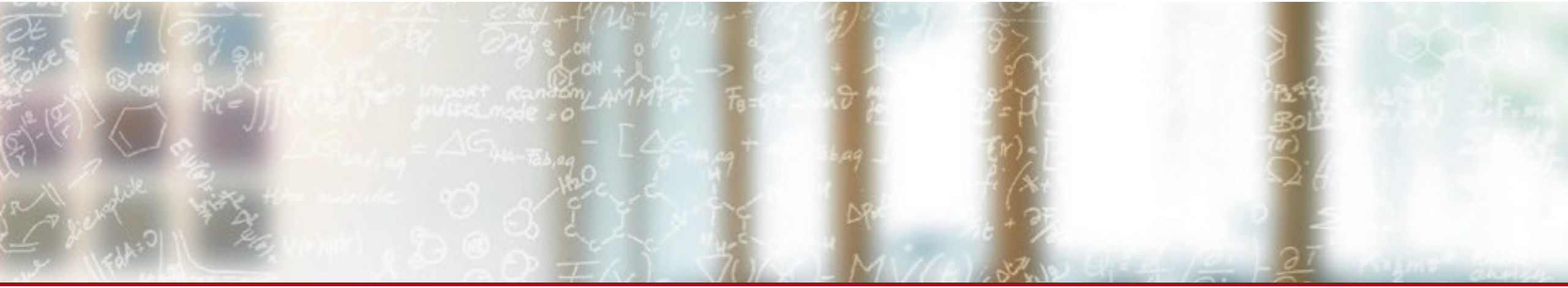
CSCS
Centro Svizzero di Calcolo Scientifico
Swiss National Supercomputing Centre

ETH zürich



Experimenting With Security Compliance Checking Using ReFrame

Victor Holanda Rusu, Matteo Basso, Chris Gamboni, Fabio Zambrino, and Massimo Benini, CSCS

May 6th, 2025

Computing Horizons: CUG 2025

Implementing DevSecOps in HPC

Because Regular HPC Wasn't Hard Enough

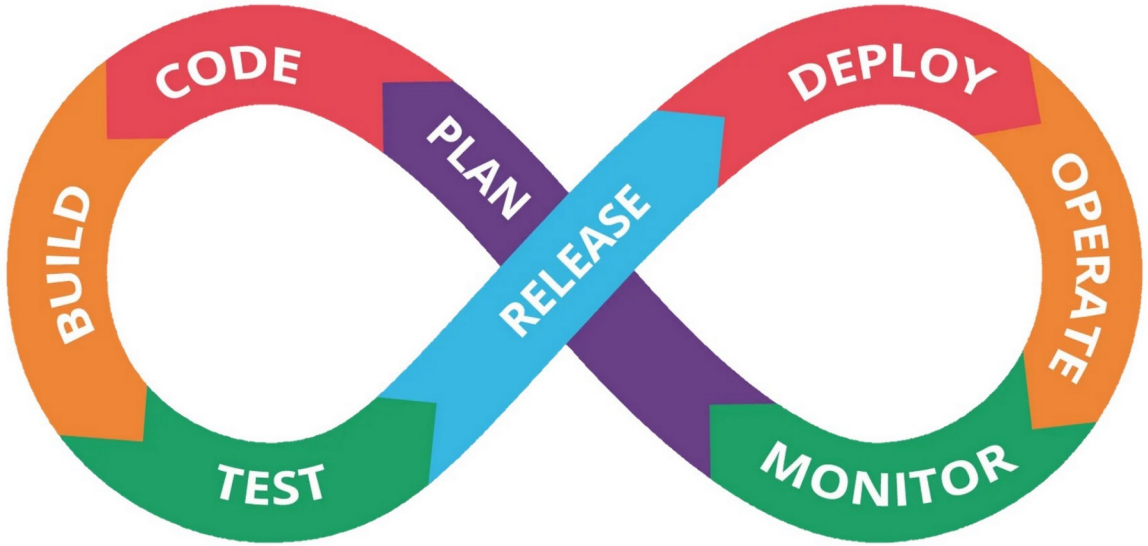
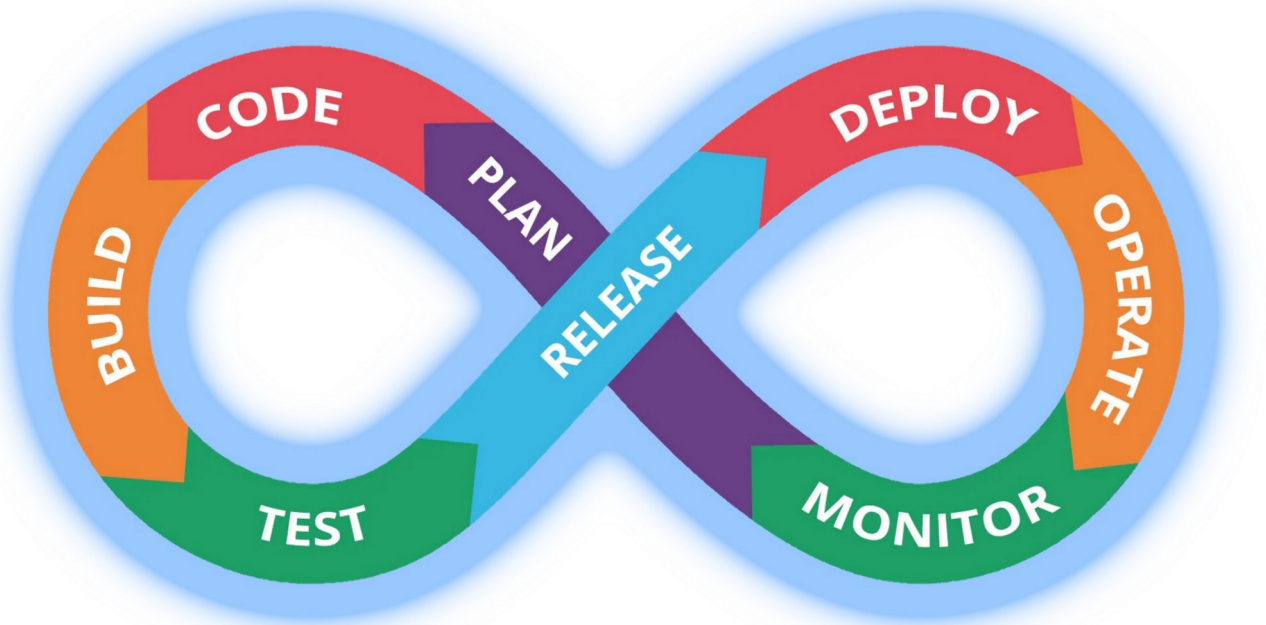


Image from https://mia-platform.eu/blog/devops/

Implementing DevSecOps in HPC

It’s Fine, Everything is Fine

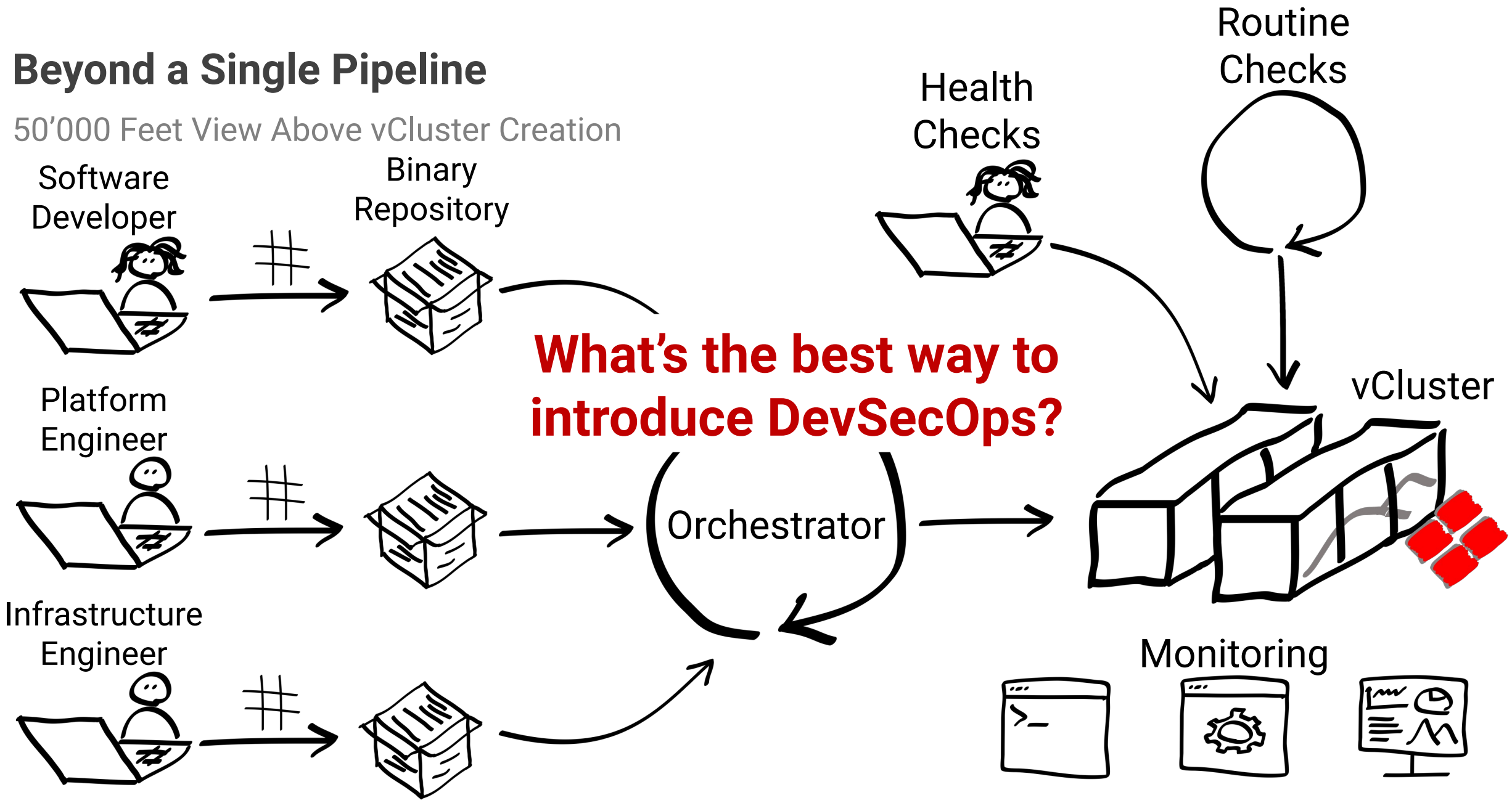


Modified from https://mia-platform.eu/blog/devops/

DevSecOps in HPC: It’s Not Just One Pipeline; It’s a Whole Lot More

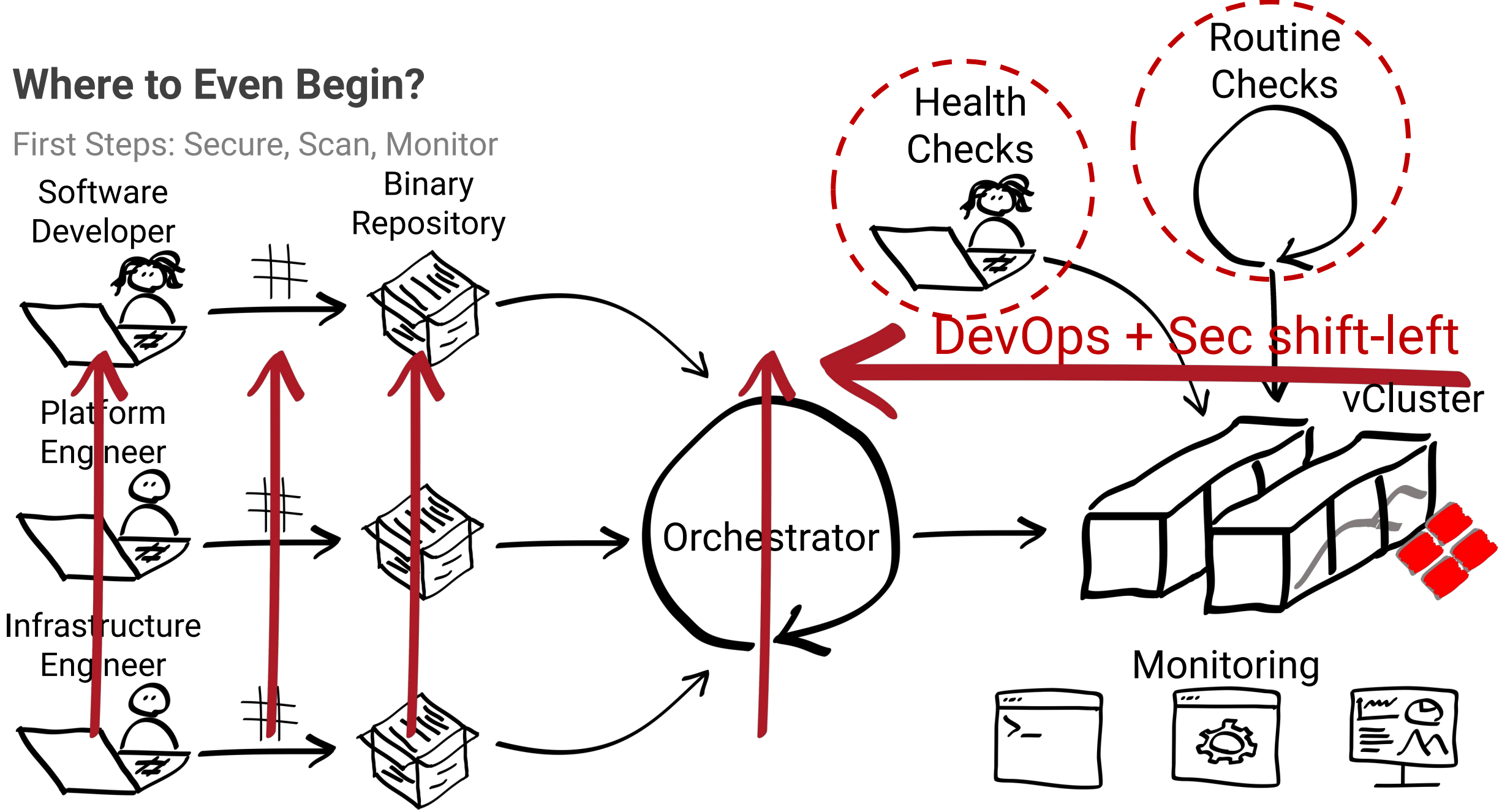
Beyond a Single Pipeline

50’000 Feet View Above vCluster Creation



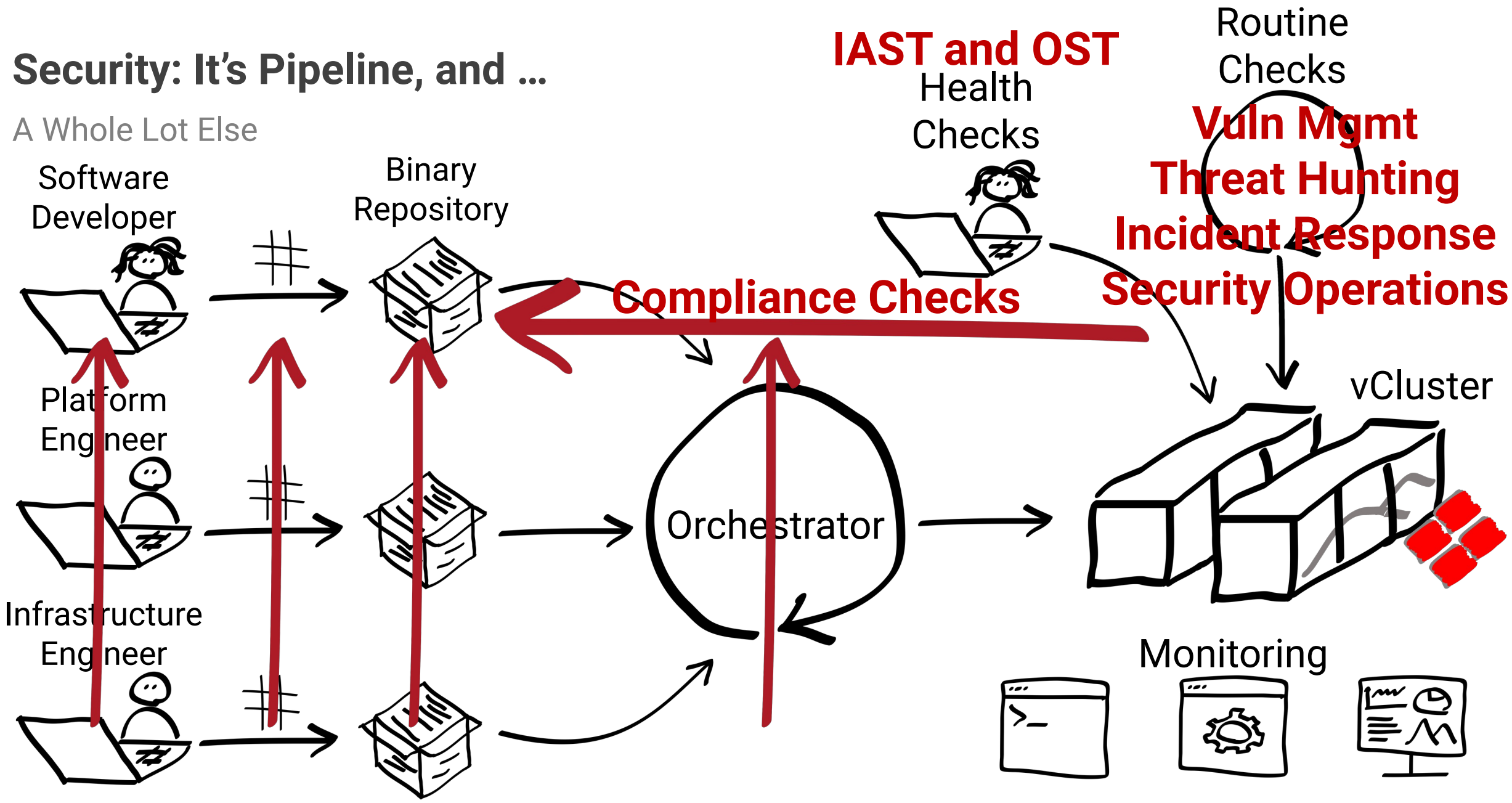
Where to Even Begin?

First Steps: Secure, Scan, Monitor



Security: It's Pipeline, and …

A Whole Lot Else



What Is Security Compliance Testing?

The Art of Checking All the Boxes (And Then Some)

- Viewed as a “Security Theatre” activity by many
- Checks conformity to standards and policies
  - Ensures a system or application adheres to predefined security requirements, e.g., DISA STIGs, ANSSI BP, ISO 27001
- Detects misconfigurations and potential vulnerabilities
- Provides measurable and reportable results
- Is mainly automatable
- Can be used as a baseline to start implementing hardened configurations
- Can be used as Indicators of Compromise

Security Compliance Testing in Practice

Where Theory Meets Reality (and It's Complicated)

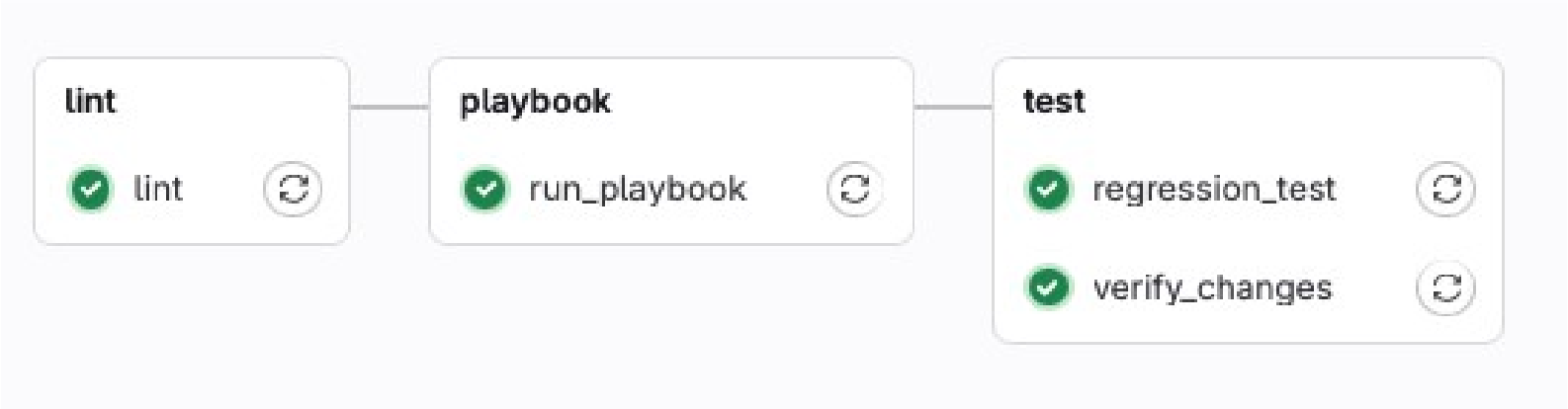
- We use Security-focused tools, vendor provided and difficult to customize
- Our hardening verification is OSCAP* centric
  - OSCAP is the industry standard in security
  - CSCS engineers are not necessarily used to them
- Support for different OSes varies
  - The security team needs to write customization
  - A bunch of additional bash scripts
- Reporting is not integrated with monitoring

*OSCAP stands for Open Security Content Automation Protocol

What a Simple Ansible CI Pipeline Looks Like?

On a Good Day

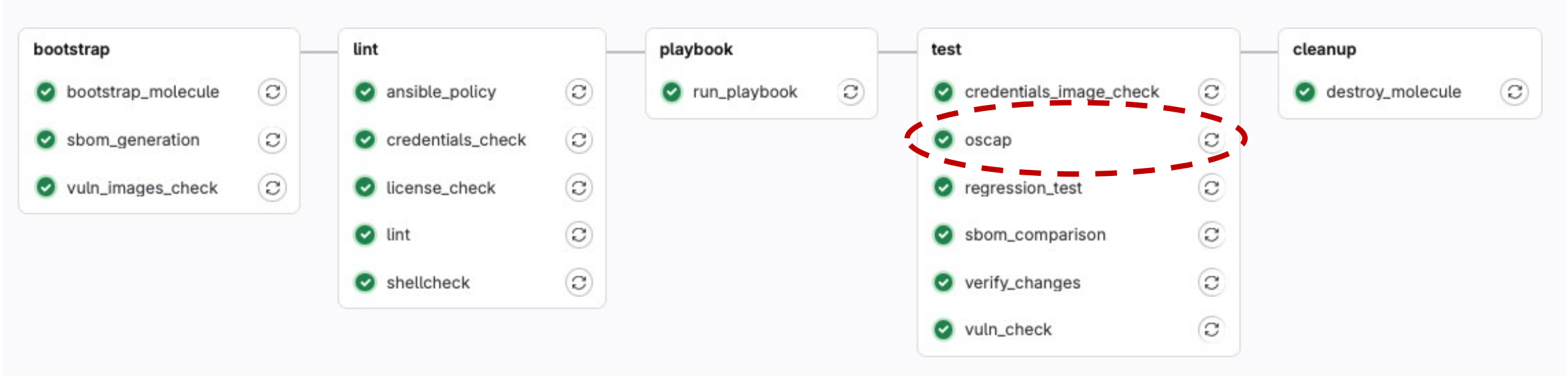
- This is a 4 jobs pipeline



DevSecOps Ansible CI Pipeline

Now with 4x the Complexity (and 5x the YAML)

- This is a 16 jobs pipeline
- Engineer owns the pipeline
- Tools must be configurable – focus on silencing false positives



How does a OSCAP Test Look Like?

Peeking Under the Hood: How OSCAP Writes Tests

```
<Rule id="xccdf_org.ssgproject.content_rule_file_groupowner_etc_passwd">
  <title>Ensure group ownership of /etc/passwd file is root</title>
  <description>
    The /etc/passwd file should be group-owned by root to prevent
    unauthorized users from obtaining sensitive information.
  </description>
  <check system="urn:xccdf:check:system:ocil">
    <check-content-ref href="checks/ocil/file_groupowner_etc_passwd.xml" />
  </check>
  <fix system="urn:xccdf:fix:system:ansible">
    <fix-content-ref name="fix_file_groupowner_etc_passwd_ansible"/>
  </fix>
</Rule>
```

How does a OCIL* Questionnaire Look Like?

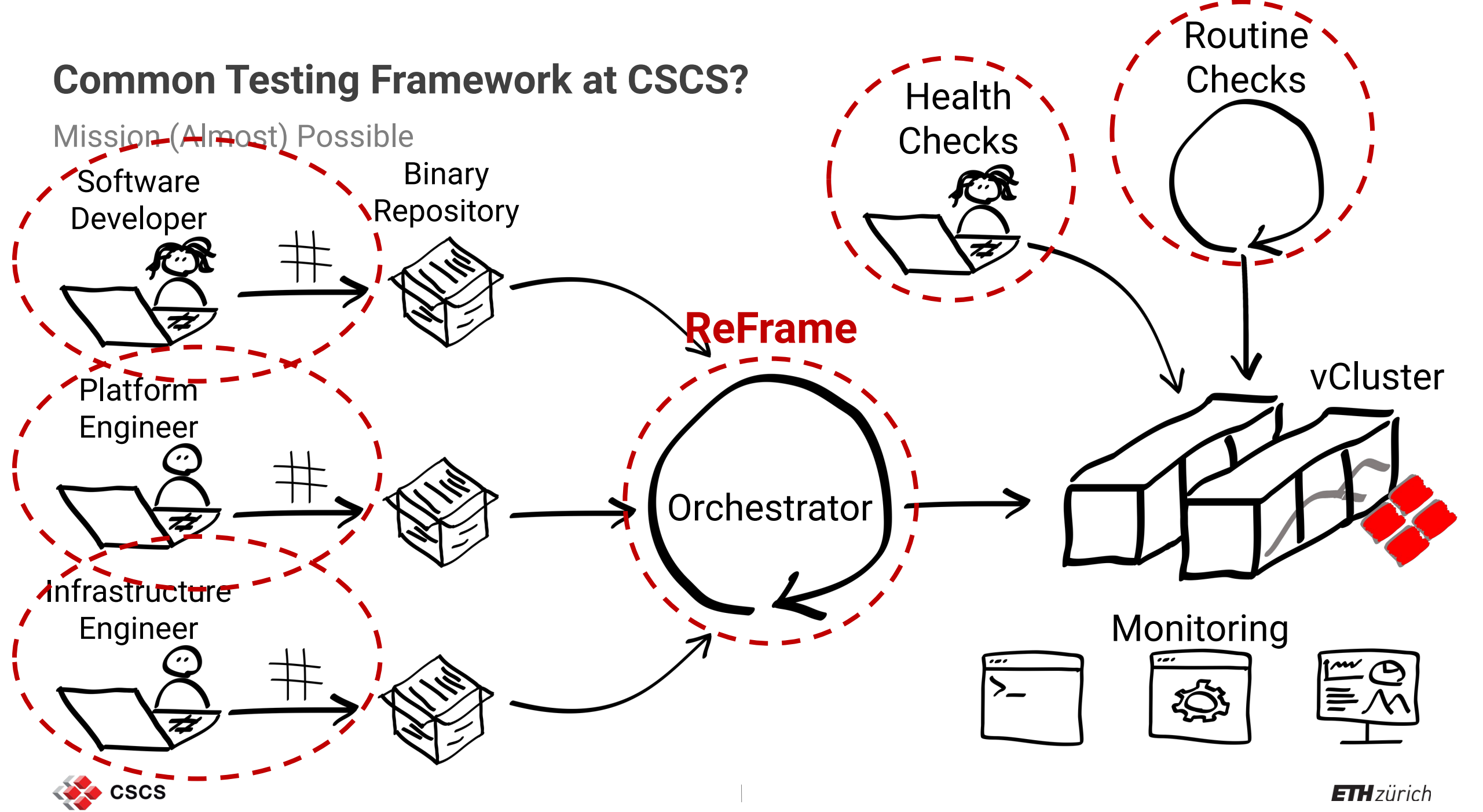
Peeking Into the World of OCIL (Yes, it's XML Again)

```
<ocil:questionnaire id="file_groupowner_etc_passwd_questionnaire">
  <ocil:question id="file_groupowner_etc_passwd_question">
    Is the group owner of the /etc/passwd file set to 'root'?
  </ocil:question>
  <ocil:action id="file_groupowner_etc_passwd_action">
    To verify the group ownership of the /etc/passwd file, run the
following command:
    <ocil:command>stat -c "%G" /etc/passwd</ocil:command>
    The output should be:
    <ocil:command_output>root</ocil:command_output>
    If the group owner is not 'root', this is a finding.
  </ocil:action>
</ocil:questionnaire>
```

*OCIL stands for Open Checklist Interactive Language

Common Testing Framework at CSCS?

Mission (Almost) Possible



ReFrame Tests: When Less Really Is More

An Engineering Perspective

```
@rfm.simple_test
class file_groupowner_etc_passwd_check(seccommon.file_perms_check):
    paths = parameter([{'/etc/passwd' : {'group' : 'root'}}])
```

Security Compliance in ReFrame

Code Hiding in a Sea of Explanations

```
@rfm.simple_test
class file_groupowner_etc_passwd_check(seccommon.file_perms_check):
    paths = parameter([{'/etc/passwd' : {'group' : 'root'}}])
    descr = 'Ensure group ownership of /etc/passwd file is root'
    rationale = variable(str, value='The /etc/passwd file contains …')
    severity = variable(str, value='medium')
    correction = variable(str, value='automated')
    tags |= {'isa-62443-2009', 'cis@sle15', 'iso27001-2013', 'cce@sle15'…}
```

Annotation Required by Compliance

A Real Engineer's ReFrame Test

One Class, All the Things

```
@rfm.simple_test
class file_perms_etc_passwd_check(seccommon.file_perms_check):
    paths = parameter([{'/etc/passwd' : {'group' : 'root'}},
                       {'/etc/passwd' : {'owner' : 'root'}},
                       {'/etc/passwd' : {'perm'  : '0644'}},])
or

@rfm.simple_test
class file_perms_etc_passwd_check(seccommon.file_perms_check):
    paths = parameter([{'/etc/passwd' : {'group' : 'root',
                                         'owner' : 'root',
                                         'perm ' : '0644'}}])
```

Our Achievements

Proof We Were Busy (Mostly)

- Ported ComplianceAsCode project checks into ReFrame
- Focused on DISA STIG, ANSSI-BP-28 enhanced, and CSCS custom standards and policies
- Created a custom OSCAP-like report generator
- We have +1200 security compliance checks
- We support SUSE and RedHat
- Labelled the tests, to support conditional execution
- Integration with our Monitoring

The Results Are In…

Our Very Own OSCAP-ish Report

System Health Check

System: MyInsecureVM

Summary | Check Results | Disclaimer

Security Tests Profile

MyInsecureVM	root	290.2 s	4.7.4	2025-04-21 09:02:04
Hostname	User	Execution Time	Reframe Version	Execution Date

Test Execution Summary

965 100%	0 0.0%	429 44.5%	164 17.0%	372 38.5%
Total	Aborted	Failure	Skipped	Success

The Results Are In...

Our Very Own OSCAP-ish Report

Failure sudo_add_noexec_check

Status
Failure

Description
The sudo NOEXEC tag, when specified, prevents user executed commands from executing other commands, like a shell for example. This should be enabled by making sure that the NOEXEC tag exists in /etc/sudoers configuration file or any sudo configuration snippets in /etc/sudoers.d/.

Rationale
Restricting the capability of sudo allowed commands to execute sub-commands prevents users from running programs with privileges they wouldn't have otherwise.

Tags
anssi

Execution time
1.1 s

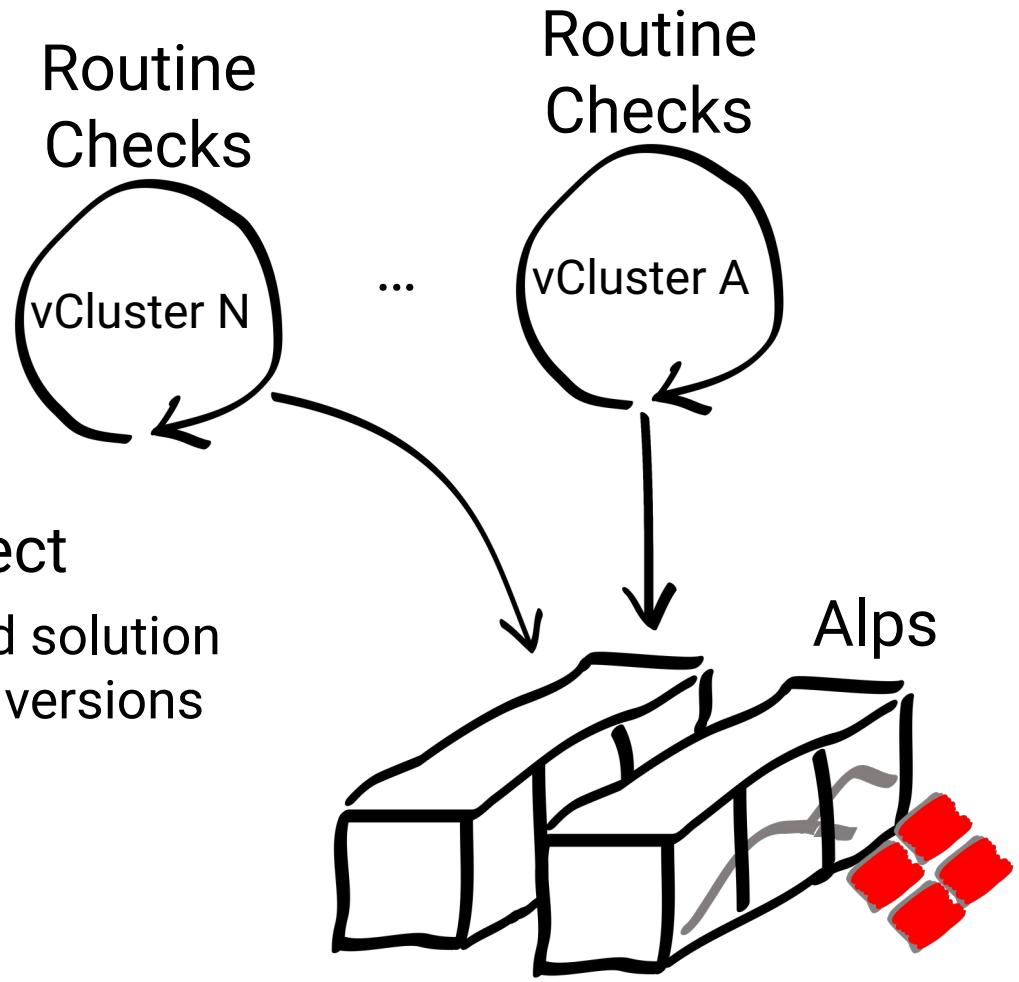
Failed Reason
▾ Display toggle ...

```
sanity error:
Defaults noexec not found in /etc/sudoers
```

Check bash script
▸ Display toggle ...

Work in Progress

Because We Are Not Done Yet

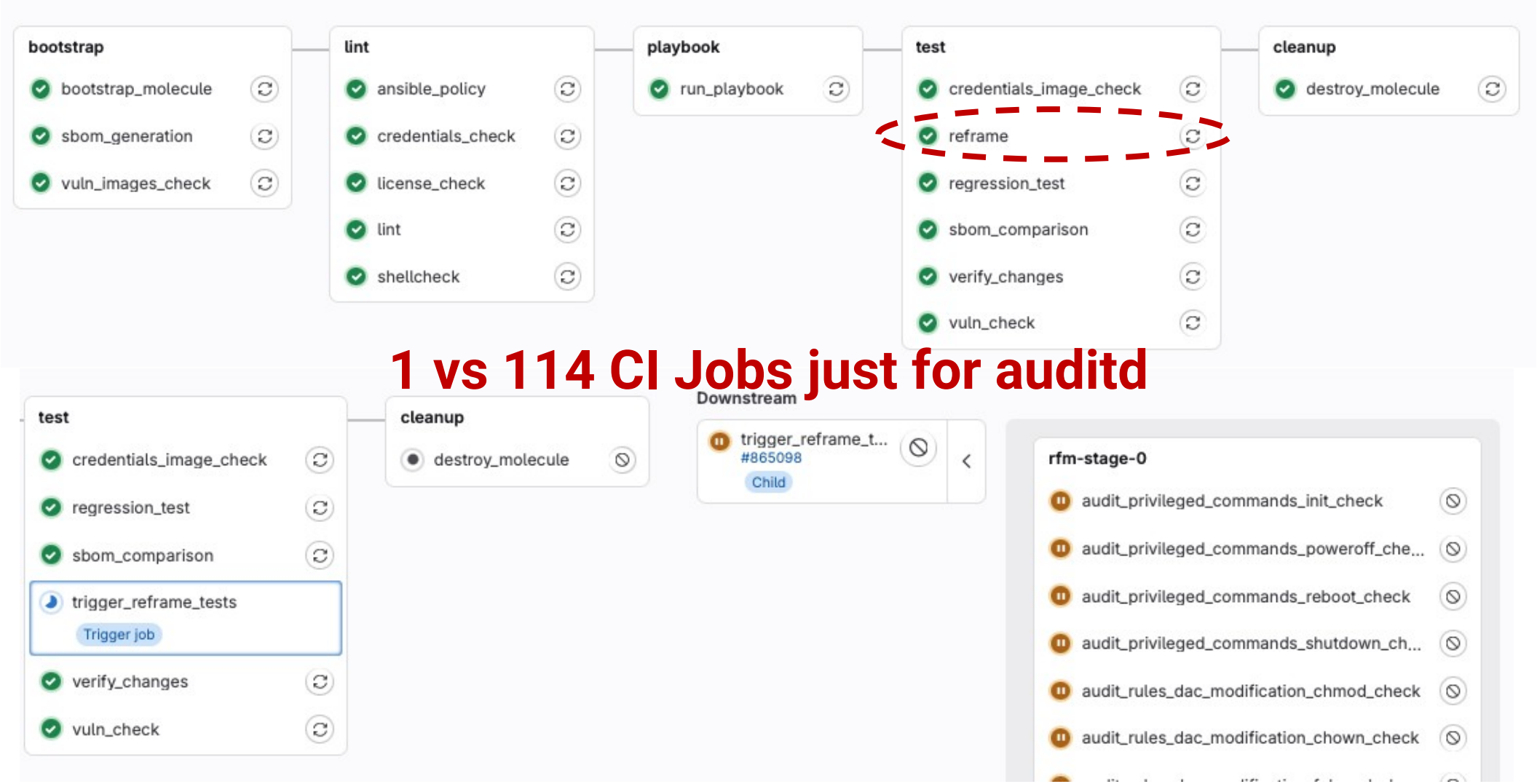


- Single repository of security checks vs per project
  - Monolithic repository (Google Style?) vs decentralized solution
  - Different security profile branches, different software versions

Current blocker for sharing our tests

How Fine Is Too Fine?

Adventures in CI Granularity

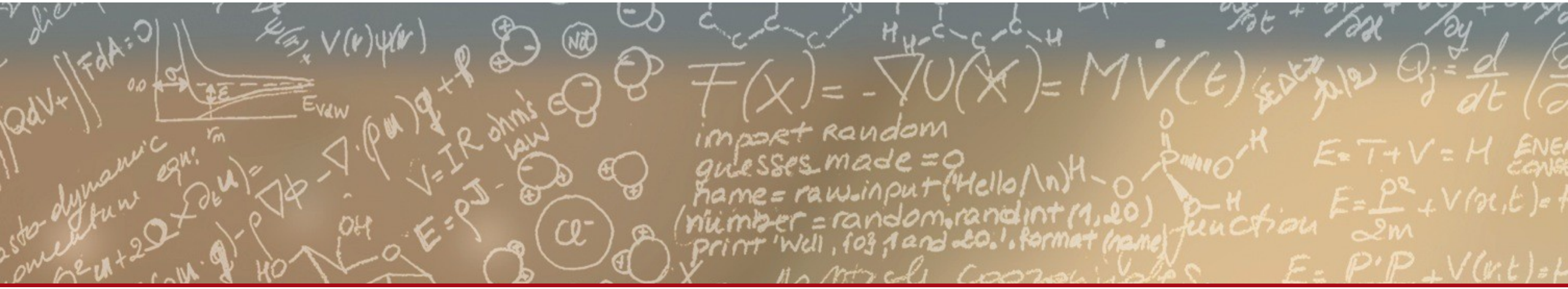


Take Home Message

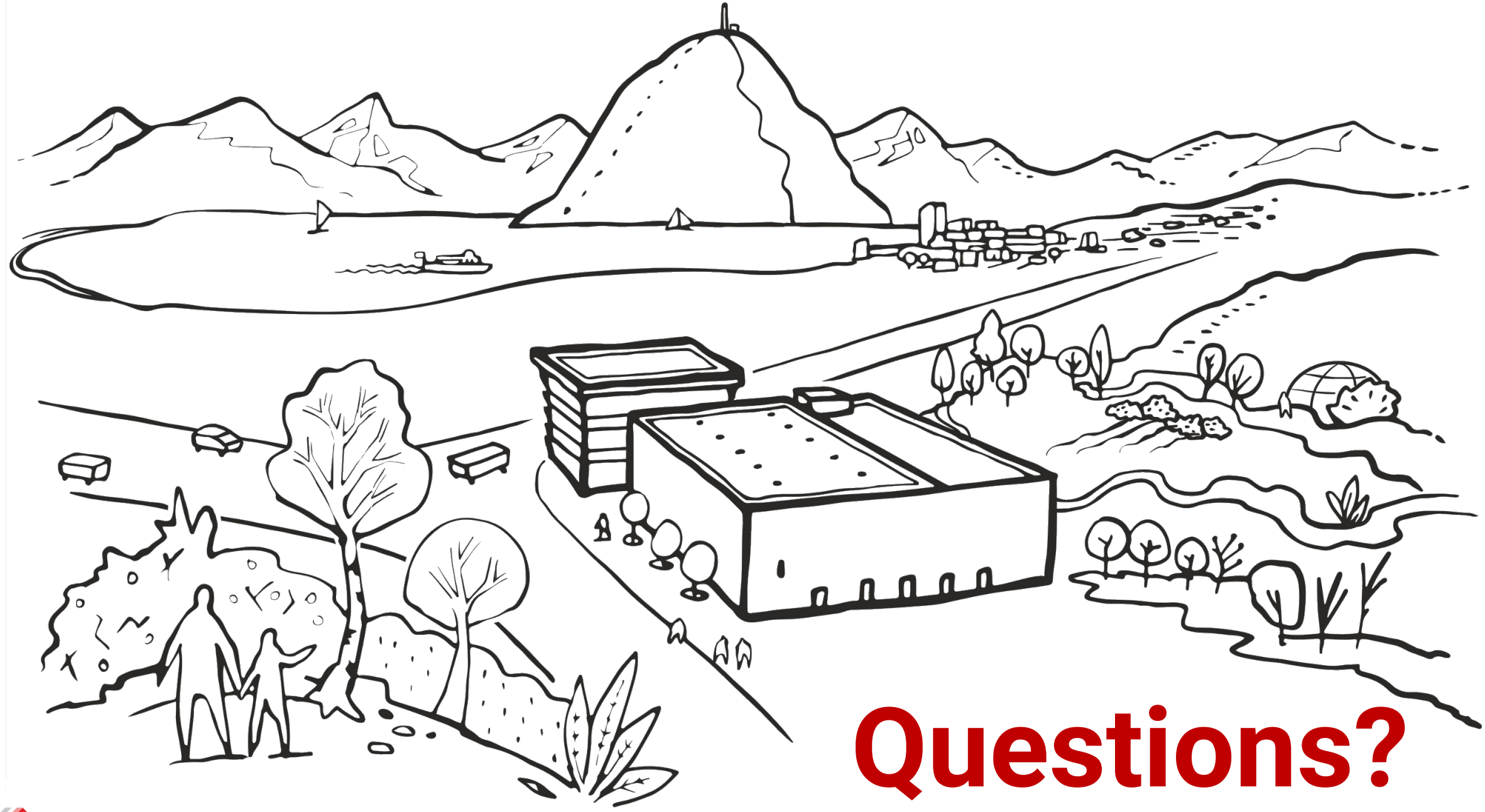
TL;DR Edition

- The Sec part in DevSecOps is very intrusive
  - Empower engineers to own their stack
  - Needs to reusable to avoid discrepancies in the security teams view and the DevSecOps view
- The tools may pose a challenge in DevSecOps adoption/implementation
- We used ReFrame because of its current adoption at CSCS
  - You are encouraged to use your own tool
- We are looking for people interested to work together to maintain these tests

The right tool speaks your team's language, cutting through noise to **focus on security**



Thank you for your attention.



Questions?