Consultoría (GRC)

numu Group

Plan Estratégico de Seguridad

Identificar y evaluar las posibles amenazas para la seguridad y mitigar los riesgos mediante una evaluación experta y medidas eficaces. Proteger la organización con un enfoque de gestión de riesgos de seguridad a medida, que garantice una mayor seguridad para su organización.

- Mejor comprensión de los procesos de seguridad de la información
- Ayuda a identificar proyectos críticos
- Ayuda a identificar las tecnologías de seguridad adecuadas

Master Plan de seguridad

Construir un programa de seguridad completo y eficaz que proteja la organización de las ciberamenazas, identificando los riesgos y vulnerabilidades potenciales a los que se enfrenta la organización e implementando soluciones a medida para mitigarlos.

- Facilita la identificación y comprensión de los riesgos críticos
- Enfoque en la mitigación de riesgos y actitud proactiva ante los mismos
- Reducción de costes

ISO 27001, 27701 & 22301

Implantar, adecuar o precertificar en ISO 27001 (ISMS), ISO 22301 (BCMS) e ISO 27701 (PIMS) para cumplir las normas internacionales y reconocidas.

- Mejora la gestión de riesgos y el cumplimiento de la privacidad
- Aumenta la confianza y la credibilidad ante clientes y proveedores
- Aumenta la resistencia de la organización

Evaluación de riesgos

Tomar decisiones informadas sobre cómo mitigar, evitar o transferir los riesgos identificados analizando y evaluando la probabilidad y el impacto que pueden afectar a su organización, como ciberamenazas, vulnerabilidades y otros posibles incidentes de seguridad.

- Mejor identificación de amenazas y vulnerabilidades
- Mejora la toma de decisiones sobre cómo asignar recursos, priorizar iniciativas y gestionar los riesgos de forma eficaz
- Mejora el cumplimiento, permitiendo a las empresas asegurarse de que satisfacen los requisitos legales

Evaluación del GDPR

Alcanzar la conformidad con el GDPR identificando los requisitos, evaluando la posición de ciberseguridad de la organización y definiendo la posición objetivo y la implementación.

- Mejora el cumplimiento y la protección de datos
- Mejora la reputación y fomenta la confianza de los clientes
- Mejora las prácticas de gestión de datos

Implementación del Esquema Nacional de Seguridad

Garantizar el cumplimiento de la normativa del ENS identificando los requisitos específicos, evaluando la postura actual de la organización en materia de ciberseguridad y definiendo una postura objetivo y un plan de implantación.

- Ayuda a mejorar la ciberseguridad aplicando medidas para proteger los sistemas de información y los datos
- Ahorro de costes al reducir la probabilidad de incidentes de seguridad y sus costes asociados
- Alineamiento con las normas nacionales

Evaluación de riesgos de IoT

Obtener información valiosa sobre los riesgos y la postura actual de seguridad de sus sistemas IoT, identificando posibles amenazas y desviaciones.

- Ayuda a identificar y mitigar los riesgos de IoT
- Mejora la postura de seguridad de IoT
- Evita posibles ciberataques y fugas de datos

Formación y concienciación

Actividades de formación

Mejorar los conocimientos de la organización sobre ciberseguridad impartiendo sesiones de formación a medida para empleados, tanto técnicos como no técnicos, mediante sesiones presenciales o virtuales con actividades prácticas y evaluaciones.

- Reducir los riesgos cibernéticos
- Cumplir con la normativa (ISO 27001, por ejemplo)
- Protección de datos sensibles

Campañas de sensibilización

Fomentar una sólida cultura de ciberseguridad promoviendo prácticas responsables en línea. Nuestras atractivas campañas de concienciación incluyen materiales como artículos, infografías, vídeos y boletines informativos para dotar a su equipo de los conocimientos necesarios para defenderse de las ciberamenazas.

- Garantizar el cumplimiento de la normativa (ISO 27001, por ejemplo)
- Mejorar los conocimientos de los empleados sobre ciberseguridad
- Capacitar a los usuarios, generar confianza y reducir la probabilidad de ciberataques

Capture The Flag (CTF)

Mejorar las habilidades técnicas y la capacidad de trabajo en equipo de los grupos técnicos de la organización con atractivos concursos de Capture The Flag (CTF) que promueven una experiencia de aprendizaje positiva y práctica en el campo de la ciberseguridad.

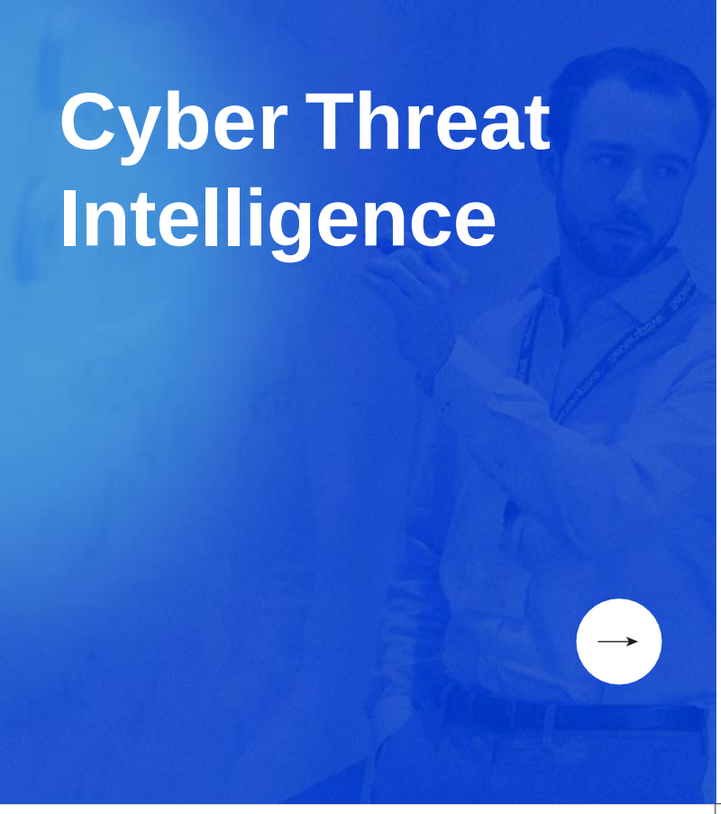
- Desarrolla habilidades de ciberseguridad
- Mejora la capacidad de resolución de problemas
- Fomenta el trabajo en equipo y la comunicación

Campañas de Ingeniería Social

Proteger a la organización de las amenazas de ingeniería social con campañas simuladas de phishing y ransomware, mejorando su resistencia general de ciberseguridad.

- Aumentar la concienciación en materia de seguridad
- Mejorar la cultura de seguridad
- Ayudar a identificar y reforzar a los empleados más vulnerables
- Ayudar a probar los planes de respuesta a incidentes

Cyber Threat Intelligence



Brand Intelligence

Defender la reputación y los activos de la organización con una Brand intelligence proactiva, supervisando y detectando actividades fraudulentas para evitar futuros ataques y acreditaciones erróneas.

- Alerta preventiva de posibles amenazas y detección proactiva de ataques
- Reduce costes y daños a la reputación (asociados a ventas de falsificaciones, abuso de marca, etc.)
- Detecta y elimina el phishing

Threat Intelligence

Adelantarse a las amenazas emergentes con una supervisión continua de la threat intelligence, centrada en grupos hacktivistas, activistas y estatales y sus campañas dirigidas a información sensible para su posible venta o publicación en foros clandestinos.

- Mejora la detección de amenazas
- Mejora el conocimiento de la situación de las empresas y ayuda a tomar decisiones de seguridad más informadas sobre su postura de seguridad
- Respuesta más rápida a los incidentes de seguridad proporcionando información práctica y orientación sobre cómo mitigar las amenazas.

Intelligence de Seguridad Internacional

Mitigar los riesgos de Seguridad Internacional analizando y evaluando acontecimientos específicos en determinadas regiones o zonas que puedan afectar a los intereses y activos de su organización.

- Mitigación de riesgos relacionados con la inestabilidad política, la volatilidad económica y el malestar social en diferentes regiones del mundo
- Ventaja competitiva al proporcionar información valiosa sobre tendencias, mercados y acontecimientos emergentes en una zona
- Ayuda a diseñar la planificación estratégica teniendo en cuenta los riesgos y oportunidades internacionales
- Ayuda a las organizaciones a prepararse para la gestión de crisis

Intelligence de terceras partes

Reforzar la seguridad de la cadena de suministro con una supervisión continua de la inteligencia de terceros, con especial atención a los eventos de riesgo relacionados con la información confidencial de los clientes casi en tiempo real.

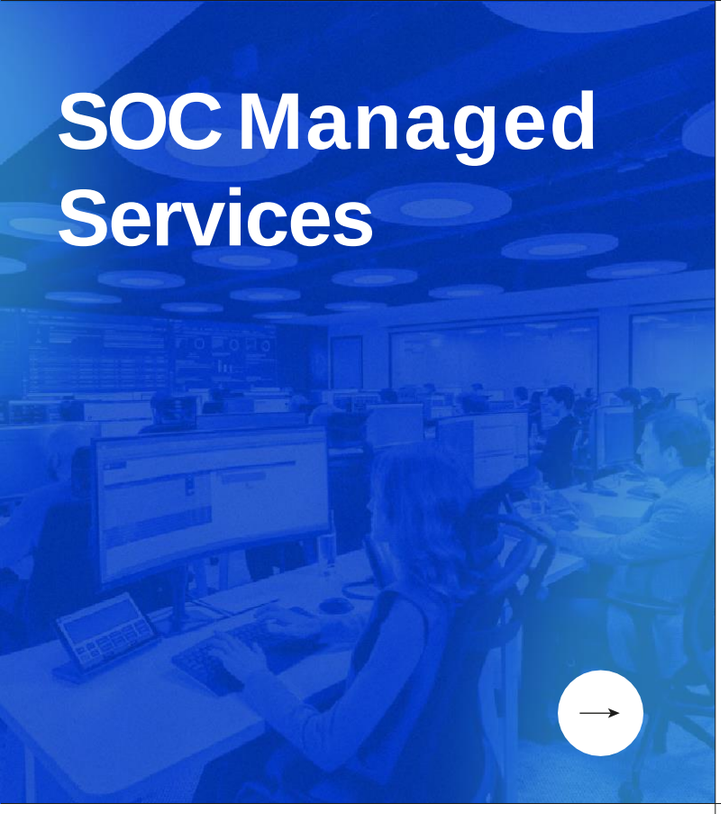
- Detecta ciberamenazas emergentes contra organizaciones de terceros en la cadena de suministro y el ecosistema de proveedores.
- Ayuda a tomar las medidas adecuadas para prevenir o mitigar esas amenazas
- Ayuda a tomar decisiones informadas sobre terceros

Intelligence de identidad

Proteger a la organización del fraude de identidad mediante la supervisión activa de indicios de estafas o campañas dañinas dirigidas a la identidad de empleados y clientes.

- Evita la apropiación de cuentas
- Detecta el fraude de identidad de los clientes
- Protege la identidad de los empleados

SOC Managed Services



MDR – Detección y respuesta gestionadas (EDR, XDR, SIEM)

Reforzar la postura de ciberseguridad de la organización con la detección y respuesta oportunas a las amenazas gracias al apoyo de un ecosistema integrado de personas, procesos y herramientas. Bloquear las amenazas en sus primeras fases con nuestras guías automatizadas y la correlación de eventos.

- Mayor visibilidad de todos los eventos de seguridad de una organización
- Gestión centralizada de los puntos finales
- Tiempos de detección más rápidos gracias al threat hunting
- Guías automatizadas personalizadas para cada entorno

DDR – Detección y Respuesta DNS

Nuestro servicio de Detección y Respuesta DNS está diseñado para ayudar a las organizaciones a salvaguardar su capa DNS, contrarrestar eficazmente las amenazas potenciales y detener las comunicaciones de los dispositivos infectados. Nos encargamos de gestionar y controlar el DNS de nuestros clientes con inteligencia procesable instantánea y sistemas de puntuación de reputación para proteger su entorno.

- Threat Hunting proactiva con feeds de amenazas globales
- Gestión simplificada de DNS
- Elimina la sobrecarga del ecosistema de seguridad mediante la reducción del tráfico malicioso y un nivel extremadamente bajo de falsas alertas

"Este servicio podría prestarse con MDR o de forma independiente"

Gestión de la tecnología de seguridad

Optimizar las tecnologías de seguridad de la organización mediante la supervisión continua, el ajuste y las últimas actualizaciones, garantizando su estado y disponibilidad tanto en las implantaciones existentes como en las nuevas.

- Gestión remota de plataformas de seguridad
- Actualización y creación de reglas y/o políticas dentro de las herramientas de seguridad
- Ayuda en el despliegue de herramientas de seguridad para una configuración correcta y segura

Exposure Management

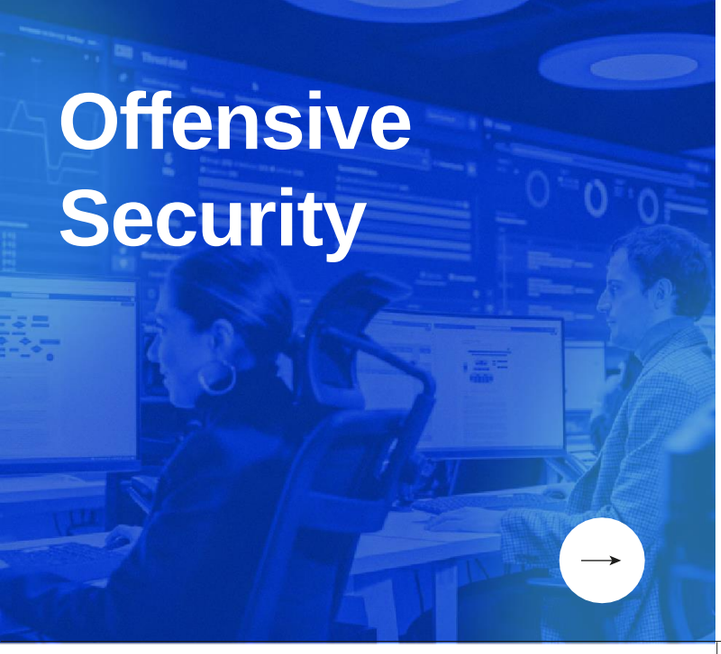
Minimizar los riesgos derivados de las vulnerabilidades y los activos expuestos combinando las perspectivas de atacantes y defensores, con el apoyo de herramientas de exploración automática e inteligencia procesable sobre la exposición de las marcas.

- Mayor rapidez de respuesta ante incidentes
- Mayor protección de la superficie de ataque que afecta a una organización
- Acciones de mitigación de riesgos más rápidas

Managed SASE

Mejorar la seguridad de la organización en la nube con un Secure Access Service Edge gestionado que proporciona una protección integral, incluido el control de acceso, la prevención de la filtración de datos, la seguridad DNS y la protección antimalware a través de una plataforma de gestión de la nube centralizada.

- Mejora y garantiza una experiencia de usuario coherente de la política y la seguridad de acceso a las aplicaciones, independientemente de la ubicación y el dispositivo de los usuarios
- Aumenta la visibilidad, la agilidad, la resistencia y la seguridad, especialmente para organizaciones distribuidas con una plantilla híbrida y una fuerte adopción de servicios en la nube
- Respuesta automatizada a incidentes más rápida y eficazmente a través de todo el ecosistema de seguridad



Servicio de aplicación de Caja Negra

Identifica vulnerabilidades en los dominios y activos de Internet de su organización con una combinación de análisis automatizado y revisión manual desde un enfoque de pruebas de penetración de caja negra.

- Priorización de los activos más críticos y vulnerables en Internet para tomar medidas
- Conocer el nivel de exposición frente a un ataque real para tomar decisiones informadas
- Descubrir las TI en la sombra para prevenir incidentes

Aplicaciones móviles

Proteger las aplicaciones móviles de la organización realizando análisis de vulnerabilidades en plataformas iOS/Android, identificando posibles exploits y revisando los permisos de usuario.

- Visión integral de la seguridad de las aplicaciones
- Optimización del código para mejorar la seguridad y el rendimiento
- Validación del diseño de seguridad de la APP móvil para cada sistema operativo (Android/iOS)

Seguridad en API

Proteger las interfaces API de la organización con un exhaustivo análisis de vulnerabilidades para identificar posibles métodos y parámetros explotables.

- Identificación de vulnerabilidades críticas y reducción de riesgos
- Protección de datos sensibles contra ciberataques
- Validación del diseño de seguridad en la integración de la API y la comunicación con el servidor

Aplicaciones Web

Proteger las aplicaciones Web de la organización con análisis de vulnerabilidades mediante técnicas de pentesting que simulan ataques reales.

- Conocimiento de las vulnerabilidades explotables y del nivel de seguridad de la aplicación web
- Prevención de fugas de datos por fallos de seguridad

Servicio antiransomware

Evaluar y mejorar la resistencia de la organización a los ataques de ransomware con auditorías de rendimiento, incluidas campañas de phishing y pentesting que simulan el comportamiento del ransomware.

- Mejorar los procesos de respuesta y contención ante ataques de ransomware
- Medir el nivel de concienciación de los empleados ante los ataques de phishing

Análisis de infraestructuras

Proteger la infraestructura de la organización realizando un análisis de caja negra para identificar y explotar errores de configuración o vulnerabilidades de software tanto en activos de Internet como en infraestructura local.

- Conocer la visibilidad que puede alcanzar un usuario malintencionado dentro de un activo comprometido
- Alcanzar el nivel de seguridad deseado en la infraestructura

Penetration testing

Reforzar las defensas de ciberseguridad de la organización con pruebas de pentesting exhaustivas, utilizando técnicas manuales para evaluar vulnerabilidades en redes internas, puntos finales y activos de Internet externos.

- Identificación de vulnerabilidades de configuración explotables y vectores de compromiso
- Evaluación de los mecanismos de seguridad de los puestos de trabajo

Auditoría WiFi

Proteger las redes inalámbricas de la organización con una auditoría WiFi exhaustiva, que identifique vulnerabilidades, garantice configuraciones de seguridad óptimas y analice la cobertura de la red.

- Evaluar el nivel de exposición frente a un posible ataque a través de la infraestructura WiFi
- Garantizar los requisitos mínimos de seguridad de la red WiFi

Aplicaciones de escritorio

Proteger las aplicaciones de escritorio de la organización con un completo análisis de vulnerabilidades que incluye tanto el análisis estático del código fuente como pruebas dinámicas mediante inyección de código para evaluar las funcionalidades de comunicación.

- Garantiza el diseño de seguridad de la aplicación de escritorio
- Garantiza la protección de los datos contra el robo, la interceptación o la manipulación

Simulación de dispositivo robado

Proteger los dispositivos de la organización en el lugar de trabajo con una evaluación de seguridad que simula situaciones de pérdida o robo de dispositivos, evaluando el impacto potencial de usuarios malintencionados y probando las configuraciones de seguridad de sus activos.

- Generar confianza con clientes y proveedores auditando y garantizando las configuraciones de seguridad de los dispositivos del lugar de trabajo.
- Evitar costes y daños a la reputación derivados de la pérdida de un dispositivo de la organización.

Campañas avanzadas de ingeniería social

Reforzar las defensas de la organización contra la ingeniería social con campañas puntuales a medida diseñadas para poner a prueba las capacidades de detección y respuesta de los empleados a través de múltiples canales, incluidos el correo electrónico, las llamadas, los SMS y los dispositivos USB.

- Detectar grupos de riesgo y reducir el riesgo de la organización
- Reducir el riesgo de la organización con campañas recurrentes
- Capacitar a los usuarios, generar confianza y reducir la probabilidad de ciberataques

Campañas de spear-phishing

Proteger a los objetivos de alto valor de su organización con campañas de spear-phishing que simulan ataques reales, evaluando la capacidad de los ejecutivos de nivel C y otro personal clave para detectar y responder a las amenazas dirigidas.

- Comprueba el nivel de concienciación de los ejecutivos y la adopción de medidas para prevenir los ataques de ingeniería social
- Mide el grado de exposición a ataques reales de phishing personalizados y el nivel de institucionalización de los procesos de seguridad

Simulación de Red Team y Adversarios

Mejorar la postura de seguridad de la organización con ejercicios de simulación de adversarios y Red Teams que imitan ataques del mundo real, descubriendo vulnerabilidades y puntos débiles en sus sistemas, aplicaciones, seguridad física y redes.

- Identificación y mitigación proactivas de los riesgos de seguridad
- Evaluación exhaustiva de la postura de seguridad de una organización
- Informes detallados con recomendaciones para mejorar la defensa de la seguridad

Contáctenos

info@numu.group

www.numu.group