ActiveState

The Frontline of Attack

Securing Your Python, Perl and Tcl Supply Chains

About ActiveState

ALTAIR GILEAD MSC Software MOODY'S Honeywell

DXC.technology STATE STREET Mentor A Siemens Business druva zenoss Own IT.

Used by Millions of Developers and 97% of Fortune 1000

20+ Years of Open Source Language Experience

ActiveState

Introductions

Pete Garcin

Director of Product

Dana Crane

Product Marketing Manager

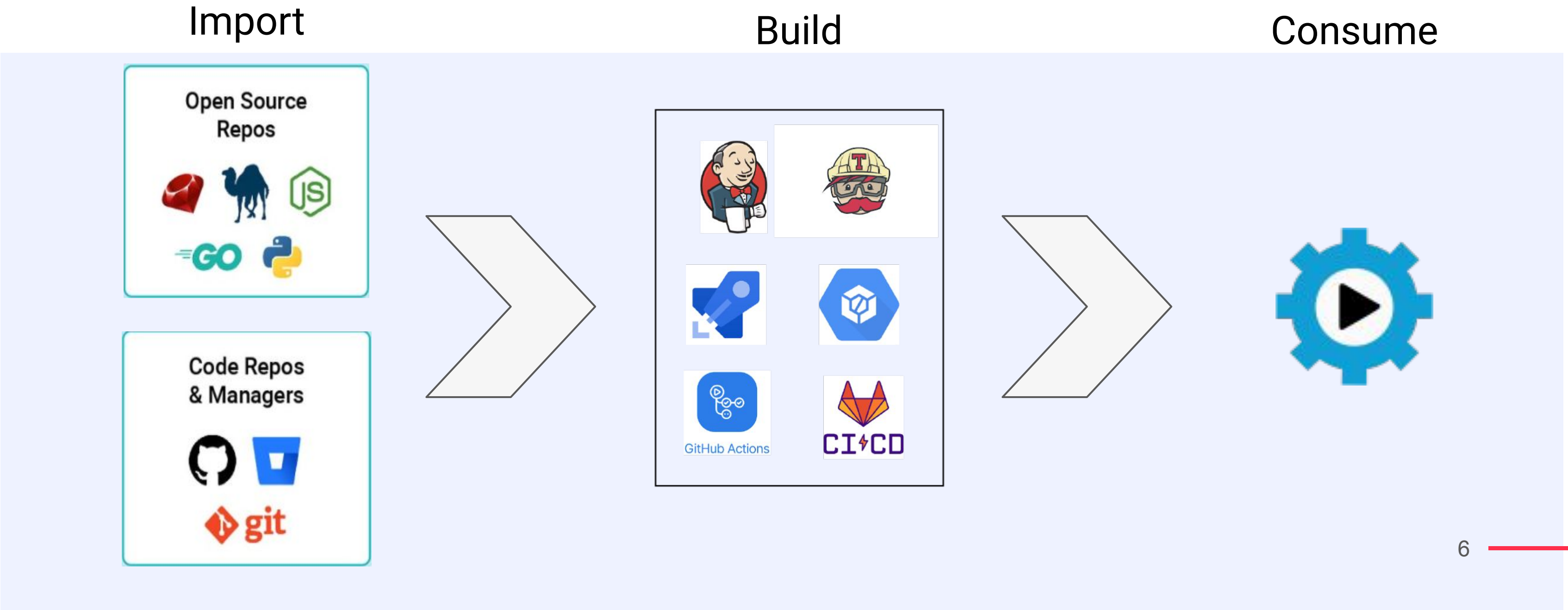
Housekeeping

- Ask questions in the Q&A tab
- There will be a poll midway through and a survey afterwards - your feedback is valuable
- Recording of this will be available and sent to you

Agenda

- Supply Chain Security Threats
- The ActiveState Platform as your out-of-the-box supply chain solution

What is the Open Source Supply Chain?



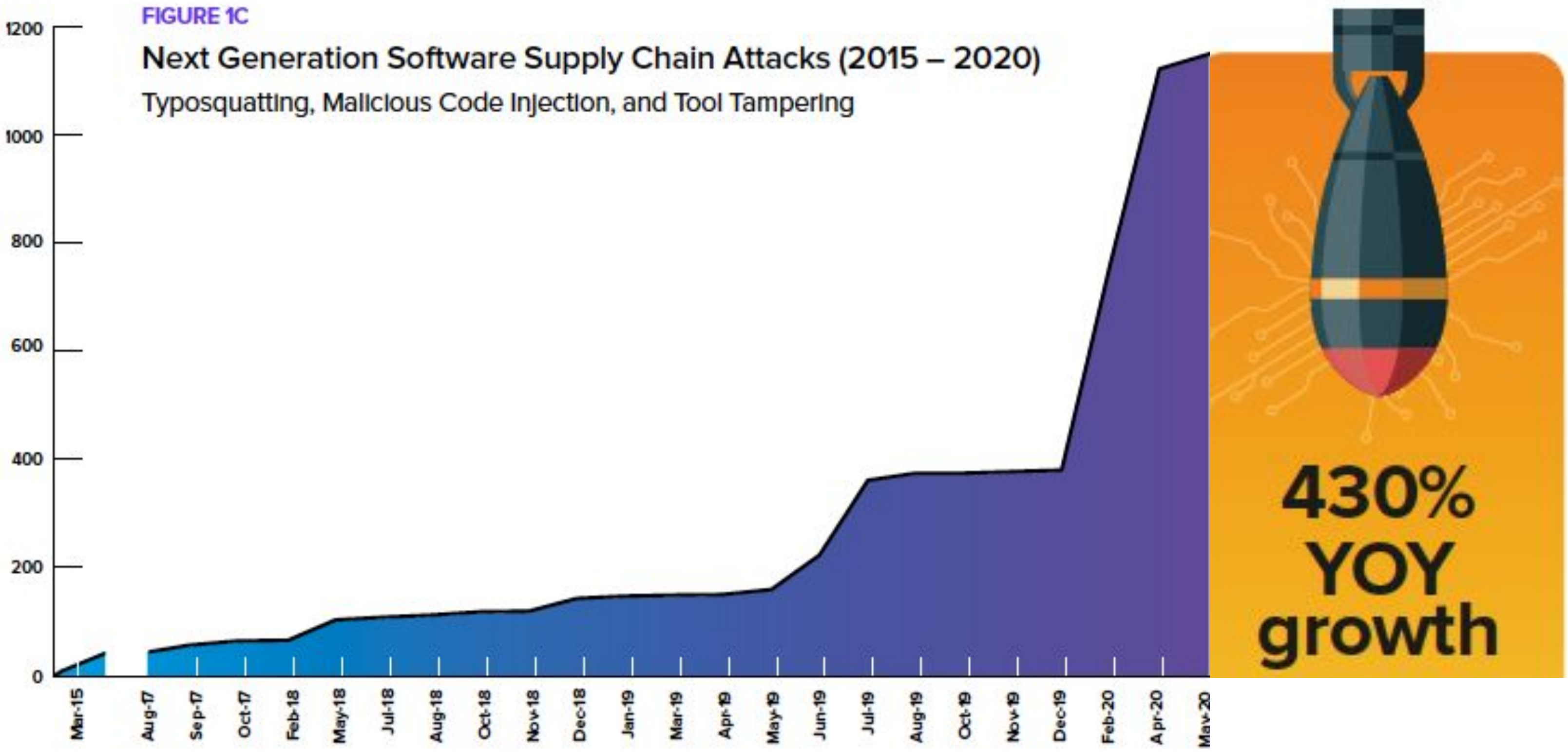


FIGURE 1C

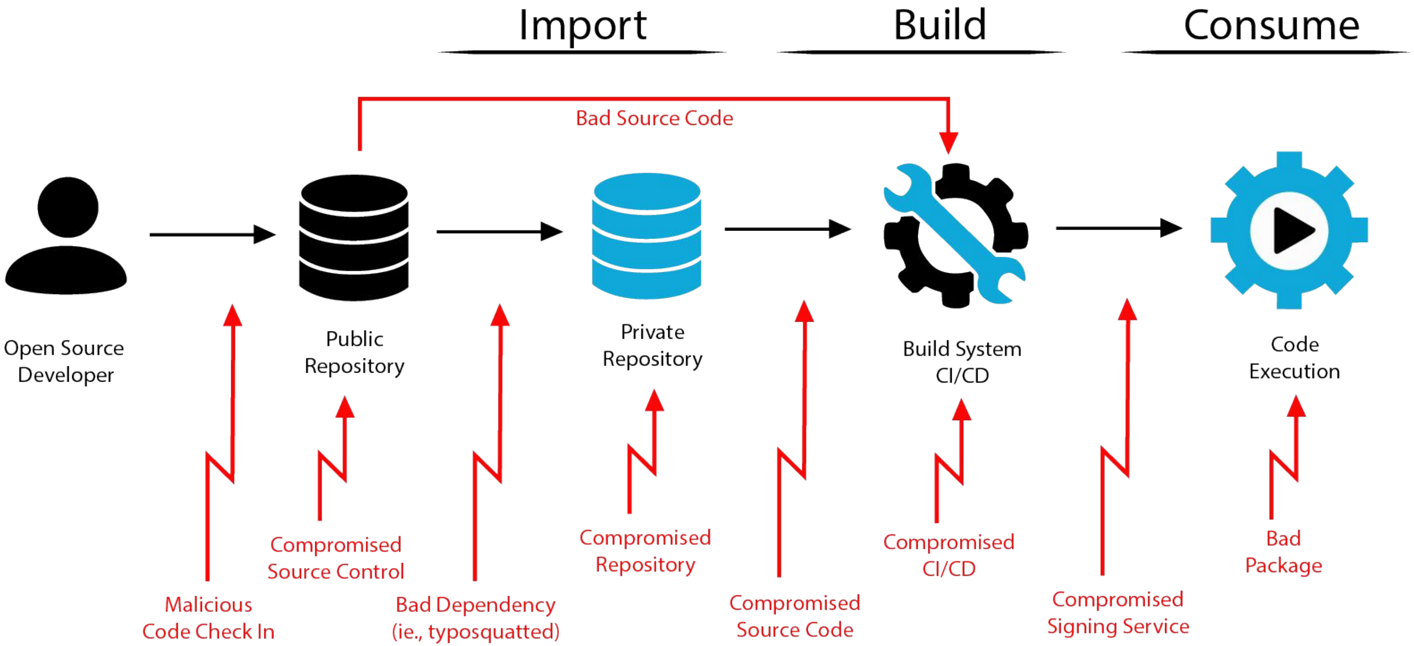
Next Generation Software Supply Chain Attacks (2015 – 2020)

Typosquatting, Malicious Code Injection, and Tool Tampering

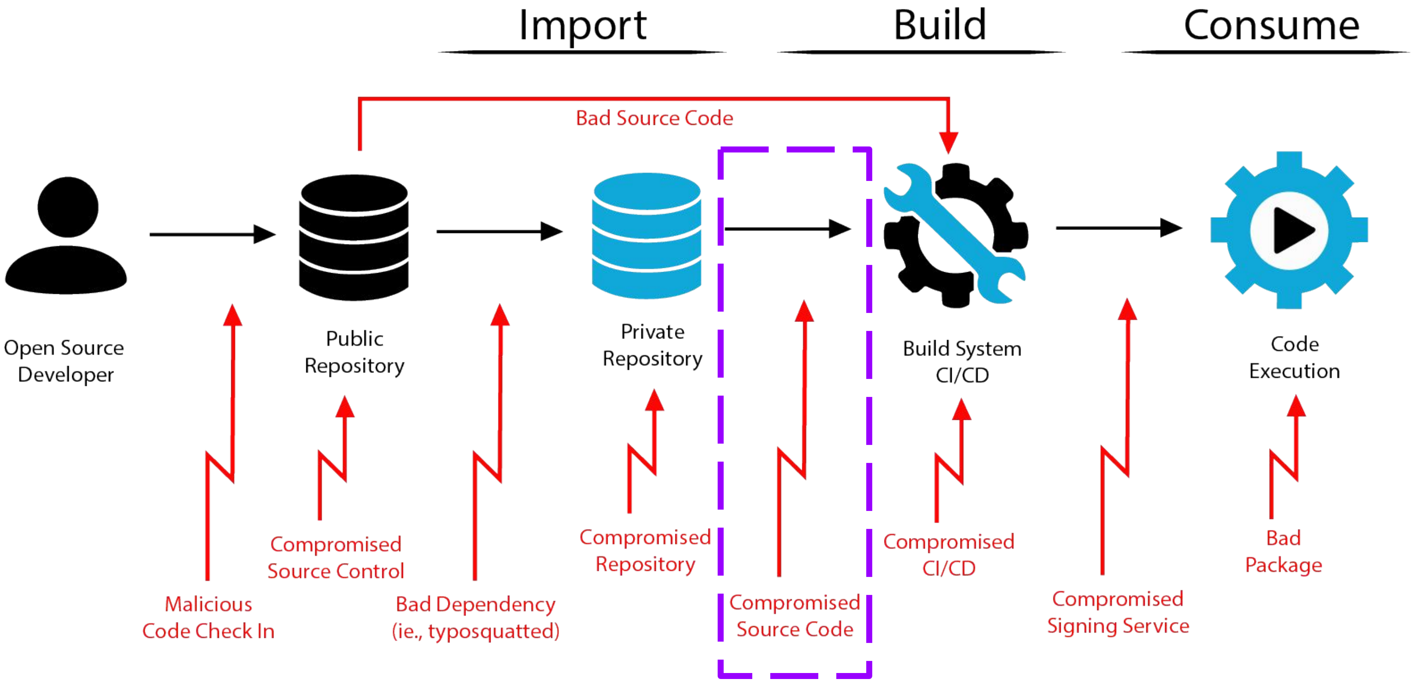
Source: Sonatype State of the Software Supply Chain 2020

ActiveState

Supply Chain Susceptibility

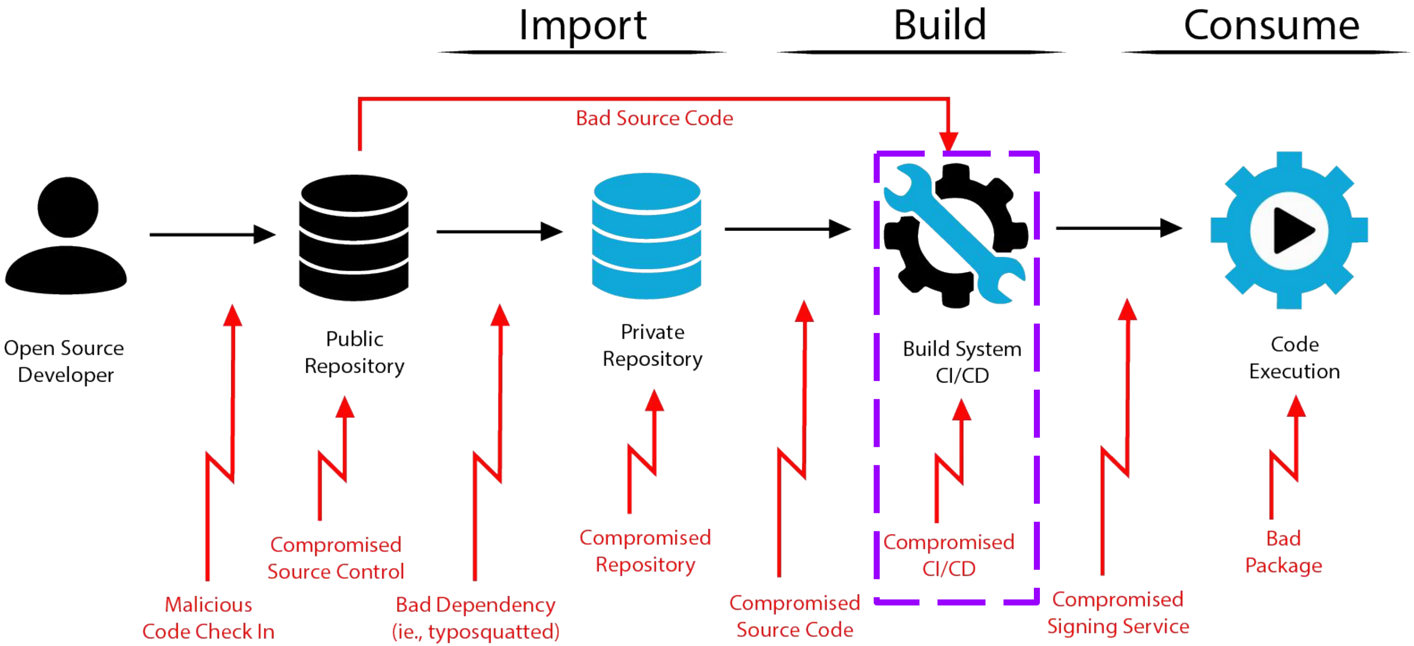


Supply Chain Susceptibility



ActiveState

Supply Chain Susceptibility



President Biden's Executive Order

Software vendors must adopt open source security best practices, including:

- A **software Bill of Materials (BOM)** associated with any software purchased by the government.
- A way to check for and automate **vulnerability remediation**.
- **Provenance**, or the ability to be able to identify the origin for all software components.

Government agencies to require best practices from vendors by Oct. 22.

Poll: How do you currently import, build and consume open source?

Supply Chain Security Survey

How mature is your supply chain security? Assess your current open source security and integrity controls by taking our quick, 8-question survey.

Import	Build	Consume
50% Implicitly trust the public repo	50% do not build packages from source code	80% work with at least some signed packages ✓
30% trust the vendor-supplied ecosystem ✓	50% build at least some packages from source code ✓	20% do not work with signed packages

Import Threats

Threat	Best Practices
Typosquatting	Check timestamp of submission Check revision history
Author Impersonation	Validate identify of uploaders & reviewers
Dependency Confusion	Validate URL / immutable reference

Consider implementing a quarantine

Build Threats

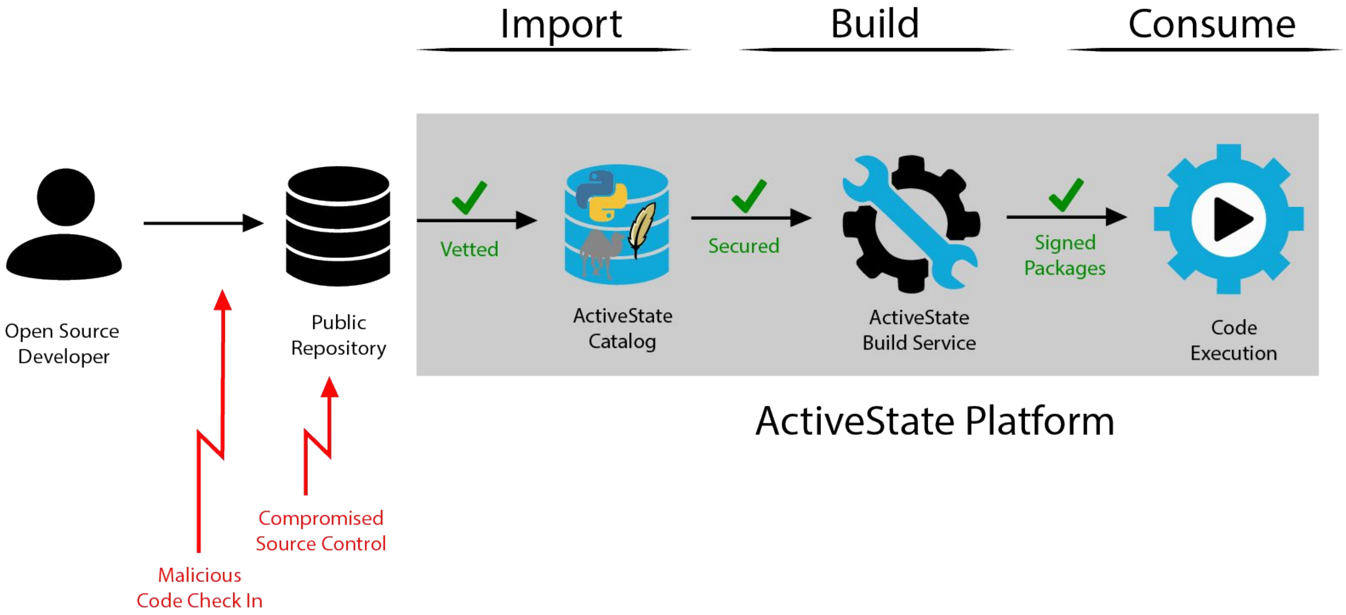
Threat	Best Practices
Malicious build/ install scripts	Scripted builds with no manual intervention
Unconstrained packages	A secure build service (as opposed to a developer's machine)
Dynamic packages that include remote resources	Ephemeral, isolated and hermetic (i.e. no network access) environments for each build step

Verifiably reproducible builds in which provenance can be established for each artifact

Consume Threats

Threat	Best Practices
Compromised Prebuilt Binaries	Build from source and sign all packages

ActiveState Platform

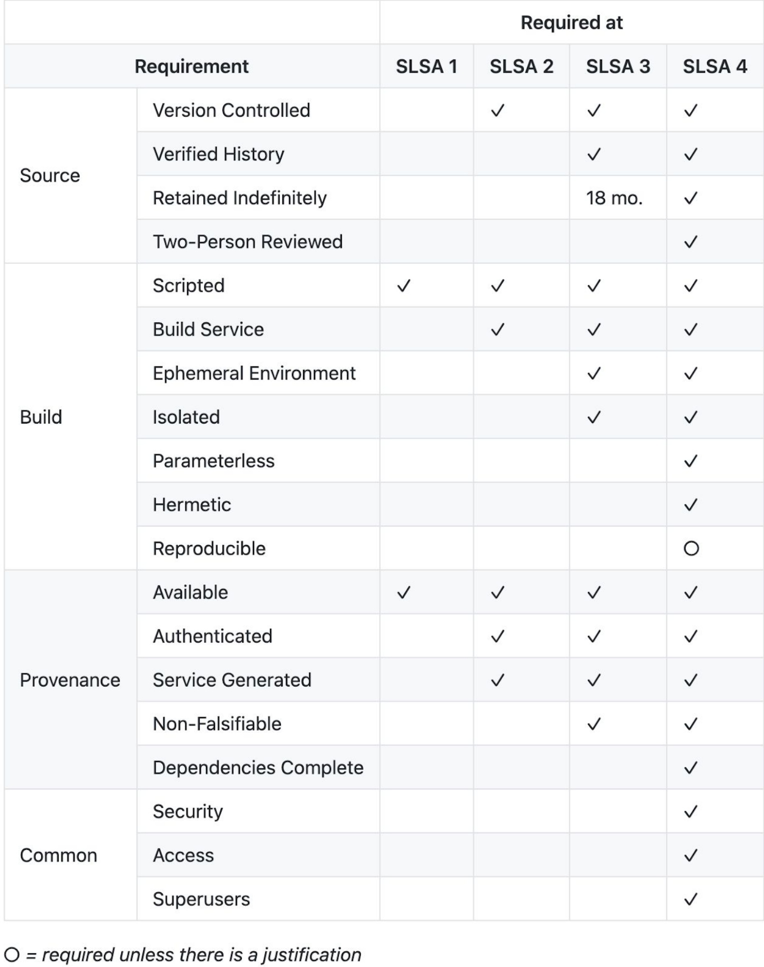


What does it mean to be secure?

- Google developing SLSA (Supply Chain Levels for Software Artifacts) framework
- Define elements required for your supply chain to be secure -- includes different levels of compliance
- Designed with open source in mind, based on Google's internal security practices

ActiveState

SLSA Levels



		Required at			
Requirement		SLSA 1	SLSA 2	SLSA 3	SLSA 4
Source	Version Controlled		✓	✓	✓
	Verified History			✓	✓
	Retained Indefinitely			18 mo.	✓
	Two-Person Reviewed				✓
Build	Scripted	✓	✓	✓	✓
	Build Service		✓	✓	✓
	Ephemeral Environment			✓	✓
	Isolated			✓	✓
	Parameterless				✓
	Hermetic				✓
	Reproducible				○
Provenance	Available	✓	✓	✓	✓
	Authenticated		✓	✓	✓
	Service Generated		✓	✓	✓
	Non-Falsifiable			✓	✓
	Dependencies Complete				✓
Common	Security				✓
	Access				✓
	Superusers				✓

○ = *required unless there is a justification*

Achieving SLSA Compliance

- Google states that, “... can take years to achieve the highest levels of SLSA compliance”, but the ActiveState Platform can get your Python (or Perl) supply chain to high levels of compliance much faster.

Major Elements

- Version Controlled
- Hermetic / Isolated Ephemeral Builds
- Reproducible Builds
- Dependencies Complete Provenance
- Access Controlled System
- Authenticated Provenance

Major Elements

- Version Controlled → **History**
- Hermetic / Isolated Ephemeral Builds → **Cloud Infrastructure**
- Reproducible Builds → **Version Control System (Commits)**
- Dependencies Complete Provenance → **Solver including C Dependencies**
- Access Controlled System → **SaaS / Role-Based Access Control (RBAC)**
- Authenticated Provenance → **Checksums / Signed**

ActiveState

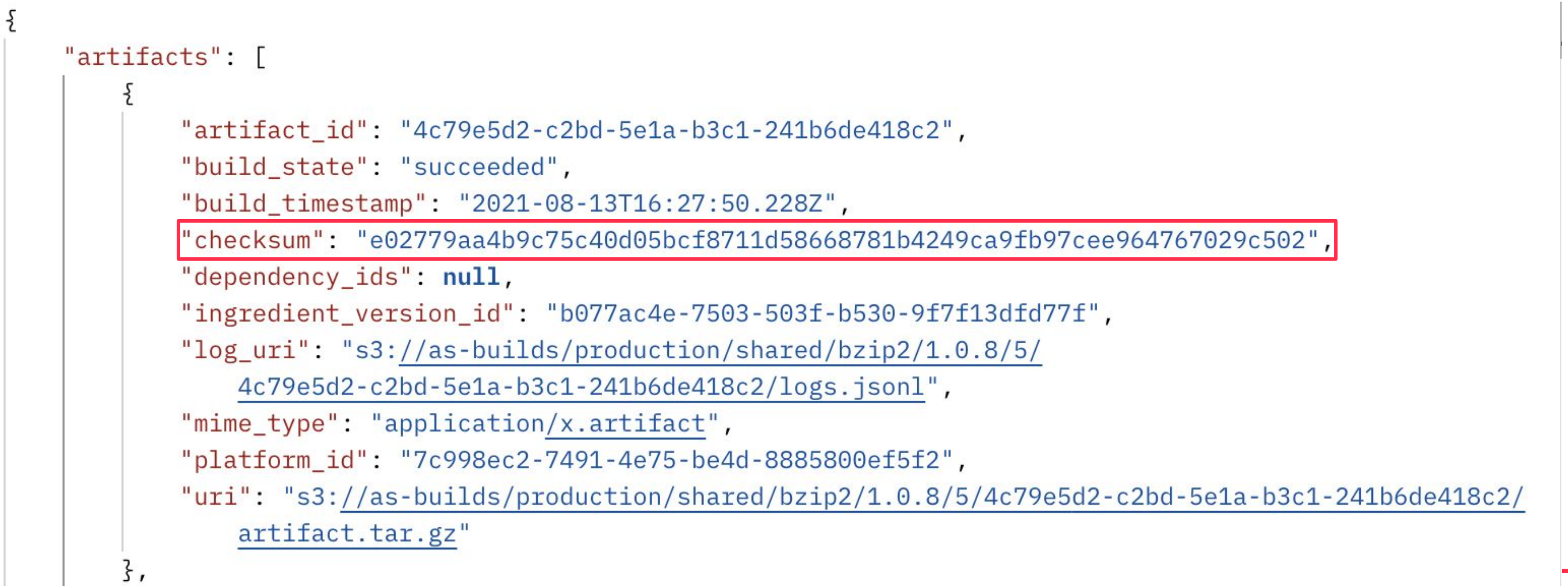
Open Source Supply Chain Security

Platform Demo

Checksums and Signing

- Signed Executables and DLLs
- Checksums for all artifacts in the system
- Accessible via the API
- Coming Soon: State Tool Integration, Digitally Signed Checksums

Checksums and Signing



```
{
    "artifacts": [
        {
            "artifact_id": "4c79e5d2-c2bd-5e1a-b3c1-241b6de418c2",
            "build_state": "succeeded",
            "build_timestamp": "2021-08-13T16:27:50.228Z",
            "checksum": "e02779aa4b9c75c40d05bcf8711d58668781b4249ca9fb97cee964767029c502",
            "dependency_ids": null,
            "ingredient_version_id": "b077ac4e-7503-503f-b530-9f7f13dfd77f",
            "log_uri": "s3://as-builds/production/shared/bzip2/1.0.8/5/
                4c79e5d2-c2bd-5e1a-b3c1-241b6de418c2/logs.jsonl",
            "mime_type": "application/x.artifact",
            "platform_id": "7c998ec2-7491-4e75-be4d-8885800ef5f2",
            "uri": "s3://as-builds/production/shared/bzip2/1.0.8/5/4c79e5d2-c2bd-5e1a-b3c1-241b6de418c2/
                artifact.tar.gz"
        },
```

Q&A

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

Book a demo for your team
https://www.activestate.com/get-demo/

Take our Supply Chain Security Assessment
https://www.surveymonkey.com/r/secure-your-supply-chain