Back to BASE-ics!

OpenSSF Security Baseline + ORBIT Working Group

Ben Cotton — OSPS Baseline SIG lead

OpenSSF
OPEN SOURCE SECURITY FOUNDATION

- The OpenSSF's OSPS and ORBIT working group curates a catalog of controls and associated tooling focused on connecting the worlds of software development and regulatory compliance, helping upstream better share what they are doing from a security perspective and aligning downstream requirements and expectations, providing them the ability to make risk-based decisions as they ingest third party components and open source software.

ABSTRACT

Who is this guy?

CRob, n, adj, and v

Pronunciation: U.S. (K-rowb)

```
# chmod 666 crob.md
```

44th level Dungeon Master

27th level Securityologist

Pirate-enthusiast & hat-owner

Chief Technology Officer & Chief Security Architect, OpenSSF - Linux Foundation

Involved in upstream OSS CVD for ~15 years

Some images generated by Microsoft Designer and ChatGPT, except that -> That's just my pal Gimp!

OpenSSF
OPEN SOURCE SECURITY FOUNDATION

Who is this guy?

Ben Cotton (he/him)
Open Source Community Lead, Kusari

Maintainer & SIG lead, OSPS Baseline

Some images generated by Microsoft Designer and ChatGPT

OpenSSF
OPEN SOURCE SECURITY FOUNDATION

What is the Baseline?

Est. 2024

OpenSSF
OPEN SOURCE SECURITY FOUNDATION

Introduction

The OpenSSF's **Open Source Project Security Baseline** (OSPS Baseline or simply "**Baseline**") refers to a collection of efforts led by the OpenSSF in collaboration with members and LF partners (CNCF, FINOS, OpenJS, and more!).

It is housed in the **ORBIT (Open Resources for Baselines, Interoperability, and Tooling)** working group, which not only helps shepherd Baseline, but works to provide tools and attestation techniques to support the Baseline criteria!

Broadly, the Baseline + ORBIT group includes a **Catalog** of requirements that map to industry standards, frameworks, and regulations, and **Tooling** to assist in determining Baseline-compliance, that automate Baseline configuration settings, and links to evidence and attestations.

All your Base are belong to us

Background

View Press Release

https://www.youtube.com/watch?v=DxiYI79SIIg

The OpenSSF Security Baseline was officially released Feb 2025. It is based on a library of well-known cybersecurity frameworks, standards, and global regulations. It includes **40** requirements across **3** levels of maturity covering **8** areas of cyber and application security practices

- Access Control
- Build & Release
- Documentation
- Governance
- Legal
- Quality
- Security Assessment
- Vulnerability Management

The criteria range from simple things like documenting processes and procedures to more complex tasks such as infrastructure configuration, all related to SDLC and modern software engineering practices

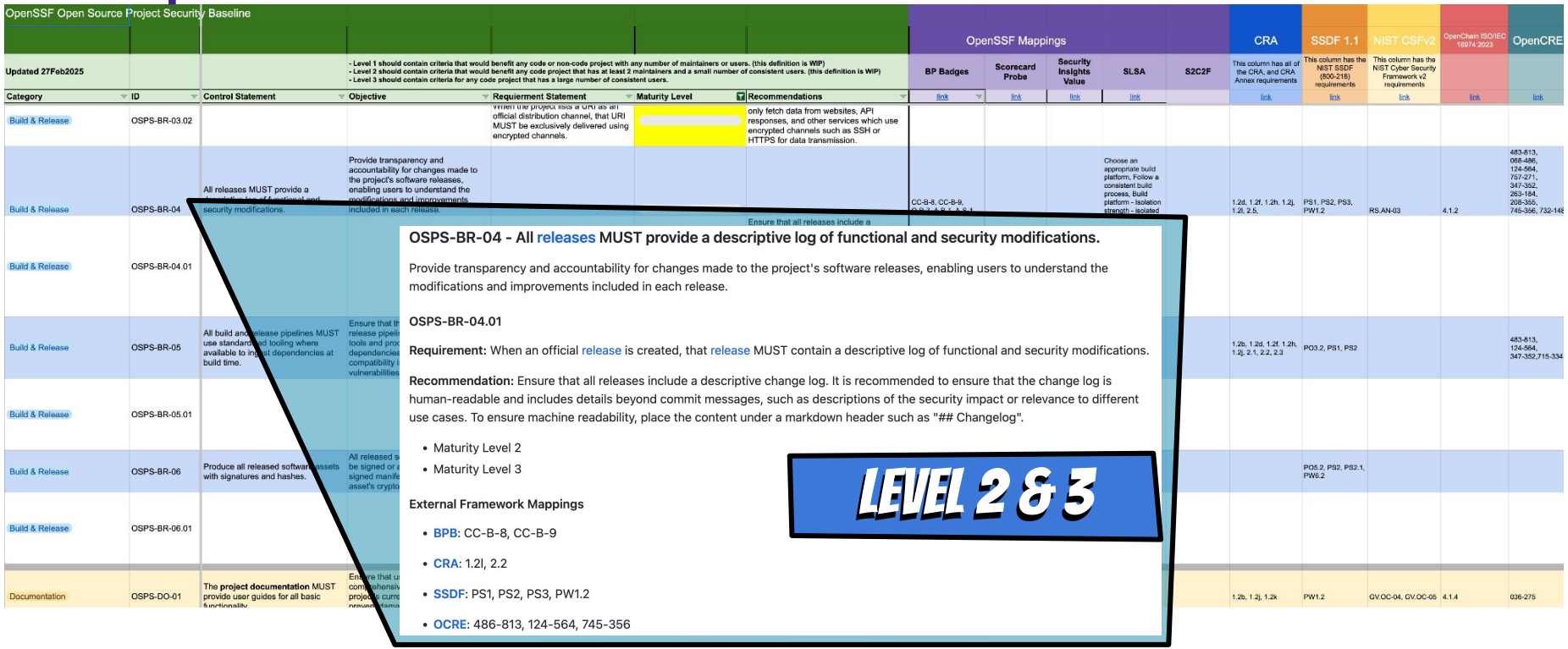
https://baseline.openssf.org
https://github.com/ossf/security-baseline
https://github.com/ossf/wg-ORBIT

What are these levels you speak of?

- "Universal security floor" for all open source - great for single maintainer or early maturity projects
  - Are you a Foundation? the level 1 baseline should be your first set of criteria for maturing projects (or even accepting projects).
- "Let me get my cli, i got this" - good for projects with 2 - 6 maintainers and maturing
- Security *flex* - good for highly mature projects that consider security a core competency
  - Are you in a Foundation with project resources? You should strive for this one.

https://baseline.openssf.org
https://github.com/ossf/security-baseline

Compliance Crosswalk



OpenSSF Open Source Project Security Baseline

Updated 27Feb2025			- Level 1 should contain criteria that would benefit any code or non-code project with any number of maintainers or users. (this definition is WIP) - Level 2 should contain criteria that would benefit any code project that has at least 2 maintainers and a small number of consistent users. (this definition is WIP) - Level 3 should contain criteria for any code project that has a large number of consistent users.				OpenSSF Mappings					CRA	SSDF 1.1	NIST CSFv2	OpenChain ISO/IEC 18974:2023	OpenCRE
Category	ID	Control Statement	Objective	Requirement Statement	Maturity Level	Recommendations	BP Badges	Scorecard Probe	Security Insights Value	SLSA	S2C2F	This column has all of the CRA, and CRA Annex requirements	This column has the NIST SSDF (800-218) requirements	This column has the NIST Cyber Security Framework v2 requirements		
							link	link	link	link		link	link	link	link	link
Build & Release	OSPS-BR-03.02			When the project lists a URI as an official distribution channel, that URI MUST be exclusively delivered using encrypted channels.		only fetch data from websites, API responses, and other services which use encrypted channels such as SSH or HTTPS for data transmission.										
Build & Release	OSPS-BR-04	All releases MUST provide a descriptive log of functional and security modifications.	Provide transparency and accountability for changes made to the project's software releases, enabling users to understand the modifications and improvements included in each release.			Ensure that all releases include a	CC-B-8, CC-B-9,			Choose an appropriate build platform. Follow a consistent build process. Build platform - Isolation strength - isolated		1.2d, 1.2f, 1.2h, 1.2j, 1.2l, 2.5,	PS1, PS2, PS3, PW1.2	RS.AN-03	4.1.2	483-813, 068-486, 124-564, 757-271, 347-352, 263-184, 208-355, 745-356, 732-148
Build & Release	OSPS-BR-04.01															
Build & Release	OSPS-BR-05	All build and release pipelines MUST use standardized tooling where available to install dependencies at build time.	Ensure that the release pipeline tools and proc dependencies compatibility vulnerabilities									1.2b, 1.2d, 1.2f, 1.2h, 1.2j, 2.1, 2.2, 2.3	PO3.2, PS1, PS2			483-813, 124-564, 347-352,715-334
Build & Release	OSPS-BR-05.01															
Build & Release	OSPS-BR-06	Produce all released software assets with signatures and hashes.	All released s be signed or a signed manife asset's crypto										PO5.2, PS2, PS2.1, PW6.2			
Build & Release	OSPS-BR-06.01															
Documentation	OSPS-DO-01	The **project documentation** MUST provide user guides for all basic	Ensure that u comprehensiv project's curre									1.2b, 1.2j, 1.2k	PW1.2	GV.OC-04, GV.OC-05	4.1.4	036-275

OSPS-BR-04 - All releases MUST provide a descriptive log of functional and security modifications.

Provide transparency and accountability for changes made to the project's software releases, enabling users to understand the modifications and improvements included in each release.

OSPS-BR-04.01

Requirement: When an official release is created, that release MUST contain a descriptive log of functional and security modifications.

Recommendation: Ensure that all releases include a descriptive change log. It is recommended to ensure that the change log is human-readable and includes details beyond commit messages, such as descriptions of the security impact or relevance to different use cases. To ensure machine readability, place the content under a markdown header such as "## Changelog".

- Maturity Level 2
- Maturity Level 3

External Framework Mappings

- BPB: CC-B-8, CC-B-9
- CRA: 1.2l, 2.2
- SSDF: PS1, PS2, PS3, PW1.2
- OCRE: 486-813, 124-564, 745-356

LEVEL 2 & 3

https://docs.google.com/spreadsheets/d/1an5mx3rayoz3JRFUepD56zgprpwXBXBG70fVZvIMCpA/

Building a Better Catalog

Baseline currently maps alignment across multiple cyber compliance frameworks and/or cyber legislations. "Baselining" helps downstream select projects that align with and that support their compliance obligations!

NIST National Institute of Standards and Technology U.S. Department of Commerce

- SSDF
- CSF
- 800-161/800-53
- CISA Software Acquisition Guide (forthcoming)

European Commission

- Cyber Resilience Act
- DORA (forthcoming)
- NIS2 (forthcoming)

National Cyber Security Centre a part of GCHQ

- Software Security Code of Practice (forthcoming)

OpenSSF OPEN SOURCE SECURITY FOUNDATION

- BP Badges
- Scorecard
- Minder
- SLSA
- OpenSSF tooling

PCI Security Standards Council

SAMM

OPENCRE

OPENCHAIN

Proactive Software Supply Chain Risk Management (P-SSCRM) Framework

Compliance Crosswalk

Have a framework or a particular piece of legislation you'd like to see integrated into the Baseline? Patches Welcome!

Why Baseline Matters - Maintainers

- Gives **direct** and **actionable** advice for improving security practices

- Provides the ability for Developers/projects to **show** they follow reasonable security measures as well as ways to improve

- **Allow projects to humble-brag** about how great they are!
  (Stars & Likes, accolades, peer recognition, CV-building, jobs, promotions, etc.)

- **Collects common downstream requests** (nags/demands) and advertises them **so Downstream can RTFM** and stop harassing their unpaid Upstream component sources

Why Baseline Matters - Downstream

- Provides **clear signals** and **evidence/attestations** about upstream component security practices *to allow corporate due-diligence and risk management*

- Provides a **clear checklist** of things that **Downstream could go** donate/**DO for their Upstream sources**

- **Aligns software development practices with global cybersec laws** and frameworks (reduces compliance costs [do once, applicable many])

- Ingesting projects that follow the Baseline **reduces time and effort** in **due-diligence activities** and help the organization defend itself to auditors and regulators.

Why Baseline Matters - Stewards

- **Security Maturity Pathway**: Provides a **graduated framework (Level 1–3)** to assess & improve project security, suitable for foundation-level quality and graduation criteria
- **Regulatory Alignment**: Covers and maps to industry and government frameworks (e.g., SSDF, NIST 800-53, CRA, DORA) — saving time on audits and compliance
- **Cross-Foundation Consistency**: Standardizes expectations across CNCF, OpenJS, FINOS, and other LF cohorts
- LF Members are REQUIRED to follow many of these rules in their own enterprises, providing them **already-hardened projects will increase adoption** & uptake within commercial enterprises and reduce regulatory burdens to them

A quick example

OpenSSF
OPEN SOURCE SECURITY FOUNDATION

Access Control - OSPS-AC-01

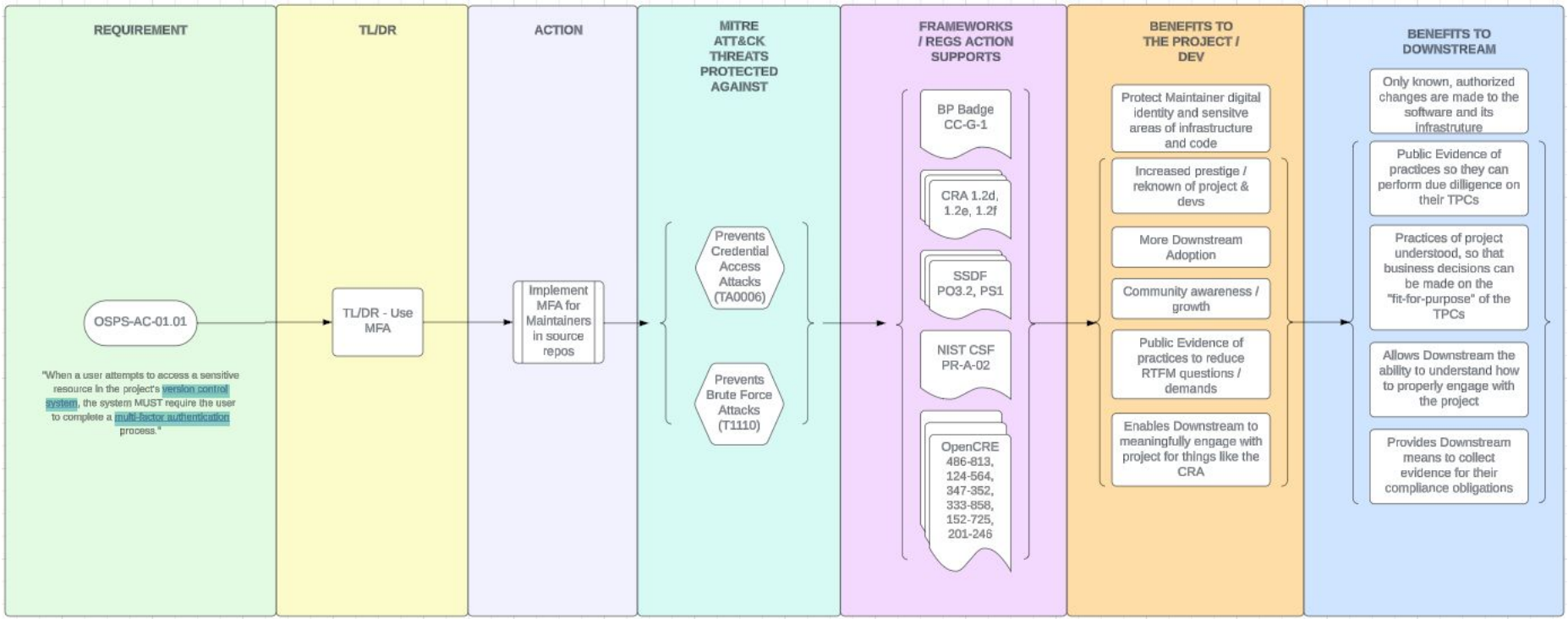
This requirement is seeking to protect maintainers and the sensitive areas of a project they oversee.

```yaml
assessment-requirements:
  - id: OSPS-AC-01.01
    text: |
      When a user attempts to read or modify a sensitive resource in the project's
      authoritative repository, the system MUST require the user to complete
      a multi-factor authentication process.
    applicability:
      - Maturity Level 1
      - Maturity Level 2
      - Maturity Level 3
    recommendation: |
      Enforce multi-factor authentication for the project's version
      control system, requiring collaborators to provide a second form of
      authentication when accessing sensitive data or modifying repository
      settings. Passkeys are acceptable for this control.
```

```yaml
controls:
  - id: OSPS-AC-01
    title: |
      The project's version control system MUST require multi-factor
      authentication for users modifying the project repository
      settings or accessing sensitive data.
    objective: |
      Reduce the risk of account compromise or insider threats by requiring
      multi-factor authentication for collaborators modifying the project
      repository settings or accessing sensitive data.
    guideline-mappings:
      - reference-id: BPB
        entries:
          - reference-id: CC-G-1
      - reference-id: CRA
        entries:
          - reference-id: 1.2d
          - reference-id: 1.2e
          - reference-id: 1.2f
      - reference-id: SSDF
        entries:
          - reference-id: PO.3.2
          - reference-id: PS.1
          - reference-id: PS.2
      - reference-id: CSF
        entries:
          - reference-id: PR.A-02
          - reference-id: PR.A-05
      - reference-id: OpenCRE
        entries:
          - reference-id: 486-813
          - reference-id: 124-564
          - reference-id: 347-352
          - reference-id: 333-858
          - reference-id: 152-725
          - reference-id: 201-246
      - reference-id: PSSCRM
        entries:
          - reference-id: G2.6
          - reference-id: P3.3
          - reference-id: E1.2
          - reference-id: E1.3
          - reference-id: E1.4
          - reference-id: E3.1
      - reference-id: SAMM
        entries:
          - reference-id: Operations -Environment Management -Configuration Hardening Lvl1
      - reference-id: PCIDSS
        entries:
          - reference-id: 2.2.1
          - reference-id: 8.2.1
          - reference-id: 8.3.1
      - reference-id: UKSSCOP
        entries:
          - reference-id: 2.1
      - reference-id: 800-161
        entries:
          - reference-id: AC-4(21)
          - reference-id: AC-17
          - reference-id: CM-5
          - reference-id: CM-6
          - reference-id: IA-2
          - reference-id: IA-5
          - reference-id: 1.2e
          - reference-id: 1.2f
```


https://docs.github.com/en/authentication/securing-your-account-with-two-factor-authentication-2fa/configuring-two-factor-authentication

The Example in action...



What we’re hoping to avoid

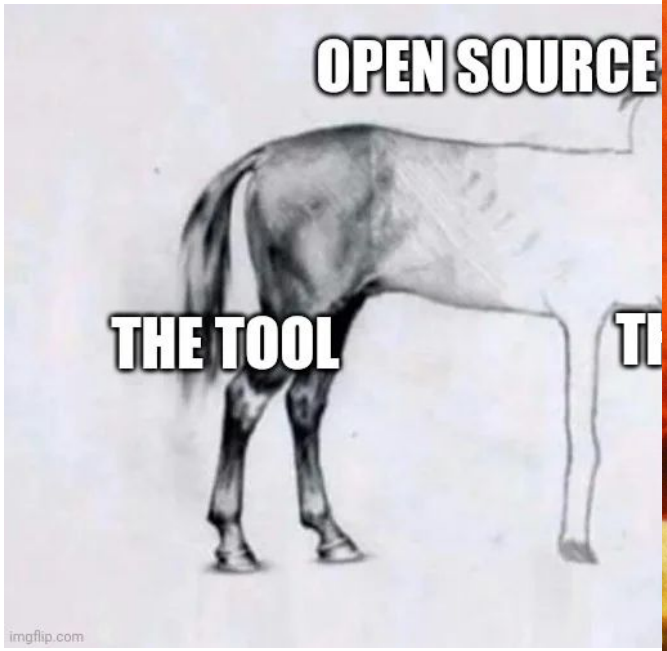


Image Source

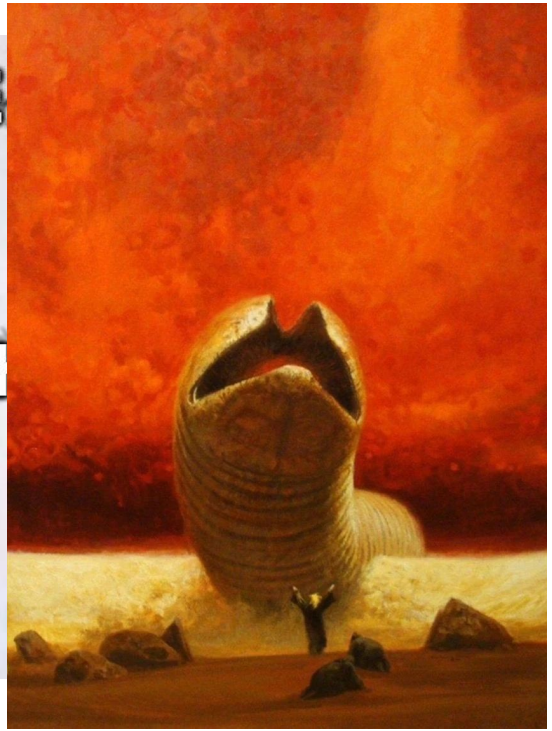


Image Source

Hello,

I hope this message finds you well.

As part of our ongoing efforts to comply with the EU Cyber Resilience Act (CRA), we are currently conducting a cybersecurity risk assessment of third-party software vendors whose products or components are integrated into our systems.

To support this initiative, we kindly request your input on the following questions related to your software product “libcurl” with version 7.87.0. Please provide your responses directly in the table below and do reply to all added in this email,

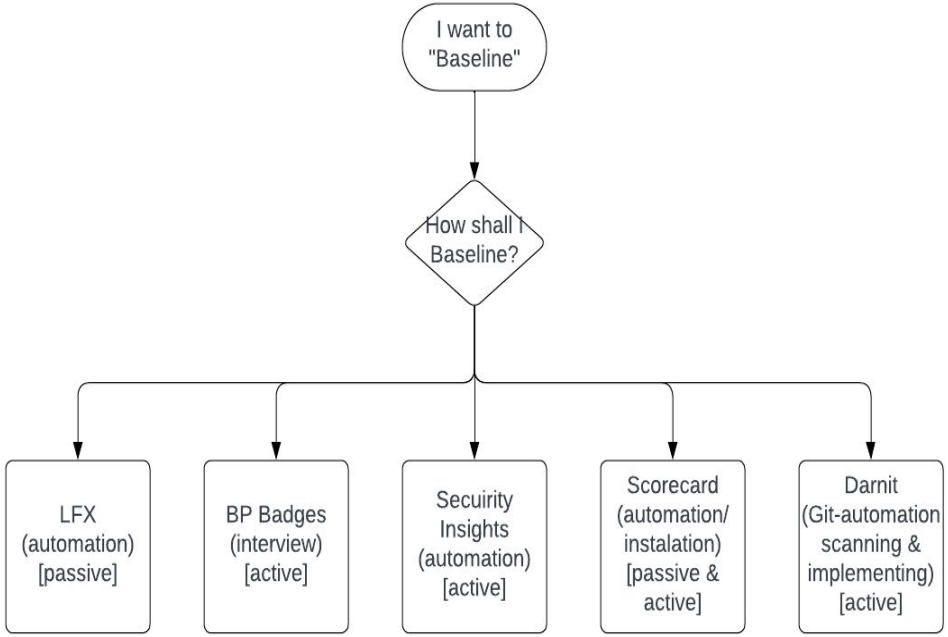
Additional Information:

- Purpose: This security assessment is part of our due diligence and regulatory compliance obligations under the EU CRA.
- Confidentiality: All information shared will be treated as confidential and used solely for the purpose of this assessment.
- Contact: Should you have any questions or need further clarification, please feel free to reach out by replying directly to this email.

We kindly request your response by Friday, July 25, 2025, to ensure timely completion of our assessment process. Thank you for your cooperation and continued partnership in maintaining a secure and resilient digital environment.

Image Source

Multiple paths to a secure outcome

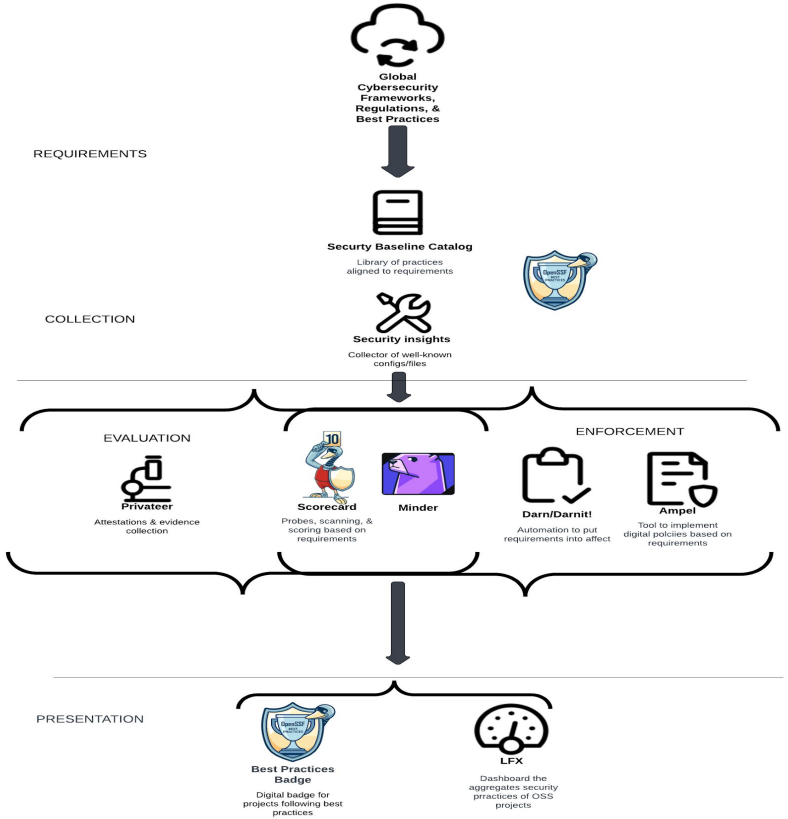


Depending on how much you actively want to do, there are multiple paths that you can take to follow the Baseline Catalog requirements.

Future Workflow

- Baseline catalog is ready today!
- Compliance Crosswalk ready today!
- Tooling to enable and empower the Baseline Catalog are being developed TODAY!

Follow the ORBIT Working group (Open Resources for Baselines, Interoperability, and Tooling) for more details - https://github.com/ossf/wg-orbit



ORBIT + Adjacent Tooling to Enable Baseline

Best Practices Badge - well-known and well=regarded by the community with hundreds of projects currently earning badges. Baseline criteria will be interwoven into the Badges adding 3 new levels of badge to earn and display along with the existing (and providing credit where requirements are already met.

Security Insights - data format that allows projects to define where files and configurations live to enable further automation in the pipeline. Enables projects to attest to security practices in a machine-readable manner.

Darnit - cli/git-enabled tool that will evaluate project's Baseline compliance and create PRs to deploy desired Baseline level settings/files.

Gemara - GRC Engineering Model for Automated Risk Assessments

Scorecard - Automated tool that seeks security practices of projects, provides a reflective score of adherence to desired security objectives. Very useful for OSPOs managing their third-party component consumption.

Minder - a policy-decision engine that can be deployed with CI/CD systems to enforce desired security policies

Ampel - a simple policy-decision engine that can be deployed with CI/CD systems to enforce desired security policies

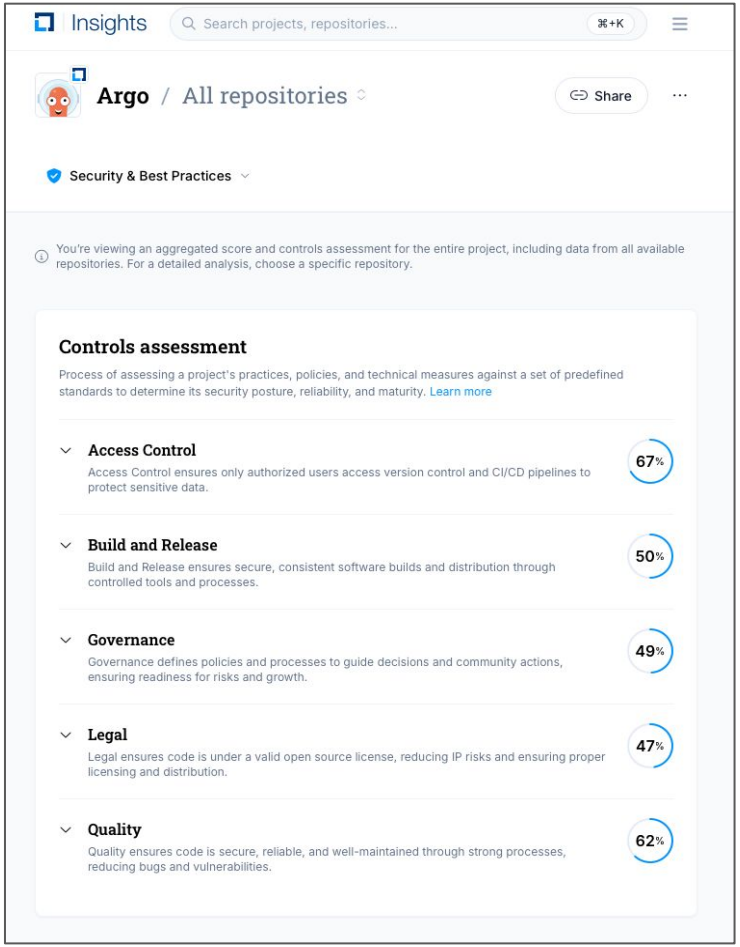
LFX - a dashboard that spans all LF-projects (and more!) that show assorted security data points, including Baseline, BP Badges, and Scorecard. A "single pane of glass" to view the security posture of OSS projects.

Tying it all together

As the group settles into a working rhythm, we're now ready to start engaging with the broader LF and ecosystem.

We'll begin work on a "Baseline workflow" on how projects can "Get Baselined", work on docs, education, and continue work on automation and attestations .

Tools Like LFX, Scorecard, and BP Badges will be outward signs for developers and consumers about the "Baselineness" of a project.




GOOSE: ALL YOUR BASE
ARE BELONG TO US.

How to get involved...

- Review the Baseline, give feedback
- Consider implementing the Baseline controls for projects you work on
- As a Consumer, consider using Baseline as part of your third-party component due-diligence
- Suggest additional cyber frameworks or legislation to add to the Compliance Crosswalk
- Participate in the new “Baseline for AI” project
- Attend a Baseline or ORBIT meeting to contribute to the Catalog and Tooling

Baseline

ORBIT

Thank You

CRob_at_OpenSSF_dot_org

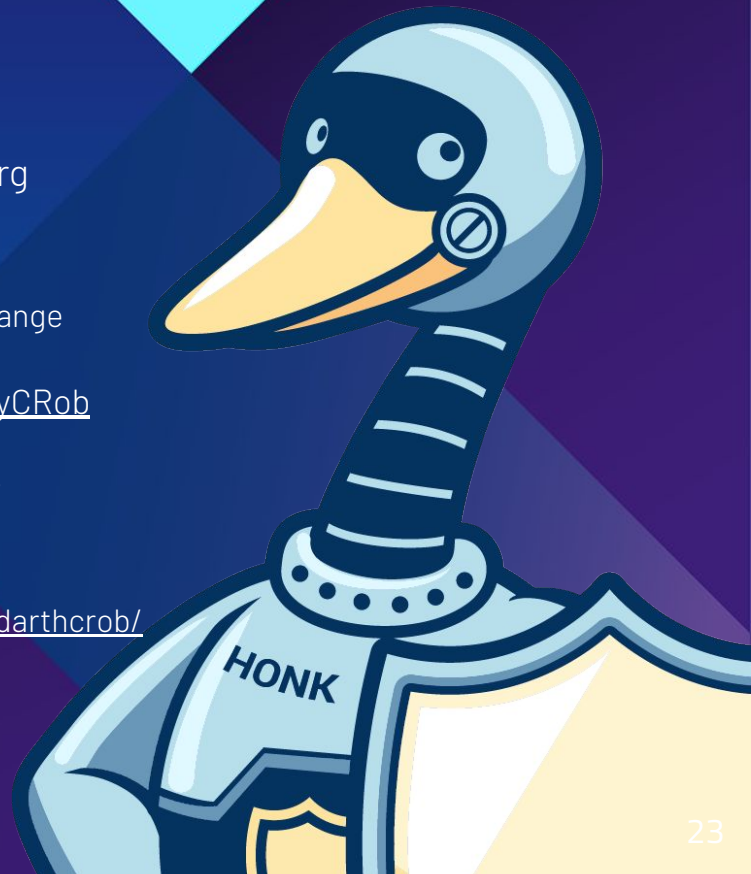
@~~SecurityCRob~~

@SecurityCRob@infosec.exchange

https://github.com/SecurityCRob

The Security Unhappy Hour,
Chips & Salsa
What's in the SOSS?

https://www.linkedin.com/in/darthcrob/



OpenSSF
OPEN SOURCE SECURITY FOUNDATION

Thank You!

OpenSSF
OPEN SOURCE SECURITY FOUNDATION

Ways to Participate

Join a Working Group/Project

Come to a Meeting (see Public Calendar)

Collaborate on Slack

Contribute on GitHub

Become an Organizational Member

Keep up to date by subscribing to the OpenSSF Mailing List

OpenSSF
OPEN SOURCE SECURITY FOUNDATION

Legal Notice