You’d better start believing in supply chains because you’re in one

Ben Cotton

YOU'D BETTER START BELIEVING IN SUPPLY CHAINS
YOU'RE IN ONE
imgflip.com

Housekeeping

Housekeeping

- **The usual disclaimers**
- **License: CC BY-SA 4.0**
- **Kind things:**
  - @FunnelFiasco.bsky.social
  - @FunnelFiasco@hachyderm.io
- **Unkind things: `/dev/null`**
- **Questions at the end**

Nobody can dislike me with the depth and precision that I bring to the table. -- John Green

Agenda

- What is a software supply chain?
- Why open source is different
- Frameworks and tools to help
- What to tell your downstreams

What is a software supply chain?

Let’s start with general supply chains

- **The inputs and efforts required to produce and deliver a product**

Your first introduction to supply chains

CC BY-SA 4.0

Toilet paper shelves empty in an Australian supermarket by Christopher Corneschi on Wikimedia Commons.

https://commons.wikimedia.org/wiki/File:Toilet_paper_shelves_empty_in_an_Australian_supermarket.jpg

Your first time laughing at supply chains

CC BY-SA 4.0

9

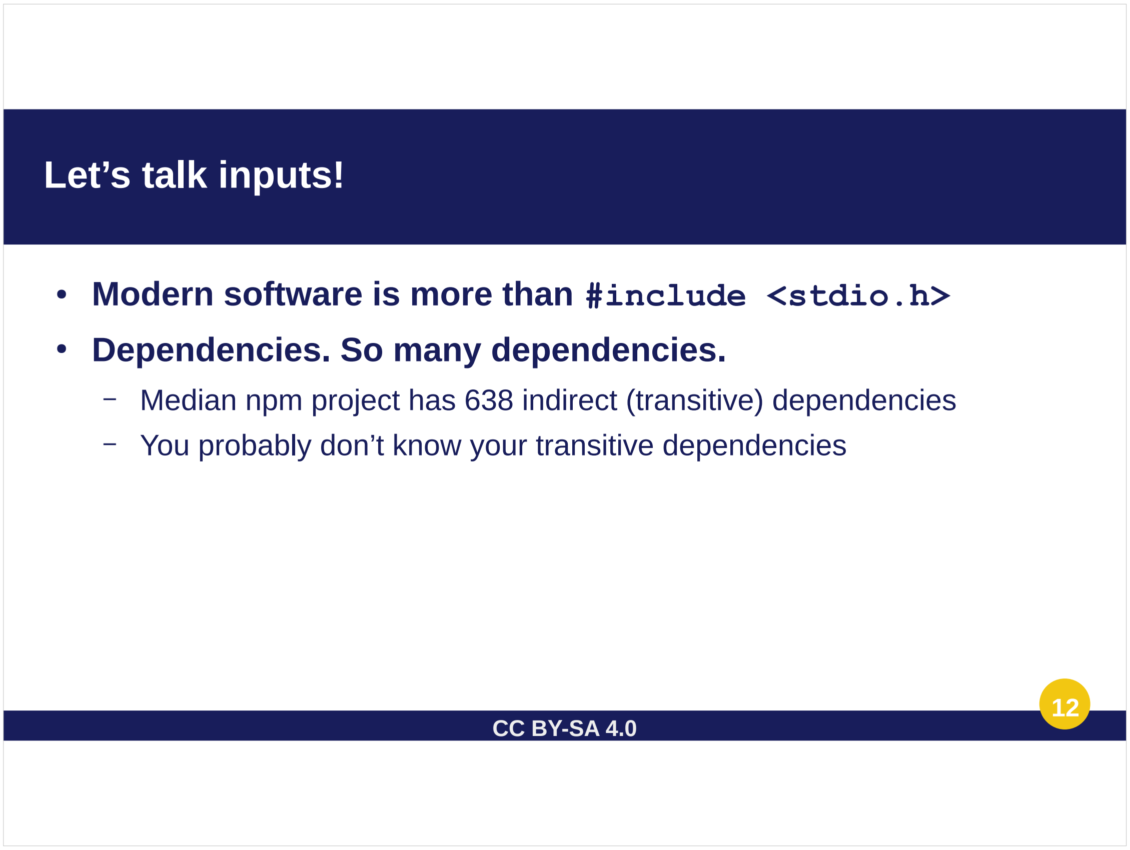
“Container Ship 'Ever Given' stuck in the Suez Canal, Egypt - March 24th, 2021” by Pierre Markuse on Wikimedia Commons

https://commons.wikimedia.org/wiki/File:Container_Ship_%27Ever_Given%27_stuck_in_the_Suez_Canal,_Egypt_-_March_24th,_2021_(51070311183).jpg

Okay, but software?

Supply chain, but make it software

- **Software has inputs and efforts!**
  - Inputs: dependencies, first-party software, tooling
  - Efforts: development, testing, building, deploying, etc
- **Software is people**
  - In-house developers, testers, DevOps engineers, …
  - Contractors
  - Vendors
  - ...



Let’s talk inputs!

- **Modern software is more than `#include <stdio.h>`**
- **Dependencies. So many dependencies.**
  - Median npm project has 638 indirect (transitive) dependencies
  - You probably don’t know your transitive dependencies

Source: https://octoverse.github.com/2020/

Why open source is different

Why open source is different

“Software is provided AS-IS”

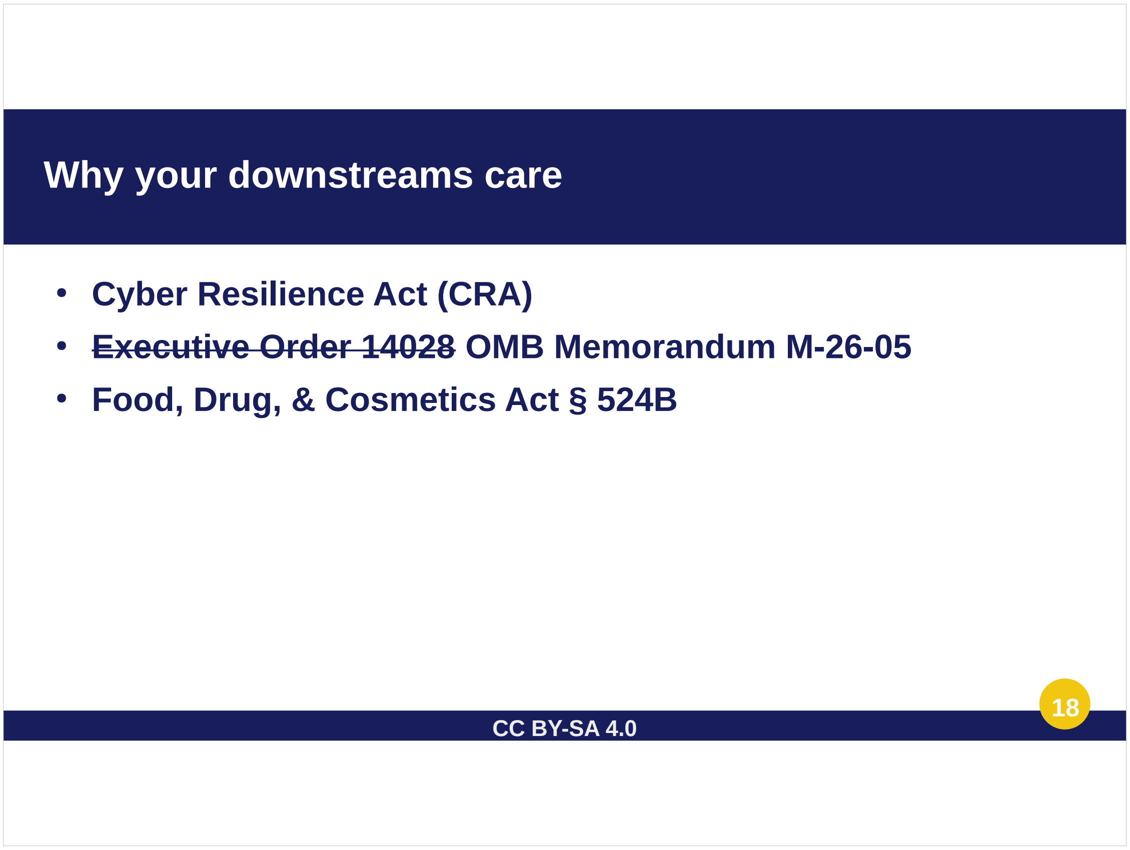
Why open source is different

There’s no bi-directional relationship
(a.k.a. “I am not a supplier”)

Why open source is different

“I thought this was supposed to be fun!”

Why your downstreams care



Why your downstreams care

- Cyber Resilience Act (CRA)
- ~~Executive Order 14028~~ OMB Memorandum M-26-05
- Food, Drug, & Cosmetics Act § 524B

https://digital-strategy.ec.europa.eu/en/policies/cyber-resilience-act

https://www.whitehouse.gov/wp-content/uploads/2026/01/M-26-05-Adopting-a-Risk-based-Approach-to-Software-and-Hardware-Security.pdf

https://www.fda.gov/medical-devices/digital-health-center-excellence/cybersecurity-medical-devices-frequently-asked-questions-faq

Why volunteer* maintainers should care

Why volunteer maintainers should care

Maybe they shouldn’t?

Why volunteer maintainers should care

If people use your software in ways you say not to, that’s a Them Problem™

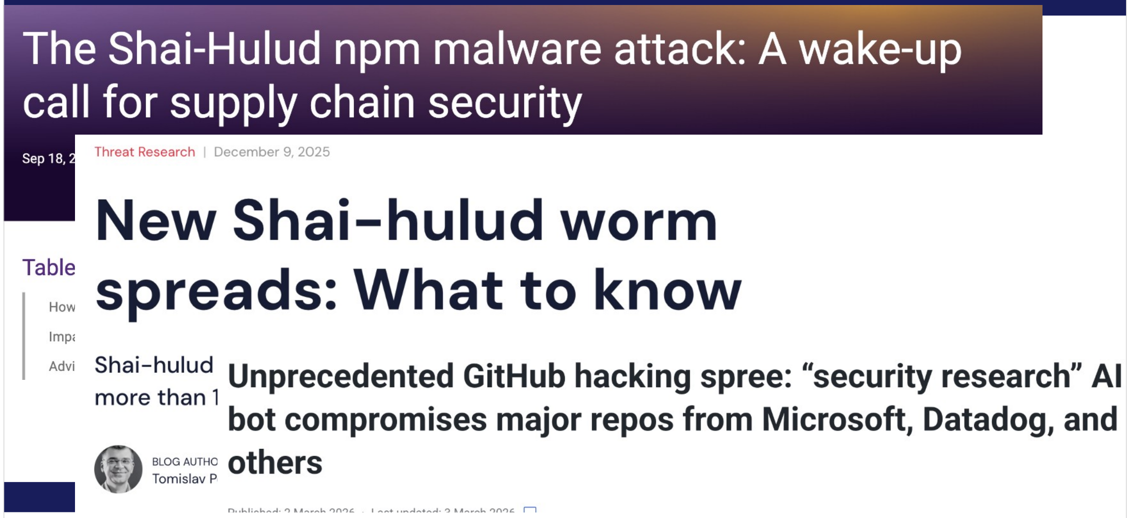
Why volunteer maintainers should care

But you probably should

An analogy!

An analogy!

We’re all in this together



The Shai-Hulud npm malware attack: A wake-up call for supply chain security

Sep 18, 2

Table

How

Impa

Advi

Threat Research | December 9, 2025

New Shai-hulud worm spreads: What to know

Shai-hulud

more than 1

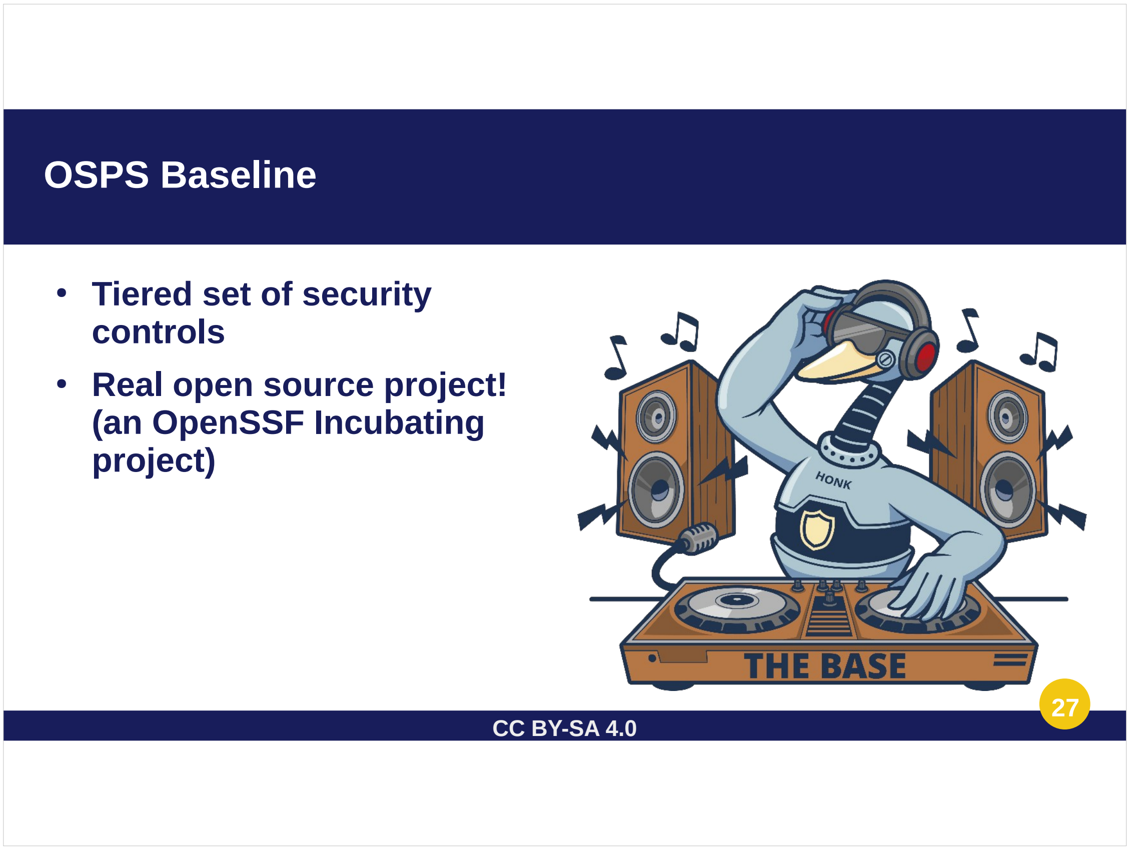
BLOG AUTHO

Tomislav P

Unprecedented GitHub hacking spree: “security research” AI bot compromises major repos from Microsoft, Datadog, and others

Published: 2 March 2026 · Last updated: 3 March 2026

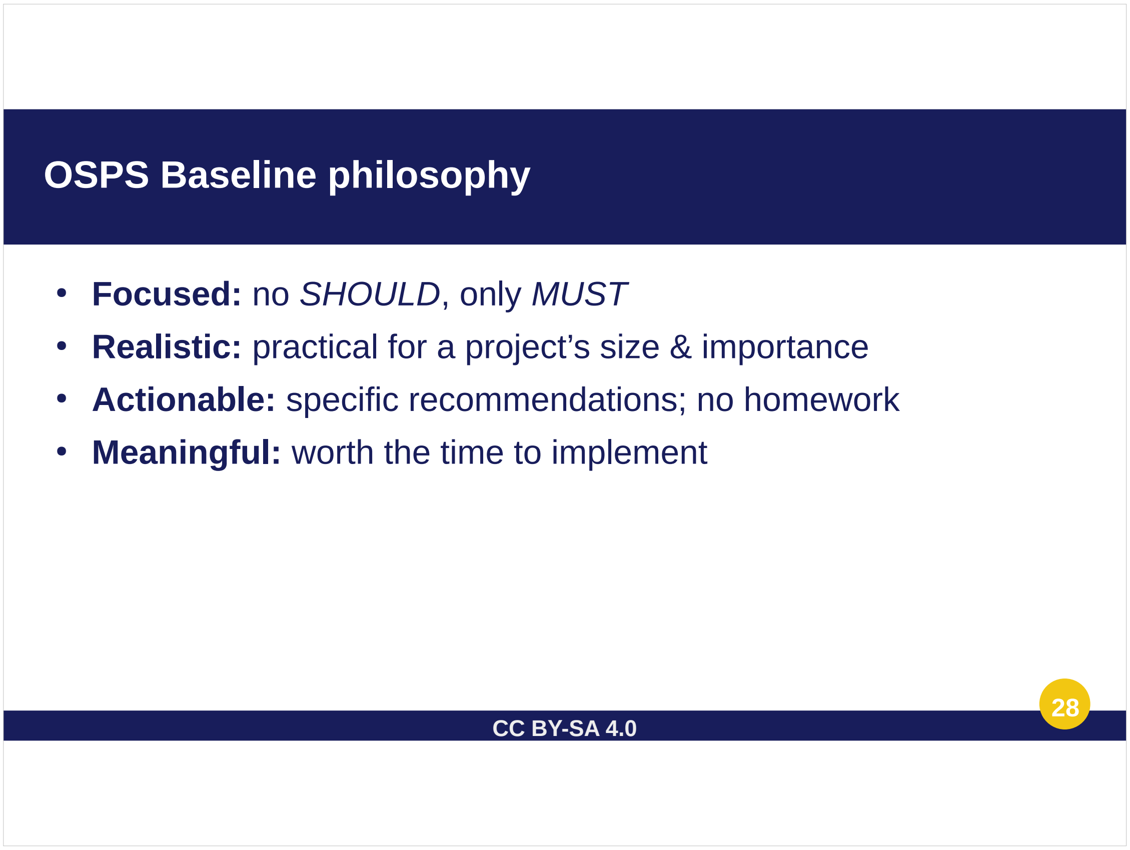
So what’s a maintainer to do?



OSPS Baseline

- Tiered set of security controls
- Real open source project! (an OpenSSF Incubating project)

Image by OpenSSF under ASL 2.0



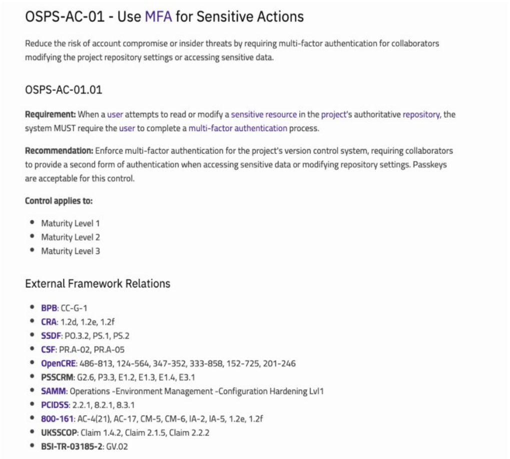
OSPS Baseline philosophy

- **Focused:** no *SHOULD*, only *MUST*
- **Realistic:** practical for a project’s size & importance
- **Actionable:** specific recommendations; no homework
- **Meaningful:** worth the time to implement

OSPS Baseline levels

1) For any code or non-code project with any number of maintainers or users
2) For any code project that has at least 2 maintainers and a small number of consistent users
3) For any code project that has a large number of consistent users

OSPS Baseline example



OSPS-AC-01 - Use MFA for Sensitive Actions

Reduce the risk of account compromise or insider threats by requiring multi-factor authentication for collaborators modifying the project repository settings or accessing sensitive data.

OSPS-AC-01.01

Requirement: When a user attempts to read or modify a sensitive resource in the project's authoritative repository, the system MUST require the user to complete a multi-factor authentication process.

Recommendation: Enforce multi-factor authentication for the project's version control system, requiring collaborators to provide a second form of authentication when accessing sensitive data or modifying repository settings. Passkeys are acceptable for this control.

Control applies to:

- Maturity Level 1
- Maturity Level 2
- Maturity Level 3

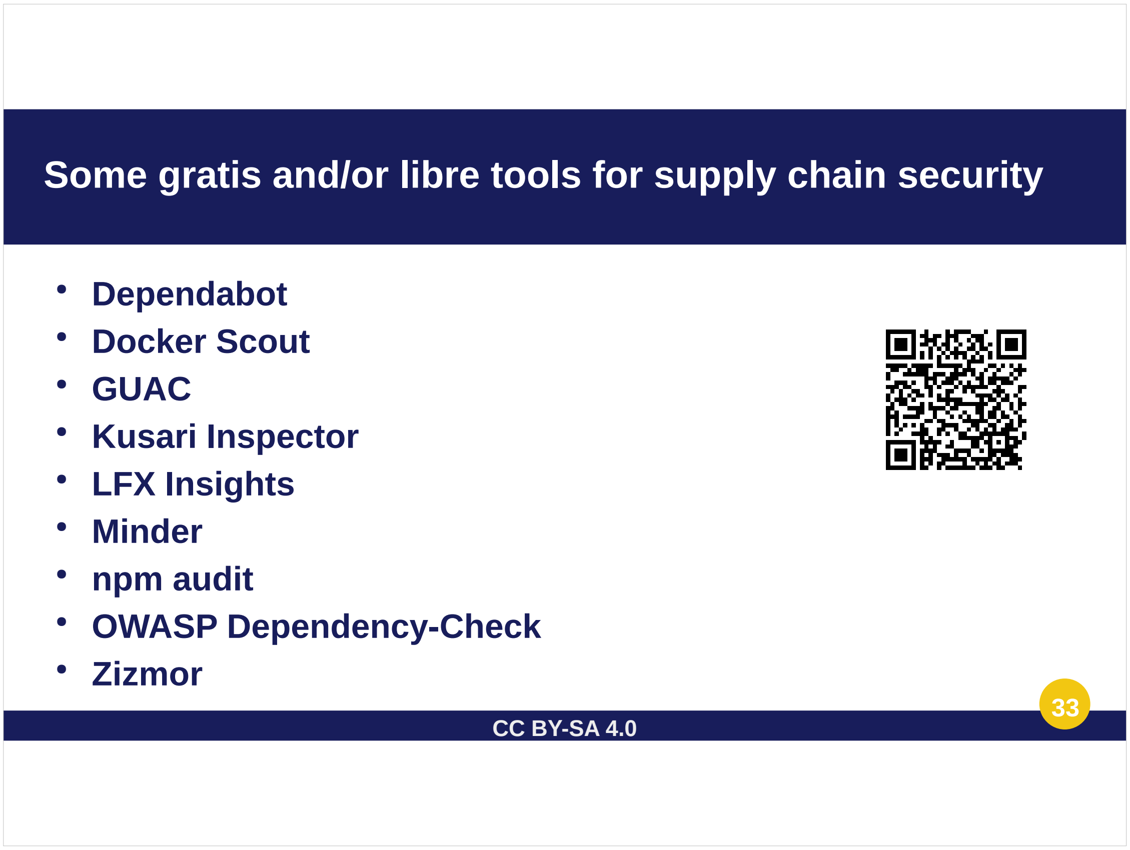
External Framework Relations

- **BPB**: CC-G-1
- **CRA**: 1.2d, 1.2e, 1.2f
- **SSDF**: PO.3.2, PS.1, PS.2
- **CSF**: PR.A-02, PR.A-05
- **OpenCRE**: 486-813, 124-564, 347-352, 333-858, 152-725, 201-246
- **PSSCRM**: G2.6, P3.3, E1.2, E1.3, E1.4, E3.1
- **SAMM**: Operations -Environment Management -Configuration Hardening Lvl1
- **PCIDSS**: 2.2.1, 8.2.1, 8.3.1
- **800-161**: AC-4(21), AC-17, CM-5, CM-6, IA-2, IA-5, 1.2e, 1.2f
- **UKSSCOP**: Claim 1.4.2, Claim 2.1.5, Claim 2.2.2
- **BSI-TR-03185-2**: GV.02

Some basic steps

- Update your dependencies (but not too quickly)
- Check into new dependencies
- Two-factor authentication
- Trusted Publishers
- (GitHub) Enable Immutable Releases

Tools to help you along the way



Some gratis and/or libre tools for supply chain security

- Dependabot
- Docker Scout
- GUAC
- Kusari Inspector
- LFX Insights
- Minder
- npm audit
- OWASP Dependency-Check
- Zizmor

https://docs.github.com/en/code-security/tutorials/secure-your-dependencies/dependabot-quickstart-guide
https://www.docker.com/products/docker-scout/
https://guac.sh/
https://www.kusari.dev/developers
https://insights.linuxfoundation.org/
https://mindersec.dev/
https://docs.npmjs.com/cli/v7/commands/npm-audit
https://owasp.org/www-project-dependency-check/
https://zizmor.sh/

“Hello, you are my supplier.
Please do my homework.”

Valid responses

- (cricket noises)
- “No”
- “Okay, here’s an invoice”
- “We meet OSPS Baseline level x. If you need more, see above.”
- (be super helpful and give them everything they ask for)

Let’s talk about it

Find me online!

- https://duckalignment.academy
- https://funnelfiasco.com/blog
- Email: bcotton@funnelfiasco.com
- Bluesky: @funnelfiasco.bsky.social
- Mastodon: @funnelfiasco@hachyderm.io