EXTENDED DETECTION & RESPONSE

Identity Threat Detection & Response

HOW CAN TELEFÓNICA TECH HELP?

Providing visibility into threats targeting your Active Directory and responding to them. We also advise you on preventive measures you can implement to ensure your identities are not compromised by an attacker

The Active Directory (AD) is a legacy tool that is a priority target for attackers due to its dominant position in the market. It also lacks the ability to detect anomalous configurations, and its interdependence with other information systems often creates vulnerabilities that attackers exploit to move laterally within an organization's IT infrastructure.

Telefónica Tech offers ITDR (Identity Threat Detection & Response) technologies, as well as a team of experts who operate the service from the SOC (present in 12 locations). Analysts investigate, respond, and report on detected threats, advise on risk mitigation due to poor AD configurations or compromised credentials, and propose prevention automation based on dynamic risk conditions.

WHO IS THIS SERVICE FOR?

Companies that want to evolve the detection, investigation, and response of workstations and servers with extended threat response capabilities in the Microsoft AD and Azure AD technology environment.

Companies that need visibility and advice on weak credential policies, vulnerable attack paths, compromised credentials on the dark web, or users with excessive privileges so they can clean up and protect their Active Directory with better guarantees.

Companies that lack sufficient knowledge and require a security partner with experience in managing sophisticated identity threats such as DCSync, Golden Ticket, Pass-the-Hash, or other Kerberos protocol attacks.

OUR VALUE PROPOSITION

Our service

The service monitors threats of lateral movements by attackers from the PC or server to the Active Directory 24/7/365, and offers guided or automatic responses, as appropriate, to remedy the attack by blocking the user, forcing a password reset, or requesting two-factor authentication (MFA).

We provide recommendations for AD hygiene through regular meetings and reports. In addition, the service recommends and deploys prevention automation with dynamic risk conditions. If, for example, an organization's credentials have been stolen and detected on the dark web, the automation will force the user of those credentials to reset their password the next time they log in.

What does it allow you to do?

This service will allow you to:

- **Gain visibility, severity, and threat risk advice based on Active Directory configuration.**
- **Detect, investigate, and respond** to lateral movements by attackers within your IT infrastructure that could compromise Active Directory as preliminary steps in their attack.
- **Deploy identity risk prevention automation based on Zero-Trust guidelines.**

Benefits

Improved detection and response coverage

The service detects anomalous behavior through continuous analysis and machine learning, identifying Active Directory risks like privilege escalation or impersonation.

Automatic prevention that closes entry doors to attackers

Continuous risk assessment from weak configurations or compromised credentials protects Active Directory and identifies privilege changes or inactive users.

Advice on best practices for Active Directory configuration

Automated risk-based access controls, like one-time MFA or blocking malicious IPs, protect identities and stop unauthorized access attempts.

Telefónica Tech's differential value

We not only alert and investigate threats, but also propose, develop, and audit automated risk-based prevention responses to anticipate the attacker's movements.

Our consulting experience will help you prevent future attacks by improving the ongoing security posture of Active Directory.

Many of our SOC's operational processes are automated, allowing us to detect, investigate, and respond to threats in a short amount of time.

EQUIPMENT, TEAMS, AND ACHIEVEMENTS

Our teams

- **+2,500** cyber security professionals.
- **+3,000** security certifications.
- **2** global digital hubs with 11 locations worldwide.

Achievements

- **+50,000 protected identities.**
- **+19 million** IoCs stored on our threat intelligence platform.
- CrowdStrike **Elite MSSP Certification.**

BUSINESS MODEL

Identity Threat Protection & Response can be purchased as a customized service, with dedicated analysts, or with a predefined scope as part of Telefónica's MDR service.

In the predefined scope mode, the price is monthly, with no setup fee, and will vary depending on the number of identities to be protected.

We offer the option of purchasing licenses as a supply or including them as part of the service.

RELATED PARTNERS

CROWDSTRIKE

RELATED SERVICES

Managed Detection & Response

Comprehensive endpoint security monitoring thanks to 24/7 detection, containment, and rapid response to security breaches with continuous proactive hunting and expert cyber crisis support, based on the best EDR and XDR technology.

Digital Forensics & Incident Response

Cyber incident and cyber crisis response solution to minimize damage and accelerate operational recovery, including dedicated incident manager, forensic/malware analysis, and assistance with containment, recovery, and eradication of threats.

SIEM Management

Monitoring and correlation of security events with 24/7 alert management, providing a solid foundation for security threat detection through our global use case catalog, SOAR, and threat intelligence platform.

Contact us to start the digital transformation of your organization.

2025 © Telefónica Cybersecurity & Cloud Tech S.L.U. with Telefónica IoT & Big Data Tech S.A. All rights reserved.