

PT Application Inspector

AppSec-платформа для управления рисками безопасности приложений, процессами безопасной разработки и цепочек поставок ПО

Уязвимости в коде остаются ключевым вектором атак на веб-приложения. Эффективная защита требует анализа исходного кода с низким уровнем ложных срабатываний. PT Application Inspector за счёт комбинации статического и динамического анализа выявляет реальные угрозы, сокращая время на реагирование и снижая нагрузку на команды AppSec.

SAST

Высокое качество и достоверность результатов сканирования исходного кода приложения за счет большого набора и комбинации алгоритмов анализа.

Поддержка языков: Java, Scala, C#, PHP, JavaScript, TypeScript, Python, C/, C++, Go, Ruby, Kotlin, Objective-C, Swift, SQL, Solidity, 1C

DAST

Корреляция результатов статического и динамического анализа помогает быстрее выявлять действительно опасные уязвимости, не тратя время на проверку ложных срабатываний.

SCA

Находит уязвимости в зависимостях и проверяет, реально ли уязвимая функция вызывается в коде. Меньше шума, точнее приоритизация

Что нового в релизе 6.0

■ MOLOT

Новый модуль на базе ML для обнаружения недеklarированных возможностей: закладок в коде, подозрительной логики и потенциально вредоносных конструкций, недоступных для выявления классическими методами анализа.

■ Сервис управления сканированиями

Централизованное управление очередями, приоритетами и ресурсами агентов. Критически важные изменения проверяются вне очереди

■ Поддержка языка 1C

Анализ приложений, написанных на языке 1C версии 8.3 и ниже методом taint-анализа.

■ Безопасность конфигураций

Выявление небезопасных настроек и ошибок конфигураций в приложениях и инфраструктуре

■ Поиск секретов в коде

Выявление паролей, токенов доступа, ключей и других конфиденциальных данных в коде

Современные атаки начинаются не только с уязвимостей



60%

проникновений происходят через веб-приложения

29%

уязвимостей эксплуатируются в день публикации

Open source, CI и CD стали новой целью атакующих

OAuth-токены и API-ключи активно используются для компрометации инфраструктуры

Ключевые преимущества PT Application Inspector



Централизованный контроль безопасности приложений

Проверяет исходный код, зависимости, конфигурации, секреты и подозрительную логику в рамках одной платформы до того, как приложение попадет в продуктивную среду. Меньше интеграций и затрат на поддержку. Единая картина уязвимостей для всей команды



Сервис управления сканированиями

Управляет очередями сканирования, приоритетами и ресурсами агентов. Критически важные изменения проверяются быстрее и не ждут в общей очереди. Безопасность меньше влияет на сроки выпуска новых версий продукта



Выявление секретов в коде

Ищет пароли, токены, API-ключи и другие конфиденциальные данные в коде. Анализ потоков данных обеспечивает высокую достоверность результатов, которая недоступна при сигнатурном анализе. Предотвращает утечку учетных данных для доступа к системам, облачным сервисам и конфиденциальной информации, снижая риски компрометации инфраструктуры



MOLOT

Использование ML-компонента позволяет находить в коде подозрительную логику работы алгоритма, для выявления которой плохо применимы классические методы статического анализа. Это предотвращает преднамеренное внедрение вредоносного кода, способного нарушить безопасность приложения



Кастомизация продукта

PT Application Inspector можно настроить под индивидуальные задачи компании за счет разработки собственных правил поиска уязвимостей на встроенном языке DSL, использования шаблонов отчетов, а также обращений к открытому API



Поиск сторонних компонентов с условиями достижимости

PT Application Inspector не просто находит сторонние компоненты с известными уязвимостями, а проверяет, реально ли уязвимая функция вызывается в коде приложения. Это повышает точность срабатываний и сокращает время на триаж: команда работает только с теми недостатками, которые могут быть эксплуатируемы

Запишитесь на «пилот» и протестируйте **PT Application Inspector** для выявления уязвимостей в коде приложения



Подробнее
о продукте