Telefónica recreates the Digital Operations Center in Barcelona with which it protects organisations

PUBLISHED MAR 3, 2025
BY TELEFÓNICA

Telefónica will show at the Mobile World Congress in Barcelona, from 3 to 6 March, the advanced capabilities of the Telefónica Tech Digital Operations Center (DOC), which monitors and operates its customers' cybersecurity and cloud services globally, 24 hours a day, every day of the year. Those attending the MWC will have the opportunity to learn about the daily work of a cybersecurity expert and participate with them in decision-making in the event of simulated security incidents.

Telefónica will use its 'Digital Operations Center' demo to show some of the capabilities offered by the DOC to protect the security of organisations. Specifically, it will exhibit three interactive use cases linked to security information and event management (SIEM), threat intelligence and the detection of and response to a ransomware attack that will be simulated at the stand. Ransomware attacks are those in which the cybercriminal blocks or encrypts information and asks the affected user for money in exchange for returning their data.

In the first use case, attendees will have to analyse, with the support of the company's cybersecurity experts, the different steps that can be taken when it is detected that the same IP has attempted to access multiple users at the same time, apparently unsuccessfully. They will see for themselves how the managed SIEM solution provides extra security by having the capacity to continuously and automatically monitor and detect security anomalies and cyberthreats before they affect organisations.

In the second use case, visitors will be faced with a data leak and its publication on the dark web. In this case, the company will show how the Threat Intelligence team, responsible for providing knowledge

about the intentions and abilities of cyber attackers, makes it possible to anticipate attacks and design more efficient responses based on comprehensive cybersecurity solutions.

And finally, in the third use case, visitors to the stand will be transported to an organisation under ransomware attack. The cybersecurity experts will explain the steps that should be followed to identify and resolve it, based on managed detection and response (MDR) services that combine the knowledge of intelligence analysts ('Threat Hunting') to proactively search for threats that have gone unnoticed in order to anticipate them and achieve zero or minimal impact on the client, continuous monitoring of these threats and the work of the digital forensics and incident response (DFIR) team to determine the origin and scope of the incident in order to provide expert assistance to contain and resolve it as early as possible.

In 2024 alone, Telefónica Tech's DOC operations team, which has locations in Madrid and Bogotá to provide uninterrupted service on both sides of the Atlantic, managed more than 50 cyber technologies, identified more than 290,000 threats through threat intelligence, deployed more than 370, 000 EDR tools were deployed, more than 50,000 hours of pentesting and red teaming (security assessments in which controlled attacks are simulated to detect possible vulnerabilities in companies) were carried out and more than 4,100 terabytes of security events were incorporated into SIEM.

The dual role of AI in the world of cybersecurity

At the MWC, Telefónica will also demonstrate the dual role that artificial intelligence is playing in the world of cybersecurity (on the one hand, it allows for the automation and improvement of incident detection and response, and, on the other hand, it is being used by cybercriminals to launch more sophisticated attacks) and will exhibit its own capabilities to stop the progress of an attack launched by this technology.

To do this, it will stage an attack in which a Generative AI will issue orders with the sole objective of stealing a manager's credentials for accessing a business application and another Generative AI will be able to detect and report the attack. In addition to detecting the malicious act, the stand visitor will also be able to verify in real time how the stolen credentials will not work to log into the application thanks to the use of Open Gateway (the global initiative of the

telecommunications sector, led by the GSMA, to transform telecommunications networks into future-ready platforms). Through Open Gateway APIs (Application Programming Interfaces) it is possible to perform tasks such as obtaining network information or configuring the network for a specific purpose.

In this case, the ‘ Number Verification’ API provides extra security, as it allows the user to be authenticated through their telephone number via the mobile network. This API reinforces security in identity authentication and verification processes without the need to rely on traditional methods such as SMS OTP, which can be vulnerable to message interception.

Press release distributed by Wire Association on behalf of Telefónica, on Mar 3, 2025. For more information subscribe and follow us.

Media Assets

Embedded Media

Visit the online press release to interact with the embedded media.

https://wireassociation.eu/newsroom/telefonica/releases/en/telefonica-recreates-the-digital-operations-center-in-barcelona-with-which-it-protects-organisations-2397

Telefónica

Newsroom: https://wireassociation.eu/newsroom/telefonica
Website: https://www.telefonica.com/
Primary Email: contacto@fundaciontelefonica.com

Social Media

Facebook - https://www.facebook.com/telefonica
Linkedin - https://www.linkedin.com/company/telef%C3%B3nica

Twitter - https://twitter.com/telefonica/
Instagram - https://www.instagram.com/telefonica/
Youtube - https://www.youtube.com/user/telefonica