The National Institute of Aerospace Technology

At a Glance

- Quick and easy to deploy
- Relieved pressure on security team with automated investigations
- Security team have full control and oversight via the Mobile App

The National Institute of Aerospace Technology (INTA) is a public research organization that works with the Spanish Ministry of Defense. It carries out research in the fields of aerospace, aeronautics, hydrodynamics, security, and defense technologies. INTA provides technological services to companies in these industries, as well as universities and other institutions.

Adapting to fast-moving change

INTA has a corporate network distributed with 15 centers throughout Spain (technology campuses, test centers and space stations). This infrastructure is managed by its IT team from its central offices in Madrid.

In recent years, INTA has undergone rapid digital transformation. Increased collaboration with other organizations (both in the public and private sector) has led to more technological integration, and this has introduced new security risks. INTA looked for a technology that could provide real-time monitoring across the digital estate, clearly alerting its security team to emerging cyber-threats.

In addition, a move to more flexible and hybrid working patterns placed a greater emphasis on endpoint protection, and the new digital work environment has considerably increased the number of services required in the cloud. The organization now relies on a series of cloud platforms including Microsoft Azure AD, Zoom, Microsoft Teams, and Webex to carry out its daily operations, and it sought a security platform that could give unified protection across the whole business.

> "In a matter of days, the AI really understood our way of working and became very effective."
>
> Jesús Garrido, CIO, INTA

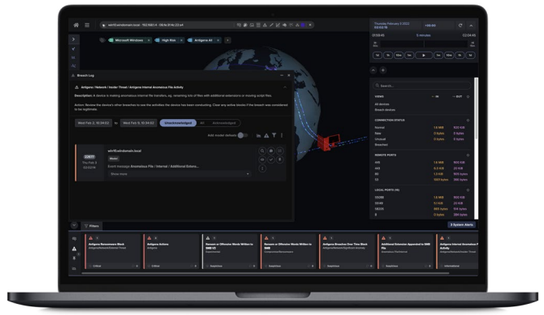
The National Institute of Aerospace Technology

The principal security challenges

The organization was aware of the increasingly hostile threat landscape as the cyber-crime industry grew and became more professional, with Jesús Garrido, CIO at INTA, noting how low-and-slow attacks and data exfiltration were a particular concern. "We hold a lot of valuable IP in the areas of aerospace, defense and security research, which makes us more vulnerable to hackers looking to steal information".

The multiplication of attack vectors created the need for more robust security, but the team wanted to ensure this didn't come at the cost of flexibility and productivity. They needed a solution that would allow it to increase its functionalities and respond to the needs of its clients, while providing strong protection from cyber-attacks.

It also wanted this solution to alleviate the workloads of its increasingly stretched security team, rather than add to the burden. To this end, it sought a technology that didn't overload users with false positives but generated meaningful and actionable insights on emerging security threats.



Darktrace's findings and autonomous actions are shown in the Threat Visualizer

> "The system learns completely autonomously, and investigation takes just seconds and a few clicks."
>
> Jesús Garrido, CIO, INTA

Finding the right technology

INTA trialed Darktrace alongside a number of other solutions in a rigorous bake-off procedure. Multiple tests were carried out with each of the products. "We carried out several penetration tests, and these were picked up by Darktrace within minutes of execution," recalls Garrido. In the end, the company opted for Darktrace due to the visibility it provided across the digital estate, the simplicity of use, and the useful and practical output of the AI.

"The installation process was simple," Garrido says. "In just a few hours, the product was learning from our data, and after some very light fine-tuning – performed with the assistance of Darktrace's engineers – in a matter of days, the AI really understood our way of working and became very effective. It started generating alerts that were really useful and relevant."

Darktrace's intuitive user interface and self-learning approach greatly relieved pressure on the security team, ultimately giving them back several hours in their day. "The system learns completely autonomously, and regardless of whether we're accessing Darktrace from desktop or mobile, investigation takes just seconds and a few mouse clicks," comments Garrido.

A crucial aspect of Darktrace that helped in this regard was the Cyber AI Analyst, which investigates on Darktrace's alerts in the background, and performs the first level of triaging, stitching together individual security events into an overarching security incident and generating incident summaries of only the most prominent threats to the organization.

The team have benefitted greatly from being able to manage the security of the organization around-the-clock, anywhere in the world. Garrido even recalls swiftly remediating an ongoing security incident in real time whilst at the cinema. "We have all the necessary information at our fingertips with the Darktrace Mobile App," he says.

The organization is now exploring extending Darktrace's coverage to the email layer. Having trialed Antigena Email, the team were impressed with its ability to respond to sophisticated email threats that other tools let through and are looking to implement AI in this critical area.