

Modern Software Pipelines

OMNISECURE 2024

2024-01-22

Bernhard Cygan

Senior Solution Architect





BP can now provision
a new environment in
7 minutes, instead
of **2-3 weeks**.

BP runs security scans on every build and container with Red Hat OpenShift running on Amazon Web Services

Challenge

Modernize a complex technology infrastructure to speed app development.

Solution

BP used Red Hat® OpenShift® to build a self-service platform that supports DevOps and provides a continuous integration/continuous delivery (CI/CD) pipeline.

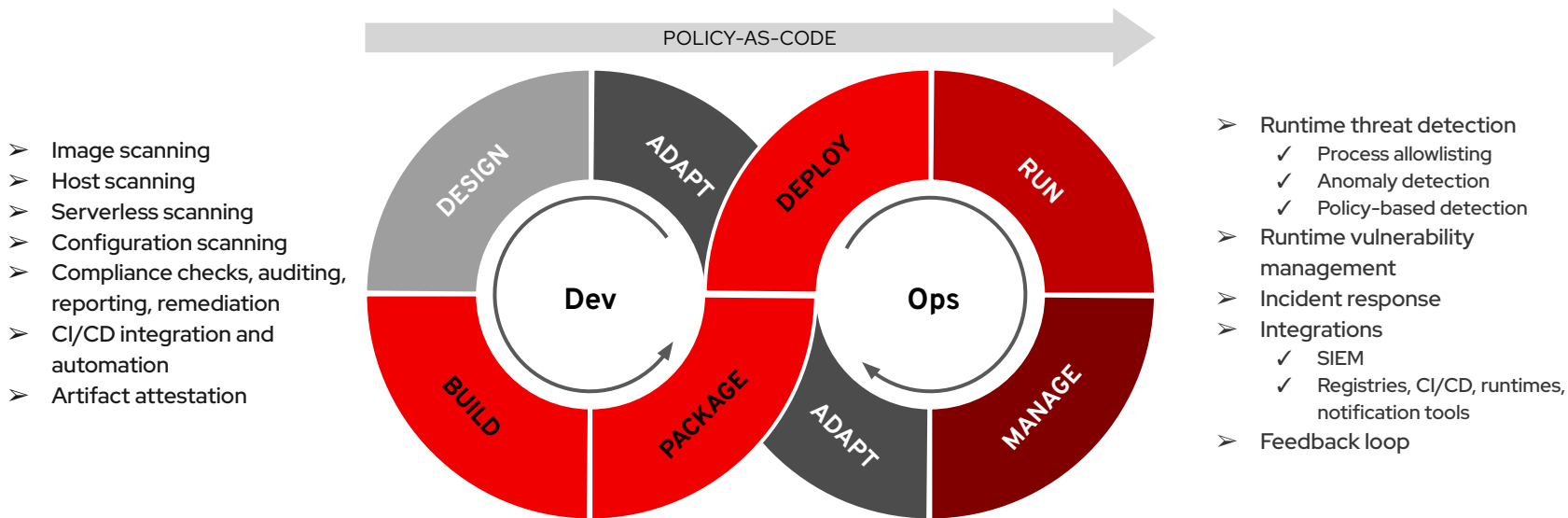
Why Red Hat

BP wanted an open source solution with enterprise support and security.

Results

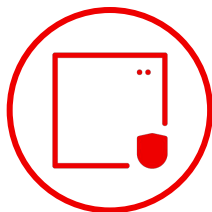
- Reduced provisioning time for faster speed to market
- Improved security with security scans on every build and container
- Increased agility with DevOps and self-service capabilities

Security across the entire application lifecycle



Secure the complete Software Delivery Lifecycle

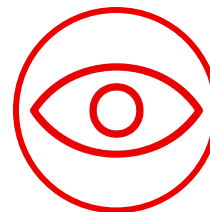
Prevent & identify
malicious **code**



Safeguard **build**
systems early



Continuously **monitor**
security at runtime



How does that look in real life ?

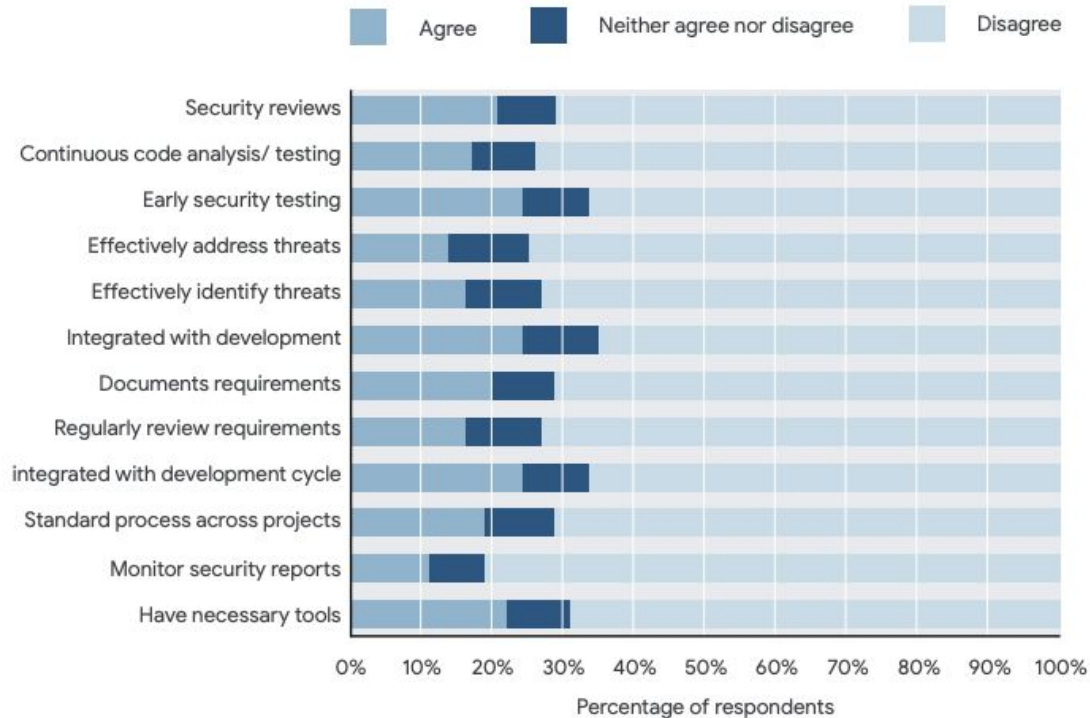
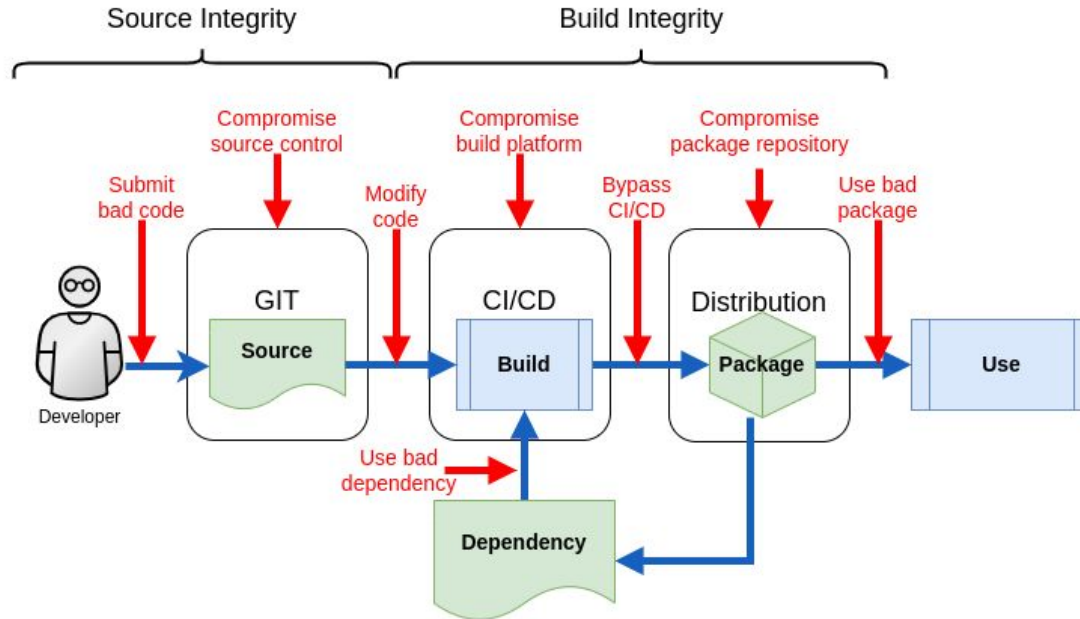


Figure 2. Establishment of SSDF practices

Survey responses about the establishment of SSDF practices. Similar to SLSA, a majority of respondents agreed that their organization followed all of these practices.

Attack Vectors of a Software Supply Chain

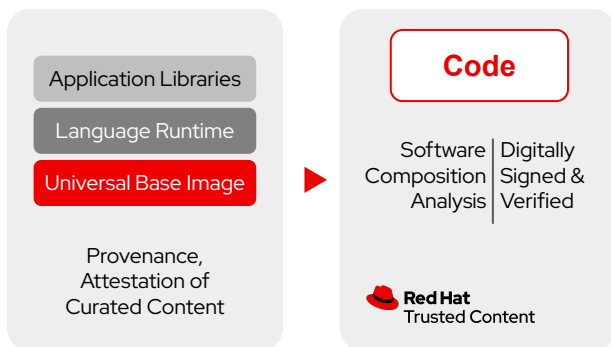


Attack Vectors

- ▶ Multiple vectors
- ▶ Fully recursive dependencies !

Eine Secure Software Supply Chain ist kein Produkt und kein Feature, sondern hauptsächlich ein Prozess!

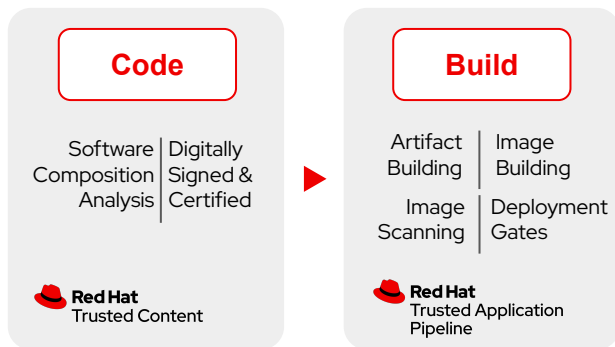
Code with integrated application security checks



Catch security issues early to
keep and grow user trust

- ▶ Trusted curated content
- ▶ Automated software composition analysis and dependency analytics
- ▶ Aggregated view with drill down on security health
- ▶ Cryptographic signing and verification

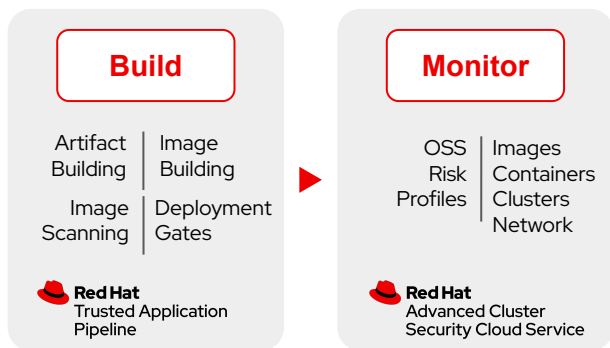
Build with security focused CI/CD workflows



Meet industry compliance while increasing productivity, efficiency

- ▶ Integrated security guardrails across pipelines
- ▶ Auto-generated Software-Bill-of-Materials (SBOM)
- ▶ Attestations and provenance checks
- ▶ Deployment based on policies to a declared state
- ▶ Continuous image vulnerability scanning
- ▶ Infrastructure and Pipeline as code

Monitor and identify runtime security incidents

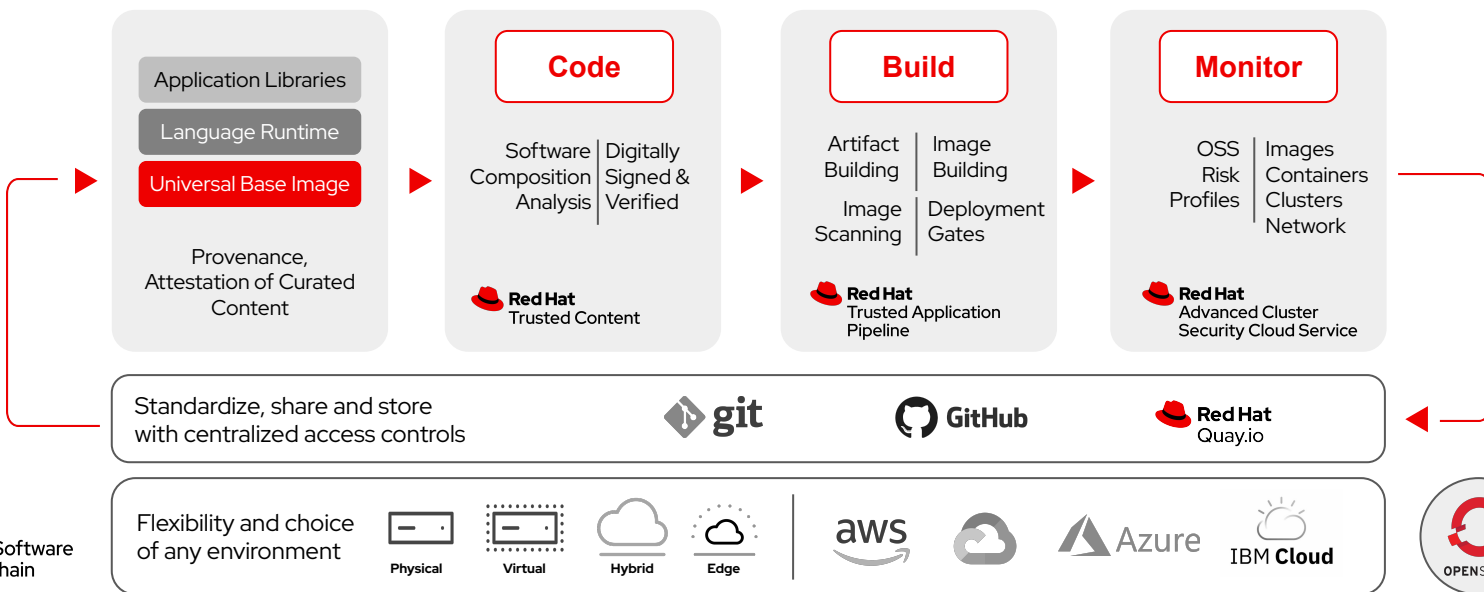


Reduce noise, alert fatigue for shorter time to response

- ▶ Continuous improvement from runtime to build
- ▶ Detect and respond to suspicious activity
- ▶ Runtime vulnerability scanning and management
- ▶ Audit for compliance across hundreds of controls
- ▶ Expedite incident response to reduce down times

Code, build, and monitor to a Trusted Software Supply Chain

Delivered as a **service** with integrated security guardrails at every phase of the software development lifecycle

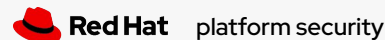


Enhance and extend security functionality

Build on Red Hat functionality through our **security partners** to better secure the entire DevOps life cycle.

- ▶ Increase Trust
- ▶ Reduce Risk
- ▶ Improve Compliance
- ▶ Enhance Collaboration
- ▶ Increase Agility
- ▶ Improve Quality

Application analysis	Identity & access management
SAST, SCA, IAST, DAST, Image risk	Authn, Authz, Secrets Vault, HSM, Provenance
Compliance	Network controls
Regulatory compliance, PCI-DSS, GDPR	CNI plugins, policies, traffic controls, service mesh
Data controls	Runtime analysis & protection
Data protection and encryption	RASP, production analysis
Audit and monitoring	Remediation
Logging, visibility, forensics	SOAR, automatic resolution



Secure host, container platform, namespace isolation, k8s and container hardening (BSI Grundschutz, FIPS, NIST SP800, ISO 27000, Zero Trust, ...)

Und am wichtigsten:

Automate the hell out of everything !

Was sonst noch ?

BSI Grundschutz -

https://www.bsi.bund.de/DE/Themen/Unternehmen-und-Organisationen/Standards-und-Zertifizierung/IT-Grundschutz/it-grundschutz_node.html

Zero Trust Architecture - https://en.wikipedia.org/wiki/Zero_trust_security_model

OpenSSF (Open Source Security Foundation) - <https://openssf.org/>

SDLC (Software Development Lifecycle) -

https://de.wikipedia.org/wiki/Vorgehensmodell_zur_Softwareentwicklung

SLSA (Reifegrad von Software-Entwicklungsprozessen) - <https://slsa.dev/>

Danke für Ihre Aufmerksamkeit!

 linkedin.com/company/red-hat

 youtube.com/user/RedHatVideos

 facebook.com/redhatinc

 twitter.com/RedHat

Lesestoff

Red Hat Trusted Application Pipeline

<https://developers.redhat.com/articles/2023/07/18/introduction-red-hat-trusted-application-pipeline>

Blog zu Tekton und Trusted Application Pipeline

<https://www.redhat.com/en/blog/operating-tekton-scale-10-lessons-learned>

Securing the Software Supply Chain

https://www.cisa.gov/sites/default/files/publications/ESF_SECURING_THE_SOFTWARE_SUPPLY_CHAIN_DEVELOPERS.PDF

Bottlenecks in Software Development

<https://www.it-economics.de/en/software/bottlenecks-in-software-development/>

DORA Metrics

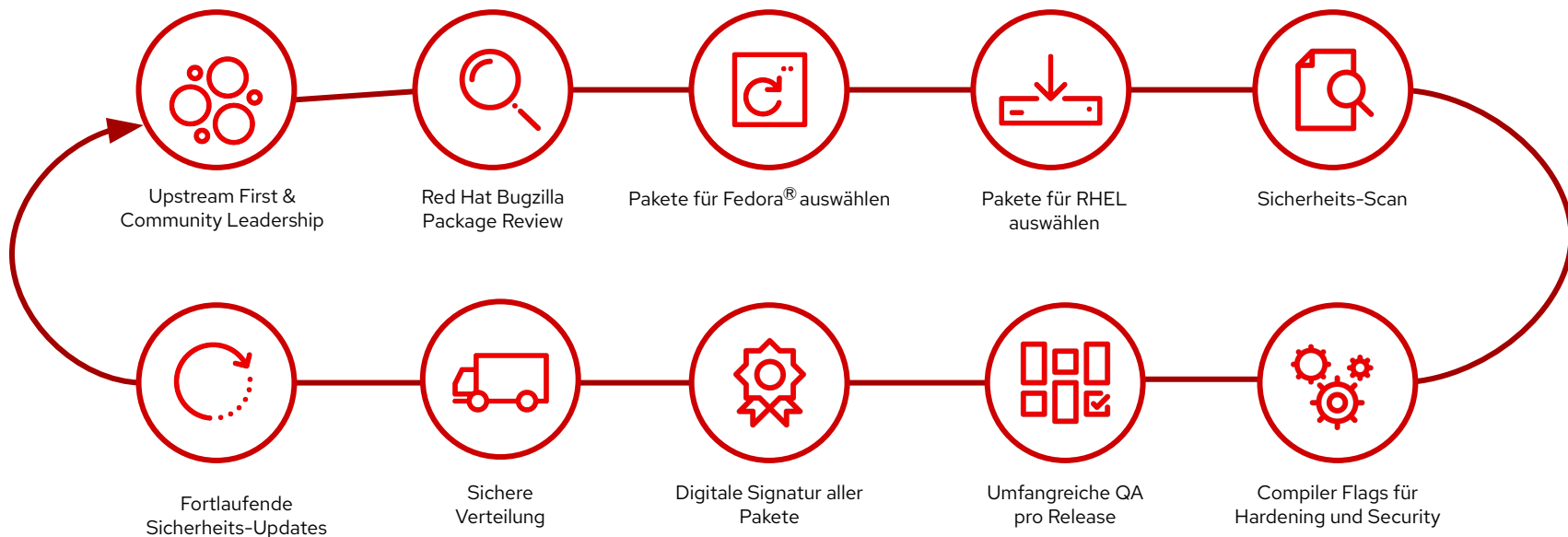
<https://cloud.google.com/blog/products/devops-sre/using-the-four-keys-to-measure-your-devops-performance>

How often do you patch ?

<https://www.opensourcerers.org/2022/12/05/how-often-do-you-patch/>

Red Hat's Secure Supply Chain für RHEL

Risiken reduzieren und Open Source für Firmen konsumierbar machen



Sicherheitsbewußtsein beim Kunden schaffen

