

Deceptive

Security

Develop cyber resilience with our Deceptive Security services

Organisations' information systems are increasingly being exposed to cyber attacks, intrusion attempts and sophisticated malware. Rather than utilising a suite of complex cyber solutions, our **Deceptive Security services** enable you to focus your cyber resources on those targeted attacks that are not easily detected by traditional means of defence.

A **HoneyPot** is a relevant deceptive security tool that helps you to investigate the motivations, equipments and methods of attackers while preserving the confidentiality, integrity and availability of your legitimate information systems.

Strengthen your detection capabilities

Our Deceptive Security services add an extra layer of cyber security through the combination of digital decoys, traps and breadcrumbs, - all combined with a wider attack surface.

A **HoneyPot** enables you to create a diversion by luring an attacker towards an artificial information system in order to slow them down, alert your SOC and gather information about the attack. This intelligence can help uncover new attacks and enrich the defences of the legitimate information system, in a cycle of continuous improvement for your security.

Increase your reaction speed and capacity

Our Deceptive Security services allow you to reinforce your reaction capabilities to face an intrusion or a cyberattack. They generate qualitative information and may capture new kinds of threats that have never been observed before.

The observation of the methods and tools used by attackers on the HoneyPot enables the improvement of the legitimate information system defences and the maintenance of activity and operational capacities in

Our **Deceptive Security** services fulfill three essential functions:



PREVENTION

by directing the attacker to the decoys and the HoneyPot



DETECTION

by alerting your SOC in the instance of intrusions or threats



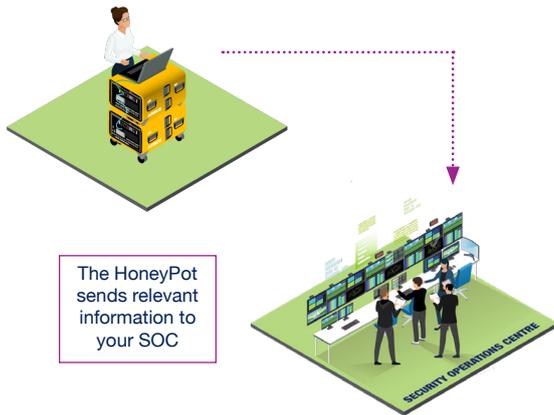
REACTION

by collecting information on the aggressor to adapt the response



An innovative Deceptive Security Solution

- **Distract, detect and isolate** attackers conducting targeted operations, towards known and unknown vulnerabilities within your systems
- Integrate an interconnected system that **increases and accelerates your ability to detect cyber attacks**
- Deploy **digital decoys, traps and breadcrumbs** to protect your systems and data
- **Increase the comprehension** of the attacks observed by the decoy information system - and use this knowledge to **continuously improve your legitimate cyber defences**
- In the event of a system failure, return - partially or totally - to the **previous state of the architecture**



Enhancing your SOC capacities

- **Simple and quick communication** with your SOC to alert it directly in case of intrusion or cyber attack
- **Improve incident response:** decoys are configured to facilitate investigations
- Add an **extra layer of cyber security** to your SOC

Airbus CyberSecurity provides 24/7/365 SOC services

Services based on our CyberRange technology

Our Deceptive Security services are made more efficient thanks to the technologies of our CyberRange platform, which enables us to **create hyper-realistic decoy information systems** that are fully representative of your legitimate systems. The HoneyPot CyberRange notably **uses bots to simulate activity on duplicate systems**. It also uses **machine learning for a continuous reinforcement of its capacity** to detect potential threats.

- An IT topology with typical services such as computer firewall and user workstations
- Network architectures according to the IEC 62443 standard and actual implementations



Contact us for more information



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



This document is not contractual. Subject to change without notice.
© 2021 Airbus CyberSecurity. AIRBUS, its logo and the product names are registered trademarks. All rights reserved.

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

