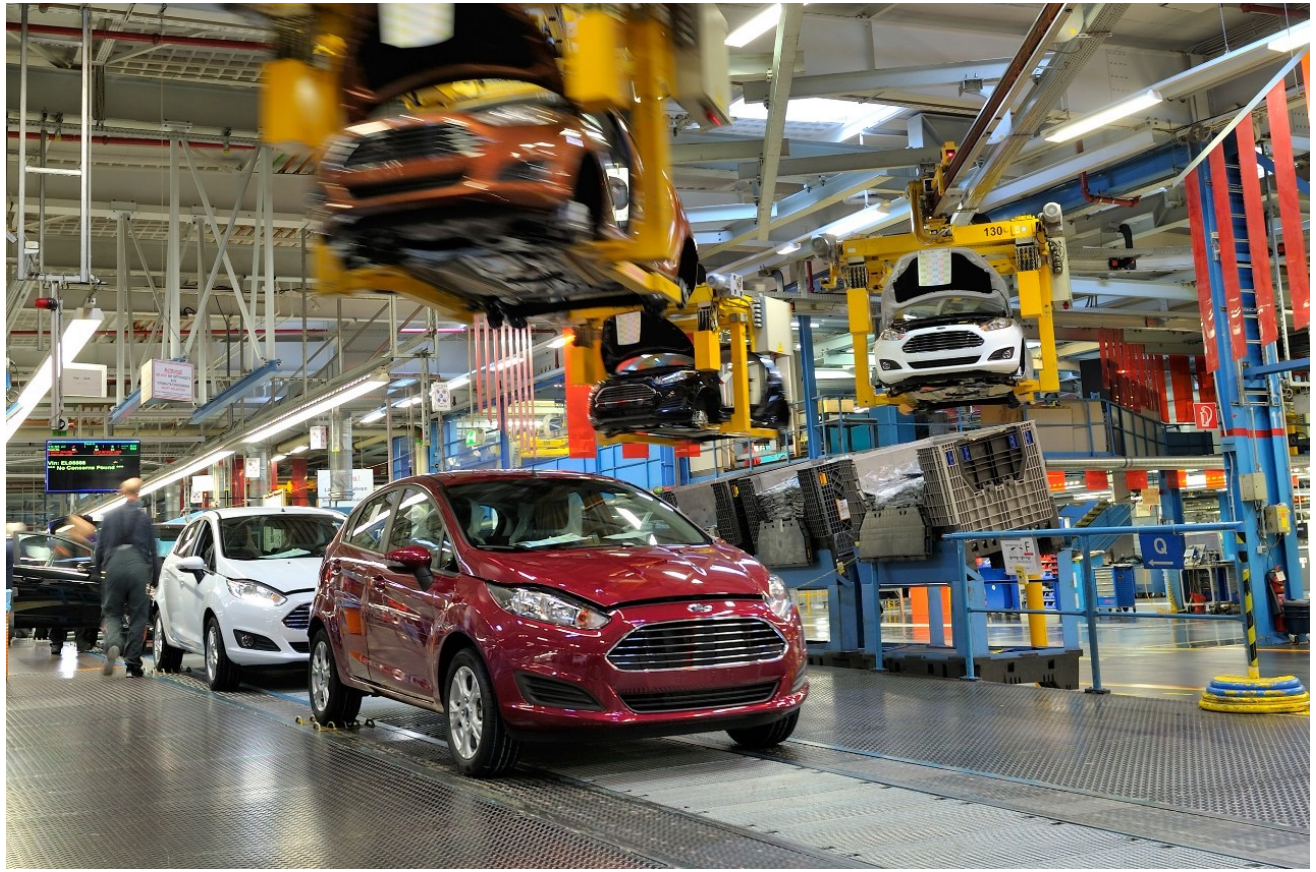
Securing the Software Supply-Chain

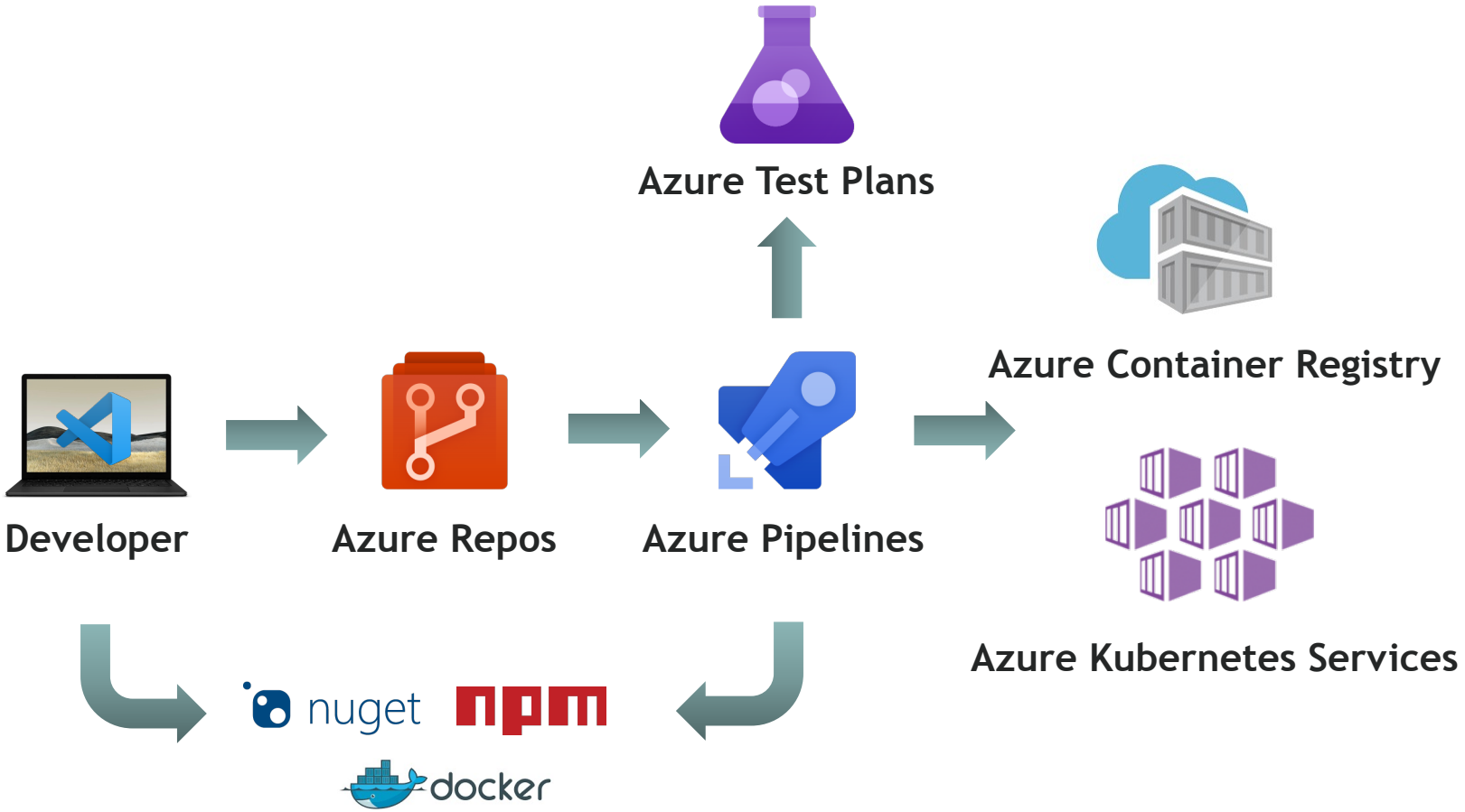
Niels Tanis

VERACODE

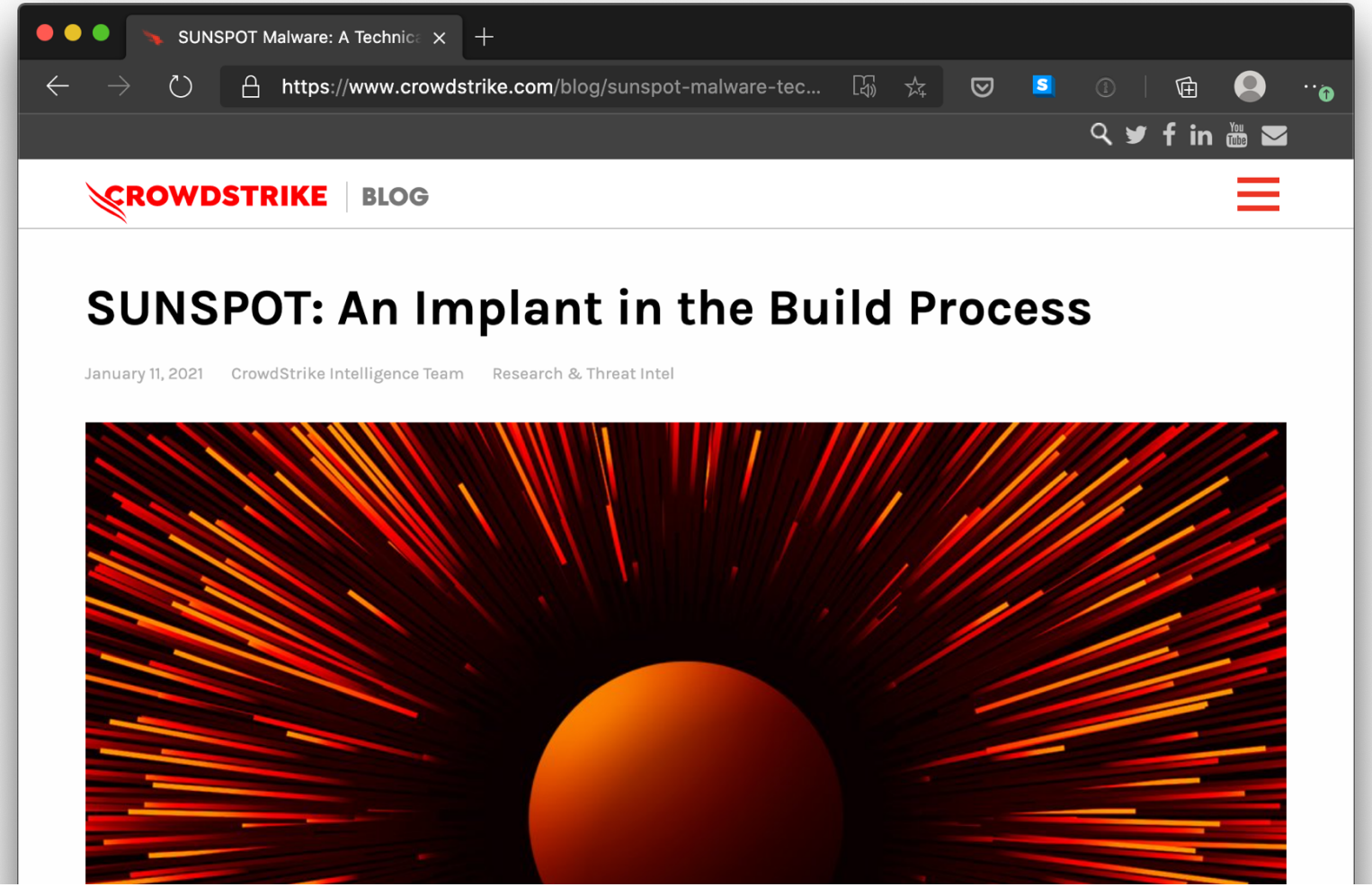
What is a Supply Chain?



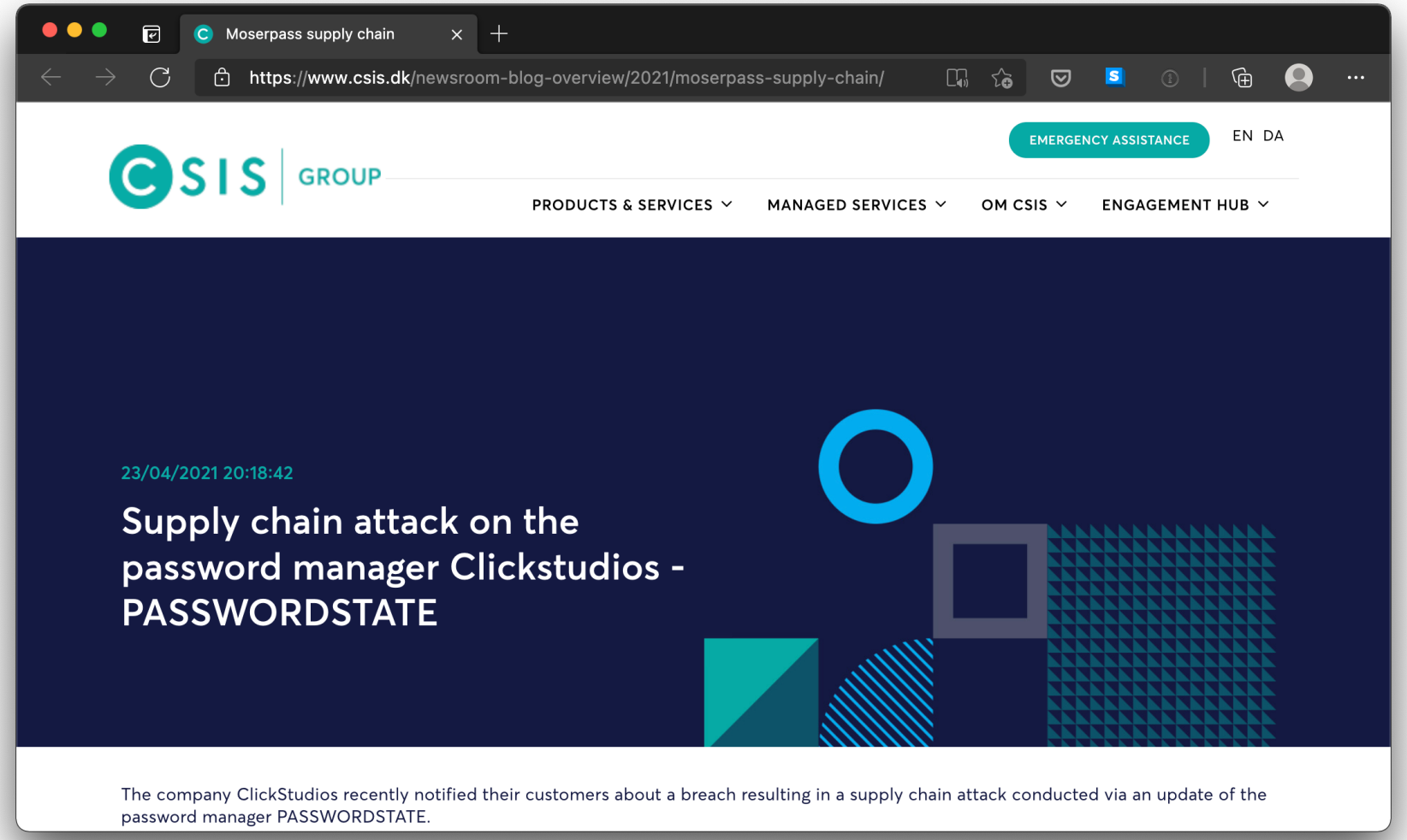
Software Supply Chain



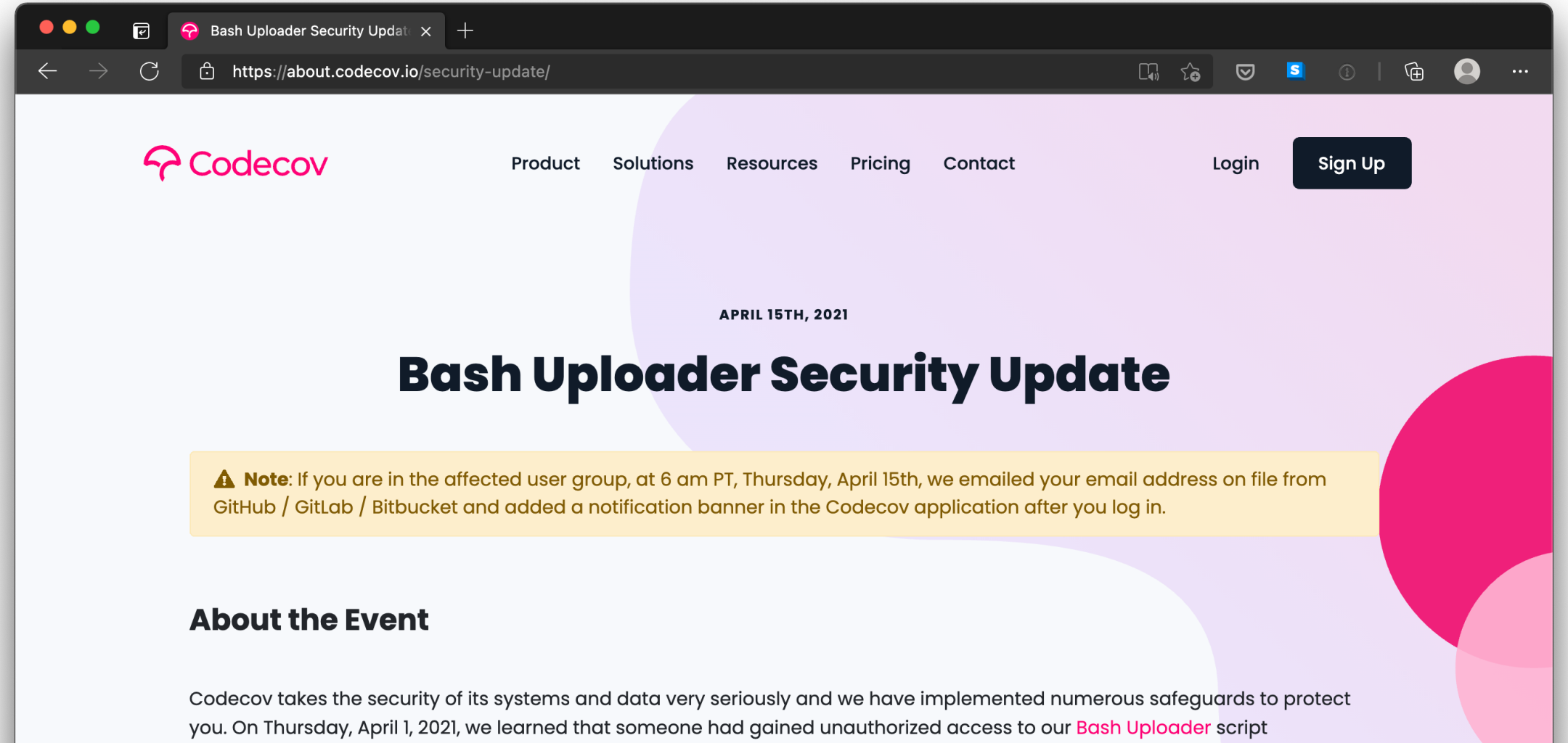
SolarWinds Sunspot



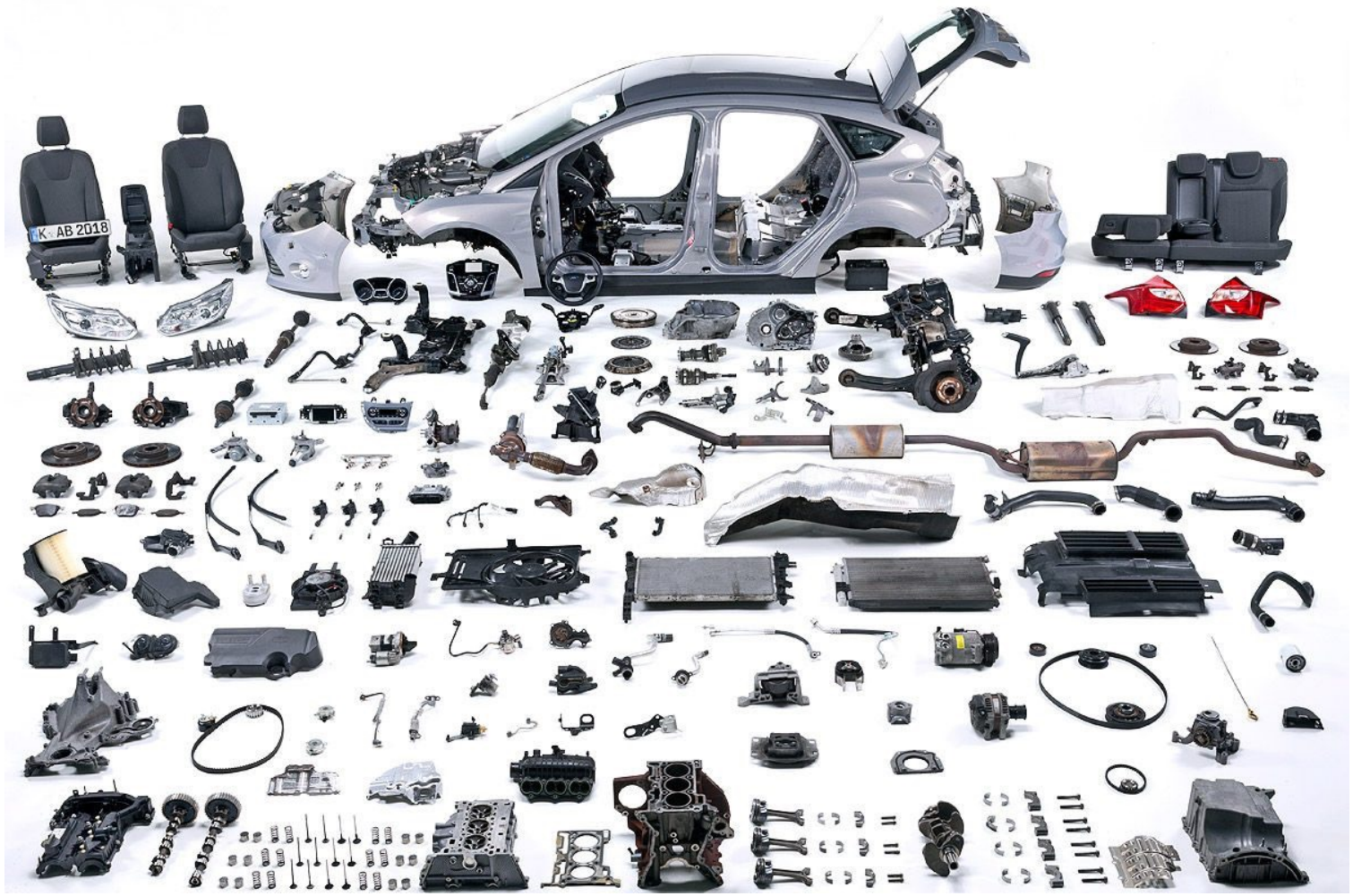
ClickStudios PASSWORDSTATE



CodeCov uploader



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

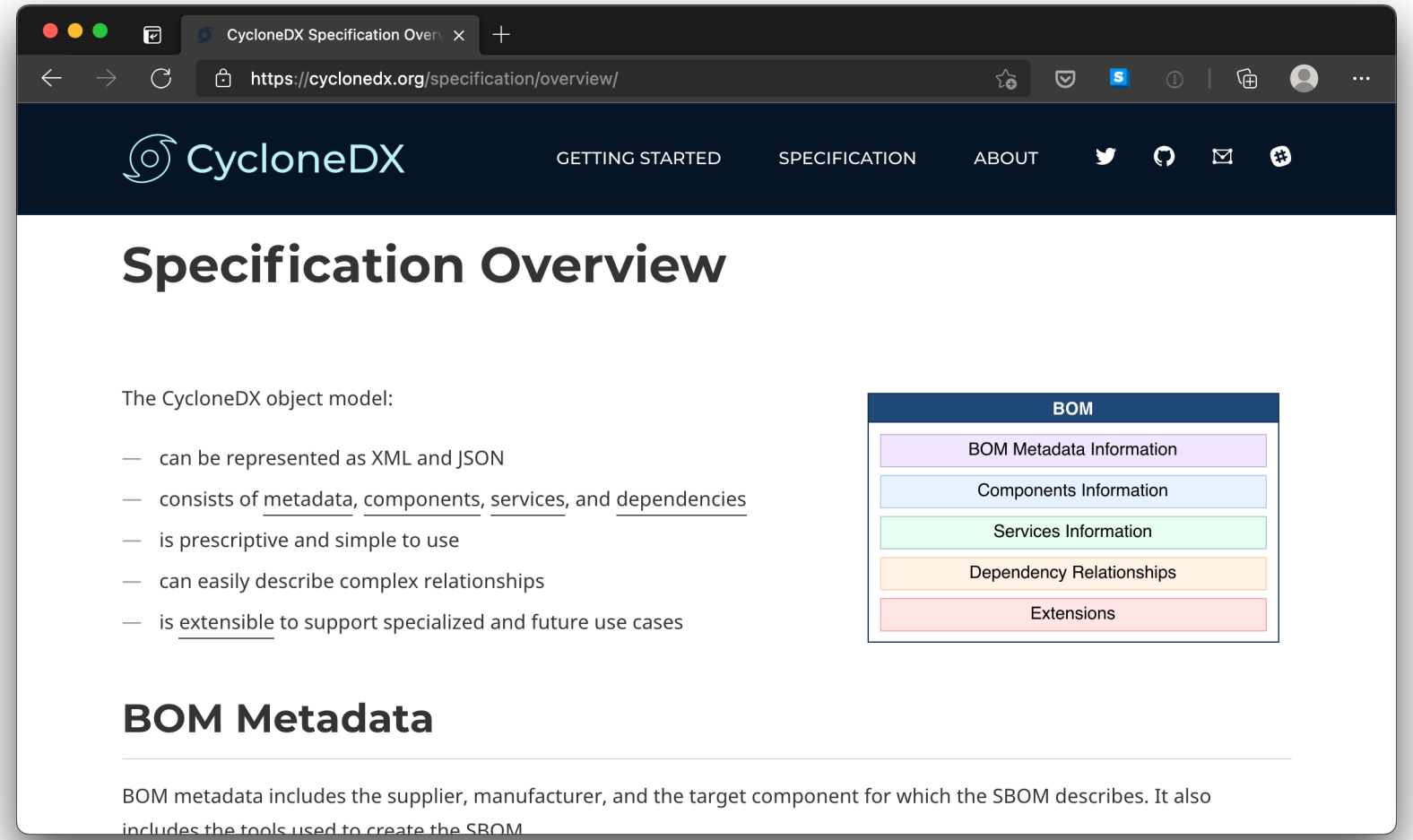
Renault Manufacturing

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

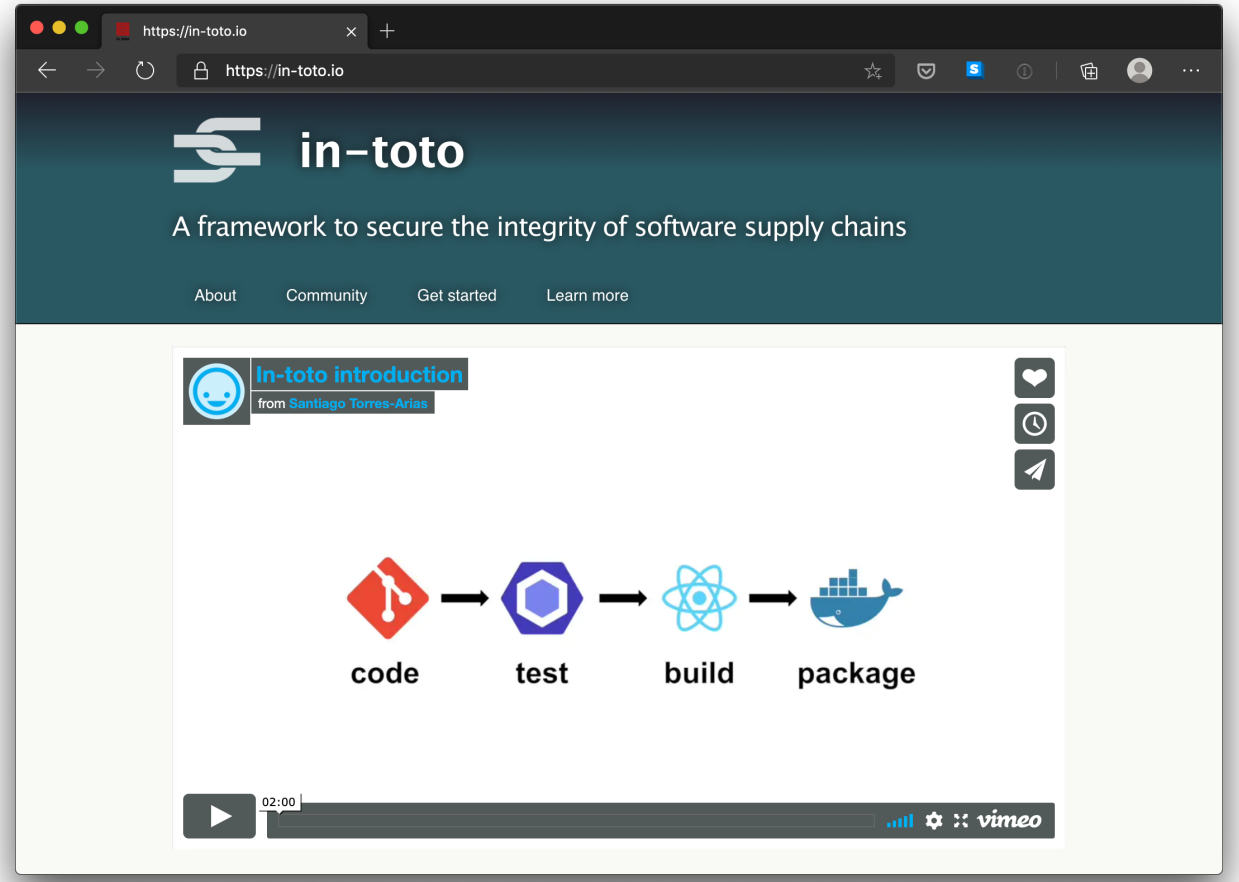
Software Bill of Materials (SBOM)

- 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


CycloneDX Specification Over
https://cyclonedx.org/specification/overview/
CycloneDX
GETTING STARTED
SPECIFICATION
ABOUT
Specification Overview
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
BOM Metadata Information
Components Information
Services Information
Dependency Relationships
Extensions
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

In-toto


https://in-toto.io
https://in-toto.io
in-toto
A framework to secure the integrity of software supply chains
About
Community
Get started
Learn more
In-toto introduction
from Santiago Torres-Arias
code
test
build
package
02:00
vimeo

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