

NDC { London }

Securing your .NET application software supply-chain the practical approach! (workshop)

Niels Tanis

VERACODE

0101
0101

Who am I?

- Niels Tanis
- Sr. Principal Security Researcher @ Veracode
 - Background .NET Development,
Pentesting/ethical hacking,
and software security consultancy
 - Research on static analysis for .NET apps



0101
0101

Agenda

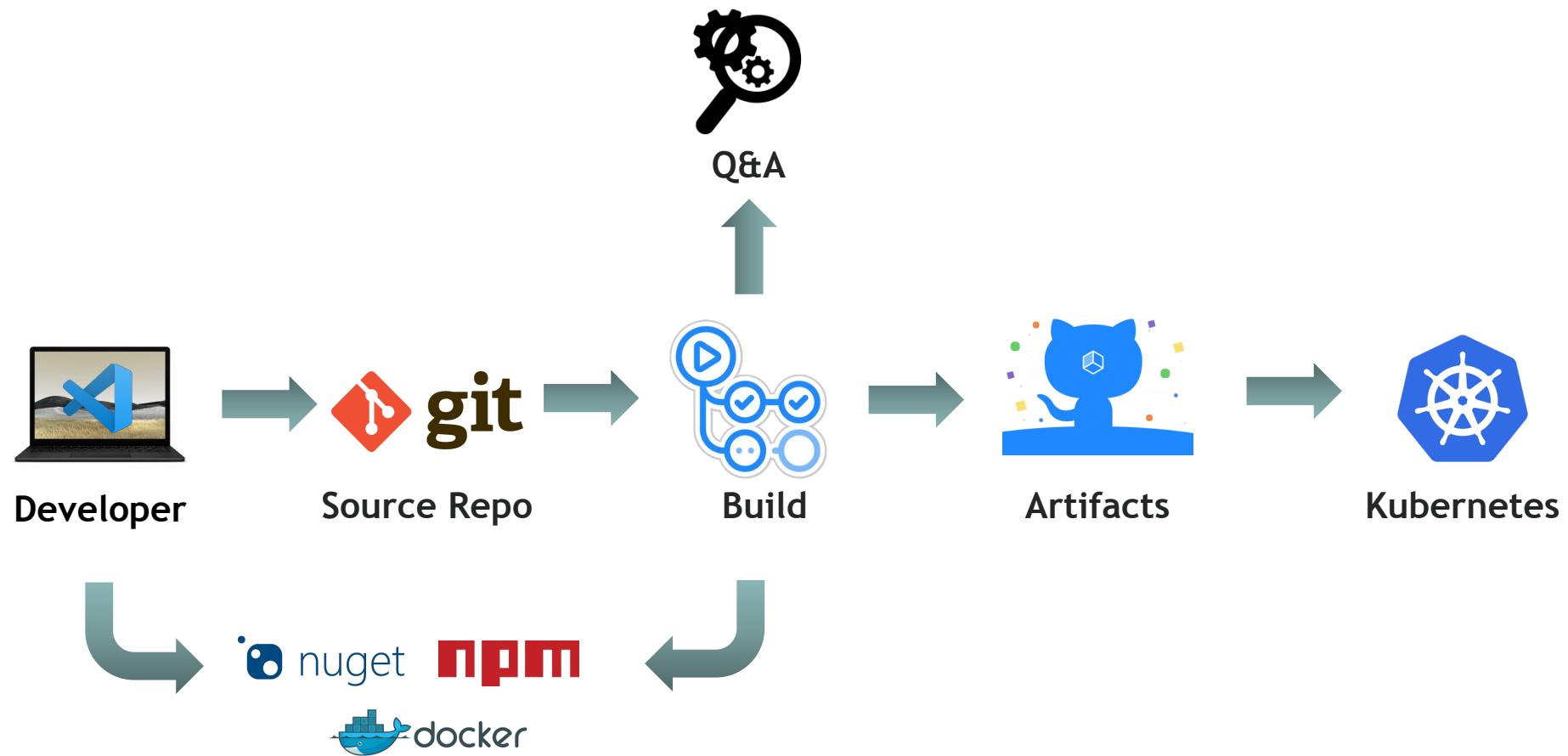
0101
0101

What is a Supply Chain?



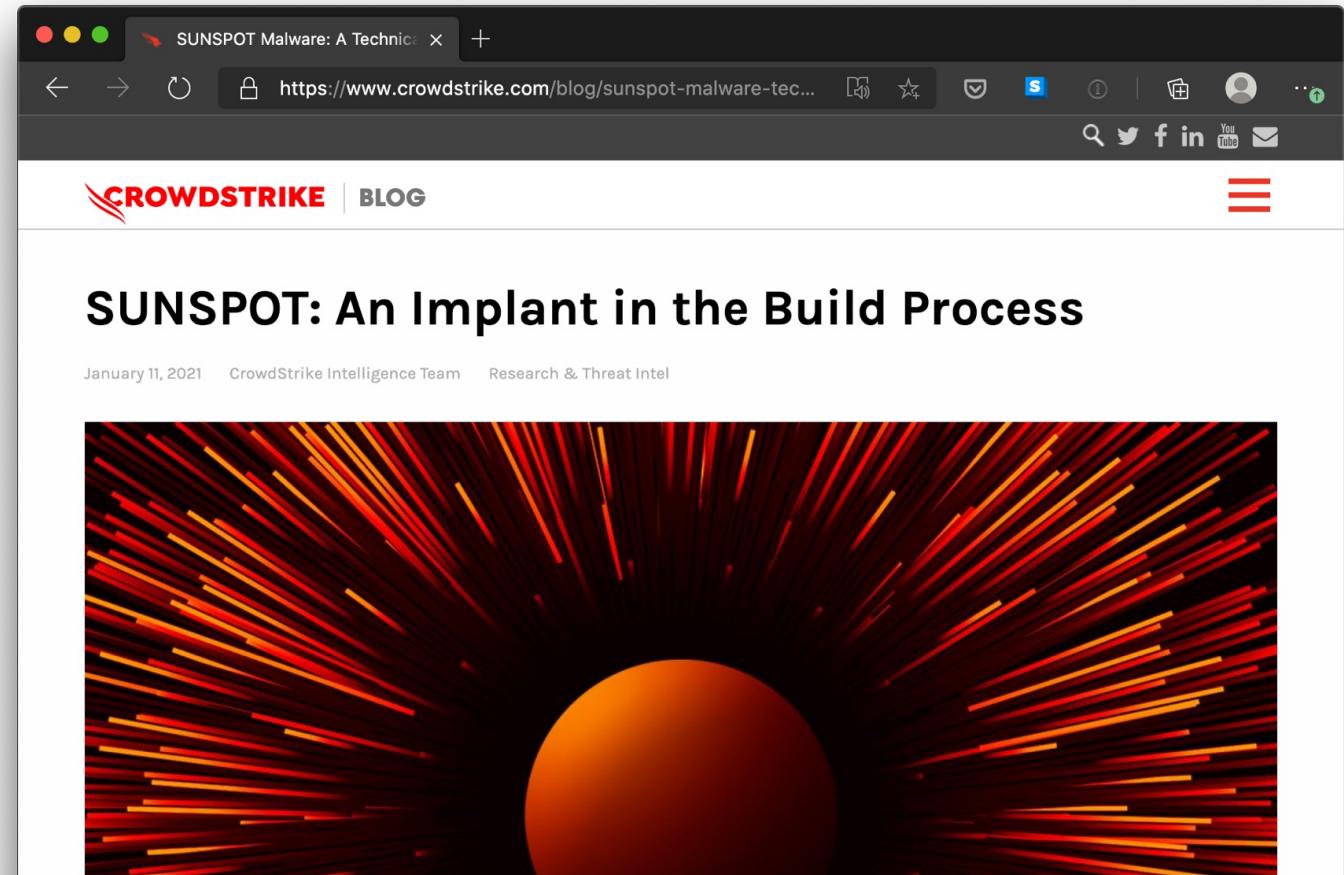
Software Supply Chain

0101
0101



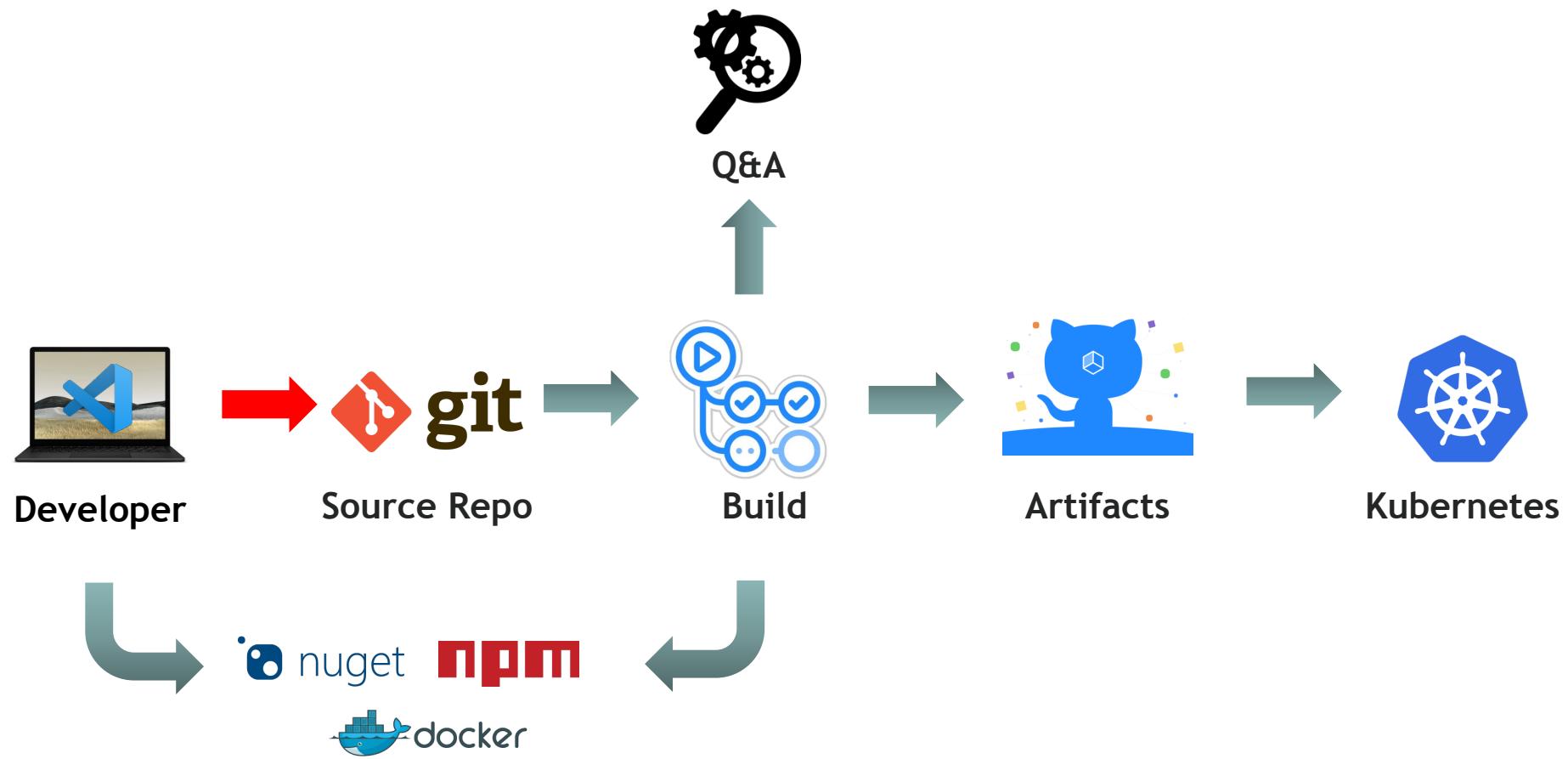
0101
0101

SolarWinds SunSpot



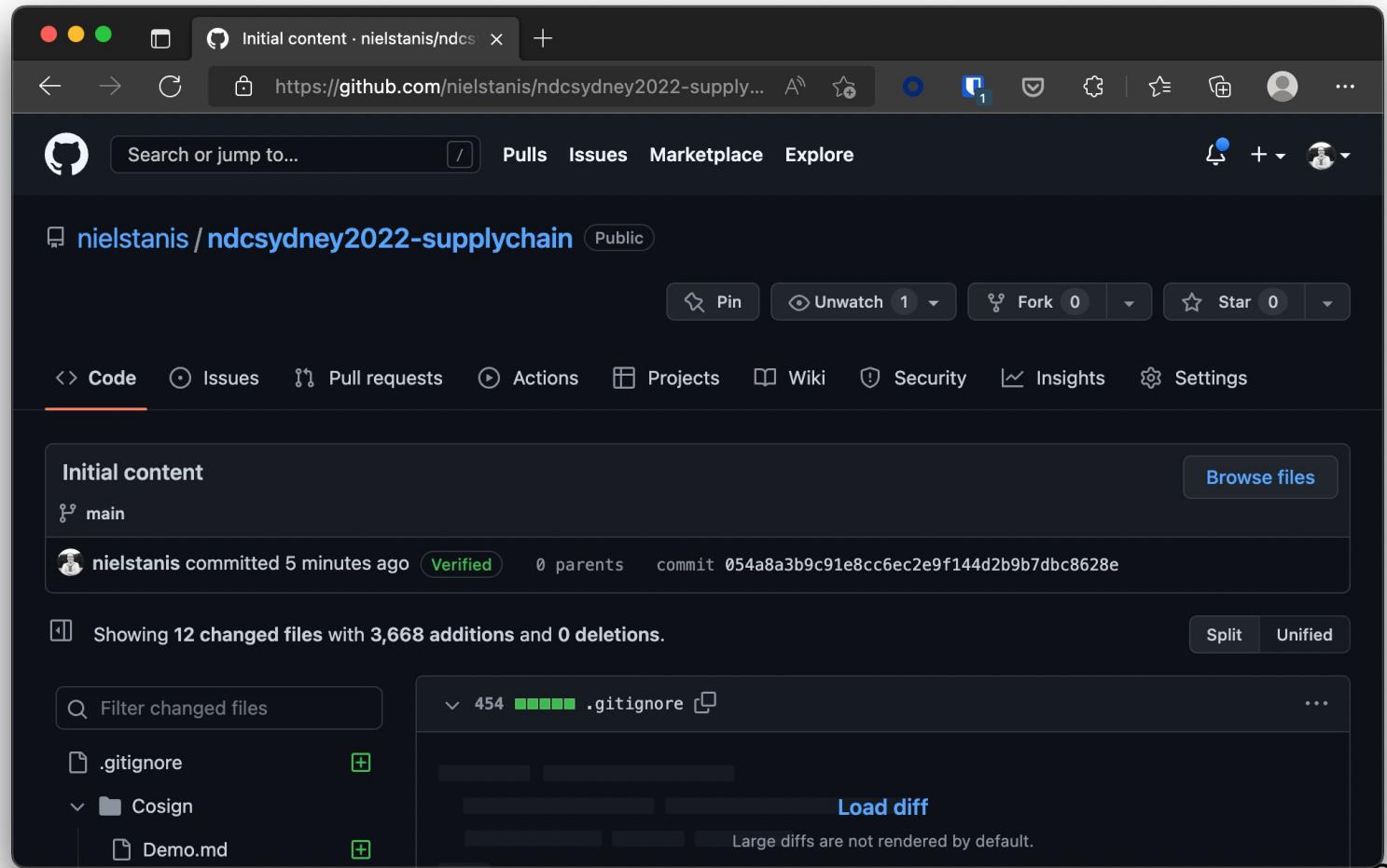
Software Supply Chain

0101
0101



0101
0101

GIT Commit Signing



Lab 1

DocGenerator





Reproducible/Deterministic Builds

The screenshot shows a website with a dark blue header bar. On the left, there's a logo consisting of four white dots arranged in a diamond shape, followed by the text "Reproducible Builds". Below the header is a vertical navigation menu with the following items: Home, Contribute, Documentation (which is highlighted in blue), Tools, Who is involved?, News, Events, and Talks. To the right of the menu, the main content area has a large heading "Definitions" and a sub-section titled "When is a build reproducible?". The text in this section explains what makes a build reproducible and defines artifacts.

Definitions

When is a build reproducible?

A build is **reproducible** if given the same source code, build environment and build instructions, any party can recreate bit-by-bit identical copies of all specified artifacts.

The relevant attributes of the build environment, the build instructions and the source code as well as the expected reproducible artifacts are defined by the authors or distributors. The artifacts of a build are the parts of the build results that are the desired primary output.



Reproducible/Deterministic Builds

- Roslyn v1.1 started supporting some kind of determinism on how items are emitted
- Given same inputs, the compiled output will always be deterministic
- Inputs can be found in Roslyn compiler docs
‘Deterministic Inputs’

Lab 2

.NET 7 reproducible



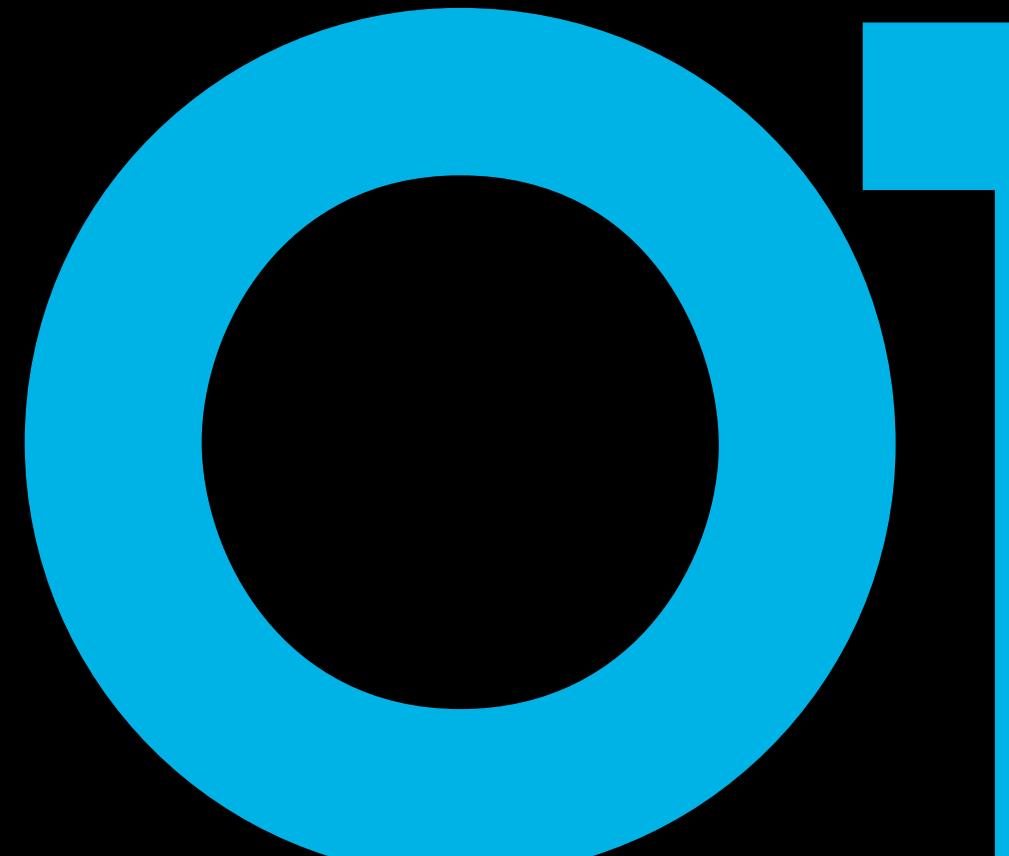


Reproducible/Deterministic Builds

- DotNet.Reproducible NuGet Package
 - MSBuild *ContinuousIntegrationBuild*
 - SourceLink
- Dotnet.Reproducible.Isolated NuGet Package
 - Hermetic builds

Lab 3

DotNet.Reproducible
NuGet Package

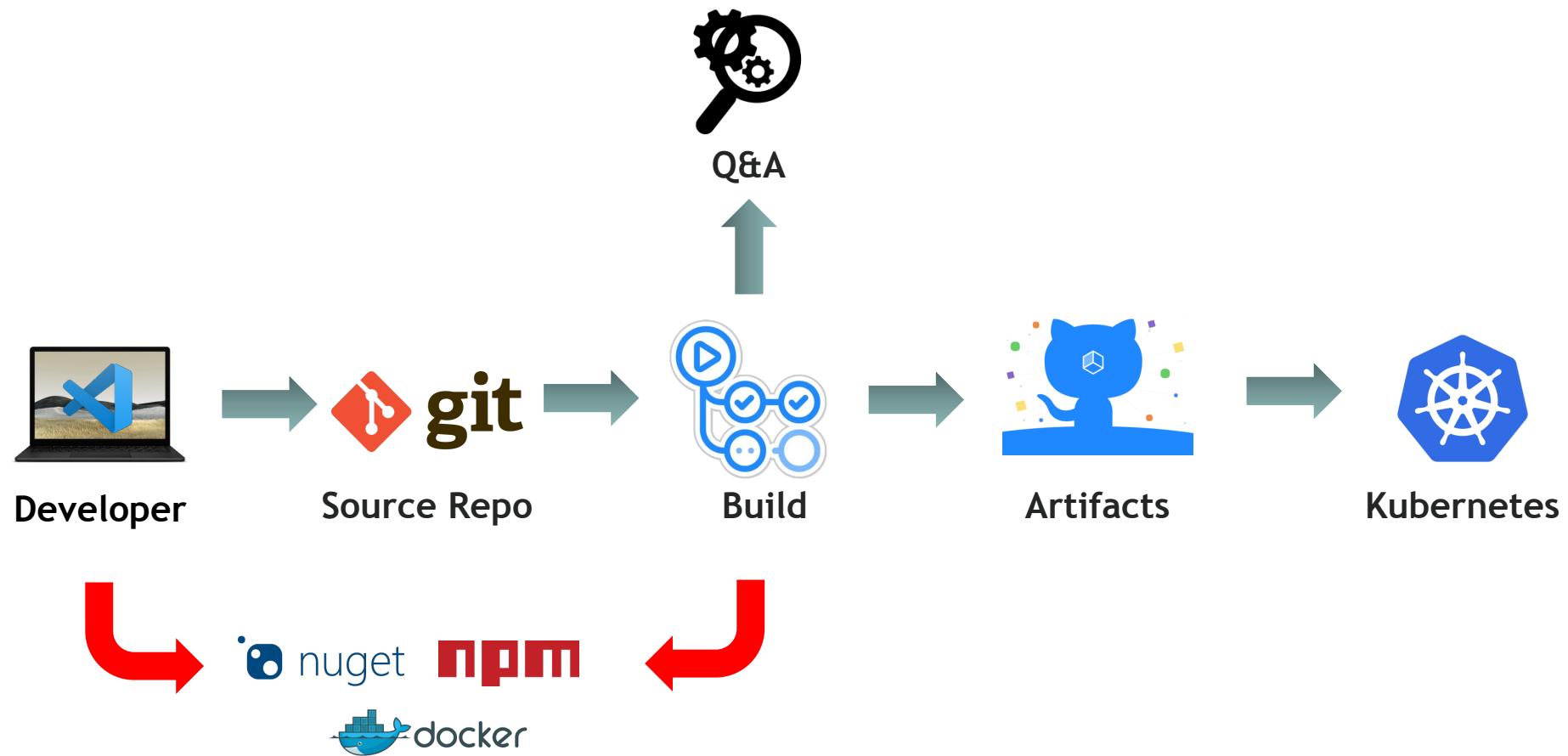




Reproducible Build Validation

- Design to validate NuGet packages & .NET binaries
 - Does linked source code match binaries?
 - Capable to compare at IL level
 - Ability to rebuild reproducible based on given inputs
 - .NET CLI Validate tool `dotnet validate`

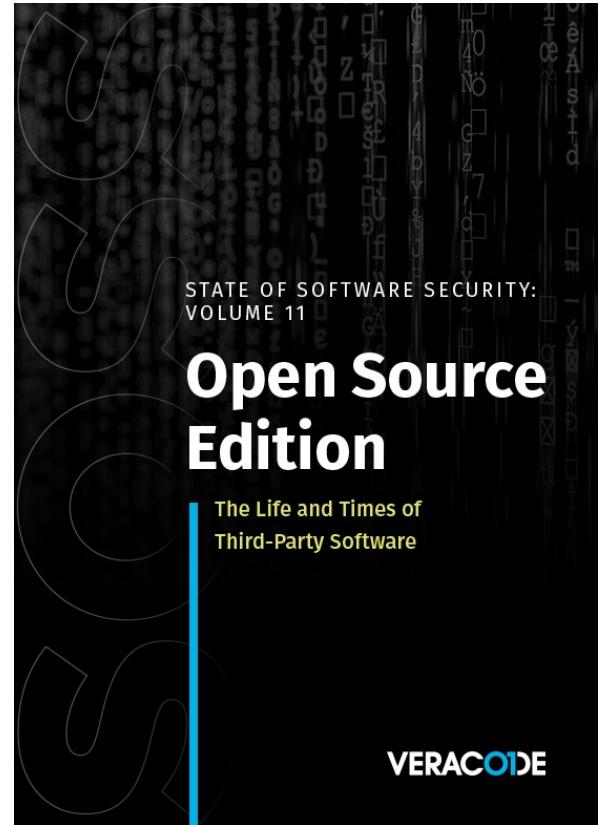
3rd Party Libraries



State Of Software Security v11 2021



*“Despite this dynamic landscape,
79 percent of the time, developers
never update third-party libraries after
including them in a codebase.”*



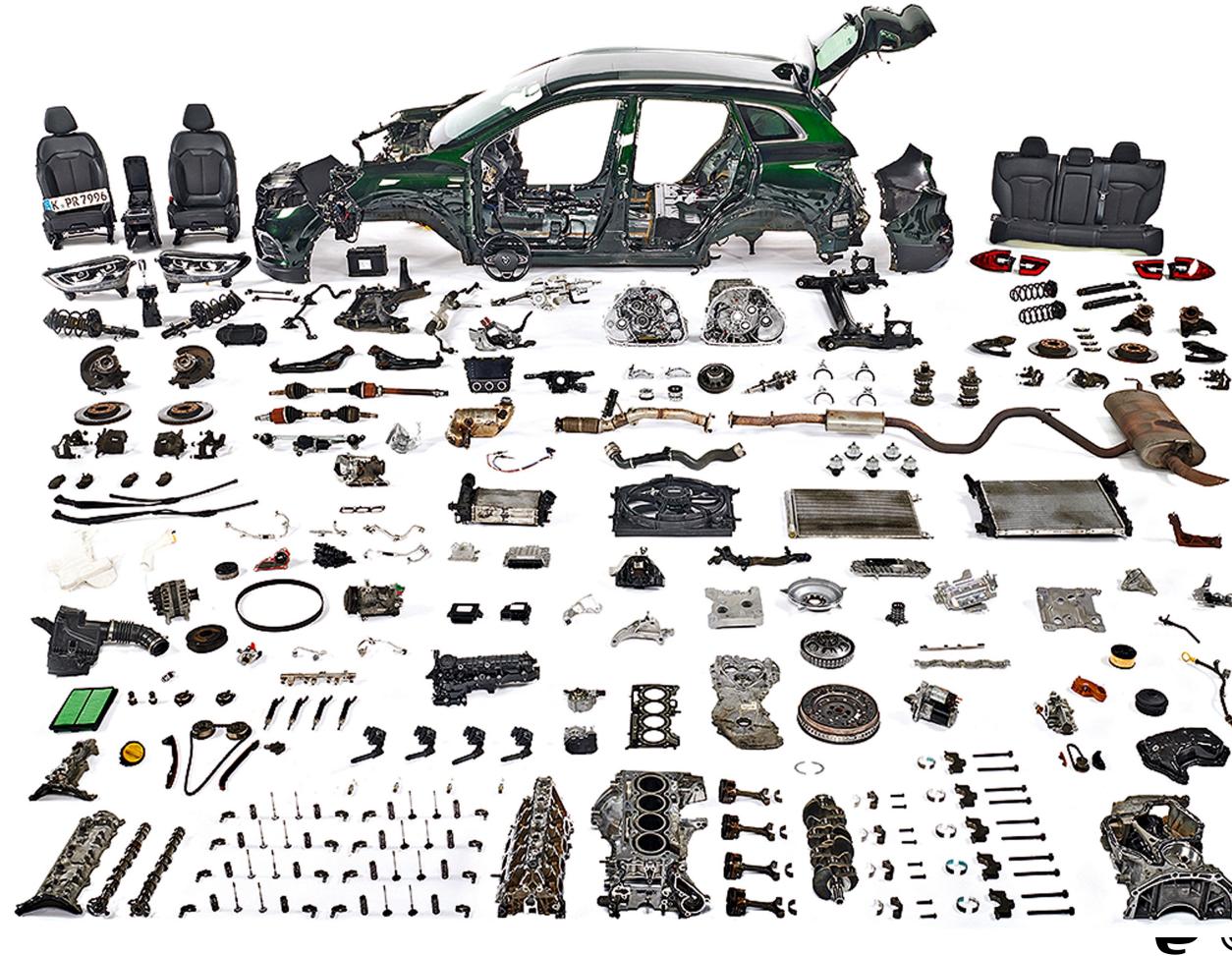
0101
0101

Vulnerabilities in libraries

The screenshot shows a GitHub issue page for the repository `dotnet/announcements`. The issue is titled "Microsoft Security Advisory CVE-2022-24512 | .NET Remote Code Execution Vulnerability #213". The issue was opened by `dcwhittaker` on March 8th, 2022, and has 0 comments. The issue body contains an executive summary and a discussion section. The executive summary states that Microsoft is releasing a security advisory for a vulnerability in .NET 6.0, .NET 5.0, and .NET Core 3.1. It describes a remote code execution vulnerability in the .NET Double Parse routine where a stack buffer overrun occurs. The discussion section points to another issue at `dotnet/runtime#66348`. On the right side of the issue page, there are sections for assignees (none assigned), labels (Monthly-Update, .NET Core 3.1, .NET 5.0, .NET 6.0, Patch-Tuesday, Security), projects (none yet), and milestones (no milestone).

0101
0101

Automotive Industry



0101
0101

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?



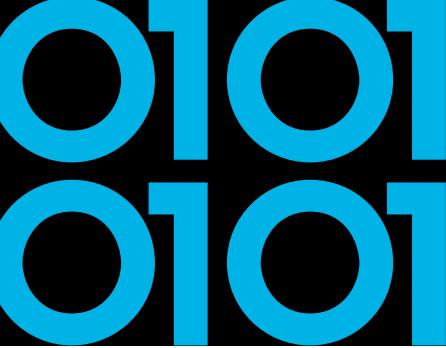
Software Bill of Materials (SBOM)

The screenshot shows a web browser window displaying the OWASP CycloneDX website at <https://cyclonedx.org>. The page has a dark blue background with a network graph pattern. At the top left is the CycloneDX logo. On the right side is a three-line menu icon. In the center, there is a paragraph of text: "OWASP CycloneDX is a lightweight software bill of materials (SBOM) standard designed for use in application security contexts and supply chain component analysis." At the bottom of the main content area, there is a footer bar with the text "16 August 2021 - OWASP CycloneDX SBOM Standard Launches Educational Learning Series".

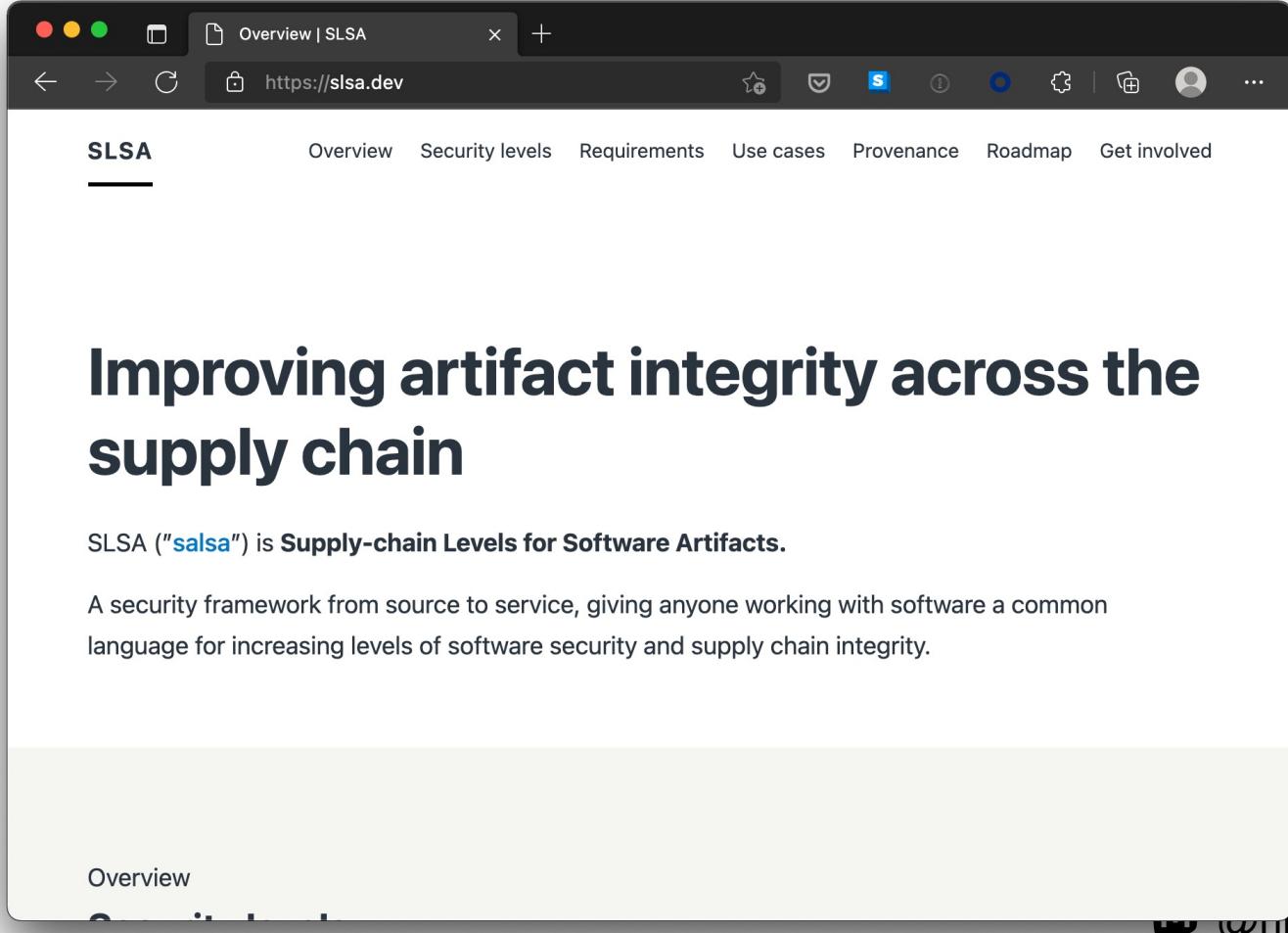
Lab 4

CycloneDX .NET

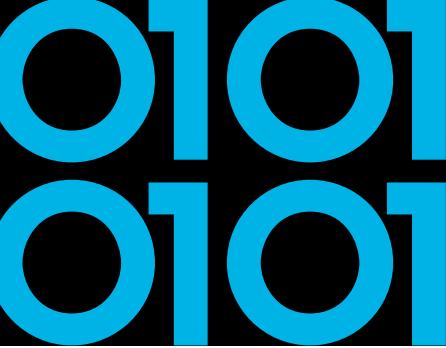




Google SLSA



The screenshot shows a web browser window displaying the official SLSA website at <https://slsa.dev>. The page has a dark header with the title "Overview | SLSA". Below the header is a navigation bar with links: SLSA (which is underlined), Overview, Security levels, Requirements, Use cases, Provenance, Roadmap, and Get involved. The main content area features a large heading "Improving artifact integrity across the supply chain" in bold black font. Below the heading, a paragraph explains what SLSA is: "SLSA ("salsa") is Supply-chain Levels for Software Artifacts. A security framework from source to service, giving anyone working with software a common language for increasing levels of software security and supply chain integrity." At the bottom of the page, there is a footer with a "Overview" link and a copyright notice: "© 2020 Google LLC. All rights reserved. Google and the Google logo are trademarks of Google LLC." The footer also includes a small icon and the text "@melstanis@infosec.exchange".



Google SLSA Levels

Level	Description	Example
1	Documentation of the build process	Unsigned provenance
2	Tamper resistance of the build service	Hosted source/build, signed provenance
3	Extra resistance to specific threats	Security controls on host, non-falsifiable provenance
4	Highest levels of confidence and trust	Two-party review + hermetic builds

Google SLSA Levels

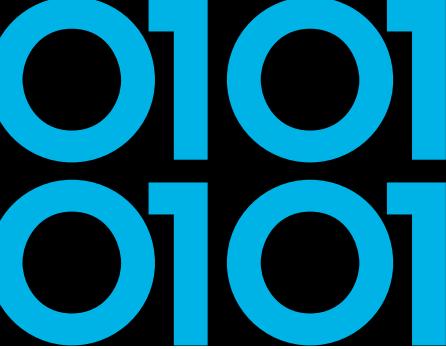


1. The build process must be fully scripted/automated and generate provenance.
2. Requires using version control and a hosted build service that generates authenticated provenance.
3. The source and build platforms meet specific standards to guarantee the auditability of the source and the integrity of the provenance respectively.
4. Requires two-person review of all changes and a hermetic, reproducible build process.



SLSA GitHub Action

- Released April 2022
- SLSA level 2 provenance generator in GitHub Action
- SLSA level 3+ provenance generator for Go binaries
- GitHub Hosted Runner
- Uses SigStore to do keyless signing with GitHub OIDC
- Verifier included



SLSA3 Generator GitHub Actions

The screenshot shows a web browser window with the following details:

- Title Bar:** SLSA - General availability of SLSA3 Generic Generator for GitHub Actions
- URL:** https://slsa.dev/blog/2022/08/slsa-github-workflows-generic-ga
- Header:** SLSA logo, navigation links: Overview, Specifications, Use cases, Get started, Community, Blog, and a GitHub icon.
- Main Content:**

General availability of SLSA3 Generic Generator for GitHub Actions

by Ian Lewis, Laurent Simon, Asra Ali
29 Aug 2022

A few months ago Google and GitHub announced [the release of a Go builder](#) that would help software developers and consumers more easily verify the origins of software by using verification files known as provenance. Since then, the SLSA community has been working to enable provenance generation for other projects that may use any number of languages or build tools. Today, we're pleased to announce that we're adding a new tool to generate similar provenance documents for projects developed in any programming language, while keeping your existing building workflows.

Lab 5

SLSA Level 3 Provenance

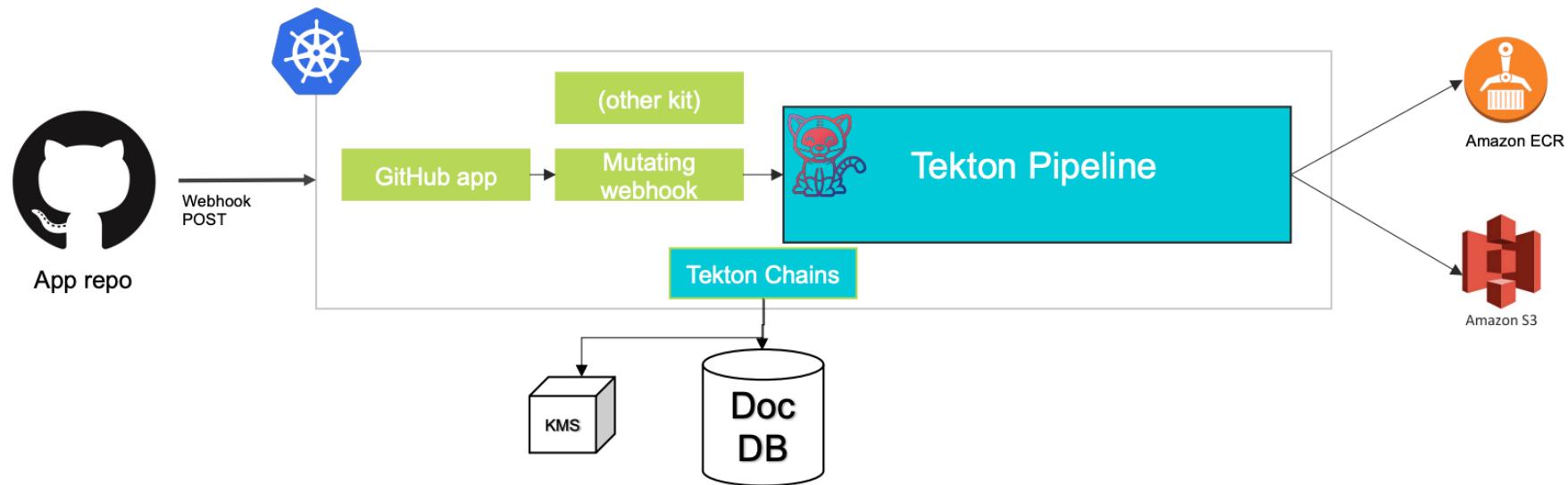




SolarWinds Project Trebuchet



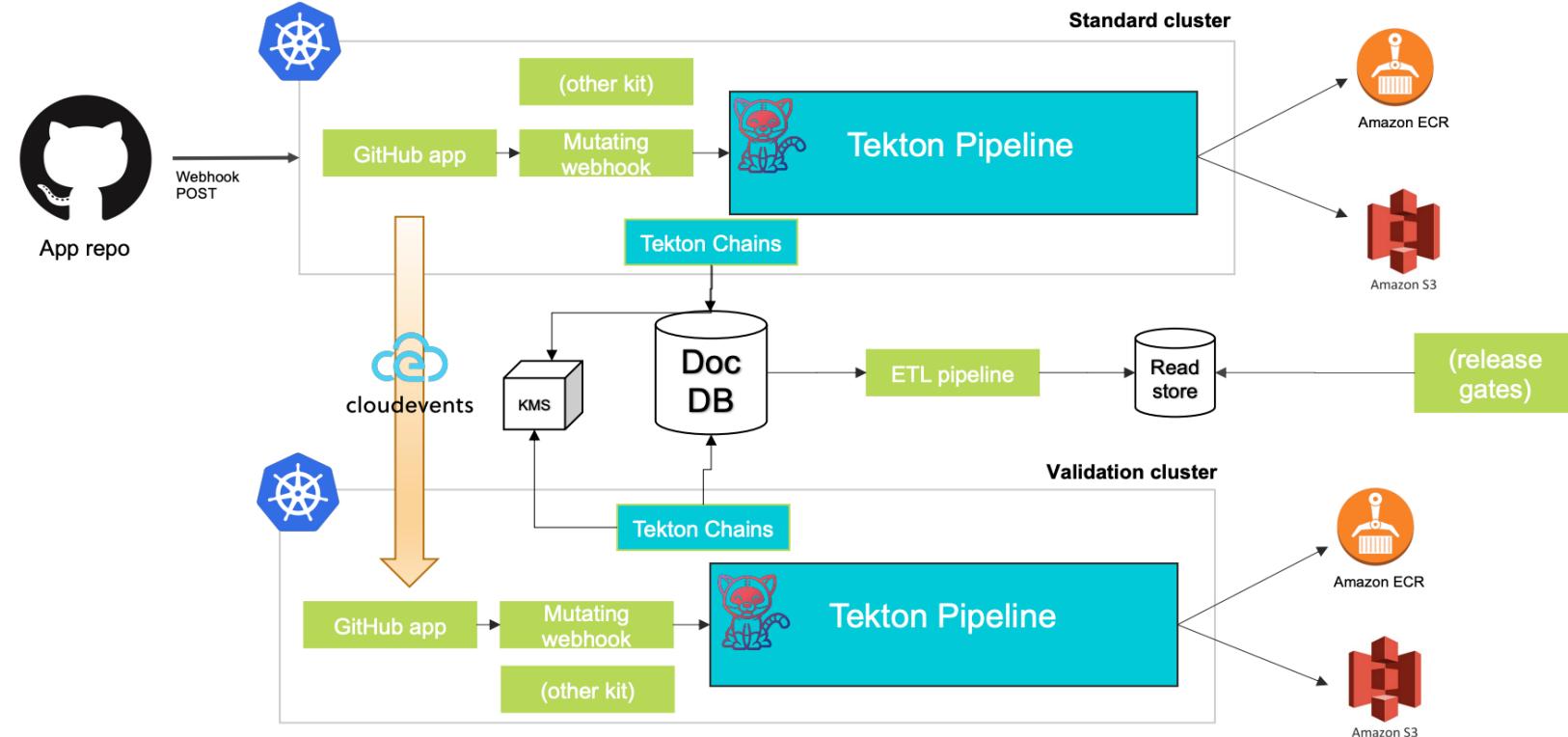
Pipeline With Attestations



SolarWinds Project Trebuchet



Reading Results



Lab 6

DocGenerator on
ASP.NET Core MVC &
Docker



Docker SBOM

0101
0101

The screenshot shows a web browser displaying a Docker blog post. The title of the post is "Announcing Docker SBOM: A step towards more visibility into Docker images". The author is listed as JUSTIN CORMACK, dated Apr 7 2022. The post content discusses Docker's first step in making container images more visible for better software supply chain security. It mentions the inclusion of a new experimental CLI command, docker sbom, which displays the SBOM of any Docker image. The Docker logo is visible at the top left of the page. The navigation bar includes links for Products, Developers, Pricing, Blog, About Us, Partners, a search bar, Sign In, and a Get Started button. A sidebar on the right contains social sharing icons (Twitter, LinkedIn, Facebook) and sections for Post Tags (docker, Docker images, sbom, Secure Software Supply Chain) and Categories (Community, Company, Engineering, Newsletters, Products).

Join us for [DockerCon](#) on May 9-10th. Preview the agenda and [register today.](#)

[Get Started](#)

Announcing Docker SBOM: A step towards more visibility into Docker images

JUSTIN CORMACK
Apr 7 2022

Today, Docker takes its first step in making what is inside your container images more visible so that you can better secure your software supply chain. Included in Docker Desktop 4.7.0 is a new, experimental `docker sbom` CLI command that displays the SBOM (Software Bill Of Materials) of any Docker image. It will

Post Tags

- # docker
- # Docker images
- # sbom
- # Secure Software Supply Chain

Categories

- Community
- Company
- Engineering
- Newsletters
- Products

Lab 7

Docker SBOM with Anchor
and Syft



Signing artifacts

0101
0101

A screenshot of a web browser displaying the Sigstore website at <https://www.sigstore.dev>. The page has a light orange background. At the top left is the Sigstore logo (a stylized 'f'). To its right are navigation links: Overview (underlined), Community, How sigstore works, Trust and security, Blog, Docs, and a user icon. Below these links is a large, bold, dark gray text block: "A new standard for signing, verifying and protecting software". Underneath it is a smaller, dark gray text: "Making sure your software's what it claims to be.". At the bottom of the page, under the heading "In collaboration with", there is a row of logos from various tech companies: ChainGuard, Cisco, Google, Hewlett Packard Enterprise, The Linux Foundation, Purdue University, Red Hat, and VMware.

0101
0101

Signing artifacts

How sigstore works

sigstore is a set of tools developers, software maintainers, package managers and security experts can benefit from. Bringing together free-to-use open source technologies like Fulcio, Cosign and Rekor, it handles digital signing, verification and checks for provenance needed to make it safer to distribute and use open source software.

A standardized approach

This means that open source software uploaded for distribution has a stricter, more standardized way of checking who's been involved, that it hasn't been tampered with. There's no risk of key compromise, so third parties can't hijack a release and slip in something malicious.

Building for future integrations

With the help of a working partnership that includes Google, the Linux Foundation, Red Hat and Purdue University, we're in constant collaboration to find new ways to improve the sigstore technology, to make it easy to adopt, integrate and become a long-lasting standard.

```
graph TD; subgraph TR [TRUST ROOT]; FC[FULCIO CERTIFICATE AUTHORITY]; ST[SIGNATURE TRANSPARENCY LOG]; KT[KEY TRANSPARENCY LOG]; end; SP[SIGN AND PUBLISH ARTIFACTS] --- FC; SC[PUBLISH SIGNING CERTIFICATES] --- ST; M[MONITOR LOGS] --- KT; subgraph DM [DEVELOPERS, MAINTAINERS, MONITORS]; direction TB; SP --- DM; SC --- DM; M --- DM; end;
```

Lab 8

Keyless Signing artifact
with cosign





Signing artifacts

- Cosign can be used for signing files like binaries, packages and Docker images
- It can do keyless signing based on OpenID Connect
- GitHub Actions have released OpenID Connect support since end 2021

Lab 9

Cosign on Docker in
GitHub Actions



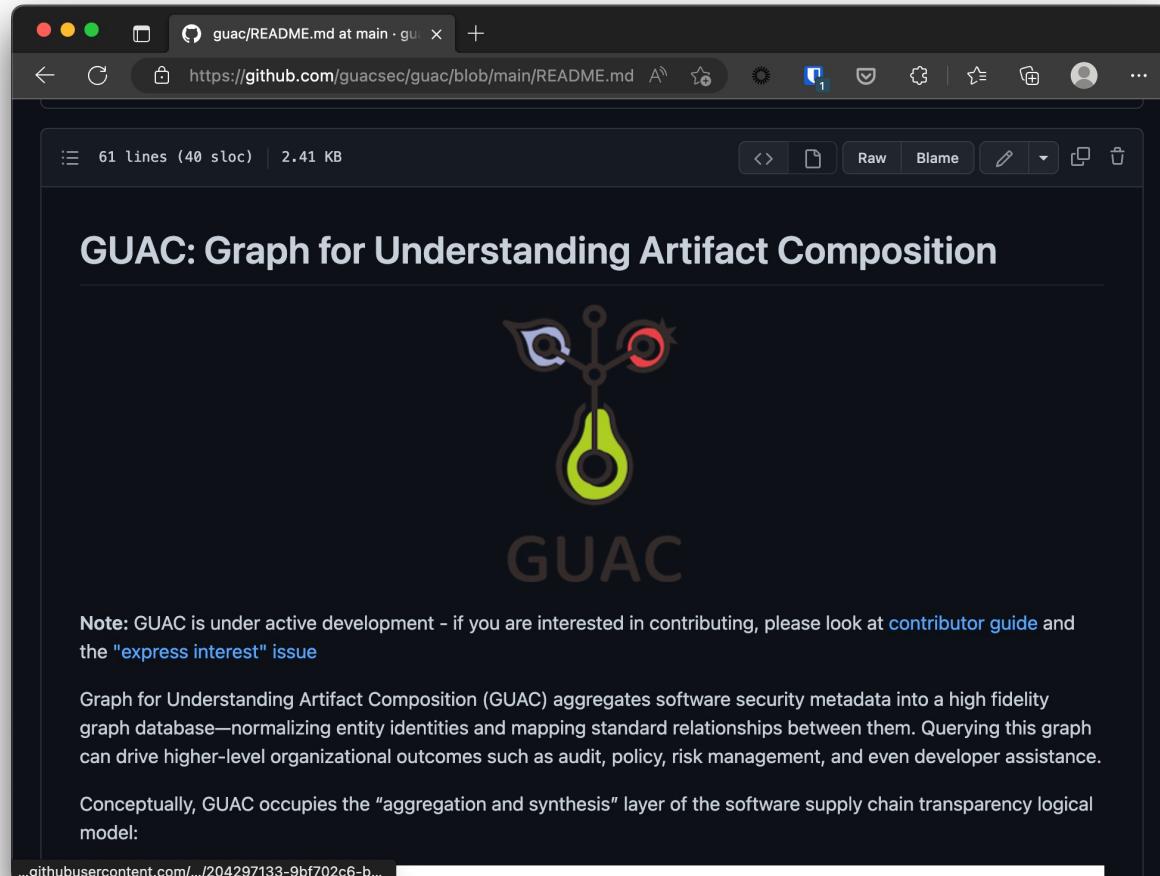
Lab 10

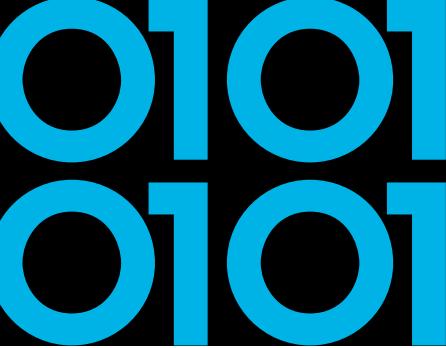
You got HACKED!



GUAC: Graph for Understanding Artifact Composition

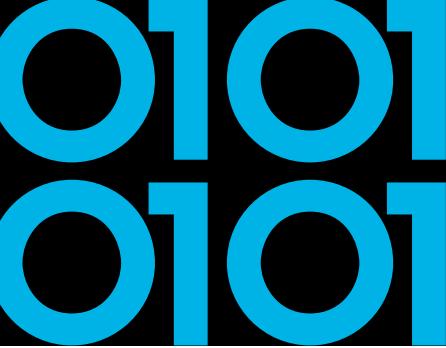
0101
0101





Conclusion

- It's not how it's more a matter of when!
- Be aware of your used software supply chain(s).
- Know what you're using and pulling into projects.



Conclusion

- Integrate security into your software lifecycle.
- Start working on creating SBOM's and see how SLSA can fit into your process.
- Try to work with SBOM output and use it!

VERACODE

Thanks! Questions?

<https://github.com/nielstanis/ndclondon2023-supplychainws>
ntanis at veracode.com
@nielstanis@infosec.exchange on Mastodon

