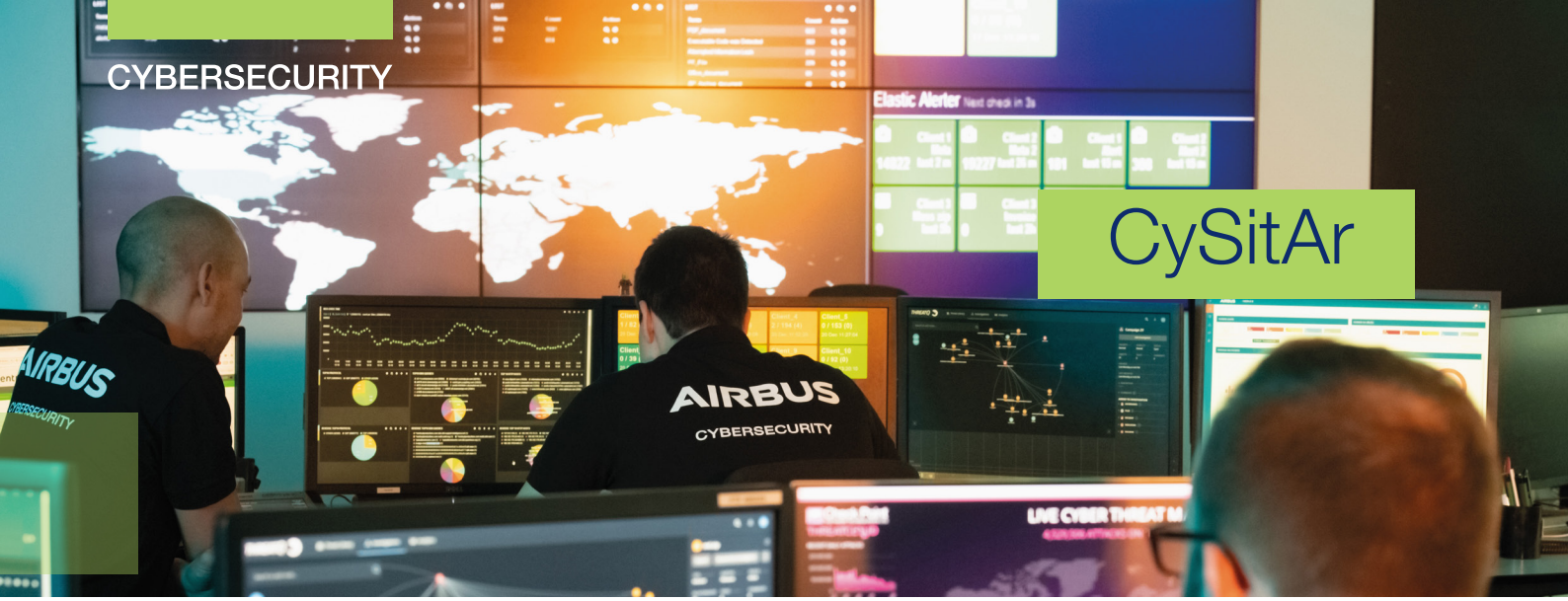
CYBERSECURITY

# CySitAr




## Cyber Situational Awareness
## Automation of Security Operations Centre (SOC) operations

### Context

- As **information systems grow increasingly complex**, cyber-attacks are becoming more sophisticated. Consequently, SOC analysts are having to carry out higher levels of investigation
- The CySitAr project aims to reduce the workload of SOC analysts as well as the costs of operations, **while improving detection by focusing on high added value tasks**


### Goal of the project

- The aim of CySitAr project is to **further automate the cyber defence cycle** by exploiting and correlating information from various sources present in the SOC
- In addition to traditional analysis techniques, CySitAr employs **Artificial Intelligence techniques**
- The use of Artificial Intelligence will automate the identification of links between extremely large databases of information, thus **saving time in the detection and investigation phases of cyber-attacks**

### 3 main challenges

There are currently 3 main issues, that impede the development and operations of a SOC:

Understanding of the defended system

Detection of adversarial behaviors

“Alert processing” part of operations

AIRBUS

## Global objectives

- **Resolve** the real operational need for the automation of the alert processing, from the initial investigation to the exchanges between the SOC and the system users
- **Strengthen** the resiliency of both the SOC and their defended organisations
- **Develop** an assistant able to advise a SOC analyst by compensating the lack of knowledge history
- **Develop** a system dedicated to the alternative detection of adversary behaviour to strengthen overall detection capabilities

## Machine learning for SOC

Case study on the **use of Machine Learning** to reduce the processing time of alerts detected by the SOC thanks to a **pre-qualification of alerts** and while **imposing constraints** such as business, timeframe, performance and maturity

The use of Machine Learning contributes to the **reduction of the workload of security analysts and enables to highlight human errors** attributed to routine processing. This project also enabled us to define the requirements (the most important is that the outputs of algorithms are accompanied by a **business context**) for the successful deployment and use of Artificial Intelligence within operations

## 3 key project results

- 50% reduction in the time taken to deal with an incident
- 80% reduction in false positives
- Reduction of investigation processing time

## About our SOCs

Thanks to our 4 SOCs in France, Germany, Spain and the UK, we provide companies, critical national infrastructure, government and defence organisations with reliable and high-performance IT/OT security services to detect, analyse and counter the most sophisticated cyber-attacks.


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**