

CONTINUOUS THREAT EXPOSURE MANAGEMENT

Tactical Intelligence

HOW CAN TELEFÓNICA TECH HELP?

Strengthen your detection and response to emerging threats with actionable tactical intelligence.

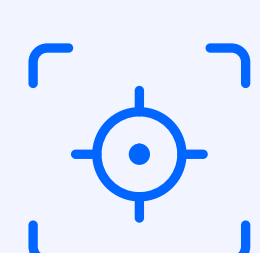
In an ever-changing threat landscape where many threats evade traditional defenses, having threat intelligence integrated into your security devices makes all the difference. It improves detection, streamlines investigation, and automates incident response.

Thanks to our **NextDefense** platform and an ecosystem of more than 160 internal, private, and public sources, our **Tactical Intelligence** service provides you with a curated, actionable, and up-to-date feed of indicators of compromise (IoC).

This feed integrates directly into your security infrastructure to expand visibility and accelerate decision-making.

In this way, we help your organization reduce exposure time, prioritize what is truly critical, and respond more effectively to threats.

WHO IS THIS SERVICE FOR?



Companies seeking to take a proactive stance in detection and response through tactical intelligence integrated into their SIEM, EDR, IPS, SOAR, or other controls.



Organizations that want to leverage verified, real-time intelligence without relying solely on open source sources.



Customers who do not have the time or resources to build, validate, or maintain their own IoC feed.



Security teams that want to save time in their investigation process by reducing false positives.

OUR VALUE PROPOSITION

Our service

Tactical Intelligence is a managed service that provides access to tactical intelligence feeds with classified and enriched indicators of compromise (IPs, domains, URLs, hashes). These indicators are generated from more than 160 public, private, and proprietary sources, including activity observed in services managed by Telefónica Tech, internal investigations, and partnerships such as the Cyber Threat Alliance and Cisco's AEGIS program.

The feed can be delivered in STIX/TAXII, CSV, or text format, and is available in two modalities (Lite and Full), adapting to your needs and maturity. Integration can be self-managed or performed by Telefónica as part of a broader service. In addition, you can expand the service with an add-on that allows you to upload your own indicators to centralize the delivery of all your intelligence sources in a single point.

What does it allow you to do?

- Receive a curated feed of IoCs, aligned with risk and trust criteria.
- Integrate these indicators into your security systems for faster and more effective detection.
- Reduce the mean time to detect (MTTD) and mean time to respond (MTTR) to incidents.
- Expand visibility into active threats with rich context (threat type, industry, region, CVE, TTP, etc.)
- Customize intake, expiration policy, risk and confidence thresholds for a feed tailored to your needs.
- Leverage intelligence generated by Telefónica Tech's global services.

Benefits

Prevention

It allows you to strengthen your security perimeter and internal systems through the use of actionable intelligence, blocking threats before they materialize.

Automated response

Activates automatic response mechanisms to known threats.

Proactive detection

Mejora la capacidad de detección temprana de amenazas de tu stack de seguridad mediante la correlación directa con IoC frescos y relevantes.

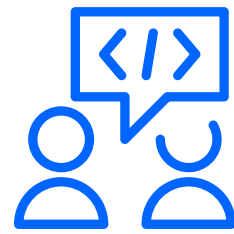
Adaptability

Adjust the service to suit your needs, with customization options and flexible management.

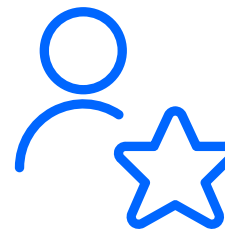
Telefónica Tech's differential value



As an MSSP, we generate our own threat intelligence, which we combine with a wide variety of sources from our ecosystem of partners and strategic alliances.



We actively participate in strategic alliances such as the Cyber Threat Alliance and the Spanish National SOC's Network.



We tailor our service to meet the needs and risk profiles of each customer, offering a personalized approach.

EQUIPMENT, TEAMS AND ACHIEVEMENTS

Our teams

- Dedicated unit of intelligence analysts providing global service from Digital Operations Centers (DOCs) located in Spain and Colombia.
- +29M indicators of compromise on our intelligence platform.
- Extensive experience in integrations with technologies such as SIEM, TIP, SOAR, EDR...

Achievements

- Recognized by CCN-CERT as the main contributor of threat intelligence to the Spanish National SOC's Network for two consecutive years.
- Ongoing collaboration with global alliances and leading organizations in sharing intelligence on emerging threats.

RELATED PARTNERS



BUSINESS MODEL

Tactical Intelligence is a service with a recurring subscription fee, available in Lite or Full modalities, with a wide variety of customization and management options tailored to each customer (integration managed by other services or by the customer themselves, delivery via TAXII or URL, risk and confidence thresholds, types of indicators to receive, sources to consume, expiration policy, number of feeds to create, possibility of adding customer-specific indicators for their exclusive use).

It does not require complex deployments and can be easily integrated into existing systems.

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.

