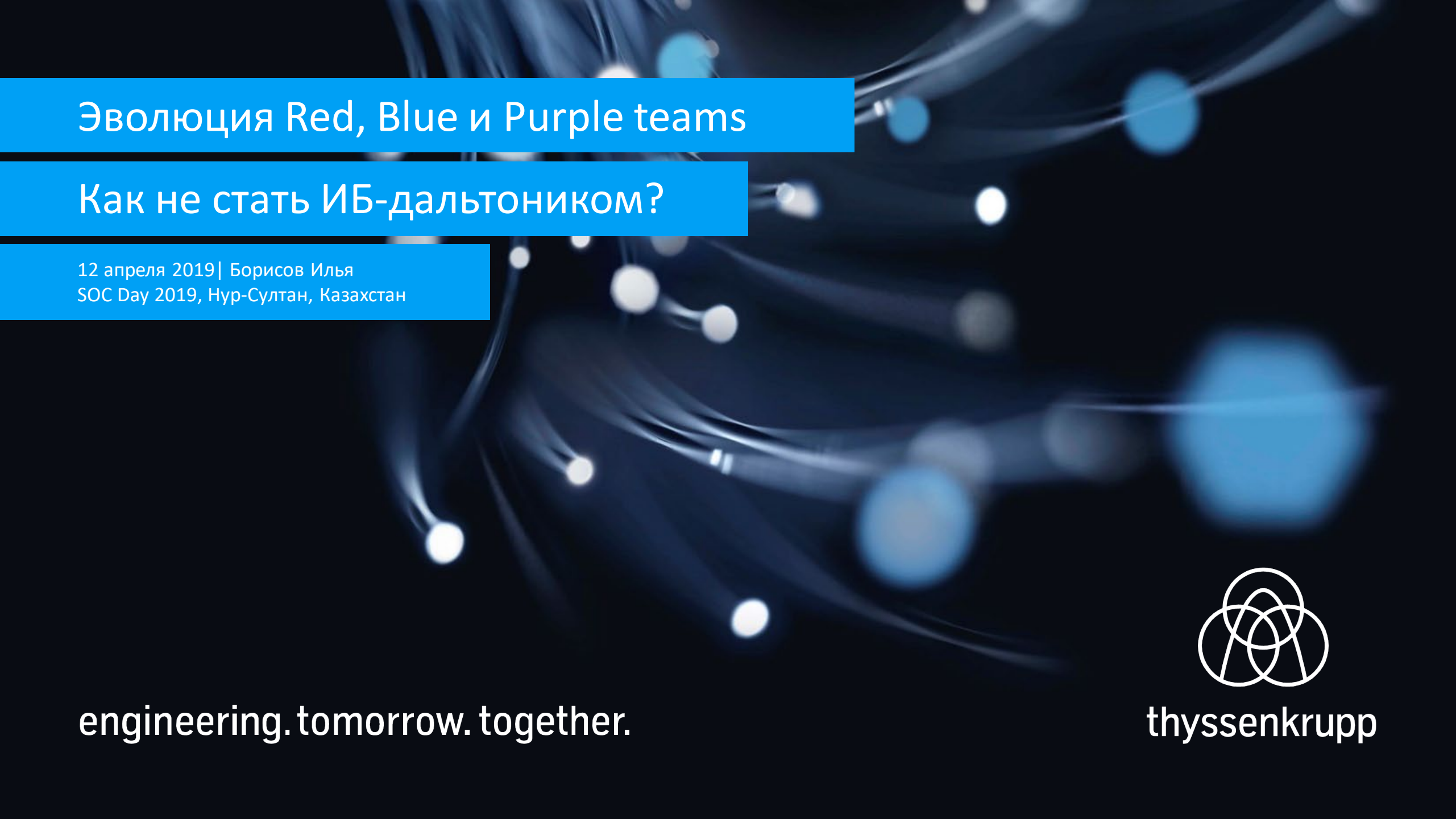
Эволюция Red, Blue и Purple teams

Как не стать ИБ-дальтоником?

12 апреля 2019| Борисов Илья
SOC Day 2019, Нур-Султан, Казахстан



Причины

- Высокие потери в ходе войны во Вьетнаме
- Отсутствие навыков ведения воздушного боя
- Низкая эффективность оружия дальнего радиуса
- Ошибки при разработке доктрины ВВС

Последствия

- Создание специальных подразделений для имитации действий противника
- Организация учений Red Flag
- Пересмотр доктрины ВВС и методов подготовки пилотов

Blue team

ОРГАНИЗОВАННОСТЬ И ВНИМАНИЕ К ДЕТАЛЯМ

АНАЛИТИЧЕСКИЕ НАВЫКИ

ГЛУБОКИЕ ЗНАНИЯ ЗАЩИТНЫХ МЕХАНИЗМОВ И МЕР

SIEM

ОБНАРУЖЕНИЕ АТАК

Red team

- НЕСТАНДАРТНОЕ МЫШЛЕНИЕ
- ГЛУБОКИЕ ЗНАНИЯ И КРУГОЗОР
- НАВЫКИ ПРОГРАММИРОВАНИЯ
- ТЕСТИРОВАНИЕ НА ПРОНИКНОВЕНИЕ
- СОЦИАЛЬНАЯ ИНЖЕНЕРИЯ

Большой и страшный отчёт для руководства

Неэффективные контроли и слабости Blue Team

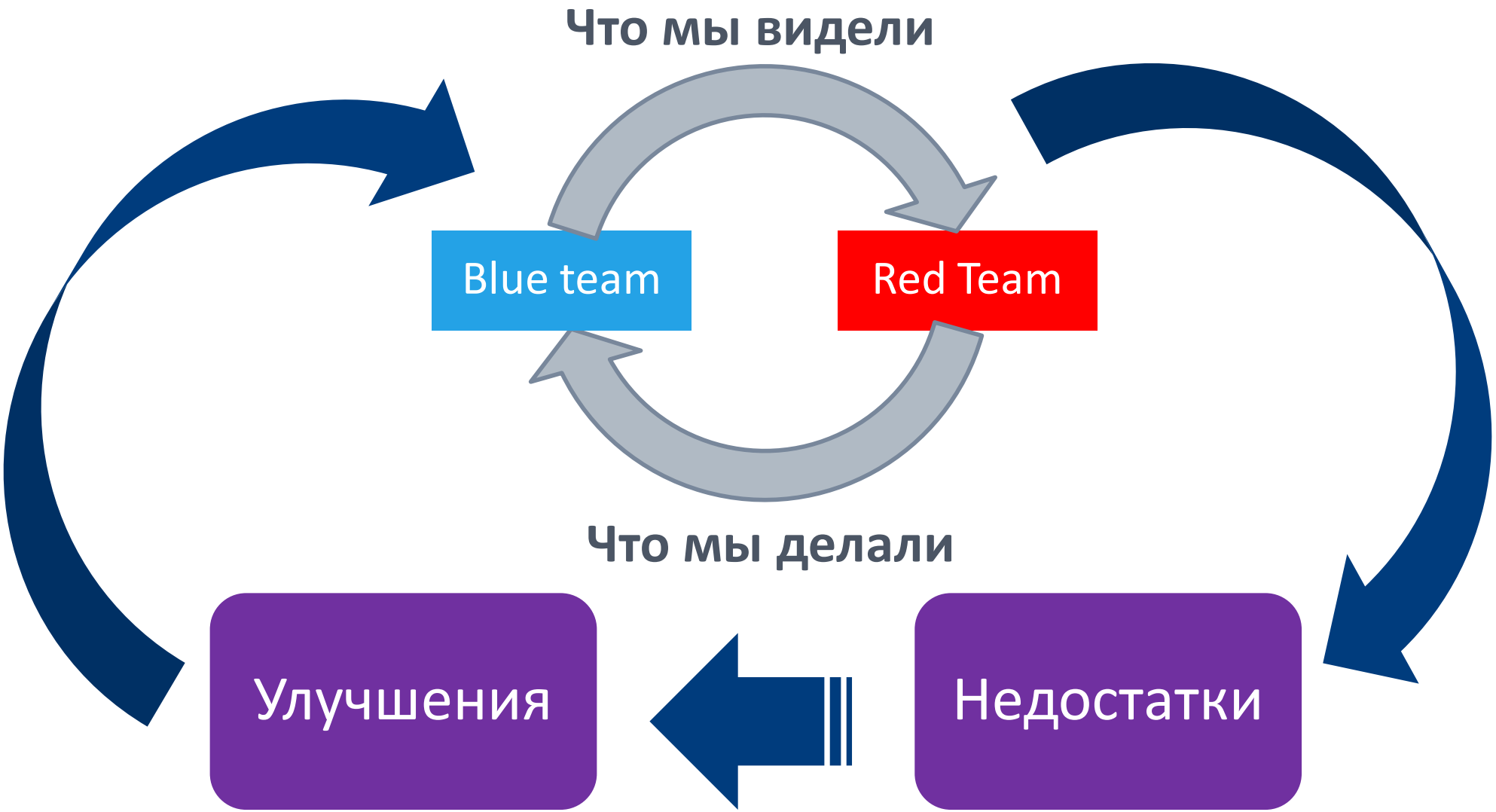
VS

Нет алертов – эффективные контроли

Много алертов – эффективная система обнаружения

Red + Blue + Purple

Purple


Что мы видели
Blue team
Red Team
Что мы делали
Улучшения
Недостатки

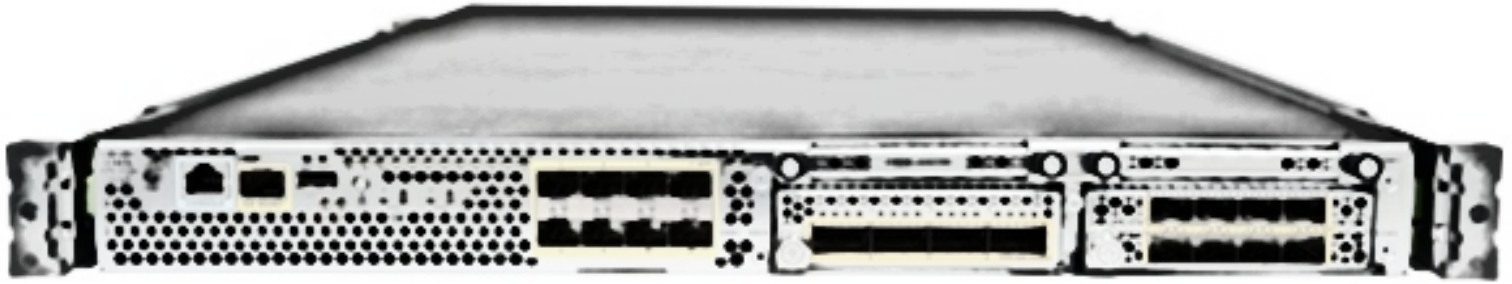
Red + Blue + Purple = ?

Детальный план реагирования на инциденты

Список уязвимостей -> шаги по устранению

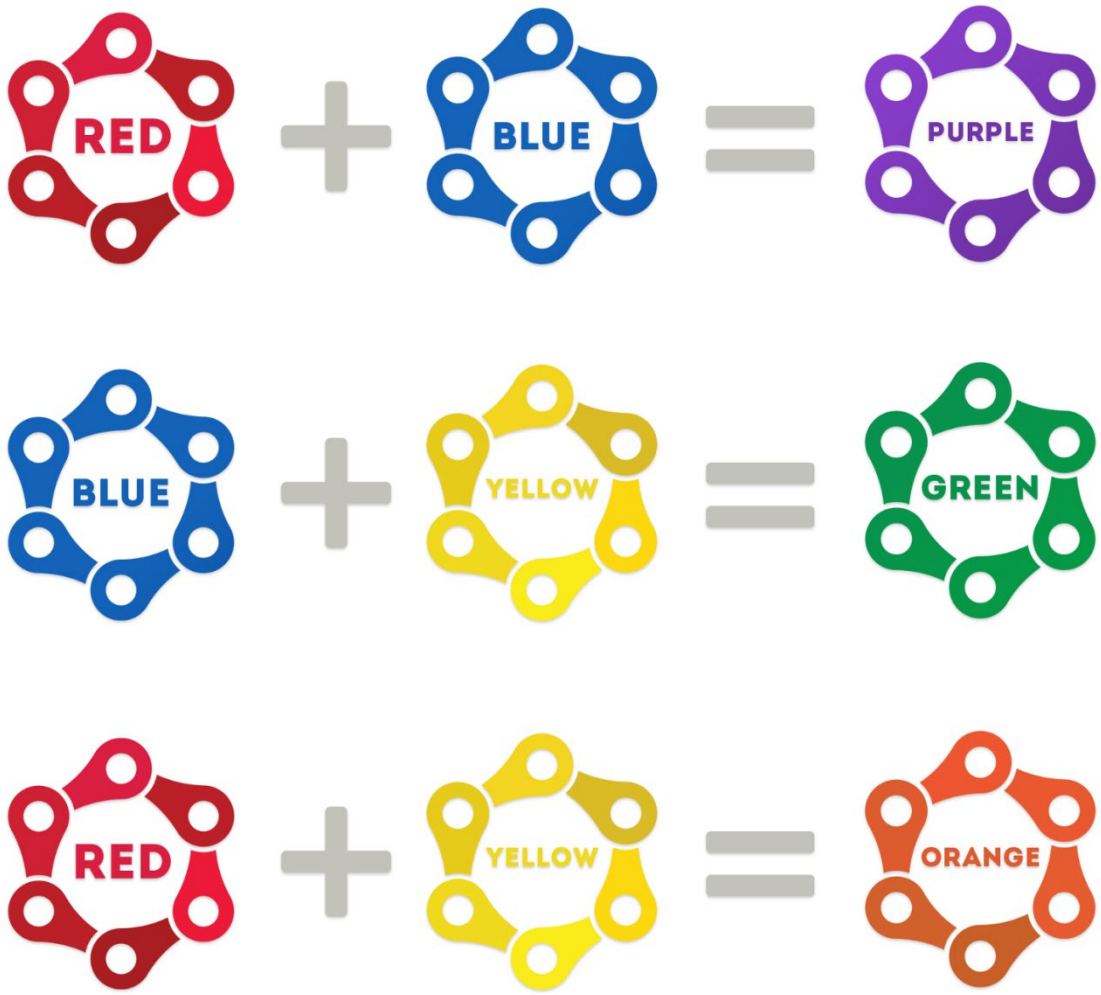
Ответ на главный вопрос

Эта дорогущая коробочка с огоньками



РАБОТАЕТ?

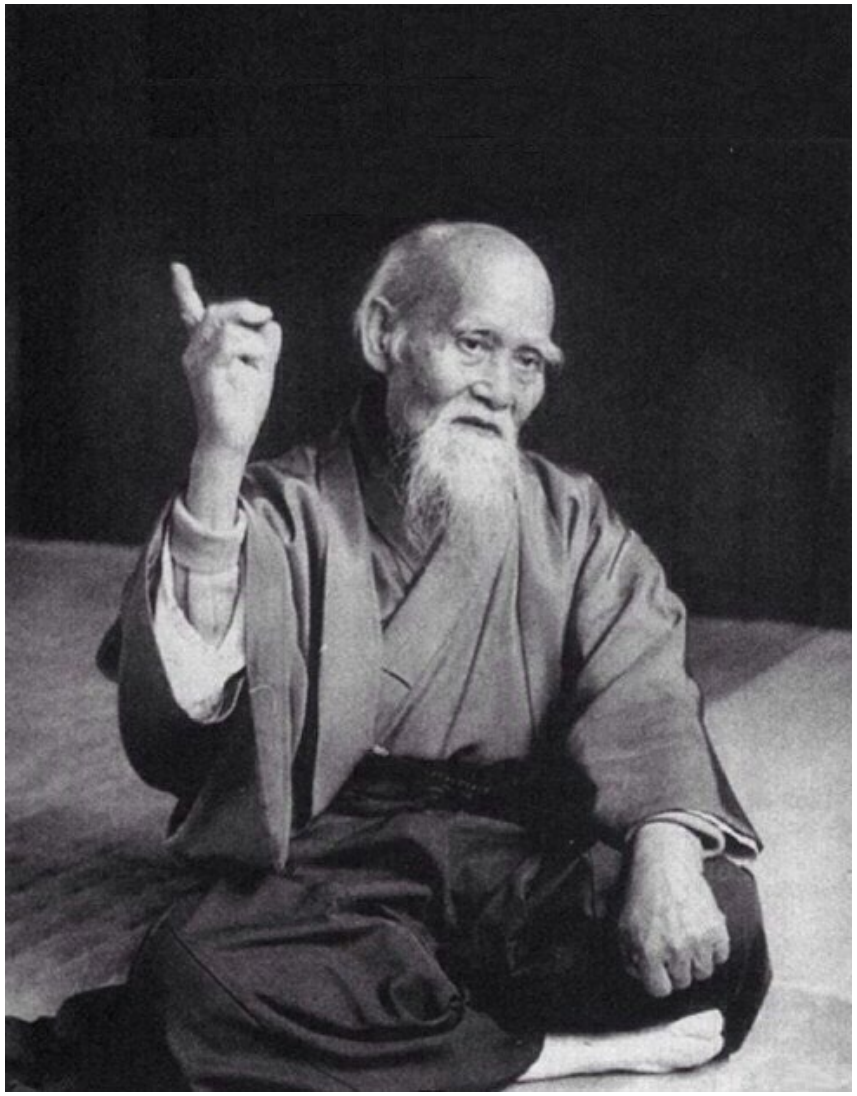
Больше цветов



YELLOW TEAM

Настоящий ИБшник в своей жизни должен сделать 3 вещи:

- **Построить SOC**
- **Посадить хакера**
- **Вырастить бюджет**



СПАСИБО ЗА ВНИМАНИЕ!

ВОПРОСЫ?