Creating a Workplace Where Cybersecurity Practitioners Want to Stay

Airbus' Holistic Approach to Talent Development

Joao Moita
CISO at Airbus

"Security isn't just about IT here," explains Joao Moita, who joined Airbus as CISO less than a year ago. At Airbus, where cybersecurity forms an integral part of the business, attracting and retaining top security talent requires a unique approach. "The unique part is the strong connection between cybersecurity and safety, and the level of integration between IT, manufacturing, and product security is higher than what I've found in other industries."

Cybersecurity presents distinct challenges for an aviation and defense company that produces aircraft designed to operate for 20-30 years. Even after delivering products to customers, Airbus maintains a level of responsibility for ensuring both safety and security remain intact throughout the product lifecycle. This unique environment requires security professionals who can bridge multiple domains.

Pascale Rousset
Cybersecurity
Strategy Manager
& Cybersecurity
Community of Practice
Leader at Airbus

Crafting a Cybersecurity Blueprint

Airbus developed its own competency framework to address these specific needs, adapting established standards like the NICE Workforce Framework for Cybersecurity (NICE Framework) to the aviation industry's unique requirements. "We've gone through extensive work defining the types of profiles we expect in our security team," Moita explains. "It's really something specific to the aviation industry, looking at the business as a whole, including both military and commercial environments."

Pascale Rousset, who works in the CISO office and leads talent development initiatives, played a crucial role in creating this framework. "We created three job families and ten job profiles, integrating both the NICE Framework and ENISA requirements to better define skills at a detailed level," she explains. The Airbus framework serves as a foundation for both recruitment and professional development, providing clear pathways for career progression within the organization. Moita cites his own supervisor as an example of such progression: evolving from an engineering role designing security for the A380 aircraft to becoming the Corporate Security Officer responsible for both physical and digital security across the entire organization.

A distinctive element of Airbus' approach is the deep integration of HR in the cybersecurity function. Unlike many organizations where HR operates as a separate department, Airbus embeds an HR Business Partner directly within the security team. "Our HR Business Partner is part of the department, sitting every day with the team and attending our weekly meetings," Moita explains. "This isn't someone sitting in HR who we talk to occasionally - they're really part of the security team."

This integration yields significant benefits, particularly in recruitment and talent development. The HR Business Partner gains deep insight into the team's day-to-day operations, projects, and challenges. "When I tell our HR Business Partner we need an architect, they know exactly what an architect does," Moita notes. "They understand the profile, the mindset we expect, the interfaces, what that person does day-to-day, what kind of connections they need to have, and what kind of understanding of the business the person must have." This level of understanding enables more effective recruitment and talent development.

The Power of Community

One of Airbus' distinctive approaches to talent management is its strong emphasis on community building. The organization fosters active communities where cybersecurity professionals can share technical knowledge, discuss innovations, and connect with experts across different domains. "We organize many events around specific technical topics," Rousset explains. "Sometimes we try to share these topics with external markets and other companies as it's important to us to share knowledge." This community-driven approach extends beyond traditional security boundaries. With cybersecurity increasingly intersecting with emerging technologies like AI, these communities provide platforms for cross-functional learning and innovation.

Structured professional development programs reinforce this knowledge sharing. Airbus provides comprehensive learning paths through its security faculty that support career growth at every level. "Within Airbus, we have academies and faculties. The security faculty covers all topics regarding assets, and we propose various learning paths," Rousset explains. Employees can use a dedicated platform for learning and development to plan their career progression.

Committed to Personal Growth

Airbus takes a holistic approach to training, combining formal certifications with practical skill development. Regular technical sessions, hands-on workshops, and competitive exercises like capture-the-flag events help security professionals enhance their capabilities. Each team member receives a substantial individual training budget for pursuing advanced certifications and attending major security conferences, enabling them to stay at the forefront of their field.

Despite the risk of trained professionals being recruited by competitors, Airbus maintains a strong commitment to professional development. The organization offers comprehensive training opportunities, including certifications and various learning paths tailored to different career trajectories. "We will never cut training just because people might be pursued by other companies," Moita emphasizes. "We have a catalog of opportunities for people to develop themselves, aligned with clear expectations and competencies for different roles." This investment in people includes technical training and opportunities to move across different functions within the organization.

Creating an Attractive Environment

Rather than focusing solely on retention strategies, Airbus aims to create an environment where people want to stay. Central to this environment is a culture that equally values technical excellence and business understanding, recognizing that effective security professionals in aviation need both to succeed. The organization maintains engagement through regular community events and technical challenges, while the strong integration between HR and the security team ensures that individual growth and development remain a priority.

> **"We will never cut training just because people might be pursued by other companies."**

The effectiveness of this approach is reflected in decreasing attrition rates and the organization's ability to attract experienced professionals, even in a highly competitive market. Moita himself provides a compelling example: "I did something I always said I would never do - change companies for the same role. However, I was intrigued by the fact that at Airbus, cybersecurity isn't just a support function; it's part of our business. We also offer cybersecurity services to some of our customers, and that was the attractiveness factor for me."

As Airbus prepares its security strategy for the next three years, the organization continues to build on what makes it unique in the industry. "We need people who understand security not just in IT but in manufacturing and products as well," Moita explains. This combination of technical depth and business impact makes cybersecurity at Airbus more than just a support function—it's a crucial part of delivering safe, secure aircraft that will operate for decades to come. This reality not only attracts top talent but gives them compelling reasons to stay and grow with the organization.

This Case Study is Just the Beginning – Download the 2025 Cybersecurity Workforce Research Report for More Insights!

This case study is part of the 2025 Cybersecurity Workforce Research Report published by SANS | GIAC. Informed by international survey results, the report delivers key insights on how HR and Cybersecurity Managers can collaborate to successfully build high-performing cybersecurity teams.

Download for More Insights

SANS | GIAC CERTIFICATIONS

AIRBUS