Трудности при интеграции SAST: разбираем и исправляем

PVS-Studio

Глеб Асламов
C# Developer

Уязвимости и SAST

Уязвимости и SAST

Трудности при интеграции и их решение

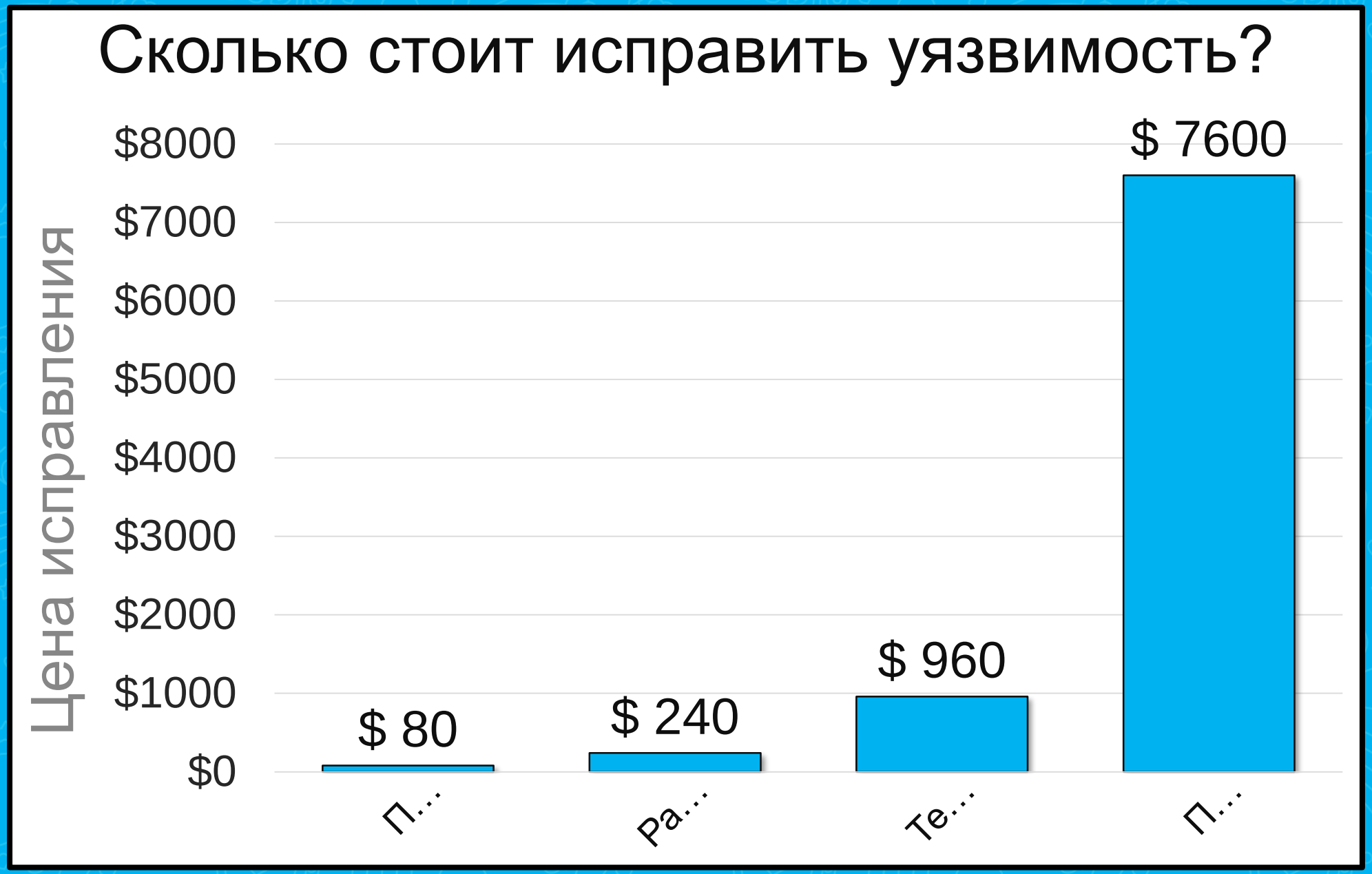
Уязвимости и SAST

Трудности при интеграции и их решение

Как быстро попробовать SAST инструмент

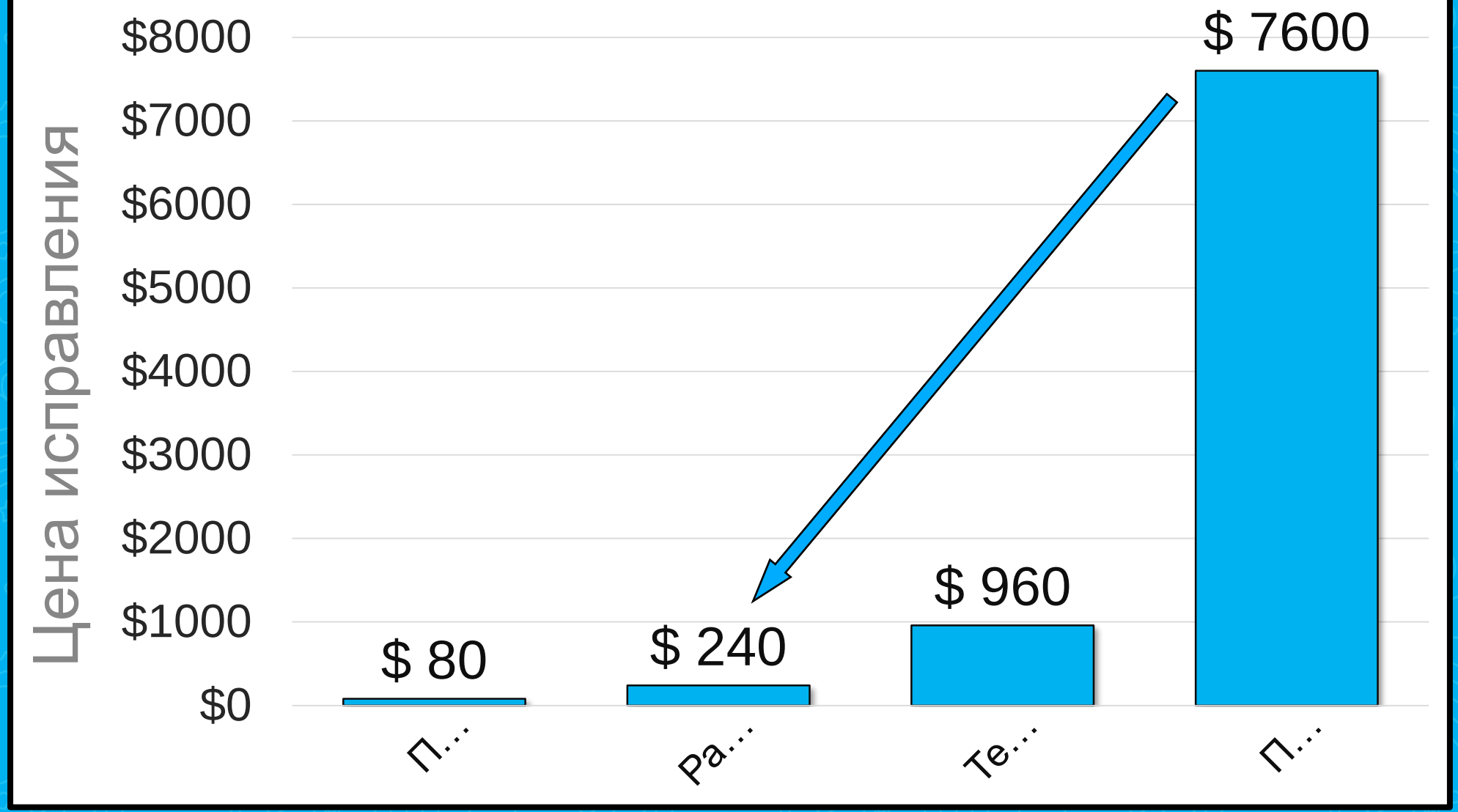
Почему уязвимости опасны?

Сколько стоит исправить уязвимость?



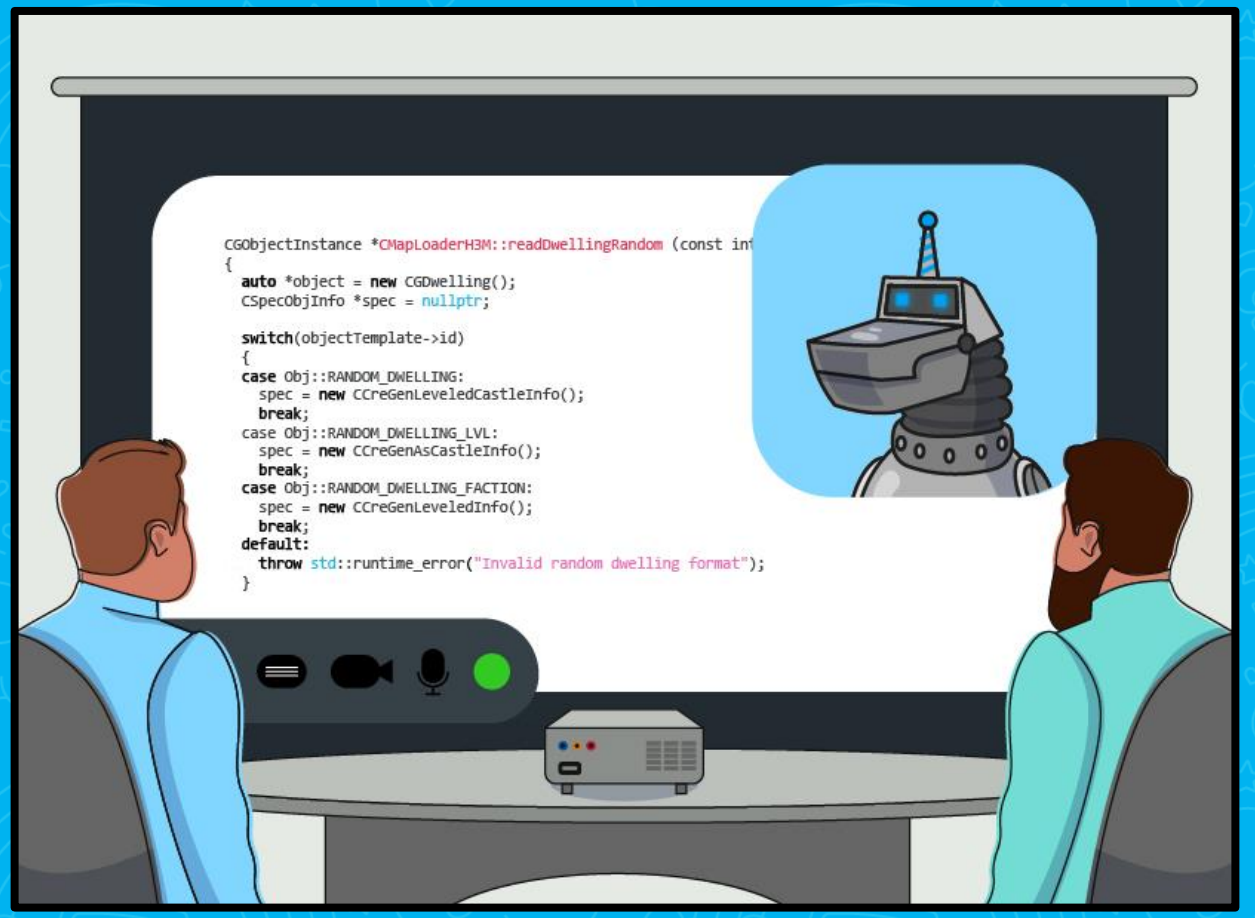
Источник - NIST: National Institute of Standards and Technology

Сколько стоит исправить уязвимость?



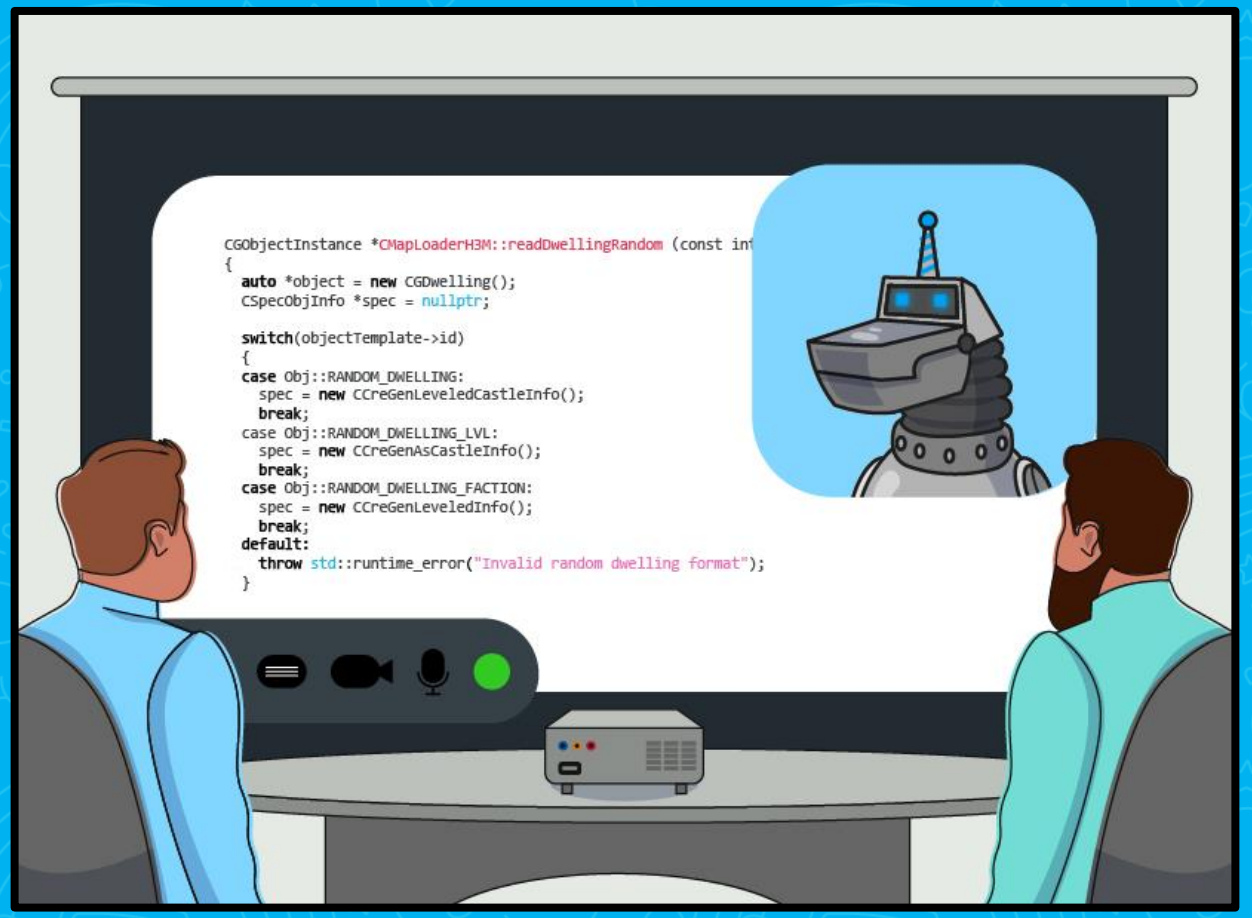
Источник - NIST: National Institute of Standards and Technology

Как искать уязвимости?



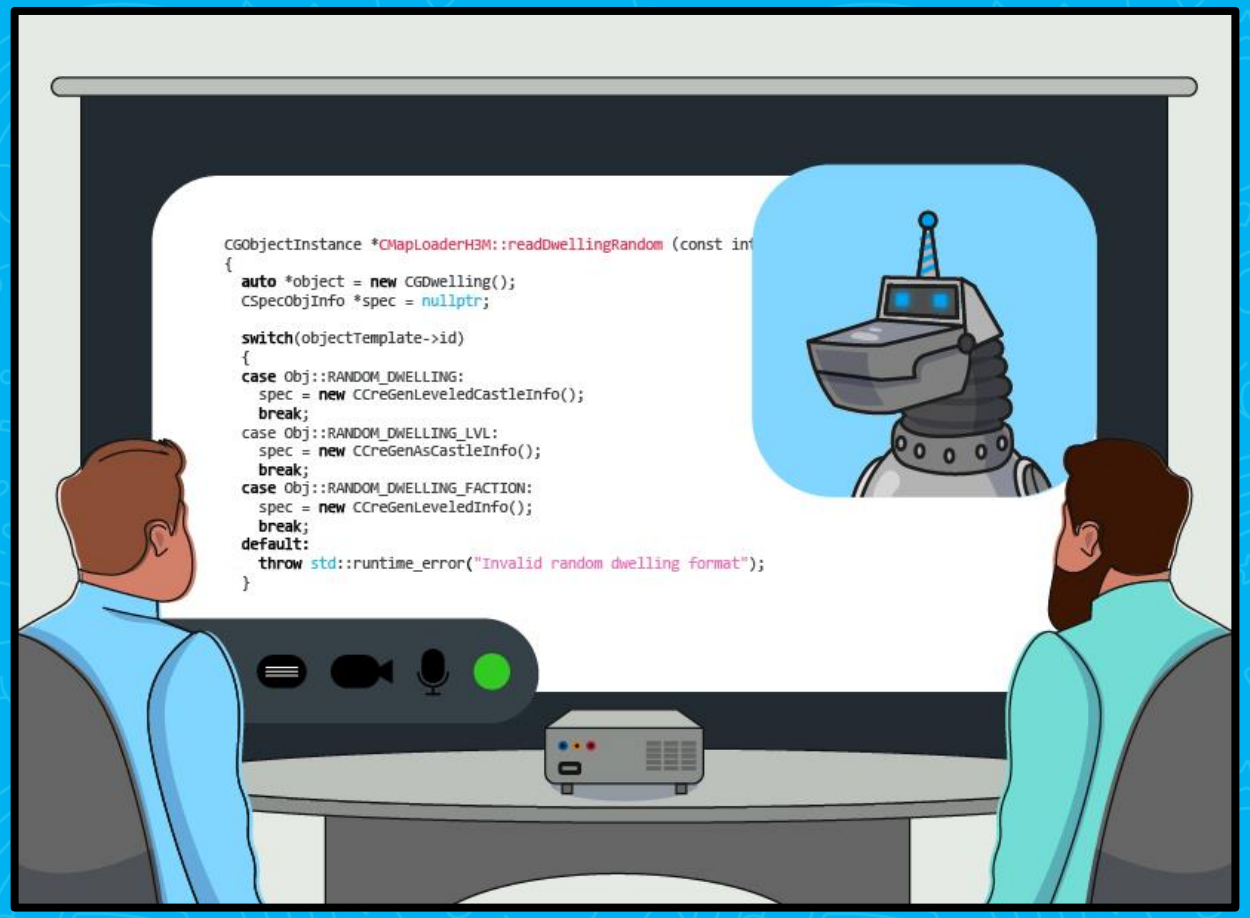
Как искать уязвимости?

- Часто ошибки == уязвимости

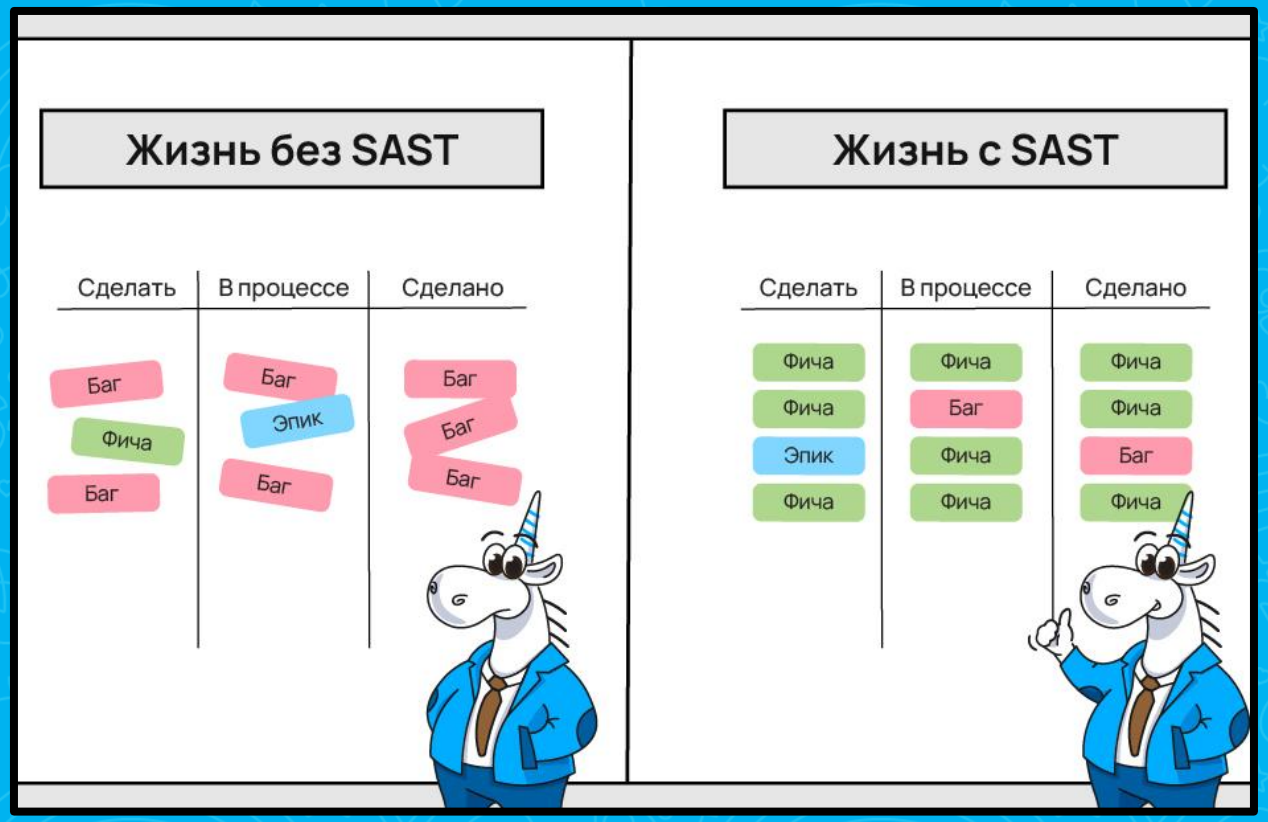


Как искать уязвимости?

- Часто уязвимости == ошибки
- Помогут найти тесты и анализаторы

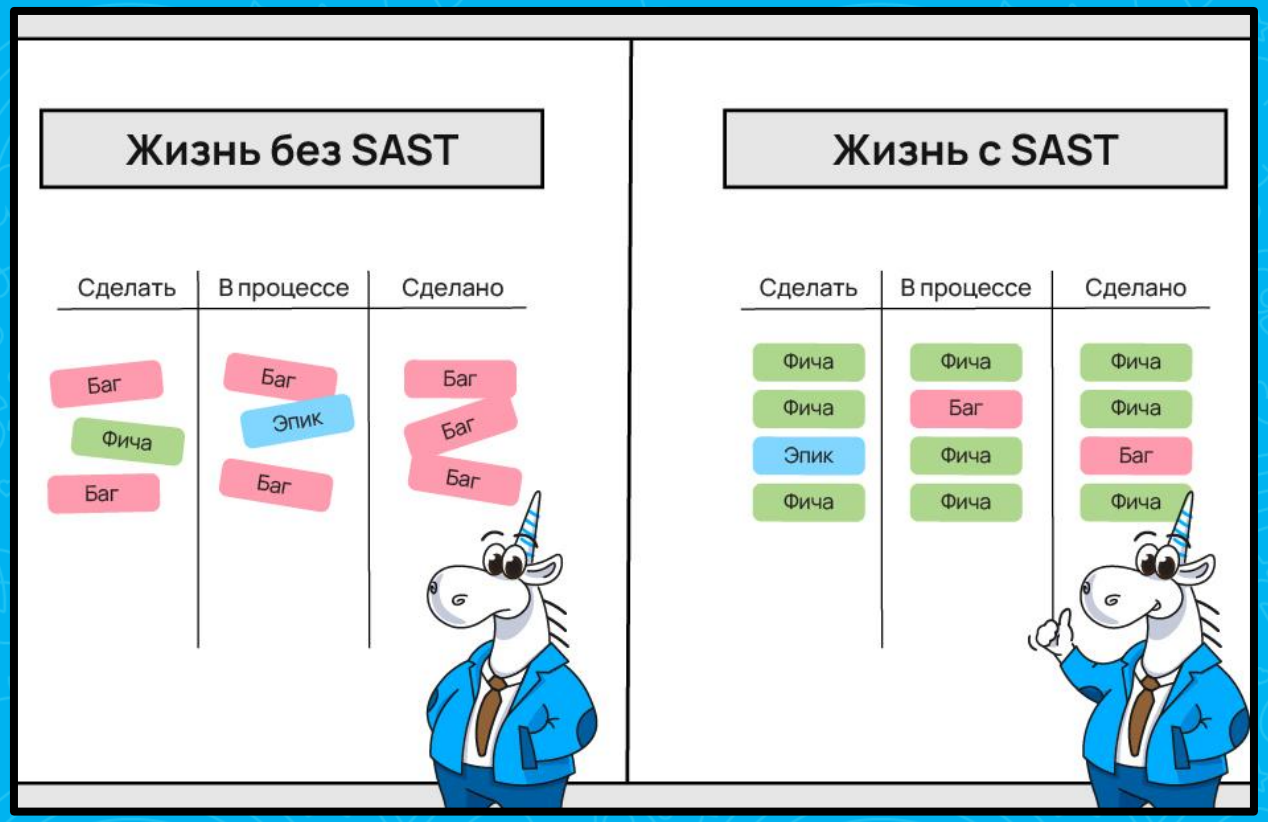


Что такое SAST?



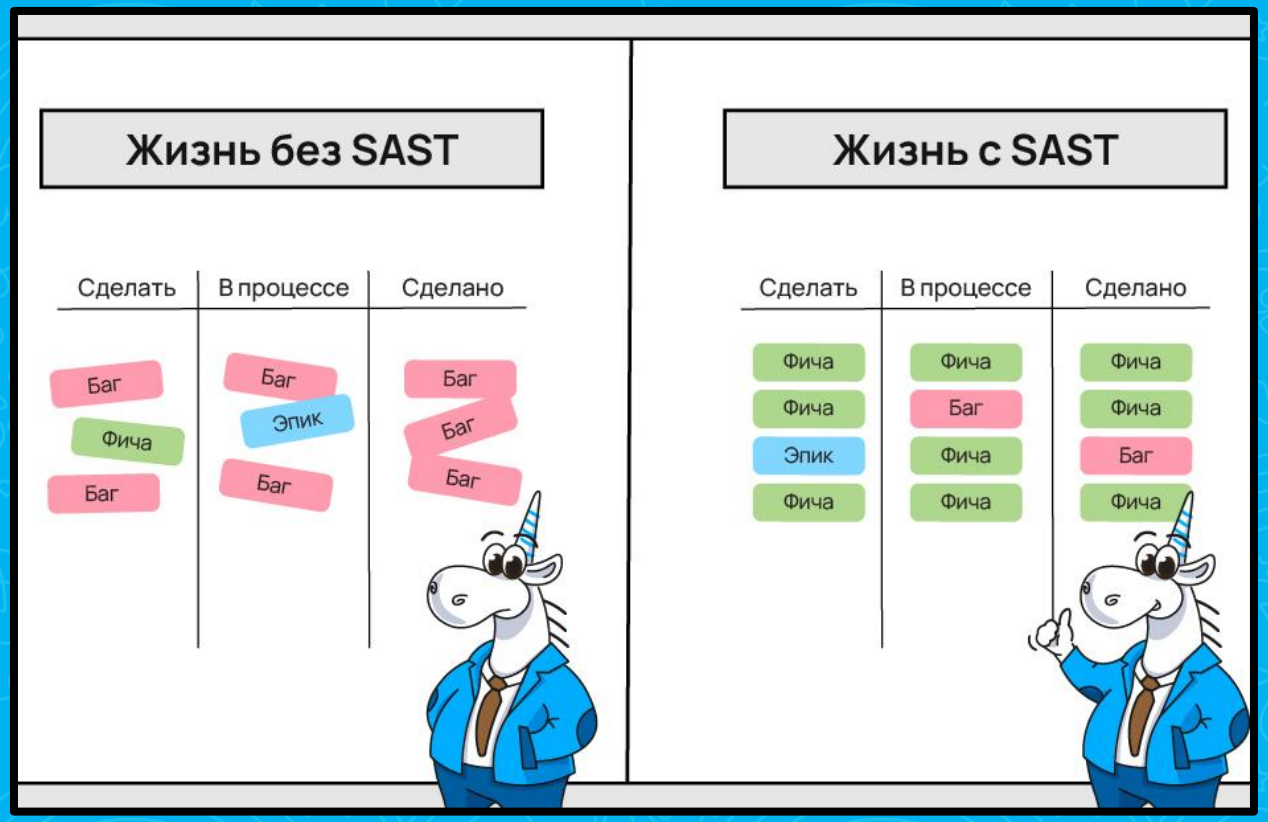
Что такое SAST?

- Статический анализ, но про уязвимости



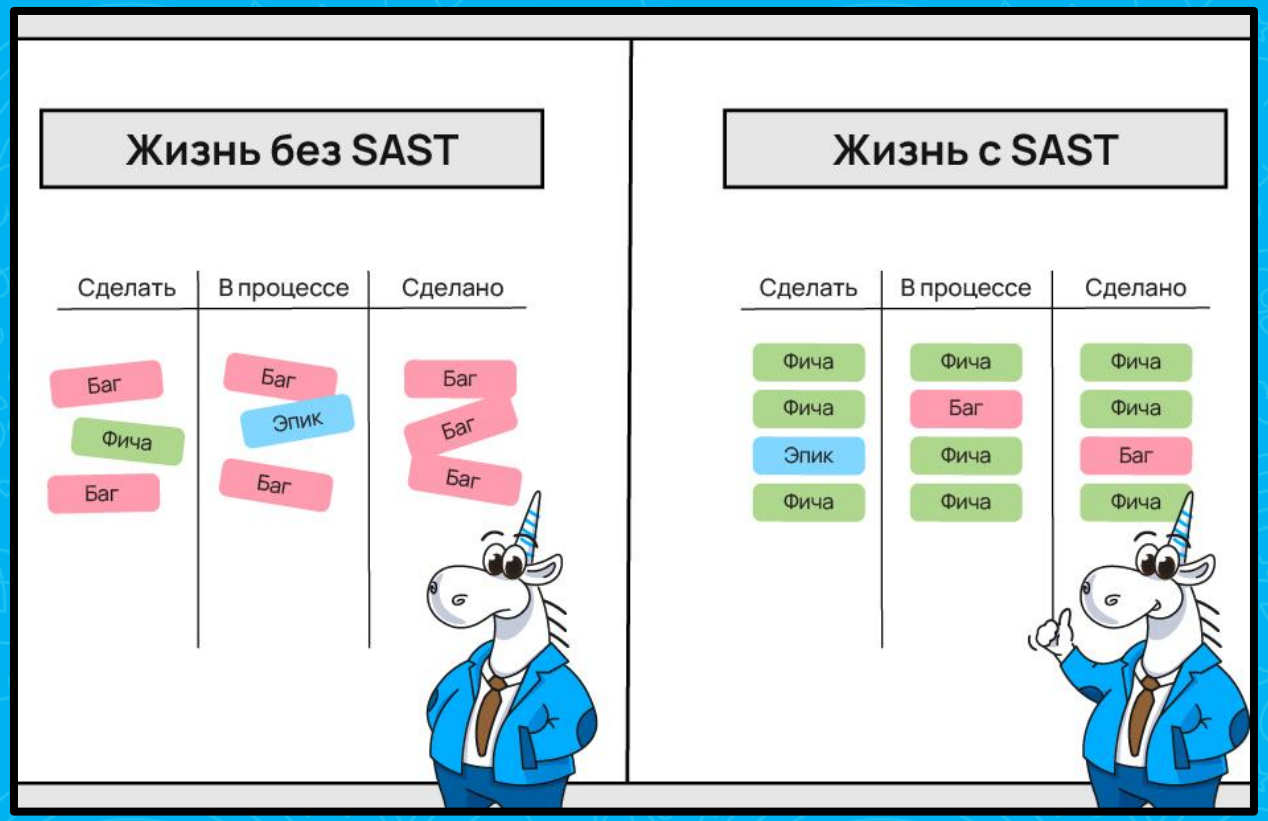
Что такое SAST?

- Статический анализ, но про уязвимости
- Нужен только код



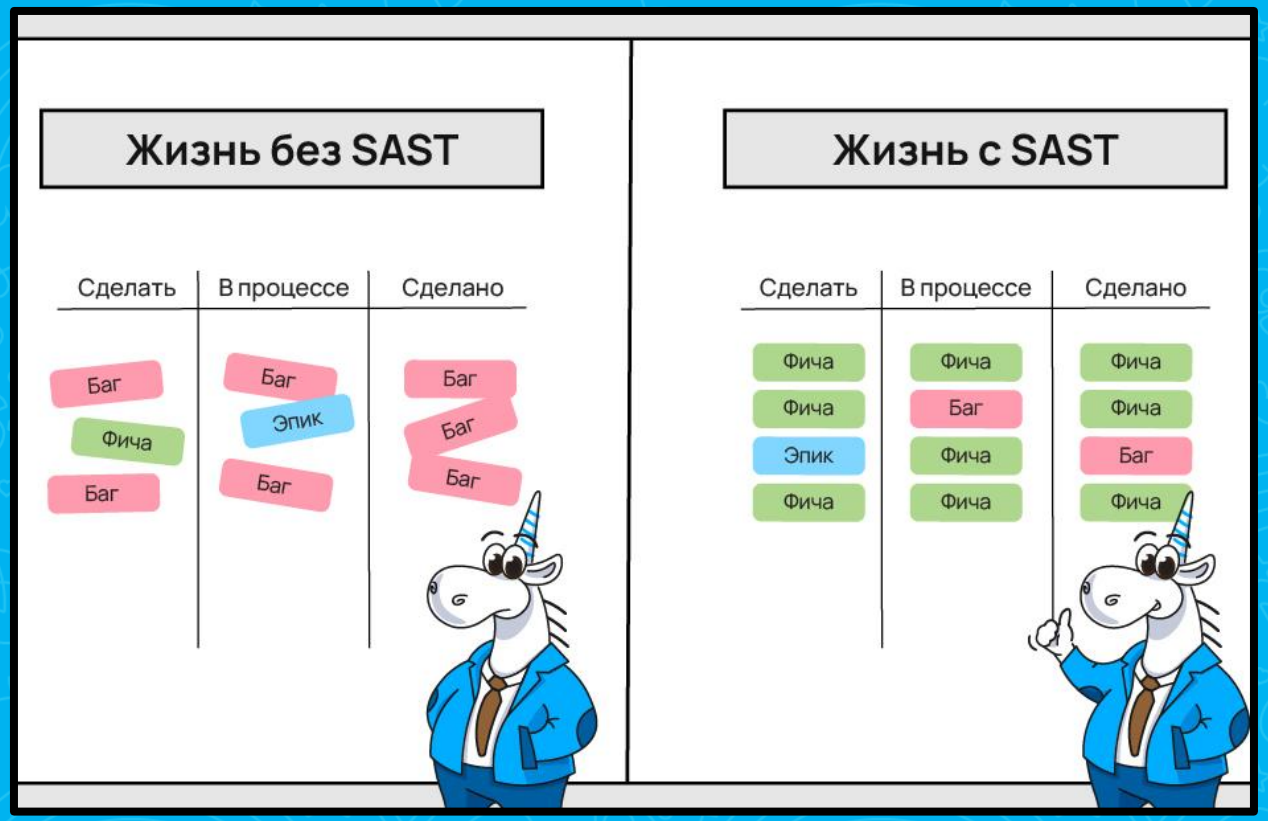
Что такое SAST?

- Статический анализ, но про уязвимости
- Нужен только код
- Полное покрытие



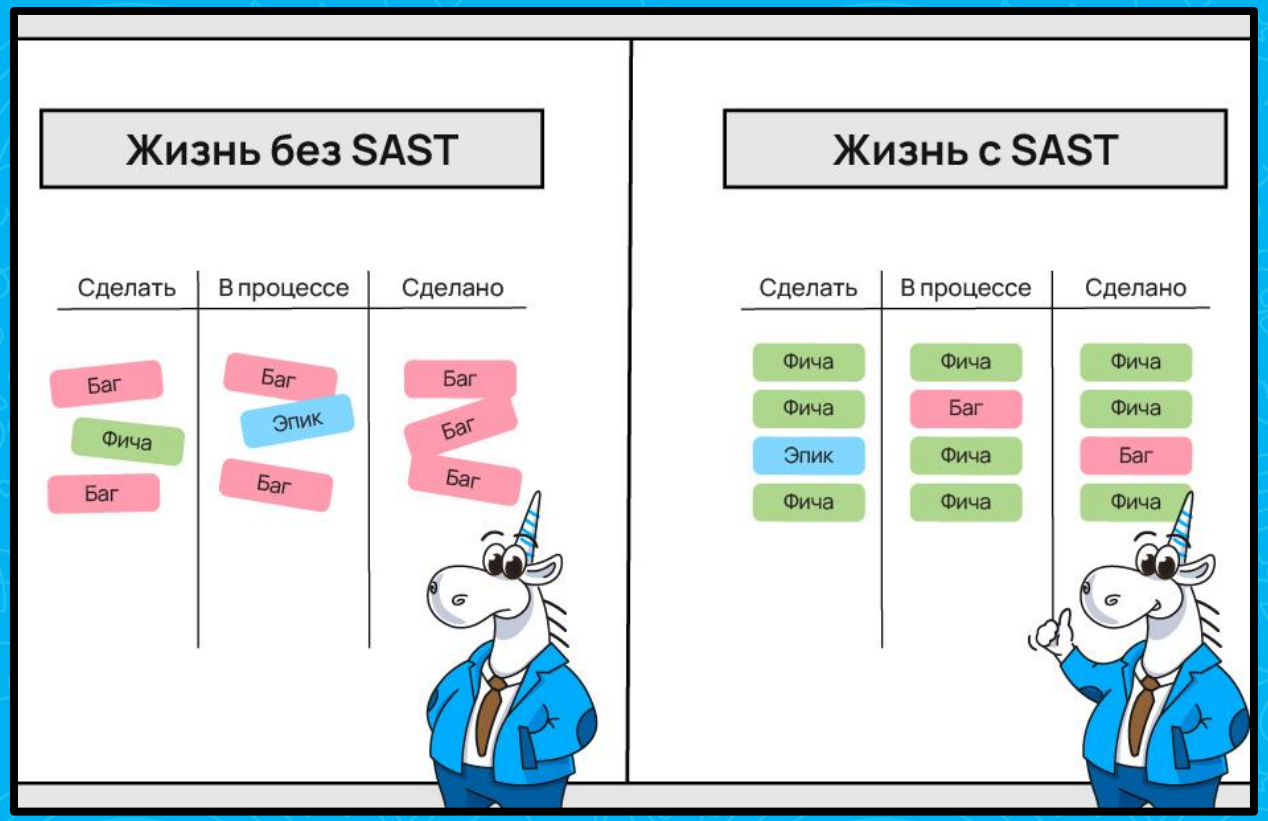
Что такое SAST?

- Статический анализ, но про уязвимости
- Нужен только код
- Полное покрытие
- Раннее обнаружение ошибок и уязвимостей



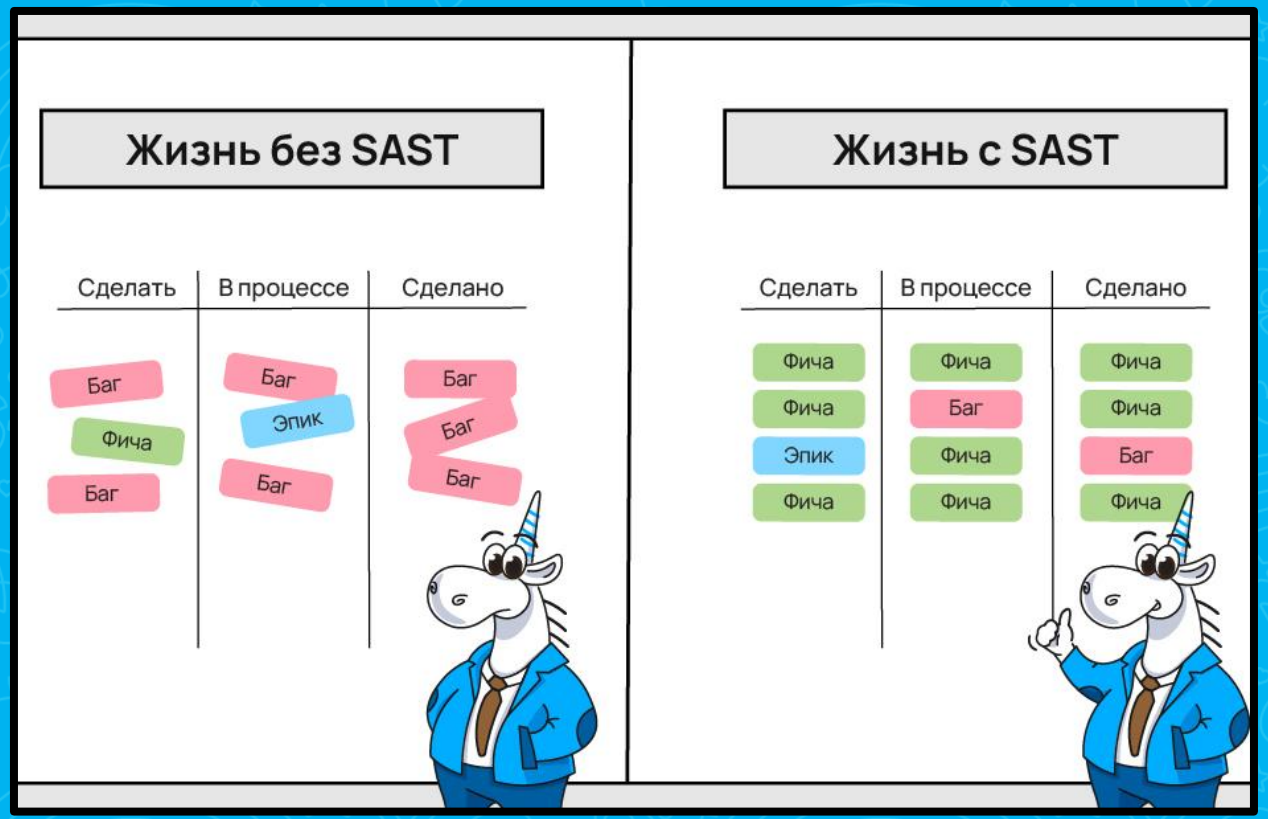
Что такое SAST?

- Статический анализ, но про уязвимости
- Нужен только код
- Полное покрытие
- Раннее обнаружение ошибок и уязвимостей
- Исправление до этапа тестирования



Что такое SAST?

- Статический анализ, но про уязвимости
- Нужен только код
- Полное покрытие
- Раннее обнаружение ошибок и уязвимостей
- Исправление до этапа тестирования
- PVS-Studio – это SAST инструмент



Пример CWE в проекте FastReport

```
ParagraphFormat paragraphFormat;

....
public ParagraphFormat ParagraphFormat
{
  get { return paragraphFormat; }
  set { ParagraphFormat = value; }
}
```

Пример CWE в проекте FastReport

```
ParagraphFormat paragraphFormat;
....
public ParagraphFormat ParagraphFormat
{
  get { return paragraphFormat; }
  set { ParagraphFormat = value; }
}
```

Поле

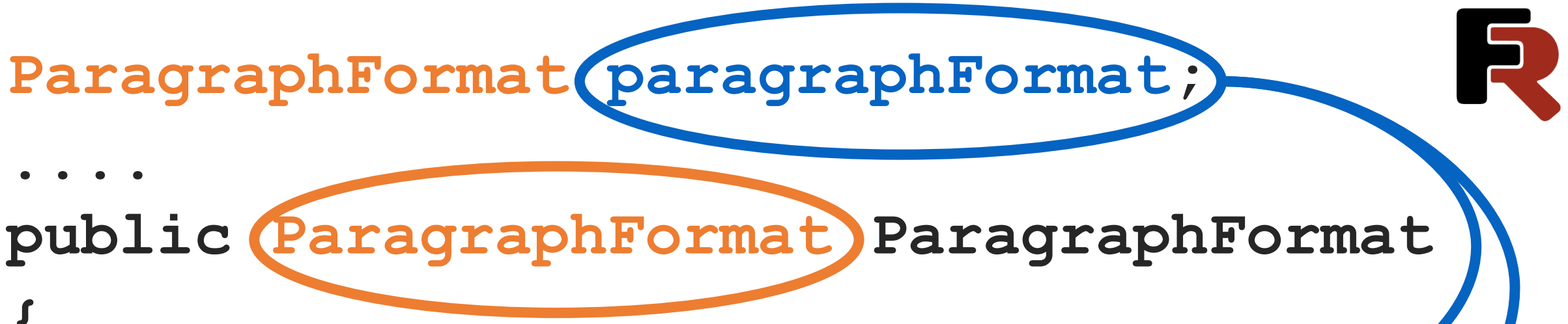
Пример CWE в проекте FastReport

```
ParagraphFormat paragraphFormat;
....
public ParagraphFormat ParagraphFormat
{
  get { return paragraphFormat; }
  set { ParagraphFormat = value; }
}
```

Поле

Свойство

Пример CWE в проекте FastReport



```
ParagraphFormat paragraphFormat;
....
public ParagraphFormat ParagraphFormat
{
  get { return paragraphFormat; }
  set { ParagraphFormat = value; }
}
```

Пример CWE в проекте FastReport

```
ParagraphFormat paragraphFormat;
....
public ParagraphFormat ParagraphFormat
{
  get { return paragraphFormat; }
  set { ParagraphFormat = value; }
}
```

Пример CWE в проекте FastReport

```
ParagraphFormat paragraphFormat;
....
public ParagraphFormat ParagraphFormat
{
  get { return paragraphFormat; }
  set { ParagraphFormat = value; }
}
```

Пример CWE в проекте FastReport

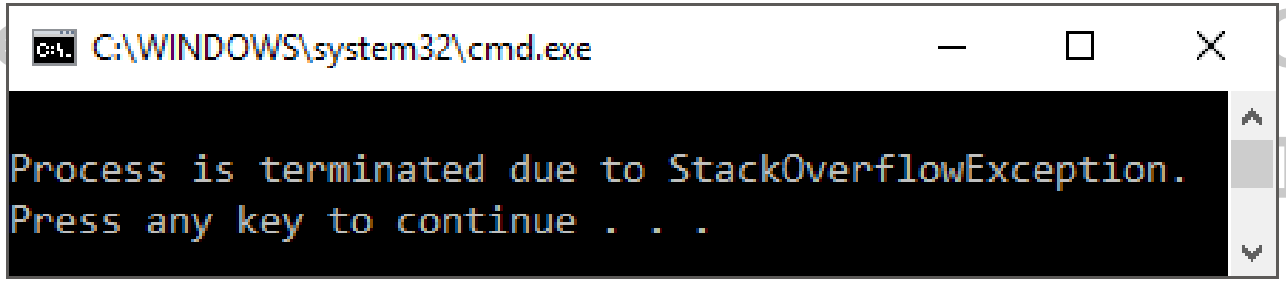
```
static void Main(string[] args)
{
  TextObject textObj = new TextObject();
  textObj.ParagraphFormat = null;

  Console.WriteLine("Ok");
}
```

Пример CWE в проекте FastReport

```
static void Main(string[] args)
{
    TextObj                                    Object();
    textObj                                    1;

    Console.WriteLine("Ok");
}
```

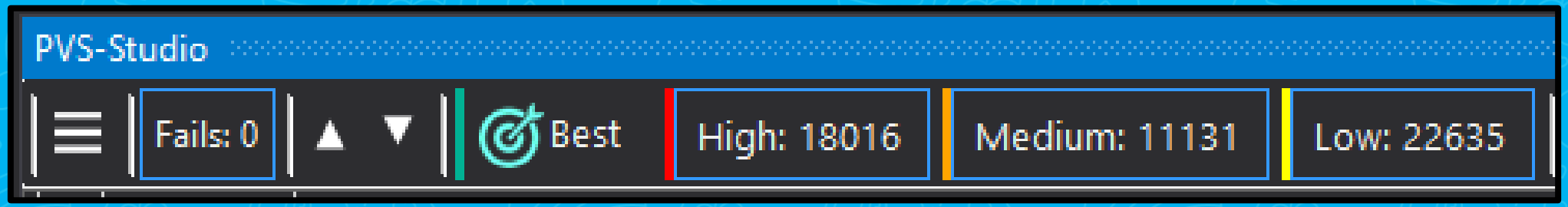


Пример CWE в проекте FastReport

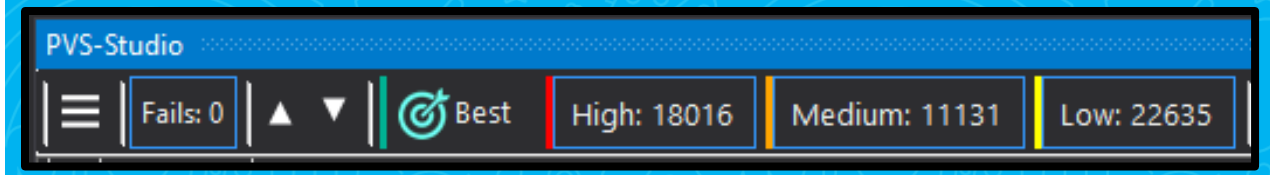
```
ParagraphFormat paragraphFormat;
....
public ParagraphFormat ParagraphFormat
{
  get { return paragraphFormat; }
  set { ParagraphFormat = value; }
```

Предупреждение PVS-Studio: V3010 [CWE-674] Possible infinite recursion inside ' ParagraphFormat' property.

Разбираем проблемы при интеграции в legacy проект


PVS-Studio
Fails: 0
Best
High: 18016
Medium: 11131
Low: 22635

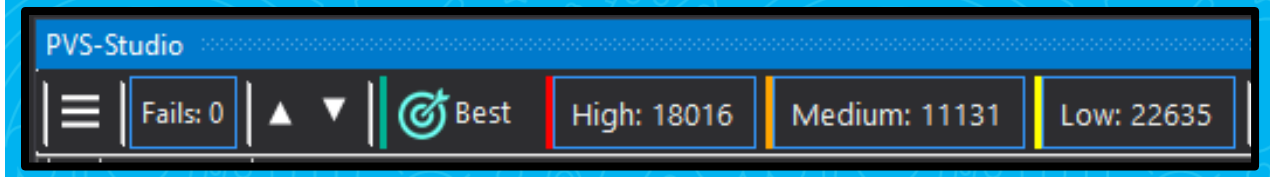
Опасность первого раза



Опасность первого раза

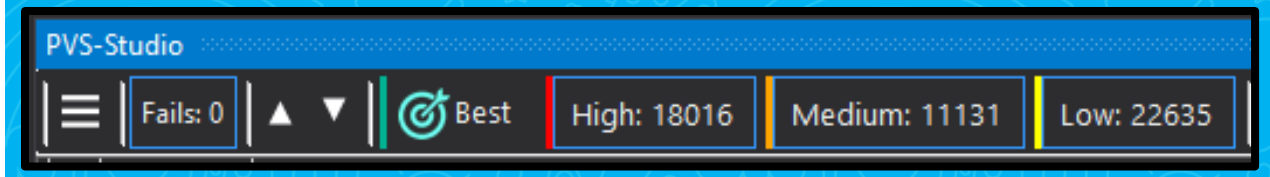
- Много срабатываний ==

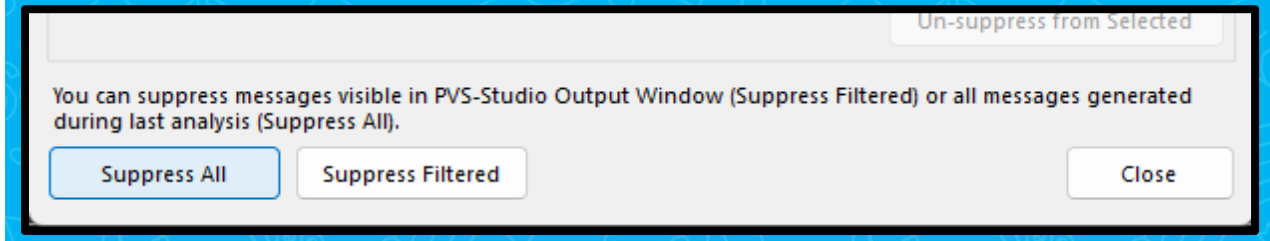
  нормально



Опасность первого раза

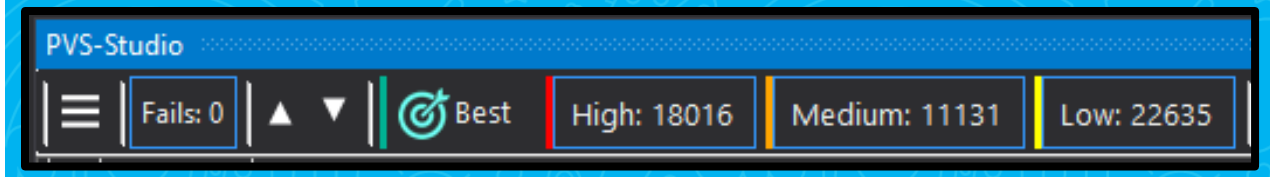
- Много срабатываний == нормально
- **Используем массовое подавление**

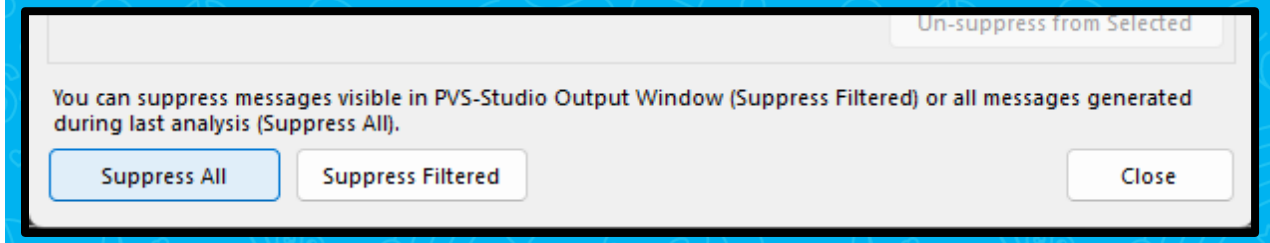




Опасность первого раза

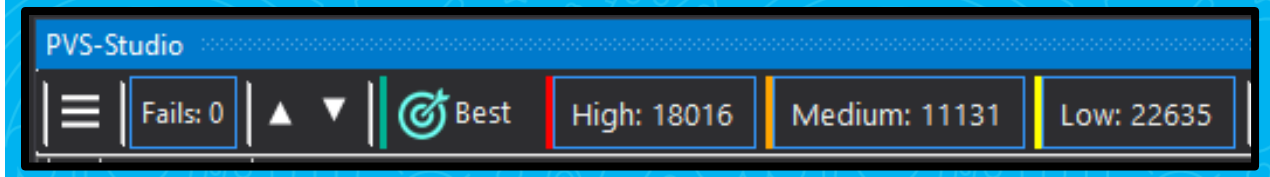
- Много срабатываний == нормально
- **Используем массовое подавление**
- Периодически возвращаемся и чиним

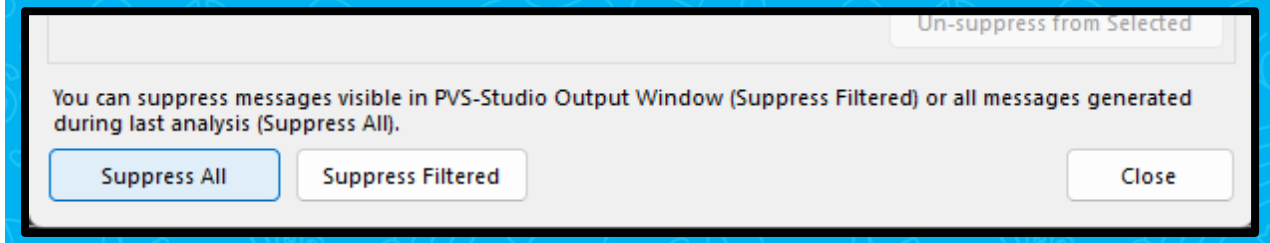




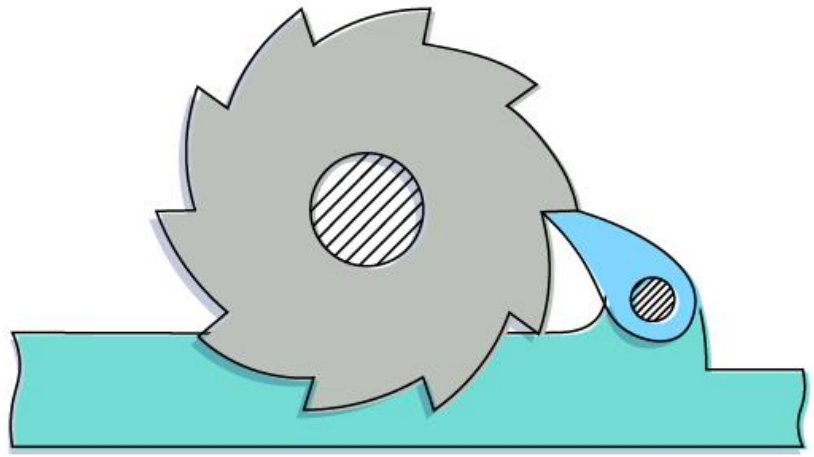
Опасность первого раза

- Много срабатываний == нормально
- **Используем массовое подавление**
- Периодически возвращаемся и чиним



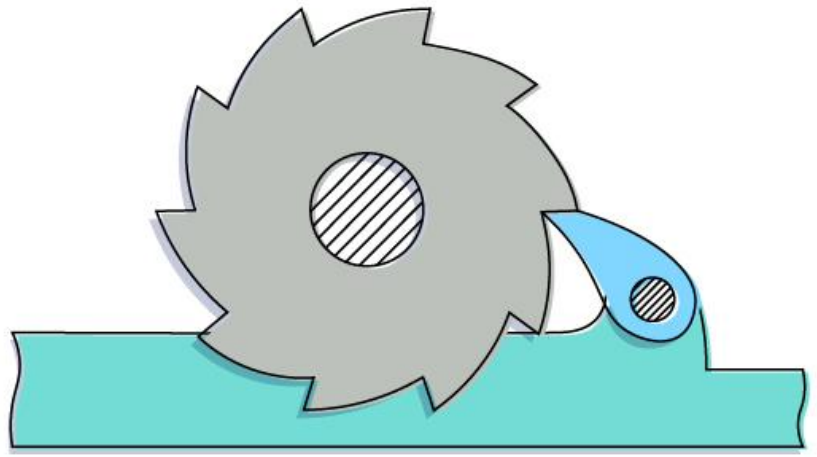


Принцип Храповика



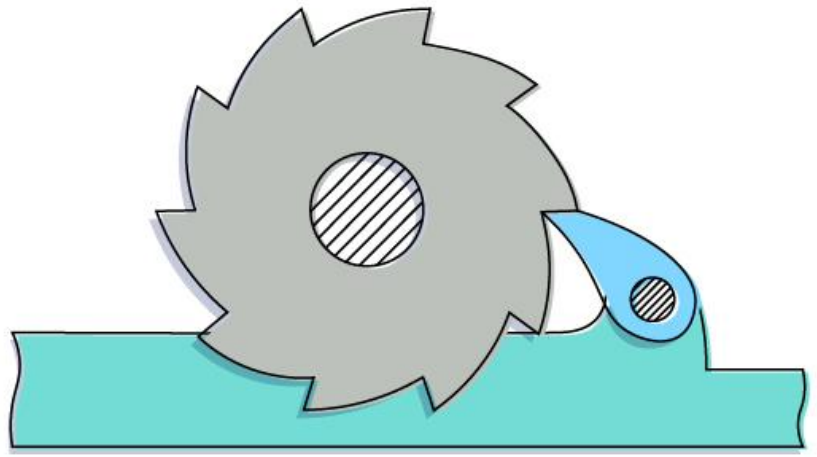
Принцип Храповика

- Выполняем анализ



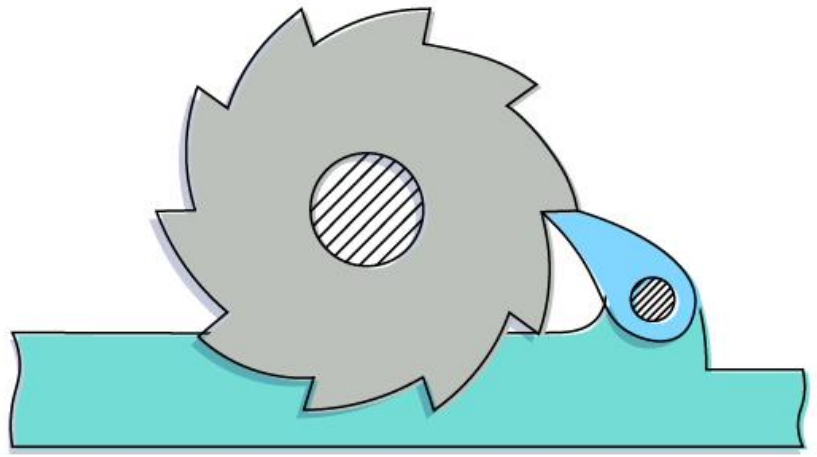
Принцип Храповика

- Выполняем анализ
- **Заносим в систему контроля версий и устанавливаем порог вхождения**



Принцип Храповика

- Выполняем анализ
- **Заносим в систему контроля версий и устанавливаем порог вхождения**
- Исправляем!



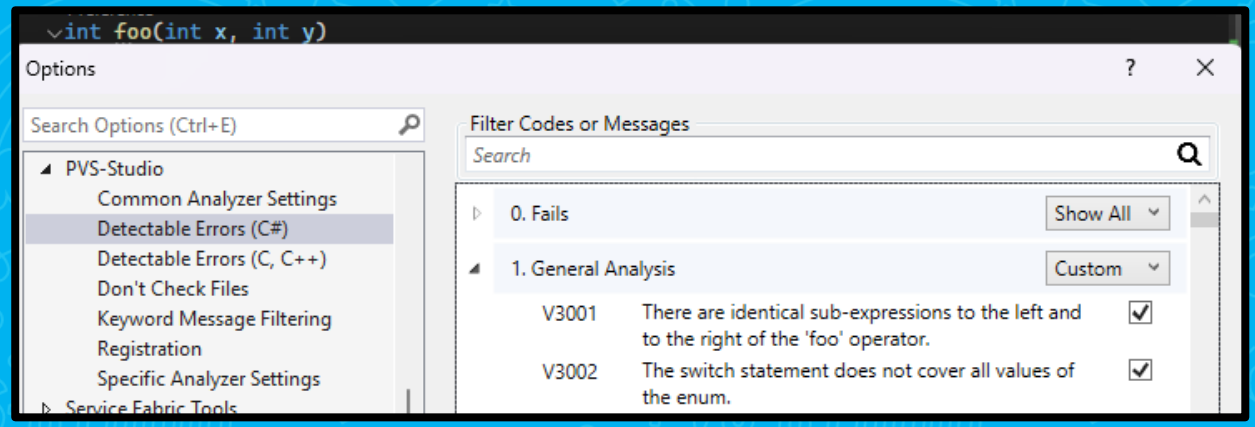
Ложные срабатывания

Ложные срабатывания

- Особенность технологии

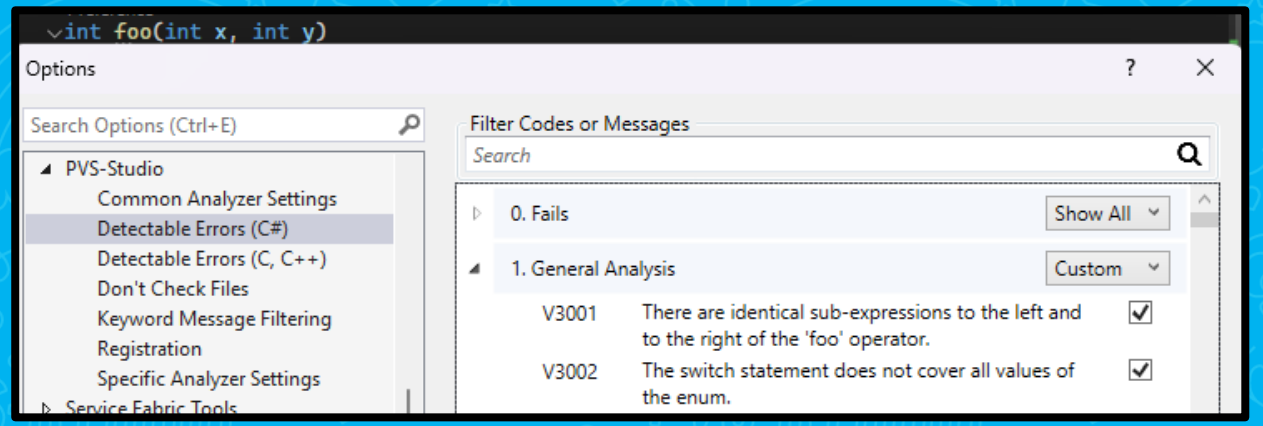
Ложные срабатывания

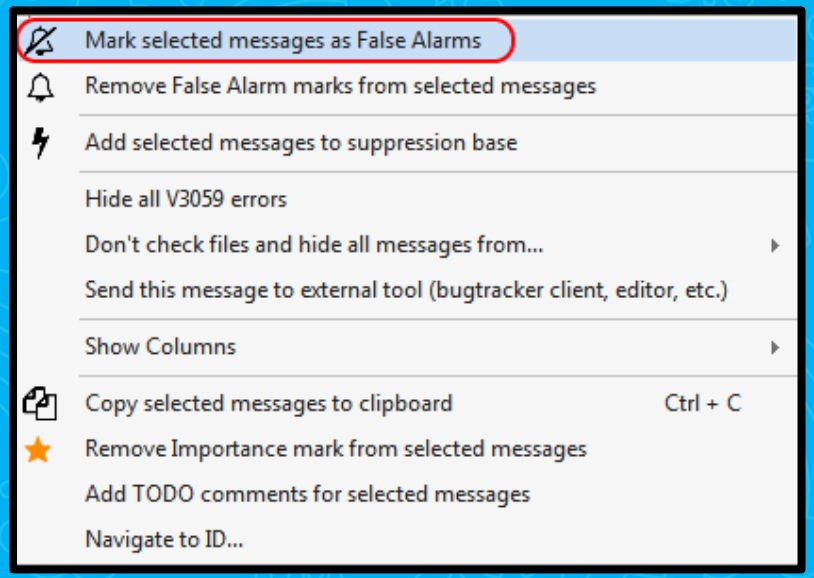
- Особенность технологии
- **Настраиваем анализатор под проект**



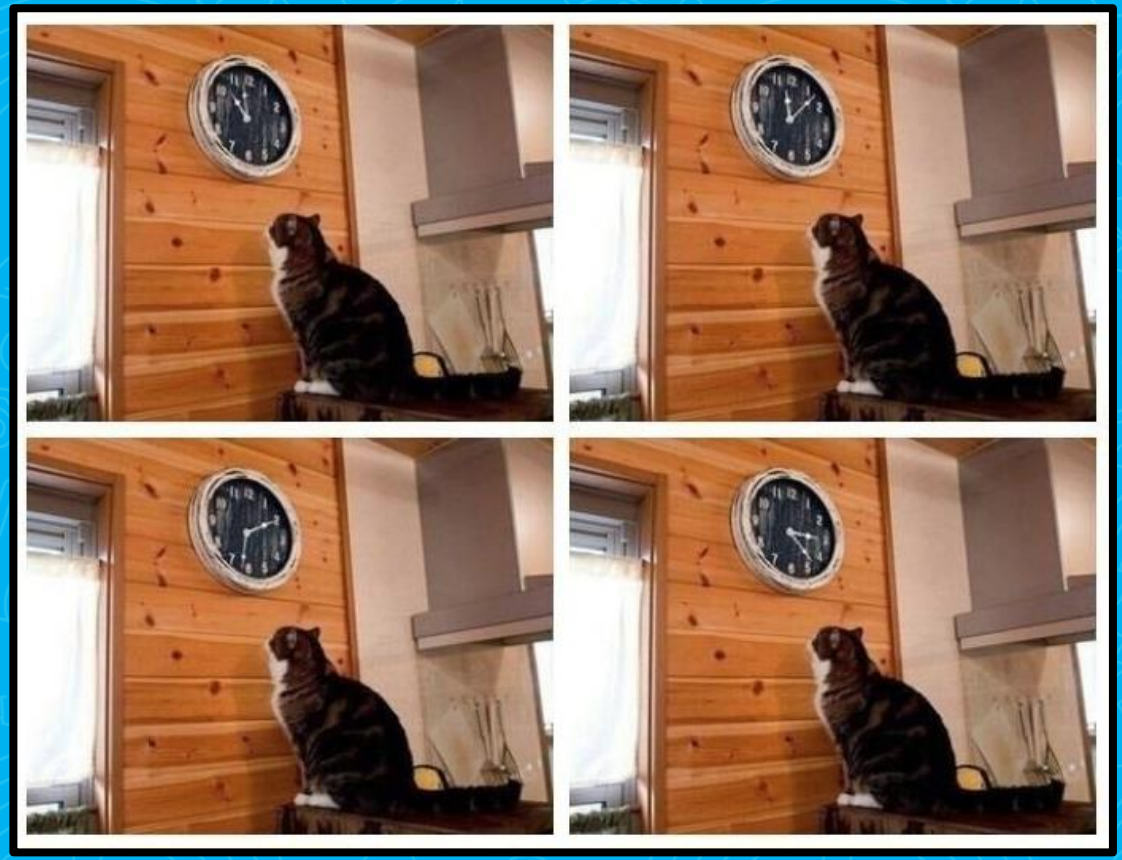
Ложные срабатывания

- Особенность технологии
- **Настраиваем анализатор под проект**



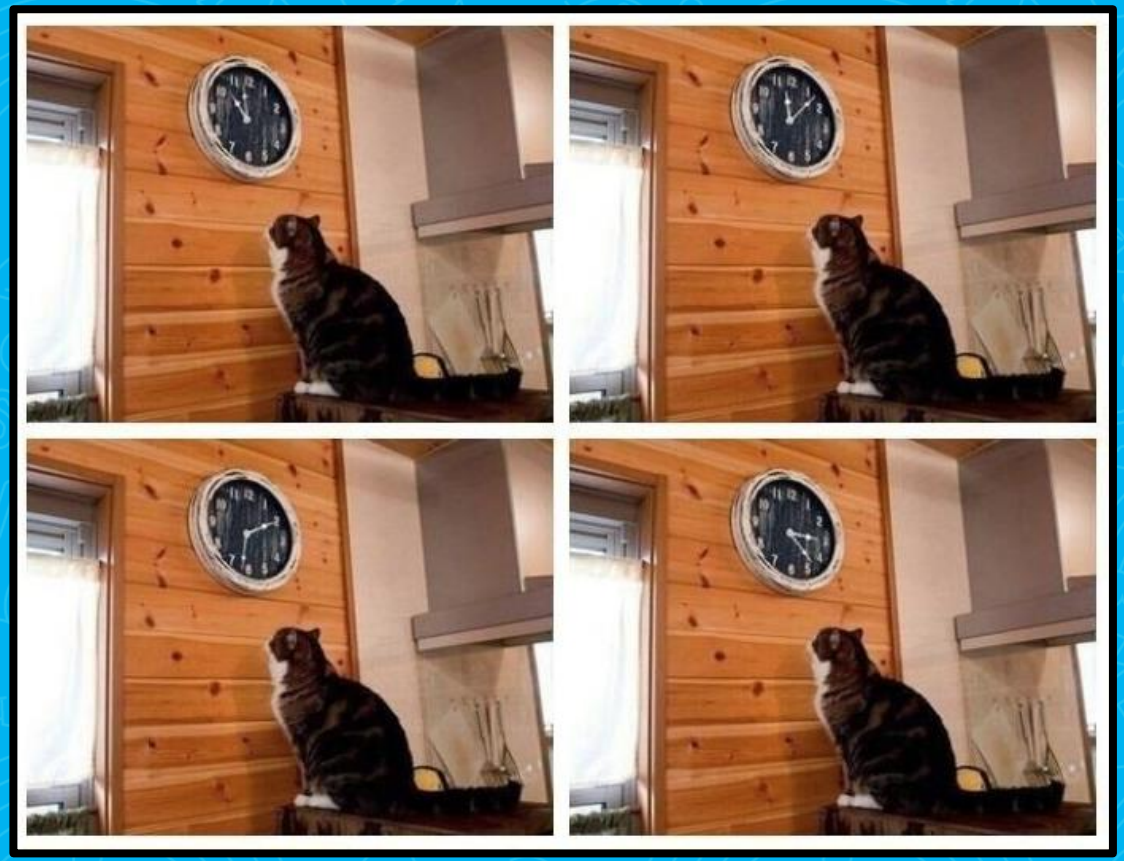


Долго время анализа



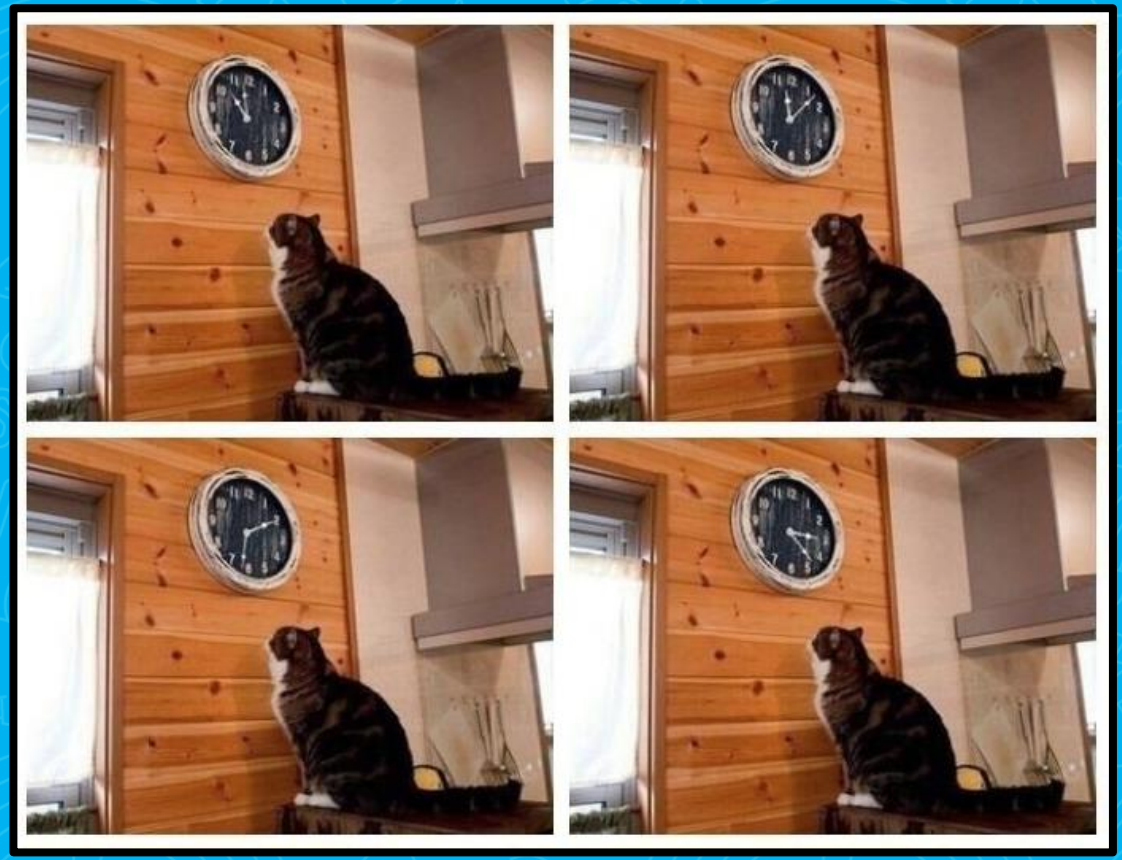
Долго время анализа

- Больше проект == больше время



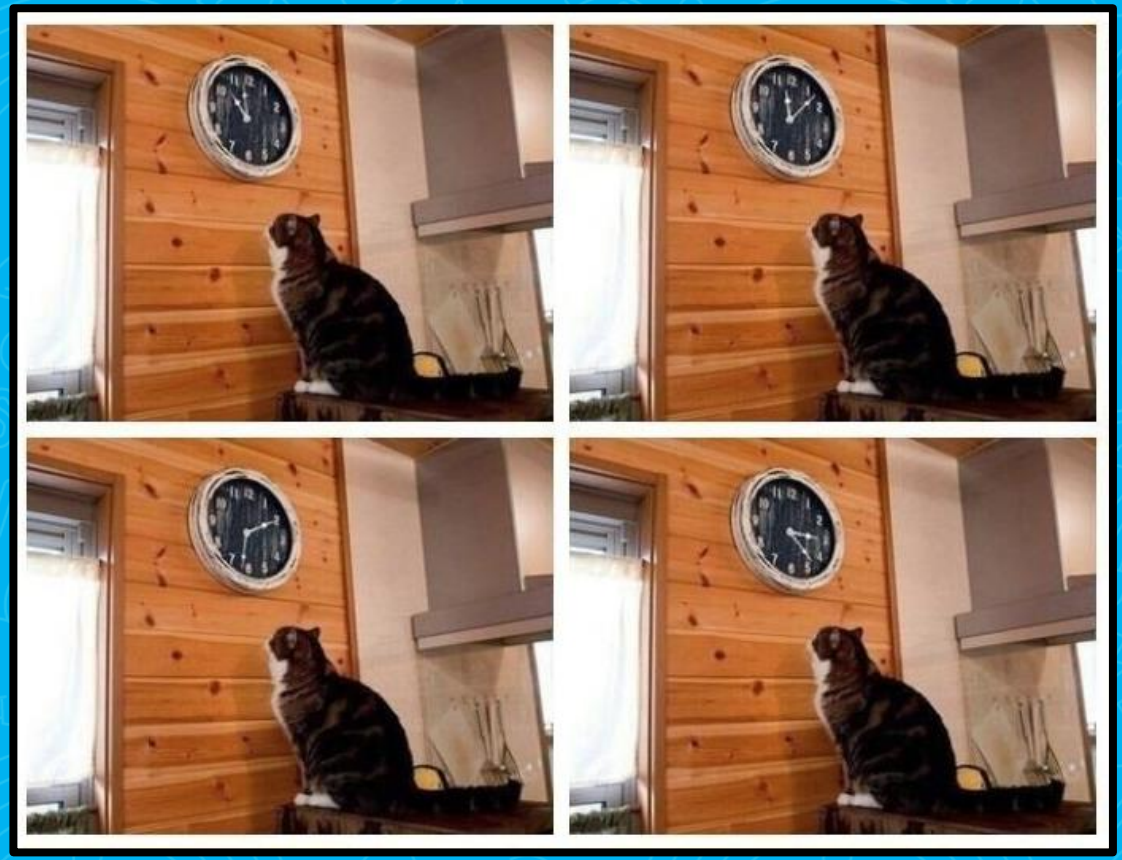
Долго время анализа

- Больше проект == больше время
- **Инкрементальный анализ**

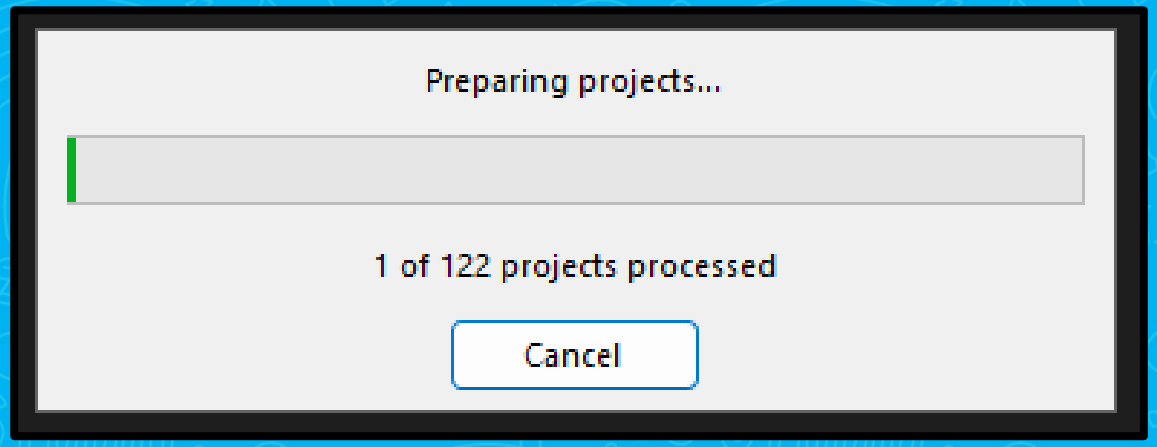


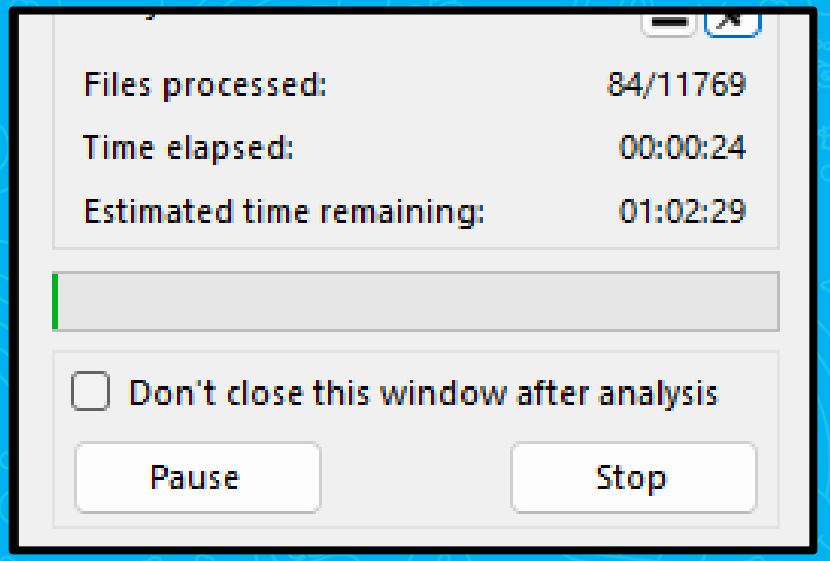
Долго время анализа

- Больше проект == больше время
- **Инкрементальный анализ**
- Проверяйте только **изменённый код**



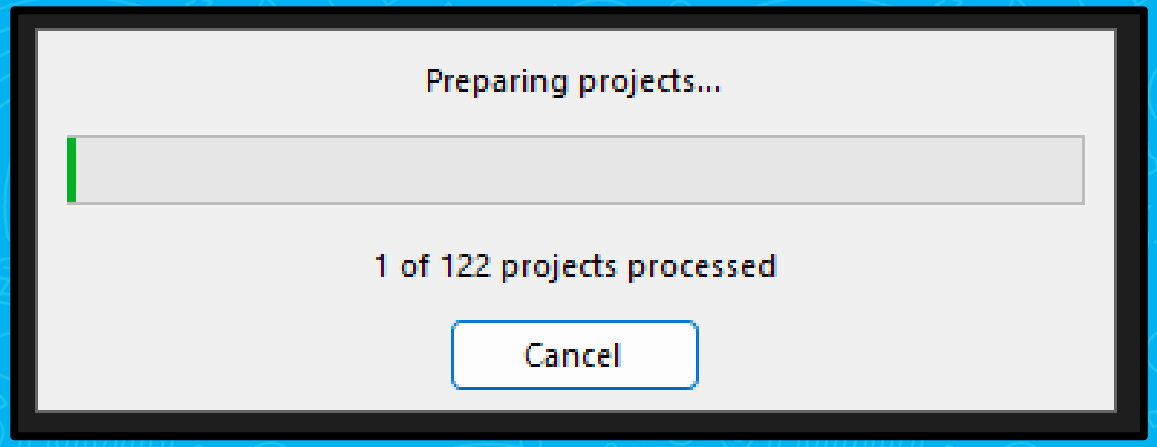
«Избыточный» анализ

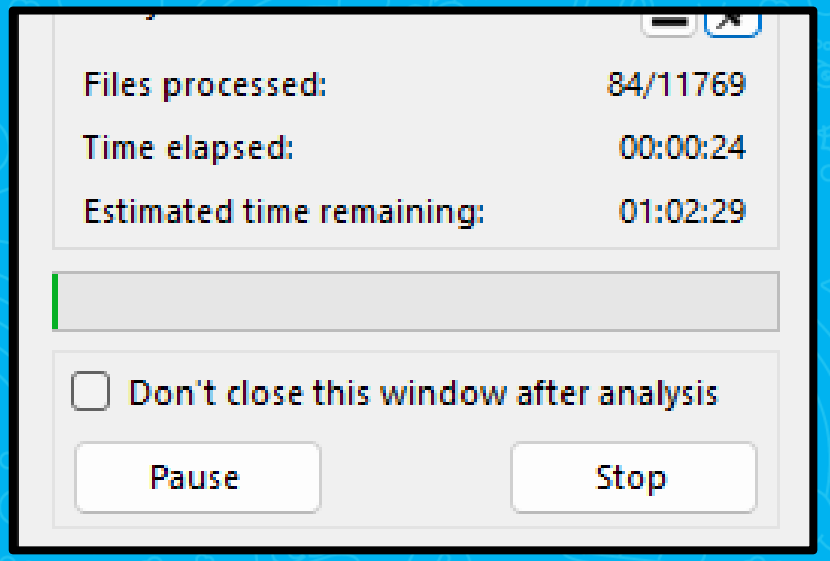




«Избыточный» анализ

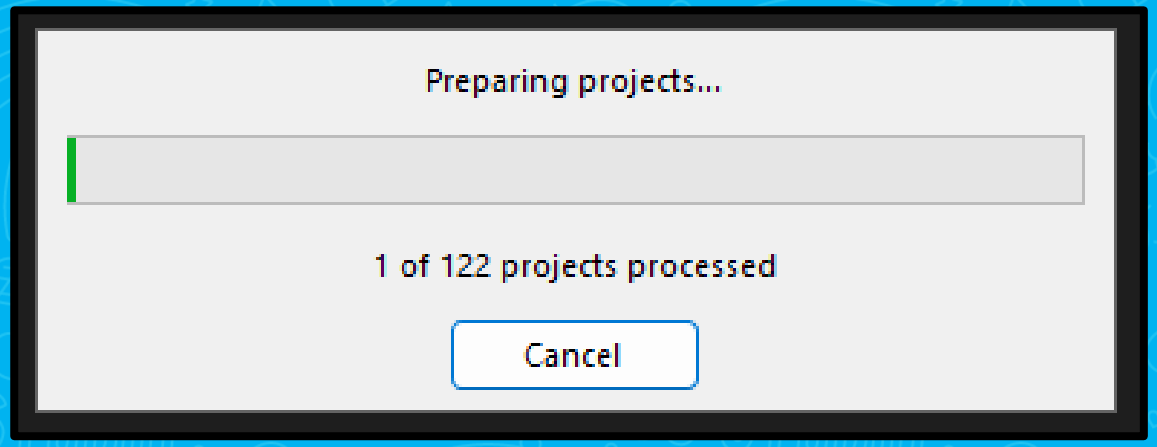
- Лишние файлы, внешние библиотеки

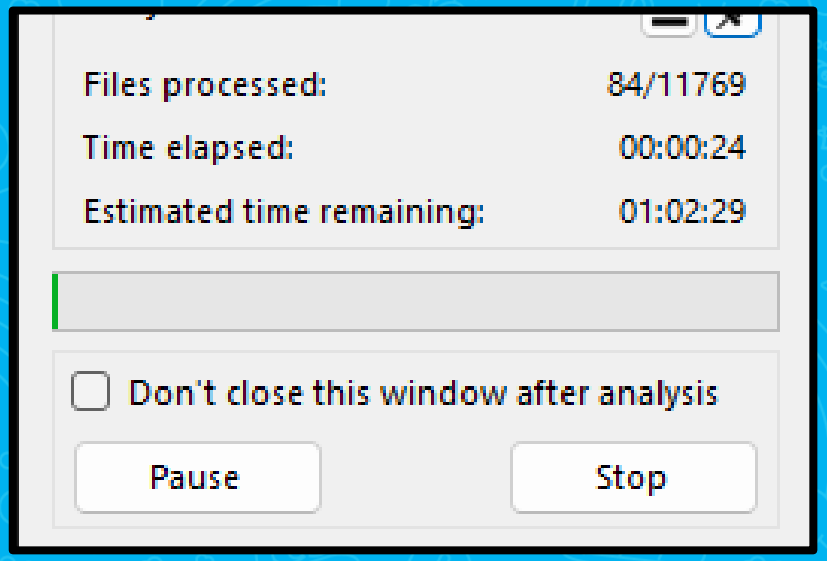




«Избыточный» анализ

- Лишние файлы, внешние библиотеки
- **Возвращаемся к настройке!**





Не хватает диагностик

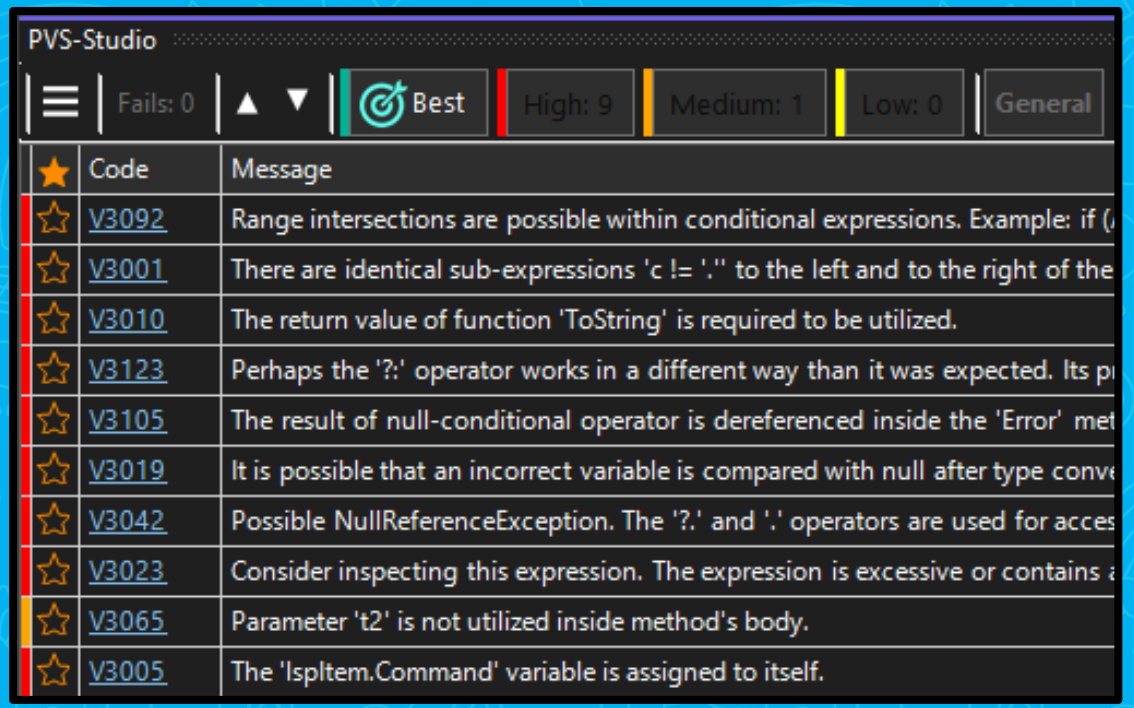
- Анализатор не идеален
- Но все решаемо!
- **Пишем в поддержку**

Привет, спишь?)

Мне нужна диагностика которая найдет вот это:

Как быстро попробовать?

- Написать проект самому?
- Взять опен-сурс?
- Использовать на целевом?
- **Попробовать TOP 10!**



Устранение неисправностей при работе PVS-Studio

Советы по повышению скорости работы PVS-Studio

Q&A

Глеб Асламов

C# Developer & DevRel