

Ampire 360°



ПЕРСПЕКТИВНЫЙ
МОНИТОРИНГ

Ampire 360°

ПОЛИГОН КИБЕРБЕЗОПАСНОСТИ



Threat Intelligence

SOC & DFIR

Offensive Security

Киберучения

ИИ и киберзащита

Киберполигон Ampire

📅 14 октября





Практика организации и проведения киберучений с органами исполнительной власти

Соколов Кирилл Вячеславович

Старший аналитик отдела реагирования на инциденты
ФГБУ НИИ Интеграл



Опыт проведения

Ampire 360°

Проводим киберучения с 2024 года

Работаем с ФОИВ и коммерческими организациями

Обучаем собственные отделы мониторинга и реагирования

Использовали программный комплекс Ampire для подготовки к аккредитации



Как мы проводим киберучения

Теория

- Сетевые сканеры и управление уязвимостями
- Системы IDS/IPS на базе Suricata
- Что такое киберучения. Знакомство с интерфейсом Ampire

Практика

- Обнаружение вредоносной активности
- Создание карточек инцидентов
- Устранение уязвимостей и ликвидация последствий

Проблема в теории

Ситуация: провёл киберучения

Проблема: лекции не дают участникам прикладных знаний

Решение: связали теорию с конкретными сценариями

Результат: участники стали увереннее проходить сценарии

Вывод: теория должна готовить к практике, а не существовать отдельно

Кому подходят киберучения

Студенты: не знакомы с SOC

Начинающие: знают основы ИБ

Опытные: аналитики SOC,
форензики, эксперты

Руководители: отработать
рабочие процессы

Ситуация на практике

Ситуация: участник решил закрыть уязвимость, заблокировав весь входящий трафик на МСЭ

Проблема: весь сетевой трафик отбрасывается – никто не может подключиться к хосту

Что делали: выбирали между перезапуском тренировки (потеря прогресса) и продолжением с незакрытой уязвимостью – выбрали второе

Урок: даже опытный специалист может ошибиться

Вывод: ошибки допускают все, но не все делают из них выводы

Форматы проведения

За два года проводили киберучения в трёх форматах:



Дистанционный



Очный



Гибридный

Плюсы

- Не нужно никуда ездить – каждый на своём месте
- Пропущенное можно посмотреть в записи

Минусы

- Сложнее подготовки: VPN, рассылки, тестовая конференция
- Участники неохотно общаются в общем чате
- Проблемы с подключением
- Разные часовые пояса усложняют выбор времени

Вывод: оптимален для распределённых команд и коммерческих организаций

Проблема с подключением

Ситуация: участник находится в закрытом контуре на объект КИИ

Проблема: нет возможности использовать VPN

Что пробовали: выдать ноутбук – не смогли; личный – не работал; подключение с телефона – без практики

Результат: участник присутствовал только теоретически, без практики

Вывод: такие случаи нужно предусматривать заранее – на этапе требований к участию

Проблема с часовым поясом

Ситуация: отправили письмо о старте в 12:00 по Москве

Проблема: участник из другого региона понял время по своему поясу и опоздал

Решение: теперь указываем время с припиской «по МСК»

Результат: путаницы больше нет

Вывод: нужно следить за часовыми поясами участников

Один участник на тренировке

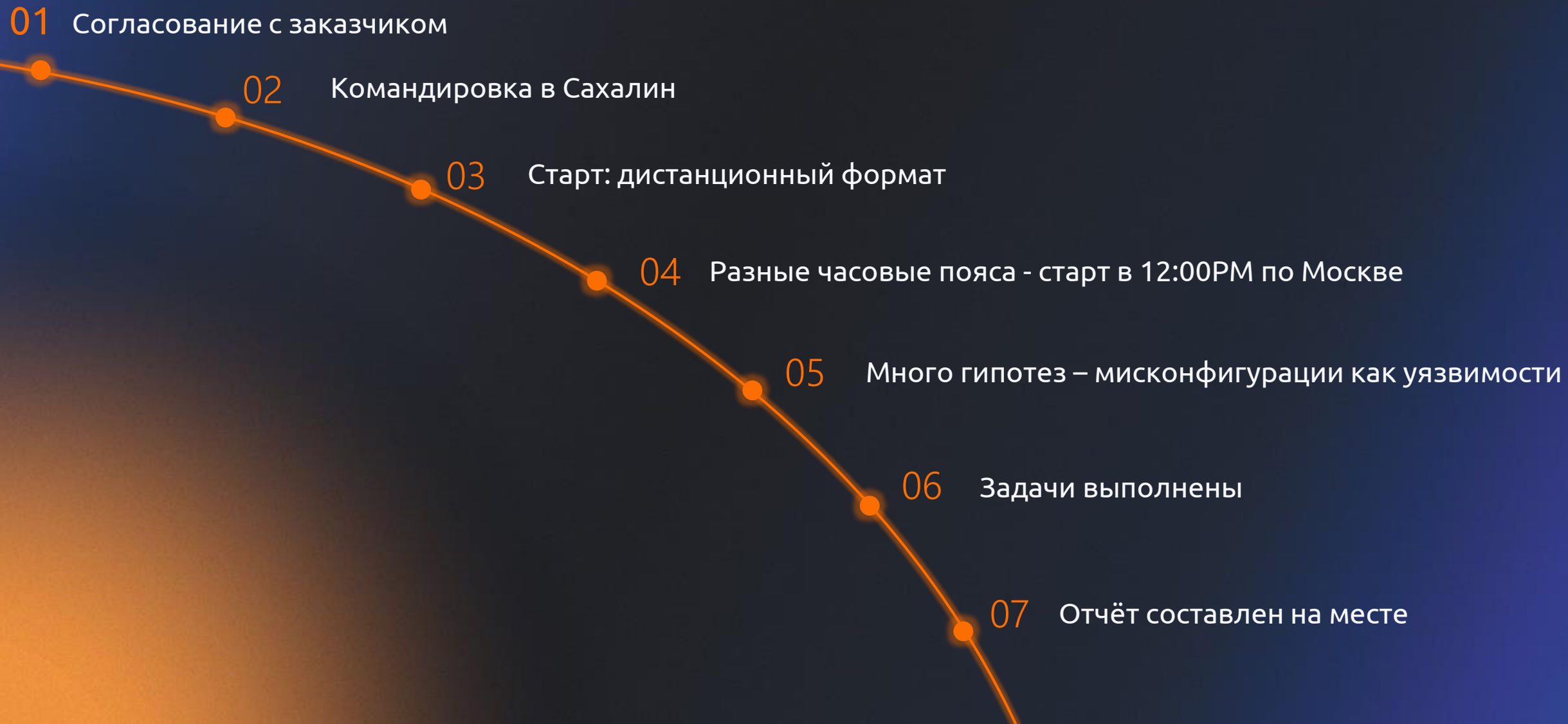
Ситуация: на тренировку заявилось 10 человек

Проблема: подключился только один – тренировка не запускается, нужно минимум два участника

Что сделали: добавил себя в команду, чтобы он мог проходить сценарий

Итог: тренировка состоялась, но как индивидуальное занятие

Вывод: заявка и реальная явка – разные вещи



Плюсы

- Живое общение и быстрая помощь
- Меньше технической подготовки
- Участники полностью вовлечены

Минусы

- Нужно собраться в одном месте
- Участники без своих привычных инструментов

Вывод: основной формат для ФОИВ и внутренних команд

Попытка автоматизировать решение

Ситуация: участник хотел, чтобы сценарий решала локальная ИИ

Проблема: установить ИИ не удалось – потратил полтора часа

Попытка: понял, что даже при успешной установке это не сработало бы

Итог: каждый сценарий разворачивает новую инфраструктуру – ИИ не адаптируется

Вывод: сценарии нужно решать самому – инструменты не заменяют навык

Киберучения для ФОИВ

Ampire 360°

01 Участники из разных регионов

02 Длительность: 3 дня

03 День 1: проблема коммуникации

04 День 2: результат лучше

05 День 3: все сценарии пройдены

06 Подведение итогов

07 Обсуждение сильных и слабых сторон

Выводы

Теория, тех. требования, часовые пояса, состав участников – всё важно

Формат зависит от желаний и возможностей заказчика

Каждый уровень подготовки получает своё

Спасибо за внимание!

Ampire 360°