

QUICKLY RECOVER AFTER A CYBER INCIDENT WITH OUR COMPUTER SECURITY INCIDENT RESPONSE TEAM (CSIRT)

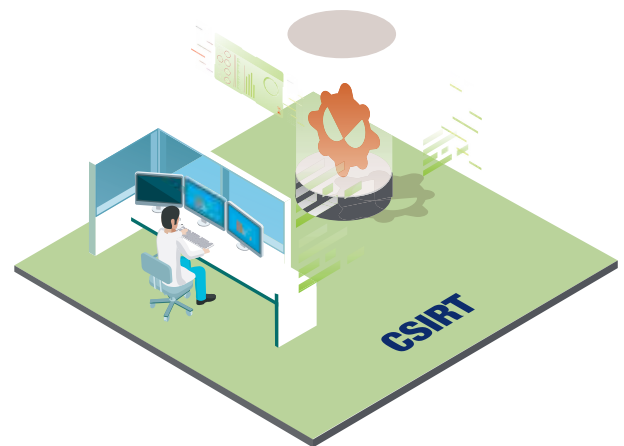
During a cyber-attack, it is important to detect and respond both quickly and appropriately - otherwise the potential impact on your organisation may grow significantly.

To ensure that these threats are contained and eradicated in a quick and efficient manner, Airbus CyberSecurity has built its own experienced Computer Security Incident Response Team (CSIRT).

Our CSIRT team applies a meticulous methodology to detect and contain the attack, before removing it from the affected system.

AIRBUS CYBERSECURITY - THE BEST CHOICE IN EUROPE FOR CYBER INCIDENT RESPONSE

- 900 specialists covering all cyber skills
- 10 years of CSIRT experience
- Trusted partner of governments, military, Airbus and Critical National Infrastructure
- 24/7 active assistance, 365 days a year



A METHODOLOGY THAT DETECTS AND CONTAINS THE ATTACK BEFORE REMOVING IT FROM THE AFFECTED SYSTEM



DIAGNOSE THE INCIDENT



ERADICATE THE PROBLEM



RECONSTRUCT SOLUTIONS



FURTHER INVESTIGATION

CSIRT 24/7

Rapid Response Team

+33 (0) 9 72 30 13 99



OUR METHODOLOGY HELPS YOU TO QUICKLY RECOVER AFTER A CYBER INCIDENT, THANKS TO THE FOLLOWING STEPS:



DIAGNOSE THE INCIDENT

- Understand the incident
- Identify compromised systems
- Survey the initial vector
- Understand the attacker's privilege level on the IT system and how it spreads
- Investigate the attacker's tools
- Identify the means of communication of the attacker
- Analyse impact of attack
- Create a timeline of the incident
- Receive a list of compromised equipment and systems, as well as a list of malicious files



ERADICATE THE PROBLEM

- Report on the removal of the problem
- Recommendations for perimeter partitioning of the compromised area
- Suggestions for adapted filtering rules
- Proposals for adapted detection rules
- Provision of markers and IOC
- Hardening recommendations
- Support throughout the process
- Advice on the potential impacts during the investigation



RECONSTRUCTION

- Deliver the information system in working order
- Reinstall infrastructure components
- Propose new security settings
- Evolution of the information system
- Remediation services
- Consultancy engagement to help implement robust cyber security policies and processes



FURTHER INVESTIGATION

- File analysis
- Program analysis
- Log analysis
- Computer analysis
- Malware analysis (propagation, possible actions, exfiltration of potential data, etc.)

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