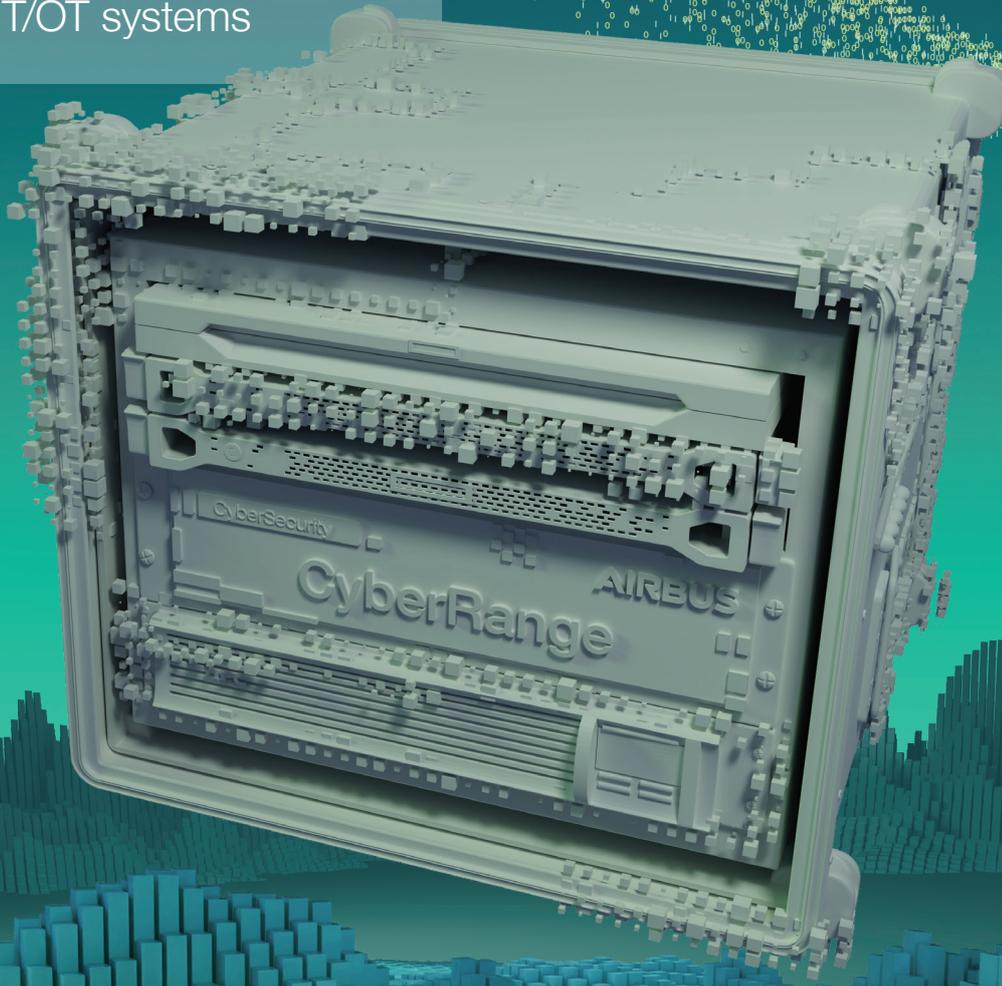


DEFENCE AND SPACE  
Cyber

# CyberRange

Integration and simulation  
platform of IT/OT systems



**AIRBUS**

# All-in-one advanced solution to meet all your simulation, testing and training needs



**Build simulation environments** made of virtual and external assets such as physical equipment and get closer to your context



**Replicate representative activities of your operations** and conduct penetration tests in an isolated environment



**Simulate realistic scenarios, (plug & play),** including real cyber-attacks

## WHY DO YOU NEED A CYBERRANGE?

- **Test & Train:** test integration changes in realistic IT/OT systems and train your teams
- **Collaboration:** Join the CyberRange community and contribute to the library of existing bundles
- **Agility:** Work alone or in a team in the same workspace or in parallel in different spaces
- **Safety:** Perform operations in an environment isolated from your production systems
- **Training:** Deliver training services for your teams, for cyber experts and for a wider public
- **Recruitment:** Asses candidates cyber skills and recruit them quickly

## A HYBRID PLATFORM WITH ADVANCED FEATURES

### DESIGN

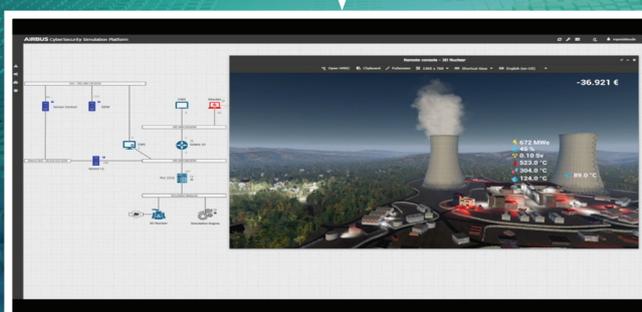
- Design of representative IT and OT systems
- Build your virtual infrastructures from our built-in library components
- Import, export and save your topologies
- Capitalise your work by extending the built-in libraries of components and actions
- Customisation of topologies' graphical representation to give more context and realism

### SIMULATION

- Creation and orchestration of complex scenarios replicating realistic actions
- A starter-pack library to configure (machines, actions, life generators, cyber-attacks)
- Hybrid modelling by combining physical and virtual systems
- Includes ready-to-use IT and OT libraries and scenario examples

### COLLABORATION

- Multi-site collaborative teamwork, light client accessible from a web browser
- 150+ ready-to-use contents available in the HUB
- Management of multiple and isolated workspaces, with access rights per user
- Resource sharing (VMs, topologies, scenarios) through a unique Community portal
- Ability to chat with connected people



# A unique and versatile platform designed for a wide range of users and sectors

CyberRange adapts to the needs of a large spectrum of users and their specific operational contexts:

## USERS

- Conduct tests, train and practice on cyber scenarios

## TRAINERS

- Define, plan and deliver collaborative training courses (including multi-site)

## INTEGRATORS

- Model systems and integrate IT/OT infrastructure

## EXPERTS

- Build test or cyber-attack scenarios

## PARTNERS & CLIENTS



### Ministries of Defence

France, Italy

### Industries

Framatome, IRSN, CEA, UIMM...

### Organisations

NeverHack, StormShield, Campus Cyber

### Schools and Universities

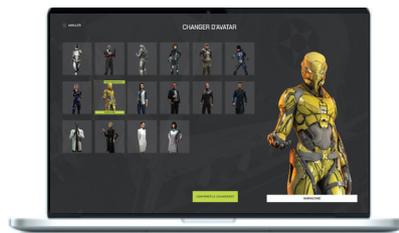
CNAM GrandEst, ENSIBS, ESIEA, ISEN, IMT Atlantique, Telecom Nancy, ESNA Bretagne, ESAIP, ECAM, AFORP, ISEP...

## We offer options to extend CyberRange's capabilities



### GAMING MODULE

Do you want an immersive experience for your users? CyberRange offers a gaming portal with designed ready-to-use realistic challenges to create instinctive skill path and self-driven practice for attendees.

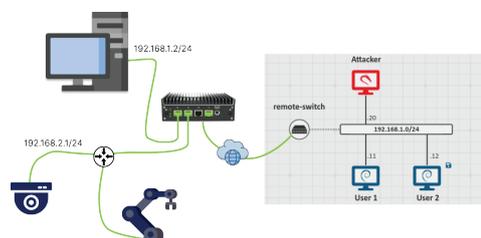


The Gaming Portal includes solo, team modes and performance reports. It offers an immersive experience through a unified interface with aesthetic graphics, scoring and live support.

### REMOTE SWITCH

The Remote Switch enhances your CyberRange capabilities by allowing you to easily interconnect your CyberRange topology to remote physical equipment, enabling the connection of your IT and OT equipments to a virtual infrastructure hosted in your CyberRange platform.

Thanks to the Remote Switch and with a very simple configuration, you will be fully ready to create large and complex topologies using both physical and virtual devices.



## MULTIPLE ACCESS SOLUTION

CyberRange is available :

- As a SaaS
- OnPremise
- Through a mobile box

Airbus Defence and Space Cyber can provide additional services on infrastructure construction, scenarios and CyberSecurity training. For more information, please consult our catalogue.

# What are the main CyberRange use-cases?

## PRE-PRODUCTION TESTING

- Easy access to an integration platform
- Work collaboratively in isolated or shared environments
- Test new equipment and safety procedures in a realistic environment

## OPERATIONAL QUALIFICATION

- Evaluate the impact of new equipment integration, new rules or security patches on a system
- Analyse the behaviour of cyber attacks on your infrastructure without taking risks

## TRAINING

- Train your teams in operational exercises close to their daily environment
- Evaluate the efficiency of your security system in the context of a cyber crisis management exercise involving technical teams



## GAMING NEW

- Raise the awareness of all your staff and train them in correct cybersecurity practices by setting up «gamified» challenges
- Increase the skills of your cyber teams or keep their knowledge up-to-date in order to deal with new threats environment

## OPERATE CAPTURE THE FLAG CHALLENGES

Hold «Defence-oriented» challenges on your CyberRange with exercises in network exploration, forensics, system hardening, integration, pentest and development.



The CyberRange is the leading platform for major events CTF (ECW, EC2)

250+ participants have already fought against each other in teams for 8 hours

1550+ machines operated simultaneously on the CyberRange platform

## A renowned solution



Used by 25 schools & universities

More than 1000 students are trained on the CyberRange across Europe



**Security Trophy**  
Gold Medal 2023  
**CyberNight Trophy**  
Silver Medal 2023  
**France Cybersecurity**  
2021 Label

« The CyberRange has strengthened our teaching approach with more technical and operational exercises in realistic environments, providing high-quality training for our customers »

**Florence Puybareau**  
Head of Operations  
Campus CYBER Hauts de France



**Airbus Defence and Space**

France, Germany, United Kingdom, Spain

This document is not contractual. Subject to change without notice.  
© 2024/05 Airbus Defence and Space. AIRBUS, its logo and the product names are registered trademarks. All rights reserved.

[www.cyber.airbus.com](http://www.cyber.airbus.com)

[contact.cybersecurity@airbus.com](mailto:contact.cybersecurity@airbus.com)



@Airbus Defence and Space Cyber

**AIRBUS**