CYBER THREAT INTELLIGENCE

Attack Surface Management

| HOW CAN TELEFÓNICA TECH HELP YOU?

Discover your externally visible vulnerable assets and correct them before they become an avenue of compromise.

Your attack surface is bigger than you think. And it's growing every day. The growing adoption of emerging technologies such as the cloud, the Internet of Things (IoT) and mobility, coupled with the increasing complexity of business environments and lack of adequate visibility, create a fertile battleground for cybercriminals.

Attackers, always on the hunt for new vulnerabilities, are taking advantage of this expansion of the attack surface to launch increasingly sophisticated attacks. Attack techniques are constantly evolving, from zero-day exploits to ransomware and malware-less attacks, forcing companies to take a proactive approach to protecting their digital assets.

In this context, an Attack Surface Management (ASM) service becomes an indispensable tool for companies seeking to protect themselves against modern cyber threats and to have a robust cybersecurity posture.

| WHO IS THIS SERVICE FOR?

Medium and large companies, multinationals and public sector entities that are interested in obtaining an accurate view of their current attack surface and making informed decisions to manage it efficiently.

Our service

According to Forrester, companies are unaware of or not managing 30% of their assets due to rapid digital transformation. And 50% of organizations' global exposure will be non-patchable by 2026, according to Gartner. This reality makes an Attack Surface Management service crucial for efficient and effective attack surface management.

At Telefónica Tech we offer you a managed service that helps you discover your assets using the same sophisticated reconnaissance techniques as attackers, identify vulnerabilities, contextualize them, prioritize them and help you remediate them before they can be exploited.

What does it allow you to do?

Our service is designed to put adversarial knowledge in the hands of defenders and help you:

› **Uncover and eliminate hidden vulnerabilities:** Gain comprehensive visibility into your entire attack surface, proactively identifying and remediating critical vulnerabilities before they can be exploited.

› **Minimize your risk exposure:** Prioritize remediation efforts based on real-time risk assessments, ensuring that you address the most impactful threats first.

› **Simplify security compliance:** Streamline compliance audits and demonstrate adherence to industry regulations with a holistic view of your security posture.

› **Empower proactive security:** Implement continuous monitoring and threat intelligence to stay ahead of evolving cyberattacks and maintain a proactive defense strategy.

› **Strengthen your brand reputation:** Protect your sensitive data and customer trust by minimizing the likelihood of costly data breaches and reputational damage.

Benefits

Comprehensive visibility

Complete view of the attack surface, both internal and external, allowing you to identify unknown assets, misconfigurations and potential vulnerabilities.

Risk prioritization

Prioritize vulnerabilities based on their level of risk and potential impact, ensuring efficient use of your security resources.

Proactive remediation

Facilitates timely remediation of vulnerabilities, significantly reducing the window of opportunity for attackers.

Continuous monitoring

Your attack surface is growing every day. It is important to monitor it continuously to be aware of it and to be able to detect and respond quickly to new threats and vulnerabilities.

Telefónica Tech's differential value

Accurate discovery designed to continuously identify any exposure.

Seamless bi-directional integrations with your security stack for greater efficiency.

Actionable context to focus remediation efforts where it really matters.

Our teams

› **~2.200** SecOps employees.

› **+3.000** security certifications.

› **+50** pentesters worldwide

› **+40** global security analysts

Achievements

› **+25K** IP addresses scanned monthly.

› **+30K** web applications analysed on a monthly basis.

The service is marketed as a combination of licenses from market-leading vendors, configurable through different options to suit each customer's needs, and a layer of professional services from our expert DOC team.

paloalto

IBM

RELATED SERIVICES

Digital Risk Protection

We monitor and protect your companys brand, reputation and business against threats directed against your organisation on the public web as well as on the deep and dark web.

Vulnerability Scanning

Monitoring and analysis of network infrastructure and web applications, providing comprehensive asset vulnerability identification and prioritised lifecycle management through our customer portal and iSOC.

Red Team Assessment

We run simulations of attacks with real scenarios adapted to the reality of your business, which allow you to validate your resilience, and train and evolve your defences, being the best way to protect the most critical assets and processes.

Contact us to start the digital transformation of your organization.