Sistema de Alerta Temprana

Sistemas de Control Industrial

Febrero 2023

LIMITACIÓN DE RESPONSABILIDAD

El presente documento se proporciona de acuerdo con los términos en él recogidos, rechazando expresamente cualquier tipo de garantía implícita que se pueda encontrar relacionada. En ningún caso, el Centro Criptológico Nacional puede ser considerado responsable del daño directo, indirecto, fortuito o extraordinario derivado de la utilización de la información y software que se indican incluso cuando se advierta de tal posibilidad.

AVISO LEGAL

ÍNDICE

1. INTRODUCCIÓN

Hasta hace relativamente poco, dentro de la categoría de sistemas de control industrial solo encajaban los **sistemas más tradicionales**: los encargados del control de las plantas industriales y sus componentes típicos: actuadores, instrumentación, PLC, remotas, software SCADA, etc**.** La convergencia tecnológica que estamos viviendo en los últimos años ha provocado la aparición de todo un nuevo conjunto de dispositivos y sistemas que podemos denominar ciberfísicos: se trata de todo el equipamiento con capacidad de procesamiento y conectividad que, además, permite una interacción con el mundo físico. En la actualidad, y como resultado del proceso de integración de estas nuevas tecnologías, en este grupo **podemos incluir otros entornos;** sistemas de gestión de grandes edificios (como centros de proceso de datos, edificios administrativos, centros sanitarios), dispositivos médicos (equipos de diagnóstico, tratamiento o análisis automático), sistemas integrados en Smart Cities como control de alumbrado, tráfico, gestión de aparcamientos, de uso de la energía, etc**.**

Como ya ocurre en otros ámbitos, el empleo de este tipo de tecnología lleva asociada una serie de riesgos de ciberseguridad que deben afrontarse adecuadamente, en parte mediante el uso de herramientas técnicas. Una de las herramientas al alcance de los responsables de seguridad de Organismos públicos que explotan o dependen de sistemas ciberfísicos es la monitorización de las comunicaciones para detectar usos indebidos, como situaciones que podrían propiciar el abuso de un potencial atacante o que directamente podrían estar relacionadas con una situación no deseada en la que se pudiera estar dando algún tipo de ataque o exfiltración de información y que, adicionalmente, podrían corresponder con anomalías en comunicaciones o comandos de operación que puedan poner en riesgo la propia operación o función que se desempeña.

Disponer de una visión holística y distribuida de los riesgos y amenazas que se producen en los distintos organismos, frente a una visión centrada en el tráfico de una única organización, permite mejorar de una forma considerable las capacidades de detección de tráfico anómalo que, de otro modo, podría pasar desapercibido.

Por este motivo, desde el año 2008 la Capacidad de Respuesta ante Incidentes de Seguridad de la Información del Centro Criptológico Nacional (CCN-CERT) viene desarrollando un Sistema de Alerta Temprana (SAT) para la detección de incidentes y anomalías que afecten a sistemas del Sector Público, a empresas y organizaciones de interés estratégico para el país que permite realizar acciones preventivas, correctivas y de contención. En un primer momento, este servicio comenzó su desarrollo con la monitorización de la Red de Intercomunicación de todos los organismos de la Administración Pública española, SARA. Posteriormente, ya en el año 2010, el servicio se extendió a los accesos de Internet de las distintas administraciones (SAT de Internet). Por último, en 2016 comenzó el desarrollo del servicio de monitorización de los sistemas de control industrial/ciberfísicos que están en operación en infraestructuras y organizaciones de interés estratégico para el país (SAT ICS).

A través de este servicio, el Centro Criptológico Nacional, en colaboración con el organismo adscrito, puede detectar multitud de tipos de ataque, evitando su expansión, respondiendo de forma rápida ante el incidente detectado y, de forma general, generar normas de actuación que eviten futuros incidentes. Al tiempo, y gracias al almacenamiento de un

número progresivo de eventos, es posible contar con una panorámica completa y veraz de la situación de los sistemas de las administraciones públicas españolas que posibilite una acción preventiva frente a las amenazas que sobre ellas se ciernen.

2. ¿QUÉ ES EL SISTEMA DE ALERTA TEMPRANA SAT-ICS?

A pesar de la multiplicidad de organizaciones que dependen para su operación de sistemas ciberfísicos, este tipo de equipamiento y sus comunicaciones reúnen una serie de características similares desde el punto de vista de la operación y la seguridad; esto hace posible el despliegue de un sistema de alerta basado en el **análisis del tráfico de red** siguiendo una estrategia común: estructura de comunicaciones bien acotada, dispositivos en la red sometidos a cambios poco frecuentes, poca diversidad de tráfico en un contexto bien definido y, finalmente, uso de protocolos específicos.

El Sistema de Alerta Temprana SAT-ICS es un servicio desarrollado e implantado por la Capacidad de Respuesta a Incidentes de Seguridad de la Información del Centro Criptológico Nacional (CCN-CERT) para la **detección en tiempo real** de las amenazas e incidentes existentes en el tráfico en las redes asociadas a sistemas ciberfísicos del Organismo adscrito. Su misión es detectar patrones de distintos tipos de ataque y amenazas mediante el análisis del tráfico, incluyendo el tráfico en protocolos de uso específico gracias a capacidades de DPI (*Deep Packet Inspection*).

Figura 1. Arquitectura SAT-ICS

3. BENEFICIOS APORTADOS A LOS ORGANISMOS ADSCRITOS

El Sistema de Alerta Temprana SAT-ICS tiene como principal función la **detección temprana en el caso que se produzca un incidente de seguridad** en la red, para que puedan aplicarse las medidas necesarias de contención y de eliminación de la amenaza y poder evitar que el intento de ataque sea fructífero o, en su caso, minimizar el posible impacto. Ofrece **ventajas significativas con independencia de que se disponga de una solución de monitorización desplegada** (siendo compatible con ella) o no. En este último caso, permite desplegar una solución gestionada por un equipo de expertos y que incorpora las últimas tecnologías.

En general, las ventajas para cualquier organización podrían resumirse en las siguientes características del servicio:

- **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.

- **Mapa de activos.** Para el apoyo a la gestión de las redes a partir de la identificación pasiva de activos y el análisis del flujo de comunicaciones entre redes internas y conexiones a Internet.

- **Inventario de activos** implicados en la monitorización.

- **Correlación.** El sistema central no solo detecta incidentes de forma individual, sino que se pueden detectar eventos mucho más complejos que pueden involucrar a distintos organismos.

- Acceso al mayor conjunto de **reglas de detección.** Mediante fuentes propias como externas, integradas por el equipo de expertos del CCN-CERT que permite la detección de un mayor número de amenazas actualizadas de manera continua.

- Detección en base a **anomalías** dentro de la red**.** La elaboración de líneas base de las comunicaciones y comandos de operación habituales de la red permite detectar anomalías dentro del comportamiento de la misma a fin de, no solo detectar algún posible abuso o riesgo para los sistemas, sino también algún tipo de problema de configuración o que pudiese ser susceptible de alguna corrección.

- Elaboración de **casos de uso específicos.** Generación de alertas mediante la información proporcionada al CCN-CERT sobre casos de uso específicos en su red de los cuales se quisiera tener constancia, elaborando nuevos analizadores de red y/o reglas de detección para éstos.

- **Informes** estadísticos y datos de estado de su red**.** Información de gran valor para los responsables de la seguridad de estos sistemas, pudiendo ver en tiempo real el estado de su red con respecto a la seguridad, así como acceder a informes estadísticos.

- **Soporte a la resolución de incidentes.** Como CERT Gubernamental/Nacional español, el CCN-CERT ofrece a todos los organismos su colaboración para una detección, contención y eliminación de cualquier ataque que pueda sufrir a sus sistemas.

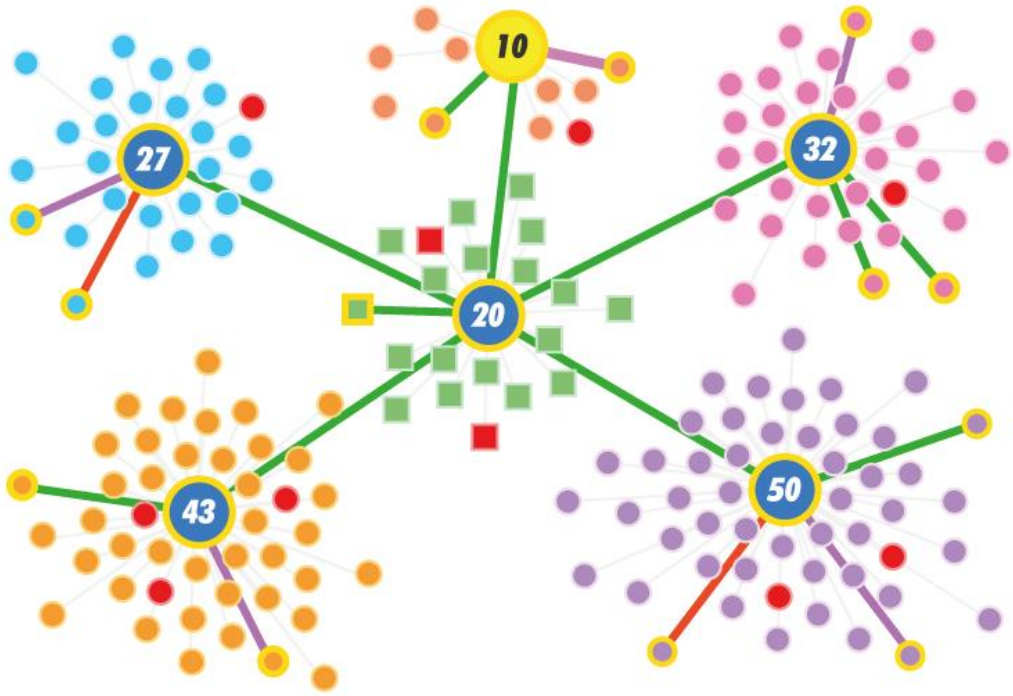

Figura 2. Mapa de activos y conexiones

4. DESPLIEGUE DE LA SONDA SAT-ICS

Para su puesta en marcha es necesaria la implantación de una **sonda individual** en la red del Organismo, que se encarga de detectar y recolectar la información de seguridad más relevante y, después de un primer filtrado, enviar estos eventos de seguridad hacia el **sistema central** que realiza una correlación entre los distintos elementos y entre los distintos dominios (organismos). Inmediatamente después, el Organismo adscrito recibe los correspondientes avisos y alertas sobre los incidentes detectados.

La sonda es un servidor dedicado que incorpora varias herramientas de detección y monitorización, incluyendo un sistema de detección de intrusos (IDS – *Intrusion Detection System*) y otros agentes de propósito específico, y que debe contar al menos con dos interfaces de red diferenciados:

- Interfaz de **análisis**: recibe una copia del tráfico del organismo para analizar. Este interfaz solo lee el tráfico fuera de línea, sin modificarlo en ningún momento, y sólo aquel que es necesario para desarrollar su función. Existen distintas opciones para garantizar que la sonda no introduce tráfico en la red a través de la interfaz de monitorización: configuración en la propia electrónica de red, empleo de cables unidireccionales, etc.
- Interfaz de **gestión**: conecta a través de Internet de forma segura con el sistema central de monitorización/correlación, haciendo uso de la infraestructura del Organismo o de una conexión independiente.

De este modo, el despliegue de la sonda se realiza de la siguiente manera:

- Instalación de la sonda en el Organismo y configuraciones necesarias en la **electrónica de red** para enviar hacia la sonda el tráfico a analizar.

- La **conexión entre la sonda y el sistema central** se realiza siempre de forma segura, a través del establecimiento de un túnel cifrado. Esta conexión puede realizarse a través de la salida a Internet del Organismo adscrito o a través de una salida dedicada hacia Internet. El establecimiento de este túnel cifrado se inicia desde la sonda hacia el sistema central, no siendo necesaria ninguna infraestructura adicional por parte del organismo.

- La sonda se **gestiona** completamente desde el **CCN-CERT**, no siendo necesaria la realización de tareas de administración por parte del personal del Organismo. Eventualmente se solicitaría apoyo al Organismo en el caso que fuera necesaria la realización de tareas puntuales que no pudieran realizarse de manera remota.

- La selección de las **redes de sistemas ciberfísicos** monitorizadas en cada Organismo dependerá de la arquitectura de red, tipo de comunicaciones existentes (TCP, serie, etc.), la existencia de conexiones remotas o con otros niveles de supervisión superiores, etc. De forma general, se recabará al Organismo información de forma previa al despliegue y tras un análisis se realizará una propuesta de arquitectura de monitorización. Con los eventos recibidos se realiza una **correlación avanzada** de eventos en el sistema central, permitiendo la detección de ataques hacia los distintos organismos adscritos al sistema, la presencia de código dañino en estas redes, usos no habituales en estos sistemas, etc.

- La **gestión, actualización y mantenimiento** del sistema central está a cargo del CCN-CERT, que lleva a cabo tareas de administración, maduración de las reglas de detección e inclusión de nuevas funcionalidades y herramientas. De hecho, periódicamente se realiza la integración de numerosas reglas de detección, propias y externas, completando y ampliando la inteligencia del servicio y su capacidad de detección. Las reglas propias son generadas a partir de la información obtenida durante la investigación de otros incidentes de seguridad y a partir de la información recibida de otros organismos con los que se mantiene un intercambio de información referente a incidentes de seguridad.

- Los usuarios pueden acceder en tiempo real a **información relevante** de los eventos generados por la sonda de su organismo, a informes periódicos y a la información de los incidentes de seguridad notificados a través de un portal accesible en Internet. Cada Organismo puede ver exclusivamente los eventos e informes relacionados con su red monitorizada.

5. PREGUNTAS MÁS FRECUENTES –FAQ-

5.1 ¿Qué es un sistema ciberfísico?

Un sistema ciberfísico es todo aquel dispositivo que integra capacidades de computación, almacenamiento y comunicación para controlar e interactuar con un proceso físico. Los sistemas ciberfísicos están, normalmente, conectados entre sí y también con servicios remotos de almacenamiento y gestión de datos.

5.2 ¿En qué entornos puede desplegarse SAT ICS?

La sonda SAT ICS puede **desplegarse en diferentes entornos**, tales como:

- Infraestructuras del ciclo integral del agua (captación, tratamiento (ETAP y EDAM), almacenamiento, distribución, saneamiento y depuración (EDAR)).
- Operadores de transporte y logísticos (autoridades portuarias, aeroportuarias, transporte terrestre, almacenes automatizados o grandes logísticas).
- Infraestructuras energéticas (generación, transporte, distribución eléctrica, plantas de regasificación y almacenamientos de hidrocarburos).
- Infraestructuras de tratamiento de residuos.
- Sistemas de radiodifusión.
- Manufactura.
- Centros sanitarios.
- Institutos y centros de investigación.
- Componentes de *Smart Cities* (sistemas de gestión de alumbrado público, control de tráfico, etc.).
- Sistemas de gestión de edificios (BMS - *Building Management Systems*).

5.3 ¿Qué es una sonda?

La sonda es un **servidor de alto rendimiento** que permite el análisis del tráfico de la red del Organismo adscrito, la generación de eventos específicos de seguridad y su envío de forma segura al sistema central. Consta de los siguientes elementos:

- La interfaz de gestión, que se conecta a la red del Organismo para enviar al sistema central del SAT los eventos generados por la sonda.
- Los interfaces de análisis, que reciben el tráfico a analizar y que no tienen dirección IP, siendo totalmente transparentes a la red.
- Un sistema de **detección de intrusiones** de red (NIDS), con reglas de detección específicas de diferentes fuentes (incluyendo específicas para sistemas SCADA) y de creación propia.

- Un conjunto de **agentes específicos** para detectar anomalías en entornos ICS, incluyendo un análisis de la estructura de comunicaciones de la red y los **disectores de protocolos industriales**.
- Un recolector de los eventos detectados para su envío al Sistema Central. Este agente inicialmente estará configurado para el análisis de los eventos generados por las distintas herramientas de detección que se incorporen.

5.4 ¿Dónde se instala una sonda?

La sonda puede implantarse en distintos puntos de la red dentro de la infraestructura del Organismo, típicamente en los anillos de comunicaciones industriales o en las interconexiones entre los niveles de control, campo y supervisión y sus comunicaciones con el exterior.

Dependiendo de la arquitectura de la red y las capacidades que esta ofrezca para la monitorización, se estudiará junto con el Organismo la estrategia que mejor se adapte a sus posibilidades, que se pueden clasificar a grandes rasgos en 2 tipos:

- **Monitorización interna** de las redes:

En aquellos casos en los que sea posible realizar un "puerto espejo" de la electrónica de red interna de las distintas redes de control o supervisión, se podrá monitorizar el tráfico interno de dichas redes de manera diferenciada, así como el tráfico que entre o salga de estas.

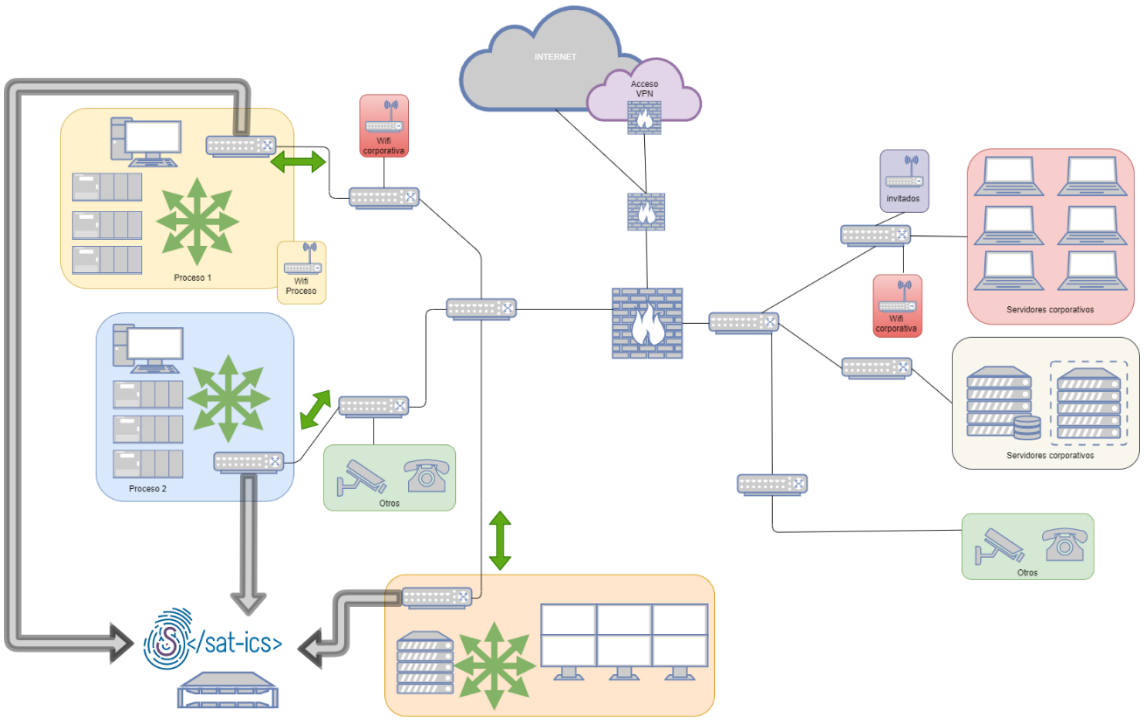

Figura 3. Esquema de monitorización interna

- **Monitorización perimetral** interna:

En aquellos casos en los que no se considere adecuado realizar un "puerto espejo" de la electrónica de red interna de las distintas redes de control o supervisión, se podrá (si la tecnología de la infraestructura lo permite) realizar una monitorización del tráfico que llega al cortafuegos o router que segmenta las distintas redes, con el fin de monitorizar todo el tráfico que entre o salga de las redes de sistemas ciberfísicos.

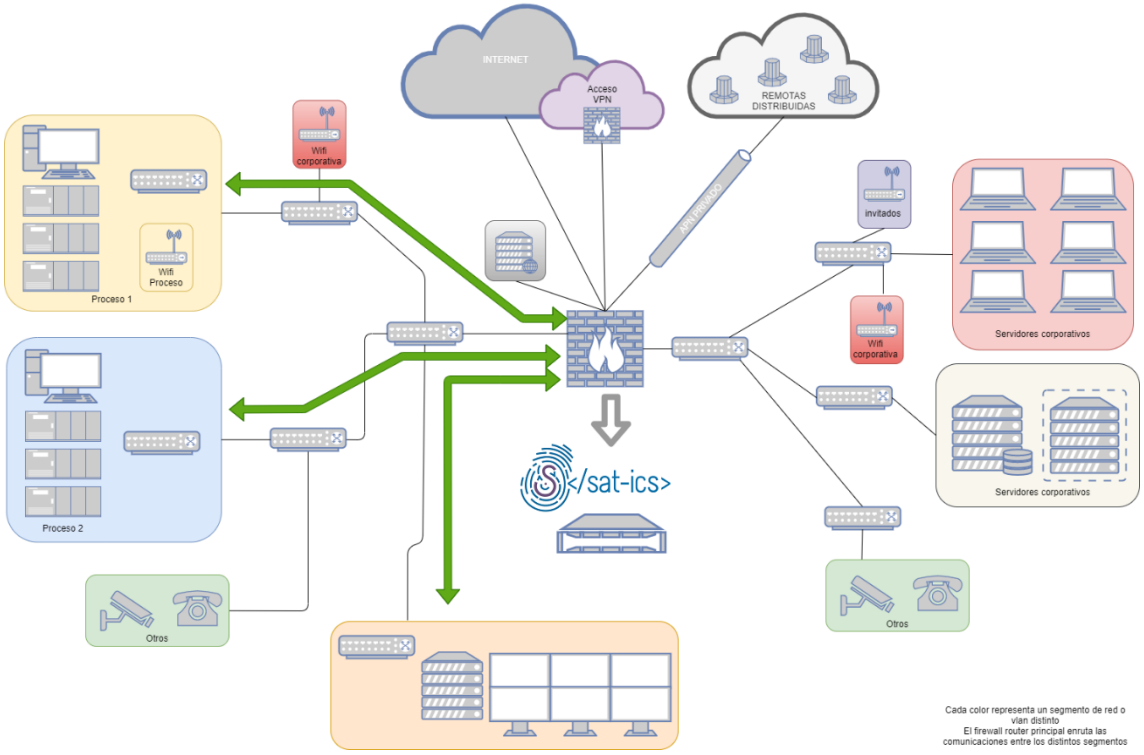

Figura 4. Esquema de monitorización perimetral

5.5 ¿Qué es el sistema central?

El sistema central es el encargado de la **recolección** de la información proveniente de las distintas sondas y de la **correlación** de eventos para detectar incidentes de seguridad.

Está compuesto por diferentes elementos:

- Recolector de eventos. Es el encargado de recibir los eventos que provienen de los diferentes sistemas a analizar y de enviarlos al bus de eventos del que se nutre el siguiente elemento.
- Motor de correlación. Es el encargado de procesar la información que llega al bus de eventos. Este elemento del sistema implementa reglas de correlación que son las que deciden si se genera o no una alerta en respuesta a los eventos recibidos.
- Consola única de operador. Es la que permite el análisis de las alertas generadas tras la correlación de los eventos recibidos por el sistema.
- Cuadro de mando activo. Es el que presenta información relativa a los procesos monitorizados y permite la visualización de indicadores.

5.6 ¿Quién monitoriza el sistema central?

La gestión, actualización y mantenimiento del sistema central está a cargo del CCN-CERT, que con un equipo de expertos en ciberseguridad lleva a cabo tareas de administración, maduración de las reglas de detección e inclusión de posibles nuevas fuentes.

5.7 ¿Qué características debe tener el servidor? (*)

Dependiendo de las características de la red y de los sistemas monitorizados, se recomiendan dos tipos diferentes de sonda, cuyos requerimientos *hardware* para el adecuado funcionamiento son los siguientes:

1) **Sonda Estándar:**

Requisitos mínimos	
Procesador	16 núcleos físicos (32 vCPU)
Memoria RAM	32 GB
Almacenamiento	2 Discos Duros 512 GB, en RAID 1 (Espejo)
Red	Interfaces de análisis (tantas como redes a analizar): tarjeta/s de red 1/10 Gigabit Ethernet con tecnología Intel (drivers e1000e, igb, ixgbe, i40e)
	Interfaz de gestión: tarjeta de red Gigabit Ethernet
Sistema Operativo	Hardware compatible con CentOS 7.7 (instalado por CCN-CERT)

2) **Minisonda:**

La minisonda (**) SAT-ICS está pensada para instalaciones industriales donde no es posible instalar la sonda SAT-ICS estándar por uno o varios de los siguientes motivos:

- Se dispone de poco espacio físico para la instalación de la sonda.
- Necesidades especiales de montaje en rack (carril DIN, etc.).
- Condiciones ambientales desfavorables (humedad, temperatura, polvo, etc.).
- El tráfico a analizar no supera 1Gbps de *throughput*.

Requisitos mínimos	
Procesador	8 cores, familia Xeon E-2*** o superior
Memoria RAM	16 GB
Almacenamiento	256 GB
Red	Interfaces de análisis (tantas como redes a analizar): tarjeta/s de red Gigabit Ethernet
	Interfaz de gestión: tarjeta de red Gigabit Ethernet
Salida video	VGA o HDMI
USB	Interfaz USB
Grado de protección ambiental	Según necesidad
Sistema Operativo	Hardware compatible con CentOS 7.7 (instalado por CCN-CERT)

(*) Los requerimientos *hardware* pueden sufrir variaciones en un futuro debido a la incorporación de nuevas capacidades de detección que incurran en una mayor demanda computacional.

(**) Cabe destacar que son equipos que van a estar trabajando 24x7 los 365 días del año. Es requerimiento esencial el uso de un equipo de tipo servidor, tanto si es enracable como para bandeja o para carril DIN. Debe evitarse el uso de equipos convencionales de puesto de trabajo.

5.8 ¿Cómo se envían los eventos al sistema central?

El transporte de los eventos se realiza de forma segura a través de un túnel cifrado por la salida de Internet del Organismo hacia el Sistema Central, con lo que la confidencialidad e integridad de la información queda garantizada. La conexión entre la sonda individual y el sistema central se puede establecer de dos formas:

- Conexión de la sonda a Internet a través de la infraestructura de Internet del Organismo adscrito.
- Conexión directa de la sonda a una conexión a Internet independiente de la red del Organismo.

5.9 ¿Qué información se envía al sistema central?

Las sondas únicamente envían hacia el sistema central alertas de seguridad generadas tras la detección de algún tipo de evento, definidos en las reglas de detección integradas en el sistema, y que responden a patrones de tráfico potencialmente dañinos, de comportamientos conocidos de determinado tipo de código dañino o a usos no habituales o potencialmente peligrosos de los sistemas de control industrial. **En ningún momento se realiza un envío del tráfico de red del Organismo** hacia el sistema central, manteniéndose así la privacidad en las comunicaciones.

5.10 ¿Qué tipo de ataques puede detectar el servicio SAT-ICS?

La finalidad de la sonda es detectar ataques que se produzcan en las redes del Organismo y dar una respuesta rápida y eficaz ante incidentes, aunque el trabajo de detección se centrará principalmente en detectar actividad anómala o potencialmente peligrosa en estos sistemas y en la detección de intentos de intrusión sobre estas redes. La base del servicio radica en la identificación de aquellas situaciones que pueden suponer un riesgo para la infraestructura y en la definición de reglas para su detección, partiendo del conocimiento de la forma en que se explotan este tipo de sistemas.

Una característica del sistema SAT-ICS es que **permite trabajar con los protocolos industriales**, analizando también el payload de los paquetes (***Deep Packet Inspection*** **o DPI**) para identificar el fin de un determinado comando: descargar o cargar programas en los PLC, escanear la red para identificar los equipos que forman parte de ella o el envío de comandos potencialmente peligrosos, por ejemplo. Actualmente es posible analizar el tráfico de los protocolos recogidos en la siguiente tabla:

Modbus TCP / RTU encapsulado	**IEC 60870-104**	**ICCP**
DNP3	**Siemens S7COM**	**EthernetIP/CIP**
DICOM	**PROFINET (DCP,RTC)**	**BACnet IP**
LonTalk	**Omrom FINS**	**SAP-20**
OPC DA	**OPC UA**	

Nuevos protocolos se añaden a la lista continuamente. También existe la posibilidad de implementar el análisis de protocolos específicos desarrollados a medida para un Organismo.

5.11 ¿Qué es el portal SAT?

El portal del SAT es el lugar en el que el personal responsable de la ciberseguridad del Organismo adscrito puede **visualizar en tiempo real** los eventos generados por su sonda y que han sido enviados al sistema central. Además, permite acceder a la herramienta LUCIA para la gestión de los incidentes que hayan sido detectados por la sonda y comunicados al organismo.

Del mismo modo, también es posible el acceso a estadísticas e informes sobre el servicio ofrecido por este Sistema de Alerta Temprana.

A través de este portal también es posible visualizar de forma gráfica el **mapa de activos** de las redes monitorizadas, con sus correspondientes comunicaciones habituales o anómalas y enriquecidas con información adicional extraída de forma pasiva. Este mapa de activos proporciona capacidades de búsqueda y filtrado para facilitar la investigación de incidentes o simplemente aumentar el conocimiento de la red.

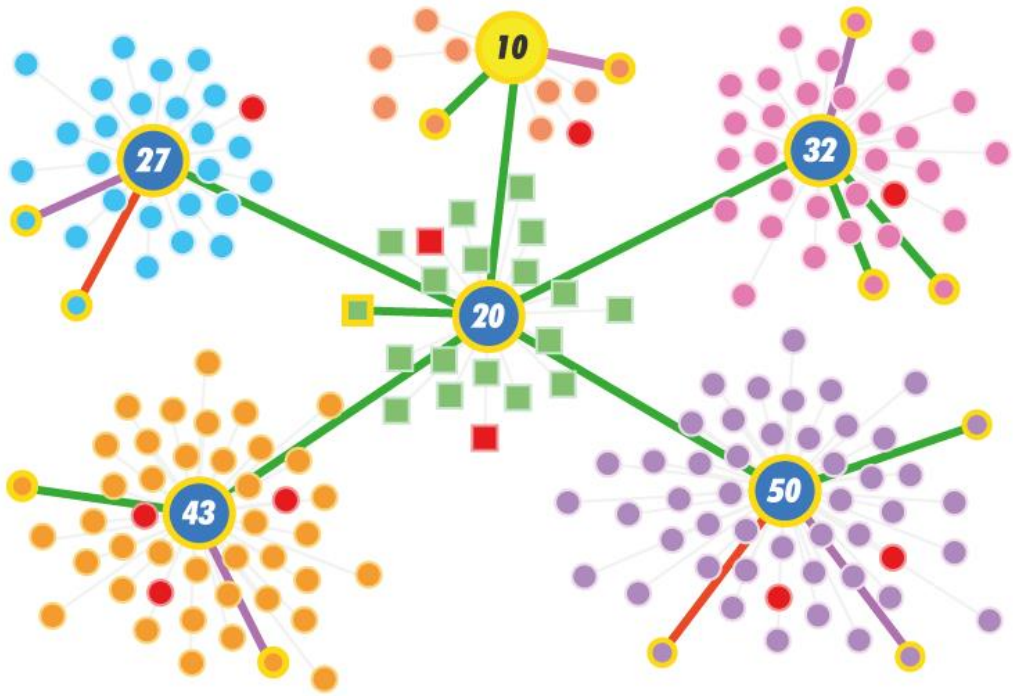

Figura 5. Mapa de activos y conexiones

El acceso a este portal se ofrece al personal del Organismo una vez se realiza la instalación de la sonda y el Organismo queda adscrito al SAT de ICS.

Adicionalmente, en el portal SAT se ofrece a los Organismos un cuestionario que permite a los operadores del sistema adaptar el tipo de alertas que se generan a sus características específicas y capacidad de gestión de incidentes de seguridad.

5.12 ¿Quién realiza la gestión de la sonda?

La gestión y administración de la sonda se realiza por el personal técnico del CCN-CERT, para mantener un sistema lo más homogéneo posible. Entre las tareas de gestión y administración se incluyen la actualización diaria de las reglas de detección, actualizaciones de sistema operativo, actualización de las aplicaciones, aplicación de parches de seguridad de sistema operativo y de aplicaciones, particularización de las reglas de detección, etc.

5.13 ¿Quién tendrá acceso a la información de mi Organismo?

Únicamente tendrán acceso a la información del Organismo adscrito los responsables de la seguridad TIC seleccionados por el propio Organismo para tal efecto y los administradores del sistema, es decir, el equipo de expertos del CCN-CERT que monitoriza el sistema central de sondas. Ninguna otra persona tendrá acceso a esta información. Es importante saber que ningún Organismo tendrá acceso a la información de otros organismos adscritos y **únicamente podrá ver el estado de seguridad de su propia red**, si bien sí que será usada la detección de eventos distribuida para la generación de la inteligencia del sistema de forma automatizada. En este sentido, como en todas las materias competencia del Centro Criptológico Nacional, la política a seguir será la de mantener en todo momento la confidencialidad de la información tratada.

5.14 ¿Quién se puede suscribir a este servicio?

Cualquier Organismo perteneciente al Sector Público o a empresas y organizaciones de interés estratégico para el país que dependan para su operación de sistemas ciberfísicos de todo tipo puede adherirse al Sistema de Alerta Temprana SAT-ICS, contactando con el CCN-CERT a través de la cuenta de correo **sat-ics@ccn-cert.cni.es.**

5.15 ¿Qué información voy a recibir si estoy suscrito al servicio SAT-ICS?

El Organismo que esté adscrito al Sistema de Alerta Temprana SAT-ICS, recibirá periódicamente informes de estado del servicio. Entre otra información, los informes incluyen la actividad anómala y los ataques detectados en cada Organismo, los incidentes gestionados en un período de tiempo y un listado de todos los incidentes pendientes de resolver.

Del mismo modo, anualmente recibirá un informe en el que se recogerá la actividad de la sonda durante ese periodo e indicadores que permitirán valorar tanto el servicio ofrecido por el SAT como la capacidad de respuesta del Organismo en la resolución de los incidentes de seguridad gestionados.

5.16 ¿Cómo voy a recibir la información de los incidentes?

Para la recepción de los incidentes el Organismo que esté adscrito al Sistema de Alerta Temprana SAT-ICS deberá disponer de una **cuenta de correo a la que enviar la notificación de los incidentes** de seguridad. Esta cuenta de correo deberá ser única, por lo que se recomienda al Organismo la creación de una lista de distribución que reciba todo el personal que vaya a encargarse de la investigación de los incidentes de seguridad.

La información referente a los incidentes de seguridad detectados por el personal técnico del CCN-CERT estará disponible en la **herramienta LUCIA**, al que tendrán acceso los responsables de seguridad de los Organismos adheridos a este servicio, donde podrán realizar el seguimiento de los incidentes notificados y donde podrán informar de las acciones llevadas a cabo para la resolución del mismo.

LUCIA es la herramienta de *ticketing* para la gestión de incidentes de seguridad desarrollada por el CCN-CERT (puede encontrar más información referente a LUCIA en https://www.ccn-cert.cni.es/herramientas-de-ciberseguridad/lucia.html).

Aunque la información relativa a los incidentes de seguridad notificados al Organismo se encontrará en la herramienta LUCIA, ante la posible necesidad de intercambio de información referente a los incidentes de seguridad a través del correo electrónico, será necesario que el organismo genere un par de claves PGP/GPG para intercambiar información de manera cifrada en el caso que fuese necesario. Una vez generadas las claves PGP/GPG asociadas a esta cuenta de correo, el Organismo deberá remitir al CCN-CERT la clave pública para poder cifrar la información que éste quisiera remitir de manera cifrada. Igualmente, el CCN-CERT proporcionará la clave pública de la cuenta de correo utilizada para la notificación de incidentes para que el Organismo pueda también enviarle información cifrada en caso necesario.

6. Sobre CCN-CERT, CERT Gubernamental Nacional

El CCN-CERT es la Capacidad de Respuesta a incidentes de Seguridad de la Información del Centro Criptológico Nacional, CCN, adscrito al Centro Nacional de Inteligencia, CNI. Este servicio se creó en el año 2006 como **CERT Gubernamental Nacional español** y sus funciones quedan recogidas en la Ley 11/2002 reguladora del CNI, el RD 421/2004 de regulación del CCN y en el RD 3/2010, de 8 de enero, regulador del Esquema Nacional de Seguridad (ENS), modificado por el RD 951/2015 de 23 de octubre.

Su misión, por tanto, es contribuir a la mejora de la ciberseguridad española, siendo el centro de alerta y respuesta nacional que coopere y ayude a responder de forma rápida y eficiente a los ciberataques y a afrontar de forma activa las ciberamenazas, incluyendo la coordinación a nivel público estatal de las distintas Capacidades de Respuesta a Incidentes o Centros de Operaciones de Ciberseguridad existentes.

Todo ello, con el fin último de conseguir un ciberespacio más seguro y confiable, preservando la **información clasificada** (tal y como recoge el art. 4. F de la Ley 11/2002) y la información sensible, defendiendo el Patrimonio Tecnológico español, formando al personal experto, aplicando políticas y procedimientos de seguridad y empleando y desarrollando las tecnologías más adecuadas a este fin.

De acuerdo a esta normativa y la Ley 40/2015 de Régimen Jurídico del **Sector Público** es competencia del CCN-CERT la gestión de ciberincidentes que afecten a cualquier organismo o empresa pública. En el caso de **operadores críticos del sector público** la gestión de ciberincidentes se realizará por el CCN-CERT en coordinación con el CNPIC.

7. Punto de contacto

- 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