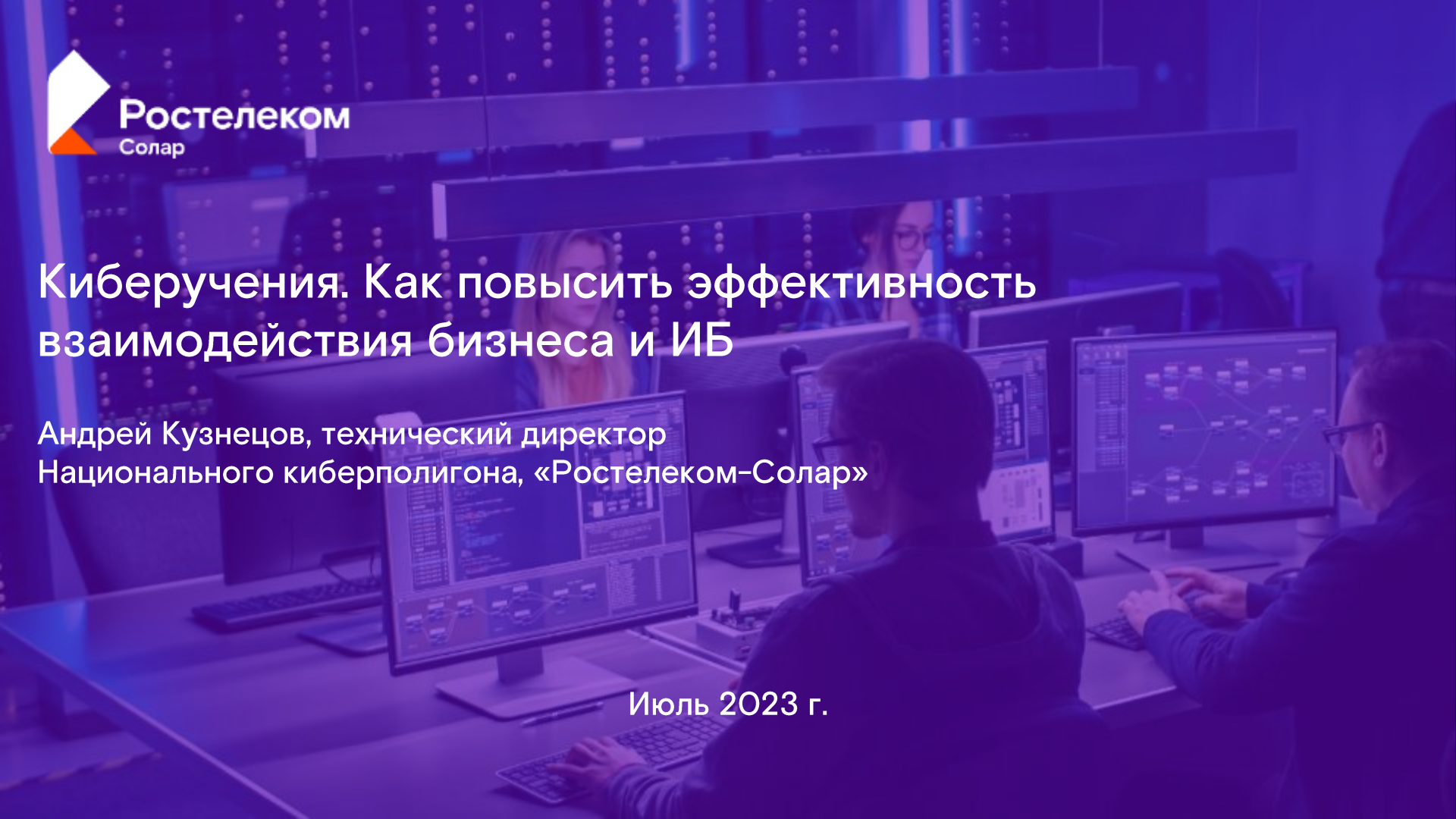


Киберучения. Как повысить эффективность взаимодействия бизнеса и ИБ

Андрей Кузнецов, технический директор
Национального киберполигона, «Ростелеком-Солар»

Июль 2023 г.

Фокус на персонале

Технологический прорыв
2000 - 2010

Процессный прорыв
2010 - 2020

Прорыв практических компетенций
2020 - ...

Ростелеком
Солар

Типовые проблемы эпохи практических компетенций и их решение

1 **Нехватка ИБ-персонала**

Помощь в создании кадрового резерва службы ИБ внутри компании за счет непрерывного обучения практическим навыкам

2 **Недостаточный уровень квалификации**

Проверка навыков сотрудников информационной безопасности и повышение их квалификации за счет практической отработки на киберполигоне

3 **Отсутствие практических навыков**

Возможность эмулировать реальную атаку на киберполигоне с целью «своими руками» отработать процесс реагирования на инцидент

4 **Отсутствие слаженности команд**

Отработка планов реагирования и ликвидации последствий киберинцидентов за счет слаженности действий работы разных подразделений компании

5 **Низкая скорость принятия решений**

Предупреждающая проработка возможных векторов развития событий для оперативного реагирования на киберинциденты

6 **Появление новых продуктов на рынке**

Практическое обучение работе с новыми ИБ-продуктами с возможностью тестирования их взаимодействия с внедренными ИТ- и ИБ-решениями

Что такое киберучения?

Киберучения – процесс практической подготовки, освоения, проверки навыков и слаживание работы специалистов, экспертов и руководителей путем моделирования компьютерных атак и отработки реакций на них в реалистичной среде

Ростелеком
Солар

Зачем нужны киберучения?

Редкие инциденты

↓

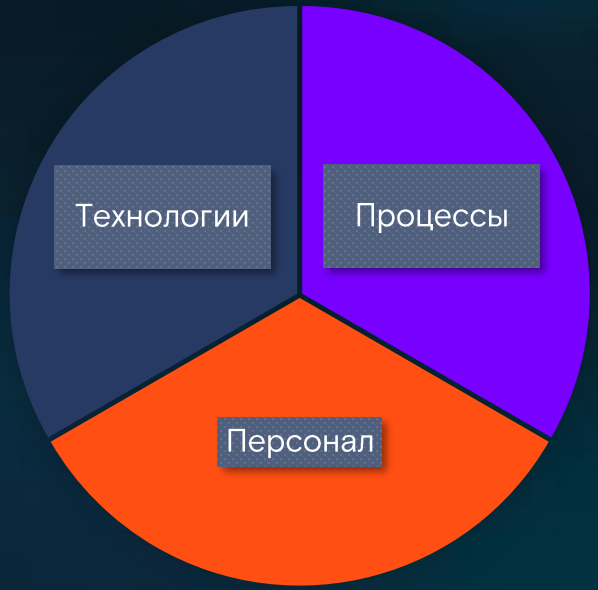
Неэффективные процессы

↓

Медленное и некачественное реагирование и восстановление

↓

Риск больших потерь от инцидентов



Киберучения

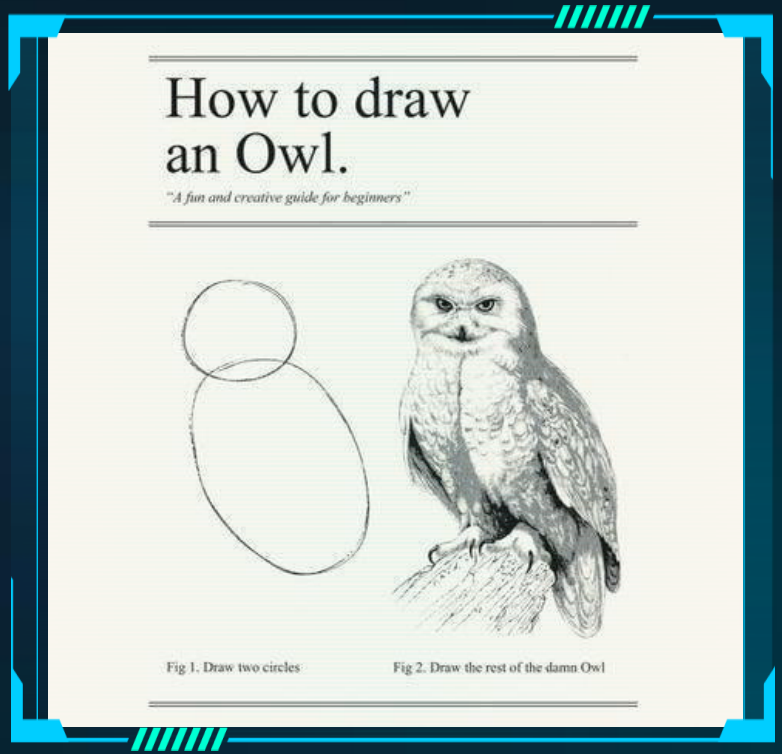
↓

Радикальное сокращение риска потерь от инцидентов

Ростелеком
Солар

Киберучения это просто?

1. Подготовить киберучения
2. Провести киберучения
3. Profit!



Ростелеком
Солар

Как правильно поставить цели киберучений

ОЦЕНИТЬ

- эффективность по документированию и анализу инцидентов для устранения возможных уязвимостей
- эффективность пройденных участниками образовательных курсов и программ
- способность выявлять атаки и реагировать на них
- способность ЛПР определять возможные последствия кибератак и формировать процедуры и регламенты реагирования

ВЫЯВИТЬ

- «слабые места» в системах защиты объекта/объектов
- недостатки в политиках и процедурах обеспечения ИБ
- средства, необходимые для обеспечения ИБ информационной системы и обеспечения стабильного функционирования

Ростелеком Солар

+

- Разработать планы действия в чрезвычайных ситуациях
- Повысить осведомленность, готовность и координацию участников

Как определить целевую аудиторию?

- Руководители?
- Специалисты ИБ?
- Специалисты смежных служб?
- PR?
- ....

Цель общая, задачи разные!

Как правильно определить тип киберучений

Штабные	Практические	Гибридные
Теоретические задания и проработка сценариев реагирования на угрозы	Практические задания для всех целевых групп участников	Теоретические и практические задания

+ Отраслевые и кросс-отраслевые
+ Локальные, региональные, федеральные

Ростелеком
Солар

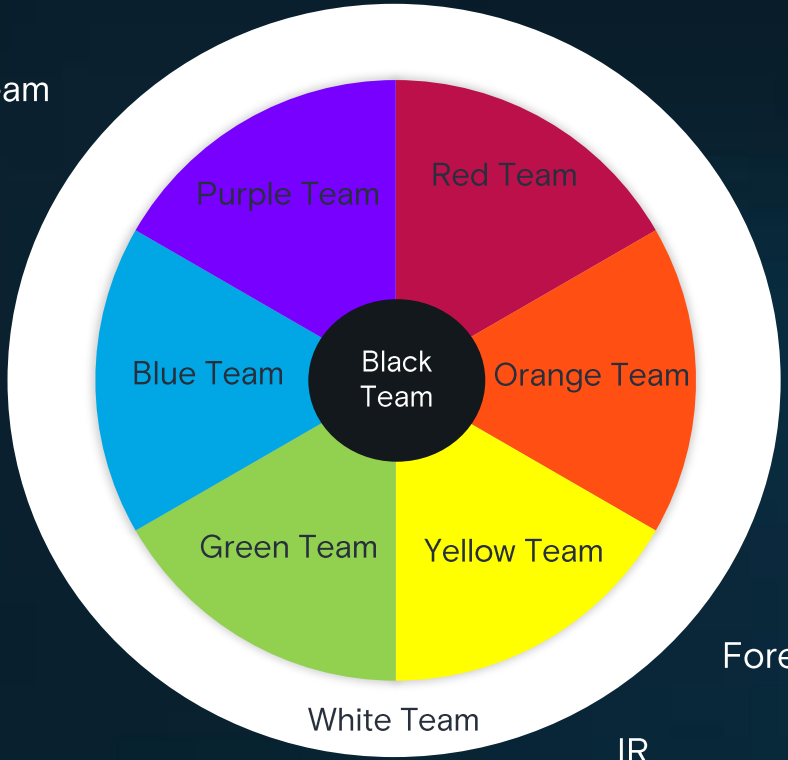
Как сформировать механику киберучений

Blue Team vs Red Team

Blue Team

Red Team

Table-Top



CTF

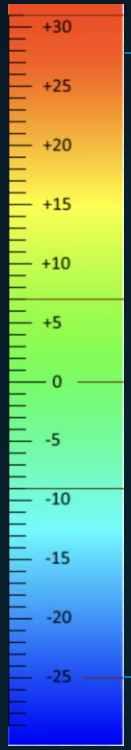
Forensic

IR

BCP

Ростелеком
Солар

Готовь инфраструктуру летом



Цифровые двойники

Цель?

Лабораторная работа

- ✓ Инфраструктурные сервисы
- ✓ Средства защиты информации
- ✓ Прикладное программное обеспечение
- ✓ Топология сети
- ✓ Белый и вредоносный трафик
- ✓ Конфигурации
- ✓ .....

Ростелеком
Солар

Документация: скучно, но важно

Концепция

- Замысел киберучений

Информация для организаторов

- Механика киберучений
- Скоринг и основные правила
- Регламент работы технической поддержки
- Регламент работы «игровых» структур (CERT, SOC и т.д.)
- Тайминг и план мероприятия
- Брифинги и вводные
- Описание сценариев

Информация для участников

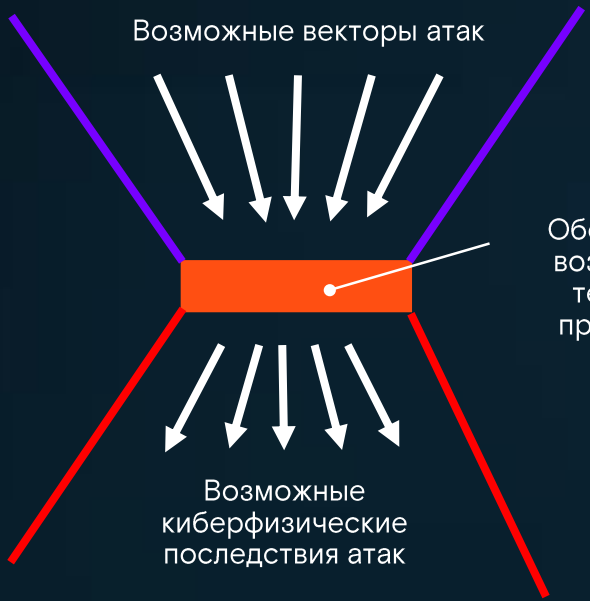
- Перечни и состав команд
- Руководство участника киберучений (основные правила)
- Регламенты взаимодействия с «игровыми» структурами (CERT, SOC и т.д.)

Прочие материалы

- Информация для доступа к инфраструктуре и ПО, ссылки на ресурсы
- Информация о каналах коммуникации
- Формы отчетов для команд

Ростелеком
Солар

Киберфизические последствия и где они обитают?



Оборудование и ИС, воздействующее на технологический производственный процесс

Модели информационных систем, АСУ, сетей связи

Модели интеллектуальных устройств и оборудования пром. автоматизации

Моделируемый технологический процесс

Ростелеком
Солар

Помогаем участникам

Организационная поддержка

Техническая поддержка

Ростелеком
Солар

Быть готовым к неожиданностям

«Если какая-нибудь неприятность может случиться, она случается»

Закон Мерфи

Вот тут нам пригодится План Б!

Ростелеком
Солар

Поработать с обратной связью

- Соберите фидбек с участников – предложите заполнить им небольшой опросник:
  - Что им понравилось, что не понравилось?
  - Хватило ли предоставленных документов? Все ли было в них понятно?
  - Как отработали организаторы, модераторы, тех. поддержка?
  - Все ли работало так, как надо?
  - Как можно было бы сделать этот опыт лучше?
- Дайте участникам обратную связь в виде отчета

Провести ретроспективу мероприятия

- Проанализируйте результаты опроса участников
- Ответьте на вопросы:
  - Что было сделано хорошо?
  - Что было сделано плохо?
  - Что пошло не так?
  - Какие риски реализовались?
- Систематизируйте и задокументируйте результаты разбора для использования в качестве «базы знаний» по проведению киберучений в дальнейшем

Национальный киберполигон

Вопросы?

Ростелеком
Солар