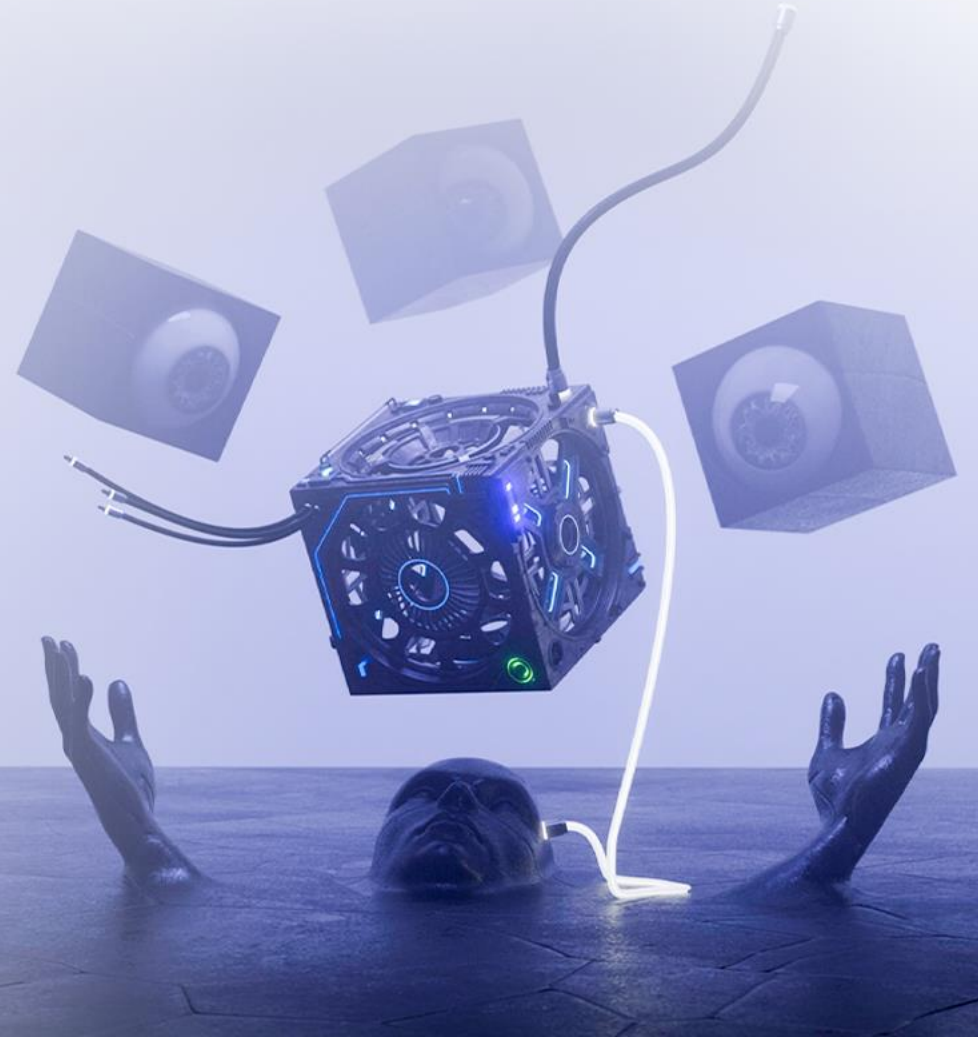
ON FF ONE 2023

How we generated SBOM and what came of it

Artsem Kadushko

Application Security Lead

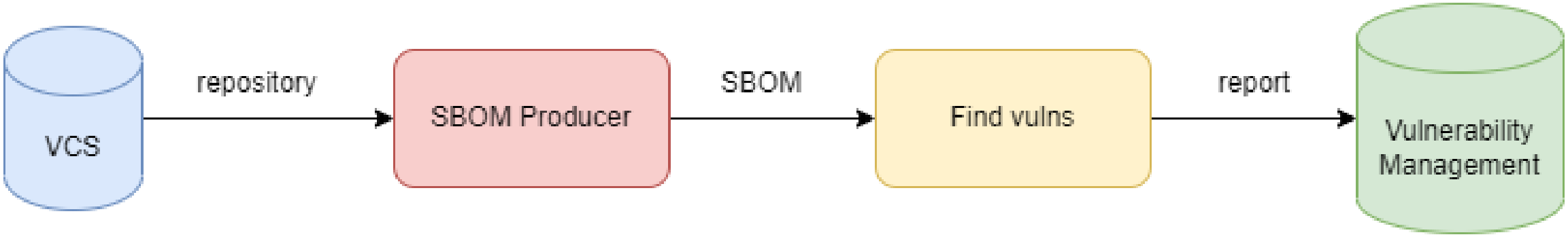


@herrlestrate

Who am I?

- Head of Bulba Hackers
- Application Security Lead
- Certified Pentester (OSCP)
- Bug Bounty Hunter
- Belarussian infosec influencer

Problem – how to generate SBOM



Why we chose SBOM?

- A certain level of abstraction. We can separate the tasks of SBOM generation and its enrichment.
- Once generated SBOM - reuse. Solves an issue with resource inventory in the prod.
- SBOM is a new trend that is gaining popularity. Many vendors allow you to generate / use SBOM for enrichment.
- The evolution of the SCA process performance metric. It used to be “number of vulnerabilities”, now it’s “number of dependencies”.

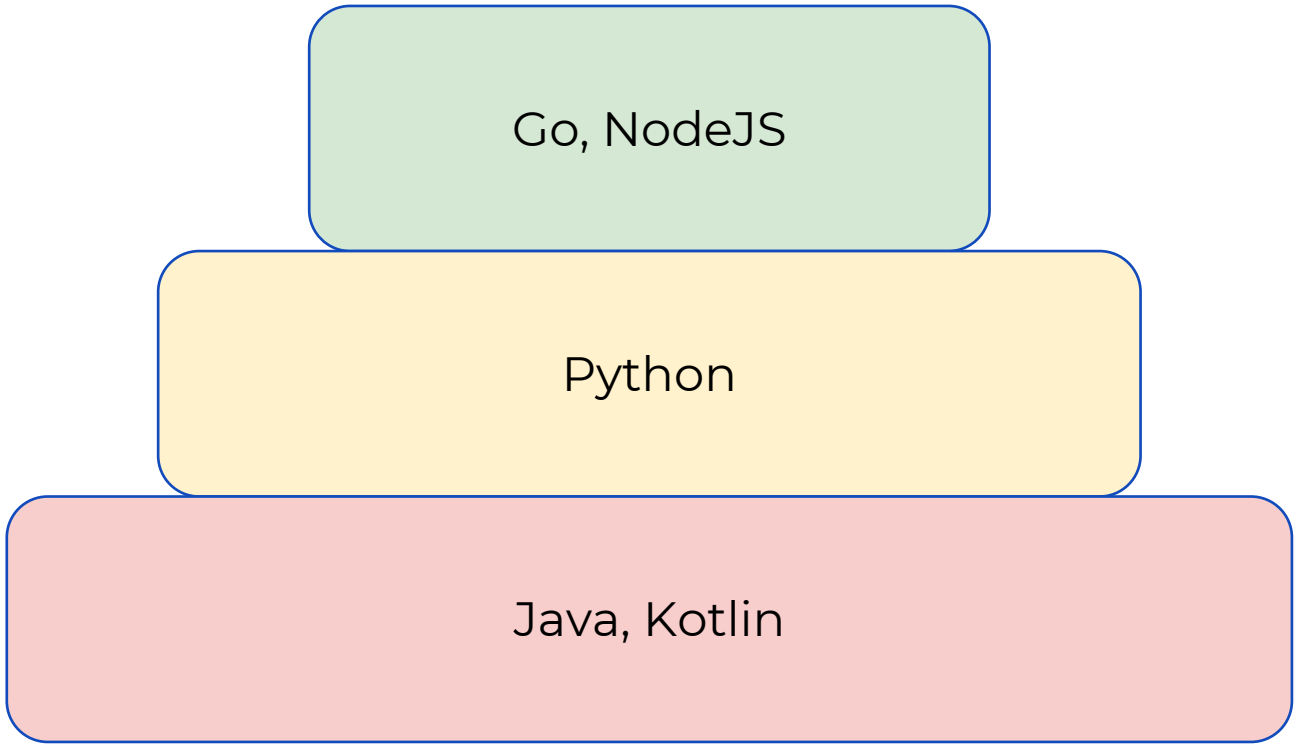
First solution – Trivy!

- Scanner for: vulnerabilities, misconfigurations, secrets and etc.
- Support for a large number of programming languages.
- SBOM format support (CycloneDX, SPDX) + SBOM enrichment feature.
- Easy to use, easy to integrate into the pipeline.

Why not Trivy?

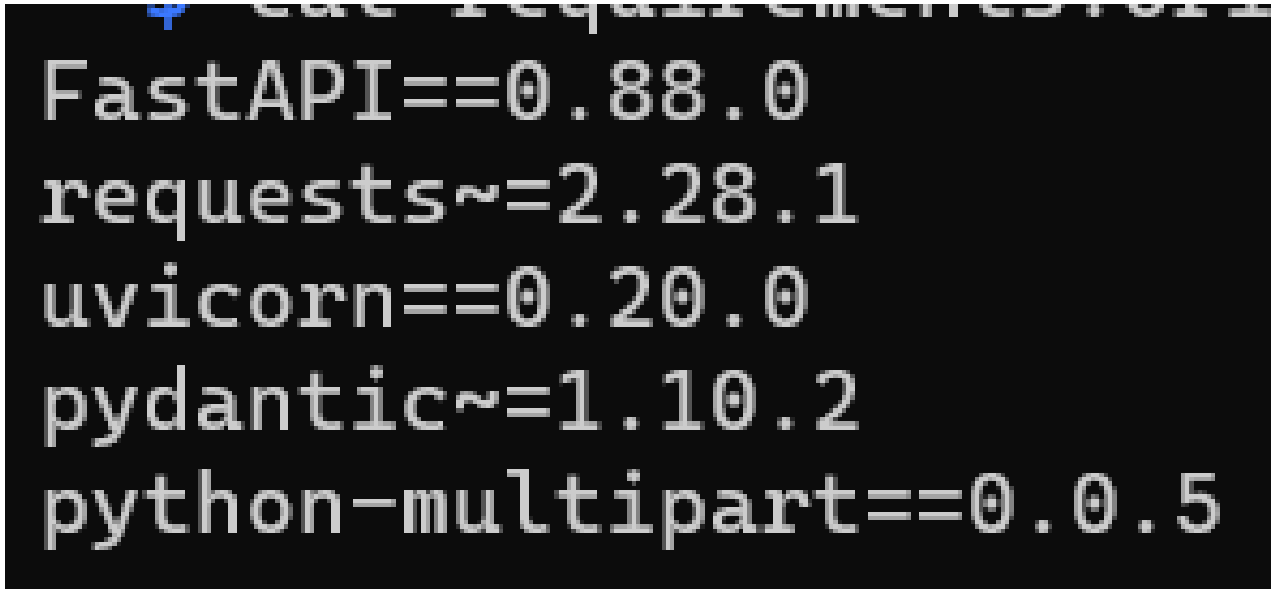
- Requires additional actions with the project before generating the SBOM (In most cases).
- No support for dependency graphs (in some languages with version < 0.42)
- Results for Java/Kotlin are poor

Dependencies enumeration complexity levels



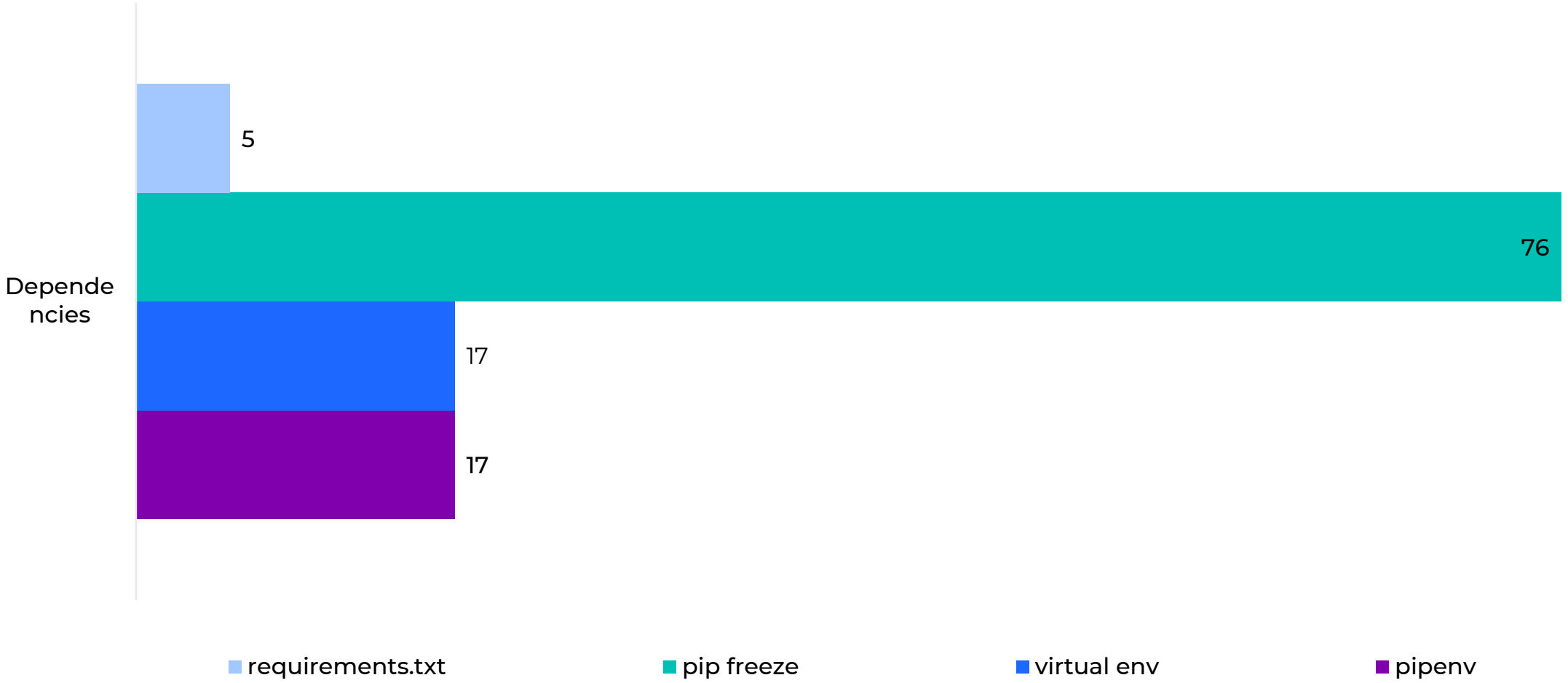
Different Approaches to enumerate dependencies (Python)

- Clear requirements.txt
- Requirements.txt generated by **pip freeze**
- Requirements.txt generated by pip freeze + **venv**
- Requirements.txt generated by **pipenv**



Requirements.txt

SBOM for Python



Next choice – cyclonedx tools

- Generates SBOM in the cyclonedx standard.
- Each package manager has its own plugin
- There is an analogue of Trivy in the world of cyclonedx - cdxgen
- Building Dependency Graph works

Why not cyclonedx tools?

- Not all package managers have plugins
- Some plugins requires additional actions like Trivy
- Issue 109 and so on

Gradle 7.1 [Android] Execution failed for task ':app:cyclonedxBom'. #109

Open gitWK86 opened this issue on Feb 7, 2022 · 3 comments

gitWK86 commented on Feb 7, 2022 • edited

os

Android Studio 2021.1.1 version
gradle 7.1.1
java version "11.0.7" 2020-04-14 LTS

details

The demo project failed to obtain dependencies,
The configuration is as follows

No problem after replacing with gradle version 4.2.2.....

build.gradle in the root directory

```
// Top-level build file where you can add configuration options common to all sub-projects/modules.
plugins {
    id 'com.android.application' version '7.1.1' apply false
    id 'com.android.library' version '7.1.1' apply false
```


Assignees
No one assigned

Labels
None yet

Projects
None yet

Milestone
No milestone

Development
No branches or pull requests

Notifications

Our research of solutions

	Trivy	cdxgen	Cyclonedx tool	gemnasium	Custom solution
NodeJS npm	1219 / 150	1483 / 766	- / 594	1329 / 584	- / -
NodeJS yarn	1934 / 496	1950 / 495	- / -	1933 / 495	- / -
Go	243	226	238	229	-
Python	4 / 76	18 / 51	5 / 77	17 / -	- / 143
Java maven	106	203	168	203	-
Java gradle	6	18	249	-	-
Android (clear)	1	0	0	- (107)	116
Android (Kotlin + gradle)	1	0	0	-	302

NodeJS Npm

	Private	Public	Comment
Trivy	1219	150	Missed packages
cdxgen	1483	766	
CycloneDX Tool	-	594	Not worked with some packages without version
gemnasium	1329	584	No Dependency Graph, Missed packages, False Positive Dependencies
Custom solution	-	-	

NodeJS Yarn

	Private	Public	Comment
Trivy	1934	496	+1 dependency -> trivy specific
cdxgen	1950	495	Additional packages from enterprise with old versions
CycloneDX Tool	-	-	No plugin
gemnasium	1933	495	No Dependency Graph
Custom solution	-	-	

Go

	Public	Comment
Trivy	243	100% from go.mod + go.sum
cdxgen	226	
CycloneDX Tool	238	
gemnasium	229	
Custom solution	-	

Python

	Private	Public (DefectDojo)	Comment
Trivy	4	76	Bad results
cdxgen	18	51	18 – special feature of cdxgen
CycloneDX Tool	5	77	Bad Results
gemnasium	17	-	Another image
Custom solution	17	143	Pipfile.lock / pip freeze

Java Maven

	Private	Comment
Trivy	106	Missed packages
cdxgen	203	Best Results
CycloneDX Tool	168	Missed packages
gemnasium	203	Best Results
Custom solution	-	

Java Gradle

	Private	Comment
Trivy	6	
cdxgen	18	
CycloneDX Tool	249	
gemnasium	-	Another image + implement plugin, exit status 1
Custom solution	-	

Android clear

	Public (Default project)	Comment
Trivy	1	
cdxgen	0	
CycloneDX Tool	0	
gemnasium	- (107)	Another image + implement plugin
Custom solution	116	Script + gradle lock file for every subproject + creating SBOM from it

Android (Kotlin + Gradle)

	Private	Comment
Trivy	1	Empty results
cdxgen	-	Exit status 1
CycloneDX Tool	0	Empty results
gemnasium	-	Exit status 1
Custom solution	302	Script + gradle lock file for every subproject + creating SBOM from it

Conclusions

Each tool and programming language is a separate entity, the analysis of which must be approached independently.

The simplest solution is not always the best. Sometimes you gotta know how deep the rabbit hole goes.

SBOM is a new trend in the field of asset inventory (Languages, containers). If you do not use this technology, it's time to pay attention to it.


OFF
ONE
2023