CUSTOMER REFERENCE

AFNOR Group

72 hours to react.

AIRBUS

At a glance

Customer	AFNOR Group
Key Challenges	• Incident Response after an attack • SOC implementation
The solution	• Digital Forensics and Incident Response • SOC

The customer

The AFNOR Group is a French Association whose goal is to design solutions based on voluntary standards, sources of progress and trust. Its mission is to support organisations and individuals in spreading this trust.

The situation: threat by ransomware

In February 2021, the AFNOR Group was infected by a ransomware. Some of their files had been encrypted and most servers became inaccessible. Infection originated from a phishing email, which was sent 3 days before the attack.

The solution: Airbus Protect

Once the AFNOR Group's information system was shut down, the Association had to understand precisely what had happened, before starting to **restore its systems**.

That is when Airbus Protect was brought in to help study the traces of the attack and identify the origin of the problem. That's the first step for a Computer Security Incident Response team; **investigation**. In only three days, our CSIRT experts were able to reconstruct the entire chain of contamination.

Thanks to this, it only took **8 days for the Afnor Group to be up and running again**. Overall, it took 3 months to rebuild and deploy the whole IS. During this time, our SOC experts set up 'contingency supervision' during the response phase (a rapidly deployable SOC that allowed us to act quickly during the crisis).

In order to be sure hackers couldn't reactivate the backdoors, our experts helped the AFNOR Group to upgrade their tools and rebuild the **entire infrastructure system**. That is what we called the "hardening" phase.

How can we prevent that from happening again?

After remediation, the AFNOR Group gradually moved to a standard Airbus Protect SOC with different monitoring tools to expand the monitoring coverage and have a **new detection approach**.

Airbus Protect also recommended **raising awareness** within the AFNOR Group for several months, with phishing campaigns and password hacking campaigns. It made employees within the AFNOR Group create stronger passwords and have better reflexes regarding emails and file attachments.

A last word:

"When you face this kind of crisis for the first time, you're momentarily stunned. It was a real advantage to be able to count on a reliable partner such as Airbus Protect and have expert responders on our side to help us manage the crisis."

Jean-Marc Aubert, CISO of AFNOR Group

Bringing together outstanding expertise in safety, cybersecurity and sustainability; Airbus Protect is a European leader in risk management.

Our Cybersecurity Offerings mentioned in this case study

SOC

We protect clients from both known and unknown cyber threats. Our comprehensive end-to-end Security Operations Centres (SOC) services are delivered 24/7 from secure premises in the UK, France, Germany and Spain.

CSIRT Services

Quickly recover after a cyber incident with our Computer Security Incident Response Team.

Contact Us
protect@airbus.com

Discover more case studies on our website

www.protect.airbus.com

AIRBUS

Airbus Protect, 31700 Blagnac, France

www.protect.airbus.com