

IOT & OT SECURITY

IoT & OT Security Monitoring

HOW CAN TELEFÓNICA TECH HELP?

We help you gain visibility over network-connected assets. We manage alerts related to vulnerabilities, security threats and anomalies arising in the OT and IoT environment.

The current trend of convergence of IT and OT/IoT networks poses several security challenges. The first challenge is to have **visibility over the devices connected to the network and their vulnerabilities**, as what cannot be seen cannot be protected. A second challenge is to **identify any threat or anomaly** that could affect the ecosystem and alert about it.

To this end, **Telefónica Tech offers specialised OT&IoT technologies as well as a team of experts who operate the service from the SOC (present in 12 locations).** The analysts **alert the customer in real time** about important threats and a series of **regular reports** are made available in order to have all the information about what is happening in the network.

WHO IS THIS SERVICE FOR?



Companies making use of operational technologies (OT) and the Internet of Things (IoT), such as energy, manufacturing, water management, food and beverage, chemical, pharmaceutical, building automation, railways, oil and gas, transportation, mining, automotive, etc.



Companies that wish to delegate the operation of the monitoring service, benefiting from the experience of the Telefónica Tech Cyber Security & Cloud SOC and receiving alerts and reports on everything that happens on their network.



Medical and healthcare companies and public bodies interested in monitoring the safety of their environments.

OUR VALUE PROPOSITION

Our service

The service is operated from our SOC, managing both security and probe health alerts. Security alerts can be related to threats to customer assets, anomalies in process variables or asset vulnerabilities. The assets connected to the network are also displayed, providing high visibility of the environment. The customer receives all this information on a regular basis in the reports provided, as well as real-time alerts in the event of serious incidents.

In addition, probes are deployed in the customer's infrastructure, which passively analyse traffic and are able to understand most industrial and IoT protocols.

What does it allow you to do?

This service will allow you to:

- › **Have visibility of the assets** connected to the monitored network and their vulnerabilities.
- › **Have a team of experts to manage alerts and warn in real time of serious incidents.**
- › **Detect security threats in the environment**, as well as anomalies that occur both at the security level and in relation to process variables.

Benefits

Visibility and risk mitigation with minimal network impact

The service identifies assets connected to industrial networks and detects security threats. This is done by analysing a copy of the traffic, avoiding network disruptions. We significantly simplify deployment because it does not rely on agents to be installed on the devices.

OT&IoT industry-specific attack detection

The threat database is regularly updated with industry-specific feeds. In addition, detection capabilities include anomalies in process variables.

Managed service

The customer can delegate the management of the service, relying on the expertise of our specialists who operate the service 24/7. Serious incidents are reported promptly and weekly reports are sent with asset and threat information, as well as a monthly risk report.

Responsiveness

Rich reporting and real-time notifications to effectively respond to cyberthreats.

Telefónica Tech's differential value



Integration with SOC tools and workflows optimised through automation, enabling effective and efficient use of technology, focusing on the most relevant customer events and streamlining their processing.



Security alerts and reports with remediation recommendations, making incident response easier and risk management more effective.



Global scalability to protect distributed locations, with dedicated service experts located in different geographical locations.

EQUIPMENT, TEAMS AND ACHIEVEMENTS

Our team

- › **+100** million of security events tracked globally each year.
- › **+1.800** SecOps employees.
- › **+1.500** security certifications.
- › **+12** types of certifications specific to the OT sector.

Achievements

- › **Industrialised and replicable** service in different geographical locations.
- › **Nozomi MSSP Elite** certifications
- › **+ 40** probes in projects with real customers.

BUSINESS MODEL

After an analysis of the client's network, the number of probes to be installed in its infrastructure, the model and their location are established. The service **includes the necessary hardware and software**, as well as deployment and configuration.

Telefónica Tech Cyber Security & Cloud's SOC experts operate the service so that you don't have to worry about anything at all, and it can be contracted on **a monthly subscription basis**.

RELATED PARTNERS



| RELATED SERVICES

OT&IoT Security Professional Services

Our experts will assist you in the development of industrial cyber security master plans, regulatory compliance analysis (e.g. 62443), technical consultancy and penetration testing including robot security assessment.



Perimeter Protection

A solution based on the design and implementation of a network architecture that allows the segregation of IT and OT environments as well as network segmentation of the OT environment, complemented by additional technologies to advance the application of ZeroTrust models.

flexSITE

A solution that integrates SD-Branch services (WiFi & LAN, secure SD-WAN) for the end-to-end of your business network.



Contact us to start the digital transformation of your organization.

