ActiveState

SBOM & Attestations

New and Emerging Requirements for Software Vendors

ActiveState

Introductions

Nicole Schwartz

Product Manager

Evan Cole

Solutions Engineer

ActiveState

Software Supply Chain Attacks

ActiveState

Poll: What do you currently do to secure your software supply chain?

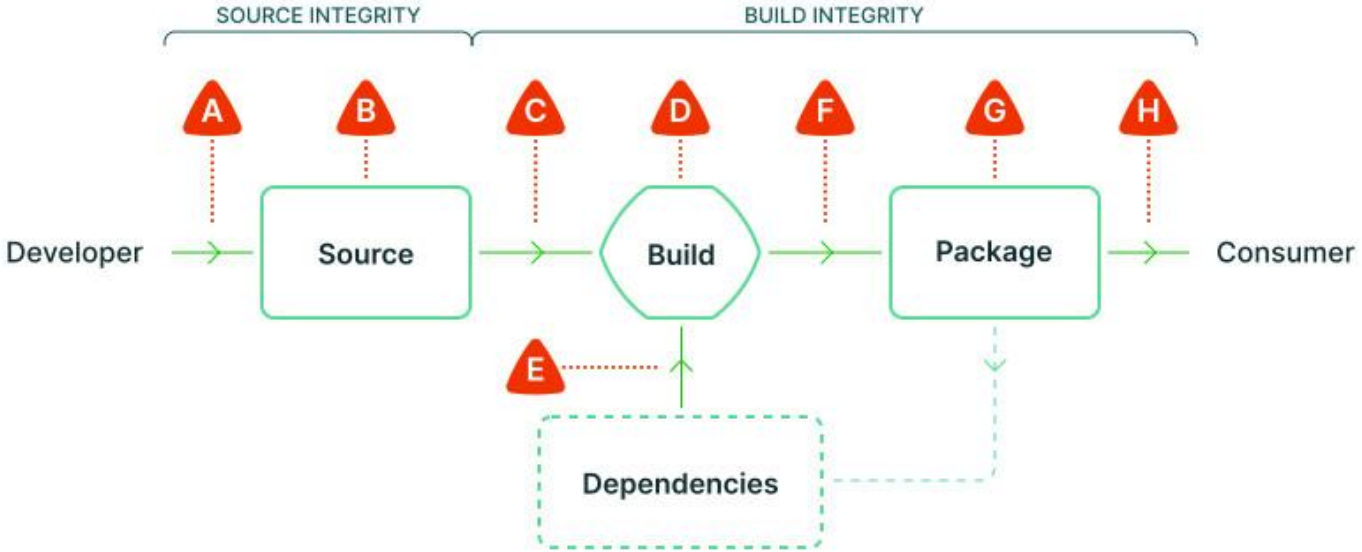
- Check for vulnerabilities (CVEs)
- Consume individually signed software artifacts
- Use 3rd party solutions (SCA, SAST, DAST, etc.)
- Nothing yet, exploring options

ActiveState

Securing the software supply chain requires more than just managing vulnerabilities (CVEs)

ActiveState

Next Gen Supply Chain Threats

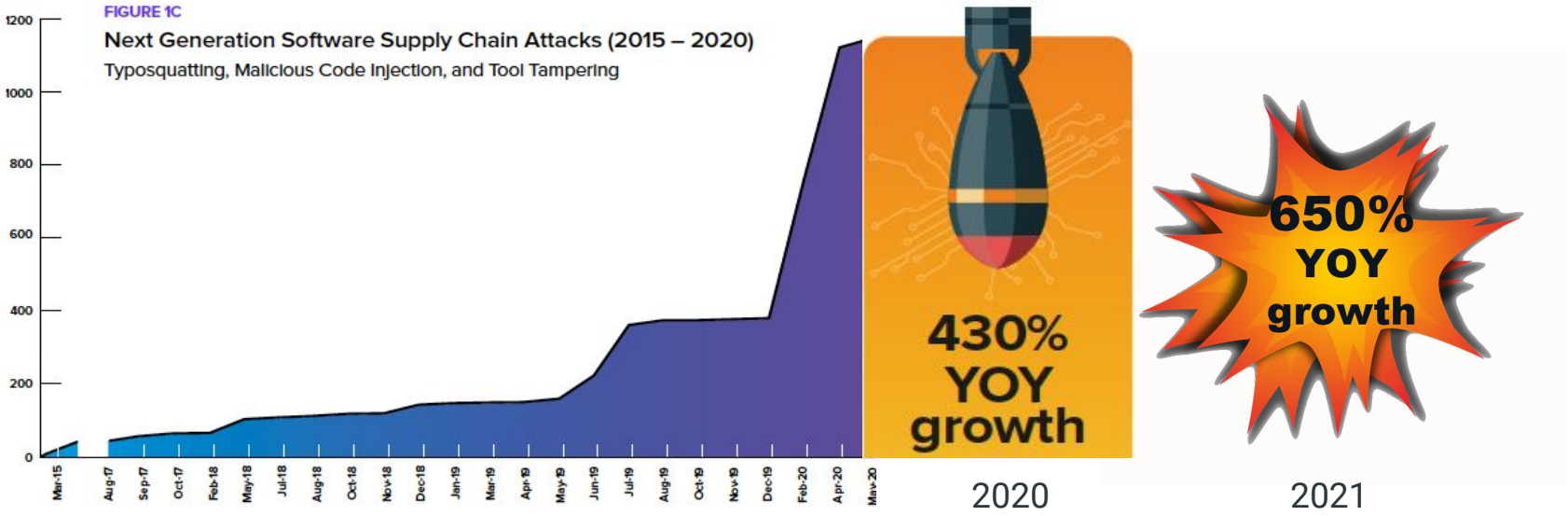


A Submit unauthorized change
B Compromise source repo
C Build from modified source
D Compromise build process
E Use compromised dependency
F Upload modified package
G Compromise package repo
H Use compromised package

Source: SLSA.dev

ActiveState

430% YoY growth in **Next Gen** Supply Chain Threats



Source: [Sonatype State of the Software Supply Chain 2021]

ActiveState

Industry Examples

- Compiler attacks
- Target
- Stuxnet
- ATM malware
- NotPetya / M.E.Doc
- British Airways
- SolarWinds
- Microsoft Exchange Server
- Golden SAML
- Ransomware attacks

ActiveState

Poll: Results

ActiveState

The Response

BRIEFING ROOM

Executive Order on Improving the Nation's Cybersecurity

MAY 12, 2021 • PRESIDENTIAL ACTIONS

By the authority vested in me as President by the Constitution and the laws of the United States of America, it is hereby ordered as follows:

Section 1. Policy. The United States faces persistent and increasingly sophisticated malicious cyber campaigns that threaten the public sector, the private sector, and ultimately the American people's security and privacy. The Federal Government must improve its efforts to identify, deter, protect against, detect, and respond to these actions and actors. The Federal Government must also carefully examine what occurred during any major cyber incident and apply lessons learned. But cybersecurity requires more than government action. Protecting our Nation from malicious cyber actors requires the Federal Government to partner with the private sector. The private sector must adapt to the continuously changing threat environment, ensure its products are built and operate securely, and partner with the Federal Government to foster a more secure cyberspace. In the end, the trust we place in our digital infrastructure should be proportional to how trustworthy and transparent that infrastructure is, and to the consequences we will incur if that trust is misplaced.

ActiveState

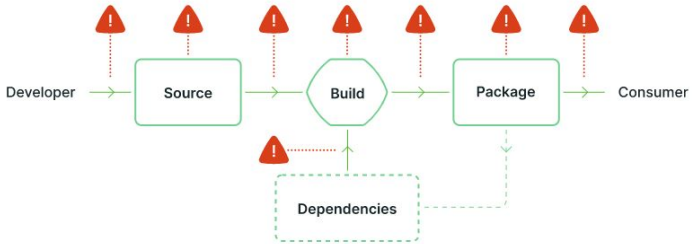
What is SLSA?

Supply chain Levels for Software Artifacts, or SLSA (salsa). It's a security framework, a check-list of standards and controls to prevent tampering, improve integrity, and secure packages and infrastructure in your projects, businesses or enterprises. It's how you get from safe enough to being as resilient as possible, at any link in the chain.

The supply chain problem

Any software can introduce vulnerabilities into a supply chain. As a system gets more complex, it's critical to already have checks and best practices in place to guarantee artifact integrity, that the source code you're relying on is the code you're actually using. Without solid foundations and a plan for the system as it grows, it's difficult to focus your efforts against tomorrow's next hack, breach or compromise.

▶ **More about supply chain attacks**



ActiveState

The Dependency Problem

ActiveState

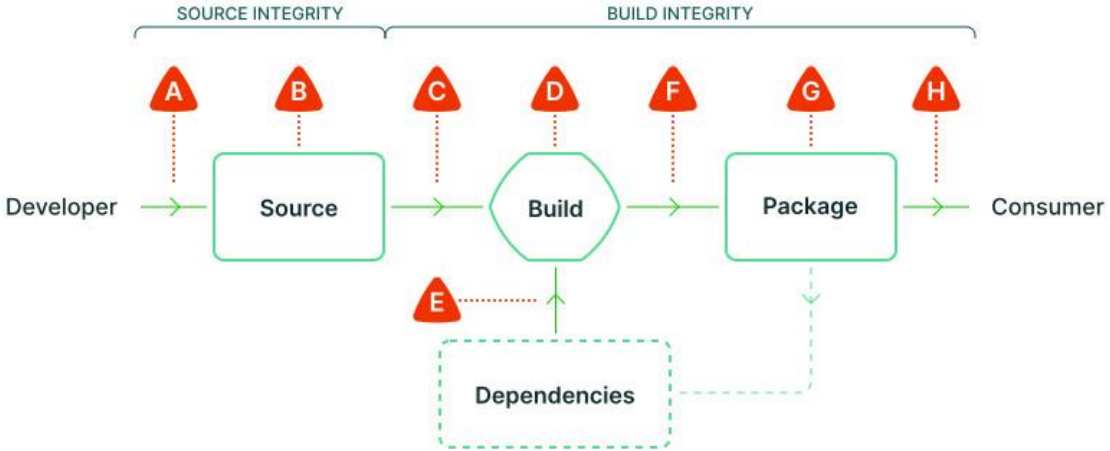
Open Source Dependencies

- Open source components make up >75% of the code in the average app.
- The average app depends on more than 500 components.

VentureBeat Research

ActiveState

Dependency Threats



Source: SLSA.dev

Open Source Dependency Vendors

ActiveState

Software Bill of Materials (SBOMs)

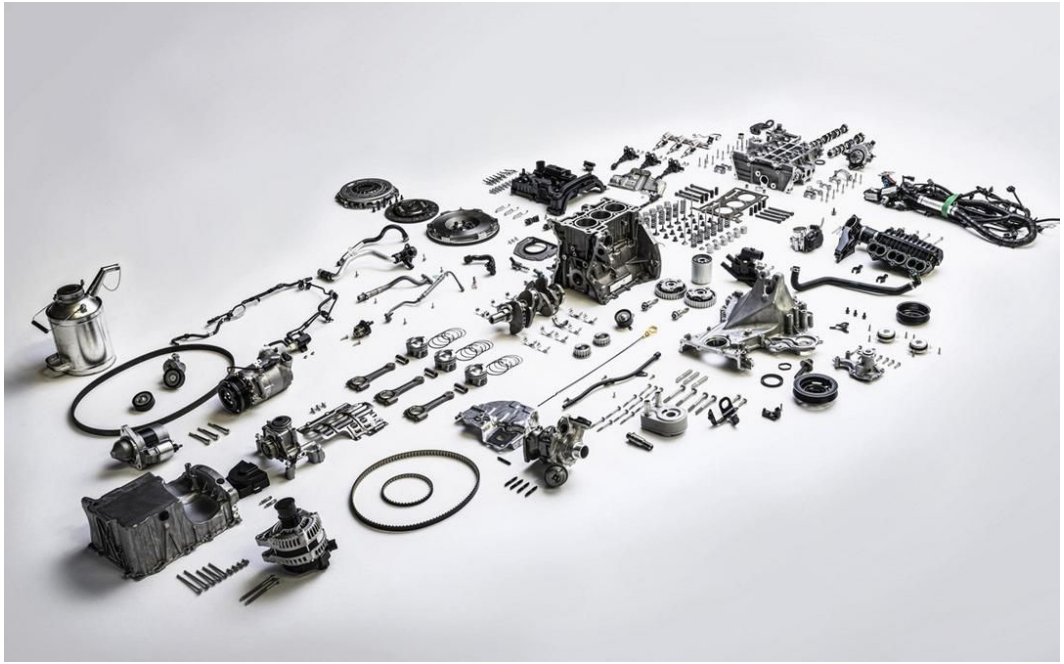
ActiveState

Poll: What is your current experience with SBOMs?

- Checking for vulnerabilities (CVEs)
- Reviewing transitive dependencies
- Supplying to customers for regulatory purposes
- Reviewing open source license utilization
- Reviewing the age of my dependencies
- None of the above

ActiveState

SBOMs - Listing of all the component parts that make up your software



ActiveState

Elements of an SBOM

The Essentials

- Defines the open source libraries/packages/extensions used
- First party (in house code) used
- Versioning , licensing status

Other Aspects:

- Vulnerability information
- External services
- Component checksums (ex SHA-256 hash)
- The entire thing is signed by the provider

ActiveState

SBOM Formats

Government Approved Formats (NIST)

- Software Package Data Exchange
- CycloneDX
- SWID

Common in Industry

- CSV
- JSON

ActiveState

What do you use an SBOM for?

- **Visibility** into all the components that make up a software application.
- **Operational capacity** to resolve vulnerabilities and manage component life cycles (EOL)
- **Automate:** Run the SBOM through a tool (ex. Daggerboard, spdx-to-osv, dependency track) to identify vulnerabilities
- **Provide** as a requirement of regulation to your customers or auditor
- **Request** as a requirement from your software vendors for pre-purchase assurance

ActiveState

Poll: Results

ActiveState

Platform Demo - SBOM

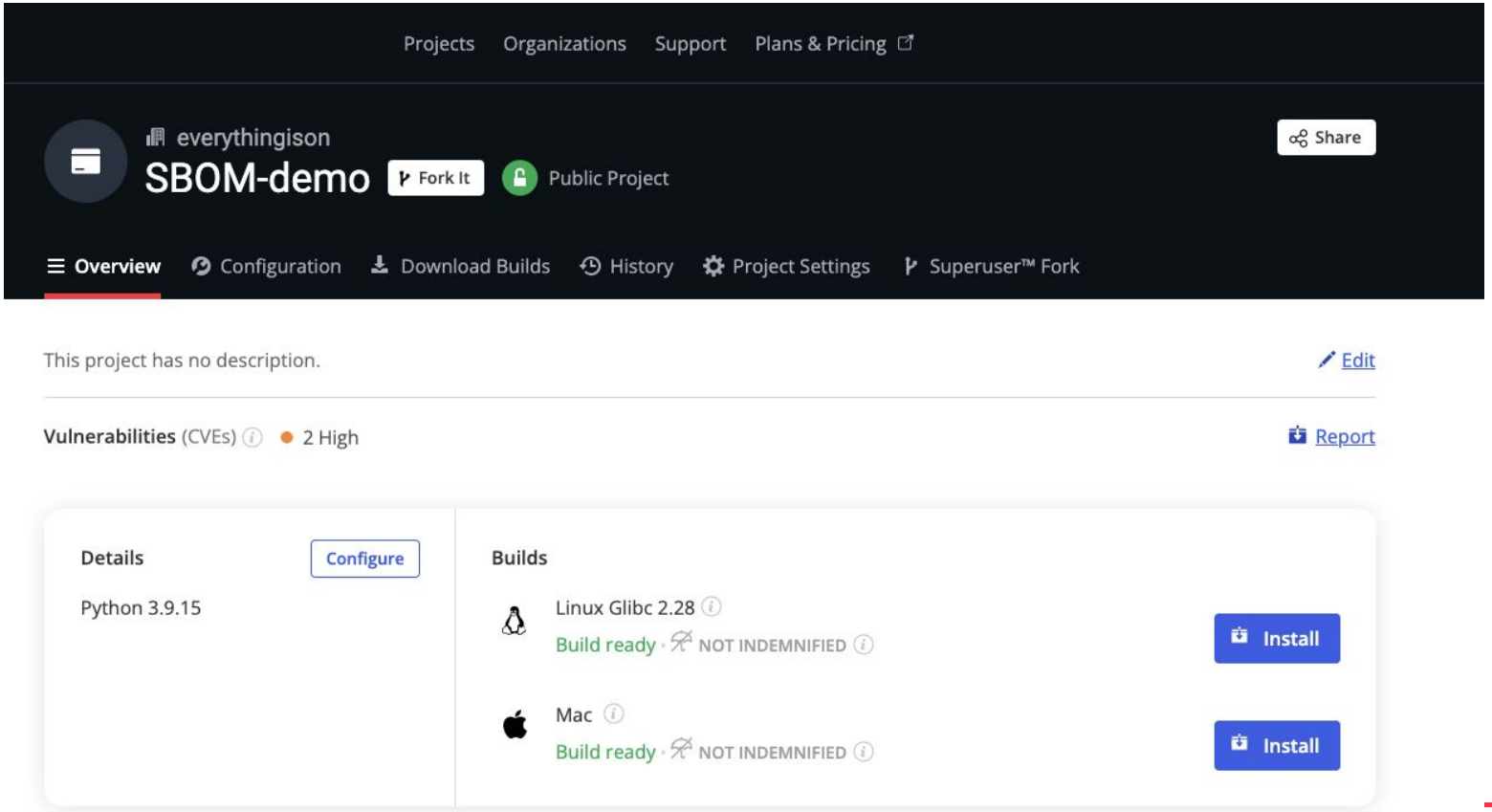
ActiveState

You can do this with a free account today

Documentation: https://docs.activestate.com/platform/projects/sbom/

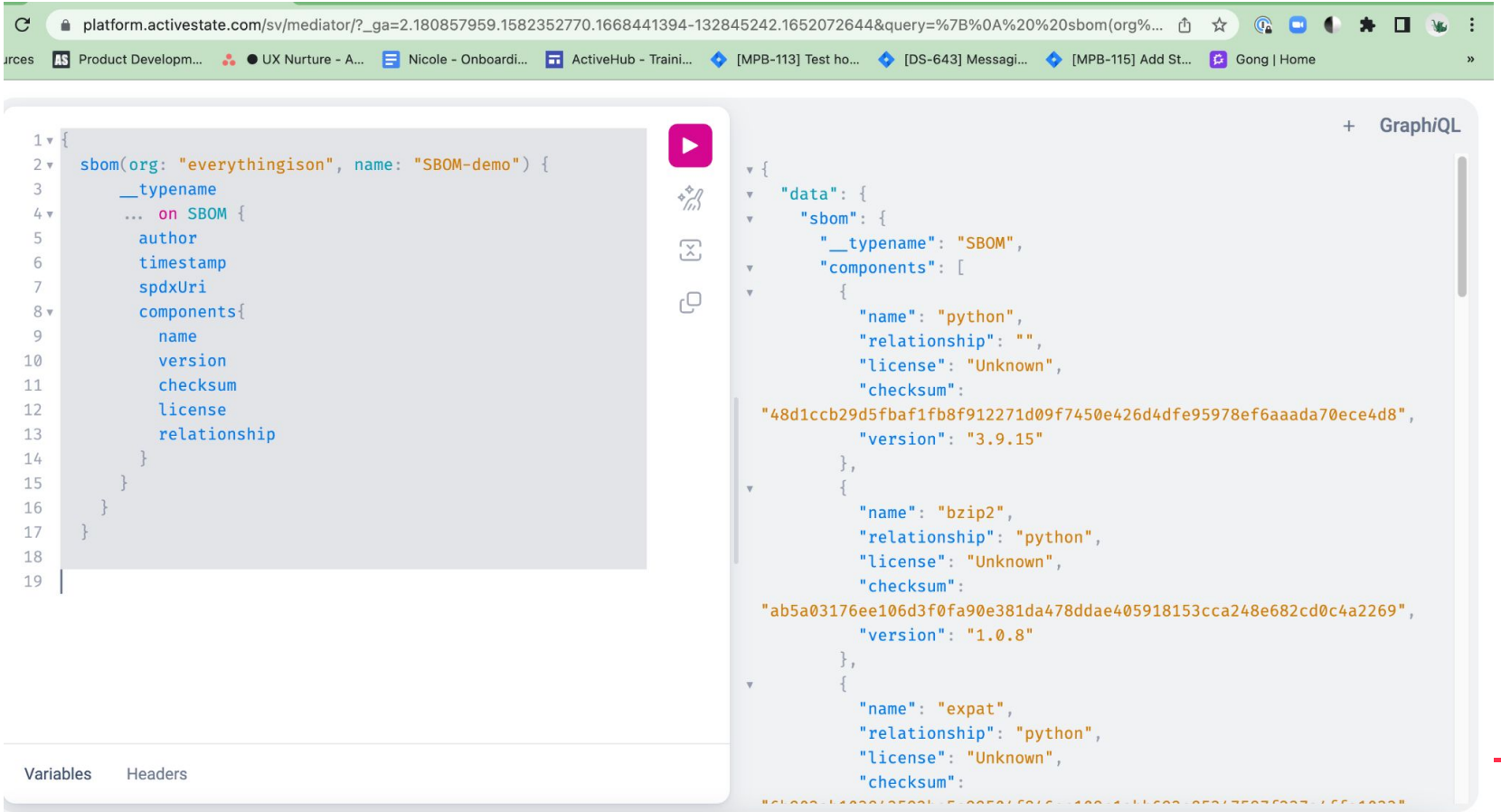
ActiveState

Project



ActiveState

JSON Format



ActiveState

SPDX Format

```
SPDXVersion: SPDX-2.2
DataLicense: CC0-1.0
SPDXID: SPDXRef-DOCUMENT
DocumentName: APEE-534-Microsoft-Rlc-NoPMC-Athnticode
DocumentNamespace: https://platform.activestate.com/download/spdx/ActiveStateBE/APEE-534-Microsoft-Rlc-NoPMC-Athnticode/e73ad540-0072-4d50-845a-03844c0a74fe
Creator: Organization: ActiveState
Created: 2022-06-02T22:31:01Z

PackageName: perl
SPDXID: SPDXRef-perl
PackageVersion: 5.34.0
PackageDownloadLocation: https://dl.activestate.com/source/ed4b2154-eaee-5fba-88bb-d1eca86b1206/versions/0fbbfdd6-68e5-5f06-86ce-b03395e79c54/revisions/5/perl-5.34.0.tar.gz
FilesAnalyzed: false
PackageChecksum: SHA256: 551efc818b968b05216024fb0b727ef2ad4c100f8cb6b43fab615fa78ae5be9a
PackageLicenseConcluded:  GPL-1.0-or-later
PackageLicenseConcluded: Artistic-1.0-Perl
PackageLicenseDeclared: NOASSERTION
PackageLicenseInfoFromFiles:  GPL-1.0-or-later
PackageLicenseInfoFromFiles: Artistic-1.0-Perl
PackageCopyrightText: NOASSERTION

PackageName: ActiveState-Utils
SPDXID: SPDXRef-ActiveState-Utils
PackageVersion: 2.11
PackageDownloadLocation: https://dl.activestate.com/source/b53f2bdf-e7f8-57fb-ab05-171e637b4061/versions/8e6d4291-e6bc-5bd3-b401-438737249669/revisions/5/main.tar.gz
FilesAnalyzed: false
PackageChecksum: SHA256: 18bc5314cf40fb093f9e26eb12d268cd9a51a928b14c0a30fbd7f9e3577fbef1
PackageLicenseConcluded: NOASSERTION
PackageLicenseDeclared: NOASSERTION
PackageLicenseInfoFromFiles: NOASSERTION
PackageCopyrightText: NOASSERTION

PackageName: ActiveState-YAML
SPDXID: SPDXRef-ActiveState-YAML
PackageVersion: 0.36
PackageDownloadLocation: https://dl.activestate.com/source/ae1a4d58-b08c-5dad-8afa-40be0e46210d/versions/85f3b8c6-a65f-500a-beda-7966b9cc5344/revisions/5/main.tar.gz
FilesAnalyzed: false
PackageChecksum: SHA256: 017e263ad6856397b7a445e5c6cb4746815bab15eca44fdc7f064b020cf07f43
```

ActiveState

Attestations (SLSA)

ActiveState

Poll: What is your current experience with software attestations?

- Heard of them
- Heard of them in relation to US regulatory requirements
- Looking into using or generating them
- Looking into them as part of meeting SLSA framework
- Haven’t heard of them

ActiveState

Artifacts and Attestations

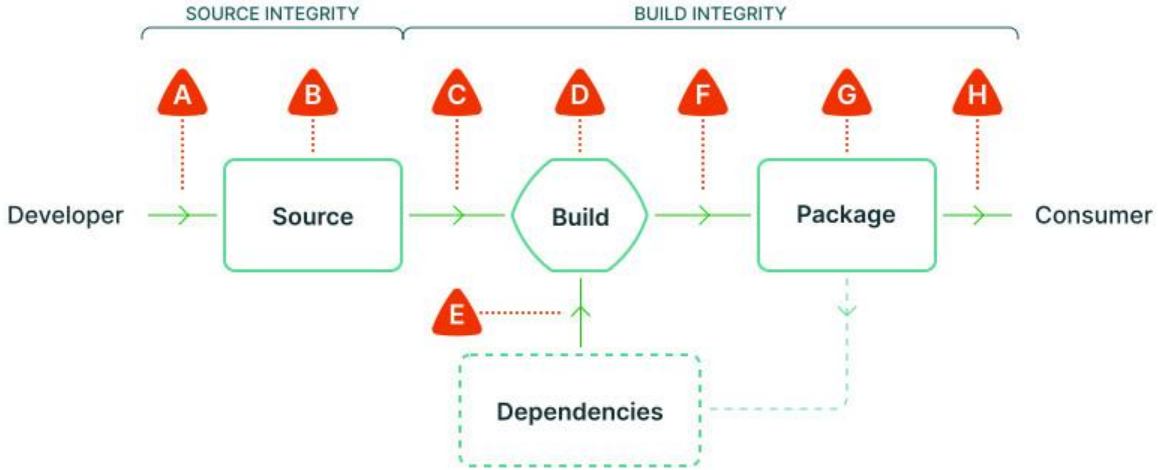
- **Artifact** - Any digital asset which forms part of a software supply chain.

  Source code, build scripts, installable binaries.
- **Attestation** - A statement about the provenance of an Artifact. Who created it,

  how, when and with what.
- **In-toto ITE-6** - The recommended format for attestations.
- **Non-Falsifiable** - SLSA levels 3 and above

ActiveState

Dependency Threats



A Submit unauthorized change
B Compromise source repo
C Build from modified source
D Compromise build process
E Use compromised dependency
F Upload modified package
G Compromise package repo
H Use compromised package

Source: SLSA.dev

ActiveState

SLSA - Addressing Supply Chain Security

- **SLSA** - Supply Chain Levels for Software Artifacts (https://slsa.dev/).
- **OSSF Initiative** - Operates under OSSF umbrella
- **Industry Backed** - Google, ChainGuard, Linux Foundation
- **Multiple Levels** - Levels providing increasing assurance.
  - 1 - Documentation of the build process
  - 2 - Tamper resistance of the build service
  - 3 - Extra resistance to specific threats
  - 4 - Highest levels of confidence and trust

ActiveState

Secure Build Service

Requirement	SLSA 1	SLSA 2	SLSA 3	SLSA 4
Build - Scripted build	✓	✓	✓	✓
Build - Build service		✓	✓	✓
Build - Build as code			✓	✓
Build - Ephemeral environment			✓	✓
Build - Isolated			✓	✓
Build - Parameterless				✓
Build - Hermetic				✓
Build - Reproducible				○

ActiveState

Dependency Vendoring Comparison

	Prebuilt?	Secure?	Up to Date?	Time & Resources
Public Repo (PyPI, npm, etc)	Yes	No	Yes	Low
Build It Yourself	No	Yes	Yes	High
ActiveState Platform	No	Yes	Yes	Low

ActiveState

Poll: Results

ActiveState

Platform Demo - Attestations

ActiveState

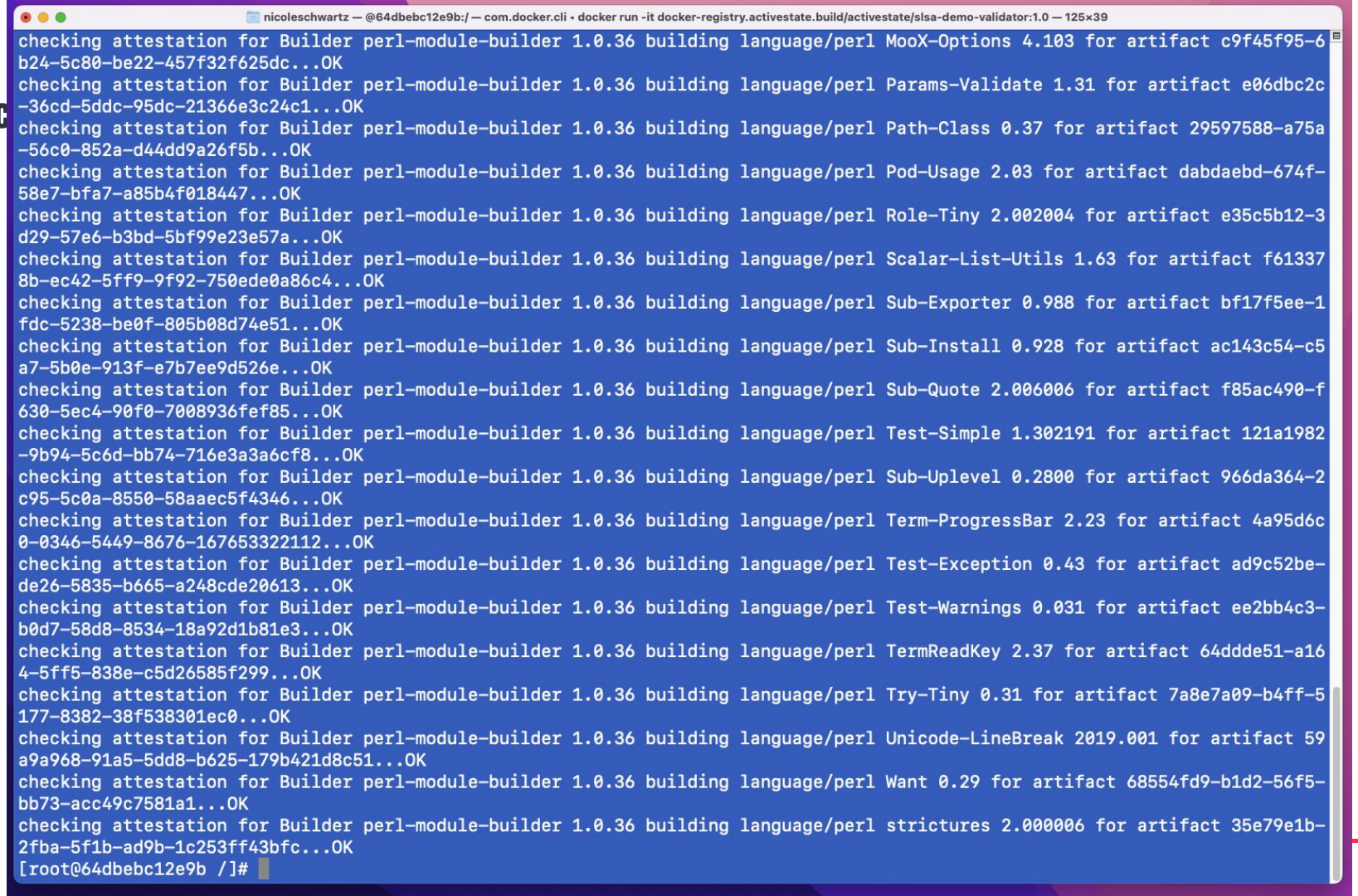
Demo: Attestation

intoto — Attestation Document — -zsh — 129×42

```
nicoleschwartz@ip-192-168-1-139 intoto % jq . attestation.in-toto.jsonl
{
  "payloadType": "application/vnd.in-toto+json",
  "payload": "eyJfdHlwZSI6ICJodHRwczovL2luLXRvdG8uaW8vU3RhdGVtZW50L3YwLjEiLCAiaW52b2NhdGlvbiI6IHsiY29uZmlnU291cmNlIjogeyJkaWdlc3Q
iOiB7InNoYTI1NiI6ICJlMjYwODVhZjhhYzM5NmY2MmFkZDhhNTMzYzNhMGVhOGM4NDk3ZDgzNmYwNjg5MzQ3YWM1YWJkN2I3YTRlMDBhIn0sICJlbnRyeVBvaW50Ijog
ImJ1aWxkIiwgInVyaSI6ICJzMzovL3BsYXRmb3JtLXNvdXJjZXMvbGFuZ3VhZ2UvZTI2MDg1YWY4YWMzOTZmNjJhZGQ4YTUzM2MzYTBlYThjODQ5N2Q4MzZmMDY4OTM0N
2FjNWFiZDdiN2E0ZTAwYS9wZXJsLTUuMzYuMC50YXIuZ3oifSwgImVudmlyb25tZW50IjogeyJlbnYiOiB7fX0sICJwYXJhbWV0ZXJzIjogW119LCAibWF0ZXJpYWxzIj
ogW3siZGlnZXN0IjogeyJzaGEyNTYiOiAiOWJiZTdjNTEwMWZmMDhkNjNmNWVmMGJiMjVlOWI3MmRjNmUxZTgxZWJmZjE5OGMyNWU5YTU0NmY4YWZhOWM1NSJ9LCAidXJ
pIjogInMzOi8vcGxhdGZvcm0tc291cmNlcy9idWlsZGVyLzliYmU3YzUxMDFmZjA4ZDYzZjVlZjBiYjI1ZTliNzJkYzZlMWU4MWViZmYxOThjMjVlOWE1NDZmOGFmYTlj
NTUvcGVybC1jb3JlLWJ1aWxkZXIudGFyLmd6In1dLCAicHJlZGljYXRlIjogeyJidWlsZENvbmZpZyI6IHsic3RlcHMiOiBbeyJjb21tYW5kIjogImJ1aWxkIiwgInBhc
mFtZXRlcnMiOiBbbXX1dfSwgImJ1aWxkVHlwZSI6ICJodHRwczovL2FjdGl2ZXN0YXRlIjogeyJidWlsZENvbmZpZyI6IHsic3RlcHMiOiBbeyJjb21tYW5kIjogImJ1aWxkIiwgInBhc
mFtZXRlcnMiOiBbbXX1dfSwgImJ1aWxkVHlwZSI6ICJodHRwczovL2FjdGl2ZXN0YXRlIjogeyJidWlsZENvbmZpZyI6IHsic3RlcHMiOiBbeyJjb21tYW5kIjogImJ1aWxkIiwgInBhc
AiaHR0cHM6Ly9hY3RpdmVzdGF0ZS5jb20vYnVpbGRlci9wZXJsLWNvcmUtYnVpbGRlckAxLjAuMjNyMTIifSwgImlldGFkYXRhIjogeyJidWlsZEZpbmlzaGVkT24iOiAi
MjAyMi0xMS0xNVQxNjozNjoxMy40NDg0NjRaIiwgImJ1aWxkSW52b2NhdGlvbklkIjogIkJ1aWxkZXIgcGVybC1jb3JlLWJ1aWxkZXIgMS4wLjIzIGJ1aWxkaW5nIGxh
bmd1YWdlIHBlcmwgNS4zNi4wIGZvciBhcnRpZmFjdCA0Y2U5MGE2MC0yZDZlLTVjZDYtOWIyYi04OTBiOWFmMDM2YjQiLCAiYnVpbGRTdGFydGVkT24iOiAiMjAyMi0xM
S0xNVQxNjozNjoxMy4yNDg0NjRaIiwgImNvbXBsZXRlbmVzcyI6IHsiZW52aXJvbm1lbnQiOiB0cnVlLCAibWF0ZXJpYWxzIjogdHJ1ZSwgInBhcmFtZXRlcnMiOiB0cn
VlfX0sICJyZXByb2R1Y2libGUiOiB0cnVlfSwgInByZWRpY2F0ZVR5cGUiOiAiaHR0cHM6Ly9zbHNhLmRldi9wcm92ZW5hbmNlL3YwLjIiLCAic3ViamVjdCI6IFt7ImR
pZ2VzdCI6IHsic2hhMjU2IjogImE2MGIyN2I3YTZlMzI3NmE0NmQzMjE3MmNiNmUzMTFkNzA1ODE4MWYwMmI2N2JiOTMxNjkxMDljMjQ4MzAzOGUifSwgInVyaSI6ICJz
MzovL2FzLWJ1aWxkcy9wcjk0MjMvbGFuZ3VhZ2UvcGVybC81LjM2LjAvMS80Y2U5MGE2MC0yZDZlLTVjZDYtOWIyYi04OTBiOWFmMDM2YjQvYXJ0aWZhY3QudGFyLmd6I
n1dfQ==",
  "signatures": [
    {
      "sig": "JAnSiwEKljEGYbZQywEFzaEWZJInNOIA+TxzftUBwqE8chk7Wixg02fDi6AIe2foy+lSmhRPFXKwfwjskRNSCXVoNueA+tTE5LHZw+f9sdWpyiqnwU5
9659bOB/UaTwZG/tynfheHoRyjK4wvJoaZaV0JH7Z02WTvGV8ER4kF5n1QzLUYKj/teyHc3cY8iDAt8HBjHOY7wnrVg3RJSb9blIO5RY53Tjka+gdYNQ0r5fe0gPSfsCP
bLSGz5MNPzaH7O7fgwuut73Zdftdor+iuD0v36rbXxWKyocG1bGSpdKSYAHPSdr1Gm/UERrk15O5AGgtR+5xCdRvFdsuNgxcdTvFOy5Raux+HTrGmlAdeOH7C08A6Xrs7
8i+TV/qQRRayQW0kEDwDvqtZIKXBQ+x2kRJodr5a5lFoYEbcFl4xxzpwsqPjiz3uhsjN3kTyP3rC/40z7TwryFJChjlyOvY4Q13qPVts4JiLSgb4BLxlA/ijDfQvs2m2d
Sgy3lIUHv+hTMqijngP5yC3CNBGL0jzeDPstiUrfonC1/VaO0A+KrfcDlJWfhxBPmKGIc3p/rZbUNRMvp/drI5k3Wp079SZj531e/Th6xAAy7vS9X6LK/4Ny0sQ4FEZaH
fI3pSAIwogp5jUOLTgTc8ezIbYHCqPoAch4QGm76LY0wp3m9UhVk=",
      "cert": "-----BEGIN CERTIFICATE-----\nMIIGWjCCBMKgAwIBAgIRAId1qIaQkVaZOKH6b4hJ/UowDQYJKoZIhvcNAQEMBQAw\nVDELMAkGA1UEBhMCR0I
xGDAWBgNVBAoTD1NlY3RpZ28gTGltaXRlZDErMCkGA1UE\nAxMiU2VjdGlnbyBQdWJsaWMgQ29kZSBTaWduaW5nIENBIFIzNjAeFw0yMjA5MjMw\nMDAwMDBaFw0yNTA5
MjIyMzU5NTlaMHAxCzAJBgNVBAYTAkNBMRkwFwYDVQQIDBBC\ncml0aXNoIENvbHVtYmlhMSIwIAYDVQQKDBlBY3RpdmVTdGF0ZSBTb2Z0d2FyZSBJ\nbmMuMSIwIAYDV
QQDDBlBY3RpdmVTdGF0ZSBTb2Z0d2FyZSBJbmMuMIICIjANBgkq\nhkiG9w0BAQEFAAOCAg8AMIICCgKCAgEAxuVly6YqqtsEYuu6DbGTjetgyilaq2Tc\nCq3W5XzYJ2
xmQ4cFMo88E3OKia6LLAmE4bRGgiuki89gsqXP7n87iC3GsoF8yjq+\n8XeH5SzIGI9sDaNyqgSeh48y7YNPokHJhvxrZ4oq6cJ2tPsPUQjJCVEZCbbg2pJk\n5U9lFe2
QoSgrlidFdHhkB/lgxnjZiqZuJNyqdYLV9PHNY3U6yEZsipzaAcS9K1OH\n4vs/LfUg3GjvXiZ/wVc7kdk1UD+bhol8UOC38uuxVEU1c/Laq6NShUyh01DWCNIt\nIcsP
hAgH/5j7fF9+dy+HM65pvWuKjOIcB/0XX3QSteYSvj+gXBwPX2hYkZoCXDeF\nlFzscM8F0Tb0lerJnZWrbYUCjXaAmuzvL8fTNaG+au/DvSqK0B9lUhyXG4xVMTsw\n4
PwtiurfEhaUoYd/iWeucTGhlDb231E4XurPXoL1xTUe3ZIcHnD2ohX2yXM1WYtt\nWnX/4oeitYl5WuQVw6nMDm5I3I6MP2P5YF6RbUW6TokZyLOm4X80HDF7T5wWj3g4
\nosHmsRQyid+Rm2zmpyP7/sSGft9SOKPLgIBghhqeFJ/JcGHdSZqZWXPPOUA2sYeS\ntMWf9nDheaSoXBvuJld3xceFMps/2OaqFI67zojRnKXxYp7kTADdgihvfnfQ7
bHD\nMvvxJkq5Ad8CAwEAAaOCAYkwggGFMB8GA1UdIwQYMBaAFA8qyyCHKLjsb0iuK1Sm\nKaoXpM0MMB0GA1UdDgQWBBQyE5wi60JUSyX7hMcX7wPhIL0EpjAOBgNVHQ
8BAf8E\nBAMCB4AwDAYDVR0TAQH/BAIwADATBgNVHSUEDDAKBggrBgEFBQcDAzBKBgNVHSAE\nQzBBMDUGDCsGAQQBsjEBAgEDAjAlMCMGCCsGAQUFBwIBFhdodHRwczo
vL3NlY3Rp\nZ28uY29tL0NQUzAIBgZngQwBBAEwSQYDVR0fBEIwQDA+oDygOoY4aHR0cDovL2Ny\nbC5zZWN0aWdvLmNvbS9TZWN0aWdvUHVibGljQ29kZVNpZ25pbmdD
QVIzNi5jcmww\neQYIKwYBBQUHAQEEbTBrMEQGCCsGAQUFBzAChjhodHRwOi8vY3J0LnNlY3RpZ28u\nY29tL1NlY3RpZ29QdWJsaWNDb2RlU2lnbmluZ0NBUjM2LmNyd
DAjBggrBgEFBQcw\nAYYXaHR0cDovL29jc3Auc2VjdGlnby5jb20wDQYJKoZIhvcNAQEMBQADggGBAHxs\nxeeGWsPNjANP3Iy71f9ViUKxJEW9lGXMeRNdLl+4j2lX1E
QGRrY4hrq4oE9ulTex\nyQTy/3F6mMBRsWzvwnkQ24oc4dwu8RlJzip82uxluZKEnXbc053BNnD6hM37PxU/\n8JVgX0dnnqxm6yCrrGiE/NNkmAwLMFgoH1foJogy3TZ
```

intoto — Attestation Document — -zsh — 129×42

```
}
nicoleschwartz@ip-192-168-1-139 intoto % jq -r .payload attestation.in-toto.jsonl | base64 -d | jq .
{
  "_type": "https://in-toto.io/Statement/v0.1",
  "invocation": {
    "configSource": {
      "digest": {
        "sha256": "e26085af8ac396f62add8a533c3a0ea8c8497d836f0689347ac5abd7b7a4e00a"
      },
      "entryPoint": "build",
      "uri": "s3://platform-sources/language/e26085af8ac396f62add8a533c3a0ea8c8497d836f0689347ac5abd7b7a4e00a/perl-5.36.0.tar.gz"
    },
    "environment": {
      "env": {}
    },
    "parameters": []
  },
  "materials": [
    {
      "digest": {
        "sha256": "9bbe7c5101ff08d63f5ef0bb25e9b72dc6e1e81ebff198c25e9a546f8afa9c55"
      },
      "uri": "s3://platform-sources/builder/9bbe7c5101ff08d63f5ef0bb25e9b72dc6e1e81ebff198c25e9a546f8afa9c55/perl-core-builder.tar.gz"
    }
  ],
  "predicate": {
    "buildConfig": {
      "steps": [
        {
          "command": "build",
          "parameters": []
        }
      ]
    },
    "buildType": "https://activestate.com/platform_builder/v0.1",
    "builder": {
      "id": "https://activestate.com/builder/perl-core-builder@1.0.23r12"
    },
    "metadata": {
      "buildFinishedOn": "2022-11-15T16:36:13.448464Z",
      "buildInvocationId": "Builder perl-core-builder 1.0.23 building language perl 5.36.0 for artifact 4ce90a60-2d6e-5cd6-9b2b-8
```


nicoleschwartz — @64dbebc12e9b:/ — com.docker.cli ◂ docker run -it docker-registry.activestate.build/activestate/slsa-demo-validator:1.0 — 125×39
checking attestation for Builder perl-module-builder 1.0.36 building language/perl MooX-Options 4.103 for artifact c9f45f95-6b24-5c80-be22-457f32f625dc...OK
checking attestation for Builder perl-module-builder 1.0.36 building language/perl Params-Validate 1.31 for artifact e06dbc2c-36cd-5ddc-95dc-21366e3c24c1...OK
checking attestation for Builder perl-module-builder 1.0.36 building language/perl Path-Class 0.37 for artifact 29597588-a75a-56c0-852a-d44dd9a26f5b...OK
checking attestation for Builder perl-module-builder 1.0.36 building language/perl Pod-Usage 2.03 for artifact dabdaebd-674f-58e7-bfa7-a85b4f018447...OK
checking attestation for Builder perl-module-builder 1.0.36 building language/perl Role-Tiny 2.002004 for artifact e35c5b12-3d29-57e6-b3bd-5bf99e23e57a...OK
checking attestation for Builder perl-module-builder 1.0.36 building language/perl Scalar-List-Utils 1.63 for artifact f613378b-ec42-5ff9-9f92-750ede0a86c4...OK
checking attestation for Builder perl-module-builder 1.0.36 building language/perl Sub-Exporter 0.988 for artifact bf17f5ee-1fdc-5238-be0f-805b08d74e51...OK
checking attestation for Builder perl-module-builder 1.0.36 building language/perl Sub-Install 0.928 for artifact ac143c54-c5a7-5b0e-913f-e7b7ee9d526e...OK
checking attestation for Builder perl-module-builder 1.0.36 building language/perl Sub-Quote 2.006006 for artifact f85ac490-f630-5ec4-90f0-7008936fef85...OK
checking attestation for Builder perl-module-builder 1.0.36 building language/perl Test-Simple 1.302191 for artifact 121a1982-9b94-5c6d-bb74-716e3a3a6cf8...OK
checking attestation for Builder perl-module-builder 1.0.36 building language/perl Sub-Uplevel 0.2800 for artifact 966da364-2c95-5c0a-8550-58aaec5f4346...OK
checking attestation for Builder perl-module-builder 1.0.36 building language/perl Term-ProgressBar 2.23 for artifact 4a95d6c0-0346-5449-8676-167653322112...OK
checking attestation for Builder perl-module-builder 1.0.36 building language/perl Test-Exception 0.43 for artifact ad9c52be-de26-5835-b665-a248cde20613...OK
checking attestation for Builder perl-module-builder 1.0.36 building language/perl Test-Warnings 0.031 for artifact ee2bb4c3-b0d7-58d8-8534-18a92d1b81e3...OK
checking attestation for Builder perl-module-builder 1.0.36 building language/perl TermReadKey 2.37 for artifact 64ddde51-a164-5ff5-838e-c5d26585f299...OK
checking attestation for Builder perl-module-builder 1.0.36 building language/perl Try-Tiny 0.31 for artifact 7a8e7a09-b4ff-5177-8382-38f538301ec0...OK
checking attestation for Builder perl-module-builder 1.0.36 building language/perl Unicode-LineBreak 2019.001 for artifact 59a9a968-91a5-5dd8-b625-179b421d8c51...OK
checking attestation for Builder perl-module-builder 1.0.36 building language/perl Want 0.29 for artifact 68554fd9-b1d2-56f5-bb73-acc49c7581a1...OK
checking attestation for Builder perl-module-builder 1.0.36 building language/perl strictures 2.000006 for artifact 35e79e1b-2fba-5f1b-ad9b-1c253ff43bfc...OK
[root@64dbebc12e9b /]#

ActiveState

Recap

ActiveState

Why are we doing this?

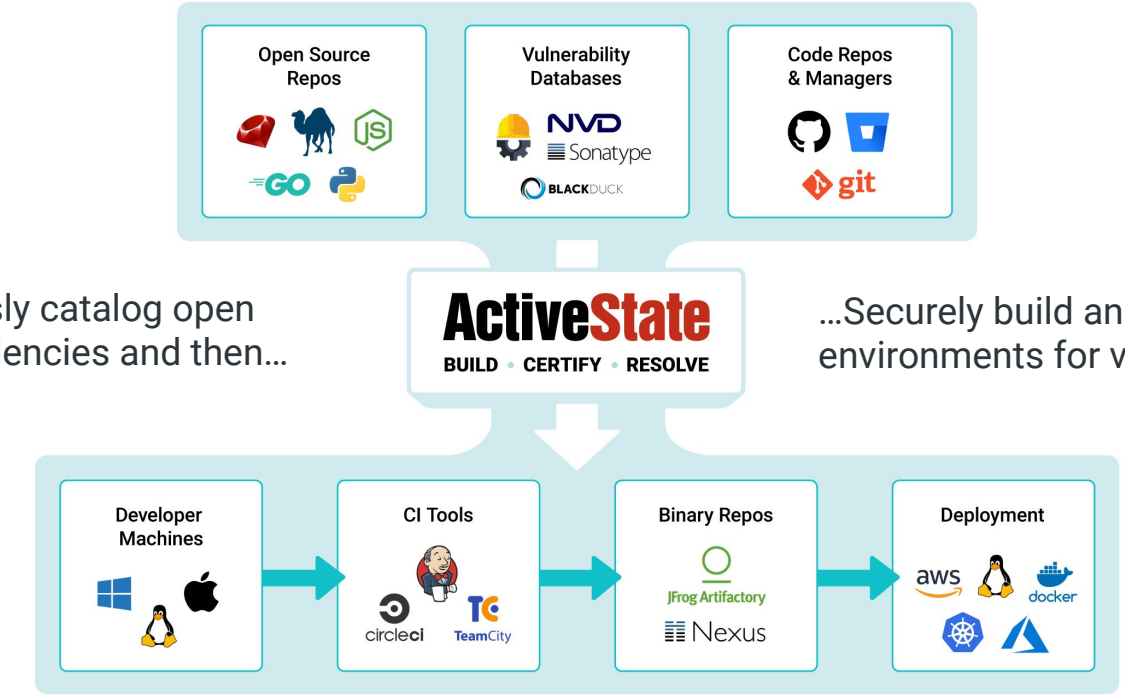
- All critical software that touches government data or systems in any way must be compliant with these new security standards no later than **June 12, 2023, 7 months from now.**
- And all software must adhere to these strict standards no later than September 14, 2023, 10 months from now.

For which you need:

- Software producer self-attestation (can use in-toto)
- SBOM

ActiveState

ActiveState Platform



ActiveState

Q&A

ActiveState

Next Steps

Schedule a demo with our product experts:
https://www.activestate.com/get-demo/

Learn more about software attestations:
https://www.activestate.com/solutions/attestations/

Learn more about Supply Chain Security:
https://www.activestate.com/solutions/slsa

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