Sistema de Alerta Temprana

Sistemas de Control Industrial

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 unos pocos años, los sistemas encargados del control de las plantas industriales estaban confinados en redes aisladas del resto de las infraestructuras y sin conexión con el exterior. Eran sistemas con un grado alto de ciberseguridad (a pesar de que este factor no se hubiese considerado como un factor de diseño) cuyas únicas medidas de protección se centraban en la seguridad física pero que, por el contrario, presentaban una serie de limitaciones en cuanto a su funcionalidad.

Las nuevas necesidades de negocio, sobre todo en cuanto a contar con información en tiempo real de lo que sucede en infraestructuras industriales, motivaron una evolución de estas redes industriales hacia arquitecturas más abiertas, de forma que aquellas fronteras bien delimitadas en su origen comenzaron a ser atravesadas por un número cada vez mayor de conexiones con el exterior: puestos de supervisión centralizados, redes corporativas e, incluso, internet.

Es un hecho que la Convergencia de las Tecnologías de la Información y las Tecnologías Operacionales (IT/OT) es una tendencia inevitable y a la vez fundamental para dar soporte a los procesos de negocio industriales actuales, pero esta convergencia debe abordarse de una manera adecuada y coordinada, y garantizando la seguridad de las instalaciones industriales.

Una de las herramientas al alcance de los responsables de seguridad de Organismos públicos que explotan o dependen de infraestructuras industriales es el análisis del tráfico en las redes de supervisión y control para detectar de forma precoz anomalías en el mismo que pudieran ser indicativas de un incidente de ciberseguridad.

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 muy importante 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 que están en operación en infraestructuras del Sector Público (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?

El Sistema de Alerta Temprana para sistemas de control industrial (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 de control y supervisión industrial 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 industriales gracias a capacidades de DPI (Deep Packet Inspection).

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, tanto de código abierto como comerciales, y que cuenta 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 el propio switch, 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.

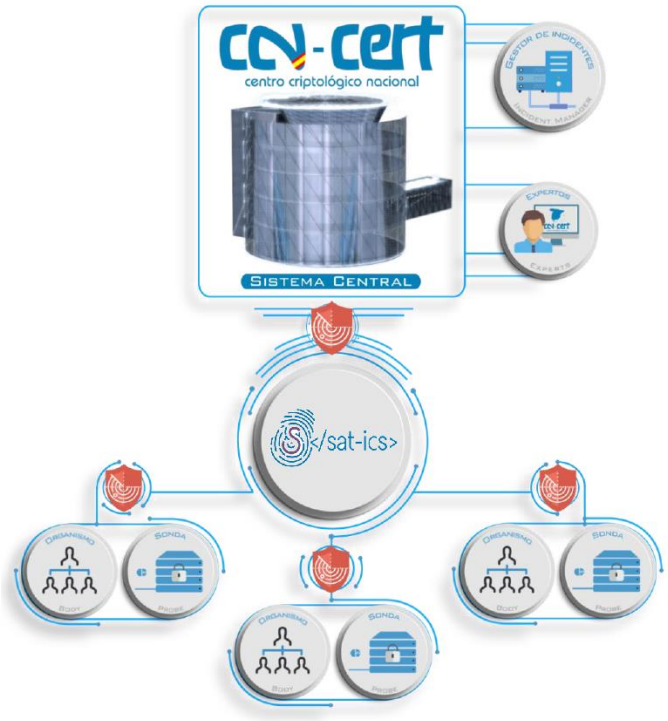

Figura 1. Arquitectura SAT-ICS

El despliegue de la sonda se realiza del siguiente modo:

- 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 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 para el establecimiento de túneles cifrados.
- 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 propósito industrial** monitorizadas en cada Organismo se acuerda de antemano y depende de la arquitectura de red, tipo de comunicaciones existentes en la red (TCP, serie, etc.), 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 de 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.

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 una infraestructura industrial, 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 tenga 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:

- **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 industriales** específicos empleados en la comunicación entre controladores, servidores SCADA, etc.
- **Correlación**. El sistema central no solo detecta incidentes importantes de forma individual, sino que se pueden detectar eventos mucho más complejos que pueden involucrar a distintos dominios.
- Acceso al mayor conjunto de **reglas de detección**, tanto propias como externas, integradas por el equipo de expertos del CCN-CERT que permite la detección de un mayor número de amenazas.
- **Información** de gran valor para los responsables de la seguridad de las infraestructuras industriales de las administraciones públicas, que pueden 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.

4. PREGUNTAS MÁS FRECUENTES –FAQ-

4.1 ¿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 (IDS), 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.

4.2 ¿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.

La sonda puede estar conectada a distintas redes para realizar una monitorización diferenciada, siempre que existan suficientes interfaces de red disponibles en el servidor (y en la electrónica de red) para llevar a cabo esta tarea. En cada caso se estudiará junto con el Organismo cual es la situación ideal donde realizar la instalación de la sonda.

4.3 ¿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.

4.4 ¿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 seguridad de la información lleva a cabo tareas de administración, maduración de las reglas de detección e inclusión de posibles nuevas fuentes.

4.5 ¿Qué características debe tener el servidor?

Dependiendo de las características de la instalación industrial, se recomiendan dos tipos diferentes de sonda, cuyos requerimientos hardware para el adecuado funcionamiento son los siguientes:

1) **Sonda Estándar:**

	Requisitos mínimos
Procesador	Multinúcleo 16 cores
Memoria RAM	16 GB
Almacenamiento	2 Discos Duros 160GB, en RAID 1 (Espejo)
Red	Interfaces de análisis (tantas como redes a analizar): tarjeta/s de red Gigabit Ethernet tecnología Intel (driver e1000e o igb)
	Interfaz de gestión: tarjeta de red Gigabit Ethernet

2) **Minisonda:**

La minisonda SAT-ICS está pensada para pequeñas 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 los 5Mbps de througput.

	Requisitos mínimos
Procesador	2 cores en procesador i5/i7 ó 4 cores en procesadores inferiores
Memoria RAM	8 GB
Almacenamiento	100GB
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

4.6 ¿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.

4.7 ¿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 industrial del Organismo** hacia el sistema central, manteniéndose así la privacidad en las comunicaciones.

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

La finalidad de la sonda es detectar ataques que se produzcan en las redes industriales 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 los ICS 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 de control y en la definición de reglas para su detección, partiendo del conocimiento de la forma en que se explotan este tipo de sistemas industriales.

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 de control 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 principales protocolos empleados en este tipo de entornos (S7COM de Siemens, FINS de Omron, Ethernet IP de Rockwell, Modbus, IEC-60.870-104, DNP3, etc.) y 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.

4.9 ¿Qué es el portal SAT?

El portal del SAT es el lugar en el que el personal responsable de la ciberseguridad de los ICS 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.

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 Internet.

4.10 ¿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.

4.11 ¿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.

4.12 ¿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 tecnologías ICS puede adherirse al Sistema de Alerta Temprana SAT-ICS, contactando con el CCN-CERT.

4.13 ¿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.

4.14 ¿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 encontrarán 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.

5. 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.

6. Punto de contacto

- Tfno. 91 283 2678 / 91 283 2313
- Web: https://www.ccn-cert.cni.es
- E-Mail: sat-ics@ccn-cert.cni.es