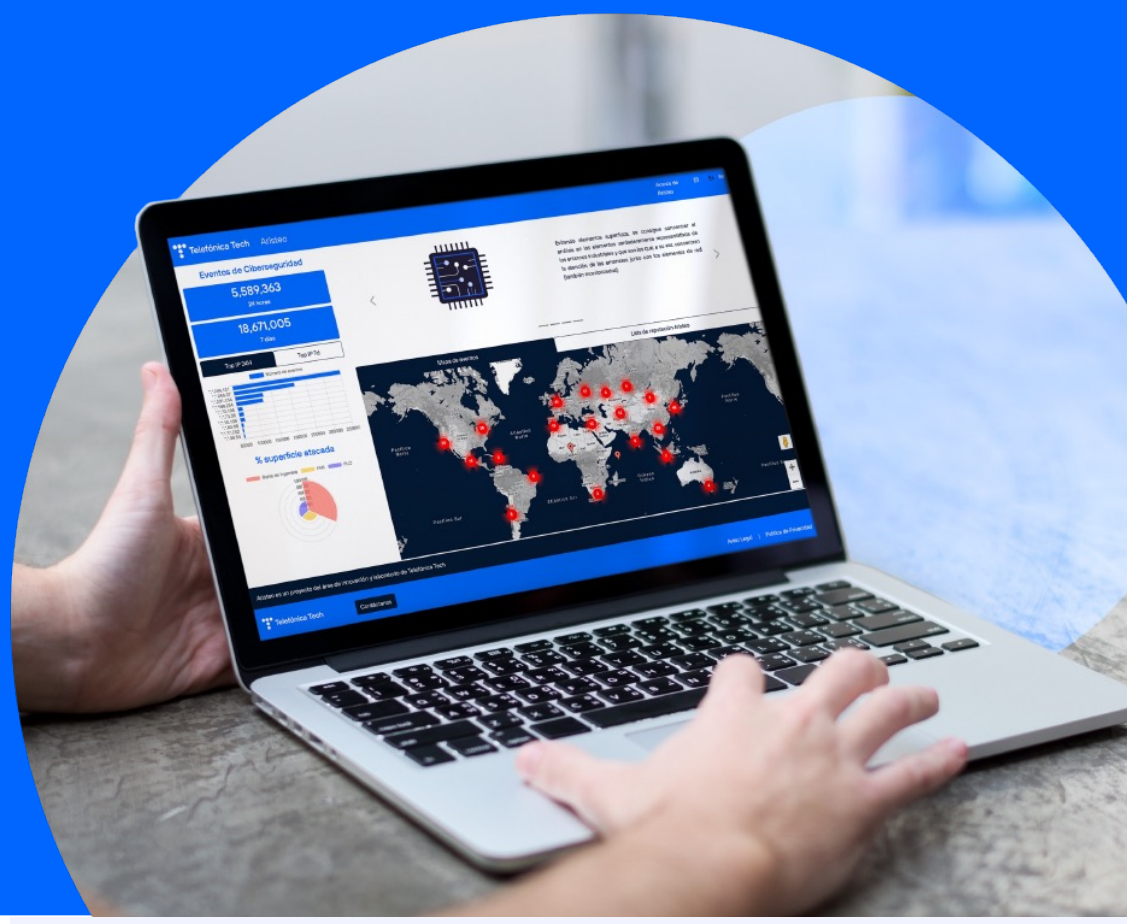
Telefónica Tech

DIGITAL OPERATIONS CENTER

Aristeo

Telefónica Tech's OT network for the capture and predictive analysis of threats, a generator of intelligence with differential value.

OT & IoT | Threat Intelligence | IA | Deception



ABOUT THE SOLUTIONS

Aristeo's deployment of its decoys with real industrial hardware **allows it to catch threats that other systems do not identify**. In this case, a customer's employee logged on to a website that was blocked by the company's security systems. The customer asked us for more information. Aristeo had detected that this machine had been attacking their decoys for a month.

None of the world's leading Threat Intelligence engines had identified this threat.

WHAT THEY SAY ABOUT ARISTEO

"Any threat can bring your business to a halt. It is important to have solutions that reinforce security systems with quality information. Aristeo finds threats fast and helps us protect ourselves."

PROYECT OBJECTIVES

Telefónica Tech's DOC required **a reliable and quality source to reinforce its customers' perimeter security systems** using **threat information from industrial environments**. Aristeo's capacity as a source of information was used to load the indicators of attack and compromise in these perimeter systems, identifying a new threat that appeared to be a legitimate service.

RESULTS

- Aristeo captures threats on real systems and not on virtualised systems. This means that analysis on them generates quality intelligence on industrial threats. **The attacker is unable to distinguish that it is not in a real environment, so it deploys its best tricks, while Aristeo learns everything from them**. This value is absolutely differential for a security team in charge of so many customers, such as Telefónica Tech's DOC.
- Aristeo also manages, on average, to **identify threats** (16% of all threats detected) **8 to 12 days earlier** than the leading intelligence engines on the market.