RAN

S.O.C.
de nueva generación

Investigar eventos de ciberseguridad ocupa gran parte del tiempo de tu equipo, mientras que las brechas de seguridad reales pueden pasar desapercibidas un promedio de 146 días.

Fortalece tu estrategia de seguridad sin agregar staff, ni activos, con nuestro servicio de **S.O.C. MDR Managed, Detection and Response**. Integra rápidamente monitoreo, visibilidad, detección, notificación y seguimiento accionable de múltiples plataformas y eventos de seguridad, a cargo de un equipo experto y con el respaldo de una Compañía especialista en ciberseguridad.

¿POR QUÉ CONTAR CON UN SERVICIO S.O.C. MDR?

- Visibilidad centralizada y completa de los eventos con un portal web de fácil uso, informes completos, cuadros de mando y análisis detallados.
- Monitorización de todo tipo de eventos por un equipo de expertos en disposición 24×7.
- Identificación de las primeras etapas de los ataques y los comportamientos sospechosos internos antes de que ocurra una pérdida de datos.
- Inteligencia de amenazas con reportes accionables que permite a los equipos de IT internos resolver eficazmente los problemas.
- Cumple normativas como: PCI, HIPAA, SOX, GLBA, NERC CIP, FISMA y otros.
- Despliegue escalable en base a la nube, sin compras de HW o SW.
- Soporte inmediato para más de 350 fuentes de registro.
- Modelo de servicio flexible: SOC-as-a-Service, SIEM como servicio y demás opciones híbridas.
- Libera a tu equipo de seguridad interno de análisis abrumadores, configuración y ajuste de firewalls, NGWs, IDS/IPS y WAFs, para concentrarlos en actividades estratégicas de ciberseguridad.

expertos@ransecurity.com

¿QUÉ DIFERENCIAL TIENE UN S.O.C. MDR?

S.O.C. MDR es diferente de los servicios de seguridad administrados tradicionales (MSS) porque se enfocan en la detección y remediación de amenazas.
El servicio que integra MDR proporciona un SOC -as-a-service, e incluyen gestión y análisis de eventos de seguridad, a partir de la inteligencia de amenazas proactiva, con un equipo humano externo dedicado.

¿QUÉ AYUDA A RESOLVER EL SERVICIO DE S.O.C. MDR?

- Visibilidad limitada de puntos finales dentro y fuera de la red
- Poca capacidad de detección de amenazas conocidas y desconocidas.
- Tiempos prolongados de resolución de incidentes
- Fatiga del equipo de TI. persiguiendo demasiados falsos positivos.
- Falta de experiencia interna para investigar y cazar proactivamente amenazas.

El servicio de S.O.C. MANAGE, DETECTION AND RESPONSE, incluye:

SUITE	TECNOLOGIA
Advanced Threat hunting	• SOAR (Security Orchestration, Automation, and Response)
Intermediate Threat hunting	• SIEM + Compliance y Control de cambios • Firewall • Antispam para la nube • Proxy web • Análisis de vulnerabilidades • Compliance y Control de cambios • IA en red • Inteligencia de amenazas
Básico + Remediación + Laboratorio de muestras	• Antimalware con IA + EDR + Análisis de muestras (dinámico, estático, ADN)
Básico + Remediación	• Antimalware con IA + EDR (Remediación)
Básico	• Antimalware con IA (Inteligencia artificial)