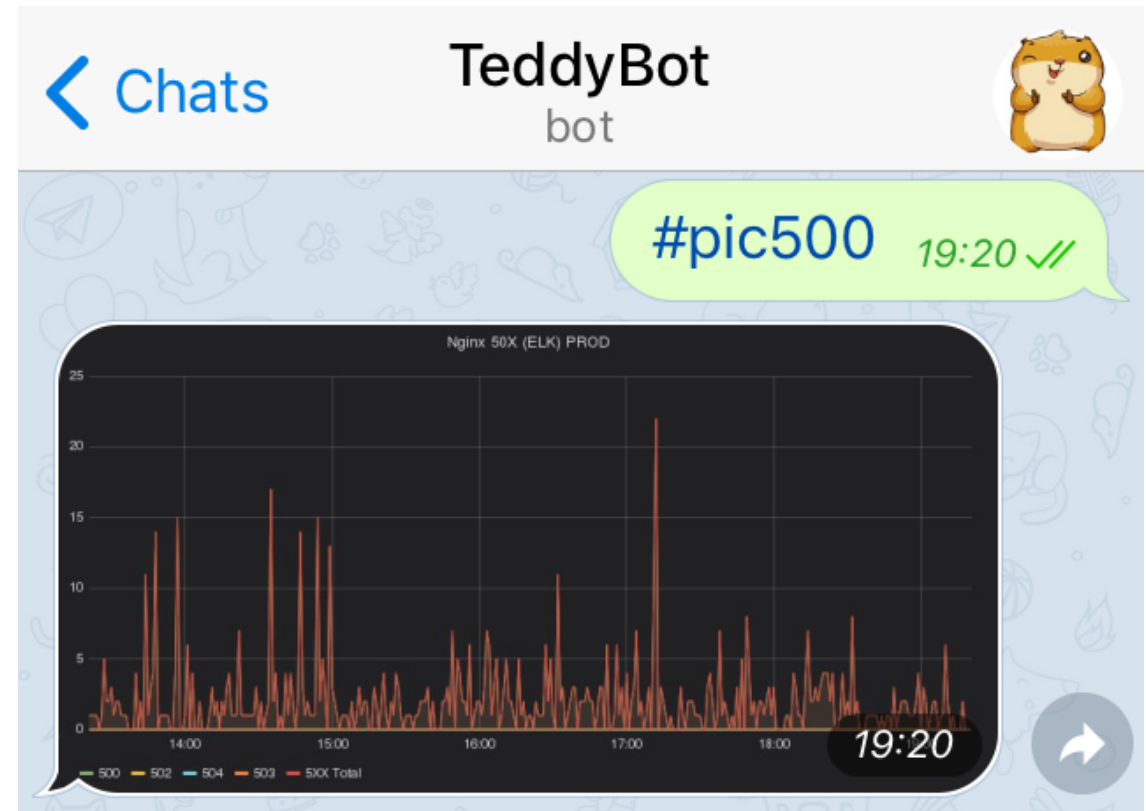
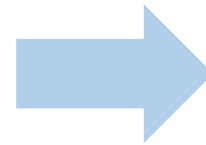
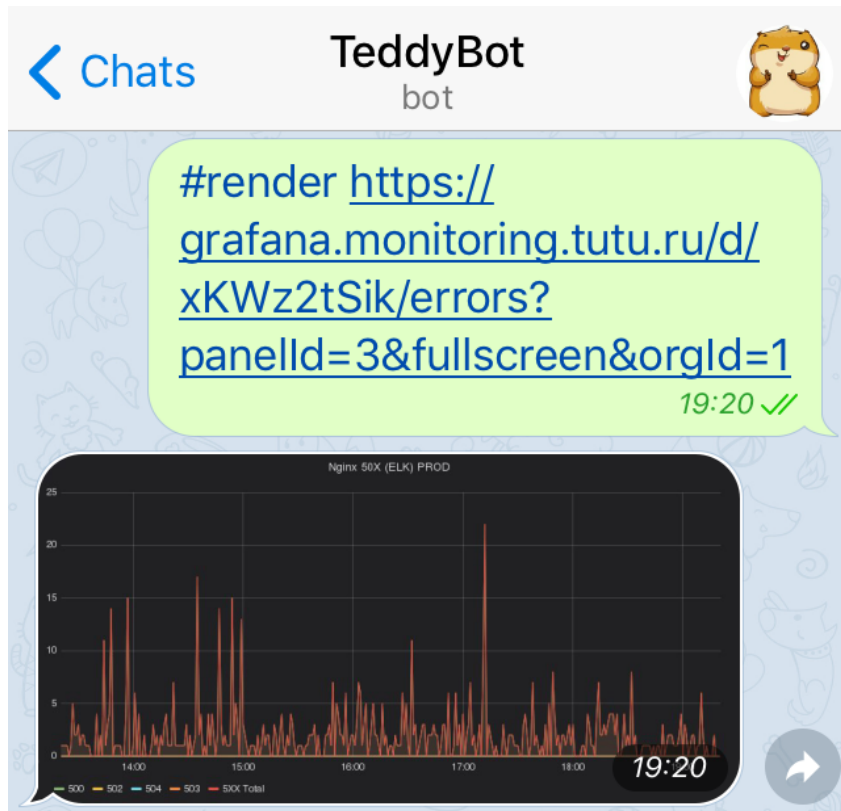
- Команды бота неудобно набирать, особенно с телефона
- Любимые команды у каждого свои
- Карта маршрутизации алертов – в коде, PR на любое изменение



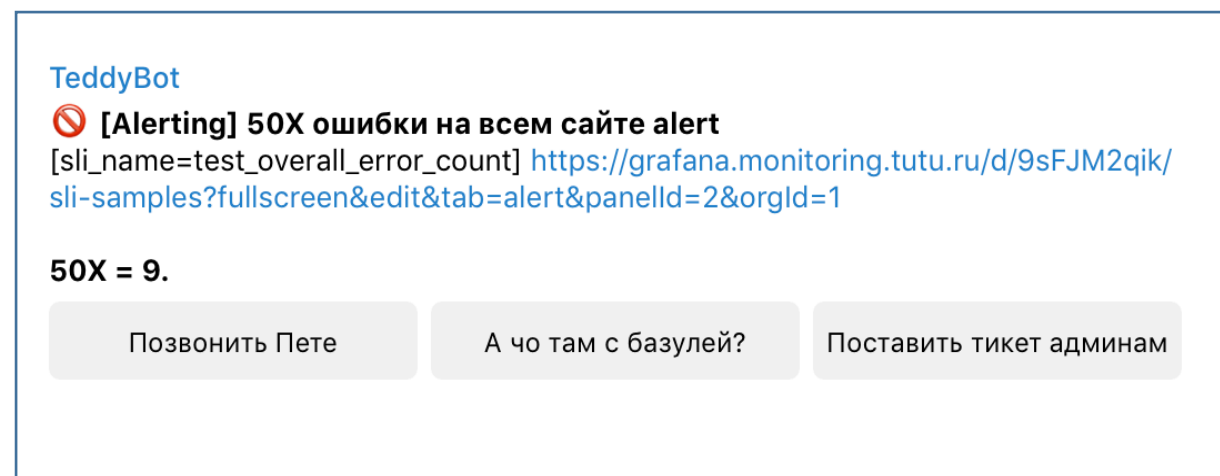
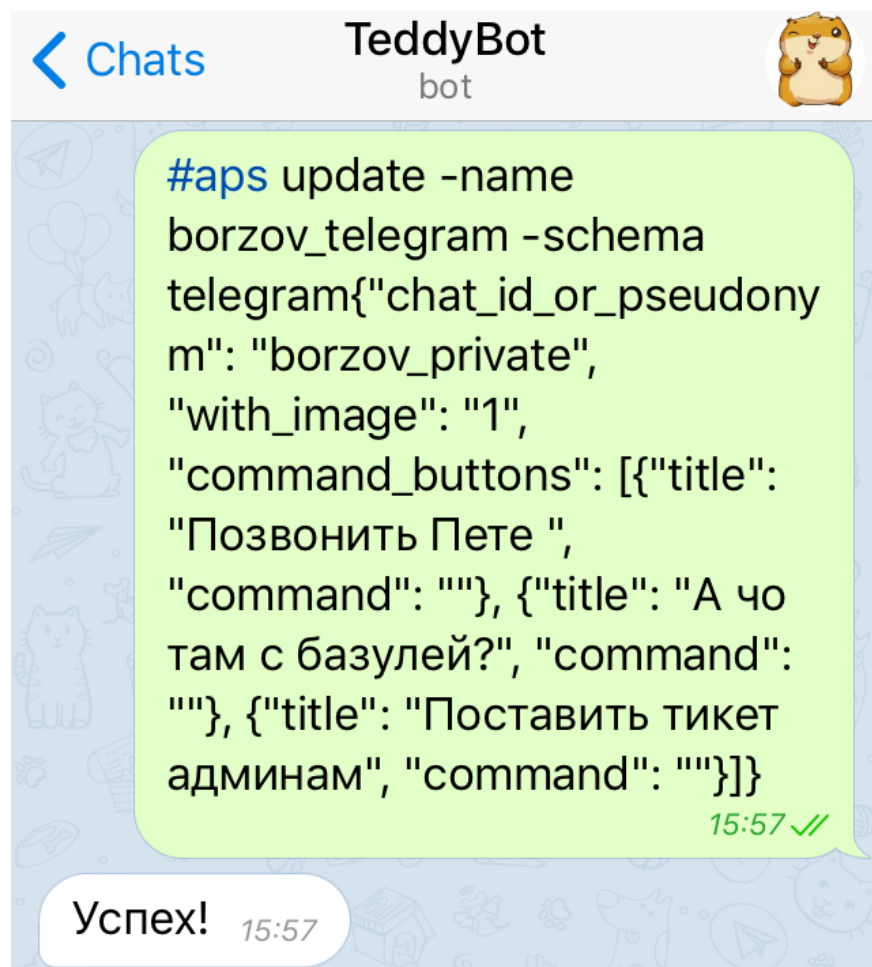
## Шаг 3: Кастомизация

- Упрощение команд – шорткаты (`#alias`, как в `bash`)
- Своя маршрутизация – «процессинговые схемы», json-описания маршрутов
- Свои кнопки – через параметры в процессинговых схемах

# Алиасы



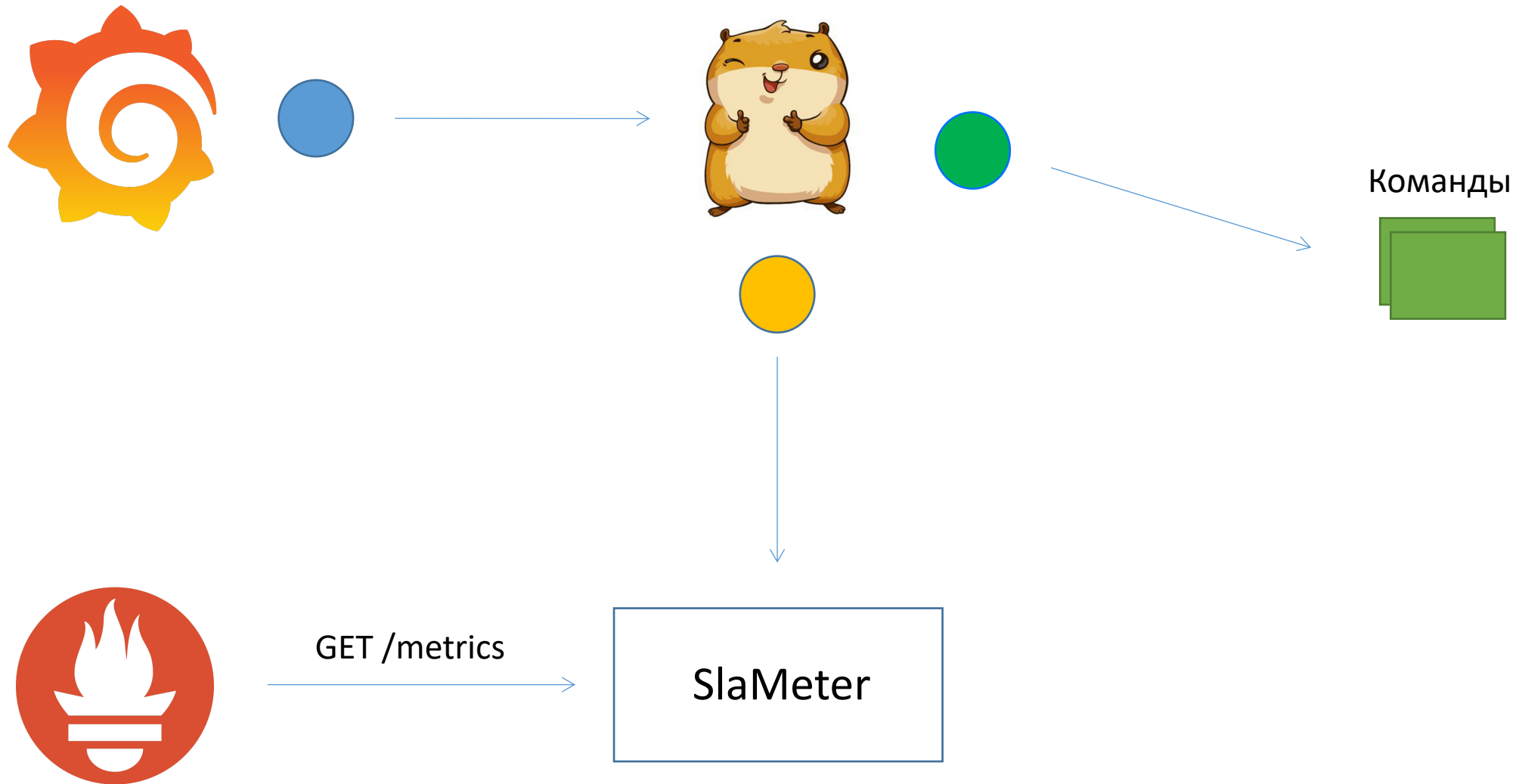
# Процессинговые схемы



# Шаги 1-3: Результаты

- Люди получают свои алерты
- Оповещения несут больше информации
- Автоматическая диагностика доступна по кнопке
- Результаты диагностики видны всем участникам
- Чтобы подключиться к системе, нужно поговорить с ботом

# Бонус. Измерение Service Level



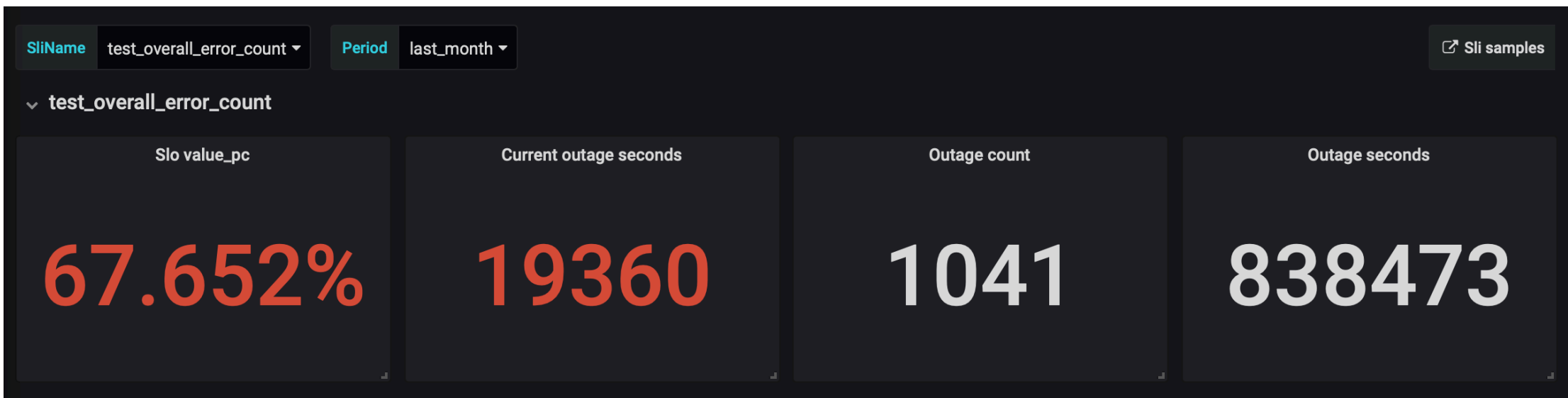
# SlaMeter

- Хранит события OK/FAIL по SLI
- Рассчитывает time-based SL и вспомогательные метрики
- Результаты – через API, Prometheus Exporter



Имя  
индикатора

Период



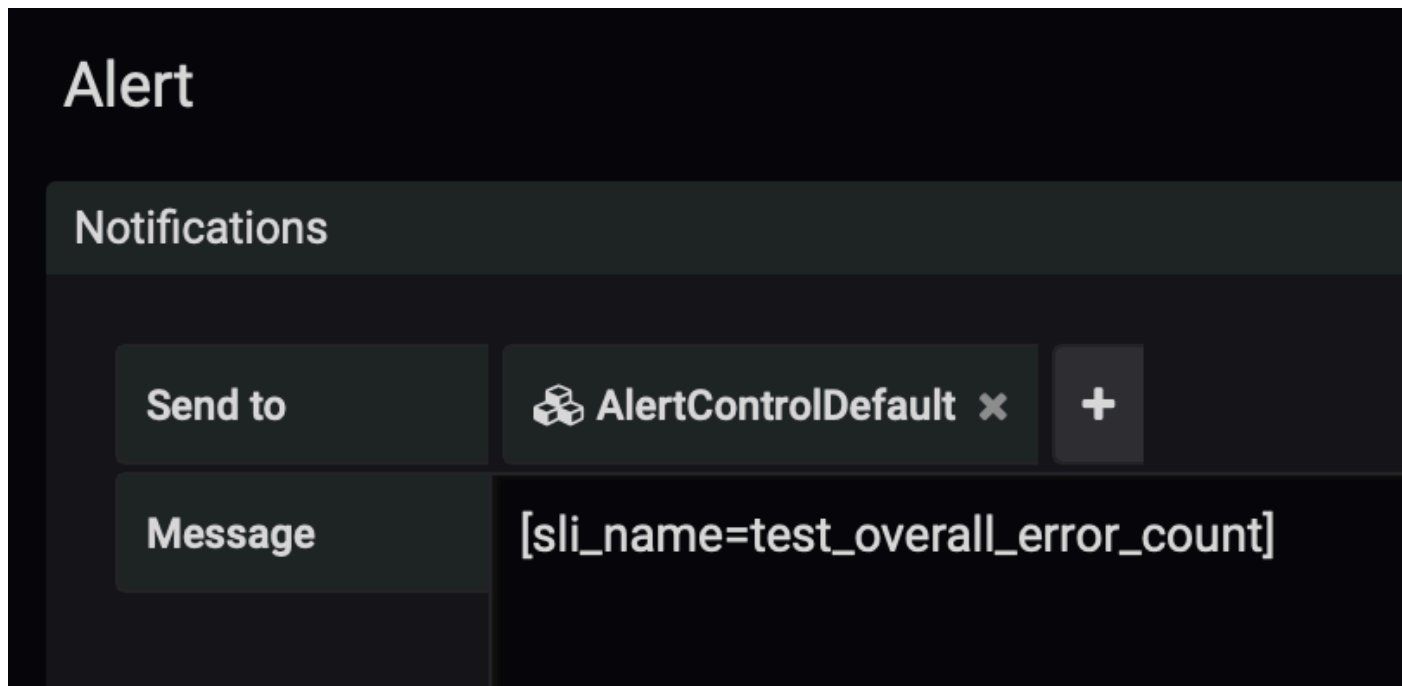
Service Level

Если недоступен  
прямо сейчас, то как  
долго

Всего инцидентов

Общее время  
недоступности

# Настройка



The screenshot shows the 'Alert' configuration page in Grafana. It features a 'Notifications' section with two main fields: 'Send to' and 'Message'. The 'Send to' field contains a dropdown menu with 'AlertControlDefault' selected, followed by a close button (x) and an add button (+). The 'Message' field contains the text '[sli\_name=test\_overall\_error\_count]'.

Alert	
Notifications	
Send to	<div>AlertControlDefault x +</div>
Message	[sli_name=test_overall_error_count]

- + Логика работы с SLI вынесена в Grafana
- + Удобный GUI, большой выбор источников данных

# TeddyBot в цифрах

- MVP каждого шага – 1-3 дня разработки
  - 30 минут, чтобы начать пользоваться
  - 50 созданных схем
  - Доставляет 500 алертов в будние дни
- + Помогает в других инструментах (SlaMeter)



# TeddyBot

## Спасибо за внимание!

[Задать вопрос](#)

[Вежливо похлопать](#)

[Обсудить в кулуарах](#)