

A person in a dark jacket and shorts stands on a rocky shore, looking out at the ocean during a sunset. The sun is low on the horizon, creating a bright orange glow and a reflection on the water. The sky is filled with dark, dramatic clouds. The scene is split by a diagonal line, with the left side being darker and the right side showing the sunset. The text "Free Fish Aren't Free" is overlaid on the bottom left.

**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?



# Why?

Speed

Agility

Innovation

Powerful ability to configure for-purpose

Penguins

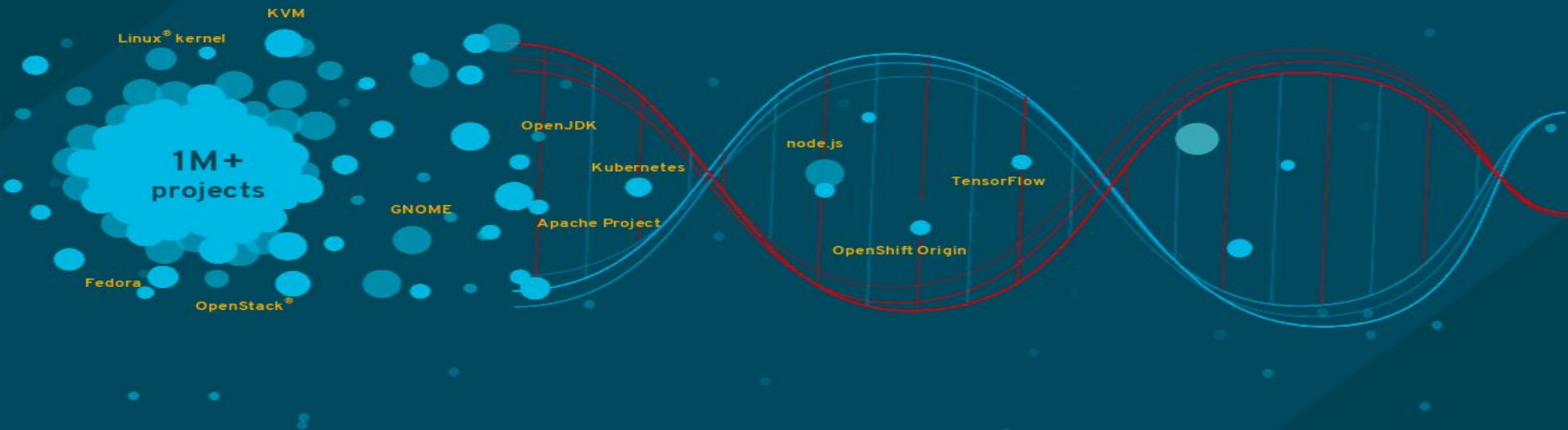
Awesome black and green screens

Open Source  
“won”

Yay us!

# OPEN SOURCE IS THE SOURCE

OF TECHNOLOGICAL INNOVATION



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



**"open source"  
refers to  
something  
people can  
modify and share  
because its  
design is publicly  
accessible.<sup>1</sup>**

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





## ***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....

9

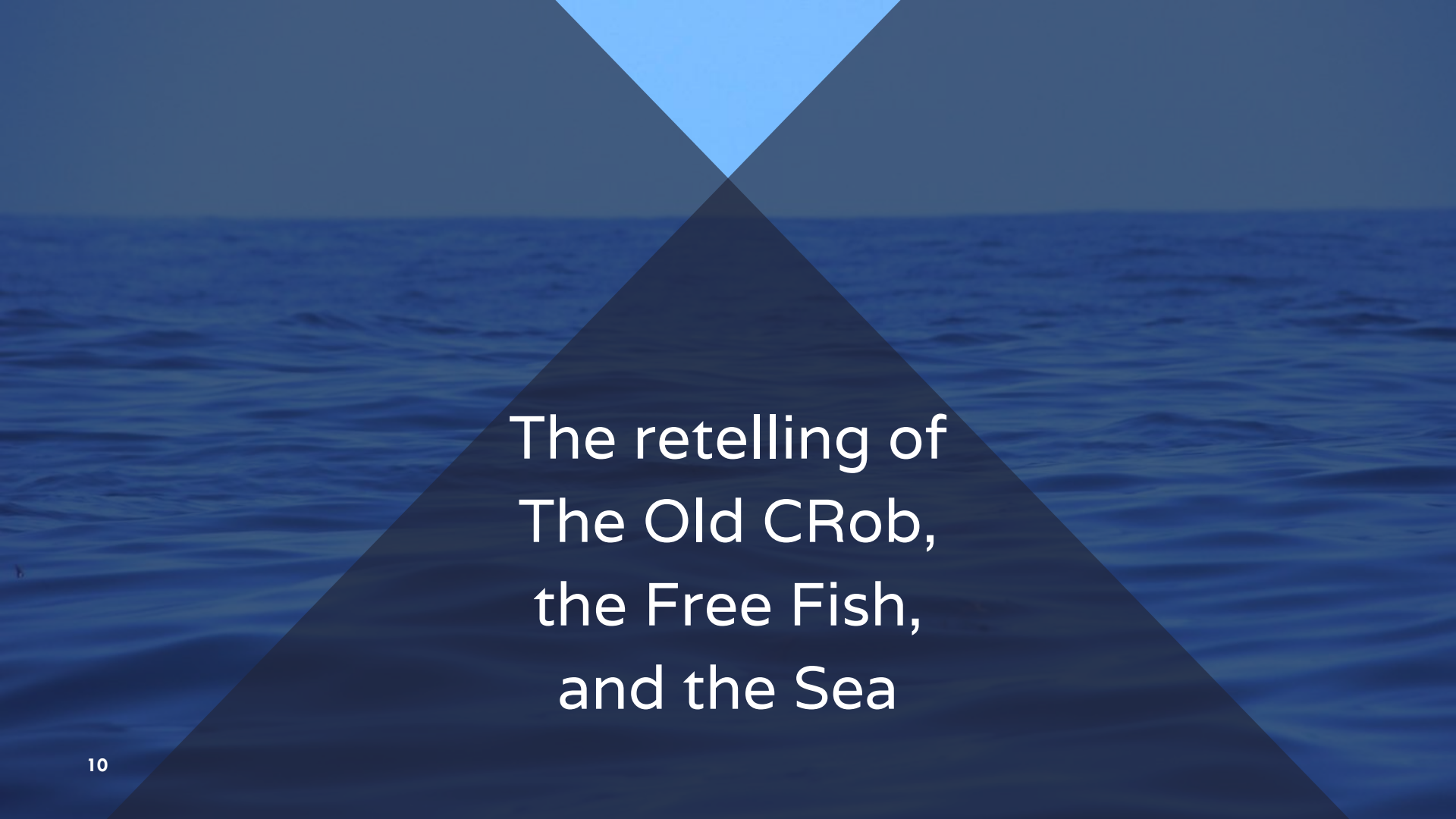
*Think: “Waterfall”*



## ***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*

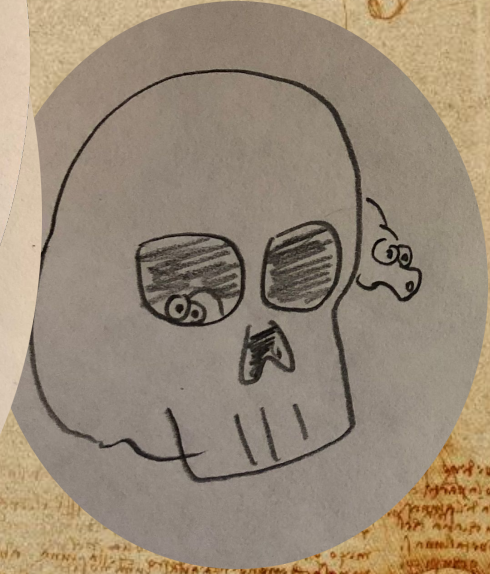
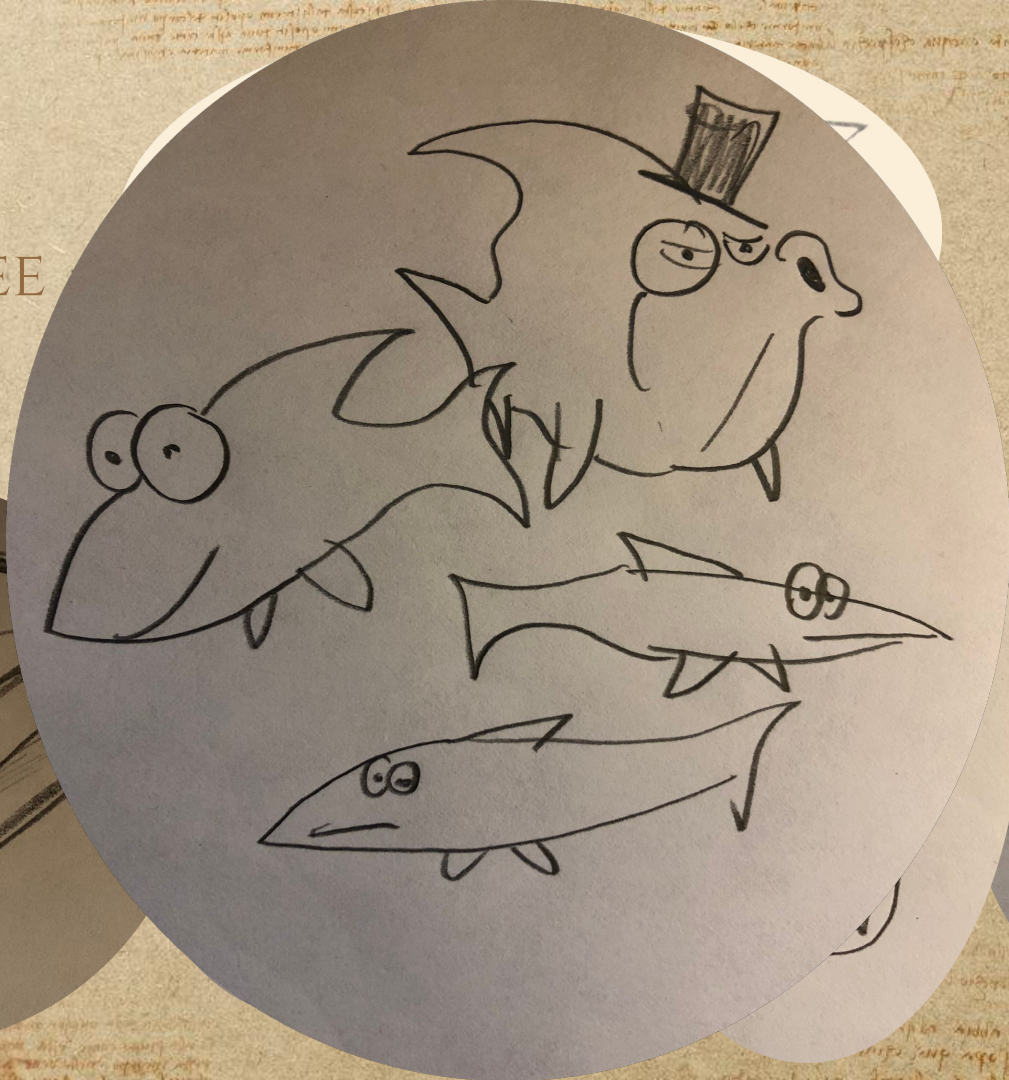
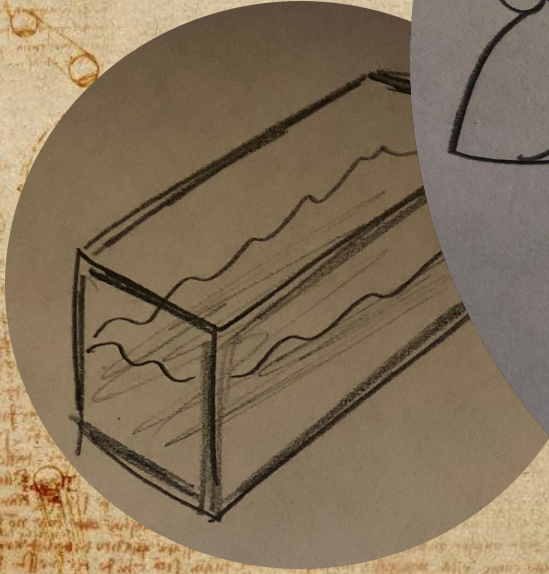


The retelling of  
The Old CRob,  
the Free Fish,  
and the Sea



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!



Faint, illegible text is visible in the background, appearing as bleed-through from the reverse side of the page. The text is scattered across the top and sides of the page, with some words like "water" and "fish" being partially legible.



### 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.

# WHAT'S IN THE SAMMICH AND HOW IT WAS MADE MATTER

---



CHAIN OF CUSTODY/PACKAGE ANCESTRY MATTER



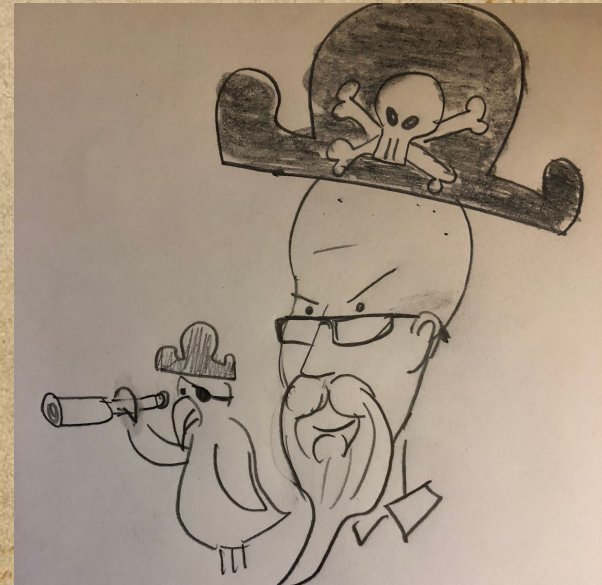
TRUSTED BUILDS BY TRUSTED MAINTAINERS ON PROTECTED  
INFRASTRUCTURE



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

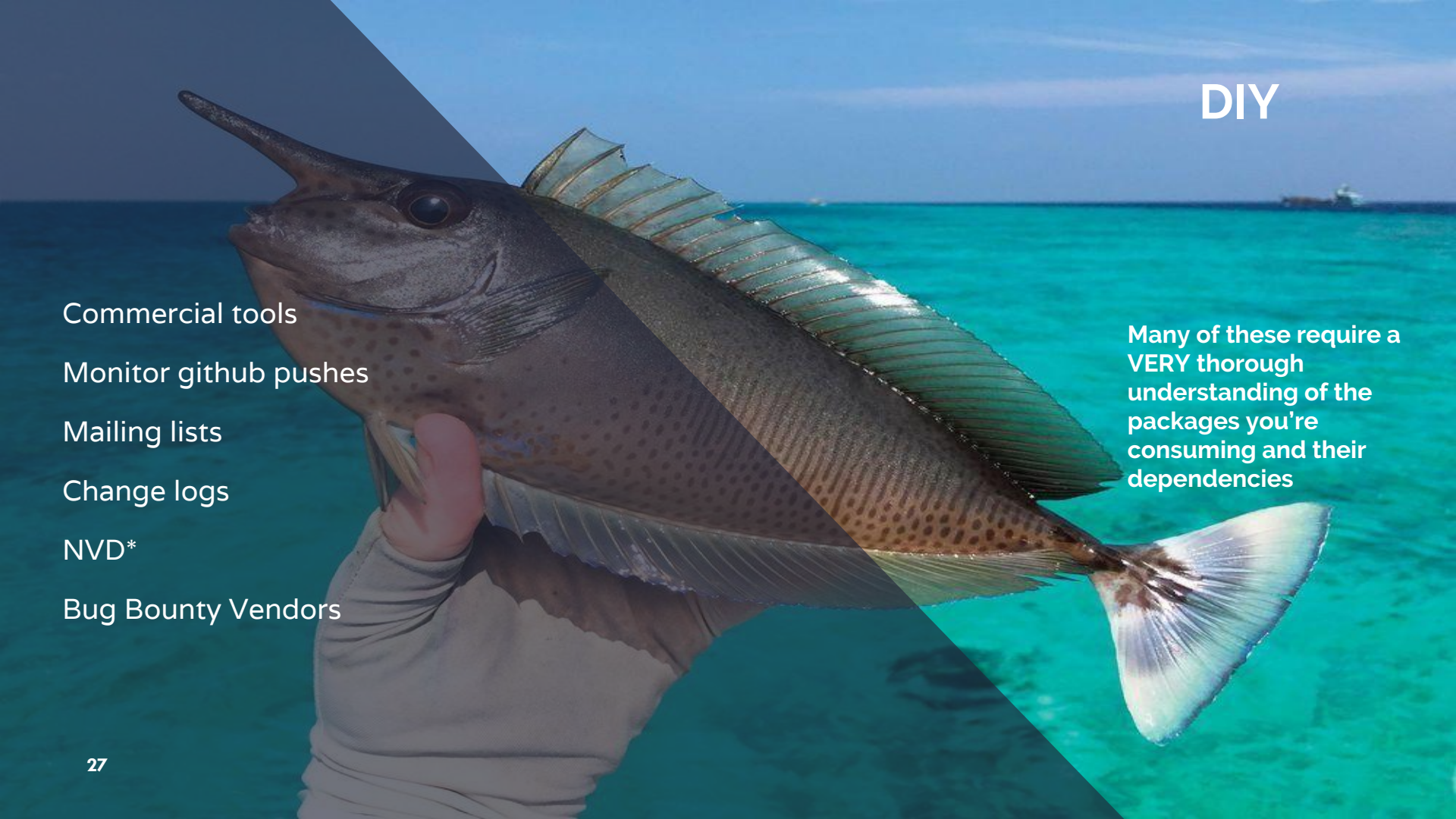
Lack of Security team or mindset

Unknown contents

A close-up photograph of two fish heads against a dark background. The fish in the foreground is in sharp focus, showing its large, prominent eye with a dark pupil and a reddish-brown ring. The fish behind it is blurred. A diagonal dark blue line runs from the top-left corner towards the bottom-right, separating the two fish.

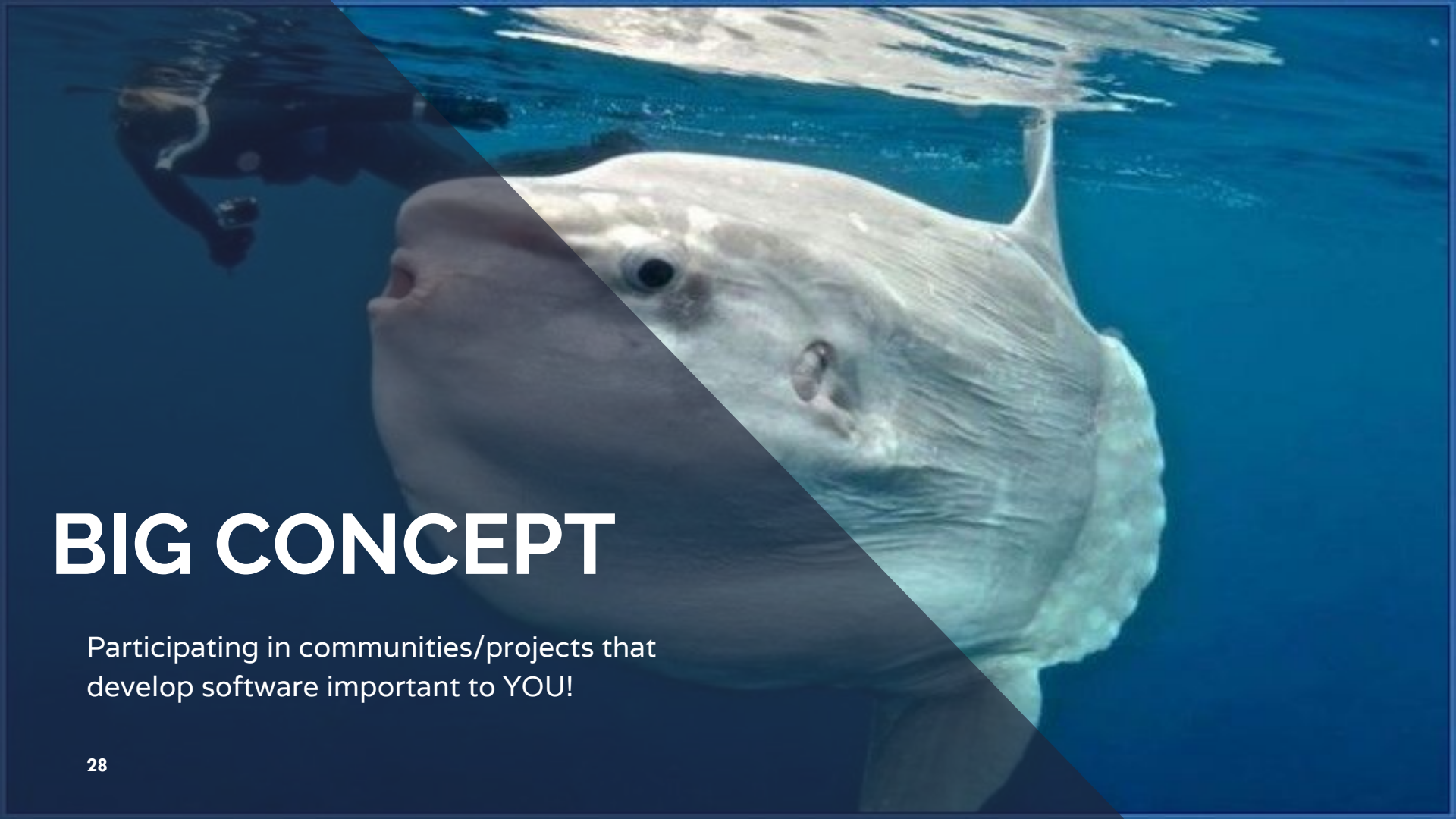
# 4. HOW?

# DIY

A hand in a grey sleeve holds a longhorn fish (Forsterygion niger) against a background of turquoise water and a blue sky. The fish has a long, pointed snout and a patterned body. The text is overlaid on the left side of the image.

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

---

SPROCKY

VISION™



A person in a dark jacket and shorts stands on dark, jagged rocks on a beach, looking out at the ocean during a sunset. The sun is low on the horizon, creating a bright orange glow and a long, shimmering reflection on the water. The sky is filled with dark, dramatic clouds, some of which are illuminated from below by the setting sun. The overall mood is serene and contemplative.

**Free Fish Aren't  
Free**

*Thanks!*



CRob\_at\_RedHat\_dot\_com



@RedHatCRob



# OUR PROCESS IS EASY

