XM Cyber | Case Study

Public Sector

XM Cyber & A European Critical Infrastructure Giant: Comprehensive Visibility for Digital Transformation and Maintaining Compliance

The Challenge

For Nicola S., Head of CERT, security challenges were mounting. His team faced an overwhelming volume of security testing requests while coordinating between various departments consumed valuable resources. The organization's rapid digital transformation initiative was shifting cybersecurity controls to IT and development teams, creating new security exposures. Adding to these pressures, new regulatory requirements – particularly DORA and NIS2 – demanded stricter security measures, especially around supply chain security. Traditional point-in-time assessments were no longer sufficient to meet these evolving compliance demands.

Nicola's team needed a solution that could provide comprehensive visibility and continuous testing capabilities, while securely enabling them to continue on their path of digital transformation.

Industry:
Finance and Critical Infrastructure

CISO:
Christophe Denis

Number of Employees:
120,155 staff and
6 subsidiaries

Bio: A historic organization dating back to the 1800s, this critical infrastructure and financial provider serves one of the largest EU countries with over 120,000 employees. Their services span communications, postal savings, logistics, and financial/insurance services, making their security needs both complex and crucial.

The Solution

When evaluating security solutions, Nicola and his team prioritize tools that allow them to automate, because, as he explains, "incidents happen and we need to react quickly. Automation, particularly in incident handling, is crucial. We need to be very fast in case of an incident, so we look for solutions that allow integration with reporting, dashboarding, and security applications that we have already implemented in our infrastructure."

Another critical capability they look for is detection and continuous monitoring. Says Nicola, "these capabilities are very important. Rather than checking cybersecurity posture statically each quarter or twice a year, we need to monitor it dynamically and continuously. This allows us to track how posture changes and to correct possible configuration mistakes or implementations that may have poor security."

"We perform several tests before deciding which solution to adopt. We normally use Gartner for understanding market analysis, so we know what solutions are available….We met XM Cyber when they were still a startup, many years ago and the impression I got was that with this solution, you could have more control," recalls Nicola.

> **One of XM Cyber's main values is the ability to run tests in production without impact, which is significant because typically, testing in production is complicated and risky for business operations."**

One of their initial challenges was cloud migration. “When you start this kind of journey, one issue is visibility. We needed visibility of cloud assets, understanding of cloud activities, and security testing capabilities. The XM Cyber Exposure Management platform was able to help us deploy in the cloud very easily.. and within a few months, we had control of our cloud infrastructure, understanding what was happening, so we could start correcting our cloud posture.”

A standout feature was XM Cyber's ability to run comprehensive exposure discovery in production without operational impact, a significant advantage, given that testing in production environments typically poses considerable risks to business operations. The platform's seamless integration with existing security tools and automated incident handling capabilities aligned perfectly with their needs for continuous security monitoring.

The Results

The implementation of XM Cyber has brought immediate and significant value and Nicola’s team has seen many benefits. “To secure infrastructure, you need to understand where your assets are and how they map against your risk analysis. With XM Cyber, we achieved visibility and automation, enabling continuous validation instead of periodic tests,” says Nicola

Another benefit is that unlike classical penetration testing, which requires IT notification and whitelisting, XM Cyber can run continuously without these administrative challenges. This has led to improved efficiency, allowing the team to conduct tests continuously. “We started with cloud security and moved to identity management, which is crucial in the cloud environment, and were able to control and remediate identity issues in that environment.”

Regarding compliance with DORA and NIS2, one of the main issues they face is supply chain security – checking and controlling the security posture of the supply chain. While they are just embarking on this journey, they are exploring how to integrate the platform for better visibility into where there are exposures in their supply chain for better supply chain control.

The partnership with XM Cyber has shown itself to be especially valuable, with an emphasis on strong support and collaborative problem-solving. “Working with the team has been a journey,” reflects Nicola. “When we started, the company was very young…but we grew together. They provide strong professional support, with knowledgeable people who are flexible and understanding when issues arise. We work together to solve problems, creating a successful partnership.”

This transformation has enabled the organization to maintain robust security while advancing digital initiatives. The partnership with XM Cyber continues to evolve, supporting their ongoing digital transformation and compliance initiatives while providing the foundation for future security enhancements.

> **We are being heard and feel like there's someone to work with (on the supply chain for example). We feel like there is a good working relationship to promote that.”**

Rapid cloud infrastructure control

Continuous testing without operational disruption

Improved identity management

Enhanced visibility of security posture