2024 OpenSSF Meeting Notes Security Tooling WG

SBOM Everywhere SIG

2025 meeting notes

Meeting Info

When: **Every other Tuesday at 11:05 Eastern -** (Open SSF Public Calendar)

Mailing list: openssl-sign-sbom (join to receive calendar invite)

Discussion: #sig-sbom-everywhere on OpenSSF Slack

GitHub: sbom-everywhere

MEETINGS: Log in to your LFX Profile and go to MEETINGS to see your upcoming and past meetings. For help, contact support@openssf.org

Legal / code of conduct

Linux Foundation meetings involve participation by industry competitors, and it is the intention of the Linux Foundation to conduct all of its activities in accordance with applicable antitrust and competition laws. It is therefore extremely important that attendees adhere to meeting agendas, and be aware of, and not participate in, any activities that are prohibited under applicable US state, federal or foreign antitrust and competition laws.

Examples of types of actions that are prohibited at Linux Foundation meetings and in connection with Linux Foundation activities are described in the Linux Foundation Antitrust Policy available at http://www.linuxfoundation.org/antitrust-policy. If you have questions about these matters, please contact your company counsel, or if you are a member of the Linux Foundation, feel free to contact Andrew Updegrove of the firm of Gesmer Updegrove LLP, which provides legal counsel to the Linux Foundation.

Meeting notes

Most recent on top.
Meeting TODO items will be tracked in GitHub
2022/2023 meeting notes

Future agenda items

- SBOM interoperability [Csaba]
- How to measure success
    - We need to better define our success criteria
    - Review the charter and update it as needed
- Someone presents on SPDX 3.0
- Dinesh explains SBOM challenges
-

2025 Meeting Notes - HERE

2024-12-17

Attendees (please add yourself)

- Josh Bressers (Anchore)
- Kate Stewart (Linux Foundation)
- Ian Dunbar-Hall (Lockheed Martin)
- Anthony Harrison (APH10)
- Dick Brooks (BCG)
- Nisha Kumar (Oracle)
- Victor Lu
- Salve J. Nilsen (CPANSec)
- Marius Biebel
- Akihiko Takahashi (Fujitsu)
- Gary O'Neall
- Jarrett Lu

Agenda:

- Please sign in
- Please paste an intro into the chat
- Last meeting of 2024
- Round Table - Announcements & Events upcoming
- Update on Catalog AI plan

- Update on SPDX 3.0 [Gary]
- Anchore Survey results [Kate]
    - Kate has ideas on some community focus for 2025 based on some of these findings
    - https://get.anchore.com/2024-software-supply-chain-security-report/
-

Announcements:

- SBOM Devroom at FOSDEM - lots of good submissions. Schedule posted with some familiar names.
- SBOM tooling meeting before FOSDEM (schedule & signup) - Friday before FOSDEM.
- Situational awareness - US Government DoD appears to be using DI-SESS-82433 as the SBOM Field Requirements
- CMU/SEI plugfest received 160 SBOMs.

Notes:

- Catalog AI Plan:
    - Josh & Marius reaching out to folk; Anthropic are willing to support PoC with funding; pending results will get more. Will be planning blog posts in the new year based on PoC.
- SPDX 3.0:
    - Released patch release 3.0.1.
        - Fixes mostly documentation.
    - Online tools (Java backend) are ready for download and playing with.
    - Can work with commandline now, online tools being updated later in the week.
    - Validators & Converters.
    - Tooling update: Java is there; Go still needs more work; Python tools via code generator, language bindings. Full library for Python is work in progress. C++ code generator is available.
        - Nisha would like the generated code to be turned into a python package
        - Anthony wants to look at Python code for 3.0.
        - Nisha points out: You have to generate it using shacl2code: https://github.com/JPEWdev/shacl2code/ So step 1: install shacl2code, step2: generate python code bindings, step3: use bindings
    - 3.0: Going from Software → Systems. 3.1 is extending trend.
        - Going from Requirements, Services, Operation & Hardware
        - Discussion about Safety and traceability

    - Discussion about VEX - and how do you signal that there are no vulnerabilities when you go to market. How do you show there are no vulnerabilities? Possibly CSAF report with no findings? What is the evidence? An empty CSAF (show ran scan, and no findings). Nothing saying how to do it. Need direction. Might be a topic for the open discussion at the end.
    - Addressing the CRA requirements. Findings released in 12 months time with a playbook. Whether it is intended for commercial use? Documented in CPAN and may be a field to be considered.

2024-12-03

Attendees (please add yourself)

- Josh Bressers (Anchore)
- Kate Stewart (Linux Foundation)
- Nisha Kumar (Oracle)
- Dick Brooks (BCG)
- Sean McGinn (AMD)
- Allen Shearin (LM)
- Jonathan Howard (LM)
- Jeff Diecks (OpenSSF)
- Akihiko Takahashi (Fujitsu)
- Justin Cappos (NYU)
- Salve J. Nilsen (CPANSec)
- Csaba Zoltani (Nokia)
- Bob Martin (MITRE)
- Kris Borchers (OpenSSF)
- Ian Dunbar-Hall (Lockheed Martin)
- Ryan Ware

Agenda:

- Please sign in
- Please paste an intro into the chat
- Round Table - Announcements & Events upcoming
- Ian's PR
    - https://github.com/bomctl/bomctl/pull/223
- Marius plan to fill out Catalog
- Next Meetings over holidays

Announcements:

- SBOM Devroom at FOSDEM - lots of good submissions. Schedule should be

- Host SBOM workshop at SOSS policy summit in DC - cryptographic attestations
    - Looking for ideas to get folks talking and doing things in general
    - Look for around March 4th (shoulder event)
- Energy Sector - SBOM News
    - Likely event in mid February
    - Link to the BSA | Software Alliance comments filed with FERC on SCRM Docket RM24-4-000 are supportive of NIST/CISA guidance is here: https://elibrary.ferc.gov/eLibrary/filelist?accession_number=20241118-5137&optimized=false

Notes:

- Marius Plans to Fill out Catalog
    - Using Scraped info, and ask LLM to interpret it.
    - Using LLM to output structured data
    - Using local GPU for testing
    - Does OpenSSF have access to any API credits from an AI org?
        - Considering asking TAC about any avenues for credits (not sure if there are any) and could also consider doing a TI funding request via the WG. https://github.com/ossf/tac/blob/main/process/TI%20Funding%20Request%20Process.md
    - Put text into LLM to get summary
    - Prompt the LLM for catalog details
    - Cataloging languages is more of a challenge today
    - Humans will review the catalog data
    - Provide some visual indicator about whether info is "AI" or "AI+Human Review" or "Manual Contribute"

- BOMctl
    - Ian, Allen, Jonathan - are maintainers.
    - Looking at linking of documents together in hierarchy.
    - SBOM Document Linking Scenarios provides overview
    - Working with protobom maintainers, and trying to figure out user experience with bomctl for the linkage.
    - Feedback from Nisha on container use cases and Kate on handling internal linkages already in some of the SBOMs - pointed to https://zephyr-dashboard.renode.io/ for examples.

- Next Meeting: Dec 17, then breaking until January

2024-11-19

Attendees (please add yourself)

- Josh Bressers (Anchore)
- Kate Stewart (Linux Foundation)

- Amar Takhar (RTEMS Project)
- Marius Biebel (hm.edu)
- Seth Larson (Python Software Foundation)
- Akihiko Takahashi (Fujitsu)
- Nisha Kumar (Oracle)
- Salve J. Nilsen (CPANSec)
- Anthony Harrison (APH10)
- Karen Bennet (IEEE/ISO)

Agenda:

- Please sign in
- Please paste an intro into the chat
- Update from Kate on the last quarter
- A discussion on future group direction

Announcements:

- CFP for FOSDEM SBOM Devroom until Dec 1 - https://fosdem.org/2025/schedule/track/sbom/
- AI BOM - https://www.linuxfoundation.org/hubfs/LF%20Research/lfr_spdx_aibom_102524a.pdf
- MITRE data normalization challenges
    - https://www.mitre.org/news-insights/publication/data-normalization-challenges-mitigations-software-bill-materials-processing
-

Notes:

- Kate's document
    - https://docs.google.com/document/d/1GJAKktTNtEzRPzLW1JKOYpqINMweE2cB-hG5Q1mnlc4/edit?tab=t.0
    - We went through many aspects of this during the call
- SBOM Framing from CISA (3rd edition)
    - https://www.cisa.gov/resources-tools/resources/framing-software-component-transparency-2024
- There are also similar documents from India and Germany
- SBOM comparison spreadsheet
    - https://docs.google.com/spreadsheets/d/1SuGv1L3H_-Iq6dmH7DnjDgAa90LCRnoHB3DTfuWh0Jg/edit?gid=1936044844#gid=1936044844
-

2024-11-05

Attendees (please add yourself)

- Josh Bressers (Anchore)
- Paul Davis (JFrog)
- Seth Larson (PSF)
- Salve J. Nilsen (CPANSec)
- Ian Dunbar-Hall (Lockheed Martin)
- Allan Friedman (CISA)
- Marius Biebel (hm.edu)
- Akihiko Takahashi (Fujitsu)
- Nisha Kumar (Oracle)
- Ryan Ware (me)

Agenda:

- Please sign in
- Please paste an intro into the chat
- Interesting projects and ideas
    - Daggerboard
        - https://github.com/nyph-infosec/daggerboard
    - Add this to the catalog [Josh (or anyone who beats him to it)]
    - Note phantom dependencies in the wiki
    -
- Trademarks? - We should ask the lawyers [JeffD]
    - This is still open with legal
- [Seth] SBOMs for non-Python software in Python packages
    - Project repo: https://github.com/sethmlarson/sboms-for-python-packages
    - Solve the phantom dependency problem for Python packages
        - There can be projects inside of packages/projects that aren't accounted for in the metadata
        - We could put an SBOM inside of a package that includes the phantom dependencies
        - This isn't a python specific problem, every ecosystem has similar problems
        - Bomctl SBOM linking
            - https://docs.google.com/document/d/1Dj-OAycyAH3d6A9vPJWIdNoLRArRVB607to_0s5Fk8w/edit?tab=t.0#heading=h.qflhf8nb1xeo
- learnings/developments that has come out of CPANSec's Supply-chain/SBOM overview [Salve]
    - https://github.com/CPAN-Security/security.metacpan.org/blob/main/docs/supplychain-sbom.md

        - Appendix of SBOM Attribute names and obligation sources
            - https://github.com/CPAN-Security/security.metacpan.org/blob/main/docs/supplychain-sbom.md#sbom-attribute-names-and-obligation-sources
        -
- Status update on projects
    - Evangelism
-
- Working session if no other topics are added

2024-10-08

Attendees (please add yourself)

- Josh Bressers (Anchore)
- Marius Biebel
- Seth Larson (Python Software Foundation)
- Salve J. Nilsen (CPANSec)
- Ben Cotton (Kusari)
- Victoria Ontiveros (CISA)
- Nisha Kumar (Oracle)
- Ryan Ware
- Akihiko Takahashi (Fujitsu)
- Jeff Dieccks (OpenSSF)

Agenda:

- Please sign in
- Please paste an intro into the chat
- Status update on projects
    - Contributing guide
        - https://github.com/joshbressers/sbom-everywhere/blob/20240901-getting-started/CONTRIBUTING.md
        - Also add a section on how to file an issue [Josh]
- Contributing policy
    - Put all this in the contributing guide
    - We need to define what the expectations are around contributing
        - Some questions to get us started
        - Can anyone update any entry?
            - Commercial vs open source?
                - Should we treat these differently
                - Trademarks? - We should ask the lawyers [JeffD]
                    - Is this fair use?
                    - Ask the operations folks

            - If we stick to factual details, can we add whatever we want?
                - We are not implying endorsement
                - If we make mistakes, it's very easy to update (PR and issues welcome)
        - How can we represent tool popularity on tooling?
            - Maybe stars
            - Days since release
            - Number of unique contributors
            - Number of issues
            - We might not want to solve this
            -
        - Who resolves conflicts?
            - Show me
                - If we are only showing provably factual details, conflicts will be harder
                - We can defer to the documentation if we can't try something out
            - Citation needed
                - Make sure we require a link to the documentation/project/blog
            - This will probably be seen as a marketing vehicle for some orgs
                - If we get complaints, we can investigate
            - Add a note that the SBOM Everywhere project has the final say
                - If they don't like it, they can remove their tool
                -
        - We should define maintainers (the people who have oversized influence)
            - We could defer the structure to the OpenSSF (send complaints to the management)
        -
    - Let's figure out those questions (we don't have to answer them today)
- CISA categories work
    - https://onedrive.live.com/view.aspx?resid=68652AA55C12F19A%216830&authkey=!AG7Yjwi-1S3rjWI
    - https://docs.google.com/document/d/1TKPIjT7Rfc38F0OMuXIlPqFRoH7wj2H8×3w13Pgy8V4/edit#heading=h.3kcprhiiv0b8
    -

2024-09-24

Attendees (please add yourself)

- Josh Bressers (Anchore)
- Marius Biebel
- Karen Bennet (IEEE)
- Ian Dunbar-Hall (Lockheed Martin)
- Ryan Ware (ST WG Chair)
- Jeff Diecks (OpenSSF)
- Akihiko Takahashi (Fujitsu)

Agenda:

- Please sign in
- Please paste an intro into the chat
- Open Source Summit update (anyone who attended)
- Status update on projects
    - Contributing guide
        - https://github.com/joshbressers/sbom-everywhere/blob/20240901-getting-started/CONTRIBUTING.md
- Working session if no other topics come up
    - Let's add some of the orgs on the CISA SBOM-a-Rama list
        - https://www.cisa.gov/resources-tools/resources/sbom-solutions-showcase
        - TODO (for the contributing)
        - Every vendor needs a product
            - Probably just start with some open source things for now
        - Clearly define the standards, abilities, and types
        - Define the languages
        - Explain the logos

Notes

- Brief overview from the Open Source Summit EU (By Marius):
    - Several talks introduced SBOM at several micro conferences.
    - There was some talk about how to produce and consume an SBOM. But not a lot on how to manage and exchange them. (Which are major use cases)
    - This leads to some confusion, such as, "Why should I produce an SBOM for myself when I can enable Dependabot or integrate Renovatebot?" This is a valid question if you don't know about the lifecycle of an SBOM and that it's intended for exchange.
    - Also, there is little to say on exchanging SBOM automatically. I only know that OWASP works on the Transparency Exchange API specification. https://tc54.org/tea/

    - CISA introduced its work on EOL / EOS, which is not directly linked to SBOM but addresses similar needs. https://github.com/oasis-tcs/openeox
- CISA Tiger Team SBOM Generation
    - https://github.com/CISA-SBOM-Community/SBOM-Generation/tree/main
- Maybe a blog post about creating SBOMs
    - Tie this into the SBOM Generation work
    - Don't try to make everyone happy
-

2024-09-10

Attendees (please add yourself)

- Josh Bressers (Anchore)
- Vivek kumar Sahu(Interlynk)
- Marius Biebel
- Kate Stewart (LF)
- Nisha Kumar (Oracle)
- Salve J. Nilsen (CPANSec)
- Ryan Ware
- Akihiko Takahashi (Fujitsu)
- Ian (briefly)

Agenda:

- Please sign in
- Please paste an intro into the chat
- Status update on projects
    - Contributing guide
        - https://github.com/joshbressers/sbom-everywhere/blob/20240901-getting-started/CONTRIBUTING.md
    - Marius added a ton of new tools
        - https://github.com/ossf/sbom-everywhere
        - https://sbom-catalog.openssf.org/catalog/#/Circle/Normalize/HowTo
- Working session if no other topics come up
    - FAQ?
- CycloneDX OSS Sustainability WG has started; Next meeting is on Thursday September 19th, at 19:00 CEST (Note the new time! One hour later)
    - Google Calendar invite
    - Video from last meeting: https://www.youtube.com/watch?v=sWrzDYrsevo

Notes

- If someone would like to add any of the orgs on the CISA SBOM-a-Rama list, please do!
    - https://www.cisa.gov/resources-tools/resources/sbom-solutions-showcase
    - Ask if you have any questions or need any help
-

2024-08-27

Attendees (please add yourself)

- Josh Bressers (Anchore)
- Kate Stewart (Linux Foundation)
- L. Jean Camp (Indiana U)
- Xinyao Ma (Indiana U)
- Marius Biebel
- Adolfo García Veytia (Stacklok)
- Salve J. Nilsen (CPANSec)
- Akihiko Takahashi (Fujitsu)
- Seth Larson (PSF)
- Ryan Ware

Agenda:

- Please sign in
- Please paste an intro into the chat
- L Jean Camp SBOM Survey
- Security Summer Camp Updates (aka BlackHat/DevCon/BSides)
- CycloneDX OSS Sustainability WG has started
    - Working document

Notes

- SBOM Survey
    - working to understand if visualization of SBOM will help with comprehension
    - Looking for folks to do the survey that are "knowledgable" and "very knowledgeable" about SBOMs
    - Figure out how effective unprocessed SBOM data actually is.
    - Research will be ending in December, and they're willing to come back and let us know their findings.
    - Survey can be found at https://iu.co1.qualtrics.com/jfe/form/SV_cY2RasQrgy0SpXE (https://go.iu.edu/8qy2) It is open to anyone, so please share with your SBOM colleagues. See email list for slides.
        - Probably close on Nov 1

- SBOM Landscape
    - Preparing for SBOM-a-rama
    - Haven't heard back from CISA
    - Josh writing a "how to submit" a pull request to add to the landscape.
- CISA SBOM-a-rama
    - Ian & Adolfo will be at OpenSSF booth.
    - Marius & Adolfo to get together
- Vegas Update
    - Operationalization is starting to show up - it's getting boring. Which is what we want.
    - Software Asset Inventory folk need interaction
- Seth has been working a cross-reference of what CPython is generating to the new guidance draft, we're not far off: https://github.com/python/cpython/issues/123038
- CycloneDX Sustainability - will include metadata for the needs, and targeting it for 1.7.
    - Meeting every other thursday - looking for help; ecosystems publish through as well as maintainers.
    - Seth pointed out https://github.com/tacosframework
- Salve still looking for input for CRA mapping. Looking for funding for CSPAN efforts.

2024-08-13

Attendees (please add yourself)

- Kate Stewart
- Seth Larson (PSF)
- Marius Biebel
- Salve J. Nilsen (CPANSec)
- Ian Dunbar-Hall (Lockheed Martin)
- Fotis Georgatos

Agenda:

- Please sign in
- Updates on CISA SBOM Framing Document [Kate]
    - Final call for comments on an update to “Minimum Elements”
    - https://docs.google.com/document/d/1z8hKtPxs5OWaspst120NHN9XXgyULGI2aKdSebwIYPc/edit
    - This document is almost finalized. We want to send it out for one last "urgent stop" read. If there is anything in this document that you feel really

should not be (or something that MUST be added) please email:, melissa.m.rhodes@medtronic.com, kstewart@linuxfoundation.org, sbom@cisa.dhs.gov
    - Salve has some suggestions based on the perspective of open source language ecosystems.
    - Would like to see future drafts include information about open source project health for components. Places for input from actors in the supply chain also needs to be considered.
    - Minimum elements need to be in both formats to extend beyond the minimum set.
- Update on SBOM Generation Reference Implementations (Ian)
    - https://github.com/CISA-SBOM-Community/SBOM-Generation
    - Keycloak for first project to target
        - https://github.com/keycloak/keycloak/discussions/31952
    - Working on pulling this together implementation with the Framing Document - Rev 3.
    - Divided into "how to" -generate SBOM with existing tool, augment toplevel meta components, dependency tree, validation it all.
    - Plan on getting a good reference of this working, for ecosystem to cut/paste. Using Trivy for first reference implementation.
    - Next challenge is enrichment - Parlay / Snyk. How validate compliance. Ideally common tool to do both. What about protobom related ones? Work is going on with bomctl project which might be useful.
- CPAN Security Group Update (Salve)
    - Has also been working on a glossary and is looking for further input. Esp. when some of the terms are used elsewhere, provide the citation.
    - https://security.metacpan.org/docs/glossary.html

2024-07-30

No meeting

2024-07-16

Attendees (please add yourself)

- Josh Bressers (Anchore)
- Ian Dunbar-Hall (Lockheed Martin)
- Allan Friedman (CISA)
- Dick Brooks (BCG)
- Seth Larson (PSF)
- Akihiko Takahashi (Fujitsu)

- Marius Biebel

Agenda:

- Please sign in
- Please paste an intro into the chat
- Update on CISA Generation Reference Implementation [Ian]
    - https://docs.google.com/document/d/11UU_Wiaemi7zBs3sE-MgovieyPx1XJEOaju2EM5btts/edit#heading=h.ljwu4fxnbeg2
    -
    - CISA moved from workstreams to targeted teams
    - Tiger team create golden path for others to follow to create SBOMs
    - We can find holes in the existing tooling
    - Outcome - create defined working example pipelines for others to reference
- OpenSSF booth at SBOM-a-rama
    - Show off OpenSSF tooling at a booth
    -
- Catalog future maintenance [Josh]
    - One idea
        - You are responsible for your entry
        - After a year of no updates, you fall off the list
    - Categorizing tooling?
        - Open source vs commercial?
            - Who is backing a project
            - Maybe list the actual license instead of open vs commercial
            - SPDX license when possible, we can use a Commercial catchall for other things
    - Create TODO tasks
        - File lots of issues with specific guidance [Josh]
        - Create a nice contributing guide
        - Add a “get involved” section
        - Add some content on how we can promote this
            - We need to promote it now for help
            - We’re not quite ready yet for more general promotion
        -

2024-07-02

Attendees (please add yourself)

- Josh Bressers (Anchore)
- Nisha Kumar (Oracle)
- Marius Biebel
- Salve J. Nilsen (CPANSec)

- Akihiko Takahashi (Fujitsu)
- Dick Brooks (BCG)
- Kate Stewart (LF)
- Dinesh Visweswaraiah (Morgan Stanley)
- Deanna Medina (Honeywell)
- Sean McGinn (AMD)

Agenda:

- Please sign in
- Please paste an intro into the chat
- If there is any time, i would like to share this addition to the Catalog. The idea was already mentioned several times that the catalog could contain more than just “The Tools”. Like the information we gather and share in this group. I went to the Meeting Notes of this year and put some topics together. The basic idea is that we have a place to point to when we want to share some information / advice / etc. Another advantage is that we don’t have to finalize every text to 120% before we share it, but we can also update something if things change or we learn something new. The page is based on Markdown files in our GitHub. So we don’t have to change our current workflow. I would like to hear your opinion on this. Put together the following as POC:
    - Getting Started
    - SBOM Compliance
    - SBOM Working Groups
    - Guidance
        - SBOM Types
        - SBOM Naming
        - About us
- Catalog future maintenance [Josh]
    - One idea
        - You are responsible for your entry
        - After a year of no updates, you fall off the list
    - We also need to see more involvement outside of the call
    -

2024-06-18

Attendees (please add yourself)

- Josh Bressers (Anchore)
- Marius Biebel
- Kate Stewart (LF)
- Allan Friedman (CISA)
- Nisha Kumar (Oracle)
- Deanna Medina, (Honeywell)
- Dick Brooks (BCG)

- Dinesh Visweswaraiah (Morgan Stanley)
- Marius Biebel
- Akihiko Takahashi (Fsas Technologies)
- Adolfo García Veytia
- Salve J. Nilsen (CPANSec)
- Karen Bennet (IEEE, ISO)

Agenda:

- Please sign in
- Please paste an intro into the chat
- SBOM-a-rama
    - Sept 11-12
    - Registration is open (max in person is 225 people, at 70 right now)
    - Hybrid event (Denver)
    - Updates from key communities
    - Solutions showcase on Sept 12
        - Registration opens on June 20 12pm Eastern
        - 22 slots
        - First come first serve
        - Looking for open source projects who want to participate as well. Not just vendors.
- Salve presents his Supply Chain SBOM overview
    - https://github.com/CPAN-Security/security.metacpan.org/blob/main/docs/supplychain-sbom.md
    - Some overlap/contrast with Tool taxonomy: https://www.ntia.gov/sites/default/files/publications/ntia_sbom_tooling_taxonomy-2021mar30_0.pdf
    - Some of the terms used are CycloneDX specific, when a general term exists.
    - Deep dive into the idea of “authoritative” authors
    - Discussion on project health, and best ways for maintainers for communicating metadata to wider set of users.
- TODO
    - Add Oasis EOL group to catalog
        - Also dig up some CISA groups to add
    -

2024-06-04

Attendees (please add yourself)

- Josh Bressers (Anchore)
- Jarrett Lu (Oracle)

- Nisha Kumar (Oracle)
- Gary O'Neall (Source Auditor, SPDX)
- Marius Biebel
- Ian Dunbar-Hall (Lockheed Martin)
- Yotam Perkal (Rezilion)
- Deanna Medina (Honeywell)
- Dana Wang(OpenSSF)
- Chris de Almeida (IBM)
- Akihiko Takahashi (Fsas Technologies)
- Salve J. Nilsen (CPANSec)

Agenda:

- Please sign in
- Please paste an intro into the chat
- Steve Spingett on all the things the CycloneDX crew has been up to
    - https://openssf.slack.com/archives/C03GKSYFRC0/p1716412930862049?thread_ts=1716405087.349399&cid=C03GKSYFRC0
- SBOM Probe now is Scorecard
- Notes
    - TC54 will be a long running group
    - To join the ecma group, you need to be an ecma member
    - Slides
        - https://docs.google.com/presentation/d/1VUYpbiB5tbDceuQfmMx4IvaRx8Hr3M7hqbUi4i_yOE4/edit
    -
- TODO
    -

2024-05-21

Attendees (please add yourself)

- Josh Bressers (Anchore)
- Salve J. Nilsen (CPANSec)
- Nisha Kumar (Oracle)
- Marius Biebel
- Jarrett Lu (Oracle)
- Dick Brooks (REA)
- Anthony Harrison (APH10)
- Karen Bennet (IEEE)
- Akihiko Takahashi (Fsas Technologies)
- Kate Stewart (Linux Foundation)
- Jarrett Lu

- Dinesh Visweswaraiah (Morgan Stanley)
- Eddie Zaneski (Defense Unicorns)
- Sean McGinn (AMD)

Agenda:

- Please sign in
- Please paste an intro into the chat
- Gary to present on SPDX 3.0
- Interesting news
    - US GSA SBOM Sharing
        - https://www.linkedin.com/feed/update/urn:li:activity:7196518054288072704/
    - CISA Sharing Primer
        - https://www.cisa.gov/resources-tools/resources/sbom-sharing-primer
    -
- TODO:
    - Are these meetings making it to Youtube?
        - We will want this particular meeting somewhere we can reference
        - They are posted to https://openprofile.dev/
    - Invite the SPDX security group to give an overview of the changes.

Notes:

- Open discussion started from DInesh: Last mile of sharing SBOMs, what are the conventions on where to fin?
    - CISA SBOM Sharing Primer is a bit too general https://www.cisa.gov/resources-tools/resources/sbom-sharing-primer
- The folks behind Open Component Model (https://ocm.software) will be coming into the Security Tooling WG.
- SPDX 3.0 presentation from Gary
    - Simplifying profiles & handing data at scale with relationship structures.

2024-05-07

Attendees (please add yourself)

- Josh Bressers (Anchore)
- Marius Biebel
- Dick Brooks (REA)
- Sean McGinn (AMD)
- Ixchel Ruiz (Karakun)
- Nicholas Strong (AMD)

- Akihiko Takahashi (Fsas Technologies)
- Kate Stewart (LF)
- Dinesh Visweswaraiah
- Eddie Zane
- Jing
- Nisha Kumar (Oracle)
- Reden Martinez
- Yotam Perkal

Agenda:

- Please sign in
- Please paste an intro into the chat
- Catalog status
    - https://github.com/ossf/sbom-everywhere/tree/main/SBOM-Catalog
    - https://sbom-catalog.openssf.org/
    - CISA catalog primer
        - https://docs.google.com/document/d/1l8qVms7YDJK4L_5gMYhrN9uYdy-SGp49WqecaimqHnw/edit#heading=h.mwk61i3dtrln
    -
- Continue discussion
    - https://github.com/ossf/sbom-everywhere/issues/46
    - Lessons learned working with CPAN
        -
        - This data is A LOT harder to figure out than I expected [Josh]
- Working with CPAN on their documents
    - This is related to the Strike Team proposal (we will learn things helping CPAN)
        - SBOM Everywhere Strike Team proposal
    - https://security.metacpan.org/docs/glossary.html
    - https://security.metacpan.org/docs/supplychain-sbom.html
- TODO
    - We need a catalog orientation
    - Can we add more CISA types
        - https://www.cisa.gov/sites/default/files/2023-04/sbom-types-document-508c.pdf
    - Catalog getting started guide [Josh]
        - Kate will verify the instructions
    -

2024-04-23

Attendees (please add yourself)

- Josh Bressers (Anchore)
- Salve J. Nilsen (CPANSec)
- Marius Biebel
- Anthony Harrison (APH10)
- Kate Stewart (LF)
- Akihiko Takahashi (Fsas Technologies)
- Allan Friedman (CISA)
- Eddie Zane
- Ian Dunbar-Hall
- Josh Buker
- Maximillian Huber (TNG)
- Reden Martinez
- Salve J. Nilsen (CPANSec)
- Sean McGinn

Agenda:

- Please sign in
- Please paste an intro into the chat
- OSS Summit Meeting
    - Summary of the meetings
    - Protobom released
    - SPDX 3.0 released
    - Scorecard maintainers and SBOMs meeting
        - No score for SBOM generation, but will collect metrics
        - Where will SBOMs be for each ecosystem
    - CISA work on end of life in software
- SPDX 3.0
    - Lifecycle concept from CISA has been added
    - EOL and support models with dates
    - AI/ML modeling
    - Dataset modeling
    - Moving toward systems
        - Hardware, services, ...
    - OMG board was part of this
    - Multiple profiles are supported
    - Small core set of required fields for all profiles
    - Software profile, licensing profile
        - https://spdx.dev/learn/areas-of-interest/
        - There is an underlying model
- Marius Catalog
    - It's nearly ready for a PR
    - We need to figure out what the next steps are

        - Some sort of openssf domain (ask openssf ops folks)
- Working with CPAN on their documents
    - This is related to the Strike Team proposal (we will learn things helping CPAN)
        - SBOM Everywhere Strike Team proposal
    - https://security.metacpan.org/docs/glossary.html
    - https://security.metacpan.org/docs/supplychain-sbom.html
    - GitHub Repo
    - https://github.com/CPAN-Security/security.metacpan.org/blob/supplychain-sbom/docs/supplychain-sbom.md
    - https://spdx.github.io/spdx-spec/v2.3/how-to-use/
    - https://spdx.github.io/spdx-spec/v3.0/annexes/using-SPDX-to-comply-with-industry-guidance/#f1-satisfying-ntia-minimum-elements-for-an-sbom-using-spdx-us-executive-order-14028
    -
- Continue discussion
    - https://github.com/ossf/sbom-everywhere/issues/46

Actions

- Invite Gary to present on SPDX 3.0 to SBOM everywhere group - DONE: Kate confirms Gary can present on May 21, 2024.
- Can we work with this for placement of SBOMs in projects
    - https://reuse.software/spec/
- Josh will review Marius PR
- Josh and Kate work with OpenSSF IT side for Catalog
- Josh will talk to Josh about Ruby
-

2024-04-09

Attendees (please add yourself)

- Josh Bressers (Anchore)
- Marius Biebel (hm.edu)
- Jarrett Lu (Oracle)
- Salve J. Nilsen (CPANSec)
- Maximilian Huber (TNG Technology Consulting)
- Allan Friedman (CISA)
- Ian Dunbar-Hall (Lockheed Martin)
- Michael Gadda (Intel)
- Akihiko Takahashi (Fsas Technologies)

Agenda:

- Please paste an intro into the chat

- OSS Summit Meetings
    - Tuesday 11:30 @ OpenSSF Booth - Scorecard conversation (adding SBOM checks, what do the scorecard maintainers need?)
    - Wed noon @ OpenSSF Booth - Tooling WG vision meeting
    - Can we also get a summary of these meetings after the summit?
- ~~Landscape~~ - Rename to “SBOM Catalog”
    - Where should we put this?
        - Put in the SBOM Everywhere repo
    - How do we get started
        - Once it’s there, submit PRs
    - Link to Landscape: https://hm-seclab.github.io/SBOM-Landscape/
    - Link to Repository: https://github.com/hm-seclab/SBOM-Landscape
    - https://docs.google.com/document/d/16mow3kRtvI-HTnXC8kHp-0DiIQCILgWxA5gST1CJUZo/edit#heading=h.joo10r6fp67j
- SBOM Everywhere to amplify guidance
    - https://github.com/ossf/sbom-everywhere/issues/46
    - How do we amplify the guidance from this SIG?
    - Do other groups do some of this?
        - Blog posts from projects/SIGs/WGs
        - There isn’t a consistent way to amplify this message
        - Can we have an open source focused SBOM stream? Work with CISA?
        - CISA is reorganizing and focusing their groups
            - There is no open source focused stream
            - Rather than having standing meetings with broad focuses, have a one stop shop for discovering what’s happening
            - Support targeted efforts
            - Try to get legitimacy from a breadth of contributions
            - We should have someone from here show up on a regular basis to provide updates
            -
- Maybe Strike team
    - SBOM Everywhere Strike Team proposal
    - Salve from CPAN is looking for some help to do something very similar to this. We are moving the discussion to Slack
        - https://security.metacpan.orlg/docs/glossary.html
        - https://security.metacpan.org/docs/supplychain-sbom.html
        -
- TODO
    - Talk to OpenSSF about amplification
        - Josh to the marketing group about this
        - Also start a discussion about this on the mailing and Slack

    - This issue talks about some ideas around how this group could work on content from others https://github.com/ossf/sbom-everywhere/issues/46
        - Some of this is already happening, we probably need to talk to other groups
    - Marius will add his catalog to the sbom everywhere repo
    - Salve and SBOM in the CPAN ecosystem

2024-03-26

No meeting

2024-03-12

Attendees (please add yourself)

- Josh Bressers (Anchore)
- Ian Dunbar-Hall (Lockheed Martin)
- Allan Friedman (CISA)
- Akihiko Takahashi (Fujitsu)
- Jarrett Lu (Oracle)
- Sean McGinn (AMD)
- Andres Orbe (Cloudflare)

Agenda:

- Please paste an intro into the chat
- Global Government Expert Forum [Allan]
    - CISA convened a meeting with partner governments cybersecurity agencies on SBOM
    - 14 countries, including European Commission and ENISA
    - Many countries are planning to issue guidance on software supply chain transparency
    - DIscussion: risks of divergence
- Amplifying SBOM Everywhere Guidance through CISA SBOM Workstreams
    - We should try to do this, yes
    - How can we do this?
    - The types document is an example of this cross-collaboration
    - OpenSSF could incubate things that feeds into other groups?
    - There is guidance from various governments already
        - We should look at what these say and identify overlap
    - Allan will share links to the various government SBOM guidance
        - We should look for commonality and differences in these documents

            - Dutch SBOM https://www.ncsc.nl/documenten/publicaties/2023/juli/5/sbom-startersgids
            - Germany https://www.bsi.bund.de/SharedDocs/Downloads/EN/BSI/Publications/TechGuidelines/TR03183/BSI-TR-03183-2.pdf?__blob=publicationFile&v=4
            - Japan https://www.meti.go.jp/english/press/2023/0728_001.html
        - Mapping all the SBOM fields could also be a valuable task
        -
- AI SBOMs
    - AI people don't understand software transparency
    - SBOM people don't understand what makes ML different from software
    - A few groups are trying to plan something at RSA
    - Active working group in SPDX welcomes participants with use cases
- Landscape
    - Link to Landscape: https://hm-seclab.github.io/SBOM-Landscape/
    - Link to Repository: https://github.com/hm-seclab/SBOM-Landscape
    - https://docs.google.com/document/d/16mow3kRtvI-HTnXC8kHp-0DilQCILgWxA5gST1CJUZo/edit#heading=h.joo10r6fp67j
- Maybe Strike team
    - SBOM Everywhere Strike Team proposal
- Measuring SBOM adoption
    - When should an SBOM be generated in OpenSource? Guidance
    - This is very related to the strike team idea
    -

2024-02-27

Attendees (please add yourself)

- Josh Bressers (Anchore)
- Seth Larson (PSF)
- Marius Biebel (hm.edu)
- Gary O'Neall (SourceAuditor)
- Dick Brooks (REA)
- Georg Kunz (Ericsson)
- Ian Dunbar-Hall (Lockheed Martin)
- Lucas Kiker (AMD)
- Akihiko Takahashi (Fujitsu)
- Josh Buker (Cloud Security Alliance)
- Allan Friedman (CISA)

- Nicholas Strong (AMD)
- Ryan Ware (Intel)
- Matt Rutkowski (IBM)
- Adolfo Harcía Veytia (Stacklok)
- Lynn Westfall (The Modem Lisa)
- Sean McGinn (AMD)
- Max Combüchen (Snyk)
- Reden Martinez (Linux Foundation)
- Karen Bennet (IEEE/ISO)
- Jarrett Lu (Oracle)
- Janane Suresh (Oracle)

Agenda:

- Please paste an intro into the chat
- [Josh] SBOM-a-Rama
    - We get 10 minutes for SBOM Everywhere
        - Actually it's titled "OPEN SSF SBOM ACTIVITIES"
- [allan] - would you like a brief CISA update?
    - Internal government wide SBOM playbook
        - Transition from "what's an SBOM" to "We have an SBOM, now what?"
    - Launching government expert group
    - NTIA minimum elements (written in 2021) will be refreshed
        - Will be a formal comment process
    - SBOM-a-Rama - talking about transitioning to phase 2 of effort
        - 5 meetings to fewer meetings
- Ian's SBOM low level tooling standardization
    - Task force in DC
    - Working session in tooling WG - expand on protobom
    - Focus on SBOM manipulation, not generation or consumption
    - Bomctl is the starting point
        - https://github.com/bomctl/bomctl
    - CycloneDX sbom-utility does some of this already
        - https://github.com/CycloneDX/sbom-utility
        - OWASP URN tagging system to identify security data
    - OWASP Software Comp. Verification Standard (SCVS)
        - OWASP WG summary page: https://owasp.org/www-project-software-component-verification-standard/
        - SCVS "How to participate"
            - https://scvs.owasp.org/participate
        - CycloneDX SBOM-relative description: https://cyclonedx.org/guides/sbom/bom/
        - Home page (new release recently): https://scvs.owasp.org/
            - BOM Maturity model: https://scvs.owasp.org/bom-maturity-model/

        - Taxonomy (component ID urn tags): https://scvs.owasp.org/bom-maturity-model/urn/owasp/scvs/bom/resource/software/identity/
        - **Sample NTIA profile**: https://scvs.owasp.org/bom-maturity-model/profiles/examples/ntia-minimum-elements/

- Landscape update
    - [marius] migrated the Landscape from Gitlab to Github and setup github actions
        - Link to Landscape: https://hm-seclab.github.io/SBOM-Landscape/
        - Link to Repository: https://github.com/hm-seclab/SBOM-Landscape
    - https://docs.google.com/document/d/16mow3kRtvI-HTnXC8kHp-0DiIQCILgWxA5gST1CJUZo/edit#heading=h.joo10r6fp67j
    - We're going to let the TAC stew on this
    - CISA tooling criteria
        - https://docs.google.com/spreadsheets/d/1VenR5q8AWdqPsMBGNiFam08IjfszUdzAx6JRyZCPc7A/edit#gid=1705310822
        - Meeting doc - https://docs.google.com/document/d/1I8qVms7YDJK4L_5gMYhrN9uYdy-SGp49WqecaimqHnw/edit#heading=h.8m5zb9te9xsj
        - White paper - https://docs.google.com/document/d/1TKPIjT7Rfc38F0OMuXIIPqFRoH7wj2H8x3w13Pgy8V4/edit#heading=h.3kcprhiiv0b8
        - Google group - https://groups.google.com/g/sbom-tooling-cataloging
        -
- Security Tooling WG TAC Update
- [Dick Brooks] - CISA buyer's guide
    - Create document for vendors to better understand how to meet the EO and attestation form
    - Conference scheduled for June about this guide
    - https://www.cisa.gov/ict-scrm-task-force-members
    -
- Maybe Strike team
    - SBOM Everywhere Strike Team proposal

2024-02-13

Attendees (please add yourself)

- Josh Bressers (Anchore)
- Kate Stewart (Linux Foundation
- Nisha Kumar (Oracle)
- Marius Biebel (hm.edu)
- Seth Larson (he/him, PSF)
- Sean McGinn (AMD)

- Lucas Kiker (AMD)
- Akihiko Takahashi (Fujitsu)
- Josh Buker (Cloud Security Alliance)
- Karen Bennet (IEEE/ISO)
- Roberth Strand (Sopra Steria)
- Janane Suresh (Oracle)
-

Agenda:

- Please paste an intro into the chat
- [Seth] CPython SBOM project status and challenges
    -
- Landscape proposal
    - https://docs.google.com/document/d/16mow3kRtvI-HTnXC8kHp-0DilQCILgWxA5gST1CJUZo/edit#heading=h.joo10r6fp67j
-

2024-01-30

Attendees (please add yourself)

- Josh Bressers (Anchore)
- Marius Biebel (hm.edu)
- Lynn Westfall (The Modem Lisa)
- Jarrett Lu (Oracle)
- Ian Dunbar-Hall (Lockheed Martin)
- Maximilian Huber (TNG Technology Consulting)
- Janane Suresh (Oracle)
- Ryan Ware (Intel)
- Georg Kunz (Ericsson)
- Nicholas Strong (AMD)
- Matt Rutkowski (IBM)
- Jon Velando (individual contributor)

Agenda:

- Please paste an intro into the chat
- Landscape proposal
    - https://docs.google.com/document/d/16mow3kRtvI-HTnXC8kHp-0DilQCILgWxA5gST1CJUZo/edit#heading=h.joo10r6fp67j
- Strike team
    - SBOM Everywhere Strike Team proposal
    - We need to figure out how to move this forward
    - TODO

        - Josh to clean up the comments
        - GB meeting in mid Feb (if we can get this on the agenda that would be nice)
        - We will gain consensus from the group
            - Set a timebox on this, we can't debate it forever
        - Mail the TAC for feedback
-

2024-01-16

Attendees (please add yourself)

- Josh Bressers (Anchore)
- Marius Biebel (hm.edu)
- Ian Dunbar-Hall (Lockheed Martin)
- Sean McGinn (AMD)
- Jon Velando (individual contributor; conda-forge feedstocks maintainer)
- Csaba Zoltani (Nokia)
- Lucas Kiker (AMD)
- Akihiko Takahashi (Fujitsu)
- Jarrett Lu (Oracle)
- Justin Cappos (NYU)
- Georg Kunz (Ericsson)
- Kate Stewart (Linux Foundation)
- Ryan Ware (Intel)

Agenda:

- Please paste an intro into the chat
- Josh to mail TAC about SBOM Naming document
    - https://github.com/ossf/sbom-everywhere/blob/main/reference/sbom_naming.md
- Marius shows off tool tracking tool
    - https://sbom-landscape-mariuxdeangelo-fcb98eaa10c9d38560ebf42b6088dfa1c.gitlab.io/
        - If we adopt this is should be brought into the OpenSSF
    -
    - Creating an SBOM landscape
        - Categories https://docs.google.com/spreadsheets/d/1VenR5q8AWdqPsMBGNiFam08IjfszUdzAx6JRyZCPc7A/edit#gid=1705310822
        - From this group https://docs.google.com/document/d/1l8qVms7YDJK4L_5gMYhrN9uYdy-SGp49WqecaimqHnw/edit

    -
    - First question - Is this a good idea?
        - Possible political problems
        - Clearly define the criteria
            - We would like to include non open source projects
        - Be as objective as possible
        - Link to more information (like a howto)
            - We can use this as a nudge to get more guidance for tooling created
        -
    - Second question - How do we start filling this out
        - How do we handle trademarks?
        - Domain?
    - How do we make sure the list stays relevant and doesn't get old?
        - We will need a way to audit the projects/data on a regular basis
        - Clearly define this criteria
    - Step 1 - write proposal [Josh]
        - Base this off the original plan to get OpenSSF funding for a landscape
        - https://docs.google.com/document/d/1gLSMHJ-l09r73aBDAIG4Id4pbC85D5UgTaICKqmKXKg/edit#heading=h.joo10r6fp67j
    -
    - Step 2 - Group reviews
    -
- Kate can show off pragmatic sbom field expectations
    - https://docs.google.com/document/d/1wQziuPhDVqI1p7D7IhIsK8psDC-cdRyZnqJCKGWsNVY/edit
- Strike team proposal
    - https://docs.google.com/document/d/15_FKO8D03VSYDTNsMQZtn1aRfgVmModF-NM6VBnlrZA/edit
- Because it came up ... for this, interested in reading my master thesis and giving feedback i a first version on my blog. This is still work in progress. I'm happy for any feedback.

2023-12-19

Attendees (please add yourself)

- Josh Bressers (Anchore)
- Marius Biebel (hm.edu)
- Karen Bennet(IEEE)

- Janane Suresh (Oracle)
- Jarrett Lu (Oracle)
- Yotam Perkal (Rezilion)

Agenda:

- Please paste an intro into the chat
- Update on SBOM Naming document
    - https://github.com/ossf/sbom-everywhere/blob/main/reference/sbom_naming.md
- CISA package naming document response
    - https://openssf.org/blog/2023/12/11/openssf-responds-to-the-cisa-rfc-on-software-identification-ecosystem-analysis/
- Tracking SBOM tools?
    - This came up in the tooling WG last week
    - The CISA SBOM tooling WG is tracking some of the tools
        - https://docs.google.com/document/d/1l8qVms7YDJK4L_5gMYhrN9uYdy-SGp49WqecaimqHnw/edit
    - All CISA groups
        - https://docs.google.com/document/d/1itBra03riwVIgvrn1xp35DuvCFOJ6T8DJgs_3pSxsCM/edit
    - Maybe start by finding working groups and listing them
    - WIP: https://gitlab.com/Mariuxdeangelo/sbom-landscape
    - WIP Page (broken): https://sbom-landscape-mariuxdeangelo-fcb98eaa10c9d38560ebf42b6088dfa1c.gitlab.io/
    -
- Review strike team proposal
    - https://docs.google.com/document/d/15_FKO8D03VSYDTNsMQZtn1aRfgVmModF-NM6VBnlrZA/edit
- FOSDEM SBOM Devroom Agenda
    - https://fosdem.org/2024/schedule/track/software-bill-of-materials/
- FOSDEM Agenda
    - https://fosdem.org/2024/schedule/tracks/
- **Action items**
    - Kate to invite Lynn to this meeting
    - Marius come back to show off tool when more people are around
        - Work with CISA to populate this
    - Josh and Kate to chat the first week of January to nail down an agenda
    - Next Meeting 16 of January