Securing Critical
Business

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**
- **Simulate realistic scenarios including real cyber-attacks**

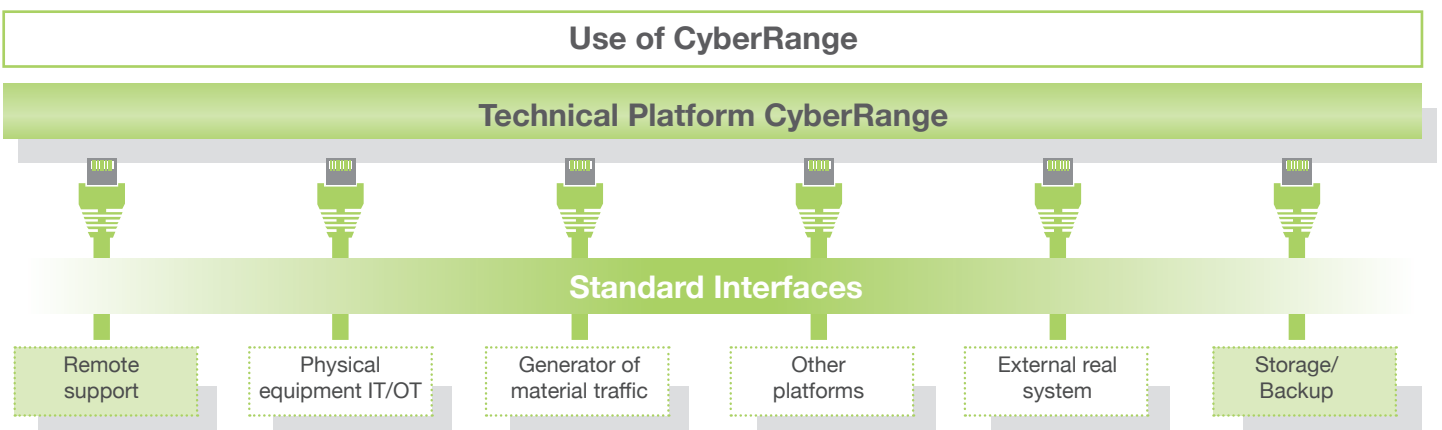# The CyberRange, an agile environment

- A technical platform composed of high-performance servers stored in a mobile box or in the cloud

- A management software (LADE) that simplifies the deployment of virtualised infrastructures and the set of attack scenarios

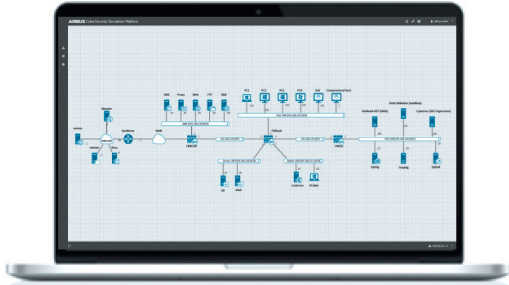# The CyberRange, advanced functionalities

- Modelling of real or representative systems (IT, OT, ICS, SCADA)
- Hybrid» modeling by integrating physical components into the system
- System animation via an integrated live traffic generator
- Orchestration of complex scenarios
- Open libraries of cyber-attacks accessible from the interface

- Backup and deployment of IT/OT topologies «on the fly» from the interface
- Import of existing VM in the application library
- Simplified network configuration
- Configuration management of the virtual machine park
- Access to the screen offset or command line to each virtualised machine

- Management of multiple workspaces isolated from external systems
- Management of access rights by user
- Collaborative team work across different sites
- Sharing of resources (VM, topologies, scenario) between users
- Thin client accessible from a web browser

Using the CyberRange

The CyberRange platform is open to interface with external equipment to serve multiple application cases.

Use of CyberRange

Technical Platform CyberRange

Standard Interfaces

Remote support	Physical equipment IT/OT	Generator of material traffic	Other platforms	External real system	Storage/ Backup

CyberRange, a platform designed to facilitate complex integration projects

OPEN SIMULATION

Simulation environment «at your fingertips» to use or create large IT/OT systems (virtual or hybrid) and reproduce a realistic activity (traffic or cyber-attack)

PRODUCTIVITY

Increased productivity and efficiency with operations component libraries as well as the deployment and network configuration «on the fly» of machines or topologies

TEAM WORK

Shared technical base to work in a team on the same project simultaneously or to exchange resources (machine templates, topologies, scenario)

Use cases of the CyberRange

Pre-production tests
- Easy access to an integration platform
- Collaborative work in isolated or shared environments
- Testing new safety equipment and procedures in a realistic environment

Operational qualification
- Assessment of the impact of new equipment or application of patch on a system
- Study of rule integration or the implementation of new procedures
- Analysis of cyber-attack behaviour on its infrastructure without taking any risks

Training
- Awareness training for all staff and training on cyber security best practices
- Development of skills of cyber teams or knowledge retention to face new threats

Exercises
- Training of teams as part of operational exercises close to their daily environment
- Evaluation of the effectiveness of its security system as part of a cyber crisis management exercise involving technical and managerial teams

ZOOM
Challenge «Capture-The-Flag»

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

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

1550 MACHINES OPERATE SIMULTANEOUSLY ON THE CYBERRANGE PLATFORM

CyberRange **Offer**

CyberRange is available in a mobile box, a bay or in the cloud. The offer is scalable with a standard version that can be completed with upgrades to create a custom CyberRange.

CyberRange

Standard CR — **Configuration of 8 work zones**
(indicative capacity 150 VMs and/or 5000 Dockers)

Tailored CR — **Upgrade to up to 64 workzones**
(indicative capacity 1200 VMs and/or 40000 Dockers)

CyberRange Cloud

Standard CR cloud — **Configuration 2 work zones**
(indicative capacity 50 VMs and/or 1500 Dockers)

Tailored CR — **Upgrade to up to 64 workzones**
(indicative capacity 1200 VMs and/or 40000 Dockers)

CyberRange **Services**

Creation of on-demand content
(topologies, scenario)

Challenge organisation
(Capture-the-Flag or Red team/Blue team)

Organisation of exercices
(operational or crisis management)

Organisation of IT/OT training
(in catalogue)

ABOUT US

Airbus CyberSecurity 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.

**FOR MORE INFORMATION:
Airbus CyberSecurity**

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

UNITED ARAB EMIRATES
Etihad Towers T3 / Corniche Road,
19th floor / P.O.Box: 72186 /
Abu Dhabi /
United Arab Emirates

contact.cybersecurity@airbus.com
www.airbus-cyber-security.com

AIRBUS