

ATTACK SIMULATOR

Security awareness training from your inbox



¿Ud. sabía que ...

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

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

Metodología propia de security awareness – CoASAR



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



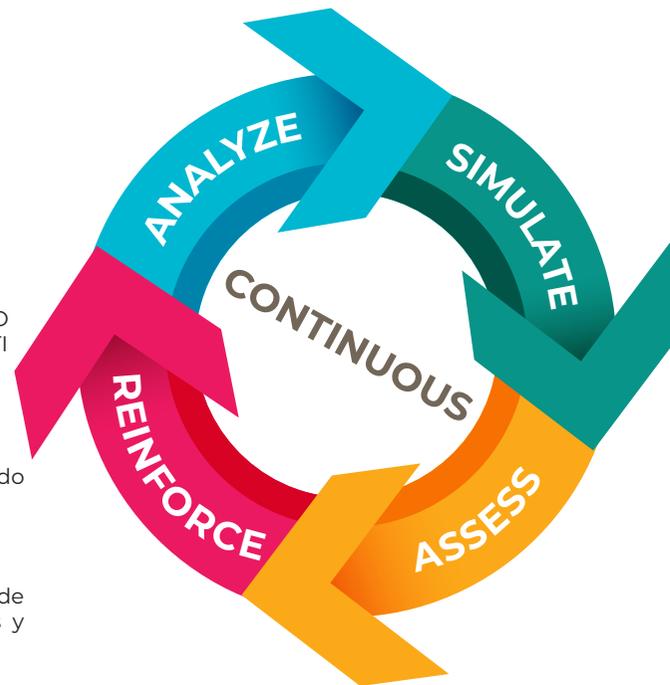
ASSESS

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



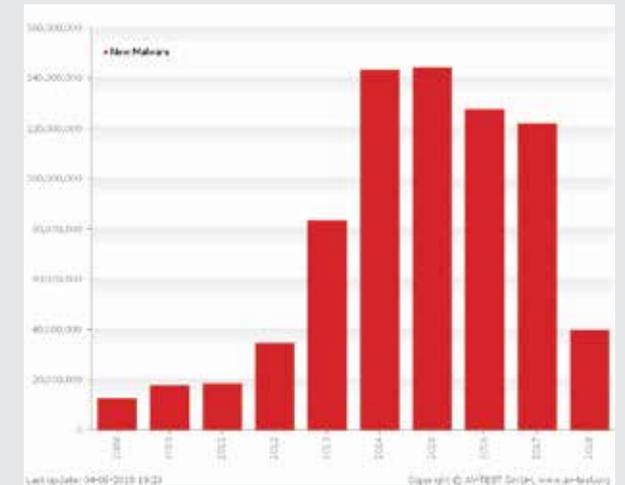
REINFORCE

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



Nuestro servicio es totalmente automatizado y transparente tanto para los responsables de TI y seguridad, como para los auditores internos y externos

+ 250.000 nuevas amenazas al DÍA
+30.000 amenazas sin detectar por las soluciones de seguridad cada MES



Ante esta situación, la formación y la concienciación de sus EMPLEADOS en temas de ciberseguridad se convierten en iniciativas básicas y fundamentales.

Attack Simulator es una herramienta CLOUD que permite al responsable de seguridad de la empresa crear un programa personalizado de CONCIENCIACIÓN en tan sólo unos minutos.

TODO EL PROCESO ES AUTOMATIZADO Y NO REQUIERE DE CONOCIMIENTOS TÉCNICOS PARA SU IMPLEMENTACIÓN.

ORIENTADO HACIA EL USUARIO

- Lo único que debe hacer el responsable de TI es agregar a los usuarios y sus funciones en la plataforma de Attack Simulator. Nosotros nos encargamos de analizar y adaptar los ataques a su perfil;
- Programa de concienciación en fases:
 - Riesgo Inicial - el usuario no sabe que está integrado en un programa de educación
 - Ataques simulados con diferentes niveles de dificultad
 - SEGURIDAD SOMOS TODOS - es el momento de involucrar a los empleados a proteger la empresa
 - Cada ataque tiene una lógica y sus indicadores de seguridad se miden de forma automática
 - Para cada tipo de ataque presentamos trucos para detectarlos (síntomas) y consejos para detectar futuras amenazas

En Seguridad, la formación y concienciación debe ser un programa continuo según nuestra visión y experiencia. Por esto hemos diseñado y preparado la metodología en un ciclo continuo (CoASAR) que toma en consideración tanto el progreso del usuario como las evoluciones y tendencias de las amenazas.

BENEFICIOS

-  **Automatizado** - Todo el programa de concienciación viene pre-configurado con todos los ataques simulados, las páginas web falsas implementadas y con el sistema de envío automatizado
-  **Resultados precisos y medibles** - Garantizamos la reducción del riesgo de seguridad. Informes disponibles para cumplir con los estándares y regulaciones actuales

 **Personalización** - El programa de concienciación se adapta por país y empresa. También se utilizan mensajes supuestamente internos para engañar al usuario

 **Comodidad** - Muy fácil de implementar y utilizar. No requiere asignar recursos adicionales. Puesta en marcha inferior a 30 minutos.



Los ataques simulados vía correo electrónico incluyen:

- Reconocer ataques de phishing
- Protección de contraseñas
- Descargas de Internet
- Ficheros Adjuntos
- Redes Sociales
- Protección de Datos
- Instalación de Software
- Protección contra Fraude
- Respuesta a incidentes

Y mucho más ...

**ATTACK
SIMULATOR**

Security awareness training from your inbox



Disponibilidad - A través de su partner habitual