

NETWORK SECURITY &amp; SECURITY MANAGEMENT

# ● Network Detection & Response

HOW CAN TELEFÓNICA TECH HELP?

Detects and identifies anomalous behaviour, defending the company against advanced threats and contributing to a more efficient security posture.

Traditional security solutions do not properly address the need for detection and response to fundamental threats such as internal or unknown threats.

Modern architectures with a greater number of systems and users emphasise the need to analyse behaviour not only in north-south traffic, but also in east-west traffic, in order to identify threats that other security controls cannot detect.

Our solution drastically reduces detection and containment times and provides complete visibility of traffic in hybrid environments.

Thanks to the support of SOC experts, the protection of critical assets is reinforced, thereby strengthening the resilience of the customer's business.

## WHO IS THIS SERVICE FOR?



Companies with distributed or hybrid networks, and which have users and partners working remotely in a mixed face-to-face model. These are companies that need complete visibility of traffic to detect internal or lateral threats that other controls do not cover.



Organisations with critical or highly exposed assets, such as those in the financial, healthcare, defence or public administration sectors, have a particular need to detect advanced threats (APTs, C2 or exfiltrations).



Companies with OT, IoT, or ICS environments where there are many agentless or EDR-less devices and where network segmentation is more complex. An NDR solution provides visibility and detects anomalous behaviour.

## OUR VALUE PROPOSITION

**Our service**

Our managed Network Detection & Response service is key to analysing network traffic in real time using AI and behavioural analysis to detect, investigate and contain threats that other controls do not cover.

- Full network coverage via SPAN or TAP.
- Advanced packet analysis of traffic to extract key metrics.
- Ingests all types of traffic using protocol-agnostic artificial intelligence.
- Understands key metadata from all sources. Does not require packet content decryption.
- Advanced solution management by security experts for maximum performance.

**What does it allow you to do?**

Our service allows you to enjoy a 100% managed NDR solution for optimal performance:

- Supply and installation: Teams of experts for the supply and installation of security technologies.
- Maintenance: Contract management and authorised return procedures (RMA).
- Specialised support: Advice on security management with best practices for equipment.
- Health monitoring: Automation of equipment health and restoration.
- Delegated administration: Ensures optimal performance and compliance with security policies by managing customer equipment with a pool of specialised engineers.

## Benefits

### Visibility

Artificial intelligence analyses all network activity (north-south, east-west) for comprehensive threat detection: all users, devices, connections, and events in the environment are monitored, stored, and accessible.

### 24/7 global coverage

A service powered by our SOC and global network of SOCs with security status monitoring and case management through real-time dashboards, coupled with robust reporting capabilities.

### Scalability

Our flexible service model and scalable infrastructure facilitate scalability in line with your business reality.

### Customisation

Our service can be customised to meet the specific needs of each customer, allowing us to adjust the customisation and proactivity of the service according to their requirements.

## Telefónica Tech's differential value



Support from an experienced security partner. A service that relies on leading technology and is provided by a team of security management experts recognised by the market.



Adapting to customer needs. The service is modular and flexible to suit customer needs. Our team of consultants and analysts helps with an appropriate adoption approach for each moment.

### BUSINESS MODEL

We help design the solution for an optimal fit through a context and needs analysis. The Service consists of the technology and services offered by the SOC, which are optional.

The technology can be either hardware or software depending on the client's needs, and it is responsible for analyzing the traffic received from the SPAN/TAP.

The SOC provisioning services ensure the correct installation and commissioning of the technology, while the operational phase services provide the ability to adjust performance to new requirements.

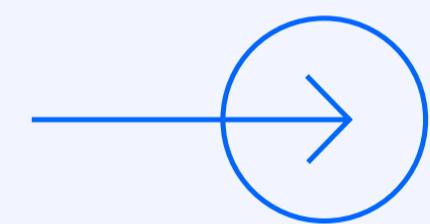
## RELATED PARTNERS

**DARKTRACE**

## OUR SOLUTIONS

**Discover all our solutions**

We believe in the transformative power of technology to improve processes, optimize resources and open new business opportunities.



Contact us to start the digital transformation of your organization.

