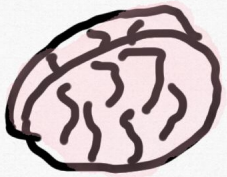
I love hard Boxes

How hardware hacking meets threat intelligence?

uh... WTF

PLAN:

- present the problema / needs
- how the project is born
- a use case
- when / why / How to contribute ?

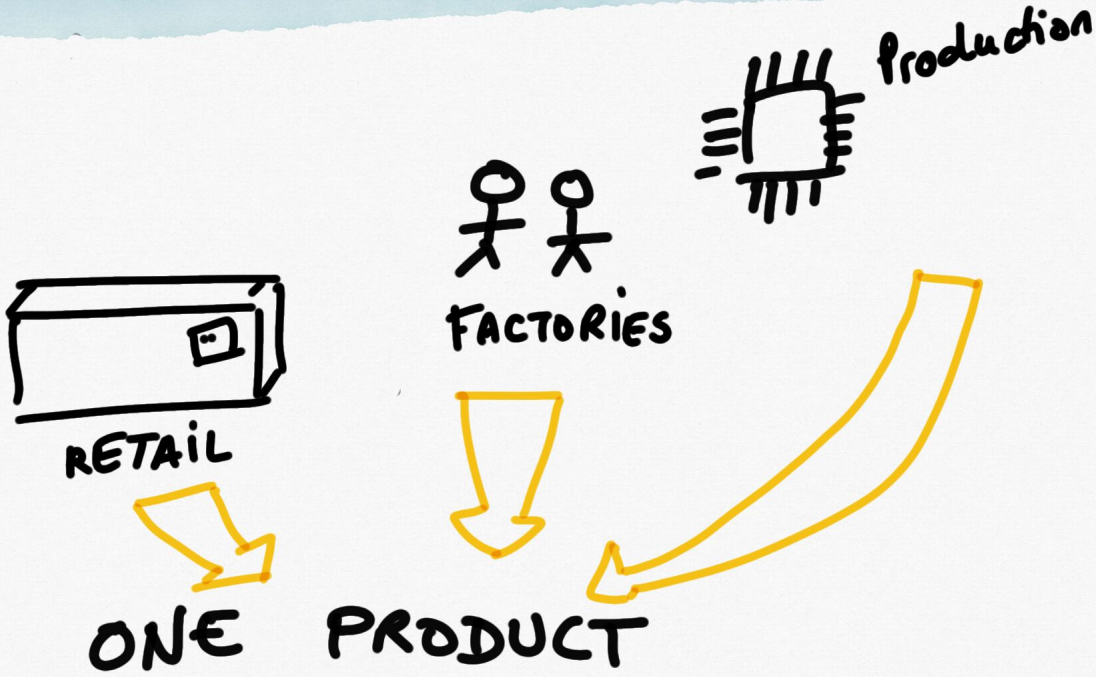


Focus :

- pedagogy
- norms
- Knowledge classification

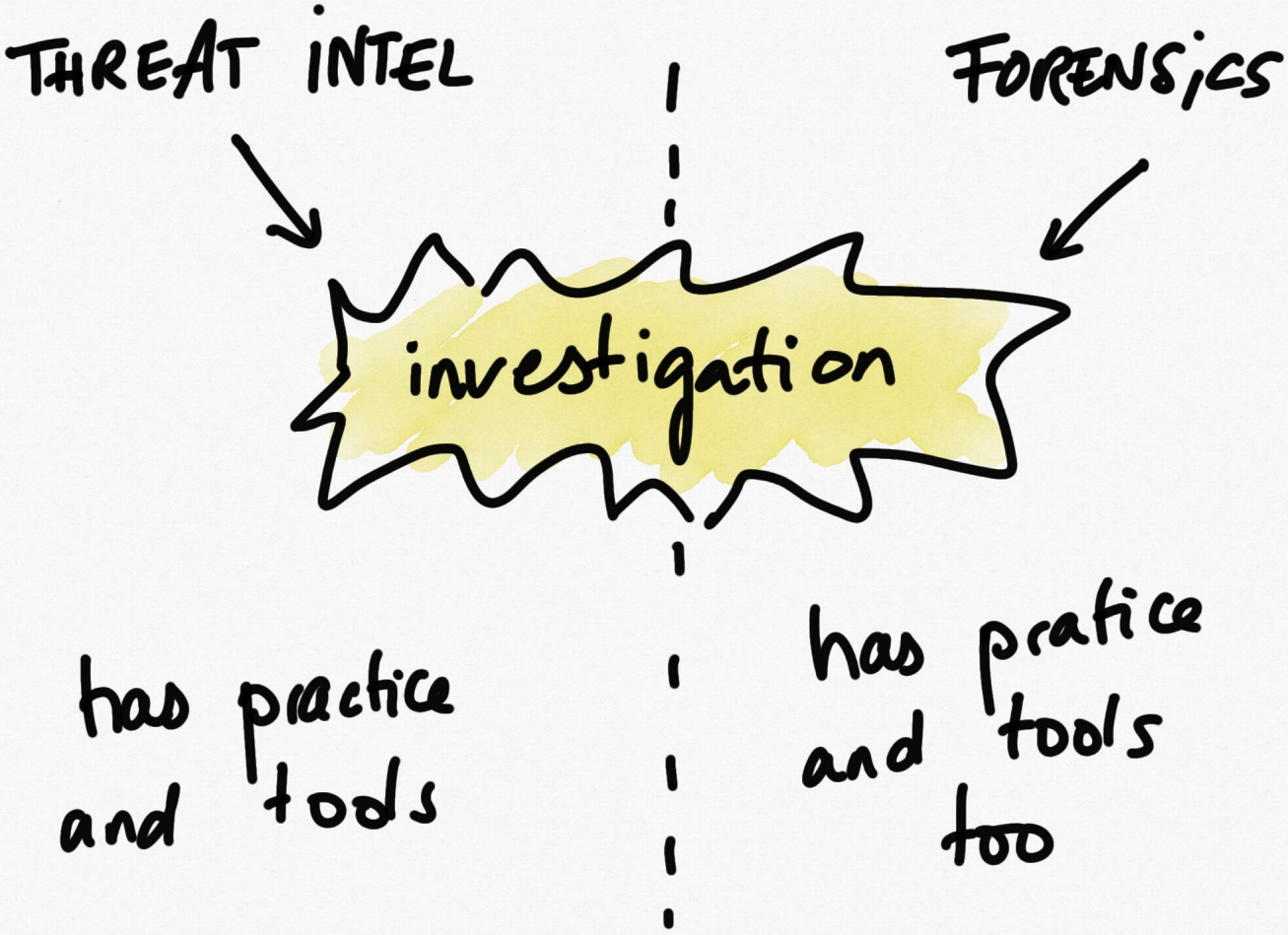
Definitions

Supply chain hardware

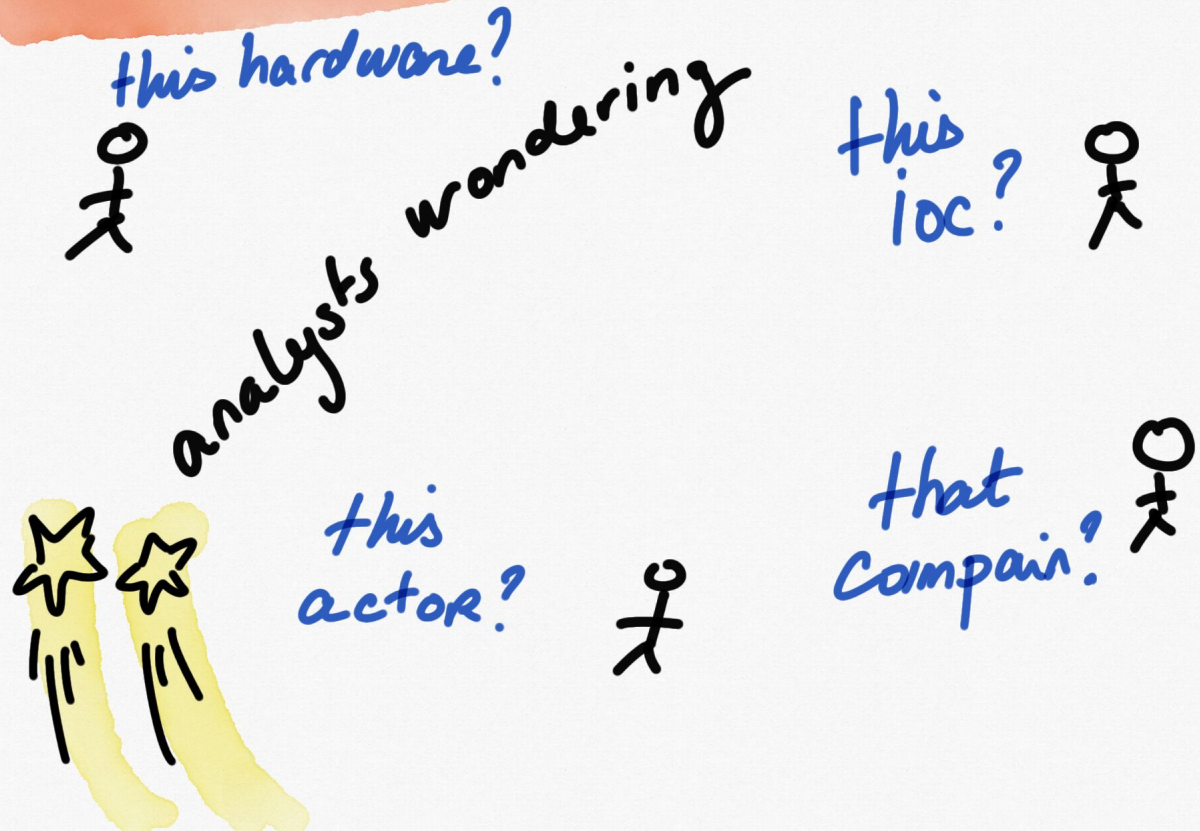


Recommended reading

Bunnie Huang - The hardware hacker


THREAT INTEL
FORENSICS
investigation
has practice and tools
has pratice and tools too

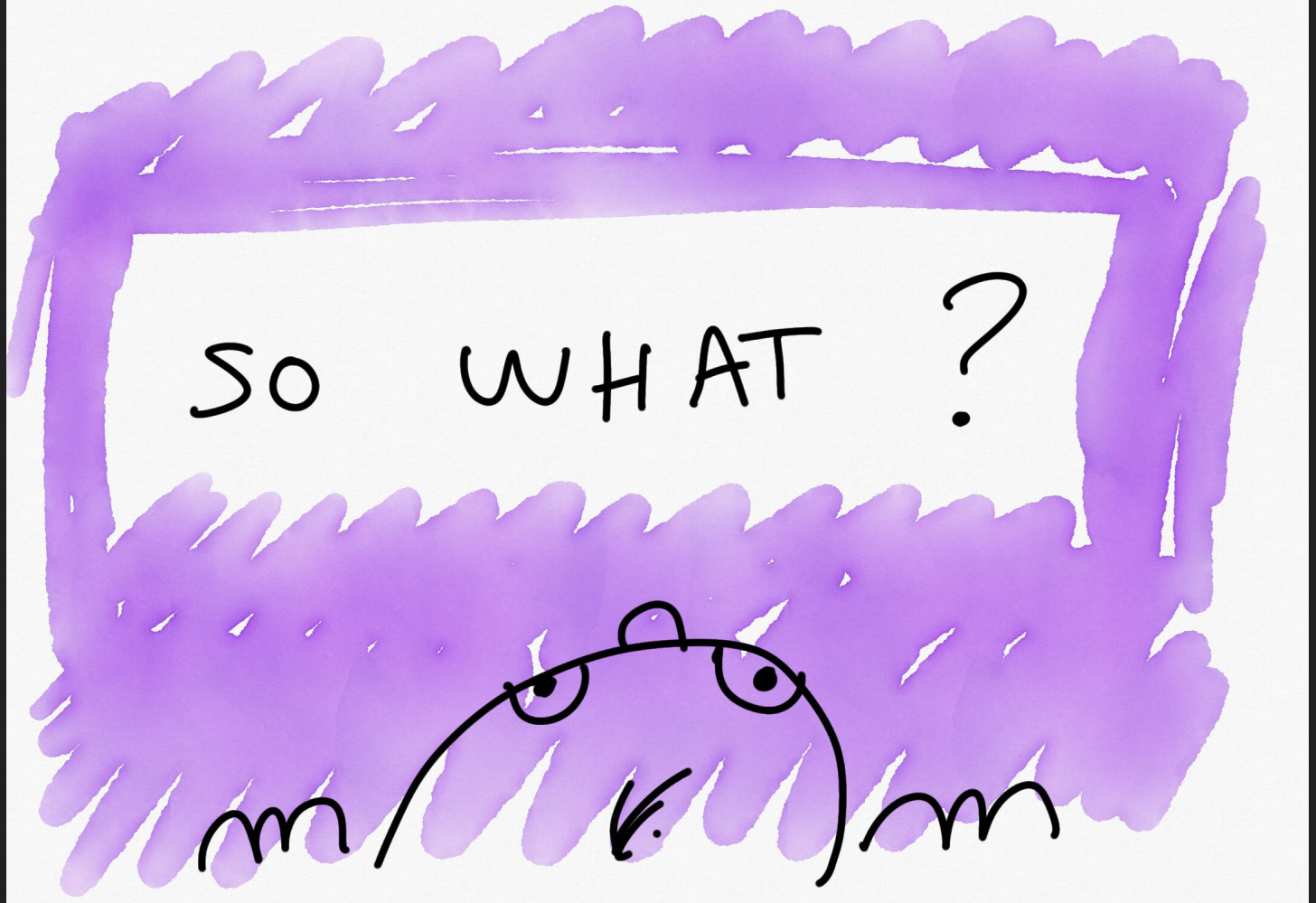
Knowledge - occurences - variables



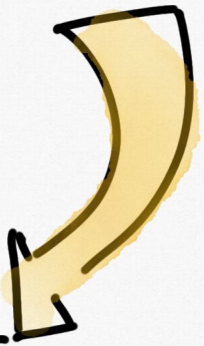
Everyone as a different experience on it:

- Knowledge
- backgrounds
- cases, targets...
- and so on ...

IT school? vs hacker

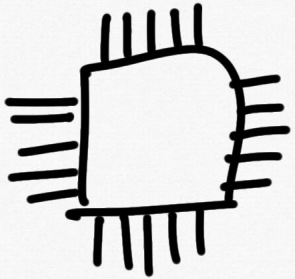

SO WHAT ?

Pieces of information
if put together

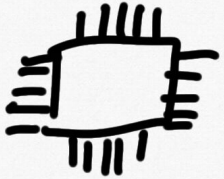


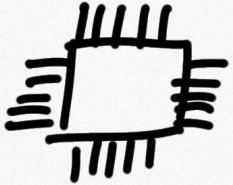
can help to profile
a threat

This little dude



- has been product in ...
- by ...
- has been powned in ...
- allows this attack ...





Knows it

↘ Pivot

↘ inform

↘ mitigate

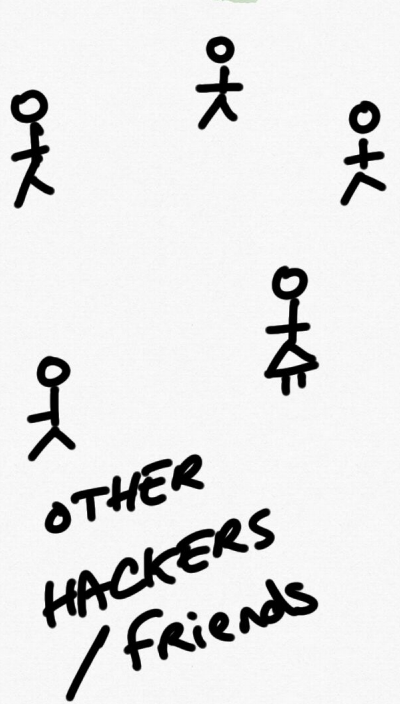
doesn't

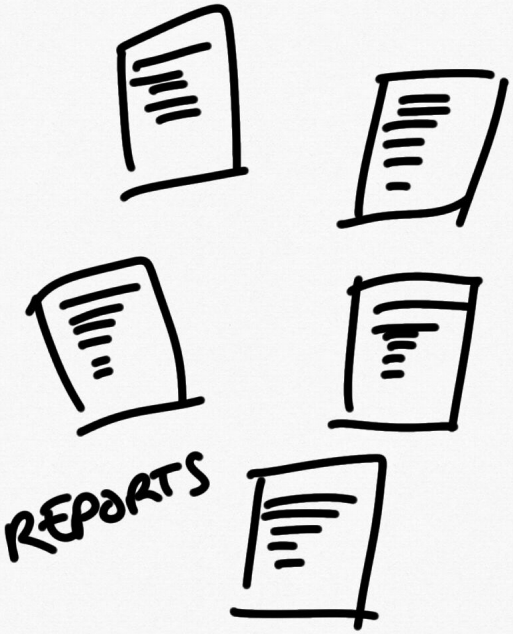
meh ...

new entry

REF ...

Where do analysts usually find intel? (info)^^






IT'S
TOUGH
(read "teuff")

we need to put
all this stuff
in one place
with an easy access

Key - Points:

- a plateform
- experience based knowledge

VS

static knowledge collection
(no temporality)

Where did the idea come from?

 → people

 → question marks

 → study cases

An example

Did a workshop about Firmware extraction

① CASE

"target"

② Technik

"firmware extraction with SERIAL"

③ GOAL

"firmware analysis"

Let's go!

is our model do-able?

1- bring the case

2- do the analysis

3- document
(diary method)

4- share with the community

The Repository

Sharing among the community

- create the database
- initiate the practice of information sharing

The Repository

* explain the project
* teach people how to contribute
* organize the knowledge
* collect "examples"

current status of dev:

- list by devices?
- list by technics?
- list by tools?
- how to display ressources?
- how to review?

contribute: submit a pull request

- theme
- goals
- device
- technics
- success and failures
- improvments
- need for help

How is the PR reviewed ?

- availibility of the device
- reproductibility of the demo
- can we teach it ? Can someone learn with the repo ?

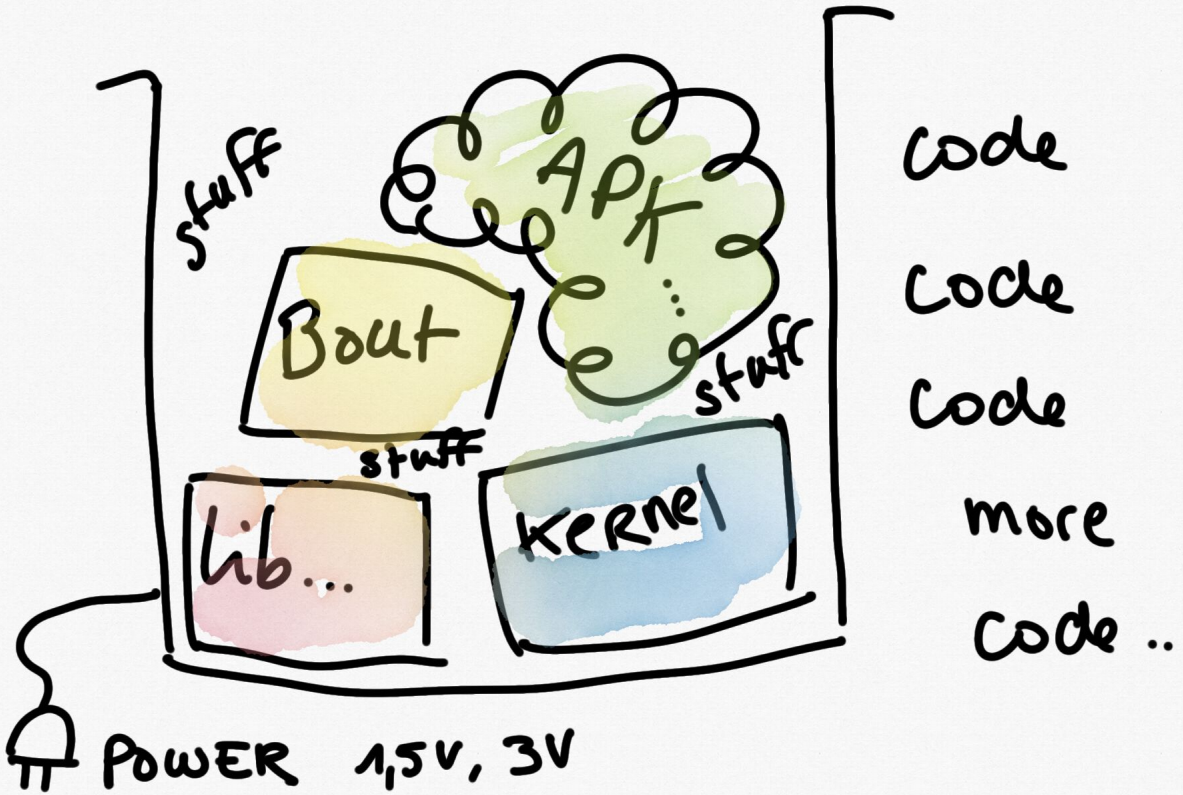
yes

no : we ask for more development

IF THE DEVICE
IS NOT
ACCESSIBLE NOW?
IT'S HARDWARE!


magic...
Emulation
magic...
magic...
magic...

Firmware Emulation...

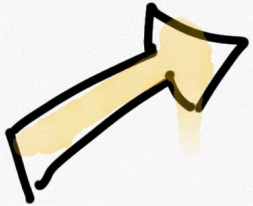


To summer-ize

- analysts search info
  as researchers, pentesters, people ... do too...
- need a space
- need a new workflow

→

MISP



people · projects, sharing

@adulau

@k0975551819


Thank
You!
xxx