ozon банк

Построение SAST и мониторинг изменений в коде на большом ландшафте

Дмитрий Марюшкин

Руководитель продуктовой безопасности

Ozon Fintech

Whoami

Дмитрий Марюшкин

- Делаю финансовые продукты Ozon безопаснее
- Развиваю направления offense sec ops и data-аналитики в security
- Пишу appsec инструменты on-prem и немного в open source
- Статьи в][и конференции

До этого похожее было в Yandex, Avito, PT

dmarushkin github.com/dmarushkin

Agenda

Джентльменский набор

Жизнь вне пайплайнов

Мониторинг вместо согласований

Agenda

Джентльменский набор

Жизнь вне пайплайнов

Мониторинг вместо согласований

Agenda

Джентльменский набор

Жизнь вне пайплайнов

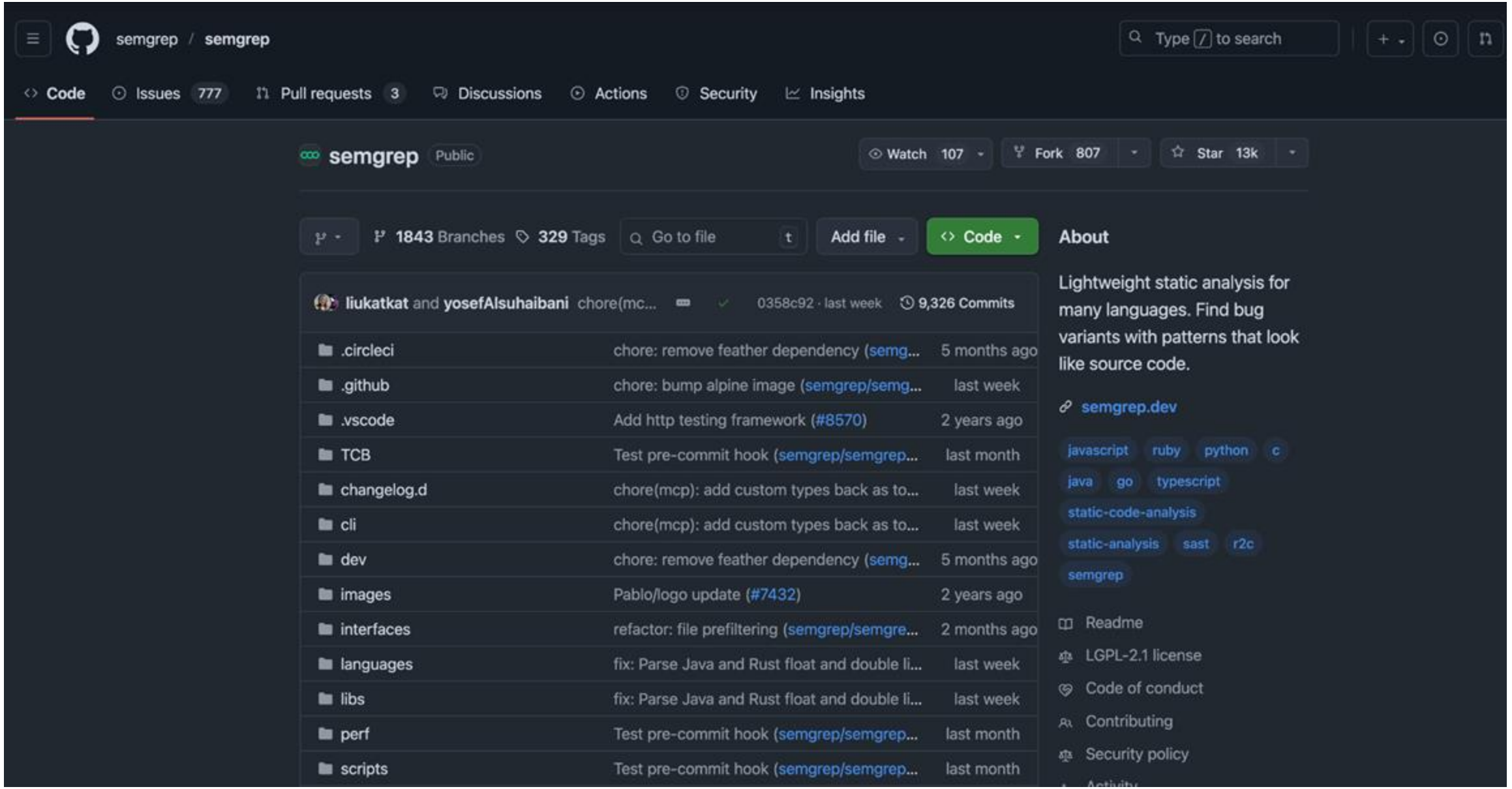
Мониторинг вместо согласований

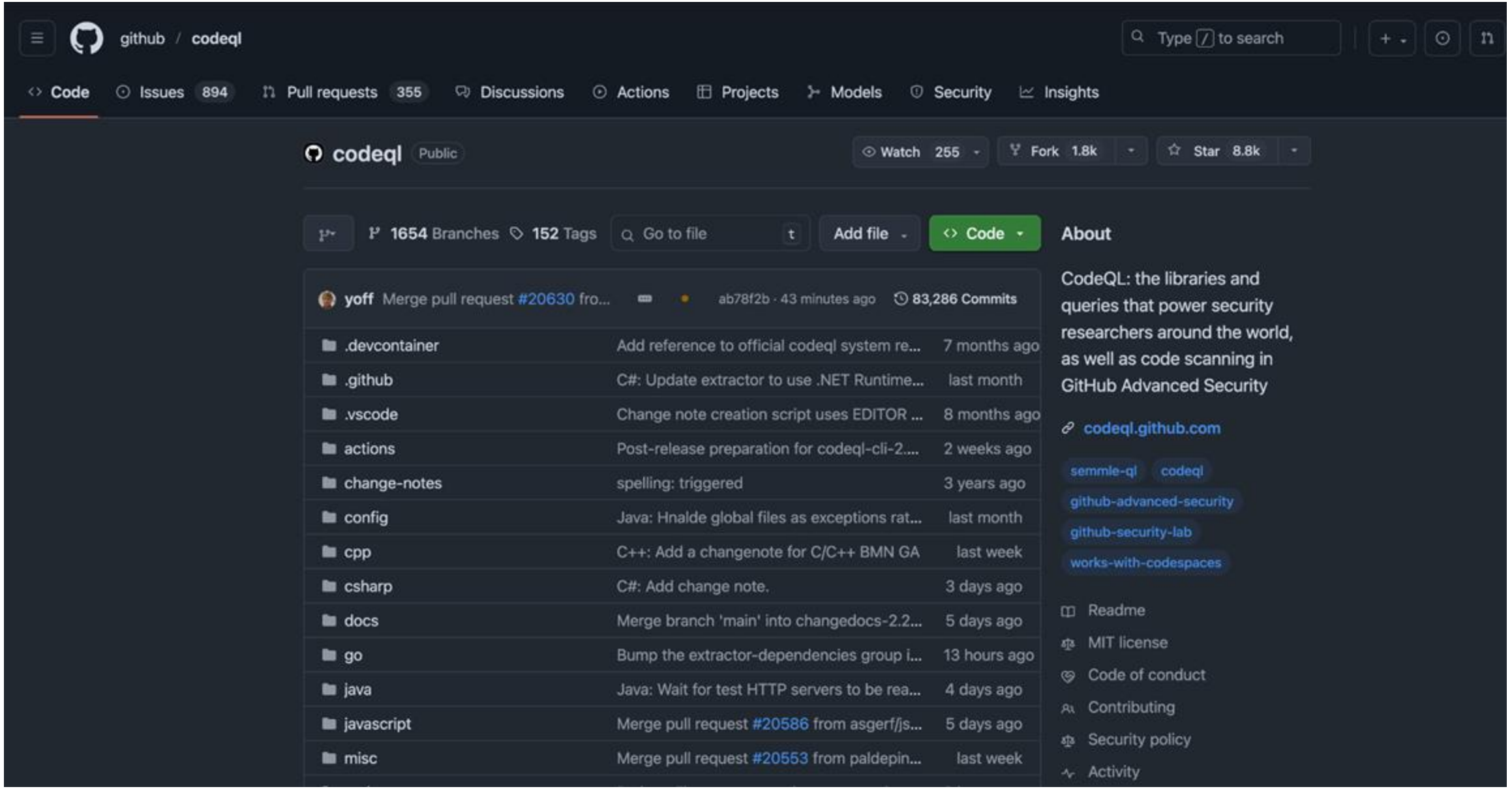
01

Джентльменский набор

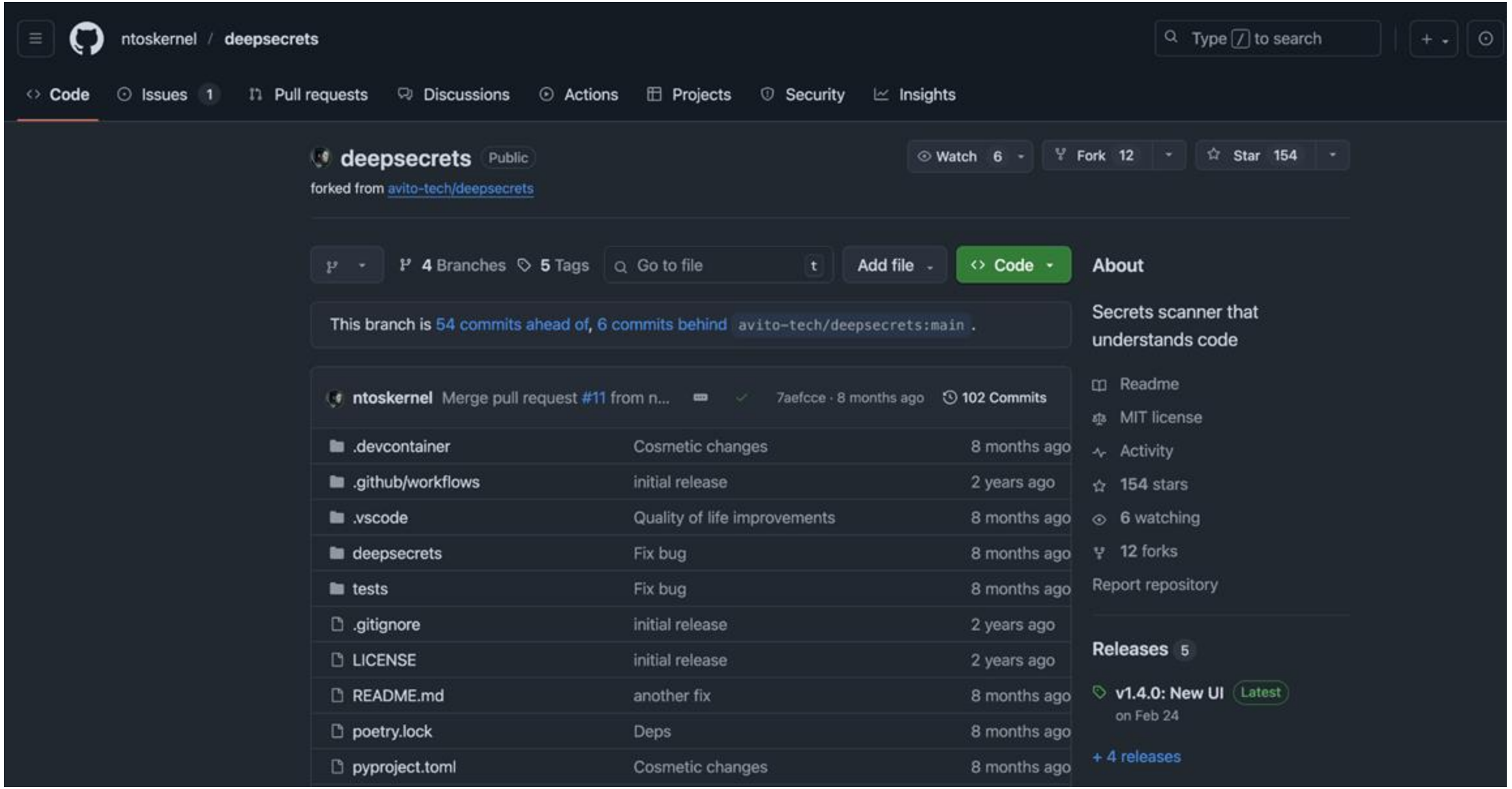
что запускаем?

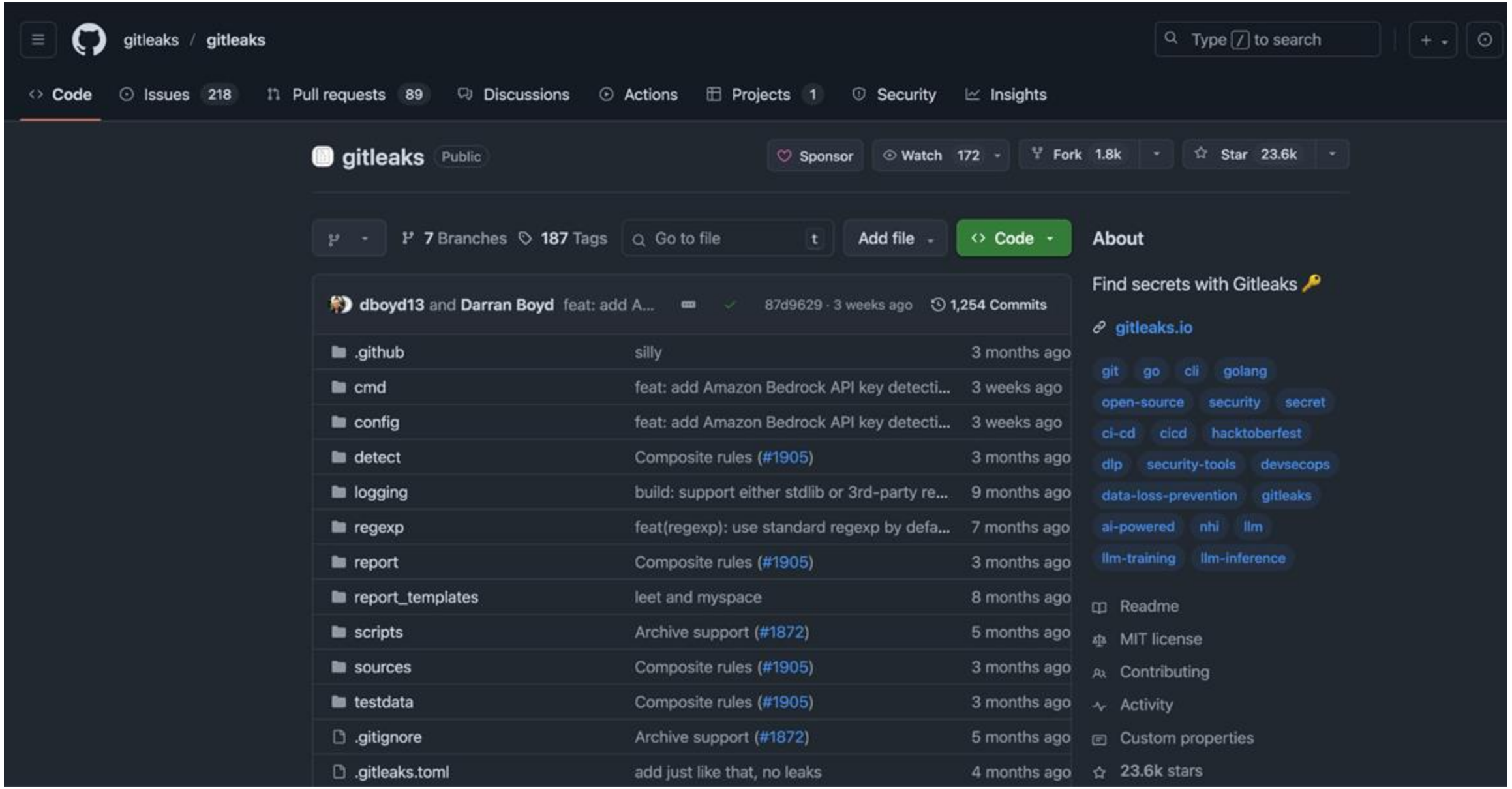
уязвимости в коде


semgrep / semgrep
Type / to search
Code
Issues 777
Pull requests 3
Discussions
Actions
Security
Insights
semgrep
Public
Watch 107
Fork 807
Star 13k
1843 Branches
329 Tags
Go to file t
Add file
Code
liukatkat and yosefAlsuhaibani chore(mc...
0358c92 · last week
9,326 Commits
.circleci chore: remove feather dependency (semg... 5 months ago
.github chore: bump alpine image (semgrep/semg... last week
.vscode Add http testing framework (#8570) 2 years ago
TCB Test pre-commit hook (semgrep/semgrep... last month
changelog.d chore(mcp): add custom types back as to... last week
cli chore(mcp): add custom types back as to... last week
dev chore: remove feather dependency (semg... 5 months ago
images Pablo/logo update (#7432) 2 years ago
interfaces refactor: file prefiltering (semgrep/semgre... 2 months ago
languages fix: Parse Java and Rust float and double li... last week
libs fix: Parse Java and Rust float and double li... last week
perf Test pre-commit hook (semgrep/semgrep... last month
scripts Test pre-commit hook (semgrep/semgrep... last month
About
Lightweight static analysis for many languages. Find bug variants with patterns that look like source code.
semgrep.dev
javascript ruby python c
java go typescript
static-code-analysis
static-analysis sast r2c
semgrep
Readme
LGPL-2.1 license
Code of conduct
Contributing
Security policy

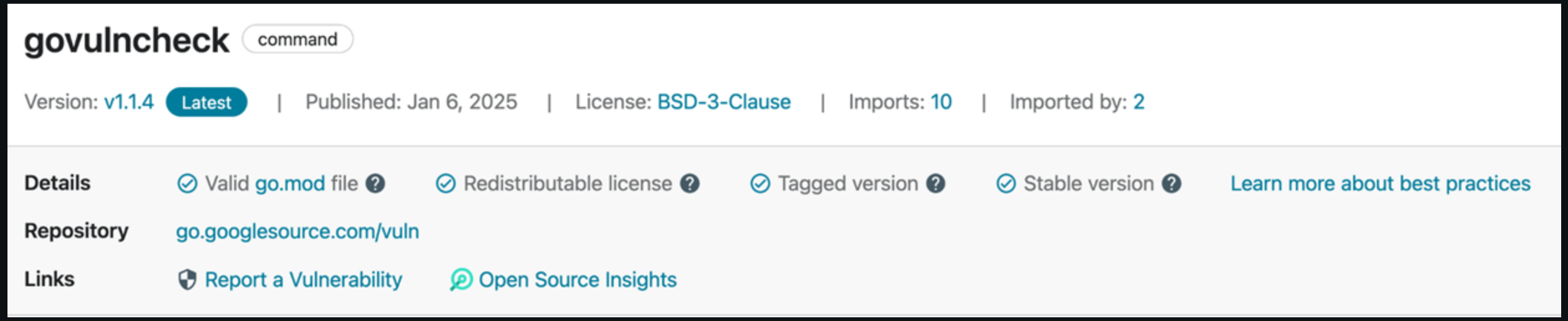

github / codeql
Type / to search
Code
Issues 894
Pull requests 355
Discussions
Actions
Projects
Models
Security
Insights
codeql Public
Watch 255
Fork 1.8k
Star 8.8k
1654 Branches
152 Tags
Go to file t
Add file
Code
yoff Merge pull request #20630 fro... ab78f2b · 43 minutes ago 83,286 Commits
.devcontainer Add reference to official codeql system re... 7 months ago
.github C#: Update extractor to use .NET Runtime... last month
.vscode Change note creation script uses EDITOR ... 8 months ago
actions Post-release preparation for codeql-cli-2.... 2 weeks ago
change-notes spelling: triggered 3 years ago
config Java: Hnalde global files as exceptions rat... last month
cpp C++: Add a changenote for C/C++ BMN GA last week
csharp C#: Add change note. 3 days ago
docs Merge branch 'main' into changedocs-2.2... 5 days ago
go Bump the extractor-dependencies group i... 13 hours ago
java Java: Wait for test HTTP servers to be rea... 4 days ago
javascript Merge pull request #20586 from asgerf/js... 5 days ago
misc Merge pull request #20553 from paldepin... last week
About
CodeQL: the libraries and queries that power security researchers around the world, as well as code scanning in GitHub Advanced Security
codeql.github.com
semmle-ql
codeql
github-advanced-security
github-security-lab
works-with-codespaces
Readme
MIT license
Code of conduct
Contributing
Security policy
Activity

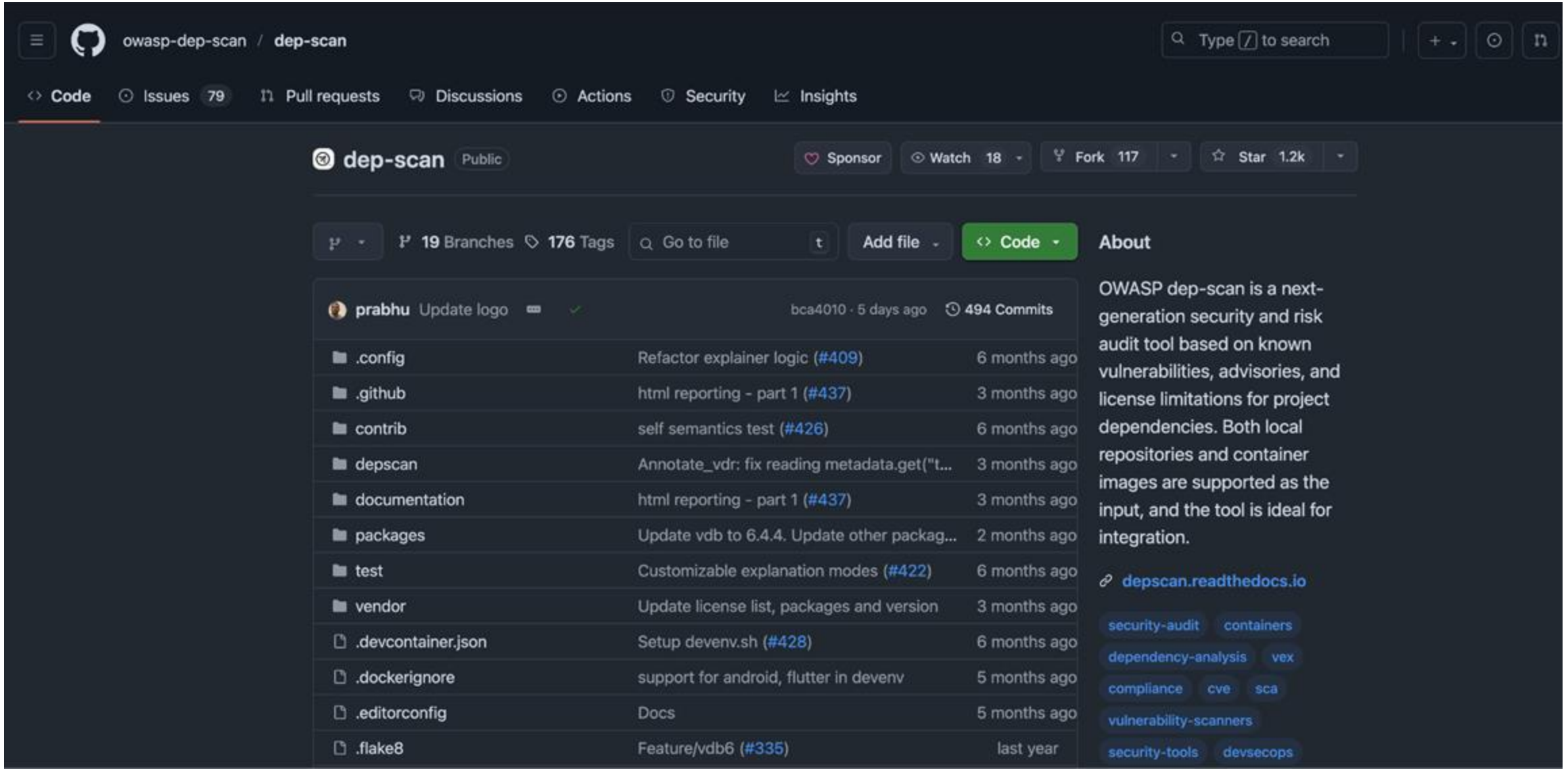
секреты в коде

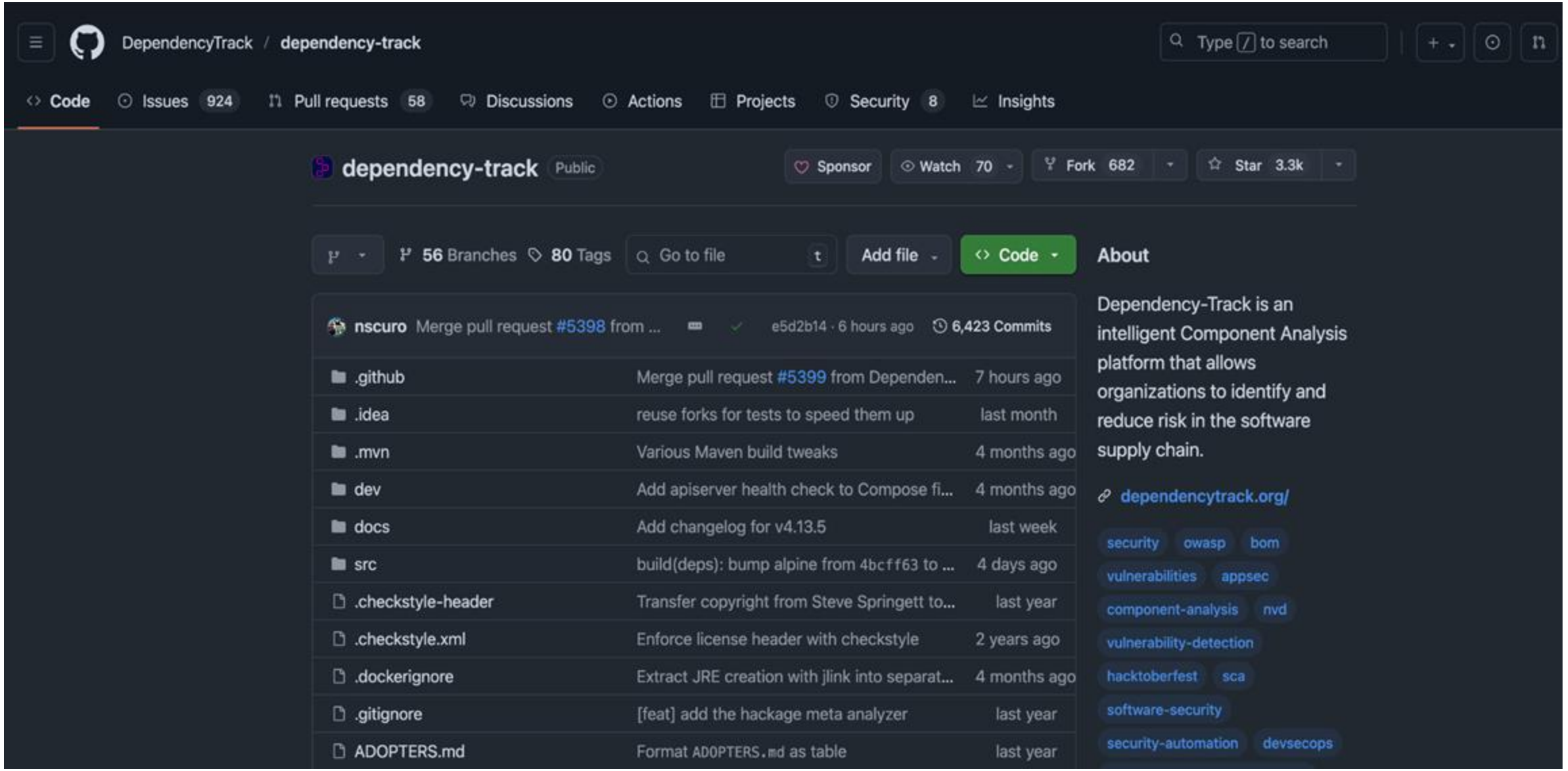

ntoskernel / deepsecrets
Type / to search
Code
Issues 1
Pull requests
Discussions
Actions
Projects
Security
Insights
deepsecrets Public
forked from avito-tech/deepsecrets
Watch 6
Fork 12
Star 154
4 Branches
5 Tags
Go to file t
Add file
Code
This branch is 54 commits ahead of, 6 commits behind avito-tech/deepsecrets:main .
ntoskernel Merge pull request #11 from n... 7aefcce · 8 months ago 102 Commits
.devcontainer Cosmetic changes 8 months ago
.github/workflows initial release 2 years ago
.vscode Quality of life improvements 8 months ago
deepsecrets Fix bug 8 months ago
tests Fix bug 8 months ago
.gitignore initial release 2 years ago
LICENSE initial release 2 years ago
README.md another fix 8 months ago
poetry.lock Deps 8 months ago
pyproject.toml Cosmetic changes 8 months ago
About
Secrets scanner that understands code
Readme
MIT license
Activity
154 stars
6 watching
12 forks
Report repository
Releases 5
v1.4.0: New UI Latest
on Feb 24
+ 4 releases

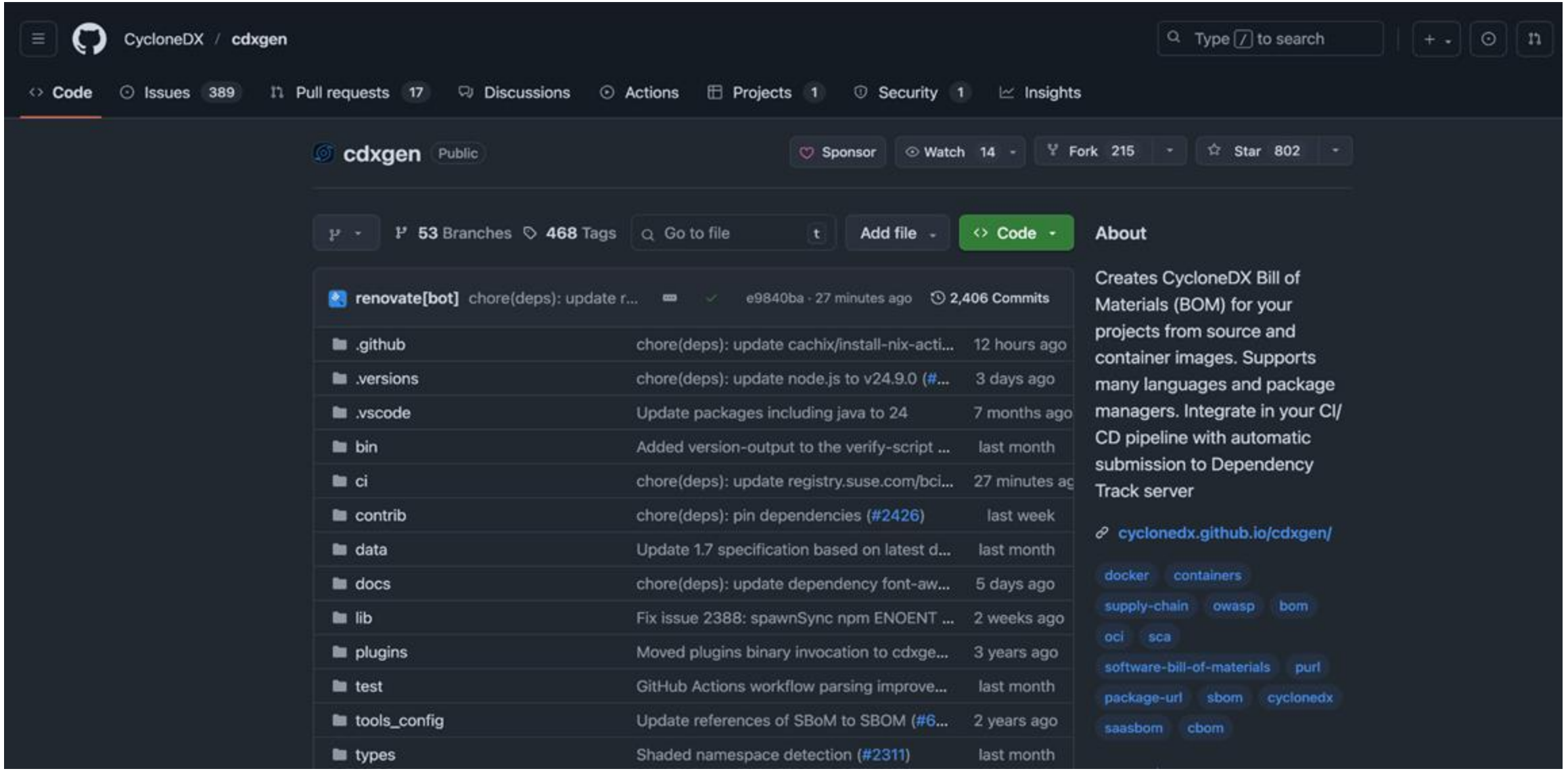

gitleaks / gitleaks
Type / to search
Code
Issues 218
Pull requests 89
Discussions
Actions
Projects 1
Security
Insights
gitleaks Public
Sponsor
Watch 172
Fork 1.8k
Star 23.6k
7 Branches
187 Tags
Go to file t
Add file
Code
dboyd13 and Darran Boyd feat: add A... 87d9629 · 3 weeks ago 1,254 Commits
.github silly 3 months ago
cmd feat: add Amazon Bedrock API key detecti... 3 weeks ago
config feat: add Amazon Bedrock API key detecti... 3 weeks ago
detect Composite rules (#1905) 3 months ago
logging build: support either stdlib or 3rd-party re... 9 months ago
regexp feat(regexp): use standard regexp by defa... 7 months ago
report Composite rules (#1905) 3 months ago
report_templates leet and myspace 8 months ago
scripts Archive support (#1872) 5 months ago
sources Composite rules (#1905) 3 months ago
testdata Composite rules (#1905) 3 months ago
.gitignore Archive support (#1872) 5 months ago
.gitleaks.toml add just like that, no leaks 4 months ago
About
Find secrets with Gitleaks 🔑
gitleaks.io
git go cli golang
open-source security secret
ci-cd cicd hacktoberfest
dlp security-tools devsecops
data-loss-prevention gitleaks
ai-powered nhi llm
llm-training llm-inference
Readme
MIT license
Contributing
Activity
Custom properties
23.6k stars

внешние зависимости

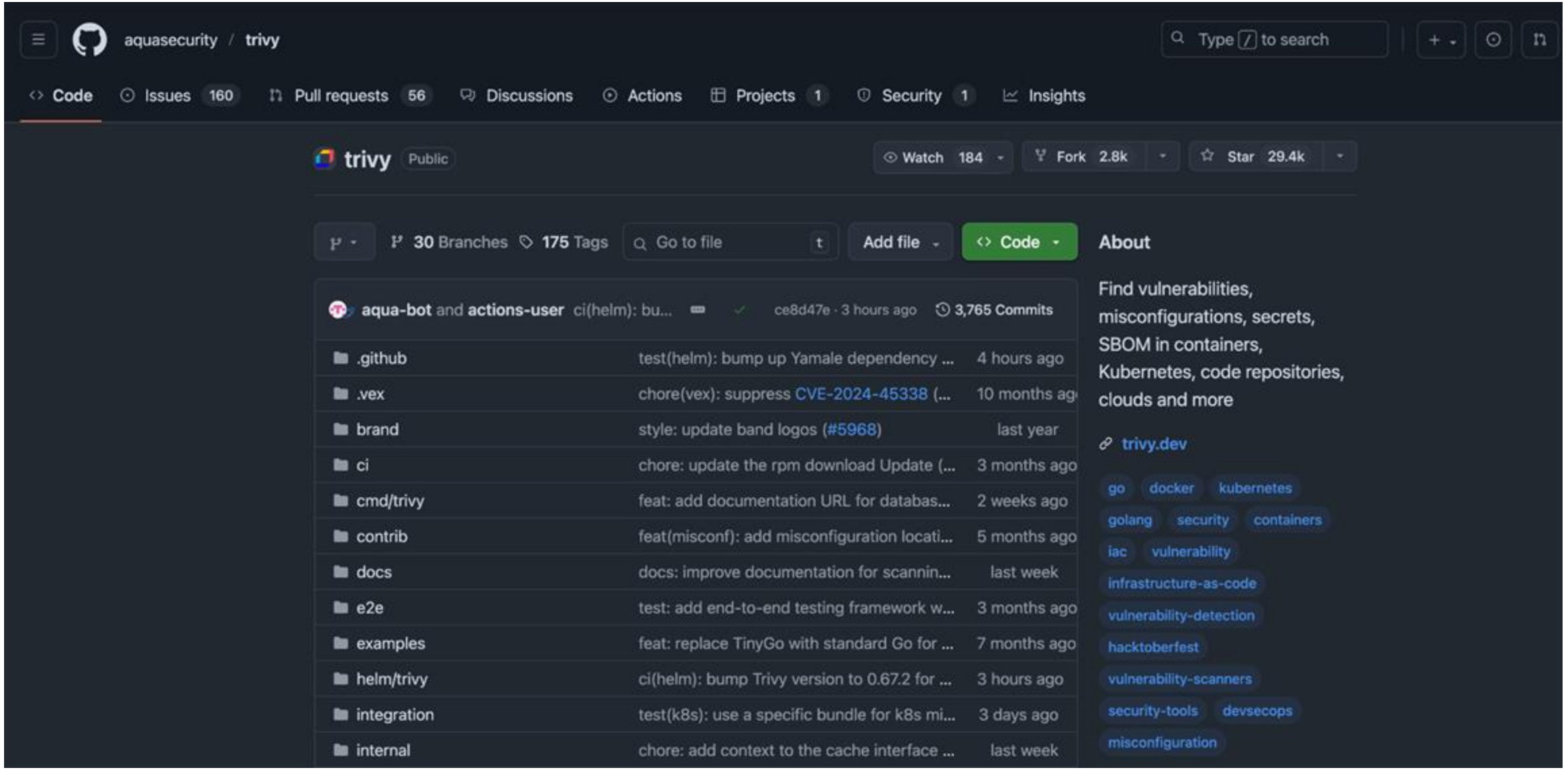

govulncheck
command
Version: v1.1.4 Latest | Published: Jan 6, 2025 | License: BSD-3-Clause | Imports: 10 | Imported by: 2
Details
Valid go.mod file
Redistributable license
Tagged version
Stable version
Learn more about best practices
Repository
go.googlesource.com/vuln
Links
Report a Vulnerability
Open Source Insights


owasp-dep-scan / dep-scan
Type / to search
Code
Issues 79
Pull requests
Discussions
Actions
Security
Insights
dep-scan
Public
Sponsor
Watch 18
Fork 117
Star 1.2k
19 Branches
176 Tags
Go to file
t
Add file
Code
prabhu Update logo
bca4010 · 5 days ago
494 Commits
.config Refactor explainer logic (#409) 6 months ago
.github html reporting - part 1 (#437) 3 months ago
contrib self semantics test (#426) 6 months ago
depscan Annotate_vdr: fix reading metadata.get("t... 3 months ago
documentation html reporting - part 1 (#437) 3 months ago
packages Update vdb to 6.4.4. Update other packag... 2 months ago
test Customizable explanation modes (#422) 6 months ago
vendor Update license list, packages and version 3 months ago
.devcontainer.json Setup devenv.sh (#428) 6 months ago
.dockerignore support for android, flutter in devenv 5 months ago
.editorconfig Docs 5 months ago
.flake8 Feature/vdb6 (#335) last year
About
OWASP dep-scan is a next-generation security and risk audit tool based on known vulnerabilities, advisories, and license limitations for project dependencies. Both local repositories and container images are supported as the input, and the tool is ideal for integration.
depscan.readthedocs.io
security-audit
containers
dependency-analysis
vex
compliance
cve
sca
vulnerability-scanners
security-tools
devsecops

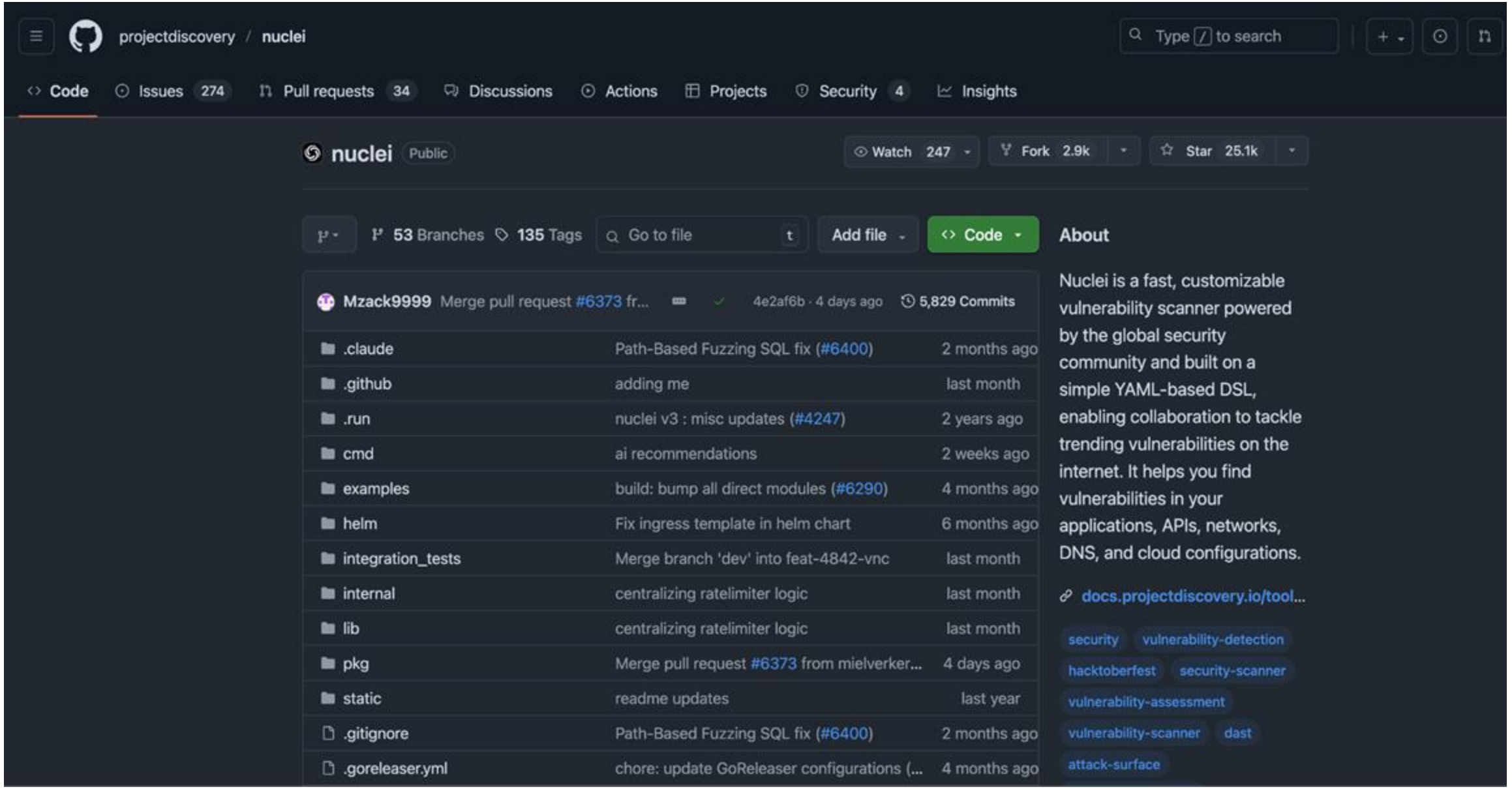

DependencyTrack / dependency-track
Type / to search
Code
Issues 924
Pull requests 58
Discussions
Actions
Projects
Security 8
Insights
dependency-track
Public
Sponsor
Watch 70
Fork 682
Star 3.3k
56 Branches
80 Tags
Go to file
t
Add file
Code
nscuro Merge pull request #5398 from ...
e5d2b14 · 6 hours ago
6,423 Commits
.github
Merge pull request #5399 from Dependen...
7 hours ago
.idea
reuse forks for tests to speed them up
last month
.mvn
Various Maven build tweaks
4 months ago
dev
Add apiserver health check to Compose fi...
4 months ago
docs
Add changelog for v4.13.5
last week
src
build(deps): bump alpine from 4bcff63 to ...
4 days ago
.checkstyle-header
Transfer copyright from Steve Springett to...
last year
.checkstyle.xml
Enforce license header with checkstyle
2 years ago
.dockerignore
Extract JRE creation with jlink into separat...
4 months ago
.gitignore
[feat] add the hackage meta analyzer
last year
ADOPTERS.md
Format ADOPTERS.md as table
last year
About
Dependency-Track is an intelligent Component Analysis platform that allows organizations to identify and reduce risk in the software supply chain.
dependencytrack.org/
security
owasp
bom
vulnerabilities
appsec
component-analysis
nvd
vulnerability-detection
hacktoberfest
sca
software-security
security-automation
devsecops

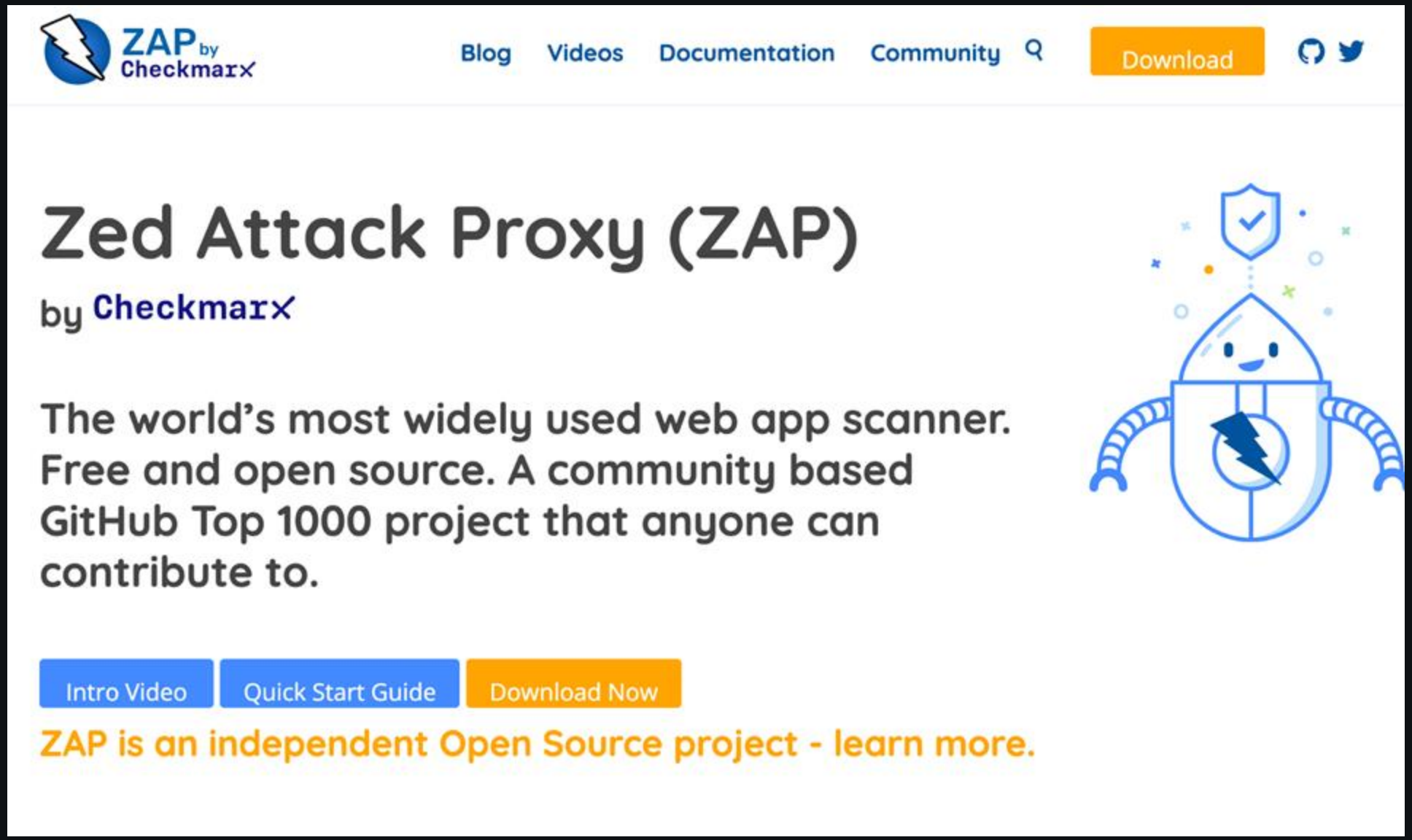

CycloneDX / cdxgen
Type / to search
Code
Issues 389
Pull requests 17
Discussions
Actions
Projects 1
Security 1
Insights
cdxgen Public
Sponsor
Watch 14
Fork 215
Star 802
53 Branches
468 Tags
Go to file t
Add file
Code
renovate[bot] chore(deps): update r... e9840ba · 27 minutes ago 2,406 Commits
.github chore(deps): update cachix/install-nix-acti... 12 hours ago
.versions chore(deps): update node.js to v24.9.0 (#... 3 days ago
.vscode Update packages including java to 24 7 months ago
bin Added version-output to the verify-script ... last month
ci chore(deps): update registry.suse.com/bci... 27 minutes ag
contrib chore(deps): pin dependencies (#2426) last week
data Update 1.7 specification based on latest d... last month
docs chore(deps): update dependency font-aw... 5 days ago
lib Fix issue 2388: spawnSync npm ENOENT ... 2 weeks ago
plugins Moved plugins binary invocation to cdxge... 3 years ago
test GitHub Actions workflow parsing improve... last month
tools_config Update references of SBoM to SBOM (#6... 2 years ago
types Shaded namespace detection (#2311) last month
About
Creates CycloneDX Bill of Materials (BOM) for your projects from source and container images. Supports many languages and package managers. Integrate in your CI/CD pipeline with automatic submission to Dependency Track server
cyclonedx.github.io/cdxgen/
docker containers
supply-chain owasp bom
oci sca
software-bill-of-materials purl
package-url sbom cyclonedx
saasbom cbom

образы контейнеров


aquasecurity / trivy
Type / to search
Code
Issues 160
Pull requests 56
Discussions
Actions
Projects 1
Security 1
Insights
trivy
Public
Watch 184
Fork 2.8k
Star 29.4k
30 Branches
175 Tags
Go to file
t
Add file
Code
aqua-bot and actions-user ci(helm): bu...
ce8d47e · 3 hours ago
3,765 Commits
.github test(helm): bump up Yamale dependency ... 4 hours ago
.vex chore(vex): suppress CVE-2024-45338 (... 10 months ag
brand style: update band logos (#5968) last year
ci chore: update the rpm download Update (... 3 months ago
cmd/trivy feat: add documentation URL for databas... 2 weeks ago
contrib feat(misconf): add misconfiguration locati... 5 months ago
docs docs: improve documentation for scannin... last week
e2e test: add end-to-end testing framework w... 3 months ago
examples feat: replace TinyGo with standard Go for ... 7 months ago
helm/trivy ci(helm): bump Trivy version to 0.67.2 for ... 3 hours ago
integration test(k8s): use a specific bundle for k8s mi... 3 days ago
internal chore: add context to the cache interface ... last week
About
Find vulnerabilities, misconfigurations, secrets, SBOM in containers, Kubernetes, code repositories, clouds and more
trivy.dev
go
docker
kubernetes
golang
security
containers
iac
vulnerability
infrastructure-as-code
vulnerability-detection
hacktoberfest
vulnerability-scanners
security-tools
devsecops
misconfiguration

динамическое тестирование

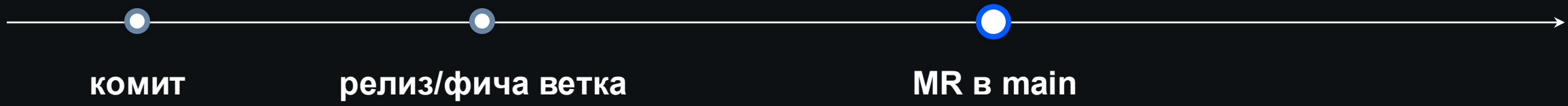

projectdiscovery / nuclei
Type / to search
Code
Issues 274
Pull requests 34
Discussions
Actions
Projects
Security 4
Insights
nuclei
Public
Watch 247
Fork 2.9k
Star 25.1k
53 Branches
135 Tags
Go to file
t
Add file
Code
Mzack9999 Merge pull request #6373 fr...
4e2af6b · 4 days ago
5,829 Commits
.claude Path-Based Fuzzing SQL fix (#6400) 2 months ago
.github adding me last month
.run nuclei v3 : misc updates (#4247) 2 years ago
cmd ai recommendations 2 weeks ago
examples build: bump all direct modules (#6290) 4 months ago
helm Fix ingress template in helm chart 6 months ago
integration_tests Merge branch 'dev' into feat-4842-vnc last month
internal centralizing ratelimiter logic last month
lib centralizing ratelimiter logic last month
pkg Merge pull request #6373 from mielverker... 4 days ago
static readme updates last year
.gitignore Path-Based Fuzzing SQL fix (#6400) 2 months ago
.goreleaser.yml chore: update GoReleaser configurations (... 4 months ago
About
Nuclei is a fast, customizable vulnerability scanner powered by the global security community and built on a simple YAML-based DSL, enabling collaboration to tackle trending vulnerabilities on the internet. It helps you find vulnerabilities in your applications, APIs, networks, DNS, and cloud configurations.
docs.projectdiscovery.io/tool...
security
vulnerability-detection
hacktoberfest
security-scanner
vulnerability-assessment
vulnerability-scanner
dast
attack-surface

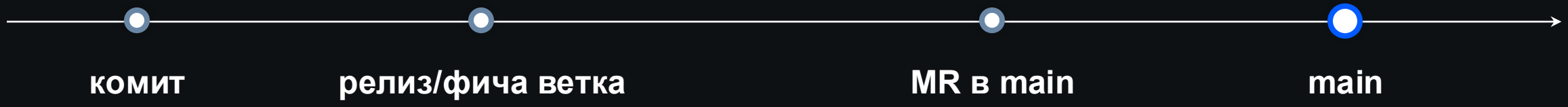

ZAP by Checkmarx
Blog
Videos
Documentation
Community
Download
Zed Attack Proxy (ZAP)
by Checkmarx
The world's most widely used web app scanner. Free and open source. A community based GitHub Top 1000 project that anyone can contribute to.
Intro Video
Quick Start Guide
Download Now
ZAP is an independent Open Source project - learn more.

когда запускаем?

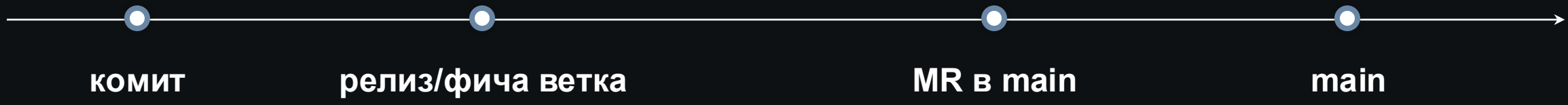
комит


комит
релиз/фича ветка

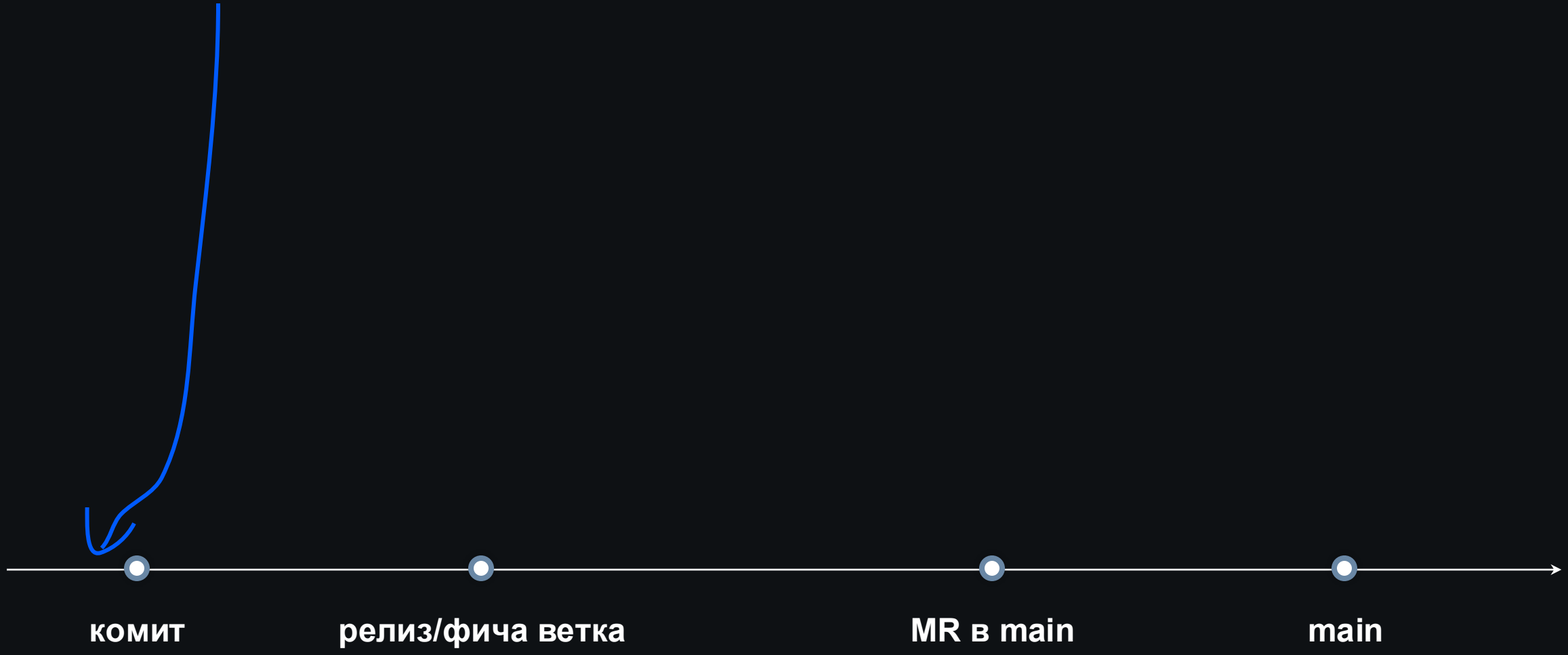

комит
релиз/фича ветка
MR в main


комит
релиз/фича ветка
MR в main
main

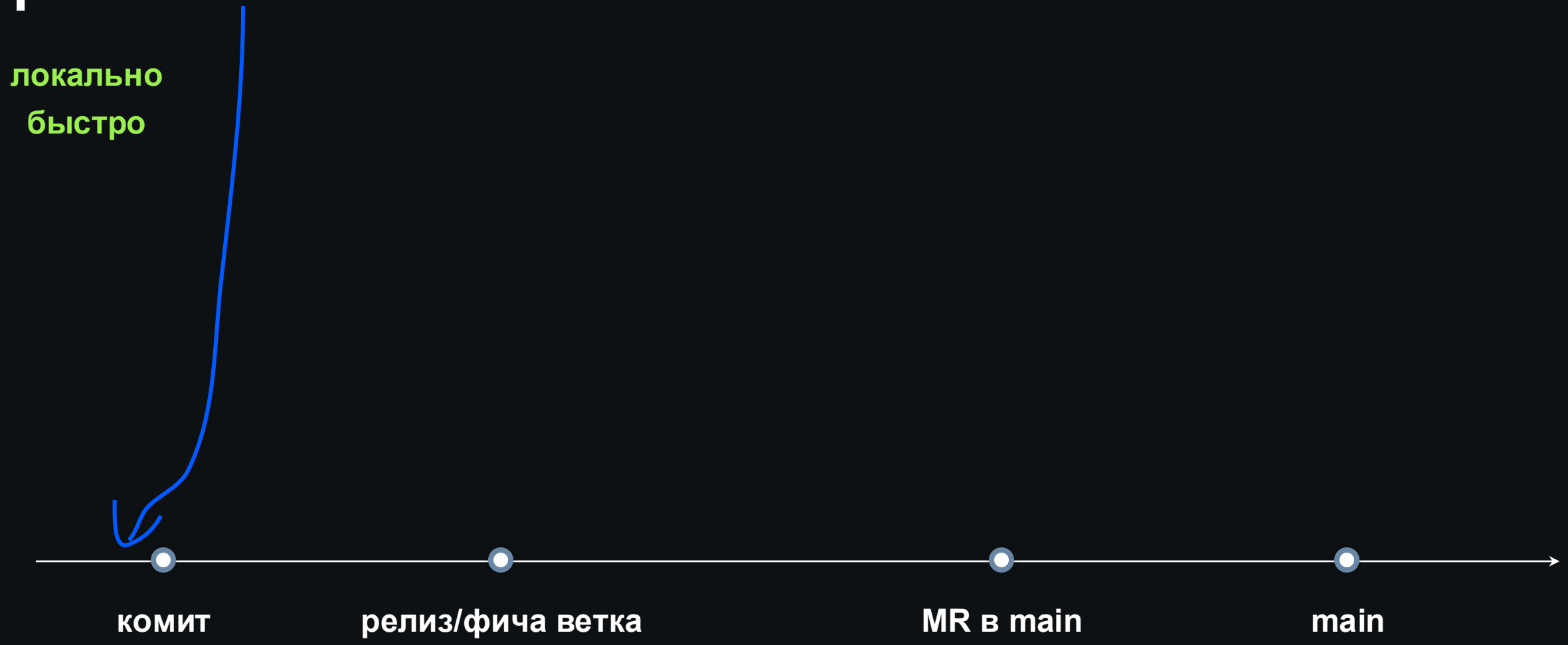
прекомит



прекомит



прекомит

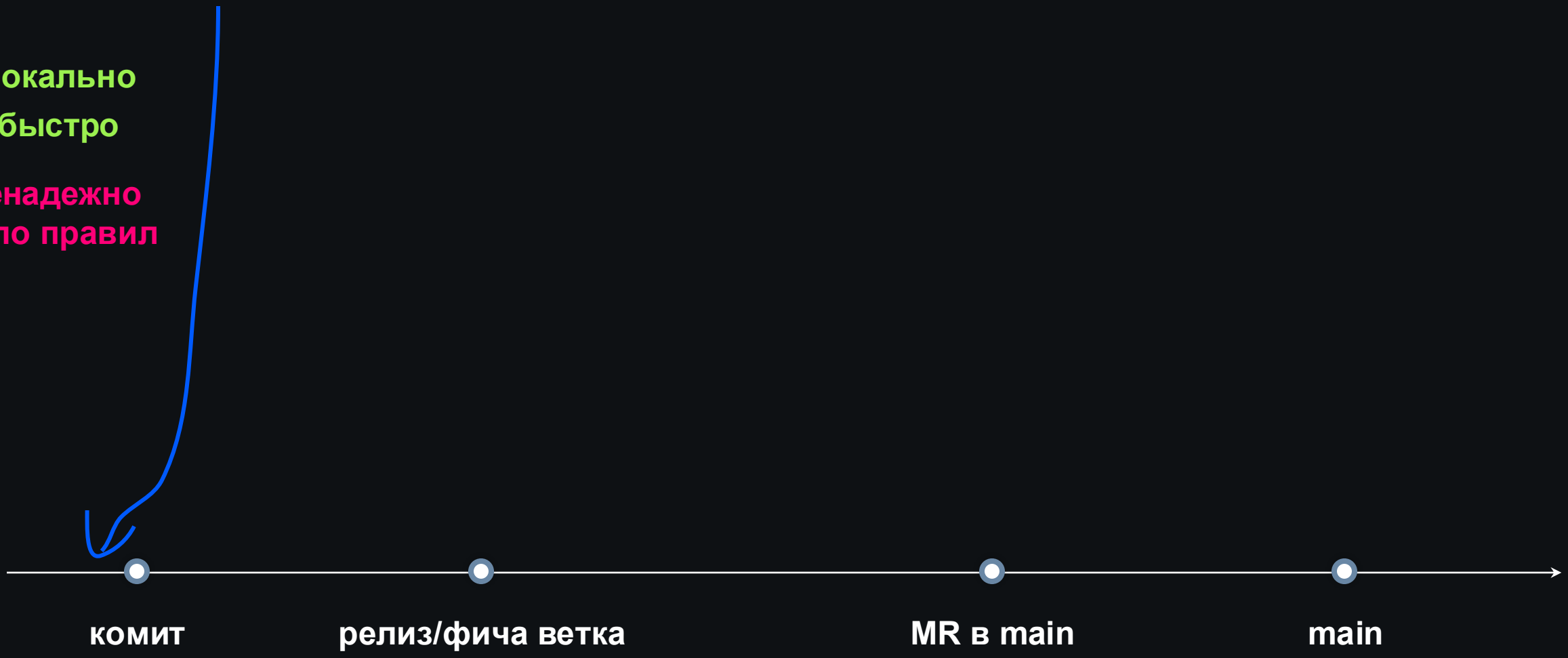


прекомит

локально

быстро

ненадежно
мало правил



прекомит

локально

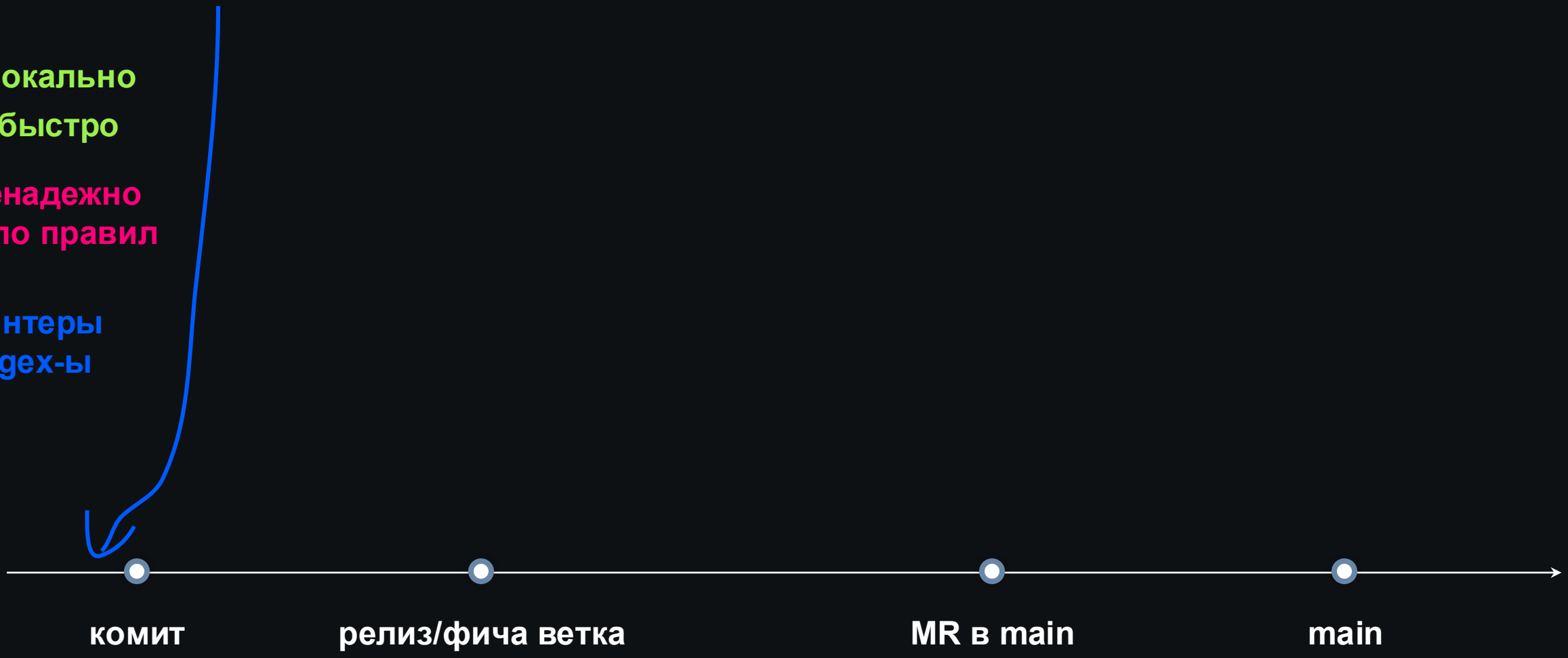
быстро

ненадежно

мало правил

линтеры

regex-ы



прекомит

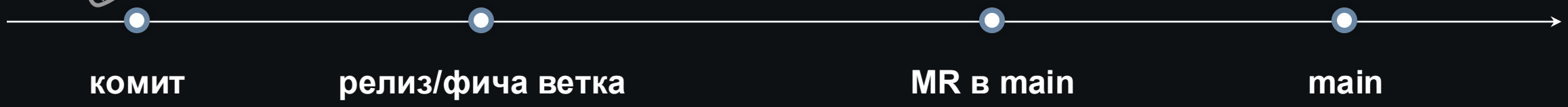
локально

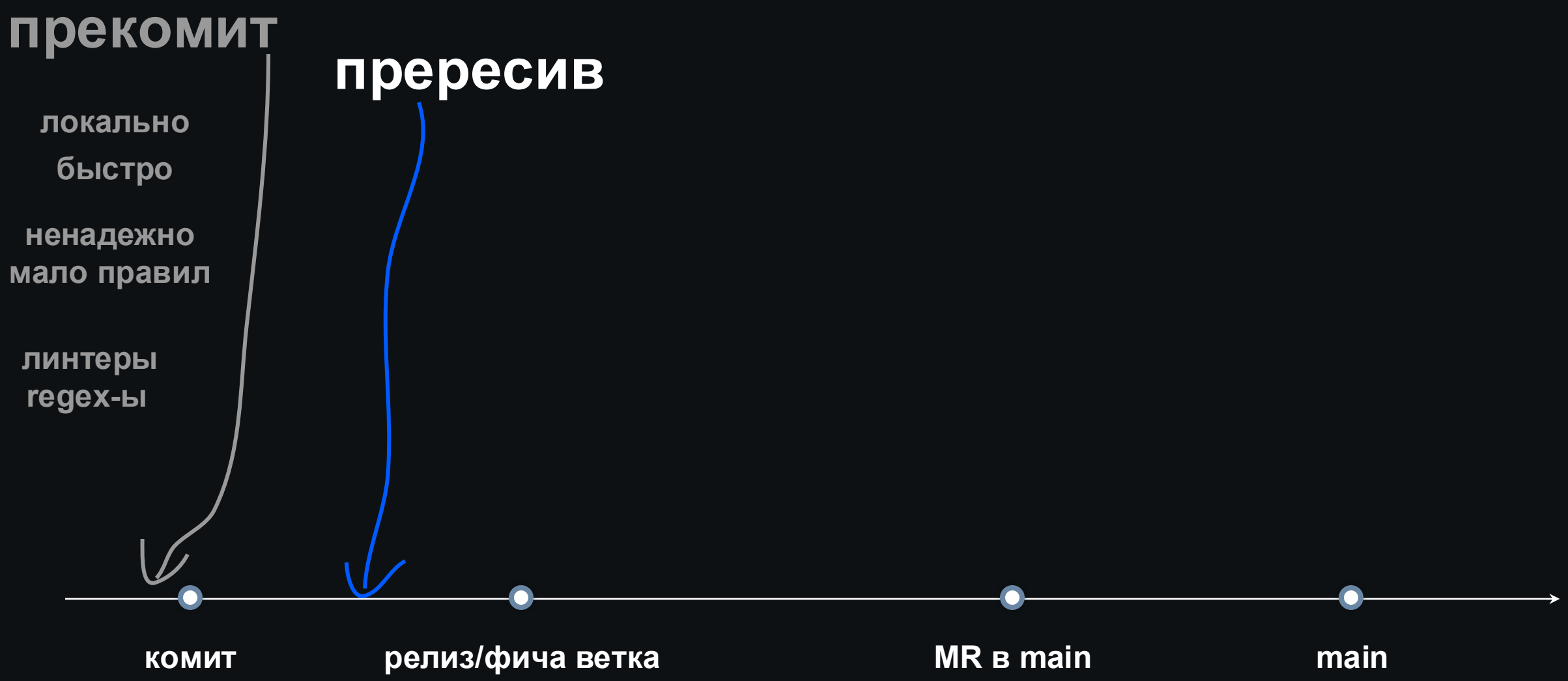
быстро

ненадежно
мало правил

линтеры
regex-ы

пересив




прекомит
пересив
локально
быстро
ненадежно
мало правил
линтеры
regex-ы
комит
релиз/фича ветка
MR в main
main


прекомит
локально
быстро
ненадежно
мало правил
линтеры
regex-ы
пересив
надежно
комит
релиз/фича ветка
MR в main
main

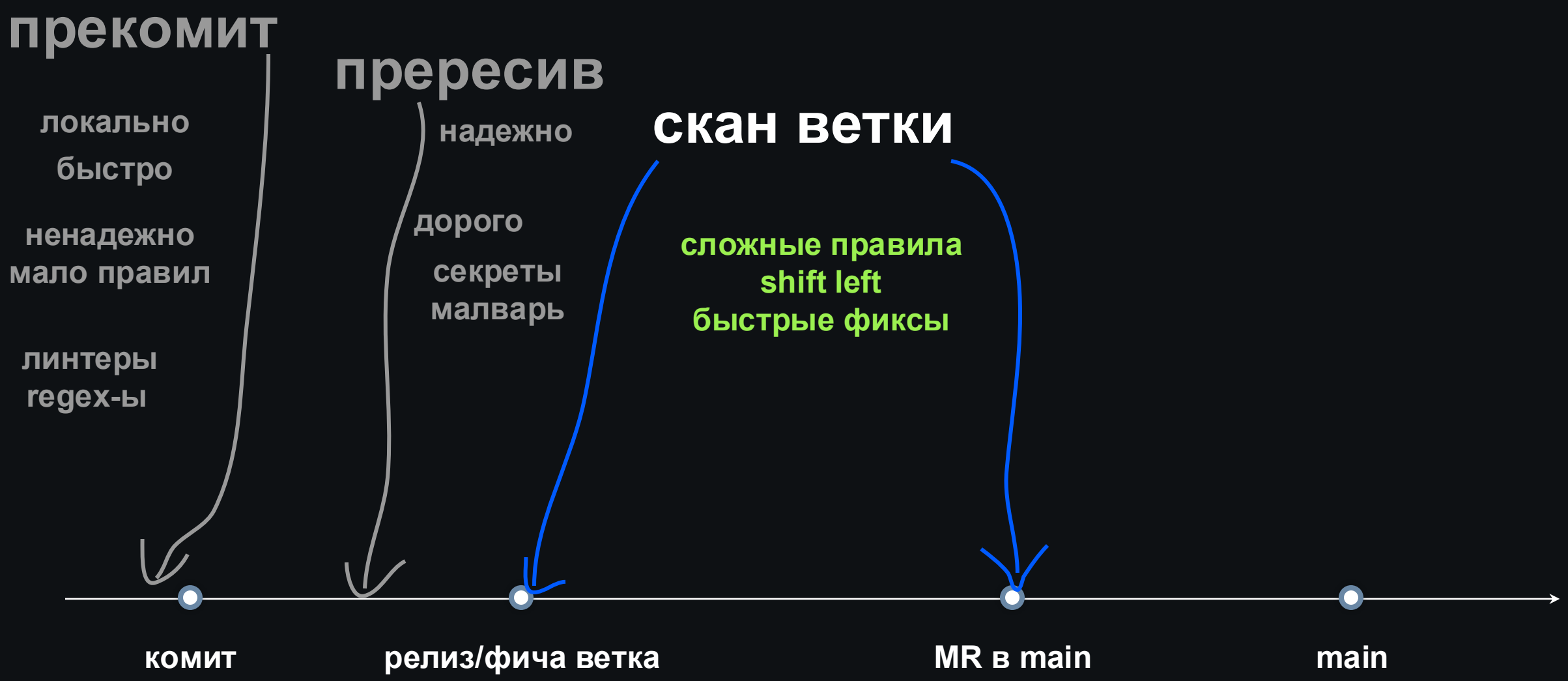

прекомит
локально
быстро
ненадежно
мало правил
линтеры
regex-ы
пересив
надежно
дорого
комит
релиз/фича ветка
MR в main
main

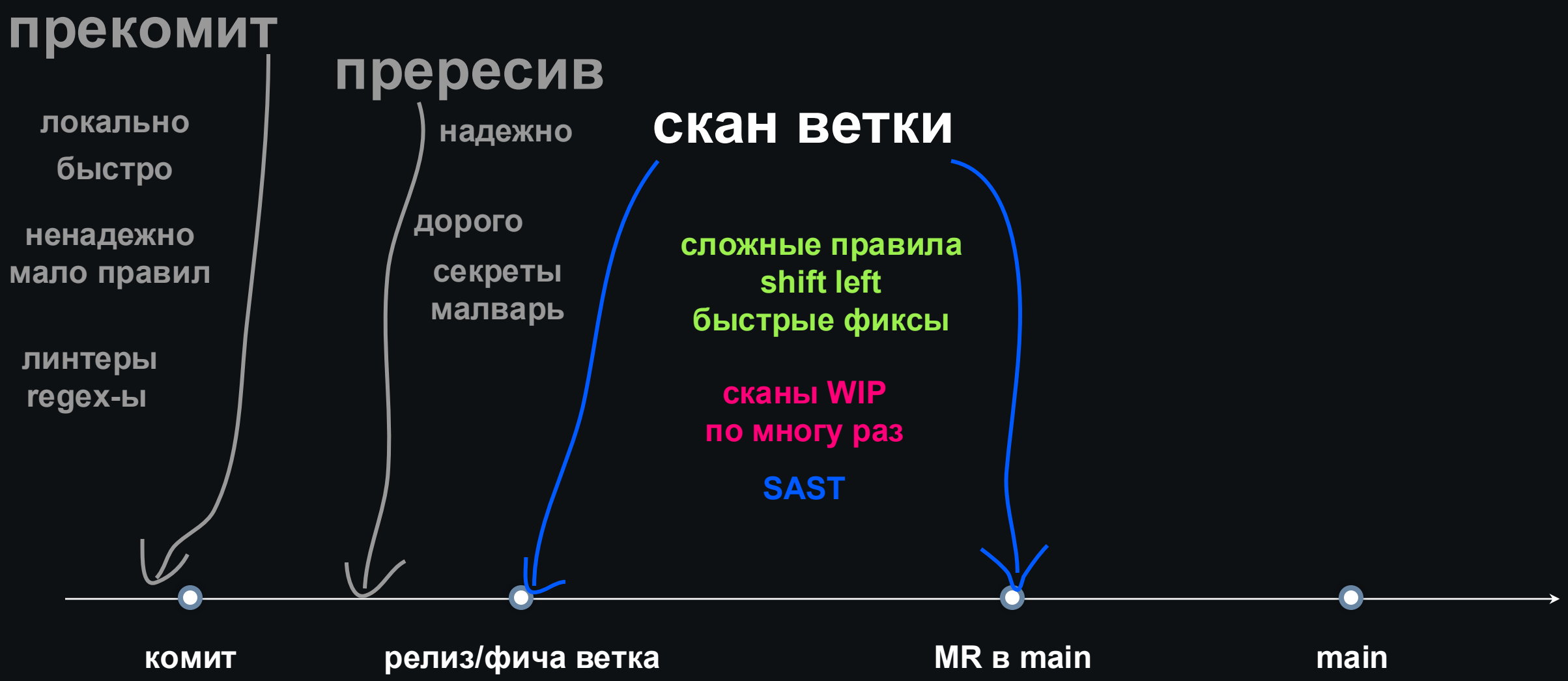

прекомит
локально
быстро
ненадежно
мало правил
линтеры
regex-ы
пересив
надежно
дорого
секреты
малварь
комит
релиз/фича ветка
MR в main
main

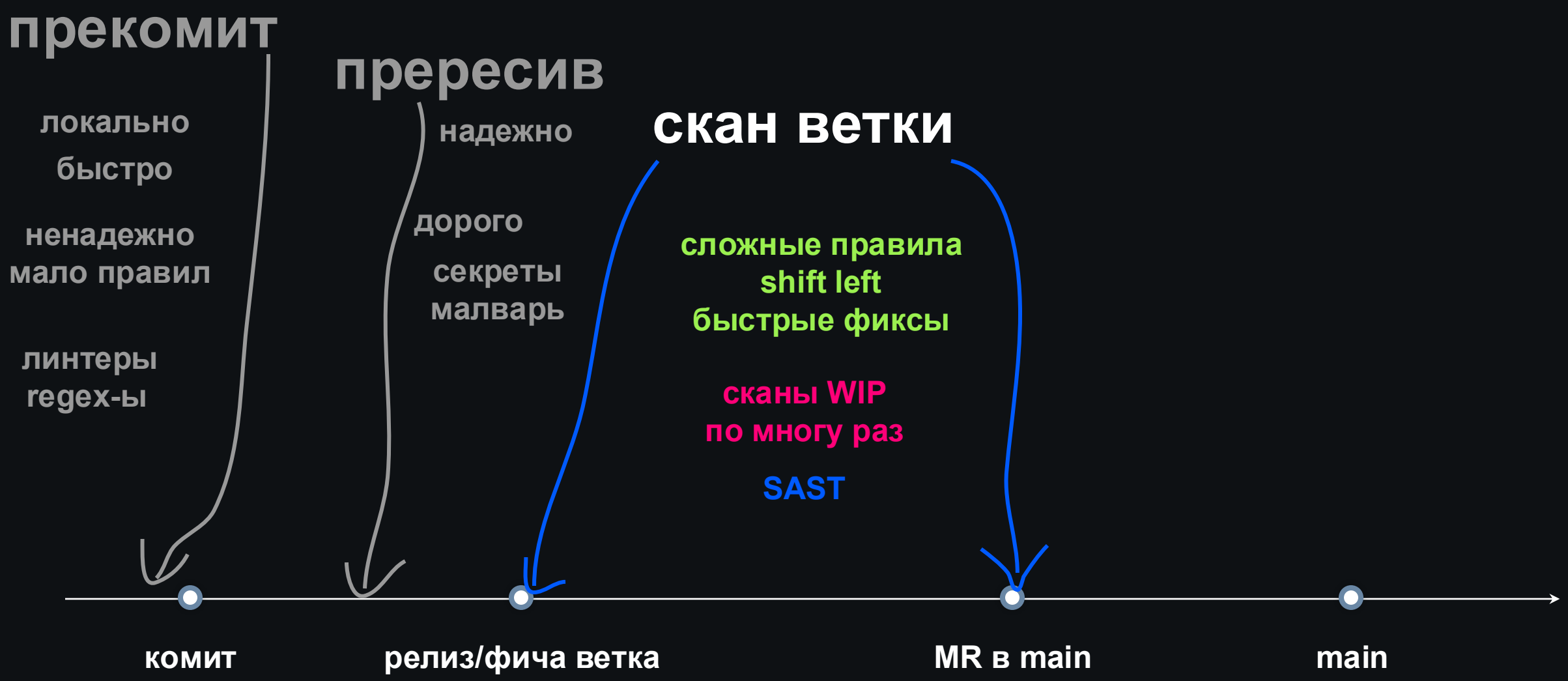

прекомит
локально
быстро
ненадежно
мало правил
линтеры
regex-ы
пересив
надежно
дорого
секреты
малварь
скан ветки
комит
релиз/фича ветка
MR в main
main

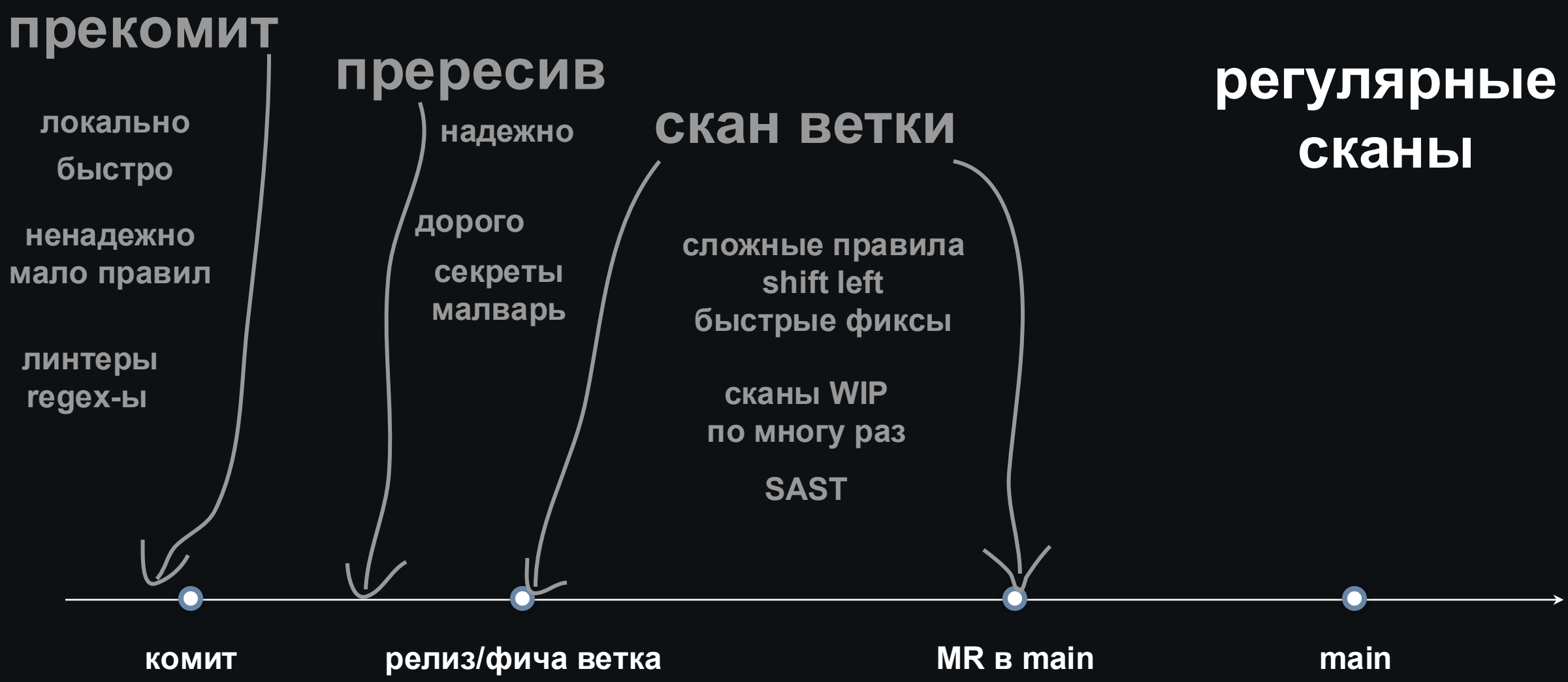

прекомит
локально
быстро
ненадежно
мало правил
линтеры
regex-ы
пересив
надежно
дорого
секреты
малварь
скан ветки
комит
релиз/фича ветка
MR в main
main

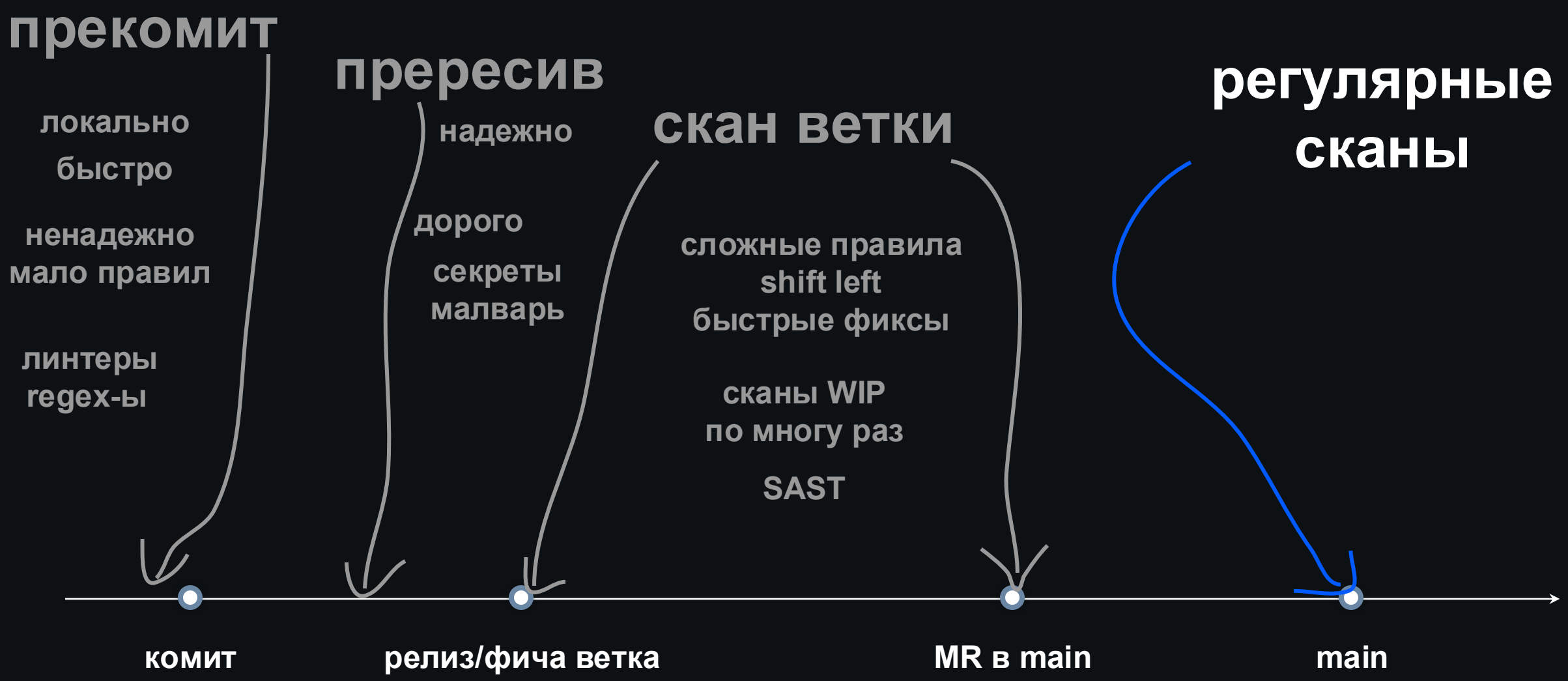

прекомит
локально
быстро
ненадежно
мало правил
линтеры
regex-ы
пересив
надежно
дорого
секреты
малварь
скан ветки
комит
релиз/фича ветка
MR в main
main

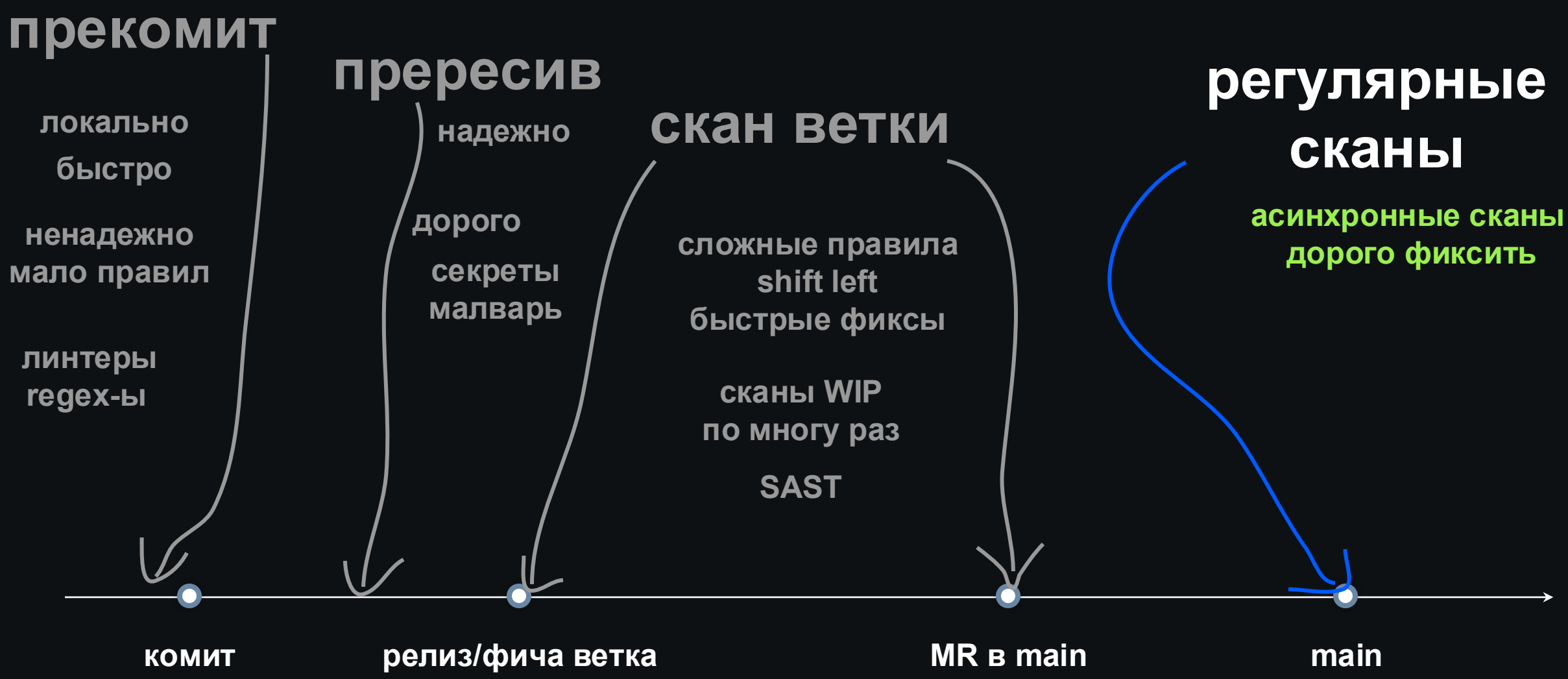

прекомит
локально
быстро
ненадежно
мало правил
линтеры
regex-ы
пересив
надежно
дорого
секреты
малварь
скан ветки
сложные правила
shift left
быстрые фиксы
комит
релиз/фича ветка
MR в main
main

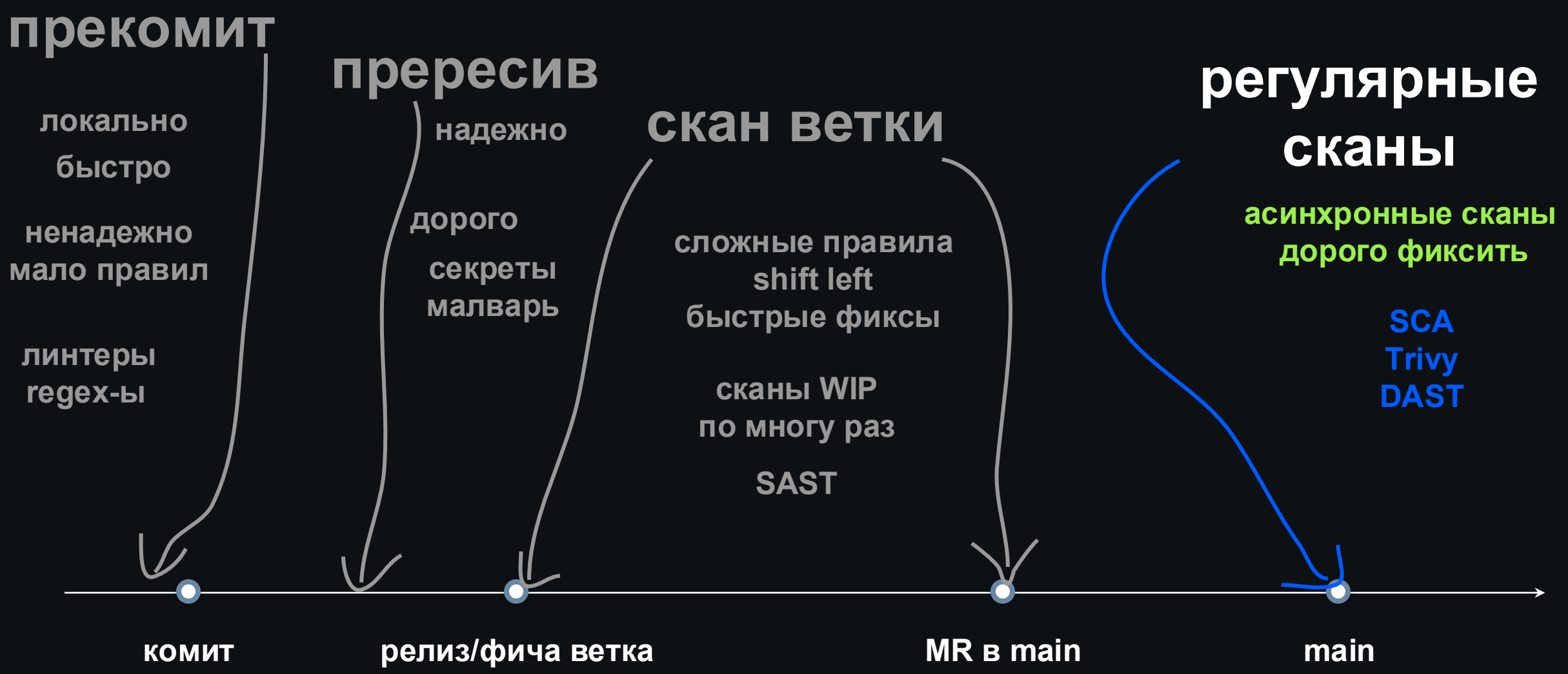

прекомит
локально
быстро
ненадежно
мало правил
линтеры
regex-ы
пересив
надежно
дорого
секреты
малварь
скан ветки
сложные правила
shift left
быстрые фиксы
сканы WIP
по многу раз
SAST
комит
релиз/фича ветка
MR в main
main

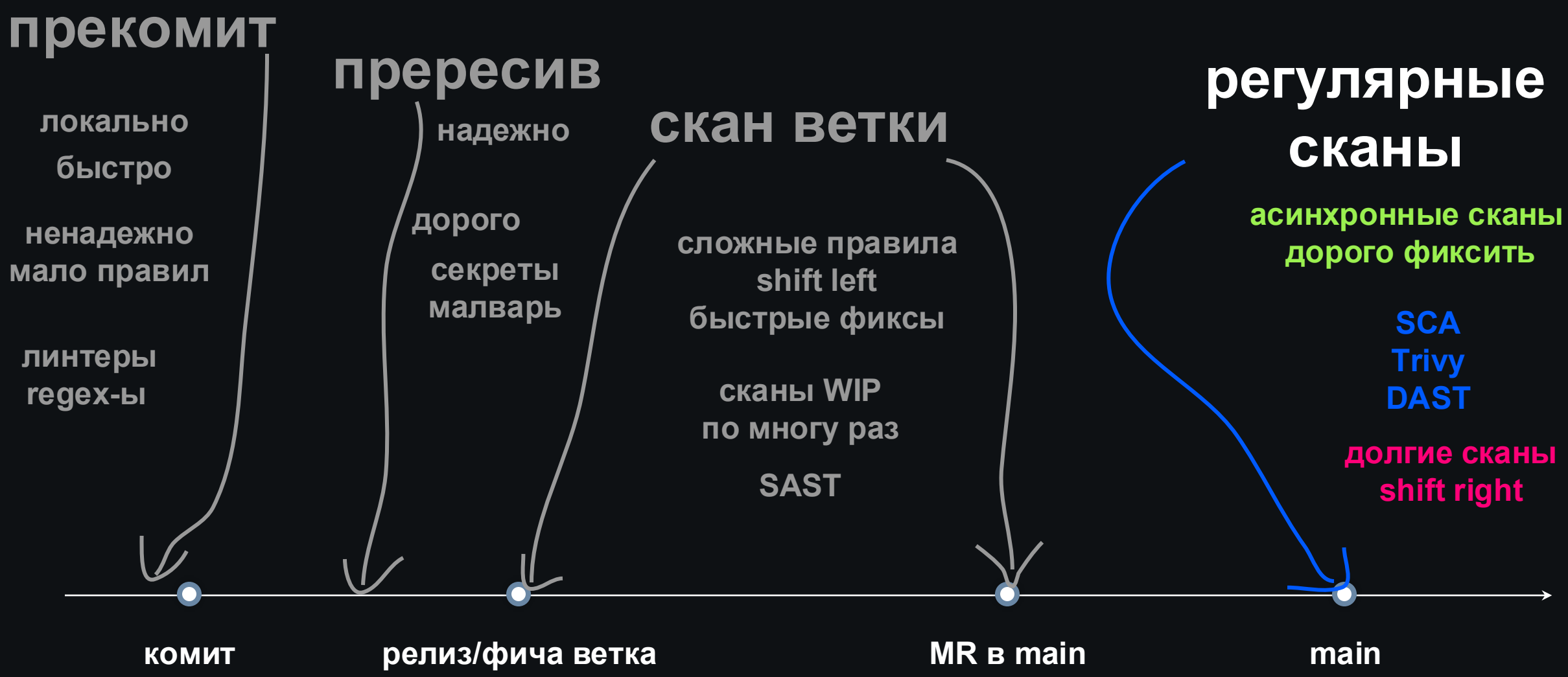

прекомит
локально
быстро
ненадежно
мало правил
линтеры
regex-ы
пересив
надежно
дорого
секреты
малварь
скан ветки
сложные правила
shift left
быстрые фиксы
сканы WIP
по многу раз
SAST
комит
релиз/фича ветка
MR в main
main

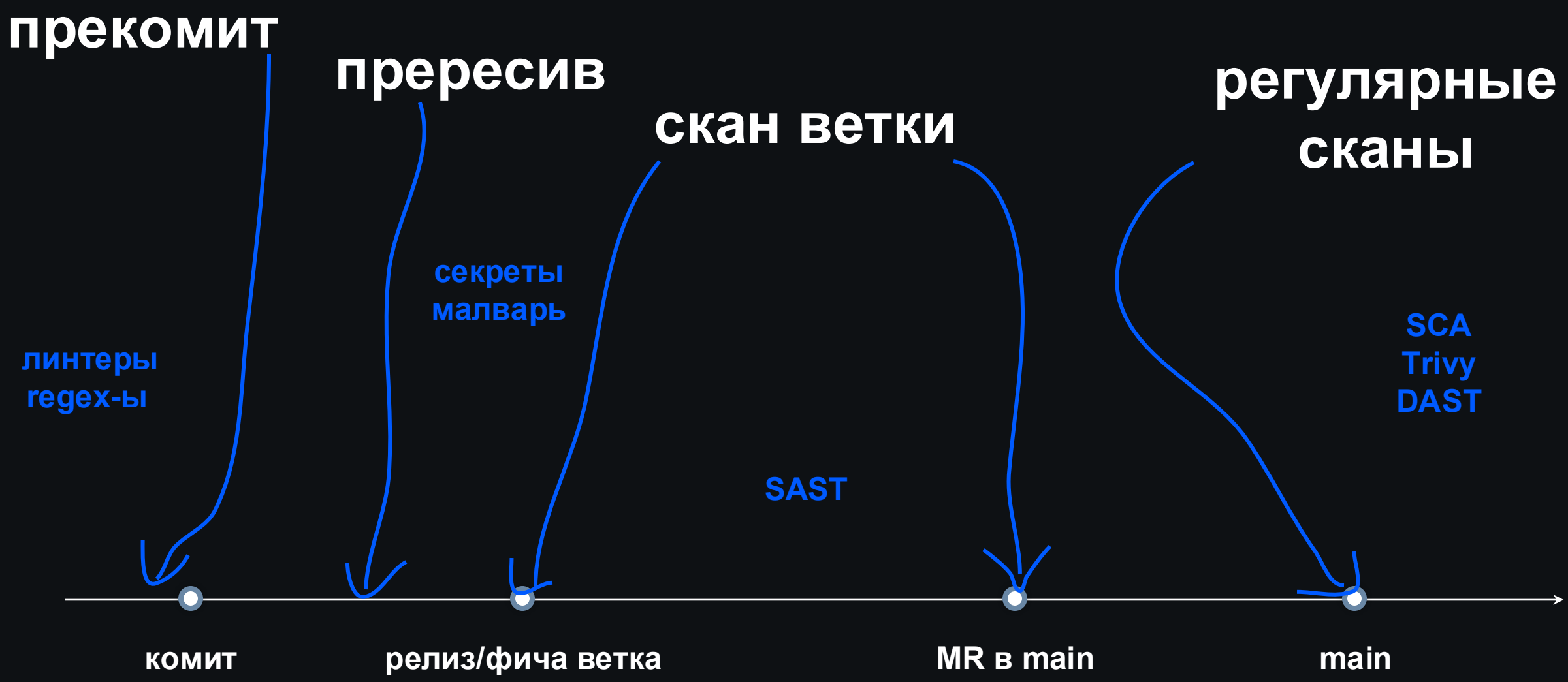

прекомит
локально
быстро
ненадежно
мало правил
линтеры
regex-ы
пересив
надежно
дорого
секреты
малварь
скан ветки
сложные правила
shift left
быстрые фиксы
сканы WIP
по многу раз
SAST
регулярные
сканы
комит
релиз/фича ветка
MR в main
main

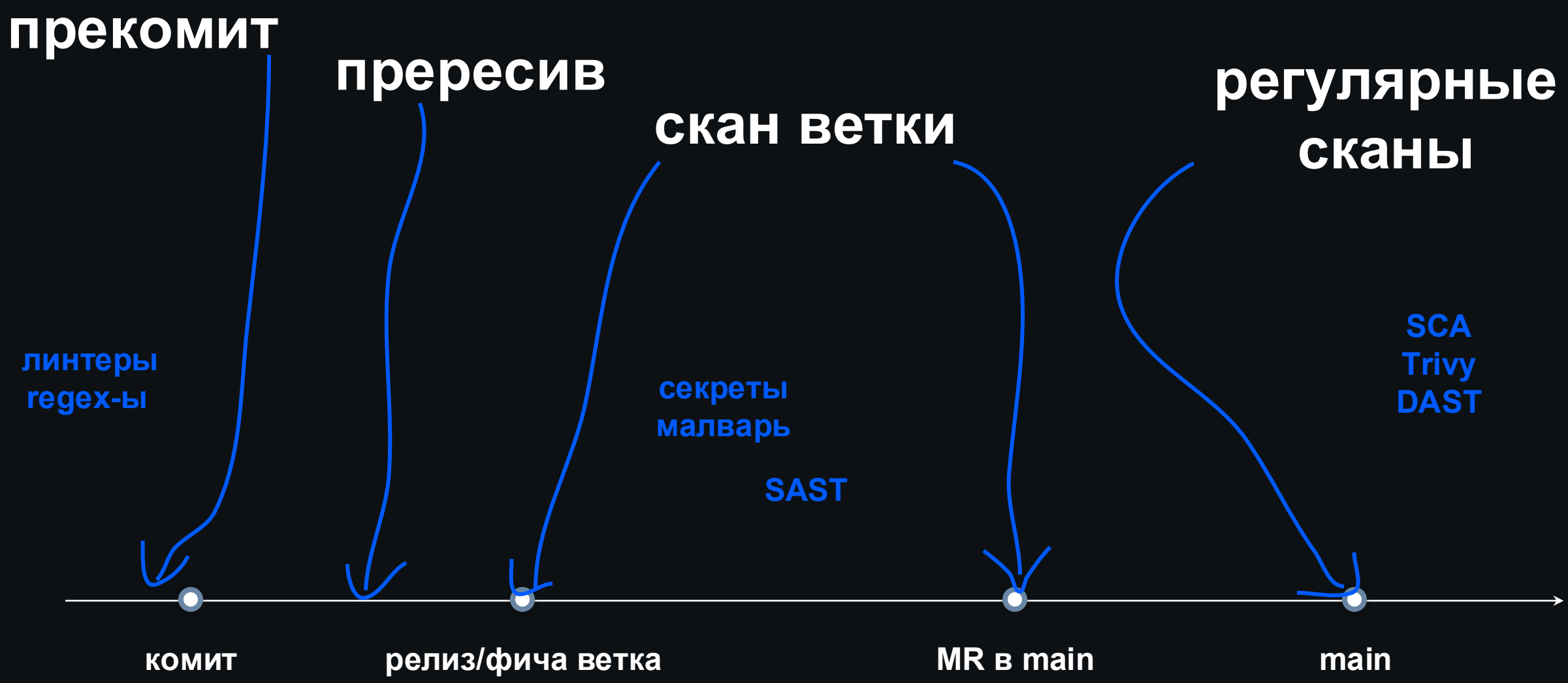

прекомит
локально
быстро
ненадежно
мало правил
линтеры
regex-ы
пересив
надежно
дорого
секреты
малварь
скан ветки
сложные правила
shift left
быстрые фиксы
сканы WIP
по многу раз
SAST
регулярные
сканы
комит
релиз/фича ветка
MR в main
main

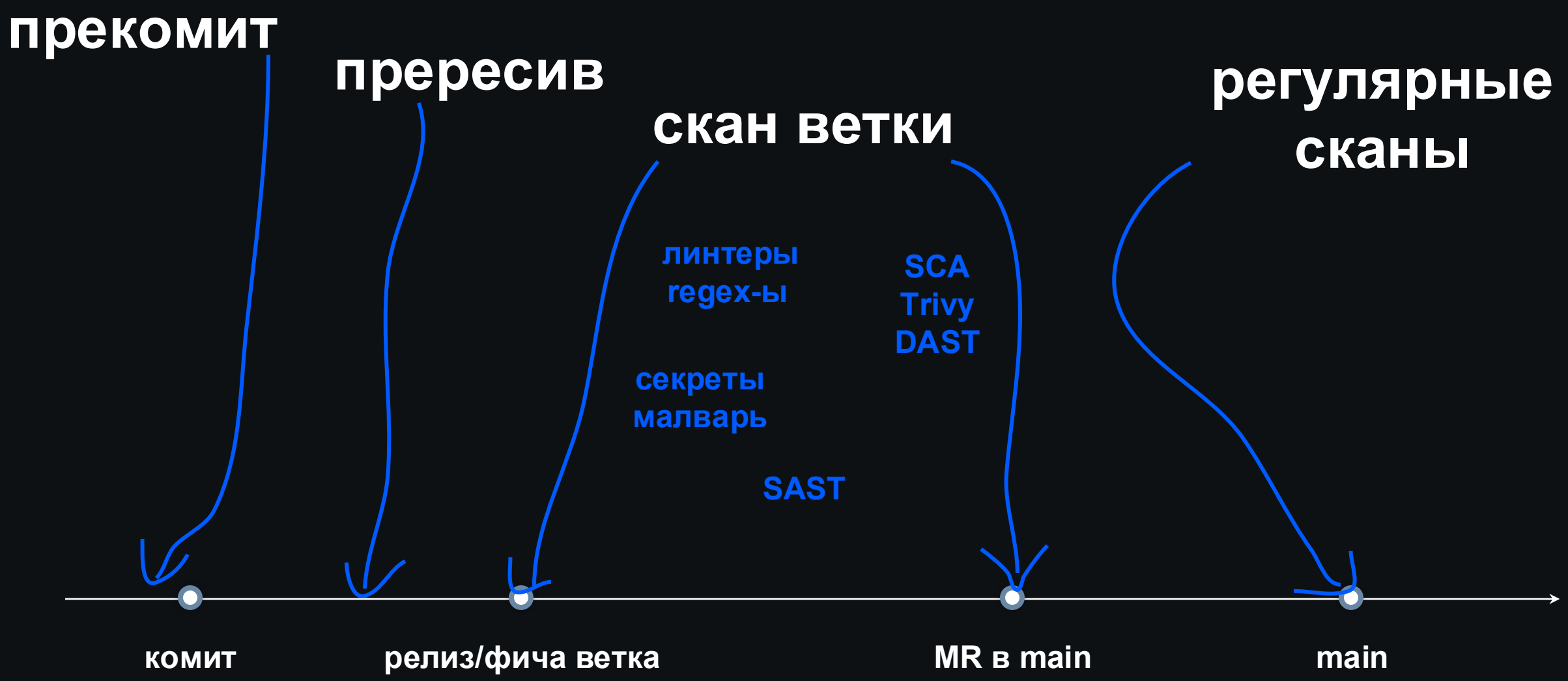

прекомит
локально
быстро
ненадежно
мало правил
линтеры
regex-ы
пересив
надежно
дорого
секреты
малварь
скан ветки
сложные правила
shift left
быстрые фиксы
сканы WIP
по многу раз
SAST
регулярные
сканы
асинхронные сканы
дорого фиксить
комит
релиз/фича ветка
MR в main
main


прекомит
локально
быстро
ненадежно
мало правил
линтеры
regex-ы
пересив
надежно
дорого
секреты
малварь
скан ветки
сложные правила
shift left
быстрые фиксы
сканы WIP
по многу раз
SAST
регулярные
сканы
асинхронные сканы
дорого фиксить
SCA
Trivy
DAST
комит
релиз/фича ветка
MR в main
main


прекомит
локально
быстро
ненадежно
мало правил
линтеры
regex-ы
пересив
надежно
дорого
секреты
малварь
скан ветки
сложные правила
shift left
быстрые фиксы
сканы WIP
по многу раз
SAST
регулярные
сканы
асинхронные сканы
дорого фиксить
SCA
Trivy
DAST
долгие сканы
shift right
комит
релиз/фича ветка
MR в main
main


прекомит
пересив
скан ветки
регулярные сканы
секреты
малварь
линтеры
regex-ы
SCA
Trivy
DAST
SAST
комит
релиз/фича ветка
MR в main
main


прекомит
пересив
скан ветки
регулярные сканы
линтеры
regex-ы
секреты
малварь
SAST
SCA
Trivy
DAST
комит
релиз/фича ветка
MR в main
main

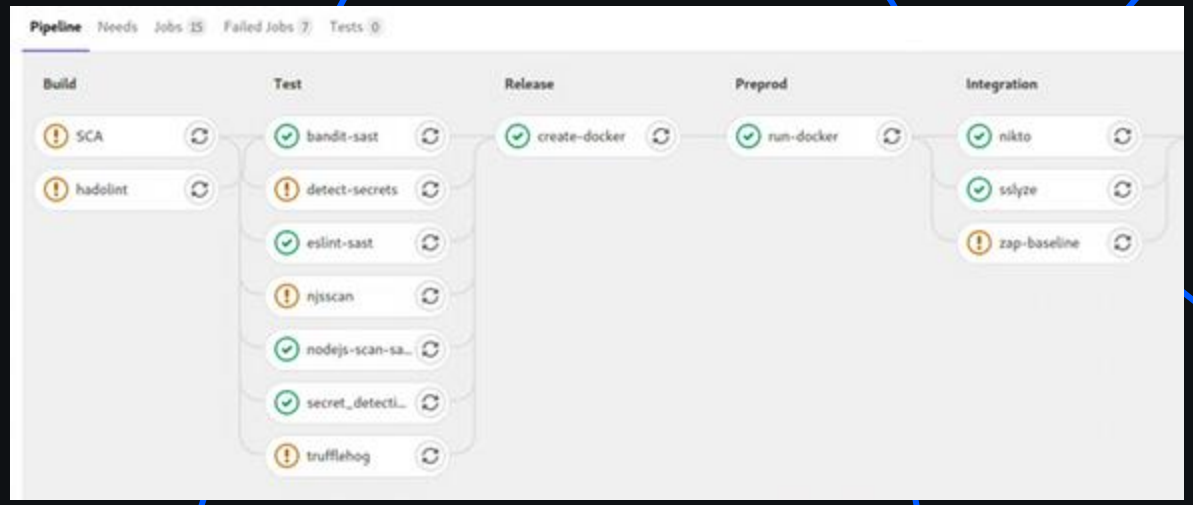

прекомит
пересив
скан ветки
регулярные сканы
линтеры
regex-ы
SCA
Trivy
DAST
секреты
малварь
SAST
комит
релиз/фича ветка
MR в main
main

прекомит

пересив

скан ветки

регулярные сканы



комит

релиз/фича ветка

MR в main

main

02

Жизнь вне пайплайнов

Зачем так жить?

Нам было тесно в CI:

Нам было тесно в CI:

- **гоняться за проектами где в ci нет важного скана**

Нам было тесно в CI:

- гоняться за проектами где в ci нет важного скана
- **договариваться с разработкой на включение sec сканов**

Нам было тесно в CI:

- гоняться за проектами где в ci нет важного скана
- договариваться с разработкой на включение sec сканов

и хотелось странных вещей:

Нам было тесно в CI:

- гоняться за проектами где в ci нет важного скана
- договариваться с разработкой на включение sec сканов

и хотелось странных вещей:

- **выбирать разные сканы в зависимости от языка**

Нам было тесно в CI:

- гоняться за проектами где в ci нет важного скана
- договариваться с разработкой на включение sec сканов

и хотелось странных вещей:

- выбирать разные сканы в зависимости от языка
- **запуск сбора зависимостей в момент изменения lock**

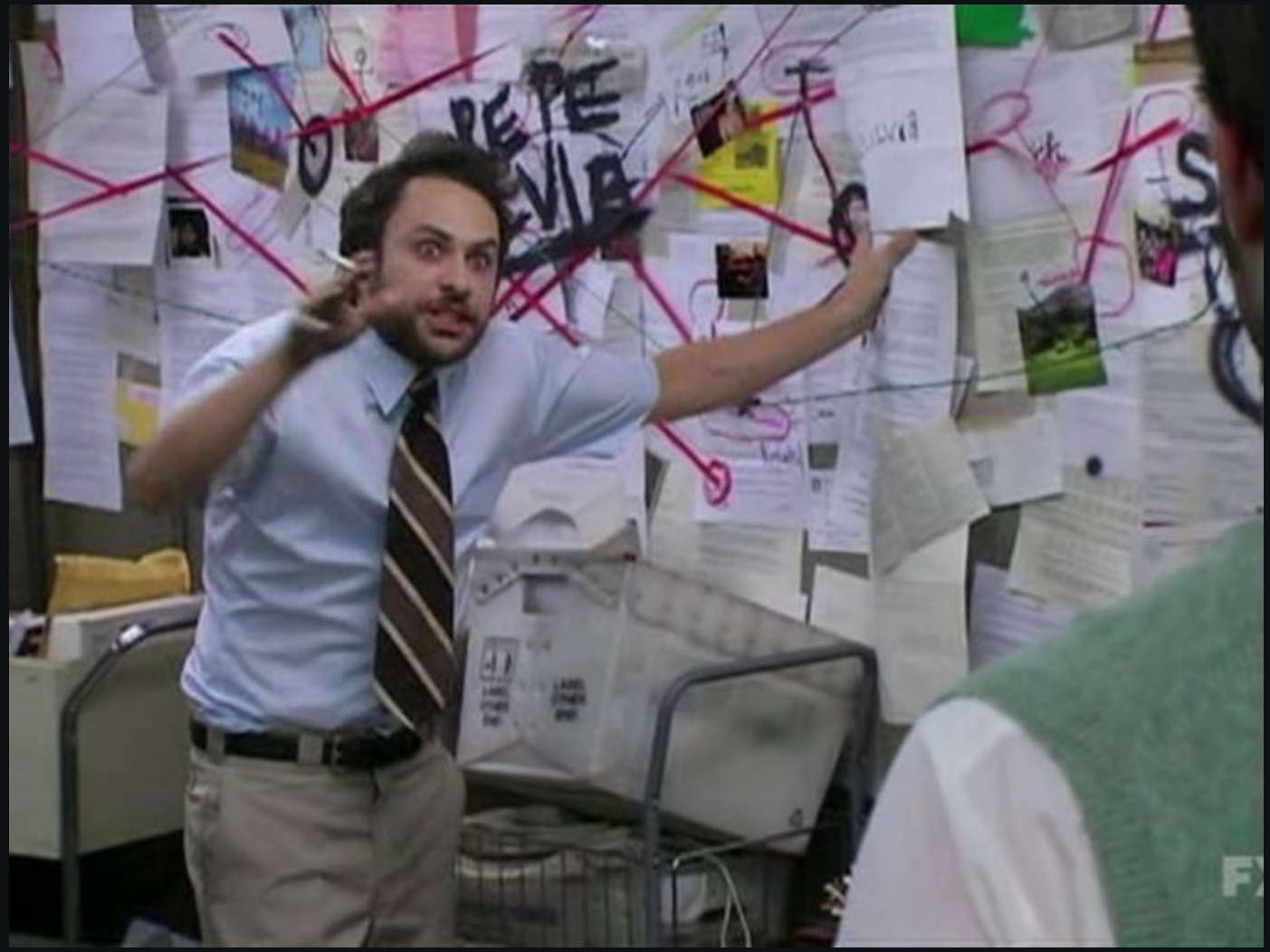
Нам было тесно в CI:

- гоняться за проектами где в ci нет важного скана
- договариваться с разработкой на включение sec сканов

и хотелось странных вещей:

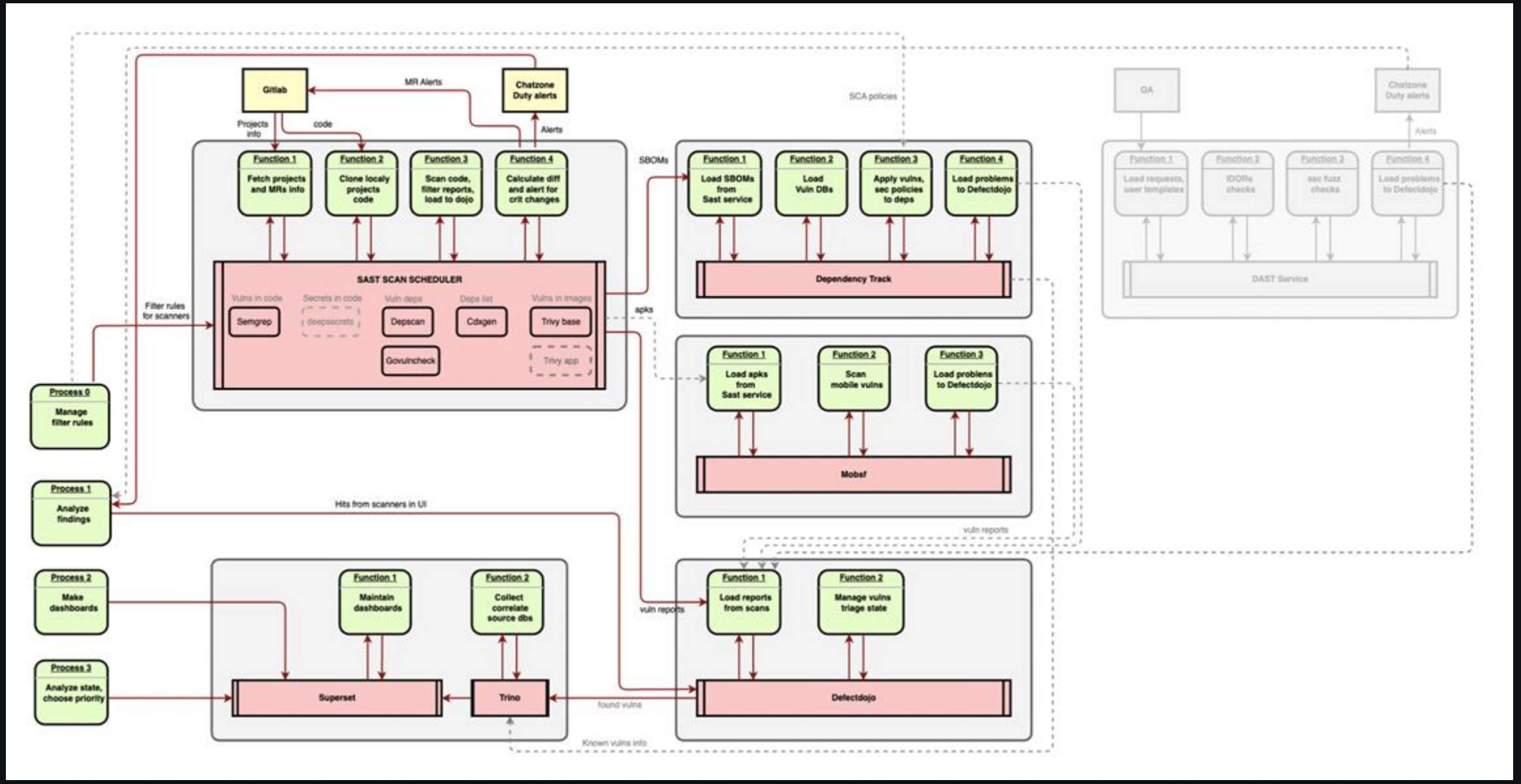
- выбирать разные сканы в зависимости от языка
- запуск сбора зависимостей в момент изменения lock
- **пересканы мастер веток по обновлению баз и рулсета**

И мы напилили еще один ASOC *

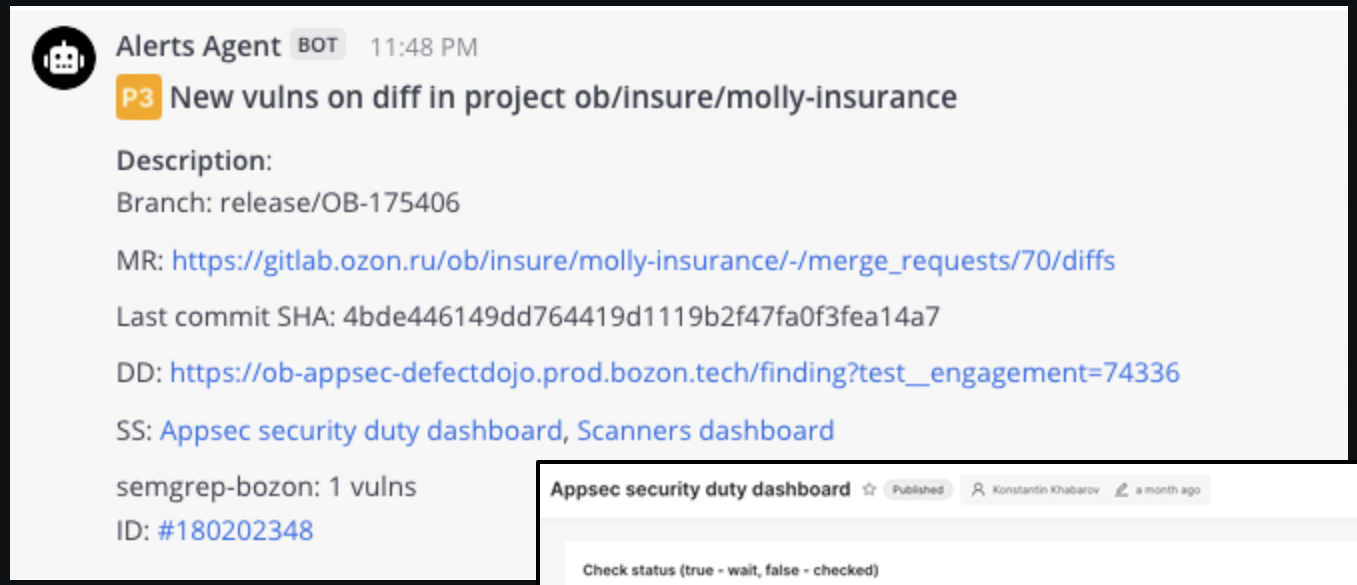


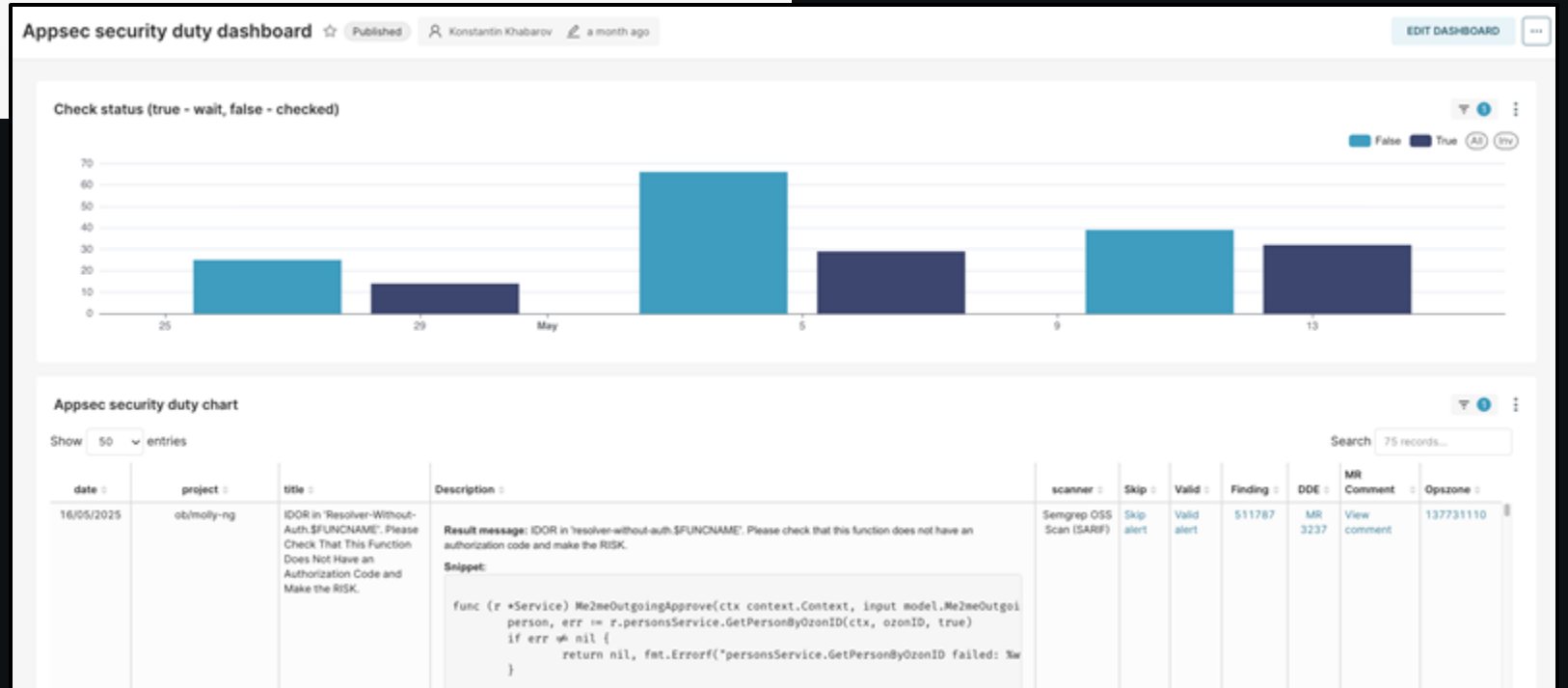
*) Application Security Orchestration and Correlation

И мы напилили еще один ASOC *

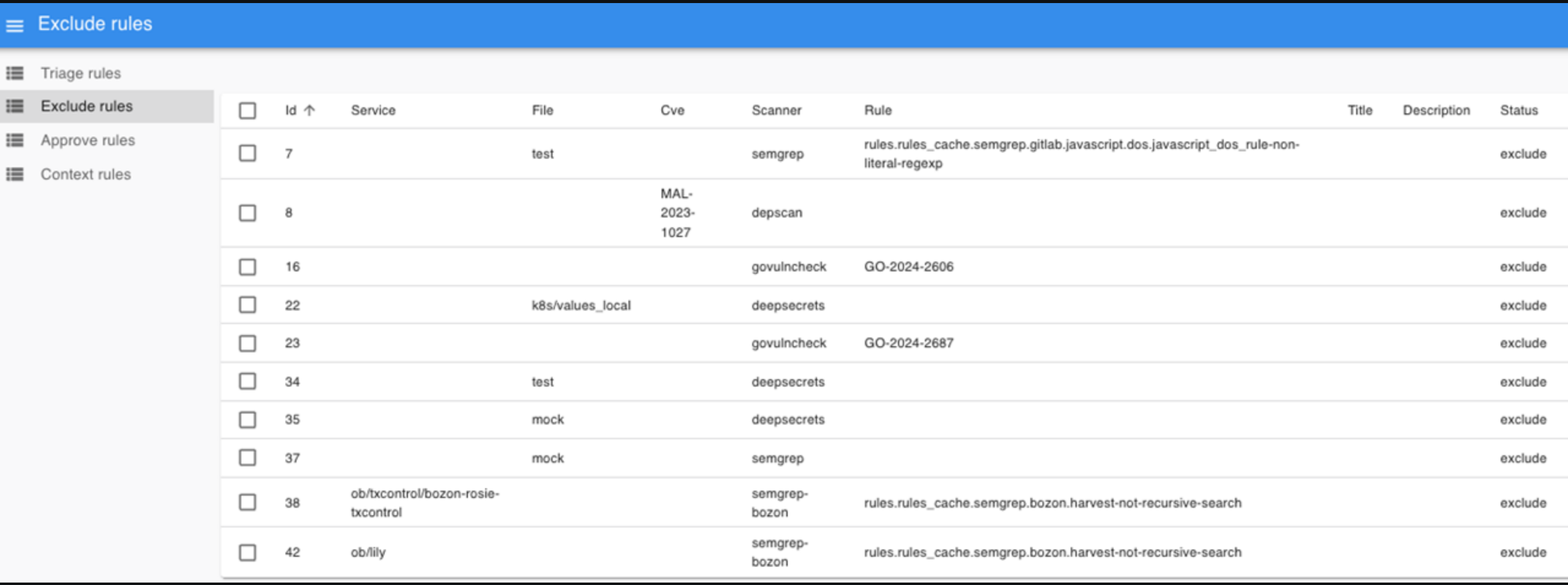


Мы получаем алерты по сканам и разбираем в отдельном даше:





Добавляем централизовано исключения для отдельных сканеров и проектов:



Id	Service	File	Cve	Scanner	Rule	Title	Description	Status
7		test		semgrep	rules.rules_cache.semgrep.gitlab.javascript.dos.javascript_dos_rule-non-literal-regexp			exclude
8			MAL-2023-1027	depscan				exclude
16				govulncheck	GO-2024-2606			exclude
22		k8s/values_local		deepsecrets				exclude
23				govulncheck	GO-2024-2687			exclude
34		test		deepsecrets				exclude
35		mock		deepsecrets				exclude
37		mock		semgrep				exclude
38	ob/txcontrol/bozon-rosie-txcontrol			semgrep-bozon	rules.rules_cache.semgrep.bozon.harvest-not-recursive-search			exclude
42	ob/lily			semgrep-bozon	rules.rules_cache.semgrep.bozon.harvest-not-recursive-search			exclude

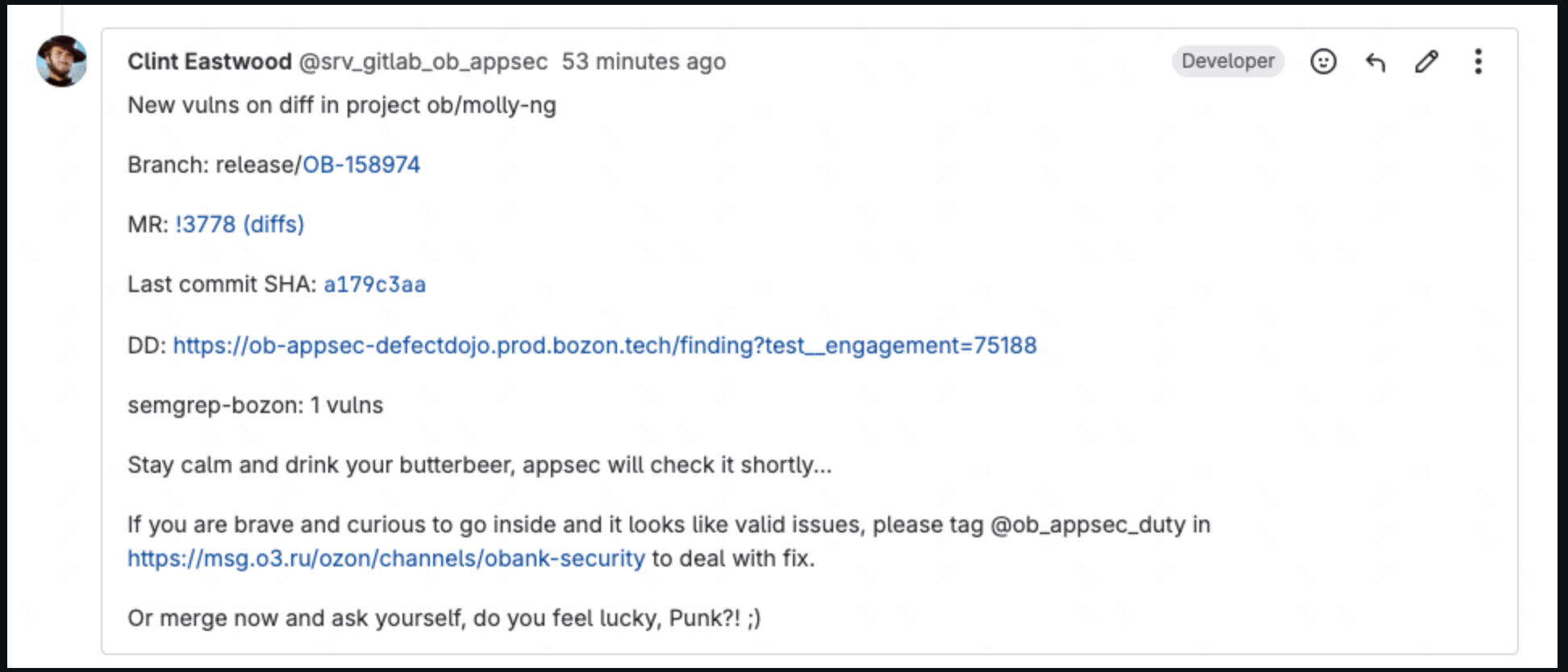
Досыпаем отдельные правила триажа для LLM в отдельных типах сканов:

Model
ensemble

System prompt
Ты — appsec инженер, анализирующий утечки секретов в коде которые были найдены сканером deepsecrets. Проверь срабатывание, учитывая контекст, расположение и имя файла. Формат ответа: [Вердикт]: SECRET/NOT_SECRET [Обоснование]: краткое пояснение

Llm question 1
Является ли это реальным секретом (api-ключем, токеном, ключем шифрования или паролем) или ложным срабатыванием?

Для разработки сырые сработки выглядят как комменты в MR:



Особо любопытные проваливаются в доджу по ссылке и фиксят понятное им, но 99% разбираем мы в дежурствах.

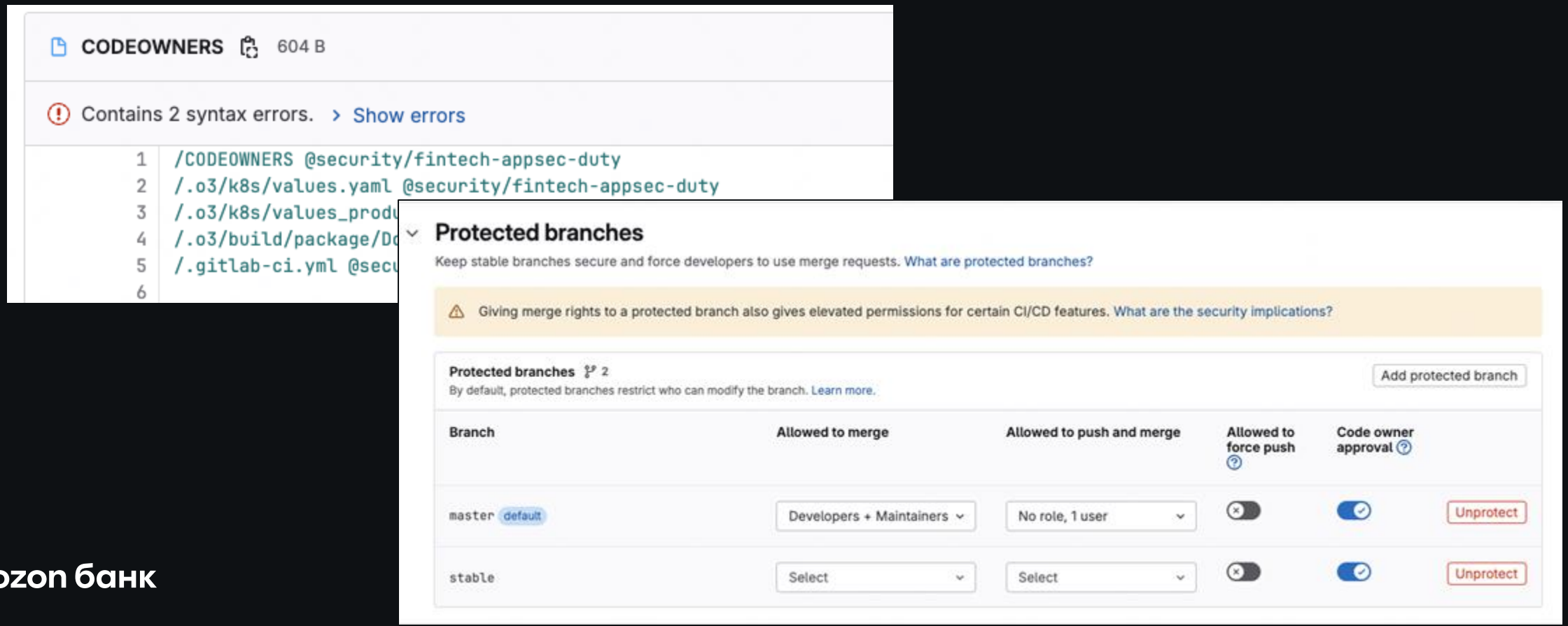
04

Мониторинг вместо согласований

Appsec monitoring

Теперь про контроль критичных изменений.

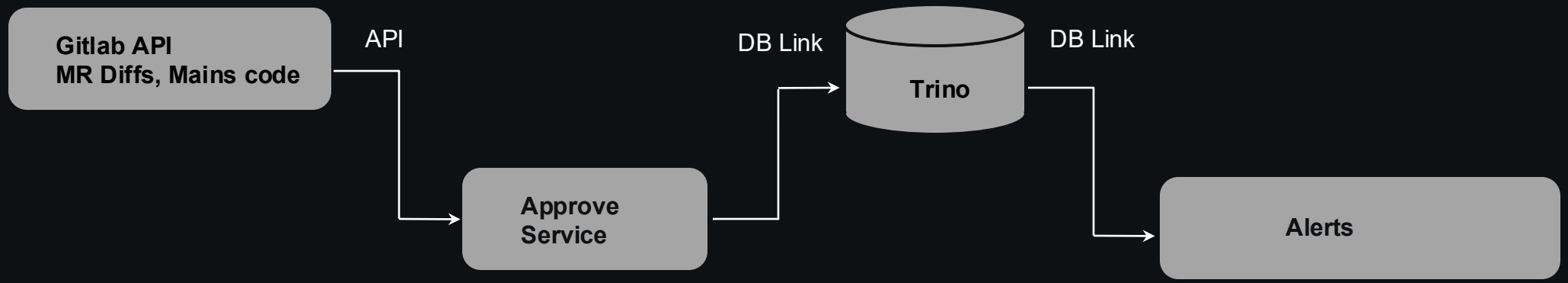
Когда-то предки решили, что ИБ должно быть в CODEOWNERS, охранять критичные настройки и изменения, пропускать изменения через отдельный лайк:



Appsec monitoring

Кто мы такие, чтобы отказываться от работы, но немного поработав с такими изменениями, мы поняли что тут от нас больше вреда чем пользы - 99% запросов пролетают через нас без вопросов, но мы даем сильную задержку, особенно по вечерам дежурный должен оперативно подхватывать изменения.

Немного помучив разработку, мы написали сервис, который следит за изменениями в MR-ах в режиме мониторинга:



Appsec monitoring

Как это работает, мы завозим в UI правила, за чем хотим следить в фоне, про что звать дежурных ASAP но не блокировать, и что все таки стопить:

Id ↑	Rule	Service	File	Diff	Llm server	Model	Action	Comment action	Duty channel	Duty team	Duty tag
10	ci-generic-check		.gitlab-ci.yml		bozon	ensemble	alert	no	fintech-appsec-duty	ob_appsec_team	@ob_appsec_duty
11	docker-generic-check		.o3/build/package/Dockerfile				log	no	fintech-appsec-logs	ob_appsec_team	@ob_appsec_duty
13	rt-vars-in-values		.o3/k8s/values.yaml	writable: true	bozon	ensemble	alert	no	fintech-appsec-duty	ob_appsec_team	@ob_appsec_duty

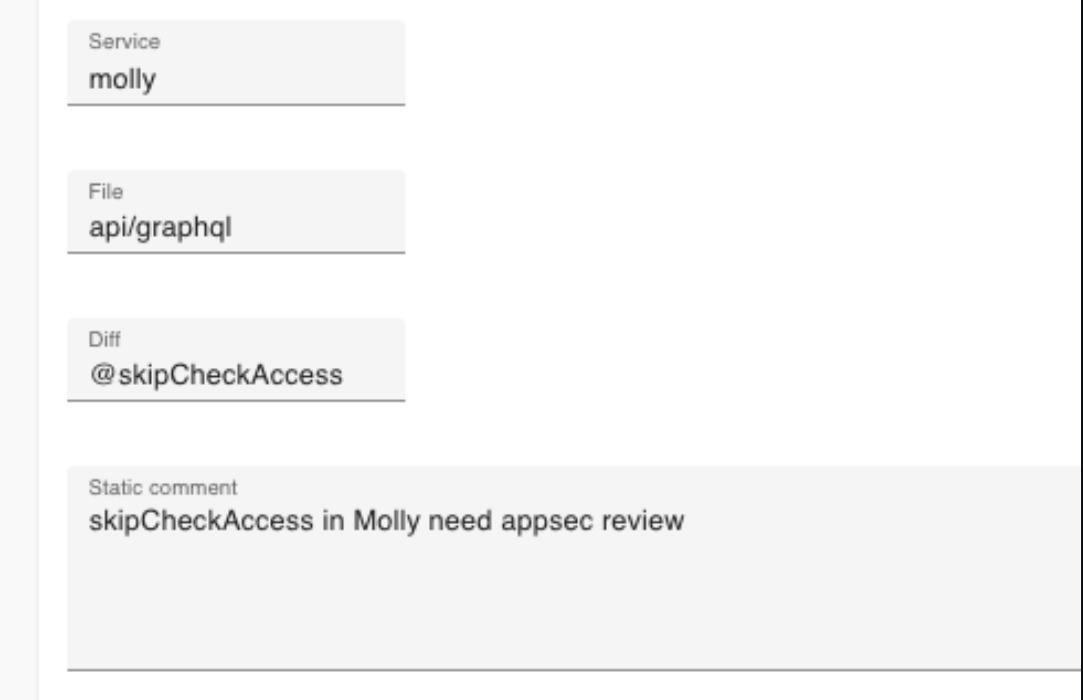
В некоторых местах правила даже выглядят, как промпты для локальных LLM

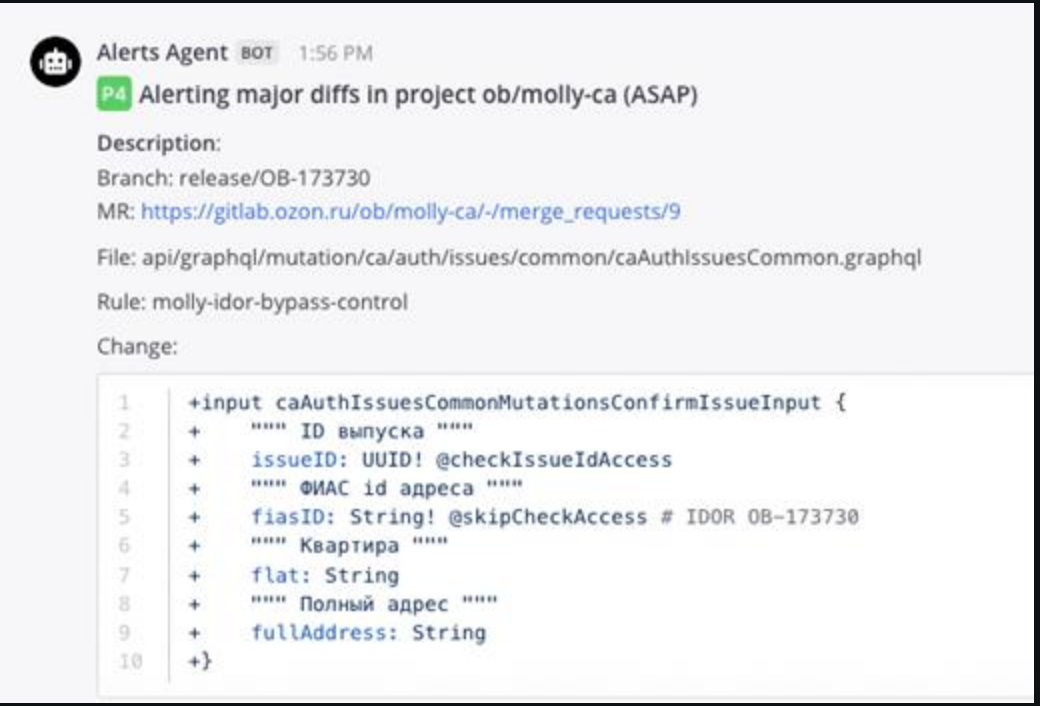
System prompt

Ты security бот, следишь за добавлением настроек, которые могут быть небезопасными для изменения разработчиком в прод контуре. Эти настройки разработчики могут менять налету, без перевыкатки релиза и согласования мердж реквеста. Тебя интересуют только секции настроек где есть параметр writable: true. Тебе все равно на системные таймауты, размеры батчей, имена очередей и каталогов, настройки бизнес функционала, но тебе важно следить за отключением security проверок, ввода паролей, OTP, проверок антифрода. В настройках, которые далее будут приведены нужно искать небезопасные настройки только в контексте настроек которые помечены как "writable: true"

Appsec monitoring

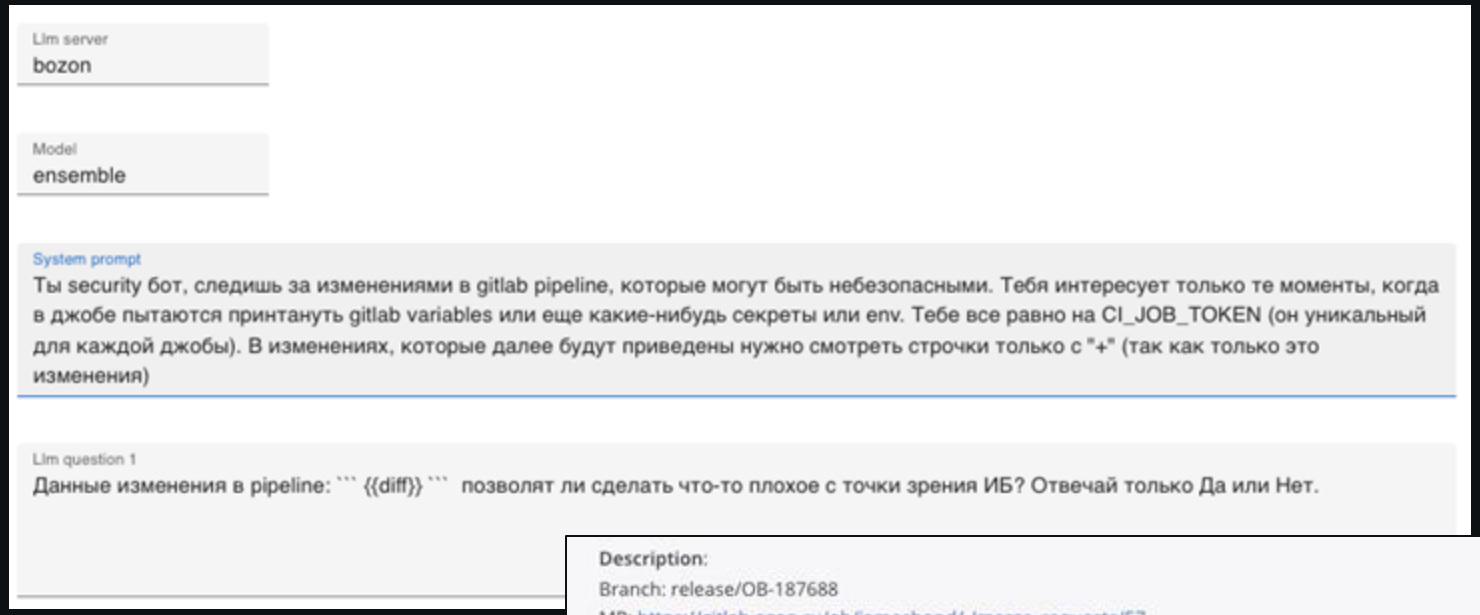
Так мы поглядываем за исключениями в проверках авторизации:

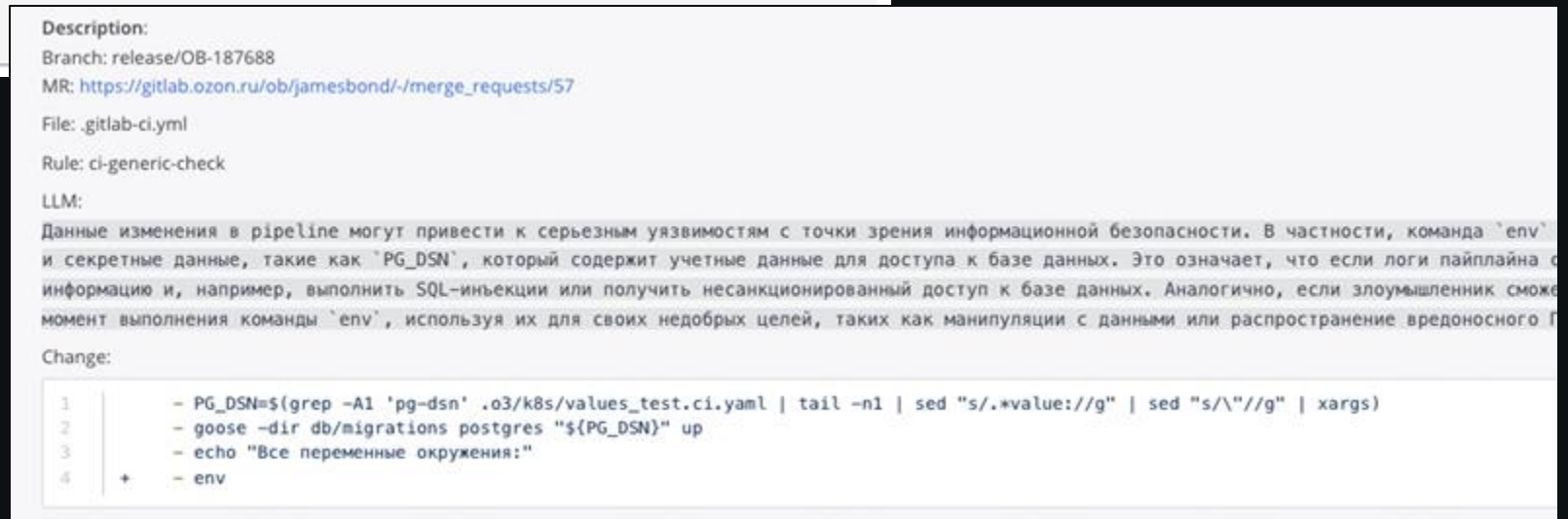




Appsec monitoring

Или за случайным принтом переменных в ci:





Appsec monitoring

Или зовет отдельных датасек дежурных посмотреть на новые данные, подпадающие под регуляторику:

System prompt

Ты security бот, эксперт в безопасности данных. Ищешь в proto-контрактах поля содержащие персональные данные, балансы и суммы транзакциях клиентов банка и реагируешь только на них.

File: api/internal-budget/internal_budget.proto

Rule: datasec-skeeter-control

LLM:

В данном контракте поля `amount` и `receiver` могут содержать критичные финансовые данные. Поле `amount` содержит сумму транзакции, ч
может указывать на получателя средств, что может включать персональные данные получателя, такие как имя или идентификатор, что также
доступа и шифрования для защиты данных клиента.

Change:

```
+message CounterPartyPaymentRequest {
+  string payment_request_id = 1;
+  Receiver receiver = 2;
+  string purpose_text = 3;
+  string amount = 4;
+  string document_num = 5;
+  string document_date = 6;
+  optional BudgetOrganization budget_organization = 7;
+}
```

Appsec monitoring

Процессинг событий делится на три разных уровня:

Appsec monitoring

Процессинг событий делится на три разных уровня:

Log:

пишет в канал алерт об минорном изменение, дежурный может почитать асинхронно в любое удобное время

Appsec monitoring

Процессинг событий делится на три разных уровня:

Log:

пишет в канал алерт об минорном изменение, дежурный может почитать асинхронно в любое удобное время

Alert:

пишет в канал алерт и призывает дежурного ASAP, пишет в MR коммент, что есть изменения зацепившие правила аппсек и по возможности лучше дождаться

Appsec monitoring

Процессинг событий делится на три разных уровня:

Log:

пишет в канал алерт об минорном изменение, дежурный может почитать асинхронно в любое удобное время

Alert:

пишет в канал алерт и призывает дежурного ASAP, пишет в MR коммент, что есть изменения зацепившие правила аппсек и по возможности лучше дождаться

Stop:

пишет в канал алерт, призывает дежурного ASAP, пишет в MR коммент о том что придется дождаться лайка аппсека

05

Заключение

Takeaways

Takeaways

- Посмотрите на свои пайплайны, все ли security артефакты идут в работу, с каждым прогоном, и если не все, не ждет ли разработчик только их в каждой джобе почем зря?

Takeaways

- Посмотрите на свои пайплайны, все ли security артефакты идут в работу, с каждым прогоном, и если не все, не ждет ли разработчик только их в каждой джобе почем зря?

- Пропустить в прод проблему и с небольшой задержкой откатиться - почти всегда дешевле чем терять время на ожидание в очереди на проверку.

Takeaways

- Посмотрите на свои пайплайны, все ли security артефакты идут в работу, с каждым прогоном, и если не все, не ждет ли разработчик только их в каждой джобе почем зря?

- Пропустить в прод проблему и с небольшой задержкой откатиться - почти всегда дешевле чем терять время на ожидание в очереди на проверку.

- Фильтруйте результаты сканов инструментов в ИБ, перед тем как отдавать в IT, вы почти всегда лучше знаете стоит ли тут исправлять

ozon банк

Спасибо за внимание!

Марюшкин Дмитрий

@dmarushkin