Прорубаем окно в DevSecOps, внедряя ASPM

Артем Пузанков
DevSecOps Cluster Lead

Кто я?

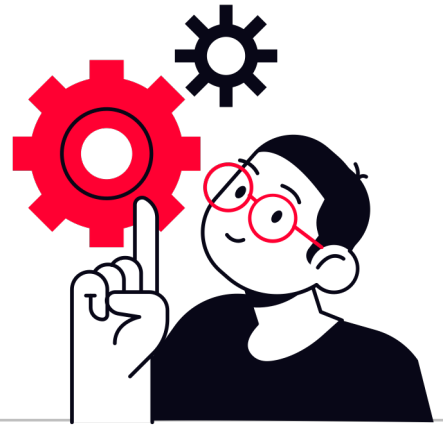
DevSecOps Cluster Lead
в MTC Digital Smarthome & IoT Cluster

- Внедряю инструменты
- Выстраиваю процессы
- Профессионально смотрю дашборды
- Выхожу работать AppSec’ом, а делаю ASPM
- А также делаю что-то ещё

ASPM. Что это и зачем?

КРУТО

Когда у вас есть куча инструментов



СЛОЖНО

Когда появляется необходимость координировать их работу, коррелировать результаты, даже если их всего два, например SAST и DAST

Ручной и полуавтоматический режимы не дают методологии работать эффективно

ASPM. Актуальность проблемы

При построении процесса безопасной разработки часто сталкиваются с некоторыми **серьезными проблемами,** со стороны пользователя платформы и со стороны разработчика платформы

ASPM. Актуальность проблемы

При построении процесса безопасной разработки часто сталкиваются с некоторыми **серьезными проблемами,** со стороны пользователя платформы и со стороны разработчика платформы

1

«Больно» и «со скрипом» интегрируются AST (Application Security Testing) инструменты в DevOps

ASPM. Актуальность проблемы

При построении процесса безопасной разработки часто сталкиваются с некоторыми **серьезными проблемами,** со стороны пользователя платформы и со стороны разработчика платформы

1. «Больно» и «со скрипом» интегрируются AST (Application Security Testing) инструменты в DevOps

2. Сложно управлять разрозненными сканерами и обрабатывать большой поток результатов проверок

ASPM. Актуальность проблемы

При построении процесса безопасной разработки часто сталкиваются с некоторыми **серьезными проблемами,** со стороны пользователя платформы и со стороны разработчика платформы

1. «Больно» и «со скрипом» интегрируются AST (Application Security Testing) инструменты в DevOps

2. Сложно управлять разрозненными сканерами и обрабатывать большой поток результатов проверок

3. Организации сосредоточены на точечной, не масштабируемой автоматизации

ASPM. Актуальность проблемы

При построении процесса безопасной разработки часто сталкиваются с некоторыми **серьезными проблемами,** со стороны пользователя платформы и со стороны разработчика платформы

1. «Больно» и «со скрипом» интегрируются AST (Application Security Testing) инструменты в DevOps

2. Сложно управлять разрозненными сканерами и обрабатывать большой поток результатов проверок

3. Организации сосредоточены на точечной, не масштабируемой автоматизации

4. Интеграции со сканерами стека разработки, либо с инструментами стека эксплуатации. Недостающие возможности интеграции не позволяют сформировать целостную картину о защищенности приложения

ASPM. Актуальность проблемы

При построении процесса безопасной разработки часто сталкиваются с некоторыми **серьезными проблемами,** со стороны пользователя платформы и со стороны разработчика платформы

1. «Больно» и «со скрипом» интегрируются AST (Application Security Testing) инструменты в DevOps

2. Сложно управлять разрозненными сканерами и обрабатывать большой поток результатов проверок

3. Организации сосредоточены на точечной, не масштабируемой автоматизации

4. Интеграции со сканерами стека разработки, либо с инструментами стека эксплуатации. Недостающие возможности интеграции не позволяют сформировать целостную картину о защищенности приложения

Решить вышеперечисленные проблемы и оптимизировать процесс DevSecOps помогает инструмент, реализующего практику **ASPM (Application Security Posture Management)**

Агенда

1. Что такое ASOC идеологически
2. Обзор требований рынка к инструментам оркестрации
3. Краткий обзор существующих решений
4. Сравнение
5. В каком направлении улучшать продукты
6. Советы для:
   - разработчиков решений
   - компаний, которые для своего использования внутри пилят оркестратор
   - пользователей и тех, кто выбирает
7. Выводы

Что такое ASOC идеологически

01

ASPM. Что это и зачем?

Application Security Posture Management, ASPM – практика, которая сочетает в себе:

- Автоматизированную оркестрацию Application Security Tools (AST) ✓
- Управление технологическими пайплайнами инструментов ✓
- Корреляцию результатов работы инструментов ✓
- Сбор метрик о продуктах ✓

Эволюция рынка решений ASOC:

2016

AVC

Gartner определяет как AVC – Application Vulnerability Correlation

ASPM. Что это и зачем?

Application Security Posture Management, ASPM – практика, которая сочетает в себе:

- Автоматизированную оркестрацию Application Security Tools (AST) ✓
- Управление технологическими пайплайнами инструментов ✓
- Корреляцию результатов работы инструментов ✓
- Сбор метрик о продуктах ✓

Эволюция рынка решений ASOC:

2016

AVC
Gartner определяет как AVC – Application Vulnerability Correlation

2017

ASTO
Gartner определяет как ASTO – Application Security Testing Orchestration

ASPM. Что это и зачем?

Application Security Posture Management, ASPM – практика, которая сочетает в себе:

- Автоматизированную оркестрацию Application Security Tools (AST) ✓
- Управление технологическими пайплайнами инструментов ✓
- Корреляцию результатов работы инструментов ✓
- Сбор метрик о продуктах ✓

Эволюция рынка решений ASOC:

2016

AVC
Gartner определяет как AVC – Application Vulnerability Correlation

2017

ASTO
Gartner определяет как ASTO – Application Security Testing Orchestration

2019

ASOC
Gartner объединяет AVC и ASTO в один продукт – ASOC (Application Security Orchestration & Correlation)

ASPM. Что это и зачем?

Application Security Posture Management, ASPM – практика, которая сочетает в себе:

- Автоматизированную оркестрацию Application Security Tools (AST) ✓
- Управление технологическими пайплайнами инструментов ✓
- Корреляцию результатов работы инструментов ✓
- Сбор метрик о продуктах ✓

Эволюция рынка решений ASOC:

2016

AVC
Gartner определяет как AVC – Application Vulnerability Correlation

2017

ASTO
Gartner определяет как ASTO – Application Security Testing Orchestration

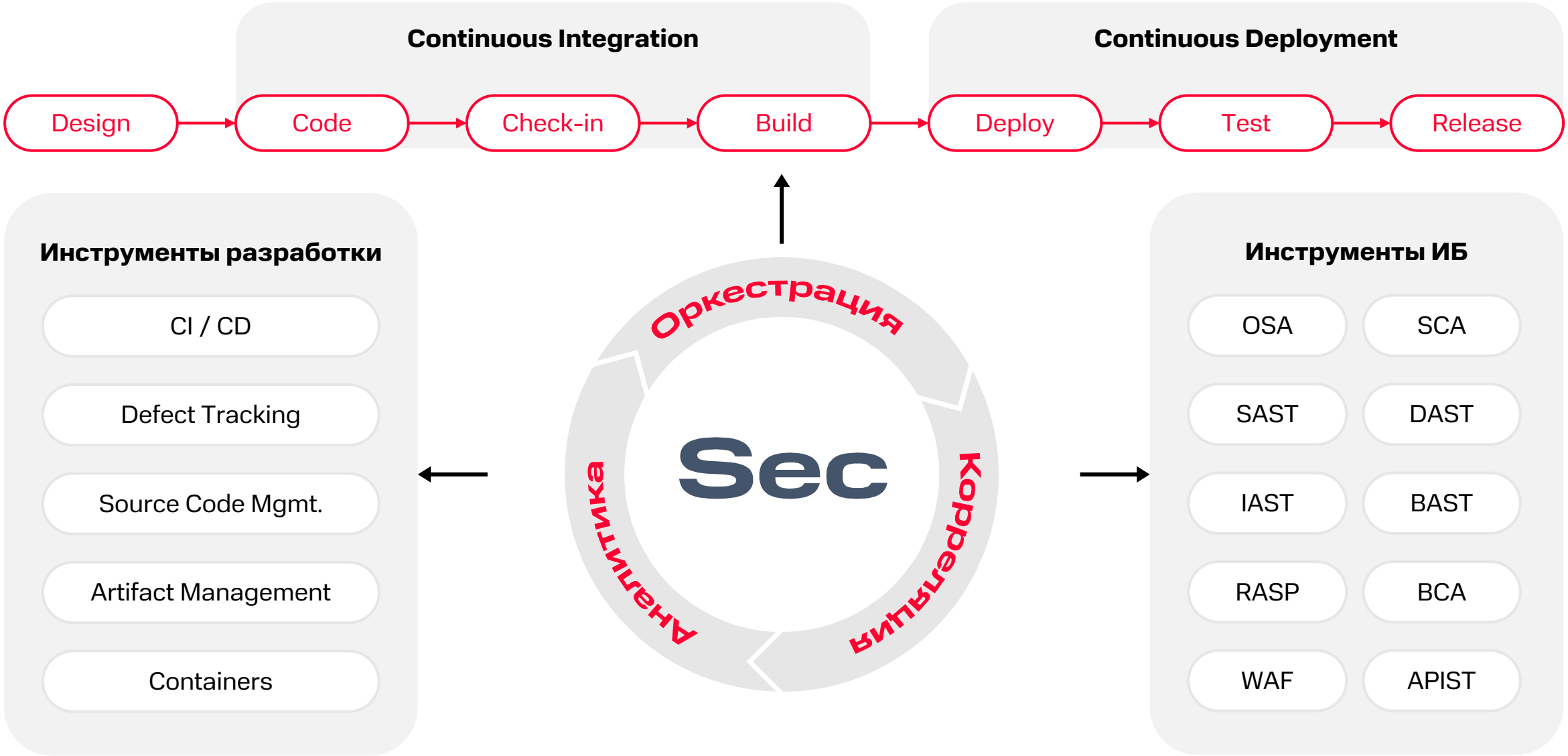
2019

ASOC
Gartner объединяет AVC и ASTO в один продукт – ASOC (Application Security Orchestration & Correlation)

2023

ASPM
Gartner пересматривает определение ASOC до ASPM (Application Security Posture Management), из-за большей функциональности

ASPM Helicopter view



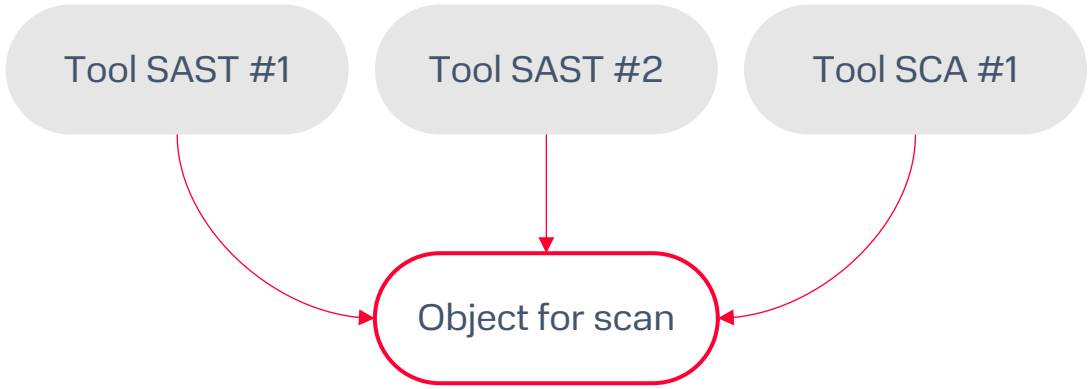
Оркестрация

Блок оркестрации помогает соединить различные ИБ-инструменты с DevOps процессами компании, централизовано и гибко управлять ИБ-инструментами для каждого уникального сканирования продуктов с учетом установленных настроек и критериев

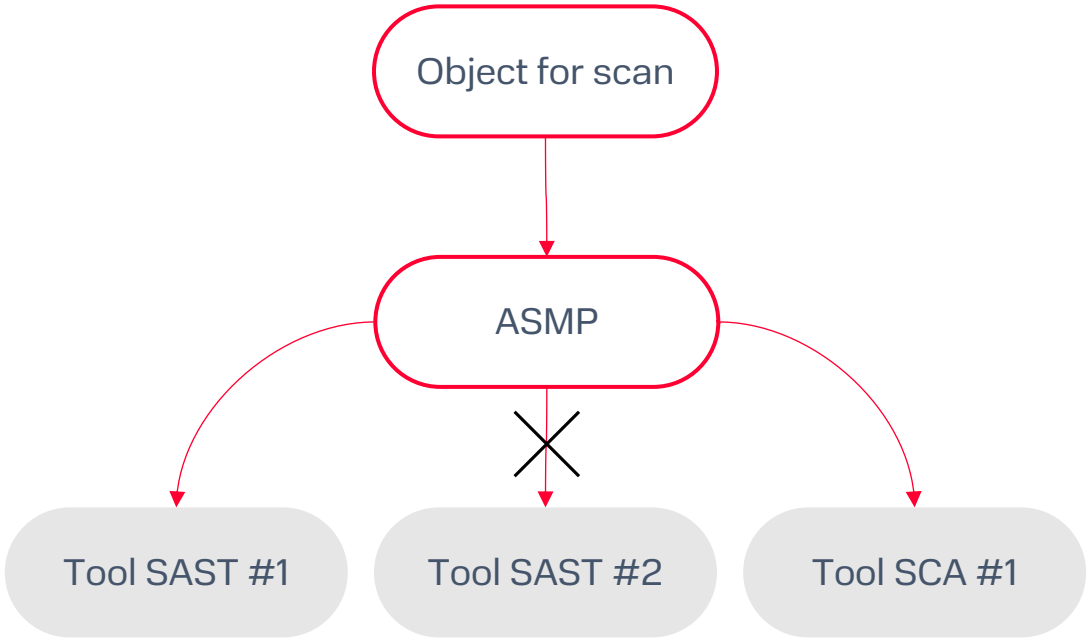
Платформа должна позволять создавать и настраивать точки контроля качества ПО (security/quality gates) для каждого ИБ-пайплайна. «Ворота» определяют критерии для успешного прохождения этапа проверок и позволяют принять решение о том, можно ли переводить конкретную сборку на следующий этап жизненного цикла разработки ПО

Оркестрация

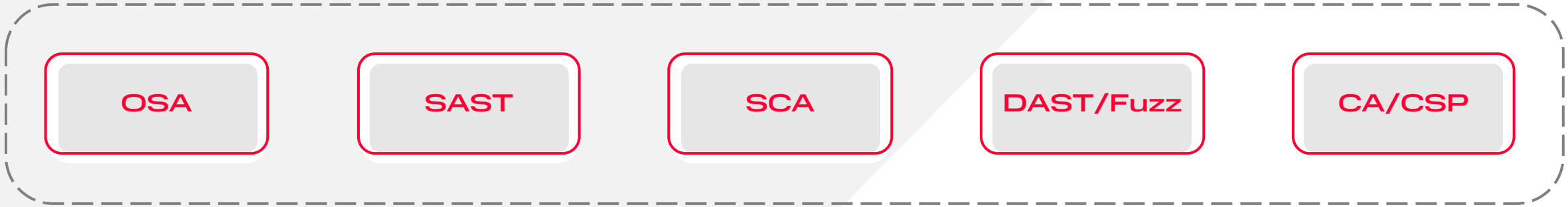
Без решения ASMP



ASMP используется



ASPM



Корреляция

**Все инструменты DevSecOps работают отдельно,
каждый из них генерирует собственные результаты,
а все вместе они порождают гигантские объемы данных**

Корреляция

**Все инструменты DevSecOps работают отдельно,
каждый из них генерирует собственные результаты,
а все вместе они порождают гигантские объемы данных**

Все знают проблему сканеров – огромное число false-positive срабатываний, осмотреть отчёты нескольких инструментов, верифицировать уязвимости в разных местах, свести их, пересканировать, чтобы убедиться в устранении – АД

Корреляция

**Все инструменты DevSecOps работают отдельно,
каждый из них генерирует собственные результаты,
а все вместе они порождают гигантские объемы данных**

Все знают проблему сканеров – огромное число false-positive срабатываний, осмотреть отчёты нескольких инструментов, верифицировать уязвимости в разных местах, свести их, пересканировать, чтобы убедиться в устранении – АД

Платформа обеспечивает централизованный подход к взаимодействию с результатами инструментов.
Она агрегирует схожие уязвимости, группирует их, удаляет дубли, а также сортирует для удобства представления

Корреляция

**Все инструменты DevSecOps работают отдельно,
каждый из них генерирует собственные результаты,
а все вместе они порождают гигантские объемы данных**

Все знают проблему сканеров – огромное число false-positive срабатываний, осмотреть отчёты нескольких инструментов, верифицировать уязвимости в разных местах, свести их, пересканировать, чтобы убедиться в устранении – АД

Платформа обеспечивает централизованный подход к взаимодействию с результатами инструментов.
Она агрегирует схожие уязвимости, группирует их, удаляет дубли, а также сортирует для удобства представления

«Пересканирование» для сравнения результатов анализа новых версий, в которых дефекты должны быть устранены, с отчетами ранних сканирований. Так в автоматическом режиме и контролируется процесс устранения уязвимостей

Корреляция

**Все инструменты DevSecOps работают отдельно,
каждый из них генерирует собственные результаты,
а все вместе они порождают гигантские объемы данных**

Все знают проблему сканеров – огромное число false-positive срабатываний, осмотреть отчёты нескольких инструментов, верифицировать уязвимости в разных местах, свести их, пересканировать, чтобы убедиться в устранении – АД

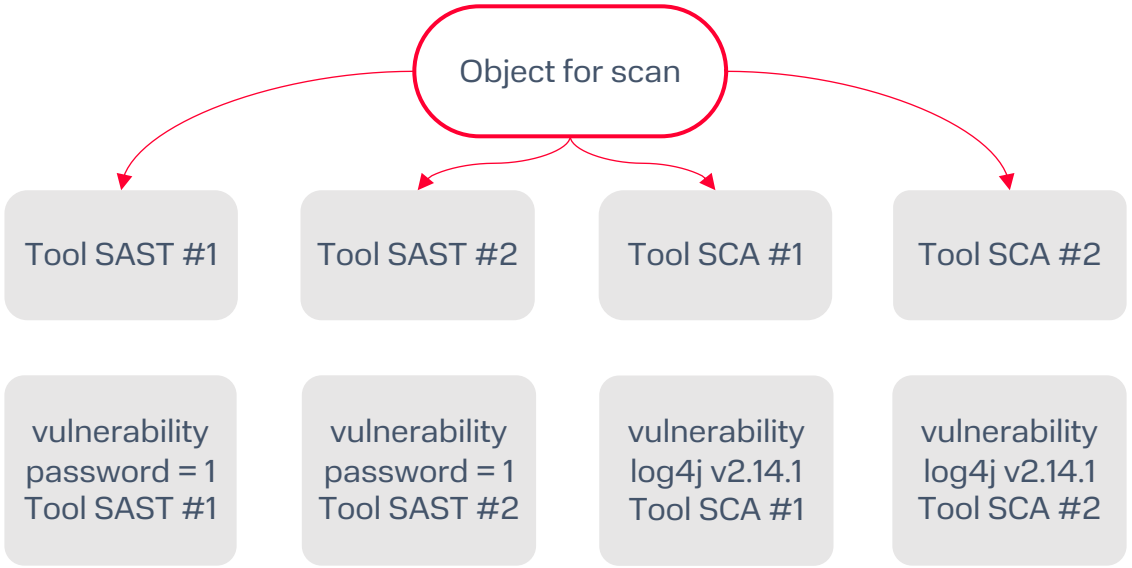
Платформа обеспечивает централизованный подход к взаимодействию с результатами инструментов.
Она агрегирует схожие уязвимости, группирует их, удаляет дубли, а также сортирует для удобства представления

«Пересканирование» для сравнения результатов анализа новых версий, в которых дефекты должны быть устранены, с отчетами ранних сканирований. Так в автоматическом режиме и контролируется процесс устранения уязвимостей

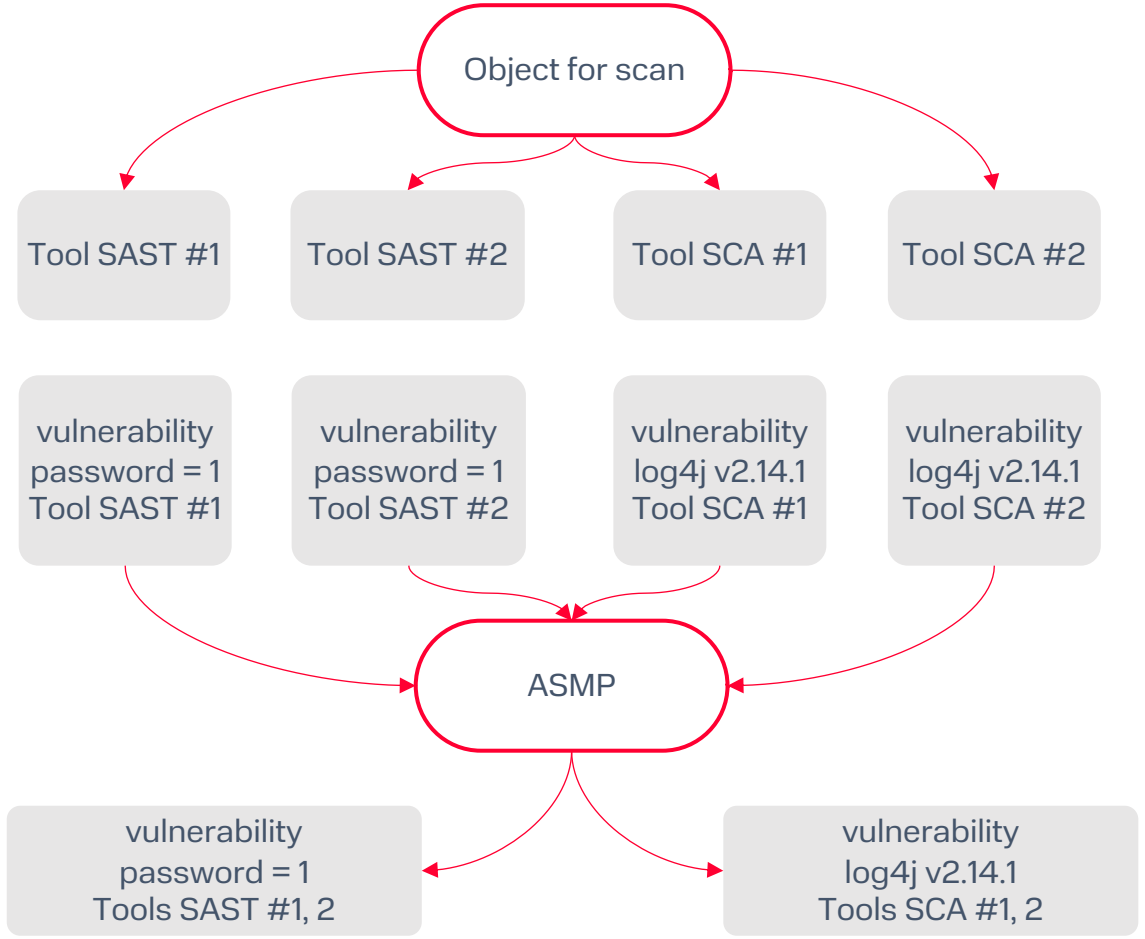
Таким образом, платформа позволяет ИБ-специалистам оптимизировать затраты ресурсов на анализ уязвимостей

Корреляция

Без решения ASMP



ASMP используется

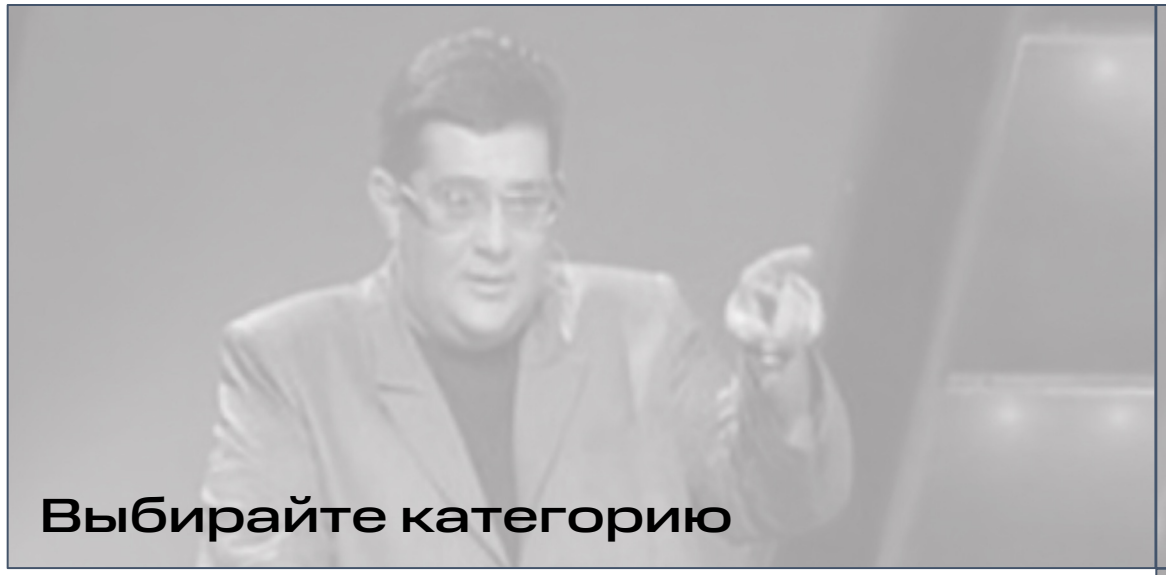


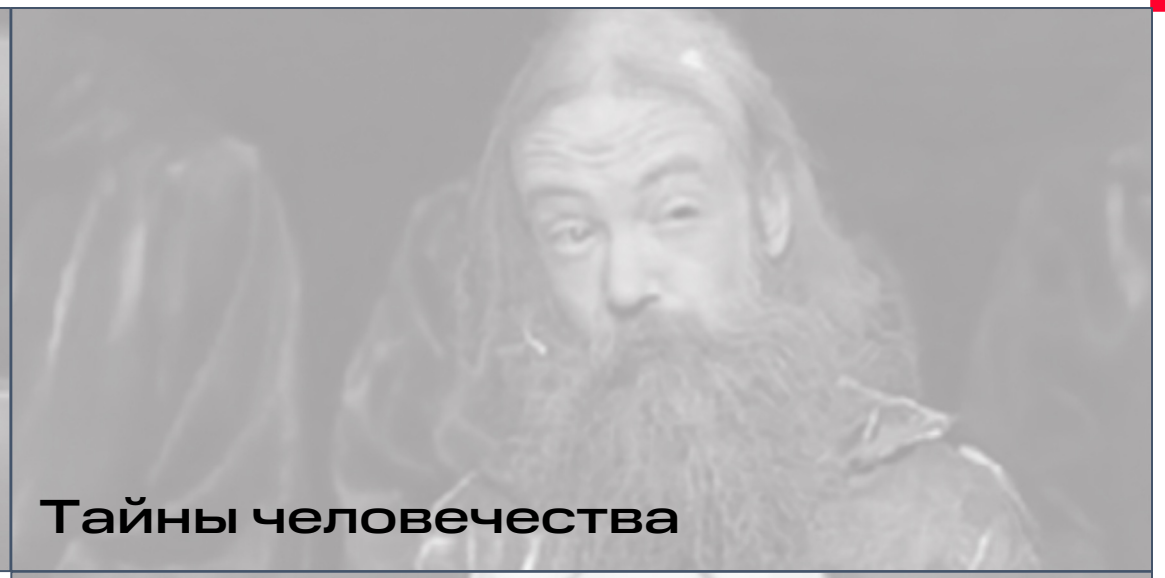
Аналитика

Блок аналитики – визуальное представление метрик

Все данные, полученные в процессе разработки защищенных программных продуктов собираются в DWH и выводятся на дашборды с учётом аналогии со светофором, ещё на их основе формируются отчёты

Такой метод подачи аналитики максимально информативен для пользователя любого уровня, транслирует уровень безопасности и эффективность ИБ-процессов в разрезе продукта





«Чем запуск
пайплайна
из гитлаба —
это не оркестратор?»

«А чем тебя доджа не устраивает?»

Обзор требований рынка к инструментам оркестрации

02

Чего хочет рынок?

Совокупные результаты тестирований

Анализ уязвимостей на основе рисков

Быстрое взаимодействие безопасности и разработки

Чего хочет рынок?

Совокупные результаты тестирований

Анализ уязвимостей на основе рисков

Быстрое взаимодействие безопасности и разработки

«Быстрый и лёгкий старт»/Pipeline

Рекомендации по устранению

Отчетность (отчёты и дашборды)

Чего хочет рынок?

Совокупные результаты тестирований

Анализ уязвимостей на основе рисков

Быстрое взаимодействие безопасности и разработки

«Быстрый и лёгкий старт»/Pipeline

Рекомендации по устранению

Отчетность (отчёты и дашборды)

Мониторинг соответствия стандартам/практикам

Повышение «культуры» написания кода

Оптимизация инструментов

Так вышло,

Так вышло,

что мне удалось поработать с несколькими платформами класса ASPM и хотелось бы рассказать,
что это (не) больно, (не) страшно,
но...

Существующие решения

03

ASPM. Существующие решения

APPSECHUB

ThreadFix

DEFECTDOJO

OWASP

Security Gate

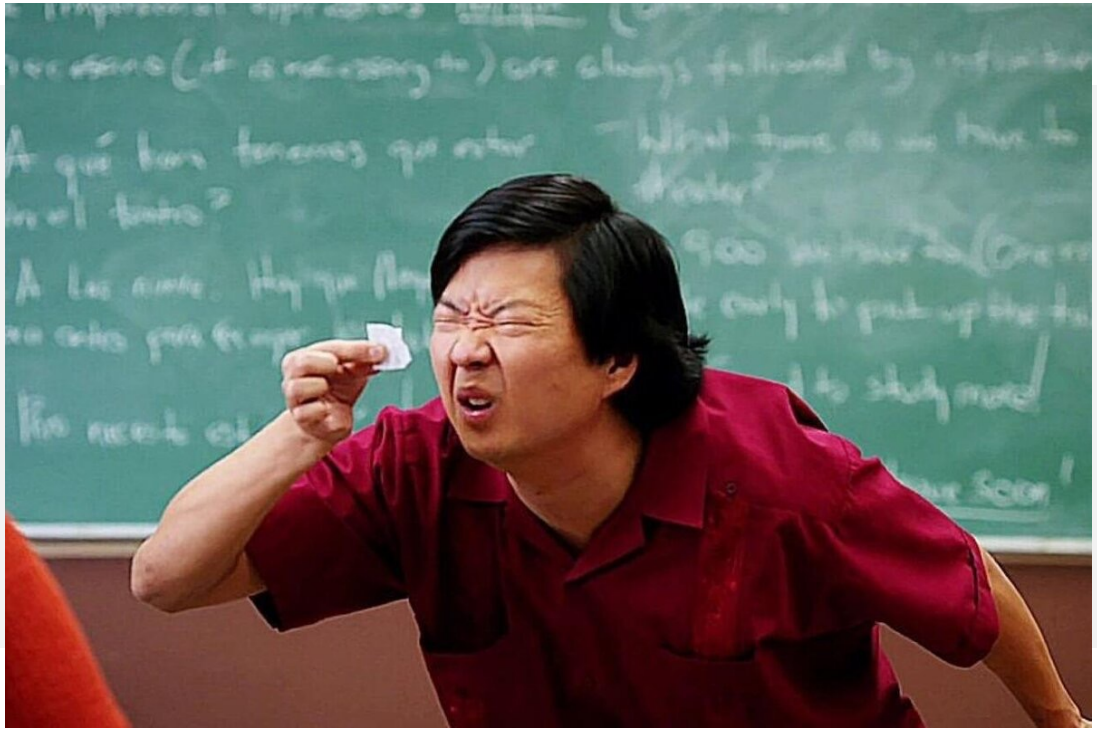
Security RAT

Сравнение

04

Чтобы вы не выглядели так,

рассматривая огромную таблицу — scan QR



Критерии сравнения

Группа критериев						Общий коэффициент соответствия ~
Продукт №1	Продукт №2	Продукт №3	Продукт №4	Продукт №5	Продукт №6	
Базовые						0.73
Интеграции с инструментами DevOps						0.64
Интеграции с инструментами DevSecOps						0.44
Создание и настройка Quality Gates						0.27
Обработка уязвимостей						0.65
Метрики						0.50
Итого						0.55

Советы для разработчиков решений

- AppSec/DevSecOps для AppSec/DevSecOps
- Динамичная разработка
- Возможность универсального подключения инструментов
- Регулярное получение обратной связи от пользователей решения, по результатам приоритезация задач в бэклоге

Советы для компаний, которые самостоятельно разрабатывают внутренний оркестратор

- «Настройка процессов»
- Делиться наработками/перенимать экспертизу, «переиспользовать» что-либо
- Выйти на рынок самостоятельно

Советы для пользователей и тех, кто только выбирает инструмент

- Если хотите относительно «легкий старт» – будьте готовы платить за инструмент
- Платформа, подходящая для вашего «зоопарка» инструментов
- На данный момент нет решения, которое подойдёт вам идеально и будет работать без каких-либо «костылей»

Выводы

Необходимо развиваться

- Соответствовать заявлениям
- Реализовать минимально необходимый функционал
- «Тюнить» продукты по результатам обратной связи от пользователей
- Возможность универсального подключения инструментов/практик
- Наполнение экспертными данными для «шаринга»

Выводы

Необходимо развиваться

- Соответствовать заявлениям
- Реализовать минимально необходимый функционал
- «Тюнить» продукты по результатам обратной связи от пользователей
- Возможность универсального подключения инструментов/практик
- Наполнение экспертными данными для «шаринга»

Больные фантазии:

Автоматизированное управление уязвимостями – система автоматически отслеживает, классифицирует и устраняет уязвимости, при этом уведомляя отделы разработки и эксплуатации

Шаблоны политик безопасности – платформа должна поддерживать настраиваемые политики безопасности и правила, которые можно установить в соответствии с требованиями организации

А значит, **в будущем подобные платформы позволят вывести DevSecOps на совершенно новый уровень с минимальным количеством ручных задач**

М

Т

Действуй!

Артем Пузанков

DevSecOps Cluster Lead

artem.puzankov@gmail.com

https://t.me/spawny2k

MTC Digital

С