PURPLE GROUND

CENTER-INFORM.RU

КИБЕРПОЛИГОН

**СИСТЕМА МОДЕЛИРОВАНИЯ КИБЕРУГРОЗ
И ЛИКВИДАЦИИ КОМПЬЮТЕРНЫХ ИНЦИДЕНТОВ
В ИНФОРМАЦИОННЫХ ИНФРАСТРУКТУРАХ**

ЦЕНТРИНФОРМ

ЧТО ТАКОЕ КИБЕРПОЛИГОН

Система моделирования киберугроз и ликвидации компьютерных инцидентов в информационных инфраструктурах

НАЗНАЧЕНИЕ СИСТЕМЫ:

- Отработка практических навыков по предотвращению компьютерных атак и ликвидации их последствий
- Тестирование средств защиты информации
- Повышение уровня командного взаимодействия
- Тренировка специалистов по ИБ

ДЛЯ:

- ОРГАНИЗАЦИЙ, ОБЕСПЕЧИВАЮЩИХ ИНФОРМАЦИОННУЮ БЕЗОПАСНОСТЬ
- ВУЗОВ, ОСУЩЕСТВЛЯЮЩИХ ПОДГОТОВКУ СПЕЦИАЛИСТОВ ИНФОРМАЦИОННОЙ БЕЗОПАСНОСТИ

ПОЧЕМУ КИБЕРПОЛИГОН

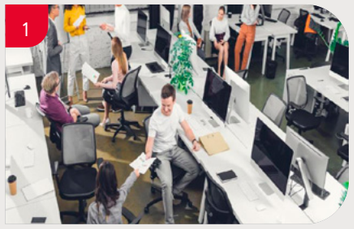
АКТУАЛЬНОСТЬ ПРОБЛЕМЫ КИБЕРАТАК	количество атак постоянно растет вектор атак меняется
АКТУАЛЬНОСТЬ ОБУЧЕНИЯ СПЕЦИАЛИСТОВ ИБ	дефицит кадров по ИБ увеличивается

КАК ПРОВОДЯТСЯ КИБЕРУЧЕНИЯ

Имитация IT-инфраструктуры для проведения киберучений

- Могут объединяться в одну для проведения масштабных учений

1



Корпоративная сеть имитирует наиболее распространенную топологию офисной сети

2

Телекоммуникационная сеть имитирует инфраструктуру, обслуживающую линии связи

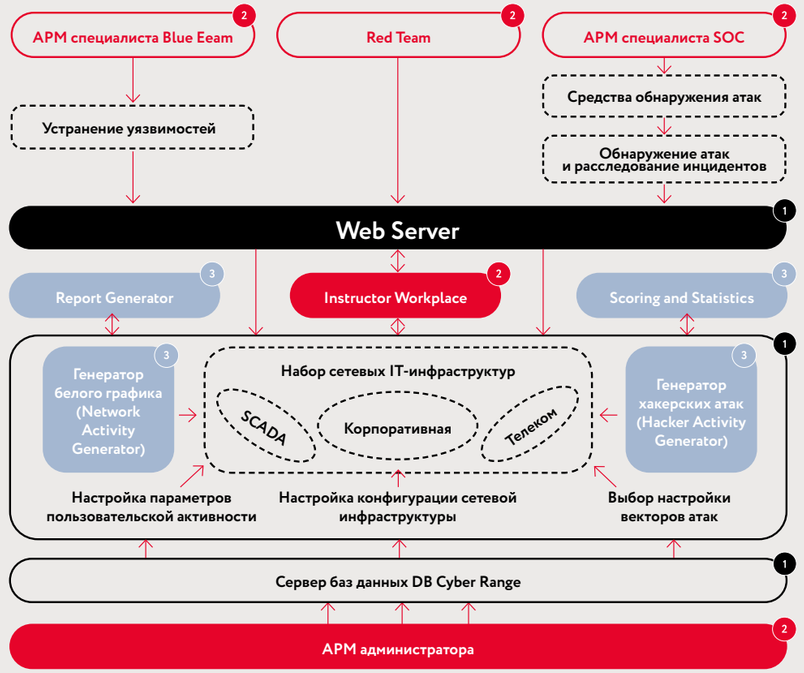
3

АСУ ТП имитирует SCADA-сеть гидроэлектростанции либо другого промышленного объекта

АРХИТЕКТУРА И СОСТАВ КИБЕРПОЛИГОНА

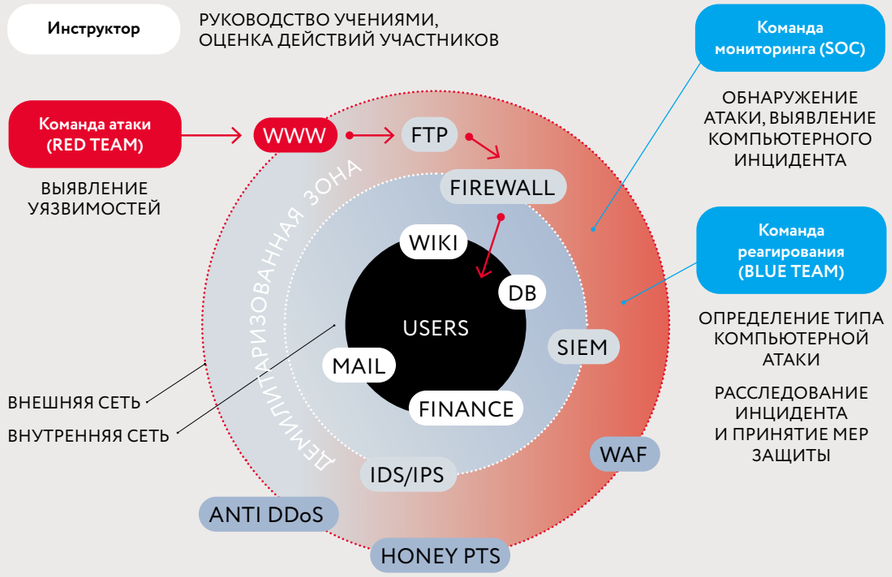
ОСНОВНЫЕ ЭЛЕМЕНТЫ:

1. **СЕРВЕРНАЯ ЧАСТЬ (ЯДРО)**
2. **КЛИЕНТСКАЯ ЧАСТЬ**
3. **СИСТЕМНЫЕ МОДУЛИ**



Защита критической информационной инфраструктуры от компьютерных атак

Цель: привитие практических навыков специалистам информационной безопасности по обнаружению, предупреждению и ликвидации последствий компьютерных атак и реагирования на компьютерные инциденты.



Программно-аппаратное обеспечение:

- Программное обеспечение системы моделирования киберугроз и ликвидации инцидентов безопасности в информационных инфраструктурах. Киберполигон
- Удаленный сервер АО «ЦентрИнформ»
- Персональные компьютеры (ноутбуки) участников с выходом в сеть интернет
- Демонстрационная панель инструктора киберучения

Задачи:

1. Практическое выявление уязвимостей КИИ.
2. Имитация компьютерной атаки на корпоративную сеть.
3. Отработка навыков обнаружения и идентификации компьютерной атаки.
4. Расследование компьютерного инцидента и ликвидация последствий компьютерной атаки.
5. Оценка индивидуальных и командных практических навыков специалистов по информационной безопасности.

ПРИМЕР КИБЕРУЧЕНИЯ НА БАЗЕ СЦЕНАРИЯ АТАКИ НА КОРПОРАТИВНУЮ СЕТЬ

ПРИМЕР СЦЕНАРИЯ АТАКИ:

- Атакующий проводит фишинговую кампанию, отправляя подготовленный скрипт на базе powershell
- Пользователь финансового департамента открывает вложение и запускает скрипт, в котором реализована функция обхода встроенного в Windows 10 антивируса
- Скрипт производит разведку, обращаясь к контроллеру домена, и обнаруживает, что пользователь является локальным администратором на машине SQL Server, где установлена сессия доменного администратора
- Подключившись с помощью winrm к SQL Server, скрипт получает доступ к аутентификационным данным администратора домена

ЗАДАЧИ КОМАНДЫ SOC И КОМАНДЫ BLUE TEAM:

- Обнаружить и пресечь распространение фишинговых писем
- Определить пользователей, которые успели прочитать содержимое фишингового письма и запустили вредоносный скрипт
- Предотвратить запуск содержимого фишингового письма для тех пользователей, которые не успели запустить вредоносный скрипт
- Расследовать инцидент и установить последствия работы вредоносного скрипта внутри сети
- Предотвратить дальнейшее развитие атаки и защитить контроллер домена

OPENSOURCE-ТЕХНОЛОГИИ

PROXMOX, Vuetify, django, NUXTJS, PostgreSQL, Ruby, python, Vue.js, BASH

Гипервизор
В качестве виртуальной среды используется Proxmox Virtual Environment, адаптированный под задачи киберполигона

Backend
Python
Фреймворк – Django
База данных PostgreSQL

Frontend
Фреймворки vue.js, vuetify, nuxt.js

Обработчик событий
База данных TinyDB и набор скриптов

Атакующий модуль
Набор скриптов на языках программирования PowerShell, Ruby, Python, Bash

Россия, 191123, Санкт-Петербург
ул. Комсомола, д. 1-3, литера АС
+7 (812) 303-90-20 доб. 0-2330
info@center-inform.ru

ЦЕНТРИНФОРМ
center-inform.ru