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
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
- Improve your security procedure
- Save money on testing
- Increase your in-house knowledge
- 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?

- **SET UP YOUR NETWORK**
- **BUILD YOUR SCENARIO**
- **DEPLOY**
- **PLAY**

Airbus CyberRange - A well proven solution

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

**SCALABILITY**
48 challenge participants

**PERFORMANCE**
1300 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

<table>
<thead>
<tr>
<th></th>
<th>Small</th>
<th>Medium</th>
<th>Large</th>
</tr>
</thead>
<tbody>
<tr>
<td>Participants</td>
<td>12</td>
<td>24</td>
<td>48</td>
</tr>
<tr>
<td>Work zones</td>
<td>4</td>
<td>8</td>
<td>16</td>
</tr>
<tr>
<td>Virtual machines</td>
<td>75</td>
<td>150</td>
<td>300</td>
</tr>
<tr>
<td>Containers</td>
<td>2.500</td>
<td>5.000</td>
<td>10.000</td>
</tr>
</tbody>
</table>

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

---

Metapole 1, boulevard Jean Moulin / CS40001
78996 Elancourt Cedex / France
T: +33 (0) 1 61 38 50 00

Willy-Messerschmitt-Str. 1
82024 Taufkirchen / Germany
T: +49 (0) 89 607 - 0

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

Follow us:
/AirbusCyber  @AirbusCyber

---

AIRBUS CyberSecurity
This document is not contractual. Subject to change without notice. © 2018 Airbus CyberSecurity. AIRBUS, its logo and the product names are registered trademarks. All rights reserved.