POSITIVE TECHNOLOGIES

POSITIVE TECHNOLOGIES

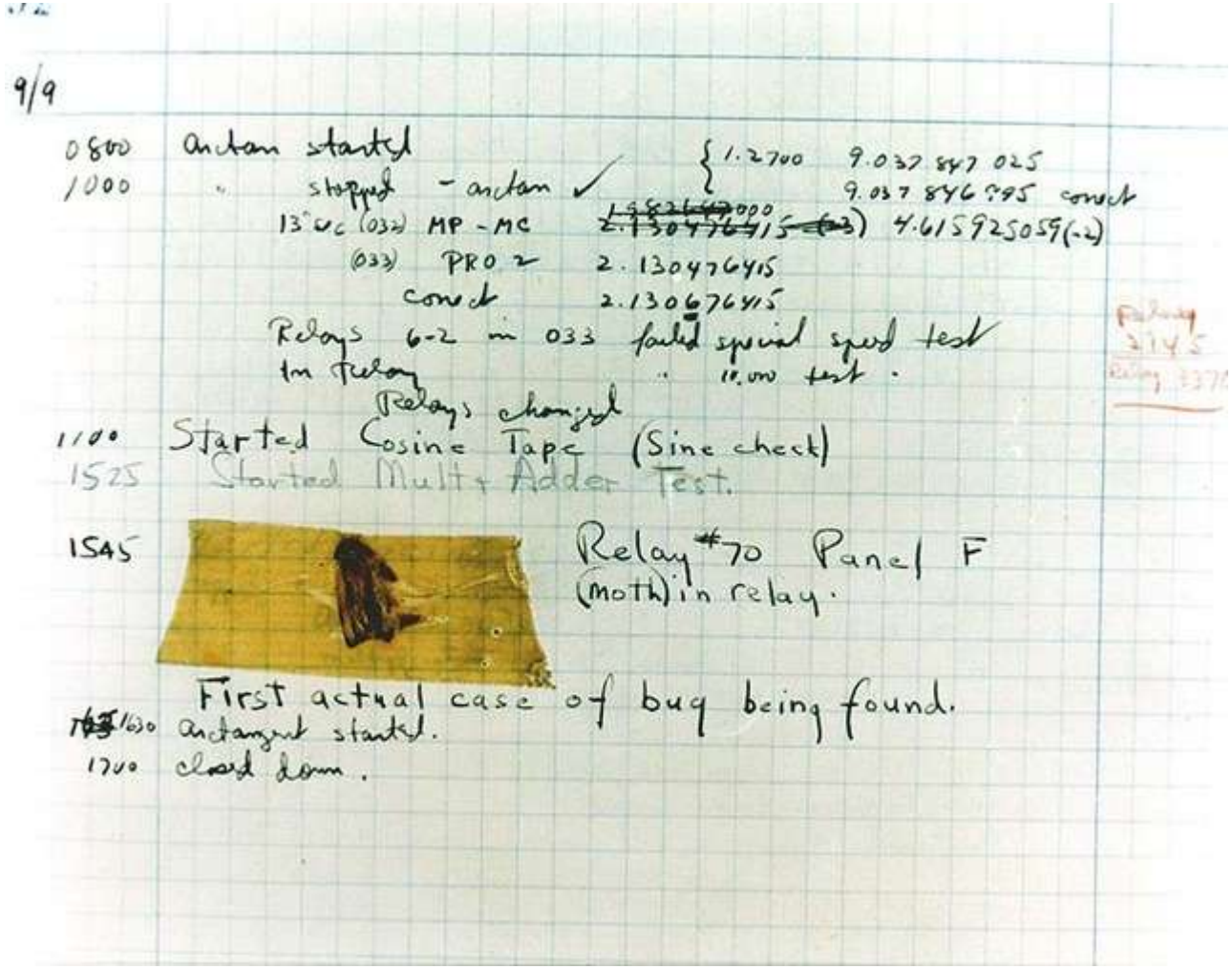
SDLC в два клика

Евгений Миньковский

Ведущий консультант

Positive Technologies

9 сентября 1945, Гарвард



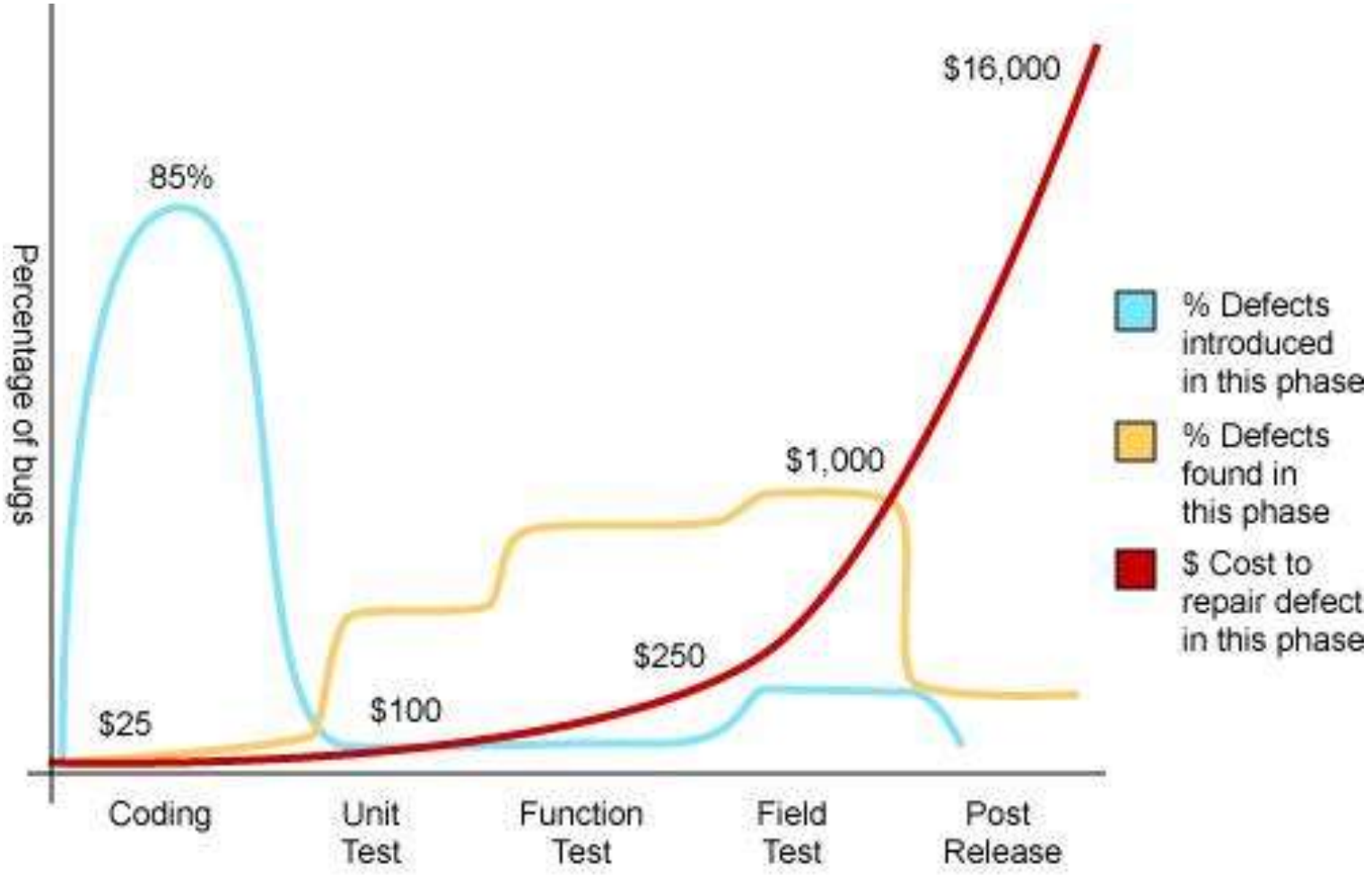
9/9

0800 Arctan started
1000 " stopped - arctan ✓ { 1.2700 9.037 847 025
9.037 846 795 correct
13 MC (033) MP - MC ~~2.130476415 (-3)~~ 4.615925059(-2)
(033) PRO 2 2.130476415
correct 2.130676415
Relays 6-2 in 033 failed special speed test
In relay " 100 test.
Relays changed
1100 Started Cosine Tape (Sine check)
1525 Started Mult + Adder Test.
1545 Relay #70 Panel F
(moth) in relay.

First actual case of bug being found.

1700 closed down.

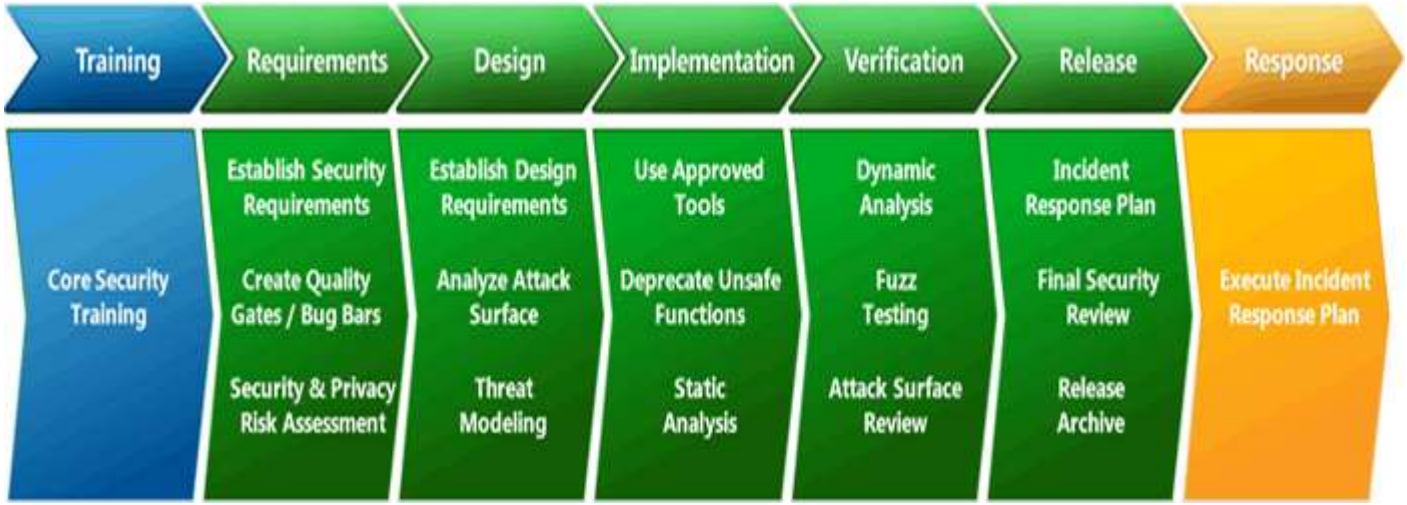
Цена уязвимости



Source: Applied Software Measurement, Capers Jones, 1996

Страшные слова

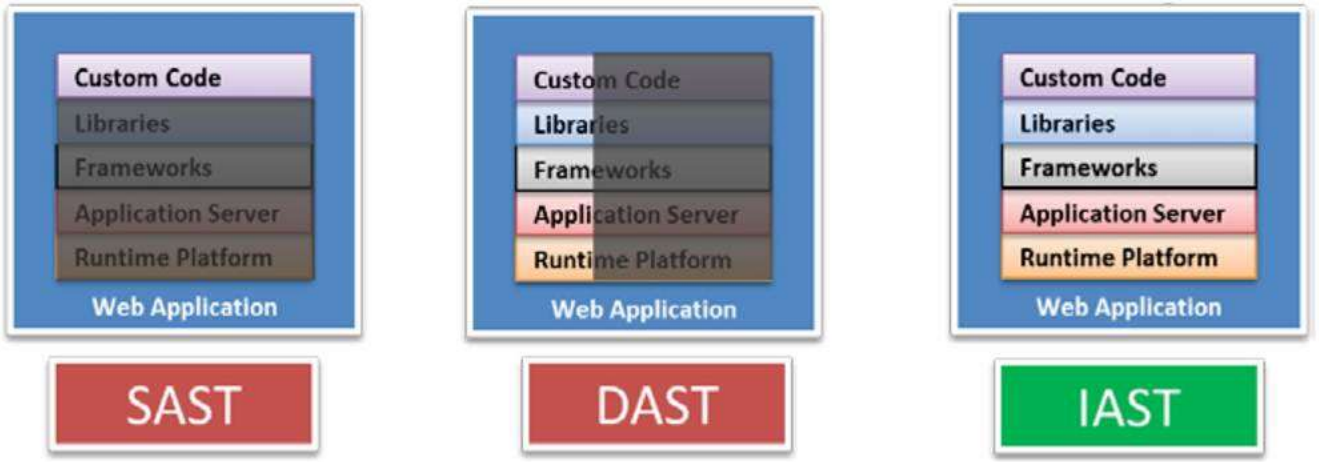
— Microsoft SDLC
— BSIMM
— OpenSAMM



PT Application Inspector

— Сканер безопасности Web-приложений в режиме «черного ящика»
  - Входит в состав XSpider/MaxPatrol с 2005 года, в 2013 полностью обновлен

— Система статического/динамического и интерактивного анализа исходных кодов (2013)

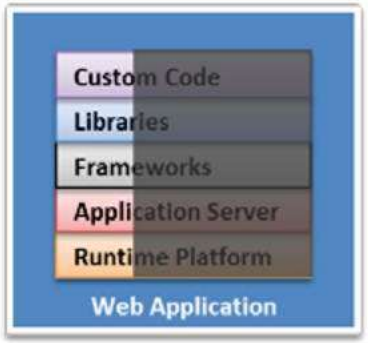


Проблемы анализа кода

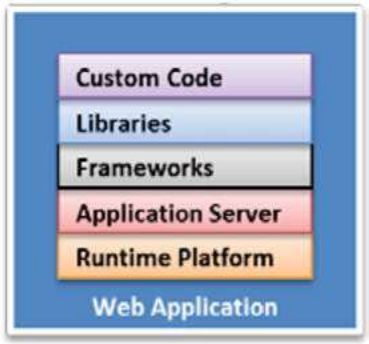
— Черный ящик – комбинаторный взрыв

— Белый ящик – теорема Райса

SAST



DAST



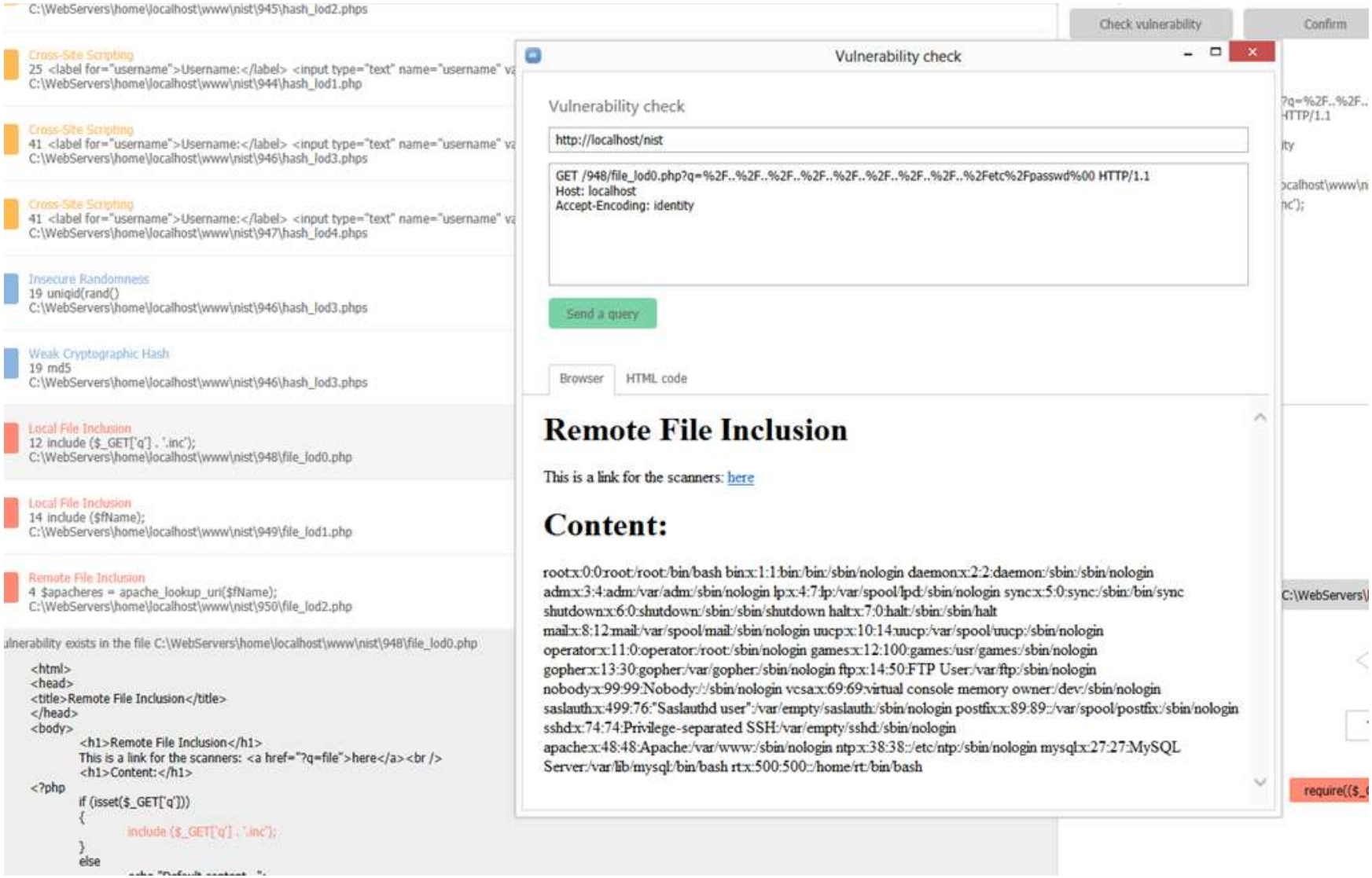
IAST

Наш подход

— Найти то, что есть

— Сделать попроще

Генерация эксплойтов



Генерация эксплойтов

— Автоматическая генерация возможных векторов атак

— Учёт механизмов фильтрации и островных грамматик

Результат:

— Облегчение процесса тестирования

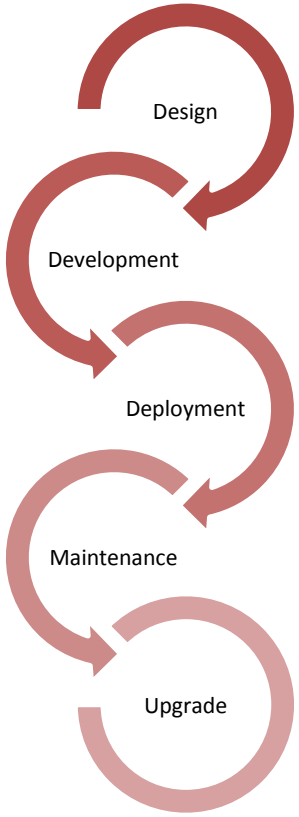
— Необязательно понимать код

— Автоматизированная верификация

Usecase 1: Smoketest

PT Application Security Suite – Вместе, а не «Вместо»

+ Application Security Suite - инструменты, для комплексного решения проблем с уязвимостями приложений



+ PT AI

+ PT AF

+ PT AF & PT AI

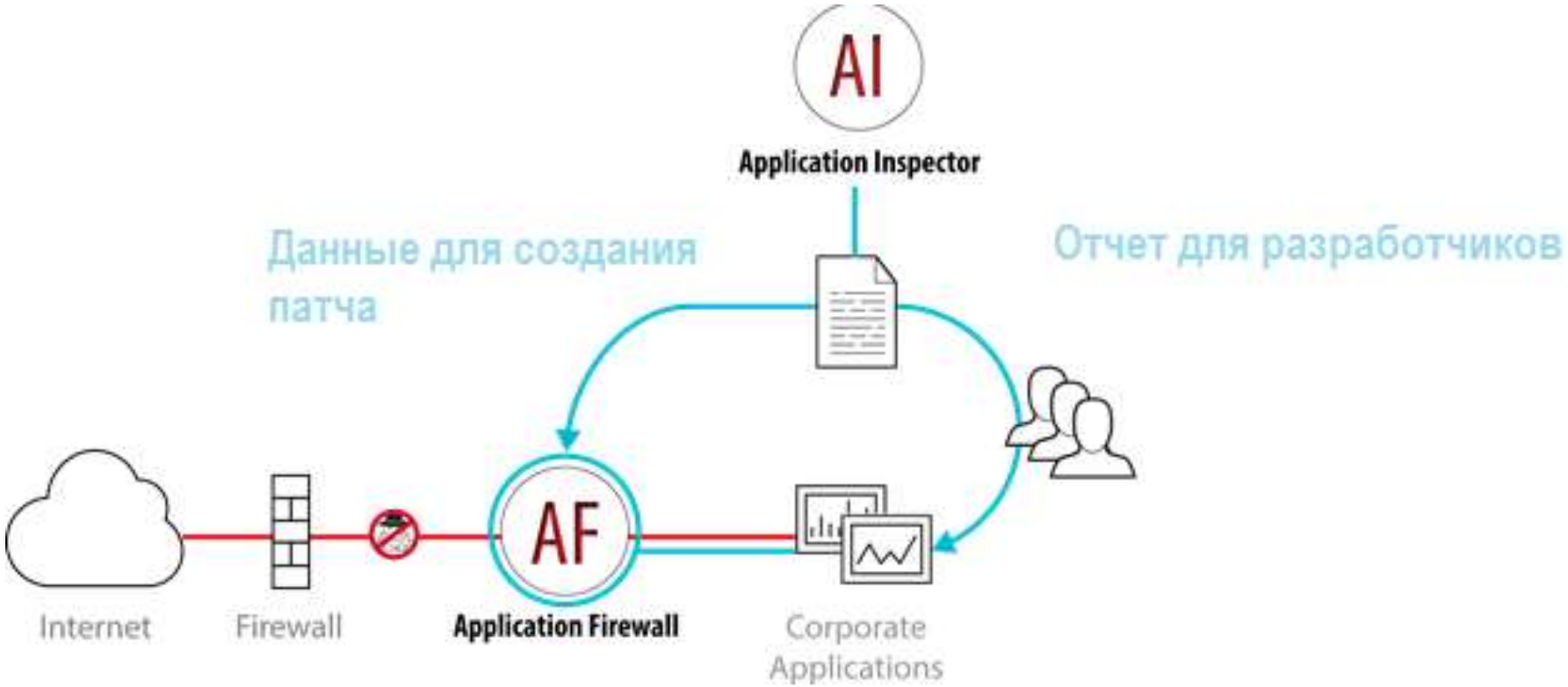
+ PT AF & PT AI

+ PT Application Inspector – Анализатор исходных кодов

+ PT Application Firewall – решение для защиты корпоративных приложений

+ Защита на всех этапах жизненного цикла – от разработки до снятия с эксплуатации

Связка из Application Inspector и Application Firewall



Usecase 2: Bug Bounty

Новосибирск

Конец рассказа
Спасибо за внимание

Евгений Миньковский

Ведущий консультант

Positive Technologies

eminkovskiy@ptsecurity.com

POSITIVE TECHNOLOGIES