Киберполигон для подготовки в области информационной безопасности диспетчеров и команды реагирования на компьютерные атаки ПАО «Россети Волга»

АКТУАЛЬНОСТЬ

- **ФЗ от 26 июля 2017 г. № 187-ФЗ «О безопасности критической информационной инфраструктуры РФ»**
  Проведение киберучений является одним из необходимых регулярных мероприятий субъекта КИИ.
  Киберполигон учитывает требования ГОССОПКА

- **Реализация концепции «Цифровая трансформация 2030» ПАО «Россети»** в рамках исполнения указов Президента РФ Путина В.В. от 09.05.2017 № 203 «О Стратегии развития информационного общества в Российской Федерации на 2017 - 2030 годы» и от 07.05.2018 № 204 «О национальных целях и стратегических задачах развития Российской Федерации на период до 2024 года»

- Целенаправленные атаки (APT) реализуются в отношении конкретной инфраструктуры ПАО «Россети» в обход установленных средств защиты информации. В этой ситуации команды диспетчеров и реагирования должны быть готовы дать отпор - быстро и эффективно

КОНЦЕПЦИЯ

- Российское программное обеспечение
- Использование технологий виртуализации для создания цифровых двойников объектов КИИ
- Проверка эффективности планов обеспечения непрерывности бизнеса (BCP) и восстановления после катастроф (DRP)
- Повышение осведомленности диспетчеров в вопросах ИБ
- Снижение среднего времени реагирования на инциденты ИБ
- Обучение персонала расследованию инцидентов ИБ и выявлению их причин на основе анализа данных системы управления событиями ИБ SIEM
- Автоматическая генерация тестовых атак

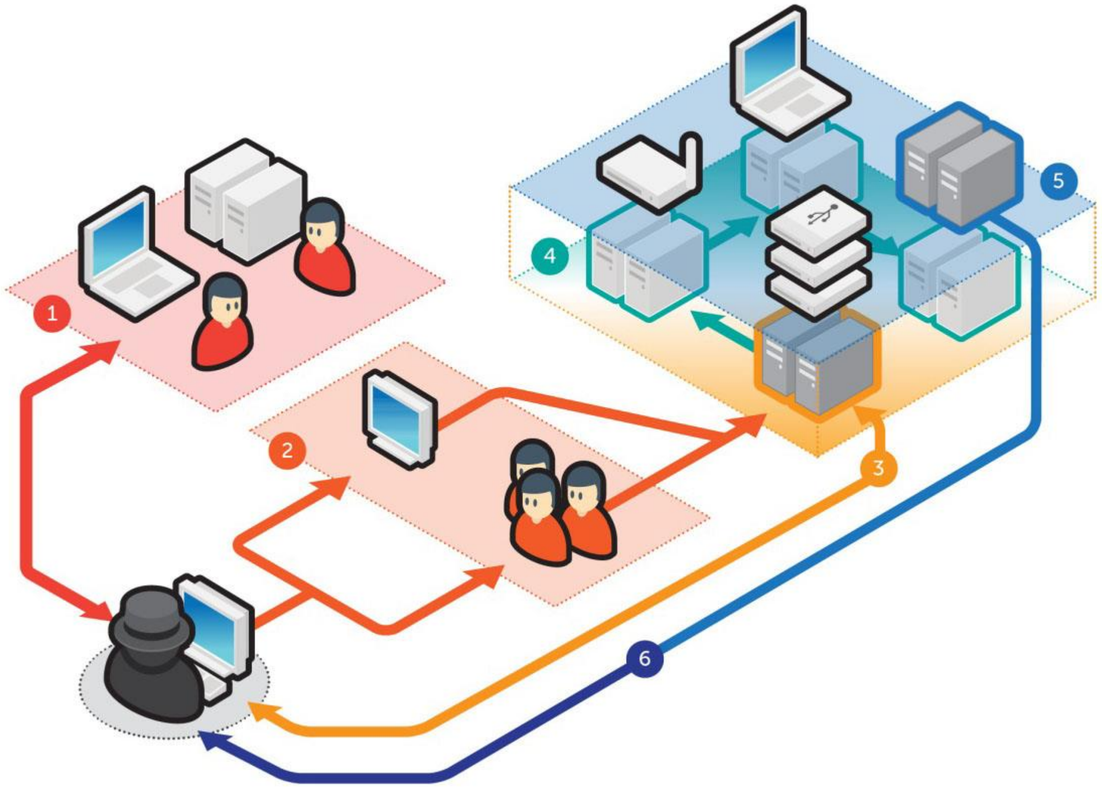
Киберполигон

многофункциональный комплекс
для подготовки в области ИБ диспетчеров
и команды реагирования на компьютерные
атаки

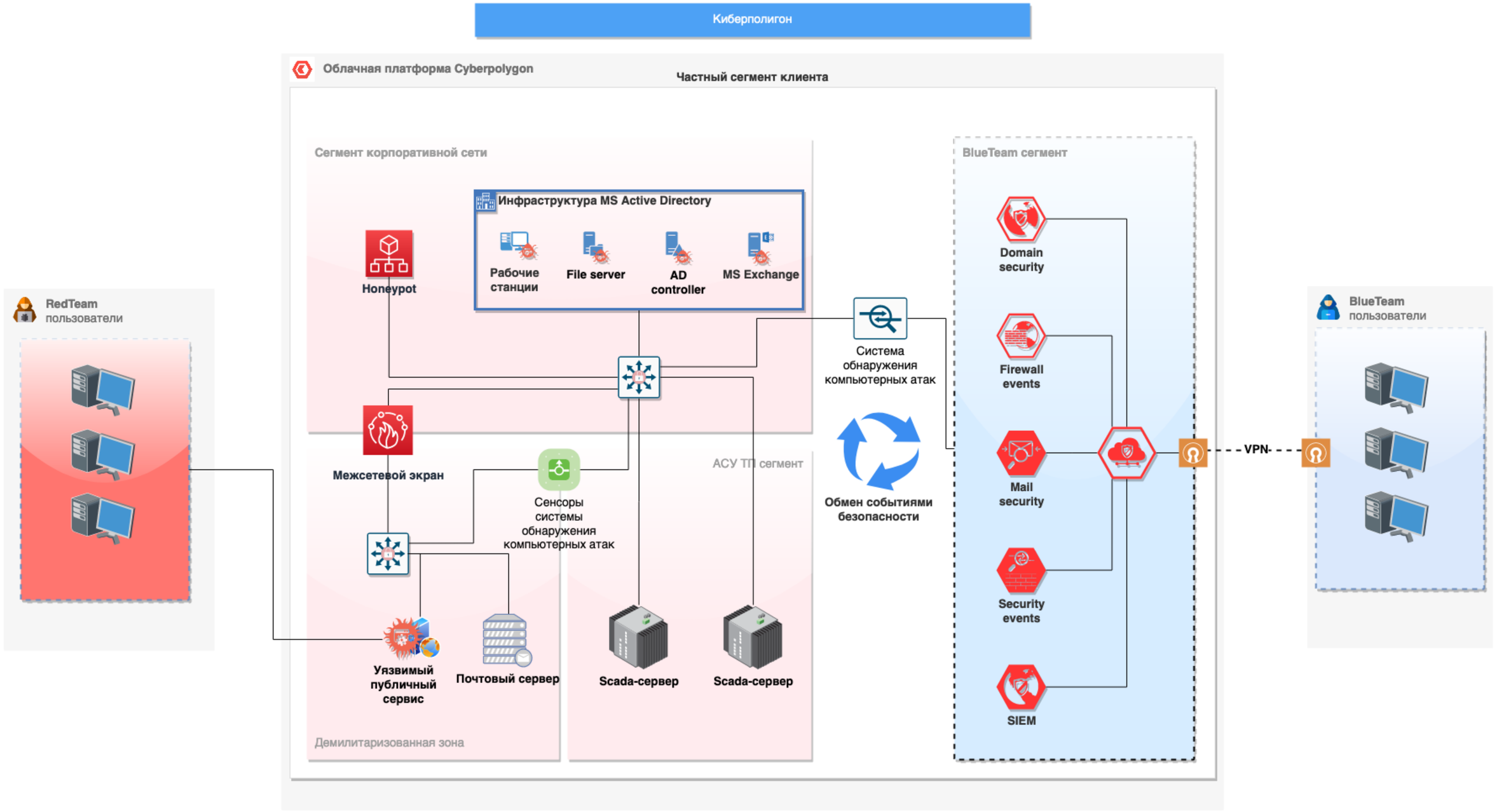
РЕШЕНИЕ

Состав Киберполигона:

1) Аппаратная платформа
2) Коммутаторы
3) Типовые шаблоны защищаемой ИТ-инфраструктуры (с оркестрацией развертывания инфраструктуры)
4) Сценарии 12 автоматически реализуемых атак
5) Эмуляция действий легитимных пользователей
6) Централизованная консоль управления
7) Учебно-методические материалы



ИНФРАСТРУКТУРА КИБЕРПОЛИГОНА



ЗАДАЧИ КИБЕРПОЛИГОНА

Повышение устойчивости функционирования ИТ-инфраструктуры ПАО «Россети Волга» посредством киберучений:

- Аудит эффективности BCP и DRP
- Регулярные киберучения
- Проверка эффективности действующего центра мониторинга ИБ (SOC)
- Оценка эффективности команд диспетчеров, ИБ, ИТ и технической поддержки в процессах реагирования на компьютерные атаки

Киберполигон

многофункциональный комплекс
для подготовки в области ИБ диспетчеров
и команды реагирования на компьютерные
атаки

ЭКСПЕРТИЗА ООО «Киберполигон»

Обширный проектный опыт аудита промышленных, финансовых, e-commerce и государственных систем России, Белоруссии, Азербайджана, Чехии, Израиля, Кипра, Ирландии, Германии.

Нахождение в «залах славы» Yandex, Mail.ru, Google, IBM, Toyota, Mozilla, Telegram, Sony, Adobe.

Контрибуция в OWASP.

Практические навыки подтверждены сертификатами CEH/OSCP/OSWE.

ООО «Киберполигон»
тел.: +7-499-113-13-37
e-mail: info@cyberpoly.ru
сайт: https://cyberpoly.ru

Киберполигон

многофункциональный комплекс
для подготовки в области ИБ диспетчеров
и команды реагирования на компьютерные
атаки