EXPOSURE MANAGEMENT

Red Team Assessment

HOW CAN TELEFÓNICA TECH HELP?

Real threats don't have scope and time restrictions. Our Service allows to measure yourself against the adversary.

Commonly confused with Penetration Testing, which is a defined, scoped, limited and point-in-time test that has specific goals for success or failure. On the contrary, **a corporate Red Team is a continuous service that runs for long periods**, is performed from as close to a zero-knowledge perspective, non-limited in scope whose main objective is to improve the already existing defenses, i.e., Blue Team.

Our Red Team Service is designed to continuously test and improve the effectiveness of detection and respond capabilities of corporate information security defenses simulating real-world scenarios by replicating the Techniques, Tactics and Procedures (TTPs) of real-world adversaries.

We provide companies an independent assessment with a deep dive into the risks and vulnerabilities of the business and serves as a baseline definition from which future security improvements can be measured.

WHO IS THIS SERVICE FOR?

Highly mature security organisations with established SecOps teams seeking to assess, measure and improve their security incident protection, detection, and response capabilities in a continuous and realistic fashion.

Customers looking for developing long-term, sophisticated internal Red Team Assessment capabilities and choose to grow and learn from a trusted partner.

Compañías del sector de **infraestructuras críticas**, el **sector público**, o aquellas que gestionen **datos personales**, **información clasificada**, y estén sujetas a **cumplimientos normativos.**

OUR VALUE PROPOSITION

Our service

We run simulations of attacks against people, software, hardware, and infrastructure, from the perspective of cybercriminals, using tactics, techniques and procedures observed in recent real-life attacks. In this way, we identify and exploit the vulnerabilities found and demonstrate how they could damage company's most critical assets.

Each of these attacks is bespoke to your organisation, considering both technological and business aspects. The service has a dedicated Red Team with multidisciplinary knowledge and skills, whose mission is to design and execute the different attack scenarios (social engineering, physical intrusion tests, application, system, and communications intrusion tests), based on the threat intelligence obtained on the technological and/or human assets of your organisation.

What does it allow you to do?

This service will allow you to:

- Get comprehensive and independent assessment of the **strengths and weaknesses** of your security.
- Obtain clear and concise guidance on how to **protect information** against nowadays sophisticated attacks.
- Gain **persistent experience against next-generation threats** and unknown vulnerabilities without risks.

Benefits

Check the real impact of a targeted attack

Without suffering real world consequences and justify the allocation of security resources and whether they are being used effectively to mitigate and prevent threats.

A complete analysis of your security's strengths and weaknesses

Receive distilled the essential information that your company needs to have and convey it in a way which is valuable to both non-technical executives and the technical security team.

Gain persistent experience

Against next-generation threats and unknown vulnerabilities without risks. Increase corporate awareness, security team motivation and readiness as defences are constantly tested and adapted to continuous evolving environment.

Telefónica Tech's differential value

We execute adversarial simulations designed to emulate real-world scenarios covering attack vectors for cyber, physical, and human elements.

We keep close engagement and communication for internal incident response and defensive teams with follow-up meetings, executive presentations for management audiences and technical reports with detailed explanations.

We have a Purple teaming framework that enables Red and Blue teams to collaborate in the best interests of the organization and make the most of the simulations.

TEAMS & ACHIEVEMENTS

Our team

- **+2,200** SecOps employees.
- **+3,000** security certifications.
- **+100** pentesters worldwide.
- **+50** global security analysts.

Achievements

- **+14,000** hours performing Red Team exercises in the last year.
- **98%** of our customers were successfully compromised during our Red Team exercises.
- **90%** of the cases, our Red Team was able to achieve the first objective in the first 5 days.
- **85%** of the cases, our Red Team was able to compromise the first asset in less than 24 hours
- **75%** of our customers believed their security defences were prepared against any threat.

BUSINESS MODEL

Our service is offered in three modalities:

•Full Red Team exercise of **3 months**, with follow-up meeting and executive and technical reports.

•**4-month** TIBER ES exercises, which allows you to comply with the Bank of Spain's TIBER regulations

•**12-month** Red Team service that adds continuous monitoring for changes in the exposed infrastructure and leakage of information on the internet.

RELATED SERVICES

Pentesting & Security Assessment

Reveal vulnerabilities an attacker could exploit to gain access to your environment and systems.

Vulnerability Scanning

Beyond traditional scanning with dynamic risk-based remediation that may affect your organisation.

Breach Attack Simulation

Simulation of attacks to identify vulnerabilities and assess the effectiveness of security defences, enabling continuous improvement of threat protection strategies.

Contact us to start the digital transformation of your organization.