gandhinagar COCON

We got the Shiny SBoM; what next?

Anant Shrivastava

Cyfinoid

Anant Shrivastava

- Chief researcher @ Cyfinoid Research
- 15+ yrs of corporate exposure
- **Speaker / Trainer:** BlackHat, c0c0n, nullcon, RootConf, RuxCon
- **Project Lead:**
  - Code Vigilant (Code Review Project)
  - Hacking Archives of India,
  - TamerPlatform (Android Security)

- (@anantshri on social platforms) https://anantshri.info

What is Software Bill of Material

- Itemized list of all the ***ingredients*** in the software
- Ingredients means mostly third-party components
  - Software name
  - Version
  - Checksum
  - License information
  - Dependencies list if possible

- SBoM's are mostly for one level depth only with other levels plugged in each other.

https://www.ntia.gov/report/2021/minimum-elements-software-bill-materials-sbom

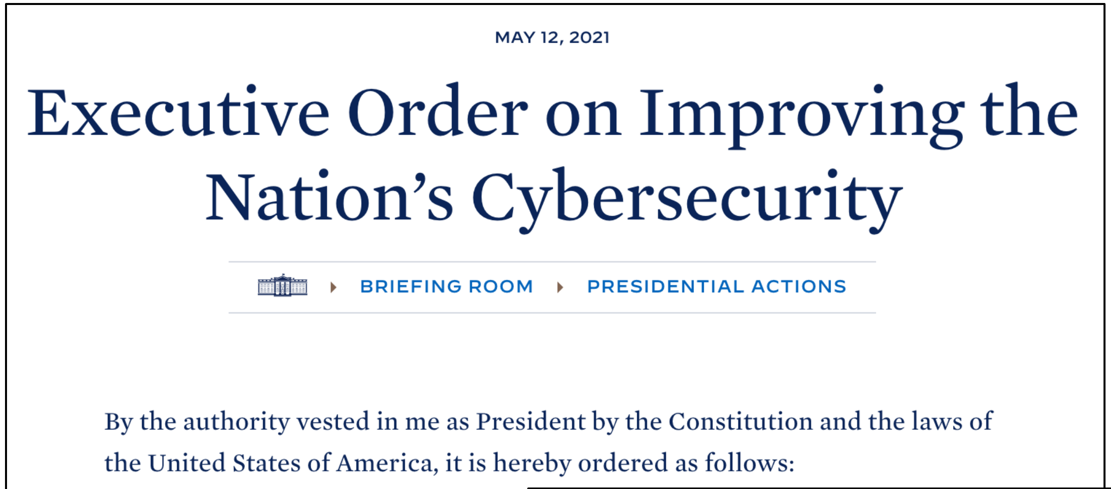
Events

Incidences

- SolarWind
- CodeCov
- Colonial Pipeline

Resultant

- EO by US President
- NIST SSDF Framework
- SLSA by google
- 2024 : Cert-in issued guidelines

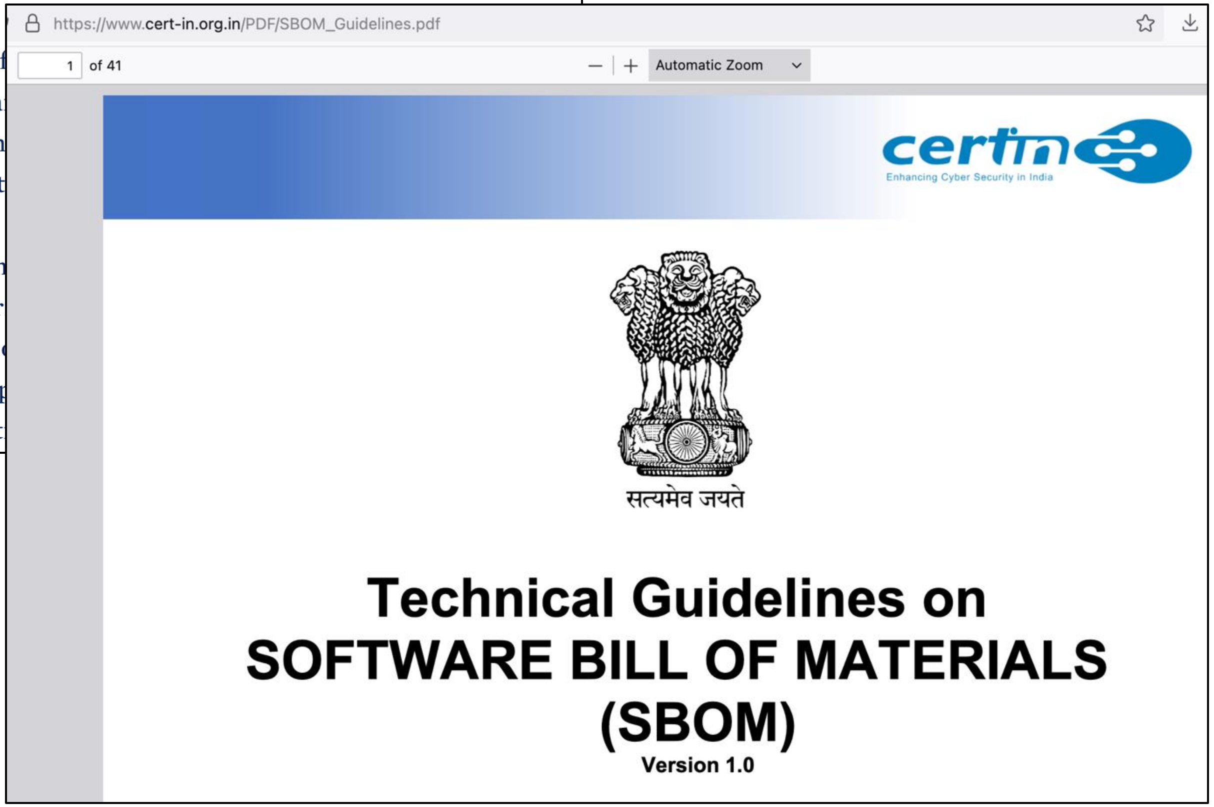


MAY 12, 2021

Executive Order on Improving the Nation's Cybersecurity

By the authority vested in me as President by the Constitution and the laws of the United States of America, it is hereby ordered as follows:

Section 1. Policy. The United States f
sophisticated malicious cyber campa
private sector, and ultimately the Am
Federal Government must improve it
against, detect, and respond to these
Government must also carefully exan
cyber incident and apply lessons lear
than government action. Protecting
requires the Federal Government to p
private sector must adapt to the cont



https://www.cert-in.org.in/PDF/SBOM_Guidelines.pdf
1
of 41
Automatic Zoom
certin
Enhancing Cyber Security in India
सत्यमेव जयते

Technical Guidelines on SOFTWARE BILL OF MATERIALS (SBOM)

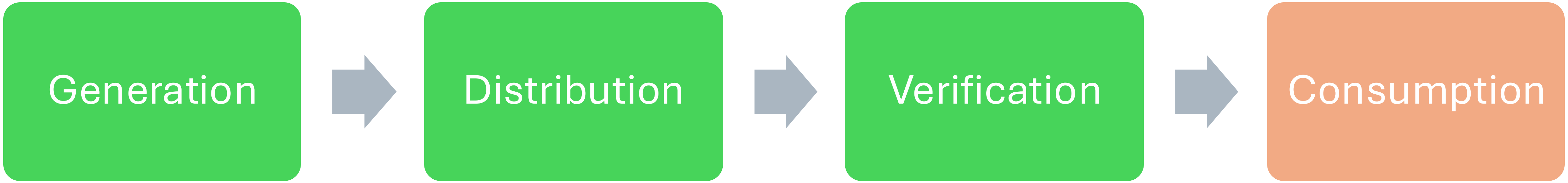
Version 1.0

Every standard starts with competition

- SPDX
  - ISO Standard
  - Github provides default export in this format
- CycloneDX
  - OWASP Supported
  - Now an ISO Standard
- SWID
  - Alternative ISO specification

https://www.ntia.gov/files/ntia/publications/sbom_formats_survey-version-2021.pdf

Where are we in the SBoM Journey



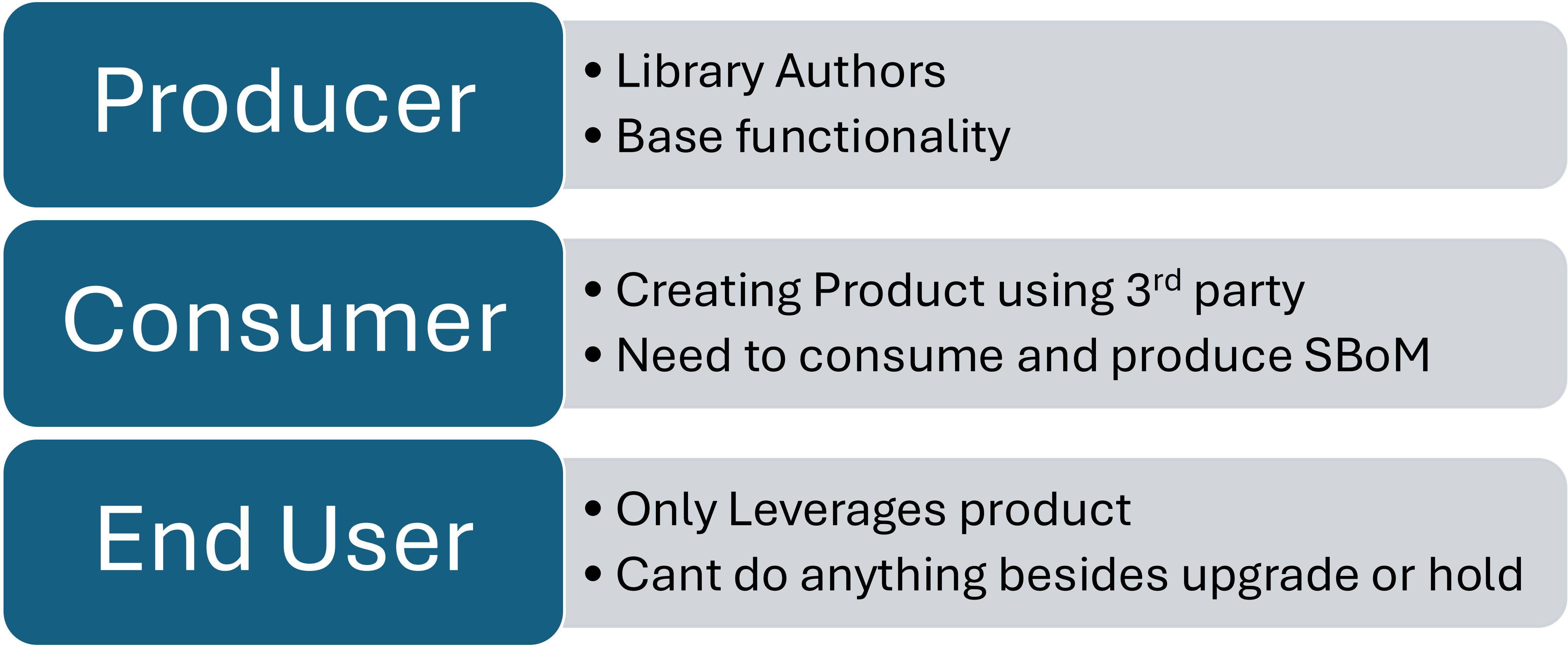
Generation

Distribution

Verification

Consumption

Users of SBoM



Producer

- Library Authors
- Base functionality

Consumer

- Creating Product using 3rd party
- Need to consume and produce SBoM

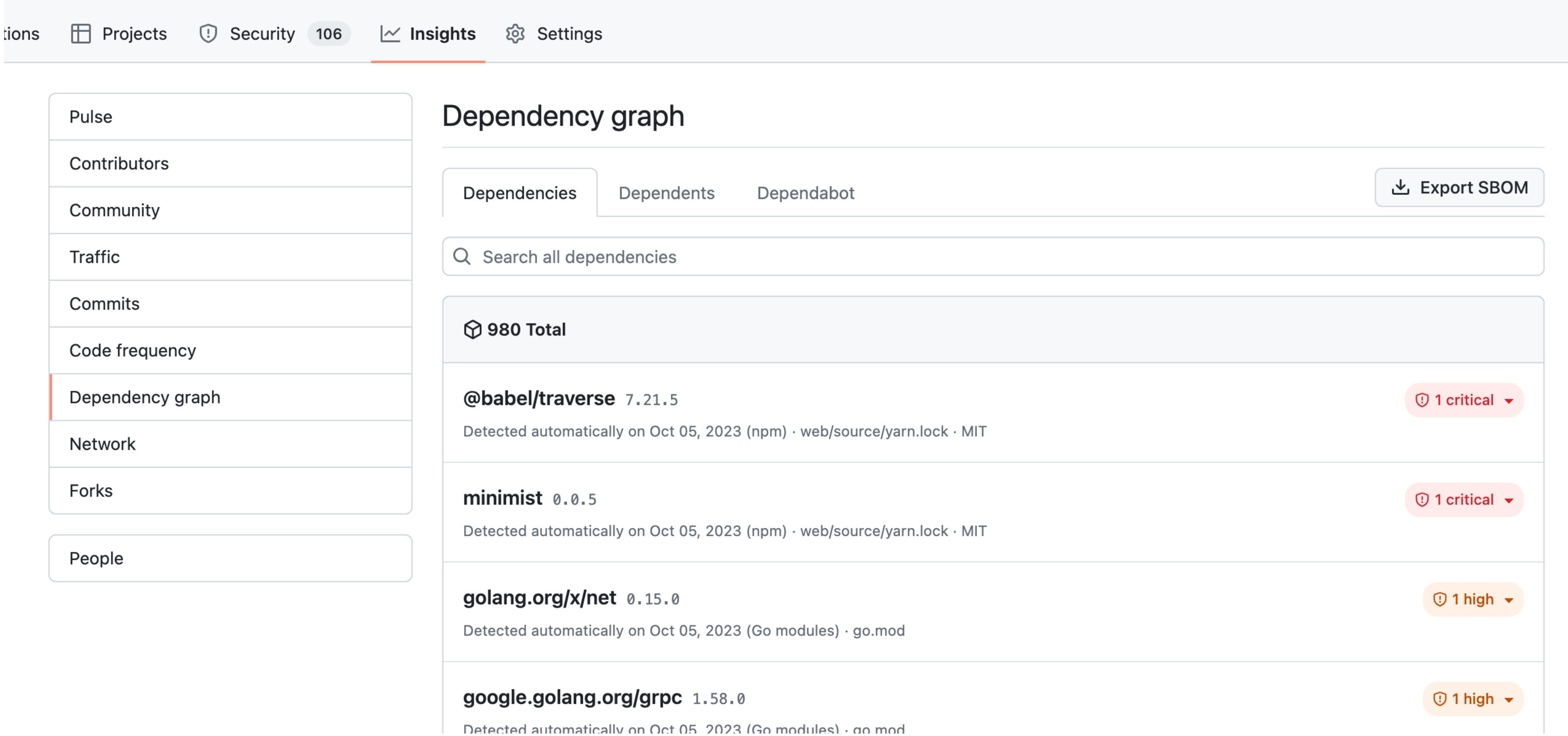
End User

- Only Leverages product
- Cant do anything besides upgrade or hold

How to create SBoM

- Github provides dependency Graph in “Insights”
- SBoM generation tools
  - Cdxgen
    - https://github.com/CycloneDX/cdxgen
  - SPDX Generator
    - https://github.com/spdx/tools
- /dev/hand if all else fails (Its XML)

GitHub Export SBOM Option



Dependency graph

980 Total

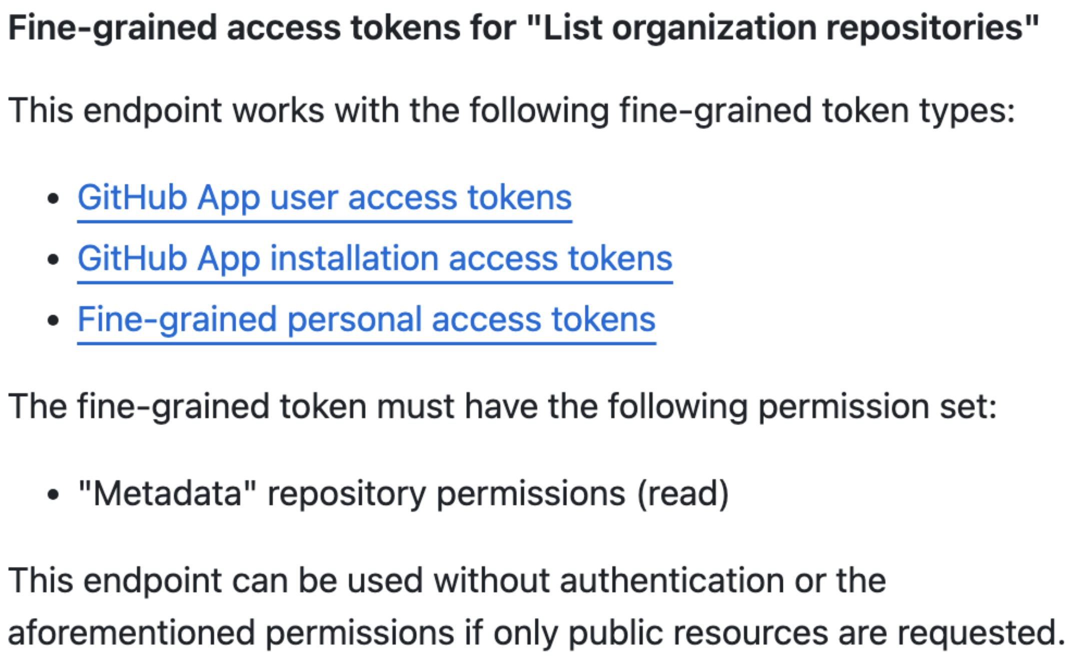
@babel/traverse 7.21.5 — 1 critical
Detected automatically on Oct 05, 2023 (npm) · web/source/yarn.lock · MIT

minimist 0.0.5 — 1 critical
Detected automatically on Oct 05, 2023 (npm) · web/source/yarn.lock · MIT

golang.org/x/net 0.15.0 — 1 high
Detected automatically on Oct 05, 2023 (Go modules) · go.mod

google.golang.org/grpc 1.58.0 — 1 high
Detected automatically on Oct 05, 2023 (Go modules) · go.mod

Github API automation



Fine-grained access tokens for "List organization repositories"

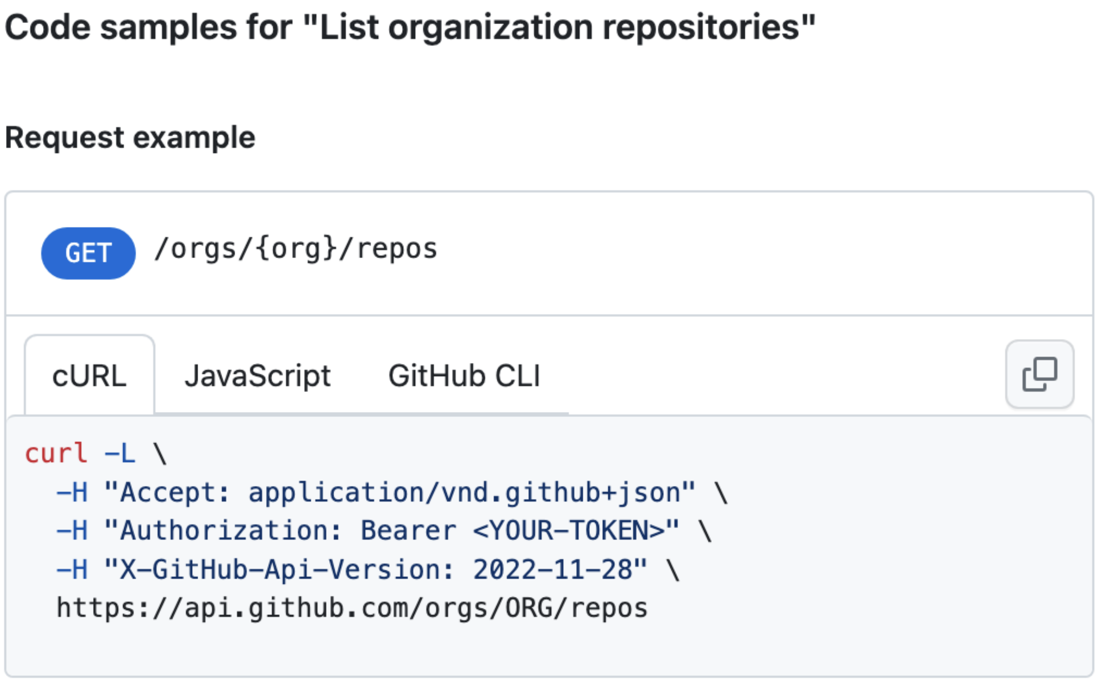
This endpoint works with the following fine-grained token types:

- GitHub App user access tokens
- GitHub App installation access tokens
- Fine-grained personal access tokens

The fine-grained token must have the following permission set:

- "Metadata" repository permissions (read)

This endpoint can be used without authentication or the aforementioned permissions if only public resources are requested.



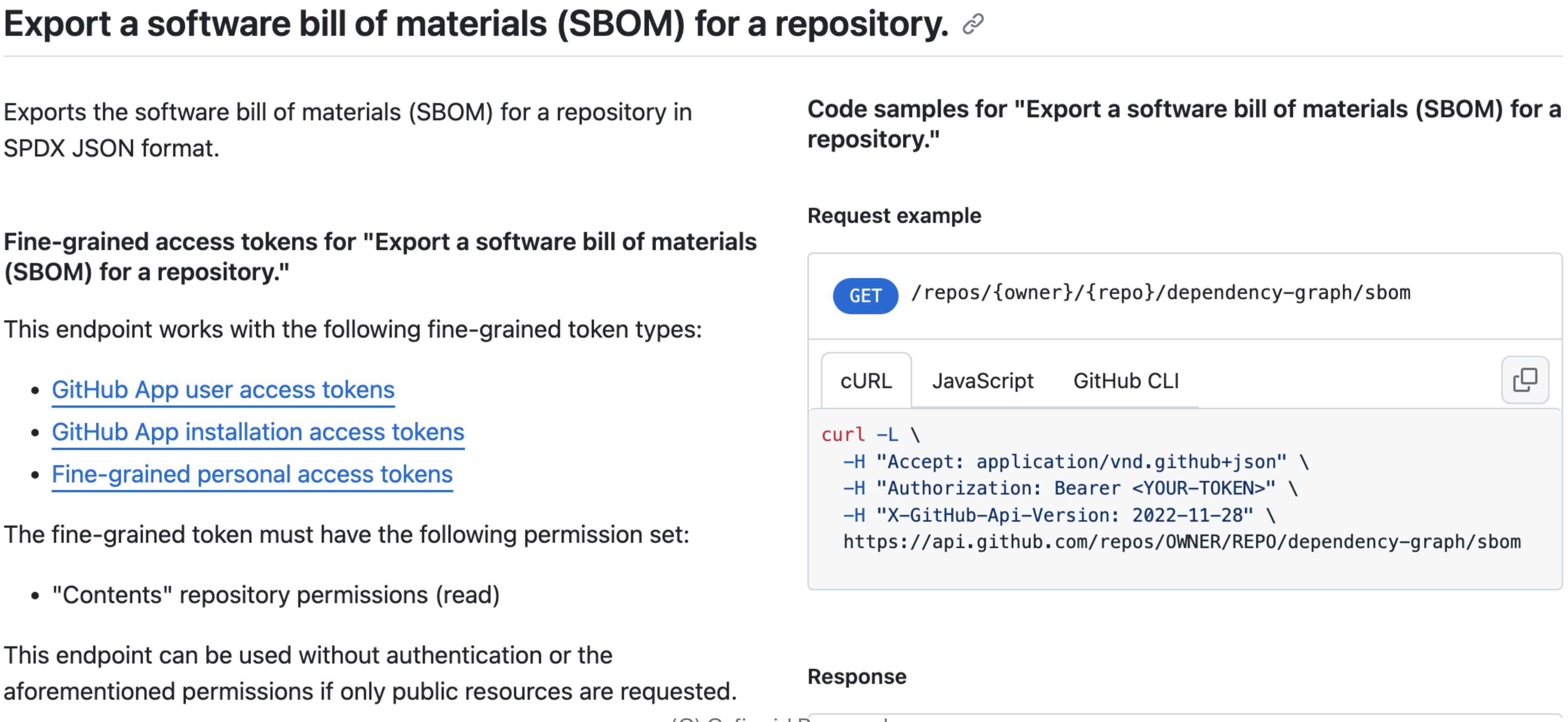
Code samples for "List organization repositories"

Request example

GET `/orgs/{org}/repos`

```
curl -L \
  -H "Accept: application/vnd.github+json" \
  -H "Authorization: Bearer <YOUR-TOKEN>" \
  -H "X-GitHub-Api-Version: 2022-11-28" \
  https://api.github.com/orgs/ORG/repos
```

Extract SBoM from Github



Export a software bill of materials (SBOM) for a repository.

Exports the software bill of materials (SBOM) for a repository in SPDX JSON format.

Fine-grained access tokens for "Export a software bill of materials (SBOM) for a repository."

This endpoint works with the following fine-grained token types:

- GitHub App user access tokens
- GitHub App installation access tokens
- Fine-grained personal access tokens

The fine-grained token must have the following permission set:

- "Contents" repository permissions (read)

This endpoint can be used without authentication or the aforementioned permissions if only public resources are requested.

Code samples for "Export a software bill of materials (SBOM) for a repository."

Request example

GET /repos/{owner}/{repo}/dependency-graph/sbom

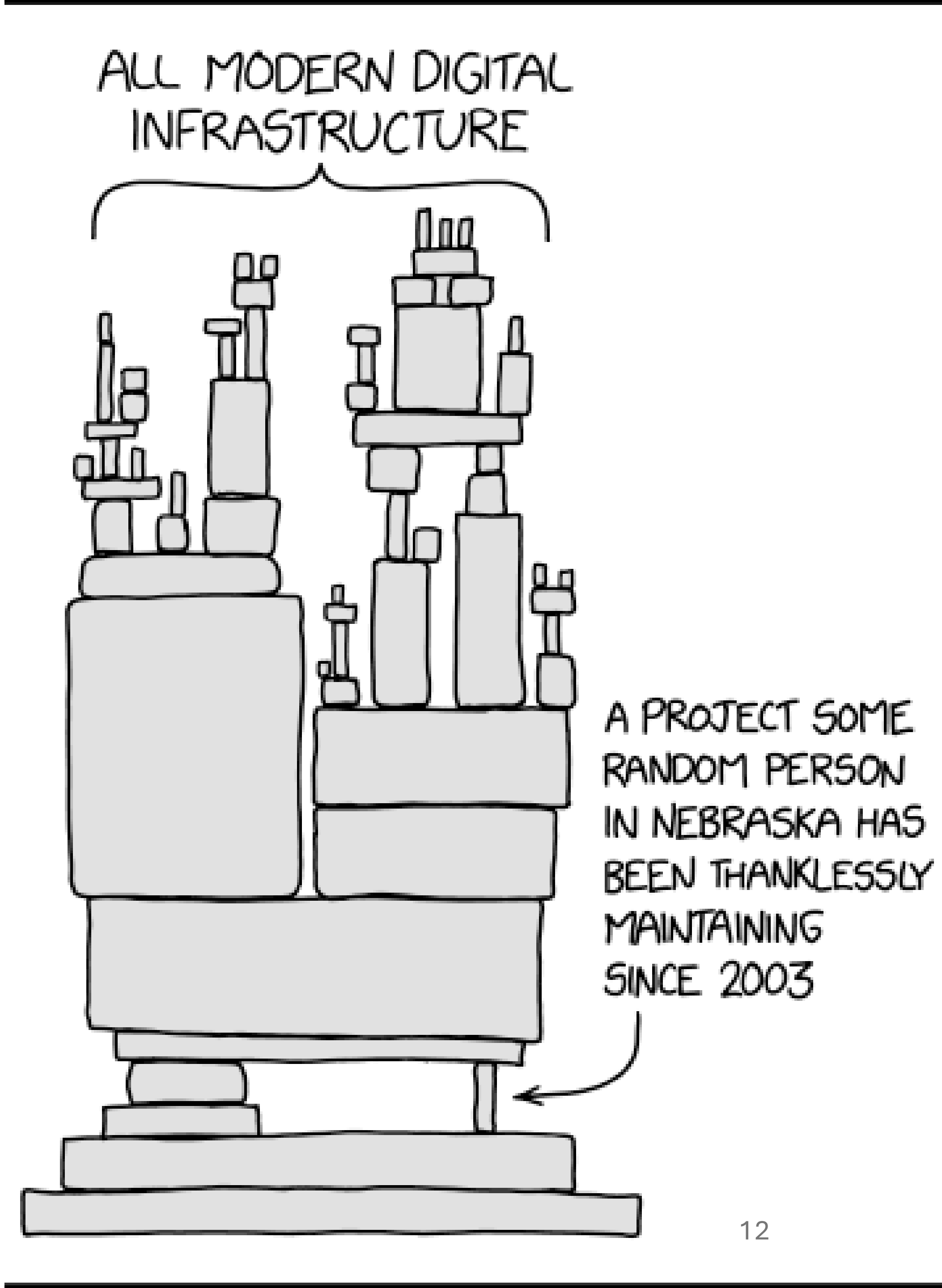
```
curl -L \
  -H "Accept: application/vnd.github+json" \
  -H "Authorization: Bearer <YOUR-TOKEN>" \
  -H "X-GitHub-Api-Version: 2022-11-28" \
  https://api.github.com/repos/OWNER/REPO/dependency-graph/sbom
```

Response

SBoM can help security

- Identifying incorrect use of software
- Identify what to fix in scenarios like log4shell
- Identify impact in sec bug release in a core component

- Basically, Inventory problems


ALL MODERN DIGITAL INFRASTRUCTURE
A PROJECT SOME RANDOM PERSON IN NEBRASKA HAS BEEN THANKLESSLY MAINTAINING SINCE 2003

Ref: XKCD.com/2347

Security efforts already in progress

- VDR : Vulnerability Disclosure Report
- VEX : Vulnerability Exploitability eXchange
- xBoM’s
  - Software-as-a-Service Bill of Materials (SaaSBOM)
  - Hardware Bill of Materials (HBOM)
  - Machine Learning Bill of Materials (ML-BOM)
  - Cryptography Bill of Materials (CBOM)
  - Manufacturing Bill of Materials (MBOM)
  - Operations Bill of Materials (OBOM)
- Attestations

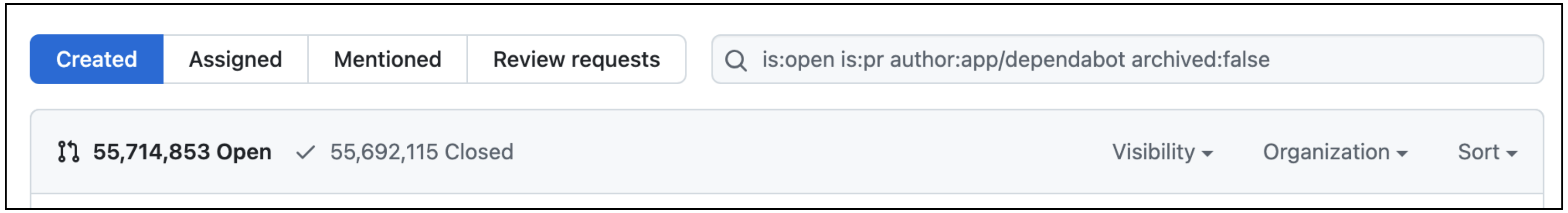
Funny thought

Most of the times

software industry is fixing problems,
that are created by software industry

What problems have we created

- Software build automation == quicker release cycle
- Automated release cycle == less wait for features
- Faster feature release == less inclination to upgrade dependencies
- Too much focus on OSS Codebase without helping the maintainers
- Impossible segregation of features and bug fixes
- Automated notification of vulnerability (hedonic hamster wheel)



is:open is:pr author:app/dependabot archived:false

55,714,853 Open ✓ 55,692,115 Closed

Is SBoM really useful

- SBoM rose to prominence coz of exec order by US President.
- Requirement is to create SBoM
- No directions around usage, consumption etc

- **SBoM Tells you software composition nothing else**

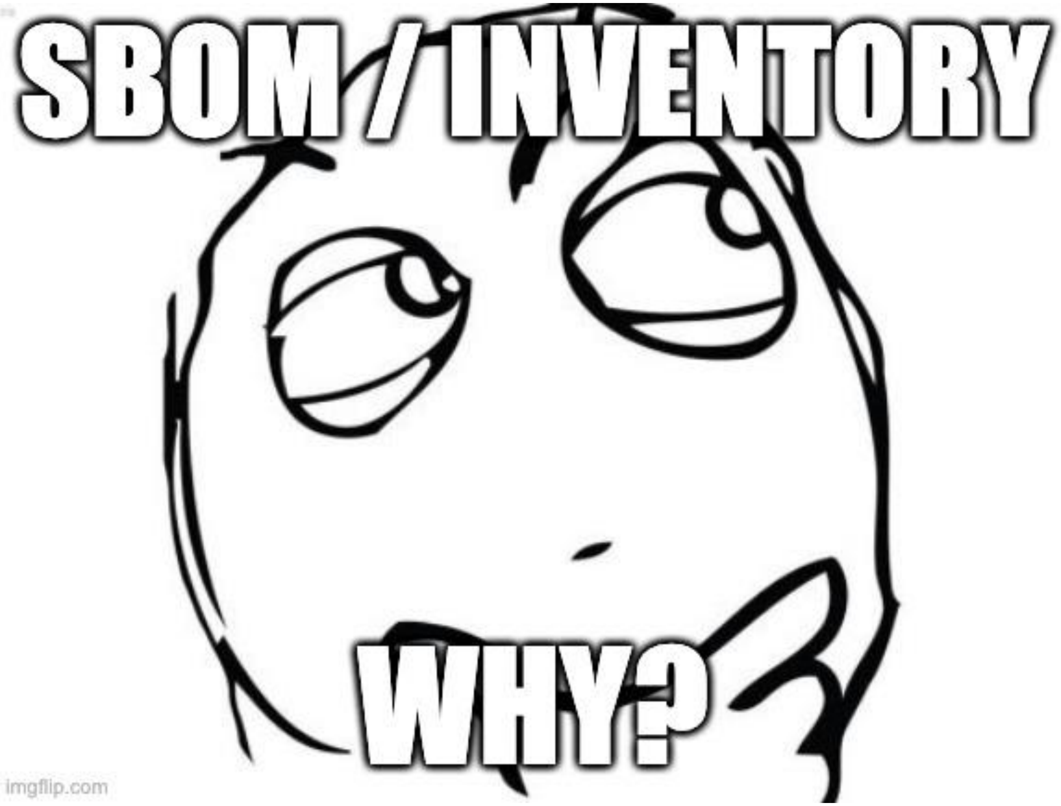
- Industry representatives have started asking Questions?
  - Should we focus on building SBOM or fix issues in that time?

Thoughts from Industry around SBoM

- Why should I disclose my composition to the world
- I will only share the SBoM to NDA covered entities
- I don’t need SBoM coz I don’t sell to USA
- Better to spend time in fixing bugs then making SBoM

Another thought

- Infosec has never had the luxury of well-maintained inventory
- SBoM can help with it
- we never had inventory; we don't even know what to do with it when its created



Consequences for Infosec

For Practitioners both infosec and Devops

- We have been asking for better visibility, this is it

For Industry entities

- This is like “opening the kimono” moment

If security practitioners want to preserve this facility they need to act now

imgflip.com

STOP THE DRAMA ALREADY!!!
imgflip.com

Security efforts already in progress

- VDR : Vulnerability Disclosure Report
- VEX : Vulnerability Exploitability eXchange
- xBoM's
  - Software-as-a-Service Bill of Materials (SaaSBOM)
  - Hardware Bill of Materials (HBOM)
  - Machine Learning Bill of Materials (ML-BOM)
  - Cryptography Bill of Materials (CBOM)
  - Manufacturing Bill of Materials (MBOM)
  - Operations Bill of Materials (OBOM)
- Attestations

What can we do

- Security is largely considered a cost center and any incentive that is solely useful for security is a cost.

- Inventory allows organization to make data driven decisions

- Make SBoM’s usefulness visible for other departments

- If more people especially profit centers and business requirements (HR, Finance) need it, its hard to kill

SBoM Usage beyond security teams

Use each SBoM as part of inventory,

Consolidate then and then draw inferences from it

- Development
- Acquisitions and mergers
- Compliance (adjunct security)
- Risk Management

Consolidated SBoM Tooling

- Format agonistic bom tools
  - Bomctl : https://github.com/bomctl/bomctl
- Policy driven security tooling
  - Vet : https://github.com/safedep/vet
- SBoM Quality check
  - sbomqs: https://github.com/interlynk-io/sbomqs
  - https://github.com/ServiceNow/sbom-status
- SBoM merging utility
  - https://github.com/interlynk-io/sbomasm
- End of Life Focused
  - https://github.com/xeol-io/xeol
- ScoreCard
  - https://github.com/eBay/sbom-scorecard
- And a lot more

Interesting terms and thoughts

- EOL Code
- Drift in packages
- License Volitation
- OSSF ScoreCard

SBoM usage for Developers

- Manage technical Debt
- Reduce dependency scatter
- Consolidate efforts for usage
- Simplified package selection in case of newer project

SBoM usage for Acquisitions & Mergers

Use SBoM as an indicator for future cost and decision

- Too many outdated / EOL / unmaintained software in use leads to high cost of ownership after acquisitions
- If the toolset / techstack is vastly different than existing, then extra talent cost
- If too many techstacks in picture, shows non cohesive teams

SBoM usage for Compliance

- Licensing policy spread not just at product but at input component level
- Possible cost of rework due to non-compliance with company policy
- Possible repercussions if my code touches this code (GPL restrictions to name as one)

SBoM usage for Risk Management

Interesting questions that can be answered

- Do I want to include X amount of risk by purchasing this vendor’s software?
- If risk is low but product will be highly visible, can I still afford it.
- Even with high risk, in a self-contained environment is it okey
- Do I really want my SSO auth token going into this software

What is needed

- Working with other teams to identify ($ / ₹ value to the scenario)
  - Changing a library
  - Upgrading a package
  - Distributing the software
  - Rewriting code
- GUI / Output in PDF / HTML / EXCEL format not pipeline / cli / cmd

What is needed : Overall

- Better tooling (tech and UX)
  - Current tools are not easy to use even for practitioners
- Collaboration and seeking feedback from other parties
  - Don’t make tooling for yourself make it for others
- Focus on usage not on glamorizing tech
  - We technologists focus too much of technical side.

Is it really hard?

- To be honest it is about intention and ideas at this point
- It is simple to play with SboM's
- Hard bit is quantifying and placing the $ / ₹ value to it

- https://github.com/cyfinoid/sbomplay
  - Download Org Level SBoM's
  - Store in Sqlite
  - Create reports from SQLite

To Conclude

- I believe SBoM is a Boon for overall IT Industry to move in better directions.
- Newton’s first law of motion stands : Inertia can only be countered by greater force
- There is a bright future ahead if we can muster the courage for it

Thanks for listening & open to Questions?

NAME

WEBSITE

anant@cyfinoid.com

EMAIL