# PREPARACIÓN ANTE EL RANSOMWARE

# **SOLUCIÓN** PROPUESTA

**Nuestros equipos de técnicos especializados han estado en primera línea de respuesta ante algunas de las brechas más complejas y ataques de mayor entidad de ransomware a nivel mundial.**

Esta experiencia consolidada, nos ha permitido adquirir un profundo conocimiento del "modus operandi" de los actores de las amenazas y, de cómo desarrollar rápidamente la resiliencia frente a estos ataques. Nuestro grupo de trabajo sobre ransomware, formado por expertos de máximo nivel y curtidos en mil operaciones, se asegurará de que su organización esté preparada para enfrentarse incluso a los ataques más avanzados.

La última tendencia, de los ciberatacantes se dirige a filtrar la información sustraída y, amenazan con publicar los datos robados para aumentar el éxito en el pago de rescates. Esto pone de relieve la necesidad de tomar medidas proactivas para reducir el riesgo de estos ataques.

## **MANTENGA ALEJADOS** A LOS GRUPOS DE RANSOMWARE

Minimizar el impacto del ransomware en su empresa.

Revele las debilidades que ponen en riesgo sus activos críticos.

Identificar las amenazas de ransomware y priorizar la respuesta.

> Nuestro grupo de trabajo sobre ransomware identifica acciones inmediatas, de alto impacto, que se pueden tomar para reducir significativamente la probabilidad de un ataque de ransomware y , aumentar asi la capacidad para resistir un ataque en caso de que ocurra.

Somos expertos en consultoría de **ciberseguridad** y respuesta a incidentes. Proporciona unos servicios de alto nivel a organizaciones de todo el mundo. Trabajamos para responder rápidamente a las amenazas y mejorar proactivamente la resiliencia. Nuestra probada trayectoria, compromiso y discreción, han hecho que nos ganemos la confianza de los equipos de seguridad, altos ejecutivos y consejos de administración de las principales organizaciones de todo el mundo, incluidas empresas de la lista Fortune 100.

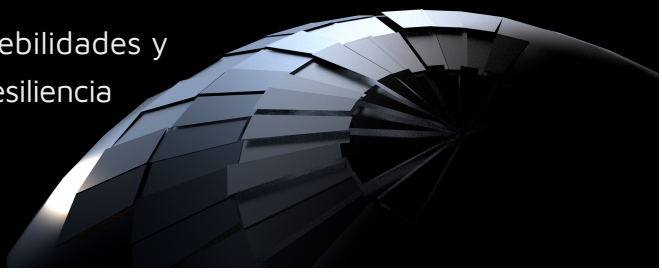
## **PUNTOS DESTACADOS** DE LA SOLUCIÓN

Garantizar la disposición del equipo de Ciberseguridad para prevenir, detectar, responder y recuperarse ante cualquier incidente.

Somos expertos con un profundo conocimiento de los grupos de ransomware y los métodos de ataque que utilizan.

Nos centramos en los mecanismos de ataque más efectivos de ransomware, según los escenarios de ataque del mundo real.

Disponemos de información práctica sobre debilidades y recomendaciones priorizadas para mejorar la resiliencia de nuestro entorno de Ciberseguridad.



## **NUESTROS** SERVICIOS

### EVALUACIÓN DE LA PREPARACIÓN FRENTE AL RANSOMWARE

Analizamos rápidamente la capacidad de su organización para Prevenir, Detectar, Responder y Recuperarse de todas las fases de un ataque, incluyendo la infiltración, la propagación a través de la red y el cifrado o la extracción de archivos y datos. Realizamos toda una serie de talleres enfocados, sesiones técnicas, análisis de planes de respuesta, método de jugadas, la revisión práctica de los controles técnicos y su configuración. Todo ello para identificar las lagunas en su preparación frente al ransomware. Desarrollamos escenarios de ataque diseñados para evaluar la vulnerabilidad de su organización a ataques híbridos de ransomware/extracción de datos. Los escenarios cubrirán varios grupos conocidos de actores de amenazas de ransomware (por ejemplo, Conti, Darkside) y sus tácticas. Tras la evaluación, proporcionamos recomendaciones prácticas y priorizadas para mejorar la capacidad de su organización para contener y recuperarse de las amenazas de ransomware.

## SIMULACIÓN DE ATAQUE DE RANSOMWARE

Nuestro equipo de Tácticas Adversarias imitará las TTPs (Tácticas, Técnicas y Procedimientos) de los grupos de actores de amenazas de ransomware a través de un ejercicio de "equipo rojo o púrpura" a medida. Simulamos un ataque de ransomware a través de su red. Aprovechamos nuestra experiencia en el campo de batalla real y la interacción previa con los actores de amenazas. El equipo ha desarrollado un ransomware benigno para imitar las actividades de ransomware dentro del entorno y poner a prueba las capacidades de detección y respuesta contra los ataques de ransomware. El ejercicio de simulación puede utilizarse para capacitar y entrenar a los equipos de respuesta y se centrará en evaluar la segmentación de la red, la capacidad de extraer datos, los puntos de infiltración y las vulnerabilidades explotables.

## JUEGO DE GUERRA DE MESA PARA EJECUTIVOS

Forme a su dirección ejecutiva y a la junta directiva, así como a los responsables de tecnología y seguridad, mediante la simulación de una situación de ataque de ransomware, de gran envergadura, hecho a medida y realista, contra su organización. Ponga a prueba las funciones y responsabilidades de cada persona, mejore los procesos, desarrolle el conocimiento y la capacidad de gestión, e infunda la confianza necesaria para liderar ante una crisis cibernética.

## EVALUACIÓN DE COMPROMISO CENTRADA EN RANSOMWARE

En nuestro día a día, hemos respondido a ataques en los que los actores de la amenaza permanecieron inactivos en la red durante varios meses antes de desplegar el ransomware en los endpoints. Nuestra Evaluación de Compromiso puede identificar y neutralizar amenazas latentes y activas en una etapa temprana; pudiendo establecer una clara línea de base de seguridad, aumentando la confianza en su red y la integridad de sus sistemas críticos y activos de datos.

Calle Bravo Murillo 178, 1° planta,
Edificio Tecnus, C.P. 28020, Madrid

915799610

entornodeseguridad@uniway.es