TECoSA Edge Computing Summit

17th June 2024

How did this CVE get into production?

Secure your software supply chain end to end with Red Hat's Trusted Software Supply Chain

Vem är jag?

Red Hat
11 yrs 5 mos

- **Principal Chief Architect, Global CTO Organisation**
  Full-time
  Feb 2023 - Present · 1 yr 5 mos
  Global · Remote
- **EMEA Chief Technologist - Infrastructure Platform and Security**
  Full-time
  Jan 2020 - Feb 2023 · 3 yrs 2 mos
  EMEA
- **Principal Architect**
  Mar 2017 - Jan 2020 · 2 yrs 11 mos
- **Senior Architect**
  Sep 2014 - Mar 2017 · 2 yrs 7 mos
  Europe, Middle East & Africa
- **Senior Consultant**
  Feb 2013 - Sep 2014 · 1 yr 8 mos

CHRIS JENKINS

Principal Chief Architect
Red Hat Global CTO Office

Red Hat

Software supply chain attacks: a matter of when, not if

742%

average annual increase in software supply chain attacks over the past 3 years

20%

data breaches are due to a compromised software supply chain

78%

have initiatives to increase collaboration between DevOps and Security teams

92%

say enterprise open source solutions are important as their business accelerates to the open hybrid cloud

Red Hat

When it can go wrong

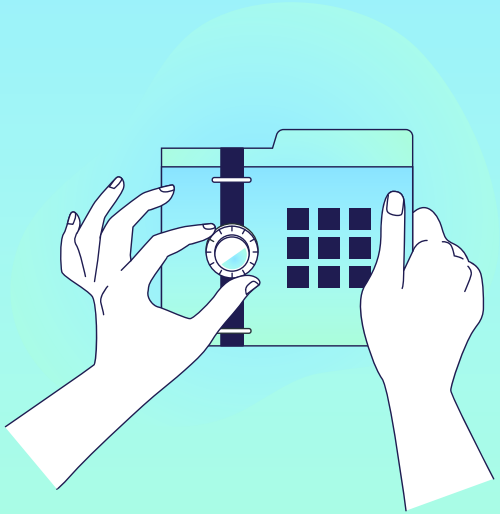
- Defence in Depth
- Patched systems
- 24/7 Monitoring and alerting
- Experienced IT/Security teams
- Annual compliance auditing

Malicious code in an untrusted or unknown dependency

Red Hat

Growing attack surfaces with new, emerging threats daily

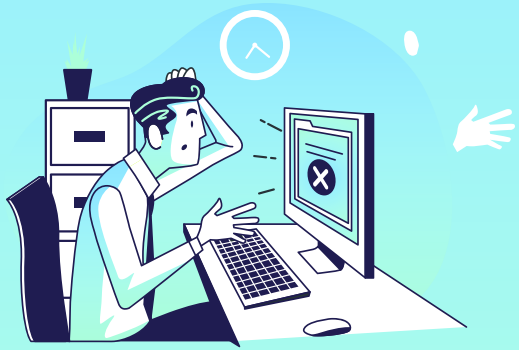
Secure software supply chain security is a critical component to securing data, Intellectual Property, source code and edge devices



- Lack of CVE awareness
- Typosquatting Attack (i.e. Goggle.com)
- Dependency Confusion
- Compromised Build Environment
- Malware preinstalled on edge devices
- Edge deployment
- Etc, etc, etc!

Red Hat

Minimum Requirements For Trust



Software Bill of Materials (SBOMs)

Understand where your software comes from (provenance), who created it (licensing) and who certifies it (signatures/attestation)

Vulnerability management

Access to vulnerabilities databases, understand vulnerability exploitability (VEX) and access to fixes and remediations

Software composition analysis

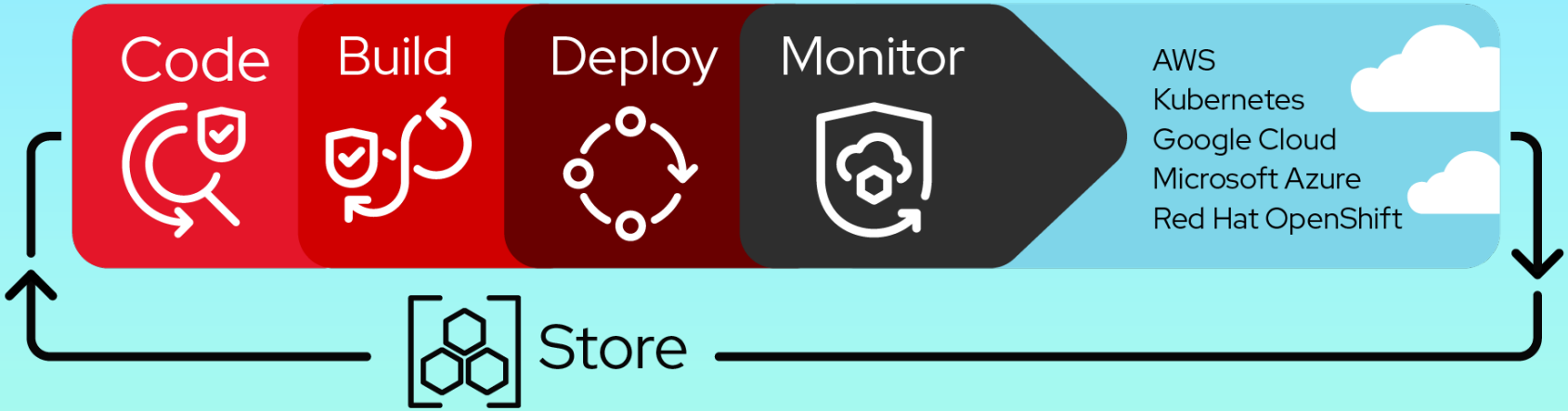
Understand and map relationships to open source software for all business critical applications across all environments

Continuous updates, monitoring and logging

Once deployed to your edge device, security doesn’t end!

Red Hat

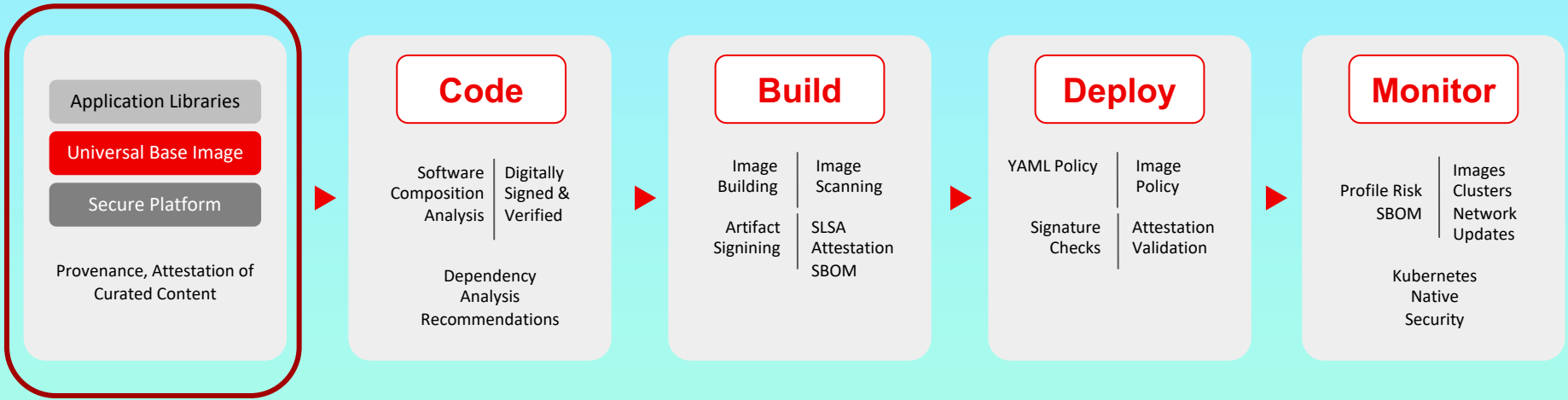
The Software Supply Chain



Red Hat

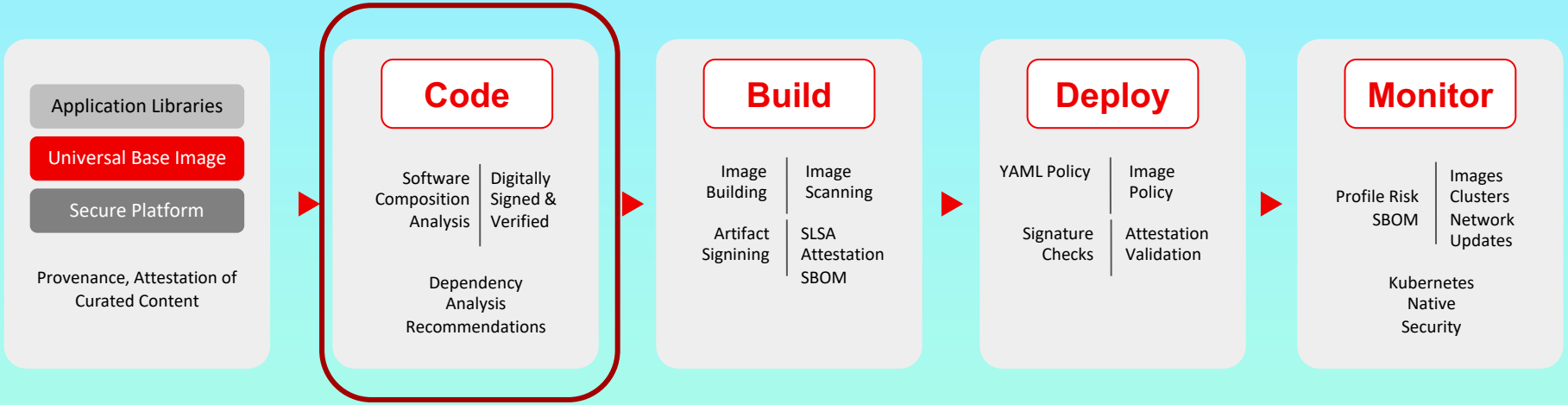

What can we do to
SECURE
the Software Supply Chain?

Start by using Trusted Content



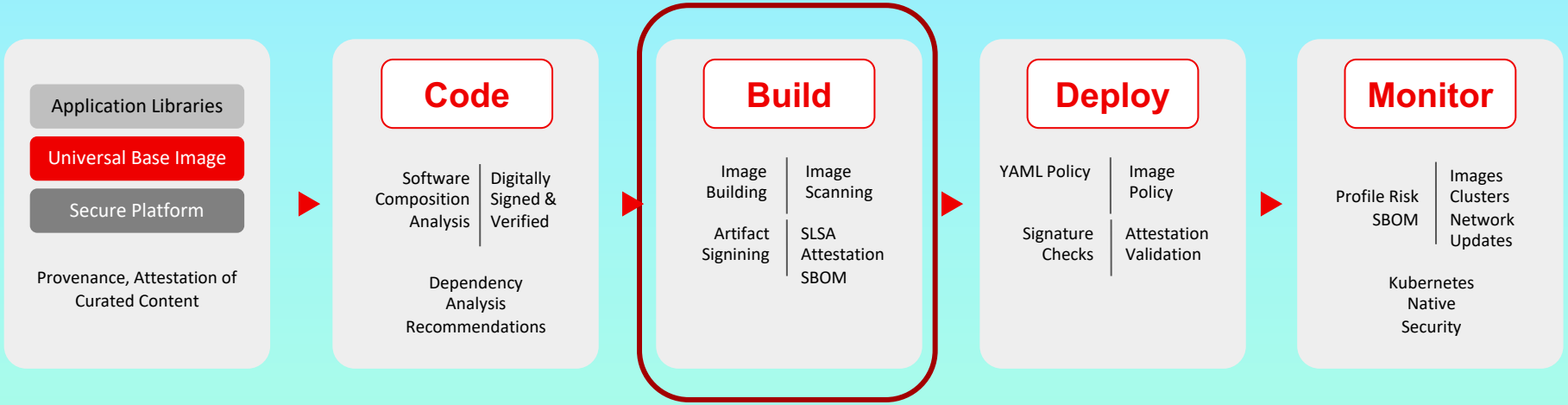
Red Hat

Ensure you have Trusted Code



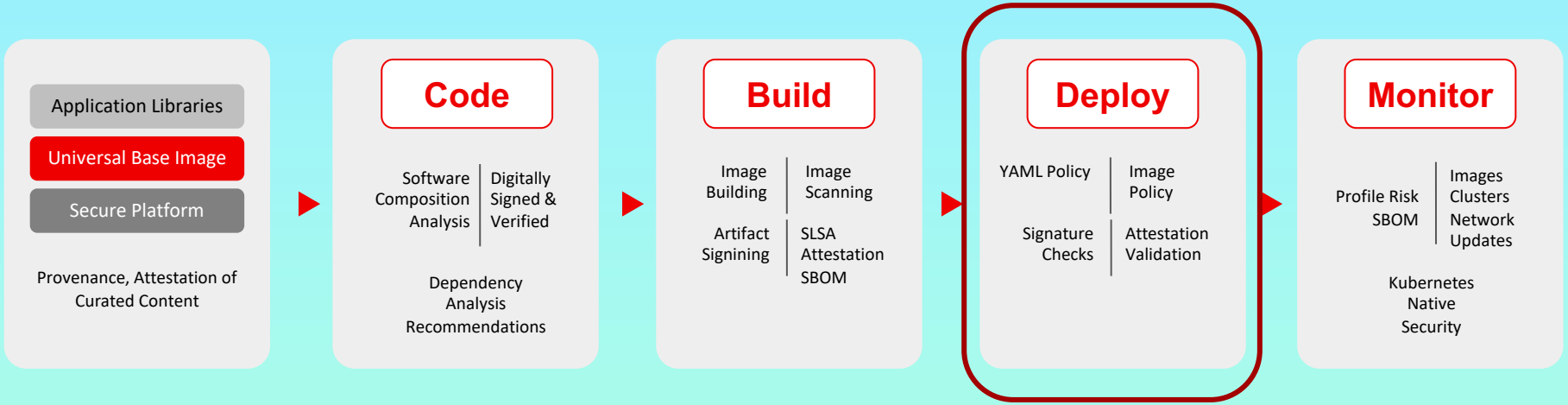
Red Hat

Automate and attest your build process



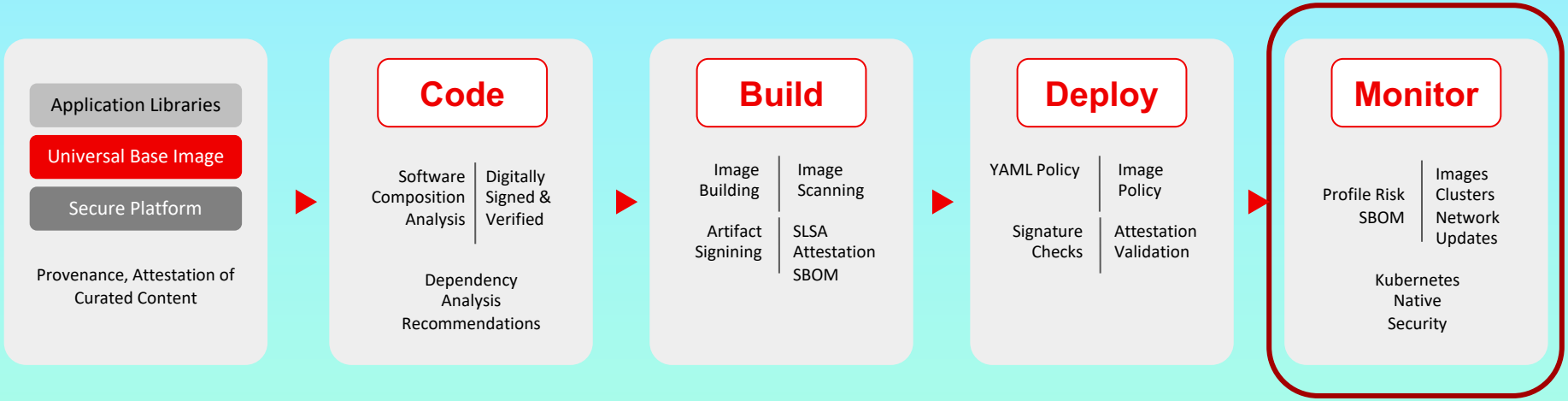
Red Hat

Secure and verified deployment



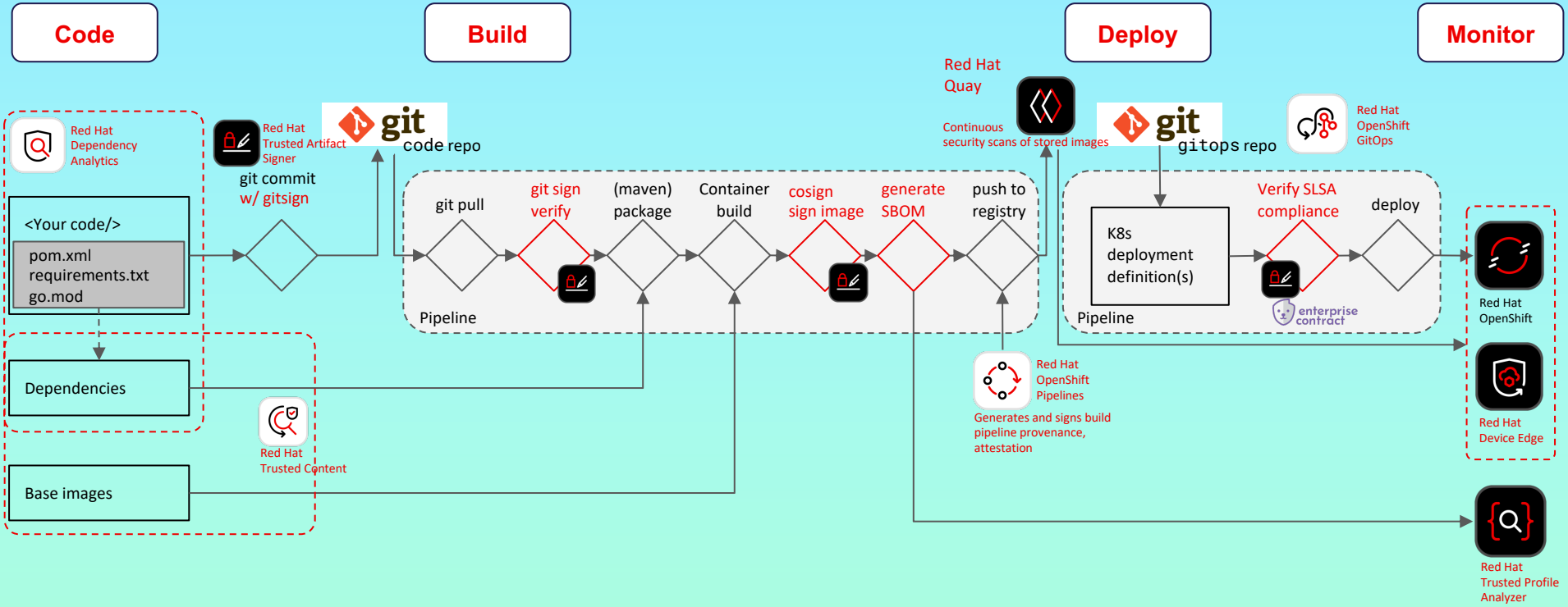
Red Hat

Continuous monitoring



Red Hat

A security-augmented development process



Red Hat

A Golden Path Pipeline Example

From Git commit to Production in 5 minutes and 39 seconds !

Red Hat
Trusted Profile
Analyzer

Red Hat

How can Red Hat help securing you Edge devices?

Red Hat
Trusted Software
Supply Chain

Developer self-service hub with pre-integrated security guardrails: artifact signatures, attestations & SBOMs

Red Hat Trusted Application Pipeline = **Red Hat** Developer Hub + **Red Hat** Trusted Artifact Signer + **Red Hat** Trusted Profile Analyzer

Red Hat OpenShift

Red Hat Advanced Cluster Security for Kubernetes

Red Hat Quay

Red Hat

QUESTIONS | THOUGHTS | COMMENTS

Red Hat

Tack så mycket!

chrisj@redhat.com

linkedin.com/company/red-hat

youtube.com/user/RedHatVideos

facebook.com/redhatinc

twitter.com/RedHat

Red Hat