Hôpitaux Universitaires de Marseille | ap·hm

Carrousel 6: End-users and risk-management / Integration of the SAFECARE solutions

SAFECARE Commercial event – Philippe Tourron, Frédéric Nodot, Stéphane Nardy
Paris, 2021-11-30

SAFECARE has received funding as part of the "Secure societies – Protecting freedom and security of Europe and its citizens" challenge of the Horizon 2020 Research and Innovation programme of the European Union under grant agreement 787002

European Commission | HORIZON 2020

Virtual Hospital

Role play session : Defend a hospital

SAFECARE

Integrated cyber-physical security for health services

A danger occurs …

PHARMACY
VACCINE PROCESS

COVID-19 VACCINE

SAFECARE
Integrated cyber-physical security for health services

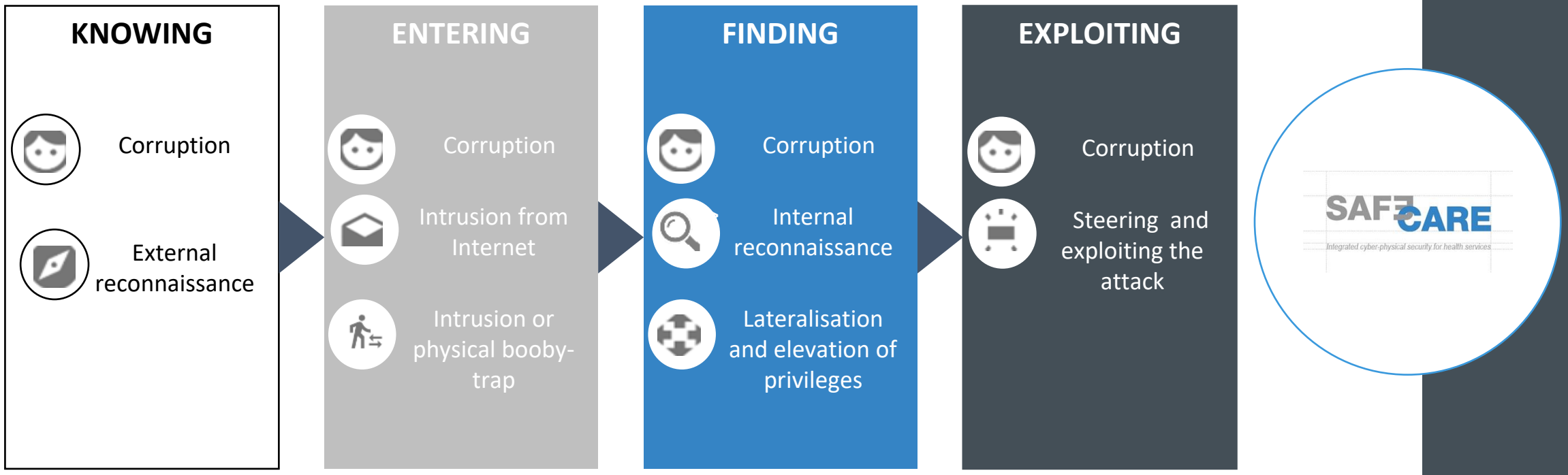
Role Play

Context	Covid-19 vaccine
Your mission	Protect Vaccine process in a hospital

- You discover an attack path step by step and you have to defend/react in front of the situation

- Feedback/Conclusion : how Safecare can bring solutions

Description method of scenarios



It is important to note that these steps are modular (for example according to whether the attacker attacks directly or by bouncing via a stakeholder of the ecosystem)

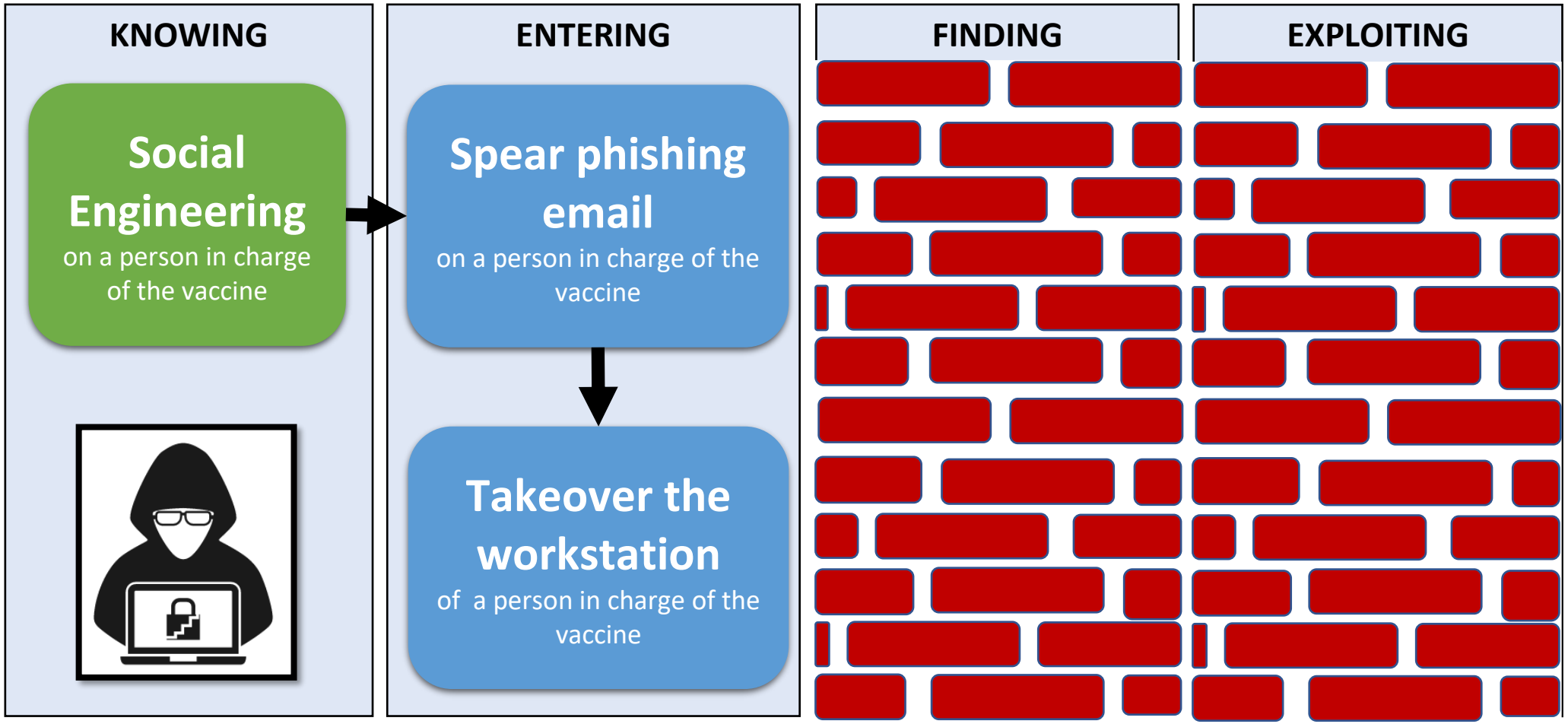
Cyber-attack in a COVID-19 context

Question 1 – INTRODUCTION - Which threat could be the most feared in the context of Covid-19 vaccine in a hospital ?

KNOWING	ENTERING	FINDING	EXPLOITING
			

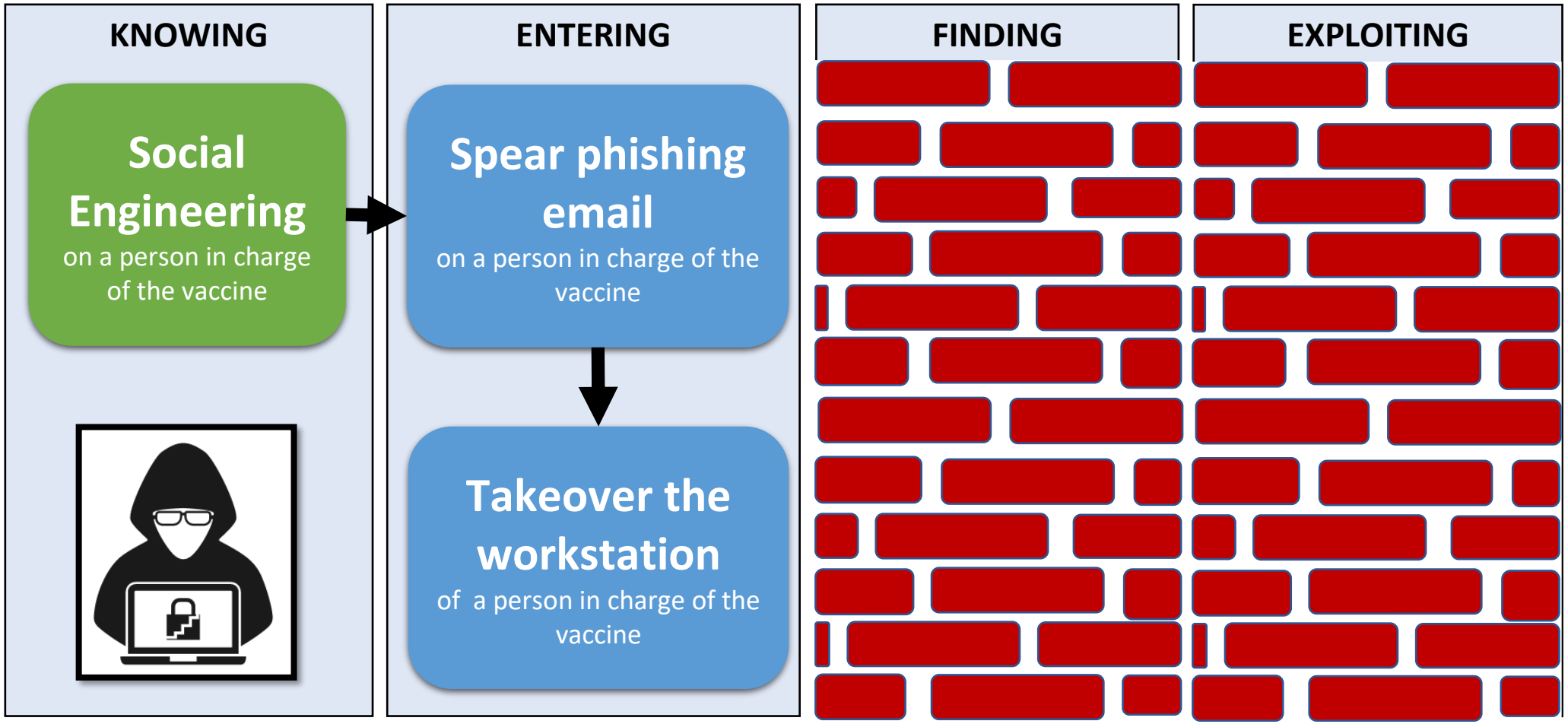
Cyber-attack in a COVID-19 context

Question 2 - the DETECTION
Which detection method is best? Who should be contacted? How Quickly?



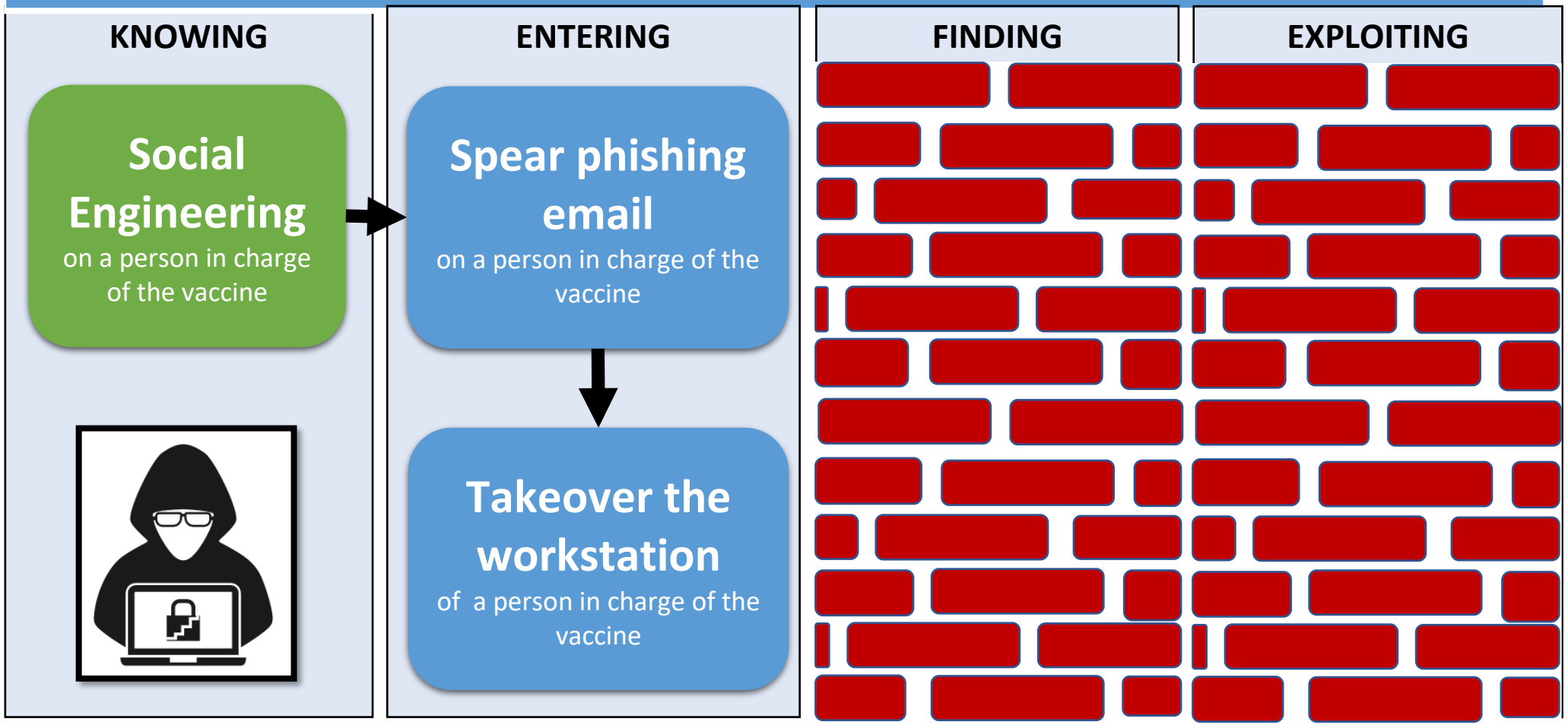
Cyber-attack in a COVID-19 context

Question 3 - the MITIGATION
Which mitigation measure to choose? How likely is the attack to succeed?



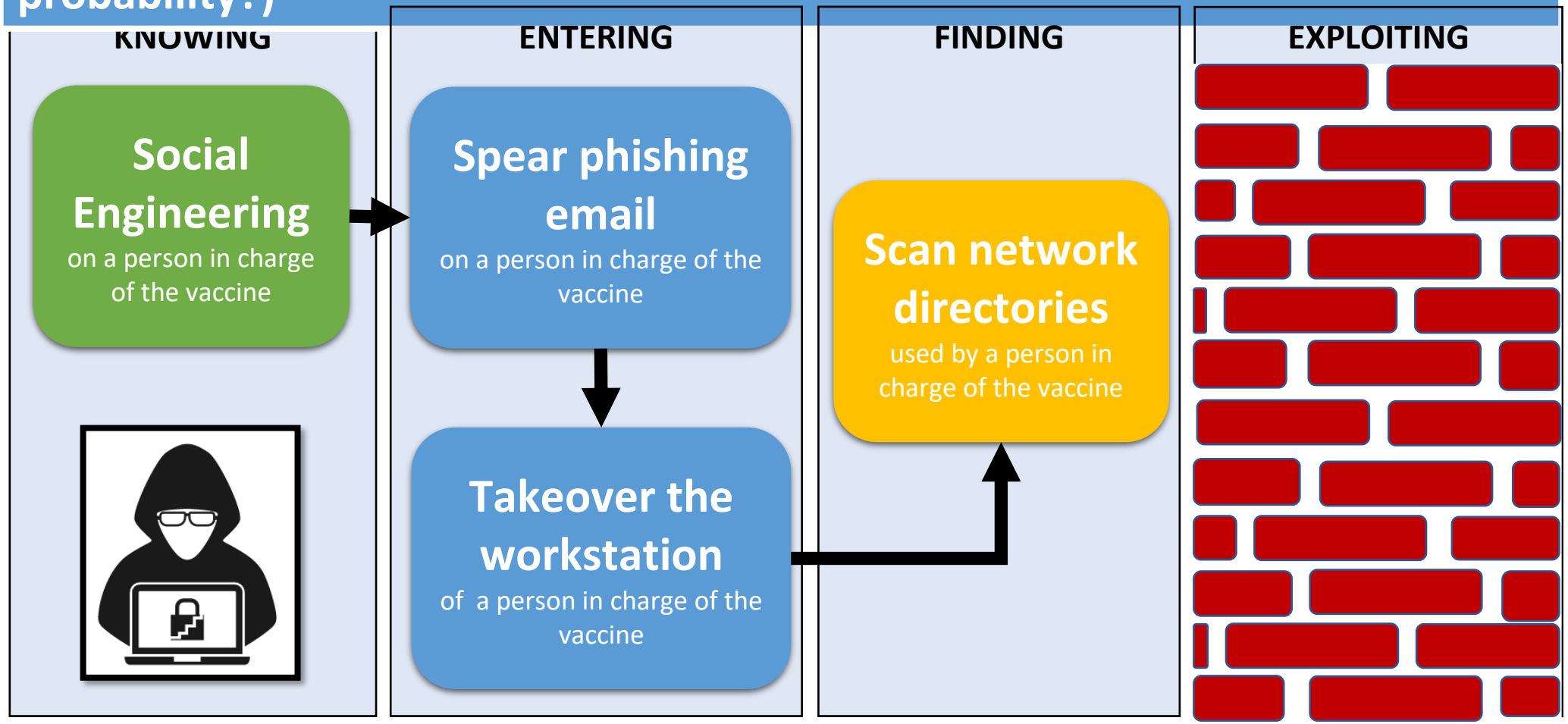
Cyber-attack in a COVID-19 context

Question 4 - the IMPACT
Do you believe that the mitigation measures (you selected or not) will have any impact to the patients' care?

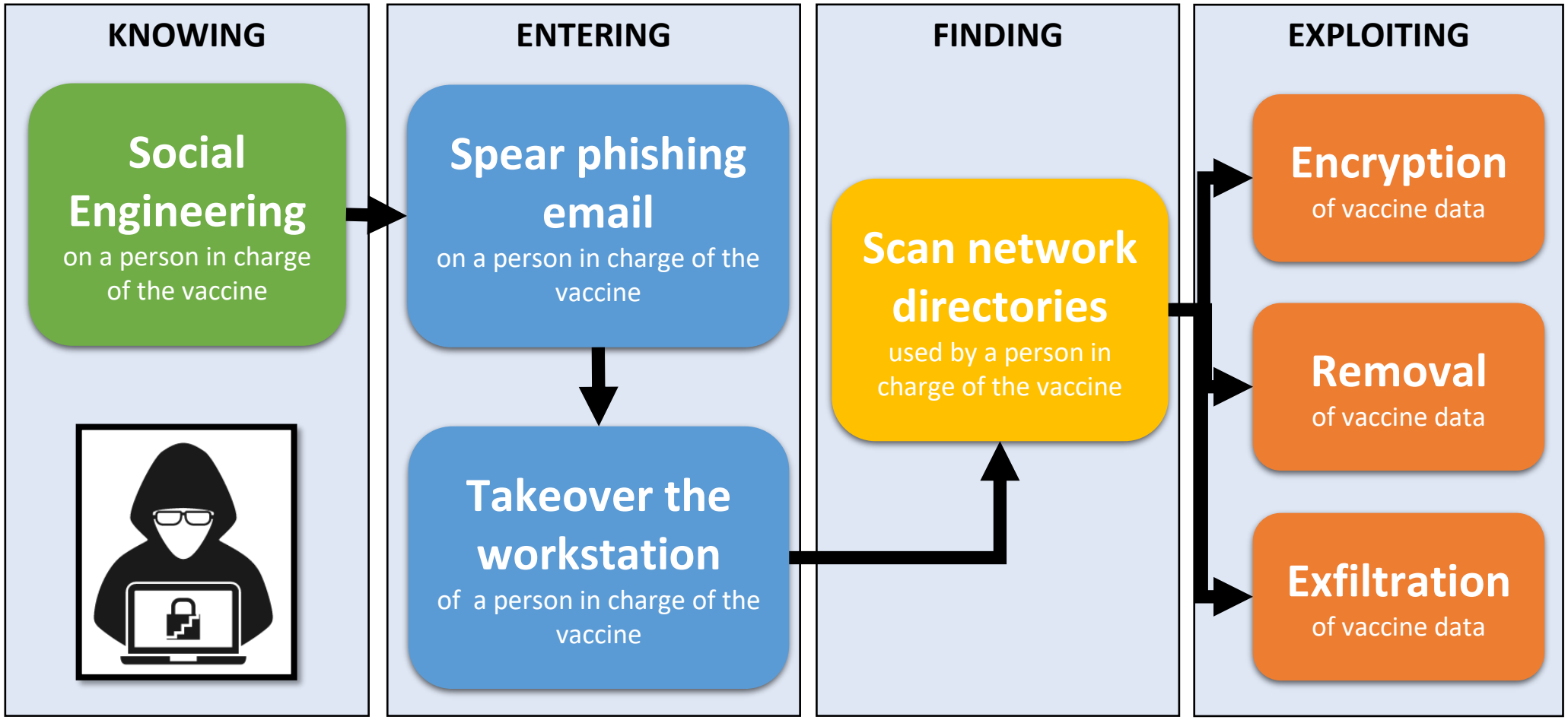


Cyber-attack in a COVID-19 context

Question 5 - the ESCALATION
What is the easiest way for the hacker to progress? (with what probability?)

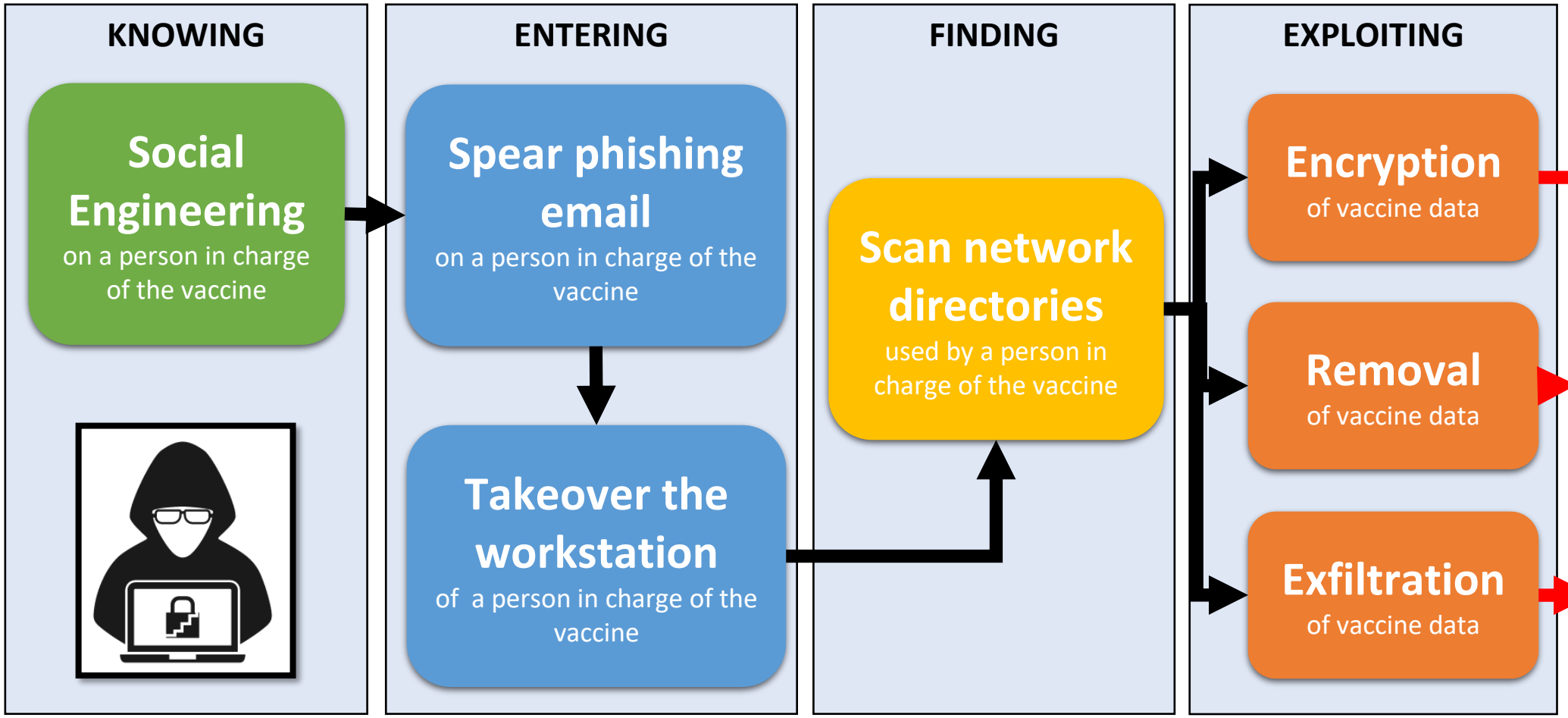


Cyber-attack in a COVID-19 context



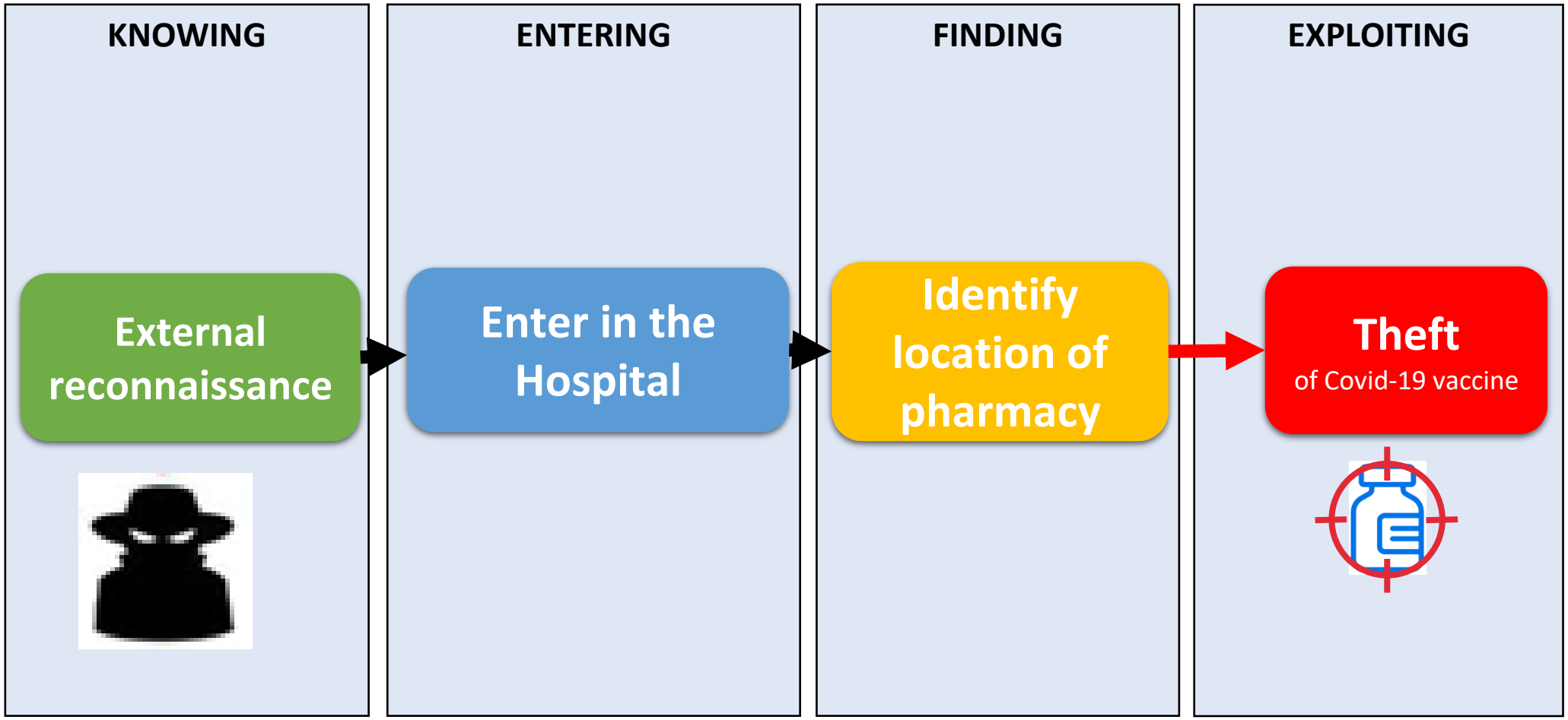
Cyber-attack in a COVID-19 context

Question 6 - CONCLUSION
What would you need the most to defend a hospital in this attack path?



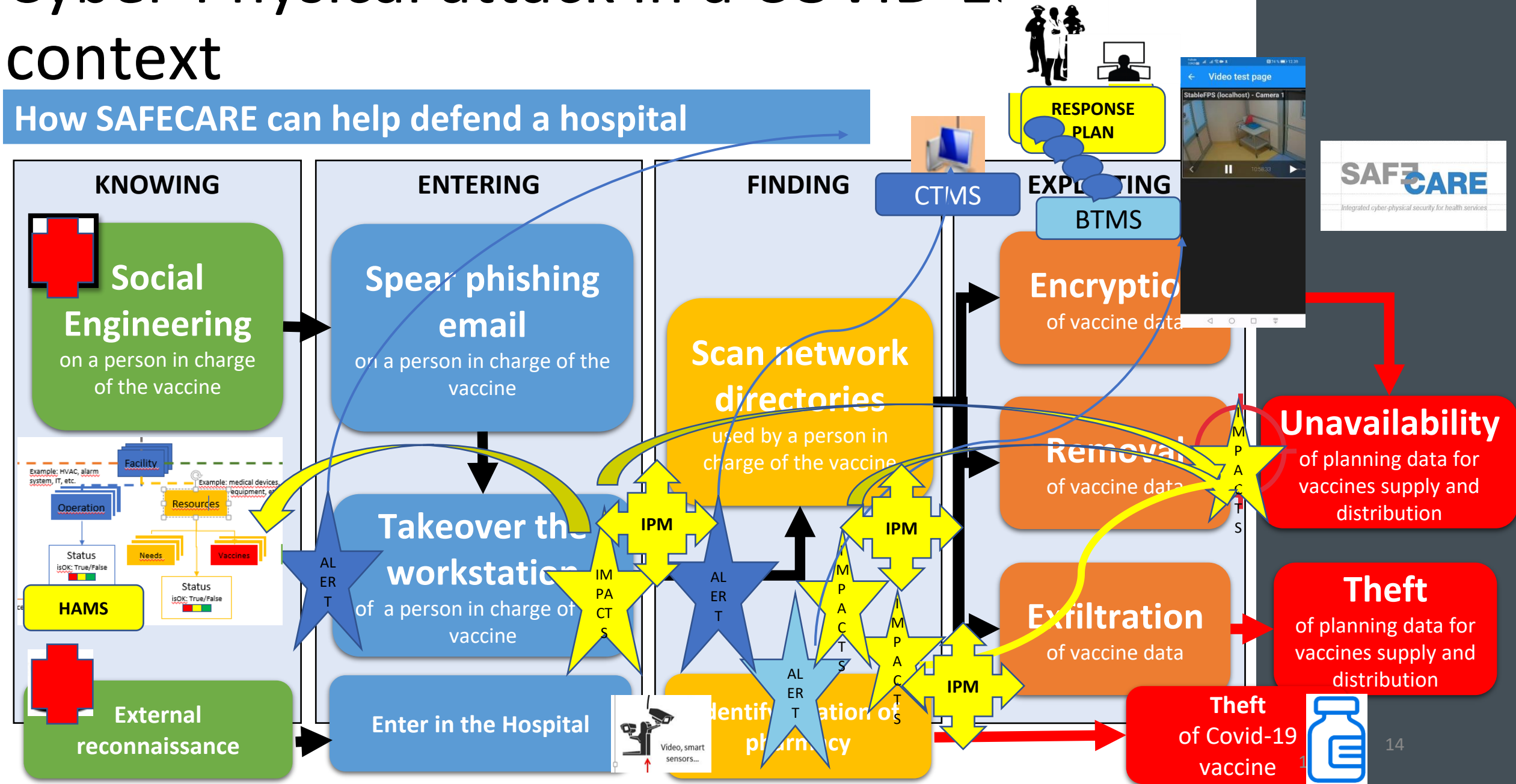
Physical-attack in a COVID-19 context

Other possibility of attack …



Cyber-Physical attack in a COVID-19 context

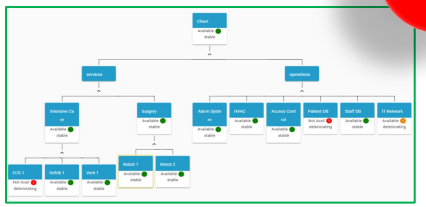
How SAFECARE can help defend a hospital

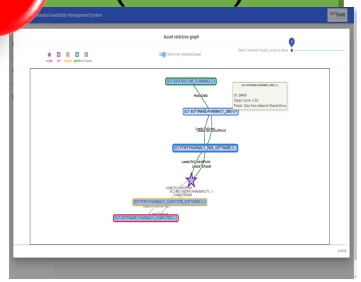


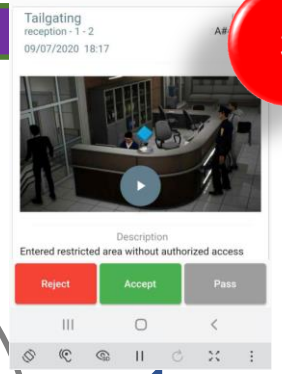
SAFECARE Four tools for End-Users

Global Supervision (HAMS)

4

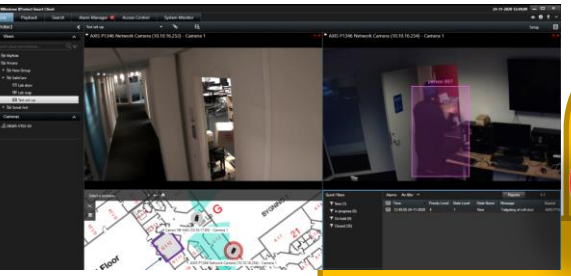






3

Alerting system (TRAS-MAS)

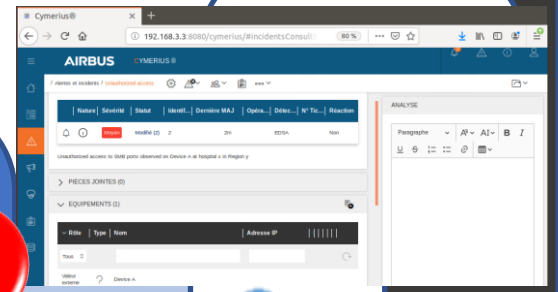


1

INCIDENTS

Cascading impacts calculation (IPM Ontology)

INCIDENTS



2

Physical security supervision (BTMS – MAS)

Cyber sécurity supervision (CTMS)

Access control

Video protection

Building monitoring system

Fire detection system

. . .

FW-IPS-IDS

SIEM

Threats detection systems

E-health AI

Hospital context

Hospital :
Real-time management
Quick communication

The work is as huge as the surface of health systems

- Detection of malicious behavior
- Emergency measures to limit the threat
- Prepare the repair
- Communicate (information about threat and mitigation) :
  - Between hospitals in a region
  - Between hospitals in a country
  - Between hospitals in Europe …

INCIDENT

High Impact

SAFECARE
Integrated cyber-physical security for health services

Paradox of health systems evolution:

- More open (towards patients, towards city medicine, etc.)
- More mobile inside and outside the hospital
- Simpler
- More secure (GDPR)

But…

- Low resources and complex ecosystems

Crisis mode :

- To be as agile as the threat
- To communicate between defensive actors (technical or human) at the speed of attacks to synchronize protection at the scale of a hospital, a territory of a country, a continent?

Needs…

- To understand possible impacts to manage appropriate decisions and…
- To organize preparation and training

Process to be prepared to manage risks and to integrate SAFECARE

1 - Critical system(s)

2 - Existing security systems and measures

3 - Organisational structure in place

4 - Crisis management process

RISK ASSESMENT TO UNDERSTAND RISKS AND POSSIBLE MITIGATION
What is detected during the kill chain ?

Technical but also managerial and organizational aspects

5 - Map crisis management actors with SAFECARE system's users

6 - New organisational crisis management (assessment of human impacts and ethics point of view)

7 - Specific knowledge to adapt the impact propagation calculation

8 – Understanding complete safecare tools and global process
Training future system by all End-users

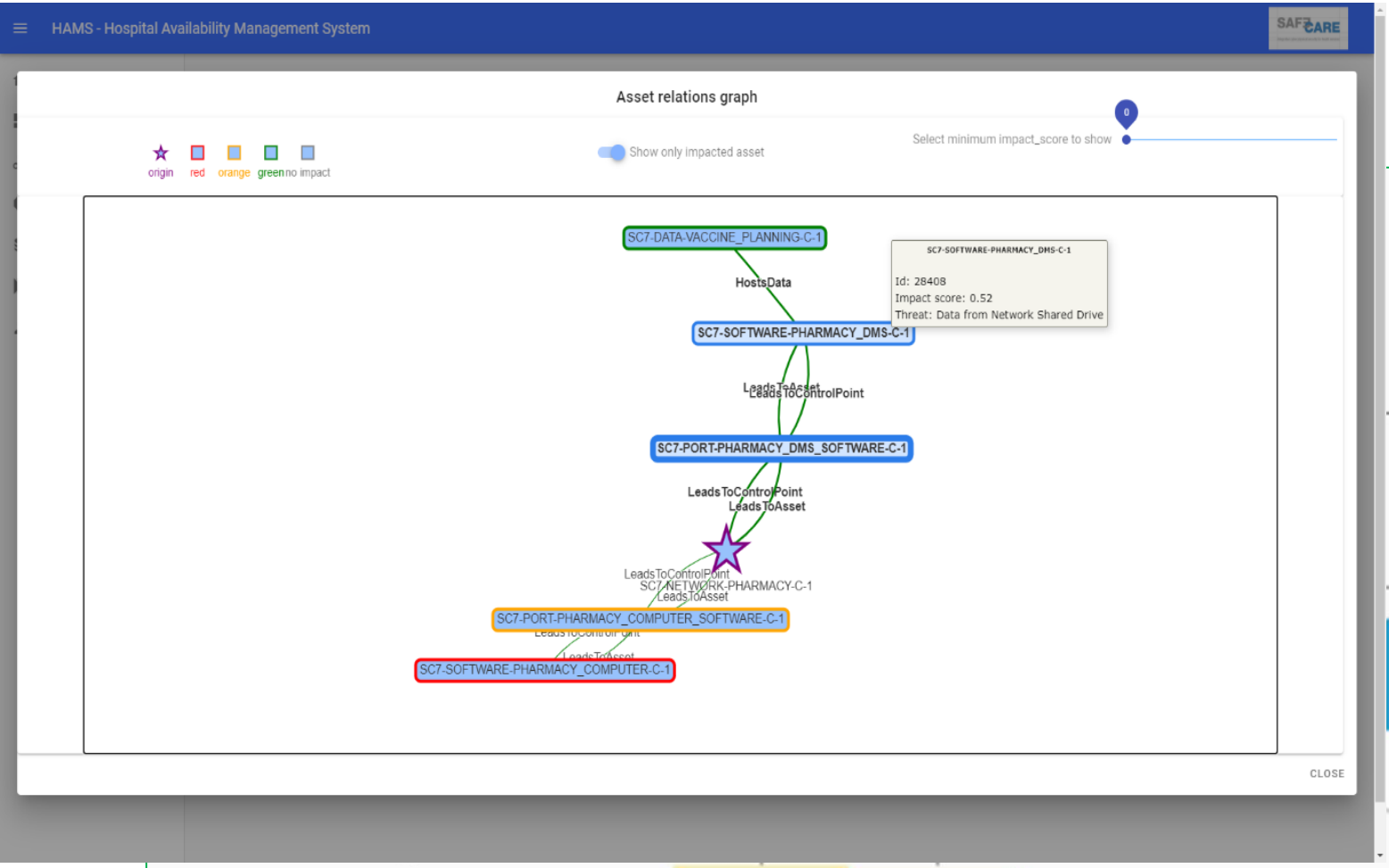
RISK SIMULATION (role play with Ebios RM/Bowtie methodology and Safecare tools), Training guide, training HAMS, …

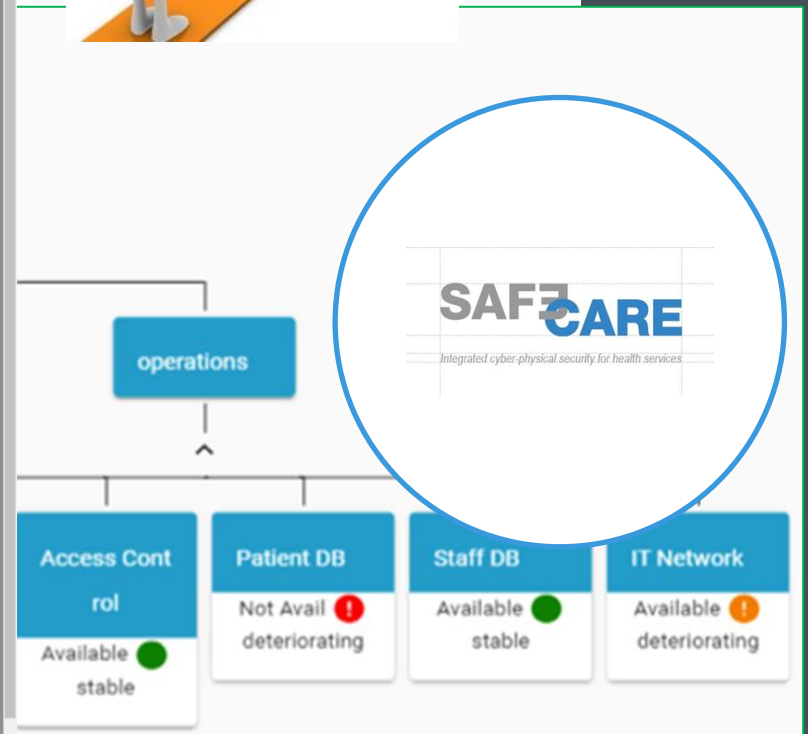
Scenarios : a representative sample of the complexity

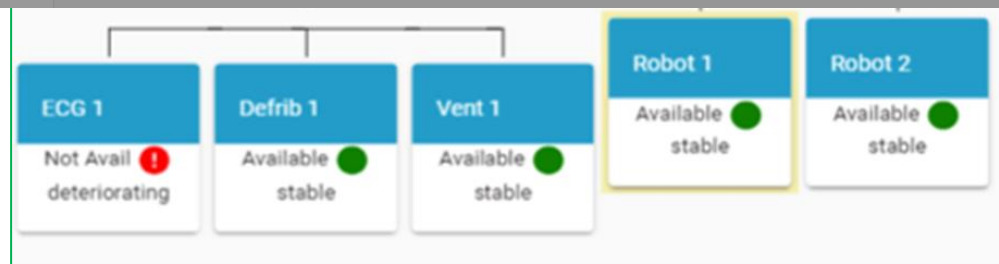
- Sc1: Cyber-physical attack targeting **power supply** of the hospital
- Sc2: Cyber-physical attack to steal **patient data** in the hospital
- Sc3: Cyber-physical attack targeting **IT systems**
- Sc4: Cyber-physical attack to cause a **hardware fault**
- Sc5: Cyber-physical attack targeting the **air-cooling system** of the hospital
- Sc6: Cyber-physical attack on **medical devices**
- Sc7: Cyber-physical attack to **steal credentials** to access IT systems
- Sc8: Cyber-Physical attack in access control provider to **steal medical devices**
- Sc9: Physical attack against hospital staff using a **gun**
- Sc10: Physical attack **to steal drugs**
- Sc11: Cyber-physical attack due to a **personal laptop**
- Sc12: Cyber-physical attack to **block national crisis management**

SAFECARE
Integrated cyber-physical security for health services

Scenarios : visualization of cascading impacts and risk assesment (HAMS)







SAFECARE Risk assesment Step by step

Operational scenarios Ebios RM

Description of Ebios RM attack paths (up to) workshop 4 (numbering of elementary actions and identification of detectable ones) : kill chains that can be used

- NEED TO IMPROVE DETECTION ?

Path of mitigation BowTie

- Describe the assets (with health repositories) corresponding to the support assets vulnerable to each elementary action of the different paths
- Highlight the measures that can counter or slow down these attacks (Miter Att & ck, ISO27002)
- Creation of a BowTie correlating threats, measures and consequences.

Asset description Tables of knowledge

- Describe asset context / links / protection measures

- NEED TO IMPROVE IMPACT PROPAGATION MODEL ?

Incident propagation Tables of knowledge

- Describe propagations : Source asset/threat/taget asset/existing protection

Ready to integrate Safecare tools

Examples of risk assessment tools

EBIOS RISK MANAGER

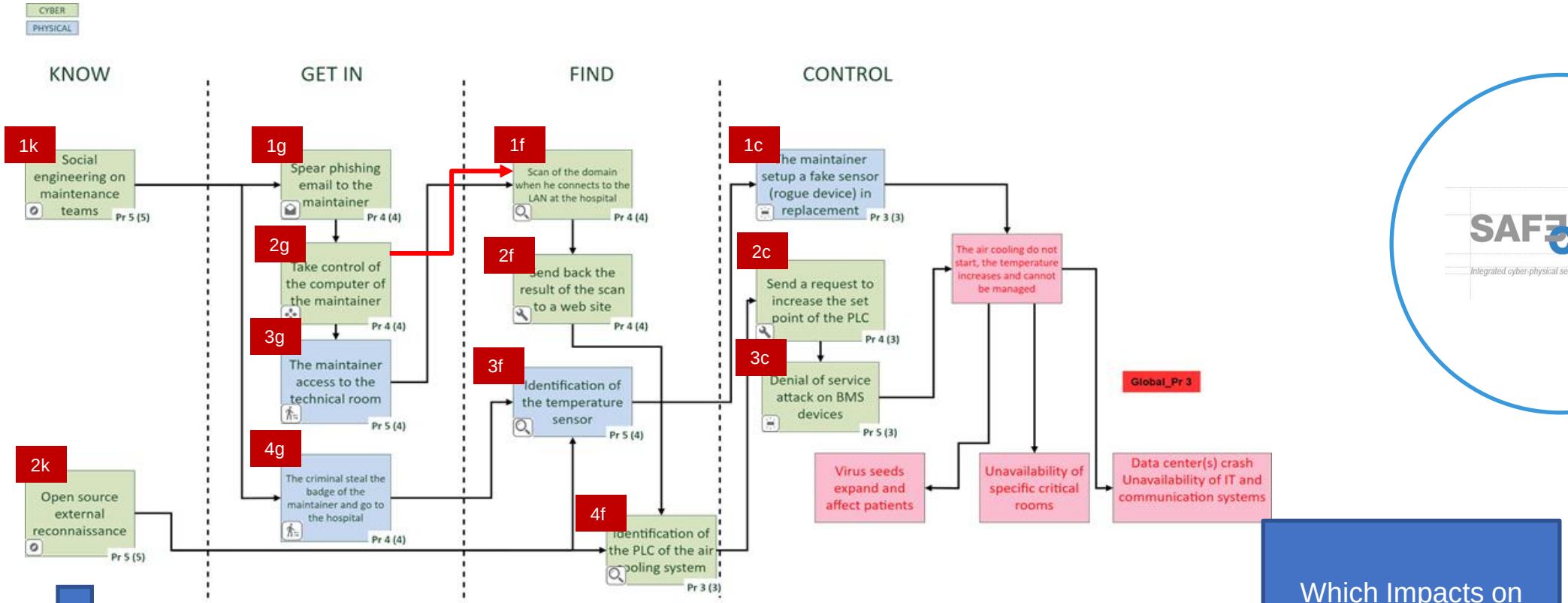
Tables of knoledge

BowTie

SAFECARE
Integrated cyber-physical security for health services

Risk assessment methodology

The risk assessment (Example with non representative data)



Which supporting assets ?

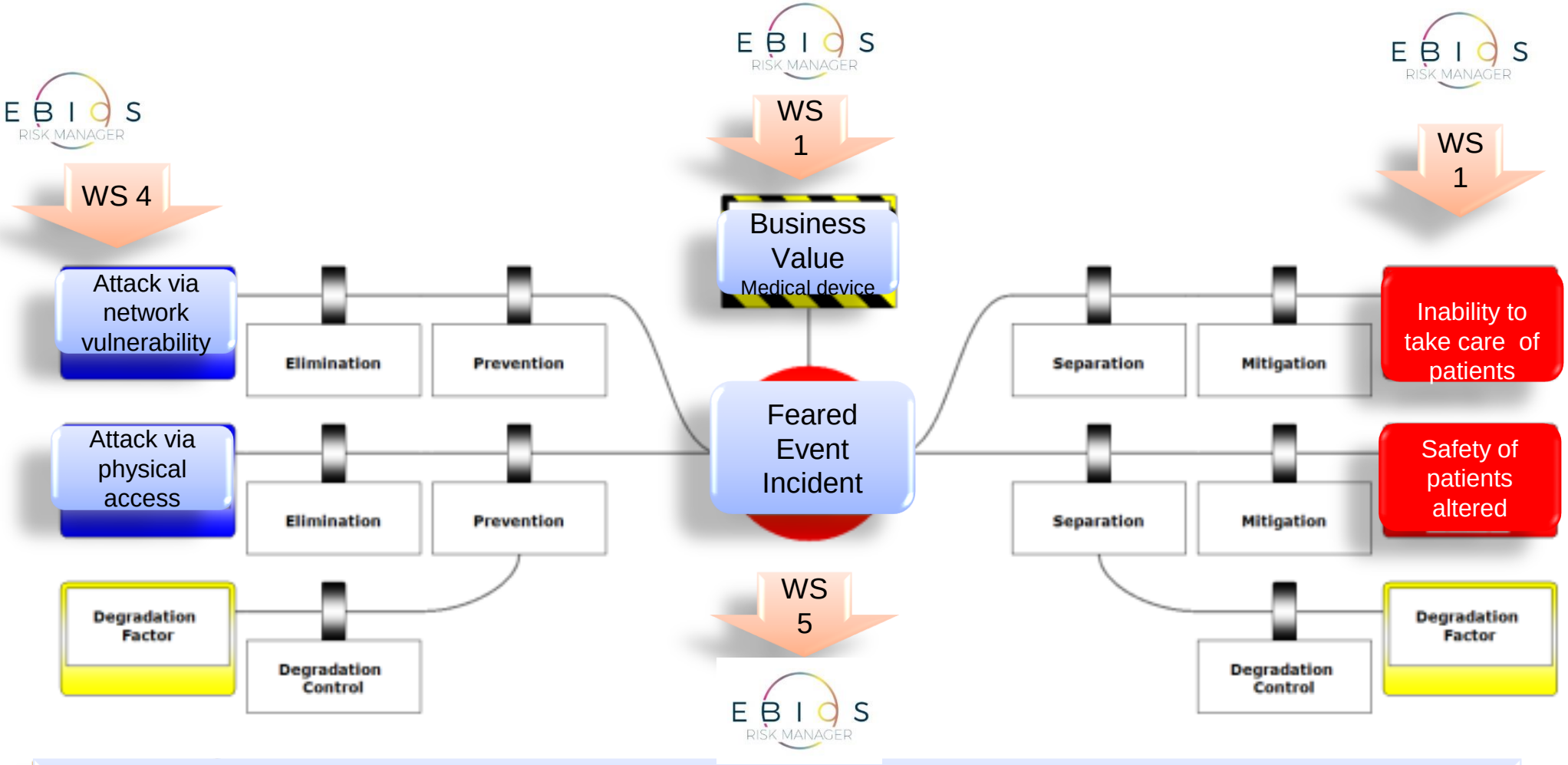
Which vulnérabilities ?

Which incidents ?

On which supporting assets ?

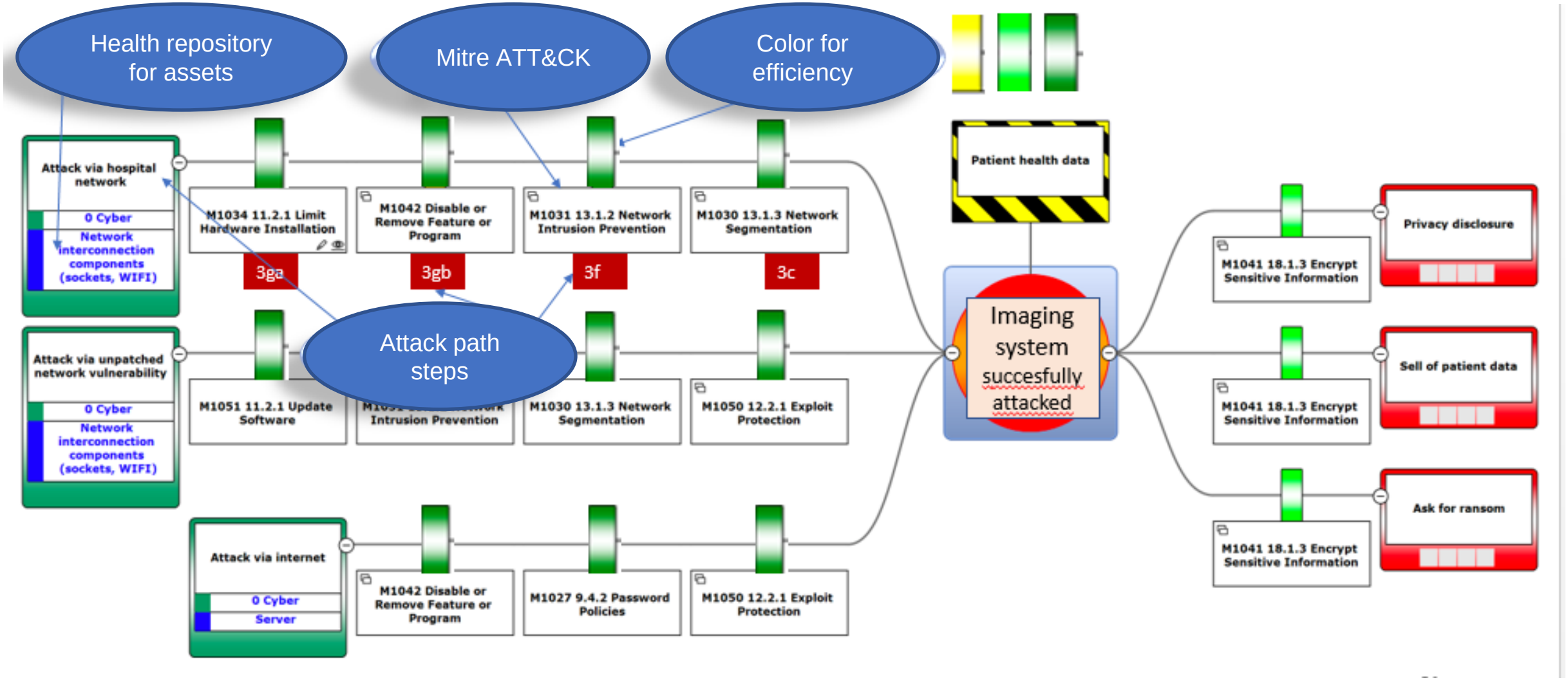
Which Impacts on which primary assets (critical/business values)

Risk Assessment - Ebios RM Combined with BowTie



To facilitate mesures and controls identification (existing and new ones) and links with degradation (or improvement) factors

Example with links to standards and repositories



Ontology based incidents propagation: Propagation rules and impact scores *(source Cnam paris)*

SAFECARE
Integrated cyber-physical security for health services

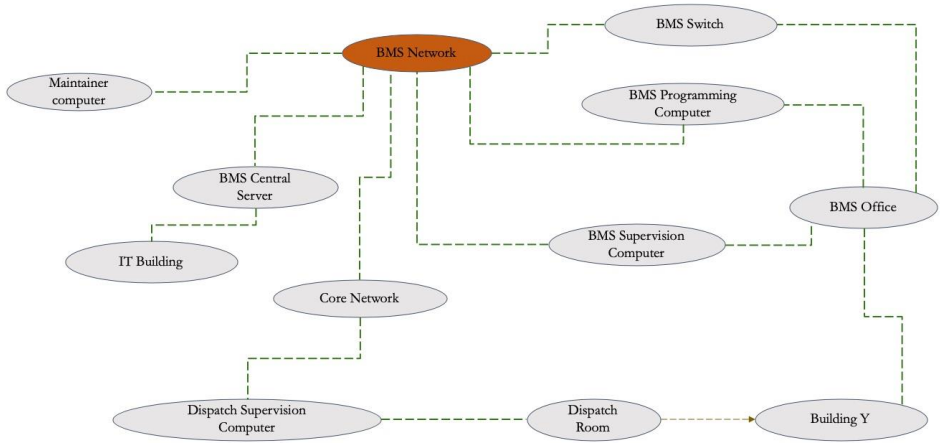
(1) Knowledge acquisition (tables of knowledge)

Asset	Asset category	Incident (on source)	Incident category	Link	Asset	Asset category	incident (on target)	Incident category
Maintainer computer	Device	threat on network	threat on network	leadsTo	BMS network	Network	trafic malveillant /anormal	trafic malveillant /anormal
Maintainer computer	Device	threat on network	threat on network	leadsTo	External access tool (VPN)	Controller	trafic malveillant /anormal	trafic malveillant /anormal
BMS network	Network	flux anormal / virus	Virus	leadsTo	PLC	Device	code malveillant	Virus
BMS network	Network	flux anormal / virus	Virus	leadsTo	PLC	Device	flux anormal / virus	Virus
BMS network	Network	flux anormal / virus	Virus	leadsTo	BMS supervision computer	Device	flux anormal / virus	Virus
BMS network	Network	flux anormal / virus	Virus	leadsTo	BMS central server	Device	flux anormal / virus	Virus
BMS network	Network	flux anormal / virus	Virus	leadsTo	BMS switch	Device	flux anormal / virus	Virus
BMS network	Network	flux anormal / virus	Virus	leadsTo	Core network	Network	flux anormal / virus	Virus

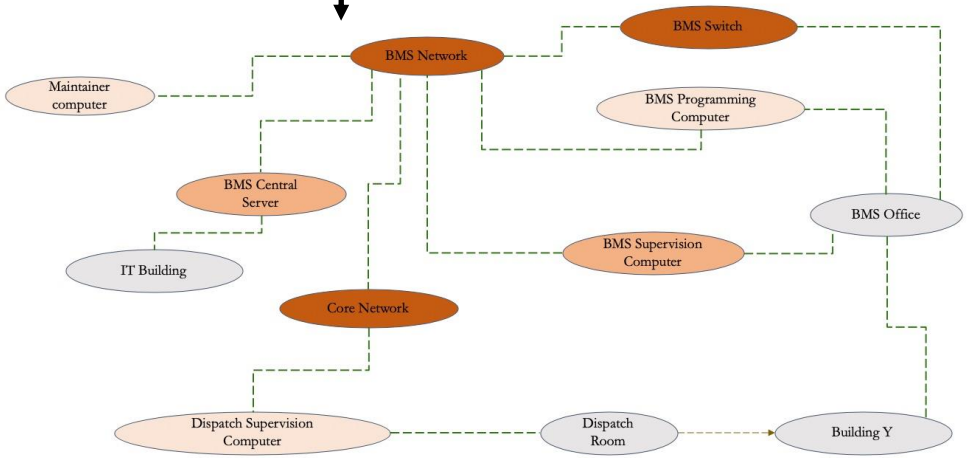
(2) Propagation rules generation

```
isImpacted(asset2), hasIncident(asset2, incident) :-
        hasIncident(asset1, incident), Network(asset1), Virus(incident),
        leadsToCP(asset1, controlPoint), leadsToAsset(controlPoint, asset2),
        Device(asset2)
```

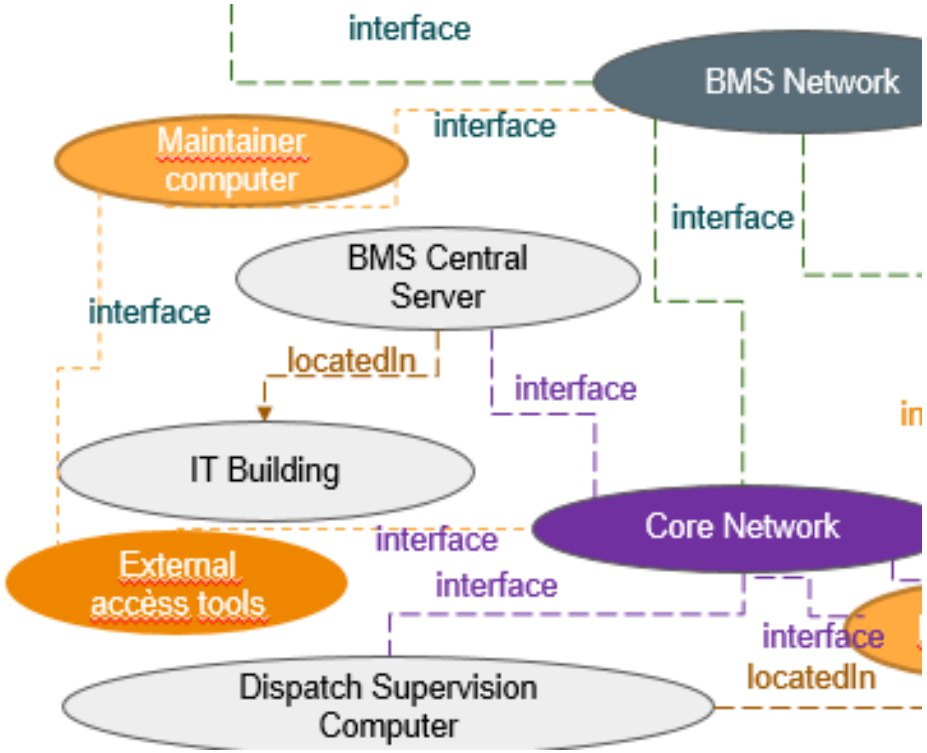
(3) Impact propagation



(4) Impact score evaluation



Assets map (from table of knowledge to map)



Bibliography

SAFECARE: https://www.safecare-project.eu

EBIOS Risk Manager: https://www.ssi.gouv.fr/entreprise/management-du-risque/la-methode-ebios-risk-manager/

Club EBIOS generic approach: https://club-ebios.org/site/ebios-lapproche-generique/

MITRE ATT&CK: https://attack.mitre.org/

ISO 27002: https://www.iso.org/obp/ui/#iso:std:iso-iec:27002:ed-2:v1:fr

BowTieXp: https://www.cgerisk.com/products/bowtiexp/

Thank you for your involvement !

More details available on:

- Our website: https://www.safecare-project.eu/
- Twitter: @SafecareP
- -LinkedIn: SAFECARE Project

Philippe.tourron@ap-hm.fr