



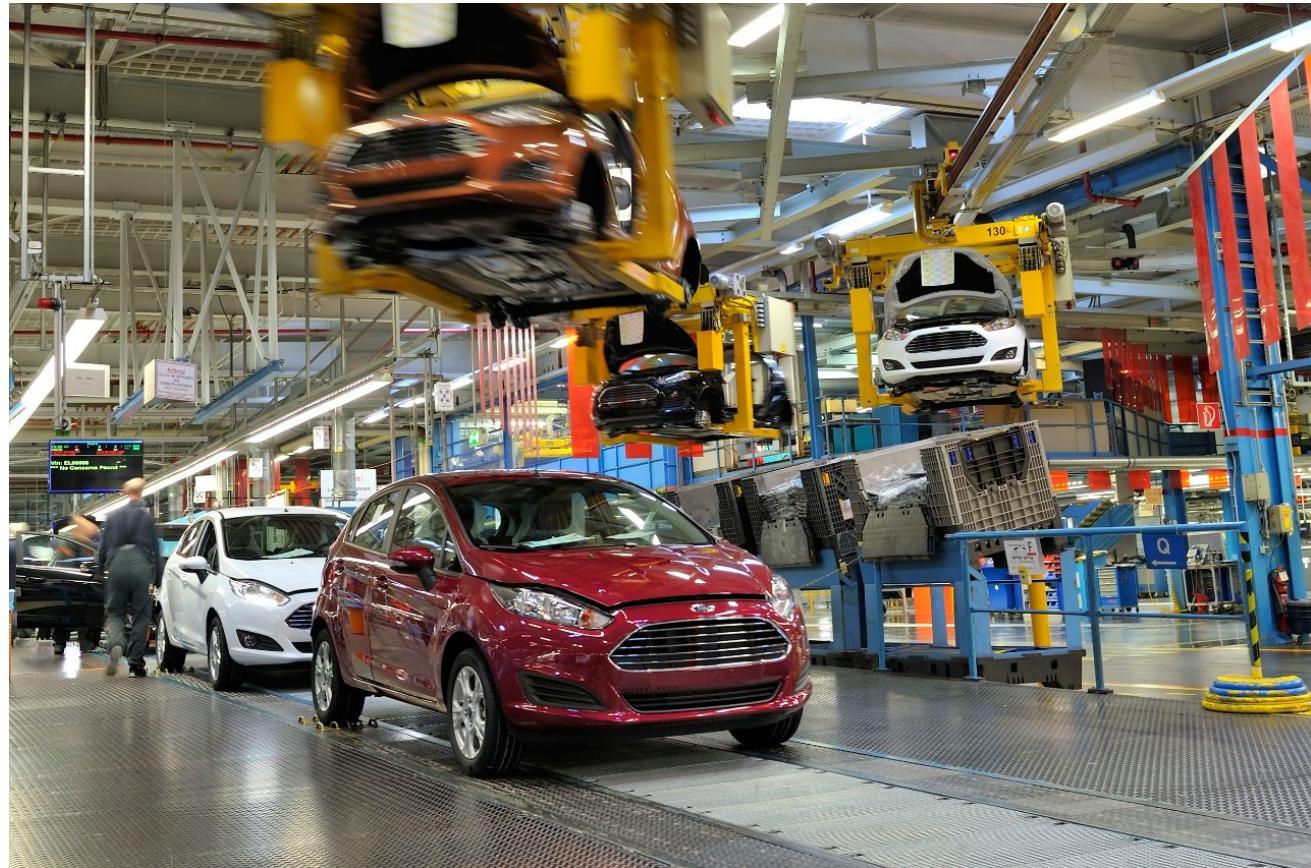
# Securing the Software Supply-Chain

Niels Tanis



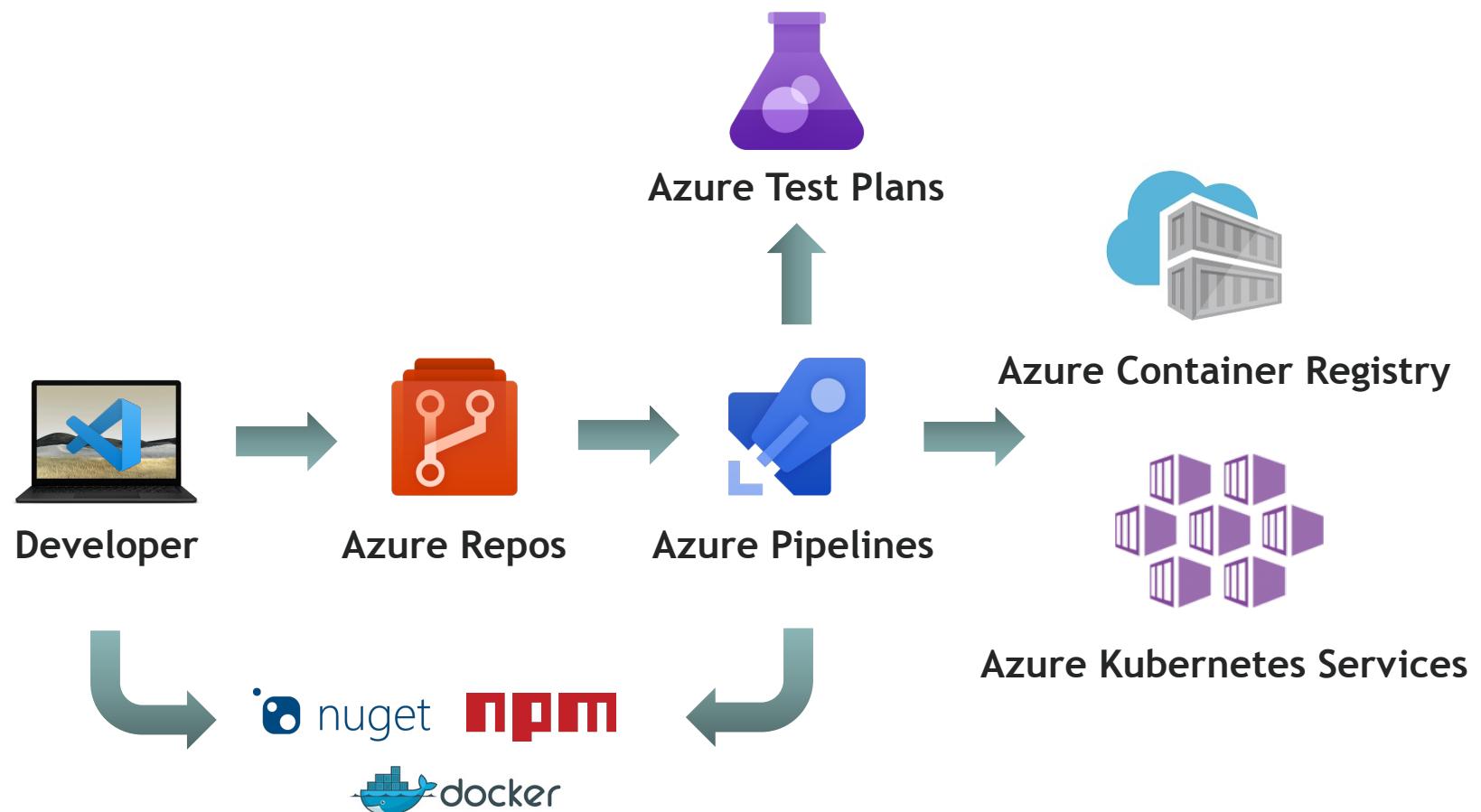
0101  
0101

# What is a Supply Chain?



# Software Supply Chain

0101  
0101



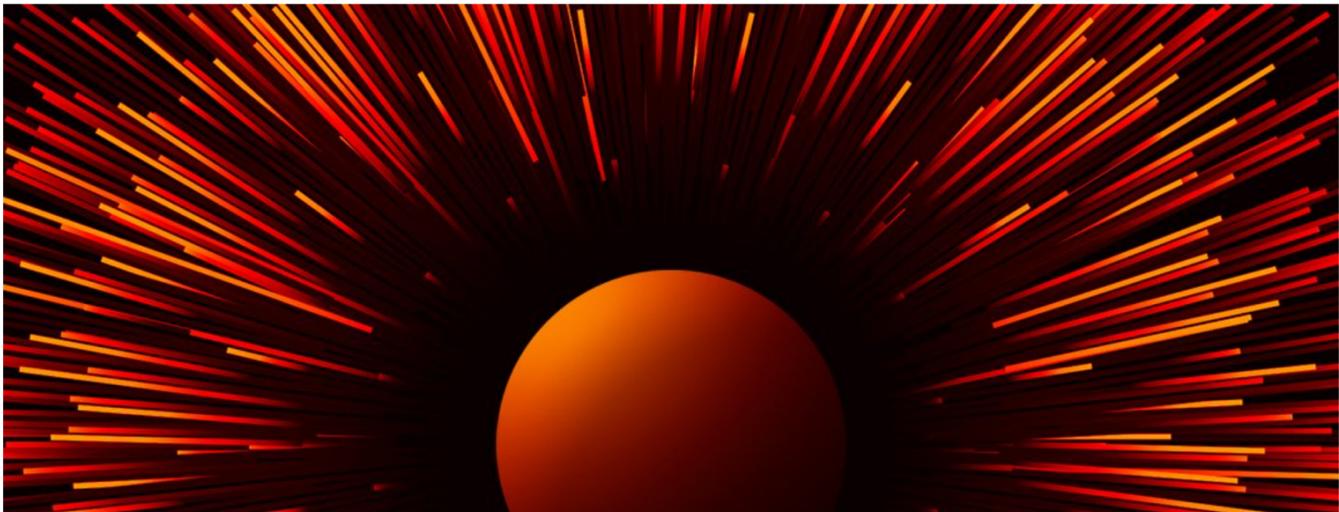
0101  
0101

# SolarWinds Sunspot

A screenshot of a web browser window showing a blog post from CrowdStrike. The title of the post is "SUNSPOT: An Implant in the Build Process". The post is dated January 11, 2021, and is attributed to the CrowdStrike Intelligence Team under the category "Research & Threat Intel". The background of the page features a large, stylized graphic of a sun with rays emanating from it.

SUNSPOT: An Implant in the Build Process

January 11, 2021 CrowdStrike Intelligence Team Research & Threat Intel



# ClickStudios PASSWORDSTATE

0101  
0101

A screenshot of a web browser displaying a news article from the CSIS Group website. The title of the article is "Moserpass supply chain". The main heading on the page reads "Supply chain attack on the password manager Clickstudios - PASSWORDSTATE". A timestamp "23/04/2021 20:18:42" is visible. The page content states: "The company ClickStudios recently notified their customers about a breach resulting in a supply chain attack conducted via an update of the password manager PASSWORDSTATE." The background of the page features abstract geometric shapes in blue and teal.

CSIS GROUP

EMERGENCY ASSISTANCE EN DA

PRODUCTS & SERVICES ▾ MANAGED SERVICES ▾ OM CSIS ▾ ENGAGEMENT HUB ▾

23/04/2021 20:18:42

**Supply chain attack on the password manager Clickstudios - PASSWORDSTATE**

The company ClickStudios recently notified their customers about a breach resulting in a supply chain attack conducted via an update of the password manager PASSWORDSTATE.

# CodeCov uploader

0101  
0101

A screenshot of a web browser displaying a security update page from CodeCov. The page has a dark header with the CodeCov logo and navigation links for Product, Solutions, Resources, Pricing, and Contact. On the right, there are Login and Sign Up buttons. The main content area features a purple and pink abstract background. At the top, it says "APRIL 15TH, 2021". Below that is a large, bold title "Bash Uploader Security Update". A yellow callout box contains a note: "⚠ Note: If you are in the affected user group, at 6 am PT, Thursday, April 15th, we emailed your email address on file from GitHub / GitLab / Bitbucket and added a notification banner in the Codecov application after you log in." At the bottom, there's a section titled "About the Event" with a paragraph about the company's commitment to security.

Bash Uploader Security Update

APRIL 15TH, 2021

## Bash Uploader Security Update

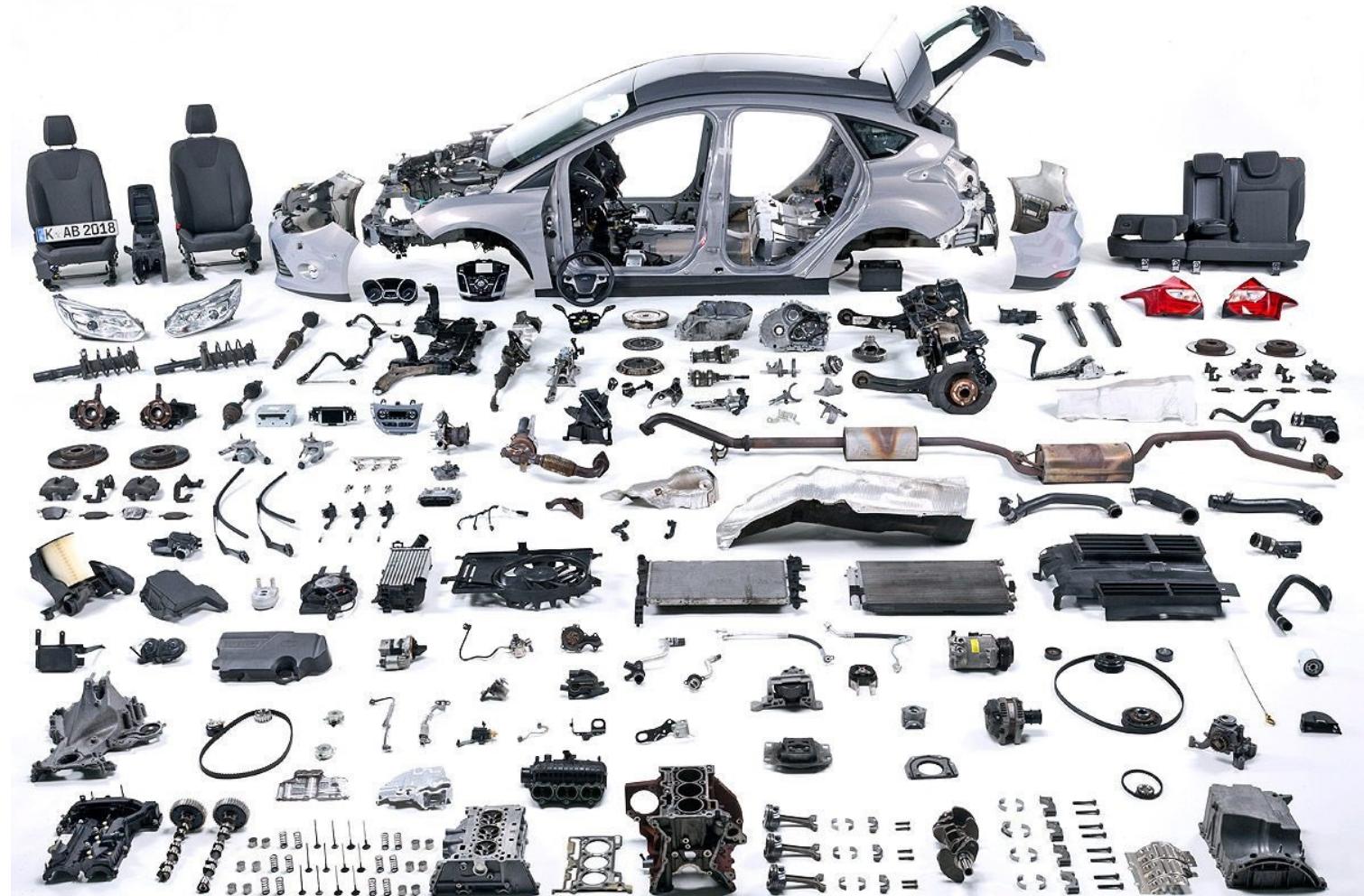
**⚠ Note:** If you are in the affected user group, at 6 am PT, Thursday, April 15th, we emailed your email address on file from GitHub / GitLab / Bitbucket and added a notification banner in the Codecov application after you log in.

### About the Event

Codecov takes the security of its systems and data very seriously and we have implemented numerous safeguards to protect you. On Thursday, April 1, 2021, we learned that someone had gained unauthorized access to our [Bash Uploader](#) script

0101  
0101

# Automotive Industry



# Car Supply Chain



## Tata Steel Factory

- Iron Ore from Sweden
- ISO 6892-1 Tested/Certified
  - Batch #1234

## Bosch Factory

- Steel Batch #1234 Tata
- ECE-R90 Tested/Certified
  - Serie #45678
- Used by Ford, Volkswagen and Renault

## Renault Manufacturing

- Bosch Disk #45678
- Bosal Exhaust #RE9876
- Goodyear Tires #GY8877
- Kadjar VIN 1234567890

0101  
0101

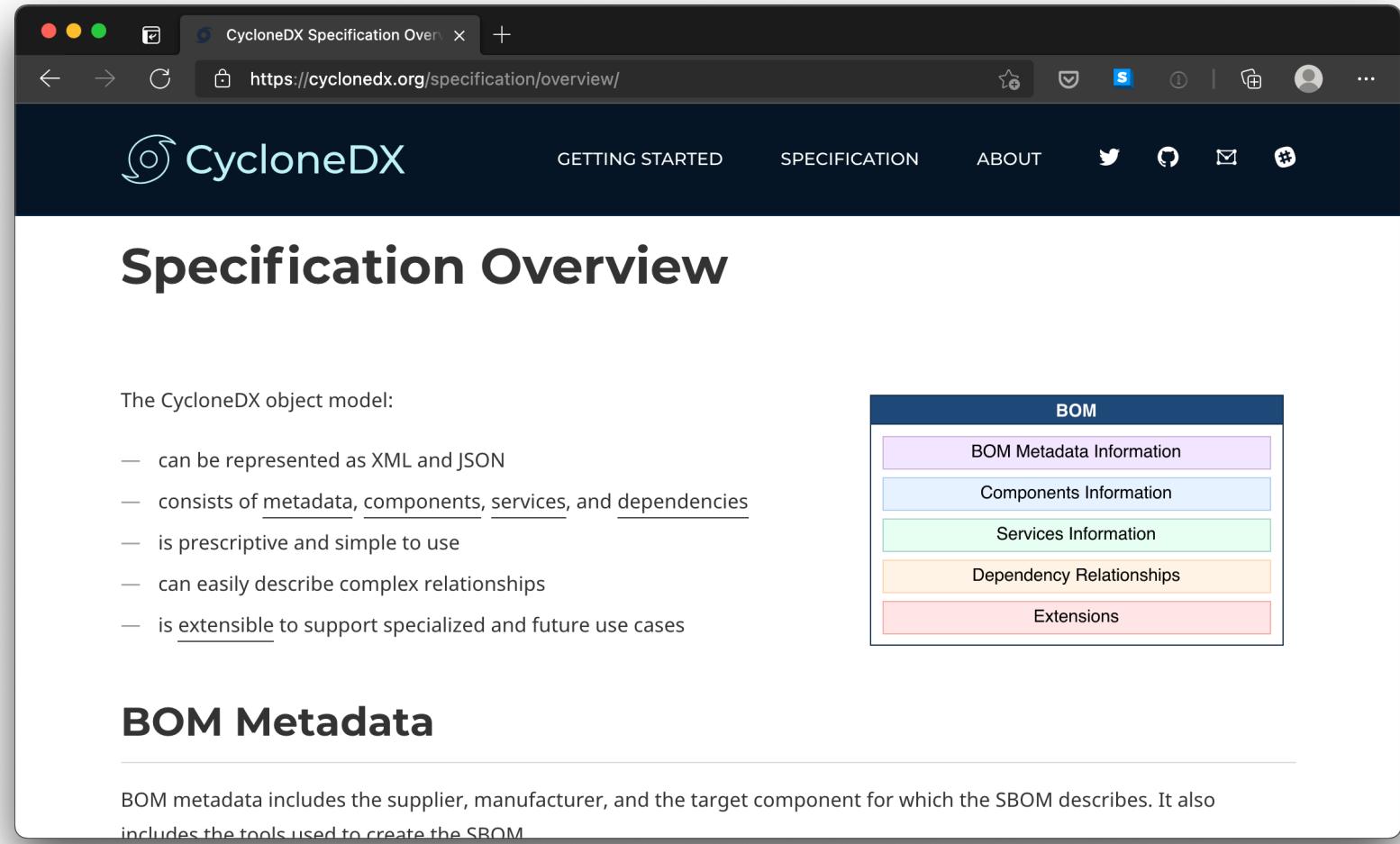


# Software Bill of Materials (SBOM)

- Industry standard of describing the software
  - Producer Identity - Who Created it?
  - Product Identity - What's the product?
  - Integrity - Is the project unaltered?
  - Licensing - How can the project be used?
  - Creation - How was the product created? Process meets requirements?
  - Materials - How was the product created? Materials/Source used?
- NTIA.gov - SBOM

# CycloneDX

0101  
0101



The screenshot shows a web browser window displaying the 'CycloneDX Specification Overview' page at <https://cyclonedx.org/specification/overview/>. The page has a dark blue header with the CycloneDX logo, navigation links for 'GETTING STARTED', 'SPECIFICATION', and 'ABOUT', and social media icons. The main content area features a large heading 'Specification Overview' and a section titled 'The CycloneDX object model:' followed by a bulleted list of its characteristics. To the right of this text is a diagram titled 'BOM' showing a vertical stack of five colored boxes: purple ('BOM Metadata Information'), light blue ('Components Information'), green ('Services Information'), orange ('Dependency Relationships'), and red ('Extensions').

The CycloneDX object model:

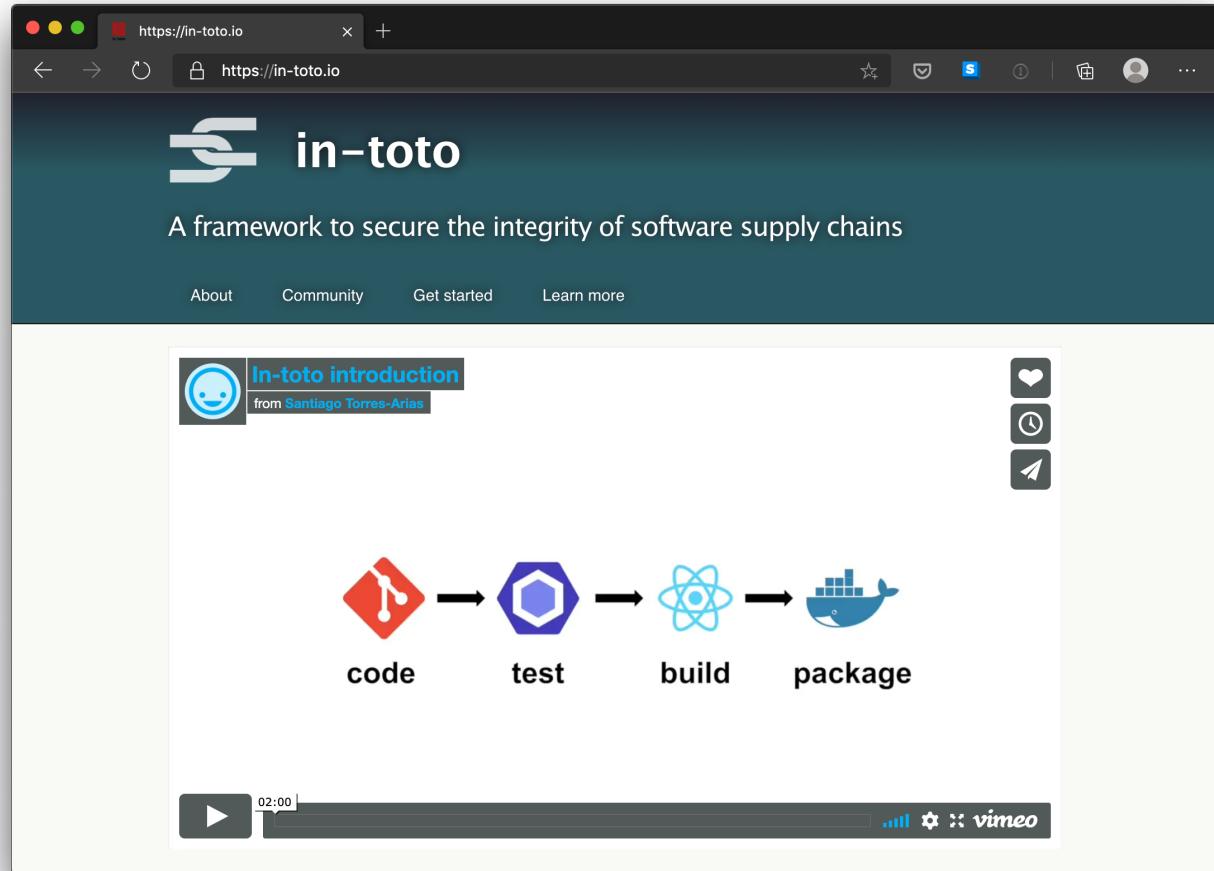
- can be represented as XML and JSON
- consists of metadata, components, services, and dependencies
- is prescriptive and simple to use
- can easily describe complex relationships
- is extensible to support specialized and future use cases

## BOM Metadata

BOM metadata includes the supplier, manufacturer, and the target component for which the SBOM describes. It also includes the tools used to create the SBOM.

0101  
0101

# In-toto





# In-Toto - Demo - Terminology

- **Functionaries** that are identified by public key our supply chain.  
Niels (Project-Owner), Aimee (Developer) and Noud (Packager)
- **Project-Owner** defines a (**Supply Chain**) **Layout** that describes **what** happens and by **who** and what the produced **Materials** and **Byproducts** are.
- Link metadata is output of executed step in the **Layout**  
**Materials** are input, **Products** are output and can be used as **Materials** in later steps



# Conclusion

- Be aware of your own (and other used) software supply chain(s).
- Know what you're consuming and pulling into software projects.
- Use MFA on all accounts!
- Integrate security into your software lifecycle.
- Learn more on Software Bill of Materials (SBOM).

VERACODE

# Thanks! Questions?

<https://github.com/nielstanis/dotnetflix>

ntanis at veracode.com

@nielstanis on Twitter

