

Scorecard and Sigstore

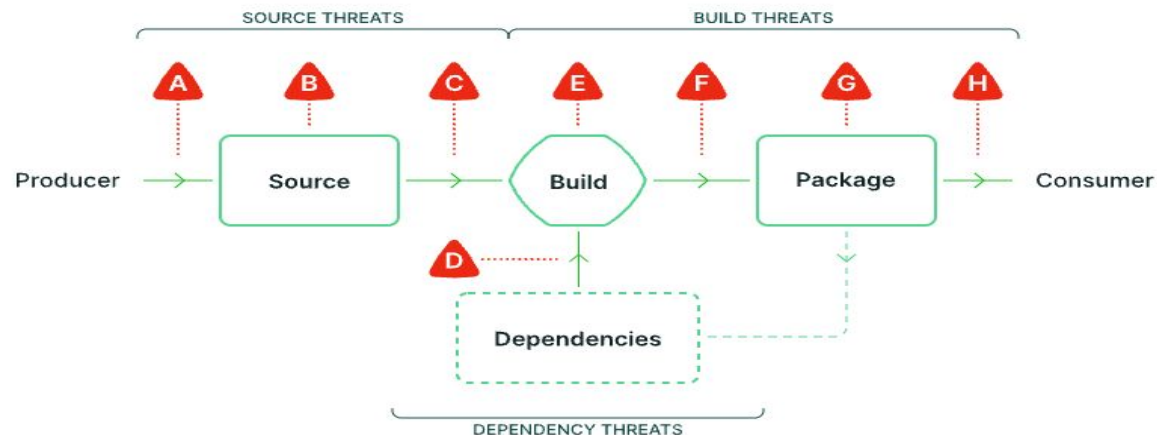
Overview



OpenSSF

OPEN SOURCE SECURITY FOUNDATION

Software Supply Chain Threats



SOURCE THREATS

- A** Submit unauthorized change
- B** Compromise source repo
- C** Build from modified source

DEPENDENCY THREATS

- D** Use compromised dependency

BUILD THREATS

- E** Compromise build process
- F** Upload modified package
- G** Compromise package registry
- H** Use compromised package

Reference: [SLSA Framework - Supply Chain Threats](#)

What is Scorecard?

*“an **automated tool** that assesses a number of important heuristics (**“checks”**) associated with software security and assigns each check a score of 0-10. ” - Scorecard*

A great [example](#) of OpenSSF Scorecard report

What is Scorecard?

*“an **automated tool** that assesses a number of important heuristics (**“checks”**) associated with software security and assigns each check a score of 0-10. ” - Scorecard*

A great [example](#) of OpenSSF Scorecard report

Scorecard - Shift Security to the Left

Measures and reports the security posture of software projects, mainly open source

- Analysing the potential threats

Improves the security posture of a software projects, close source and open source

- Provides recommendations

Help software producers to produce more secure software

Help software consumers to manage dependencies more effectively

- Software producers are consumers

Scorecard Adoption - By Maintainers

Make your open source software more secure

Showcase your security achievements using [Scorecard Badge](#)

Increase project adoption

How to?

- Use [Scorecard GitHub Action](#) to enable Scorecard on GitHub public repositories you own
- [Focus on the most important findings first](#) to improve security posture in the shortest time
- Refer to [OpenSSF GUAC Scorecard Configuration](#) as an example

Scorecard Adoption - By Consumers

Make fact-driven decisions on software dependencies

- Scorecard scans 1 million most critical open source projects weekly and publish the results publicly

Make your products/services more secure

Increase products/services market share

How to?

- Use BigQuery Explorer to [check an OSS project security scoring history](#).
- Use the [REST API](#)
- Incorporate Scorecard measurements into your SDLC process to reduce dependency threats

Scorecard Resources

Website

<https://securityscorecards.dev/>

GitHub repository

<https://github.com/ossf/scorecard>

Scorecard training:

<https://openssf.org/training/securing-projects-with-openssf-scorecard-course/>

What is Sigstore?

An open source internet service that creates and verifies digital signatures using ephemeral certificates

Policy and insight

Automation, risk management, and compliance throughout the SDLC.
Governance, developer assistance, and policy shifted left.

Embed security into SDLC process

Aggregation and synthesis

Smart aggregation turning data into meaning. Intelligent linking of project, resource, developer, artifact, repo, toolchain.

Automation capabilities for
data-driven security decisions

Software attestations

Schemas and sources for rich security metadata. SBOM, SLSA provenance, VEX, OSV, security scorecards, developer reputation, plus proprietary data.



Verifiable evidence of artifacts
authenticity and integrity

Trust foundation

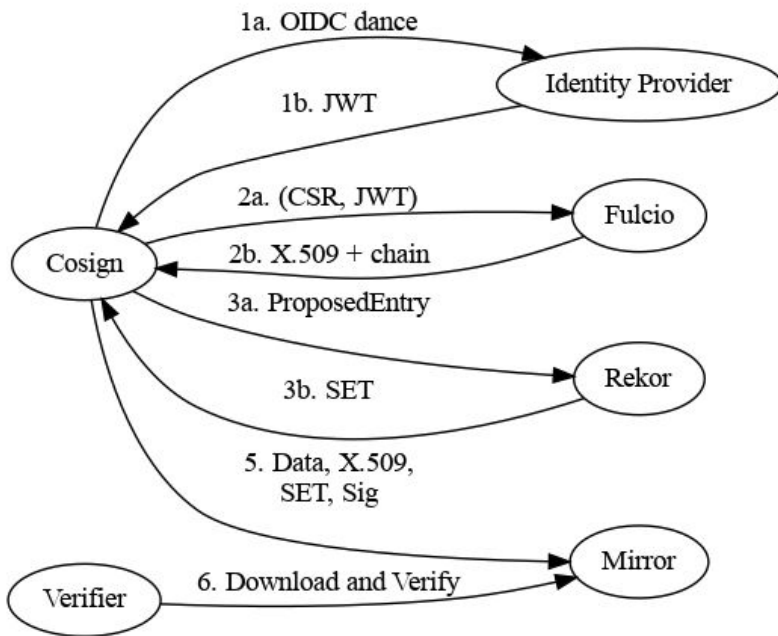
A decentralized, flexibly anchored trust fabric. Signatures, strong identities, distributed timestamping, federation.



Foundational layer of trust

Reference: [Sigstore: Simplifying Code Signing for Open Source Ecosystems](#)

Sigstore Architecture



IdP - Verifies the signer's identity via [OIDC](#)

Fulcio - the CA that issues ephemeral x.509 certificates

Rekor - Timestamping authority, transparency log of software artifacts metadata and their signature

Reference: [Life of a Sigstore Signature](#), [What is Sigstore](#)

Sigstore - Software Artifact Signing

[sigstore-python](#) to sign and verify Python package distributions.

Scorecard scanning result signed and verifiable

- Rekor [evidence](#)
- Scorecard [analysis workflow log](#)
- Scorecard [code base](#) for signing artifacts

Sigstore - SLSA Build Provenance

SLSA - Supply chain Levels for Software Artifacts

[SLSA](#) is a specification for describing and incrementally improving supply chain security, established by industry consensus. It is organized into a series of levels that describe increasing security guarantees.

Track/Level	Requirements	Focus
Build L0	(none)	(n/a)
Build L1	Provenance showing how the package was built	Mistakes, documentation
Build L2	Signed provenance, generated by a hosted build platform	Tampering after the build
Build L3	Hardened build platform	Tampering during the build

Sigstore - SLSA Build Provenance

Build provenance provides traceability of software artifacts back to its origin

- Where the source code is
- When, where, and how the artifacts are build
- Who triggers the build and why

Scorecard again!

- [Release v4.13.1](#) [build provenance](#)
- Uses GitHub action to [produce](#) SLSA build Level 3 provenance
- Verify a tar ball

```
danawang@DW-MacP downloads % slsa-verifier verify-artifact scorecard_4.13.1_darwin_amd64.tar.gz --provenance-path multiple.intoto.jsonl --source-uri github.com/ossf/scorecard --source-tag v4.13.1
Verified signature against tlog entry index 44413894 at URL: https://rekor.sigstore.dev/api/v1/log/entries/24296fb24b8ad77a6ed6002a1c284e6cccd5271682edf404e7849b1ae591e71eceb83a4a061a828e
Verified build using builder "https://github.com/slsa-framework/slsa-github-generator/.github/workflows/generator_generic_slsa3.yml@refs/tags/v1.9.0" at commit 49c0eed3a423f00c872b5c3c9f1bbca9e8aae799
Verifying artifact scorecard_4.13.1_darwin_amd64.tar.gz: PASSED
```

Sigstore Resources

Website

<https://www.sigstore.dev/>

GitHub repository

<https://github.com/sigstore>

Training

<https://openssf.org/training/securing-your-software-supply-chain-with-sigstore-course/>

SLSA Resources

Website

<https://slsa.dev/>

GitHub repository

<https://github.com/slsa-framework>

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](#)

Engage with us on social media



X
[@openssf](https://twitter.com/openssf)



LinkedIn
[OpenSSF](https://www.linkedin.com/company/openssf)



Mastodon
social.lfx.dev/@openssf



YouTube
[OpenSSF](https://www.youtube.com/openssf)



Facebook
[OpenSSF](https://www.facebook.com/openssf)

Subscribe to our mailing list

openssf.org/sign-up



Is your organization a member?

Questions? Contact membership@openssf.org

openssf.org/join



Thank You



Legal Notice

Copyright © [Open Source Security Foundation](#)®, [The Linux Foundation](#)®, & their contributors. The Linux Foundation has registered trademarks and uses trademarks. All other trademarks are those of their respective owners.

Per the [OpenSSF Charter](#), this presentation is released under the Creative Commons Attribution 4.0 International License (CC-BY-4.0), available at <<https://creativecommons.org/licenses/by/4.0/>>. You are free to:

- Share — copy and redistribute the material in any medium or format for any purpose, even commercially.
- Adapt — remix, transform, and build upon the material for any purpose, even commercially.

The licensor cannot revoke these freedoms as long as you follow the license terms:

- Attribution — You must give appropriate credit , provide a link to the license, and indicate if changes were made . You may do so in any reasonable manner, but not in any way that suggests the licensor endorses you or your use.
- No additional restrictions — You may not apply legal terms or technological measures that legally restrict others from doing anything the license permits.

Appendix

Elements

Copyright Text

Copyright © 2024 The Linux Foundation®. All rights reserved. The Linux Foundation has registered trademarks and uses trademarks.

Table

	Heading 1			
Row 1				