

SAT-ICS para la monitorización de Entornos Portuarios

Contexto

Los entornos portuarios se han convertido en infraestructuras clave debido al auge del comercio internacional y la globalización. La búsqueda de una mayor eficiencia en las operaciones y la competencia entre puertos ha llevado a una digitalización del sector masiva en los últimos años que no es ajena a las infraestructuras industriales que permiten su operación. Pero este proceso ha abierto también una puerta a riesgos que debemos de ser capaces de identificar y gestionar, ya que de materializarse pueden resultar en un impacto grave en las operaciones portuarias.

Dispositivos implicados

Sistemas de control industrial

En el entorno portuario aparecen múltiples subsistemas de control tanto para los procesos específicos del entorno portuario como el sistema de ayudas a la navegación (faros, balizas, boyas, etc.), controles de acceso y portones o sistemas de detección de radiactividad en contenedores, como para otros sistemas auxiliares como redes de distribución de agua, redes de saneamiento, de contraincendios, de control de tráfico, distribución y medida de energía eléctrica., sistemas de seguridad como CCTV o control de accesos.

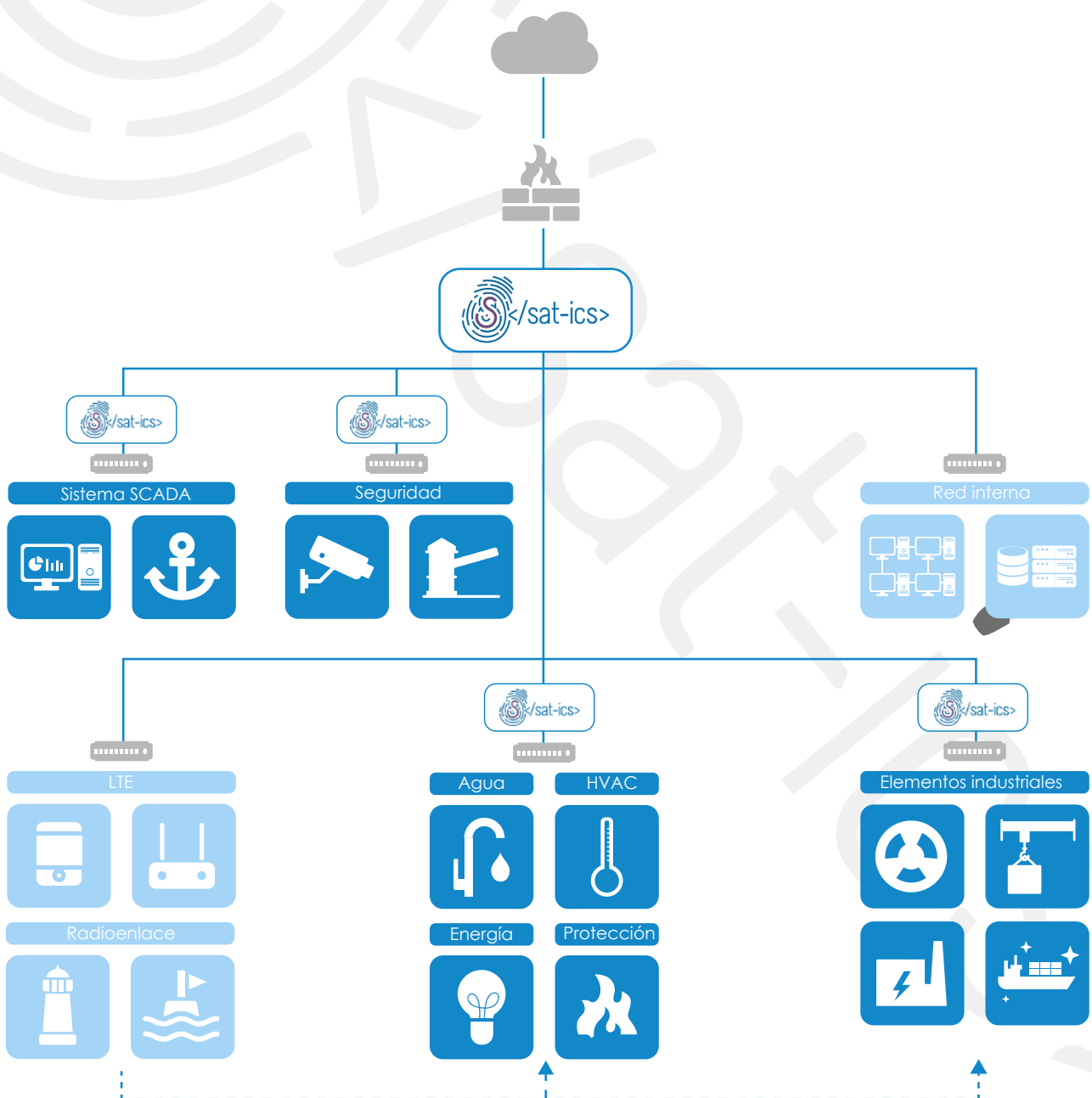
Tipología de comunicaciones

En este tipo de entornos se dan varios tipos de comunicaciones inalámbricas y cableadas: redes de comunicaciones móviles (3G, 4G o 5G en algunos casos), enlaces de microondas, fibra o cobre, entre otros. Aunque esta variedad de comunicaciones dificultan el monitoreo de algunos subsistemas, es posible analizar el tráfico en los puntos en los que estos sistemas se interconectan hacia los sistemas centrales.

¿Por qué SAT-ICS?

El sistema alerta temprana ICS (SAT-ICS), permite la detección a tiempo real de las amenazas e incidentes en el tráfico de las redes asociadas a estos dispositivos, incluso la rápida reacción y coordinación de la respuesta ante un posible incidente de seguridad. Los puertos pertenecen a un sector crítico y su protección debe afrontarse como tal.

Monitorización de entornos portuarios



¿Qué aporta a estos sistemas?

Detección de ataques e incidentes:

Con generación de alertas basadas no sólo en el análisis del tráfico de protocolos típicamente TI, sino también del tráfico en los protocolos específicos empleados en la comunicación entre controladores PLC, RTU, instrumentación, servidores SCADA, sistemas de seguridad, equipamiento IoT, etc.

Inventario y mapa de activos:

Para el apoyo a la gestión de las redes de dispositivos ciberfísicos a partir de la identificación pasiva de activos y el análisis del flujo de comunicaciones entre redes y conexiones a Internet.

Detección en base a anomalías:

El Sistema de Alerta Temprana en Sistemas de control Industrial (SAT-ICS) del CCN-CERT permite la detección en tiempo real de las amenazas e incidentes en el tráfico de las redes asociadas a estos dispositivos. Además, favorece una respuesta rápida ante un posible incidente de seguridad; algo fundamental en unas infraestructuras que pertenecen a un sector considerado como crítico.

Correlación:

El sistema central no solo detecta incidentes importantes de forma individual, sino que localiza eventos mucho más complejos que pueden involucrar a distintos organismos. Adicionalmente, proporciona acceso al mayor conjunto de reglas de detección que permite la detección de un mayor número de amenazas actualizadas de manera continua y enfocada para este tipo de entornos.

Elaboración de casos de uso específicos:

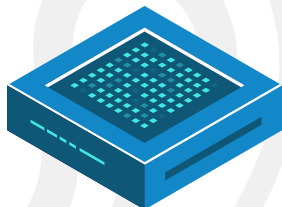
Es posible generar alertas específicas del tráfico de red para situaciones de riesgo definidas por el propio organismo y de las cuales se quisiera tener constancia. Para esto CCN-CERT requerirá que este facilite la información necesaria para poder configurar las reglas de detección apropiadas.

Informes estadísticos y soporte a la resolución de incidentes:

Información de gran valor para los responsables de seguridad de estos sistemas, que pueden ver en tiempo real el estado de su red y acceder a diversos informes estadísticos.

¿Qué se necesita para instalar el servicio SAT-ICS?

SAT-ICS es un sistema de monitorización que requiere de una sonda (servidor físico de alto rendimiento) para poder recolectar la información de los sistemas ciberfísicos y poder analizarla posteriormente.



Requisitos mínimos:

16 núcleos
32 GB de RAM
2 discos duros de 160 GB
2 interfaces de red
Hardware compatible con CentOS 7

¿Cómo se instala SAT-ICS?

Una vez adquirido el hardware necesario se instalará la ISO proporcionada por el CCN-CERT una vez cumplimentado el cuestionario de adhesión.



¿Qué coste aproximado tiene?

El coste de adquisición de la sonda de alto rendimiento se estima en un valor de 3000€. La gestión y administración de la sonda se realiza por el personal técnico del CCN-CERT, para mantener un sistema lo más homogéneo posible.



Para más información:

- Web: <https://www.ccn-cert.cni.es/gestion-de-incidentes/sistema-de-alerta-temprana-sat/sat-ics.html>
- E-mail: sat-ics@ccn-cert.cni.es

