GUARD CONF

Shift Everywhere

Технологии защиты цепочки поставки на каждом этапе разработки ПО



Антон Володченко

Руководитель
разработки продуктов
CodeScoring



План

- Цепочка поставки и риски
- Защита и технологии
- Результаты, политики, метрики



Что за цепочка поставки?

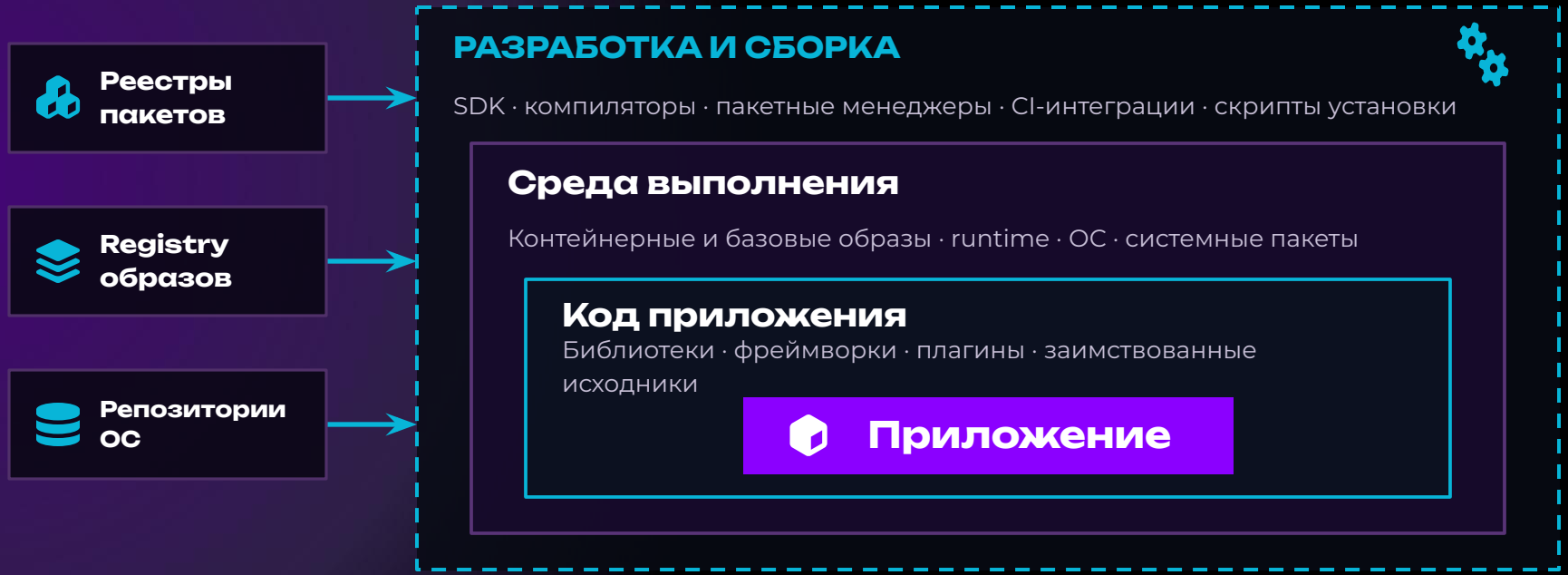
GUARDCORE

Цепочка поставки — совокупность организационно-технических мер и действий по обеспечению необходимым программным обеспечением процессов разработки программного обеспечения организации.

из проекта ГОСТ КАПО

Что входит в цепочку поставки?

GUARDCORE



GUARDCORE

456 тыс.

Вредоносных пакетов
в 2025 году



подробнее на Habr

Наша аналитика Open Source

250 млн

Open Source-проектов
2025

100 млн

Разработчиков OSS
2025

×4

Новых уязвимостей в октябре 2025 к 2026
6,5 тыс. → 26 тыс.

14 тыс.

Новых уязвимостей
в пакетах · 2025

Чёрный октябрь 2026

GUARDCORE

PHP / PHP2Shell

21 октября

CVE-2026-109618
CVE-2026-109619

Повреждение памяти при обработке запросов

Node.js / Brotli

21 октября

CVE-2026-111497

Выход за границы буфера декодера

Linux Kernel

15 октября

CVE-2026-98432

Use-after-free в IPv4 / TCP

Другие атаки в 2026

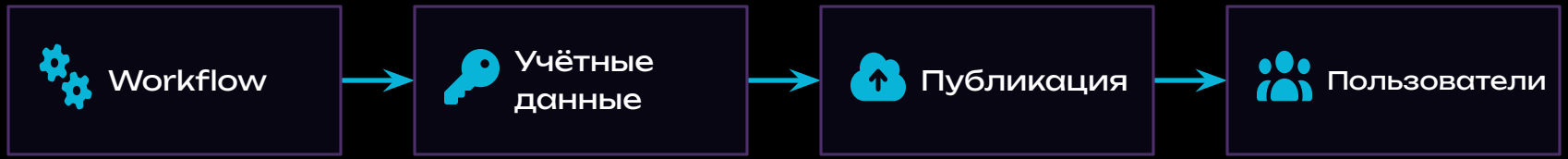
GUARDCORP

Trivy

19 марта 2026
Вредоносная публикация

LiteLLM

24 марта 2026
Скомпрометированные PyPI-версии



Доверенный канал поставки становится вектором атаки

Червь Shai-Hulud

GUARDCORE

Заражённый пакет

Попадает в разработку

Кража секретов

Токены разработчика и CI



SHAI-HULUD

самораспространяется

Новые заражения

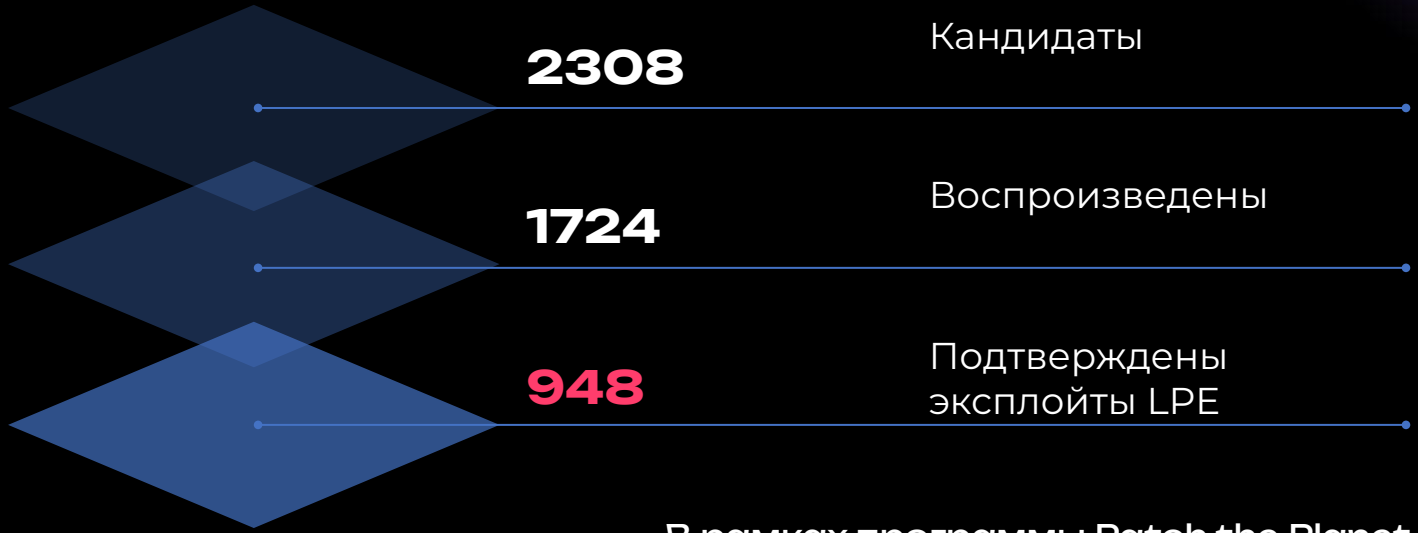
Другие пакеты и команды

Новые публикации

Червь использует токены

Больше секретов → больше доступов → больше заражённых пакетов

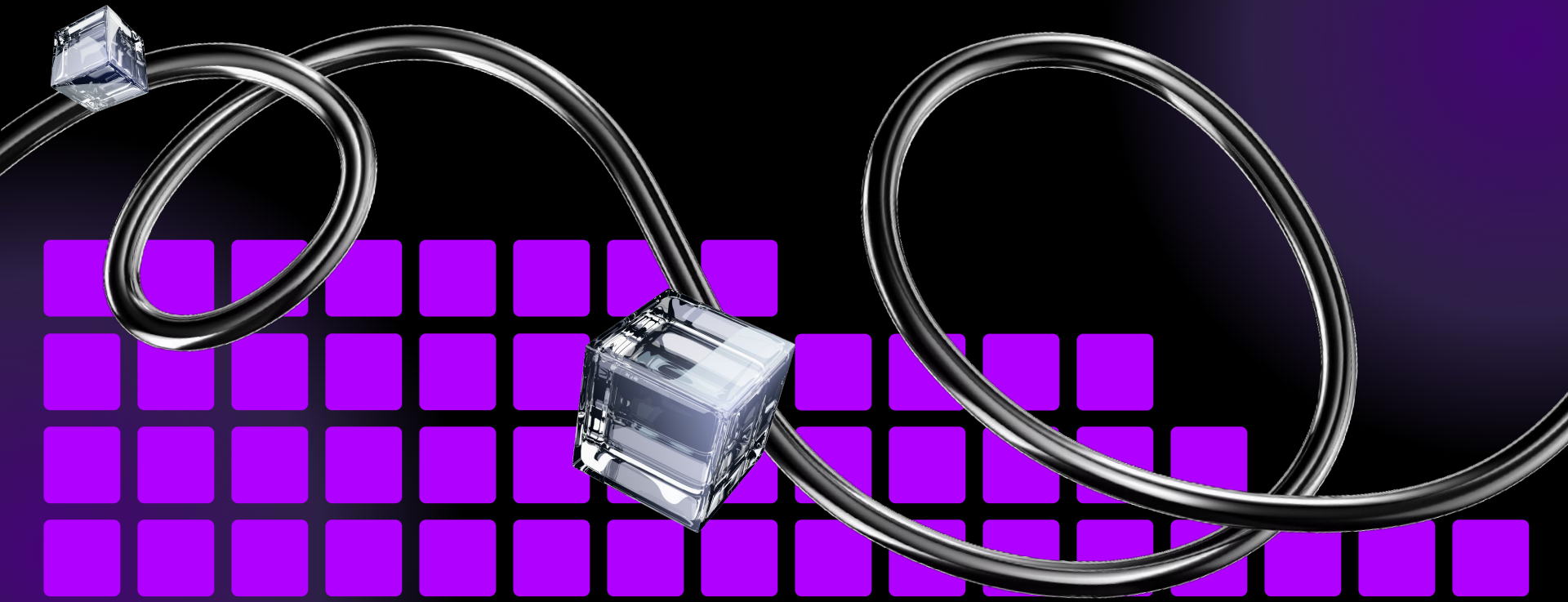
Уязвимости от OpenAI



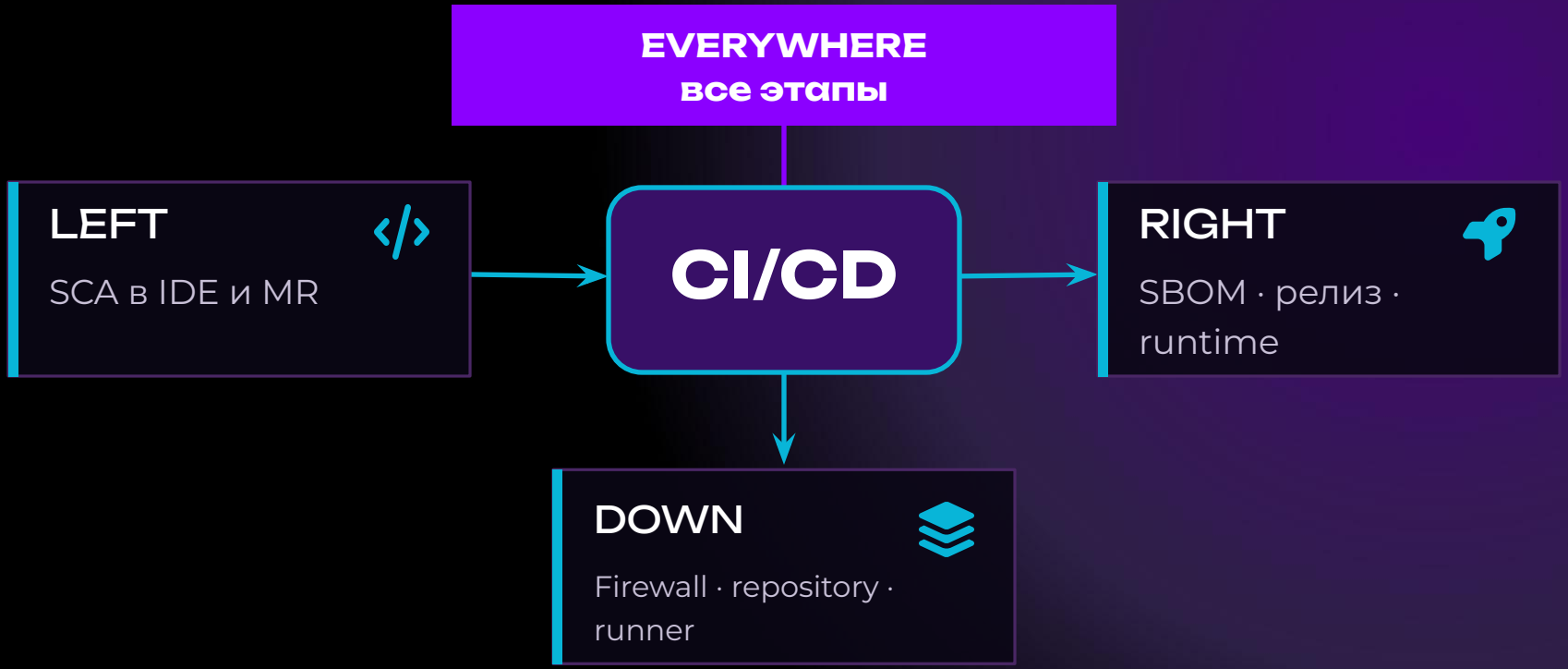
В рамках программы Patch the Planet
от OpenAI

GUARDCORP

Защита



Безопасность во всех направлениях



Три уровня защиты

GUARDCORE

OSA

Контроль поступающих пакетов
Допуск по политикам

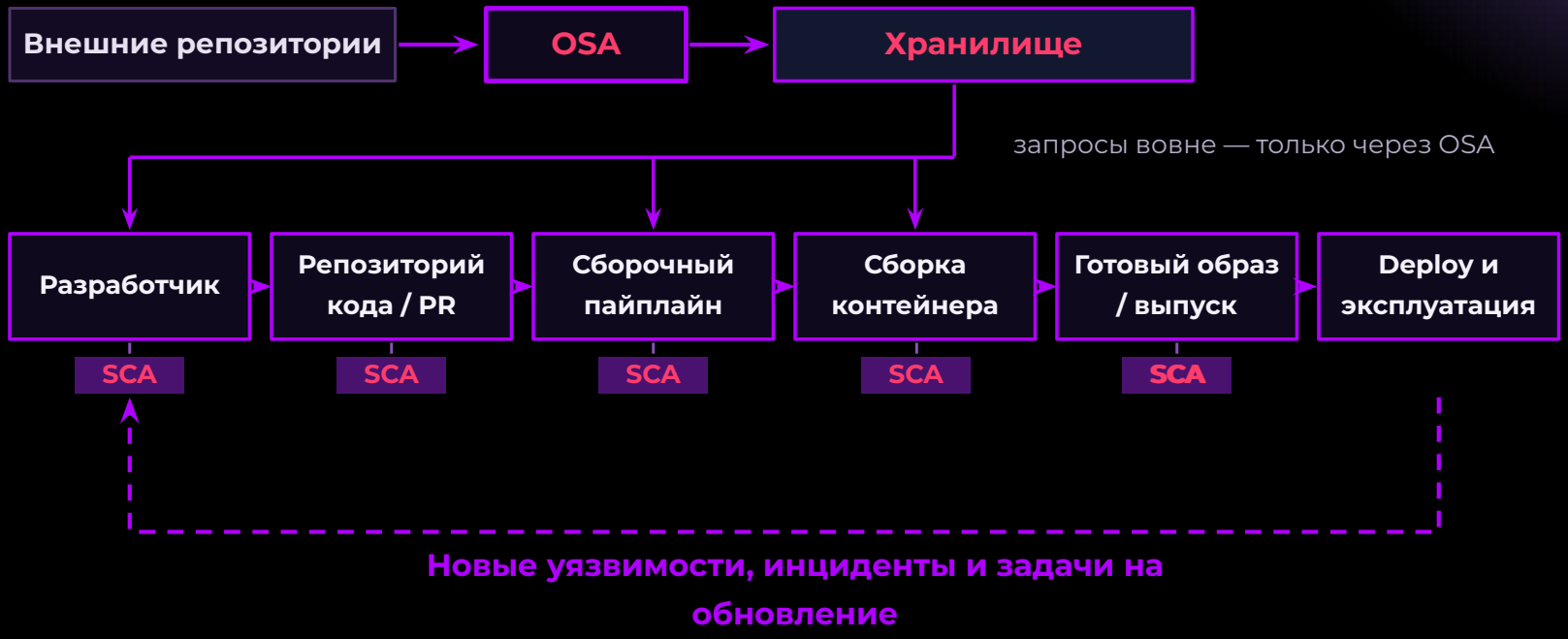
Repository

Доверенное хранение артефактов
Контролируемая выдача

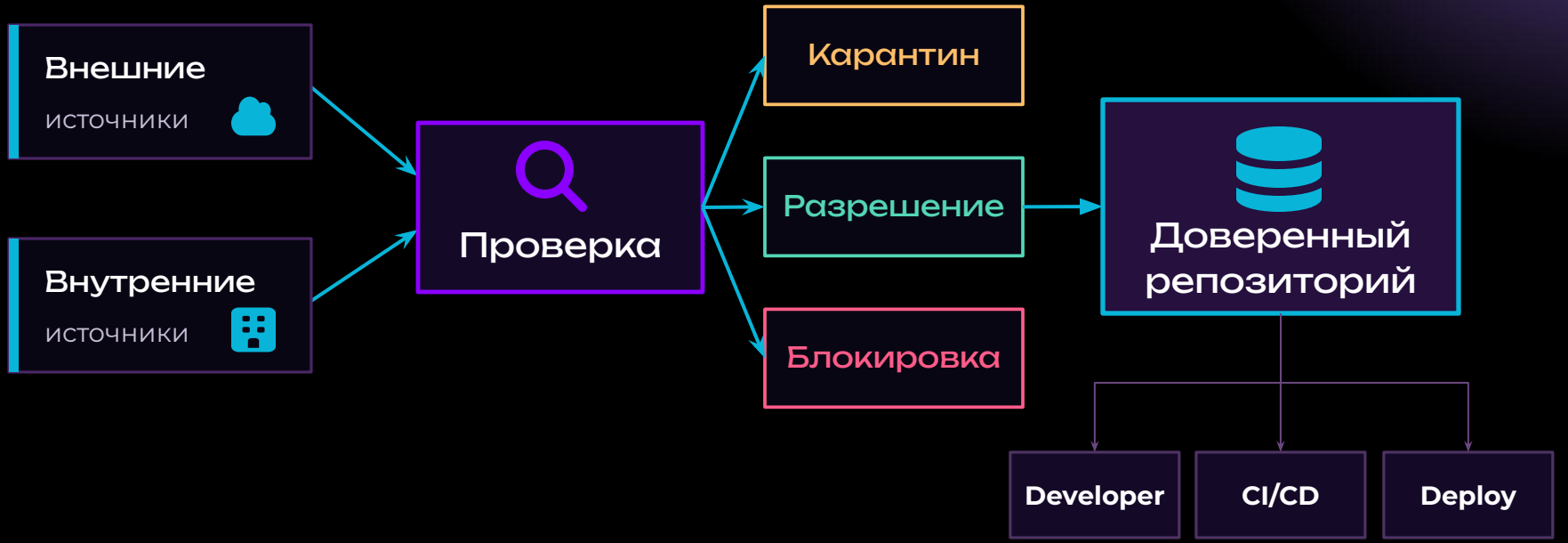
SCA + SBOM

Анализ зависимостей и состава
Инвентаризация и приоритеты

Контроли на этапах CI/CD



Доверенный репозиторий + OSA



OSA: без блокировки

GUARDCONF

Тупиковая блокировка

Запрос версии 1.2.x

↓

BLOCK

↓

Время на исправление

Управляемая альтернатива

Запрос версии 1.2.x

↓

Рекомендация: 1.2.3

↓

Lock-файл + сборка

Проверка до установки · разрешённая альтернатива · работа продолжается

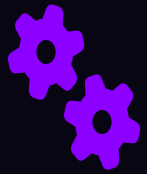
SCA на каждом этапе

GUARDCORP



IDE и MR

Новые зависимости
и изменения



CI/CD

Разрешённый граф
и артефакт

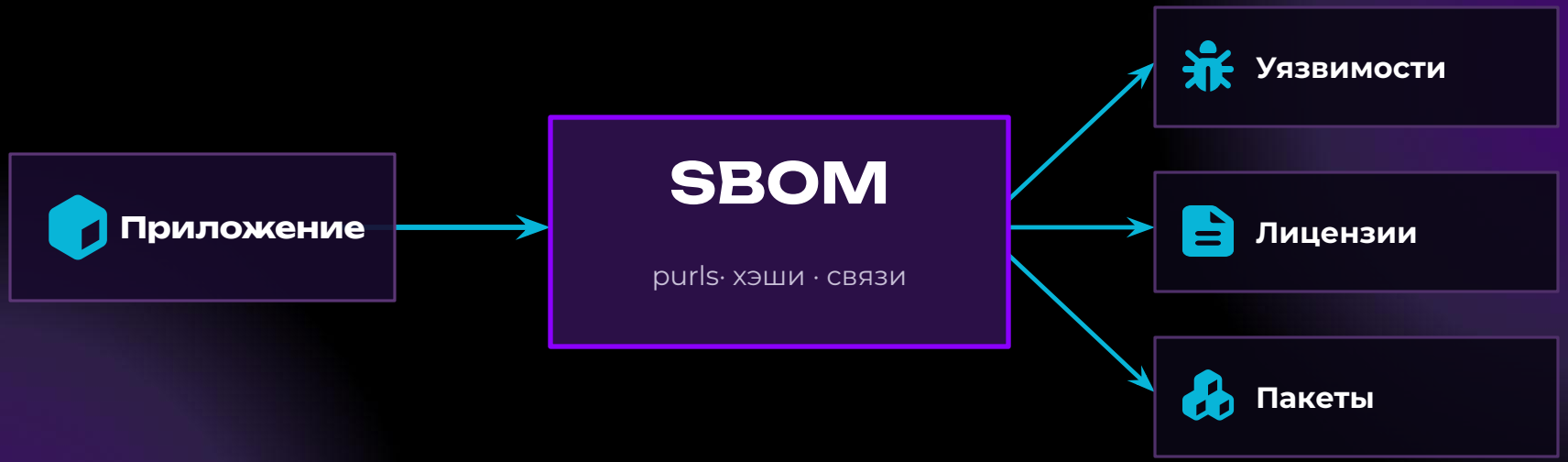


После релиза

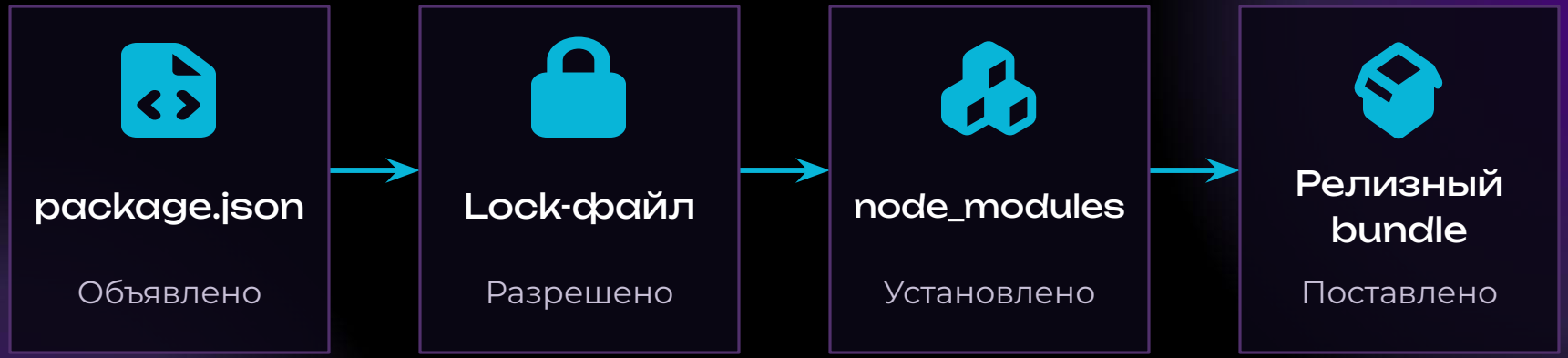
SBOM и новые
сведения об угрозах

Ранняя проверка · анализ собранного · повторная оценка

SBOM и инвентаризация



Манифест и реальный состав



Фактический состав зависит от окружения

Транзитивные зависимости

Экосистема	Зависимости	Директивные	Транзитивные	**Уязвимости** прямые / транзитивные
JavaScript	488	42	446	14 / 86
Java	90	54	36	34 / 66
C#	58	23	35	50 / 50
Python	39	16	23	42 / 58

аналитика CodeScoring за 2024 год

Базы знаний и сложности

GUARDCORE

Множество источников

- БДУ ФСТЭК, CVE.org, NVD, GitHub и многие другие

+ Нужна дедупликация и агрегация

Неточность данных

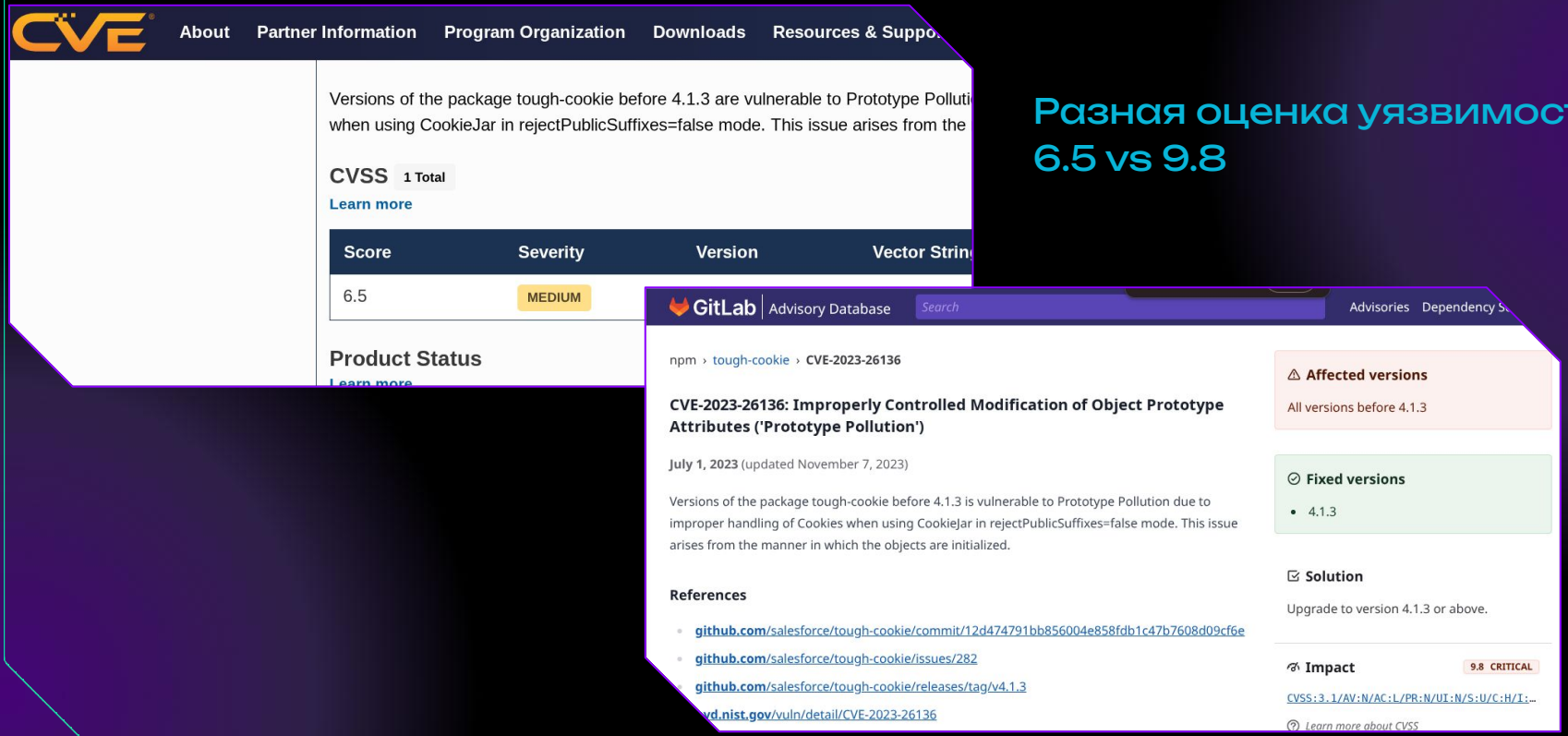
- Разные диапазоны версий, применимость, cpe/purl, False Positives

+ Нужно обогащение

Скорость обновления

+ Важно **быстро** получать актуальные данные

Пример проблем



Разная оценка уязвимости: 6.5 vs 9.8

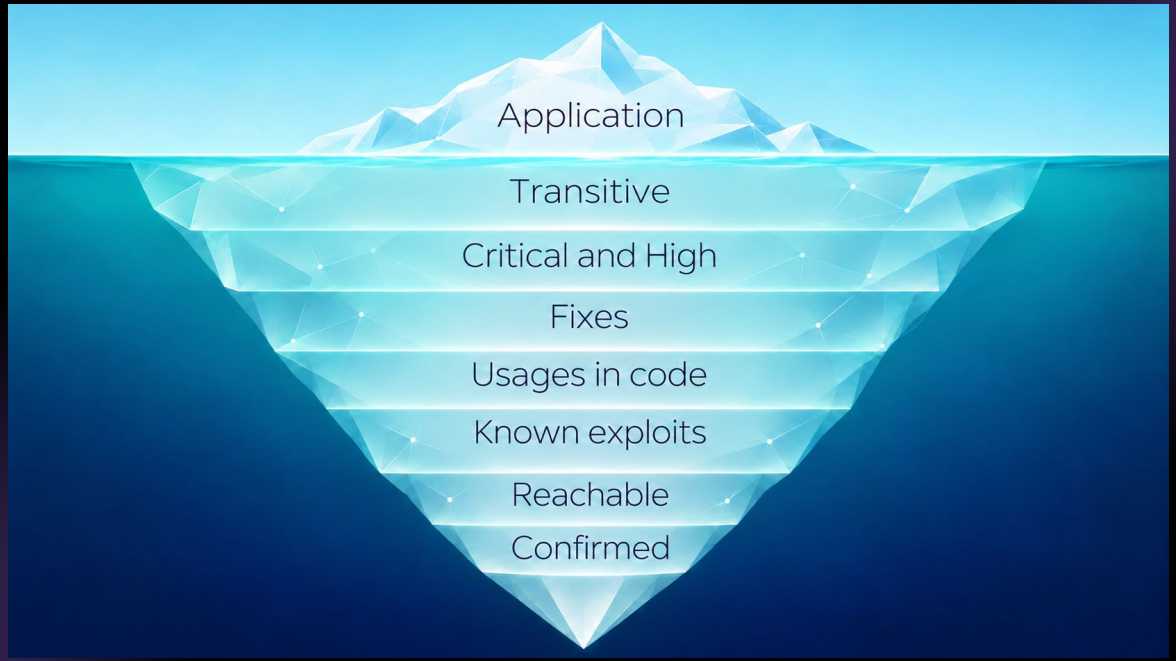
GUARDCORE



Результаты
Политики
Метрики

Воронка приоритетов

Малая часть на поверхности



Оценки и метрики

GUARDCORP

CVSS

Техническая оценка и предпосылки

EPSS

Прогноз эксплуатации в течение 30 дней

PoC / KEV

Рабочий пример и известная эксплуатация

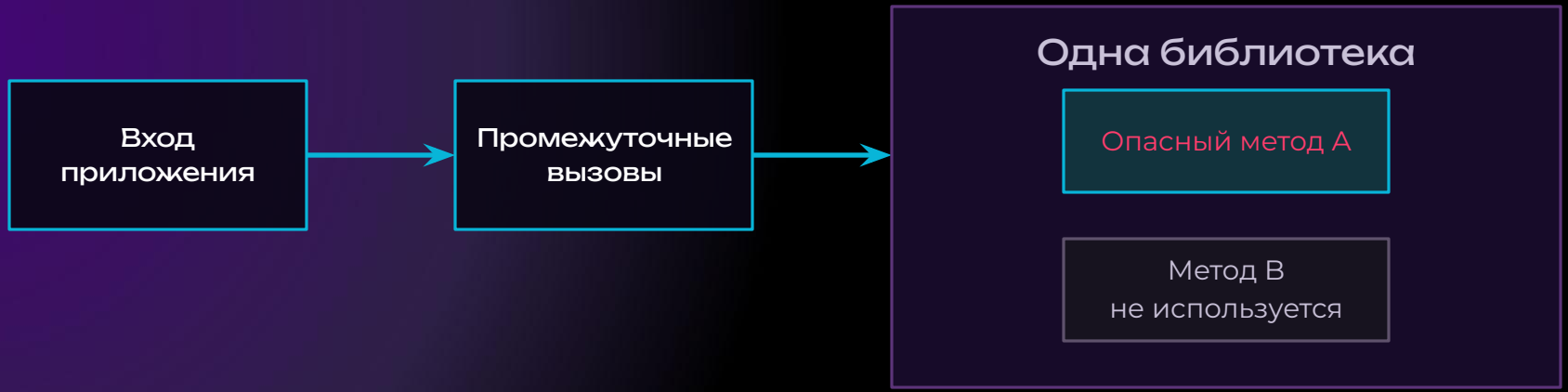
Анализ достижимости

GUARDCORE

Опасные методы

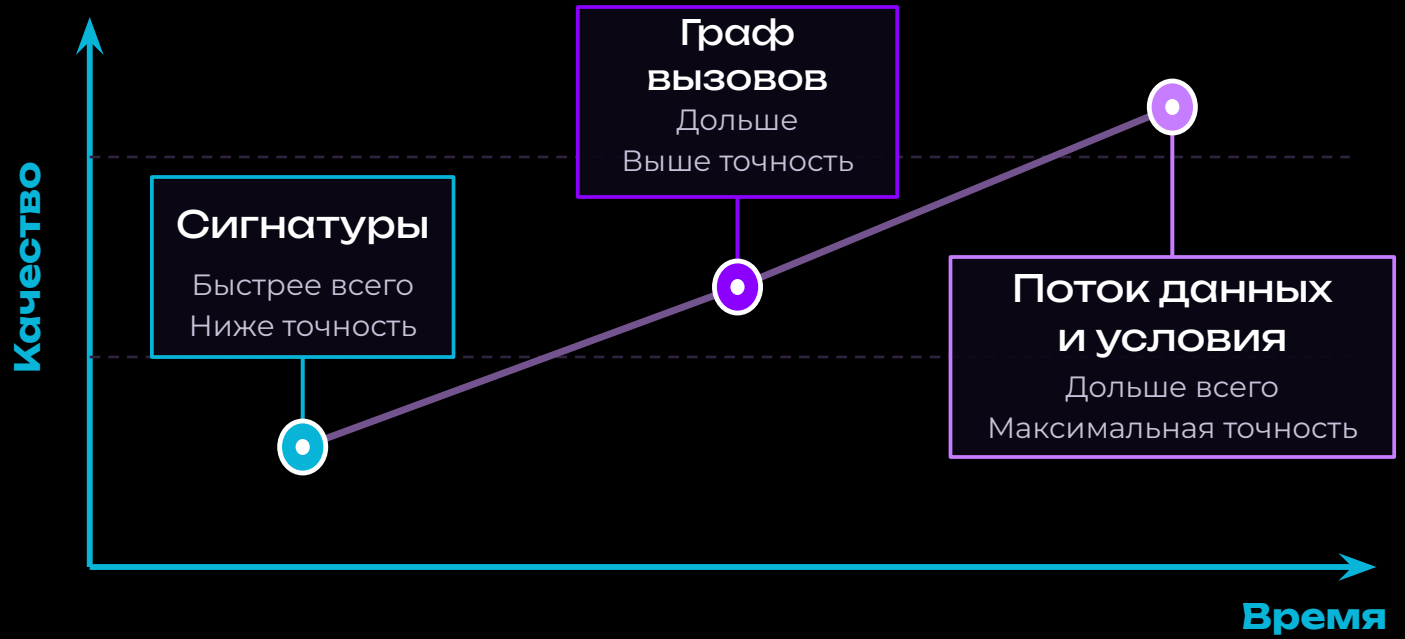
Пути до уязвимости

Приоритет используемого кода



Подтверждённый путь вызовов повышает приоритет триажа

Ограничения анализа достижимости



Виды достижимости

Отсутствие доказательств ≠ доказательство отсутствия

Политики и security gates

GUARDCORP

LEFT



Новая уязвимость

Warn: подсказать и исправить

DOWN



Вредоносный пакет

Block до установки

RIGHT



Риск готового релиза

Review / block по политике

EVERYWHERE



Согласованные исключения

Срок · владелец · аудит

Стандарты и регламенты

GUARDCORP



Нормы и стандарты

ГОСТ
ФСТЭК и НПА



Рекомендации

OWASP SAMM /
SCVS SLSA



Внутренние правила

Политики
и регламенты

Непрерывная защита компонентов

GUARDCORP

- Поступление компонентов
- Весь граф зависимостей
- Повторная оценка угроз
- Политики и метрики



LEFT · DOWN · RIGHT → EVERYWHERE

Пасхалка

Знаки везде



Ссылки

GUARDCORE

CodeScoring

Youtube

VK Video

Habr

GUARDCORE

Спасибо за внимание!

t.me/@parazero5

