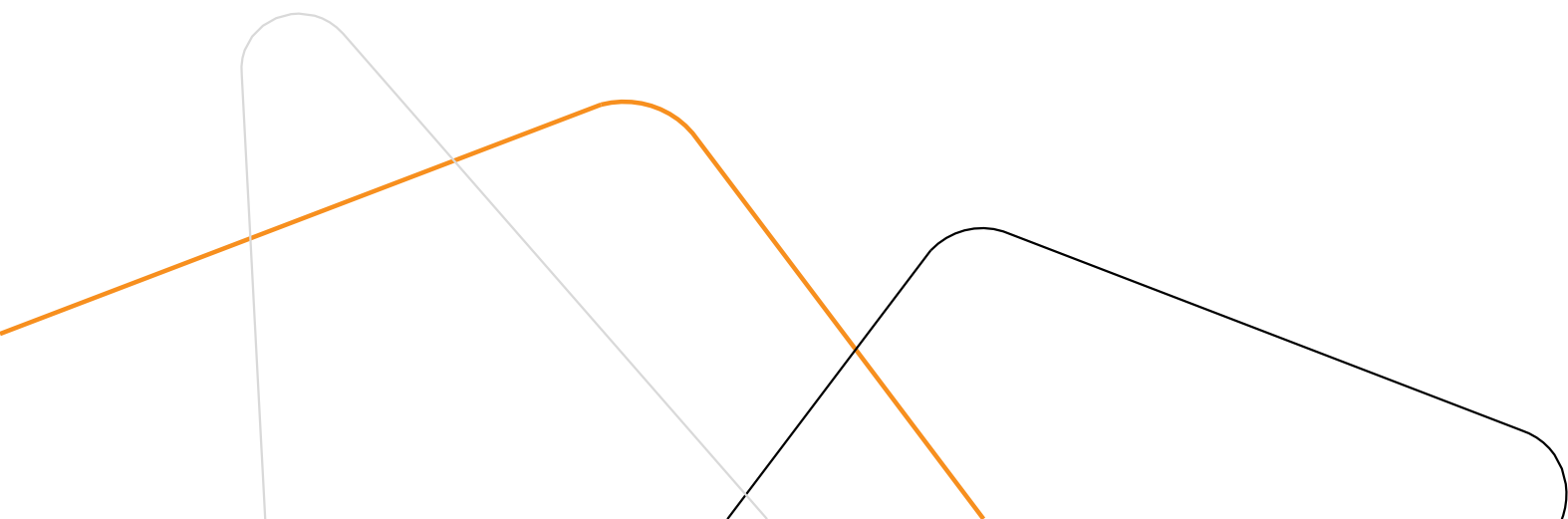


Технические особенности платформы **Ampire**

Программный комплекс обучения методам обнаружения,
анализа и устранения последствий компьютерных атак

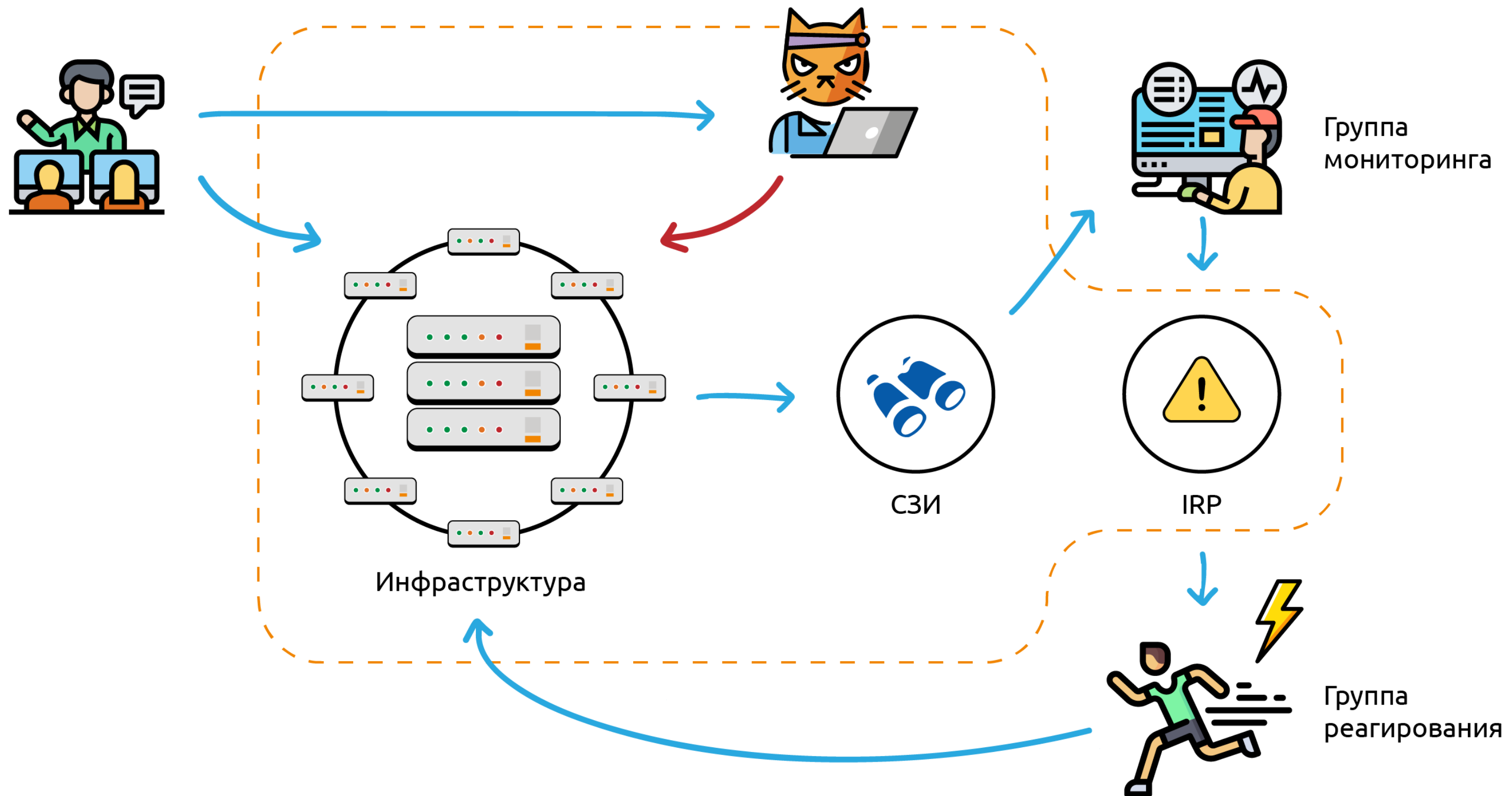




Технические преимущества Ampire

- 1) Полностью **автоматические сценарии атак**, разработанные экспертами по пентестам и базирующиеся на реальных инцидентах
- 2) Возможность создавать **собственные сценарии**
- 3) Подтверждение компетенций и **развитие навыков группы реагирования** на КА
- 4) Возможность **заказной** разработки

Полностью **автоматические** сценарии атак,
разработанные **экспертами по пентестам** и
базирующиеся на **реальных инцидентах**





Особенности проведения атак экспертом по пентестам

1) Дорого пригласить



Особенности проведения атак экспертом по пентестам

- 1) Дорого пригласить
- 2) В 100% этапы и техника атак будут отличаться



Особенности проведения атак экспертом по пентестам

- 1) Дорого пригласить
- 2) В 100% этапы и техника атак будут отличаться
- 3) Результат не гарантирован



Особенности проведения атак экспертом по пентестам

- 1) Дорого пригласить
- 2) В 100% этапы и техника атак будут отличаться
- 3) Результат не гарантирован
- 4) Учебный процесс не организовать

Что дает **автоматизация**



1) Непрерывный учебный процесс

Что дает **автоматизация**



- 1) Непрерывный учебный процесс
- 2) Масштабирование

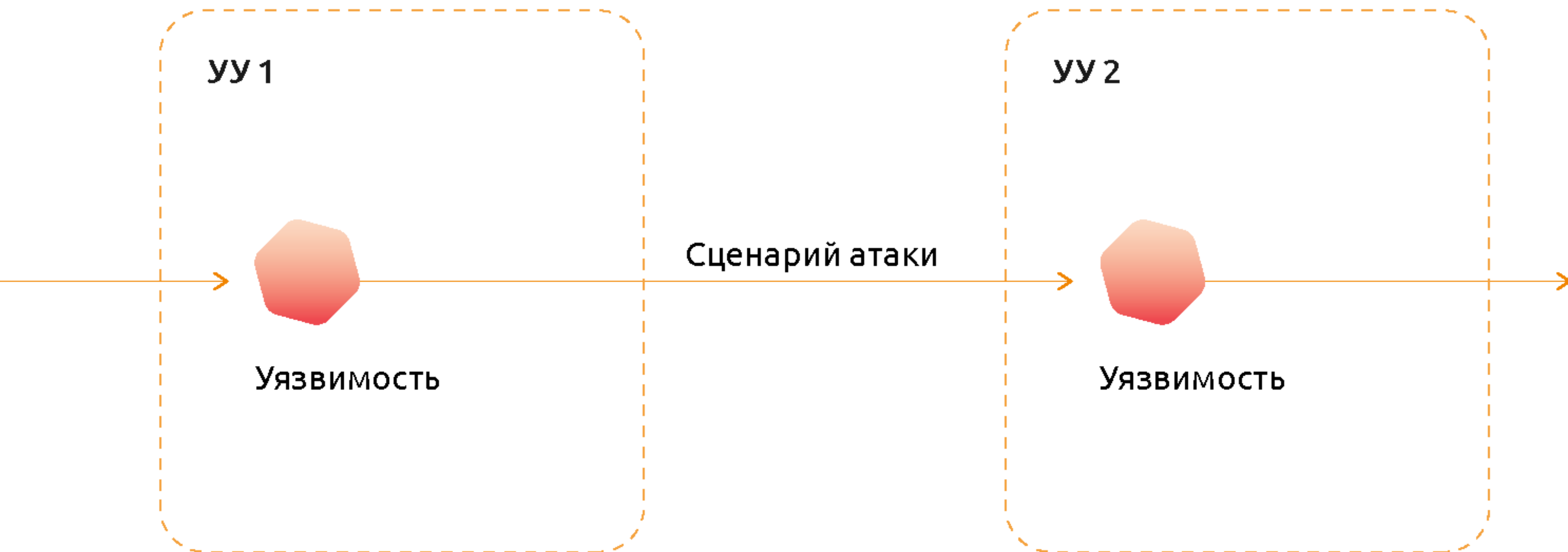
Что дает **автоматизация**



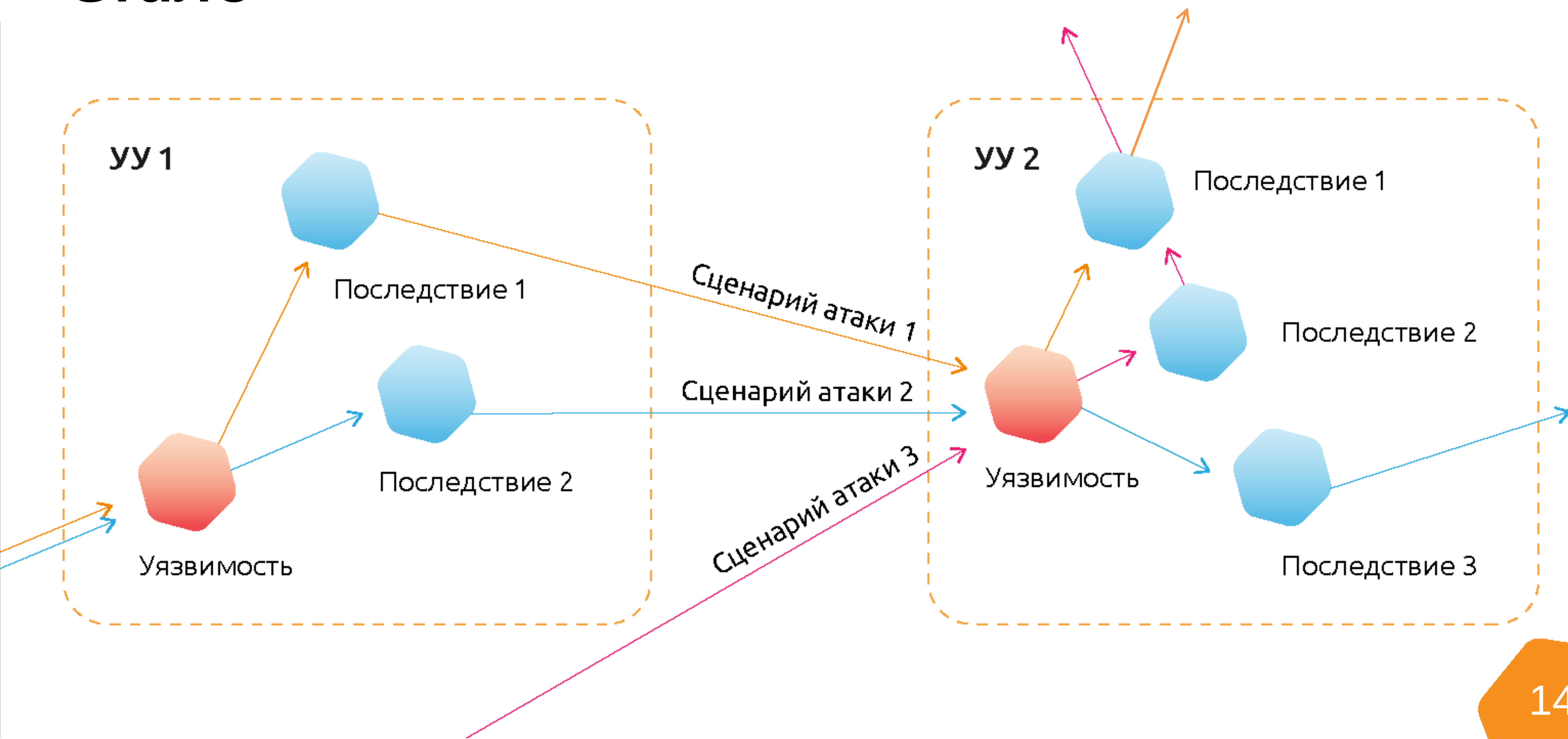
- 1) Непрерывный учебный процесс
- 2) Масштабирование
- 3) Снижение на порядок требований к преподавателям

Возможность создавать **собственные
сценарии**

Было



Стало



Шаблон

Сегмент

ОС

Поиск



MS Exchange

Уязвимостей: 3 Последствий: 5

Шаблон: Предприятие (конфигуратор)

Сегмент: Data Center

Операционная система: -

SSH Server

Уязвимостей: 1 Последствий: 1

Шаблон: Предприятие (конфигуратор)

Сегмент: DMZ

Операционная система: -

Umbraco

Уязвимостей: 1 Последствий: 5

Шаблон: Предприятие (конфигуратор)

Сегмент: DMZ

Операционная система: -

CMS WordPress

Уязвимостей: 2 Последствий: 5

Шаблон: Предприятие (конфигуратор)

Сегмент: DMZ

Операционная система: -

MS Active Directory

Уязвимостей: 1 Последствий: 7

Шаблон: Предприятие (конфигуратор)

Сегмент: Data Center

Операционная система: -

Веб сервер Osint

Уязвимостей: 0 Последствий: 0

Шаблон: OSINT

Сегмент: Внутренняя сеть OSINT

Операционная система: -

GitLab

Уязвимостей: 0 Последствий: 0

Шаблон: Предприятие (конфигуратор)

Сегмент: Data Center

Операционная система: -

SuiteCRM

Уязвимостей: 0 Последствий: 0

Шаблон: Предприятие (конфигуратор)

Сегмент: Data Center

Операционная система: -

RocketChat

Уязвимостей: 0 Последствий: 0

Шаблон: Предприятие (конфигуратор)

Сегмент: Data Center

Операционная система: -

Solr

Уязвимостей: 0 Последствий: 0

Шаблон: Предприятие (конфигуратор)

Сегмент: Data Center

Операционная система: -

OpenSMTPD

Уязвимостей: 0 Последствий: 0

Шаблон: Предприятие (конфигуратор)

Сегмент: Data Center

Операционная система: -



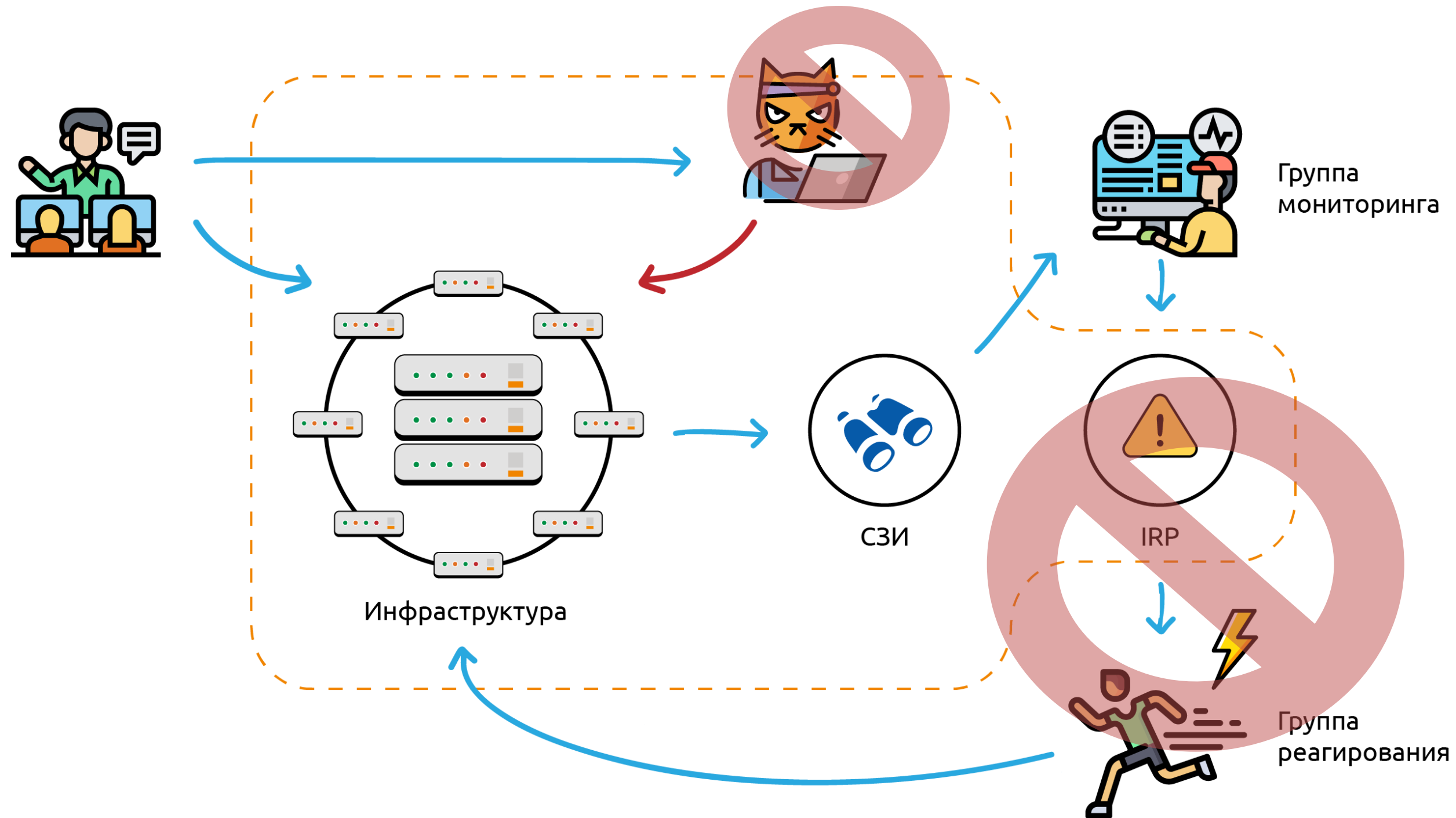
Авторизация



войти

Подтверждение **компетенций и развитие**
навыков группы реагирования на
компьютерные атаки

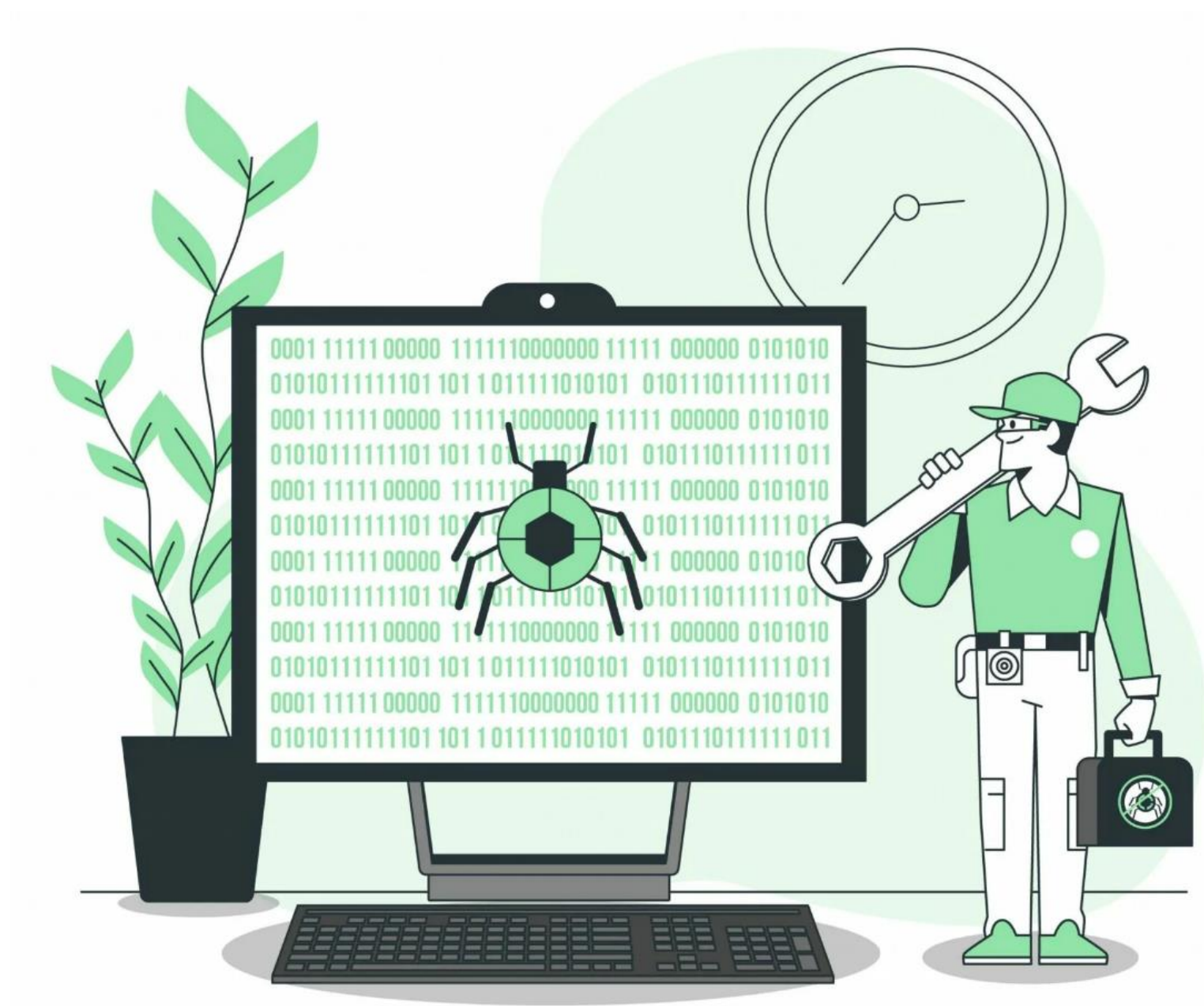
Что мы видим в других полигонах



Заметить - важно, а устранить - важнее



- 1) Учим эффективно исправлять
- 2) Собственные исследования и разработка хотфиксов
- 3) Устранение последствий компьютерных атак



Возможность **заказной** разработки

Империя в коробке



Сделаем на заказ:

- 1) Новый тип занятий
- 2) Новый шаблон
- 3) Новый сценарий



Анонс новых версий **Ampire**



- 1) Формат RedTeam (версия 1.3 – июль 2023)
- 2) Формат PurpleTeam, Empire Junior (версия 1.4 – октябрь 2023)
- 3) Лабораторные работы, Тематические курсы (версия 1.5 – март 2024)

Спасибо
за внимание!



t.me/pm_public

amonitoring.ru

Александр Пушкин

Технический директор
«Перспективный мониторинг»

@Nesergeevich