Security Operations Center (SOC)

¿Qué es el SOC?

Es un servicio de monitoreo integral de seguridad de los activos tecnológicos de las organizaciones y respuesta a incidentes.

¿Cuál es su importancia?

El SOC genera visibilidad para la organización de los incidentes de seguridad mediante monitoreo 24x7x365 para responder de manera ágil a un posible ataque.

Se debe adaptar un enfoque documentado y sistemático, que ayudado por diferentes servicios brindados permite la detección temprana de los incidentes y su remediación.

pwc

www.pwc.com.ar

SkyOnline
Datacenter & Cloud Services

Soluciones

Nuestro enfoque de Managed Detection and Response (MDR)

SIEM

Gestión de logs
Correlación y análisis de eventos de los activos monitoreados.

Detección de intrusos
Identificación de actividades sospechosas en la red.

Comportamiento
Identificación de sospechosos.

Descubrimientos de activos
Identificación de quién y qué está conectado en la red.

Control de endpoint
Supervisión de endpoints en la nube para detectar amenazas y cambios en archivos críticos.

Informes
Informes a medida para estándares o compliance.

Vulnerabilidades
Identificación de vulnerabilidades en los activos.

XDR

Detecciones
Detección de amenazas sin firmas y ataques día zero.

Protección autónoma
Motores de detección de IA y machine learning por endpoints de manera offline.

Protección Ransomware
Rollback para una fácil recuperación después de su detección.

Acciones de respuesta
Remediación, rollback, eliminación de procesos y aislamiento de host.

Control de dispositivos
Bloqueo de dispositivos en los endpoints.

Recopilación de eventos
Centralización de los eventos de seguridad en un solo lugar.

Protección multiplataforma
Protección en Windows, linux y MacOS.

Servicios Complementarios

Brindamos un servicio de búsqueda específica de amenazas en la Deep y Dark Web utilizando tecnologías automatizadas.

Monitoreo proactivo
Monitoreo continuo del panorama de amenazas y remedición proactiva de las vulnerabilidades más críticas.

Inteligencia de amenazas
Proporciona información detallada sobre riesgos y amenazas para mejorar la postura de seguridad.

Descubrimiento
Identificación, seguimiento y mapeo de activos conectados a la organización.

Monitoreo proactivo
Evaluación y cumplimiento de seguridad para redes externas (AWS, Azure y Google Cloud).

Prueba de penetración
Servicio de hackeo ético y soporte a la remediación de brechas de seguridad identificadas.

Vulnerabilidades
Identificación y priorización de vulnerabilidades en aplicaciones, infraestructura de red, conexiones inalámbricas y nube.

Cumplimiento de PCI DSS
Escaneo de red externo certificado para gestionar las vulnerabilidades.

Riesgos
Descubrimiento y evaluación de riesgos en redes y servicio de nube.

Gestión de amenazas continuas (CTEM)
Programa para abordar y mejorar continuamente las prioridades de remediación.

Brindamos un servicio de protección y monitoreo para Tecnología de Operaciones (OP).

Protección multicapa
Protección con múltiples capas de seguridad para protegere los sistemas de control industrias (ICS).

Automatización de tareas
Ejecución automática de tareas en cada servicio detectado en el host.

Protección en tiempo real
Proporcionamientos de alertas en tiempo real para detectar y responder rápidamente a cualquier actividad sospechosa.

Informe de seguridad
Informes detallados y personalizables para análisis o compliance.

Detección y prevención de intrusiones
Integra un sistema de intrusiones de la red (NIDS) y un sistema de prevención de intrusiones de Host (HIPS).

Nuestro servicio de Security Operation Center tiene la

Certificación ISAE (International Standard on Assurance Engagements) 3402 | Tipo 2 que avala su gestión y operación confiable y segura

Nuestro portafolio de soluciones

Forensics
Análisis forense de equipos afectados por un incidente grave.

T-Risk
Evaluación, diseño e implementación de herramientas de medición y seguimiento de riesgos tecnológicos.

Security framework
Evaluación, diseño e implementación de SGSI acorde a estándares ISO 2700X, PCI-DSS, NIST, etc.

Datacenter Services
Servicios de housing/ hosting, administración de infraestructura, servicios de cloud.

Contactos

Diego Taich
Socio de PwC Argentina,
Ciberseguridad & IT.
(+5411) 4850-6834
diego.taich@pwc.com

Rafael Eloy Ibanez
CEO
Datacenter & Cloud Services
(+5411) 3431-5804
ribanez@skyonline.net

@PwC_Argentina /PwCArgentina /PwCArgentina @pwcargentina @pwc_argentina /pwc-argentina

© 2025 Price Waterhouse & Co. Asesores de Empresas S.R.L. Todos los derechos reservados.

En Argentina, las firmas miembro de la red global de PricewaterhouseCoopers International Limited son las sociedades Price Waterhouse & Co. S.R.L., Price Waterhouse & Co. Asesores de Empresas S.R.L., PwC Legal S.R.L. y PwC Servicios de Argentina S.R.L., cada una de las cuales es una entidad legal independiente, que en forma separada o conjunta son identificadas como PwC Argentina. Para más información visitá www.pwc.com/structure. Este contenido es solo para fines de información general y no debe utilizarse en reemplazo de consulta y asesoramiento profesional.

pwc

www.pwc.com.ar

SkyOnline Datacenter & Cloud Services