Ростелеком
Солар

Программный комплекс кибертренировок «Солар Кибермир»

Описание технической архитектуры

МОСКВА, 2023

Содержание

1. Назначение и решаемые задачи

1.1. Назначение

Программный комплекс кибертренировок «Солар Кибермир» (далее – Комплекс) предназначен для повышения уровня практической подготовки специалистов в области информационной безопасности по выявлению компьютерных атак, расследованию инцидентов информационной безопасности за счет автоматизации следующих процессов:

- проведение практических занятий по информационной безопасности (далее – ИБ): обнаружение, расследование и защита от кибератак (далее – КА);
- проведение учений и соревнований по информационной безопасности и защите от кибератак для специалистов по ИБ;
- оценка практических навыков специалистов в области ИБ;
- проведение исследований в области информационной безопасности программного обеспечения и автоматизированных систем.

1.2. Функциональные возможности и решаемые задачи

Основные функции комплекса кибертренировок «Солар Кибермир»:

- развертывание и управление виртуальными инфраструктурами мероприятий;
- создание шаблона мероприятия, состоящего из сценария кибератак и эталонного отчета;
- создание модели визуализации хода мероприятия на графической карте инфраструктуры;
- обеспечение доступа пользователей к удаленным рабочим столам виртуальной инфраструктуры мероприятия;
- автоматизированная оценка практических навыков участников мероприятия.

Комплекс кибертренировок «Солар Кибермир» решает следующие задачи:

- управление пользователями и организациями;
- ролевой контроль доступа пользователей;
- проведение учебных мероприятий – практических занятий по обнаружению и расследованию компьютерных атак;

- управление учебными мероприятиями
- отображение результатов мероприятия;
- графическая визуализация хода учебного мероприятия;
- обеспечение доступа пользователей к удаленным рабочим столам виртуальной инфраструктуры мероприятия;
- автоматизированная оценка результатов учебных мероприятий и навыков участников мероприятия;
- разработка модели визуализации хода учебного мероприятия на графической карте инфраструктуры.

2. Описание архитектуры

Серверная часть программного комплекса кибертренировок «Солар Кибермир» (backend) реализована в виде набора слабосвязанных программных модулей (микросервисов), выполняющих различные функции (Рис.1).

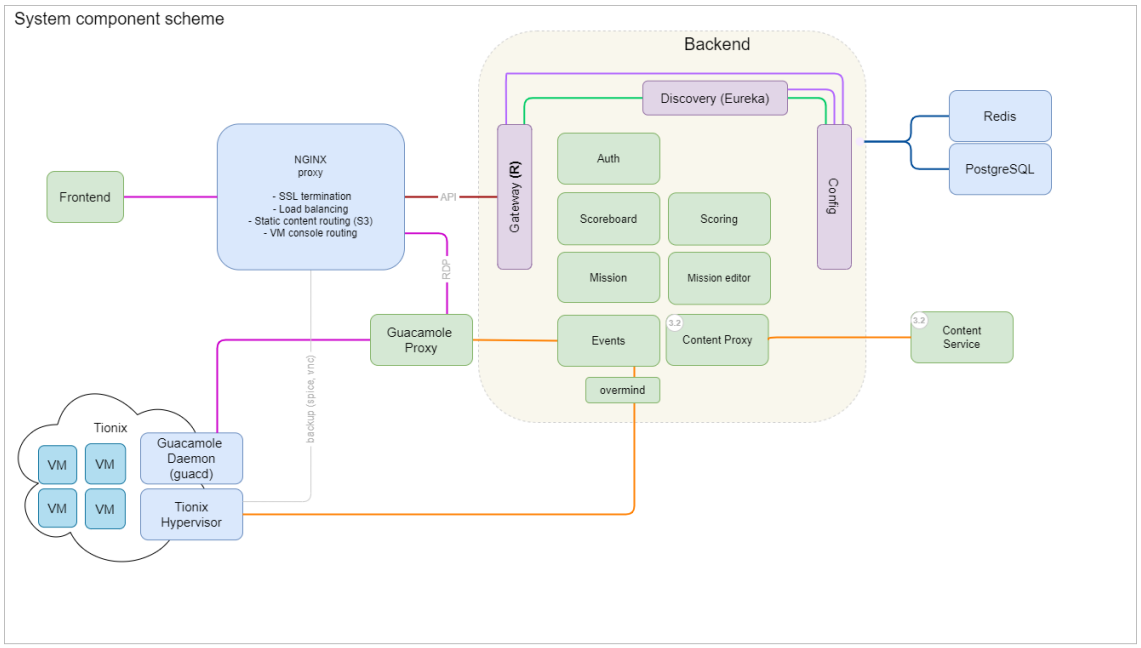

Рис. 1 – Архитектура ПК кибертренировок «Солар Кибермир»

Реализованы следующие сервисы:

- сервис аутентификации (Auth);
- сервис проведения мероприятий (Events);
- сервис хранения миссий (Mission);
- сервис редактора миссий (Mission editor);
- сервис скоринга (Scoring);
- сервис доски результатов (Scoreboad);
- сервис хранения контента (Content service, Content Proxy).

При этом:

- сервисы напрямую обращаются друг к другу (без использования брокеров сообщений);
- пользовательский интерфейс платформы реализован на языке программирования JavaScript.
- доступ к функциональности серверной части платформы осуществляется через фасадный сервис (API Gateway);

- обращения к функциональности серверной части защищены механизмами аутентификации и авторизации;
- для хранения данных применяется СУБД PostgreSQL;
- для хранения эфемерных данных применяется СУБД Redis;
- платформа использует сервер на базе ОС Linux;
- серверная часть реализована с применением языка программирования Java.

Программный комплекс кибертренировок «Солар Кибермир» обеспечивает доступ участников мероприятий к функциональности при помощи браузера по протоколу HTTPS, включая:

- доступ к удаленным рабочим столам гостевых операционных систем через браузер по протоколу RDP;
- работу с виртуальными машинами на базе Windows и Linux;
- поддержку обмена данными через буфер обмена между пользовательской ОС и гостевой ОС на виртуальной машине.

3. Условия эксплуатации

3.1. Требования к серверу приложения

Минимальные требования к аппаратному обеспечению сервера приложений:

- процессор не менее 12 ядер с тактовой частотой не менее 3 ГГц и поддержкой архитектуры x64;
- объем оперативной памяти не менее 32 ГБ;
- объем жесткого диска не менее 250 ГБ;
- сетевой адаптер Ethernet с пропускной способностью не ниже 100 Мбит/с.

Требования к программному обеспечению сервера:

- операционная система Linux x64 без графического интерфейса с установленными средствами защиты информации.

3.2. Требования к автоматизированному рабочему месту пользователя

Требования к аппаратному обеспечению:

- процессор не менее 4 ядер с тактовой частотой не менее 2,8 ГГц;
- объем оперативной памяти не менее 4 ГБ;
- объем жесткого диска не менее 128 ГБ;
- разрешение экрана при работе с интерфейсом не менее 1024x768 (интерфейс оптимизирован для разрешения 1920x1080);
- сетевой адаптер Ethernet с пропускной способностью не ниже 10 Мбит/с.

Требования к программному обеспечению:

- операционная система Linux x64 с установленным графическим интерфейсом.

Перечень принятых сокращений

АРМ	Автоматизированное рабочее место
ИБ	Информационная безопасность