positive technologies

Application Inspector 4

АНАЛИЗИРУЕТ ИСХОДНЫЙ КОД. ТОЧНО ВЫЯВЛЯЕТ УЯЗВИМОСТИ. ВСТРАИВАЕТСЯ В ТЕКУЩИЕ ПРОЦЕССЫ РАЗРАБОТКИ.

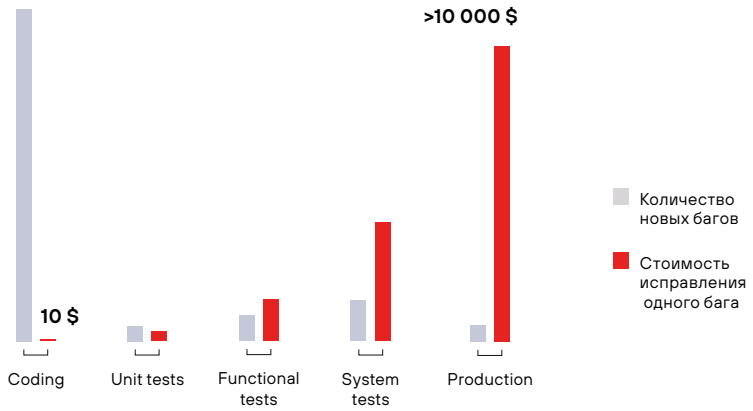
PT Application Inspector —

инструмент, который выявляет уязвимости как в исходном коде, так и в работающем приложении, позволяет устранить их на ранней стадии, поддерживает процесс безопасной разработки.

Веб-приложения по-прежнему остаются популярной целью для злоумышленников. Наши исследования показали, что каждая пятая атака направлена на веб-ресурсы организаций, чаще всего — государственных и финансовых учреждений, онлайн-сервисов, научных организаций и IT-компаний.

Атакующие эксплуатируют имеющиеся в организации уязвимости. В среднем в одном приложении их больше двух десятков, пятая часть из которых опасные. Если злоумышленник использует их во время атаки, компания может столкнуться с реализацией серьезных финансовых и репутационных рисков: кражей важных данных, проникновением в инфраструктуру, простоями или полной остановкой информационных систем.

Большинство уязвимостей содержатся в исходном коде, и лучше устранить их на самых ранних этапах создания приложения. Такой подход на порядок эффективнее, чем устранение уязвимостей на стадии эксплуатации.



Стоимость устранения дефекта на разных стадиях жизненного цикла приложения (Applied Software Measurement, Capers Jones)

Бесплатный пилот.

Проверьте уязвимость вашего кода — закажите бесплатный пилотный проект PT Application Inspector.

Преимущества продукта

Комбинирует четыре технологии анализа — статистический (SAST), динамический (DAST), интерактивный (IAST), а также анализ сторонних компонентов (SCA). Комбинация позволяет охватить максимальное количество уязвимостей, а гибкая система фильтрации дает возможность приоритизировать их по уровню опасности.

Генерирует тестовые эксплойты, позволяющие проверить возможность эксплуатации уязвимости. Учитывает грамматику, фаззинг в среде выполнения. Это экономит трудозатраты команд разработки на подтверждение уязвимостей.

Поддерживаемые языки: Java, PHP, C#, Visual Basic .NET, JavaScript, TypeScript, Python, Kotlin, Go, C/C++, Objective-C, Swift, SQL (T-SQL, PL/SQL, MySQL)

Развертывание: Linux + Docker containers + SSO (SAML, OpenID Connect, LDAP)

Интеграции CI/CD: Jenkins, TeamCity, GitLab CI (CLI), Azure

Интеграции IDE: JetBrains, Visual Studio Code

Интеграция баг-трекеров: Jira

API: REST API (Swagger)

Удобная и прозрачная система лицензирования позволяет включить в работу всю команду в неограниченном количестве проектов.

Эффективно встраивается в процессы разработки. Поддерживает интеграции с Jenkins, TeamCity, GitLab CI, Azure, имеет ролевую модель разграничения доступа, а также готовые плагины для подключения к системам сборки и доставки приложений, баг-трекерам и средам разработки (IDE).

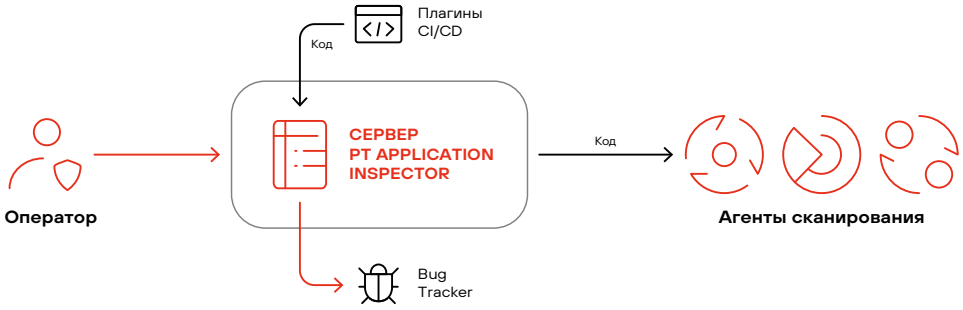
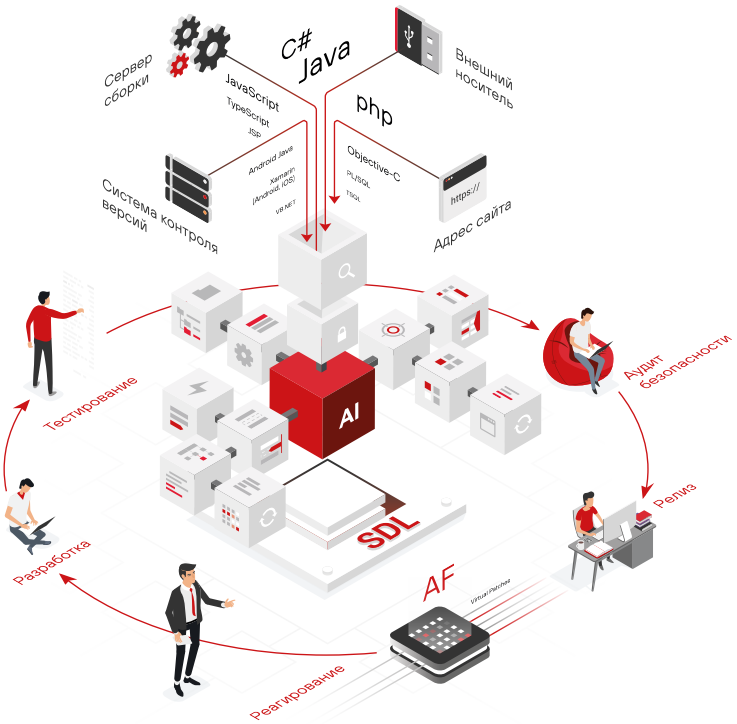


Схема встраивания PT Application Inspector в существующий процесс разработки

Как работает



PT Application Inspector — единственный анализатор исходного кода на российском рынке, предоставляющий удобные инструменты для автоматического подтверждения уязвимостей, что существенно экономит трудозатраты и облегчает взаимодействие специалистов по ИБ с разработчиками.

Абстрактная интерпретация

Поиск по шаблону

Проверка конфигурации

Анализ сторонних компонентов

Динамический анализ

Автоматическая проверка с помощью эксплойтов

ptsecurity.com
pr@ptsecurity.com

Positive Technologies — ведущий разработчик решений для информационной безопасности. Уже 21 год наша основная задача — предотвращать кибератаки до того, как они причинят неприемлемый ущерб бизнесу и целым отраслям экономики.Наши технологии и сервисы используют более 2900 организаций по всему миру, в том числе 80% компаний из рейтинга «Эксперт-400». Positive Technologies — первая и единственная компания из сферы кибербезопасности на Московской бирже (MOEX: POSI).

Следите за нами в соцсетях (Telegram, ВКонтакте, Twitter, Хабр) и в разделе «Новости» на сайте ptsecurity.com, а также подписывайтесь на телеграм-канал IT's positive investing.

PT-AI_PB_A4.RUS.0012.23.FEB.13.2023