СВД
Встраиваемые
Системы

Использование инструментов композиционного анализа для контроля комплектности продуктов

Зворыгин Александр

Техник-программист группы разработки СЗИ

План доклада

- Термины
- Утилиты
- Реализация
- Проблемы

Термины

Композиционный анализ — процесс выявления уязвимостей в Open Source компонентах системы

SBOM — Software Bill of Materials представляет собой перечень зависимостей, файлов, библиотек и других элементов, имеющих отношение к системе

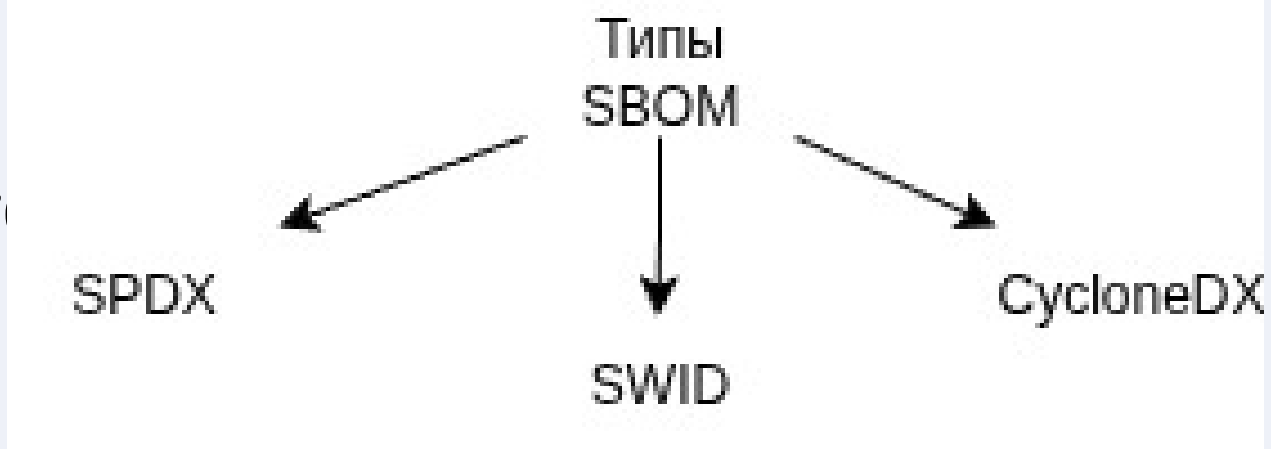
Термины

Типы SBOM файлов

SPDX — международный стандарт, поддерживаемый Linux Foundation

SWID — стандарт соответствующий ISO/IEC 1977 2:2015

CycloneDX — наиболее легковесный стандарт, поддерживаемый ФСТЭК



Утилиты для генерации SBOM файла

cdxgen

Trivy

Утилиты

Для минимального анализа необходимо определить тип компонента, его имя, версию и идентификатор в пакетной системе

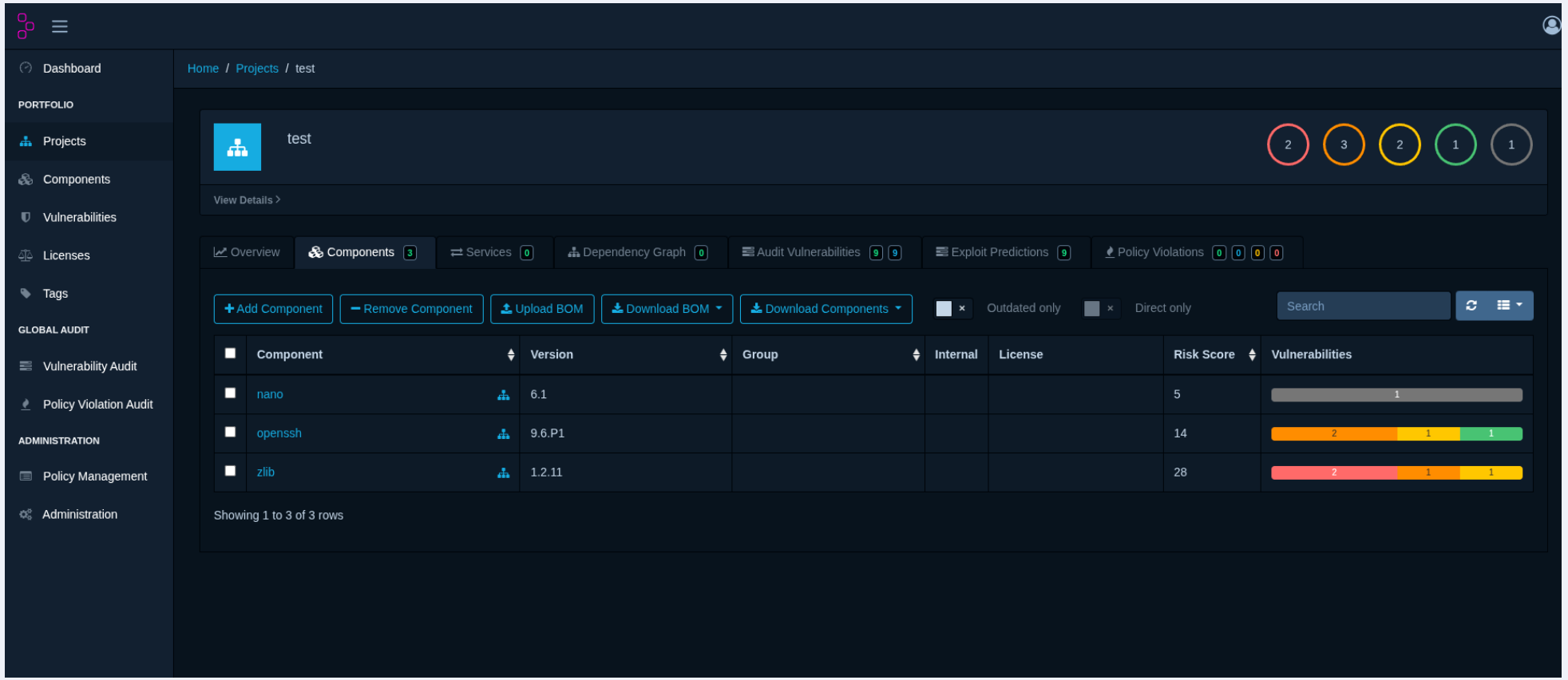

```
{
  "bomFormat": "CycloneDX",
  "specVersion": "1.6",
  "version": 1,
  "components": [
    {
      "type": "library",
      "name": "zlib",
      "version": "1.2.11",
      "purl": "pkg:pacman/zlib@1.2.11?arch=x86"
    },
    {
      "type": "service",
      "name": "openssh",
      "version": "9.6.P1",
      "purl": "pkg:pacman/openssh@9.6.P1?arch=x86"
    },
    {
      "type": "application",
      "name": "nano",
      "version": "6.1",
      "purl": "pkg:pacman/nano@6.1?arch=x86"
    }
  ]
}
```

Утилиты

Dependency Track

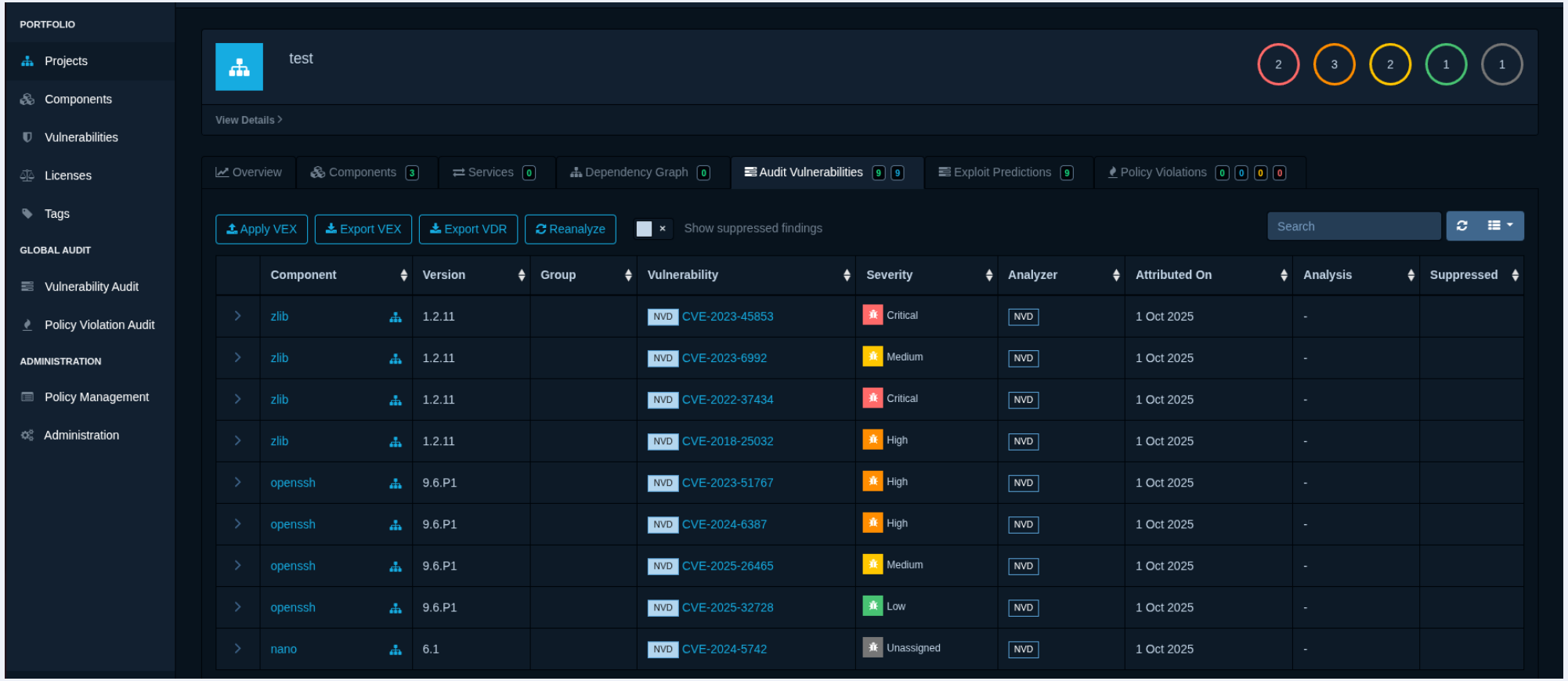
Утилиты

Dependency Track



Утилиты

Dependency Track



Утилиты

- **Cve-bin-tool**

cve-bin-tool --detailed --sbom cyclonedx --sbom-file sbom.json -f html -o out

Утилиты

cve-bin-tool

CVE Binary Tool — Descriptive Report — 03 Oct 2025 — Print Mode

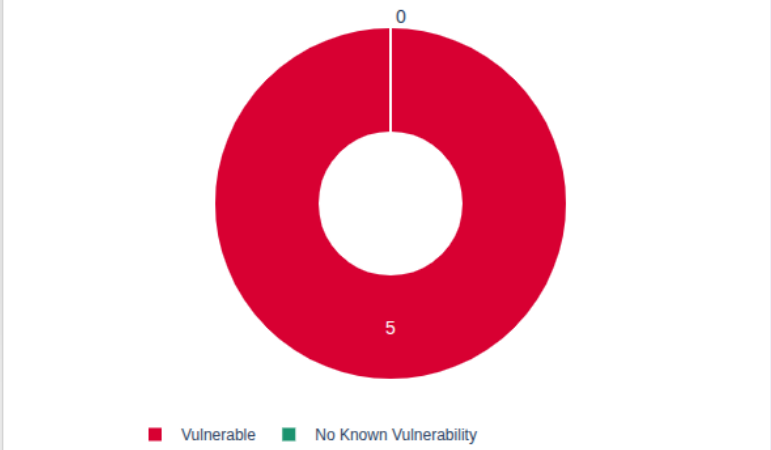
CVE Summary

Severity	Count
CRITICAL	3
HIGH	4
MEDIUM	2
LOW	1

CVE Remarks

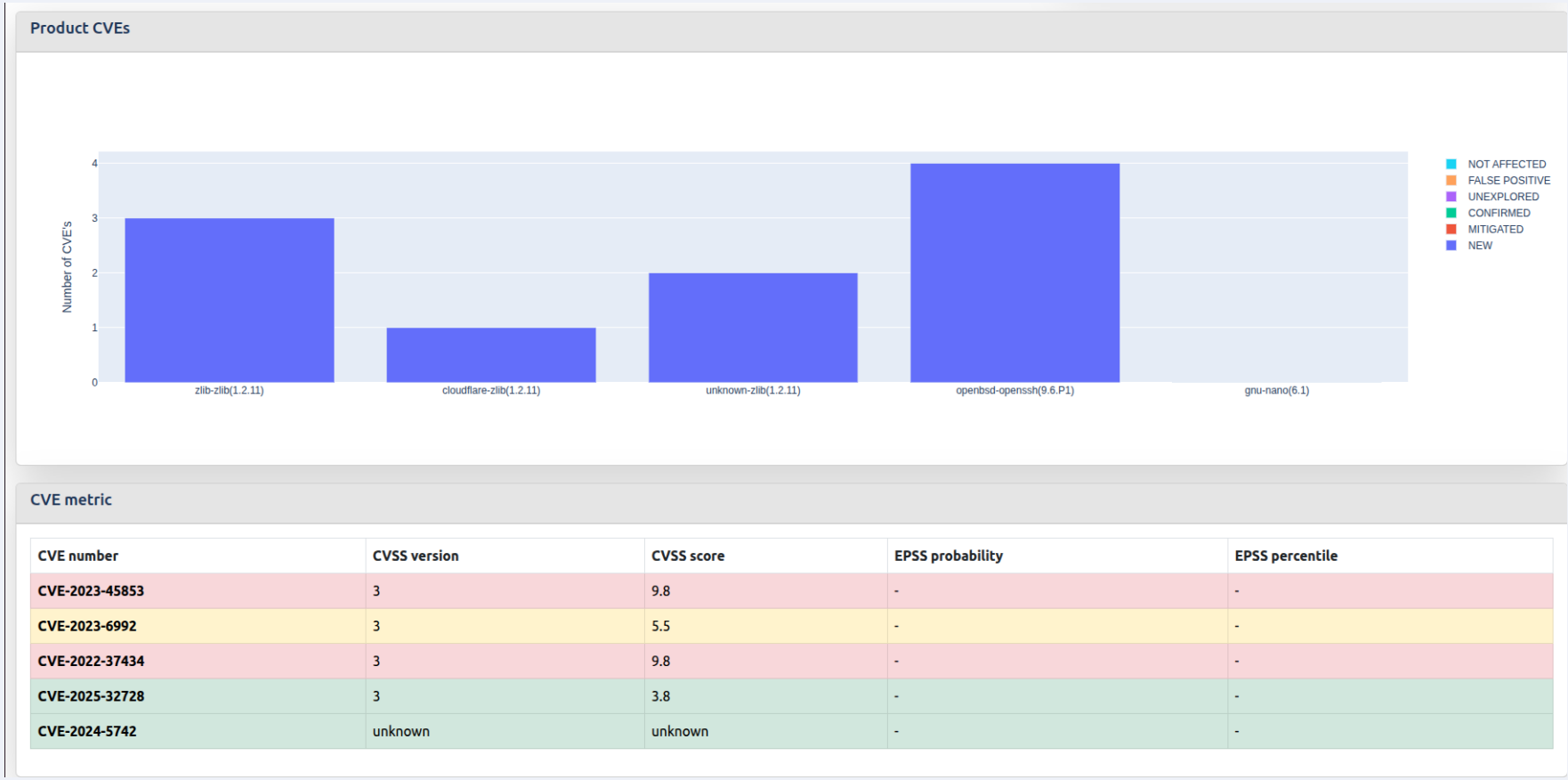
Remark	Count
NEW	11
CONFIRMED	0
MITIGATED	0
UNEXPLORED	0
FALSE POSITIVE	0
NOT AFFECTED	0

Scanned Files: 5 Vulnerable Files: 5



Утилиты

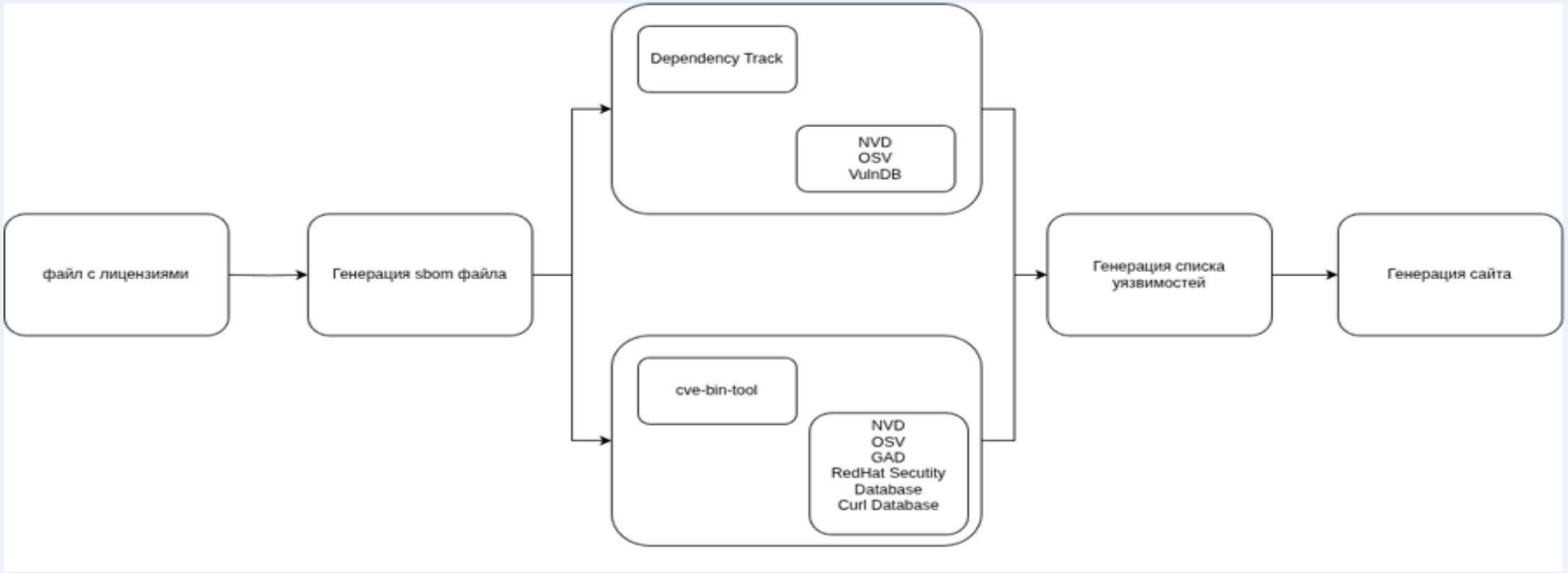
cve-bin-tool



CVE metric

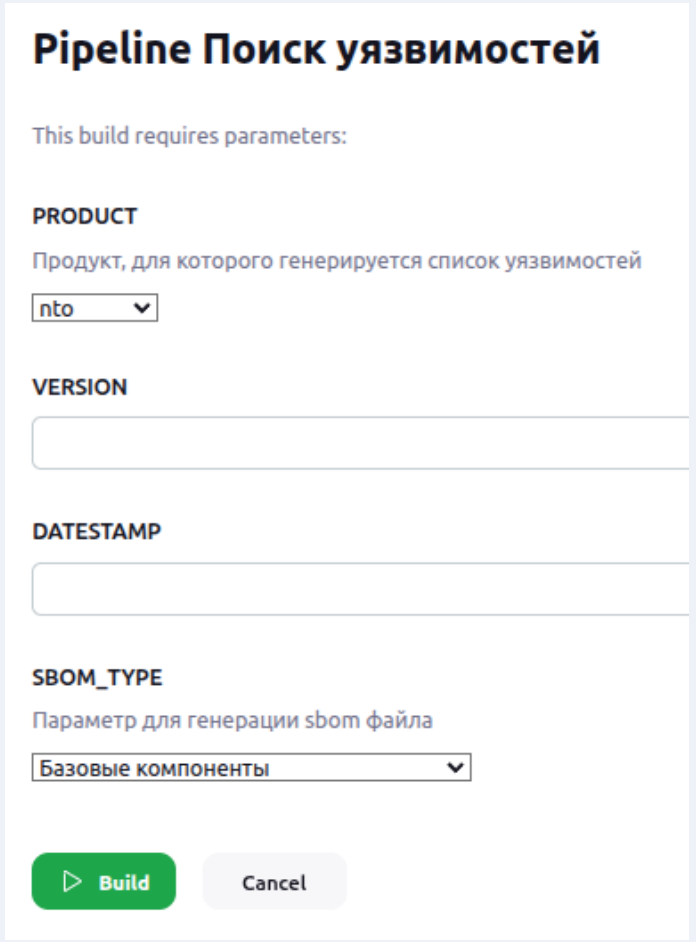
CVE number	CVSS version	CVSS score	EPSS probability	EPSS percentile
CVE-2023-45853	3	9.8	-	-
CVE-2023-6992	3	5.5	-	-
CVE-2022-37434	3	9.8	-	-
CVE-2025-32728	3	3.8	-	-
CVE-2024-5742	unknown	unknown	-	-

Реализация


Dependency Track
NVD
OSV
VulnDB
файл с лицензиями
Генерация sbom файла
Генерация списка уязвимостей
Генерация сайта
cve-bin-tool
NVD
OSV
GAD
RedHat Secutity Database
Curl Database

Реализация

- **Параметры для основного скрипта**



Реализация

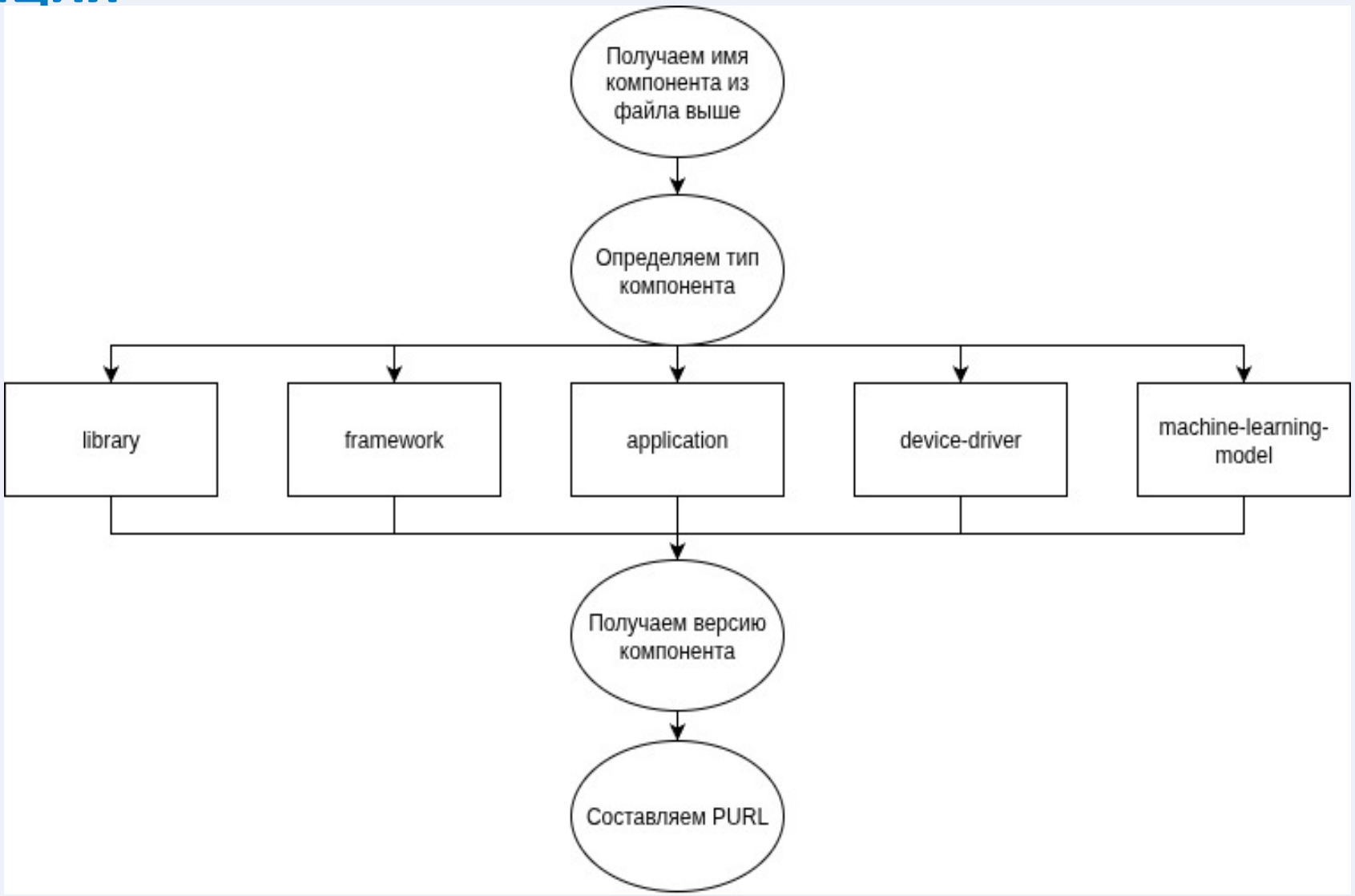
- 1 этап — парсинг

```
zlib :: ZLIB license :: A Massively Spiffy Yet Delicately Unobtrusive Compression Library (ZLIB license) :: 1.2.11
```

- 2 этап — генерация SBOM


```
{
  "bomFormat": "CycloneDX",
  "specVersion": "1.6",
  "version": 1,
  "components": [
    {
      "type": "library",
      "name": "zlib",
      "version": "1.2.11",
      "purl": "pkg:pacman/zlib@1.2.11?arch=x86"
    }
  ]
}
```

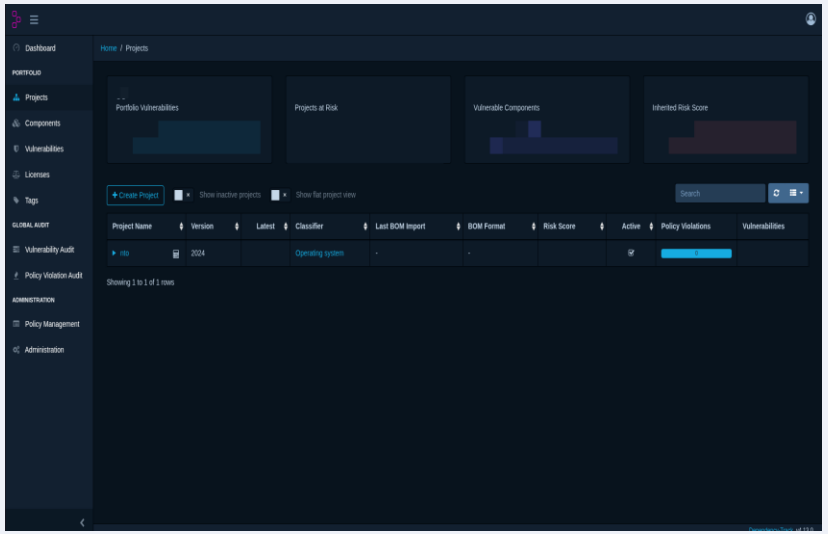
Реализация



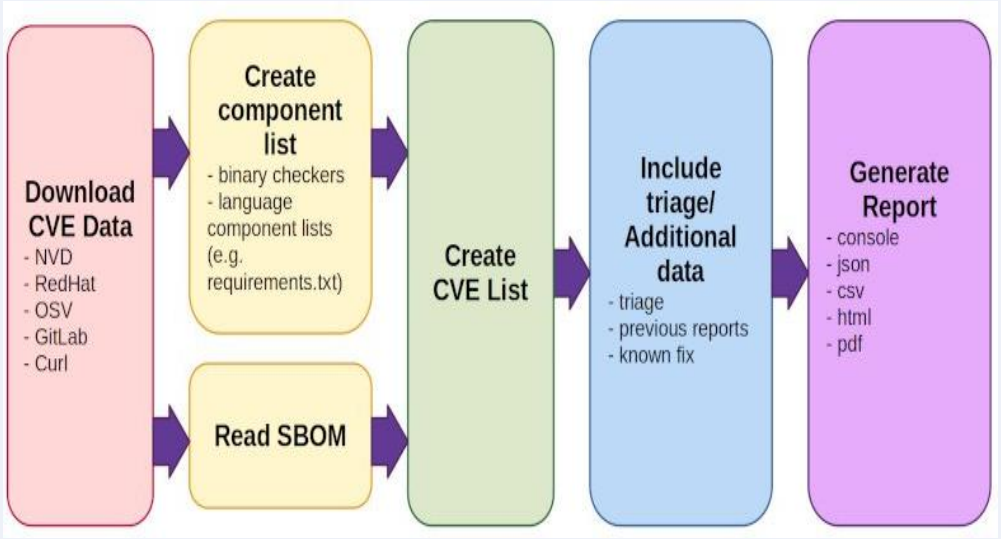

```
"pkg:pacman/zlib@1.2.11?arch=x86"
```

Реализация

3 этап — анализ SBOM



Dependency Track



Cve-bin-tool

Реализация

- **Этап 3.1 Dependency Track**

  1. Получить список проектов

  http://localhost:8081/api/v1/project

  2. Загрузить SBOM в нужный

  http://localhost:8081/api/v1/bom/?{project-id}

  3. Скачать список уязвимостей

  http://localhost:8081/api/v1/finding/project/{project-id}/export

Реализация

Этап 3.2 cve-bin-tool

cve-bin-tool --detailed --sbom cyclonedx --sbom-file sbom.json -f json -o out

_

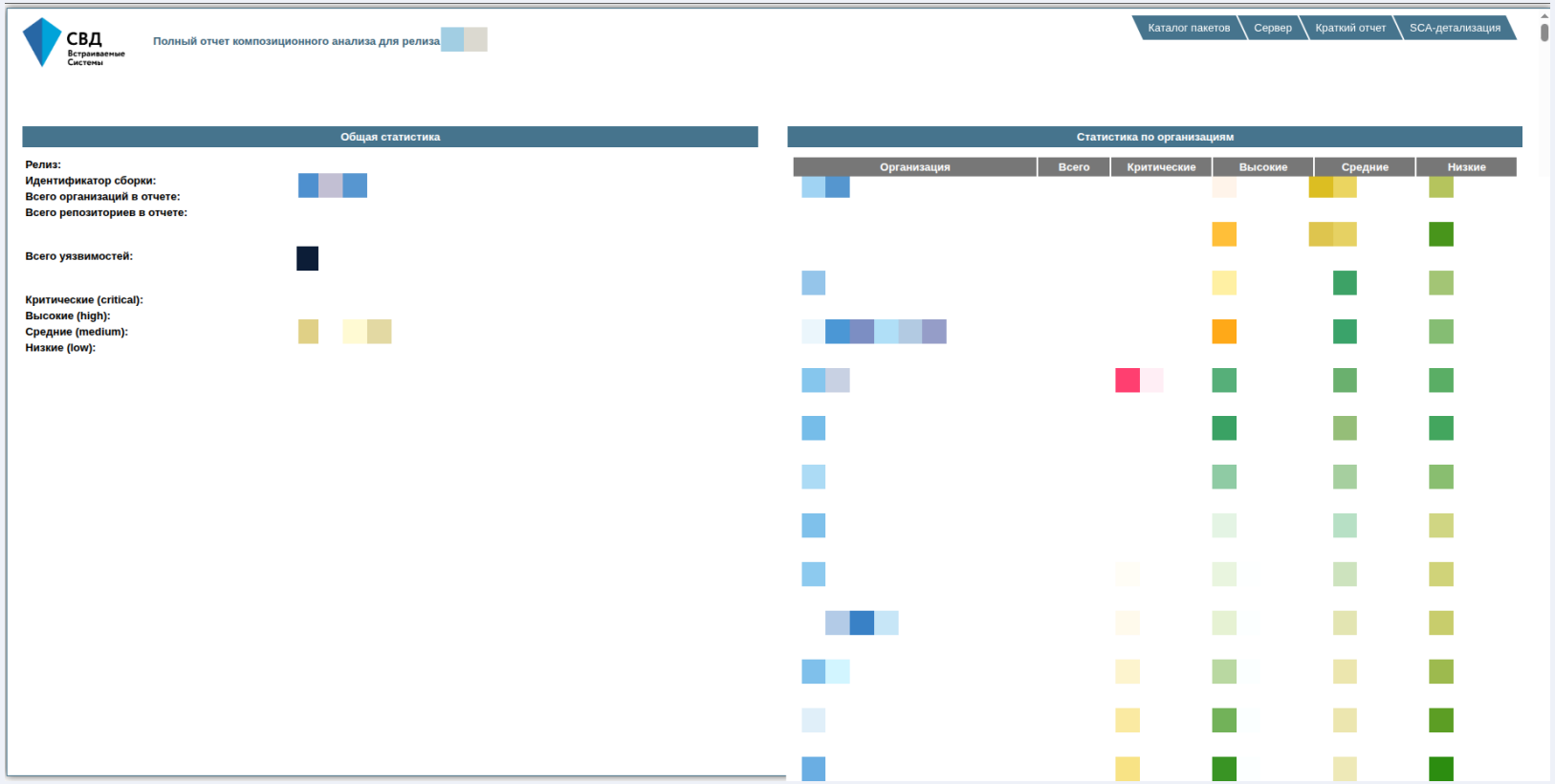
Реализация

- 4 этап — генерация списка уязвимостей


```
{
  "name": "zlib"
},
{
  "version": [
    {
      "1.2.11": {
        "vuln": [
          {
            "CVE-2023-45853": [
              "CRITICAL",
              "MiniZip in zlib through 1.3 has an integer overflow and resultant heap-based buffer overflow in zipOpenNewFileInZip4_64 via a long filename
            ]
          },
          {
            "CVE-2023-6992": [
              "MEDIUM",
              "Cloudflare version of zlib library was found to be vulnerable to memory corruption issues affecting the deflation algorithm implementation
            ]
          },
```

Реализация

5 этап — генерация отчета



Проблемы

- **Непонятные пакеты**
  - Решение: сборка в закрытом контуре
- **Сложность ручной проверки**
  - Решение: автоматизация всего
- **Совпадение имен пакетов с именами Open Source компонентов**
  - Решение: написали правила, которые позволяют отличать компоненты

СВД
Встраиваемые
Системы

Спасибо за внимание!

Зворыгин Александр

Техник-программист группы разработки СЗИ

a.zvorygin@kpda.ru

+79043549531