

CONTINUOUS THREAT EXPOSURE MANAGEMENT

# Breach Attack Simulation

## HOW CAN TELEFÓNICA TECH HELP?

Breach Attack Simulation transforms your Cyber Security strategy, allowing you to detect what escapes on paper and strengthen your environment with real data.

Many organizations continue to rely on the theoretical configuration of their security systems. Telefónica Tech's Breach Attack Simulation (BAS) service provides continuous, automated, and impact-free validation to test the real-world effectiveness of your defenses against modern attacks.

We assess the detection, blocking, and response capabilities of your tools (EDR, AV, SEG, WAF, SIEM, etc.) through secure and controlled offensive simulations, reproducing real TTPs, MITRE ATT&CK scenarios, and emerging threats. This helps identify exploitable weaknesses and prioritize their remediation based on the real risk to the business.

## WHO IS THIS SERVICE FOR?



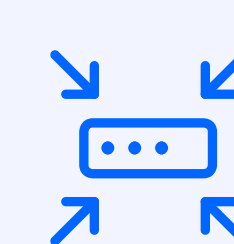
Organizations that want to know with certainty whether their security controls are working against real attacks.



Companies seeking continuous validation of their defenses without disrupting operations.



Environments with high compliance requirements that need evidence of offensive validation for audits.



Security teams that require expert support to identify, interpret, and remediate real vulnerabilities.



## OUR VALUE PROPOSITION

### Our service

Breach Attack Simulation is a managed service that allows you to continuously and securely test the resilience of your defenses against real threats. We run automated offensive simulations on internal, cloud, perimeter, and user environments through the Cymulate platform, evaluating everything from basic techniques to advanced post-exploitation scenarios.

The service adapts to every level of maturity through scalable packages (Essentials, Pro, Enterprise, and Cloud Native) and can be complemented with add-ons such as automated Red Teaming, WAF validation, phishing campaigns, or AI-powered offensive strategies. The results are integrated into interactive dashboards and technical and executive reports, along with Purple Teaming sessions that allow you to continuously optimize your controls.

### What does it allow you to do?

- Automatically and securely validate the effectiveness of your security controls against real threats.
- Emulate attacks aligned with MITRE ATT&CK, simulating intrusion, persistence, escalation, and exfiltration techniques.
- Detect ineffective configurations and blind spots before they are exploited by a real attacker.
- Incorporate new threats in less than 24 hours after their global identification.
- Validate cloud environments, WAFs, EDRs, containers, DLP, and other critical technologies.
- Automate remediation tasks, generate customized scenarios, and perform Red Teaming without impact.

## Benefits

### Realistic and continuous verification

Allows you to verify whether security controls detect and block real threats by emulating current offensive techniques in real environments, without generating operational impact. These are not theoretical tests, but dynamic and adaptive simulations.

### Integration into your ecosystem

The results and findings are integrated with SIEM, SOAR, XDR, and other defensive tools, generating actionable alerts and facilitating response automation.

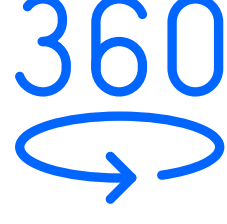
### Modular and scalable assessment

El servicio se adapta a tu nivel de madurez en seguridad. Desde validaciones tácticas sobre Email Gateway o Antivirus hasta campañas ofensivas completas, puede crecer junto a tus necesidades sin cambiar de plataforma ni proveedor.

### Improved compliance and resilience

The service provides traceable technical evidence useful for compliance audits and validations (such as ISO 27001, ENS, etc.) while strengthening your defensive posture against threats such as ransomware or exploitation of known vulnerabilities.

## Telefónica Tech's differential value



360° managed service with delegated administration and ongoing advice.



SaaS platform with no complex deployments, secure and scalable.



Secure simulations in production and cloud environments.



Incorporation of real TTPs and vulnerabilities with more than 7,000 offensive payloads.

### EQUIPMENT, TEAMS AND ACHIEVEMENTS

#### Our teams

- Certified security analysts with over 10 years of experience in offensive security.

#### Achievements

- Telefónica Tech named "Cymulate Best Partner 2024"
- Cymulate: "Leader in BAS" according to Frost Radar y G2, Customer's Choice 2024.

### BUSINESS MODEL

- Recurring subscription based on the selected package (Essentials, Pro, Enterprise, Cloud Native).
- Available add-ons: Automated Red Teaming, WAF validation, automatic remediation, custom scenarios, phishing simulation.
- Deliverables: Access to SaaS platform, dashboards, technical and executive reports, Purple Teaming sessions.
- Training, support, and follow-up included.



## RELATED PARTNERS

 cymulate

## 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.

