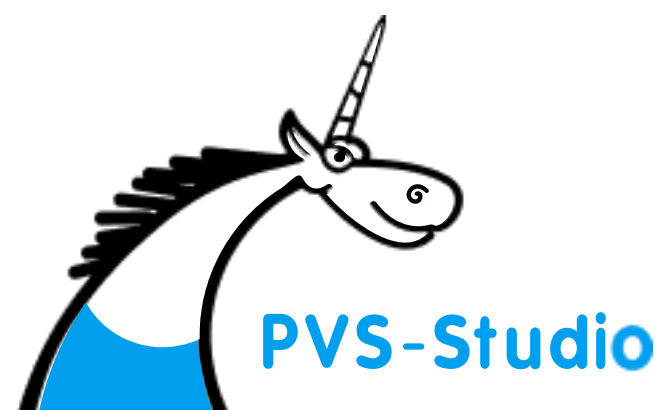


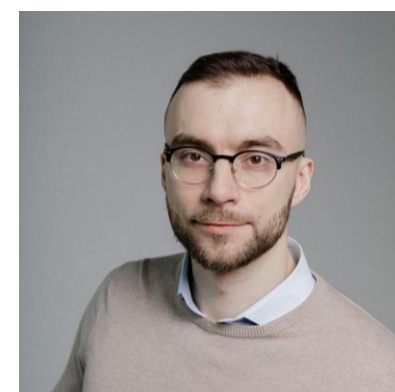
Внедрение процессов безопасной разработки

Практическая интеграция PVS-Studio и Securitm



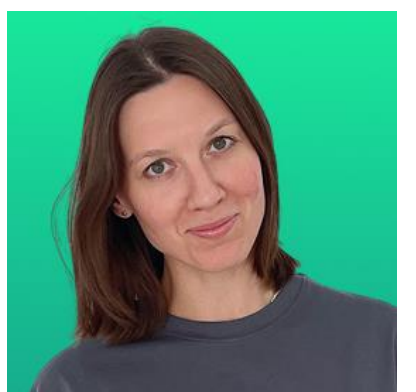
Антон Третьяков

Разработчик, Tools&DevOps



Евгения Карпова

Инженер отдела
внедрения и поддержки



Антон Третьяков

Разработчик, Tools&DevOps

- Делаю инструменты PVS-Studio
- Развиваю инфраструктуру
- Пишу статьи о C++ и рассказываю доклады



Что такое статический анализ (по ГОСТ Р 71207-2024)

Что такое статический анализ (по ГОСТ Р 71207-2024)

- Вид работ по инструментальному исследованию программы, основанный на анализе исходных кодов в режиме, не предусматривающем реального выполнения кода, и выполняемый для определения свойств программы (п.3.1.33).

Что такое статический анализ

- Вид работ по инструментальному исследованию программы, основанный на анализе исходных кодов в режиме, не предусматривающем реального выполнения кода, и выполняемый для определения свойств программы (п.3.1.33).

Статический анализ обязан

Статический анализ обязан

- Искать **критические ошибки** (п.7.3)

Статический анализ обязан

- Искать критические ошибки (*п.7.3*)

Перевод

Критические ошибки – просто термин. Список в *пп.6.3-6.5*

Статический анализ обязан

- Реализовывать **методы анализа** (п.7.4)

Статический анализ обязан

- Реализовывать **методы анализа** (п.7.4)

Перевод

То, **как** ищутся критические ошибки.

Статический анализ обязан

- Поддерживать **межмодульный анализ** (п.7.5)

Статический анализ обязан

- Поддерживать **межмодульный анализ** (п.7.5)

Перевод

Важно для языков с **раздельной** компиляцией.

Статический анализ обязан

- Делать разметку для **taint-анализа** (п.7.6)

Статический анализ обязан

- Делать разметку для **taint-анализа** (п.7.6)

Перевод

Пользовательская разметка **ИСТОЧНИКОВ** и **СТОКОВ**.

Статический анализ обязан

- Анализировать проект **меньше 2 суток** (п.8.3)

Статический анализ обязан

- Анализировать проект **меньше 2 суток** (п.8.3)

Перевод

Срок выглядит **достаточным**.

Статический анализ обязан

- Делать **отчёт об ошибках** (пп.8.5, 8.6, 8.8, 8.11)

Статический анализ обязан

- Делать **отчёт об ошибках** (пп.8.5, 8.6, 8.8, 8.11)

Перевод

ГОСТ хочет, чтобы мы **смотрели** ошибки!

Статический анализ обязан

- Делать **диффы** и **подавление FA** (п.8.9)

Статический анализ обязан

- Делать **диффы** и **подавление FA** (п.8.9)

Перевод

Анализ должен проводиться **регулярно**.

Статический анализ обязан

- Иметь документацию (*п.8.10*)

Статический анализ обязан

- Иметь документацию *(п.8.10)*

Перевод

Нужно иметь описания **ошибок** и их **типа**.

Статический анализ обязан

- Искать критические ошибки (п.7.3)
- Реализовывать методы анализа (п.7.4)
- Поддерживать межмодульный анализ (п.7.5)
- Делать разметку для taint-анализа (п.7.6)
- Анализировать проект меньше 2 суток (п.8.3)
- Делать отчёт об ошибках (пп.8.5, 8.6, 8.8, 8.11)
- Делать диффы и подавление FA (п.8.9)
- Иметь документацию (п.8.10)

Что значит делать анализ **регулярно**?

Что значит делать анализ регулярно?

- Регулярно **проводить** (п.5.6.)
 - NB – важный нюанс дальше в слайдах!

Что значит делать анализ регулярно?

- Регулярно **проводить** (п.5.6.)
 - NB – важный нюанс дальше в слайдах!
- **Сохранять** отчёты (п.5.6.)

Что значит делать анализ регулярно?

- Регулярно **проводить** (п.5.6.)
 - NB – важный нюанс дальше в слайдах!
- **Сохранять** отчёты (п.5.6.)
- Регулярно **смотреть** отчёты (п.5.8.)

Что значит делать анализ регулярно?

- Регулярно **проводить** (п.5.6.)
 - NB – важный нюанс дальше в слайдах!
- **Сохранять** отчёты (п.5.6.)
- Регулярно **смотреть** отчёты (п.5.8.)
- Исправлять **ошибки** ☹️ (п.5.9.)

Как внедрять статический анализатор?

Как внедрять статический анализатор?

- На места разработчиков

Как внедрять статический анализатор?

- На места разработчиков
- В CI/CD

Как внедрять статический анализатор?

- На места разработчиков
- В CI/CD

Для своевременного выявления и исправления ошибок статический анализ должен регулярно применяться к разрабатываемому ПО. (п.5.6)

Регулярность ... обеспечивается автоматизацией процедуры проведения ..., например с помощью системы непрерывной интеграции. (п.5.6)

Как внедрять статический анализатор?

- На места разработчиков
- **В CI/CD**

Для своевременного выявления и исправления ошибок статический анализ должен регулярно применяться к разрабатываемому ПО. (п.5.6)

Регулярность ... обеспечивается автоматизацией процедуры проведения ..., например с помощью системы непрерывной интеграции. (п.5.6)

Демонстрация работы с PVS-Studio

Можно использовать разные инструменты

Можно использовать разные инструменты

- Можно использовать **несколько** статических анализаторов (п.5.2)

Можно использовать разные инструменты

- Можно использовать **несколько** статических анализаторов (п.5.2)
- Хранить результаты анализа нужно в **хранилище результатов** (п.5.6)

Можно использовать разные инструменты

- Можно использовать **несколько** статических анализаторов (п.5.2)
- Хранить результаты анализа нужно в **хранилище результатов** (п.5.6)
- Рекомендуется использовать **систему отслеживания ошибок** ПО (п.5.11)

Можно использовать разные инструменты

- Можно использовать **несколько** статических анализаторов (п.5.2)
- Хранить результаты анализа нужно в **хранилище результатов** (п.5.6)
- Рекомендуется использовать **систему отслеживания ошибок** ПО (п.5.11)

Это поможет сделать сервис **Securitm**

Презентация Securitm