GUARD CONF

SAST в DevSecOps

Как не оставить уязвимостям ни шанса



Валерий Филатов

Developer Advocate & Project Lead
PVS-Studio



О спикере

- Занимаюсь разработкой и поддержкой интеграций продукта — от IDE до CI/CD
- Регулярно выступаю на конференциях, митапах и вебинарах. Пишу статьи, документацию и другие технические тексты.
- Выпустил несколько групп начинающих Python-разработчиков.
- Веду авторский Telegram-канал о разработке и технологиях.

Валерий Филатов

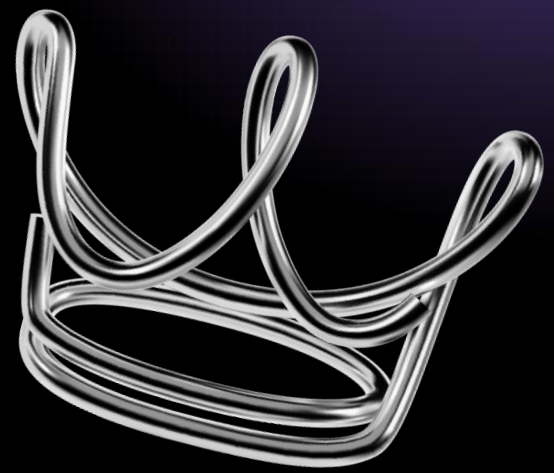
Developer Advocate & Project Lead
PVS-Studio



GUARDCORE

Часть первая

Что такое SAST



Static Application Security Testing

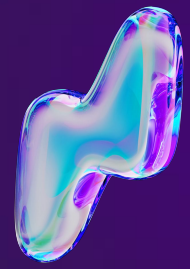
Набор технологий, предназначенных для анализа исходного кода ПО в области безопасности.



GUARDCORE

Потенциальная уязвимость

Ошибка, которая может быть использована для нарушения целостности системы или влияния на её логику работы.



FreeSwitch

```
static const char *basic_gets(int *cnt)
{
  ....
  int c = getchar();
  if (c < 0) {
    if (fgets(command_buf, sizeof(command_buf) - 1, stdin)
          != command_buf) {
      break;
    }
    command_buf[strlen(command_buf)-1] = '\0';
    break;
  }
  ....
}
```

FreeSwitch

```
static const char *basic_gets(int *cnt)
{
  ....
  int c = getchar();
  if (c < 0) {
     if (fgets(command_buf, sizeof(command_buf) - 1, stdin)
           != command_buf) {
       break;
     }
     command_buf[strlen(command_buf)-1] = '\0';
     break;
  }
  ....
}
```

FreeSwitch

```
static const char *basic_gets(int *cnt)
{
  ....
  int c = getchar();
  if (c < 0) {
    if (fgets(command_buf, sizeof(command_buf) - 1, stdin)
          != command_buf) {
      break;
    }
    command_buf[strlen(command_buf)-1] = '\0';
    break;
  }
  ....
}
```

V1010 Unchecked tainted data is used in index: 'strlen(command_buf)'.

```
int m_offsetFromUtc;
....
void QDateTime::setMSecsSinceEpoch(qint64 msecs)
{
  ....
  if (!add_overflow(msecs,
                    qint64(d->m_offsetFromUtc * 1000),
                    &msecs))
    status |= QDateTimePrivate::ValidWhenMask;
  ....
}
```

Qt

```
int m_offsetFromUtc;
....
void QDateTime::setMSecsSinceEpoch(qint64 msecs)
{
  ....
  if (!add_overflow(msecs,
                    qint64(d->m_offsetFromUtc * 1000),
                    &msecs))
    status |= QDateTimePrivate::ValidWhenMask;
  ....
}
```

V1028 Possible overflow. Consider casting operands of the 'd->m_offsetFromUtc * 1000' operator to the 'qint64' type, not the result.

IronPython

```
class DictThreadGlobalState {
  public int DoneCount;
  ....
}
private static void RunThreadTest(
  DictThreadGlobalState globalState) {
  ....
  globalState.DoneEvent.Reset();
  globalState.Event.Set();
  while (globalState.DoneCount != 0) {
    // wait for threads to get back to finish
  }
  ....
}
```

IronPython

```
class DictThreadGlobalState {
  public int DoneCount;
  ....
}
private static void RunThreadTest(
  DictThreadGlobalState globalState) {
  ....
  globalState.DoneEvent.Reset();
  globalState.Event.Set();
  while (globalState.DoneCount != 0) {
    // wait for threads to get back to finish
  }
  ....
}
```

V3032 Waiting on this expression is unreliable, as compiler may optimize some of the variables. Use volatile variable(s) or synchronization primitives to avoid this.

GUARDCORE

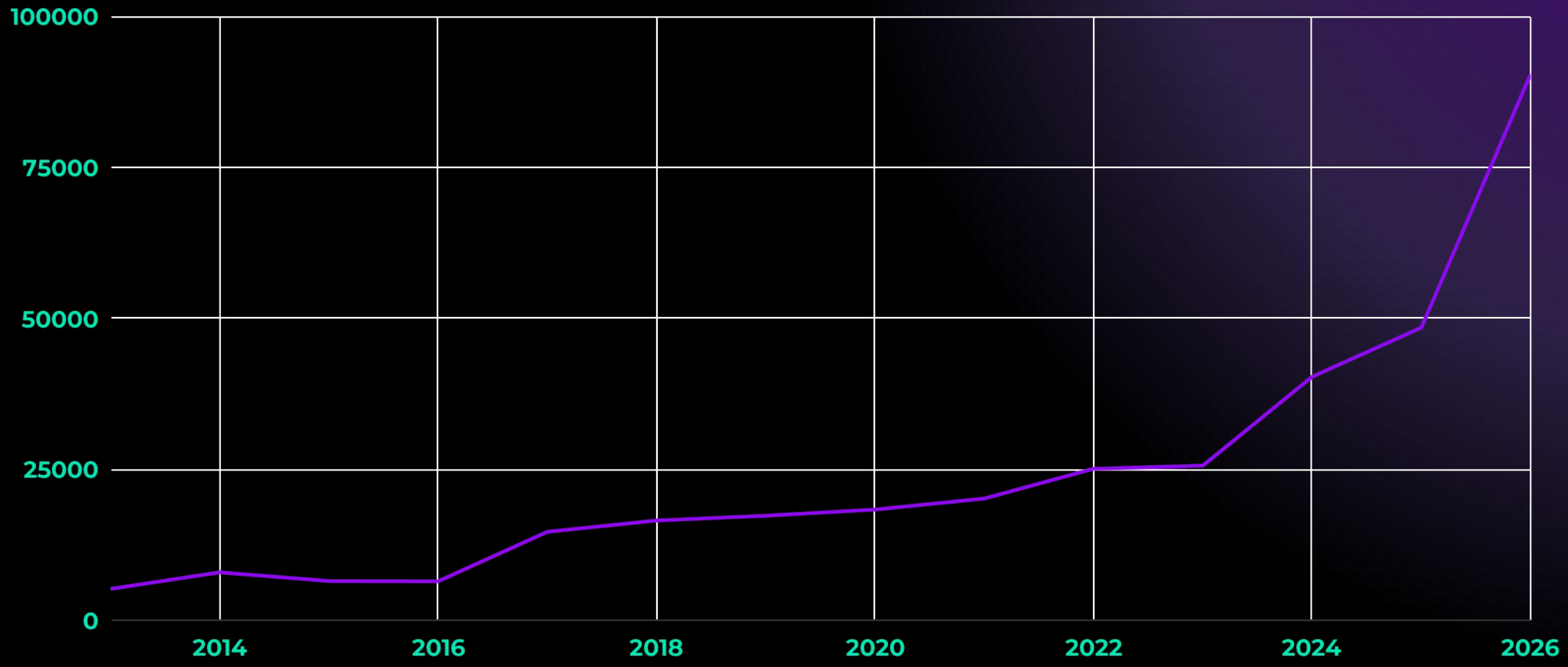
А зачем?







Число выявленных уязвимостей



Источник – cvedetails.com

GUARDCORE

Часть вторая

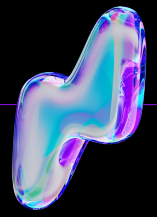
Это база



Опора для SAST

GUARDCONF

Стандарты и перечисления – источник вдохновения для правил.



CWE

Самый большой в мире список потенциальных уязвимостей.

Опора для SAST

Стандарты и перечисления – источник вдохновения для правил.



CWE

Самый большой в мире список потенциальных уязвимостей.



OWASP ASVS

Стандарт для поддержки безопасности веб-приложений и не только.

Опора для SAST

GUARDCONF

Стандарты и перечисления – источник вдохновения для правил.



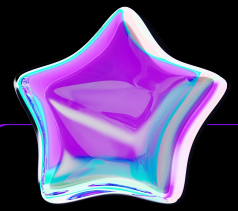
CWE

Самый большой в мире список потенциальных уязвимостей.



OWASP ASVS

Стандарт для поддержки безопасности веб-приложений и не только.



ГОСТ Р 71207-2024

Ответвление стандарта о разработке безопасного программного обеспечения, отдельно посвящённое статическому анализу.

GUARDCORE

Что за ГОСТ?

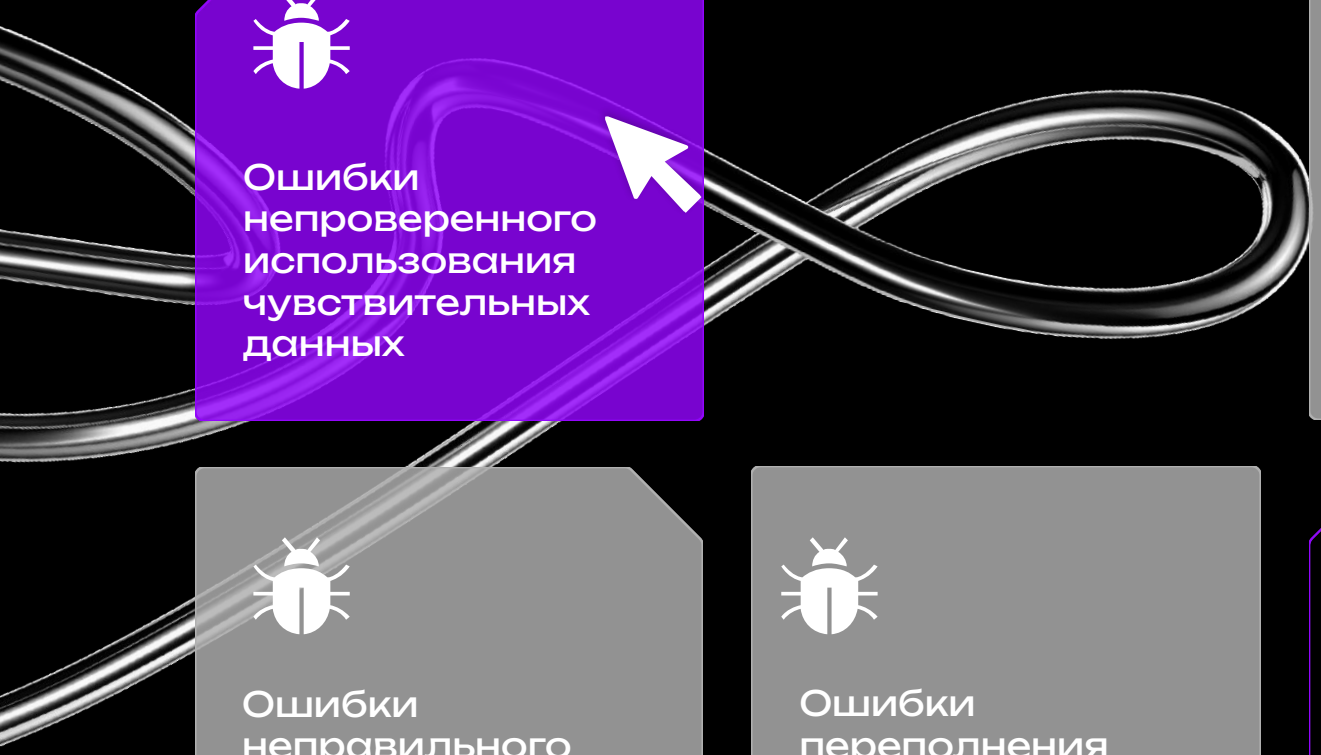






Критические ошибки

GUARDCORE



Ошибки непроверенного использования чувствительных данных

Ошибки переполнения и некорректного использования чисел

Ошибки неправильного использования процедур и интерфейсов

Ошибки переполнения буфера

Ошибки при работе с многопоточными примитивами

Критические ошибки

GUARDCORE

Ошибки непроверенного использования чувствительных данных

Ошибки переполнения и некорректного использования чисел

Ошибки неправильного использования процедур и интерфейсов

Ошибки переполнения буфера

Ошибки при работе с многопоточными примитивами

Критические ошибки

GUARDCORE

Ошибки непроверенного использования чувствительных данных

Ошибки переполнения и некорректного использования чисел

Ошибки неправильного использования процедур и интерфейсов

Ошибки переполнения буфера

Ошибки при работе с многопоточными примитивами

Критические ошибки

GUARDCORE

Ошибки непроверенного использования чувствительных данных

Ошибки переполнения и некорректного использования чисел

Ошибки неправильного использования процедур и интерфейсов

Ошибки переполнения буфера

Ошибки при работе с многопоточными примитивами

Критические ошибки

GUARDCORE

Ошибки непроверенного использования чувствительных данных

Ошибки переполнения и некорректного использования чисел

Ошибки неправильного использования процедур и интерфейсов

Ошибки переполнения буфера

Ошибки при работе с многопоточными примитивами

Требуемые технологии анализа

- **Data-flow анализ**
- Control-flow анализ
- Taint анализ
- Сигнатурный поиск
- Статистический анализ



Требуемые технологии анализа

GUARDCORE

- Data-flow анализ
- **Control-flow анализ**
- Taint анализ
- Сигнатурный поиск
- Статистический анализ



Требуемые технологии анализа

- Data-flow анализ
- Control-flow анализ
- **Taint анализ**
- Сигнатурный поиск
- Статистический анализ



Требуемые технологии анализа

- Data-flow анализ
- Control-flow анализ
- Taint анализ
- **Сигнатурный поиск**
- Статистический анализ



Требуемые технологии анализа

GUARDCONF

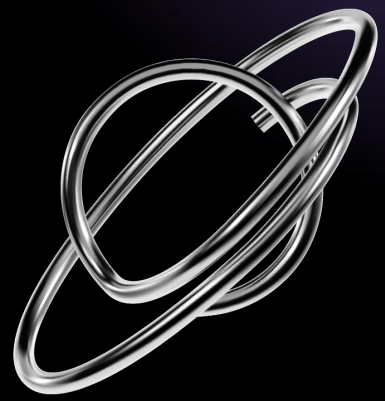
- Data-flow анализ
- Control-flow анализ
- Taint анализ
- Сигнатурный поиск
- **Статистический анализ**



GUARDCORE

Часть третья

Давай уже DevSecOps

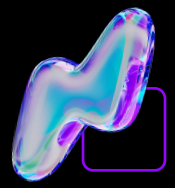


Три уровня SAST



Локальный

Анализ на машинах разработчиков из IDE или CLI.



Непрерывный

SAST становится этапом непрерывной интеграции.



Серверный

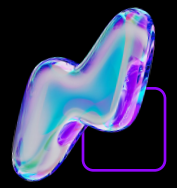
Анализ всего проекта целиком по расписанию.

Три уровня SAST



Локальный

Анализ на машинах разработчиков из IDE или CLI.



Непрерывный

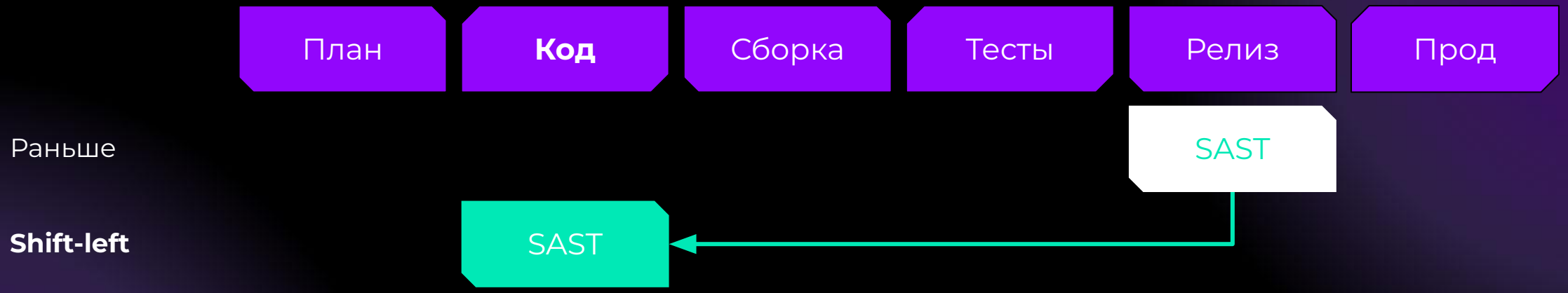
SAST становится этапом непрерывной интеграции.



Серверный

Анализ всего проекта целиком по расписанию.

Shift-left принцип



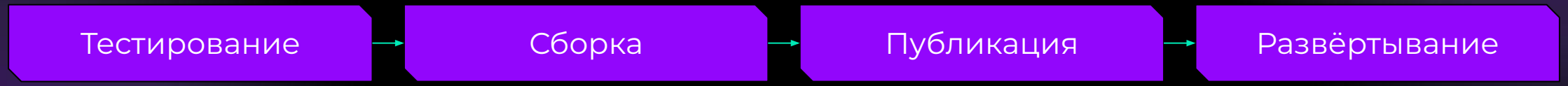
Непрерывный SAST

GUARDCORE

Проверяем каждое изменение и разворачиваем разработчика, если нашли срабатывания.

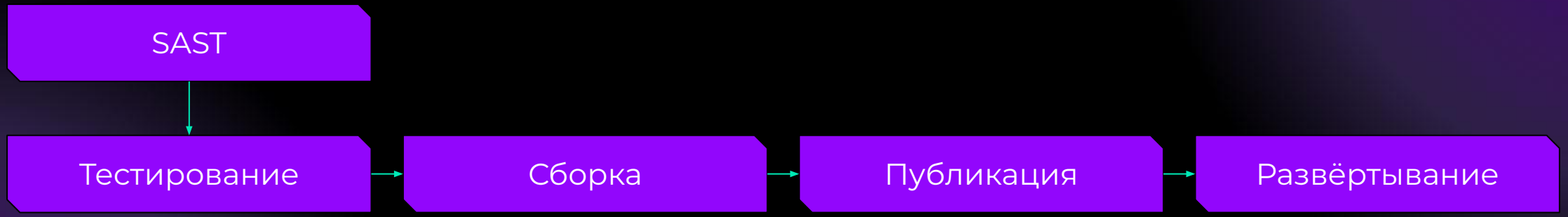
Непрерывный SAST

Проверяем каждое изменение и разворачиваем разработчика, если нашли срабатывания.



Непрерывный SAST

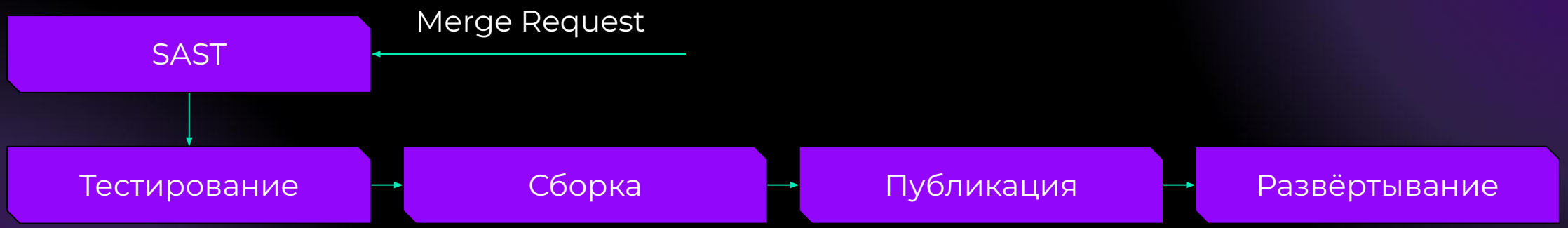
Проверяем каждое изменение и разворачиваем разработчика, если нашли срабатывания.



Непрерывный SAST

GUARDCORE

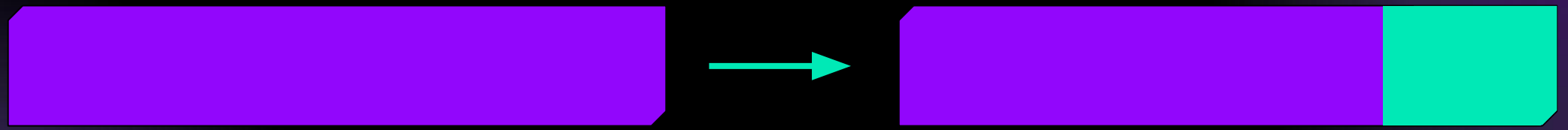
Проверяем каждое изменение и разворачиваем разработчика, если нашли срабатывания.



Инкрементальный анализ

GUARDCORE

Предыдущий результат



Анализ всего проекта

Следующий запуск

Проверяем только изменения



А что, если нет?





А что, если нет?

Время

Увеличится время экспертизы результатов анализа.



А что, если нет?

GUARDCORE

Время

Увеличится время экспертизы результатов анализа.

Качество

Упадёт качество экспертизы результатов анализа.



А что, если нет?

GUARDCORE

Время

Увеличится время экспертизы результатов анализа.

Качество

Упадёт качество экспертизы результатов анализа.

Исправление

Найденные ошибки будут исправляться дольше и сложнее.



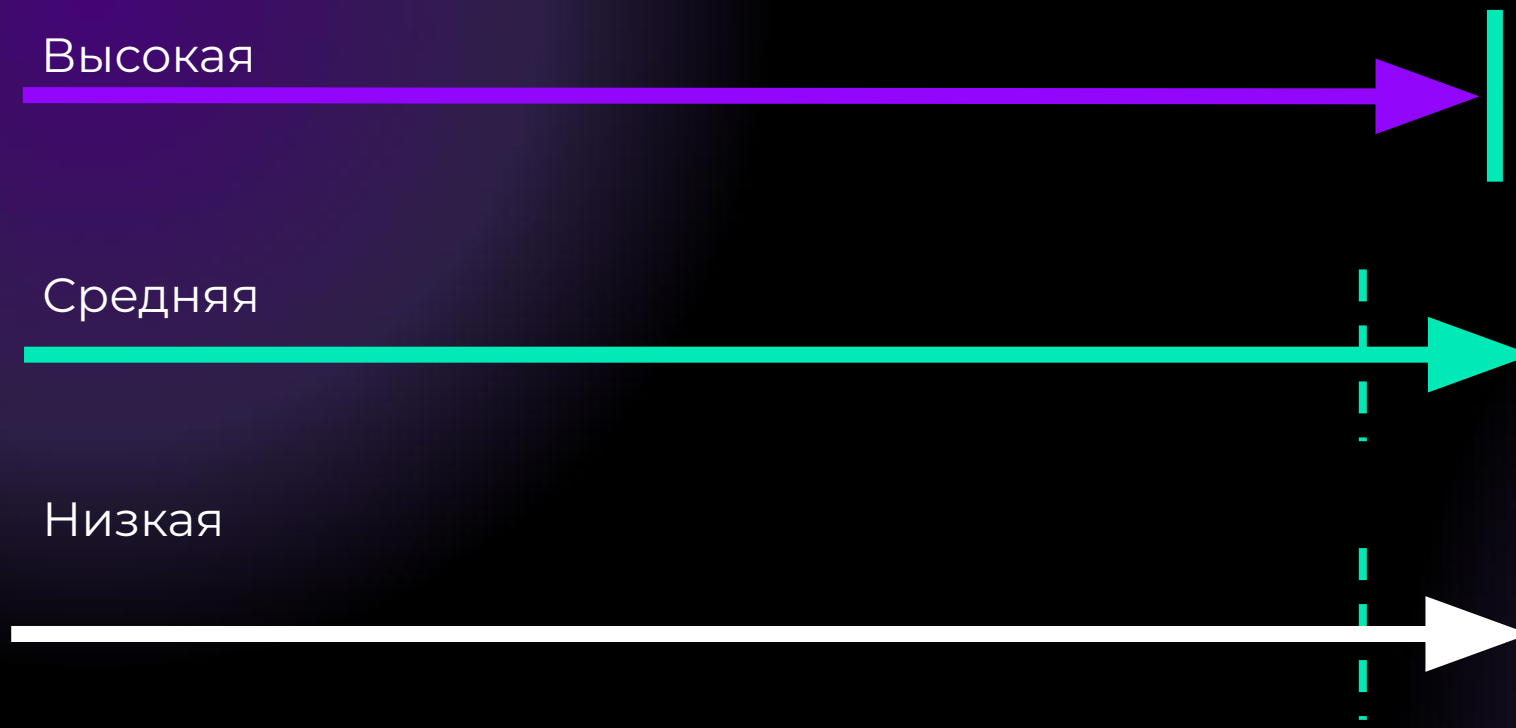
GUARDCONF

Quality Gate

Автоматическая проверка в пайплайне: набор условий, которым должен соответствовать код.



Quality Gate



Hard Gate

Zero Tolerance: ни одного срабатывания, сборка останавливается

Soft Gate

Предупреждение в отчёте, сборка идёт дальше

Soft Gate

Информация для разработчика, сборка идёт дальше

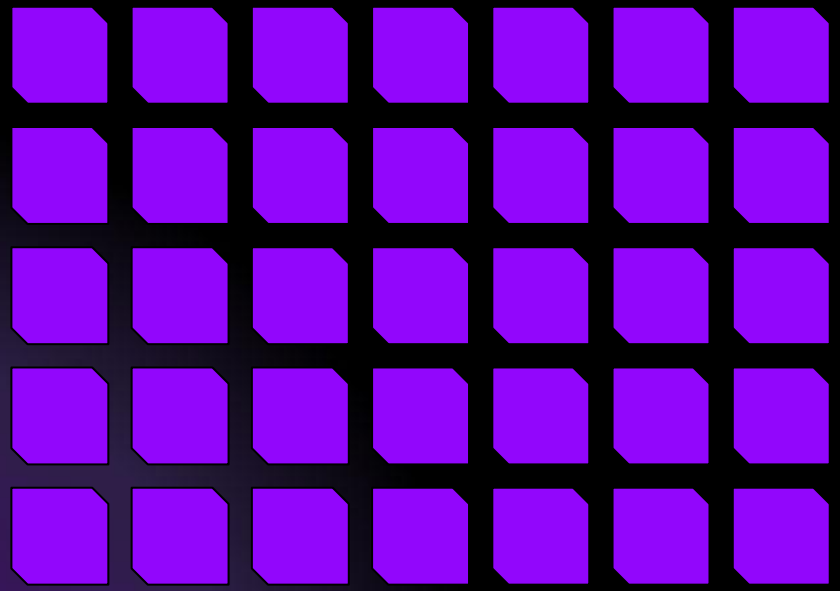
ASOC – единая точка входа

GUARDCONF



Механизм Baseline

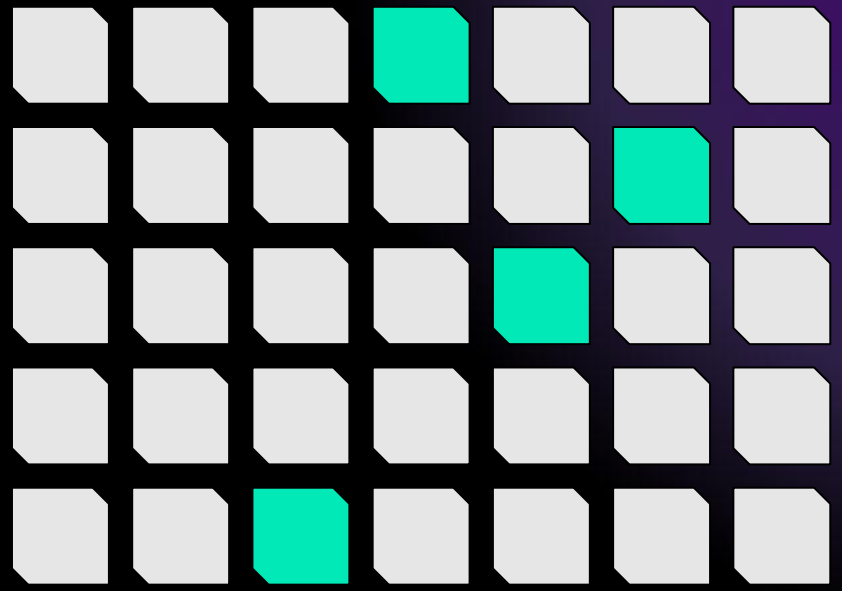
Старые срабатывания



Подавляем и принимаем как технический долг

BASELINE

Новые изменения



Проверяем только новые срабатывания в отчёте

GUARDCORP

Finale

Roll the credits





GUARDCORE

/feelindev

Мой авторский канал о разработке и технологиях: разработка, чистый код, AI, безопасность — и ещё миллион тем для холиваров.





Спасибо за внимание!



Валерий Филатов

Developer Advocate & Project Lead
PVS-Studio

