A survey to investigate the state of practice in open software supply chain management

Survey Flow

Standard: Consent Form (2 Questions)
Standard: Self-Identification (1 Question)
Standard: Shared (10 Questions)

Branch: New Branch
If
If From the list below, select all the options that apply to you: I create SBOMs for the software projects I am involved in Is Selected

Block: SBOM Producers (8 Questions)

Branch: New Branch
If
If From the list below, select all the options that apply to you: I use the SBOMs of (third-party) software components/dependencies Is Selected

Block: SBOM Consumers (7 Questions)

Branch: New Branch
If
If From the list below, select all the options that apply to you: I create tools that generate or process SBOMs Is Selected

Block: SBOM Tool Developers (6 Questions)

Branch: New Branch
If
If From the list below, select all the options that apply to you: I am involved in defining standards / specifications for SBOMs Is Selected

Block: SBOM Standard Makers (3 Questions)

Branch: New Branch
If
If From the list below, select all the options that apply to you: I develop, compile, or apply educational resources related to SBOMs Is Selected

Block: SBOM Educators (5 Questions)

Standard: Security (9 Questions)
Standard: Demographic Questions (12 Questions)

Page Break

Start of Block: Consent Form

CF1 Investigating the state of practice in software supply chain management RESEARCH GOAL AND PROCEDURE

The purpose of this study is to investigate issues, needs, and opportunities related to software supply chain management.

The (open source) software supply chain is the set of processes, components, and tools used to develop, build, and publish a software product (a system, library, tool, etc.). Software vendors often create software products by assembling open source software components (aka dependencies) developed by third-party developers or organizations. Common tasks involved in supply chain management include maintaining license compliance among components, managing and screening dependencies, and mitigating security threats introduced in software dependencies.

If you decide to participate, you will take a brief survey/questionnaire. The survey will last about 20-30 minutes during which time you will be asked questions regarding your familiarity and experience with several topics related to the open source supply chain, **including dependency management, Software Bills of Materials (SBOMs), security issues related to the supply chain, and open source licensing.**

We may contact you by email to invite you to participate in a follow-up interview.

RISKS AND BENEFITS There are no foreseeable risks for participating in this research. There are no benefits to you as a participant other than to further research in software engineering and the open source software supply chain. PARTICIPATION You must be at least 18 years old to participate. Your participation is voluntary, and you may withdraw from the study at any time and for any reason. If you decide not to participate or if you withdraw from the study, there is no penalty or loss of benefits to which you are otherwise entitled. There are no costs to you or any other party. Your decision whether or not to participate will not prejudice your future relations with [Organization]. If you decide to participate, you will be entered into a drawing for a $50 USD Amazon gift card upon completion of this survey. We will randomly choose respondents and give out 10 gift cards. CONFIDENTIALITY The data collected by this study will be confidential, including your responses. Any information obtained in connection with this study that can be identified with you will remain confidential and disclosed only with your permission. You will be assigned a code number to protect your identity and all data will be kept secure. If you give us your permission by signing this document, we plan to disclose the results of the questionnaire in any publication resulting from this study. The disclosed results will not be personally identifiable (if needed, they will be anonymized). The de-identified data could be used for future research without additional consent from participants. The Institutional Review Board (IRB) and [committee] that monitor research on human subjects may inspect study records during internal auditing procedures and are required to keep all information confidential. CONTACT This research is being conducted by [Anonymous Author(s)] from [Organization].

Questions regarding the rights of research subjects may be directed to [redacted].

Such committee has reviewed and approved the present research

([protocol]) CONSENT You are welcome to print this page to keep a copy of this form.
Do you consent to participate in this survey?

JS

CF2 **YOU ARE MAKING A DECISION WHETHER OR NOT TO PARTICIPATE.**

IF YOU WANT TO PARTICIPATE, PLEASE ENTER YOUR NAME IN THE TEXT FIELD BELOW, AND START THE SURVEY.

Please enter your name.

_____

End of Block: Consent Form

Start of Block: Self-Identification

*

ID Please indicate your knowledge/involvement with SBOMs (Software Bill of Materials), by selecting all the options that apply to you:

- ☐ I create SBOMs for the software projects I am involved in (1)
- ☐ I use the SBOMs of software projects I am involved in or third-party software components/dependencies (2)
- ☐ I create tools that generate or process SBOMs (3)
- ☐ I am involved in defining standards / specifications for SBOMs (4)
- ☐ I develop, compile, and/or apply educational resources related to SBOMs (5)
- ☒ I am not familiar with SBOMs (6)
- ☐ Other (please specify) (7)

_____

End of Block: Self-Identification

Start of Block: Shared

Display This Question:

If Please indicate your knowledge/involvement with SBOMs (Software Bill of Materials), by selecting... != I am not familiar with SBOMs

S1 Please briefly describe the concept of SBOMs. What are they? What is their purpose?

_____

_____

_____

_____

_____

Display This Question:

If Please indicate your knowledge/involvement with SBOMs (Software Bill of Materials), by selecting... = I create SBOMs for the software projects I am involved in

Or Please indicate your knowledge/involvement with SBOMs (Software Bill of Materials), by selecting... = I use the SBOMs of software projects I am involved in or third-party software components/dependencies

S2 Which SBOM format(s) do you use?

- [ ] SPDX (1)
- [ ] CycloneDX (2)
- [ ] SWID (3)
- [ ] Other (please specify) (4) _____

Display This Question:

If Please indicate your knowledge/involvement with SBOMs (Software Bill of Materials), by selecting... = I create SBOMs for the software projects I am involved in

Or Please indicate your knowledge/involvement with SBOMs (Software Bill of Materials), by selecting... = I create tools that generate or process SBOMs

Or Please indicate your knowledge/involvement with SBOMs (Software Bill of Materials), by selecting... = I am involved in defining standards / specifications for SBOMs

S3 Please list which data fields you think should be included in SBOMs.

_____

_____

_____

_____

_____

Display This Question:

If Please indicate your knowledge/involvement with SBOMs (Software Bill of Materials), by selecting... != I am not familiar with SBOMs

S4
Indicate your agreement with the following statement:
“The use of SBOMs is critical in software development.”

- ○ Strongly disagree (1)
- ○ Disagree (2)
- ○ Neutral (3)
- ○ Agree (4)
- ○ Strongly agree (5)

Display This Question:

If Please indicate your knowledge/involvement with SBOMs (Software Bill of Materials), by selecting... = I am involved in defining standards / specifications for SBOMs

Or Please indicate your knowledge/involvement with SBOMs (Software Bill of Materials), by selecting... = I develop, compile, and/or apply educational resources related to SBOMs

S5 What deficiencies currently exist in SBOM standards / specifications?

_____

_____

_____

_____

_____

Display This Question:

If Please indicate your knowledge/involvement with SBOMs (Software Bill of Materials), by selecting... = I am involved in defining standards / specifications for SBOMs

Or Please indicate your knowledge/involvement with SBOMs (Software Bill of Materials), by selecting... = I develop, compile, and/or apply educational resources related to SBOMs

S6 How can we address current deficiencies in SBOM standards / specifications?

_____

_____

_____

_____

_____

Display This Question:

If Please indicate your knowledge/involvement with SBOMs (Software Bill of Materials), by selecting... = I use the SBOMs of software projects I am involved in or third-party software components/dependencies

Or Please indicate your knowledge/involvement with SBOMs (Software Bill of Materials), by selecting... = I create tools that generate or process SBOMs

Or Please indicate your knowledge/involvement with SBOMs (Software Bill of Materials), by selecting... = I develop, compile, and/or apply educational resources related to SBOMs

S7 Indicate your agreement with the following statement:
"Current SBOM tool support meets the needs of users."

- ○ Strongly disagree (6)
- ○ Disagree (7)
- ○ Neutral (8)
- ○ Agree (9)
- ○ Strongly agree (10)

Display This Question:

If Please indicate your knowledge/involvement with SBOMs (Software Bill of Materials), by selecting... = I use the SBOMs of software projects I am involved in or third-party software components/dependencies

Or Please indicate your knowledge/involvement with SBOMs (Software Bill of Materials), by selecting... = I create tools that generate or process SBOMs

Or Please indicate your knowledge/involvement with SBOMs (Software Bill of Materials), by selecting... = I develop, compile, and/or apply educational resources related to SBOMs

S8 How can we address current deficiencies in SBOM tooling?

_____

_____

_____

_____

_____

Display This Question:

If Please indicate your knowledge/involvement with SBOMs (Software Bill of Materials), by selecting... = I create SBOMs for the software projects I am involved in

Or Please indicate your knowledge/involvement with SBOMs (Software Bill of Materials), by selecting... = I use the SBOMs of software projects I am involved in or third-party software components/dependencies

S9 How would you prefer SBOMs be distributed? Rank by preference by dragging the options.

_____ Stored with trusted third party (1)
_____ Located in repositories along with source code (2)
_____ Downloadable from project website (3)
_____ Available from the project developers upon request (4)
_____ Attached to software binaries (5)
_____ Other(s) (6)

Display This Question:

If Please indicate your knowledge/involvement with SBOMs (Software Bill of Materials), by selecting... = I create SBOMs for the software projects I am involved in

Or Please indicate your knowledge/involvement with SBOMs (Software Bill of Materials), by selecting... = I use the SBOMs of software projects I am involved in or third-party software components/dependencies

S10 (Optional) Feel free to explain you preferences about how SBOMs should be distributed.

_____

_____

_____

_____

_____

End of Block: Shared

Start of Block: SBOM Producers

P1 Please answer the following questions based on your experience creating SBOMs for software projects you are involved in.

P2 At what point(s) in the software development process should SBOMs be generated? (select all that apply)

- [ ] During project planning (1)
- [ ] At the developer's discretion, from source code (2)
- [ ] During each software build (3)
- [ ] During each software deployment (4)
- [ ] When publishing a major software release (5)
- [ ] Other (please specify) (6) _____
- [ ] ⊗ I don't know (7)

*

P3 Why do you create SBOMs? (select all that apply)

- [ ] To meet regulatory requirements (1)
- [ ] To meet software licensing requirements (2)
- [ ] To provide others with information about my project (3)
- [ ] To monitor project dependencies (4)
- [ ] To keep track of dependency vulnerabilities (5)
- [ ] Because my organization asks me to (6)
- [ ] To make it easier to understand dependencies in complex projects (7)
- [ ] To proactively identify replacements for components that reach end-of-life (8)
- [ ] Other (please specify) (9)

_____

- [ ] ⊗ I don't know (10)

Display This Question:

If If Why do you create SBOMs? (select all that apply) q://QID12/SelectedChoicesCount Is Greater Than or Equal to 1

And Why do you create SBOMs? (select all that apply) != I don't know

P4 (Optional) Please elaborate on the benefits from creating SBOMS that you identified.

_____

_____

_____

_____

_____

P5 What tool(s) do you use to assist the creation of SBOMs, if any?

_____

_____

_____

_____

_____

P7 Does your organization have strategies for managing SBOM versions?

- Yes (1)
- No (2)
- I don't know (3)
- N/A (4)

Display This Question:

If Does your organization have strategies for managing SBOM versions? = Yes

P8 What strategies does your organization have for managing SBOM versions? Are there any specific tools involved?

_____

_____

_____

_____

_____

P9 What issues have you faced when creating SBOMs? Feel free to give examples.

_____

_____

_____

_____

_____

End of Block: SBOM Producers

Start of Block: SBOM Consumers

C1 Please answer the following questions based on your experience using (consuming) SBOMs of the software projects you are involved in or third-party software components/dependencies.

C2 What do you use SBOMs for? (select all that apply)

- ☐ To meet regulatory requirements (1)
- ☐ To meet software licensing requirements (2)
- ☐ To learn more about other projects (3)
- ☐ To monitor my project's dependencies (4)
- ☐ To keep track of dependency vulnerabilities (5)
- ☐ Because my organization asks me to (6)
- ☐ To make it easier to understand dependencies in complex projects (7)
- ☐ To proactively identify replacements for components that reach end-of-life (8)
- ☐ Other (please specify) (9) _____
- ☐ ⊗ I don't know (10)

Display This Question:

If If What do you use SBOMs for? (select all that apply) q://QID85/SelectedChoicesCount Is Greater Than or Equal to 1

And What do you use SBOMs for? (select all that apply) != I don't know

C3 (Optional) Please elaborate on the benefits from consuming SBOMS that you identified.

_____

_____

_____

_____

_____

C4 How often do you use SBOMs during software development?

- ○ Very rarely (1)
- ○ Once per month (2)
- ○ Once per week (3)
- ○ Every day (4)
- ○ Never (5)
- ○ Other (6) _____

C5 Do you process or analyze the SBOMs of the software dependencies that you use (if available)?

- ○ Yes (1)
- ○ No (2)
- ○ I don't know (3)

Display This Question:

If Do you process or analyze the SBOMs of the software dependencies that you use (if available)? = Yes

C6 How do you process or analyze the SBOMs of your dependencies? What tools, if any, are involved in the process?

_____

_____

_____

_____

_____

C7 What issues have you faced when consuming SBOMs? Feel free to give examples.

_____

_____

_____

_____

_____

End of Block: SBOM Consumers

Start of Block: SBOM Tool Developers

T1 Please answer the following questions based on your experience developing SBOM tools.

*

T2 Which SBOM format(s) does your tool(s) support?

- [ ] SPDX (1)
- [ ] CycloneDX (2)
- [ ] SWID (3)
- [ ] Other (please specify) (4)

_____

*

T3 What do you use SBOMs for? (select all that apply)

- [ ] To meet regulatory requirements (1)
- [ ] To meet software licensing requirements (2)
- [ ] To learn more about other projects (3)
- [ ] To monitor my project's dependencies (4)
- [ ] To keep track of dependency vulnerabilities (5)
- [ ] Because my organization asks me to (6)
- [ ] To make it easier to understand dependencies in complex projects (7)
- [ ] To proactively identify replacements for components that reach end-of-life (8)
- [ ] Other (please specify) (9) _____
- [ ] ⊗ I don't know (10)

T4 Who is your tool primarily designed for? (select all that apply)

- [ ] Businesses and organizations seeking to meet requirements set by regulatory bodies (1)
- [ ] Software stakeholders seeking to meet licensing requirements (2)
- [ ] Software stakeholders seeking to create SBOMs for their projects (3)
- [ ] Software stakeholders seeking to analyze a project's dependencies (4)
- [ ] Software stakeholders seeking to enhance their projects' security (5)
- [ ] Businesses and organizations seeking to gain insights into the connections between different pieces of software that they use and/or maintain (6)
- [ ] Software stakeholders seeking to remove/replace end-of-life components (7)
- [ ] Other (please specify) (8) _____

T5 Indicate your agreement with the following statement:
"In my industry, developers and other stakeholders are aware of the SBOM tools available to them."

- ○ Strongly disagree (1)
- ○ Disagree (2)
- ○ Neutral (3)
- ○ Agree (4)
- ○ Strongly agree (5)

T6 Which SBOM tools have you developed (or helped develop)? Please give their names.

_____

_____

_____

_____

_____

End of Block: SBOM Tool Developers

Start of Block: SBOM Standard Makers

Sm1 Please answer the following questions based on your experience defining standards / specifications for SBOMs.

Sm2 Where should standards / specifications regarding SBOM creation and usage originate from?

- [ ] Government bodies (1)
- [ ] SBOM Format creators (2)
- [ ] SBOM Tool creators (3)
- [ ] SBOM Producers (4)
- [ ] SBOM Consumers (5)
- [ ] Other (please specify) (6) _____
- [ ] I don't know (7)

Sm3 How should SBOM standards / specifications be effectively communicated?

_____

_____

_____

_____

_____

End of Block: SBOM Standard Makers

Start of Block: SBOM Educators

E1 Please answer the following questions based on your experience developing, compiling, and/or applying educational resources related to SBOMs.

E2 Indicate your agreement with the following statement:
“Software stakeholders understand the purposes / capabilities of SBOMs.”

- Strongly disagree (1)
- Disagree (2)
- Neutral (3)
- Agree (4)
- Strongly agree (5)

E3 Indicate your agreement with the following statement:
“Software stakeholders understand how to use SBOMs.”

- ○ Strongly disagree (1)
- ○ Disagree (2)
- ○ Neutral (3)
- ○ Agree (4)
- ○ Strongly agree (5)

E4 Which SBOM format(s) do you teach about / compile resources for?

- ☐ SPDX (1)
- ☐ CycloneDX (2)
- ☐ SWID (3)
- ☐ Generic: can be applied to any format (4)
- ☐ Other (please specify): (5) _____

E5 What types of resources are best to inform people about SBOMs? Rank by preference by dragging the options.

_____ Official SBOM format documentation (1)
_____ Specialized training courses or seminars (2)
_____ Conference presentations (3)
_____ Curated SBOM examples (4)
_____ Requirements set by regulatory bodies (5)
_____ Integration of SBOM functionality into existing tools (6)
_____ Other (please specify) (7)

End of Block: SBOM Educators

Start of Block: Security

Sc1 Indicate your agreement with the following statement:
“Vulnerabilities reported for software dependencies I use are important issues for my organization.”

- ○ Strongly disagree (1)
- ○ Disagree (2)
- ○ Neutral (3)
- ○ Agree (4)
- ○ Strongly agree (5)
- ○ I don’t know (6)
- ○ I don’t work for any organization (7)

Sc2 Are you involved with writing, reviewing, or maintaining source code?

- ○ Yes (1)
- ○ No (2)

Skip To: End of Block If Are you involved with writing, reviewing, or maintaining source code? = No

Sc3 Indicate your agreement with the following statement:
“I trust security scanners and static analysis tools to find vulnerabilities in my code.”

- ○ Strongly disagree (1)
- ○ Disagree (2)
- ○ Neutral (3)
- ○ Agree (4)
- ○ Strongly agree (5)

Sc4 Indicate your agreement with the following statement:
“I trust that my dependencies are free from security vulnerabilities.”

- ○ Strongly disagree (1)
- ○ Disagree (2)
- ○ Neutral (3)
- ○ Agree (4)
- ○ Strongly agree (5)

Sc5 Do you use a dependency tracking system (e.g. Eclipse SW360, ORT, OWASP Dependency-Track)?

- ○ Yes (1)
- ○ No (2)

Display This Question:

If Do you use a dependency tracking system (e.g. Eclipse SW360, ORT, OWASP Dependency-Track)? = Yes

Sc6 If you use a dependency tracking system (e.g. Eclipse SW360, ORT, OWASP Dependency-Track, etc.), does it allow you to easily determine if your project is impacted by a discovered upstream vulnerability?

- ○ Yes (1)
- ○ No (2)
- ○ I don't know (3)
- ○ I don't use a dependency tracking system (4)

Display This Question:

If Do you use a dependency tracking system (e.g. Eclipse SW360, ORT, OWASP Dependency-Track)? = Yes

And If you use a dependency tracking system (e.g. Eclipse SW360, ORT, OWASP Dependency-Track, etc.),... != I don't use a dependency tracking system

Sc7 What dependency tracking system do you use, and how does it allow you to determine if your project is impacted by a discovered upstream vulnerability?

_____

_____

_____

_____

_____

Sc8 How do you evaluate the security vulnerabilities of the dependencies you use?

_____

_____

Sc9 In the software that you develop, how do you obtain the list of libraries that it uses? Feel free to provide details about any tools used.

End of Block: Security

Start of Block: Demographic Questions

Display This Question:

If Are you involved with writing, reviewing, or maintaining source code? = Yes

Q1 How many years of experience in software development do you have?

Q2 How would you describe your primary role?

- ○ Programmer (1)
- ○ Tester (2)
- ○ Project Lead (3)
- ○ Project Manager (4)
- ○ IT Manager (5)
- ○ DevOps Engineer (6)
- ○ Consultant (7)
- ○ Educator (8)
- ○ Other (please specify): (9) _____

Q3 What is your highest level of education?

- ○ Did not graduate from high school (1)
- ○ High School (2)
- ○ Some college (3)
- ○ Bachelor's Degree (4)
- ○ Master's Degree (5)
- ○ Doctoral Degree (6)
- ○ Other (7) _____

Display This Question:

If Please indicate your knowledge/involvement with SBOMs (Software Bill of Materials), by selecting... = I create SBOMs for the software projects I am involved in

Or Please indicate your knowledge/involvement with SBOMs (Software Bill of Materials), by selecting... = I use the SBOMs of software projects I am involved in or third-party software components/dependencies

Or Please indicate your knowledge/involvement with SBOMs (Software Bill of Materials), by selecting... = I create tools that generate or process SBOMs

Q4 Which programming languages have you most used in past project(s)?

- [ ] Python (1)
- [ ] Java (2)
- [ ] C / C++ (3)
- [ ] Javascript (4)
- [ ] C# (5)
- [ ] Others (please specify): (6) _____

Display This Question:

If Please indicate your knowledge/involvement with SBOMs (Software Bill of Materials), by selecting... = I create SBOMs for the software projects I am involved in

Or Please indicate your knowledge/involvement with SBOMs (Software Bill of Materials), by selecting... = I use the SBOMs of software projects I am involved in or third-party software components/dependencies

Or Please indicate your knowledge/involvement with SBOMs (Software Bill of Materials), by selecting... = I create tools that generate or process SBOMs

Q5 What types of systems have you developed?

- ☐ Operating systems (1)
- ☐ Web applications (2)
- ☐ Mobile applications (3)
- ☐ Desktop applications (4)
- ☐ Middleware (5)
- ☐ Databases (6)
- ☐ Development tools (compilers, prog. languages, etc.) (7)
- ☐ Others (8) _____

Display This Question:

If Please indicate your knowledge/involvement with SBOMs (Software Bill of Materials), by selecting... = I create SBOMs for the software projects I am involved in

Or Please indicate your knowledge/involvement with SBOMs (Software Bill of Materials), by selecting... = I use the SBOMs of software projects I am involved in or third-party software components/dependencies

Or Please indicate your knowledge/involvement with SBOMs (Software Bill of Materials), by selecting... = I create tools that generate or process SBOMs

Q7 For which domains (e.g., banking or healthcare) have you developed applications / systems?

_____

Display This Question:

If Please indicate your knowledge/involvement with SBOMs (Software Bill of Materials), by selecting... = I create SBOMs for the software projects I am involved in

Or Please indicate your knowledge/involvement with SBOMs (Software Bill of Materials), by selecting... = I use the SBOMs of software projects I am involved in or third-party software components/dependencies

Or Please indicate your knowledge/involvement with SBOMs (Software Bill of Materials), by selecting... = I create tools that generate or process SBOMs

Q6 Do you primarily work on open source or closed source projects?

- ○ Open source only (1)
- ○ Closed source only (2)
- ○ Both open source and closed source (3)

Q8 Do you have a background in computer security? Formal (college classes, degree, certification) or informal (self-learning or other training)?

- ○ Yes, formal (1)
- ○ Yes, informal (2)
- ○ No (3)

Q9 Do you have a background in software licensing? Formal (college classes, degree, certification) or informal (self-learning or other training)?

- ○ Yes, formal (1)
- ○ Yes, informal (2)
- ○ No (3)

Display This Question:

If Please indicate your knowledge/involvement with SBOMs (Software Bill of Materials), by selecting... = I create SBOMs for the software projects I am involved in

Or Please indicate your knowledge/involvement with SBOMs (Software Bill of Materials), by selecting... = I use the SBOMs of software projects I am involved in or third-party software components/dependencies

Or Please indicate your knowledge/involvement with SBOMs (Software Bill of Materials), by selecting... = I create tools that generate or process SBOMs

Q10 How often did you release or help release a new major version of an application / software over the past two years?

Please give your best estimate; if you develop more than one software / application, please answer based on the most frequently updated software / application.

- ○ Never (1)
- ○ Annually (2)
- ○ Quarterly (3)
- ○ Monthly (4)
- ○ More frequently (5)

Q11 Which country / countries are you and / or your organization based in?

_____

Q12 Please enter your email address. This will be used to contact you for compensation. If we are interested in your responses, we may contact you for a follow-up interview, if you are willing.

_____

End of Block: Demographic Questions