Telefónica Tech

NextDefense

DETECTION & RESPONSE

Managed Detection & Response

Improve your security operations to defend your business against today's cyber risks.

Let's face it, most organizations do not have the capability to respond to today's sophisticated threats, resulting in painful business operations downtime, hefty ransom payments, legal and PR expenses, and so forth.

Effective detection and response require a first-class detection technology, enhanced by SecOps experts focused on optimizing tooling, as well as hunting teams enabling proactive threat assessments and rapid breach containment.

Telefónica's Managed Detection and Response service helps modern organizations to extend their detection and response operations by allowing them to offload the efforts of 24x7 alert monitoring, proactive threat hunting, and incident response, backed up by Telefónica Tech's fixed technology stack.

Who is this service for?

Mid-size organizations that require a modern effective detection and response capability but wish to **reduce the cost burden** from **hiring staff** and **buying technology.**

Large organizations with already established SecOps capability but looking to **outsource the high-volume workload** to focus their security teams on more high-value strategic activities.

Companies looking to **develop their own in-house capability in the long-term** and choose to grow and learn from a trusted Managed Detection and Response partner.

Our value proposal

Telefónica's Managed Detection and Response service aims to improve security teams and accelerate the deployment of a fully functional detection and response capability, removing the hassle of having to choose, purchase, operate and maintain a security toolset.

This service will allow your business to:

- **Adopt first-class Endpoint Detection Response technology (EDR).**
- **Grow your own security capability and team expertise.**
- **Gain effective breach response capability.**

To achieve this, Telefónica has joined forces with the **global endpoint security leader** to provide you with a complete turnkey solution, integrating in one single offer both the EDR technology and security operations to enable rapid threat detection and response:

EDR delivery, fully managed by Telefónica

Our team takes care of the delivery and configuration of the EDR, providing close guidance and support throughout the entire setup process.

Proactive threat hunting

Our elite threat hunters leverage the latest intel from the latest TTPs and freshest IoCs to carry out proactive searches for ongoing threats in your network which have gone unnoticed by security controls.

24x7 monitoring and response

Including the triage and validation of threat alerts, and remote containment and escalation of any confirmed breach. Our clients benefit from a 4-hour escalation Service Level Agreement (SLA) for confirmed contextualized breaches.

Digital forensics and incident response

This service includes a DFIR retainer at no extra cost, which provides expert assistance for on-demand forensic analysis and emergency response to ongoing cyber-crisis.

DFIR retainer included in the service

In addition to threat detection and containment, the service also includes a **DFIR (Digital Forensics and Incident Response) retainer at no extra cost.** This DFIR capability **complements** and **extends** the MDR service, providing a safety net and allowing your CSIRT team to get rapid assistance from our DFIR team to help you respond and recover from a cyber-crisis.

Our DFIR retainer includes:

- **Access to our elite DFIR unit, 24x7 available** to provide expertise on-demand and rapid response and forensics capabilities upon your request.
- An **incident response** plan design during the initial kick-off. This protocol describes the relevant procedures and contact points and standardizes the response actions based on each use-case.
- In the event of a cyber-crisis, our client can promptly **activate our DFIR capability**. The service will grant you a **dedicated incident handler** providing end-to-end support to your teams throughout the entire incident lifecycle, including initial triage and evidence collection, first containment recommendations, assistance to build an effective eradication and recovery strategy.
- The DFIR retainer includes **standard SLAs** for time to first response, time for initial analysis and time for boots-on-ground. Additionally, our clients can purchase **premium assistance SLAs** for an even faster response.
- In addition to gaining the DFIR retainer at no cost, our service's clients also benefit from a **significant price discount on DFIR workdays**, when on-demand analysis or emergency response is requested.

Benefits of Maged Detection and Response

Significantly reducing the risk of a cyber-attack.

Controlling your Managed Detection and Response spending.

Improving your cyber security maturity.

The best EDR technology from Telefónica, a leading supplier

- Proactive threat hunting based on Telefónica Tech' proprietary threat intel.
- DFIR capability to support on-demand forensic analysis and response.
- Telefónica Tech success team and 24x7 emergency hotline.
- Weekly service reports and quarterly follow-ups.
- Client portal with real-time dashboard and collaborative case management.
- Integration with SOAR and TIP.

Meet our team and achievements

Our Teams

- +1,800 SecOps personnel.
- +1,500 security certifications.
- +200 elite Threat hunting analysts.

Achievements

- 159 adversaries monitored.
- 565K campaigns detected last year.
- Over 32,7M IoCs generated in the last 12 months.
- < 1 h average initial ransomware containment.
- +100 h boots-on-the-ground DFIR interventions in 2020.

Our business model

It is an all-in-one service; a yearly subscription that includes everything you need to stay protected. Get a top iSOC, backed up by leading EDR technology, without putting a dent on your finance while protecting you from ransomware and other attacks.

Available Editions

Service price depends on the number of covered endpoints and the edition selected:

	CORE Edition	PRO Edition	ENTERPRISE Edition
Delivery & assistance on deployment	NG-AV	NG-AV	NG-AV+EDR
Health monitoring & troubleshooting	✓	✓	✓
24x7 threat monitoring, analysis & reporting	X	✓	✓
Proactive threat hunting	X	X	✓
Support assistance 8x5	✓	✓	✓
DFIR - Assistance for complex incidents	✓	✓	✓

Note: The service includes RETAINER, Incident Response protocol and SLAs.