MERCURY: Seguridad Activa para Infraestructuras Industriales

La compañía

· Fundada en 2012 para el desarrollo de tecnología de cifrado para entornos industriales.

· Participada por Mundi Ventures, uno de los fondos de inversión tecnológicos más relevantes de UE.

· **appsec consulting** es una firma especialista en seguridad y partner estratégico de **Enigmedia**.

Nuestra tecnología

· Protege frente a amenazas avanzadas.

· Máxima seguridad con el mínimo impacto en el rendimiento.

· Despliegue fácil y adaptable a cada entorno industrial.

· Solución transparente y compatible con multitud de protocolos industriales: Modbus, CANBus, OPC-UA, etc.

· Autentica dispositivos y garantiza quién tiene acceso al dato.

· Configuración y monitorización remota. de todo el sistema

"Las **brechas de seguridad** en empresas de infraestructuras críticas cotizadas implican **devaluaciones de las acciones entre 17% al 30%** así como una disrupción del mercado que dura semanas"[1]

Los servicios de **analítica de datos y mantenimiento** predictivo habilitan importantes mejoras en los procesos productivos y reducción de costes. Pero también introducen vulnerabilidades y problemas que afectan a las necesidades de las plantas:

- **Asegurar disponibilidad de planta, es decir, tener el menor número de paradas posibles.**
- **Segmentar y monitorizar las comunicaciones**.
- Asegurar la comunicación y monitorización remotas.
- **Mantener una comunicación en tiempo real al añadir los elementos de seguridad.**

Por otro lado, las soluciones de seguridad IT no sirven para un enfoque OT, ya que tanto las técnicas como las limitaciones son distintas. Por ejemplo, el tiempo de vida medio de los dispositivos cambia de más de 20 años en OT a 3/5 años en IT.

Cada vez es más sencillo encontrar herramientas para hacer ataques automáticos. De hecho, más del **"40% de los ordenadores industriales sufrió un ataque durante el Q2 del 2016" - Ponemon'17**

Enigmedia ayuda a la industria en este proceso de digitalización a **securizar las redes industriales** de forma clara mediante**:**

- Incremento de la disponibilidad de la planta.
- Segmentación de las comunicaciones por dispositivo.
- Autenticación de usuarios y dispositivos.
- Control de acceso a los datos.
- Verificación de la integridad del dato.
- Mínima exposición de los procesos productivos a la red IT.
- Protección de la propiedad industrial e intelectual.

Todo ello **sin modificar la infraestructura existente**, integrando la seguridad a lo largo de toda la cadena de valor y el ciclo productivo, y con un despliegue entendible por los distintos equipos de trabajo/departamentos.

Además, gracias a su tecnología, Enigmedia garantiza la propiedad del dato y quién tiene acceso a él, desde el dispositivo inicial hasta su visualización. En resumen, Enigmedia asegura la integridad y confidencialidad de los activos digitales más importantes, los datos, sin que la transformación a la Industria 4.0 impacte en la infraestructura.

Casos de uso > INDUSTRIA GASÍSTICA:

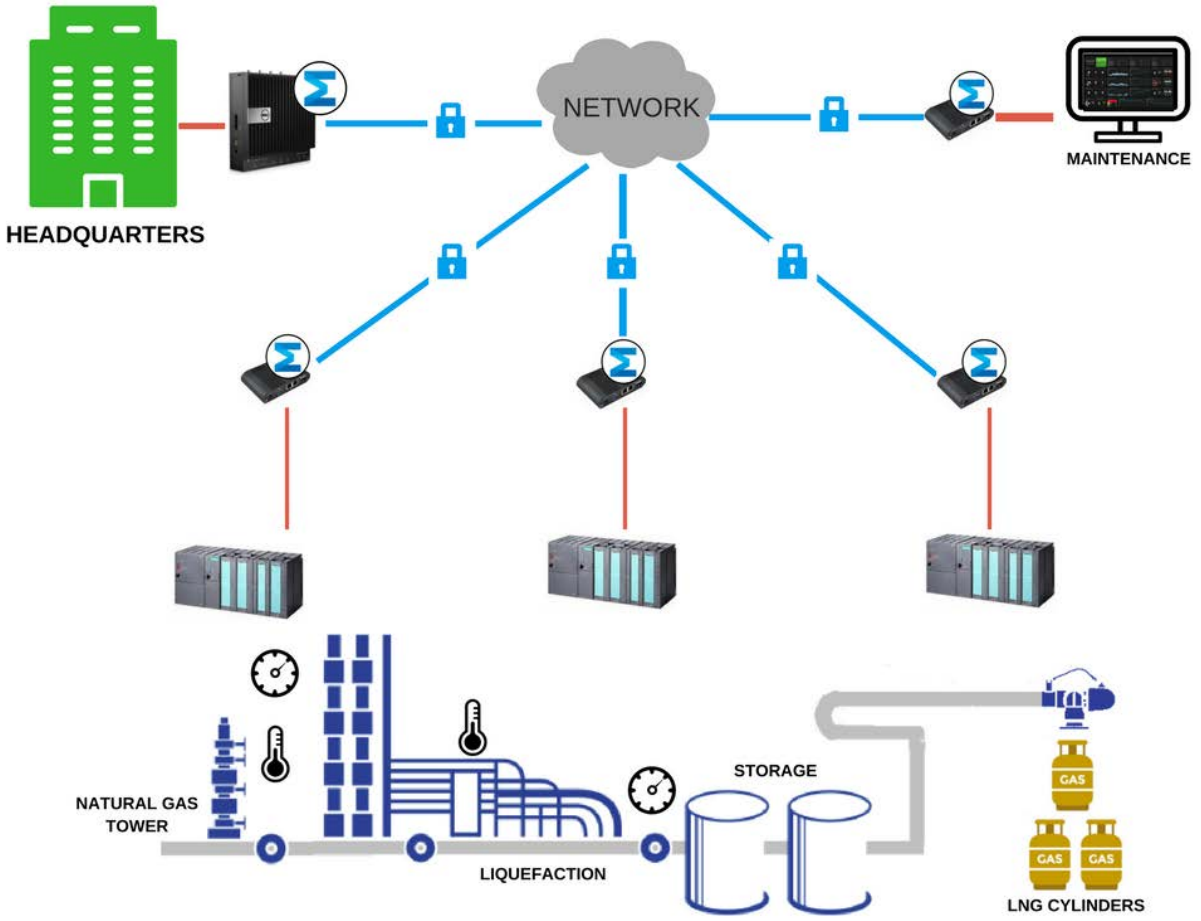
[1] Noah Susskind, *Cybersecurity Compliance and Risk Management Strategies: What Directors, Officer, and Managers Need to Know*, 11 N.Y.U. J.L. & Bus, 575.

ENIGMEDIA SL
Donostia -
San Sebastián
www.enigmedia.es

appsec consulting SL
Valencia
info@appsec.es
www.appsec.es

Enigmedia & appsec - © Copyright 2018 - All Rights Reserved

Máxima disponibilidad del equipamiento y total integridad de los datos



En la industria del gas se han dado ataques donde se ha inestabilizado la red inyectando información falsa a dispositivos de control. Estos ataques pueden costar hasta $8.4 M al día[2].

Mercury permite proteger dispositivos sin alterar la configuración de red, esto es, sin modificar los switches y dispositivos de red que transmiten la información. Además impide que un atacante con acceso a la red pueda averiguar el modelo de dispositivo está actuando gracias a que Mercury aísla el dispositivo de la red no protegida.

Si un atacante consiguiera acceso a la red, solo podría comprometer la seguridad de los dispositivos que no estén protegidos por Mercury, gracias a su capacidad para segmentar la red por dispositivo y cifrar la información de los mismos. De esta manera se garantiza la confidencialidad de todos los actores con acceso remoto a la red.

[2] Hillary Hellmann, Comment, Acknowledging the Threat: Securing United States Pipeline SCADA Systems, 36 Energy L.J. 157, 158 (2015)

Enigmedia & appsec - © Copyright 2018 - All Rights Reserved