Ampire 2.0: новый формат, карточки НКЦКИ и требования регулятора

Георгий Мелихов

Руководитель направления развития продуктов
и услуг компании «Перспективный мониторинг

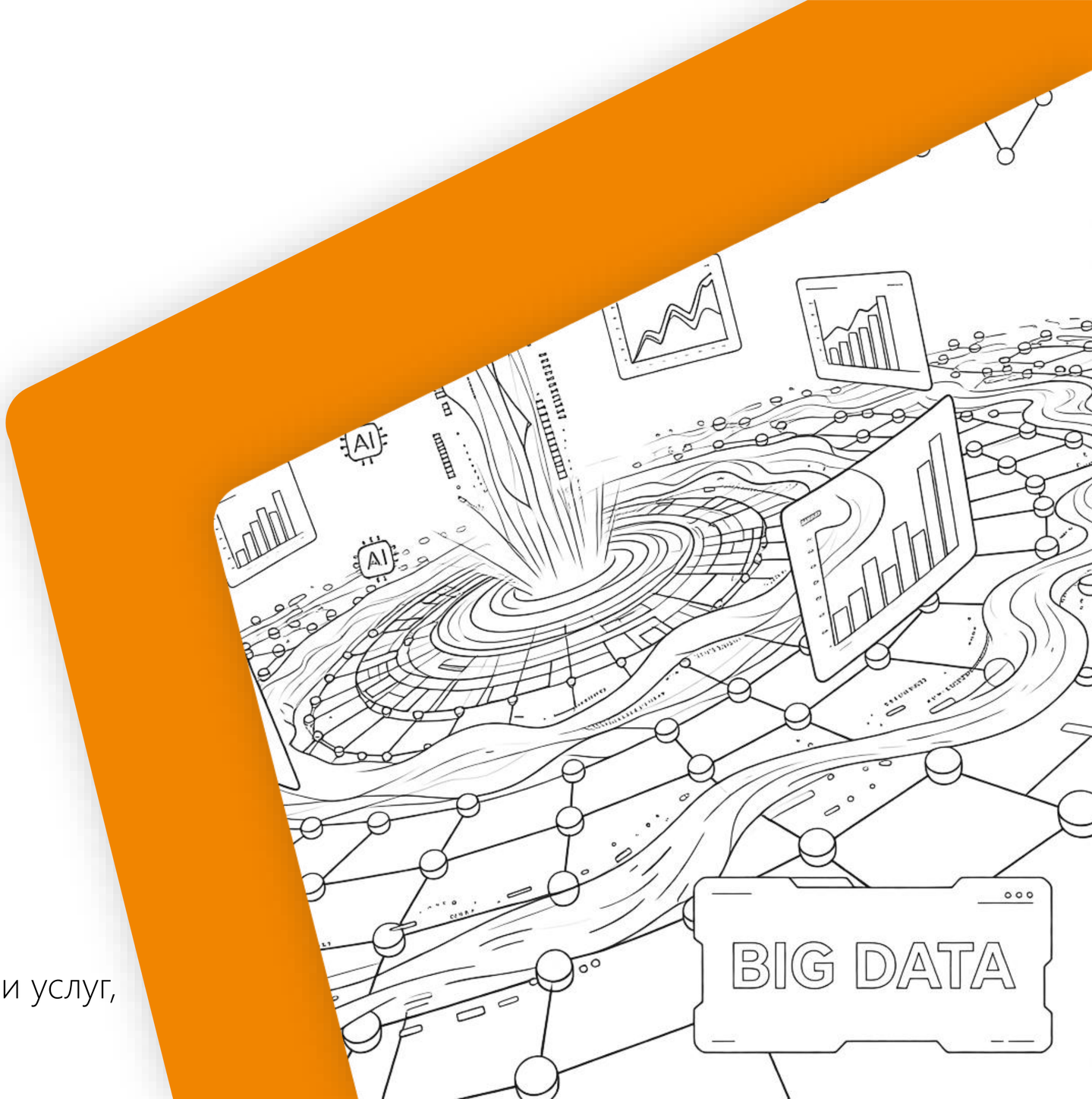
инфотекс
ТЕХНОДЕСТ

Белый поток

ПЕРСПЕКТИВНЫЙ МОНИТОРИНГ

AMPIRE

Ampire 2.0:
новый формат, карточки НКЦКИ и требования регулятора

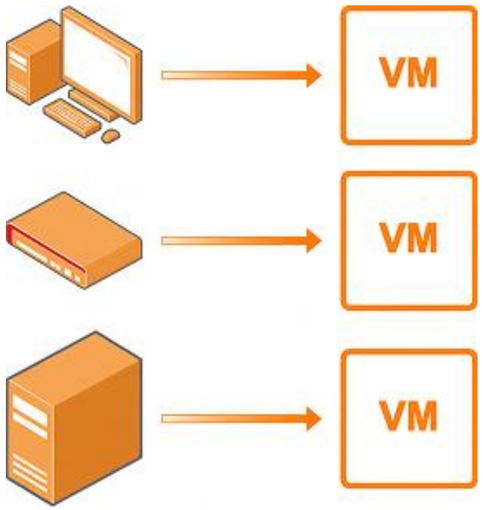


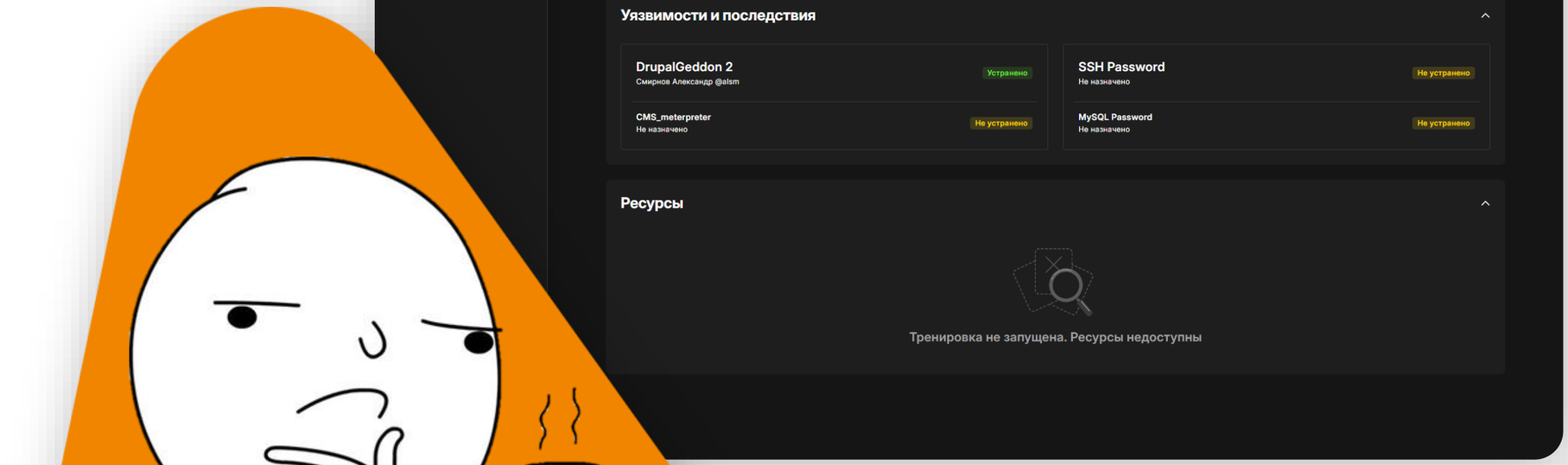
Георгий Мелихов,

Руководитель направления развития продуктов и услуг,
«Перспективный мониторинг»

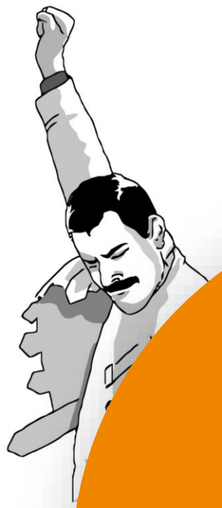
Что такое Ampire

Учебно-тренировочная платформа для отработки навыков противодействия киберугрозам





Ampireметр



40
действующих киберполигонов

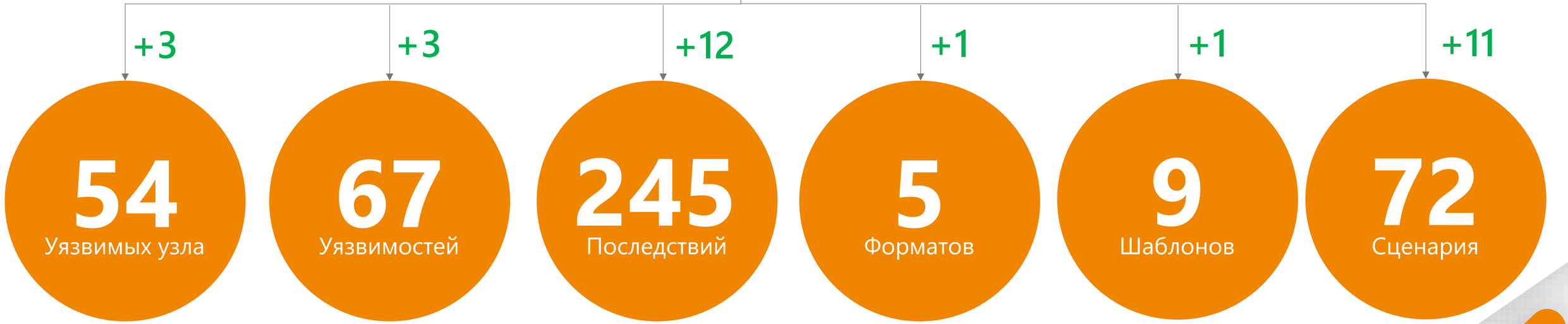
610
проведено киберучений

11
брендированных лабораторий

405
сертифицировано преподавателей

Ampireметр: доступно из коробки

Вклад Ampire 2.0 в «Ампирметр»



Что новенького в Ampire 2.0

- Red Team Labs
- Карточки инцидентов в формате НКЦКИ
- Сценарий фишинга в Red Team, новые уязвимые узлы, улучшение стабильности

Новый формат Red Team Labs

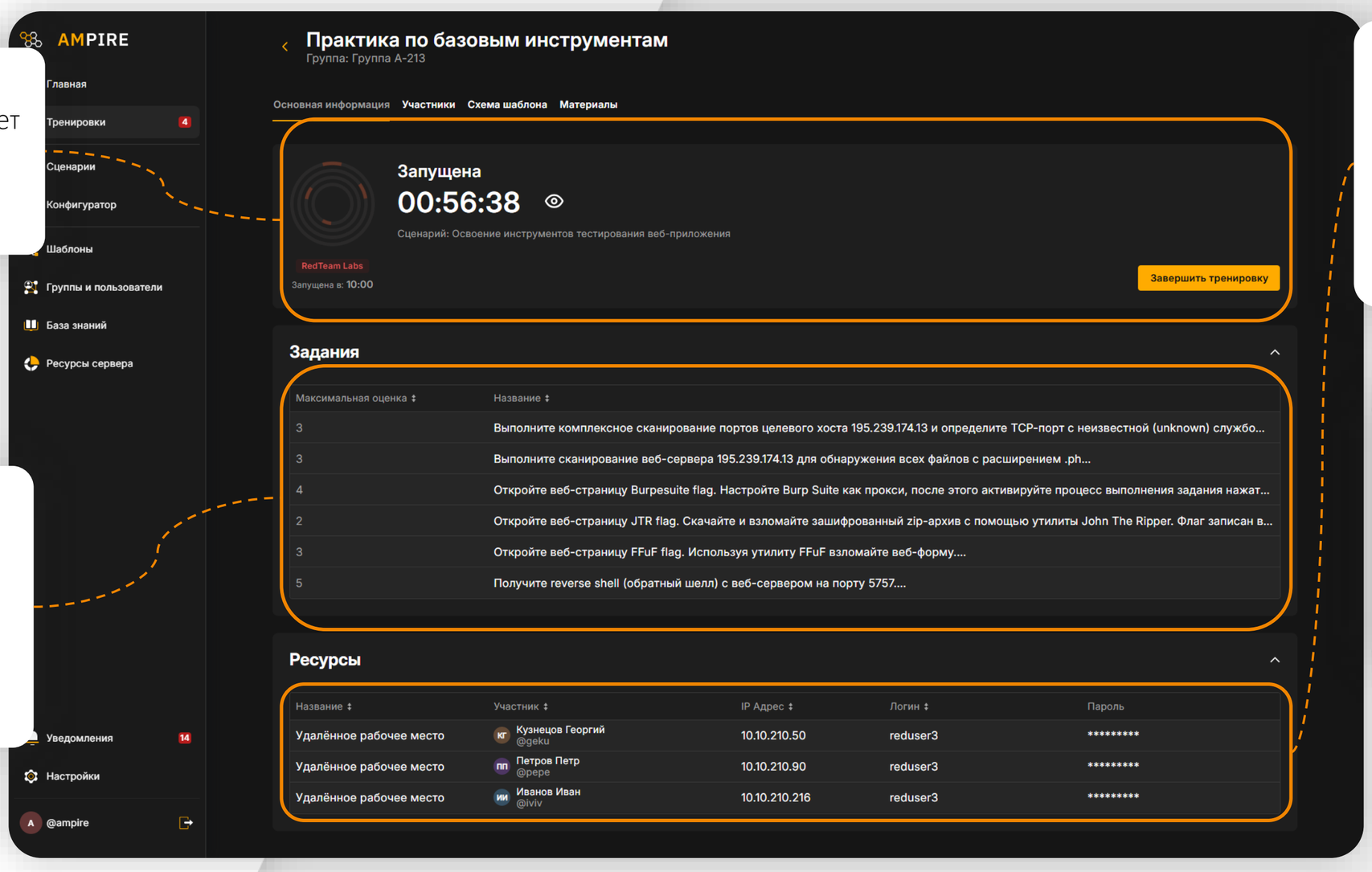
- Командный формат «Red Team» сложный
- Не хватает практических навыков
- Потребность в снижении порога входа
- Желание тренироваться в индивидуальном темпе

- Индивидуальный формат «Red Team Labs»
- Пентест и исследование защищенности
- Пошаговое прохождение сценария
- Поиск флага, ответы на теоретические вопросы
- Полностью автоматическая проверка заданий

Как работает Red Team Labs

1

Преподаватель выбирает сценарий и запускает тренировку



2

Участник подключается к индивидуальному экземпляру инфраструктуры для прохождения сценария

3

Участник пошагово проходит задания на поиск флага и на теорию

4

Участник отправляет задания на проверку – система автоматически их проверяет и ставит балл

Что доступно в Red Team Labs

В Red Team Labs для версии Ampire 2.0:

- 2 модуля – «Web» и «AD»
- 10 сценариев разного уровня сложности
- Методическое пособие для обучаемого по каждому сценарию
- Решебник для преподавателя по каждому сценарию
- Автоматическое создание групповых и индивидуальных отчётов о тренировке

Сценарии применения Red Team Labs

- Практическое сопровождение лекций по различным ИБ-дисциплинам, например, «Анализ безопасности Web-приложений», «Тестирование ИС на проникновение» и др.
- Создание индивидуального графика отработки навыков, обеспечение индивидуального контроля успеваемости
- Проведение зачётов, экзаменов, вступительных испытаний, собеседований и аналогичных мероприятий для разной целевой аудитории
- Разработка собственных сценариев с учётом желаемой специфики в рамках курсовых и дипломных работ, грантов и иных дополнительных активностях

Инциденты в форме НКЦКИ

Тренировки Blue Team и CSIRT

Карточки инцидентов в упрощенной форме

Знакомство с процессом оформления инцидентов

Практика базовых навыков передачи данных
о компьютерной атаке

Карточки инцидентов в формате НКЦКИ

Отработка навыков передачи данных
об инцидентах
и компьютерных атаках
по требованиям регулятора

Воссоздание ситуаций, требующих взаимодействия
с НКЦКИ

Тренировка с карточками НКЦКИ

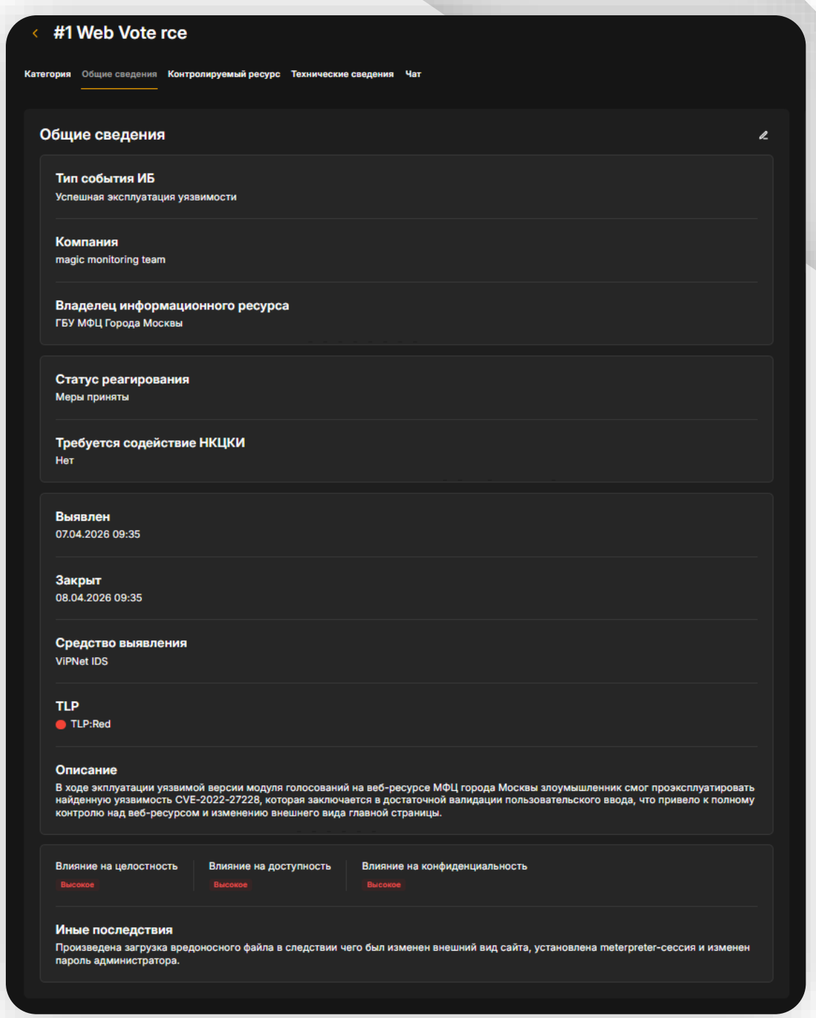
Как можно практиковаться:

1. Участники детектируют атаку, проводят расследования и по итогам подробно оформляют карточку инцидентов НКЦКИ

   Преподаватель рассматривает заведенный инцидент и оценивает корректность заполнения

2. Преподаватель или организатор самостоятельно составляет легенду сценария и определяет сам сценарий

   Участники знакомятся с форматом отправки данных об инциденте и заполняют карточку по требованиям преподавателя



Киберучения | Зачет, экзамен | Соревнования | Олимпиады | Мастер-классы

Что ещё нового

Фишинг в Red Team

Участники должны организовать фишинговую рассылку на виртуальной инфраструктуре, «убедить» виртуального пользователя скачать вредоносное вложение и установить сессию с пользовательской АРМ

Уязвимые узлы

Новые уязвимые узлы для конфигуратора, связанные с настройками безопасности ОС и особенностями работы SSL-сертификатов.

Новый уязвимый узел для шаблона «Телеком ОКС-7», который моделирует систему биллинга с уязвимостью, приводящей к удаленном выполнению кода в обход аутентификации

Стабильность

Дополнительный контроль над процессом развертывания тренировки и автоматический учёт готовности всех необходимых для сценария элементов инфраструктуры

Влияние Ampire

Специалисты

Разработчики СЗИ

Школьники

Непрофильные специалисты

Специалисты ИТ

Начинающие специалисты

Разработчики и DevOps

Отраслевые специалисты

- Резюме с Ampire за месяц: 120
- Резюме с Ampire за год: 288

Ampire де-факто становится стандартом практической подготовки в области ИБ

ПЕРСПЕКТИВНЫЙ МОНИТОРИНГ

AMPIRE

Спасибо за внимание!

@AMonitoring

ampire.team

amonitoring.ru

Георгий Мелихов,

Руководитель направления развития продуктов и услуг,

«Перспективный мониторинг»

+7 (495) 737-61-97

info@amonitoring.ru

САНКТ ПЕТЕРБУРГ

инфотекс

ТЕХНОДЕСТ

инфотекс Академия | Учебный центр инфотекс | AMPIRE | TELEOFIS | КОМФОРТЕЛ оператор связи бизнес-класса | РУТОКЕН компания ПРАКТИВ | TS Solution | AXOFT

Подписывайтесь на наши соцсети