INNOVATE
a MNEMO company

Your trusted partner
for cloud security

Microsoft SOC by INNOVATE

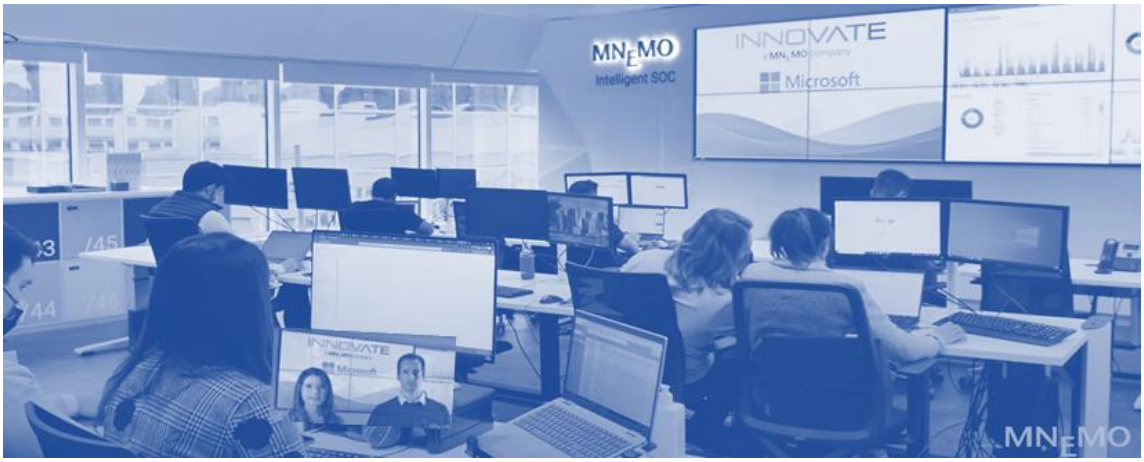
INNOVATE
a MNEMO company

Microsoft

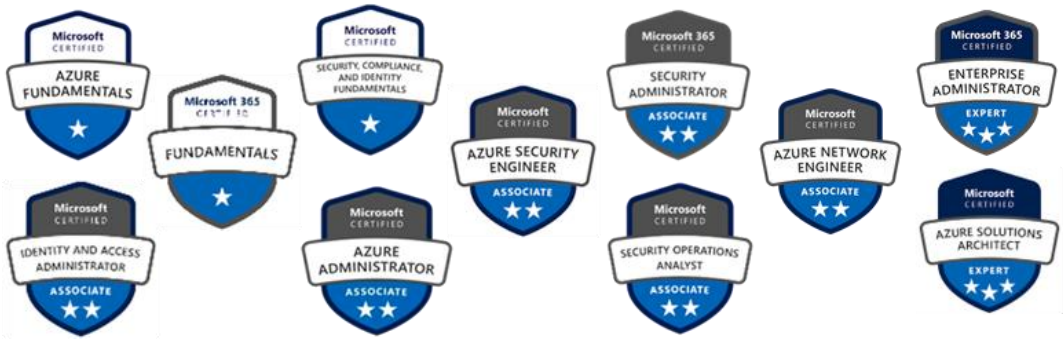
Your trusted partner for cloud security

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, él 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.**

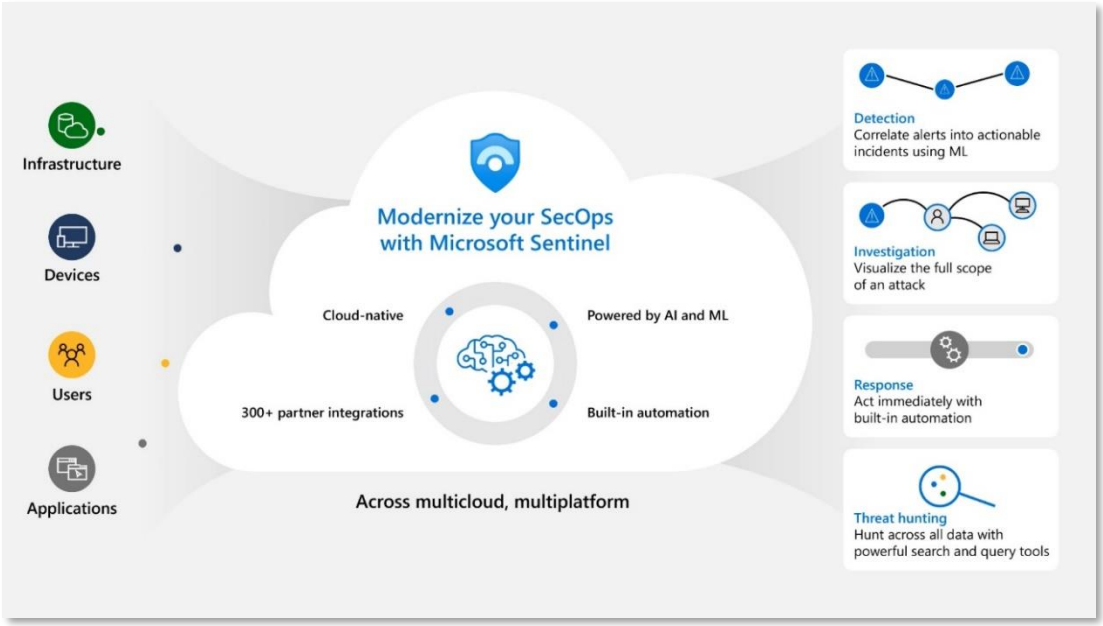


Contamos con un **equipo de profesionales de Seguridad**, **certificados** y con experiencia en la securización de las nubes de Microsoft y entornos híbridos a todos los niveles:

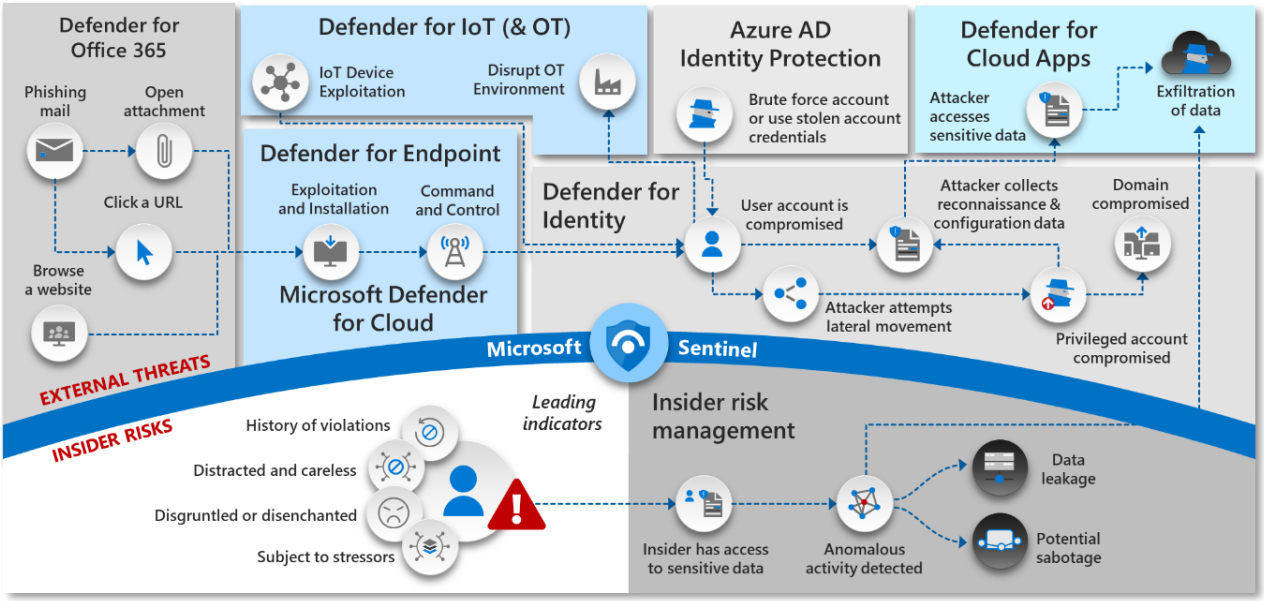


Microsoft SOC by INNOVATE

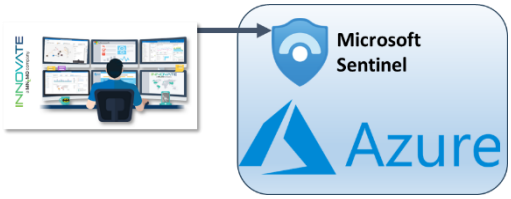
INNOVATE ha creado un servicio gestionado con base en la tecnología de **Microsoft Sentinel**, un **SOC as a Service** diseñado para aumentar la **visibilidad** de las organizaciones sobre su **postura de seguridad** y responder mejor a los **incidentes de ciberseguridad**.



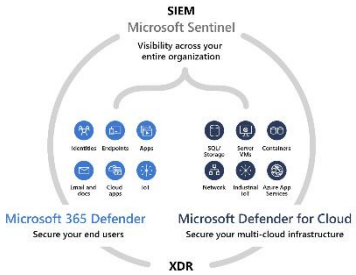
A través de nuestro servicio **Microsoft SOC by INNOVATE**, las empresas pueden beneficiarse de una rápida implementación de SIEM integrando las **fuentes de datos nativas Microsoft** para aumentar las capacidades de **detección, análisis y respuesta** basadas en los servicios de nube de Microsoft Azure,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



Alcance del Servicio

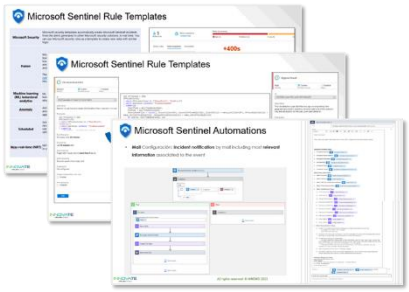


- Despliegue y configuración de Microsoft Sentinel en suscripción y tenant propiedad del cliente



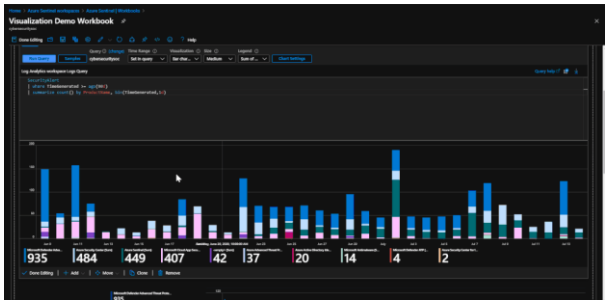
- Integración de **fuentes nativas Microsoft** (M365/Azure) mediante conectores
- Posibilidad de integrar **soluciones de seguridad de terceros** como fuentes de datos

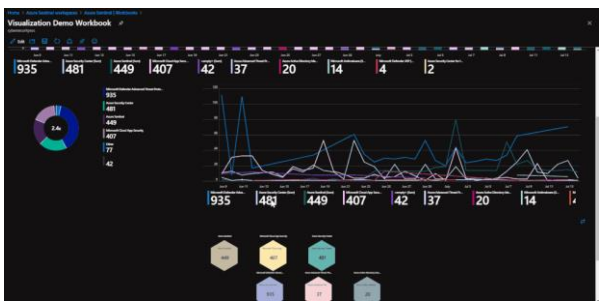
- Configuración y activación de **casos de uso** asociados a las fuentes de datos integradas
  - INNOVATE dispone de un **amplio catálogo** de casos de uso probados y operativos en **continua evolución** en entornos de producción reales
  - **Fine-tuning:** ajuste continuo de los casos de uso activos. 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**
- **Triaje, 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