Respuesta ante ciberincidentes/ ciberataques

Ventajas de anticiparse: limitar el impacto, acortar el tiempo de recuperación y mejorar la eficacia de la respuesta.

RESPUESTA RÁPIDA Y MÚLTIPLE

El factor tiempo es el elemento determinante. Nuestros técnicos comienzan a actuar para acelerar la resolución del incidente, minimizar el impacto, contener su expansión, proceder a la reparación y recuperación de los entorno. Somos capaces de ejecutar todos los flujos de trabajo en paralelo, orquestándolos y gestionando el incidente de principio a fin.

GESTIÓN EJECUTIVA DE CRISIS

Trabajamos en equipo con la dirección ejecutiva de nuestros clientes para proporcionar respuestas precisas. En paralelo con la resolución de incidentes, gestionamos las crisis en todos los aspectos, incluidos los aspectos legales y normativos de gestión interna.

CONTENCIÓN

Es crítico asegurar rápidamente las áreas del entorno que aún no han sido impactadas por el ataque y evitar que se vean comprometidas. Esto puede lograrse mediante la segregación o poniéndolas en cuarentena. Los resultados de la investigación se aprovechan para contener rápidamente la amenaza y evitar daños mayores a la empresa.

INVESTIGACIÓN

Realizamos un triaje e investigamos para identificar el punto de entrada inicial, el alcance del compromiso, cómo el ataque se ha propagado a través de nuestro entorno, las herramientas utilizadas por el atacante y el nivel de amenaza actual. Identificamos de forma rápida y precisa las capacidades del atacante y los plazos en los que deben ser remediados.

NEGOCIACIÓN TÁCTICA

Disponemos y utilizamos a nuestros expertos negociadores para ganar un tiempo crítico e información valiosa del atacante. Este enfoque sirve, no sólo para reducir significativamente las peticiones de rescate, sino también para mejorar sustancialmente la velocidad de la investigación técnica y los esfuerzos de recuperación.

REMEDIACIÓN Y RECUPERACIÓN

La recuperación se inicia inmediatamente y en paralelo con la investigación. Definiremos un entorno de "isla segura" del que se haya eliminado el entorno comprometido y así, la organización puede volver a funcionar a pleno rendimiento y mucho más rápido. El esfuerzo de remediación identifica y cierra el entorno de seguridad y la presencia del atacante en este entorno es erradicada.

SUPERVISIÓN DE AMENZAS

Los atacantes pueden intentar acciones maliciosas adicionales en cualquier momento. Para minimizar este riesgo, nuestro equipo de respuesta a incidentes realiza una monitorización a medida durante y después de un incidente para asegurar que las actividades maliciosas adicionales y los intentos de reentrada sean detectados y bloqueados inmediatamente.

VENTAJAS DE NUESTRO SERVICIO DE CONTENCIÓN Y RESPUESTA (IRR)

El factor tiempo es el elemento determinante. Nuestros técnicos comienzan a actuar para acelerar la resolución del incidente, minimizar el impacto, contener su expansión, proceder a la reparación y recuperación de los entorno. Somos capaces de ejecutar todos los flujos de trabajo en paralelo, orquestándolos y gestionando el incidente de principio a fin.

MÚLTIPLES NIVELES
Adaptable a las necesidades de las organizaciones.

PROCESO DE INCORPORACIÓN
Garantía de respuesta rápida y fluida.

100% DE UTILIZACIÓN
Las horas no empleadas se pueden reutilizar

RESPUESTA RÁPIDA
Según SLA.

CUENTA DEDICADA
Consultor dedicado al cliente.

SERVICIOS COMPLEMENTARIOS
para clientes IRR

Nuestra propuesta abarca hasta cuatro niveles diferentes de servicios de contención y respuesta. Con esto facilitamos que los clientes puedan elegir el nivel que mejor se adapte a sus necesidades de negocio y su capacidad

	NIVEL 1	NIVEL 2	NIVEL 3	NIVEL 4
Acuerdo firmado con términos y condiciones	●	●	●	●
Línea directa de notificación de IR 24/7	●	●	●	●
Despliegue de tecnologías propias	●	●	●	●
IRR Onboarding Session	○	●	●	●
Tiempo de respuesta a distancia SLA	Mínimo posible	6 h	4 h	2 h
Tiempo de respuesta en ruta SLA	Mínimo posible	48 h	24 h	24 h
Tiempo de soporte IR prepagado	●	100 h	200 h	300 h
Tarifa con descuento para servicios de IR	Tarifa estándar	-10%	15%	-20%
Plazo de contratación	1 año	1 año	1 año	1 año

El Incident Response Retainer (IRR) que ofrecemos, proporciona parámetros críticos predeterminados que reducen el tiempo de resolución de un incidente de ciberseguridad. Esto permite que el equipo de trabajo se ponga manos a la obra e inicie inmediatamente los esfuerzos de respuesta.

El IRR (nivel 2 y superiores) incluyen una sesión de onboarding con cada nuevo cliente. La sesión incluye una revisión de alto nivel de la red y la arquitectura de TI del cliente, los sistemas críticos, el intercambio seguro de datos y los procesos de acceso. Las directrices de respuesta son capturadas e incorporadas en un manual de activación de IRR específico del cliente que permite una respuesta ante incidentes.

UTILIZACIÓN FLEXIBLE DE LAS HORAS DE RETENCIÓN

Las horas de IRR no utilizadas pueden dedicarse para cualquier otro servicio de nuestra propuesta. También ofrecemos un conjunto de servicios diseñados específicamente para clientes IRR, que incluye simulacro de ataques (wargames), entornos técnicos de simulación, ejercicios de clasificación, escalación y simulaciones de adversidades.

RESPUESTA A INCIDENTES

Cuando nos enfrentamos a una brecha de seguridad, se necesita contar con los mejores recursos. Nuestros equipos globales de respuesta a incidentes tienen historial probado de contener y derrotar rápidamente ciberataques, minimizando la interrupción del negocio y guiando a las organizaciones a través de la crisis.

Tanto si la amenaza es un grupo delictivo, un actor patrocinado por un Estado o una amenaza interna, nosotros estamos a su lado.

Ante una amenaza interna, ayudamos a nuestros clientes a investigar con rapidez el origen, contener y erradicar al atacante. Desplegamos los mejores talentos con experiencia en ciberwar en unidades militares especializados de élite y un profundo conocimiento de las tácticas de los creadores de amenazas.

BENEFICIOS PROBADOS

Rápida contención y derrota de los ciberataques.

Minimizar las interrupciones y los daños a la empresa.

Gestionar eficazmente la crisis.

Salir reforzado de la crisis (aprendizaje y refuerzo frente a situaciones futuras).

VENTAJAS DEL SERVICIO

PERSPECTIVA DEL ATACANTE

Contamos con equipos altamente experimentados, con amplios conocimientos en ciberguerra a nivel de estado-nación, capacidades ofensivas y defensivas, con décadas de experiencia en la respuesta ante incidentes. Nuestros equipos son capaces de pensar, maniobrar y superar a los atacantes.

METODOLOGÍA DE COMBATE PROBADA Y RESPUESTA RÁPIDA

Nuestro "modus operandi" es producto de una amplia experiencia militar cibernética. Nuestra metodología de respuesta abarca la ejecución paralela de amplia variedad de actividades necesarias para hacer frente a un ataque: contención, investigación y análisis forense, negociación táctica, recuperación, gestión ejecutiva de crisis, y supervisión posterior a la violación de seguridad.

SUPERIORIDAD TECNOLÓGICA

Nuestros ágiles equipos responden eficazmente a incidentes en cualquier entorno, con cualquier IT o entorno de seguridad. Nuestra experiencia incluye nube, aplicaciones, CI/CD, OT, móvil e IoT. También hemos desarrollado una avanzada plataforma XDR que se utiliza para potenciar y aumentar las capacidades de las herramientas de seguridad del cliente cuando sea necesario.

EQUIPO DE INVESTIGACIÓN DE AMENAZAS

La investigación de cada amenaza y su continua monitorización global a lo largo del mundo se incorpora a los esfuerzos de respuesta a incidencias, asegurando y revelando nuevos vectores de amenazas a la comunidad global de seguridad.

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

915799610
entornodeseguridad@uniway.es