Что в образе тебе моём?

Анатолий Карпенко

Luntry

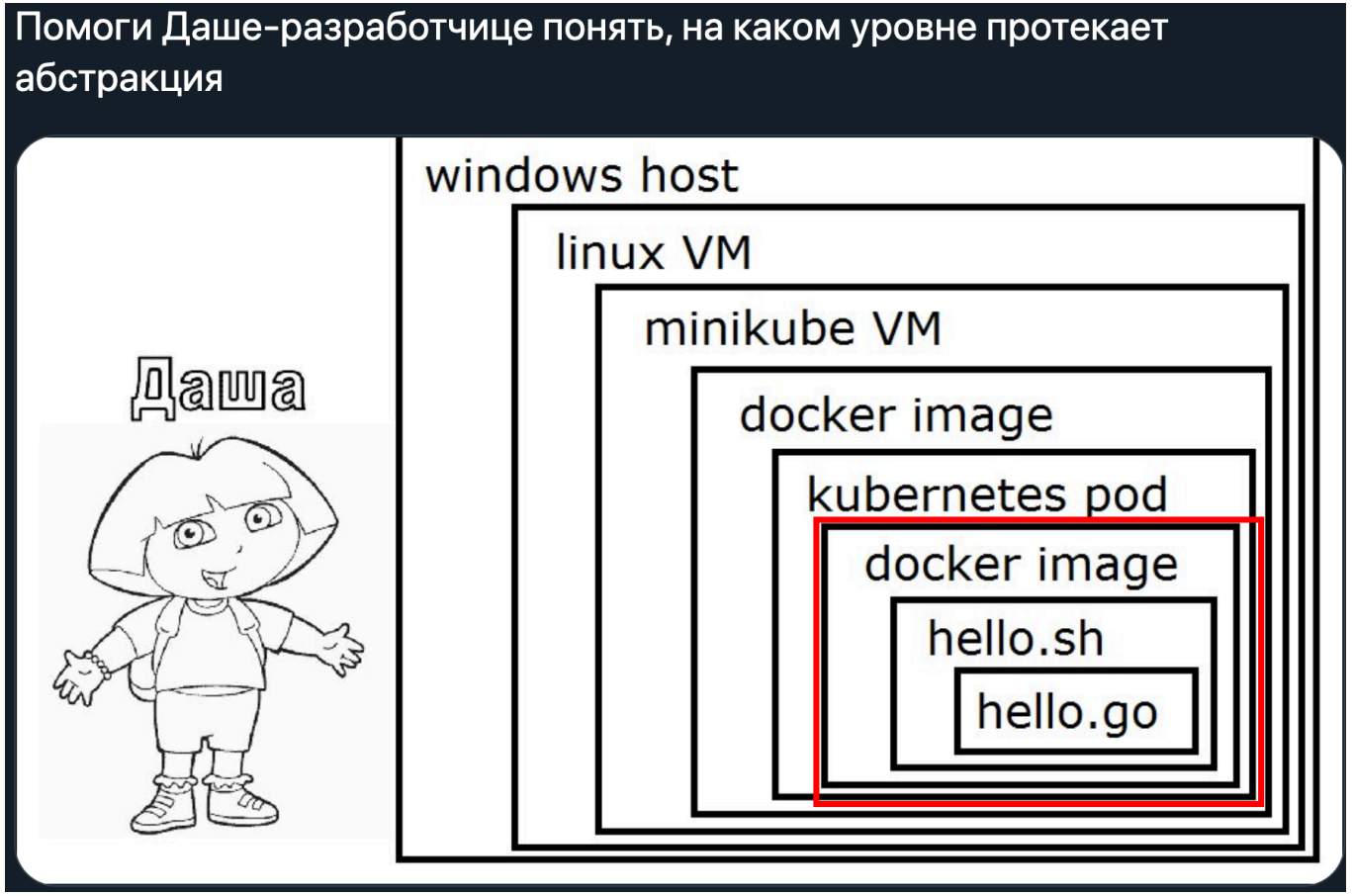
whoami

- Автоматизатор автоматизации в Luntry
- Любитель митапошных форматов; SPb Reliability Meetup, ITGM, TechTrain, DevOops, DEFCON'ы, SafeCode, БЕКОН, ТБ Форум, UDW
- Веду канал «Технологический Болт Генона»
- Рисую несмешные мемы

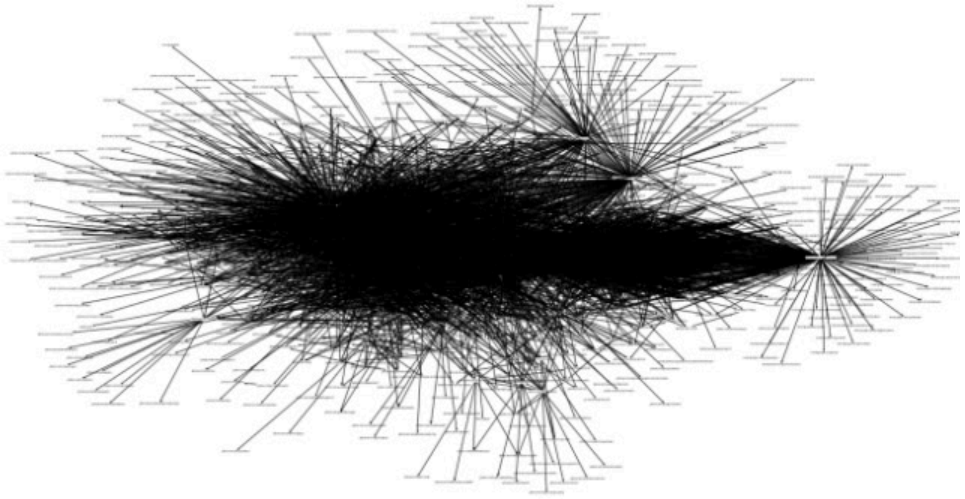
Кто пользовался Trivy, Grype и прочими сканерами docker-образов?

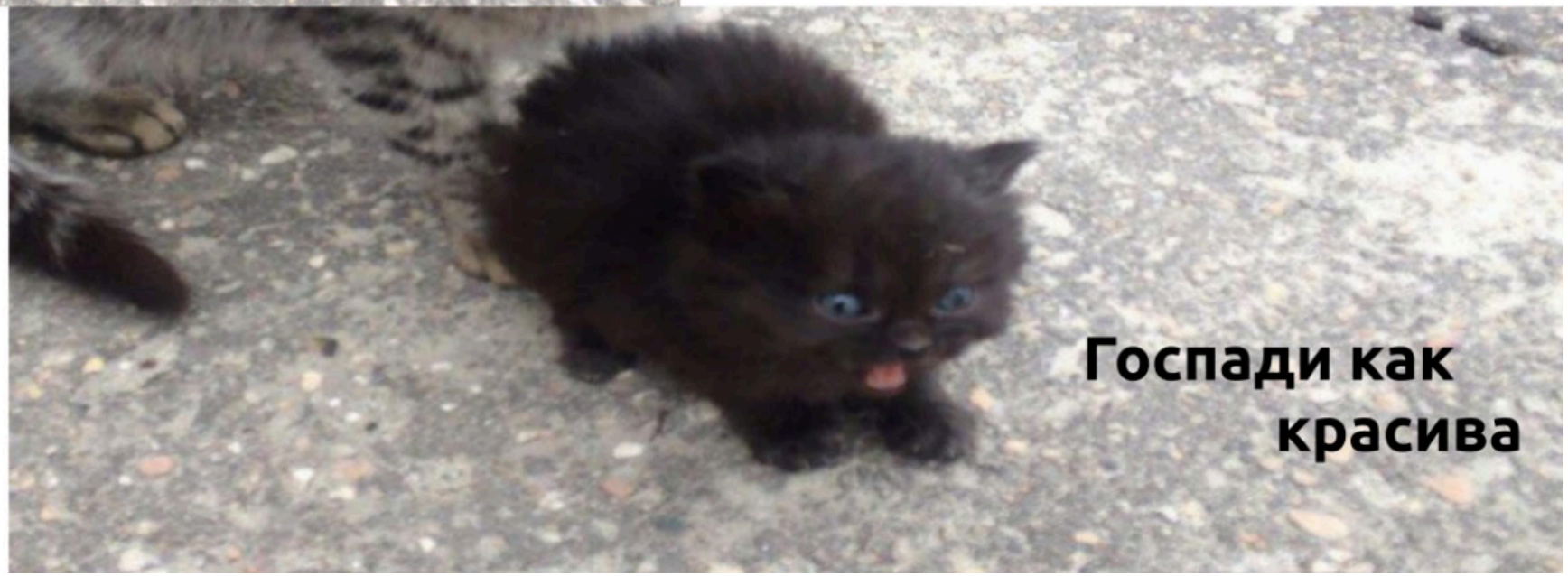
Приложение сейчас

Помоги Даше-разработчице понять, на каком уровне протекает абстракция




Сматри, джун, ето граф
зависимостей пакетов
нашева сервиса

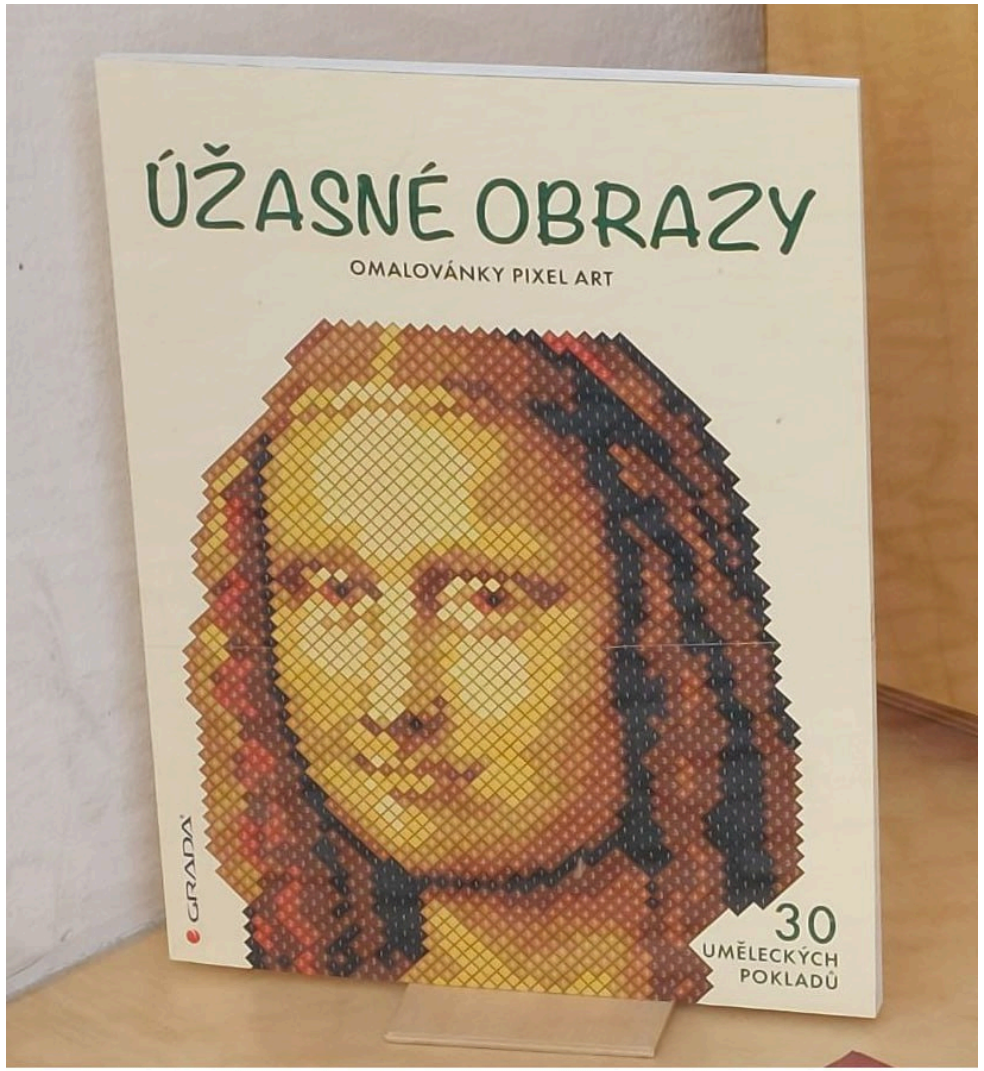



Госпади как
красива


PO: 0510268632
WMIT: 263304459
6057
Сторонние компоненты
ваши компоненты
0 00 12345 67890 5

Что нас интересует

- Анализ Dockerfile на лучшие практики
- Компонентный анализ
- Анализ на известные уязвимости
- Поиск чувствительной информации
- Анализ на вредоносный код



Про твои образы Docker написали книгу

Зачем это нужно?

- Процессы (внутренние регламенты, CI/CD и т.д.)

Зачем это нужно?

- Процессы (внутренние регламенты, CI/CD и т.д.)
- Регуляторика

Зачем это нужно?

- Процессы (внутренние регламенты, CI/CD и т.д.)
- Регуляторика
- Исследования

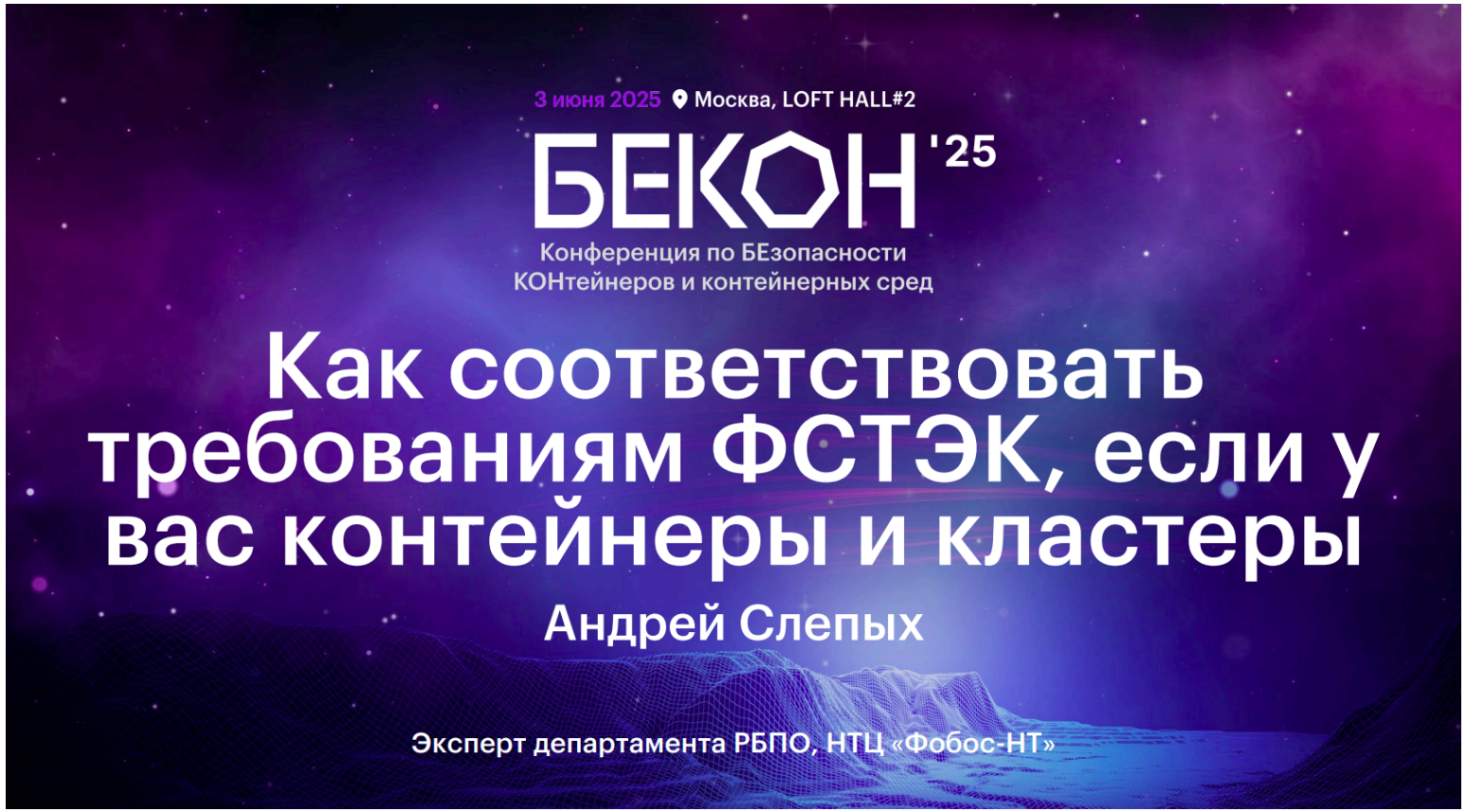
Зачем это нужно?

- Процессы (внутренние регламенты, CI/CD и т.д.)
- Регуляторика
- Исследования
- Bug Bounty
- ...

Регуляторика

- Проект национального стандарта ГОСТ Р Защита информации. Разработка безопасного программного обеспечения. Композиционный анализ программного обеспечения. Общие требования
- О повышении безопасности средств защиты информации, в состав которых разработчики включают средства контейнеризации или образы контейнеров
- ГОСТ Р 56939-2024 Разработка безопасного программного обеспечения. Общие требования

Как соответствовать требованиям ФСТЭК

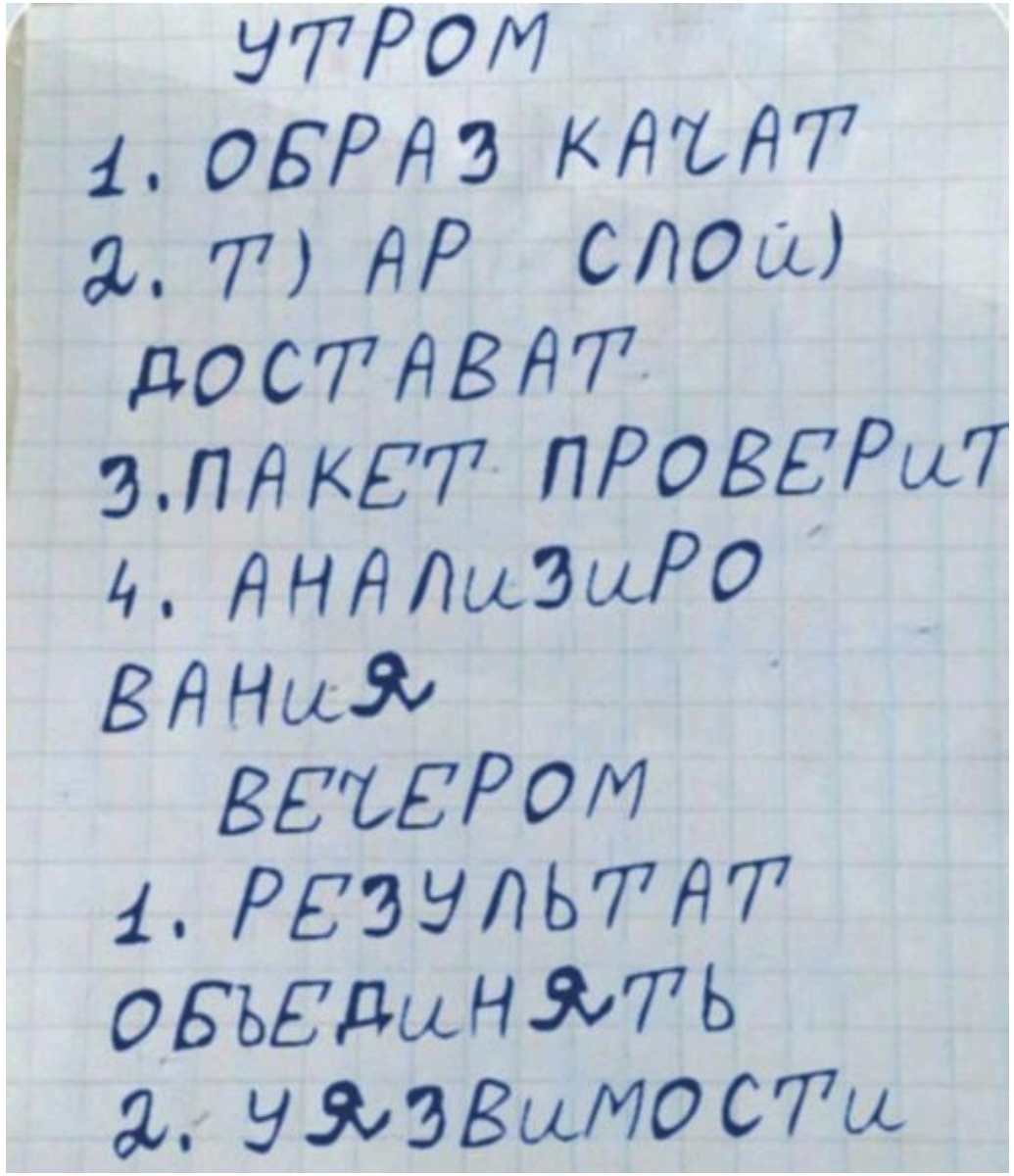


https://vkvideo.ru/video-224467080_456239058

Давайте разбираться!

Как работают сканеры образов

- Скачивается образ
- Послойный анализ
  - Извлечение tar-ов
  - Проверка путей пакетов
  - ...
- Объединение результатов анализа
- Сканирование на уязвимости



Container Image Layers and Container Image Scanning Explained

Пример - слои (1)

```
$ cat key.api
-----BEGIN OPENSSH PRIVATE KEY-----
. . .
MaCaMNBWiWMSGrOMDHi. . .3NTc3AQIDBAUG
-----END OPENSSH PRIVATE KEY-----
```

```
$ cat Dockerfile

FROM busybox:latest

COPY key.api .
RUN rm key.api
```

```
$  docker build -t secrets-test .
```

Пример - слои (2)

```
$ docker save secrets-test:latest | tar -x -C .
```

```
$ find blobs/sha256/ -type f -exec file {} \; | grep "tar"
blobs/sha256/80e840...e6bf5a: POSIX tar archive (GNU)
blobs/sha256/946040...e1fcad: POSIX tar archive
blobs/sha256/b00389...f17b98: POSIX tar archive
```

```
$ tar xvf blobs/sha256/b00389...f17b98
key.api
```

```
$ cat key.api
-----BEGIN OPENSSH PRIVATE KEY-----
. . .
MaCaMNBWiWMSGrOMDHi. . .3NTc3AQIDBAUG
-----END OPENSSH PRIVATE KEY-----
```

SBOM (1)

> Software Bill of Materials — перечень модулей и библиотек, необходимых для сборки и работы ПО, а также их связи друг с другом

- SPDX (Linux Foundation)
- CycloneDX (OWASP)
- SWID (ISO/IEC 19770-2:2015)


```
{
  "$schema": "http://cyclonedx.org/schema/bom-1.6.schema.json",
  "bomFormat": "CycloneDX",
  "specVersion": "1.6",
  "serialNumber": "urn:uuid:48e5b3ed-8340-4972-963f-c1669149b091",
  "version": 1,
  "metadata": {
    "timestamp": "2026-04-09T12:04:48+00:00",
    "tools": {
      "components": [
        {
          "type": "application",
          "manufacturer": {
            "name": "Aqua Security Software Ltd."
          },
          "group": "aquasecurity",
          "name": "trivy",
          "version": "0.69.3"
        }
      ]
    },
    "component": {…
    }
  },
  "components": […
  ],
  "dependencies": […
  ],
  "vulnerabilities": []
}
```

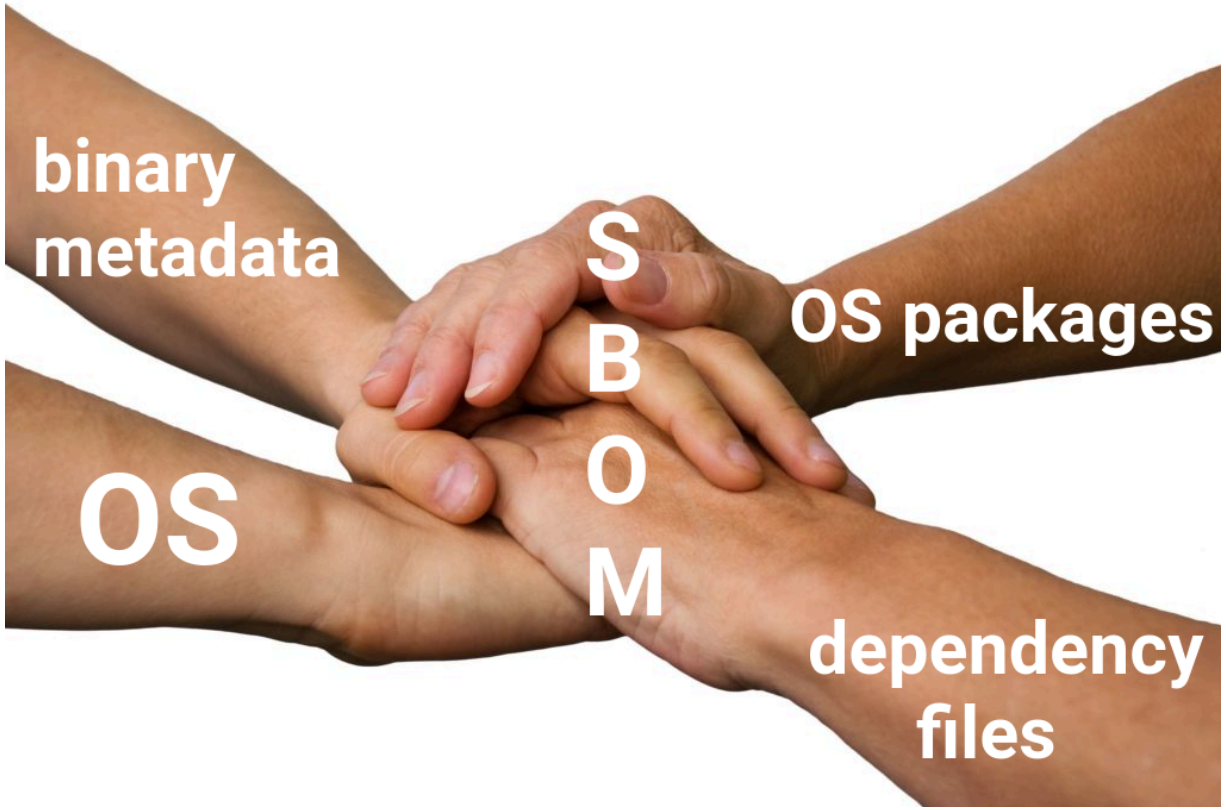
SBOM (2)

```
{
  "bom-ref": "pkg:golang/github.com/beorn7/perks@
                                  v1.0.1?type=module",
  "type": "library",
  "name": "github.com/beorn7/perks",
  "version": "v1.0.1",
  "scope": "required",
  "hashes": [
    {
      "alg": "SHA-256",
      "content": "565...b0e3"
    }
  ],
  "purl": "pkg:golang/github.com/beorn7/perks@
          v1.0.1?type=module&goos=linux&goarch=amd64",
  "externalReferences": [
    {
      "url": "https://github.com/beorn7/perks",
      "type": "vcs"
    }
  ]
},
```

```
{
  "bom-ref": "pkg:deb/debian/base-files@
            13.8%2Bdeb13u3?arch=amd64&distro=debian-13.3",
  "type": "library",
  "supplier": {
    "name": "Santiago Vila <sanvila@debian.org>"
  },
  "name": "base-files",
  "version": "13.8+deb13u3",
  "licenses": [
    {
      "license": {
        "id": "GPL-2.0-or-later"
      }
    },
    {
      "license": {
        "name": "verbatim"
      }
    }
  ],
  "purl": "pkg:deb/debian/base-files@
            13.8%2Bdeb13u3?arch=amd64&distro=debian-13.3",
  "properties": [
    . . .
  ]
},
```

Откуда собирается информация

- Информация об ОС
- Информация о пакетах ОС
- Зависимости
- Метаданные из бинарных файлов



Информация об ОС

- /etc/os-release
- /usr/lib/os-release
- /etc/lsb-release
- /etc/issue
- /etc/alpine-release
- /etc/secfixes.d/alpine

```
# cat /etc/os-release
NAME="CentOS Stream"
VERSION="10 (Coughlan)"
ID="centos"
ID_LIKE="rhel fedora"
VERSION_ID="10"
PLATFORM_ID="platform:el10"
...
```

```
# cat /etc/issue
Ubuntu Resolute Raccoon
        (development branch) \n \l
```

```
cat /etc/alpine-release
3.23.3
```

Информация о пакетах

- Alpine
  - /etc/apk/
  - /lib/apk/
- Ubuntu/Debian
  - /var/cache/apt/archives
  - /var/lib/dpkg/*
  - /var/lib/apt/*
  - /var/log/dpkg.log
- Redhat
  - /var/cache/yum/
  - /var/lib/rpm/

```
# cat /var/lib/dpkg/status \
                  | grep 'Package:'
Package: apt
Package: base-files
...
Package: ubuntu-keyring
Package: zlib1g
```

```
# cat /lib/apk/db/installed \
                    | grep 'P:'
P:alpine-baselayout
P:alpine-baselayout-data
...
P:musl
P:musl-utils
P:scanelf
P:ssl_client
P:zlib
```

Зависимости

- JS/TS
  - package.json / package-lock.json
  - yarn.lock
- Python
  - requirements.txt
  - pyproject.toml / poetry.lock
  - uv.lock / pipfile.lock
- Ruby
  - Gemfile.lock
- Java
  - pom.xml
  - build.gradle
- PHP
  - composer.json
- Rust
  - Cargo.toml / Cargo.lock
- Go
  - go.mod

Метаданные из бинарных файлов

- go version -m ./go-binary
- cargo audit bin ./rust-binary
- blint
- ...

```
$ cargo audit bin ~/.cargo/bin/*
Crate:     paste
Version:   1.0.15
...
ID:        RUSTSEC-2024-0436
URL:       https://rustsec.org/advisories/RUSTSEC-2024-0436
Dependency tree:
paste 1.0.15
└── rmp 0.8.14
    └── rmp-serde 1.3.0
        └── askalono 0.5.0
            └── cargo-about 0.8.2
```

```
$ blint sbom -i /usr/bin/ping --deep
                && jq . reports/sbom-binary-postbuild.cdx.json | grep 'bom-ref'
      "bom-ref": "pkg:generic/ping",
      "bom-ref": "pkg:file/libc.so.6",
      "bom-ref": "pkg:file/libcap.so.2",
      "bom-ref": "pkg:file/libidn2.so.0",
      "bom-ref": "pkg:generic/gnu/libc@2.11?hash=110530961",
      . . .
      "bom-ref": "pkg:generic/gnu/libc@2.4?hash=225011988",
      "bom-ref": "pkg:generic/idn2@0.0.0?hash=136825856",
```

Метаданные из бинарных файлов (go example)

```
$ go build
```

```
$ go version -m ./golang-example-app | grep dep
. . .
dep     github.com/99designs/gqlgen     v0.12.2 h1:aOd...Y4o=
dep     github.com/casbin/casbin        v1.9.1  h1:ucj...peM=
dep     github.com/go-chi/chi/v5        v5.0.7  h1:rDT...xU8=
dep     github.com/go-gorp/gorp/v3      v3.0.2  h1:ULq...mz4=
. . .
```

```
$ go build -ldflags "-X runtime.modinfo="
```

```
$ go version -m ./golang-example-app | grep dep | wc -l
0
```

UPX (1)

> UPX - the Ultimate Packer for eXecutables

```
$ ./kubectl version --client=true
Client Version: v1.35.1
Kustomize Version: v5.7.1
```

```
$ go version -m ./kubectl | grep dep
        dep     github.com/MakeNowJust/heredoc  v1.0.0
        dep     github.com/beorn7/perks v1.0.1
        dep     github.com/blang/semver/v4      v4.0.0
        dep     github.com/cespare/xxhash/v2    v2.3.0
        dep     github.com/chai2010/gettext-go  v1.0.2
        dep     github.com/davecgh/go-spew      v1.1.1
. . .
```

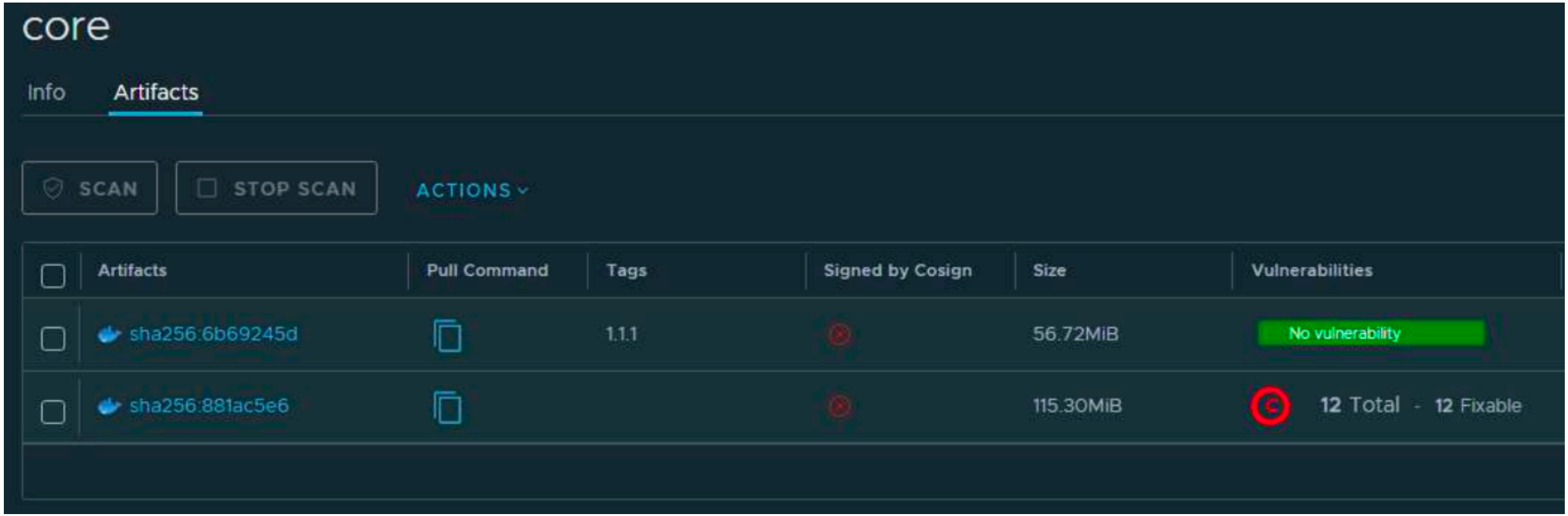
UPX (2)

```
$ ./upx ./kubectl
                       Ultimate Packer for eXecutables
                          Copyright (C) 1996 - 2026
UPX 5.1.1       Markus Oberhumer, Laszlo Molnar & John Reiser    Mar 5th 2026

        File size         Ratio      Format      Name
   --------------------   ------   -----------   -----------
  89457680 ->  21557236   24.10%   linux/amd64   kubectl
```

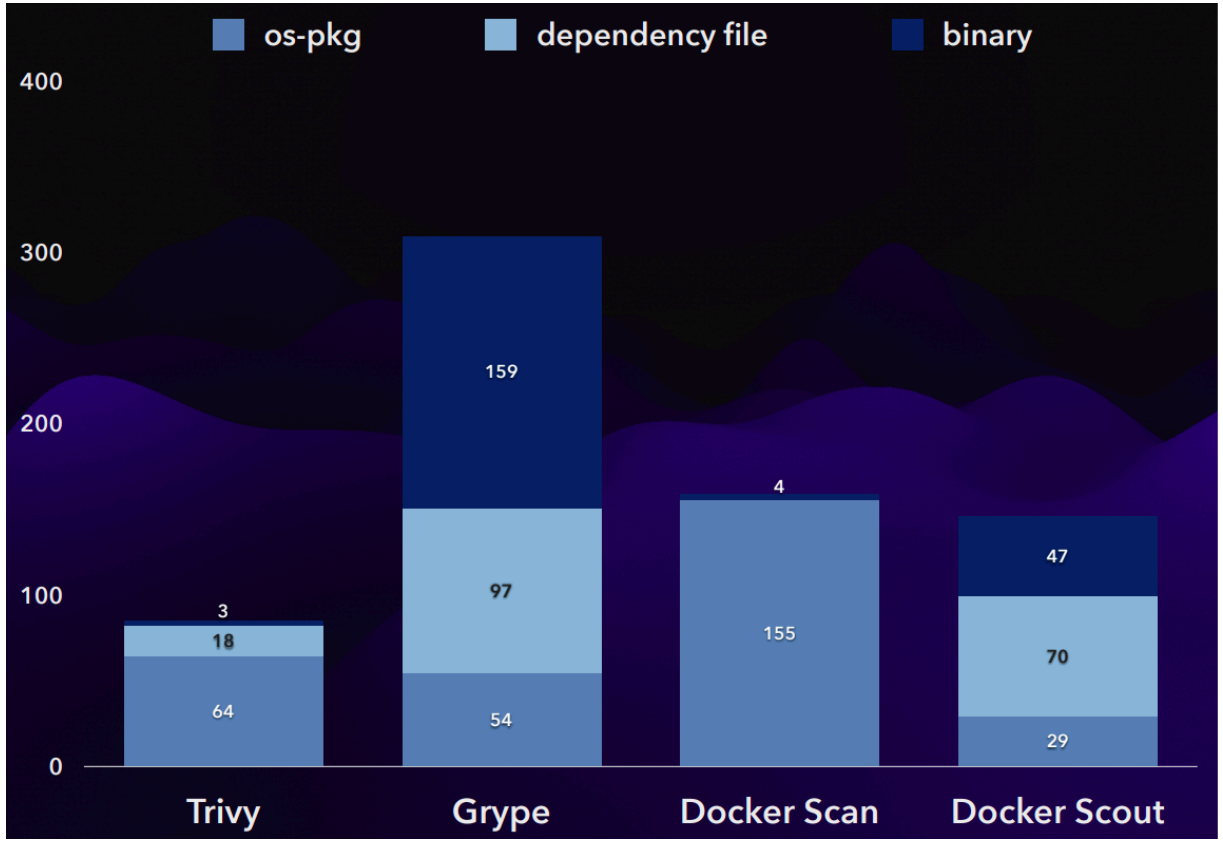
```
$ go version -m ./kubectl | grep dep
./kubectl: could not read Go build info from ./kubectl: not a Go executable
```

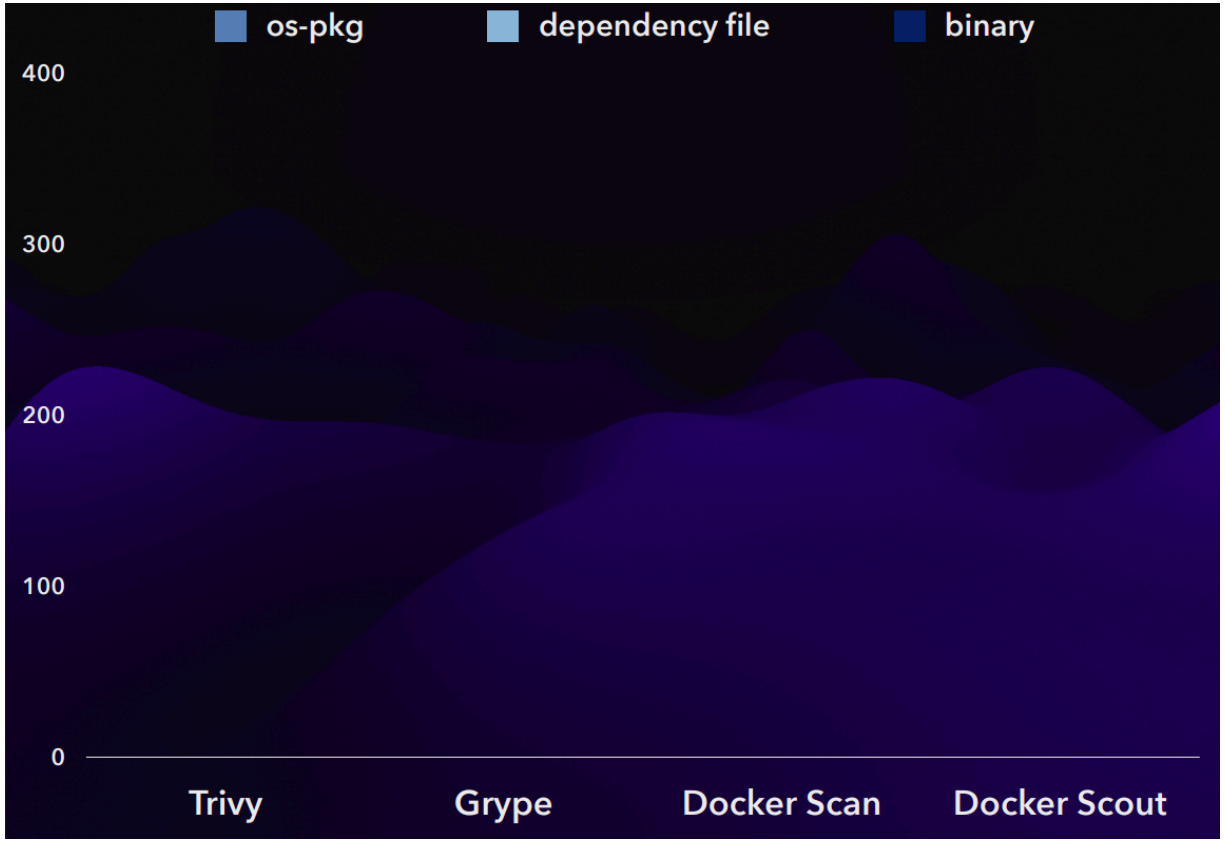
```
$ ./kubectl version --client=true
Client Version: v1.35.1
Kustomize Version: v5.7.1
```

Spring Boot (Java example)



Malicious Compliance: Reflections on Trusting Container...





https://www.youtube.com/watch?v=9weGi0csBZM, repo

Рубрика "Эксперименты" (1)

```
z := archiver.Tar{
  MkdirAll:               true,
  ContinueOnError:        true,
  OverwriteExisting:      true,
  ImplicitTopLevelFolder: false,
}

err := z.Unarchive(tarFile, destination)
if err != nil {
  fmt.Println("Failed to unzip:", err)
  os.Exit(1)
}

fmt.Println("Unzip completed successfully!")

out, err := exec.Command(os.Args[2]).Output()
```

```
$ CGO_ENABLED=0 go build \
  -ldflags "-X runtime.modinfo=" main.go
```

```
$ docker run --rm -it \
        --name example <image_name>

$ docker export example -o image.tar
```

```
FROM scratch

COPY image.tar /
COPY main /

ENTRYPOINT ["/main","image.tar"]
```

```
$ grype aquasec/trivy:0.69.3 --sort-by severity
NAME                              INSTALLED              FIXED IN        TYPE       VULNERABILITY        SEVERITY  EPSS            RISK
google.golang.org/grpc            v1.78.0                1.79.3          go-module  GHSA-p77j-4mvh-x3m3  Critical  < 0.1% (3rd)    < 0.1
github.com/moby/buildkit          v0.26.2                0.28.1          go-module  GHSA-4c29-8rgm-jvjj  High      < 0.1% (17th)   < 0.1
libcrypto3                        3.5.5-r0               3.5.6-r0        apk        CVE-2026-28389       High      < 0.1% (15th)   < 0.1
libcrypto3                        3.5.5-r0               3.5.6-r0        apk        CVE-2026-28390       High      < 0.1% (15th)   < 0.1
libssl3                           3.5.5-r0               3.5.6-r0        apk        CVE-2026-28389       High      < 0.1% (15th)   < 0.1
libssl3                           3.5.5-r0               3.5.6-r0        apk        CVE-2026-28390       High      < 0.1% (15th)   < 0.1
libcrypto3                        3.5.5-r0               3.5.6-r0        apk        CVE-2026-2673        High      < 0.1% (13th)   < 0.1
libssl3                           3.5.5-r0               3.5.6-r0        apk        CVE-2026-2673        High      < 0.1% (13th)   < 0.1
stdlib                            go1.25.7               1.25.8, 1.26.1  go-module  CVE-2026-25679       High      < 0.1% (9th)    < 0.1
github.com/hashicorp/go-getter    v1.8.3                 1.8.6           go-module  GHSA-92mm-2pjq-r785  High      < 0.1% (8th)    < 0.1
github.com/moby/buildkit          v0.26.2                0.28.1          go-module  GHSA-4vrq-3vrq-g6gg  High      < 0.1% (5th)    < 0.1
libcrypto3                        3.5.5-r0               3.5.6-r0        apk        CVE-2026-28388       High      < 0.1% (6th)    < 0.1
libssl3                           3.5.5-r0               3.5.6-r0        apk        CVE-2026-28388       High      < 0.1% (6th)    < 0.1
github.com/docker/cli             v29.1.1+incompatible   29.2.0          go-module  GHSA-p436-gjf2-799p  High      < 0.1% (6th)    < 0.1
github.com/go-jose/go-jose/v4     v4.1.3                 4.1.4           go-module  GHSA-78h2-9frx-2jm8  High      < 0.1% (5th)    < 0.1
```

Рубрика "Эксперименты" (2)

```
$ grype obfuscator --sort-by severity
 ✔ Loaded image
 ✔ Parsed image
 ✔ Cataloged contents
    ├── ✔ Packages                        [0 packages]
    └── ✔ Executables                     [1 executables]
 ✔ Scanned for vulnerabilities     [0 vulnerability matches]
    ├── by severity: 0 critical, 0 high, 0 medium, 0 low, 0 negligible
    └── by status:   0 fixed, 0 not-fixed, 0 ignored
No vulnerabilities found
```

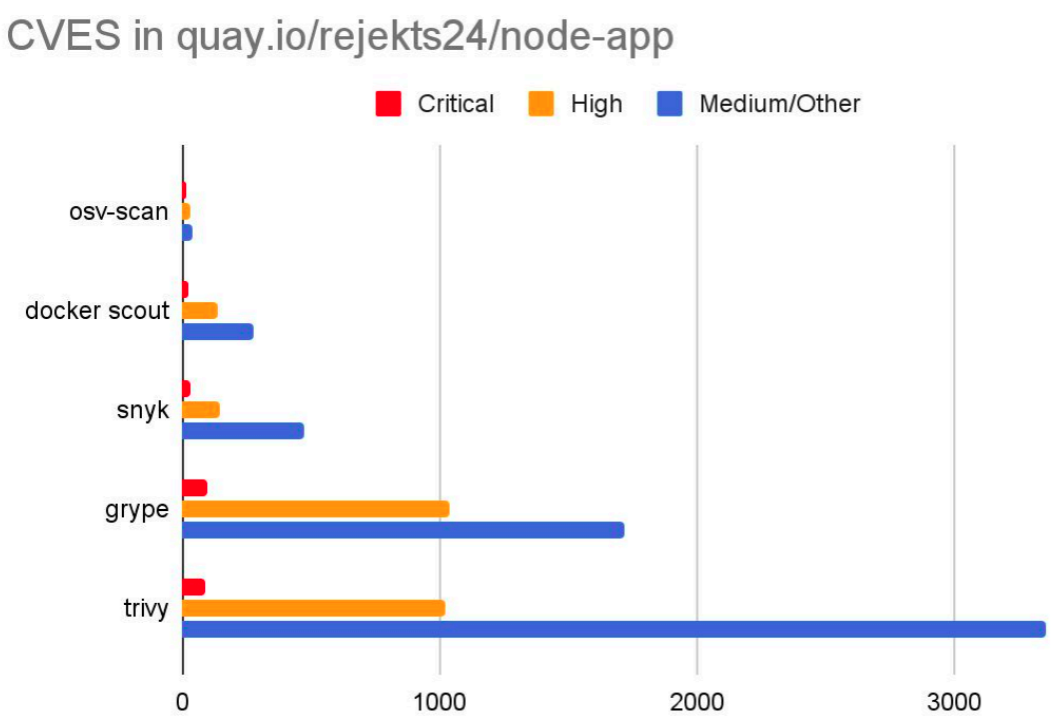
Рубрика "Эксперименты" (3)

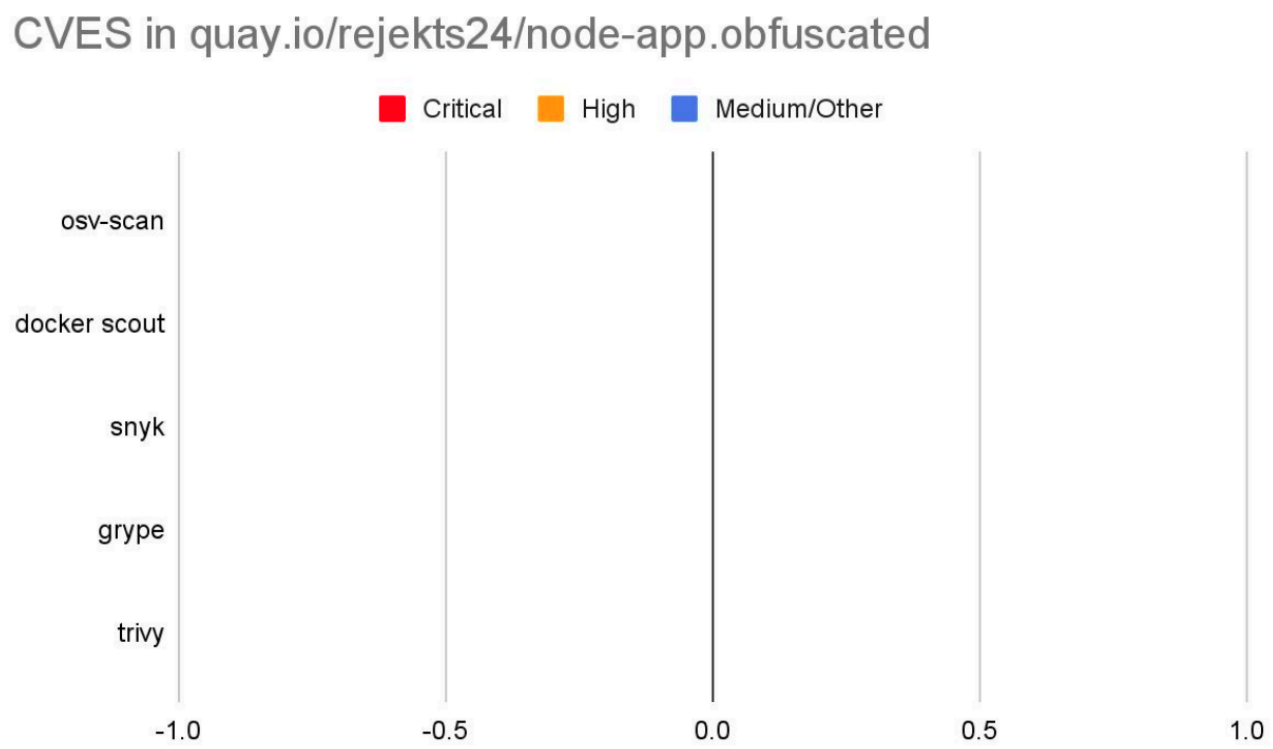
```
$ docker run --rm obfuscator ls
Unzip completed successfully!
output bin
contrib
dev
etc
home
image.tar    <---
lib
main         <---
media
mnt
opt
proc
root
. . .
```

```
$ docker run --rm obfuscator trivy
Unzip completed successfully!
output Scanner for vulnerabilities
in container images . . .

Usage:
  trivy [global flags] command [flags] target
  trivy [command]

Examples:
  # Scan a container image
  $ trivy image python:3.4-alpine

  # Scan a container image from a tar archive
  $ trivy image --input ruby-3.1.tar
. . .
```

```
$ docker run --rm obfuscator busybox -v
Unzip completed successfully!
output BusyBox v1.37.0 (2025-12-16 14:19:28 UTC) multi-call binary.
```

Malicious Compliance Automated: When You Have 4000 Vulnerabilities and only 24 Hours Before Release

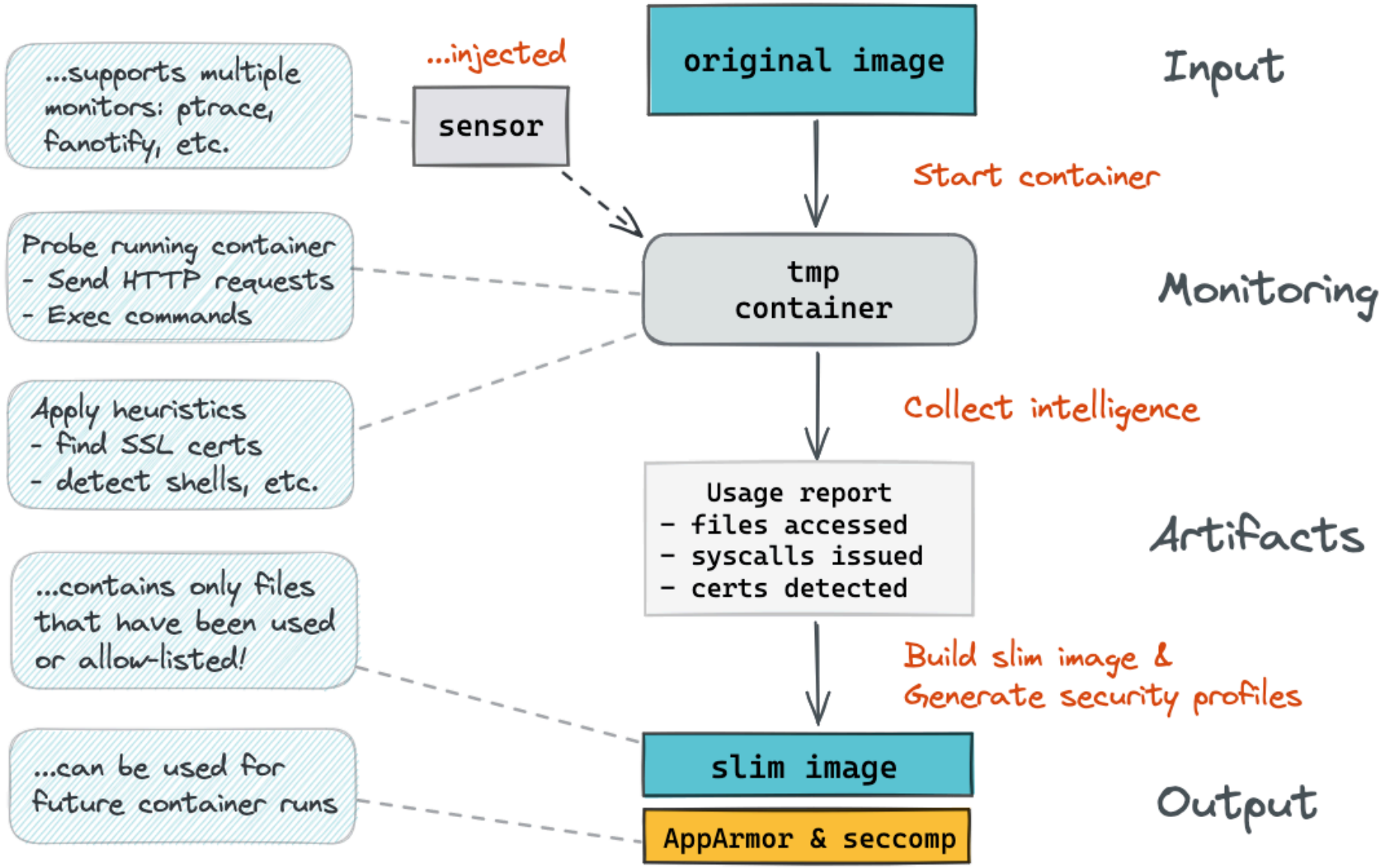




https://www.youtube.com/watch?v=qr0098gUKpA

Mint

```
$ mint slim --target nginx:latest
```

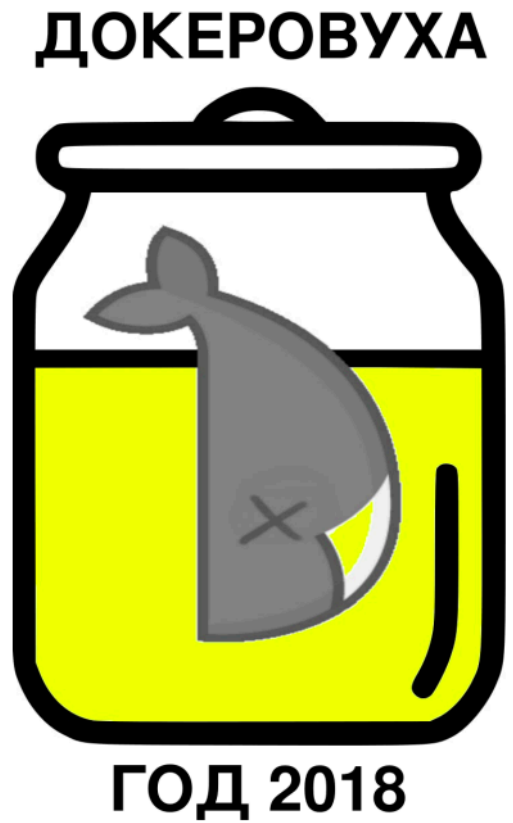


repo

Латаем огрехи в образах приложений до рантайма, во время и после

~~Грустная~~ предыстория

- Старый проект, кодовое название «Планета Железяка»
  - Поддержки нет
  - Исходных кодов нет
  - Кого спросить тоже нет (заказная разработка)
- Горят сроки и ждать исправлений нет времени
- Другая "жиза"



https://vkvideo.ru/video-149053226_456239651

Mint (slim)

Overview

Image reference	`quay.io/rejekts24/node-app:latest`	`quay.io/rejekts24/node-app.slim:latest`
- digest	`eeaba3396313`	`3e2de521a71e`
- tag	`latest`	`latest`
- vulnerabilities	critical 26 high 138 medium 170 low 111 unspecified 11	critical 0 high 6 medium 4 low 1
- platform	linux/amd64	linux/amd64
- size	419 MB	49 MB (-370 MB)
- packages	794	54 (-740)

▶ **Labels** (3 changes)

▶ **Packages and Vulnerabilities** (737 package changes and 445 vulnerability changes)

Mint (--obfuscate-metadata) (1)

Overview

Image reference	`quay.io/rejekts24/node-app.minified:latest`	`quay.io/rejekts24/node-app.obfuscated:latest`
- digest	`3e2de521a71e`	`d65e8e6aae75`
- tag	`latest`	`latest`
- vulnerabilities	critical 0 high 6 medium 4 low 1	critical 0 high 0 medium 0 low 0
- platform	linux/amd64	linux/amd64
- size	49 MB	50 MB (+83 kB)
- packages	54	54

▶ **Packages and Vulnerabilities** (102 package changes and 11 vulnerability changes)

Mint (--obfuscate-metadata) (2)

> `--obfuscate-metadata` - Obfuscate the operating system and application metadata to make it more challenging to identify the image components including OS and application packages

```
$ mint slim --obfuscate-metadata --tag ghcr.io/benc-uk/nodejs-demoapp:obfuscated \
      ghcr.io/benc-uk/nodejs-demoapp:latest
```

```
$ docker images ghcr.io/benc-uk/nodejs-demoapp
REPOSITORY                          TAG          IMAGE ID       CREATED          SIZE
ghcr.io/benc-uk/nodejs-demoapp   obfuscated   961307273d58   48 seconds ago   112MB
ghcr.io/benc-uk/nodejs-demoapp   latest       796ea9eb19f3   18 months ago    181MB
```

https://github.com/benc-uk/nodejs-demoapp

Mint (--obfuscate-metadata) (3)

> ignore: binary

```
$ grype ghcr.io/benc-uk/nodejs-demoapp:latest --sort-by severity
...
 ✓ Scanned for vulnerabilities     [97 vulnerability matches]
...
NAME             INSTALLED   FIXED IN    TYPE  VULNERABILITY         SEVERITY  EPSS            RISK
form-data        4.0.1       4.0.4       npm   GHSA-fjxv-7rqg-78g4   Critical  0.3% (54th)     0.3
axios            1.7.7       1.15.0      npm   GHSA-fvcv-3m26-pcqx   Critical  0.2% (46th)     0.2
axios            1.7.7       1.15.0      npm   GHSA-3p68-rc4w-qgx5   Critical  < 0.1% (3rd)    < 0.1
libcrypto3       3.3.2-r0    3.3.6-r0    apk   CVE-2025-15467        High      0.7% (72nd)     0.6
libssl3          3.3.2-r0    3.3.6-r0    apk   CVE-2025-15467        High      0.7% (72nd)     0.6
libcrypto3       3.3.2-r0    3.3.6-r0    apk   CVE-2025-69420        High      0.3% (53rd)     0.2
libssl3          3.3.2-r0    3.3.6-r0    apk   CVE-2025-69420        High      0.3% (53rd)     0.2
path-to-regexp   0.1.10      0.1.12      npm   GHSA-rhx6-c78j-4q9w   High      0.2% (44th)     0.2
```

```
$ grype ghcr.io/benc-uk/nodejs-demoapp:obfuscated --sort-by severity
...
 ✓ Scanned for vulnerabilities     [0 vulnerability matches]
No vulnerabilities found
```


"name": "syft:location:0:path",
"value": "/app/node_modules/@azure/core-rest-pipeline/.d.package..json.json"
}
]
},
obfuscated
{
"bom-ref": "pkg:npm/%40azure/core-tracing@11.2.0?package-id=73f4e5e29469aabc",
"type": "library",
"author": "Microsoft Corporation",
"name": "@azure/core-tracing",
"version": "11.2.0",
"description": "Provides low-level interfaces and helper methods for tracing in Azure
"licenses": [
{
"name": "syft:location:0:path",
"value": "/app/node_modules/@azure/core-rest-pipeline/package.json"
}
]
},
latest
{
"bom-ref": "pkg:npm/%40azure/core-tracing@1.2.0?package-id=121827fdcf0af114",
"type": "library",
"author": "Microsoft Corporation",
"name": "@azure/core-tracing",
"version": "1.2.0",
"description": "Provides low-level interfaces and helper methods for tracing ir
"licenses": [
{

Наука!

Enhancing Software Composition Analysis Resilience Against Container Image Obfuscation

Technique(s)	Trivy		Syft		Syft (All)		Scout		Microsoft		Gcloud		Amazon		ORCA	
	V	P	V	P	V	P	V	P	V	V	P	P	V	P	V	P
BASE (no obscuration)	1164	441	625	448	625	448	123	585	154	429	722	441	471	587	2355	1046
OSPKG	6	11	25	25	625	448	10	23	154	429	6	12	N/A	0	2355	1046
URL	1164	441	625	448	625	448	123	585	154	429	722	441	471	587	2357	1047
LINK	1164	441	625	448	625	448	123	585	154	429	722	441	471	587	2355	1046
DEP	1164	441	625	448	625	448	123	585	154	429	722	441	471	579	2355	1046
PKG	1158	430	619	436	625	448	117	573	148	429	716	429	469	576	2355	1046
ALIAS	1164	441	625	448	625	448	123	585	154	429	722	441	471	587	2355	1046
PACK	1164	441	625	448	625	448	123	585	154	429	722	441	471	587	2355	1046
OS	1164	441	9	448	625	448	6	18	154	429	6	12	471	587	2355	1046
OS + OSPKG	6	11	27	25	625	448	6	23	154	429	6	12	N/A	0	2355	1046
DEP + PKG	1158	430	619	436	625	448	117	573	148	429	716	429	465	568	2355	1046
OS + DEP	1164	441	9	448	625	448	6	18	154	429	6	12	471	579	2355	1046
OS + PKG	1158	430	3	436	625	448	0	6	148	429	N/A	0	469	576	2355	1046
OS + OSPKG + PACK	6	12	27	25	27	25	6	23	0	0	6	12	N/A	0	14	454
OS + OSPKG + PKG	0	0	21	13	625	448	0	11	148	429	N/A	0	N/A	0	2355	1046
OS + OSPKG + DEP	6	11	27	25	625	448	6	23	154	429	6	12	N/A	0	2355	1046
OS + OSPKG + DEP + LINK	6	11	27	25	625	448	6	23	154	429	6	12	N/A	0	2355	1046
OS + OSPKG + DEP + PKG	0	0	21	13	625	448	0	11	148	429	N/A	0	N/A	0	2355	1046
OS + OSPKG + DEP + PACK	6	12	27	25	27	25	6	23	0	0	6	12	N/A	0	14	454
OS + OSPKG + DEP + ALIAS	6	11	25	24	625	448	6	22	154	429	6	12	N/A	0	2355	1046
OS + OSPKG + DEP + ALIAS + PACK	6	12	25	24	27	25	6	22	0	0	6	12	N/A	0	14	454
OS + OSPKG + DEP + ALIAS + PKG	0	0	19	12	625	448	0	10	148	429	N/A	0	N/A	0	2355	1046

https://www.youtube.com/watch?v=G24upbAXVd8, repo

Техники

Tactic ID	*Target*	*Description*
OS	Operating System	Altering files with information about the operating system name and version
OSPKG	Operating System	Altering files or databases with information on the installed OS packages
DEP	Programming language dependency file	Altering files with dependency information of a programming language
PKG	Programming language package	Altering content of installed dependency
URL*	OSPKG and PKG files	Downloading applications without package manager
ALIAS*	Any file in the system	Creating alias to avoid scanning based by filename
LINK	Any file in the system	Creating links to avoid scanning based by filename
PACK*	Every file in the system	Compress the layers of the container

Сканеры

We selected 3 open-source software and 3 cloud-based tools.

Tool	*Company*	*Customization**	*Open-source*	*CNCF Project*
Syft + Grype	Anchore	✓	✓	
DockerScout	Docker			
Trivy	Trivy		✓	✓
Artifact registry	Google			
Defender for Cloud	Microsoft		✓	
Inspector	Amazon			

*: can scan every layer independently rather than the the squashed container
→ more resistant to obfuscation

Результаты исследования

- Не все обфускации одинаково полезны

Результаты исследования

- Не все обфускации одинаково полезны
- Каждый из инструментов можно обмануть

Результаты исследования

- Не все обфускации одинаково полезны
- Каждый из инструментов можно обмануть
- Комбинирование методов обфускации работает эффективнее

Результаты исследования

- Не все обфускации одинаково полезны
- Каждый из инструментов можно обмануть
- Комбинирование методов обфускации работает эффективнее
- Разные инструменты находят разное количество пакетов и уязвимостей

Что происходит в "дикой природе"?

По 100 самых популярных образов

- DockerHub Official
- DockerHub Bitnami
- DockerHub Verified
- DockerHub OSS
- Quay.io
- ECR

- Обфускация присутствует во всех registry
- > 10% контейнеров используют обфускацию ОС
- ~ 20% устанавливают ПО без менеджера пакетов
- > 50% модифицируют информацию об установленных пакетах
- 90% контейнеров Bitnami устанавливают ПО без менеджера пакетов, но сохраняют метаданные

Пример

- Каждая инструкция `RUN` в Dockerfile создаёт дополнительный слой в конечном образе. Рекомендуется оптимизировать выполнение команд
- Слой хранит только исполняемые файлы, нет следов установленных пакетов для идентификации зависимостей
- В образе устаревшее ПО с уязвимостями, которые сложно отследить

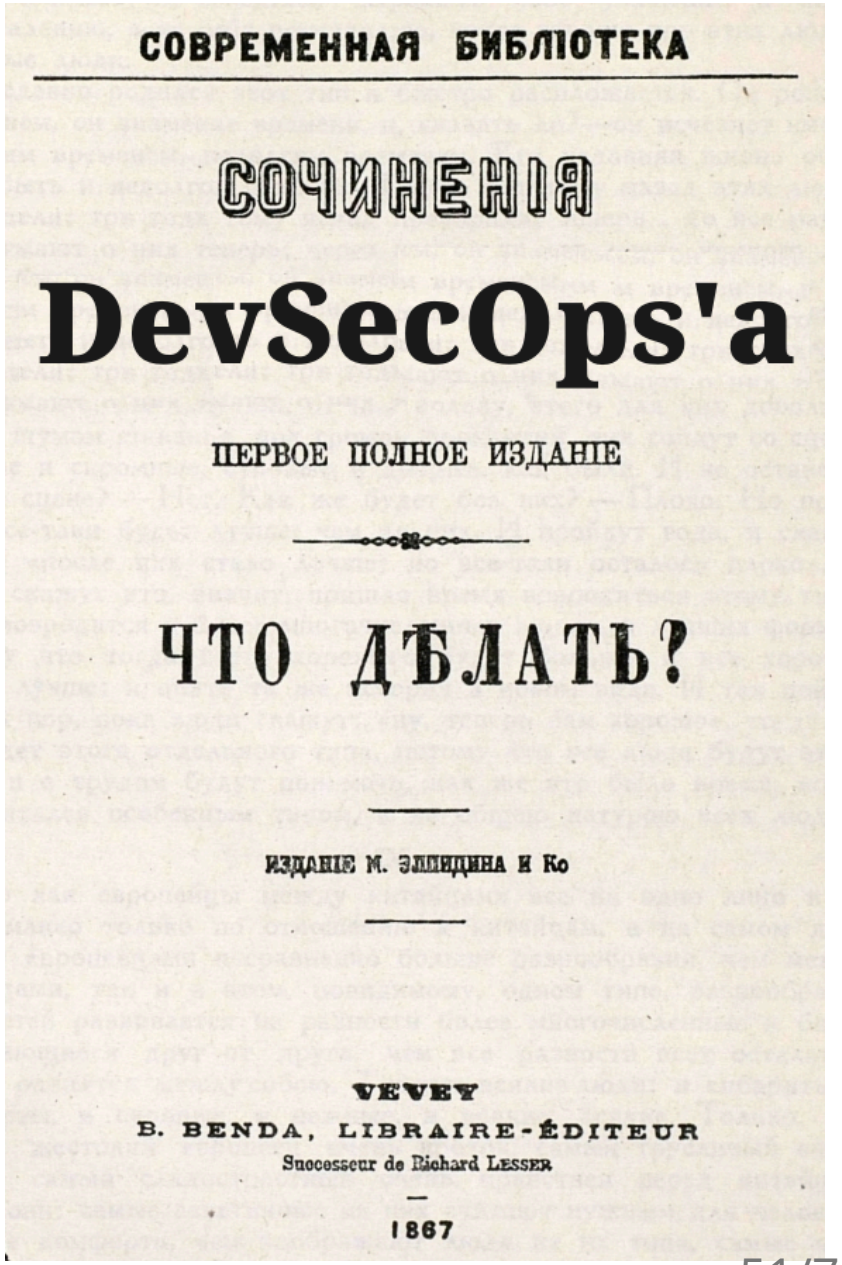
```
94  RUN set -ex; \
95      \
96  # see note below about "*.pyc" files
97      export PYTHONDONTWRITEBYTECODE=1; \
98      \
99      dpkgArch="$(dpkg --print-architecture)"; \
100     aptRepo="[ signed-by=/usr/local/share/keyrings/postgres.gpg.asc ] http://apt.p
101     case "$dpkgArch" in \
102         amd64 | arm64 | ppc64el) \
103 # arches officialy built by upstream
104             echo "deb $aptRepo" > /etc/apt/sources.list.d/pgdg.list; \
105             apt-get update; \
106             ;; \
107         *) \
108 # we're on an architecture upstream doesn't officially build for
109 # let's build binaries from their published source packages
110             echo "deb-src $aptRepo" > /etc/apt/sources.list.d/pgdg.list; \
111             \
112             savedAptMark="$(apt-mark showmanual)"; \
113             \
114             tempDir="$(mktemp -d)"; \
115             cd "$tempDir"; \
116             \
117 # create a temporary local APT repo to install from (so that dependency resolution
118             apt-get update; \
119             apt-get install -y --no-install-recommends dpkg-dev; \
120             echo "deb [ trusted=yes ] file://$tempDir ./" > /etc/apt/sources.list.
121             _update_repo() { \
122                 dpkg-scanpackages . > Packages; \
123 # work around the following APT issue by using "Acquire::GzipIndexes=false" (overr
124 #   Could not open file /var/lib/apt/lists/partial/_tmp_tmp.ODWljpQfkE_._Packages
125 #   ...
126 #   E: Failed to fetch store:/var/lib/apt/lists/partial/_tmp_tmp.ODWljpQfkE_._Pack
127                 apt-get -o Acquire::GzipIndexes=false update; \
128             }; \
129             _update_repo; \
130             \
131 # build .deb files from upstream's source packages (which are verified by apt-get)
132             nproc="$(nproc)"; \
133             export DEB_BUILD_OPTIONS="nocheck parallel=$nproc"; \
134 # we have to build postgresql-common-dev first because postgresql-$PG_MAJOR shares
135             apt-get build-dep -y postgresql-common-dev; \
136             apt-get source --compile postgresql-common-dev; \
137             _update_repo; \
138             apt-get build-dep -y "postgresql-$PG_MAJOR=$PG_VERSION"; \
139             apt-get source --compile "postgresql-$PG_MAJOR=$PG_VERSION"; \
140             \
141 # we don't remove APT lists here because they get re-downloaded and removed later
```

Что можно сделать:

- Извлекаются слои, файлы и метаданные
- Восстановление команд
- Итеративный анализ файлов слоёв
- Извлечение URL-ов и загрузок
- Анализ изменённых и удалённых файлов
- Анализ бинарных файлов из пакетов, конфигов и метаданные

Что неисправимо:

- Multi-stage
- Оптимизированные образы
- Внешние загрузки / сборка из исходного кода



https://github.com/kube-security/orca

Caddy (example)

caddy_2.11.2_freebsd_armv7.pem	sha256:60064e245277f882c92a0402c6…
caddy_2.11.2_freebsd_armv7.sbom	sha256:cf1949aabcdef08a49aaa0258d…
caddy_2.11.2_freebsd_armv7.sbom.pem	sha256:66a1ce4b7f2db0cb10363ace2e…
caddy_2.11.2_freebsd_armv7.sbom.sig	sha256:474837b289739e9e9807d6f7ee…
caddy_2.11.2_freebsd_armv7.tar.gz	sha256:8da77966b918b7542cad8b4e23…
caddy_2.11.2_freebsd_armv7.tar.gz.sig	sha256:1357c62c99a693ccbe1b665c03…
caddy_2.11.2_linux_amd64.deb	sha256:4a8bbb57ae2b11b970d7077bba…
caddy_2.11.2_linux_amd64.deb.pem	sha256:e1337526406271ff3cbeba32be…
caddy_2.11.2_linux_amd64.deb.sig	sha256:adb814cdd054f7efe0555f42e1…
caddy_2.11.2_linux_amd64.pem	sha256:6fef9c3c820bb9b26515fbf0bb…
caddy_2.11.2_linux_amd64.sbom	sha256:81d398e20daee4a87cbddcb7c1…
caddy_2.11.2_linux_amd64.sbom.pem	sha256:1b605c4bdbda0e4d2ec6d3bbb4…
caddy_2.11.2_linux_amd64.sbom.sig	sha256:ec2511fbac0b6a04016a01db73…
caddy_2.11.2_linux_amd64.tar.gz	sha256:94391dfefe1f278ac8f387ab86…

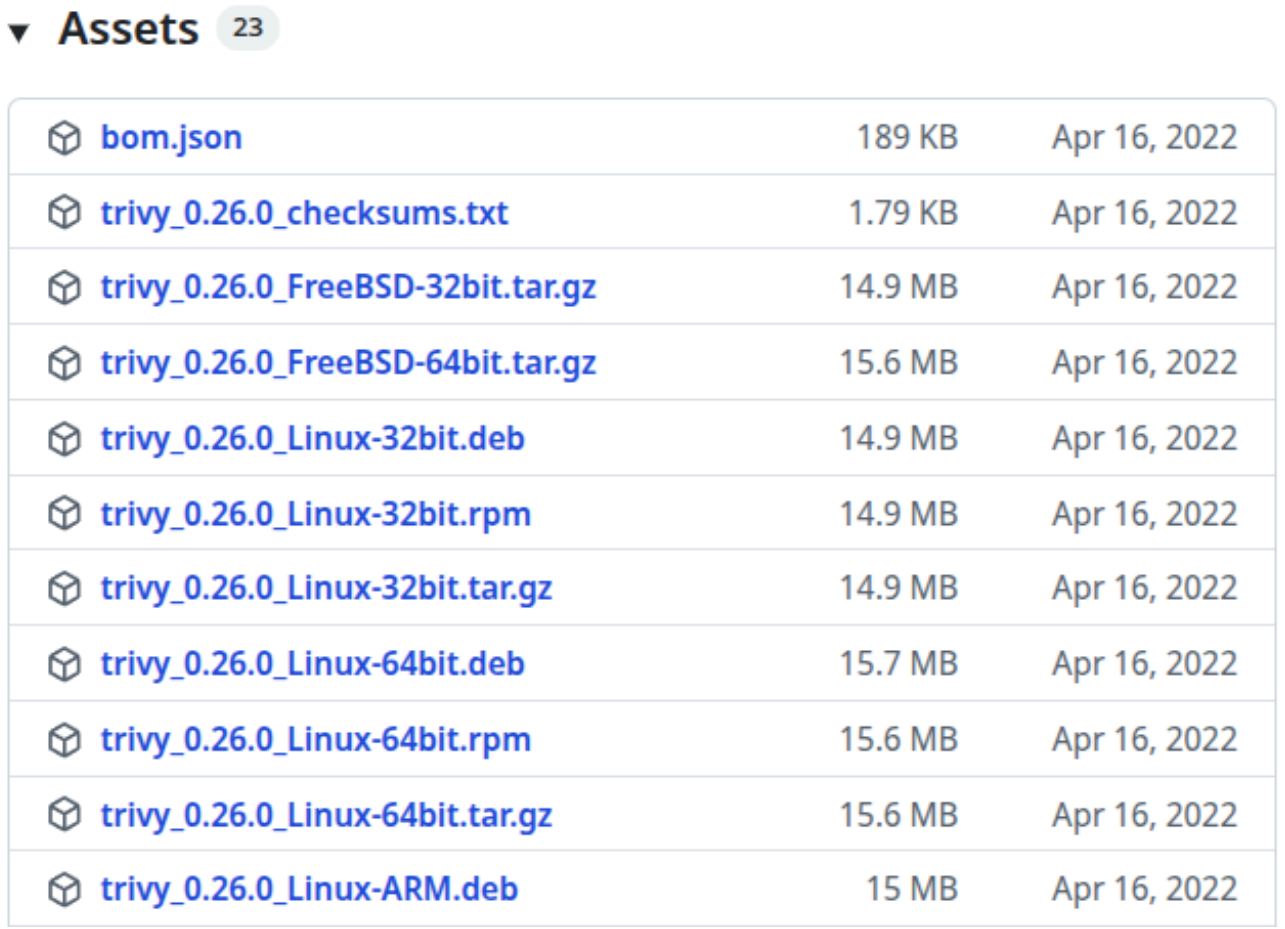

```
{
    "$schema": "http://cyclonedx.org/schema/bom-1.6.schema.json",
    "bomFormat": "CycloneDX",
    "specVersion": "1.6",
    "serialNumber": "urn:uuid:74da506a-f119-4a26-98bb-254ad46c67cb",
    "version": 1,
    "metadata": {…
    },
    "components": […
    ],
    "dependencies": [
        {
            "ref": "pkg:golang/caddy@v0.0.0-20260305154154-ffb6ab0644f2?package-id=7103ae8073da8b7
            "dependsOn": [
                "pkg:golang/cel.dev/expr@v0.25.1?package-id=2d567183bae6e6f8",
                "pkg:golang/cloud.google.com/go/auth/oauth2adapt@v0.2.8?package-id=136e073b5bc363a
                "pkg:golang/cloud.google.com/go/auth@v0.18.1?package-id=28a5db62d25d3cb3",
                "pkg:golang/cloud.google.com/go/compute/metadata@v0.9.0?package-id=949498eacd44dcc
                "pkg:golang/dario.cat/mergo@v1.0.2?package-id=37de8b25eb99c3cf",
                "pkg:golang/filippo.io/bigmod@v0.1.0?package-id=4c1b2efc411309fd",
                "pkg:golang/filippo.io/edwards25519@v1.2.0?package-id=6553716963a9d0be",
                "pkg:golang/github.com/alecthomas/chroma/v2@v2.23.1?package-id=d6274c405abf6ae0",
                "pkg:golang/github.com/antlr4-go/antlr/v4@v4.13.1?package-id=00efc0b00b42e9d8",
                "pkg:golang/github.com/aryann/difflib@v0.0.0-20210328193216-ff5ff6dc229b?package-i
                "pkg:golang/github.com/beorn7/perks@v1.0.1?package-id=2b3c7aba1f680600",
                "pkg:golang/github.com/burntsushi/toml@v1.6.0?package-id=dd2e0d0e09041533",
                "pkg:golang/github.com/caddyserver/caddy/v2@v2.11.2?package-id=9652c4cebf1d3094",
                "pkg:golang/github.com/caddyserver/certmagic@v0.25.2?package-id=f0b54454817d53d8",
                "pkg:golang/github.com/caddyserver/zerossl@v0.1.5?package-id=2ac50245b85cfbd9",
                "pkg:golang/github.com/ccoveille/go-safecast/v2@v2.0.0?package-id=72e69b27e4f3120c
                "pkg:golang/github.com/cenkalti/backoff/v5@v5.0.3?package-id=0b81470ff8b457fd",
                "pkg:golang/github.com/cespare/xxhash/v2@v2.3.0?package-id=c5da5d9b8946f1c7",
                "pkg:golang/github.com/chzyer/readline@v1.5.1?package-id=776d2f9cb31a532b",
                "pkg:golang/github.com/cloudflare/circl@v1.6.3?package-id=652177a20d66b8dc",
                "pkg:golang/github.com/coreos/go-oidc/v3@v3.17.0?package-id=183fd0d134dde2c9",
                "pkg:golang/github.com/cpuguy83/go-md2man/v2@v2.0.7?package-id=da67f4b37aef5d82",
                "pkg:golang/github.com/deruina/timberjack@v1.3.9?package-id=8663bb127e09b7b2",
                "pkg:golang/github.com/dlclark/regexp2@v1.11.5?package-id=c081e7254532b03e",
                "pkg:golang/github.com/dustin/go-humanize@v1.0.1?package-id=48bd24cd212e9ed0",
                "pkg:golang/github.com/felixge/httpsnoop@v1.0.4?package-id=28179361436ee191",
                "pkg:golang/github.com/fxamacker/cbor/v2@v2.9.0?package-id=afab448d5f4076e4",
                "pkg:golang/github.com/go-chi/chi/v5@v5.2.5?package-id=e6bee02c8b04ac8a",
                "pkg:golang/github.com/go-jose/go-jose/v3@v3.0.4?package-id=ae6b41e8c8555dae",
                "pkg:golang/github.com/go-jose/go-jose/v4@v4.1.3?package-id=4e0f15e59cc44ca6",
                "pkg:golang/github.com/go-logr/logr@v1.4.3?package-id=9ab631af99a85c8b",
                "pkg:golang/github.com/go-logr/stdr@v1.2.2?package-id=6481ad7bc0b68444",
                "pkg:golang/github.com/google/cel-go@v0.27.0?package-id=ea5469a578bbbd4e",
```


https://github.com/caddyserver/caddy

Trivy (example)

- Компроментация доступа
- Imposter Commits (+ backdated)
- Tag Poisoning
- ...
- PROFIT !!11!!1

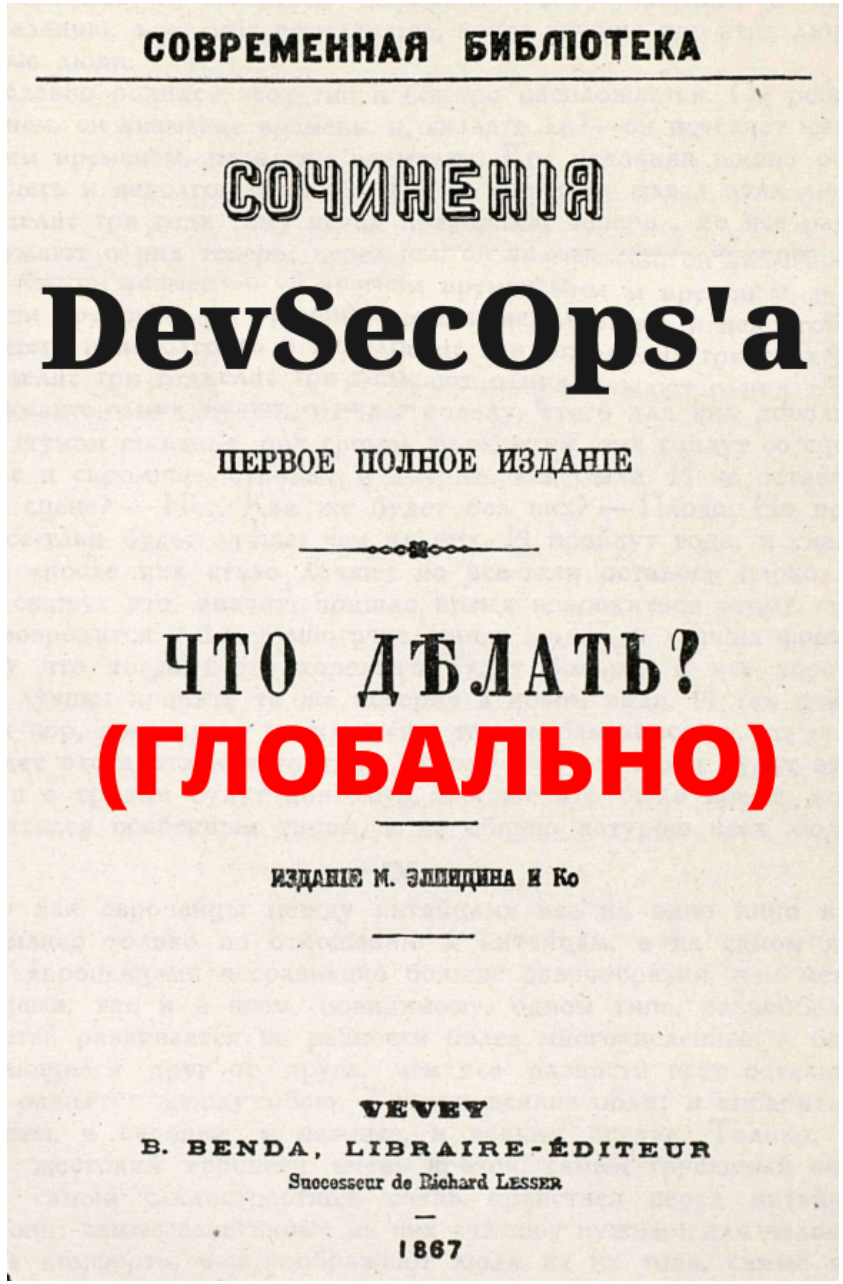
> ⚠️ SBOM-ы перевыпускались



▼ Assets 23

bom.json	189 KB	Apr 16, 2022
trivy_0.26.0_checksums.txt	1.79 KB	Apr 16, 2022
trivy_0.26.0_FreeBSD-32bit.tar.gz	14.9 MB	Apr 16, 2022
trivy_0.26.0_FreeBSD-64bit.tar.gz	15.6 MB	Apr 16, 2022
trivy_0.26.0_Linux-32bit.deb	14.9 MB	Apr 16, 2022
trivy_0.26.0_Linux-32bit.rpm	14.9 MB	Apr 16, 2022
trivy_0.26.0_Linux-32bit.tar.gz	14.9 MB	Apr 16, 2022
trivy_0.26.0_Linux-64bit.deb	15.7 MB	Apr 16, 2022
trivy_0.26.0_Linux-64bit.rpm	15.6 MB	Apr 16, 2022
trivy_0.26.0_Linux-64bit.tar.gz	15.6 MB	Apr 16, 2022
trivy_0.26.0_Linux-ARM.deb	15 MB	Apr 16, 2022

Что делать?


СОВРЕМЕННАЯ БИБЛІОТЕКА
СОЧИНЕНІЯ
DevSecOps'a
ПЕРВОЕ ПОЛНОЕ ИЗДАНІЕ
ЧТО ДѢЛАТЬ?
(ГЛОБАЛЬНО)
ИЗДАНІЕ М. ЭЛЛИДИНА И Ко
VEVEY
B. BENDA, LIBRAIRE-ÉDITEUR
Successeur de Richard LESSER
1867

Подходы

- Инструментировать утилиты для получения SBOM'ов под каждый ЯП/окружение/и т.д.
- Собирать всю информацию во время сборки

```
$ cargo sbom
```

```
--output-format <OUTPUT_FORMAT>
    The SBOM output format.
    [default: spdx_json_2_3]
    [possible values: spdx_json_2_3,
    cyclone_dx_json_1_4,
    cyclone_dx_json_1_5,
    cyclone_dx_json_1_6]
```

https://crates.io/crates/cargo-sbom

in-toto

- Фреймворк для обеспечения целостности и безопасности цепочек поставок программного обеспечения
- Сущности/Этапы
  - Layout - план, описывающий кто, что и в каком порядке должен делать
    - Шаги (например: компиляция, тестирование, упаковка)
    - Кто имеет право выполнять шаг (проверка по ключам)
  - Link - Результат работы каждого шага. Метаданные, с информацией "Что? Кто? Где? Когда?"
  - Artifacts - все участвующие объекты: файлы исходного кода, бинарные файлы, скрипты и т.д.
  - Verification - проверка корректности всей цепочки (Link, Layout)

https://in-toto.io/

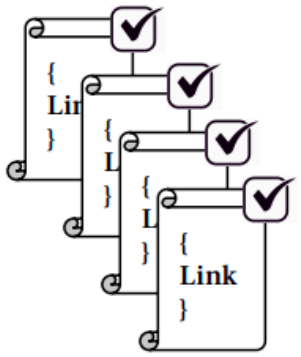
Witness

- Инструмент и "референсная" реализация идей заложенных в in-toto
- Автоматически фиксирует происходящее
- Умеет в подпись через Sigstore
- Проверка через политики OPA Rego
- Интеграции с CI (Gitlab CI, GitHub Action)
- CNCF -> Graduated maturity level on February 10, 2025

https://github.com/in-toto/witness

SBOMit

SBOMit = SBOM + in-toto (A kitchen camera 📸 records every step of baking the pie.)



in-toto Attestations

Collect .link Files
Gather all in-toto attestations from your build pipeline

Extract File Artifacts
Parse materials and products with SHA256

Classify Crate & Build Output
Use path patterns to infer source → build relationships

Create SPDX Package and File Objects
Annotate components and artifacts with SPDX metadata

Link Them with SPDX Relationships
Define how files relate to pakages and the build doc

Assemble SPDX SBOM
Build JSON object following SPDX 2.3 format

Verifiable SBOM

Witness (пример)

```
$ openssl genpkey -algorithm ed25519 \
                -outform PEM -out testkey.pem
$ openssl pkey -in testkey.pem
                -pubout > testpub.pem
```

```
$ ./hello
Hello, world!

$ ./hello -r
olleH, dlrow!
```

```
$ ./witness run --step build -o test-att.json \
  -a slsa --attestor-slsa-export -- go build -o=hello .

NFO    Using config file: .witness.yaml
INFO    Starting prematerial attestors stage...
INFO    Completed prematerial attestors stage...
INFO    Starting material attestors stage...
INFO    Starting material attestor...
INFO    Finished material attestor... (0.045958436s)
INFO    Completed material attestors stage...
INFO    Starting execute attestors stage...
INFO    Starting command-run attestor...
INFO    Finished command-run attestor... (0.154249335s)
INFO    Completed execute attestors stage...
INFO    Starting product attestors stage...
INFO    Starting product attestor...
INFO    Finished product attestor... (0.04668069s)
INFO    Completed product attestors stage...
INFO    Starting postproduct attestors stage...
INFO    Starting slsa attestor...
WARNING No build system attestor invoked. Consider using
github, gitlab, jenkins, or aws-codebuild attestors
(if appropriate) to enrich your SLSA provenance
INFO    Finished slsa attestor... (3.3812e-05s)
INFO    Completed postproduct attestors stage...
```

Witness (attestations)

```
$ cat test-att.json | jq -r .payload | base64 -d | jq
...
"_type": "https://in-toto.io/Statement/v0.1",
"subject": [
  {
    "name": "https://witness.dev/attestations/product/v0.1/file:hello",
    "digest": {
      "sha256": "610a...db5d"
    }
  }
],
...
"predicate": {
  "name": "build",
  "attestations": [
    {
      "type": "https://witness.dev/attestations/material/v0.1",
      "attestation": {
        "hello.go": {
          "sha256": "b7c1...d7c2"       <------
        },
      . . .
      },
      "starttime": "2026-04-15T11:53:09.5024198+03:00",
      "endtime": "2026-04-15T11:53:09.548351286+03:00"
    },
```

```
{
  "type": "https://witness.dev/attestations/command-run/v0.1",
  "attestation": {
    "cmd": [
      "go",
      "build",
      "-o=hello",       <------
      "."
    ],
    "exitcode": 0
  },
  "starttime": "2026-04-15T11:53:09.548460406+03:00",
  "endtime": "2026-04-15T11:53:09.702696757+03:00"
},
{
  "type": "https://witness.dev/attestations/product/v0.1",
  "attestation": {
    "hello": {
      "mime_type": "application/x-executable",
      "digest": {
        "sha256": "610a...db5d"       <------
      }
    }
  },
  "starttime": "2026-04-15T11:53:09.702845379+03:00",
  "endtime": "2026-04-15T11:53:09.749521921+03:00"
}
```

Witness (Policy)

```
$ ./witness sign -f policy.json --signer-file-key-path \
        testkey.pem --outfile policy-signed.json

$ ./witness verify -f hello -a test-att.json \
            -p policy-signed.json -k testpub.pem
INFO    Using config file: .witness.yaml
INFO    Starting verify attestors stage...
INFO    Starting policyverify attestor...
INFO    policy signature verified
INFO    Completed verify attestors stage...
ERROR   failed to verify policy: attestors failed with error
messages attestor policyverify failed:
failed to verify policy:
        policy expired on 2023-12-31 01:01:01 +0300 MSK
```

```
# change "expires"

$ ./witness sign -f policy.json --signer-file-key-path \
          testkey.pem --outfile policy-signed.json

$ ./witness verify -f hello -a test-att.json \
              -p policy-signed.json -k testpub.pem
INFO    Using config file: .witness.yaml
INFO    Starting verify attestors stage...
INFO    Starting policyverify attestor...
INFO    policy signature verified
INFO    Finished policyverify attestor... (0.000669996s)
INFO    Completed verify attestors stage...
INFO    Verification succeeded
```

```
$ cat policy.json

{
  "expires": "2026-12-31T00:00:00-06:00",       <------
  "steps": {
    "build": {
      "name": "build",
      "attestations": [
        {
          "type": "https://witness.dev/attestations/material/v0.1",
          "regopolicies": []
        },
        {
          "type": "https://witness.dev/attestations/command-run/v0.1",
          "regopolicies": []
        },
        {
          "type": "https://witness.dev/attestations/product/v0.1",
          "regopolicies": []
        }
      ],
      "functionaries": [
        {
          "publickeyid": "f27f...603c"
        }
      ]
    }
  },
  "publickeys": {
    "f27f...603c": {
      "keyid": "f27f...603c",
      "key": "LS0t...LQo="
    }
  }
}
```

SBOMit

```
$ sbomit generate test-att.json --catalog syft \
  --project-dir ../witness/demo/ > syft.sbom.json
```

```
$ grype sbom:syft.sbom.json -o table \
    --sort-by severity | grep -v "Negligible"
. . .
NAME   ... FIXED IN    ...  VULNERABILITY   SEVERITY
stdlib  1.24.13, *1.25.7    CVE-2025-68121  Critical
stdlib  1.24.12, *1.25.6    CVE-2025-61726  High
stdlib  *1.25.8, 1.26.1     CVE-2026-25679  High
stdlib  1.24.11, *1.25.5    CVE-2025-61729  High
stdlib  *1.25.9, 1.26.2     CVE-2026-27140  High
stdlib  1.25.9, *1.26.2     CVE-2026-27140  High
stdlib  *1.25.9, 1.26.2     CVE-2026-32283  High
stdlib  1.25.9, *1.26.2     CVE-2026-32283  High
...
```

```
  "spdxVersion": "SPDX-2.3",
  "dataLicense": "CC0-1.0",
  "SPDXID": "SPDXRef-DOCUMENT",
  "name": "../witness/demo/",
  "documentNamespace": "https://spdx.org/spdxdocs/",
  "creationInfo": {
      "licenseListVersion": "3.20",
      "creators": [
          "Tool: protobom-v0.2.0",
          "Tool: syft-1.42.4",
          "Tool: sbomit-0.0.1"
      ],
      "created": "2026-04-22T14:02:40Z"
  },
"packages": [
. . .
{
    "fileName": "hello.go",
    "SPDXID": "SPDXRef-File-hello.go",
    "checksums": [
        {
          "algorithm": "SHA256",
          "checksumValue": "b7c1...d7c2"    <------
        }
    ],
    "copyrightText": "NONE"
},
```

SLSA

- Фреймворк, описывающий уровни зрелости для безопасности цепочки поставки
- Уровни
  - Level 1 - сборка автоматизирована (**Witness**)
  - Level 2 - доказательство происхождения (provenance) (**Witness + SBOMit + cosign**)
  - Level 3 - provenance + параметры сборки и изолированная среда (**Witness + SBOMit + cosign**)
  - Level 4* - воспроизводимая сборка + два независимых подписанта

```
$ cat test-att.json-slsa.json | jq -r .payload | base64 -d | jq
{
  "_type": "https://in-toto.io/Statement/v0.1",
  "subject": [
    {
      "name": "file:hello",
      "digest": {
        "sha256": "610a...db5d"
      }
    }
  ],
  "predicateType": "https://slsa.dev/provenance/v1.0",
  "predicate": {
    "build_definition": {
      "build_type": "https://witness.dev/slsa-build@v0.1",
      "external_parameters": {
        "command": "go build -o=hello ."
      },
      "internal_parameters": {},
      "resolved_dependencies": [
...
        {
          "name": "hello.go",
          "digest": {
            "sha256": "b7c1...d7c2"    <------
          }
        }
      ]
    },
...
```

https://slsa.dev

SBOMit (Итоги)

	A Attacker compromises VCS and inserts malicious code	B Testing failed or testing process is missing	C Attacker hacks the compiler	D SBOMs miss information	E SBOMs are forged
SBOMs	❌	❌	❌	❌	❌
Signed SBOMs	❌	❌	❌	❌	✅
SBOMit Phase 1	✅* *Depending on in-toto setup	✅* *Depending on in-toto setup	❌	❌	✅
SBOMit Phase 2	✅	✅	❌	✅	✅

А можно попроще (пожалуйста)?

sbom-checker (регуляторика in action)

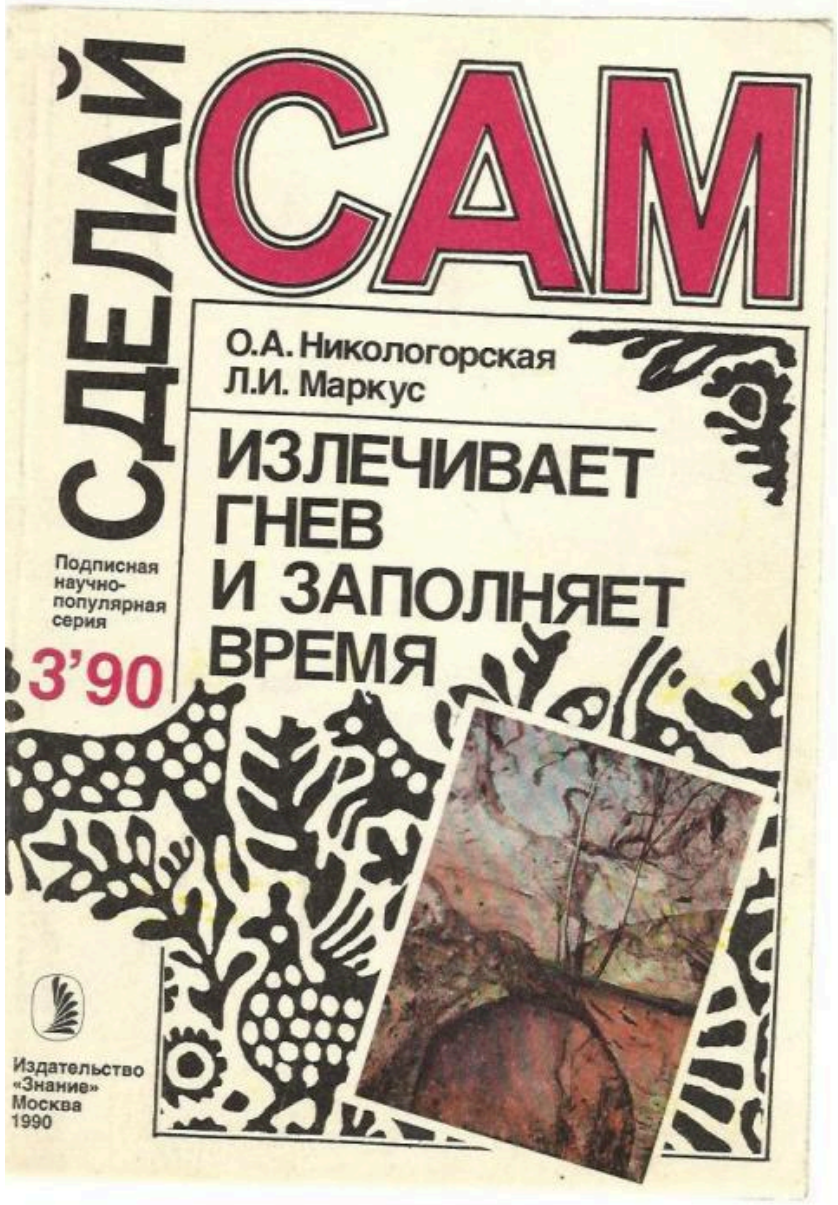
- sbom-updater
  - добавление полей ПА и ФБ
  - указание источника зависимости
- sbom-checker
  - проверка репозитория зависимости
  - проверка корректности SBOM'а зависимостей
  - проверка корректности SBOM'а образов контейнеров


```
{
  "bom-ref": "pkg:deb/debian/netbase@6.4?arch=all&distro=debian-12.11",
  "type": "library",
  "supplier": {
    "name": "Marco d'Itri <md@linux.it>"
  },
  "name": "netbase",
  "version": "6.4",
  "licenses": [
    {
      "license": {
        "id": "GPL-2.0-only"
      }
    }
  ],
  "purl": "pkg:deb/debian/netbase@6.4?arch=all&distro=debian-12.11",
  "properties": [
    {…
    },
    {…
    },
    {
      "name": "GOST:attack_surface",
      "value": "no"
    },
    {
      "name": "GOST:security_function",
      "value": "no"
    }
  ]
```

Сделай сам

- Комбинирование инструментов
- Написание инструментов
- Скрипты и прочие "костыли"


```
{
  "image": "registry/luntry/3dparty/redis:7.2.11-distroless",
  "timestamp": "2026-03-12T01:54:40.123376+03:00",
  "image_layer_hash": "GOST R 34.11-2012
        (/tmp/tmp.wZU0kv8YJb) = s256:246f...e924",
  "components": [
    {
      "path": "/usr/lib/x86_64-linux-gnu/libc_malloc_debug.so.0",
      "hash": "s256:ae87...732e3",
      "timestamp": "2026-03-12T01:54:40.137476+03:00"
    }    ,
    {
      "path": "/usr/lib/x86_64-linux-gnu/libdl.so.2",
      "hash": "s256:8b24...7ed19",
      "timestamp": "2026-03-12T01:54:40.141897+03:00"
    }    ,
    {
      "path": "/usr/lib/x86_64-linux-gnu/libssl.so.3",
      "hash": "s256:dce4...02057",
      "timestamp": "2026-03-12T01:54:40.155545+03:00"
    }    ,
```

Вместо заключения

- SBOM это непросто

Вместо заключения

- SBOM это непросто
- Правильный SBOM ещё сложней

Вместо заключения

- SBOM это непросто
- Правильный SBOM ещё сложней
- Избавляемся от неизвестности всеми доступными способами

Вместо заключения

- SBOM это непросто
- Правильный SBOM ещё сложней
- Избавляемся от неизвестности всеми доступными способами
- Доверяй, но проверяй

Вместо заключения

- SBOM это непросто
- Правильный SBOM ещё сложней
- Избавляемся от неизвестности всеми доступными способами
- Доверяй, но проверяй
- Подходы на базе "статики" позволяют защититься только от легитимного пользователя, но не являются никакой помехой для вредоносного

Вместо заключения

- SBOM это непросто
- Правильный SBOM ещё сложней
- Избавляемся от неизвестности всеми доступными способами
- Доверяй, но проверяй
- Подходы на базе "статики" позволяют защититься только от легитимного пользователя, но не являются никакой помехой для вредоносного
- Делая статику не забывайте о динамике

Спасибо за внимание!

site: luntry.ru

tg: @rusdacent

channel: @tech_b0lt_Genona

Вопросы?