Cyber Situational Awareness

Retos e iniciativas

Comandante Mónica Mateos Calle

Mando Conjunto de Ciberdefensa.

Jefatura de Simulación ,Auditorias y Desarrollo.

Grupo de Tecnologías

Monica.mateos@et.mde.es

Índice

Visión de Cyber Situational Awareness

- **Definición de "Situation Awareness"**
  - ✓ Percepción de los elementos en el entorno dentro de un volumen temporal y espacial, la comprensión de su significado y la proyección de su estado en un futuro próximo.

    Endsley, M. R., Toward a theory of situation awareness in dynamic systems. Human Factors, 37(1) :32-64, March, 1995.

- **Cyber Situational Awareness**
  - ✓ Conocimiento de la situación sobre la parte del ciberespacio que pueda afectar a las áreas de interés.

TOMA DE DECISIONES

Aplicación de CySA en Ciberdefensa

Fuentes de Información CySA

Gestión de Activos
- Descubrimiento
- Estado / eventos
- Dependencias
- Criticidad…

Información sobre Activos Ajenos

ACTIVOS

Análisis de Vulnerabilidades

Valoración de Vulnerabilidades

VULNERABILIDADES

Análisis de Amenazas

Gestión de Incidentes

AMENAZAS E INCIDENTES

Defensa
- Prevención
- Detección
- Reacción
- Recuperación

Explotación

Respuesta

MEDIDAS DE CIBERDEFENSA

CYBER SITUATIONAL AWARENESS

VISUALIZACIÓN

Iniciativas para la obtención de la capacidad CySA en el MCCD

Iniciativas

Convenio entre el MDEF y la Universidad Politécnica de Madrid

Desarrollo de una Herramienta de visualización y trazado de un ciberataque

Proyectos con EDA

CySAP: Cyber Situational Awareness Package

Programa COINCIDENTE (DGAM)

CyCOP: Cyber Common Operational Picture

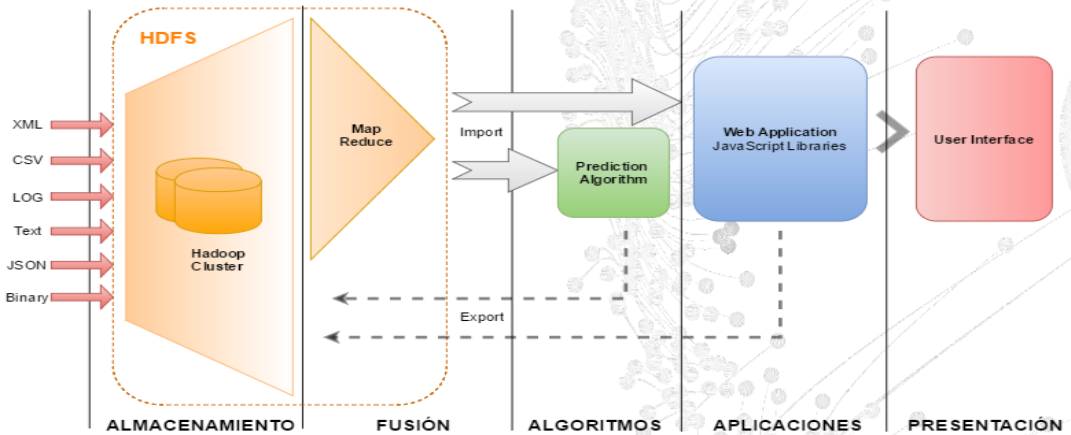
Iniciativas

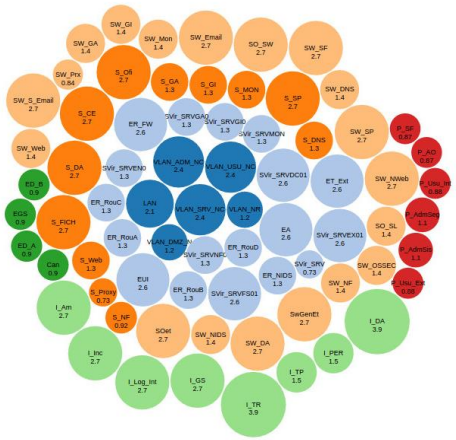
I+D+i: Desarrollo de una Herramienta de visualización y trazado de un ciberataque

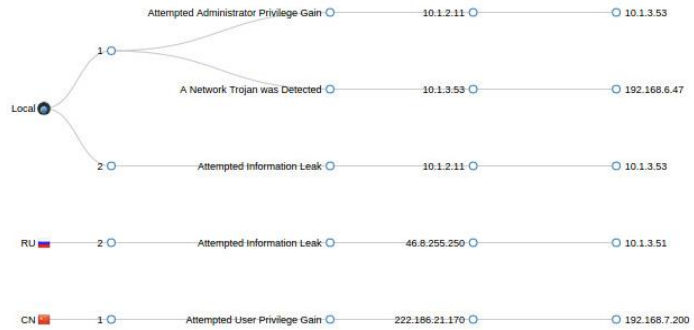
- Desarrollo de una herramienta que permita **visualizar** y **trazar** un ciberataque.
- Determinar probabilísticamente su **evolución**, basado en **aprendizaje** (técnicas Machine Learning) sobre datos existentes.
- Mostrará:
  - ✓ Nivel y Características del **Compromiso**
  - ✓ **Técnicas** utilizadas y origen potencial del ataque
  - ✓ Distintas capas de **visualización**

Iniciativas

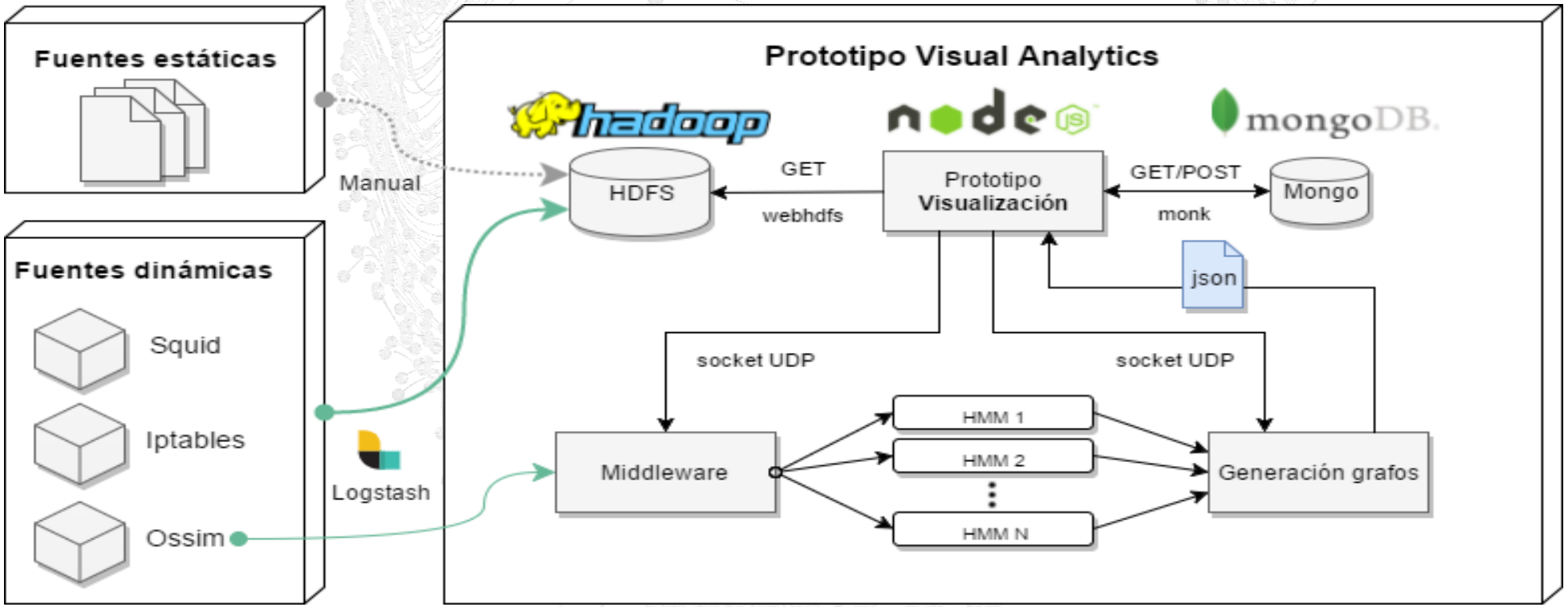
I+D+i: Desarrollo de una Herramienta de visualización y trazado de un ciberataque







I+D+i: Desarrollo de una Herramienta de visualización y trazado de un ciberataque



Iniciativas

I+D+i: CySAP: Cyber Situational Awareness Package (CySAP - EDA)

- **Objetivo**: *"The objective is for commanders and other decision-makers to have a clear understanding of the threat landscape and to equip them with the tools (competent personnel, effective procedures and technology platforms) to manage risks during the planning and conduct phases of an operation."*

- Obtención completa de la **capacidad de CySA** enfocada a los sistemas de ciberdefensa, que sea capaz de integrar en tiempo real datos múltiples fuentes, analizarlos y presentar información precisa y comprensible que sirva como apoyo a la toma de decisión en cada misión.

- Diseño, desarrollo e integración de diferentes módulos y funcionalidades, entre los que destacan **Análisis de Riesgos Dinámico** y **Apoyo a la toma de decisión**.

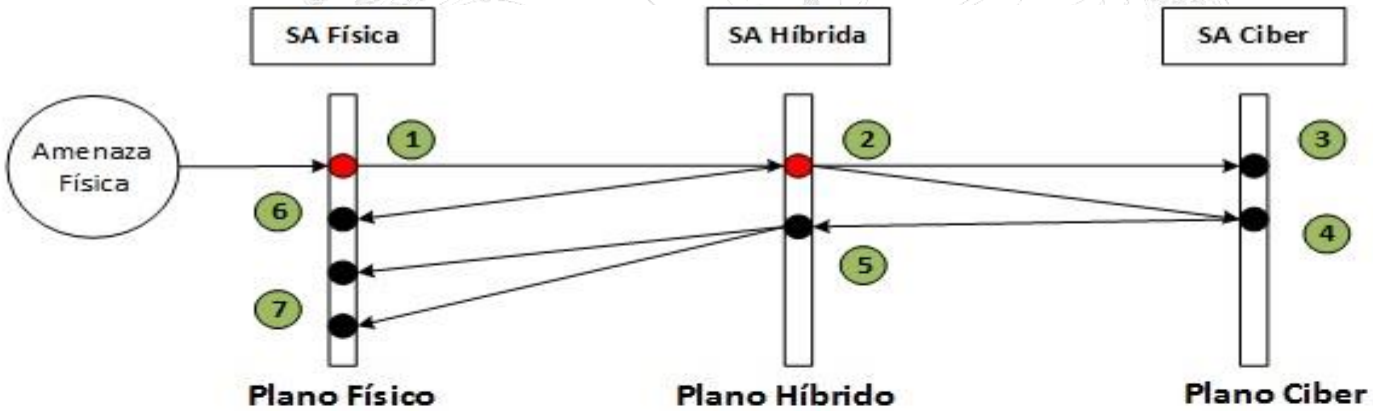
- Consorcio Multinacional de empresas .

Iniciativas

I+D+i: CyCOP (Cyber Common Operational Picture)

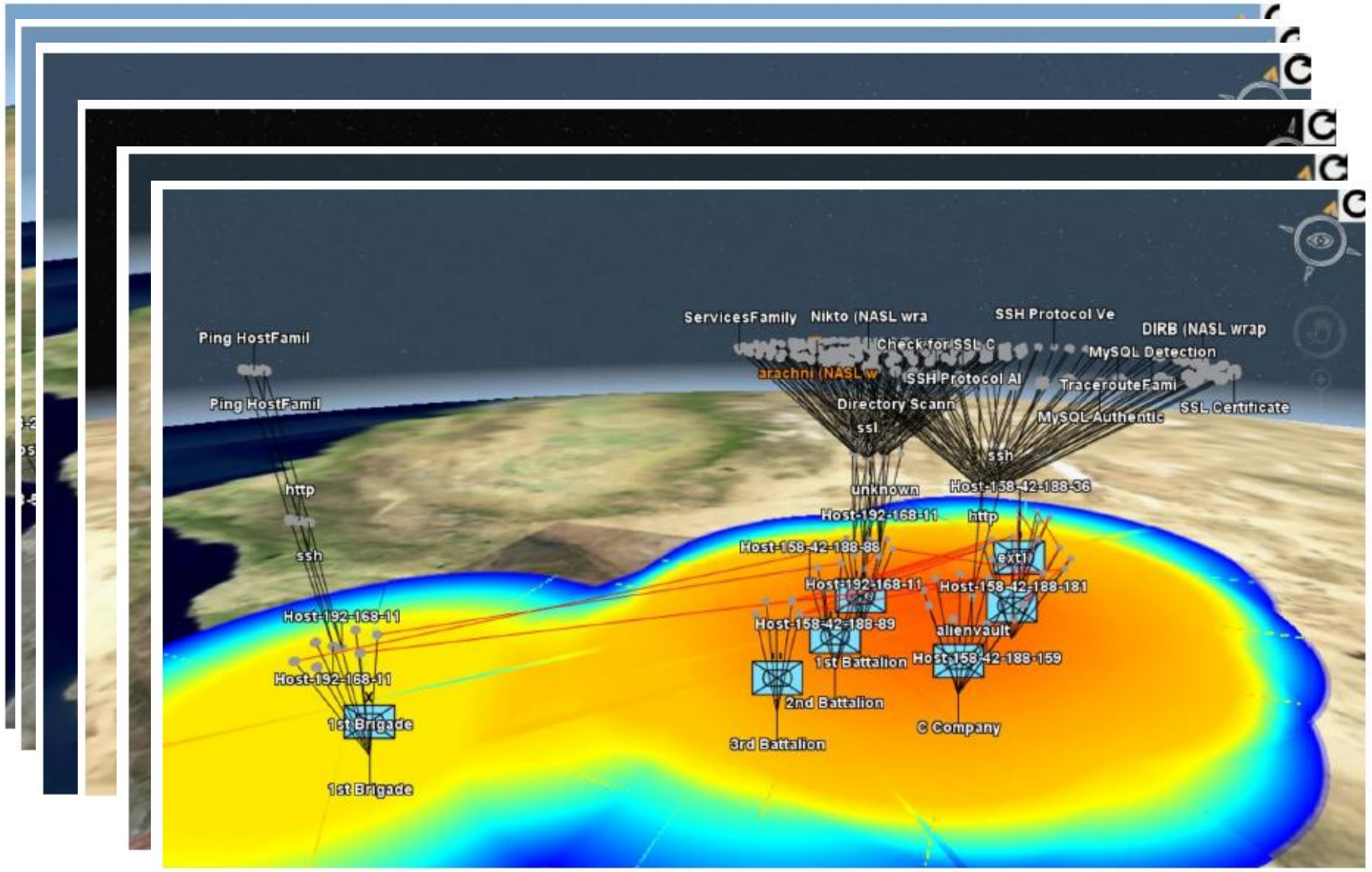
- **Proyecto realizado en el marco de programa COINCIDENTE (MINISDEF – DGAM) por la Universidad Politécnica de Valencia.**
- Desarrollo de una **COP híbrida** entre el mundo físico y el ciberespacio
- **Percepción conjunta** de la situación en el ámbito de tierra, mar, aire y ciberespacio como un único “campo de batalla integrado”

CyCOP

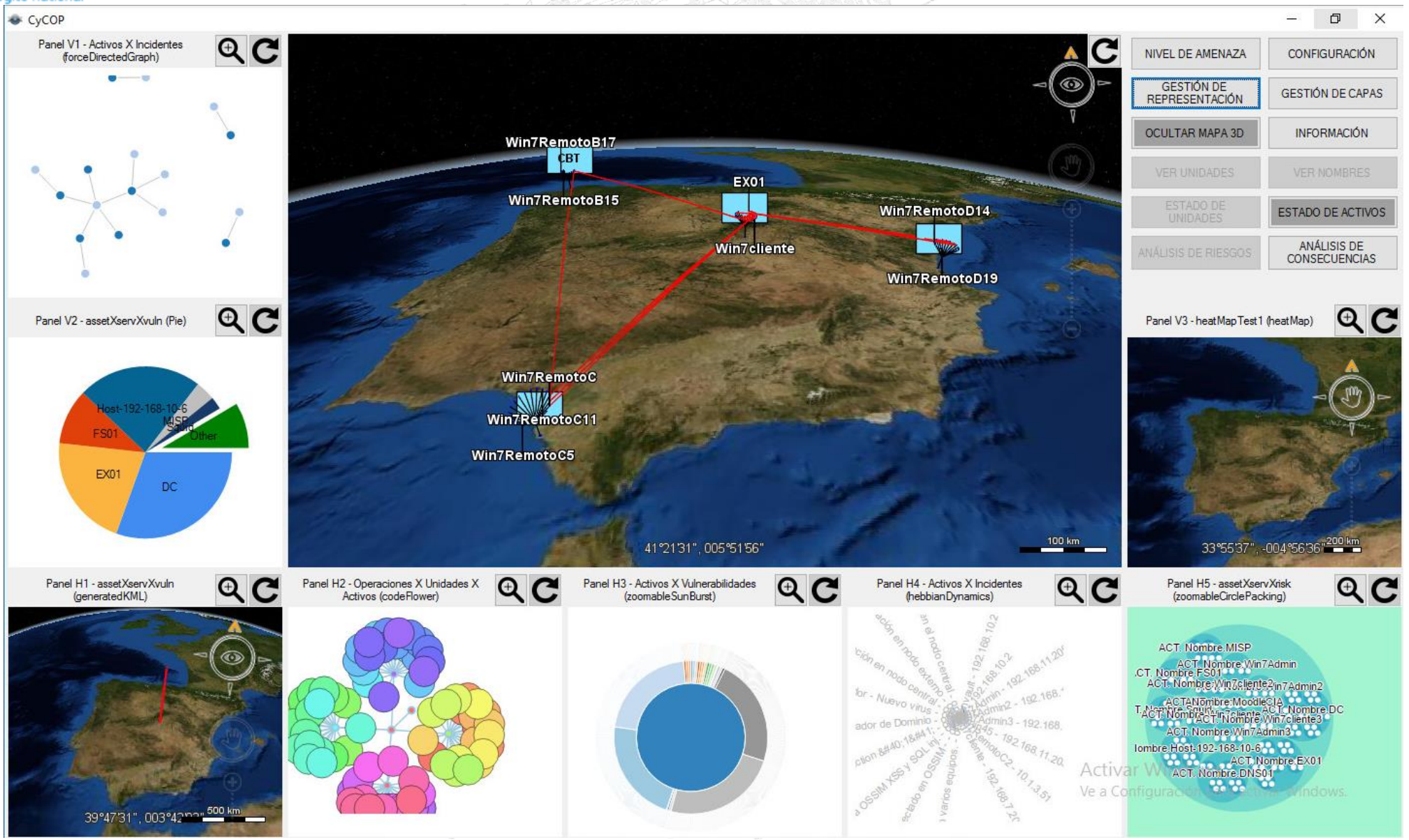


1. Amenaza física detectada y visualizada en la aplicación de SA
2. Amenaza física detectada y visualizada en la aplicación de SA Híbrida
3. Amenaza potencial en el plano cyber como consecuencia de la amenaza física detectada sin consecuencias posteriores en el plano físico
4. Amenaza potencial en el plano cyber como consecuencia de la amenaza física detectada con consecuencias potenciales posteriores en el plano físico
5. Amenaza potencial en el plano cyber como consecuencia de la amenaza física detectada con consecuencias potenciales posteriores en el plano físico visualizada en la aplicación de SA Híbrida
6. Amenaza potencial en el plano físico como directa consecuencia de la amenaza física detectada
7. Amenazas potenciales en el plano físico como consecuencia de las amenazas potenciales cyber (Efecto cascada) visualizadas en el la aplicación de SA Física

CyCOP


ServicesFamily
Nikto (NASL wra
SSH Protocol Ve
DIRB (NASL wrap
Ping HostFamil
Check for SSL C
MySQL Detection
arachni (NASL w
SSH Protocol Al
TracerouteFami
Ping HostFamil
Directory Scann
MySQL Authentic
SSL Certificate
ssl
ssh
http
unknown
Host-138-42-188-36
Host-192-168-11
http
Host-158-42-188-98
ssh
ext1
Host-192-168-11
Host-158-42-188-181
Host-192-168-11
Host-158-42-188-89
alienvault
1st Battalion
Host-158-42-188-159
2nd Battalion
1st Brigade
C Company
3rd Battalion
1st Brigade

CyCOP


CyCOP
Panel V1 - Activos X Incidentes (forceDirectedGraph)
Panel V2 - assetXservXvuln (Pie)
Host-192-168-10-6
MISP
FS01
Other
EX01
DC
Win7RemotoB17
CBT
Win7RemotoB15
EX01
Win7RemotoD14
Win7cliente
Win7RemotoD19
Win7RemotoC
Win7RemotoC11
Win7RemotoC5
41°21'31", 005°51'56"
100 km
NIVEL DE AMENAZA
CONFIGURACIÓN
GESTIÓN DE REPRESENTACIÓN
GESTIÓN DE CAPAS
OCULTAR MAPA 3D
INFORMACIÓN
VER UNIDADES
VER NOMBRES
ESTADO DE UNIDADES
ESTADO DE ACTIVOS
ANÁLISIS DE RIESGOS
ANÁLISIS DE CONSECUENCIAS
Panel V3 - heatMapTest1 (heatMap)
33°55'37", -004°56'36"
200 km
Panel H1 - assetXservXvuln (generatedKML)
39°47'31"
500 km
Panel H2 - Operaciones X Unidades X Activos (codeFlower)
Panel H3 - Activos X Vulnerabilidades (zoomableSunBurst)
Panel H4 - Activos X Incidentes (hebbianDynamics)
Panel H5 - assetXservXrisk (zoomableCirclePacking)
ACT. Nombre:MISP
ACT. Nombre:Win7Admin
ACT. Nombre:FS01
ACT. Nombre:Win7cliente2
ACT. Nombre:Win7Admin2
ACT. Nombre:ModeloCIA
ACT. Nombre:DC
ACT. Nombre:Win7cliente3
ACT. Nombre:Win7Admin3
ACT. Nombre:Host-192-168-10-6
ACT. Nombre:EX01
ACT. Nombre:DNS01

Conclusiones

- Las soluciones de CYSA deben ser capaces de recoger y procesar gran volumen de datos y con origenes y formatos muy heterogéneos por lo que las aproximaciones basadas big data y tecnicas machine learning parecen ser mas adecuadas.
- La presentacion y visualización de la informacion que configure la CYSA debe ser:
  - clara y relevante
  - debe satisfacer a cada uno de los niveles (estratégico, operacional y táctico)
  - Debe reflejar los cambios en tiempo cuas real para obtener el escenario mas veráz en todo momento
  - Adecuada al tipo de operación que se está realizado
  - Disponible tanto en el planeamiento como en la conducción de operaciones
- Se han dado grandes pasos en el desarrollo de la consciencia situacional integrada, pero el camino todavía es muy largo y el tiempo apremia. Todas las iniciativas en este campo son bienvenidas.

E-Mails

- info@ccn-cert.cni.es
- ccn@cni.es
- sat-inet@ccn-cert.cni.es
- sat-sara@ccn-cert.cni.es
- organismo.certificacion@cni.es

Websites

- www.ccn.cni.es
- www.ccn-cert.cni.es
- www.oc.ccn.cni.es

Síguenos en