Microsoft Sentinel

Microsoft Sentinel es una solución de Administración de eventos e información de seguridad (SIEM) y Respuesta automatizada de orquestación de seguridad (SOAR) que es escalable y nativa de nube. Microsoft Sentinel ofrece análisis de seguridad inteligente e inteligencia frente a amenazas en toda la empresa, de forma que proporciona una única solución para la detección de alertas, la visibilidad de amenazas, la búsqueda proactiva y la respuesta a amenazas.

Microsoft Sentinel proporciona una velocidad y escalabilidad casi ilimitadas en la nube para satisfacer sus necesidades de seguridad. Piense en Microsoft Sentinel como el primer SIEM como servicio que combina el poder de la nube y la IA para ayudar a los equipos de operaciones de seguridad a detectar de manera eficiente los ataques cibernéticos y detenerlos antes de que causen daños. Microsoft Sentinel mejora la investigación y la detección al proporcionar flujos de inteligencia de amenazas tanto de Microsoft como externos.

Microsoft Sentinel se integra con las soluciones de Microsoft 365 y ofrece cientos de productos de varios productos,

- Azure Identity Protection
- Microsoft Cloud App Security
- Azure Advanced Threat Protection
- Windows Advanced Threat Protection
- O365 Advanced Threat Protection
- Azure Information Protection

Recopila datos a escala de la nube de todos los usuarios, dispositivos, aplicaciones e infraestructura, tanto en las instalaciones como en las nubes. Detecte amenazas no detectadas anteriormente y reduzca los falsos positivos con análisis e inteligencia de amenazas de Microsoft sin igual. Aproveche las décadas de esfuerzos de seguridad cibernética de Microsoft para investigar amenazas con IA y buscar actividades sospechosas a escala. Responda a los

Microsoft Sentinel

incidentes más rápido con la orquestación integrada y la automatización de tareas comunes.