

## SAFECARE SAFEGUARD OF CRITICAL HEALTH INFRASTRUCTURE



Integrated cyber-physical security for health services

Integrated cyber-physical security for health services

### PURPOSE

The lines between the physical and cyber world are becoming increasingly blurred as the IoT takes off and digital connections become omnipresent.

In areas where this is not currently the case, physical intrusion may break down barriers. Threats can no longer be analysed solely as physical or cyber and **it is therefore critical to develop an integrated approach in order to fight against such a combination of threats.** Health services are among the most critical infrastructure, and most vulnerable.

### OBJECTIVE

Bringing together the most advanced technologies from the physical and cyber security spheres, SAFECARE aims to deliver high-quality, innovative and cost-effective solutions in system security. These solutions focus on mitigating cyber-physical threats and incidents and their interconnections and potential cascading effects.

SAFECARE aims to **provide solutions that will improve physical and cyber security** by promoting new technologies and novel approaches to enhance threat prevention, threat detection, incident response and mitigation of impacts.



### RESEARCH AREAS



Risk assessment and solution requirements



Cyber security solutions



Physical security solutions



Integrated cyber-physical security solutions

## USE-CASE



**Real demonstrations** are planned in three European hospitals: Amsterdam, Marseille and Turin.

## OUR ROLE IN THE PROJECT

- **Act** as project technical coordinator
- **Lead** in cyber security solutions taking into account the whole eco-system of a hospital including IT networks, OT infrastructure (medical devices) and Building Management System (BMS)
- **Provide** the interconnection of Orion Malware with the Stormshield Network Security (SNS) firewall, the Suricata NIDS and the Forescout's sensor, an OT intrusion detection sensor
- **Carry out** the integration of an impact propagation model with Cymerius security hypervisor and visualise the potential effective cascades of an attack
- **Integrate** all the solutions into our CyberRange virtual environment
- **Simulate** SAFECARE designed cyber-physical scenarios of threats
- **Enable** the investigation of zero-day attacks based on artificial intelligence
- **Address** OT vulnerabilities in hospitals and combined physical and cyber security incidents to assess the propagation of any impact in a critical infrastructure

## ABOUT ORION MALWARE

Orion Malware is a file analysis network platform designed to be able to analyse hundreds of files submitted at the same time by users or systems in order to detect malicious content.

Orion Malware, was produced by our own CSIRT team and is available as an all-in-one application that can perform up to 50,000 analyses per day, or as a specialised application to meet larger needs. We recently developed a functionality to take into account **medical files**.



**HORIZON 2020:** [ec.europa.eu/programmes/horizon2020](https://ec.europa.eu/programmes/horizon2020)

**SAFECARE:** <https://www.safecare-project.eu>

This project has received funding from the European Union's H2020 research and innovation programme under grant agreement no. 787002.



Programme co-funded by the  
EUROPEAN UNION

## AIRBUS

### FRANCE

Metapole 1, boulevard Jean Moulin  
CS 40001 / 78996 Elancourt Cedex  
France

### GERMANY

Willy-Messerschmitt-Str. 1  
82024 Taufkirchen  
Germany

### UNITED KINGDOM

Quadrant House / Celtic Springs  
Coedkernew / South Wales  
NP10 8FZ / United Kingdom

This document is not contractual. Subject to change without notice.  
© 2020 Airbus CyberSecurity. AIRBUS, its logo and the product names are  
registered trademarks. All rights reserved. // 917 E 0875

[contact.cybersecurity@airbus.com](mailto:contact.cybersecurity@airbus.com)  
[www.airbus-cyber-security.com](http://www.airbus-cyber-security.com)

