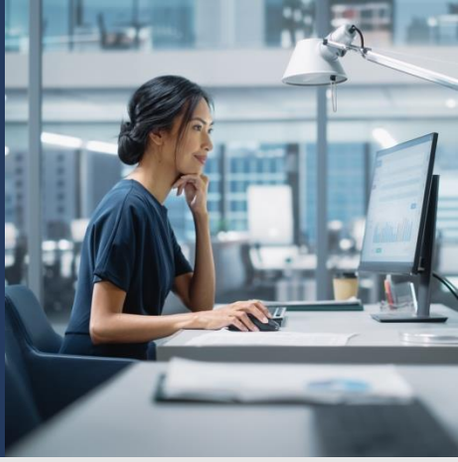
yourdevs
Transformando negocios

Modernice su centro de operaciones de seguridad (SOC) con Microsoft Sentinel

Microsoft Security



La frecuencia y la intensidad de los ciberataques siguen aumentando y el auge de las tecnologías de IA contribuye al creciente problema. **¿Puede su gestión tradicional de eventos e información de seguridad (SIEM) mantenerse al día?** Somos un socio de Microsoft centrado en la seguridad y queremos ayudarle a modernizar su SIEM.

Proteja su entorno multinube y multiplataforma con un SIEM impulsado por IA

Microsoft Sentinel ofrece una solución escalable y nativa de la nube para la detección y respuesta completas a las amenazas. Diseñada para funcionar en todo su patrimonio digital, obtendrá una única solución para la detección de ataques, la visibilidad de amenazas, la búsqueda proactiva, el análisis del comportamiento de usuarios y entidades (UEBA) y la respuesta a amenazas.

Recopilación y análisis de datos

- Elimine la configuración y el mantenimiento de la infraestructura con un SIEM nativo de la nube
- Opciones flexibles de ingesta y almacenamiento de datos
- Más de 350 conectores listos para usar
- Detección e implementación de casos de uso con un solo clic

Detección de amenazas en constante evolución

- Alertas correlacionadas automáticamente con incidentes priorizados
- Visibilidad completa de una ruta de ataque, incluso a través de múltiples fuentes
- UEBA incorporado para detectar automáticamente anomalías
- Enriquecimiento automático con inteligencia de amenazas respaldada por la investigación de amenazas de Microsoft

Responda en todas sus herramientas

- Orquestación, automatización y respuesta de seguridad (SOAR) integradas
- Automatizaciones personalizables para una respuesta rápida mediante aplicaciones lógicas
- Más de 200 soluciones creadas por Microsoft y más de 280 contribuciones de la comunidad

Uso de la búsqueda avanzada de amenazas

- Búsqueda integral en todos sus datos, incluidos los archivos
- Realice un seguimiento de la cobertura con el panel de MITRE
- Realice consultas sencilla sobre amenazas mediante KQL
- Busque en datos detallados mediante reglas de resumen

Investigue incidentes con todo el contexto

- Security Copilot integrado en la experiencia
- Aprendizaje automático integrado para la correlación de incidentes, optimizaciones de SOC, interrupción automática de ataques y mucho más
- Investigaciones visuales del alcance completo de los incidentes
- Modelo de datos unificado en Defender XDR y Defender for Cloud para la creación completa de incidentes y respuestas un 50 % más rápidas

Modernicemos juntos su SOC

Yourdevs está excepcionalmente calificado para acelerar su proyecto de modernización de operaciones de seguridad con nuestras ofertas de servicios.

Comuníquese con nosotros hoy mismo

contacto@yourdevs.cl
www.yourdevs.cl