|  |
| --- |
| ***UMIL*** |
| **STRENGTHS (+)** | **WEAKNESSES (-)** |
| * Provide hands-on cybersecurity training activities tailored on real pilot environments
* Modeling of training activities using CRSA models, interoperability among different pilots, easy customization, reuse of specific CRSA submodels in different training programmes
* Modeling of the real Pilots’ cybersystems allows automatic adaptation of training programmes to new training requirements
 | * Complexity of CRSA models, that should be prepared after a deep analysis of pilots’ systems
* Configuration of the whole environments and interoperability of different tools
* Complexity in the definition of specific training environments that can target different level of users (common employee, ICT staff, healthcare managers, …)
* Privacy risk due to healthcare data processing, that could reduce platform potentialities
 |
| **OPPORTUNITIES (+)** | **THREATS (-)** |
| * High demand in cyber range tool for cybersecurity training, that poses AERAS platform in an advantage point due to its model-based approach
* Exchange of training scenario among different cyber range platforms that share a common training programme metamodel
* Tailored on healthcare pilots, allowing to have a major awareness on privacy and security issues of this context
 | * Difficulties in the definition of complete and strong CRST programmes
* Technical requirements can be higher in what expected, causing a critical reduction of working performances
 |