GUAC Tech Talk

Proactive Supply Chain Security with Graph for Understanding Artifact Composition (GUAC)

June 6th, 10AM PT/1PM ET

GUAC

OpenSSF

OPEN SOURCE SECURITY FOUNDATION

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

Welcome!

- Thank you for joining us today! We will begin at 10:02am PT.
- While we wait for everyone to join, please take a moment to do one (or more) of the following:
    - Please add questions using the Zoom Q&A feature
    - Follow us on Twitter: @openssf, Mastodon: social.lfx.dev/@openssf, & LinkedIn: OpenSSF
    - Visit our website: https://openssf.org
    - Sign up for training: https://openssf.org/training/courses/
- This Tech Talk is being recorded

OpenSSF
OPEN SOURCE SECURITY FOUNDATION

Agenda

- Housekeeping
- Panelist Introductions
- Introduction to GUAC
- Understanding GUAC
- Insights from Implementing Organizations
- Panel Discussion: Member Organizations’ Experiences
- Q&A from the Audience

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.

Code of Conduct

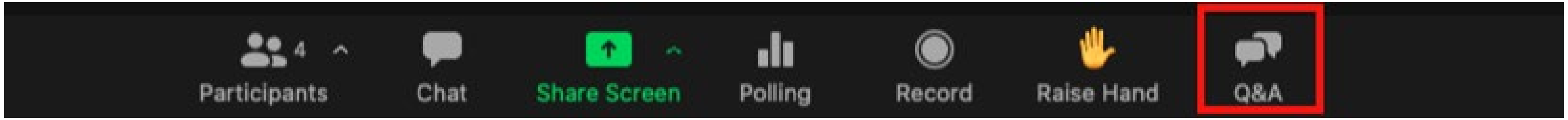
- The Linux Foundation and its project communities a**dedicated to providing a harassment-free experience** for participants at all of our events, whether they are held in person or virtually.

- All event participants, whether they are attending an in-person event or a virtual event, **are expected to behave in accordance with professional standards**, with both this Code of Conduct as well as their respective employer's policies governing appropriate workplace behavior and applicable laws.

- https://openssf.org/community/code-of-conduct/

Q&A

Please submit your questions during the meeting by using the Q&A feature on Zoom.



Thank you!

OpenSSF & GUAC

- Open Source Security Foundation (OpenSSF)
  - “a community of software developers, security engineers, and more who are working together to secure open source software for the greater public good.”
  - a non-profit foundation that’s part of the Linux Foundation.
  - Has many projects & other efforts, today we’ll focus on one: the GUAC project
- GUAC
  - Team members from Kusari, Google, Citi and Purdue University had been dealing with the problem of software supply chain transparency
  - Decided to work together to find a solution & built GUAC - Graph for Understanding Artifact Composition

Introductions

David A. Wheeler

OpenSSF
OPEN SOURCE SECURITY FOUNDATION

David A. Wheeler - Director of Open Source Supply Chain Security, the Linux Foundation

Dr. David A. Wheeler is an expert on developing secure software and on open source software (OSS) development. He wrote the book “Secure Programming HOWTO” on how to develop secure software, and his work on countering malicious tools (“Fully Countering Trusting Trust through Diverse Double-Compiling (DDC)”) is widely cited. He is the Director of Open Source Supply Chain Security at the Linux Foundation, and teaches graduate courses in developing secure software at George Mason University (GMU). He is also the lead for the Linux Foundation’s OpenSSF Best Practices badge project. Dr. Wheeler has a PhD in Information Technology, a Master’s in Computer Science, a certificate in Information Security, and a B.S. in Electronics Engineering, all from George Mason University (GMU). He is also a Certified Information Systems Security Professional (CISSP) and a Senior Member of the Institute of Electrical and Electronics Engineers (IEEE).

OpenSSF
OPEN SOURCE SECURITY FOUNDATION

Rose Judge - Senior Open Source Engineer at Broadcom

Rose Judge is a Senior Open Source Engineer at Broadcom (formerly VMware) focused on Open Source Security. She is the Chair of the SPDX Steering Committee and plays an active role in developing both the technical and security profile specification. She's also an open source maintainer for Tern, a container SBOM tool, and spends the rest of her time in open source trying to improve gaps around SBOM creation, quality, and distribution.

Brandon Lum - Open Source Security Engineer, Google

Brandon loves designing and implementing computer systems (with a focus on Security, Operating Systems, and Distributed/Parallel Systems). Brandon is Co-chair Emeritus of the CNCF Security TAG, and as a part of Google’s Open Source Security and BCID team, he works on improving the security of the Open Source ecosystem and observability into all of Google's software supply chain metadata (SBOMs, SLSA, etc.). Previously at IBM Research, Brandon worked on various security areas such as: Container content protection via encryption and image signing, identity, and kernel attack surface reduction.

OpenSSF
OPEN SOURCE SECURITY FOUNDATION

OpenSSF
OPEN SOURCE SECURITY FOUNDATION

Parth Patel, CPO/Co-Founder, Kusari

Parth Patel focuses on bringing transparency and security to the forefront of all projects. He is an engineering leader with more than 15 years of cybersecurity, DevOps, software development, and automation experience. Parth is an active member within the open-source community, serving as a co-creator and lead maintainer on the GUAC project, and a maintainer for the CNCF in-toto attestations, CNCF in-toto golang, and FRSCA projects. He has successfully led multiple consulting and development projects for modernization/migration, cloud adoption, and a secure software supply chain, including with government contractors where security was paramount.

OpenSSF
OPEN SOURCE SECURITY FOUNDATION

Umang Jain, Director of Technical Program Management, Platform Engineering, Guidewire

Umang Jain has been with Guidewire Software for more than six years and is the Director of Technical Program Management, Platform Engineering. He has worked with Agile software practices for more than a decade. His passion is enabling Platform Engineering teams to be effective partners with application developers in shipping software features.

Understanding Software Bill of Materials (SBOM), OSS Security

Rose Judge

SBOM

A formal record of the components and processes used to create a piece of software

OpenSSF
OPEN SOURCE SECURITY FOUNDATION

SBOM Application

- Transparency
  - Trust
- Inventory
  - Security
  - Compliance
- Supply Chain Security
  - Risk Assessment
  - Vulnerability Remediation
  - Security Audits
- Policy

Understanding Graph for Understanding Artifact Composition (GUAC)

Brandon Lum, Parth Patel

Our software supply chains are COMPLICATED in-toto

SLSA

SBOM
Software Bill of Materials

SPDX

VEX

SLSA

CycloneDX

VEX

SPDX

SBOM
Software Bill of Materials

SLSA

SBOM
Software Bill of Materials

in-toto

SLSA

SBOM
Software Bill of Materials

SPDX

SLSA

CycloneDX

VEX

SPDX

in-toto

SLSA

VEX

in-toto

CycloneDX

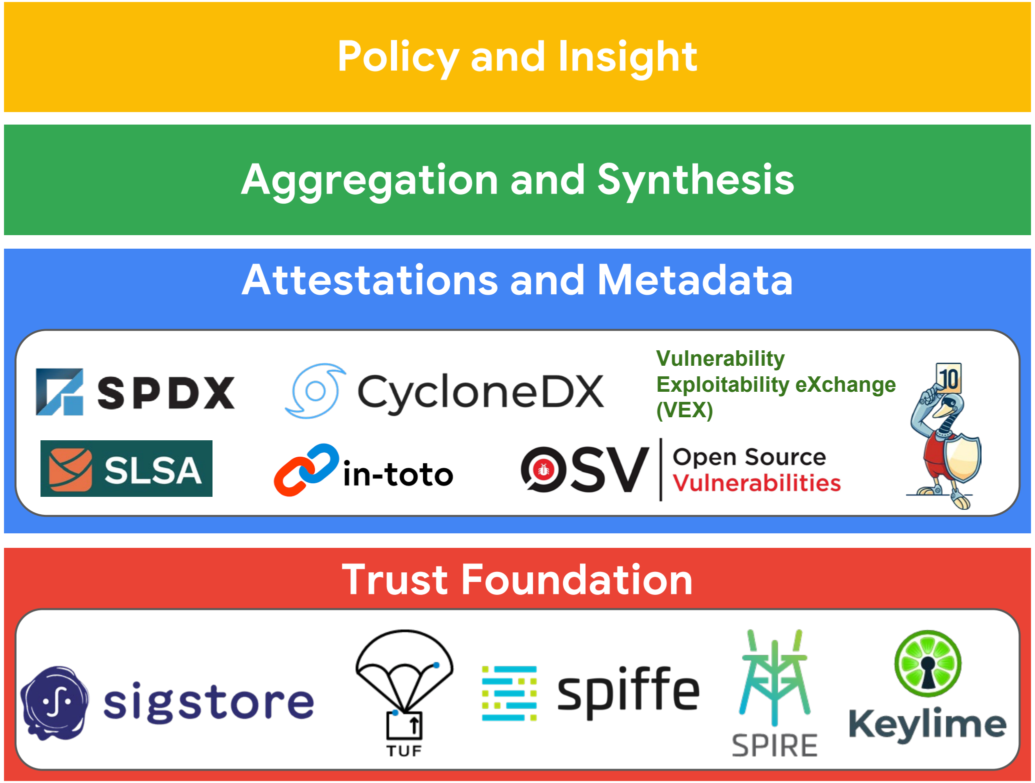
in-toto

SBOM
Software Bill of Materials

SPDX

SBOM
Software Bill of Materials
CycloneDX
SPDX
in-toto
SLSA
???

GUAC is here!



Policy and Insight

Automation and compliance throughout the SDLC

Aggregation and Synthesis

Intelligent aggregation across artifacts and identities

Attestations and Metadata

SPDX
CycloneDX
Vulnerability Exploitability eXchange (VEX)
10
SLSA
in-toto
OSV
Open Source Vulnerabilities

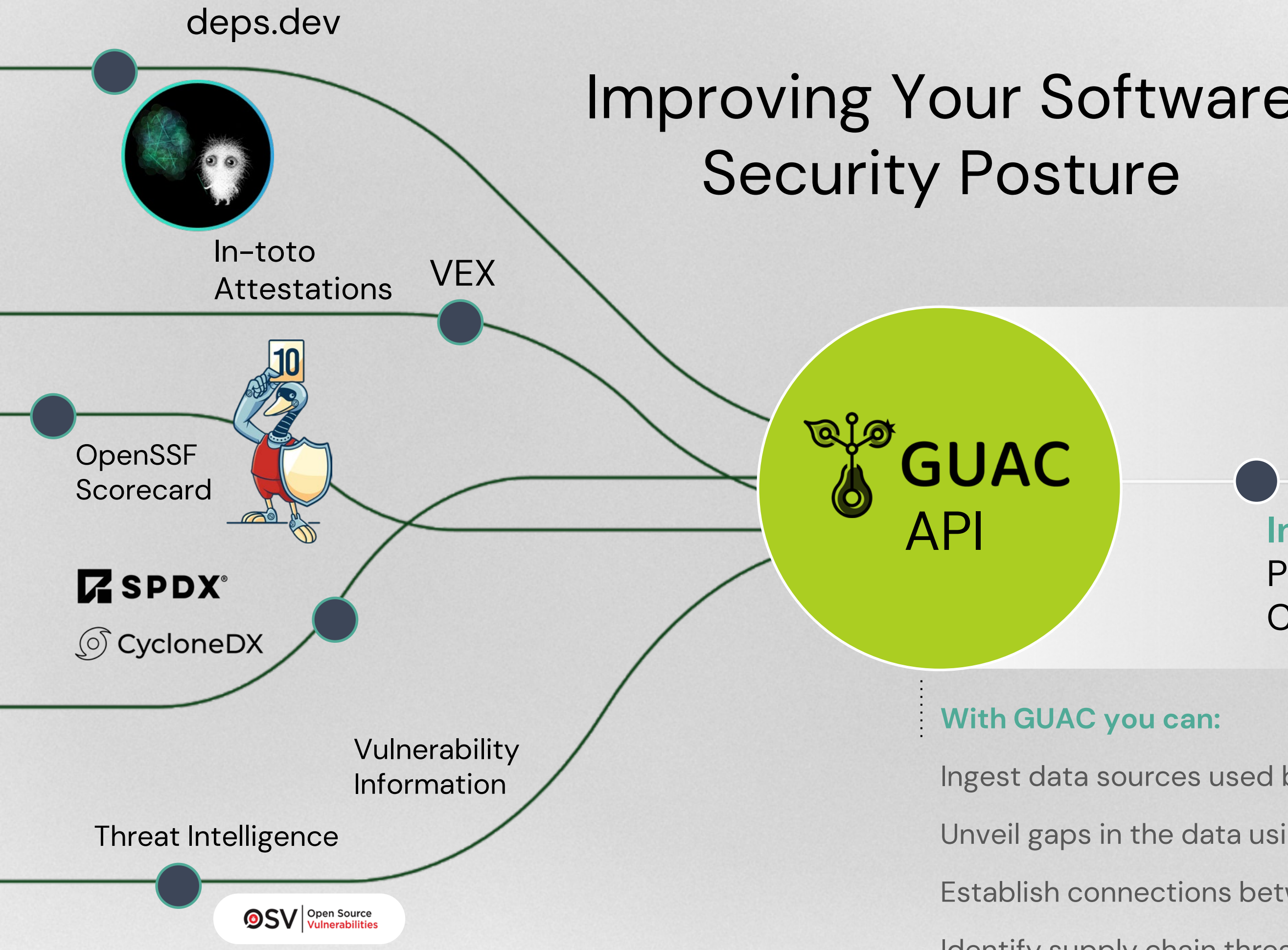
Schemas and sources for rich security metadata

Trust Foundation

sigstore
TUF
spiffe
SPIRE
Keylime

A decentralized, flexibly anchored trust fabric

Improving Your Software Security Posture



Insights for Policy Checks, Patch Planning, Identifying Critical Infrastructure

With GUAC you can:

Ingest data sources used by your organization

Unveil gaps in the data using other data sources

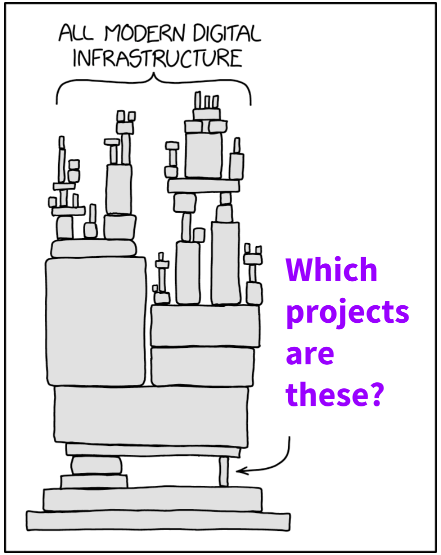
Establish connections between your software catalog

Identify supply chain threats, enable remediation

What Supply Chain questions?

Proactive

How do I prevent large scale supply chain compromises?



Which projects are these?

https://xkcd.com/2347/

Preventive

Have I taken the right safeguards?

When deciding to use and deploy software, are there sufficient security checks and approvals?

SLSA

aqua trivy

grype

Reactive

HOW AM I AFFECTED???

A vulnerability or supply chain compromise is discovered!

+ Codecov, Solarwinds compromises

Latest Updates

- GUAC is an OpenSSF Incubating Project
- Latest release is 0.7.0 with full support for PostgreSQL, allowing persistent backend storage as well as several pagination features + reading from a directory inside an S3 bucket
- 300+ members, 50+ contributors
- Technical and non-technical involvement is welcome!

- Active OpenSSF Slack channel #guac
- Community calls are the 3rd Thursday of every month - next one is June 20
- Learn more → www.guac.sh

Active Users:

Adobe
AWS
Bloomberg
Cisco
ClearAlpha
GitHub
Google
Guidewire
Intel
Kusari
VMware
Yahoo!

Insights from a GUAC User: Guidewire

Umang Jain

About Guidewire

- Guidewire Software is NYSE listed enterprise, based in the San Mateo, CA and a recognized leader in InsurTech.

- Our customers -Property and Casualty insurers, rely on our cloud platform which has been tailored to run their unique business and analytics applications.

- Guidewire Cloud Platform (GWCP) runs more than 10,000 workloads on AWS with applications focusing on Policy, Billing & Claims Management, and plethora of other services that are constantly being discovered in our interactions with customers.

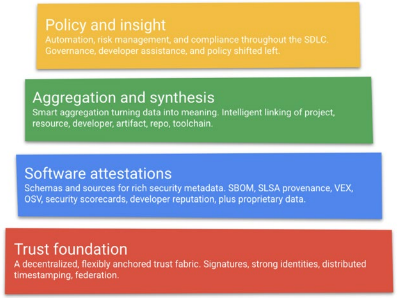
- Within Guidewire, we are the Platform Engineering team with the responsibility to provide a secure and scalable Internal Development Platform to power Guidewire Products and Services that our customers love.

Why Guidewire uses GUAC

- **Software Supply Chain attacks** continue to be on a rise and all responsible Software providers must plan for this emerging threat vector.
- **Internal Developer Platforms need to provide security benefits OOTB.**
- Leveraging **SLSA** to drive evolution of our journey.
- Specifically, we needed a solution in the Aggregation and Synthesis space.
- Started journey using **bespoke** solution, but then pivoted to GUAC as it met most of our needs, aligns with SLSA and was headed in a direction which resonated with us.

Where we are at the moment...

- Focus on demonstrating ability to generate necessary artifacts (SBOM & Provenance) and make it available for decision making against implemented policies.
- Integrate the solution seamlessly with our evolving GWCP Platform.



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

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

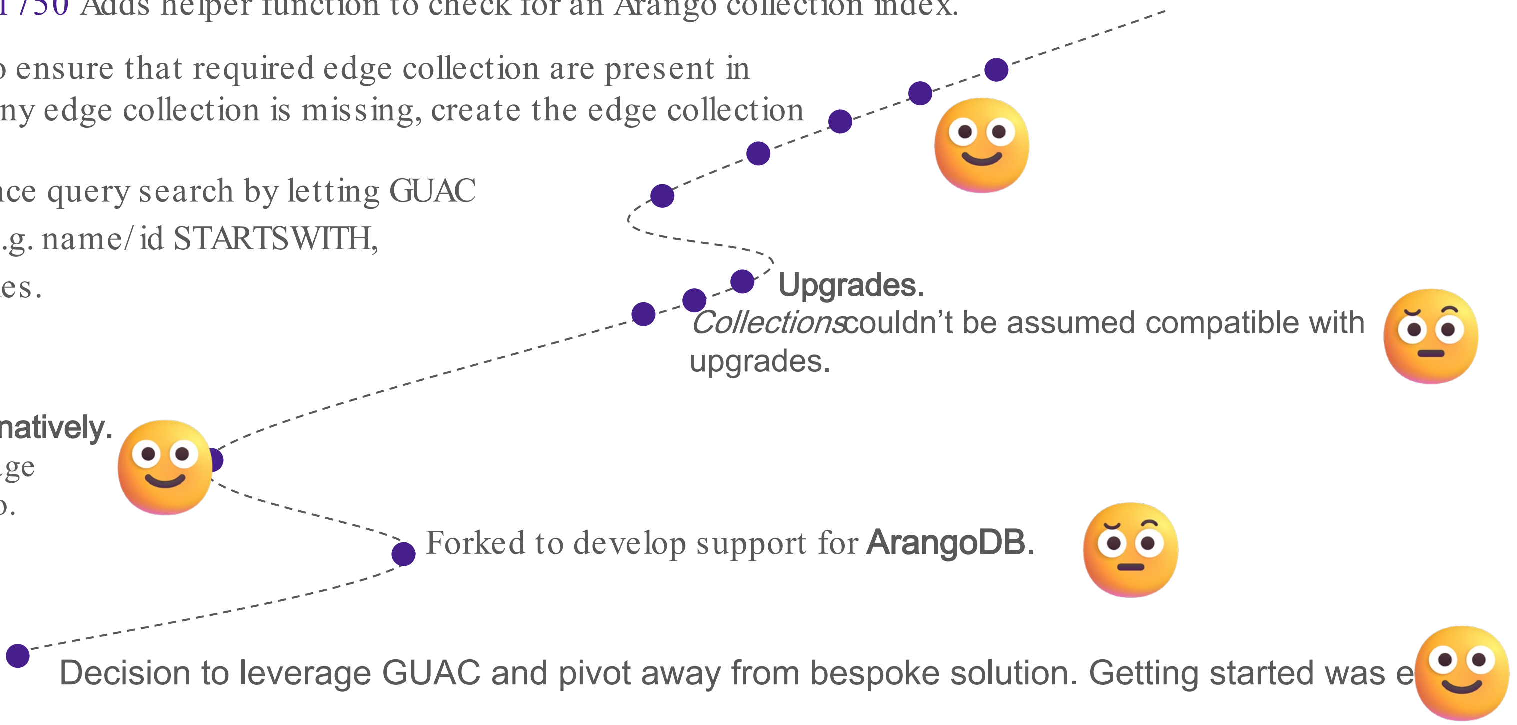
Software attestations
Schemas and sources for rich security metadata. SBOM, SLSA provenance, VEX, OSV, security scorecards, developer reputation, plus proprietary data.

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

- **Next**: Focus on leveraging insights from GUAC to proactively identify and surface risks for corrective actions.

https://security.googleblog.com/2022/10/announcing-guac-great-pairing-with-slsa.html

Working with GUAC..



#1750 Adds helper function to check for an Arango collection index.

#1649 Adds the check to ensure that required edge collection are present in ArangoDB graph and if any edge collection is missing, create the edge collection

#1618 and #1610 enhance query search by letting GUAC users set filter criteria (e.g. name/id STARTSWITH, CONTAINS) in their queries.

Upgrades.
Collections couldn't be assumed compatible with upgrades.

GUAC supports **ArangoDB natively.** Dropped the fork and leverage native GUAC SDK for Arango.

Forked to develop support for **ArangoDB.**

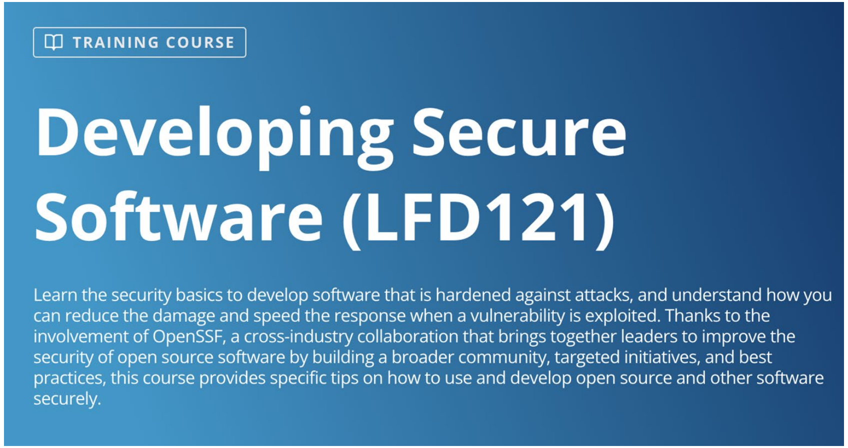
Decision to leverage GUAC and pivot away from bespoke solution. Getting started was e

Panel Discussion & Audience Q&A

Developing Secure Software (LFD121)

OpenSSF
OPEN SOURCE SECURITY FOUNDATION

The “Developing Secure Software” (LFD121) course is available on the Linux Foundation Training & Certification platform. It focuses on the fundamentals of developing secure software. Both the course and certificate of completion are free. It is entirely online, takes about 14-18 hours to complete, and you can go at your own pace. Those who complete the course and pass the final exam will earn a certificate of completion valid for two years.



TRAINING COURSE

Developing Secure Software (LFD121)

Learn the security basics to develop software that is hardened against attacks, and understand how you can reduce the damage and speed the response when a vulnerability is exploited. Thanks to the involvement of OpenSSF, a cross-industry collaboration that brings together leaders to improve the security of open source software by building a broader community, targeted initiatives, and best practices, this course provides specific tips on how to use and develop open source and other software securely.

Upcoming Events

OpenSSF
OPEN SOURCE SECURITY FOUNDATION

SOSS Fusion Conference

When: October 22-23, 2024

Where: Atlanta, Georgia

Call for Proposals & Registration are open!

LF Open Source Summit Europe + SOSS Community Day Europe

When: September 16-18, 19 (SOSS Community Day), 2024

Where: Vienna, Austria

https://events.linuxfoundation.org/open-source-summit-europe/register/

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

Engage with us on social media

X
@openssf

LinkedIn
OpenSSF

Mastodon
social.lfx.dev/@openssf

YouTube
OpenSSF

Facebook
OpenSSF

OpenSSF
OPEN SOURCE SECURITY FOUNDATION

Subscribe to our mailing list

openssf.org/sign-up

Is your organization a member?

Questions? Contact membership@openssf.org

openssf.org/join

Thank You

Take our quick Tech Talk Survey

https://zoom.us/webinar/register/WN_jxAYJJieTVel2bdwzd3Aag

OpenSSF

OPEN SOURCE SECURITY FOUNDATION

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.