ATTACK SIMULATOR

Fortaleciendo al Factor Humano

Nuestra misión:
Masificar la cultura de ciberseguridad en cada empresa

La Ciberseguridad es importante

La ciberseguridad abarca todo lo relacionado con la protección de nuestra información personal, la propiedad intelectual, los datos y los sistemas de información gubernamentales e industriales, contra el robo y los daños que procuran realizar delincuentes y adversarios.

Los colaboradores reciben **121 correos electrónicos falsos** al día.
Lo que nos lleva a superar el trillón de éstos al año.

Los ataques de phishing están en su nivel más alto en tres años, llegando a **3.4 billones** de incidentes en el último año.

En los últimos tres años hubo más de 160.000 incidentes de alto nivel, ocasionando **26 Billones de dólares en perdidas** el último año.

La Ciberseguridad es difícil

y la pandemia, con las nuevas medidas de trabajo desde casa, solo empeora las cosas.

El software no es suficiente

El software de seguridad suele ser demasiado complejo y costoso; además en muchos casos no protege completamente contra amenazas de día cero, en las que el usuario final juega el papel más importante.

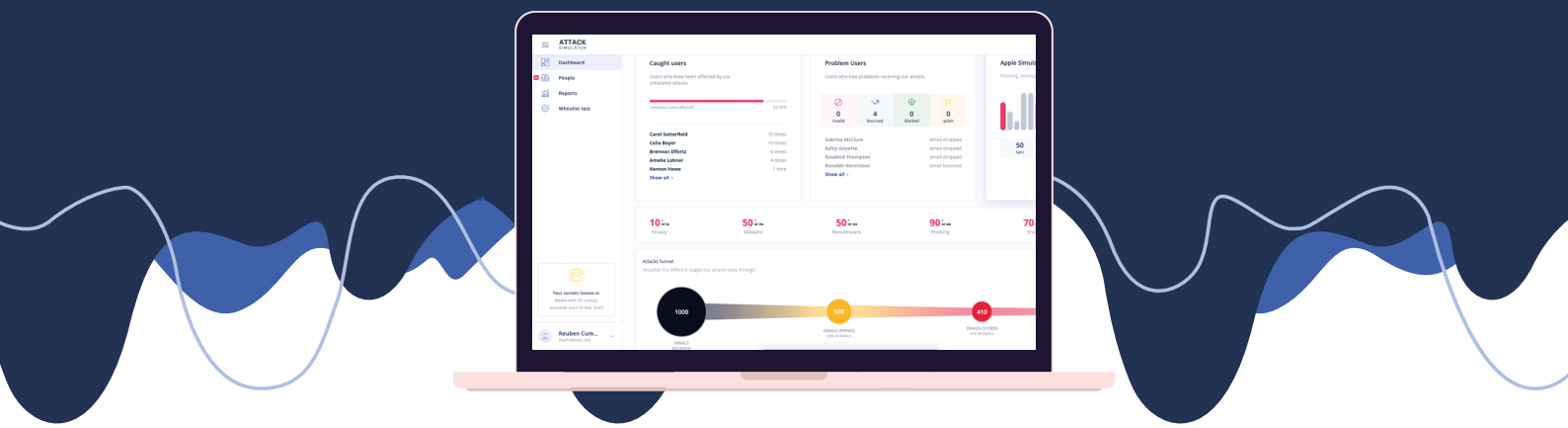
El factor humano y su rol

Las acciones de los colaboradores a menudo conducen a incidentes de ciberseguridad. La mayoría de los empleados tienen poco o ningún conocimiento de seguridad.

El training tradicional y sus problemas

La formación clásica en ciberseguridad es muy costosa, lo que la deja fuera del alcance de pequeñas y medianas empresas; las grandes empresas también tienen problemas, porque suelen ser muy complicadas y demandantes.

ATTACK
SIMULATOR



Los pilares de ATTACK Simulator

ATTACK Simulator es un programa de evaluación y capacitación en ciberseguridad, basado en los requerimientos de empresas de todo tamaño y sector, y deseñado para transformar la manera en que sus empleados entienden y manejan la seguridad.

Automático

Comenzar una simulación es fácil: basado en el perfil de su compañía, seleccionamos inteligentemente un conjunto de correos electrónicos para enviar a sus empleados

Avanzado

Simulamos toda la experiencia de phishing, permitiendo a los empleados entender mejor los riesgos y cómo protegerse de ellos.

Fácil de implementar

Puesta en marcha en menos de 30 minutos. Consola de gestión en la nube. No se requiere ningún hardware o recursos operativos adicionales.

Recomendado por

1

Empresas que han sufrido un ciberataque y están familiarizadas con las consecuencias.

2

Empresas que estuvieron a punto de sufrir las consecuencias de un ataque y tuvieron una visión de lo que podía suceder.

3

Empresas que requieran un cumplimiento normativo como ISO27001, ENS, GDPR, PCI-DSS, etc.

ATTACK
SIMULATOR

Nuestros Planes

Evaluación

AUDITORÍA

Funciona como introducción al mundo de la concientización sobre ciberseguridad.
Si elige este plan, tendrá acceso a:

- Una simulación de auditoría
- Informes de usuario estándar
- Asistencia al cliente por correo electrónico

Essentials

INTRO

Aparte que funciona como una introducción al mundo de la concientización en ciberseguridad, el Plan Essentials ofrece acceso ilimitado a ataques de phishing automatizados de larga duración.
Es prácticamente un aumento del Plan de Evaluación, repleto de:

- Simulaciones ilimitadas de auditoría
- Informes de usuarios
- Atención al cliente por correo electrónico y por teléfono.

Pro

CUMPLIMIENTO

El Plan Pro es nuestro primer plan que **incluye acceso a la plataforma educativa**, una simulación personalizada y acceso a varios administradores.

Al elegir este plan, se le concede acceso a los **recursos de concientización de seguridad** necesarios para el **cumplimiento de la certificación.**

Enterprise

ALTA GAMA

El plan Enterprise ofrece **acceso ilimitado a todas las funciones**, junto con herramientas de gestión avanzadas, como **integración de Active Directory.**

Además, al optar por el Plan Enterprise tendrá acceso a la **API de ATTACK Simulator**, lo que permite una mayor integración de nuestros servicios.

También recibirá acceso a nuestro **complemento de alerta de phishing** por correo electrónico para informar de actividades sospechosas directamente desde su buzón.

Solicite su cotización ¡AHORA!

+593 (02) 2444451

ventas@attacksimulator.lat

www.attacksimulator.lat

Isla Seymour N44-160 y Río Coca
Quito, Ecuador.

ATTACK
SIMULATOR