

Operationalizing SBOM

With CycloneDX and Dependency-Track



Niklas Düster

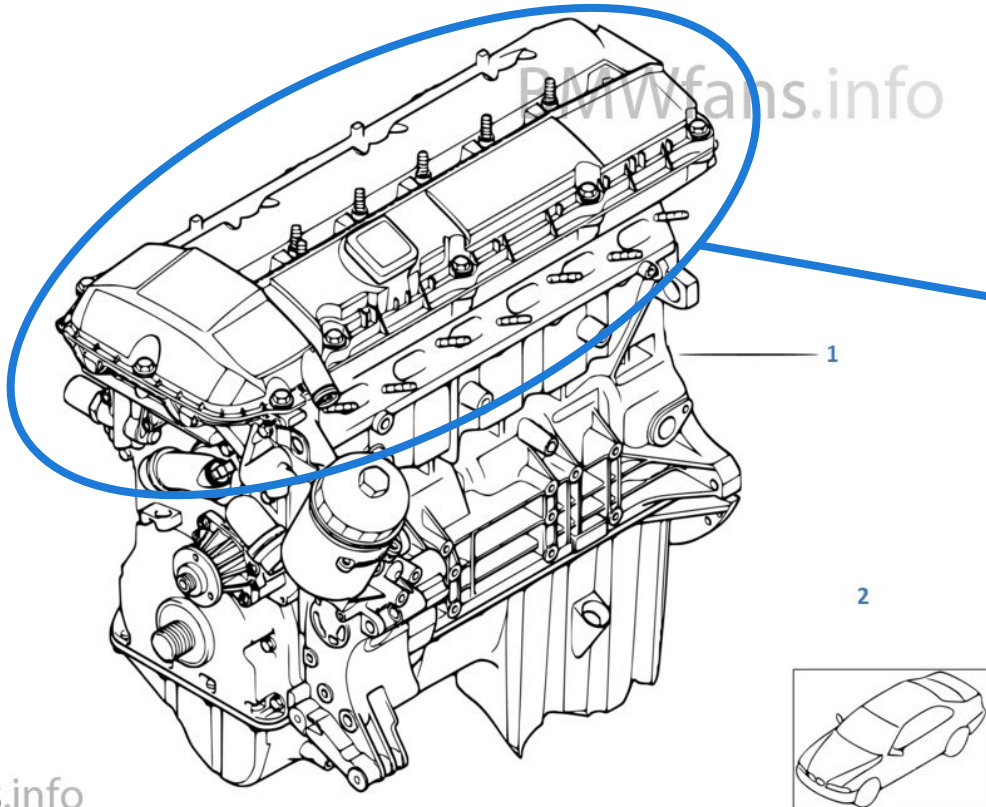
✉ niklas.duester@owasp.org

🐙 github.com/nscuro

🐦 twitter.com/nscuro0

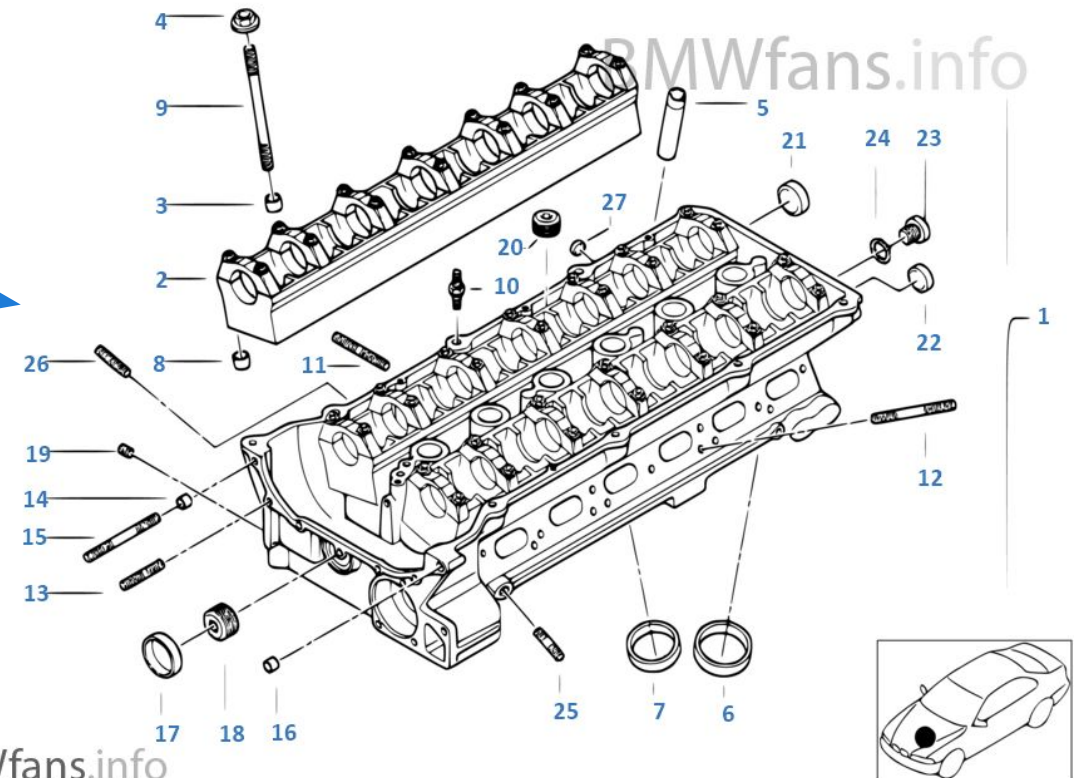
- Security Engineer @ 
- OWASP Dependency-Track Project Co-Lead
- OWASP CycloneDX contributor (I maintain the `go` stuff)

BOM



BMWfans.info

Assembly of the BMW M54 Engine



BMWfans.info

Sub-assembly of the Cylinder Head

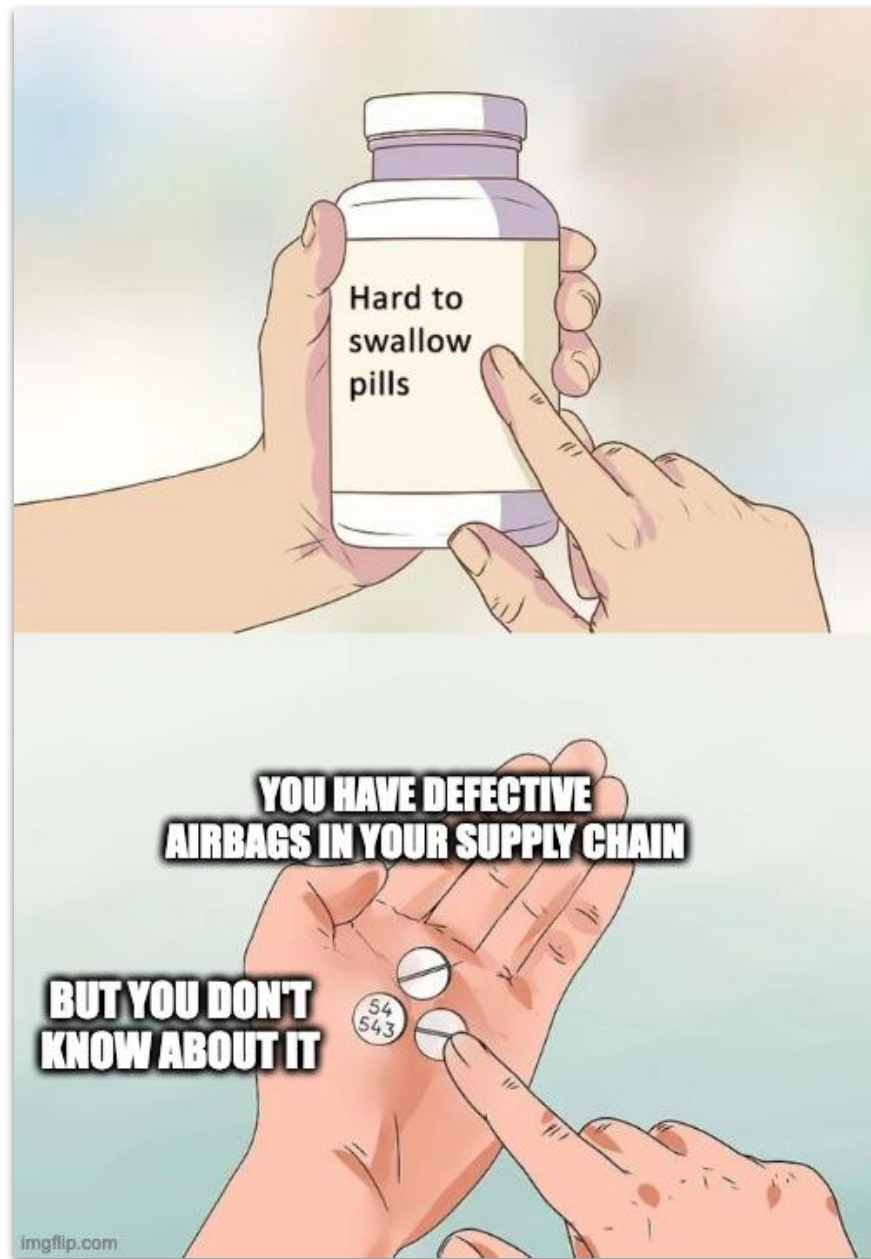
Source: bmwfans.info

IS MY NISSAN AFFECTED?

Due to the defective Takata airbag installed in the models below, you and others in your vehicle are at risk of **serious injury and death** from this problem and we need you to take urgent action.

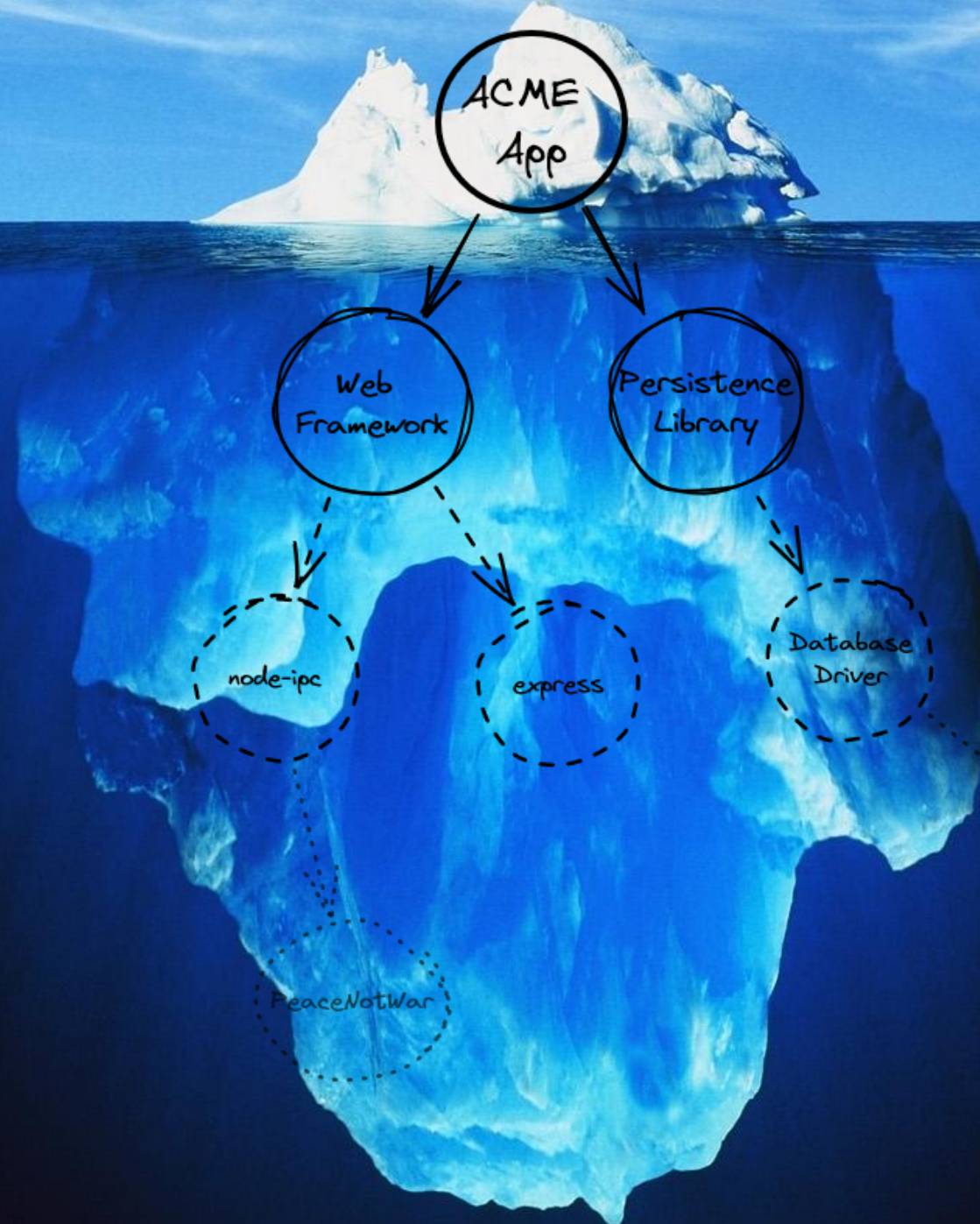
Model	Airbag Affected	Vehicle build date
X-TRAIL (T30)	Passenger	2001-2007
Pulsar Sedan (N16)	Passenger	2001-2005
Pulsar Hatch (N16)	Passenger	2001-2005
Patrol Wagon (Y61)	Passenger	2001-2016
Patrol Cab Chassis (Y61)	Passenger	2006-2016
Navara (D22)	Passenger	2002-2015
Maxima (J31)	Passenger	2003-2008
Navara (D40 Thailand build)	Driver & Passenger	2007-2015
Tiida (C11 Thailand build)	Driver & Passenger	2006-2012

Source: www.nissan.com.au



97%

of commercial codebases contain OSS¹



78%

of code in commercial codebases is made up of OSS¹

[1] Synopsys 2022 Open Source Security and Risk Analysis Report

SBOM



BRIEFING ROOM

Executive Order on Improving the Nation's Cybersecurity

MAY 12, 2021 • PRESIDENTIAL ACTIONS

Elements of SBOM

Bare Minimum¹

- ✓ Supplier Name
- ✓ Component Name & Version
- ✓ Other Unique Identifiers
- ✓ Dependency Relationships
- ✓ SBOM Author
- ✓ Timestamp

We probably also want

- ✓ Hashes
- ✓ Licenses
- ✓ Provenance
- ✓ Pedigree
- ✓ (Much, much more tbh)

[1] [ntia.gov/files/ntia/publications/sbom_minimum_elements_report.pdf](https://www.ntia.gov/files/ntia/publications/sbom_minimum_elements_report.pdf)

This is not an SBOM talk



**SBOM SmackDown: Conquer Dragons
in the Shadows with OWASP CycloneDX**
Steve Springett @ OWASP AppSec USA 2021
[youtube.com/watch?v=vNpj6ogou9U](https://www.youtube.com/watch?v=vNpj6ogou9U)

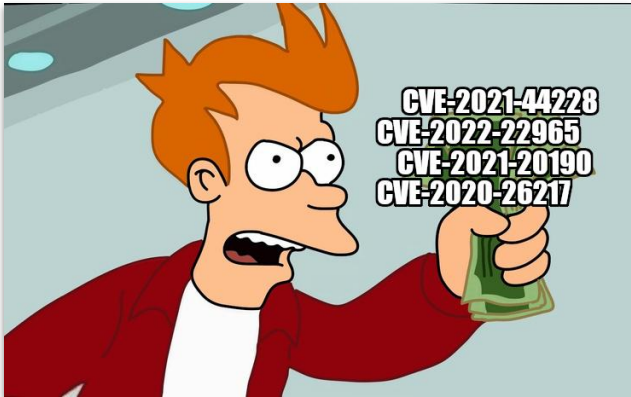
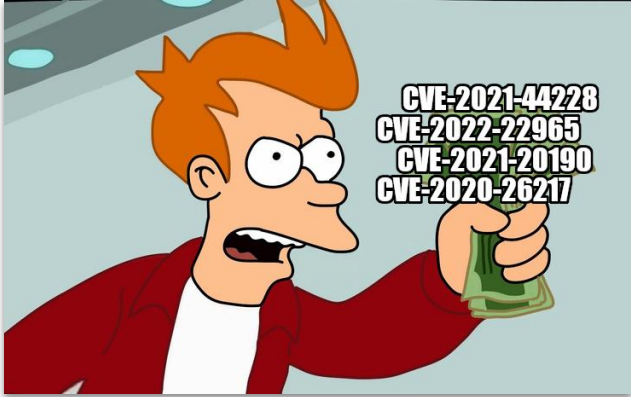
So we share SBOMs now

ACME App 1.0.0

- acme-web-framework 3.1.4
 - spring-web 5.3.7
 - spring-core 5.3.7
 - acme-logging 0.4.0
 - log4j-core 2.14.1
- acme-persistence-framework 1.1.0
 - hibernate-core 5.6.9.Final
- guava 30.0-jre

SBOM of ACME App

So we share SBOMs now



ACME App 1.0.0

- acme-web-framework 3.1.4
- spring-web 5.3.7
 - spring-core 5.3.7
- acme-logging 0.4.0
- log4j-core 2.14.1
- acme-persistence-framework 1.1.0
- hibernate-core 5.6.9.Final
- guava 30.0-jre

SBOM of ACME App



(1) A certification that each item listed on the submitted bill of materials is free from all known vulnerabilities or defects affecting the security of the end product or service identified in--

(A) the National Institute of Standards and Technology National Vulnerability Database; and

(B) any database designated by the Under Secretary, in coordination with the Director of the Cybersecurity and Infrastructure Security Agency, that tracks security vulnerabilities and defects in open source or third-party developed software.

Source: [congress.gov/bill/117th-congress/house-bill/7900](https://www.congress.gov/bills/117/congress/house-bills/7900)



VEX

Minimum Elements of VEX

- ✓ **Metadata.** *What is this? Who created this and when?*
- ✓ **Product Details.** *What product are we talking about?*
- ✓ **Vulnerability Details.** *Which vulnerability are we talking about?*
- ✓ **Vulnerability Status.** *Is the product affected? Do I have to do something about it?*



[Vulnerability Exploitability eXchange \(VEX\) – Use Cases
cisa.gov/sites/default/files/publications/VEX_Use_Cases_April2022.pdf](https://cisa.gov/sites/default/files/publications/VEX_Use_Cases_April2022.pdf)

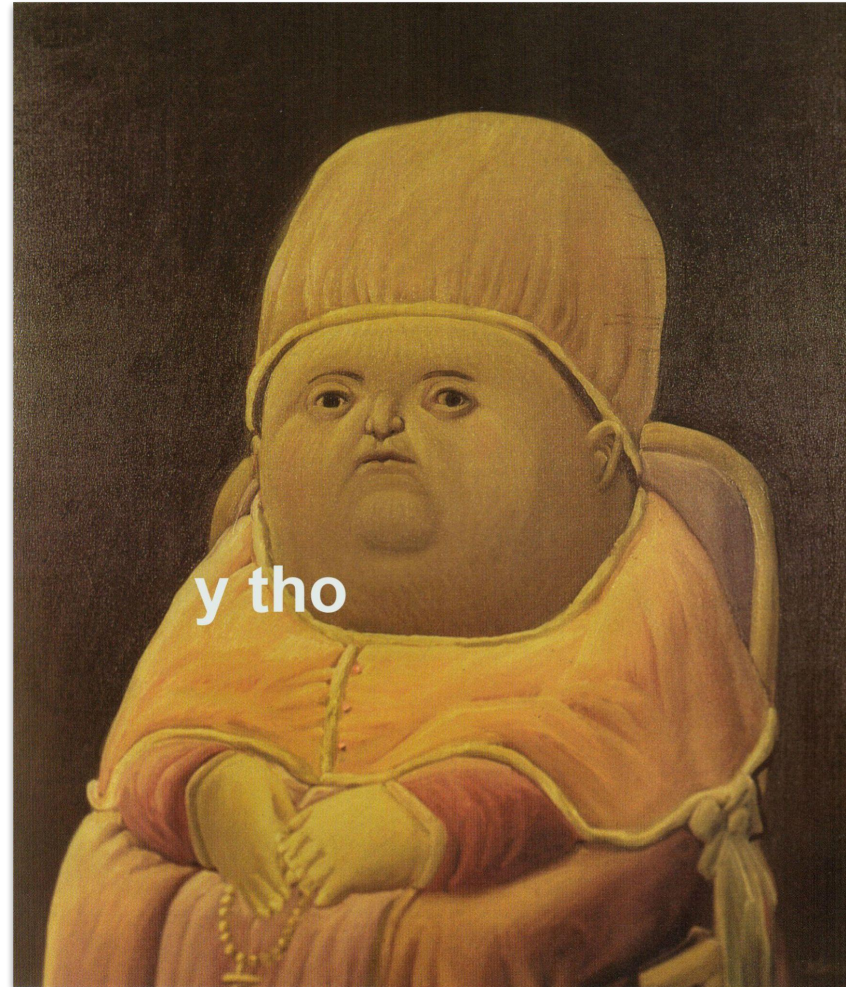
Affected not?



- ☠️ Affected
- 👉 Not Affected
- ✅ Fixed
- 🚧 Under Investigation

Source: cisa.gov/sites/default/files/publications/VEX_Use_Cases_April2022.pdf

Not affected?



✗ Uhh, uhm, so, I mean, ...

✗ Dave said so, but he's on vacation right now

✗ Just trust me OK, why would I lie?

- ✓ Component not present
- ✓ Vulnerable code not present
- ✓ Vulnerable code not in execution path
- ✓ Vulnerable code not controllable by adversary
- ✓ Inline mitigations exist

Source: [cisa.gov/sites/default/files/publications/VEX_Status_Justification_Jun22.pdf](https://www.cisa.gov/sites/default/files/publications/VEX_Status_Justification_Jun22.pdf)



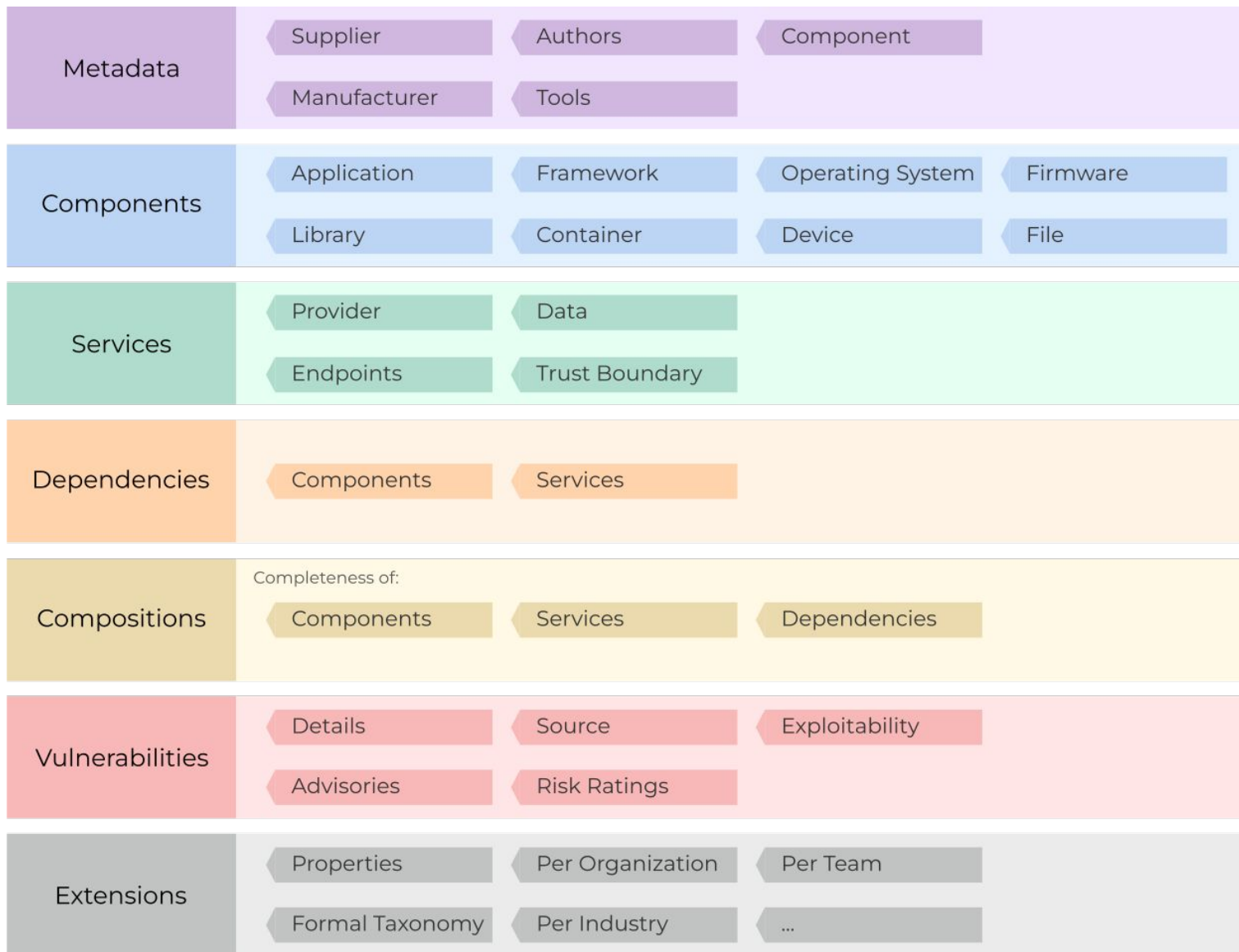
CycloneDX

- Bill of Materials Standard for Cybersecurity Use Cases
 - ✓ Lightweight: Simplicity > Complexity
 - ✓ Optimized for Automation
- Lead by Steve Springett, Patrick Dwyer, Jeffry Hesse

 OWASP Standards Flagship Project

 Recommended by multiple government orgs worldwide

 Used in production at an estimated 100k organizations



High-level data model of CycloneDX

Source: cyclonedx.org

cyclonedx.org

CycloneDX GETTING STARTED SPECIFICATION ABOUT

Use Cases

The following examples provide guidance as to the minimal fields required to achieve specific use cases. Ideally, all optional fields would be populated in order to achieve all use cases. Many of the cases highlighted are directly or closely related to security.

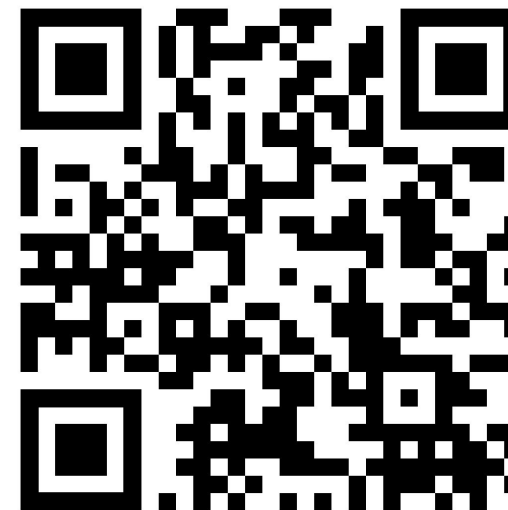
Inventory

A complete and accurate inventory of all first-party and third-party components is essential for risk identification. BOMs should ideally contain all direct and transitive components and the dependency relationships between them.

CycloneDX is capable of describing the following types of components:

COMPONENT TYPE	CLASS
Application	Component
Container	Component
Device	Component
Library	Component

- Inventory
- Known vulnerabilities
- Integrity verification
- Authenticity
- Package evaluation
- License compliance
- Assembly
- Dependency graph
- Provenance
- Pedigree
- Service definition
- Properties / name-value store
- Packaging and distribution
- Composition completeness
- OpenChain conformance
- Vulnerability remediation



[CycloneDX Use Cases](https://cyclonedx.org/use-cases/)
cyclonedx.org/use-cases/

CycloneDX GETTING STARTED SPECIFICATION ABOUT

Tool Center

All tools 143 Open Source 111 Proprietary 34 Build Integration 59 Analysis 45 Author 2 GitHub Action 12 Transform 7

Library 9 Signing / Notary 5 Distribute 4

Apiiro
Apiiro
Apiiro enables security & development teams to proactively remediate critical risks in their cloud-native applications such as design flaws, secrets, IaC misconfigurations, API & OSS vulnerabilities across the software supply chain.

AppSonar
CyberTest
AppSonar Static Code Analyzer helps improve the security and quality of application code and can generate CycloneDX BOMs during analysis.

Auditjs
Sonatype
Audits an NPM package.json file to identify known vulnerabilities

BOM Repository Server
CycloneDX
A lightweight repository server used to publish, manage, and distribute CycloneDX SBOMs

Black Duck
Synopsys
Black Duck software composition analysis (SCA) helps teams manage the security, quality, and license compliance risks that come from the use of open source and third-party code in applications and containers.

BlackBerry Jarvis
BlackBerry
Software composition analysis (SCA) and security testing solution that detects and list open-source software and software licenses within embedded systems and associated cybersecurity vulnerabilities and exposures



CycloneDX Tool Center
cyclonedx.org/tool-center/





dependency track

- Intelligent Component Analysis Platform
- Ideal for Procurement and ✨ DevSecOps ✨
- Lead by Steve Springett and yours truly 🙌🕶️🙌



OWASP Tools Flagship Project



20B Components Analyzed each Month



>7M Docker Pulls

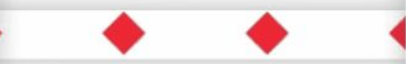
SBOM Production

Generated during CI/CD or acquired from suppliers



SBOM Ingestion

Via REST API, Web Interface, Jenkins Plugin, GitHub Action



SBOM Analysis

Component analysis for security, operational, and license risk



Continuous Monitoring

Continuous analysis of portfolio for risk and policy compliance

Intelligence Streams

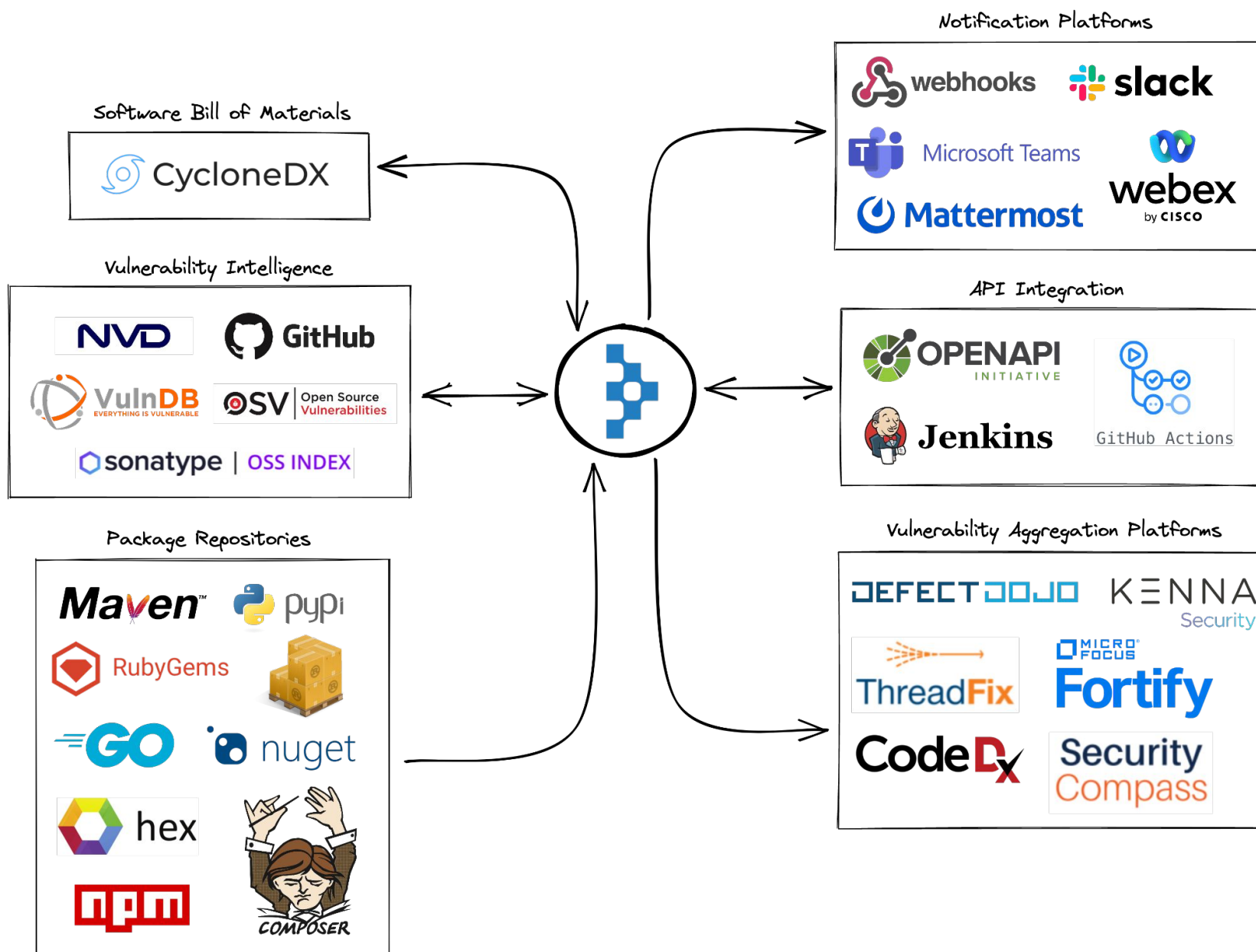
Real-time analysis and security events delivering actionable findings to external systems



Intelligent Response

Events delivered via Webhooks or ChatOps and findings published to risk management and vulnerability aggregation platforms

Demo



Get Involved!

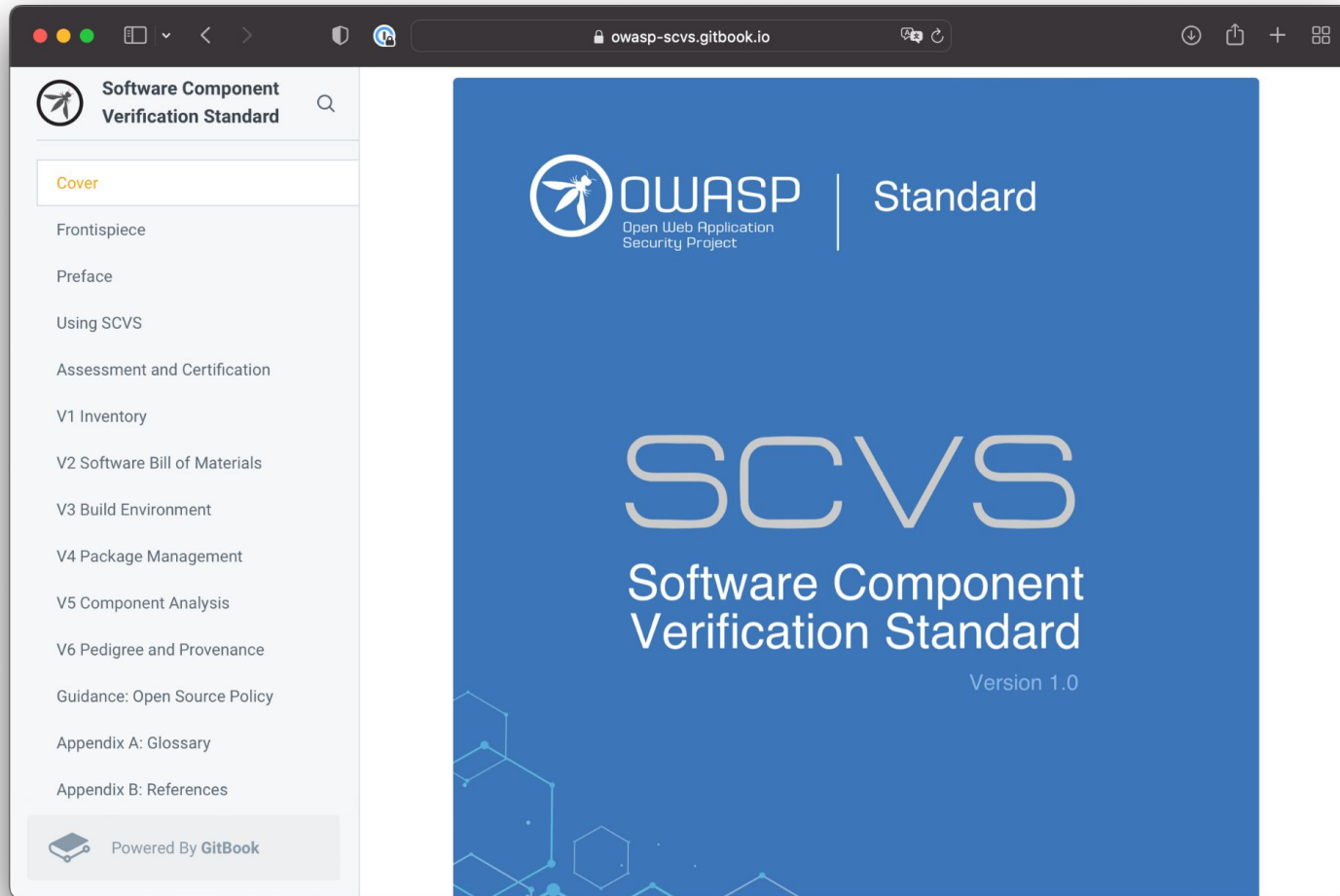


cyclonedx.org/about/participate/



github.com/DependencyTrack/dependency-track/CONTRIBUTING.md

But wait, there is more!



OWASP Software Component Verification Standard
owasp-scvs.gitbook.io/scvs/

Your turn.





OWASP

TM