
#speedMAX
@PERROGRAFF
@TIMEOVER86
@PERROGRAFF
@PATI_GALLARDO
Turtle
Sec

Tweet

Gabriel A. Devenyi
@gadevenyi

@troyhunt I just got phished with an old password from the NCIX security breach
nakedsecurity.sophos.com/2018/09/24/ban...

Its in the wild.

Make it Fixable

Living with Risk

Patricia Aas
CppCon 2018

@pati_gallardo

Turtle Sec

Patricia Aas - Consultant

Programmer, Application Security
Currently : **TurtleSec**

Previously : Vivaldi, Cisco Systems, Knowit, Opera Software
Master in Computer Science - main language Java

Pronouns: she/her

@pati_gallardo

Turtle Sec

Security is Hard

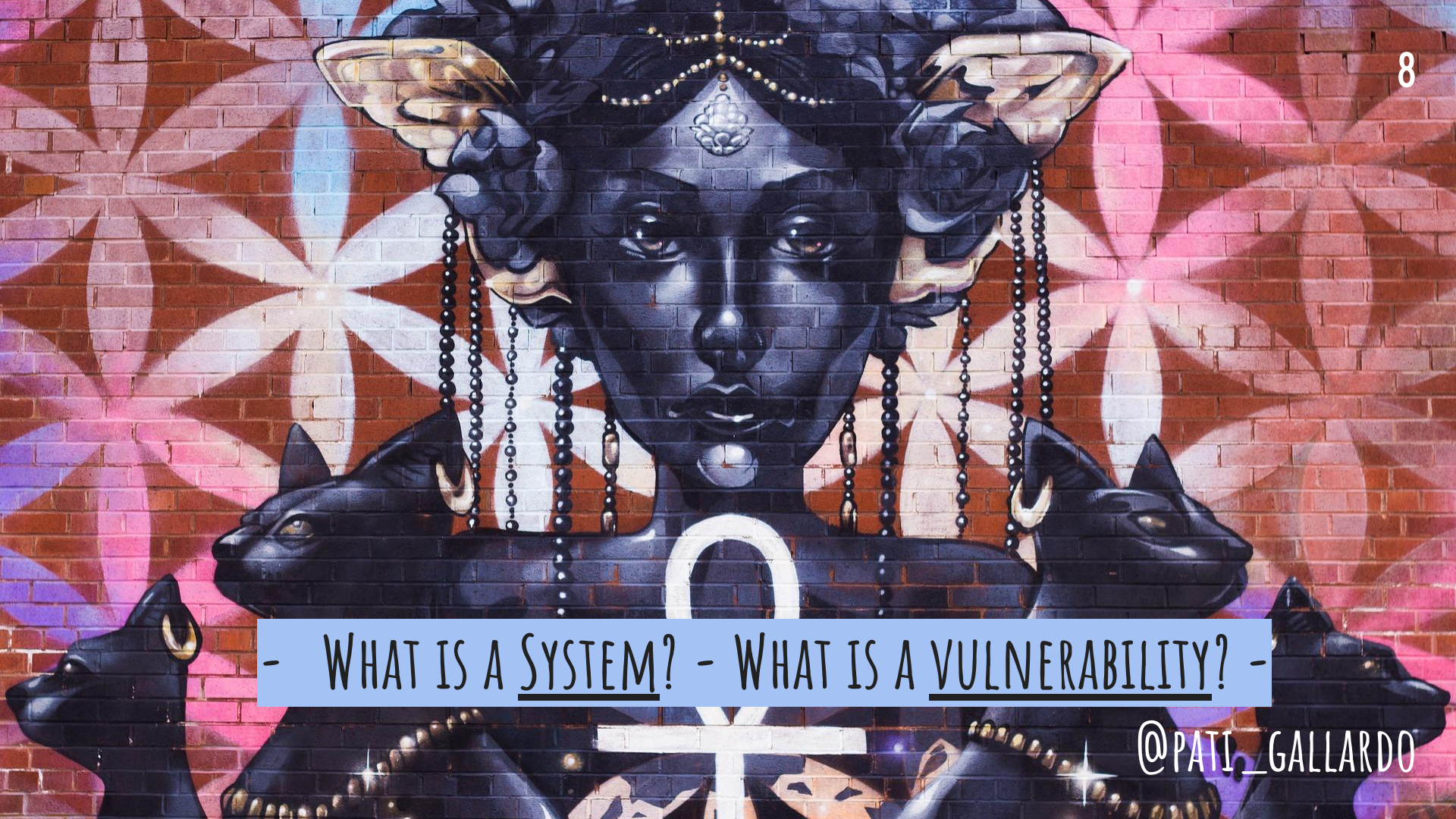
Just Remember :

- You live in the real world
- Take one step at a time
- Make a Plan

You Need A Security "Hotline"

security@example.com

Symbiotic relationship
Be polite
Be grateful
Be professional
Be efficient and transparent



- What is a System? - What is a vulnerability? -

@pati_gallardo

Outline

1. Unable to Roll Out Fixes
2. No Control over Dependencies
3. The Team is Gone
4. It's in Our Code
5. My Boss Made Me Do It
6. User Experience of Security

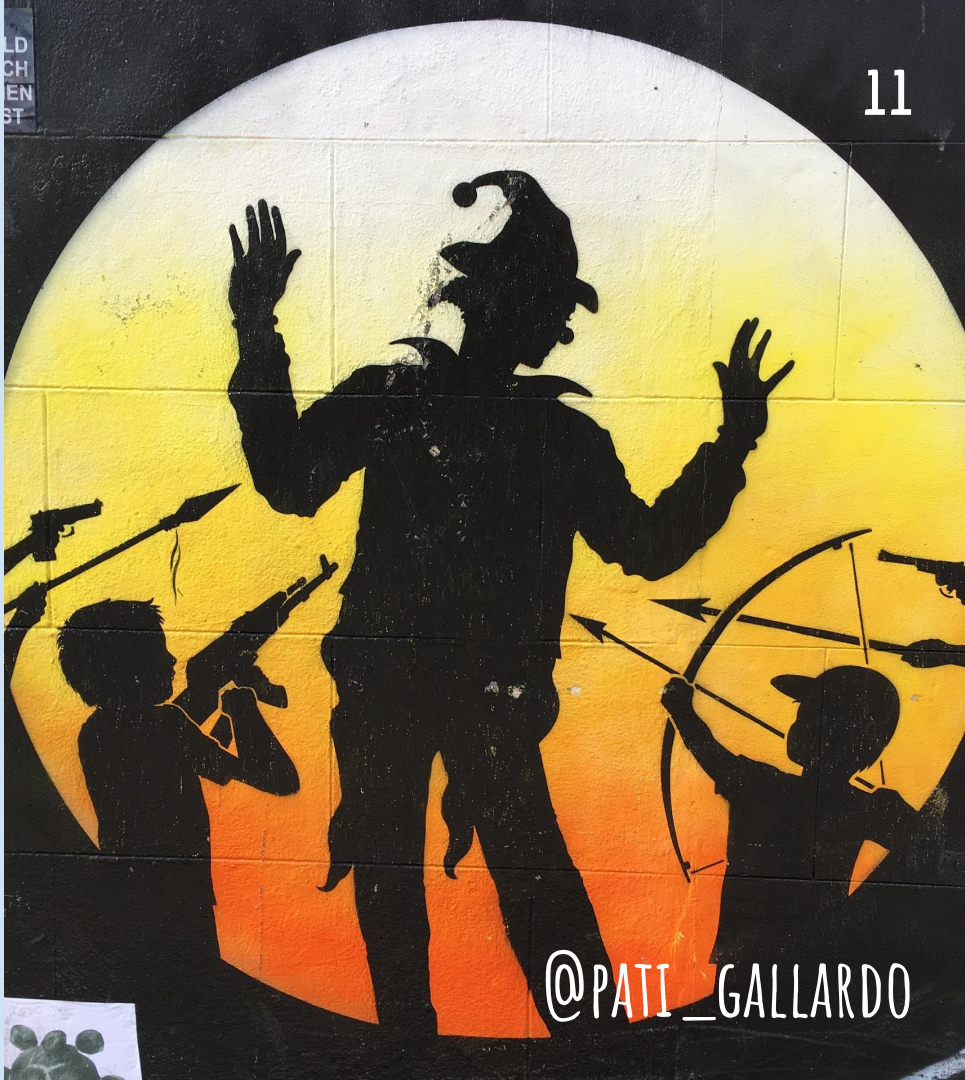
1

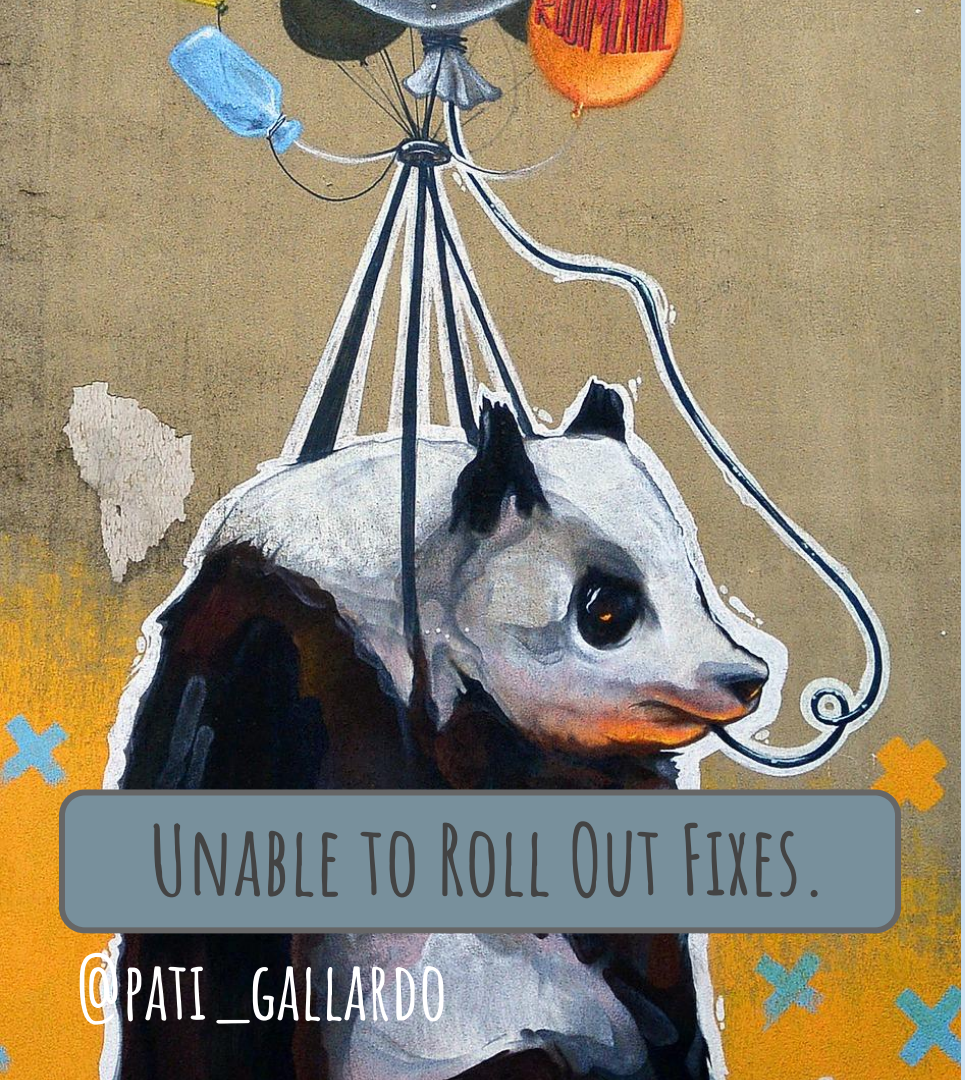
Unable to Roll Out Fixes

@pati_gallardo

Unable to Roll out Fixes

Unable to Update
Unable to Build





Internet of Things

Toys: My Friend Cayla, i-Que Intelligent Robots, Hello Barbie

Mirai: Botnets created with IOT devices, users don't update

"Shelfware"

No Maintenance contract

Abandonware

Closed source - no way to fix/fork

Internet of Things

- Auto-update
- Different default passwords
- Unboxing security (make the user change the password)

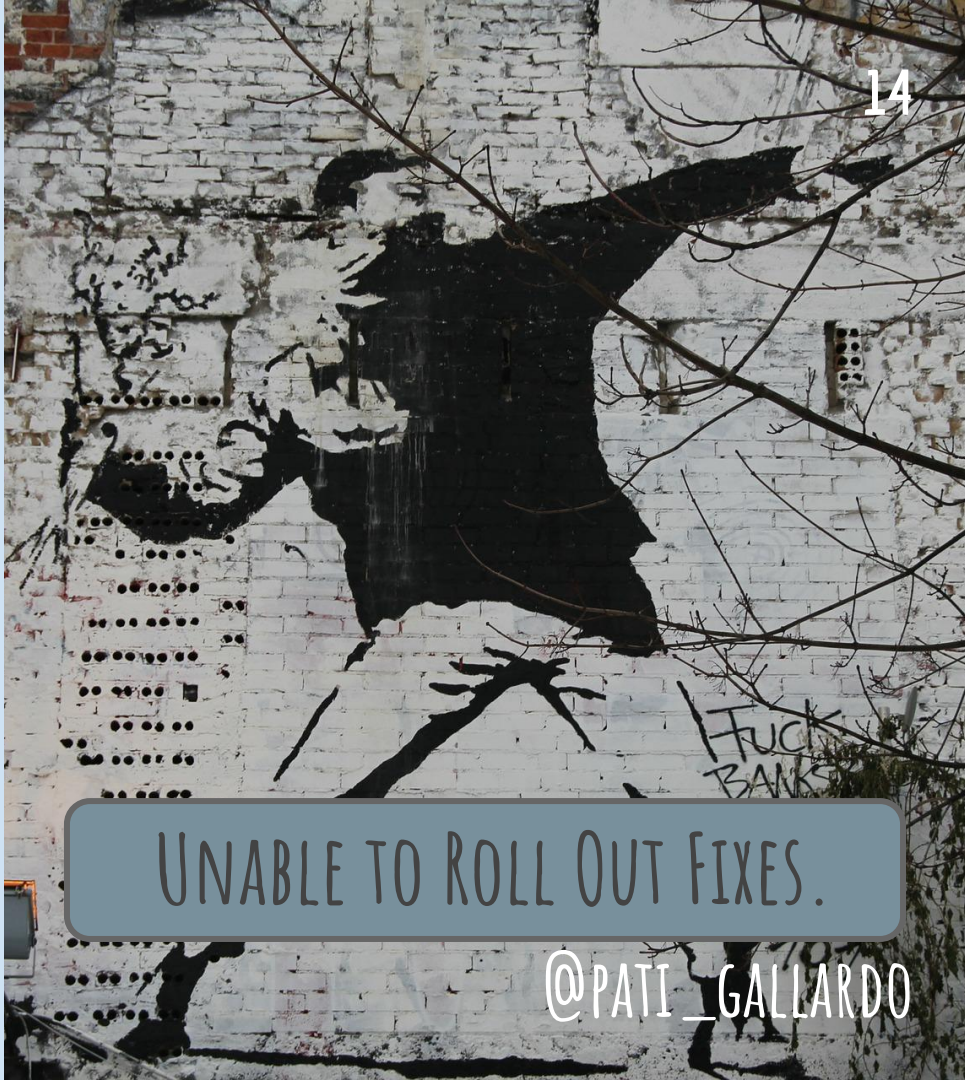
"Shelfware"

- Get maintenance contract
- Change supplier
- Do in-house
- Use only Open Source Software

Fix : Ship It!

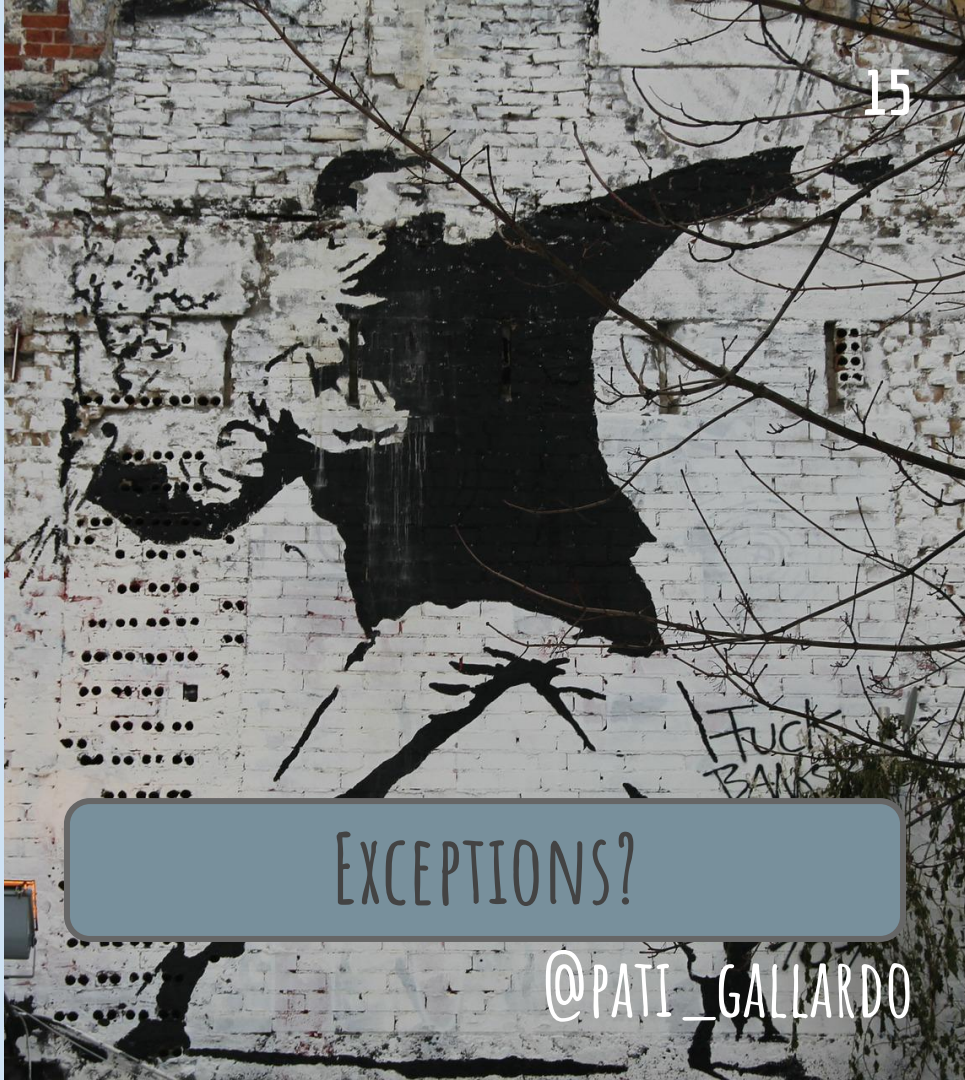
Holy Grail : Continuous Deployment and Auto Update

- A Build Environment
- Update Mechanism



Some systems should not be “fixed”

A major election software maker allowed remote access on its systems for years



No Control over Dependencies

@pati_gallardo

No Control over Dependencies

No inventory
No update routines
No auditing

Equifax Breach

Known vulunerability in Apache Struts 2

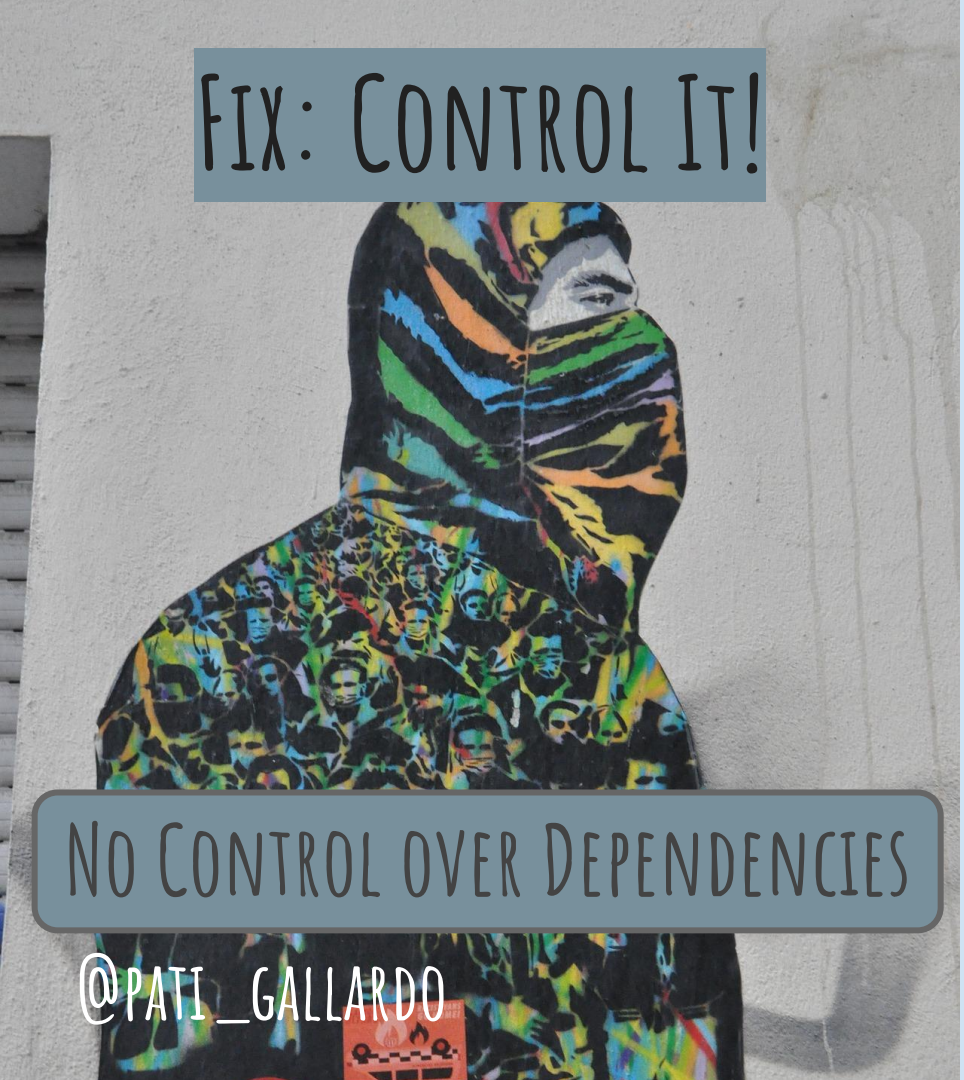
Heartbleed

Bug in openssl

Left-Pad

Developer unpublished a mini-Js library

Fix: Control It!



No Control over Dependencies

@pati_gallardo

Equifax Breach

Continuous Dependency Auditing

Heartbleed

Control over production environment

Left-Pad

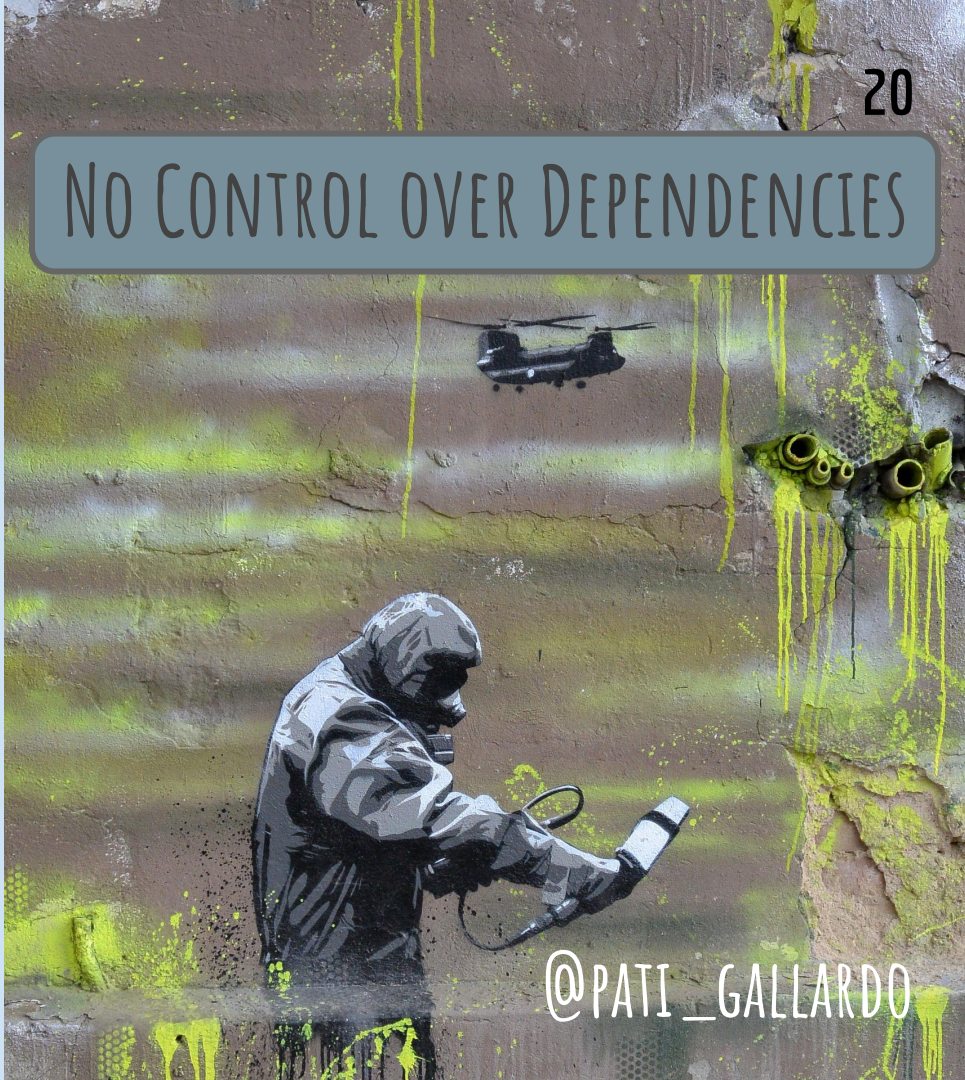
Remove unnecessary dependencies

Fix: Control It!

Goal : Largely Automated Dependency Monitoring

Remember transitive dependencies

Monitor and Update



3

The Team is Gone

@pati_gallardo

The Team Is Gone

- Team were consultants
- They were downsized
- The job was outsourced
- “Bus factor”
- “Binary blob”
- Abandonware

Fix : Own It!

Goal : Complete Build Environment

Fork it, own it

Use It!

4

It's in Our Code

@pati_gallardo

It's in Our Code

Congratulations!

This is Actually

the

Best Case Scenario

Keeper Password Manager

- Reporter: *Tavis Ormandy* (@taviso)
- "allowing any website to steal any password"
- Browser plugin preinstalled on Windows
- *Badly handled report: Sues news reporter Dan Goodin*

GitLab.com

- "rm -rf"
- Sysadmin maintenance
- Cascading errors as backups fail
- All logged Publicly in real time

Transparency Breeds Trust

That is how you recover

Fix : Live It!

Goal : Prevent & Cure

Prevention is great,
but
the Cure is to Ship

5

My Boss Made Me Do It

@pati_gallardo

My Boss Made Me Do It

The Feature is the Bug

How?

- Security Problem
- Privacy Problem
- Unethical
- Illegal

Capcom's Street Fighter V

- Installed a driver
- “anti-crack solution”

“...disables supervisor-mode execution protection and then runs the arbitrary code passed in through the ioctl buffer with kernel permissions..”

- Reddit user extrwi

KrebsOnSecurity: "For 2nd Time in 3 Years, Mobile Spyware Maker mSpy Leaks Millions of Sensitive Records"

@PATI_GALLARDO

Fix : Protect It!

Goal : Protect your user

Prevent : Protect your team

- Workers rights
- Team can diffuse blame

Cure : Protect your company

- Find a Powerful Ally
- Do Risk Analysis : Brand Reputation, Trust
- Use the Law

Last resort : Whistleblowing & Quitting

Google: DragonFly

- "A plan to launch a censored search engine in China"
- Employee authors a memo
- Internal protests

Maersk: NotPetya

- Ransomware spreads globally, insufficient network segmentation
- "IT executives had pushed for a preemptive security redesign"

*These are often the **Unsung Heroes***

(Last Resort : Edward Snowden)

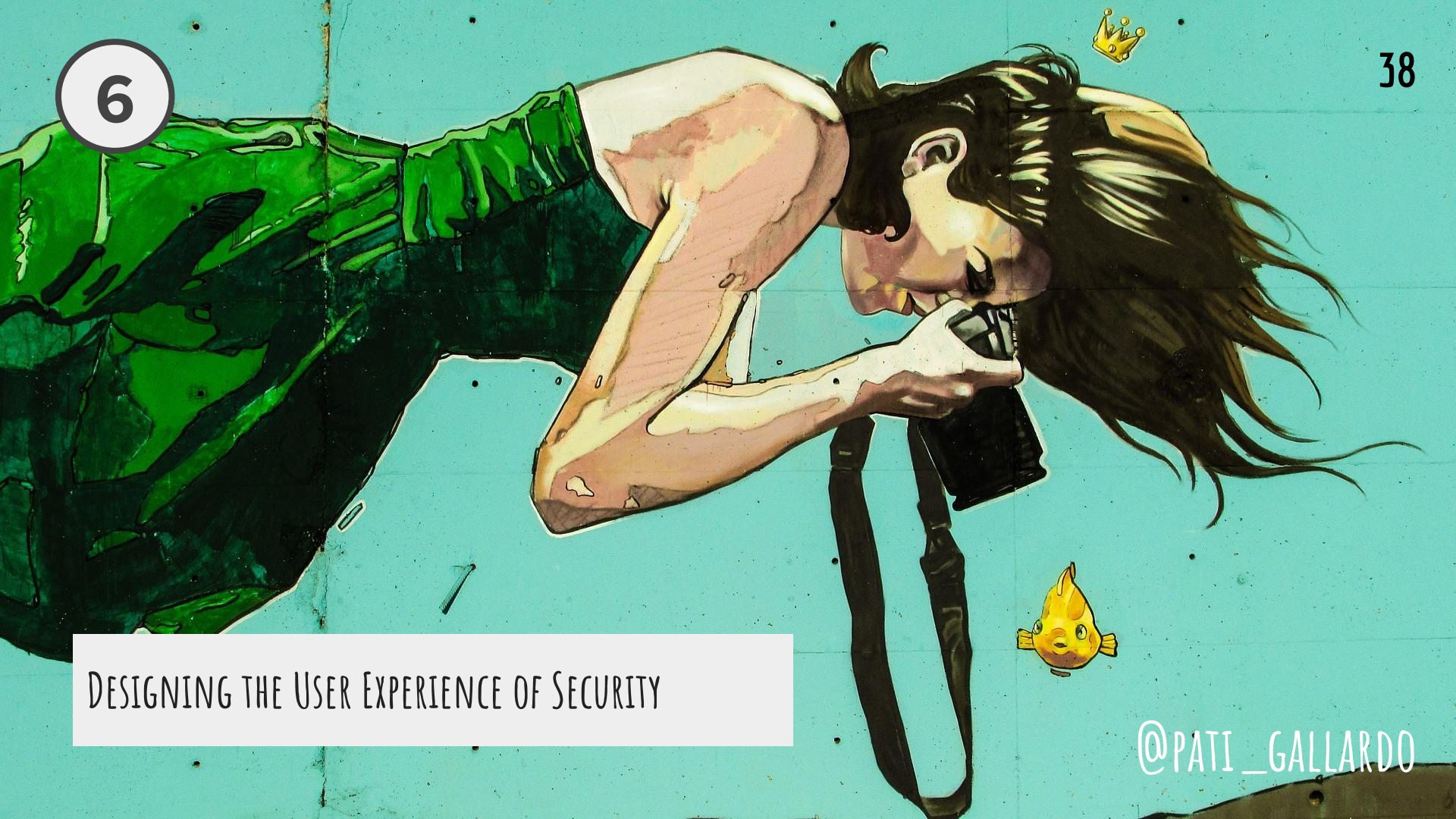
Ship It, Control It, Own It, Live It & Protect It

@pati_gallardo

Recap

- You need a Security Hotline
- You Have to Ship

6



Designing the User Experience of Security

@pati_gallardo

Amber Alert (CAE) - Kauai County Only

Amber Alert (CAE) Statewide

1. TEST Message

PACOM (CDW) - STATE ONLY

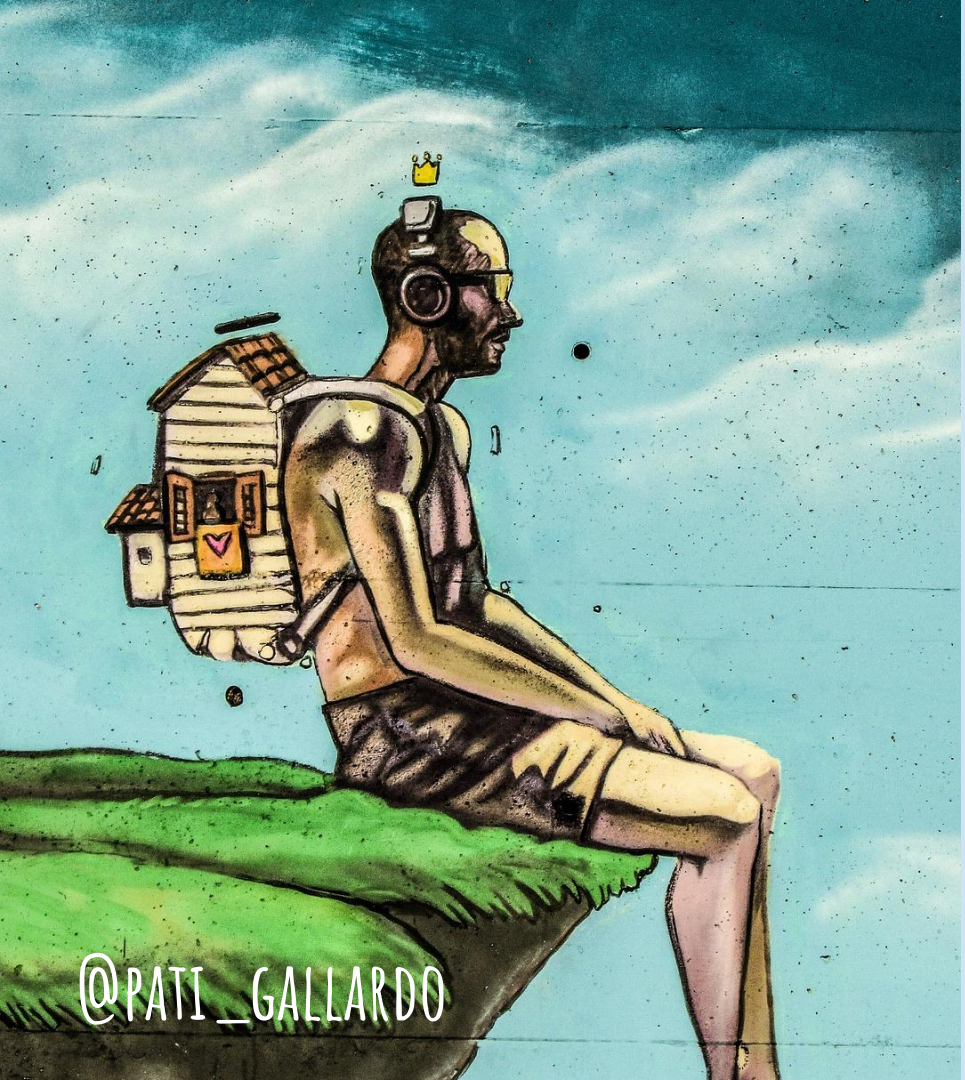
Tsunami Warning (CEM) - STATE ONLY

DRILL - PACOM (CDW) - STATE ONLY

Landslide - Hana Road Closure

Amber Alert DEMO TEST

High Surf Warning North Shores



The Users Won't Read

Error blindness

"Just click next"

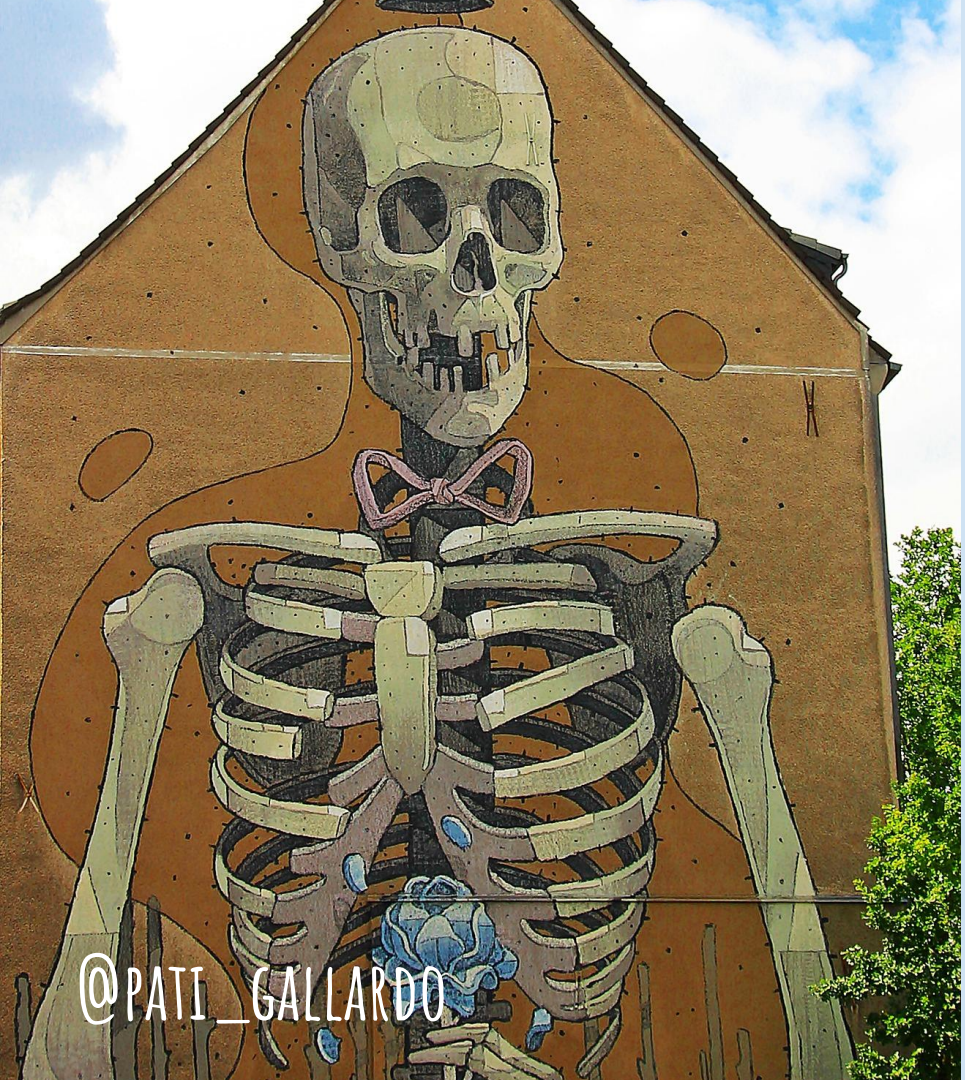
"Make it go away"

Fix : Less is More

Don’t leave it to the user

Have good defaults

Be very explicit when needed



They Trust You

With Personal Information

With Data

With Money

Fix : Be Trustworthy

Only store what you have to

Back up everything

Use third party payment

Be loyal to your end user

Ship It, Control It, Own It, Live It & Protect It

Design For It

@pati_gallardo

Photos from pixabay.com

Patricia Aas, TurtleSec
@pati_gallardo

Turtle Sec


#SPEEDMAX
@PERROGRAFF
@PERROGRAFF
@pati_gallardo
Turtle Sec