SOLAR

Платформа «Кибермир»

МОСКВА 2024

Безопасность это навыки

Безопасность это задачи

Апробация новых технологий и решений
пилоты, тестирование,
поиск уязвимостей, проверка гипотез

Проверка работоспособности процессов и их развитие
документирование, учения,
тестирования, практика применения

Кадровые вопросы
поиск кадров, оценка квалификации,
развитие навыков,
формализация подхода к обучению

Для чего нужен киберполигон?

SOLAR

ИССЛЕДОВАНИЯ И ТЕСТИРОВАНИЕ
ПОСТРОЕНИЕ КИБЕРПОЛИГОНОВ

Построение киберполигонов
на базе инфраструктуры заказчика
с использованием платформы
«Кибермир»

Создание цифровых двойников
сегментов ИТ-инфраструктуры
заказчика на базе мощностей
киберполигона

ПРОВЕРКА ГОТОВНОСТИ
КИБЕРУЧЕНИЯ

Практические киберучения
на платформе «Кибермир»
- Стандартные сценарии
- Кастомные сценарии

Командно-штабные тренировки для
организационной отработки
сценариев реагирования

Командные соревнования
в формате CTF

РАЗВИТИЕ НАВЫКОВ
КИБЕРБУСТ

Комплексная образовательная
программа развития навыков
киберзащиты для Blue Team,
практическая отработка
на киберполигоне

Модульный образовательный
киберинтенсив для получения
ключевых знаний и навыков ИБ

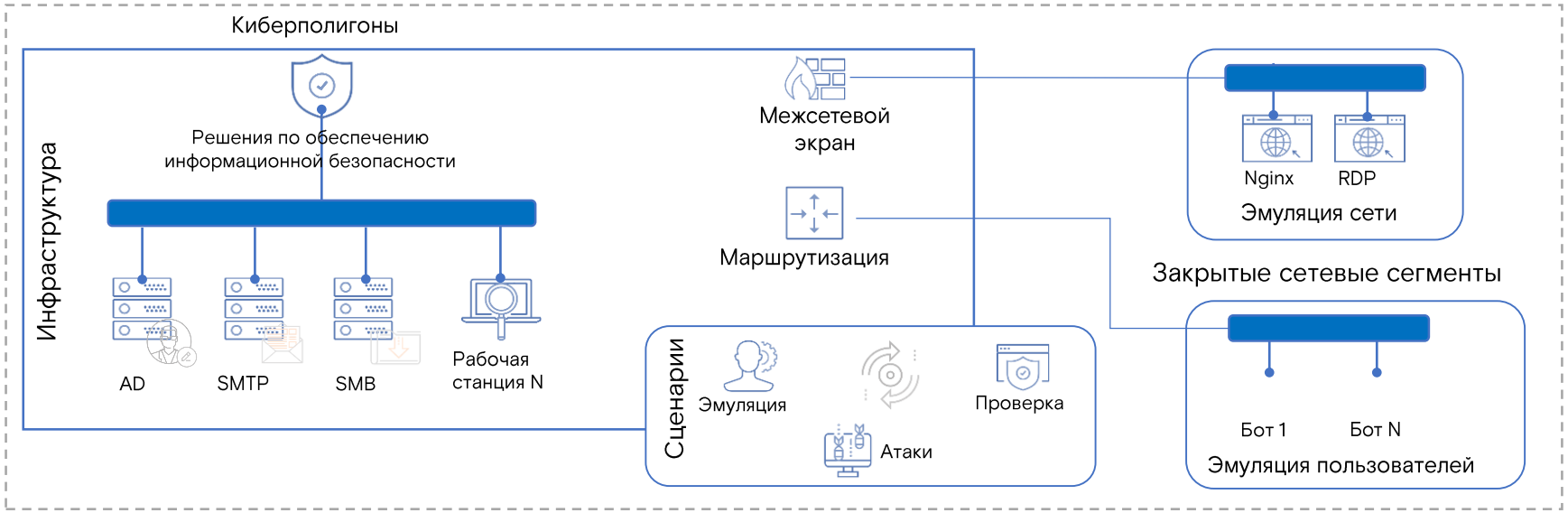
Платформа «Кибермир» лежит в основе всех для организации киберучений, построения киберполигонов и развития навыков кибербезопасности

Структура Кибермира

ТИПОВЫЕ ОТРАСЛЕВЫЕ ИНФРАСТРУКТУРЫ МАКСИМАЛЬНО ПРИБЛИЖЕНЫ К РЕАЛЬНЫМ

- Транспортировка нефти и газа
- Добыча нефти и газа
- Передача электроэнергии
- Генерация электроэнергии
- Финансовый сектор
- Телеком
- Корпоративный офис

Архитектура



Серверная часть платформы (бэкенд) — Генератор сценариев | Подсчет баллов | Полигоны | Хранилище событий

Внешний интерфейс платформы (фронтенд) — Удаленный доступ | Топология ВМ | Визуализация событий | Прогресс | Чат

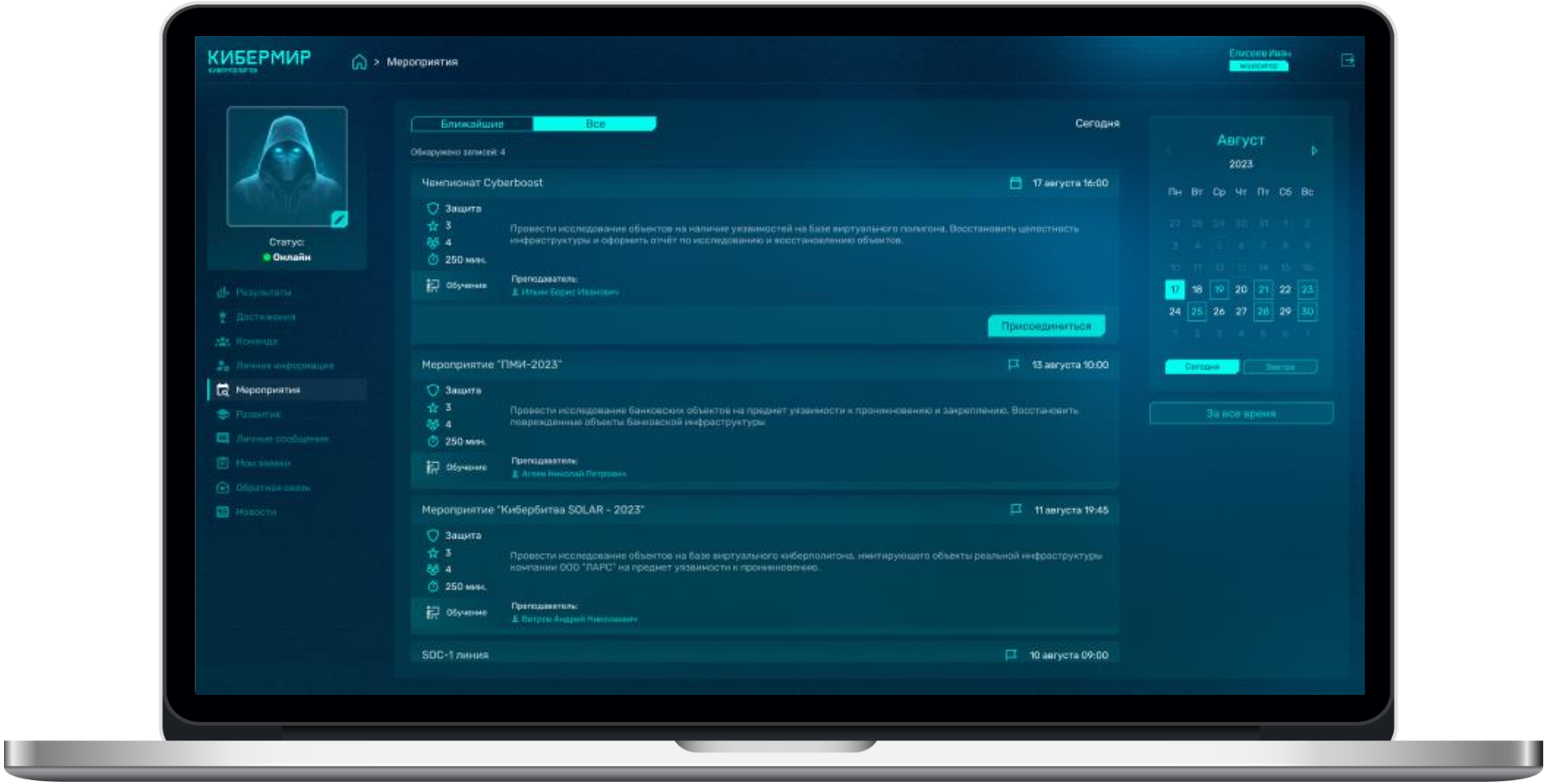
Участники

Пользователь 1	Пользователь N	Пользователь 1	Пользователь N

Ростелеком
Солар

Интерфейс платформы Solar CyberMir

Личный кабинет участника с информацией о пройденных и запланированных киберучениях

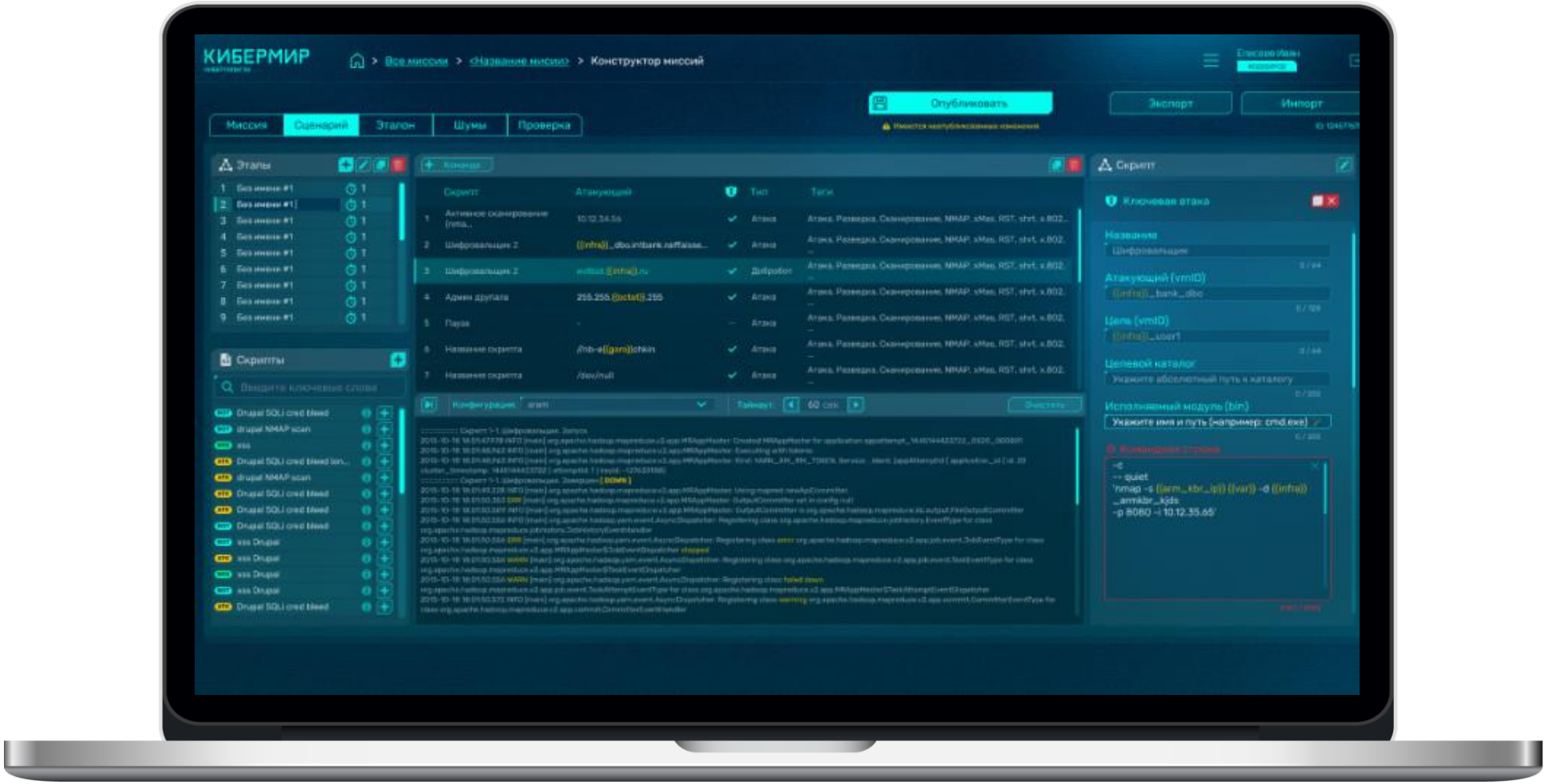


Оценка результатов киберучений

Автоматическая оценка отчета участника с возможностью ручной корректировки тренером

Конструктор сценариев

Создание сценариев атак с помощью визуального конструктора

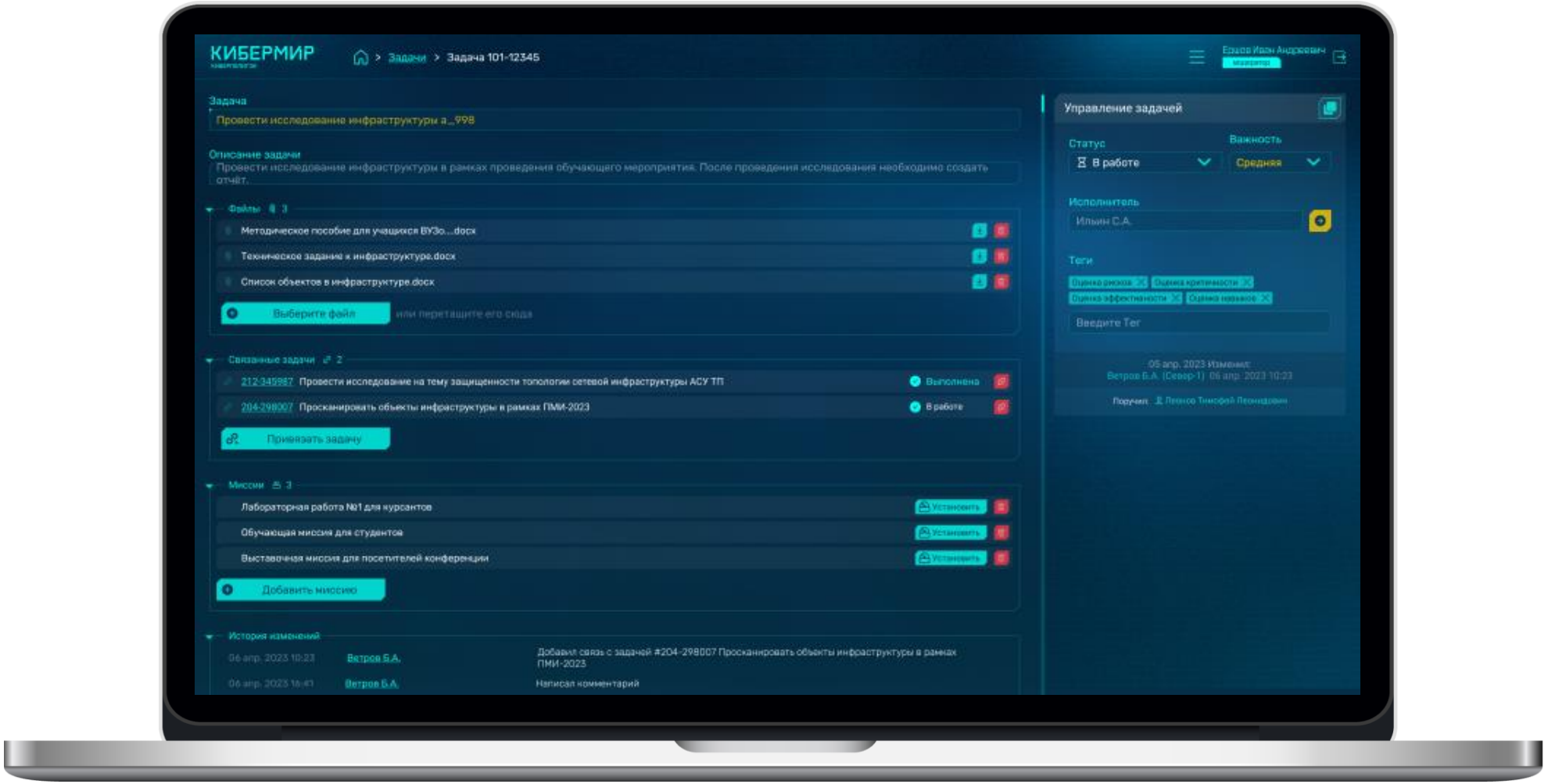


Визуализация прохождения атаки

Визуализация этапов прохождения учебной атаки на топологии сети виртуальных инфраструктур

Таск-трекер для назначения задач

Таск-трекер с возможностью распределения задач по сотрудникам службы ИБ



ПОСТРОЕНИЕ КИБЕРПОЛИГОНОВ

Сценарии использования киберполигонов

РАЗВИТИЕ КОМАНД

Регулярная проверка компетенций сотрудников службы ИБ, повышение практических навыков команды и выстраивание процесса непрерывного обучения на базе киберполигона

ПРОВЕРКА РЕШЕНИЙ

Подбор и тестирование СЗИ в различных конфигурациях и с различными сценариями с учетом совместимости с существующими системами заказчика

АНАЛИЗ ЗАЩИЩЕННОСТИ

Проведение регулярного анализа защищенности различных СЗИ перед их внедрением и обеспечение соответствия требованиям регуляторов

ДЛЯ КОГО АКТУАЛЬНО

Большой штат сотрудников службы ИБ

Наличие Red, Blue и Purple Team

Необходимость проведения регулярных киберучений

Необходимость тестирования нового оборудования

Необходимость проведения анализа защищенности для нового ПО

Построение киберполигонов

ПОСТРОЕНИЕ КИБЕРПОЛИГОНОВ НА БАЗЕ ИНФРАСТРУКТУРЫ ЗАКАЗЧИКА

- Разработка концепции
- Проектирование
- Поставка и внедрение «железа»
- Поставка и разворачивание лицензии Solar CyberMir с набором учебных атак
- Разработка уникальных сценариев и их регулярное обновление
- Техническая поддержка

ВАРИАНТЫ КОНФИГУРАЦИИ

Создание цифровых двойников с возможностью полного копирования ИБ-инфраструктуры

Использование типовых отраслевых инфраструктур, максимально приближенных к реальным

КИБЕРПОЛИГОН

Это виртуализированная ИТ-инфраструктура для практической тренировки специалистов и апробации технологических решений для организаций из разных отраслей

В ОСНОВЕ КИБЕРПОЛИГОНА ПРОГРАММНАЯ ПЛАТФОРМА SOLAR CYBERMIR

КИБЕРУЧЕНИЯ

Цели проведения киберучений

ОЦЕНКА

Проверка навыков сотрудников службы ИБ по выявлению и предотвращению последствий кибератак

ТРЕНИРОВКА

Повышение компетенций специалистов служб ИБ за счет практического применения навыков на киберполигоне

РАЗВИТИЕ

Подготовка рекомендаций и разработка программ развития сотрудников службы ИБ

ГЛАВНЫЙ РЕЗУЛЬТАТ КИБЕРУЧЕНИЙ

Слаженная работа службы ИБ, где каждый сотрудник понимает свои задачи и знает о необходимых действия в случае наступления инцидента информационной безопасности

Киберучения сегодня – это базовый инструмент для проверки уровня навыков службы ИБ и тренировки противодействия атакам злоумышленников

52%

компаний уже имеют опыт проведения киберучений*

75%

компаний планируют проведение киберучений в будущем*

87%

компаний считают, что киберучения нужно проводить минимум каждые полгода*

* По данным исследования ГК «Солар», октябрь 2023, выборка более 100 компаний

Типы киберучений

ПРАКТИЧЕСКИЕ КИБЕРУЧЕНИЯ

Это стандартные киберучения
на типовой учебной инфраструктуре
с готовыми сценариями.

ONE-DAY SOC

Проверка навыков по обнаружению и расследованию кибератак и рекомендации по развитию компетенций сотрудников

ONE-DAY RESPONSE

Проверка уровня подготовки команды к расследованию и противодействию кибератакам и рекомендации по развитию компетенций сотрудников

КАСТОМНЫЕ КИБЕРУЧЕНИЯ

Киберучения с возможностью изменения СЗИ, инфраструктуры и сценариев по требованиям заказчика. От одной команды участников до 40 команд.
Разные форматы тренировки, соревнования и т.д.

КОМАНДНО-ШТАБНЫЕ ТРЕНИРОВКИ

Проверка процессов реагирования на инциденты ИБ выстроенным у Заказчика на примере кейсов

Участвуют сотрудники ИБ-, ИТ- и смежных подразделений согласно существующим регламентам реагирования Заказчика

КИБЕРУЧЕНИЯ И ОБУЧЕНИЕ

Интеграция киберучений в программы развития специалистов, например:

+ Киберучения ONE-DAY SOC – оценка исходного уровня компетенций

+ киберинтенсив – развитие теоретических знаний и практических навыков

+ Киберучения ONE-DAY SOC – оценка прогресса

Наш опыт проведения киберучений

300+

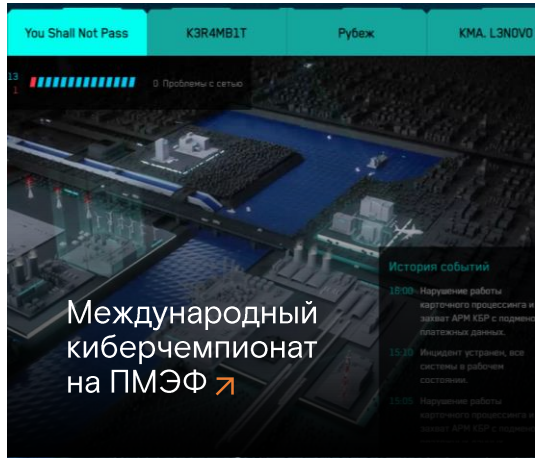
ПРОВЕДЕННЫХ КИБЕРУЧЕНИЙ

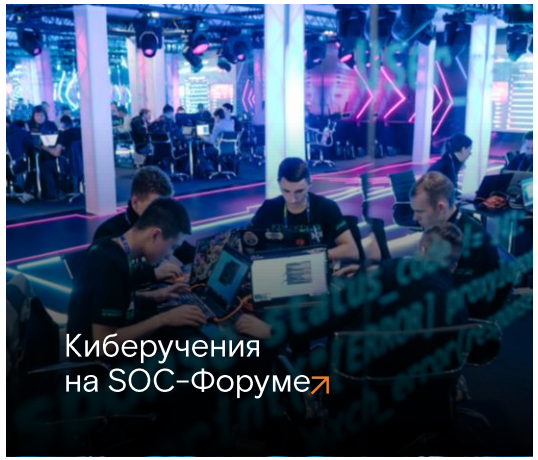
5000+

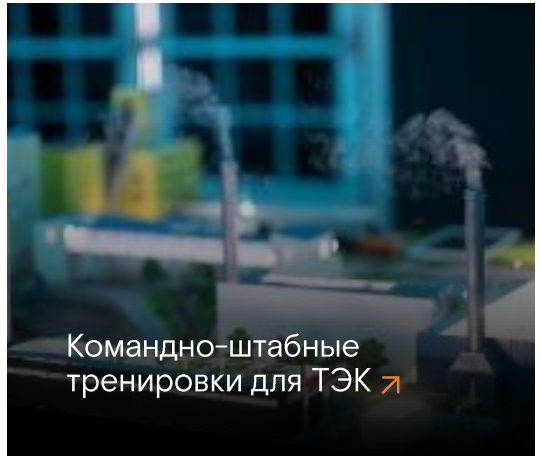
УЧАСТНИКОВ КИБЕРУЧЕНИЙ

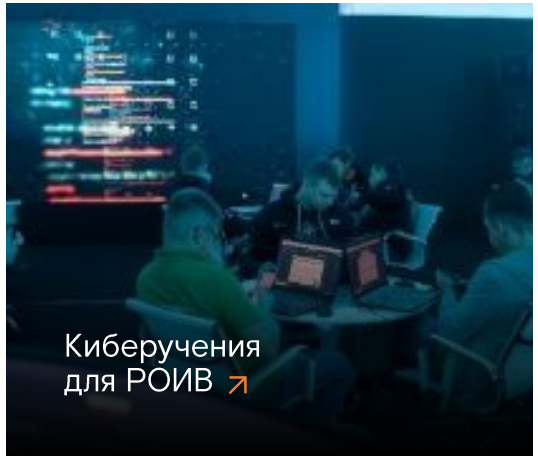
365 ДНЕЙ

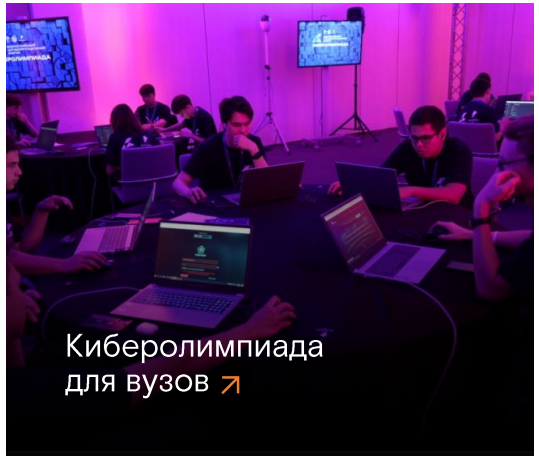
ДОСТУПНОСТИ ПЛАТФОРМЫ В ОБЛАКЕ











Практические киберучения

УЛУЧШЕНИЕ НАВЫКОВ ЗАЩИТЫ ОТ КИБЕРУГРОЗ

Проверка знаний и отработка навыков противодействия кибератакам с помощью прохождения сценариев киберучений с последующим их разбором тренером

ЦЕЛИ ПРОВЕДЕНИЯ

Увеличение скорости реакции группы реагирования для минимизации ущерба от киберинцидентов

Проверка и развитие компетенций специалистов для предотвращения киберинцидентов

Изучение тактик и техник злоумышленников на киберполигоне

РЕЗУЛЬТАТЫ

- Оценка практических навыков специалистов
- Рекомендации по развитию компетенций для команды участников или для конкретного специалиста

ДЛЯ КОГО

- **ИТ-специалисты** (в том числе инженеры АСУ ТП)
- **ИБ-специалисты**

Рекомендуемая регулярность проведения:

- каждые 3 месяца

Практические киберучения проводятся на платформе Solar CyberMir

SOLAR

Образование

MOSCOW 2023

Команда киберзащиты: роли и навыки для отражения кибератак

SOLAR

КОМАНДА КИБЕРЗАЩИТЫ обеспечивает обработку инцидента в моменте:

- Обнаружение
- Реагирование
  - Анализ
  - Сдерживание
  - Уничтожение
  - Восстановление

(подготовка и работа после инцидента – отдельно)

РОЛИ ДЛЯ ВЫПОЛНЕНИЯ

- Инженеры мониторинга инцидентов
- Эксперты по анализу артефактов и ВПО
- Администраторы СЗИ
- Доменные администраторы
- Сетевые администраторы
- Инженеры систем резервного копирования

НАВЫКИ

- Экспертиза в SIEM
  - настройка
  - операционная работа
- Анализ инцидентов (артефактов) по MITRE ATT&CK
- Администрирование СЗИ
  - NGFW, IPS, WAF, EDR…
- Администрирование безопасности OS и сети
  - Windows / Linux
  - сетевая безопасность
- Аудит и анализ
  - сетевого траффика
  - Windows / Linux
  - анализ кода
- Восстановление
  - работа с Back-up системами
  - Windows / Linux
  - приложений
- Коммуникации в команде

Для команды киберзащиты - Киберинтенсив

SOLAR

Модули (160 часов):

- Основы информационной безопасности
- Безопасность ОС Linux & Windows
- Сетевая безопасность
- Управление угрозами информационной безопасности
- Управление инцидентами информационной безопасности
- Межсетевые экраны нового поколения
- Системы расширенного обнаружения и устранения угроз
- Работа с Honeypot
- Компьютерная криминалистика
- OWASP Top 10
- Системы предотвращения утечек
- Социальная инженерия
- Разведка по открытым источникам
- Построение безопасности IT-архитектуры
- Безопасность Active Directory
- Администрирование и безопасность протокола LDAP

Для команд исследователей уязвимостей

SOLAR

Исследование уязвимостей – основы (120 часов)

- Курс 1 - Анализ защищенности информационных систем- разведка периметра
- Курс 2 - Активное тестирование безопасности информационных систем
- Курс 3 - Продвинутый анализ защищенности web-приложений
- Курс 4 - Анализ защищенности сетей Windows
- Курс 5 - Анализ защищенности инфраструктуры

Для команд исследователей уязвимостей

SOLAR

Этичный хакинг – продвинутый (200 часов)

- Модуль 1. Введение в этичный хакинг
- Модуль 2. Сбор информации
- Модуль 3. Сканирование сети
- Модуль 4. Анализ уязвимостей
- Модуль 5. Хакинг системы
- Модуль 6. Трояны и другое вредоносное программное обеспечение
- Модуль 7. Снифферы
- Модуль 8. Социальная инженерия
- Модуль 9. Отказ в обслуживании
- Модуль 10. Перехват сеанса
- Модуль 11. Криптография и стеганография
- Модуль 12. Обход систем обнаружения вторжений, фаерволлов и систем-ловушек
- Модуль 13. Хакинг веб-серверов
- Модуль 14. Хакинг веб-приложений
- Модуль 15. SQL инъекции
- Модуль 16. Киберучения
- [extra] Модуль 17. Хакинг беспроводных сетей
- [extra] Модуль 18. Хакинг мобильных платформ
- [extra] Модуль 19. Хакинг интернета вещей
- [extra] Модуль 20. Облачные вычисления

SOLAR

+7 (499) 755-07-70
cybermir@rt-solar.ru

Central office.
125009, Moscow, Nikitsiy
lane, 7c1