

PT BlackBox

Динамический анализатор
приложений





Защищаем крупные информационные системы от киберугроз:

20 лет

опыта исследований
и разработок

1200 сотрудников:

инженеров по ИБ,
разработчиков, аналитиков
и других специалистов

250 экспертов

в нашем
исследовательском
центре безопасности

200+

обнаруженных
уязвимостей
нулевого дня в год

200+

аудитов безопасности
корпоративных систем
делаем ежегодно

50%

всех уязвимостей
в промышленности
и телекомах обнаружили
наши эксперты

■ создаем продукты и решения

■ проводим аудиты безопасности

■ расследуем инциденты

■ анализируем угрозы



Уязвимости веб-приложений

98%

случаев
злоумышленники имеют
возможность проводить
атаки на пользователей

91%

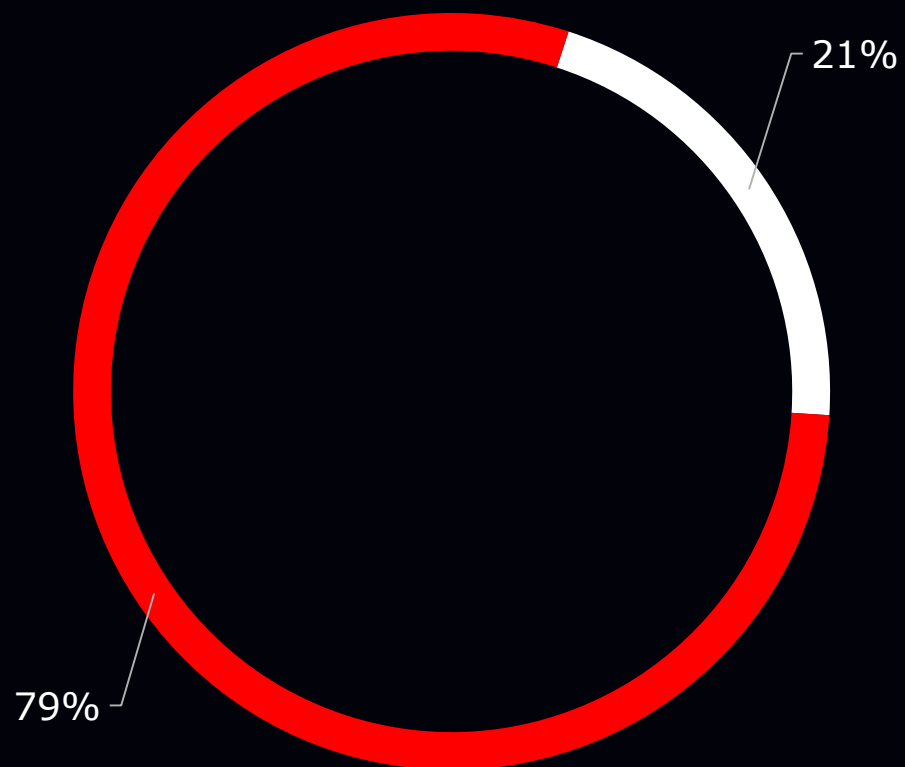
веб-приложений
возможны утечки важных
данных пользователей

84%

веб-приложений
есть возможность
несанкционированного
доступа



Результаты анализа методом черного ящика



- Белый ящик
- Черный или серый ящик

В 2020–2021 г. исследования методом черного или серого ящика стали самыми популярными среди клиентов Positive Technologies

Уровень опасности уязвимостей, выявляемых при анализе методом черного или серого ящика

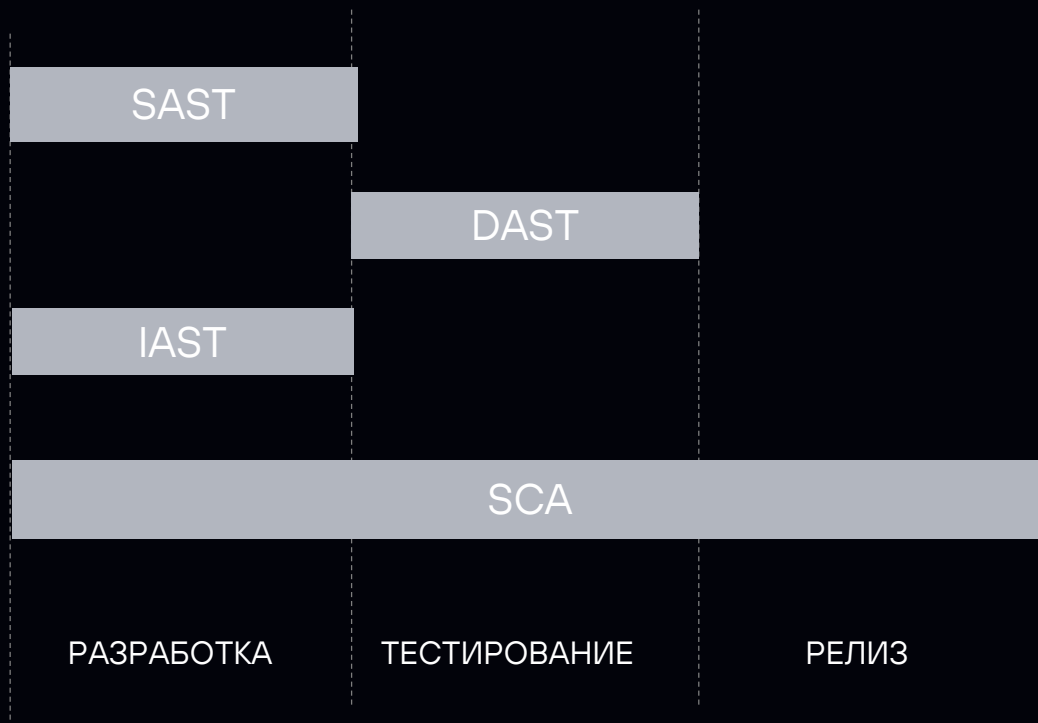




Для исследования методом черного ящика
клиентам **НЕ нужно** предоставлять
тестировщикам все имеющиеся данные
о приложении, включая исходный код



Анализаторы защищенности приложений



- **Статический анализ (SAST)**
находит уязвимости в исходном коде
- **Динамический анализ (DAST)**
проверяет готовое приложение
- **Интерактивный анализ (IAST)**
инструментирует код, ищет уязвимости в ходе его выполнения
- **Анализ сторонних компонентов (SCA)**
выявляет уязвимости в стороннем коде



История

2011 г.

Появление
ядра

2014 – 2015 г.

Внедрение в PT Application
Inspector и Max Patrol 8

2017 г.

Запуск PT Black
Box Scanner

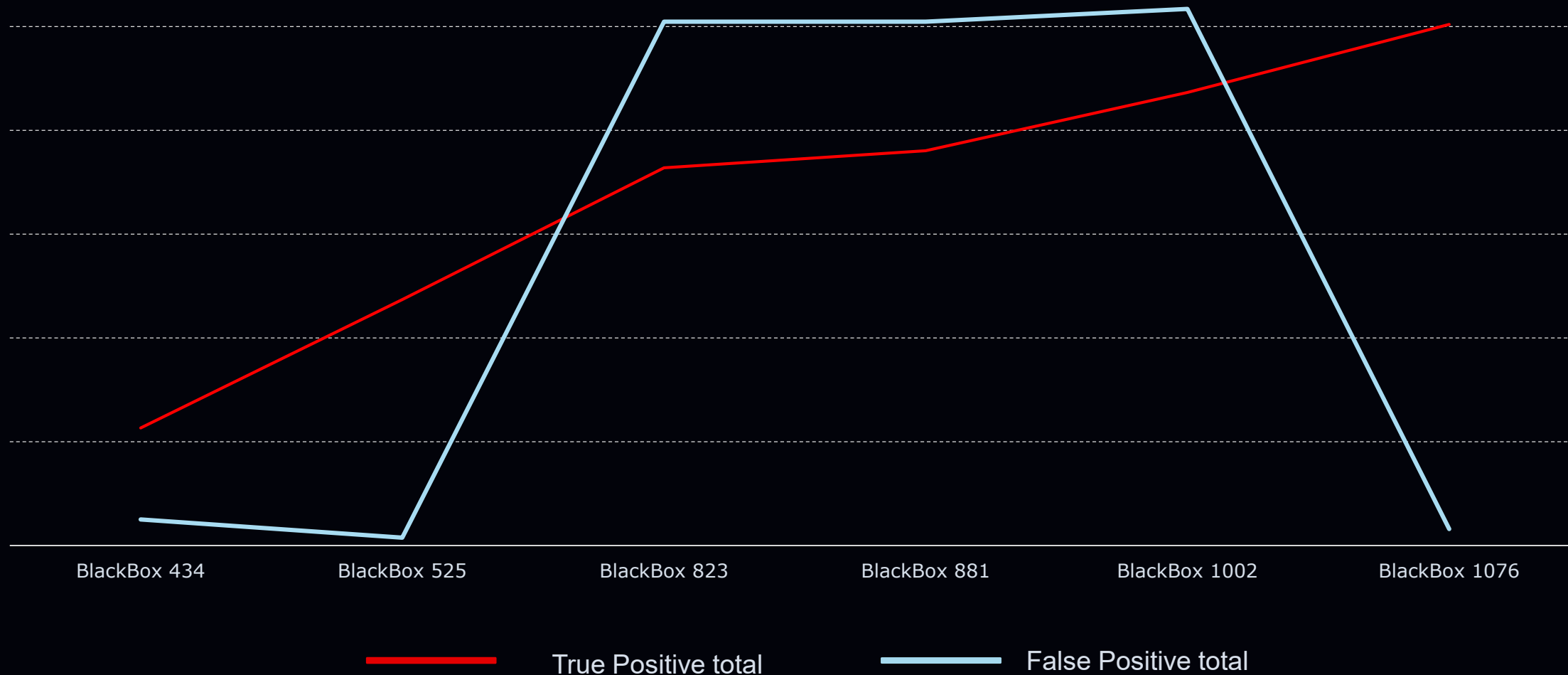
Сегодня

Запуск
PT BlackBox

А как мы проверяли
наш продукт?

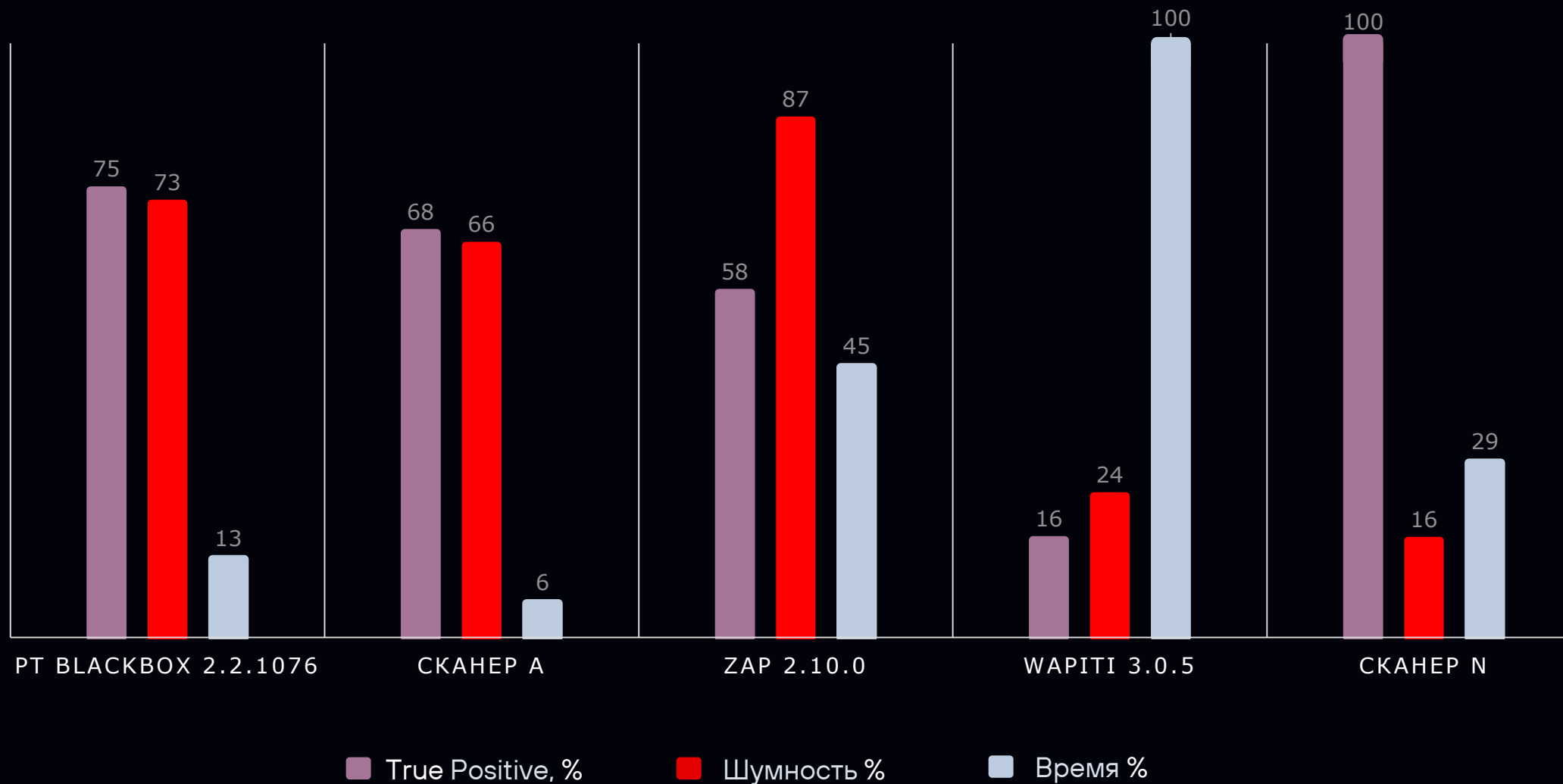


Развитие продукта: True / False Positive



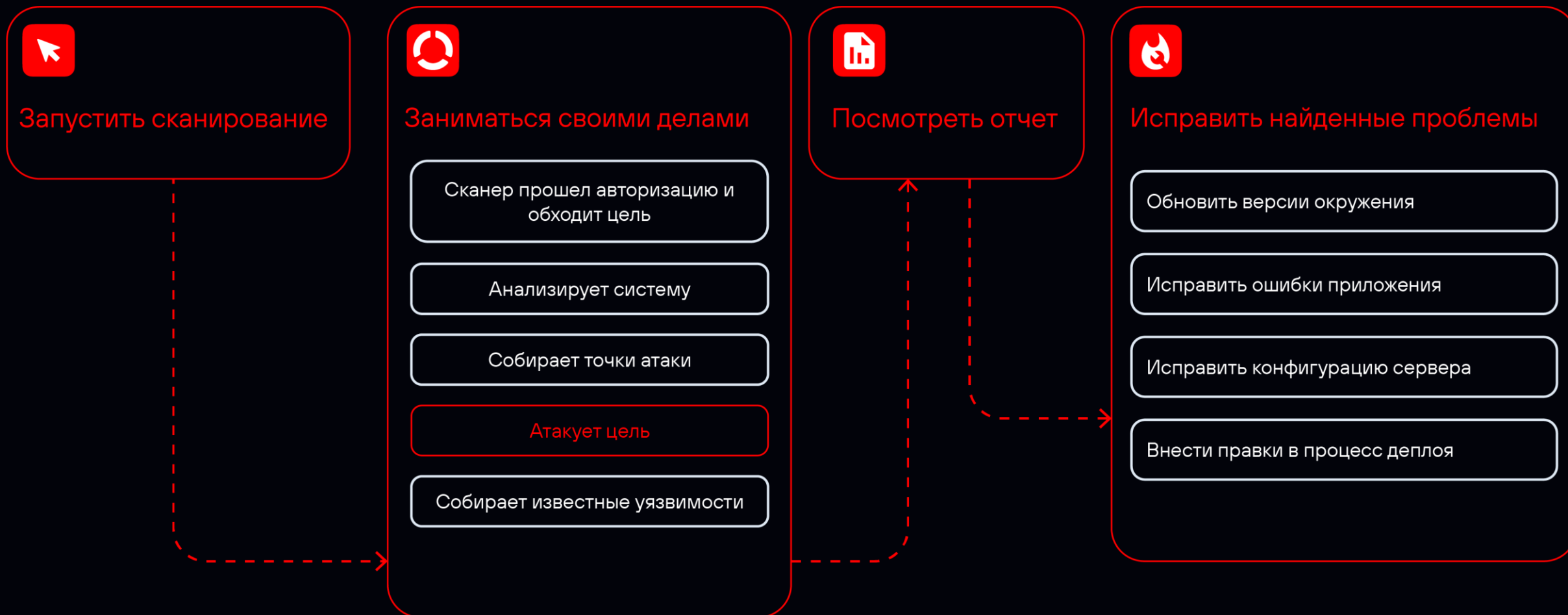


Сравнение показателей разных сканеров



Как работает PT BlackBox.

Архитектура продукта





Системные требования

Рекомендуемые

- **CPU** рассчитывается по схеме 4 ядра на одно сканирование + 1 ядро для системы. Для 5 параллельных сканирований необходимо – 21 CPU.
- **RAM** рассчитывается по схеме 4 GB на одно сканирование + 2 GB для системы. Для 5 параллельных сканирований необходимо – 22 GB RAM.
- **HDD** от 50 GB





Ключевые особенности PT BlackBox



Экономит ресурсы на сканирование. Определяет шаблонные повторяющиеся страницы и не тратит на них время.



Находит то, что скрыто. Использует комбинацию сигнатурного и эвристического анализа. Непрерывно обновляет данные об уязвимостях.



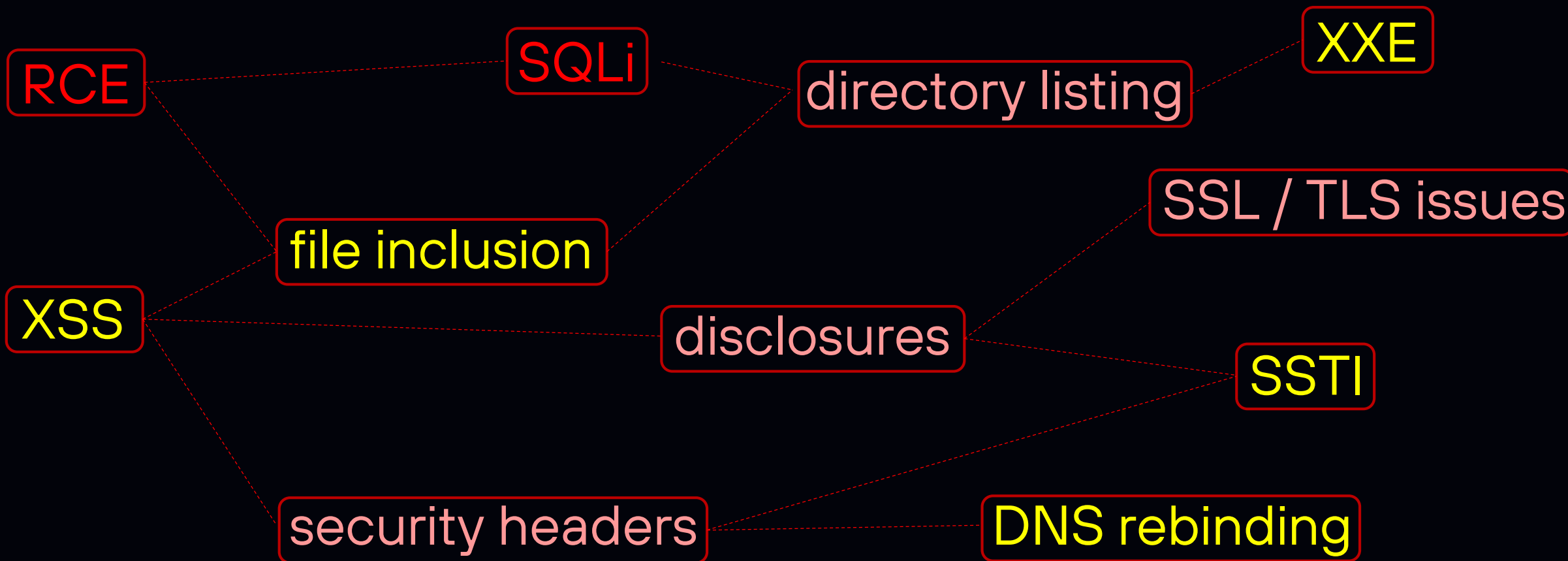
Встраивается в процесс разработки и релизный цикл. Позволяет эффективно обнаруживать и исправлять уязвимости.



Тонкая настройка сканирования и авторизации позволяет пользователю задавать параметры анализа, добавлять профили сканирования.



Обнаруживаемые уязвимости





Модель лицензирования

ПО КОЛИЧЕСТВУ ЦЕЛЕЙ И
ПАРАЛЛЕЛЬНЫХ СКАНИРОВАНИЙ

ПО КОЛИЧЕСТВУ
СКАНИРУЮЩИХ АГЕНТОВ

Нет ограничений

- По количеству проектов
- По количеству пользователей

Как провести «пилот» PT BlackBox



pt blackbox

Будем на связи

Присоединяйтесь
к нашему комьюнити
в Telegram, посвященному
безопасной разработке



@POSIddev

