How SLSA Fires Up Your Software Supply Chain Security

Real World Examples

ActiveState

kusari

Housekeeping

- We will be emailing everyone the slides after the webinar
- Submit your questions in the Q&A tab and we will answer at the end

Agenda

- SLSA Levels – Is your level mild, medium or hot?
- The landscape of solutions, ranging from design to container and open source components
- Why SLSA is better with ActiveState and GUAC
- Examples of organizations adopting SLSA
- The SLSA roadmap, with v1.0 focusing on the “build” track and Level 3 attainment
- Demos and Q&A

Introductions

ActiveState

Loreli Cadapan
Chief Product Officer
ActiveState

- Focused on DevOps and DevSecOps, 20+ years in enterprise software at enterprises and startups.
- Held different roles from coding, architecture, development management to product management.
- Currently leads Product team at ActiveState, powering the world's software development teams and accelerating their application security.

Introductions

kusari

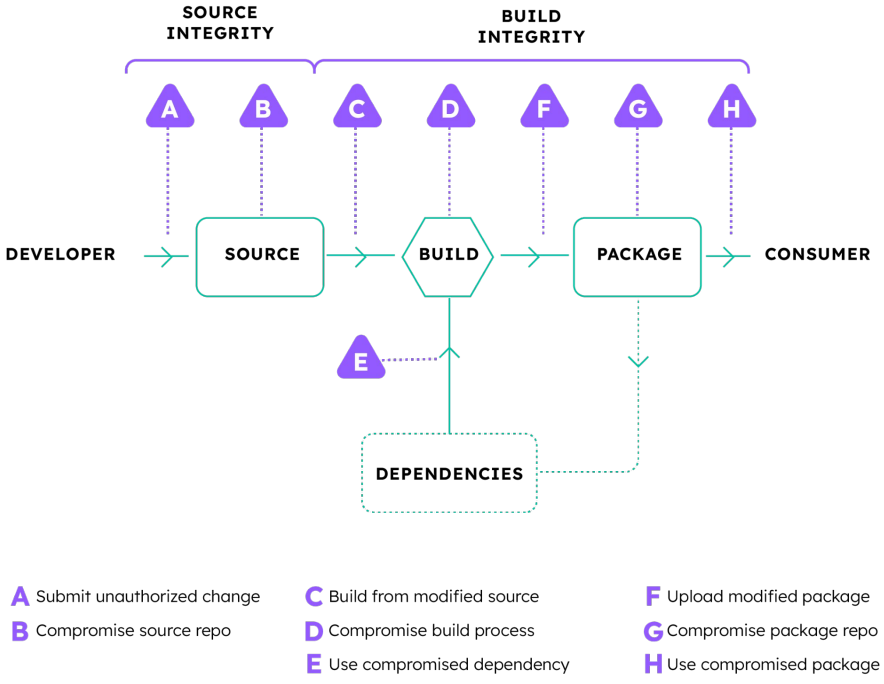
Michael Lieberman

CTO & Co-Founder
Kusari

- His passion is in applying his expertise to use cases where privacy and security are paramount.
- Mostly recently he has been focused on work within the software supply chain security space.
- He is also highly committed to open-source, having co-created projects like GUAC and FRSCA, along with having co-lead white papers like the CNCF's Secure Software Factory Reference Architecture.
- He is an OpenSSF SLSA steering committee member, OpenSSF Technical Advisory Council (TAC) member, tech lead for the CNCF Security Technical Advisory Group (STAG), and formerly co-chaired the CNCF FinServ User Group.

Yet Another Introduction to SLSA

- **SLSA is a Supply Chain Security Framework aimed at the source and build stage of your SDLC**
  - Provenance
  - Build Service Security



Why does SLSA Matter?

How Does SLSA 1.0 Help?

Implementer	Requirement	Degree	L1	L2	L3
Producer	Choose an appropriate build platform		✓	✓	✓
	Follow a consistent build process		✓	✓	✓
	Distribute provenance		✓	✓	✓

Organization and Projects - e.g. Kubernetes, NPM packages, Hello World, etc.

What makes a good SBOM?

- **Document**
  - What is being claimed by the SBOM
    - Complete/Incomplete?
  - Is it compliant with the spec
  - How many layers deep are dependencies specified for
- **Process**
  - Is it part of CI/CD?
  - Is it required for every new release?

How Does SLSA Protect You?

- **SLSA L1 (Mild)**
  - Something is better than nothing
  - Helps with investigation
  - Only as good as the trustworth

How Does SLSA Protect You?

- **SLSA L2 (Medium)**
  - Associates identities and systems with the software
  - Helps prevent attacks against developers and their workstations
  - Helps with understanding where the software was built

How Does SLSA Protect You?

- **SLSA L3 (Hot)**
  - Enforces security at the individual builds
  - Helps prevent attacks against the build systems
  - Provides granular identities that can be tied back to an individual build
  - A compromise of a single build can't compromise other builds on the same system

How Does SLSA 1.0 Help?

Implementer	Requirement	Degree	L1	L2	L3
Build platform	Provenance generation	Exists	✓	✓	✓
		Authentic		✓	✓
		Unforgeable			✓
	Isolation strength	Hosted		✓	✓
		Isolated			✓

Build Systems - e.g. FRSCA, Github Actions, Gitlab CI, Jenkins, etc.

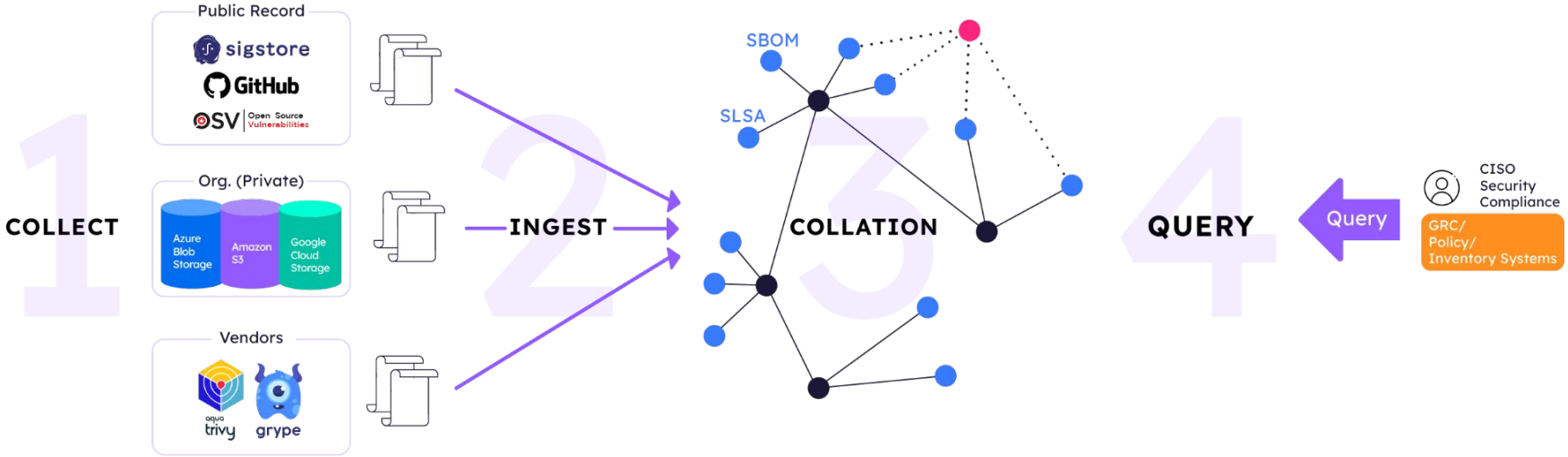
Landscape of Software Supply Chain Security Solutions

- Static application security testing (SAST)
- Software Composition Analysis (SCA)
- Dynamic Application Security Testing (DAST)
- Policy Management
- Trusted Build Service (e.g. SLSA)
- Supply Chain Analysis / Observability

Why SLSA is Better with ActiveState

- **Trusted vendor for your open source dependencies**
  - Built using SLSA L3 requirements
  - Vulnerability and License compliance
  - Complete and up-to-date SBOM and attestations
- **Observability**
- **Scalability**
  - Ensure compatibility in all your open source dependencies
  - Reproducible and shareable environments
- **Rapid Remediation**
  - Vulnerability reports
  - Fearless dependency updates

Why SLSA is Better with GUAC



Examples of Organizations Adopting SLSA

- **Google**
- **Samsung**
- **CNCF**
  - Various projects including Kubernetes
- **Github**
  - NPM

SLSA Roadmap

- **New Tracks!**
  - Source
  - Dependencies
  - Build System

- **Where's SLSA Level 4???**
  - Come help us define it!

- **Tools**
  - Come integrate your tool with SLSA and join the SLSA tooling SIG!

Kusari & ActiveState Better Together

- **Your open source dependencies are built from source by ActiveState**
  - Comprehensive SBOM
  - Provenance Attestation
  - Composition Analysis complete with CVE and License information
- **Complete, holistic view of your software supply chain security through Kusari**
  - GUAC
  - Complete SDLC integration

kusari & ActiveState

Better Together

Demos

Q&A

Next Steps

Schedule a demo with our product experts:
www.activestate.com/solutions/contact-sales/

Take our Supply Chain Security Survey & find out how you rate:
https://www.surveymonkey.com/r/BNGZPH6

Try the ActiveState Platform for free:
https://platform.activestate.com/

Come check out GUAC, it's open source!:
https://guac.sh/

Learn more about how Kusari can help secure your software supply chain:
https://kusari.dev

ActiveState

Thank You!