CLOUDNATIVE SECURITYCON

NORTH AMERICA 2023

CLOUDNATIVE SECURITYCON NORTH AMERICA 2023

The Next Steps in Software Supply Chain Security

Brandon Lum (@lumjjb)
Software Engineer, Google

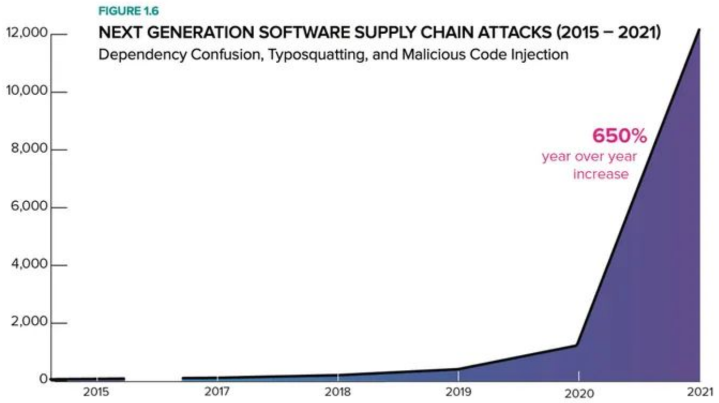


FIGURE 1.6

NEXT GENERATION SOFTWARE SUPPLY CHAIN ATTACKS (2015 – 2021)

Dependency Confusion, Typosquatting, and Malicious Code Injection

There has been an astonishing

742%

average annual increase in Software Supply Chain attacks over the past 3 years.

Read the 8th Annual State of the Software Supply Chain Report

01010
11101
00101
66%
OF ATTACKS FOCUS ON THE SUPPLIER'S CODE
58%
of attacks aimed to access data
SUPPLY CHAIN ATTACKS ON THE RISE
62%
of the attacks exploit the trust of customers in their supplier
62%
OF ATTACKS RELY ON MALWARE

ENISA Threat Landscape for Supply Chain Attacks

Increase in Attacks lead to strong industry response

Producing Trusted Software & Attestations

TEKTON

SLSA

FRSCA

in-toto

sigstore

SPDX

TUF

trivy

grype

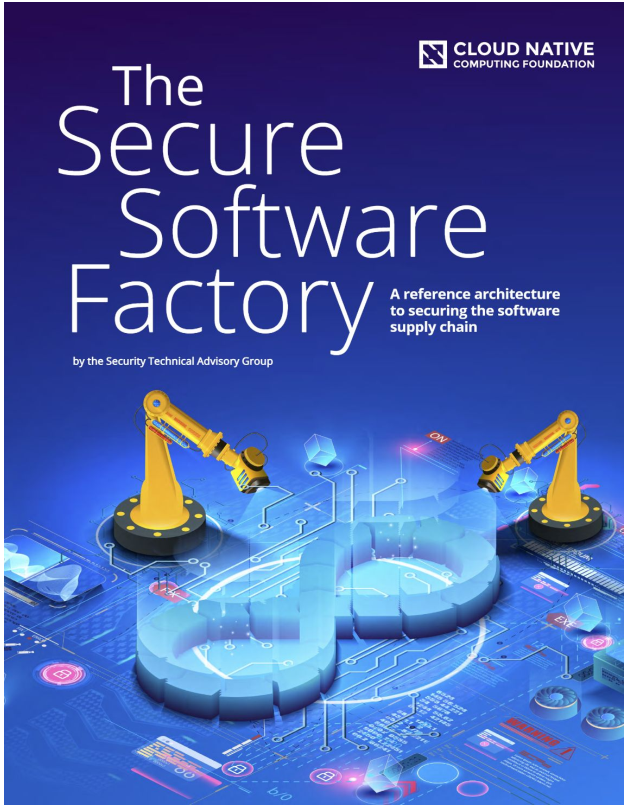
Scorecards

Keylime

SPIRE

CycloneDX

spiffe



CLOUD NATIVE COMPUTING FOUNDATION

The Secure Software Factory

A reference architecture to securing the software supply chain

by the Security Technical Advisory Group

Producing Trusted Software & Attestations

TEKTON

SLSA

FRSCA

in-toto

sigstore

SPDX

TUF

trivy

grype

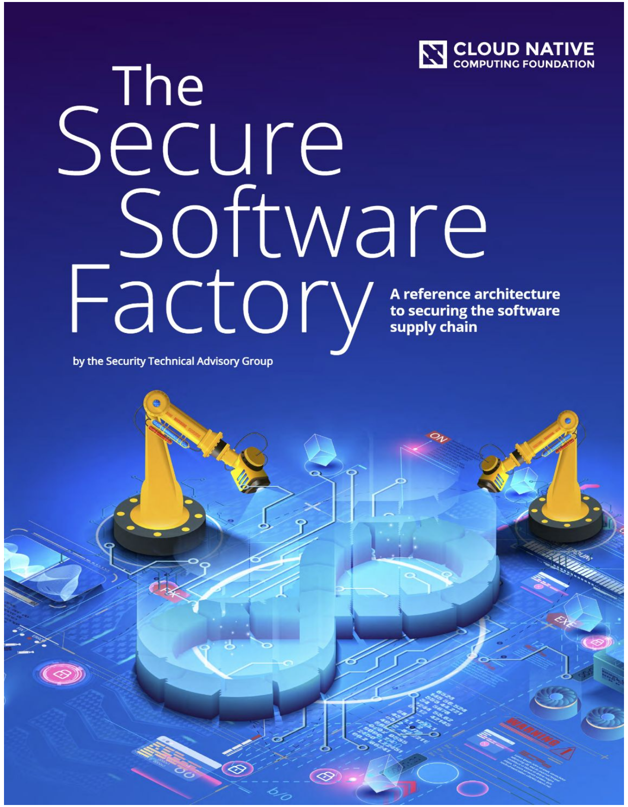
Scorecards

Keylime

SPIRE

CycloneDX

spiffe



CLOUD NATIVE
COMPUTING FOUNDATION

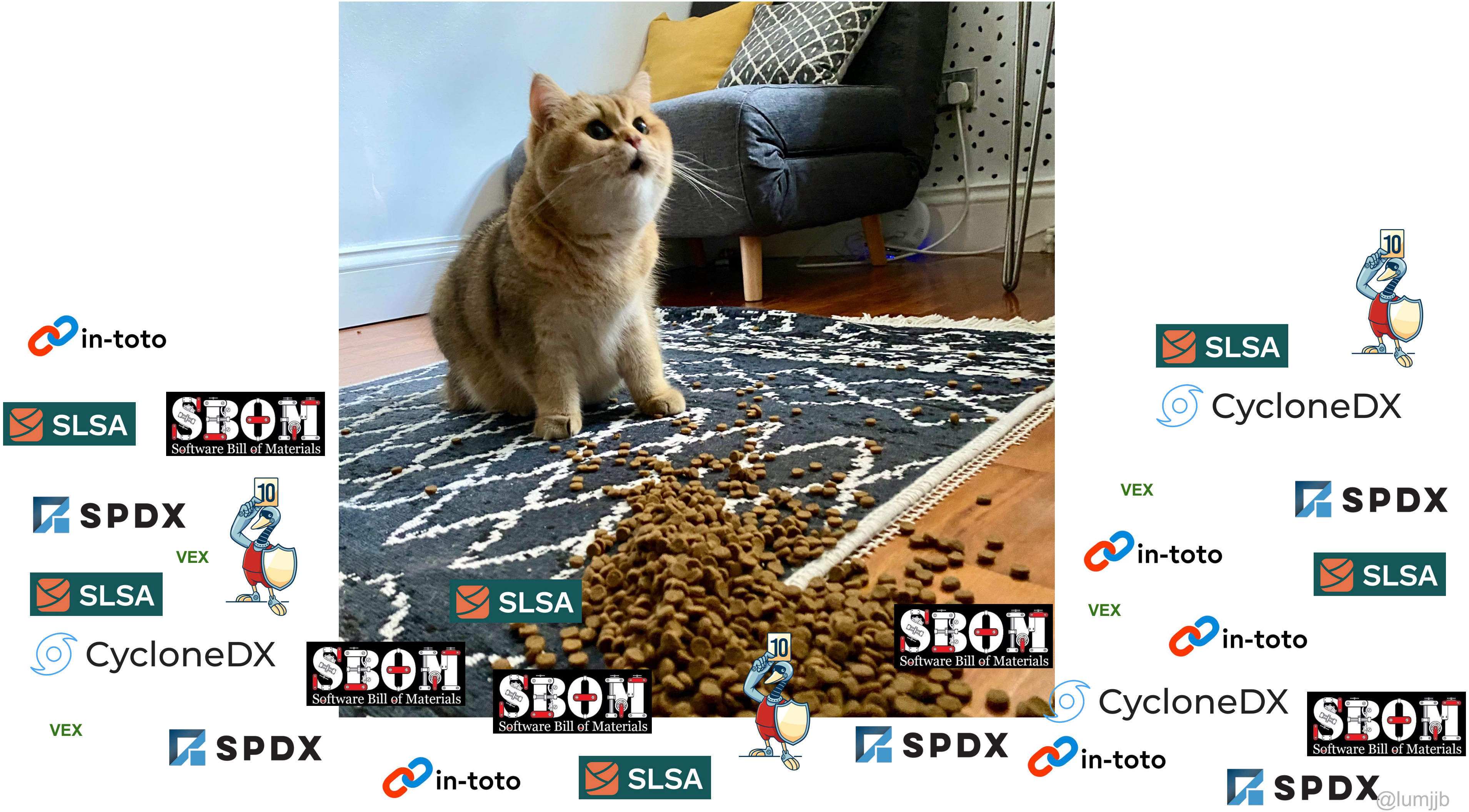
The
Secure
Software
Factory

A reference architecture to securing the software supply chain

by the Security Technical Advisory Group

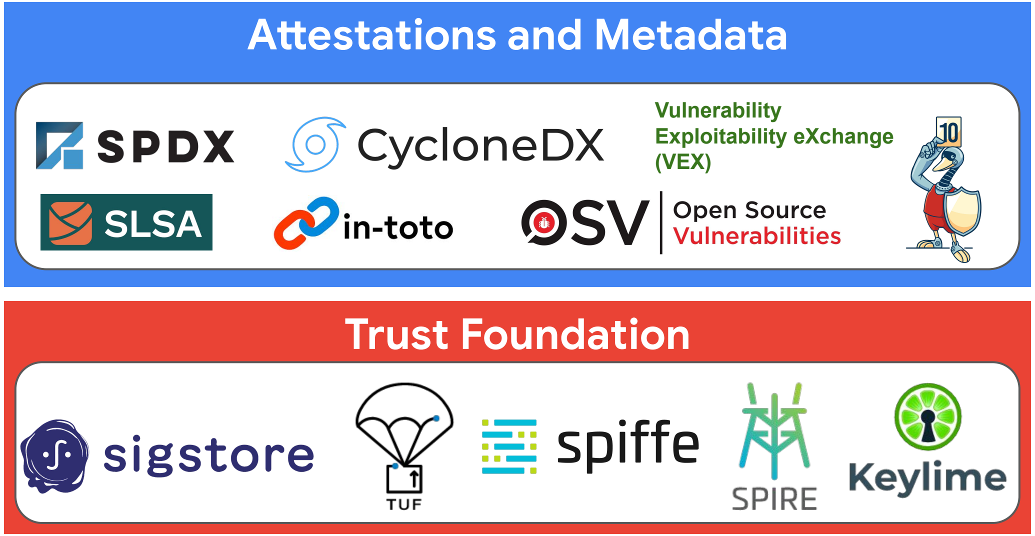
Producing and Consuming

Producing and Consuming


in-toto
SLSA
SBOM
Software Bill of Materials
SPDX
10
VEX
SLSA
CycloneDX
VEX
SPDX
SLSA
SBOM
Software Bill of Materials
SBOM
Software Bill of Materials
in-toto
SLSA
10
SBOM
Software Bill of Materials
SPDX
10
SLSA
CycloneDX
VEX
SPDX
in-toto
SLSA
VEX
in-toto
CycloneDX
SBOM
Software Bill of Materials
in-toto
SPDX

@lumjjb

Outcome of Producing



Attestations and Metadata

SPDX
CycloneDX
Vulnerability Exploitability eXchange (VEX)
10
SLSA
in-toto
OSV
Open Source Vulnerabilities

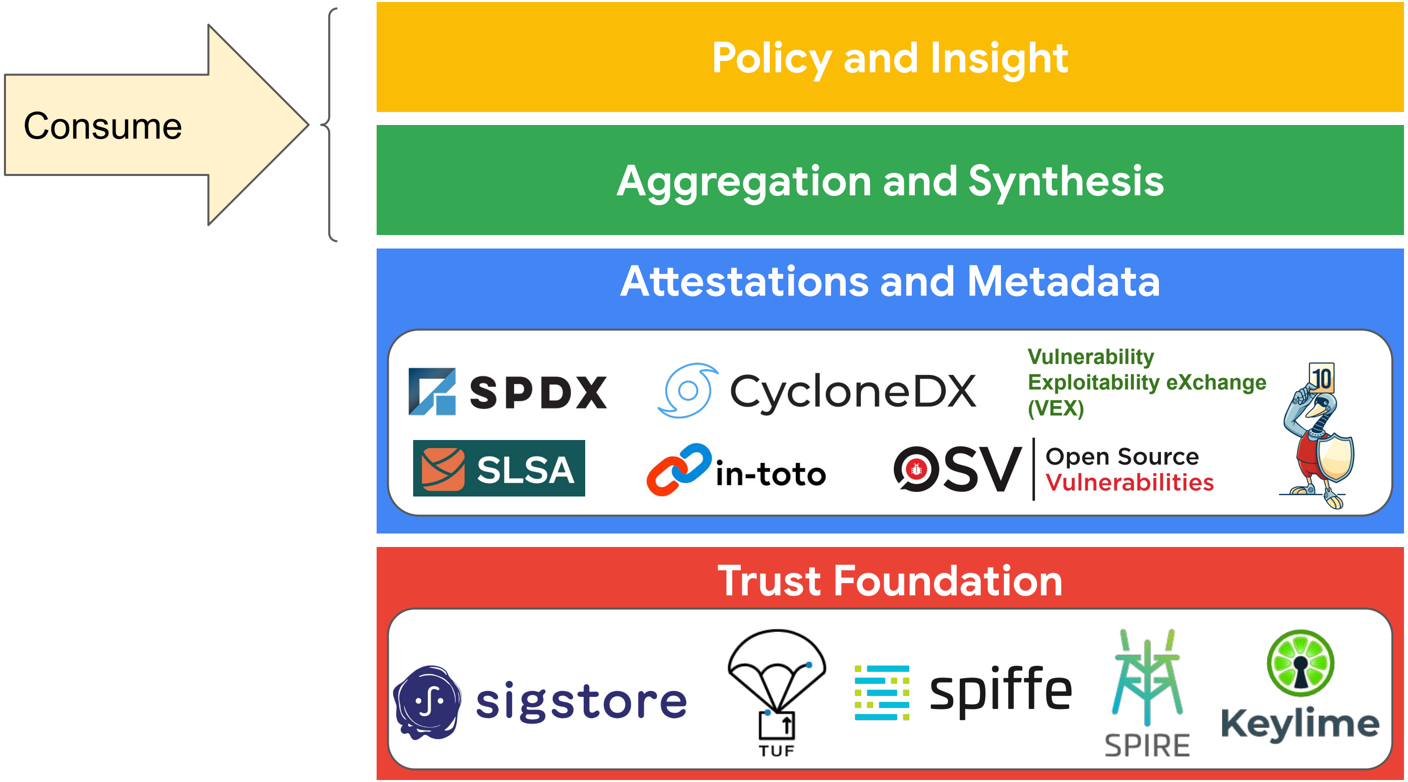
Trust Foundation

sigstore
TUF
spiffe
SPIRE
Keylime

Schemas and sources for rich security metadata

A decentralized, flexibly anchored trust fabric

Software Supply Chain Integrity Consumption


Consume
Policy and Insight
Aggregation and Synthesis
Attestations and Metadata
SPDX
CycloneDX
Vulnerability Exploitability eXchange (VEX)
10
SLSA
in-toto
OSV
Open Source Vulnerabilities
Trust Foundation
sigstore
TUF
spiffe
SPIRE
Keylime

Automation and compliance throughout the SDLC

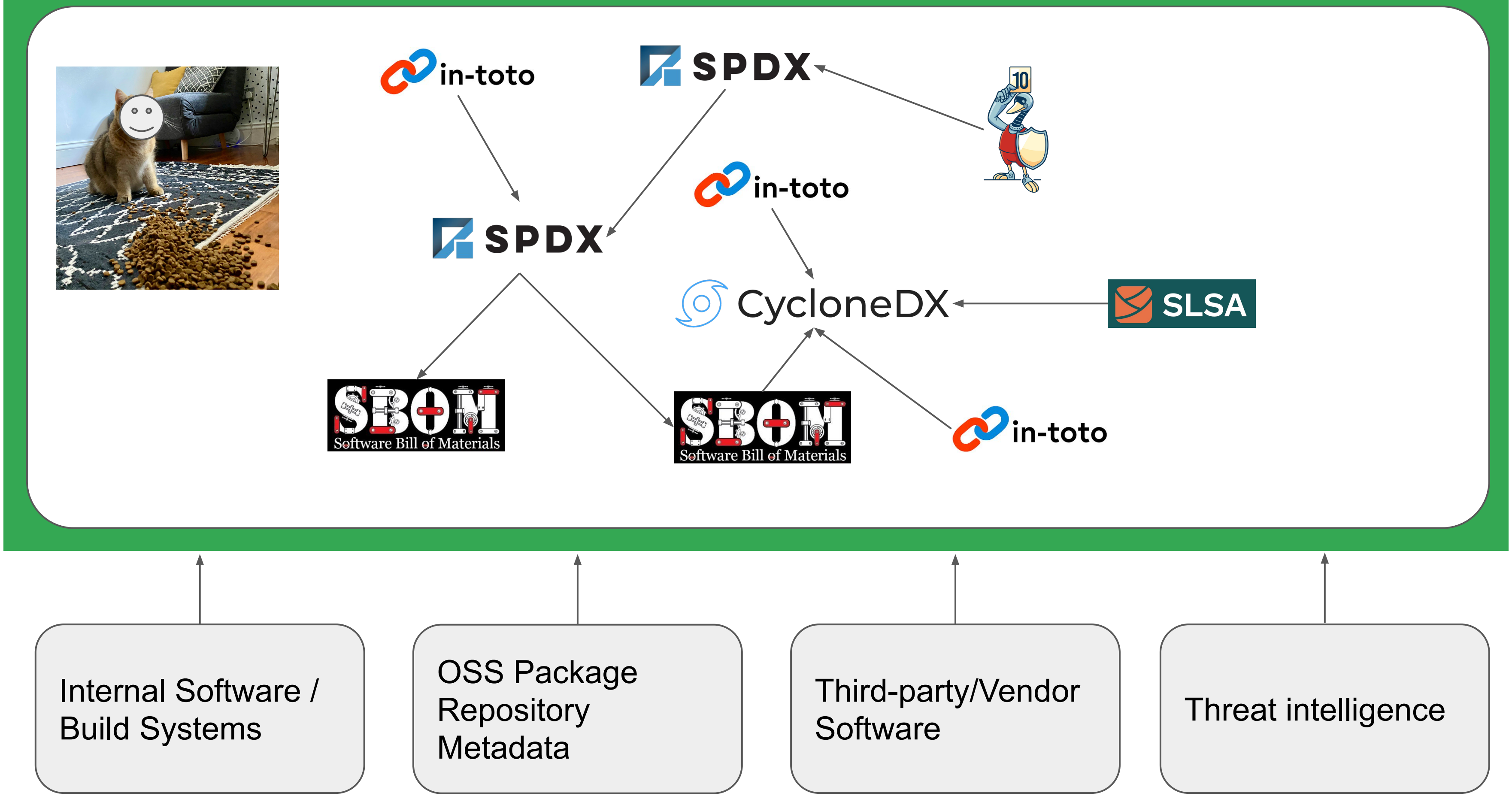
Intelligent aggregation across artifacts and identities

Schemas and sources for rich security metadata

A decentralized, flexibly anchored trust fabric

@lumjjb

Aggregation and Synthesis



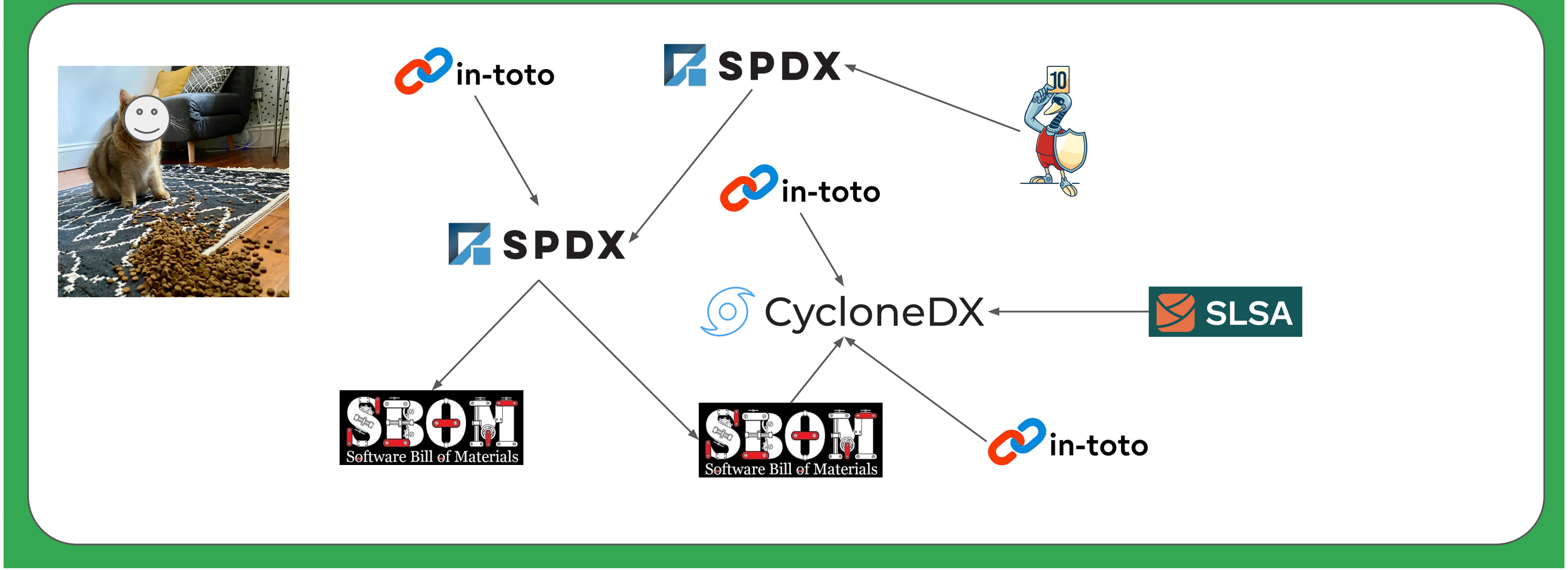
Internal Software / Build Systems

OSS Package Repository Metadata

Third-party/Vendor Software

Threat intelligence

Aggregation and Synthesis



Internal Software / Build Systems

OSS Package Repository Metadata

Third-party/Vendor Software

Threat intelligence

Consuming - Aggregation & Synthesis

Multi-source generic aggregator

GUAC

Public Data Source Aggregators

deps.dev

Repology

Package Managers

python™ Package Index

RubyGems

…

OPEN CONTAINER INITIATIVE

Consuming - Policy

Mechanism to create and enforce

Kyverno

Open Policy Agent

+ Proprietary GRC / CMDB systems

How to evaluate and enforce

What are checks for “Good” Supply Chain Security”?

TAG Security Issue #987

Consuming - Policy

Mechanism to create and enforce

Kyverno

Open Policy Agent

+ Proprietary GRC / CMDB systems

How to evaluate and enforce

What are checks for “Good” Supply Chain Security”?

TAG Security Issue #987

Consuming - Policy

Mechanism to create and enforce

Kyverno

Open Policy Agent

+ Proprietary GRC / CMDB systems

How to evaluate and enforce

What are checks for “Good” Supply Chain Security”?

TAG Security Issue #987

Consuming - Policy and Insights

Reactive

HOW AM I AFFECTED???

A vulnerability or supply chain compromise is discovered!

+ Codecov, Solarwinds compromises

Preventive

Have I taken the right safeguards?

When deciding to use and deploy software, are there sufficient security checks and approvals?

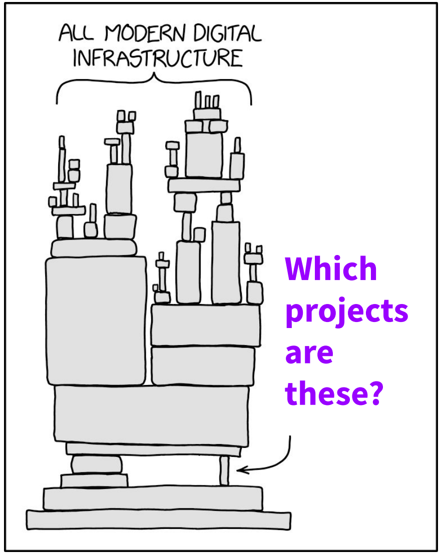
SLSA

aqua trivy

grype

Proactive

How do I prevent large scale supply chain compromises?



Which projects are these?

https://xkcd.com/2347/

Consuming - Policy and Insights

Reactive

HOW AM I AFFECTED???

A vulnerability or supply chain compromise is discovered!

+ Codecov, Solarwinds compromises

Preventive

Have I taken the right safeguards?

When deciding to use and deploy software, are there sufficient security checks and approvals?

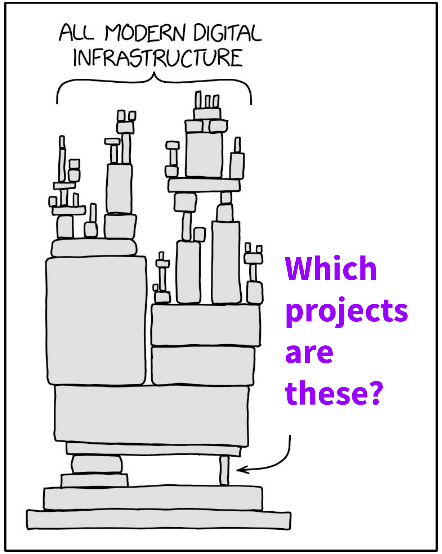
SLSA

aqua trivy

grype

Proactive

How do I prevent large scale supply chain compromises?



Which projects are these?

https://xkcd.com/2347/

Call to Action

SBOM
Software Bill of Materials
CycloneDX
SPDX
in-toto
SLSA
Yes, all the ingredients used are certified

- Let's start to dive deeper into **"Aggregation & Synthesis"** and **"Policy and Insights"**

- Join community efforts: TAG Security Issue #987

- Talks at CNSCon related to consumption
  - Not All That's Signed Is Secure: Verify the Right Way with TUF and Sigstore
  - Spicing up Container Image Security with SLSA & GUAC