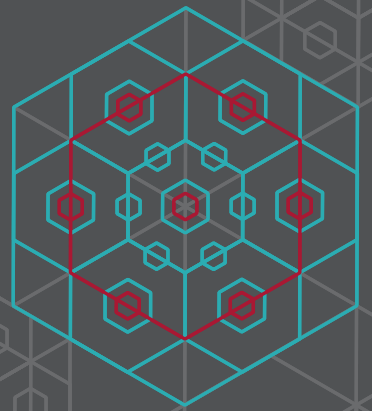
IT РОСГОССТРАХ

Как мы делали APM мониторинг на Open source

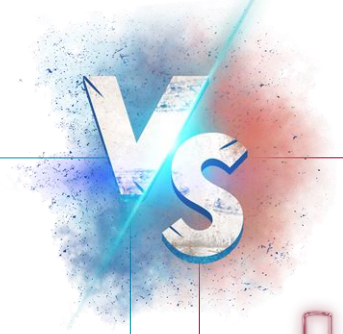


Макас Даниил

Директор департамента сопровождения и эксплуатации
Блок ИТ
ПАО СК "Росгосстрах"

IT РОСГОССТРАХ

Open source



Enterprise

Open source

+

- Гибкость
- Отсутствие лицензионных платежей

−

- Необходимость внутренней экспертизы
- Стоимость эксплуатации
- Отсутствие вендорской поддержки
- Проблематика соблюдения требований безопасности

Enterprise

+

- Соблюдение требований о конфиденциальности/безопасности данных
- Стабильность

−

- Гибкость (требует значительных затрат)
- Необходимость покупки лицензий
- Стоимость вендорской поддержки

Путь к Open source

IT РОСГОССТРАХ

2019 | 2020-2021 | 2022 | 2023

Enterprise implementation

- Переход от инфраструктурного мониторинга к мониторингу бизнес процессов
- Заключение первых SLA
- Тестирование нового подхода на процессе продаж
- Внедрение AppDynamics

В качестве нового подхода был выбран **Application Performance Monitoring**

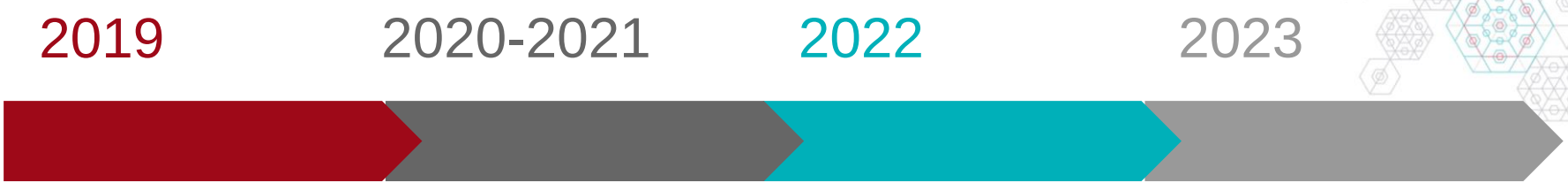
APM позволяет анализировать не только производительность ИТ-инфраструктуры, но и отслеживать ошибки внутри кода приложения для дальнейшей оценки критичности их влияния.

Для «первых шагов» в APM было найдено enterprise решение – **AppDynamics (AppD)**

Во время пилота функционал **AppD** позволил **найти и устранить** ряд критичных ошибок, влияющих на производительность, **автоматически** сформировал **baseline** по ключевым метрикам процесса.

Путь к Open source

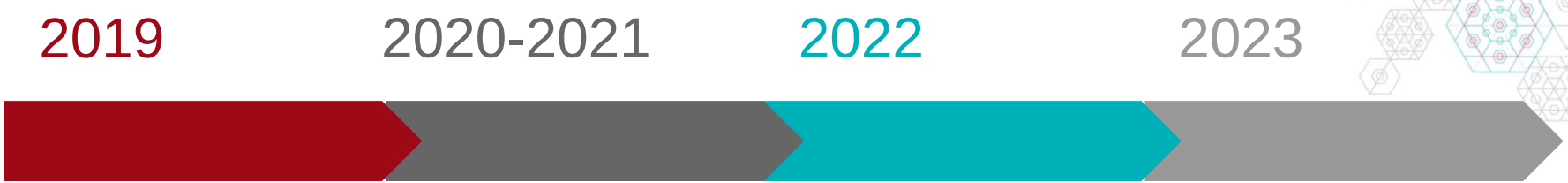
IT РОСГОССТРАХ



➢ Расширение мониторинга на Business critical процессы Компании	Настроили мониторинг таких процессов как: Учет, урегулирование убытков, расчет страховых премий, расчет комиссионных вознаграждений
➢ Внедрение новых метрик	Под **каждый бизнес процесс** был доработан процесс мониторинга путем ручного инструментирования входящих данных.
➢ Анализ опыта работы с enterprise решением	Несмотря на проработку показателей, AppD **допускал ряд ложных срабатываний**. Часть необходимых для увеличения точности алертинга доработок не удалось реализовать через запрос вендору. Проработать функционал AppD под специфику бизнеса полностью не удалось.

Путь к Open source

IT РОСГОССТРАХ



- Изменение геополитической ситуации приводит к ограничениям/полной потери поддержки со стороны вендора enterprise решений
- Государство и компании начинают рассматривать open source решения

Splunk – потерял вендорскую поддержку, закрыл доступ к репозиториям и форумам.

AppDynamics – потерял вендорскую поддержку, возможность продления лицензий, невозможно развивать и дорабатывать систему.

Минцифры объявляет о проведении с 01.05.22 г. по 30.04.24 г эксперимента по созданию **репозитория** open source продуктов в РФ.

Блок ИТ ПАО СК "Росгосстрах" проводит проработку и пилотирование первых решений на базе **open source.**

Путь к Open source

IT РОСГОССТРАХ

- Создание собственных baseline

Добавили ряд важных **исключений** в процесс построения baseline: учитываем периоды технических работ по системам, исключаем данные периодов сбоев, внесли корректировку на дни календарных праздников.

- Перевод визуализации в Grafana

Grafana позволила осуществить **более тонкую настройку** визуализаций, обеднить визуализацию данных из разных источников (реализовать **зонтичный мониторинг**).

- Создание собственного Бота и работа с каналами в Telegram

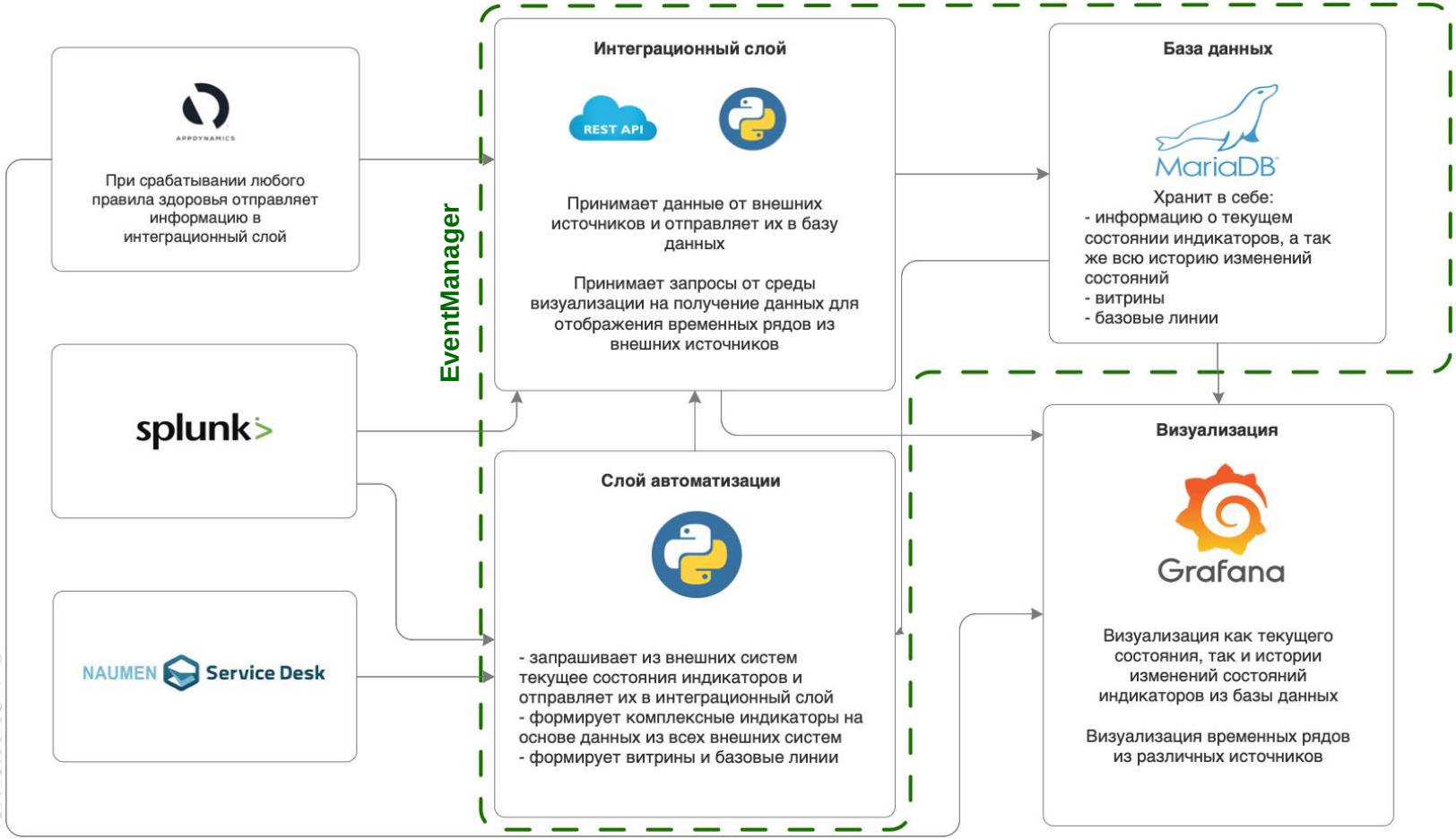
Внедрение решения на базе Telegram позволило **сократить время реакции** на алертинг, **Увеличить объём** и **функциональность** предоставляемых первичных данных по сбою.

IT РОСГОССТРАХ

Собственные решения с использованием Open Source

EventManager & Grafana

IT РОСГОССТРАХ



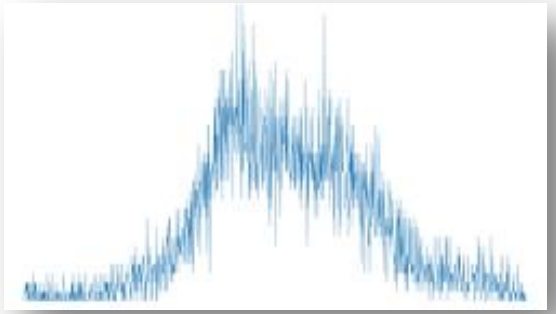
Baseline

IT РОСГОССТРАХ

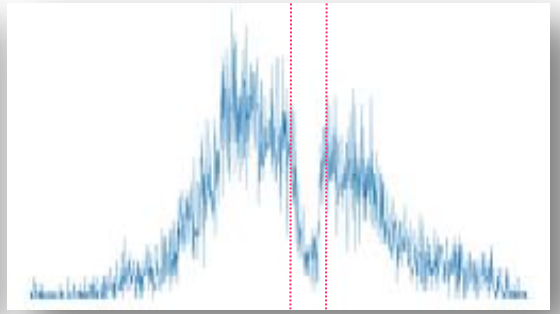
Принципы построения:

- Основывается на исторических данных, учитывая периоды сбоев в разрезе систем и продуктов
- Строится на базе производственного календаря (учитывает праздничные дни)
- Сглаживает линии за счет усреднения в окне 60 минут
- Исключает ложные срабатывания алертинга

День 1

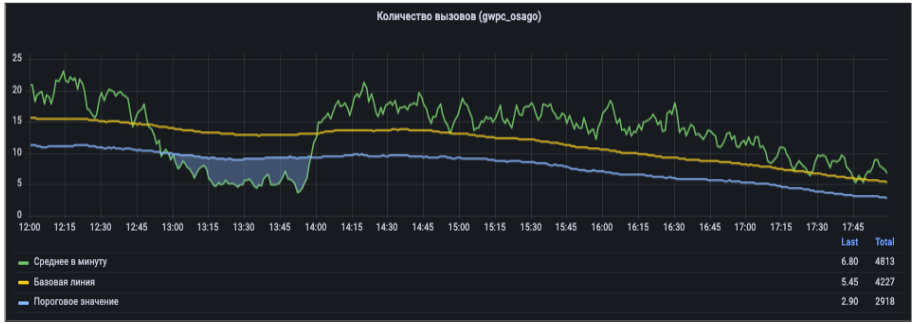


День 2



Инцидент
12:55 - 15:00

Представление на графике базовой линии из Event Manager



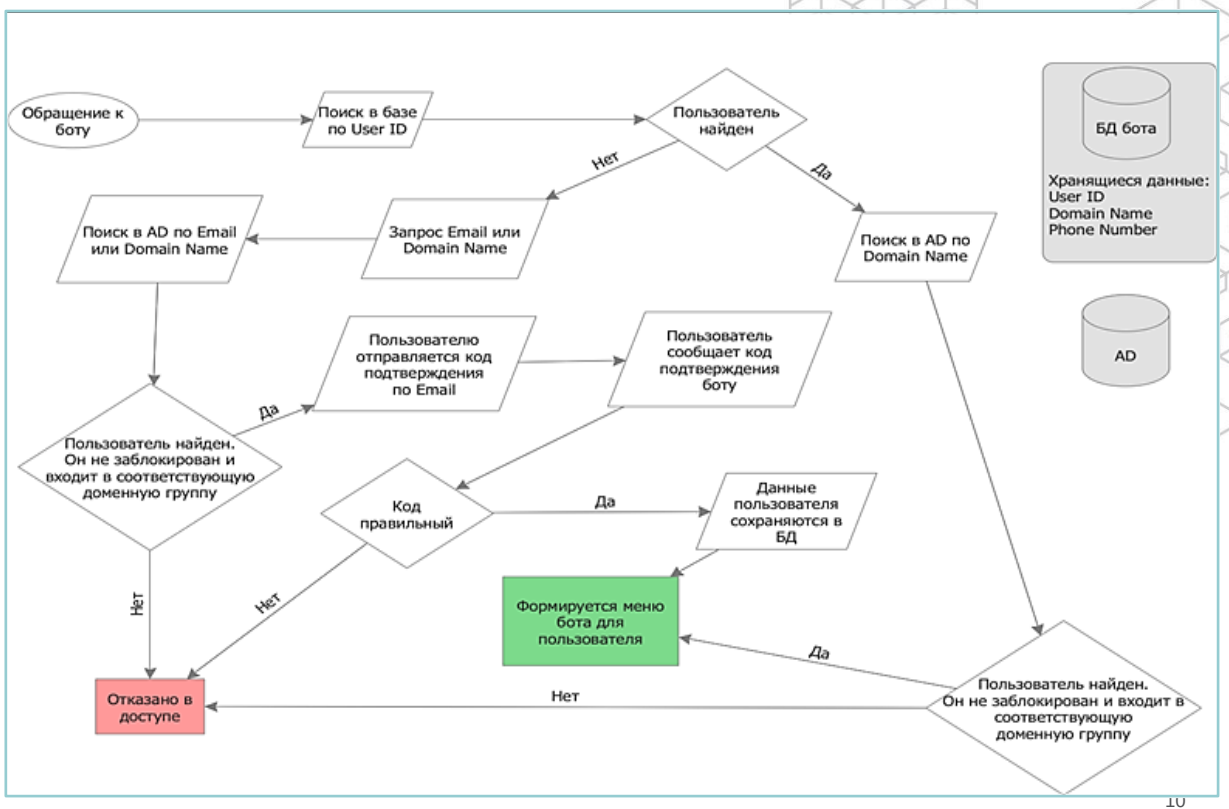
Бот в Telegram

IT РОСГОССТРАХ

Принцип работы:

Настроенные в Grafana алерты размещают информацию о своем срабатывании в каналах или группах Telegram от имени Бота

Доступ к этим каналам и группам организуется посредством добавления пользователя в соответствующие доменные группы



Бот в Telegram

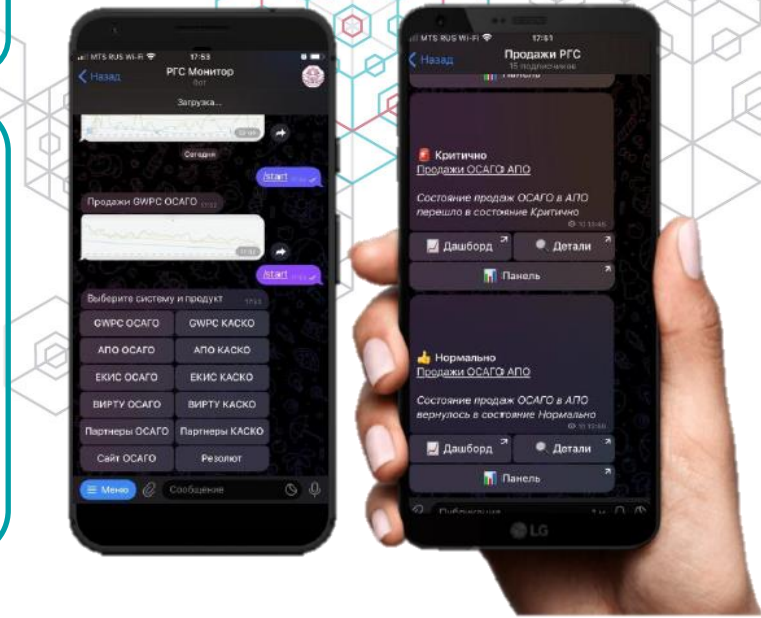
IT РОСГОССТРАХ

Текущие возможности:

- Мгновенное предоставление информации о текущем состоянии витрин по продажам;
- управление доступом к каналам оповещений и группам в Telegram.

Потенциальные возможности:

- оперативное получение любых данных, связанных с мониторингом систем;
- предоставление пользовательского интерфейса (в формате диалога с ботом) для задач, требующих принятия решения в формате «as soon as possible»



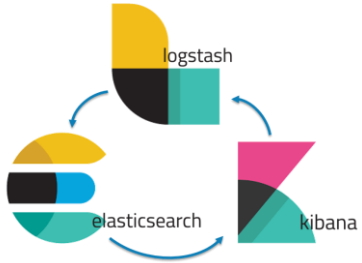
Результаты внедрения Open Source

IT РОСГОССТРАХ

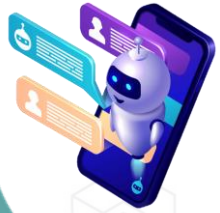
- Выстроили более точную визуализацию
- Учитываем больше метрик из разных источников
- Сократили кол-во ложных алертов, что позволило автоматизировать создание инцидентов
- Сократили время реакции при срабатывании индикатора
- При помощи бота можно получить несколько вариаций визуализации графика сбоя
- Получили экономию на лицензионной поддержке
- Нарастили внутреннюю экспертизу
- Снизили нагрузку на сотрудников отдела мониторинга
- Создали удобный сервис для просмотра динамики работы приложений в режиме on-line, что позволило произвести включение Бизнеса в мониторинг

Планы по развитию Open Source

IT РОСГОССТРАХ



Замена Splunk и AppDynamics на стек ELK



Разработка функциональности Бота

- ❑ работа с элементами service desk
- ❑ автоматизация базовых операций

Проработка интеграций с другими системами

Повышение бизнес ценности мониторинга

- ❑ разработка инструментов для Бизнеса
- ❑ введение новых метрик

IT РОСГОССТРАХ

Спасибо за внимание!