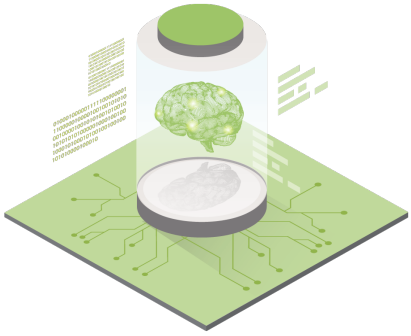
CYBERSECURITY

Artificial Intelligence

Our AI improves the performance of defensive solutions by introducing an additional cognitive layer to your system

Airbus CyberSecurity, with its many years of experience and research in Artificial Intelligence, offers both **operational AI - implemented using Orion Malware - as well as research into AI-driven cyber security processes, such as User and Entity Behaviour Analytics (UEBA)**. By combining defensive AI and adversarial AI with its R&D research, Airbus CyberSecurity has built a virtuous system that, given time, **will be capable of diagnosing and certifying all AI products on the market.**



The purpose of AI research is to enrich existing SOCs by bringing together the best of SIEM detection and AI through the sharing of threat intelligence resources. AI introduces an additional cognitive and predictive layer that reinforces human expertise without replacing it.

Use-case: Defensive AI

- HoneyPot, the only European machine learning solution
- Increase the detection of attacks by extending and duplicating the attack surface (deceptive security) while simultaneously correcting any detected weaknesses
- Ability to detect and isolate unknown and sophisticated threats, such as unrecognised attacks from enemy AIs
- Straight-forward and fast communication with your SOC and receive immediate alerts in the event of an intrusion

Use-case: Adversarial AI

- Identify weaknesses within the organisation to enhance cyber security policy, educate employees about vulnerabilities, and ensure that the organisation is prepared for even the most sophisticated attacks
- Contribute to improving the detection rate and protection mechanisms for cyber defenders, in particular by SOC teams

AIRBUS

What we offer

Behavioural Analysis

- UEBA (User and Entity Behaviour Analytics) cognitive supervision
- Improved profiling and analysers (40 file formats already supported)
- Machine learning techniques
- Interconnects with the MISP and APT databases

Assessment and Certification

- Assessment of business AI
- Help administrations certify AIs
- Validate AI compliance with CyberRange
- Studies on IoT with artificial intelligence

Prediction

- Anticipation of solutions
- Advanced Cyber Threat Intelligence
- Cross-functional and context-independent analyses
- Ability to customise sandboxes

AI already intervenes cross-functionally on our solutions

Thanks to the skills of a multi-faceted team (researchers, experts, data scientists, AI architects) combined with significant technical capacities, Airbus CyberSecurity is at the forefront of innovation and the implementation of use cases in the field of AI:

- Improved static analysis
- Improved dynamic analysis
- Improved detection of advanced persistent threats (APT)
- Improved detection of weak signals
- Improved categorisation of security events

To meet the technological and human limits encountered by systems cyber security, AI technologies are involved in all areas of Airbus CyberSecurity:

- Restructure processes and save time for experts
- Enable cross-functional action
- Embedded intelligence (edge computing)

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