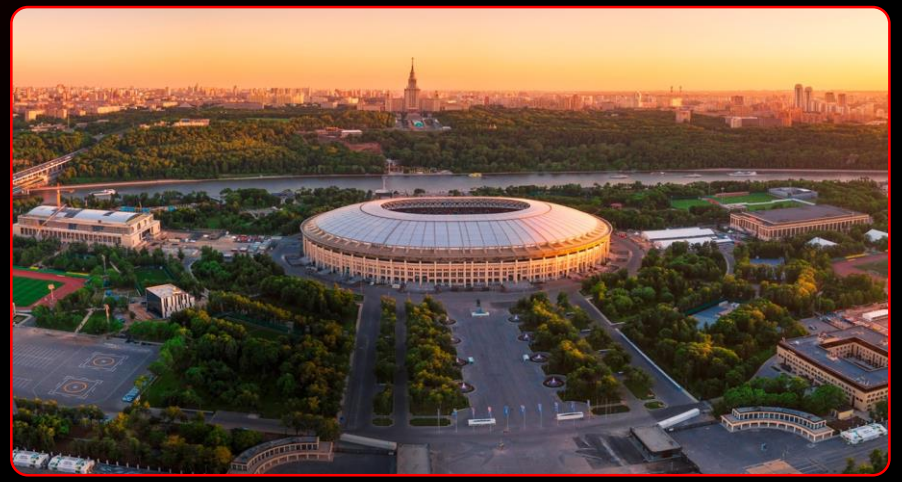
Елена Молчанова
бизнес-лидер киберполигона Standoff

Киберполигон:

Как держать в форме сотрудников службы ИБ

01

Люди, которые в форме

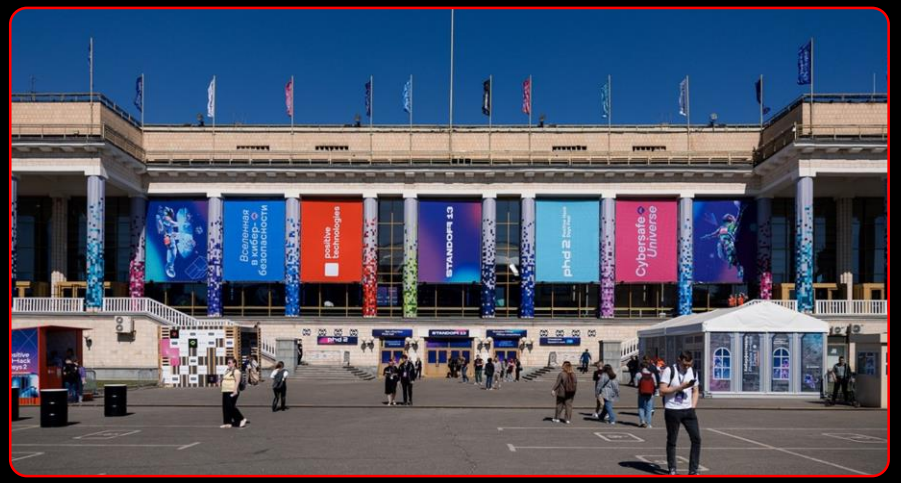


Май 2024, Москва, «Лужники»:

Кибербитва Standoff,

в которой ИБ-команды крупнейших компаний

успешно противостояли сильнейшим командам хакеров



133
атаки за 3 дня

45
успешных расследований

66
атомарных инцидентов

112
инцидентов предотвращено

100%
прошедших атак расследовано

24 минуты
среднее время реагирования

31 минуты
среднее время расследования

positive technologies

Свидетельство

№

подтверждает что

прошел(прошла) киберучения по предупреждению, реагированию и ликвидации последствий компьютерных атак

Генеральный директор
Positive Technologies

Денис Баранов

Выдан:

План | Программа | Технические требования | Преподаватели | Контакты

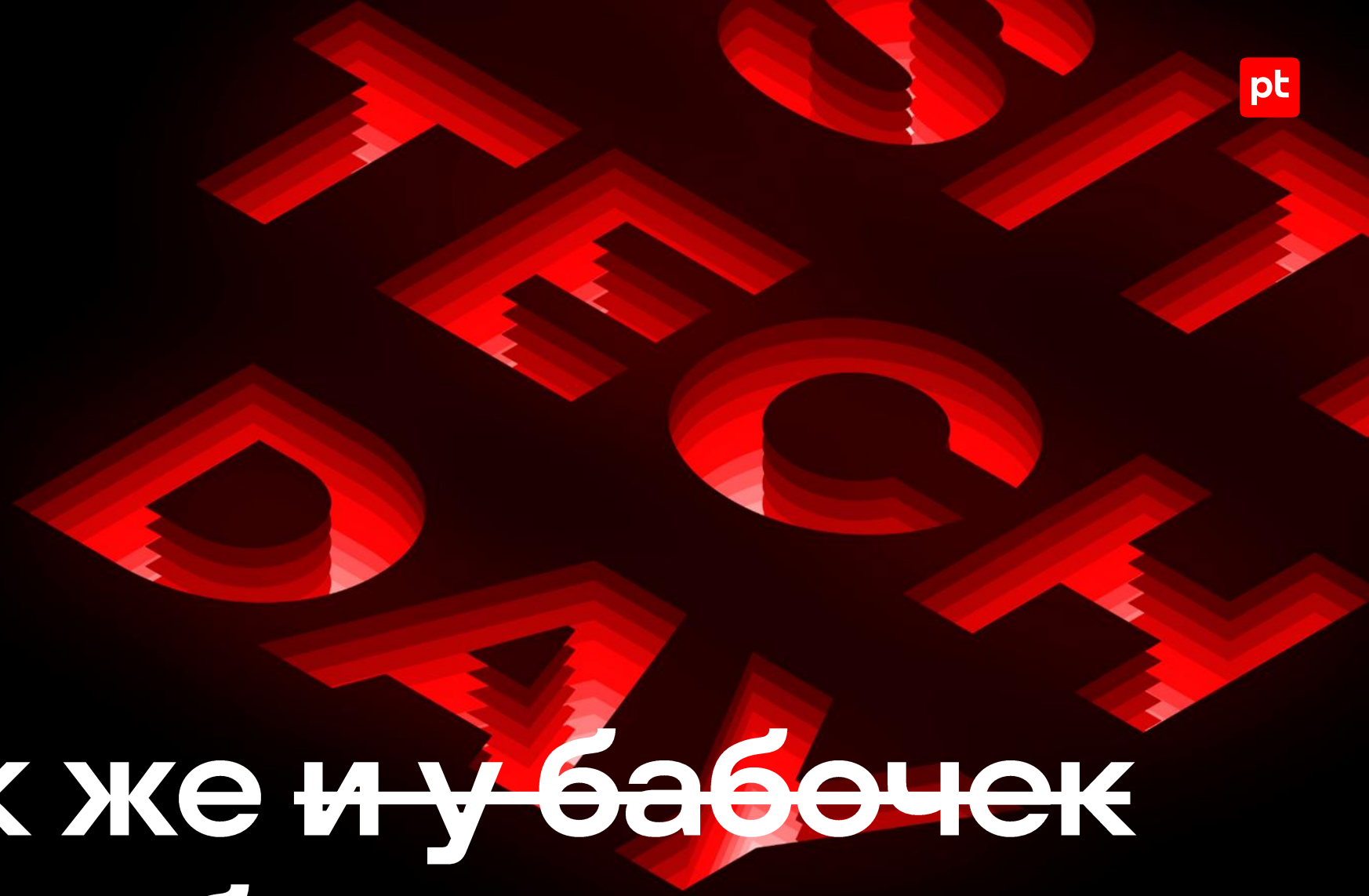
01

План обучения

12.07	Установочная встреча
13.07	Вход на платформу
13.07-17.07	Входное тестирование
18.07	Встреча по результатам тестирования
19.07-01.08	PT-START
02.08	Встреча по результатам PT-START и началу новых модулей
02.08-17.08	PT-PROFF
18.08	Встреча по результатам модуля
21.08-29.08	PT-PRODUCT
30.08	Подготовка к киберучениям на платформе Standoff
31.08-06.09	Мониторинг инфраструктуры. Разбор типовых инцидентов ИБ
07.09	Встреча по результатам обучения и объяснение дальнейших шагов
08.09	Доступ к платформе Standoff 365
08.09-21.09	Киберполигон Standoff
22.09	Встреча по результатам обучения

Правила нормализации, теория.

02



Вот так же ~~и у бабочек~~ и в кибербезе

Разные задачи для ИБ-команд разных уровней зрелости и их решение на полигоне standoff

Начальный уровень: теория и compliance	Квалифицированные команды с недостатком практики	Развитые команды – справляются со стандартными атаками	«Звёздные» команды
Показать, как работают злоумышленники	Научить мониторингу и расследованию инцидентов	Развить «насмотренность»	Показать самые сложные тактики и техники атакующих
Научить работать с ИБ-продуктами	Оптимально настроить СЗИ	Растить и развивать команду	
ОБУЧЕНИЕ	**ТРЕНАЖЁР**	**ОНЛАЙН-ПОЛИГОН**	**КИБЕРБИТВА**

Обучение:

теория + практика + вендоронейтральность

Входное тестирование

PT-START:

Выравнивание уровня членов группы

Асинхронный формат
Библиотека на 63 часа

PT-PROFF:

Курс по мониторингу ИБ

Асинхронный формат
+ преподаватель 96 часов

Выходное тестирование

Тренажёр «Мёртвый город»

Дополнительная платная опция 2 недели

Курс «Мониторинг ИБ»

PT-START

ОС семейства Windows
Windows Server & Domain Services & Active Directory Management, администрирование Windows, служба каталогов Active Directory, AAA в Windows, средства мониторинга Windows, инфраструктурные сервисы в домене, обмен данными в домене, основные протоколы в Windows-инфраструктуре

ОС семейства Linux
Основы Linux, администрирование Linux, сервисы в Linux, безопасность Linuxсерверов, работа с файловой системой Linux

Основы Web
Введение в Web технологии, архитектура WEB, основные атаки и паттерны, Web Application Firewall

Основы сетей и сетевых технологий
Введение в сетевые технологии, модель OSI. Канальный уровень -L2, модель OSI. Сетевой уровень -L3, модель OSI. Транспортный уровень -L4, безопасность локальной сети, протоколы верхних уровней

PT-PROFF

Популярные атаки и способы проникновения в инфраструктуру
Безопасность корп. инфраструктуры, OSINT, соц. инженерия, Сканирование сети, SSH Port forwarding/ SSH Tunneling. Проксирование трафика. Проникновение за периметр. OpenVPN L3, L2 Tunneling. ВПО в корпоративной среде. MITM. Bruteforce. Инструменты скрытия трафика от систем защиты

СЗИ. Компонентная база SOC
SOC. Firewalls (Pfsense & iptables). NGFW и IDS (SNORT and Surricata). Proxi Servers (Squid) и Reverse Proxy Servers (Nginx). Endpoint Security (AV), Mail Security GW, HoneyPots. Network traffic anomaly analysers). MS AD и Group Policy Security Settings. Sysmon. SIEM-системы включая Opensource (ELK, Wazuh)

Программные СЗИ Positive Technologies
MaxPatrol SIEM. PT NAD. PT MultiScanner и PT Sandbox. PT AF

Мониторинг инфраструктуры. Разбор типовых инцидентов
Мониторинг инцидентов ИБ. Сбор и анализ данных. Killchain и ATT&CK. Тактика реагирования. Типовые инциденты. Практические примеры использования SIEM, NAD, AF в реальной работе.

Есть специальный вариант для ИБ-специалистов РОИВ

Разные задачи для ИБ-команд разных уровней зрелости и их решение на полигоне standoff

Начальный уровень: теория и compliance	Квалифицированные команды с недостатком практики	Развитые команды – справляются со стандартными атаками	«Звёздные» команды
Показать, как работают злоумышленники	Научить мониторингу и расследованию инцидентов	Развить «насмотренность»	Показать самые сложные тактики и техники атакующих
Научить работать с ИБ-продуктами	Оптимально настроить СЗИ	Растить и развивать команду	
ОБУЧЕНИЕ	**ТРЕНАЖЁР**	**ОНЛАЙН-ПОЛИГОН**	**КИБЕРБИТВА**

Практикум «мертвый город»:

создан на базе артефактов кибербитвы standoff

1 **Аудитория:**

- ИБ-специалисты базового и начального уровня

2 **Цели:**

- Расследование инцидентов
- Знакомство с СЗИ

3 **Подход:**

- Артефакты и логи из живых атак, полученные во время кибербитвы Standoff (загружены в СЗИ)
- Разработаны специальные задания, которые надо выполнять с помощью этих СЗИ

3 **Продукты для мониторинга (СЗИ):**

- PT SIEM
- PT Sandbox
- PT NAD
- PT AF

4 **Формат и пререквизиты:**

- Онлайн, группы до 10 человек
- Доступ к онлайн-курсам по продуктам

5 **Продолжительность:**

- 2-4 недели

Задания на основе > 15 реальных атак

01. Файл wtf.exe

Задание 1.1	Задание 1.2	Задание 1.3
10	20	40

02. Подмена контента для видео-банера

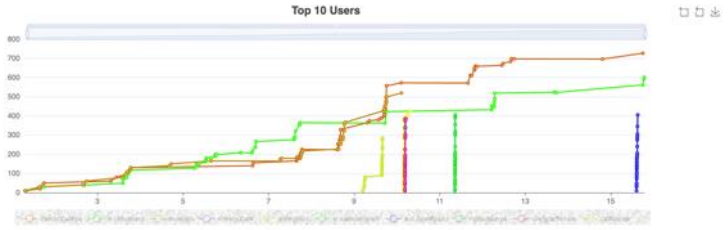
Задание 2.1	Задание 2.2	Задание 2.3	Задание 2.4
10	20	10	10

03. Поиск "плохого" файла

Задание 3.1	Задание 3.2	Задание 3.3	Задание 3.4
10	20	10	30

Задание 3.5	Задание 3.6	Задание 3.7
10	10	10

Статистика по каждому заданию и практикуму в целом. Обнаружение «списывания»



Challenge 10 Solves

Задание 5.3

5

> В УК Сити произошла утечка конфиденциальных данных. Нарушителям удалось загрузить шпионское ПО Cobalt Strike на один из узлов инфраструктуры, на котором было зафиксировано наибольшее количество таких событий.
>
> Предстоит определить детали событий, которые происходили в период с 22 ноября 17:00 по 23 ноября 17:00.

IP-адрес атакующего хоста.

Flag | Submit

Challenge 10 Solves

Задание 2.4

10

> Руководитель отдела информационной безопасности в бешенстве. Буквально несколько часов назад был совершен взлом видео-баннера в городе и продемонстрирован чувствительный для граждан видео ряд. В этот момент он докладывал об успешном достижении показателей информационной безопасности. Время прошло, скандалы утихли. Вам необходимо восстановить последовательность действий атакующего.
>
> По оперативным данным атака проходила с 2022-11-22 12:10:00 по 2022-11-22 12:20:00 \ UTC: 09:10:00 - 09:20:00

Название загружаемого атакующими видео файла

Flag | Submit

Разные задачи для ИБ-команд разных уровней зрелости и их решение на полигоне standoff

Начальный уровень: теория и compliance	Квалифицированные команды с недостатком практики	Развитые команды – справляются со стандартными атаками	«Звёздные» команды
Показать, как работают злоумышленники	Научить мониторингу и расследованию инцидентов	Развить «насмотренность»	Показать самые сложные тактики и техники атакующих
Научить работать с ИБ-продуктами	Оптимально настроить СЗИ	Растить и развивать команду	
ОБУЧЕНИЕ	ТРЕНАЖЁР	ОНЛАЙН-ПОЛИГОН	КИБЕРБИТВА

Базовая механика киберполигона

Атаки

Высококвалифицированные исследователи из сообщества Standoff

Регулируемые атаки, покрывающие ~ 70% матрицы MITRE

Red teams Заказчика или его подрядчиков

Веб-портал атакующего

Веб-портал защитника

СЗИ

Мониторинг
Расследование
Реагирование

ИБ-команды Заказчиков (прежде всего SOC)

Возможно подключение дочерних структур и ключевых подрядчиков

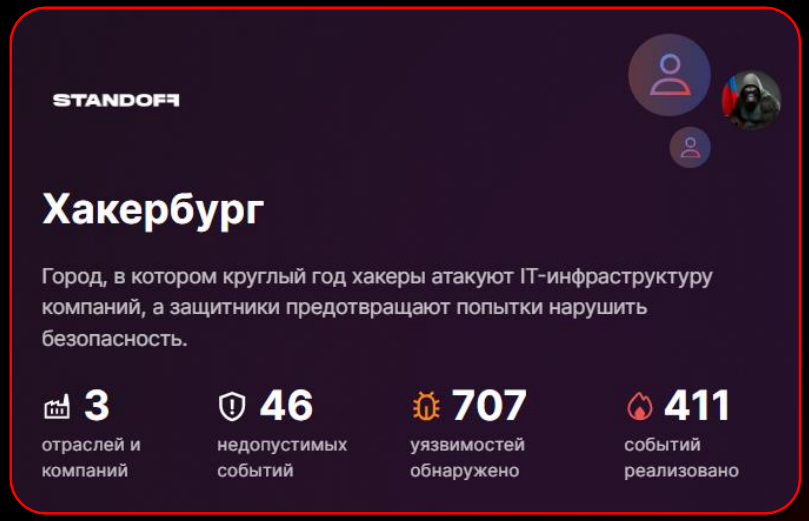
Рекомендуется добавлять представителей ИТ и DevSecOps

Два главных формата киберполигона

Кибербитва

- 3-5 дней
- Экстремальная «прокачка» ИБ-команды
- Максимальный «красный» трафик
- Визуализация влияния ИБ на реальную жизнь

Онлайн-полигон



- Доступ на 1 год
- Планомерное развитие ИБ-команды
- Сложные и долгие (persistent) атаки
- Кастомизация инфраструктуры

Онлайн-полигон Standoff

Виртуальная ИТ-инфраструктура компаний, доступная онлайн в режиме 24/7, для регулярной отработки специалистами по ИБ навыков выявления, расследования и отражения атак.

1. **Цели и задачи**
2. Онбординг
3. Назначение сервис-менеджера
4. Регулируемые атаки
5. Результаты
6. Разбор с ментором
7. Список рекомендаций
8. Повторная регулируемая атака
9. Анализ динамики
10. Командная кибербитва

- Поддержка ментора-эксперта на протяжении всего периода
- Доступ к лабораторным заданиям в личном кабинете участника и его персональная карта MITRE ATT&CK
- Регулярное добавление новых сценариев атак и обновление инфраструктуры

Что используют хакеры

Пара примеров

3 Назначение сервис-менеджера

- Зафиксирует все ваши цели
- Проведет экспресс-тестирование для оценки текущих навыков
- Подберет оптимальное расписание тренировок и обучения под ваш запрос
- Подберет уровень сложности атак в зависимости от уровня текущих навыков (продолжительность атак от 1 часа до 1 недели)

Что используют хакеры

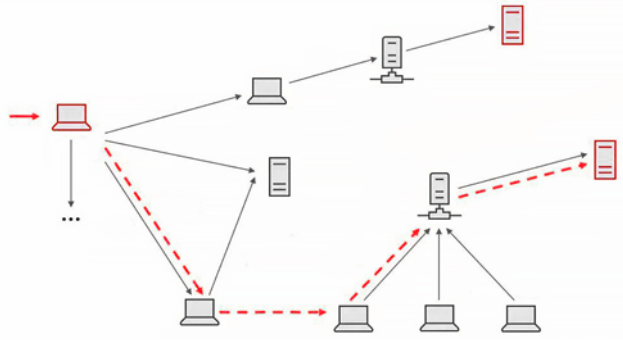
Пара примеров

4

Регулируемые атаки

Проведение регулируемых атак на онлайн-полигоне Standoff

Ваша сотрудники в комфортном темпе смогут подготовится к разнообразным атакам, продолжительностью от 1 часа до 1 недели в зависимости от уровня сложности



- Harvesting and infiltration, Charming Kitten APT
- MadMxShell, malvertising campaign
- Goldoo, Linux botnet
- GuptiMiner, Kimsuky APT
- Loaders and exfiltration, ToddyCat APT

Что используют хакеры

Пара примеров

5

Результаты

Мы автоматически проверяем отчеты и показываем процент раскрытия атаки, а также формируем индивидуальную карту MITRE ATT&CK.

Участники видят свои результаты в личном кабинете

Участник	Пройдено учебных модулей	% раскрытия атаки	MITRE ATT&CK	Рекомендации
Участник 1	1 из 3	25	20	link
Участник 2	3 из 5	28	34	link
Участник 3	1 из 4	32	37	link
Участник 4	4 из 4	39	58	link
Участник 5	1 из 5	44	47	link

Что используют хакеры

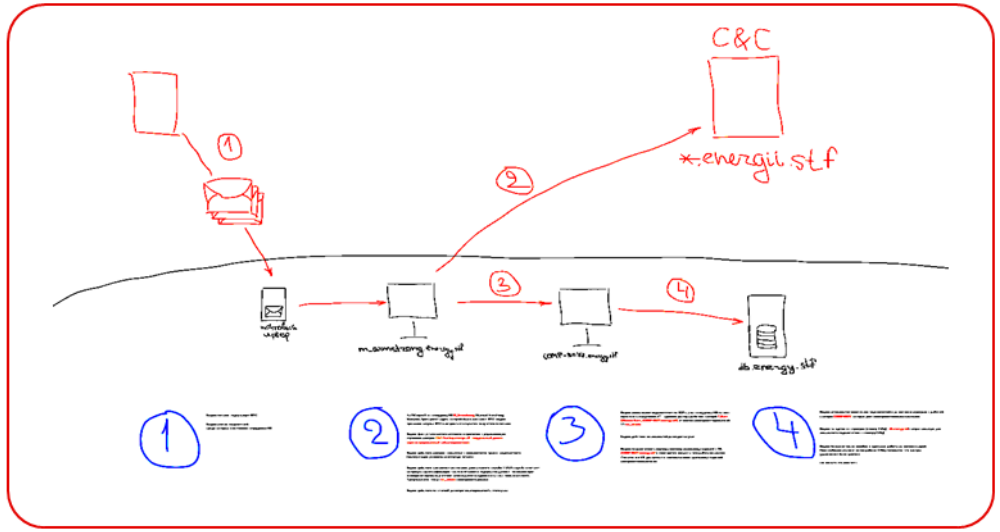
Пара примеров

6

Разбор с ментором

Проведение воркшопа или мастер-класса с разбором атак

Вы получите обратную связь по слабым местам, какие техники и тактики не удалось обнаружить участникам



Разные задачи для ИБ-команд разных уровней зрелости и их решение на полигоне standoff

Начальный уровень: теория и compliance	Квалифицированные команды с недостатком практики	Развитые команды – справляются со стандартными атаками	«Звёздные» команды
Показать, как работают злоумышленники	Научить мониторингу и расследованию инцидентов	Развить «насмотренность»	Показать самые сложные тактики и техники атакующих
Научить работать с ИБ-продуктами	Оптимально настроить СЗИ	Растить и развивать команду	
ОБУЧЕНИЕ	ТРЕНАЖЁР	ОНЛАЙН-ПОЛИГОН	КИБЕРБИТВА

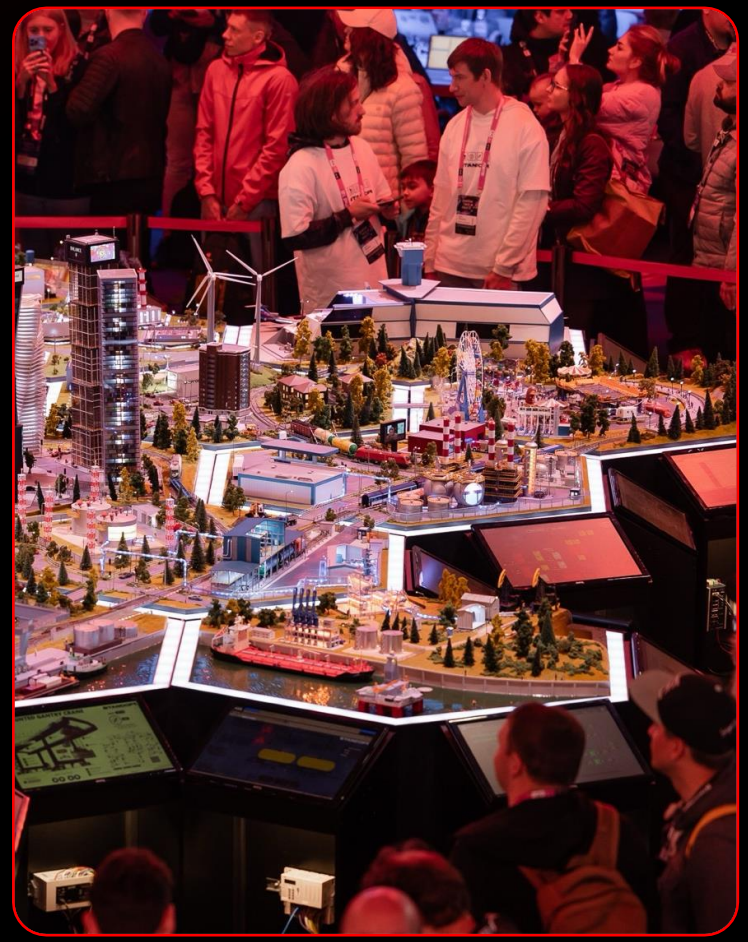
Онлайн-полигон Standoff

Международные киберучения,
где команды защитников
и хакеров могут проверить
свои навыки

Или – приватная битва

Standoff 13:

Те, кто бьют рекорды



8	отраслей
11	«синих» команд (мониторинг или реагирование; онлайн или на площадке)
26	сильнейших команд атакующих
189	уникальных событий (77 реализовано)
419	атак
182	успешных расследования
848	инцидентов обнаружено

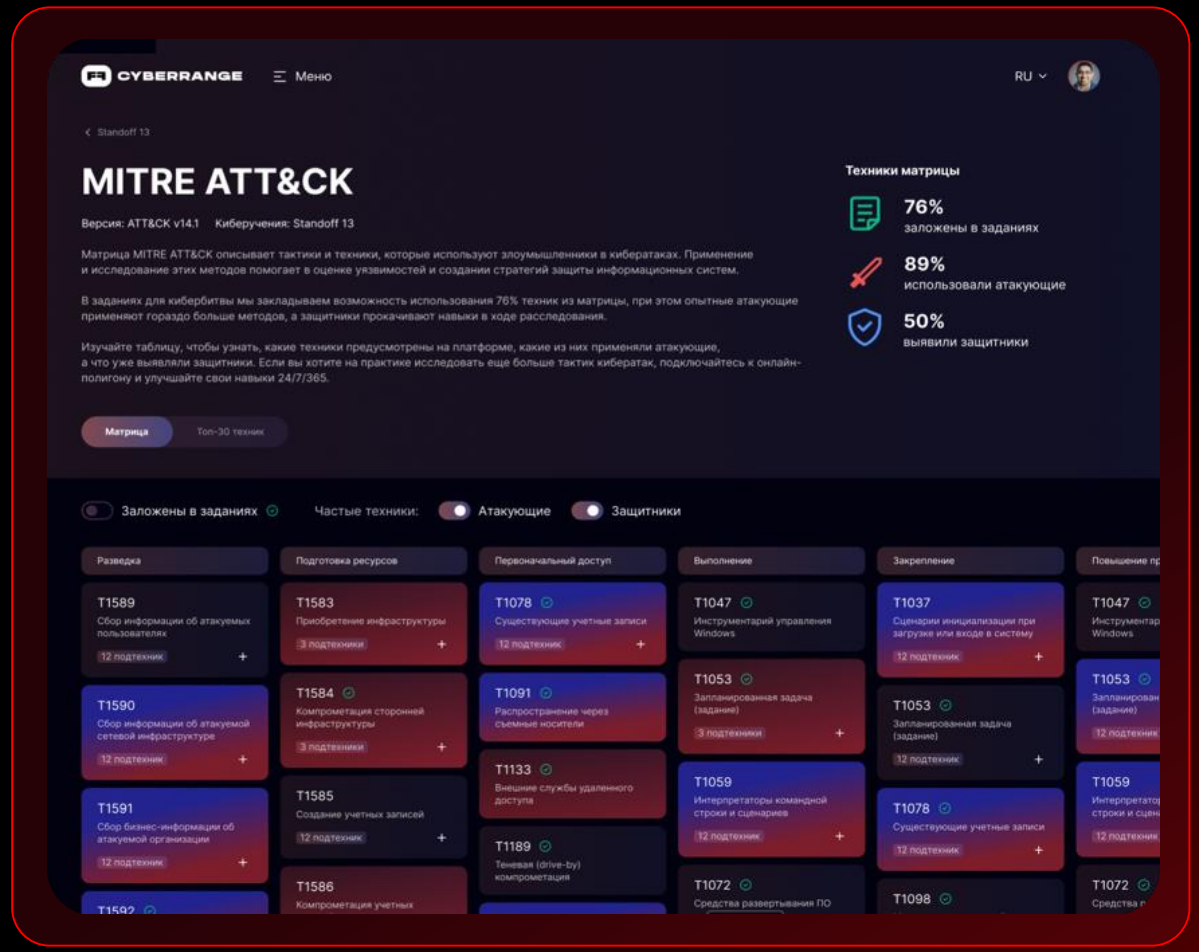
Карта MITRE ATT&CK

Индивидуальная карта MITRE ATT&CK

В личном кабинете каждого участника отображается число освоенных техник

Конкурс

1. QR-код
2. Опрос
3. Брендированная MITRE ATT&CK для первых 30 заполнивших



Обобщенная карта MITRE ATT&CK для Standoff 13

Спасибо!