#solucionesCCNCERT

SISTEMA DE ALERTA TEMPRANA

Detección en tiempo real de las amenazas y posibles incidentes mediante el análisis del tráfico de la organización.

Finalidad

Detectar en tiempo real las amenazas existentes en el tráfico de red y/o en las redes de control y supervisión industrial para responder de forma ágil al incidente detectado, con la intención de reducir su impacto y alcance.

Conexión con el CCN-CERT

El sistema Central del CCN-CERT recibe los eventos de seguridad de las diferentes sondas, los relaciona entre sí con patrones identificables y emite los avisos y alertas oportunos a los organismos adscritos.

Portal de informes

Los usuarios pueden acceder en tiempo real a información relevante de los eventos generados por su sonda y a estadísticas e informes sobre el servicio ofrecido por el **SAT**.

Despliegue mediante sondas

La adhesión de un organismo al SAT se puede realizar de tres formas diferentes:

Sonda individual: Una sonda desplegada en los sistemas del organismo analizará el tráfico de red en busca de amenazas.

SAT distribuido multisede: Sondas desplegadas en cada una de las sedes del organismo, canalizando la conexión con el CCN-CERT a través de la sede principal.

SAT distribuido multifuente: Además del despliegue de la sonda, se recogen eventos de seguridad provenientes de otros dispositivos de seguridad de la organización, para analizarlos de manera conjunta.

Adhesión

Cualquier organismo público o empresas y organizaciones de sectores estratégicos pueden adherirse a este Sistema.

ccn-cert centro criptológico nacional

@ sat-inet@ccn-cert.cni.es

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