Panacea

People-centric cybersecurity in healthcare

Dynamic Risk Management Platform

Resilient Response Engine

Martina Bossini Baroggi
RINA-C

2nd End User Workshop

15 September 2020

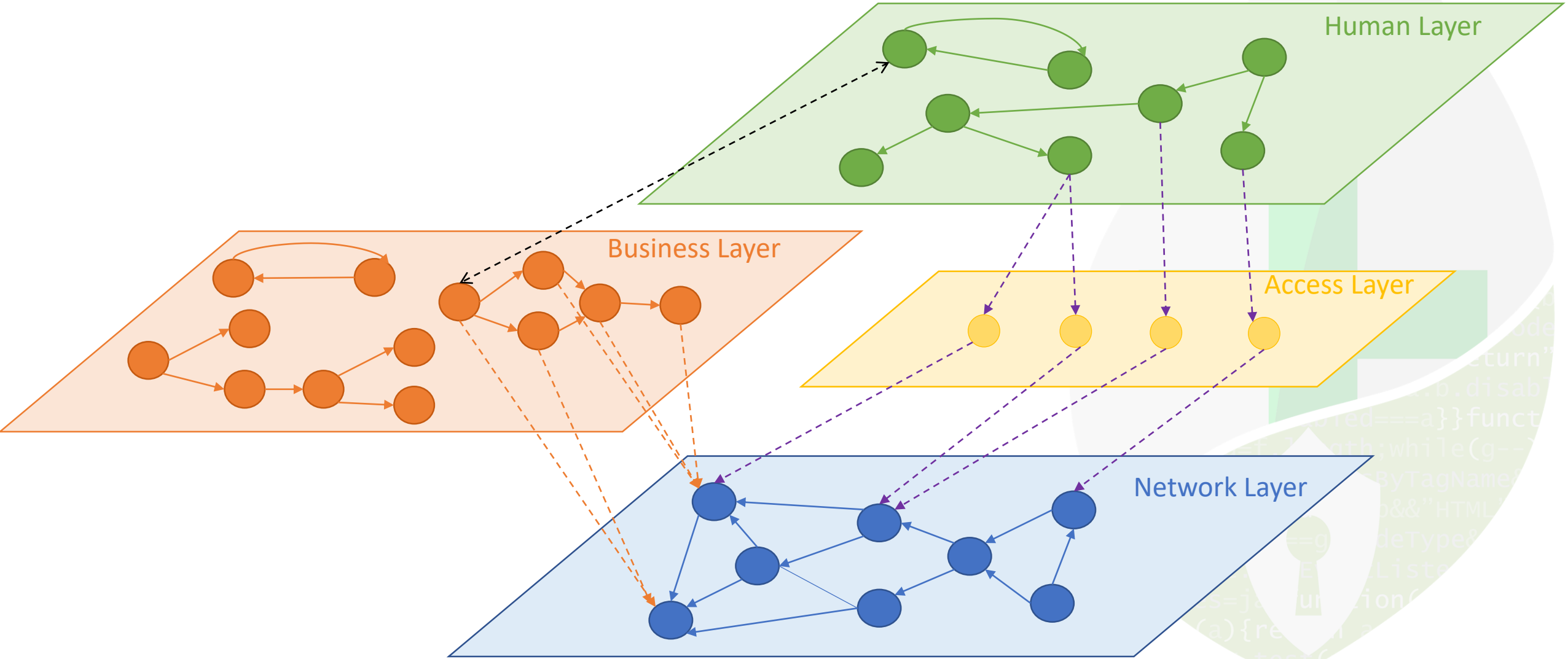
Funded by the European Union's Horizon 2020
Research and Innovation Programme, under Grant Agreement no 826293

Resilient Response Engine

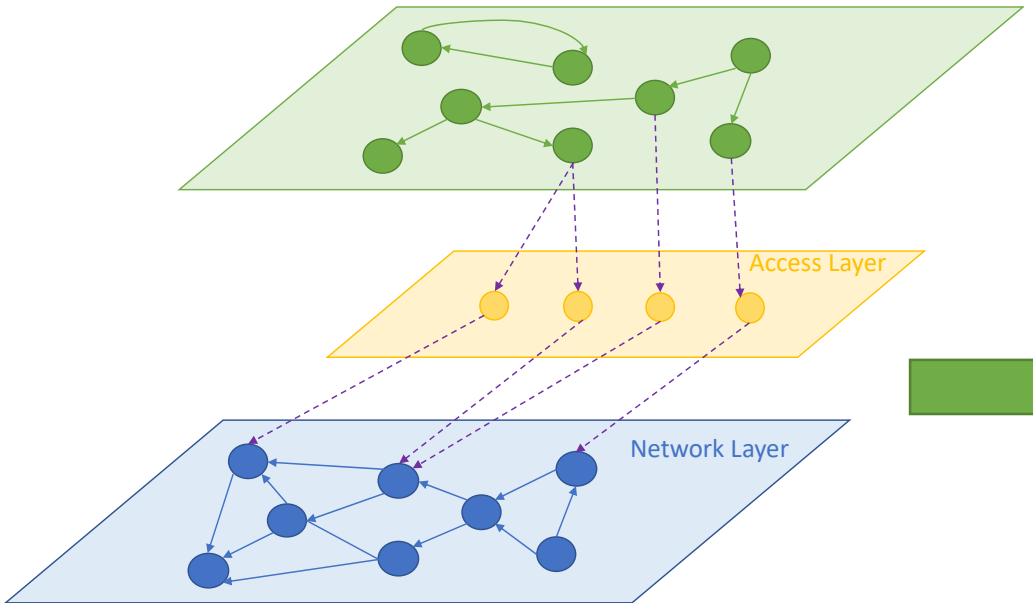
- **Main Objective**: proposing a list of actions to mitigate risks, derived from a pre-configured list of approved technical and non-technical mitigation actions.

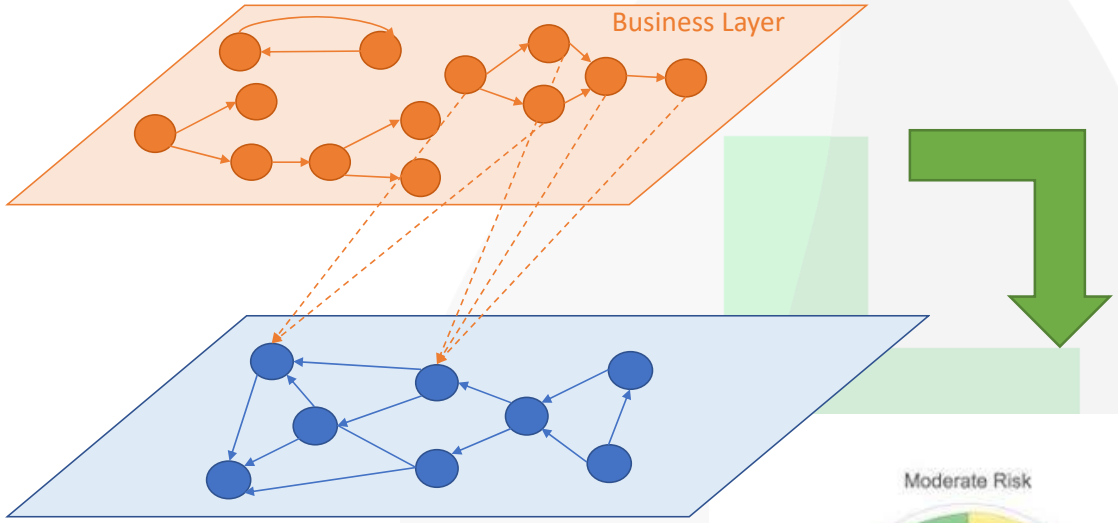
- **Basic Algorithmic Idea**: optimization problem having the objective function of minimizing the risk of attack paths by selecting remediation actions (both technical and non-technical) with the lowest overall cost (considering both direct and indirect costs).

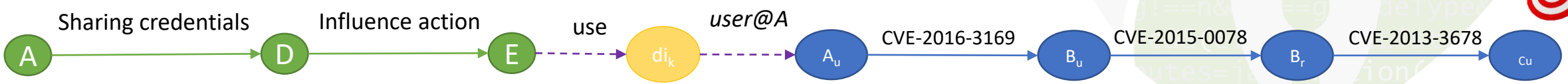
Let's recall our model…



Traversing Human, Access and Network Layer



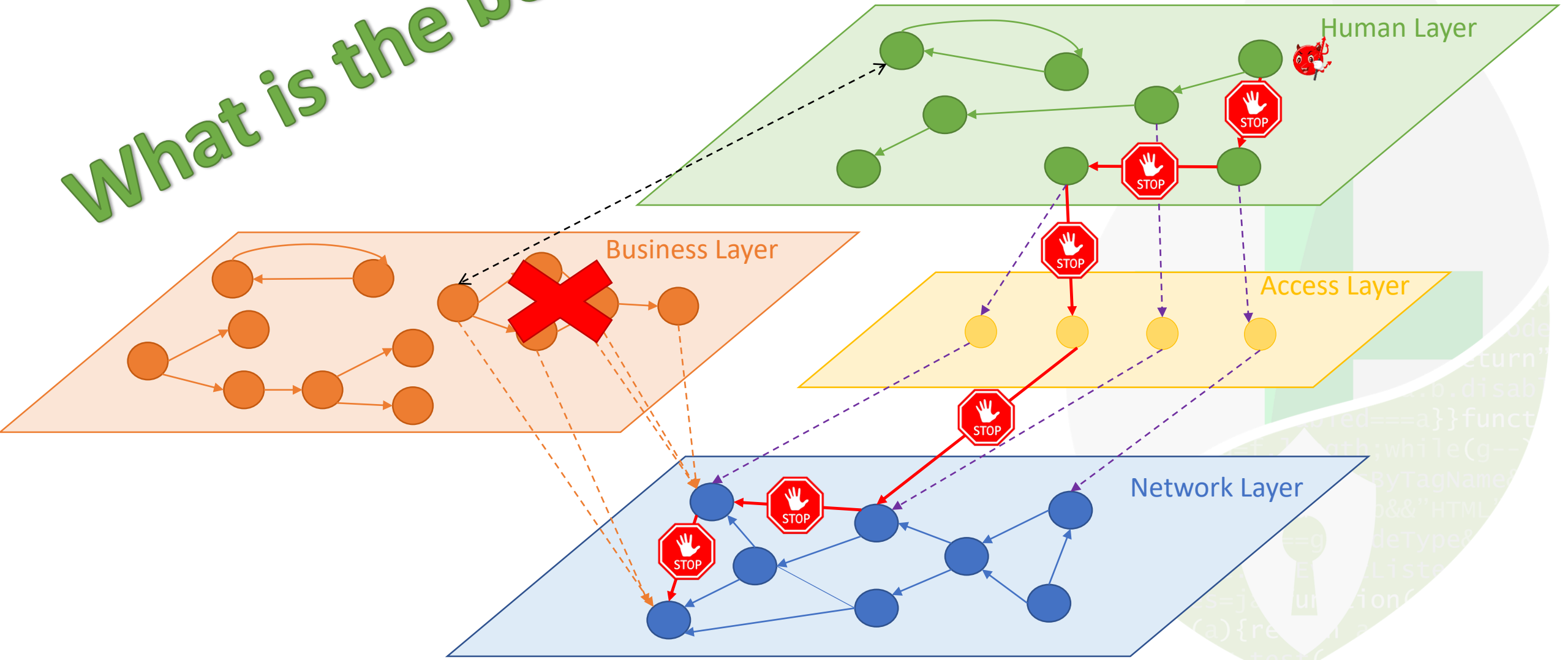




Panacea
People-centric cybersecurity in healthcare

Problem Formulation

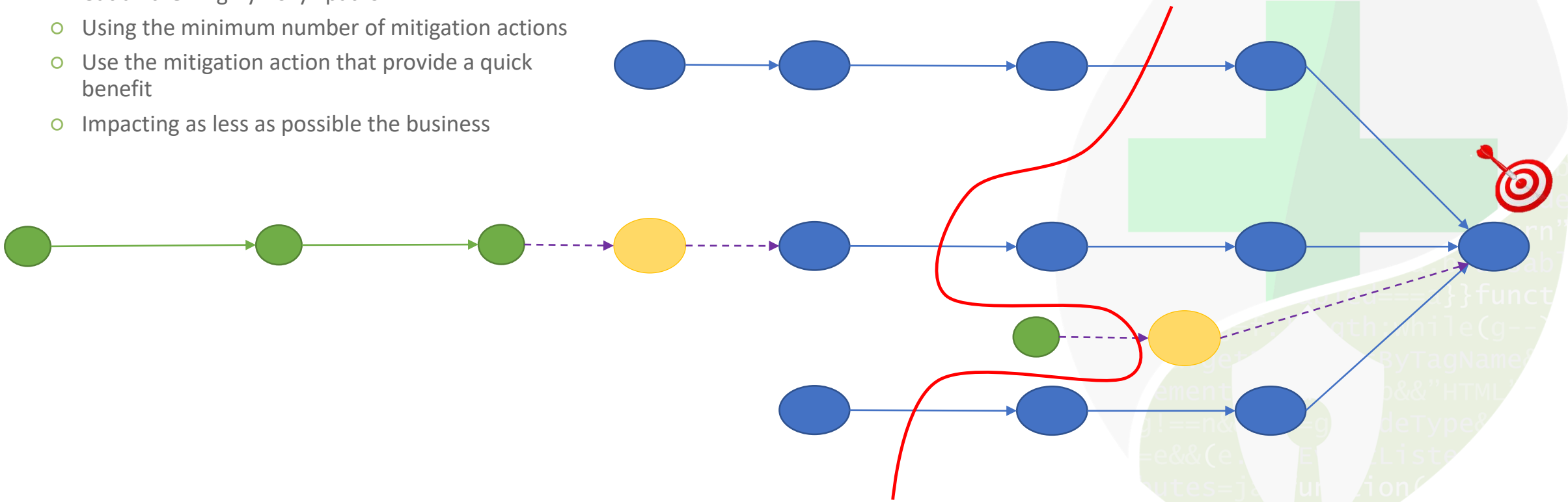
What is the best?



Panacea
People-centric cybersecurity in healthcare

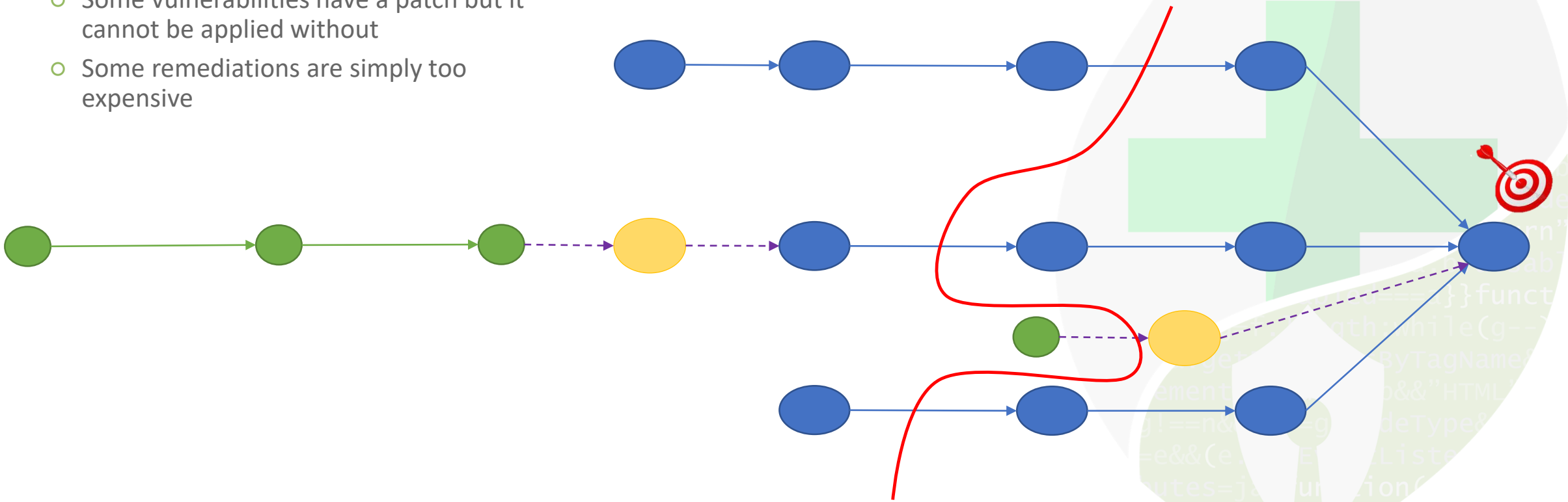
Intuition of the Problem Formulation

- In order to maximize the risk reduction, we should
  - Cut all the ”highly risky” paths
  - Using the minimum number of mitigation actions
  - Use the mitigation action that provide a quick benefit
  - Impacting as less as possible the business



Issues

- However…
  - Some vulnerabilities have not patch
  - Some vulnerabilities have a patch but it cannot be applied without
  - Some remediations are simply too expensive



RRE Input

- Human, Access and Network Layer Attack Graph Representation,
- Vulnerability catalogue ,
- list of start nodes,
- list of target nodes,
- pre-configured list of mitigation actions,
- information about budget for mitigations actions.

Output – Mitigation Actions

- The list of mitigation actions to be adopted:
  - First choice: the best combination of mitigation actions taking into account budget
  - From the second choice: the mitigation actions combinations ordered according to the risk reduction
- The effectiveness value of these mitigation actions,
- The nodes of the relative path in the attack graph.