2025 WG Security Tooling Meeting Notes

Our mission is to provide the best security tools for open source developers and make them universally accessible. We talk a lot about SBOMs currently.

This WG is chaired by Ryan Ware

Antitrust Policy Notice

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.

All OpenSSF meeting participants must comply with the OpenSSF Code of Conduct: https://openssf.org/community/code-of-conduct/

Archived 2023 Notes are linked here.
Archived 2024 Notes are linked here.

Upcoming Topics

Please add your agenda item, name and approximate time allocation to the bottom of the list.

Resources

- Slack Channel: #wg_security_tooling
- Zoom Link:
    - LFX Zoom - Every 2 weeks on Friday 11:00 am ET

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

2025-11-28

Attendance ((please **mark an "X" if you are here,** or add-row name/email/affiliation if joining)

	Name/Affiliation	**Pronouns**	**GH ID**
	Ryan Ware	he/him	ware
	Josh Bressers (Anchore)	he/him	joshbressers
	Ian Dunbar-Hall (Lockheed Martin)	he/him	idunbarh
	Georg Kunz (Ericsson)	he/him	gkunz
	Matt Rutkowski (IBM)	he/him	mrutkows
	Mike Lieberman (Kusari)	he/him	mlieberman85
	Kirby Linvill (CU Boulder)	he/him	klinvill
	David Kirichen (Intel)	he/him	Kirich
	Dennis Zhang (New York University)	he/him	yzhang0701
	Adrianne Marcum (OpenSSF)	she/her	amarcum
	Jared Miller (SAP)		jdmcyber
	Evan Anderson (Stacklok)	he/him	evankanderson
	Terri Oda (Intel)	she/her	terriko
	Jonathan Howard (Lockheed Martin)	he/him	jhoward-lm

	Nisha Kumar (Oracle)	she/they	nishakm
	Adolfo Garcia Veytia (Carabiner Systems)	he/him	puerco
	Seth Larson (PSF)	he/him	sethmlarson
	Chan Voong (Comcast)	she/her	voongc
	Jerod Heck (Lockheed Martin)		jhlmco
	Victor Lu (Independent)	he/him	victorjunlu
	Keith Ganger (Lockheed Martin)	he/him	kgangerlm
	Frederick Kautz (TestifySec)	he/him	fkautz
	Mikey Strauss (Scribe Security)	he/him	Houdini91
	Jeff Diecks (OpenSSF)	he/him	GeauxJD
	Tracy Ragan (DeployHub / Ortelius)	she/her	tracyragan
	Yuchen (Dennis) Zhang		NYU
	Jay Lindquist (Target)	he/him	jaylindquist
	Scott Moore (Galois, Inc.)	he/him	thinkmoore
	Dave Welch	he/him	dwelch2344
	Alex Scheel (GitLab, OpenBao)	he/him	cipherboy
	Matt Bauman (JuliaHub)	he/him	mbauman
	Igor Ageyev (Wind River)	he/him	xparkm

Agenda:

- Intros
- Opens
- Future Topics?
    -
-

2025-11-14

Attendance ((please **mark an "X" if you are here,** or add-row name/email/affiliation if joining)

	Name/Affiliation	**Pronouns**	**GH ID**
x	Ryan Ware	he/him	ware
x	Nisha Kumar (Oracle)	she/they	nishakm
x	Jeff Diecks (OpenSSF)	he/him	GeauxJD
x	Alex Scheel (GitLab, OpenBao)	he/him	cipherboy
x	Igor Ageyev (Wind River)	he/him	xparkm

Agenda:

- Intros
- Opens
    - Bomctl has canceled its community meeting
    - CVE-BIN tool donation process continues. One item from licensing scan to be addressed. PR accepted to remove a conflicting file that wasn't needed, moving forward to GB.
    - OpenBao -
        - Stickers to LF booths?
        - Quarterly update?
            - Next update scheduled for Dec. 9
        - Read scalability landing in our next release, per-namespaces encryption backends will be in the following release, aiming for smaller release more frequently now it seems. UI WG seems more like a UI+clients WG, swift client is being built in the community.
        - Saw some initial progress on an IBM/HashiCorp coordinated disclosure but that seems to have stalled again. Of course, happy to have others to nudge.
- Future Topics?
    -

2025-10-31 - Canceled

2025-10-17

Attendance ((please **mark an "X" if you are here,** or add-row name/email/affiliation if joining)

	Name/Affiliation	**Pronouns**	**GH ID**
x	Ryan Ware	he/him	ware
x	Adolfo Garcia Veytia (Carabiner Systems)	he/him	puerco
x	Jeff Diecks (OpenSSF)	he/him	GeauxJD
x	Alex Scheel (GitLab, OpenBao)	he/him	cipherboy
x	Matt Bauman (JuliaHub)	he/him	mbauman

Agenda:

- Intros
- OpenBao:
    - Met Sandbox requirement; working on to-be incubating for security-insights: https://github.com/openbao/openbao/pull/1692 (merged) & scorecard: https://github.com/openbao/openbao/pull/1963 (open)
- Opens
- Future Topics?
    -

2025-10-03

Attendance ((please **mark an "X" if you are here,** or add-row name/email/affiliation if joining)

	Name/Affiliation	Pronouns	GH ID
x	Ryan Ware	he/him	ware
x	Jeff Diecks (OpenSSF)	he/him	GeauxJD
x	Jay Lindquist (Target)	he/him	jaylindquist
x	Scott Moore (Galois, Inc.)	he/him	thinkmoore
x	Dave Welch	he/him	dwelch2344
x (late)	Alex Scheel (GitLab, OpenBao)	he/him	cipherboy

Agenda:

- Intros
  - David Welch, Hero Devs chief software architect
- Opens
  - CVE-BIN tool summary
  - Reliable Software Disassembly updates
    - SIG comprised of people participating in DARPA E-BOSS research program
    - One of the sub-problems of E-BOSS, if you want to do deep analysis of binary artifacts, one of the first steps is you have to extract from the binary what it is
    - Goal is to take tweaks and get adoption from GCC, Clang, etc
    - Experimenting with what is already in the compilers. It seems there's a small set of things to turn on in the compiler to get what we need.
    - Technically, shifting to take the disparate metadata and how would we embed it in ELF format. SIG to make a specification of this to take upstream.
    - Feedback is to make sure no performance impacts. For adoption would need to bring to the communities like LLVM and GCC conference
    -
  - E-BOSS summary
    - Building updated toolchains so that when you compile, you can take the version information and embed it into the artifacts.
    - Determine if you can reach the vulnerable code and if so can you automate a remediation
  - Hero Devs building an EOL dataset. Have an open source tool that does scanning.
  - Two new SIGs from the AI / ML Security Working Group have been formed and will have their first meetings on Monday 10/6:
    - SAFE-MCP
    - Cyber Reasoning Systems

2025-09-19

Attendance ((please **mark an "X" if you are here,** or add-row name/email/affiliation if joining)

	Name/Affiliation	**Pronouns**	**GH ID**
x	Ryan Ware	he/him	ware
x	Jeff Diecks (OpenSSF)	he/him	GeauxJD
x	Alex Scheel (GitLab, OpenBao)	he/him	cipherboy
x	satwikd	he/him	
x	Jay Lindquist (Target)	he/him	jaylindquist

Agenda:

- Intros
- Opens
    - OpenBao live coding: https://www.youtube.com/watch?v=lr7_YmElOro / https://www.youtube.com/@OpenBao
- Agenda:
    - Updates from OpenBao TSC call - Alex Scheel
        - SAP has been voted as a member after their application: https://lists.openssf.org/g/OpenBao-TSC/message/180
        - Roadmap for 2025-2026 has been proposed to TSC e-vote: https://gist.github.com/cipherboy/22420578c6682b54ca6883201e8db1c2
            - Three themes:
                - "**Operator Experience**": to enable easier or safer operation of OpenBao, through changes like profiles, break-glass and backup/restore procedures, and improved monitoring capabilities;
                - "**Scalability**": to improve optimization and utilization of OpenBao in large, complex environments; and
                - "**Sustainability**": to ensure the long-term viability of the code base, react to changing secrets management directives, and stabilize our ability to maintain the project indefinitely.

    - SBOM Whitepaper released https://openssf.org/resources/improving-risk-management-decisions-with-sbom-data/

2025-09-05

Attendance ((please **mark an "X" if you are here,** or add-row name/email/affiliation if joining)

	Name/Affiliation	**Pronouns**	**GH ID**
x	Jeff Diecks (OpenSSF)	he/him	GeauxJD
x	Alex Scheel (GitLab, OpenBao)	he/him	cipherboy
x	Jay Lindquist (Target)	he/him	jaylindquist
x	Jacopo Bufalino		jackap
x	Roman Zhukov		

Agenda:

- Intros
    - Jay from Target, a new OpenSSF member. Principal Engineer in product security. Making sure the engineers produce secure software
    - Jacopo, doctoral candidate at university. Doing research on open source security. Interested to find if some of his work is covered by existing tools. Main interest is on SBOM and standards
- Alex: Should I open a PR to add OpenBao's Q3 update to the WG's?
    - https://gist.github.com/cipherboy/4bb66fe9967fd103a44ea561baaaa4e9
- Alex: OpenBao updates
    - Dev WG Chair and TSC Chair elections finalized by TSC, I've been re-elected to both.
    - Blendbyte has offered S3 hosting for .RPM/.DEBs, Adfinis has taken up work on that. Very appreciative to Blendbyte for the offer.
    - Proton has offered @openbao.org email addresses to the maintainers, which we intend on accepting barring objections from the org?
    - v2.4.0 has been released, including deeper remediations for several security issues.

    - Working on formalizing our vulnerability management processes in writing for external visibility.
    - I think we're aware of the patched CVEs, but we've got work on two outstanding, including the next Hashi-disclosed one (Audit log JSON DoS).
        - https://cyata.ai/blog/cracking-the-vault-how-we-found-zero-day-flaws-in-authentication-identity-and-authorization-in-hashicorp-vault/ and https://discuss.hashicorp.com/t/hcsec-2025-22-multiple-vulnerabilities-impacting-hashicorp-vault-and-vault-enterprise/76096 were earlier vulnerabilities, remediated in v2.3.2
        - https://discuss.hashicorp.com/t/hcsec-2025-24-vault-denial-of-service-though-complex-json-payloads/76393
    - Related to the CVE topic, Vulnerability Disclosure Guides https://github.com/ossf/oss-vulnerability-guide
- Jacopo:
    - Best practices to build “easy to scan” containers
        - Presented research at Kubecon Europe. Recording here
        - Built a list of actions developers can do to make it easier to scan. Interest in OpenSSF contribution - blog post or a guide
    - SBOM malicious compliance: is this a real problem and can we do something to fix it?
        - Two parts: creating SBOM & using SBOM to find CVEs. Tool to scan vulnerabilities on the SBOM
        - Translator tool between different SPDX dialects. OpenSSF interest in this tool?

2025-08-22

Attendance ((please **mark an “X” if you are here,** or add-row name/email/affiliation if joining)

	Name/Affiliation	**Pronouns**	**GH ID**
x	Alex Scheel (GitLab, OpenBao)	he/him	cipherboy
x	Matt Bauman (JuliaHub)	he/him	mbauman

Agenda:

- Intros
- Opens
- Future Topics?
    -

2025-08-08 - Canceled

2025-07-25

Attendance ((please **mark an "X" if you are here,** or add-row name/email/affiliation if joining)

	Name/Affiliation	**Pronouns**	**GH ID**
x	Ryan Ware	he/him	ware
x	Ian Dunbar-Hall (Lockheed Martin)	he/him	idunbarh
x	Alex Scheel (GitLab, OpenBao)	he/him	cipherboy

Agenda:

- Intros
- CVE-bin-tool TAC approval: https://github.com/ossf/tac/pull/503
- OpenBao - Poll on a community call AMER+APAC timeslot if anyone is interested:
    - https://github.com/orgs/openbao/discussions/1588
- OpenBao - Also, do we have a formal WG sponsor individual? I realized on the project lifecycle document it suggests the sponsor should attend project meetings. I think we've got a couple that might work better or worse for different individuals if anyone is interested in attending:
    - Community call is on Thursdays, 10 AM Central (this time slot).
    - Dev WG calls on Thursdays at 8AM Central, bi-weekly.
    - TSC calls monthly, second Thursday of the month at 9AM Central.
    - WG as a whole sponsors OpenBao, Ryan could attend potentially.

2025-07-11

Attendance ((please **mark an "X" if you are here,** or add-row name/email/affiliation if joining)

	Name/Affiliation	Pronouns	GH ID
x	Ryan Ware	he/him	ware
x	Evan Anderson (Custcodian)	he/him	evankanderson
x	Jeff Diecks (OpenSSF)	he/him	GeauxJD
x	Michael Hofer (Adfinis, OpenBao)	he/him	karras
x	Terri Oda	she/her	terriko
x	Mohammed Anghabo (Dhamen Information Technologies)		

Agenda:

- Intros
- OpenBao - Inclusion on TAC update?
    - Was missed by accident
- OpenBao - Project maturity gauge against Incubating requirements?
    - Get started by looking at the PR template to get the discussions and review started, which should help OpenBao also evaluate their current state
    - Recent previous applications can provide further insights and examples
- Opens
    - `cve-bin-tool` as a new project
        - Both linux components and library components
        - Over 400 detectors
        - Current frontier: VEX
        - Looking to donate from Intel to OpenSSF as primary maintainer (terriko) is leaving Intel

2025-06-27 - Canceled

2025-06-13

Attendance ((please **mark an "X" if you are here,** or add-row name/email/affiliation if joining)

	Name/Affiliation	Pronouns	GH ID
x	Ryan Ware	he/him	ware

x	Ian Dunbar-Hall (Lockheed Martin)	he/him	idunbarh
x	Evan Anderson (Custcodian)	he/him	evankanderson
x	Nisha Kumar (Oracle)	she/they	nishakm
x	Jeff Diecks (OpenSSF)	he/him	GeauxJD
x	Alex Scheel (GitLab, OpenBao)	he/him	cipherboy
x	Michael Hofer (Adfinis, OpenBao)	he/him	karras

Agenda:

- Intros
- Opens
- Fuzz Introspector project update
    - https://github.com/ossf/fuzz-introspector
- Open Source Summit North America - Project Demos at OpenSSF booth
  OpenSSF OSS NA 2025 Booth Schedule
- Minder updates
    - Can now carry more context over from evaluation to remediation. E.g. warn on missing dependabot ecosystems, but pass all detected ecosystems to remediation.
    - Documentation updates on writing rules
        - Rego engine details
        - JQ engine details
- OpenBao updates
    - Approved new contributor and TSC member
    - Working on finalizing the GA release for 2.3.0, which includes exciting features such as Namespaces (tenancy)
    - Upcoming initiatives and activities include UI 2.0, Horizontal Scalability (no doc yet), External Keys (RFC, PKCS#11 implementation), Static Auto Unseal, Per-Namespace Seals, inline authentication, and others
    - Will be at OSS Summit EU; Christoph is in touch with Stacey to help with OpenSSF booth
- SBOM tool updates
    - Getting ready for community day. Presentation on bomctl

2025-05-30

Attendance ((please **mark an "X" if you are here,** or add-row name/email/affiliation if joining)

	Name/Affiliation	Pronouns	GH ID
x	Ryan Ware	he/him	ware
x	Dennis Zhang (New York University)	he/him	yzhang0701
x	Evan Anderson (Custcodian)	he/him	evankanderson
x	Jeff Diecks (OpenSSF)	he/him	GeauxJD
x	Enock Kasaadha (University of Missouri)	he/him	kaxada

Agenda:

- Intros
  - Enock Kasaadha, researching OSS security at Missouri, interest in dependencies
- Opens
  - Status on sbomit
    - Currently in sandbox, as of April 2024
    - Adding in-toto attestations to SBOMs
    - Licensed as CC-BY in 2023
    - March 2025: first workshop in Washington, DC\
    - Timeline
    - Looking to be able to extract an SBOM from multiple in-toto attestations
    - Glad to see timeline, would like to see timeline tracking / updates when timelines change
    - Thinking about going to incubation
      - Looking at adoption criteria as a blocker
  - WG housekeeping - updates needed in readme (meeting notes link, meeting times)
    - A few items needed – CONTRIBUTING.md in SBOMit-strace-prototype, meeting notes / time update, maintainers
  - Minder update
    - Created https://github.com/custcodian/minder-rules-and-profiles/tree/main/top-5 to remediate (fix) 5 high-priority supply chain items:
      - Dependabot
      - SCA (Semgrep)
      - Actions pinning
      - Branch protection
      - Actions permissions
    - Also improved UX by allowing names as well as IDs in most commands / API calls

2025-05-16

Attendance ((please **mark an "X" if you are here,** or add-row name/email/affiliation if joining)

	Name/Affiliation	**Pronouns**	**GH ID**
x	Ian Dunbar-Hall (Lockheed Martin)	he/him	idunbarh
x	Evan Anderson (Custcodian)	he/him	evankanderson
x	Adolfo Garcia Veytia (uServers)	he/him	puerco
x	Jeff Diecks (OpenSSF)	he/him	GeauxJD
x	Alex Scheel (GitLab, OpenBao)	he/him	cipherboy
x	Michael Hofer (Adfinis)	he/him	karras

Agenda:

- Intros
- Opens
    - Jeff: Recorded podcast with maintainers of projects, edited to video, and then an update to the README's content
    - Alex: Podcast at OSS Summit EU as well?
        - Jeff: Potentially, will see.
    - OpenBao: Status of migration?
        - Logistic delay, how to move project inside of LFX between two umbrellas
- Future Topics?
    - Jeff+Ian: SBOMit updates deferred to the next call.

2025-05-02

Attendance ((please **mark an "X" if you are here,** or add-row name/email/affiliation if joining)

	Name/Affiliation	**Pronouns**	**GH ID**

x	Ryan Ware	he/him	ware
x	Josh Bressers (Anchore)	he/him	joshbressers
x	Ian Dunbar-Hall (Lockheed Martin)	he/him	idunbarh
x	Evan Anderson (Custcodian)	he/him	evankanderson
x	Jeff Diecks (OpenSSF)	he/him	GeauxJD
x	Scott Moore (Galois, Inc)	he/him	thinkmoore
x	Eduardo Gonzalez (Independent)	he/him	egongu90

Agenda:

- Intros
- Opens
    - Reliable Software Decomposition SIG
        - 5 votes, 4 thumbs up & a supportive comment
        - Discussion in Slack about tools and terms but no dissent
        - (passed)
        - Scott to check PR for name change and follow up on DCO
        - Time and dates for the meetings - every other week on Mondays?
            - Jeff Diecks can help add the calendar entry and video bridge
            - Can run a doodle poll to have interested SIG members vote for a time
    - Minder updates
        - Announcements have gone out for project changes
        - Couple of Stacklok members continue to contribute with personal time.
        - Evan is at a new company focused on Minder. Looking for Minder to do less build infra and use the tools we already have. Build on top of the platform.
        - Built some tools to migrate from Stacklok instance which will be shut down shortly: https://custcodian.dev/hosted/migration/
        - Reach out to Evan if you are interested in Minder and need help getting started (including new rules and usage of existing rules)
        - Jeff will schedule time to discuss Minder/Baseline/Scorecard sharing the evaluation engine so that rule set format can be shared
    - SBOMit update in 2 weeks
        - Use list of maintainers from TAC issue
        - Will also try to schedule the other SBOM tools for updates in the following weeks

2025-04-18

Attendance ((please **mark an "X" if you are here,** or add-row name/email/affiliation if joining)

	Name/Affiliation	**Pronouns**	**GH ID**
x	Ian Dunbar-Hall (Lockheed Martin)	he/him	idunbarh
x	Evan Anderson (Stacklok)	he/him	evankanderson
x	Jeff Diecks (OpenSSF)	he/him	GeauxJD
x	Alex Scheel (GitLab + OpenBao)	he/him	cipherboy
x	Allen Shearin	he/him	
x	Hannah Sutor (GitLab)	she/her	hsutor
x	Daniel Moch (Lockheed Martin)	he/him	djmoch
x	Scott Moore (Galois, Inc.)	he/him	thinkmoore
x	Ding Sun		

Agenda:

- Intros
  -
- Open Items
  - Reliable Disassembly SIG proposal
    - Only one comment on the proposal – rename to Reliable Software Decomposition
      - Happy to take on
      - Try to do an asynchronous vote – Evan will figure out who is eligible and tag people on Slack / record votes on the GitHub issue
    - Meetings on biweekly on Mondays at 11 Eastern / 16 UK, starting on Apr 28
      - Opposite the Python SIG
  - OpenBao approved by TAC, but MPL license was flagged and is awaiting GB review / approval for IP & Licensing
    - Alex: currently in a holding pattern on license approval
    - Got a free booth at Open Source Summit EU
  - Open Source Summit Booths - NA & EU
    - Opening up slots for demos at the booths for OpenSSF projects
    - Reach out to Stacey Potter if you are interested

    - SBOM-O-Rama with CISA – Ian and Stacey are organizing, or maybe a separate mini summit if CISA falls through.
    - **Reminder:** Stacklok's public good Minder instance is shutting down on 1 May, but there are migration options to another public instance.
    - Minder: Evan connecting with Stephen Augustus from scorecards, and will be looking at importing the Minder evaluation engine into Scorecards
        - Baseline: https://github.com/ossf/wg-orbit
        - Scorecards: Best practices WG (https://github.com/ossf/scorecard/)

2025-04-04

Attendance ((please **mark an "X" if you are here,** or add-row name/email/affiliation if joining)

	Name/Affiliation	**Pronouns**	**GH ID**
x	Ryan Ware	he/him	ware
x	Jeff Diecks (OpenSSF)	he/him	GeauxJD
x	Ian Dunbar-Hall	he/him	idunbarh
x	Alex Scheel (GitLab + OpenBao)	he/him	cipherboy
x	Florian Micklich	he/him	
x	Allen Shearin	he/him	
x	Tabatha DiDomenico (G-Research)	she/her	tabdido

Agenda:

- Intros
- Opens
    - Mike, Puerco, and Ian Presenting at VulnCon Monday
    -
- Topics
    - Circle back on Reliable Disassembly SIG proposal
        - Consider naming to help describe what this is to outsiders. "Reliable Software Decomposition"?
        - Suggest to create a PR for the proposal, gather feedback on the PR and bring back for a vote. PR has been created (link above). Will announce on the slack channel.

- OpenBao presented to TAC https://github.com/ossf/tac/pull/461 , PR is available for comments etc.
- Check in with CISA about SBOM-a-rama, consider a breakout session. Planning is in progress.

2025-03-21

Attendance ((please **mark an "X" if you are here,** or add-row name/email/affiliation if joining)

	Name/Affiliation	**Pronouns**	**GH ID**
x	Adolfo Garcia Veytia (ChainGuard)	he/him	puerco
x	Jeff Diecks (OpenSSF)	he/him	GeauxJD
x	Scott Moore (Galois)	he/him	thinkmoore
x	Hannah Sutor (GitLab)	she/her	hsutor
x	Ian Dunbar-Hall	he/him	idunbarh
x	Alex Scheel (GitLab + OpenBao)	he/him	cipherboy
x	Florian Micklich	he/him	
x	Anjica Malla	she/her	amalla2016
x	Evan Anderson	he/him	
x	Nisha Kumar	she/they	nishakm

Agenda:

- Intros
- Opens
  - [Alex] OpenBao - Waiting on voting agreement from OpenBao TSC to decide to proceed with donation on March 27th. Once that happen sandbox application will be submitted.
  - [Evan] Change meeting time?
    - Jeff to talk with Ryan about creating a new poll, existing poll can be found here.
    - Evan prefers an hour later

        - Ian + Evan prefers a different day
- Topics
    - [Scott] Reliable Disassembly SIG proposal
        - (part of the E-BOSS effort)
        - Attempting to use ELF debugging data to determine software composition analysis and am-I-affected
    - [Evan] Minder update
        - Stacklok has reduced full-time staff working on Minder, but Evan is working to up his outside-work time on Minder
        - Improvements since last time:
            - Authorization with GitHub Actions tokens
            - Simplify switching servers with the `minder` CLI
            - Building endpoints for a generic entities model.
        - More to announce next meeting
    - [Florian] Toolbelt / Catalog of OpenSSF tools
        - Jeff highlighted the website projects revamp
            - https://openssf.org/projects/
            - OpenSSF Projects Overview
        - Is Florian looking for “what OpenSSF recommends” or “what OpenSSF hosts”?
            - OpenSSF Recommendations for tooling (golden path) documentation.
            -
    - Bomctl questions
        - Using CDX 1.6
        - `FATAL import: importing document: failed to store document: storing document urn:uuid:141d3e1b-3a7c-4c49-9485-3a3ed7e5fff2: saving nodes: insert nodes to table "nodes": SQL logic error: too many SQL variables (1)`
- Actions
    - [Jeff] Talk with Ryan on time change.
    - [Jeff] Talk with Ryan and voting process for Scott’s Reliable Disassembly SIG proposal
    - [Ian] Document Nisha’s usecase of iteratively adding and modifying links between nodes.

2025-03-07

Attendance ((please **mark an "X" if you are here,** or add-row name/email/affiliation if joining)

	Name/Affiliation	**Pronouns**	**GH ID**
x	Ryan Ware	he/him	ware
x	Jeff Diecks (OpenSSF)	he/him	GeauxJD
x	Hannah Sutor (GitLab)	she/her	hsutor
x	Ian Dunbar-Hall	he/him	idunbarh
x	Alex Scheel (GitLab + OpenBao)	he/him	cipherboy
x	Florian Micklich	he/him	
x	Georg Kunz	he/him	gkunz

Agenda:

- Intros
- Opens:
    - (Ian) OpenSSF SBOMit Workshop Summary
        - Created a rough roadmap
            - You have a SBOM - how do you know all components are represented? In-toto attestation that traces it all the way back to source code. How do we resolve the differences between SBOMs based on the tool they are generated with?
        - Follow on discussion at open source summit in Denver in June
- Topics:
    - Minder - Evan Anderson - 20m
    - OpenBao - Alex Scheel - 20m
        - Currently in LF Edge - LF group in IoT/edge computing
        - Not meeting a couple requirements, which will put us in the 60 day window of needing to move
            - Premier membership company
            - 2 TAC sponsors
        - Interested in becoming an OpenSSF project
        - Project must be aligned with OpenSSF mission, novel approach to an area or address an unmet need. What do you think about the latter portion?
            - Primarily trying to avoid duplication
            - Vault/OpenBao integral solution for key management
            - Compliments OpenSSF projects without creating duplication
            - Where could OpenBao enhance existing efforts in OpenSSF?
        - Need a sponsor for the TAC

        - Georg is supportive, we should bring it to the TAC in general
        - Sponsor could also be from the WG
    - How is it decided which WG it does into?
        - WG can decide, plus guidance from TAC members, project itself can figure out where they want their home to be
        - Getting on schedule for next TAC meeting would be a good idea
    - OpenBao is not yet fully voted to move it, or to any particular place
    - What are the opportunities for interop?
        - Had built in usage for OpenBao due to Vault license issues. What do existing integrations and collaboration look like here?
            - Project <> Project integration

2025-02-21

Attendance ((please **mark an "X" if you are here,** or add-row name/email/affiliation if joining)

	Name/Affiliation	**Pronouns**	**GH ID**
x	Ryan Ware	he/him	ware
x	Josh Bressers (Anchore)	he/him	joshbressers
x	Mike Lieberman (Kusari)	he/him	mlieberman85
x	Adolfo Garcia Veytia (ChainGuard)	he/him	puerco
x	Jeff Diecks (OpenSSF)	he/him	GeauxJD
x	Daniel Moch (Lockheed Martin)	he/him	djmoch
x	Scott Moore (Galois)	he/him	thinkmoore
x	Allen Shearin (Lockheed Martin)	he/him	ashearin
x	Hannah Sutor (GitLab)	she/her	hsutor

Agenda:

- Intros
- Opens
    - PR for TAC graduation status

- https://github.com/ossf/tac/pull/446E-BOSS program - interested presenters on SBOM tools?
- CISA whitepaper on SBOM tools is in progress
- New SBOM Tools page of website https://openssf.org/technical-initiatives/sbom-tools/
- Overview of different BOM tooling
  - Protobom
    - Library and suite of tooling that makes it easy to manipulate and transform SBOM programmatically
  - bomctl
    - Format agnostic - you don't have to care about the format of the SBOM. Ingest and export any/every format
    - Allows you to build a tree of BOMs in any format and link together
    - Link to boms of subcomponents
    - Working on fetch/push for dependency track. We want to be platform agnostic
  - SBOMit
    - Still in R&D phase
    - A way of attesting to what's in the SBOM so that you can say, I built this SBOM in this way, and these things are cryptographically verified
  - OpenSSF projects overview deck
  - SBOM Catalog

2025-02-07

Attendance ((please **mark an "X" if you are here,** or add-row name/email/affiliation if joining)

	Name/Affiliation	**Pronouns**	**GH ID**
x	Ryan Ware	he/him	ware
x	Mike Lieberman (Kusari)	he/him	mlieberman85
x	Evan Anderson (Stacklok)	he/him	evankanderson

x	Stacey Potter (Stacklok)	she/her	staceypotter
x	Katherine Druckman (Intel)	she/her	kdruckman
x	Allen Shearin (Lockheed Martin)	he/him	ashearin
x	Hannah Sutor (GitLab)	she/her	hsutor
x	Tracy Ragan (DeployHub / Ortelius)	she/her	tracyragan
x	Scott Moore (Galois)	he/him	thinkmoore
x	Ali Shokri (Virginia Tech)	he/him	a-shokri
x	Binoy Ravindran (Virginia Tech)		
x	Ryan O'Neill (Red Balloon Security)	he/him	elfmaster
x	Wyatt Ford (Red Balloon Security)	he/him	whyitfor

Agenda:

- Intros
    - DARPA E-BOSS program collaborators:
        - Scott Moore: Galois Inc., program analysis and security background, working on DARPA E-BOSS program
        - Ryan O'Neill: Red Balloon security. Working in security since mid 90s.
        - Binoy: Academic research. Also involved in DARPA, tools for extended SBOM formats
        - Ali Shokri: Post-doc at VT.
        - Wyatt Ford: Red Balloon.
- Opens
    - Ryan: PR to update Working Group status. Previously, no formal documentation other than what was done when OpenSSF was started. We want to be a graduated working group.
        - Graduated working group means we need a co-chair. Ryan will continue the work, but sometimes he is unable to attend.
        - Mike L offered to handle it on a temporary basis
- Topics
    - What can the WG do to help DevRel?
        - Katherine: Packaging up tools, creating a reference architecture. We may need to change the way we evangelize the tools coming out of this organization. I am here to get a lay of the land.
        - Katherine: Distilled updates, with an eye towards how things fit together.

        - Ryan: OpenSSF is great at announcing new tools, but not so great at talking about them after that. How do we showcase the good work being done.
        - Tracy: Adoption. Who are we serving with these tools? OpenSSF side is all about security and standards. Many of them are command line driven. Have to start reaching out to people on the DevOps side.
            - Bring OpenSSF tools to audience that needs to adopt them
            - Started a CI/CD SIG
                - Goal to define where tools should be used, put them in an easy place to find
            - Outreach to correct persona
        - Ryan: How do I implement these tools in an automated way. Needs to be SAST, composition analysis - what do I plug in?
        - Tracy: https://cicd-cybersecurity.netlify.app/
        - Hannah: We should look at it from a use case perspective. What are you trying to accomplish, outcomes to achieve, then here are the tools.
            - Katherine: We have started on this here
            - Tracy: We've created 3: code, build/deploy, post-deployment
    - Scott Moore: Previously chatted about the DARPA E-BOSS program. Thinking about SMBOMs and other enhancements to build toolchains. Help vuln assessment and triage process. How can we improve the formats in which binaries are produced, so when you want to assess if a vuln is exploitable in your program, can we make this easier. We want to align with the industry.
        - May be interested in setting up a SIG in OSSF
        - https://docs.google.com/document/d/1_j7WoHXKJtLOA1VHIk2ASFchOpop5Fk2RPEhvk5d3bs/edit?usp=sharing
        - Ryan: https://github.com/ossf/tac/blob/main/process/sig-lifecycle.md
        - MichaelL:
            - Would need:
                - more detail on what you expect to put into ELF
                - more planning around how we plan to get upstreaming to happen
    -
- Future Topics?
    - Evan to provide an update on Minder in 1 month
        - Short artifact/standard format
            - 3 wins / 3 losses
            - Status of bug backlog (how old are bugs, how many good first issues)
            - Any new contributors?
            - Any needs for the WG?
    - Ryan will do a state of the group, goals for the year

2025-01-24

Attendance ((please **mark an "X" if you are here,** or add-row name/email/affiliation if joining)

	Name/Affiliation	**Pronouns**	**GH ID**
x	Ryan Ware	he/him	ware
x	Ian Dunbar-Hall (Lockheed Martin)	he/him	idunbarh
x	Mike Lieberman (Kusari)	he/him	mlieberman85
x	Nisha Kumar (Oracle)	she/they	nishakm
x	Hannah Sutor (GitLab)	she/her	hsutor
x	Jeff Diecks	he/him	GeauxJD

Agenda:

- Intros
- Opens
    - [Jeff] TAC status / paperwork for the group
        - The group decided to submit for Graduated status. Jeff will start a PR,
        - Ryan to reach out for co-lead candidate
    - [Jeff] OpenSSF Website Nav - project categorizations
      OpenSSF 2025 Nav Updates v1
        - Contact Jeff for any input / feedback
    - [Jeff] Plug for CRA tech bi-weekly meetings, future speaking opps for this group
        - New WG is here on Slack: https://openssf.slack.com/archives/C084A6XPX0F
    - [Nisha + Hannah] - Conversation on Identity
        - How do we evaluate trustworthiness? Any conversations in OpenSSF about this?
        - Mike: Siren mailing list - track suspicious behavior. No way to tell if a particular pseudoanonymous person is trustworthy. We can provide indicators, but OpenSSF has said that they are not going to get into that space since it's hard to tell, and not easy to say who is and isn't trustworthy.

        - Ian: Linux kernel maintainer has some more strict requirements, in person ID. Other sensitive OSS projects have similar requirements.
            - Doesn't scale, not inclusive
            - Mike: Critical projects, on a case by case basis. Linux kernel has a specific set of requirements.
            - Ryan: When Linux kernel folks meet IRL, they verify identity and GPG keys
        - Hannah: Who makes these requirements?
            - Ian: Groups themselves. Maintainer decision to exclude certain people based on reason
        - Michael: Seeing some of this with CRA. Going to be up to the company to enforce rules that the contributions coming in are good - scanning, pull requests + reviews
            - Companies that are allowing external contributors, looking at them with a bit of a magnifying glass to make sure of security
            - Hannah: IF we can gauge the security of their contribution, does it matter who they are?
            - Mike: Generally, yes. Looking at content of their contribution, but need to do due diligence to make sure these people aren't on a list etc
                - Ex: Doing a lot of good, get promoted to maintainership, now maybe they do something nefarious
            - Ian: OpenSSF could provide guidance where we provide inclusive environment for contributions, but guidance on when the additional security checks should occur
                - Scorecard does this to some degree, at risk
                - Mike: baseline. Are there a set of things we can do that we can look at the content of the contribution, know when it may be risky
                - GitHub has said not to look at contribution graph as canonical because dates can be backdated
            - https://baseline.openssf.org/
            - https://github.com/ossf/security-baseline
    - 2025 Areas of Focus
        - Tracking on https://github.com/ossf/wg-security-tooling/issues/68
- Future Topics?
    -

2025-01-10

Attendance ((please **mark an "X" if you are here,** or add-row name/email/affiliation if joining)

	Name/Affiliation	**Pronouns**	**GH ID**

x	Ian Dunbar-Hall (Lockheed Martin)	he/him	idunbarh
x	Evan Anderson (Stacklok)	he/him	evankanderson
x	Nisha Kumar (Oracle)	she/they	nishakm
x	Jeff Diecks (OpenSSF)	he/him	GeauxJD
x	Hannah Sutor (GitLab)	she/her	hsutor
x	Daniel Moch (Lockheed Martin)	he/him	djmoch
x	Dan Becker (Kudu)		

Agenda:

- Intros
  - Daniel Moch
  - Hannah Sutor
  - Dan Becker
- Opens
  - Jeff: Each OpenSSF project will have a TPM assigned. We can help identify overlap, collaboration across groups. Also help with funding requests that we want to apply to the TAC.
  - Ian: SBOMit project looking to have co-located event with public policy summit in DC. Any updates?
    - Jeff: We have a venue secured. You can reach out to Chris, he would be your point of contact.
  - OpenSSF Website Nav Updates (review & input of where to sort some of the projects) OpenSSF 2025 Nav Updates v1
  - TAC Processes: need status & submit PRs for This WG and Fuzzing Introspector project https://github.com/ossf/tac/blob/main/process/working-group-lifecycle.md
  - CRA Bi-weekly tech talks
- Future Topics?
  - 2025 OKRs?
    - Transitioning the tooling into active use. Driving adoption
    - Work with Crob to get SBOM architecture in place
      - What does SBOM architecture mean?
        - Can we show a lifecycle for SBOMs. Have them mapping to the tooling and representative implementation of the lifecycle.
          - Generation, movement, analysis. How does it all fit together?
          - Proposed SBOM lifecycle diagram from CISA BOMOps subgroup: https://docs.google.com/document/d/1vFVbWEJmN

sAbNPRAtHclC89YQlLUt6xYIvKmFGRkcQA/edit?tab=t.0#heading=h.xfu93z734nsf

- Nisha: Still seeing that people are stuck on BOM format. Part of the BOMOps work we are doing is to try to get beyond that, and help people move beyond that. After we tackle that problem, or once we have a SBOM, what can we do with it?
    - Currently, SBOM is a compliance thing, not useful beyond that.
    - Not trying to create a quality SBOM, just creating one to check the box.
    - Quality SBOM is subjective
    - How do we make SBOMs valuable in implementing in open source projects
- Evan: SBOMs are great as way to understand artifacts, but there are a bunch of security steps that need to go along the whole chain. It doesn't feel like we have tooling that makes sure every step along the chain is guarded.
    - Concern about reliance on build time attestations
        - SolarWinds: Build machines were compromised. So you couldn't trust anything coming out of those build machines.
    - SBOM everywhere WG - compilers producing SBOMs.
        - Evan: The timeline still seems far out
        - Nisha: OpenSSF is in a good position. Fairly easy for GoLang to instrument module struct so compiler can show us the metadata
        - Evan would really like to be able to have reproducible builds that could also reproduce the SBOM
        - Golang is in a good place (according to Evan), but e.g. CPython modules
        - E-BOSS is a DARPA program attempting to build SBOMs from C/C++ compilers
- Supporting OSSF Baseline measurement
    - Goal for Minder is to provide automated measurement of Level 1 end-of-January
    - Includes support for EU CRA requirements

- This group doesn't have group status on file with the TAC
    - Ryan / Jeff / ?? may help with this
    - Fuzzing introspector is missing process information
- EU CRA workshops every other week
    -
- SPDX 3.0 - currently depend on go modules that support SPDX 2.3
    - Creating a new repository for SPDX 3.0 module bindings for golang

            - Will primarily be data structures, etc, generated from the shackle-to-code tool
            - GUAC is also looking for this
    - Minder updates:
        - Started a monthly community meeting – second Thursday of the month @ 16:00GMT
        - Hackathon at end of the years to write rules. Generated 24 new rules.
        - Trying out functionality that will need to be documented
        - Added data sources - callout to http endpoint and fetch structured data
        - New dependency ingester based on OSV
        - Added alert type that can be used to send PR comments. New setup driven by config you can load in per-project
        - Tested integrating with tools for static analysis

TEMPLATE - 2025-MM-DD

Attendance ((please **mark an "X" if you are here,** or add-row name/email/affiliation if joining)

	Name/Affiliation	**Pronouns**	**GH ID**
	Ryan Ware	he/him	ware
	Josh Bressers (Anchore)	he/him	joshbressers
	Ian Dunbar-Hall (Lockheed Martin)	he/him	idunbarh
	Georg Kunz (Ericsson)	he/him	gkunz
	Matt Rutkowski (IBM)	he/him	mrutkows
	Mike Lieberman (Kusari)	he/him	mlieberman85
	Kirby Linvill (CU Boulder)	he/him	klinvill
	David Kirichen (Intel)	he/him	Kirich
	Dennis Zhang (New York University)	he/him	yzhang0701
	Adrianne Marcum (OpenSSF)	she/her	amarcum
	Jared Miller (SAP)		jdmcyber

	Evan Anderson (Stacklok)	he/him	evankanderson
	Terri Oda (Intel)	she/her	terriko
	Jonathan Howard (Lockheed Martin)	he/him	jhoward-lm
	Nisha Kumar (Oracle)	she/they	nishakm
	Adolfo Garcia Veytia (ChainGuard)	he/him	puerco
	Seth Larson (PSF)	he/him	sethmlarson
	Chan Voong (Comcast)	she/her	voongc
	Jerod Heck (Lockheed Martin)		jhlmco
	Victor Lu (Independent)	he/him	victorjunlu
	Keith Ganger (Lockheed Martin)	he/him	kgangerlm
	Frederick Kautz (TestifySec)	he/him	fkautz
	Mikey Strauss (Scribe Security)	he/him	Houdini91
	Jeff Diecks (OpenSSF)	he/him	GeauxJD
	Tracy Ragan (DeployHub / Ortelius)	she/her	tracyragan
	Yuchen (Dennis) Zhang		NYU

Agenda:

- Intros
- Opens
- Future Topics?
    -