NEXT DEFENSE

Detection & Response

HOW CAN TELEFÓNICA TECH HELP?

We help you keep your business protected from cybercriminals by offering dedicated services to detect and respond to advanced threats

We face numerous challenges with **the increasing sophistication of cyber-attack techniques, the limited visibility of IT infrastructure and the large number of alerts** from security systems and technologies that today's security operations must filter and analyse.

Telefónica Tech's family of Detection & Response services protect your business against cybercriminals, digital risks and emerging threats, identifying and detecting threats proactively and providing a comprehensive response in the event of a cyber incident.

Our main objective is to provide solid cybersecurity through advanced technology and expert knowledge, establishing the best threat detection and containment capabilities.

WHO IS THIS SERVICE FOR?

Medium to large organisations that require a fast, efficient and comprehensive response capability but wish to reduce the cost burden of hiring staff and tools for EDR, SIEM and DFIR activities.

Companies that require a modern and effective detection and response capability and wish to reduce the burden of staffing costs and technology purchases.

Companies looking to develop their own ad-hoc alerts and security events correlation and monitoring capabilities in the long term and choose to grow and learn from a trusted partner.

OUR VALUE PROPOSITION

Our service

We offer a wide range of Detection and Response services including continuous threat surveillance, proactive threat hunting, event correlation and monitoring, and incident response. Our core capabilities include:

- Multi-disciplinary security experts with in-depth knowledge in the field of detection and response.
- Complete infrastructure visibility for holistic protection.
- Automation and orchestration of a multitude of analysis, management and response processes.

What does it allow you to do?

Our services will allow you to:

- **Proactively anticipate threat detection through advanced telemetry analysis** and asset behaviours.
- **Respond comprehensively to cyber-crisis or cyber-attack situations** with an expert incident and forensic analysis team.
- **Uncover undetected compromises (IoCs or IoAs)** through threat hunting techniques and analysis by malware experts.

Benefits

Global operations model

Global and coordinated capability through our Security Operations Centers located in Europe, LATAM and the United States with homogenous processes and platforms.

Your organisation under control thanks to our experts

Multidisciplinary team highly specialised in endpoint and network threat monitoring and detection, advanced threat search, threat intelligence, malware analysis, forensics, and incident response.

Centralised cost control

Thanks to a simple and intuitive business model, based on a modular fixed subscription with no hidden costs or adapted to the needs of the service.

Management and control through the Customer Portal

Our Cybersecurity Customer Portal allows you to review all service activity in one place: view alerts, reports, graphs, service metrics and support ticketing.

Telefónica Tech's differential value

We offer full integration with proprietary SOAR automation, ticketing, threat intelligence and customer portal capabilities.

We help you significantly reduce the risk of a cyber-attack by increasing your business maturity.

We have a global team with local support and 24x7 availability for rapid detection, response and containment.

TEAMS & ACHIEVEMENTS

Our team

- **+1.800 analysts and experts** in SecOps.
- **+1.500** security **certifications.**
- **12** Global security **operations centers.**
- **+10 years of** global industry **experience.**

Achievements

- More than **565,000 malicious campaigns** managed annually.
- Recognised by IDC as a European leader in managed security services.
- Recognized as "Strong performer" by Forrester in its report "European Managed Security Services Providers, Q3 2022".
- **More than 4,000 million** SIEM security events monitored per day.
- More than **600,000 tickets** serviced per year.
- **4,000 critical incidents** managed on average per year.
- More than **19 million IoCs stored** in our threat intelligence platform.

RELATED PARTNERS

CROWDSTRIKE paloalto NETWORKS RSA Microsoft splunk> IBM

RELATED SERVICES

Managed Detection & Response

Comprehensive endpoint security monitoring through 24x7 detection, containment and rapid response to security breaches with continuous Proactive Hunting and expert cyber-crisis support, based on best-of-breed EDR and XDR technology.

Digital Forensics & Incident Response

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

SIEM Management

Monitoring and correlation of security events with 24x7 alert management, providing a solid foundation in security threat detection via our global use case catalogue, SOAR, and threat intelligence platform.

Contact us to start the digital transformation of your organization.