Intelligent Cybersecurity| Brochure

# Centro de Operaciones seguras para tecnologías Operativas (SOC OT)

# SOC Tecnologías Operativas (SOCT OT)

IT y OT están convergiendo, y las tecnologías como Big Data y Analytics, Cloud Computing, IoT, robótica y automatización, impresión 3D y realidad aumentada, están llevando la convergencia entre esos dos mundos anteriormente separados.

Por esta razón, las empresas están intentando recoger los beneficios de esos sistemas para apoyar sus objetivos. Con el aumento de esta convergencia, los ataques cibernéticos han alcanzado las redes de automatización. **Aunque utilicen protocolos específicos, las redes de automatización industrial también pueden sufrir ataques o invasiones cibernéticas,** y en esos casos el desastre puede ser mucho mayor que el de un ataque cibernético convencional, de hecho, puede afectar vidas a gran escala en un periodo corto de tiempo.

**Para reducir esos riesgos, NTT DATA ofrece el servicio SOC OT:** un monitoreo completo del ambiente OT de las empresas, detectando vulnerabilidades en los sistemas, identificando amenazas, analizando los comportamientos anormales y alertando sobre incidentes de **seguridad en ambientes críticos**.

Riesgos adicionales son introducidos cuando los sistemas OT están online, y existen varias suposiciones en torno a la seguridad OT que puede dejar a las organizaciones vulnerables a los ataques:

> **Los beneficios de que su compañía cuente con un servicio SOC (Security Operation Center) asegura una ventaja para estar protegida contra incidentes y ataques externos, sin importar hora ni lugar de donde provenga el incidente.**

# SOC OT

**Mi empresa necesita evolucionar rápidamente. ¿Puedo considerar la seguridad OT más adelante o "cuando sea necesario"?**

Seguridad, productividad, eficiencia operacional y rentabilidad, todas quedan comprometidas si usted no incorporara seguridad cibernética en sus ambientes de TI y OT desde el inicio, ya que estará vulnerable a las amenazas cibernéticas.

**Los dispositivos OT han funcionado bien durante años; no es una prioridad aplicar parches, y eso puede provocar la interrupción de los negocios, si se hace.**

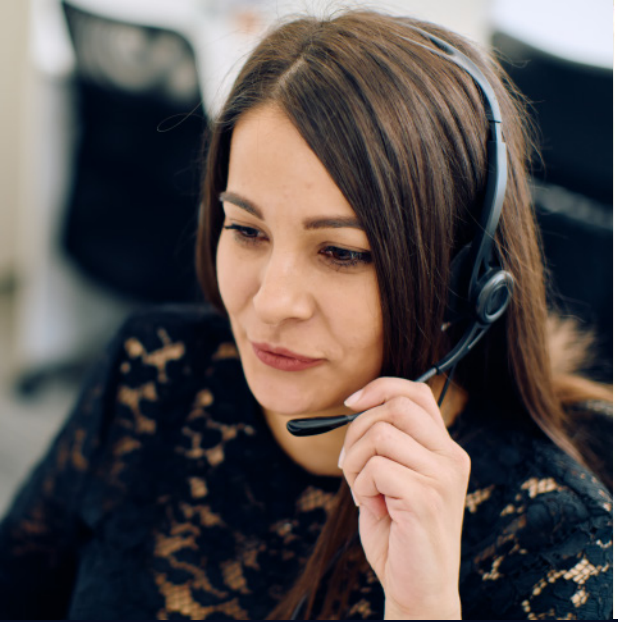
Higiene de seguridad básica en dispositivos OT nuevos y antiguos, como parches y actualizaciones de firmware, son esenciales para reducir el riesgo.

**Mi red OT no necesita ser segmentada de mi red de TI.**

La segmentación es crítica para minimizar la propagación de amenazas en su red de TI y en su red OT, para monitorear de forma eficiente el comportamiento anormal y para controlar y prevenir accesos innecesarios.

**Las operaciones de seguridadno necesitan ser centralizadas.**

Si no se aborda la seguridad que incluye TI, OT y otras áreas relevantes de su empresa, es muy probable que su postura de Ciberseguridad presente brechas, dejando su empresa vulnerable. Mejore la visibilidad de las amenazas y vulnerabilidades en su infraestructura de OT, permitiendo que identifique, proteja, detecte, responda y recupere de forma más eficaz que antes.



# Cómo opera el servicio SOC OT

**SOC OT es un servicio** que contempla la implantación y/o gestión de sensores pasivos específicos para las redes de automatización (IDS). Estos sensores reciben copia del tráfico y, a través de esa información, es posible obtener la visibilidad de la red OT, determinando los activos existentes. A partir de ese momento, de forma constante, son identificadas las vulnerabilidades del ambiente y se realizan recomendaciones de mejoras como, por ejemplo, segmentaciones de red siguiendo el modelo Purdue.

**De forma proactiva, NTT DATA identifica las vulnerabilidades,** los desvíos de comportamiento y las amenazas de seguridad, y alerta al cliente a través de recomendaciones de remediación y/o mitigación

# Nuestro SOC OT ofrece:

- SOC 24x7 con especialistas certificados en seguridad.
- Gestión de la plataforma de monitoreo, incluyendo el estado y disponibilidad, aplicación de parches y respaldo de las configuraciones.
- Visibilidad.
- Gestión de riesgos y vulnerabilidades.
- Detección de amenazas.
- Configuración de la plataforma, incluyendo ajuste preciso de reglas y alertas.
- Monitoreo de eventos y alertas de incidentes de seguridad 24x7.


NTT DATA