Ciberseguridad & NaaS

Telefónica Tech

MISSION CRITICAL SOC

We support you on your journey towards business resilience

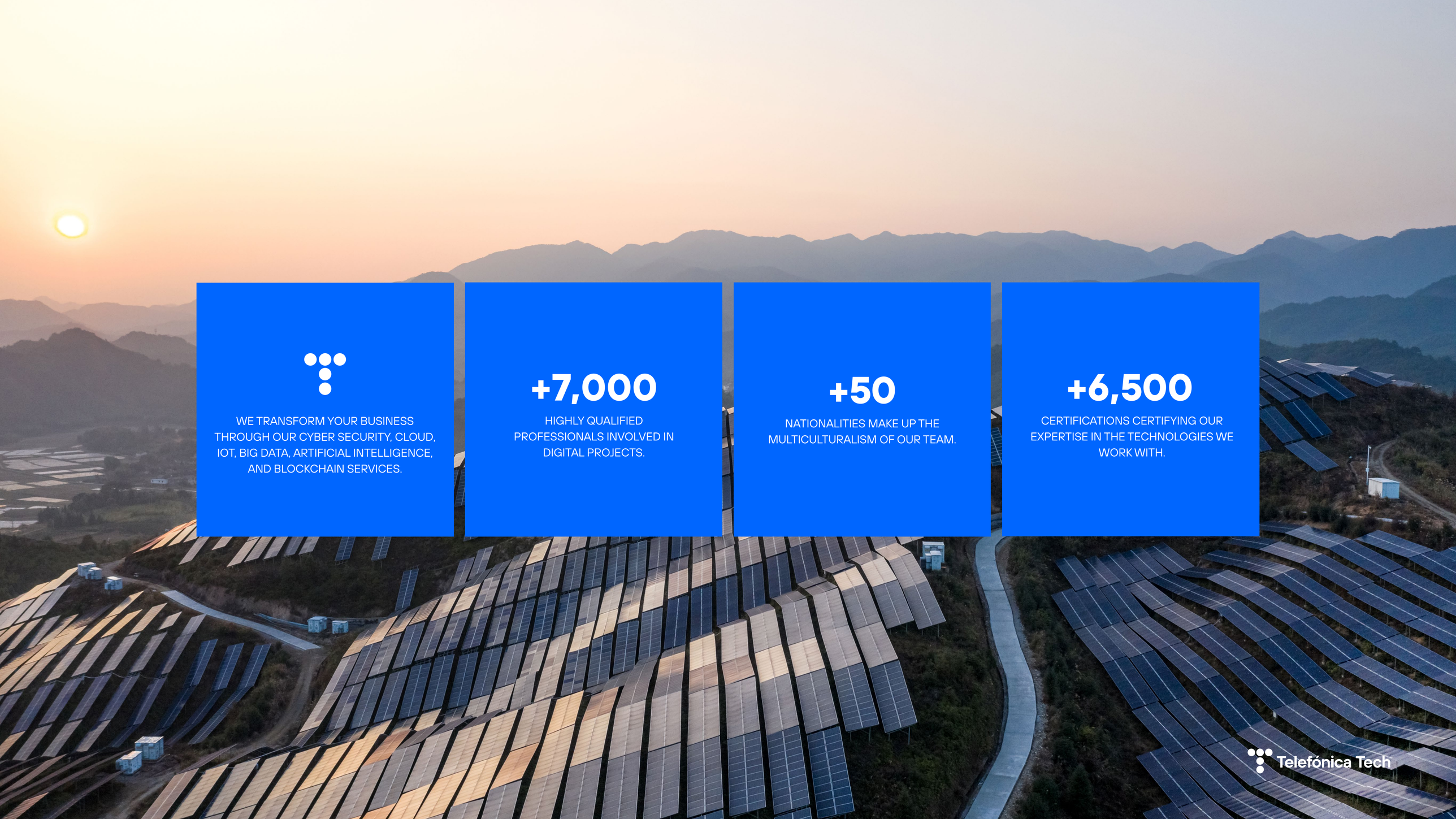
telefonicatech.com

Telefónica Tech

Telefónica Tech's **Mission Critical SOC**

Telefónica Tech's **Mission Critical SOC** proposal is designed to protect critical environments by integrating OT and IoT technologies and an end-to-end approach that involves people, processes, and tools. It acts as a specialized operations center (SOC) to monitor, detect, analyze, and respond to cyber threats in cyber-physical systems and critical infrastructures. It also reinforces cyber resilience with a formula based on understanding risk, protecting assets, and establishing detection, response, and recovery capabilities.

TELEFONICATECH.COM



WE TRANSFORM YOUR BUSINESS THROUGH OUR CYBER SECURITY, CLOUD, IOT, BIG DATA, ARTIFICIAL INTELLIGENCE, AND BLOCKCHAIN SERVICES.

+7,000

HIGHLY QUALIFIED PROFESSIONALS INVOLVED IN DIGITAL PROJECTS.

+50

NATIONALITIES MAKE UP THE MULTICULTURALISM OF OUR TEAM.

+6,500

CERTIFICATIONS CERTIFYING OUR EXPERTISE IN THE TECHNOLOGIES WE WORK WITH.

Telefónica Tech

¿Who is Telefónica Tech in Mission Critical SOC?

"We offer a managed Cyber Security solution designed to protect critical infrastructure and cyber-physical environments, integrating 24/7 monitoring, advanced detection, incident response, and OT/IoT regulatory compliance."

+30

PROFESSIONALS

DEDICATED EXCLUSIVELY TO CYBER SECURITY OT & IOT

1

DOC

WITH TWO GEOGRAPHICAL LOCATIONS WITH PROFESSIONALS SPECIALIZING IN CYBER SECURITY OPERATIONS OT

+15

SECTORS

FROM ENERGY, HYDROCARBONS AND PAPER, TO HOSPITALS, PORTS, AND THEME PARKS

+80

CERTIFICATIONS IN CYBER SECURITY

STANDARDS SUCH AS IEC 62443 AND TECHNOLOGIES FROM LEADING VENDORS LIKE FORTINET NSE OT, TXONE, CISCO, NOZOMI NETWORKS, AND CLAROTY

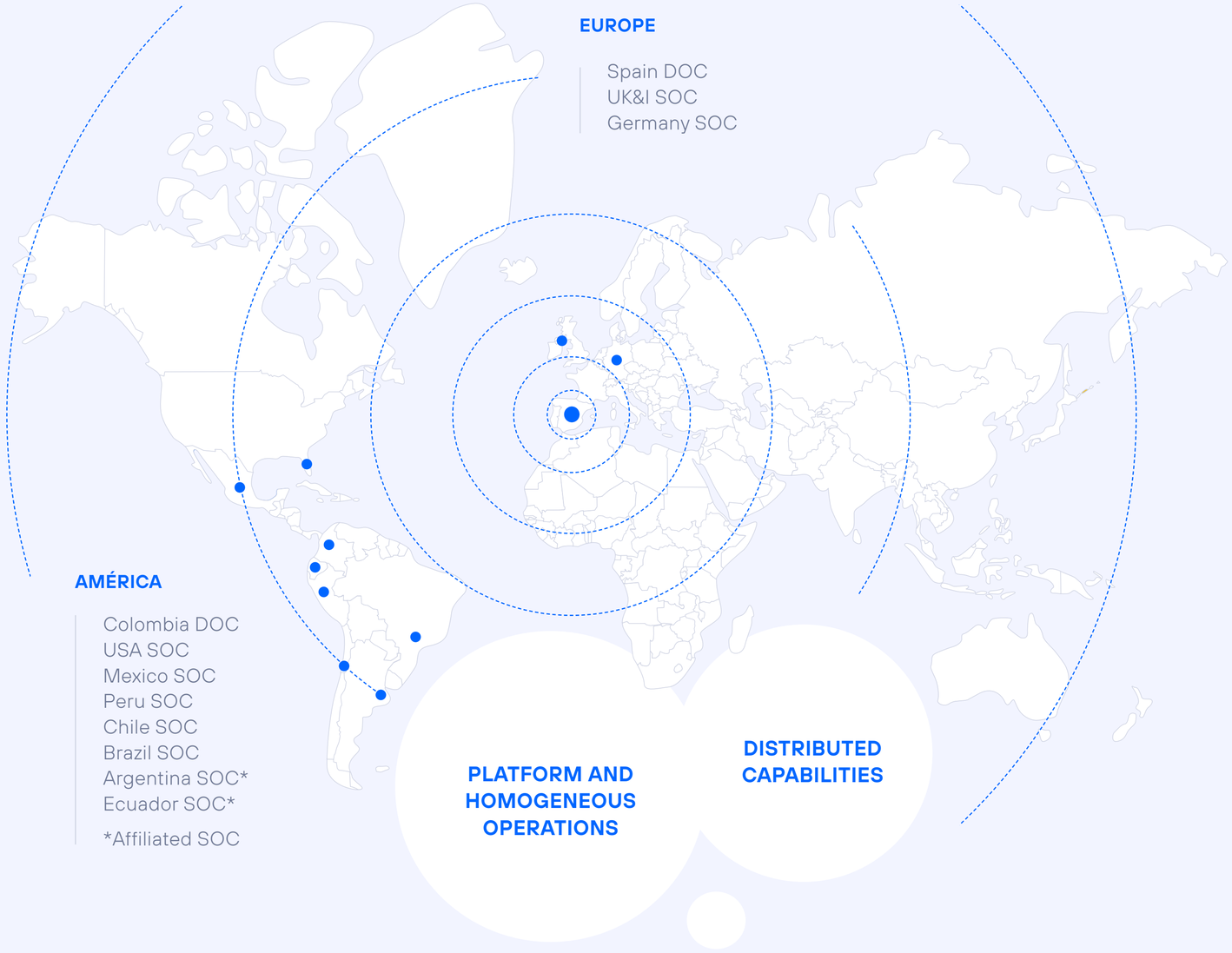
- **+100k** MONITORED OT DEVICES
- **+10** ACTIVE TECHNICAL OFFICES
- **+340** OT MONITORING DEVICES IMPLEMENTED OVER THE LAST YEAR
- **3** LEADING INTEGRATED OT PLATFORMS FOR TOTAL VISIBILITY AND DETECTION
- **~60** INDUSTRIAL SECURITY ASSESSMENTS

Telefónica Tech

One Digital Operations Center (DOC) with two geographic locations and 11 SOCs around the world

Developing the best end-to-end capabilities in Cyber Security and cloud operations.

- GLOBAL REACH AND LOCAL PRESENCE
- 24/7/365 SECURITY PROFESSIONALS THAT ARE ALWAYS READY
- MULTIDISCIPLINARY TEAM
- SYNERGIES FOR A BETTER CUSTOMER EXPERIENCE
- THE BEST PLATFORMS AND INFRASTRUCTURES
- INTEGRATED VIEW WITH SINGLE POINT OF CONTACT



Telefónica Tech

Ciberseguridad & NaaS

Mission Critical SOC

We increase the resilience of your critical infrastructures with advanced Cyber Security, offering customized solutions to detect, respond to, and recover from threats in industrial OT and IoT environments.

Telefónica Tech

Industrial Cyber Security Assessment

DISCOVER MORE ON OUR WEBSITE

We assess Cyber Security in OT environments using the ISA/IEC 62443 standard as a reference. It combines analysis of the documentation provided by the organization with a technical assessment based on analysis of captured network traffic. A compliance assessment can also be carried out regarding applicable regulations, such as ISA/IEC 62443 or other industry-specific standards (e.g., NERC for energy, LPIC for critical infrastructure). Ethical hacking activities are also included to assess the security level of infrastructures.

ABOUT THE SERVICE

The service allows the Cyber Security level of OT environments to be assessed, using the ISA/IEC 62443 standard as the main reference. This assessment is carried out by combining the analysis of information and documentation provided by the organization with a technical assessment based on the analysis of network traffic captured in these environments.

An assessment of regulatory compliance with ISA/IEC 62443 or other standards applicable to the sector in question (e.g., NERC for the energy sector, LPIC for critical infrastructure) can also be provided. Ethical hacking activities are also included to assess the security level of the infrastructure.

WHAT DOES IT ALLOW?

- To have visibility of operational environments (assets, communications architecture) and knowledge of their security level.
- To have a proposal for architecture and security solutions.
- To define an industrial Cyber Security master plan to establish a roadmap for the implementation of solutions.

BENEFITS

Activity report

Our team is responsible for preparing and presenting a report summarizing the activities carried out, Cyber Security findings, and recommendations for improvement.

Proposed recommended solutions

The catalog of existing products and services complements the solution by offering specific proposals for implementing the actions identified in the master plan.

Security master plan

As a complement to the report, it is possible to extend the activity by developing a security master plan that allows you to draw up a roadmap for the implementation of Cyber Security solutions and achieve the established security levels by defining milestones that help to monitor progress.

OT & IT Segregation & Segmentation

DISCOVER MORE ON OUR WEBSITE

A solution based on the design and implementation of a network architecture that allows IT and OT environments to be segregated and OT environment networks to be segmented, complemented by additional technologies to advance the application of ZeroTrust models.

ABOUT THE SERVICE

Telefónica Tech's value proposition in IT/OT segregation and OT segmentation for industry lies in its ability to offer a comprehensive, customized solution that ensures the integrity, availability, and confidentiality of industrial systems.

WHAT DOES IT ALLOW?

- To isolate critical OT networks: ensure that networks controlling production processes are completely separated from IT networks, thereby reducing the attack surface and protecting industrial control systems (ICS) from potential cyberattacks.
- To control and monitor network traffic: to enable detailed monitoring and control of traffic between different segments of the OT network, ensuring that only necessary and authorized communications take place, thereby limiting the risks of lateral movement of threats within the network.
- Optimizing security and performance: maintaining the balance between security and operational efficiency, allowing the plant to continue operating smoothly while minimizing Cyber Security risks.

BENEFITS

Protection against advanced cyberattacks

The risk of a cyberattack compromising critical production systems is significantly reduced by segmenting the OT network. This is vital in an environment where disruption to the production process can lead to significant financial losses.

Regulatory compliance

Comply with Cyber Security regulations specific to the automotive sector, facilitating audits and improving trust among customers and business partners.

Improved operational resilience

A well segmented network means that an incident in one segment does not affect the entire plant, enabling rapid containment and recovery while keeping most operations running without interruption.

Enhanced visibility and control

Log collection and analysis, reporting, and graphical representations provide a clear and detailed understanding of system status, enabling organizations to make informed and strategic decisions.

OT & IoT Security Monitoring

DISCOVER MORE ON OUR WEBSITE

A comprehensive solution for gaining visibility into assets and detecting threats through traffic analysis, offered as a managed service by Telefónica Tech as part of a SOC specializing in industrial and healthcare environments

ABOUT THE SERVICE

The service is operated from our DOC and SOCs, managing both security and health alerts for probes. Security alerts may be related to threats to customer assets, anomalies in process variables, or asset vulnerabilities. In addition, assets connected to the network are displayed, providing great visibility of the environment.

The customer receives all this information periodically in the reports provided to them, as well as real-time alerts in the event of serious incidents.

WHAT DOES IT ALLOW?

- To gain visibility into the assets connected to the monitored network and their vulnerabilities.
- Enrichment of asset inventory through automatic asset tagging and alerts to improve risk management with proprietary tool (Telefónica Custom Tag*).
- To detect security threats in the environment, as well as any anomalies that occur both at the security level and in relation to process variables.
- To monitor the Cyber Security of private cellular networks (4G and 5G) using technologies specific to these environments.
- To have a team of experts who manage alerts and provide real-time notifications of serious incidents.

BENEFITS

Visibility and risk mitigation with minimal impact on the network

The service identifies assets connected to industrial networks and detects security threats. All this is done by analyzing a copy of the traffic, avoiding network disruptions.

Detection of OT & IoT sector-specific attacks

The threat database is regularly updated with industry-specific feeds. Detection capabilities also include anomalies in process variables.

Reaction capability

Enriched reports and real-time notifications to respond effectively to cyber threats.

Managed service

Customers can delegate service management to our experts, who operate the service 24/7. Serious incidents are reported quickly, and weekly reports are sent with information on assets and threats, as well as a monthly risk report.

OT EDR

DISCOVER MORE ON OUR WEBSITE

Comprehensive and advanced protection for industrial OT environments, with an emphasis on operational continuity. They protect all components and communications within the system by implementing the Zero Trust model, thereby mitigating risks without interfering with ongoing operations. They also offer implementation, support, maintenance, and technology management services. A 360° service.

ABOUT THE SERVICE

Telefónica Tech focuses on offering comprehensive and advanced protection for industrial OT environments, with an emphasis on operational continuity. It uses a robust model that secures every component and communication within the system, thereby mitigating risks without interfering with ongoing operations. It also provides implementation, support, maintenance, and technology operation services.

WHAT DOES IT ALLOW?

It enables industrial companies to ensure operational continuity by offering comprehensive and advanced protection for their Operational Technology (OT) environments, securing every component and communication in the system, which helps mitigate risks without interrupting operations. We also provide technology implementation, support, maintenance, and operation services, ensuring efficient and secure management of your systems.

BENEFITS

Performance and availability optimization

Proactive implementation, maintenance, and updating of hardware and software ensure that devices operate optimally, reducing downtime and improving operational efficiency.

Efficient incident management and updates

Technical issues are quickly identified and resolved through reactive and proactive support and ongoing maintenance, minimizing disruptions and maximizing business continuity.

Security and compliance

Specialized support services and proactive operation ensure that systems are always protected against new threats, comply with security regulations, and maintain information integrity.

Enhanced visibility and control

Log collection and analysis, reporting, and graphical representations provide a clear and detailed understanding of system status, enabling organizations to make informed and strategic decisions.

Aristeo – Deception as a Service

DISCOVER MORE ON OUR WEBSITE

Deception technology substantially improves detection mechanisms through early detection of malicious activity and better understanding of cybercriminals.

ABOUT THE SERVICE

Our DaaS platform integrates two types of solutions: one is the Aristeo advanced cyber intelligence platform (patented and developed entirely by Telefónica TECH's Innovation department) that uses real industrial hardware. The second is third-party systems and appliances that are market leaders in the development of deception cases.

The integration of the two technologies ensures the authenticity and accuracy of threat information. We offer a joint, innovative, and distinctive solution designed to adapt to the specific needs of each customer, allowing the configuration of decoys to represent any industrial process or productive sector.

WHAT DOES IT ALLOW?

- **Capture and predictive analysis:** Creation of industrial decoys to attract attackers in order to analyze their tactics and predict threats.
- **Realistic simulation:** Interaction with real decoys to better capture threat behavior.
- **Predictive intelligence:** Pattern detection to anticipate attacks and protect critical assets.
- **Integration with existing defense:** Works with SIEM and TIP managed by our own SOC or the customer's SOC.
- **Operational continuity:** Operating without altering the infrastructure or interrupting operations.
- **Customized reports:** Generate detailed analyses to improve security according to your needs.

BENEFITS

Advanced threat detection

Early identification of advanced threats, including APT (Advanced Persistent Threats) groups and unknown vulnerabilities (0-day).

Predictive intelligence

Continuous analysis of threats to anticipate potential attacks and strengthen security.

Adaptability and flexibility

Ability to adapt to the customer's specific infrastructure and processes, without taking up space in their infrastructure or facilities in the case of physical decoys, although the service is also available on premises.

Constant protection

Our DaaS solution operates 24/7, providing continuous monitoring and real-time updates on new threats.

Regulatory compliance support

DaaS supports regulatory compliance by providing a testing environment to ensure security measures meet industry standards and protect against current and emerging threats.

Telefónica Tech

Ready to transform your business?

Telefónica Tech is the leading company in digital transformation. It has a wide range of services and integrated technological solutions in Cyber Security and NaaS, Hybrid Cloud, Connectivity and IoT, AI & Data, Future Workplace, Business Apps and Consulting and Professional Services.

telefonicatech.com