Что под капотом у Ampire или почему так больно строить свой киберполигон

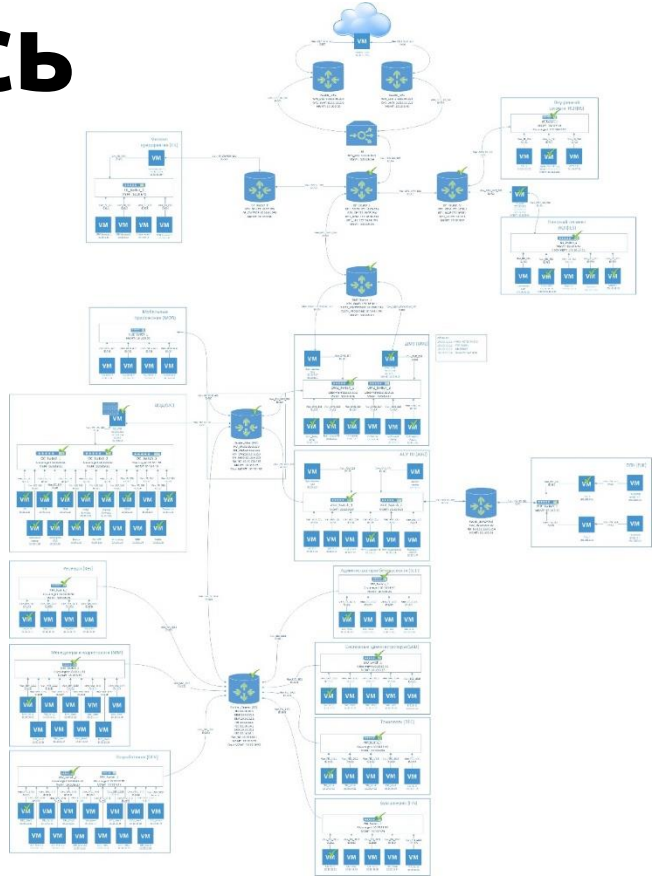
Юрий Худой
Начальник отдела ВСИП
Перспективный мониторинг

Ampire 360°

С чего всё начиналось

Первый киберполигон ПМ

- 4 гипервизора в кластере VMware
- 115 виртуальных машин
- 14 сетевых сегментов
- 30 виртуальных коммутаторов и маршрутизаторов
- Эмуляция физического подключения к виртуальным коммутаторам
- Эмуляция действий пользователей
- Время подготовки к занятию ≈1 часа



Проблемы

- Долгое время подготовки
- Слишком большая инфраструктура
- Ограниченное число участников
- Избыточное потребление ресурсов
- Сложно поддерживать и развивать

Ampire 360°

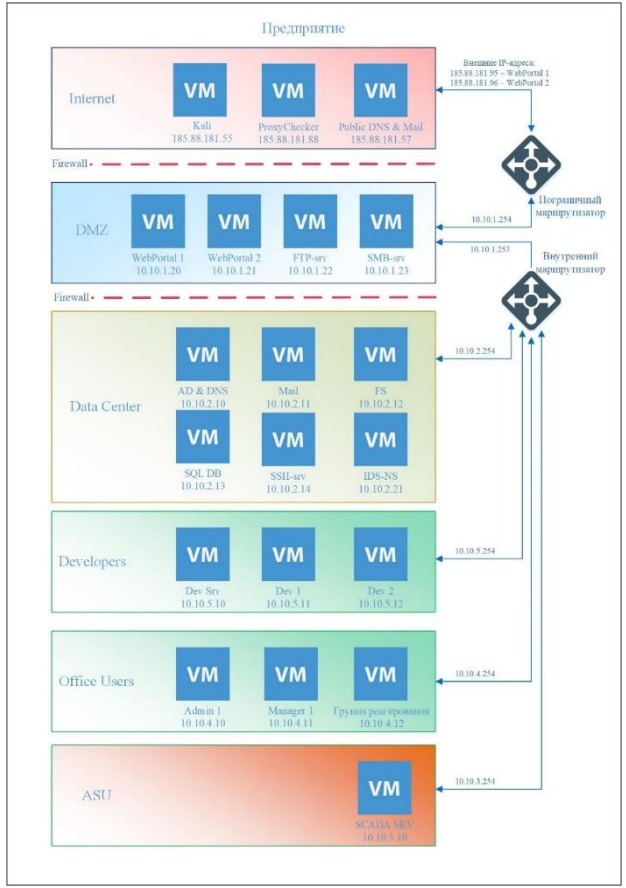
Новая реализация

Три основных компонента

- Портал
- Шаблон инфраструктуры
- Сценарии

Изменения

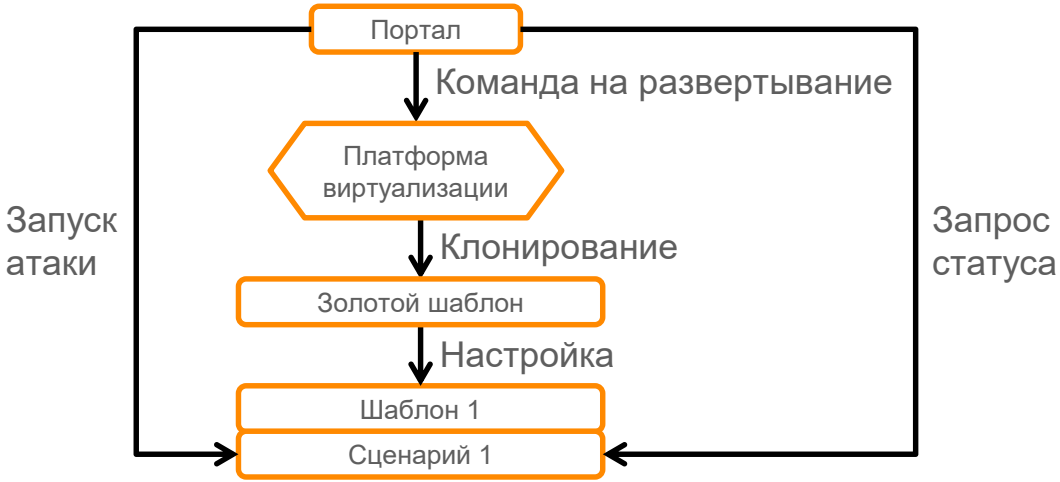
- Уменьшение размера инфраструктуры
- Одна тренировка – один шаблон инфраструктуры
- Время жизни шаблона ограничено тренировкой
- Есть “горячие” шаблоны
- Запуск параллельных тренировок

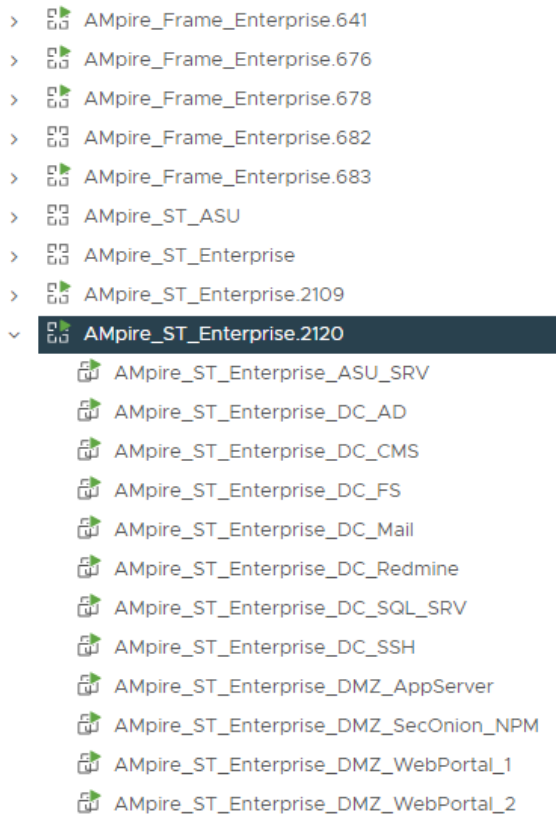


Ampire 360°

Шаблоны и сценарии

Общая схема взаимодействия





Ampire 360°

Шаблоны и сценарии

Доступ к шаблону и служебные ВМ

Особенности

- Необходимость запуска команд внутри ВМ, не имея к ним сетевого доступа
- Сетевая изолированность шаблона
- Управляющая подсеть

Служебные ВМ

- ВМ группы реагирования
- ВМ группы мониторинга (СЗИ)
- ВМ атакующего (Kali)
- ВМ контроля статусов уязвимостей (ProxyChecker)

Ampire 360°

Шаблоны и сценарии

Особенности сценариев

Типы нарушителей

- Внешний
- Внутренний
- Зараженный хост

Элементы сценария

- Вектор атаки
- Библиотека действий нарушителя на ВМ атакующего
- Чекеры на уязвимых ВМ
- Статусы уязвимостей

Ampire 360°

Так в чем боль?

Железо и инфраструктура

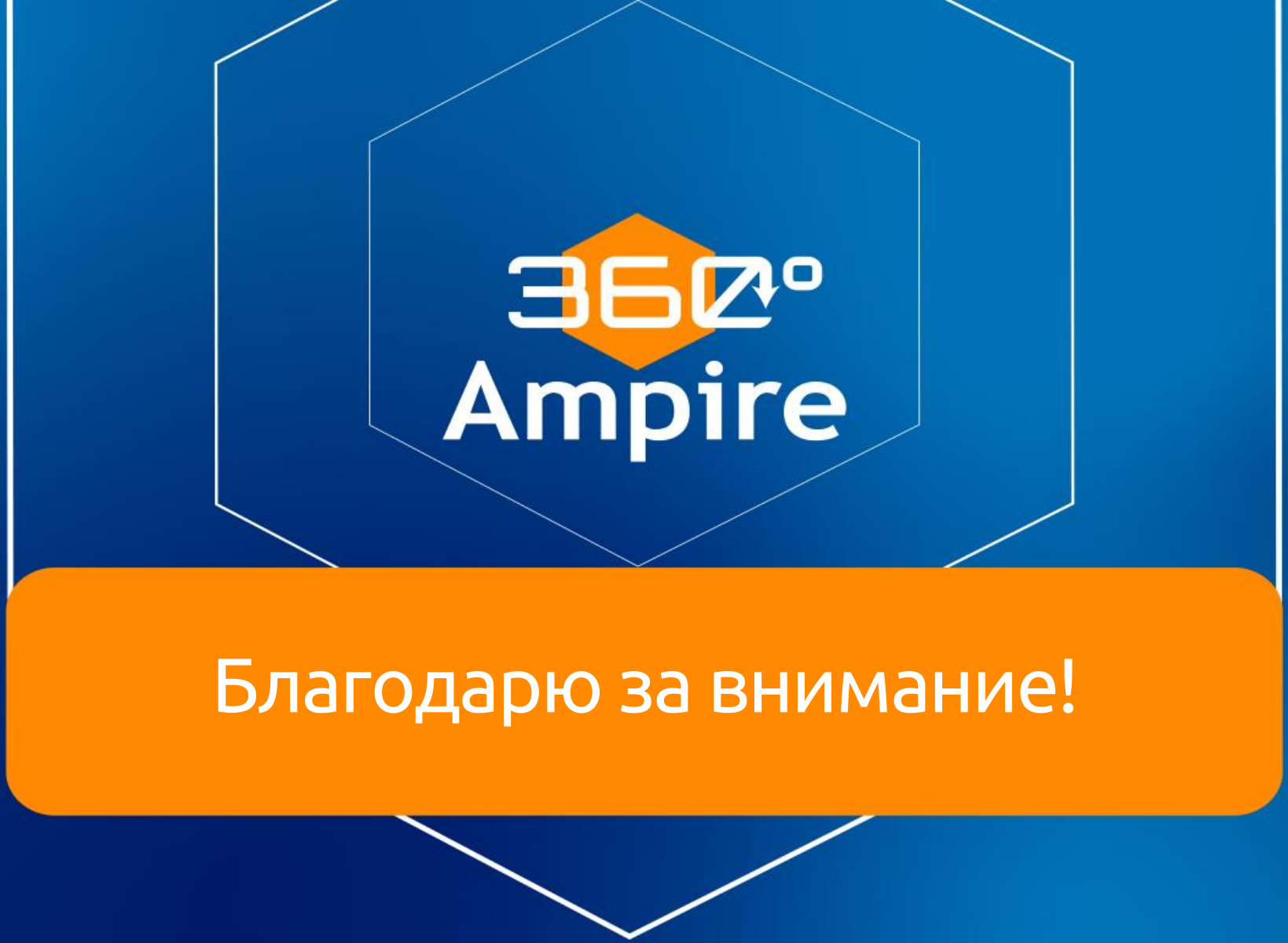
- Только SSD
- Баланс потребления ресурсов
- Тайминг развертывания
- Разные гипервизоры
- Зеркалирование трафика
- Лицензирование и СЗИ

Сценарии атак

- Сложности виртуализации
- Стабильность атак
- Требования к уязвимостям

Обновления

- Портал
- Виртуальные машины
- Содержимое виртуальных машин
- Базы правил СЗИ



Благодарю за внимание!