SOC
DE MÉXICO
CASO DE ESTUDIO

EL PROBLEMA

Duración del Proyecto: 3 meses

El reto del proyecto era encontrar una tecnología que permita complementar el portafolio de servicios de la compañía especializada en Servicios de Seguridad y Monitoreo de Redes.

¿Cómo ofrecer los mejores servicios con calidad y con un apoyo sólido de la marca y de un canal con alta especialización en la solución?

LOS RETOS

- Habilitar nuevos servicios de seguridad de la información con rapidez y efectividad.
- Ofrecer excelentes niveles de servicio en detección de incidentes de seguridad.
- Tener excelentes tiempos de respuesta en amenazas avanzadas.
- Tener la confianza de una marca y canal con experiencia que los apoye.

LA COMPAÑÍA

Antigüedad: 30 años
Empleados: 400
Ubicación: Guadalajara, México

El giro del cliente son Servicios de Seguridad y Monitoreo de redes. Por lo tanto, el buscar una solución robusta que aumente la oferta de servicios a sus clientes era el reto.

La responsabilidad de brindar estos servicios demandaba encontrar una solución que cuide de sus clientes, sea fácil de implementar, cumpla con los mejores estándares de calidad y que cuente con el respaldo de una marca de renombre, así como un canal de alta especialización que respalde en todo momento.

Guillermo Cataneo
gcataneo@m3security.mx
Tel. +55 5985 2959

LA SOLUCIÓN

1. **Las herramientas adecuadas**
   Se utilizó: **IBM QRadar SIEM** brindando respuesta y la detección de amenazas más abierta y completa de la industria que elimina las amenazas avanzadas más rápido.

2. **Experiencia del Usuario**
   Se brindan los mejores niveles de servicio a los clientes en rapidez de detección de incidentes en menos de 2 horas y generando de manera automática los reportes a los clientes.

3. **Flexibilidad**
   Se tiene la flexibilidad y tranquilidad de contar con una solución de las más completas del mercado en detección y respuesta que elimina amenazas de nivel avanzado.

4. **Soporte**
   Hoy cuentan con un fabricante de renombre a nivel mundial y con el soporte local con los especialistas en seguridad de información asegurando los mejores niveles de servicio.

IBM QRadar SIEM

- **Descubre actividades sospechosas de los usuarios que pudieran identificar credenciales comprometidas o una amenaza interna.**
- **Detecta amenazas en tiempo real identificando un posible ciberataque de alto riesgo.**
- **Protección a la nube exponiendo los riesgos ocultos en entornos multi-nube híbridos.**

RESULTADOS

Se integró una herramienta con gran flexibilidad que les permite identificar amenazas internas, de alto riesgo y todo en tiempo real.

Integración en los mejores tiempos: Integración de eventos en menos de 1 día

Excelente nivel de servicio de detección de incidentes menor a 2 horas.

Generación y envío automático de reportes

El apoyo y respaldo de la marca y canal de alta especialización brinda la seguridad a los clientes para garantizar los niveles de servicio requeridos.

Cuentan con el respaldo y tranquilidad de cumplimiento de regulaciones como GDRP, PCI, SOX, HIPAA y más.

REFLEXIÓN

Una estrategia de seguridad completa considera todos los elementos de manera continua y cubriendo a cada usuario, cada dispositivo y cada conexión, en todo momento.

Y tu negocio ¿Está protegido?

It's all about prevention

It's all about cybersecurity

It's all about YOU

M3 SECURITY