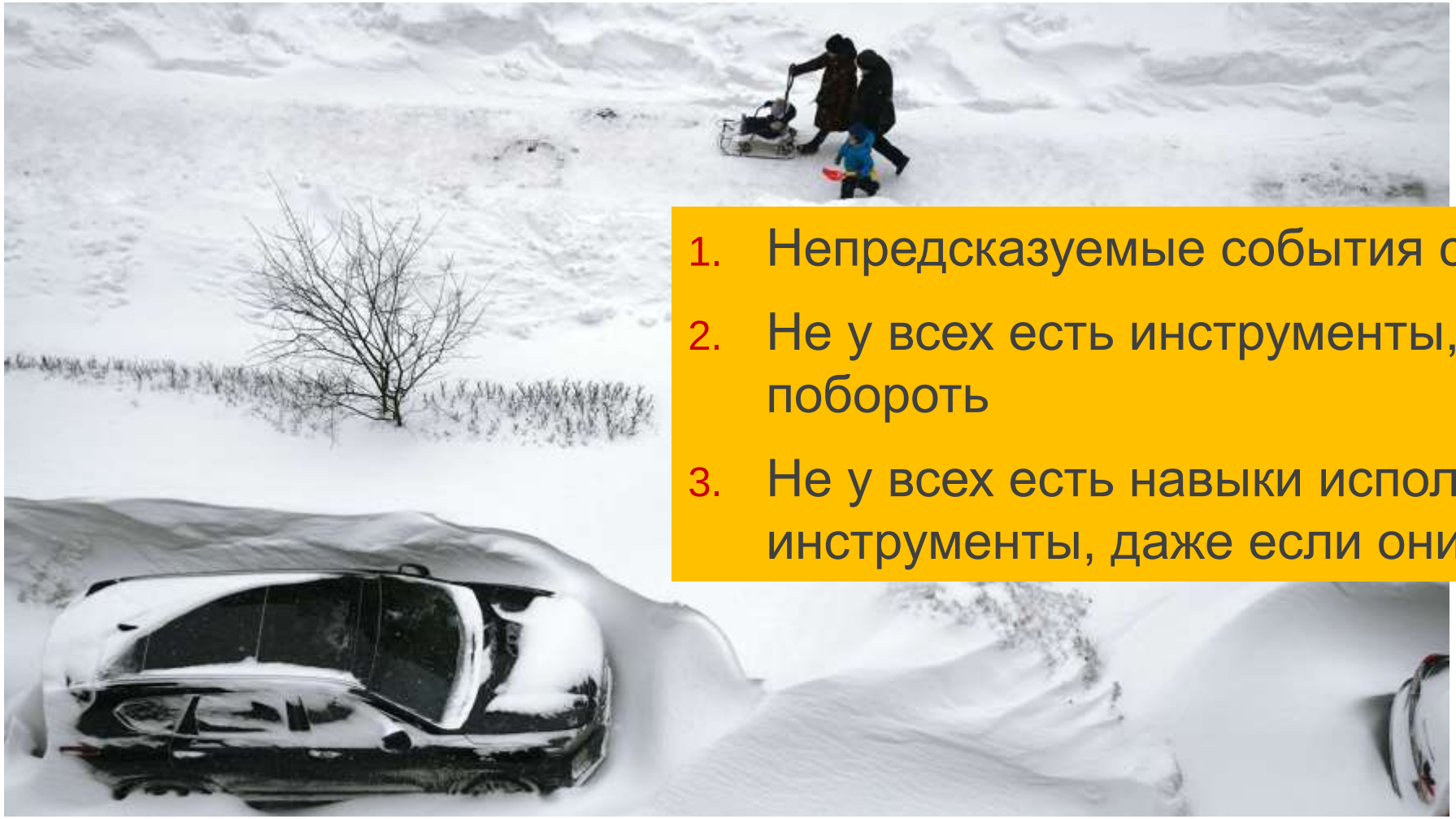
POSITIVE TECHNOLOGIES

Опыт The Standoff

Киберполигон как единственный высокоэффективный инструмент моделирования угроз и оценки реального уровня защищенности технологий

ptsecurity.com

Зачем что-то моделировать?



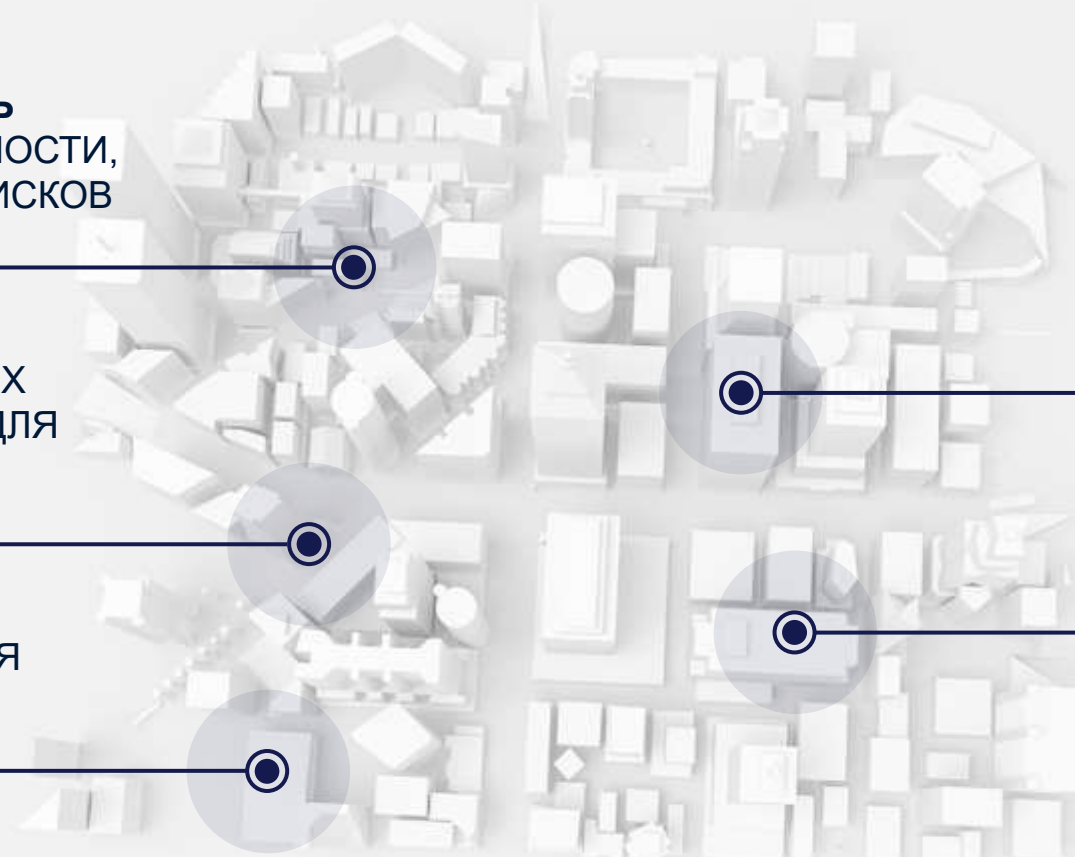
1. Непредсказуемые события случаются
2. Не у всех есть инструменты, чтобы их побороть
3. Не у всех есть навыки использовать инструменты, даже если они есть

Проблемы кибербезопасности промышленных компаний

«ПРАКТИЧЕСКАЯ» НЕЗРЕЛОСТЬ ИНФОРМАЦИОННОЙ БЕЗОПАСНОСТИ, ОТСУТСТВИЕ ВЕРИФИКАЦИИ РИСКОВ

СЛОЖНОСТЬ РАЗРАБОТКИ И ВНЕДРЕНИЯ УНИВЕРСАЛЬНЫХ СТАНДАРТОВ БЕЗОПАСНОСТИ ДЛЯ ВСЕХ ИТ-ПРОЕКТОВ

ОТСУТСТВИЕ ИНСТРУМЕНТОВ БЫСТРОЙ ПРОВЕРКИ УГРОЗ ДЛЯ СЕРВИСОВ И ПРИЛОЖЕНИЙ



«ЧЕЛОВЕЧЕСКИЙ ФАКТОР» — МНОГИЕ АТАКИ ПРОИСХОДЯТ ИЗ-ЗА НЕГРАМОТНОСТИ СОТРУДНИКОВ

ОГРОМНАЯ СТОИМОСТЬ УЩЕРБА И РИСК КАТАСТРОФ

ПРИВЫЧКА РАССМАТРИВАТЬ ФИЗИЧЕСКИЕ УГРОЗЫ, А НЕ КИБЕРУГРОЗЫ

Примеры рисков

БЕЗОПАСНОСТЬ ТЕХНОЛОГИЧЕСКИХ ПРОЦЕССОВ

БЕЗОПАСНОСТЬ ПУБЛИЧНЫХ СЕРВИСОВ И РЕПУТАЦИЯ КОМПАНИИ

БЕЗОПАСНОСТЬ ФИНАНСОВЫХ СИСТЕМ (КРАЖА ДЕНЕГ)

16 февраля 2021 – США переживает энергетический кризис

Из-за аномальных морозов ветряные и солнечные электростанции перестали работать, что вызвало рост цен на электроэнергию и газ.

За последние 10 лет, штат Техас в США на 18% сократил выработку электроэнергии при помощи угля в пользу поддерживаемых государством ветряков, солнечных панелей, а также дешёвого природного газа.

В результате цены на газ и электроэнергию резко подскочили. Газ с $3 неделей ранее до $600 за 1 млн BTU (британская тепловая единица). Оптовые цены на электроэнергию выросли с $25 за мегаватт-час до $9000 за мегаватт-час

Ограничения обычных средств «моделирования»

Почему Киберполигон действительно важен и каким он должен быть

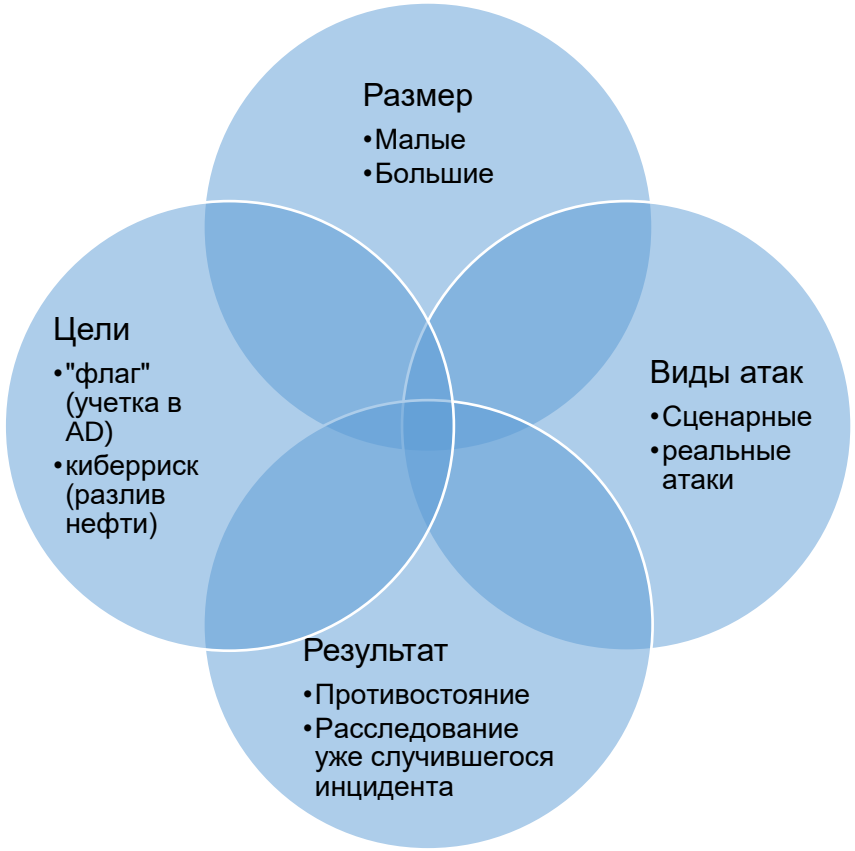
Pentest, RedTeam
Ограничено
временем и скоупом

Ограничение response
из-за влияния на живую
инфраструктуру

Невозможность
довести до конца
и реализовать
реальные бизнес-риски

Ограничение в сценариях
поведения атакующих.
**Одна команда —
одно поведение**

Отличие киберполигонов



«ОБЫЧНЫЙ ПОЛИГОН»

THE STANDOFF

Главные преимущества

- Максимально приближено к реальной жизни
  - Бизнес-риски и их верификация
- Настоящий и разнообразный хакерский трафик
- Экосистема мира ИБ

Зачем киберучения?

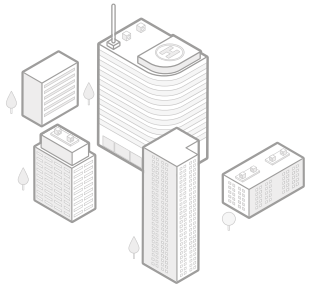
- **Вообще нет тестового сегмента**
  - Учим новых людей
  - Повышаем квалификацию существующих
- Как **реальная смоделированная инфра** позволяет защищаться от атак (what if)
- **Отработка взаимодействия** подразделений (ИБ, ИТ и технологи…)

Эволюция The Standoff

2011

CTF С ПРИЦЕЛОМ НА РЕАЛЬНОСТЬ

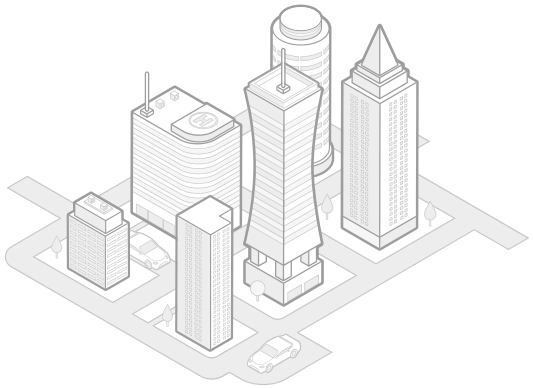
- Реальные IT системы
- Иностранные специалисты-участники
- Мгновенное признание в хакерской среде
- Уязвимости и вектора атак на базе консалтинговых работ PT



2015

ПЕРВЫЙ МАКЕТ РЕАЛЬНОГО ГОРОДА

- Формат противостояния — командам нападающих противостоят защитники
- Реальная инфраструктура, выполняющая реальные бизнес-задачи
- 10 команд хакеров и 5 защитников
- Появление мониторингового центра



2020

МАКЕТ РЕАЛЬНОГО ГОРОДА

- Реальная инфраструктура
- 30 команд хакеров и 6 защитников
- SOC центр «города F»
- 365 дней в году
- Международный охват

2021

The Standoff в 2020

- 29 команд атакующих со всего мира
- одновременно действующие 6(7) команд защитников
- 2 городских мониторинговых центра (SOC)

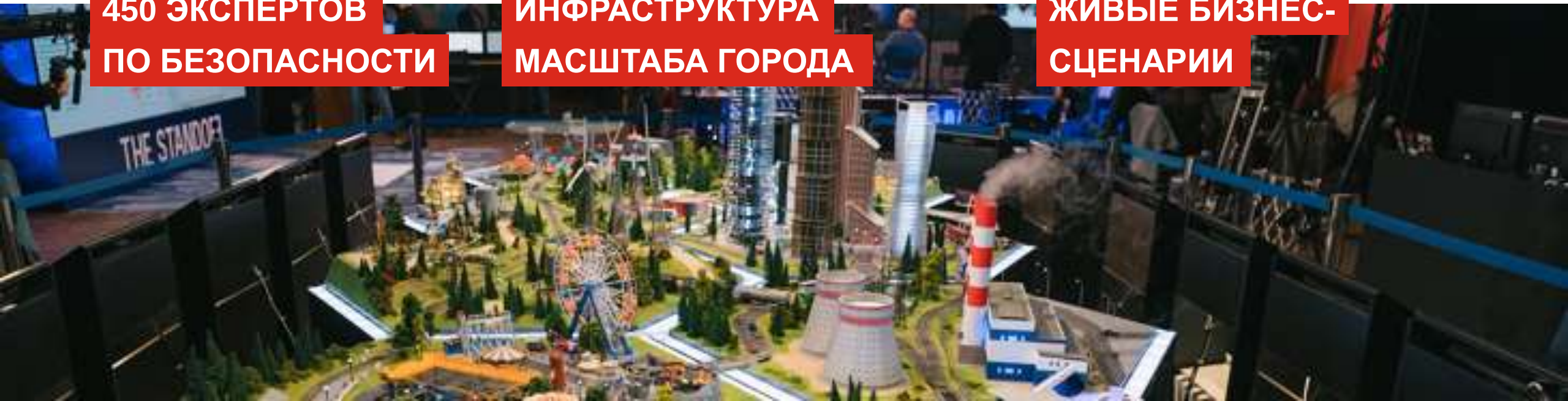
- 3.000+ виртуальных машин в инфраструктуре
- 1.500+ виртуальных пользователей, которые выполняют обычные для людей действия (включая открытие ссылок в письмах)
- 800.000 + звонков и сообщений в день
- 30.000+ электронных писем
- 400.000 + банковских транзакций

- Городская инфраструктура – парк развлечений, светофоры и трафик, информация о штрафах, продажа билетов, Нефтяная компания, химический завод, газораспределение, телерадиовещание, электроэнергетика: генерация и сбыт, аэропорт, железная дорога, морской порт, Банк, процессинг и ДБО, электронная коммерция

450 ЭКСПЕРТОВ ПО БЕЗОПАСНОСТИ

ИНФРАСТРУКТУРА МАСШТАБА ГОРОДА

ЖИВЫЕ БИЗНЕС-СЦЕНАРИИ



Оценка результатов

Примеры рисков

- Разглашение или утечка персональных данных клиентов
- Разглашение или утечка персональных данных сотрудников
- Нарушение работы процессингового центра
- Разглашение или утечка данных клиентов ДБО
- Мошеннические операции с банковскими картами
- Хищение денежных средств со счетов банка

Укрупненная схема 2020

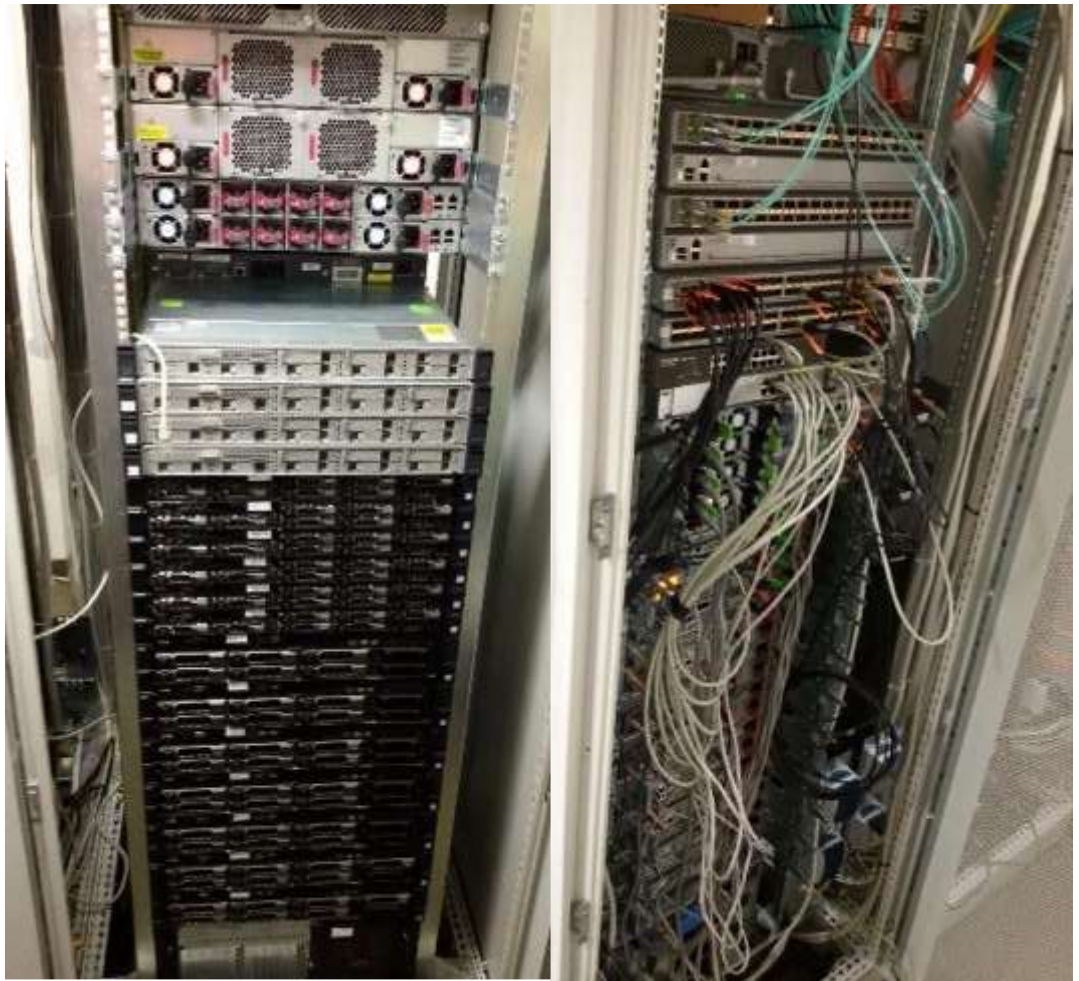
Инфраструктура The Standoff

2020

468 cores CPU →

7,5 TB RAM →

146 TB HDD →



2021

← **5372** cores vCPU

← **9,1** TB RAM

← **485** TB SDD/HDD

Возможности киберполигона

Максимальное соответствие жизненным условиям

Киберучения

- Максимально близко к реальной жизни
- Оттачивание процессов и регламентов
- Отработка playbook
- Тестирование средств защиты

Подключение к экосистеме

- Воссоздание типовых инфраструктур
- Подключение важных сервисов и бизнес процессов

КАКИМИ ОНИ ДОЛЖНЫ БЫТЬ

Поиск уязвимостей (BugBounty + SSDL)

Форматы участия
в киберучениях The Standoff 2021

По уровню зрелости компании и слаженности ИТ и ИБ процессов

МОНИТОРИНГ

- Нет опыта участия
- Изучение продуктов
- Изучение навыков – повторение действий участников
- **Изучить работу с продуктом в «живой» среде**

СТАНДАРТНАЯ ИНФРАСТРУКТУРА

- Не участвовал в Standoff ранее
- Небольшой опыт выявления инцидентов
- Оценка действий команды
- Риск-ориентированный подход
- **Научиться работать с рисками, выявлять и отслеживать атакующих**

АДАПТИРОВАННАЯ ИНФРАСТРУКТУРА

- Есть опыт участия в Standoff
- Понимание риск-ориентированного подхода
- Уверенное использование средств защиты
- Изучение безопасности своих сервисов и методов их защиты (мониторинга)
- **Обнаружение и расследование на инфраструктуре со своим сервисов (системой)**

МОДЕЛИРОВАНИЕ ИНФРАСТРУКТУРЫ

- Большой опыт расследования инцидентов
- Уверенная работа со средствами защиты
- Понимание риск-ориентированного подхода
- Отработка навыков защиты своих сервисов на своих СЗИ
- **Самостоятельное противостояние с максимальной зоной ответственности**

Цель и задачи
киберучений на The Standoff 2021

ЦЕЛЬ

Уметь выявить действия атакующего на разных этапах реализации нежелательных событий

ЗАДАЧИ

- Отработка эффективности работы уже закупленных средств защиты
- Тестирование дополнительных средств защиты на макете бизнес-процессов, приближенных к своей компании
- Анализ и харденинг инфраструктуры с возможностью ответа на вопрос «***What if?***»
- Отработка навыков **взаимодействия** и решения задач **на стыке ИБ и ИТ**

КОМАНДА

ИБ: 5-10 человек

ИТ: 2-4 человека (зависит от эксплуатируемых систем

РЕЗУЛЬТАТЫ КИБЕРУЧЕНИЙ

- Выявление важных точек защиты сервисов
- Навыки совместного (ИТ и ИБ) противодействия атакам на риски
- Подобранные настройки средств мониторинга инфраструктуры

Результаты киберучений

БЕСЦЕННЫЙ ПРАКТИЧЕСКИЙ ОПЫТ

- Выявления и расследования инцидентов на живых атаках
  в режиме реального времени
  - Концентрация — большое количество реальных атак и разных команд в одном месте
  - Полнота охвата действующих правил выявления инцидентов
- Моделирование рисков
  - Интеграция систем
  - Навыки и важность безопасной настройки инфраструктуры
- Обучение специалистов
  - Аналитики
  - Специалисты по СЗИ (внутрь/периметр)
  - Взаимодействие в условиях атаки и жестких рамок

БЕСЦЕННЫЕ АРТЕФАКТЫ

- в т.ч.уязвимости при bug bounty
- варианты настроек защиты конкретных систем
- Варианты настроек самих средств защиты

КООРДИНАЦИЯ РАБОТЫ КОМАНД ИБ (ИТ, технологи)

- Понимание процессов и приоритетов по их улучшению

План проведения мероприятий

ПОДГОТОВКА | **ПРОВЕДЕНИЕ** | **ИТОГИ**

февраль | март | апрель | май | июнь

01 — Согласование

02 — Подготовка инфраструктуры РТ

03 — Подготовка базовой инфраструктуры на полигоне — ИТ

04 — Настройка средств защиты на полигоне — ИБ

05 — Подготовка к участию, процессы

06 — Легенда, риски для полигона - РТ

07 — Реагирование на инциденты

08 — Отчеты и выводы по результатам киберучений


POSITIVE
TECHNOLOGIES
Резервируйте
свой макет!
ЗАЩИТА
И БЕЗОПАСНОСТЬ
ТЕСТИРОВАНИЕ
И ИНТЕГРАЦИЯ
БЫСТРЫЙ ВЫВОД
ТЕХНОЛОГИЙ НА РЫНОК
ptsecurity.com