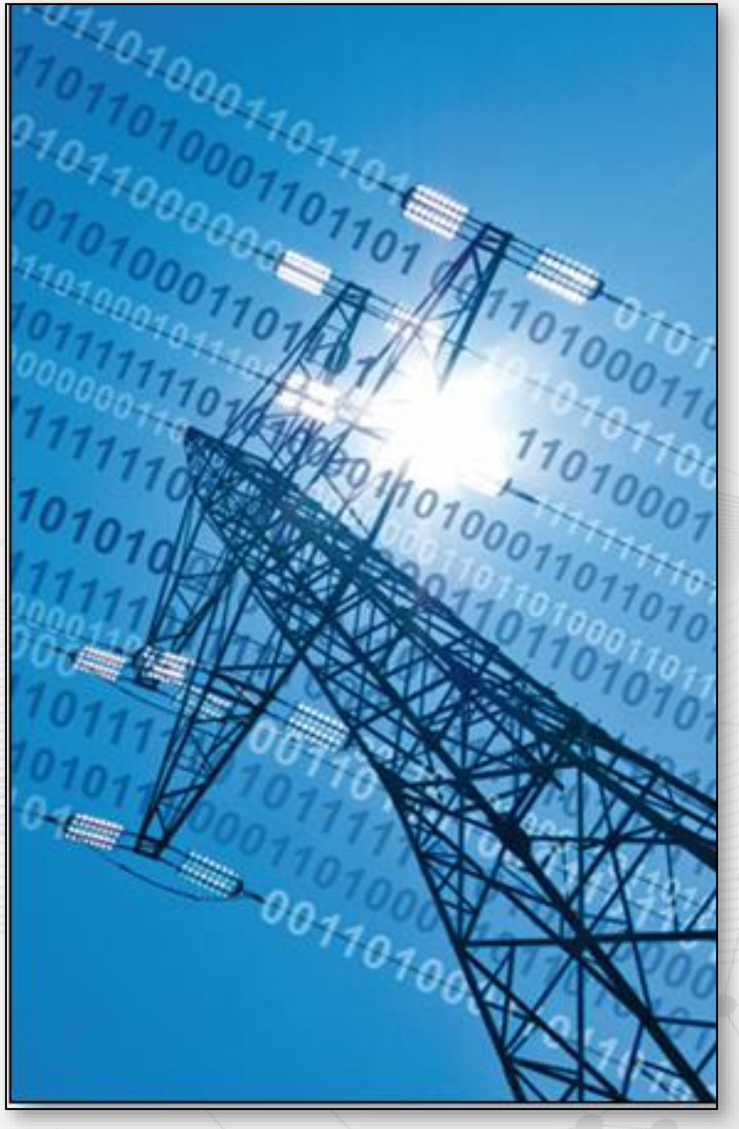
Managed Cyber Security for Protecting Critical Infrastructures

Stefan Beyer – S2 Grupo

Cyber Security Threats to Critical Infrastructures

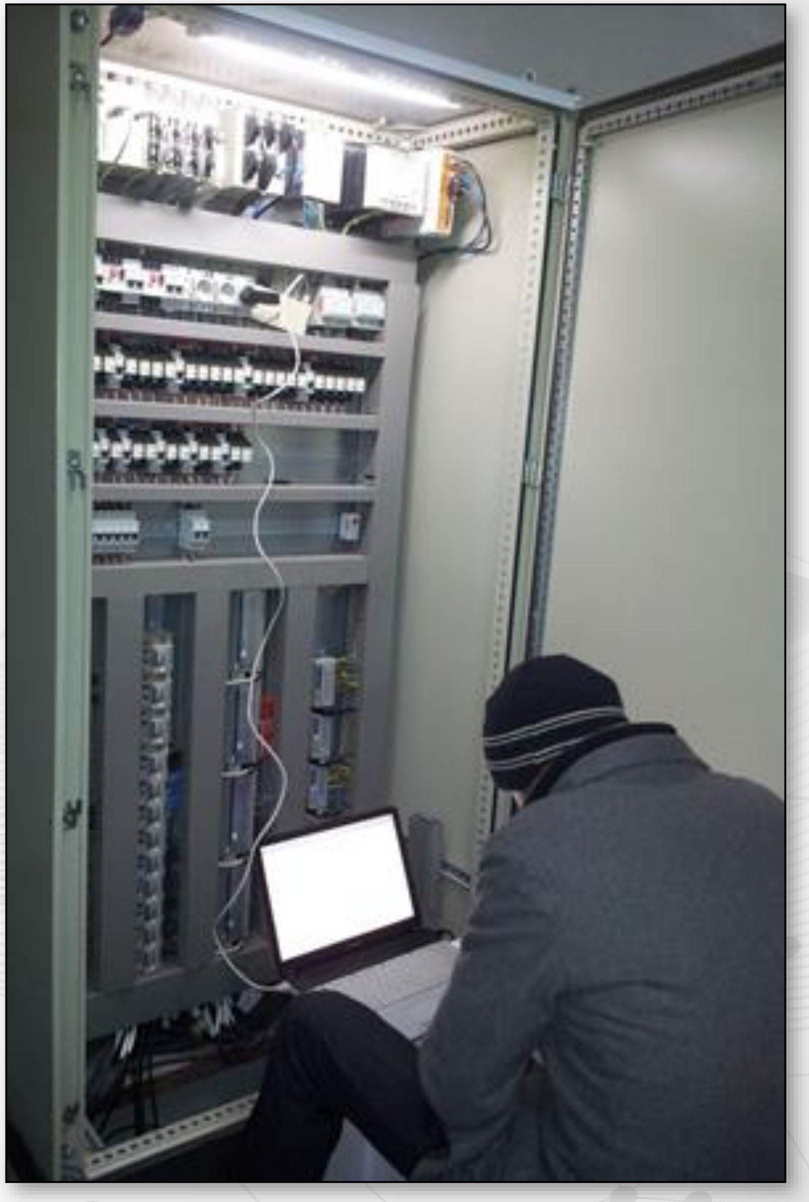
- Critical Infrastructures are high value targets for cyber attacks
- Economic cost globally estimated between 330 and 506 billion € (McAffee)

- Impact:
  - Sabotage / Cyber-Terrorism
  - Information Loss
  - Fraud
  - Blackmail
  - Damage to Reputation
  - Societal / Environmental Impact



Cyber Security Threats to Critical Infrastructures

- Attacks becoming more and more advanced and targeted
- Advanced Persistent Threats (APTs)
  - Executed by professional team
  - Long timeframe
  - Targeted methods (social engineering, spear phishing, etc.)
  - Custom made
- Difficult to detect by traditional security monitoring (IDS, malware detection, etc.)



S2 Managed Cyber Security Services

S2 GRUPO

24x7 Service Centre

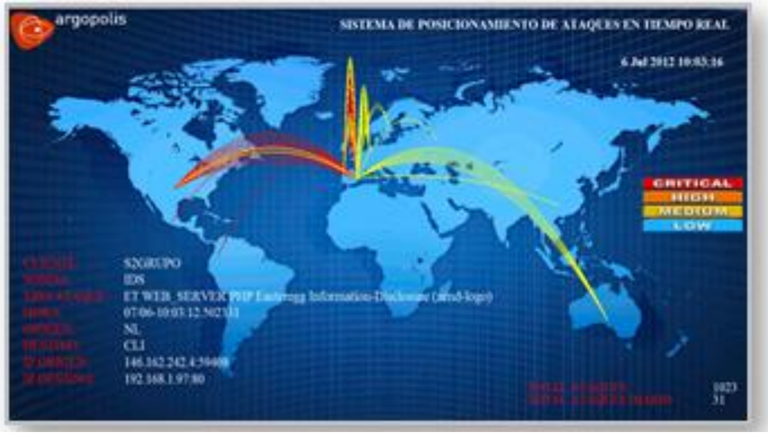
Security Incident Management

Unified monitoring and management of IT and OT installations

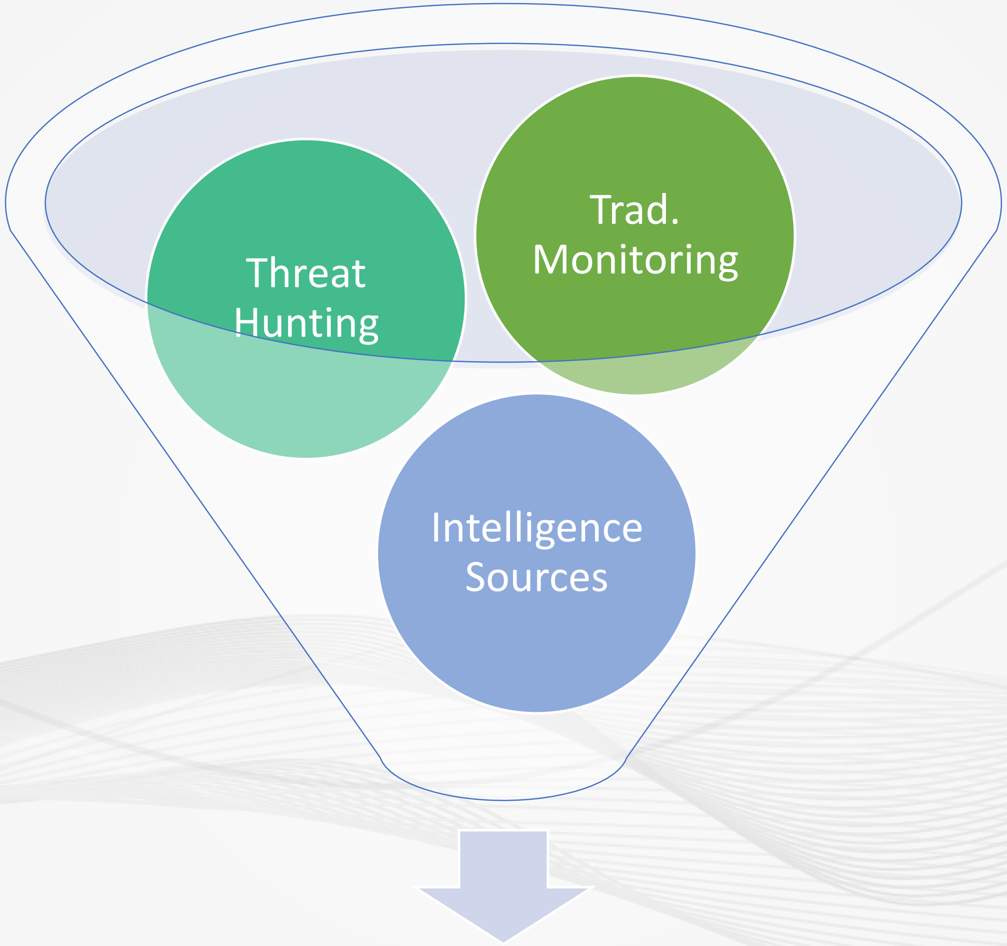
Advanced Threat Hunting Capabilities

iSOC

Industrial Security Operation Center

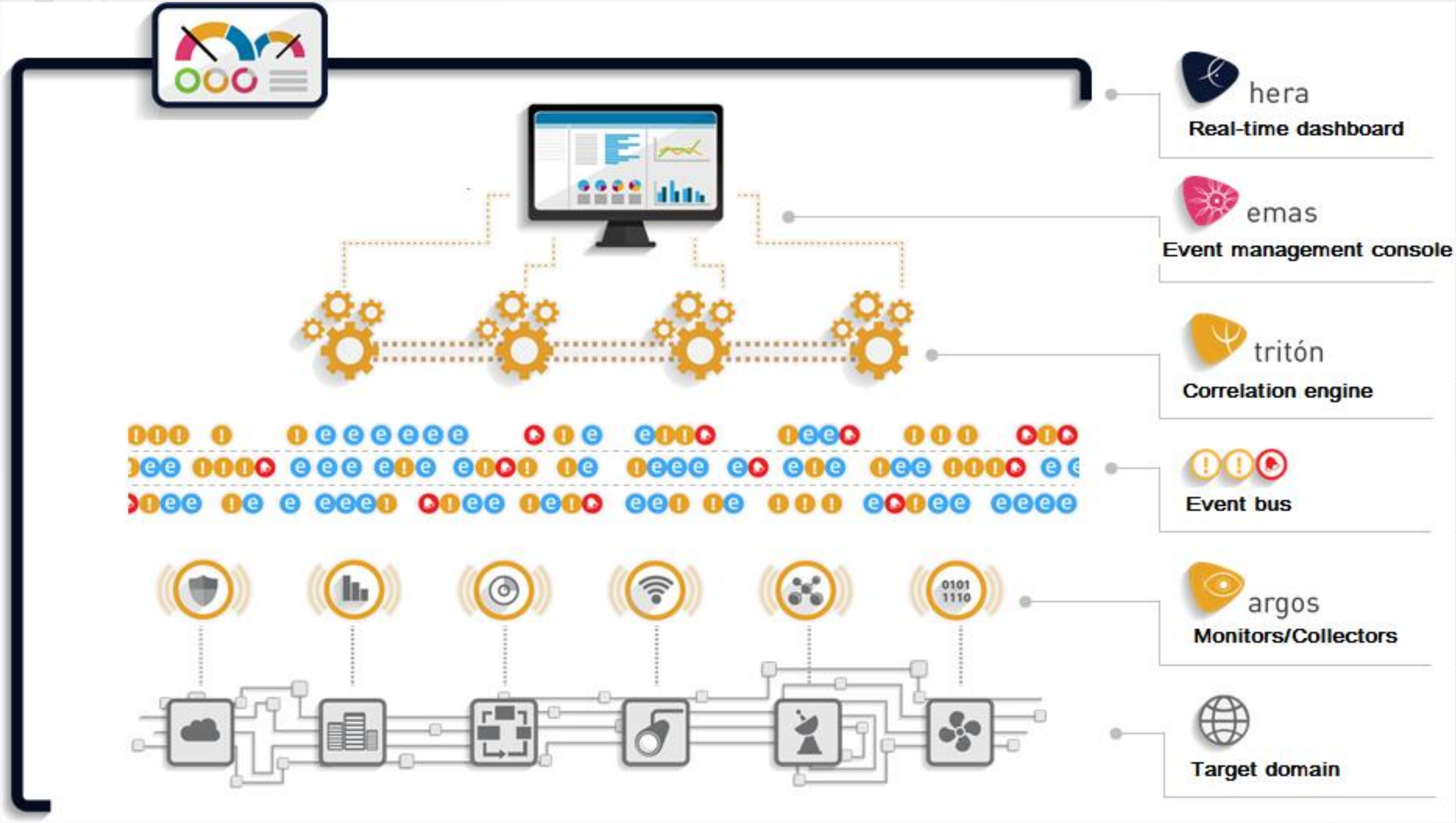


Managed Security Services for CIP

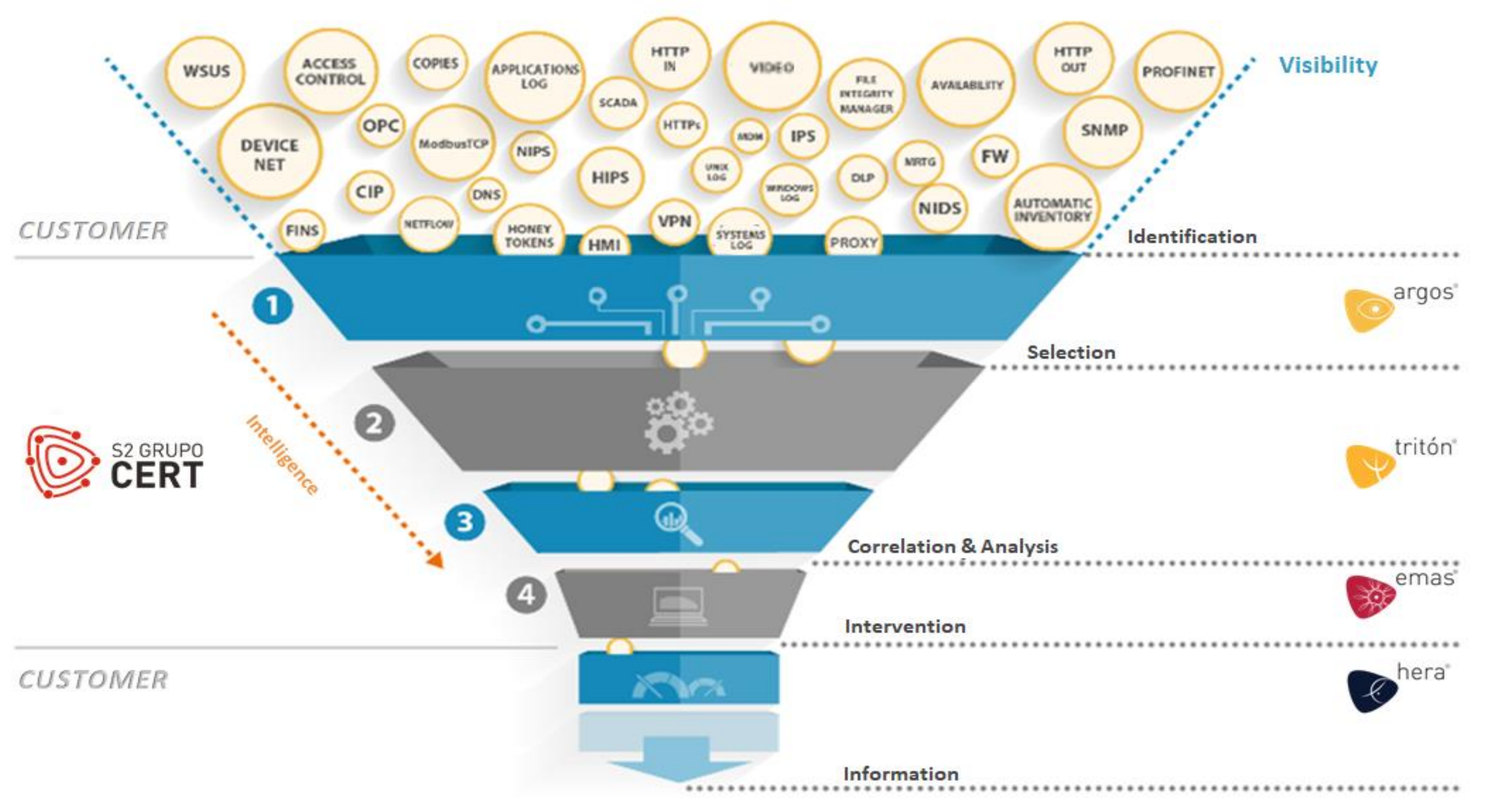


Detection of Advanced Attacks

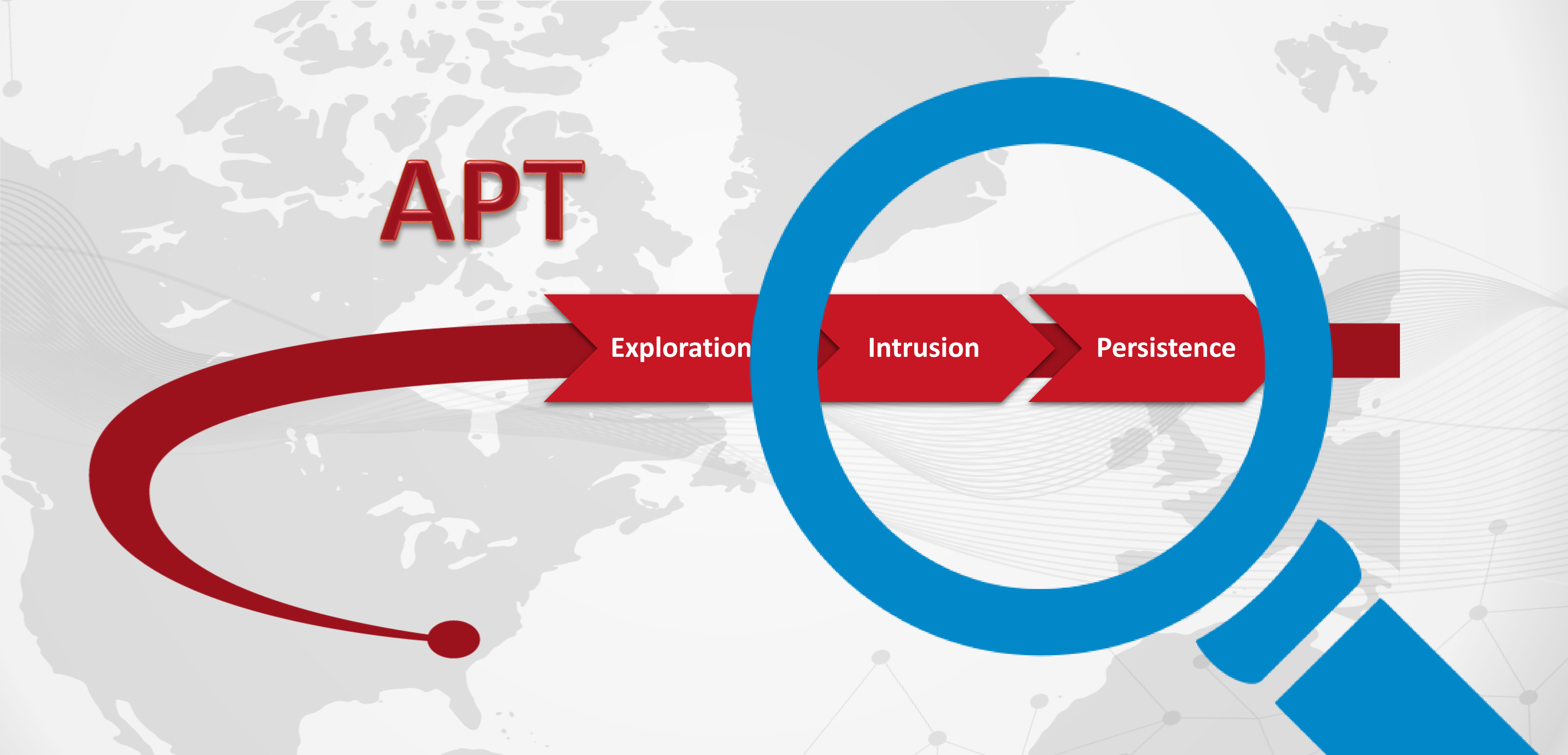
Managed Security Services for CIP – Monitoring



Managed Security Services for CIP – Monitoring



Managed Security Services for CIP – Threat Hunting



Managed Security Services for CIP – Manual Threat Hunting

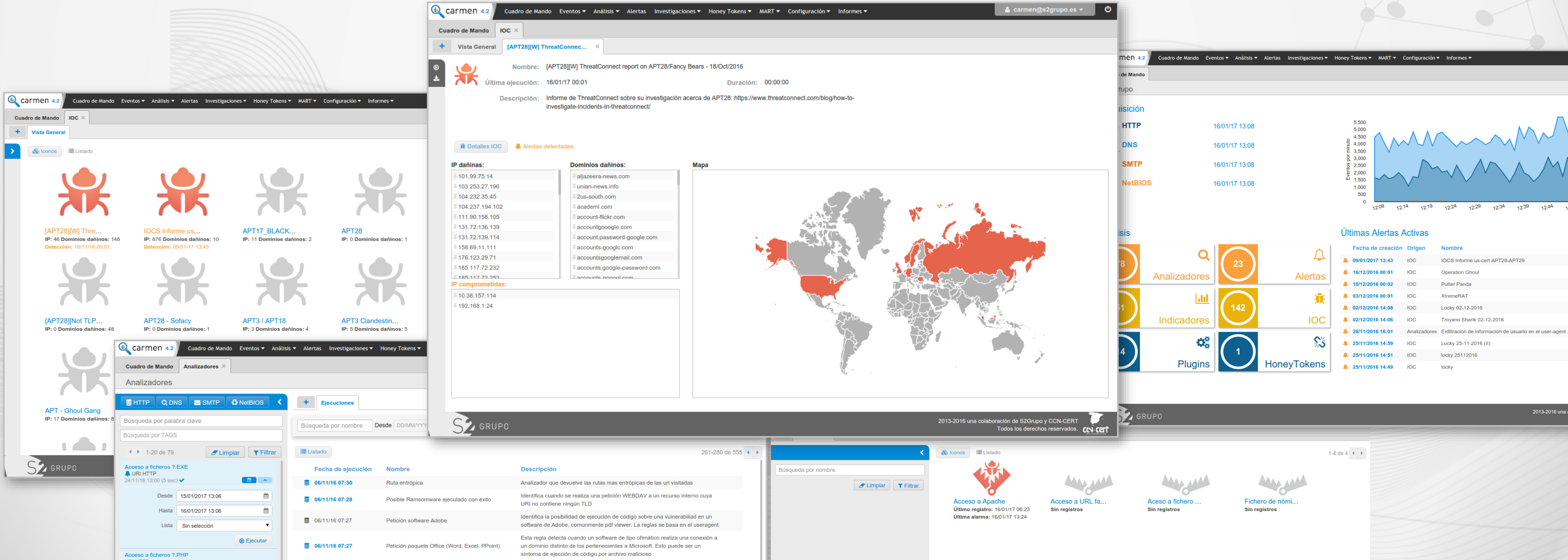
- Experienced Security Analyst tries to find needle in the haystack
- Proactive measures to scan network for anomalies
- Assume system has been infiltrated as some stage
  - Focus on lateral movement
  - Data Exfiltration
- Time consuming
- High level of expertise required

Managed Security Services for CIP – Threat Hunting tool support

carmen

Threat Hunting Platform

Carmen is the European capacity for **APT detection**.
It's objective is to provide the security analysts with a series of tools to **semi-automate Threat Hunting**



[APT28][W] Thre...
IP: 46 Dominios dañinos: 148
Detección: 16/11/16 00:01

IOCS Informe us...
IP: 876 Dominios dañinos: 10
Detección: 09/01/17 13:43

APT17_BLACK...
IP: 11 Dominios dañinos: 2

APT28
IP: 0 Dominios dañinos: 1

[APT28][Not TLP...
IP: 0 Dominios dañinos: 48

APT28 - Sofacy
IP: 0 Dominios dañinos: 1

APT3 / APT18
IP: 3 Dominios dañinos: 4

APT3 Clandestin...
IP: 5 Dominios dañinos: 5

APT - Ghoul Gang
IP: 17 Dominios dañinos: 8

Nombre: [APT28][W] ThreatConnect report on APT28/Fancy Bears - 18/Oct/2016
Última ejecución: 16/01/17 00:01
Duración: 00:00:00
Descripción: Informe de ThreatConnect sobre su investigación acerca de APT28: https://www.threatconnect.com/blog/how-to-investigate-incidents-in-threatconnect/

IP dañinas:
101.99.75.14
103.253.27.196
104.232.35.45
104.237.194.102
111.90.158.105
131.72.136.139
131.72.139.114
158.69.11.111
176.123.29.71
185.117.72.232
185.117.72.253

Dominios dañinos:
aljazeera-news.com
unian-news.info
2us-south.com
academl.com
account-flickr.com
accountgooogle.com
account.password-google.com
accounts-googlc.com
accountsgooglemail.com
accounts.google-password.com
accounts-gooogl.com

IP comprometidas:
10.38.157.114
192.168.1.24

2013-2016 una colaboración de S2Grupo y CCN-CERT
Todos los derechos reservados.

HTTP	16/01/17 13:08
DNS	16/01/17 13:08
SMTP	16/01/17 13:08
NetBIOS	16/01/17 13:08

Analizadores	23 Alertas
Indicadores	142 IOC
Plugins	1 HoneyTokens

Últimas Alertas Activas

Fecha de creación	Origen	Nombre
09/01/2017 13:43	IOC	IOCS Informe us-cert APT28-APT29
16/12/2016 00:01	IOC	Operation Ghoul
10/12/2016 00:02	IOC	Putter Panda
03/12/2016 00:01	IOC	XtremeRAT
02/12/2016 14:08	IOC	Locky 02-12-2016
02/12/2016 14:06	IOC	Troyano Sharik 02-12-2016
28/11/2016 16:01	Analizadores	Exfiltración de información de usuario en el user-agent
25/11/2016 14:59	IOC	Locky 25-11-2016 (II)
25/11/2016 14:51	IOC	locky 25112016
25/11/2016 14:49	IOC	locky

Búsqueda por palabra clave
Búsqueda por TAGS
1-20 de 79

Acceso a ficheros ?.EXE
URI HTTP
24/11/16 13:00 (5 sec) ✓
Desde: 15/01/2017 13:06
Hasta: 16/01/2017 13:06
Lista: Sin selección

Acceso a ficheros ?.PHP

Búsqueda por nombre
Desde: DD/MM/YYY

261-280 de 555

Fecha de ejecución	Nombre	Descripción
06/11/16 07:30	Ruta entrópica	Analizador que devuelve las rutas mas entrópicas de las url visitadas
06/11/16 07:28	Posible Ramsomware ejecutado con éxito	Identifica cuando se realiza una petición WEBDAV a un recurso interno cuya URI no contiene ningún TLD
06/11/16 07:27	Petición software Adobe	Identifica la posibilidad de ejecución de código sobre una vulnerabilidad en un software de Adobe, comunmente pdf viewer. La reglas se basa en el useragent
06/11/16 07:27	Petición paquete Office (Word, Excel, PPoint)	Esta regla detecta cuando un software de tipo ofimático realiza una conexión a un dominio distinto de los pertenecientes a Microsoft. Esto puede ser un síntoma de ejección de código por archivo malicioso

Búsqueda por nombre
1-4 de 4

Acceso a Apache
Último registro: 16/01/17 06:23
Última alarma: 16/01/17 13:24

Acceso a URL fa...
Sin registros

Aceso a fichero ...
Sin registros

Fichero de nómi...
Sin registros

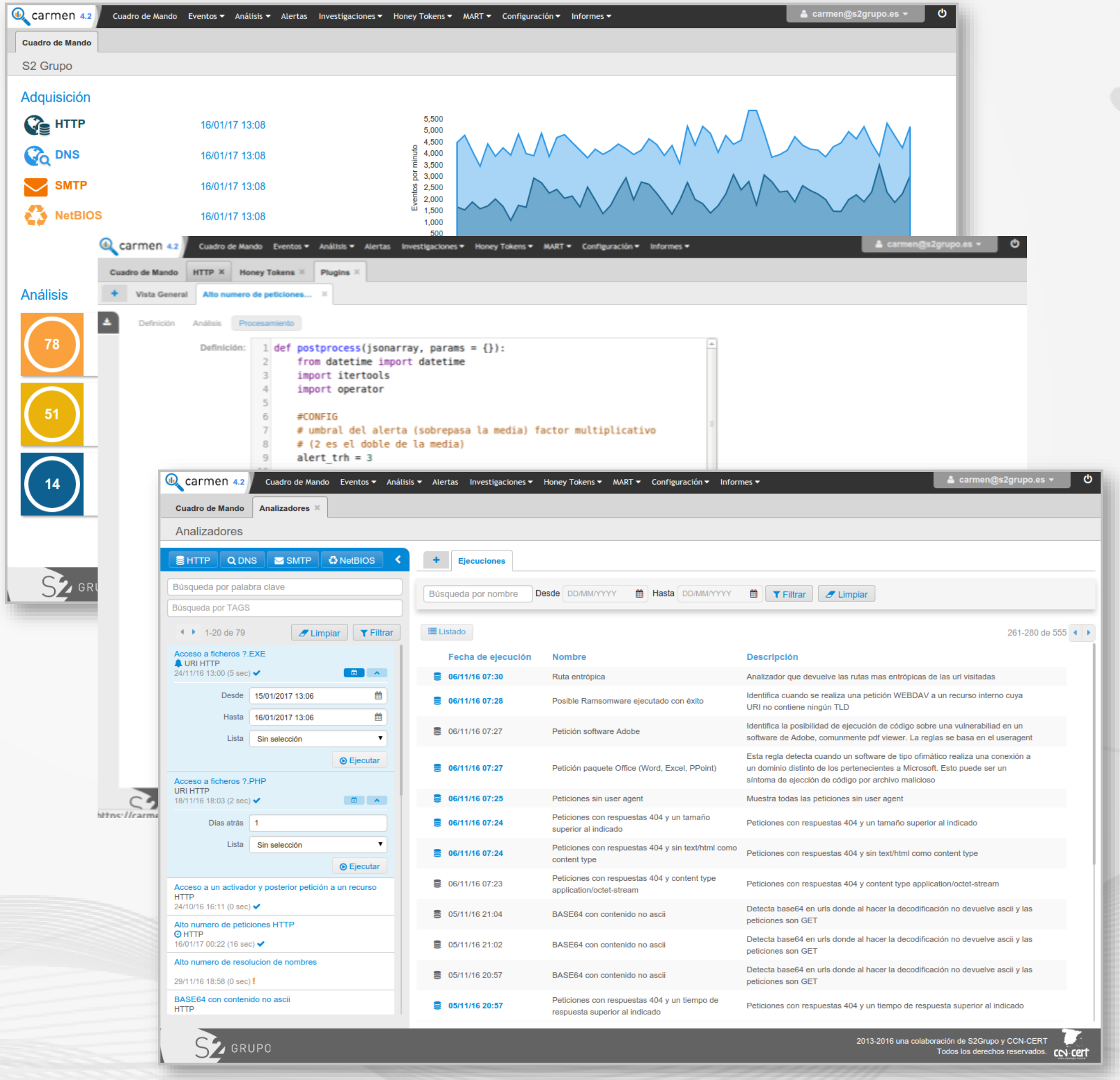
2013-2016 una

Managed Security Services for CIP – Threat Hunting tool support

carmen

To support **Threat Hunting**, carmen work in various areas:

- **Detection of improper use (b/w/g listing, IOC, honeytokens)**
- **Behavioral Analysis**
- **Anomaly Detection**
  - **Statistical Anomalies**
  - **User behavior anomalies**
  - **Time series anomalies**
  - **Knowledge based anomaly detection**
  - **URL anomalies**



HTTP	16/01/17 13:08
DNS	16/01/17 13:08
SMTP	16/01/17 13:08
NetBIOS	16/01/17 13:08

Definición:

```
def postprocess(jsonarray, params = {}):
    from datetime import datetime
    import itertools
    import operator

    #CONFIG
    # umbral del alerta (sobrepasa la media) factor multiplicativo
    # (2 es el doble de la media)
    alert_trh = 3
```

HTTP | DNS | SMTP | NetBIOS

Búsqueda por palabra clave

Búsqueda por TAGS

1-20 de 79

Acceso a ficheros ?.EXE
URI HTTP
24/11/16 13:00 (5 sec) ✓

Desde 15/01/2017 13:06
Hasta 16/01/2017 13:06
Lista Sin selección

Acceso a ficheros ?.PHP
URI HTTP
18/11/16 18:03 (2 sec) ✓

Días atrás 1
Lista Sin selección

Acceso a un activador y posterior petición a un recurso
HTTP
24/10/16 16:11 (0 sec) ✓

Alto numero de peticiones HTTP
HTTP
16/01/17 00:22 (16 sec) ✓

Alto numero de resolucion de nombres
29/11/16 18:58 (0 sec) !

BASE64 con contenido no ascii
HTTP

Búsqueda por nombre Desde DD/MM/YYYY Hasta DD/MM/YYYY

261-280 de 555

Fecha de ejecución	Nombre	Descripción
06/11/16 07:30	Ruta entrópica	Analizador que devuelve las rutas mas entrópicas de las url visitadas
06/11/16 07:28	Posible Ramsomware ejecutado con éxito	Identifica cuando se realiza una petición WEBDAV a un recurso interno cuya URI no contiene ningún TLD
06/11/16 07:27	Petición software Adobe	Identifica la posibilidad de ejecución de código sobre una vulnerabiliad en un software de Adobe, comunmente pdf viewer. La reglas se basa en el useragent
06/11/16 07:27	Petición paquete Office (Word, Excel, PPoint)	Esta regla detecta cuando un software de tipo ofimático realiza una conexión a un dominio distinto de los pertenecientes a Microsoft. Esto puede ser un síntoma de ejección de código por archivo malicioso
06/11/16 07:25	Peticiones sin user agent	Muestra todas las peticiones sin user agent
06/11/16 07:24	Peticiones con respuestas 404 y un tamaño superior al indicado	Peticiones con respuestas 404 y un tamaño superior al indicado
06/11/16 07:24	Peticiones con respuestas 404 y sin text/html como content type	Peticiones con respuestas 404 y sin text/html como content type
06/11/16 07:23	Peticiones con respuestas 404 y content type application/octet-stream	Peticiones con respuestas 404 y content type application/octet-stream
05/11/16 21:04	BASE64 con contenido no ascii	Detecta base64 en urls donde al hacer la decodificación no devuelve ascii y las peticiones son GET
05/11/16 21:02	BASE64 con contenido no ascii	Detecta base64 en urls donde al hacer la decodificación no devuelve ascii y las peticiones son GET
05/11/16 20:57	BASE64 con contenido no ascii	Detecta base64 en urls donde al hacer la decodificación no devuelve ascii y las peticiones son GET
05/11/16 20:57	Peticiones con respuestas 404 y un tiempo de respuesta superior al indicado	Peticiones con respuestas 404 y un tiempo de respuesta superior al indicado

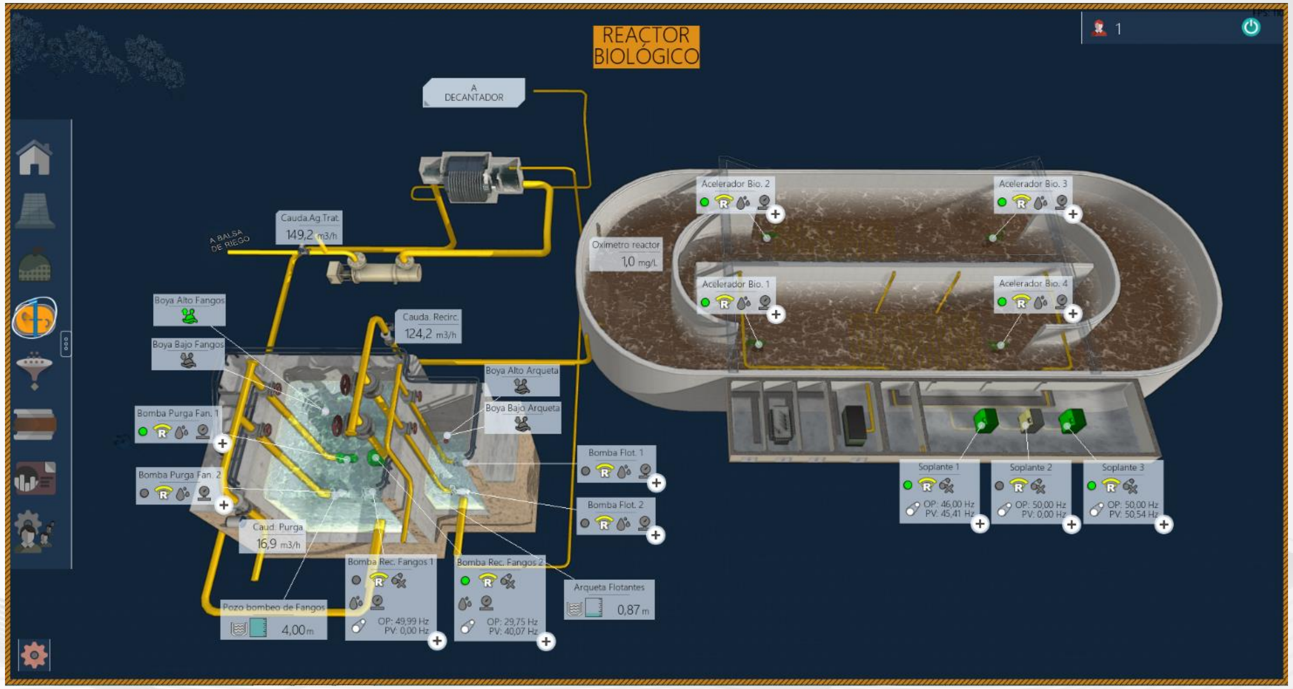
2013-2016 una colaboración de S2Grupo y CCN-CERT
Todos los derechos reservados.

Managed Security Services for CIP – Threat Hunting with AI

- Focus on Industrial Control Traffic in CI
  - Deterministic
  - Repetitive
- Deep Packet Inspection to detect Anomalies
  - Train system to model normality → signatures
  - Unobserved signature == anomaly
  - Inverse Malware detection
- Packet Sequence Analysis
  - Model normality with LSTM Neural networks
  - Predict probability of next packet

The importance of Intelligence

- Intelligence on attacks, suspicious IPs, IDS signatures, etc.
- Open Source Intelligence
- Commercial Intelligence Feeds
- Own Intelligence
  - Network of intelligence exchange between different tool deployments
  - Honeypots


REACTOR BIOLÓGICO
1
A DECANTADOR
A BALSA DE RIEGO
Cauda.Ag.Trat
149,2 m3/h
Cauda. Recirc.
124,2 m3/h
Oximetro reactor
1,0 mg/L
Boya Alto Fangos
Boya Bajo Fangos
Boya Alto Arqueta
Boya Bajo Arqueta
Bomba Purga Fan. 1
Bomba Purga Fan. 2
Caud. Purga
16,9 m3/h
Pozo bombeo de Fangos
4,00 m
Bomba Rec. Fangos 1
OP: 49,99 Hz
PV: 0,00 Hz
Bomba Rec. Fangos 2
OP: 29,75 Hz
PV: 40,07 Hz
Bomba Flot. 1
Bomba Flot. 2
Arqueta Flotantes
0,87 m
Acelerador Bio. 2
Acelerador Bio. 3
Acelerador Bio. 1
Acelerador Bio. 4
Soplante 1
OP: 46,00 Hz
PV: 45,41 Hz
Soplante 2
OP: 50,00 Hz
PV: 0,00 Hz
Soplante 3
OP: 50,00 Hz
PV: 50,54 Hz