ПЕРСПЕКТИВНЫЙ
МОНИТОРИНГ

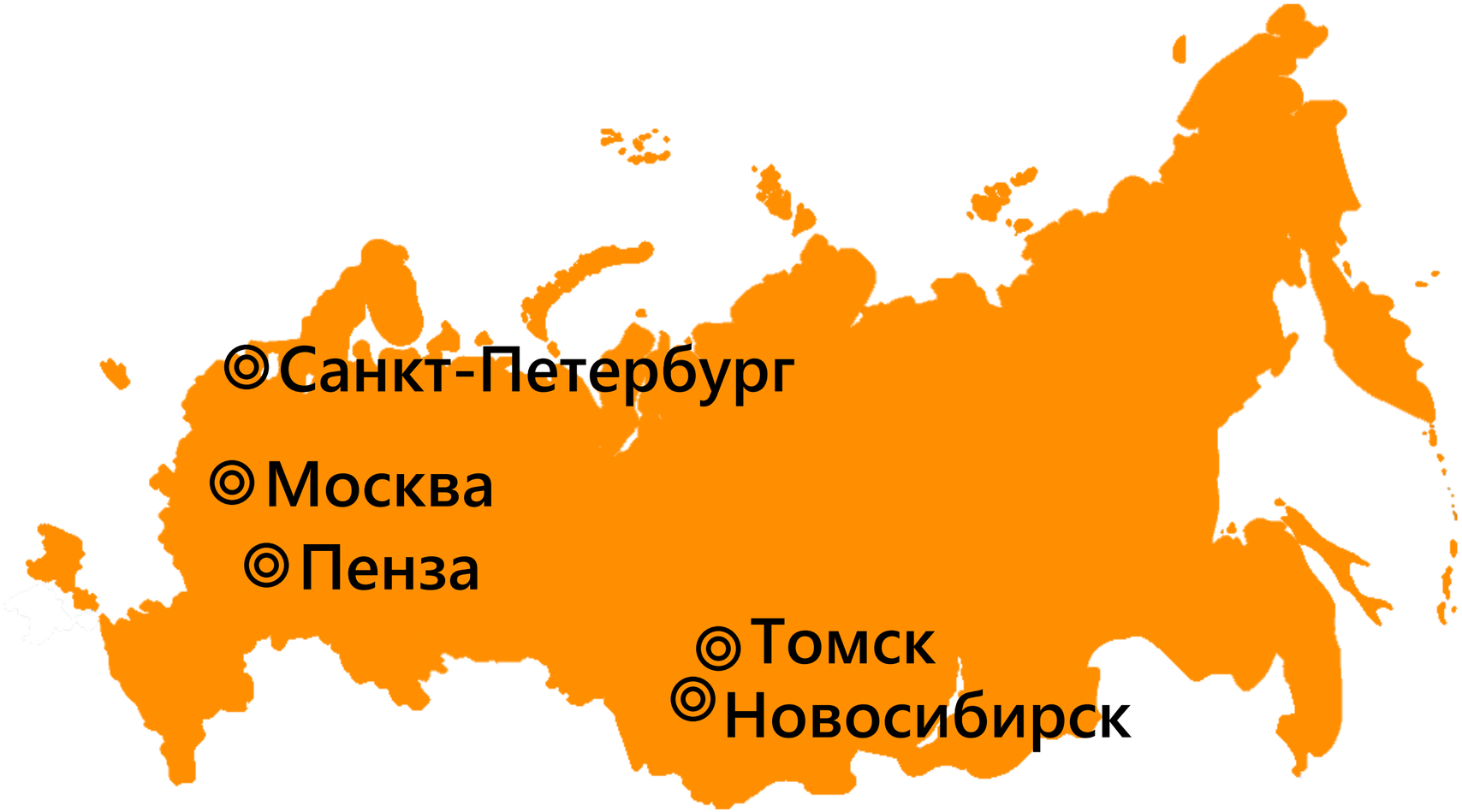
Киберполигон
Ampire

Возможности применения и развития

Сегодня поговорим

- Про киберполигон Ampire
- Про сотрудничество с ВУЗами
- Про разработку шаблонов и сценариев

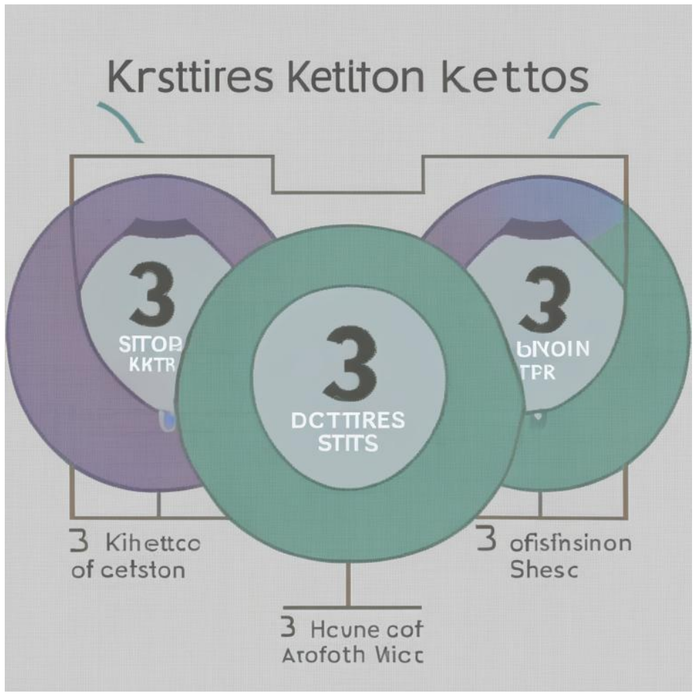
Регионы присутствия



Три кита ИБ ©ruDALL-E Kandinsky 2.1

Техника

Люди



Процессы

Проактивная позиция

Не можем повлиять

1) Сам факт атаки
2) Квалификация атакующего
3) Инструментарий
4) Объём ресурсов

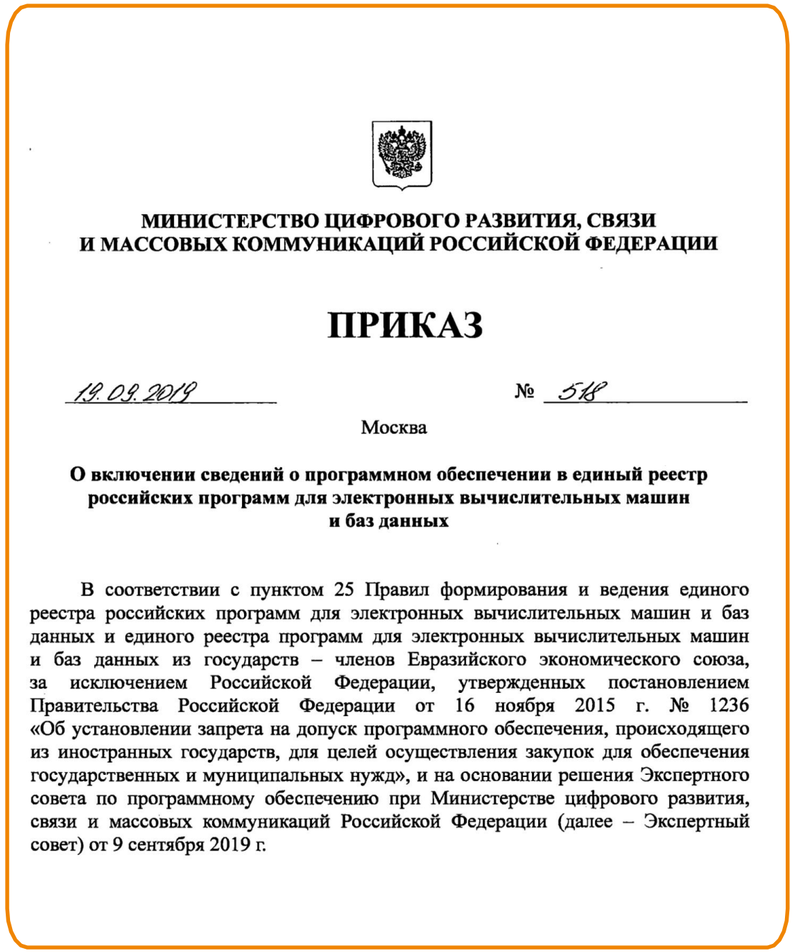
Можем повлиять

1) Стоимость атаки
2) Скорость реакции
3) Содержание реакции
4) Собственный опыт
5) Планы и изменения

Способность действовать в экстренной ситуации зависит не от уровня знаний, а от уровня подготовки.

Единый реестр российских программ для ЭВМ и БД

- **Класс ПО:** Информационные системы для решения специфических отраслевых задач
- **Сайт производителя:**
- **Дата регистрации:** 20 Сентября 2019
- **Решение уполномоченного органа:** Приказ Минкомсвязи России от 19.09.2019 №518



МИНИСТЕРСТВО ЦИФРОВОГО РАЗВИТИЯ, СВЯЗИ
И МАССОВЫХ КОММУНИКАЦИЙ РОССИЙСКОЙ ФЕДЕРАЦИИ

ПРИКАЗ

19.09.2019 № 518

Москва

О включении сведений о программном обеспечении в единый реестр российских программ для электронных вычислительных машин и баз данных

В соответствии с пунктом 25 Правил формирования и ведения единого реестра российских программ для электронных вычислительных машин и баз данных и единого реестра программ для электронных вычислительных машин и баз данных из государств – членов Евразийского экономического союза, за исключением Российской Федерации, утвержденных постановлением Правительства Российской Федерации от 16 ноября 2015 г. № 1236 «Об установлении запрета на допуск программного обеспечения, происходящего из иностранных государств, для целей осуществления закупок для обеспечения государственных и муниципальных нужд», и на основании решения Экспертного совета по программному обеспечению при Министерстве цифрового развития, связи и массовых коммуникаций Российской Федерации (далее – Экспертный совет) от 9 сентября 2019 г.

РОССИЙСКАЯ ФЕДЕРАЦИЯ

СВИДЕТЕЛЬСТВО

о государственной регистрации программы для ЭВМ

№ 2019613098

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

Правообладатель: *Закрытое акционерное общество «Перспективный мониторинг» (ЗАО «ПМ») (RU)*

Авторы: *Костюлин Илья Николаевич (RU), Наумова Александра Вячеславовна (RU), Овчинников Сергей Александрович (RU), Пушкин Александр Александрович (RU), Худой Юрий Игоревич (RU)*

Заявка № 2019612022
Дата поступления 01 марта 2019 г.
Дата государственной регистрации в Реестре программ для ЭВМ 07 марта 2019 г.

Руководитель Федеральной службы по интеллектуальной собственности

Г.П. Ивлиев

Целевая аудитория

- Школьники и студенты с базовым знанием TCP/IP сетей, которые планируют работать в сфере защиты информации.
- ИБ-специалисты, которые хотели бы выделиться среди других кандидатов глубокими знаниями в определённых областях.
- ИТ-специалисты: новички и те, кто хотел бы увеличить перечень навыков в резюме.

AMPIRE

Наша учебно-тренировочная платформа содержит сценарии различной сложности для проведения киберучений, сертификационных тестов и отработки необходимых навыков.

Цели киберучений

Создать собственный SOC

Научиться выявлять компьютерные атаки

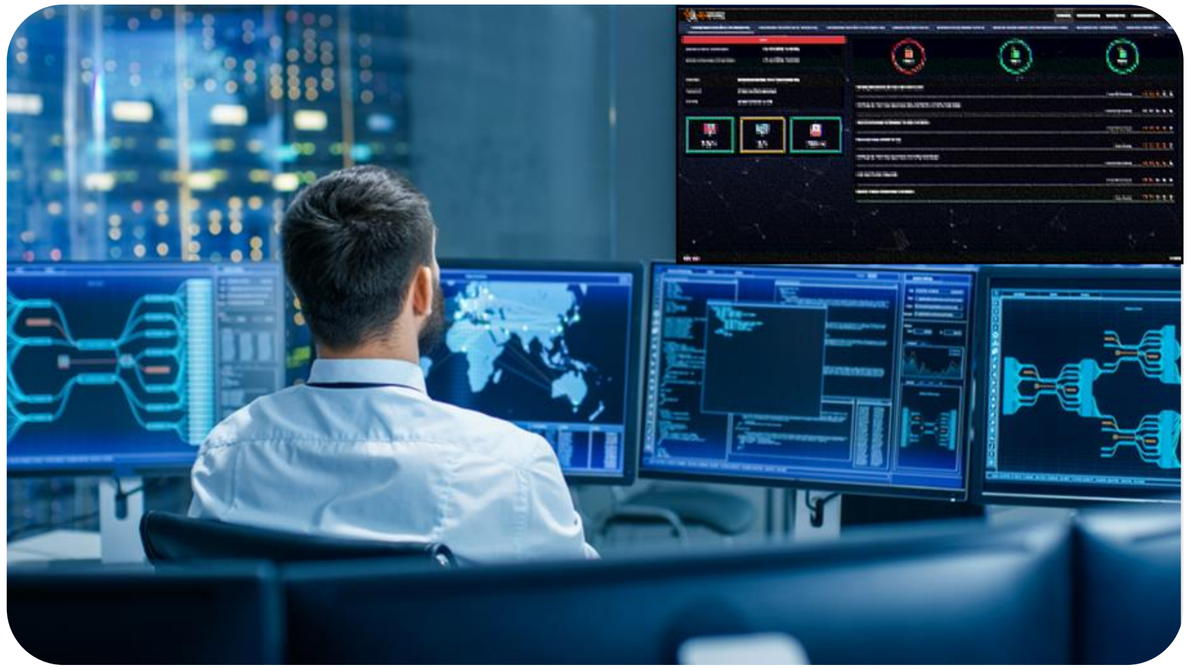
Наладить взаимодействие между подразделениями

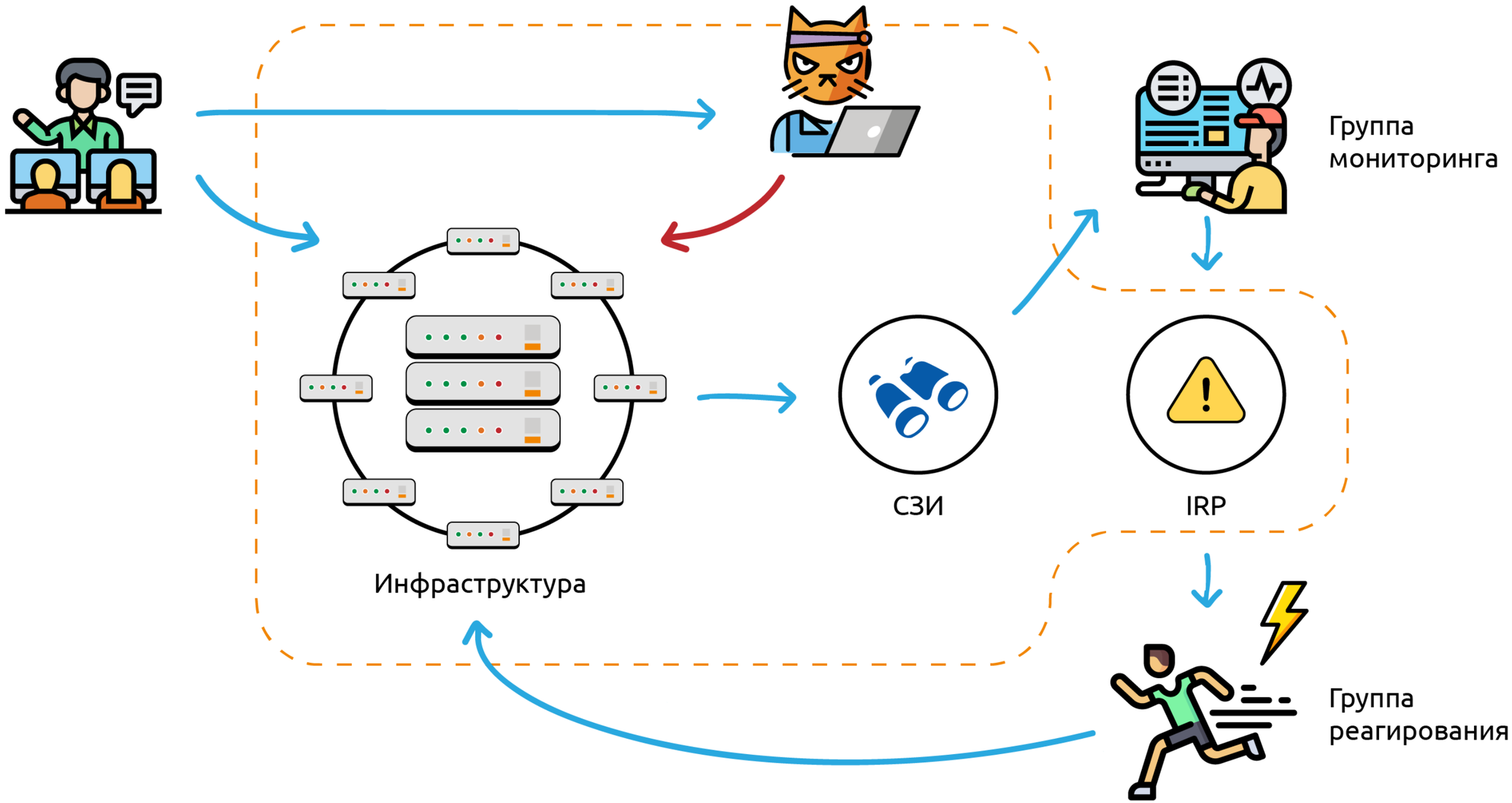
Устранить существующие уязвимости

Проведение киберучений на базе ПК

Киберучения – это процесс моделирования целевых компьютерных атак на некую ИТ-инфраструктуру с акцентом в сторону отработки навыков защиты:

- анализ событий ИБ;
- регистрация и расследование инцидентов ИБ;
- устранение причин успешного выполнения КА;
- командное взаимодействие.




Группа
мониторинга
СЗИ
IRP
Инфраструктура
Группа
реагирования

СЗИ

- VipNet IDS NS
- VipNet IDS HS
- VipNet TIAS
- IDS/IPS Suricata
- ELK
- Security Onion
- IDS/IPS Snort

И почти любые другие

Типы проводимых занятий

1. Киберучения
2. Анализ защищённости и аудит ИТ-инфраструктуры виртуальной организации
3. Противодействие группе реальных нарушителей (концепция Red Team и Blue team)
4. Лабораторные работы по настройке средств безопасности и прикладных сервисов
5. Киберквесты

Организационные преимущества

1. Круглосуточная готовность проводить занятия. Старт тренировки через 2 минуты после начала занятия.
2. Возможность зарабатывать на ДПО и повышении квалификации.
3. Бессрочная лицензия. Продолжит работать даже по истечению срока оплаченной технической поддержки.
4. Возможность заказной разработки тренировочной ИТ-инфраструктуры и сценариев.

Оснащение лабораторий

Лаборатория на основе Учебно-тренировочной платформы Ampire выполняет требования федеральных государственных стандартов к материально-техническому и учебно-методическому обеспечению программ по специальностям в информационной безопасности и позволяет региону в короткие сроки подготовить специалистов, обладающих практическими навыками выявления компьютерных атак, расследования инцидентов информационной безопасности, реализации защитных мер для нейтрализации существующих недостатков безопасности в информационных сетях общего и специального назначения (связь, энергетика, финансовая сфера, ТЭК, промышленные предприятия различных отраслей).

В поставку входят

- Программное обеспечение Ampire
- Подготовка преподавателей для работы с комплексом
- Рабочая программа, методические материалы
- Техническая поддержка
- Обновление контента

Комплекс продолжит работать и без техподдержки

14

в 23

Сотрудничаем с ВУЗами

МТУСИ
Московский технический университет связи и информатики

1890
КНИТУ

МИРЭА
Российский технологический университет

ТУСУР | TUSUR UNIVERSITY

Пример готового класса

Поддерживаем Олимпиаду

Перспективный мониторинг

🏆 Завершился финал Всероссийской студенческой олимпиады по информационной безопасности. Лучшими в 2023 году стали:
1 место – Даниил Трошкин, студент Академии ФСО России;
2 место – Дмитрий Буренок, студент НИУ МИЭТ;
3 место –Александр Андреев, студент МТУСИ.
С заданиями на киберполигоне Ampire лучше всех справились:
– Андреев Александр, МТУСИ;
– Романько Максим, РТУ МИРЭА;
– Трошкин Даниил Алексеевич, Академия ФСО России.
Наши искренние поздравления победителям!

🔥 5 👍 1 👏 1

167 edited 15:11

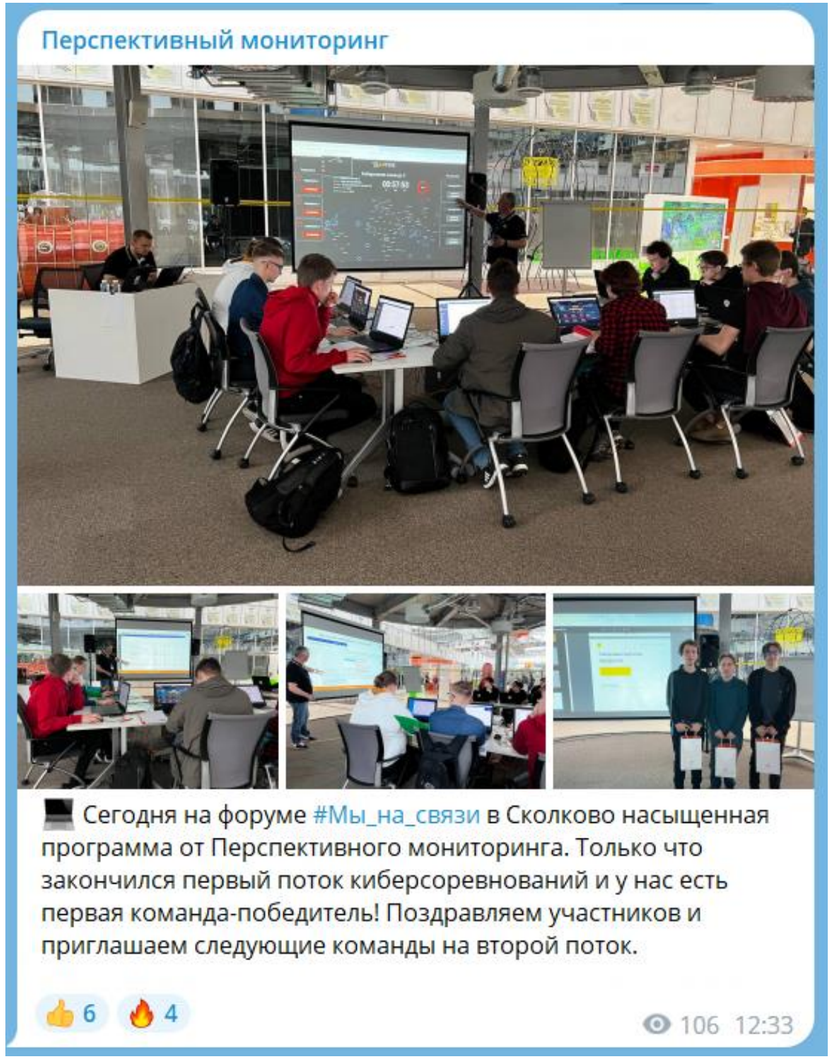
Перспективный мониторинг

🥇 Сегодня на базе Губкинец проходит финал Всероссийской студенческой олимпиады по информационной безопасности. Прямо сейчас ребята выполняют практическое задание на киберполигоне Ampire. За всех искренне болеем и желаем удачи в поисках уязвимостей! 🤞

👍 11

189 16:46

И мы, и #Мы_на_связи



Join us в Telere

ПЕРСПЕКТИВНЫЙ
МОНИТОРИНГ

Как мы можем помочь друг другу

Нужно больше инфраструктур и сценариев!

Уязвимостей МНОГО!

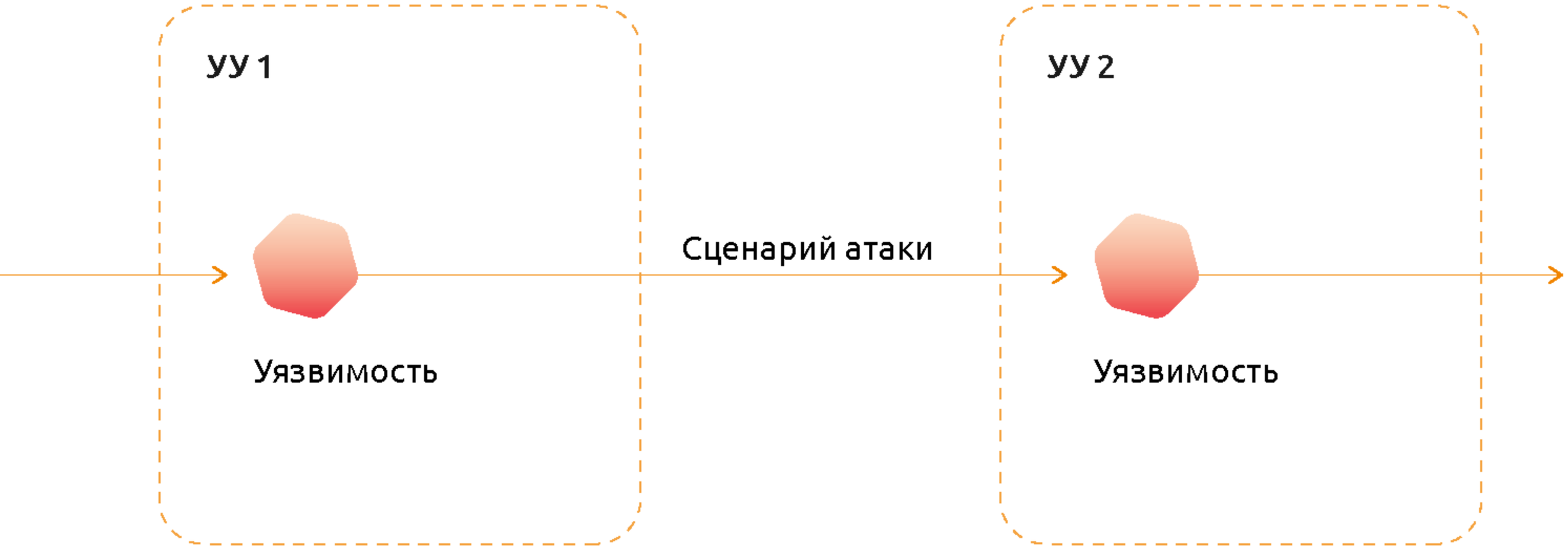
И понятно, что

- Хочется тренироваться на своих ИТ
- Хочется тренироваться на своих угрозах
- Хочется отрабатывать актуальные уязвимости
- Курсач сам себя не напишет.
  (Алиса, как зарегистрироваться в KursatchGPT)
- «Вы не видите?! Вас много, а я один!»

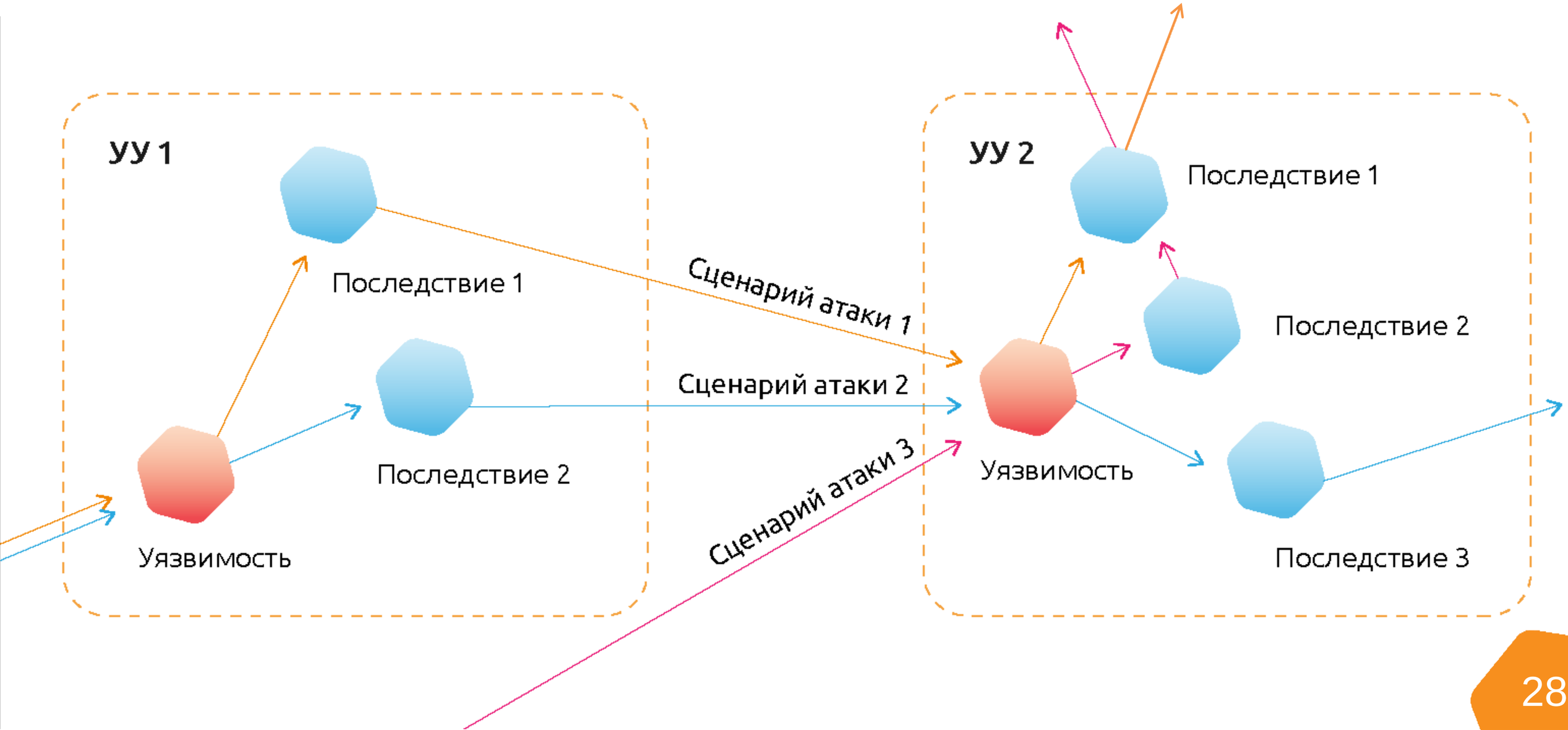
Нам есть, чем ответить!

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

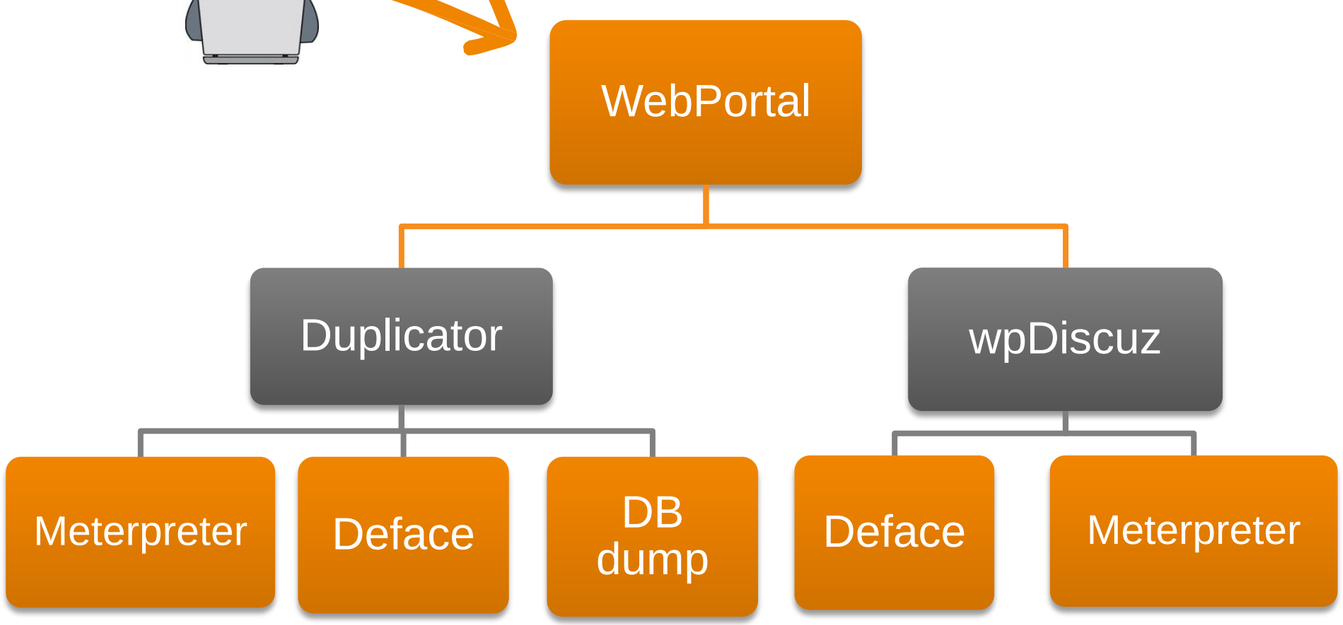
Было

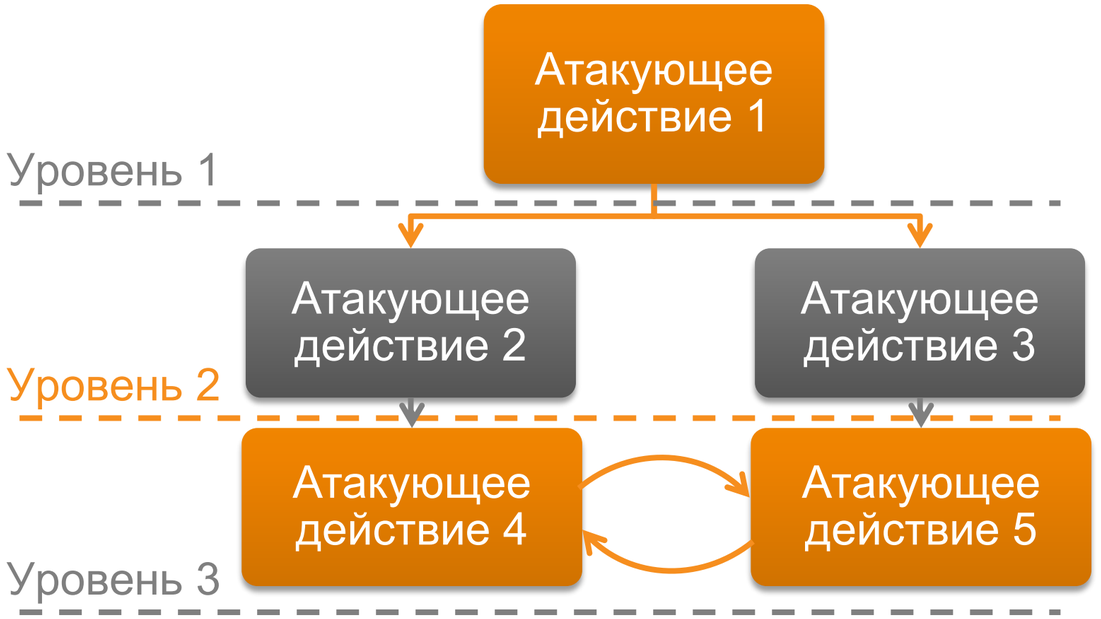


Стало

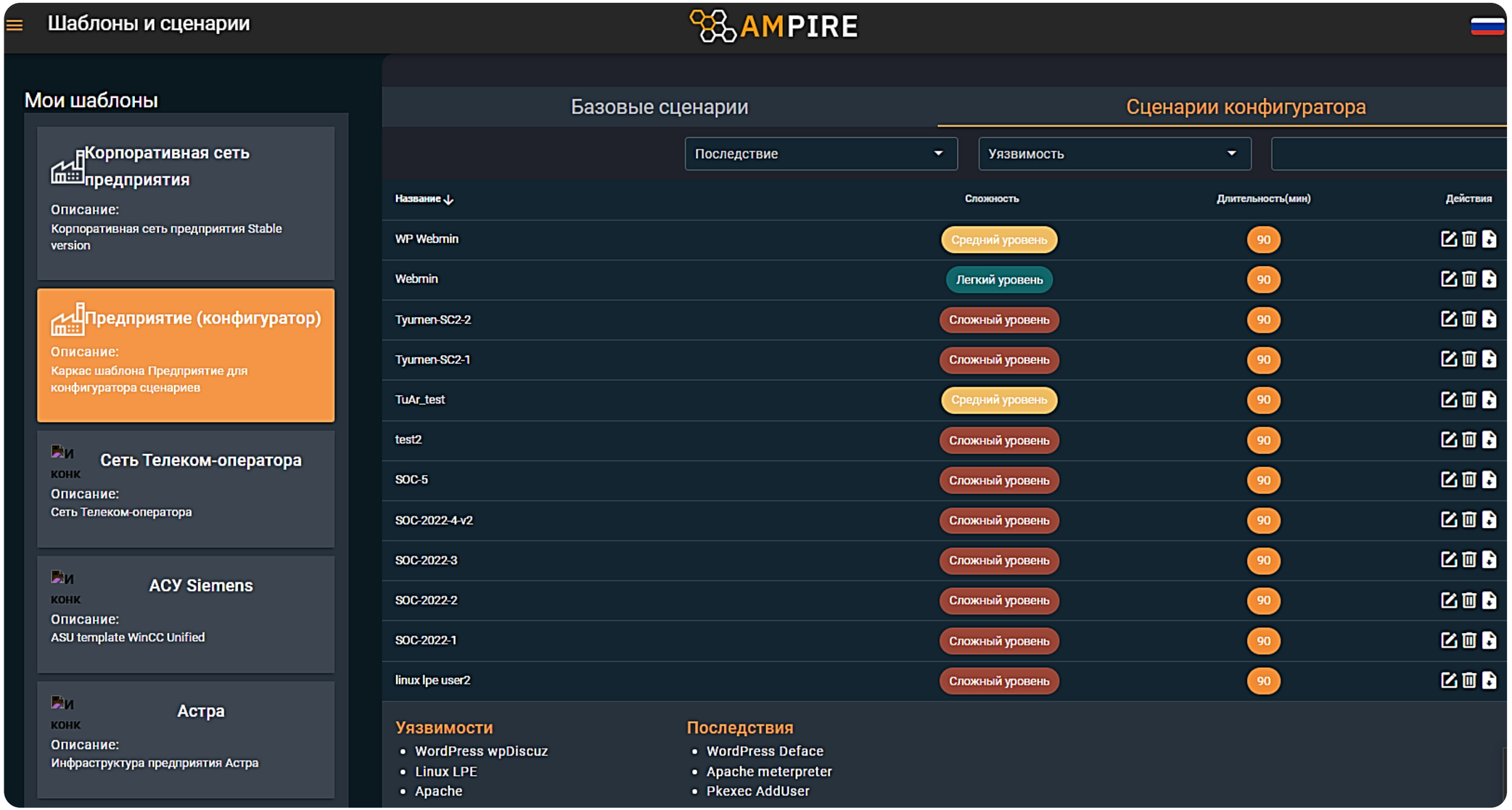

УУ 1
Последствие 1
Последствие 2
Уязвимость
Сценарий атаки 1
Сценарий атаки 2
Сценарий атаки 3
УУ 2
Последствие 1
Последствие 2
Уязвимость
Последствие 3

Конфигуратор





Конфигуратор



Автор SE Shirkunov Evgeny 6 месяцев назад Обновлено IA Ilyin Anton около 2 часов назад

Разработка сценариев

В этой статье ничего нет. Нажмите здесь, чтобы добавить содержимое.

Подстатьи[20]

Уязвимые узлы (таблица)

Правила ведения таблицы

Реестр уязвимостей V2

Уязвимости, потенциально возможные для разработки

Гайд для разработчика сценариев

Процесс разработки уязвимого узла V2

Процесс создания уязвимого узла

Артефакты для интеграции уязвимого узла

Чеклист интеграции уязвимого узла

Полезные куски кода

Правила именования

Полезные материалы

Конфигуратор. Функционал сканирования

Сценарии Конфигуратора

Сторонняя разработка

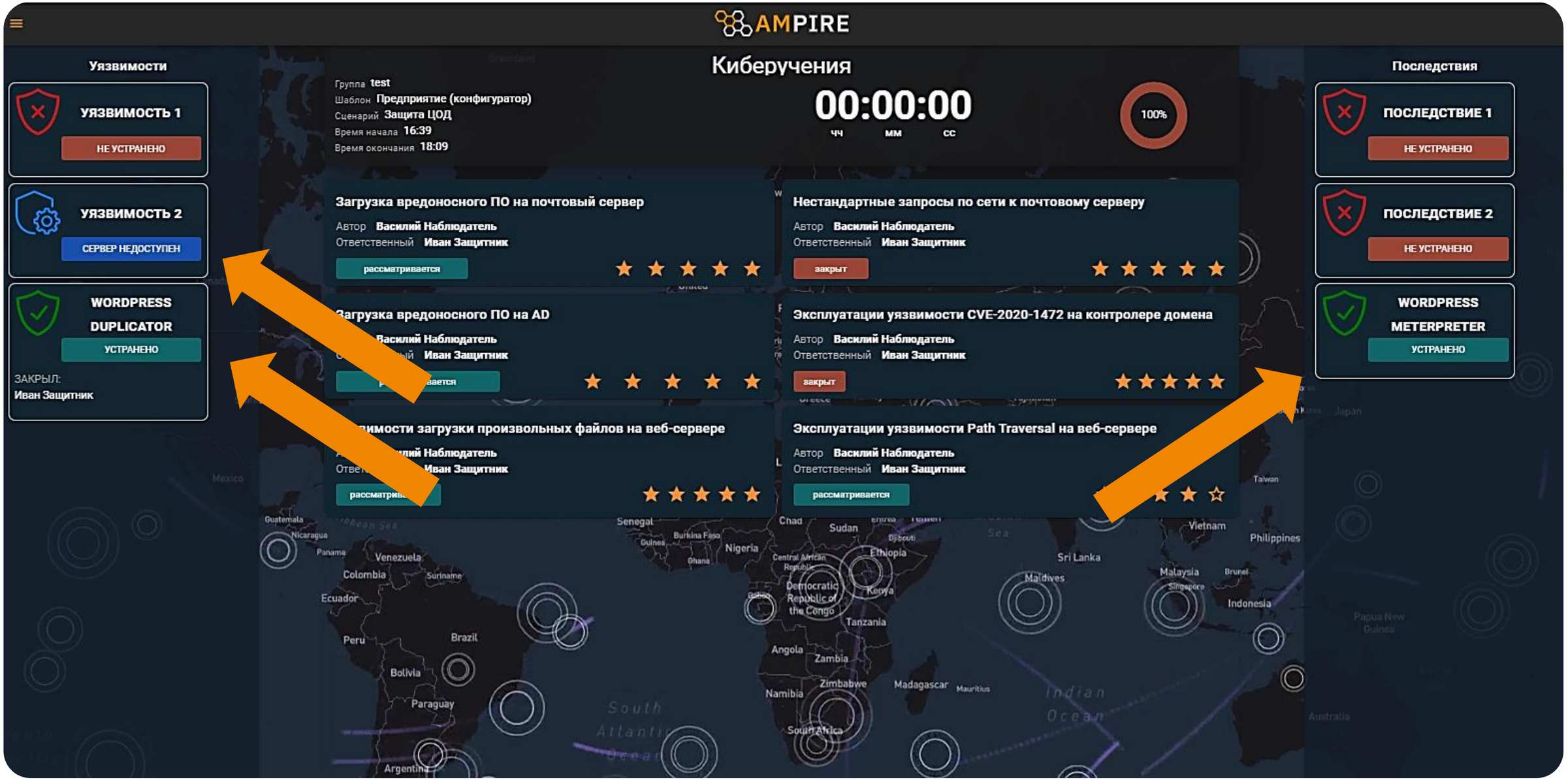
Процесс ведения документации УУ

Версии ВМ УУ

GitLab

Разработка скриптов автоматизации

Kali


AMPIRE
Киберучения
Уязвимости
УЯЗВИМОСТЬ 1
НЕ УСТРАНЕНО
УЯЗВИМОСТЬ 2
СЕРВЕР НЕДОСТУПЕН
WORDPRESS DUPLICATOR
УСТРАНЕНО
ЗАКРЫЛ:
Иван Защитник
Группа test
Шаблон Предприятие (конфигуратор)
Сценарий Защита ЦОД
Время начала 16:39
Время окончания 18:09
00:00:00
чч мм сс
100%
Загрузка вредоносного ПО на почтовый сервер
Автор Василий Наблюдатель
Ответственный Иван Защитник
рассматривается
Нестандартные запросы по сети к почтовому серверу
Автор Василий Наблюдатель
Ответственный Иван Защитник
закрыт
Загрузка вредоносного ПО на AD
Эксплуатации уязвимости CVE-2020-1472 на контролере домена
Автор Василий Наблюдатель
Ответственный Иван Защитник
закрыт
Эксплуатации уязвимости Path Traversal на веб-сервере
Автор Василий Наблюдатель
Ответственный Иван Защитник
рассматривается
Последствия
ПОСЛЕДСТВИЕ 1
НЕ УСТРАНЕНО
ПОСЛЕДСТВИЕ 2
НЕ УСТРАНЕНО
WORDPRESS METERPRETER
УСТРАНЕНО

ПЕРСПЕКТИВНЫЙ
МОНИТОРИНГ

Спасибо
за внимание!

Бугай Иван

Руководитель направления по работе с ключевыми Заказчиками «Перспективный мониторинг»

Ivan.Bugay@amonitoring.ru

t.me/pm_public

amonitoring.ru