



Cerberus

Implementación Básica de Sentinel (SIEM)

Mediante el servicio de Implementación Básica de Sentinel (SIEM) de Noventiq podrá Compilar operaciones de seguridad de última generación con la nube y la IA de Microsoft Azure.

Alcance

- Implementación de Azure Sentinel y Configuración hasta 3 conectores.
- Horario de 8x5
- Definición de Arquitectura, configuraciones de políticas y Relevamiento físico.
- Creación de servicio Log Analytics workspace
- Creación de servicio Microsoft Sentinel
- Alistamiento de escenarios a monitorear
- Configuración de conector de Microsoft 365
- Configuración de conector de Plataforma Antivirus
- Configuración de conector de Azure Active Directory
- Validación funcionamiento conectores
- Validación funcionamiento eventos de los conectores
- Ajuste de datos y eventos de Microsoft 365
- Ajuste de datos y eventos de Plataforma de Antivirus
- Ajuste de datos y eventos de Azure Active Directory
- Monitoreo de los servicios
- Resolución y ajustes a problemas
- Optimización o configuración de servicios
- Documentación de servicio y configuraciones
- Transferencia de conocimiento

**En caso de necesitar más conectores podrán realizar la solicitud a el área de servicios para su estimación de tiempos y precios.*

**La implementación esta estipulada a ser realizada en un espacio de 60 horas, en caso de verse afectado este cronograma la adición de tiempos será asumida por el cliente solicitante del servicio.*

