ORY / summit-22

Artur Balsam

Security Engineer

rtrblsm@gmail.com

@:praying_frog:

Threat Modelling 101 aka “Hacking application on paper”

October 20th 2022

01

About me

I’ve used to like breaking things.

Right now I could see myself more as a **builder**:

- Authentication / Authorization solutions
- Security automations

02

How to do Threat Modelling?

02

How to do Threat Modelling?

What a Threat Modelling is not

- Subsidiary of penetration testing
- CI/CD security tools
- any other SDLC activity

it is addition

What a Threat Modelling is

- What we are creating?
- What can go wrong?
- What we are going to do when things will gone wrong? (because they will)

05

How to do perfect/good Threat Modelling

06

Reconnaissance that is Scope

07

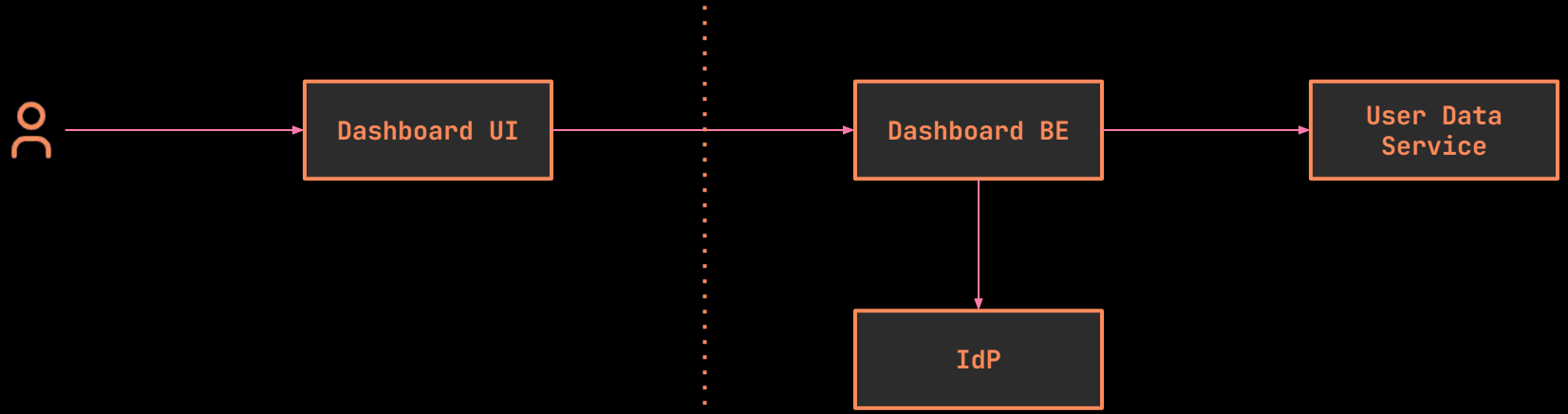
Fix title

- Actors
- Assets
- Components
- Data Flows
- Trust
- Boundaries

08

The Foundation Diagrams

The Foundation Diagrams



08

The Foundation Diagrams

08

Diagram DFD

08

Diagram C4

08

Diagram about vital product

09

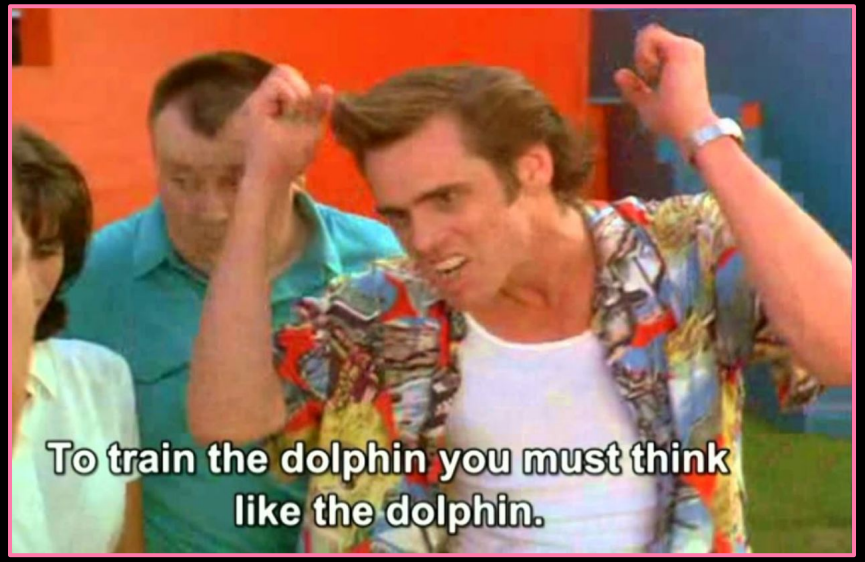
Let´s hack our application on paper known as Brainstorming

Pro(amateur)tips

- Who
- Scope
- Frequency
- Jira
- Specialization

Traps and fallbacks

- Think like you!
- Best, finite, non-existent



11

Protips for Home Office times

- Real-time notepad approved by sec-team

12

Let’s find out how it works and what we can find

12

My name is JSON

DoS JSON

11

DoS JSON

```
{
   "cow": [
     {
   "id": "5fc0129a7fa53fd88d75e4fb",
   "isActive": true,
   "registered": "2017-03-31T08:55:27 -02:00",
   "daily": [
  {
         "day": 1,
         "state": "dirty",
         "amountOfMilk": "???",
         "health":"good",
         "otherCowsThings":"jumping like a kangaroo"

     }
     ]
     }
  ]
}
```

12

email as user id-normalization

gmail.com vs hotmail.com

13

eventual consistency

or

race condition

14

Application for service man with all clients data

Q and A

When you program is a complete mess, but it does its job