MISSION CRITICAL SOC

OT&IoT 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 occurring in the OT and IoT environment.

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

For this purpose, Telefónica Tech offers specialized OT & IoT technologies as well as a team of experts who operate the service from our global network of SOCs. Analysts **alert the customer in real time** about important threats and a **series of periodic reports** are made available to the customer in order to have all the information about what is happening in the network.

WHO IS THIS SERVICE FOR

Companies that make use of operating technologies (OT) and Internet of Things (IoT), such as energy, manufacturing, water management, food and beverage, chemical, pharmaceutical, building automation, railroads, oil and gas, transportation, mining, automotive, etc.

Companies that want to delegate the operation of the monitoring service, benefiting from the experience of Telefónica Tech's SOCs and receiving alerts and reports on everything that happens in their network.

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

OUR VALUE PROPOSITION

Our service

The service is operated from our SOCs, managing both security and probe health alerts. Security alerts can be related to threats to customer assets, anomalies in process variables or asset vulnerabilities. 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 case of serious incidents.

Probes are additionally deployed in the customer's infrastructure, which passively analyze 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 over the assets** connected to the monitored network and their vulnerabilities.

› **Detect security threats in the environment,** as well as anomalies that occur both at the security level and in relation to process variables.

› **Monitor the cybersecurity of private cellular networks (4G and 5G)** using technologies specific to these environments.

› **Having a team of experts to manage alerts and warn in real time of serious incidents.**

Benefits

Visibility and risk mitigation with minimal network impact.

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. We significantly simplify deployment because it does not rely on agents to be installed on the devices.

Managed Service

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

Detection of OT & IoT industry-specific attacks.

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

Responsiveness

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

Telefónica Tech's differential value

Integration with SOCs' tools and workflows optimized through automation, allowing for 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 geographies.

EQUIPMENT, TEAMS, AND ACHIEVEMENTS

Our teams

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

Achievements

- **Industrialized and replicable** service in different geographies.
- **Nozomi MSSP Elite** certification
- **+ 40** probes in projects with real customers.

BUSINESS MODEL

After an analysis of the customer'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's global network of SOCs experts operate the service so you do not worry about anything. The service can be contracted on a **monthly subscription basis.**

RELATED PARTNERS

NOZOMI NETWORKS

GARLAND TECHNOLOGY
See every bit, byte, and packet®

RELATED SERVICES

Industrial Cyber Security Assessment

The service evaluates cyber security in OT environments using the ISA/IEC 62443 standard as a reference. It combines the analysis of documentation provided by the organization with a technical assessment based on the analysis of captured network traffic. A compliance assessment with respect to applicable regulations, such as ISA/IEC 62443 or other industry-specific standards (e.g. NERC for energy, LPIC for critical infrastructure) can also be performed. Additionally, it includes ethical hacking activities to assess the security level of infrastructures.

Cloud WiFi/SD-LAN

Optimize the service with integrated connectivity at your site, creating an SD-Branch solution governed by the same policies across the network and managed from a single dashboard

OT & IT Segregation and OT Segmentation

A solution based on the design and implementation of a network architecture that allows segregating IT and OT environments as well as segmenting OT environment networks, complemented with additional technologies to drive the application of Zero Trust models.

Contact us to start the digital transformation of your organization.