EXTENDED DETECTION & RESPONSE

Managed Detection & Response

HOW CAN TELEFÓNICA TECH HELP?

Our Managed Detection and Response (MDR) helps modern organisations protect themselves and respond to advanced threats

Most organisations today **do not have sufficient capacity to respond to advanced cyber threats,** resulting in complex business processes, increased costs, operational loss, legal implications or reputational loss, among other factors.

Effective detection and response requires **world-class security technology,** enhanced by SecOps experts, focused on optimising tools and supported by the expertise of threat hunting teams, enabling proactive threat assessments and rapid containment of attacks.

Our service's mission is to protect companies 24/7, increasing their own security capacity and generating a higher degree of maturity and resilience.

WHO IS THIS SERVICE FOR?

Medium-sized organisations that need to comply with industry standards and regulations but **want to reduce the financial burden of personnel recruitment costs and technology purchases.**

Large organisations with an established SecOps capability but **looking to outsource the heavy workload and 24/7 monitoring** to focus their security teams on strategic value-added activities.

Companies looking **to develop their own in-house capacity for the long term** and choosing to grow and learn from a trusted global partner with MDR services expertise.

OUR VALUE PROPOSITION

Our service

Telefónica Tech assist security teams and accelerate the deployment of an advanced and mature detection and response capability, avoiding the complex processes of purchasing, operating and maintaining a 24-hour security toolset.

We have the best market-leading technologies, security experts and automated processes to ensure complete protection.

What does it allow you to do?

This service will allow you to:

- Adopt leading **Endpoint Detection and Response (EDR) technology managed by teams of analysts who have been involved in many incidents.**
- Increase your own **security capacity, average response time and anticipation of threats.**
- Gain an effective, rapid, and comprehensive **response capability to cyber breaches** including DFIR capabilities (optional).

Benefits

Delivery, deployment, configuration and support

Our team will take care of the delivery and configuration of the EDR technology, providing personalised guidance and support throughout the implementation process.

24/7 monitoring and response

Including triage, analysis, contextualisation and validation of threat alerts. The service includes remote containment and escalation of any confirmed security breaches enriched with our intelligence platform.

Proactive Threat Hunting

Our elite threat hunters leverage the latest threat intelligence to proactively search for threats based on TTPs that have slipped through the cracks and managed to evade security systems.

Extended responsiveness

Early detection and blocking of critical threats, automatic mitigations and DFIR capability (optional) for global response.

Telefónica Tech's differential value

Control the Detection and Managed Response cost of your security and incident management operations.

Significantly reduce the risk of a cyber-attack by increasing your business maturity.

Visualisation of metrics and ticketing with our team of SOC analysts via our Customer Portal.

TEAMS & ACHIEVEMENTS

Our teams

- **+1.800** SecOps experts.
- **+1.500** security certifications.
- **+25 threat hunting** experts.

Achievements

- More than **300.000 devices** monitored.
- **4,000 critical incidents** managed on average per year.
- More than **160 attackers monitored, and 565,000 malicious campaigns** handled annually.

BUSINESS MODEL

MDR is a **complete service,** consisting of several modes adapted to the main needs of organisations, with different capacities and security protection options. The commercial model of the service offers a closed monthly price (avoiding unexpected costs) depending on the chosen modality and the number of endpoints to be protected.

The service can optionally be complemented with DFIR services, through flexible working days, for a complete response.

RELATED PARTNERS

CROWDSTRIKE paloalto NETWORKS Microsoft WatchGuard

RELATED SERVICES

Digital Forensics & Incident Response

Cyber-incident and cyber-crisis response solution to minimise damage and speed operational recovery.

SIEM Management

Monitoring and correlation of security events with 24/7 alert management, providing a solid foundation in security threat detection.

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.

Contact us to start the digital transformation of your organization.