cerc 2023

The 5Th Cybersecurity Education and Research Conference

Enhancing Supply Chain Risk Management with OWASP CycloneDX and Dependency-Track

Eng. Faisal Albuloushi

OWASP Kuwait Chapter Leader

Supported By

SPONSORED BY KFAS مؤسسة الكويت للتقدم العلمي Kuwait Foundation for the Advancement of Sciences

UK Science & Innovation Network

Organizers

جامعة الكويت Kuwait University

المركز الوطني للأمن السيبراني National Cyber Security Center

British Embassy Kuwait

Agenda

- What is OWASP?
- Supply Chain Risk
- SBOM Definition
- OWASP CycloneDX
- OWASP Dependency-Track
- Recommendations

What is OWASP?

- **OWASP**: **O**pen **W**orldwide **A**pplication **S**ecurity **P**roject
- OWASP is a global community-driven organization dedicated to improving software security.
- Currently, there are (250+) projects under OWASP umbrella. All projects are open source and are built by a community of volunteers.
- OWASP Mission: “To be the global open community that powers secure software through education, tools, and collaboration”

Supply Chain

1. Raw materials
2. manufacture components
3. sub-assemblies
4. logistics and transportation services
5. tooling and equipment
6. software and technology, and more...

Supply Chain *(continued)*

- Example of components and dependencies in the software supply chain:
  1. Libraries
  2. Frameworks
  3. Packages
  4. IDEs
  5. Open-Source Software
  6. Operating Systems
  7. Cloud Services
  8. Third-Party APIs, more...

Supply Chain Risk

- In March 2020, an APT group successfully injected their trojan into a well-known platform's update using supply chain attack.
- More 18,000 clients applied the vulnerable update!
- It took (9) months to detect the breach.
- The same company got compromised again in July 2021 using another supply chain attack!

Supply Chain Risk *(continued)*

- In May 2021, Colonial Pipeline fell victim to supply chain attack that led to ransomware.
- The operation was down for approximately six days!
- The company paid $4.4 million USD as a ransom.
- The U.S. government declared a state of emergency in affected regions. The attack had a significant economic impact.

Supply Chain Risk *(continued)*

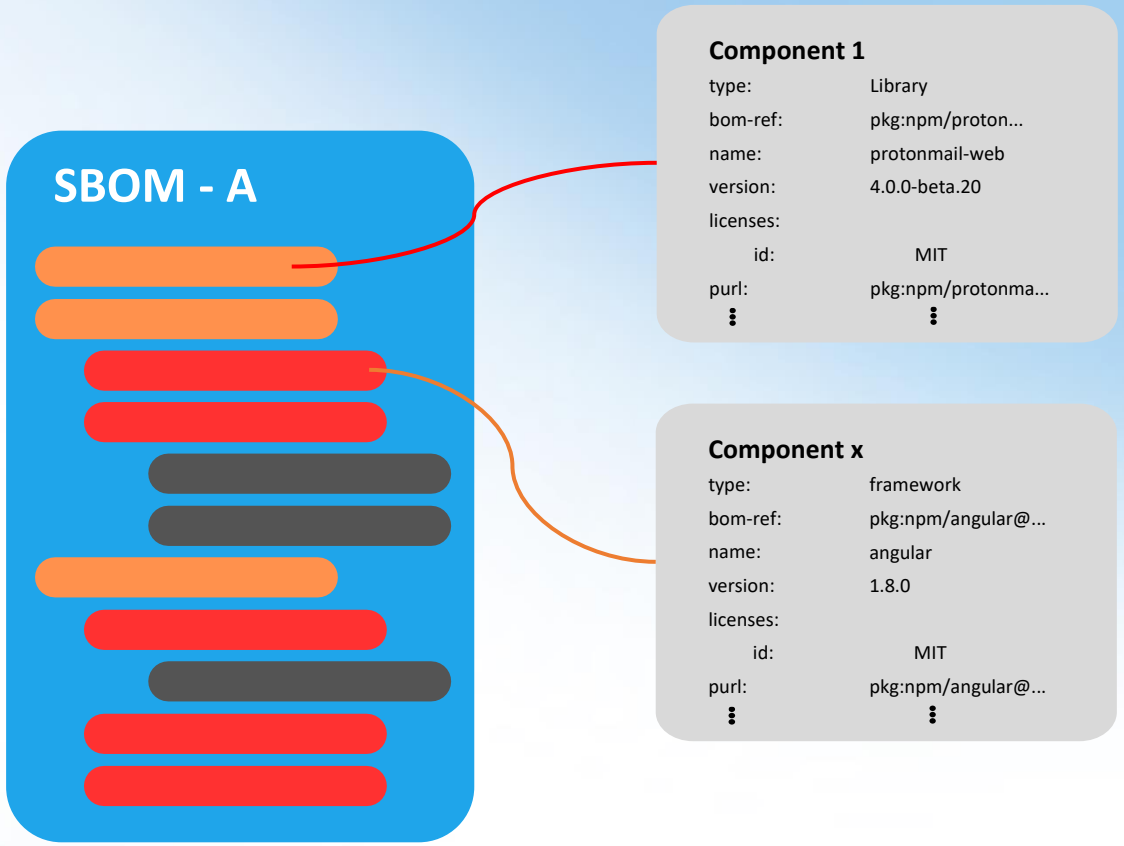
Packages	No. of Vulnerabilities
PyPI	10,999
Npm	12,460
Linux	13,573
NuGet	524

Supply Chain Risk *(continued)*

This component/package is vulnerable to Authentication Bypass!

What is SBOM?

- Definition: “a formal, machine-readable inventory of software components and dependencies, information about those components, and their hierarchical relationships” – NTIA



OWASP CycloneDX

- OWASP CycloneDX is a full-stack Bill of Materials (BOM) standard
  - Software Bill of Materials (SBOM)
  - Software-as-a-Service Bill of Materials (SaaSBOM)
  - Hardware Bill of Materials (HBOM)
  - Machine Learning Bill of Materials (ML-BOM)
  - Manufacturing Bill of Materials (MBOM)
  - Operations Bill of Materials (OBOM)
  - Vulnerability Disclosure Reports (VDR)
  - Vulnerability Exploitability eXchange (VEX)

CycloneDX Tool Centre

- Open Source
- Proprietary
- Specific Languages: Java, PHP, Python, Go ...etc.
- Example “CycloneDX Generator”:
  - Supports most of languages and package formats
  - Supports CI/CD integration
  - Automatically submits the generated BoM to the dependency track server for analysis

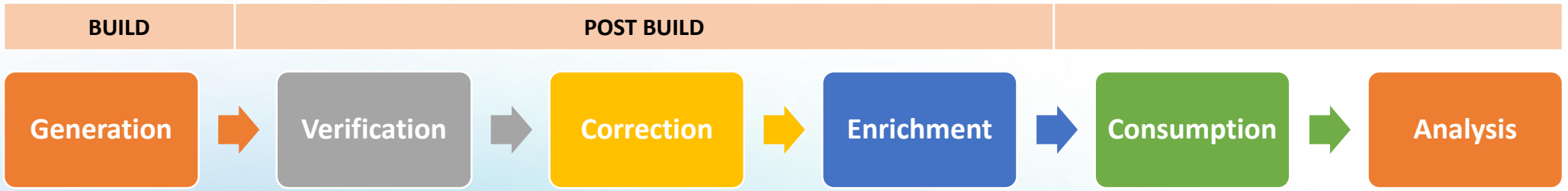
CycloneDX Use Cases

- Inventory
- Known vulnerabilities
- Integrity verification
- Authenticity
- Assembly
- Dependency graph
- Vulnerability exploitability

Generating CycloneDX BOMs

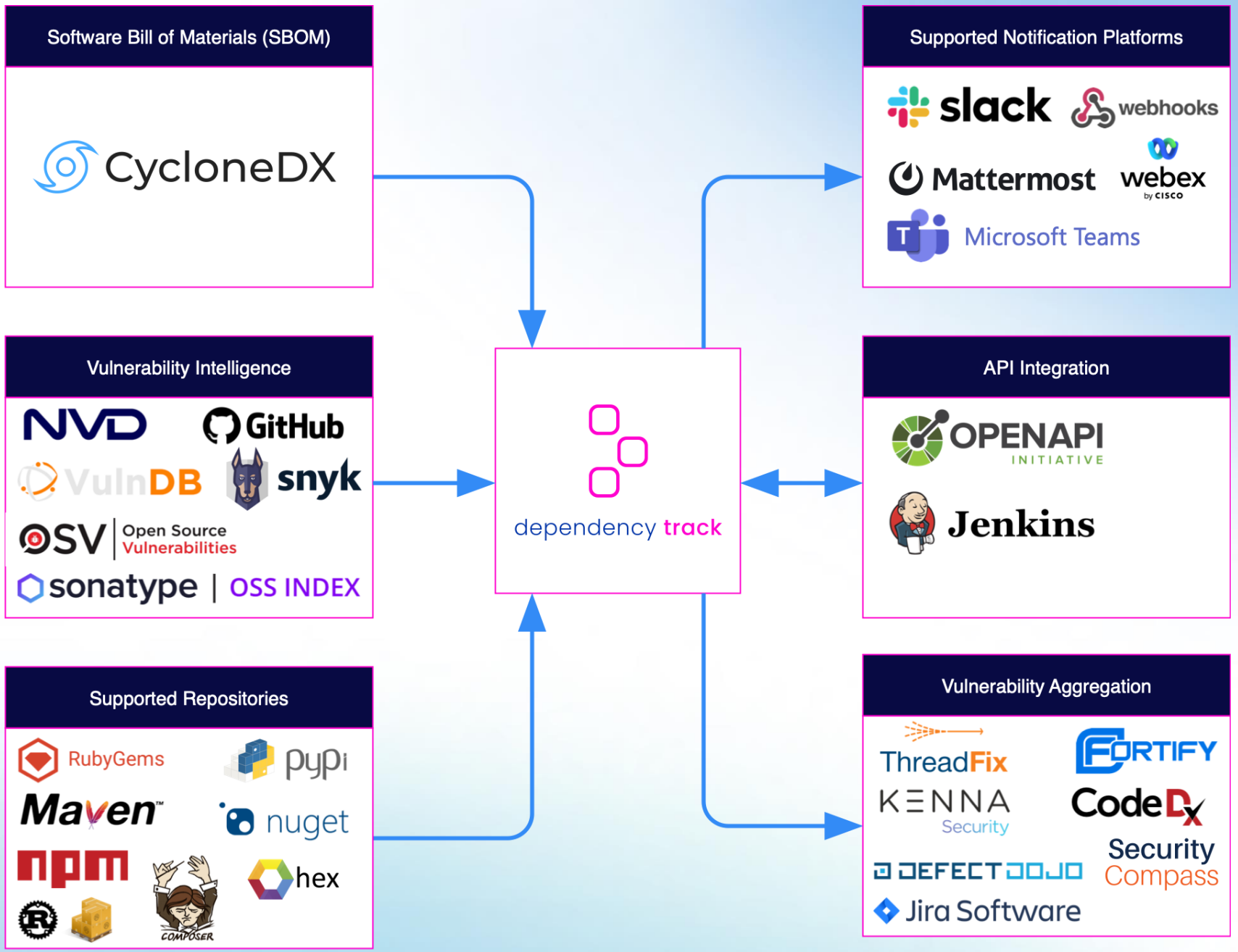
- First adoption process:

- Recommended process:



OWASP Dependency-Track

- Dependency-Track is a component analysis platform that help to identify and reduce risk in the software supply chain.
- Provides detailed insights into project dependencies, including vulnerabilities, licenses, and out-of-date libraries.


Software Bill of Materials (SBOM)
CycloneDX
Supported Notification Platforms
slack
webhooks
Mattermost
webex by cisco
Microsoft Teams
Vulnerability Intelligence
NVD
GitHub
VulnDB
snyk
OSV Open Source Vulnerabilities
sonatype | OSS INDEX
dependency track
API Integration
OPENAPI INITIATIVE
Jenkins
Supported Repositories
RubyGems
pypi
Maven
nuget
npm
hex
COMPOSER
Vulnerability Aggregation
ThreadFix
FORTIFY
KENNA Security
CodeDx
DEFECTDOJO
Security Compass
Jira Software

Recommendations

- Prioritizing supply chain risk management.
- Incorporating SBOM/xBOM within SDLC and Security policies to ensure comprehensive software visibility and enhance security measures.
- Ensuring comprehensive SBOM/xBOM coverage for all software classes (purchased, open source, and in-house).
- Teaching students to integrate SBOM/xBOM for a well-rounded understanding of Supply Chain Risk Management.

Thank you