Our experience working with OT environments enables us to conduct successful OT Penetration Tests on your industrial

Internal attackers and malicious malware are not easy to spot in OT networks. We help you detect intrusions by providing device, network and alarm level penetration testing that exposes detection capabilities, abnormal activities or attack paths inside the network.

We test OT systems through realistic hacking simulations and cyber-attacks

OT networks are often a combination of different operative systems, sensors, IT/OT protocols and wireless protocols. This makes the attack surface much larger than in IT networks. Therefore, **we combine methodologies and tools from both IT and OT pentesting.**

As risk analysis for cyber-attacks is often carried out based on only theoretical assessments and «cyber incidents», and does not represent a theoretical threat, **we offer you a realistic simulation of a «hacker attack»** to enable a genuine assessment of the attack resistance capabilities of your OT network. The purpose of the practical findings is to (a) revise the risk assessment of the OT system and (b) fix the identified cyber security vulnerabilities before an attack takes place.

We support you to:

- *Understand your current cyber security posture and identify critical processes and devices*
- *Expose hidden weaknesses and vulnerabilities at an early stage to mitigate issues*
- *Detect and isolate malicious activities at an early stage or prevent these activities in the first place*
- *Protect your automation network against external or internal attackers*
- *Create adequate security measures to ensure production will not be interrupted, or cause financial and reputational damage as well as maintaining human safety*
- *Make the right investments in security*
- *Raise your employees' awareness of safety processes*

AIRBUS

OT Penetration Test Modules

1. Attack Vector Analysis
Map all attack vectors that can be executed against infrastructure and devices

You will discover:
- Any flaws e.g. in network architecture, design, configuration and firewalls
- How attackers can use these flaws as attack paths into networks or devices

2. Vulnerability Scanning
Look for any vulnerability to avoid any disruption

You will discover:
- An overview on device, network and communication level vulnerabilities and their severity and exploitability
- How the found vulnerabilities will be tested and documented

3. OT Penetration Test
(Live system hacking)
Test all access points from external to internal networks

You will discover:
- Exploitability of the system, devices, frequencies and its impact to system security
- How to mitigate all found vulnerabilities

4. Process Assessment for OT-Security Operations
Evaluation of your cyber security situation

You will discover:
- Missing processes, gaps based on standards
- Issues in security practices and policies
- Detailed information of weaknesses in implementation, guidelines and processes
- How to master them to avoid any issues in operations

5. OT Device Level Testing
Deep level of device testing: Test all weaknesses and vulnerabilities and possibilities to exploit the devices

You will discover:
- Exploitability of the devices and the impact on system security

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