

A photograph of a person standing on a rocky beach at sunset. The person is seen from behind, wearing a dark jacket and shorts, looking out at the ocean. The sky is filled with dramatic orange and yellow clouds, and the sun is low on the horizon, reflecting brightly on the water. A large, semi-transparent dark blue triangle is overlaid on the left side of the image, containing the text.

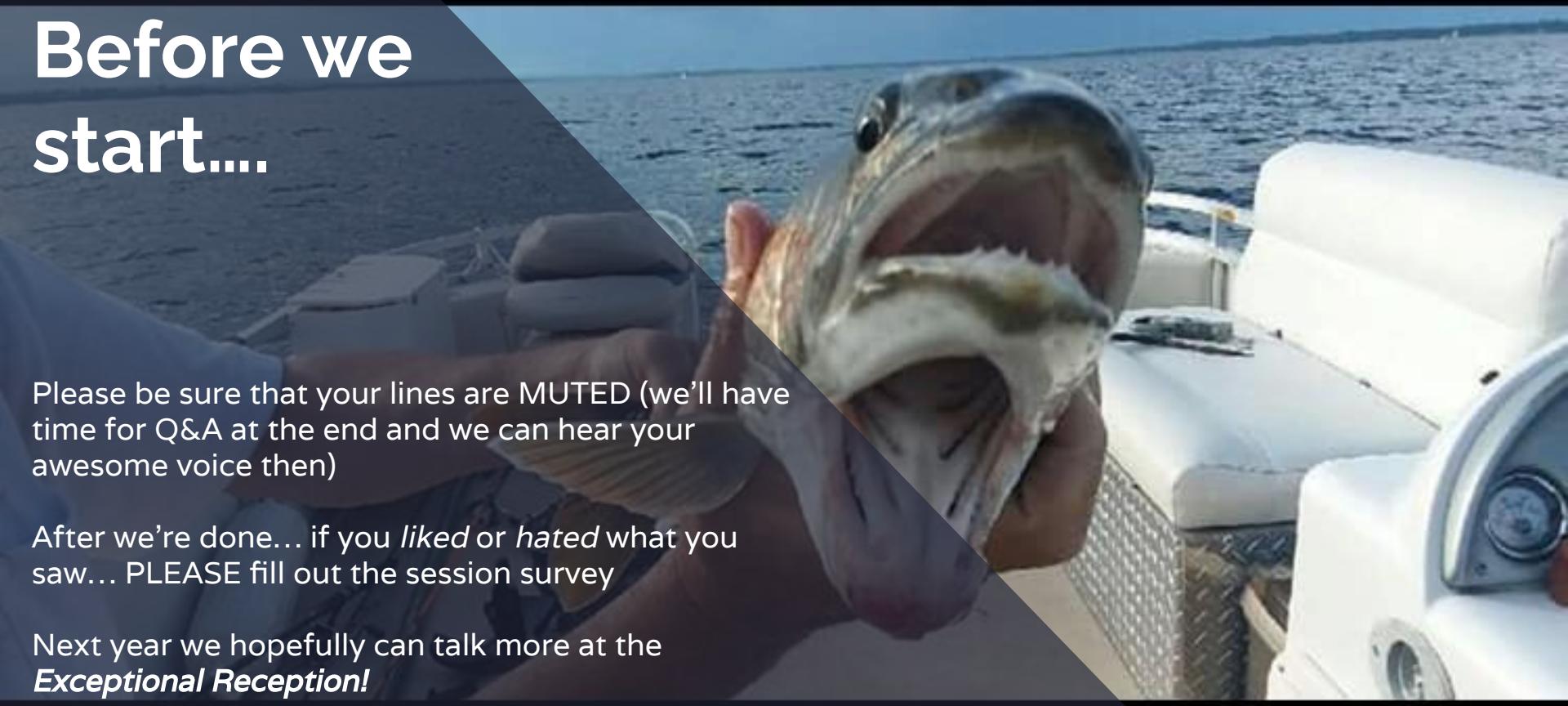
Free Fish Aren't
Free

Before we start....

Please be sure that your lines are MUTED (we'll have time for Q&A at the end and we can hear your awesome voice then)

After we're done... if you *liked* or *hated* what you saw... PLEASE fill out the session survey

Next year we hopefully can talk more at the ***Exceptional Reception!***



Agenda

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

1. Who?

- CRob, n, adj, and v
 - Pronunciation: U.S. (K-robe)
- Over 25 years of Enterprise-class Leadership, Architecture, Engineering, Operations, and Security experience
- Ambassador of Red Hat Product Security
- Participant in the FIRST PSIRT SIG, VulnCoord SIG, OpenSSF, and others
- Co-Author FIRST PSIRT Services Framework & PSIRT Maturity Framework
- Herds cats while doing stuff and things
- Pirate-enthusiast & hat-owner



2. WAT?

What's up with all this THE Open Source?



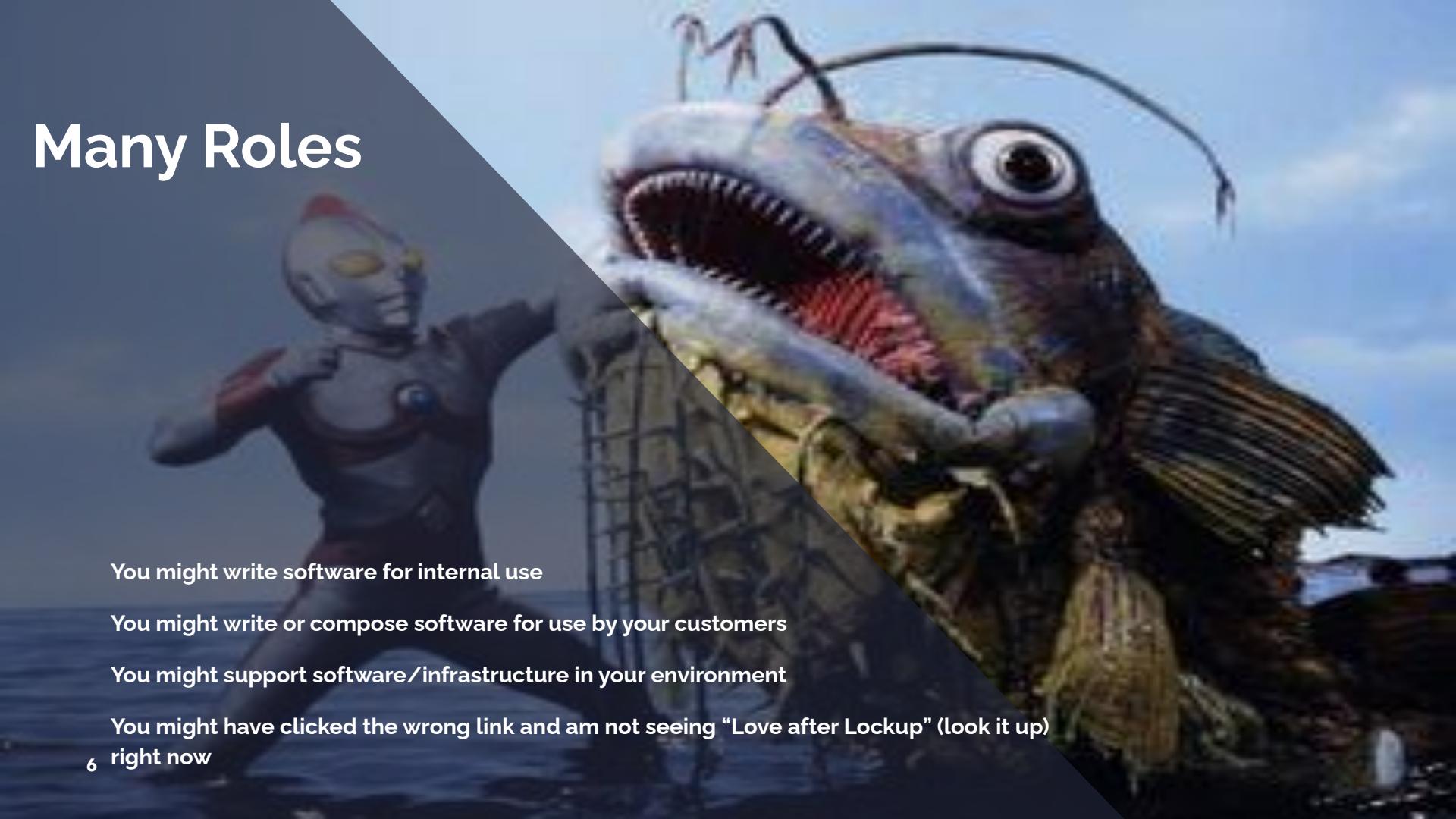
Many Roles

You might write software for internal use

You might write or compose software for use by your customers

You might support software/infrastructure in your environment

You might have clicked the wrong link and am not seeing “Love after Lockup” (look it up
right now



Pop Quiz! (yay!)

Who here knows they use OSS in their Enterprises?

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

A 2019 Synopsis report states that somewhere between 60-80% of modern software is comprised of OSS (yay!)[1]

[1] -
https://www.linuxfoundation.org/wp-content/uploads/2020/02/oss_supply_chain_security.pdf

Open Source “won”

Yay us!

Why?

Speed

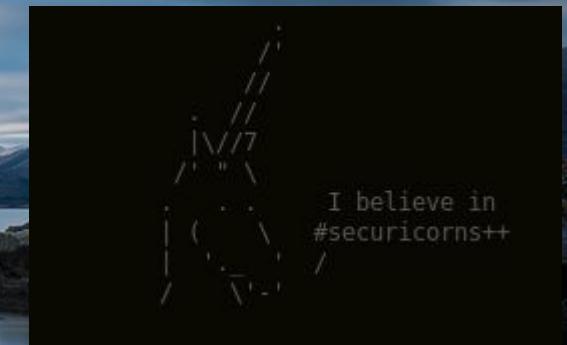
Agility

Innovation

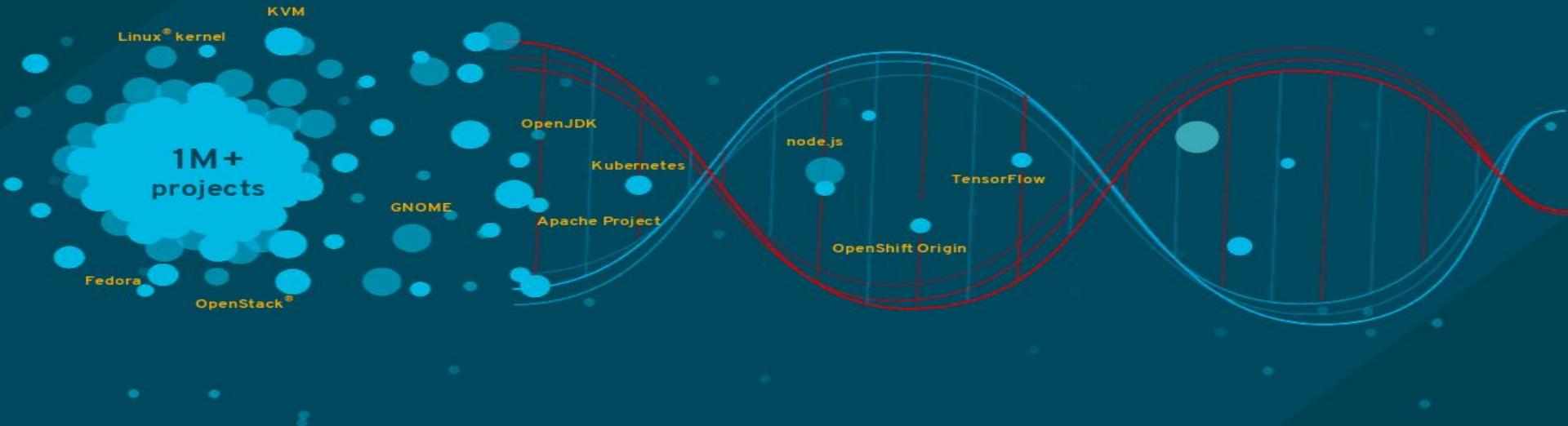
Powerful ability to configure for-purpose

Penguins

Awesome black and green screens



OPEN SOURCE IS THE SOURCE OF TECHNOLOGICAL INNOVATION



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

A large, vibrant red fish with white, irregular spots swims diagonally across the frame. The fish has a textured, almost bumpy skin surface. It is set against a solid blue background.

"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?



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....



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



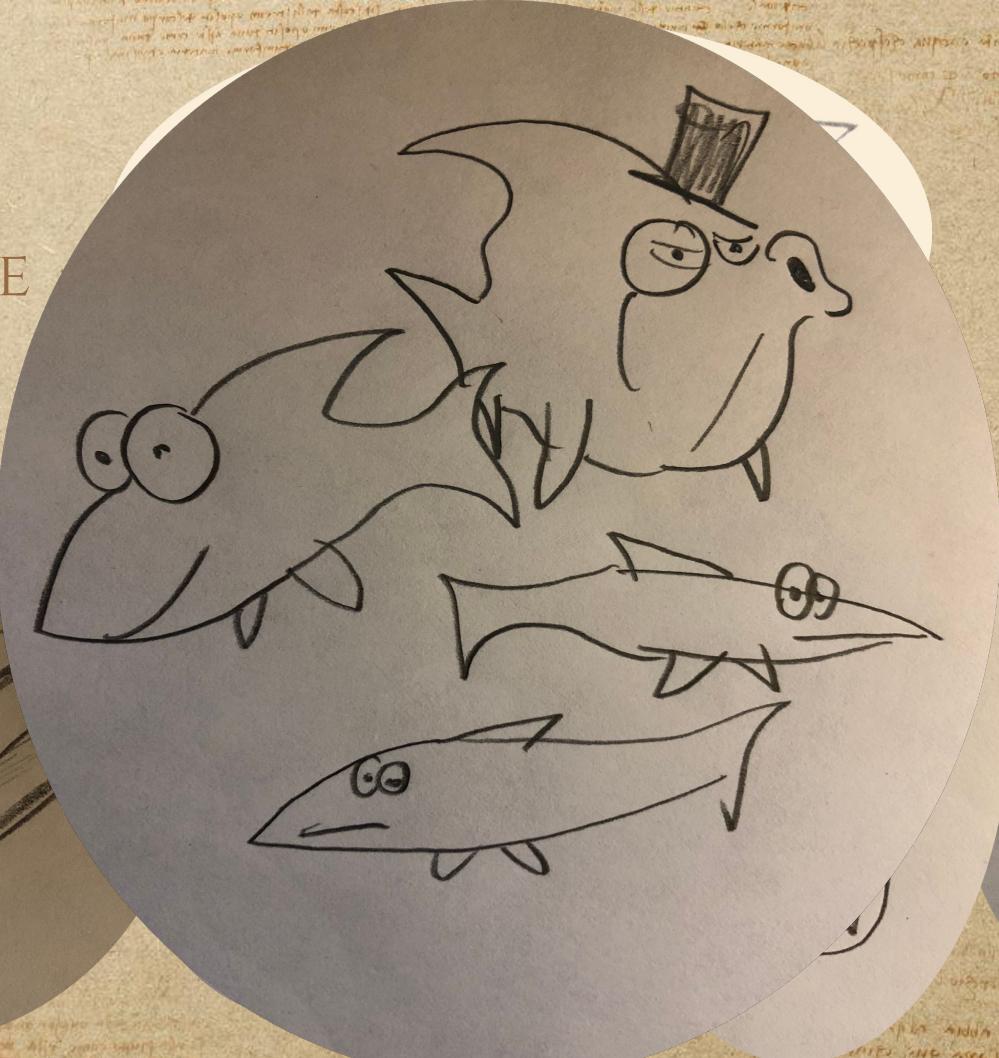
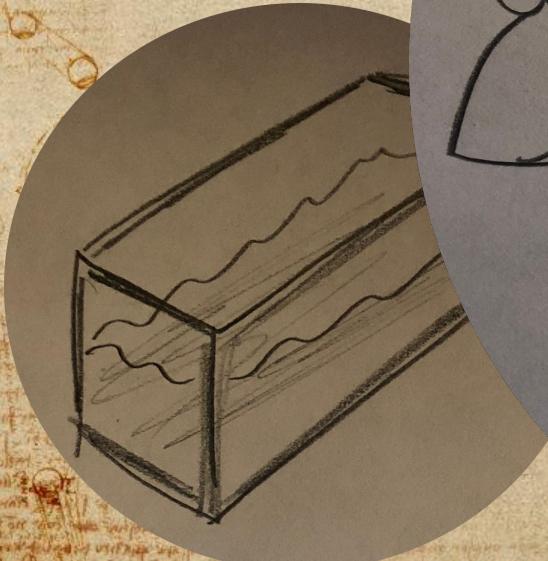
The retelling of
The Old CRob,
the Free Fish,
and the Sea

....IT ALL STARTED ONE BRIGHT AND
BEAUTIFUL DAY WITH A SIMPLE 5TH
GRADE SCIENCE EXPERIMENT

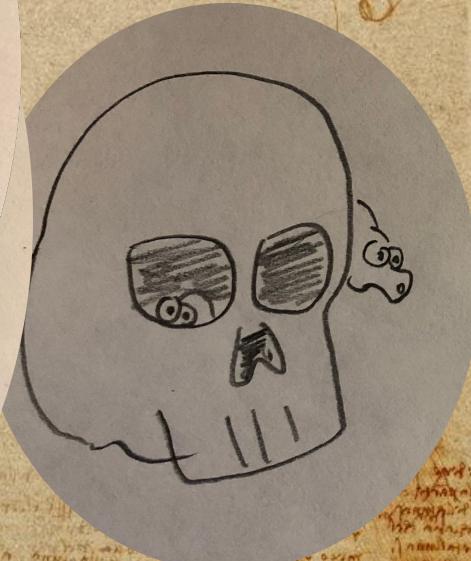




CROB'S "FREE FISH" BILL:



>\$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?

Why it is important to know MOAR about OSS (aside from the obvious coolness of it all!)

a.) What's on the inside?



Why should I care about what is inside my software?

The Sandwich Paradox



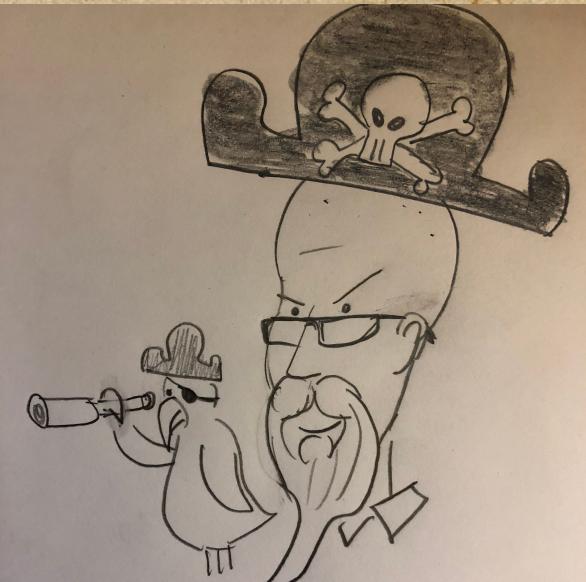
SCHRODINGER'S SAMMICH

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?

*Does it REALLY matter who made my
software or where it comes from?*

RIPPED! From the headlines.... (zomg!)

<https://www.infosecurity-magazine.com/news/open-source-supply-chain-attacks/>

The image shows a news article from Infosecurity Magazine. The main title is "Open Source Supply Chain Attacks Surge 430%" displayed prominently on a tablet screen. The article is dated 13 AUG 2020 and categorized under NEWS. Below the title, there is a photo of a person's hands typing on a keyboard. On the left side of the article, there is a portrait of Phil Muncaster, UK / EMEA News Reporter, Infosecurity Magazine. Below his photo, there are links to email him and follow him on Twitter (@philmuncaster). There are also social media sharing icons for Facebook and Twitter. The text of the article discusses a 430% year-on-year increase in attacks targeting open source components directly to infect software supply chains. It cites Sonatype's annual report and includes quotes from developers. A sidebar on the right features a yellow padlock icon and the words "Lat Ind Wh" and "Downl".

Open Source Supply Chain Attacks Surge 430%

13 AUG 2020 NEWS

Phil Muncaster UK / EMEA News Reporter , Infosecurity Magazine

Email Phil Follow @philmuncaster

Security experts are warning of a 430% year-on-year increase in attacks targeting open source components directly in order to covertly infect key software supply chains.

There were 929 attacks recorded between July 2019 and May 2020, according to Sonatype's annual *State of the Software Supply Chain* report. The study was compiled from analysis of 24,000 open source projects and 15,000 development organizations alongside interviews with 5600 software developers.

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?

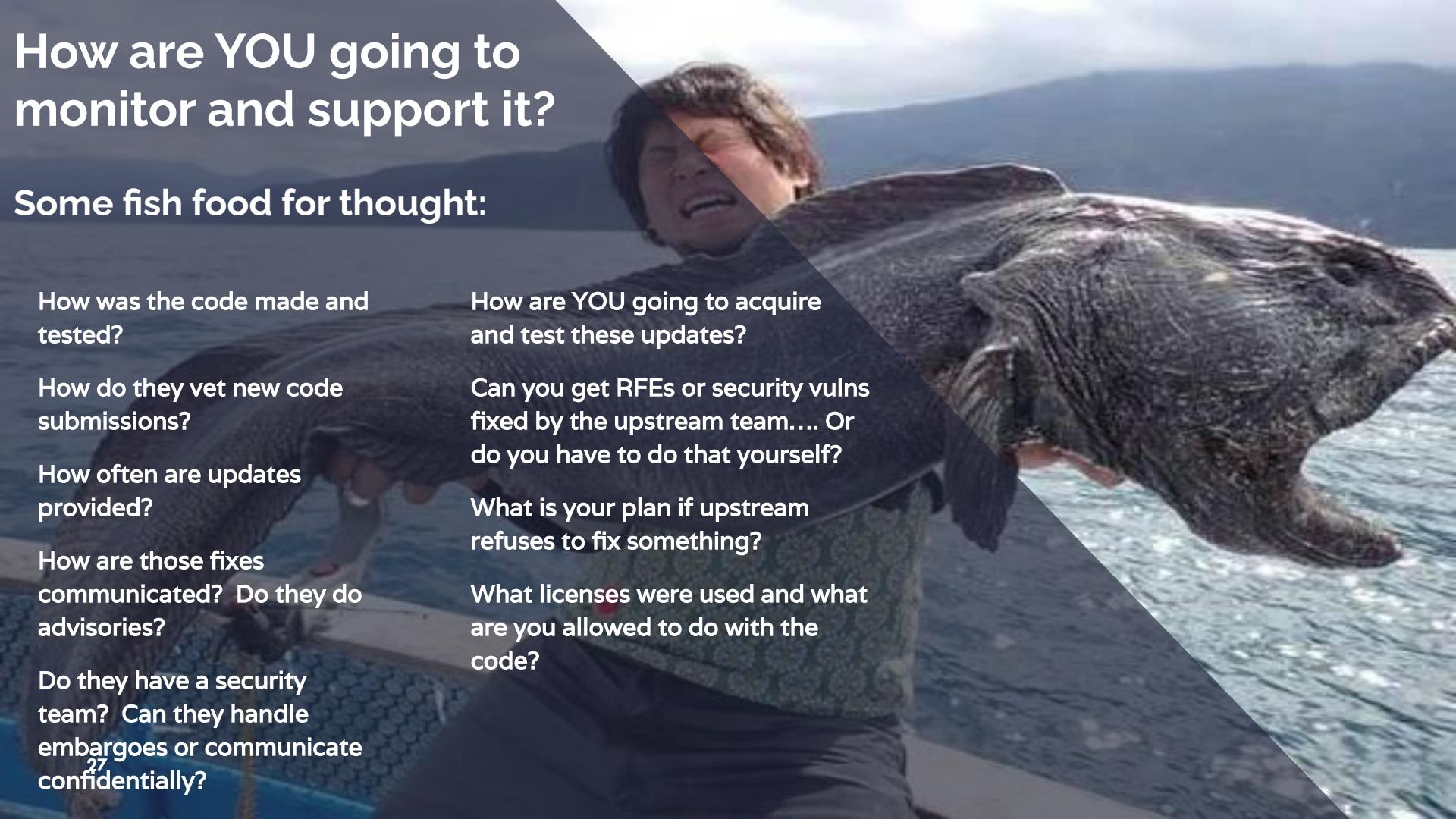
Do they have a security team? Can they handle embargoes or communicate confidentially?

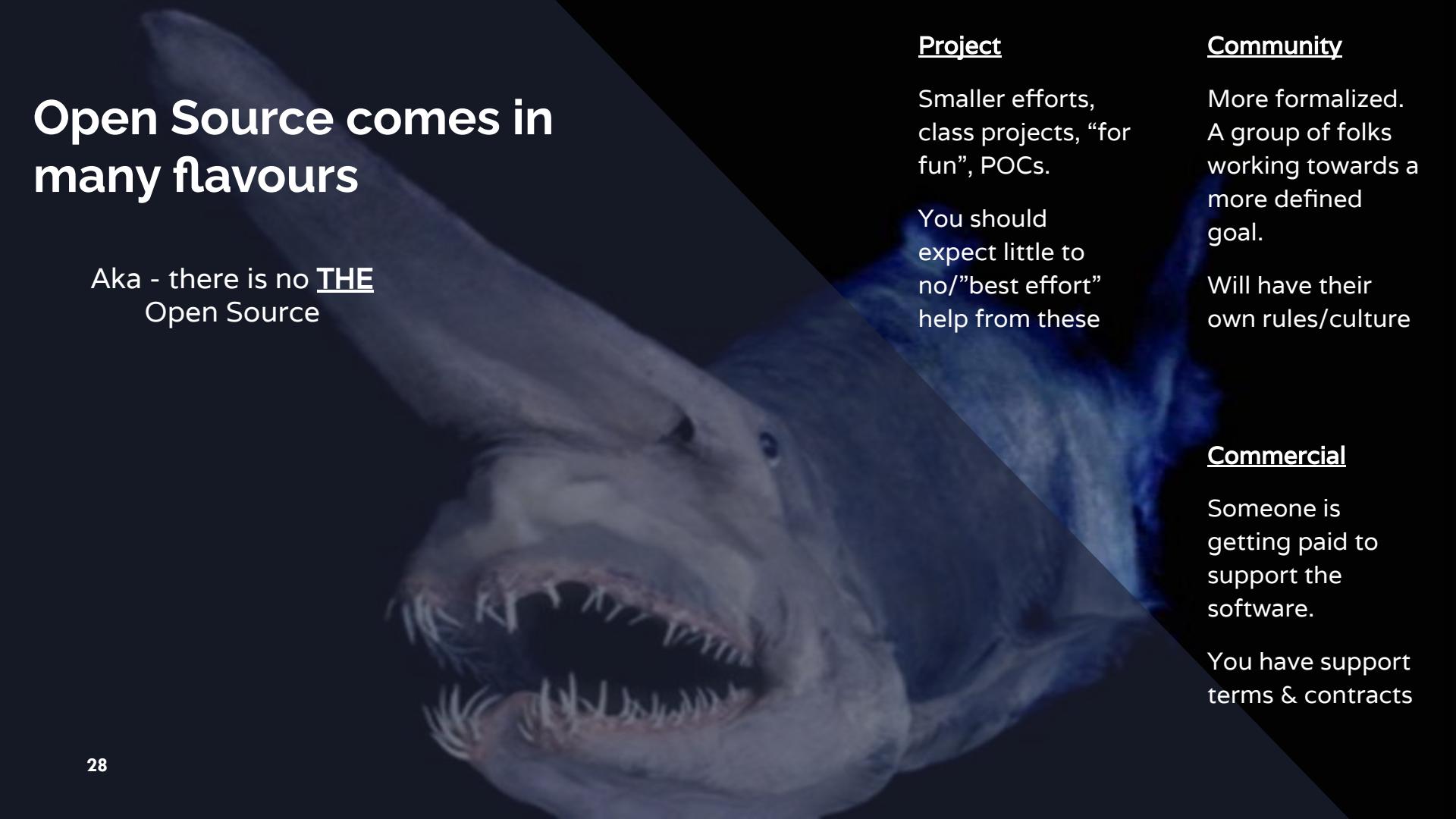
How are YOU going to acquire and test these updates?

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

Aka - there is no **THE**
Open Source

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

A dramatic photograph of a person's arm and hand holding a spear gun, aiming at a large fish leaping out of the ocean. The fish, possibly a barracuda, is captured mid-air with its mouth open, showing sharp teeth. The background is a vast, blue sea under a clear sky.

Risk? Wut Risk?

Uncontrollable upstream

Unknown Contributors

Immature project

Change in Technical direction

Abandoned Project

Lack of Security team or mindset

Unknown contents

It may be shocking to find out, but even the mighty OSS has some potential risks that need managed.....

A close-up photograph of two cockatoos' heads. The birds have white feathers and large, expressive eyes with red and yellow irises. They are looking slightly to the right of the camera. The background is dark.

4. HOW?

How can you better MANAGE your OSS-usage?

A large marlin fish is being held by a person's hand against a background of blue ocean and sky. The fish has a long, pointed dorsal fin and a dark, mottled pattern on its body.

DIY

Commercial tools

Monitor “github” commits

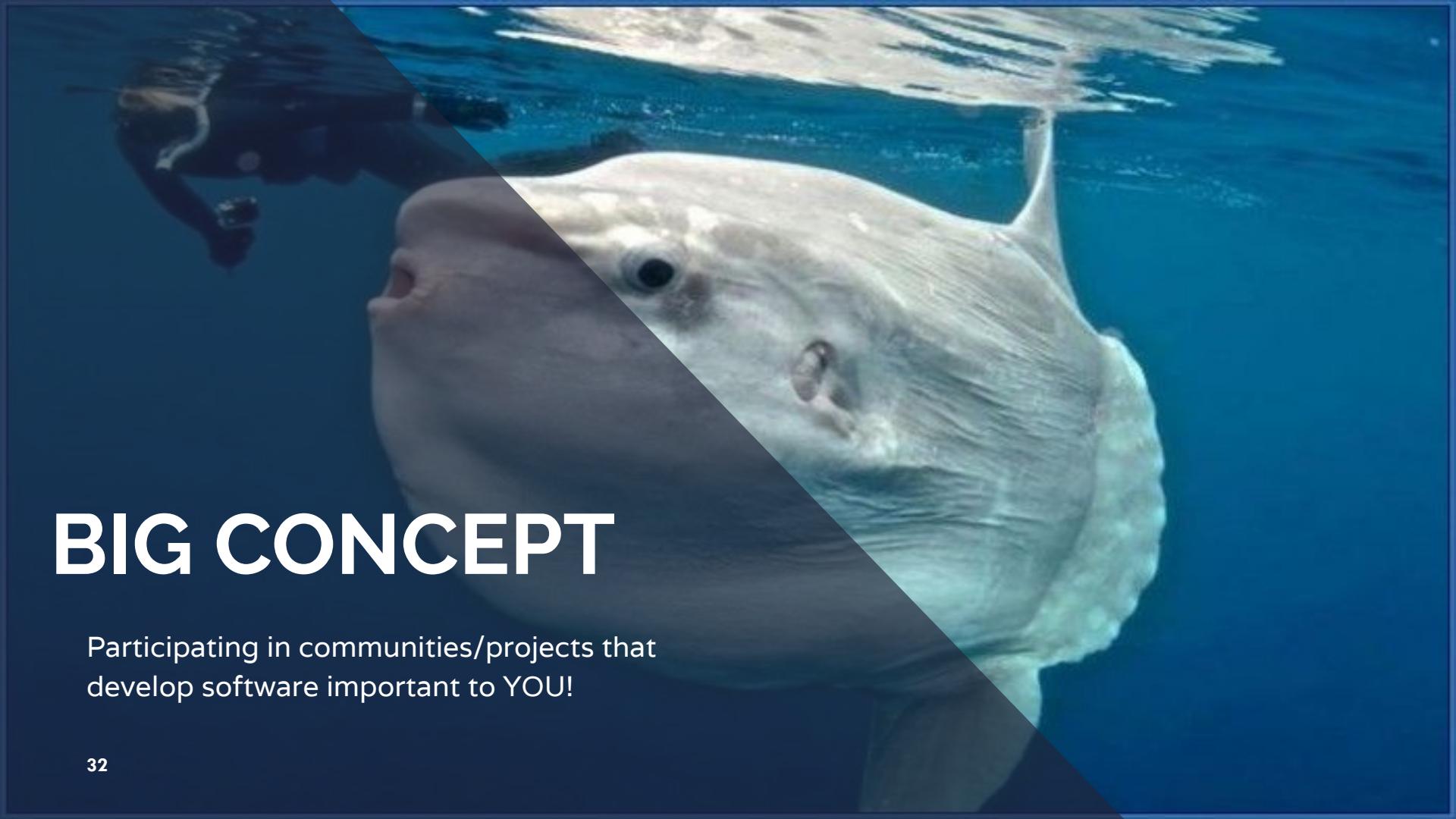
Mailing lists

Change logs

NVD*

Bug Bounty Vendors

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

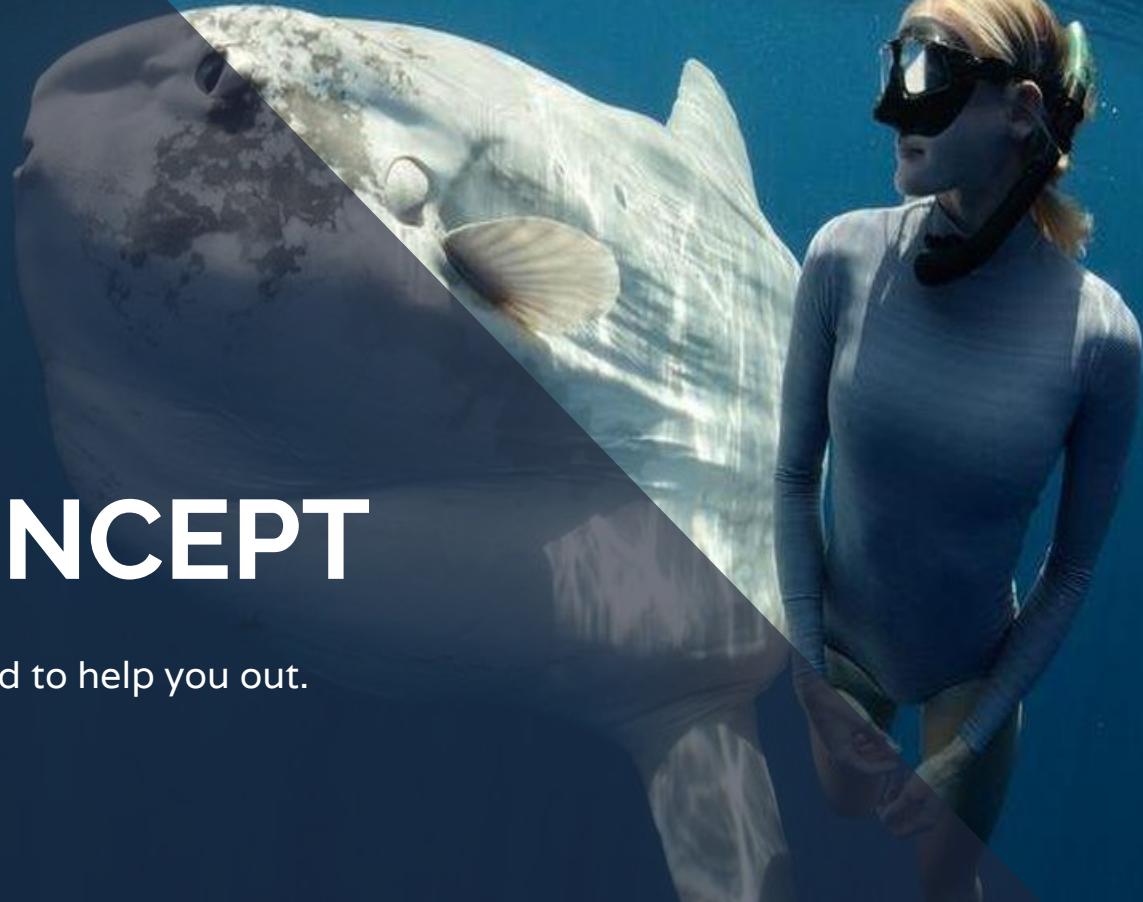
A large sunfish, also known as a mola, is swimming in the ocean. The fish has a very large, flattened body with a light-colored, mottled pattern. It is positioned diagonally across the frame, from the top left towards the bottom right. The background shows the blue water of the ocean.

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

You have A LOT of options, educate yourselves on what is best for YOUR business and Risk appetites

Free-ish Tools & Tricks

GitHub Stuffs

<https://github.com/features/security>

Vuln Scanner

Dependabot

Secret Scanning

...

OWASP Dependency Checker (SCA Tool)

<https://owasp.org/www-project-dependency-check/>

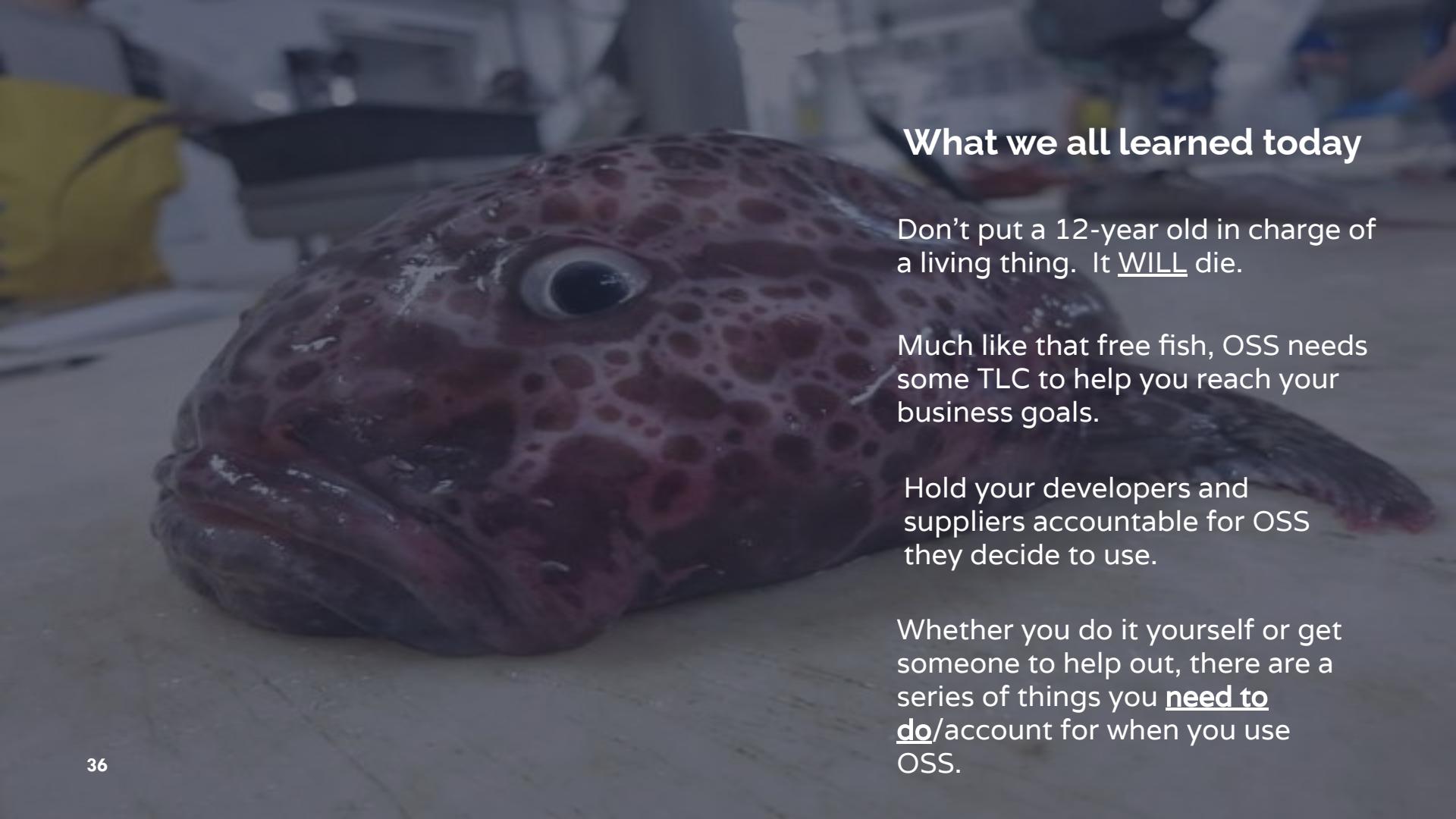
ZAP (Webapp Attack Proxy)

<https://owasp.org/www-project-zap/>

Linux Foundation CII Best Practices Badges

<https://bestpractices.coreinfrastructure.org/en>

- Wherever possible automate ALL THE THINGS
- Depending on your SCM tooling/build infrastructure, leverage built-in or bolt-on tools
- Only choose software from known, good sources



What we all learned today

Don't put a 12-year old in charge of a living thing. It WILL die.

Much like that free fish, OSS needs some TLC to help you reach your business goals.

Hold your developers and suppliers accountable for OSS they decide to use.

Whether you do it yourself or get someone to help out, there are a series of things you need to do/account for when you use OSS.



QUESTIONS

S P O O K Y

Y I S I D O N

A photograph of a man standing on a rocky beach at sunset. He is seen from behind, wearing a dark jacket and shorts, looking out at the ocean. The sky is filled with dramatic orange and yellow clouds, and the sun is low on the horizon, reflecting off the water. The foreground is composed of dark, silhouetted rocks.

Free Fish Aren't Free

Thanks!



CRob_at_RedHat_dot_com



@RedHatCRob