Guía para la gestión de un inventario de activos en sistemas de control industrial

GOBIERNO DE ESPAÑA
MINISTERIO DE ASUNTOS ECONÓMICOS Y TRANSFORMACIÓN DIGITAL

incibe_
INSTITUTO NACIONAL DE CIBERSEGURIDAD

incibe cert_

Marzo 2020

INCIBE-CERT_GUIA_INVENTARIO_DE_ACTIVOS_2020_v1

Índice

ÍNDICE DE FIGURAS

ÍNDICE DE TABLAS

1. Sobre esta guía

En esta guía se recogen los pasos necesarios para la realización de un inventario de activos en entornos industriales.

Además, se abordan diferentes métodos posibles para la elaboración de un inventario, así como una clasificación de los distintos tipos de activos que en él se pueden encontrar.

Por último, se incluye también un conjunto de herramientas, tanto de código abierto como propietarias, que se puede utilizar para la realización del inventariado.

2. Organización del documento

Este documento consta de una 3.- Introducción al inventario de activos, que se detalla con mayor profundidad en los 5 apartados siguientes

El apartado 4.- Inventario de activos en SCI explica los tipos de inventariado que se pueden implementar. Para ello, se abordan los tipos de inventariado desde dos puntos de vista. El primero, desde la implementación y el segundo desde la metodología.

A través del apartado 5.- Gestión de activos, se expone una clasificación de los activos según su naturaleza y se describe qué información es relevante a almacenar en un inventario dependiendo de cada activo.

Siguiendo con el punto 6.- Clasificación de herramientas para el inventariado de activos, se presentan, a modo de ejemplo, un conjunto de herramientas que se pueden utilizar para el inventariado de los activos. En este apartado del documento se describen tanto herramientas libres como de pago.

Una vez que se dispone de las herramientas, es necesario identificar los 7.- Pasos para la creación de un inventario de activos en SCI de una manera correcta.

Antes de cerrar el documento es necesario tratar el apartado 8.- Mantenimiento de los inventarios. Aquí se plantea la necesidad del mantenimiento del inventario y la explicación de por qué el no hacerlo supone una pérdida de valor del mismo.

El último apartado de la guía, 9.- Conclusiones, se recogen los puntos clave que ponen en valor el hecho de realizar un inventario con los activos de los sistemas de control industrial.

3. Introducción

Durante los últimos años hemos sido testigos de cómo los sistemas de control industrial (SCI) también son susceptibles de sufrir un incidente de ciberseguridad. Cada vez es mayor la concienciación, y cada vez más organizaciones implementan medidas de seguridad para conseguir elevar el nivel de ciberseguridad de sus dispositivos y redes Sin embargo, sigue habiendo un problema recurrente: el desconocimiento del total de activos por parte de las organizaciones y su respectivo alcance.

Si no se conoce el alcance total difícilmente vamos a poder tomar medidas para asegurar todos nuestros dispositivos, quedando algunos desprotegidos. Siguiendo el principio de que una cadena es tan fuerte como su eslabón más débil, podemos concluir que, si no aseguramos todos los activos por igual, estas medidas son insuficientes.

Por ello, el primer paso a la hora de asegurar los sistemas de control industrial es la realización de un inventario, que contenga todos los activos implicados en el proceso. Este inventario, si es realizado correctamente recogerá información de manera detallada por cada activo, incluyendo versiones de *software* instalado o de *firmware*. Gracias a esta información el inventario podrá servir para una correcta gestión de las vulnerabilidades, pudiendo tomar las medidas de solución y mitigación necesarias.

A lo largo de este documento veremos los tipos de inventario que podemos realizar, junto con algunas herramientas que podemos utilizar para su realización, así como los pasos a seguir para que se haga de manera correcta.

4. Inventario de activos en SCI

Contar con un inventario de activos en sistemas de control industrial permite tener una visión global de todos los elementos que forman parte del proceso, lo que ofrece numerosas ventajas, entre ellas:

- **Facilidad a la hora de gestionar vulnerabilidades** de los sistemas, ya que, en todo momento, tendremos identificadas las versiones presentes en los mismos.
- Una **respuesta a incidentes más eficiente y estructurada**, ya que, al conocer todos los activos implicados en el proceso es más fácil determinar el alcance del incidente y agilizar la subsanación del mismo.
- **Identificación de fallos a nivel operativo**. Un inventario de activos no solo proporciona ventajas a nivel de ciberseguridad, sino que también permite mejorar los procesos para hacerlos cada vez más eficientes.
- Todas estas ventajas conllevarán también la **reducción de costes**, debido a la mejora de la seguridad y conocimiento de todos los activos.

La realización de un inventario de activos debería ser uno de los primeros pasos a ejecutar en la implementación de un plan para la gestión de la ciberseguridad en sistemas de control industrial, con el objetivo de asegurar los elementos que los componen, y de esta manera poder descubrir elementos de los que no se tenía conocimiento.

Existen diferentes formas y soluciones que permiten el desarrollo de un inventario de activos. Entre las más comunes se encuentra el uso de hojas Excel, que permiten almacenar información de cada activo identificado y modificar sus datos en cualquier momento; el uso de bases de datos con una interfaz gráfica, ya sea de escritorio o web, para comodidad de uso por parte de los usuarios responsables, etc.

Estas soluciones guardan algunas características comunes, como pueden ser la facilidad de uso y de acceso o la posibilidad de exportar la información para ser tratada posteriormente, obteniendo inteligencia derivada de la información procesada.

4.1. Tipos de implementación

La forma de llevar a cabo un inventariado de activos define el tipo de implementación. Esta puede ser: manual, automática o mixta.

4.1.1. Manual

Un inventario manual es aquel elaborado por una o varias personas designadas, con los conocimientos suficientes para recopilar los datos que aportarán valor a dicho inventario y sin la ayuda de *software* complementario.

En la mayoría de los casos realizar el inventario de manera manual supone una tarea inabarcable, debido al tiempo necesario para su elaboración y futura actualización por la cantidad de activos y su complejidad. Si bien realizar un inventario de manera manual es una buena manera de asegurarnos de que poseemos toda la información necesaria sobre cada activo, solo sería recomendable cuando el número de activos es reducido.

4.1.2. Automática

Un inventario automático se elabora gracias al uso de herramientas que permiten agilizar las tareas de recopilación de datos de cada activo de manera automática, algo especialmente útil cuando el número de activos de una organización es muy elevado.

Un posible problema que puede darse en el uso de estas herramientas es la falta de información deseable sobre cada uno de los activos, que podría ser insuficiente, puesto que las herramientas podrían no facilitar todo el material necesario de cada activo, debido a que no se ha recopilado o no se ha conseguido toda la información que se necesita de él.

4.1.3. Mixta

Un inventario elaborado de forma mixta es aquel en el que se combinan el empleo de herramientas automatizadas, que corresponde a un inventario automático, y, a su vez, el uso de técnicas manuales, para de esta forma ser lo más preciso posible.

Esta forma de elaborar un inventario permite realizar una gestión de los activos de una manera más completa, ya que se recogen todos los posibles activos utilizando las herramientas automatizadas y se completa manualmente con información adicional. De la misma manera que ocurre con el inventario manual, si el número de activos es muy elevado no siempre es recomendable una implementación mixta, puesto que, según la cantidad de información necesaria a completar, el esfuerzo sería muy elevado.

Por tanto, una implementación mixta del inventario será preferible cuando el número de activos es intermedio.

4.2. Tipos de inventariado

Según la metodología utilizada a la hora de realizar el inventario, se pueden distinguir dos tipos de inventariado: el activo y el pasivo.

4.2.1. Activo

Un inventariado elaborado de forma activa es aquel que requiere realizar una acción directa, como revisar la configuración del activo o lanzar un pequeño *script* que nos dé información sobre los activos de una manera detallada, a costa de tener un posible impacto sobre los mismos. Dentro de este tipo de inventariados podemos encontrar el uso de escaneos activos o la inspección física de los mismos. En relación con la forma de implementar este tipo de inventario, un escaneo activo en la red sería un claro ejemplo de implementación con posibilidad de automatización, mientras que la inspección física de los activos sería un ejemplo de inventario activo cuya implementación es manual.

4.2.2. Pasivo

Un inventariado realizado de forma pasiva es aquel que no realiza ninguna acción de manera directa sobre los activos para obtener información sobre los mismos y, por lo tanto, no es tan intrusiva como la forma activa. Este tipo de inventariado nos permite conocer cierta información sobre los activos, no siempre de manera precisa, pero sin provocar algún impacto sobre los mismos. Dentro de los inventariados ejecutados de manera pasiva podemos encontrar el inventariado realizado a través de un análisis de tráfico o el análisis

de los ficheros de configuración de los activos. Un inventariado pasivo realizado de manera mixta sería el análisis de red, ya que se utilizan herramientas automáticas pero cierta información se analiza de manera manual; mientras que el análisis de los ficheros de configuración sería un ejemplo análisis pasivo manual.

Ilustración 1. Relación entre el riesgo en las operaciones TO y el tiempo utilizado

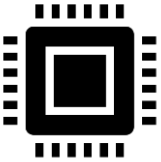
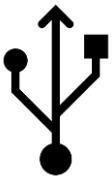
	Inventariado activo	Inventariado pasivo
Ventajas	Posibilidad de utilizar *scripts*. Rápido y se consigue gran cantidad de información sobre el activo.	Seguro al revisar configuraciones a mano y no tener que realizar ninguna acción de manera directa en el activo. Posibilidad de realizarlo de manera mixta al usar un análisis de tráfico de red y revisión manual a la vez. Útil si hay una cantidad de activos desmesurada.
Desventajas	Posibilidad de causar desperfectos en el activo al interactuar con este. Problemas de tiempo si hay una gran cantidad de activos que revisar.	Menos cantidad de información recopilada de cada activo.

Tabla 1. Ventajas e inconvenientes según el tipo de inventariado

5. Gestión de activos

Para poder llevar a cabo una correcta gestión de los activos, estos se podrían clasificar según su naturaleza. De esta manera, existe la posibilidad de tener un inventario o varios (uno por categoría) con todos los posibles activos de la organización. A su vez, es importante almacenar la información suficiente por cada activo para que el inventario aporte cierto valor.

5.1. Clasificación de activos

Activo		Descripción	Ejemplos
Hardware		Todos los equipos físicos empleados en el desarrollo del proceso industrial.	■ PLC ■ RTU ■ IED ■ Servidores
Software		Aplicaciones utilizadas para la gestión del proceso.	■ SCADA ■ Sistemas operativos ■ *Firmware* ■ Herramientas de desarrollo
Personal		Personal que trabaje en la organización.	■ Fijos ■ Subcontratados
Información		Datos que se generan, recogen, gestionan, trasmiten y destruyen, independiente de su formato.	■ Bases de datos ■ Documentación ■ Manuales
Red		Los dispositivos de conectividad de red.	■ *Routers* ■ *Switches* ■ Cortafuegos

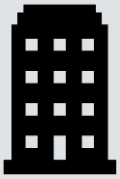
Tecnología		Equipos necesarios para gestionar las personas y el negocio de la empresa.	■ Ordenadores ■ Teléfonos ■ Impresoras ■ Cableado
Equipamiento auxiliar		Activos que no se encuentran en ninguna de las categorías anteriores y que dan soporte al resto de sistemas.	■ Climatización ■ Iluminación
Instalaciones		Lugares en los que se alojan los equipos relevantes de la empresa.	■ Oficinas ■ Edificios

Tabla 2. Clasificación de activos

5.2. Información referente de los activos

Para que el inventario aporte un cierto valor a nivel de seguridad y de gestión de riesgos, es importante almacenar información detallada sobre cada activo incluido en el mismo. Para ello, algunos de los campos más importantes que se deberían de recoger para cada activo son:

- **Identificador:** código único que identificará a cada activo.
- **Nombre:** puede incluir el modelo, marca, versión, etc.
- **Fabricante:** fabricante o desarrollador si se trata de un activo *software*. Puede incluirse en el campo "nombre".
- **Descripción:** debe contener información sobre el uso del activo.
- **Tipo:** clasificación del activo.
- **Propietario:** encargado de tomar las decisiones sobre el activo.
- **Responsable:** persona encargada de asegurarse de que el activo se encuentre operativo y de gestionar los accesos al mismo. Puede coincidir con el propietario.
- **Ubicación:** lugar donde se encuentra el activo. Si se trata de un activo físico la ubicación será un lugar, si se trata de uno lógico la ubicación será un activo físico.
- **Versiones de *software*:** en el caso de los activos físicos, se puede incluir un breve resumen del *software* presente en el dispositivo incluyendo sus versiones.
- **Valoración del activo:** permite evaluar su impacto y criticidad en el sistema. Para establecer la valoración se pueden emplear distintos parámetros como:
  - **Disponibilidad:** valor cualitativo o cuantitativo que determina la importancia que tiene la ausencia del activo.
  - **Integridad:** valor cualitativo o cuantitativo que determina las repercusiones para el negocio que tendría la modificación del activo sin autorización.
  - **Confidencialidad:** valor cualitativo o cuantitativo que determina el grado de confidencialidad que requiere el activo.

- **Criticidad:** valor que determina la dependencia del proceso con el activo. A mayor valor de criticidad, mayores consecuencias para el negocio supone la pérdida del activo.
- **Coste:** valor económico del activo.

Hay que tener en cuenta que algunos campos no aplican dependiendo del tipo de activo que estamos inventariando. Por ejemplo, para un PLC se rellenarían los siguientes campos:

- **Identificador**
- **Nombre:** PLC.2
- **Fabricante:** Siemens
- **Descripción:** control de las revoluciones de la bomba principal
- **Tipo:** S7-1200
- **Propietario:** jefe de planta
- **Responsable:** jefe de planta
- **Ubicación:** sala de bombeo
- **Versiones de *software*:** V1.2
- **Valoración del activo:**
  - Disponibilidad
  - Integridad
  - Confidencialidad
  - Criticidad
  - Coste: 290€

6. Clasificación de herramientas para el inventariado de activos

Dentro de las herramientas que se pueden utilizar para la realización de un inventariado de activos se distinguen principalmente dos tipos: las herramientas gratuitas (*open source* y libres) y las herramientas propietarias o comerciales, que también podrían considerarse libres. Las herramientas *open source* son aquellas que se pueden utilizar de manera gratuita y cuyo código fuente se encuentra disponible para todo el mundo, de manera que se pueden hacer los cambios y modificaciones que se crean oportunos a diferencia de las libres, que se encuentran también disponibles de manera gratuita, pero no se proporciona su código fuente.

Las herramientas comerciales son herramientas propietarias, y para poder hacer uso de ellas es necesario comprarlas, disponer de una licencia o realizar algún registro, aunque algunas pueden ofrecer una versión de pruebas o demo limitada en tiempo o funcionalidades. En ocasiones, las herramientas comerciales también pueden catalogarse como libres, ya que sus desarrolladores podrían poner a disposición de los usuarios las herramientas desarrolladas sin dar acceso al código fuente.

A continuación, se incluyen algunos ejemplos, tanto de herramientas *open source* y libres como de herramientas comerciales. Debido al alcance del documento no se incluyen todas las herramientas actualmente disponibles, sino algunos ejemplos representativos de cada una de las categorías anteriormente mencionadas. Aunque algunas de estas herramientas no son específicas para la creación de un inventario de activos, su correcto uso nos puede permitir hacerlo de forma detallada, principalmente activos red.

6.1. Herramientas *open source* y libres

6.1.1. Wireshark

Wireshark[1] es una herramienta de código libre desarrollada para el análisis de protocolos de red, que permite la realización de un inventario mediante la identificación de los equipos implicados en las comunicaciones de forma pasiva gracias a la captura de tráfico de red.

[1] https://www.wireshark.org/

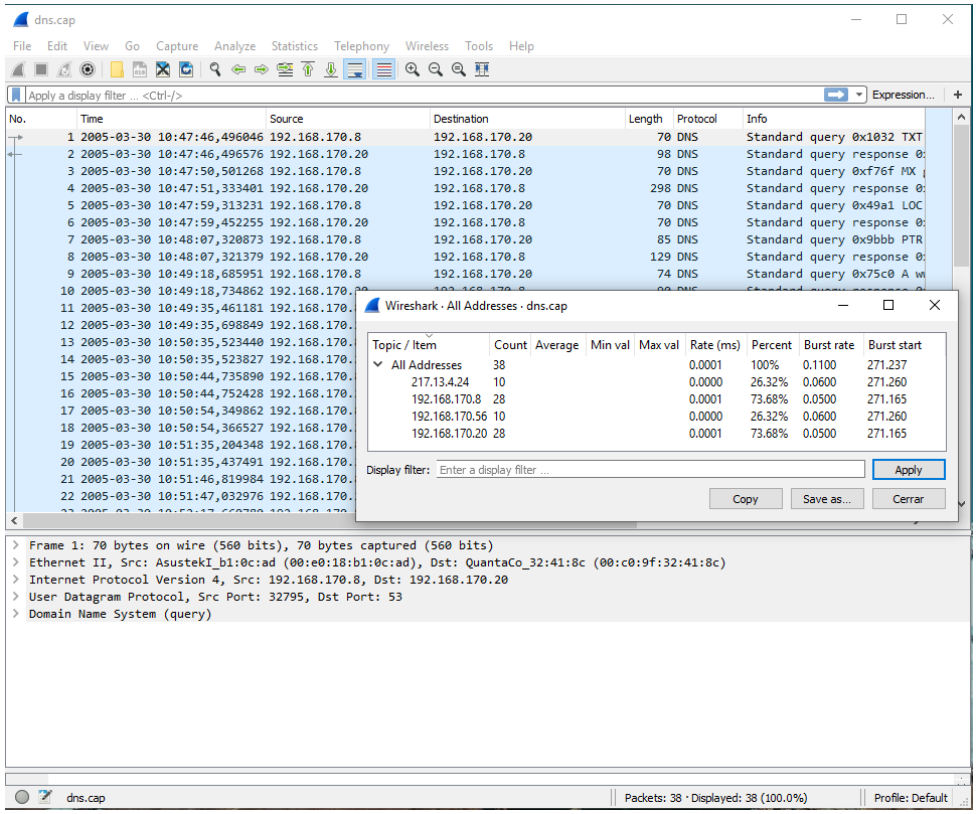


Ilustración 2. Ejemplo de activos descubiertos a través de Wireshark

6.1.2. Nmap

Nmap[2] es una herramienta utilizada para el descubrimiento de activos de red y auditorías de seguridad que, además, permite la identificación de servicios presentes en los mismos, asociados a puertos de red abiertos o a la escucha. Su tipo de inventariado es activo, realizando un escaneo sobre los activos de la red, luego su resultado debe ser cuidadosamente estudiado para evitar un posible impacto negativo sobre los activos.

Este impacto negativo podría aumentar el consumo de recursos en los equipos, saturar la red si es muy sensible, provocar funcionamientos erróneos en los equipos e, incluso, condiciones de denegación de servicio en los equipos.

```
sana@linux:~$ nmap -sP 192.168.100.0/24

Starting Nmap 7.60 ( https://nmap.org ) at 2018-11-29 10:32 PKT
Nmap scan report for _gateway (192.168.100.1)
Host is up (0.00063s latency).
Nmap scan report for 192.168.100.2
Host is up (0.086s latency).
Nmap scan report for linux (192.168.100.4)
Host is up (0.00024s latency).
Nmap done: 256 IP addresses (3 hosts up) scanned in 2.93 seconds
sana@linux:~$
```

Ilustración 3. Descubrimiento de activos mediante Nmap

[2] https://nmap.org/

6.1.3. Security Onion

Security Onion[3] es una distribución Linux, basada en Ubuntu, que incorpora varias herramientas para auditar la seguridad de los equipos de red. Entre las herramientas que posee se encuentran Wireshark, Snort (IDS) y Kibana (herramienta para visualización de datos). Security Onion permite realizar un inventario de activos de manera pasiva a través de la captura de tráfico de red.

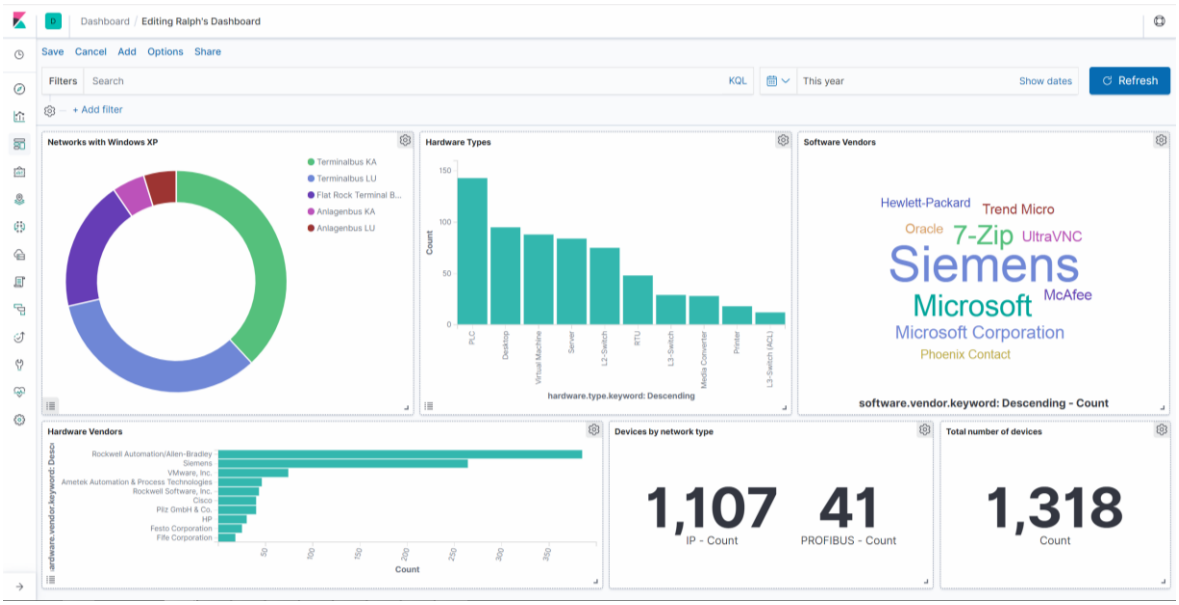


Ilustración 4. Uso de Kibana en Security Onion para un inventario de activos TO[4]

6.1.4. OpenVAS

OpenVAS[5] es una herramienta para la identificación y la gestión de vulnerabilidades en los activos. Permite obtener información detallada sobre los activos, como versiones de *software* y vulnerabilidades asociadas. La herramienta permite realizar un inventario de forma activa, realizando un escaneo sobre los activos de la red, luego su resultado debe ser cuidadosamente estudiado para evitar un posible impacto negativo sobre los activos.

Como ocurre con Nmap, podrían darse varias condiciones negativas debido al impacto de esta herramienta. Además, la ejecución de *scripts* NVT[6] para la identificación de vulnerabilidades de seguridad presentes en los equipos podría causar problemas en la actividad de los equipos.

[3] https://securityonion.net/

[4] https://www.langner.com/2019/06/ot-ics-asset-inventory-using-elasticsearch/

[5] http://www.openvas.org/

[6] https://www.incibe-cert.es/blog/nvt-testeando-seguridad-redes-industriales

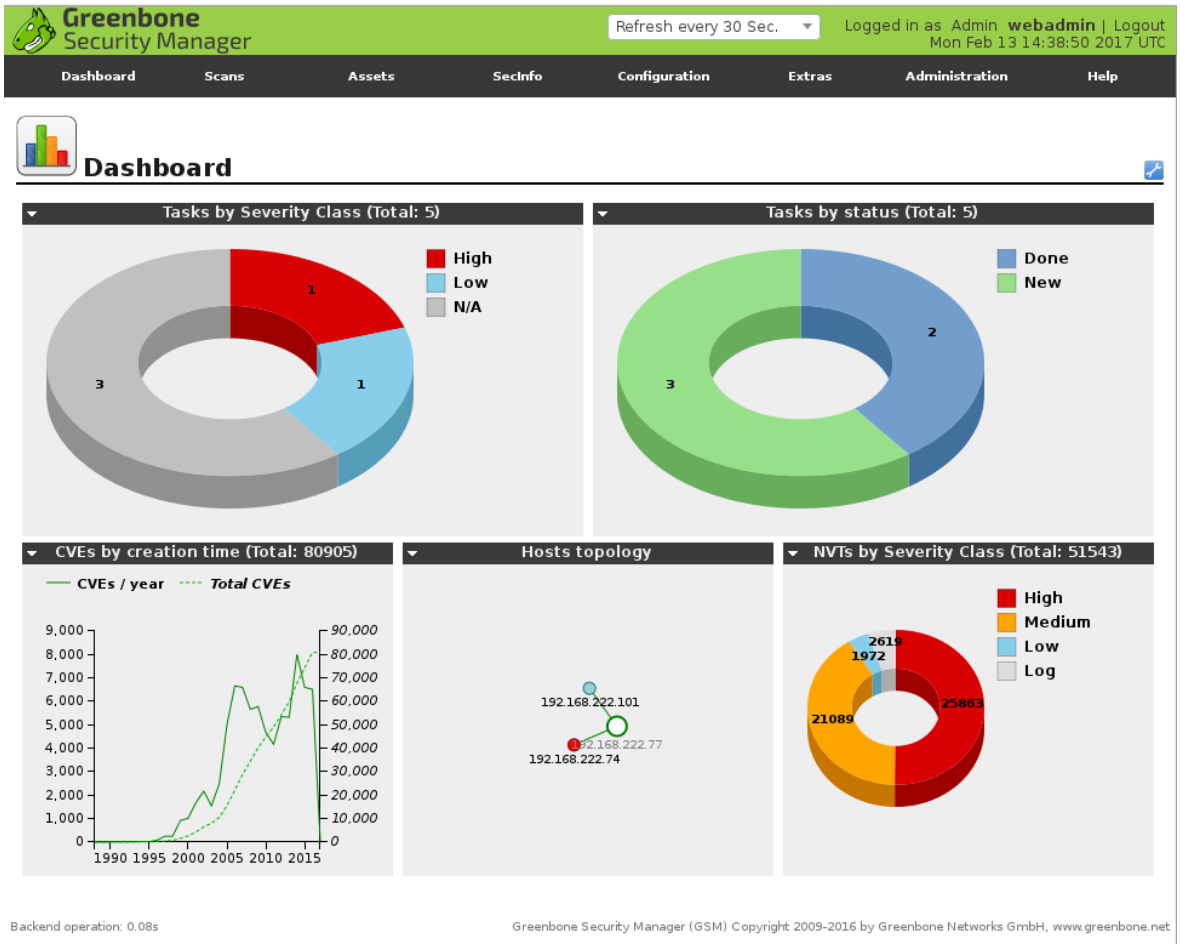


Ilustración 5. Panel principal de OpenVAS

6.1.5. GRASSMARLIN

GRASSMARLIN[7] es una herramienta para el descubrimiento de activos en redes TO. Entre las capacidades que incorpora cabe destacar la posibilidad de generación de un inventario, así como de un diagrama de red de los equipos identificados, permitiendo realizar un inventario de activos de forma pasiva gracias a la captura de tráfico de red.

[7] https://github.com/nsacyber/GRASSMARLIN

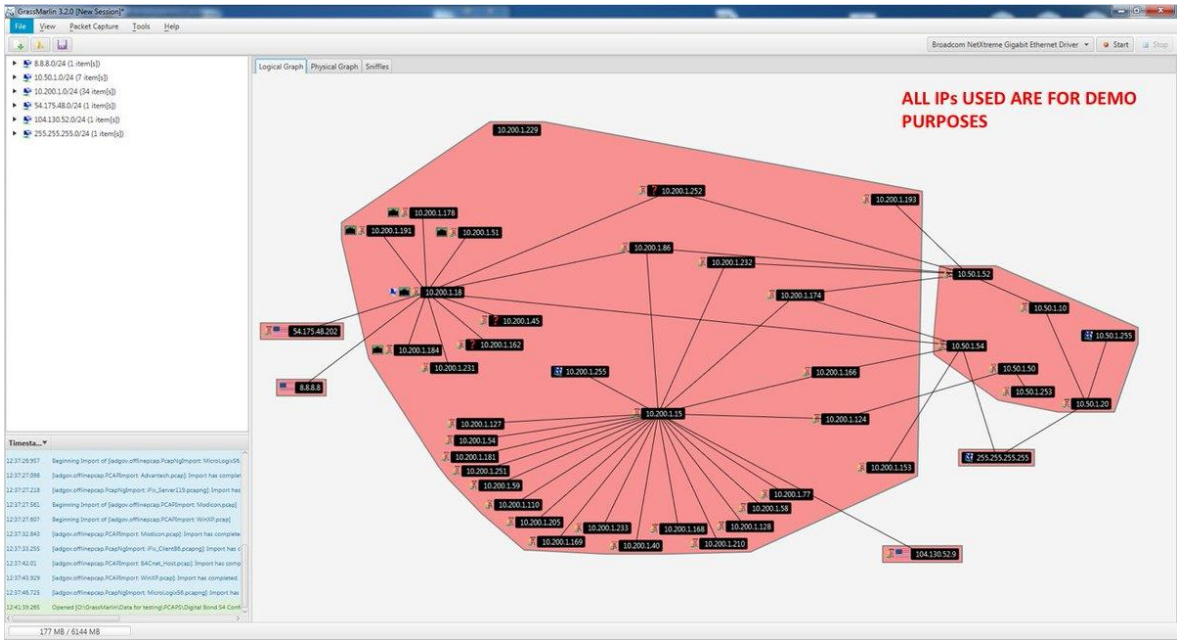


Ilustración 6. Mapa de red generado por GRASSMARLIN [8]

6.1.6. Cyberlens

Cyberlens es una herramienta para el descubrimiento y clasificación de activos de red que permite el descubrimiento y clasificación de activos tanto TI como TO, consiguiendo un inventario global de todos los activos de la red. La herramienta permite realizar un inventario de activos de manera pasiva a través de la captura de tráfico de red.

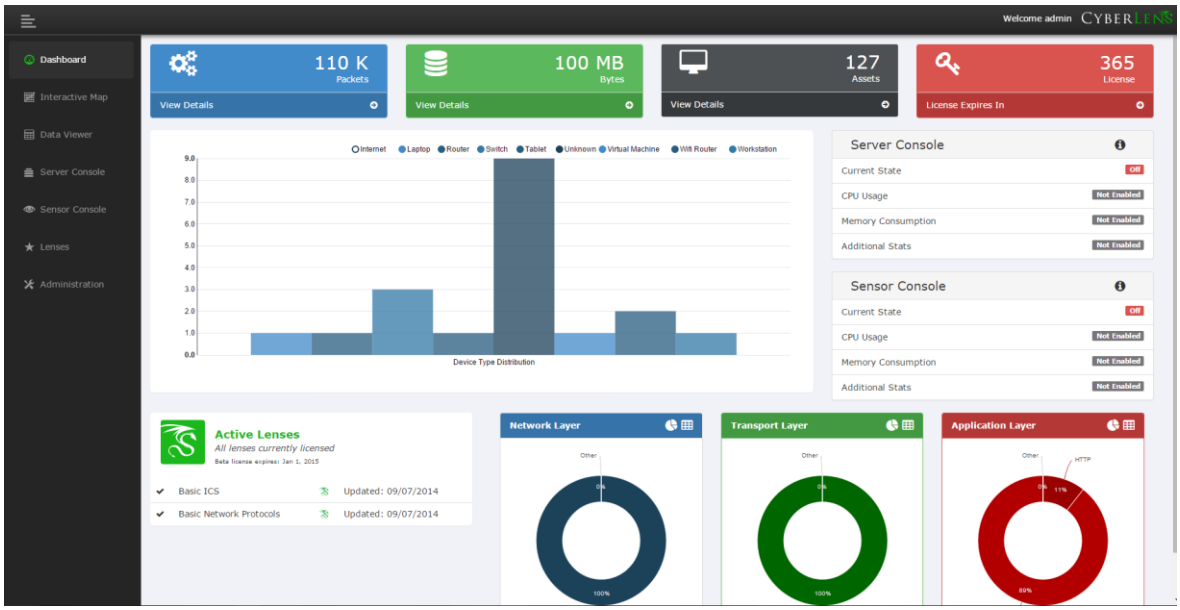


Ilustración 7. Panel principal de Cyberlens

[8] https://twitter.com/ItsReallyNick/status/879556271715889152

6.1.7. Sophia

Sophia[9] es una herramienta de detección de intrusos (IDS) de la empresa Dragos que permite el descubrimiento y clasificación de activos de red. Es capaz de realizar una inspección profunda de paquetes (DPI) de protocolos industriales como Modbus/TCP, DNP3, EthernetIP, BacNet y OPC UA[10], lo que le permite tener mayor conocimiento sobre activos TO. A través de una captura de tráfico de red la herramienta permite realizar un inventario de activos de manera pasiva.

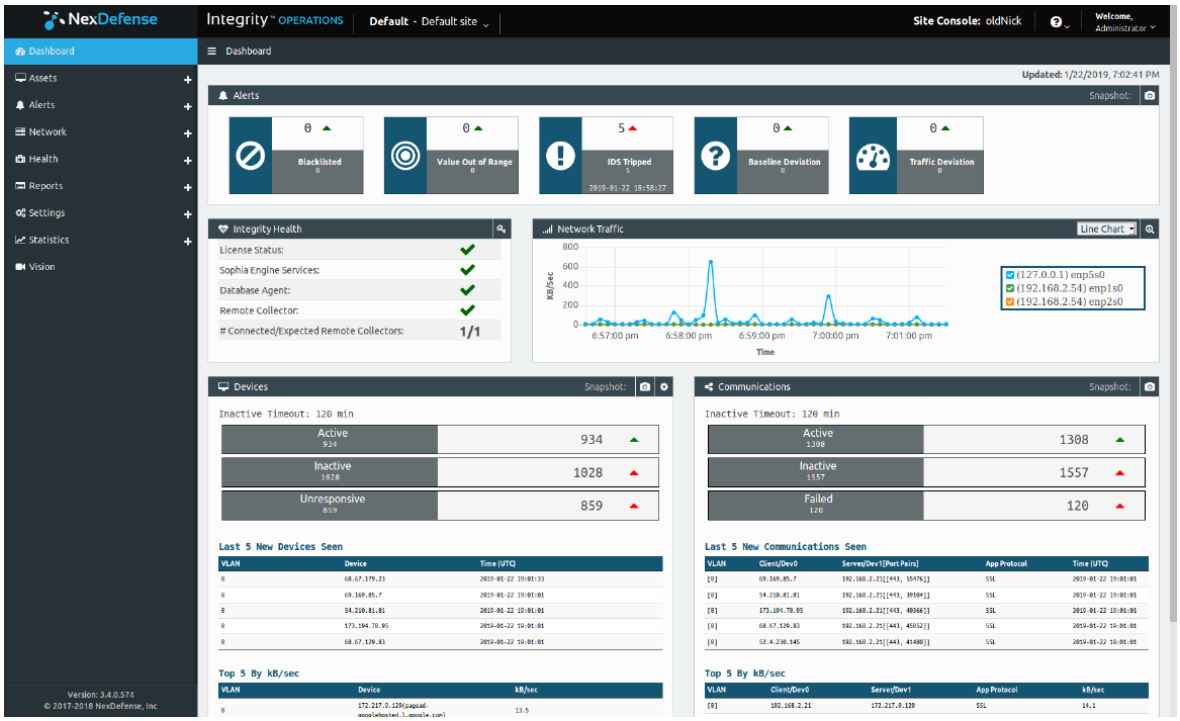


Ilustración 8. Panel principal de Sophia

6.2. Herramientas comerciales

6.2.1. OT-Base

OT-Base[11], desarrollada por la empresa Langner, es una solución de seguridad orientada a los equipos y redes TO. Entre sus capacidades se encuentra el descubrimiento de activos de la red y la gestión de un inventario TO. Para ello, realiza escaneos de forma activa empleando protocolos de comunicación industriales, como Modbus y otros protocolos de ámbito TI, de forma menos intrusiva que otras soluciones, de manera que no llega a provocar impactos en la operación.

[9] https://dragos.com/sophia-download/

[10] https://www.incibe-cert.es/blog/estandarizacion-y-seguridad-el-protocolo-opc-ua

[11] https://www.langner.com/ot-base/

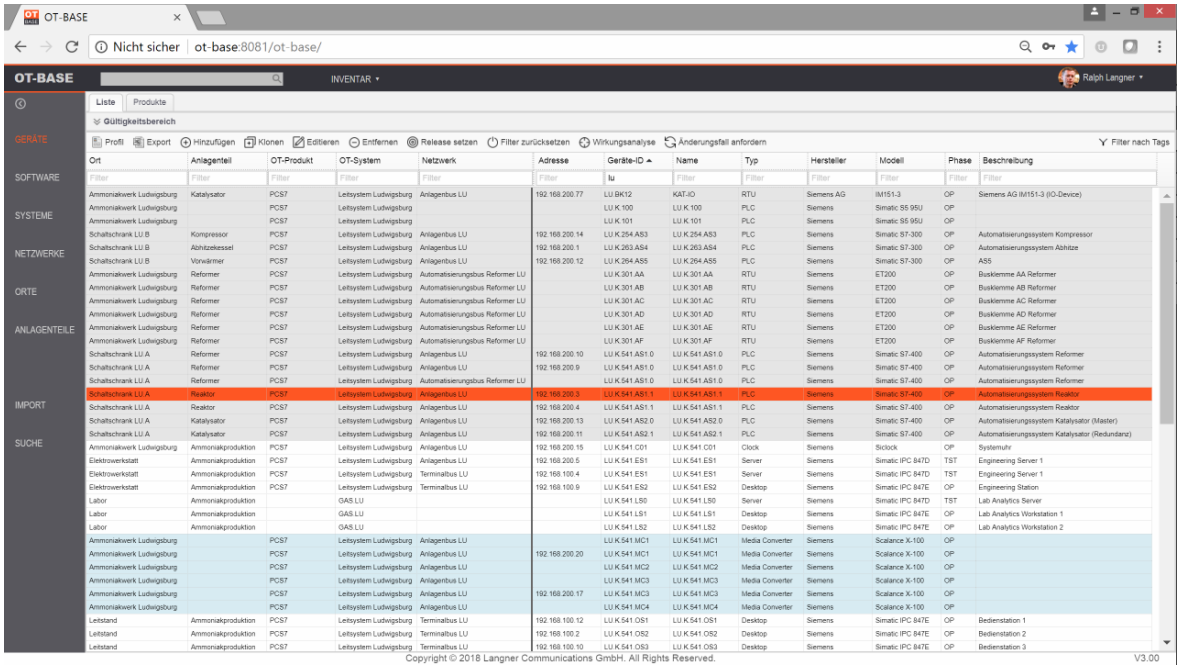


Ilustración 9. Panel principal OT-Base

6.2.2. eyeSight

eyeSight[12], desarrollada por la empresa Forescout, es una herramienta para el descubrimiento y clasificación de activos de la red. Permite el descubrimiento de activos, tanto de redes TI como de redes TO, posibilitando la realización de un inventario global de todos los activos. La herramienta permite realizar un descubrimiento de activos tanto de manera pasiva, a través de la captura de tráfico de red, como de manera activa, mediante comandos Nmap y consultas HTTP y SNMP.

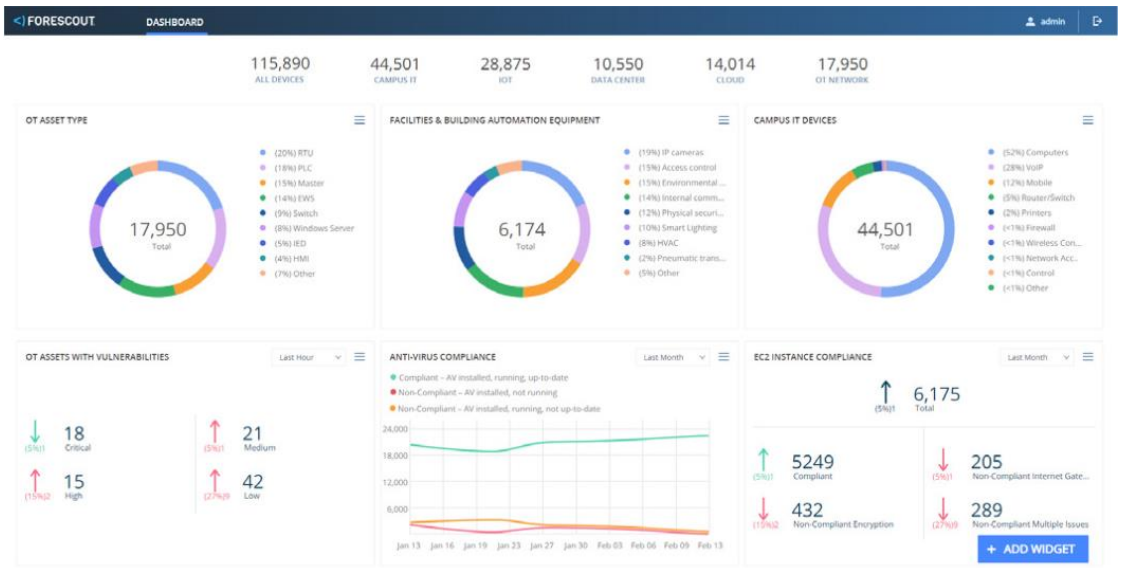


Ilustración 10. Panel principal eyeSight

[12] https://www.forescout.com/platform/eyesight/

7. Pasos para la creación de un inventario de activos en SCI

Una de las principales ayudas cuando se trabaja en los sistemas de control industrial (SCI) es poder tener a mano un inventario de activos que permita manejar con facilidad todos los dispositivos que existen dentro de TO, ya que permitirá tener todos los equipos controlados, mejorando la eficiencia a la hora de buscar algún dispositivo en concreto o la seguridad. Para ello, es necesario seguir ciertos pasos a la hora de la creación del inventario de activos desde cero, puesto que, debido a la cantidad de dispositivos que se podrán tener conectados, dicha tarea puede resultar bastante difícil si no se hace con un orden y pautas estipulados.

7.1. Definir el alcance

Para empezar, se tendrá que definir el alcance del inventario, el cual no hace referencia a la cantidad de activos a incluir, que deberán ser todos, sino al tipo de profundidad en la información a recopilar de cada uno de ellos. Esto supondrá que se revise exhaustivamente el alcance de los dispositivos, incluyendo, si fuese necesario, varios inventarios; o clasificarlos en distintos grupos debido a la cantidad y tipos diferentes que se puedan tener a la hora de gestionarlos. La necesidad de un buen inventario de activos a la hora de realizar proyectos de ciberseguridad es un factor clave que ayudará a la realización de un buen trabajo. Además, al definir un alcance correcto de la información de los activos que se van a incluir, se podrán proteger de una manera más eficiente a la hora de gestionar sus vulnerabilidades.

7.2. Definir el tipo de inventario

Una vez definido el alcance que tendrá el inventario habrá que preguntarse cuál será el tipo de implementación que se busca para su creación (manual, automática o mixta), ya que, dependiendo de la infraestructura y topología de los dispositivos que se tengan, convendrá mejor utilizar un tipo u otro. Esto mismo ocurrirá a la hora de elegir el tipo de inventariado (activo o pasivo), puesto que repercutirá en mayor o menor medida en la infraestructura o topología de dispositivos que están en plena ejecución.

7.3. Búsqueda de activos y creación del inventario

La creación de un buen inventario de activos inicial requerirá bastante tiempo para su implementación, aunque esto no siempre es fácil porque entran en juego otros factores (costes, proyectos). Además, posteriormente se deberá seguir revisando de forma continua para que se encuentre correctamente actualizado.

Es aconsejable invertir todo el tiempo posible para crear un inventario que satisfaga unos requisitos mínimos, ya que al tener más información sobre los activos bien inventariados se podrá conseguir una mejor seguridad.

Dependiendo del tipo de implementación o inventariado elegidos se utilizarán unas técnicas u otras para poder recopilar todos los dispositivos que están conectados o distribuidos en la planta.

Es necesario asegurarse de que todos los equipos están dentro del inventario y clasificarlos adecuadamente.

7.4. Revisión del inventario y copias de seguridad

Por último, cuando ya se tenga creado el inventario o inventarios, lo más importante será mantenerlo actualizado en todo momento; de lo contrario, el inventario se volverá anticuado y no aportará toda la información que se necesita, dando lugar a una mala gestión de la seguridad.

Es importante revisar los inventarios, no solo cuando haya nuevos activos sino también de forma periódica, por si en algún momento no se ha llegado a actualizar.

Una copia de seguridad del propio inventario también ayudará a prevenir un desastre, producido por terceros o gente de la propia empresa, que conlleve el robo o eliminación del inventario principal. De esta manera, no habrá que preocuparse si hubiese algún incidente con el inventario, ya que podremos restaurar dicha copia de seguridad sin perder información. Es deseable mantener una copia actualizada para que, en caso de perder la información del inventario, podamos recuperar una versión lo más actualizada posible.

Ilustración 11. Pasos para la creación de un inventario de activos

8. Mantenimiento de los inventarios

Para que el inventario de los activos sea correcto y pueda aportar valor a nivel de seguridad, ha de ser un elemento dinámico, es decir, que se actualice constantemente, estableciendo la periodicidad máxima cada vez que ocurre un cambio sobre el sistema; por ejemplo, al añadir dispositivos nuevos a la red o quitar equipos que ya están obsoletos y no son necesarios. Si bien esta periodicidad es la más deseada, casi nunca es alcanzable, y se suele establecer la realización de revisiones trimestrales, anuales o según convenga a la organización.

Por ello, es importante fijar una continuidad abarcable para la actualización del inventario. Esta periodicidad dependerá normalmente del tipo de activo o de la información que se desea actualizar. Por ejemplo, un activo de tipo personal es más propenso a cambiar en el tiempo y que se realicen altas o bajas, cambios de responsable sobre los otros activos u otras acciones relacionadas con personal. En este caso, los cambios deberían realizarse de manera manual al momento de suceder el cambio. En otro caso, como por ejemplo cambios en el *software* instalado en los equipos, si es muy numeroso se deberá revisar periódicamente a través de las herramientas automáticas utilizadas en la realización del inventario. Otra opción es que dependa del tipo de inventario que sea, ya que, si se realiza de forma manual será necesaria una persona dedicada a la ejecución de este trabajo. En función del volumen de activos de la organización es posible que se requiera más de una persona para llevar a cabo esta función.

Un inventario actualizado permitirá tener una imagen de todos los activos que forman parte del proceso. Por ello, es importante no solo realizar el inventariado una vez sino también un mantenimiento de este, de manera que sea lo más fiel a la realidad posible.

El control de accesos al inventario debe ser monitorizado para que únicamente los usuarios que pueden realizar cambios sobre el mismo estén controlados. Normalmente, el propietario del inventario será el personal de sistemas, pero determinados perfiles de otros departamentos tendrán acceso a algunas partes para establecer modificaciones. El acceso de lectura al mismo se debería permitir a cualquier usuario, al menos a las partes que no son críticas del mismo, para que conozcan los activos identificados y propongan cambios si detectan errores.

En las tareas de mantenimiento de un inventario también hay que tener en cuenta las copias de seguridad. Si está bien hecho, un inventario es una herramienta muy buena para ayudar en la resolución de incidentes. Por este motivo, es importante disponer de una copia de respaldo que permita mantener los datos a salvo de ciberataques o errores fortuitos que pudieran acabar con la información almacenada. De la misma manera que sucede con el periodo de actualización y revisión, el tiempo transcurrido entre una copia de seguridad y otra está gestionado por cada organización, pero un cambio relevante en su contenido debiera llevar asociada la realización de una nueva copia de seguridad, independientemente de cuándo fue la última vez que se realizó.

9. Conclusiones

Hoy en día cada vez es mayor la concienciación en materia de ciberseguridad y cada vez son más las empresas que buscan asegurar sus sistemas de control industrial. Pero hay un punto muy importante a tener en cuenta: no se pueden asegurar los elementos que no se conocen, por lo que un buen punto de partida podría ser llevar a cabo un inventario de todos nuestros activos.

Gracias a él se puede obtener una visión general de todos los elementos implicados en el proceso. A mayor detalle almacenado por cada activo, más fácil será la utilización del inventario como herramienta de seguridad. Por ejemplo, si se almacenan las versiones de *software* instalado en un equipo, más fácil será identificar vulnerabilidades asociadas a esas versiones.

No solo es importante realizar el inventario sino también un mantenimiento sobre el mismo, de manera que se encuentre actualizado y refleje de una manera fiel la realidad de los activos, ya que un inventario desactualizado pierde su valor.

10. Referencias

Referencia	Título, autor, fecha y enlace web
[Ref.- 1]	"Inventario de activos y gestión de la seguridad en SCI". INCIBE. 2 de junio de 2019. URL: https://www.incibe-cert.es/blog/inventario-activos-y-gestion-seguridad-sci
[Ref.- 2]	"Hardware asset inventory: A fundamental requirement for managing cyber-risk". Jeff Herbert. 2 de junio de 2019. URL: https://www.linkedin.com/pulse/hardware-asset-inventory-fundamental-requirement-managing-herbert
[Ref.- 3]	"Gestión de parches en sistemas de control". INCIBE. 2 de junio de 2019. URL: https://www.incibe-cert.es/blog/gestion-parches-sistemas-control
[Ref.- 4]	"ICS Cybersecurity: How to Protect the Proprietary Cyber Assets That Hackers Covet and WMI Cannot See". David Zahn, PAS. 2 de junio de 2019. URL: https://www.slideshare.net/EnergySec/ics-cybersecurity-how-to-protect-the-proprietary-cyber-assets-that-hackers-covet-and-wmi-cannot-see
[Ref.- 5]	"Practical Industrial Control System (ICS) Cybersecurity: IT and OT Have Converged--Discover and Defend Your Assets". Ted Gary, Dean Parsons y Doug Wylie. 2 de junio de 2019. URL: https://www.sans.org/webcasts/practical-industrial-control-system-ics-cybersecurity-ot-converged-discover-defend-assets-108515
[Ref.- 6]	"The asset management system for OT/ICS is here, and you'll like it". Langer. 10 de junio de 2019. URL: https://www.langner.com/ot-base/
[Ref.- 7]	"OT/ICS Asset Inventory using Elasticsearch". Langer. 10 de julio de 2019. URL: https://www.langner.com/2019/06/ot-ics-asset-inventory-using-elasticsearch/
[Ref.- 8]	"Analyzing the ICS Asset Inventory / Detection Market". Dale Peterson, S4. 12 de julio de 2019. URL: https://www.youtube.com/watch?v=ciM-n_JI9Ao

Anexo 1: Glosario de términos

ARP: Address Resolution Protocol

DPI: Deep Packet Inspection

HMI: Human Machine Interface

IDS: Intrusion Detection System

IED: Intelligent Electronic Device

LAN: Local Area Network

NVT: Network Vulnerability Tests

OT: Operation Technology

PLC: Programmable Logic Controller

RTU: Remote Terminal Unit

SCADA: Supervisory Control and Data Acquisition

SCI: Sistema de control industrial

SIEM: Security Information and Event Management

TI: Tecnologías de la información

TO: Tecnologías de la operación

Anexo 2: Tabla de inventario

Este anexo recoge un ejemplo de inventario de activos. La Tabla 3 incluye una serie de campos y cómo se podrían rellenar. En la página siguiente se encuentra la tabla vacía para que pueda ser impresa para su utilización. Las columnas podrían variar en función de las necesidades propias de cada inventario.

Fabricante	Descripción	Tipo	Versión de software	Estado	Responsable	Ubicación	Valoración del activo				
							Disponibilidad	Integridad	Confidencialidad	Criticidad	Coste (€)
Siemens	Control de revoluciones de la bomba principal	s7-1200	V7.1	Mantenimiento	Jefe de planta	sala de bombeo	5	6	8	10	3500
Siemens	Adquisición remota de valores	ET200	---	Activo	Jefe de planta	sala de bombeo	5	6	8	10	1000
Hirschmann	Switch de sala de bombas	Eagle 20	V3.2.34	Activo	Sistemas	sala de bombeo	10	6	8	10	2100

Tabla 3. Ejemplo de inventario de activos

Inventario: Planta 3: Sala de bombeo
Responsable: Max
Fecha: 01 / 01 / 2020.

Firma: 

Fabricante	Descripción	Tipo	Versión de software	Estado	Responsable	Ubicación	Valoración del activo				
							Disponibilidad	Integridad	Confidencialidad	Criticidad	Coste (€)

Inventario: _____ Firma:
Responsable: _____
Fecha: ____/____/_____

incibe cert_

GOBIERNO DE ESPAÑA
MINISTERIO DE ASUNTOS ECONÓMICOS Y TRANSFORMACIÓN DIGITAL

incibe_
INSTITUTO NACIONAL DE CIBERSEGURIDAD

017 TU AYUDA EN CIBERSEGURIDAD