

Практические подходы к обеспечению безопасности современных приложений



Михаил Кадер

АО «Позитив Текнолоджиз»

07.02.2023

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
- Искусственный интеллект (ChatGPT)
<https://habr.com/ru/post/715492/>
<https://habr.com/ru/post/703568/>

А что у нас есть?



- SDLC
- BSIMM
- DevSecOps 😊
- И много других страшных слов ...

- Планирование
- Разработка
- Эксплуатация

Планирование



- Знание угроз
- Процесс разработки
- Применение внутренних защитных механизмов
- Внешние (наложенные) средства защиты

Разработка



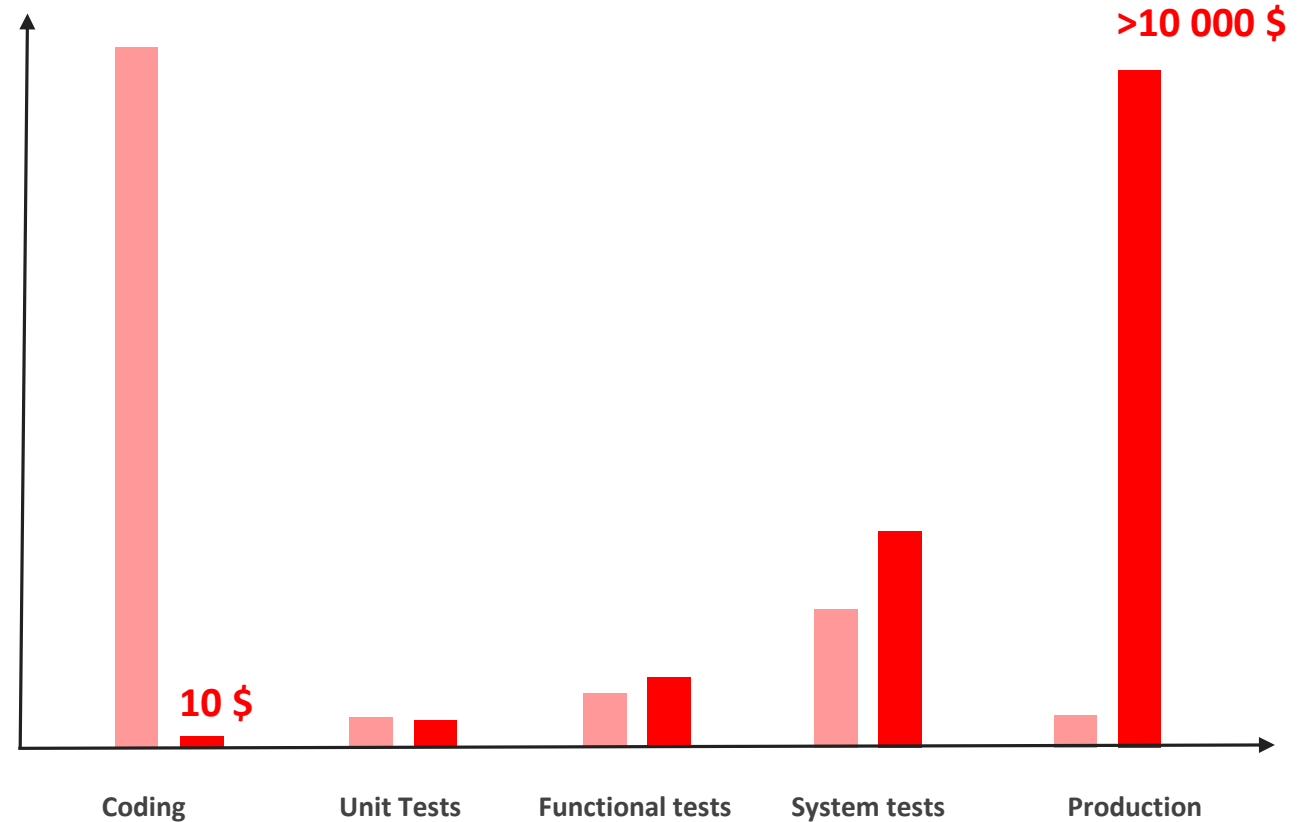
- Плагины для IDE
- Системы статического анализа кода (SAST)
- Системы динамического анализа кода (DAST)
- Интеграция в конвейер разработки и внедрения (CI/CD)
- Интерактивный анализ (IAST)

«Удешевление» ошибок - Shift Left

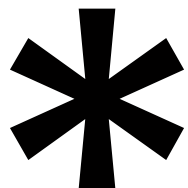


Сколько стоит
баг и зачем
нужен Shift Left

- Количество новых багов
- Стоимость исправления одного бага

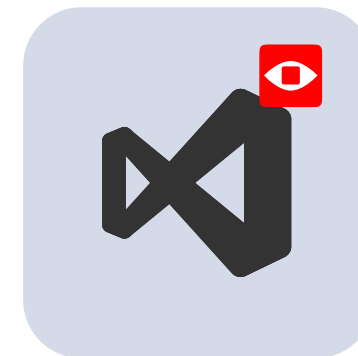
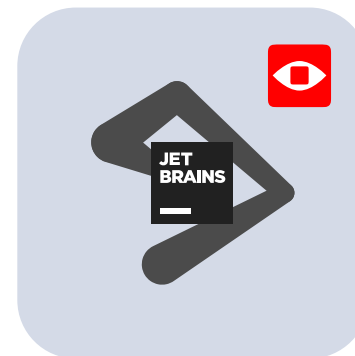


Плагины IDE



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

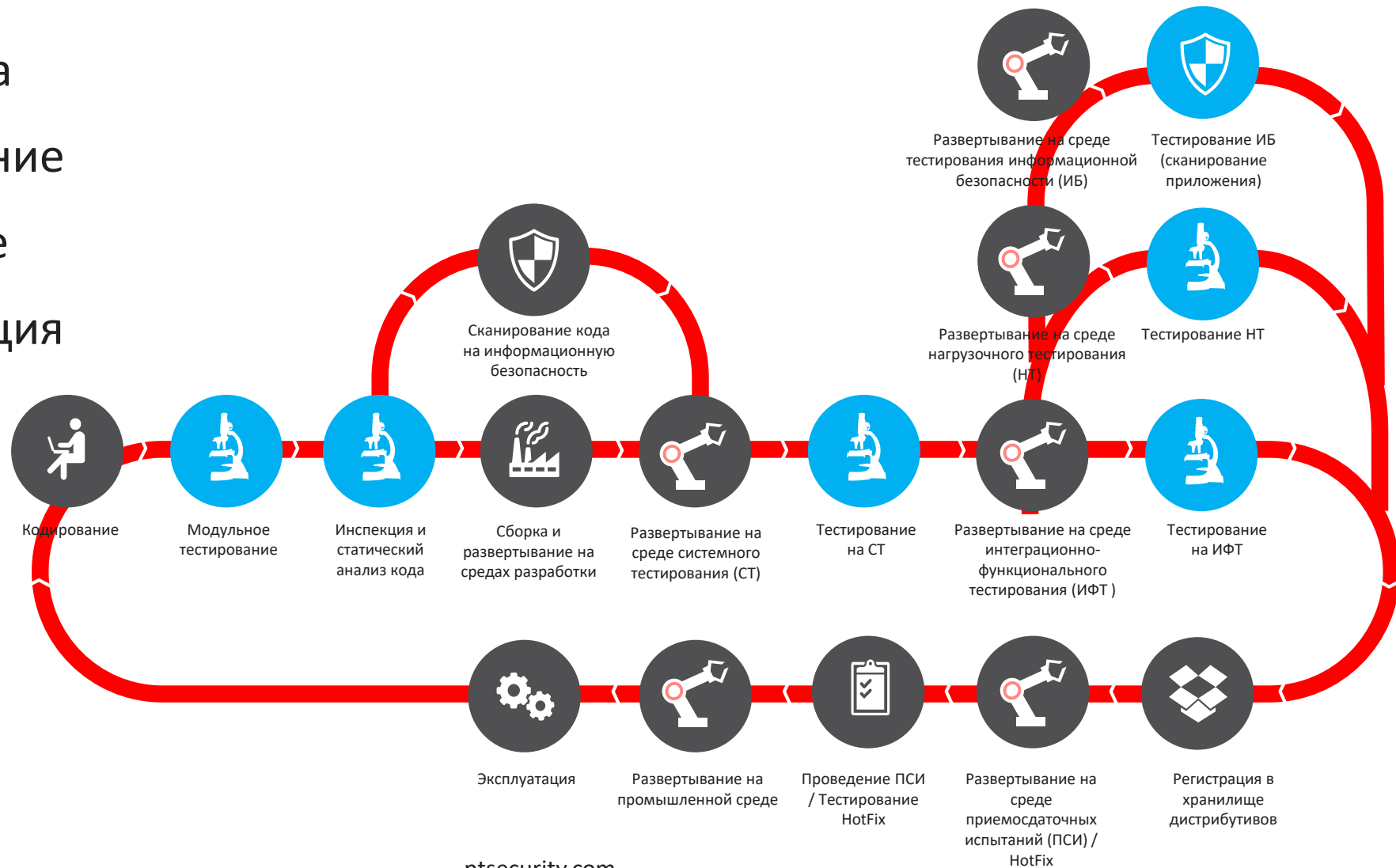
PT BlackBox

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

Циклический автоматизированный процесс



- Разработка
- Тестирование
- Внедрение
- Эксплуатация



Эксплуатация



- Опять же понимание угроз

- Отказ в обслуживании, OWASP, и т.п.

- Процессы

- Непрерывность
 - Управление уязвимостями
 - Мониторинг
 - И т.п. ...

- Наложенные сервисы защиты

- Упрощение сервисного обслуживания
 - Оперативная информация о новых угрозах
 - «Удлинение» пути злоумышленника
 - «Закрытие» уязвимостей
 - Оперативное реагирование
 - Данные для расследования
 - Поведенческий анализ
 - Отчетность
 - Интеграции

Межсетевой экран уровня веб-приложений



66% веб-приложений – содержат уязвимости высокого риска
98% веб-приложений – возможность проводить атаки на пользователя



Запрос от ИТ

- Гибкое масштабирование под увеличивающиеся нагрузки на веб-приложения
- Защита веб-ресурсов организации от известных и неизвестных атак

PT AF

- ✓ Защищает веб-приложения от целевых и массовых атак
- ✓ Быстро встраивается в инфраструктуру.
- ✓ Поддерживает непрерывность бизнес-процессов.

Выводы



- «Контрразведчик должен знать всегда, как никто другой, что верить в наше время нельзя никому, порой даже самому себе. Мне — можно.»
(«17 мгновений весны», Мюллер, 9 серия)
- Применение переиспользуемого ПО с открытым кодом продолжает нести в себе угрозу
- Современные процессы разработки ПО позволяют частично повысить его уровень защищенности
- Внедрение внешних средств защиты часто может оказаться более быстрым и экономически, более эффективным вариантом, чем радикальное повышение качества кода
- ИИ может быть как помощником, так и принести новые риски

Спасибо
за внимание

