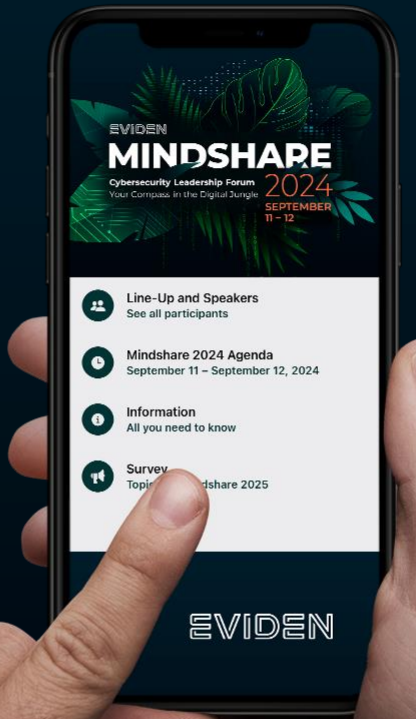
MINDSHARE 2024 AGENDA

SCAN NOW !



CASA
Cyber Security in the Age of Large-Scale Adversaries

RUHR UNIVERSITÄT BOCHUM

RUB

EVIDEN MINDSHARE 2024

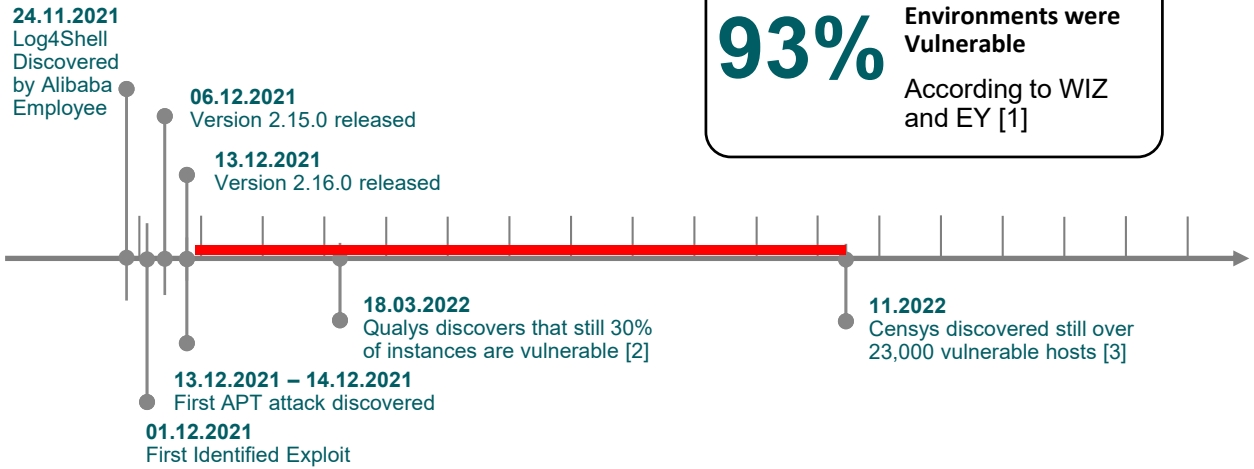
SBOMs for IT-Security

Driving Transparency in Software Development

Felix Reichmann | CISSP
Ruhr-University Bochum (Cluster of excellence CASA)

Log4Shell – A timeline

Log4Shell shows that patches for vulnerabilities are released promptly. However, the lack of dependency detection makes mitigation very difficult



93% **Of Cloud Environments were Vulnerable**

According to WIZ and EY [1]

Challenges

1. Enterprise Software Projects are complex
2. Log4Shell might not be found by DAST approaches
3. It took weeks until scanning signatures were broadly available

[1] https://www.wiz.io/blog/10-days-later-enterprises-halfway-through-patching-log4shell; last accessed: 02.08.2024
[2] https://blog.qualys.com/vulnerabilities-threat-research/2022/03/18/infographic-log4shell-vulnerability-impact-by-the-numbers; last accessed: 02.08.2024
[3] https://censys.com/tis-the-season-%F0%9F%AB%A3-a-look-back-at-the-critical-log4j-vulnerability/; last accessed: 02.08.2024

Similar Incidents

We will not be able to prevent vulnerabilities from appearing in the software supply chain. But we can work on incident response

Heartbleed
(2014; CVSS 7.5)

Log4Shell
(2021; CVSS 10.0)

XZ Utils
(2024; CVSS 10.0)

SolarWinds
(2019)

Supply Chain Challenges

We see a similar picture with corresponding incidents. We need to identify vulnerable systems more quickly

Point in time	Weeks to Months	Few Days

Detection

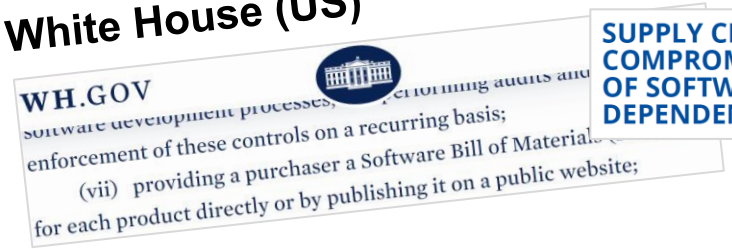
Identification of affected products

Mitigation

Political Voices

Supply chain attacks are not just a theoretical risk, but also have a massive impact in practice. This is also shown by the reactions from politicians

White House (US)



WH.GOV

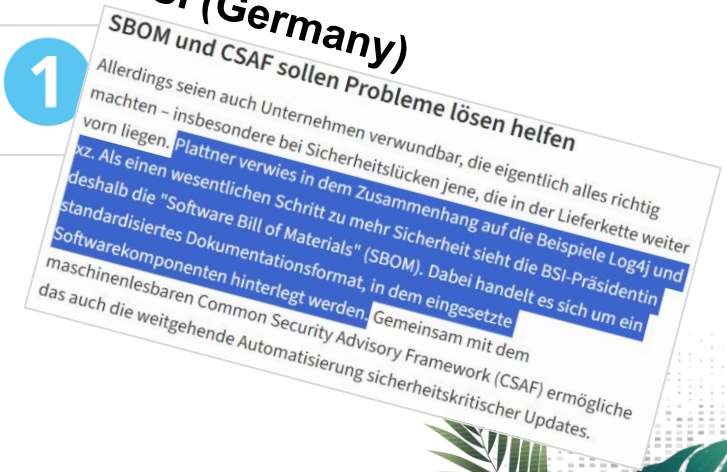
enforcement of these controls on a recurring basis;

(vii) providing a purchaser a Software Bill of Materia

for each product directly or by publishing it on a public website;

ENISA (EU)

BSI (Germany)



SBOM und CSAF sollen Probleme lösen helfen

Allerdings seien auch Unternehmen verwundbar, die eigentlich alles richtig machten – insbesondere bei Sicherheitslücken jene, die in der Lieferkette weiter vorn liegen. Plattner verwies in dem Zusammenhang auf die Beispiele Log4j und xz. Als einen wesentlichen Schritt zu mehr Sicherheit sieht die BSI-Präsidentin deshalb die "Software Bill of Materials" (SBOM). Dabei handelt es sich um ein standardisiertes Dokumentationsformat, in dem eingesetzte Softwarekomponenten hinterlegt werden. Gemeinsam mit dem maschinenlesbaren Common Security Advisory Framework (CSAF) ermögliche das auch die weitgehende Automatisierung sicherheitskritischer Updates.

[1] Executive Order 14028 of the White House: https://www.whitehouse.gov/briefing-room/presidential-actions/2021/05/12/executive-order-on-improving-the-nations-cybersecurity/
[2] Top 1 Risk of the ENISA Foresight 2030 Threat Report: https://www.enisa.europa.eu/publications/enisa-foresight-cybersecurity-threats-for-2030
[3] Heise Report about the upcoming BSI Strategy: https://www.heise.de/news/BSI-Praesidentin-Allerhoechste-Eisenbahn-fuer-mehr-Schutz-9710743.html

Other Industries

Bill of materials are therefore used in other industries, such as automotive. This is a precise list of the parts used so that defective parts can be identified

Defect Identified

A component is identified as defective

Check BOM

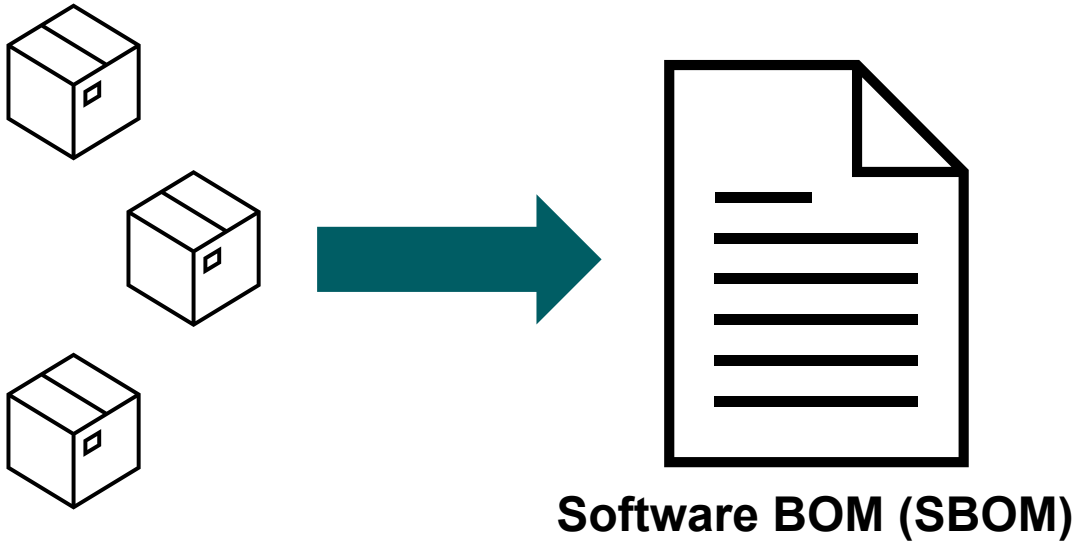
Affected vehicles can be identified via the Bill of Materials (BOM) efficiently

Recall and replacement

Vehicles are recalled and the components are replaced

Adoption in Cybersecurity

We can copy this approach in cybersecurity and create a standardized list of all the components of a software. This is the Software Bill of Material (SBOM)



Three Leading SBOM Standards

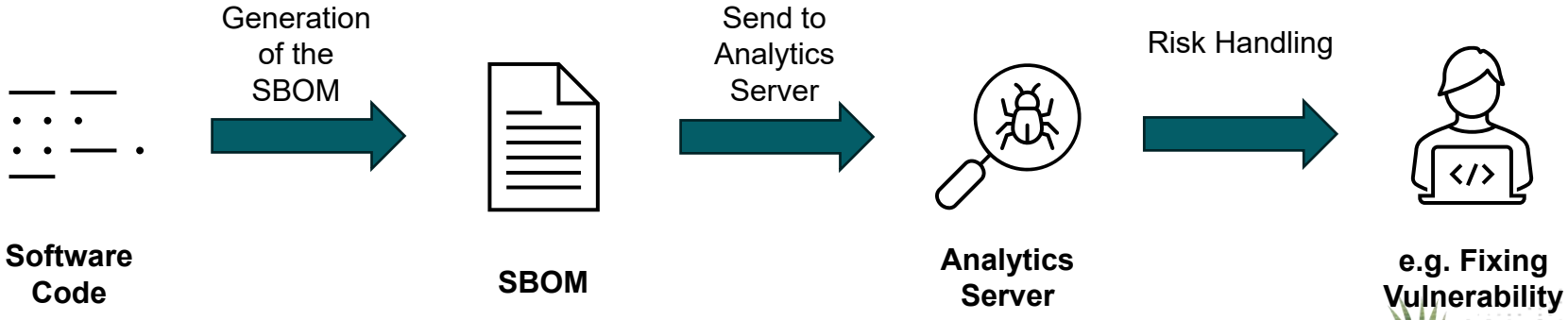
CycloneDX
(OWASP)

SPDX
(Linux Foundation)

SWID
(NIST)

SBOM Process

This results in a largely automated process that ranges from the generation to analysis and risk management. Different stakeholders must be involved



SBOM as Game Changer

SBOM is not only an effective and efficient way to reduce risk. It is becoming more and more mandatory due to its embedding in regulations

1

SBOM as proactive cybersecurity measure

Since SBOMs are based on the source code, they can identify problematic dependencies before they end up in productive systems. A very good cost-benefit ratio is achieved through a high degree of automation

2

Legal Risk Minimization

Licenses in the open-source sector quickly become a legal challenge for companies. Licenses can be included in the generation of SBOMs and thus problematic license types to be identified and prevented

3

Fulfillment of Regulatory Requirements

It is becoming apparent that regulatory authorities and standards are increasingly focusing on the software supply chain and SBOMs. Companies should act proactively to avoid being forced into action

Regulatory Requirements

Essential standards have already addressed the topic of supply chain security, some with SBOMs. It can be assumed that this trend will intensify

	Supply Chain mentioned	SBOM mentioned	Wording
NIST CSF 2.0	✓	✗	GV.SC: **Cyber supply chain risk management** processes are identified, established, managed, monitored, and improved by organizational stakeholders
EU CRA	✓	✓	2.Vulnerability handling requirements: Manufacturers of the products with digital elements shall: (1) identify and document vulnerabilities and components contained in the product, including by **drawing up a software bill of materials** in a commonly used and machine-readable format covering at the very least the top-level dependencies of the product;
NIS 2	✓	✗	2. As part of the national cybersecurity strategy, Member States shall in particular adopt policies: (a) addressing **cybersecurity in the supply chain** for ICT products and ICT services used by entities for the provision of their services;
NIST SSDF	✓	✓	PS.3.2: Collect, safeguard, maintain, and share provenance data for all components of each software release (e.g., in a software bill of materials **[SBOM]**, through Supply-chain Levels for Software Artifacts [SLSA]).

Tooling Landscape

There are several products out there supporting the SBOM Technology. OWASP is providing the CycloneDX standard together with a free toolset

https://cyclonedx.org/tool-center/ https://dependencytrack.org/ https://www.atlassian.com/software/jira

Exemplary Tooling

CycloneDX dependency track Jira Software *

* Product by Atlassian; May results in costs

Research Perspective

Research is currently still in an exploratory state. We work together with practitioners to identify challenges and derive recommendations for action

Literature Review

[1] Zahan et al.: Software Bills of Materials Are Required. Are We There Yet? (2023)
Review of Internet Articles

[2] Bi et al.: On the Way to SBOMs: Investigating Design Issues and Solutions in Practice (2023)
Analysis of public online discussions

[3] Sehgal et al.: A Taxonomy and Survey of Software Bill of Materials (SBOM) Generation Approaches (2024)
Literature Review

Identification of challenges with interaction

[4] Xia et al.: An Empirical Study on Software Bill of Materials: Where We Stand and the Road Ahead (2023)
Interview + survey

[5] Chaora et al.: Discourse, Challenges, and Prospects Around the Adoption and Dissemination of Software Bills of Materials (SBOMs) (2023)
Ethnographic study (monitoring of meetings in an organization)

[6] Stalnaker et al.: BOMs Away! Inside the Minds of Stakeholders: A Comprehensive Study of Bills of Materials for Software Systems (2024)
Interview + survey

Innovations

[7] Xia et al.: Trust in Software Supply Chains: Blockchain-Enabled SBOM and the AIBOM Future (2023)
Proposal of a technology for sharing SBOMs

The full citations are available at the end of the presentation.

Personal Opinion

I am convinced that SBOMs have potential to positively impact the security landscape. It brings transparency, can be automated and reduced legal risks

01

Transparency
Situations like Log4Shell or Heartbleed will occur more and more frequently in the future. Simple measures such as SBOMs can drastically reduce the response time and thus improve security as well as operational efficiency

02

Automation
Both the creation and large parts of the analysis process can be automated with simple means, so that the greatest effort is required to minimize risk. Therefore, SBOMs to not prevent developers to concentrate on their primary tasks

03

Legal Risk Reduction
Open-Source applications can contain clauses regarding copyleft or non-commercial use, which is why the legal situation quickly becomes complex. SBOMs can help to automatically generate an overview so that difficult legal libraries can be proactively identified

Questions?

CASA
CYBER SECURITY IN THE AGE OF LARGE-SCALE ADVERSARIES

Felix Reichmann, Ruhr-University Bochum (Excellenzcluster CASA)

Full Citations

For Slide 12

- [1] N. Zahan, E. Lin, M. Tamanna, W. Enck and L. Williams, "Software Bills of Materials Are Required. Are We There Yet?," in IEEE Security & Privacy, vol. 21, no. 2, pp. 82-88, March-April 2023, doi: 10.1109/MSEC.2023.3237100.
- [2] Bi, T., Xia, B., Xing, Z., Lu, Q., & Zhu, L. (2023). On the Way to SBOMs: Investigating Design Issues and Solutions in Practice. *ArXiv, abs/2304.13261*.
- [3] Sehgal, V.V., Ambili, P.S. (2024). A Taxonomy and Survey of Software Bill of Materials (SBOM) Generation Approaches. In: Dhar, S., Goswami, S., Dinesh Kumar, U., Bose, I., Dubey, R., Mazumdar, C. (eds) AGC 2023. AGC 2023. Communications in Computer and Information Science, vol 2008. Springer, Cham. https://doi.org/10.1007/978-3-031-50815-8_3
- [4] Xia, B., Bi, T., Xing, Z., Lu, Q., & Zhu, L. (2023). An Empirical Study on Software Bill of Materials: Where We Stand and the Road Ahead. *2023 IEEE/ACM 45th International Conference on Software Engineering (ICSE)*, 2630-2642.
- [5] A. Chaora, N. Ensmenger and L. J. Camp, "Discourse, Challenges, and Prospects Around the Adoption and Dissemination of Software Bills of Materials (SBOMs)," 2023 IEEE International Symposium on Technology and Society (ISTAS), Swansea, United Kingdom, 2023, pp. 1-4, doi: 10.1109/ISTAS57930.2023.10305922. Future. *ArXiv, abs/2307.02088*.
- [6] Trevor Stalnaker, Nathan Wintersgill, Oscar Chaparro, Massimiliano Di Penta, Daniel M German, and Denys Poshyvanyk. 2024. BOMs Away! Inside the Minds of Stakeholders: A Comprehensive Study of Bills of Materials for Software Systems. In Proceedings of the IEEE/ACM 46th International Conference on Software Engineering (ICSE '24). Association for Computing Machinery, New York, NY, USA, Article 44, 1–13. https://doi.org/10.1145/3597503.3623347
- [7] Xia, B., Zhang, D., Liu, Y., Lu, Q., Xing, Z., & Zhu, L. (2023). Trust in Software Supply Chains: Blockchain-Enabled SBOM and the AIBOM

TAKE A MINUTE AND GIVE US FEEDBACK …

RATE NOW!