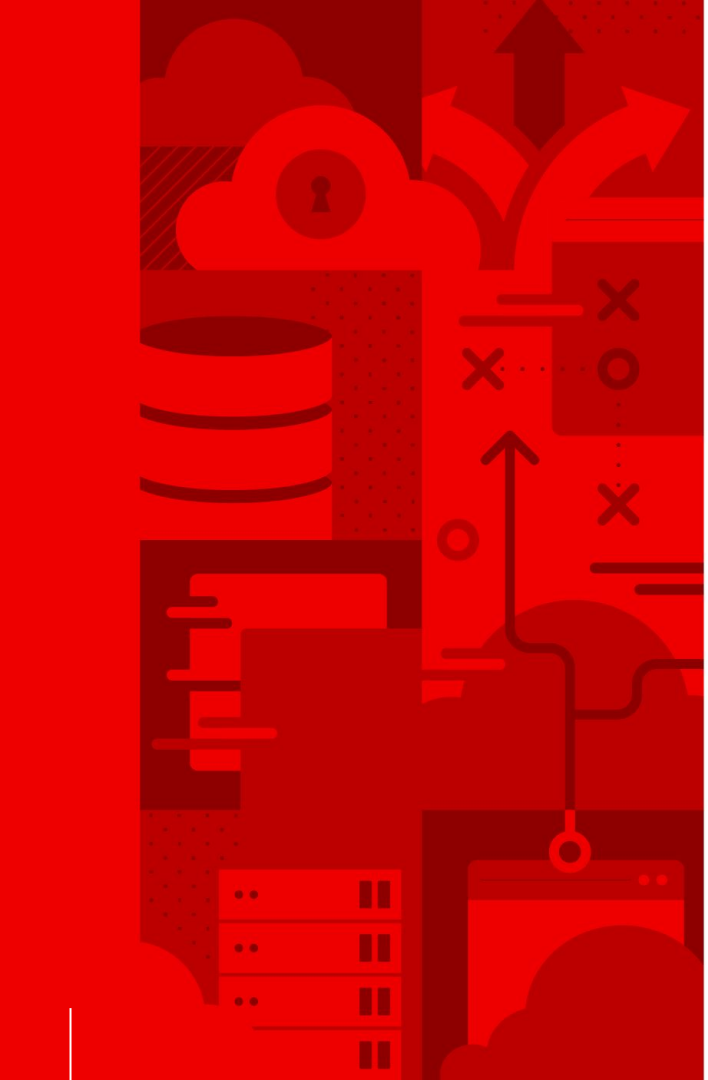


# Building Trust Through Proactive Security

- key parts of the trusted software supply chain

Przemyslaw “Rogue” Roguski

Principal Product Security Engineer

Red Hat
Product Security

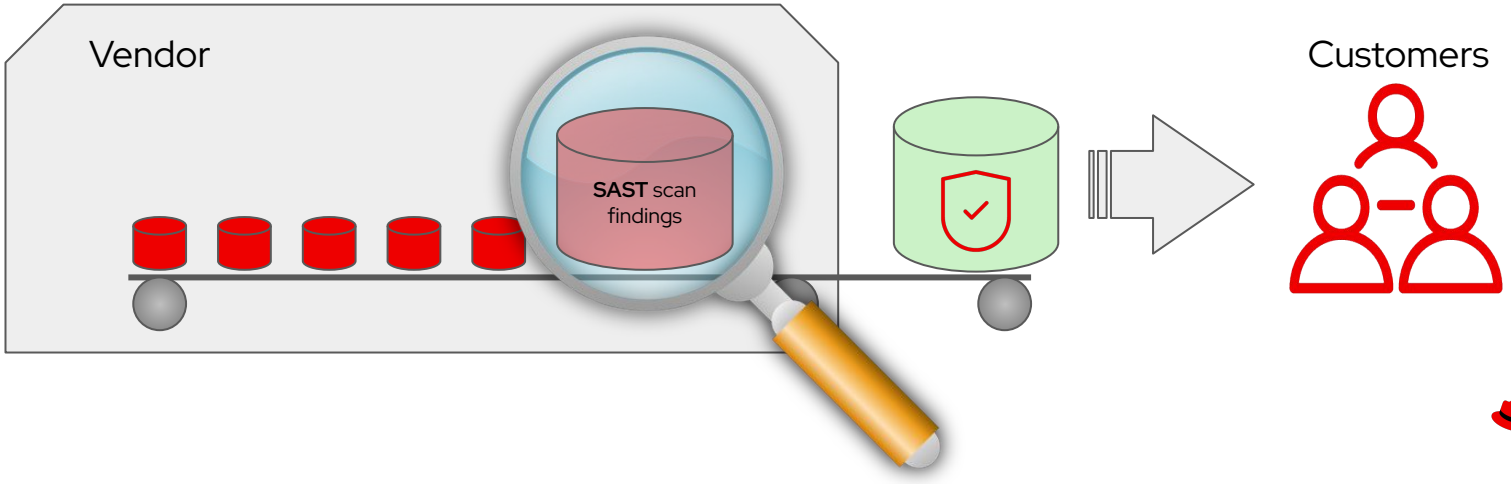
# What we'll discuss today

- Key difference between proactive and reactive security measures
- Secure Software Development Lifecycle (SDLC)
- Automated testing and open-source solutions
- Examples of proactive vulnerability management
- AI testing within the software supply chain security

## What does proactive work exactly mean?

All work you can do to verify the product/component before the release:

- SAST
- DAST
- Threat Modeling
- Malware/AV
- deep diff checks
- regression testing
- product metadata verification
- ...



# Secure Code Development & Architecture - what can be done to prevent security issue

Yesterday | Today | Tomorrow

## Vulnerability - response focus

- ★ Best-in-class incident response providing accurate and timely information
- ★ Go the extra mile to analyze flaws
- ★ Distribute patches securely

## Shift left approach

- ❑ Deep software testing and verification before release
- ❑ Data for quality security information and automation
- ❑ Build and deliver software securely
- ❑ Influence standards bodies and emerging standards
- ❑ Industry understands risk-based security, no more “security theatre”

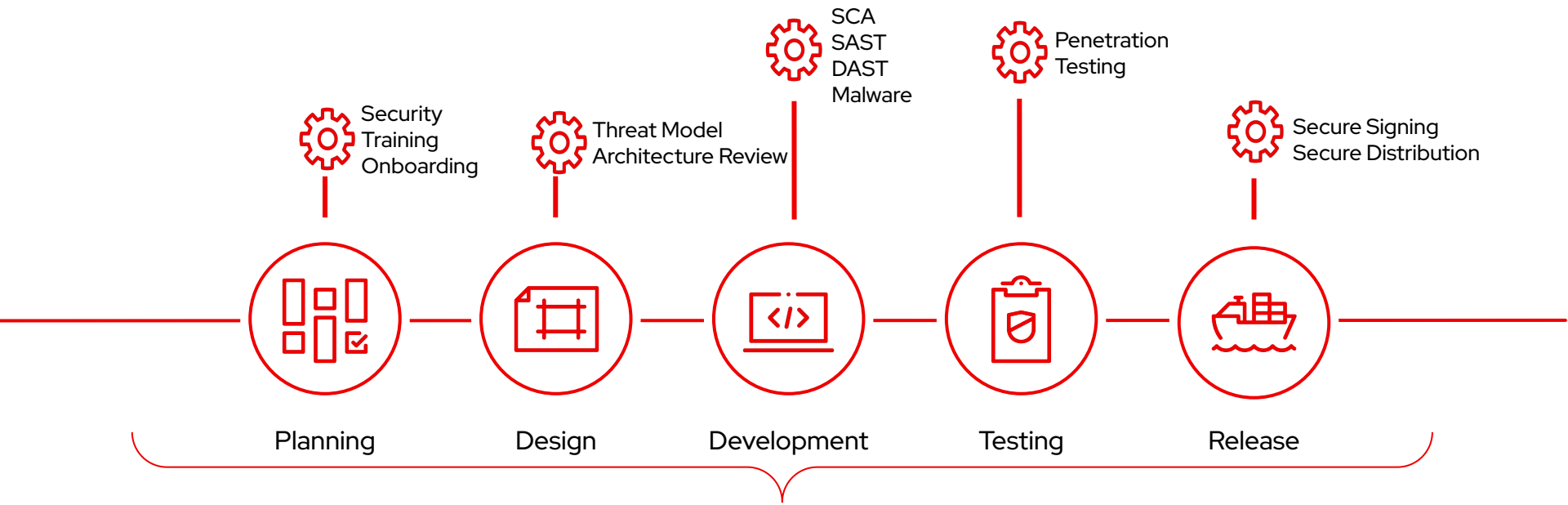
## More precise and automated testing

- ➔ Automated gating based on security findings in case not compliance results
- ➔ Contextual SBOMs
- ➔ Precise weaknesses identification and remediation
- ➔ AI based testing within software supply chain security

*"Rarely is anyone thanked for the work they did to prevent the disaster that didn't happen."*

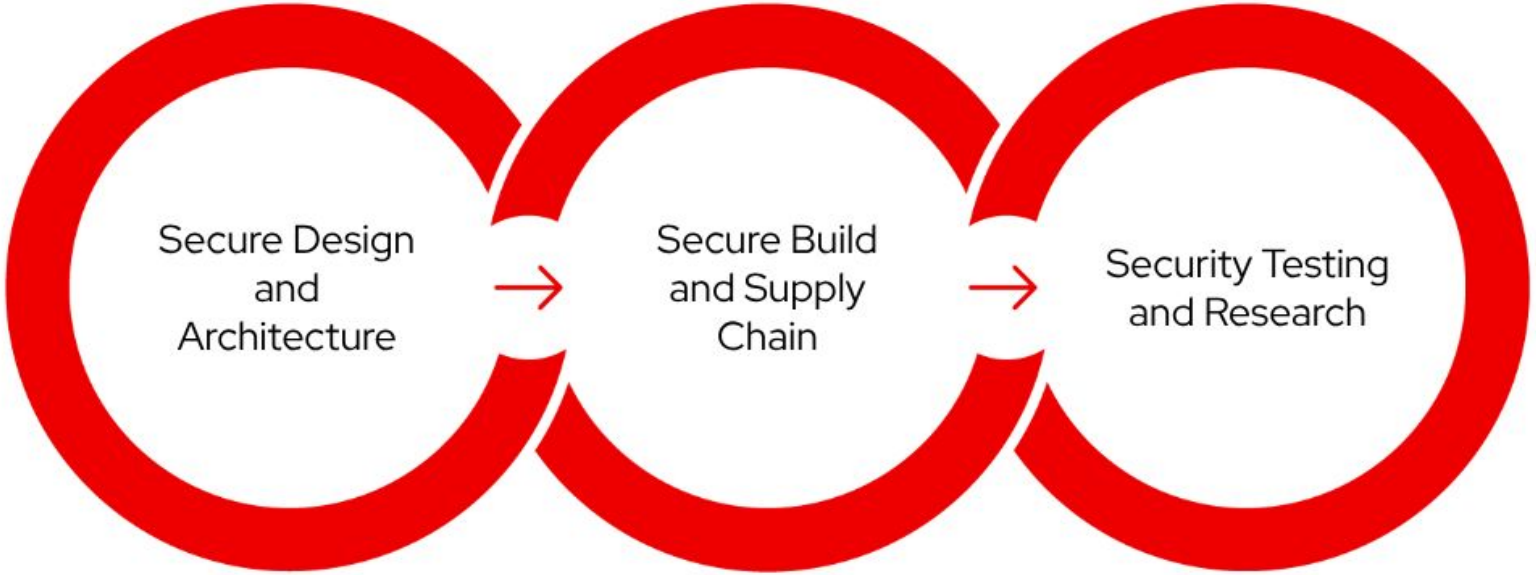
– Mikko Hypponen

# Testing during Red Hat's Software Development Lifecycle

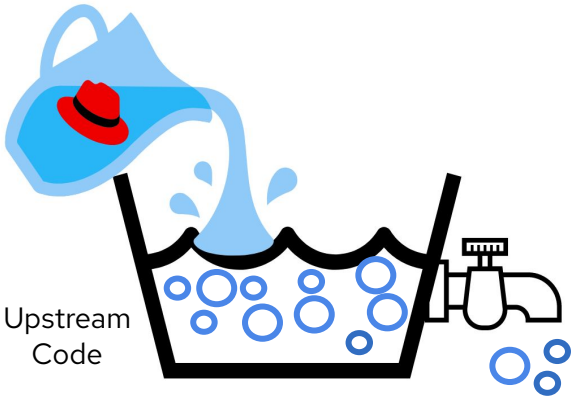



Test for the right things in the right place

Security built in rather than bolted on.



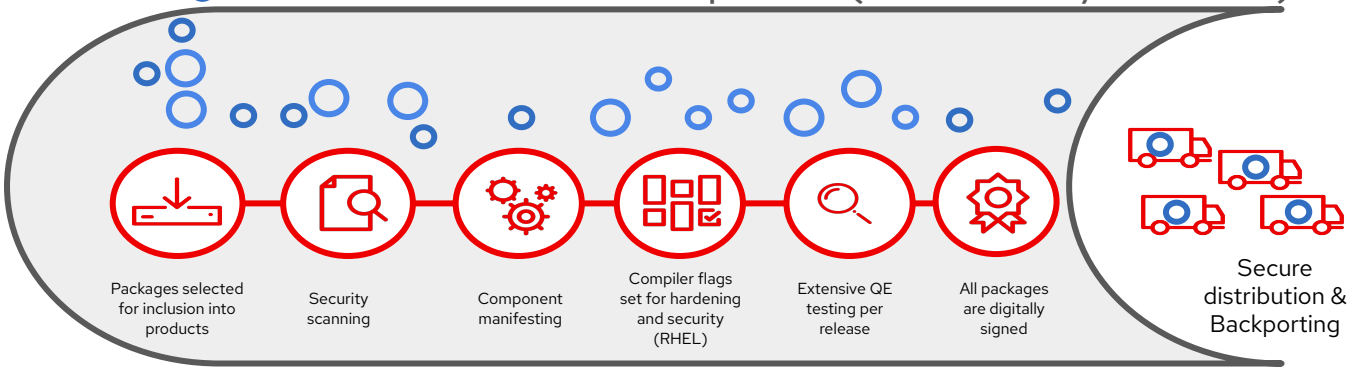
# Red Hat's Software Supply Chain




Red Hat Trusted Application Pipeline

KONFLUX

## Red Hat Product Pipeline (ie. RHTAP / Konflux)




Trusted & Patched Build Systems | Logged Pipeline Actions | Best IDM Practices | Encryption | CIS Standards

**Pipeline Hardening**

Red Hat Product Security

Konflux is an open source, cloud-native software **build**, **test** and **release** factory based on Tekton, built around software supply chain security. It is a comprehensive solution (one robust pipeline), that fortifies software supply chain against various threats, allowing precise tracking what and how software is built and validate if build meets various security requirements.

KONFLUX

### Build

Build artifacts of all kinds from source. Enable hermetic builds and produce accurate SBOMs.

### Securely Sign

Generate secure & detailed provenance, an immutable record of what happened during each and every build step.

### Identify Vulnerabilities

Catch critical vulnerabilities quickly with each pull request.

### Supply Chain Safeguards

Verify container images against major secure software frameworks or your own custom rules.

### SCM Integration

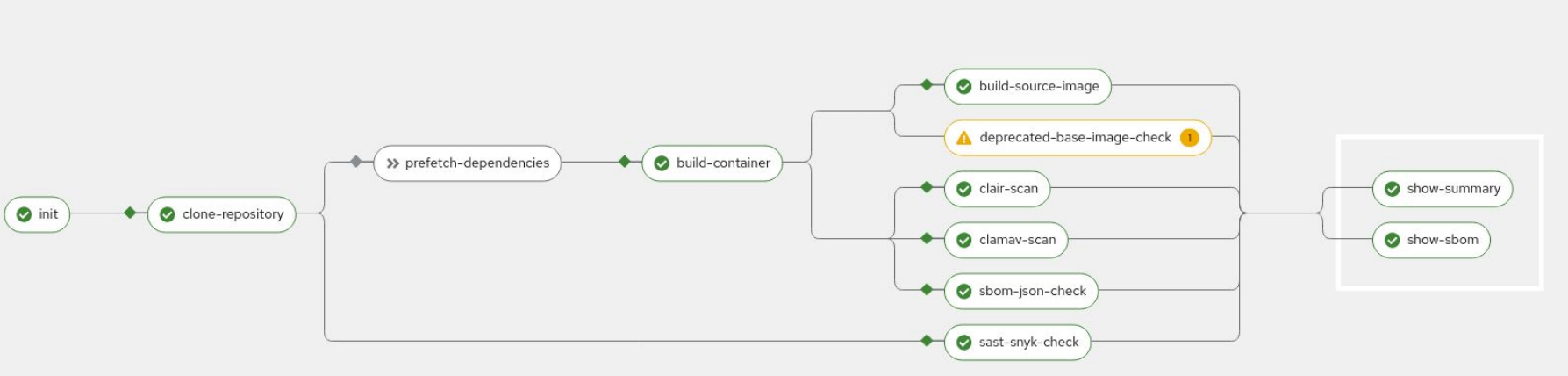
Build in response to git events, post results of builds and tests back to your Pull or Merge requests

### Integration Tests

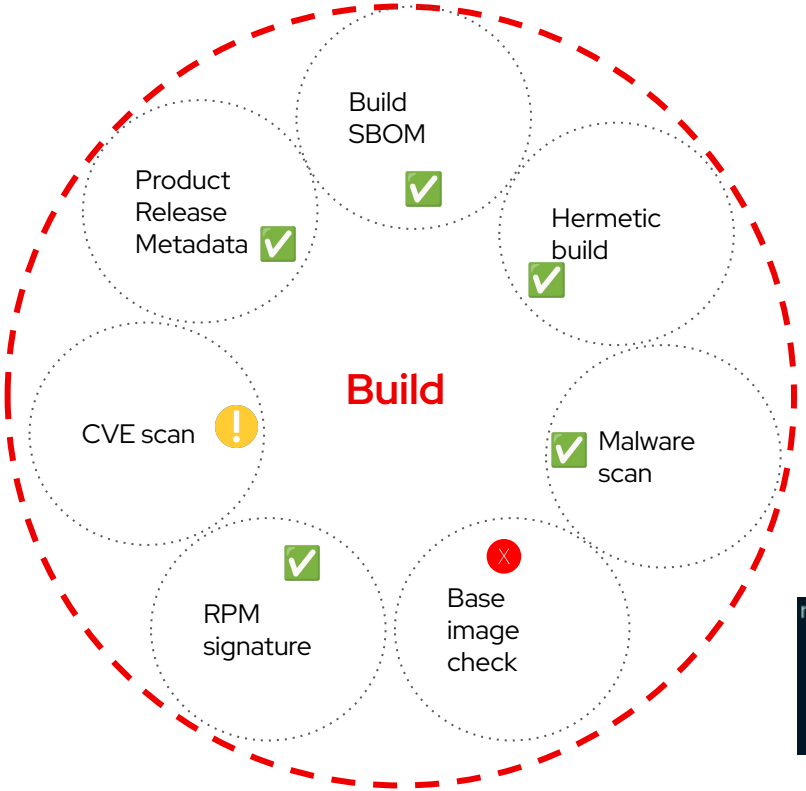
Execute integration tests for complex applications and see results in your SCM.

**Every task** in the pipeline is executed in a controlled way and produce provenance data. We use Tekton Chains, together with Conforma (formerly Enterprise Contract or EC), to determine if an artifact meets the required policy.

KONFLUX



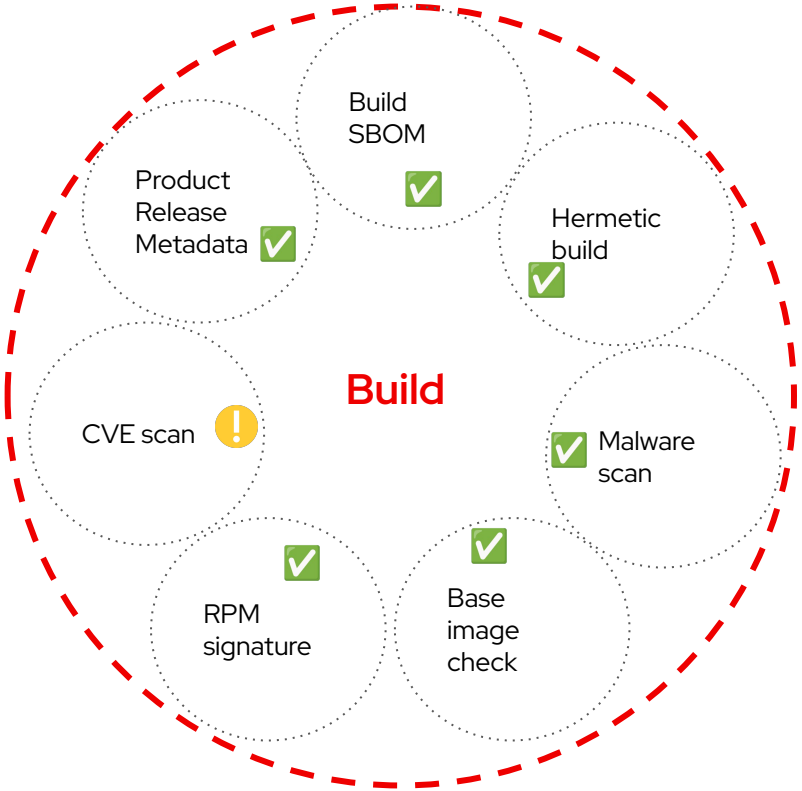

Red Hat
Product Security




conforma

*verify artifacts, enforce policies*

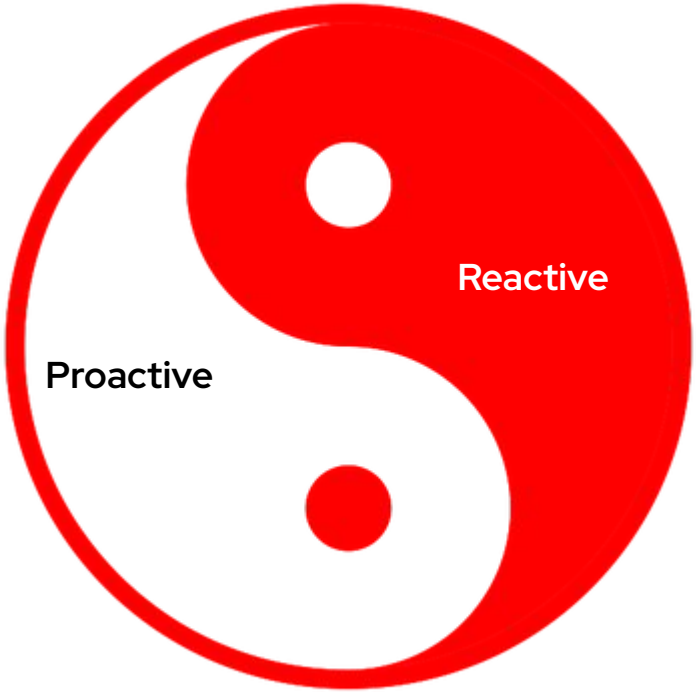
```
ruleData:
  rule_data_custom:
    allowed_registry_prefixes:
      - trusted-registry.io/trusted-images/
```



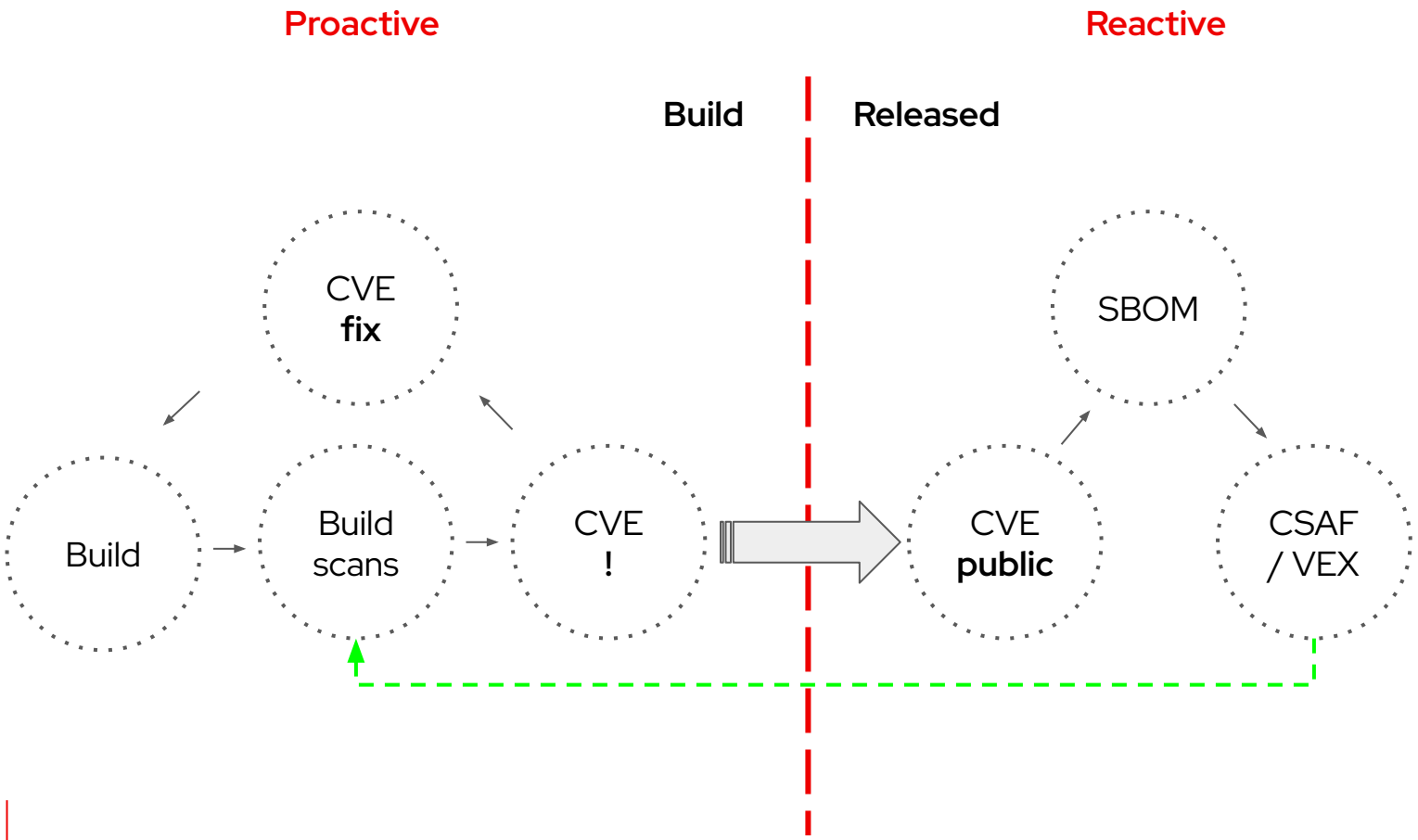

conforma

*verify artifacts, enforce policies*

Vulnerability detection Alert
(not blocking rule)




How can it be achieved ? ...


Proactive
Reactive
Build
Released
CVE
fix
SBOM
Build
Build
scans
CVE
!
CVE
public
CSAF
/ VEX

## Today:

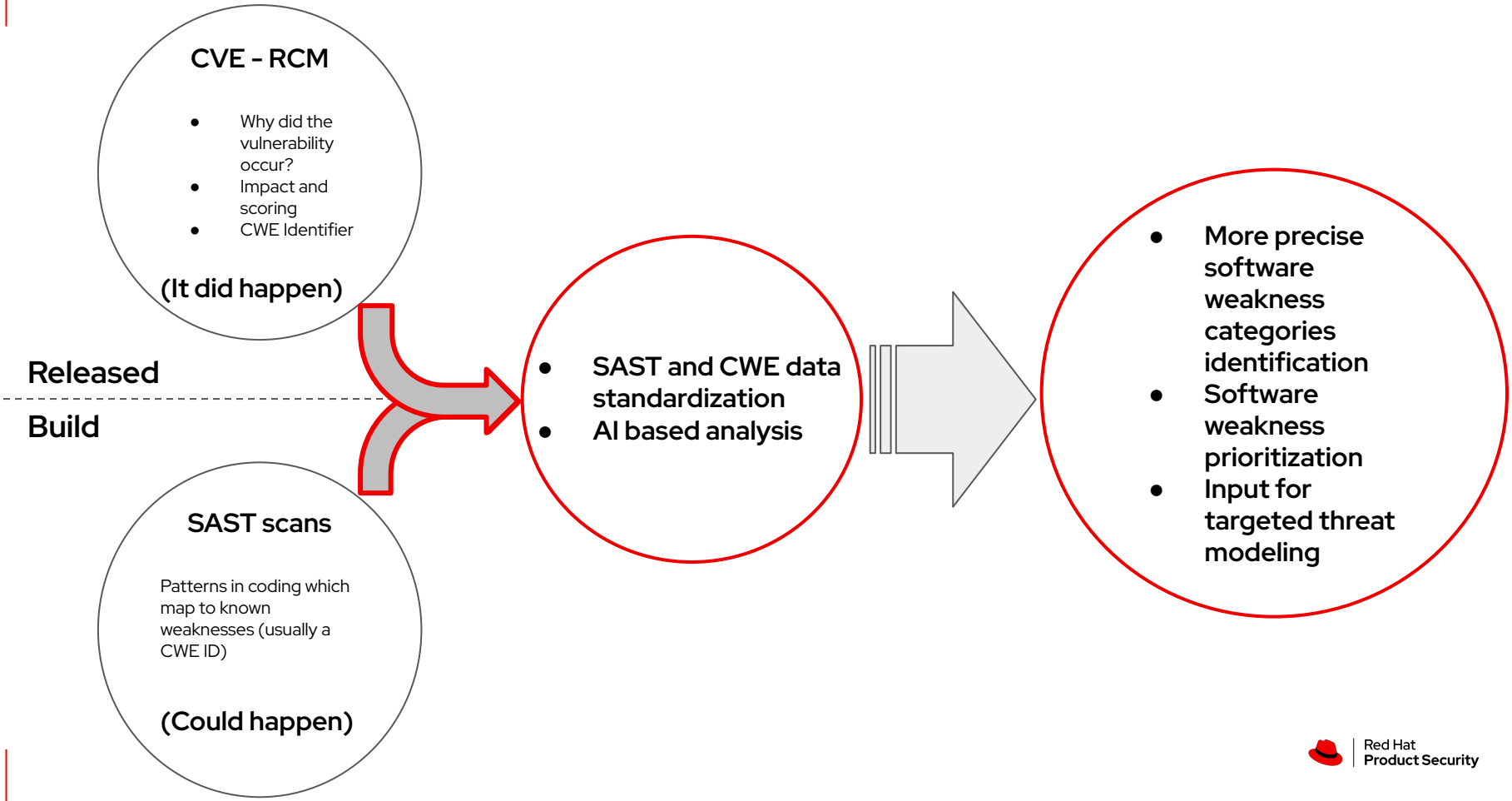
- SAST scanning results contain a lot of false positive findings
- processing all automatically triggered SAST results is:
  - time consuming
  - not efficient

## What next:

SAST scanning findings improved by CWE data from the CVE records could help to identify the most important software weaknesses and potentially avoid flaws in the future.

## Benefits:

- Reduce the Engineering time spent on patch production and release process
- Reduce the number of reported CVEs against Red Hat portfolio
- Improve the customer experience by showing that Red Hat products are secure by default.

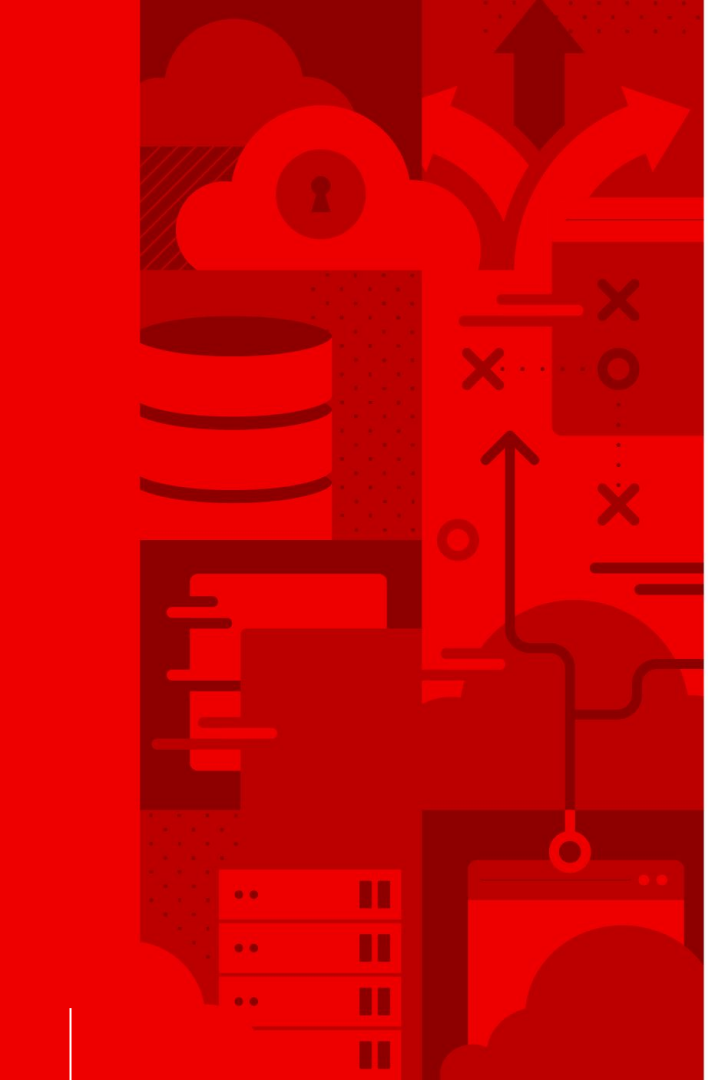

CVE - RCM
Why did the vulnerability occur?
Impact and scoring
CWE Identifier
(It did happen)
Released
Build
SAST scans
Patterns in coding which map to known weaknesses (usually a CWE ID)
(Could happen)
SAST and CWE data standardization
AI based analysis
More precise software weakness categories identification
Software weakness prioritization
Input for targeted threat modeling

## SAST results

| SAST CWE List: | CWE Category |
|---|---|
| 755 | ? |
| 778 | Audit / Logging Errors |
| 284 | Authorization Errors |
| 561 | Bad Coding Practices |
| 688 | Bad Coding Practices |
| 79 | Data Neutralization Issues |
| 252 | Error Conditions, Return Values, Status Codes |
| 394 | Error Conditions, Return Values, Status Codes |
| 319 | Information Management Errors |
| 200 | Information Management Errors |
| 401 | Memory Buffer Errors |
| 476 | Pointer Issues |
| 269 | Privilege Issues |
| 398 | THIS IS CATEGORY |

## CWE data from CVE records

| CVE | CWE | Mapped CWE Category | CVE Severity |
|---|---|---|---|
| CVE-2024-8676 | CWE-285 | Authorization Errors | **Moderate** |
| CVE-2024-24786 | CWE-835 | Behavioral Problems | |
| CVE-2024-24790 | CWE-115 | Behavioral Problems | |
| CVE-2024-3727 | CWE-354 | Data Integrity Issues | |
| CVE-2024-3154 | CWE-77 | Data Neutralization Issues | **Important** |
| CVE-2024-28180 | CWE-409 | Data Processing Errors | |
| CVE-2024-5154 | CWE-22 | File Handling Issues | |
| CVE-2024-9341 | CWE-59 | File Handling Issues | |
| CVE-2024-9676 | CWE-22 | File Handling Issues | |
| CVE-2024-1394 | CWE-401 | Memory Buffer Errors | **Important** |
| CVE-2024-24783 | CWE-400 | Resource Management Errors | |



# Q&A

linkedin.com/company/red-hat

facebook.com/redhatinc

youtube.com/user/RedHatVideos

twitter.com/RedHat

Red Hat
Product Security