Nota de prensa MWC 2025

Telefónica recrea en Barcelona el Centro de Operaciones Digitales con el que protege a las organizaciones

- Telefónica mostrará en su stand del MWC con la demo 'Digital Operations Center' cómo es el trabajo de los expertos de Telefónica Tech encargados de monitorizar y operar globalmente los servicios de ciberseguridad y cloud de los clientes durante las 24 horas y todos los días del año.

- La demo exhibirá tres casos de uso interactivos y permitirá a los asistentes participar en la toma de decisiones ante diferentes incidentes de seguridad simulados (incluido un ataque de tipo 'ransomware').

- La compañía demostrará, además, el potencial de la inteligencia artificial, tanto para potenciar los ataques de ciberseguridad como para robustecer los mecanismos de protección, y destacará la capa extra de seguridad que aporta a través de la API de 'Number Verification' de Open Gateway.

Barcelona, 3 de marzo de 2025.- Telefónica mostrará en su stand del Mobile World Congress (MWC), evento que se celebra en Barcelona entre el 3 y el 6 de marzo, las capacidades avanzadas del Centro de Operaciones Digitales (DOC) de Telefónica Tech con el que monitoriza y opera globalmente los servicios de ciberseguridad y cloud de sus clientes durante las 24 horas y todos los días del año. Los asistentes al MWC tendrán la oportunidad de conocer cómo es el trabajo diario de un experto en ciberseguridad y participar junto a ellos en la toma de decisiones ante incidentes de seguridad simulados.

Telefónica representará con su demo 'Digital Operations Center' algunas de las capacidades que ofrece desde el DOC para proteger la seguridad de las organizaciones. Exhibirá, concretamente, tres casos de uso interactivos vinculados a la gestión de eventos e información de seguridad (SIEM, por sus siglas en inglés), a la inteligencia de amenazas ('Threat Intelligence') y a la detección y respuesta ante un ataque de tipo 'ransomware' que se simulará en el stand. Los ataques 'ransomware' son aquellos en los que el ciberdelincuente bloquea o cifra información y pide dinero al usuario afectado a cambio de devolverle sus datos.

En el primer caso de uso, los asistentes tendrán que analizar, con el apoyo de los expertos de ciberseguridad de la compañía, los diferentes pasos que pueden tomar cuando se detecta que una misma IP ha intentado acceder, de forma aparentemente fallida, a múltiples usuarios a la vez. Comprobarán en primera persona cómo la solución de SIEM gestionado proporciona un extra de seguridad al tener la capacidad

Telefónica, S.A.
Dirección de Comunicación Corporativa
email: prensatelefonica@telefonica.com
saladeprensa.telefonica.com

***Este documento está clasificado como PUBLICO por TELEFÓNICA.
***This document is classified as PUBLIC by TELEFÓNICA.

de monitorizar y detectar de forma continuada y automatizada anomalías de seguridad y ciberamenazas antes de que afecten a las organizaciones.

En el segundo caso de uso, los visitantes se enfrentarán a una fuga de datos y a su publicación en la 'dark web'. En este caso, la compañía mostrará cómo el equipo de 'Threat Intelligence', encargado de aportar conocimiento sobre las intenciones y habilidades de los ciberatacantes, permite anticiparse a los ataques y diseñar respuestas más eficientes apoyándose en soluciones integrales de ciberseguridad.

Y, por último, en el tercer caso de uso los asistentes al stand se transportarán a una organización atacada con un ataque de tipo 'ransomware'. Los expertos en ciberseguridad explicarán los pasos que deben seguirse para identificarlo y resolverlo, apoyándose en servicios de detección y respuesta gestionada (MDR, por sus siglas en inglés) que aúnan el conocimiento de los analistas de inteligencia ('Threat Hunting') para hacer búsquedas proactivas de amenazas que hayan pasado desapercibidas para anticiparse a ellas y lograr un impacto nulo o mínimo en el cliente, la monitorización continua de las mismas y el trabajo del equipo de análisis forense digital y respuesta a incidentes (DFIR) para determinar el origen y alcance del incidente con el fin de proporcionar asistencia experta para contenerlo y resolverlo de la forma más temprana posible.

Solo en 2024 el equipo de operaciones del DOC de Telefónica Tech, que cuenta con localizaciones en Madrid y Bogotá para prestar un servicio ininterrumpido a ambos lados del Atlántico, gestionó más de 50 cibertecnologías, identificó más de 290.000 amenazas a través de inteligencia de amenazas, se desplegaron más de 370.000 herramientas EDR, se realizaron más de 50.000 horas de 'pentesting' y 'red team' (evaluaciones de seguridad en las que se simulan ataques controlados para detectar posibles vulnerabilidades en las empresas) y se incorporaron más de 4.100 terabytes de eventos de seguridad en SIEM.

El doble papel de la IA en el mundo de la ciberseguridad

Telefónica demostrará también en el MWC el doble papel que está desempeñando la inteligencia artificial en el mundo de la ciberseguridad (por un lado, permite automatizar y mejorar la detección y respuesta a incidentes, y, por otro, está siendo utilizada por los ciberdelincuentes para lanzar ataques más sofisticados) y exhibirá capacidades propias para frenar el avance de un ataque lanzado por esta tecnología.

Para ello, escenificará un ataque en el que una IA Generativa lanzará órdenes con el único objetivo de robar a un directivo sus credenciales de acceso a una aplicación empresarial y otra (IA Generativa) será capaz de detectar y notificar el ataque. Además de detectar el acto malicioso, el visitante del estand también podrá comprobar en tiempo real cómo las credenciales robadas no servirán finalmente para iniciar sesión en la aplicación gracias al uso de Open Gateway (la iniciativa global del sector de telecomunicaciones, liderada por la GSMA, para transformar las redes de telecomunicaciones en plataformas preparadas para el futuro). A través de las APIs (Application Programming Interfaces) de Open Gateway es posible realizar tareas como obtener información de la red o configurarla para algún propósito especifico.

Telefónica, S.A.
Dirección de Comunicación Corporativa
email: prensatelefonica@telefonica.com
saladeprensa.telefonica.com

***Este documento está clasificado como PUBLICO por TELEFÓNICA.
***This document is classified as PUBLIC by TELEFÓNICA.

En este caso, la API de ‘Number Verification’ aporta un extra de seguridad, ya que permite autenticar al usuario a través de su número de teléfono a través de la red móvil. Esta API refuerza la seguridad en procesos de autenticación y verificación de identidad sin necesidad de depender de métodos tradicionales como el SMS OTP, los cuales pueden ser vulnerables a la interceptación de mensajes.

Para más información: Telefónica en el MWC 2025

Telefónica, S.A.
Dirección de Comunicación Corporativa
email: prensatelefonica@telefonica.com
saladeprensa.telefonica.com

***Este documento está clasificado como PUBLICO por TELEFÓNICA.
***This document is classified as PUBLIC by TELEFÓNICA.