

## Development of a federated CyberRange solution

- FORE SIGHT aims to develop a federated CyberRange solution **to enhance the preparedness of cyber security professionals** at all levels and **advance their skills** towards preventing, detecting, reacting and mitigating sophisticated cyber-attacks.
- This is achieved by delivering an **ecosystem of networked realistic training and simulation platforms** that collaboratively bring unique cyber security aspects from the aviation, power grids and naval domains.



AVIATION



POWER GRID



NAVAL

**Ability to create a complex, accurate and realistic environment to train cyber security professionals in an innovative way**



- The proposed platform will extend the capabilities of existing CyberRanges and will allow the **creation of complex cross-domain/hybrid scenarios** to be built jointly with the IoT domain.
- Emphasis is put on the **design and implementation of realistic and dynamic scenarios** that are based on identified and forecasted trends of cyber-attacks and vulnerabilities extracted from cyber threat intelligence gathered from the dark web; this will enable cyber security professionals to rapidly adapt to an evolving threat landscape.

## Objectives

- 1 CREATE** a state-of-the art platform that will greatly extend the capabilities of existing cyber-ranges by allowing them to be a part of a CyberRange federation
- 2 DELIVER** training curriculum aimed at cyber security professionals to implement and combine security measures in innovative ways
- 3 DEVELOP** realistic and dynamic scenarios based on identified and forecasted trends and needs in terms of cyber-attacks and vulnerabilities
- 4 INCREASE** the dynamics of training and awareness methods in order to match or even exceed the rate of evolution of cyber-attackers
- 5 IMPROVE** the preparedness of cyber security professionals and the availability of talents (from junior to senior)
- 6 IDENTIFY** the impact of cyber risks and the most appropriate security measures to protect valuable assets, minimise costs and recovery time

## Our role in the project

Our CyberRange is an **advanced training and simulation solution** that allows you to easily model IT/OT systems composed of tens or hundreds of machines and **simulate realistic scenarios** including real cyber-attacks.

The platform is open to interface with **external equipment** such as a physical industrial control system, a hardware traffic generator, a real physical or virtual system, to meet the constraints of a **complex environment**.

An **international Airport in Europe** is currently reproduced in our CyberRange for security practitioner to be **trained on real systems**. We also model **access control, management of public announcement and flight displays systems**.



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

**FORESIGHT:** <http://foresight-h2020.eu>

This project has received funding from the European Union's Horizon 2020 research and innovation programme under grant agreement No 833673



## AIRBUS

**FRANCE**  
Metropole 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.  
© 2021 Airbus CyberSecurity. AIRBUS, its logo and the product names are registered trademarks. All rights reserved.

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



**FORESIGHT**