Vulnerabilities and the Future

Multilayered Software Vulnerabilities and Response Tactics

Riotaro Okada

Update: 2024/11/27
Release: 2/3/2024

Riotaro OKADA

Security researcher in Japan.

(Executive Director of Asterisk Research Inc.

- OWASP Project committer / Japan chapter lead

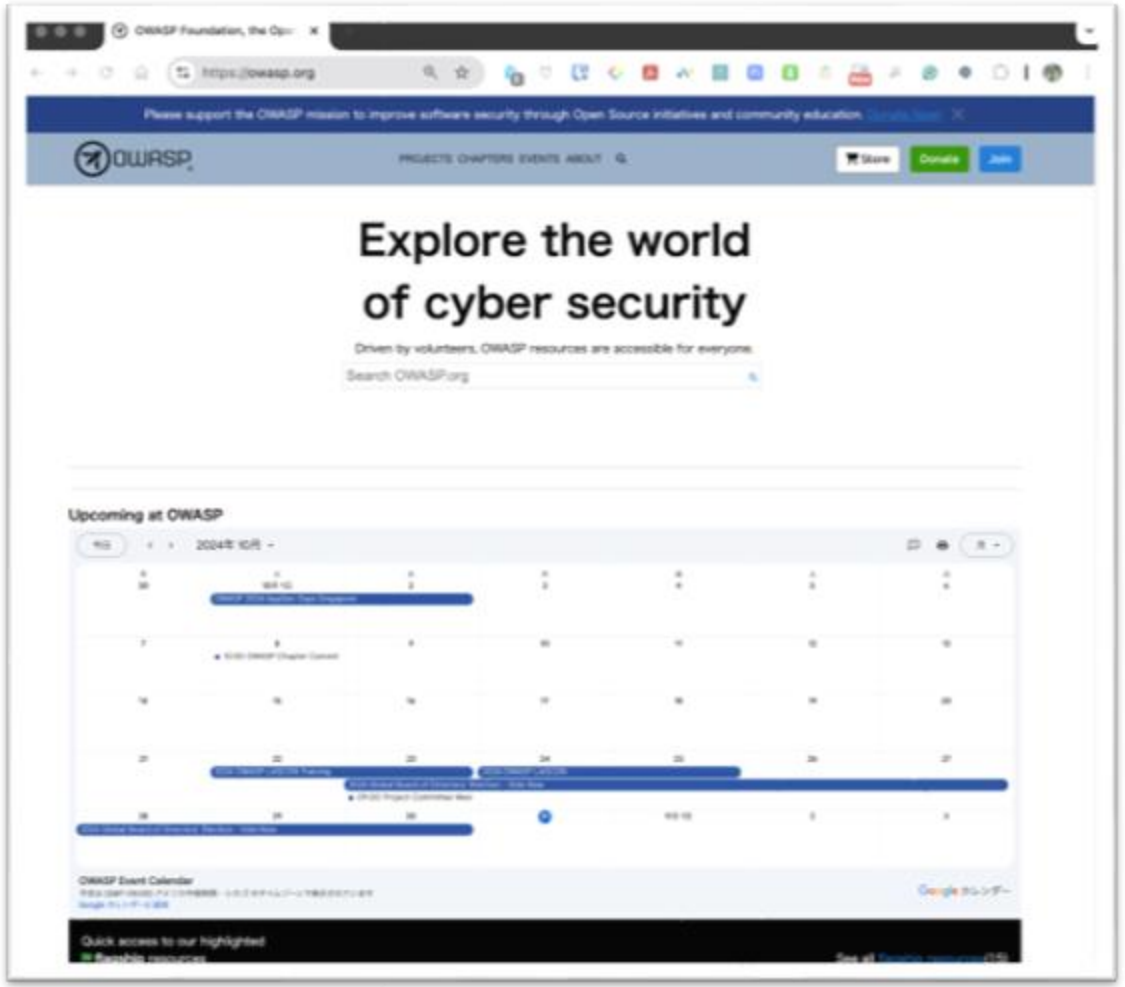
  (Distinguished Lifetime member Award 2024)

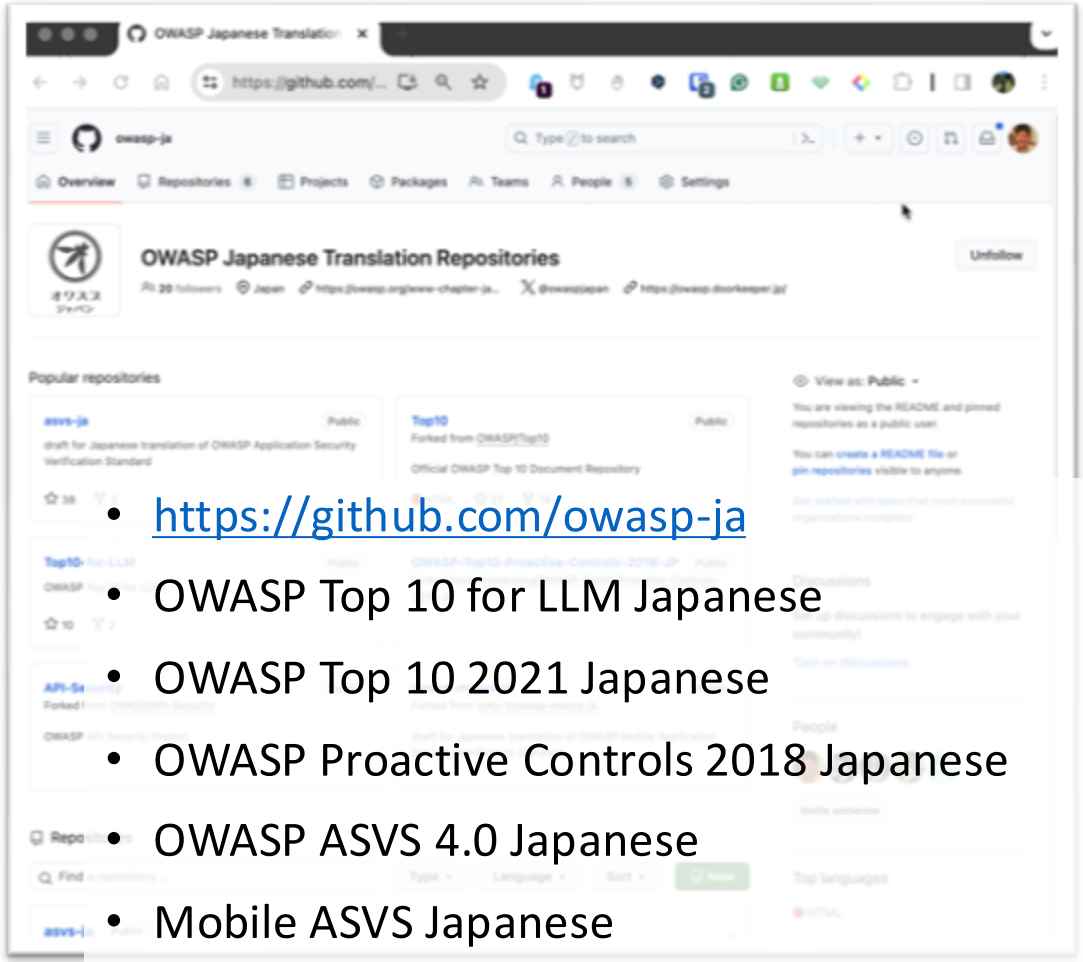
- Hardening Project (Good Design Award 2023)
- Part-time lecturer at BBT University
- Cyber Training CYDER Executive Committee Member
- Members of the writing team for the CISO Handbook, published in January 2021.

OWASP.org / OWASP Japan chapter

Open Worldwide Application Security Project

Github: owasp-en





- https://github.com/owasp-ja
- OWASP Top 10 for LLM Japanese
- OWASP Top 10 2021 Japanese
- OWASP Proactive Controls 2018 Japanese
- OWASP ASVS 4.0 Japanese
- Mobile ASVS Japanese
- OWASP Cheat Sheet List for Developers

About the OWASP Foundation

To be the global open community that powers secure software through education, tools, and collaboration.

Local Chapters

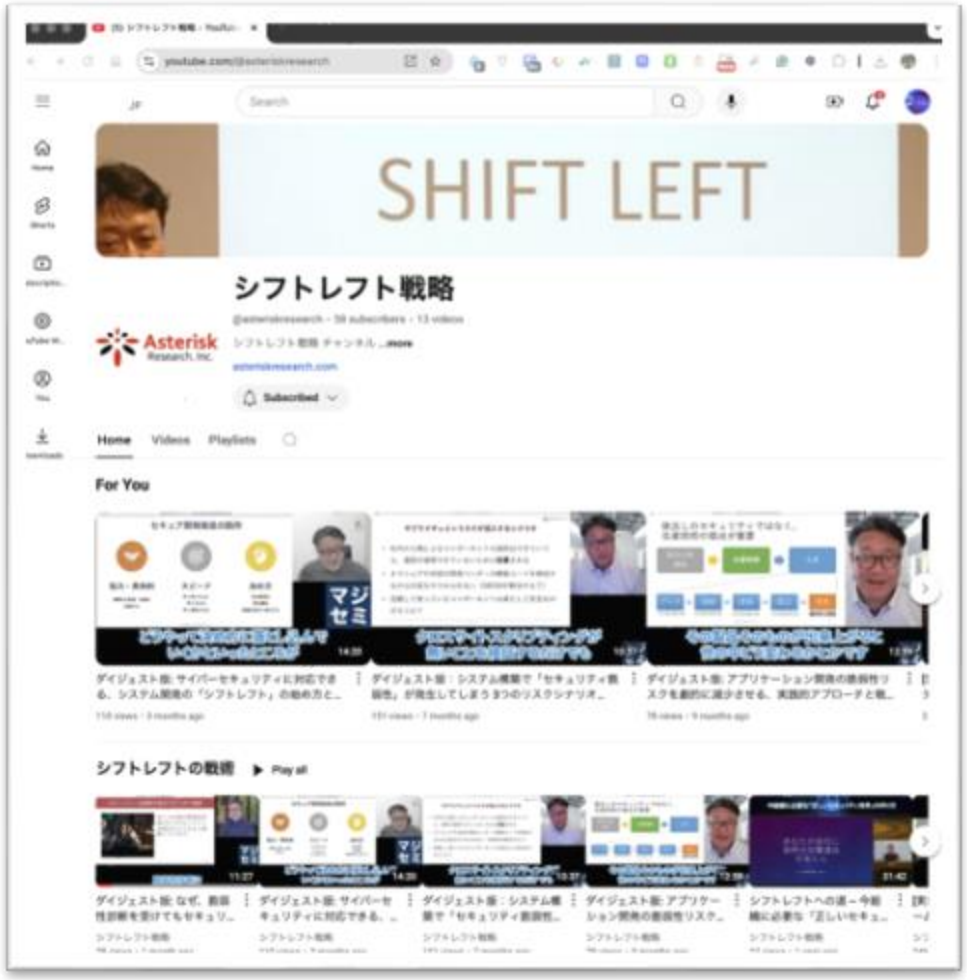
Projects

Events

I've become a youtuber(?)

https://www.youtube.com/watch?v=Rp9uPVahpUw

Maji-Semi: Introduction to Vulnerability



youtube.com/@asteriskresearch

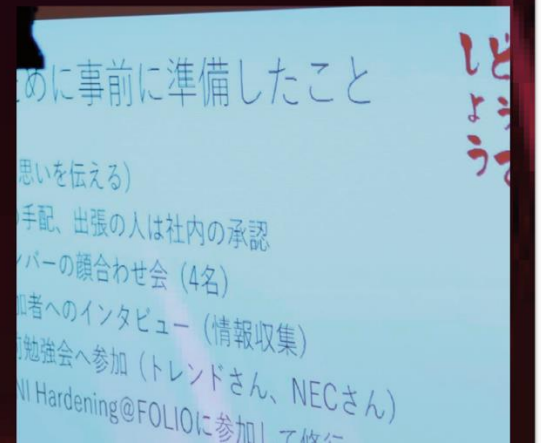
審査ユニット20　一般向けの取り組み・活動
活動審査番号G2005467
事業主体名 ハードニングプロジェクト

Hardening Project

今日突然、あなたの会社に
サイバー攻撃予告が届いたら、どうしますか。

情報収集、被害想定、技術確保、広報、事業継続、防御とバックアップ、集中監視、対応体制、警察・関係省庁との連絡、取引先やお客様への連絡、専門家やベンダーの活用、プレスリリースと記者会見、リスクファイナンス、ハッカー集団との折衝、被害想定、それらすべてに責任をもつ経営者の判断...

「弊社にとってサイバーセキュリティは重要」
被害の経験をしてはじめて、どうすれば良かったのかを理解する



Asterisk Research Security Practice Support Company
asteriskresearch.com

Advisory for fast management decision making

Advisory Service

PSIRT/CSIRT Advisory

DevOps Transformation

Security Scorecard Analysis

Executive Briefing

CISO, CTO, CRO hands-on

Tools to enhance QCD in the practice phase

Professional Tools

Tools for development environment (CI/CD)

Training Design

Risk Profiles

Threat Analysis Training

Software Configuration Management

Services that work from security vulnerability discovery to remediation

Security Test Managed Service

Design Threat Analysis Threat Analysis

Component Analysis SCA

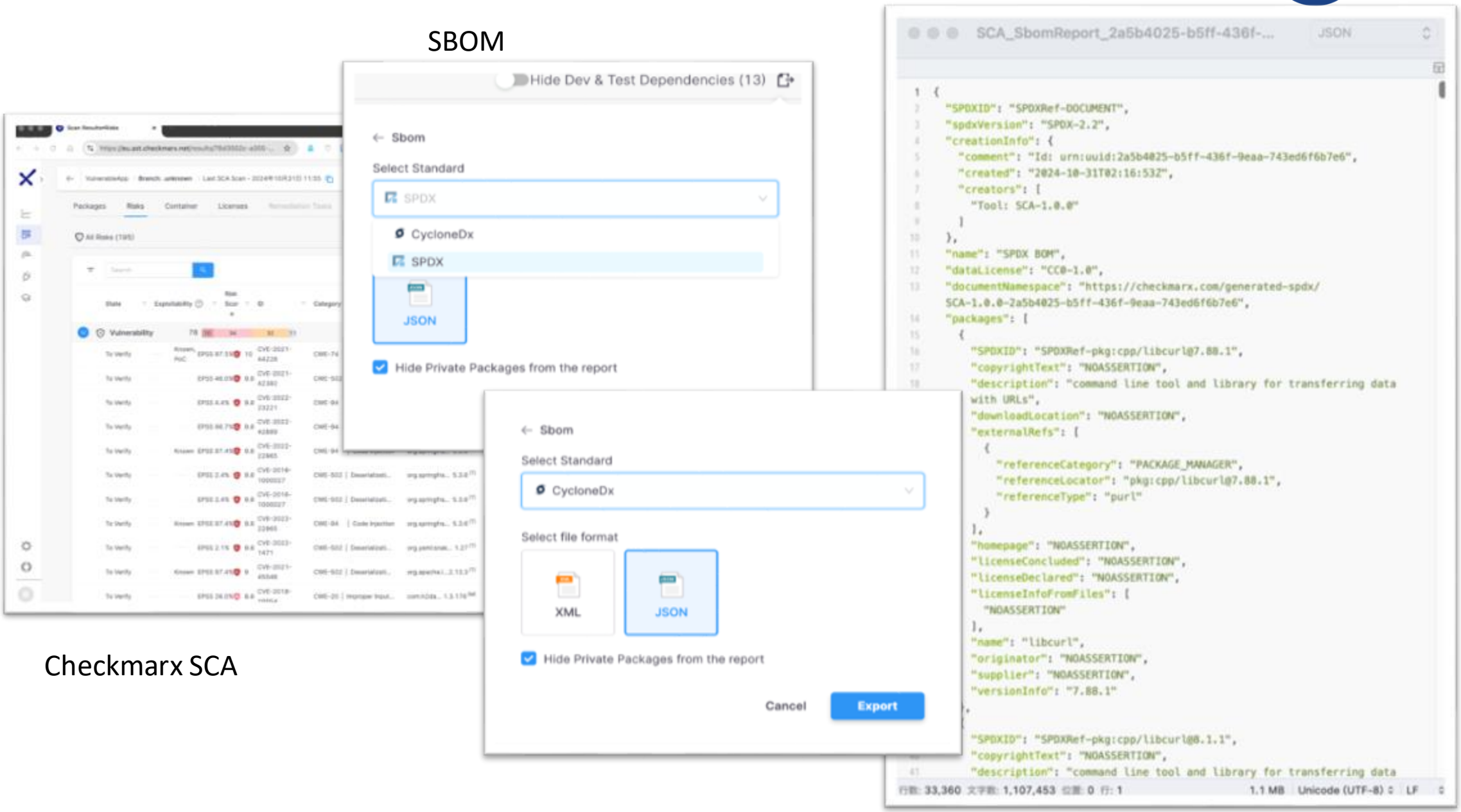
Source code analysis SAST

System Vulnerability Testing DAST

Platform Testing NST

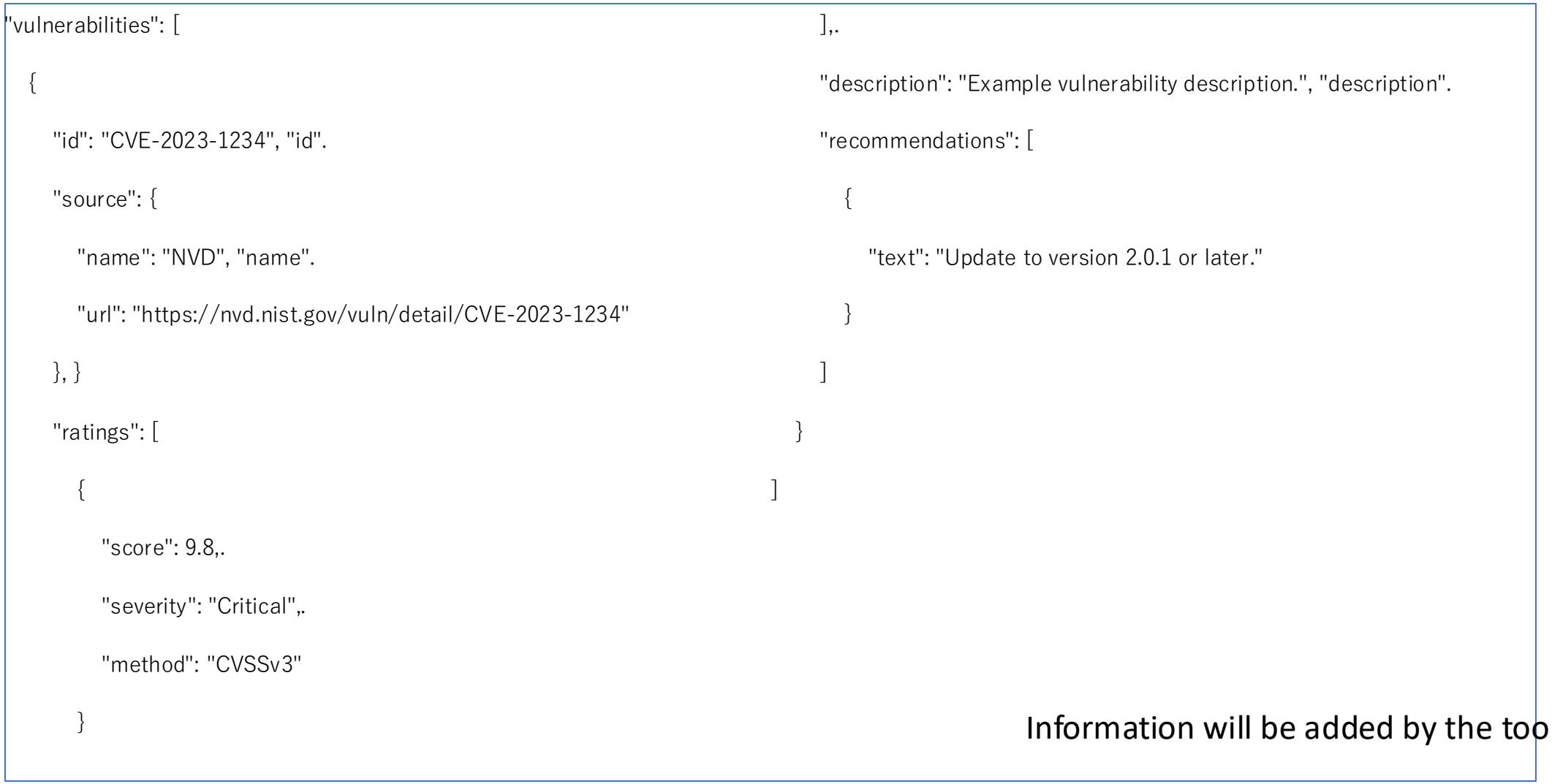
Has the SBOM become familiar to you?

SBOM



Checkmarx SCA

Vulnerabilities section for each component



```
"vulnerabilities": [
  {
    "id": "CVE-2023-1234", "id".
    "source": {
      "name": "NVD", "name".
      "url": "https://nvd.nist.gov/vuln/detail/CVE-2023-1234"
    }, }
    "ratings": [
      {
        "score": 9.8,.
        "severity": "Critical",.
        "method": "CVSSv3"
      }
    ],.
    "description": "Example vulnerability description.", "description".
    "recommendations": [
      {
        "text": "Update to version 2.0.1 or later."
      }
    ]
  }
]
```

Information will be added by the tool.

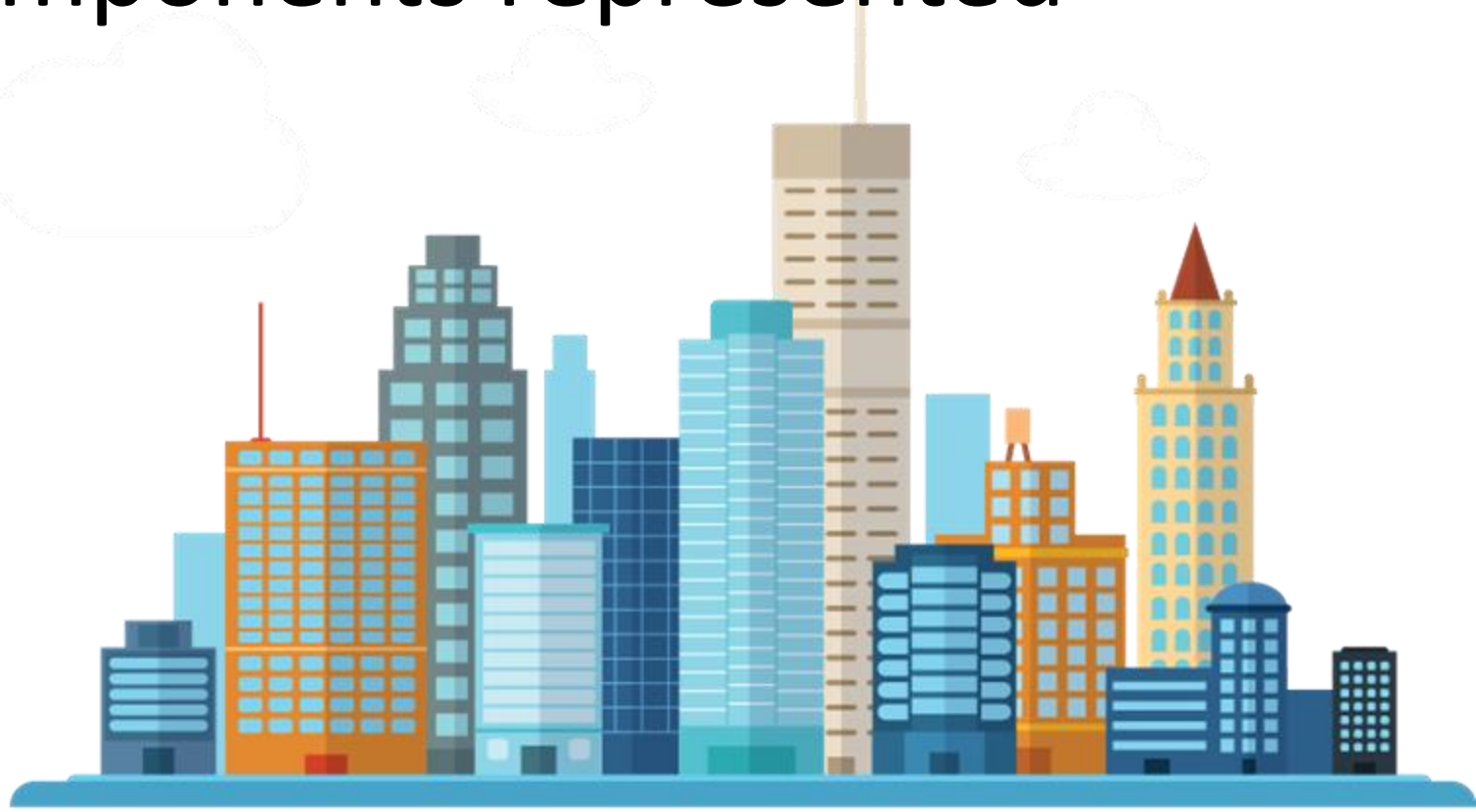
CycloneDX is a Full Stack BOM Standard

Provides advanced supply chain capabilities for cyber risk reduction

In Production!

At an estimated 100K organizations

Over 300-500M components represented monthly



Source: Sonatype
One tool using a single source of vulnerability intelligence
Actual usage much greater

Community Driven

Website

https://cyclonedx.org/

https://owasp.org/cyclonedx

GitHub

https://github.com/CycloneDX

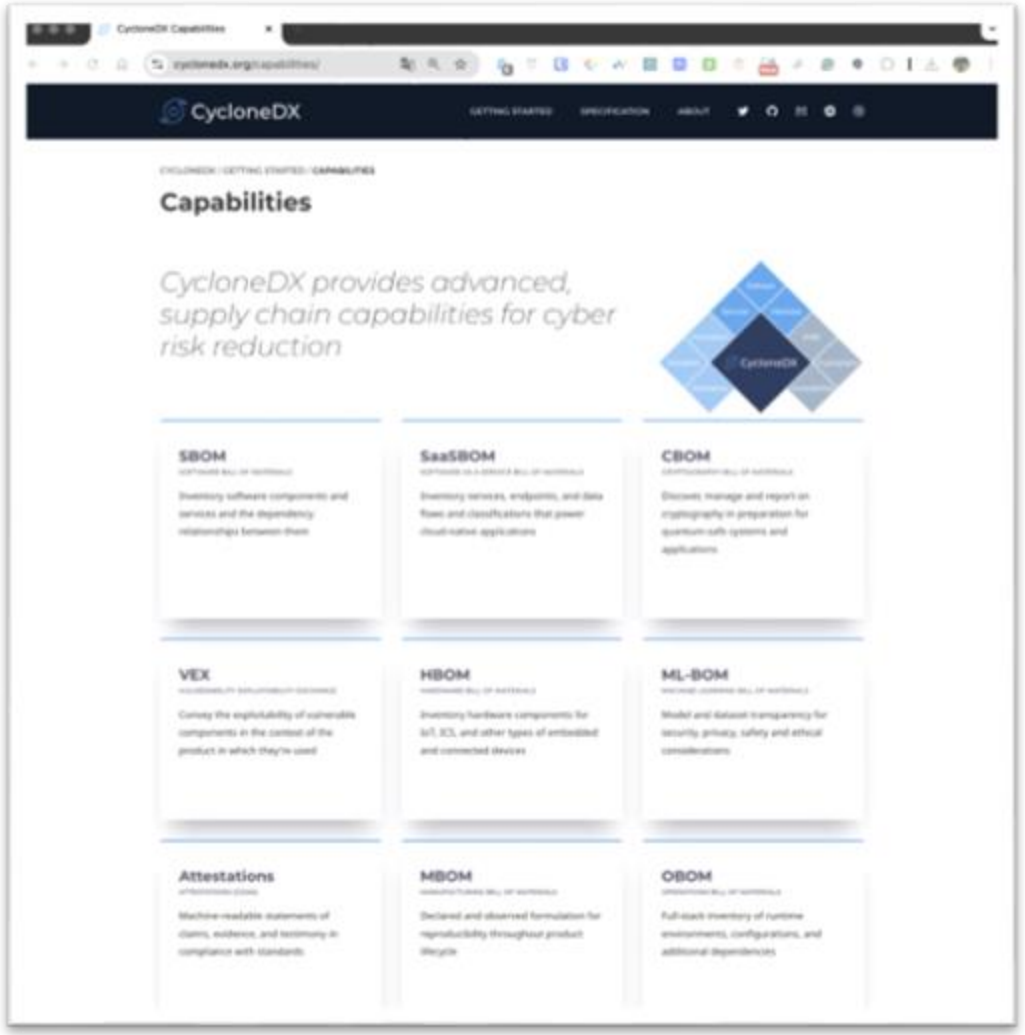
Slack

https://cyclonedx.org/slack

https://cyclonedx.org/slack/invite

Introducing CycloneDX

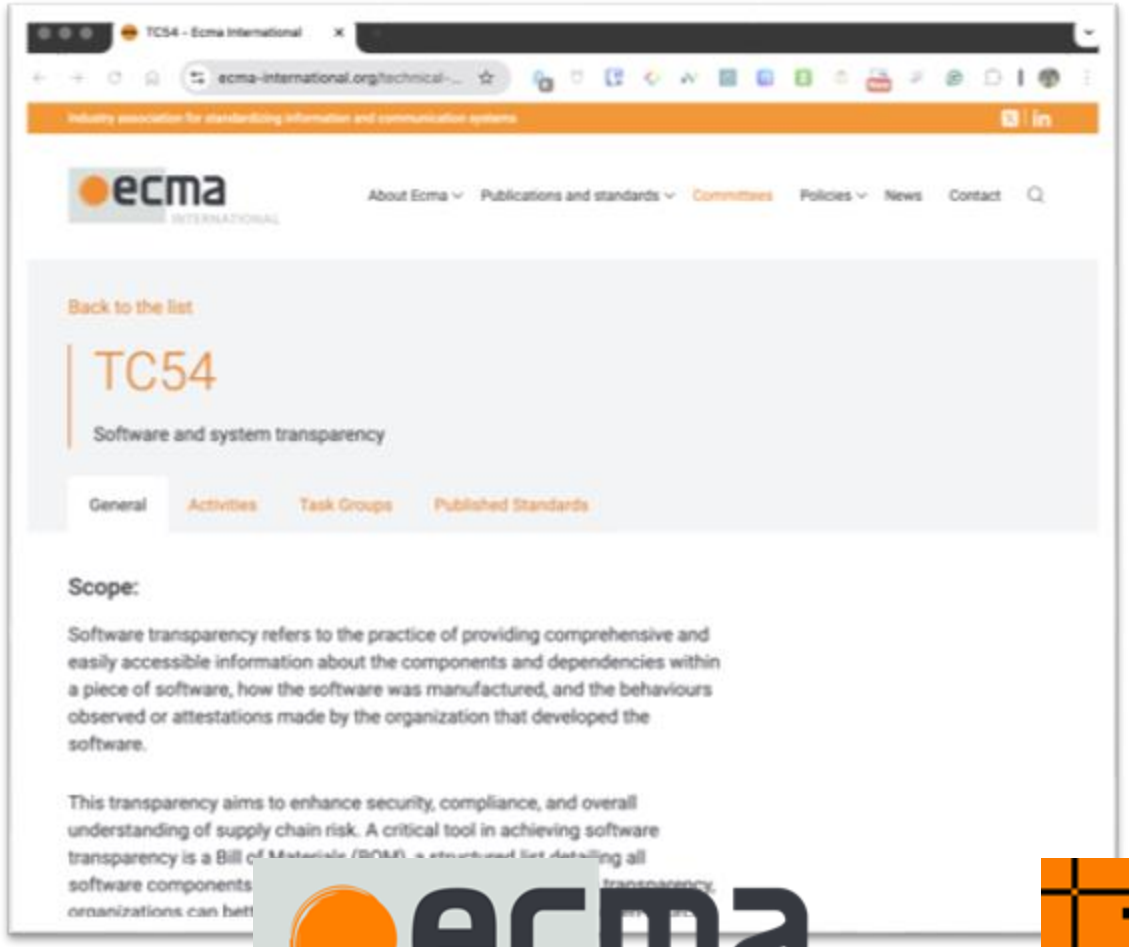
- Flagship OWASP standards project
- Lightweight BOM standard purpose built for cybersecurity use cases
- Designed in May 2017
- Initial release March 2018
- Yearly releases since
- Formal governance and standards process
- Adopted by multiple world governments
- Large and growing industry and vendor support



Vendor & Project Support

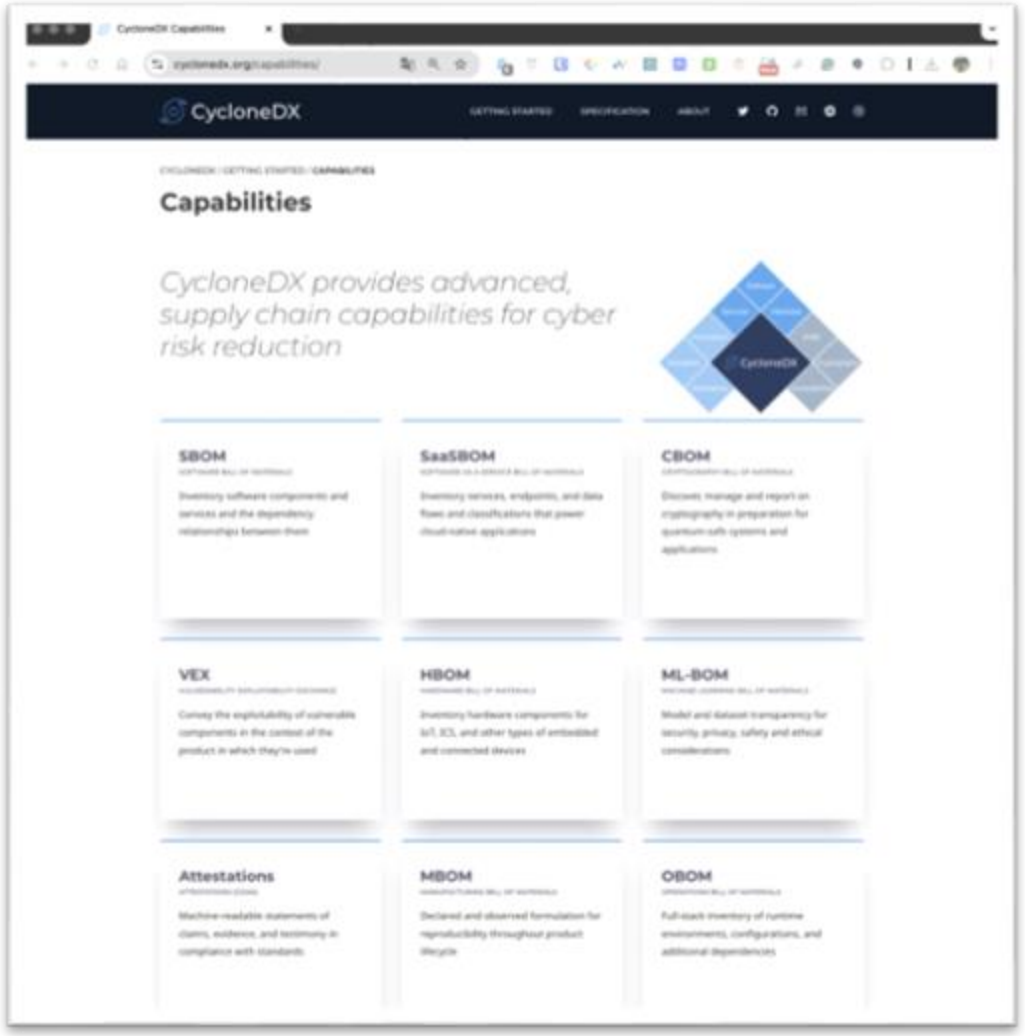
CycloneDX is now internationally standardized

- CycloneDX v1.6 is now ECMA standard (June, 2024)
- Purpose: CycloneDX is a standard aimed at improving transparency in software and systems supply chains.
- Core Functionality: Defines specifications for creating a Software Bill of Materials (SBOM).
- Content: Includes comprehensive details about software components, dependencies, manufacturing processes, and organizational actions.
- Key Benefits:
  - Enhances security and compliance efforts.
  - Promotes a better understanding of supply chain risks.
  - Facilitates easy access to critical software supply chain information.



CycloneDX Design Principles

- Lightweight yet full featured
- Prescriptive
- Easy to understand, implement, and adopt
- Gradual adoption path
- Embrace digital signatures
- Design for everything in mind



Direct to various supply chain risk

OBOM

Operations Bill of Materials

HBOM

Hardware Bill of Materials

VEX

Vulnerability Exploitability Exchange

SaaSBOM

Software-as-a-Service Bill of Materials

BOV

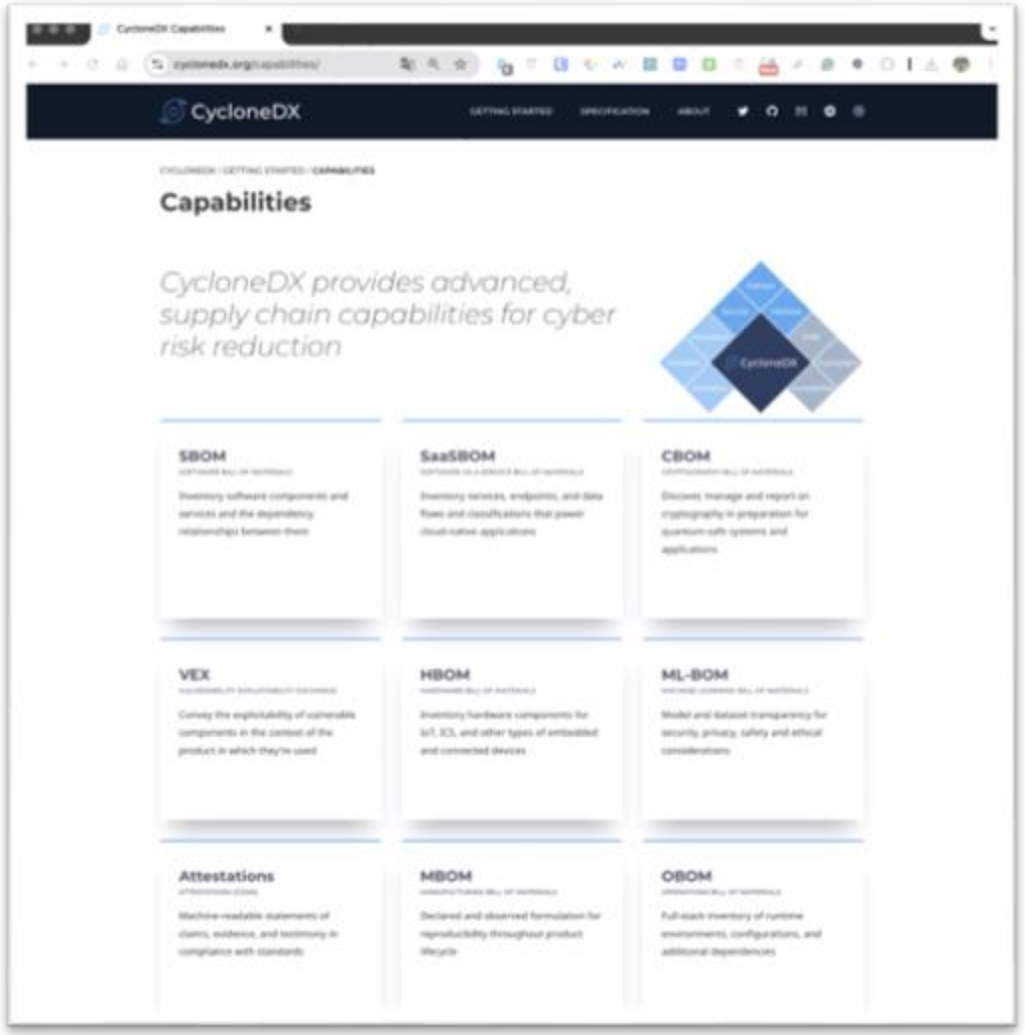
Bill of Vulnerabilities

VDR

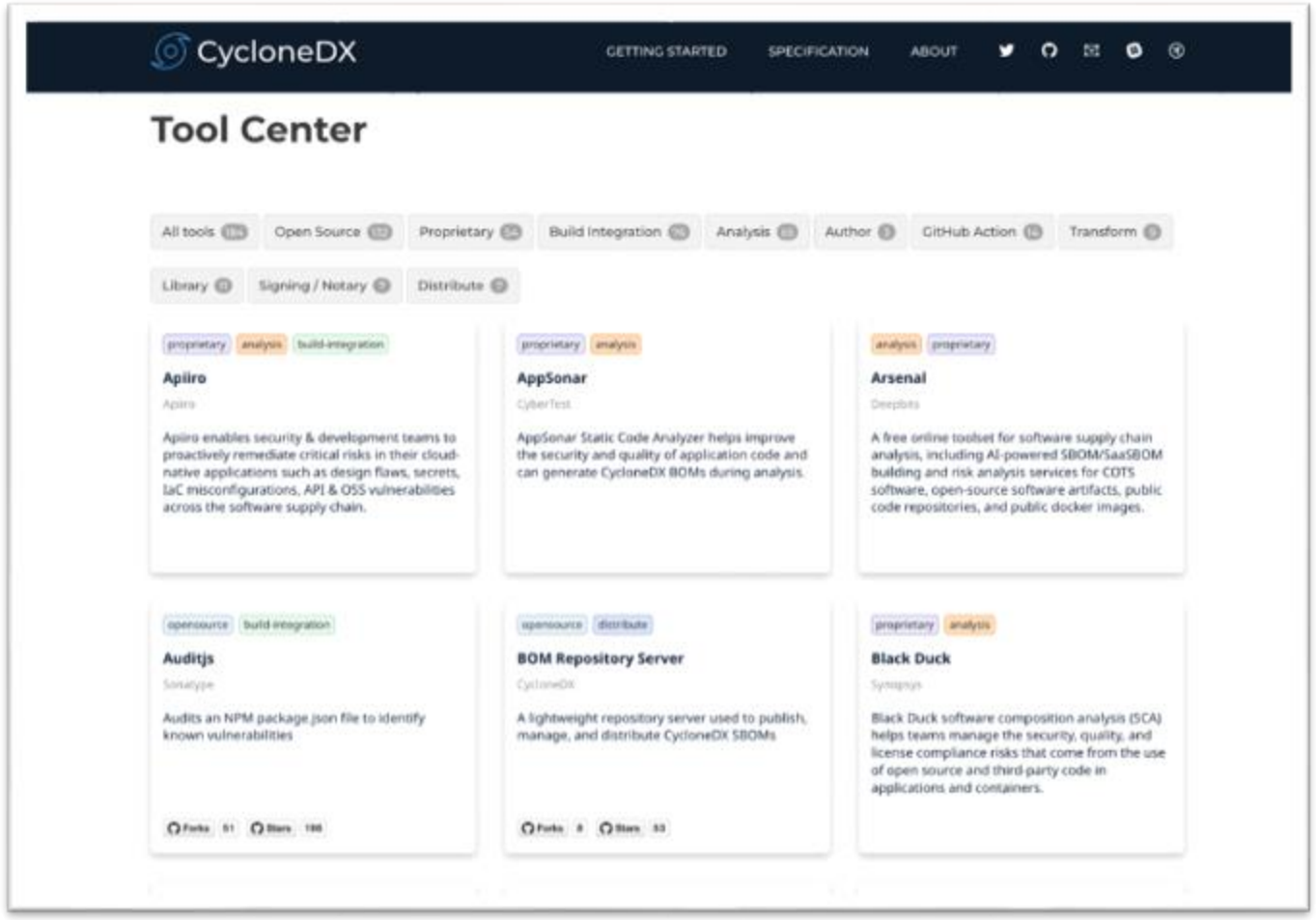
Vulnerability Disclosure Report

SBOM

Software Bill of Materials



Tool Center



Community effort to establish a marketplace of free, open source, and proprietary tools and solutions that support CycloneDX.

https://cyclonedx.org/tool-center/

“OWASP Dependency Track” to handle BOM

Source

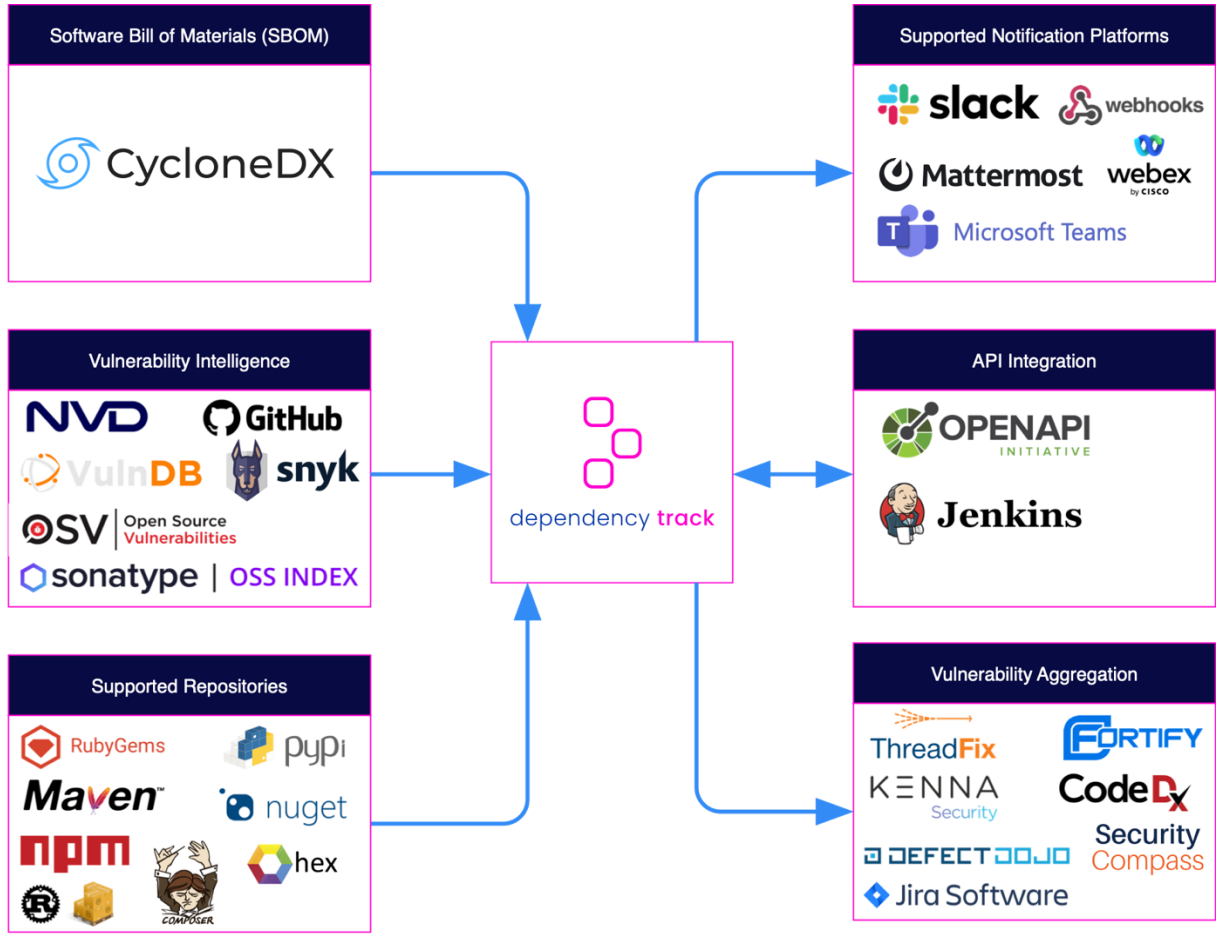
- Standard formats such as CycloneDX SBOM and VEX
- External information such as vulnerability databases (NVD, GitHub Advisories, Sonatype OSS Index, etc.) and license information (SPDX standard ID)

for whom

- Corporate security managers and compliance officers
- Software developers and engineering teams
- Risk management and supply chain personnel

What it does.

- Manage utilization of all stack components (libraries, OS, hardware, APIs, even service providers)
- Identify risks and present priority mitigation measures (known vulnerabilities, licensing risks, modified components, etc.)
- Integrated vulnerability information collection and policy management
- Visualization and management of security risks and licensing and operational risks



Q:

If we keep updating,

will we no longer be at risk of vulnerabilities?

Unresolved Issues:

Supply Chain Risk

What to do about problems that are not "vulnerabilities"?

Really, how can we make OSS packages and their updates reliable?

Severe Supply Chain Risks in Software

The risk posed by an attacker's method of inserting malicious code or entire malicious components into trusted software or hardware.

Trustworthy?

OSS as a target

Low security maturity of OSS developers

Users who blindly trust updates

ENISA Threat Landscape 2024

- Threats to availability (DDoS) and ransomware continue to be the most significant threats.
- Stealth attack (LOTS technique) using cloud environment, C2 communication using legitimate sites became active.
- Geopolitical factors continue to be a major motivation for cyber attacks.
- Evolution of defensive evasion techniques: cybercriminals use Living Off The Land (LOT) methods to blend into the environment.
- Surge in business email fraud (BEC).
- Extortion using reporting deadlines is the new modus operandi.
- Ransomware attacks have stabilized at a high level.
- AI-based fraud and cybercrime: FraudGPT and LLM for fraudulent email and malicious script generation.
- 19,754 vulnerabilities were reported, of which 9.3% were "critical" and 21.8% were "high".
- Information theft tools have become a key element in the attack chain.
- Similarities between hacktivist and state involvement.
- Data leakage site unreliable; duplicates and misreporting increase.
- The proliferation of mobile banking Trojans and the increasing complexity of attack methods.
- Malware-as-a-Service (MaaS) is evolving rapidly.
- Social Engineering of Supply Chain Attacks:
  A case study of a backdoor embedded in the OSS XZ Utils.
- Data leakage is on the rise.
- DDoS-for-Hire service allows even inexperienced attackers to launch large-scale attacks.
- Russian information operations remain critical in the invasion of Ukraine.
- The possibility of AI-based information manipulation emerged.

Intentional inclusion of malicious code

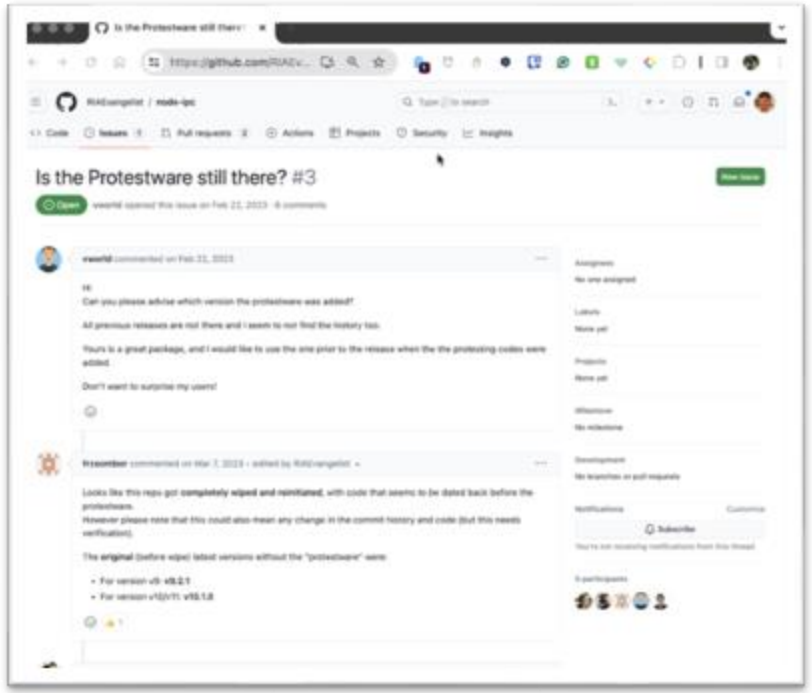
Target!

- Third Party OSS Repository Services
  - NPM, PyPI, RubyGems, Maven, NuGet, CPAN
- Development Platforms, Developer Accounts
  - Github, Gitlab, etc.
- Issues that are not listed in CVE

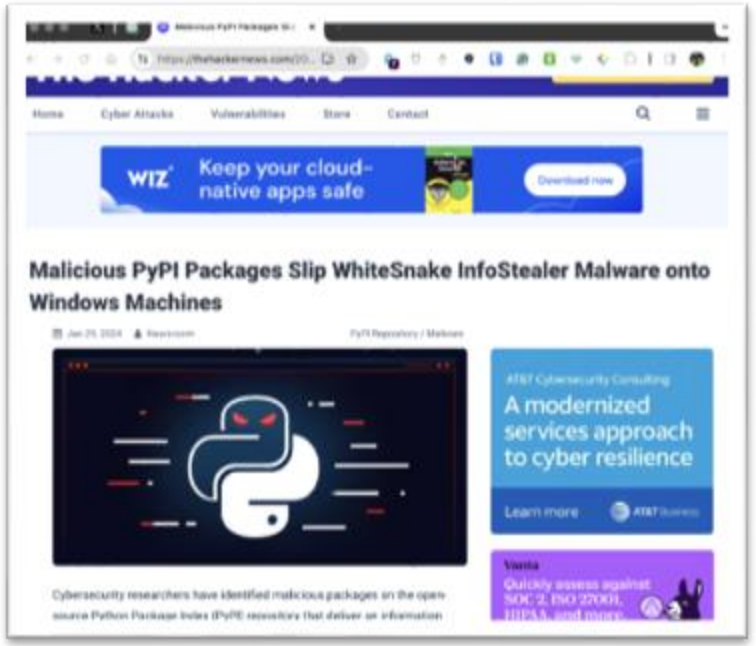
Offensive techniques

- 0-day
- typosquatting
- Project Hijack
- Masquerade attack
- Dependency Data Corruption
- Intentional neglect or inclusion of vulnerabilities
- protestware

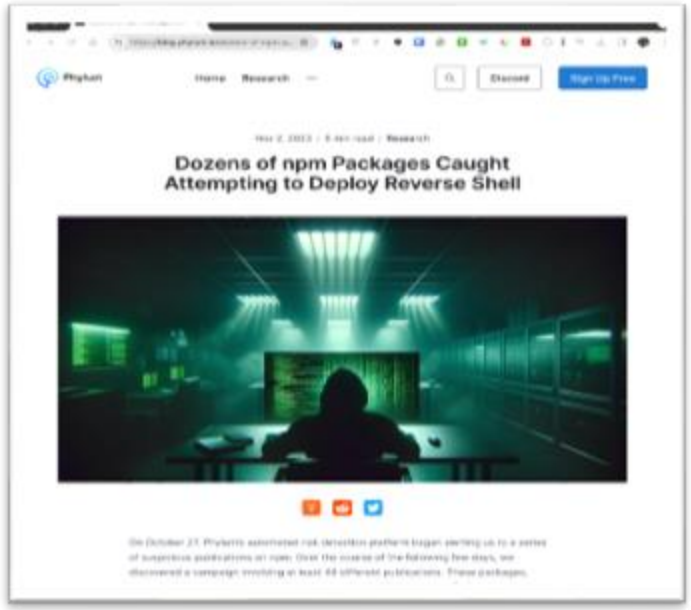
Intentional inclusion of malicious code



- Against war! The committer himself intentionally embedded aggressive code that would be triggered under certain conditions
- The wiper code was only for users from Russia and Belarus! (Aggressive)



- Malware in projects registered on PyPI
- setup.py downloads qualified information leakage software for each OS
- Appropriate packaging from the outside



- Uploaded to npm on October 27-30, 2023
- Obfuscated reverse shells were deployed in 48 separate packages.
- It is still observed that it is actively used.

Trustworthy?

OSS as a target

Low security maturity of OSS developers

Users who blindly trust updates

Challenges in OSS Security

- **Lack of Security Focus**: Many projects prioritize functionality over security. (more than 70%: High-Risk)
- OpenSSF 2024: Survey data reveals that nearly **one-third** of professionals report feeling unfamiliar with secure software development practices
- **Limited Resources**: OSS maintainers often need more resources or expertise to implement strong security measures.
- **Unmonitored Dependencies**: Reliance on external libraries can introduce hidden vulnerabilities.

Trustworthy?

OSS as a target

Low security maturity of OSS developers

Users who blindly trust “updates”

Is the resolution of “vulnerability” sufficient?

Vulnerability Location	What condition is it in?	Provider of means of response	Immediate response	shift left

Resolution of "Vulnerability."

Vulnerability Location	What condition is it in?	Provider of means of response	Immediate response	shift left
Desktops and smartphones	The device's operating system has problems, leaving it poorly protected or vulnerable	platformer (Apple, Google, etc.)	Update applied, Setting Adjustment	Automatic update utilization, Enhanced update information process
application software	Bugs, stepping stones, and other vulnerabilities	Developers and distributors	Apply updates and adjust settings,	Update or uninstall
Network equipment and devices	Equipment is vulnerable due to outdated firmware or exploitable configurations	Manufacturer	Apply Update	Network equipment and Review of configuration

Resolution of "Vulnerability."

Vulnerability Location	What condition is it in?	Provider of means of response	Immediate response	shift left
Desktops and smartphones	The device's operating system has problems, leaving it poorly protected or vulnerable	platformer (Apple, Google, etc.)	**Update applied, Setting Adjustment**	Automatic update utilization, Enhanced update information process
application software	Bugs, stepping stones, and other vulnerabilities	Developers and distributors	**Apply updates and adjust settings,**	**Update** or uninstall
Network equipment and devices	Equipment is vulnerable due to outdated firmware or exploitable configurations	Manufacturer	**Apply Update**	Network equipment and Review of configuration
Systems: open source, third-party APIs, etc.	A problem is discovered in the OSS source code used in the OS used in the system, and it becomes widely known that the system is vulnerable.	OSS Projects, Linux, Microsoft, etc. OS Vendors	**Verification of Operation and Application of updates**	Software Configuration Analysis SCA implementation, SBOM
System: Program code	Code developed by the company or SIer is problematic and vulnerable	No one wrote the code, and the development project team	Program Modifications	SAST, hands-on Production technical enhancements, including education and training, enhanced inspection tools
System: Cloud services, application configuration, protocol usage	Vulnerable due to configuration issues, e.g., data vulnerable to compromise	Cloud vendors or their advanced users	Modification of settings	Appropriate vulnerability testing and Enhanced monitoring
User, operator	Misuse of permitted functions or data handling	Users themselves and their organizations	Emergency Response and Cause Determination	Emergency response training Business data handling training Usability improvement Enhanced monitoring

Resolution of "Vulnerability."

Vulnerability Location	What condition is it in?	Provider of means of response	Immediate response	shift left
Desktops and smartphones	The device's operating system has problems, leaving it poorly protected or vulnerable	platformer (Apple, Google, etc.)	**Update applied, Setting Adjustment**	Automatic update utilization, Enhanced update information process
application software	Bugs, stepping stones, and other vulnerabilities	Developers and distributors	**Apply updates and adjust settings,**	**Update** or uninstall
Network equipment and devices	Equipment is vulnerable due to outdated firmware or exploitable configurations	Manufacturer	**Apply Update**	Network equipment and Review of configuration
Systems: open source, third-party APIs, etc.	A problem is discovered in the OSS source code used in the OS used in the system, and it becomes widely known that the system is vulnerable.	OSS Projects, Linux, Microsoft, etc. OS Vendors	**Verification of Operation and Application of updates**	Software Configuration Analysis SCA implementation, SBOM
System: Program code	Code developed by the company or SIer is problematic and vulnerable	No one wrote the code and the development project team	**Program Modifications**	SAST, hands-on Production technical enhancements, including education and training, enhanced inspection tools
System: Cloud services, application configuration, protocol usage	Vulnerable due to configuration issues, e.g., data vulnerable to compromise	Cloud vendors or their advanced users	**Modification of settings**	Appropriate vulnerability testing and Enhanced monitoring
User, operator	Misuse of permitted functions or data handling	Users themselves and their organizations	Emergency Response and Cause Determination	Emergency response training Business data handling training Usability improvement Enhanced monitoring

Open Source Software

SCA (Software Composition Analysis)
Key Points of Software Composition Analysis

Don't be satisfied with just finding problem components in the system with SBOM

- Quality Verification
- Not only enumerate update leaks, but also evaluate the severity of the leaks.
- Existence of POC/KEV

Facing Vulnerabilities

- Ensure intelligence to cover issues that do not appear on the CVE
- The relationship between the codes used should also be analyzed

Need to improve evaluation of projects, developers, and code

Drill down to the software project

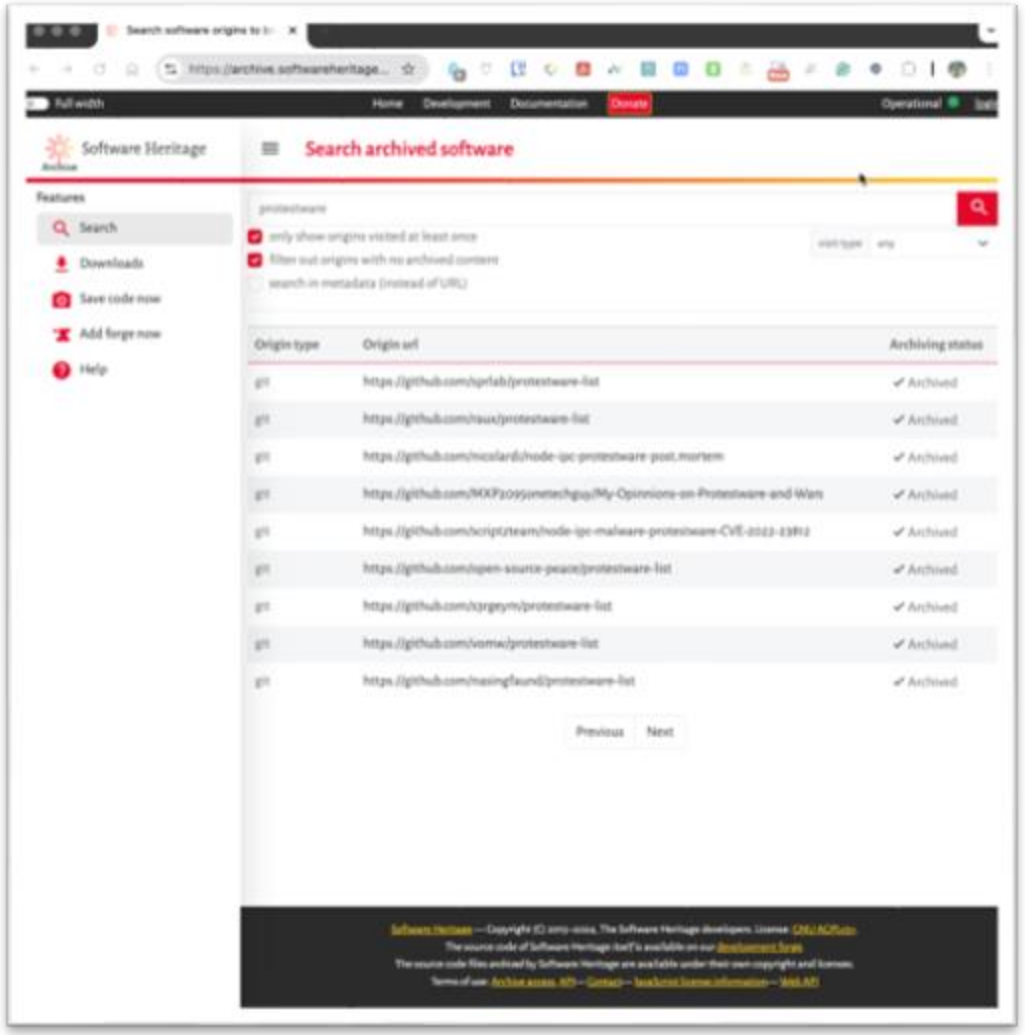
- Perspectives on whether to continue to use
  - Can the system be configured to reduce the occurrence of vulnerabilities?
  - Has the updated version of the code itself been appropriately modified to address the functionality used?
  - Reputation of the developer or development team

Software Heritage Project

Useful for Component Evaluation

Useful for finding out different things about the project

- Long-term maintenance and support system
- Vulnerability report history and speed of response
- Manage dependencies and assess supply chain risk
- Transparency of security processes
- Licensing (with or without a license sign!?!)
- Community vitality and number and quality of developers

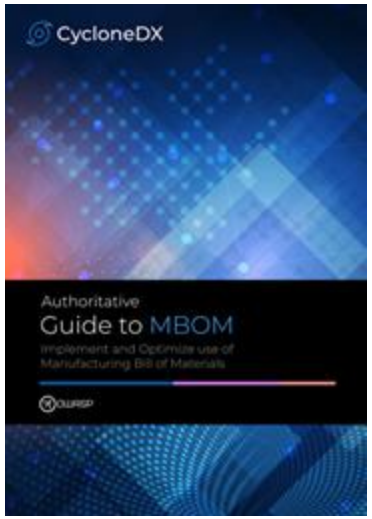


Software Heritage Project

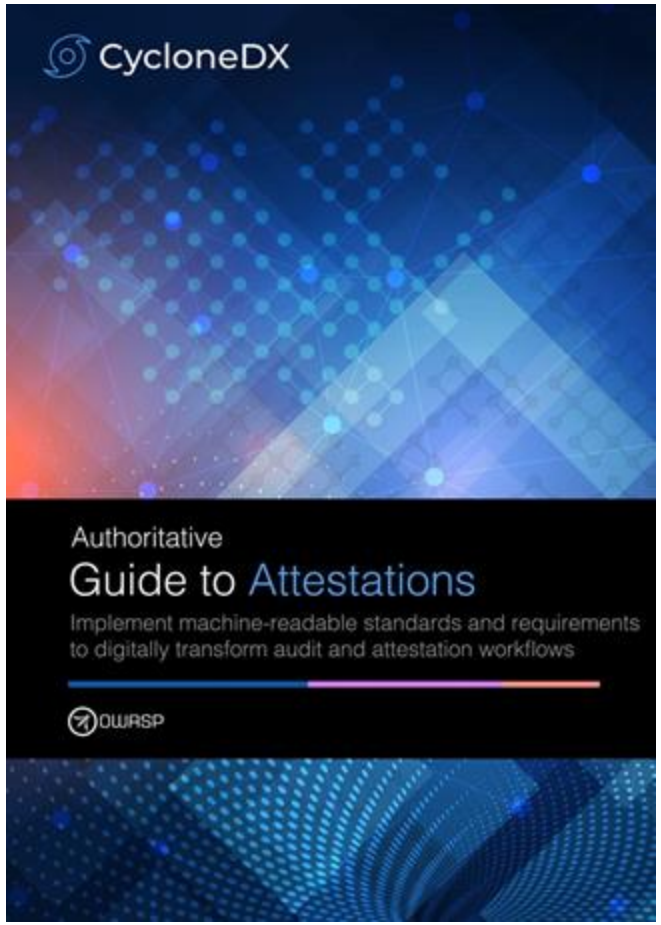
Authoritative Guides

- First in a series of guides
- Written with feedback from the community
- Future guides include:

https://cyclonedx.org/guides

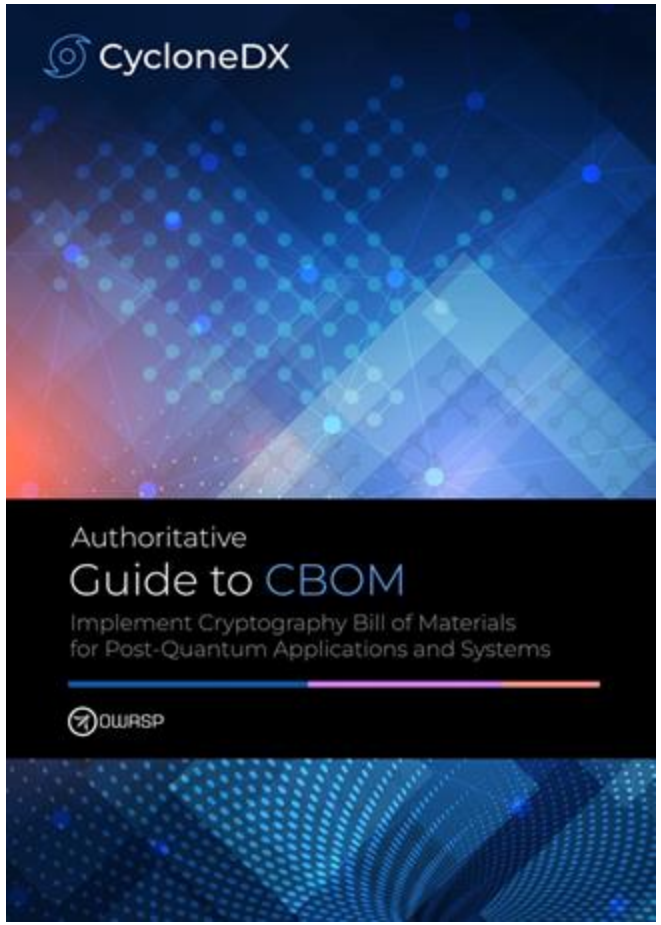


Authoritative Guides

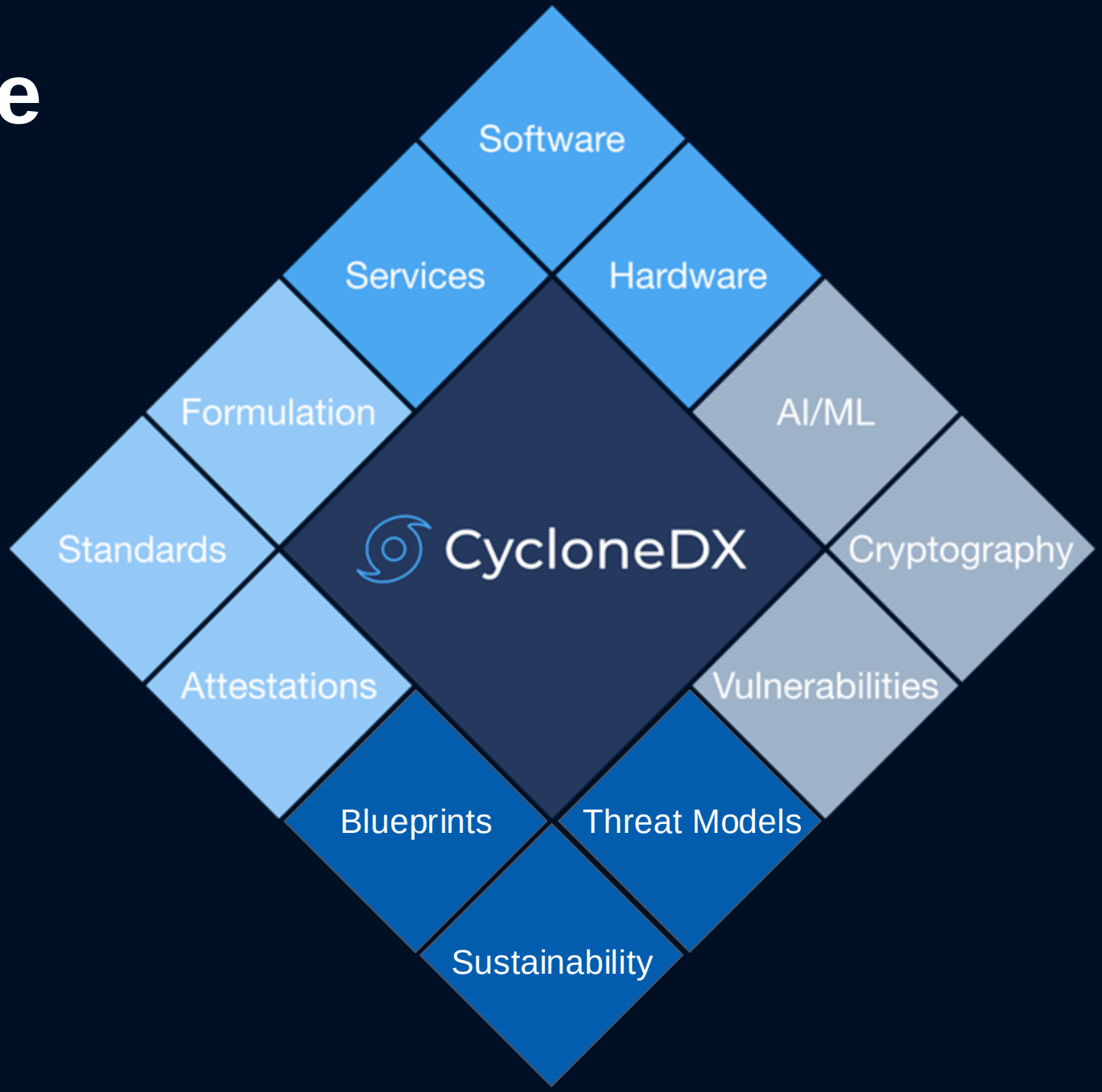


Now Available

https://cyclonedx.org/guides



Challenge

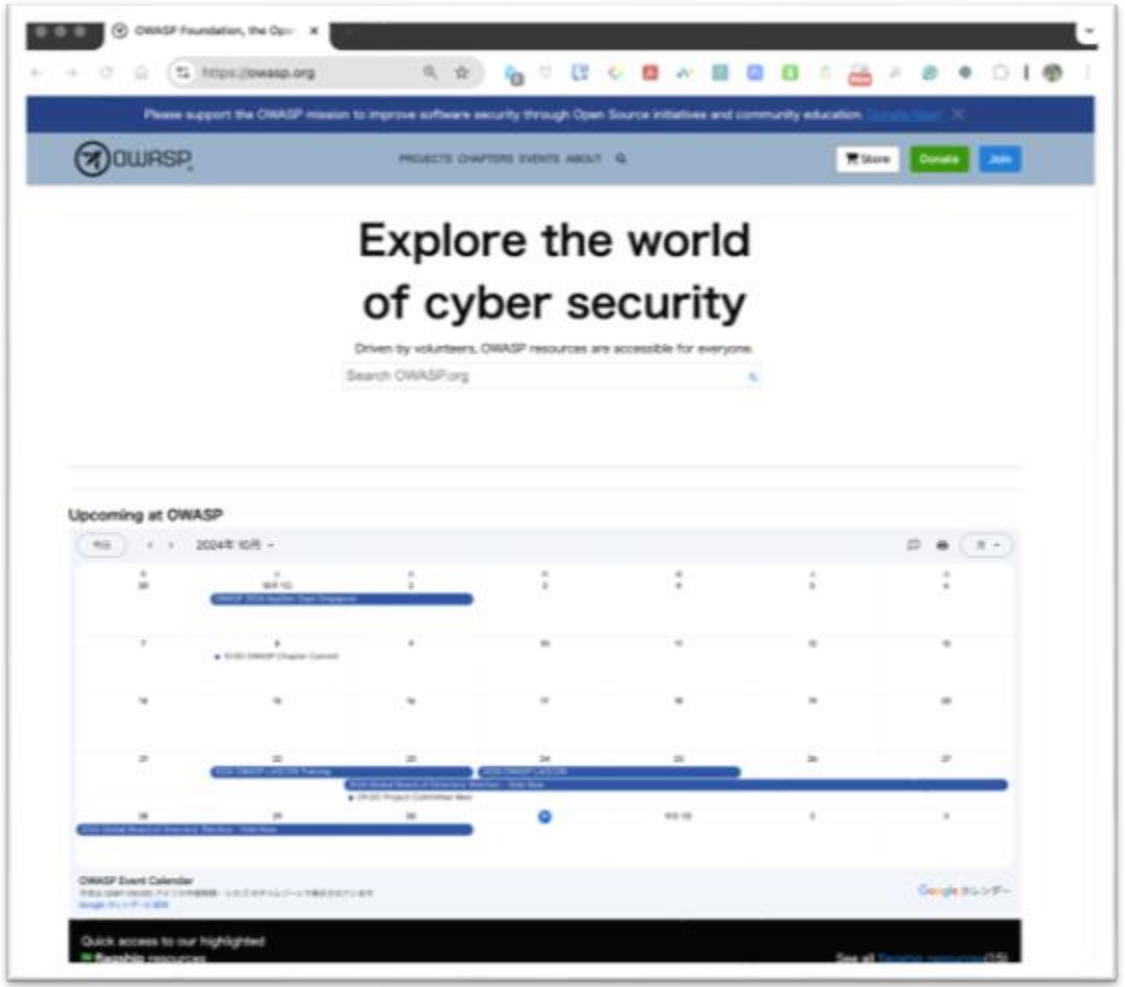

Software
Services
Hardware
Formulation
AI/ML
Standards
CycloneDX
Cryptography
Attestations
Vulnerabilities
Blueprints
Threat Models
Sustainability

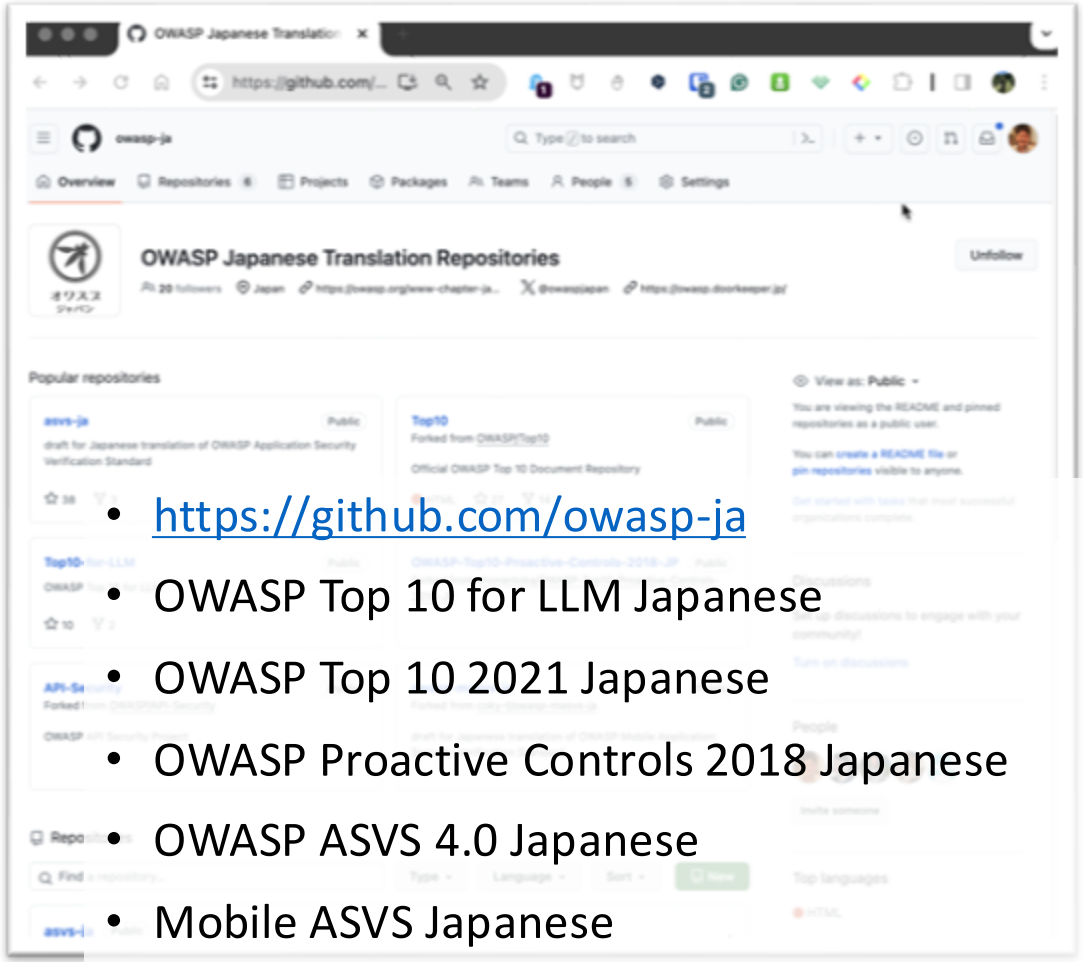
Contribute to the Ecosystem!

- We should be on the “creating” side, not just “using”.
- As community and industry organizations, we need to not only improve our educational materials, but also conduct joint training to increase “responsiveness” in the community and industry.
- NISC, JPCERT/CC, IPA, OWASP, Hardening Project, The Linux Foundation

OWASP.org / OWASP Japan chapter

Open Worldwide Application Security Project





- https://github.com/owasp-ja
- OWASP Top 10 for LLM Japanese
- OWASP Top 10 2021 Japanese
- OWASP Proactive Controls 2018 Japanese
- OWASP ASVS 4.0 Japanese
- Mobile ASVS Japanese
- OWASP Cheat Sheet List for Developers

Thank you

OWASP Japan

Github/speakerdeck/X: okdt

LinkedIn: riotaro

Youtube: asteriskresearch