



Más allá del SIEM: Protección unificada de entornos IT-OT

Diciembre 2016

Acerca de nosotros



Óscar Navarro Carrasco

Ingeniero Industrial

Responsable de Ciberseguridad Industrial

Área de GRC

S2 Grupo



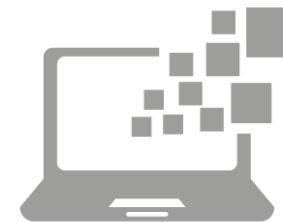
Lorenzo Mateu Palacios

Ingeniero en Informática

Subdirector de proyectos

Área de Producto

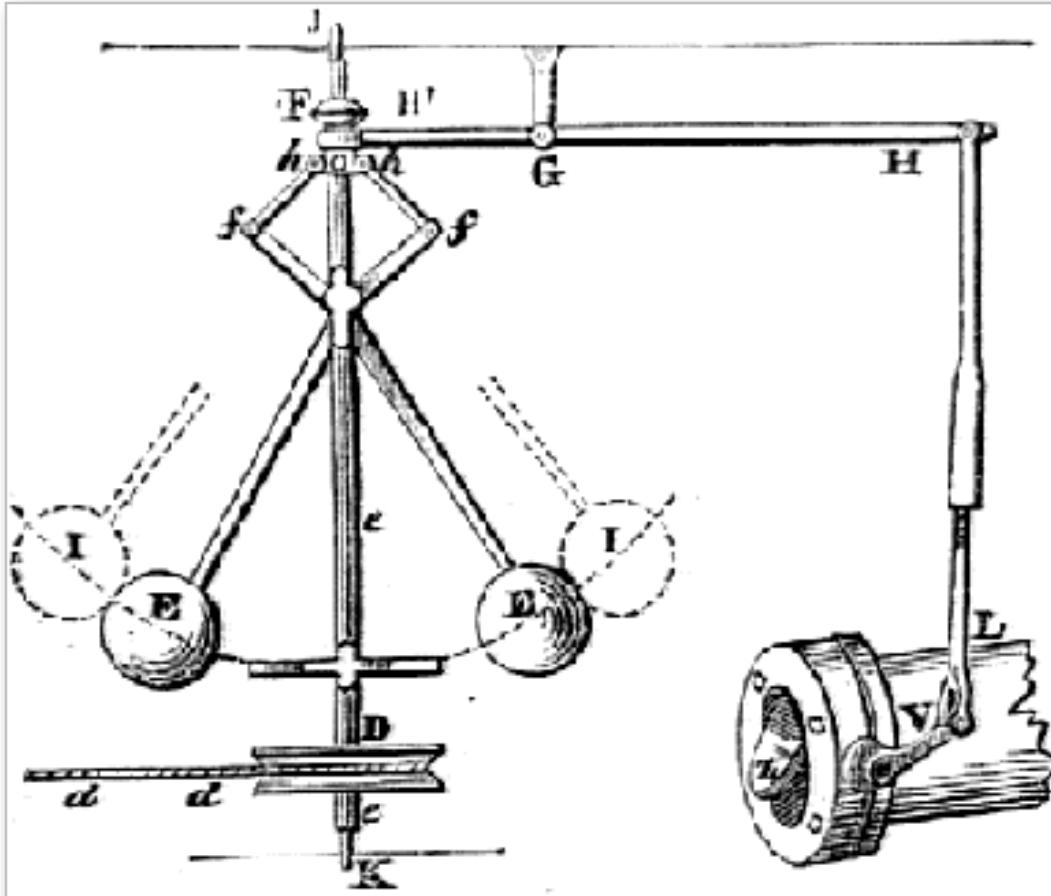
S2 Grupo





¡Ah! ¡Los sistemas aislados!



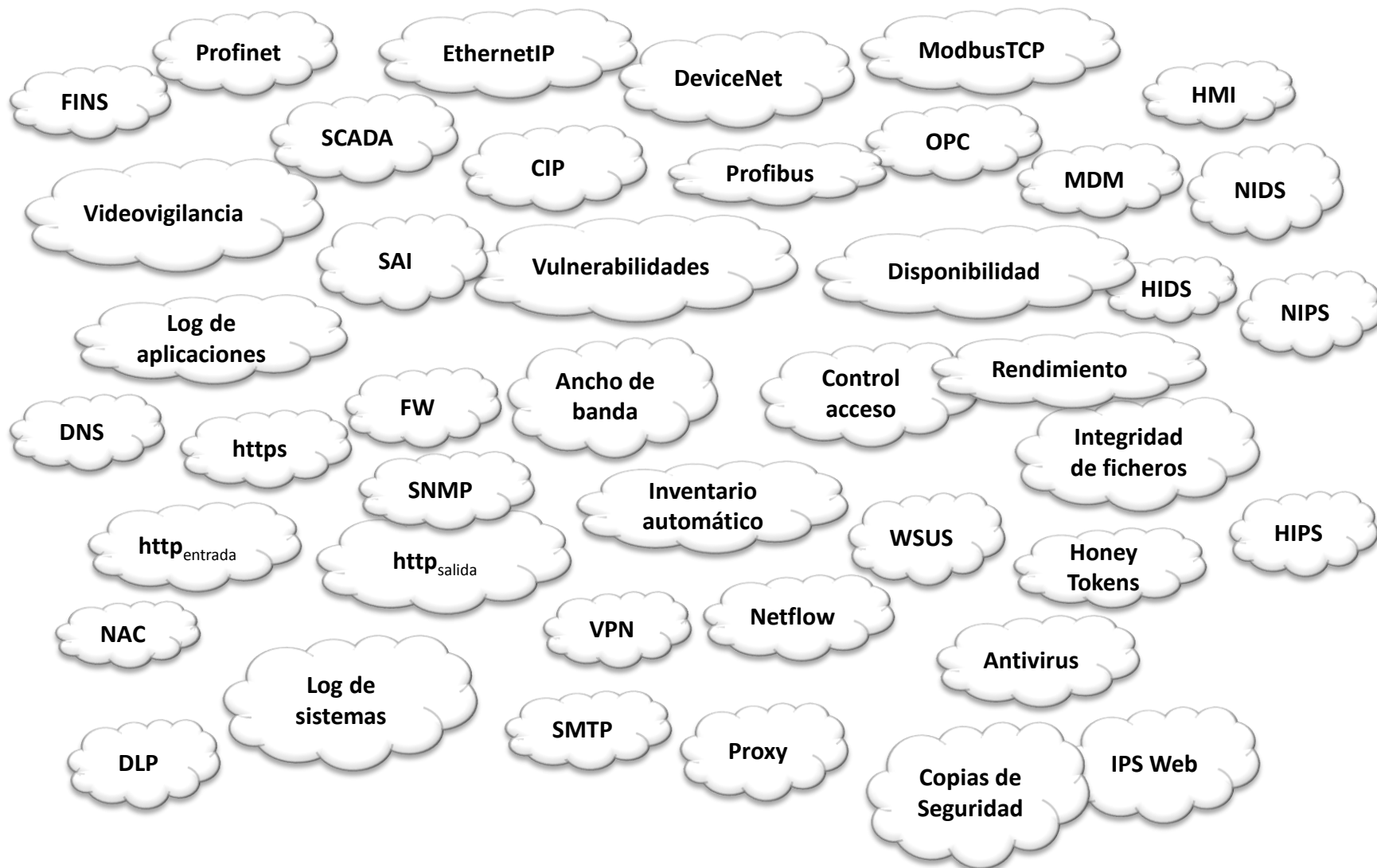




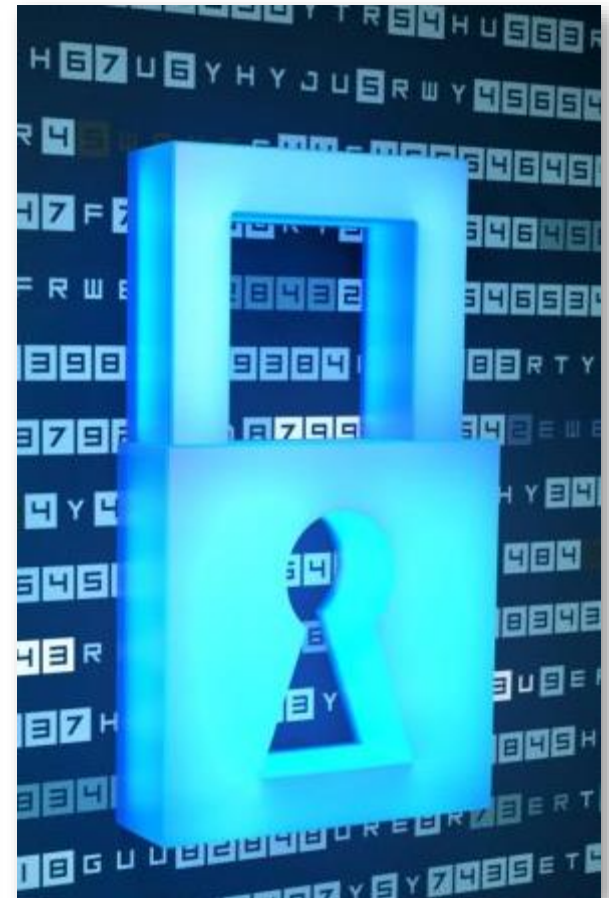
Los CPD son infraestructuras industriales dotadas de sistemas de control industrial y, como tales, son susceptibles de sufrir incidentes de ciberseguridad







- No solo detección basada en firmas, necesidad de herramientas de ayuda al analista de seguridad para trabajar con “lo desconocido”.
- Análisis del entorno de aplicación.
- Conocimiento de las **políticas de Seguridad** aplicables en la Organización.
- Aplicación de inteligencia de detección de forma global. Correlación entre la información de este nuevo entorno unificado.
- Disponer de una interfaz unificada de monitorización, correlación y gestión de alertas.



- Trabajar desde el conocimiento de las diferencias IT-OT.
- Evitar trasladar tal cual las soluciones del ámbito IT.
- No existen soluciones completamente generalizables. Es necesario estudiar el entorno concreto de aplicación.

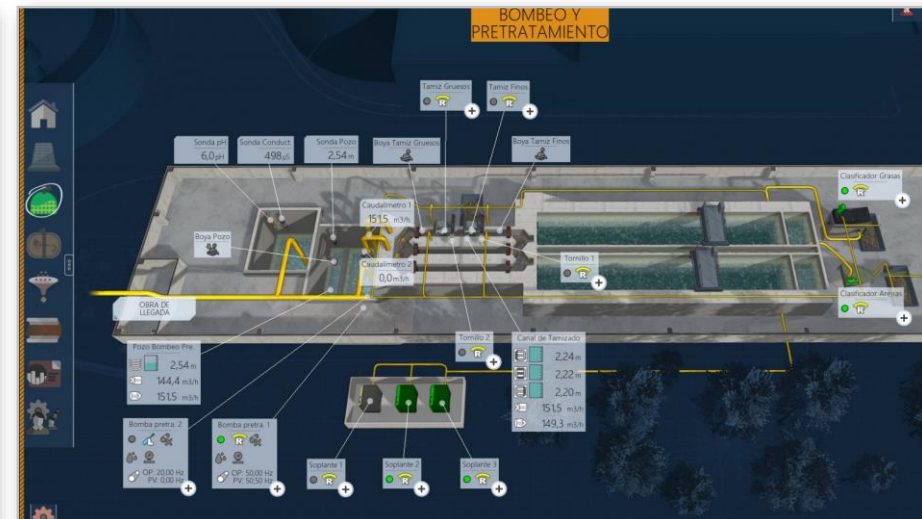


- **Mínima intrusión** en el sistema monitorizado. La concepción es la de un sistema de alerta, sin bloquear en ningún caso ni restringir la operación del mismo.
- Orientado al nivel de supervisión y las comunicaciones hacia los niveles de control y corporativos.
- Un planteamiento adecuado debe partir del **conocimiento de los procesos industriales y su contexto**.
- Detección de acciones anómalas contra los procesos industriales **basadas en el análisis del contexto y en detección tradicional basada en firmas**.
- Capacidades de detección basadas en DPI (**Deep Packet Inspection**).

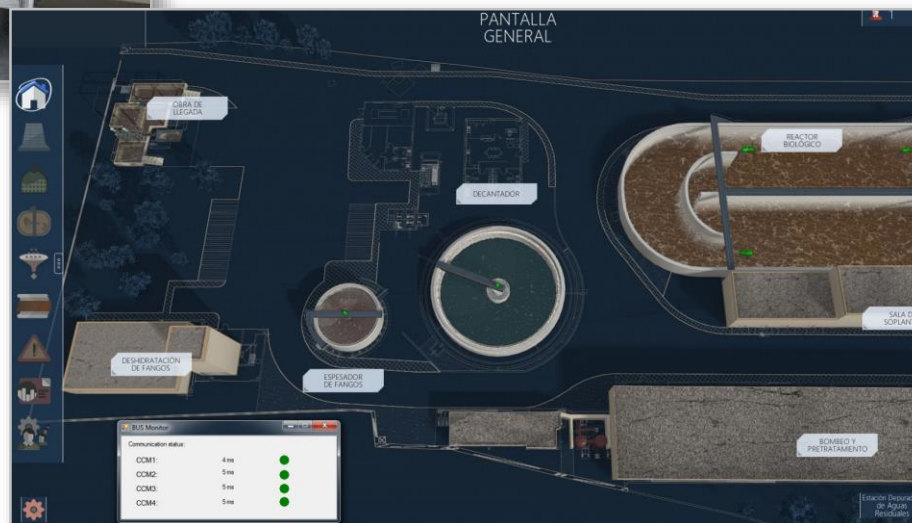


Proyecto iHoney. Desarrollo de herramientas específicas para la ciberseguridad de sistemas de control industrial

- Proyecto de investigación de 2 años de duración.
- Financiado por el MINETUR.
- Objetivo: desarrollo de herramientas específicas de ciberseguridad para Sistemas de Control Industrial.
- Honeypot basado en un sistema de control industrial que reproduce una infraestructura pública.



Proyecto iHoney. Desarrollo de herramientas específicas para la ciberseguridad de sistemas de control industrial

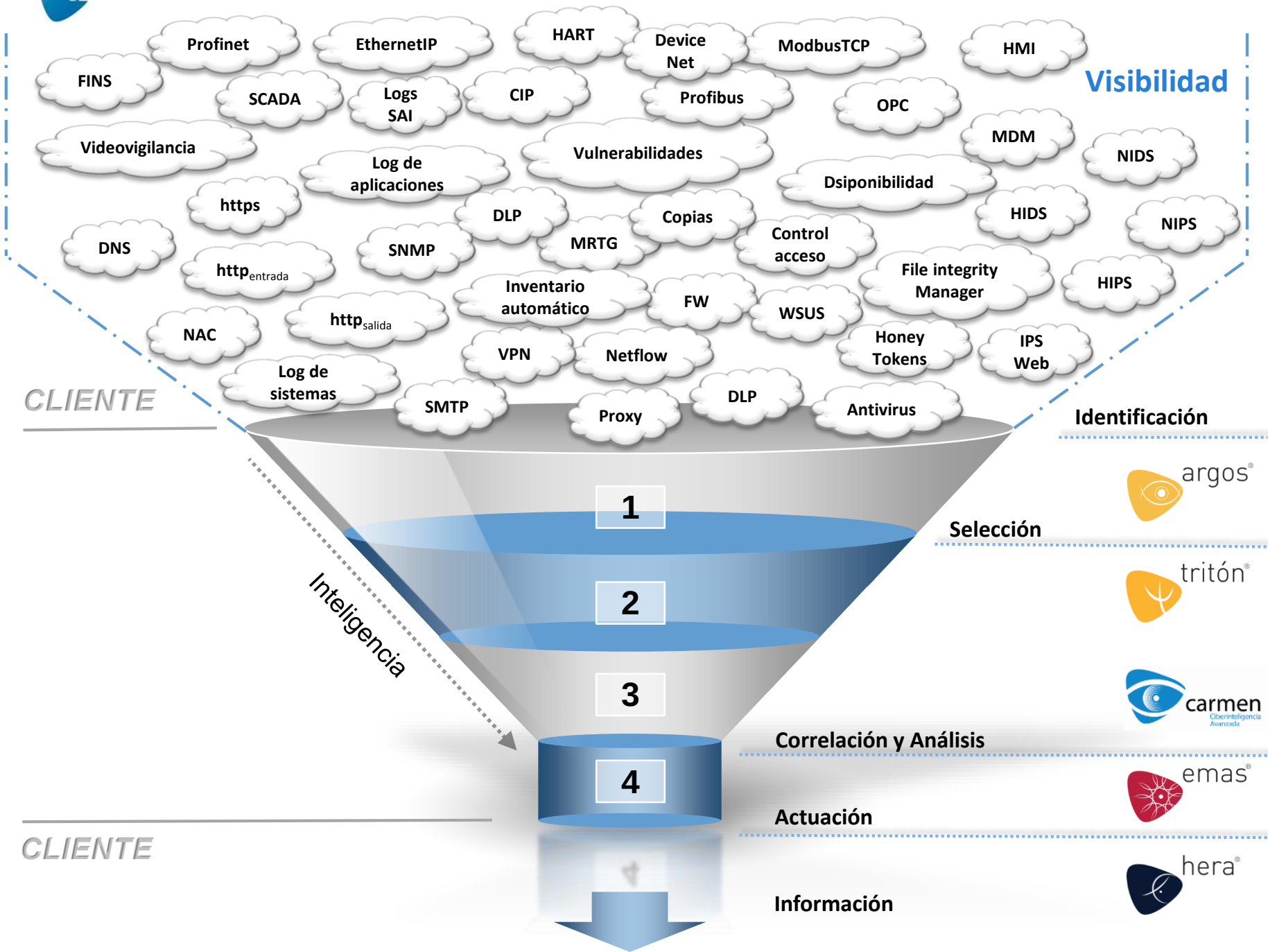


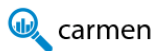
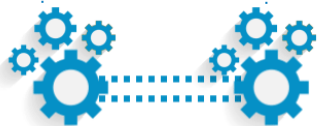


Solución de S2 Grupo

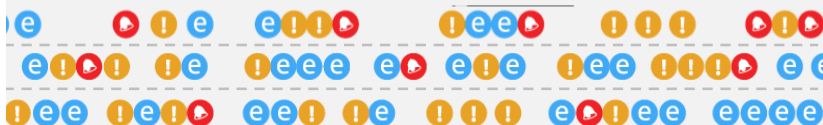
*La solución de S2 Grupo para la
operación de Centros de
Servicios de Ciberseguridad*







carmen



hera

Cuadro de mando activo



emas

Consola única de eventos



tritón

**Motor de correlación
Dominio protegible**

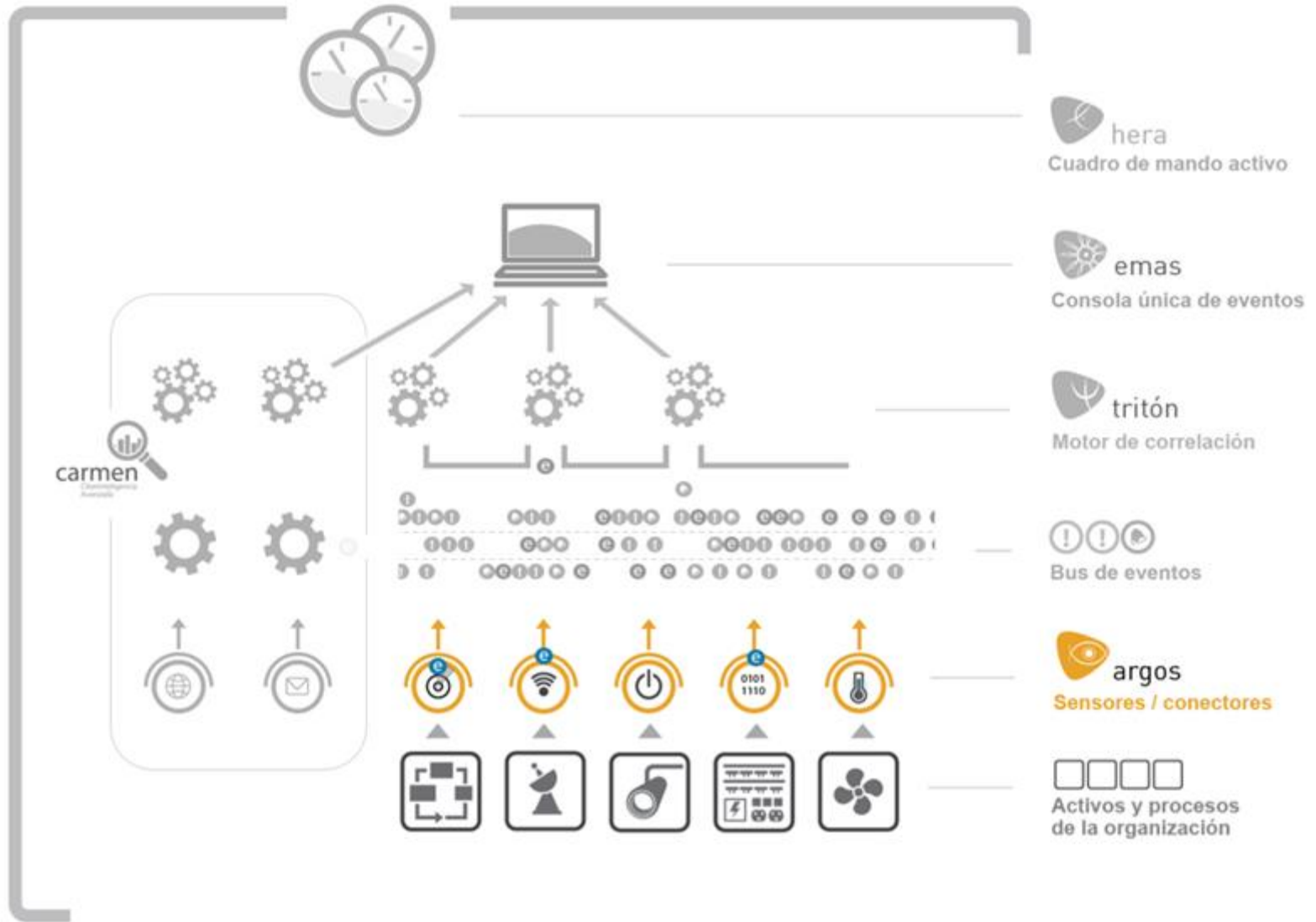


Bus de eventos



argos

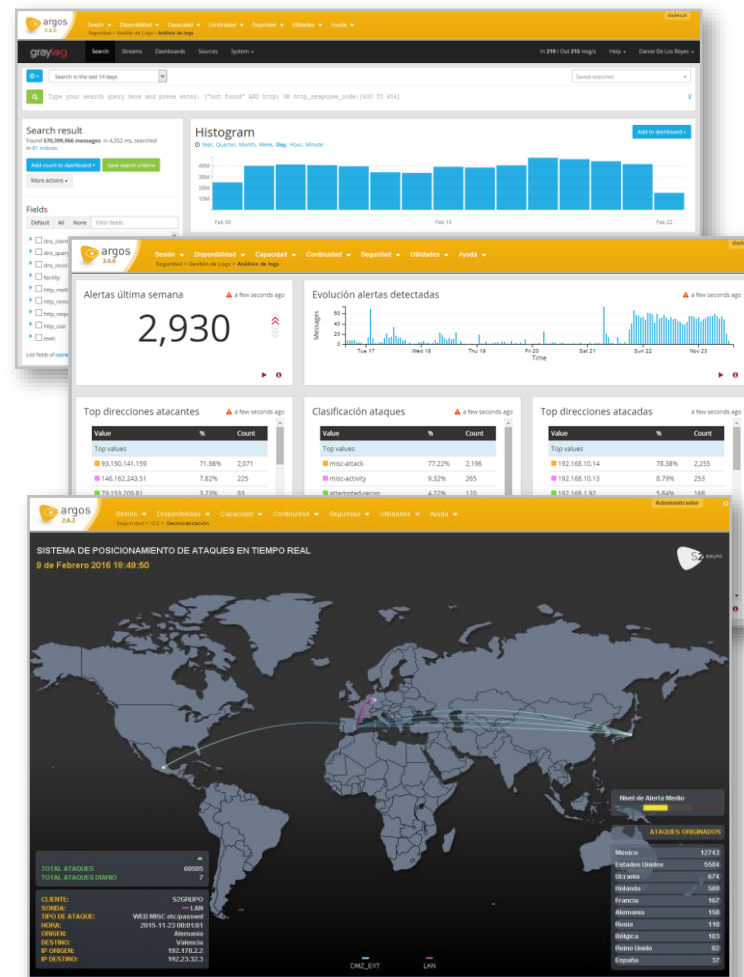
Sensores / conectores



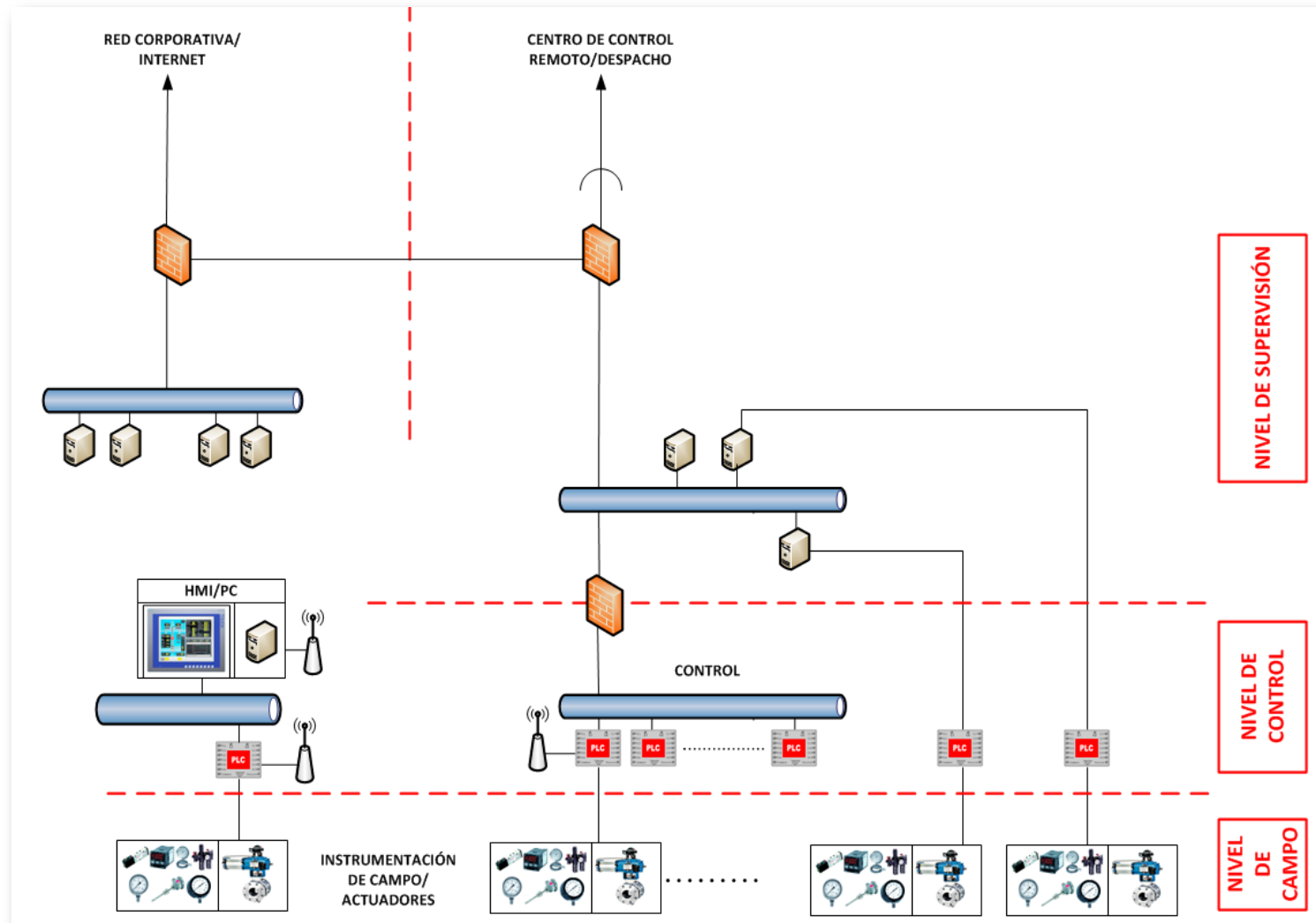
La capa de monitorización se compone de una selección de herramientas de monitorización Open Source así como de módulos y agentes de desarrollo propio para la integración con herramientas de terceros. Integrados con la plataforma de correlación y el sistema de gestión de eventos y alarmas

Resumen capacidades generales monitorización:

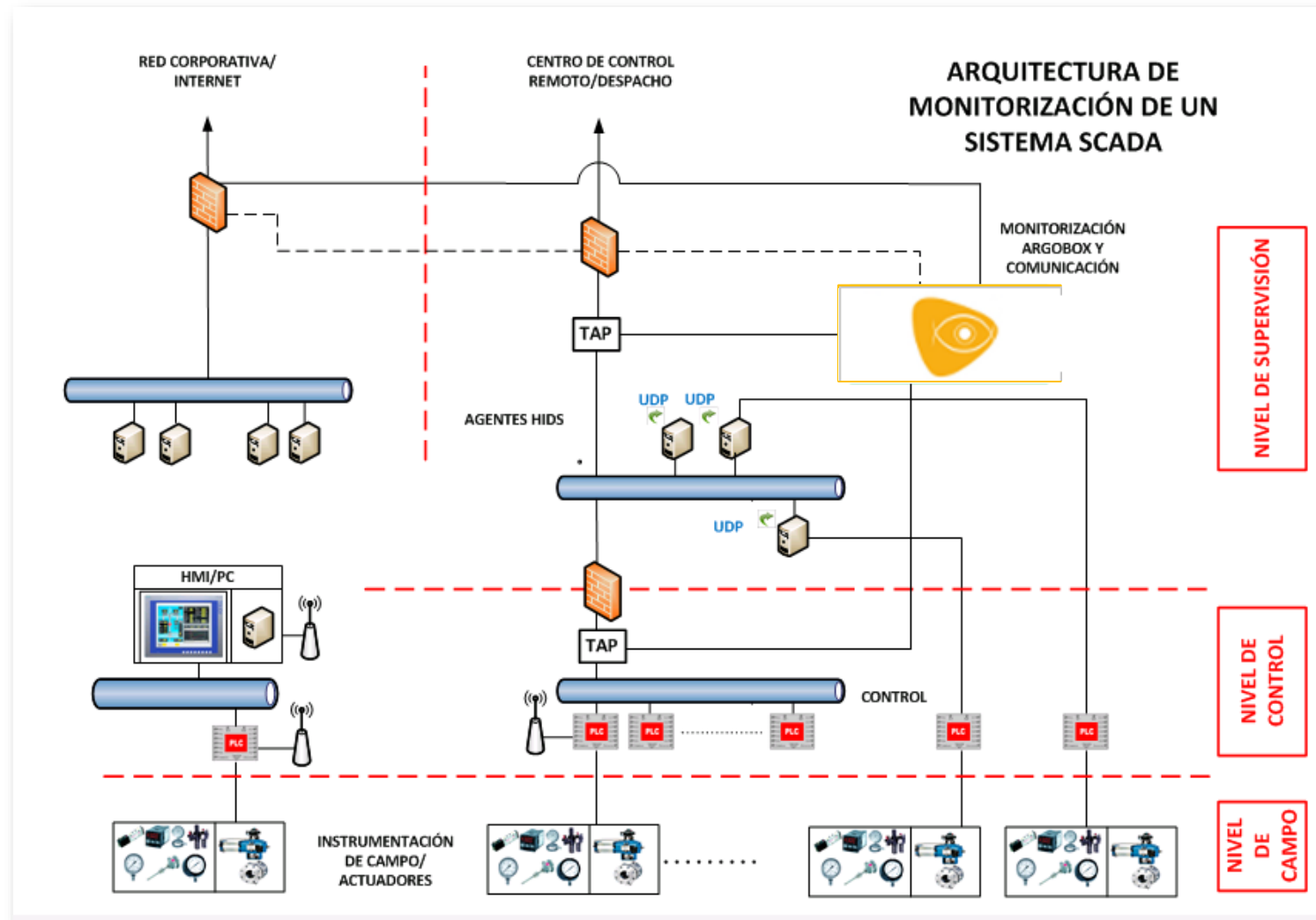
- Centralización y análisis de logs
- Análisis de vulnerabilidades
- Detección de intrusos (NIDS)
- Monitorización de integridad (HIDS)
- Control de acceso lógico
- Descubrimiento de nuevas direcciones IP
- Descubrimiento de equipos en la red
- Inventario automático de activos
- Monitorización de disponibilidad
- Analizadores de protocolos industriales



La arquitectura mostrada es una abstracción lo más general posible de este tipo de sistemas.

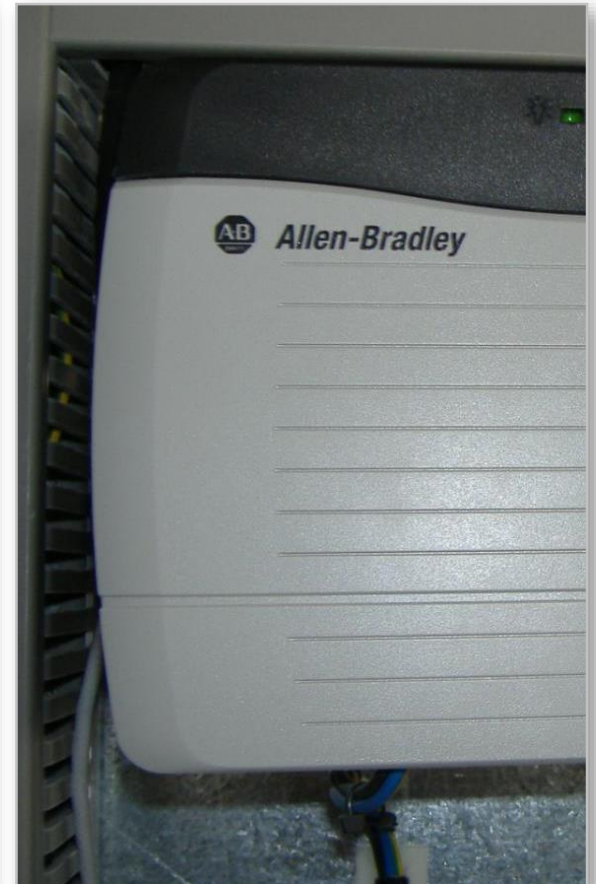


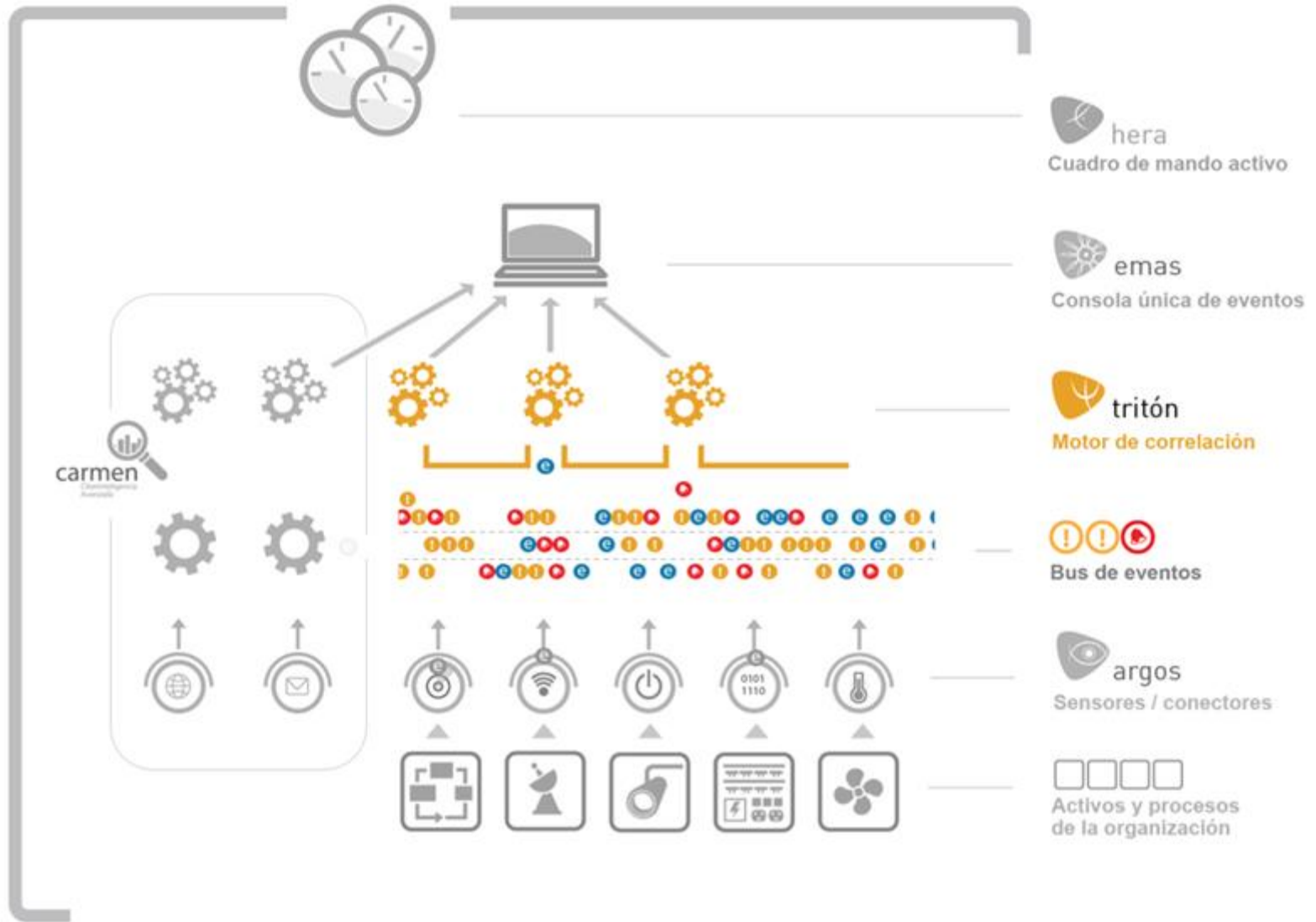
La arquitectura general propuesta tiene en cuenta factores como la garantía total de no intervención externa sobre los sistemas monitorizados. Requerirá de un ajuste final en cada infraestructura.



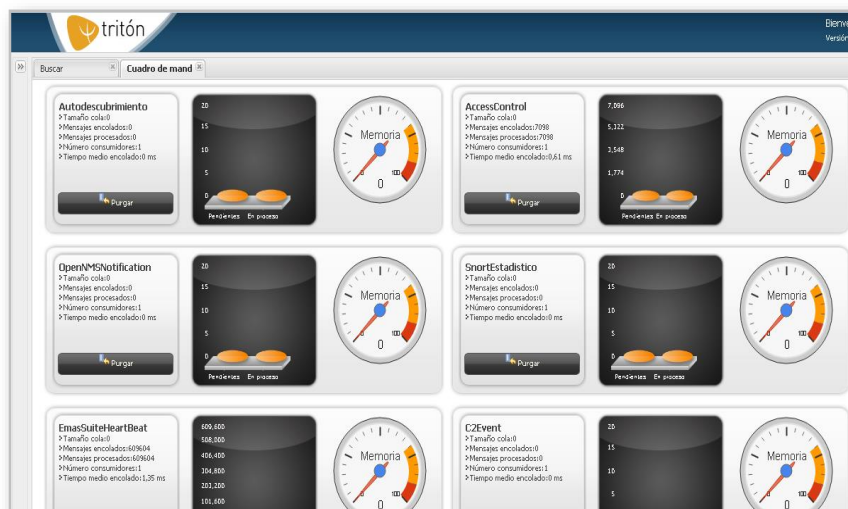
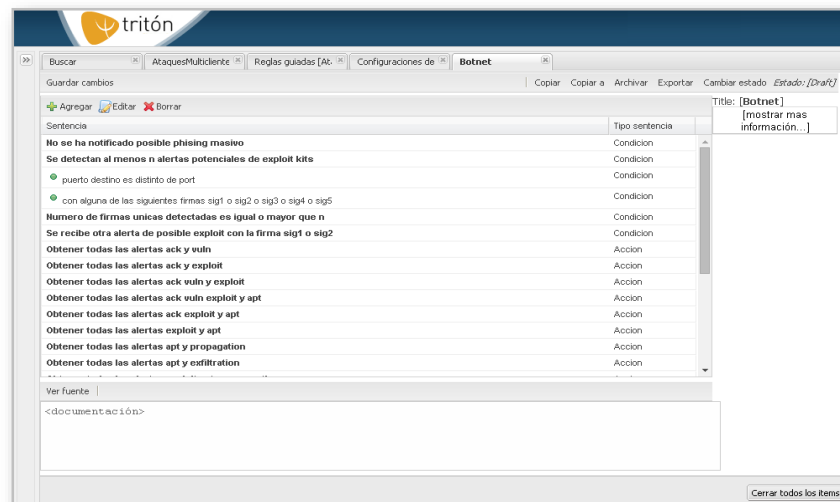
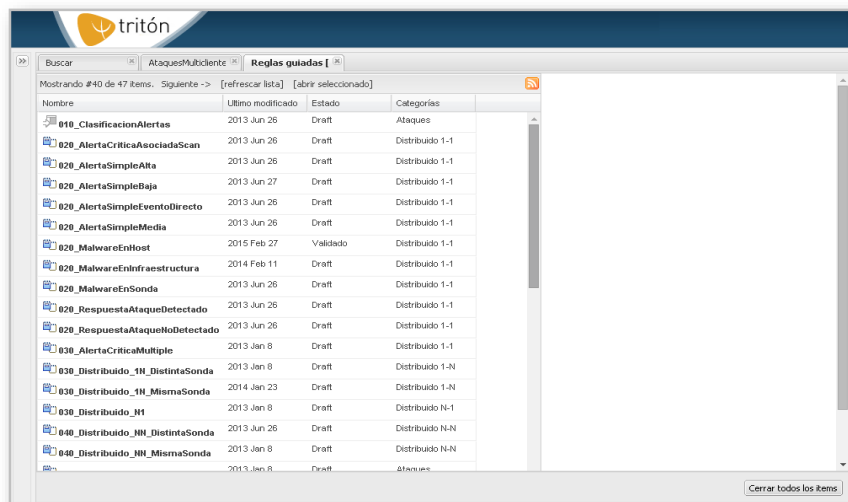
iSOC Dissector: Analizador de protocolos industriales integrado en argos

- Permite analizar el contenido de los paquetes enviados a través de la red supervisada (DPI) de cada uno de los protocolos implementados
- El análisis de los paquetes permite identificar situaciones de riesgo, **como el envío de comandos potencialmente peligrosos.**
- Los dissectores se implementan conforme a las necesidades de cada cliente.





Capa de inteligencia de la solución. El comportamiento del correlador se define mediante el uso de reglas. El sistema soporta la definición de Lenguajes Específicos de Dominio (DSL) que permiten al usuario describir el escenario a correlar en un lenguaje próximo al del dominio del problema.



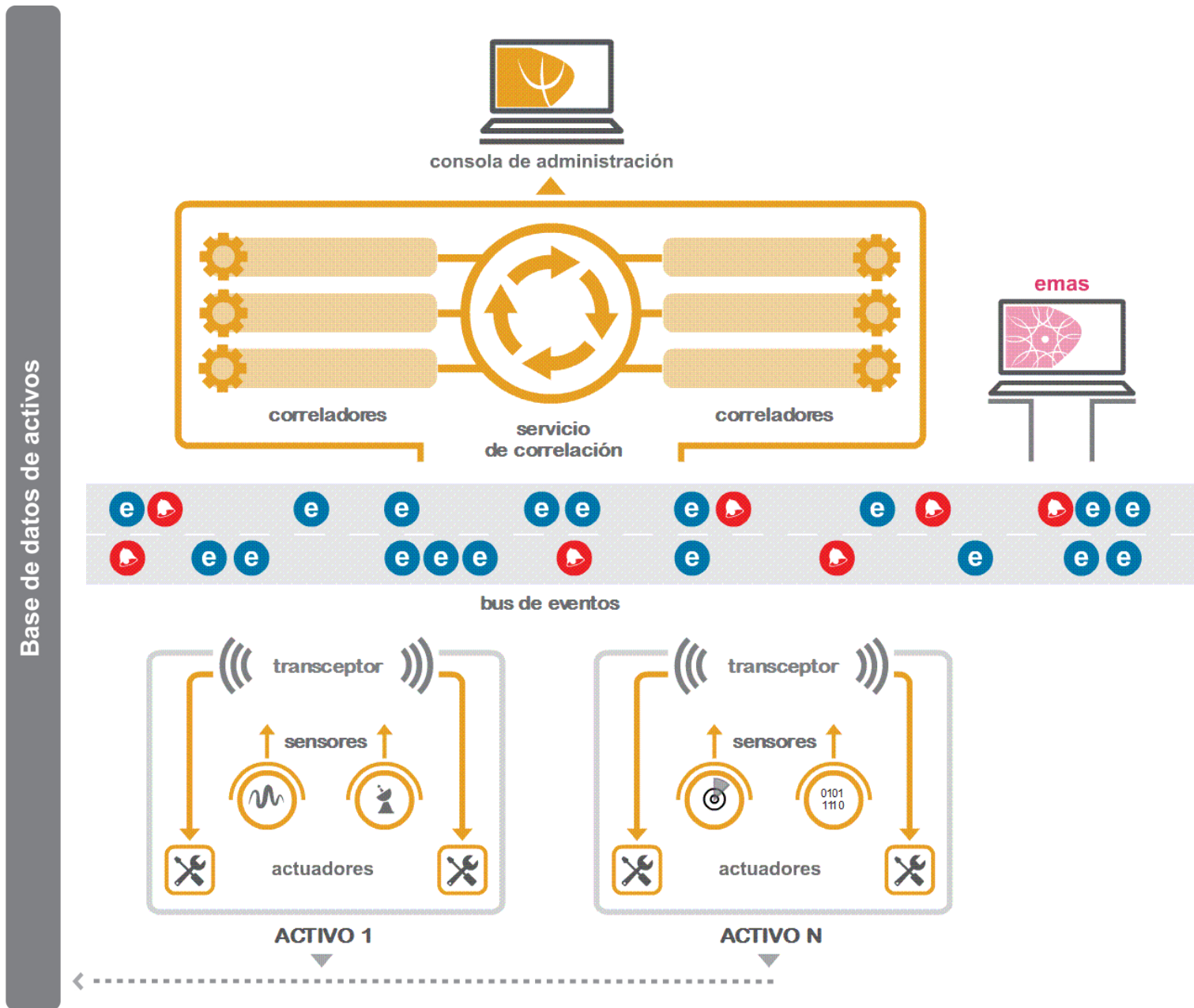
Resumen capacidades generales:

- Inteligencia
- Correlación simple / compleja
- Lenguaje específico de dominio
- Paquetes de reglas predefinidos
- Definición de reglas
- Asistente guiado
- Cuadro de mando de correlación



tritón

Arquitectura del
sistema
de correlación
de eventos

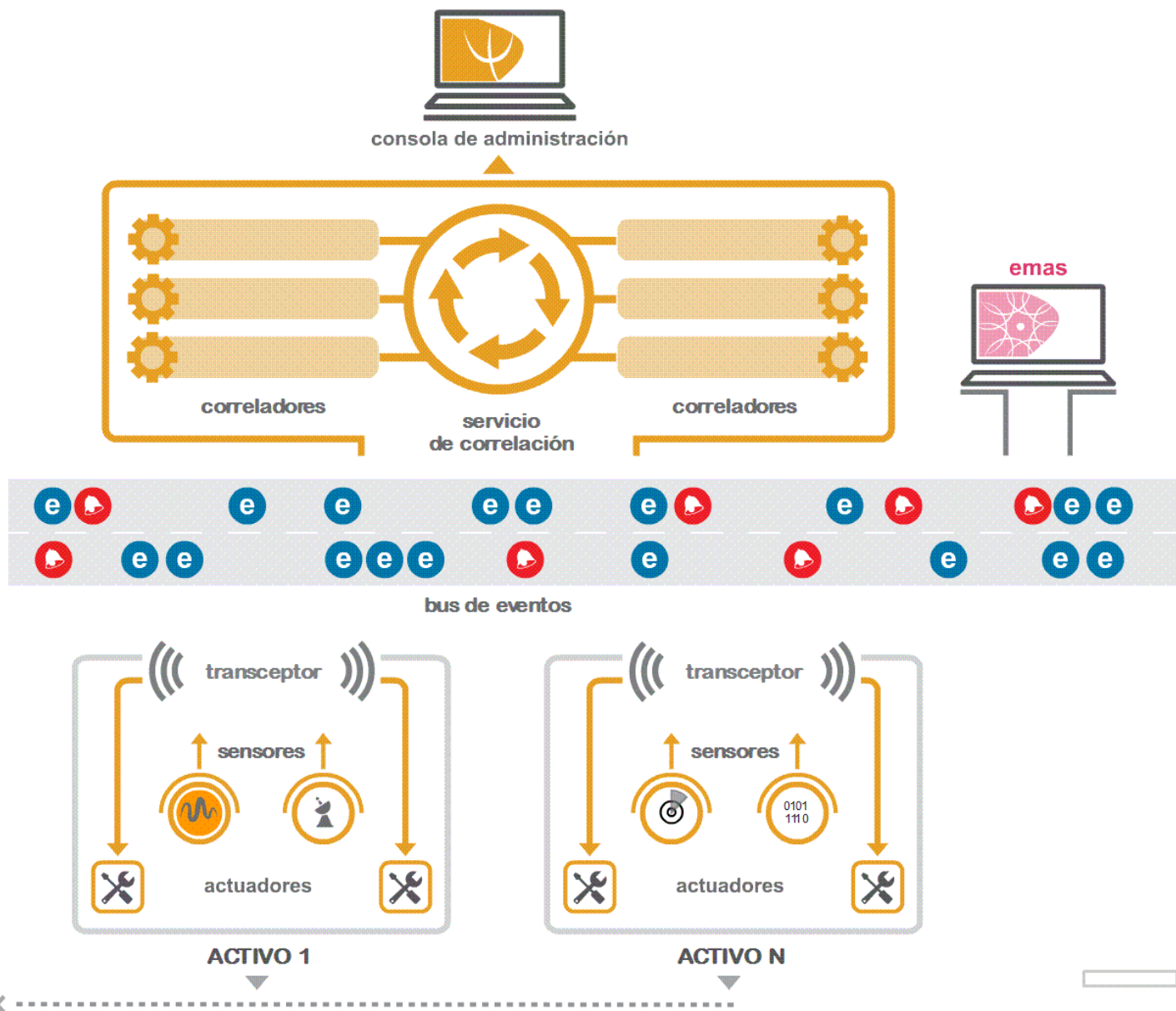




tritón

Arquitectura del
sistema
de correlación
de eventos

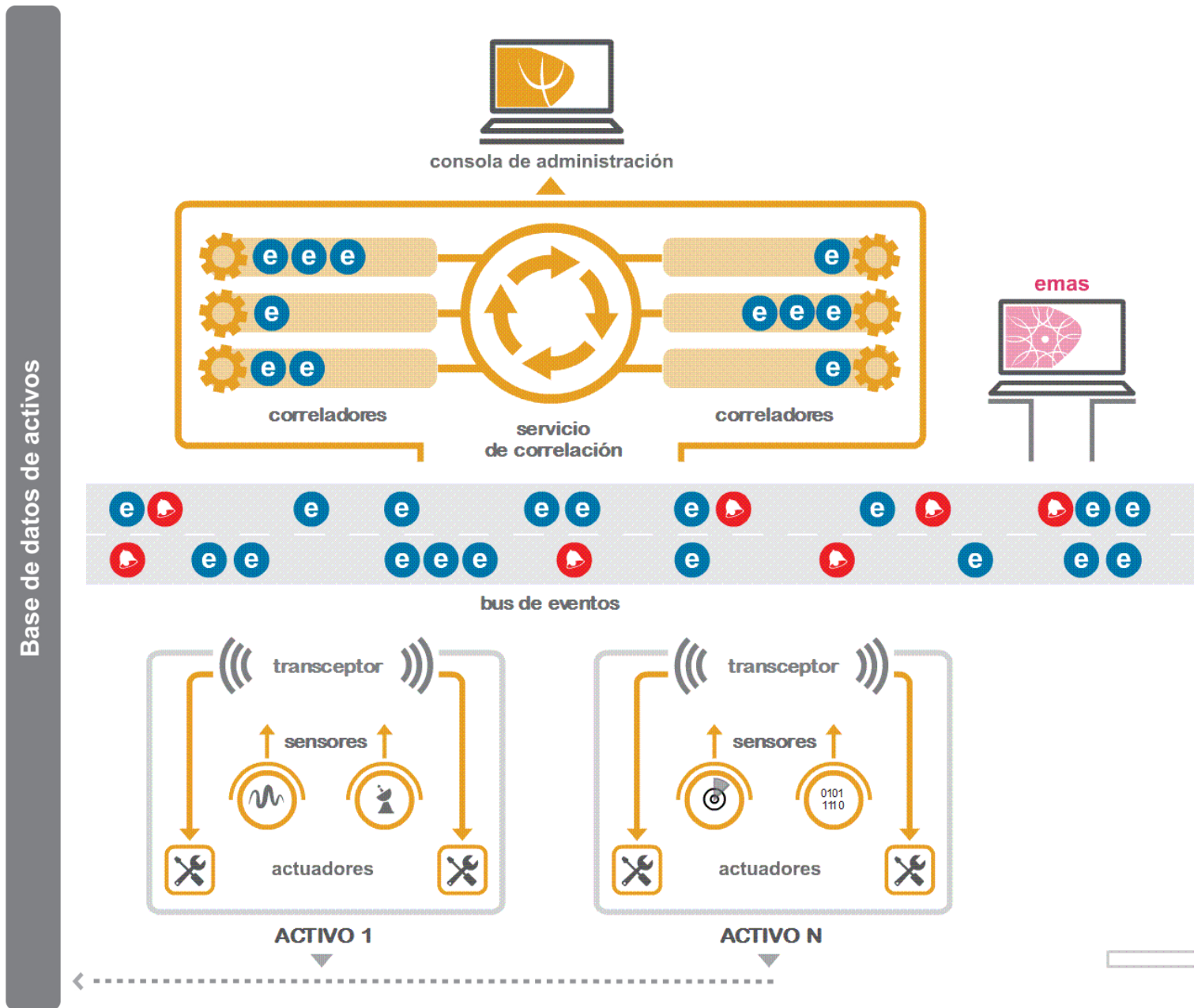
Base de datos de activos





tritón

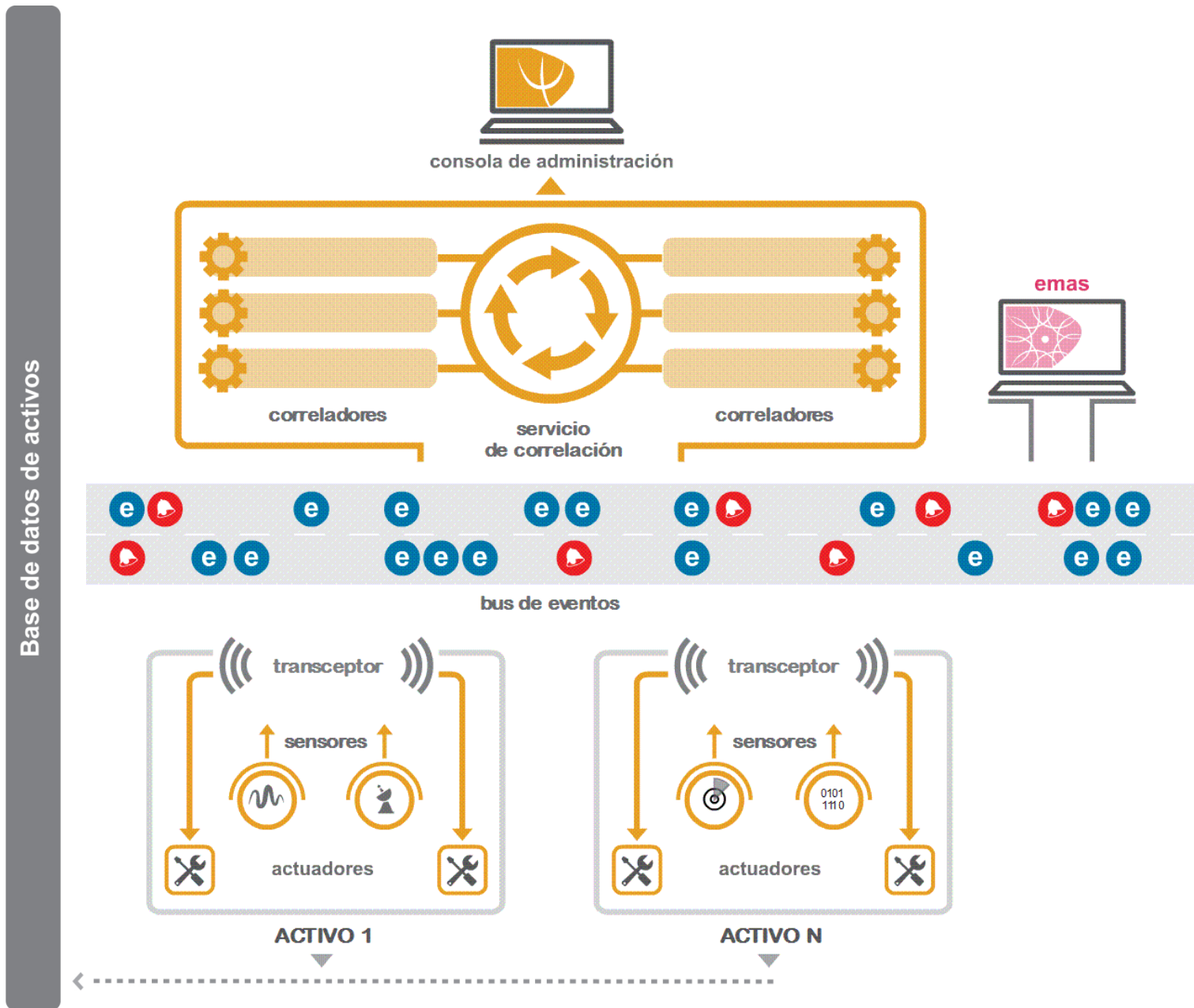
Arquitectura del
sistema
de correlación
de eventos





tritón

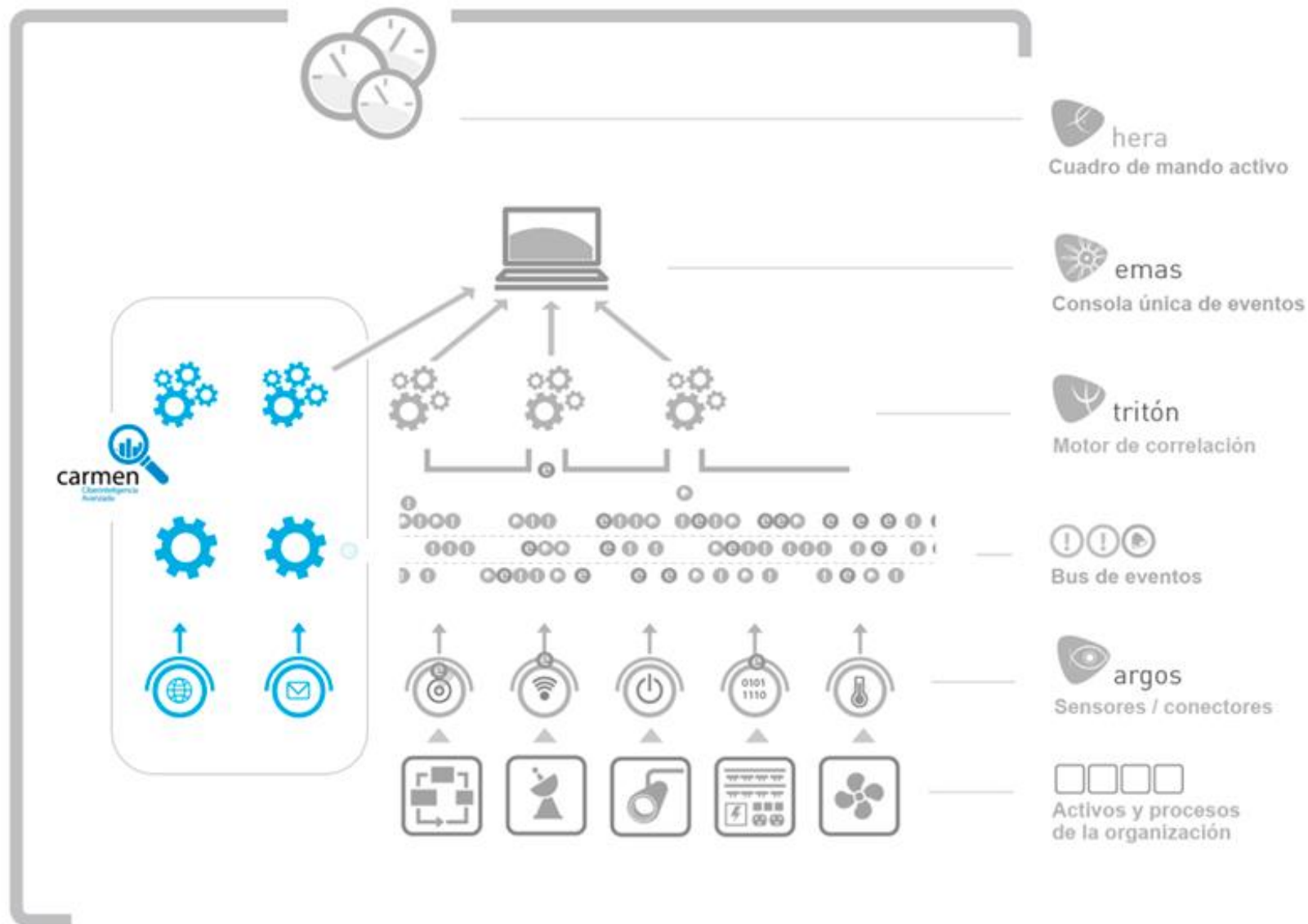
Arquitectura del
sistema
de correlación
de eventos



Existen diversos factores que intervienen en la caracterización del tráfico anómalo en sistemas industriales:

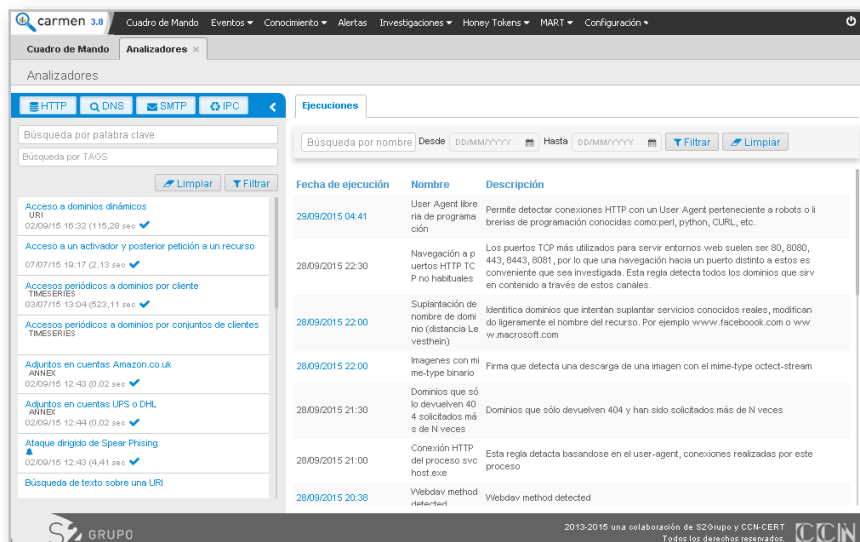
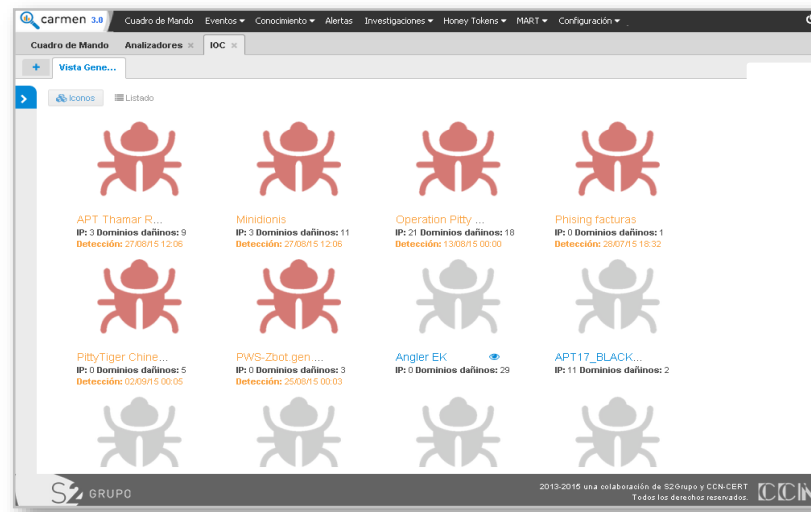
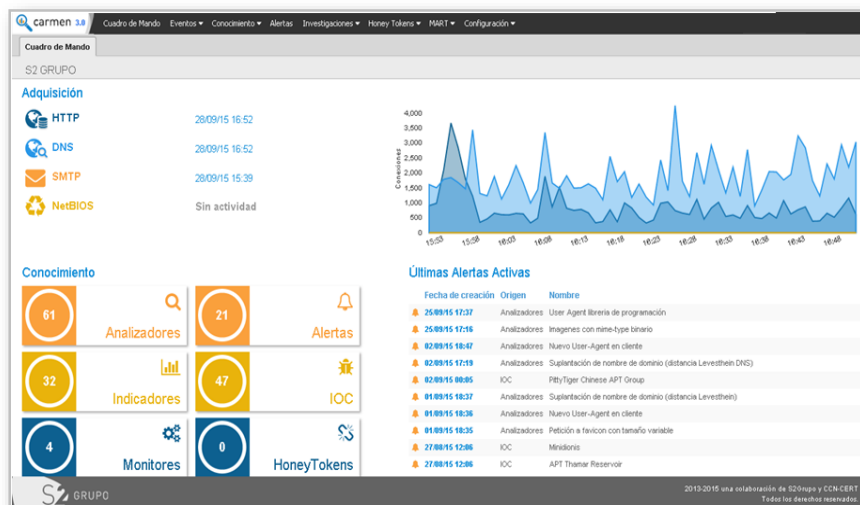
- Estructura de comunicaciones habituales bien definida funcionalmente (puertos/IP origen/IP destino).
- Poca diversidad de tráfico entre servidores y controladores y dentro de la red de control.
- Las redes de control no están sometidas a cambios frecuentes (topología y dispositivos).
- Las acciones ilegítimas contra los controladores son difícilmente distinguibles de las legítimas: necesidad de contexto.
- Diversidad de protocolos específicos.
- El nivel de supervisión suele ser análogo a un sistema TI convencional.





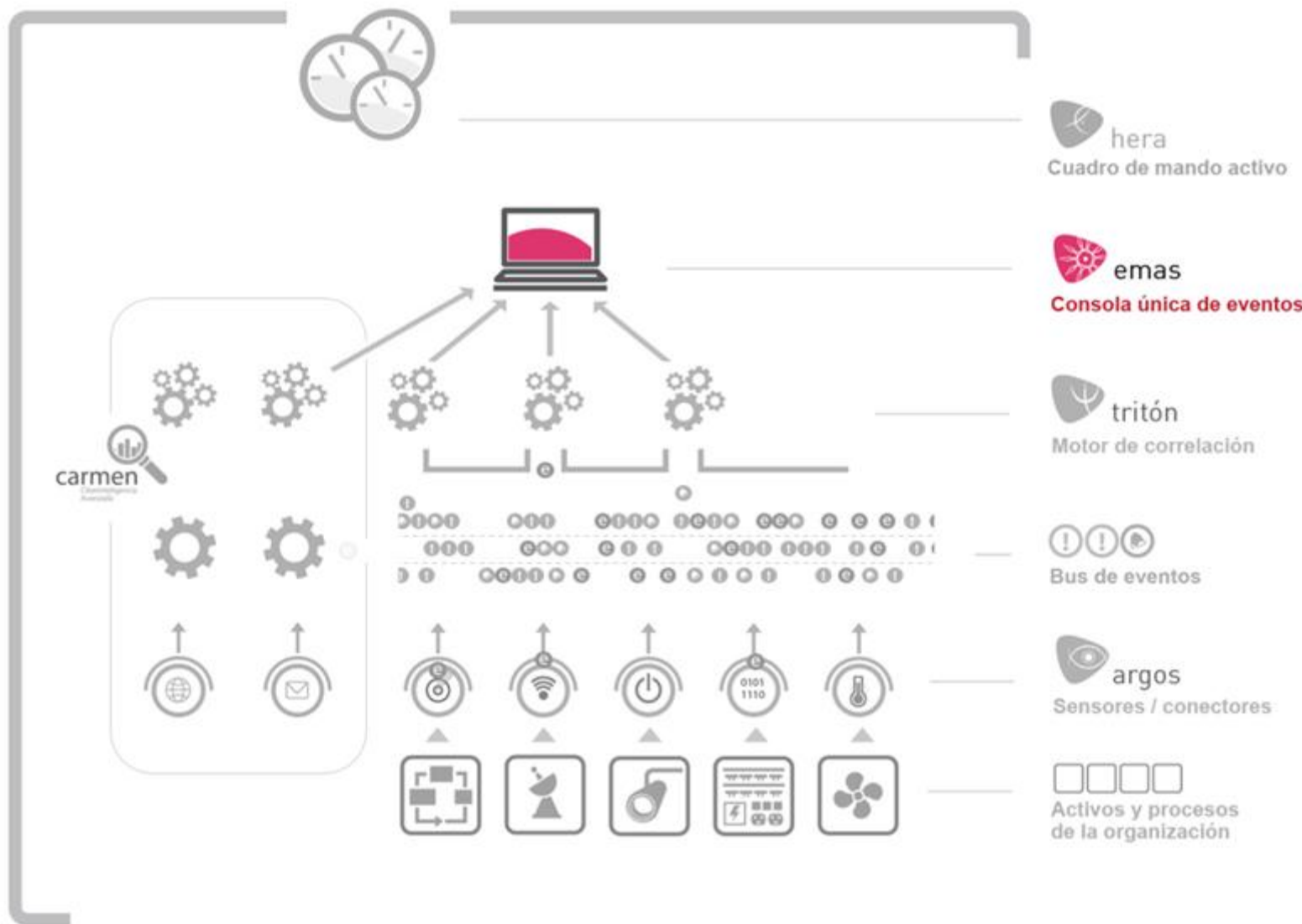
Capacidad española para la detección de amenazas persistentes avanzadas (APT)

Tratamiento de la información adquirida en una red por diferentes protocolos como HTTP, DNS, SMTP, etc

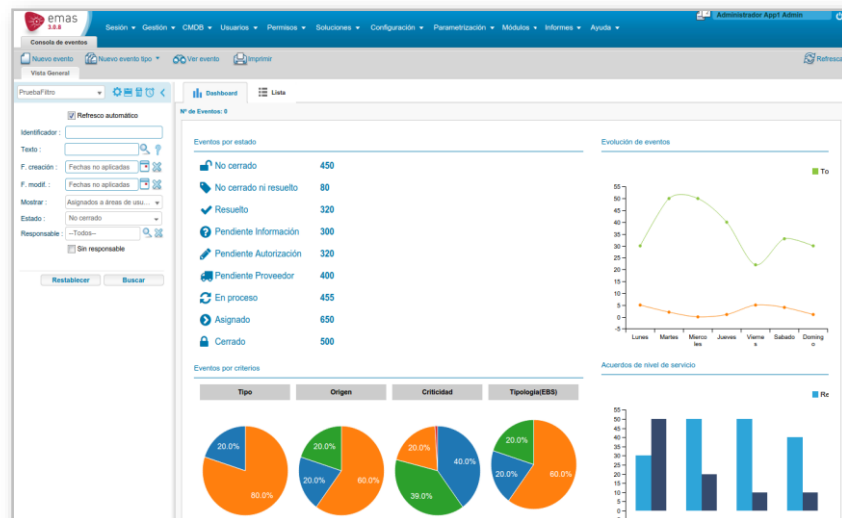
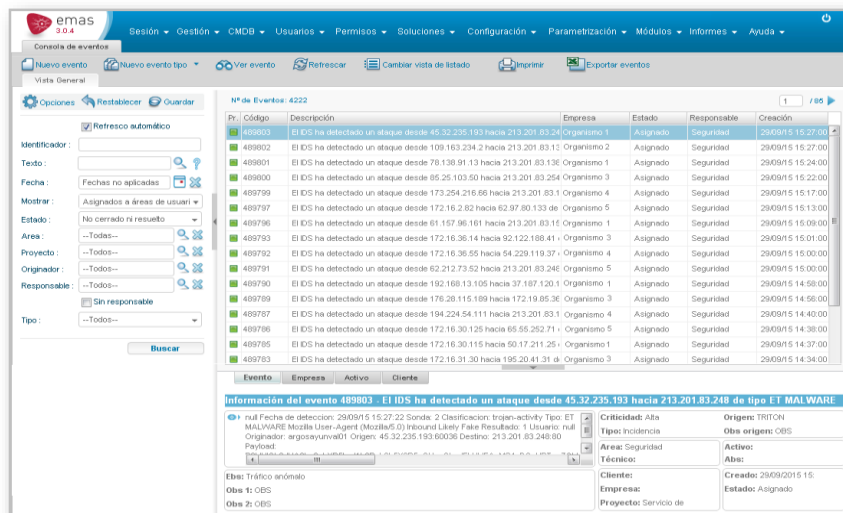


Resumen capacidades generales:

- APT
- Malware
- IOC
- Anomalías estadísticas
- Anomalías conocimiento
- Usos indebidos
- Extensible



Consola central para la gestión del ciclo de vida de eventos e incidentes, con capacidad para implementar un modelo de actuación procedimentado y trazable, vigilando la calidad de servicio, gestionando el conocimiento del centro y optimizando el uso de los recursos.



Resumen capacidades generales:

- Consola Gestión Centralizada
- Control de visibilidad
- Control de acceso
- Categorización de eventos
- Ciclo de vida eventos
- Análisis de la información

Detección de situaciones propias de entornos OT:

Modificar

Imprimir

Salir

Id. evento: 1954

Fecha alta: 09/09/2016 12:29:15

Estado: En proceso

Información del evento

Histórico solicitante

Trazabilidad

Originador:

Administrador Administrador -

Área:

OBS:

Origen:

INTERNO

Cliente:

Administrador Administrador -

Empresa:

OBS cliente:

Proyecto:

Monitorización sistemas industriales

Activo:

OBS activo:

Tipo:

Incidencia

EBS:

Red ICS

Criticidad:

Media

Área asignada:

Responsable:

Administrador Administrador -

Nuevo equipo detectado 10.7.201.160

Descripción

Relaciones (67)

Tiempos

Depende de:

Código	Estado	Descripción
Sin padre		

Eventos dependientes:

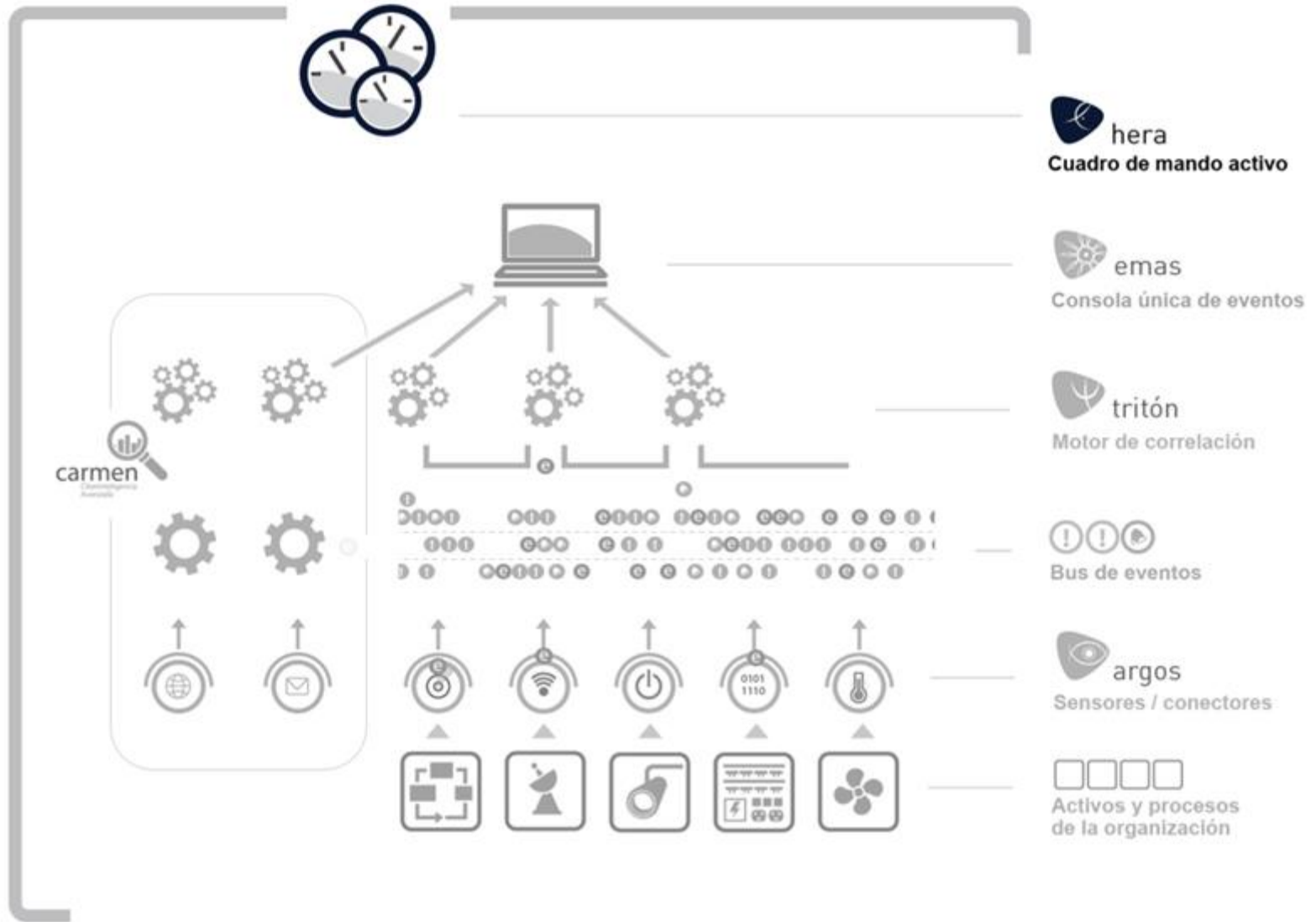
Código	Estado	Descripción
1903	En proceso	Se ha detectado el envío de comandos EIP desde el activo no habitual con dirección IP 10.7.201.160
1883	En proceso	Se ha detectado un escaneo de interfaces Ethernet/IP de la red de control desde la IP 10.7.201.160
1882	En proceso	Se ha detectado un escaneo de servicios Ethernet/IP de la red de control desde la IP 10.7.201.160
1881	En proceso	Se ha detectado el envío de comandos EIP desde el activo no habitual con dirección IP 10.7.201.160
1853	En proceso	Se ha detectado el envío de comandos EIP desde el activo no habitual con dirección IP 10.7.201.160
1852	En proceso	Se ha detectado un paquete Ethernet/IP malformado desde la IP 10.7.201.160 hacia la IP 10.7.201.39 con el comando EIP 1
1851	En proceso	Se ha detectado un escaneo de servicios Ethernet/IP de la red de control desde la IP 10.7.201.160
1850	En proceso	Se ha detectado un escaneo de interfaces Ethernet/IP de la red de control desde la IP 10.7.201.160

☒ Hacer visibles las notas de trabajo en eventos dependientes
 ☒ Hacer visible la solución en eventos dependientes
 ☒ Trasladar cambio de estado a los eventos dependientes

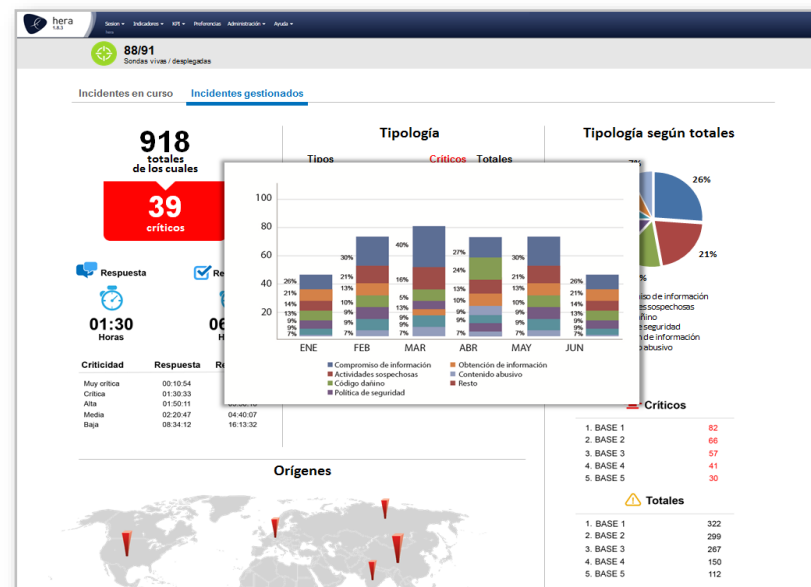
Eventos dependientes:

Código	Estado	Descripción
1903	En proceso	Se ha detectado el envío de comandos EIP desde el activo no habitual con dirección IP 10.7.201.160
1883	En proceso	Se ha detectado un escaneo de interfaces Ethernet/IP de la red de control desde la IP 10.7.201.160
1882	En proceso	Se ha detectado un escaneo de servicios Ethernet/IP de la red de control desde la IP 10.7.201.160
1881	En proceso	Se ha detectado el envío de comandos EIP desde el activo no habitual con dirección IP 10.7.201.160
1853	En proceso	Se ha detectado el envío de comandos EIP desde el activo no habitual con dirección IP 10.7.201.160
1852	En proceso	Se ha detectado un paquete Ethernet/IP malformado desde la IP 10.7.201.160 hacia la IP 10.7.201.39 con el comando EIP 1
1851	En proceso	Se ha detectado un escaneo de servicios Ethernet/IP de la red de control desde la IP 10.7.201.160
1850	En proceso	Se ha detectado un escaneo de interfaces Ethernet/IP de la red de control desde la IP 10.7.201.160

☒ Hacer visibles las notas de trabajo en eventos dependientes
 ☒ Hacer visible la solución en eventos dependientes
 ☒ Trasladar cambio de estado a los eventos dependientes

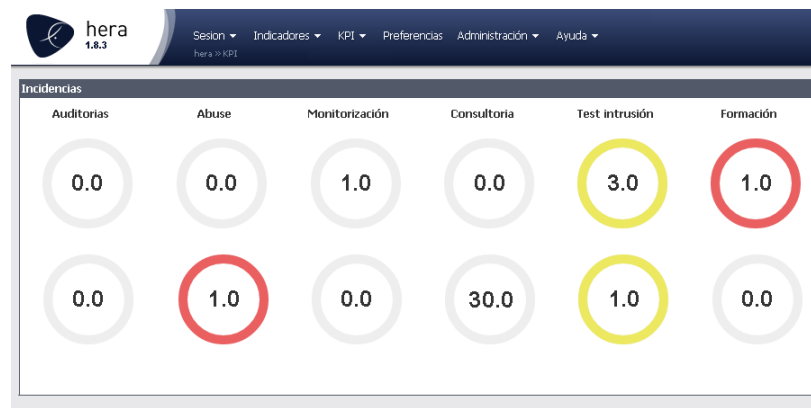


Hera representa en tiempo real indicadores de funcionamiento del Centro de Servicios de Seguridad

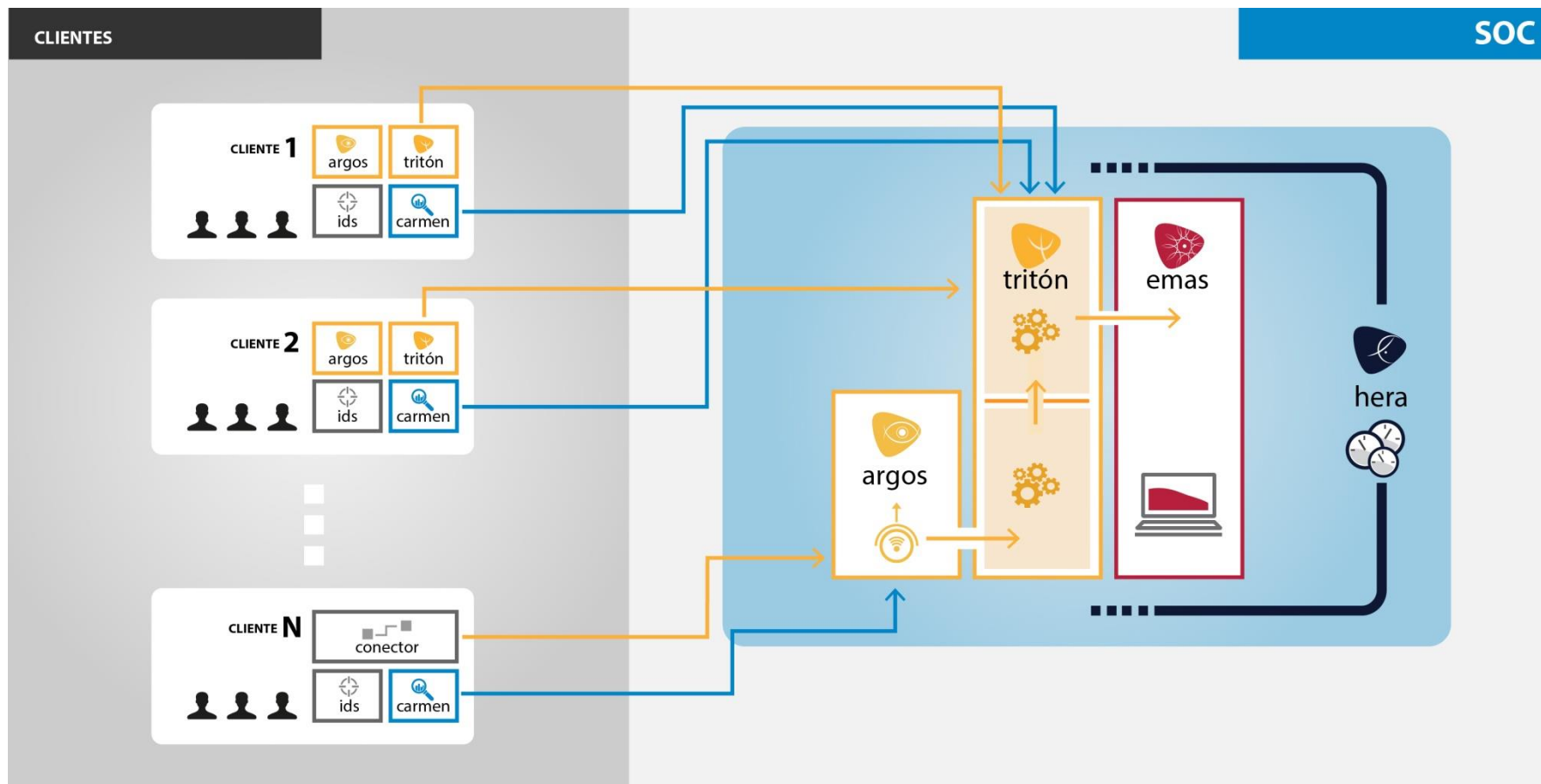


Resumen capacidades generales:

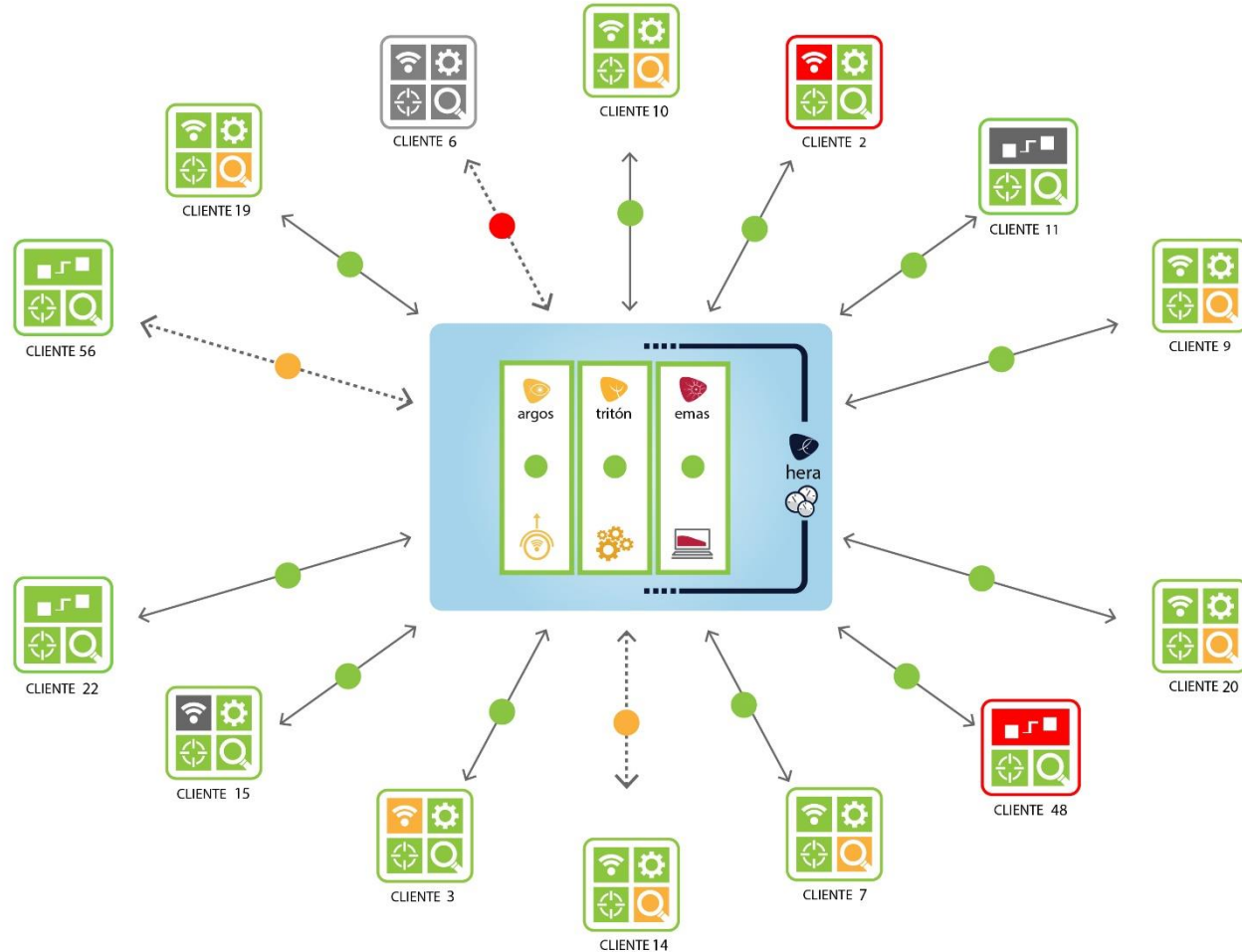
- Cuadro de mando Seguridad
- Evolución de volumetría
- Clasificación de incidentes
- Gráfico por tipologías
- Indicadores personalizados



Como situación de tránsito, o simplemente por conveniencia, la arquitectura soporta un **modelo mixto**, en el que parte de los orígenes funcionan con recolección y correlación distribuida, mientras que otros envían sus eventos directamente al nodo central. De esta forma los nodos que más tráfico generan disponen de una sonda distribuida y el resto se apoyan en los recursos del nodo central.

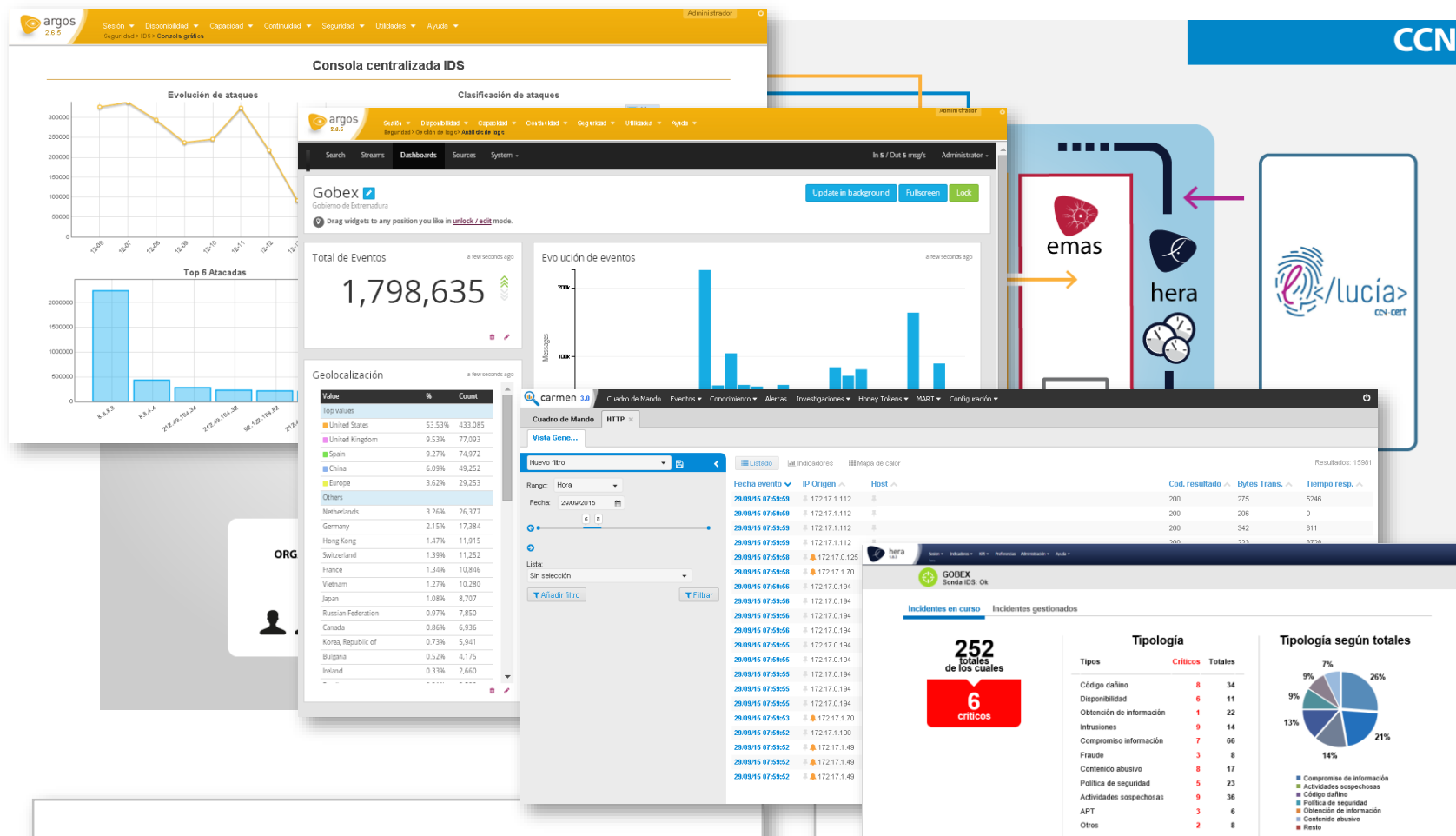


*Vigilancia del correcto funcionamiento de la propia infraestructura desde el punto de vista de la **disponibilidad** y la **capacidad***





eMas en SAT INET / ICS



Organismos:

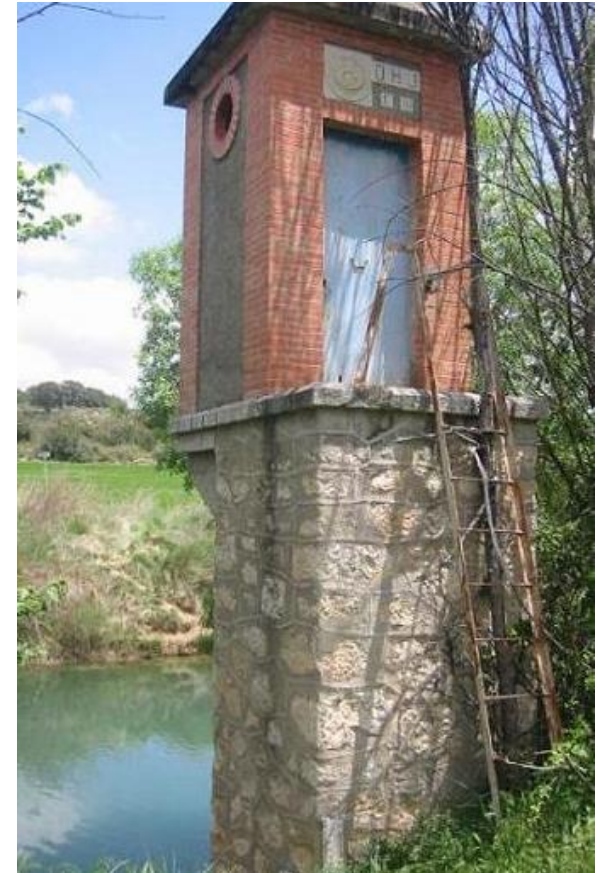
- Recolección y análisis local (argos)
- Correlación distribuida (tritón)
- Posibilidad de carmen

CCN:

- Correlación centralizada 2º nivel
- Consola de gestión incidentes
- Cuadro de mando

El despliegue de SAT ICS comenzó en noviembre de 2016

- Despliegue de la primera sonda SAT ICS en la red del SAIH (Sistema Automático de Información Hidrológica) de una Confederación Hidrográfica.
- El sistema recolecta las medidas de parámetros de interés hidrográfico de la instrumentación distribuida en las cuencas de la Confederación (aforos, pluviómetros, etc.)
- La sonda SAT ICS monitoriza la red y las comunicaciones con los concentradores y las remotas en campo.



Plantas de tratamiento de agua, sistemas de distribución de agua potable, sistemas de distribución de energía eléctrica









MADRID

Velázquez 150, 2ª planta,
28002
T.(+34) 902 882 992



BARCELONA

Llull, 321 (Edifici Cinc)
08019
T.(+34) 902 882 992



VALENCIA

Ramiro de Maeztu 7,
46022
T.(+34) 902 882 992



BOGOTÁ

Carrera 11 N° 93A - 53,
Of. 401
T.(+571) 745 74 39



MÉXICO

S2 Iberoamérica, Praga
44-7, México D.F.
06600
T.(+52) 55 2128 0681

info@s2grupo.es
www.s2grupo.es
www.securityartwork.es

