GUAC Community Meeting Notes

https://github.com/guacsec/guac/

Cursor Parking lot [ ]

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.linuhttps://www.youtube.com/channel/UCUdhiXNEBEayowJXY_v7AXQ/videosxfoundation.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.

Code of Conduct

All OpenSSF meetings are subject to its code of conduct. See https://openssf.org/community/code-of-conduct/

Youtube Channel for past recorded Community meetings:
https://www.youtube.com/@guacsec/videos

Attendees:

Brandon Lum, Michael Lieberman, Jeff Mendoza, Dana Wang, Dejan Bosanac, Amanda Martin, Parth Patel, Marco Rizzi, Max Dessi, Ridwan Hoq, Eman, Phil Cattanach, Abhishek Reddypalle, Nathan Naveen, Tim Miller, Sunny Yip, Kevin Conner, Marco Deicas, Santiago Torres-Arias, Jennifer Pospishek, Soham Arora, Ed Baunton,Yotam Perkal, Narsimham Chelluri, Arnav Joshi, Casey Fahey, Mihai Maruseac, Hari Kunduru

Planning

Participation in this meeting is in acceptance with GUAC open source project governance.

Future Agenda topics:

- Apache Jena
- Using semantic web technologies
- Alpha-Omega assertions project (https://github.com/ossf/alpha-omega/issues/28)
- [Brandon] SBOMs and SLSA talk at Kubecon (from Kubecon)

Action Items:

- ~~Dejan to show integration into policy engine (https://github.com/dejanb/guac-rs)~~

- ~~Dejan: Show S3 collector~~
-

Meeting notes

2025-06-12 Community meeting

Attendees:

- Ben Cotton (Kusari)
- Brandt Keller (Defense Unicorns)
- Jeff Mendoza (Kusari)
- Kris Borchers (Linux Foundation)
- Michael Lieberman (Kusari)
- Parth Patel (Kusari)
-

Agenda:

- Reminders
    - This meeting is recorded and will be posted to the GUAC YouTube channel
    - This is an OpenSSF meeting subject to the Code of Conduct and the Linux Foundation Antitrust Policy
- Welcome new friends!
- GUAC 1.0!
- [Brandt] Zarf+GUAC
- Upcoming events (see OpenSSF calendar for meeting details)
    - Weekly Maintainer Meeting: Mondays
    - Community Meeting: Thursday 16 July
    - Open Source Summit North America & OpenSSF Community Day
        - Mihai Maruseac will be on a panel about strengthening software supply chains

        - Mihai Maruseac will be presenting a talk on model signing on Kaggle, a talk about extending model signing with secure model cards, and a talk about secure AI agents
        - Brandt Keller will be presenting a talk on GUAC and Zarf
        - Mihai Maruseac will be on a tabletop exercise panel
    - Open Source Summit Europe & OpenSSF Community Day
        - Mike Lieberman will be on a CRA panel
        - Ben Cotton will be co-presenting an OpenSSF Community Day keynote on OpenSSF's ORBIT working group
        - Dejan Bosanac and Ben Cotton will be presenting a talk on the GUAC+Trustify merge
        - Mihai Maruseac will be presenting a talk on extending model signing to cover other ML metadata

2025-04-17 Community meeting

Attendees:

- Ben Cotton (Kusari)
- Dejan Bosanac (Red Hat)
- Michael Lieberman (Kusari)
- Brandon Lum (Google)
- Jeff Mendoza (Kusari)
- Casey Fahey
- Mihai Maruseac (Google)

Agenda:

- Reminders
    - This meeting is recorded and will be posted to the GUAC YouTube channel
    - This is an OpenSSF meeting subject to the Code of Conduct and the Linux Foundation Antitrust Policy
- Welcome new friends!
- (Ben) ladder climbs
    - Ben Cotton promoted to Reviewer for GUAC Visualizer
- (Jeff) Kubescape collector
    - Introduced in GUAC v0.14.0
    - Jeff and Ben Hirschberg gave a talk at KubeCon Europe
    - Supports "filtered" SBOMs — a custom resource that Kubescape adds. It shows the SBOMs for what is running in the cluster.
        - Regular SBOMs provide a list of packages
        - Filtered SBOMs provide only the packages that eBPF detects are loaded into memory. If a package exists in the filtered SBOM but not in the unfiltered SBOM, it's not being run
    - Kubescape also supports producing VEX statements for packages it detects are not loaded into memory. Jeff wants to add support for that to GUAC
- GUAC 1.0 technical overview and feedback
- Topics being discussed in maintainer meetings
    - GUAC/Trustification community discussion

        - Trustification came from an earlier version of GUAC but kept in the same problem space
        - Looking at combining the two projects under one community in order to tackle common problems and give users an easier way to address their needs at any scale
        - First steps
            - Identify common ground for shared tools/libraries/protocols
            - Brandon: it would be good to think about better support of extension to the data
- KubeCon EU thoughts
    - Mike: CNCF plans to try out using GUAC to do supply chain analysis across all CNCF projects.
        - They have issues with license and vulnerability management. That's typically left to individual projects, but they want to be able to have a broad-level view to ensure there aren't issues that projects need to address.
        - Over the next few months, they plan to start looking at this in earnest. Mike is working with them to help build an understanding of their needs and getting them started.
    - Mike: Did a talk with Andrew Martin of ControlPlane about Flux and GUAC. Talked through using GUAC to locate vulnerable packages in Flux-deployed applications. Possible future work to use GUAC as a data source for policy engines on GUAC deployment.
    - Mike: eventually we'll want to look at supporting OSPS Baseline. The data will probably come in via Scorecard
- Mike: gave a talk at VulnCon. Couldn't do a demo because it was slides-only.
- Mike: There's ongoing discussion of what the future of CVEs looks like. Maybe there's no centralized authority and things are distributed. Similarly, SBOM information and other stuff is decentralized. This could have impacts on how GUAC collectors work.
- Upcoming events (see OpenSSF calendar for meeting details)
    - Weekly Maintainer Meeting: Mondays
    - Community Meeting: Thursday 15 May

2025-03-20 Community meeting

Attendees:

- Ben Cotton (Kusari)
- Jeff Mendoza (Kusari)
- Parth Patel (Kusari)
- Nathan Naveen (Kusari)

Agenda:

- Reminders
    - This meeting is recorded and will be posted to the GUAC YouTube channel
    - This is an OpenSSF meeting subject to the Code of Conduct and the Linux Foundation Antitrust Policy
- Welcome new friends!

- (Jeff) Kubescape collector
- (Maintainers) 2.0 discussion
- Upcoming events (see OpenSSF calendar for meeting details)
    - Weekly Maintainer Meeting: Mondays
    - Community Meeting: Thursday 17 April
    - KubeCon Europe (1-4 April in London)
        - DevSecOps on the Rocks party (1 April)
        - Kusari booth: S482

2025-02-20 Community meeting:

Attendees:

- Ben Cotton (Kusari)
- Mihai Maruseac (Google)
- Dejan Bosanac (Red Hat)
- Ria Farrell Schalnat (Hewlett Packard Enterprise)
- Arnav Joshi (Akamai)
- Craig Pearce (AWS)
- Parth Patel (Kusari)
- Michael Lieberman (Kusari)
- Casey Fahey (Net Goalie)

Agenda:

- Reminders
    - This meeting is recorded and will be posted to the GUAC YouTube channel
    - This is an OpenSSF meeting subject to the Code of Conduct and the Linux Foundation Antitrust Policy
- Welcome new friends!
    - Craig was recently geeking out over GUAC and Sigstore
    - Ria is interested in the ClearlyDefined integration and learning more about GUAC generally
    - Arnav has general interest in the software supply chain space. Attended meetings a few months ago
- Releases since the last meeting:
    - GUAC v0.13.0 (and 0.13.1 and 0.13.2)
        - Adds support for OpenTelemetry
    - Upcoming work
        - Continuing to work on defining the feature set for 1.0. We're close to getting it ready for that
        - Also working on improving the usability with design changes, etc for "GUAC 2.0"
        - Folks from Microsoft are working to unify SBOM representation across multiple image registries (issue 2387)
- FOSDEM recap (1-2 Feb in Brussels)
    - Jeff and Michael attended attended fringe event: FOSS license and security compliance tools workshop (31 Jan)

        - Lots of discussion of CycloneDX and SPDX formats. SBOMs are starting to hit a critical mass. People are now looking to do useful things like that, and therefore need tools (like GUAC!)
            - Looking for vulnerabilities, license issues, etc
            - Also a view over time as new versions are developed
    - Talks
        - Brandon Lum & Marco Deicas: "A retrospective on Google's SBOM implementation"
        - Jeff Mendoza & Qing Tomlinson: "Discover Dependency License Information Using SBOMs and ClearlyDefined"
        - Michael Lieberman: "The Breadth and Depth of SBOMs"
            - How do you get from zero to full end-to-end visibility?
    - CRA discussions:
        - Some conversations about SBOMs and how tools like GUAC can help folks understand risk and compliance
- [Ria] Using GUAC to improve license compliance
    - At the CISA community meeting, Ben presented on GUAC, with a discussion of the ClearlyDefined support. Opened her eyes as to how ClearlyDefined could be a more scalable resource for day-to-day input to her process.
    - At an SPDX general meeting, there was discussion of Snyk's parlay tool. Parlay uses a different information backend (ecosyste.ms)
    - More confidence in the ClearlyDefined data, but parlay has a useful feature to her: ingesting and then producing an improved SBOM.
    - The goal is to reduce the number of "NO ASSERTIONS" in the dependency graph.
    - Mini test: one SBOM went from 35 NO ASSERTIONS down to 25. That's a material improvement.
    - Wants to use guacone to decorate the SBOM or produce a decorated SBOMs
    - Is this something that GUAC would consider?
        - Michael: open question is where that integration lands. For example, OpenSSF's bomctl is intended to be an SBOM improver, with integration into tools like GUAC
        - Parth: the goal for GUAC was always to take the information you have and add data from the outside to make it better. Then we could support getting it back out to an SBOM or however you need to consume it.
    - Another area for improving the SBOM is creating an attribution document for complying with licenses that require it. Ria would like to see SBOM and attribution merged together into one machine-readable whole.
- Upcoming events (see OpenSSF calendar for meeting details)
    - Weekly Maintainer Meeting: Mondays
    - Community Meeting: Thursday 20 March
    - KubeCon Europe (1-4 April in London)
        - Michael Lieberman is presenting a keynote "Cutting Through The Fog: Clarifying CRA Compliance in Cloud Native" with Eddie Knight
        - Jeff Mendoza is presenting a talk "Why Don't We Have Both? Track Build- and Run-time Information for Security With Kubescape and GUAC" with Ben Hirschberg

        - Michael Lieberman is presenting a talk “Bridging Supply Chain Policy with Git-less GitOps and GUAC” with Andrew Martin.

2025-01-16 Community meeting:

Attendees:

- Ben Cotton (Kusari)
- Mihai Maruseac (Google)
- Brandon Lum (Google)
- Narsa Chelluri (Kusari)
- Jeff Mendoza (Kusari)
- Parth Patel (Kusari)
- Alex Feng (Microsoft)
- Casey Fahey (NetGoalie)
- Michael Lieberman (Kusari)

Agenda:

- Reminders
    - This meeting is recorded and will be posted to the GUAC YouTube channel
    - This is an OpenSSF meeting subject to the Code of Conduct and the Linux Foundation Antitrust Policy
- Welcome new friends!
- Contributor ladder climbs
    - Robbie Cronin:
        - Reviewer for CLI
        - Reviewer for Collectors
    - Nathan Naveen
        - Reviewer for CLI
    - Ben Cotton
        - Owner for Docs
- Releases since the last meeting:
    - GUAC: v0.12.0
        - New certifier for EOL.date (Thanks Robbie!)
        - New collector for OCI registry (Thanks Robbie!)
        - Improvements to OSV certifier
        - Deps.dev scanner on ingestion
- Cool new features
    - Datadog dataset certifier
        - https://github.com/guacsec/guac/pull/2366
        - Brandon: this shows how simple it is to add additional certifiers for datasets. This is a nice PR to use an example if anyone wants to add a new certifier.
- Blog post on 2024 looking back
    - https://github.com/guacsec/guac-landing/issues/122
    - Brandon: thanks for joining us in 2024, Ben
- What to do about 1.0? What should go in it? Should we jump directly to the refactor?
    - Update on that discussion

        - Reviewing with Red Hat folks on their data model and experiences with using GUAC
        - Google work on mapping internal supply chain to GUAC ontology
    - Brandon: For 1.0, we want to know what parts users want to be stable
    - Mihai: We've experimented a lot with the current setup (DB backends, etc). Now it's time to settle on an architecture that works for users
    - Parth: Original architecture may have been too ambitious, trying to please everyone and became too pluggable. Now that the supply chain space has evolved and it's become more stabilized in terms of what people want. From a developer standpoint, how do we make this easier for someone to pick up and use on their own project? Right now it's very scalable, great for enterprises, but doesn't address the small developer & easy adoption. How do we go about that?
    - Jeff: I support calling what we have here 1.0. There's some worry that it's an "empty promise" since we're not going to continue it as it is exactly. It's essentially a complete idea that could be used and picked up, so we should put a stamp on it. "2.0" might be called something else that makes it more clear that it's different and we could have, for example, "GUAC Monolith" and "GUAC components"
    - What is in scope of 1.0
        - Parsers
        - Collectors
            - File, OCI, etc.
        - Ingestor
        - Postgres backend
- [Alex] How should we represent/ingest multiple instances of the same image?
    - https://github.com/guacsec/guac/issues/2387
    - Current backend assumptions
        - Can't trust SBOM contents subject, which GUAC relies on.
            - 1. SBOMs should be created at image build time and should follow across registries
            - 2. SBOMs should be signed, which means you can't regenerate when moved across registries
    - Considering an option to override the subject at ingestion time
    - In the graph, should there be a node for the digest that other objects are connected to?
    - Brandon: in the HasSBOM, we could create a predicate that connects it to the artifact hash, which would solve the problem of moving the image to another registry.
        - Jeff: the ontology supports SBOM on the artifact, but the parsers don't
        - Parth: it will do it on artifact first, if it's not there, it will do it on the package. So if the SBOM contains the proper digest for the image, it will behave correctly
        - Brandon: this section from a previous talk may be helpful: https://youtu.be/ZYsUbN6oT7Q?feature=shared&t=1431
    - ACTION: Alex to set up a follow-up meeting with Brandon, Parth
- Upcoming events (see OpenSSF calendar for meeting details)
    - Weekly Maintainer Meeting: Mondays, but cancelled next week

    - Community Meeting: Thursday 20 February
    - FOSDEM (1-2 Feb in Brussels)
        - Several contributors attending fringe event: FOSS license and security compliance tools workshop (31 Jan)
        - Brandon Lum & Marco Deicas: "A retrospective on Google's SBOM implementation"
        - Jeff Mendoza & Qing Tomlinson: "Discover Dependency License Information Using SBOMs and ClearlyDefined"
        - Michael Lieberman: "The Breadth and Depth of SBOMs"
    - KubeCon Europe (1-4 April in London)
        - Michael Lieberman is presenting a keynote "Cutting Through The Fog: Clarifying CRA Compliance in Cloud Native" with Eddie Knight
        - Jeff Mendoza is presenting a talk "Why Don't We Have Both? Track Build- and Run-time Information for Security With Kubescape and GUAC" with Ben Hirschberg
        - Michael Lieberman is presenting a talk "Bridging Supply Chain Policy with Git-less GitOps and GUAC" with Andrew Martin.

2024-11-21 Community meeting:

Attendees:

- Ben Cotton (Kusari)
- Brandon Lum (Google)
- Mihai Maruseac (Google)
- Brandt Keller (Defense Unicorns)
- Lukas Hoehl (STACKIT)
- Dejan Bosanac (Red Hat)
- Casey Fahey (NetGoalie)
- Tim Miller (Kusari)
- Marco Deicas (Google)
- Alex Feng (Microsoft)
- Parth Patel (Kusari)
- Ridwan Hoq (Microsoft)
- Hari Kunduru (ARA)

Agenda:

- Reminders
    - This meeting is recorded and will be posted to the GUAC YouTube channel
    - This is an OpenSSF meeting subject to the Code of Conduct and the Linux Foundation Antitrust Policy
- Welcome new friends!
    - Lukas: based in Germany working for STACKIT. Has been watching the GUAC repo for a year.
    - Brandt: works for Defense Unicorns (large focus on public sector). Sees a lot of the problems that GUAC helps solve. Met with Kusari team at KubeCon
- Releases since the last meeting:
    - GUAC: v0.10.2, v0.11.0, v0.11.1, v0.11.2

        - Adds HTTP handler to display version string
        - Add batch querying for isDependency, CertifyVuln and CertifyLegal via Package Version ID
- Decisions:
    - We're canceling the GUAC Time office hours due to low attendance
        - Weekly Maintainer Meetings are still public
- [Brandon Lum] Update on GUAC refactor
    - At recent Maintainer Meetings, we've been chatting about lessons learned and feedback on GUAC. The goal is to make GUAC easier to use for people. For example, GraphQL is hard to get started with. People want an easier way to get started
    - Making a shift in the audience we're serving as a project. Initially, the idea was an all-in-one where you put in documents and get insights. But we realized there are more audiences and some of them (e.g. Kusari and Red Hat products) would like to use parts of GUAC with their own interfaces
    - Three main areas
        - Easy to build solutions on top of GUAC
        - Easier on-ramp to see what GUAC can do without having to get deep into graph database
        - Foster an insights/policy building community around the project
    - GUAC = Aggregation + Synthesis
        - guac-ingest: How do I make meaning out of metadata? This can be a starting point for basic users.
        - guac-graph: How do I create a scalable supply chain knowledge graph (this is what current GUAC is). More advanced users can integrate this into their infrastructure.
        - guac-insights: Insights for policy checks, patch planning, etc
    - Ben: How much work will this take and what help do we need?
        - There's some work to split up the current project into more modular pieces. In particular, converting the GraphQL schema to Protobuf. We could use community feedback in how people want to use the graph interface and how we can design it better.
    - Rough roadmap
        - Graph v1, which exposes ent SQL and hides GQL interface, for Q1 2025
        - Ingest v2 ontology (protobuf/json ontology) worked on in parallel for Q3 2025
        - Graph v1.x compatible with both ent and GQL, in Q3-4 2025
        - Insights, continual experimentation (not looking to create specific versions yet). Not looking to package yet
    - What does this actually look like?
        - Guac-ingest: CLIs that allow converting metadata files into a guactology JSON, piping output into JQ and a query language
- KubeCon NA recap
    - Parth & Mihai presented "Papers, Please: Scrutinizing AI Model Creation" at SigStore Con
    - GUAC got mentions in three separate keynotes
- [Lukas Hoehl] Ingesting trivy SBOMReports into guac

    - https://github.com/hown3d/guac-trivy-operator-webhook
    - Background: using the trivy operator in a lot of clusters. Using collectors like s3 buckets is not easy because it would need to be pull from trivy into the s3 bucket first. But the trivy operator has a webhook, so he can use that to ingest documents into GUAC
    - Parth: is the trivy scan giving a runtime SBOM?
        - If there's no SBOM attached, it will generate a new one by scanning the image. If there's an SBOM in the registry, it will use that.
    - Parth: we also chatted with Kubescape (has similar functionality to trivy) maintainers, which generates a runtime SBOM and a network report of ingress/egress traffic. One thought we were having is to use that to implement isDeployed support. With that info, GUAC could do analysis for difference between build- and run-time dependencies. Produces VEX docs that indicates if a dependency is not being used in runtime.
    - Hari: uses both trivy and GUAC. Does this bridge the gap between the trivy operator and GUAC?
        - Yes
- Cool in-progress contributions:
    - Feat/registry collector cli additions #2241
        - https://github.com/guacsec/guac/pull/2241
    - Collect additional metadata for vulnerabilities from OSV #2219
        - https://github.com/guacsec/guac/pull/2219
        - OSV has more information than we currently use. Created an option to include additional metadata like severity, so users can filter out lower-severity vulns to help with prioritization
- [Brandt] Airgap Support
    - https://github.com/guacsec/guac/issues/2294
    - In talking with others at KubeCon, there's a lot of nuances to running GUAC in air-gapped environments. For example: accessing data. But we have tools like zarf that can help. Wants to start discussion about how this could work.
    - Availability survey: https://whenisgood.net/air-guac
- Upcoming events (see OpenSSF calendar for meeting details)
    - Weekly Maintainer Meeting: Monday
    - Community Meeting: Thursday 19 December

2024-10-17 Community meeting:

Attendees:

- Ben Cotton (Kusari)
- Brandon Lum (Google)
- Marco Deicas (Google)
- Mihai Maruseac (Google)
- Shreyas Pandya (Guidewire)
- Casey Fahey (NetGoalie)
- Parth Patel (Kusari)
- Mohamed Chorfa (Thales SA)
- Jeff Mendoza (Kusari)

Agenda:

- Reminders
  - This meeting is recorded and will be posted to the GUAC YouTube channel
  - This is an OpenSSF meeting subject to the Code of Conduct and the Linux Foundation Antitrust Policy
- Welcome new friends!
- Releases since the last meeting
  - GUAC: v0.8.7, v0.8.8, v0.8.9, v0.9.0, v0.9.0, v0.10.0, v0.10.1
    - Upgrades to ent backends and lots of QOL and bugfixes (especially around clearly defined ingestor)
    - In 0.8.9 there was a small compatibility breaking change in the vulnerability query, it will be documented in the release flow.
  - guac-visualizer: v0.4.5
    - Adds a view of known package information
    - Now with CI builds
- Decisions:
  - We're deprecating all other backends, one backend to rule them all
  - Key-value will be testing only
- Heads up on maintainer discussions (on Monday):
  - Discussion on going from GQL → SQL as an interface
- [Ben Cotton] How our demo flow is working
  - GUAC "sizzle reel" (https://www.youtube.com/watch?v=JZOIAfrpKek)
  - Slides: GUAC Demo Pages - October 2024
- Upcoming events (see OpenSSF calendar for meeting details)
  - Hacktoberfest (ongoing through 31 October!)
  - Weekly Maintainer Meeting: Monday
  - SOSS Fusion (Atlanta, GA): 22–23 October
    - Jeff and Mihai will be there
  - GUAC Time office hours: next Friday (25 October)
  - KubeCon NA (Salt Lake City, UT): 12–15 November
    - Open Source Security on Tap party hosted by Kusari, ActiveState, and ControlPlane
  - Community Meeting: Thursday 21 November

2024-09-19 Community meeting

Attendees:

- Ben Cotton (Kusari)
- Brandon Lum (Google)
- Jeff Mendoza (Kusari)
- Marci Rizzi (Red Hat)
- Shreyas Pandya (Guidewire)
- Parth Patel (Kusari)
- Casey Fahey (NetGoalie)

Agenda:

- Reminders
    - This meeting is recorded and will be posted to the GUAC YouTube channel
    - This is an OpenSSF meeting subject to the Code of Conduct and the Linux Foundation Antitrust Policy
- Welcome
    - Shreyas (Guidewire) - joining for the first time - meets with parth on the regular basis.
- Demos
    - [Ben] guac-scripts: guactober & license_check
    - [Ben] New guac-visualizer release
- Incremental releases
    - Two today (v0.8.5 and v0.8.6)
- Hacktoberfest participation: guac-docs and guac-visualizer
    - https://github.com/guacsec/governance/issues/30
- [Brandon] Is writing the SQL for the REST queries easy for what you want to do, Marco?
    - Marco: Things had been based on 0.3, now we're trying to keep up with latest GUAC. I have been adapting all of that. I've been trying to upstream fixes as quickly as possible. Regarding the queries, I've rewritten them all to work with the new data model. There's a lot of stuff going on. Updating GUAC is part of making the product more reliable.
    - Marco: With the new data model, the queries are easier and better. The good news is that Ent supported everything I had to do.
- Upcoming events (see OpenSSF calendar for meeting details)
    - Weekly Maintainer Meeting: Monday
    - Cloud Native Live: Tuesday 24 September
    - GUAC Time office hours: next Friday (27 September)
    - Community Meeting: Thursday 17 October

2024-08-15 Community meeting

Attendees:

- Ben Cotton (Kusari)
- Jeff Mendoza (Kusari)
- Nathan Naveen (Kusari)
- Dejan Bosanac (Red Hat)
- Brandon Lum (Google)
- Marco Deicas (Google)
- Mike Lieberman (Kusari)
- Narsa Chelluri (Kusari)
- Parth Patel (Kusari)
- Nick Vidal (Open Source Initiative)
- Alex Feng (Microsoft)
- Arvind Singharpuria
- Tim Miller (Kusari)
- Sunny Yip (Kusari)

Agenda:

- Reminders
  - This meeting is recorded and will be posted to the GUAC YouTube channel
  - This is an OpenSSF meeting subject to the Code of Conduct and the Linux Foundation Antitrust Policy
- Welcome:
  - Arvind, joining back after a long time! Recent college graduate! Looking to contribute.
- [Ben Cotton] Contributor ladder updates: https://guac.sh/contributing/#contributor-ladder
- [Nathan Naveen] rate limiting for Deps Dev, OSV, and ClearlyDefined
  - Don't want to hit external APIs too much and get blocked
  - Currently open PR
  - 2 limiters
    - HTTP - for osv and clearly defined
    - GRPC limiter - deps.dev
- [Nathan Naveen] REST endpoints to find the latest SBOM as well as the vulns and licenses in the latest SBOM
  - Do we want to have an endpoint that lists all of the packages that match a specific query? For example "list all versions of Log4j/core". Brandon suggested something like the "Terror of cURL" blog post.
  - ACTION: Mike to open an issue to discuss the specific use case
- [Nathan Naveen] end-to-end testing updates
- [Jeff/Parth] Demo ClearlyDefined integration
  - Included in v0.8.0. See the blog post: https://guac.sh/blog/2024-08-01-clearlydefined/
  - ClearlyDefined provides "discovered" licenses beyond just the declared license of a package
  - Includes attribution information
- [Parth Patel] Breaking change in Ent databases if re-ingesting existing SBOMs: https://github.com/pxp928/guac-update-db
  - Due to `IsDependency` being changed in v0.8.0 to only version-to-version, not package name
  - With existing databases, upgrades from <= 0.7.2 to 0.8.0 will break. Parth's script will check the database and fix the relationships if run *prior* to the upgrade.
- [Abhisekh / Brandon] User Journey interviews and looking for participation
  - GUAC user journey study
- What are users expecting for ingestion time?
- Upcoming events (see OpenSSF calendar for meeting details)
  - GUAC Time office hours: tomorrow! (EMEA & eastern Americas)
  - Weekly Maintainer Meeting: Monday
  - GUAC Time office hours: Friday 30 August (Americas)
  - Community Meeting: Thursday 19 September

2024-07-18 Community meeting

Attendees:

- Narsa Chelluri (Kusari)
- Jeff Mendoza (Kusari)
- Ridwan Hoq (Microsoft)
- Parth Patel (Kusari)
- Soham Arora (Purdue)
- Ben Cotton (Kusari)
- Tim Miller (Kusari)
- Sunny Yip (Kusari)

Agenda:

- Reminders
    - This meeting is recorded and will be posted to the GUAC YouTube channel
    - This is an OpenSSF meeting subject to the Code of Conduct and the Linux Foundation Antitrust Policy
    - Mailing lists are moving. Should we mass-migrate everyone?
- Introductions and welcome members!
- [Ben Cotton] Community updates
    - Stats from the last quarter
        - 6 first-time contributors
        - 2 contributor ladder promotions
        - 7 non-maintainers joined the Maintainers Meetings, representing 5 different affiliations
    - Goals for this quarter
        - 6 first-time contributors
        - 2 contributor ladder promotions
        - Add 1 major company or FOSS project as a reference user
- [Ben Cotton] web & marketing updates
    - New Why GUAC? page to help with messaging
    - GUAC added to the OpenSSF SBOM Catalog
- What are the maintainers working on?
    - Vuln scan on ingestion (not certifier)
        - Ridwan: can Deps.Dev be done at the same time to fill out the entire tree at time-of-ingestion?
            - Parth: It's possible, but it adds a lot of latency to the ingestion. Deps.Dev runs as a collector-subscriber so it's not waiting on an interval. Once the SBOM is ingested, the Deps.Dev request gets queued, so you'll get the data in (probably) a few minutes.
            - Ridwan: Should the vulnerability certifier then be done the same way?
            - Parth: Collector-subscribers only run once, but certifiers run at an interval. We want vulnerability info to be updated if new vulns are discovered. It's not using ingestion data, it's using graph data.
    - Delete HasSBOM HasSLSA and CertifyVuln

- [Nathan Naveen] end-to-end testing updates
    - We'll wait until next month when Nathan can present
- Upcoming events (see OpenSSF calendar for meeting details)
    - GUAC Time office hours: tomorrow! (EMEA & eastern Americas)
    - Weekly Maintainer Meeting: Monday
    - GUAC Time office hours: 2 August (Americas)
    - Community Meeting: 15 August

2024-06-20 Community meeting

Attendees:

- Ben Cotton (Kusari)
- Marco Rizzi (Red Hat)
- Narsa Chelluri (Kusari)
- Jeff Mendoza (Kusari)
- Dejan Bosanac (Red Hat)
- Parth Patel (Kusari)
- Ridwan Hoq (Microsoft)
- Alex Feng
- Sunny Yip (Kusari)

Agenda:

- Record the meeting!
- Introductions and welcome members!
- V0.7.0 (blog post)
    - Include Pagination for KeyValue
    - Added annotate-metadata command via guacone CLI (Experimental)
    - WIP for Get Next Actionable Critical Dependencies (Experimental - REST API)
    - Improved CDX parsing for transitive dependencies
    - GraphQL - Expose all client queries (paginated and non-paginated)
    - [ENT] Controlled and automated schema version migration via Atlas
    - Update certifiers to use paginated query for package and source
    - Update S3 collector to support collecting from a directory within the bucket
- [Ben Cotton] assorted updates!
    - Blog posts are now individual files
    - Blog now has an RSS feed
    - Old meetings are now on the YouTube channel with notes in the governance repo.
    - Moving the mailing list to lists.openssf.org (governance#6)
- [Ben Cotton] Proposal to add additional topic areas to the contributor ladder (guac#1935)
- What are the maintainers working on section
    - [Parth] Expose certifier and deps.dev batch size and add optional latency
    - [Parth] Query OSV during ingestion for vulnerability feedback
        - Mention the pubsub idea to get feedback, and get folks to join this call if they're interested
    - [Brandon] Golang PURL trickiness

        - Ben: Brandon mentioned ECMA TC54-TG2 should we have a maintainer join that?
- Next meetings
    - GUAC Time office hours: (EMEA & eastern Americas) tomorrow!
    - Weekly Maintainer Meeting: Monday
    - GUAC Time office hours: (Americas) Friday, July 5
    - Community Meeting: Thursday July 18

Meeting notes
May 16, 2024 : Community meeting

Attendees
- Jon Zeolla (Zenable)
- Ben Cotton (Kusari)
- Jeff Mendoza (Kusari)
- Narsa Chelluri (Kusari)
- Sunny Yip (Kusari)
- Ridwan Hoq (Microsoft)
- Alex Feng (Microsoft)
- Tim Miller (Kusari)
- Marco Rizzi (Red Hat)
- Arnav Joshi (Akami)
- Parth Patel (Kusari)
- Michael Lieberman (Kusari)
- Soham Arora (Purdue)
- Hari Kunduru (ARA)

Agenda:
- Record the meeting!
- Introductions and welcome members!
    - Ben just joined Kusari as the Open Source community lead
        - Welcome Ben!
- Announce new community promos (mdeicas)
    - Congrats to Marco D, Dejan, and Marco R!!
- Guacanalyze (soham)
    - Command addition to guacone
    - Unified tree diff between two sboms
    - Union as well as intersect
    - Demo: guacone analyze diff –uri –sboms=<sbom1>,<sbom2>
    - Differences are shown
    - Code is in PR currently: https://github.com/guacsec/guac/pull/1809
- V0.6.0 Release and blogpost (Jeff)
    - Support for ENT (Postgres) and KeyValue (inmem)
    - https://guac.sh/blogs/
    - https://github.com/guacsec/guac?tab=readme-ov-file#graphql-backends
    - https://github.com/guacsec/guac/releases/tag/v0.6.0
- New contributors recognition

        - https://github.com/guacsec/guac/pulls?q=is%3Apr+author%3Arakshitgondwal
        - https://github.com/guacsec/guac/pulls/Yaxhveer
        - https://github.com/guacsec/guac/pulls?q=is%3Apr+author%3Anchelluri+is%3Aclosed (Narsa)
        - https://github.com/guacsec/guac/pull/1779 (ribby bibby)
- Proposal for IsRunning nodes (Alex and Ridwan)
    - Usecase - you have log4j running, where is it?
    - Inventory where a vuln is running is a hard problem
    - Need to have more discussion about what the IsRunning node consist of
    - Will this be complimentary to IsDeployed?
    - What about shadow IT? A deployment occurs without following the proper procedure
    - The discrepancy between what is running and what is not?
        - One cause for this could be the `isRunning` may not be up to date with the attestation
- [Mike] Update to meetings
    - Now that GUAC is growing, should we meet more frequently for working group meetings?
    - Ben suggests no, since video meetings can be exclusive. Let's focus on async conversation in Slack and GitHub until we reach a point where we consistently can't cover the full agenda in meetings
- Pick facilitator for next time June 20th
    - It's Ben!
- Upcoming events
    - GUAC Time office hours: 24 May at 1300 UTC
    - OpenSSF Tech Talk: 6 June at 1700 UTC
    - CNCF Live: 11 June at 1600 UTC

Apr 25, 2024 : Community Meeting

Attendees

- Mike Lieberman (Kusari)
- Parth Patel (Kusari)
- Alex Feng (Microsoft)
- Brandon Lum (Google)
- Marco Deicas (Google)
- Narsa Chelluri (Kusari)
- Tim Miller (Kusari)
- Jeff Mendoza (Kusari)
- Arnav Joshi (Akamai)
- Casey Fahey (NetGoalie)
- Ridwan Hoq (Microsoft)
- Yotam Perkal (Rezilion)

- Brandon Whitfield (Kusari)
- Sunny Yip (Kusari)
- Ed Snible (IBM)
- Nathan Naveen (Kusari)
-

Agenda:

- Record the meeting!
- Introductions and welcome members!
    - Arnav here as an observer
        - Welcome Arnav!!
    - Yotam - research for startup in israel called Rezilion, tricky time for meeting
        - Welcome Yotam!!
- [Brandon] SBOMs and SLSA talk (from Kubecon)
    - Lessons Learned from Generating 100M SBOMs: Google's Approach to…
    - https://static.sched.com/hosted_files/kccnceu2024/1c/KubeCon%20EU%2024_%20Lessons%20Learned%20from%20Generating%20100m%20SBOMs%20%281%29.pdf
    - Questions on intoto attestations passed alongside sboms to add additional information
- [Parth] Fully functionality via ENT(running the guac demos)
    - Ent/Postgres is complete
    - About ready to do a release as fully supported
    - Demo of docs examples all working on ent
- [Parth] Pagination Demo for ENT and InMem
    - Queries return a "list" object that contains objects with "cursor" and "node"
    - Pageinfo object will have end cursor and next page bool
    - SBOMS > 50MB cause problems with postgres, but GUAC will handle it
    - Total count is number of all nodes that meet the filter
    - Are any queries particularly slow?
        - SBOMs are large, but not otherwise
    - List queries are being created separately to not break current integrations
        - When all list queries are done, we will break and change the api and replace the current queries with the paginated ones
- [Marco] Transitive dependencies endpoint demo
    - Added to REST api to traverse graph and return all transitive deps of a given package
    - Demo:
        - run graphql and rest api
        - Ingest some sboms - sandwich
        - Get /query/dependencies endpoint - give purl query param
        - Get the components
        - Bread has its own sbom - ingest that
        - Contains flour and nuts, these were not shown in original query
        - Now run original, and see nuts
        - Can also search by digest instead of purl
        - linkCondition specifies what relationships to observe between nouns

        - Name to assume packages with same name are equal
        - Digest to only search if artifact digests are the same
    - Would it make sense to try both name and digest traversals at the same time?
        - Depends on way hassbom is attached to pkg or artifact
        - May be tricky
    - Does spdx provide digest for top-level package being described?
        - Syft is not filling this out - all zeros - https://github.com/anchore/syft/issues/1256
        - New minimal elements may? Require this
        - We do need this data
        - Currently hassbom is only being attached to package, even if we have digest for subject
        -

Mar 28, 2024 : Community Meeting

Attendees

- Parth Patel (Kusari)
- Mike Lieberman (Kusari)
- Jeff Mendoza (Kusari)
- Tim Miller (Kusari)
- Marco Deicas (Google)
- Dejan Bosanac (Red Hat)
- Nathan Naveen (Kusari)
- Marco Rizzi (Red Hat)
- Ridwan Hoq (Microsoft)
- Alex Feng (Microsoft)
- Casey Fahey (NetGoalie)
- Yotam Perkal (Rezilion)

Agenda:

- Record the meeting!
- Introductions and welcome members!
    - Narsa - new engineer at Kusari
    - Yotam - joining from Rezilion
    - Nick - From OSI and ClearlyDefined
    - Casey Fahey @ NetGoalie, long time listener first time caller, I am a dev and consultant in New York City
    - Welcome all !!
- [Parth] Rolling community promotion recognitions
    - Contributor ladder: https://github.com/guacsec/guac/blob/main/CONTRIBUTING.md#contributor-ladder
    - Dejan Bosanac (https://github.com/dejanb) +reviewer:ingestion
        - SPDX and CDX parser additions [1,2,3,4]
        - Fix: s3 collector [1]
        - TLS for servers [1,2]

    - Marco Rizzi (https://github.com/mrizzi), +owner:backend
        - Foundational in creation and development of the Ent backend! (https://github.com/guacsec/guac/pulls?q=is%3Apr+author%3Amrizzi+is%3Aclosed)
- [Parth] Ent optimization demo
    - Started at 10min for ingestion of “guac-data/docs”
    - Now at 29 seconds
- [Parth] Discussion and feedback on proposal for focusing on backends
    - GraphQL interface has an abstraction to work with multiple backends
        - Ex: neo4j/opencypher, gremlin, etc.
    - Looking to focus on KV and Ent backends
        - Keyvalue + inmemory storage
        - Ent + Postgres
    - Discuss mechanics of other backends - move to other repositories, separate ownership, etc.
        - Open an issue to gather feedback
        - Could you BYO Go package in a separate repo?
- [Parth/Dejan] OPA Gatekeeper / GUAC Demo (from Kubecon)
    - Current location: https://github.com/dejanb/guac-provider
    - Planning to move to GUAC org, need some changes in upstream GUAC first
    - Some work needed to make it more generic
    - Can this policy-as-code pattern be used outside k8s? Ex: on package download
        - GUAC can be used as a source for these types of policy decisions
        - Depend on how the tool is able to ingest this information
        - OPA outside of gatekeeper? Are there other enforcement mechanisms that others are aware of?
        - Kyverno is another option for k8s
        - Some interest in an Identity Aware Proxy use case - not sure which exact proxy
        - OPA is general purpose, all we need for this implementation is the image digest, could be used as an input to other systems
- Opens
- IsDeployed discussion https://github.com/guacsec/guac/issues/1777
    - Overall, do we feel that this is in the scope of GUAC?
    - Mike: yes in the scope of area. Folks want to know “where is that deployed” in supply chain. Is this something that goes in GUAC or is something where GUAC is compared to a known state.
        - If it does belong in the graph, how granular does it go. GUAC doesn’t become a “monitoring system”
    - Do want to explore this space and figure out where we land
    - Look into other tools as well (OpenClarity)
    - Tim: Biggest request at KubeCon EU - need to know “what is running”
        - Need to sort out how to answer this question, not sure if it is in graph or now
    - Mike: ran a script of osquery to query against GUAC,

- Jeff: “HasSBOM” can represent source, build, or deploy currency. Could be that or a new node. The node should be an “attestation” that X was deployed by foo at this time
- Ridwan: Also would want an “X was un deployed” as well with timestamp
- Parth: Also inToto attestations can be used for deployment

Feb 15, 2024 : Community Meeting

Attendees

- Parth Patel (Kusari)
- Brandon Lum (Google)
- Sunny Yip (Kusari)
- Michael Lieberman (Kusari)
- Marco Deicas (Google)
- Jeff Mendoza (Kusari)
- Nathan Naveen (Kusari)
- Mike Lieberman (Kusari)
- Alex Feng (Microsoft)
- Kanchan Dhamane(Guidewire)
- Marco Rizzi (Red Hat)

Agenda:

- Record the meeting! ✅
- Introductions and welcome members!
  - Alex - Microsoft, on Azure container registry team focused on container supply chain efforts
  - Kanchan Dhamane, Guidewire - work on project related to security supply chain
  - Arvind Singharpuria - part of ortellius?, came to contribute to the community
- [Parth] Flexibility of blob store and pubsub
  - Demo use of S3 and SQS
  - https://github.com/guacsec/guac/pull/1664
  -
- [Nathan] What is your “most critical dependency”?
  - [Nathan] Won’t be able to actually demo it because of a couple of technical difficulties.
  - https://github.com/guacsec/guac/pull/1705 - contains the design doc
  - Output:
    - the number of dependents: the package name
    - ----------
    - 41 deb_debian_base-files
    - 35 deb_debian_tzdata
    - 32 golang_k8s.io/release/images/build_go-runner
    - 32 deb_debian_netbase
    - 17 deb_debian_libssl1.1
    - 17 deb_debian_grep
    - 17 deb_debian_dash

        - 15 deb_debian_adduser
- [Marco Deicas] Google Scorecard Dashboard via GUAC
- [Brandon] Recursive search for query known
    - https://github.com/guacsec/guac/pull/1692
- [Jeff] Backend Test suite
    - https://github.com/guacsec/guac/blob/main/internal/testing/backend/README.md
    -
-
- Open Discussion

Jan 18, 2024 : Community Meeting

Attendees

- Parth Patel (Kusari)
- Brandon Lum (Google)
- Justin Cappos (NYU)
- Jon Zeolla (Seiso)
- Marco Deicas (Google)
- Dejan Bosanac (Red Hat)
- Marco Rizzi (Red Hat)
- Max Dessì (Red Hat)
- Ridwan Hoq (Microsoft)
- Abhishek Reddypalle (Purdue University)
- Jeff Mendoza (Kusari)
- Ed Snible (IBM) failed to join using an invalid/old link (it's a new openssf meeting link - found in https://guac.sh/community/ - meeting just ended)

Agenda:

- Record the meeting! ✅
- Introductions and welcome members!
    - Ed - freelancer engineer, been playing around with GUAC
    -
- LFX mentorship https://mentorship.lfx.linuxfoundation.org/project/88e6bd6c-abb1-4910-823a-8f0420fbca90
    - Useful for new to open source or the field
    - Contributions could be anything - docs, code, etc.
- [marco deicas] Quick overview of REST API - https://github.com/guacsec/guac/issues/1544
    - Going to use code generator for server stubs oapicodegen
    - Schema would be OpenAPI (previously known as swagger)
    -
- [Parth] Custom directives for GraphQL
    - PURL will show up now when searching for packages
        - Answer questions on what is the PURL

        - Contains/Starts with
            - Is there better way to query graphQL like a submatch like contains or start with
- [Parth] Update to Vulnerability CLI - SBOM URI
- GUAC 0.4.0 release! All these above are included!
- PURL check update (https://github.com/guacsec/guac/issues/1545)
- Requirements for v1.0 release - open conversation about https://github.com/guacsec/guac/issues/1436
    - Persistent, can handle large inputs and well tested
    - Having issues with utilizing pubsub with document blobs since they all have limited size, using gocloud library to abstract it away for blob store.
        - Folks have asked can we use other pubsub besides NATS like kafka (gocloud can allow this flexibility)
    - Doing something akin to case study with an end user as an acceptable criteria for 1.0
    - Authn/Authz on 1.0?
        - Authz is complicated for graphql
        - A lot of it are paid solutions
        - REST API not tied to 1.0, but likely done before 1.0
    - Raising the bar on API changes as we approach 1.0
- [Mike] - Very quick update on upcoming GUAC webinar
- We provided some feedback on CISA software identifier RFC (https://www.regulations.gov/comment/CISA-2023-0026-0011)

Nov 16, 2023 : Community Meeting

Attendees

- Parth Patel (Kusari)
- Brandon Lum (Google)
- Mike Lieberman (Kusari)
- Abhishek Reddypalle (Purdue)
- Jeff Mendoza (Kusari)
- Dejan Bosanac (Red Hat)
- Ridwan Hoq (Microsoft)
- Nathan Naveen (Kusari)
- Tim Miller (Kusari)
- Sunny Yip (Kusari)
- Marco Deicas (Google)
- Kevin Conner (Independent)
- Santiago Torres-Arias (Purdue)
- Dana Wang (OpenSSF)
- Eman Abu Ishgair (Purdue)
- Marco Rizzi (Red Hat)
- Phil Cattanach (Red Hat)
- Max Dessì (Red Hat)

Agenda:

- Record the meeting! ✅
- Introductions and welcome members!
    - Abhishek Reddypalle (Purdue) - student
    - Dana Wang (OpenSSF) - Architect for OpenSSF
    - Jennifer (Kusari)
- Show off Key/Value (redis, TiKV) (Jeff)
    - GUAC has default in-mem backend using internal golang map structs, etc.
    - Allows for plugin key/value stores
    - Demo with redis and TiKV
    - 20 lines of code to add other key/value stores
    - Try etcd next
    - Try performance query testing
- Experimental REST API demo (Nathan)
    - https://github.com/guacsec/guac/issues/1326
    - Feedback on queries, inputs and outputs
- GUAC community feedback on use cases (SBOM, metadata attachment, most critical/actionable dependencies type thing) (Brandon and Parth)
    - https://github.com/guacsec/guac/issues/1483
    - https://github.com/guacsec/guac/issues/1505
    - https://github.com/guacsec/guac/issues/1508
    - Dejan
        - here is the sbom, give me all vulns
        - Here is vuln, what packages are affected
        - Push upstream in a few months
    - Dana
        - MVP security standards openssf is developing
- Identifier problems (RFI) discussion
    - Problem statement - https://www.federalregister.gov/documents/2023/10/26/2023-23668/request-for-comment-on-software-identification-ecosystem-option-analysis
    - GUAC RFI working doc link - https://docs.google.com/document/d/1h9Ko-myqAfQc-pWlvYay0CENIDhfFHVZdxLY74Jdw9w/edit#heading=h.2l3uzjuzf7tn
- Open Discussion

Oct 19, 2023 : Community Meeting

Attendees

- Parth Patel (Kusari)
- Nathan Naveen (Kusari)
- Kevin Conner (independent)
- Shafee Ahmed (Kusari)
- Mike Lieberman (Kusari)
- Marco Rizzi (Red Hat)
- Phil Cattanach (Red Hat)
- Massimiliano (Max) Dessì (Red Hat)

- Tim Miller (Kusari)
- Naveen Srinivasan
- Jeff Mendoza (Kusari)
- Sunny Yip (Kusari)
- John Kjell (TestifySec)
- Marcela Melara (Intel)

Agenda:

- Record the meeting! ✅
- Introductions and welcome members!
    - Marcela (intel) - research
- OpenSSF Incubation (Mike)
    - OpenSSF Zoom, new community meeting notes
    - Paperwork still needs to be signed
    - Neutral governance
    - Funding and support from the OpenSSF
    - Working with other projects within the OpenSSF
- Inmem Key/Value store changes/demo (Jeff)
    - Can we use that implementation and store that on disk
    - Issue: https://github.com/guacsec/guac/issues/1406
    - Interface implementation - swappable with other
    - Question: do keys not need pagination?
        - Yes, that will be added.
    - Testing with Redis, bblot
    - A disadvantage is that this is not a full-fledged database. We do not get the benefits of querying and traversal..etc.
- Updates on Ent (Marco)
    - All the queries and ingestion for software trie and evidence trie are implemented!
    - Path, nodes, and neighbors query WIP
    - Optimization phase after that
- Updates on Arango (Parth)
- Open Discussion

Sep 21, 2023 : Community Meeting

Attendees

- Parth Patel (Kusari)
- Brandon Lum (Google)
- Dejan Bosanac (Red Hat)
- John Kjell (TestifySec)
- Jeff Mendoza (Kusari)
- Shafee Ahmed (Kusari)
- Nathan Naveen (Kusari)
- Tim Miller (Kusari)
- (Max) Massimiliano Dessì (Red Hat)

- Marco Rizzi (Red Hat)
- Ridwan Hoq (Microsoft)
- Toddy (Microsoft)
- Jeremy Rickard (Microsoft)
- Sajay Antony
- Marco Deicas (Google)

Agenda:

- Record the meeting! ✅
- Introductions and welcome members!
    - Andre, works with Ridwan on container registry
    - Marco D, works with Brandon on GUAC
    - Nathan, intern at Kusari, working on GUAC
    - Toddy, works with Ridwan and Andre on Azure container registry
    - Max, works with Dejan and Marco R
- Guac-ai-mole demo!!
    - https://github.com/sozercan/guac-ai-mole
    - UI to query GraphQL api using LLM
    - Sample questions: “What are the deps of x?”
    - “Which images contain vuln id x?”
    - Can shell out to kubectl to see what is running in a cluster, and cross reference with guac output
    - Put whole GQL schema from GUAC into LLM
    - Reference the runtime info from call out to a kubectl command to the cluster
    -
- OCI registry collector demo
    - Today GUAC support colelcting from single OCI repo, however, only support “registry fallback” artifacts
    - Should look towards using OCI referrer artifacts to allow an artifact to be attached to another one.
    - New command “guacone collect registry” Ingests sboms across the entire registry
    - Dev feedback: Need to read the makefile to get up and running locally
        - Have a contributor guide
        - Guide to dev-loop, what to have running
        - Postgres was running locally, but not being used
        - What is the difference between guacollect and guacone collect
        -
- OpenVex demo (Nathan/Parth)
    -
- Recognizing contributors
    - Marco R
    - Soham
    - https://github.com/guacsec/guac/blob/main/CONTRIBUTING.md#contributor-ladder
- CDX VEX implementation question (if time)
    - Currently “CertifyVEX” points to a “package-version”

        - CDX VEX uses version ranges, may not be a specific “package-version” in GUAC to point to
        - We can change “CertifyVEX” to also point to a “package-name” optionally
        - It will need to include a “VersionRange”.
        - What to do about multiple “VersionRange”s, a list? Or multiple “CertifyVEX” nodes?
        - Clients will need to map version range in CertifyVEX to specific versions of a package
- Base images - Dejan (if time)
    - Anyone have any experience providing container images for a project with multiple base images?
    - alpine/ubi/wolfi, etc.
- Should we have snapshots between releases?
    - What about patch releases?
    - Should have something that is lower effort - not guaranteed to be stable
    - Have nightly now
    - Jeff to create issue
- Understanding plans to enforce authenticity of calls like certify. [sajay]
    - API/CLI can “certify” a package, what is the authenticity?
    - https://github.com/guacsec/guac/issues/75
    -

Aug 17, 2023 : Community Meeting

Attendees

- Parth Patel (Kusari)
- Brandon Lum (Google)
- Jon Zeolla (Seiso)
- Mike Lieberman (Kusari)
- Dejan Bosanac (Red Hat)
- Jeff Mendoza (Kusari)
- Sunny Yip (Kusari)
- Noah Spahn (Open University)
- Tom Hennen (Google)
- Shripad Nadgowda (Intel)
- Bob McWhirter (Red Hat)

Agenda:

- Record the meeting! ✅
- Introductions and welcome members!
    - Noah - security researcher with open university, work at research lab at UCSB, has been looking at GUAC for a bit
    - Ivan Vanderbyl - working on ent backend for postgres SQL
    - Tom - TL for couple SSCI things in Google
- Announce new maintainer: Jeff Mendoza (Kusari)
    - Info on legal information design: https://github.com/guacsec/guac/issues/1014
- Updates of graphQL API

        - Vulnerability changes (Parth)
            - https://github.com/guacsec/guac/pull/1147
        - WIP - Quick update on plans to only return IDs for ingestion (Parth)
            - https://github.com/guacsec/guac/issues/1116
        - WIP - Quick update on plans to add vulnerability metadata/score
            - https://github.com/guacsec/guac/issues/1072
        - isDependency changes (Brandon)
            - https://github.com/guacsec/guac/pull/1125
- Show Patch Planning demo (Brandon)
- Visualizer updates (Shafee)
- Storing signatures (Bob/Dejan)
    - https://github.com/guacsec/guac/issues/75
    - Like collectors/certifiers for documents
    - Want to store signature nodes inside GUAC as well
    - https://github.com/guacsec/guac/blob/main/pkg/assembler/graphql/schema/metadata.graphql
- Compressed files support (Dejan)
    - S3 collector in rust gets file from s3 and puts it in NATS
    - Nice to have interface to ingestor to be raw bytes since other languages have
    - Add processor for compressed

Jul 20, 2023 : Community Meeting

Attendees
- Mike Lieberman (Kusari)
- Tim Miller (Kusari)
- Dan Perry (Google)
- Jesse White (independent)
- Will Armiros (Protect AI)
- Lindsay Newton (VMware)
- Dejan Bosanac (Red Hat)
- Parth Patel (Kusari)
- Jeff Mendoza (Kusari)
- Sunny Yip (Kusari)
- Rebecca Metzman (Google)
- Shripad Nadgowda (Intel)
- Phil Cattanach (Red Hat)
- Marco Rizzi (Red Hat)
- Brandon Lum (Google)
- Mihai Maruseac (Google)

Agenda:
- Record the meeting! ✅
- Introductions and welcome members!
    - Marco Rizzi from Red Hat
    - Phil Cattanach from Red Hat

    - Lindsay Newton from VMware
    - Amim Knabben from VMware
- Quick update on OpenSSF contribution
- Ent backend presentation (ivan)
    - Using Ent (https://entgo.io/docs/traversals/)
    - Interest in GUAC and don't quite want to support additional tech so implementing it through ent on postgres
    - Running compose on the feature branch that sets up postgres
    - Running queries through graphQL
    - Upserting package trees runs in a transaction - have some ideas around doing bulk upserts on the DB
    - Ent will behind the scenes generate the files
    - Ent will also do the schema stuff for you
    - Feedback/Questions
        - Awesome stuff!
        - Put questions in GUAC slack
- Friends of GUAC poll (Brandon)
    - Friends of GUAC markdown on main repo
    - Guacsec org repos with labels:
        - Different labels
            - Community (Maintained by community)
            - Supported (Maintained by community + GUAC maintainers)
        - Questions:
            - Individual repo vs monorepo with directories
                - graphQL consistency will help with monorepos if there are issues vs repo management
    - Given a lot of GUAC right now is GraphQL API, suggestions on making API queries easier
    - Submodule may be a good way
    - Brandon to create MD file with process
- ArangoDB / Neptune Updates (Parth)
    - Ingest SBOMs, and potentially docs
    - Talk through changes / improvements from backend to get it faster
    - Added bulk ingestion - reduce round trips
    - Search function
        - Higher level CLI functions
- Tilt integration and Gremlin/Tinkerpop backend work (Jesse White) (if he can make it to the meeting)
    - Would be nice to have a conformance test suite
- Office hours time (Dejan, if there's time)
    - Hard for some EMEA timezones to get to
    - Alternating office hours (Brandon will take this up)
- Large files support (Dejan, if there's time)
    - Brandon: Is this related to https://github.com/guacsec/guac/issues/731?
- Brainstorm discussion on higher level CLI (https://github.com/guacsec/guac/issues/1044)
    - Use-cases: https://github.com/guacsec/guac/blob/main/use-cases.md
- Visualizer (shaffee, if there's time)

Jun 15, 2023 Community Meeting
Recording: GUAC Community Meeting 2023-06-15

Attendees:

- Jeff Mendoza (Kusari)
- Dan Perry (Google)
- Tim Miller (Kusari)
- Mike Lieberman (Kusari)
- John Kjell (VMware)
- Dejan Bosanac (Red Hat)
- Parth Patel (Kusari)
- Marcela Melara (Intel)
- John Andersen (Intel)
- Nick Vidal (ClearlyDefined, Open Source Initiative)
- Jacques Chester (independent)
- Sunny Yip (Kusari)
- Jesse White (independent)
-

Apologies:

-

Agenda:

- Record the meeting! ✅
- Introductions and welcome members!
    - Nick Vidal - ClearlyDefined community manager
        - Part of OSI, looking to see how can work together
    - Dan Perry - looking to contribute, docs mostly
    - John Andersen - looking to engage, works with Marcela
    -
- General Project Updates
    - [Mike Lieberman] - Submission to OpenSSF
- ArangoDB work [Parth]
- Ent / SQL DB work [Jeff]
- Product identifiers question [Dejan]
- S3 collector update [Dejan]
- Docs - where can i support to get started?
    - (Tim M) - The doc site is here if you'd like to take a look: https://docs.guac.sh/
- How do I get events on GUAC
    - Tightly coupled, part of GUAC: collector-subscriber interface, current certifiers and collectors use this (OSV, deps.dev, etc.)
    - Loosely coupled: not yet, looking to design and figure out how to integrate with "cloud event" type things, cdevents, etc. https://github.com/guacsec/guac/issues/460
- Any community experts in graph databases, or similar technologies?

-

May 26, 2023
GUAC Office Hours

May 18, 2023 :Community Meeting
Recording: GUAC Community Meeting 2023-05-18
Attendees:

- Mihai Maruseac (Google)
- Rebecca Metzman (Google)
- Mike Lieberman (Kusari)
- Jacques Chester (Independent)
- Tim Miller (Kusari)
- Will Armiros (Protect AI)
- Sunny Yip (Kusari)
- Shafee Ahmed (Kusari)
- Dejan Bosanac (Red Hat)
- John Kjell (VMware)
- Jeff Mendoza (Kusari)
- Jon Zeolla (Seiso)
- Ed Snible (IBM)
- Kevin Conner (Independent)
- Justin Perez (Microsoft)
- Parth Patel (Kusari)
- Ashmita (Opsmx)
- Verónica López (PlanetScale / Kubernetes)
- Raj Krishnamurthy (ComplianceCow)
- Anjali Batra (OpsMx)
- Brandon Lum (Google)
- Shripad Nadgowda (Intel)
- Satya Kiran (OpsMx)

Apologies:

-

Agenda:

- Record the meeting! ✅
- Introductions and welcome members!
    - Will Armiros - Heard about us, looking to learn more
    - Justin - Microsoft
    - Rebecca - Intern at Google
    - Anjali - OpsMx
- General Project Updates
    - GUAC Beta coming up!
- Contributor ladder (mihai)

- Microsoft component detection presentation (Justin Perez)
    - https://github.com/microsoft/component-detection
- Guac Rust library and Seedwing integration (dejan)
    - https://github.com/de_janb/guac-rs
    - https://docs.seedwing.io/seedwing/index.html
    - https://docs.seedwing.io/seedwing/policies/guac/index.html
- Understanding the guac repo and the new documentation (parth) - guac.sh
- Discussion on Persistent database (everyone)
    - https://github.com/guacsec/guac/issues/851
    - Some suggestions
        - Apache Age
        - SQLite / Filesystem
        - Cloud spanner
        - https://duckdb.org/2021/10/29/duckdb-wasm.html
        - Parquet to help run on top of database / inmem for failures/easy persistence
    - Have a stress test suite so we can benchmark against different implementations
    - Looking at feature sets as well - like bitemporal features
    - It would be good to have the public instance be able to scale, which will make it usable for a lot of users to federate against (will lower the cost of internal use by federating to the public instance)
    - AI: Create a doc for discussion (Brandon to create)
    -
- GUAC Office hours (GUAC TiME) - 2:00-2:30 pm Fridays bi-weekly starting on 26 May
- Open chat (add items here if you want)
    -

Apr 20, 2023 :Community Meeting

Attendees:

- Parth Patel (Kusari)
- Mihai Maruseac (Google)
- Brandon Lum (Google)
- Jon Zeolla (Seiso)
- Tim Miller (Kusari)
- Dejan Bosanac (Red Hat)
- Justin Abrahms (hire me?)
- Dan Perry (Google)
- Sunny Yip (Kusari)
- Jeff Mendoza (Kusari)
- Marcela Melara (Intel)
- Ed Snible (IBM)
- Shripad (Intel)

- Yotam Perkal (Rezilion)

Apologies:
- Jacques Chester (Shopify)

Agenda:
- Record the meeting! ✅
- Introductions and welcome members!
    -
- General Project Updates
    - GUAC Beta coming up!
    -
- Demo demo demo
    - GraphQL API demo
    - Compose tutorial
    - Query CLI vuln demo
    - Deps.dev collector demo
    - Bad Packages Demo
- Contributor ladder (mihai)
- Open chat (add items here if you want)
    - sbom-scorecard (abrahms)
        - Create collector and ingestor
    - Diff between collector vs ingestor
        - a collector takes documents from various sources and brings them to GUAC - these are just document blobs
        - The ingestor is in charge or parsing and understanding them and converting them to the guac datamodel / ontology.
- https://security.googleblog.com/2023/04/supply-chain-security-for-go-part-1.html?m=1
    - New metadata (affected functions) on vulns with Go. Can you query Guac to understand / remove false postives
    - https://pkg.go.dev/golang.org/x/vuln/vulncheck

16 Mar 2023 :Community Meeting
Recording: GUAC Community Meeting 2023 03 16
Attendees:
- Brandon Lum (Google)
- Jon Zeolla (Seiso)
- Nathan Naveen (High School)
- Sunny Yip (Kusari)
- Tim Miller (Kusari)
- Hemil Kadakia (Yahoo)
- Dejan Bosanac (Red Hat)
- Jeff Mendoza (Kusari)
- Mihai Maruseac (Google)
- Jacques Chester (Shopify)
- Shripad Nadgowda (Intel)

- Mike Lieberman (Kusari)
- Parth Patel (Kusari)
- Rajesh Jain (Palo Alto Networks)

Agenda:

- Record the meeting! ✅
- Introductions and welcome members!
    - Jeff Mendoza, Nathan Naveen, Rajesh Jain
- General Project Updates
    - GraphQL Backend changes
        - Construction ongoing
        - Focus on inmem
    - New good first issues
        - Identifier strings
            - https://github.com/guacsec/guac/issues/590
            - https://github.com/guacsec/guac/issues/591
    - Call for UI/UX contributors
- Scorecards Certifier Demo - by Nathan Naveen
    - https://hackmd.io/@y50F62YUQPy0CbkmYYkjeQ/r1BkJ1p1h
    -
- Open Agenda
    - Dejan to show integration into policy engine

16 Feb 2023 : Community Meeting

Recording: GUAC Community Meeting 2023-02-16

Attendees:

- Jon Zeolla (Seiso)
- Brandon Lum (Google)
- Mihai Maruseac (Google)
- Parth Patel (Kusari)
- Tim Miller (Kusari)
- Dejan Bosanac (Red Hat)
- Rob Honeybul (Snyk)
- Dan Perry (Google Cloud)
- Hemil Kadakia (Yahoo)
- Jacques Chester (Shopify)
- Verónica López (PlanetScale)
- Mike Lieberman (Kusari)
- Kevin Conner (Red Hat)
- Randall T. Vasquez (Gentoo/SKF/LF)
- Raj Krishnamurthy (ComplianceCow)
- Eman Abu Ishgair (Purdue University)
- Furkan Türkal (Trendyol)
- Leo Alvarez (Baker Tilly)

Agenda:

- Record the meeting! ✅
- Introductions and welcome members!

- Sharing workshop notes (5 mins)
    - GUAC 2023 Q1 Summit Notes - SHARED EXTERNALLY (available on README.md)
- Demo of GraphQL interface (10 mins)
    - [External] Refactoring the GUAC Assembler
    - Qualifier ontology to include semantic
    - https://github.com/guacsec/guac/pull/454 , https://github.com/guacsec/guac/pull/457, https://github.com/guacsec/guac/pull/452, https://github.com/guacsec/guac/pull/451, https://github.com/guacsec/guac/pull/447, …
      More PRs being made this week and next (WIP)

- Demo of Collectsub service (10 mins)
- Highlight SETUP.md (5 mins)
- Issues for community engagement:
    - https://github.com/guacsec/guac/issues/281
    - https://github.com/guacsec/guac/issues/443
    - https://github.com/guacsec/guac/issues/250
- Open discussion
    - Signaling containment
        - Container image container layers
        - Layers contain files
        - Also ruby gems, and the physical identity of gem file, etc.
    - System dependencies across teams, across departments and also across systems
        - From a framework/infrastructure/productivity, help internal releases, etc.
        - For legal and operational perspective
    - Policy engine a bit more focused than OPA
        - https://github.com/seedwing-io/seedwing-policy
            - Query all the attestations and use it to make policy decisions
        - https://github.com/seedwing-io/seedwing-proxy
            - Proxy between build process and package manager (Secure Ingestion)
    - GUAC as policy information point to enrich and inform to do decisioning and enforcement
    - Risk Management, similar to VEX work to make sure something is OK or not OK

12 Dec 2022 : Community Meeting

Recording: GUAC Community Meeting 2022-12-13
Attendees:

- Brandon Lum (Google)
- Mihai Maruseac (Google)
- Justin Abrahms, eBay
- Alex Goodman (Anchore)
- Theofilos Petsios (Crash Override)
- Mike Lieberman (Kusari)
- Tim Miller (Kusari)
- Jude Safo (Haiphen)
- Parth Patel (Kusari)
- Shripad Nadgowda (intel)
- Jacques Chester (Shopify)
- Fridolin "fridex" Pokorny (Datadog)
- Christopher Phillips (Anchore)
- Rewanth Tammana (Freelancer)
- Aditya Sirish (NYU)
- Rob Honeybul (Snyk)
- Randall T. Vasquez (Gentoo/Homebrew/SKF)
- Michael Scovetta (Microsoft / Alpha-Omega)
- Shafee Ahmed (Kusari)
- Stephan Pinto Spindler
- Philippe Ombredanne (package-url/VulnerableCode/ScanCode/nexB)

Agenda:

- Record the meeting!
- Introductions and welcome members!
- Recognizing contributors!
    - Cpendary
    - Nadgowdas
    - Lukehinds
    - Fridex
    - Krishnaindani
    - Fbiville
    - Desenna
    - Robh-snyk
- [brandon] Overview of GUAC, community meetings
    - Contributing, Collaboration and Philosophy
    - Community meetings (monthly)
    - Maintainer meetings (weekly)
    - Technical Discussions through issues
    - Fun stuff, chatting and memes at Slack channel
    - Looking at good first issues
- [brandon] GUAC Beta Roadmap
- [parth] OSV Certifier Demo

    - Based around Demo of https://github.com/guacsec/guac/blob/main/SETUP.md
    - With additional container image vulnerable to log4shell & text4shell
    -
- Some topics for next time:
    - Apache Jena
    - Using semantic web technologies
    - Alpha-Omega assertions project
    - sbom-scorecard (abrahms)?