KRIPTERIA

BUSINESS INTELLIGENCE

# SERVICIOS INTEGRALES DE CIBERSEGURIDAD

# NUESTROS SERVICIOS

PLT y Red Team, nuestros dos pilares fundamentales en la ciberseguridad

## PLT

Anticipación y protección avanzada a través del monitoreo especializado de foros y grupos cerrados.

## RED TEAM

Evaluación de seguridad exhaustiva mediante simulaciones de ataque realistas para fortalecer su infraestructura cibernética.

KRIPTERIA

BUSINESS INTELLIGENCE

# INTRODUCCIÓN A PLT

En el corazón de nuestro servicio Proactive Listening Threads (PLT) yace una estrategia meticulosamente diseñada para la seguridad y el resguardo de información crítica. Este servicio único, llevado a cabo por nuestro equipo especializado, se enfoca en la monitorización constante de foros privados y grupos de acceso restringido.

KRIPTERIA
BUSINESS INTELLIGENCE

# ÁMBITOS DE MONITOREO EN PLT


Estos foros y grupos discuten una amplia gama de temas, desde accesos corporativos no autorizados, pasando por la venta de credenciales, hasta la distribución de información confidencial y preparativos de ataques cibernéticos. PLT cubre todo, asegurando un conocimiento profundo y actualizado de las amenazas emergentes.

KRIPTERIA
BUSINESS INTELLIGENCE

# ENFOQUE GEOLOCALIZADO DE PLT

PLT se distingue por su enfoque geolocalizado. Monitorizamos foros específicos en cada país, garantizando que la información recopilada sea relevante y aplicable a cada contexto regional. Esto nos permite identificar amenazas locales específicas, un aspecto clave para una seguridad efectiva.

KRIPTERIA
BUSINESS INTELLIGENCE

# PLT EN ACCIÓN

Con PLT, obtenemos acceso a información crítica, desde preparativos de estafas hasta negociaciones de vulnerabilidades. Esto nos permite anticipar y mitigar amenazas que podrían afectar tanto la seguridad financiera como la reputación corporativa

KRIPTERIA
BUSINESS INTELLIGENCE

# WHISPER SHOUTING


Whisper Shouting es nuestro sistema especializado para la detección de credenciales comprometidas. Utiliza capacidades de búsqueda profunda para monitorear fuentes ocultas en internet y la dark web, proporcionando alertas tempranas sobre posibles brechas de seguridad.

KRIPTERIA
BUSINESS INTELLIGENCE

# LA IMPORTANCIA DE LAS CREDENCIALES

Nuestro enfoque en la seguridad de las credenciales se centra en la monitorización activa de la red para detectar credenciales a la venta o filtradas. Esta vigilancia constante es parte esencial de nuestra estrategia de ciberseguridad. Al monitorear activamente los mercados y foros donde se comercializan credenciales comprometidas, podemos identificar y responder rápidamente a las amenazas, asegurando que sus credenciales estén protegidas contra accesos no autorizados y reduciendo significativamente el riesgo de ataques cibernéticos

KRIPTERIA
BUSINESS INTELLIGENCE

# RED TEAM: 7 PUNTOS PARA LA CIBERSEGURIDAD

Nuestro servicio de RED TEAM está meticulosamente estructurado en siete puntos esenciales, diseñadas para cubrir el espectro completo de la ciberseguridad. Reconocemos que en el mundo real, los atacantes no se enfrentan a límites; por ello, nuestro enfoque es exhaustivo y sin restricciones. Simulamos la tenacidad y la creatividad de los adversarios más decididos, empleando desde sofisticadas campañas de phishing hasta intrusiones físicas en las redes WiFi empresariales. Nuestra misión es pensar como un atacante para proteger como un guardián, garantizando que cada punto de contacto esté fortificado contra las amenazas más astutas y persistentes.

KRIPTERIA

BUSINESS INTELLIGENCE

# DESARROLLO DE HERRAMIENTAS PROPIAS

## Desarrollo de Herramientas Personalizadas

Usamos herramientas desarrolladas internamente, diseñadas para identificar vulnerabilidades específicas y patrones de comportamiento inusuales que las herramientas convencionales podrían pasar por alto.

## Explotación de Vulnerabilidades Únicas

Nuestras herramientas nos permiten explotar vulnerabilidades avanzadas, desde la manipulación de cookies para acceder a cuentas de usuario o fallos de programación que permiten modificar las solicitudes HTTP para controlar el comportamiento de las aplicaciones, hasta el desarrollo de POCs y exploits complejos.

KRIPTERIA

BUSINESS INTELLIGENCE

# INGENIERÍA SOCIAL E INFILTRACIÓN DE ALTO NIVEL

## Campañas de Ingeniería Social Avanzadas

Empleamos tácticas de ingeniería social personalizadas para evaluar la conciencia de seguridad de los empleados y la efectividad de los protocolos de seguridad internos.

## Simulaciones de Infiltración Física

Realizamos operaciones de campo para probar la seguridad física de las instalaciones, utilizando métodos innovadores adaptados a cada entorno específico.

KRIPTERIA
BUSINESS INTELLIGENCE

# PRUEBAS AVANZADAS DE PENETRACIÓN

## Evaluación de Seguridad de Red Personalizada

Nuestro enfoque en pruebas de penetración va más allá de lo convencional, utilizando técnicas y herramientas desarrolladas internamente para descubrir vulnerabilidades ocultas en la infraestructura de TI.

## Explotación de Red Compleja

Exploramos cada segmento de la red, cada script que se ejecuta, cada posible filtración de información, utilizando herramientas que pueden detectar anomalías sutiles y puntos de entrada inusuales.

KRIPTERIA
BUSINESS INTELLIGENCE

# PRUEBAS DE SEGURIDAD INALÁMBRICA

## Evaluación Exhaustiva de Redes Inalámbricas

Nuestro equipo realiza pruebas de seguridad inalámbrica que incluyen la identificación de vulnerabilidades en protocolos Wi-Fi, sistemas de comunicación Bluetooth y otros dispositivos inalámbricos.

KRIPTERIA
BUSINESS INTELLIGENCE

# ANÁLISIS FORENSE Y RESPUESTA A INCIDENTES

## Simulaciones de Incidentes Complejas

Creamos escenarios de ataque realistas para probar la capacidad de respuesta de la organización frente a incidentes de seguridad.

## Análisis Forense Avanzado

Utilizamos técnicas forenses sofisticadas para evaluar cómo se manejan los datos después de un incidente de seguridad y para mejorar las estrategias de recuperación.

KRIPTERIA
BUSINESS INTELLIGENCE

# REPORTES DETALLADOS Y ESTRATEGIA DE MEJORA

## Informes Exhaustivos y Personalizados

Proporcionamos informes detallados, destacando vulnerabilidades específicas encontradas y ofreciendo recomendaciones de seguridad a medida.

## Sesiones de Debriefing Estratégicas

Realizamos sesiones de análisis en profundidad con los equipos de seguridad y la alta dirección para discutir hallazgos y estrategias de mejora.

KRIPTERIA
BUSINESS INTELLIGENCE

# SEGUIMIENTO Y VERIFICACIÓN DE MEJORAS

## Revisión de Implementaciones de Seguridad

Realizamos un seguimiento para asegurarnos de que las recomendaciones de seguridad se implementen correctamente y se mantengan efectivas a lo largo del tiempo.

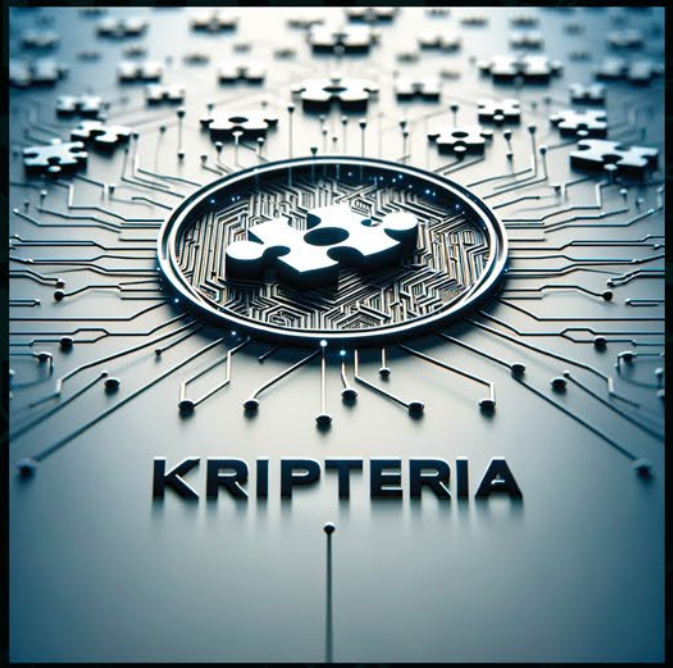
## Evaluaciones de Seguridad Periódicas

Ofrecemos pruebas de seguridad continuas para garantizar que la organización se mantenga protegida frente a las amenazas emergentes.

KRIPTERIA
BUSINESS INTELLIGENCE

# RESUMEN

PLT y Red Team son los pilares de nuestra estrategia integral de ciberseguridad. PLT ofrece vigilancia anticipada, monitoreando foros privados para detectar amenazas emergentes, mientras que Red Team evalúa activamente la robustez de sus defensas mediante simulaciones de ataques reales. Juntos, estos servicios garantizan una protección proactiva y reactiva completa, preparando a su empresa para enfrentar tanto amenazas conocidas como imprevistas en el cambiante entorno digital.




KRIPTERIA
BUSINESS INTELLIGENCE

# KRIPTERIA

BUSINESS INTELLIGENCE


| | |
|---|---|
| Página Web | kripteria.com |
| Email | info@kripteria.com |
| Teléfono | +34 910 56 59 27 |

C/ Profesor Waksman 5. 10D
28036 Madrid