Telefónica Tech

NextDefense

CONTINUOUS THREAT EXPOSURE MANAGEMENT

Automated Security Validation

HOW CAN TELEFÓNICA TECH HELP?

Automated Security Validation represents the new generation of offensive managed services: agile, secure, traceable, and with a direct impact on companies' Cyber Security posture.

Traditional security audits are no longer enough to guarantee an organization's resilience. Systems are constantly changing, threats evolve daily, and breaches can arise at any time. This makes continuous validation a must.

Telefónica Tech helps you evolve towards an offensive and automated validation model that allows you to discover real weaknesses in your systems before attackers find them. Our Automated Security Validation (ASV) service provides you with continuous visibility, real risk-based prioritization, and clear evidence for the continuous improvement of your security.

WHO IS THIS SERVICE FOR?

Organizations with complex environments (internal, cloud, and hybrid) seeking to continuously validate their security posture against real attacks.

Companies seeking to prioritize defense actions based on evidence and real exploitability, not just theoretical scores.

Cyber Security teams that need clear evidence and prioritization based on real exploitation, not theoretical scoring.

Any organization that must comply with regulations, audits, or certifications and requires traceability and documentation of its defenses.

OUR VALUE PROPOSITION

Our service

Automated Security Validation is a managed service that allows you to securely emulate real attacks on your internal, cloud, and perimeter environments. We run controlled offensive tests that identify exploitable vulnerabilities, configuration errors, and deficiencies in your controls through an agentless platform, without the need to install software on your systems.

The service is tailored to each customer through specialized modules: Core, Cloud, and Surface. It also prioritizes findings based on actual risk and provides technical and executive reports, monthly meetings, and purple teaming sessions. All of this, without disrupting your business operations.

What does it allow you to do?

- Reproduce real attack techniques (lateral movement, privilege escalation, vulnerability exploitation) without impacting production.
- Validate internal environments, cloud, and external surface automatically.
- Prioritize remediation based on real risk and ease of exploitation, not just CVSS.
- Align your security posture with MITRE ATT&CK and OWASP frameworks.
- Gain useful audit trailability with deliverables that document each phase of validation.
- Scale testing quickly, frequently, and without manual intervention.

Benefits

Seamless continuous offensive validation

The platform launches thousands of automated tests that simulate real attacks without the need to install agents or interrupt operations. This allows you to securely and frequently validate whether your defenses are working as they should in real environments.

Prioritization by technical and operational impact

Los resultados no se basan en métricas genéricas como el CVSS, sino en el impacto real dentro del entorno de tu compañía. Se priorizan vulnerabilidades según su facilidad de explotación y su potencial de compromiso, lo que permite actuar donde realmente importa.

Complete closure of the remediation cycle

The service allows automatic revalidation of whether the corrective measures applied have worked, thus closing the loop between identification and resolution. This reduces uncertainty and ensures continuous and verifiable improvement.

Improved return on investment in security

The service helps optimize Cyber Security investments by clearly identifying which controls are working and which are not. This prevents oversizing and justifies spending based on tangible results.

Telefónica Tech's differential value

A service managed globally from our DOCs, with local proximity and a team of experts in offensive simulation.

Comprehensive delegated administration of the validation environment, without the need for offensive internal profiles from the customer.

Ability to assess entire surfaces (internal, cloud, external, credentials, ransomware) through a single platform.

EQUIPMENT, TEAMS AND ACHIEVEMENTS

Our teams

- Certified security analysts with over 10 years of experience in offensive security.
- Ability to operate in regulated, distributed, and sensitive environments.

Achievements

- Pentera: Top 10 most innovative Cyber Security companies according to Inc. and Fast Company.
- Telefónica Tech: recognized as a European leader in managed Cyber Security services.

BUSINESS MODEL

- Recurring subscription based on number of assets (endpoints, workloads, subdomains).
- Service modalities: Pentera Core, Pentera Cloud, Pentera Surface.
- Deliverables: real-time access to platform, technical/executive reports, Purple Teaming sessions.
- Support and training included.

RELATED PARTNERS

PENTERA

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.