Inycom
innovation technologies

SMART SOLUTIONS FOR INDUSTRY 4.0

+34 902 500 001
industriadefuturo@inycom.es
www.industriadefuturo.es

NETWORK SECURITY

SEGURIDAD DE NUEVA GENERACIÓN PARA ACTIVOS CRÍTICOS EN EL SECTOR INDUSTRIAL

MANTÉN PROTEGIDAS TUS REDES SCADA/ICS

La plataforma de seguridad de nueva generación de Inycom puede utilizarse para **proteger las redes SCADA/ICS en cualquier entorno industrial con infraestructuras críticas**, mediante:

- Tecnología de inspección profunda de paquetes que proporciona funciones intuitivas e inteligencia sobre el tráfico de red.
- Control granular de aplicaciones, usuarios, contenido y tráfico web.
- Prevención de amenazas nativas contra amenazas conocidas y desconocidas.
- Gestión centralizada que agiliza la investigación forense y la remediación.

APLICACIÓN DE FIRMAS SCADA/ICS

La capacidad para controlar aplicaciones está basada en una gran base de datos de firmas de aplicaciones, válidas tanto para la informática general como para protocolos y aplicaciones del sector industrial para SCADA/ICS.

- Modbus
- DNP3
- Ethernet IP
- IEC 60870-5-104
- Synchrophasor
- OPC
- OSIsoft PI
- Cygnet
- FactoryLink
- ICCP

Además de contar con una gran base de datos de firmas de aplicaciones, protocolos específicos como Modbus y IEC 60870-5-104 tienen capacidades de control que permiten la monitorización y el control de subfunciones tales como lecturas y escrituras.

Modbus Function Control Signatures
Modbus-base
Modbus-write-multiple
Modbus-write-file-record
Modbus-read-write-register
Modbus-read-write-single coil
Modbus-read-single-register
Modbus-read-multiple-registers
Modbus-read-input-registers
Modbus-encapsulated-transport
Modbus-read-coils
Modbus-read-discrete-inputs
Modbus-mask-write-registers
Modbus-read-fifo-queue
Modbus-read-file-record
Modbus-read-holding-register

BENEFICIOS

- Mayor concienciación en seguridad, provocandon una **respuesta de incidentes más rápida** y una mejora de la política de seguridad.
- El **modelo de acceso con menos privilegios** reduce los ataques Footprint y promueve la integración **segura IT-OT**, el uso seguro de web y apliaciones SaaS.
- **Protección nativa de amenazas**, detectando exploits, virus y spyware, así como también malware moderno y APTs en todo su ciclo de vida de ataque.

Inycom
innovation technologies

NETWORK SECURITY

SEGURIDAD DE ACTIVOS CRÍTICOS EN EL SECTOR INDUSTRIAL

FIRMAS DE AMENAZAS PARA VULNERABILIDADES ESPECÍFICAS SCADA/ICS

Además de las firmas antivirus y antispyware, la base de datos de amenazas incluye firmas para exploits como:

- Específicos de proveedores, exploits para HMI, SCADA masters y otras aplicaciones sofware.
- Específicos de protocolo, exploits para Modbus, DNP3 y ICCP.
- Aplicaciones informáticas generales y de sistema operativo.

El objetivo prinicipal, es emplear estas firmas para proteger los sistemas de posibles exploits y reducir el tiempo de inactividad asociado a incidentes de seguridad.

A través del equipo mundial de investigación de amenazas se rastrean alertas de vulnerabilidad de múltiples organizaciones públicas y privadas para asegurar una cobertura óptima.

MODELO DE ACCESO A LA RED DE MENOR PRIVILEGIO

Una de las mejores prácticas recomendadas en guías como ISA-99 y IEC 62443 para definir zonas de seguirdad es la **segmentación de la red.** Mediante técnicas de segmentación no solo aportamos seguridad a la red, sino que también nos permite definir un control de acceso basado en privilegios.

Algunos ejemplos de casos de uso incluyen:

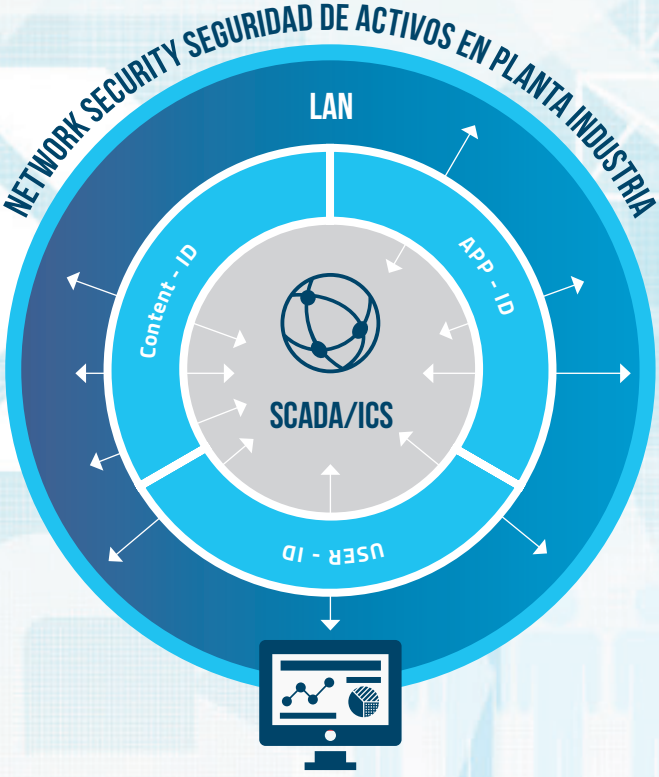
- Permitir el uso de aquellas apliaciones que están alojadas en el DataCenter.
- Control de usuarios, contenidos y apliación de QoS para apliaciones específicas.
- Restringir el uso de las apliaciones orientadas a la administración y gestión de equipos (SSH, Telnet, SNMP, FTP, etc.).
- Controlar el acceso a URLs y aplicaciones basadas en SaaS.
- Limitar el tráfico para controlar protocolos de red y un conjunto controlado de aplicaciones/protocolos necesarios.
- Rastreo de comandos ejecutados por el usuario para yudar en la correlacion de eventos.
- Permitir el acceso a determinadas zonas de red en función del tipo de aplicación y del rol del usuario.
- Supervisar y controlar el acceso de terceros a la VPN y a la máquina de Terminal Server.
- Implementar políticas cuyo comportamiento variará en función de la hora del día, la aplicación involucrada y la identificación del usuario.
- Aplicar en movilidad, las reglas de un Next Generation Firewall (NGFW) de forma consistente.

SOLUCIÓN DISEÑADA PARA REDES OT

En el corazón de esta plataforma hay un motor de clasificación avanzado que incluye App-ID, User-ID y Content-ID, donde:

- App-ID identifca todas las aplicaciones en todos los puertos durante todo el tiempo (vs. puerto/protocolo).
- User-ID identifica los usuarios o grupos de usuarios (frente a direcciones IP).
- Content-ID analiza el contenido de datos/archivos, amenazas, URLs, etc.

Inycom mitiga los riesgos asociados proactivamente con servicios integrados y soluciones que cumplen con requerimientos de un ***Proceso Industrial Seguro***



Diseñado para protocolos y ***apliaciones del sector industrial*** *para SCADA/ICS*

ENFOQUE EFECTIVO PARA LA PREVENCIÓN DE AMENAZAS OT

Los ciberataques modernos y los APTs se basan en el sigilo, la persistencia y la gran capacidad para evitar la seguridad tradicional durante todo el ciclo de vida del ataque.

La propuesta que desde Inycom aconsejamos es un efoque de extremo a extremo, combinado con soluciones de Sandbox basado en nube pública o privada capaz de detectar ataques que explotan vulnerabilidades de día cero a través de malware desconocido.

+34 902 500 001 / industriadefuturo@inycom.es / www.inycom.es