CAPÍTULO 13. Cybersecurity

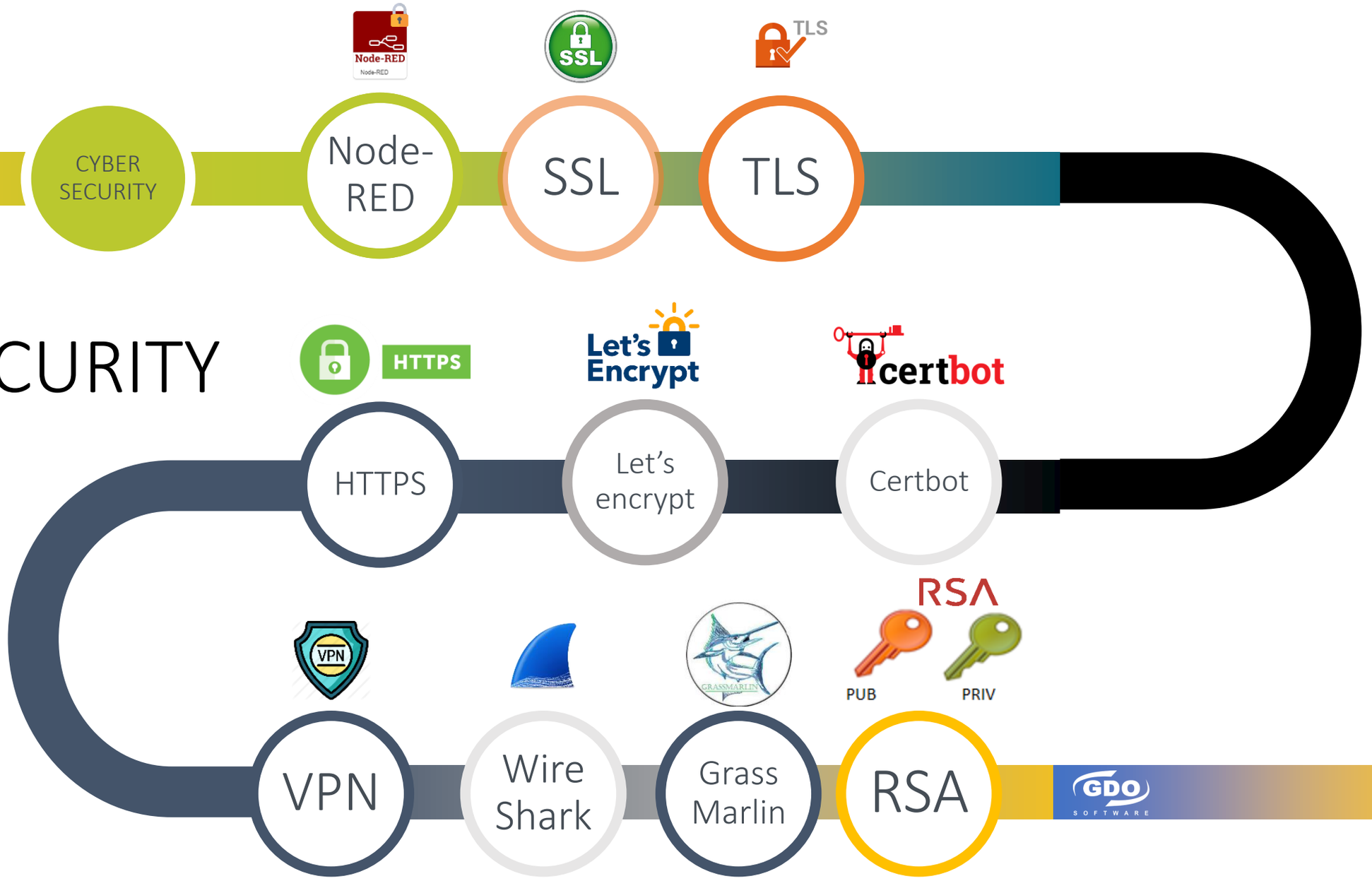
v.1.2 ABRIL 2024

Ricardo Moraleda Gareta

[Director departamento de software de GDO Software]

CYBERSECURITY

v.1.2 ABRIL 2024



CIBERSEGURIDAD

Ciberseguridad

Definición: La seguridad informática, también conocida como ciberseguridad o seguridad de tecnología de la información, es el área relacionada con la informática y la telemática que se enfoca en la protección de la infraestructura computacional y todo lo vinculado con la misma, y especialmente la información contenida en una computadora o circulante a través de las redes de computadoras.

Temas clave (industrial)

Durante este capítulo se van a cubrir estos temas clave y orientados a nivel industrial de manera muy básica.

1. Autenticación (Login y password)

2. Cifrado de la información que viaja por las redes (entre emisor y receptor)

3. Establecimiento de túneles seguros entre origen y destino (VPN) para conectar usuarios remotos a una red corporativa.



LOGIN/PASS


Securing Node-RED

Sobre la autenticación y cifrado de la información me basaré en Node-RED (web)

Está muy bien explicado en el siguiente enlace: https://nodered.org/docs/user-guide/runtime/securing-node-red

En la parte de Login se explicará:

- Securing the editor and admin API
- Securing the HTTP Nodes and Node-RED Dashboard

Para hacer esta configuración se realizará en el fichero **settings.js** de Node-RED.

Acceso al editor

Usuario para acceder al editor de Node-RED

1. admin y password encriptado.

```
// Securing Node-RED
// -----------------
// To password protect the Node-RED editor and admin API, the following
// property can be used. See http://nodered.org/docs/security.html for details.
adminAuth: {
    type: "credentials",
    users: [{
        username: "admin",
        password: "$2a$08$RRWGe.VuoFml.2y5LfxxUOQZKQzhqcNXTSdawlk0BOSm.l5WaYcuW",
        permissions: "*"
    }]
},
```

2. Para generarlo usar el comando siguiente. Poniendo textualmente el password, te genera el hash correspondiente.

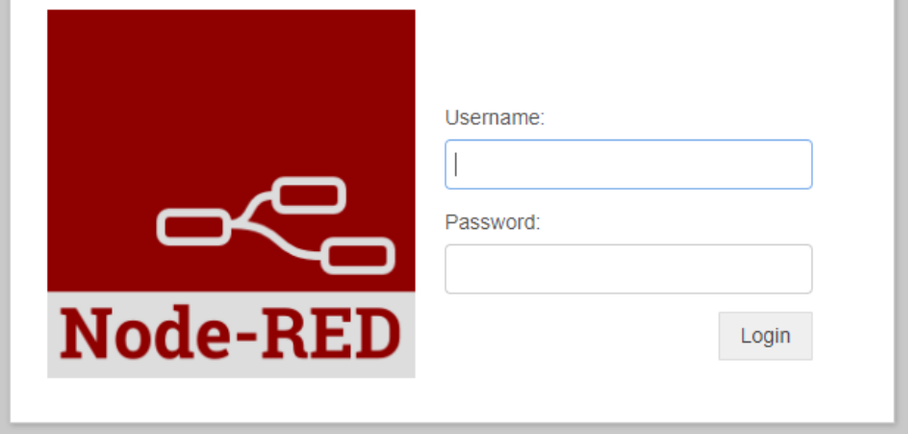
```
C:\Users\administrator>node-red admin hash-pw
Password:
$2a$08$qtSvJ29Tny8bWd4MWKZeAe3Vl36LcCZ9nCsHu/GBNNbl.rUssQPO6
```

3. Se pueden crear varios usuarios con diferentes permisos.

LOGIN/PASS

Pantalla Login acceso editor

Login y password para acceder al editor.

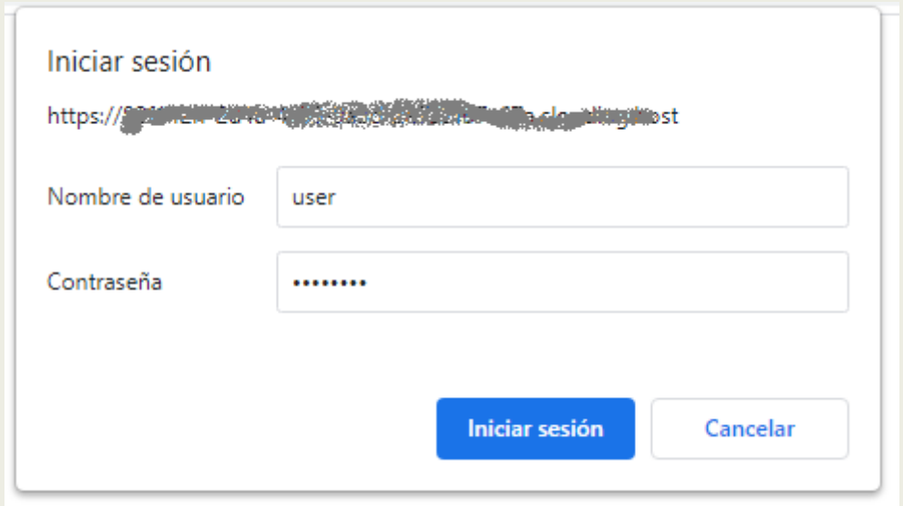


Acceso al Dashboard

Usuario para acceder al dashboard (UI) y su contenido estático de Node-RED

1. User y password encriptado

```
httpNodeAuth: {user:"user",pass:"$2a$08$RRWGe.VuoFml.2y5LfxxUOQZKQzhqcNXTSdawlk0BOSm.15WaYcuW"},
httpStaticAuth: {user:"user",pass:"$2a$08$RRWGe.VuoFml.2y5LfxxUOQZKQzhqcNXTSdawlk0BOSm.15WaYcuW"},
```



Habilitar HTTPS (443)

HyperText Transfer Protocol Secure – Port 443 [http-over-tls]

```
module.exports = {
    // the tcp port that the Node-RED web server is listening on
    uiPort: process.env.PORT || 443,
```

```
  // The following property can be used to enable HTTPS
  // See http://nodejs.org/api/https.html#https_https_createserver_options_requestlistener
  // for details on its contents.
  // This property can be either an object, containing both a (private) key and a (public) certificate,
  // or a function that returns such an object:
  //// https object:
  https: {
    key: require("fs").readFileSync(__dirname + '/privkey.pem'),
    cert: require("fs").readFileSync(__dirname + '/cert.pem')
  },
```

```
  // The following property can be used to cause insecure HTTP connections to
  // be redirected to HTTPS.
  requireHttps: true,
```

Se deben crear 2 ficheros: clave privada y certificado.

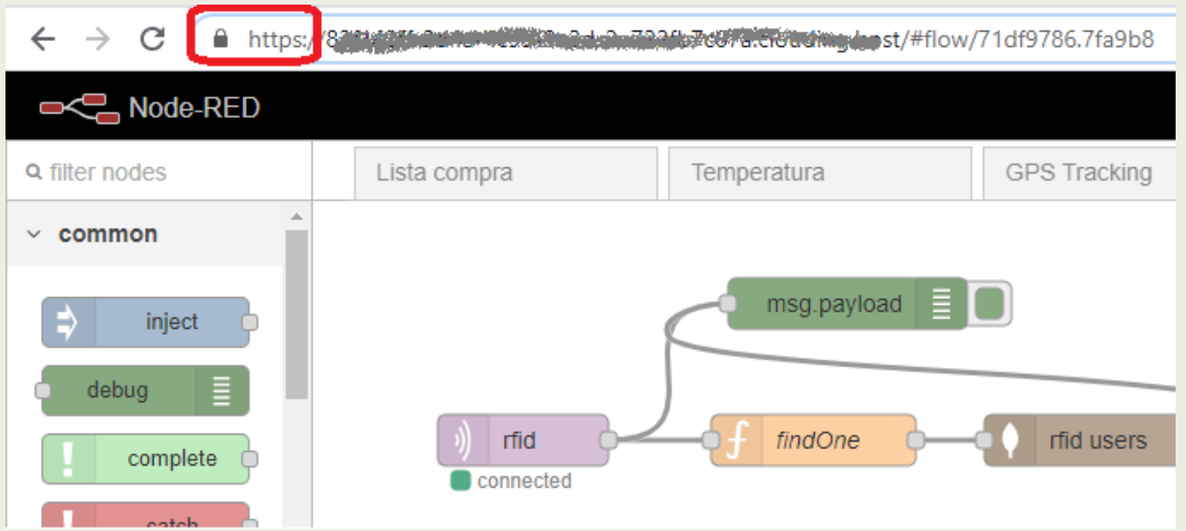
Se ubicarán en la carpeta raíz, donde settings.js.

Node-RED

En la consola de Node-RED (servidor):

```
16 Apr 19:08:03 - [info] Server now running at https://127.0.0.1:443/
```

En el navegador web (cliente):

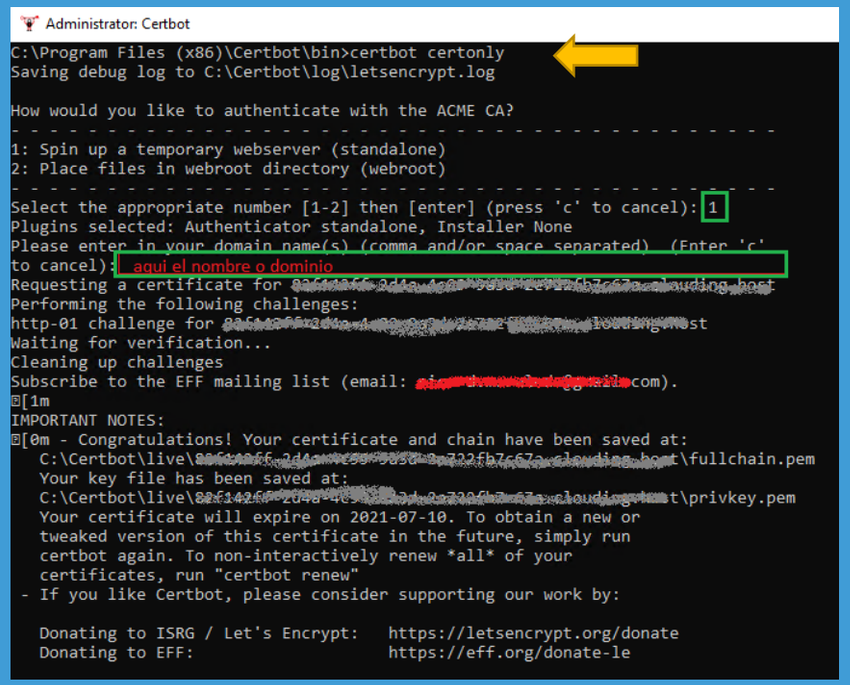


Certificado

Private Key / Certificate

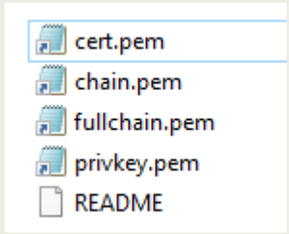
Para generar un certificado (X.509 v3) emitido por R3-Let's Encrypt usaré la aplicación Certbot.

https://dl.eff.org/certbot-beta-installer-win32.exe



Private Key / Certificate

La aplicación certbot genera los siguientes ficheros en formato PEM.



Los que usaré para securizar Node-RED son:

1. **cert.pem**
2. **privkey.pem**

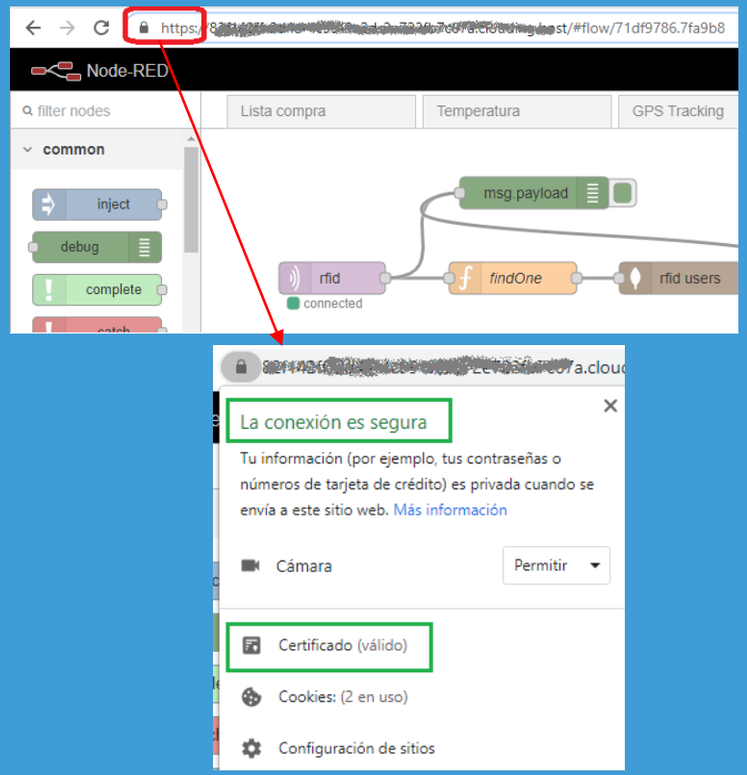
Privacy-Enhanced Mail (PEM) is a de facto file format for storing and sending cryptographic keys, certificates, and other data, based on a set of 1993 IETF standards defining "privacy-enhanced mail".

https://en.wikipedia.org/wiki/Privacy-Enhanced_Mail

Certificado

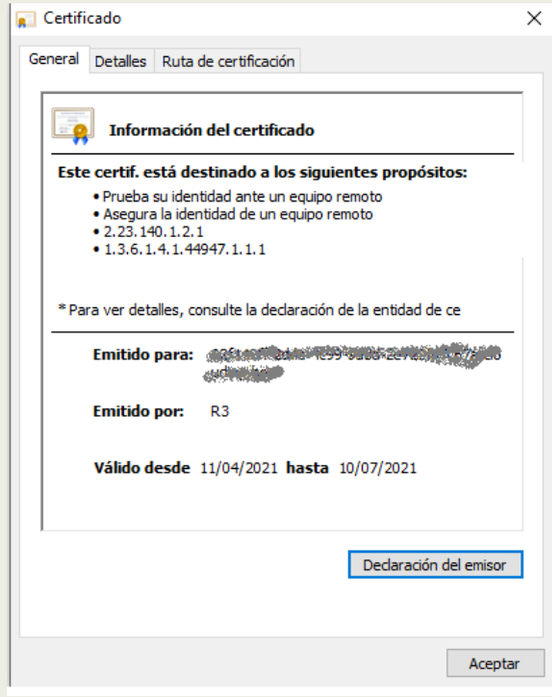
HTTPS. Certificado válido

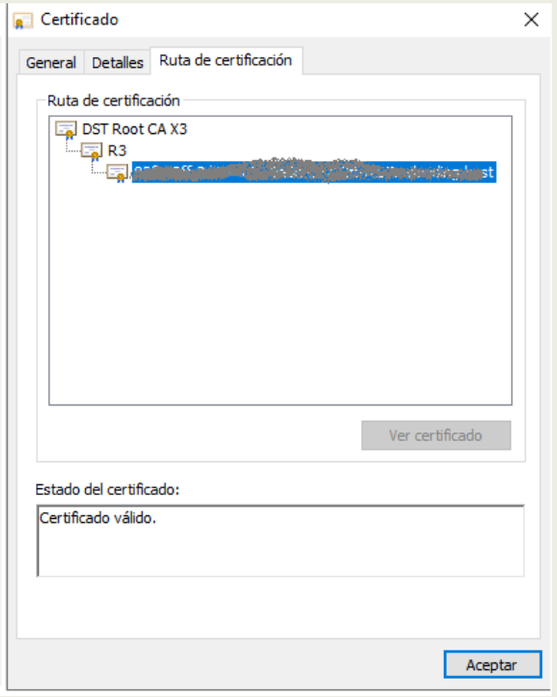
El resultado es el siguiente: (válido para 3 meses).



Certificate

El navegador cliente confía en él ya que está firmado por una CA (autoridad de certificación): R3

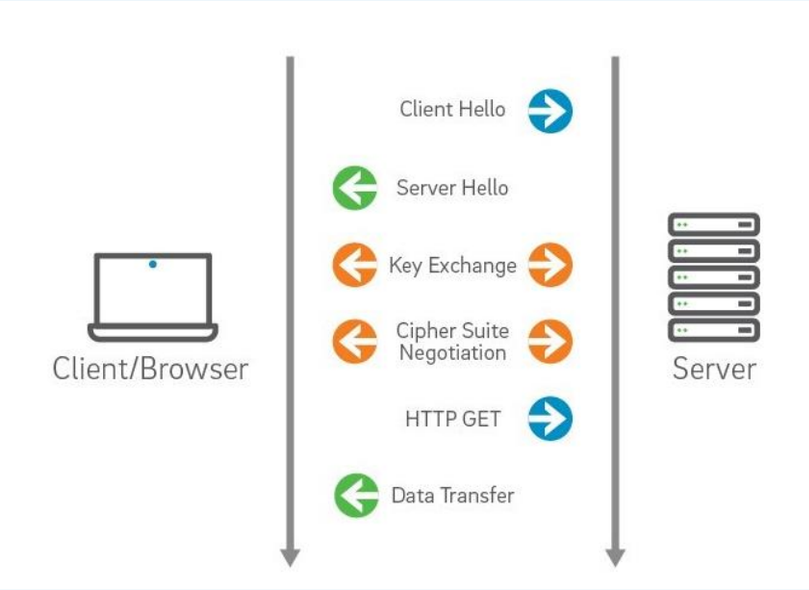




TLS

Transport Layer Security

TLS es el protocolo sucesor de SSL, que se lanzó en 1999 como una versión mejorada de SSL 3.0. Inicialmente, se le conocía como SSL 3.1. La versión actual es **TLS 1.3** (desde 2018)

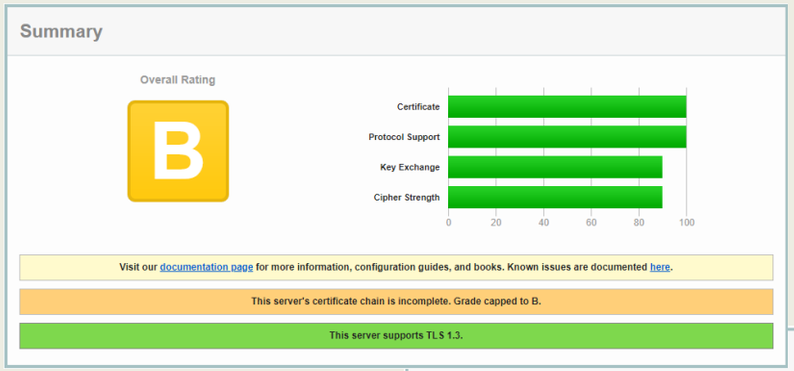


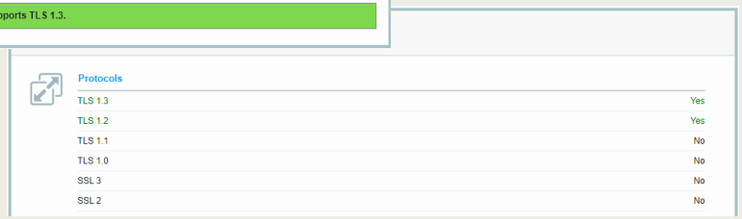
Análisis servidor

Con esta herramienta de GlobalSign podrás comprobar qué protocolos de cifrado tiene habilitados el servidor de un sitio web específico. Hace un buen informe.

https://globalsign.ssllabs.com/analyze.html

Pruebo la URL del servidor Node-RED securizado:





Wireshark

Handshake protocol

TLSv1.3

Protocol	Length	Info
TLSv1.3	700	Client Hello
TLSv1.3	571	Client Hello
TLSv1.3	571	Client Hello
TLSv1.3	373	Application Data
TLSv1.3	738	Application Data
TLSv1.3	310	Server Hello, Change Cipher Spec, Application Data, Application Data
TLSv1.3	134	Change Cipher Spec, Application Data
TLSv1.3	374	Application Data
TLSv1.3	735	Application Data
TLSv1.3	734	Application Data
TLSv1.3	1514	Server Hello, Change Cipher Spec, Application Data
TLSv1.3	555	Application Data, Application Data, Application Data
TLSv1.3	310	Server Hello, Change Cipher Spec, Application Data, Application Data
TLSv1.3	134	Change Cipher Spec, Application Data
TLSv1.3	134	Change Cipher Spec, Application Data
TLSv1.3	375	Application Data
TLSv1.3	1514	Server Hello, Change Cipher Spec, Application Data
TLSv1.3	555	Application Data, Application Data, Application Data
TLSv1.3	134	Change Cipher Spec, Application Data
TLSv1.3	374	Application Data
TLSv1.3	372	Application Data
TLSv1.3	628	Application Data, Application Data
TLSv1.3	628	Application Data, Application Data
TLSv1.3	763	Application Data
TLSv1.3	781	Application Data
TLSv1.3	784	Application Data
TLSv1.3	783	Application Data
TLSv1.3	786	Application Data
TLSv1.3	782	Application Data
TLSv1.3	286	Application Data
TLSv1.3	785	Application Data

Application Data

Los datos de aplicación viajan **encriptados**

```
Transport Layer Security
  TLSv1.3 Record Layer: Application Data Protocol: http-over-tls
      Opaque Type: Application Data (23)
      Version: TLS 1.2 (0x0303)
      Length: 313
      Encrypted Application Data: e933cd84dfe597aec772b6e9750b54505044160d62091842…
```

```
0000  c0 b6 f9 89 cf 79 70 0b  01 23 f7 61 08 00 45 00   ·····yp· ·#·a··E·
0010  01 66 ab e5 40 00 7a 06  3e b9 b9 fd 98 b6 c0 a8   ·f··@·z· >·······
0020  01 97 01 bb 22 20 97 8b  12 bc 19 75 ff 30 50 18   ····" ·· ···u·0P·
0030  03 fd e0 80 00 00 17 03  03 01 39 e9 33 cd 84 df   ········ ··9·3···
0040  e5 97 ae c7 72 b6 e9 75  0b 54 50 50 44 16 0d 62   ····r··u ·TPPD··b
0050  09 18 42 f8 f4 4a 13 82  a8 b0 6e 21 18 95 60 63   ··B··J·· ··n!··`c
0060  9a 31 5e 76 a0 7a 1b 6c  88 38 91 54 b8 2d 0a f1   ·1^v·z·l ·8·T·-··
0070  f5 b5 00 29 61 bd 97 a7  45 7d 79 df e4 51 6e 1e   ···)a··· E}y··Qn·
0080  a3 ff 9c 60 13 06 db 15  13 b3 6f 2b dd e7 3a 76   ···`···· ··o+··:v
0090  a3 54 bb 52 d6 34 85 9d  41 98 e6 4b 13 44 0b 19   ·T·R·4·· A··K·D··
00a0  80 de 6f 1b bd 4b 64 50  c0 ab 2d 55 a3 a7 39 4b   ··o··KdP ··-U··9K
00b0  29 8e 89 d6 bd 6b e4 97  29 18 db f4 8c 55 f5 f2   )····k·· )····U··
00c0  15 fe bc 11 42 4c 0d ae  ea cc af 0a e5 b9 7b b8   ····BL·· ·····{·
00d0  67 bc d3 ec 7b 0c 0e e2  af 53 8d 44 4b 47 ec b1   g···{··· ·S·DKG··
00e0  42 ab 6d 93 86 19 22 ed  cf f1 0b 13 bd ad 32 76   B·m···"· ·····2v
00f0  01 53 9b 2a 89 6a c6 b2  01 c0 3d c7 10 05 4c 22   ·S·*·j·· ··=···L"
0100  38 76 7f 2e b4 8e 6d 38  3c 54 f3 3f b1 95 b1 77   8v····m8 <T·?···w
0110  50 31 db e2 cf b5 b6 f5  08 f5 e8 74 77 1f 8e 1d   P1····· ···tw···
0120  97 75 2d c2 45 05 a4 75  78 89 44 42 15 27 9b 57   ·u-·E··u x·DB·'·W
0130  97 8d 07 d1 08 55 b9 e2  44 3b 3e 8d c8 4a 4d 16   ·····U·· D;>··JM·
0140  fe a5 5a f2 a1 f8 06 85  33 52 67 3c aa 13 fe 18   ··Z····· 3Rg<····
0150  54 5f 22 11 2e f4 58 7a  63 40 7a 45 77 63 db fe   T_"···Xz c@zEwc··
0160  f2 7a 08 f2 38 0b 73 26  92 38 1e 9c 63 02 11 cb   ·z··8·s& ·8··c···
0170  b9 9c 01 87                                       ····
```

Criptografía asimétrica

Cifrado de mensaje

https://es.wikipedia.org/wiki/Criptograf%C3%ADa_asim%C3%A9trica

Clave pública y privada (pareja): Son algoritmos de Euler unidireccionales no reversibles. En el ejemplo las 2 claves son de David. La pública se comparte y la privada nunca.

https://youtu.be/Q8K311s7EiM RSA

1. Ana redacta un mensaje.
2. Ana cifra el mensaje con la **clave pública** de David.
3. Ana envía el mensaje cifrado a David a través de internet, ya sea por correo electrónico, mensajería instantánea o cualquier otro medio.
4. David recibe el mensaje cifrado y lo descifra con su **clave privada**.
5. David ya puede leer el mensaje original que le mandó Ana.

Firma digital con clave asimétrica

FIRMA DIGITAL CON CLAVE ASIMÉTRICA

1. David redacta un mensaje.
2. David firma digitalmente el mensaje con su clave privada.
3. David envía el mensaje firmado digitalmente a Ana a través de internet, ya sea por correo electrónico, mensajería instantánea o cualquier otro medio.
4. Ana recibe el mensaje firmado digitalmente y comprueba su autenticidad usando la clave pública de David.
5. Ana ya puede leer el mensaje con total seguridad de que ha sido David el remitente.

VPN

Virtual Private Network

Definición: Es una tecnología de red de ordenadores que permite una extensión segura de la red de área local (LAN) sobre una red pública o no controlada como Internet.

Hay varios tipos de VPN: IPSec para conexiones fijas (capa de red) y SSL/TLS para conexiones puntuales y móviles (capa aplicación), entre otras (MPLS, L2TP, …).

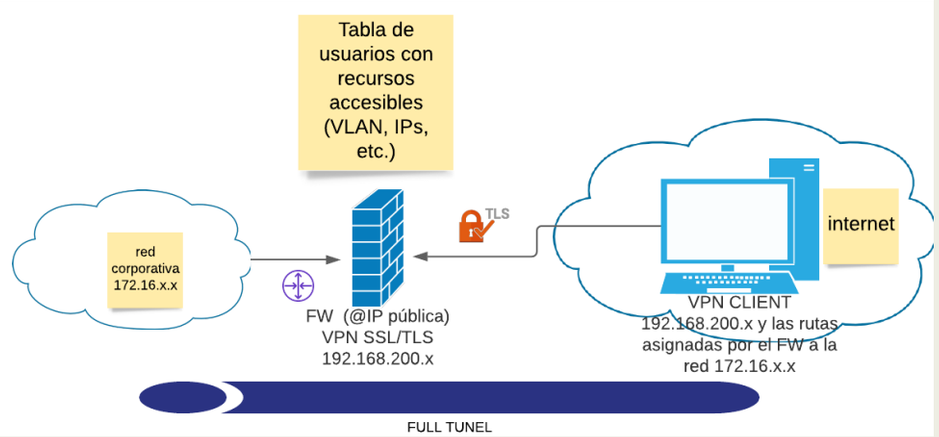
VPN SSL/TLS (puerto TCP 443 HTTPS http-over-tls)

El usuario remoto que usa este tipo de túnel puede ingresar de manera controlada a recursos perimetrales específicos. Conexión granular a recursos: óptima para conectar mano de obra remota.

Se crea un rango local diferente al rango corporativo para asignar IPs a los clientes. Ambos rangos están enrutados.

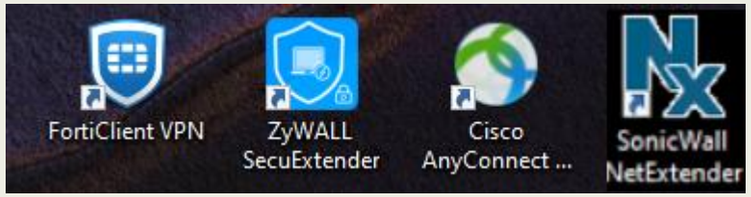
Firewall (FW)

El FW hará la gestión de accesos VPN SSL/TLS. Según la configuración, hará que un usuario concreto pueda acceder a ciertos recursos de la red corporativa.



Normalmente el usuario cliente se conectará a la VPN a través de un software de estos (según el FW):

- FORTI
- ZYXEL
- CISCO
- SONICWALL



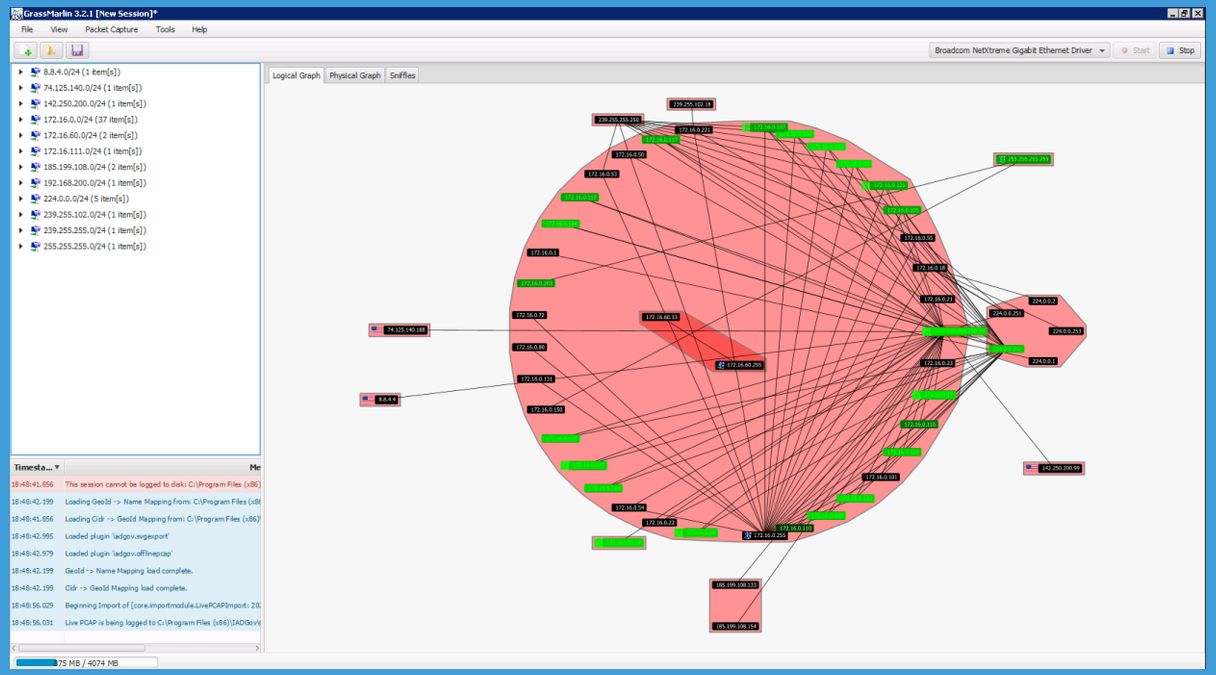
Herramientas

Grassmarlin 3.3

SCADA and ICS analysis tool (passive ICS network mapping)

https://enredandoconredes.com/2016/11/28/identificando-trafico-en-redes-ics-grassmarlin/

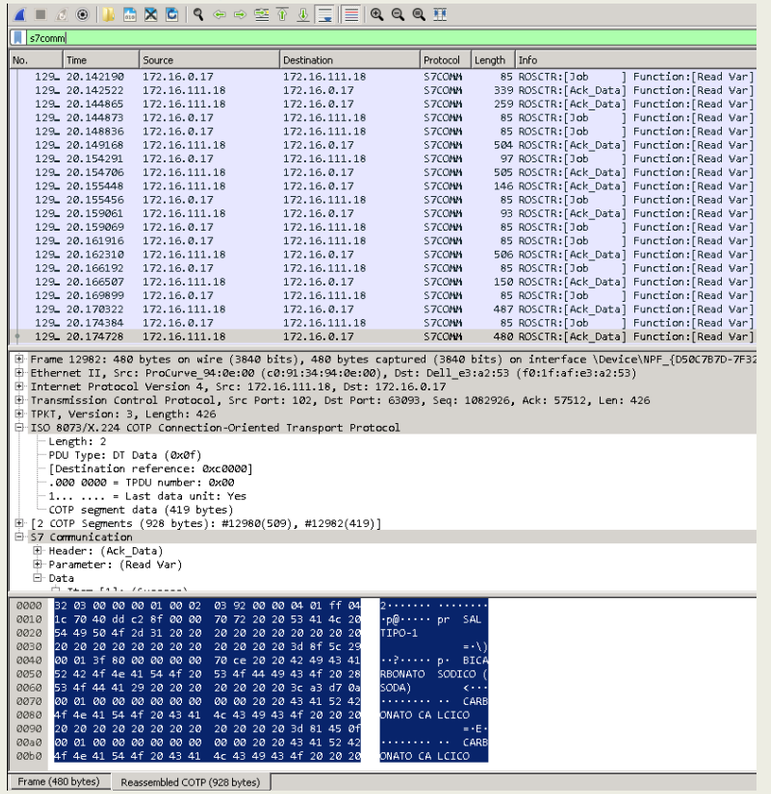
https://github.com/nsacyber/GRASSMARLIN



WireShark 4.2.4

https://zerontek.com/zt/2021/04/12/wireshark-filters-for-ics-protocols/

La última versión ya soporta unos 32 protocolos industriales. Por ejemplo:



SIEMENS

S7 COMM

Port 102

Resumen

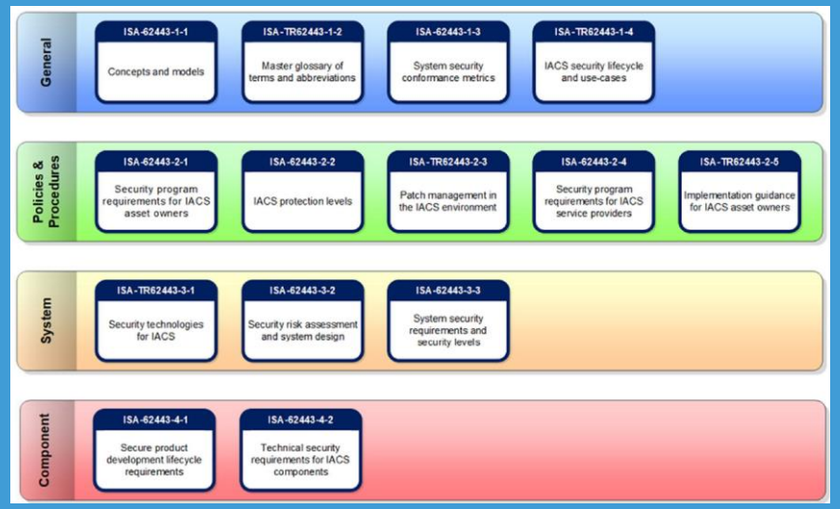
Resumen

Estas son unas pinceladas de como securizar, pero existen muchos niveles de ciberseguridad.

- Infraestructura, sistemas, y software.

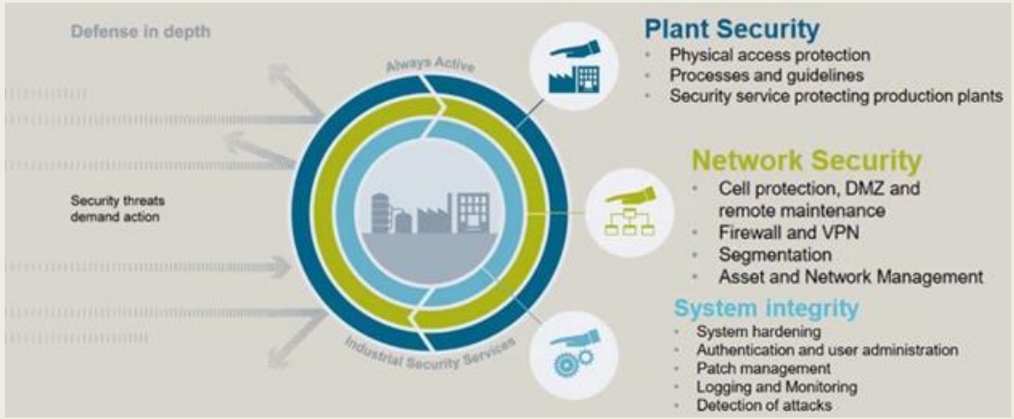
Buenas prácticas:

- Hacer una auditoría para evaluar el estado de seguridad actual basándose en la norma **IEC62443**



https://becolve.com/blog/desmontando-la-iec-62443/

Resumen



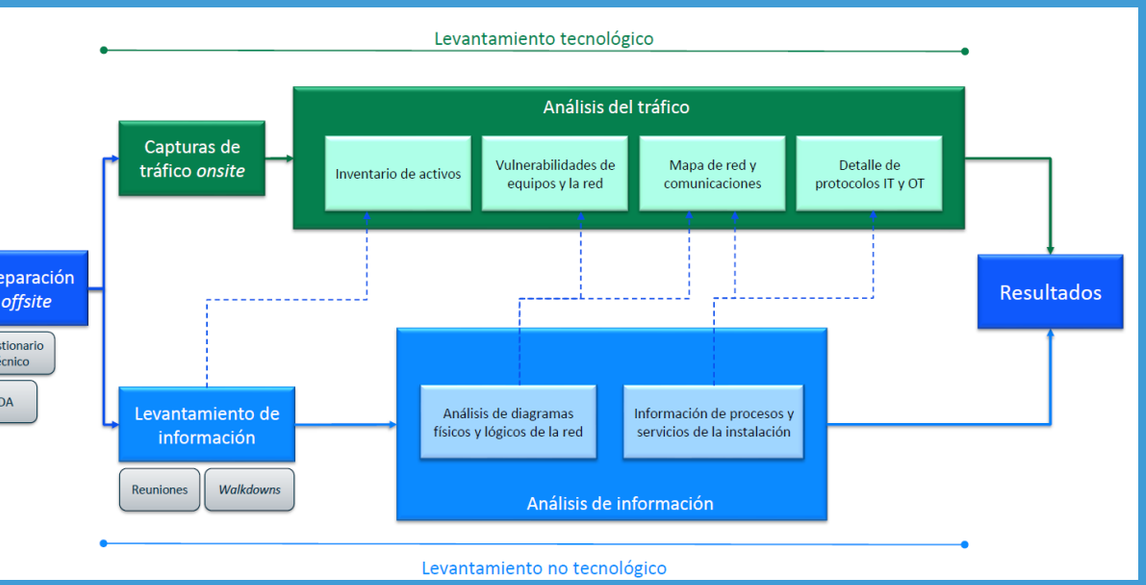
Mitigar riesgos mediante implementación de medidas:

1. Seguridad de red (DMZ, FW, VPN, VLANs, …)
2. Versiones de sistemas operativos, sistemas de virtualización y aplicaciones actualizadas.
3. Software antivirus y firewall activados y actualizados.
4. Accesos a la red controlados (autenticación, VPN, …)
5. Firmware de equipos actualizados.
6. Autenticación de los dispositivos.
7. Mecanismos para poder actualizar remotamente los sensores, si se detecta un bug.
8. Software de detección de ataques y análisis de tráfico en tiempo real.

Auditoría

Auditoría

Los trabajos de una auditoría de ciberseguridad en red industrial (OT) podrían ser estos:



Capturas de tráfico *onsite*

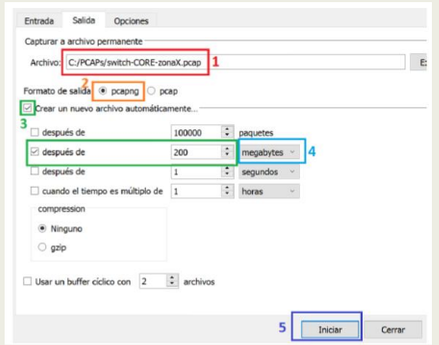
En las reuniones previas determinar los puntos de captura de tráfico.

El tráfico se capturará de forma pasiva en los switches clave elegidos. Se derivará el tráfico o **PORT MIRRORING** de las N VLANS en cada switch a un puerto libre, también llamado **SPAN** (SWTCH PORT ANALYZER). Los switches tienen que ser gestionables evidentemente para que soporten esta función.

A este puerto SPAN se conectará un portátil corriendo un software llamado **WireShark**.

```
Switch(config)# monitor session 1 source remote vlan 901
Switch(config)# monitor session 1 destination interface fastEthernet0/5
Switch(config)# end
```

.pcapng files



Auditoría

Herramienta análisis

Se analizan los N ficheros .pcap extraídos de WireShark de todas las muestras de todos los switches clave de la red OT mediante herramientas.

Por ejemplo, Telefónica Tech dispone de su propia herramienta vASPI_ (Analizador virtual de Seguridad de Plantas Industriales)

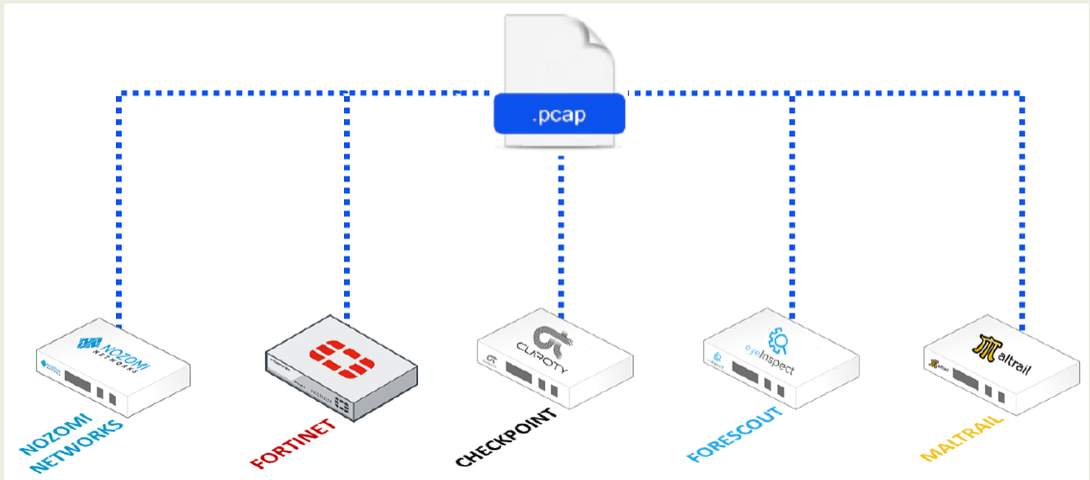
Basada en 3 tipos de análisis:

- Sondas de monitorización de tráfico industrial: Nozomi Guardian, Claroty y eyeInspect.
- Firewall de nueva generación: FortiGate y su generador de informes FortiAnalyzer.
- Detección de dominios maliciosos o de mala reputación: Maltrail.

Telefónica Tech

vASPI_

Telefónica Tech



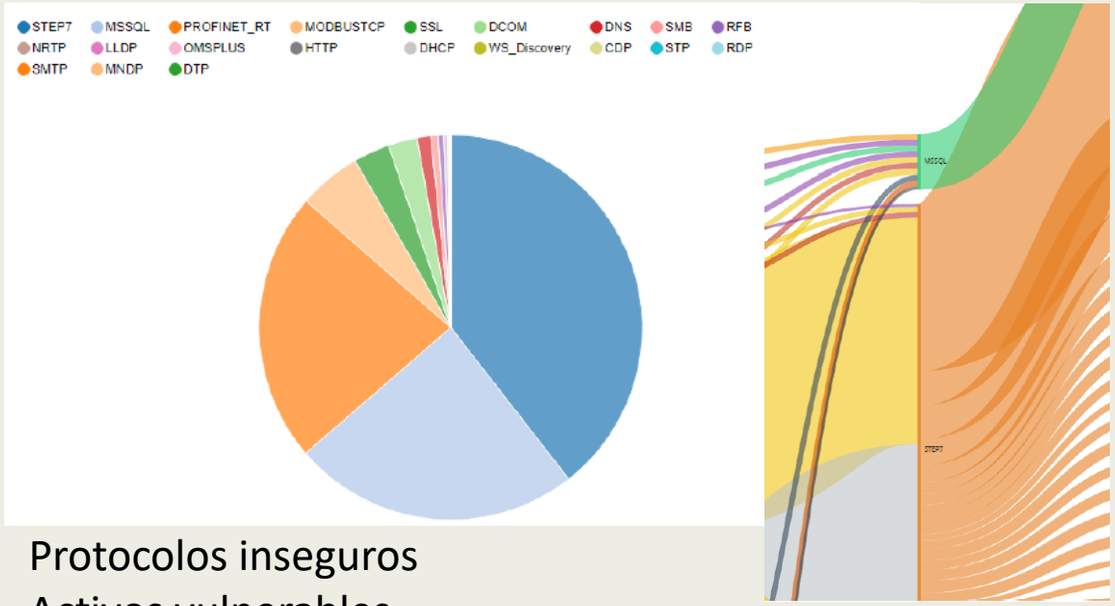
Auditoría

Resultados a obtener

Esta herramienta permite obtener:

- Mapa de red y asignación a niveles Purdue (1,2, 3 para OT)
- Uso de la red por protocolo OT
- Matriz de comunicaciones IP
- Conexiones a IPs públicas maliciosas
- Malas configuraciones en dispositivos
- Problemas de conectividad
- Pérdida de sesiones
- Sistemas "Dual-homed" (con conexión a dos o más redes)
- Programas maliciosos de carácter industrial:
  - Wannacry/NotPetya/Conficker/Industroyer/Triton/Trisis/…
- Violaciones de la arquitectura/pirámide Purdue
- Operaciones potencialmente peligrosas
  - Carga de nuevo Firmware / Conexiones de las estaciones de ingeniería / Cambio de estado en PLCs/RTUs
- Vulnerabilidades conocidas (CVEs) en dispositivos OT

Resultados



- Protocolos inseguros
- Activos vulnerables
- Sistemas fuera de soporte
- Actividad malware y ataques a la red (vectores)
- …

Address	Role	Vendor	Nr. of vuln.	Top vulnerability
10.191.219.204	Master	Siemens	50	10.0 - CVE-2011-4513 - Low - might match affected software/firmware
172.16.20.16	Master		50	10.0 - CVE-2011-4513 - Low - might match affected software/firmware
10.191.219.120	PLC	Siemens (S7-300)	7	7.8 - CVE-2015-2177 - High - matches affected software/firmware and version
172.16.20.51	PLC	Siemens (S7-400)	4	7.8 - CVE-2017-12741 - High - matches affected software/firmware and version

Auditoría

Medidas correctivas

Medidas Correctivas: Son aquellas recomendaciones cuya dedicación y recursos podrían ser poco destacables, podrían implementarse con recursos propios de forma sencilla y requerir un esfuerzo económico bajo. Estas medidas se caracterizan también por no requerir un cambio estructural o de diseño, sino que su aplicación depende principalmente de una reconfiguración de los sistemas afectados. Gran parte de estas medidas tienen su origen en los hallazgos de seguridad encontrados en el análisis de tráfico.

Ejemplos

Medidas correctivas

A continuación, se listan las medidas correctivas, que pueden implementarse de forma más sencilla y sin una gran inversión económica, clasificadas según su nivel de criticidad:

- Crítica:
  - Conformar una política de contraseñas en equipos industriales.
  - Revisar actividad sospechosa y ataques a la red.
- Prioridad alta:
  - Revisar cuentas de usuarios en sistemas industriales.
  - Actualizar *firmware* y *software*.
  - Solucionar vulnerabilidades detectadas.
- Prioridad media:
  - Utilizar protocolos y versiones seguras.
  - Revisar y minimizar flujos de comunicación.
  - Desarrollar diagramas físicos y actualizar diagramas lógicos.
- Recomendable:
  - Bloquear puertos libres de los switches.
  - Revisar etiquetado de cableado y equipos.



Auditoría



Medidas preventivas

Medidas Preventivas: Son aquellas recomendaciones cuya dedicación y recursos podrían ser notables y podrían tener un gran impacto en el diseño de la infraestructura actual o traer consigo el despliegue de soluciones de seguridad o el desarrollo de políticas de seguridad. Estas medidas tienen su origen en los hallazgos de seguridad encontrados tanto en el levantamiento de información realizado mediante la visita y las reuniones de contextualización, como con el análisis de tráfico.

Ejemplos

Medidas preventivas

Se muestran las medidas preventivas que sirven para mitigar los hallazgos encontrados y que van a requerir, en general, un cambio de diseño y/o un esfuerzo, tanto de tiempo, recursos y económico, mayor que el de las medidas correctivas.

A continuación, se listan las medidas preventivas clasificadas según su índole (*administrativas*, relacionadas con controles de gestión de la ciberseguridad; *técnicas*, más ligadas a la implantación de tecnología; y *auxiliares*, de índole variado):

- Cuestiones administrativas:
  - Desarrollar una política de ciberseguridad industrial.
  - Crear una política de copias de seguridad para equipos industriales.
  - Crear una política de actualización de *firmware* y *software*.
  - Revisión de la electrónica de red.
  - Requisitos de seguridad en suministros y nuevos proyectos.
- Cuestiones técnicas:
  - Proteger equipos vulnerables o fuera de soporte.
  - Soluciones de protección antivirus
  - Acceso remoto seguro.
  - Monitorización de la red industrial.
  - Control de medios extraíbles.
  - Control de dispositivos portátiles.
  - Revisar segregación de las redes IT/iDMZ/OT.
  - Creación de directorio activo en red OT.
- Servicios auxiliares:
  - Hacking ético.
  - Consultoría de cumplimiento normativo.
  - Servicio gestionado de seguridad.

Lecturas

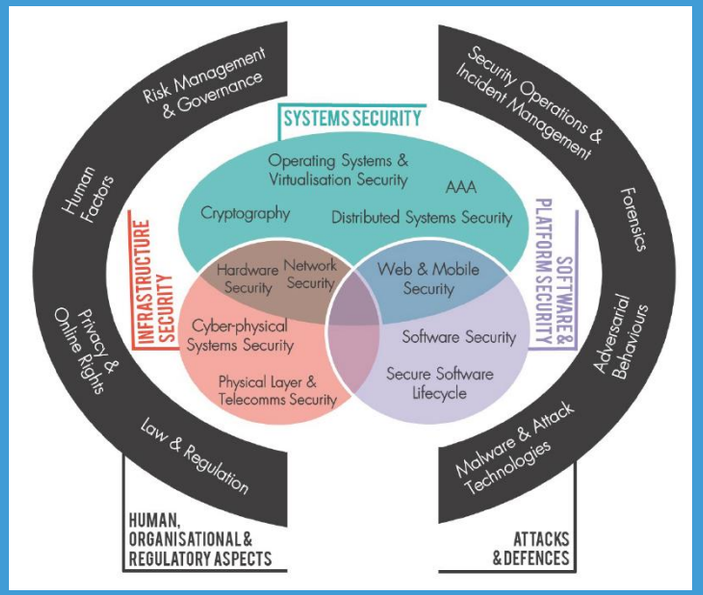
Lecturas recomendadas

CyBOK (The Cyber Security Body Of Knowledge) 1.1 [Julio 2021]

https://www.cybok.org/

https://www.pmmi.org/report/2021-cybersecurity-assess-your-risk

CyBOK



Lecturas recomendadas

"Ciberseguridad Industrial e Infraestructuras Críticas" de @FernandoSevillano y varios autores. [Abril 2021]

CYBERSECURITY
v.1.2 ABRIL 2024

https://www.linkedin.com/in/ricardo-moraleda-gareta-9421099

https://www.linkedin.com/company/gdo-electric1996/

RICARDO MORALEDA GARETA

GDO SOFTWARE