ATTACK
SIMULATOR

Human is the weakest link

Attack Simulator

Concienciación en ciberseguridad basada en entrenamiento interactivo continuo

Attack Simulator

Resumen de la presentación:

- Introducción.
- Propuesta de valor.
- Informes y ROI.
- Cuadro comparativo de versiones y servicios.
- Ayudamos a las personas para ayudar a las organizaciones.
- Ayudamos en la concienciación en ciberseguridad automatizando todo el plan anual.
- ¿Preguntas? ¿Siguientes pasos?

Introducción

- Attack Simulator es un servicio de entrenamiento interactivo continuo y automatizado de concienciación, para la prevención de riesgos en ciberseguridad, basado en ataques simulados con varios niveles de complejidad como por ejemplo: Ransomware, Phishing, Malware, Exploits, Privacidad, Fraude, etc.

- Attack Simulator mantiene formado, informado y alerta TODO el año al personal de la organización sobre los riesgos y ataques en ciberseguridad, simulándolos directamente en sus dispositivos, ya sea por email o por SMS.

- Attack Simulator, auditoría inicial. Como los ciberdelincuentes para tener éxito usan las emociones que provocan en los usuarios, principalmente el miedo, la codicia, la confianza, etc., ¿qué creéis que ocurre cuando hacemos una auditoría a un posible cliente que hace 4 u 8 meses acabo un curso online con muchos capítulos y horas, con su examen final para "acabar" y empezar a olvidar, si mandamos un phishing que produzca miedo al usuario? 😇

Propuesta de Valor: El diferencial de la automatización y beneficios tangibles

- **Automatización de programa anual de Security Awareness.** Todo el programa de concienciación viene pre-configurado con todos los ataques simulados, con fecha y hora de envío aleatorios desde dominios de envío también aleatorios. Páginas web falsas implementadas y con todo el sistema de envío automatizado.

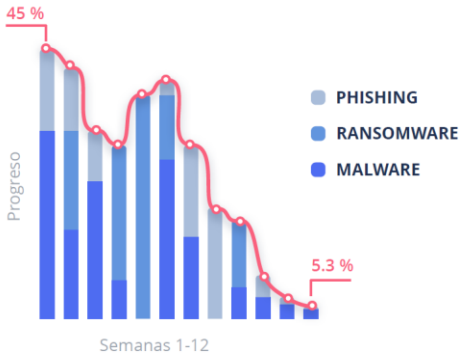
- **Posibilidad de enviar simulaciones personalizables.** Tanto por email (incluso desde el dominio del cliente) como por SMS, el cliente puede diseñar y enviar sus propias simulaciones o escoger entre las plantillas que hay para tal efecto.

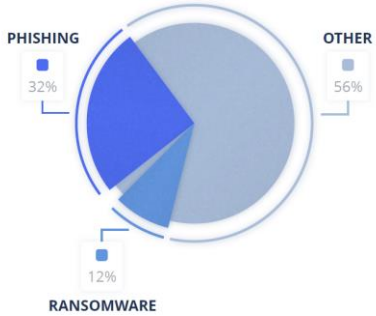
- **Adaptación.** Plan de Phishing adaptado a España y plan de spoofing customizado por empresa.

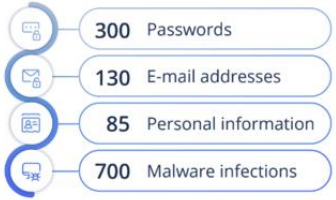
- **Gestión y ROI.** Resultados precisos y medibles. Informes detallados por empresa y por usuarios. Dashboard de reportes granulares automatizados que evidencian la disminución gradual del riesgo en los usuarios y la efectividad del programa de Security Awareness. Consola de gestión cloud. No requiere recursos operativos o de hardware adicionales.

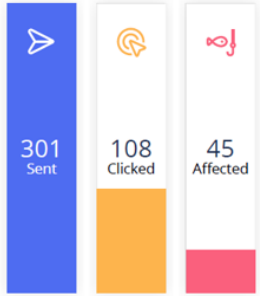
- **Cumplimiento de Normatividad.-** Con nuestros servicios, la organización cumple con auditorías y en general con cualquier obligación en Security Awareness ligada a certificaciones de ciberseguridad como ENS e ISO27001, etc.

Informes y ROI



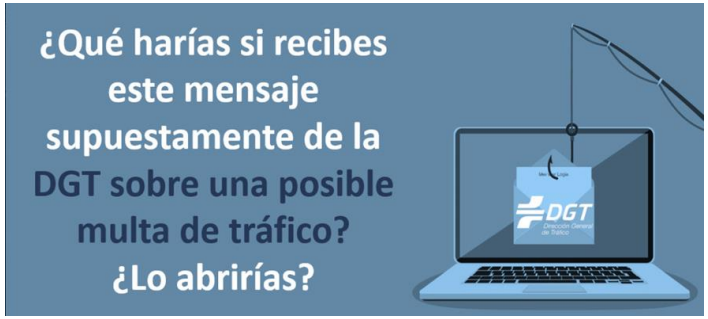






Attack Simulator 2021 - Cuadro comparativo de versiones

Funcionalidades	Evaluation	Essentials	Pro '21	Enterprise '21
Duración	1-2 Semanas	1 / 2 / 3 años	1 / 2 / 3 años	1 / 2 / 3 años
Automatización				
Auditoría de seguridad de phishing automatizada	Si	Si	Si	Si
Simulaciones de ataques por e-mail	Si	Si	Si	Si
Informes de usuarios y de empresa	Si	Si	Si	Si
Sugerencias y consejos automatizados	No	Si	Si	Si
Plataforma de e-learning	No	No	Si	Si
Otros				
Creación de grupos de usuarios	No	No	Si	Si
Múltiples administradores	No	No	Si	Si
Sim. ataques via e-mail personalizables / usuario	No	No	Si (6)	Si (24)
Simulaciones de ataques via SMS / usuarios	No	No	Si (n)	Si (4n)
Pluguin para Outlook y Gmail	No	No	Si	Si
Creación identidad del remitente	No	No	Si	Si
Agregación / autenticación de dominio	No	No	No	Si
Integración con Active Directory	No	No	No	Si
Acceso a la API de Attack Simulator	No	No	No	Si
Soporte				
Soporte por e-mail	Si	Si	Si	Si
Soporte por e-mail y teléfono	No	No	Si	Si
Soporte preferente por e-mail y teléfono	No	No	No	Si



Attack Simulator

Ayudamos a las personas para ayudar a las organizaciones

Imagina que te llega este correo a tu nombre. ¿Lo abrirías?

Sr./Sra. xxx, en el lugar, fecha y hora señalados en el archivo que se puede descargar en el enlace adjunto, ha sido detectada la circulación de un vehículo de su titularidad a una velocidad superior a la legalmente establecida en dicha vía según el código de circulación vigente.

Casi el 60% de los empleados abrirían ese tipo de correos, como se puede ver en la siguiente tabla donde se muestra la situación real de una empresa de más de 400 empleados.

TIPO DE EMAIL	ENVIADOS	ABIERTOS	INFECTADOS	PORCENTAJE DE INFECTADOS
Ataque simulado Facebook – **Phishing**	409	43	6	15%
Ataque simulado de File Sharing – **Phishing**	409	61	16	25%
Ataque simulado de CEO – **Ingeniería Social**	409	90	41	46%
Ataque simulado de Recursos Humanos – **Ingeniería Social**	409	170	149	88%
TOTAL	**1636**	**365**	**212**	**58%***

Attack Simulator

Ayudamos primero con una auditoría gratuita

Evaluación del estado real del nivel de concienciación de todas las personas de una organización o empresa.

- Evaluación compuesta por hasta cuatro simulaciones de ataques en dos semanas, de manera automatizada y aleatoria, sin límite de usuarios y sin ningún coste.
- Comprobamos primero si es fácil acceder a los usuarios.
- Posteriormente se lanza la evaluación para obtener una "fotografía" de como responderían si les llegan determinados tipos de correos.
- Se entregan dos informes, uno gráfico ejecutivo y otro textual descriptivo de la "fotografía" obtenida.
- El objetivo es ayudar a concienciar a quien corresponda de la organización de que se debe concienciar en ciberseguridad a todos los usuarios, para ello y mediante los informes, se muestra de manera real, su situación actual.

Attack Simulator

Ayudamos en la concienciación en ciberseguridad automatizando todo el plan anual

Attack Simulator es un servicio de entrenamiento interactivo continuo y automatizado de concienciación para la prevención de riesgos en ciberseguridad, basado en ataques simulados con varios niveles de complejidad como por ejemplo: Ransomware, Phishing, Malware, Exploits, Privacidad, Fraude, etc.

Attack Simulator mantiene formado, informado y alerta TODO el año al personal de la organización sobre los riesgos y ataques en ciberseguridad, simulándolos directamente en sus dispositivos, ya sea por email o por SMS.

- **Automatización de programa anual de Security Awareness.** Todo el programa de concienciación viene pre-configurado con todos los ataques simulados, con fecha y hora de envío aleatorios desde dominios de envío también aleatorios. Páginas web falsas implementadas y con todo el sistema de envío automatizado.

- **Posibilidad de enviar simulaciones personalizables.** Tanto por email (incluso desde el dominio del cliente) como por SMS, el cliente puede diseñar y enviar sus propias simulaciones o escoger entre las plantillas que hay para tal efecto.

- **Gestión y ROI.** Resultados precisos y medibles. Dashboard de reportes granulares automatizados que evidencian la disminución gradual del riesgo en los usuarios y la efectividad del programa de Security Awareness. Consola de gestión cloud. No requiere recursos operativos o de hardware adicionales.

- **Algunos servicios:**

- 80 Simulaciones de ataques anuales automatizadas y randomizadas con páginas web falsas, píldoras formativas y cuestionarios trimestrales, por cada usuario.
- Simulaciones de ataques vía email o SMS, personalizables en el envío y en el contenido a mostrar al caer en la simulación.
- Pluguins para Outlook y Gmail.
- Creación identidad del remitente, envío posible desde varios dominios.
- Agregación / autenticación de dominio del cliente.
- Plataforma de e-learning gratuita y complementaria a las píldoras formativas.
- Integración con Active Directory.
- Acceso a la API de Attack Simulator.

ATTACK
SIMULATOR

Human is the weakest link

¿Preguntas?

¿Siguientes pasos?