Microsoft

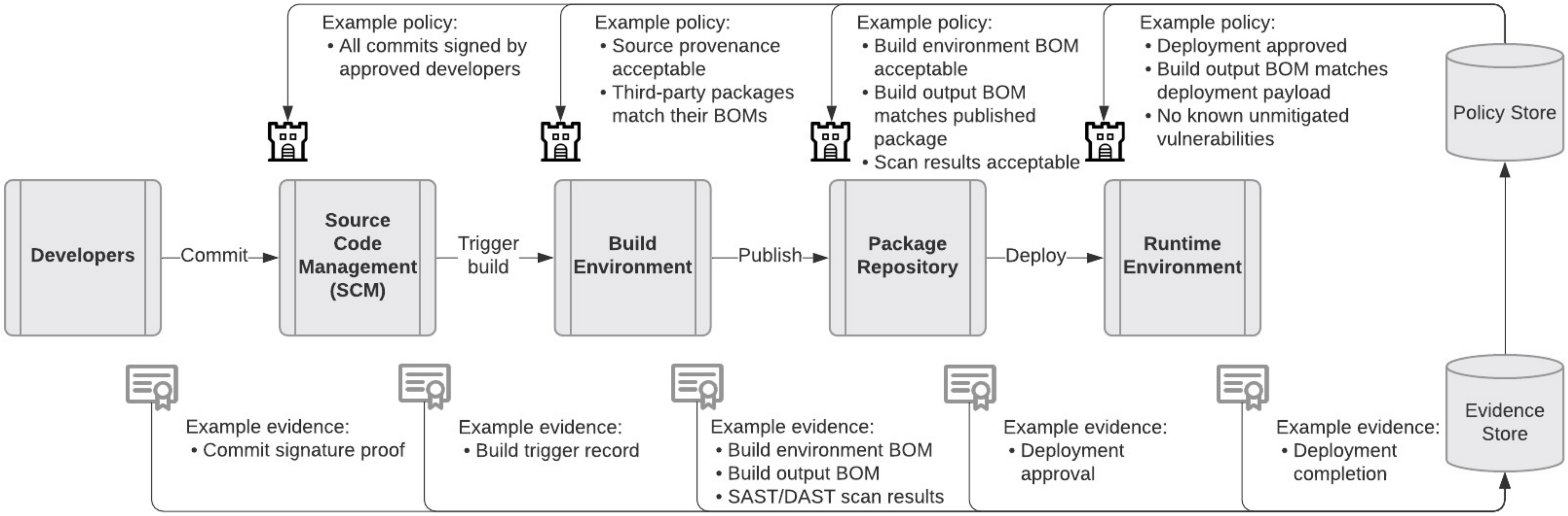
Criteria and attestation for maintaining provenance of code and components including open-source software

NIST Executive Order on Cyber Security Workshop
November 8, 2021

Relevant Executive Order Sections

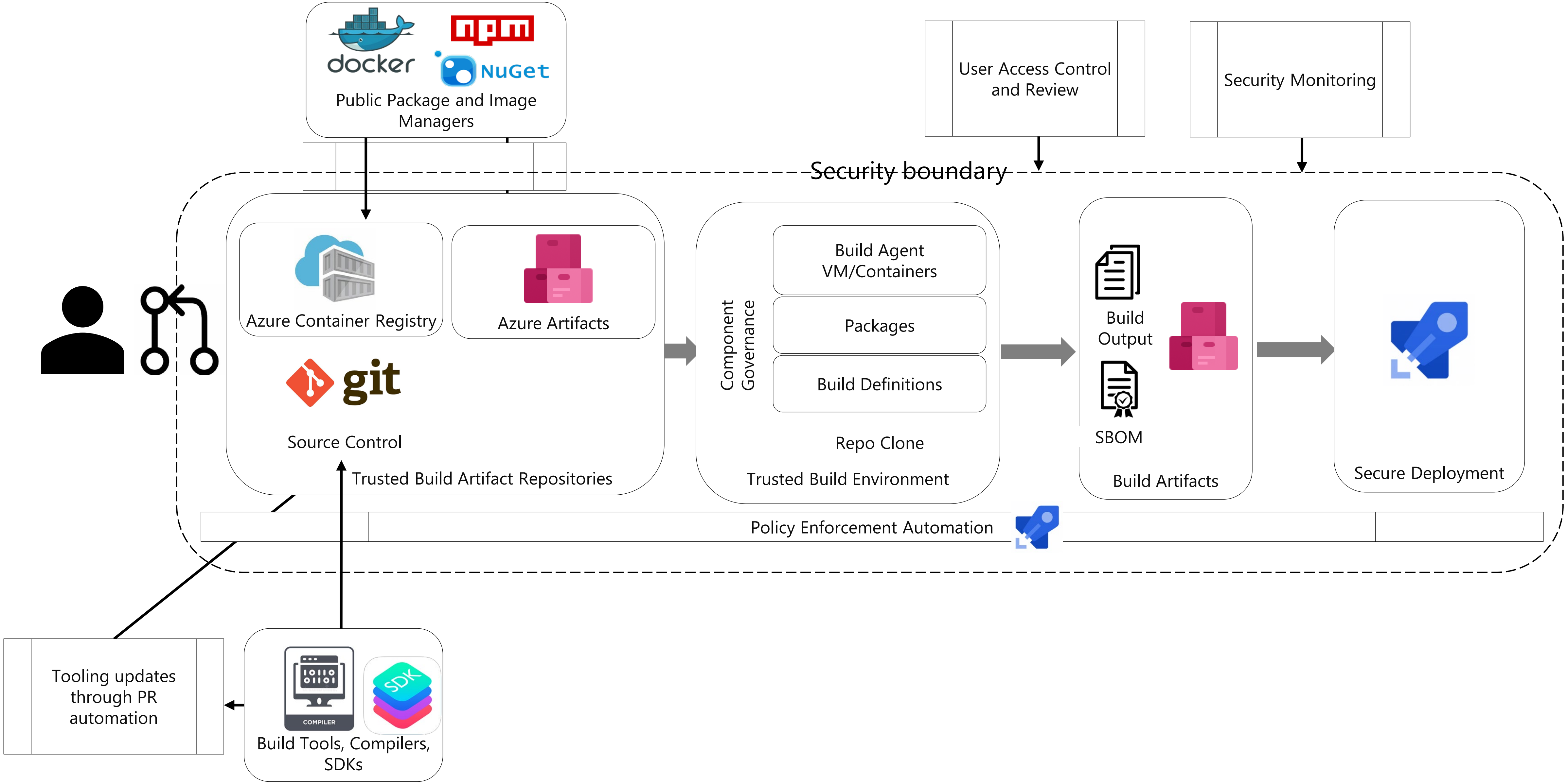
- 4 (e) (vi) maintaining accurate and up-to-date data, provenance (i.e., origin) of software code or components, and controls on internal and third-party software components, tools, and services present in software development processes, and performing audits and enforcement of these controls on a recurring basis;
- 4 (e) (vii) providing a purchaser a Software Bill of Materials (SBOM) for each product directly or by publishing it on a public website;
- 4 (e) (x) ensuring and attesting, to the extent practicable, to the integrity and provenance of open source software used within any portion of a product.

Supply Chain Integrity Model

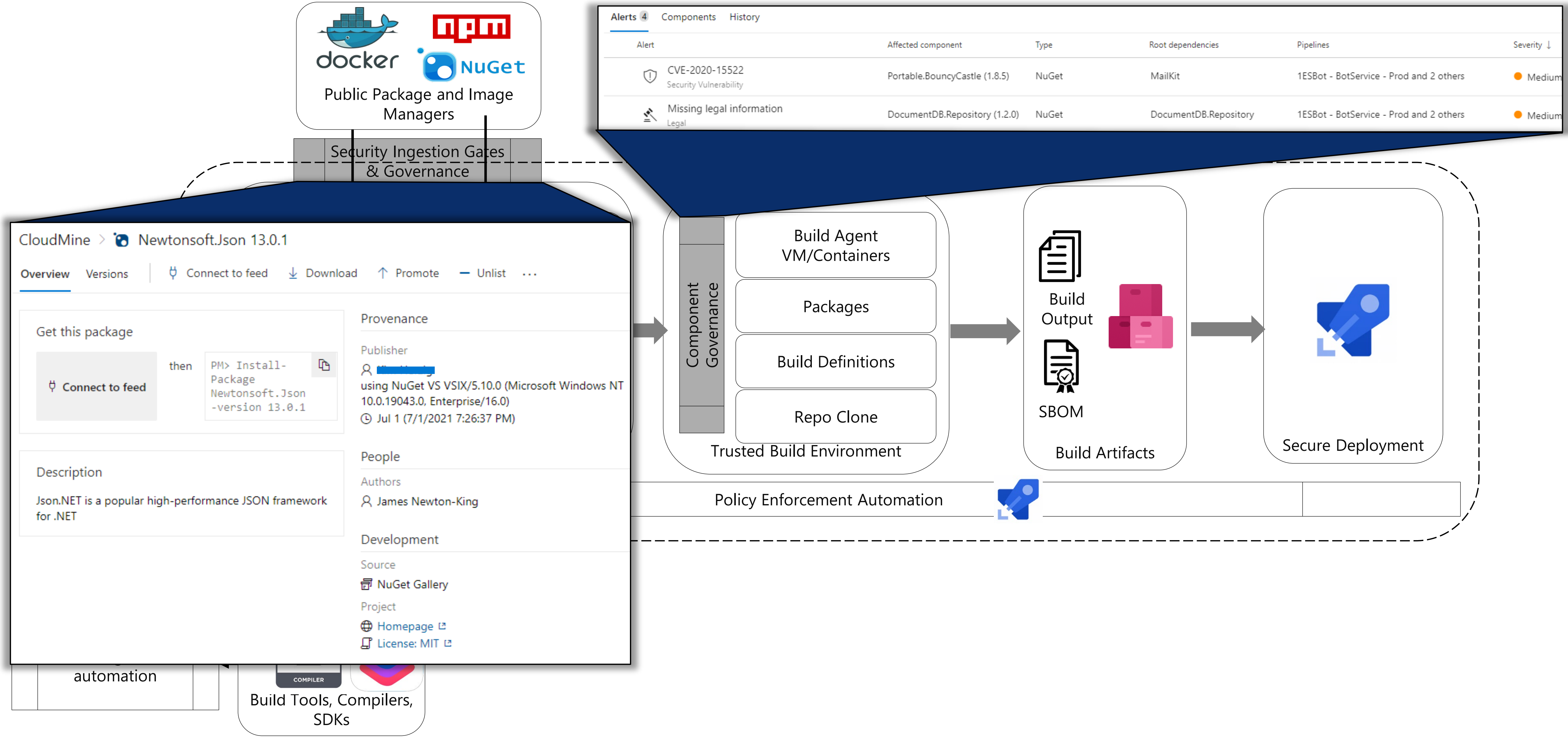


GitHub - microsoft/scim: Supply Chain Integrity Model

Build tool and OSS provenance management today


docker
npm
NuGet
Public Package and Image Managers
User Access Control and Review
Security Monitoring
Security boundary
Azure Container Registry
Azure Artifacts
git
Source Control
Trusted Build Artifact Repositories
Component Governance
Build Agent VM/Containers
Packages
Build Definitions
Repo Clone
Trusted Build Environment
Build Output
SBOM
Build Artifacts
Secure Deployment
Policy Enforcement Automation
Tooling updates through PR automation
COMPILER
SDK
Build Tools, Compilers, SDKs

OSS ingestion & provenance



Public Package and Image Managers
docker
npm
NuGet
Security Ingestion Gates & Governance
Component Governance
Build Agent VM/Containers
Packages
Build Definitions
Repo Clone
Trusted Build Environment
Build Output
SBOM
Build Artifacts
Secure Deployment
Policy Enforcement Automation
automation
COMPILER
Build Tools, Compilers, SDKs

Alerts 4 | Components | History

	Alert	Affected component	Type	Root dependencies	Pipelines	Severity ↓
	CVE-2020-15522 Security Vulnerability	Portable.BouncyCastle (1.8.5)	NuGet	MailKit	1ESBot - BotService - Prod and 2 others	● Medium
	Missing legal information Legal	DocumentDB.Repository (1.2.0)	NuGet	DocumentDB.Repository	1ESBot - BotService - Prod and 2 others	● Medium

CloudMine > Newtonsoft.Json 13.0.1

Overview | Versions | Connect to feed | Download | Promote | Unlist | ...

Get this package

Connect to feed then

```
PM> Install-Package Newtonsoft.Json -version 13.0.1
```

Description

Json.NET is a popular high-performance JSON framework for .NET

Provenance

Publisher

[redacted]

using NuGet VS VSIX/5.10.0 (Microsoft Windows NT 10.0.19043.0, Enterprise/16.0)

Jul 1 (7/1/2021 7:26:37 PM)

People

Authors

James Newton-King

Development

Source

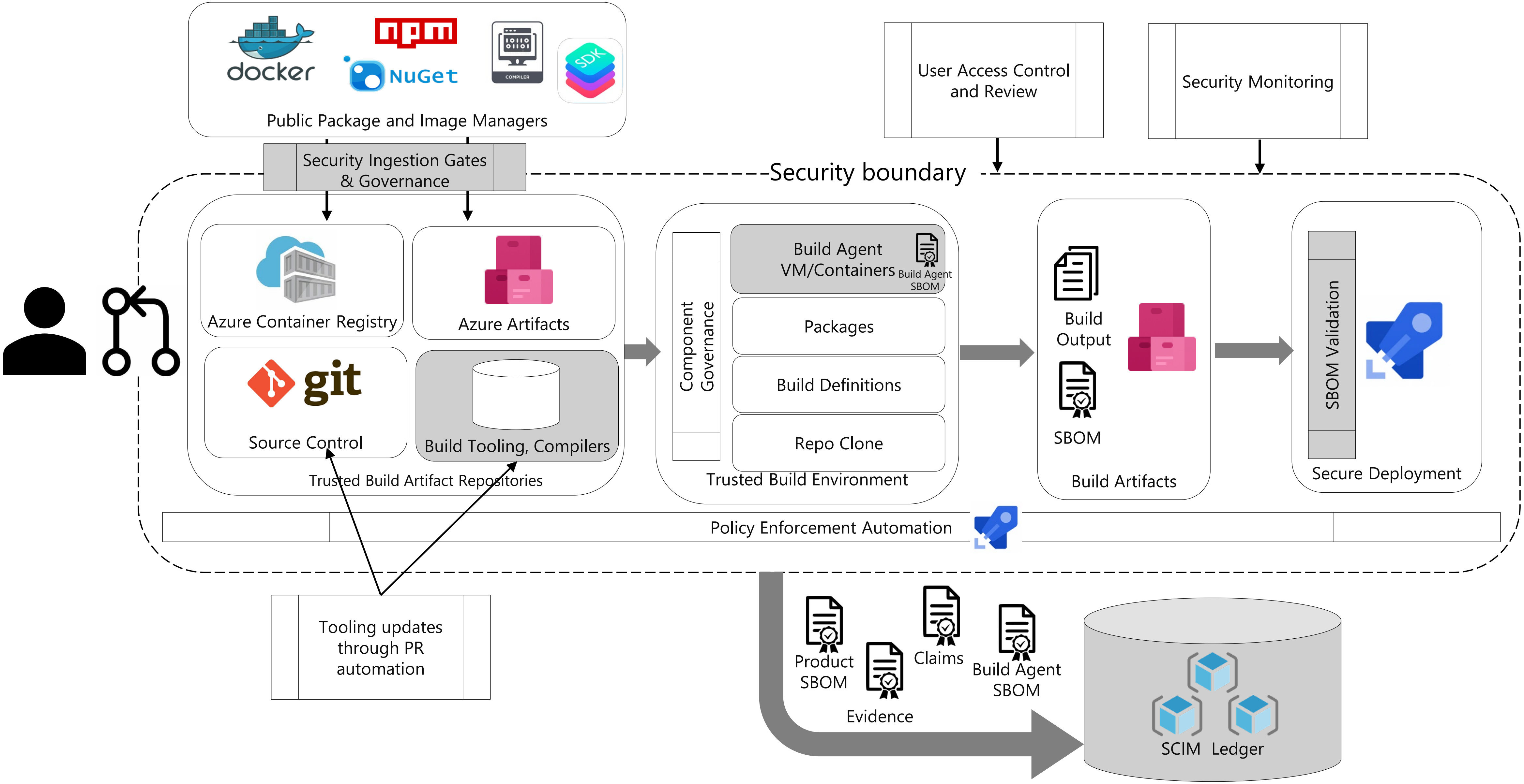
NuGet Gallery

Project

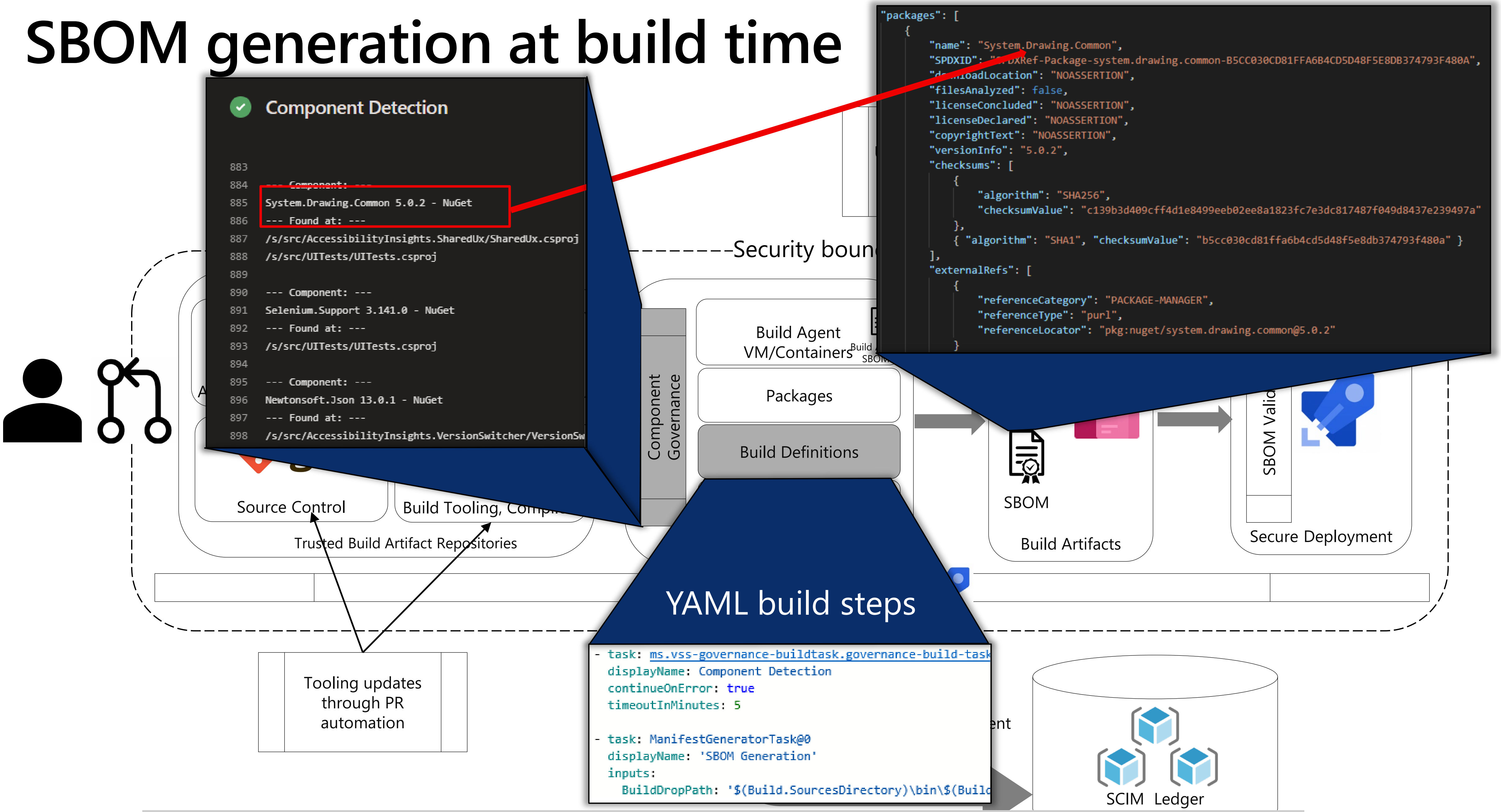
Homepage

License: MIT

Future tool and OSS provenance management



SBOM generation at build time



Component Detection

```
--- Component: ---
System.Drawing.Common 5.0.2 - NuGet
--- Found at: ---
/s/src/AccessibilityInsights.SharedUx/SharedUx.csproj
/s/src/UITests/UITests.csproj

--- Component: ---
Selenium.Support 3.141.0 - NuGet
--- Found at: ---
/s/src/UITests/UITests.csproj

--- Component: ---
Newtonsoft.Json 13.0.1 - NuGet
--- Found at: ---
/s/src/AccessibilityInsights.VersionSwitcher/VersionSw
```

```
"packages": [
    {
        "name": "System.Drawing.Common",
        "SPDXID": "SPDXRef-Package-system.drawing.common-B5CC030CD81FFA6B4CD5D48F5E8DB374793F480A",
        "downloadLocation": "NOASSERTION",
        "filesAnalyzed": false,
        "licenseConcluded": "NOASSERTION",
        "licenseDeclared": "NOASSERTION",
        "copyrightText": "NOASSERTION",
        "versionInfo": "5.0.2",
        "checksums": [
            {
                "algorithm": "SHA256",
                "checksumValue": "c139b3d409cff4d1e8499eeb02ee8a1823fc7e3dc817487f049d8437e239497a"
            },
            { "algorithm": "SHA1", "checksumValue": "b5cc030cd81ffa6b4cd5d48f5e8db374793f480a" }
        ],
        "externalRefs": [
            {
                "referenceCategory": "PACKAGE-MANAGER",
                "referenceType": "purl",
                "referenceLocator": "pkg:nuget/system.drawing.common@5.0.2"
            }
```

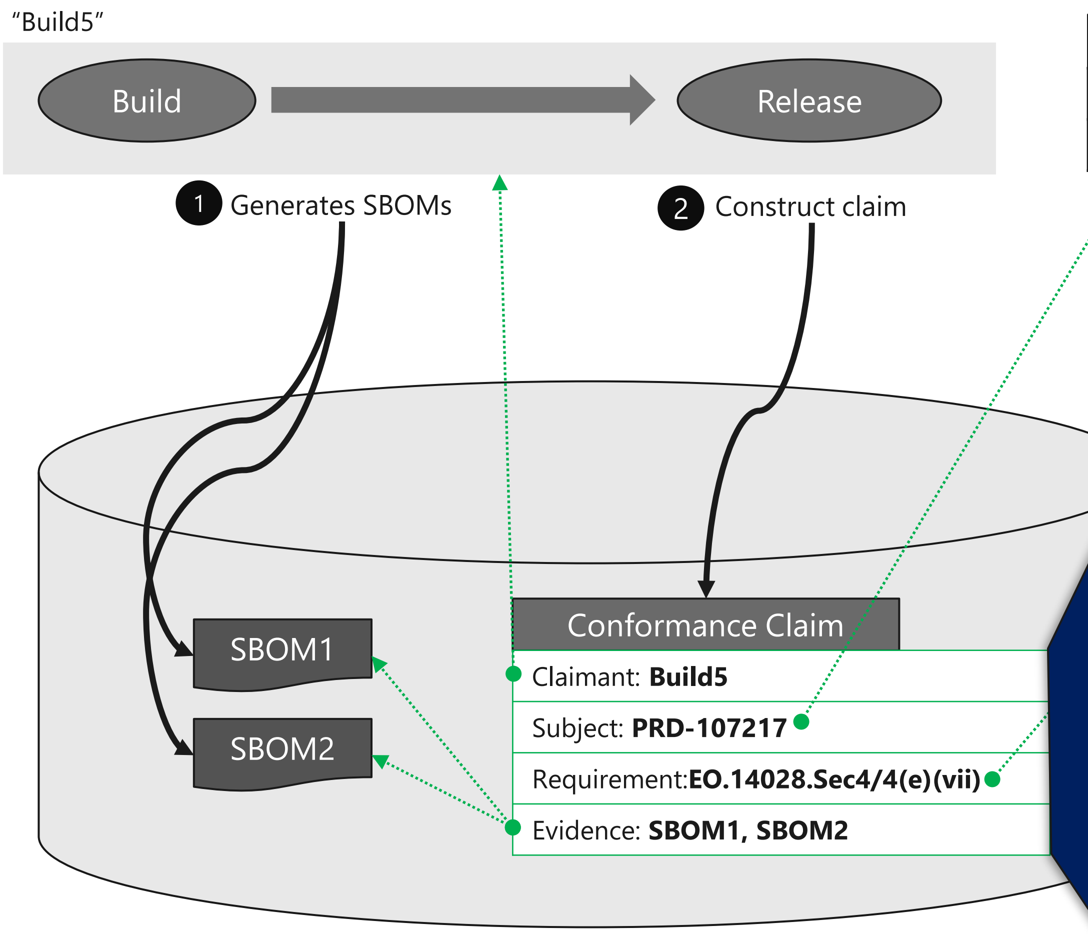
YAML build steps

```
- task: ms.vss-governance-buildtask.governance-build-task
  displayName: Component Detection
  continueOnError: true
  timeoutInMinutes: 5

- task: ManifestGeneratorTask@0
  displayName: 'SBOM Generation'
  inputs:
    BuildDropPath: '$(Build.SourcesDirectory)\bin\$(Build
```

For more info: Generating Software Bills of Materials (SBOMs) with SPDX at Microsoft - Engineering@Microsoft

Tracking conformance



"Build5"

Build → Release

1 Generates SBOMs

2 Construct claim

SBOM1

SBOM2

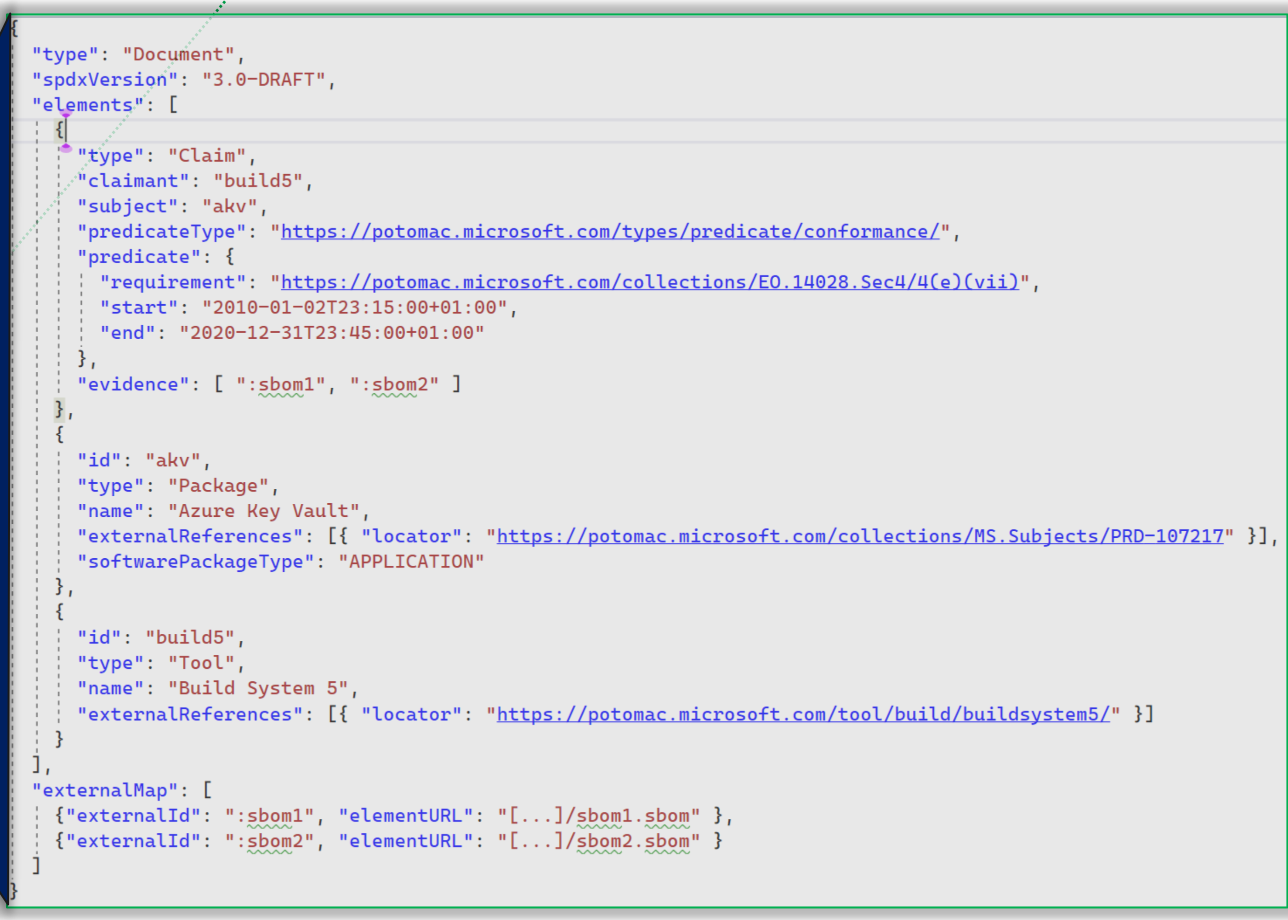
Conformance Claim
Claimant: **Build5**
Subject: **PRD-107217**
Requirement:**EO.14028.Sec4/4(e)(vii)**
Evidence: **SBOM1, SBOM2**

Subject Inventory

PRD-107217	Azure Key Vault
…	…

Requirement Inventory

EO.14028.Sec4/4(e)(vii)	Provide a purchaser an (SBOM) for each product
…	…



```
{
  "type": "Document",
  "spdxVersion": "3.0-DRAFT",
  "elements": [
    {
      "type": "Claim",
      "claimant": "build5",
      "subject": "akv",
      "predicateType": "https://potomac.microsoft.com/types/predicate/conformance/",
      "predicate": {
        "requirement": "https://potomac.microsoft.com/collections/EO.14028.Sec4/4(e)(vii)",
        "start": "2010-01-02T23:15:00+01:00",
        "end": "2020-12-31T23:45:00+01:00"
      },
      "evidence": [ ":sbom1", ":sbom2" ]
    },
    {
      "id": "akv",
      "type": "Package",
      "name": "Azure Key Vault",
      "externalReferences": [{ "locator": "https://potomac.microsoft.com/collections/MS.Subjects/PRD-107217" }],
      "softwarePackageType": "APPLICATION"
    },
    {
      "id": "build5",
      "type": "Tool",
      "name": "Build System 5",
      "externalReferences": [{ "locator": "https://potomac.microsoft.com/tool/build/buildsystem5/" }]
    }
  ],
  "externalMap": [
    {"externalId": ":sbom1", "elementURL": "[...]/sbom1.sbom" },
    {"externalId": ":sbom2", "elementURL": "[...]/sbom2.sbom" }
  ]
}
```

Microsoft

Thank you

NIST Executive Order on Cyber Security Workshop
November 8, 2021