CERBERUS

Security Laboratories

From Zero to Security Hero

Making products that are secure by design

Dr Carl Shaw

IoTSF Security Conference

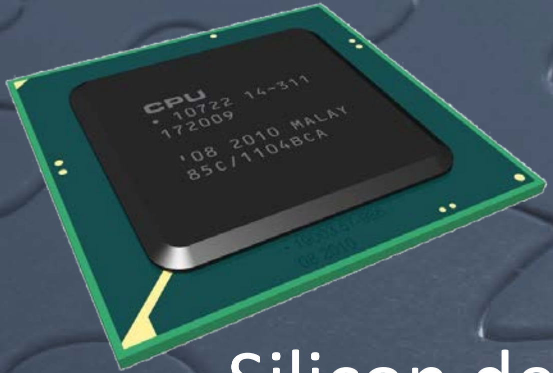
December 2018

PUBLIC

Who am I?

Some of our clients:

Our recent project types



Silicon devices

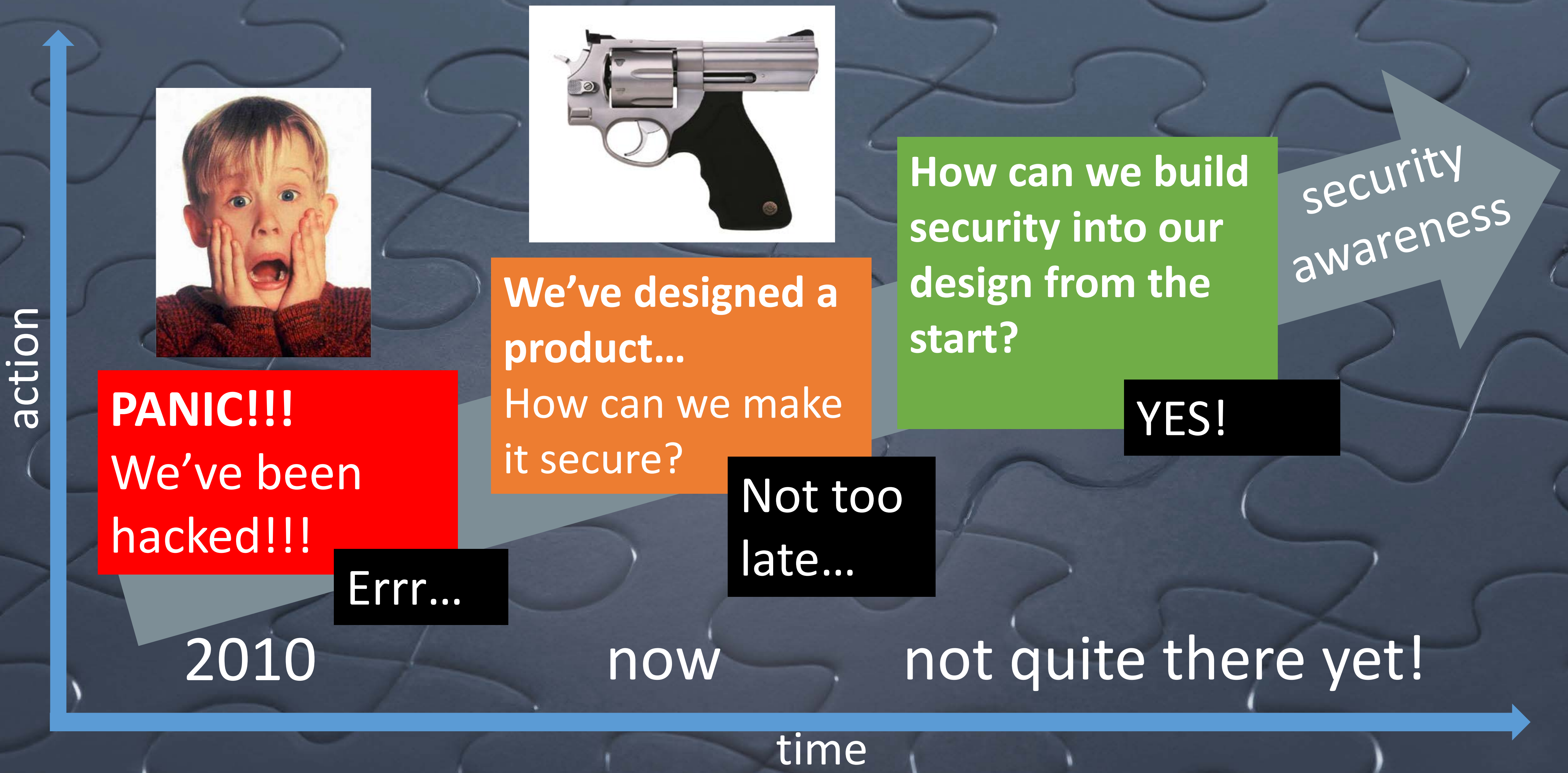
Automotive electronics

White goods

Medical devices

Access control

The good news!



action

PANIC!!!
We've been hacked!!!

Errr…

We've designed a product…
How can we make it secure?

Not too late…

How can we build security into our design from the start?

YES!

security awareness

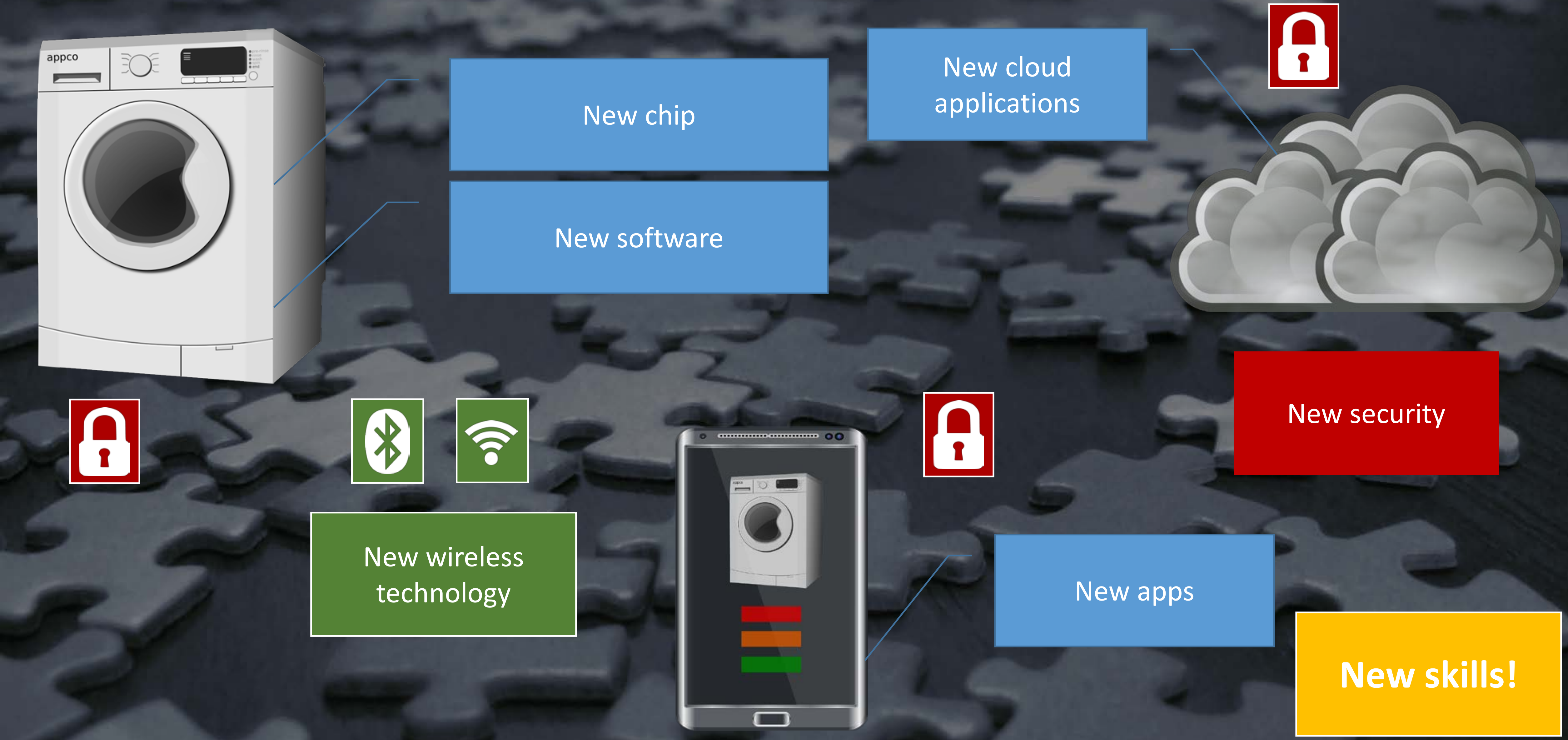
2010

now

not quite there yet!

time

Manufacturers have a lot to worry about…



New chip

New software

New cloud applications

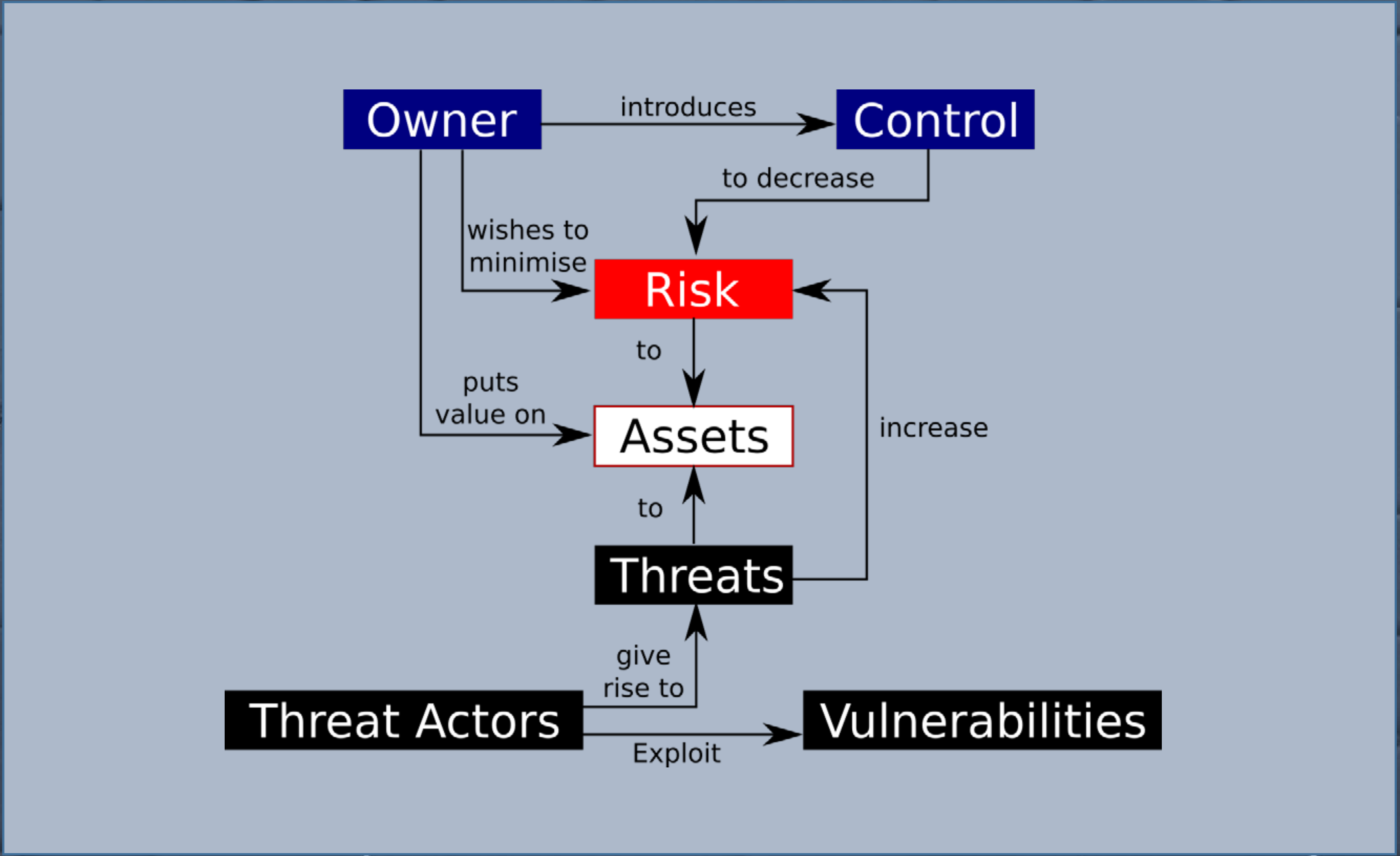
New security

New wireless technology

New apps

New skills!

How we see security



How our clients see security

time

security black hole

skills

£££

Compliance requirements don't help…

EU Medical Device Regulation 2017/74

Annex I "GENERAL SAFETY AND PERF
Chapter II "REQUIREMENTS REG UFACTURE"

17.2. "For devices that in tware that are devices in themselves, the software shal ctured in accordance with the state of the art taking in development life cycle, risk management, including on security, verification and validation."

DO SECURITY STUFF

Down the rabbit hole…

What stuff?

How much stuff?

How can I do the stuff?

Is the stuff right?

Security frameworks, guidance and standards often don’t help…

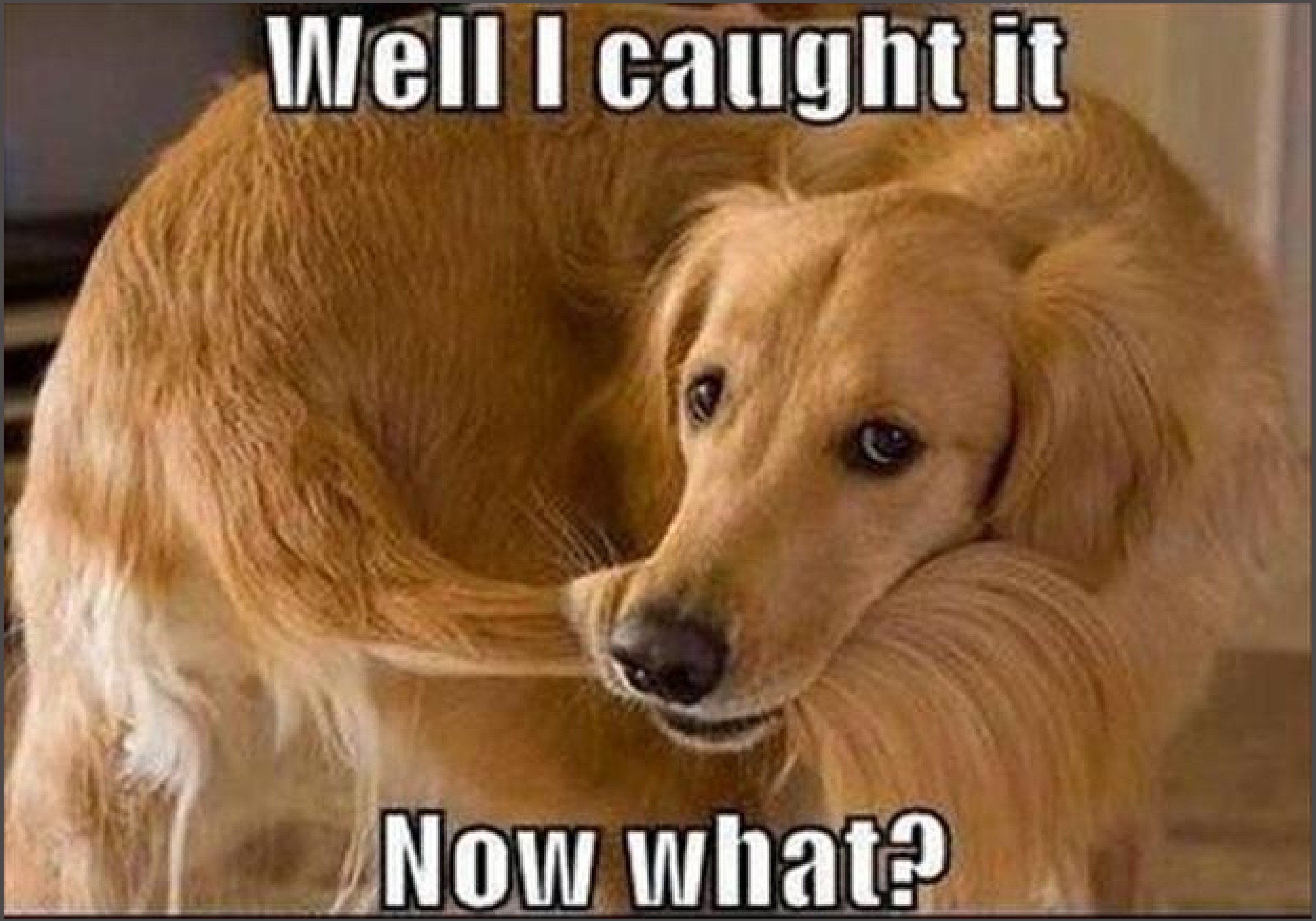
NIST SP800-37r2(draft) Risk Managem

Task P-14 “Conduct a system-level risk a isk assessment on an

“[blah blah blah] the form of risk assessment conducted … and
d of reporting results.”

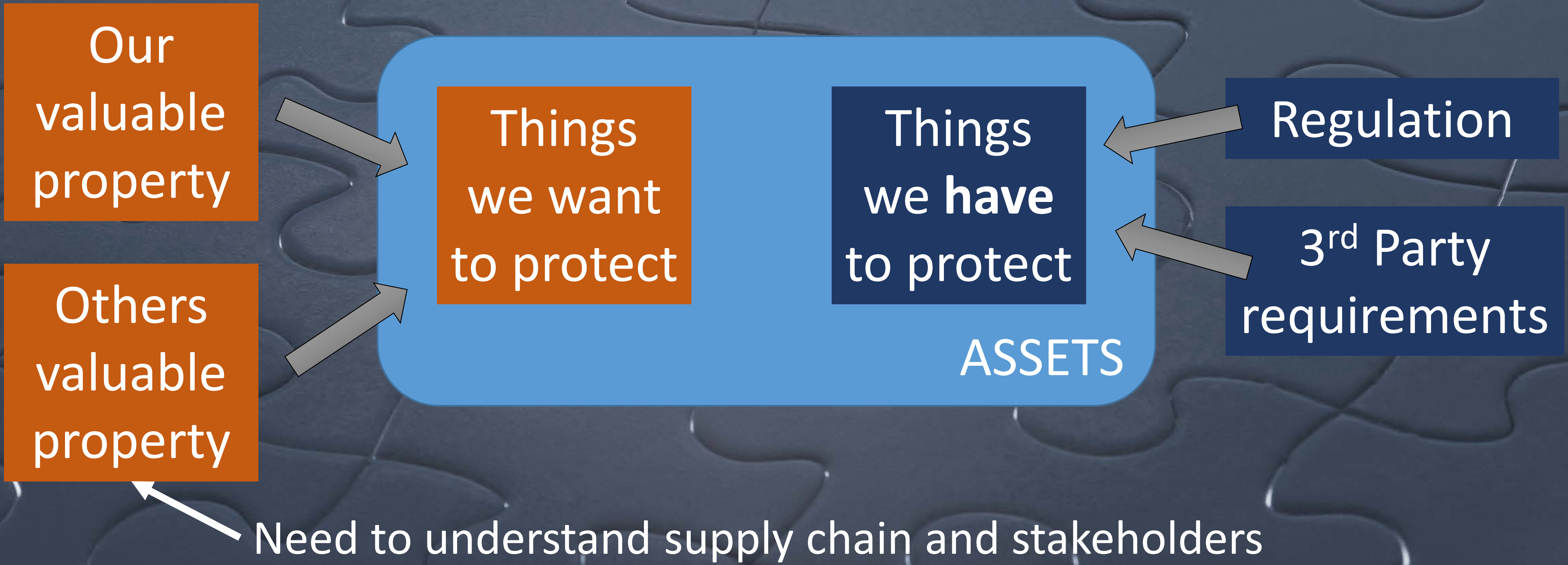
BUT HOW????!!!!

Security frameworks, guidance and standards often don’t help…



Where to start?

Preparation : We first need to work out **what needs to be protected!**



Our valuable property

Others valuable property

Things we want to protect

Things we **have** to protect

ASSETS

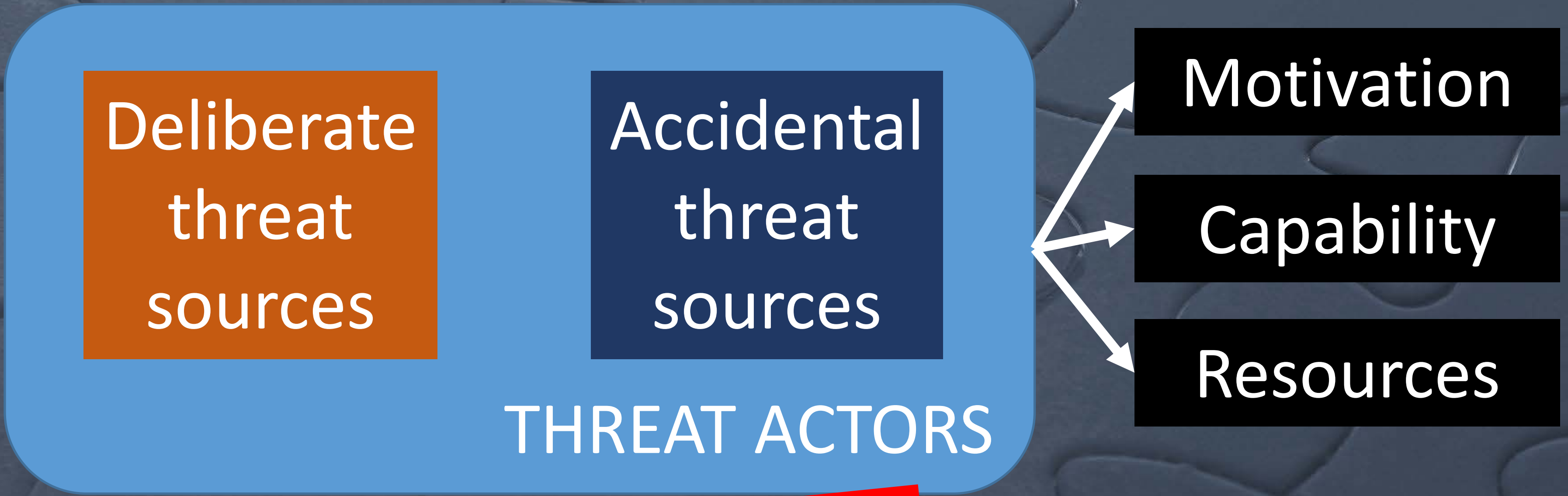
Regulation

3rd Party requirements

Need to understand supply chain and stakeholders

Where to start?

Then: **how much protection does it need**?
We need to start by understanding **who or what could attack it**



Deliberate threat sources

Accidental threat sources

THREAT ACTORS

Motivation

Capability

Resources

How much stuff?

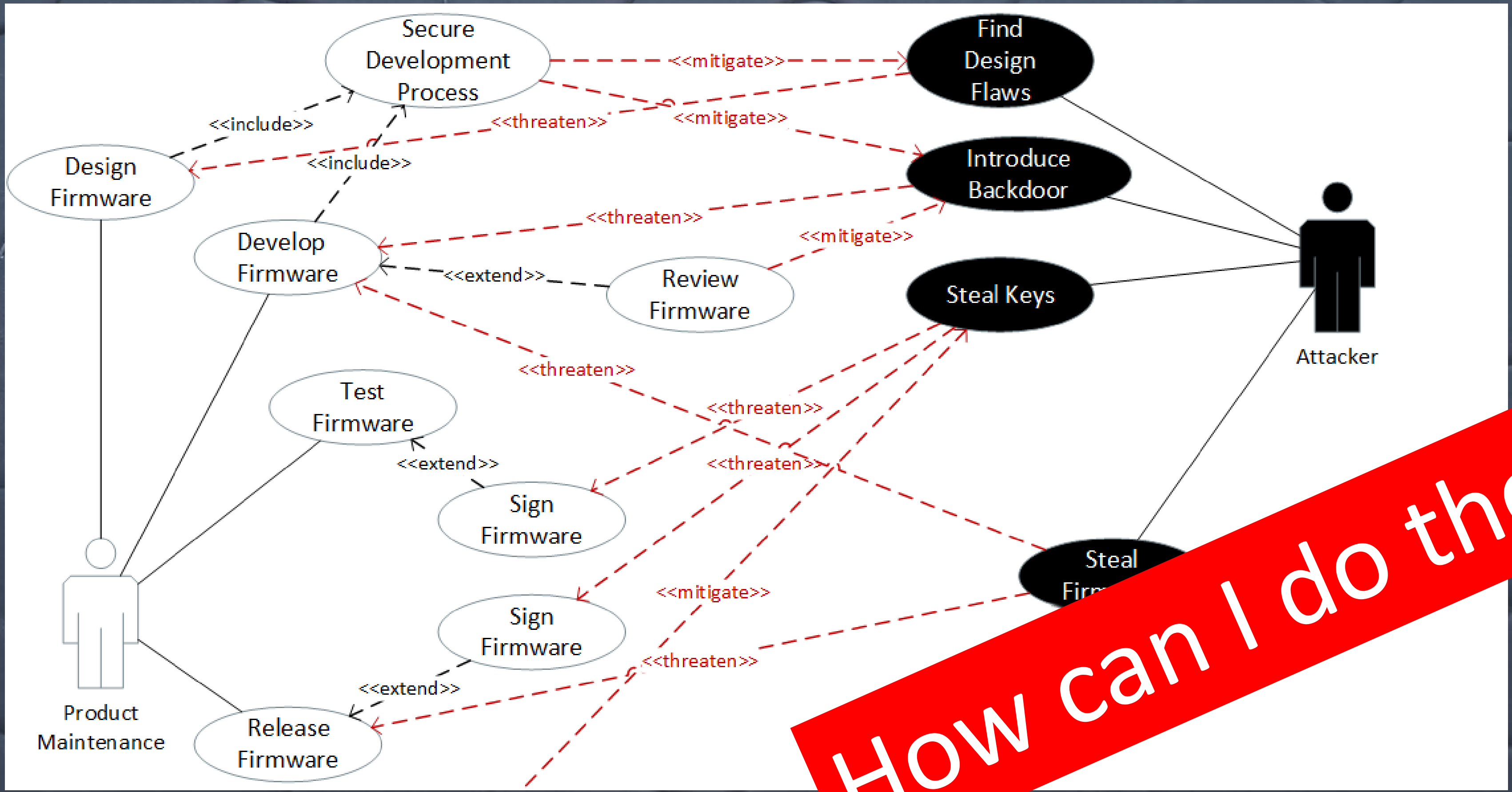
Helps b f attack

Where to start?

Then **how could it be attacked?**

System Level (Top Down) view

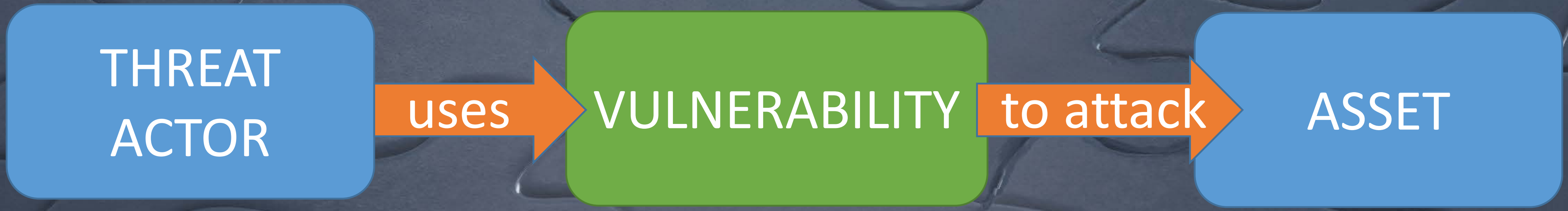
MIS-USE CASES



How can I do the stuff?

Where to start?

Also **how could it be attacked?**
Component Level (Bottom Up) view



THREAT ACTOR

uses

VULNERABILITY

to attack

ASSET

THREAT

Where to start?

Component-level threat modelling (good for existing designs)

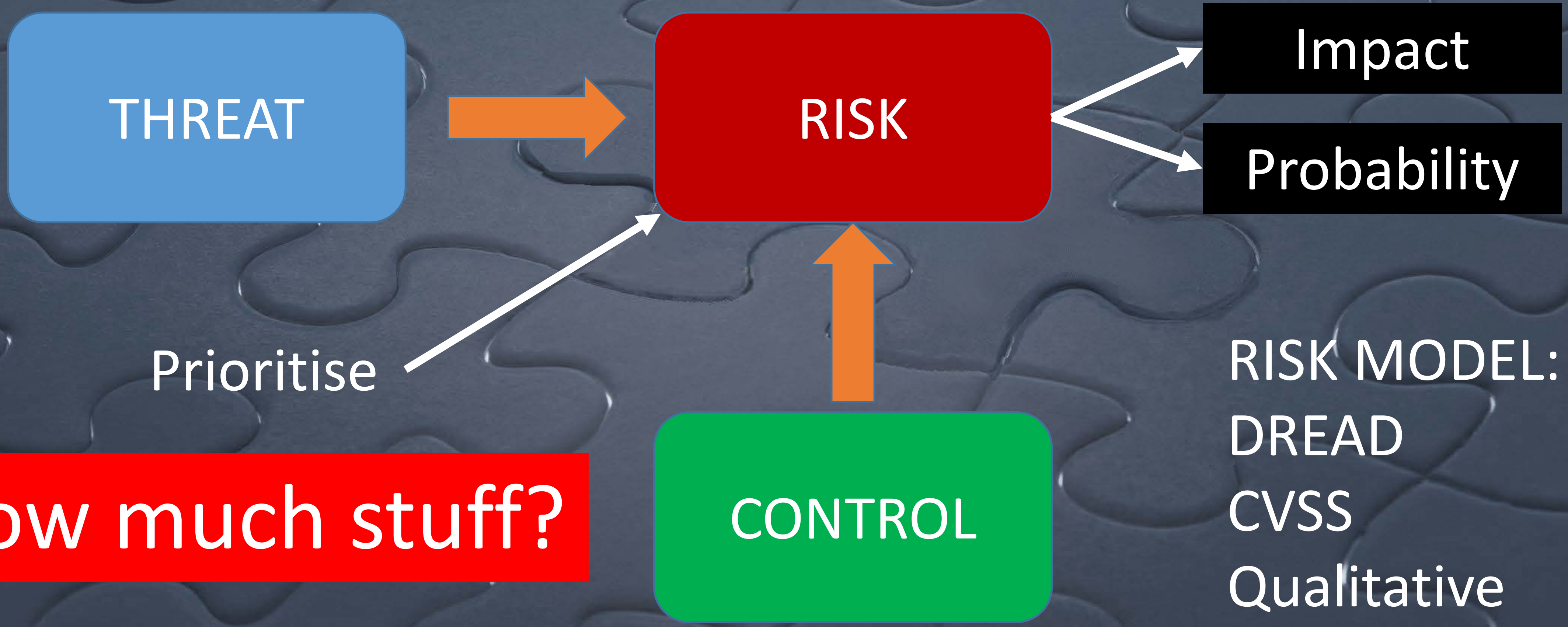
How can I do the stuff?

STRIDE ANALYSIS

- **S**poofing
- **T**ampering
- **R**epudiation
- **I**nformation leakage
- **D**enial of Service
- **E**levation of priviledge

Where to start?

The output from the threat modelling can then be used in a risk analysis

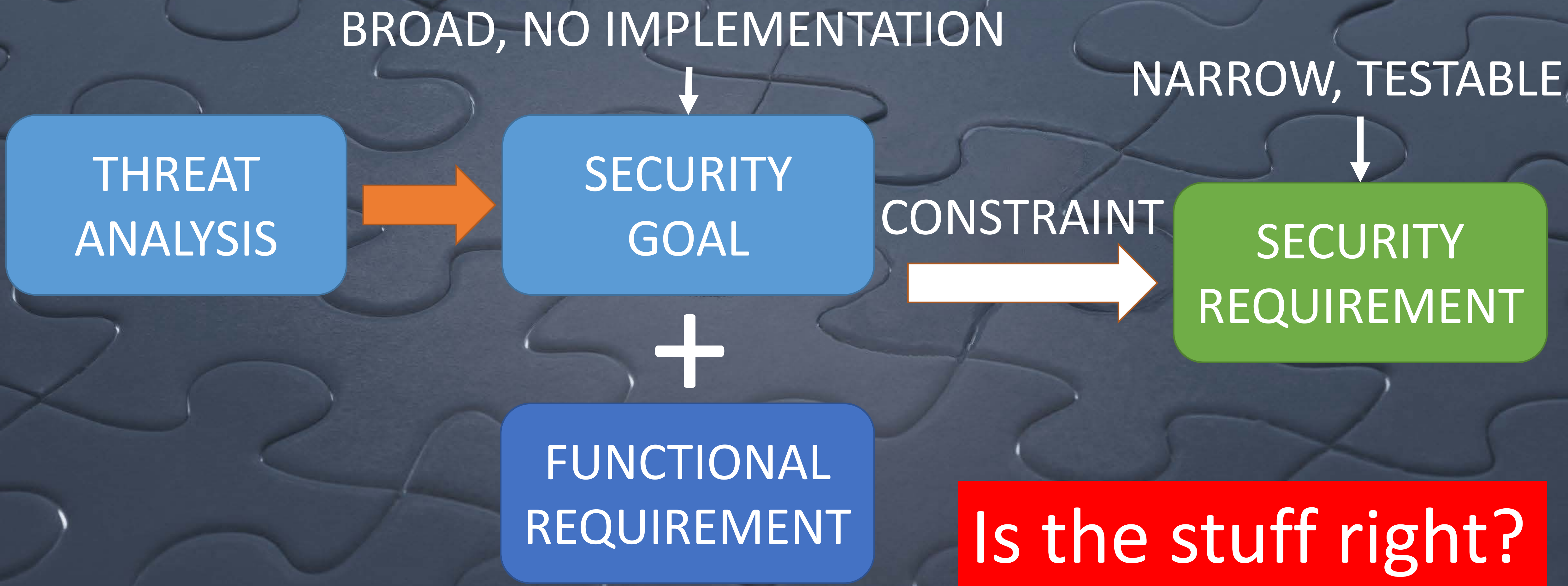


How much stuff?

RISK MODEL:
DREAD
CVSS
Qualitative

Where to start?

Security requirements generation



BROAD, NO IMPLEMENTATION

THREAT ANALYSIS

SECURITY GOAL

+

FUNCTIONAL REQUIREMENT

CONSTRAINT

NARROW, TESTABLE

SECURITY REQUIREMENT

Is the stuff right?

Summary

- Security awareness is growing
- Reputable companies DO want secure products
- Starting is difficult : where to find help?
- It takes time : there are other things need done
- It is a gradual process
    - Secure an existing design
    - Build into a new design
    - Own it
    - Add security to the organisation
    - Security is for life not just for Christmas

Questions?

CERBERUS

Security Laboratories

https://cerberus-laboratories.com
carl.shaw@cerb-labs.com