Security of Airport Transport Infrastructure in Europe

A new toolkit to boost airport security

Kelly Burke (NIS) June 25, 2020

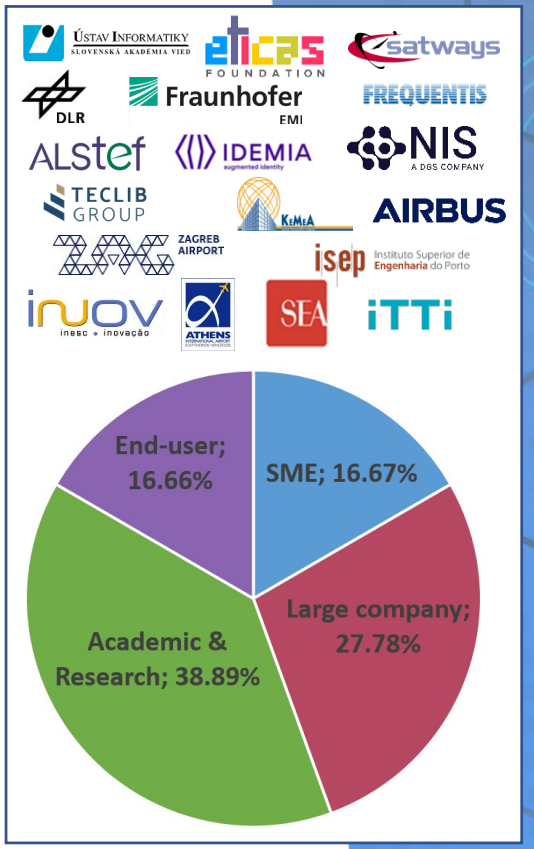
This project has received funding from the European Union's Horizon 2020 research and innovation programme under grant agreement number 832969.

1. Basic project information
2. Bringing the theory into practice
3. Challenges and issues

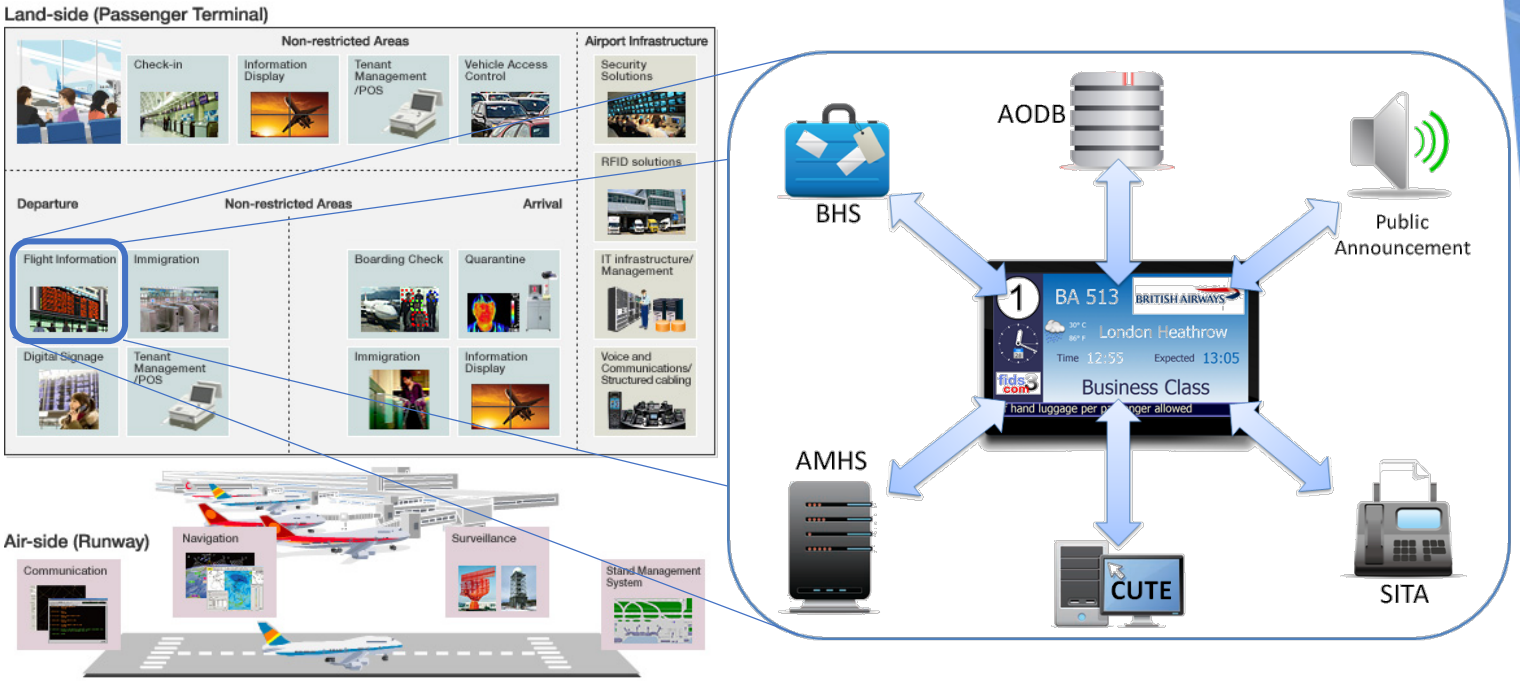
1. Basic project information

Project setup

18 partners, 10 nations
Total Costs: €9,890,595
Funding: €7,989,264
PM planned: 1058
Duration: 24 months
3 airport end-users★



Motivation 1/2



Motivation 2/2

[1]ACI Europe research 2015
[2]PwC survey 2015
[3]HP/Ponemon research 2014
[4]UK BIS 2015 survey

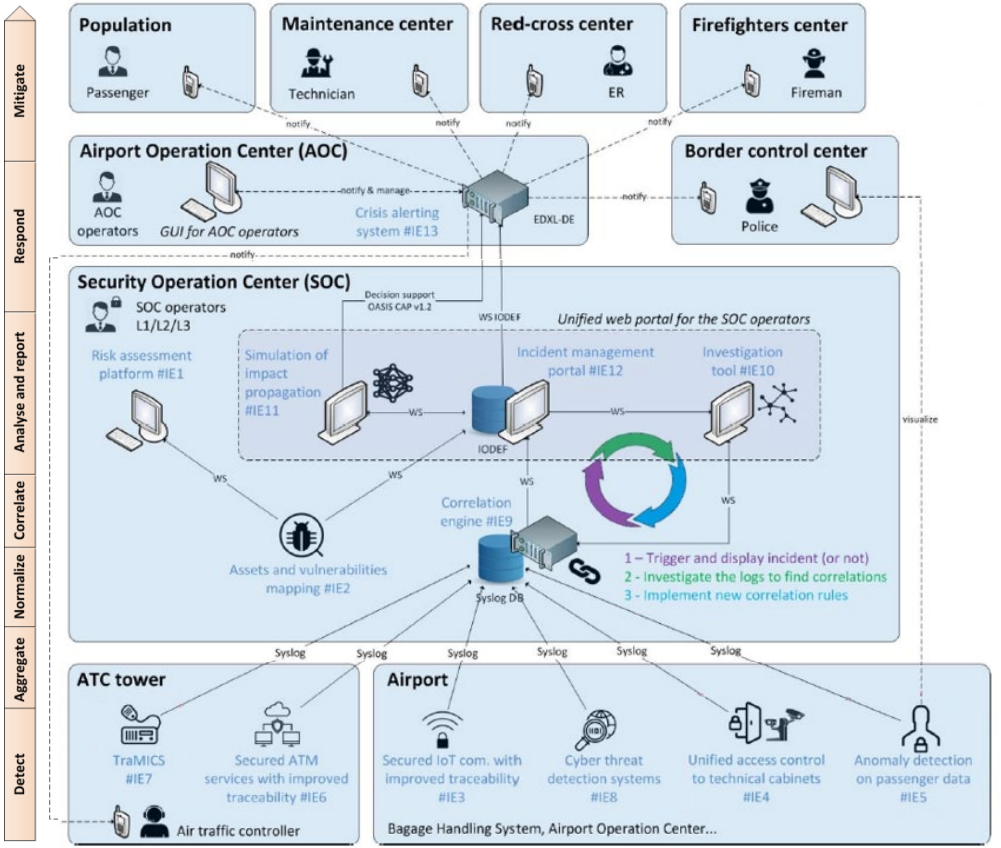
Costs of cyber-security breaches are high:

- €1M/hour for a disruption at a major European airport[1].
- €2M+ direct cost of a serious cyber-compromise[2].
- €250M in losses of European airport revenue for a six-day closure (estimate following Eyjafjallajokull eruption 2010[1]).

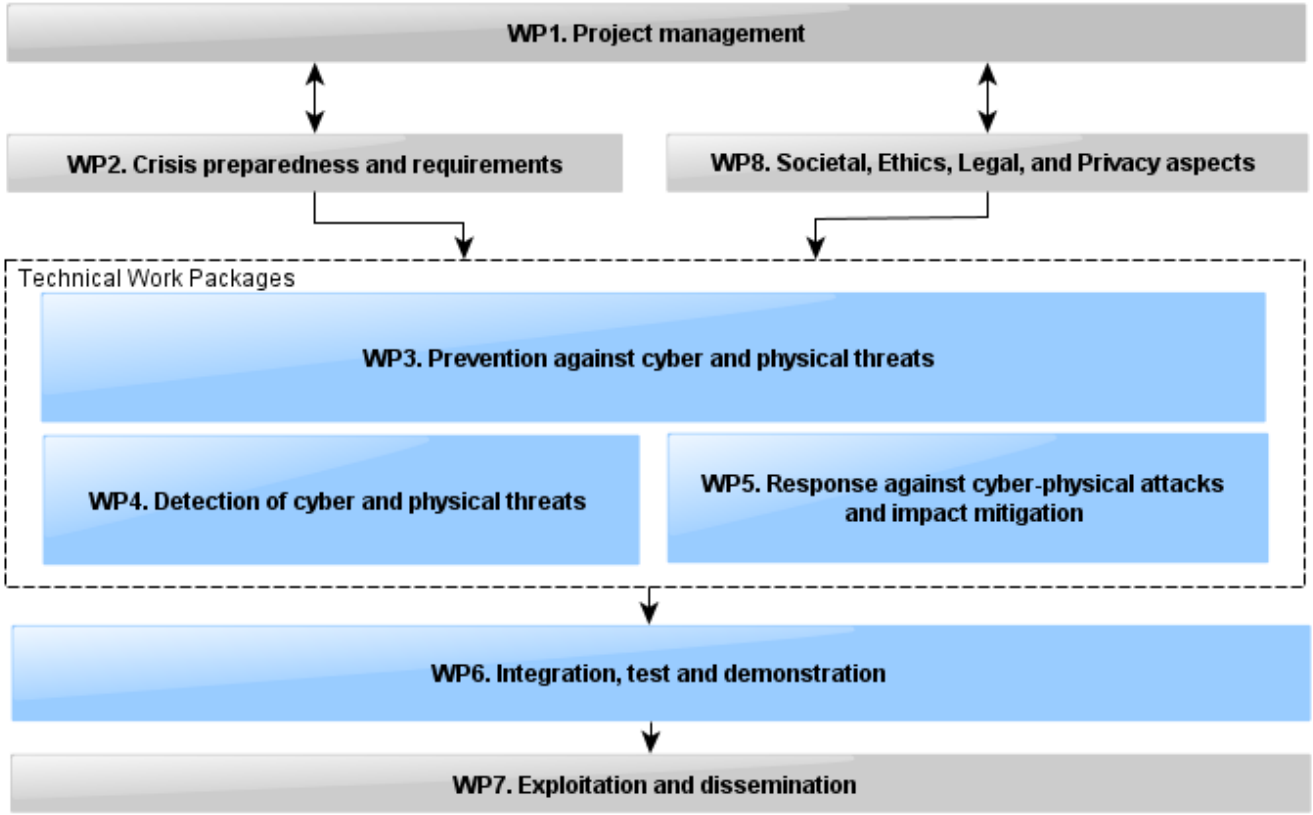
It's important to take cyber-security seriously, especially as:

- 170 days = average time to detect a malicious or criminal attack[3].
- 90% of large organisations reported suffering a security breach[4].
- 75% of board directors are not involved in review of cyber-security risks[2].

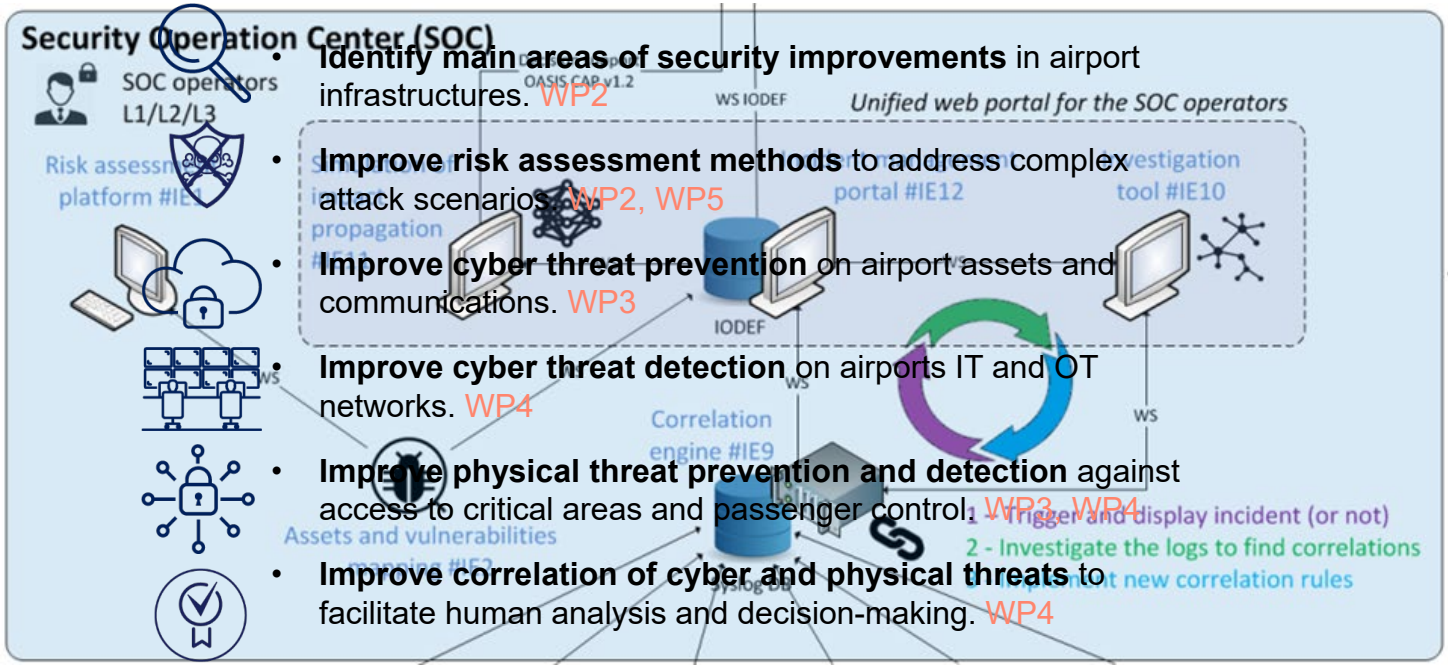
Project Goal



Project structure

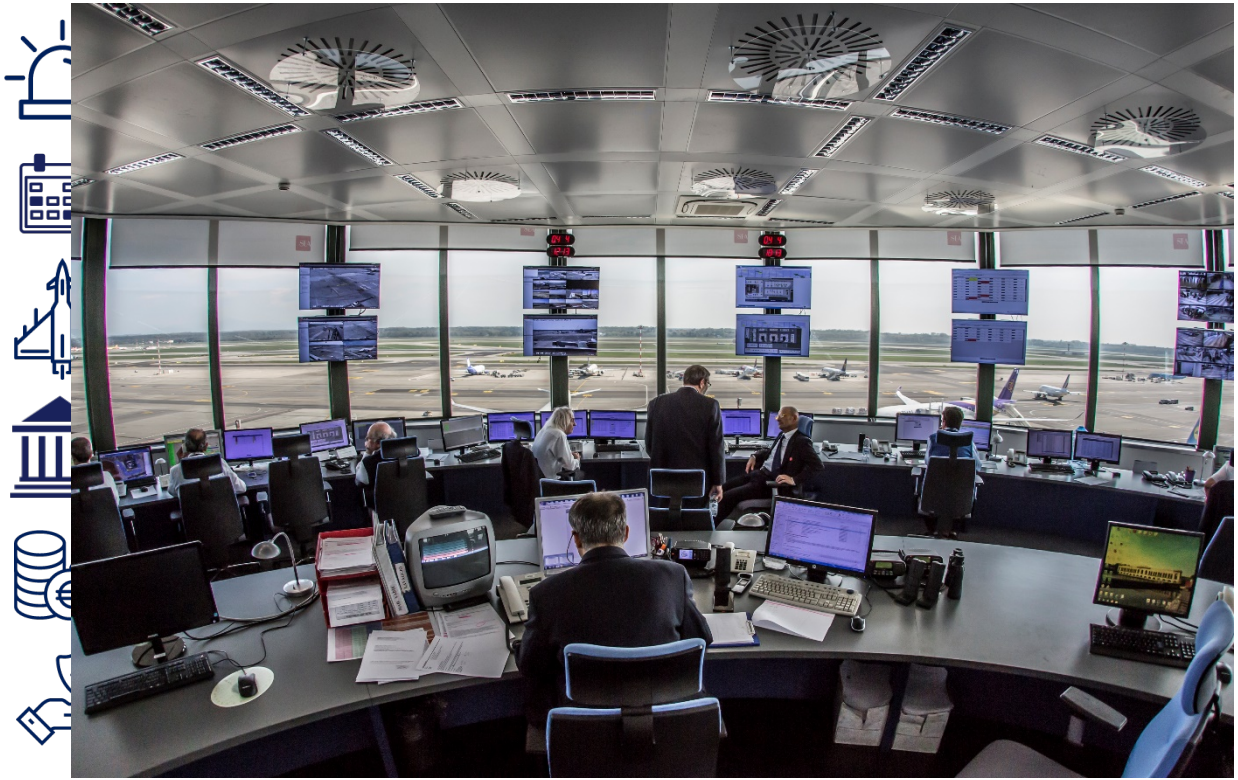


Objectives of SATIE - Part 1



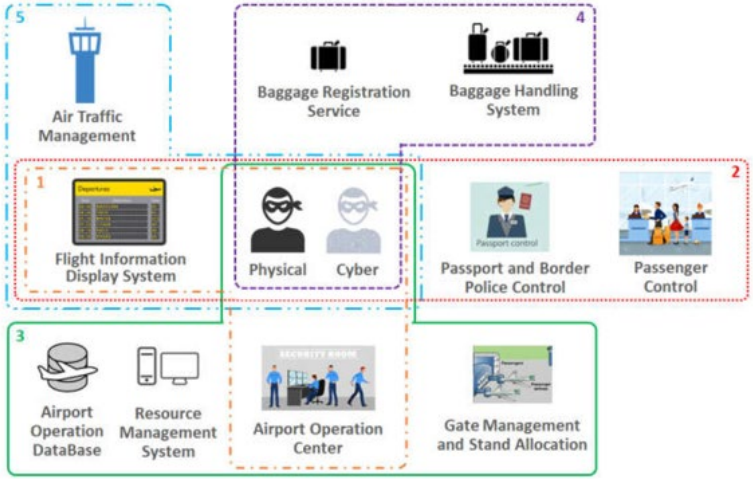
- **Identify main areas of security improvements** in airport infrastructures. WP2
- **Improve risk assessment methods** to address complex attack scenarios. WP2, WP5
- **Improve cyber threat prevention** on airport assets and communications. WP3
- **Improve cyber threat detection** on airports IT and OT networks. WP4
- **Improve physical threat prevention and detection** against access to critical areas and passenger control. WP3, WP4
- **Improve correlation of cyber and physical threats** to facilitate human analysis and decision-making. WP4

Objectives of SATIE – Part 2



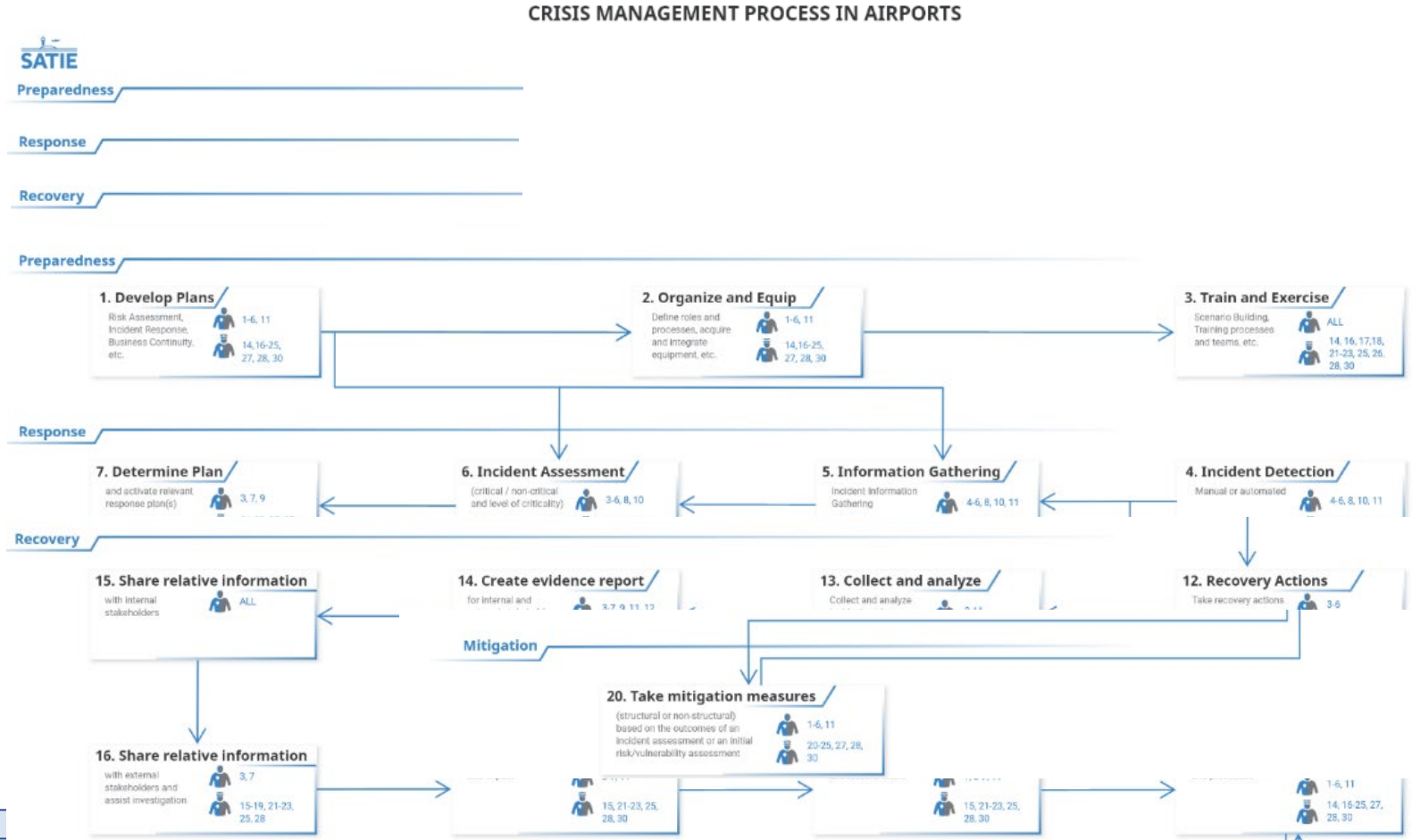
2. Bringing the theory into practice

Scenarios for simulation and demonstrations

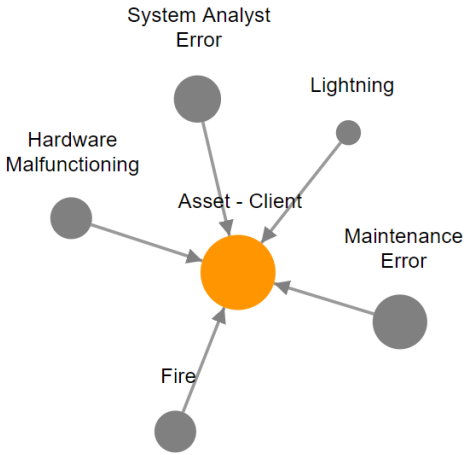


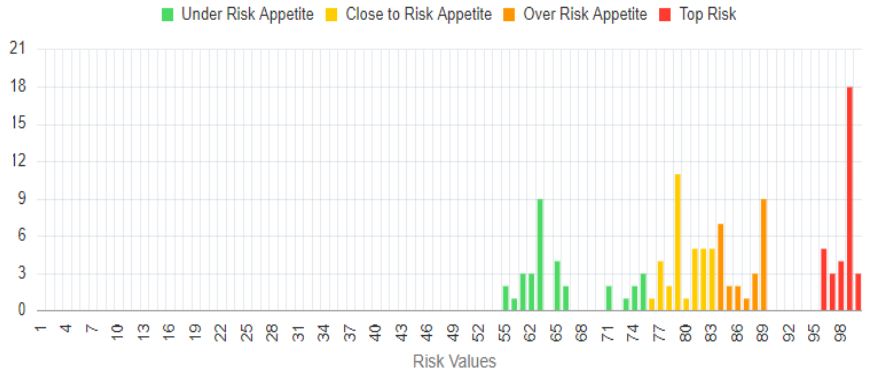
Scenario	Description
Scenario 1	Cyber-physical attack targeting passengers' security (Athens airport)
Scenario 2	Disturbance of the passenger controls (Athens airport)
Scenario 3	Compromising of the Airport Operations Database (Milan airport)
Scenario 4	Disorganization of Baggage Handling Services (Zagreb airport)
Scenario 5	Endangered Air Traffic Management (simulation airport)

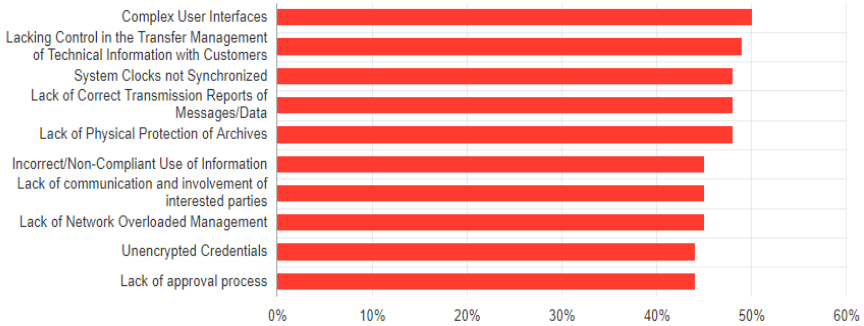
✓As-is analysis of the airports and harmonization of security procedures



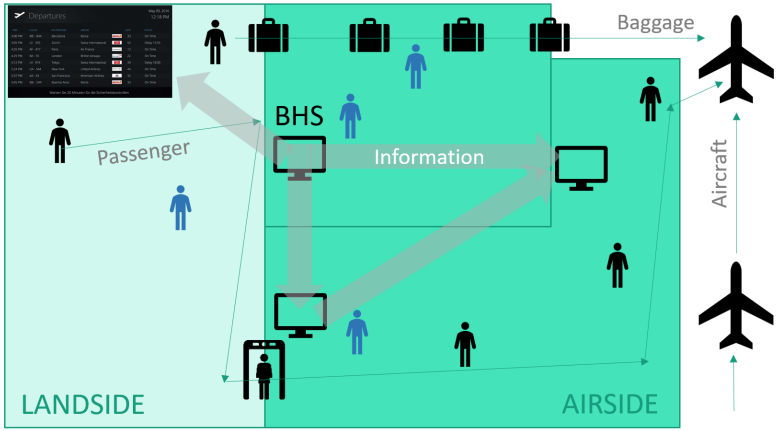
Risk assessment performed for the airports of each scenario

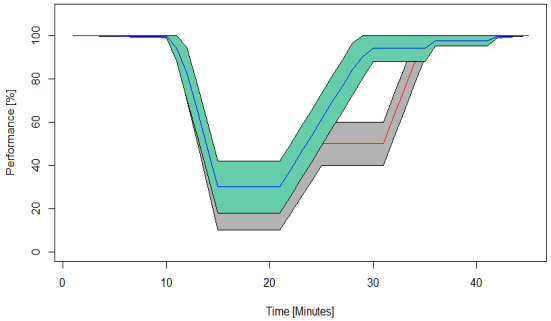


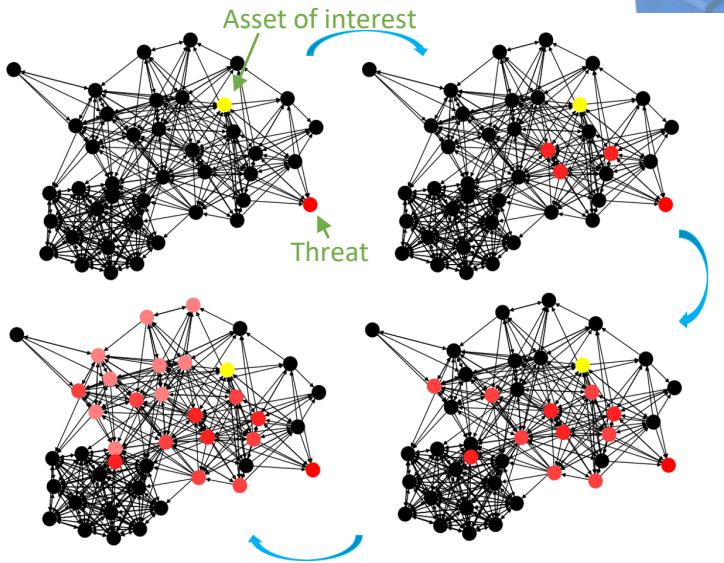




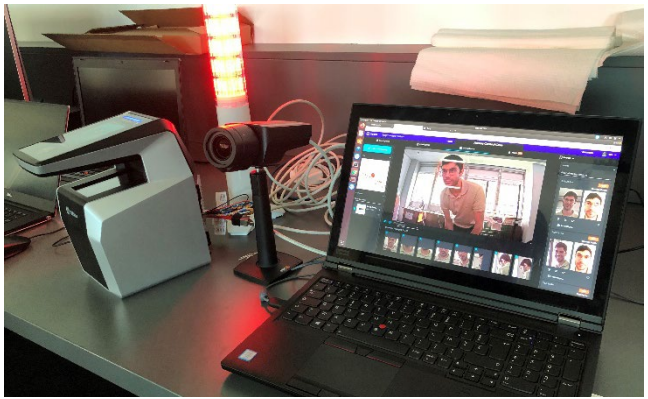
Threat propagation model created for each scenario

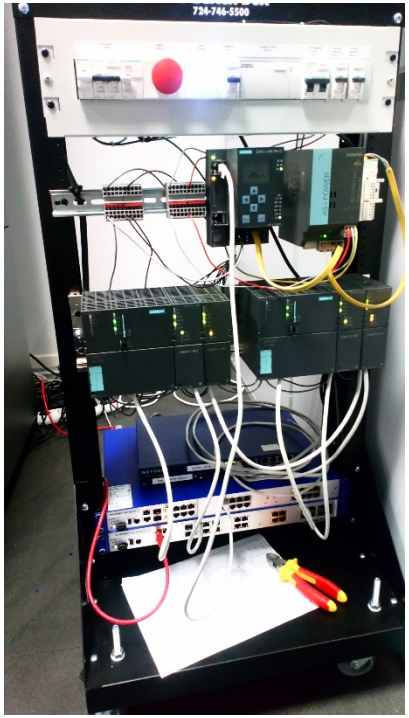




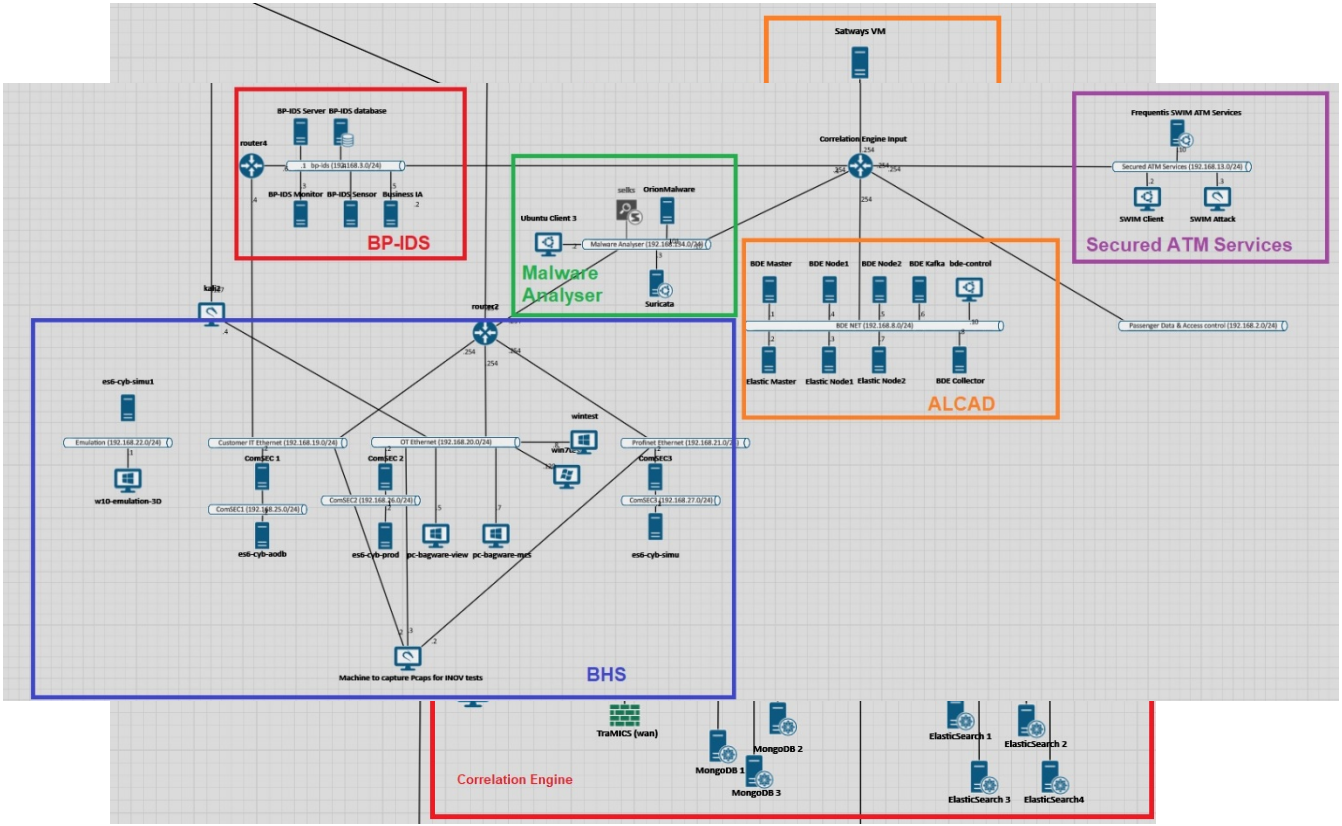


Integration room available in Elancourt

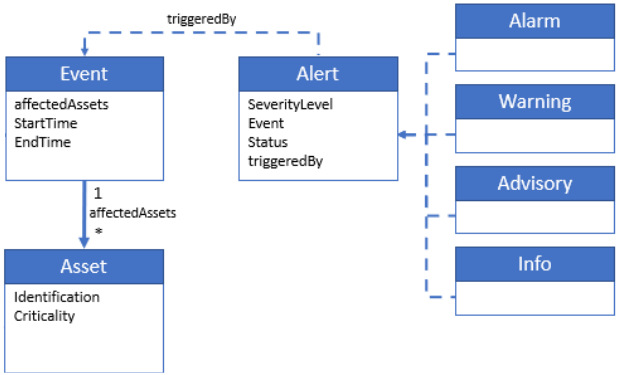




Each system has been deployed on the CyberRange platform



Ontology and semantics of the system were defined



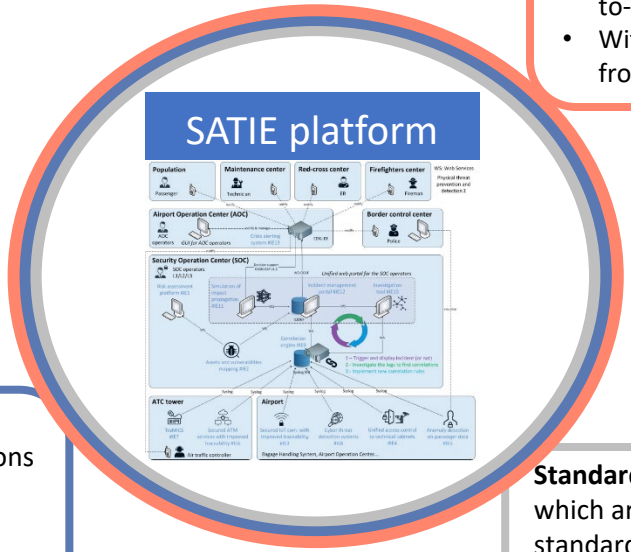
Steps of the scenario (e.g. MITM attack) are being decided on

	Detail	Information
Step 3	Description	A cyber-attack on the SWIM services
	Feared event	Unavailability of SWIM services
	Attacker	APT group (criminal organization)
	Attacker's objective	To produce chaos and confusion
	Motivation	Money/terrorism
	Simulation	SWIM services need authontication, DoS new user request overload, bruteforce attack
	Attack path	1) DoS attack on an unpatched Linux machine with user authorization which is connected to the SWIM services (exploit a known OS vulnerability) 2) The attacker takes control of the computer
	Assets	One computer, SWIM services server, network infrastructure
	Impacts	Flight plans are unavailable; flights are cancelled, aircraft stay grounded
	Means of detection	Correlation Engine
	Incident response	The Air Traffic Management services team enters a new security level

The platform verification & validation plan is being developed

Bespoke validation questions – based on each system (IE), both quantitative checks and qualitative questions will be tailored to determine the validity:

- Do you trust this system's results to be accurate and up-to-date?
- With what frequency (per minute) do you receive updates from this system?



General validation questions – both quantitative checks and qualitative questions about the SATIE solution:

- Is this solution **useful** and **acceptable**?
- Was it an acceptable length of time to receive an alert?
- Does the solution produce too many false positives?

Standard validation questionnaires – questionnaires which are already on the market in order to standardize and legitimize our approach:

- System Usability Scale (**usability**, **trustworthiness**)
- Trust questionnaire from Eurocontrol SHAPE project

3. Challenges and issues

Sensitive information

- Collecting necessary information from end-users to perform the risk assessment and threat propagation while abiding by all EU-restricted regulations (international and national)
- Meeting project needs with end-user operational needs:
  - Having real-time vulnerability detectors installed on airport systems
  - Performing accurate demonstration scenarios with shadow systems in the airports with access to sensitive data

Covid-19 Related Unavailability

- Decreased availability of end-users (airport closures)
- Unavailability of partner personnel to work (due to restricted working hours, forced vacation, etc.)
- Lack of physical access to some systems has prevented particular progress to be made
- Unreliability of teleconferencing (especially audio) has decreased the efficiency of the meetings

Further information and results can be found at http://satie-h2020.eu/

This project has received funding from the European Union's Horizon 2020 research and innovation programme under grant agreement No 832969. This output reflects the views only of the author(s), and the European Union cannot be held responsible for any use which may be made of the information contained therein.