SAT-ICS para la monitorización de Centros Sanitarios

Contexto

Debido a la convergencia tecnológica que estamos viviendo en los últimos años, los equipos existentes en los centros sanitarios cuentan con nuevas capacidades de interacción. Del mismo modo, han aparecido nuevos dispositivos y sistemas que también están interconectados y que, de presentarse algún ataque o abuso en su utilización, podrían tener un impacto directo en la seguridad de los pacientes.

Dispositivos implicados

Sistemas de control del edificio

Tecnologías como sistemas de gestión de edificios (o sus siglas en inglés: BMS -Building Management Systems-) que pudieran estar gestionados desde un mismo o varios SCADA y que gestionasen sistemas como: Agua Caliente Sanitaria (ACS), iluminación, elevadores, detección de incendios, gases clínicos, medidores de energía, abastecimiento de agua, sistemas de control de accesos, cámaras de seguridad (CCTV), etc.

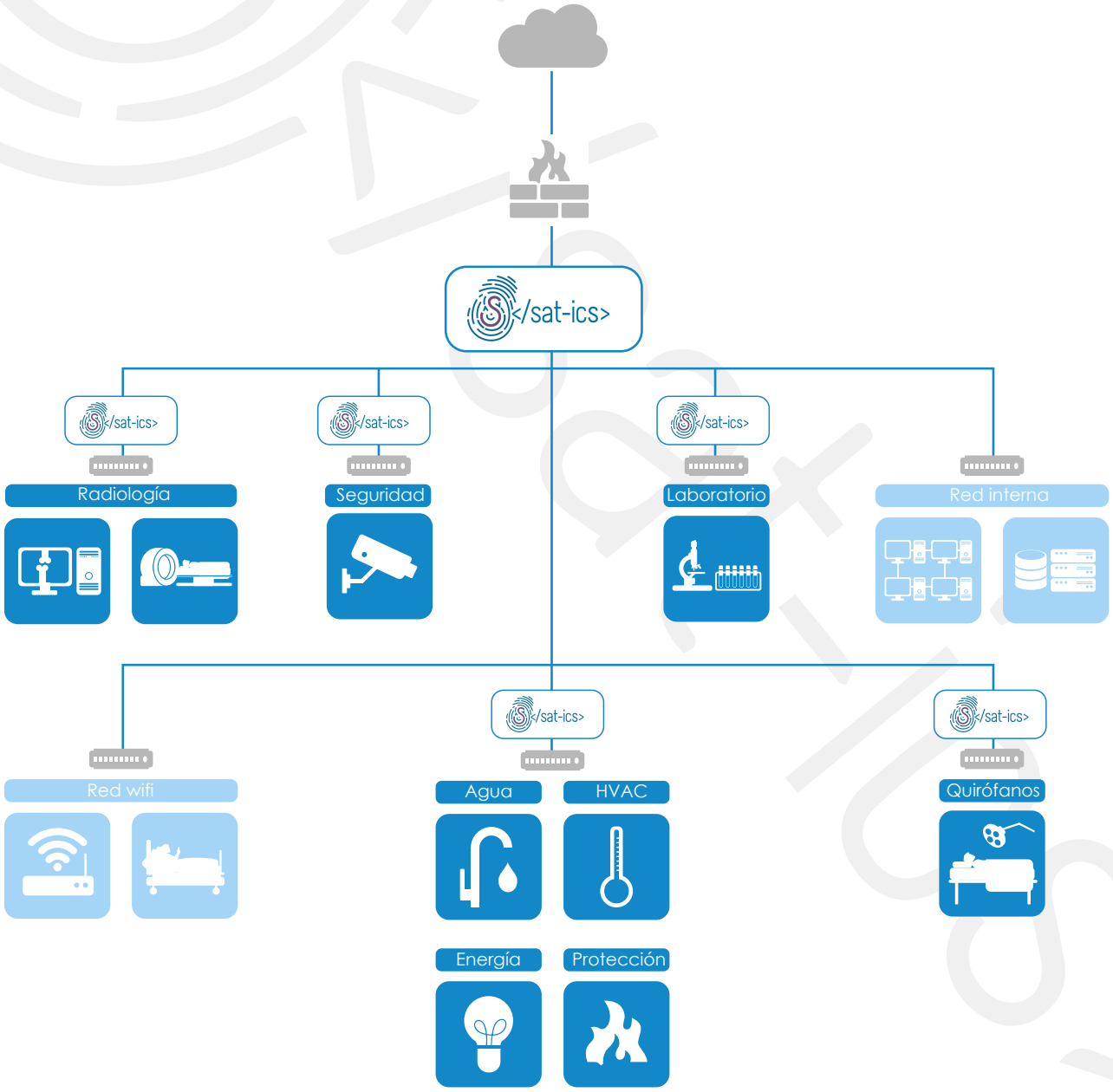
Electroimagen

Las comunicaciones y la transferencia de datos entre y con los dispositivos de electromedicina (DICOM, HL7, etc.) requieren de una supervisión y control para evitar cualquier posible abuso que pueda generar la ralentización del servicio o incluso la parada completa del centro sanitario.

¿Por qué SAT-ICS?

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 donde cada minuto cuenta.

Monitorización de entornos médicos



¿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, equipos de diagnóstico por imagen, 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 donde cada minuto cuenta.

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.