APPSEC SOLUTIONS

Кратко о российской безопасной разработке

На базе продуктов AppSec Solutions

Мы работаем вместе с вами

Андрей Юрченко

Руководитель группы развития продаж
AppSec Solutions

APPSEC SOLUTIONS

Частые предпосылки для РБПО

Бизнес

- Требования регулятора выполняются частично / с нарушениями / несистемно
- Данные для принятия решений собираются и обрабатываются вручную
- Данные являются неактуальными на момент обработки

- Compliance формален
- Негативное влияние на скорость релизов
- Отчёты «ручные»

Безопасность

- Разработка не принимает во внимание вопросы безопасности
- Тесты безопасности проводятся в ручном режиме или не проводятся вообще

- Разработка игнорирует
- Безопасность лоскутная

Разработка

- Безопасность «мешает» и тормозит разработку
- Проблемы безопасности возвращаются после теста множественными табличными документами без учета ранее выставленных, принятых и/или отвергнутых комментариев и поправок

- ИБ «мешает»
- В отчёте — «уязвимости»
- «Костыльное» исправление уязвимостей приводящее к деградации качества ПО

APPSEC SOLUTIONS

Цели РБПО

Скорость реализации программного обеспечения (Time-to-market)

- Снизить время вывода на рынок защищенных программных продуктов;
- Наращивать объемы выпуска бизнес-функций, сохраняя качество и защищенность ПО на индустриальном уровне;
- Реализовать для разработчиков прозрачный процесс оперативного и бесшовного внесения любых ИБ-изменений в ПО.

APPSEC SOLUTIONS

Цели РБПО

Соответствие требованиям регуляторов и индустриальных стандартов (Compliance)

- Обеспечить контроль уровня соответствия процессов индустриальным стандартам;
- Обеспечить соответствие ПО регуляторным требованиям;
- Обеспечить лицензионную частоту используемых компонент с открытым исходным кодом;
- Обеспечить контроль рисков кибербезопасности ПО.

APPSEC SOLUTIONS

Цели РБПО

Непрерывность и защищенность цифрового бизнеса (Digital Business Continuity & Security)

- Повысить киберустойчивость программных продуктов и цифровых сервисов;
- Снизить уровень подверженности рискам безопасности ПО;
- Обеспечить снижение плотности уязвимостей в коде программных продуктов;
- Реализовать проактивное выявление уязвимостей ПО на ранних стадиях разработки;
- Повысить скорость устранения технического долга дефектов ИБ.

APPSEC SOLUTIONS

Цели РБПО

Зрелость технологий и процессов разработки защищенного ПО (Development Maturity)

- Повысить продуктивность разработчиков при создании защищенного ПО;
- Интегрировать непрерывный технологический процесс применения практик анализа защищенности в инженерный конвейер разработки ПО;
- Повысить уровень экспертизы разработчиков в области кибербезопасности;
- Снизить стоимость выявления и устранения уязвимостей.

Портфель продуктов

APPSEC SOLUTIONS

OSA

Анализ библиотек с открытым исходным кодом

Open-Source Analysis

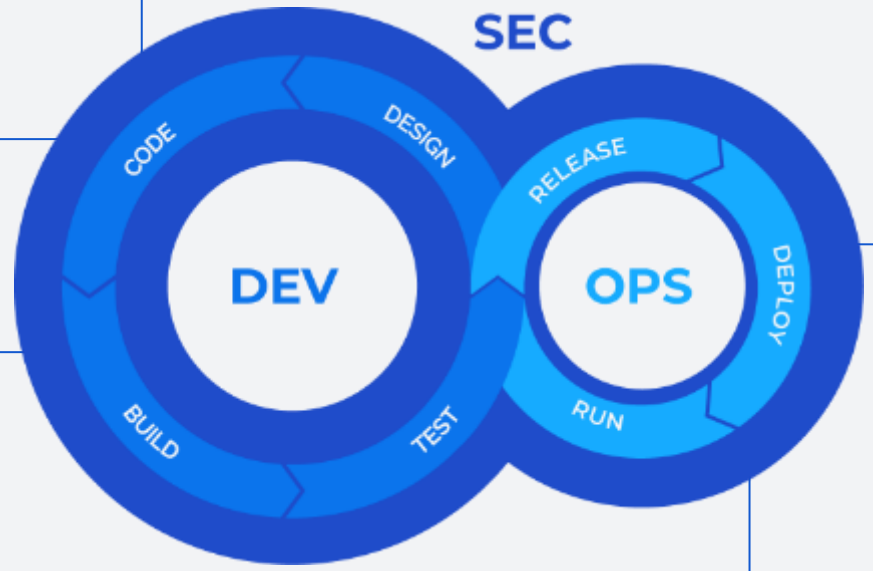
APPSEC.TRACK

SCM

Контроль исходного кода

Source Code Management

APPSEC.CODE



SCA

Компонентный анализ ПО

Software Composition Analysis

APPSEC.TRACK

MAST

Анализ защищенности мобильных приложений

Mobile Application Security Testing

СТИНГРЕЙ

ASPM

Управление состоянием безопасности приложений

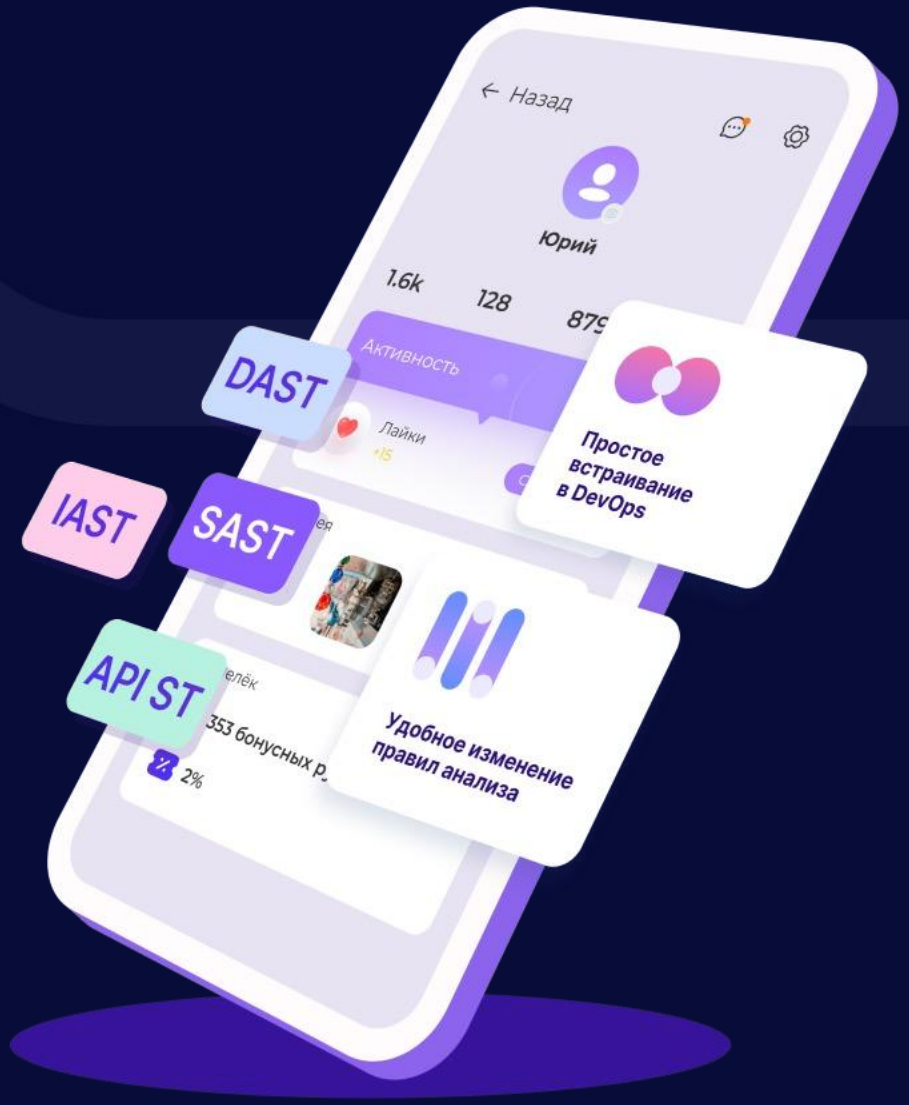
Application Security Posture Management

APPSEC.HUB

Российское Программное Обеспечение

СТИНГРЕЙ

Платформа автоматизированного анализа защищенности мобильных приложений



Свидетельство о регистрации в Федеральной службе по интеллектуальной собственности: 2020660236

Регистрационный номер в реестре российского ПО Министерства Цифрового Развития РФ: 7699

Распространенные заблуждения о безопасности мобильных приложений

СТИНГРЕЙ

- ☒ Мобильное приложение – это только один пользователь и его безопасность;
- ☒ Приложение – это всего лишь витрина данных для серверной части системы;
- ☒ Приложения и так проверяются на стороне Google и Apple перед публикацией;
- ☒ Мобильные приложения не попадают под требования регуляторов;
- ☒ Атаки на мобильные приложения могут повлечь за собой не самый большой ущерб, который покроется рисками;
- ☒ У мобильных приложений узкий вектор атаки, для которого часто необходим физический доступ, а значит, клиент будет виноват сам.

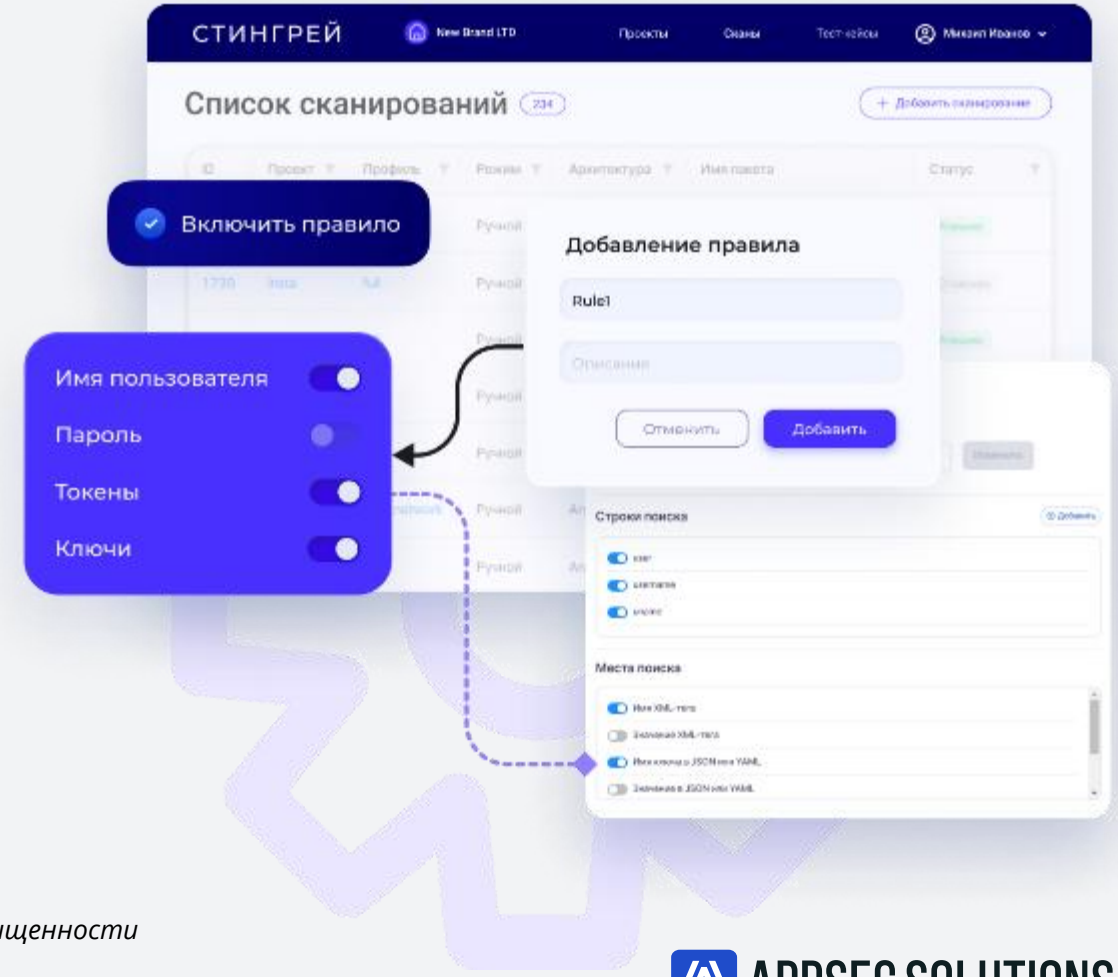
Незащищенные цифровые продукты могут стать легкой добычей для мошенников.

APPSEC SOLUTIONS

Стингрей– лучшая на рынке* платформа автоматизированного анализа защищенности мобильных приложений

СТИНГРЕЙ

- Не только выявляет уязвимости в iOS и Android-приложениях, но и предлагает подробные рекомендации по их устранению
- Снижает на 60% затраты на обеспечение безопасности за счет автоматизации и комплексного анализа



По данным конкурентного мониторинга российских и западных решений для анализа защищенности мобильных приложений, Стингрей Технолоджиз, Февраль 2023

APPSEC SOLUTIONS

1 Высокое качество анализа

Стингрей комбинирует и коррелирует ключевые практики анализа защищенности:
DAST, SAST / BCA, IAST, API ST

2 Простота и информативность

Стингрей выполняет анализ без использования исходного кода и предоставляет детальные рекомендации по устранению найденных уязвимостей.

3 Автоматизация

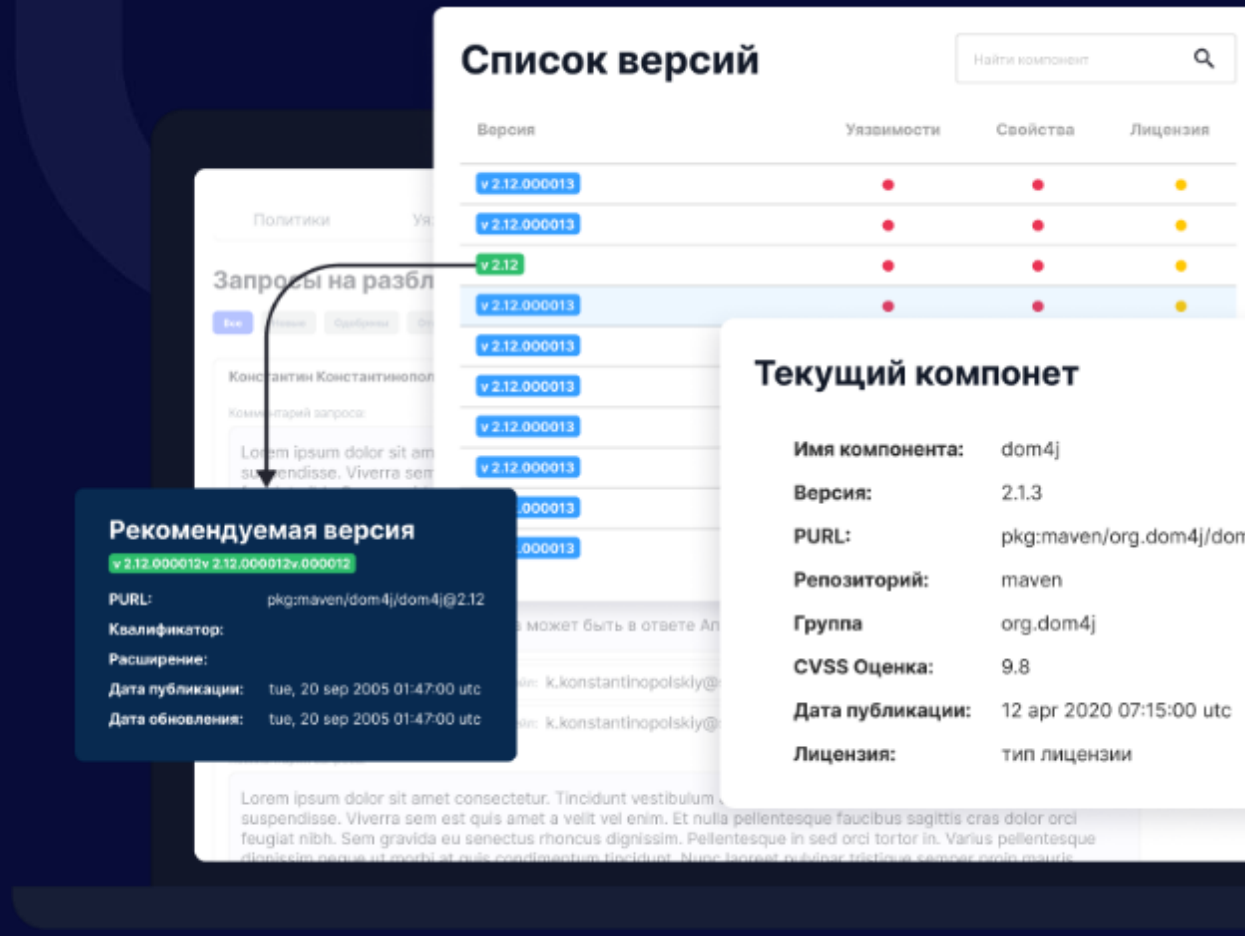
Стингрей автоматизирует ручное тестирование за счет разового создания тест-кейсов и возможности их переиспользования. Быстро внедрить, легко управлять. Платформа поддерживает интеграцию с Appium.

4 Мониторинг

Стингрей умеет самостоятельно отслеживать выпуск новых версий в магазинах приложений и автоматически проверять их.

APPSEC.TRACK

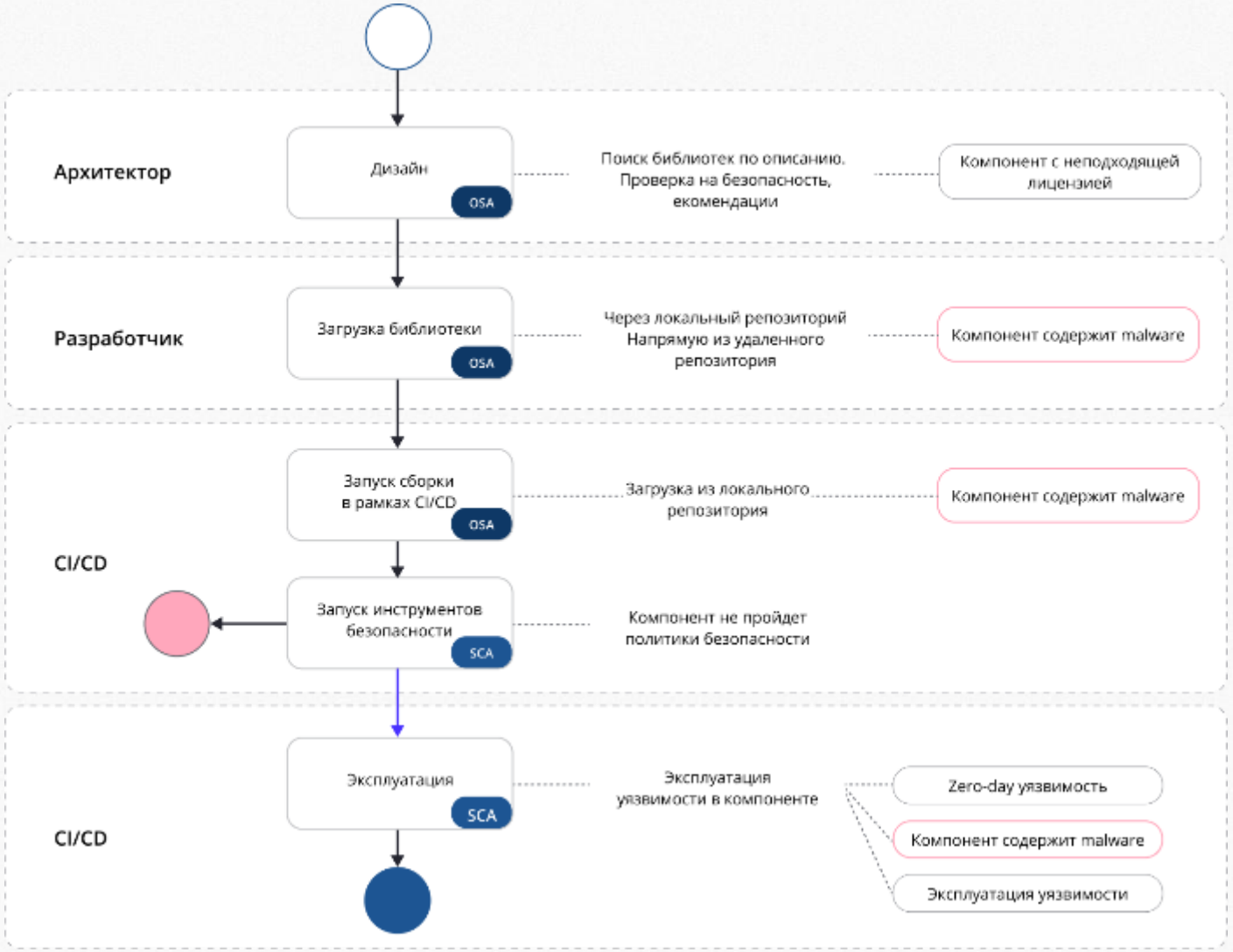
Сервис предотвращения атак на цепочку поставок ПО через компоненты с открытым исходным кодом



Проблемы OSS

- Выбор компонента с неподходящей лицензией;
- Выполнение вредоносных/нежелательных действий на машинах разработчиков, агентах CI/CD, стендах приложений;
- Эксплуатация известных уязвимостей;
- Эксплуатация неизвестных (zero-day) уязвимостей.

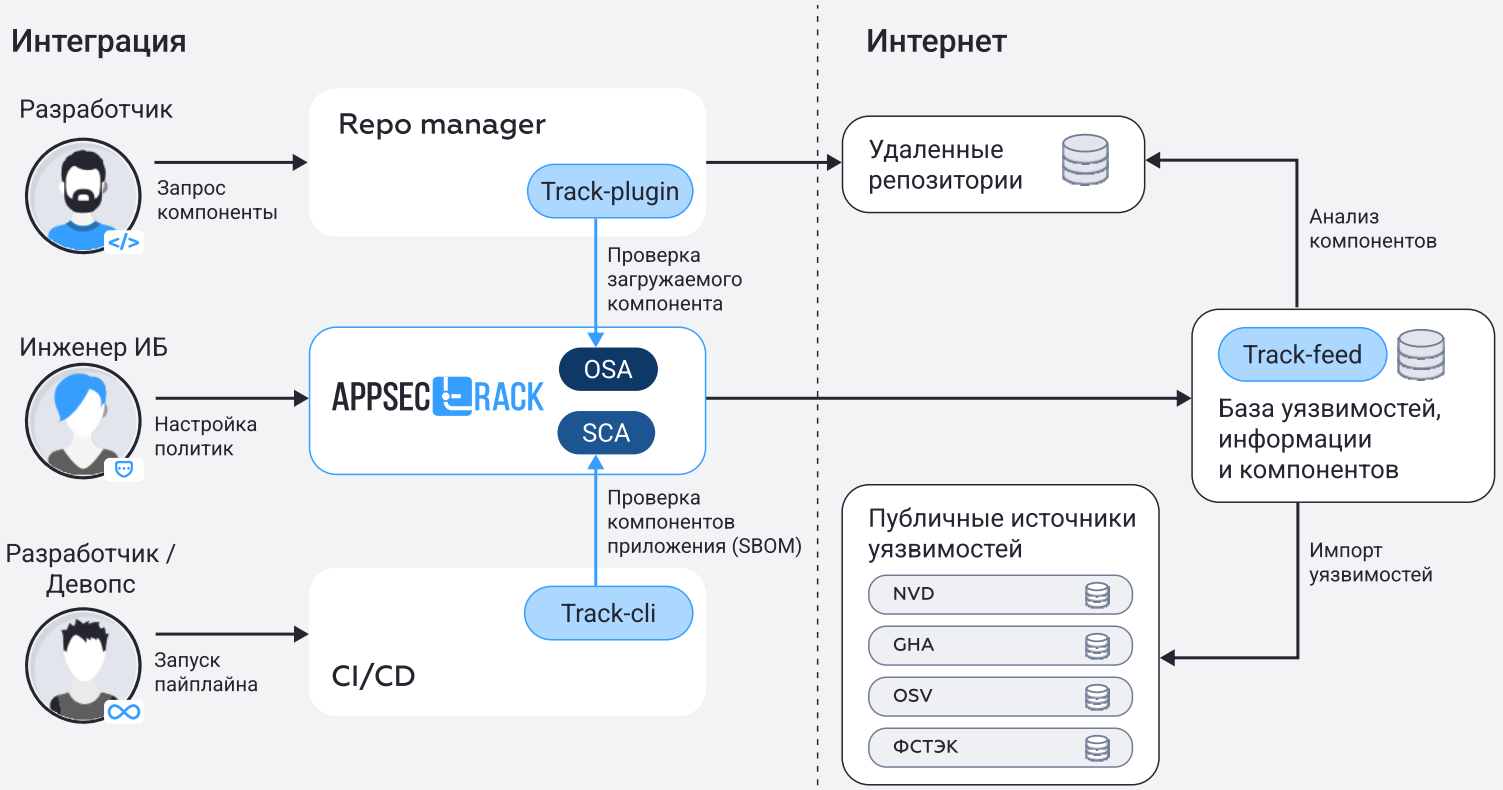
> Malware/Protestware зачастую не требуют специфических условий эксплуатации, могут выполняться без дополнительных команд и потока данных от злоумышленника.



Архитектура системы

APPSEC.TRACK

Система поставляется в виде комплекта Docker-образов, может быть запущена как в рамках k8s-кластера, так и на отдельное машине через Docker Compose. Загрузка информации об уязвимостях и компонентах происходит с облачного источника Track-Feed.



Особенности

- Образы на базе Astra Linux
- Работа в режиме HA
- Работа в внешней БД (PostgreSQL)

Track.Feed

- Собственная проприетарная база зловредных компонентов
- Импорт уязвимостей из публичных баз
- Автоматический анализ Python и на наличие признаков Malware/Protestware

APPSEC SOLUTIONS

AppSec.Track. Модуль OSA

APPSEC.TRACK

Реализация практики Open Source Analysis.

Проверка компонентов с открытым исходным кодом на этапе загрузки в контур безопасной разработки. При нарушении политик разработчик получает сообщение об ошибке с описанием и рекомендациями по выбору безопасной версии.

Функциональные возможности

- Защита от вредоносных, уязвимых и protestware компонентов;
- Блокировка загрузки неизвестных и измененных компонентов;
- Настройка политик для отдельных репозиториев и менеджеров репозиториев;
- Поддержка ключевых менеджеров артефактов: Nexus Repository, JFrog Artifactory.

Особенности

- Возможность запроса разработчиком разблокировки необходимого компонента;
- Рекомендации по выбору безопасной версии компонента;
- Инсталляция в менеджеры артефактов в виде плагина, не требующая изменения существующих CI/CD процессов.

APPSEC SOLUTIONS

AppSec.Track. Модуль SCA

APPSEC.TRACK

Реализация практики Software Composition Analysis.

Проверка компонентов с открытым исходным кодом в рамках пайплайнов сборки и доставки приложения.
При нарушении политик происходит блокировка пайплайна, а также отправка уведомлений командам разработки и безопасности.

Функциональные возможности

- Выполнение сканирования OSS-компонентов приложений на этапах Build и Deploy;
- Интеграция в пайплайны с помощью инструмента CLI;
- Настройка политик и исключения для отдельных команд и приложений;
- Формирование отчетов по проведенным сканированиям.

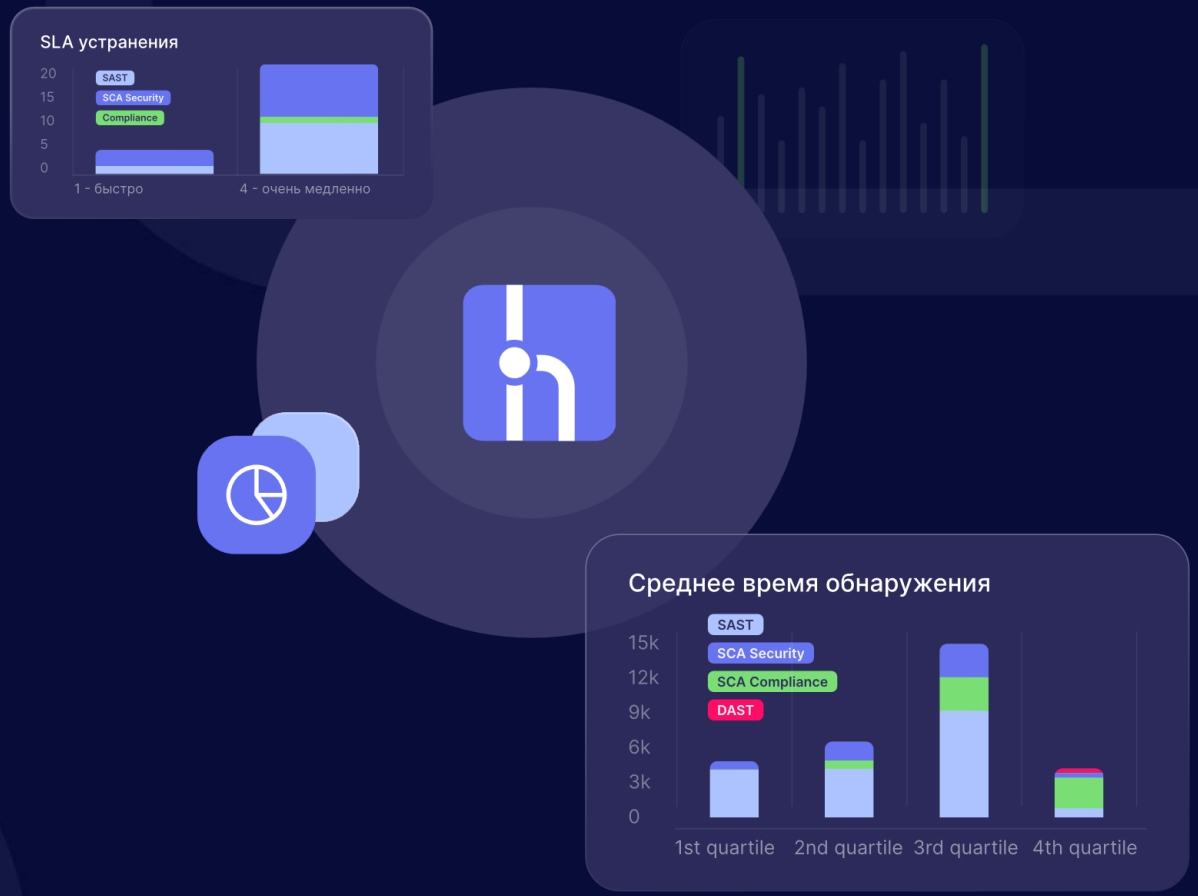
Особенности

- Сканирование файлов манифестов (pom.xml, build.gradle, package.json, go.sum и т.д.);
- Сканирование файлов артефактов (.jar, .war, .whl, .tar и т.д.);
- Сканирование образов Docker;
- Сканирование файлов SBOM (CycloneDX).

APPSEC SOLUTIONS

APPSEC.HUB

Инструменты непрерывной интеграции безопасности и управления уязвимостями

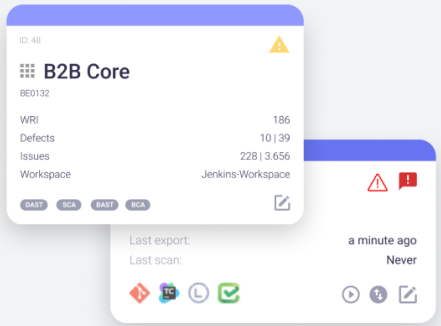


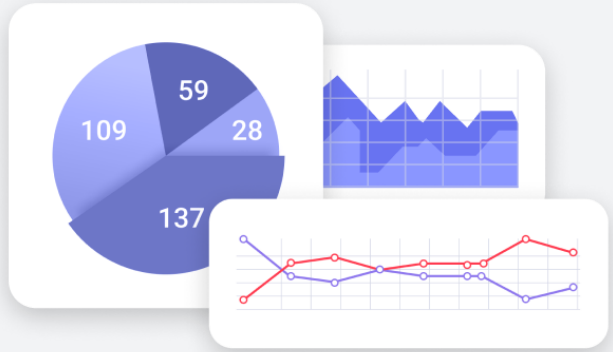
Функциональные домены AppSec.Hub

APPSEC.HUB

Оркестрация

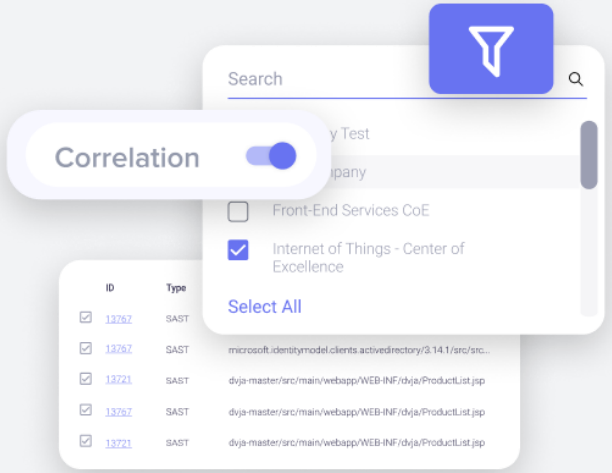
Создание ИБ-конвейеров (пайплайнов) и управление ими, настройка AST-инструментов





Аналитика

Управление процессом DevSecOps на основе сформированных метрик



Корреляция

Анализ и приоритезация уязвимостей ПО, группировка ошибок в дефекты ИБ, синхронизация данных с дефект-менеджмент системами

APPSEC SOLUTIONS

Ключевые особенности

APPSEC.HUB APPSEC SOLUTIONS

1 Стратегический уровень

- Автоматизированное выполнение требований регуляторов и корпоративных политик ИБ и разработки;
- Управляемая трансформация процессов безопасной разработки ПО;
- Быстрый запуск инициативы РБПО в корпоративном масштабе.

2 Управленческий уровень

- Сокращение расходов на устранение риска ИБ, дефектов ИБ, времени вывода новых продуктов;
- Отслеживание исполнения дорожной карты для внедрения методов РБПО;
- Обеспечение прозрачного управления ИБ с помощью KPI на основе инструментов бизнес анализа.

3 Операционный уровень

- Обеспечение Plug&Play подключений к существующим и новым разрозненным инструментам РБПО;
- Инструментальный контроль снижения риска и других Бизнес и DevOps показателей эффективности безопасной разработки на основе метрик процесса безопасной разработки, зрелости отдельных практик, производительности РБПО процесса и состояния защищенности программных продуктов.

APPSEC.HUB

Обработка результатов сканирования (многократные сканирования в день)

Минимизация трудозатрат AppSec-инженеров и разработчиков

APPSEC.HUB

Метрики РБПО: покрытие практиками

Оценка картины покрытия систем и подсистем практиками ИБ

Частота сканирований

Aug 2023

63

+57.5% от прошлого месяца

Среднее время успешных сканирований

Aug 2023

1m 57.5s

-68.0% от прошлого месяца

Коэффициент пройденных контрольных точек

Aug 2023

23%

-43.2% от прошлого месяца

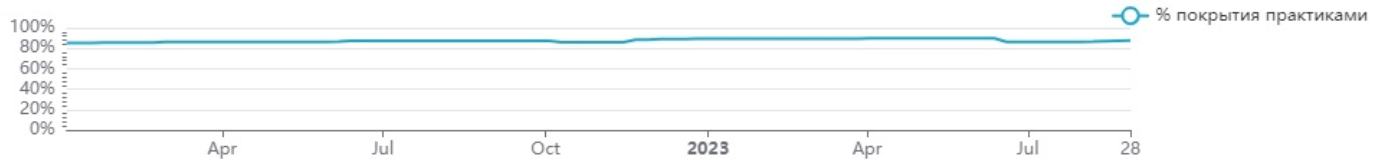
Покрытие пайплайнами | Применение практик ИБ

Покрытие практиками AppSec

87.6%

на текущую дату/конец периода

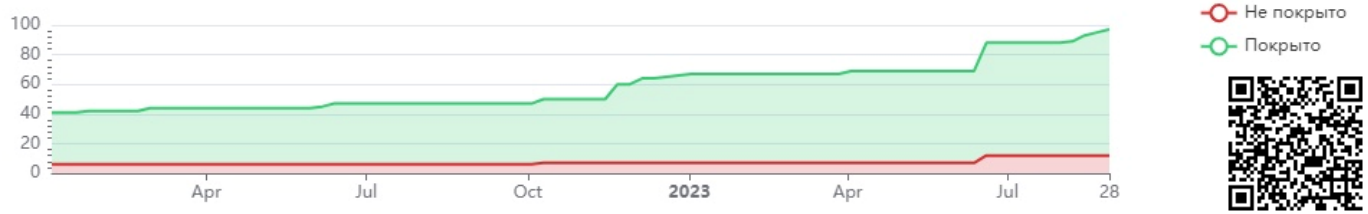
% покрытия, динамика



–

Тип эл-та	Кол-во элементов	% покрытия практиками
Кодовая база	55	92.73%
Артефакт сборки	35	80.00%
Стенд	7	85.71%

Покрытые практиками элементы, динамика

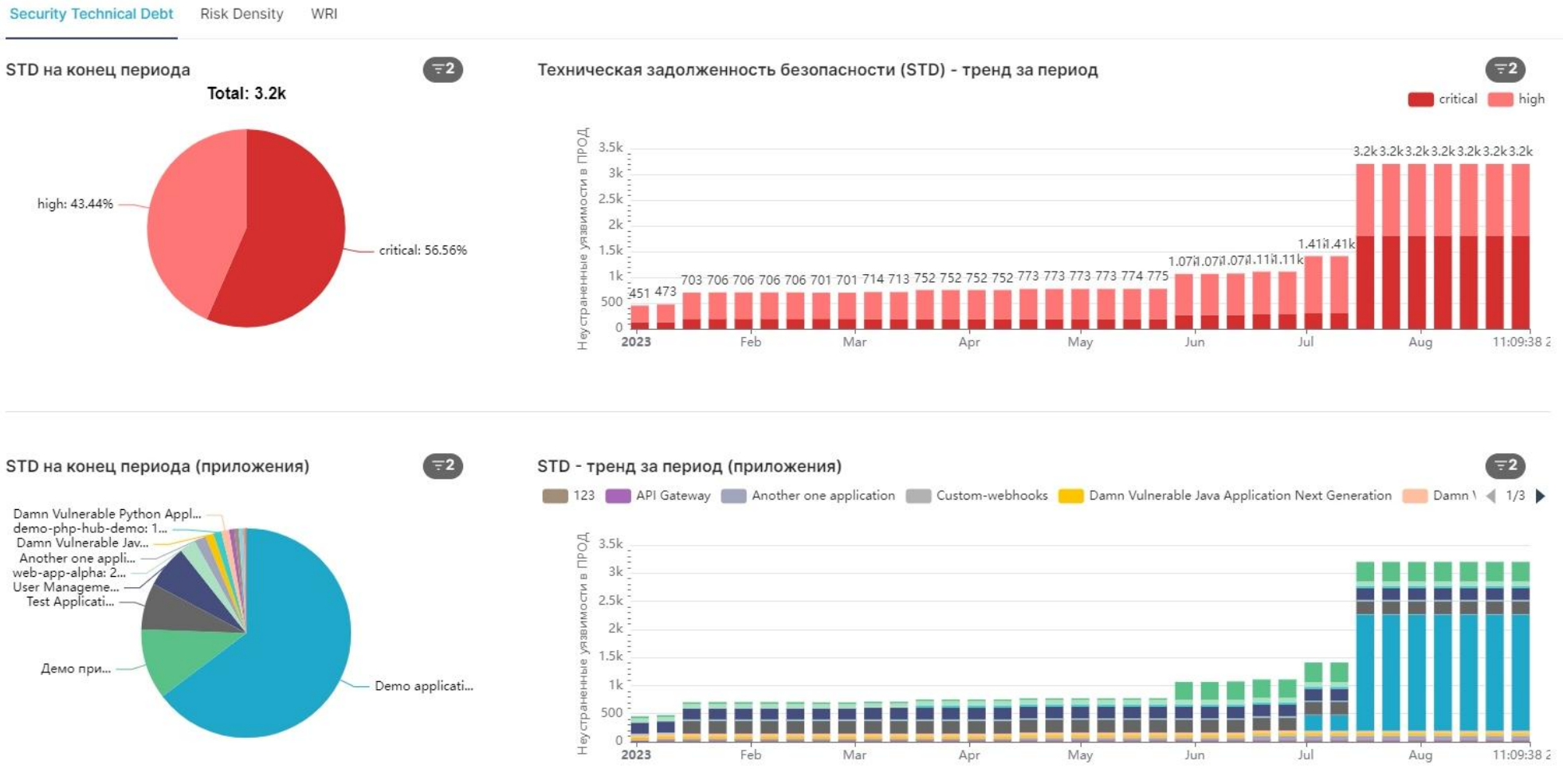


APPSEC SOLUTIONS

APPSEC.HUB

Метрики РБПО: технический долг ИБ

Базовая и наиболее интуитивно понятная метрика для оценки риска ИБ



APPSEC SOLUTIONS

ASPM/ASOC — управление инструментальными практиками ИБ

APPSEC.HUB

Метрики РБПО: раннее обнаружение и устранение

Оценка текущей нагрузки на команду разработки и ресурсов для исправления проблем ИБ

Достаточен ли shift-left?

MTTD (дни)

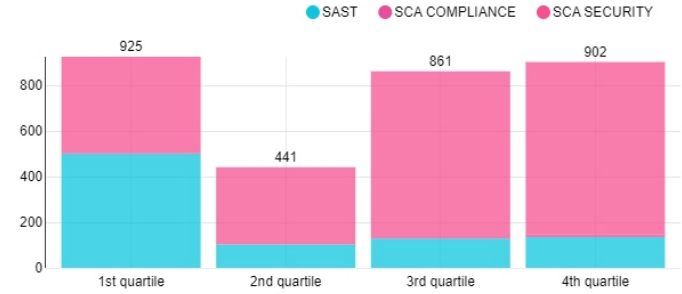
15.99

за выбранный период

Обнаруженные уязв-ти

Total: 3.13k

Стадия обнаружения уязвимостей (Практика ИБ)



Справляется ли AppSec команда?

MTT (дни)

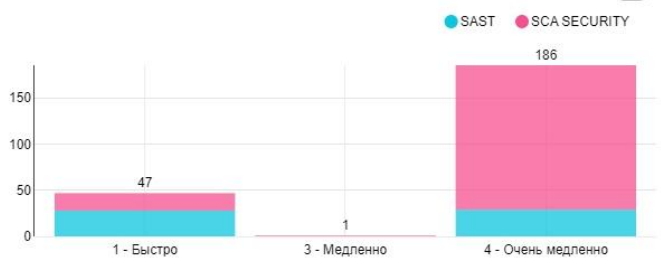
99.45

за выбранный период

Проанализированные уязв-ти

Total: 233

SLA триажа (практика ИБ)



Справляется ли Dev команда?

MTTR (дни)

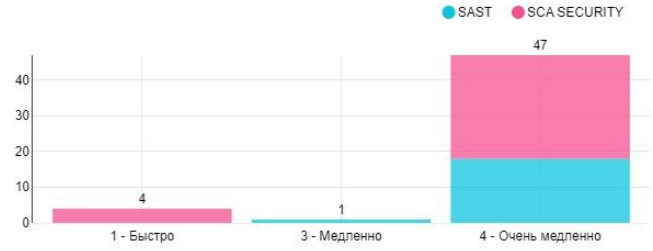
56.30

за выбранный период

Устраненные уязв-ти

Total: 52

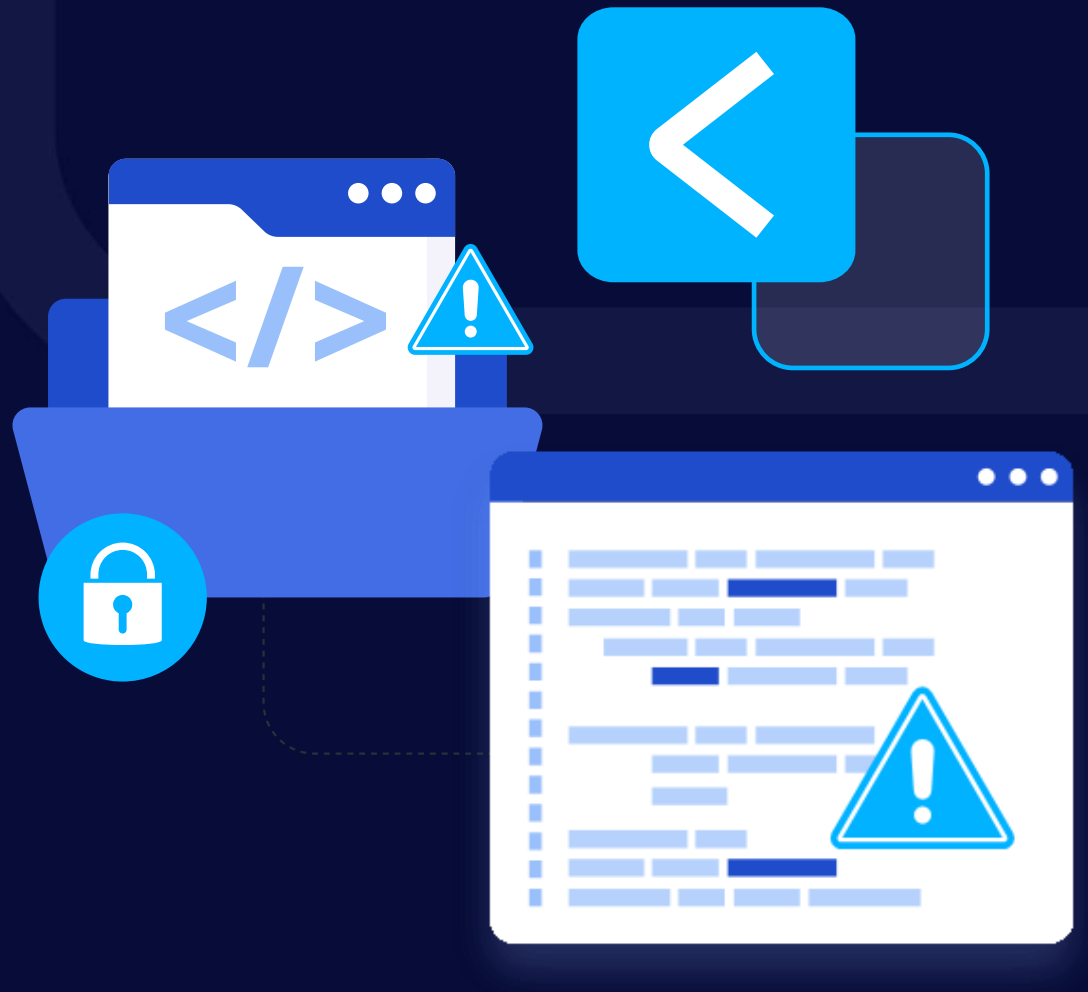
SLA устранения (практика ИБ)



APPSEC SOLUTIONS

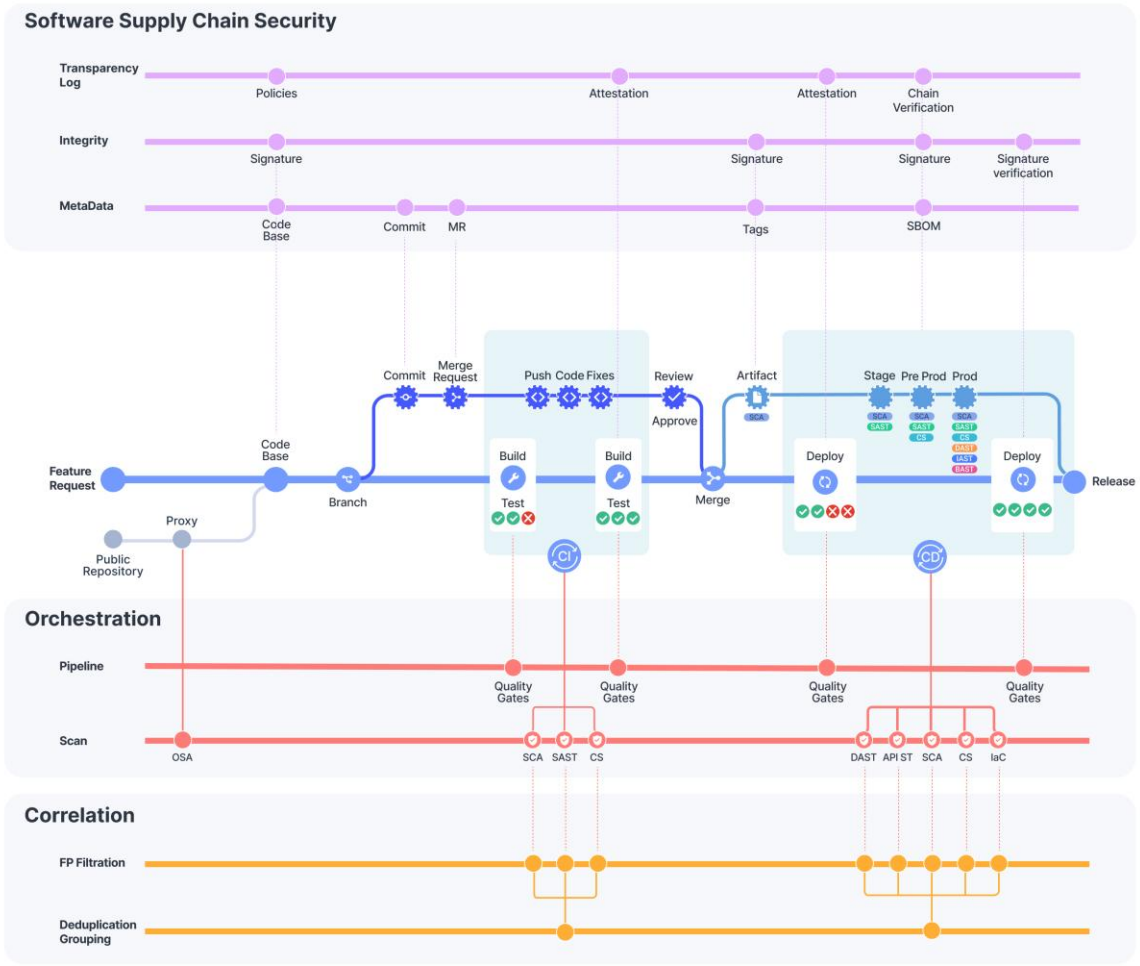
APPSEC.CODE

**Российский продукт
для управления
исходным кодом
и разработки защищенного ПО**



Единая CI/CD платформа для создания защищенного исходного кода

APPSEC.CODE



- AppSec.Code обеспечивает бесперебойную совместную работу над кодом и непрерывные рабочие процессы интеграции и развертывания благодаря надежной системе контроля версий и расширенным возможностям CI/CD-конвейера.
- AppSec.Code предоставляет разработчикам единую инфраструктуру для совместной работы над кодом оптимизируя DevOps-процесс, повышая качество кода, сохраняя целостность и обеспечивая защищенность разрабатываемого программного обеспечения при помощи бесшовной интеграции с AppSec.Hub.

APPSEC SOLUTIONS

Ключевые возможности

APPSEC.CODE

Разработка

- Совместная работа над исходным кодом
- Единая среда контроля версий
- Прозрачное управление ветками кода

Сборка

- Интеграция с Git
- Единый конвейер сборки
- Хранилище Docker-образов

Выпуск релизов

- Автоматизация операций по сборке и установке релизов
- Полноценный CI/CD конвейер
- Доставка и установка релизов на необходимое количество серверов

Масштабируемость

- Балансировщик нагрузки для PostgreSQL
- Полноценные функции аудита
- Поддержка нескольких серверов LDAP

Защищенное управление исходным кодом

- Правила согласования для код-ревью
- Push-правила
- Управление доступом к веткам кода
- Блокировка изменений
- Импорт проектов

Нативная интеграция с AppSec.Hub

- Полная настройка и запуск сканирований
- Поддержка всех видов анализа защищенности (SAST, DAST, SCA, CS)
- Интерфейс работы с «очищенными» результатами сканирования
- Удобная навигация по коду

Управление запросами на слияние (MR)

- Обязательные согласователи
- MR-зависимости
- Ревью MR

APPSEC SOLUTIONS

Планы на 2025г.

APPSEC SOLUTIONS

SAST

- Универсальный движок
- Агенты в контейнерах
- Простота и экономия ресурсов

GenAI

- Проверка ML-моделей
- Поиск ошибок кода и уязвимостей
- Снижение вероятности деградации ML

Co.Pilot

- Минимизация Falce
- Уменьшение трудозатрат
- Ускорение Time to market

Protector

- Защита мобильных приложений (iOs, Andriod)
- Модификация готового приложения
- Выполнение требований НСПК по защите моб приложений (в процессе тестов)

Прогнозные сроки MVP, выход на PoC

- 2-3Q 2025

Как быть в курсе

- Оставить нам данные с комментариями

Какие преференции

- Ценовые привилегии
- Приоритет бэклога
- PR-активности (по желанию)

Спасибо за внимание!

Андрей Юрченко

Руководитель группы
развития продаж
AppSec Solutions

+7 (925) 094-62-36

ayurchenko@appsec.global

Подписывайтесь
на наш телеграм-канал!