# CPHoneynets

Mathis DURAND*, Marc-Oliver PAHL*, Yvon KERMARREC*

*{prénom.nom}@imt-atlantique.fr

+

speaker series

PhD schools

MOOCs

Institut Mines-Télécom

AIRBUS

IMT Atlantique
Bretagne-Pays de la Loire
École Mines-Télécom

TELECOM Paris

BNP PARIBAS
La banque d'un monde qui change

UNION EUROPÉENNE
UNANIEZH EUROPA
L'Europe s'engage en Bretagne

Région BRETAGNE

eDF

PÔLE D'EXCELLENCE
CYBER

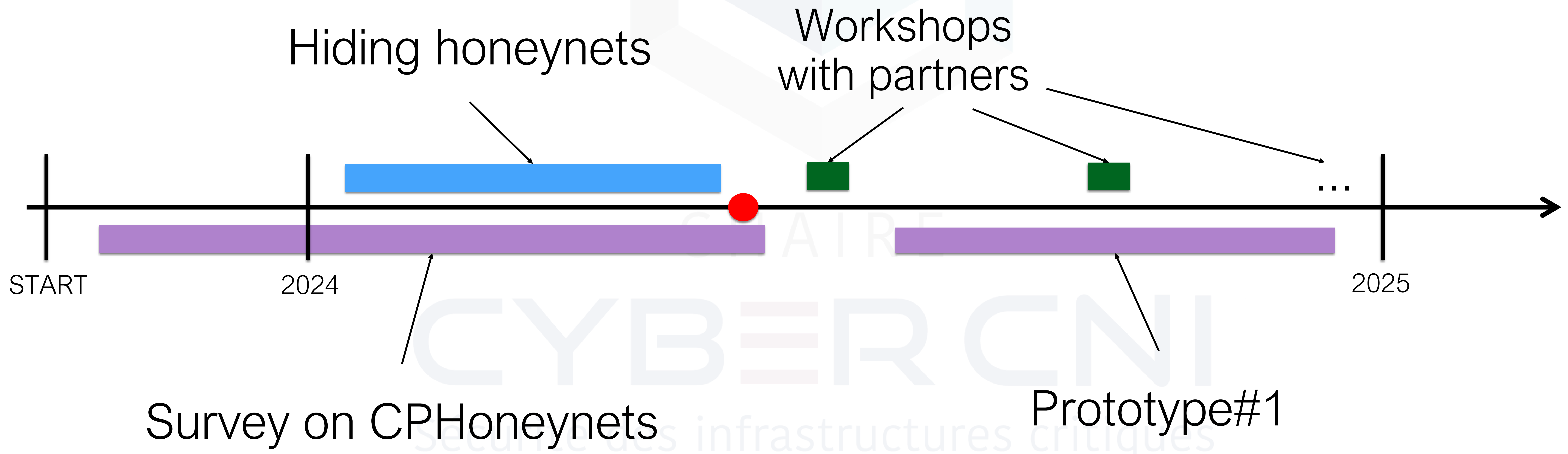
TELECOM SudParis

SNCF

# Timeline

# Context of the thesis

Timeline



# Current activities

Survey: Publication in 1-2 months [Challenge#1]

Honeynet-based CTF: TBA (ECW2024 19.11.2024) [Challenge#2]

# Next milestones

First prototype *P*: fall 2024

Evaluation of *P*: winter 2024 (automated -> real attacks)

Enhancement with new techniques: spring 2025

Levelling *CPHoneynets*: from botnets to APT-like attackers

# Thesis challenges

# Challenges identified

**Challenge#1:** Familiarize with the state of the art

**Challenge#2:** Implement different *CPHoneynets on representative use cases*

**Challenge#3:** Evaluate the prototypes quantitavtively and qualitatively

GOTO #2

# Challenges identified

Challenge#1: Identify reference architecture; open challenges

Almost done

Challenge#2:

Challenge#3:

# Challenges identified

Challenge#1:

**Challenge#2:**

- Integrate existing SW/HW to honeynet to implement use cases
- Advancing the complexity of the Honeynets

Challenge#3:

# Challenges identified

| | |
|---|---|
| Challenge#1: | Evaluate CTI gathering |
| Challenge#2: | Evaluate security mechanisms testing |
| **Challenge#3:** | Evaluate retainment |

# What is *CPHoneynet*?

# CPHoneynet

## Definition

*CPHoneynet*: a **network of honeypots** designed to mimic an **Operational Technology** system or a Cyber-Physical system.
Goals: **collect data** on attackers or **keep cybercriminals away**.

# Usage of Honeynets in the wild

## Context

**Solution Provider:** Enhance CPHoneynet to sell security solutions

**Infrastructure owner:** Find use cases to integrate CPHoneynet solutions in their infrastructure

**Aim:** Collect data on tools, behaviors, and vulnerabilities

**Target:** High-skill and high-ressource attackers

**Context:** OT Systems (Cyber-Physical Systems)

# CPHoneynet

## Reference Architecture

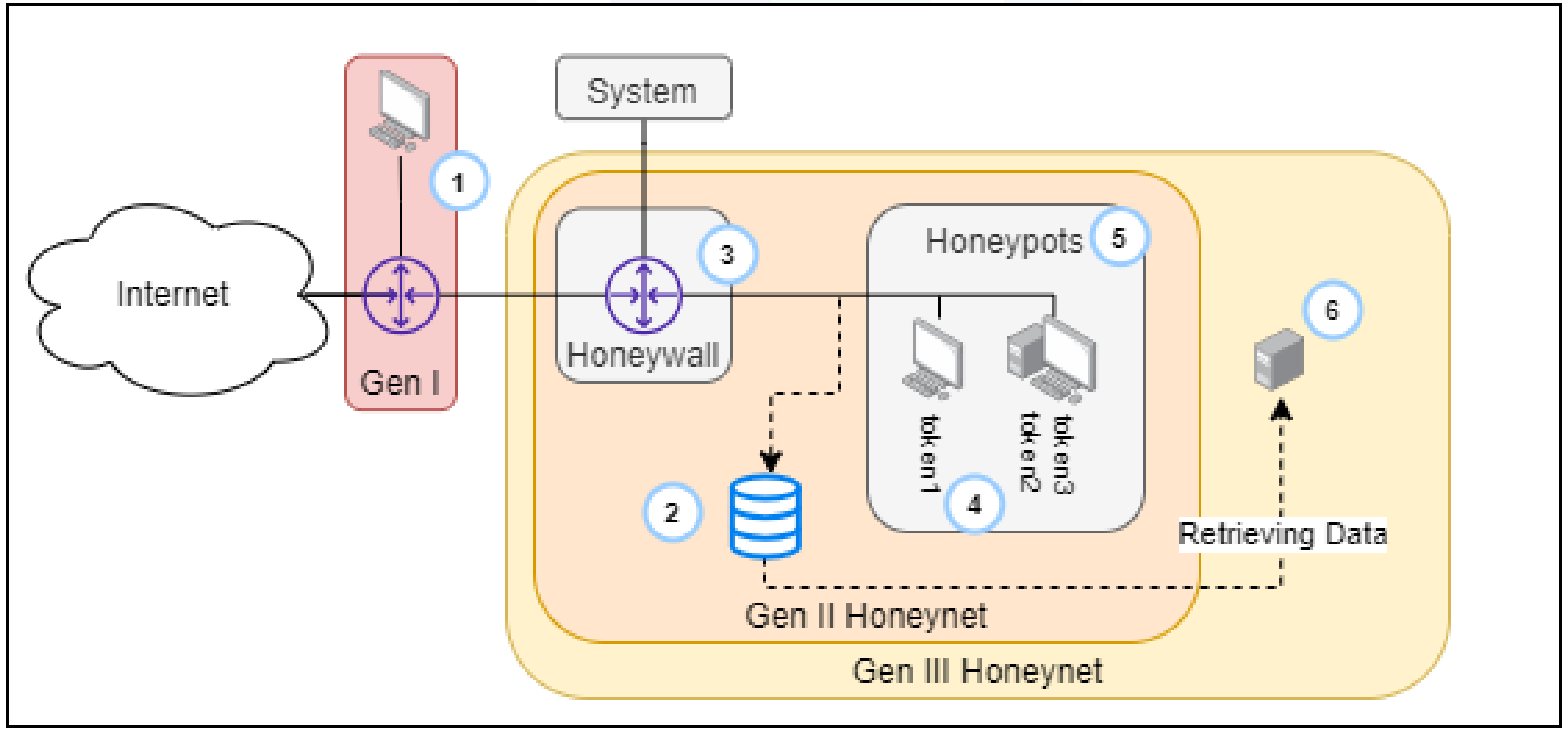
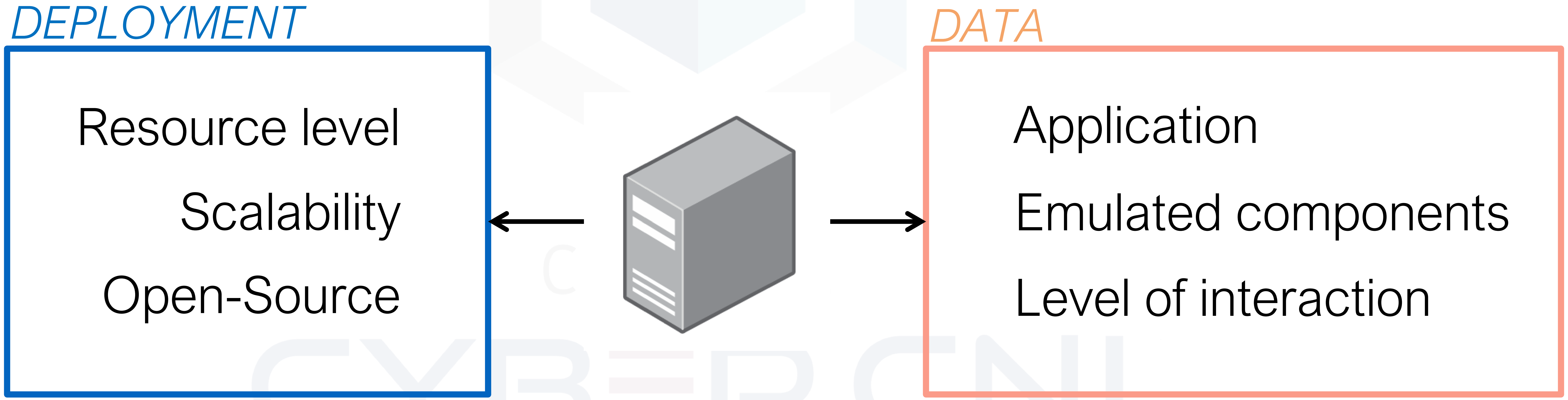


Fig.3: Reference Architecture of Honeynet

# CPHoneynet

## Taxonomy [Lackner2021]



*DEPLOYMENT*

Resource level

Scalability

Open-Source

*DATA*

Application

Emulated components

Level of interaction

# CPHoneynet

## Use Cases

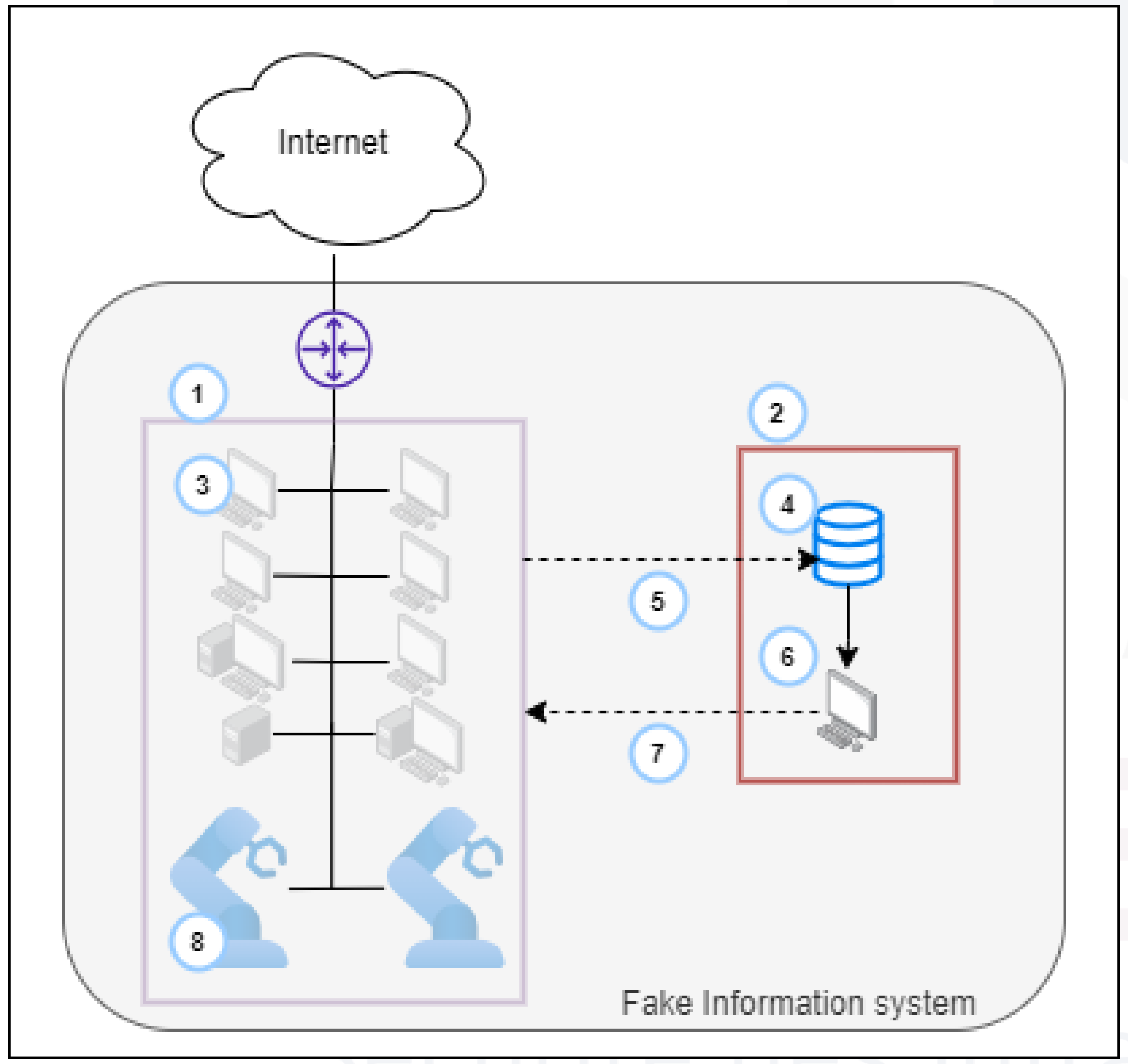


Fig.1: Architecture of CTI Collector CPHoneynet

### USE CASE #1: CTI Collector

- “Realistic” system [Bernieri2019]

- “Attractive” system [Bernieri2019]

# CPHoneynet

## Use Cases

USE CASE #2: Attack Decoy

Sealing -

Competitiveness -

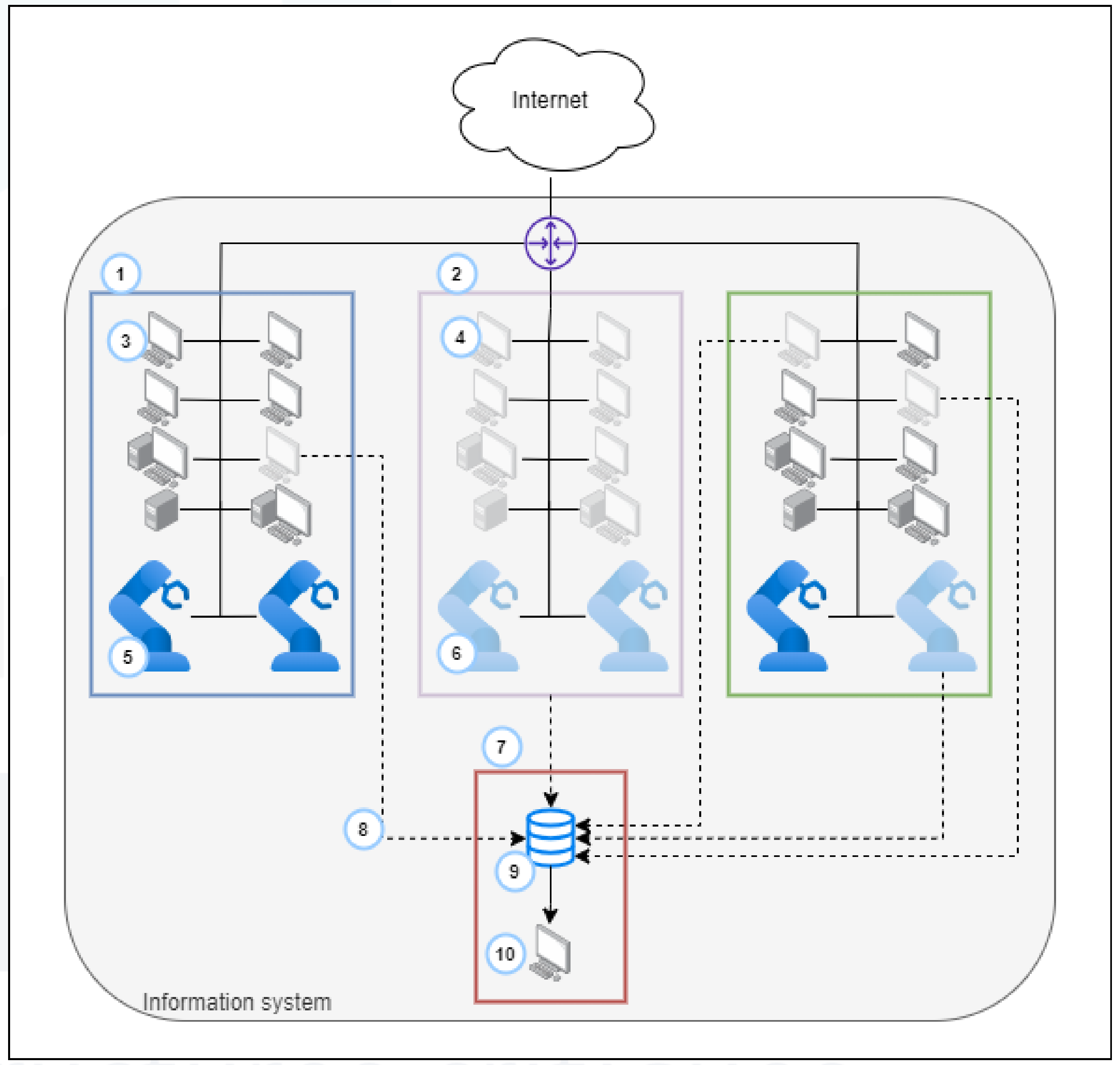


Fig.2: Architecture of Attack Decoy CPHoneynet

# CPHoneynet

Research topics

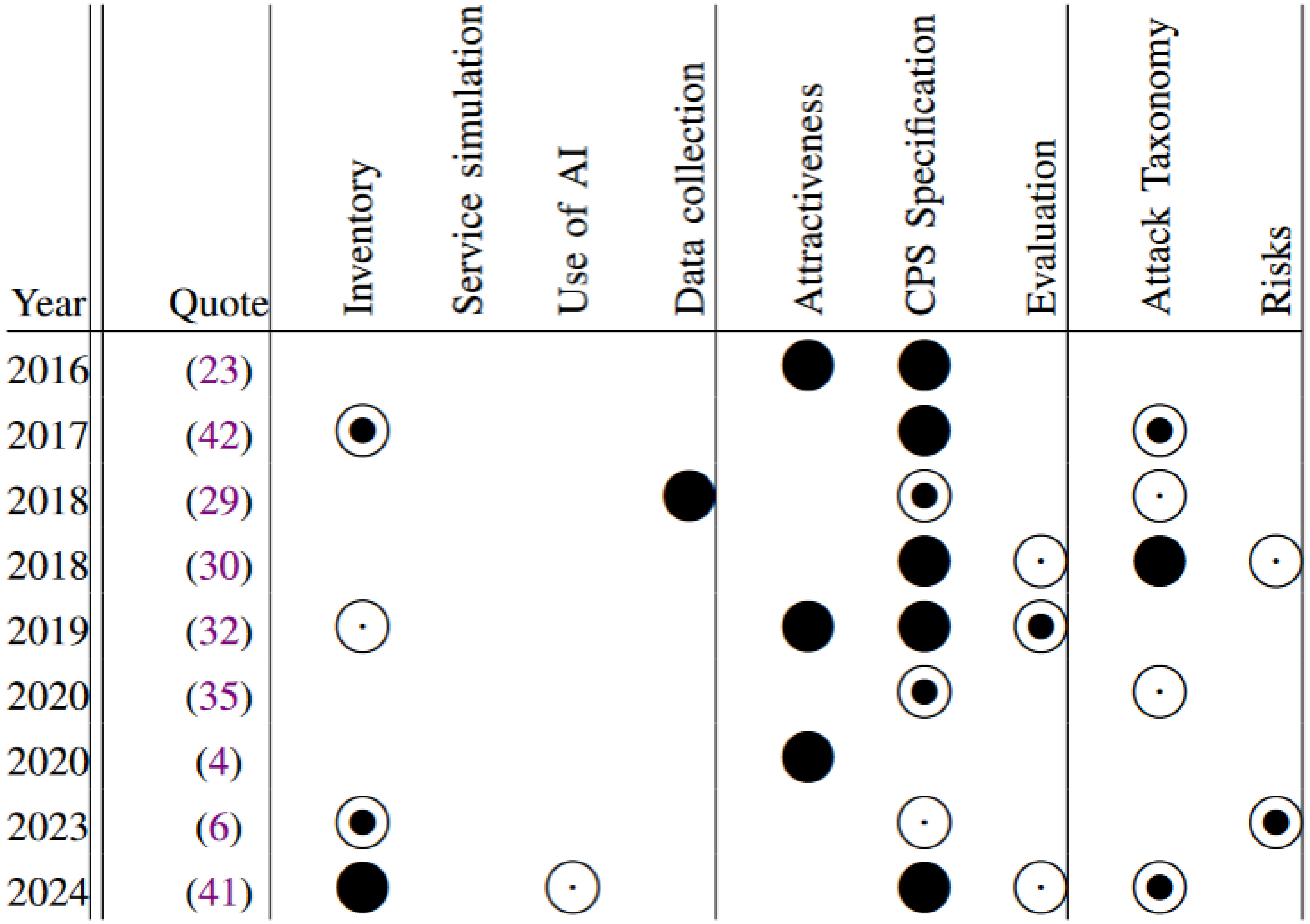
## Challenges of adapting honeynets to CPS

| | |
|---|---|
| MimePot: attractive and stealthy CPHoneynet | [Bernieri2019] |
| Large-scale and real-time CPHoneynet | [Almulla2018] |
| Digital twin and CPHoneynets | [Hadar2020] |

## Threat analysis in CPS context

| | |
|---|---|
| 5 frequent scenarii | [Sousa2024] |
| Game-theory for optimal strategy | [Li2020] |
| Misuse a Honeypot | [Dornseif2004] |

# CPHoneynet

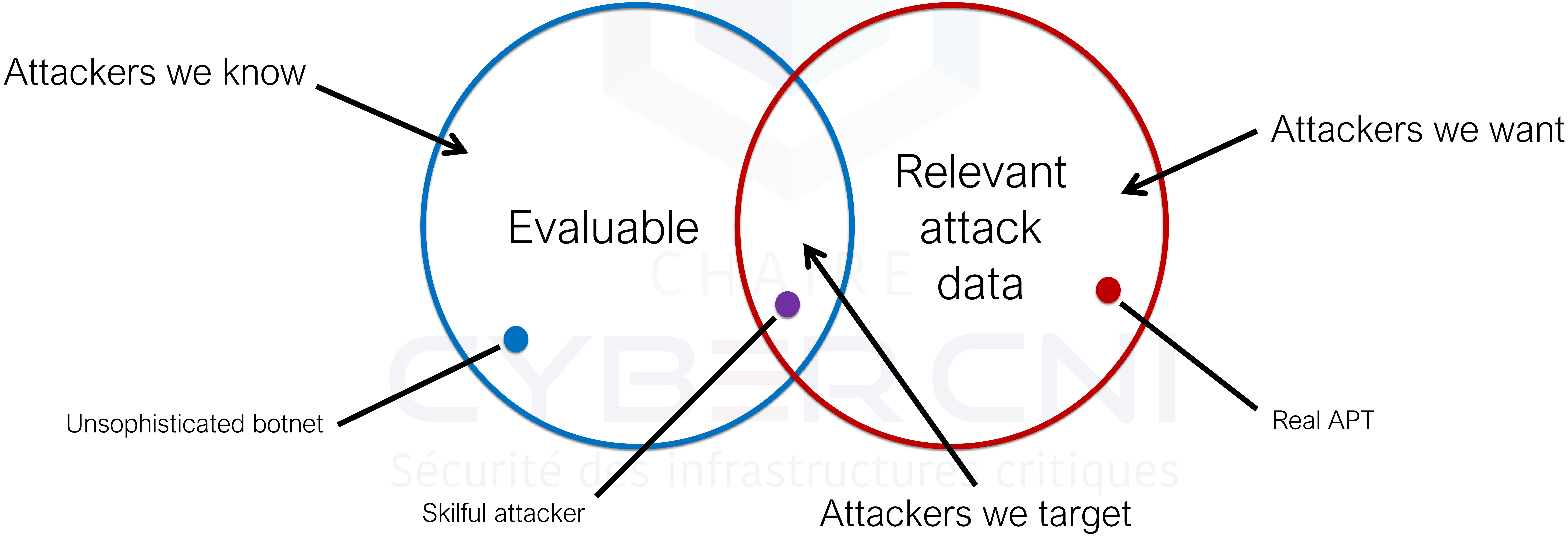


| Year | Quote | Inventory | Service simulation | Use of AI | Data collection | Attractiveness | CPS Specification | Evaluation | Attack Taxonomy | Risks |
|---|---|---|---|---|---|---|---|---|---|---|
| 2016 | (23) | | | | | ● | ● | | | |
| 2017 | (42) | ◉ | | | | | ● | | ◉ | |
| 2018 | (29) | | | | ● | | ◉ | | ⊙ | |
| 2018 | (30) | | | | | | ● | ⊙ | ● | ⊙ |
| 2019 | (32) | ⊙ | | | | ● | ● | ◉ | | |
| 2020 | (35) | | | | | | ◉ | | ⊙ | |
| 2020 | (4) | | | | | ● | | | | |
| 2023 | (6) | ◉ | | | | | ⊙ | | | ◉ |
| 2024 | (41) | ● | | ⊙ | | | ● | ⊙ | ◉ | |

Fig.4: Research topics on CPHoneynets

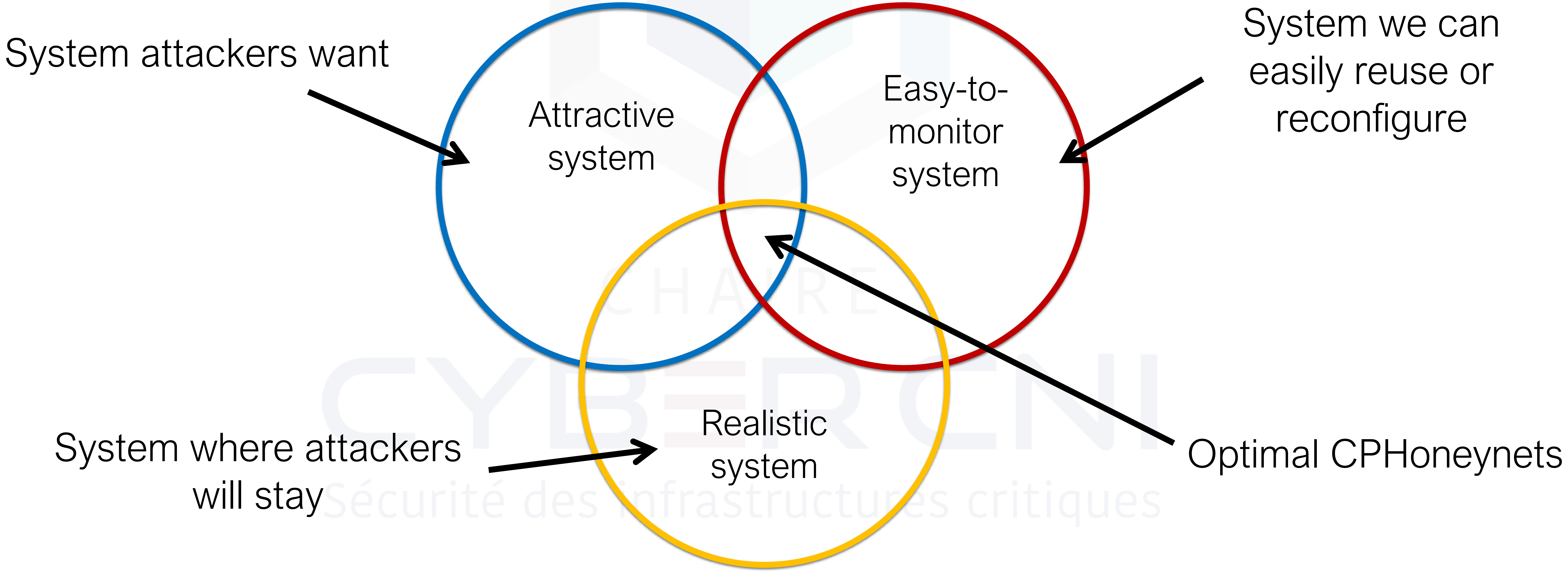
# CPHoneynet

## Attacker model



# CPHoneynet

## Specific context



# Relation with partners

# Context of the thesis

Chair

- Partners:
  - State of the art
  - Users stories

- CyberCNI:
  - Fischertechnik
  - CyberRange

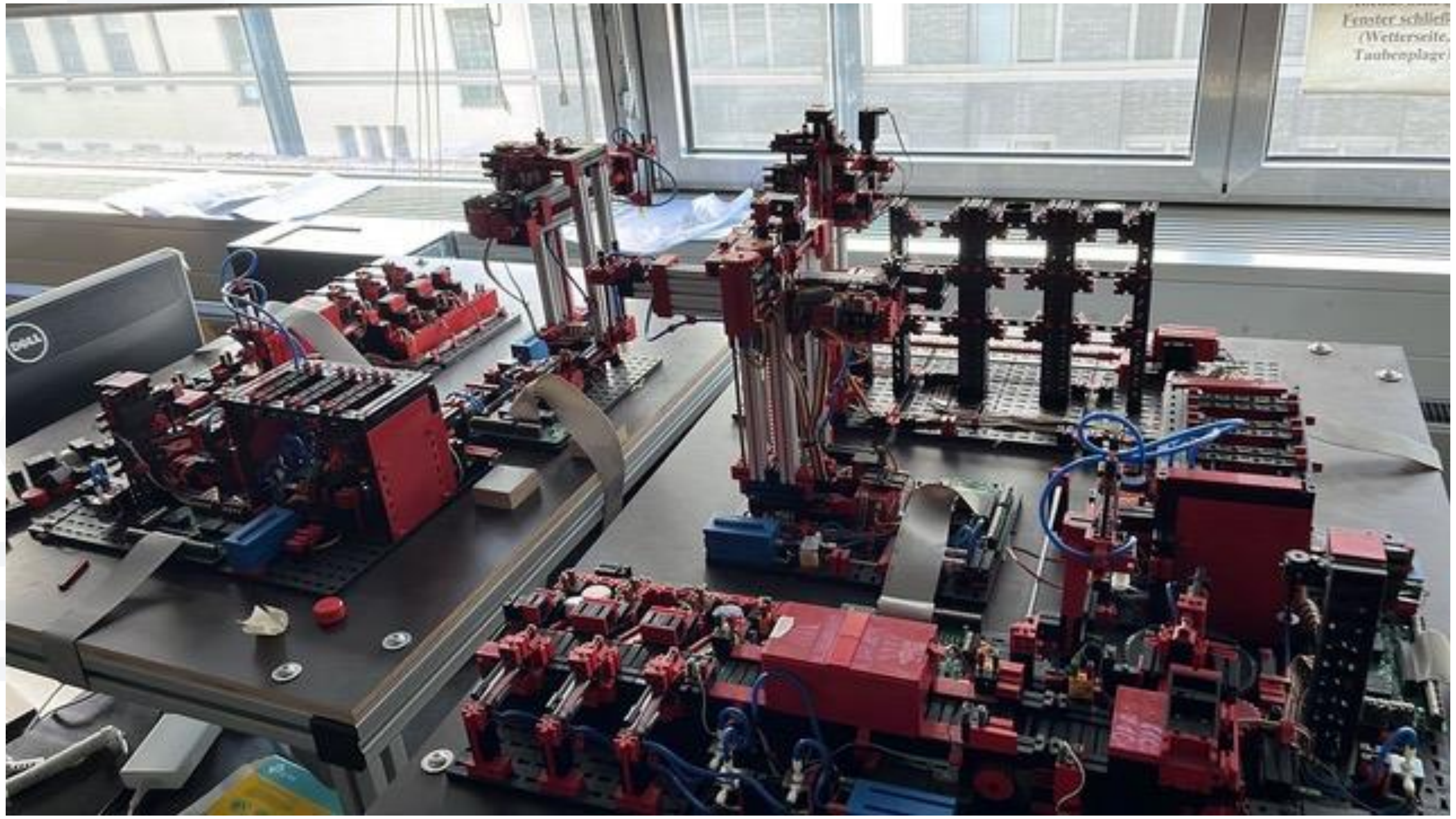
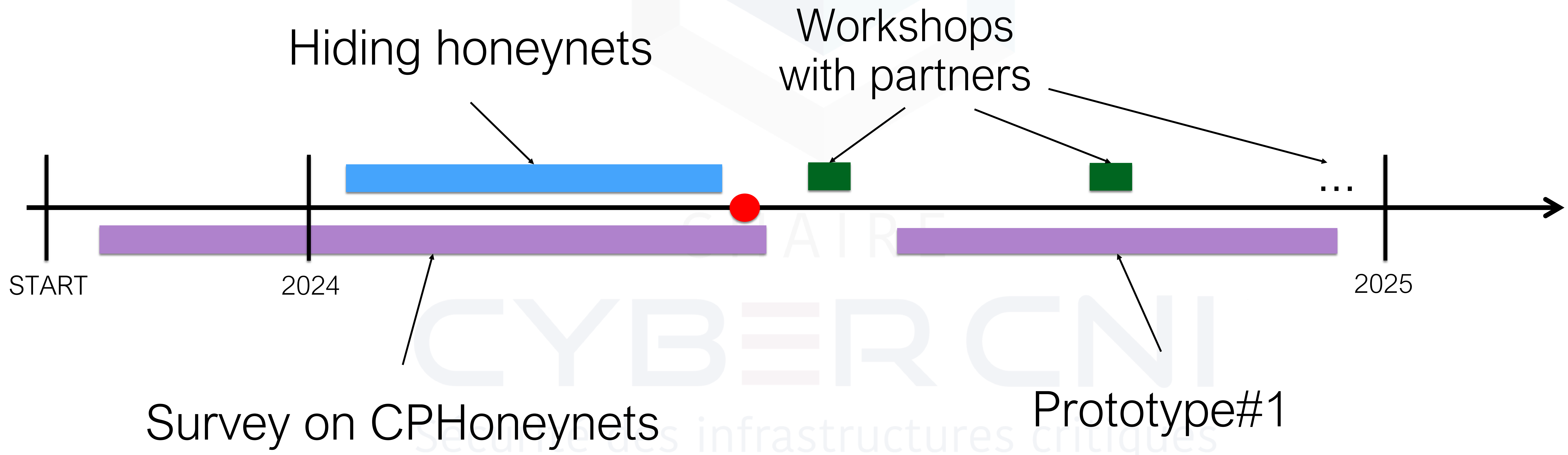


Fig.5: Fischertechnik (IMT Atlantique)

# Context of the thesis

Timeline



# Thank you for your attention.

Question time!

mathis.durand@imt-atlantique.fr

# References

[Dornseif2004] M. Dornseif, T. Holz, and C. N. Klein, “Nosebreak-attacking honeynets,” pp. 10–11, 2004

[Almulla2018] S. Almulla, C. Fachkha, and E. Bou-Harb, “Cyber security threats targeting cps systems: A novel approach using honeypots,” in The Twelfth International Conference on Emerging Security Information, Systems and Technologies, SECURWARE, 2018

[Bernieri2019] G. Bernieri, M. Conti, and F. Pascucci, “Mimepot: a model-based honeypot for industrial control networks,” in 2019 IEEE International Conference on Systems, Man and Cybernetics (SMC), 2019, pp. 433–438.

[Hadar2020] E. Hadar, D. Kravchenko, and A. Basovskiy, “Cyber digital twin simulator for automatic gathering and prioritization of security controls’ requirements,” in 2020 IEEE 28th International Requirements Engineering Conference (RE). IEEE, 2020, pp. 250–259

[Li2020] B. Li, Y. Xiao, Y. Shi, Q. Kong, Y. Wu, and H. Bao, “Anti-honeypot enabled optimal attack strategy for in- dustrial cyber-physical systems,” IEEE Open Journal of the Computer Society, vol. 1, pp. 250–261, 2020.

[Lackner2021] P. Lackner, “How to mock a bear: Honeypot, honeynet, honeywall & honeytoken: A survey,” in ICEIS (2), vol. 2. Science and Technology Publications, Lda, 2021, pp. 181–188

[Sousa2024] L. Sousa, J. Cec´ılio, P. Ferreira, and A. Oliveira, “Reconfigurable and scalable honeynet for cyber-physical systems,” arXiv preprint arXiv:2404.04385, 2024.