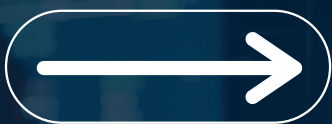


Your trusted partner for Cloud Security

SOC Platform by INNOVATE



INNOVATE
a MNE_EMO company

—> **Introducción**

INNOVATE es una empresa de **Servicios de Seguridad en la Nube**, fundada en Madrid, España en **2020**, con la misión de ser la empresa de referencia en Seguridad Cloud en España y Latinoamérica. Brindamos soluciones que abarcan todo el espectro de la problemática y complejidad de la definición, aplicación y operación de controles y servicios de seguridad en entornos Cloud nativos e híbridos. Somos una empresa del **grupo MNEMO**, una corporación multinacional con más de 20 años dedicada a los servicios de ciberseguridad en **España, Colombia y Panamá**.



INNOVATE, empresa referente en **Servicios de Seguridad Cloud**, ha apostado por la tecnología de Microsoft Sentinel para operar su servicio de monitorización y respuesta de incidentes, impulsado por la experiencia del SOC de MNEMO, el cual ha brindado sus capacidades en el análisis y escalabilidad (SIEM + SOAR) para la recopilación de datos de seguridad, detección de amenazas, investigación de incidentes, y una y respuesta eficaz y automatizada. Lo que ha proporcionado una capacidad para integrarse con fuentes de datos de terceros (on-prem y otras nubes), y de forma nativa, con el resto de los productos y soluciones Microsoft.

INNOVATE ha adaptado con éxito la red de SOCs de MNEMO para aprovechar al 100% las ventajas que las tecnologías de Microsoft ofrecen a nuestros clientes, prestando servicios de monitorización 24x7 basados en **Microsoft Sentinel**.

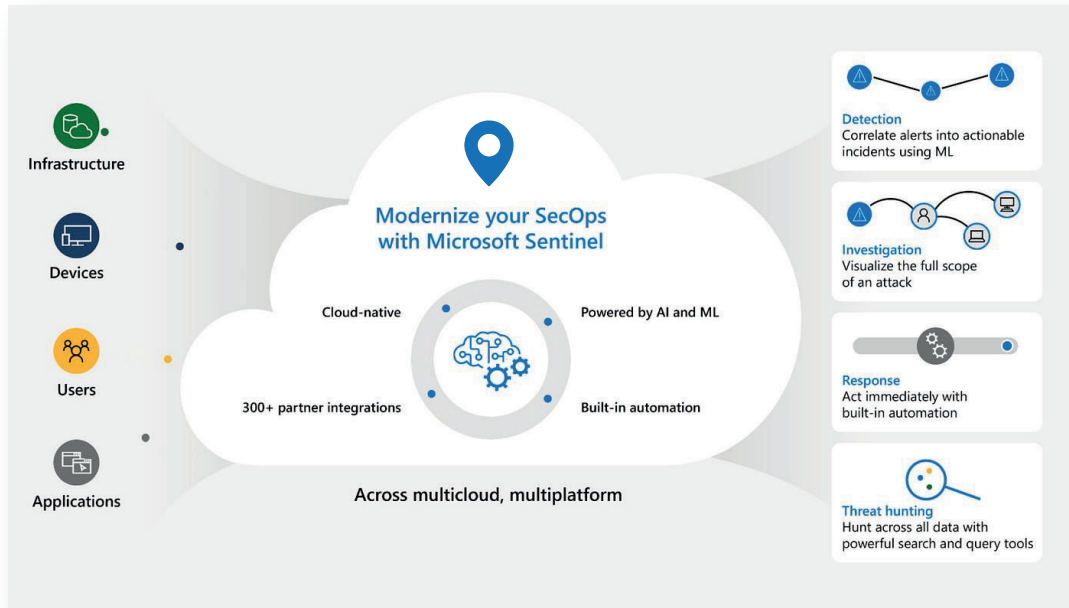
Contamos con un **equipo de profesionales de Seguridad, certificados y con experiencia** en la securización de las nubes de Microsoft y entornos híbridos a todos los niveles:

Certificaciones de Microsoft →

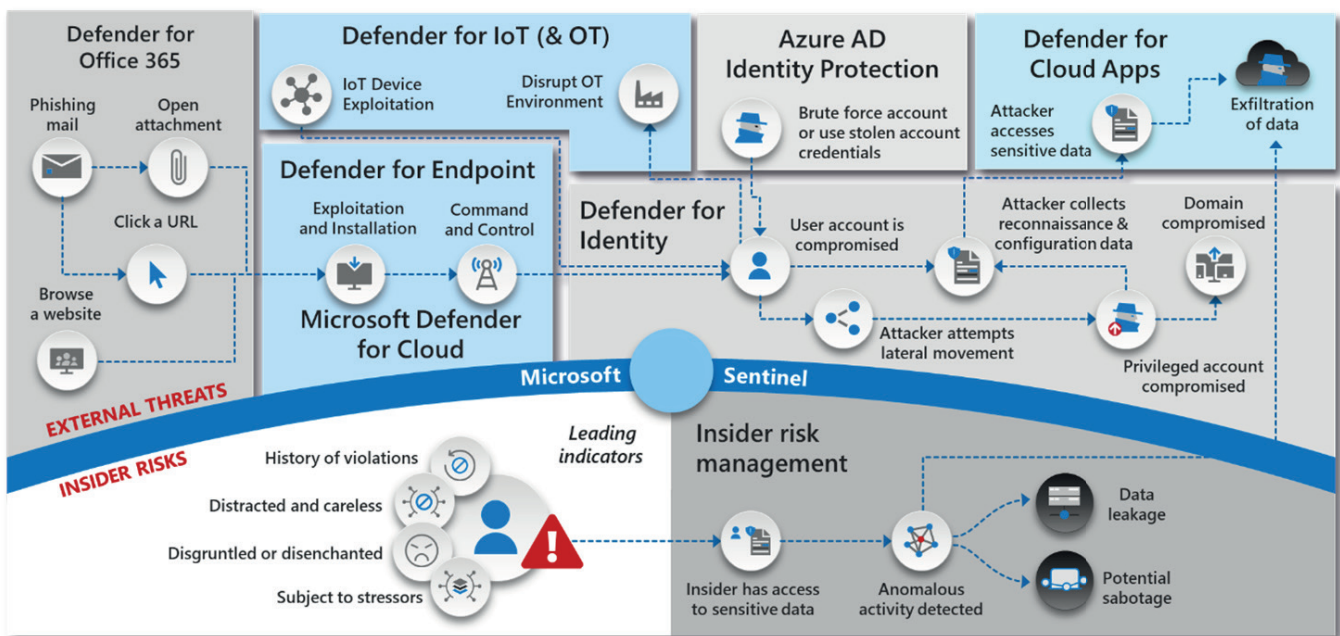
Certificación	Nivel
Azure Fundamental	1 Star
Fundamentals	1 Star
Security, Compliance, and Identity Fundamentals	1 Star
Azure Security Engineer	Associate (2 Stars)
Security Administrator	Associate (2 Stars)
Azure Network Engineer	Associate (2 Stars)
Enterprise Administrator	Expert (3 Stars)
Identity and Access Administrator	Associate (2 Stars)
Azure Administrator	Associate (2 Stars)
Security Operations Analyst	Associate (2 Stars)
Azure Solutions Architect	Expert (3 Stars)

→ **SOC Platform by INNOVATE**

INNOVATE ha creado un servicio gestionado con base en la tecnología de **Microsoft Sentinel**, un **SOC as a Service** diseñado para aumentar la **visibilidad** de las organizaciones sobre su **postura de seguridad** y responder mejor a los **incidentes de ciberseguridad**.



A través de nuestro servicio **Microsoft SOC by INNOVATE**, las empresas pueden beneficiarse de una rápida implementación de SIEM integrando las **fuentes de datos nativas Microsoft** para aumentar las capacidades de **detección, análisis y respuesta** basadas en los servicios de nube de Microsoft Azure, lo que permite reducir significativamente el nivel de riesgo y por lo tanto mejorar su postura de seguridad cibernética.



→ **Alcance del Servicio**



Despliegue y configuración de **Microsoft Sentinel** en suscripción y tenant propiedad del cliente.



Integración de **fuentes nativas Microsoft** (M365/Azure) mediante conectores.



Posibilidad de integrar **soluciones de seguridad de terceros** como fuentes de datos.



Configuración y activación de **casos de uso** asociados a las fuentes de datos integradas.

→ INNOVATE dispone de un **amplio catálogo** de casos de uso probados y operativos en **continua evolución** en entornos de producción reales.

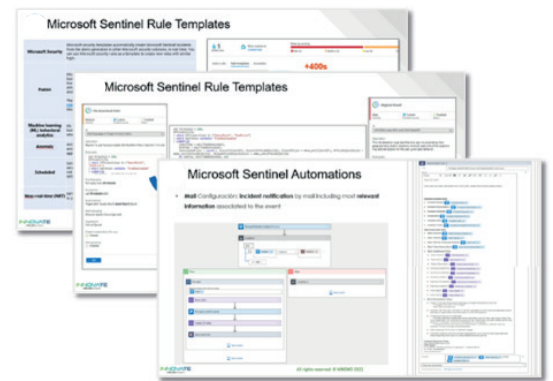
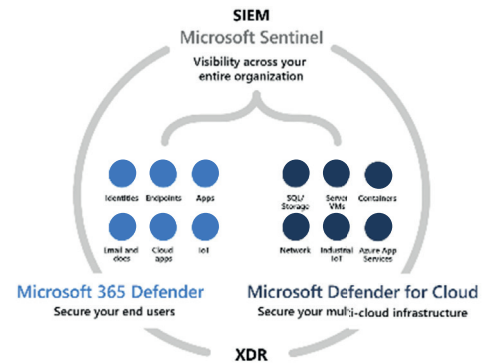
→ **Fine-tuning:** ajuste continuo de los casos de uso activos. Eliminación de falsos positivos, creación de white/-blacklists y ajuste de parámetros para una mayor optimización de las capacidades de detección alineadas con la necesidad del cliente y con el panorama de amenazas actual.



Monitorización de seguridad tiempo real + **Detección** de amenazas y anomalías 24x7.



Triage, control y priorización de eventos causantes de incidentes.





Configuración de **paneles de control** (Workbooks) para mostrar informes **personalizados interactivos y en tiempo real**.



Alertas automatizadas de incidentes de seguridad priorizados.



Configuración de **correos personalizados** con la información relevante de la alerta y planes de acción **recomendaciones de contención, mitigación y remediación**.

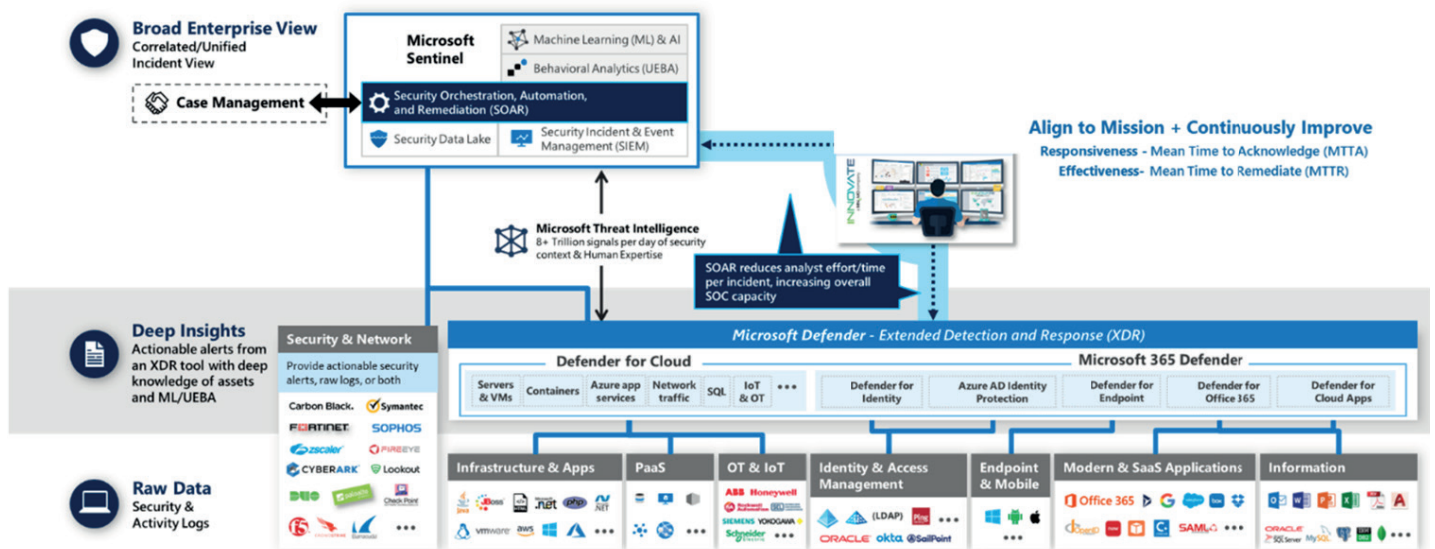


Posibilidad de integrarse con **herramienta de ticketing**.



Reporting periódico de métricas, tendencias y recomendaciones.

→ **Arquitectura de la Solución**





Contacto

Desde INNOVATE, a MNEMO company, te invitamos a ponerte en contacto con nosotros. Te ofreceremos el mejor asesoramiento y solventaremos tus dudas. Tendrás la posibilidad de hacerlo a través de diferentes métodos.



(+34) 91 417 67 76



Cardenal Marcelo Spínola 14,
Planta 5, 28016, (Madrid)



www.innovate.mnemo.com



innovate@mnemo.com