Software Supply Chain Security

An Industry Approach, CDF – Security SIG

Kay Williams, @kaywilyums
Principal Program Manager – Supply Chain Security, Azure Office of the CTO, Microsoft
Chair - Security Special Interest Group (SIG), CD Foundation
Co-Chair – Software Bill of Materials Working Group, Consortium for Information and Software Quality

Santiago Torres Arias
PHD student - in-toto project
NYU Center for Cyber Security

Agenda

Concepts

User Scenarios

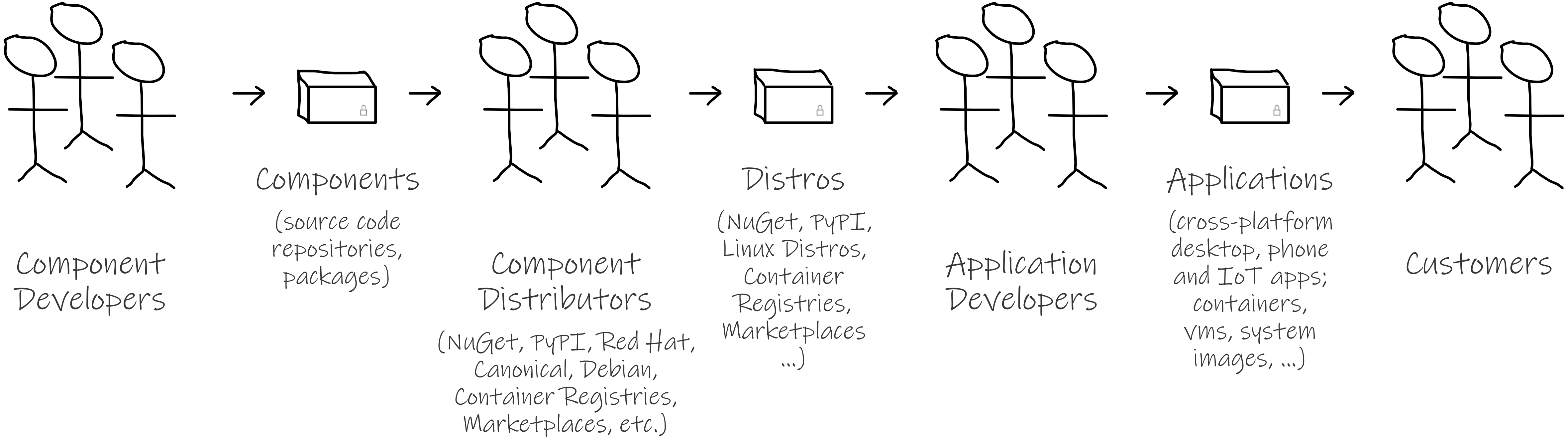
Demo – in-toto and KubeSec

Industry Collaboration

Timeline

How to Get Involved

Software Supply Chain - Overview



Component Developers

→ Components

(source code repositories, packages)

→ Component Distributors

(NuGet, PyPI, Red Hat, Canonical, Debian, Container Registries, Marketplaces, etc.)

→ Distros

(NuGet, PyPI, Linux Distros, Container Registries, Marketplaces ...)

→ Application Developers

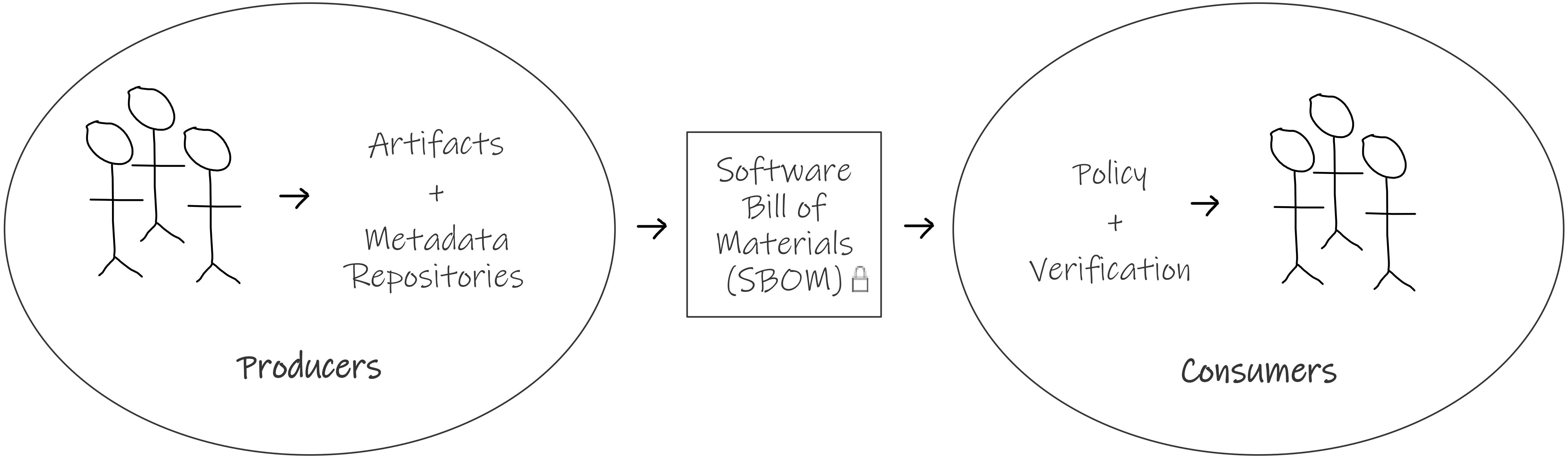
→ Applications

(cross-platform desktop, phone and IoT apps; containers, vms, system images, ...)

→ Customers

Job to be Done: As a participant in the software supply chain, I can produce and consume trustworthy software.

Software Supply Chain – Concepts



Artifact

- Component of Software
  - File
  - Package - grouping of files
  - Package repository - grouping of packages
  - Container - grouping of packages and files
  - Cloud Service - grouping of containers, packages and files
  - Installed System – grouping of packages and files
  - Snippet - byte range in a file

Artifact metadata

- Describes artifacts
  - Identity (name, producer, version, hash)
  - Authenticity (cryptographic signatures)
  - Build information (tools, environment, configuration)
  - Intellectual property information (license)
  - Relationships with other artifacts (describes, contains)

Metadata Repositories

- Distribute Metadata
  - Storage, query and retrieval
  - Cryptographically sign metadata
  - Manage key distribution, revocation and replacement
- Examples (future):
  - Source Code Repositories – e.g. GitHub, GitLabs, etc.
  - Container Registries - Docker, Google, Microsoft, etc.
  - Package Repositories - Windows Update, Debian, Red Hat, etc.
  - Installed System Package Repositories - Windows, iOS, Linux, etc.

Software Bill of Materials (SBOM)

- Allows artifact metadata exchange
  - Data format for exchange between producers and consumers
  - Standard format based on XML Metadata Interchange (XMI)
  - Can be converted to JSON, XML, other data formats

Artifact Policy

- Describes requirements for artifact consumption
  - Allowed producers
  - Allowed licenses
  - Allowed build environments
  - Required security steps (e.g. scanning)
  - Required certifications (e.g. SDL, industry audits)
  - Expected order of steps in the chain (e.g. to prevent man in the middle attacks)

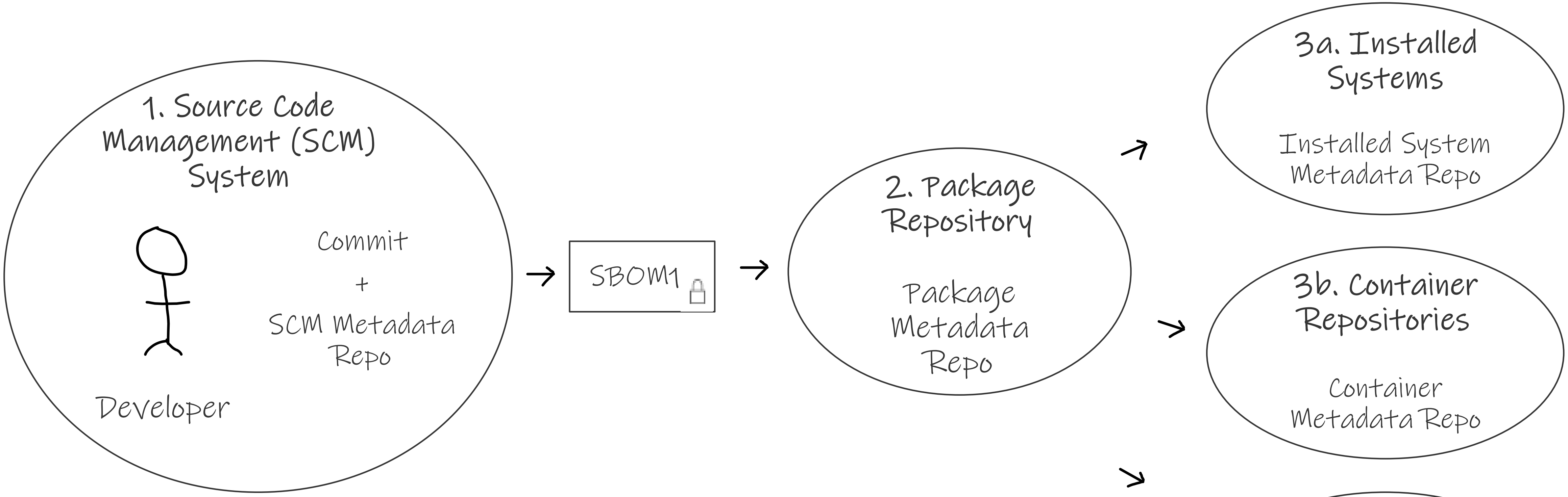
Artifact Verification

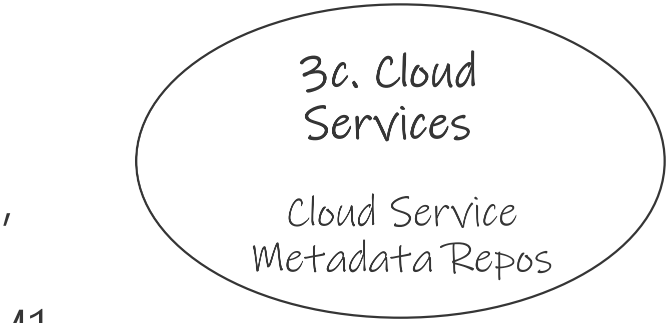
- Allows inspection and policy enforcement of artifacts
  - Signature verification
  - Artifact hash validation
  - License validation
  - Build/build environment validation (e.g. reproducible build)
  - Required steps validation
  - Required certification validation

Software Supply Chain - Scenarios

Scenario	Description	Bill of Materials	Policy
Identity	Enable unambiguous referral to software components, e.g. to consume, purchase, transfer, inventory or associate with outside databases, e.g. security vulnerability	Unique identity	Allowed identities
Build Security	Enable validation of choices made for securing software during the creation process (pedigree)	Information about build environment	Allowed build environments
Authenticity	Enable validation of the software provider (provenance)	Cryptographic signature	Allowed signatures
Integrity	Enable validation of whether software (or the SBOM itself) has been altered, e.g. during transmission or on deployed systems	SBOM signature, component hashes	Allowed hash and signature types
License	Enable validation of proper and legal use of software	Intellectual property information	Allowed intellectual property
Chain of Custody	Enable validation that software has completed expected steps in expected order, e.g. including security and compliance audits	Steps in the chain	Allowed and required steps and order

Identity Scenario – Security Vulnerability

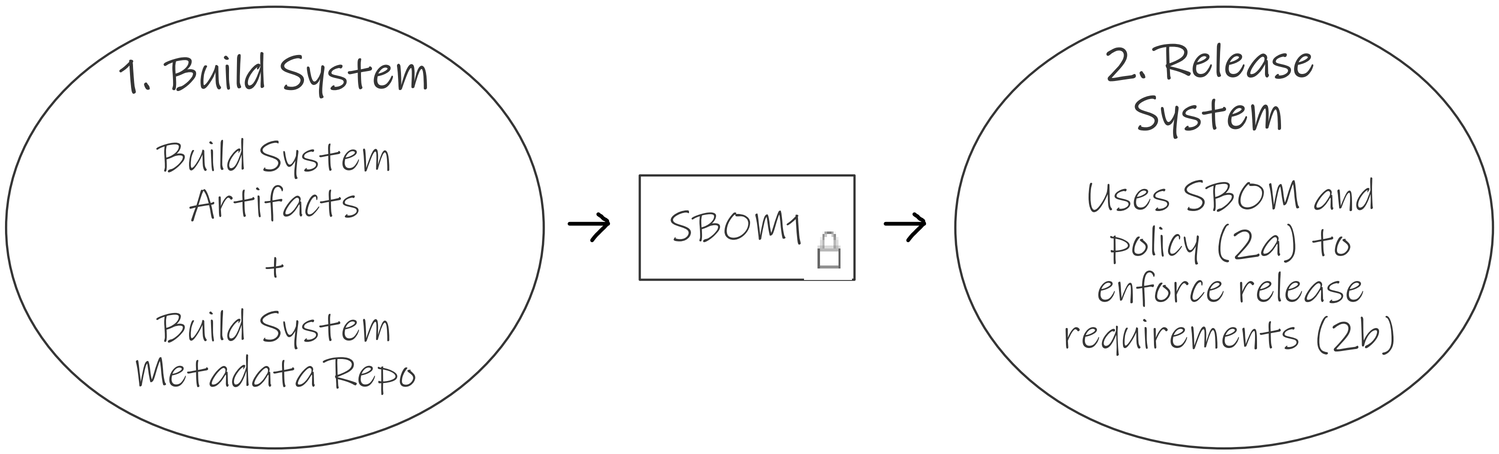




4. Security professional reports a new zero-day vulnerability in the commit identified by SBOM1

5. Scanning tools query metadata repos to identify files, packages, containers, systems, cloud services containing SBOM1

Integrity Scenario – Enforce Signature and Hash


1. Build System
Build System Artifacts
+
Build System Metadata Repo
→
SBOM1
→
2. Release System
Uses SBOM and policy (2a) to enforce release requirements (2b)

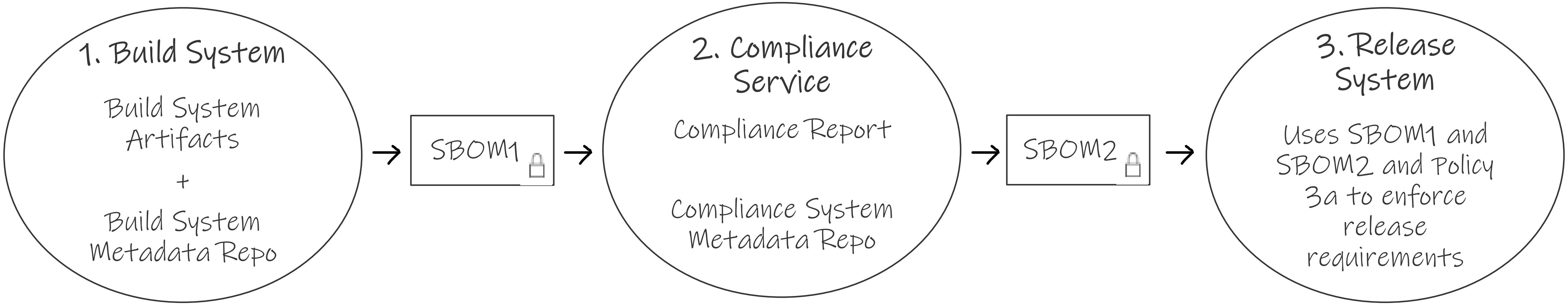
2a. Policy:

- Signature of build system must match signature of allowed build systems
- Hashes of received artifacts must match hash in SBOM

2b. Verification:

- Allowed build system?
- Hashes match?

Chain of Custody Scenario – Enforce Certifications


1. Build System
Build System Artifacts
+
Build System Metadata Repo
SBOM1
2. Compliance Service
Compliance Report
Compliance System Metadata Repo
SBOM2
3. Release System
Uses SBOM1 and SBOM2 and Policy 3a to enforce release requirements

3a. Policy

- Compliance service must be in chain
- Compliance report must be positive

In-toto and KubeSec

Software Supply Chain - Collaboration

IDEs

Android Studio, Code Blocks ppCode, CodeCharge Studio Atom, CodeLobster BlueJ, CodePen, Clion, DataGrip Cloud9 IDE, Eclipse, GoLand, IDLE, IntelliJ, IDEA LINX, Microsoft Visual Studio, MPLAB, NetBeans, PhpStorm, Pycharm, Rider, RubyMine, Spiralogics Application Architecture, WebStorm, Xcode, Zend Studio

Frameworks/Libraries/Tools

.NET, Angular, Ansible. Apache Spark, ASP.NET, Bootstrap, Chef, Cordova, CryEngine, Django, Drupal, Express, Flask, Flutter, Hadoop, HTML5 Builder, Laravel, Node.js, Pandas, Puppet, React Native, React.js, Ruby on Rails, Spring, TensorFlow, Torch/PyTorch, Unity D, Unreal Engine, Visual Online, Vue.js. Xamarin

Cloud Tools

Azure DevOps, AWS, CodeBuild, Cloud Foundry, Google Cloud Build, Kwatee, Pivotal Red Hat

Source Code & Package Repositories

Amazon ECR, Assembla, Azure Container Registry, Beanstalk, Bitbucket, Codebase, Docker Hub, GitHub, GitLab, Glitch, Google Container Registry, JFrog Artifactory, JFrog Xray, inedo, Kubernetes, Launchpad, Maven, Nexus (Sonatype), Phabricator, ProjectLocker Repository Hosting, Savannah, SourceForge, SourceRepo, Subversion, Unfuddle

Build & Build Choreography Capabilities

Ansible, Autorabit, Bamboo, Bitrise, Buildkite, Buildroot, CircleCI, CMake, CruiseControl, Final builder, GCC, GitHub Actions, Gitlab CI, GoCD, Integrity, Jenkins, Spinnaker, Strider CD, TeamCity, Tekton, Terraform, Travis CI, Urbancode, Vagrant

Software Composition Analysis Capabilities

Black Duck Software Composition Analysis (Synopsys), CAST Highlight (CAST Software), Finate State, FlexNet Code Insite (Flexera), Ion Channel, Insignary, SourceClear, Sonatype, Snyk, WhiteSource

Software Update Systems

apt-get, dnf, Windows Update, yum, …

Runtime Security Systems

AppLocker, …

Software Supply Chain – Current Collaborators

Apache Foundation

Cast Software

CD Foundation (SIG-Security)

Center for Information and Software Quality (CISQ)

CloudBees (Jenkins)

GitHub

Google (Grafeas, Kritis)

IBM

Ion Channel

JFrog

Linux Foundation (SPDX)

Microsoft

MITRE Corporation

Linux Foundation

National Telecommunications and Information Administration (NTIA)

New York University (in-toto, TUF)

Snyk

Software Package Data Exchange (SPDX)

Sonatype

Source Auditor

WhiteSource

Timeline

FY 2019

- CDF Security SIG
- Software Bill of Materials Working Group (Nashville)
- Software Supply Chain Meetup (San Diego)

FY 2020

- Draft Standards - SBOM, Policy, Artifact Repositories
- Pilot Implementations

FY 2021, 2022

- OMG Standards, ISO Standards
- Production Implementations

Get Involved

Attend the Supply Chain Meetup

- Thursday 9AM-12PM
- Conference Room Torrey Pines 3
- 1st Floor – North Tower
- kayw@microsoft.com

Connect with us:

- Slack: #sig-security-supply-chain
- List: sig-security-supply-chain@lists.cd.foundation
- Github: https://github.com/cdfoundation/sig-security-software-supply-chain

Related Talks

Securing the Software Supply Chain with in-toto

- Tuesday 10:55
- Room 23BC – San Diego Convention Center

Using TUF and in-toto to Tighten the Release Process

- Wednesday 10:55
- Room 23BC – San Diego Convention Center