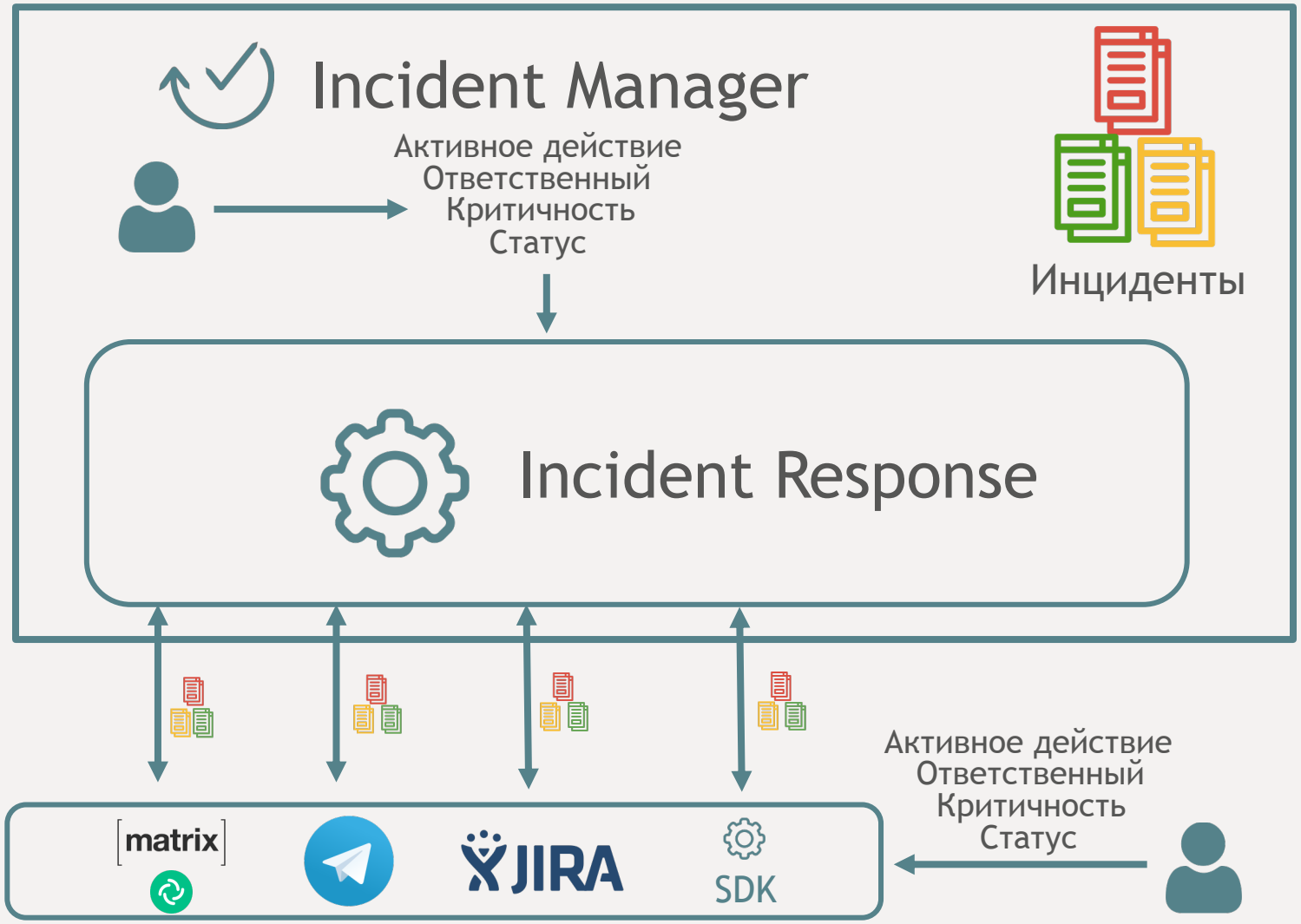
Incident Response

VB-Trend 2020

Структура модуля



Слышали про [matrix] до VB-Trend 2020?

Интеграция с [matrix]

- Matrix – opensource проект, реализующий децентрализованную систему обмена и хранения сообщения

- С помощью Synapse, который реализует весь API Matrix, можно развернуть сервер для общения у себя в инфраструктуре

- Существует множество реализаций клиентской части. Самый популярный из них – Element(Riot). Есть поддержка всех платформ!

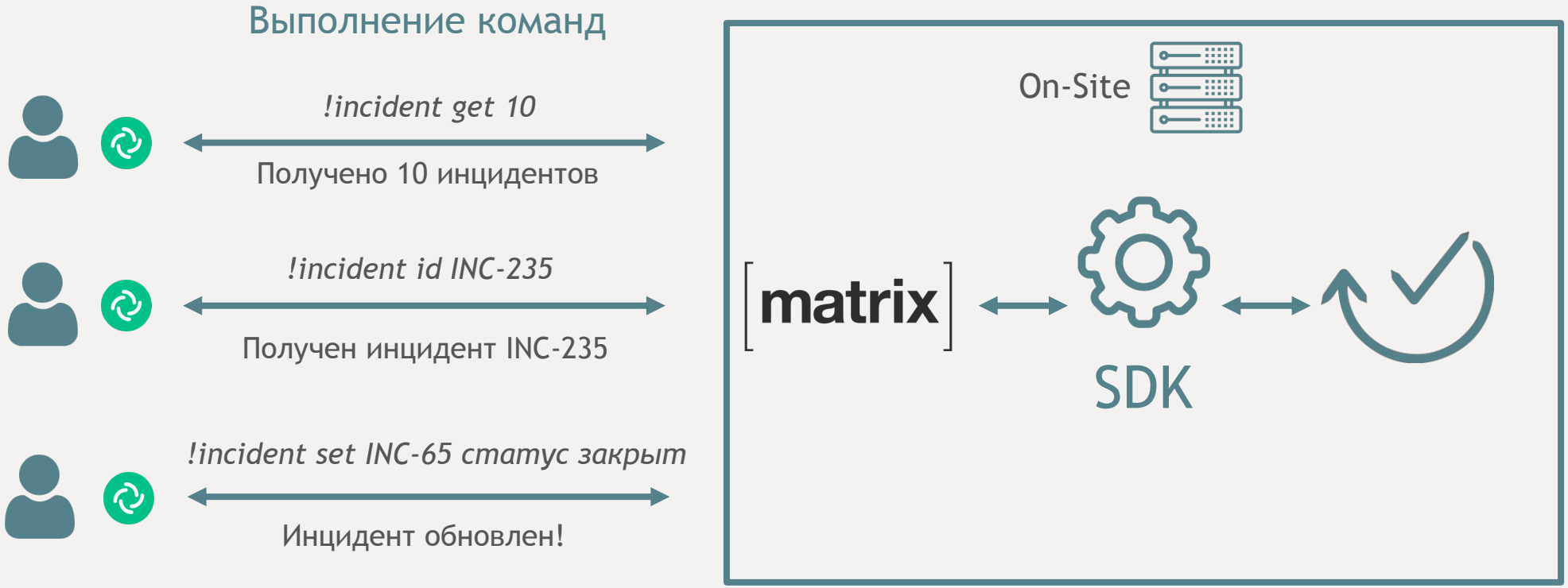
Интеграция с matrix

&

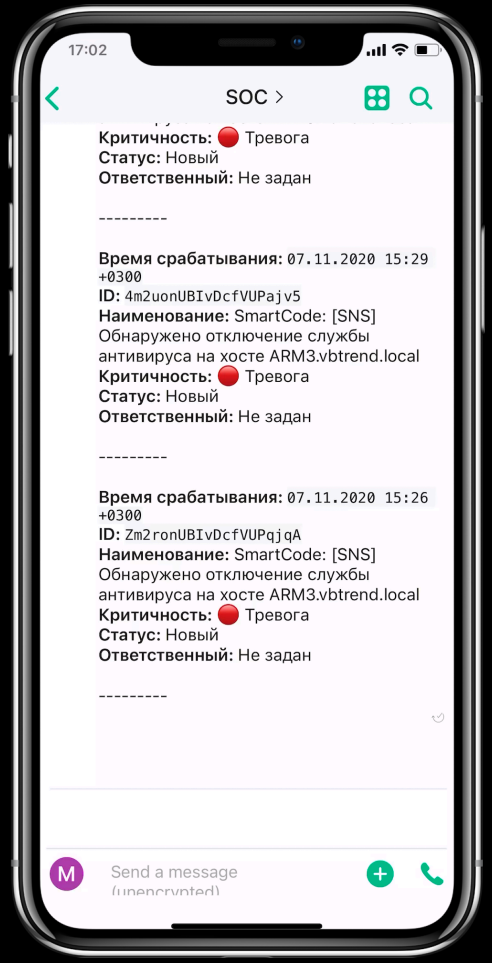
matrix

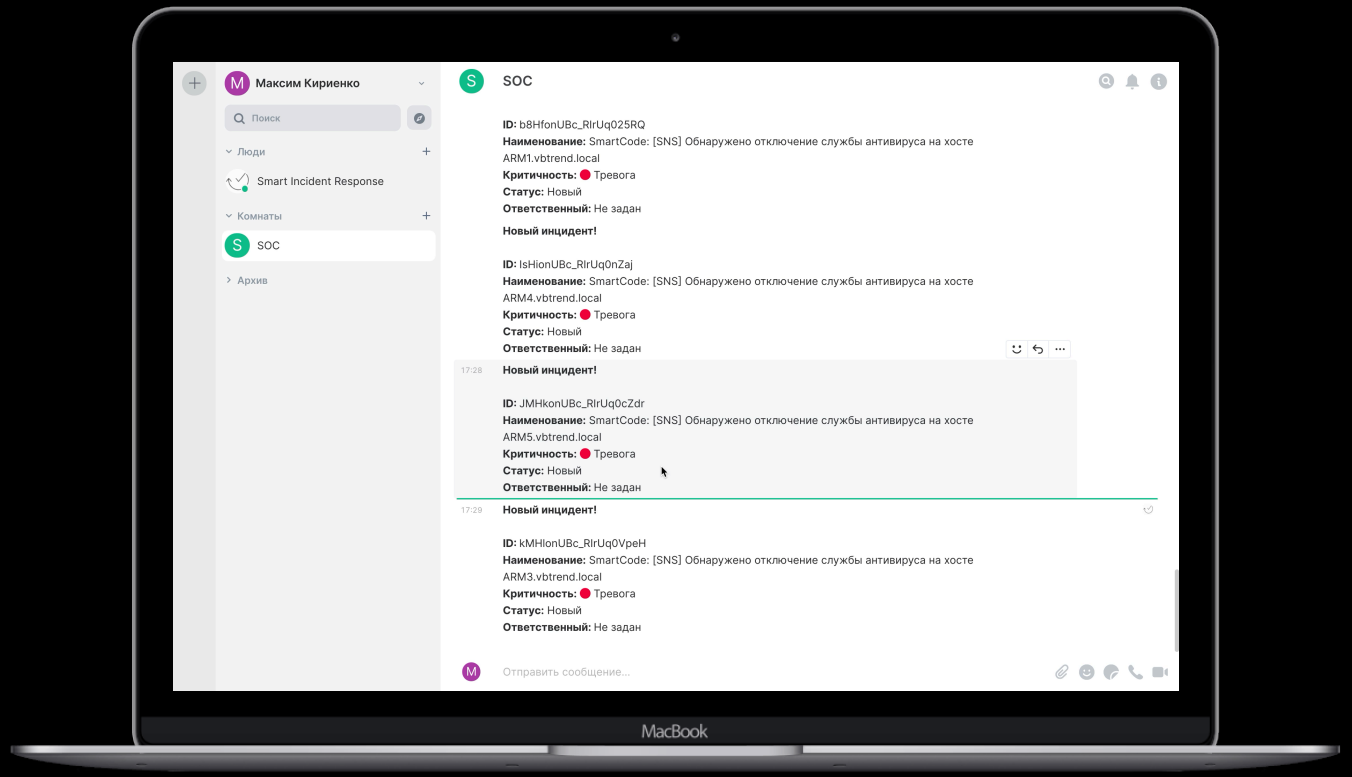
- Уведомления о создании инцидента
- Уведомления об изменении инцидента
- Получение списка последних инцидентов
- Получение информации об инциденте по ID
- Изменение параметров инцидента прямо из комнаты
- Выполнение активного действия

Архитектура решения



Интеграция с [matrix]

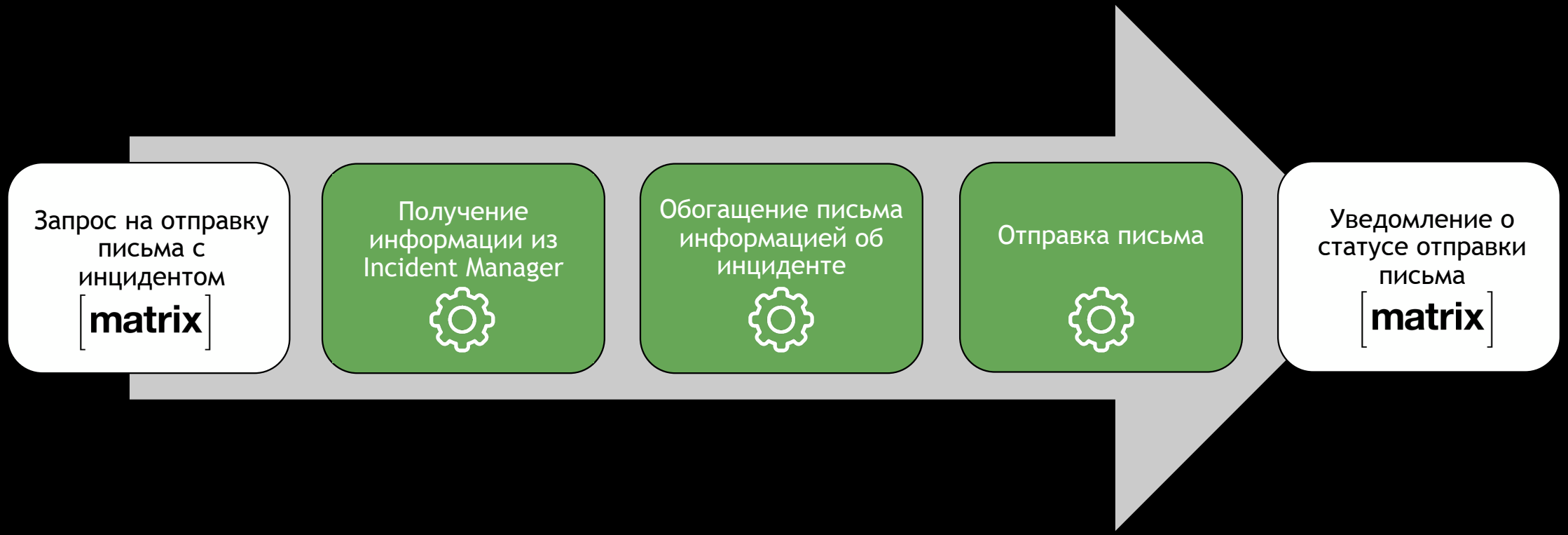




Активные действия

- Можно выполнить из любой системы, которая поддерживается в модуле Incident Response.
- Активные действия могут быть выполнены на основе информации об инцидентах
- Активное действия – это отправка письма или же запуск сканирования. Не важно!

Активное действие Email



Меньше слов, больше дела!

Демонстрация

Диапазон id инцидентов: inc-1 - inc-150

!incident set inc-1 **статус закрыт**

Спасибо за внимание!