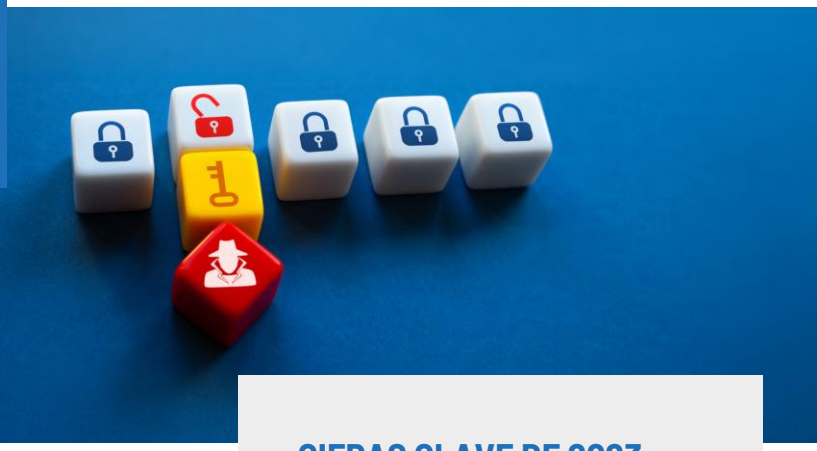
Servicio de ***Alerta Temprana de vulnerabilidades de Ciberseguridad***



CIFRAS CLAVE DE 2023

- El **74% de los CEOs** están **preocupados** por la **capacidad** de sus organizaciones para **responder** ante un **ciberincidente**.
- España **es el país europeo más ciberatacado** y el **tercero a nivel mundial,** por detrás de EEUU y Japón.
- El **93%** de los **sistemas** podrían ser **vulnerados** en la actualidad.

RETOS

Las organizaciones se enfrentan a una serie de complejos desafíos, azuzados por un mercado tremendamente ágil y en constante evolución. Desde la incertidumbre económica hasta la competencia feroz, las empresas deben adaptarse a las cambiantes tendencias y a la rápida evolución de la tecnología, manteniéndose actualizadas y flexibles para garantizar la relevancia de sus productos y servicios. La digitalización también está poniendo de manifiesto el crecimiento de la superficie de ataque, aumentando así las posibilidades de sufrir un ciberincidente con las consecuencias que ello puede conllevar para su supervivencia.

SOLUCIONES

Conocemos profundamente las necesidades de las organizaciones, y tratamos de darles cumplimiento diseñando, implantando, manteniendo y operando planes integrales de seguridad basados en las seis funciones del NIST (Gobierno, Identificación, Protección, Detección, Respuesta y Recuperación). Dentro de ellas, nuestro servicio de *Alerta Temprana de Vulnerabilidades* se enmarca dentro de las acciones preventivas de identificación que pueden adoptar las empresas para su protección.

Objetivo

Como expertos en *Inteligencia* y en *detección y gestión de vulnerabilidades*, el objetivo de este servicio es **alertar a nuestros clientes** sobre la aparición de nuevas **vulnerabilidades 0-day** en sus activos **hardware y software**, adelantándonos así a potenciales ciberincidentes que puedan producirse si estas llegan a ser explotadas por atacantes maliciosos.

Funcionamiento

Cuando identificamos una amenaza, esta se clasifica y notifica a través de nuestro sistema de alertas. En el caso de tratarse de una amenaza alta o crítica, esta es notificada en menos de 24 horas desde su descubrimiento, analizando además a los posibles actores implicados, las motivaciones que pueden justificar a los mismos, así como conclusiones e hipótesis de su evolución que puedan brindar apoyo para su resolución.

El servicio se compone de dos fases, una fase inicial de recopilación de datos que a su vez es retroalimentada durante todo el servicio y el posterior proceso de monitorización. Tras confirmarse los activos, plataformas, fabricantes y versiones a monitorizar, y el punto de contacto del cliente, damos inicio al servicio de forma inmediata.

Identificamos tus Vulnerabilidades

- Delimitamos tus activos a monitorizar.
- Clasificamos los activos en base a diferentes indicadores internos.
- Iniciamos su monitorización en modalidad 24/7.

Analizamos y documentamos los hallazgos

- Identificamos las nuevas vulnerabilidades.
- Eliminamos posibles falsos positivos.
- Evaluamos su puntuación CVSS.
- Analizamos la vulnerabilidad y evaluamos su viabilidad.

Comunicamos los resultados y proponemos mejoras

- Evaluamos y priorizamos las posibles medidas correctivas.
- Definimos diferentes recomendaciones de mejora.
- Comunicamos la vulnerabilidad para su corrección.

SOBRE ZEROLYNX

Proveedor europeo de Ciberseguridad e Inteligencia.
Global Top 100 Providers ranked 2023.

info@zerolynx.com

CYBERSECURITY MADE IN EUROPE