ANÁLISIS DE SITUACIÓN

Nuestra amplia experiencia ayudando a los clientes a contener y remediar graves brechas de seguridad y mejorar sus defensas, ha demostrado que las organizaciones pueden lograr mejoras significativas y rápidas en su infraestructura de seguridad, maximizar el ROI de su inversión en el entorno de seguridad existente y, simultáneamente acelerar el logro de sus objetivos estratégicos de seguridad a largo plazo.

El servicio de mejora de nuestro entorno de Ciberseguridad proporciona a los clientes un conocimiento exhaustivo de su ciberresiliencia y un camino detallado para reducir enormemente el nivel de riesgo cibernético que tengamos inicialmente.

BENEFICIOS PROBADOS

- Lograr una comprensión completa y holística de la resistencia de los activos y organización a los ataques cibernéticos.
- Descubrir y aprender a corregir los vectores de ataque que probablemente se utilizarán contra la organización en un ataque real.
- Recibir un conjunto priorizado y pragmático de iniciativas de mejora cibernética.
- Maximizar la rentabilidad de la inversión de los elementos de seguridad existente.
- Acelerar la consecución de los objetivos cibernéticos corporativos estratégicos y tácticos.
- Reducir enormemente el riesgo de infracción normativa y los daños potenciales.

Un camino rápido para conocer la situación de nuestra infraestructura cibernética en cada organización.

El servicio está diseñado para proporcionar un impacto significativo en tan sólo unas semanas, impulsado por un eficiente proceso de 3 pasos.

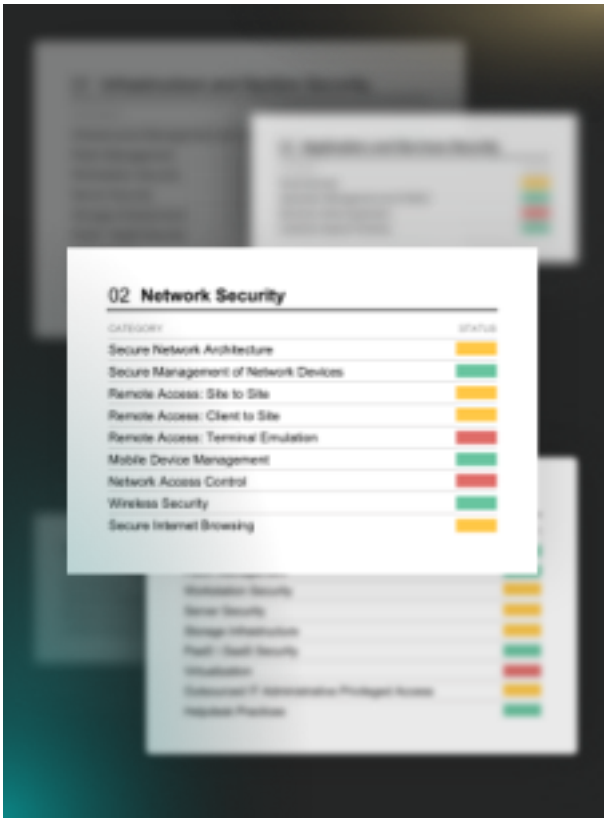
PASO UNO: DESCUBRIMIENTO

Comienza con una revisión de los sistemas de negocio y de TI. Comprenden el contexto empresarial, la estructura organizativa, los activos críticos y los procesos de la organización. Se revisa el entorno tecnológico, incluidos los sistemas de TI, la arquitectura de red y el "stack" de seguridad.

A continuación, se realizan simulaciones prácticas de ataques de adversarios en la red, reproduciendo las tácticas, técnicas y procedimientos de los actores de la amenaza. Las simulaciones de adversarios incorporan las últimas actualizaciones sobre las tácticas de los actores de amenazas de nuestro Grupo de Investigación de Amenazas y de los equipos de respuesta a incidentes. Se identifican las desconfiguraciones del sistema de seguridad, los fallos de diseño y las vulnerabilidades explotables.

PASO DOS: ANÁLISIS

El segundo paso es un análisis de las capacidades de la organización en comparación con las mejores prácticas definidas. Seleccionamos las mejores prácticas de la industria a partir de estándares internacionales como NIST e ISO, y las fusionamos con nuestra amplia experiencia de primera línea. Para evaluar las verdaderas capacidades de la organización, desarrollamos escenarios de ataque de alto impacto que ponen a prueba las formas en que los adversarios podrían materializar sus objetivos contra la organización. Identificamos si la organización puede prevenir, detectar, responder y si se recuperase de cada escenario y cómo lo haría. Los resultados se utilizan para formar una imagen precisa y detallada de la postura de seguridad actual de la organización, incluyendo las brechas de seguridad, fortalezas y oportunidades de mejora.



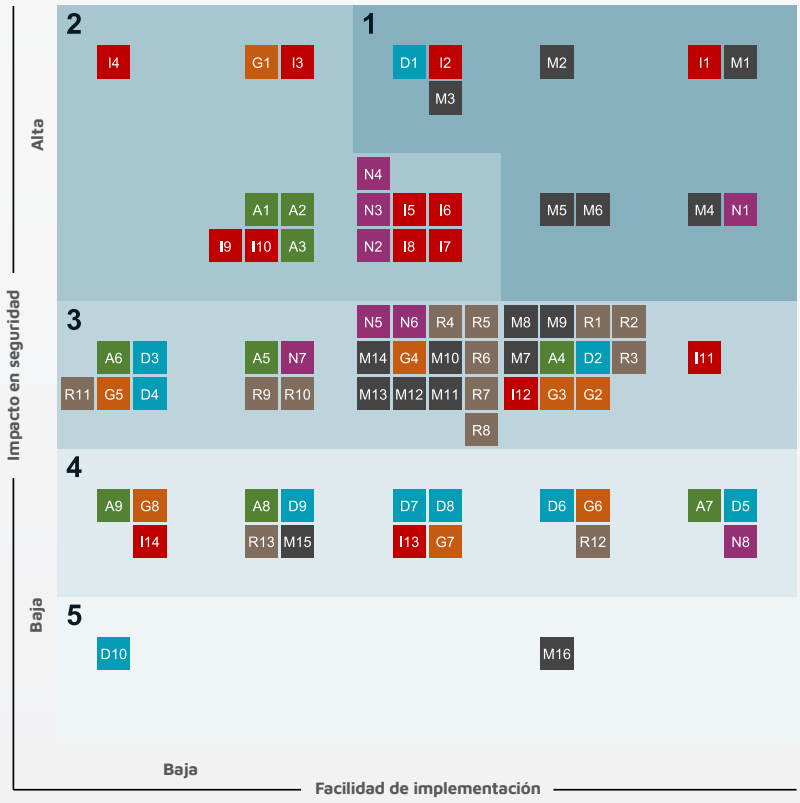
PASO TRES: RECOMENDACIONES ESTRATÉGICAS Y TÁCTICAS

En el tercer paso, desarrollamos una visión consolidada, iniciativas priorizadas por impacto y facilidad de implementación. Identificamos, no sólo las brechas de seguridad, sino también los pasos específicos que una organización debe tomar para hacerlas frente, tanto a nivel estratégico como técnico.

Para los ejecutivos, proporcionamos una visión estratégica que incluye los puntos fuertes actuales de la organización y las oportunidades para reforzar las defensas, las ideas estratégicas clave y una hoja de ruta con un plan de acción recomendado.

Para los equipos de seguridad, proporcionamos un análisis detallado y visual de las deficiencias que ilustra los puntos fuertes y débiles de la organización y las áreas de mejora. Se proporcionan iniciativas detalladas y priorizadas con el nivel de granularidad necesario para garantizar el éxito de la implementación. Se abordan todos los ámbitos de la ciberseguridad, incluyendo la detección y respuesta, la gestión de identidades y accesos, la protección de datos, la seguridad de las aplicaciones, la gobernanza de la seguridad, la seguridad de la red y la infraestructura de TI.

Nuestras recomendaciones son pragmáticas, viables y orientadas al impacto. Nuestro enfoque prioritario es buscar siempre las formas de optimizar el "stack" de seguridad existente del cliente.



Initiatives pillars

- **I#** Infraestructura y sitema de seguridad
- **N#** Seguridad en la red
- **A#** Seguridad de aplicaciones y servicios
- **M#** Gestión de identidades y accesos
- **D#** Protección de datos
- **R#** Detección y respuesta
- **G#** Gestión de seguridad

HA LLEGADO EL MOMENTO DE ACTUAR

Las ciberdefensas suelen ser mucho más permeables de lo que se cree, pero la asimetría entre atacantes y defensores puede invertirse. Las organizaciones deben comenzar con una evaluación de su situación para obtener una visibilidad completa de la resistencia actual a los ciberataques. Se identificarán los puntos fuertes de la ciberseguridad y se revelarán las lagunas explotables. Las brechas críticas se cerrarán inmediatamente, antes de que sean explotadas por un atacante. A continuación, la organización puede avanzar en la aplicación de una hoja de ruta estratégica de mejora de situación y lograr mejoras espectaculares en la resiliencia cibernética.

NUESTRAS VENTAJAS

SOLO EQUIPOS A

Empleamos sólo equipos altamente experimentados con demostrables antecedentes en ciberguerra y seguridad empresarial. Nuestra experiencia en respuesta a incidentes y seguridad empresarial está integrada en nuestras evaluaciones y mejoras de situación, incluyendo conocimientos profundos sobre el tejido defensivo requerido y las tácticas necesarias para maximizar las defensas cibernéticas.

PRAGMÁTICO Y ORIENTADO AL IMPACTO

Nuestras recomendaciones son pragmáticas y orientadas al impacto. Nuestros equipos siempre buscan primero las formas de optimizar el "stack" de seguridad existente y, hacer el mejor uso de cualquier inversión prexistente en seguridad. Facilitamos una hoja de ruta priorizada, clara y estratégica para el nivel ejecutivo.

EQUIPO DE INVESTIGACIÓN DE AMENAZAS AVANZADAS

Las últimas investigaciones sobre los actores de amenazas globales y sus tácticas se incorporan a las simulaciones de adversarios y a la evaluación comparativa que realizamos, lo que garantiza evaluaciones de situación sólidas.

DOMINIO TECNOLÓGICO

Nuestros equipos especializados realizan una evaluación efectiva de la situación real de seguridad en cualquier entorno, con cualquier infraestructura de TI o seguridad, en cualquier dominio, incluida la nube, la aplicación, CI / CD, OT, móvil, IOT y la infraestructura de red tradicional.

MEJORA DE SITUACIÓN CASOS DE USO

EVALUACIÓN ESTRATÉGICA

Realizamos un análisis completo para evaluar la resiliencia cibernética actual de la organización y desarrollar una hoja de ruta estratégica para mejorar la resiliencia.

BENCHMARKING VS. PARES DE LA INDUSTRIA

Los puntos fuertes y débiles de la seguridad actual se evalúan en relación con los marcos de seguridad de la industria y se comparan con las puntuaciones típicas de los pares de la industria.

POST-ACCIDENTE

Después de un ciberataque importante a la organización realizamos una evaluación completa de situación y proporcionamos una hoja de ruta detallada para fortalecer la red del cliente contra todo el espectro de amenazas relevantes.

FUSIONES Y ADQUISICIONES (M&A)

Antes de completar una adquisición, aportamos un análisis completo de la situación de ciberseguridad de la empresa objetivo, como parte integrante de la "Due Diligence".

OPTIMIZACIÓN DEL GASTO EN SEGURIDAD

Proporcionamos un análisis de postura priorizado y una hoja de ruta de mejora detallada que se puede utilizar para validar y optimizar el presupuesto de seguridad de la organización.

CUMPLIMIENTO NORMATIVO

Comprobamos las medidas, controles y capacidades de seguridad existentes en la organización en comparación con los requisitos normativos.

MIGRACIÓN A LA NUBE

Antes de una migración planificada de la infraestructura de TI a la nube, proporcionamos un marco completo de seguridad en la nube. Tras una migración a la nube, realizamos una evaluación y validación de la seguridad de esta.

TRANSFORMACIÓN DIGITAL

Evalúamos la resistencia cibernética de un producto o aplicación crítica dentro del ecosistema de TI más amplio de la organización para exponer cualquier debilidad inherente.

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

915799610
entornodeseguridad@uniway.es