JORNADA STIC

CAPÍTULO COLOMBIA

“Detección de anomalías en redes de Infraestructura Críticas mediante el uso de CARMEN”

En colaboración con:

ccn-cert centro criptológico nacional

incibe_

ean universidad

fundación in-n-va

Enrique Fenollosa Romero

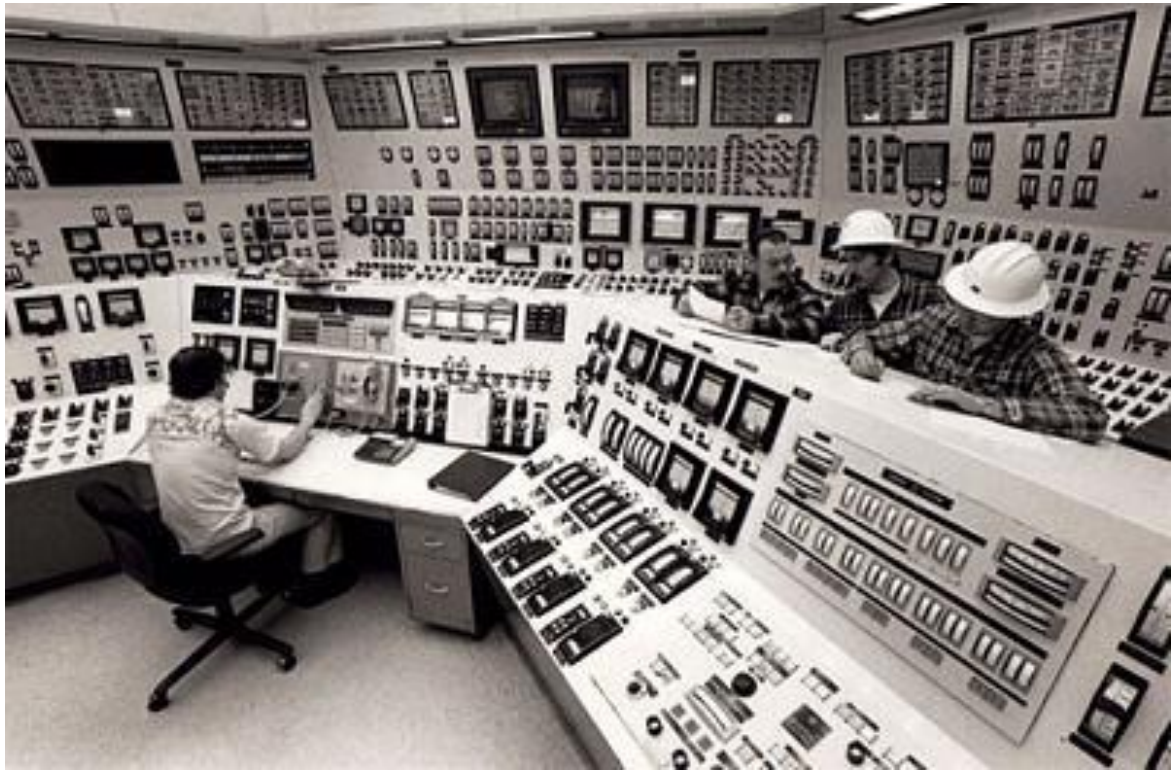
LATAM General Manager
S2 Grupo

enrique.fenollosa@s2grupo.com

Contexto actual

Tecnologías Operacionales e Infraestructuras Críticas

Anteriormente…



- Poca consideración de la ciberseguridad en ninguna fase, salvo en ámbitos muy específicos.
- Con escasa concienciación en ningún nivel de las compañías, salvo en ámbitos muy específicos.
- Sin metodologías, sin referentes, antecedentes ni experiencia.
- Clara separación entre IT y OT

Contexto actual

Tecnologías Operacionales e Infraestructuras Críticas

Actualmente…

- **Más incidentes** en compañías industriales
- **Integración creciente** de redes y sistemas de distinto propósito, generalmente **sin un plan definido**.
- **Escasa integración de los equipos de personas implicados en la seguridad** de estos sistemas, lo que resulta en problemas a la hora de adoptar e implantar controles.
- **Dificultades de la gestión técnica** de la ciberseguridad por falta de especialistas.
- Aparición de **marcos normativos y legislativos**, tanto generales como específicos.
- Aumento del grado de **concienciación** de los directivos y personal de estas compañías.
- Aumento en la demanda de **formación especializada**.

Características de los entornos Industriales

- *"Conjunto de dispositivos y procesos que actúan en tiempo real sobre sistemas operacionales físicos como las redes de distribución de electricidad, las plantas de producción de vehículos, cadenas de fabricación, sistemas de control de acceso, sistemas automáticos de extinción de incendios, etcétera."*

- Estos dispositivos dan **soporte** a los **procesos** de **fabricación** y de **control industrial**, en una amplia variedad de entornos, tales como:
  - **Sector eléctrico**: generación, transporte y distribución
  - **Aguas**: potabilización, distribución y tratamiento de aguas residuales
  - **Hospitales**: distribución de gases medicinales
  - **Sector alimentación:** producción de alimentos
  - **Manufactura**: fábricas que cualquier tipo de componente
  - **Sistemas de gestión de edificios**
  - **Otros**

Vulnerabilidades comunes y factores de riesgo de los entornos Industriales

- Perímetros de red indefinidos (no segmentación de las redes)
- Puertos físicos accesibles
- **Configuraciones por defecto**
- Aplicaciones y servicios innecesarios
- **Protocolos de comunicaciones industriales desarrollados sin mecanismos de seguridad**
- Indebida aplicación de **actualizaciones de seguridad**
- Controles de acceso inadecuados o inexistentes
- Incorrecta gestión de logs
- **Sistemas conectados y expuestos a internet**
- **Profesionales en seguridad no involucrados desde el diseño y el mantenimiento**
- Falta de procesos, herramientas y plataformas de seguridad
- **Convergencia con tecnologías IT** de propósito general (**protocolos, servicios, sistemas operativos**)
- Profesionales expertos en procesos industriales sin conocimiento de Ciberseguridad
- Profesionales responsables de la Seguridad IT encargados también de la Seguridad OT
- **Ausencia de monitorización especializada de redes OT**

Contexto actual

Amenazas que afectan las Infraestructuras Críticas

ESI AFRICA — AFRICA'S POWER JOURNAL

NEWS & COMMENTARY · RESOURCES · MAGAZINE · EVENTS · TENDERS · ENGAGE · PARTNERS · JOIN

Industry Sectors | Business and markets | Metering | News | Regional News | Southern Africa | Transmission and Distribution

Cyberattack leaves South African power utility customers in the dark

Jul 26, 2019

MOST READ

Siemens Energy scores a deal in the Mozambique LNG project

Oct 15, 2020

Ifeoma Malo has just one goal: Ending energy poverty

Oct 13, 2020

Connecting investors with energy developers operating in Africa

BlackEnergy trojan strikes again: Attacks Ukrainian electric power industry

The recent attacks on the electrical power industry in Ukraine are connected to attacks on the media and to targeted cyber-espionage attacks against Ukrainian governmental agencies.

COMPUTERWORLD UNITED STATES

NEWS

Attack campaign infects industrial control systems with BlackEnergy malware

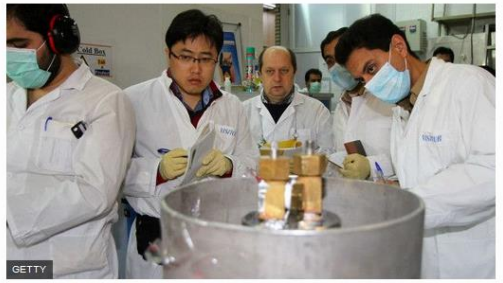
Customers of three SCADA human-machine interfa vendors were potentially affected, ICS-CERT said

By Lucian Constantin

CSO Senior Writer, IDG News Service | OCT 29, 2014 8:58 AM PDT

El virus que tomó control de mil máquinas y les ordenó autodestruirse

11 octubre 2015



GETTY

El ataque del gusano Stuxnet destruyó 1000 máquinas en la central nuclear de Natanz, Irán

40 Telangana sub-stations attacked by Chinese malware

Telangana SLDC, which manages power supply in the state, says state agencies have removed all malware in these substations after alert from central agency. They have strengthened firewall as well

BusinessToday.In | March 3, 2021 | Updated 10:34 IST

Monitorización de los entornos Industriales

- En la sociedad moderna actual, los entornos Industriales son integrados por una colección de dispositivos, diseñados para trabajar conjuntamente como un sistema integrado y homogéneo, **Sí uno de estos sistemas falla, puede desencadenar un efecto dominó catastrófico.** Por eso, a diferencia de los **entornos IT,** donde la ***confidencialidad*** es lo más importante, en los **sistemas de control industrial** la ***disponibilidad*** prima. Por ello es importante ***la Monitorización en tiempo real de las redes de control (OT).***

- La monitorización especializada en entornos OT, permite solventar:

  - La identificación de **ataques conocidos mediante firmas**

  - El descubrimiento de **equipos no identificados**

  - Detección de **comunicaciones no habituales**

  - Detección de **anomalías en el uso de protocolos industriales** y **detección** de **comandos** altamente **peligrosos** para un entorno industrial

Ventajas de la Monitorización de los entornos Industriales

Identificación de ataques conocidos mediante firmas

- Los equipos específicos desplegados en entornos industriales contienen el **mismo tipo de vulnerabilidades que los de otros entornos**.
- Los **sistemas y protocolos** tradicionales **de redes corporativas** también están **presentes** en las redes OT
- Las técnicas de **ataque típicas** a **redes corporativas** siguen afectando a las **redes industriales**

Descubrimiento de equipos no identificados

- Las redes de **control no están sometidas a cambios frecuentes (topología y dispositivos)**.
- **Definir el comportamiento normal de la red** y los equipos de una forma mucho **más precisa** que en otro tipo de redes, lo que se traduce en poder **detectar más fácilmente comportamientos sospechosos** basándonos en anomalías.

Detección de comunicaciones no habituales en entornos aislados

- **Estructura de comunicaciones habituales bien definida**
- Los ataques pueden utilizar las **mismas técnicas que las actividades legítimas**, por lo que para identificarlas es **importante el contexto**

Detección de anomalías en el uso de protocolos industriales

- **La propia funcionalidad de los protocolos industriales y su bajo nivel de seguridad, junto a las configuraciones inseguras por defecto**, disminuye la necesidad de utilizar exploits o ataques conocidos por parte de los atacantes para causar un gran impacto

Convergencia IT-OT

Evolución reciente: Convergencia IT-OT

Anteriormente…..

Las tecnologías de la información (TI) y las tecnologías operacionales (OT) tienen **historias largas y aisladas** con muchos ejemplos de intentos fallidos de integrarlas o incluso utilizar herramientas de un entorno en el otro.

En la actualidad …..

El uso y los beneficios derivados de las tecnologías de la información (TI) y la **convergencia** de la tecnología operativa (OT) están creciendo y permiten una **gestión y operación más efectivas** de los sistemas de control contemporáneos. La convergencia mejora los tiempos de actividad, el rendimiento, la calidad y la productividad, todo lo cual genera mayores beneficios para los operadores de Infraestructuras Críticas.

Sin embargo, la **convergencia** de TI /OT conlleva **desafíos** únicos que dificultan la administración y seguridad de los sistemas de control industrial (ICS). Esto se debe a una mayor **complejidad técnica**, una mayor **complejidad de riesgos** y más importante aún, la aparición de ***nuevas amenazas cada vez más sofisticadas***

Evolución reciente: Convergencia IT-OT

Implicaciones en la Monitorización y nuevos desafíos

- La **Monitorización de seguridad** en tiempo real se enfoca en la **estabilidad** y el **determinismo** de las redes: equipos, comunicaciones, protocolos.

- La **combinación** y uso de **protocolos de comunicación** comunes de **IT** y protocolos industriales **OT**, genera una diversa variedad de tráfico en las redes de **Infraestructura Crítica**.

- El monitoreo basado en **comportamientos deterministas,** presenta un **enfoque de seguridad** reactivo y no **anticipado**, la gestión de los **incidentes** se presenta luego de verse afectadas las **infraestructuras críticas**.

- Las **amenazas** a su vez **convergen**, las **APT's** trabajan de manera **organizada**, los **atacantes** aprenden sobre el funcionamiento de los **Sistemas de Control Industrial** a profundidad**.**
  Las amenazas están **creciendo** a un ritmo tres veces más rápido de lo que están inactivas con el pasar de los últimos años

Detección de anomalías en entornos IT-OT

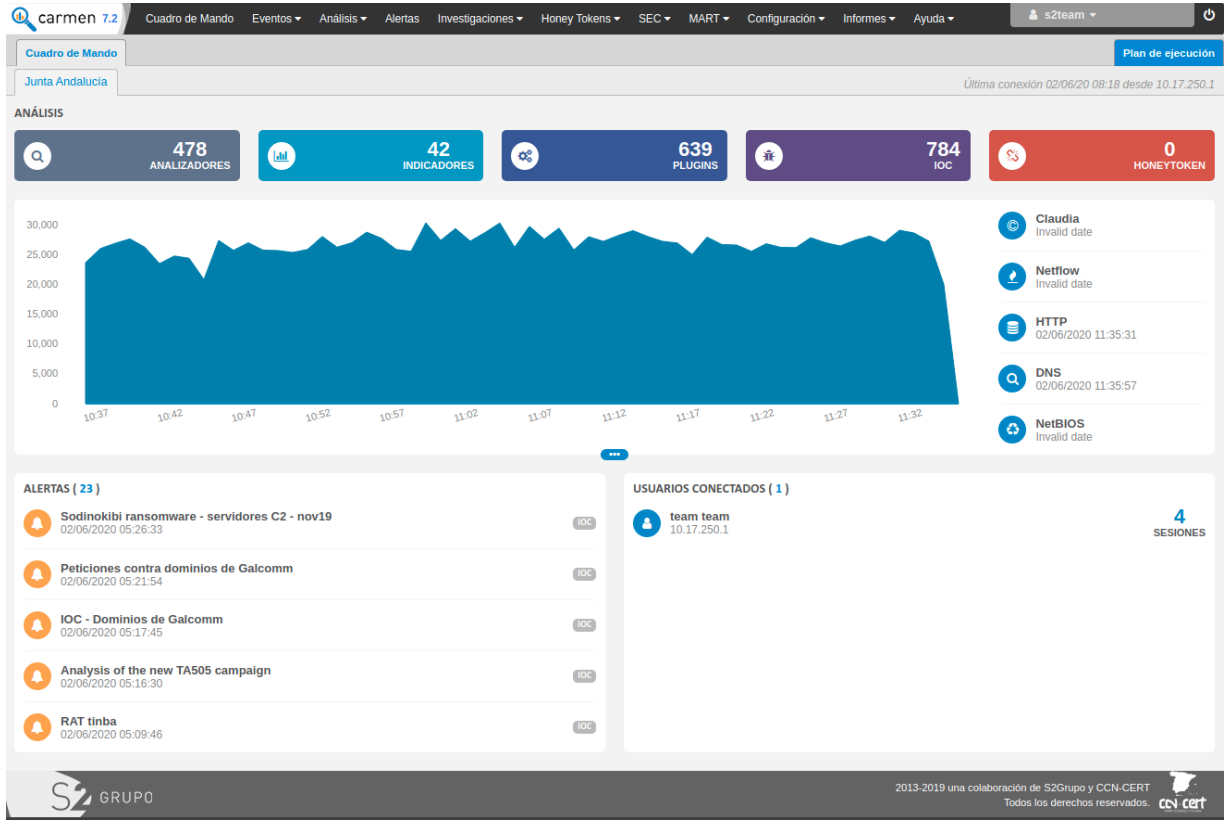
Características de CARMEN

- Dispone de **capacidades** para la **protección avanzada** ante **amenazas** en la organización.
- **Analiza** todo el **tráfico (saliente/entrante)** de la red de una organización.
- **Adquiere**, **procesa** y **analiza** el tráfico para la **defensa** de las organizaciones.
- Identifica usos **indebidos** y detecta **anomalías** o intentos de **intrusión** mediante el uso de reglas de detección.

Detección de anomalías en entornos IT-OT

Características de CARMEN

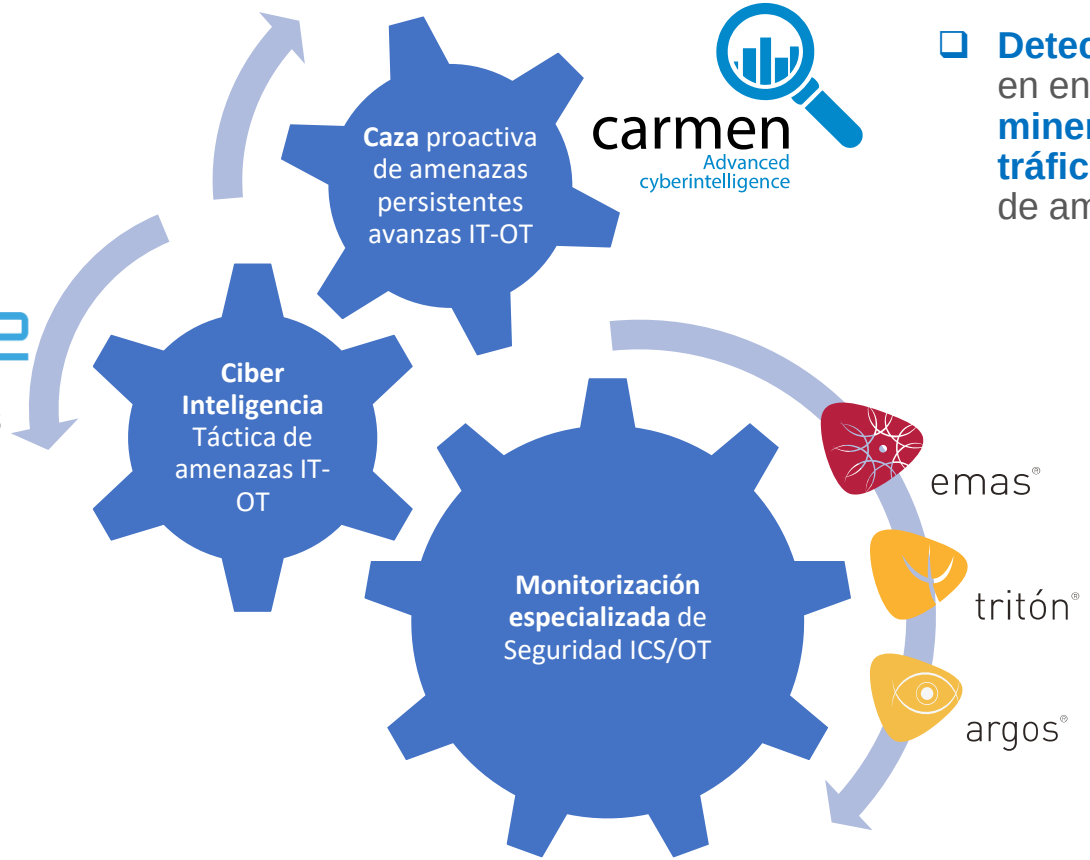
- La **información** es **organizada** y representada para facilitar el desempeño de los equipos de **seguridad**.
- Herramienta de **análisis** y **generación** de **inteligencia** táctica de **amenazas** persistentes avanzadas.
- Facilita la **identificación** de grupos **APT**
- Provee **capacidades** para la oportuna **respuesta** ante **incidentes** de seguridad.



Convergencia de amenazas IT-OT

Implicaciones en la Monitorización y nuevos desafíos

- Con **amenazas** cada vez más **sofisticadas** y **avanzadas,** la ***Monitorización*** de Seguridad de las ***redes industriales,*** se complementa con el **análisis de anomalías**, la ***Ciber inteligencia*** táctica de amenazas y la ***caza proactiva*** de las mismas o **Threat Hunting**



- ❑ **Detección de anomalías avanzadas** en entornos IT/OT a través de la **minería de datos** resultante del **tráfico de red** monitorizado – Caza de amenazas

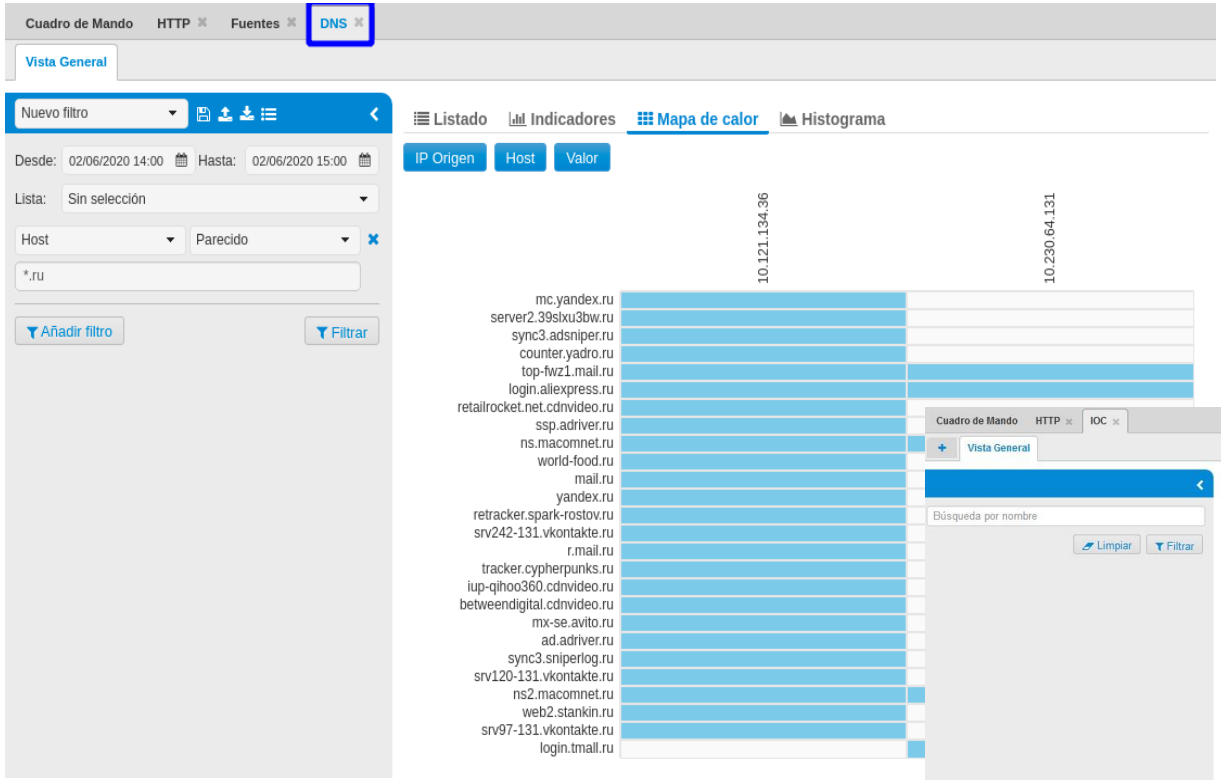
Lab52

- ❑ Proceso de **vigilancia** de amenazas Persistentes avanzadas (**APT**)
- ❑ Correlación de **Indicadores de Compromiso**
- ❑ **Modelamiento** de amenazas IT-OT

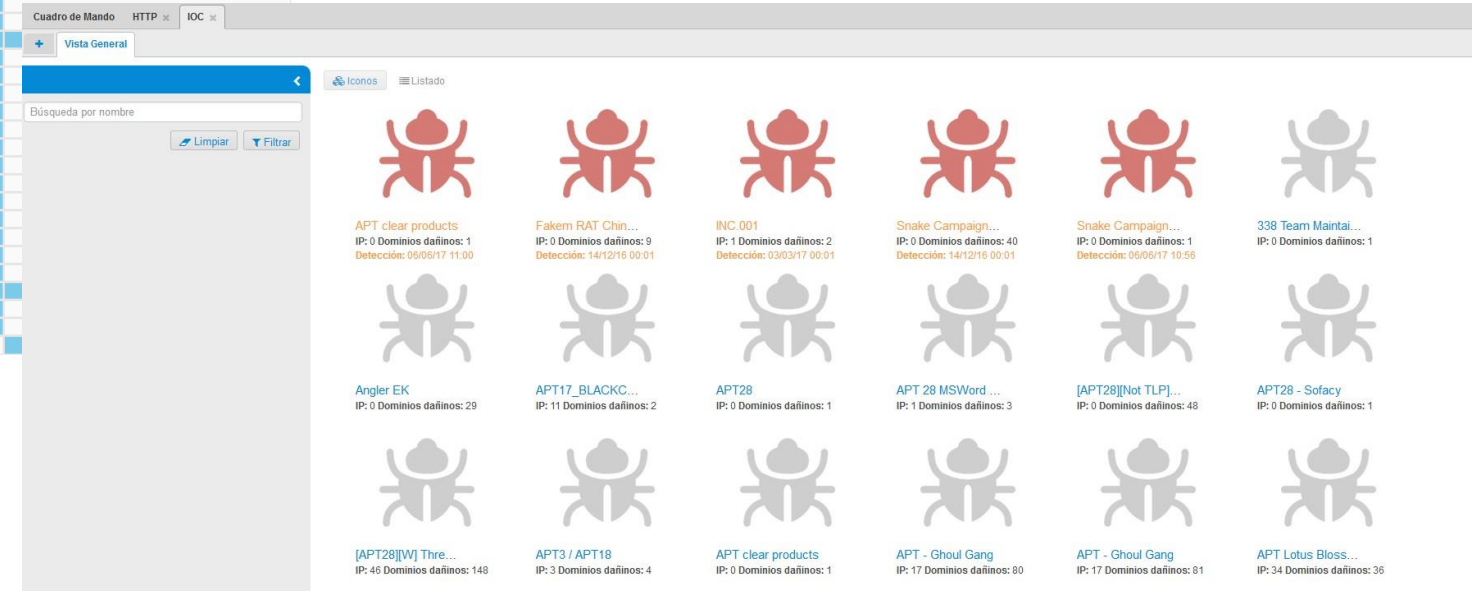
- ❑ Identificación de **ataques conocidos** mediante **firmas**
- ❑ Descubrimiento de **equipos no identificados**
- ❑ Detección de **comunicaciones no habituales**
- ❑ Detección de **anomalías** en el uso de **protocolos industriales** y detección de **comandos peligrosos**

Detección de anomalías en entornos IT-OT

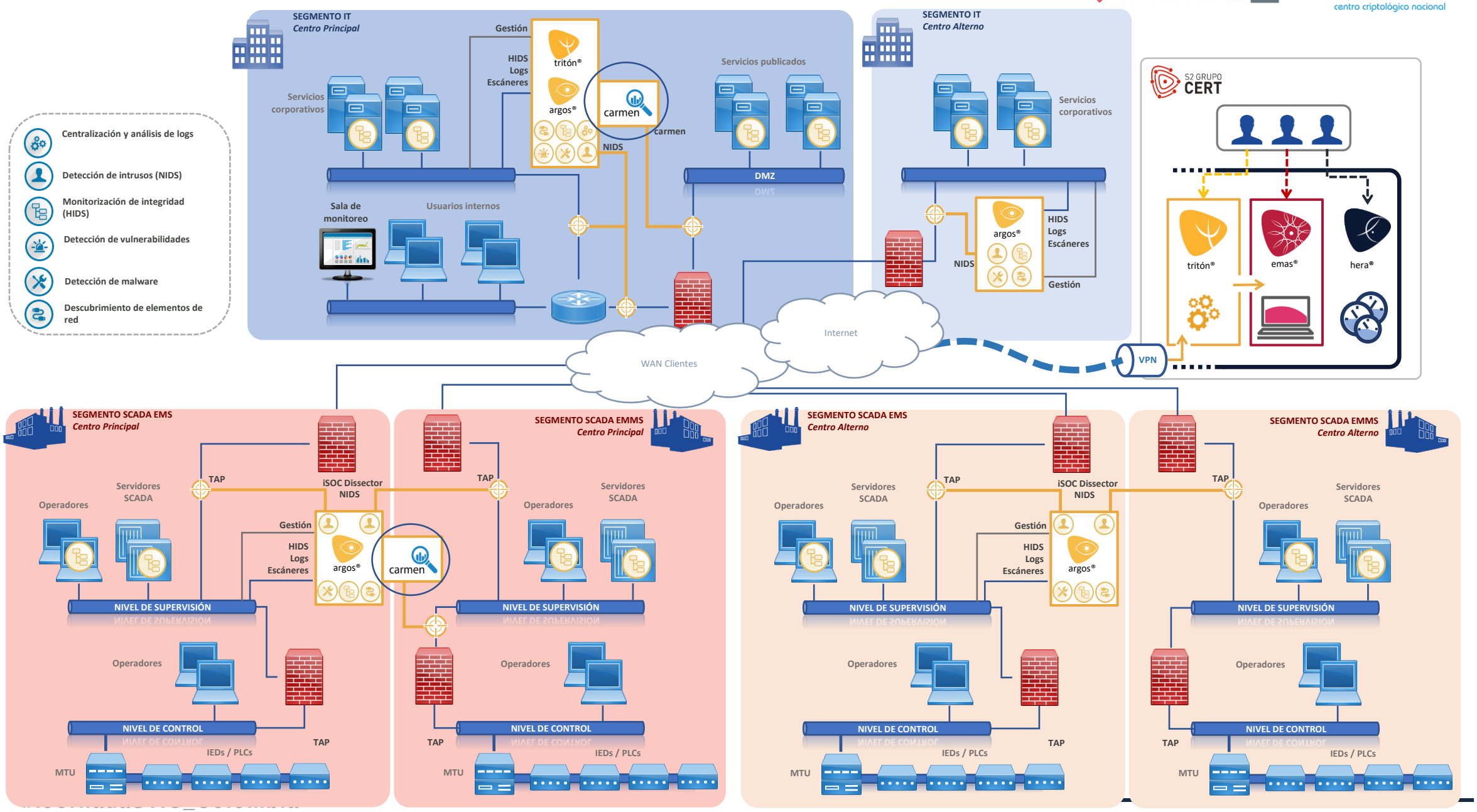
Ejemplos de uso de CARMEN

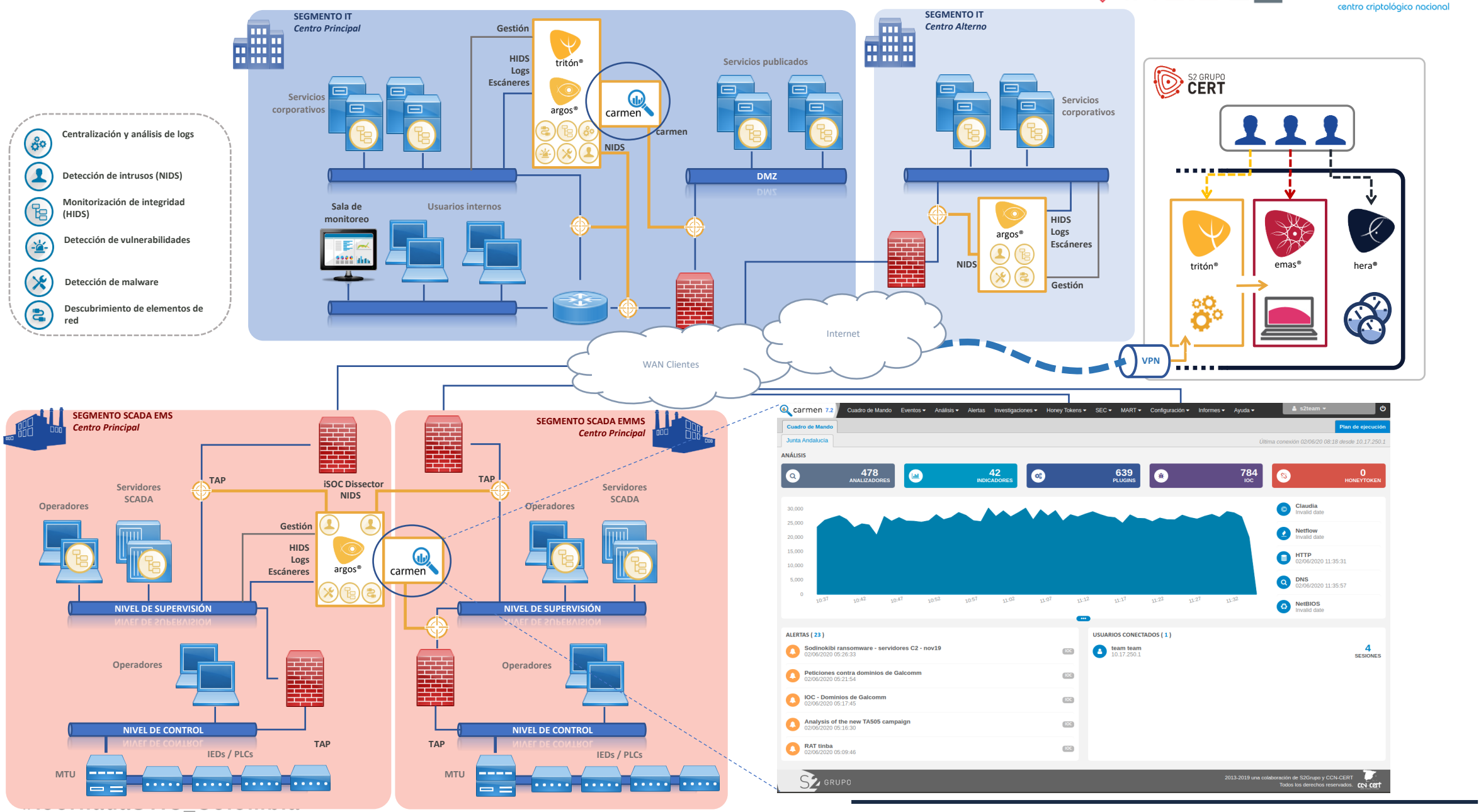


- Análisis de **comunicaciones** externas



- Identificación de grupos **APT**´s


Centralización y análisis de logs
Detección de intrusos (NIDS)
Monitorización de integridad (HIDS)
Detección de vulnerabilidades
Detección de malware
Descubrimiento de elementos de red
SEGMENTO IT
Centro Principal
Gestión
HIDS
Logs
Escáneres
tritón®
argos®
carmen
NIDS
Servicios publicados
Servicios corporativos
DMZ
Sala de monitoreo
Usuarios internos
SEGMENTO IT
Centro Alterno
Servicios corporativos
argos®
NIDS
HIDS
Logs
Escáneres
Gestión
S2 GRUPO
CERT
tritón®
emas®
hera®
VPN
Internet
WAN Clientes
SEGMENTO SCADA EMS
Centro Principal
TAP
iSOC Dissector
NIDS
Servidores SCADA
Operadores
Gestión
HIDS
Logs
Escáneres
argos®
carmen
NIVEL DE SUPERVISIÓN
Operadores
NIVEL DE CONTROL
TAP
IEDs / PLCs
MTU
SEGMENTO SCADA EMMS
Centro Principal
SEGMENTO SCADA EMS
Centro Alterno
SEGMENTO SCADA EMMS
Centro Alterno

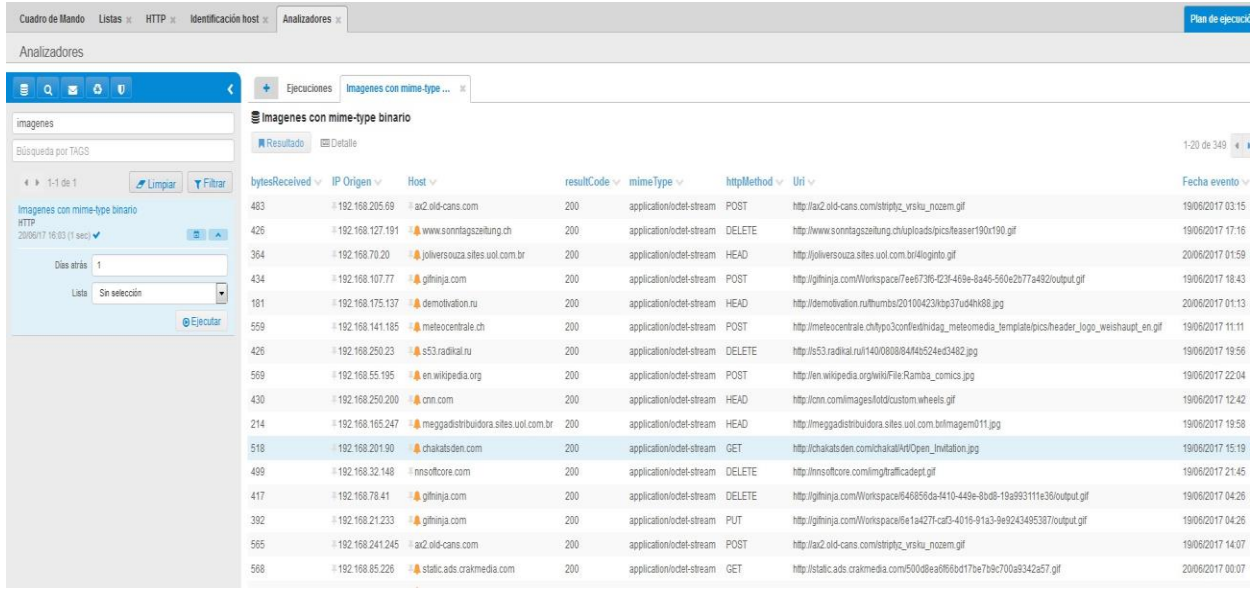

Centralización y análisis de logs
Detección de intrusos (NIDS)
Monitorización de integridad (HIDS)
Detección de vulnerabilidades
Detección de malware
Descubrimiento de elementos de red
SEGMENTO IT
Centro Principal
Gestión
HIDS
Logs
Escáneres
tritón®
argos®
carmen
NIDS
Servicios publicados
Servicios corporativos
DMZ
Sala de monitoreo
Usuarios internos
SEGMENTO IT
Centro Alterno
Servicios corporativos
argos®
NIDS
HIDS
Logs
Escáneres
Gestión
S2 GRUPO
CERT
tritón®
emas®
hera®
VPN
Internet
WAN Clientes
SEGMENTO SCADA EMS
Centro Principal
TAP
iSOC Dissector
NIDS
Servidores SCADA
Operadores
Gestión
HIDS
Logs
Escáneres
argos®
carmen
NIVEL DE SUPERVISIÓN
Operadores
NIVEL DE CONTROL
TAP
IEDs / PLCs
MTU
SEGMENTO SCADA EMMS
Centro Principal
TAP
Servidores SCADA
Operadores
NIVEL DE SUPERVISIÓN
Operadores
NIVEL DE CONTROL
TAP
IEDs / PLCs
MTU
carmen 7.2
Cuadro de Mando
Eventos
Análisis
Alertas
Investigaciones
Honey Tokens
SEC
MART
Configuración
Informes
Ayuda
s2team
Cuadro de Mando
Plan de ejecución
Junta Andalucía
Última conexión 02/06/20 08:18 desde 10.17.250.1
ANÁLISIS
478 ANALIZADORES
42 INDICADORES
639 PLUGINS
784 IOC
0 HONEYTOKEN
Claudia
Invalid date
Netflow
Invalid date
HTTP
02/06/2020 11:35:31
DNS
02/06/2020 11:35:57
NetBIOS
Invalid date
ALERTAS (23)
Sodinokibi ransomware - servidores C2 - nov19
02/06/2020 05:26:33
Peticiones contra dominios de Galcomm
02/06/2020 05:21:54
IOC - Dominios de Galcomm
02/06/2020 05:17:45
Analysis of the new TA505 campaign
02/06/2020 05:16:30
RAT tinba
02/06/2020 05:09:46
USUARIOS CONECTADOS (1)
team team
10.17.250.1
4 SESIONES
S2 GRUPO
2013-2019 una colaboración de S2Grupo y CCN-CERT
Todos los derechos reservados.

Detección de anomalías en entornos IT-OT

Aplicación de CARMEN a entornos Industriales

Implementación de analizadores/sensores para:

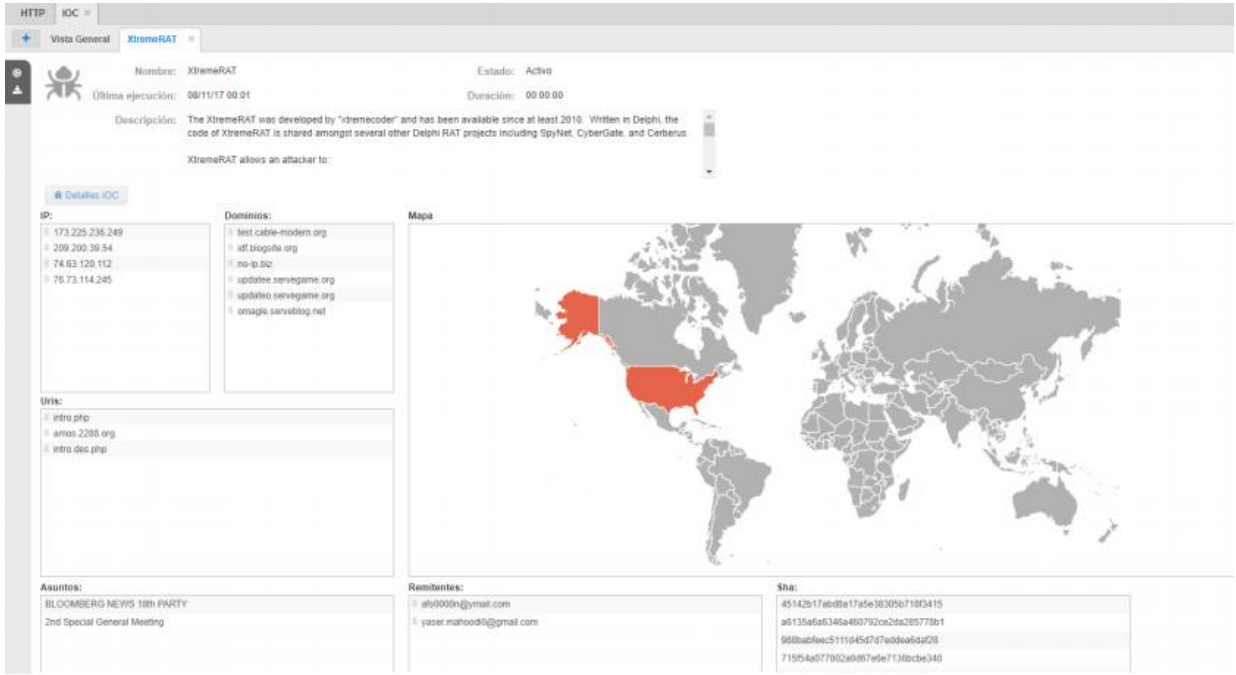
- Detectar **tráfico inusual** en redes **industriales** físicamente aisladas.
- **Analizar** el **tráfico** de **protocolos industriales** que convergen con protocolos comunes de **IT**.
- **Identificar comunicaciones dentro** y **fuera** del perímetro de las **redes industriales**.
- **Identificar puertos** de conexión/servicios **anómalos**.
- Detectar **amenazas sofisticadas** dentro del perímetro de red, y las **actividades maliciosas** que se ejecutan en **equipos** de la red.



Detección de anomalías en entornos IT-OT

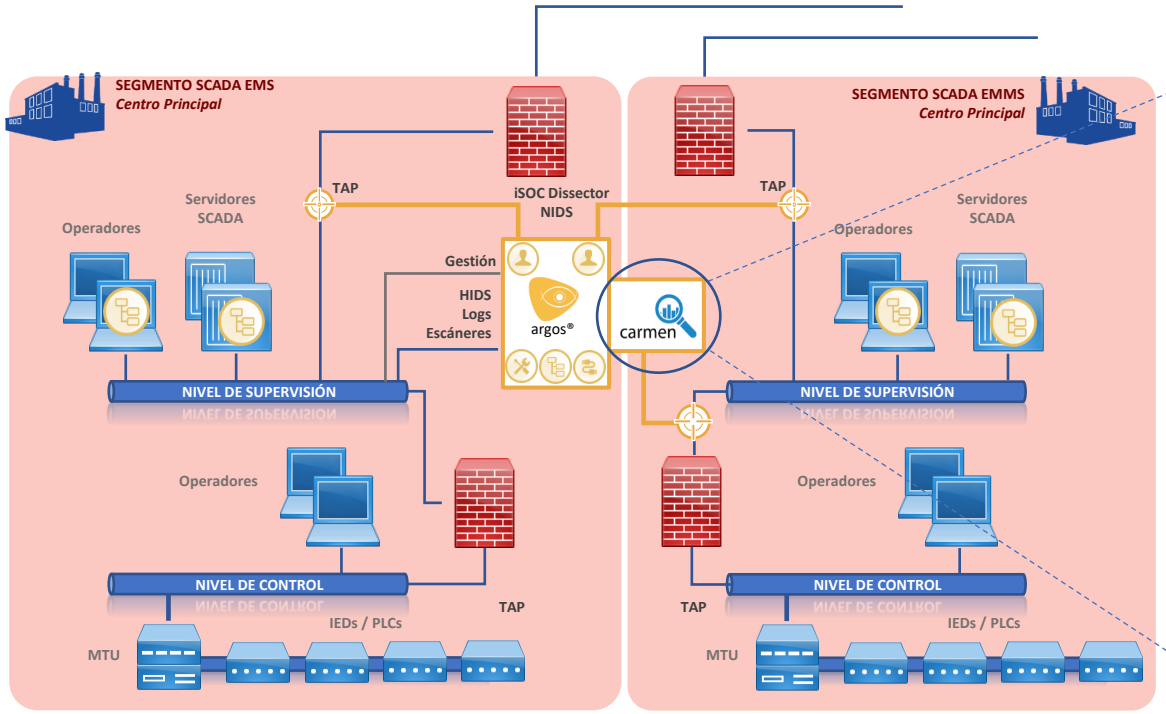
Aplicación de CARMEN a entornos Industriales

- Identificar **conexiones externas** hacia determinados **países**.
- **Detectar descargas** de **herramientas especializadas** y recursos **maliciosos** desde **internet**.
- Detectar procesos **maliciosos** que son ejecutados en **equipos**
- Detectar **direcciones maliciosas** en **internet** utilizadas por determinados grupos APT’s.
- Detectar profundamente la presencia de **adversarios avanzados** que **evaden controles** de seguridad típicos mediante el uso de **investigaciones.**



Detección de anomalías en entornos IT-OT

Ejemplo - Aplicación de CARMEN a entornos Industriales



- **Objetivo:**

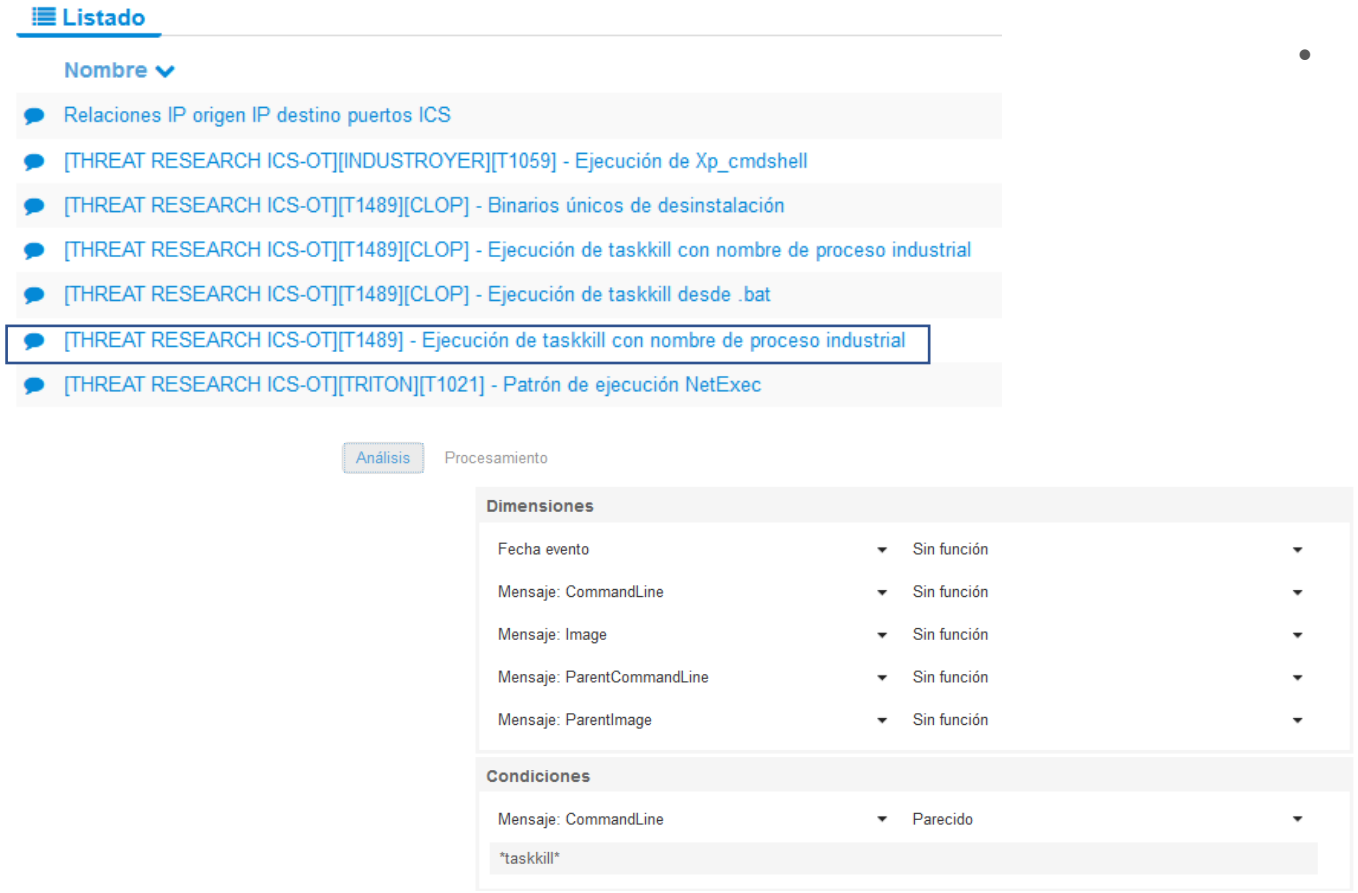
- Identificar **anomalías** relacionadas con intentos de **forzado** de **procesos** que ocasionan **perdida** de **visibilidad** de la red de **supervisión** sobre la red de **control**.

- Esta **técnica** es utilizada por 6 familias de **ransomware** dirigido al **Sector Industrial**

  - DoppelPaymer
  - LockerGoga
  - Maze
  - MegaCortex
  - Nefilim
  - SNAKEHOSE

Detección de anomalías en entornos IT-OT

Ejemplo - Aplicación de CARMEN a entornos Industriales



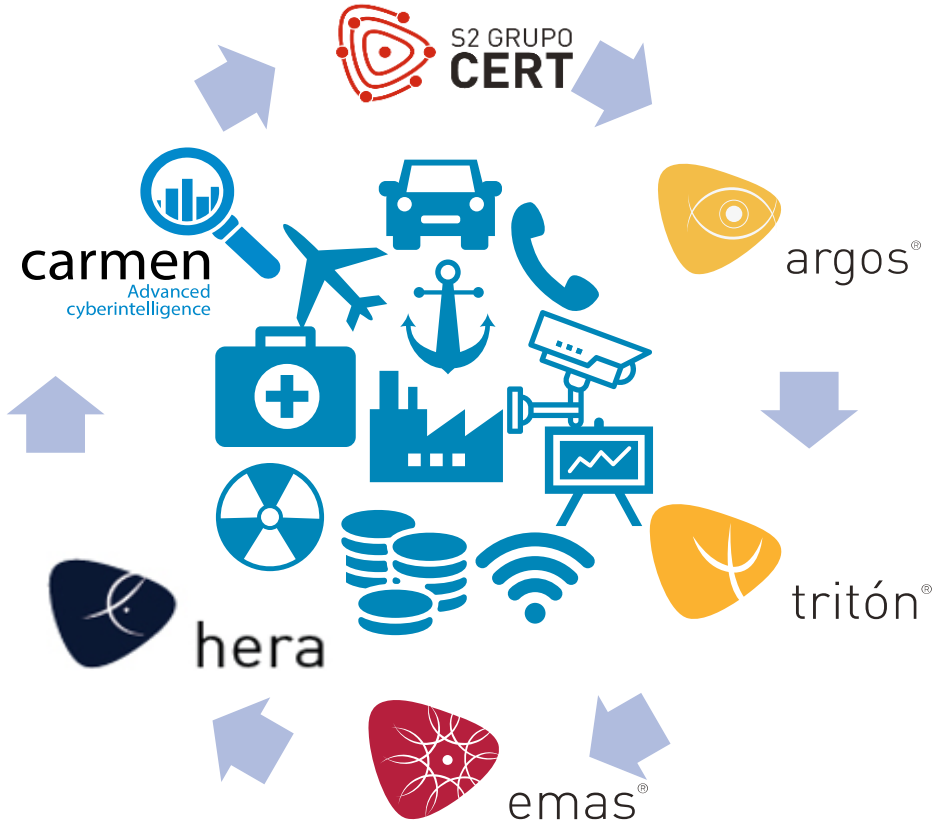
- **Solución:**
  - Mediante este analizador, se **detectan** intentos de ejecución del comando **taskkill,** utilizado para **detener procesos críticos** en entornos de **control industrial**
  - taskkill /im proficyclient.exe
  - taskkill /im OPCUASERVERWINCC.exe
  - taskkill /im SIEMENS.INFORMATIONSERVER.exe

Conclusiones…

- Los **sistemas de monitorización especializada** posibilitan, **identificar casos de seguridad** en entornos **IT -OT**. Este enfoque se **complementa** a través de la implementación de una capa adicional de detección de anomalías avanzadas mediante la ***minería de datos.***

- Este **nuevo enfoque** de seguridad **aplicado** a entornos ***industriales,*** es **anticipado** y no **reactivo**, de tal manera que provee a los equipos y operadores de Infraestructuras Críticas una **mayor** y **oportuna** respuesta en la gestión de **incidentes.**

- La combinación entre **Monitorización**, **CiberInteligencia Táctica** de amenazas y la detección de **anomalías avanzadas,** hace que los principales sectores de la Industria, sus redes e infraestructuras se anticipen ante la aparición de potenciales riesgos. Esto es de vital **importancia** en la protección continua de las **Infraestructuras Críticas** de una **Nación**.



I JORNADA STIC

CAPÍTULO COLOMBIA

GRACIAS

En colaboración con:

cn-cert centro criptológico nacional

incibe_

ean universidad

fundación in-n-va