Red Hat Summit

Connect

Lab: From Development to Deployment: Securing The Software Supply Chain with Red Hat OpenShift

Anne Faulhaber
Technical Account Manager

Markus Nagel
Principal Technical Marketing Manager

Red Hat

Setting the Scene...

(less than 10mins. I hope...)

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

Ransom paid but a mere fraction to the overall downtime and recovery costs of a data breach

742%

average annual increase in software supply chain attacks over the past 3 years[1]

20%

data breaches are due to a compromised software supply chain[2]

78%

have initiatives to increase collaboration between DevOps and Security teams[3]

92%

say enterprise open source solutions are important as their business accelerates to the open hybrid cloud[4]

[1] State of the Software Supply Chain | [2] Cost of a Data Breach 2022 - IBM Report | [3] State of Kubernetes Security Report 2022 - Red Hat Report | [4] State of Enterprise Open Source 2022 - Red Hat Report

Red Hat

Increased Government Regulations after several SSC attacks

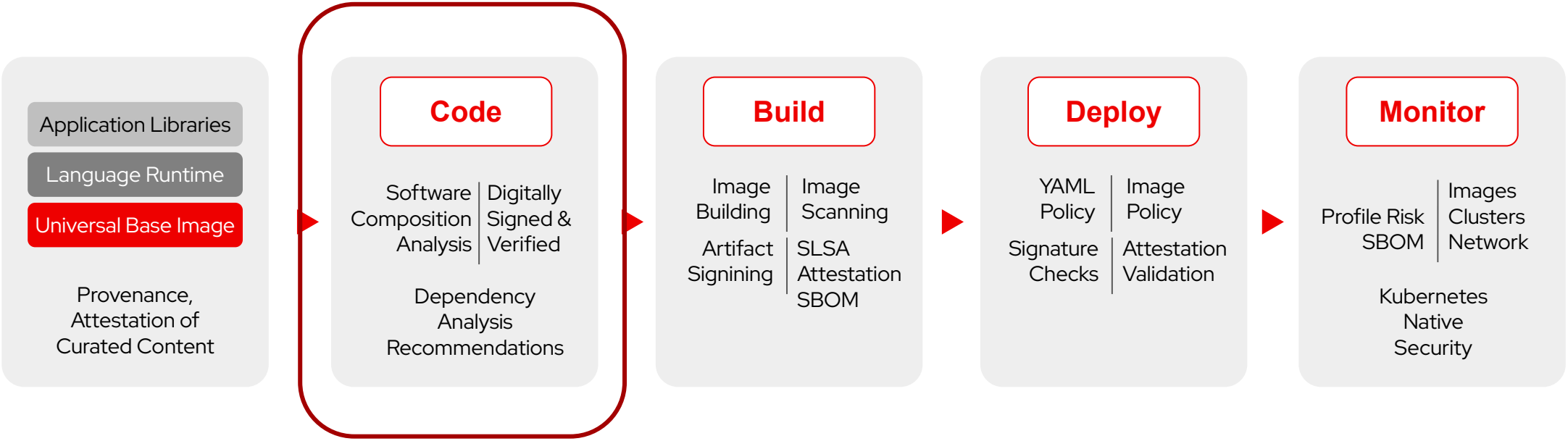
- US Executive Order on Improving the Nation's Cybersecurity
- US Executive Order 14017 - America's Supply Chains
- US Executive order 14018 Improving the Nation's Cybersecurity
- EU Network and Information Security 2 Directive
- Government willingness to enforce and fine executives ignoring SSC
  - SEC fines SolarWinds and CISO for concealing vulnerabilities
  - Log4J vulnerability

Red Hat

The Software Supply Chain

Red Hat

Give your developers the right tools



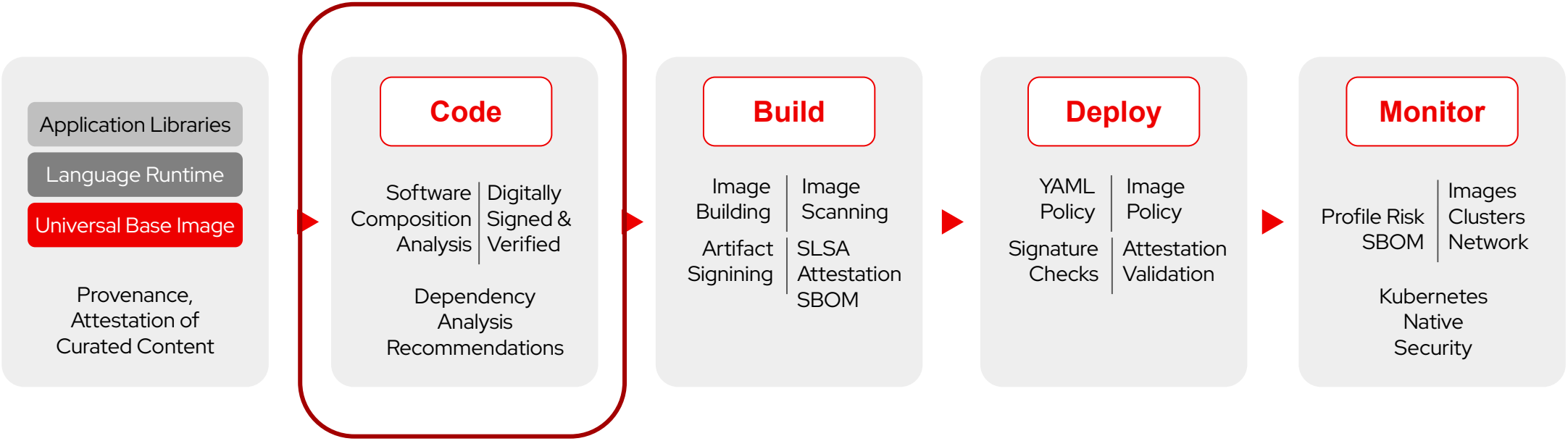
Red Hat Trusted Profile Analyzer

- Software composition analysis, dependency analysis, recommendations
- As report or as IDE Plugin

Red Hat Trusted Artifact Signer

- “Keyless” signing and verification of artifacts
- Sign on commit (gitsign)
- Events are stored in tamper-proof ledger for verification
- Signature is tied to OIDC Identity (Keycloak, Google, GitHub,...)
- No need to manage signing keys

Give your developers the right tools



Red Hat Developer Hub

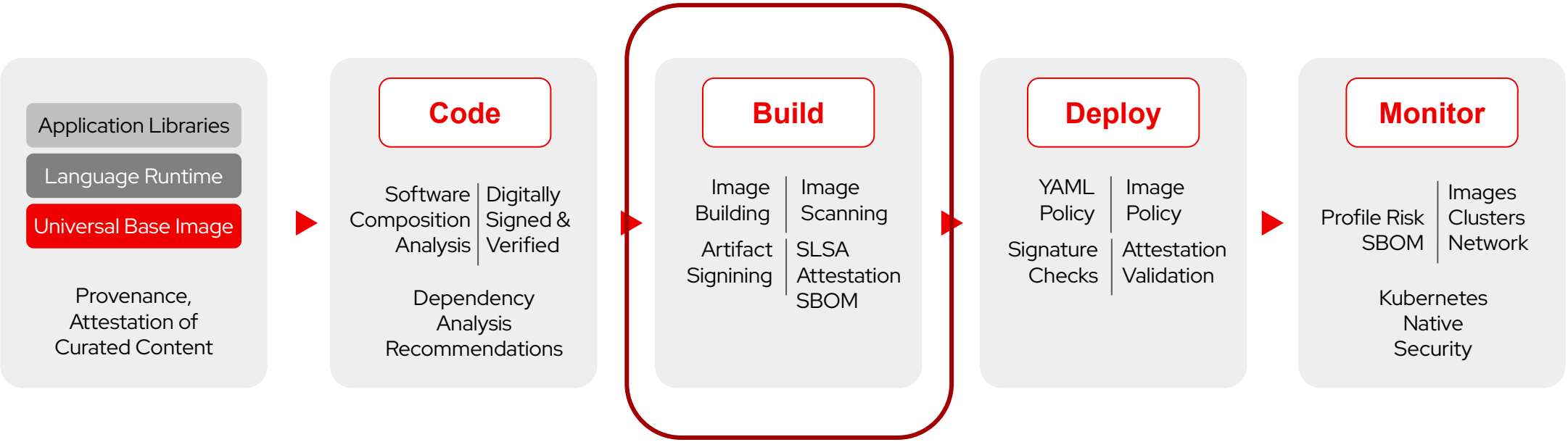
- IDP (Internal Developer Platform), based on Backstage.io
- Provides not only development templates and a developer-focused view on infrastructure, build systems, code repositories, etc - but **in the TSSC context**:

- Security-related guardrails and automated build and deployment pipelines
- When using Red Hat Developer Hub (RHDH), developers can
  - be onboarded easily to company security standards & procedures
  - start coding using security-focused coding templates

  without those security best practices and tools “standing in their way”

Red Hat

Augment and secure your build process (CI)



Red Hat Trusted Profile Analyzer

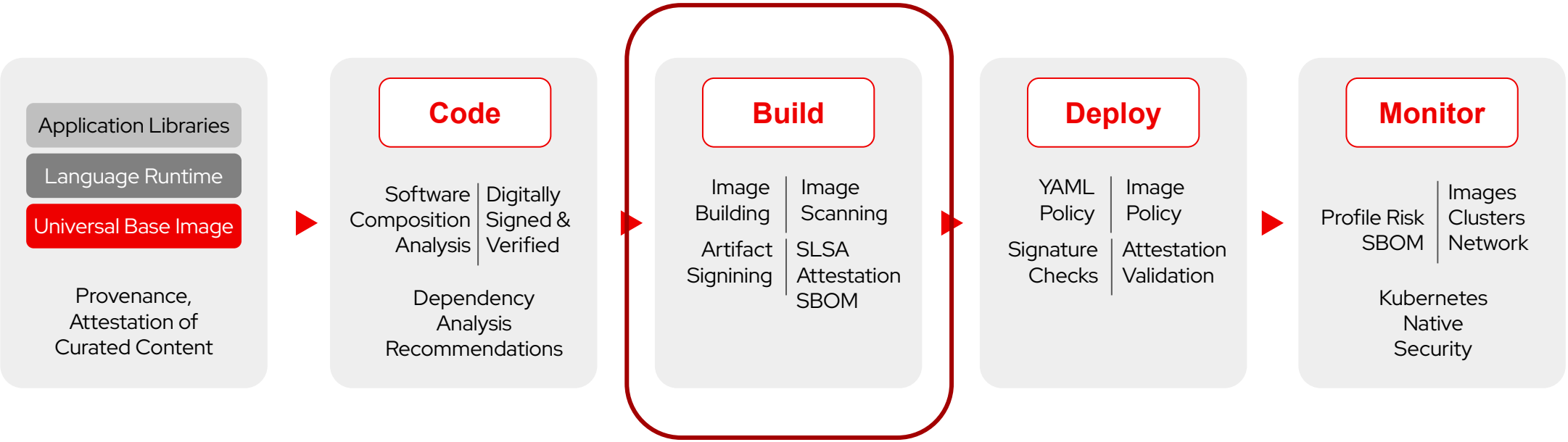
- Generate your SBOMs with e.g. CycloneDX plugin during maven / gradle build or via SYFT, analyzing image layers (just two examples) and feed them into Trusted Profile Analyzer
- Sign your generated SBOMs with RH Trusted Artifact Signer

Red Hat Trusted Artifact Signer

- Keyless verification against ledger that code has been signed and is authentic
- Sign your built artifacts
- Verify the integrity of the build platform (depends on Pipeline capabilities, works with e.g. Tekton/OpenShift Pipelines), providing attestations

Red Hat

Augment and secure your build process (CI)



Red Hat Quay

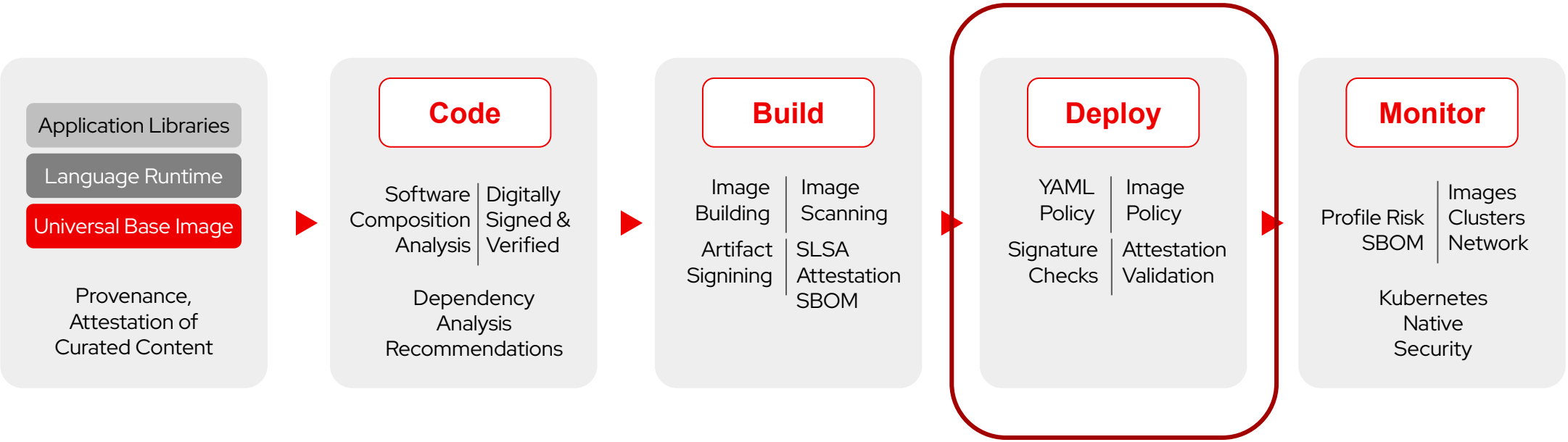
- Secure image registry. Also stores image related signatures, attestations and SBOMs
- Continuous image scanning (no pipeline run or other action required)

Red Hat
Advanced Cluster Security
for Kubernetes

- Policy-based image scanning (e.g. no log4j allowed)
- Policy-based deployment scanning (e.g. have resources and limits been set according to policy, etc)

Red Hat

Augment and secure your deployment process (CD)

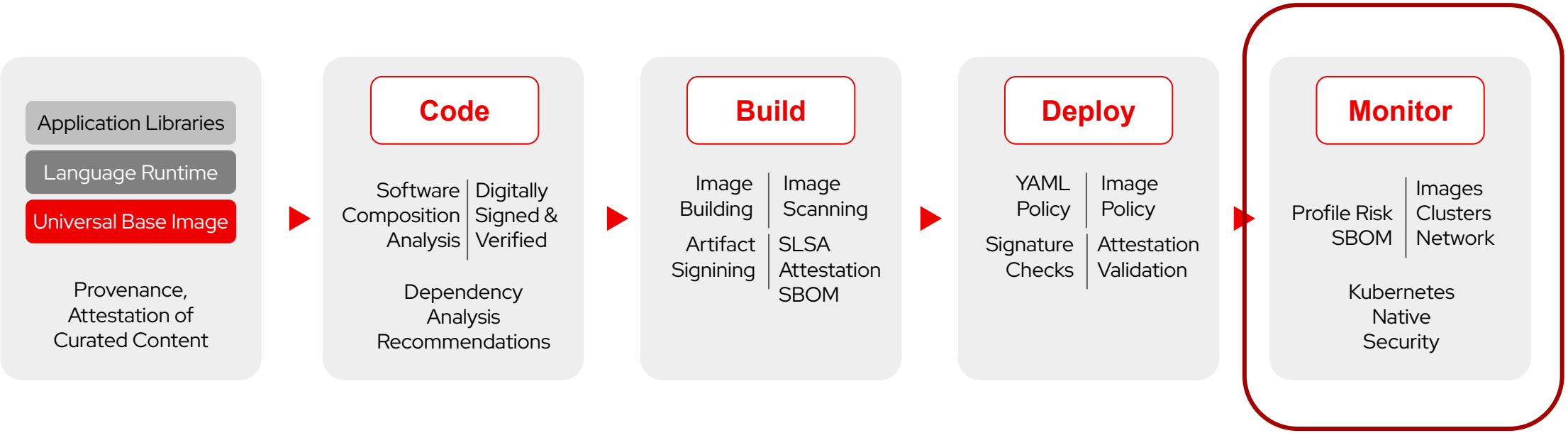


Red Hat Trusted Artifact Signer

- Only allow propagation / deployment of signed and verified build artifacts (keyless verification)
- Sign test results from automated testing frameworks to provide audit trail
- Use Enterprise Contract (EC) to validate attestations (has it really been built on the secure build system or on someone's laptop?)

Red Hat

Manage your Security Posture and monitor your platform



Red Hat
Trusted Profile Analyzer

- Ingest and manage SBOMs and VEXs from your own build process and 3rd parties
- Analyze CVE impact (where am I using library xyz in my own or 3rd party code/apps, is it relevant in my context)
- Manage Risk, improve your security posture

Red Hat
Advanced Cluster Security for Kubernetes

- Ensure policy compliance across clusters, especially production. “Don’t run xyz (e.g. log4j, struts, etc)” - regardless where it came from/how it was deployed.
- Networking: Are namespaces hardened, properly isolated and locked down? Don’t let a 3rd party vulnerability impact other namespaces.

Red Hat

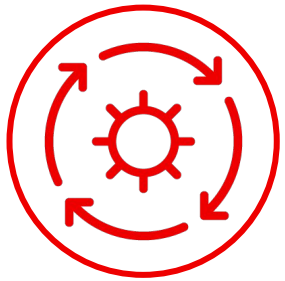
Red Hat Developer Hub - Empowering engineering to deliver business value faster

A renewed developer experience

Single pane of glass to increase engineering productivity.

Self-service **with guardrails** for cloud-native development **and security.**

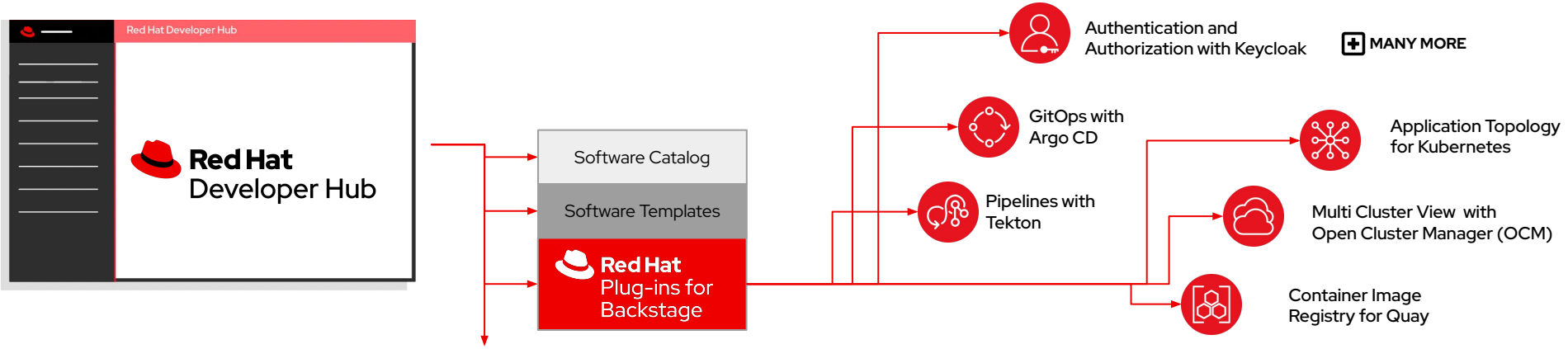
Best practices with **GitOps** and **automation**.



Real-time view of application and infrastructure **health & security.**

Red Hat

Red Hat Developer Hub - Empowering engineering to deliver business value faster



Integrates with industry standards and technologies through a broad ecosystem.

git Jenkins MANY MORE

Based on Backstage, an open source platform for building developer portals.

Backstage

Consistent developer experience across environments.

Physical Virtual Hybrid aws Azure IBM Cloud Red Hat OpenShift

Red Hat

Accelerate Innovation that Safeguards User Trust

Delivered with integrated security guardrails at every phase of the software development lifecycle

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

Included in **Red Hat** OpenShift Platform Plus but also available separately

Red Hat OpenShift

Red Hat Advanced Cluster Security for Kubernetes

Red Hat Quay

**Red Hat Trusted Application Pipeline is a single product SKU*
Includes Red Hat Developer Hub, Red Hat Trusted Artifact Signer, Red Hat Trusted Profile Analyzer capabilities with its own installer

Red Hat

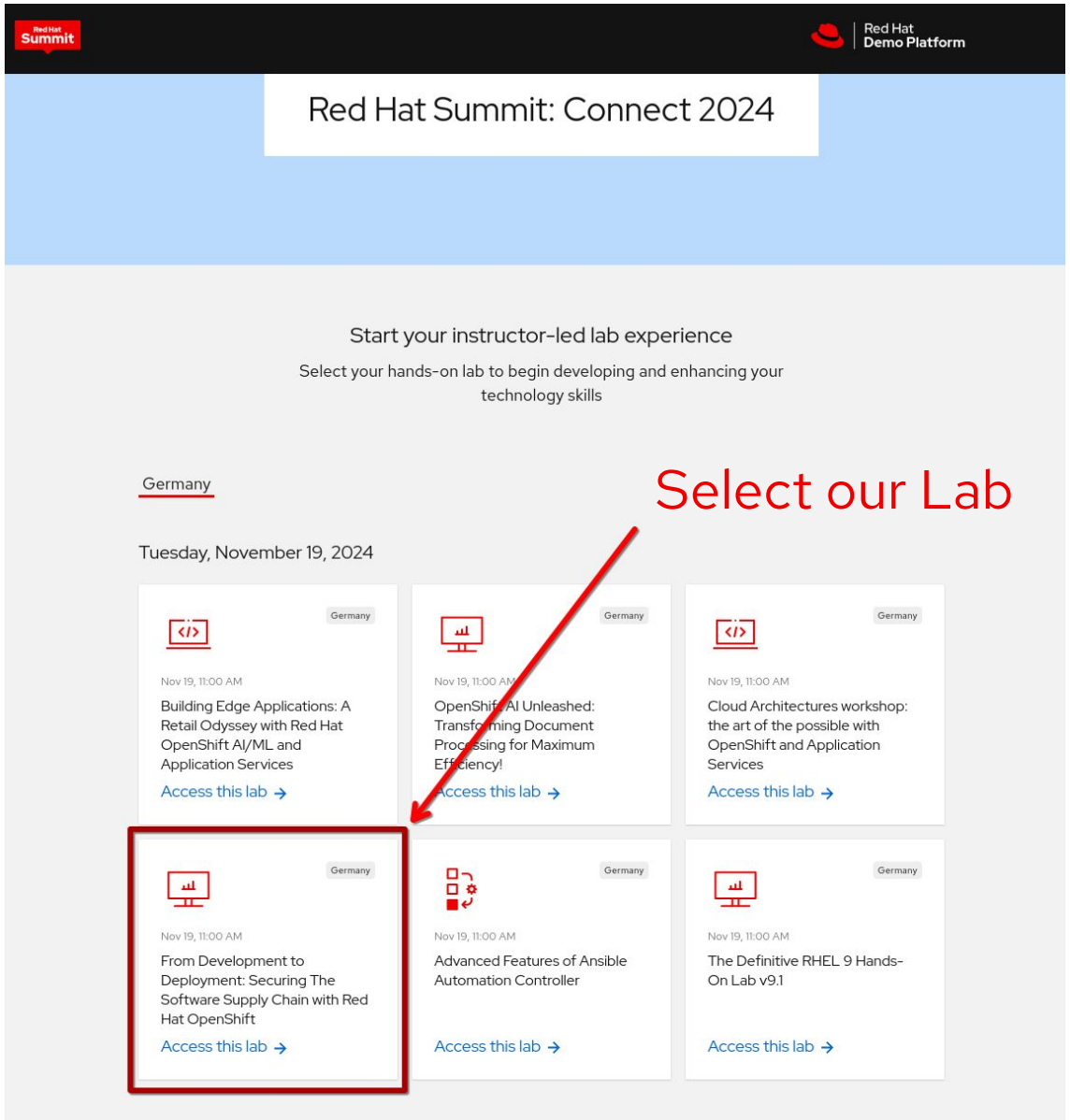
Red Hat Summit

Connect

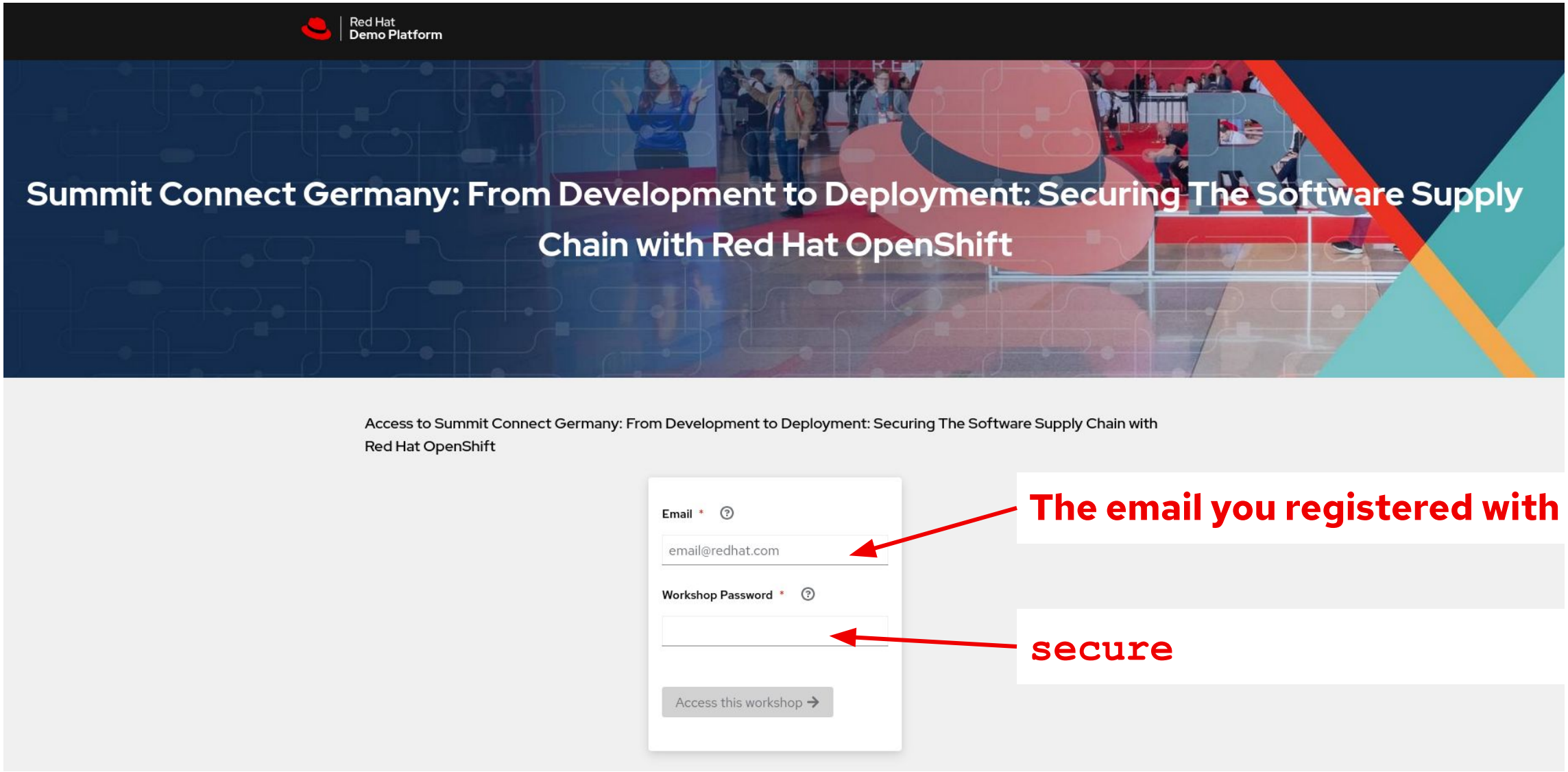
Launch ~~Firefox~~ Chrome and go to https://summit.demo.redhat.com

Red Hat

Supply Chain Security - OpenShift and Trusted Application Pipeline



Red Hat



Make sure you remember the (unique) e-mail address you used!

It will allow you to come back to your lab if you lose connection.

Lab Guide

self-paced

Red Hat Summit | AnsibleFest | Supercharge Developer Experience with Red Hat Developer ...

You can expand the TOC

Enhancing Security wi ne Workshop

Contents

This workshop focuses on the critical integration of security practices into the development and deployment processes using Red Hat OpenShift and a suite of Red Hat security tools. It highlights the necessity of embedding security early in the development lifecycle, known as "shifting left." It guides participants through hands-on activities that transition from non-secure to secure development pipelines.

Introduction to the Workshop

Welcome to an engaging session where integrating security into the development and deployment practices is discussed theoretically and applied practically. This workshop showcases the Red Hat Developer Hub (RHDH) and its significance in enhancing the developer experience through a centralized platform for resources, documentation, and tools.

Participants will journey through the transformation from a non-secure to a secure

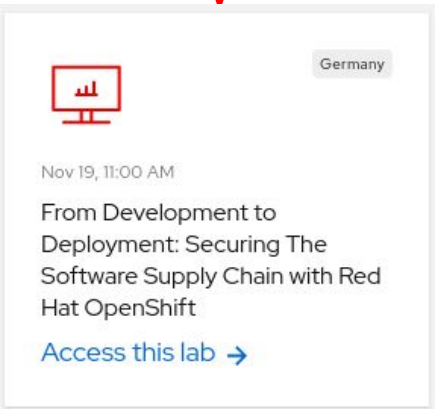
Terminals | Red Hat Demo Platform

```
Warning: Permanently added 'qa.cwzvz-1.sandbox1779.opentlc.com' (ED25519) to the list of known hosts.
Last login: Mon Nov 18 11:48:24 2024 from 3.22.215.43
[lab-user@qa ~]$
```

You can move the split screen

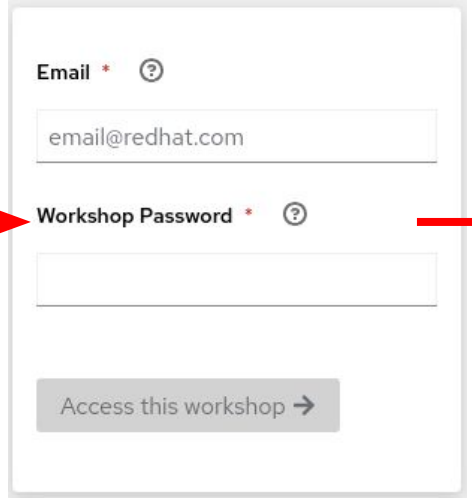
```
Warning: Permanently added 'qa.cwzvz-1.sandbox1779.opentlc.com' (ED25519) to the list of known hosts.
Last login: Mon Nov 18 11:58:24 2024 from 3.22.215.43
[lab-user@qa ~]$
```

https://summit.demo.redhat.com



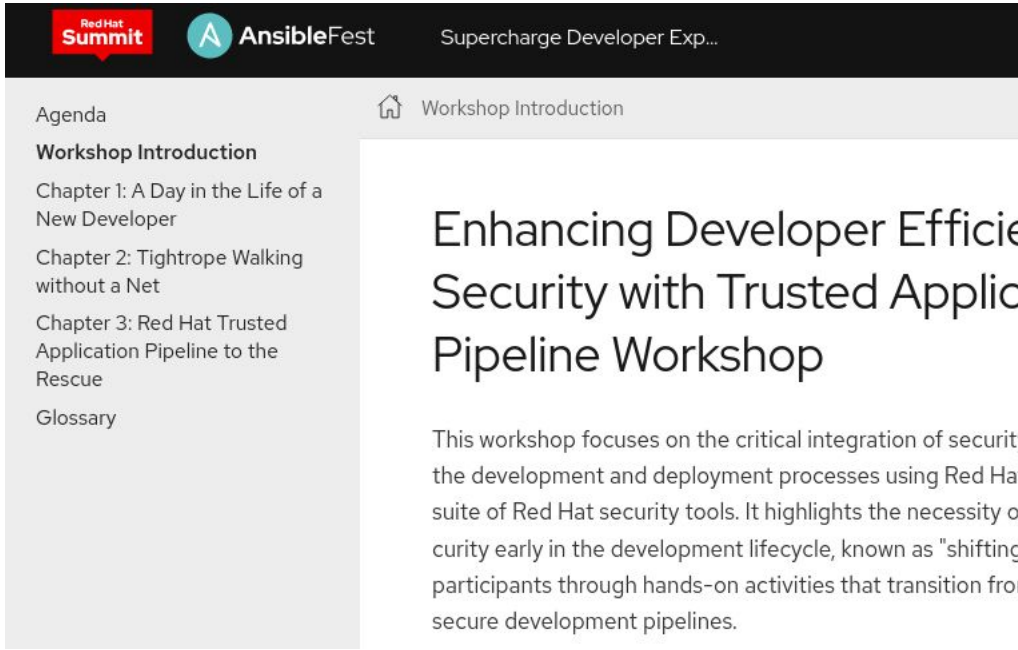
Select Lab

From Development to Deployment: Securing The Software Supply Chain with Red Hat OpenShift



Login with your email and the password:

secure



Follow the lab guide in your personalized "Showroom"

We're here to help, unstuck you and answer your questions

Red Hat

Red Hat Summit

Connect

Thank you

linkedin.com/company/red-hat

facebook.com/redhatinc

youtube.com/user/RedHatVideos

twitter.com/RedHat

Red Hat

Session: 15:50 - 16:20

Jetzt Session bewerten!

Einfach QR-Code scannen, Session wählen und bewerten.
Vielen Dank!

red.ht/rhsc24-de-s6

Red Hat