Infraestructuras del ciclo integral del agua

SAT-ICS para la monitorización del Sector del Agua

Contexto

Los procesos relacionados con el sector del agua son considerados servicios esenciales y es por ello que deben proveerse los recursos necesarios para su protección. Dado el creciente número de ciberataques a infraestructuras críticas no debe descuidarse el impacto potencial de uno de estos incidentes sobre poblaciones completas.

Sistemas de monitorización

El agua, un sector diverso

El sector del agua es muy diverso, tanto desde el punto de vista de los procesos (captación, potabilización, distribución, saneamiento o depuración) como del número de actores implicados (entidades locales, empresas explotadoras, organismos gestores…) o tecnologías específicas (filtración, desinfección, procesos físico-químicos, desalación, bombeos, depósitos, telemandos de distribución, etc.)

Sistemas de control industrial

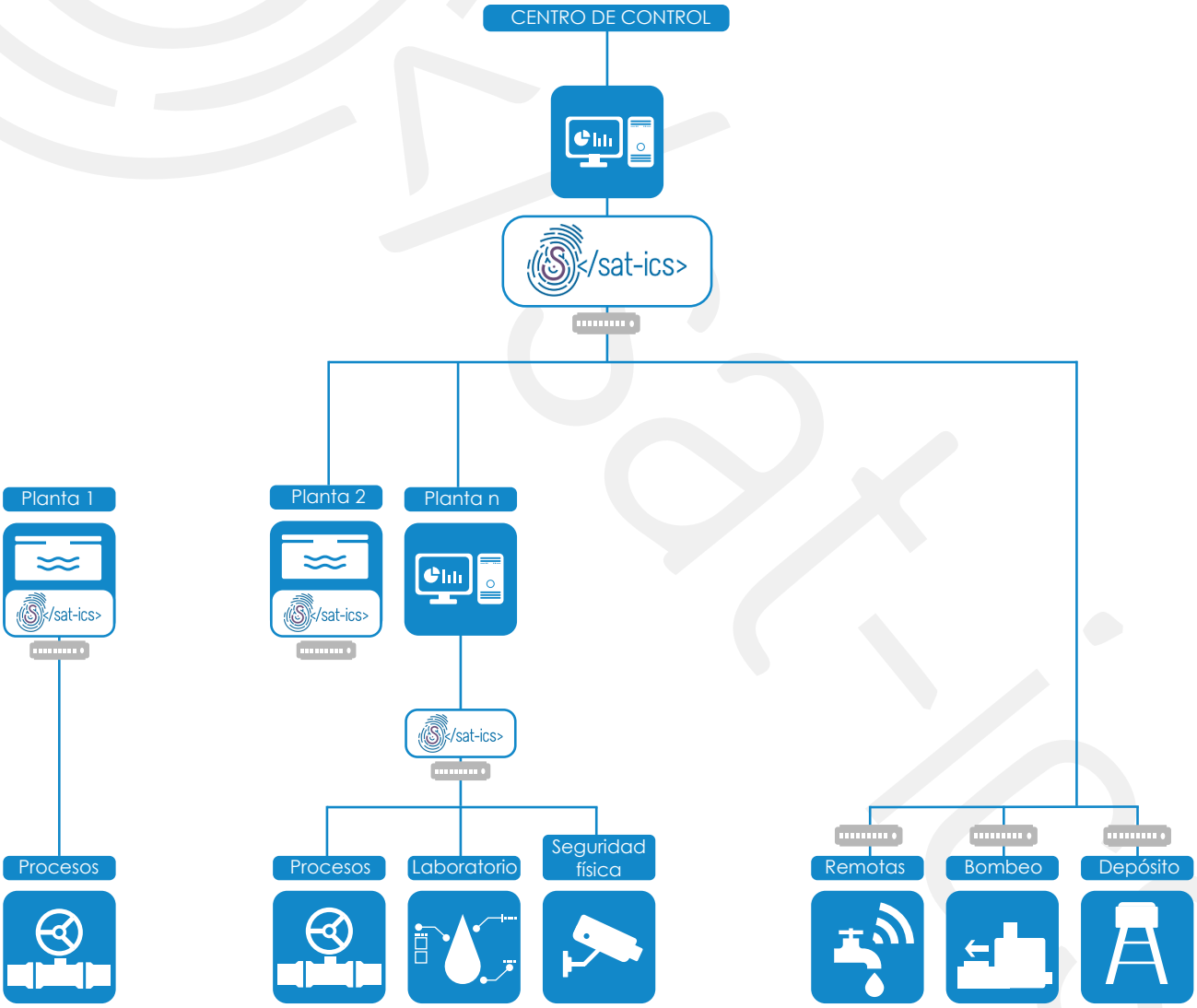
Esta diversidad se traslada a los procesos industriales y los equipos empleados para su control y supervisión, que además suelen incluir comunicación con instalaciones repartidas en áreas geográficas amplias, laboratorios, centros de control, plantas de tratamiento, unidades remotas, etc. No existe una única arquitectura que represente todos los tipos de infraestructuras y modos de explotación posibles dentro del sector, por lo que los puntos de red monitorizados dependen de la realidad de cada caso.

sat-ics@ccn-cert.cni.es www.ccn-cert.cni.es

¿Por qué SAT-ICS?

El Sistema de Alerta Temprana para Sistemas de Control Industrial ICS (SAT-ICS), permite la detección en tiempo real de las amenazas e incidentes en el tráfico de las redes asociadas a estos sistemas, incluyendo las comunicaciones internas y con ubicaciones remotas. De esta manera es posible detectar amenazas en entornos remotos que normalmente no son monitoreables, como las estaciones remotas, mediante el análisis del tráfico en los puntos de interconexión hacia el resto de sistemas centrales.

Monitorización de infraestructuras de gestión del agua



¿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, 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 unos entornos catalogados como infraestructura crítica.

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:

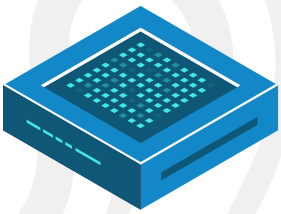
Es posible generar alertas específicas del tráfico de red para situaciones de riesgo definidas por el propio organismo y de las cuales se quisiera tener constancia. Para esto CCN-CERT requerirá que este facilite la información necesaria para poder configurar las reglas de detección apropiadas.

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 es aproximadamente 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

</sat-ics>

Infraestructuras del ciclo integral del agua

CCN-CERT centro criptológico nacional