SURVIVING “AGILE” AS A SECURITY TEAM

… and become friends with the DevOps crowd

REDGUARD
SECURING YOUR ASSETS

Sven Vetsch
Co-Founder & Head of Security Research
sven.vetsch@redguard.ch

For today let’s keep it simple

- Agile = Staying flexible down the road and make changes to our goals, decisions, … whenever needed. Working in fast/small iterations instead of handing out huge work packages.

- DevOps = Combining skills and people from software development and IT operations to minimize friction and share responsibilities.

- Agile != DevOps

Challenge 1: Lack of security specialists

Dev

1

Challenge 1: Lack of security specialists

Dev	Ops
10	1

Challenge 1: Lack of security specialists

Dev	Sec	Ops
100	1	10

Challenge 1: Lack of security specialists

Dev Sec Ops

This reads “Sec”

Challenge 2: Different Mindset

- Issue 1: ✅
- Issue 2: ✅
- Issue 3: ✅
- Issue 4: ❌
- Issue 5: ✅
- Issue 6: ✅

Security / Compliance

OMG we’re vulnerable 😱

Software Engineering / DevOps

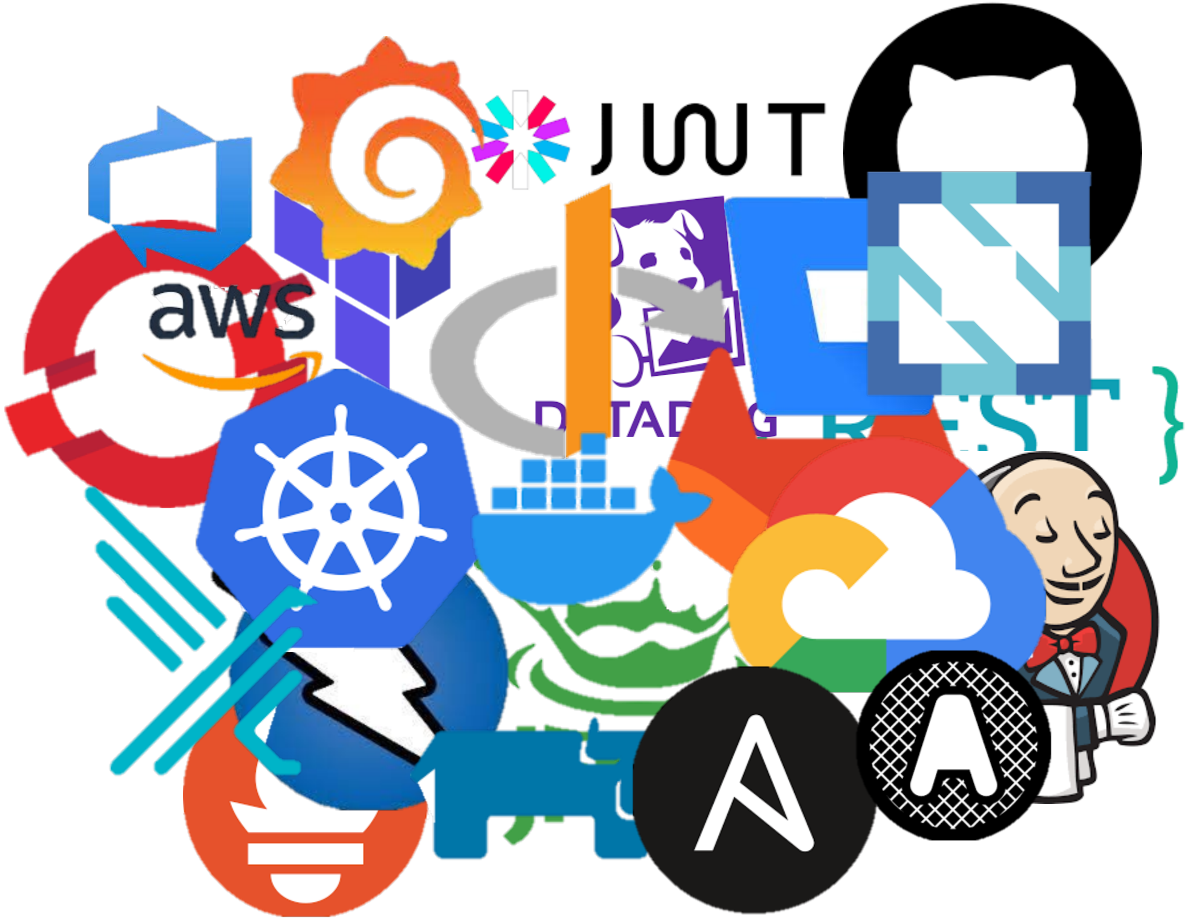
Yay, only one bug left, we’re right on track 🥳

Challenge 3: Technical capabilities / know-how

Old world

TREND MICRO
Active Directory
CISCO
CHECK POINT
kaspersky
nessus

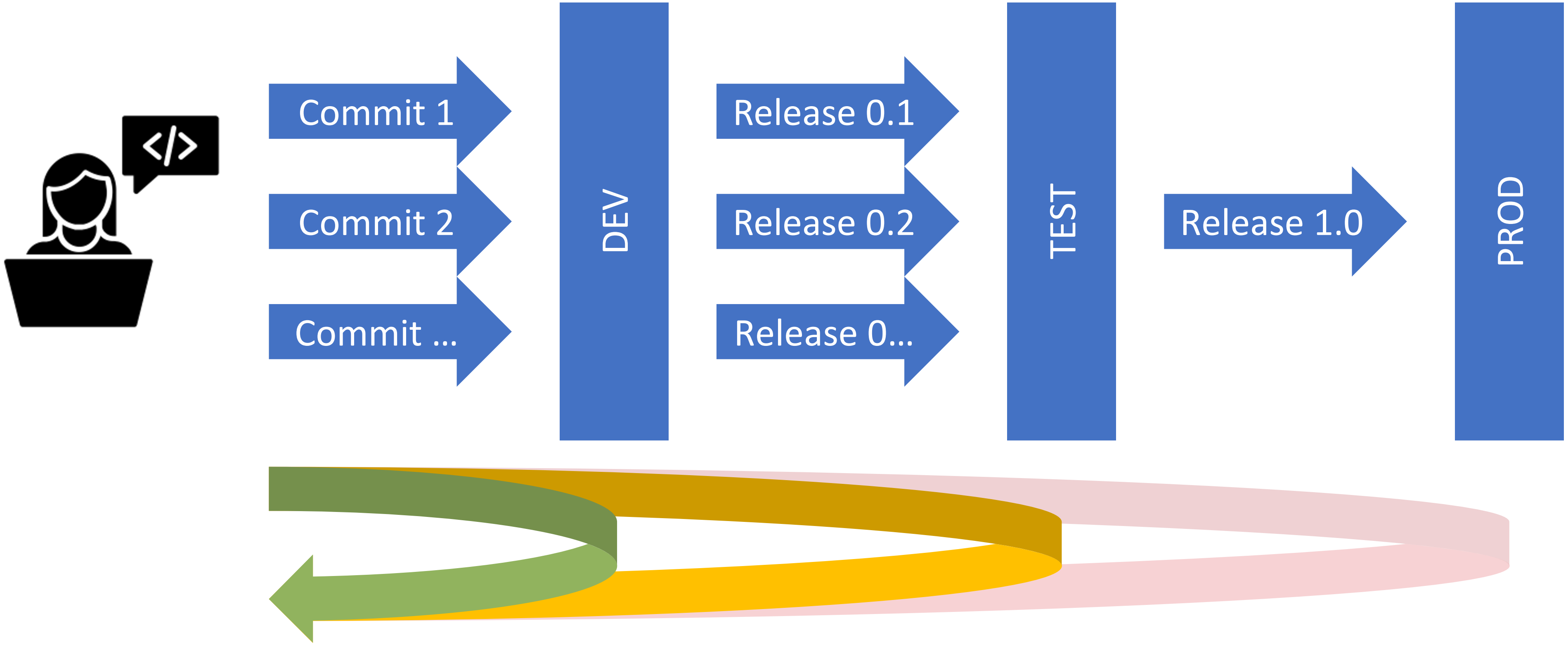
New world

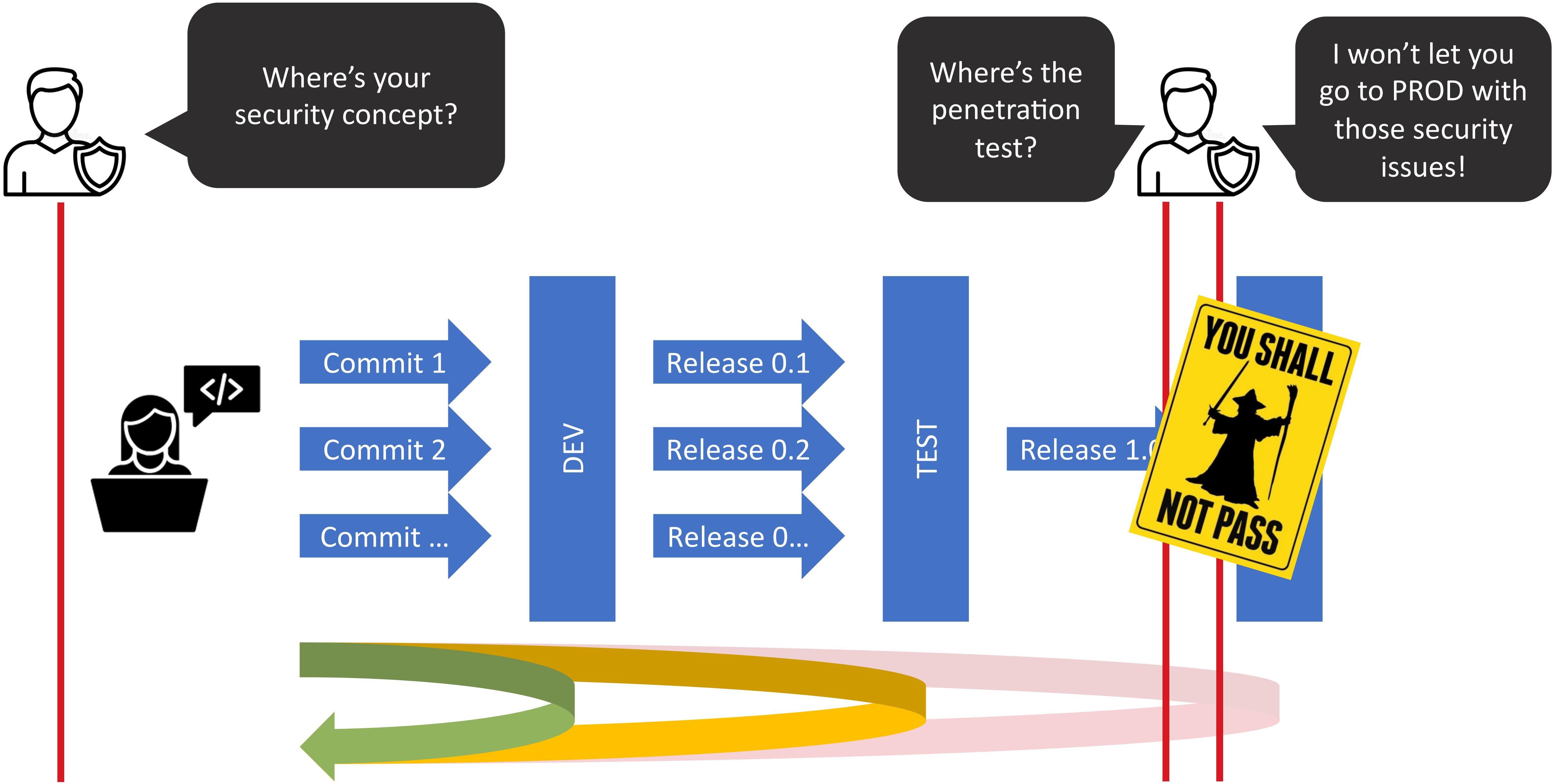


Problems for security teams

- Can’t keep up with the high frequency of changes
- Frustration over not being involved
- Can’t handle the extended permissions for developers (on their own projects)
- Don’t know all of the modern tools
- Don’t have experience in coding (business applications as well as in …-as-code)
- Not leveraging automation
- Trying to enforce compliance by reviews/audits instead of process/architecture/tooling

USUAL BEHAVIOUR OF THE SECURITY TEAM


Commit 1
Commit 2
Commit ...
DEV
Release 0.1
Release 0.2
Release 0...
TEST
Release 1.0
PROD



Where's your security concept?

Where's the penetration test?

I won't let you go to PROD with those security issues!

Commit 1

Commit 2

Commit …

DEV

Release 0.1

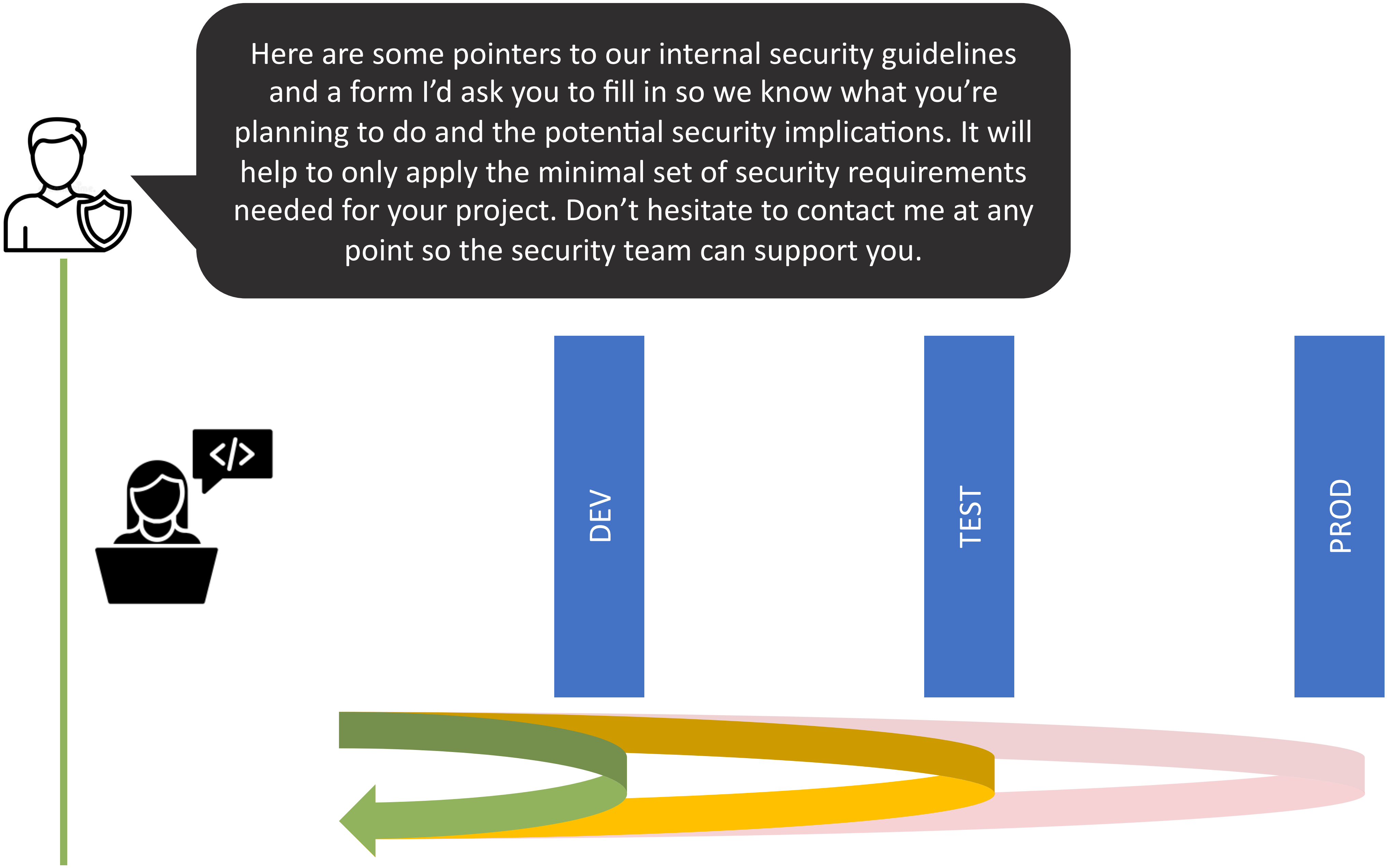
Release 0.2

Release 0…

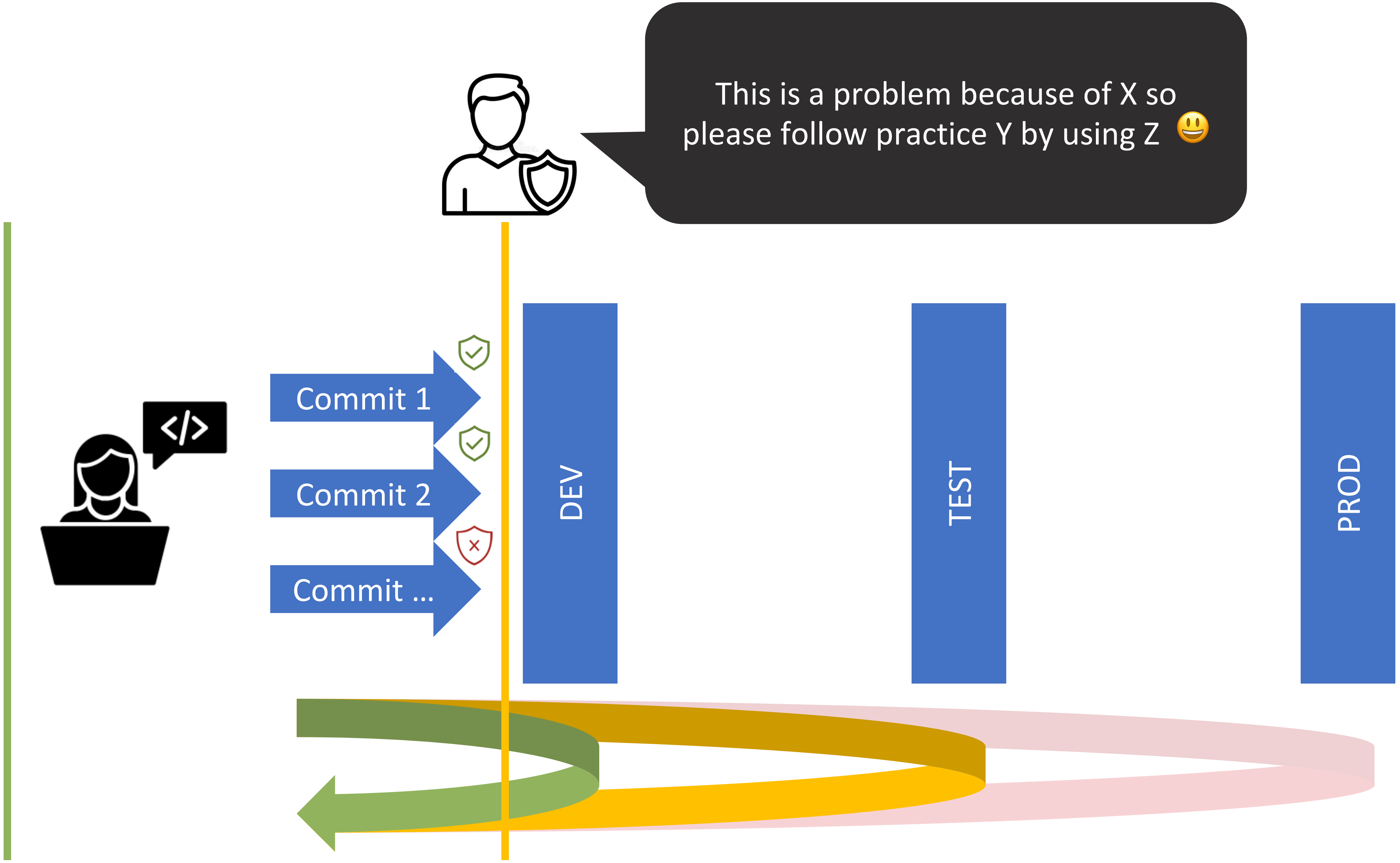
TEST

Release 1.(

PROPOSED BEHAVIOUR OF THE SECURITY TEAM



Here are some pointers to our internal security guidelines and a form I'd ask you to fill in so we know what you're planning to do and the potential security implications. It will help to only apply the minimal set of security requirements needed for your project. Don't hesitate to contact me at any point so the security team can support you.



This is a problem because of X so please follow practice Y by using Z 😃

Commit 1

Commit 2

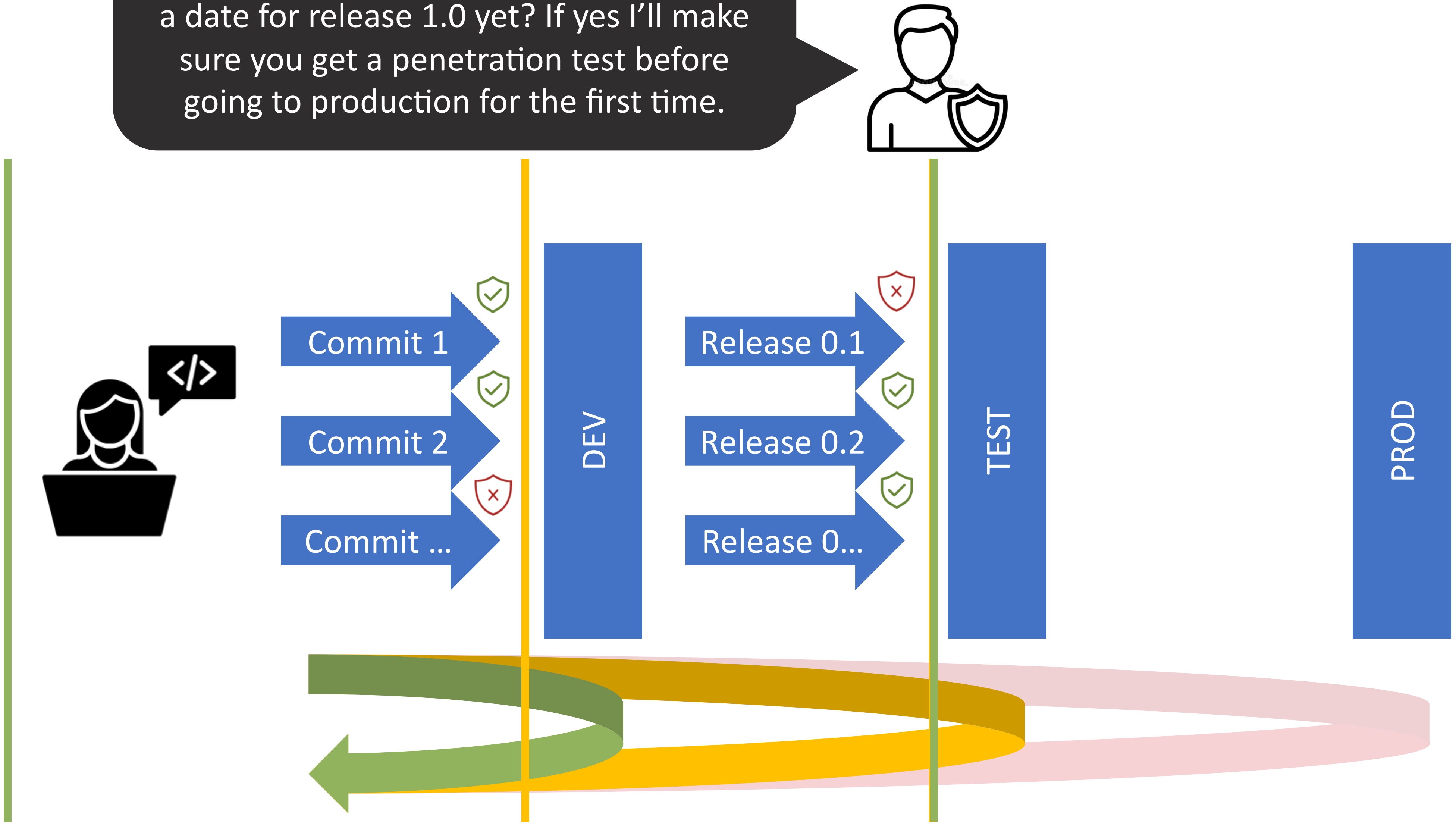
Commit …

DEV

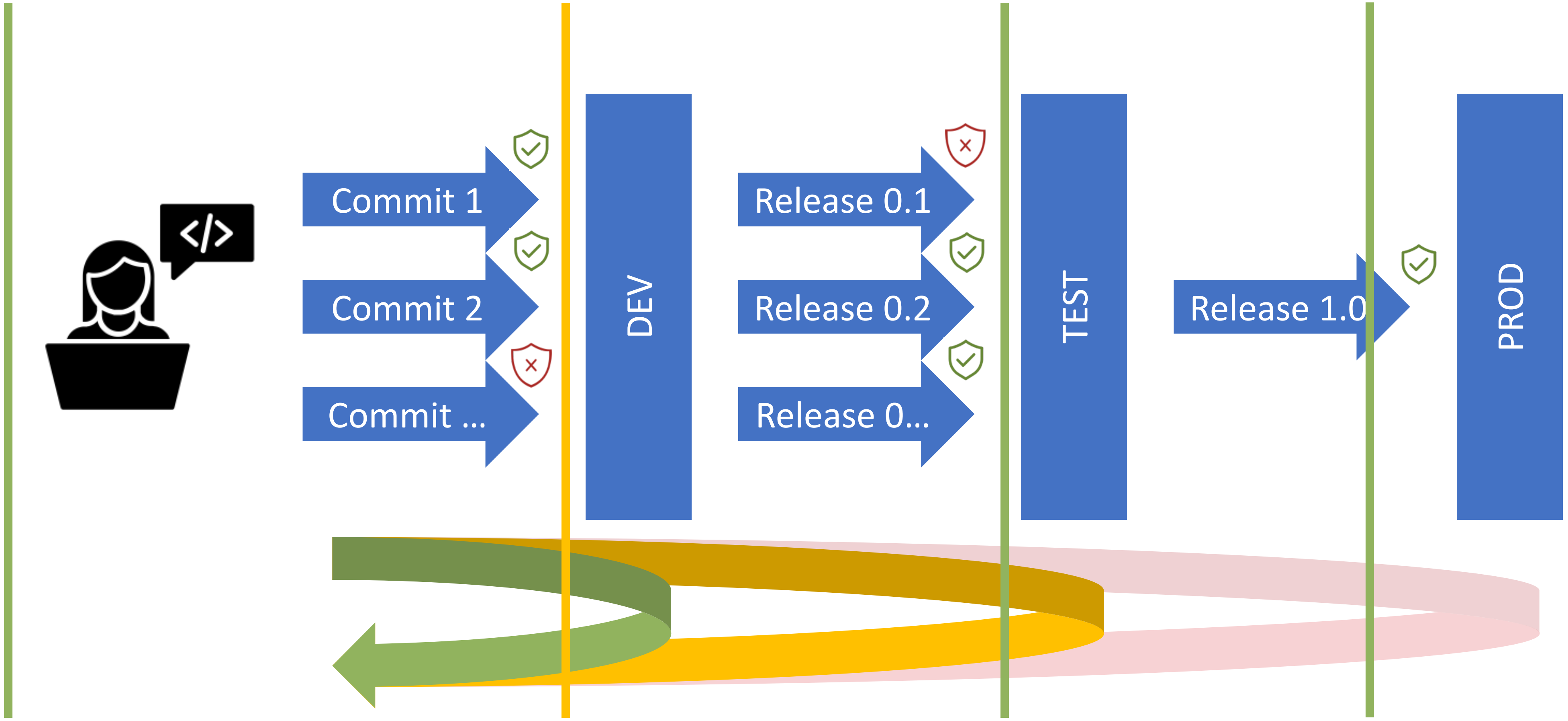
TEST

PROD

This really won’t fly in production. Do you need help addressing it? Btw. do you have a date for release 1.0 yet? If yes I’ll make sure you get a penetration test before going to production for the first time.

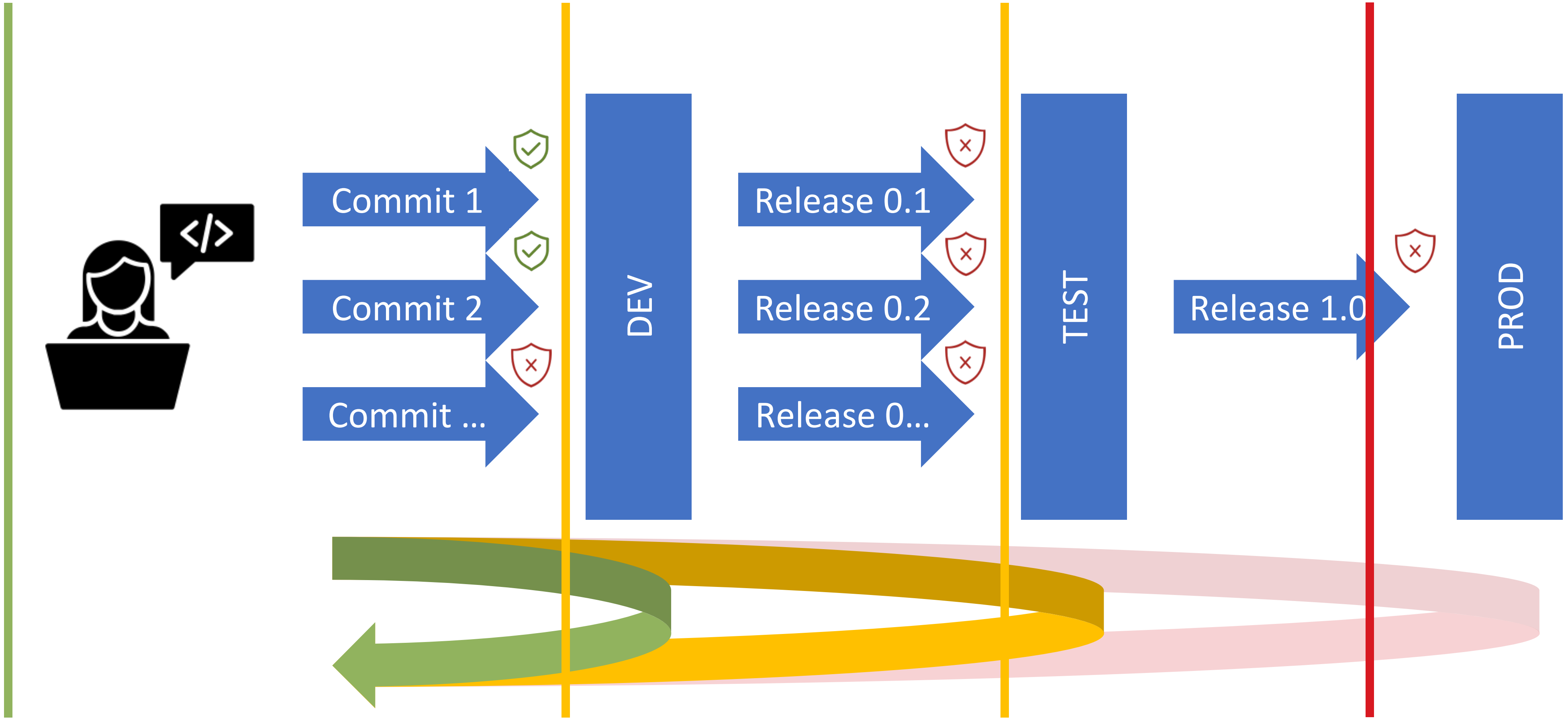


No major security issues, great job! We also made sure all results of the security scans and penetration tests are available to you for further tracking and we'll get back to you from time to time to discuss them and plan security tests for future releases.



… or

Sorry but as said in DEV and TEST we can’t let the release pass with this security issue. How can I help you to address it?



Commit 1

Commit 2

Commit …

DEV

Release 0.1

Release 0.2

Release 0…

TEST

Release 1.0

PROD

Proposed Changes (1/2)

- Make your security policies and guidelines worth to be read or at least minimal
  - Instead (or better in addition to) provide essential principles to be followed.
  - Should also include reasoning so engineers understand why they should follow each principle.
- Don’t just be a gatekeeper but an enabler/supporter instead. Work together!
  - Only block something if absolutely needed → Don’t be a Gandalf 🧙
- Offer in-house consulting
- Share responsibility with project teams (can be a security champions model but doesn’t have to)
- Learn about the “new” technologies your engineers use and start using it too

Proposed Changes (2/2)

- Make your tooling (e.g. security scanners) and results available to other teams to create visibility
- Provide easy to use tooling and data/information to projects and individuals (e.g. if there's a vulnerability in my code I'd like to be informed about it as a developer)
  - CI/CD pipeline integrations, APIs, dashboards, … are highly apprechiated
- Start "coding" (as in e.g. policy-as-code) instead of providing MS Word and Excel documents
- Provide turn-key ready solutions (tools, libraries, services, …) and secure defaults
- Test often and early
  - Automation, automation, automation
- …

And they all were friends and lived happily ever after

A wild DALL·E 2 AI creation appears

THE END - Thank you!

BERN
Redguard AG
Eigerstrasse 60
CH-3007 Bern

ZÜRICH
Redguard AG
Thurgauerstrasse 36/38
CH-8050 Zürich

Phone: +41 (0)31 511 37 50
contact@redguard.ch
www.redguard.ch