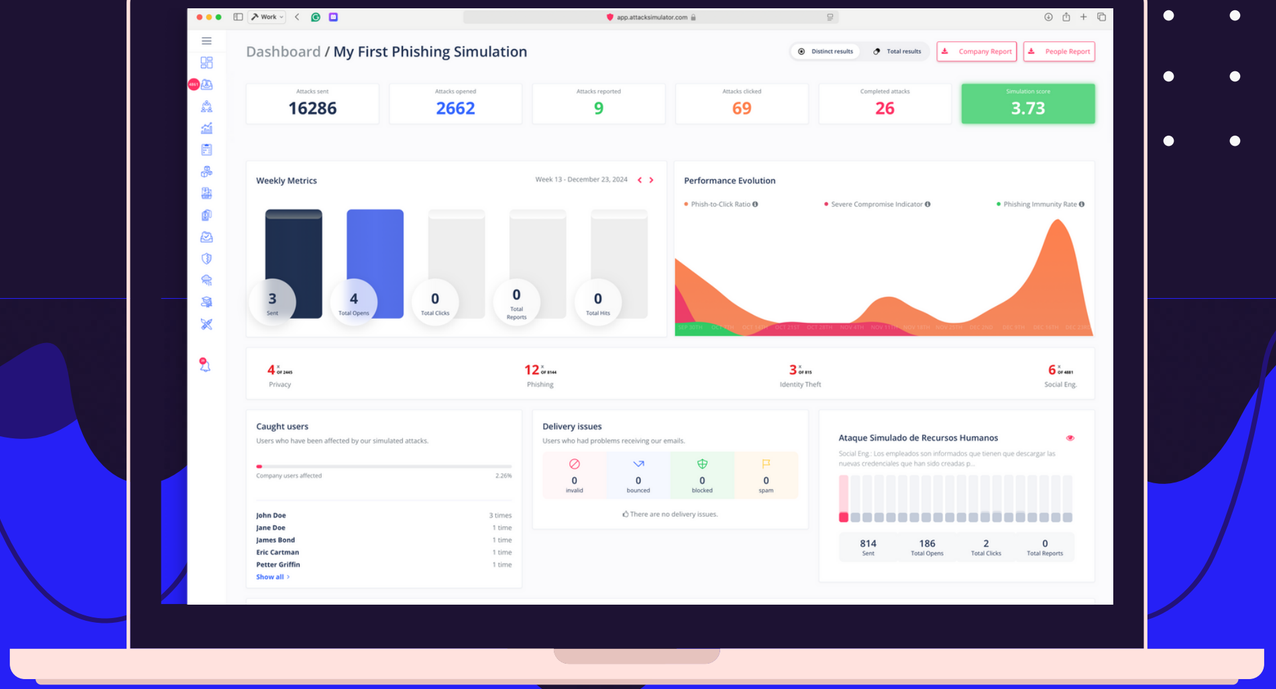
ATTACK SIMULATOR

2025

Concienciación en ciberseguridad basada en formación y entrenamiento interactivo continuo

NIS2, ENS, Kit Digital, ISO 27001



ATTACK Simulator es una plataforma automática de concienciación sobre seguridad que utiliza simulaciones de phishing para entrenar a los empleados en cómo reconocer, evitar y mitigar amenazas de ciberseguridad.

Acerca de ATTACK Simulator

Attack Simulator es una empresa con sede en Rumanía, país donde y como ejemplo tiene su sede el Centro Europeo de Competencia Industrial, Tecnológica y de Investigación en Ciberseguridad.

Colaboración con DNSC

ATTACK Simulator colabora con el Dirección de Ciberseguridad y la policía nacional de Rumania para ayudar a sensibilizar a la población y las empresas rumanas sobre los riesgos en ciberseguridad.

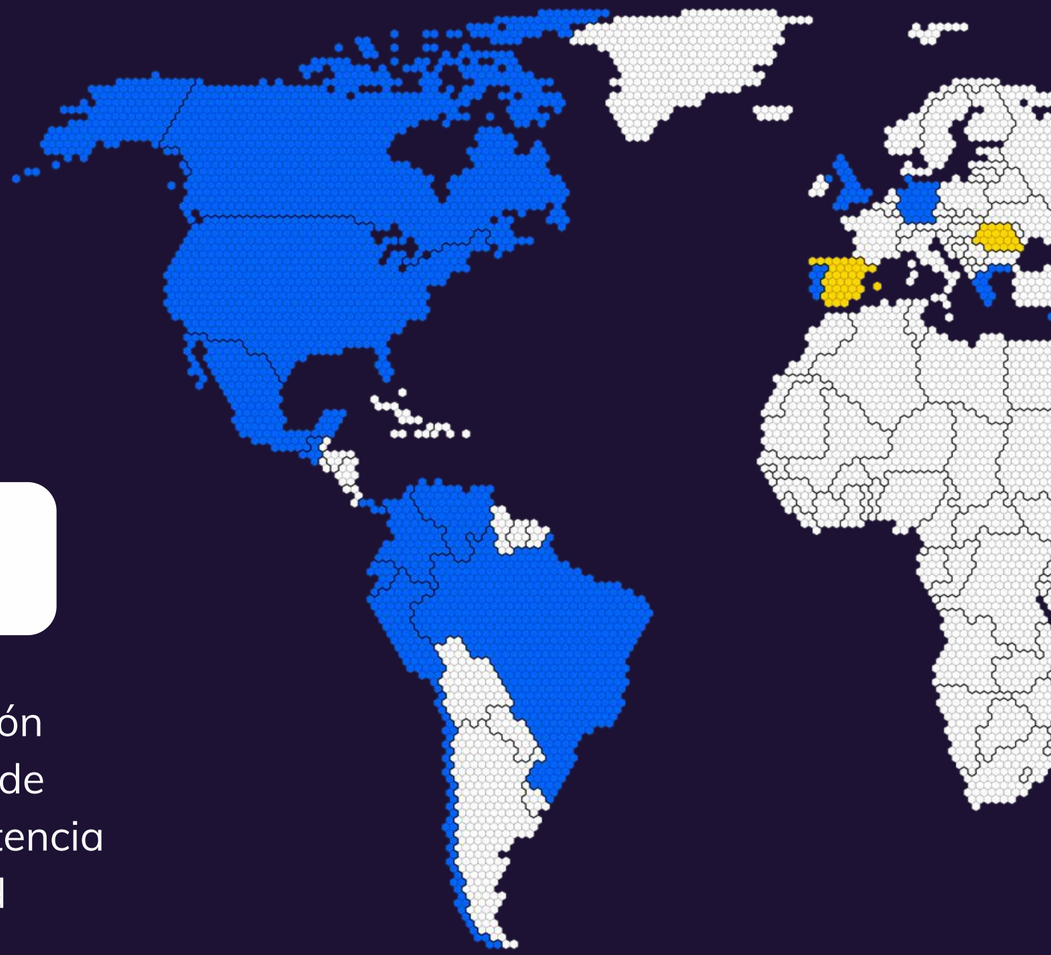
Mercado mundial

Aunque el desarrollo esta en Rumanía, la visión de ventas de ATTACK Simulator es global con claro foco en Estados Unidos y Europa

Producto maduro

Con más de 2000 clientes, ATTACK Simulator formó a más de 100000 empleados de con más de 500000 correos electrónicos simulados enviados.

Respaldado por Líderes en Ciberseguridad Alrededor del Mundo



Centro Criptológico Nacional de España certifica el manejo de información sensible en organizaciones del sector público

- Centro Criptológico Nacional
- Autoridad de máxima seguridad de España
- Valida la seguridad para el sector público

DIRECTORATUL NAȚIONAL DE SECURITATE CIBERNETICĂ

Recomendado por la Dirección Nacional de Ciberseguridad de Rumanía - procedente de la potencia europea en ciberseguridad

- La principal autoridad cibernética de Rumanía
- De la capital europea de la ciberseguridad
- Sede del Centro de Ciberseguridad de la UE (ECCC)

Diferentes tipos de concienciación

Charlas presenciales

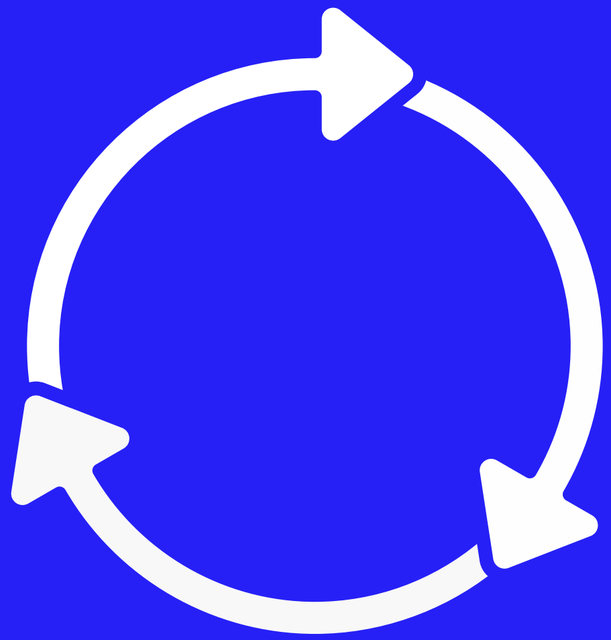
Para grupos reducidos y en momentos concretos

Cuatro simulaciones al año.

Con sus posteriores recomendaciones.

Cursos on-line gamificados.

Excelente manera de intentar transmitir conocimientos de ciberseguridad a todas las personas de una organización.



Entrenamiento interactivo continuo

Un servicio automatizado de prevención contra ciberriesgos que utiliza simulaciones realistas de ataques en España. Abordamos amenazas como ransomware, phishing y fraude centrándose en el factor emocional.

¿Por qué? Porque los ciberdelincuentes no triunfan por nuestra falta de formación, sino por cómo manipulan nuestras emociones - miedo, codicia y confianza. Al fin y al cabo, por mucho que estudiemos, seguimos siendo seres emocionales.

Propuestas de valor

del entrenamiento interactivo continuo y beneficios tangibles

Entrenamiento Interactivo Continuo

Mantiene a su equipo formado, alerta e informado todo el año mediante simulaciones de ciberataques enviadas directamente a sus dispositivos por email o SMS. Sin exámenes con fecha de caducidad que el subconsciente pueda olvidar.

Simulaciones Personalizadas

Envíe ataques simulados específicos por email (incluso desde su propio dominio) o SMS, de forma puntual o recurrente según sus necesidades.

Gestión y ROI

Informes detallados por empresa y usuario a través de consola cloud. Sin instalación ni requisitos adicionales de hardware o recursos operativos.

Programa Anual Preconfigurado

Sistema completamente automatizado con ataques simulados en fechas y horas aleatorias desde dominios variables. Incluye páginas web falsas, cuestionarios trimestrales y recordatorios, todo listo para usar.

Simulaciones Adaptadas a España

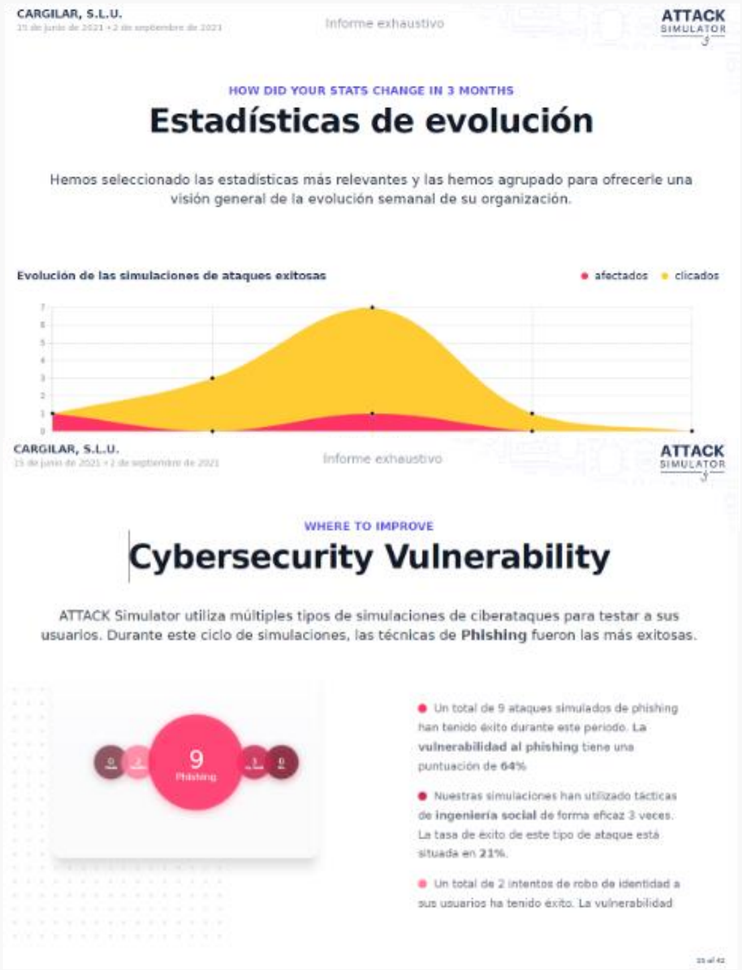
Ataques simulados diseñados específicamente para el contexto español, con opción de crear un plan de suplantación (spoofing) personalizado.

Cumplimiento Normativo

Compatible con NIS2, ENS, Kit Digital, ISO27001 y otras regulaciones relevantes.

ATTACK SIMULATOR

Informe exhaustivo trimestral



ATTACK SIMULATOR

Informes Completos

Acceda a reportes de empresa, usuarios, calificaciones, eventos y estadísticas, complementados con un informe exhaustivo trimestral.

Análisis de Vulnerabilidades

Identifique la principal debilidad en ciberseguridad de su organización y conozca el TOP25 de usuarios que requieren atención inmediata por nivel de riesgo.

Acción Preventiva Dirigida

Además de entrenar y concienciar, detectamos los puntos débiles en la cultura de ciberseguridad de su organización, permitiéndole enfocar acciones correctivas en las 25 personas con mayor riesgo.

ATTACK SIMULATOR

Alerta todo el año

Propuesta de plan anual de concienciación

1. Diagnóstico Inicial

Simulación personalizada que proporciona una fotografía del nivel actual de concienciación de los usuarios.

2. Entrenamiento Trimestral

Programa completo con envíos aleatorios, páginas falsas y píldoras formativas distribuido en cuatro trimestres. Cada periodo concluye con un cuestionario y genera un informe detallado de las principales vulnerabilidades.

3. Refuerzo Específico

Al identificar las vulnerabilidades, se programan una o dos simulaciones personalizadas como refuerzo en las áreas más críticas.

4. Formación Adicional

Opción de inscribir en la plataforma de e-learning a los usuarios que requieren atención prioritaria.

5. Campañas SMS

Posibilidad de enviar una o varias campañas por SMS para determinados usuarios que necesitan un canal adicional de sensibilización.

Servicios 2025

Innovación y protección integral para los desafíos del mañana

- Simulaciones puntuales o recurrentes por email.
- Simulaciones puntuales o recurrentes por SMS.
- Auditorias pre y/o post.
- Plataforma de elearning.
- Formación por capítulos por email (No Ransomware)
- Programa completo anual de concienciación:
  - Versión Pro (hasta 250 usuarios).
  - Versión Enterprise.
- Servicios profesionales (para partners).

ATTACK Simulator

ATTACK SIMULATOR

Cuadro comparativo de versiones

Descripción de funcionalidades de las versiones	Pro	Enterprise	Enterprise '25
Duración	1 / 2 / 3 años		
Entrenamiento interactivo continuo			
Campaña de phishing para evaluar el nivel de concienciación de los usuarios automatizada con informe ejecutivo	Si	Si	Si
Posibilidad de con una única consola de empresa, tener diferentes grupos, idiomas y programas	Si	Si	Si
Hasta 20 simulaciones de ataques trimestrales por e-mail por usuario, totalmente automatizadas y aleatorias	Si	Si	Si
Informe exhaustivo trimestral, las vulnerabilidades de los usuarios concretas en cada organización, etc.	Si	Si	Si
Escaneo de brechas de datos de las cuentas de email, tanto filtraciones, como publicaciones	Si	Si	Si
Smart Groups automatizados con el rendimiento/riesgo en usuarios	Si	Si	Si
Plataforma de e-learning, complementaria a las píldoras formativas	Si	Si	Si
Plataforma de e-learning con nuevos cursos, complementaria a las píldoras formativas	No	No	Si
Nuevos contenidos en las simulaciones, páginas de aterrizaje, etc.	No	No	Si
Funcionalidades adicionales			
Posibilidad de adquirir créditos para simulaciones de ataques vía SMS y/o servicos profesionales, €	Si (x)	Si (x)	Si (x)
Creación de identidad del remitente, envío posible desde varios dominios	Si	Si	Si
Simulaciones de ataques via e-mail personalizables en el envío y en el contenido a mostrar al "picar"	Si (12)	Si (∞)	Si (∞)
Posibilidad de servicio profesional de simulaciones de ataques via e-mail personalizables, €	Si	Si	Si
Posibilidad de servicio profesional de simulaciones de ataques via e-mail personalizables con spoofing y alojamiento, €	No	Si	Si
Agregación / autenticación del dominio del cliente	No	Si	Si
Integración con Active Directory, local y cloud	No	Si	Si
Integraciones via API con Office 365 y Google Workspace para entregas directa a las bandejas de entrada	Si	Si	Si
Posibilidad de Spoofing, tanto en el entrenamiento interactivo como en las en simulaciones personalizadas	Si	Si	Si
Reunión con el fabricante para preparar el inicio del servicio, detalles del mismo, puesta en marcha,etc.	Si	Si	Si
Visibilidad gráfica en consola con solo tres clicks de simulaciones de ataques con éxito y con qué plantilla	No	Si	Si
Reuniones trimestrales con el fabricante para análisis de resultados, propuestas y sugerencias, el primer año	No	Si	Si
Reuniones trimestrales con el fabricante para análisis de resultados, propuestas y sugerencias, todos los años	No	No	Si
Acceso a la API de Attack Simulator (integradores, MSSP)	No	Si	Si
Posibilidad de añadir white label y que solo salga el logo y dominio del cliente (integradores, MSSP, €)	No	Si	Si
Soporte			
Soporte por e-mail	Si	Si	Si
Soporte por e-mail y teléfono	Si	Si	Si
Soporte preferente por e-mail, teléfono y en caso de necesidad, con reunión remota	No	Si	Si

ATTACK SIMULATOR

¿Por qué concienciar con ATTACK Simulator?

1

ATTACK Simulator **ofrece 4 "vías" interconectables en lugar de una sola** para una mayor eficacia, combinando entrenamiento y creación de hábitos para abordar el factor emocional humano.

2

ATTACK Simulator es una empresa **100% focalizada en concienciación** y formación en seguridad y **no un producto complementario a otros.**

3

ATTACK Simulator supera las limitaciones de los cursos online tradicionales, donde el conocimiento se olvida tras aprobar el examen, independientemente de su duración o contenido.

4

ATTACK Simulator proporciona **entrenamiento interactivo continuo**, manteniendo a los miembros de su organización formados, informados y ALERTA TODO EL AÑO frente a riesgos y ataques de ciberseguridad.