CASE STUDY | ANA AEROPORTOS DE PORTUGAL

Strengthening Cybersecurity at ANA Aeroportos with Ethiack's Ethical Hacking

ETHIACK
autonomous ethical hacking

ANA AEROPORTOS DE PORTUGAL

About ANA

ANA Aeroportos is Portugal's leading airport operator, overseeing 10 airports crucial to the country's transportation and economic infrastructure.

João Annes, Chief Information Security Officer (CISO), leads efforts to mitigate cyber risks and ensure a safe 24/7 operation of these hubs. He had a chat with André, our CTO, to explain his unique challenges and how Ethiack has helped overcome them.

ANA faces a dual challenge: safeguarding its extensive and always-changing IT and OT (Operational Technology) environments while maintaining uninterrupted airport operations.

In 2023 alone, ANA handled more than **60 million passengers**, six times the population of the country in which it operates.

As geopolitical tensions escalate and technological advancements transform the aviation industry, ANA Aeroportos must stay ahead of increasingly sophisticated cyber threats.

Checking in on Challenges

If you work in cybersecurity, you know the threat landscape has changed drastically in the last few years. This is especially true for airports and critical infrastructures. Airports, as symbols of national power and economic importance, have become prime targets for state-sponsored attacks and hacktivists.

Since the onset of the Ukraine war in 2022, these geopolitical risks have intensified, demanding heightened vigilance. Additionally, new technologies such as biometric authentication and integrated e-commerce platforms have introduced new attack vectors, broadening the scope of potential vulnerabilities.

Operational complexity adds another layer of difficulty. ANA operates within a highly integrated ecosystem of IT and OT systems. This interplay exposes weaknesses that require comprehensive protective measures. As in other critical infrastructures, the 24/7 operational nature of airports compounds this challenge, demanding that cybersecurity efforts be robust yet unobtrusive, ensuring continuity of service while defending against persistent threats. All of this happens as passenger traffic keeps increasing year over year for their airports.

Finally, ANA must comply with the new, complex, and increasingly demanding regulations for critical infrastructures. The EU has been introducing much tighter cybersecurity laws, which only exacerbates this point.

Giving ANA a Smooth Cybersecurity Flight

Our symbiosis of Continuous AI Pentesting and Elite Human Ethical Hacking caught ANA's eyes, matching perfectly with their need for 24/7 operationability:

1. **Continuous Penetration Testing:** Ethiack's AI-powered platform provides 24/7 automated penetration testing to identify vulnerabilities in ANA's external attack surface. This is useful to quickly respond to new CVEs or when new components are added to their attack surface. Unlike traditional biannual pen tests, this approach ensured ANA could respond to threats in real-time.

2. **Human-Driven Ethical Hacking Events:** Ethiack's elite ethical hackers conducted in-depth manual testing of ANA's internal systems. These human events uncovered nuanced vulnerabilities missed by automated tools and enhanced the cybersecurity awareness of ANA's IT and OT teams through hands-on collaboration.

3. **Attack Surface Management:** Ethiack's ASM tools mapped ANA's digital infrastructure, identifying unknown assets and changes in real-time. This proactive approach minimized ANA's exposure to potential threats.

4. **High-Impact Vulnerability Identification:** Ethiack's automated testing modules prioritized vulnerabilities with the greatest business impact. With false-positives below 0.5%, ANA's security team could focus on actionable threats, reducing noise and optimizing resources.

Using Elite Ethical Hacking to Protect Thousands of Flights

João highlighted the frequent use of Elite Ethical Hacking events, which he mentions are essential for their security strategy. Sometimes lasting for a whole week, our ethical hackers get the opportunity to find the most critical vulnerabilities by exploiting business logic and attack vectors often untouched by automated tools.

João highlights how these events also become learning opportunities for his team, as they learn from our approach to strengthen their systems. By adopting Ethiack's ethical hacker mindset, ANA's internal teams understood potential abuse scenarios and ended up with:

1. **Enhanced Cyber Resilience:** Ethiack's continuous testing approach ensured ANA's digital infrastructure was consistently monitored and fortified, reducing the window of exposure for emerging threats.
2. **Operational Insights:** Collaboration during ethical hacking events equipped ANA's teams with the skills to identify and mitigate risks proactively.
3. **Cost-Effective Security Optimizations:** Ethiack's platform streamlined vulnerability management by automating triage and prioritization, enabling ANA to allocate resources effectively while maintaining compliance.
4. **Future-Proofing Against Threats:** Ethiack's adaptable AI-driven tools are aligned with ANA's need for continuous evolution in the face of rapidly changing cyber risks.

Until The Next Flight

Ethiack's partnership with ANA Aeroportos demonstrates the great power of combining AI Continuous Pentesting and Elite Ethical Hacking. By addressing vulnerabilities in real-time and equipping internal teams with attacker mindsets, Ethiack ensures its clients are not just protected but prepared for the challenges ahead.

For ANA Aeroportos, this collaboration with Ethiack marks a pivotal step in fortifying their operations against the complex cyber threats of the modern world.

Watch the full video case study here.

Ethiack's combination of automated testing and human expertise brought a unique perspective to our security challenges. Their continuous monitoring of our attack surface and in-depth manual testing of our internal systems have transformed how we approach cybersecurity. Ethiack teaches us to think like attackers, making us better equipped to handle threats proactively.

- João Annes, Chief Information Security Officer at ANA Airports

Autonomous Ethical Hacking

ethiack.com