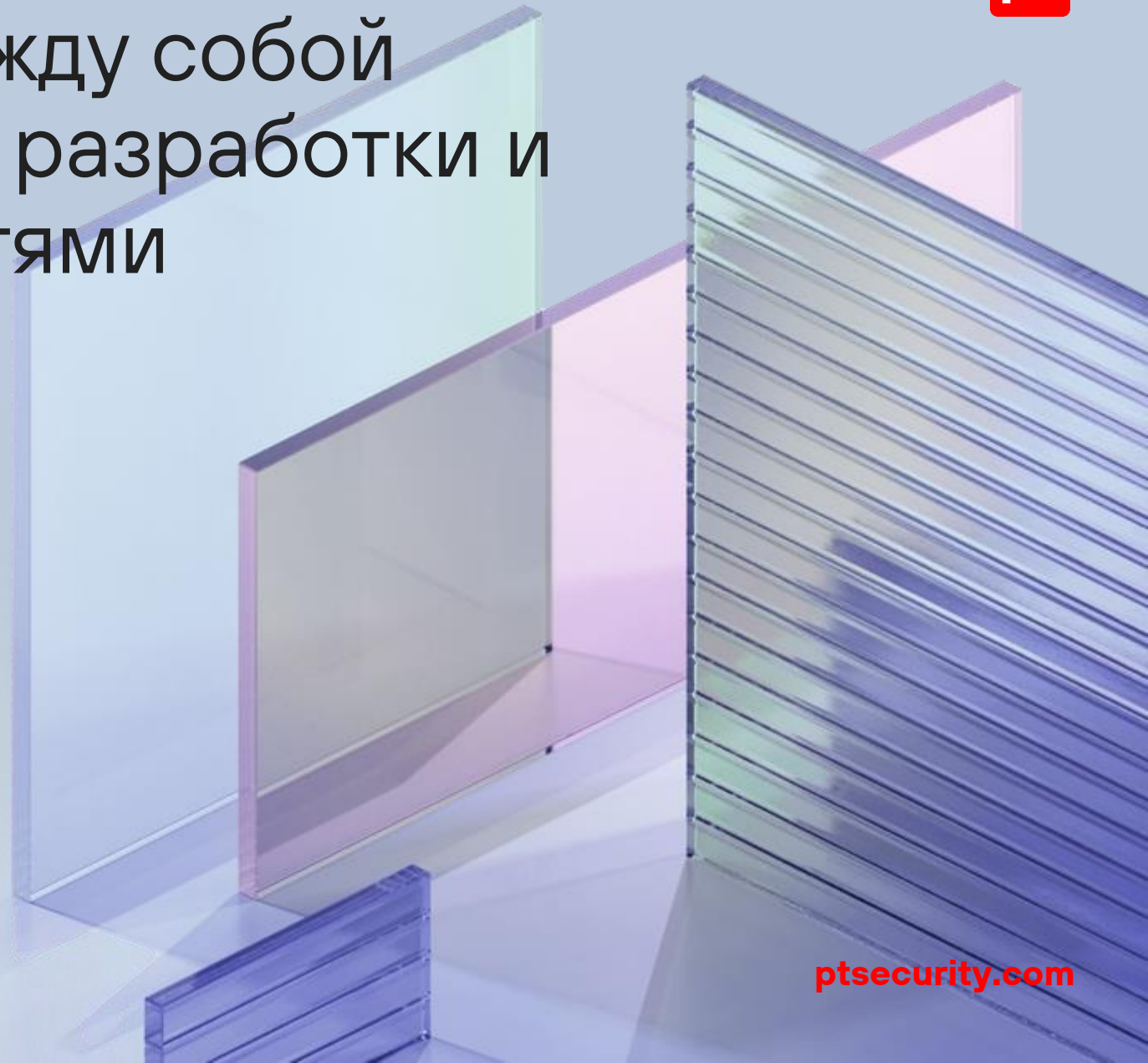
Как интегрировать между собой процессы безопасной разработки и управления уязвимостями

Михаил Кадер

АО «Позитив Текнолоджиз»

13.10.2023



ptsecurity.com

Актуальный «баян»

Если бы строители строили здания так же,
как программисты пишут программы,
первый залетевший дятел разрушил бы
цивилизацию.

Второй закон Вейнберга

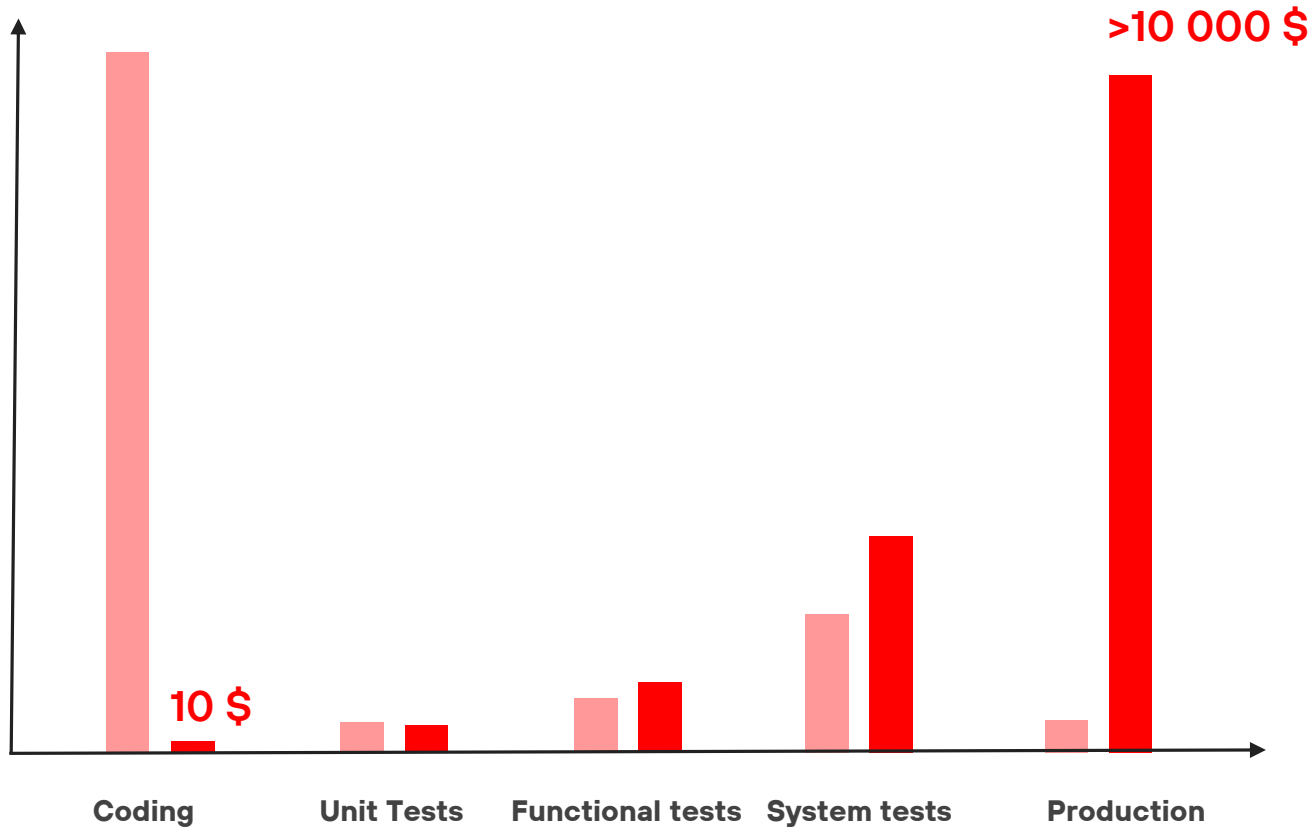
А может быть качество современных приложений уже на высоте?

- 14 ошибок на 1000 строчек кода (иногда получше)
  https://www.securitylab.ru/news/420674.php
- Сценарии использования против качества?
  Слишком сложное ПО
- ПО с открытым кодом (1000 глаз ☺)
  https://habr.com/ru/company/pvs-studio/blog/596109/
  https://www.securitylab.ru/analytics/536146.php
- Переиспользуемый код
- Искуственный интеллект (ChatGPT)
  https://habr.com/ru/post/715492/
  https://habr.com/ru/post/703568/

«Удешевление» ошибок - Shift Left

Сколько стоит баг и зачем нужен Shift Left

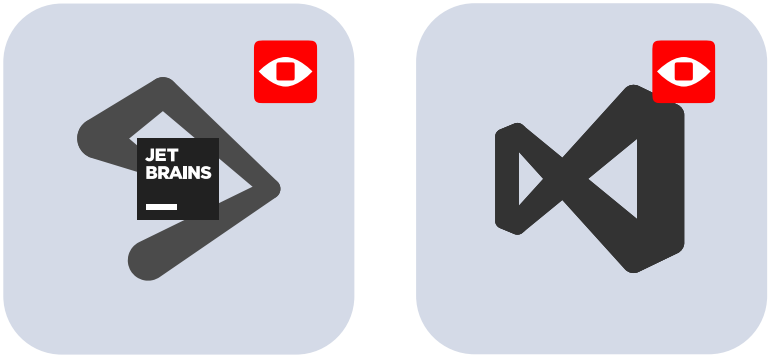
- Количество новых багов
- Стоимость исправления одного бага



Плагины IDE

Например

- JetBrains (PHP)
- Visual Studio Code (PHP)



Статический анализ кода (SAST)

Появилась необходимость тестировать все ПО, образы, библиотеки

Запрос от ИТ

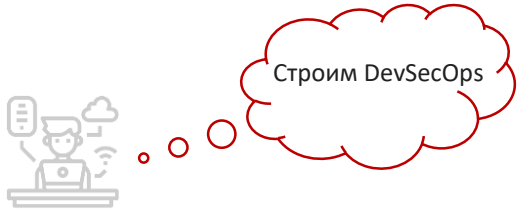
- Интеграция в среды разработки
- Приоритезация уязвимостей
- Автоматизация проверок SAST на этапах CI/CD pipeline

PT AI

- Экспертиза: из практики в продукт
  200+
  уязвимостей нулевого дня наши эксперты обнаруживают ежегодно
- Минимум ложных срабатываний
- Гибкое масштабирование
- Быстрое закрытие уязвимостей и виртуальный патчинг (PT Application firewall)

Динамический анализ кода (DAST)

91% веб-приложений – возможность утечки КИ
84% веб-приложений – возможность НСД



Запрос от ИТ

- Тестирование защищенности без предоставления исходного кода, УЗ и пр.
- Автоматизация проверок DAST на этапах CI/CD pipeline

PT BlackBox

- Развитие ядра с 2011г. Экспертиза PT
- Минимум ложных срабатываний
- Сигнатурный и эвристический анализ

Уязвимости

Недостаток вычислительной логики (например, в коде), обнаруженный в программном или аппаратном компоненте (например, в прошивке), использование которого может оказать негативное воздействие на конфиденциальность, целостность или доступность данных.

Статистика (не)врет?
Количество новых уязвимостей

>18 000 уязвимостей	>20 000 уязвимостей	>25 000 уязвимостей	?
2020 г.	2021 г.	2022 г.	2023 г.

* По информации из базы данных National Vulnerability Database

Среднее количество уязвимостей, обнаруженных на одном пилотном проекте

Результаты пилотных проектов MaxPatrol VM

3 %

До 3% уязвимостей являются крайне опасными.
При этом они могут не иметь максимальной оценки по CVSS

31 000

уязвимостей всех типов

861

трендовая уязвимость (их нужно устранить как можно скорее)

9 000

критически опасных уязвимостей по оценке CVSS

42

трендовые уязвимости на активах высокой значимости

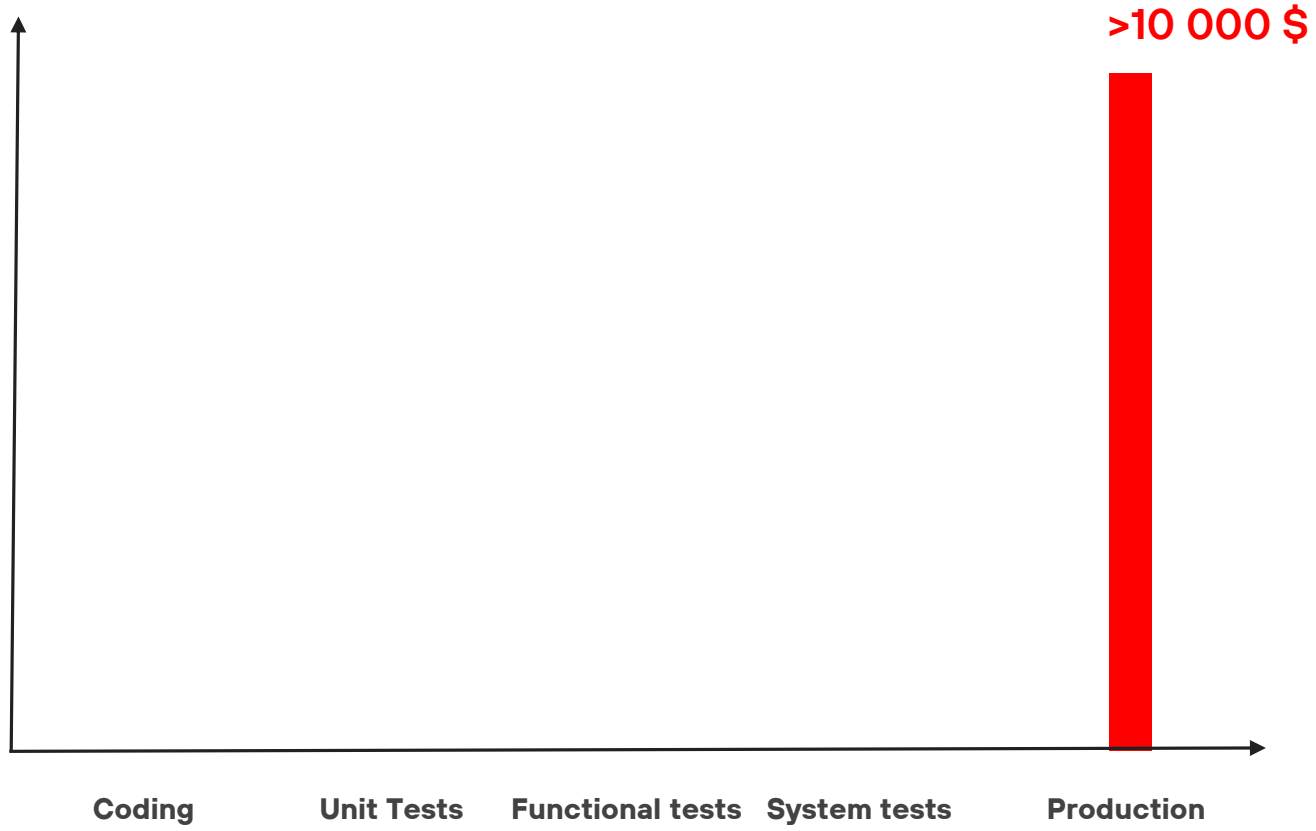
«Как выстроен процесс управления уязвимостями в российских компаниях», Positive Technologies

«Удешевление» и «ускорение» исправления уязвимостей – Shift Down

Сократить окно возможностей злоумышленника?

... или иначе ...

Повысить уровень киберустойчивости ключевых бизнес процессов!



Управление уязвимостями

1
Постоянная актуализация данных об активах

2
Классификация и оценка активов

3
Выявление уязвимостей

4
Сортировка и приоритизация уязвимостей

5
Устранение или компенсация уязвимостей

6
Проверка устранения уязвимостей

VM

AM — **Asset management** (управление активами)

VA — **Vulnerability assessment** (определение уязвимостей)

VR — **Vulnerability remediation** (устранение уязвимостей)

И не забыть про ...

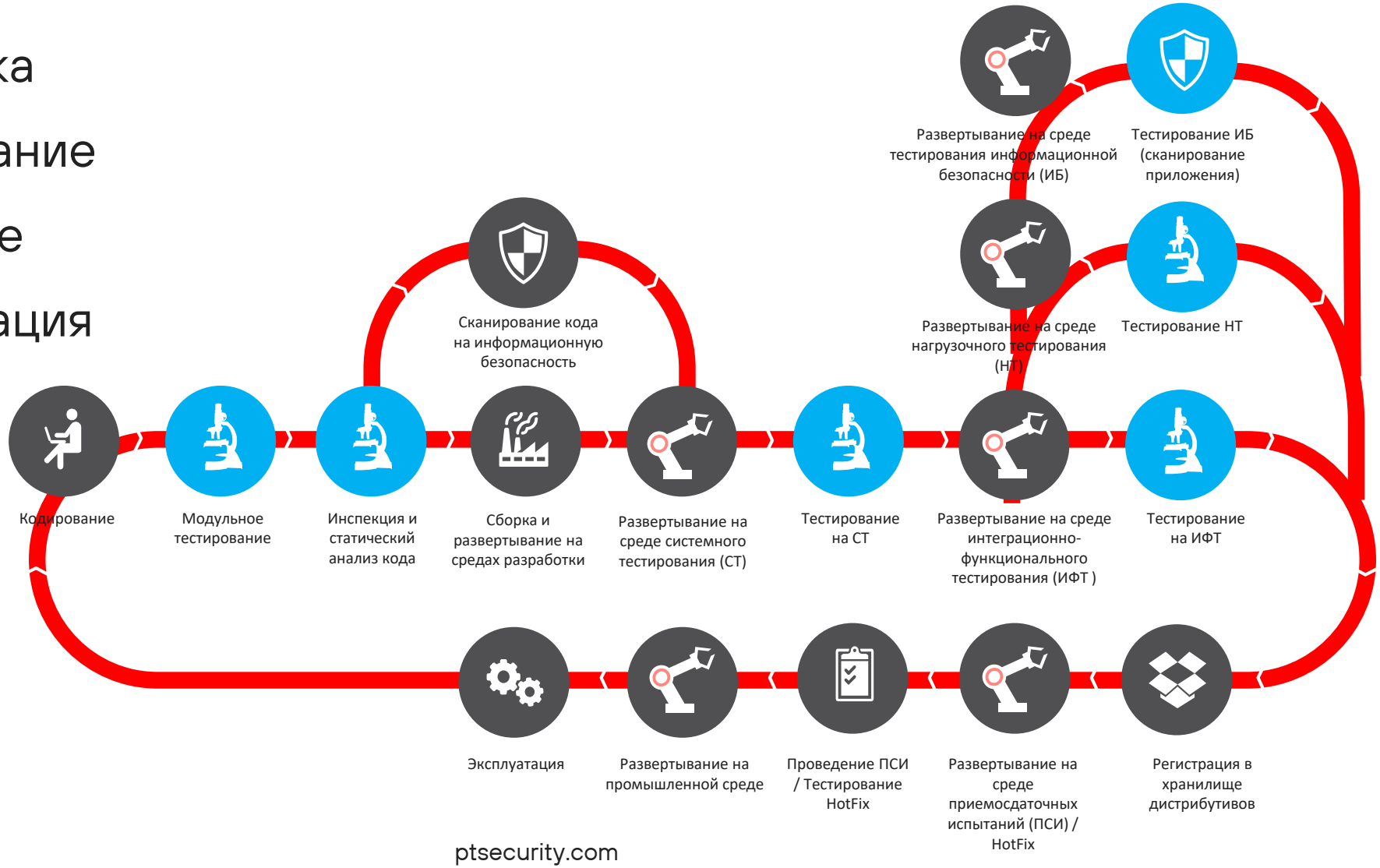
Использовать анализаторы исходного кода на наличие 0-day уязвимостей

Использовать промежуточный репозиторий, куда попадают только проверенные пакеты, библиотеки, компоненты

Встраивать автоматические проверки в процесс CI/CD

Циклический автоматизированный процесс

- Разработка
- Тестирование
- Внедрение
- Эксплуатация



Багбаунти (Кибериспытания) как процесс

- Что это?
  - Платформа для тестирования киберустойчивости
- Как работает?
  - Этичные хакеры ищут и сдают уязвимости 24/7/365
  - Компания награждает исследователя
- Зачем?
  - Выявить узкие места в разработке
  - Проверить работу SOC
  - Публично заявить: «мы заботимся о безопасности»
  - Рейтинг киберустойчивости – страхование остаточных рисков?
- Заодно
  - Эффективный расход бюджета. Ничего не нашли – можно не платить

Кибериспытания на Киберполигоне

Red team

- Ведущие исследователи защищенности
- Участники bug bounty
- Победители CTF-соревнований
- Эксперты безопасности промышленных систем

Blue team

- Собственная команда заказчика
- Менторы PT ESC
- Сильнейшие команды поставщиков услуг

The Standoff

Управление киберполигоном заказчика

Портал управления киберучениями
Портал управления скриптами-чекерами

Кастомизация и управление киберполигоном

Позволяет реконфигурировать полигон заказчика:
изменить количество сегментов,
изменить состав сервисов и сегментов

Мониторинг ИБ

Решения Positive Technologies: PT NAD, MaxPatrol SIEM,PT AF, PT MultiScanner
Решения других вендоров
Blue teams: ведущие команды из России, Европы, США

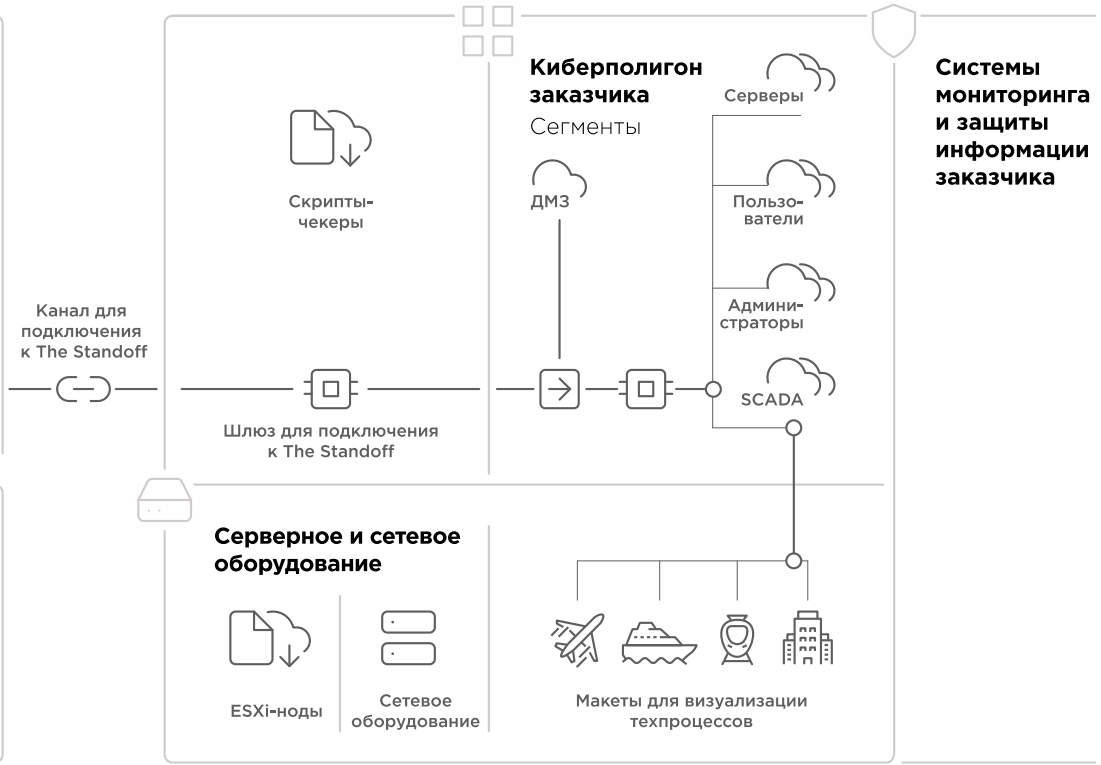
Инфраструктура The Standoff

Enterprise
Telecom
Bank
SCADA
Red teams:
ведущие пентестеры со всего мира,
участники bug bounty,
победители CTF,
исследователи промышленных систем

Доступ к мероприятиям Standoff

Подключение инфраструктуры заказчика к открытым и закрытым мероприятиям The Standoff

Киберполигон, реальная инфраструктура



Выводы

- Основная цель - обеспечение киберустойчивости предприятия
- Современные процессы разработки и эксплуатации ПО позволяют частично повысить его уровень защищенности
- Непрерывное тестирование – залог успеха

Спасибо
за внимание

ptsecurity.com