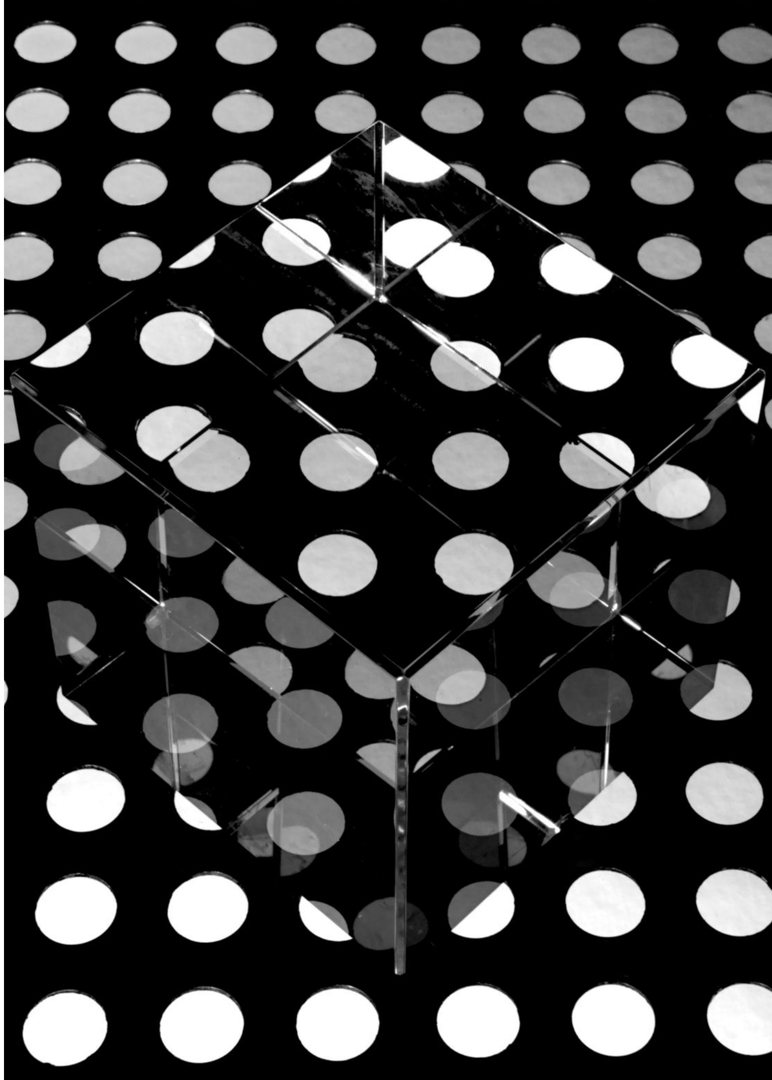
ActiveState

SBOM Platform Workshop

August, 2022



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

Introduction

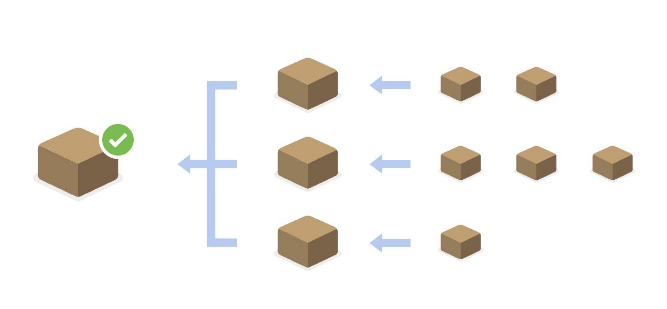
Jeff Rouse

Senior Product Strategist

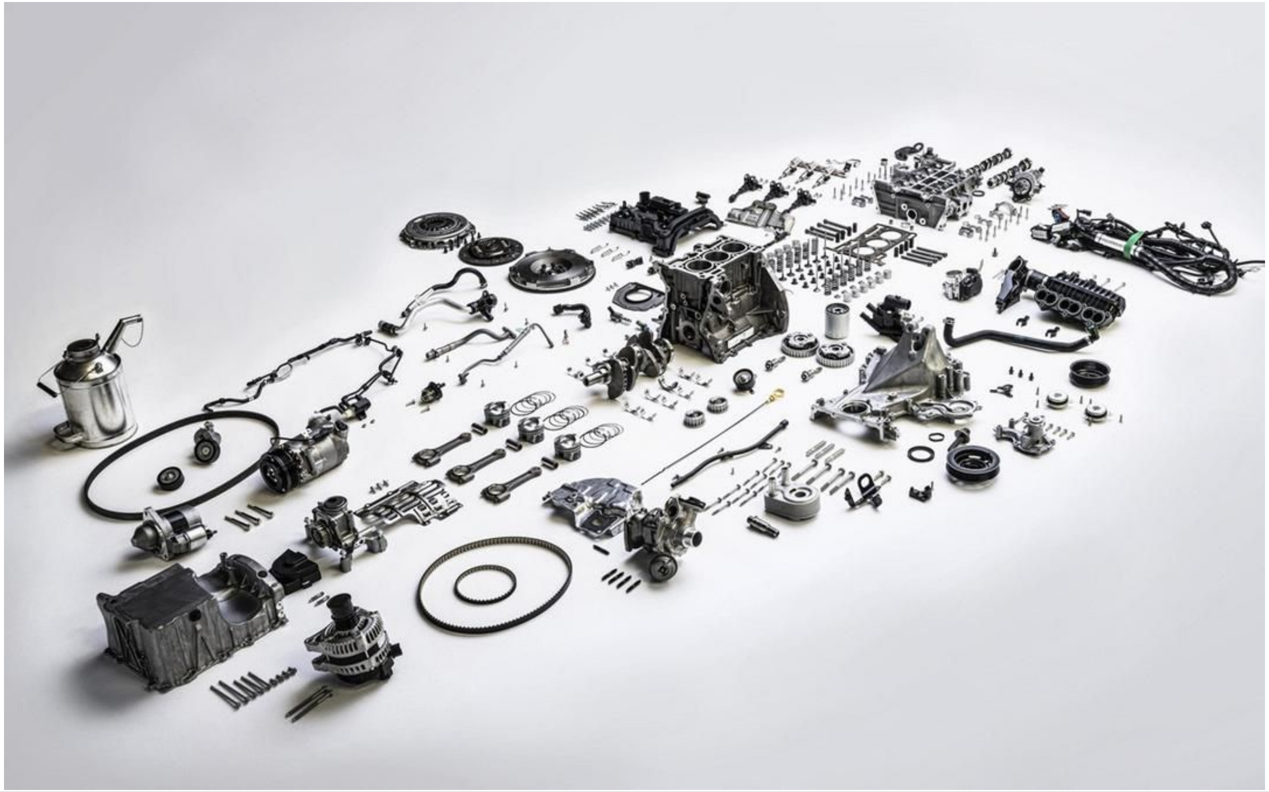
ActiveState Platform — Your Team's Supply Chain for Trusted Open Source Artifacts

Includes:

- Catalog of 4M+ Vendored Open Source Components & Recipes
- Universal Dependency Solver
- Hermetically Sealed Multi-OS Build Farm
- Declarative Project Oriented UX/API
- Powerful Revision Control Features
- SBOMs and Vulnerability Reports



Software Bill of Materials - listing of all the component parts that make up your software



Common Elements of an SBOM

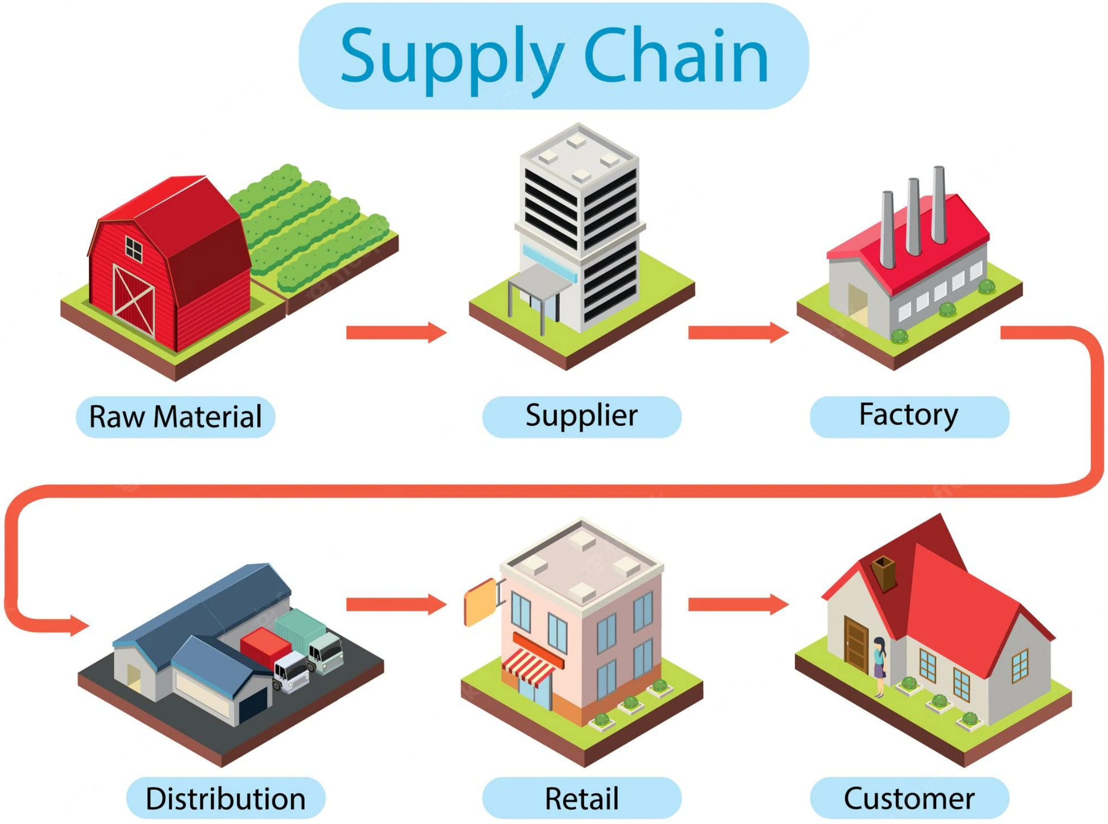
For a given piece of software, it is made up of all of the components it needs at runtime:

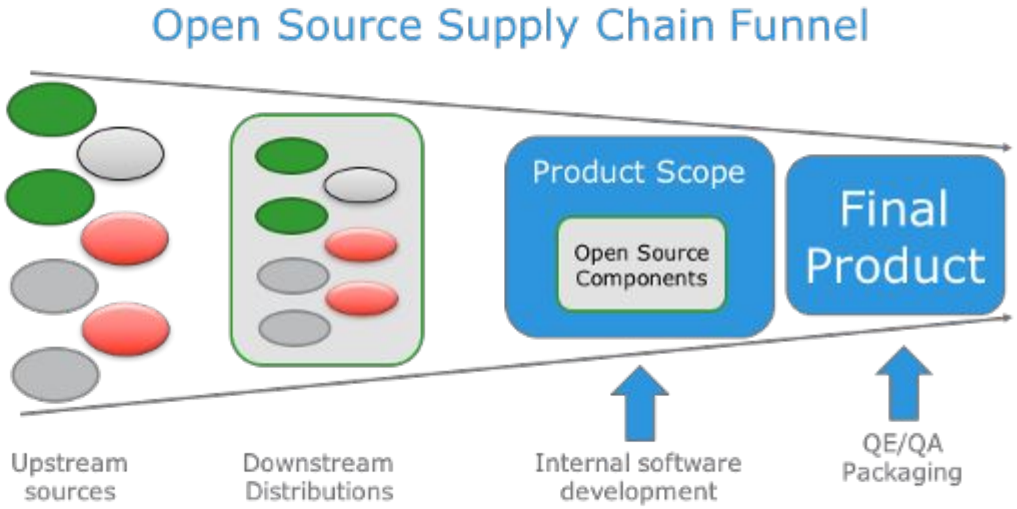
- Open source components (packages, gems, modules, libraries)
- Plugins, extensions or other add-ons
- Custom source code written by in-house developers
- Information about the component versions, licensing, and other metadata depending on the standard/vendor

Other Aspects:

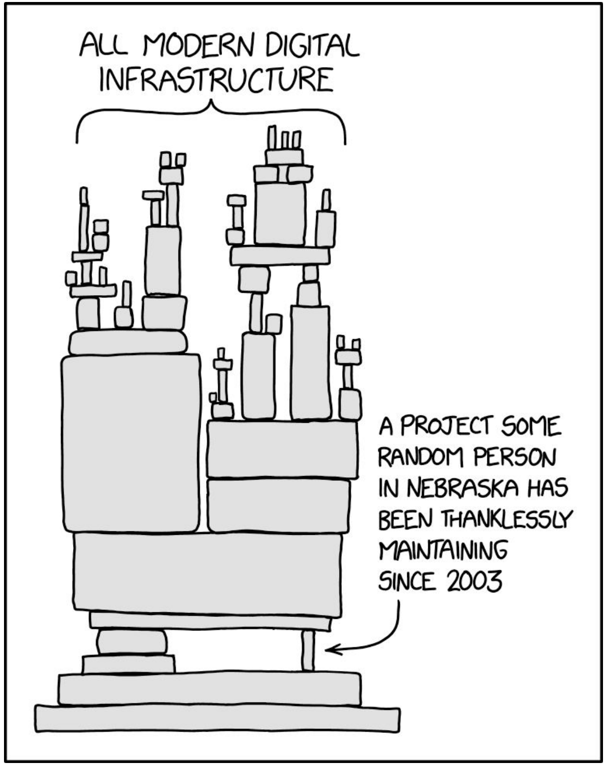
- Can include vulnerability information
- Can include external services it relies on
- Includes component checksums
- Typically signed by the provider

If SBOM is the answer, what was the question?


Supply Chain
Raw Material
Supplier
Factory
Distribution
Retail
Customer

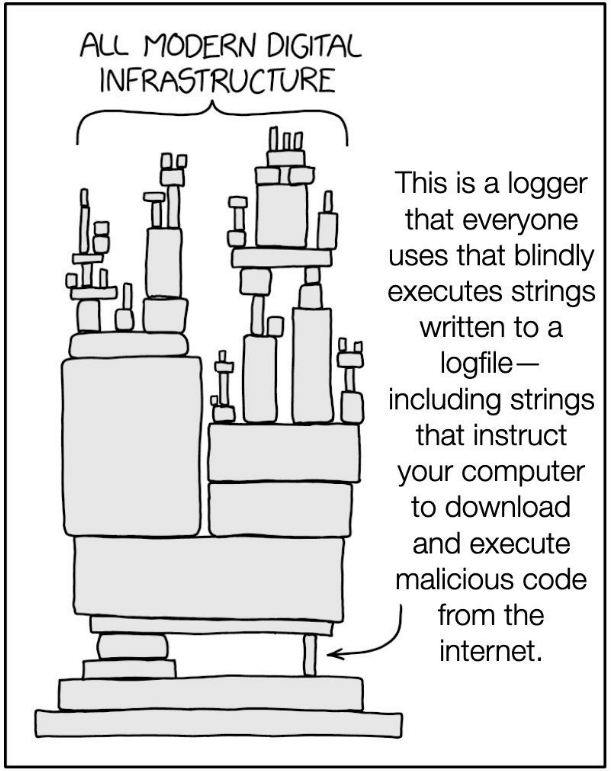


Credit: Opensource.com


ALL MODERN DIGITAL INFRASTRUCTURE
A PROJECT SOME RANDOM PERSON IN NEBRASKA HAS BEEN THANKLESSLY MAINTAINING SINCE 2003

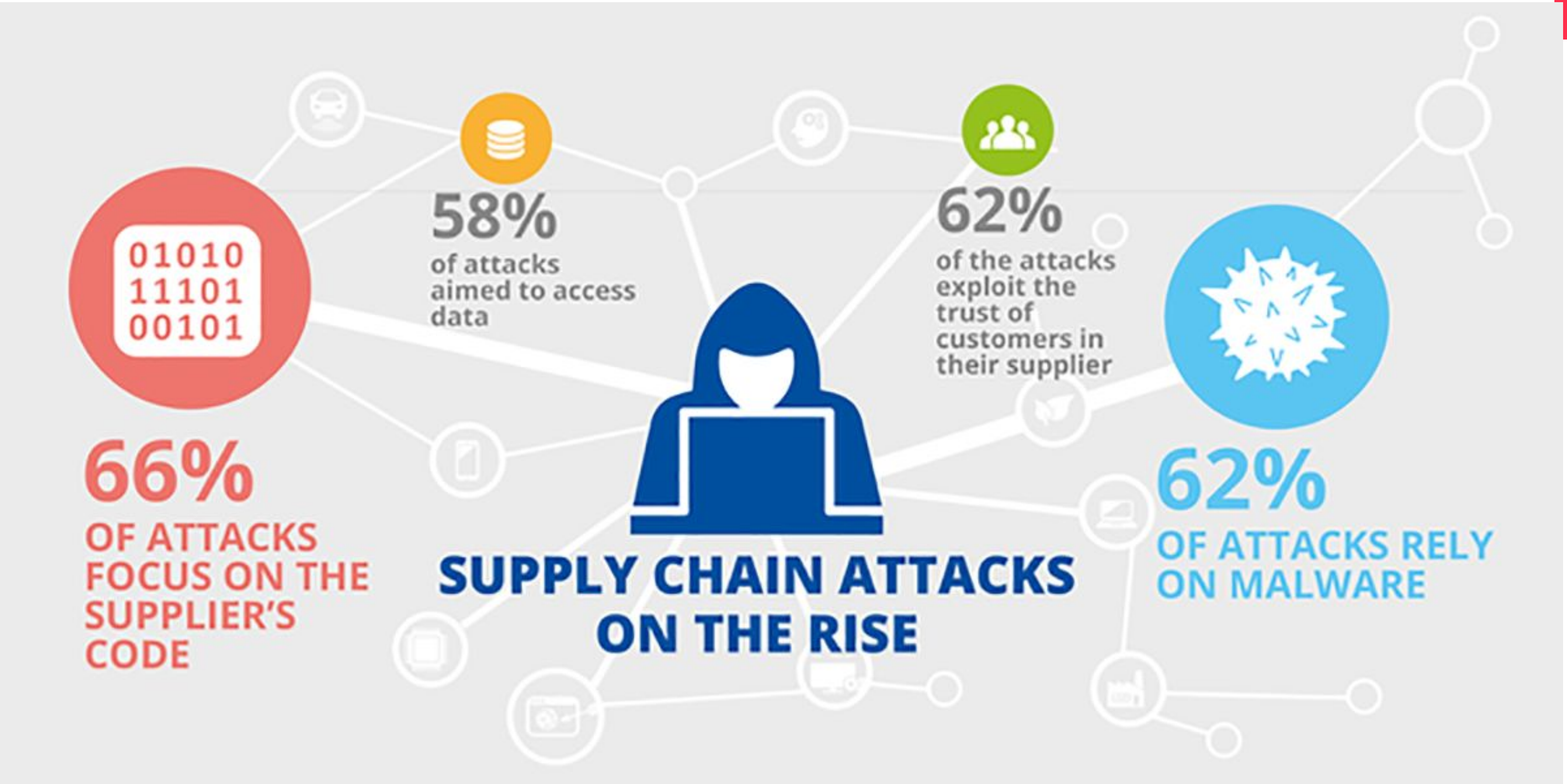
Modern software supply chains run very deep.

But…


ALL MODERN DIGITAL INFRASTRUCTURE
This is a logger that everyone uses that blindly executes strings written to a logfile— including strings that instruct your computer to download and execute malicious code from the internet.

…has its downsides.

Credit: https://xkcd.com/2347/



66%

OF ATTACKS FOCUS ON THE SUPPLIER'S CODE

58%

of attacks aimed to access data

62%

of the attacks exploit the trust of customers in their supplier

62%

OF ATTACKS RELY ON MALWARE

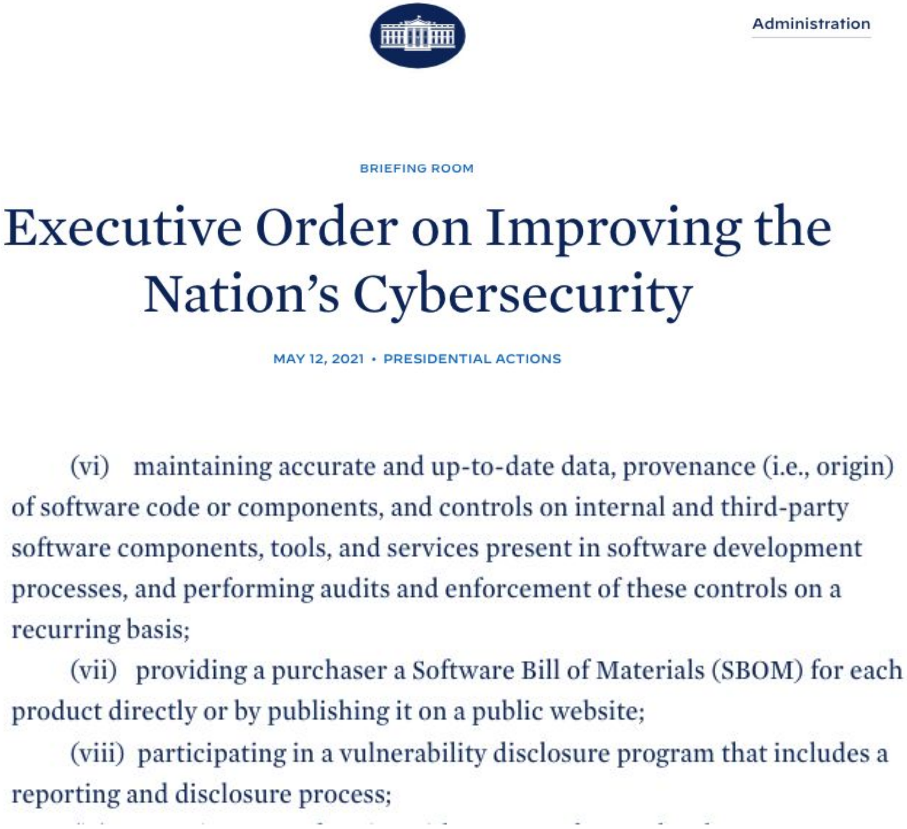
SUPPLY CHAIN ATTACKS ON THE RISE

Noteworthy Supply Chain Attacks

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

Source: Wikipedia

Y’all better get some SBOMs.



Administration

BRIEFING ROOM

Executive Order on Improving the Nation’s Cybersecurity

MAY 12, 2021 • PRESIDENTIAL ACTIONS

(vi) maintaining accurate and up-to-date data, provenance (i.e., origin) of software code or components, and controls on internal and third-party software components, tools, and services present in software development processes, and performing audits and enforcement of these controls on a recurring basis;

(vii) providing a purchaser a Software Bill of Materials (SBOM) for each product directly or by publishing it on a public website;

(viii) participating in a vulnerability disclosure program that includes a reporting and disclosure process;

SBOM Summary of Benefits

- Security
- Can automate collection/aggregation, keep up to date
- Licensing
- Locate and describe components (metadata)

SBOM Common Formats

These three formats were identified by NTIA (National Telecommunications and Information Administration) as meeting their criteria:

- SPDX - Software Package Data Exchange
- CycloneDX - built originally to capture OWASP data and subsequently enhanced for SBOM support
- SWID - came out of the software asset management space and isn't as popular

Other formats also seen in the industry:

- CSV
- JSON

Our SBOM implementation is available as a lightweight JSON or an ISO standard SPDX format both for Python, Perl, and Ruby.

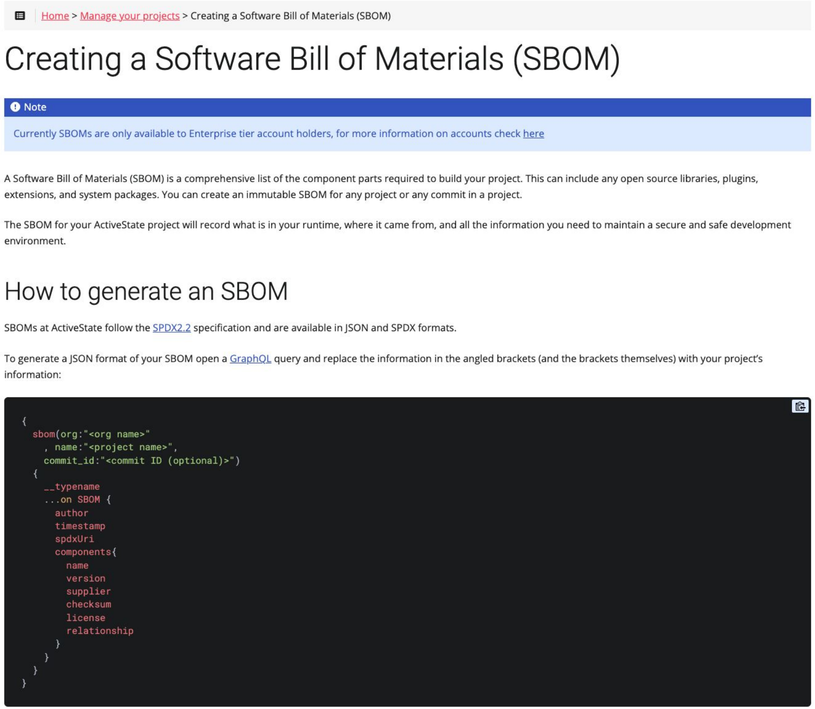
- SPDX
    a. project of the Linux Foundation
    b. ISO Standard: ISO/IEC 5962:2021
    c. Machine-readable inventory of software components
    d. The model of an SPDX SBOM defines three elements: Document, Package, and File
        i. Document defines metadata about the SBOM
        ii. Package is a concept that groups together one or more elements
        iii. File - each individual file in each package

Platform and SBOM Demo

Supply Chain Security & SBOM - Key Takeaways

- Know what is in your software, to the level of all the component parts
- Get a new SBOM on each new update
- Aggregate the entirety of your software portfolio to search/determine where all the components are that need remediation
- Strive for nimble DevOps processes to address security issues in hours not days (i.e. What happens if there is a serious zero-day?)

SBOM Documentation



Home > Manage your projects > Creating a Software Bill of Materials (SBOM)

Creating a Software Bill of Materials (SBOM)

Note

Currently SBOMs are only available to Enterprise tier account holders, for more information on accounts check here

A Software Bill of Materials (SBOM) is a comprehensive list of the component parts required to build your project. This can include any open source libraries, plugins, extensions, and system packages. You can create an immutable SBOM for any project or any commit in a project.

The SBOM for your ActiveState project will record what is in your runtime, where it came from, and all the information you need to maintain a secure and safe development environment.

How to generate an SBOM

SBOMs at ActiveState follow the SPDX2.2 specification and are available in JSON and SPDX formats.

To generate a JSON format of your SBOM open a GraphQL query and replace the information in the angled brackets (and the brackets themselves) with your project's information:

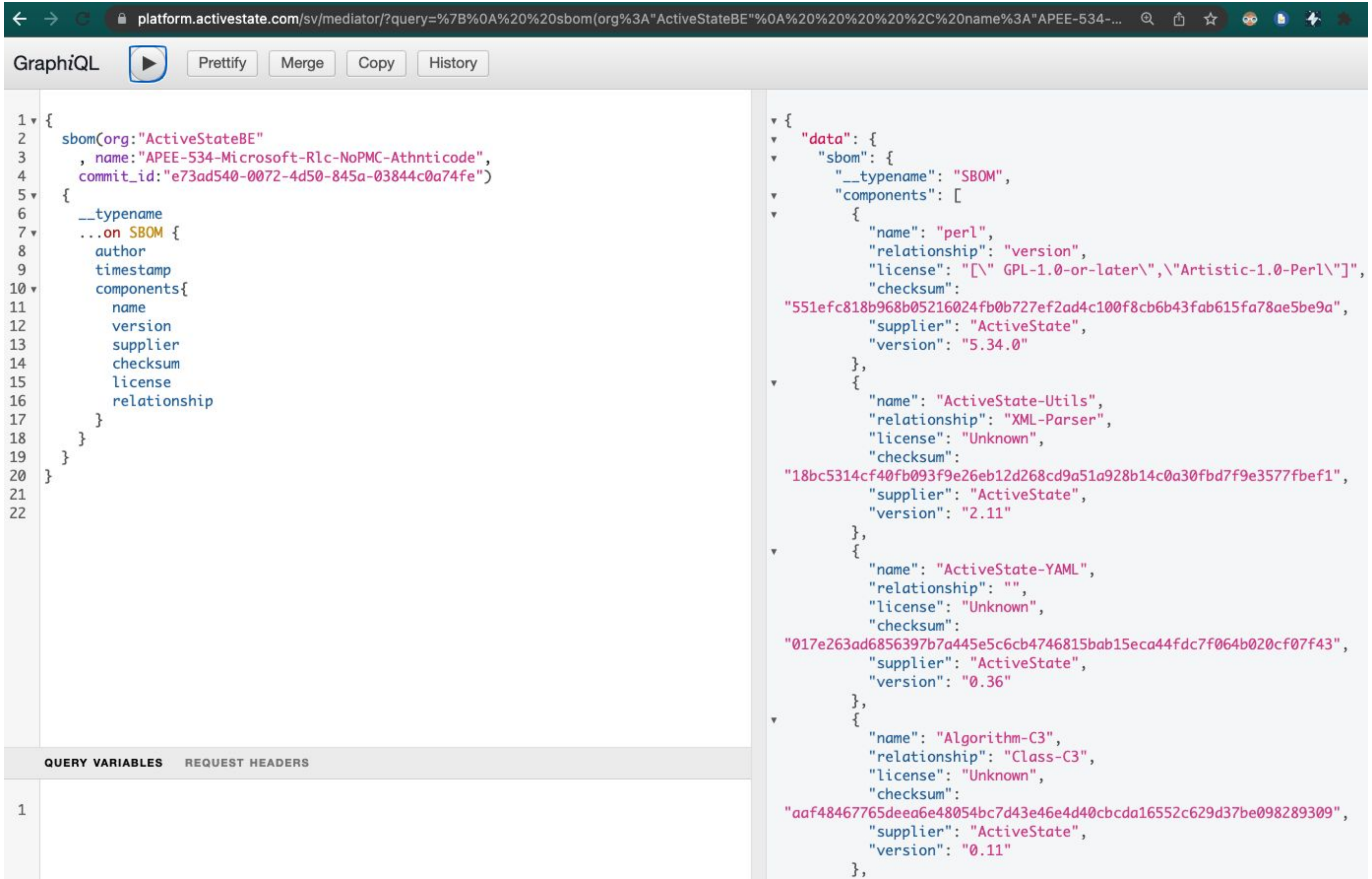
```
{
  sbom(org:"<org name>"
    , name:"<project name>",
    commit_id:"<commit ID (optional)>")
  {
    __typename
    ...on SBOM {
      author
      timestamp
      spdxUri
      components{
        name
        version
        supplier
        checksum
        license
        relationship
      }
    }
  }
}
```

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

Questions?

ActiveState

JSON format

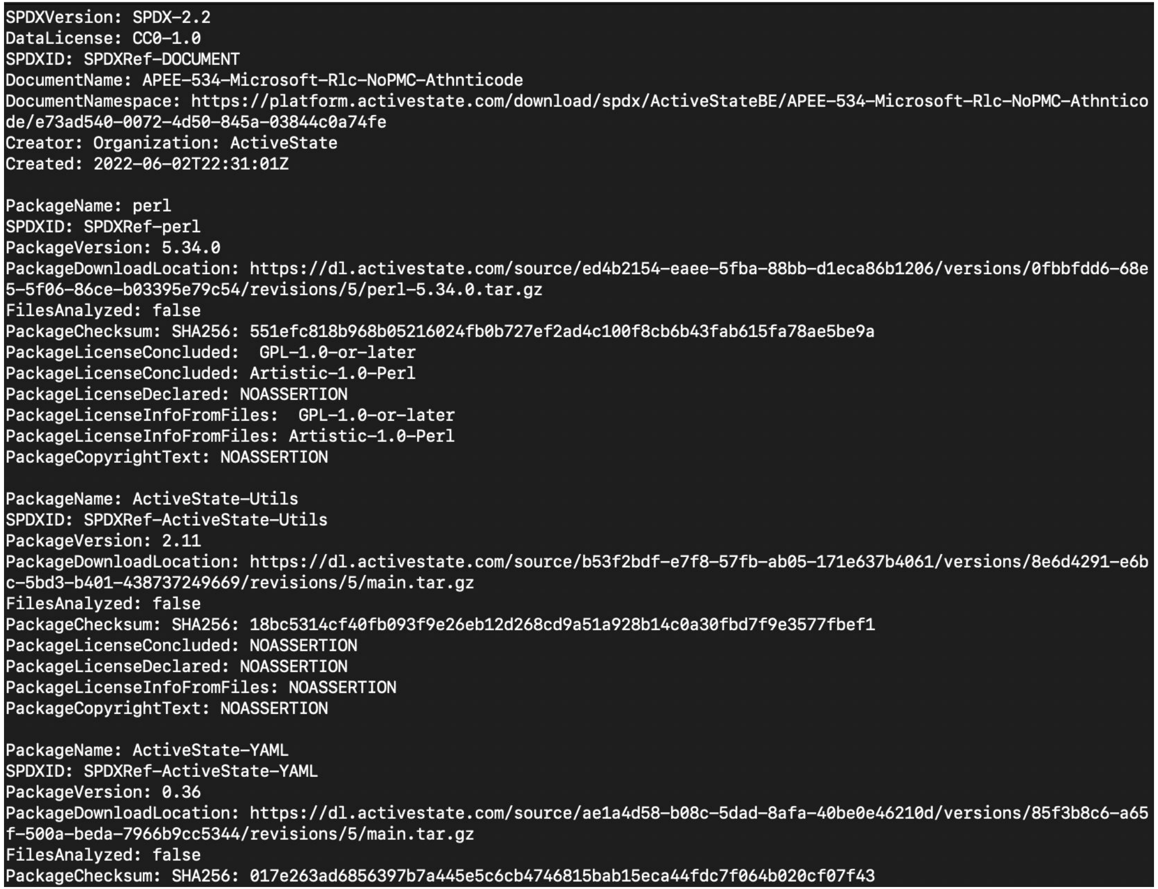

platform.activestate.com/sv/mediator/?query=%7B%0A%20%20sbom(org%3A"ActiveStateBE"%0A%20%20%20%20%2C%20name%3A"APEE-534-...
GraphiQL
Prettify
Merge
Copy
History
QUERY VARIABLES
REQUEST HEADERS

```
{
  sbom(org:"ActiveStateBE"
    , name:"APEE-534-Microsoft-Rlc-NoPMC-Athnticode",
    commit_id:"e73ad540-0072-4d50-845a-03844c0a74fe")
  {
    __typename
    ...on SBOM {
      author
      timestamp
      components{
        name
        version
        supplier
        checksum
        license
        relationship
      }
    }
  }
}
```

```
{
  "data": {
    "sbom": {
      "__typename": "SBOM",
      "components": [
        {
          "name": "perl",
          "relationship": "version",
          "license": "[\" GPL-1.0-or-later\",\"Artistic-1.0-Perl\"]",
          "checksum":
"551efc818b968b05216024fb0b727ef2ad4c100f8cb6b43fab615fa78ae5be9a",
          "supplier": "ActiveState",
          "version": "5.34.0"
        },
        {
          "name": "ActiveState-Utils",
          "relationship": "XML-Parser",
          "license": "Unknown",
          "checksum":
"18bc5314cf40fb093f9e26eb12d268cd9a51a928b14c0a30fbd7f9e3577fbef1",
          "supplier": "ActiveState",
          "version": "2.11"
        },
        {
          "name": "ActiveState-YAML",
          "relationship": "",
          "license": "Unknown",
          "checksum":
"017e263ad6856397b7a445e5c6cb4746815bab15eca44fdc7f064b020cf07f43",
          "supplier": "ActiveState",
          "version": "0.36"
        },
        {
          "name": "Algorithm-C3",
          "relationship": "Class-C3",
          "license": "Unknown",
          "checksum":
"aaf48467765deea6e48054bc7d43e46e4d40cbcda16552c629d37be098289309",
          "supplier": "ActiveState",
          "version": "0.11"
        },
```

ActiveState

SPDX format



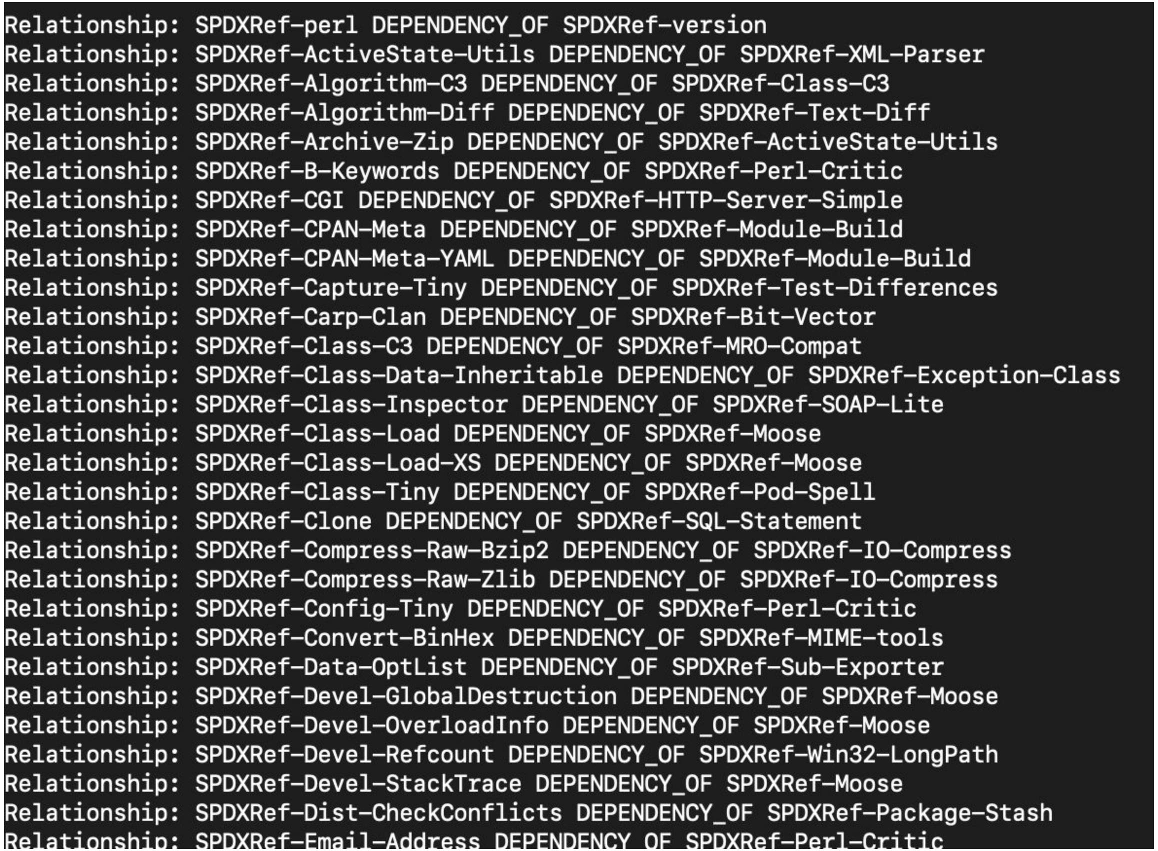
```
SPDXVersion: SPDX-2.2
DataLicense: CC0-1.0
SPDXID: SPDXRef-DOCUMENT
DocumentName: APEE-534-Microsoft-Rlc-NoPMC-Athnticode
DocumentNamespace: https://platform.activestate.com/download/spdx/ActiveStateBE/APEE-534-Microsoft-Rlc-NoPMC-Athntico
de/e73ad540-0072-4d50-845a-03844c0a74fe
Creator: Organization: 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/0fbbfdd6-68e
5-5f06-86ce-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-e6b
c-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-a65
f-500a-beda-7966b9cc5344/revisions/5/main.tar.gz
FilesAnalyzed: false
PackageChecksum: SHA256: 017e263ad6856397b7a445e5c6cb4746815bab15eca44fdc7f064b020cf07f43
```

SPDX format



```
Relationship: SPDXRef-perl DEPENDENCY_OF SPDXRef-version
Relationship: SPDXRef-ActiveState-Utils DEPENDENCY_OF SPDXRef-XML-Parser
Relationship: SPDXRef-Algorithm-C3 DEPENDENCY_OF SPDXRef-Class-C3
Relationship: SPDXRef-Algorithm-Diff DEPENDENCY_OF SPDXRef-Text-Diff
Relationship: SPDXRef-Archive-Zip DEPENDENCY_OF SPDXRef-ActiveState-Utils
Relationship: SPDXRef-B-Keywords DEPENDENCY_OF SPDXRef-Perl-Critic
Relationship: SPDXRef-CGI DEPENDENCY_OF SPDXRef-HTTP-Server-Simple
Relationship: SPDXRef-CPAN-Meta DEPENDENCY_OF SPDXRef-Module-Build
Relationship: SPDXRef-CPAN-Meta-YAML DEPENDENCY_OF SPDXRef-Module-Build
Relationship: SPDXRef-Capture-Tiny DEPENDENCY_OF SPDXRef-Test-Differences
Relationship: SPDXRef-Carp-Clan DEPENDENCY_OF SPDXRef-Bit-Vector
Relationship: SPDXRef-Class-C3 DEPENDENCY_OF SPDXRef-MRO-Compat
Relationship: SPDXRef-Class-Data-Inheritable DEPENDENCY_OF SPDXRef-Exception-Class
Relationship: SPDXRef-Class-Inspector DEPENDENCY_OF SPDXRef-SOAP-Lite
Relationship: SPDXRef-Class-Load DEPENDENCY_OF SPDXRef-Moose
Relationship: SPDXRef-Class-Load-XS DEPENDENCY_OF SPDXRef-Moose
Relationship: SPDXRef-Class-Tiny DEPENDENCY_OF SPDXRef-Pod-Spell
Relationship: SPDXRef-Clone DEPENDENCY_OF SPDXRef-SQL-Statement
Relationship: SPDXRef-Compress-Raw-Bzip2 DEPENDENCY_OF SPDXRef-IO-Compress
Relationship: SPDXRef-Compress-Raw-Zlib DEPENDENCY_OF SPDXRef-IO-Compress
Relationship: SPDXRef-Config-Tiny DEPENDENCY_OF SPDXRef-Perl-Critic
Relationship: SPDXRef-Convert-BinHex DEPENDENCY_OF SPDXRef-MIME-tools
Relationship: SPDXRef-Data-OptList DEPENDENCY_OF SPDXRef-Sub-Exporter
Relationship: SPDXRef-Devel-GlobalDestruction DEPENDENCY_OF SPDXRef-Moose
Relationship: SPDXRef-Devel-OverloadInfo DEPENDENCY_OF SPDXRef-Moose
Relationship: SPDXRef-Devel-Refcount DEPENDENCY_OF SPDXRef-Win32-LongPath
Relationship: SPDXRef-Devel-StackTrace DEPENDENCY_OF SPDXRef-Moose
Relationship: SPDXRef-Dist-CheckConflicts DEPENDENCY_OF SPDXRef-Package-Stash
Relationship: SPDXRef-Email-Address DEPENDENCY_OF SPDXRef-Perl-Critic
```