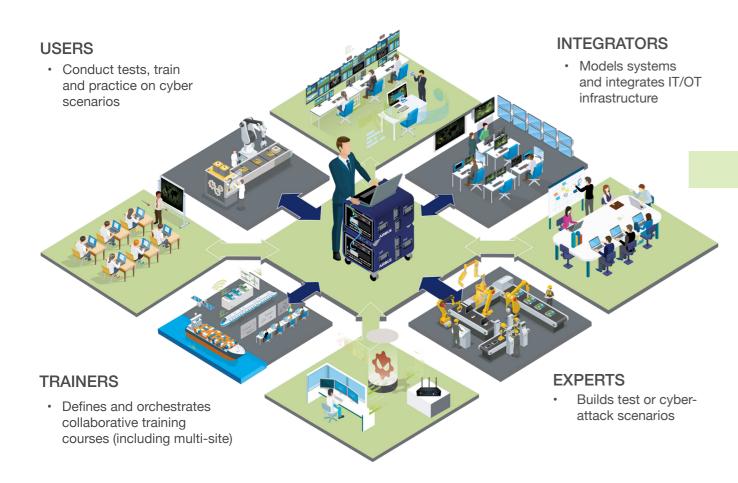# CyberRange

Integration and simulation platform of IT/OT systems

- **Build complex virtual and physical systems** close to your environment

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

- **Simulate realistic scenarios,** without delay (plug & play) and in collaborative mode, including real cyber-attacks

AIRBUS

CyberRange, an agile and versatile environment

USERS
- Conduct tests, train and practice on cyber scenarios

INTEGRATORS
- Models systems and integrates IT/OT infrastructure

TRAINERS
- Defines and orchestrates collaborative training courses (including multi-site)

EXPERTS
- Builds test or cyber-attack scenarios

- A WEB interface enables easy **modeling**, **deployment** of virtualized infrastructures and **execution** of attack scenarios
- The CyberRange integrates ready-to-use libraries and allows you to integrate your existing content, or available content directly on the Internet market place

A platform designed to build complex simulations tailored to your needs

OPEN SIMULATION
Simulation environment «at your command» to use or create large IT/OT systems (virtual or hybrid) and reproduce a realistic activity

PRODUCTIVITY
Efficiency gains with the use of component libraries and «on-the-go» deployment and network configuration of machines or topologies

COMMUNITY
Shared technical base to work in teams on the same project simultaneously or to exchange resources (machines, topologies, scenarios)

A hybrid platform with advanced features

Designing
- Design of real or representative IT/OT systems
- Integration of existing equipment or from your own system
- Light client accessible from a web browser
- Configuration management of your component library
- Import and/or export capability to exchange your designs

Simulating
- Creation and orchestration of complex scenarios replicating realistic actions
- A comprehensive library of actions to configure (tests, life generators, cyber-attacks)
- Hybrid» modeling by coupling physical and virtual systems
- Includes ready-to-use IT and OT libraries and scenario examples

Collaboration
- Multi-site collaborative teamwork
- 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

CyberRange Offer

CyberRange is available as **SaaS**, **OnPremise**, or through **a mobile box.**

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

ZOOM

Crisis Management Challenges «Capture-The-Flag»

> «Defence-oriented» challenge with exercises in network exploration, forensics, system hardening, integration of security tools, reverse, pentest and development

250
PARTICIPANTS ARE FIGHTING AGAINST EACH OTHER
IN TEAMS OF 3 FOR 8 HOURS

1550
MACHINES OPERATE SIMULTANEOUSLY ON THE CYBERRANGE PLATFORM

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

Formation and 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

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

CyberRange **benefits**

Network of partners

(Seela, Stormshield, Orsys, schools and universities)

France Cybersecurity 2021 Label

(cyber excellence)

« The Airbus CyberRange is one of the most well executed pieces of infrastructure I have ever seen »
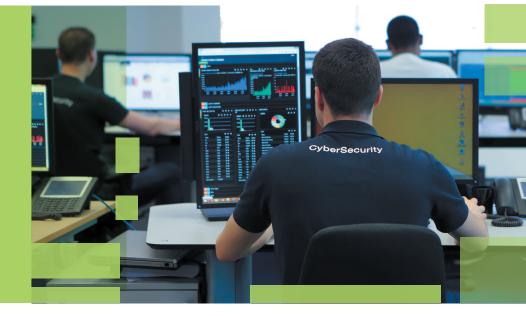
Mark Howell
Managing Director Europe
Attivo Networks

Attivo
NETWORKS

A PROPOS

The Cyber business within Airbus Defence and Space provides companies, critical national infrastructure, government and defence organisations with reliable and high-performance security products and services to detect, analyse and counter the most sophisticated cyber-attacks.

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

contact.cyber@airbus.com
www.cyber.airbus.com