Артем Пузанков
Руководитель группы внедрения
практик безопасной разработки

Как защитить свой конвейер

добавив немножечко ~~боли~~ инструментов безопасности

«Раньше было лучше»

«Раньше было лучше»

Раньше было круто
просто писать код
не думая
о качестве, а теперь
стало понятно, что
качество =
безопасность

Кто я

«А я че, знаю? Я сам ниче не знаю» © Сократ

Разрабатывал

AppSec platforms в двух компаниях large enterprise в разных ролях

Строю процессы SSDLC

в различных организациях, где-то даже с нуля

Внедряю инструменты DevSecOps

Собрал первый в жизни пайплайн на коммерческих инструментах, а потом открыл для себя опенсорс и теперь вижу его части в коммерческих инструментах :)

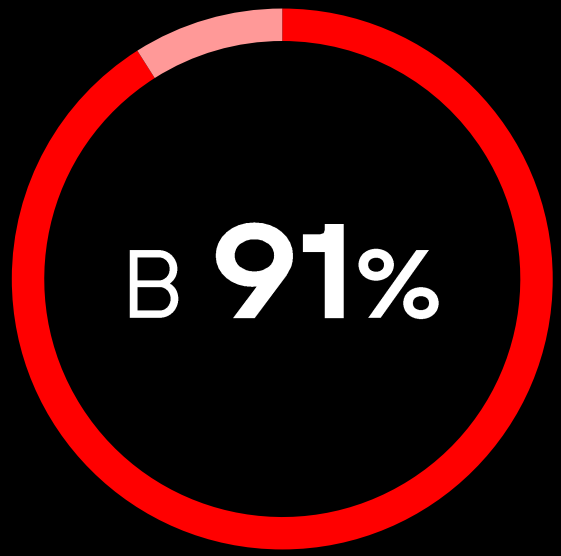
Есть кот

Лысый!

Статистические данные

Угрозы

веб-приложений злоумышленники могут проводить атаки на пользователей



веб-приложений была утечка важных данных

веб-приложений есть возможность получить несанкционированный доступ

Трендовые уязвимости

2023 год

Модули и библиотеки

- libwebp
- vm2
- Struts
- libvpx
- xz

Средства разработки и деплоя

- GitLab
- Oracle WebLogic Server
- TeamCity

БД и брокеры сообщений

- Apache ActiveMQ
- Redis

Жить страшно!
Все «дырявое»
Но что же делать?

Не переживать!
Индустрия придумала направление application security

Application security

Что это такое и с чем это есть

Application security — это...

А на простом?

1. Совокупность процессов и практик, которые помогают делать защищенные продукты
2. Работает со всеми сущностями приложения, такими как дизайн, код, артефакт, сборка на стендах, эксплуатация
3. Встраивается в текущий процесс разработки*

* И не мешает

Методология

Слышали ли вы что-то о DevSecOps?

Какой еще DevSecOps?

DevOps

- Достигли автоматизации и стандартизации производственных процессов
- В стороне оставили направление безопасности
- В попытках как можно быстрее разработать продукт теряется качество, один из критериев которого — безопасность

В условиях современного производства и скорости выпуска ПО безопасность была вынуждена эволюционировать

Так появилось направление **DevSecOps**

Методология

Waterfall
Минусы очевидны

Agile
Скорее философия, чем методология

Kanban
Визуализация и оптимизация рабочего процесса

Scrum
Сотрудничество, прозрачность и непрерывное улучшение

DevOps
Автоматизируйте все, что только можно

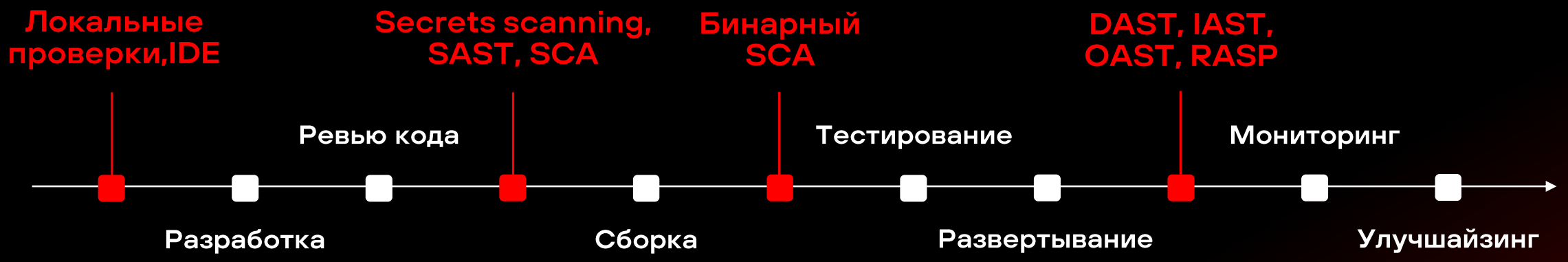
И даже то, что нельзя

DevSecOps
DevOps + Sec (инструменты безопасности)

Идеальный процесс разработки

А фактический?

Идеальный процесс разработки
+ инструменты DevSecOps



SAST

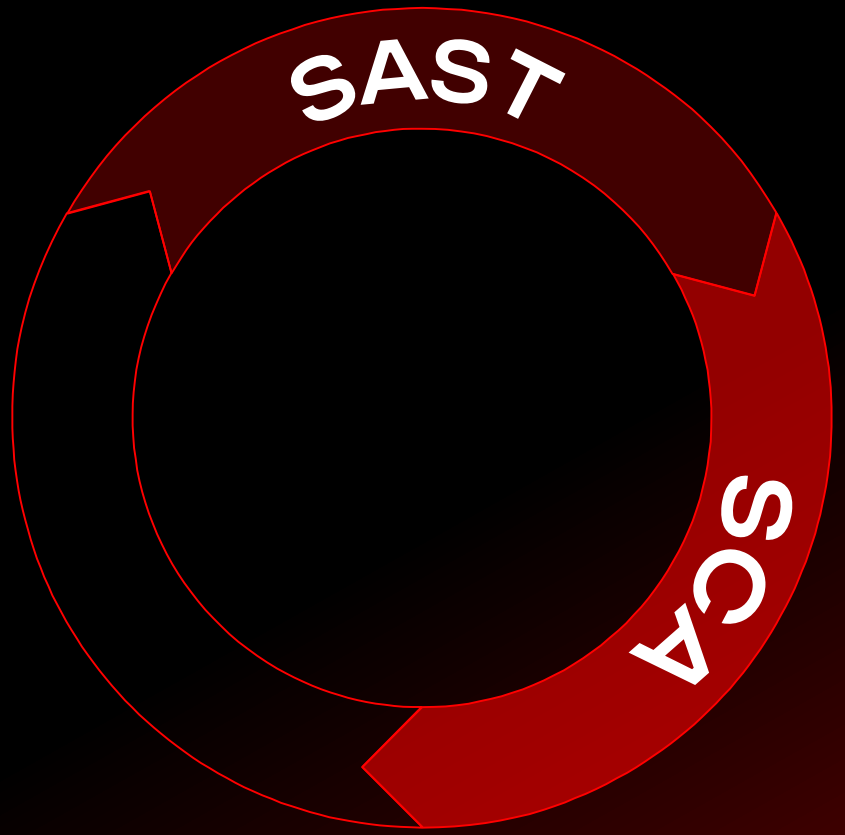
Static application security testing

- SAST — проверка с помощью метода белого ящика (white box testing): анализаторы имеют доступ к внутренней структуре приложения
- Сканеры проверяют исходный код не запуская его, поэтому могут генерировать ложные срабатывания и не обнаруживать некоторые типы уязвимостей
- Основная задача SAST-сканеров — тестирование на безопасность, в частности проверка исходного кода на наличие распространенных уязвимостей (например, из списка OWASP Top 10)
- Анализаторы находят не только саму уязвимость, но и фрагмент кода, из-за которого она появилась

SCA

Software composition analysis

- SCA — анализ компонентного состава приложения
- В ходе такого анализа можно отыскать устаревшие зависимости, содержащие известные уязвимости и эксплойты
- Некоторые SCA-инструменты могут определить лицензионную совместимость компонентов и риск нарушения лицензионных прав
- В ходе source SCA анализируется исходный код, а точнее — зависимости приложения, определенные в исходном коде



DAST

Dynamic application security testing

- DAST — тестирование приложений с помощью метода черного ящика
- В ходе анализа имитируются внешние атаки для эксплуатации распространенных уязвимостей
- Динамическое тестирование позволяет выявлять уязвимости, связанные с внедрением кода в запрос (например, к веб-странице) или с некорректной конфигурацией (самый простой пример — возможность аутентификации по пустому паролю)

ASOC

Application security orchestration and correlation, он же — AppSec posture management, AppSec platform

Решения ASOC позволяют реализовать:

- автоматизированную оркестрацию application security tools (AST)
- управление технологическими пайплайнами инструментов
- корреляцию результатов работы инструментов
- сбор метрик о продуктах

ASPM — что это и зачем?

Эволюция рынка решений ASOC:

AVC (Gartner)

Application Vulnerability Correlation — агрегация результатов работы инструментов, корреляция

ASTO (Gartner)

Application Security Testing Orchestration — управление AST (запуск)

ASOC (AVC + ASTO)

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

ASPM (Gartner)

Переосмысляет название ASOC → ASPM (Application Security Posture Management): большая функциональность дает понимание об уровне ИБ продукта на всех этапах жизненного цикла (о рисках, business critical и т. д.)

AppSec Platform

~~Gartner~~ Мы определяем, а скорее даже замечаем то, что происходит сегодня ☺

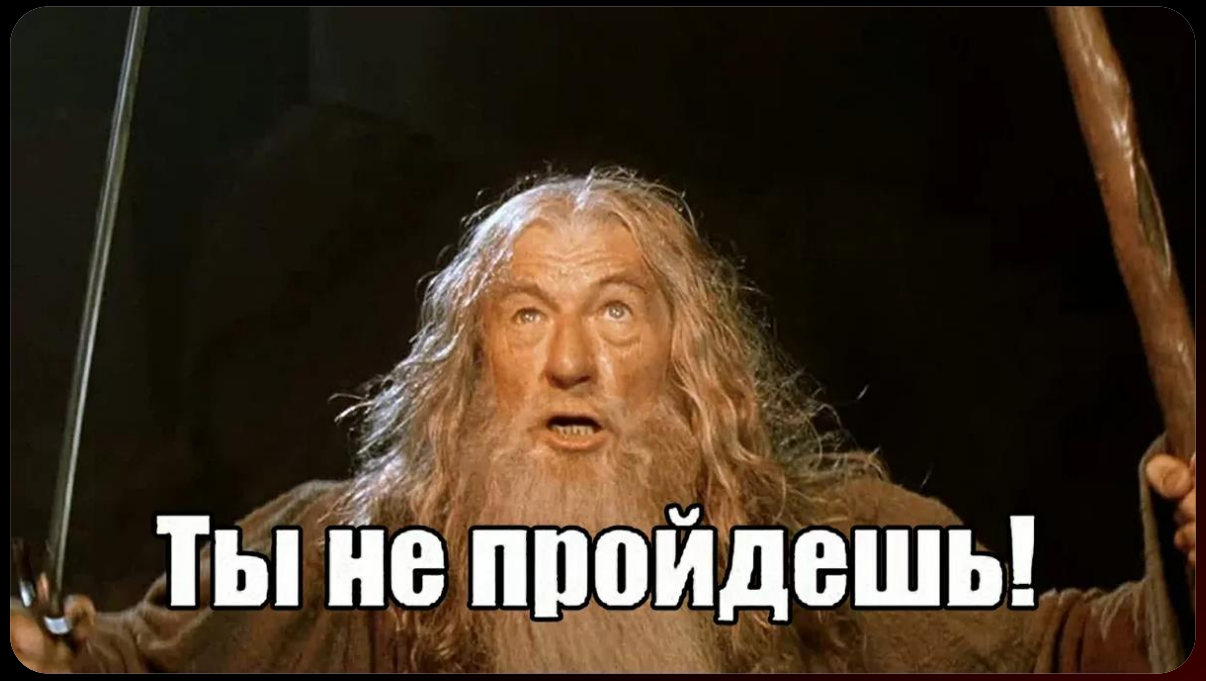
Quality (security) gates

Или блокирующий фактор

Quality (security) gates — своего рода ворота качества, через которые проходит продукт на каждом этапе разработки. Есть недочеты — на доработку, все ок — идем дальше

По мере развития экспертизы в командах разработки, рекомендуется внедрять quality gates в блокирующем режиме

Применяется индивидуально для каждой команды (кто-то готов к этому этапу через три месяца, кто-то — через полтора года)

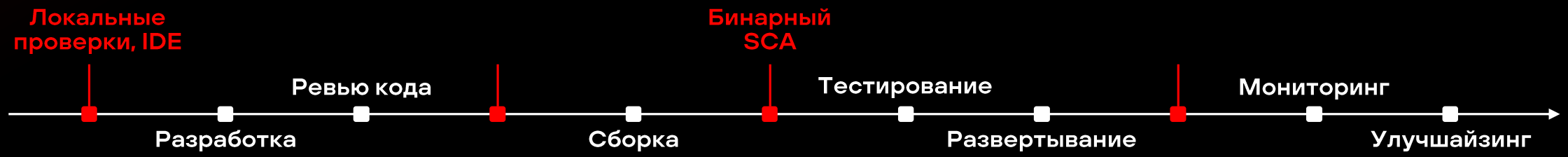


Если вы думаете, что вас это не коснется, вы ошибаетесь

При наличии направления AppSec (а оно есть в любой уважающей себя компании) рано или поздно появятся и quality gates.

Application security tooling

Или просто инструменты DevSecOps



Local checks, IDE

- Плагин PT Application Inspector IDE
- Gitleaks
- git-secrets
- Trivy

Secret detection

- Gitleaks
- git-secrets
- GitLab Secret Detection

SAST

- PT Application Inspector
- SonarQube
- Checkmarx SAST
- PVS-Studio

SCA

- Trivy
- CodeScoring

Применим к собранным бинарным артефактам

- Trivy
- Clair
- Grype
- JFrog Xray
- Docker Hub

DAST

- PT BlackBox
- Zed Attack Proxy (ZAP)
- Fortify WebInspect
- Veracode Dynamic Analysis
- Acunetix

IAST

- PT Application Inspector
- Acunetix

OAST

- Burp Suite
- ZAP (OAST-плагин, сервисы BOAST, TukTuk и interacts)

RASP

- Fortify
- Aqua
- OpenRASP
- Jscrambler
- Hdiv
- Imperva RASP

ASOC

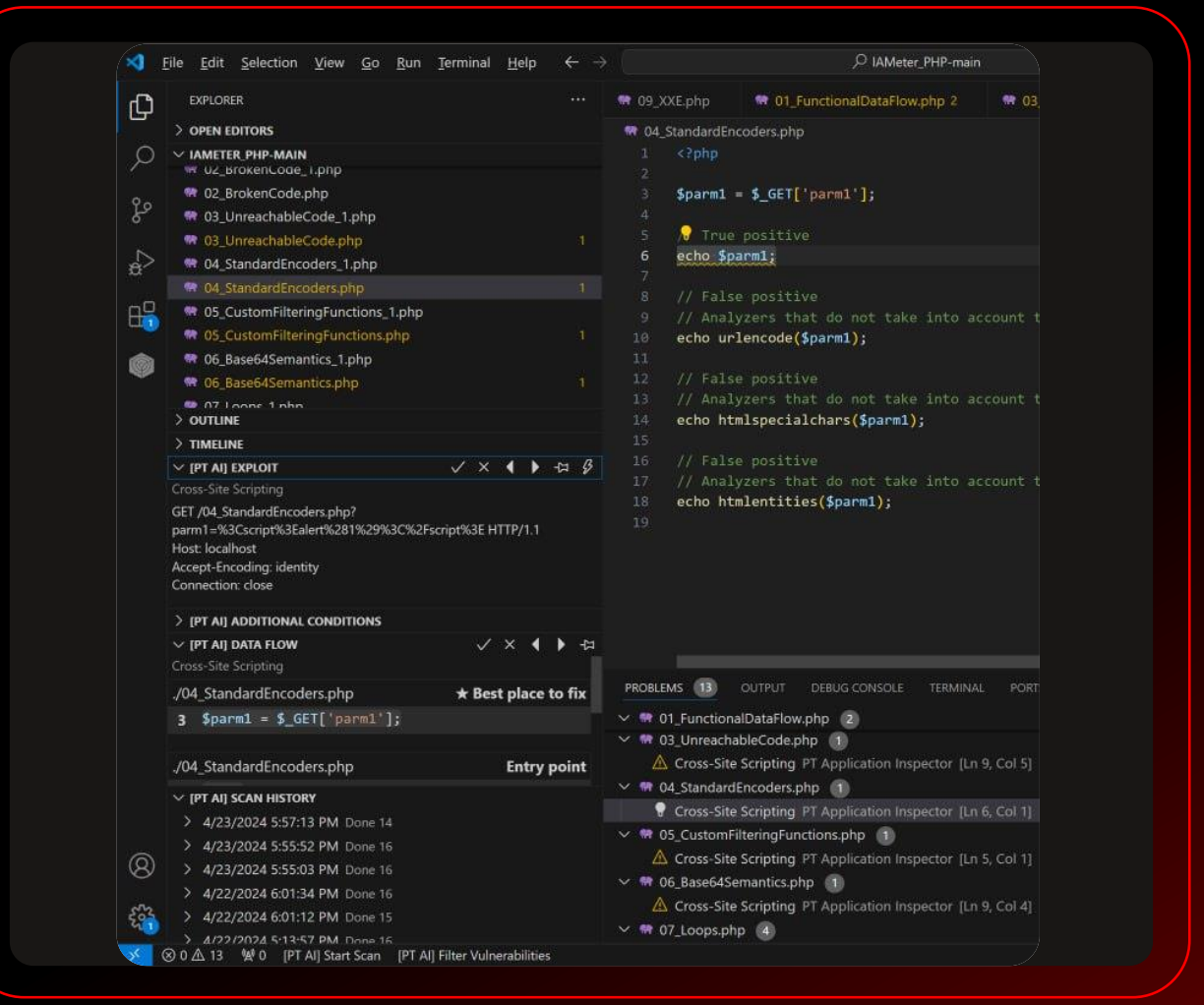
- DefectDojo
- OWASP SecurityRAT
- Hexway
- ThreadFix
- secureCodeBox
- AppSec.Hub

Плагин PT AI для IDE

Pre-commit проверки

Анализ исходного кода проводится локально в среде разработки на устройстве разработчика до коммита кода в Git

Это позволяет выявлять уязвимости в коде на самых ранних стадиях, например находить секреты, которые не должны попасть в историю Git, проверять конфигурационные файлы с точки зрения безопасности



github.com/POSIdev-community/AI.Plugin.VSCode

Плагин PT AI для IDE

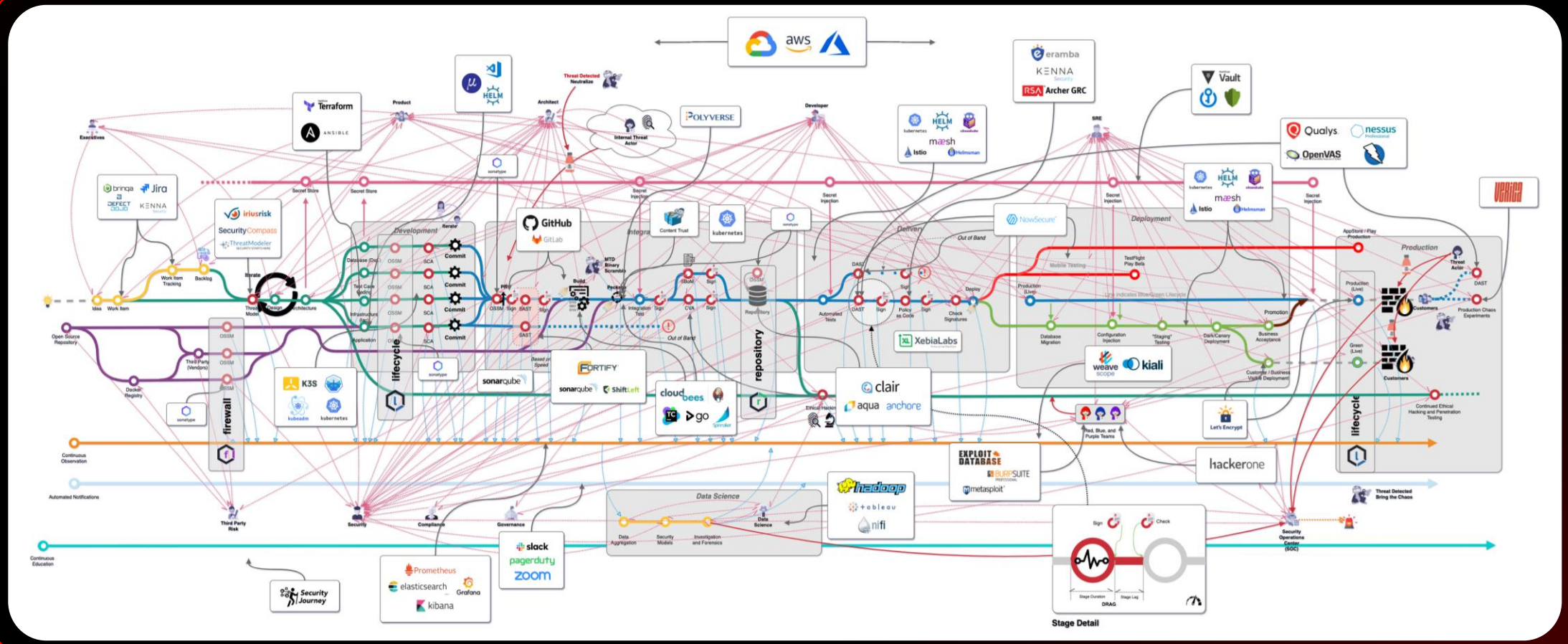
Pre-commit проверки

Для
IntelliJ IDEA

Для
Visual Studio

Плагин для IDE

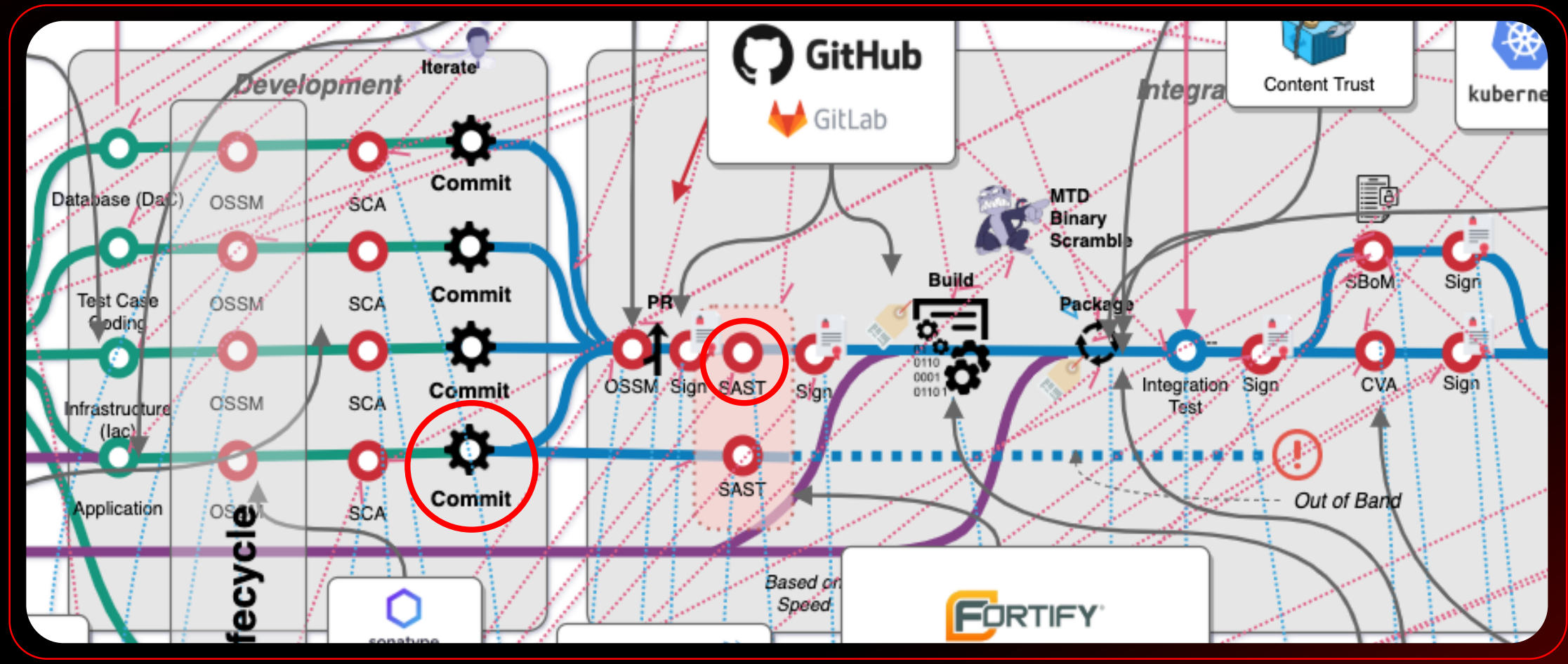
Pre-commit проверки



github.com/POSIdev-community/AI.Plugin.VSCode

Плагин для IDE

Pre-commit проверки



Источник: Sonatype DevSecOps Reference Architecture

Контакты

apuzankov@ptsecurity.com

@spawny2k

Внимание, опрос!

Спасибо!