

# Система мониторинга сетевых сервисов

Система, которая собирает информацию, приводит её к единому формату и генерирует отчёты о текущем состоянии сетевых сервисов.

## Задача

Заказчик занимается консалтингом и поддержкой в сфере безопасности сетевых инфраструктур. Число клиентов компании росло, поэтому возникла потребность в создании системы для автоматического анализа работы обслуживаемых сетевых сервисов и оперативного оповещения сотрудников заказчика о возникающих проблемах. Она могла значительно облегчить труд операторов SOC-команды и повысить эффективность работы.

Наша компания хорошо знакома с проблематикой оптимизации служб мониторинга и сокращения времени реагирования на неполадки в работе онлайн-сервисов, поэтому заказчик обратился за помощью именно к нам.

### Индустрия

Информационные технологии

### Ключевые моменты

- частично автоматизировали работу SOC-специалистов;
- сократили время реагирования на возникающие проблемы;
- снизили расходы на мониторинг онлайн-сервисов.

### Команда

Менеджер проекта — 1  
Back-end разработчик — 2  
Front-end разработчик — 2  
Аналитик — 1

### Продолжительность

8 месяцев

### Технологии

Python, TypeScript, React,  
Elasticsearch, Logstash,  
Kibana, Google Cloud  
Platform

## Подход

Работа с клиентом строилась на следующих принципах:



Быстрый запуск проекта



Прозрачность процессов



Ответ в течение часа



Масштабируемость



Высокий уровень доверия

## Стек технологий

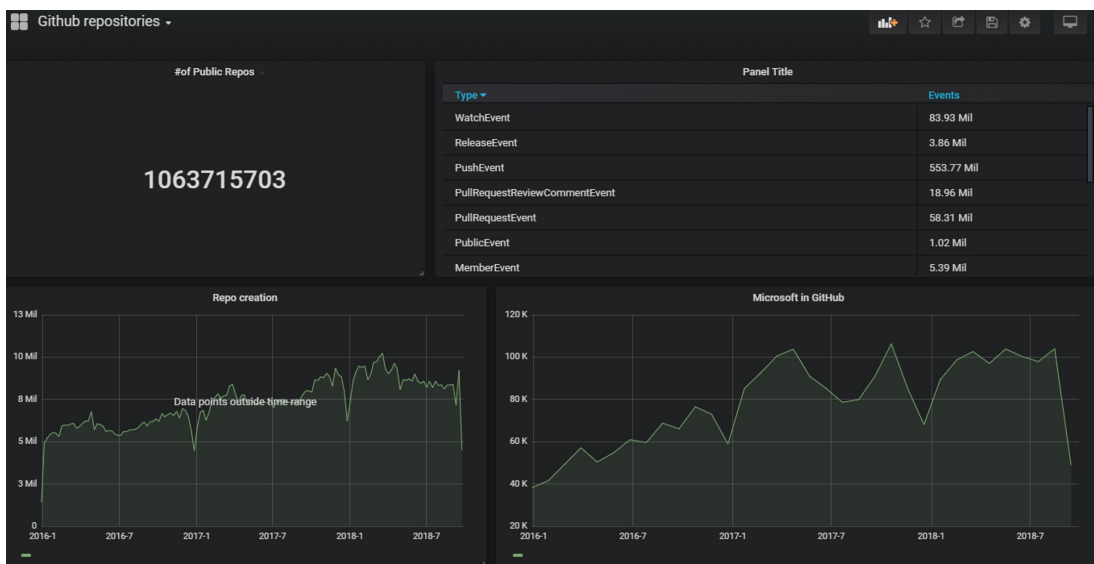
Мы спроектировали систему, которая собирает информацию, приводит её к единому формату и генерирует отчёты о текущем состоянии сетевых сервисов. Логи извлекаются из репозитория на основе стека технологий ELK (Elasticsearch, Logstash и Kibana). Затем данные конвертируются, фильтруются и упорядочиваются.

## Гибкость системы

Алгоритм находит любые отклонения от нормы и вносит обнаруженные записи в отдельную базу данных. Сотрудники SOC-команды самостоятельно задают пороговые значения и создают правила, на которые ориентируется система.

## Доступность и скорость

Полученная информация визуализируется аналитической платформой Grafana, а оповещения об инцидентах отправляются операторам через Telegram и по электронной почте. На протяжении 4 месяцев над проектом работала команда из 6 специалистов.



## Результат

Созданное нами программное решение позволяет в режиме близком к реальному времени отслеживать малейшие расхождения показателей работы сервисов с установленными нормами. Вся информация отображается на экране в понятном графическом виде, а уведомления рассылаются операторам, даже когда их нет на рабочем месте.

Например, система проинформирует персонал, если время ответа сервера должно составлять не более 500 мс, но внезапно превысило 1000 мс. Это позволит оперативно принять соответствующие меры и предотвратить сбои в работе сервисов.

Благодаря внедрению решения заказчик не только сократил расходы на мониторинг онлайн-инфраструктур, но также смог предоставлять своим клиентам ещё более качественные услуги.

**contacts@sibedge.com**

### **United States**

10362 Leola Ct # 1  
Cupertino, CA 95014

### **Australia**

1/237 Stirling Hwy,  
Claremont, 6010

### **Russia**

Tomsk  
75 Pushkina Street

Moscow  
10 Bolshaja Tulsckaja  
Street