Newsletter

January 2019

Welcome to the second SAURON project newsletter. SAURON was funded in the H2020 SEC-2016 call under the topic CIP-01-2016-2017: Prevention, detection, response and mitigation of the combination of physical and cyber threats to the critical infrastructure of Europe. This second newsletter presents to the general public the innovative visualization techniques proposed by the project for enhancing the Situation Awareness (SA) of the cyber security analysts.

SAURON INNOVATIVE VISUALIZATION TECHNIQUES

The innovation and increasing the current ports cyber security is one of the main objectives of SAURON project and therefore several developments have been performed for this purpose.

In T4.3 and T4.4 the whole pack of the innovative cyber security features that form the Cyber Situation Awareness application (CSA) have been developed. In addition, in T4.2, which results are summarized in this newsletter, the new advanced visualization techniques that will help the ports cyber security analysts to perform their work in a more efficient manner has been developed.

In the following sections, the innovative views of the cyber space that SAURON offers to the cyber security analyst and the data sets to be shown through the advanced visualization techniques implemented in the CSA HMI are described in detail.

Through the CSA advanced HMI design SAURON offers to the cyber security analyst new tools and views for increasing their SA and speed up the threat evaluation process and therefore increasing the ports resilience to cyber-attacks.

On the other hand, the CSA HMI design cover all the CSA HMI requirements stated in Deliverable 3.3. The explanation of the requirements coverage is detailed in Deliverable 4.2 where the main HMI functionalities and features are described in detail.

The advanced CSA HMI design goes beyond the current state of the art (current cyber security HMIs only show lines of text explaining the threat/attack nature). This new approach offers to cyber security analyst a visual view of the cyber space and linking it with the physical domain adding accurate geo-location information.

The central frame of the CSA HMI shows a geo-located view of all cyber assets stated in the data port model. This visualization type allows to see in a quick view all cyber assets and their connections including their current status through a colour code (e.g. all assets non compromised/attacked are described in blue colour and a compromised/attacked asset is described in red colour).

An example on this advanced visualization feature showing all cyber assets of Valencia port network in a normal status (Blue colour) and one cyber asset compromised (Red colour) is described in figure 1.

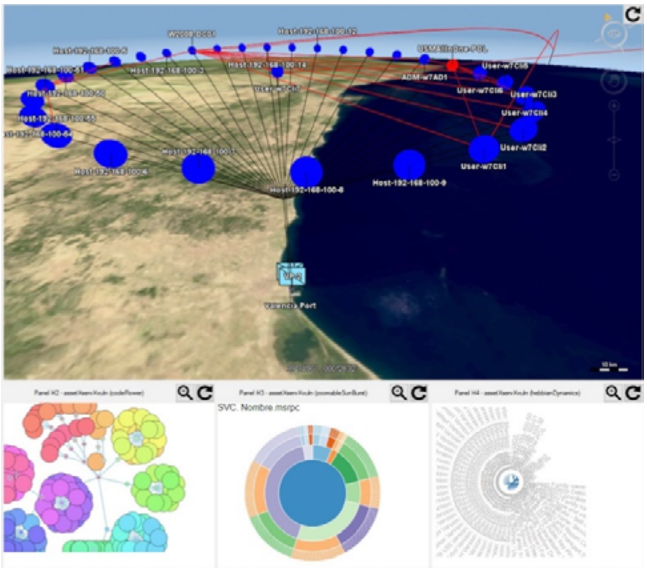


Figure 1| Valencia port network model stating one cyber asset compromised

Once this alarm is detected the cyber security analyst zoom the affected asset and click on it in order to know all information available on the asset and it status. In figure 2 can be seen the affected asset selected by the cyber security analyst and the information window that appears on click.

The information window of each cyber asset includes information of different fields such as assets details, known asset vulnerabilities, Alarms detected, past incidents of this asset, risks and threats for the asset. In figure 3 the detail of the asset information window is described (see red circle).

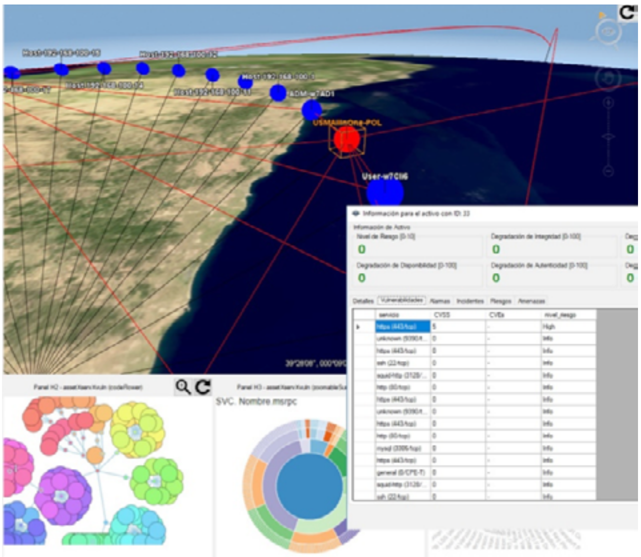
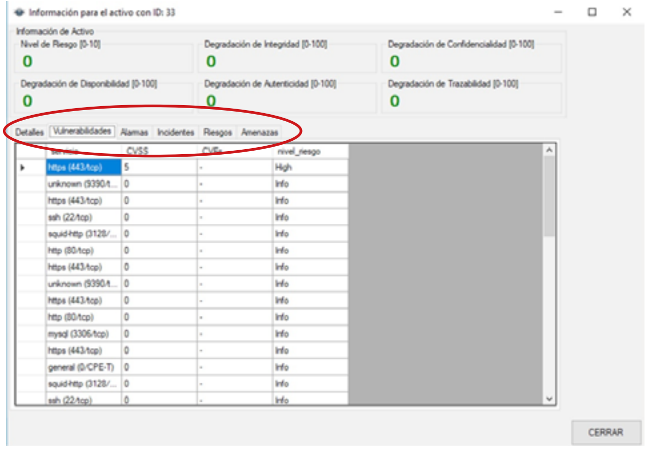


Figure 2| Affected asset selection and associated information

In this figure the vulnerability tap of the affected asset is selected showing all vulnerabilities known for this cyber asset.



Información para el activo con ID: 33

Información de Activo

Nivel de Riesgo [0-10] 0	Degradación de Integridad [0-100] 0	Degradación de Confidencialidad [0-100] 0
Degradación de Disponibilidad [0-100] 0	Degradación de Autenticidad [0-100] 0	Degradación de Trazabilidad [0-100] 0

Detalles | Vulnerabilidades | Alarmas | Incidentes | Riesgos | Amenazas

servicio	CVSS	CVEs	nivel_riesgo
https (443/tcp)	5	-	High
unknown (9390/t...	0	-	Info
https (443/tcp)	0	-	Info
ssh (22/tcp)	0	-	Info
squid-http (3128/...	0	-	Info
http (80/tcp)	0	-	Info
https (443/tcp)	0	-	Info
unknown (9390/t...	0	-	Info
https (443/tcp)	0	-	Info
http (80/tcp)	0	-	Info
mysql (3306/tcp)	0	-	Info
https (443/tcp)	0	-	Info
general (0/CPE-T)	0	-	Info
squid-http (3128/...	0	-	Info
ssh (22/tcp)	0	-	Info

Figure 3| Information window of the affected asset

The information columns in the red circle are: Details, Vulnerabilities, Alarms, Incidents, Risks and Threats. Regarding the classification of the alarm/attack type detected, the consortium has decided to follow the ICT security guide CCN-STIC 817[1] of the Spanish National Security Framework. Cyber-Incident Management provided by the National Cryptologic Centre [2].

This guide stated seven main categories of cyber events: Intrusions, Fraud, Abusive content, Information compromised, Malware, Security policy and Information gathering. Each of these main categories include different incidents/attacks, which allows to show to the cyber security analyst a more accurate information in real time.

In addition, the consortium has added other important information associated to the alarm/attack detected such us the IP and country of the attacker in case of outbound attack or the asset IP in case of inbound attack.

[1] https://www.ccn-cert.cni.es/en/series-ccn-stic/800-guia-esquema-nacional-de-seguridad/ 2025-ccn-stic-817-national-security-framework-cyber-incident-management/file.html

[2] https://www.ccn-cert.cni.es/

ADDITIONAL ADVANCED VISUALIZATION FEATURES DEVELOPED

In this section the main additional visualization features developed for completing the CSA advanced HMI are described in detail. These features will be new visualization tools which will increase the ports cyber security analyst SA, providing them a multidimensional HMI capable of offering new perspectives of the cyber space.

IMMERSIVE TECHNOLOGIES

As one of the more innovative and advanced visualization features that SAURON brings to the cyber security domain is the use of immersive interfaces such as OCULUS Rift CV1.

Through this kind of immersive interface, the cyber security analyst can have a different view of the network and also to check the different connections and characteristics of a determinate asset in the middle of a complex network in a visual manner.

In case of very large networks the analyst can enter inside the network represented in a 3D environment and look for additional information and topology details that could be very difficult to find in a 2D environment in a normal screen even with 3D representations.

It is difficult to show in this document the new perspectives that this kind of immersive interfaces offering to the cyber security analyst. Nevertheless, figures 4 and 5 give an idea on how this new manner of visualizing networks looks like. In figure 4 a multi-node network is shown from a top view which makes difficult to analyse the network nodes and their connection.

The analyst has the possibility of entering virtually inside the network in order to check easily nodes characteristics, vulnerabilities, risks and so on. This 3D view of the network is described in figure 5.

It is important to note that this advanced visualization feature will be able to be tested during the review meetings and also during the project pilots' demonstration execution.

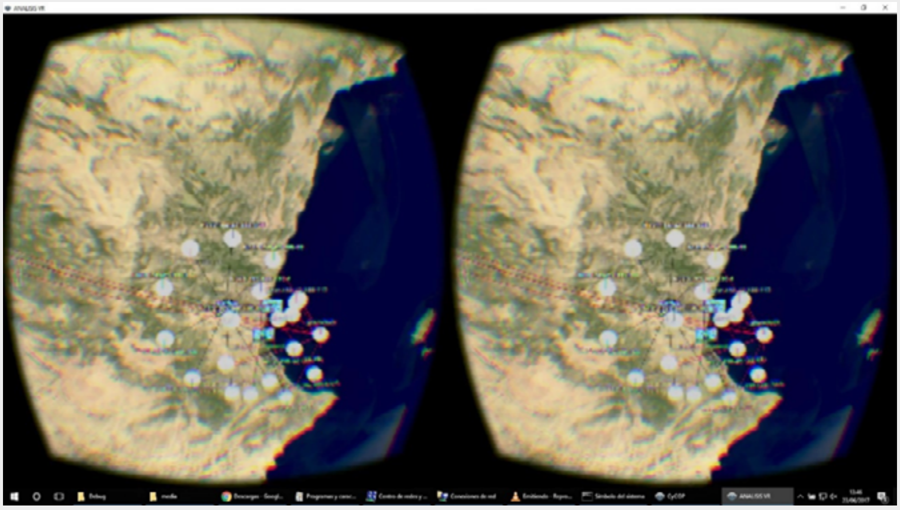


Figure 4| Network top view with a immersive interface

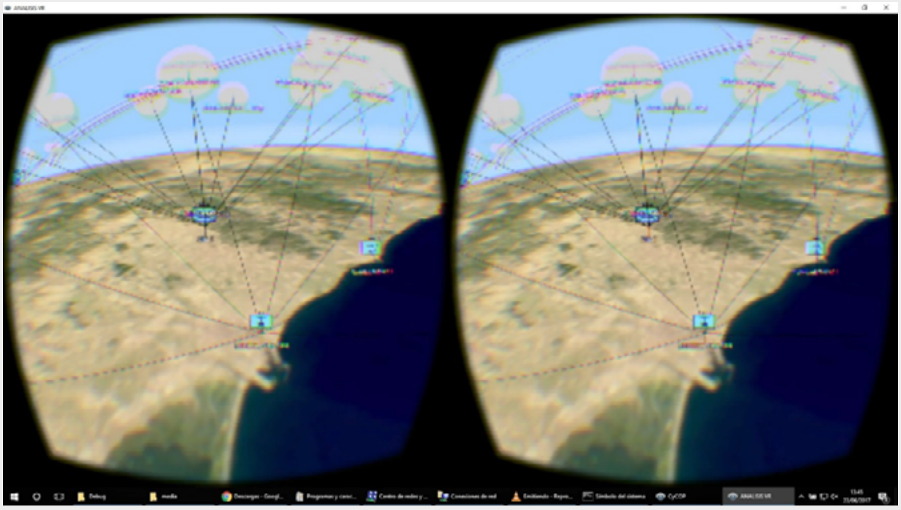


Figure 5| Detailed view of the network in immersive 3D

ADVANCED CYBER DATA GRAPHICAL REPRESENTATION

As part of the CSA HMI the consortium has developed additional advanced visualization techniques in order to help the cyber security analyst offering them different views of the situation of the network. These new ways of cyber space visualization use interactive graphs capable of showing in real time relevant network information. The first example is described in figure 6. In this interactive graph the service HTTP has been selected by the operator (see red circle) and the graph shows in which hosts is installed this service (see hosts in green colour) and also the vulnerabilities associated to this service. (see vulnerabilities in red colour).

In the same graph when the operator selects whatever host, the graph shows in blue colour all services installed in this host. Finally, if the operator selects a vulnerability the graph shows also in blue colour all services in which this vulnerability is present.

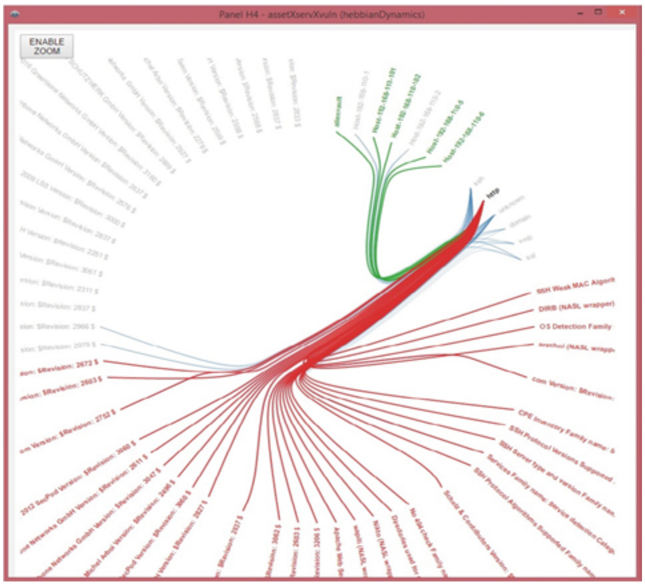
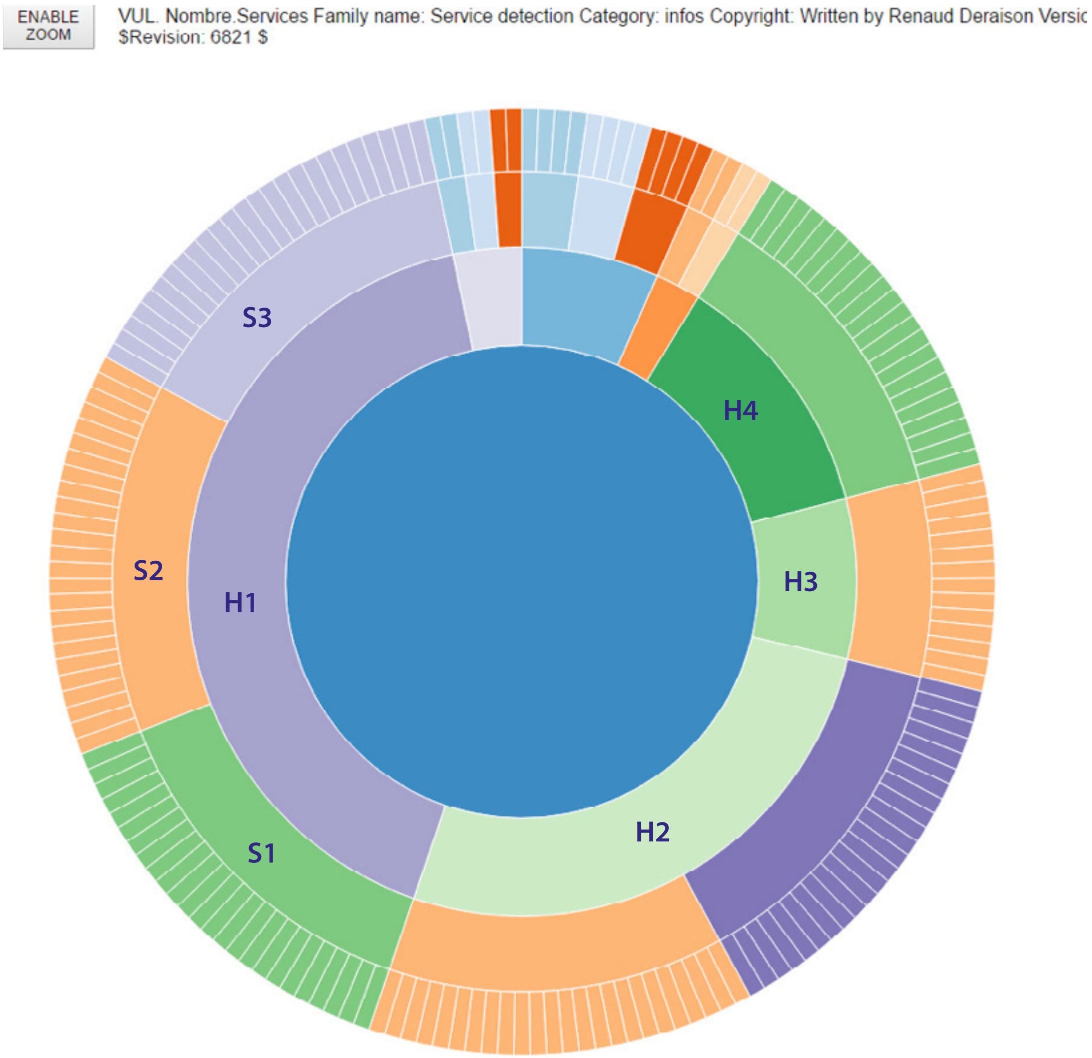

Panel H4 - assetXservXvuln (hebbianDynamics)
ENABLE ZOOM
http
SSH Weak MAC Algorit
DIRB (NASL wrapper)
OS Detection Family
CPE Inventory Family name: &
SSH Protocol Versions Supported
SSH Server type and version Family nam
Services Family name: Service detection Categ
SSH Protocol Algorithms Supported Family

Figure 6| Interactive graph for linking hosts, services installed and vulnerabilities of each service

In figure 7 another interactive graph integrated in the CSA HMI also links in a different manner the host present in the network, the services installed in each host and the vulnerabilities associated to each of the services.

The inner circle represents the hosts of the network in different colours, for example H1 mark host 1 defined by purple colour, H2 mark host 2 defined by light green colour, etc. When the operator selects some of the hosts in the circle its associated information appears in text format in the upper part of the graph.

In the second circle are stated all services installed to each host. For example, host 1 has three services installed defined by green (S1), orange (S2) and light purple (S3) colours. Finally, the last circle represent all the vulnerabilities associated to each service in the same colour that the service. When the operator selects one of these vulnerabilities its associated information appears in text format in the upper of the graph. As can be seen in figure 7 a vulnerability has been selected and its textual description appears in the graph.



VUL. Nombre.Services Family name: Service detection Category: infos Copyright: Written by Renaud Deraison Versic
$Revision: 6821 $

Figure 7| Interactive graph for linking host, services installed and vulnerabilities of each service