CyberSecurity

CyberRange
Stay ahead of the threat

Operational capability for Cyber Training and Cyber Testing

- Assess your cyber defense capabilities
- Enhance your security processes
- Prepare your security team for the next cyber attack
- Stay in control of your Cyber Defense strategy

AIRBUS

What are your challenges ?

OPERATIONAL EFFECTIVENESS

There is a skills shortage in Cyber which makes it complicated to hire employees and maintain a high level of operational effectiveness.

RESILIENCE OF THE SYSTEM

Systems are complex and fragile, requiring an additional effort in design & integration - including testing - to build a resilient system.

One solution: Airbus CyberRange

CyberRange provides operational capability for Cyber Training and Cyber Testing.

The platform recreates realistic IT infrastructures that can be used as a lab to play realistic scenario including real Cyber Attacks in a secured environment.

Key benefits

Reduce the impact of cyber attacks

Build your Cyber Workforce

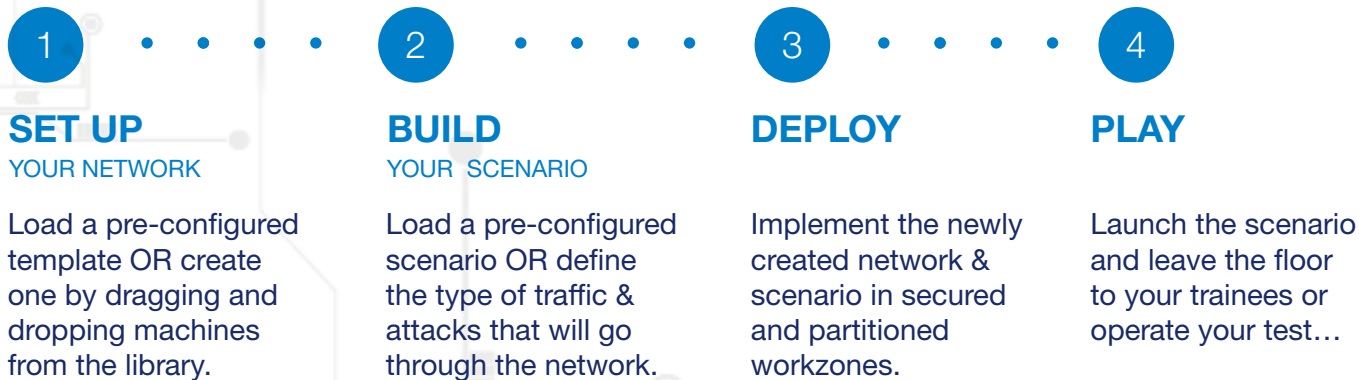Increase your in-house knowledge

Improve your security procedure
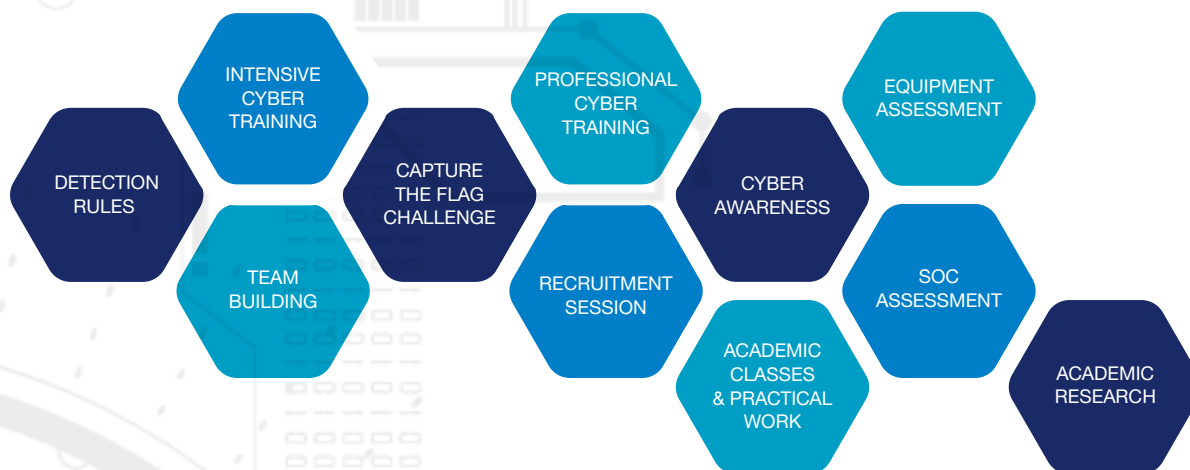
Save money on testing

Increase employee engagement

How does it work ?

1

SET UP
YOUR NETWORK

Load a pre-configured template OR create one by dragging and dropping machines from the library.

2

BUILD
YOUR SCENARIO

Load a pre-configured scenario OR define the type of traffic & attacks that will go through the network.

3

DEPLOY

Implement the newly created network & scenario in secured and partitioned workzones.

4

PLAY

Launch the scenario and leave the floor to your trainees or operate your test…

What are the use cases for the CyberRange ?

- INTENSIVE CYBER TRAINING
- DETECTION RULES
- CAPTURE THE FLAG CHALLENGE
- TEAM BUILDING
- PROFESSIONAL CYBER TRAINING
- CYBER AWARENESS
- EQUIPMENT ASSESSMENT
- RECRUITMENT SESSION
- SOC ASSESSMENT
- ACADEMIC CLASSES & PRACTICAL WORK
- ACADEMIC RESEARCH

Airbus CyberRange - A well proven solution

CyberRange run the official playground for the European Cyber Week Challenge Final.

SCALABILITY
48 challenge participants

PERFORMANCE
1 300 machines running on 1 CyberRange

STABILITY
6 hours of competition

RELIABILITY
0 resource required to monitor the CyberRange

Performance & Scalability

CyberRange is available in different packages
to fit the particular needs of your organization

	Small	Medium	Large
Participants (simultaneously)	12	24	48
Work zones	4	8	16
Virtual machines (up to)	75	150	300
Containers (up to)	2.500	5.000	10.000

Our team support your effort to stay ahead of the threat

**KNOWLEDGE
OF THE THREAT**
Airbus CTI and
Pen test teams

**KNOWLEDGE
OF THE BUSINESS**
Airbus CSIRT
and SOC

**OPERATIONS
FEEDBACK**
Integration
team

**CONCEPTUAL
APPROACH**
University & Research
institute

Tailored approach

Our experts can create specific exercises
& scenarios for your organization taking
into consideration your background,
your IT environment and your exposure
to cyber Threats.

What now ?

We can plan a product presentation, a demo or simply talk about CyberRange.

contact.cybersecurity@airbus.com

AIRBUS

Airbus CyberSecurity