Security pro

A system for automatic monitoring of network services

Challenge

The customer specialises in consulting and network infrastructure security support. The number of clients was growing constantly, so a system was required to automatically analyse the operation of network services and promptly notify customer employees of any emerging issues. Such a system could remove a significant part of the burden from SOC team operators and increase effectiveness. Our company is well aware of the challenges related to optimising monitoring services and improving response times for online service issues, so the customer came to us for help.

Python React

Duration
4 months

Team
Project manager — 1
Analyst — 1
Front-end developer — 2
Back-end developer — 2

Industry
Information security

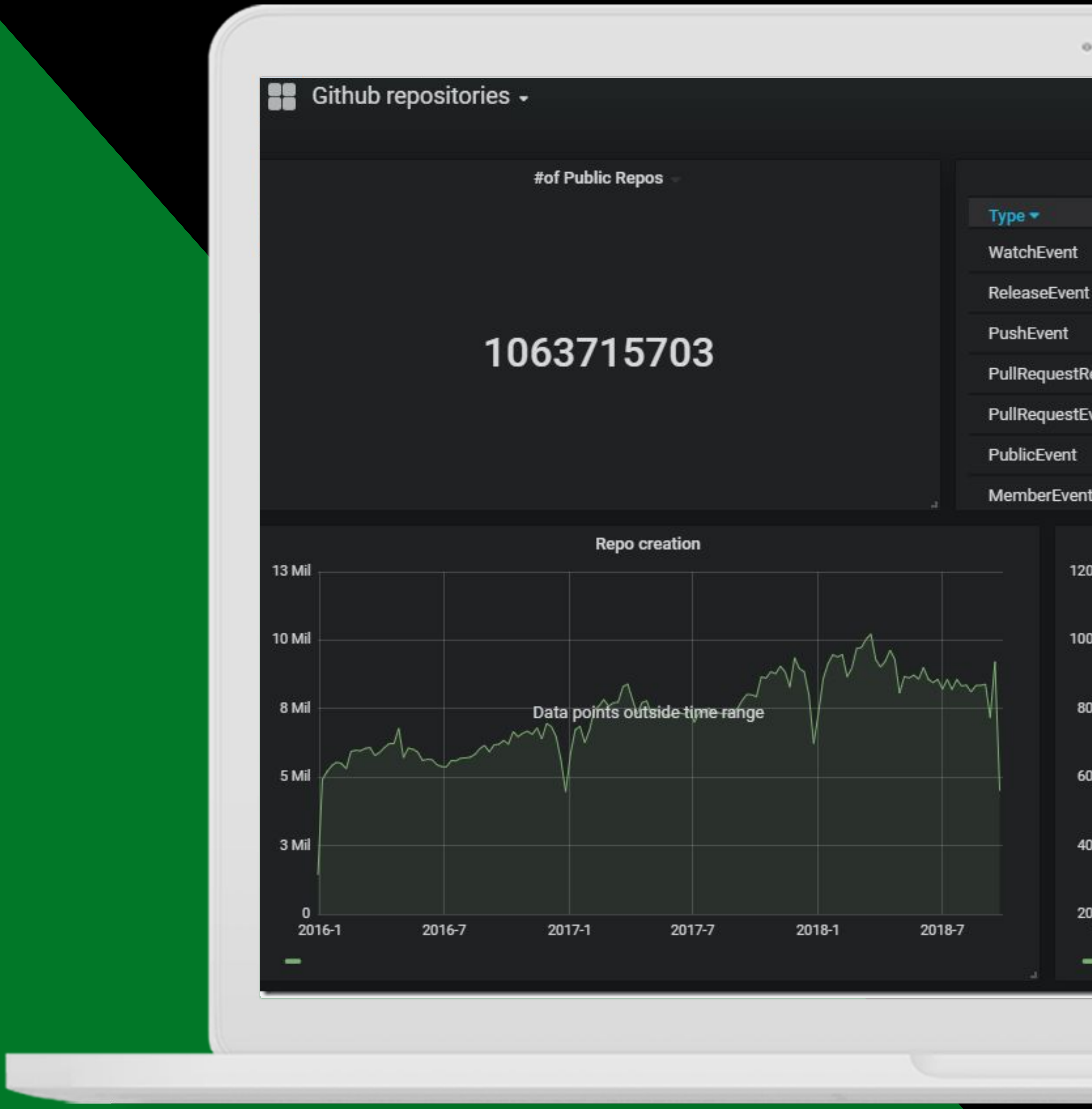
A system for automatic monitoring of network services

Solution

We designed a system which collects information, translates it into a single format and generates reports on the current status of network services. Logs are retrieved from a repository based on a stack of ELK (Elasticsearch, Logstash and Kibana) technologies. Data are then converted, filtered and organised. The algorithm finds any deviations and adds corresponding entries into a separate database. The SOC team sets customised threshold values and rules to control the operation of the system. The information obtained is then visualised by the Grafana analytics platform, and incident reports are sent to operators via the Telegram messenger and email. A team of 6 had been working at the project for 4 months.

Result

Our software solution can be used to monitor services for the slightest deviations from set values in near real time. All the information is displayed on the screen in a clear graphic format, and notifications are sent to operators even when they are away from their workplace. For instance, the system will inform personnel if server response time exceeds 1000 ms when it should not exceed 500 ms. This will allow for prompt response and prevention of any faults in the service operation. After the solution was deployed, the customer not only reduced costs for online infrastructure monitoring but also improved the quality of services provided to clients.


Github repositories
#of Public Repos
1063715703
Type
WatchEvent
ReleaseEvent
PushEvent
PullRequestR
PullRequestE
PublicEvent
MemberEvent
Repo creation
13 Mil
10 Mil
8 Mil
5 Mil
3 Mil
0
2016-1
2016-7
2017-1
2017-7
2018-1
2018-7
Data points outside time range
120
100
80
60
40
20