360° Ampire

КОНФЕРЕНЦИЯ КИБЕРПОЛИГОНОВ

Вместе против цифровой уязвимости

24 апреля

г.Москва, Кибердом

Конфигуратор в действии. Как создать свой сценарий на киберполигоне

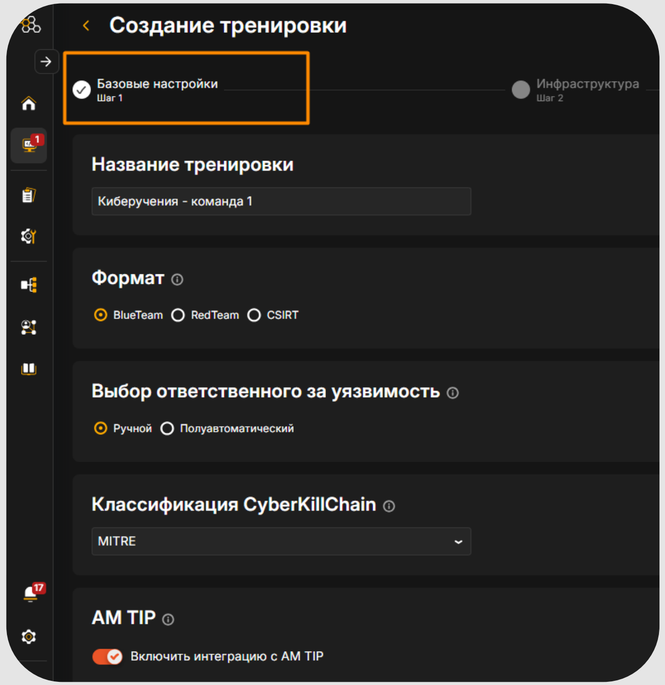
Кабакова Наталия,

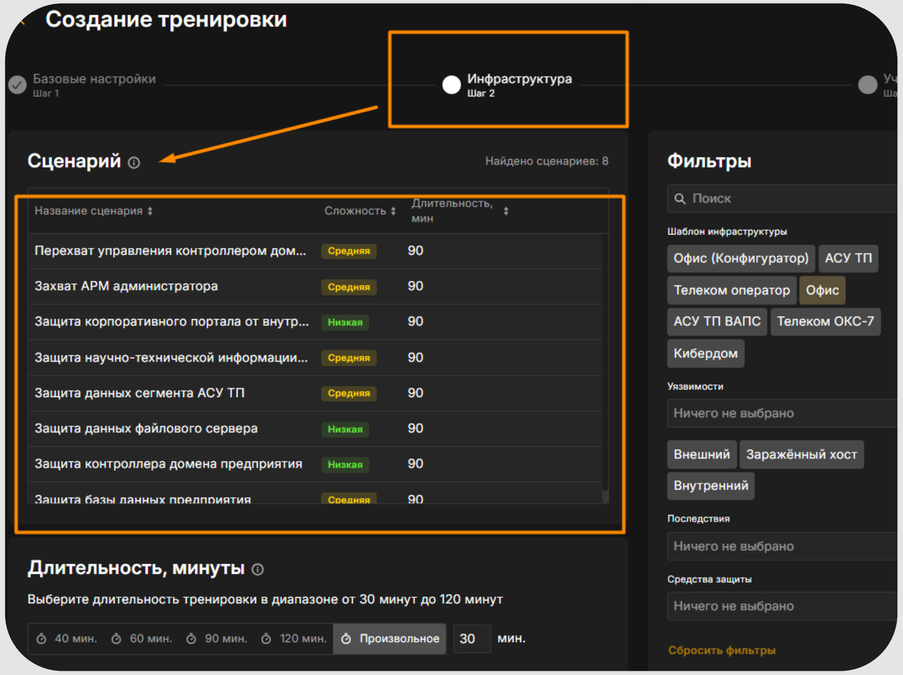
старший специалист по ИБ,
«Перспективный мониторинг»

Ampire 360°

Конфигуратор в действии

Создание тренировки





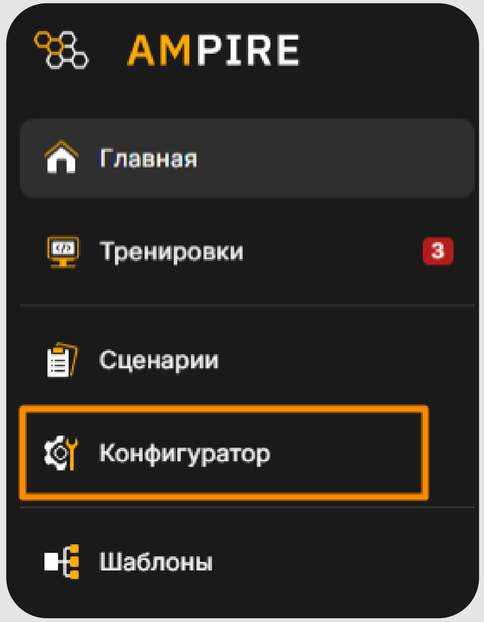
Ограниченный набор сценариев

Ampire 360°

Конфигуратор в действии

Создание тренировки

Ограниченный набор сценариев → Что делать? → Идея Конфигуратора



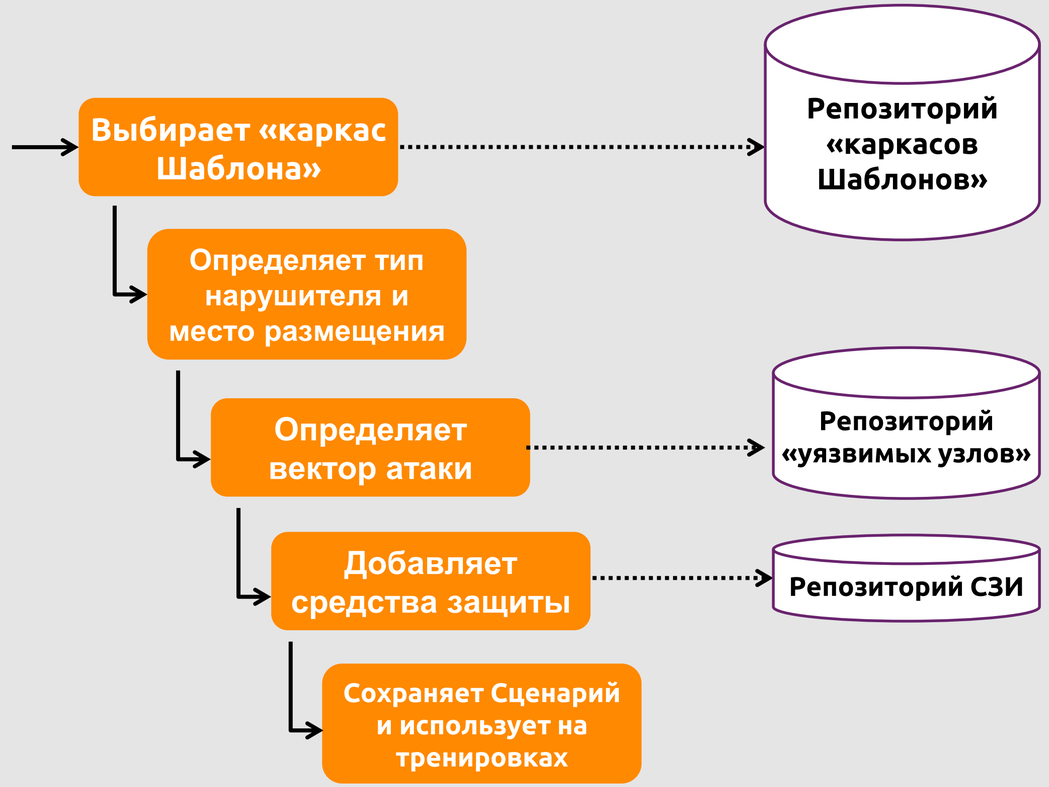
Идея Конфигуратора —
дать возможность преподавателю самостоятельно подготавливать шаблон организации и формировать вектор атаки

Ampire 360°

Конфигуратор в действии

Идея Конфигуратора

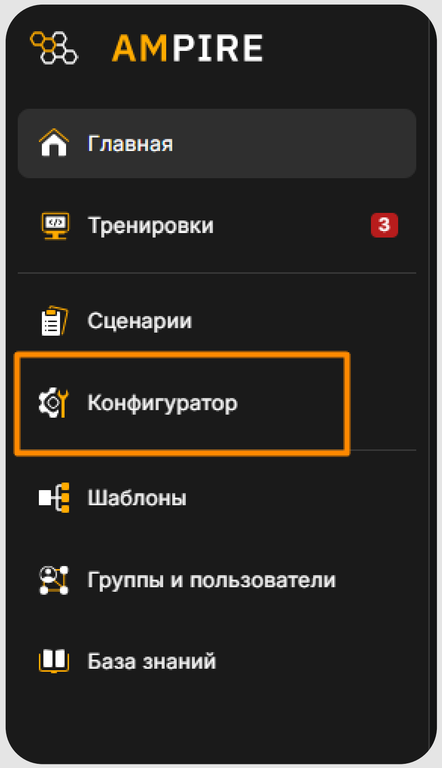
Конфигуратор дает возможность преподавателю самостоятельно подготавливать шаблон организации и формировать вектор атаки

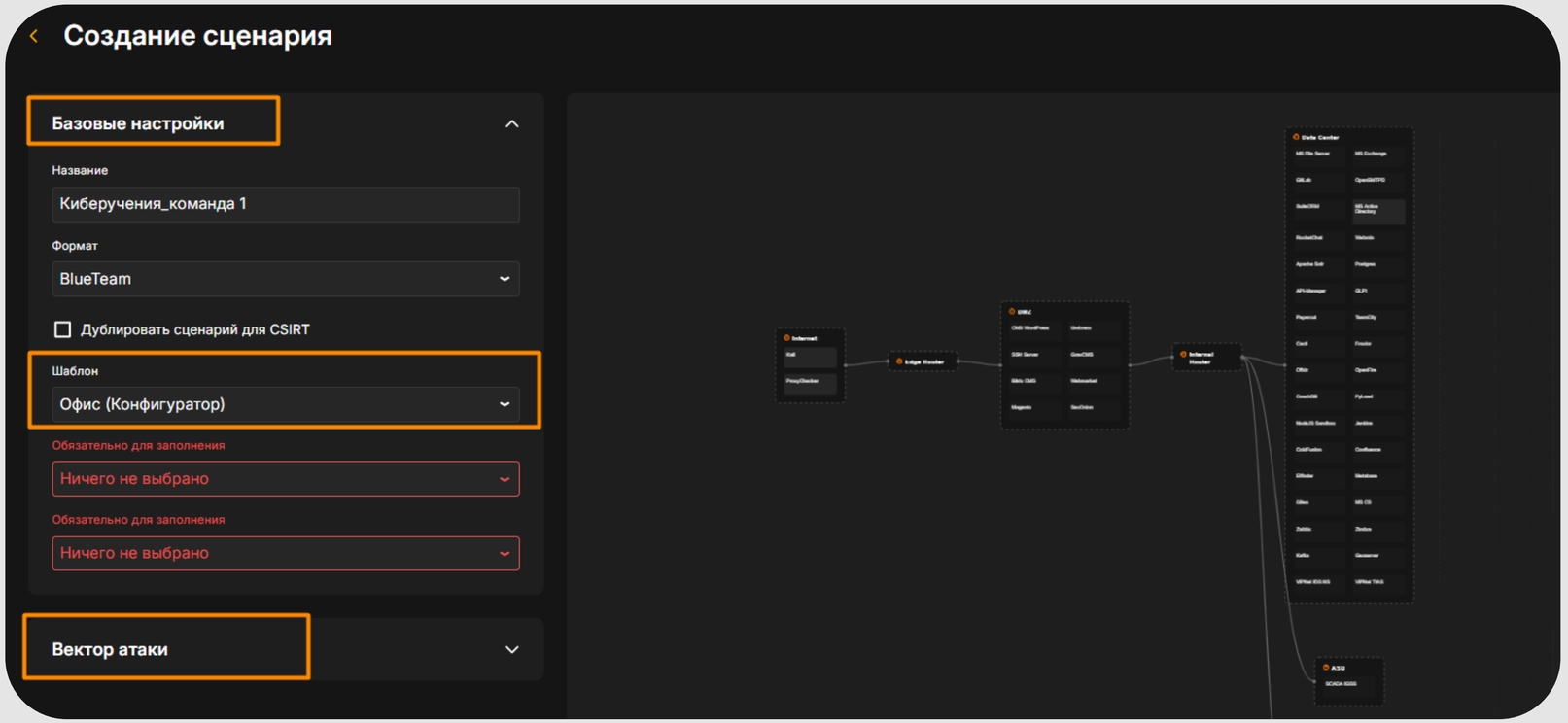


Ampire 360°

Конфигуратор в действии

Интерфейс





Ampire 360°

Конфигуратор в действии

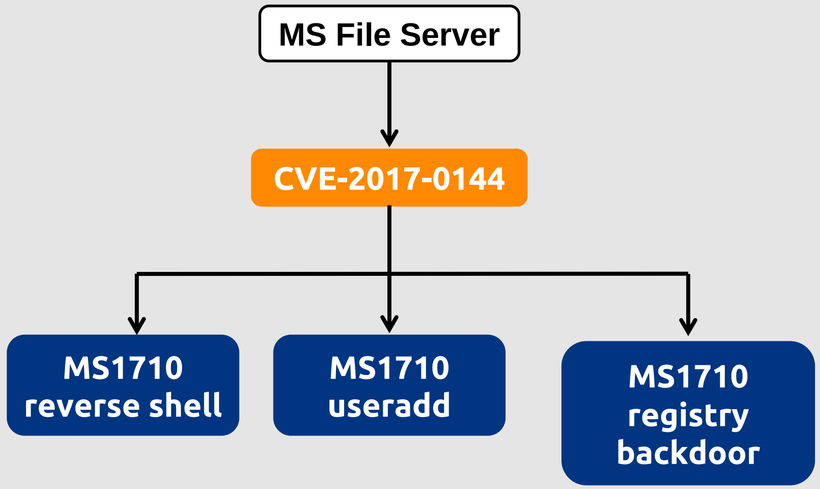
Уязвимый узел

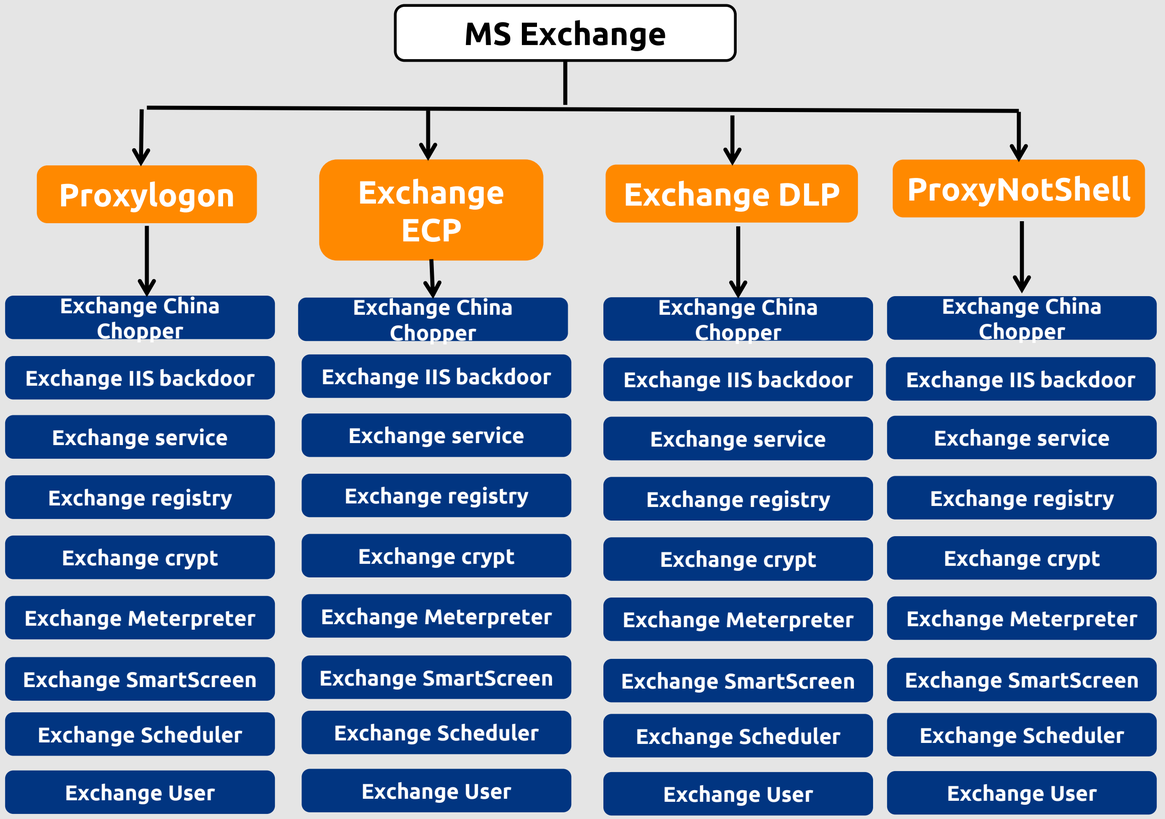
1. Виртуальная машина
2. Содержит 1 или более уязвимостей
3. Содержит 1 или более последствий эксплуатации уязвимости
4. Содержит чекеры
5. Документация в установленном формате

Ampire 360°

Конфигуратор в действии

Уязвимый узел





Ampire 360°

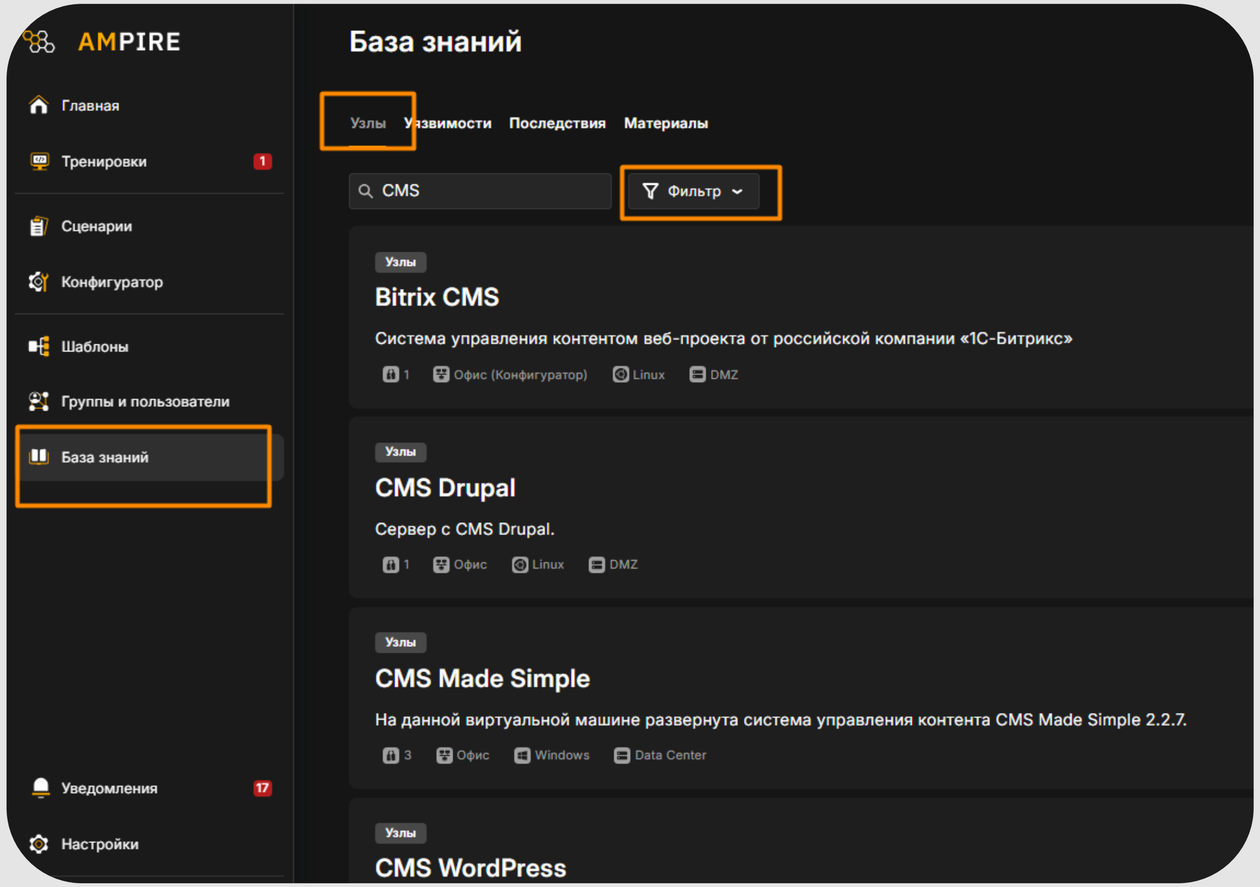
Конфигуратор в действии

Уязвимый узел

База знаний – источник информации

об уязвимых узлах, интегрированных

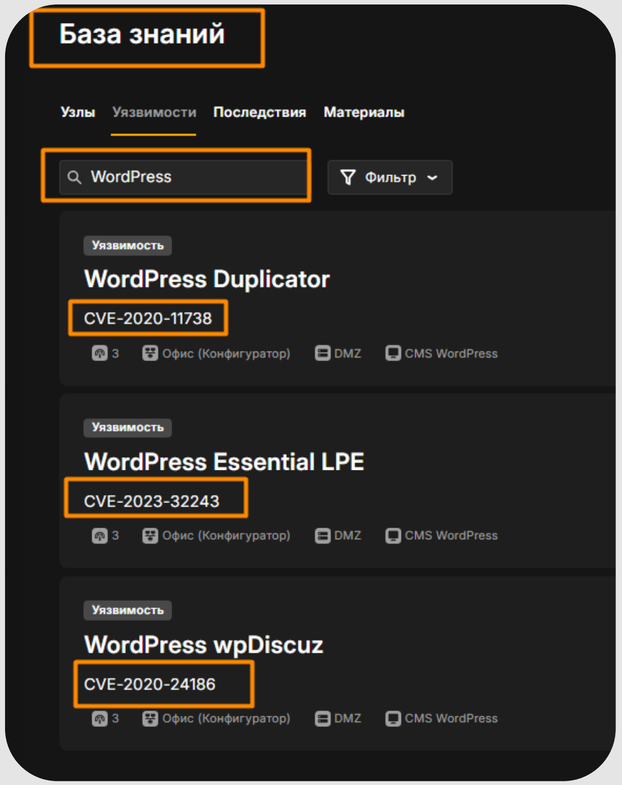
в Киберполигон

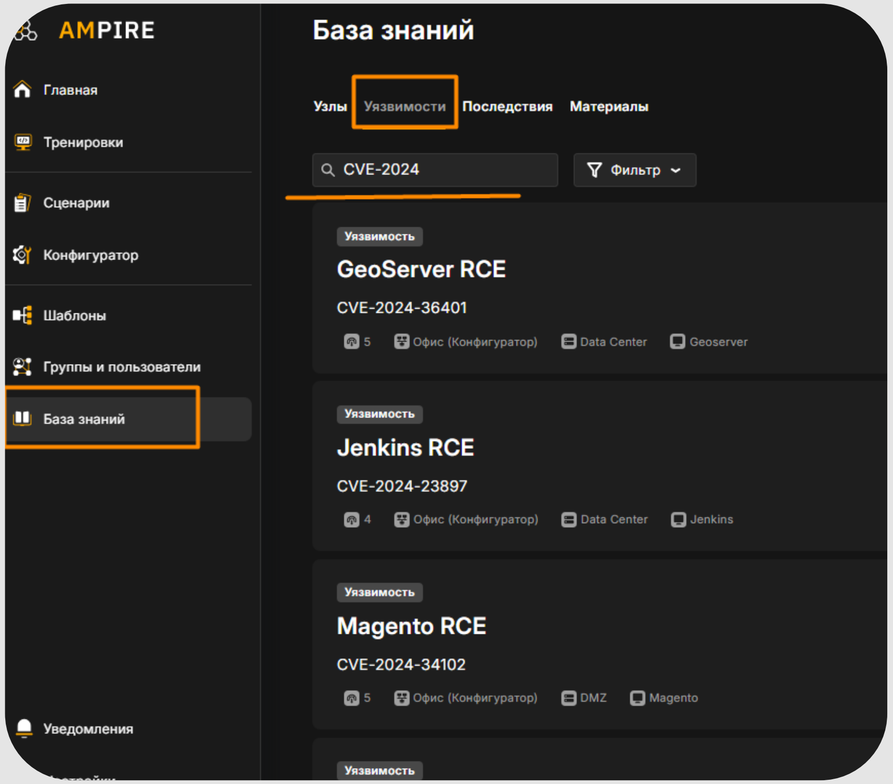


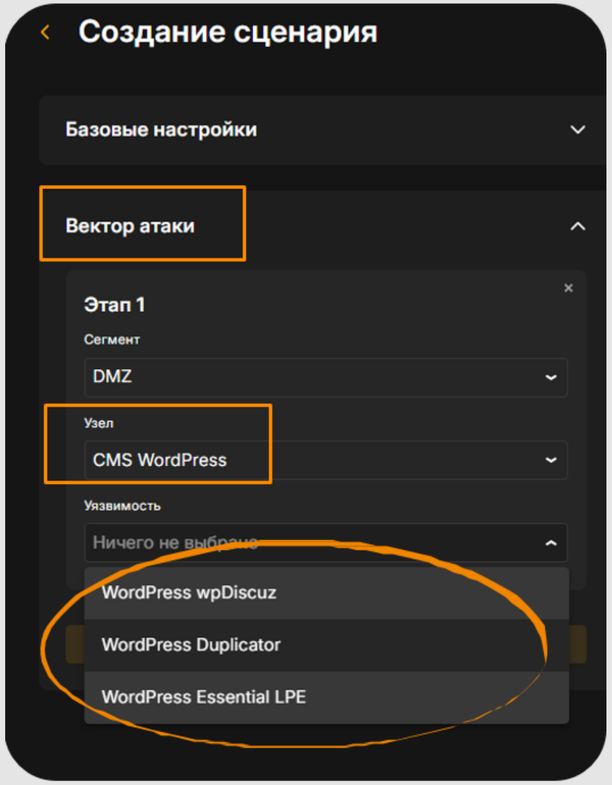
Ampire 360°

Конфигуратор в действии

Актуальность сценария: выбор уязвимости



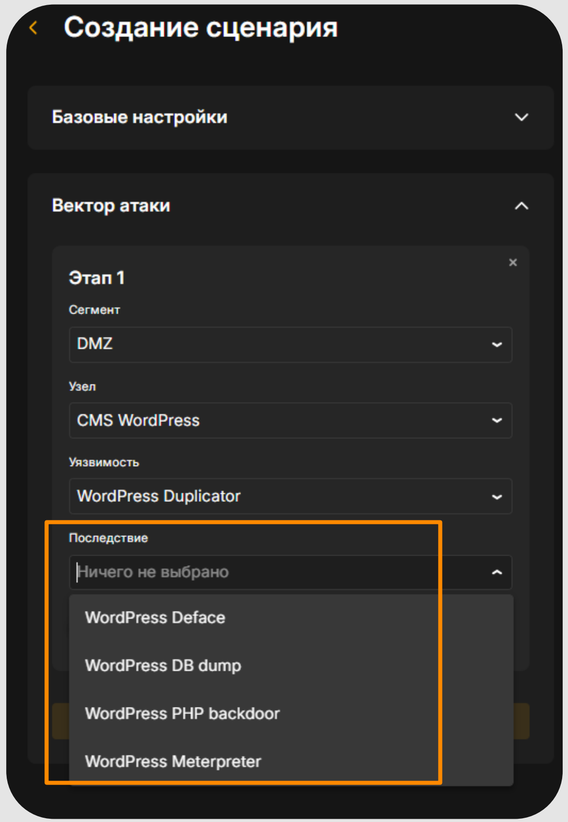


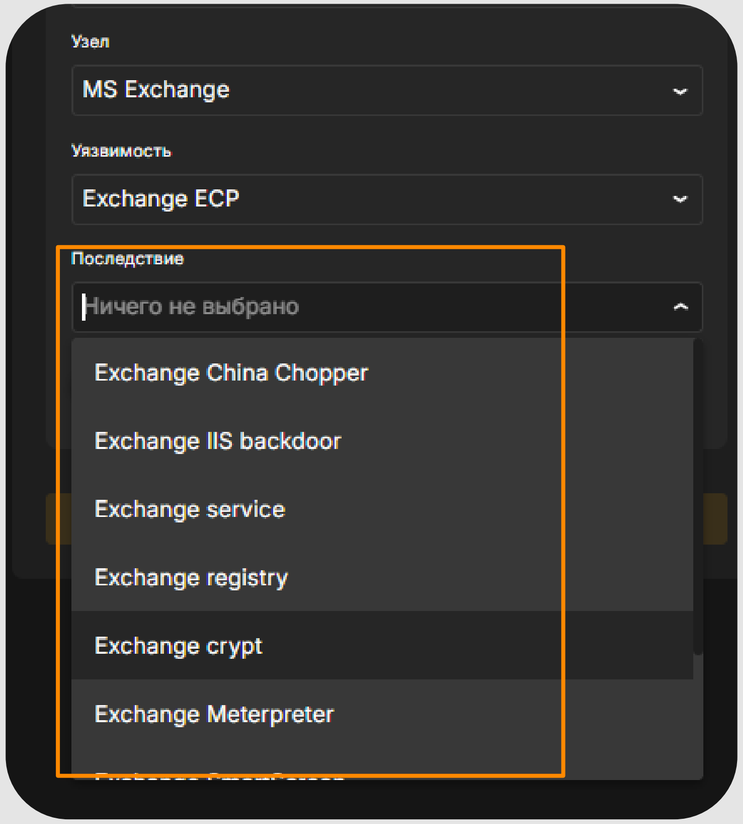


Ampire 360°

Конфигуратор в действии

Актуальность сценария: выбор последствия



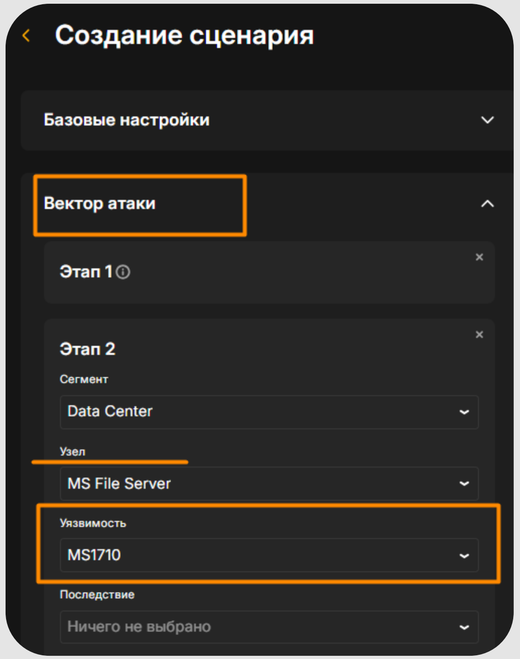


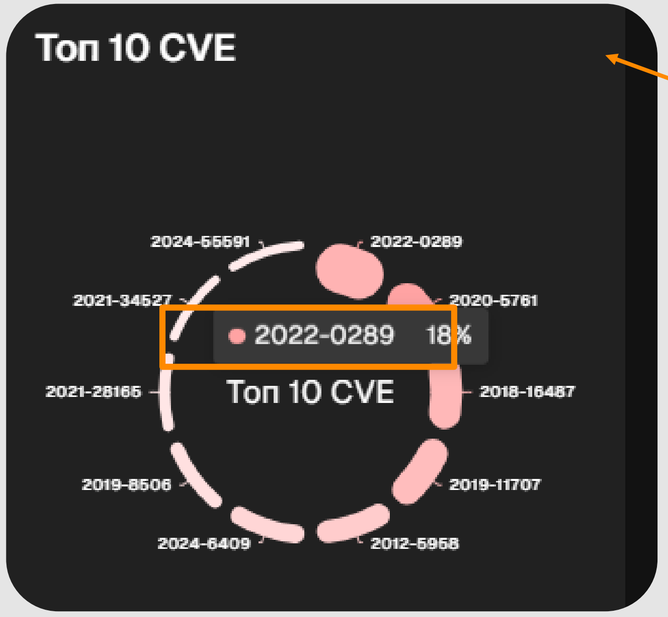
Ampire 360°

Конфигуратор в действии

Актуальность сценария:
топ-10 угроз недели

https://amtip.ru

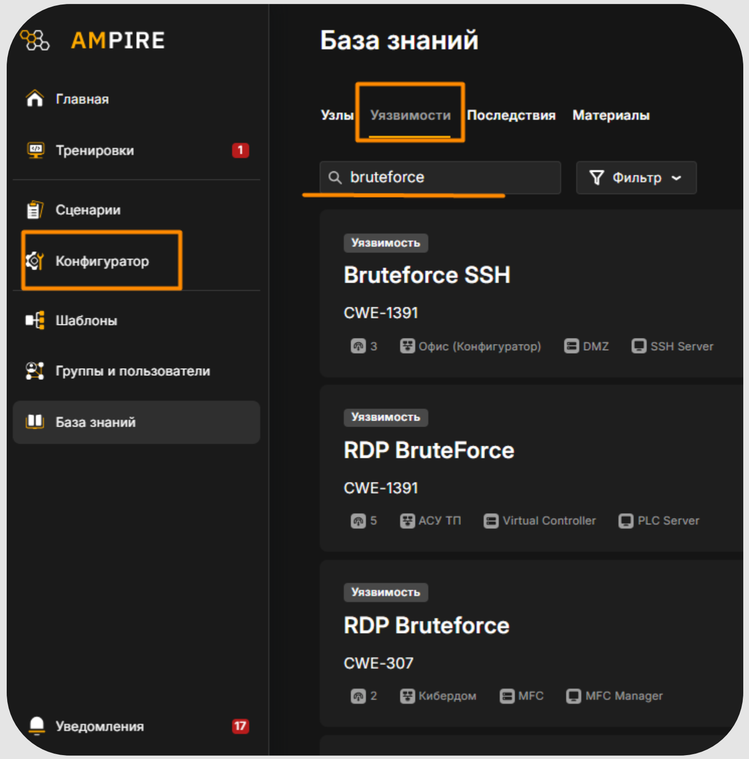




Ampire 360°

Конфигуратор в действии

Актуальность сценария: цели занятия

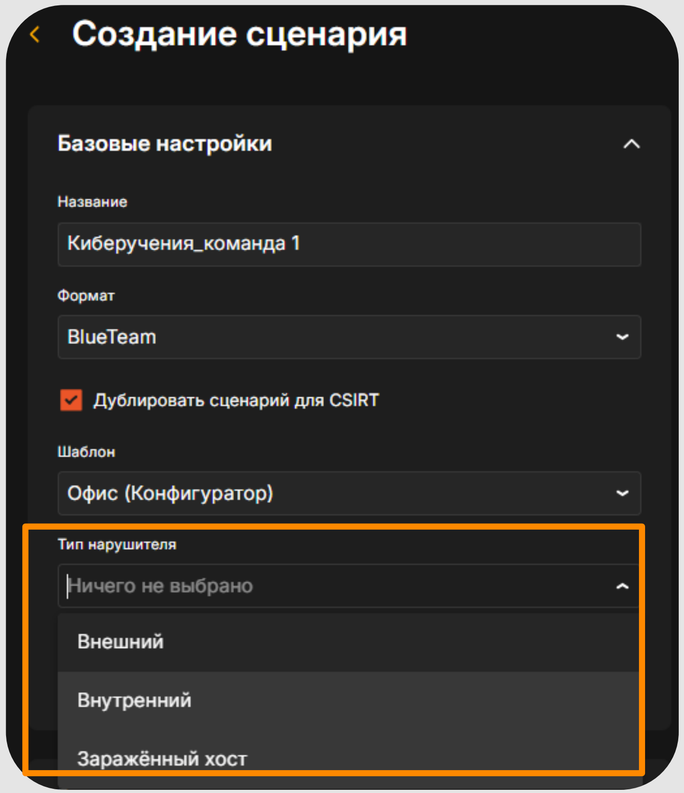


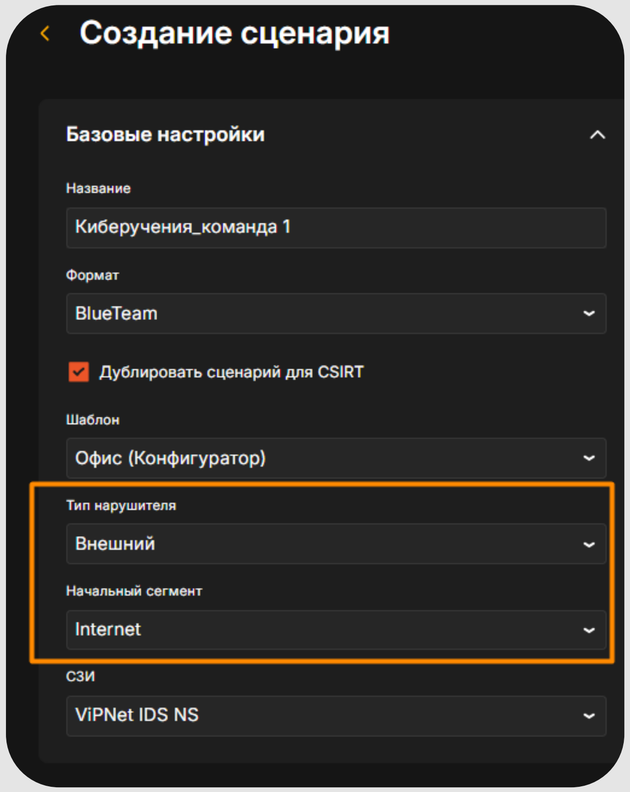
1. Знакомство с «логикой нарушителя»: простые сценарии
2. Отработка навыков мониторинга
3. Отработка навыков реагирования
4. Формирование умения работать с сетевыми сенсорами
5. Отработка навыков защиты ОС на базе Linux, Windows
6. Подготовка к соревнованиям, и др.

Ampire 360°

Конфигуратор в действии

Актуальность сценария: выбор типа нарушителя

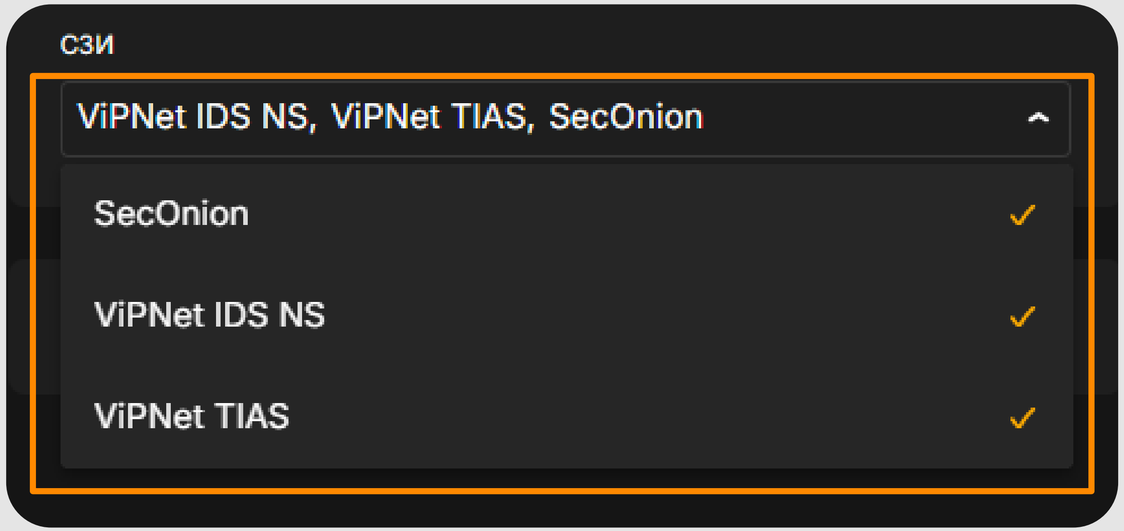




- Внешний нарушитель
- Внутренний нарушитель
- Заражённый хост

Конфигуратор в действии

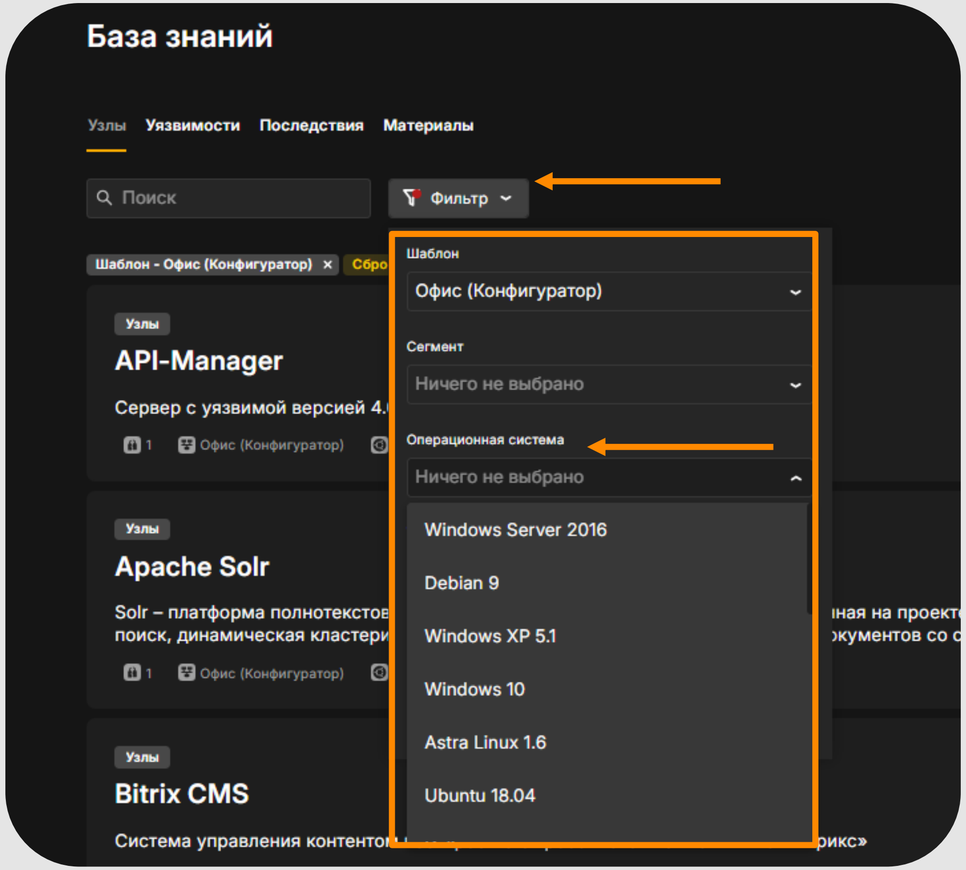
Актуальность сценария: выбор СЗИ



- ViPNet IDS NS
- ViPNet TIAS
- Security Onion

Конфигуратор в действии

Работа с различными ОС

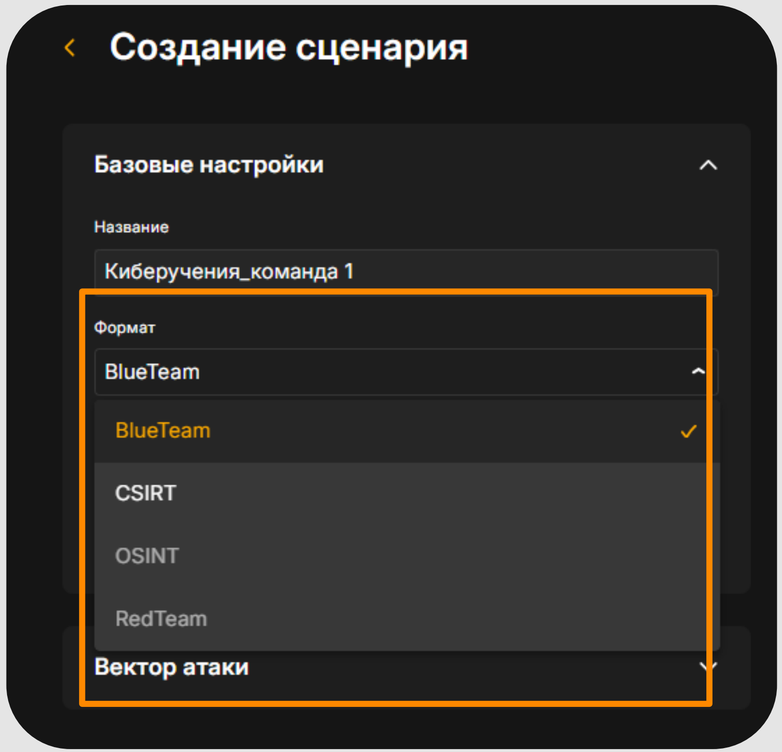


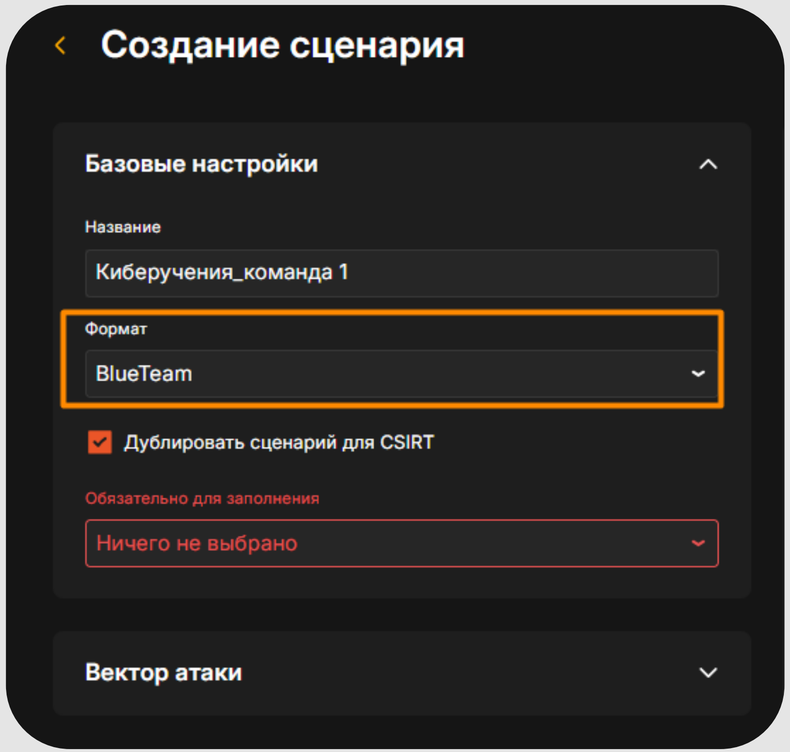
Функция «Фильтр» на странице Базы знаний позволяет выбрать сценарий для отработки навыков защиты определенных ОС

Ampire 360°

Конфигуратор в действии

Формат тренировки



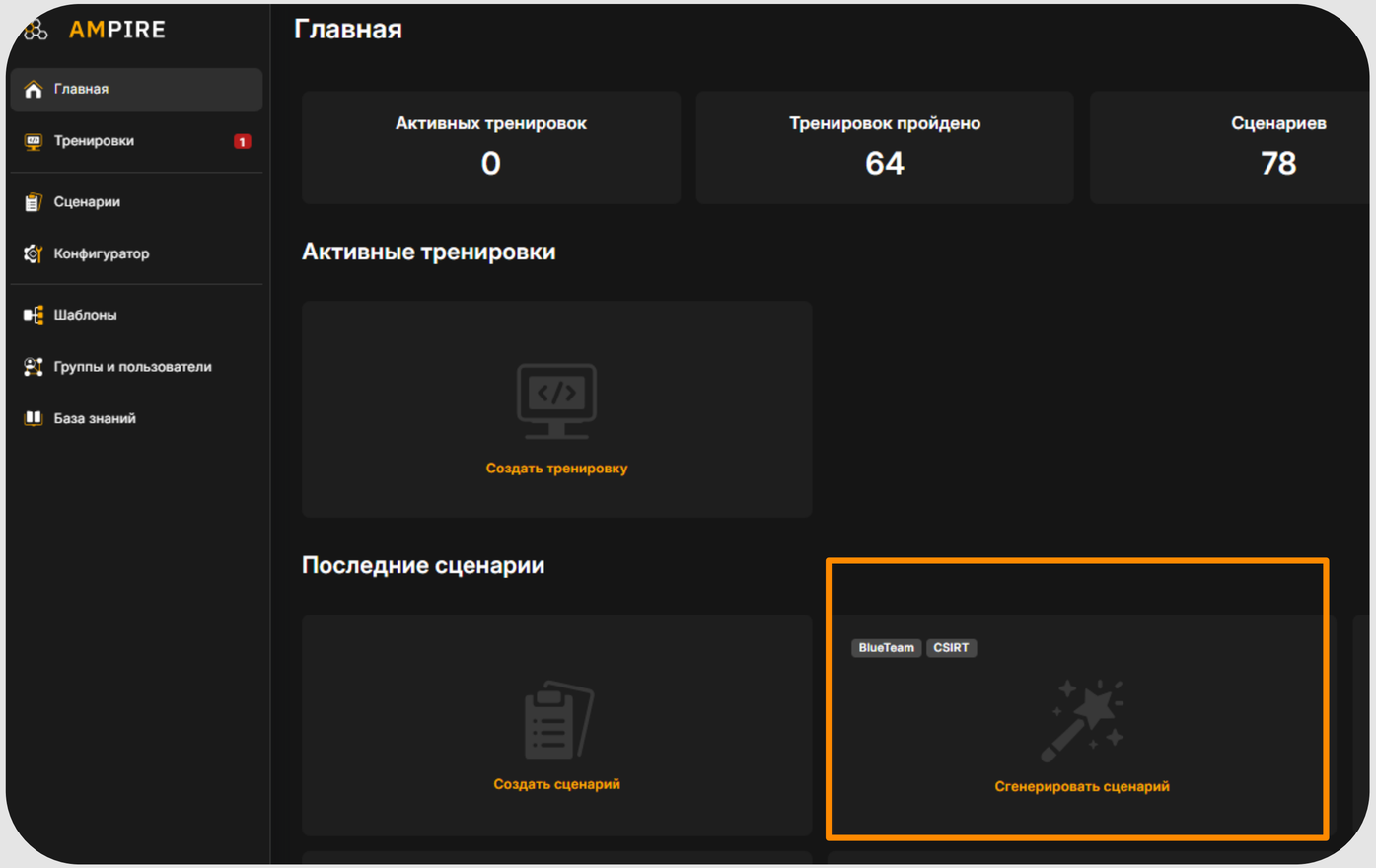


- Blue Team
- CSIRT

Ampire 360°

Конфигуратор в действии

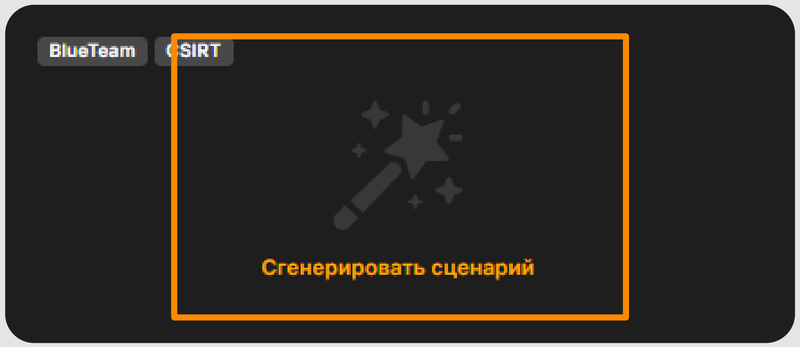
Сгенерировать сценарий

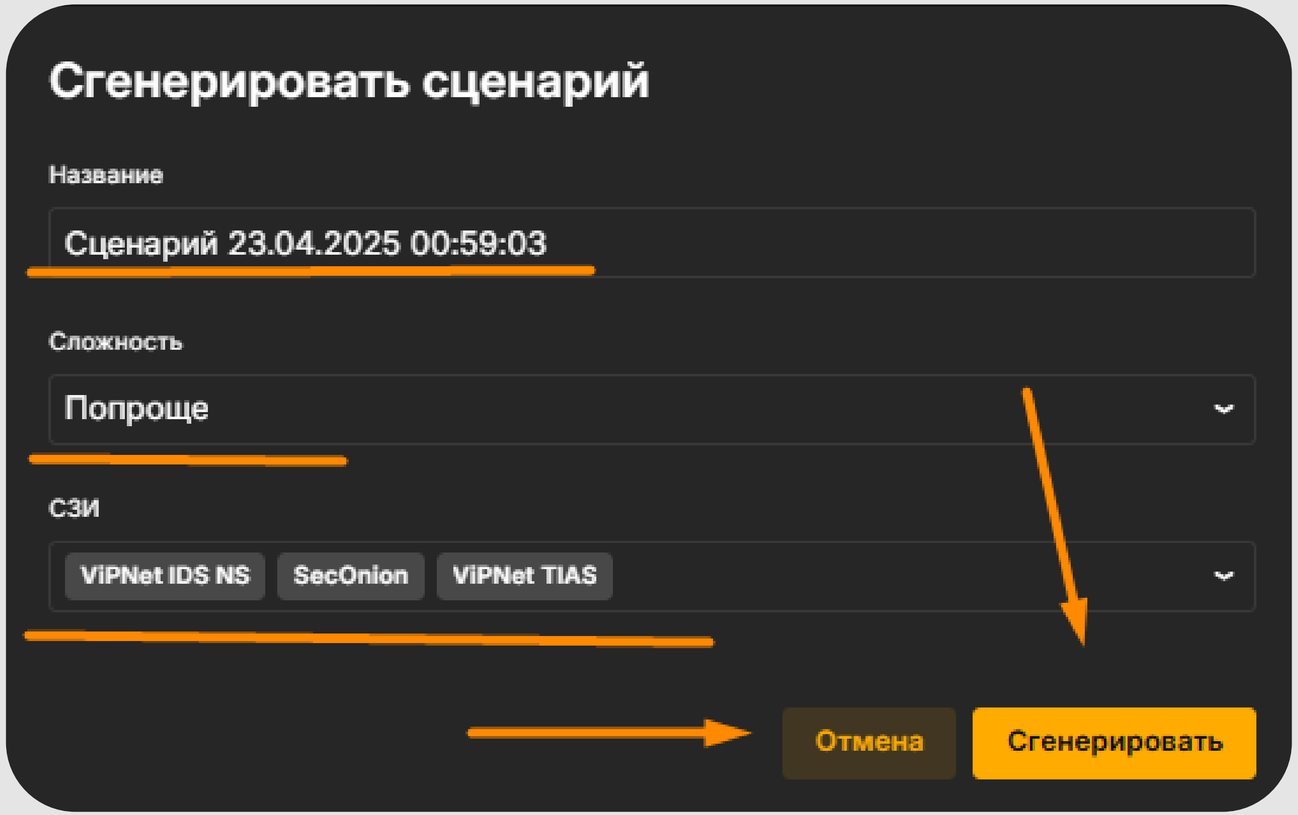


Ampire 360°

Конфигуратор в действии

Сгенерировать сценарий



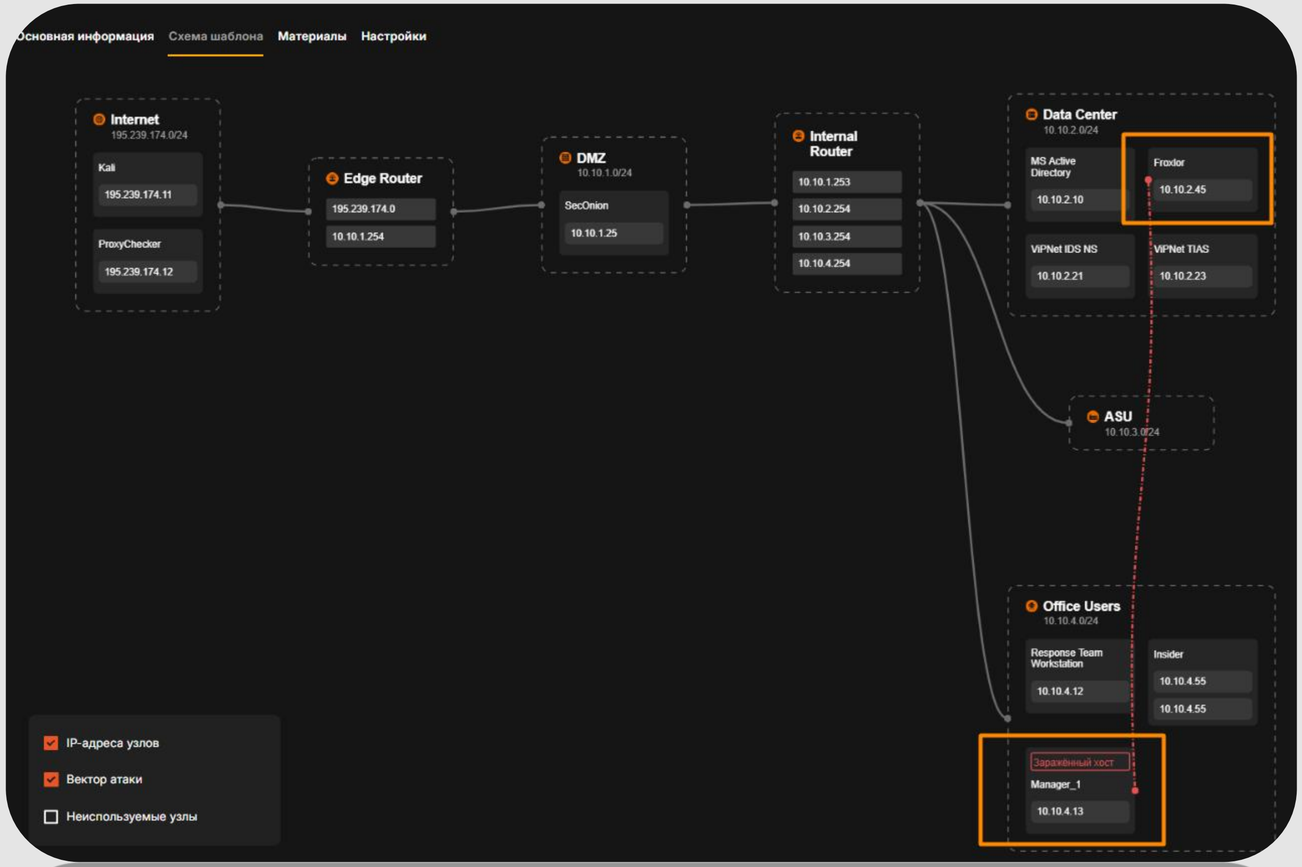


Ampire 360°

Конфигуратор в действии

Сгенерировать сценарий

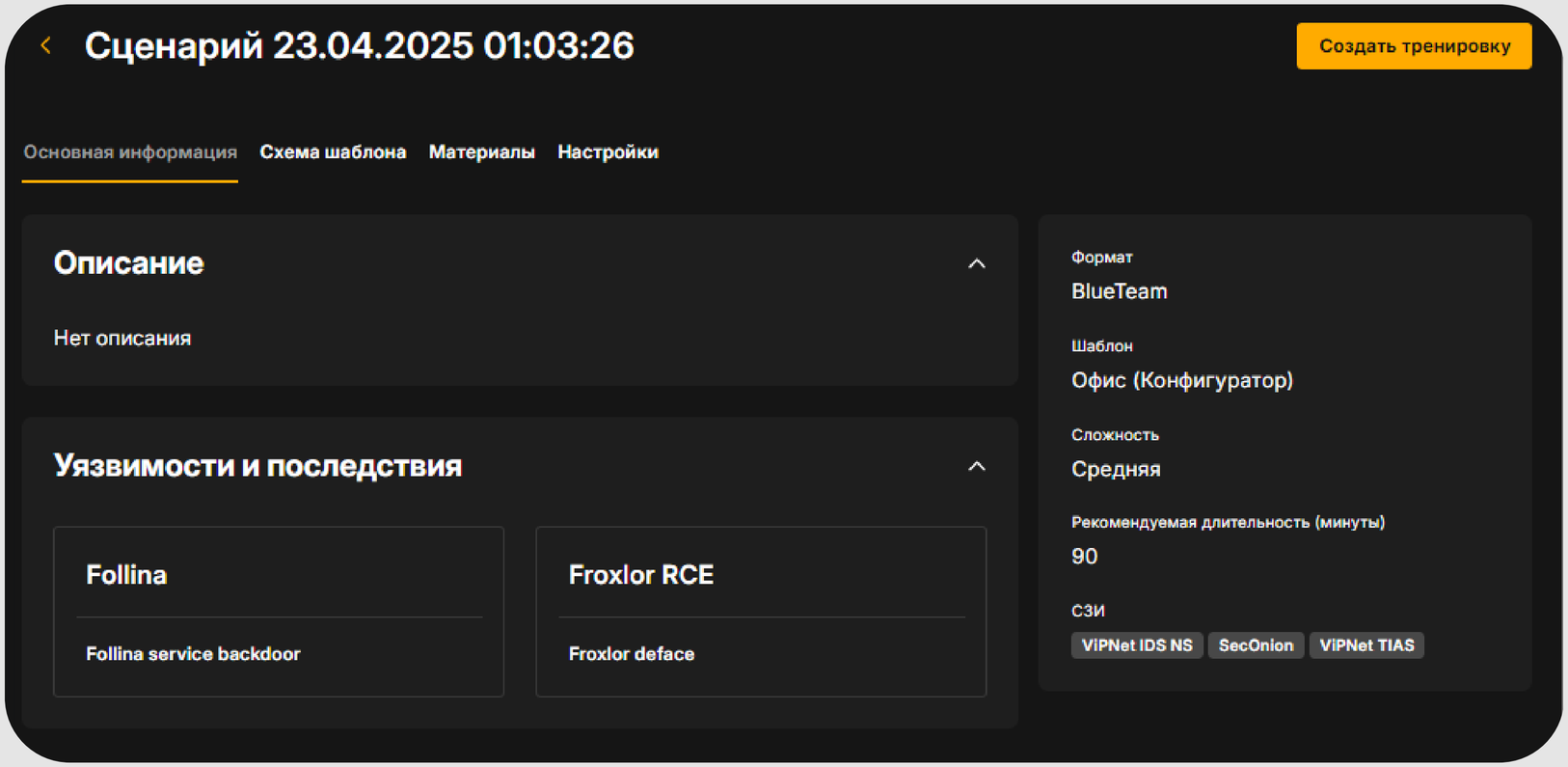
Пример схемы шаблона



Ampire 360°

Конфигуратор в действии

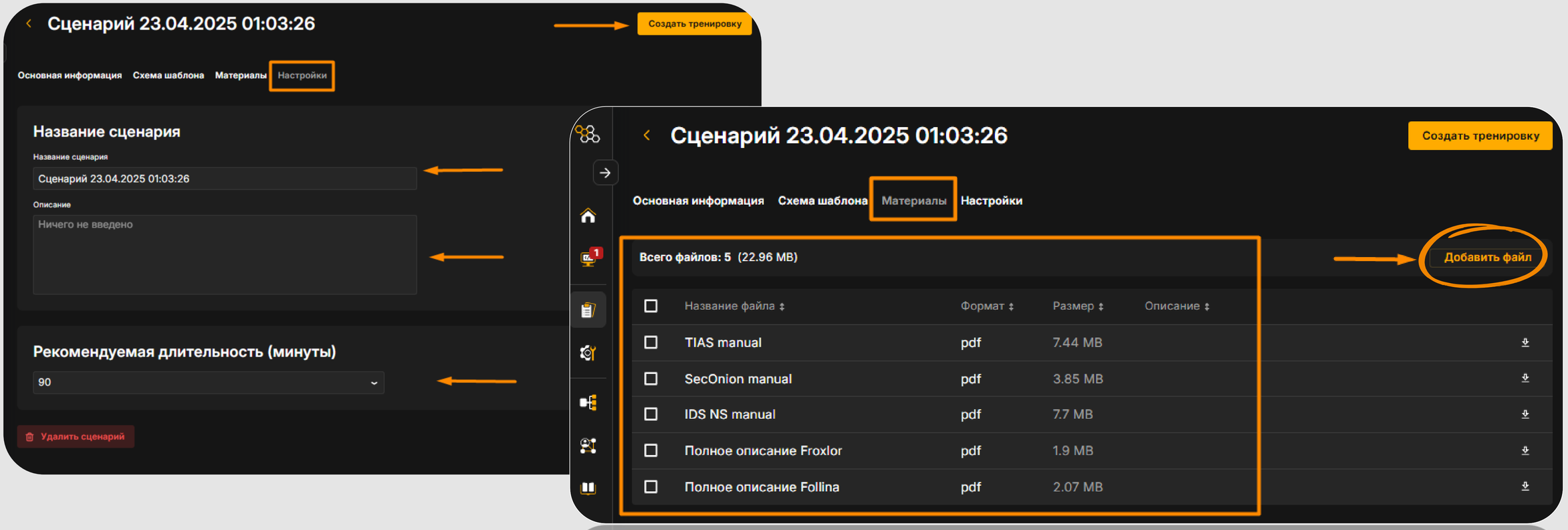
Сгенерировать сценарий



Ampire 360°

Конфигуратор в действии

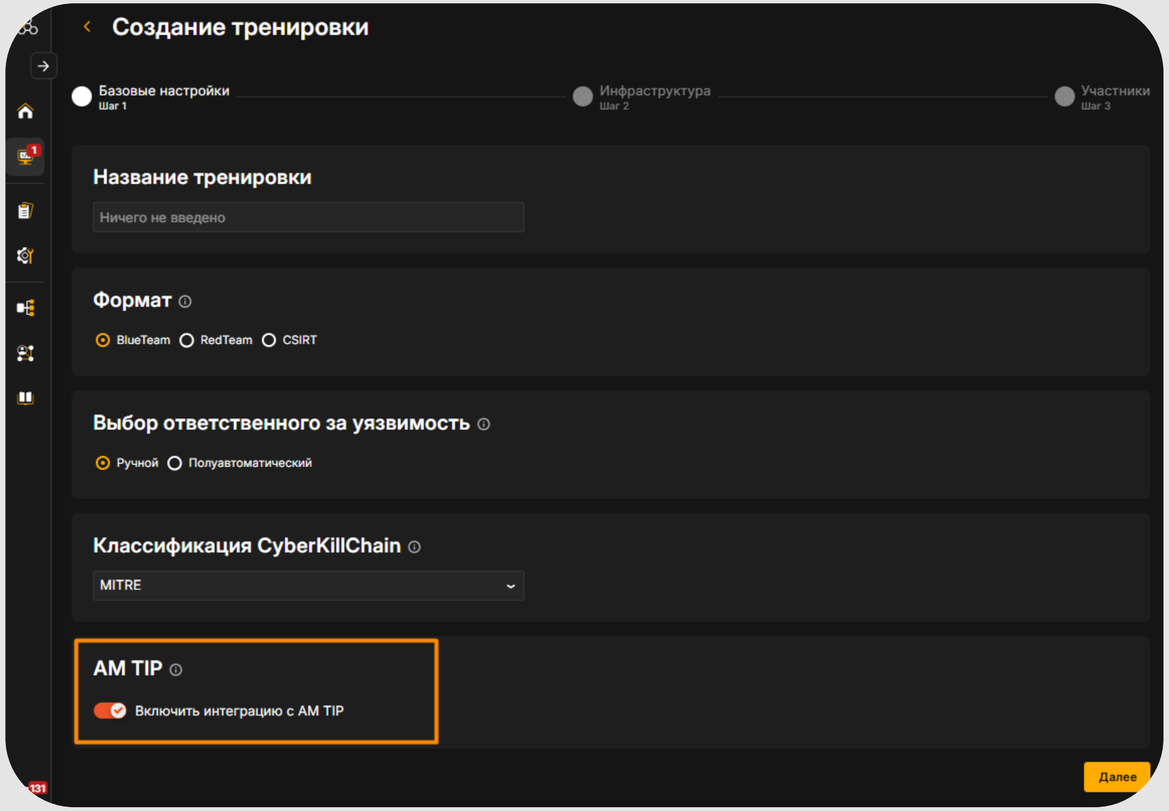
Дополнительные возможности

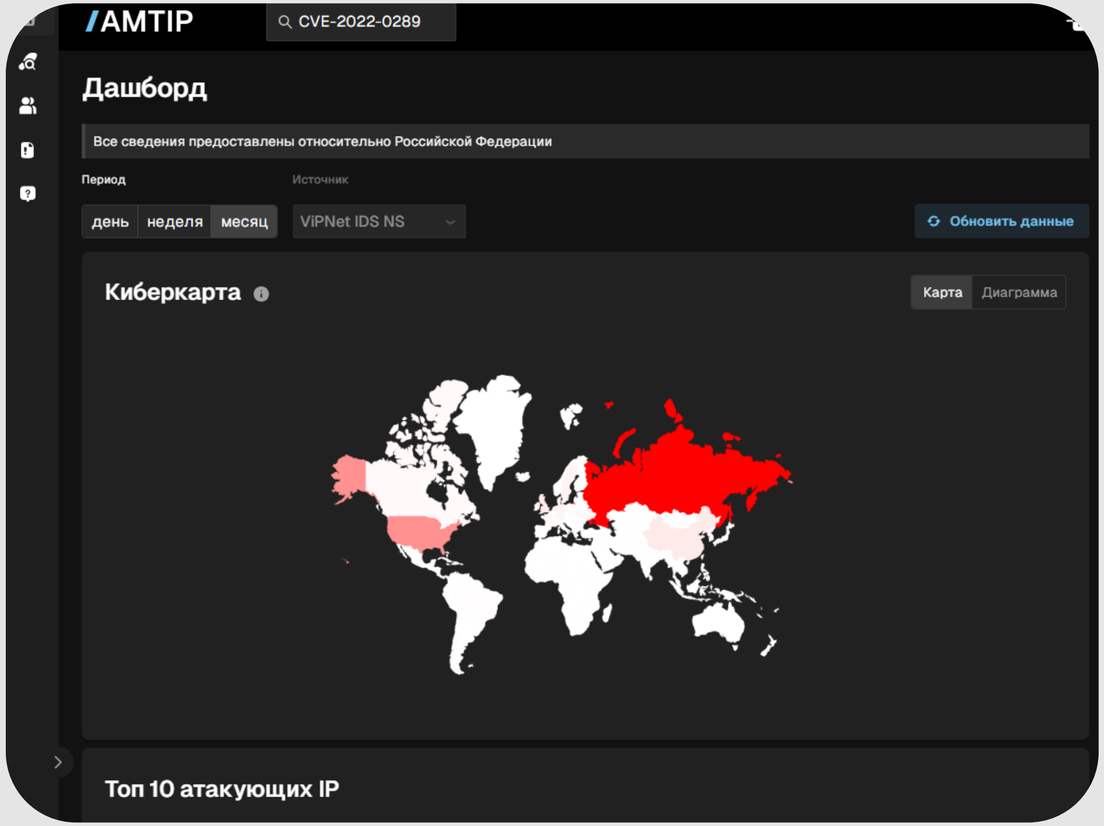


Ampire 360°

Конфигуратор в действии

Дополнительные возможности





Ampire 360°

Конфигуратор в действии

Преимущества

1. Новизна – актуальные угрозы.
2. Сценарии под ваши задачи. Вариативность.
3. Автоматическая генерация случайных сценариев.
4. Статичные сценарии и презентации.

360° Ampire

Благодарю за внимание!