TÉRMINOS Y CONDICIONES DEL SERVICIO DE CIBERPATRULLAJE

Ofrecemos servicios especializados de Ethical Hacking también conocido como Pentesting o Pruebas de Penetración. Se trata de un servicio de ciberseguridad que simula ataques reales a los sistemas, redes o aplicaciones de una organización para identificar vulnerabilidades que podrían ser explotadas por atacantes malintencionados, cuyos principales objetivos son:

1. **Ciber Patrullaje**: Es un servicio de monitoreo, el cual puede ser continuo o por evento único (duración de 24 horas) que implica la vigilancia proactiva de del entorno digital para identificar y mitigar posibles amenazas. Este servicio incluye:

   - **Monitoreo de la Web**: Supervisión de sitios web públicos y foros en busca de amenazas y actividades maliciosas.
   - **Monitoreo de Redes Sociales**: Vigilancia de plataformas de redes sociales para identificar menciones, amenazas o actividades relacionadas extorsiones**.**
   - **Monitoreo de la Dark y Deep Web**: Exploración de áreas de la dark y deep web para detectar menciones de datos del Cliente o posibles actividades delictivas que puedan afectar al Cliente.

   Notros te notificaremos sobre amenazas detectadas y te ofreceremos recomendaciones. Sin embargo, no garantizamos la detección de todas las amenazas, ni que las amenazas detectadas serán mitigadas eficazmente.

   Objetivo: Proporcionar alertas tempranas y sugerir acciones para reducir riesgos.

2. **CiberInteligencia**: Se enfoca en recolocar y analizar información del entorno digital para anticipar y prepararse para posibles amenazas. Incluye:

   - **Recolección de Información**: Obtención de datos relevantes de diversas fuentes digitales, como Internet, redes sociales, dark y deep web.
   - **Análisis de datos**: Evaluación de la información recolectada para identificar patrones de amenaza y generar informes detallados.
   - **Recomendaciones Estratégicas**: Provisión de recomendaciones basadas en el análisis para anticipar amenazas y mejorar tu seguridad.

   No garantizamos la recolección de toda la información relevante ni de la exhaustividad o precisión del análisis.

   Objetivo: Ofrecer perspectivas estratégicas y recomendaciones prácticas para prevenir amenazas futuras.

3. **Protección de la Marca en la Web**: El Servicio de Protección de la Marca en la Web está orientado a salvaguardar la reputación e integridad de tu marca en el entorno digital. Incluye:

   - **Vigilancia de Marca:** Supervisión de la web y las redes sociales para detectar el uso no autorizado de la marca, como sitios web falsos o uso indebido de logotipos y nombres.
   - **Detección de Sitios Apócrifos:** Identificación de sitios web fraudulentos que imitan o suplantan la marca del Cliente con fines maliciosos.
   - **Suplantación de Identidad en Redes Sociales:** Monitoreo de perfiles y páginas falsas que utilicen la marca del Cliente de manera indebida.
   - **Defensa de la Reputación:** Respuesta a incidentes detectados, incluyendo coordinación con plataformas para la eliminar contenido falso.

   Objetivo: Preservar la reputación de tu marca y prevenir el uso indebido de su identidad en el entorno digital.

PLAZO DE CONTRATACIÓN DE SERVICIOS

1. **Anual:** Si la contratación se maneja bajo un esquema anual incluye:
   - **Monitoreo Continuo:** Incluye monitoreo continuo de sistemas, redes y otras áreas relevantes del entorno digital del Cliente, para detectar amenazas y vulnerabilidades en tiempo real.
   - **Notificación y Generación de Boletines:** Ante la detección de vulnerabilidades o actividades sospechosas, Te notificaremos de manera inmediata y genera boletines con la información necesaria para mitigar los riesgos detectados.
   - **Informes Periódicos:** Se entregarán informes mensuales y trimestrales detallando las actividades realizadas, amenazas detectadas, acciones correctivas sugeridas y el estado general de la seguridad del Cliente.
   - **Duración y Continuidad:** El servicio es anual y se renueva automáticamente, salvo que ambas partes acuerden lo contrario.

2. **Evento Único:** Este servicio está limitado a una seré de actividades especificadas y realizadas dentro de un cronograma acordado entre las partes.
   - **Entregables:** Se entregan solo 2 reportes. Son los siguientes:
   - **Reporte Ejecutivo:** Que contiene: (i) El resumen de las principales amenazas detectadas durante el evento, (ii) Un análisis general de la situación de seguridad del Cliente y las posibles implicaciones para su negocio, y (iii) Recomendaciones y acciones que pueden tomarse para mitigar los riesgos detectados.
   - **Reporte Técnico:** Es un documento que contiene el detalle técnico de las vulnerabilidades detectadas y las acciones recomendadas. (i)Describe de manera precisa las vulnerabilidades o amenazas detectadas, incluyendo detalles técnicos como la naturaleza del ataque, el método utilizado, la gravedad y las áreas afectadas, (ii) Análisis detallado de los sistemas, redes o componentes comprometidos, (iii) Recomendaciones técnicas y acciones para mitigar riesgos y reforzar la seguridad de los sistemas a largo plazo.

3. **Tiempo Limitado (24 horas):** Al ser un servicio de duración limitada a 24 horas, no aplica monitoreo continuo ni seguimiento posterior, a menos que se acuerden servicios adicionales entre las partes.

ESPECIFICACIONES GENERALES DEL SERVICIO

Alcance del Servicio: El monitoreo incluirá, pero no se limitará a:

- Sitios web públicos y accesibles a través de motores de búsqueda estándar.
- Plataformas de redes sociales y foros en línea relevantes para la presencia y reputación del Cliente.
- Sitios y foros que no son accesibles públicamente (Dark web y Deep web) que requieran permisos especiales o navegadores específicos para acceder.
- Otros entornos digitales relevantes acordados por ambas partes.

Los servicios se entregan en función de la información y condiciones disponibles al momento de su ejecución. Debido a la naturaleza del entorno digital, siempre existe un riesgo residual los servicios proporcionados están diseñados para reducir dicho riesgo.

Límites de la responsabilidad: No será nuestra responsabilidad los fallos en los servicios debido a:

- Uso incorrecto o no autorizado de los servicios por parte del Cliente.
- Problemas técnicos fuera de nuestro control, como fallos en hardware, software o infraestructura del Cliente.
- Modificaciones o alteraciones no autorizadas realizadas por el Cliente.

1. Implementaremos medidas de seguridad estándar para proteger la información y los sistemas del cliente. Sin embargo, no garantiza que los servicios sean ininterrumpidos, libres de errores o completamente seguros frente a ataques o accesos no autorizados.

2. Los servicios se proporcionan "Tal Cual" y sin garantías adicionales, ya sean explicitas o implícitas y no aseguramos:
   - La detección de todas las amenazas o actividades maliciosas.
   - La recolección de toda la información relevante ni un análisis exhaustivo y sin errores.
   - La detección de todas las infracciones de marca o la efectividad total de las recomendaciones y/o acciones correctivas.
3. Entiendes que no seremos responsables por daños indirectos, incidentales, consecuentes, especiales, punitivos o ejemplares, incluyendo, pero no limitándose a la pérdida de ingresos, pérdida de beneficios, pérdida de datos, interrupción de negocio o cualquier otra pérdida económica.
4. No somos responsables por fallos en los servicios que resulten de (i) el uso incorrecto o no autorizado de los servicios por parte del Cliente, (ii) problemas técnicos que surjan fuera de nuestro control, incluyendo, pero no limitándose a fallos en el hardware, software o infraestructura, y (iii) cualquier modificación o alteración de los servicios de tu parte sin nuestra autorización previa.
5. Eres consciente y estás de acuerdo que implementaremos medidas de seguridad estándar de la industria para proteger tu información y sistemas; sin embargo, no garantiza que los servicios sean ininterrumpidos, libres de errores o completamente seguros contra todos los posibles ataques cibernéticos o accesos no autorizados.
6. No garantizamos la detección de todas las amenazas o actividades maliciosas y aceptas que no seremos responsables por la falta de detección de amenazas que puedan surgir después de la entrega del informe de Ciber Patrullaje.
7. No garantizamos que toda la información relevante será recolectada ni que el análisis será exhaustivo. Aceptas que no seremos responsables por cualquier decisión tomada basándose en la información o recomendaciones proporcionadas, ni por las consecuencias de posibles amenazas que no hayan sido anticipadas.
8. Entiendes que no garantizamos que todas las infracciones de marca serán detectadas ni que las acciones correctivas sable por el impacto de cualquier uso indebido de la marca o por la efectividad de las medidas tomadas para proteger la marca.
9. No ofrecemos garantías en cuanto a la exhaustividad, precisión o eficacia de los Servicios prestados. La aceptación de los Servicios de tu parte es a riesgo propio, y no nos comprometemos a proporcionar un nivel específico de desempeño o a prevenir todas las posibles amenazas.
10. Eres responsable de implementar las recomendaciones y acciones sugeridas por nosotros y no seremos responsables por los resultados de dicha implementación ni por cualquier impacto derivado de la adopción o falta de adopción de las recomendaciones.
11. Entiendes que no somos responsables por problemas, fallos o daños que resulten de la interacción de sus servicios con otros sistemas, servicios o productos no suministrados.
12. El Cliente es responsable por errores, omisiones o fallos causados por errores humanos de sus empleados, contratistas o agentes.

Confidencialidad:

1. Nos comprometemos a mantener la confidencialidad de toda la información nos sea proporcionada durante la prestación de los Servicios, incluyendo datos de sistemas, redes, y cualquier otra información técnica o empresarial revelada (en adelante, "Información Confidencial").
2. Por ningún motivo divulgaremos dicha Información Confidencial a terceros sin el consentimiento previo por escrito del Cliente, excepto en los casos en los que dicha divulgación sea requerida por ley, regulación o por una orden de una autoridad competente.
3. Utilizaremos la Información Confidencial únicamente para los fines específicos relacionados con la prestación del Servicio contratado y no para ningún otro propósito. La Información Confidencial no será utilizada para beneficio propio.
4. Implementaremos medidas de seguridad razonables para proteger la Información Confidencial contra el acceso no autorizado, la divulgación, la modificación o la destrucción utilizando controles físicos, técnicos y administrativos adecuados.

Colaboración y Notificación:

1. Trabajaremos estrechamente contigo, designando puntos de contacto específicos y estableciendo procedimientos de escalación para incidentes críticos.
2. En caso de detectar amenazas criticas o vulnerabilidades significativas, te notificaremos inmediatamente con detalles del incidente y las medidas correctivas recomendadas.

- **Acceso a Datos Personales:** Aceptas y estas consiente que, durante la realización de las pruebas de seguridad, podríamos tener acceso a datos personales del Cliente.
- **Demoras o Incumplimientos por causas fuera de Control:** No seremos responsables por demoras en el cumplimiento o por incumplimiento debido a causas fuera de su control razonable.
- **Acuerdo Completo entre las Partes:** Estos términos y condiciones, junto con el Contrato y la Propuesta, constituyen el acuerdo completo entre las Partes.

Cualquier modificación a los términos económicos, comerciales o legales del Servicio señalado, serán notificados por anticipado a los correos electrónicos referidos en el Contrato.