ATTACK SIMULATOR

¿Ud. sabía que ...

más del 90% de los ataques cibernéticos se ejecutan debido a factores humanos?

Sus empleados pueden ser los siguientes...
y seguramente no será divertido.

¿Su equipo está preparado contra los ataques vía e-mail?
Sorpréndelos con una simulación de ataques.

Nuestro objetivo es de corregir de una vez por todas las debilidades humanas.
Con una cuenta de Attack Simulator, su empresa puede realizar simulaciones de ataques vía correo electrónico o Windows y ver el comportamiento de sus empleados, así como si son susceptibles de ser atacados con técnicas de ingeniería social.

Recibir formación sobre seguridad informática y estar bajo situaciones de riesgo diariamente son dos cosas muy diferentes.

Sus empleados en la mayoría de los casos tienen poca experiencia en gestionar amenazas cibernéticas, en parte porque las técnicas y las situaciones van cambiando y los atacantes buscan aprovechar las vulnerabilidades humanas.

Simulamos los ataques y después informamos a sus empleados donde se han equivocado, y como protegerse en el futuro.

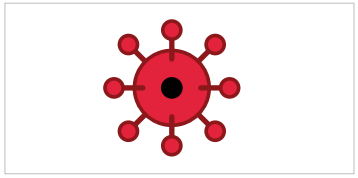
¿Sus empleados reconocen los ataques vía e-mail?

RANSOMWARE

PHISHING

ROBO DE IDENTIDAD

¿Y los ataques de PC?



MALWARE

ADWARE

SPYWARE

ATTACK SIMULATOR

Foco de Proyecto

VULNERABILIDADES HUMANAS

Programa de concienciación en ciberseguridad; identificamos situaciones de riesgo, asesoramos a sus empleados y proporcionamos informes detallados a la gerencia

REDUCCIÓN DE COSTES

A través de la automatización; Automatizamos la mayor parte de los ataques simulados y generamos informes detallados

REDUCCIÓN DE RIESGO

Personalizamos los ataque por cada grupo de usuarios y medimos la evolución de manera independiente, permite reducir considerablemente el riesgo de su empresa

Características Principales

- ASESORÍA EN CIBERSEGURIDAD
- ANÁLISIS DE COMPORTAMIENTO AUTOMATIZADO
- PROGRAMA DE EDUCACIÓN CONTINUA
- ATAQUES PERSONALIZADOS Y CONSEJOS

MANTENGA A SUS EMPLEADOS ALERTA CON ATAQUES CIBERNÉTICOS SIMULADOS DIRECTAMENTE EN SUS DISPOSITIVOS

CoASAR – Metodología propia de security awareness

CONTINUOUS

Proceso continuo de concienciación de la seguridad

ANALYZE

Analizamos y actualizamos los ataques simulados con las últimas amenazas de seguridad

SIMULATE

Simulamos el envío de los ataques reales y actuales. TODO AUTOMATIZADO y sin la intervención del responsable de TI

ASSESS

Evaluamos el riesgo de la empresa y de cada usuario, detallando los informes por cada departamento o empleado

REINFORCE

Ayudamos a implementar un programa continuo de CONCIENCIACIÓN que complementamos con webinars y consejos sobre la seguridad informática