Free Fish Aren’t Free

Agenda

1. Who?
2. Wat?
3. Why?
4. How?

1. Who?

- CRob, n, adj, and v
  - Pronunciation: U.S. (K-robe)
- Over 20 years of Enterprise-class Architecture, Engineering, Operations, and Security experience
- Ambassador of Red Hat Product Security
- Participant in the FIRST PSIRT SIG, VulnCoord SIG, and others
- Co-Author FIRST PSIRT Services Framework
- Pirate-enthusiast & hat-owner

2.
WAT?

Pop Quiz! (yay!)

Who here knows they use OSS in their Enterprises?

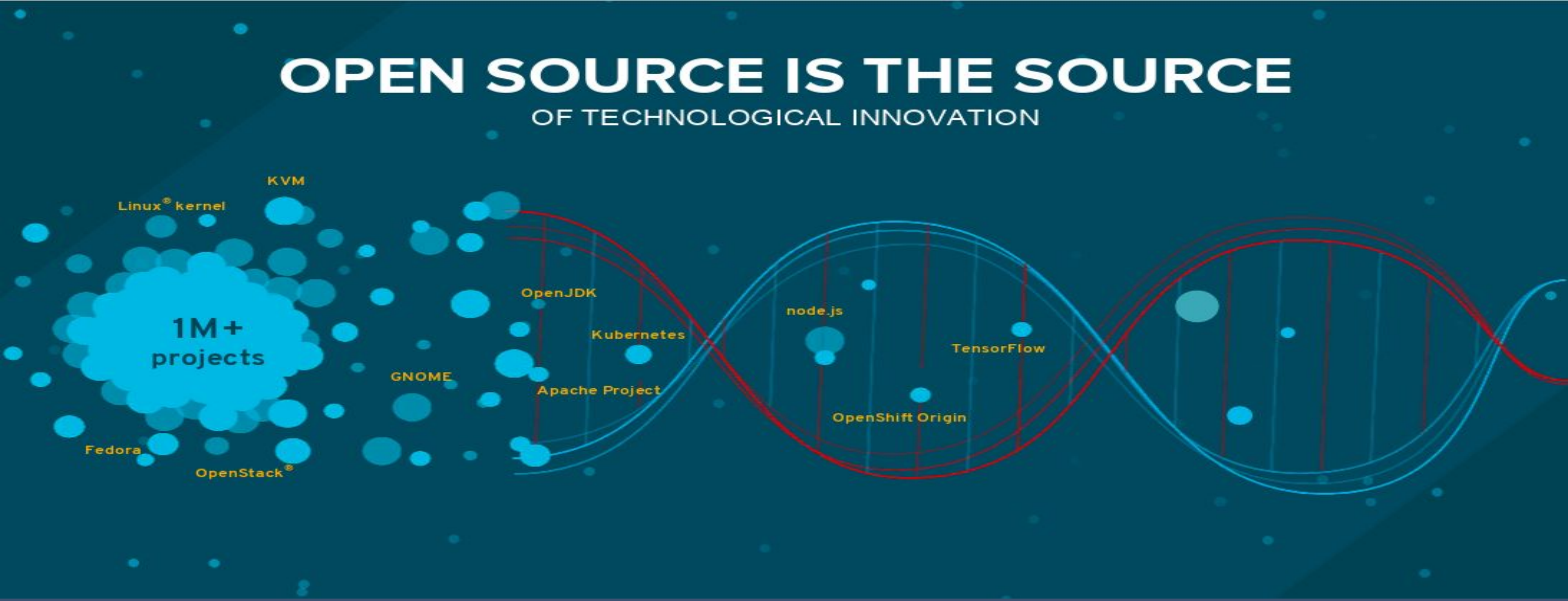
Who thinks they don’t have ANY OSS on their network?

Open Source “won”

Yay us!

Why?

Speed
Agility
Innovation
Powerful ability to configure for-purpose
Penguins
Awesome black and green screens



> *“Blah, Blah, Blah, Marketing slide, Blah, Innovation, Blah, plus tax”*
> *- CRob*

https://octoverse.github.com/ - GitHub reports over **96mil** projects with active utilization in 2018

"open source" refers to something people can modify and share because its design is publicly accessible.[1]

It's FREE, so it MUST be good, right?

1 - https://opensource.com/resources/what-open-source

CLOSED SOURCE

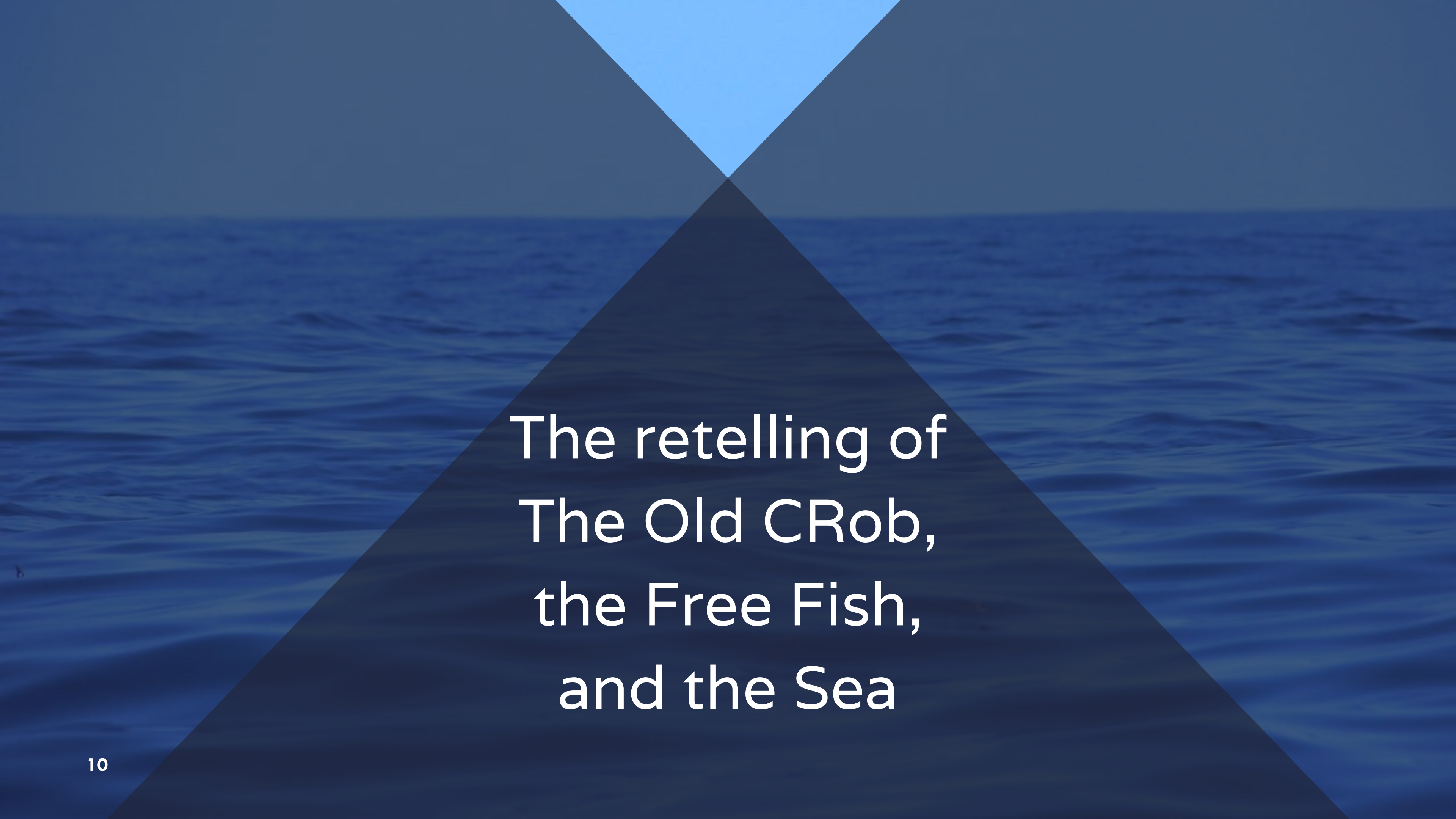
- “Traditional” Software.
- Probably single-supplier.
- Unknown practices to create, package, & deploy products (might have great docs to share)
- “One throat to choke” for support, updates, etc
- Might be embedding/using OSS….

Think: “Waterfall”

OPEN SOURCE

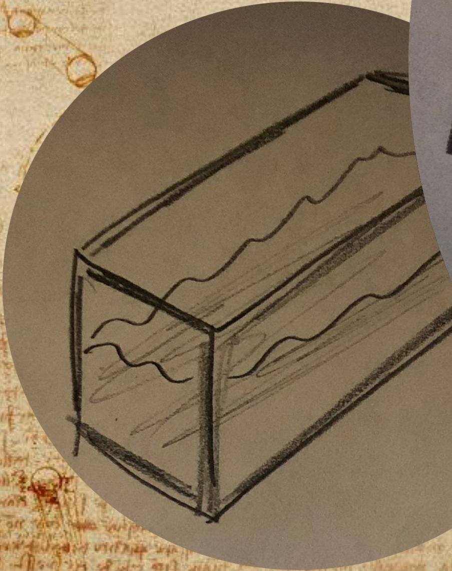
- “New” software model with different processes/practices
- Multiple contributors
- Open and auditable processes and code (that YOU can go audit)
- Rarely a single source for support and updates
- Depending on size/maturity of “team” varying levels of quality

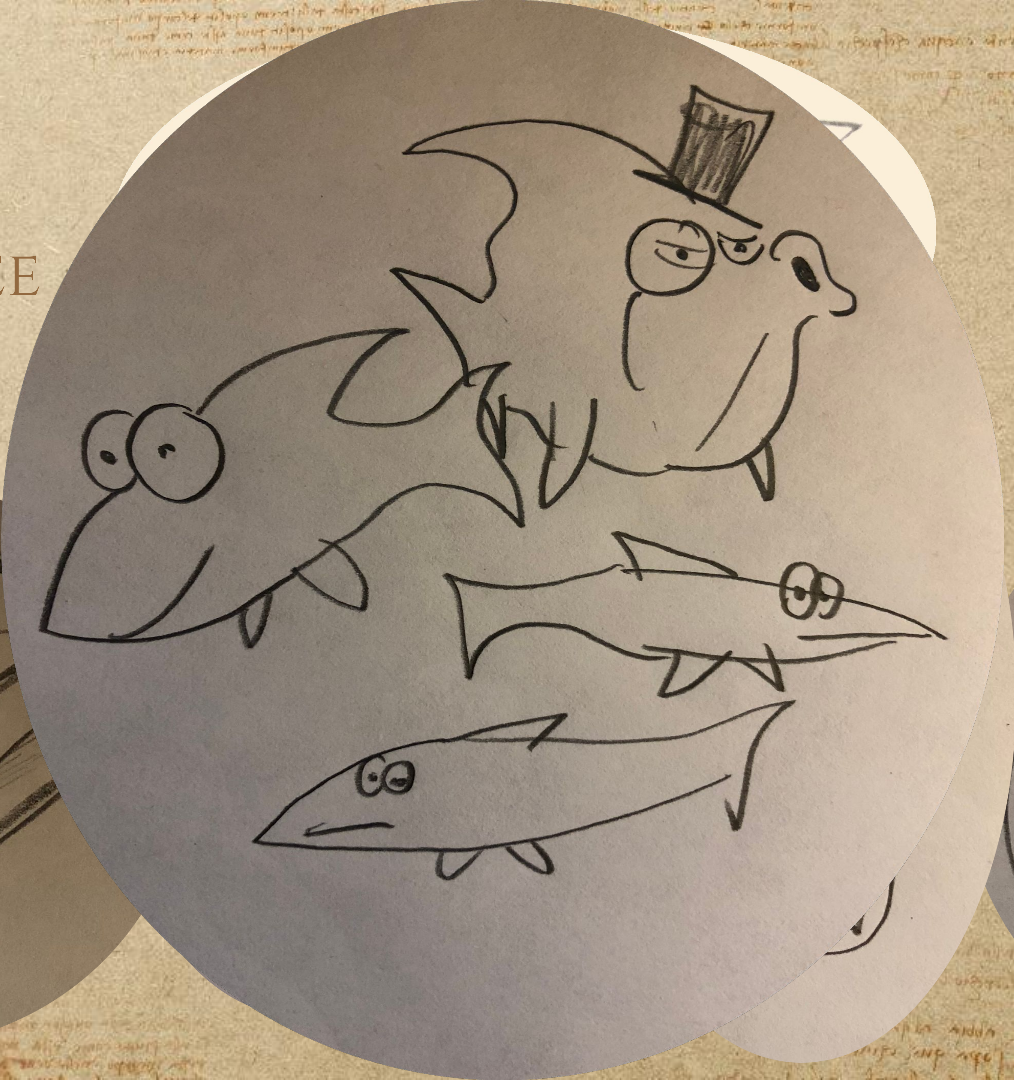
Think: “Agile”, but with stronger opinions



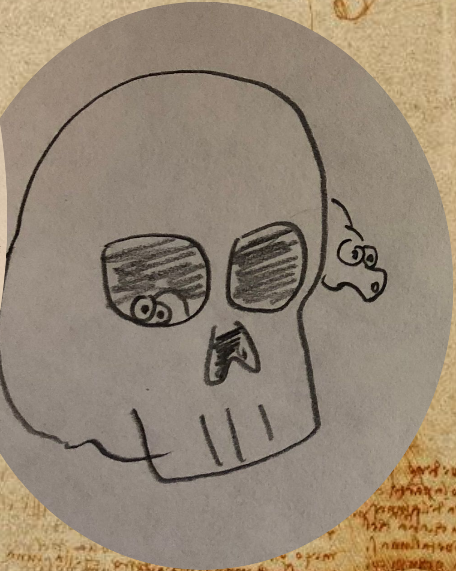
The retelling of The Old CRob, the Free Fish, and the Sea

CRob’s “free fish” bill:





>$200 USD



The moral

Open Source is kinda like a free fish

You generally have extra work to do around the fish.

It can be pretty cool (that bubbly pirate chest was THA AWESOMES)!

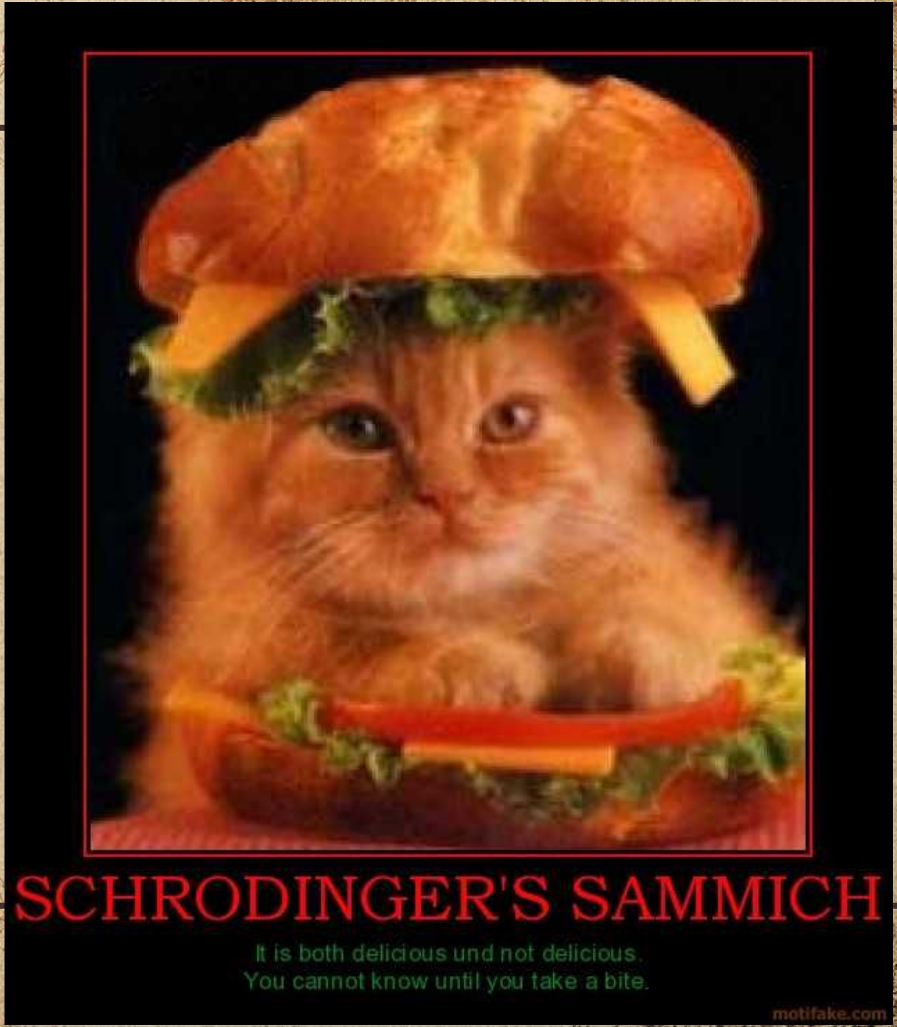
If you leave a 12 yr old to oversee it it's GOING to die. <--**FACT**

.... In other words, with a little bit of effort, it can be beautiful, but it takes work!

3.
WHY?

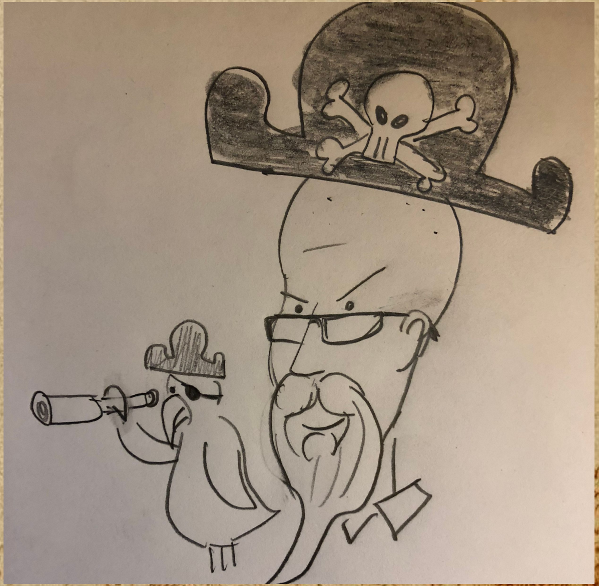
a.) What’s on the inside?

The Sandwich Paradox


SCHRODINGER'S SAMMICH
It is both delicious und not delicious.
You cannot know until you take a bite.
motifake.com

What's in the sammich and how it was made matter

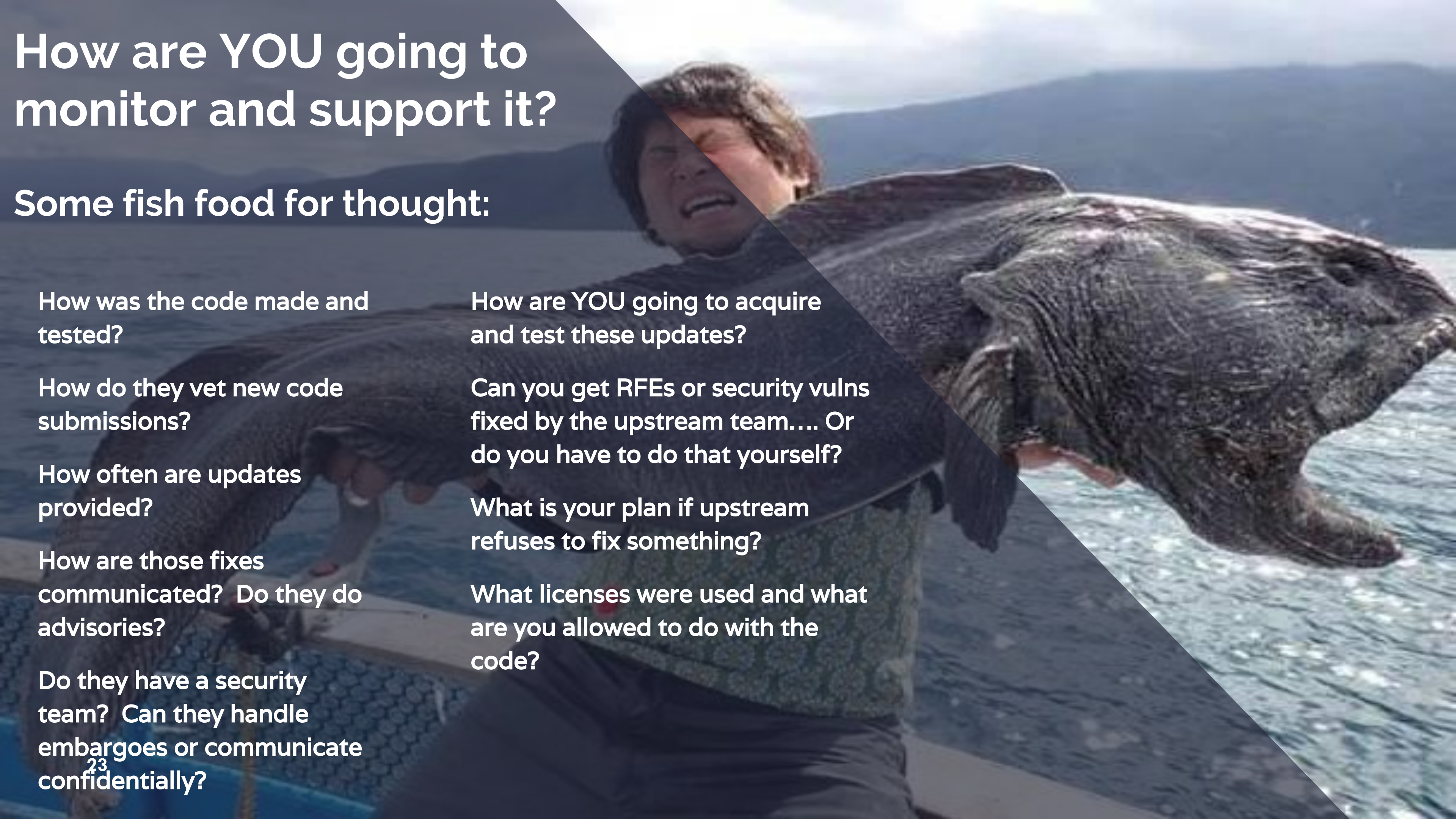
- Chain of custody/package ancestry matter
- Trusted builds by trusted maintainers on protected infrastructure
- Changes documented and tracked
- Signed with authorized_keys



How do you know what’s in that package you just installed?

b.) Who made it and how is it going to be supported?

How are YOU going to monitor and support it?



Some fish food for thought:

How was the code made and tested?

How do they vet new code submissions?

How often are updates provided?

How are those fixes communicated? Do they do advisories?

Do they have a security team? Can they handle embargoes or communicate confidentially?

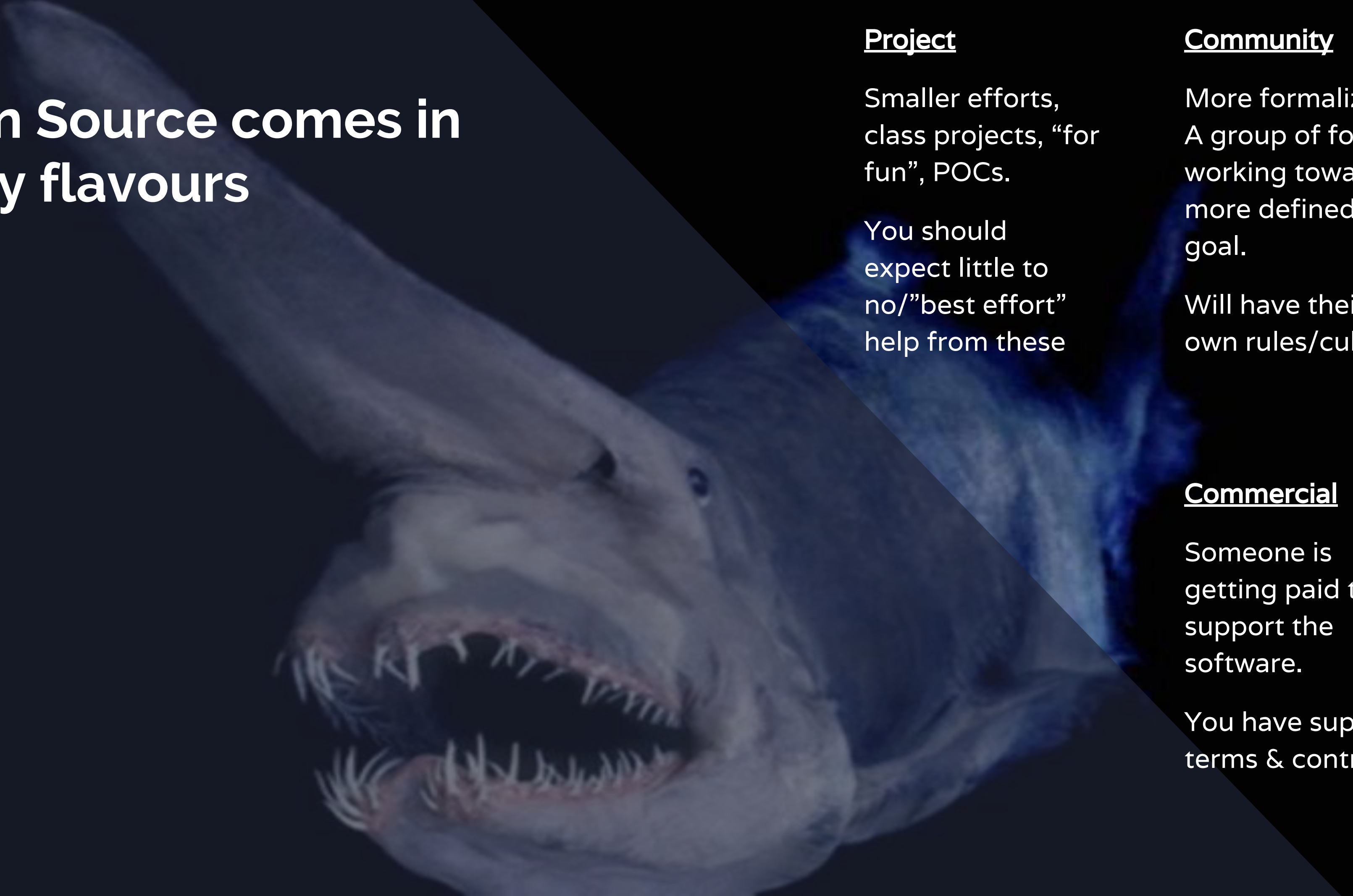
How are YOU going to acquire and test these updates?

Can you get RFEs or security vulns fixed by the upstream team…. Or do you have to do that yourself?

What is your plan if upstream refuses to fix something?

What licenses were used and what are you allowed to do with the code?

Open Source comes in many flavours



Project

Smaller efforts, class projects, “for fun”, POCs.

You should expect little to no/”best effort” help from these

Community

More formalized. A group of folks working towards a more defined goal.

Will have their own rules/culture

Commercial

Someone is getting paid to support the software.

You have support terms & contracts

Risk? Wut Risk?

Uncontrollable upstream

Unknown Contributors

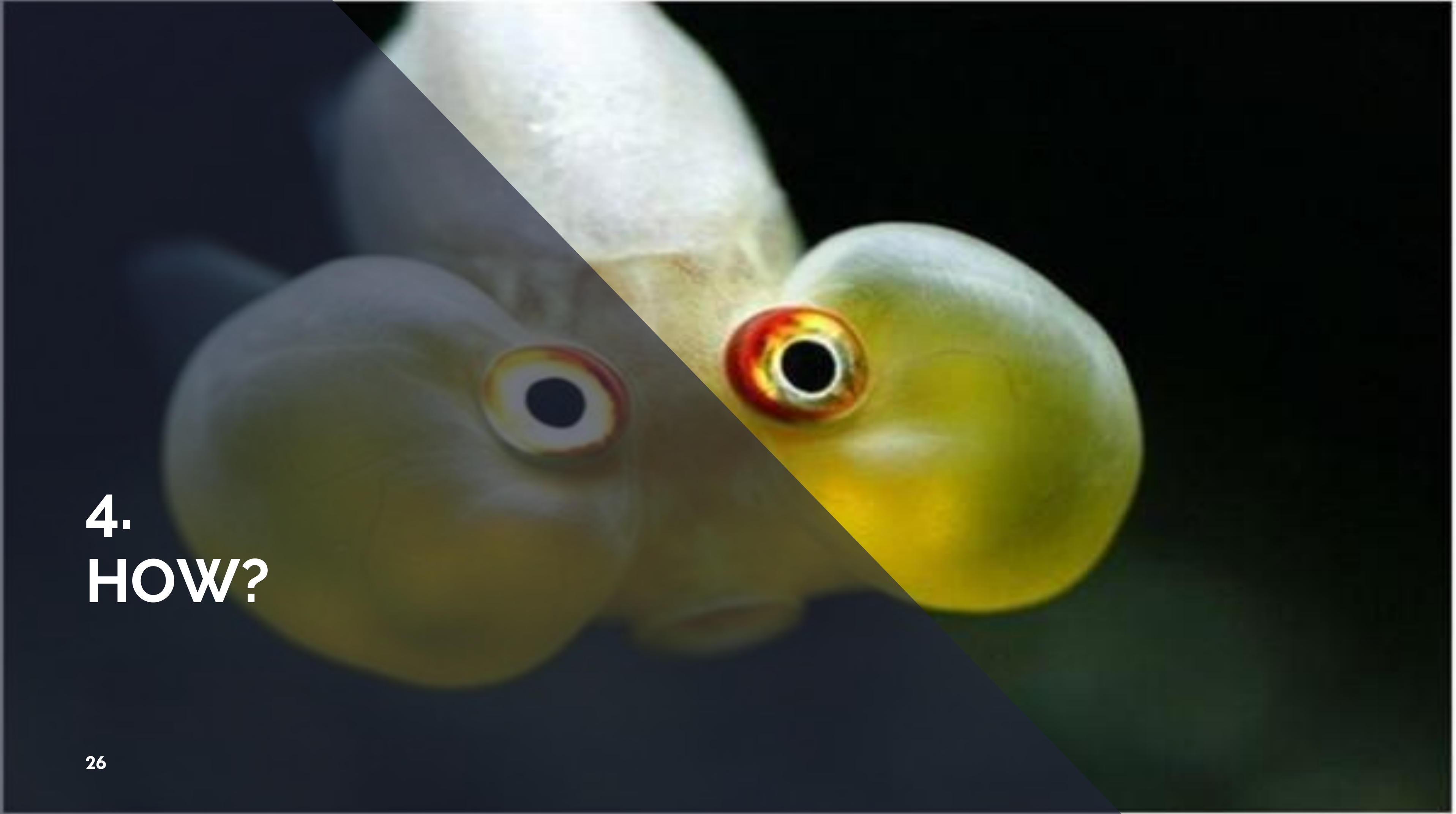
Immature project

Change in Technical direction

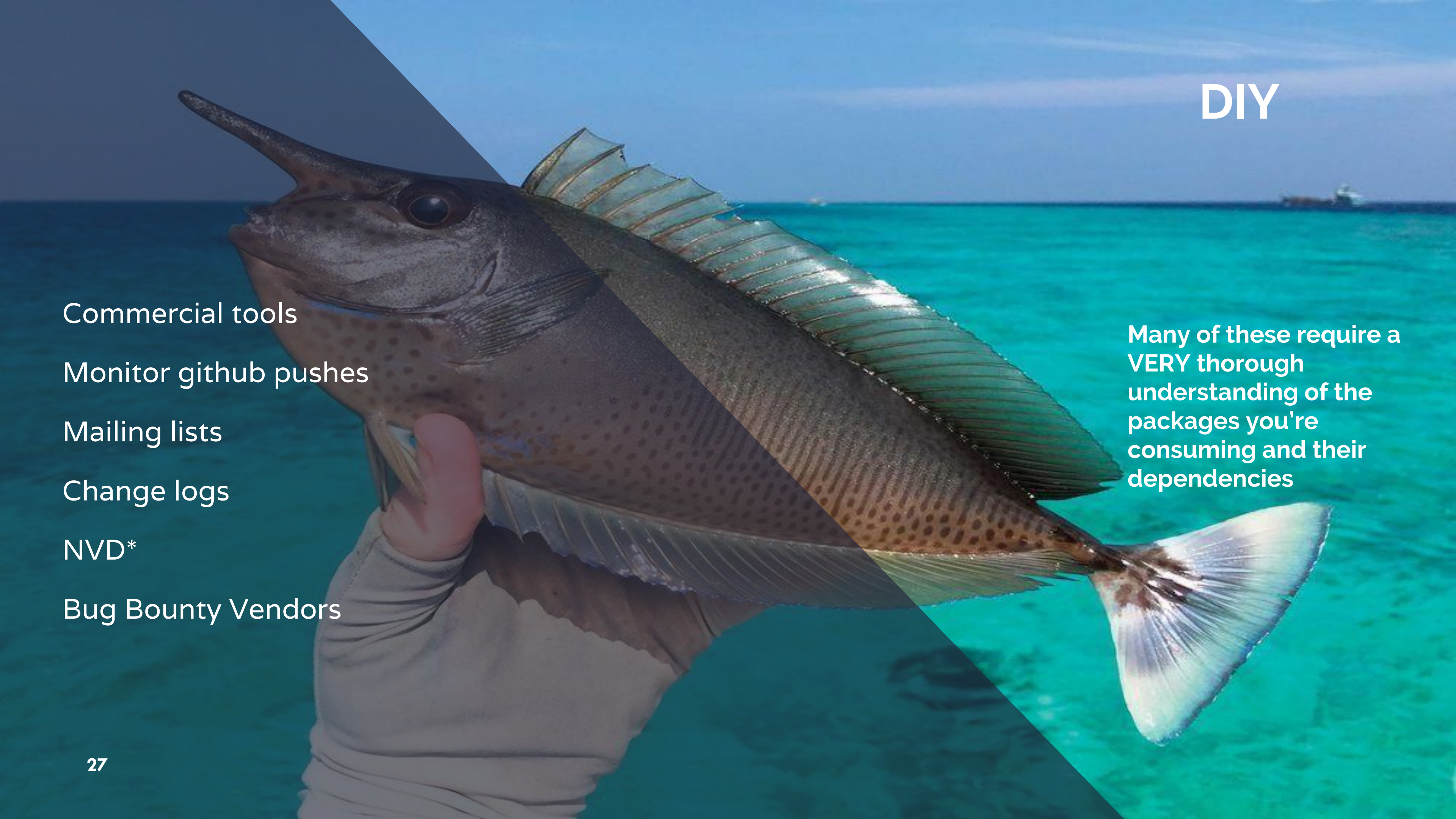
Abandoned Project

Lack of Security team or mindset

Unknown contents



4.
HOW?



DIY

Commercial tools

Monitor github pushes

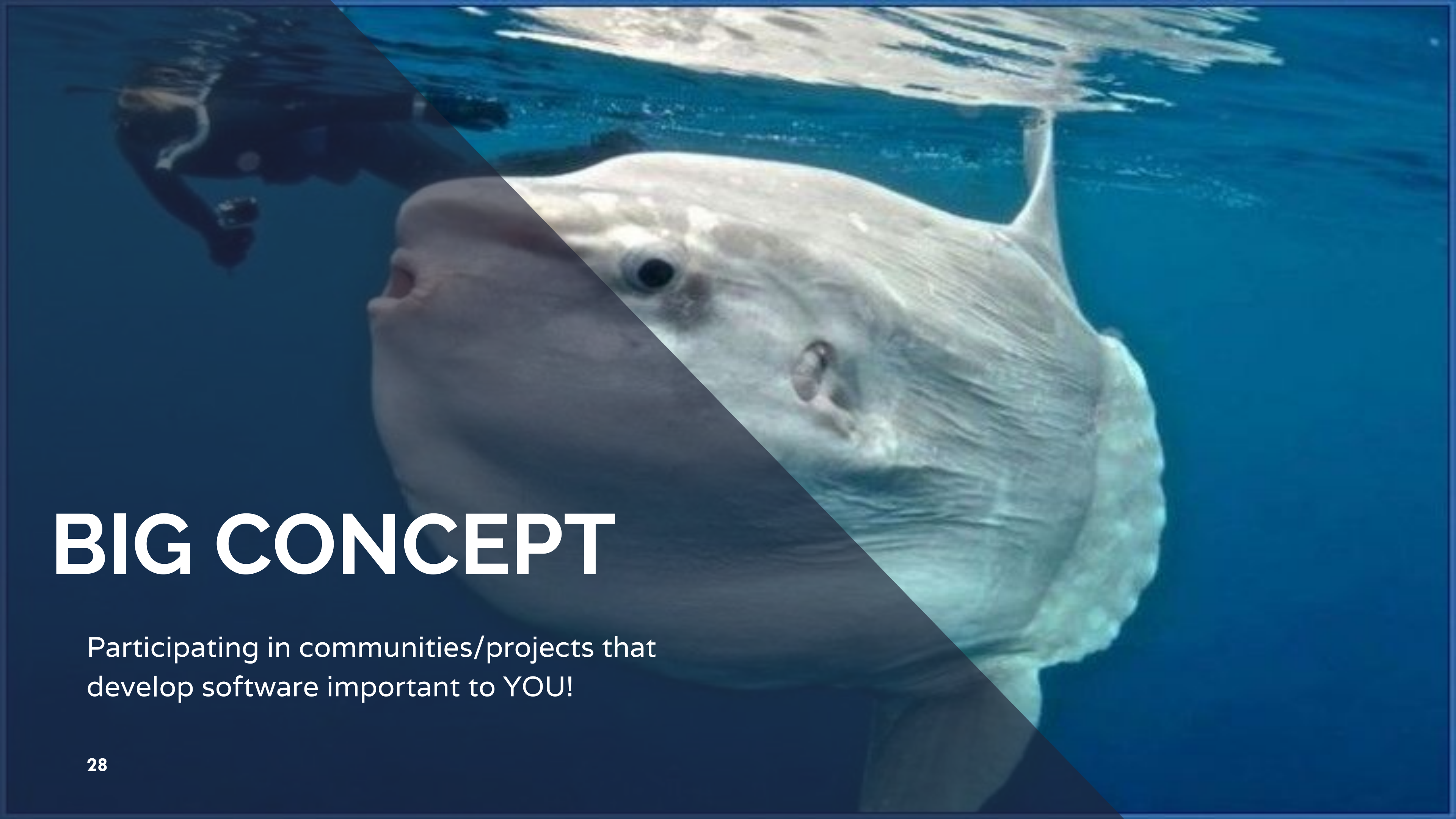
Mailing lists

Change logs

NVD*

Bug Bounty Vendors

Many of these require a VERY thorough understanding of the packages you’re consuming and their dependencies



BIG CONCEPT

Participating in communities/projects that develop software important to YOU!

BIG CONCEPT

...OR… find a friend to help you out.

Commercial OSS Support - *Free software for a Fee*

Your mileage may vary, but in general, what you should expect -

Trusted/reproducible builds

Regression/security testing

Contracts to support you

License indemnification

A Product Security Team

Questions

Free Fish Aren't Free

Thanks!

✉ CRob_at_RedHat_dot_com

@RedHatCRob

OUR PROCESS IS EASY

Animated by +Dunken K Bliths

first

second

last