Software Supply Chain Security in Large Engineering Organizations

Rosalind Radcliffe

IBM Fellow, CIO DevSecOps CTO, AoT DevOps and SRE Co-Team Lead

Thomas Lawless

IBM Senior Technical Staff Member, CIO Developer Experience

IBM’s CIO organization runs the IT which runs IBM

Including HR, Sales, Supply Chain

12,000

IBMers
(6,000 Developers)

6,000

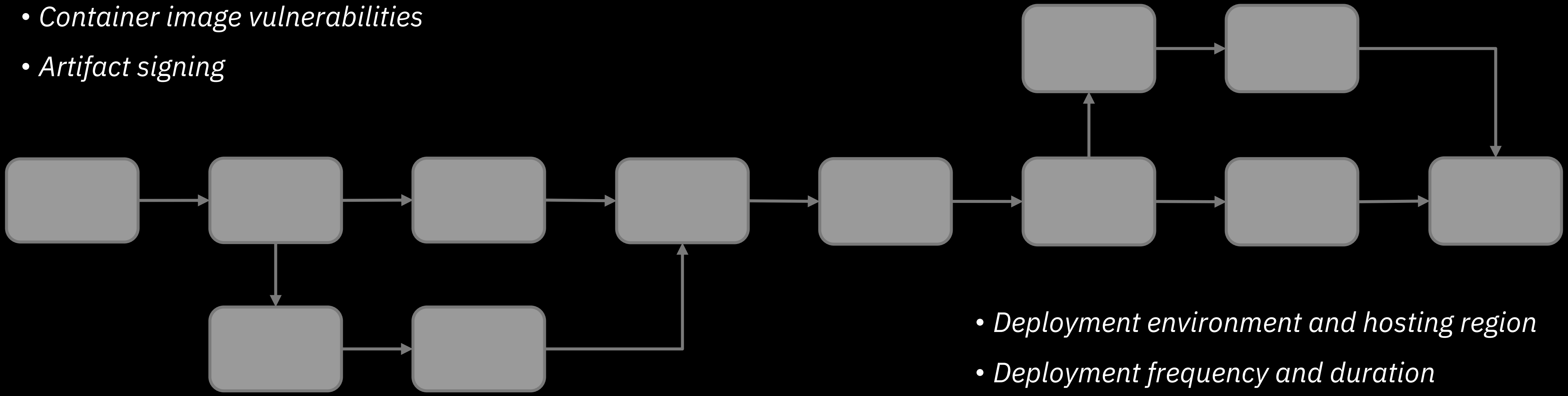
Applications,
& Services

70,000

GitHub Enterprise
Repositories

The Responsibility of all CI / CD Pipelines

- *Secrets and credentials detection*
- *Inventory of open-source libraries*
- *Open-source vulnerabilities*
- *Code quality and automated test coverage*
- *Static Application Security Testing vulnerabilities*
- *Container image vulnerabilities*
- *Artifact signing*



- *Deployment environment and hosting region*
- *Deployment frequency and duration*
- *Dynamic Application Security Testing vulnerabilities*
- *Production deployment approval auditing*

The log4j vulnerability in 4Q 2021 exposed issues with visibility into our source code repositories

Software Supply Chain Security

Automation enables developers to focus on writing high-quality, secure source code

The Automation Catalog

Creating an engineering culture of contribution

Pipeline Execution Management

Abstracting pipeline execution to minimize the uniqueness of our platforms

The Developer Data Lake

Providing insight into applications from source code to deployment

The Automation Catalog

Creating an engineering culture of contribution

Classification & Metadata

Management of assets which control how tasks, stages and pipelines are defined, classified and discovered within the catalog.

Publication

A standardized process to ensure the quality and secure of each automated task.

Discovery & Configuration

Ensuring automation is easy to find and consume based on the catalog's classification and metadata components.

Transformation

Transforming the catalog's definition of an automated task, stage and pipeline into the format of a pipeline execution engine.

Pipeline Execution Management

Abstracting pipeline execution to minimize the uniqueness of our platforms

Platform Integrations

Providing an extendable platform integrating with developer tools and services

Pipeline Execution Orchestration

A common mechanism of executing automation on various hosting environments and platforms

The Developer Data Lake

Providing insight into applications from source code to deployment

Data Aggregation

Retrieval and retention of data, metrics and evidence created during pipeline execution

Analytics & Reporting

Access to aggregated data for exploration and report generation

The Developer Portal

A tailored developer centric web experience based on aggregated data

Pipeline Gates

Automated policy enforcement based on aggregated data to ensure security and compliance

Thank you

Help we are looking for:

- *How do you provide the high-level visibility to security issues such as Log4j with your CI/CD approach?*

- *Do you have experiences with centralized management or standardization of CI/CD that you can share?*