The Developer’s Nightmare

How To Survive Compliance Checklists (and Still Ship Fast)

Alexandra Aldershaab & Thomas Vitale
KubeCon+CloudNativeCon Europe
24th Mar 2026

@thomasvitale.com

linkedin.com/in/housa

Alexandra Aldershaab

Eficode



TAG DEVELOPER EXPERIENCE

FRIENDS OF DOROTHY
CNCF COMMUNITY

EDGE NATIVE MEETUP



linkedin.com/in/housa

Thomas Vitale

Systematic

Arconia





Java™ Champions

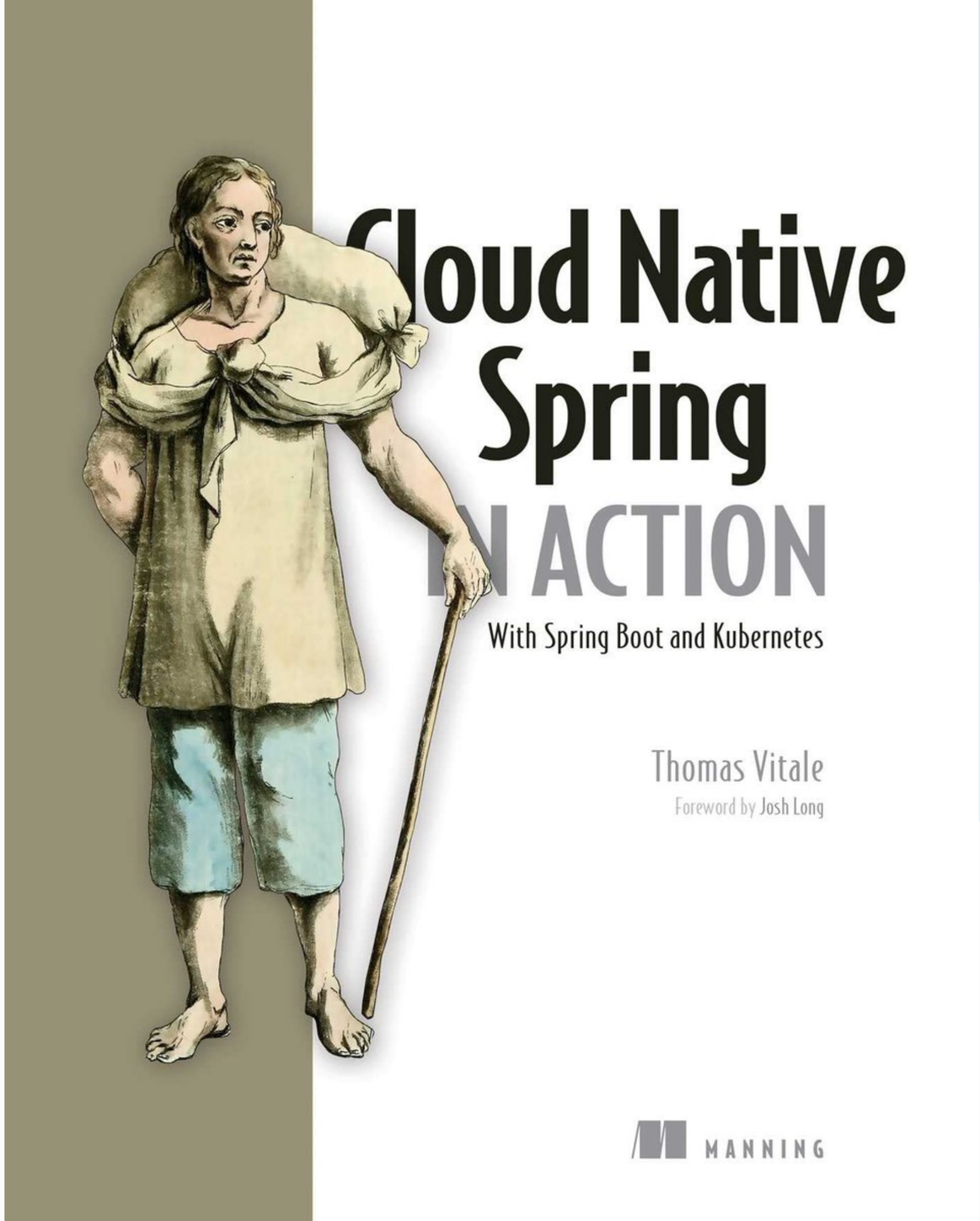
AMBASSADOR

CLOUD NATIVE COMPUTING FOUNDATION

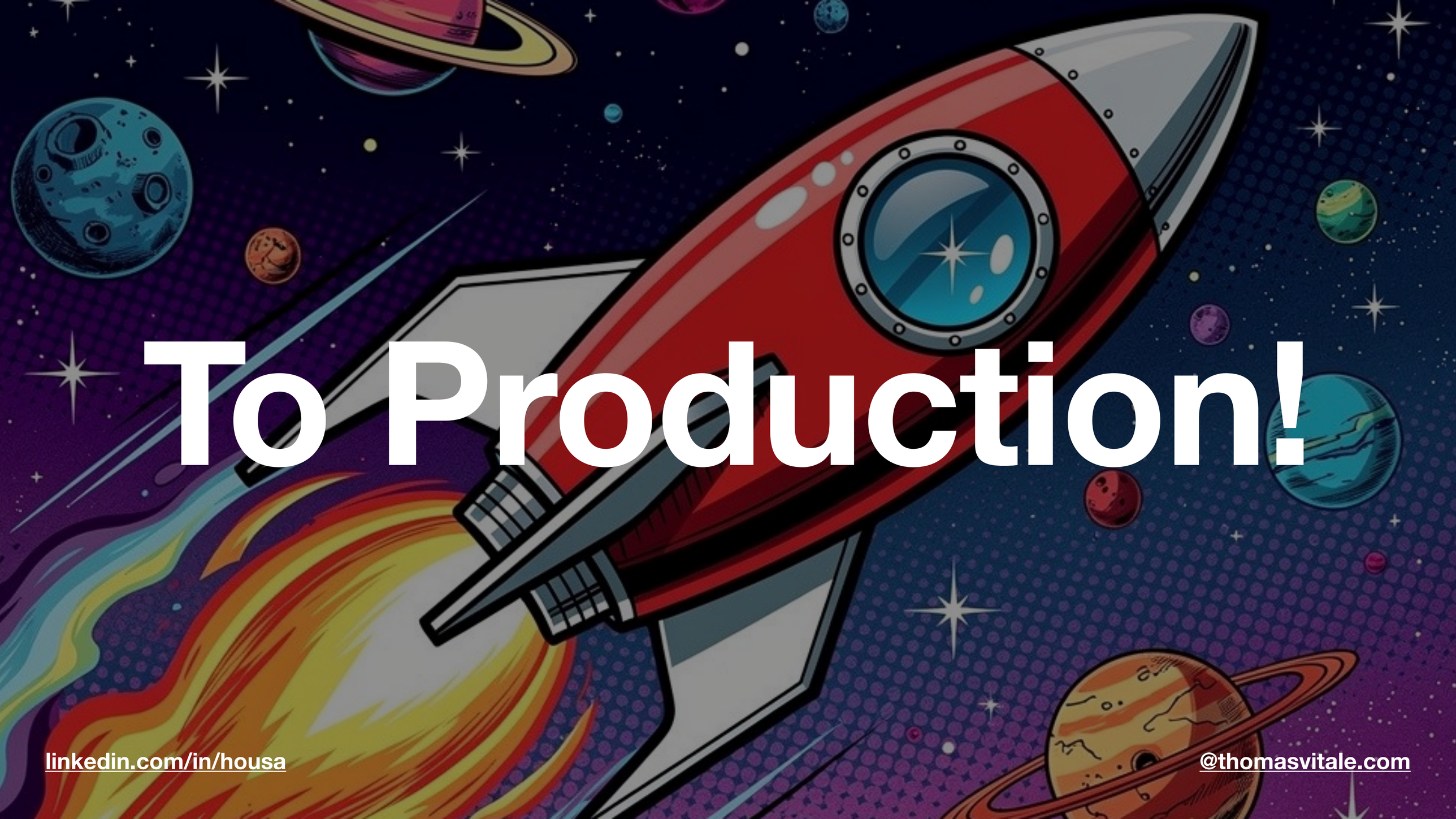
spring AI

@thomasvitale.com

Testcontainers®




Can you
approve my PR?
linkedin.com/in/housa
@thomasvitale.com



linkedin.com/in/housa

@thomasvitale.com



linkedin.com/in/housa

@thomasvitale.com



linkedin.com/in/housa

@thomasvitale.com

License Management


NOPE

License Approval Request - Q1 2026 Release Cycle - Message (HTML)

Reply | Reply All | Forward | Move to Folder... | Delete | Print | Flag

From: Drew Patterson <d.patterson@example-corp.net>

To: Jesse Nakamura <j.nakamura@example-corp.net>

Cc: James Whitfield <j.whitfield@example-corp.net>

Date: Tuesday, March 10, 2026 09:14 AM

Subject: **License Approval Request - Q1 2026 Release Cycle** ⚠ NORMAL PRIORITY

release_notes_q1_2026.pdf (142 KB) · license_delta_summary.xlsx (38 KB)

Hi Jesse,

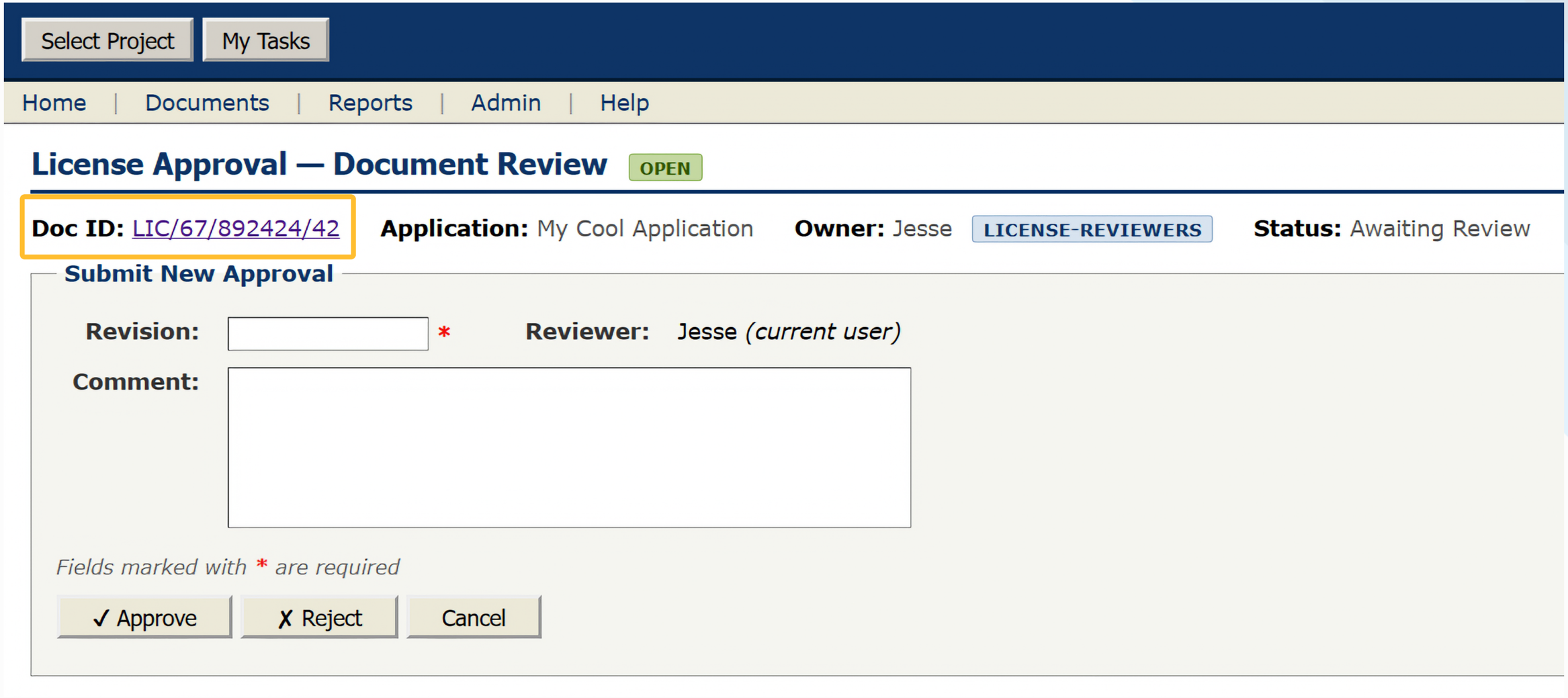
Hope you're doing well. We've got a new batch of application releases coming through the pipeline and they need your license sign-off before we can push to production. Below are the details for each application along with links to the SBOM reports and the approval system.

Could you please review and approve when you get a chance? We're targeting end of week for the rollout, so no crazy rush but sooner is better.

Application	Version	SBOM Report	Approval Link
User Service	`2.0.2` prev. approved: 2.0.1	https://sbom-system.example.net/user-service	https://approval.example.net/licenses/LIC-67-892424-42
Payment Gateway	`4.1.0` prev. approved: 4.0.3	https://sbom-system.example.net/payment-gateway	https://approval.example.net/licenses/LIC-67-892425-18
Notification Engine	`1.8.5` prev. approved: 1.8.4	https://sbom-system.example.net/notification-engine	https://approval.example.net/licenses/LIC-67-892430-07
My Cool Application	`2.1.0` prev. approved: 2.0.1	https://sbom-system.example.net/my-cool-application	https://approval.example.net/licenses/LIC-67-892424-42
Auth Proxy	`3.0.0` prev. approved: 2.9.1	https://sbom-system.example.net/auth-proxy	https://approval.example.net/licenses/LIC-67-892441-33

Approval History (showing 10 records)

Rev.	Reviewer	Date / Time	Comment
2.0.1	Jesse	07-03-2026 11:22:04	Approved v. 2.0.1 compared to v. 2.0.0. No changes.
2.0.0	James	21-02-2026 09:17:38	Approved v. 2.0.0 compared to v. 1.3.0. No changes.
1.3.0	Jesse	06-02-2026 16:41:19	Approved v. 1.3.0 compared to v. 1.2.2, no new licenses with license risk.
1.2.2	James	22-01-2026 10:53:47	Approved v. 1.2.2 compared to v. 1.2.0. No changes.
1.2.0	Jesse	09-01-2026 08:35:52	Approved v. 1.2.0 compared to v. 1.1.1. No changes.
1.1.1	James	12-12-2025 15:28:11	Approved v. 1.1.1 compared to v. 1.1.0. No changes.
1.1.0	Jesse	27-11-2025 10:04:46	Approved v. 1.1.0 compared to v. 1.0.2. No changes.
1.0.2	James	14-11-2025 13:51:23	Approved v. 1.0.2 compared to v. 1.0.1. No new licenses with license risk.
1.0.1	Jesse	30-10-2025 09:42:37	Approved v. 1.0.1 compared to v. 1.0.0. No new licenses with license risk.
1.0.0	James	16-10-2025 17:20:09	Approved v. 1.0.0. Initial license baseline established.


Select Project
My Tasks
Home | Documents | Reports | Admin | Help
License Approval — Document Review
OPEN
Doc ID: LIC/67/892424/42
Application: My Cool Application
Owner: Jesse
LICENSE-REVIEWERS
Status: Awaiting Review
Submit New Approval
Revision: *
Reviewer: Jesse (current user)
Comment:
Fields marked with * are required
✓ Approve
✗ Reject
Cancel

SBOM

"A Software Bill of Materials (SBOM) is a nested inventory for software, **a list of ingredients** that make up software components."

SBOM as part of the build lifecycle

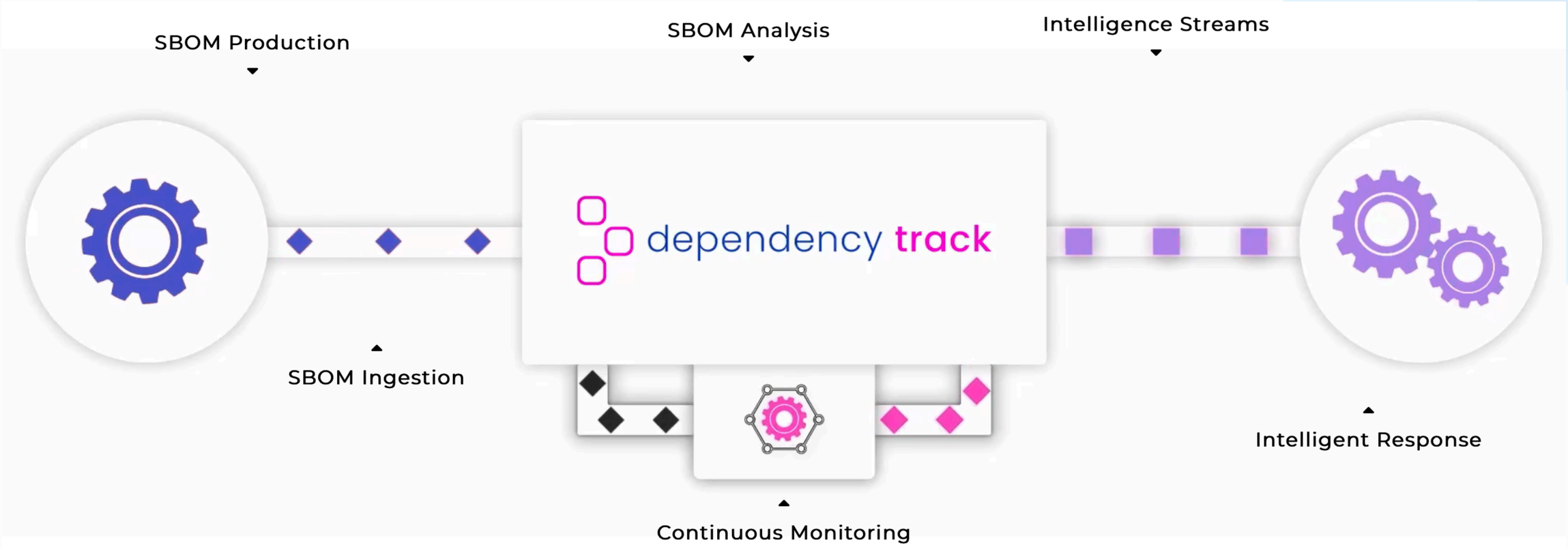
Using the CycloneDX Gradle plugin for Java

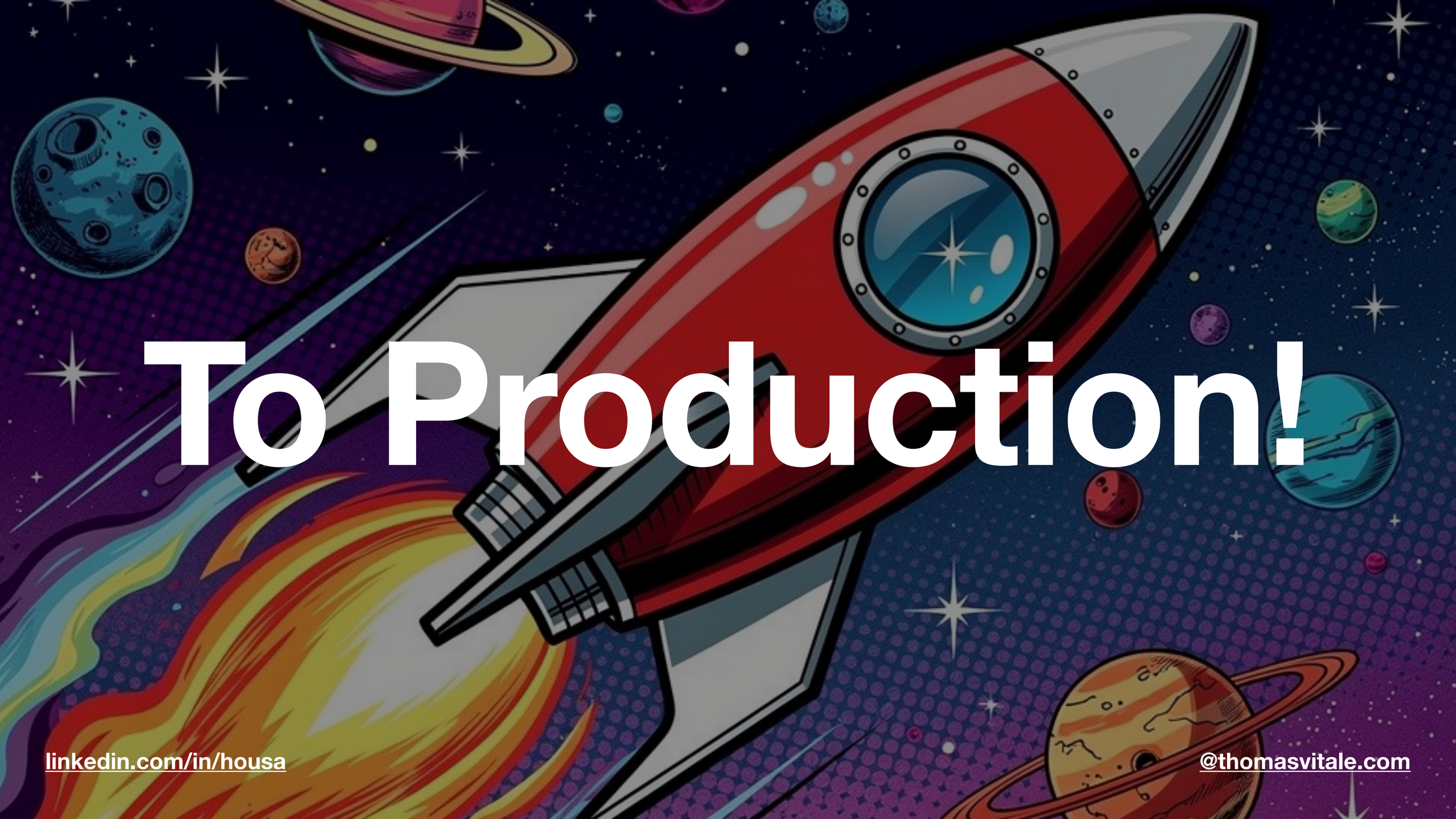


```
plugins {
    id 'org.cyclonedx.bom' version '3.2.2'
}
```

Managing Supply Chain Risks

OWASP Dependency Track





linkedin.com/in/housa

@thomasvitale.com

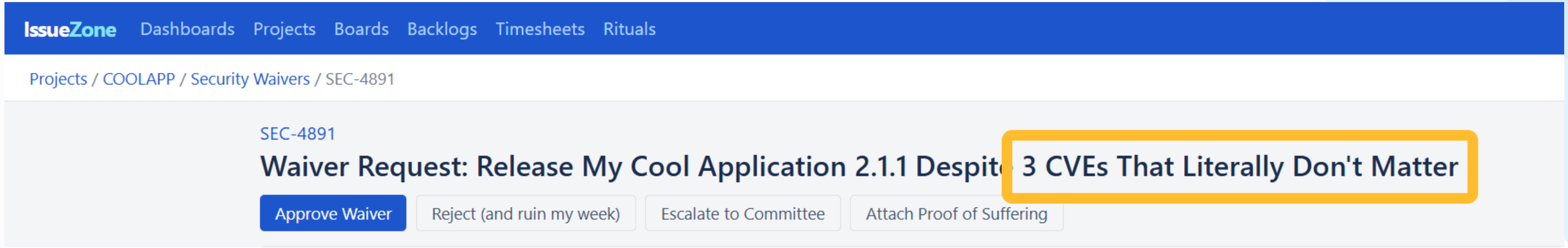
Vulnerability Management

NOPE



linkedin.com/in/housa

@thomasvitale.com


IssueZone
Dashboards
Projects
Boards
Backlogs
Timesheets
Rituals
Projects / COOLAPP / Security Waivers / SEC-4891
SEC-4891
Waiver Request: Release My Cool Application 2.1.1 Despite 3 CVEs That Literally Don't Matter
Approve Waiver
Reject (and ruin my week)
Escalate to Committee
Attach Proof of Suffering

DESCRIPTION

Requesting a security waiver to proceed with the release of **My Cool Application v2.1.1**. The latest vulnerability scan flagged 3 CVEs, all of which are abou as threatening as a goldfish in a desert:

`CVE-2025-31822` Theoretical timing attack on a logging library we use in debug mode only. Exploitable if the attacker has physical access to the server, a PhD in quantum physics, and nothing better to do on a Friday night.

`CVE-2025-28104` XSS in an HTML sanitizer's *demo page* which we don't ship, don't use, and didn't know existed until the scanner found it.

`CVE-2025-33510` Denial of service via malformed YAML. Our application does not accept YAML. We don't even know what YAML stands for. *(Yet Another Markup Language, apparently.)*

Patch versions for the affected libraries are not yet available. Estimated fix from upstream: "sometime between next week and the heat death of the universe."

MANDATORY WAIVER CHECKLIST (BECAUSE COMPLIANCE SAID SO)

- [x] ~~I have read the 47-page Security Waiver Policy (skimmed it, close enough)~~
- [x] ~~Risk assessment attached in the format nobody can open (.oxps)~~
- [x] ~~SBOM reviewed and no new licenses with risk introduced~~
- [x] ~~Business justification: "customers are waiting and Slack is on fire"~~
- [x] ~~Confirmed CVEs don't apply to our deployment (for the third time)~~
- [x] ~~Sacrificed a rubber duck to the AppSec gods~~
- [ ] Obtained verbal approval from someone who "doesn't do email"

Status	AWAITING MIRACLE
Type	🛡 Security Waiver
Priority	↑ Urgent-ish
Resolution	*Pending since forever*
Labels	security waiver release
Fix Version	2.1.1
Affected Ver.	2.1.1-rc3
Sprint	Sprint 42: The Answer
Story Points	0.5 (lol)
SBOM	View Report ↗
Approval	Doc Tracking ↗


0 OKRs ?



CURL AND LIBCURL

DEATH BY A THOUSAND SLOPS

JULY 14, 2025 DANIEL STENBERG 58 COMMENTS

I have previously blogged about the relatively new trend of AI slop in vulnerability reports submitted to curl and how it hurts and exhausts us.

#2199174

18

[Critical] Curl CVE-2023-38545 vulnerability code changes are disclosed on the internet

Share:

Report

TIMELINE

shelldoit submitted a report to curl. October 10, 2023, 4:25am UTC

Summary:

Curl CVE-2023-38545 vulnerability code changes are disclosed on the internet

Steps To Reproduce:

To replicate the issue, I have searched in the Bard about this vulnerability. It disclosed what this vulnerability is about, code changes made for this fix, who made these changes, commit details etc even though this information is not released yet on the internet. In addition to it, I was able to easily craft the exploit based on the information available. Remove this information from the internet ASAP!!!!

Reported on
October 10, 2023, 4:25am UTC

Reported by
shelldoit

Reported to
curl

Participants



Report Id
#2199174 N/A

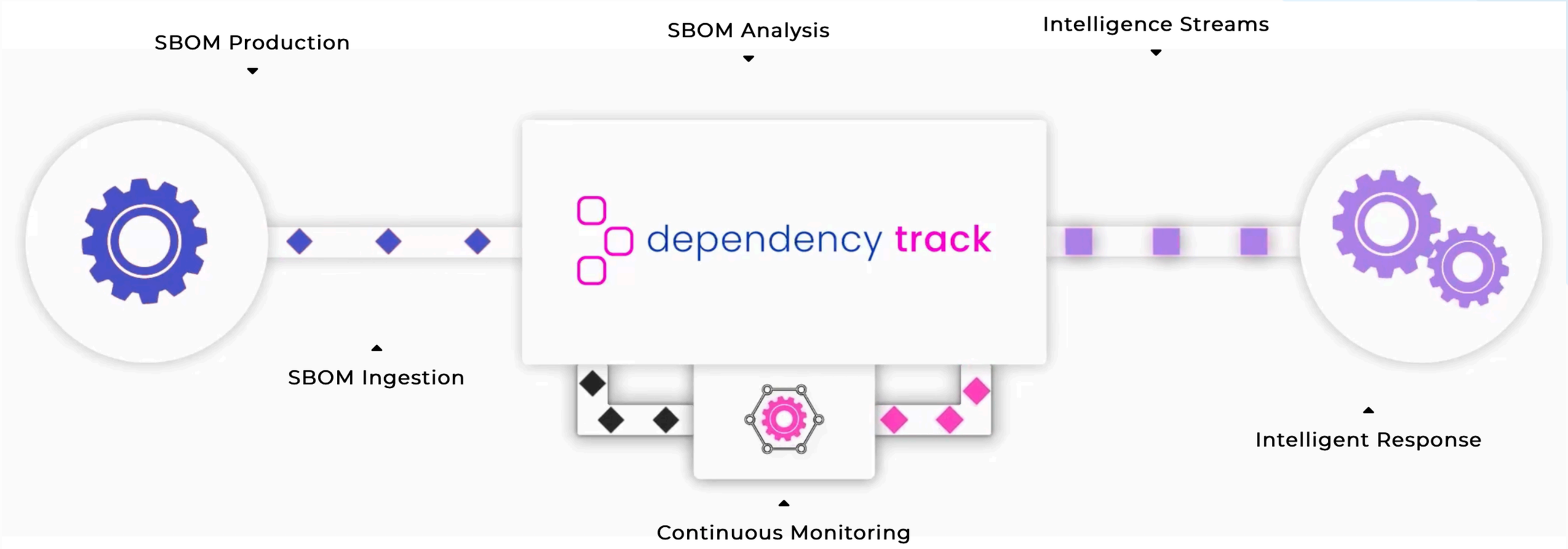
Severity
Critical (9 ~ 10)

Disclosed
October 16, 2023, 12:32pm UTC

Weakness
Information Disclosure

Managing Supply Chain Risks

OWASP Dependency Track



SBOMs

What can we use them for?

Inventory of all software components

Check for security vulnerabilities

Validate the licenses for each component

Find outdated components

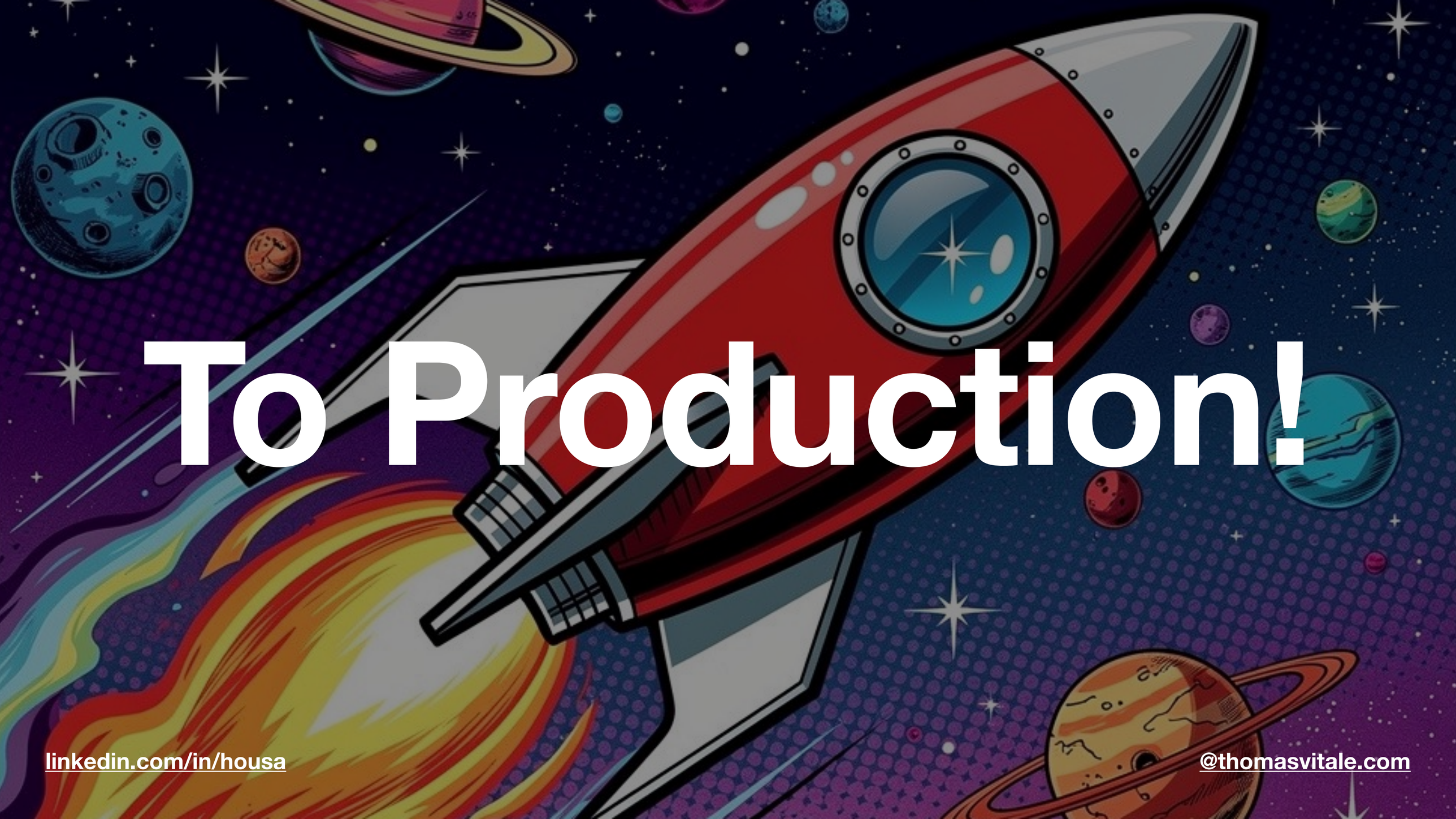
Verify integrity for each component

VEX

“Vulnerability Exploitability eXchange (VEX) is a vulnerability document designed to complement a Software Bill of Materials (SBOM) that informs users of a software product about the applicability of one or more vulnerability findings.”

OpenVEX
http://openvex.dev

@vitalethomas



linkedin.com/in/housa

@thomasvitale.com

Provenance Management


NOPE

WikiForge Spaces People Templates Apps Calendar Search WikiForge... DP

Engineering / My Cool Application / Build & Release / How We Build My Cool Application

PAGES IN THIS SPACE

- Overview
- Architecture (circa 2019)
- How We Build MCA
- Release Checklist
- Environments (Outdated)
- Secrets & Credentials
- On-Call Runbook
- Post-Mortems
- Why We Can't Have Nice Things

How We Build My Cool Application

Edit · More · Watch

Created by Drew Patterson · Last updated: Mar 06, 2026 · 14 people viewed this · 23 people should have

build release-process probably-outdated tribal-knowledge

⚠ **This page is the single source of truth for building MCA.** Yes, we know this should be a pipeline. Yes, we've filed a ticket. Yes, the ticket is in the backlog. It's been there since 2021. We've accepted our fate. If you're from the future and we finally have CI/CD — delete this page and throw a party.

TABLE OF CONTENTS

1. Prerequisites
2. Build Steps (The Sacred Ritual)
3. The Artifact Naming Convention
4. Environment Variables
5. How to Release
6. Known Quirks

1. Prerequisites

Before you attempt to build MCA, make sure you have the following. And no, you can't skip any of them. We tried.

Tool	Version	Status	Notes
Java	17.0.6	OK	Not 17.0.5. Not 17.0.7. **17.0.6.** Don't ask.
Maven	3.9.2	OK	Must be installed via SDKMAN or it won't find the settings.xml
Docker	24.x	FLAKY	Works on Linux. Mostly works on Mac. Thoughts and prayers on Windows.
Node.js	18 LTS	OK	Only used to compile 1 CSS file. Yes, really.
Greg's Script	???	MISSING	Greg left in 2023. The script lives on his laptop. We have a *partial* copy.

2. Build Steps (The Sacred Ritual)

Follow these steps **in exact order**. The build is not idempotent. If you run step 4 before step 3, the artifact will compile but silently produce incorrect checksums. We lost two days to this in Q3 2024.

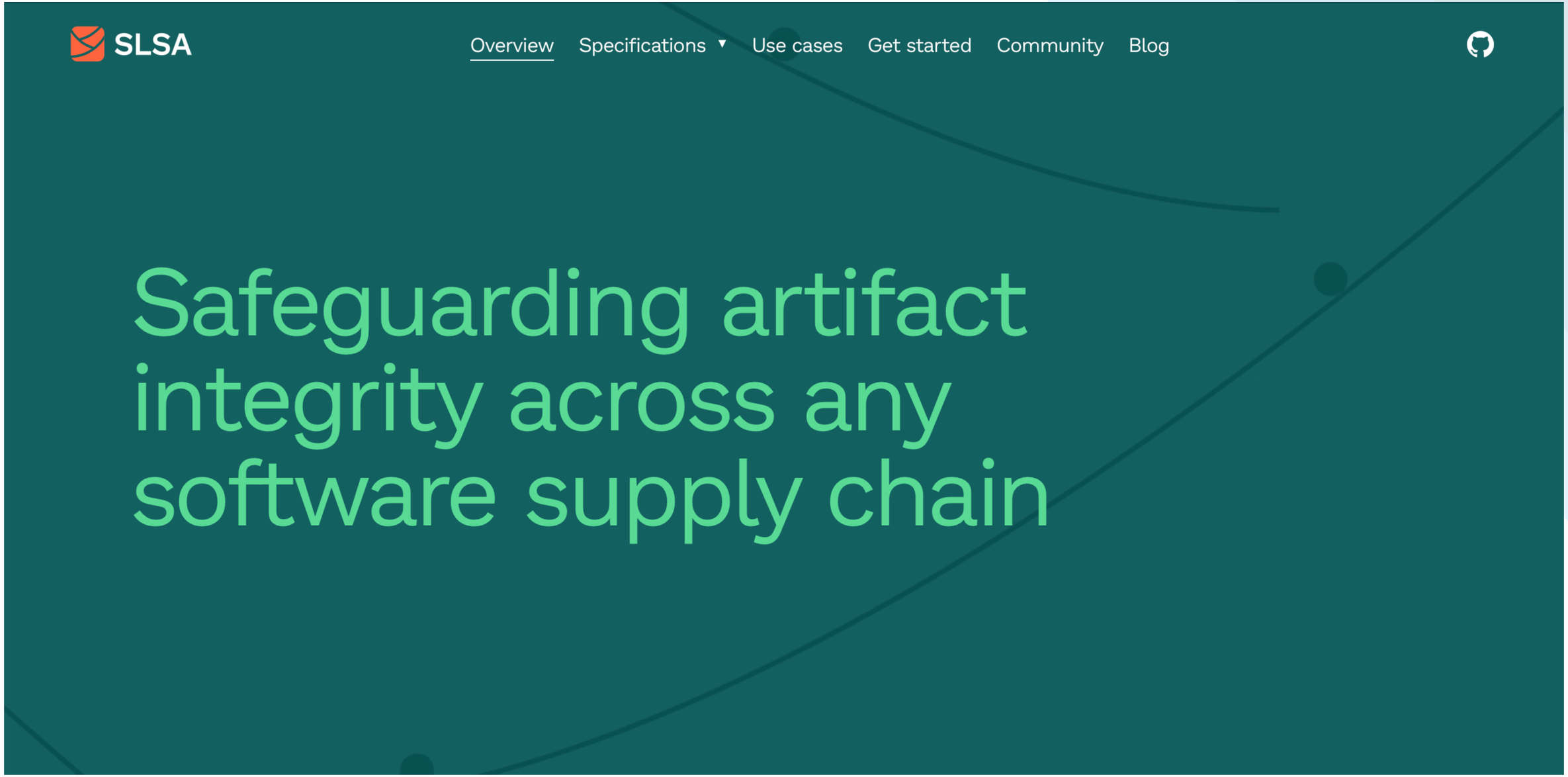
SLSA



SLSA
https://slsa.dev

linkedin.com/in/housa

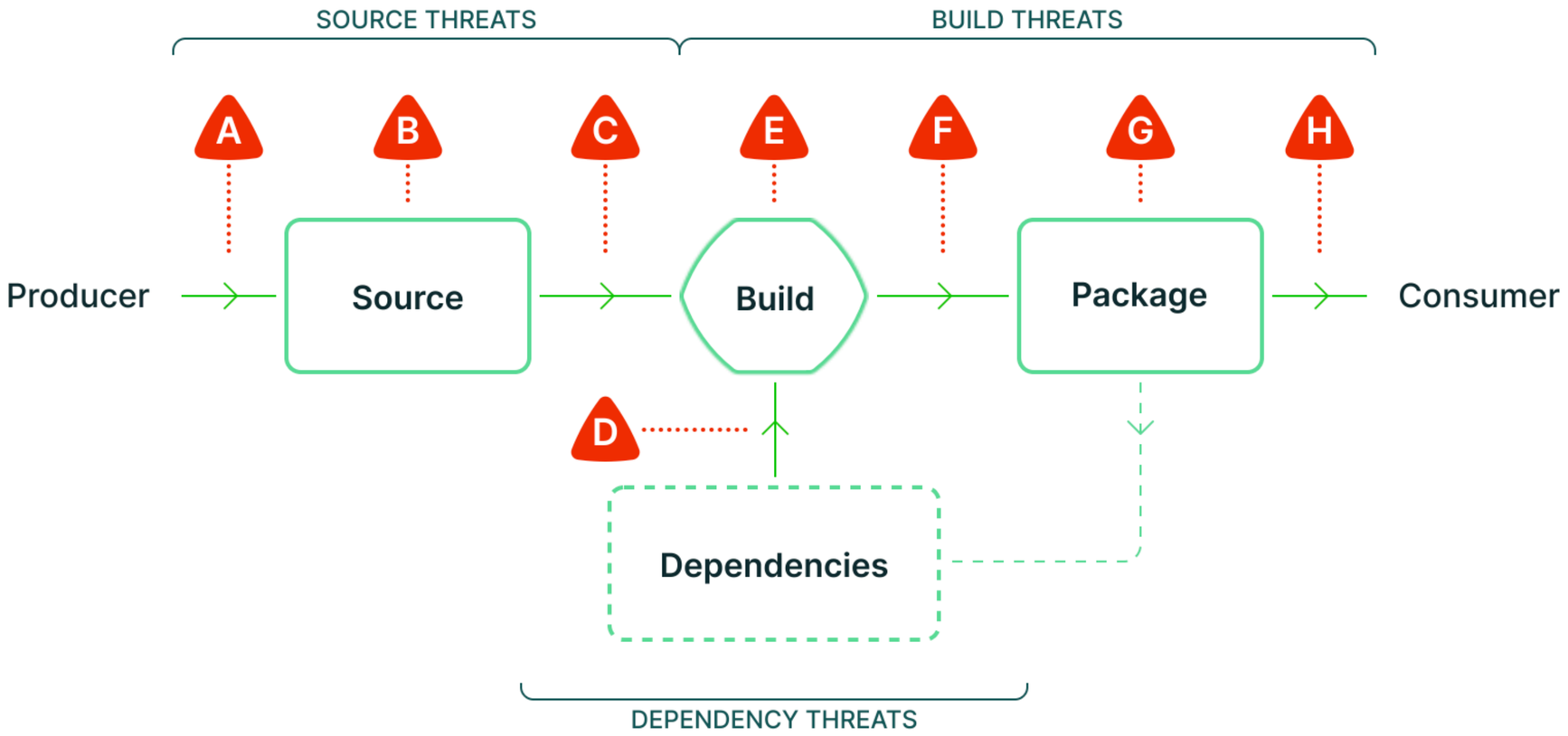
@thomasvitale.com



linkedin.com/in/housa

SLSA
https://slsa.dev

@thomasvitale.com



SOURCE THREATS

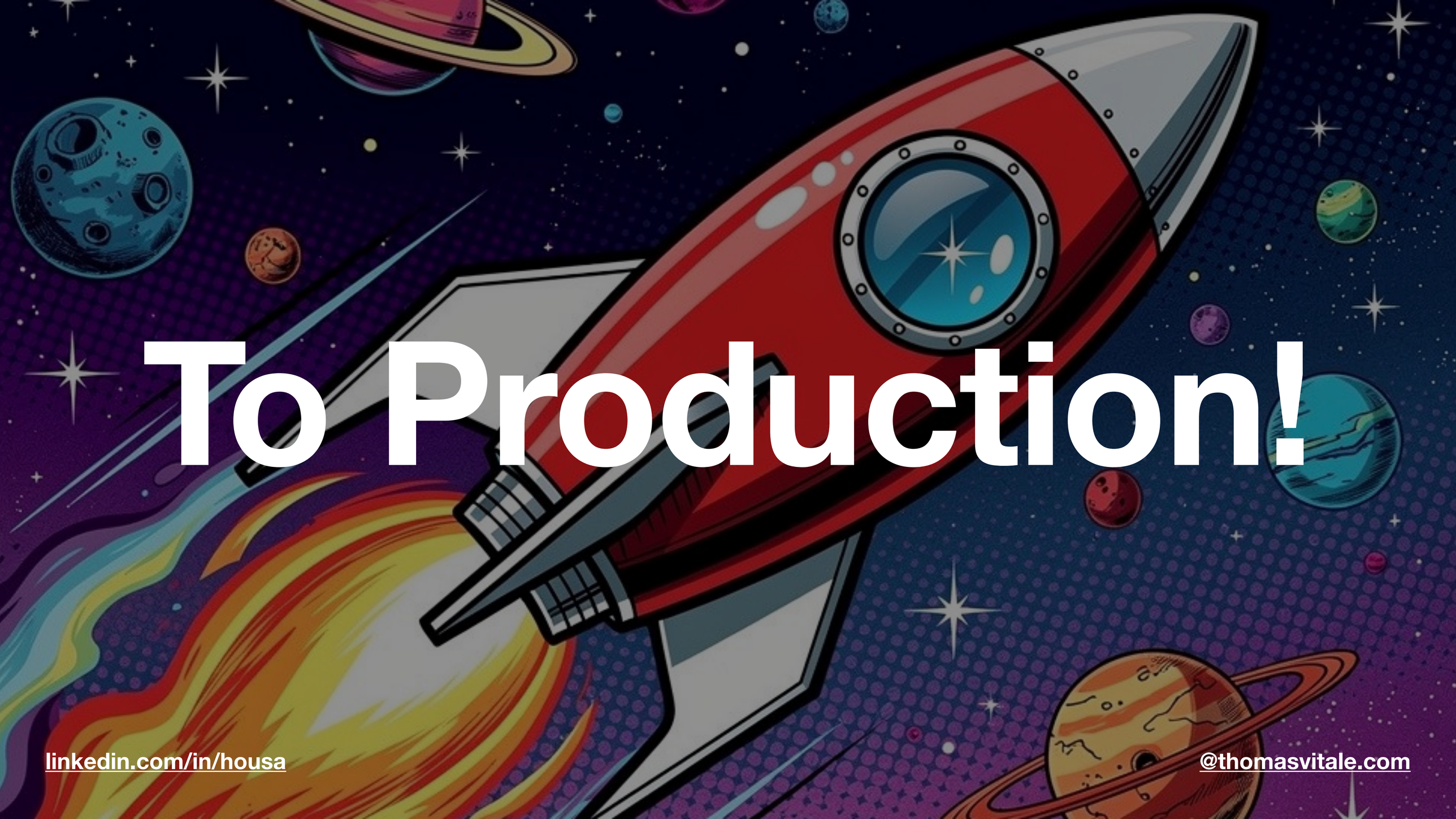
- **A** Submit unauthorized change
- **B** Compromise source repo
- **C** Build from modified source

DEPENDENCY THREATS

- **D** Use compromised dependency

BUILD THREATS

- **E** Compromise build process
- **F** Upload modified package
- **G** Compromise package repo
- **H** Use compromised package



linkedin.com/in/housa

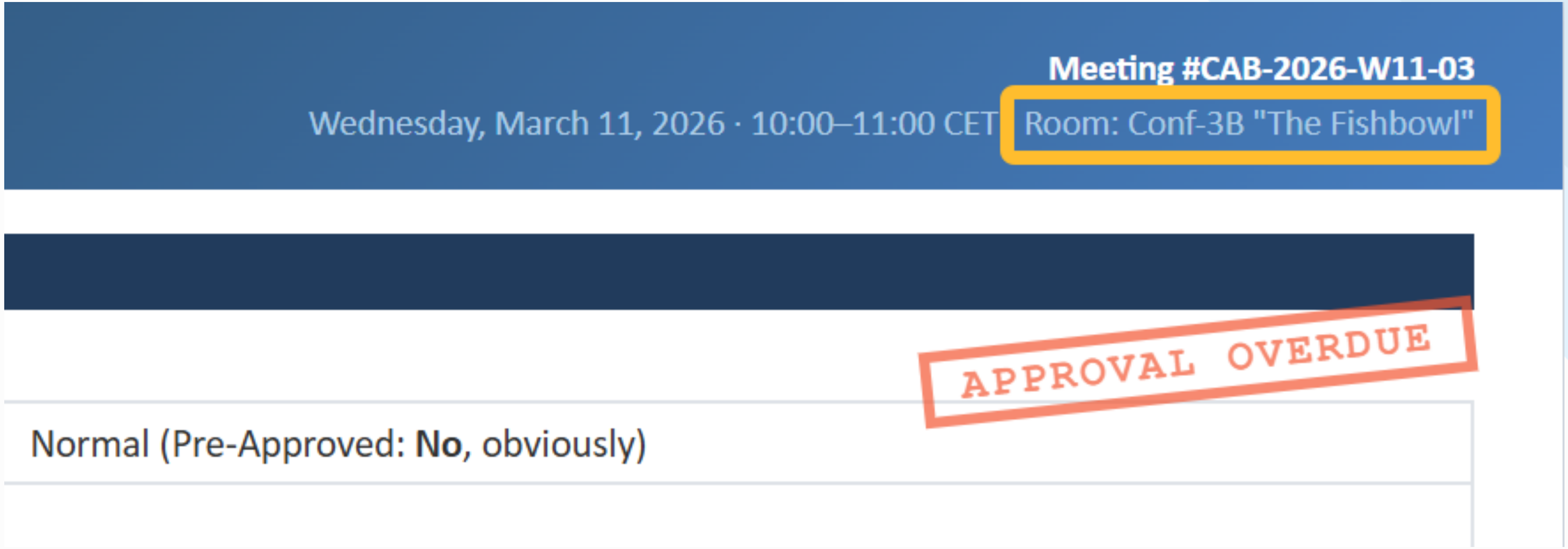
@thomasvitale.com

CHANGE ADVISORY BOARD — Meeting Agenda

Enterprise Change Management Office · ITIL-Compliant Since 2014 (Allegedly)

1. CHANGE UNDER REVIEW

Change ID	**CHG-2026-0847**
Title	**Release My Cool Application v2.0.2 to Production**
Requested By	Drew Patterson (Development)
Proposed Start	March 14, 2026 — 22:00 CET


Meeting #CAB-2026-W11-03
Wednesday, March 11, 2026 · 10:00–11:00 CET
Room: Conf-3B "The Fishbowl"
APPROVAL OVERDUE
Normal (Pre-Approved: No, obviously)

2. PRE-SUBMITTED QUESTIONS

⚠ MANDATORY Q&A (ALL ALREADY ANSWERED ELSEWHERE)

Q1. Can you walk us through the CVEs again? They're in the waiver, the email, and the SBOM, but we'd love to hear it live. — *Ka*

Q2. Has QA signed off? David is absent so Drew will answer for QA too. — *Patricia U., Chair*

Q3. What's the blast radius if this goes wrong? — *Raj M., Ops // It's a pagination fix, Raj.*

Q4. Is the rollback plan documented? — *Alan C. // Yes. See the table above. And the wiki. And the email. And the ticket.*

Q5. Why wasn't this submitted as an emergency change to skip CAB? — *Drew P. // Great question Drew. We'll take it offline.*

3. CAB DECISION

DECISION — CHG-2026-0847

- ○ Approved
- ○ **Conditionally Approved** *(always this one)*
- ○ **Deferred** *(see you next Wed, Drew)*
- ○ **Rejected**

Spoiler: they'll ask Drew to update the wiki page again.

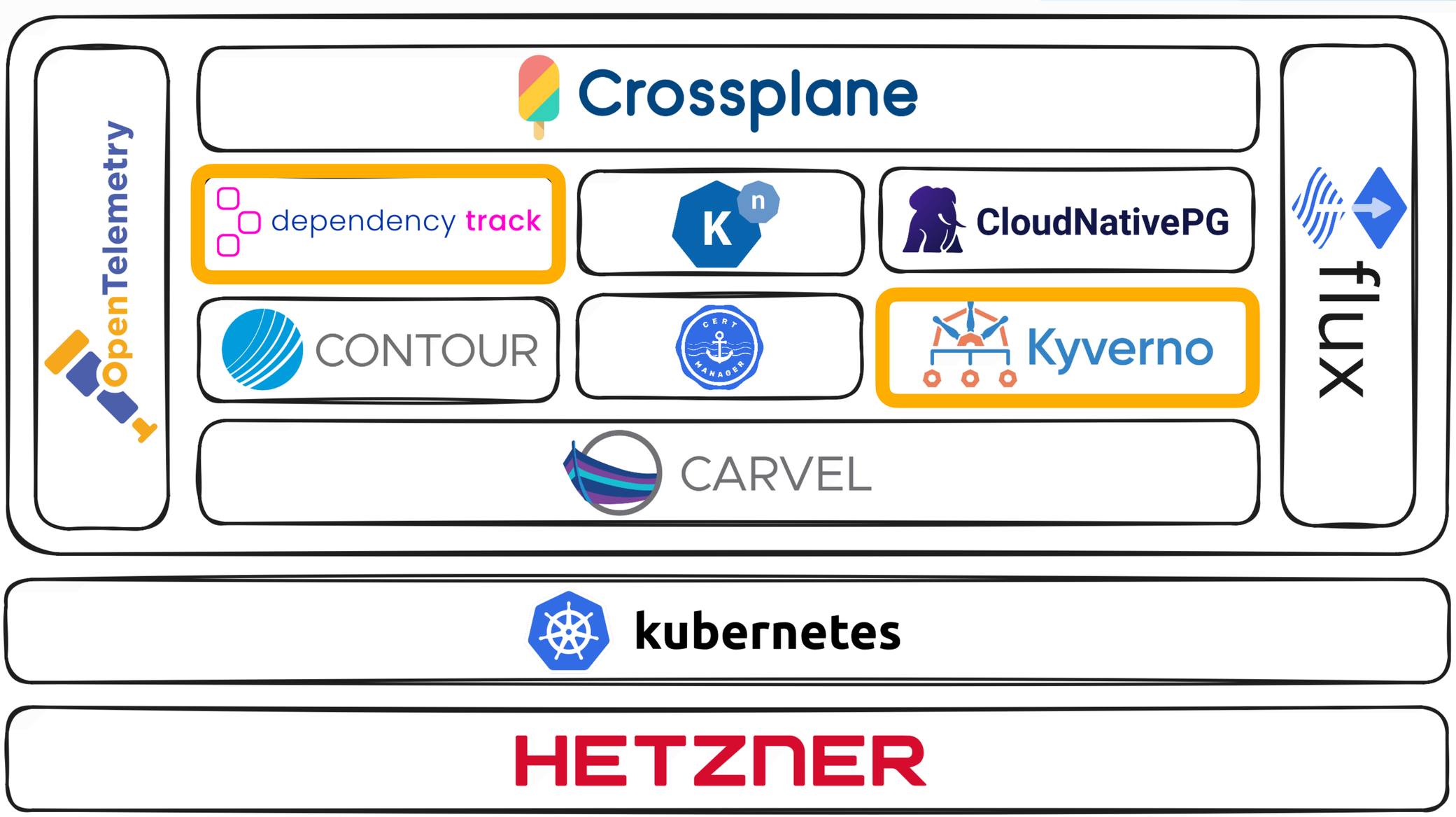


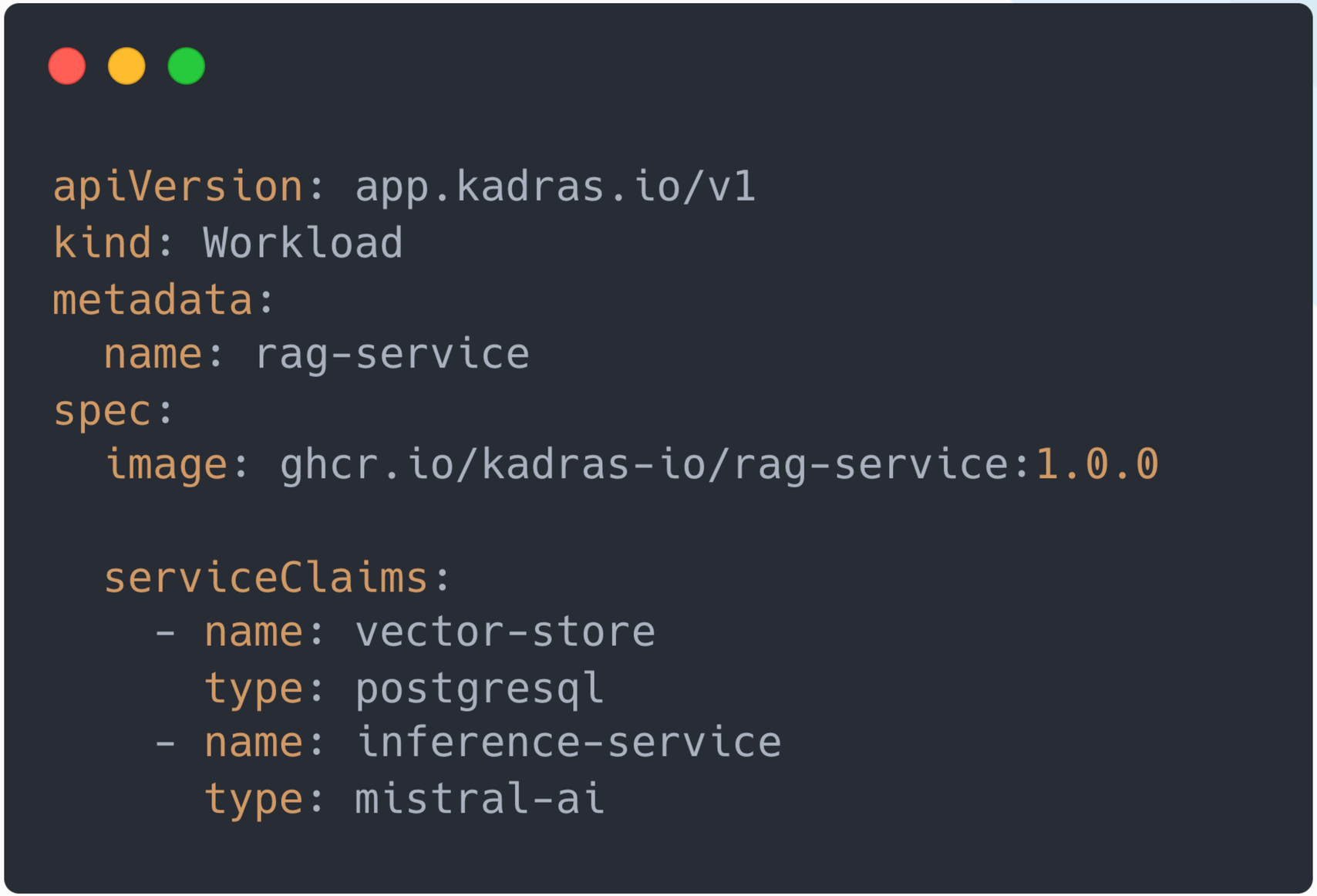
linkedin.com/in/housa

@thomasvitale.com


Do we really need
COMPLIANCE?
linkedin.com/in/housa
@thomasvitale.com

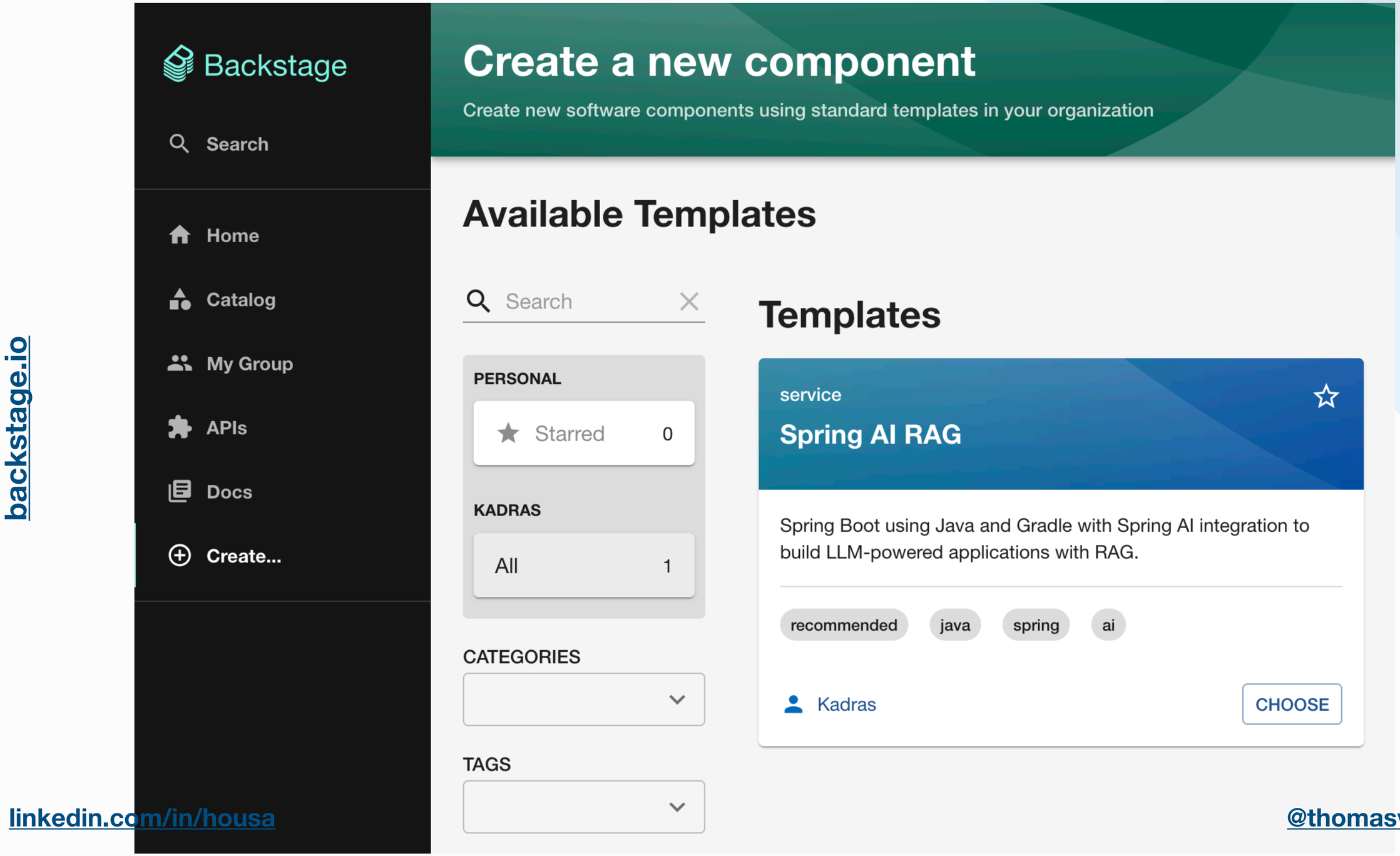

YES!
Now more than ever!
linkedin.com/in/housa
@thomasvitale.com


OpenTelemetry
Crossplane
dependency track
CloudNativePG
CONTOUR
Kyverno
CARVEL
flux
kubernetes
HETZNER



```yaml
apiVersion: app.kadras.io/v1
kind: Workload
metadata:
  name: rag-service
spec:
  image: ghcr.io/kadras-io/rag-service:1.0.0

  serviceClaims:
    - name: vector-store
      type: postgresql
    - name: inference-service
      type: mistral-ai
```



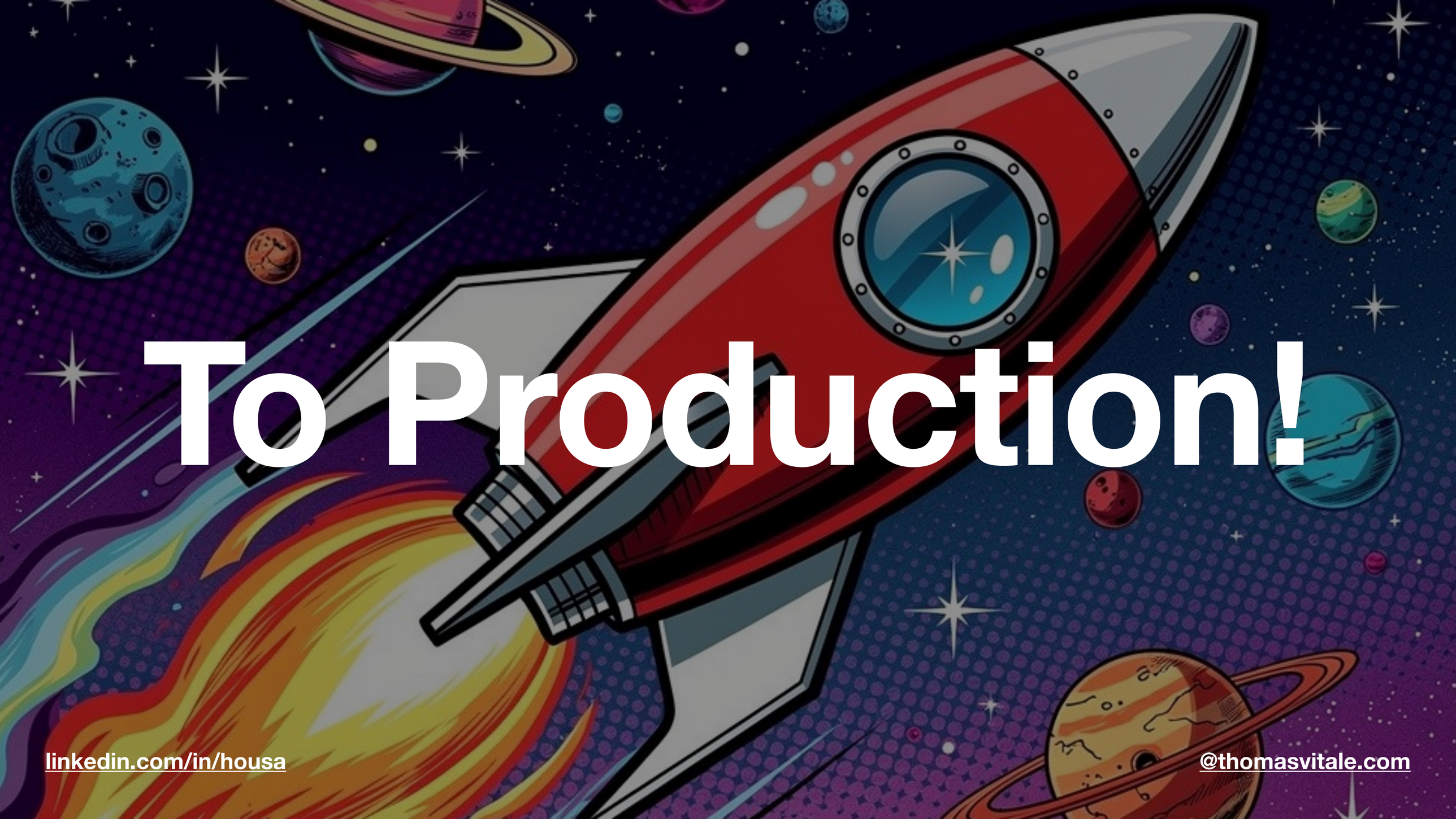
backstage.io

linkedin.com/in/housa

@thomasvitale.com


GUARDIANS
OF
COMPLIANCE
linkedin.com/in/housa
@thomasvitale.com


Can you
approve my PR?
linkedin.com/in/housa
@thomasvitale.com



linkedin.com/in/housa

@thomasvitale.com

Alexandra Aldershaab

linkedin.com/in/housa

Thomas Vitale

@thomasvitale.com

thomasvitale.com

The Developer's Nightmare

How To Survive Compliance Checklists (and Still Ship Fast)

https://github.com/ThomasVitale/developers-nightmare
https://github.com/ThomasVitale/kubecon-eu-2026-gitops