Uploaded on Github

OpenSSF OpenVEX SIG Meeting Notes

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/

Upcoming Topics

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

Resources

Meeting Schedule: Mondays - 12:00:01p PT/3:00p ET/2000 UTC - occurs every 2 weeks
LFX Zoom
Github Repository
Discussions
Mailing List
Youtube Channel: OpenSSF

Meetings

Meetings alternate between Technical Calls (dealing with the spec & tools) and Evangelism (dealing with industry engagement & VEDX usage)

Please use the 2024 Meeting Notes

2023-12-11 - Evangelism/Ecosystem

Attendees

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

Present ?	Name	Email	Affiliation	Pronouns	GH ID
x	CRob	CRob@intel.com	Intel/OSSF	he/him	SecurityCRob
x	Madison Oliver	taladrane@github.com	GitHub	she/her	taladrane
x	Adolfo García Veytia*	puerco@chainguard.dev	Chainguard	he/him/él	puerco

Meeting Agenda

- Who wants to help out and scribe for us today?
- New Friends intros
- Updates from CISA VEX WG
    - The group reviewed Oracle's survey results
    - We'll wlk through owr
- Review Issues/PRs
- Opens

Opens

-

Meeting Notes

-

Sub-Projects

(leads, please enter updates to inform full group; highlight anything for larger group discussion)

2023-11-27 - Tech Call

Attendees

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

Present ?	Name	Email	Affiliation	Pronouns	GH ID
x	CRob	CRob@intel.com	Intel/OSSF	he/him	SecurityCRob
x	Jay White*	jaywhite@microsoft.com	Microsoft	he/him	camaleon2016
x	Adolfo García Veytia*	puerco@chainguard.dev	Chainguard	he/him/él	puerco
x	Brandon Mitchell	git@bmitch.net	Independent	he/him	sudo-bmitch
x	John Andersen	john.s.andersen@intel.com	Intel	he/him	pdxjohnny
x	Alex Goodman	alex.goodman@anchore.com	Anchore	he/him	wagoodman

Meeting Agenda

- Who wants to help out and scribe for us today?
  - CRob!
- New Friends intros
  - Alex Goodman rejoinsus!
  -
- Updates from CISA VEX WG
  - VEX Survey
- Review Issues/PRs
- Opens
- [CRob} CISA VEX Survey - https://docs.google.com/forms/d/e/1FAIpQLSejXd3or5DtfhPCwJYVhzofJyYFpxCkqo_GyAFaD_k1eIb3ww/viewform

    - The CISA WG is organizing a survey to understand how people are using VEX and where they are in their VEX journey. It is aimed at about a dozen organizations.
    - Who & when do we want to do this?
- VulnCon CFP now open
    - CRob & Adolfo have a few abstracts we are working on to represent VEX & the SIG
    -
- VEX AutoDiscovery Module
    - Making VEX should be transparent for people.
    - Adolfo has demo to sho. Uses cosign to attest to a vex statement and shows how grype leverages that
    - Grype use purls to talk to openvex backend
    - Seth from python is talking about enabling vex for that ecosystem
    - Brandon speaks to not only what, but whom to trust with the attestations. No sigs are being verified yet (with statement being “hosted” by the same entity as the software creator), but will be a future work-item. Brandon also mentions if software is downloaded as a binary, source/tracking info could be lost. Adolfo currently feels we’d need SBOM along with binary for verification. Thirdly will be vex sigs coming from 3rd parties. How do yuo keep track of which 3rd parties you want to trust
    - Alex has a few questions - 1.) grype output - is there an audit trail yet to show where docs were gotten from and what grype took into account when it ran(Puerco says this will be part of his forthcoming PR to grype team). 2.) backends - is this exposed at an API level to select which backends you wish to use or not? Adolfo says Yes! That will be selectable, and you can provide your own driver.
    - Module is ready, need to scaffold the repo and get the tests ready. Ideally will be available & submitted this week
    - Hoping to work on feature that would enable finding vex statements in git repos maybe by the end of the year
    - We have the opportunity to help set the standard in a manner that is most palatable to upstream oss (i.e. storing with your sourcecode). We should talk with SPDX & Cyclone to see if we all can come to agreement on a “well known file” (for example) and help set that for open source implementations issuing vex’es
    -

Opens

-

Meeting Notes

-

Sub-Projects

(leads, please enter updates to inform full group; highlight anything for larger group discussion)

2023-11-13 - Evangelism/Ecosystem

Attendees

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

Present ?	Name	Email	Affiliation	Pronouns	GH ID
X	John Andersen	john.s.andersen@intel.com	Intel	he/him	pdxjohnny

Meeting Agenda

- Who wants to help out and scribe for us today?
- New Friends intros
- Updates from CISA VEX WG
- Review Issues/PRs
- Opens

Opens

-

Meeting Notes

-

Sub-Projects

(leads, please enter updates to inform full group; highlight anything for larger group discussion)

2023-10-30 - Tech Call

Attendees

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

Present ?	Name	Email	Affiliation	Pronouns	GH ID
x	CRob	CRob@intel.com	Intel/OSSF	he/him	SecurityCRob
x	Madison Oliver	taladrane@github.com	GitHub	she/her	taladrane
x	Jay White*	jaywhite@microsoft.com	Microsoft	he/him	camaleon2016
x	Art Manion	zmanion@protonmail.com			zmanion
x	Brandon Mitchell	git@bmitch.net	IBM	he/him	sudo-bmitch

Meeting Agenda

- Who wants to help out and scribe for us today?
- New Friends intros
- Updates from CISA VEX WG
- Review Issues/PRs
- Opens

Opens

-

Meeting Notes

-

Sub-Projects

(leads, please enter updates to inform full group; highlight anything for larger group discussion)

2023-10-16 - Evangelism/Ecosystem

Attendees

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

Present?	Name	Email	Affiliation	Pronouns	GH ID
x	Jay White*	jaywhite@microsoft.com	Microsoft	he/him	camaleon2016
x	Art Manion	zmanion@protonmail.com			zmanion
X	Brandon Mitchell	git@bmitch.net	IBM	he/him	sudo-bmitch
X	John Andersen	john.s.andersen@intel.com	Intel	he/him	pdxjohnny
X	Tony Homer	tony.homer@intel.com	Intel	he/him	tony--
X	Ryan Ware	ryan.ware@intel.com	Intel	he/him	ware
X	Dana Wang	dwang@linuxfoundation.org	OpenSSF	She/Her	danajoyluck

Meeting Agenda

- Who wants to help out and scribe for us today?
- New Friends intros
    - Ryan Ware - Directory of OSS Security, alt on OSSF gov board, runs security tooling working group
    - Tony Homer - Security Researcher at Intel, focus area is third party components
- Updates from CISA VEX WG
    - Next action item is survey, interview people in supply chain to understand their current and future plans with VEX
    - Alpha version of survey linked below
    - Understand which communities OpenVEX is engaged with
    - Intel has been volunteered to talk about our plans (Ryan Love)
        - Believe Intel is going with CSAF route
    - Going to talk with Software companies, downstream consumers, government
    - State of art and current challenges around use of VEX
    - If you have feedback please let CRob know

        - Curated repos could benefit from VEX (S2C2F ING-4: Mirror a copy of all OSS source code to an internal location)
        - Art Manion suggests collecting data to create an end-to-end picture of how VEX is used
        - SBOM WG has a paper out for comment: When to issue a VEX document
            - It's coming from the CISA community and related to SBOM and VEX
            - The legal disclaimer saying it's from the community is taking a while
- Review Issues/PRs
    - Spec Issue 9 - Notifications of new VEX
        - In two weeks we'll talk about what OpenVEX's plans are with regards to notification
        - Survey might tell us how people are doing for advertisement
        - Some folks plan on inserting statements into containers
        - People would like to have a webpage and post a line on a webpage
        - Brandon agrees with Puerco
- Puerco did talks at OpenSSF days
    - Scanner integrations, worked with scanner vendors to ingest VEX data
        - Grype
        - Close to announcing integration with "dog based" scanner company
        - TODO link
    - Live demo of how to generate SBOM and VEX and align them
        - OSS-EU OSSFDay talk - https://www.youtube.com/watch?v=rYfFd8GDN1Q
        - This talk is not yet live
        - Well done demo that helps tie things together
- SBOM Everywhere's SBOM Strike Team proposal
- CISA VEX Practices Survey
    - Will be form-i-fied shortly; once ready they would like to interview us
    - Will probably be live in ~1week
- OSS-EU talk live
- Opens

Opens

-

Meeting Notes

-

Sub-Projects

(leads, please enter updates to inform full group; highlight anything for larger group discussion)
2023-10-02 - Tech Call

Attendees

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

Present ?	Name	Email	Affiliation	Pronouns	GH ID
x	Adolfo García Veytia*	puerco@chainguard.dev	Chainguard	he/him/él	puerco

Meeting Agenda

- Who wants to help out and scribe for us today?
- New Friends intros
- Updates from CISA VEX WG
- Review Issues/PRs
- Opens
- Grype integration is in 🎉
- New Integration: copa
- Recap from OpenSSF Day
- Continuing work on the OpenVEX uses cases/HOWTOs.
- Upcoming features
    - vexctl add
    - vexctl sbom
    - vexctl show

Opens

-

Meeting Notes

-

Sub-Projects

(leads, please enter updates to inform full group; highlight anything for larger group discussion)

2023-09-18 - Evangelism/Ecosystem

Meeting Notes

- Canceled for OSS-EU

2023-09-04 - Tech Call

Meeting Notes

- Canceled for US Labor Day

2023-08-21 - Evangelism/Ecosystem

Attendees

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

Present ?	Name	Email	Affiliation	Pronouns	GH ID
x	CRob	CRob@intel.com	Intel/OSSF	he/him	SecurityCRob
x	Madison Oliver	taladrane@github.com	GitHub	she/her	taladrane
x	Adolfo García Veytia*	puerco@chainguard.dev	Chainguard	he/him/él	puerco
X	Brandon Mitchell	git@bmitch.net	IBM	he/him	sudo-bmitch
X	Altaz Valani	altaz@devsecopsmentor.com	DevSecOps Mentor.com		altazv

Meeting Agenda

- Who wants to help out and scribe for us today?
- New Friends intros
- Updates from CISA VEX WG

- Review Issues/PRs
- Opens
- Working on a guide on how to implement openvex in a security scanner, expectations of the libraries, explanation of role of scanner implementing openvex in their tools
    - https://docs.google.com/document/d/1toPl2iMVd8DRY6KEKnpfsZhKBFv4cUhRy3qSL1TghOI/edit?usp=sharing
- Vuln WG MVSR - https://docs.google.com/document/d/1p83YgnkT9YJLMQoppQx9KyMbRzYqO-ALb4TrmhTh1q0/edit#heading=h.h9d3nj3ybue3

Opens

-

Meeting Notes

- Update from the CISA WG > things are progressing well 🎉
    - They're working on a OpenVEX Security Scanner Adoption Guide, our WG members are encouraged to contribute or comment on it
- Adolfo is giving an OpenVEX presentation during OpenSSF Day at Open Source Summit EU
    - Adolfo is looking for help reviewing/writing the presentation for this if community members could help with this
- The governance model for OpenVEX was created with the intention to move quickly, but it only includes the maintainer, it doesn't currently include a contributor role, so only maintainers have the capacity to review/merge PRs. How can we redo this to be more community focused?
    - How many levels do we think we need?
        - Maintainer
        - Contributor
        - These two are likely enough and should be well documented
    - Specification PRs and technical PRs, but the spec seems to be moving a bit slower than the tooling (the tooling supports the 0.2 spec, but those changes haven't yet been merged in the spec)
    - OpenVEX Specification v0.2.0 is open for review and feedback!
        - All the changes in the proposal should be captured in this PR 🤞
    - A helpful reference for OSS governance: https://opensource.guide/leadership-and-governance/
    - And reference for finding users and getting more involvement: https://opensource.guide/finding-users/
- Looking for feedback on Vulnerability Disclosure Working Group Mission - Vision - Strategy - Roadmap for the LF

    - Should include ideally 12-16 month plans, but if we have longer term plans (3-5 years) or shorter term plans, we can include them too
- We want to get more concrete use cases for OpenVEX and CSAF - we can start more theoretical and work towards a functional demo
    - We'll have a full demo for OpenSSF Day (Sept 18)
    - We'd like to get this for both the creator of VEX docs, and also the consumer of VEX docs
    - Crob has some prior examples of developing use cases and personas from the OSSF Security Toolbelt for reference
    - AI: Add list of use cases to develop, first in a google doc then move to project docs/examples

Sub-Projects

(leads, please enter updates to inform full group; highlight anything for larger group discussion)

2023-08-07 - Tech Call

Attendees

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

Present ?	Name	Email	Affiliation	Pronouns	GH ID
X	CRob	CRob@intel.com	Intel/OSSF	he/him	SecurityCRob
X	Madison Oliver	taladrane@github.com	GitHub	she/her	taladrane
X	Jay White*	jaywhite@microsoft.com	Microsoft	he/him	camaleon2016
X	Adolfo García Veytia*	puerco@chainguard.dev	Chainguard	he/him/él	puerco
X	Brandon Mitchell	git@bmitch.net	IBM	he/him	sudo-bmitch
X	Feroz Salam	feroz@argh.in	Isovalent		ferozsalam
X	Trevor Dunlap	trevor.dunlap@chainguard.dev	Chainguard	he/him	tdunlap607

X	Cheuk Ho	cheuk@openssf.org	OpenSSF	she/her	Cheukting

Meeting Agenda

- Who wants to help out and scribe for us today?
- New Friends intros
- Updates from CISA VEX WG
    - https://docs.google.com/document/d/18fbLaj5V2xpHbiRMLSbrYEH9RJ5UhuurT3WFkbBVShE/edit#heading=h.1tntg84853bg
    - They will be doing a “CFP” for next WG topics to collab on. If this team has ideas, please let Puerco and I know, adn we can pass that back to them
- Review Issues/PRs
- Lazy Consensus reached for the proposals for the first revision of the spec. Any comments before merging?
    - https://github.com/openvex/community/issues/15
    - https://github.com/openvex/community/issues/14
    - Follow up PRS:
        - go–vex: https://github.com/openvex/go-vex/pull/45
        - vexctl: https://github.com/openvex/vexctl/pull/92

- Updates being made will be backwards-compatible with original openvex spec
- 2 PRs will be opened to match identifiers and matching SBOMs (if openvex doc points to an element inside an SBOM, should allow leverage of full SBOM format)
- Working on a guide on how to implement openvex in a security scanner, expectations of the libraries, explanation of role of scanner implementing openvex in their tools
    - https://docs.google.com/document/d/1toPl2iMVd8DRY6KEKnpfsZhKBFv4cUhRy3qSL1TghOI/edit?usp=sharing
    - Comments welcome!
- Puerco will be presenting an openvex demo at OPenSSF Day in Bilbao, Spain on 18 September. Video should be on Youtube ~2weeks later

Opens

-

Meeting Notes

-

2023-07-24 - Evangelism/Ecosystem

Attendees

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

Present ?	Name	Email	Affiliation	Pronouns	GH ID
x	CRob	CRob@intel.com	Intel/OSSF	he/him	SecurityCRob
X	Madison Oliver	taladrane@github.com	GitHub	she/her	taladrane
X	Adolfo García Veytia*	puerco@chainguard.dev	Chainguard	he/him/él	puerco
X	Yotam Perkal	yotamp@rezilion.com	Rezilion	he/him	pyotam
X	Brandon Mitchell	git@bmitch.net	IBM	he/him	sudo-bmitch
X	Matt Rutkowski	mrutkowski91@gmail.com	IBM	he/him	mrutkows

Meeting Agenda

- Who wants to help out and scribe for us today?
- New Friends intros
- Updates from CISA VEX WG
- Review Issues/PRs
    - First OpenVEX Enhancement Proposals:
      OPEV-0014: Expansion of the VEX Product Field [link]
      OPEV-0015: Expansion of the Vulnerability Field [link]
    - Work to start building VEX support in Grype has been started! The pull request is open here: https://github.com/anchore/grype/pull/1397
- Puerco 's OpenVEX talk and Andrew's OSV talk have BOTH been accepted to OSSF Day in Bilbao! - https://openssf.org/blog/2023/07/19/openssf-day-europe-agenda-now-live/
    - How can we reuse this preso in other forums to spread the word?
- Thursday is the VEX Summit
    - https://vexsummit.org/schedule.html

Opens

- None

Meeting Notes

- Updates from CISA VEX WG
    - Should be getting comments back next week for review, and we will be close to a finalized version of when to issue a VEX document
    - Ongoing discussion around continuing to meet as a CISA Working Group > planning on continuing to meet to work through additional items
    - Discoverability/distribution (how do we find VEX documents when they're issued?) is a huge concern and point of discussion for that group as well - this is something our working group has discussed and would be a good collaboration across both WGs
        - Both production and consumption of VEX documents needs more discussion, and is often paired with SBOM generation, so the consumer needs should be considered as well
- Review Issues/PRs
    - First OpenVEX Enhancement Proposals:
      OPEV-0014: Expansion of the VEX Product Field [link]
      OPEV-0015: Expansion of the Vulnerability Field [link]
        - Feedback/comments on the PR are welcome!
    - Work to start building VEX support in Grype has been started! The pull request is open here: https://github.com/anchore/grype/pull/1397
- Puerco 's OpenVEX talk and Andrew's OSV talk have BOTH been accepted to OSSF Day in Bilbao! - https://openssf.org/blog/2023/07/19/openssf-day-europe-agenda-now-live/
    - How can we reuse this preso in other forums to spread the word?
    - Maybe we can collaborate with the OSV folks at this conference since we'll be together in person
    - Yotam was accepted to speak at OpenSSF day 🎉TBD if he'll be attending in person
- Thursday is the VEX Summit (Cisco sponsored)
    - https://vexsummit.org/schedule.html
    - There's a good mix of vendors doing presentations there
    - Those from this WG who are attending can share their thoughts with the group via Slack or the mailing list after the summi

Sub-Projects

(leads, please enter updates to inform full group; highlight anything for larger group discussion)

2023-07-10 - Tech Call

Attendees

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

Present ?	Name	Email	Affiliation	Pronouns	GH ID
X	CRob	CRob@intel.com	Intel/OSSF	he/him	SecurityCRob
X	Jay White*	jaywhite@microsoft.com	Microsoft	he/him	camaleon2016
X	Adolfo García Veytia*	puerco@chainguard.dev	Chainguard	he/him/él	puerco
X	Art Manion	zmanion@protonmail.com			zmanion
X	Yotam Perkal	yotamp@rezilion.com	Rezilion	he/him	pyotam
X	Brandon Mitchell	git@bmitch.net	IBM	he/him	sudo-bmitch
X	Matt Rutkowski	mrutkowski91@gmail.com	IBM	he/him	mrutkows
X	John Speed Meyers	jsmeyers@chainguard.dev	Chainguard	he/him	jspeed-meyers

Meeting Agenda

- Who wants to help out and scribe for us today?
- New Friends intros
- Updates from CISA VEX WG
- Review Issues/PRs
    - First OpenVEX Enhancement Proposals:
      OPEV-0014: Expansion of the VEX Product Field [link]
      OPEV-0015: Expansion of the Vulnerability Field [link]
      Single PR Implementing changes in both enhancements: opevex/go-vex#45
      Update to vexctl to implement the new model opevex/vexctl#92

Opens

-

Meeting Notes

- No new friends
- CISA VEX WG update
    - “When to issue VEX” doc out for final WG review
    - Will soon be considering what the WG work on next
- Review Issues/PRs
    - OPEV-0014: Expansion of the VEX Product Field [link]
    - OPEV-0015: Expansion of the Vulnerability Field [link]
    - Single PR Implementing changes in both enhancements: opevex/go-vex#45
    - Update to vexctl to implement the new model opevex/vexctl#92
    - Summary: there are needs/wants/reasons to have product and vulnerability be more than just single references or IDs, this change makes them objects with the ability to have additional fields now and in the future.

Sub-Projects

(leads, please enter updates to inform full group; highlight anything for larger group discussion)

20230626 - Evangelism/Ecosystem call

Attendees

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

Present ?	Name	Email	Affiliation	Pronouns	GH ID
X	CRob	CRob@intel.com	Intel/OSSF	he/him	SecurityCRob
X	Madison Oliver	taladrane@github.com	GitHub	she/her	taladrane
X	Art Manion	zmanion@protonmail.com			zmanion
X	Yotam Perkal	yotamp@rezilion.com	Rezilion	he/him	pyotam
X	Brandon Mitchell	git@bmitch.net	IBM	he/him	sudo-bmitch

x	Matt Rutkowski	mrutkowski91@gmail.com	IBM	he/him	mrutkows
x	Sanket Naik	sanket.naik@palosade.com	Palosade	he/him	sanketnaik-palosade
X	Trevor Dunlap	trevor.dunlap@chainguard.dev	Chainguard	he/him	tdunlap607

Meeting Agenda

- Who wants to help out and scribe for us today?
- New Friends intros
- Updates from CISA VEX WG
- Review Issues/PRs
- Opens
- https://vexsummit.org/
    - Cisco-hosted “show and tell”; looking for demos
    - Art proposes a possible “openvex” bake off./demo day sometime
- “VulnCon”
    - Vulnerability-adjacent conference forming (CVE, CVSS, EPSS, VEX, CSAF, CVD folks) https://openssf.slack.com/archives/C019Y2A28Q6/p1686843757513549
- NVD consortium participation interest?
    - Look for Federal Register notice
    - We could influence NVD to be more OSS friendly
-

Opens

-

Meeting Notes

-

Sub-Projects

(leads, please enter updates to inform full group; highlight anything for larger group discussion)

20230612 - Tech call

Attendees

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

Present ?	Name	Email	Affiliation	Pronouns	GH ID
X	CRob	CRob@intel.com	Intel/OSSF	he/him	SecurityCRob
x	Jay White*	jaywhite@microsoft.com	Microsoft	he/him	camaleon2016
X	Adolfo García Veytia*	puerco@chainguard.dev	Chainguard	he/him/él	puerco
X	Yotam Perkal	yotamp@rezilion.com	Rezilion	he/him	pyotam
X	John Speed Meyers	jsmeyers@chainguard.dev	Chainguard		jspeed-meyers
X	Trevor Dunlap	trevor.dunlap@chainguard.dev	Chainguard		tdunlap607
X	Isaac Hepworth	isaac.hepworth@gmail.com	Google		hepwori
X	Brandon Mitchell	git@bmitch.net	IBM	he/him	sudo-bmitch

Meeting Agenda

- Who wants to help out and scribe for us today?
  - John Speed volunteered
- New Friends intros
- Updates from CISA VEX WG
- Review Issues/PRs
- VEX Summit - https://vexsummit.org/
  - Are we interested in participating?
- Meeting Change proposal - Change call to weekly, and alternate between technical call and evangelism call, or keep 2-calls a month cadence and just meet once a month for each focus topic
- (@puerco) Proposed VEX workflow / tooling improvements

- (@puerco) Unify maintainers and WG governance?

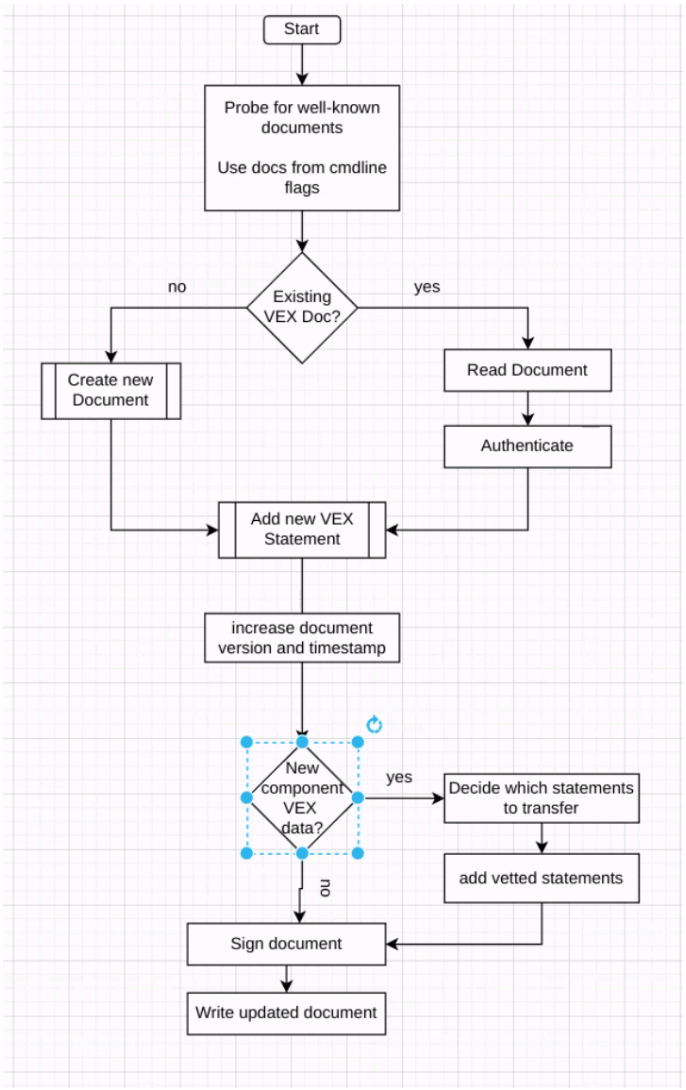
Opens

-

Meeting Notes

- Introductions
    - John Speed Meyers @ Chainguard
    - Trevor Dunlap @ Chainguard
- CISA VEX working group updates
    - Puerco
        - New document on when to issue VEX
        - Discussion on transitivity of VEX from product to component
    - Yotam:
        - Can you update a VEX with a status by issuing a new VEX?
    - Puerco
        - There was a “camp” in the past that said VEX statements should not be updated.
        - Others believed that VEX statements should be able to be updated.
        - Minimum requirements for VEX “captured both”
        - At the document level -- Puerco believes that VEX documents should be update-able
    - Yotam:
        - Does OpenVEX support updating VEX statement and updating documents?
    - Puerco:
        - Yes. OpenVEX supports both.
    - Yotam: Could it be the case that VEX statements need to be updated hourly, or very frequently, because frequent changes to configuration (or circumstances or conditions)?
        - For instance, log4j requires
    - Jay White
        - Timestamps and justifications
        - Caution: Will sometimes have to issue new documents
        - What’s the good intention if something is affected?
            - Worried about malicious actions and constant updating and appending.
            - What happens if someone does a different configuration and you are affected?
    - Yotam
        - Relates what his company does: analyze in-memory

        - Relates current state right at this moment
    - Jay White
    - Crob - Suggests a potential GH issue or GH discussion on this task
    - Brandon Mitchell
        - End user perspective - Cares about the most recent full VEX report. Not the history.
    - Puerco
        - Different use cases
            - A VEX document that comes from manual triage
            - Rapidly changing VEX from, for instance, configuration changes
            - Room for all of them
    - CRob
        - OASIS (CSAF people) holding a VEX summit. Both physical in North Carolina and enabling virtual attendance.
        - Strongly encourages this group to participate.
        - CRob will be there in the room.
        - Alternating calls between technical and evangelism - Proposal
            - Will send an email to the mailing list. Wants useful meetings and a time to collaborate.
    - Puerco
        - Need to make it easy for projects to generate VEX data
    - Puerco
        - Presentation of potential VEX User Flow diagram (draft below)



- Brandon Mitchell:
  - Where do we determine to release the VEX document?
  - Three groups may generate a VEX report: Software producer, Vulnerability scanner, and End user. Above chart is focused on the first group.
- Puerco:
  - We need to keep it simple so any project can release a VEX document. Would like to have a demo in the future.
- Puerco:
  - How can we get groups together?
- CRob:
  - Could scrape issues/PRs to get info here.
- Puerco:
  - Opening issue to discuss the idea of informing other groups.
- Isaac:

        - VEX could be an API instead of a document, we would want a real-time query on the current status of a VEX report.
    - Brandon:
        - Supporting an API means maintaining a server.
        - Attaching metadata to container images, we have been developing the referrers API in OCI for this.
    - Isaac:
        - Have we made the correct choices to make VEX look like metadata?
    - Brandon:
        - Specific to OCI, we can already obtain the metadata with an associated timestamp.
    - CRob:
        - For an enterprise, spinning up an API is achievable. For a single project with few people may find it challenging.
    - Yotam:
        - We want to allow as much flexibility as possible. Ability to build on data provided. The API would allow for us to see data from historical standpoints and a current status.
    - Josh:
        - Would make sense to set an expiration notice.
    - Isaac:
        - Worried about the time-sensitive data and static data with VEX. What's the justification that a static document is the correct way to distribute VEX? VEX has a different lifecycle and can change overtime.
    - Brandon:
        - Highlighting an issue with distribution and not a problem with the format of the document.
    - CRob:
        - Has this challenge been brought up of VEX distribution ?
    - Yotam:
        - Majority of the talks have been on the producer side (drives discussions) and less on the consumer side.
    - Puerco:
        - VEX captures a lot of human insight into the vulnerability. So the cadence for VEX distribution is much slower, due to human judgment.
    - Isaac:
        - We need to address future distribution approaches in the terms of a document centric approach
    - CRob:
        - Another future topic: the trustworthiness of the source of the issuer

Sub-Projects

(leads, please enter updates to inform full group; highlight anything for larger group discussion)

20230529 - Tech

Attendees

(please **Mark your name is black if you are here,** or add-row name/email/affiliation if joining)

Name	Email	Affiliation	Pronouns	GH ID

Meeting Agenda

- Who wants to help out and scribe for us today?
- New Friends intros
- Review Issues/PRs
- Opens

Opens

-

20230515 - Evang

Attendees

(please **Mark your name is black if you are here,** or add-row name/email/affiliation if joining)

Name	Email	Affiliation	Pronouns	GH ID
CRob	CRob@intel.com	Intel/OSSF	he/him	SecurityCRob
Madison Oliver	taladrane@github.com	GitHub	she/her	taladrane
Jay White	jaywhite@microsoft.com	Microsoft	he/him	camaleon2016
Adolfo García Veytia	puerco@chainguard.dev	Chainguard	he/him/él	puerco
Art Manion	zmanion@protonmail.com			zmanion
Brandon Lum	lumjjb@gmail.com	Google	he/him	lumjjb
Brandon Mitchell	git@bmitch.net	IBM	he/him	sudo-bmitch

Sanket Naik	sanket.naik@palosade.com	Palosade	he/him	
Yotam Perkal	yotamp@rezilion.com	Rezilion	he/him	pyotam

Meeting Agenda

- Who wants to help out and scribe for us today?
- New Friends intros
- Updates from CISA VEX WG
- Review Issues/PRs
- Opens
- Status of LF Legal review - Dan L
- Work on SIG Goals, Mission, & readme.md
    - Issac took Jay's proposal and suggested the following updates:
    - Vision: Software consumers can understand, manage, and reduce risk from known vulnerabilities in upstream components. Free tools and standard formats provide a foundation on which to build reliable, efficient, and pragmatic end-to-end risk management workflows.
    - Mission: Create an ergonomic specification for interchange of vulnerability exploitability information, and drive adoption of operational patterns putting it to practical use.
    - Scope: OpenVEX Specification, VEX Implementation, Operationalization of Vulnerability Lifecycle.

Opens

- [puerco] Final pass of the OpenVEX spec vs. minimum requirements for VEX, PR coming soon.
- VEX product discussion [example issue].
- Repository VEX project bootstrap (@puerco may do a demo in 2 weeks)

Meeting Notes

- Welcome Brandon Lum and Sanket Naik 🎉
- VEX minimum requirements document is out, not expecting more updates from the CISA VEX WG until after the SBOMorama June 14th
    - OpenVEX is missing some fields from the CISA Minimum Elements document, Adolfo will be opening a PR in the OpenVEX repo later today for discussion
    - SPDX (4.x?) has VEX already baked into its security profile, we published rc 1 last week with VEX in it

    - ➡️May 25 - next Vul Disclosure WG Australian call that often has OSV representation
        - **OpenVEX members are encouraged to join that call to see if there's any overlap or opportunities for improvement/collaboration between the projects**
- Do we have an update on the IP transfer of VEX to this WG?
    - A: not yet, but this doesn't affect our updating of the OpenVEX readme document
    - We should examine the original VEX repo to suggest improvements to their readme/docs as well since we're going through a very similar effort
- SIG vision, mission, scope discussion
    - *Proposal* > Vision: Software consumers can understand, manage, and reduce risk from known vulnerabilities in upstream components. Free tools and standard formats provide a foundation on which to build reliable, efficient, and pragmatic end-to-end risk management workflows.
        - Suggestion to s/control/management for additional focus - approved by the group
    - *Proposal* > Mission: Create an ergonomic specification for interchange of vulnerability exploitability information and drive adoption of operational patterns putting it to practical use.
    - + (crob) Provide tools and education to promote the use of VEX. Engage with industry stakeholders and open source ecosystems to encourage the use and continued refinement of VEX.
        - Is the mission too specific or broad? It's meant to be aligned with the vision which is a bit more broad than the mission proposal
        - Should we mention interoperability?
            - Do we want to diverge much from VEX specification standards, or explicitly state here that we don't intend to?
            -
    - *Proposal* > Scope: OpenVEX Specification, VEX Implementation, Operationalization of Vulnerability Lifecycle.
        - What do we mean by implementation? s/implementation/tooling if that's what we intend (like the openvex clt)
        - Vulnerability lifecycle seems very broad, and larger than VEX, so maybe s/operationalization of vulnerability lifecycle/something more specific…
        - The scope could be a constantly evolving statement that changes as we onboard new projects
        - "Use cases for OpenVEX" is something missing from this and potentially something we want to cover > we can use the CISA use cases as a starting point and will help drive adoption
    - ⏭️Crob will send an update to the mailing list to ask for feedback after today's discussion and changes to have it voted on/completed by our next discussion

- This SIG will have alternating meeting focuses > one call focused on the technology and spec maintenance, and the other will focus on the evangelism and engagement with other teams
    - Demo planned for next week's call that will be the kick off to our more technically focused alternating meetings 🎉

Sub-Projects

(leads, please enter updates to inform full group; highlight anything for larger group discussion)

20230501

Attendees

(please **Mark your name is black if you are here,** or add-row name/email/affiliation if joining)

Name	Email	Affiliation	Pronouns	GH ID
CRob	CRob@intel.com	Intel/OSSF	he/him	SecurityCRob
Madison Oliver	taladrane@github.com	GitHub	she/her	taladrane
Jay White	jaywhite@microsoft.com	Microsoft	he/him	camaleon2016
Art Manion	zmanion@protonmail.com			zmanion
Teppei Fukuda	teppei.fukuda@aquasec.com	Aqua Security	he/him	knqyf263
Isaac Hepworth	isaach@google.com	Google		hepwori
Brandon Mitchell	git@bmitch.net	IBM	he/him	sudo-bmitch
Alex Goodman	alex.goodman@anchore.com	Anchore	he/him	wagoodman

Meeting Agenda

- Who wants to help out and scribe for us today?
- New Friends intros
    - Madison
    - Teppei
    - Brandon

- Updates from CISA VEX WG
- Review Issues/PRs
- Opens
- Status of LF Legal review - Dan L
- Work on SIG Goals, Mission, & readme.md
    - Jay's proposal:
        - Vision: An internationally recognized VEX Specification tightly coupled with open developed industry best practices. A universally accepted and centralized used tool for the development of VEX documents
        - Mission: To create a universal industry-accepted VEX specification and toolset for creating multilanguage machine readable VEX documents
        - Scope: OpenVEX Specification, VEX community involvement, VEX tool creation
    - Isaac's noodling, with the intent to (a) expand scope explicitly beyond the specification to encompass operationalization (the hard part!) as well; and (b) separate vision and mission a bit:
        - Vision: Software consumers can understand, manage, and reduce risk from known vulnerabilities in upstream components. Free tools and standard formats provide a foundation on which to build reliable, efficient, and pragmatic end-to-end risk control workflows.
        - Mission: Create an ergonomic specification for interchange of vulnerability exploitability information, and drive adoption of operational patterns putting it to practical use.
        - Scope: OpenVEX Specification, VEX Implementation, Operationalization of Vulnerability Lifecycle.

Opens

- None!

Meeting Notes

- Updates from CISA VEX WG
    - Minimum Requirements for VEX published last week https://www.cisa.gov/resources-tools/resources/minimum-requirements-vulnerability-exploitability-exchange-vex
    - Long awaited publication 🎉 open to evolving the document overtime after community and use feedback
    - Crob will reach out to stakeholders to review this doc explicitly for uniformity with other VEX public guidance
    - Current doc in progress: "When (+maybe Who) to issue VEX" https://docs.google.com/document/d/152d2oRNcd7n8h8BRJpkl8zPEwC35m8x27VjFsYACavw/
- SIG mission and goal discussion

    - Please remain flexible! There is more than one working group working on VEX-related tasks, so any of the work we do here or any of the work done by others will impact each other so we will need to adjust as needed
    - Isaac: the scope is the easier part to figure out, but how to implement this and how to operationally manage this is the hard/interesting part
        - Could we call ourselves the *exploitability* SIG? Orient ourselves with the *problem*, and not necessarily the *solution*, and OpenVEX could be a solution to this. This also allows us to remain flexible and open to other solutions
    - Jay: As a SIG, our focus is on OpenVEX, so maybe the “what is the problem that we need to solve for?” conversation makes more sense at a higher level (like the Vulnerability Disclosure WG?). This may also allow us to have greater impact over time.
    - Art: SIG scope is that we did choose this as a solution, so it makes more sense to keep this particular SIG more focused on that. Broader discussions around exploitability should still happen though within the OpenSSF.
    - Isaac: Let's focus on the end to end implementation of a solution in the SIG and that might be a more impactful way to do this. Vulnerability management feels like the broader scope for the OpenSSF, and the Vulnerability Disclosure WG might want to consider a broader name.
    - Crob: we will have broader industry conversations as part of this SIG to evangelize the tooling and “spec”. The VEX standard still needs to work through quirks in open source unique properties, but we can cover some of that in the SIG. We intend to alternate the SIG focus between the specification/tooling and the broader industry adoptability and community needs.
    - Feedback is welcome on this on the notes page above! Isaac will be sharing some post-meeting and will flag folks in Slack once ready for review
    - Idea remains for alternating meetings
        - OpenVEX spec, tooling, format,
        - Higher layer left-to-right/end-to-end vulnerability management, exploitability, etc (of which VEX/OpenVEX are parts)
- No updates on the IP transfer of the VEX spec and tooling from the LF teams
- OSS-EU CFP closes tomorrow! It's in Spain in September, as always members are encouraged to submit
    - There will be an OpenSSF day held there
        - We should consider submitting a group proposal there about OpenVEX and exploitability in general
        - That CFP is separate from the OSS-EU CFP that’s closing

Sub-Projects

(leads, please enter updates to inform full group; highlight anything for larger group discussion)

20230417

Attendees

(please **Mark your name is black if you are here,** or add-row name/email/affiliation if joining)

Name	Email	Affiliation	Pronouns	GH ID
CRob	CRob@intel.com	Intel/OSSF	he/him	SecurityCRob
Jay White	jaywhite@microsoft.com	Microsoft	he/him	camaleon2016
Adolfo García Veytia	puerco@chainguard.dev	Chainguard	he/him/él	puerco
Art Manion	zmanion@protonmail.com			zmanion
Jeff Borek	jtborek206@gmail.com	IBM	He/Him	
Rose Judge	rjudge@vmware.com	VMware	she/her	rnjudge
Isaac Hepworth	isaac.hepworth@gmail.com	Google	he/him	hepwori
Alex Goodman	alex.goodman@anchore.com	Anchore	he/him	wagoodman
Ben Edgar	ben.edgar.a@gmail.com		he/him	

Meeting Agenda

- Who wants to help out and scribe for us today? Rose
- New Friends intros
- Updates from CISA VEX WG
- Review Issues/PRs
- Opens
- Status of LF Legal review - Dan L
- Work on SIG Goals, Mission, & readme.md
- Proposal - Alternating SIG meeting foci: Development (code, spec, etc.) and Evangelism (ecosystem & tools engagement, training, “marketing “ use of VEX)
- Opportunity to collaborate with OSV?
- Incoming support in Trivy
- SBOM Panel at OpenSSF Day

Opens

-

Meeting Notes

- New Friend: Art Manion - contractor to CISA; VEX WG member
- No open issues/PRs
- OpenSSF/LF legal review required - CRob to follow up with Dan on status
- How do we want to organize our meeting topics?
    - A topics - technical; B topics - VEX community/evangelism
    - Should we alternate between A and B topics?
    - Isaac: What are the outcomes we are trying to drive? What is success for VEX and what is success for OpenVEX? (Hopefully these overlap a little bit). Let's work backwards from the outcomes we want. How does VEX become operationalized?
    - Jay: There should be subcommittees since OpenVEX spec is so tightly coupled with CISA VEX wg. We need conversation updates from that wg.
        - Technical wg for vexctl as well as less technical wg for community discussions
    - Adolfo: VEX is not operationalizable right now. For OpenVEX we have tooling and libraries that can be put to work. OpenVEX is an important trailblazer to show that VEX can work. For evangelism we need to show that OpenVEX can be integrated into projects (and actually have projects using it)
    - Rose: the project needs onboarding "how to" material for easy getting started. Also need to make it clear how OpenVEX can be used with SBOMs.
        - Art: Plans to publish OpenVEX and/or CSAF VEX *without* SBOM (sometimes).
    - Adolfo: SPDX working really hard to get their VEX implementation ready for 3.0
    - CRob: Might also want to reach out to OSV team for collaboration opportunities
- Updates from CISA VEX wg:
    - Working on a VEX paper (still deciding on when to publish)
        - https://docs.google.com/document/d/152d2oRNcd7n8h8BRJpkl8zPEwC35m8x27VjFsYACavw/edit?pli=1#
    - Once that document gets finalized, it can serve as a starting point for how to get started.
    - The document speaks about VEX statements, documents and information - are they all synonymous?
        - They don't necessarily mean anything yet
        - Minimum requirements doc does make a clear distinction between VEX documents that can make VEX statements
        - It also explicitly says APIs and services are OK

- VEX has interest from many different industries (automotive, hardware, etc)
- Not everyone sees VEX in the same way: some see it as manual, some see it as zero human intervention. Once the info starts flowing through supply chain we will see what works and what doesn't
- The EO has been a forcing function to create a pathway for security metadata
- VEX would've been super useful for the Log4j: CRob had to answer lots and lots of the same question - "Is this exploitable?" and could've used VEX to make responding easier
- Jay shared vision, mission, scope document
    - Vision: An internationally recognized VEX Specification tightly coupled with open developed industry best practices. A universally accepted and centralized used tool for the development of VEX documents
    - Mission: To create a universal industry-accepted VEX specification and toolset for creating multilanguage machine readable VEX documents
    - Scope: OpenVEX Specification, VEX community involvement, VEX tool creation
    - Does "internationally recognized" indicate ISO certification (or something similar?) - We are talking to CISA *and* CSAF
    - Useful for vision or mission to speak to how we see OpenVEX alongside other VEX standards - *a* standard or *the* standard? Assume the former
    - We should capture that we want interoperability to flow from OpenVEX to CISA working group to other implementations. We can be friendly with other VEX standards when it's easy but we want to follow CISA and by default should be interoperable.
    - We should incorporate that "this is useful in practice" in the vision - needs to actually help people and be usable
- Trivy support (+ scanner discussion)
    - https://github.com/aquasecurity/trivy/pull/4053
    - There is an open PR for Trivy (vuln scanner) adding VEX support. Currently it plans to support CDX VEX and OpenVEX
    - Proposal to build in filters to vexctl but some see this as "cheating"
    - Yotam has done a bunch of research around scanner false positives and non-reported vulnerabilities and vulnerability management is not scalable. We need a new paradigm for vulnerability management that you won't patch everything but the percent of vulnerabilities actually exploitable is small - this is where he sees VEX come into play. Utopian vision is that vendors will update VEX based on various conditions
    - Adolfo will talk to security scanners at KubeCon this week
    - Human assessment will be required for most VEXs - how do we make this scalable? This is a big potential problem for VEX. - Mark this for future discussion
    - How do you trust the producer of a VEX statement? Probably want to invest time here
- SBOM Panel at OpenSSF Day

- Adolfo invited to speak on OpenVEX
- If you want to attend OpenSSF day at the conference, you must add it to your registration for a small fee ($25)
- This talk is great for evangelism and OpeVEX exposure

Sub-Projects

(leads, please enter updates to inform full group; highlight anything for larger group discussion)

20230403

Attendees

(please **Mark your name is black if you are here,** or add-row name/email/affiliation if joining)

Name	Email	Affiliation	Pronouns	GH ID
CRob	CRob@intel.com	Intel/OSSF	he/him	SecurityCRob
Madison Oliver	taladrane@github.com	GitHub	she/her	taladrane
Jay White	jaywhite@microsoft.com	Microsoft	he/him	camaleon2016
Adolfo García Veytia	puerco@chainguard.dev	Chainguard	he/him/él	puerco
Tracy Miranda		Chainguard	she/her	
Dan Luhring	dluhring@chainguard.dev	Chainguard	he/him	luhring
Isaac Hepworth	isaach@google.com	Google	he/him	hepwori
Alex Goodman	alex.goodman@anchore.com	Anchore	he/him	wagoodman
Yotam Perkal	yotamp@rezilion.com	Rezilion	he/him	pyotam

Meeting Agenda

- Who wants to help out and scribe for us today?
- New Friends intros

- Opens
- Welcome to the OpenVEX sig!
- Let's talk about the current state of openvex projects & artifacts & participants (let's make sure everyone is included in our slack and mailing lists so we don't miss them)
    - Quick background on VEX itself:
        - As software component information becomes more voluminous, more transparency will lead to more false positives (same proportion to true positives as today)
        - Need a way to help software consumers understand when scanner findings aren't applicable
        - Two VEX implementations existed prior to OpenVEX:
            - CSAF
            - CycloneDX
        - A CISA working group came up with a "spec for VEX specs", with participants from interested people
    - Why OpenVEX?
        - Want something simpler and more focused on a single use case
        - Want something that's easily embedded (e.g. as in-toto attestations)
    - Repos to know:
        - The spec itself: https://github.com/openvex/spec
        - Go library: https://github.com/openvex/go-vex
        - CLI tool: https://github.com/openvex/vexctl
            - You can use this to create new OpenVEX documents
            - You can also consume OpenVEX documents to apply them to scanner results
        - There are also independent implementations of OpenVEX in other languages:
            - Rust: https://github.com/seedwing-io/openvex-rs
            - .NET https://github.com/JamieMagee/openvex.net, https://www.nuget.org/packages/OpenVEX/
- Talk about next steps, SIG goals
    - Tracy - the integration story
    - Jay - that we're scaling; how can we work from the middle out and build the connective tissue to other groups
    - Dan - keep an eye on the ever-growing utility of the openvex spec and help people start using the spec; is it becoming more useful or do we need to adjust?
    - Adolfo - work on the understanding of how we can get upstream's life easier so that the info can filter downstream; piggy back on SBOM as well
    - Crob - shared diagram showing relationships between OpenSSF projects and how they fit together from a CI/CD perspective (https://github.com/ossf/Diagrammers-Society/blob/main/drawings/ossf-cicd2-0.png)
- Look for volunteers to assist in filling out our git repo readme.md to match other sigs/wgs
    - https://github.com/ossf/OpenVEX

    - Puerco
    - Jay
-

Opens

- [tracy]Announcement blog post for OpenSSF
    - Looking for some authors and reviewers - crob & jay can start drafting & share for more input
- [tracy]OpenVEX logo?
    - Branding
    - Either an OSSF goose picture or an independently created
    - Rose offered to do an initial drawing
    - Team - let's talk about ideas for logo in our Slack and we'll make this one of the 1st items to talk about on our next call. Submit ideas or drawings and we can get real artists to assist too
- [puerco] Recap of first maintainers meeting
    - OpenVEX has been moving fast, and is still very young
    - Held the first meeting of all maintainers last week
    - Talked about:
        - Where we want to head as a project
        - Do we like the existing governance model, and what changes might be needed as part of the OpenSSF donation?
        - Crob:
            - Four tiers of participation:
                - Lurkers
                - Contributors
                - Collaborators (more active, several issues/commits)
                - Maintainers
            - We'll figure out how this works and make sure this is appropriately reflected in the access control of the GitHub projects themselves
            - Crob will work with the operations team to get things into place
        - Ideally the project/governance is fairly low maintenance, since this is a specification first and foremost
        - Discussed meeting cadence
            - Monthly?
            - Currently the OpenVEX SIG meeting is set for every two weeks
                - We could alternate these between:
                    - Implementation/technical focused
                    - Community/outreach focused
        - It's important to us that we not overstep the direction from the central CISA VEX working group
            - Crob: We should regularly read back latest from this group to the SIG

- What should the relationship be with other independent implementations? Try to bring them under the OpenVEX org, or collaborate with the current state?
    - Group leaned toward leaving that to the maintainers of those projects, and defaulting to letting them stay independent
    - This consensus seems shared with the SIG folks
- What does the road to greater adoption of OpenVEX look like?
    - **Thinking about this question could be good homework for members of the SIG :)**

Meeting Notes

-

Sub-Projects

(leads, please enter updates to inform full group; highlight anything for larger group discussion)

<TEMPLATE DATE>

Attendees

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

Present ?	Name	Email	Affiliation	Pronouns	GH ID
	CRob	CRob@intel.com	Intel/OSSF	he/him	SecurityCRob
	David A. Wheeler	dwheeler@linuxfoundation.org	Linux Foundation		
	Madison Oliver	taladrane@github.com	GitHub	she/her	taladrane

	Brandon Lum	lumjjb@gmail.com	Google	he/him	lumjjb
	Jay White*	jaywhite@microsoft.com	Microsoft	he/him	camaleon2016
	Olle E. Johansson	oej@edvina.net	Edvina AB	he/him	oej
	Adolfo García Veytia*	puerco@chainguard.dev	Chainguard	he/him/él	puerco
	Tracy Miranda		Chainguard	she/her	
	Randall T. Vasquez	randall@icloud.com	Gentoo	he/him	ran-dall
	Dan Lorenc				
	Art Manion	zmanion@protonmail.com			zmanion
	Sandipan Roy				
	Yogesh Mital				
	Roberth Strand				
	Andrew Pollock				
	Yotam Perkal	yotamp@rezilion.com	Rezilion	he/him	pyotam
	Brandon Mitchell	git@bmitch.net	Independent	he/him	sudo-bmitch

Meeting Agenda

- Who wants to help out and scribe for us today?
- New Friends intros
- Updates from CISA VEX WG
- Review Issues/PRs
- Opens

Opens

-

Meeting Notes

-

Sub-Projects

(leads, please enter updates to inform full group; highlight anything for larger group discussion)