CYBERSECURITY

Cyber Incident Games

Play the role of a cyber attacker and plan your own cyber attack

Cyber Incident Games are training sessions for your employees who have only ever experienced IT / OT as users.

In the game, **participants play the role of a cyber attacker**, receive missions and plan cyber attacks to compromise the IT infrastructure.

Cyber Incident Games use different IT infrastructure depending on the needs of the customer. A classic business network comprising of different elements - such as laptops, stationary workstations, a website - offers angles of attack for theft, phishing attempts or other insidious plans.

A game plan is also available with an industrial infrastructure composed of not only production facilities, but also important production data.

The participants are free to choose how they complete their mission and what methods they use. **Social engineering methods, malicious USB sticks or email attachments** can all be used and be combined.

The possibilities are endless in terms of creative and imaginative methods of cyber-attacks. **The winner is the participant who develops the most insidious cyber attack and successfully completes the mission.**

AIRBUS

Cyber Incident Games

Play the role of a cyber attacker and plan your own cyber attack

After the cyber attacks have been planned, **the attack techniques used are analysed and IT security measures for defence are discussed**.

Here, the four dimensions of the BSI (German Federal Office for Information Security) – namely personnel, technology, organisation and infrastructure – play a special role.

This creates realistic situations to better detect vulnerabilities, risks and opportunities for attackers. This perception of the vulnerabilities, risks and opportunities in turn leads to faster initiation of security measures, and of course, also leads to the acceptance of measures that, from the user's point of view, are perhaps more of a hindrance.

Cyber Incident Games are used as a means **to increase IT/OT security awareness and promote the target dimensions of perception, knowledge and safe behaviour.** To achieve synergies, Cyber Incident Games can be combined with other Airbus IT/OT security awareness measures. For example, a live hacking lecture could provide additional inspiration to participants for their own cyber attacks and protective measures.

Think about the scope and the extent that you would prefer when organising Cyber Incident Games with us!

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