Trust and Risk in the software supply chain

Emmy Eide
Director, Supply Chain Security
Product Security, Red Hat

What is happening?

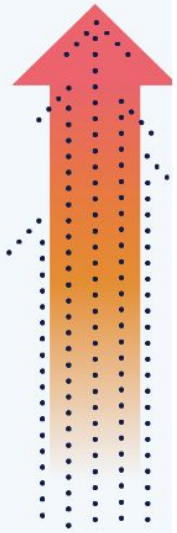
Supply chain attacks are increasing

We are probably more vulnerable than we think

There has been an astonishing

742%

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



Key Finding

About

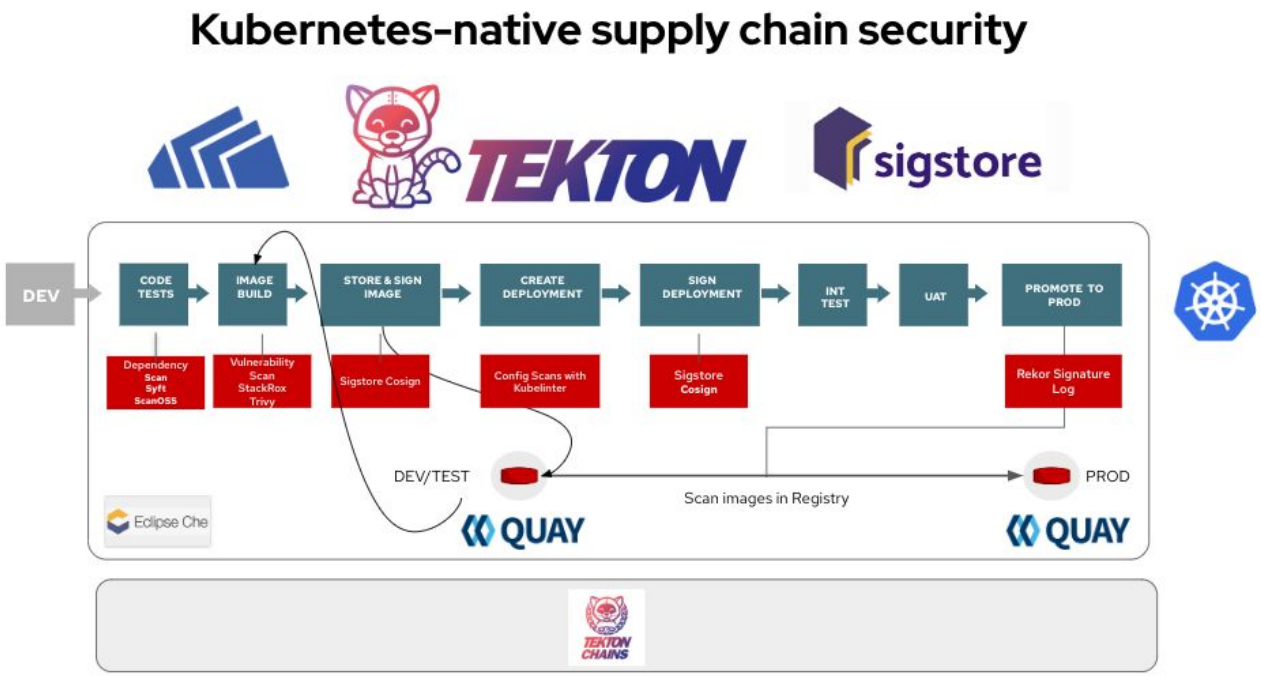
6 out of every **7**

project vulnerabilities come from transitive dependencies.

Key Finding

2022 State of the Software Supply Chain - Sonatype

Security Tools and Ideas



User Identity and Access Management

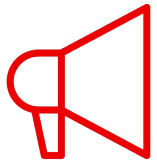
Standard user accounts are the primary entrypoint for accessing an environment.

Implement robust policies to increase security and reduce threat vector

- Integrate with an external identity provider that offers 2-factor auth
- Manage cluster access and application access separately
- Limit host access to break-glass scenarios
- Minimize privileged access with role based access controls

Requirement	SLSA 1	SLSA 2	SLSA 3	SLSA 4
Source - Version controlled		✓	✓	✓
Source - Verified history			✓	✓
Source - Retained indefinitely			18 mo.	✓
Source - Two-person reviewed				✓
Build - Scripted build	✓	✓	✓	✓
Build - Build service		✓	✓	✓
Build - Build as code			✓	✓
Build - Ephemeral environment			✓	✓
Build - Isolated			✓	✓
Build - Parameterless				✓
Build - Hermetic				✓
Build - Reproducible				○
Provenance - Available	✓	✓	✓	✓
Provenance - Authenticated		✓	✓	✓
Provenance - Service generated		✓	✓	✓
Provenance - Non-falsifiable			✓	✓
Provenance - Dependencies complete				✓
Common - Security				✓
Common - Access				✓
Common - Superusers				✓

Partnership



Security partnerships transform ideas to results

Guidelines and Expectations

Set forth ground rules (driven by policies as code) that engineers should be aware of up front

Coordinate Implementation

Consider development planning timelines, integration requirements, and maintenance upkeep

Tie it back to Risk

Be able to articulate why IdM is important, what signing provides our customer, the risk of not scanning code and infrastructure throughout the supply chain.

Thank you

Red Hat is the world's leading provider of enterprise open source software solutions. Award-winning support, training, and consulting services make
Red Hat a trusted adviser to the Fortune 500.


linkedin.com/company/red-hat


youtube.com/user/RedHatVideos


facebook.com/redhatinc


twitter.com/RedHat

Red Hat