“Arquitecturas de seguridad OT y protección mediante Deception”

Alumno: Alejandro Scatton Lóndero

Plan de estudios: Máster Universitario en Ciberseguridad y Privacidad

M1.887 Seguridad empresarial

Tutor trabajo: Manuel Jesús Mendoza Flores

Profesor responsable asignatura: Víctor García Font

Fecha de entrega: 28 de diciembre de 2021

Dedicatoria:

Gracias a ti Valentina por siempre apoyarme a dar lo mejor de mí.

A mi familia y amigos que siempre me han tendido una mano.

FICHA DEL TRABAJO FINAL

Título del trabajo:	*Arquitectura de seguridad OT y aplicación de mecanismos Deception*
Nombre del autor:	*Alejandro Scatton Lóndero*
Nombre del consultor/a:	*Manuel Jesús Mendoza Flores*
Nombre del PRA:	Víctor García Font
Fecha de entrega (mm/aaaa):	01/2022
Titulación:	*Máster Universitario en Ciberseguridad y Privacidad*
Área del Trabajo Final:	*M1.887 Seguridad empresarial*
Idioma del trabajo:	Castellano
Palabras clave	*Ciberseguridad, OT, Deception*

Resumen del Trabajo (máximo 250 palabras): *Con la finalidad, contexto de aplicación, metodología, resultados y conclusiones del trabajo.*

La finalidad de este trabajo persigue ahondar sobre el estado del arte de un sector que hasta hace no demasiado no era considerado desde el punto de vista de la ciberseguridad: los entornos industriales. Este tipo de entornos se han caracterizado por sufrir una gran evolución en las últimas décadas de forma que se han incorporado multitud de tecnologías que han permitido mejorar los procesos productivos. Sin embargo, esta incorporación de tecnologías, como por ejemplo la incorporación de dispositivos IoT, han traído consigo una serie de amenazas y problemas de seguridad, que en este tipo de entornos una interrupción de la operación puede tener un impacto muy elevado ya que pueden ser infraestructuras críticas para la vida cotidiana.

De forma que se apliquen principios de seguridad básicos como pueden ser defensa en profundidad o segmentación de red se ha definido una arquitectura de referencia en base a estándares del sector como el IEC 62443. Adicionalmente, se ha implantado de manera práctica un entorno industrial virtualizado que ha permitido realizar pruebas con una tecnología como Deception, la cual aporta capacidades avanzadas de detección y permite mejorar las capacidades de ciber inteligencia de las organizaciones.

Las conclusiones del trabajo han sido satisfactorias y han permitido definir esta serie de requisitos de seguridad en torno a una arquitectura de referencia, además de la aplicación de tecnologías deception con un resultado satisfactorio, lo cual permite dilucidad su posible incorporación como un mecanismo adicional de seguridad como parte del ecosistema OT.

Abstract (in English, 250 words or less):

The purpose of this work is to study in depth the state of the art of a sector that until recently was not considered from the point of view of cybersecurity: industrial environments. This type of environment has undergone a great evolution in recent decades, with the incorporation of a wide range of technologies that have made it possible to improve production processes. However, this incorporation of technologies, such as the incorporation of IoT devices, has brought with it a series of threats and security problems, which in this type of environment an interruption of the operation can have a very high impact since they can be critical infrastructures for everyday life.

In order to apply basic security principles such as defense in depth or network segmentation, a reference architecture has been defined based on industry standards such as IEC 62443. Additionally, a virtualized industrial environment has been implemented in a practical way, which has allowed testing with a technology such as Deception, which provides advanced detection capabilities and allows improving the cyber intelligence capabilities of organizations.

The results of the work were positive and have made it possible to define a set of security requirements based on a reference architecture, in addition to the application of deception technologies with a successful result, which suggests its possible incorporation as an additional security mechanism as part of the OT ecosystem.

Índice de contenidos

Índice de Figuras

Índice de Tablas

1. Introducción

1.1 Contexto y justificación del trabajo

En los últimos años se ha puesto de manifiesto la más que latente aparición y continua evolución de nuevas tecnologías las cuales han potenciado y estimulado en muchos aspectos los modelos de negocio de diversos sectores. Adicionalmente, este auge de nuevas tecnologías e interconexión ha producido también la aparición de multitud de problemas de seguridad relativos a la seguridad de la información en cuanto a sus 3 principales pilares: confidencialidad, integridad y disponibilidad. Tanto es así que en el último informe de riesgos globales (World Economic Forum, 2021) elaborado en enero de 2021 la ciberseguridad se perfila como una de las mayores preocupaciones a nivel global a niveles similares con pandemias (gran subida en la clasificación debido al COVID-19), el terrorismo o el cambio climático.

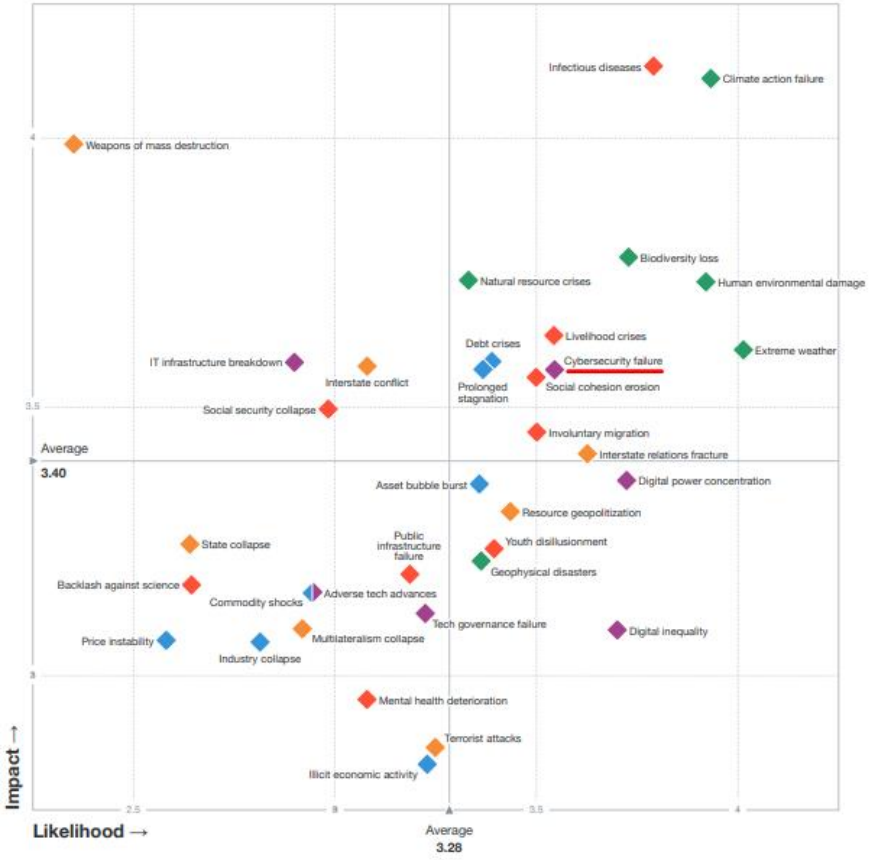

Ilustración 1: Mapa de riesgos globales 2021 por el WEF

Como se puede ver en el gráfico anterior, el fallo en concreto relativo a ciberseguridad se refiere a fallo en cuanto a ciberseguridad y este es una de las mayores motivaciones de este trabajo. En este presente trabajo de fin de máster se pretende ahondar en uno de los sectores más críticos en lo que se refiere a ciberseguridad: el industrial o también conocido como Tecnología Operacional (OT en adelante). Dichos entornos de automatización son los responsables de la producción de distintos elementos, desde artículos de poca importancia vital

como pueden ser cadenas de producción de juguetes hasta fábricas responsables de proporcionar servicios básicos para la vida como plantas de tratamiento de agua, centrales eléctricas o nucleares.

Es por tanto evidente la importancia de proteger de manera adecuada dichos entornos, priorizando especialmente lo que se refiere a la protección de las vidas humanas en el entorno industrial además de garantizar la disponibilidad de la producción, la cual en ocasiones puede ser de una criticidad extremadamente elevada.

A diferencia del sector IT tradicional, los entornos OT tienen un ritmo en lo referido a la seguridad informática totalmente distinto. Se trata de entornos los cuales fueron diseñados hace años para operar de forma aislada, inclusive en algunos casos en localizaciones remotas, poco accesibles[1] o inhóspitas. Sin embargo, fruto de la incorporación de nuevas tecnologías se han sometido a una evolución de interconexión de componentes con el objetivo de optimizar procesos que permitan mejorar la producción. Estos cambios han provocado la sobreexposición de dispositivos sin elementos y mecanismos de seguridad, de forma que se han perfilado estos entornos como muy apetecibles para posibles atacantes, además de por su gran impacto.

Teniendo en cuenta esta situación se han propuesto diversas referencias y normativas con la intención de aumentar la seguridad y resiliencia de estos entornos. Entre ellos destaca el IEC 62443[2], el cual se perfila como uno de los estándares del sector. Adicionalmente se cuenta con el NERC CIP[3] para entornos eléctricos de EE. UU. o la LPIC[4] en España como ley para la protección de entornos críticos. Sin embargo, todos estos requisitos y controles de seguridad en muchas ocasiones se antojan complicados de aplicar al tratarse de entornos los cuales no fueron diseñados siguiendo un método de "*Security by design*" y "*Security by default*" por lo que la aplicación de medidas de seguridad puede provocar afectación directa a la disponibilidad de la información y por ende a la operación.

En base a esta situación, el presente trabajo Final de Máster persigue definir de manera teórica desde un principio una arquitectura de seguridad de referencia para entornos industriales. Dicha arquitectura de referencia girará alineada con las mejores prácticas como las definidas por el IEC 62443, en torno a seguridad en profundidad o modelo Purdue para la definición del flujo de comunicaciones. Esta arquitectura contará con los diversos segmentos de red definidos de forma que se pueda garantizar una segmentación de red basada en cortafuegos, accesos remotos seguros, arquitectura de aplicación de parches y demás funcionalidades empleadas hoy en día por este tipo de organizaciones de modo que se pretende esbozar una arquitectura de referencia teórica que

[1] https://cordis.europa.eu/article/id/430428-overcoming-rough-seas-hurdle-in-offshore-wind-farm-maintenance/es
[2] https://www.isa.org/intech-home/2018/september-october/departments/new-standard-specifies-security-capabilities-for-c
[3] https://www.nerc.com/Pages/default.aspx
[4] https://www.boe.es/buscar/pdf/2011/BOE-A-2011-8849-consolidado.pdf

potencialmente podría ser aplicada en escenarios realistas aplicando los ajustes y cambios necesarios.

De forma que se complemente el trabajo se realizará una virtualización de la red industrial, con las limitaciones propias de la virtualización, donde se probarán una serie de mecanismos adicionales de seguridad y que son considerados medianamente recientes como tecnologías Deception[5]. Estas tecnologías se antojan de gran interés para este tipo de entornos tan críticos al ser muy poco intrusivas y no dependientes de agentes. A nivel corporativo se cuenta con diversos fabricantes, pero para el presente trabajo se aplicarán mecanismos basados en software libre por un abaratamiento de costes, sin que eso afecte a la obtención de premisas del trabajo realizado.

1.2 Objetivos del trabajo

Los principales objetivos que persigue el presente trabajo son los que se describen a continuación:

- Análisis del estado del arte en lo referido a seguridad industrial, OT e IoT y últimas tendencias de seguridad informática.

- Investigación sobre la aplicación teórica de la normativa IEC 62443 3-3 (requisitos de seguridad) además de otras referencias del sector analizado. Dicho análisis e investigación derivará en la definición de una arquitectura de seguridad de referencia para entornos industriales la cual podría ser implantada en entornos de estas características.

- Análisis y aplicación de medidas de protección adicionales, en concreto Deception y su integración en una arquitectura de seguridad de referencia para entornos industriales como la definida. Para ello se efectuará una implementación práctica en un entorno virtualizado basado en herramientas *open source* tanto para la emulación de sistemas industriales como mecanismos de seguridad. Para visualizar los resultados de hallazgos se empleará un cuadro de visualización basado en distintas herramientas *open source*.

- Tras la ejecución de las pruebas prácticas unido al estudio teórico en lo referente al estado del arte de seguridad OT y el uso de tecnologías Deception se podrá aterrizar la viabilidad de estas tecnologías, además de verificar de forma tangible la penetración o no de la seguridad OT en este tipo de entornos.

[5] Applying Deception Technologies and Techniques to Improve Threat Detection and Response

1.3 Enfoque y método seguido

El enfoque aplicado en el presente trabajo se centra en realizar una investigación referente a los estándares de seguridad para el mundo OT de manera que se puedan aunar distintos conceptos de forma que se defina una arquitectura de seguridad de referencia para entornos industriales. Adicionalmente, se realizarán pruebas teórico-prácticas con una tecnología medianamente reciente y en auge como es la de Deception, la cual es también conocida como la evolución de los tradicionales Honeypots.
Debido a la criticidad de estos entornos industriales en los cuales la disponibilidad de la información y la operación son críticas, se plantea la ejecución de forma teórica y práctica hasta el punto de poder obtener conclusiones pero que, a su vez, en caso de aplicación en el mundo real se deberá aplicar con precaución y de forma controlada.

Partiendo de estas premisas podemos diferenciar distintas etapas del trabajo:

1. Investigación del estado del arte en lo referido a ciberseguridad en entornos industriales, incluyendo estándares de referencia y mejores prácticas.

2. Definición de arquitectura de referencia en conjunto con mecanismos de seguridad aplicables.

3. Pruebas técnicas sobre el uso de tecnologías Deception en entornos OT.

4. Análisis final de resultados y obtención de conclusiones.

Las tareas a ejecutar se desglosan en la siguiente sección de este documento.

1.4 Planificación del trabajo y recursos empleados

En base a lo mencionado en puntos anteriores se desglosan a continuación una serie de recursos a emplear como parte del trabajo:

- **IEC 62443:** estándar de referencia para la protección de entornos industriales frente a ciber amenazas, en concreto con la definición de requisitos de seguridad a cumplir de forma que se tenga un nivel aceptable de madurez en ciberseguridad OT. Es posible que se empleen de manera más limitada otros estándares como el NERC CIP, ISO 27001, etc.

- **Oracle VirtualBox:** software de virtualización que permitirá el despliegue de máquinas virtuales y una red local en la cual ejecutar las demostraciones.

- **OpenPLC (Alves 2019):** es un controlador lógico programable (PLC) de código abierto.

- **ScadaBR (Alves 2019):** Sistema de Control de Supervisión y Adquisición de Datos (SCADA) de código abierto que permite crear pantallas interactivas, también llamadas Human Machine Interface (HMI), para sus proyectos de automatización.

- **Ubuntu Server:** servidor basado en Linux que se empleará como dispositivo de la red.

- **Windows Server:** servidor de Microsoft ampliamente utilizado en entornos productivos. Se empleará como dispositivo de la red.

- **Soluciones de seguridad basadas en Deception:** T-Pot [6]y DejaVu[7].

En base a los objetivos descritos anteriormente se desglosan las siguientes tareas en la Tabla 1, encuadradas en la planificación del trabajo. Dicha planificación engloba las tareas necesarias para la consecución satisfactoria de los objetivos del trabajo. Adicionalmente se ha divido en base a las diferentes entregas parciales planificadas como parte de la asignatura, de forma que sea una planificación lógica tanto a nivel de plazos como de objetivos.

ID	Tarea	Inicio	Fin	Jornadas
1	**Definición y plan de trabajo**	**15/09/2021**	**28/09/2021**	**14**
1.1	Definir motivación del trabajo y alcance	15/09/2021	19/09/2021	5
1.2	Definición de objetivos	18/09/2021	20/09/2021	3
1.3	Definición de metodología y enfoque	20/09/2021	22/09/2021	3
1.4	Definición del plan de trabajo	23/09/2021	25/09/2021	3
1.4.1	*Definición de tareas bajo el alcance*	23/09/2021	24/09/2021	2
1.4.2	*Identificación de dependencias*	25/09/2021	25/09/2021	1
1.4.3	*Estimación de tiempos para cada tarea*	24/09/2021	25/09/2021	2
1.5	Análisis de costes y recursos	25/09/2021	27/09/2021	3
1.6	Entrega del Plan de Trabajo: PEC 1	27/09/2021	28/09/2021	2
2	**Investigación y análisis previo**	**29/09/2021**	**26/10/2021**	**28**
2.1	Investigación estado del arte seguridad OT	29/09/2021	03/10/2021	5
2.2	Investigación nuevas tendencias y predicciones	02/10/2021	06/10/2021	5
2.3	Estudio de necesidades del sector	03/10/2021	06/10/2021	4
2.4	Análisis normativas y buenas prácticas	07/10/2021	10/10/2021	4
2.5	Estudio y análisis de tecnologías Deception	11/10/2021	17/10/2021	7
2.5.1	*Estudio de T-Pot y dependencias*	11/10/2021	16/10/2021	6
2.5.2	*Estudio de DejaVu y dependencias*	12/10/2021	17/10/2021	6
2.6	Análisis de posibilidades de virtualización industrial	15/10/2021	20/10/2021	6
2.8	Entrega de memoria actualizada: PEC 2	21/10/2021	26/10/2021	6
3	**Definición e implantación**	**27/10/2021**	**23/11/2021**	**28**
3.1	Adquisición de recursos teóricos y prácticos	27/10/2021	31/10/2021	5

[6] T-Pot: https://github.com/telekom-security/tpotce
[7] Deja-VU Framework: https://github.com/bhdresh/Dejavu

3.2	Definición de arquitectura de referencia	30/10/2021	13/11/2021	15
3.2.1	*Definición de entorno ficticio*	30/10/2021	01/11/2021	3
3.2.2	*Definición de topología de red*	31/10/2021	02/11/2021	3
3.2.3	*Definición de mecanismos implantados*	01/11/2021	05/11/2021	6
3.2.4	*Definición de procedimientos a alto nivel*	04/11/2021	09/11/2021	6
3.2.5	*Incorporación de elementos de seguridad*	03/11/2021	10/11/2021	8
3.2.6	*Documentación y definición de arquitectura*	01/11/2021	13/11/2021	14
3.3	Implantación entorno virtual	10/11/2021	16/11/2021	7
3.3.1	*Preparación de SW de virtualización*	10/11/2021	10/11/2021	1
3.3.2	*Definición de arquitectura de red*	09/11/2021	12/11/2021	4
3.3.3	*Despliegue de dispositivos virtualizados*	12/11/2021	16/11/2021	5
3.4	Implantación tecnologías Deception	14/11/2021	16/11/2021	3
3.5	Simulación de eventos de relevancia	17/11/2021	18/11/2021	2
3.6	Análisis de resultados	18/11/2021	20/11/2021	3
3.7	Documentación y entrega PEC 3	20/11/2021	23/11/2021	4
4	**Presentación**	**24/11/2021**	**28/12/2021**	**35**
4.1	Análisis de resultados	24/11/2021	03/12/2021	11
4.2	Elaboración de conclusiones	30/11/2021	05/12/2021	7
4.3	Preparación de memoria final	28/11/2021	21/12/2021	25
4.4	Elaboración vídeo presentación	17/12/2021	28/12/2021	14
4.5	Preparación presentación	29/12/2021	04/01/2022	8
4.6	Preparación defensa	05/01/2022	14/01/2022	10

Tabla 1: Planificación de tareas

Se adjunta de igual forma en la Tabla 2 la planificación de tareas en forma de diagrama con la planificación elaborada.

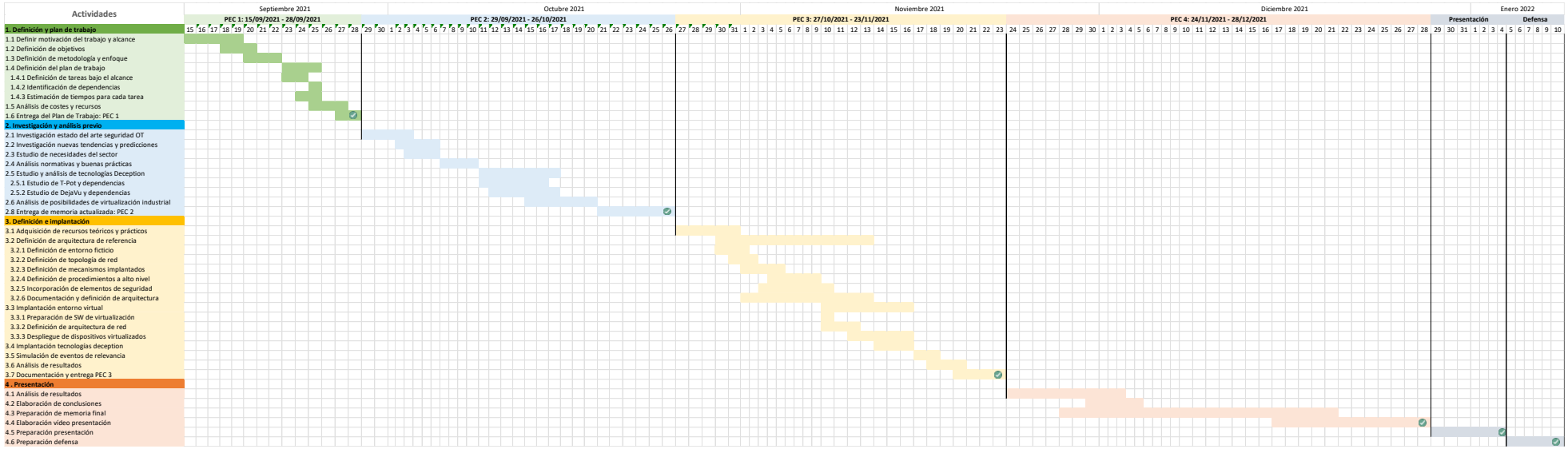

Ilustración 2: Planificación temporal del trabajo

1.5 Breve sumario de productos obtenidos

Como fruto de la ejecución del presente trabajo se pretenden conseguir al menos los siguientes tangibles que permitan extraer una serie de conclusiones que se adjuntarán y analizarán en la presente memoria:

- Investigación y repaso del estado del arte sobre la ciberseguridad industrial.

- Arquitectura de referencia de seguridad para entornos industriales basada en las mejores prácticas y estándares.

- Entorno de simulación virtual donde poder aplicar mecanismos de protección basados en tecnologías Deception.

2. Fase de investigación

En el presente capítulo del trabajo se desglosará la investigación realizada de forma que se cimenten las bases sobre las cuales se definirá posteriormente la arquitectura de referencia junto con la parte práctica focalizada en tecnologías Deception en entornos industriales.

2.1 Ciberseguridad industrial: estado del arte

En los últimos años hemos presenciado un auge tecnológico muy importante ligado a la evolución de la vida humana. Esta gran evolución ha permitido optimizar y automatizar tareas o procesos de forma que a nivel general han derivado en una mejora de la calidad de vida de las personas y una evolución de los modelos de negocio. Unido a esta evolución tecnológica también hemos asistido al desarrollo de problemas de seguridad informática asociados a esta evolución, desde los primeros virus informáticos como *Creeper* por el principio de la década de 1970, pasando por el auge de los gusanos de los 2000 hasta el modelo actual de RaaS (Ransomware as a Service).

Es evidente por tanto que la seguridad informática cobra una gran relevancia en los últimos años, especialmente focalizada en proteger la información desde los 3 principales pilares de esta:

- Confidencialidad
- Integridad
- Disponibilidad

Para ello además de la aplicación de medidas técnicas para proteger la información también se han desarrollado normativas y procedimientos de gran importancia como el Reglamento General de Protección de Datos (GDPR[8]) para la protección de datos de carácter personal a nivel europeo o la normativa HIPAA[9] para la protección de datos personales médicos en Estados Unidos.

Sin embargo, esta serie de normativas, regulaciones y tendencias se definen de manera general para entornos conocidos como tradicionales de IT (Tecnología de la Información) y en el presente trabajo nos focalizaremos en otra vertiente distinta a IT, pero con un componente tecnológico cada vez mayor: el sector OT (Tecnología Operacional) o también conocido como industrial y en algunos casos inclusive de infraestructuras críticas.
Es importante reseñar que en este entorno se diferencia de manera muy clara la seguridad relativa a la seguridad de las personas y medioambiente, conocido en el lenguaje anglosajón como *Safety*, está presente prácticamente desde la concepción de este tipo de entornos y por otro lado la seguridad de tipo *ciber*, la

[8] https://gdpr.eu/
[9] https://www.hhs.gov/hipaa/index.html

cual ha entrado con fuerza en este tipo de entornos en los últimos años debido a la evolución tecnológica antes comentada.

De forma que podamos comprender como se ha puesto el foco en la ciberseguridad en OT pasaremos a desglosar el cómo hemos llegado hasta la situación actual fruto de la revolución industrial.

2.1.1 Revolución industrial e industria 4.0

De forma que podamos entender el escenario actual pasaremos a desglosar la revolución industrial que nos ha traído hasta aquí a la denominada Industria 4.0 de nuestros días, caracterizada por su alto componente tecnológico y específicamente ligado a la transformación digital.
Para llegar a la conocida como Industria 4.0 ha habido una serie de evoluciones y cambios que han provocado diversos impactos de gran calado en la sociedad, los cuales desglosaremos a continuación de manera resumida.

Sobre la década de 1770 se define el punto de partida de la conocida como revolución industrial basada esencialmente en la maquinaria de vapor, la cual se extenderá por aproximadamente 100 años. Este hito produjo importantísimos cambios en la sociedad fruto de un cambio de paradigma: pasar de una economía basada en tareas manuales (focalizadas en la agricultura) a un engranaje medianamente mecanizado y con miras a la industrialización que se produciría más adelante en mayor medida.

Posteriormente, sobre el año 1870 se da el pistoletazo a la siguiente revolución industrial la cual también tendría una duración de unos 100 años y pivotaría principalmente sobre la electrificación de los procesos y por ende del despliegue de las conocidas como cadenas de producción y las primeras cadenas de ensamblado para tareas automáticas y repetitivas. El ejemplo más claro de esta serie de cambios profundos lo podemos ver en la compañía norteamericana Ford[10], la cual desplegó uno los sistemas de ensamblado más revolucionarios de la época en la ciudad de Detroit – EE. UU. para la producción en masa de sus vehículos.

Tal y como se comentó anteriormente, unos 100 años después sobre la década de 1970 se produce la conocida como tercera revolución industrial ya mucho más cercana a lo que conocemos hoy en día como procesos de fabricación, al tratarse de la incorporación de sistemas informáticos en los procesos industriales. Estos mecanismos permiten automatizar más procesos, además de empezar el proceso de digitalización de este tipo de entornos el cual tendrá su gran explosión más adelante.
Su principal valedor y figura elemental gira en torno a un pequeño dispositivo conocido como “controlador lógico programable” o mejor conocido por sus siglas: PLC. Estos pequeños dispositivos permitieron sustituir los mecanismos

[10] https://corporate.ford.com/articles/history/moving-assembly-line.html

electromecánicos de relés para el control de procesos por un único dispositivo programable según la necesidad de cada momento y especialmente diseñado para entornos industriales, con medidas de protección físicas contra polvo o temperaturas extremas. Es importante reseñar que estos dispositivos se utilizan a gran escala hoy en día en los procesos industriales de forma que controlan dichos procesos y actúan sobre ellos en base a las señales que se recogen mediante sensores o dispositivos similares.

En la siguiente imagen podemos ver uno de los últimos modelos de PLC de uno de los principales fabricantes del mercado. Entre sus novedades destaca su conexión a entornos en nube, lo cual le permite disminuir la dependencia de almacenamiento local en tarjetas SD, pero por contraparte puede acarrear múltiples problemas de seguridad fruto de esta digitalización.

Ilustración 3: PLC Logo Mini de Siemens

Tras estas tres primeras iteraciones de revoluciones industriales llegamos al siglo XXI actual, en el cual se produce una gran evolución relativa a nuevas tecnologías como la expansión de conectividad y velocidad de Internet, tecnologías inalámbricas o dispositivos móviles en primera instancia y llegando hasta vertientes muy específicas como puede ser la Robótica, la Inteligencia Artificial, el Big Data o el IoT. La piedra angular que caracteriza esta cuarta revolución industrial radica en el paradigma conocido como PDP, es decir *physical to digital & digital to physical*[11], el cual está estrechamente ligado con la transformación digital de las empresas. De este modo, lo que se pretende es recoger información del mundo físico y posteriormente trasladarla al mundo digital de forma que esto potencie el negocio de una manera determinada, como podría ser la lectura de velocidad de una línea de ensamblado con ciertos parámetros de forma que sea posible obtener de manera objetiva y automatizada unos valores relativos a la optimización del proceso en cuestión. En

[11] https://www2.deloitte.com/us/en/insights/focus/industry-4-0/challenges-on-path-to-digital-transformation/physical-digital-physical-loop.html

consecuencia, gracias a ese análisis digital de la información, por ejemplo, mediante tecnologías tipo Big Data, se podrá trasladar una acción al mundo físico (*digital to physical*) lo cual derivará en última instancia en una mejora del proceso y por tanto potencialmente en una mejora de la operación y del modelo de negocio.

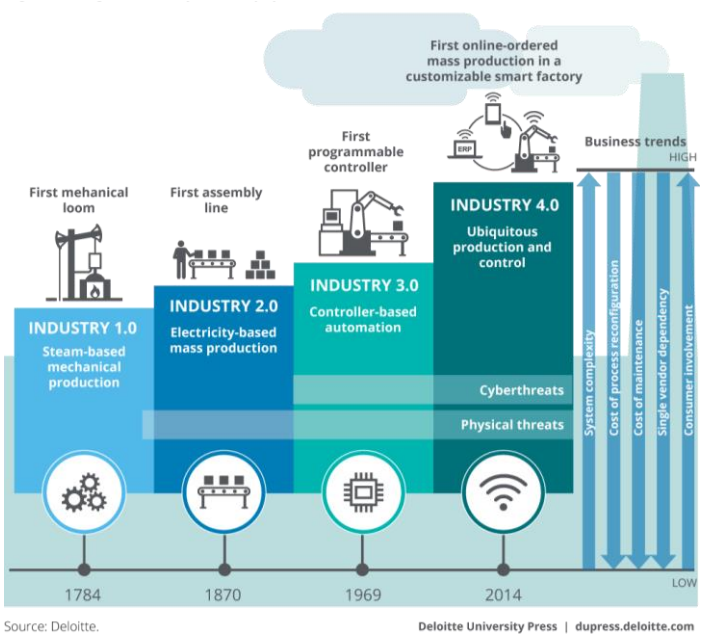

Ilustración 4: Revoluciones industriales (Deloitte, s.f.)

Vemos por tanto que, para llegar hasta el escenario actual, los entornos industriales han evolucionado enormemente desde su concepción hace ya más de 200 años con el nacimiento de la revolución industrial, pasando por distintas épocas las cuales han tenido un impacto directo de dicha revolución industrial.
Actualmente se emplea el término “Industria 4.0” o 4ta revolución industrial, dicho concepto fue utilizado por primera vez en Alemania sobre el año 2014 y se refiere en concreto a la convergencia de los sistemas industriales tradicionales con la nueva época de hiper conectividad que se vive a nivel tecnológico. Dicho escenario permite una mejora de los resultados vía la optimización de la operación gracias a estas nuevas tecnologías y se nos presentan ahora como “fábricas inteligentes”.

Esta gran digitalización e implementación de conectividad en los entornos industriales viene a consecuencia de la mejora de procesos, los cuales se han visto en gran medida beneficiados de esta evolución tecnológica, pero a su vez, también se ha producido una exposición de este tipo de entornos, usualmente aislados, lo cual ha permitido la aparición de multitud de problemas de seguridad de la información que se utiliza en los entornos OT.
Tal y como se mencionó anteriormente, esta gran evolución y digitalización de los entornos industriales trajo consigo un aumento considerable en los problemas relativos a la seguridad de estos entornos. Este tipo de problemas son la principal motivación del presente trabajo y por ende ahondaremos un poco más en ello.

En el siguiente diagrama podemos ver de manera resumida la evolución de las ciber-amenazas más conocidas y su relación con la evolución tecnológica desde los años 1970 hasta la actualidad, lo cual esboza de manera clara que son dos vertientes que avanzan de manera sincronizada y paralelamente:

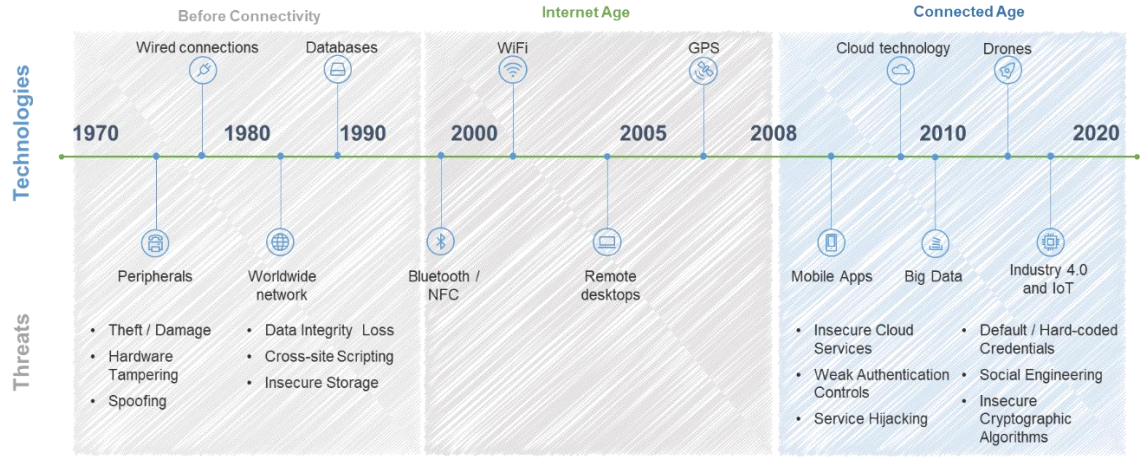

Ilustración 5: evolución tecnológica y de amenazas asociadas

En el siguiente capítulo repasaremos de manera breve la relación de ciberataques con este tipo de entornos, las principales motivaciones, consecuencias y de este modo podremos comprender la vital importancia de proteger de manera segura los entornos OT.

2.1.2 Recientes incidentes relevantes: de Stuxnet a Colonial Pipeline

Como se ha mencionado anteriormente, la conocida como Industria 4.0 ha permitido optimizar procesos hasta tal punto de considerarse hoy día el término “fábrica inteligente”. Sin embargo, esta etapa de digitalización del sector industrial debe conllevar, de manera natural, también una evolución asociada a medidas de ciberseguridad y es en este punto donde radica la importancia de este trabajo.

Estos entornos industriales, en muchas ocasiones, son entornos con décadas en funcionamiento, con equipos y elementos pensados para su durabilidad y fiabilidad. Dichos dispositivos en muchos casos no han sido pensados para el escenario de hiper conectividad de la Industria 4.0 y en ese intercambio de información que se realiza entre los mundos físicos y digitales es donde surge la necesidad de aplicar mecanismos de ciberseguridad para proteger, en primera instancia la seguridad de las personas, tanto en el propio entorno como las que requieren el servicio proporcionado, y en segunda instancia la información como tal y por ende el negocio.

Este intercambio de información es un concepto vital para comprender este escenario, ya que la consecuencia de ello es la convergencia progresiva del mundo OT con el mundo de IT, tanto a nivel de conectividad como de hardware, sistemas periféricos, aplicaciones y software, entre otros.

Los ataques a este tipo de entornos en muchas ocasiones no se publican para evitar una afectación a la reputación de la empresa atacada, sin embargo, mediante regulaciones del sector y por como son este tipo de ataques se van conociendo cada vez más.

Se suele marcar como punto de partida de los ciberataques a entornos industriales el conocido como Stuxnet[12], acaecido durante el periodo entre 2005 y 2010, año en que salió a la luz pública, aunque aún hoy en día existen gran cantidad de detalles sin confirmar sobre este ataque, incluyendo teorías sobre el verdadero autor de este, llegando a involucrar a gobiernos y agencias como la NSA o la CIA.

El ataque en cuestión tuvo lugar en las instalaciones y fábricas encargadas de la producción nuclear de Irán y su impacto fue bastante elevado ya que derivó en la parada de las centrifugadoras encargadas del enriquecimiento de uranio. El origen del ataque fue un USB que contenía un gusano el cual una vez dentro de la red industrial era capaz de replicarse y afectar específicamente a los sistemas SCADA y PLCs empleados para la automatización de procesos. Dicho gusano modificaba el flujo de información entre los sensores/actuadores y los propios PLCs de forma que se enviaban comandos erróneos sin que fuese posible detectarlos, los cuales en última instancia provocaban un sobrecalentamiento de las centrifugadoras las cuales acabaron quemándose y en consecuencia autodestruyéndose.

En este escenario vemos claramente una afectación a la integridad de la información, de modo que los comandos enviados y recibidos por los sensores y actuadores fueron vulnerados de modo que se perdió la visibilidad real del proceso mediante la toma de control de la programación de los PLCs. Sin embargo, el fin último era afectar a la disponibilidad de la operación, lo cual fue conseguido en este caso con éxito ocasionando graves pérdidas económicas y un impacto mediático enorme.

[12] https://www.mcafee.com/enterprise/en-us/security-awareness/ransomware/what-is-stuxnet.html

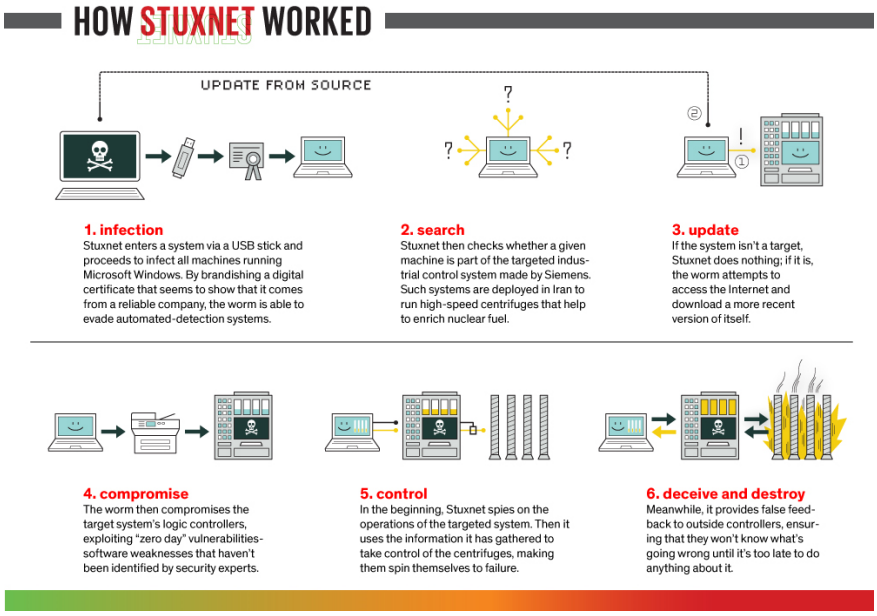

Ilustración 6: Flujo de ejecución de Stuxnet por IEEE Spectrum

Es este último punto de especial importancia, ya que como se ha mencionado anteriormente, nos encontramos en un momento de convergencia entre el mundo IT y el mundo OT. Dicha convergencia sin embargo tiene diversos aspectos que diferencian ambos entornos, especialmente relevante por ejemplo la priorización de la disponibilidad en la práctica totalidad de los casos en los entornos OT, en comparación con los entornos IT en los cuales la confidencialidad de la información suele ser la prioridad.
El motivo por el cual la disponibilidad es absolutamente prioritaria en estos entornos es evidente: si la operación se detiene hay un impacto económico y en ocasiones incluso puede escalar a haber un impacto a la vida de las personas, de manera más o menos directa. Para ello repasaremos de manera breve otro de los ciberataques más recientes a este tipo de entornos, el cual tuvo lugar en 2021 en Estados Unidos: Colonial Pipeline.

Entre finales del mes de abril y principios del mes de mayo de 2021 se produjo un ciberataque a un entorno industrial el cual derivó en una afectación directa a la vida de las personas de una zona geográfica bastante amplia. La compañía afectada en cuestión fue Colonial Pipeline la cual es la responsable del mayor oleoducto de combustible de todos los Estados Unidos, en concreto casi el 50% del combustible de la costa este, por lo que como es de imaginar la correcta operación de dicha compañía y su sistema de oleoductos es vital para el funcionamiento tanto a nivel económico como social de una extensión de terreno enorme como se puede ver a continuación:

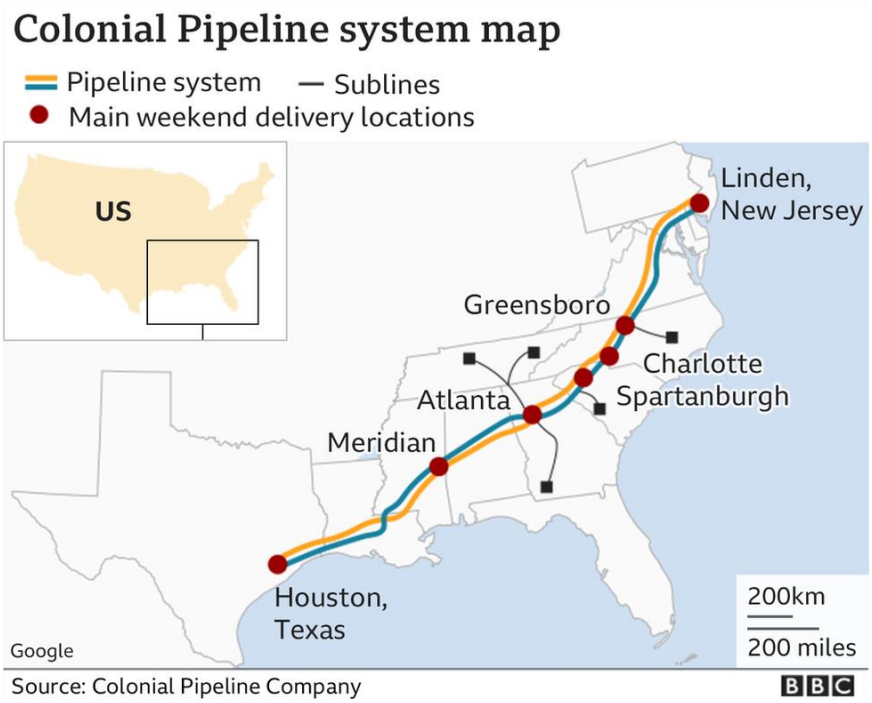

Ilustración 7: Oleoducto afectado de Colonial Pipeline por BBC

Tras una parada en la operación de varios días se desató una situación de caos social en esta gran zona geográfica, provocando que las personas acudiesen en masa a por combustible por una posible interrupción del suministro y disparando su precio a máximos valores[13], todo ello provocando situaciones de violencia en las calles, además del evidente perjuicio económico directo a Colonial Pipeline y empresas dependientes de este servicio.

A nivel técnico, de acuerdo con el informe especializado emitido por Mandiant FireEye[14], vemos que lo que ocurrió en este entorno fue un ataque de tipo Ransomware lo cual cifró la información de la compañía y produciendo por tanto una interrupción del servicio, para evitar una afectación mayor mediante la propagación del malware y una pérdida de datos (potencialmente irreversible) se procedió a parar la operación apagando los sistemas.

En este caso podemos aspectos muy interesantes que reflejan la evolución tecnológica acaecida en los últimos años. Por ejemplo, se ha llegado a determinar que el autor del ataque es un actor denominado “Darkside”, es decir una organización de ciberdelincuentes altamente especializados y que explotan estos ataques como un modelo de negocio. Dicho modelo de negocio en los últimos años pivota en una de las tendencias más importantes como es el Ransomware, derivando incluso al escenario actual en el que tenemos lo que se denomina RaaS: Ransomware as a Service.

[13] https://www.infobae.com/america/fotos/2021/05/13/largas-filas-y-estaciones-cerradas-en-el-sudeste-de-estados-unidos-por-la-escasez-de-combustible-tras-el-ciberataque-al-mayor-oleoducto/

[14] https://www.zdnet.com/article/darkside-the-ransomware-group-responsible-for-colonial-pipeline-cyberattack-explained/

Sin embargo, a pesar de ser de una alta especificación el perfil del actor, es especialmente interesante el “kill-chain” seguido en este incidente de seguridad ya que vemos que el vector de ataque empleado se basa en una consecución de problemas de seguridad que en el mundo IT se podrían considerar básicos:

- El acceso de los atacantes se produjo empleando mecanismos de acceso remoto vía VPN.
- Las credenciales empleadas para acceder no fueron desactivadas en su momento y se piensa que fueron obtenidas en un dump de contraseñas de la Dark Web.
- No se contaba con un segundo factor de autenticación para dicho acceso remoto.
- La segmentación de la red no era lo suficientemente robusta como para impedir el acceso a máquinas con vulnerabilidades conocidas ni prevenir la propagación del Ransomware.

Tras las labores de respuesta ante incidentes por parte de la compañía se recuperó de manera progresiva la operación hasta niveles normales tras una parada superior a una semana. Adicionalmente al enorme coste asociado a esta parada forzosa hay que sumar aproximadamente 5 millones de dólares pagados en criptodivisas a los atacantes para el desencriptado de la información.

Hemos visto por tanto como la ciberseguridad en entornos industriales es algo crítico para tener en cuenta hoy en día, tanto por su impacto económico, pero sobre todo por su impacto en el mundo físico, tanto a nivel de seguridad de las personas como de impacto a nivel de suministros básicos para la sociedad.
Se podría resumir en los siguientes puntos el motivo por el cual este tipo de ataques están en auge[15] desde el punto de vista de ciber atacantes:

- La creciente madurez de entornos IT ha provocado que muchos atacantes migren de manera progresiva a este tipo de entornos OT al ser más susceptibles en un principio de sufrir un ciberataque.
- Son ataques con un gran poder de impacto y notoriedad, lo cual los perfila como idóneos para atacantes asociados a ciberterrorismo o hacktivismo.
- Al tratarse de entornos en los cuales la gran mayoría no están preparados con mecanismos de seguridad avanzados ni fueron diseñados con este propósito en mente, suelen ser potencialmente más vulnerables por posibles atacantes.

[15] https://www.infosecurity-magazine.com/news/third-industrial-control-systems/

2.1.3 Arquitectura y elementos principales de un entorno OT

Tras haber visto la importancia y el impacto tan grande que puede acarrear un ciberataque en este tipo de entornos procedemos en la presente sección a explicar unas breves pinceladas sobre cómo es una típica arquitectura industrial según los estándares. Es importante tener en cuenta que esto no puede ser considerado como una norma ya que dependiendo de cada sector (eléctrico, renovables, producción de materias primas, etc.) se emplean una serie de mecanismos y elementos propios los cuales acarrean cambios en la propia arquitectura del entorno para adecuarlo a su operación.

En el sector industrial se emplea la denominada "pirámide de automatización" propuesta por la ISA95 (International Society of Automation[16]) la cual se desglosa en 5 niveles en el cual se efectúan distintas tareas y donde se integran las tecnologías OT con las tecnologías IT:

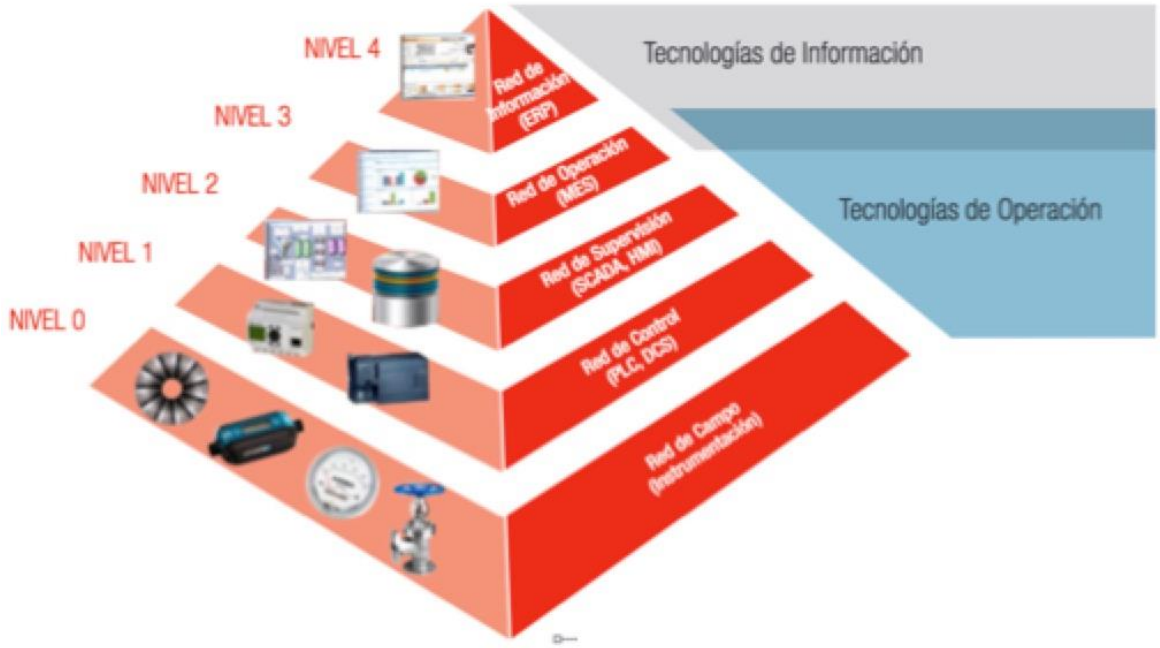

Ilustración 8: Pirámide de automatización ISA95 por el CCI

Si analizamos por niveles:

- **Nivel 0 - Red de campo:** el cual es el que se encuentra en relación directa con el proceso industrial en cuestión. Por este motivo en este nivel se encuentran multitud de dispositivos de distintos fabricantes y con cada vez más funciones pero que en esencia se basa en 2 grandes grupos, los sensores por un lado y los actuadores por el otro.

[16] https://www.isa.org/standards-and-publications/isa-standards/isa-standards-committees/isa95

Los sensores se encargan de recoger información del proceso, como puede ser temperatura, velocidad, presión, nivel de líquido y un casi infinito etcétera. Por su parte los actuadores, mediante señales enviadas de capas superiores ejecutan acciones sobre el proceso vía señales de control con válvulas, aperturas o cierres de compuertas, relés eléctricos, entre muchos otros.

- **Nivel 1 – Red de control:** en este nivel el elemento más representativo y del cual ya hemos hablado anteriormente es el PLC el cual actúa como el controlador del proceso recibiendo valores por parte de los sensores del nivel 0 y enviando señales a los actuadores del mismo nivel en consecuencia. Como se puede deducir su labor es muy importante ya que en base a su funcionamiento el proceso hará una cosa u otra y es por este motivo por el cual es uno de los elementos críticos a proteger.

- **Nivel 2 – Red de supervisión:** pasamos al 2do nivel de la pirámide de automatización la cual es la que mediante aplicaciones recoge datos operativos del proceso, lo visualiza y actúa en consecuencia modificando u operando. Este tipo de operación es la que se realiza mediante los sistemas SCADA y la visualización del proceso mediante los conocidos como HMI (*Human-Machine Interface*).

- **Nivel 3 – Red de operación:** en este nivel nos encontramos con un sistema típicamente denominado MES (Manufacturing Execution System) el cual permite registrar el histórico de ejecución del proceso de capas inferiores. Es por ello por lo que su labor va especialmente dedicada a analizar la operación y verificar que su ejecución es correcta y optimizada de acuerdo con el negocio.

- **Nivel 4 – Red de información:** categorizado de esta forma al ser el más IT de los niveles de la pirámide. Su objetivo principal es alimentarse de la información generada en niveles inferiores y almacenada en el nivel 3 mediante los "*Historians"* de procesos, para ello emplean plataformas de tipo ERP (Enterprise Resources Planning) de forma que se integren con el negocio y su evolución, planificación, gestión, etc.

Una vez desglosados y explicado los distintos niveles de automatización, es importante reseñar también que en este tipo de entornos industriales los protocolos empleados no son iguales a los del mundo IT. En su mayoría hablamos de protocolos simples, sin grandes medidas de seguridad (como cifrado o autenticación) y cuya prioridad es la sencillez y velocidad para garantizar la mejor operación.
Los protocolos más extendidos en este sector son Modbus y OPC. Modbus por su parte funciona en un esquema maestro-esclavo y sus orígenes se remontan al año 1979 lo cual evidencia su estrecha relación con el auge los PLCs que hemos comentado previamente. Los protocolos más comunes son el conocido

como RTU y la variante propia para TCP/IP. Al ser un protocolo maestro-esclavo tiene limitaciones en base a que la comunicación siempre se origina del maestro, a pesar de que pueda surgir algún evento a notificar. Por otro lado, los principales problemas de seguridad vienen referidos a la ausencia de mecanismos de autenticación además de protección de la integridad de la información.
Por otro lado, está el otro protocolo más extendido: OPC. Este por su parte, originalmente basado en tecnología Microsoft, opera en un modelo cliente-servidor. Su principal ventaja es la abstracción que ofrece a través de software unificado, lo cual minimiza los problemas por hardware diverso y entornos con elementos heterogéneos. El principal problema de seguridad de este protocolo radica en el intercambio de usuarios y contraseñas de dispositivos vía protocolo DCOM, lo cual es vulnerable a una serie de problemas de seguridad como pueden ser los hashes NTLM o tickets de Kerberos.

Fruto de la evolución del estado de la seguridad, ambos protocolos han sufrido variaciones y evoluciones en los últimos años como por ejemplo la incorporación de TLS a Modbus o la versión OPC UA la cual permite añadir ciertas funcionalidades de seguridad como cifrado SSL. En el presente trabajo no se entrará más en detalle sobre protocolos industriales ya que no es el objetivo de este, sin embargo, como recomendación de seguridad siempre se debe optar por emplear protocolos seguros y si ello requiere llevar a cabo una migración de hardware gestionarla en consecuencia siempre que sea posible.

Por tanto, hemos visto a alto nivel cómo funciona un entorno industrial de acuerdo con la ISA95, ahora pasaremos a ver como se lleva a cabo esta integración entre el mundo IT y el mundo OT lo cual ha derivado en lo que se conoce como la convergencia entre entornos, tanto para la optimización de la operación como para la inclusión de nuevos riesgos. Estos nuevos riesgos es la principal motivación de las normativas y buenas prácticas aplicables que desglosaremos en el siguiente capítulo.

2.2 Ciberseguridad industrial: normativas y tendencias

Los entornos industriales son entornos muy distintos a los tradicionales de IT y es por este motivo que la aplicación de mecanismos de ciberseguridad no se puede realizar de manera análoga.
Si analizamos ambos entornos vemos las siguientes diferencias las cuales justifican una dedicación especial a los entornos OT:

Entorno IT	Entorno OT
Prioridad: Confidencialidad	Prioridad: Disponibilidad
Ciclo de vida: corto, 2-3 años	Ciclo de vida: largo, hasta 20 años
Cultura de análisis de riesgos implantada	Cultura de análisis de riesgos como tarea no prioritaria
Aplicación de parches y actualizaciones de manera periódica y automatizada	Aplicación de parches y actualizaciones muy reducida y compleja sin afectar a la operación

Mecanismos de protección avanzados: EDR, Zero Trust, etc	Mecanismos de protección inexistentes o muy básicos
Normativas: definidas e implantadas	Normativas: específicas y a veces no aplicadas
Capacidades de ciberseguridad elevadas: respuesta ante incidentes, forense, auditorías, etc	Capacidades de ciberseguridad muy limitadas: solo aplicadas cuando es necesario y priorizando siempre la disponibilidad

Tabla 2: Ciberseguridad IT vs OT

Pasamos ahora a desglosar las normativas de referencia de este sector, al igual que para entornos IT se tienen regulaciones como GDPR para la protección de datos personales o HIPAA para la salvaguarda de datos médicos en los EE. UU., existen una serie de marcos de controles, regulaciones y guías de buenas prácticas específicas para entornos OT las cuales desglosamos a continuación:

- **IEC-62443:** originalmente denominado ISA 99 al ser generado inicialmente por la International Society of Automation. A partir del año 2009/2010 pasa a denominarse ANSI/ISA-62443 evolucionando hasta lo que conocemos a día de hoy como IEC 62443, una serie de documentos e informes técnicos especializados para ciberseguridad en entornos OT, aunque muchos presentan un estado de desarrollo continuo y publicaciones limitadas a modo de borrador. El enfoque principal de la misma es reducir los ciber-riesgos que puedan afectar a este tipo de entornos y sus activos.

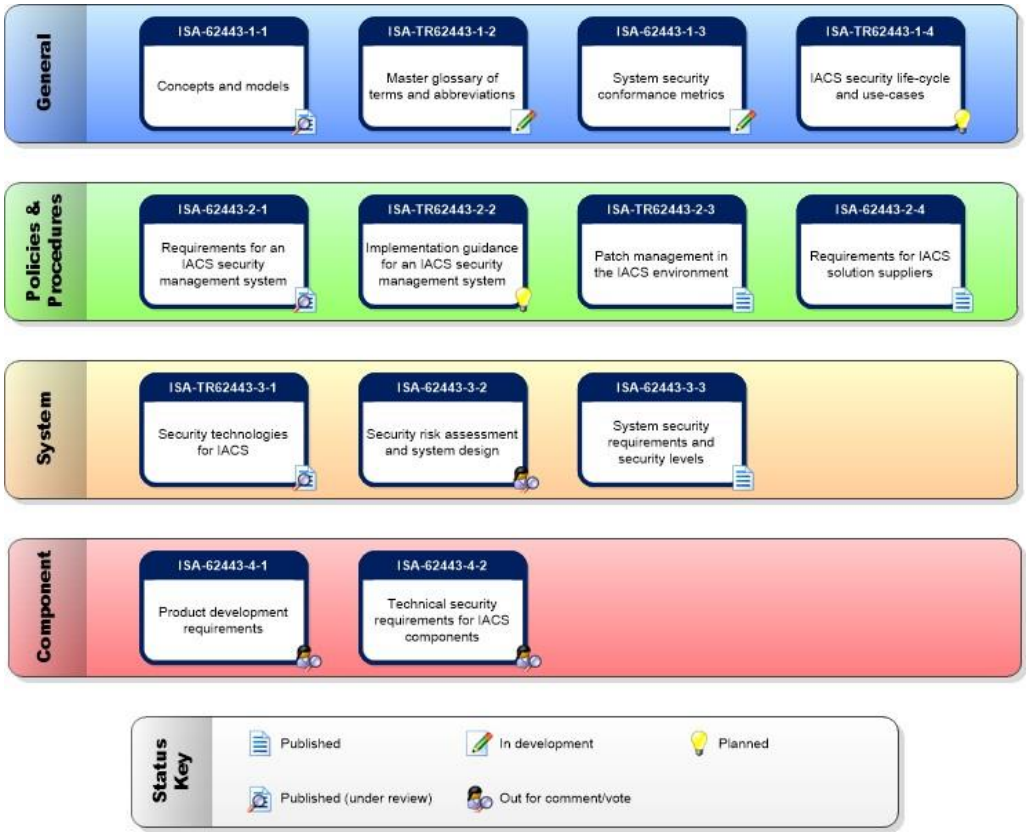

Ilustración 9: IEC-62443 estado de la norma

Como vemos en el diagrama anterior solo se encuentran en estado publicado 3 documentos, 2 correspondientes a políticas y procedimientos:

- 2-3: Gestión de parches en entornos industriales y de automatización
- 2-4: Requisitos para proveedores de soluciones industriales y de automatización

Por otro lado, se encuentra publicado otro referido a la sección de sistemas, la cual es la que más emplearemos en el presente trabajo:

- 3-3: Requisitos de seguridad de los sistemas y niveles de seguridad

Es importante destacar de igual forma que el IEC 62443 se desarrolla en base a dos pilares principales:

- **Defensa en profundidad:** tal y como se aplica en entornos IT de forma que se pueda aportar una capacidad de redundancia a las medidas de seguridad aplicadas.
- **Definición de zonas y conductos:** agrupando activos en zonas para las cuales las medidas de seguridad son iguales en base a los niveles de seguridad definidos. Por su parte los conductos se denominan a la agrupación de elementos que permiten comunicación entre distintas zonas de forma limitada.

Actualmente es posible estar certificado en esta norma para un entorno industrial concreto, tanto a nivel de procesos como de sistemas o productos.

- **NIST SP 800-82:** titulado como "*Guide to Industrial Control Systems ICS Security*" se perfila como uno de los estándares de facto del sector. Incluye controles de como *securizar* entornos OT incluyendo sistemas SCADA, Sistemas de Control Distribuidos y PLCs. Adicionalmente aporta distintas topologías de sistemas ICS, identifica amenazas típicas y proporciona recomendaciones y contramedidas para mitigar los riesgos asociados.

- **NERC CIP:** se trata de un estándar específico para empresas del sector eléctrico en EE. UU., sin embargo, debido a su contenido y expansión se utiliza como referencia de seguridad para entornos industriales de diversa índole. La norma es bastante extensa al tratarse de la protección de entornos especialmente críticos y se desglosa en 12 secciones de diferente naturaleza desde seguridad física hasta protección de la cadena de suministro.

- **LPIC:** a nivel nacional en España nos encontramos con la Ley de Protección de infraestructuras críticas la cual permite catalogar el conjunto de infraestructuras categorizadas como prestadoras de servicios

esenciales de la sociedad y por otro lado diseñar un plan con medidas de prevención y protección para dichos entornos.

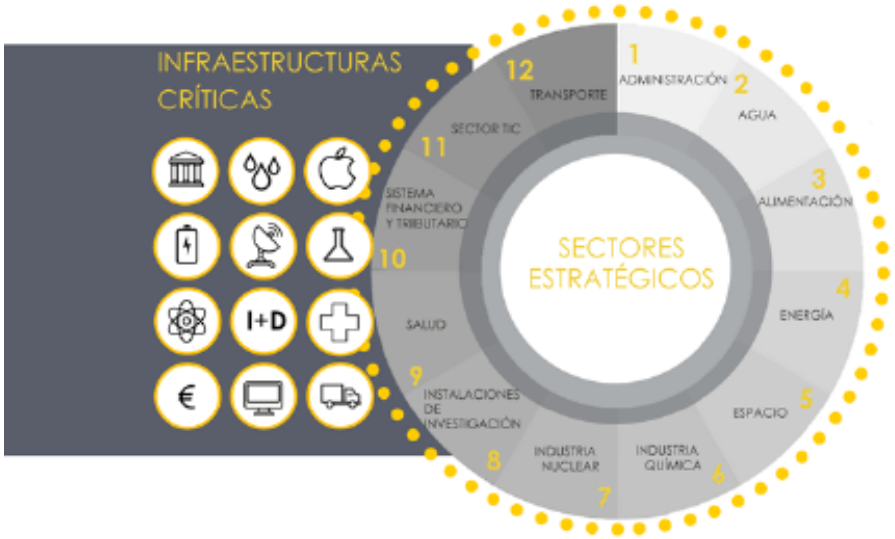

Ilustración 10: Infraestructuras críticas ENS 2017

Si acudimos a mecanismos de seguridad recomendados en entornos industriales debemos tener en cuenta por tanto que es un entorno distinto al IT y su ritmo de evolución es diferente. Por ello en muchas ocasiones uno de los primeros pasos a ejecutar para empezar a pensar en *securizar* un entorno industrial pasa por llevar a cabo un descubrimiento de activos. Aunque parezca sorprendente, esta es una carencia bastante común en este tipo de entornos y debe ser considerado como el paso inicial ya que es muy complejo proteger de manera efectiva un entorno sin saber previamente lo que se está protegiendo.

Posteriormente, las demás medidas de seguridad pasan por aplicar mecanismos basados en defensa en profundidad, desde definición de políticas y procedimientos, hasta aplicación de medidas de bastionado pasando por un elemento vital en este tipo de entornos como es la seguridad física. Adicionalmente, es de gran importancia establecer un procedimiento de actualización y aplicación de parches, definiendo ventanas de tiempo para su aplicación de forma que afecte lo menos posible a la operación y siempre de la mano de los fabricantes de dispositivos industriales de forma que se cuente con su aprobación previa y se disponga de mantenimiento y soporte por su parte.
En los casos en los que no sea posible aplicar una migración o actualización se deberán aplicar medidas compensatorias que permitan minimizar el riesgo de sufrir un problema de seguridad en dicho activo. Es importante reseñar que este escenario de migración o actualización no posible es más frecuente de lo que podría parecer al tratarse de entornos desplegados en ocasiones hace más de 20 años, basados en software o hardware que en algunos casos no cuentan con soporte e incluso pertenecientes a empresas que han desaparecido con el paso del tiempo.

Una de las medidas de seguridad más extendidas y recomendadas es la referida a aplicar una segmentación de red en la fábrica, de forma que no se cuente con una arquitectura plana a nivel de comunicación y se establezcan flujos de comunicación limitados mediante cortafuegos. De este modo, para el caso de dispositivos conocidos como *legacy* se recomienda desplegar un segmento de red dedicado lo más aislado posible, en el cual se localizarán dichos dispositivos vulnerables y desactualizados con la menor interacción posible. Este mecanismo suele denominar como "microsegmentación".
En capítulos posteriores veremos el esbozo de una arquitectura de seguridad de referencia en base a las mejores prácticas mencionadas anteriormente de una empresa ficticia genérica.

En cuanto a las tendencias del sector industrial de cara al presente y futuro ya hemos visto previamente los últimos acontecimientos. Por un lado, el Ransomware como malware de tendencia, afectando a la parte de IT y esparciéndose hasta OT o incluso llegando a afectar a dispositivos tipo PLC como el conocido LogicLocker[17].
A nivel técnico se cuenta cada día a medida que avanza la tecnología con nuevas amenazas: conexiones inalámbricas, dispositivos móviles, IoT, etc. Es por ello que la industria debe avanzar en paralelo con la protección de estas tecnologías abogando por principios básicos de seguridad desde el diseño y seguridad por defecto. Existen además una serie de contramedidas técnicas las cuales son tendencia actualmente como puede ser Zero Trust, Virtual Patching o Deception del cual hablaremos en los próximos capítulos.
Por último, pero igualmente importante, se ha evidenciado que la solución no es tecnológica, si no que va de la mano de las personas y procesos. Es por este motivo por el cual la formación y concienciación en ciberseguridad debe ser una prioridad en este tipo de entornos.

2.3 Tecnologías Deception

Para comprender el concepto de Deception como mecanismo de protección vale la pena repasar primero una serie de ideas que se han empleado desde hace años en entornos IT. En este caso concreto nos referimos a los Honeypots. Su origen se remonta a la década de 1990, momento en el cual se empezó a emplear en seguridad informática como mecanismo de detección de atacantes mediante la utilización de señuelos. Su funcionamiento es sencillo, se trata de emplear una o más máquinas o sistemas de forma que se perfilen como vulnerables o accesibles para posibles atacantes. De este modo es posible registrar ataques sobre el mismo hasta el punto de poder aprender de las técnicas empleadas y por tanto aplicar contramedidas correspondientes en los sistemas reales.

[17] https://www.skyboxsecurity.com/blog/logiclocker-brings-ransomware-to-scada-networks/

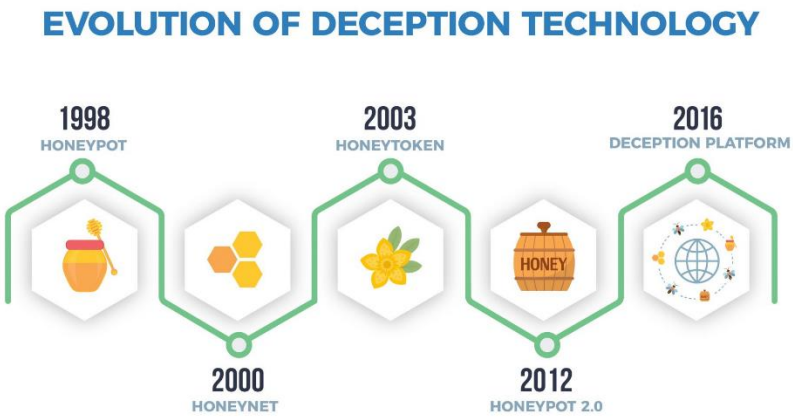

Ilustración 11: Evolución de Honeypot a Deception por Proveho Networks

Fruto de los Honeypots surge la tecnología Deception, o por cómo se intuye de su traducción tecnología basada en el engaño. La tecnología Deception se perfila como la evolución lógica de los Honeypots: un sistema estático, poco configurable y con funcionalidades limitadas, incluyendo poca evolución en el tiempo para recolección de información. Partiendo de esa base se acuña el término Deception como la utilización de tecnologías Honeypot de manera inteligente y dinámica, en ocasiones con mecanismos de Inteligencia Artificial, de forma que la superficie de ataque expuesta de manera intencionada para el atacante no sea estática si no todo lo contrario y de este modo sea mucho más complejo detectar su verdadera naturaleza, además de presentarse como una motivación mayor para un posible atacante.

De este modo la inclusión de este tipo de tecnologías avanzadas permite mejorar las capacidades de detección y respuesta ante amenazas de una organización sin requerir instalación de agentes en sistemas o abrir conexiones hacia el exterior a repositorios de seguridad. De hecho, en su informe de tecnologías de futuro de 2016 Garner incluyó Deception en su Top 10[18].

De hecho, se considera como que nos encontramos actualmente en la 3era generación de tecnologías Deception a nivel de madurez, ya que se ha mejorado a nivel de funcionalidades incluyendo nuevas tendencias como inteligencia artificial además de haber industrializado su distribución por empresas a nivel global y su incorporación es cada vez más frecuente como parte de los mecanismos de seguridad de empresas globalmente.

[18] https://www.smokescreen.io/gartner-identifies-deception-as-a-top-10-security-technology-for-2016/

2.3.1 Principios de la tecnología Deception

La tecnología Deception se basa en el engaño mediante la utilización de distintas técnicas. La manera en la que se orquesta esta tecnología es mediante la utilización de una serie de componentes considerados genéricos del sector, aunque depende de la solución en concreto:

- **Campañas:** son el elemento central de la tecnología Deception ya que se definen como los elementos a implementar bajo una lógica alineada con la estrategia de ciberseguridad de la compañía. Debe contar con un objetivo claro, el tipo de ataque o atacante para el cual se desplegará, el hilo conductor, el entorno requerido para la consecución de objetivos, además de definir los criterios de monitorización de ataque para su posterior análisis.

- **Sistemas Deception:** se perfilan como los activos de engaño a emplear como parte de la campaña. Servirán como señuelos para el atacante de forma que centre sus esfuerzos en vulnerar su seguridad con el objetivo definido en la campaña. Estos dispositivos deben ser capaces de registrar la actividad de forma que se pueda analizar por parte del equipo especialista.

- **Servicios Deception:** al igual que existen los propios sistemas Deception también contamos con servicios de tipo señuelo, los cuales permitirán motivar al atacante a investigar sobre los mismos y por ende dando un hilo argumental a la campaña mayor. Dichos servicios pueden ir desde portales web hasta servidores de ficheros tipo FTP.

- **Migajas o pistas:** se definen de esta forma tan gráfica a una serie de elementos, como pueden ser ficheros con información relevante, alojados en ubicaciones específicas de manera intencionada. Por lo general se trata de información que facilitará que el atacante continue el flujo de ataque por donde la campaña ha definido.

- **Reglas:** las reglas definidas por cada campaña las cuales otorgan el gobierno de lo que ocurre y por ende actúan como el disparador de acciones, tanto defensivas como de creación de nuevos señuelos, en base al flujo ejecutado en cada momento.

Es evidente que la creación de campañas es un procedimiento bastante ad-hoc para cada escenario y deberá ser tratado con el mayor secretismo posible de forma que se minimice su conocimiento más allá de lo mínimo indispensable. Es importante comprender que en cuanto se conozca dicha iniciativa y la campaña asociada, la validez de los resultados quedará en entredicho.

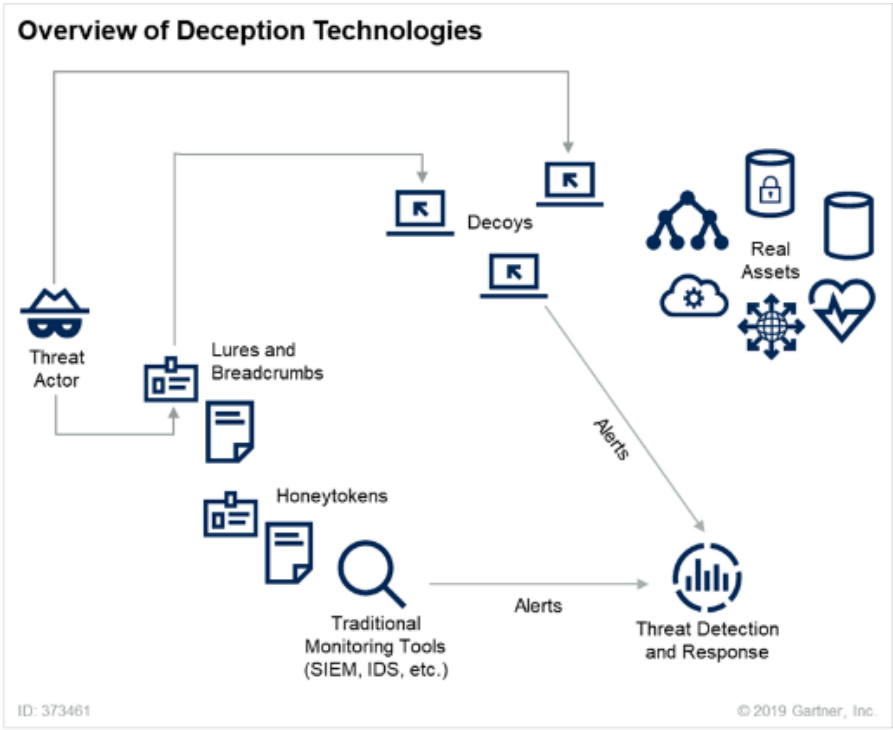

Ilustración 12: Arquitectura típica Deception por Gartner

Por otro lado, al igual que ocurría en los Honeypots, es de especial relevancia definir comportamientos realistas en base al objetivo perseguido. Es decir, un sistema el cual es claramente vulnerable y está expuesto a nivel de red puede levantar rápidamente las sospechas en un atacante por lo que omitiría intentar nada en esta dirección. Igualmente, unido a este punto, en base a la interacción mantenida con el señuelo por parte del atacante será posible recabar más o menos información y por tanto la utilidad de este mecanismo será mayor o menor.

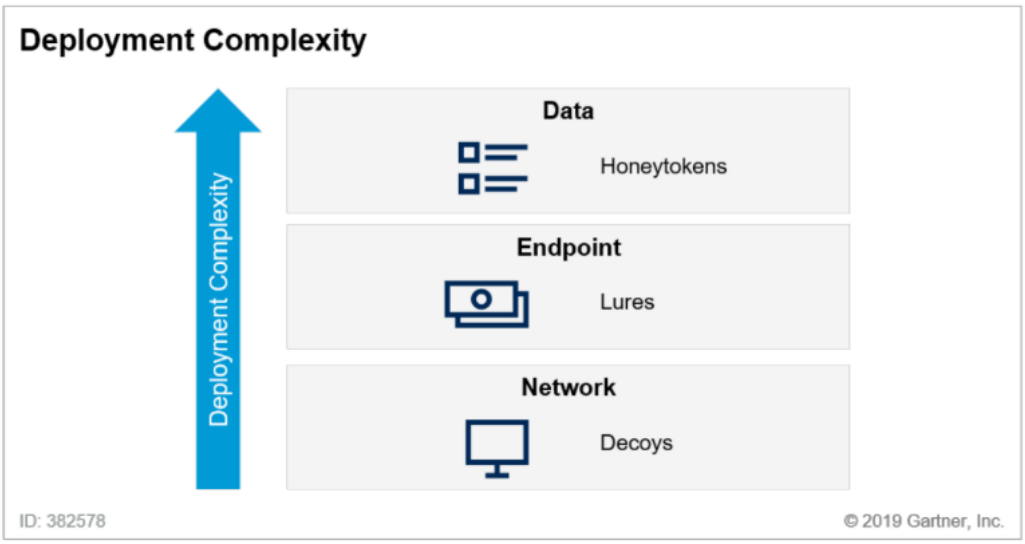

Ilustración 13: definición de elementos Deception en base a la complejidad

2.3.2 Uso de Tecnologías Deception en entornos OT

En base lo descrito anteriormente, surge la motivación de emplear este tipo de tecnologías en entornos industriales. Este tipo de entornos tiene una serie de particularidades las cuales perfilan a Deception como una alternativa más que válida y que puede ser considerada dentro de la estrategia de seguridad de multitud de organizaciones con un nivel de madurez suficiente para ello.

Analizando las características propias de los entornos industriales y de automatización y uniéndolo con las propiedades de tecnologías Deception tenemos una serie de ventajas que se enumeran a continuación:

- Se trata de una solución autocontenida, es decir no se basa en despliegue de agentes o similares sobre los dispositivos reales lo cual en entornos OT puede ser de una complejidad muy elevada o directamente incompatible.
- La interacción con demás activos del entorno es mínima o nula por lo que la disponibilidad de la operación no tiene afectación por el uso de esta tecnología.
- Su despliegue es sencillo y su customización es elevada lo cual permite definir campañas y requisitos acordes a cada negocio y entornos, incluyendo la simulación de dispositivos de tipo industrial e inclusive de tipo IoT.
- Permite aplicar contramedidas en tiempo real en base a las campañas definidas.
- Aporta una capacidad de monitorización y control mediante alertas avanzado.

Fruto de estas características tan atractivas para entornos industriales se plantea dicha idea y se desglosará en mayor profundidad en el capítulo 4. Caso práctico: Deception para entornos OT en el cual se aplicarán tecnologías Deception basadas en proyectos de código abierto y aplicando mecanismos de virtualización de forma que se pueda apreciar de manera práctica la utilidad de esta tecnología. De este modo, se podrá obtener una experiencia práctica que permita obtener ciertas conclusiones con respecto a los objetivos planteados en este trabajo, teniendo siempre en cuenta el aspecto teórico y las salvedades que puede haber en entornos reales.

3. Arquitectura de referencia para entornos OT

Basado en lo que se ha visto hasta este punto, ha quedado evidenciado de forma clara que no puede existir una digitalización industrial sin ciberseguridad, ambas deben ir de la mano de forma que se llegue a buen puerto a nivel operativo y de forma segura. Por este motivo las organizaciones que quieran ejecutar una digitalización de su modelo de negocio, incorporando nuevas tecnologías y procesos que permitan optimizar su operación mediante el intercambio y explotación de datos deberán de igual forma adoptar una postura clara frente a la seguridad de la información en sus activos, tanto físicos como digitales.

De este modo, como hemos visto en aspectos anteriormente destacados, los entornos industriales son muy distintos a los tradicionales de IT por lo cual la postura de ciberseguridad debe ser también distinta, pero a la vez compatible con la aplicada en el mundo IT de forma que sea posible alcanzar lo que se denomina convergencia IT-OT la cual permite optimizar la productividad y eficiencia de la organización de manera segura[19].
Cuando nos referimos a dichas diferencias sobre todo van enfocadas en conceptos clásicos de la ciberseguridad de IT los cuales no son aplicables en OT, como por ejemplo la prioridad de la confidencialidad de los datos en IT contra la disponibilidad de estos en OT. Otro ejemplo podría ser la aplicación de mecanismos de protección “intrusivos” como pueden ser IPS o EDR de última generación los cuales mediante la aplicación de contramedidas en tiempo real evitan problemas de seguridad en IT como la propagación de un Ransomware, pero en OT podrían ocasionar la parada de una fábrica de energía produciendo por tanto un corte en el suministro de miles de personas y afectando directamente a las vidas humanas.

Se antoja por tanto fundamental la definición de unos principios de seguridad que sean aplicables al mundo industrial, al no poderse extrapolar de manera directa los del sector IT. De este modo uno de los principios básicos que se recomienda aplicar para la definición de estrategia de seguridad (tanto para IT como OT) es el conocido como defensa en profundidad, el cual tiene su origen en una estrategia militar en la cual mediante el despliegue de distintas líneas de defensa en puntos estratégicos conseguían mejores resultados que volcando todos los esfuerzos en una única línea de defensa estática. De igual forma se puede aplicar al mundo OT y mediante la definición de distintas capas de defensa se consigue un nivel medio de seguridad bastante robusto.

[19] https://www.automaticaeinstrumentacion.com/texto-diario/mostrar/2734961/convergencia-it-ot-como-barrera-ciberseguridad

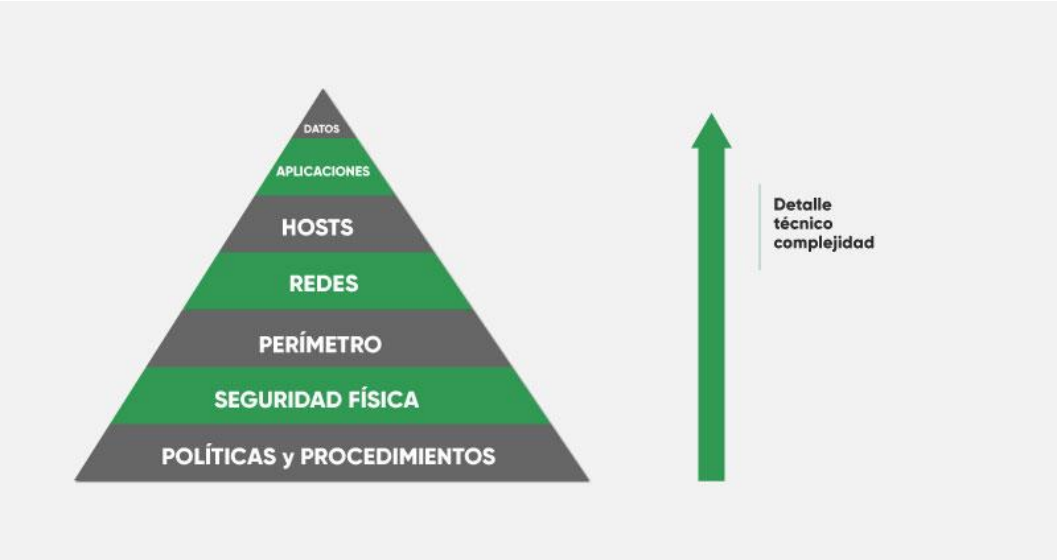

Ilustración 14: Modelo de Defensa en Profundidad - Logitek

Como vemos, dicho modelo abarca distintas temáticas desde la definición teórica de políticas y procedimientos, pasando por la seguridad perimetral y acabando en la protección e implementación técnica a nivel de aplicaciones o datos.

En el presente capítulo nos focalizaremos en el primer nivel referido a la definición de políticas y procedimientos de seguridad en profundidad. Para ello procederemos a esbozar un concepto vital en muchas organizaciones de naturaleza industrial: una arquitectura de referencia de seguridad industrial. Este documento por lo general suele emplearse como guía para el despliegue, mantenimiento y aplicación de cambios en entornos industriales de una organización, de tal modo que dichas tareas se ejecuten de manera uniforme y siguiendo una serie de requisitos alineados con el apetito de riesgo de la organización y su postura de ciberseguridad.

Para ello se tomará de referencia las mejores prácticas definidas por diferentes organismos de seguridad como puede ser el INCIBE o las guías CCN-STIC a nivel nacional español. Sin embargo, tal y como hemos visto anteriormente en el mundo OT el estándar de referencia IEC 62443 emitido por la ISA. De este modo, esta guía pretende cubrir con una serie de requisitos mínimos de seguridad de entornos industriales, sin embargo, no es su objetivo convertirse en el documento único de seguridad de una organización, por dos motivos principalmente: no es su naturaleza, siendo poco realista y práctico, y en caso de querer abarcar dicha magnitud sería un trabajo que superaría con creces el objetivo de este trabajo.

Adicionalmente, la presente arquitectura de referencia debe considerarse un documento vivo y el cual deberá actualizarse de manera continua como parte de un plan de mejora continua. Por otro lado, al tratarse de la seguridad un entorno bastante amplio y en constante cambio, es posible que en la presente arquitectura se esbocen conceptos y mecanismos de seguridad los cuales puedan ser mejorados e incluso sustituidos como parte de nuevos desarrollos

enfocados a mejorar el nivel de seguridad general de la organización. En referencia a este último punto, en la presente arquitectura se hablará de mecanismos de seguridad de manera general sin entrar en detalles específicos de fabricantes concretos, como podrían ser para electrónica de red como cortafuegos o switches o dispositivos industriales como PLCs.

Es importante reseñar que en la presente arquitectura de referencia no se entrará en detalle con respecto a los mecanismos denominados SIS: *Safety Instrumented Systems*, es decir los referidos a la protección de vidas humanas en el propio entorno industrial. Solo cabe decir que este tipo de mecanismos son evidentemente prioritarios para la operación y por tanto se deben tratar con la mayor relevancia. El requisito indispensable para este tipo de instrumentación suele estar referido a que sus comunicaciones deben ser totalmente ajenas a la operación, redundadas y no dependientes de mecanismos únicos, siguiendo conceptos como *failover* y utilizan sistemas bajo SAI (sistemas de alimentación ininterrumpida).

3.1 Caso práctico de arquitectura OT: La Genérica S.A.

De forma que sea más ilustrativo el poder desarrollar esta arquitectura de referencia pasaremos a esbozarlo sobre una empresa ficticia creada para tal circunstancia. La empresa en cuestión tiene como nombre comercial “La Genérica S.A.”, a partir de ahora denominada la empresa, la cual se perfila como líder del sector de distribución de papel. Dicha empresa cuenta con una red corporativa o de oficinas, donde se realizan todas las tareas asociadas al negocio que no son propiamente la operación de distribución de papel. Por otro lado, cuenta con dos principales centros de distribución de papel, uno en la zona central peninsular y otro por la zona de la costa mediterránea, los cuales son los que denominaremos en esta ocasión como los entornos industriales de la organización.

Desglosando de manera un poco más detallada el modelo operativo de la empresa tenemos como mencionábamos anteriormente 1 entorno industrial en la costa mediterránea. Este se focaliza en lo que es la generación propiamente del papel y para ello cuenta con un total de 5 procesos en la fábrica, además de ser el centro logístico al contar con acceso por mar, tierra y aire.
Por su parte, la oficina corporativa ubicada en la zona central peninsular es el responsable de las tareas de adquisición de clientes y demás labores de oficina.

La empresa tiene una ventaja a su favor y es que su creación es de solo hace 5 años, sobre el año 2016, por lo que a pesar de ser un entorno industrial se ha podido aplicar principios muy importantes como seguridad desde el diseño siempre que ha sido posible.

Gracias a la presente arquitectura de referencia la empresa podrá expandir su negocio con evoluciones de los centros de operación actuales o inclusive con la

adquisición de nuevos centros operativos a nivel nacional o internacional siguiendo las mejores prácticas de seguridad industrial.

Ilustración 15: Distribución de oficinas de la empresa

3.1.1 Arquitectura de seguridad basada en modelo Purdue

Unido a este punto uno de los pilares que se ha seguido para el despliegue de la arquitectura es la aplicación del modelo Purdue emitido por la ISA 95. Dicho modelo permite aplicar una separación basada en niveles alineada con la pirámide de automatización que vimos anteriormente, pero mostrando de forma más clara la convergencia entre el mundo OT e IT. A pesar de ser un modelo antiguo, publicado en la década de los 90, sigue siendo aplicable hoy en día y sobre todo a nivel teórico está bastante extendido.

Ilustración 16: Modelo Purdue de la ISA95

Gracias a la aplicación de este modelo, es posible distribuir en distintos niveles los dispositivos de acuerdo con su naturaleza dentro del proceso industrial

consiguiendo al final una separación entre el entorno tradicional IT y el OT, pero a su vez permitiendo la ya mencionada convergencia cuando es aplicable.

Si analizamos el anterior diagrama, desde abajo hacia arriba, vemos que partimos del nivel 0 el cual se refiere a los procesos (actuadores y sensores esencialmente). Posteriormente vemos el nivel 1 o nivel de control, donde se alojan los dispositivos de campo como los PLCs o RTUs los cuales se encargarán de actuar en consecuencia a los eventos generados en niveles inferiores. De igual forma tenemos el nivel 2 con los HMI locales que nos permiten visualizar el proceso subyacente, si analizamos detenidamente el gráfico podemos ver que se despliega un cortafuegos que permitirá controlar el tráfico del proceso. Este tipo de elementos de red estarán presentes en distintos puntos la arquitectura de forma que se pueda conseguir una segmentación real basada en una política de comunicaciones seguras, alineado con buenas prácticas como la definida por el IEC 62443 referente a la definición de zonas de confianza y establecimiento de conductos.
Posteriormente pasamos al nivel 2/3 el cual puede estar presente o no según la arquitectura desplegada, dicho nivel destaca especialmente por tener los dispositivos de operación del entorno OT como puede ser un Historian para almacenamiento de datos o una estación de ingeniería, la cual se utilizará como máquina de salto para operar y modificar parámetros en dispositivos de capas inferiores.
Luego dentro del propio nivel 3 tendríamos la denominada DMZ industrial la cual ejercerá su función de manera similar a una DMZ corporativa IT, pero en este caso para el entorno OT, como por ejemplo con el despliegue de servidores de actualizaciones o con máquinas de salto para accesos remotos de forma segura.
En este punto ya empezamos a plantarnos en entorno IT, desde el punto de vista de los procesos la red interna o corporativa de IT se debe considerar de no confianza por lo que la comunicación deberá estar restringida y únicamente parcialmente en sentido OT-IT.
Por último, tras el firewall de red corporativa vemos lo que se conoce como DMZ de Internet o corporativa, la cual cuenta con ciertos servicios expuestos como puede ser el portal web de pedidos de la organización. Para la conectividad con los entornos operacionales se cuenta con una MPLS dedicada la cual permite establecer conectividad con la parte corporativa de manera segura.

Teniendo este modelo en cuenta pasamos a esbozar la matriz de comunicaciones que definirán el criterio en base al flujo necesario de la comunicación.

Permitido No permitido	**Nivel 0: Red de proceso**	**Nivel 1: Red de control**	**Nivel 2: Red de datos**	**Nivel 3: DMZ industrial**	**Nivel 4: Red IT**	**Nivel 5: Red Externa**

Nivel 0: Red de proceso		Si	No	No	No	No
Nivel 1: Red de control	Si		Si	No	No	No
Nivel 2: Red de datos	No	Si		Si	No	No
Nivel 3: DMZ industrial	No	No	Si		Si	Si*
Nivel 4: Red IT	No	No	No	Si		No
Nivel 5: Red Externa	No	No	No	Si*	No	

Tabla 3: Matriz de comunicación

**En caso de entornos de red industriales en los cuales no exista comunicación con red corporativa, se permitirá el despliegue de comunicaciones con redes de no confianza desde la DMZ industrial al ser la red más segmentada desde el proceso.*

En este sentido, se deberá optar por la utilización de los conocidos como NGFW o cortafuegos de nueva generación, los cuales permiten realizar un filtrado del tráfico de red incluso por capas superiores como puede ser a nivel de usuario, además de incorporar otras funciones como detección de intrusos (IDS). Este tipo de cortafuegos nos permitirá aplicar un filtrado entre los distintos niveles de Purdue, sobre todo los más altos ya que para capas más operacionales se deberán emplear cortafuegos industriales que permitan filtrar protocolos industriales y además estén preparados físicamente para dichos entornos, con protección frente a humedad, polvo o altas temperaturas.

Ilustración 17: Firewall entornos industriales - Checkpoint modelo 1200R

3.1.2 Análisis de riesgos basado en procesos industriales

Unido a la utilización del modelo Purdue, la empresa aplica de igual forma un análisis de riesgos basado en procesos. De esta forma mediante la utilización de la ISA/IEC 62443 3-2[20] *"Standard addresses security risk assessment and system design for IACS"* se aplica una gestión de riesgos industriales la cual permite identificar los procesos de un entorno industrial y la criticidad de cada uno de ellos, incluyendo así también la criticidad de los activos que lo conforman.

Este conjunto de activos y sistemas que conforman un proceso es lo que se denomina en el IEC 62443 3-2 como zonas. En base a la criticidad e impacto de cada zona se definen los niveles de seguridad requeridos (SLR) y a su vez se define el nivel de seguridad objetivo (SLT). Mediante estos dos valores es posible calcular el riesgo residual frente al cual se posiciona la empresa.

Estas zonas a su vez, como se puede inferir en el modelo de Purdue, se comunicarán con otros sistemas como por ejemplo los de capas superiores que adquieren datos, estas comunicaciones se denominan conductos y se protegen mediante la utilización de cortafuegos.

Por ello se emplea la utilización de zonas y conductos de forma que se tiene en cuenta la criticidad de cada zona y por ende se minimizan los conductos disponibles entre zonas. Al final todo esto radica en principios de segmentación de red aplicados a entornos industriales.

De esta forma, la empresa deberá contar con un inventario de zonas y conductos los cuales permitirán aplicar una segmentación a nivel de procesos. Dicho inventario deberá incluir para cada zona al menos:

- Nombre de la zona
- Activos que pertenecen a la zona

[20] https://www.certsi.es/blog/iec62443-evolucion-isa99

- Aplicaciones o modelo operativo relacionado con la zona
- Nivel de seguridad requerido (SLR)
- Nivel de seguridad objetivo (SLT)
- Límites físicos y lógicos
- Conductos asociados

Este inventario, como casi cualquier aspecto definido en la presente arquitectura de referencia, debe ser considerado como un elemento vivo y el cual se someterá a cambios en base a la inclusión de nuevos activos en la red o cambios debido a la operación. De igual forma se deberá someter a revisiones periódicas que permitan garantizar su aplicabilidad, tanto desde el punto de vista teórico como práctico mediante auditorías o revisiones de seguridad tanto internas como externas.

3.1.3 Gestión de ciclo de vida de los activos

Uno de los aspectos más básicos para contar con medidas de protección adecuadas es saber que se tiene en el entorno industrial, es decir contar con un inventario de activos actualizado y completo.
Por este motivo se deberá contar con un inventario de activos el cual permita llevar un registro de estos, sus características y de este modo un control sobre el ciclo de vida de estos. Igualmente es importante registrar un responsable del activo de forma que se pueda tener una trazabilidad de este.
Este tipo de actividad es especialmente relevante en los entornos industriales, donde es bastante común encontrarse con dispositivos con a lo mejor 20 años de antigüedad y donde los mecanismos de seguridad y actualizaciones frente a problemas de seguridad suelen ser altamente complejas y en ocasiones directamente imposible de aplicar sin comprometer la operación. Es por ello, que en caso de contar con dispositivos fuera de soporte, se debe tener un inventario para poder aplicar medidas compensatorias de seguridad o por el contrario poder detectar dichos parches y actualizaciones faltantes y proceder a su despliegue.

En los entornos IT suele ser medianamente sencillo contar con este tipo de inventarios mediante la información proporcionada por vías como puede ser un directorio activo o mediante agentes de protección tipo antivirus. Sin embargo, en entornos industriales no suele ser tan sencillo. Por este motivo se propone la utilización de sondas de detección pasiva de tráfico como alternativa, de forma que mediante mecanismos muy poco intrusivos se pueda contar con un inventario de activos actualizado. Este tipo de mecanismos de detección se basan en la escucha de tráfico mediante la utilización de mecanismos como Port-SPAN o port-mirror en los switches de comunicación, de forma que mediante dicha escucha son capaces de registrar los dispositivos conectados a la red y sus características (de forma más o menos limitada basada en el tráfico generado).

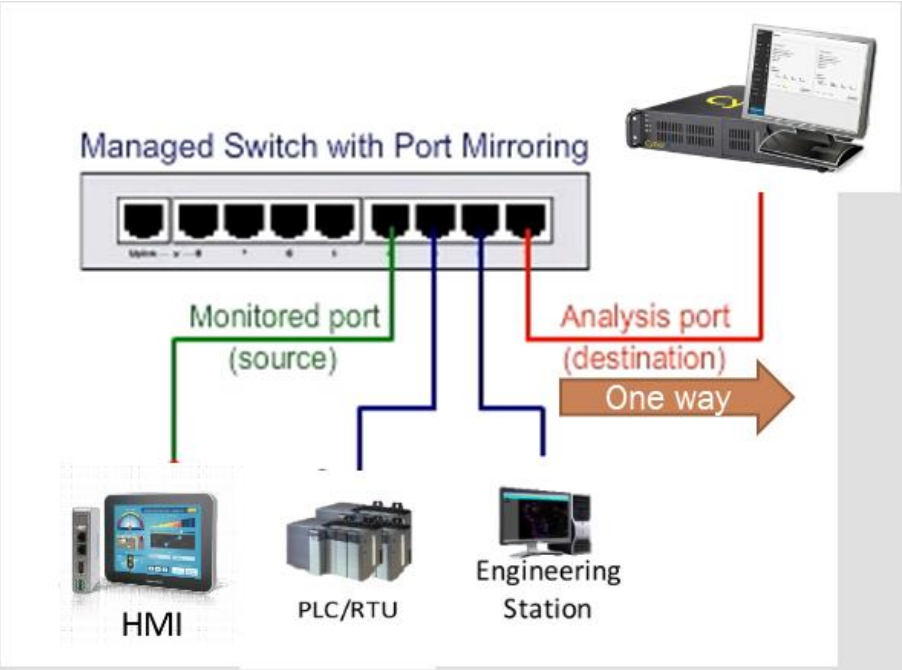

Ilustración 18: Port Mirror por Azure Defender IoT

Dicho inventario deberá mantenerse actualizado, tanto de manera automatizada como de forma manual en los casos que sea necesario como puede ser la ubicación física del activo. De igual manera gracias a la información recabada se deberán definir planes de acción como puede ser la aplicación de parches faltantes o migración de sistemas operativos en caso de ser obsoletos. Dichas actividades se definirán en mayor detalle en la política y procedimiento de parcheado para entornos industriales de la empresa.

3.1.4 Arquitectura de referencia general

De este modo, con lo mencionado anteriormente, se cuenta con los principios básicos de seguridad tanto desde el punto de vista como análisis de riesgos como para la gestión de activos del entorno industrial. Por ello pasamos a desglosar lo que sería la arquitectura de referencia general que se aplica a este entorno de la empresa ficticia sobre la cual hemos desarrollado el presente apartado.

La arquitectura esbozada a continuación se enfoca siguiendo el modelo Purdue el cual permite segmentar la red en distintos niveles y es lo que permite que la seguridad y la segmentación tenga un valor adicional. Tal y como se ha comentado previamente, el modelo Purdue permite definir de manera jerárquica la arquitectura de red, sin embargo, este modelo en ocasiones se considera obsoleto con la inclusión de las tecnologías IoT, sin embargo una de las soluciones que se plantean es la de minimizar las comunicaciones entre distintos niveles de la red y desplegar un nivel único para los dispositivos IoT el cual deberá estar gestionado con reglas de tráfico de red dedicadas en base a los objetivos de los dispositivos desplegados.

De esta forma el principio seguido en la arquitectura de referencia de La Genérica S.A. define que cada proceso debe estar segmentado de tal forma que los dispositivos de cada proceso sólo tengan comunicación mediante protocolos seguros, evitando protocolos tipo *telnet,* por ejemplo, con los demás dispositivos asociados al proceso industrial. De este modo los niveles 0, 1 y 2 del modelo de arquitectura de referencia serán únicos por cada proceso, es decir en el caso del centro de distribución de la costa mediterránea se trataría de 5 procesos segmentados entre sí y a su vez compartiendo desde el nivel 3 y superiores al tratarse de un mismo emplazamiento físico.

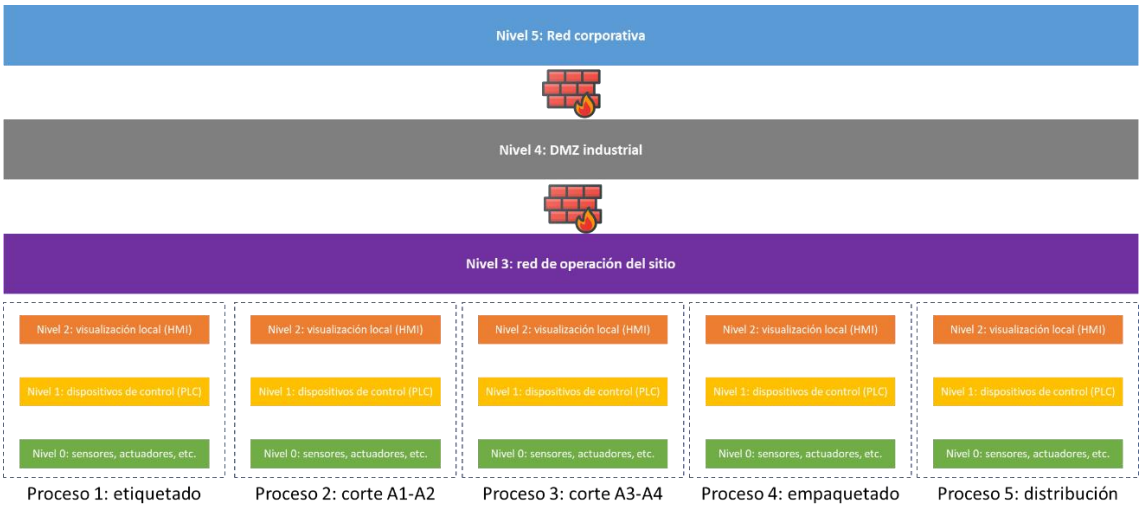

Ilustración 19: Arquitectura de referencia La Genérica S.A.

Como vemos, por tanto, cada proceso cuenta con sus niveles inferiores de elementos OT de forma que se comparte el nivel 3 como la red de operación, alojando por ejemplo Historian locales o estaciones de ingeniería. Este nivel 3 compartido permite un filtrado de tráfico de forma que un compromiso de un dispositivo en uno de los procesos sólo afectaría al resto de dispositivos asociados al mismo proceso, pero no así al resto de elementos del entorno industrial, garantizando de este modo la operación y disponibilidad. Otro elemento relevante que se define como parte de esta arquitectura de referencia es la conectividad a Internet, tal y como se mencionó en el apartado 3.1.1 con la matriz de comunicaciones. La salida a Internet requiere un salto de al menos 2 cortafuegos y de manera preferente se deberá realizar por la red corporativa aplicando navegación vía proxy al igual que se hace en la red de oficinas. De este modo se minimiza en gran medida la posible exposición del entorno industrial en redes de no confianza.

Con esta arquitectura de referencia definida, la empresa La Genérica S.A. podrá contar con mecanismos de seguridad básicos tanto para los entornos industriales que actualmente tiene como para los posibles nuevos centros que pueda tener en un futuro próximo, los cuales deberán adaptarse a las políticas definidas, además de mantenerse actualizados con respecto a las mejores prácticas, como por ejemplo podría ser el uso de tecnología Deception para Ciber inteligencia como veremos en siguientes apartados.

4. Caso práctico: Deception para entornos OT

En el presente apartado se procederá a aplicar mecanismos de seguridad avanzados basados en detección como es Deception para entornos industriales. En apartados anteriores ya se ha mencionado los beneficios que podría tener este tipo de tecnología en entornos industriales, sin embargo, al ser este el segmento específico del mismo profundizaremos un poco en ello para posteriormente realizar unas pruebas técnicas empleando mecanismos de virtualización y herramientas de código abierto que permitirán obtener una aproximación de lo que podría ser la utilización de esta tecnología en entornos OT.

La tecnología Deception ha irrumpido de manera bastante fuerte en el mercado en los últimos años[21], siendo la evolución de los tradicionales Honeypots, ofreciendo una capacidad de detección de amenazas basado en el uso de señuelos, pero aplicando una capa adicional de inteligencia mediante la orquestación de elementos de engaño. De este modo se utilizan las denominadas campañas, que no dejan de ser los casos de uso definidos para los cuales se quiere desplegar la tecnología.

Sin embargo, el foco de esta tecnología suele estar asociado al mundo tradicional de IT, de forma que se pueda desplegar en dichos entornos como una herramienta más de seguridad que permite añadir una capa más de detección de posibles vectores de ataque y entender cómo funcionan los actores del entorno.

Lo que se propone en el presente trabajo es el uso de esta tecnología en entornos industriales, al proporcionar una serie de características las cuales pueden ser de gran interés para el sector tal y como se mencionó en la sección 2.3.2.

Es importante reseñar que la aplicación de dicha tecnología dependerá en gran medida de la madurez del entorno en cuestión, ya que se no se trata de un mecanismo que pueda considerarse de protección básico y por ende requiere cierto nivel de madurez que permita se incorporación de forma eficaz.

Por otro lado, los entornos industriales son especialmente complejos de emular a nivel virtual al tratarse de entornos con tecnologías propietarias y con poca expansión a nivel virtual. Es por eso que en el presente trabajo se realizará la aproximación más adecuada pero no debe perderse el foco del mismo, el cual es esbozar de forma general la posible utilidad de estos mecanismos de detección de amenazas como un elemento candidato a ser incorporado en este tipo de entornos. De igual forma es importante reseñar de nuevo que estos mecanismos de seguridad no representan una capa infranqueable ni se pueden considerar como la seguridad total si no como un elemento más dentro de la

[21] https://cso.computerworld.es/empresas/countercraft-lleva-su-tecnologia-de-ciberinteligencia-al-departamento-de-defensa-de-estados-unidos

cadena de seguridad la cual deberá estar basada en mecanismos conocidos y mencionados en este trabajo como defensa en profundidad.

Para el despliegue del entorno se ha empleado un equipo con las siguientes características:

- Sistema operativo 64 bits - Windows 10
- Procesador: Intel ® Core™ i5-6300U CPU 2.40 Ghz
- Memoria RAM: 16 Gb
- Espacio en disco duro de almacenamiento: 500 Gb
- Tarjeta de red Ethernet y Wi-Fi, incluyendo virtualización.
- Fabricante: HP

Dicho equipo se empleará para el despliegue de elementos virtuales mediante la utilización del software Oracle VM VirtualBox.

Dicho software de virtualización nos permitirá desplegar mediante máquinas virtuales diversos elementos que podrían encontrarse en una red industrial, además de la tecnología Deception.

En cuanto a esta última, se ha llevado a cabo una investigación previa que ha permitido encontrar diversas opciones de código abierto para probar este tipo de tecnología, sin embargo, tras hacer diversas pruebas y analizar los pros y contras la opción escogida ha sido el framework open source DejaVu[22] el cual permite orquestar campañas Deception mediante la utilización de motores de acción y una consola de gestión centralizada de eventos. Es importante mencionar también se planteó la utilización de otro proyecto denominado T-Pot, el cual fue desestimado, especialmente por las capacidades limitadas de orquestación que ofrece y al estar, en base al análisis realizado, en un estado más cercano a Honeypots tradicionales que a Deception, a pesar de por ejemplo contar con una interfaz gráfica muy potente basada en Kibana la cual permite pensar en posibles mejoras de cara al proyecto DejaVu.

[22] https://github.com/bhdresh/Dejavu

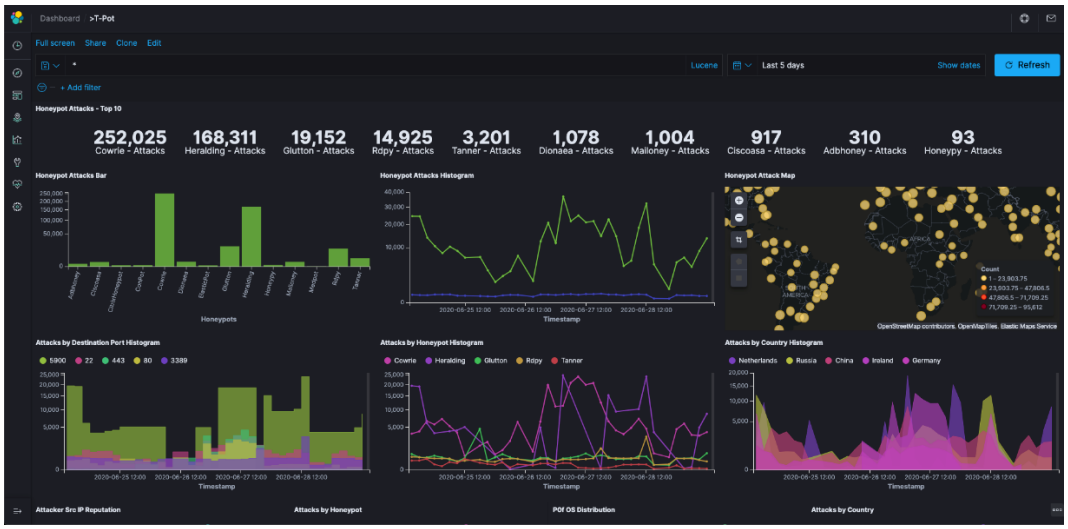

Ilustración 20: Visualización cuadro de mando T-Pot

En el presente escenario esbozaremos el uso de tecnología Deception en 2 posibles segmentos de red que se podrían encajar en la arquitectura de referencia anteriormente definida. Por un lado, realizaremos una demostración en niveles inferiores más cercanos al proceso en cuestión, donde contaremos con dispositivos como PLCs y servidores SCADA los cuales estarán ejecutando una lógica por defecto para emular un comportamiento industrial. Por otro lado, emularemos una DMZ industrial en la cual se podrán encontrar servidores de actualizaciones o máquinas de salto para accesos remotos al entorno industrial. En ambos escenarios simplificarán las comunicaciones para efectos del propio laboratorio y poder potenciar al máximo la capacidad de acción de la tecnología Deception, motivo por el cual no se contará con electrónica de red tipo cortafuegos que filtre el tráfico.

4.1 Escenario 1: niveles inferiores del entorno industrial

Para el presente escenario emplearemos la virtualización para poder emular dispositivos de capas inferiores del modelo Purdue. En concreto emplearemos virtualización para emular un par de controladores lógicos programables (PLCs) mediante OpenPLC[23]. OpenPLC es un proyecto de código abierto que permite emular el comportamiento de un PLC tanto a nivel de software como hardware. En este caso concreto emplearemos una virtualización basada en software mediante el sistema operativo Ubuntu de forma que contaremos con un par de PLCs virtualizando un proceso inocuo.

De la misma forma se empleará SCADABR para virtualización de HMI (interfaz humano máquina) del proceso a virtualizar. Al igual que los PLCs, está instalado sobre el sistema operativo Ubuntu.

[23] https://www.openplcproject.com/

Empezamos por tanto por crear las máquinas virtuales necesarias para el presente escenario nº 1. De esta manera crearemos una máquina la cual podremos clonar posteriormente ya que sus requisitos son bastante similares tanto para PLC como HMI.

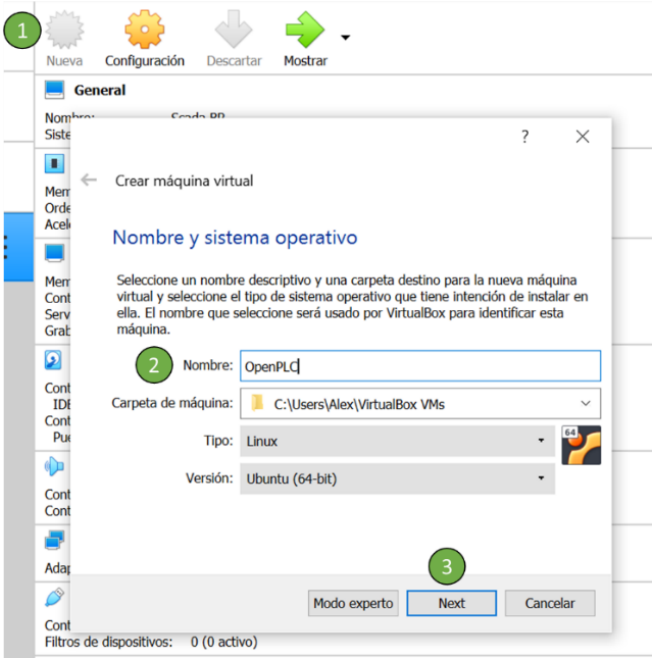

Ilustración 21: Creación de las máquinas Ubuntu

Llevamos a cabo la creación de la máquina virtual asignando unos recursos mínimos de disco duro y RAM para la instalación del sistema operativo Ubuntu y finalizamos el proceso.

Una vez creada la máquina virtual entramos en la configuración de esta para poder asignar como disco de instalación la imagen ISO del Sistema Operativo, en este caso concreto se empleará Ubuntu Desktop 20.04.3.

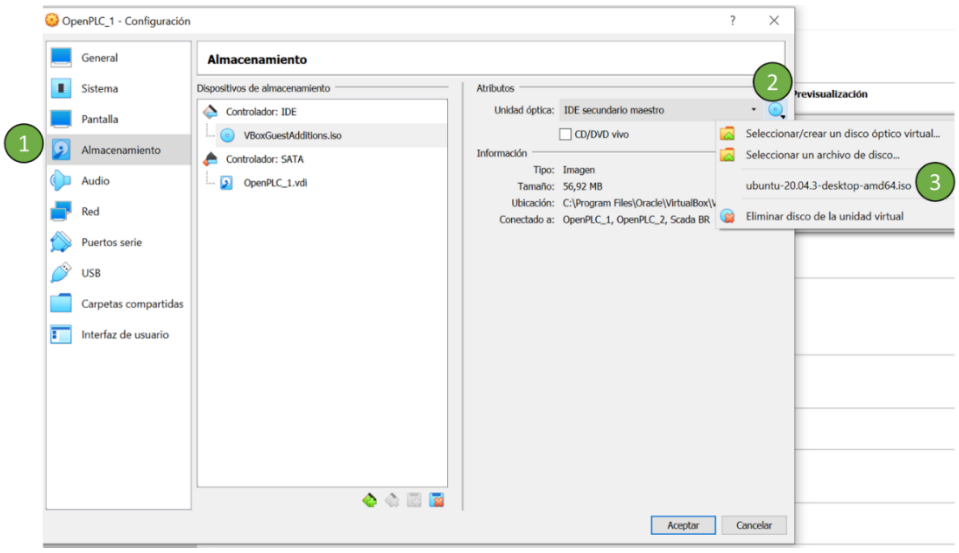

Ilustración 22: Asignación de imagen Ubuntu

Con la imagen asignada para el arranque del sistema ya podemos arrancar la máquina virtual para instalar el propio Sistema Operativo Ubuntu basado en Linux:

Ilustración 23: Arranque instalador Ubuntu

Tras el arranque de la imagen del sistema operativo empezaremos con la instalación, para ello seguiremos los pasos de manera sencilla como por ejemplo omitiendo la aplicación de particiones de disco. Tras estos pasos el Ubuntu Desktop arrancará y finalizará su configuración inicial en donde deberemos definir ciertos parámetros básicos del propio sistema operativo.

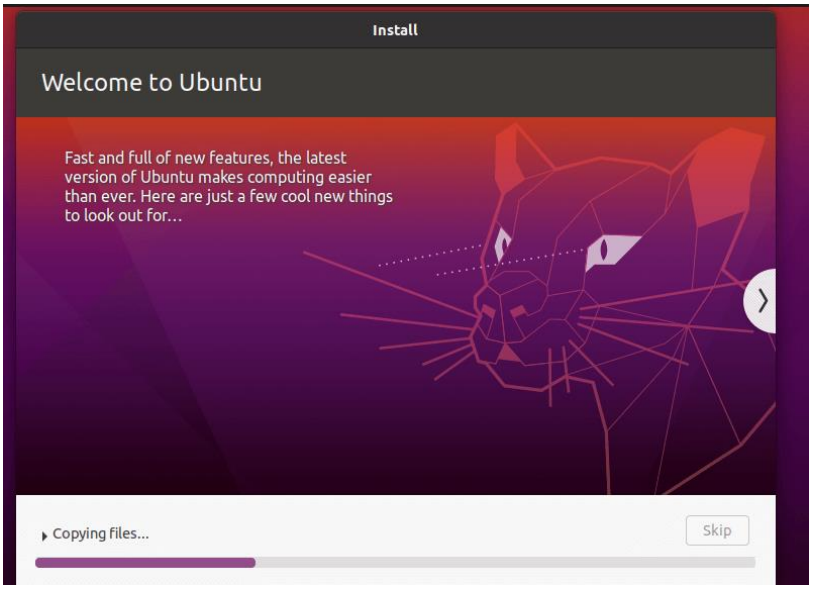

Ilustración 24: Instalación de Ubuntu

Una vez instalado el Sistema Operativo por completo pasamos a configurar los PLCs a emplear mediante OpenPLC. Para ello instalamos la utilidad de git para descargar proyectos de repositorios de código, en concreto de GitHub como el de OpenPLC.

```
openplc@openplc-VirtualBox:~$ sudo apt-get install git
[sudo] contraseña para openplc:
Leyendo lista de paquetes... Hecho
Creando árbol de dependencias
Leyendo la información de estado... Hecho
Se instalarán los siguientes paquetes adicionales:
  git-man liberror-perl
Paquetes sugeridos:
  git-daemon-run | git-daemon-sysvinit git-doc git-el git-email git-gui gitk
  gitweb git-cvs git-mediawiki git-svn
Se instalarán los siguientes paquetes NUEVOS:
  git git-man liberror-perl
0 actualizados, 3 nuevos se instalarán, 0 para eliminar y 116 no actualizados.
Se necesita descargar 5.465 kB de archivos.
Se utilizarán 38,4 MB de espacio de disco adicional después de esta operación.
¿Desea continuar? [S/n] S
Des:1 http://es.archive.ubuntu.com/ubuntu focal/main amd64 liberror-perl all 0.17029-1 [26,5
kB]
Des:2 http://es.archive.ubuntu.com/ubuntu focal-updates/main amd64 git-man all 1:2.25.1-1ubun
tu3.2 [884 kB]
Des:3 http://es.archive.ubuntu.com/ubuntu focal-updates/main amd64 git amd64 1:2.25.1-1ubuntu
3.2 [4.554 kB]
Descargados 5.465 kB en 10s (538 kB/s)
```

Ilustración 25: Instalación herramientas y actualizaciones Ubuntu

Una vez instalada la utilidad git pasamos a instalar la propia solución de virtualización de OpenPLC.

```
openplc@openplc-VirtualBox:~$ git clone https://github.com/thiagoralves/OpenPLC_v3.git
Clonando en 'OpenPLC_v3'...
remote: Enumerating objects: 5162, done.
remote: Counting objects: 100% (185/185), done.
remote: Compressing objects: 100% (132/132), done.
remote: Total 5162 (delta 97), reused 95 (delta 51), pack-reused 4977
Recibiendo objetos: 100% (5162/5162), 11.36 MiB | 7.85 MiB/s, listo.
Resolviendo deltas: 100% (2784/2784), listo.
openplc@openplc-VirtualBox:~/OpenPLC_v3$ ./install.sh linux
Installing OpenPLC on Linux
Obj:1 http://es.archive.ubuntu.com/ubuntu focal InRelease
Des:2 http://security.ubuntu.com/ubuntu focal-security InRelease [114 kB]
Des:3 http://es.archive.ubuntu.com/ubuntu focal-updates InRelease [114 kB]
Des:4 http://es.archive.ubuntu.com/ubuntu focal-backports InRelease [101 kB]
Des:5 http://security.ubuntu.com/ubuntu focal-security/main i386 Packages [306 kB]
Des:6 http://es.archive.ubuntu.com/ubuntu focal-updates/main i386 Packages [563 kB]
Des:7 http://security.ubuntu.com/ubuntu focal-security/main amd64 Packages [987 kB]
Des:8 http://es.archive.ubuntu.com/ubuntu focal-updates/main amd64 Packages [1.344 kB]
Des:9 http://security.ubuntu.com/ubuntu focal-security/main Translation-en [184 kB]
Des:10 http://security.ubuntu.com/ubuntu focal-security/main amd64 DEP-11 Metadata [29,0 kB]
Des:11 http://security.ubuntu.com/ubuntu focal-security/main amd64 c-n-f Metadata [8.880 B]
Des:12 http://security.ubuntu.com/ubuntu focal-security/universe i386 Packages [515 kB]
```

Ilustración 26: Instalación OpenPLC

Una vez instalado el proyecto OpenPLC automáticamente tras un reinicio de la máquina virtual el servidor web de la aplicación ofrecerá las funciones disponibles. Como hemos comentado previamente, no emplearemos mecanismos de entrada salida que emulen el proceso en niveles inferiores,

básicamente por tratarse de un aspecto fuera del alcance del presente trabajo el cual se focaliza en la utilización de tecnologías Deception en entornos industriales.

Una vez instalado OpenPLC procedemos a acceder a su interfaz web para poder emular un proceso vacío basado en Modbus:

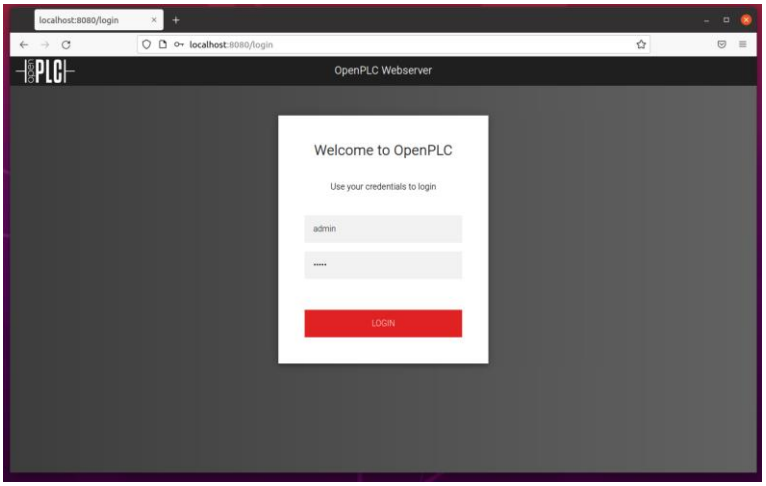

Ilustración 27: Interfaz web OpenPLC

Una vez dentro de la interfaz web podemos modificar diversos parámetros de la configuración del PLC como puede ser la asociación de elementos esclavos, la configuración de proyectos, gestión de usuarios, entre otros. Para nuestra demostración emplearemos como hemos dicho un programa vacío de forma que el PLC se encuentre en modo “RUN” del mismo tal y como podría hacerlo un PLC que se encontrase en un entorno industrial real controlando un proceso físico, por ejemplo, una cinta que distribuye paquetes de papel como los que se podrían encontrar en los centros de distribución de la empresa La Genérica S.A. que vimos en el capítulo anterior.

Dicho esto, procedemos a modificar el estado del PLC pasando a modo “RUN”:

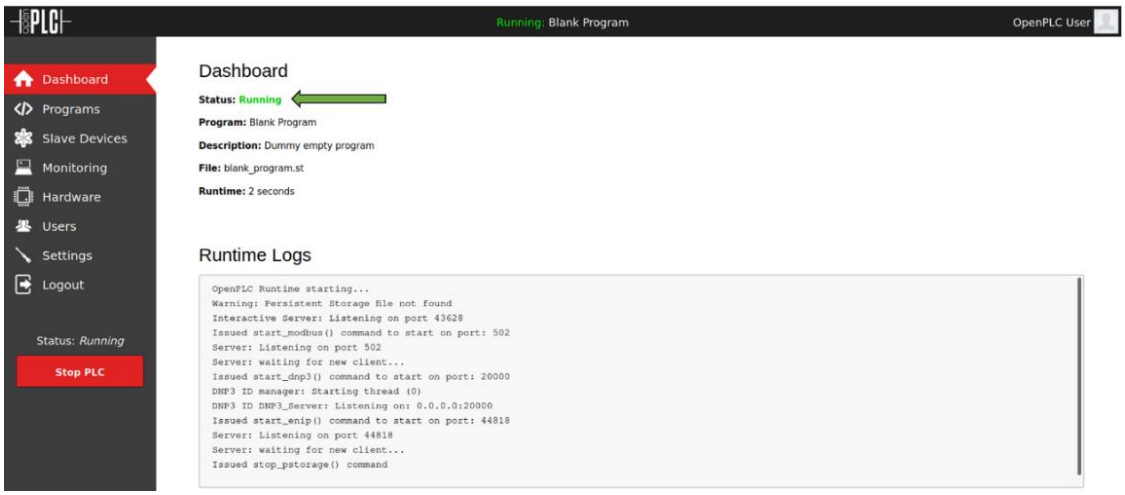

Ilustración 28: OpenPLC modo RUN

Repetimos estos últimos pasos de manera análoga para el otro PLC desplegado en el entorno virtualizado, de forma que ambos forman parte de un hipotético proceso, el cual veremos ahora como podríamos visualizar mediante la utilización de un HMI.

Una vez desplegados los PLCs, procedemos a configurar ScadaBR. Para la instalación los pasos son prácticamente análogos a los empleados anteriormente. Una vez instalado procedemos a configurar nuestro HMI en la interfaz web. Como vimos en la ejecución del programa de OpenPLC estamos empleando protocolo Modbus por el puerto por defecto 502, de este modo procedemos a configurar los conocidos como “Data Sources” del HMI, los cuales serán los PLCs vía Modbus (a partir de este punto aplicamos una configuración de red restringida solo a conexión local sin salida a Internet).

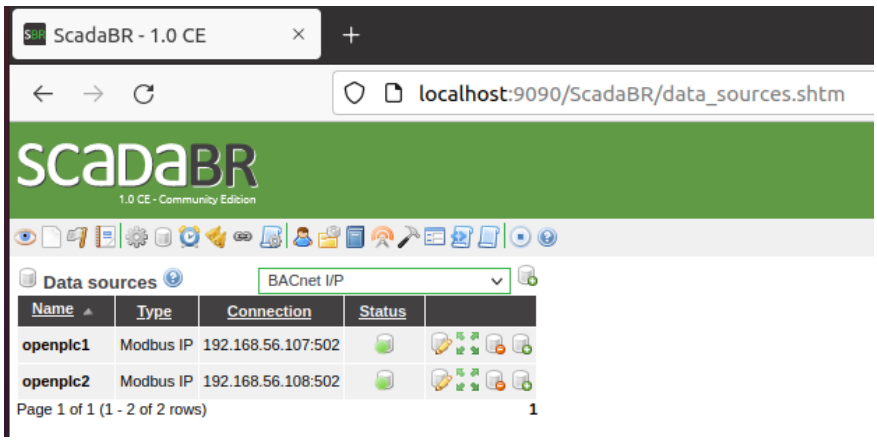

Ilustración 29: OpenPLC asignados en ScadaBR

De este modo enlazamos ambos PLCs como fuentes de datos al HMI y desde este punto podemos crear los denominados puntos que controlan las variables de entrada y salida del hipotético proceso y su interacción con los PLCs. En este momento tenemos por tanto ya una primera versión del HMI con la visualización por ejemplo de dos puntos, uno por cada PLC y ambos de tipo binario (por ejemplo, apertura-cierre de una compuerta).

Ilustración 30: ScadaBR HMI

Inclusive, una vez configuradas dichas variables podemos crear multitud de distintas vistas, por ejemplo, forzando un cambio del valor binario en uno de ellos en base a una gráfica de tiempo:

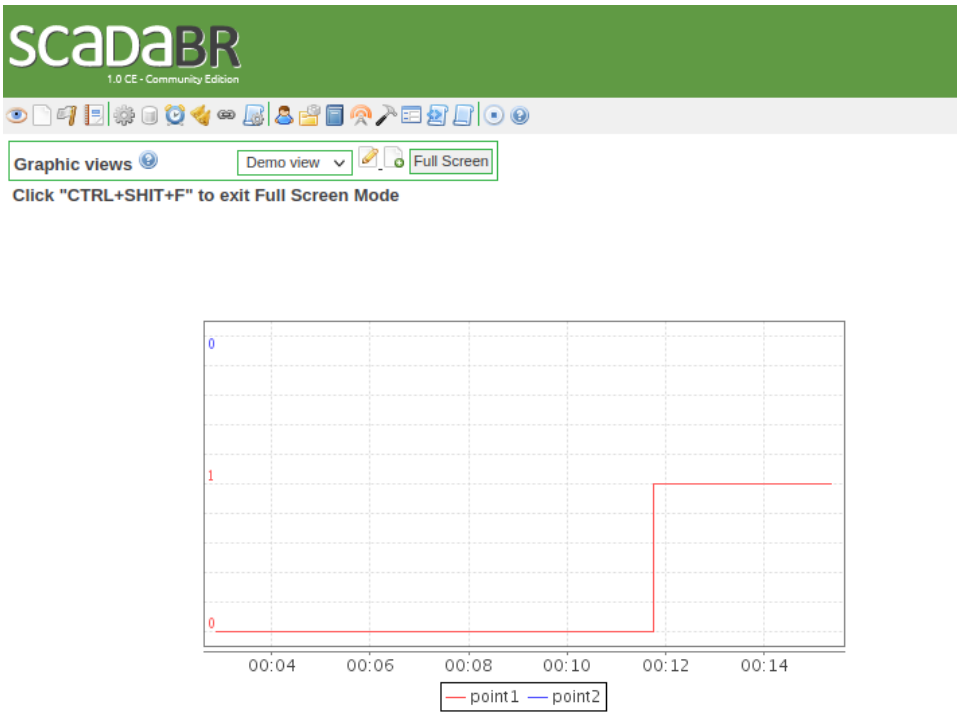

Ilustración 31: Visualización de variables vía HMI

En este punto contamos ya por tanto con el escenario básico descrito al principio: un par de PLCs ejecutando un programa industrial inocuo y una máquina actuando como HMI que permite una visualización de variables del proceso industrial. A nivel esquemático puede ser representado de la siguiente forma:

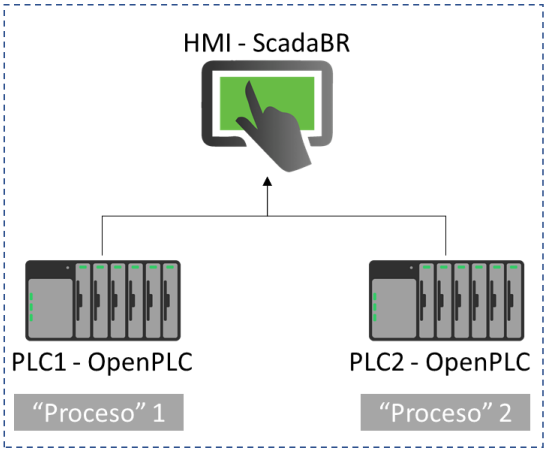

Ilustración 32: Esquema para virtualizar entorno industrial

Pasamos por tanto en este punto a desplegar la tecnología Deception en dicho entorno. Para ello se empleará el framework open source denominado DejaVu, el cual permite probar esta tecnología tipo Deception mediante la utilización de señuelos desplegados en la infraestructura bajo el alcance.

La arquitectura tipo de DejaVu pivota sobre todo en 2 elementos principales:

- Motor: máquina encargada de desplegar los señuelos definidos en cada campaña Deception. Idealmente se emplearán tantos motores como redes estén bajo el alcance al tratarse despliegues locales.
- Consola de administración: consola integral de gestión centralizada que permite gestionar los distintos motores y alertas generadas propias de la naturaleza de las campañas. De manera gráfica permite tener una visión general del entorno.

De esta manera la arquitectura de esta solución se perfila como se ve en la siguiente ilustración:

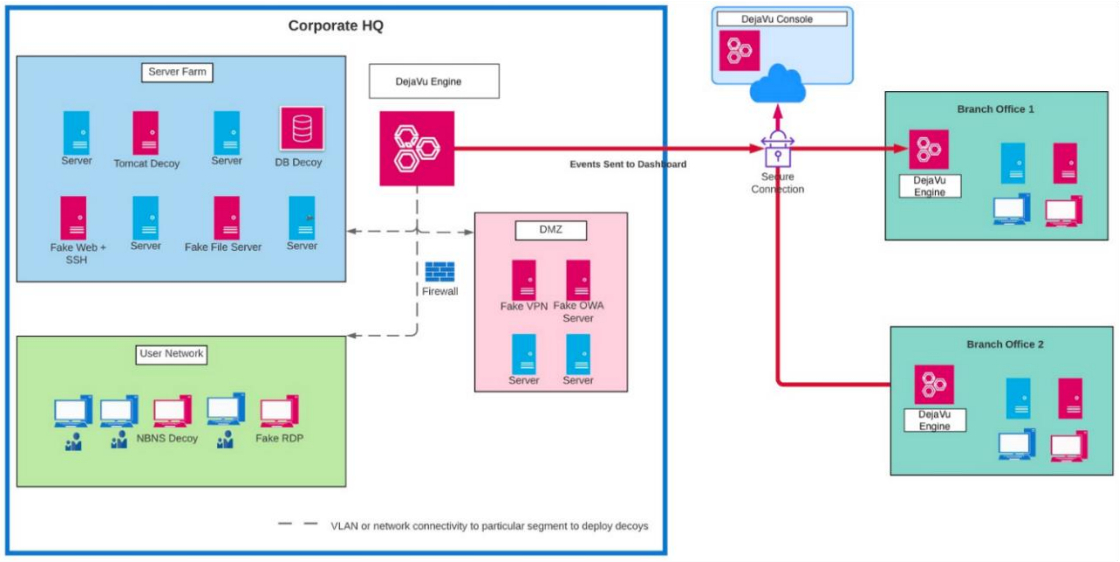

Ilustración 33: Arquitectura genérica DejaVu Deception

Para nuestro caso de estudio concreto, emplearemos únicamente 1 motor al tratarse de una única red local y limitada. Igualmente se empleará 1 consola de gestión que permitirá realizar las tareas de administración de la herramienta asociada a la lógica de las campañas.

Pasamos por tanto a desplegar en nuestro laboratorio virtual local ambos elementos que permitirán añadir estas capacidades de detección de seguridad a nuestra red de proceso industrial. Para ello, desde la propia web del proyecto podemos descargar de manera oficial las imágenes de disco duro en formato VDI el cual es compatible con Oracle VirtualBox.

Empezamos por crear la máquina para la consola de gestión, asignando el disco en cuestión y arrancando dicha máquina para obtener acceso a la consola de gestión de forma local tras aplicar la configuración de red requerida.

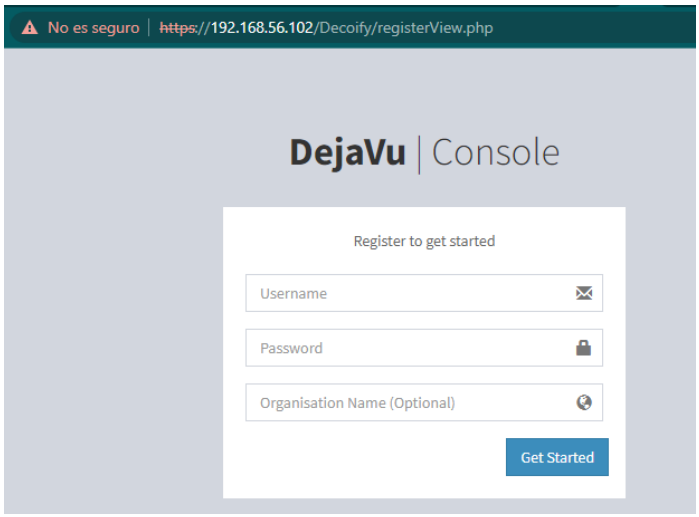

Ilustración 34: DejaVu Console instalación

Registramos un usuario de forma local en la aplicación y accedemos al cuadro de mando donde podremos gestionar a futuro el motor Deception que desplegaremos a continuación.

Para ello seguimos pasos definidos en la creación de máquina virtual. El punto característico más importante en este caso consiste en que el motor emplea dos adaptadores de red, uno para conexión con la propia consola de gestión y otro para el uso de señuelos, en este caso concreto se trata de la misma red, pero en circunstancias de entornos reales lo más usual es que la consola de gestión esté separada del alcance de la campaña, tanto por razones operativas enfocadas a resultados como propias de seguridad.

Una vez configurado el motor pasamos a establecer la comunicación con la consola de gestión y arrancar el motor:

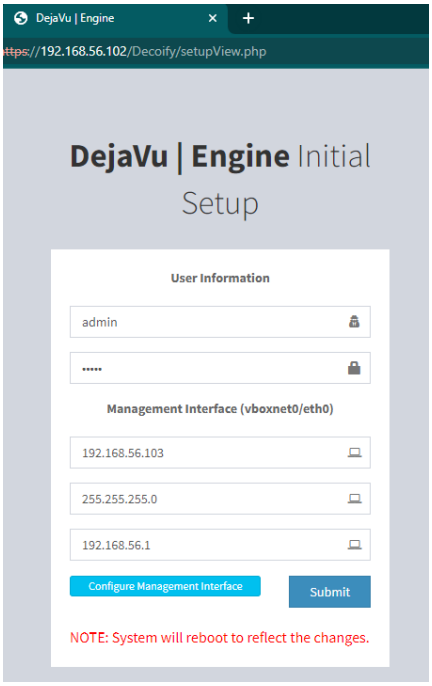

Ilustración 35: DejaVu Engine configuración

De este modo podremos acceder ya a la consola del motor de DejaVu con lo cual podremos empezar a desplegar los señuelos como parte de la campaña Deception diseñada.

El escenario actual tras los despliegues y configuraciones realizadas ha quedado de la siguiente manera, incluyendo una máquina atacante basada en la conocida suite de seguridad Kali Linux, la cual emplearemos para futuras pruebas de seguridad sobre el entorno y la campaña Deception diseñada:

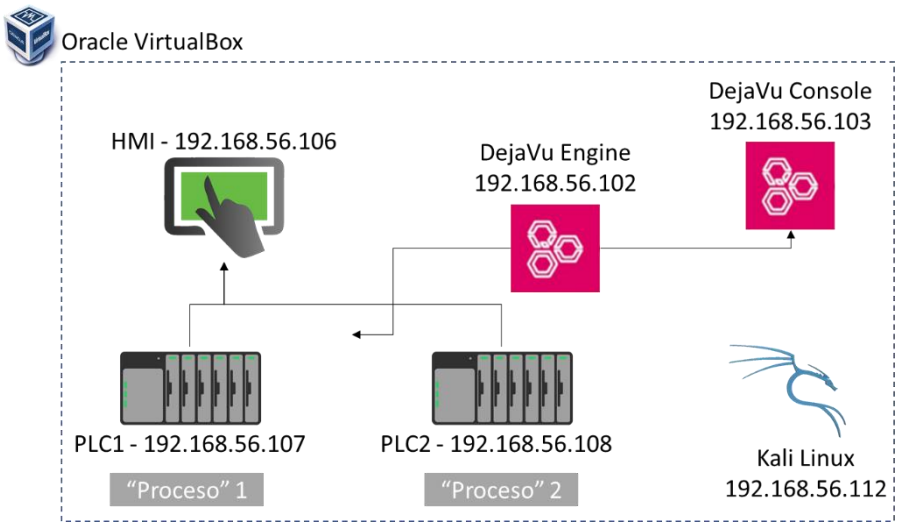

Ilustración 36: Arquitectura escenario 1

A partir de este punto pasamos a enlazar los componentes de DejaVu de forma que la consola central sea capaz de recoger los eventos generados por los señuelos y distintos artefactos creados y gestionados por el motor.

Para ello se emplean comunicaciones vía API con autenticación basada en claves para establecer dicha comunicación.

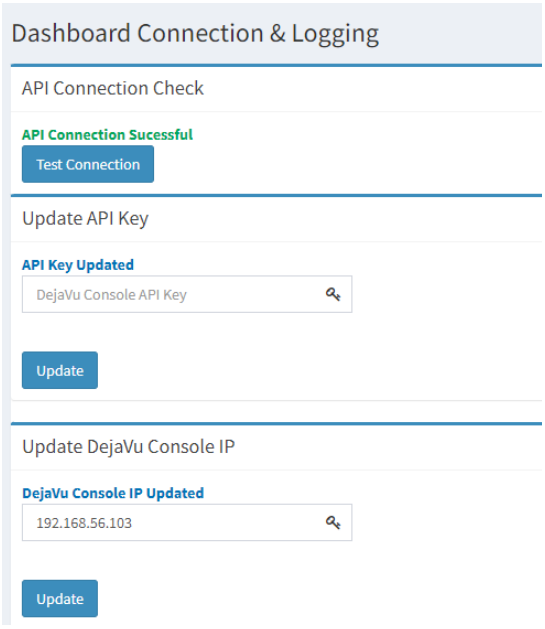

Ilustración 37: Conexión entre consola central y motor

Pensando que estamos en el escenario 1, focalizado en entornos industriales en niveles más bajos, diseñaremos una campaña Deception acorde a dicho escenario. Para ello, los señuelos a emplear serán de una naturaleza que tenga sentido de cara un atacante, de forma que le permita interactuar con él y de este modo se pueda recabar información del actor en cuestión y sus TTPs[24].

De esta manera empleamos el servidor e*ngine* (motor) de DejaVu para empezar el despliegue de dichos señuelos. En paralelo, como se ha mencionado anteriormente, desplegaremos una máquina atacante basada en la distribución Kali, de forma que se perfile bajo el escenario planteado como un posible atacante con acceso a la red virtualizada, por ejemplo: mediante acceso físico como podría ser un *insider* o mediante incluso acceso remoto debido a una incorrecta segmentación de la red unido a un compromiso de credenciales, escenarios bastante usuales de ataques reales.

Si accedemos a la consola de creación de señuelos vemos que de forma bastante esquemática es posible realizar diversas acciones para dar comienzo a la campaña de Deception:

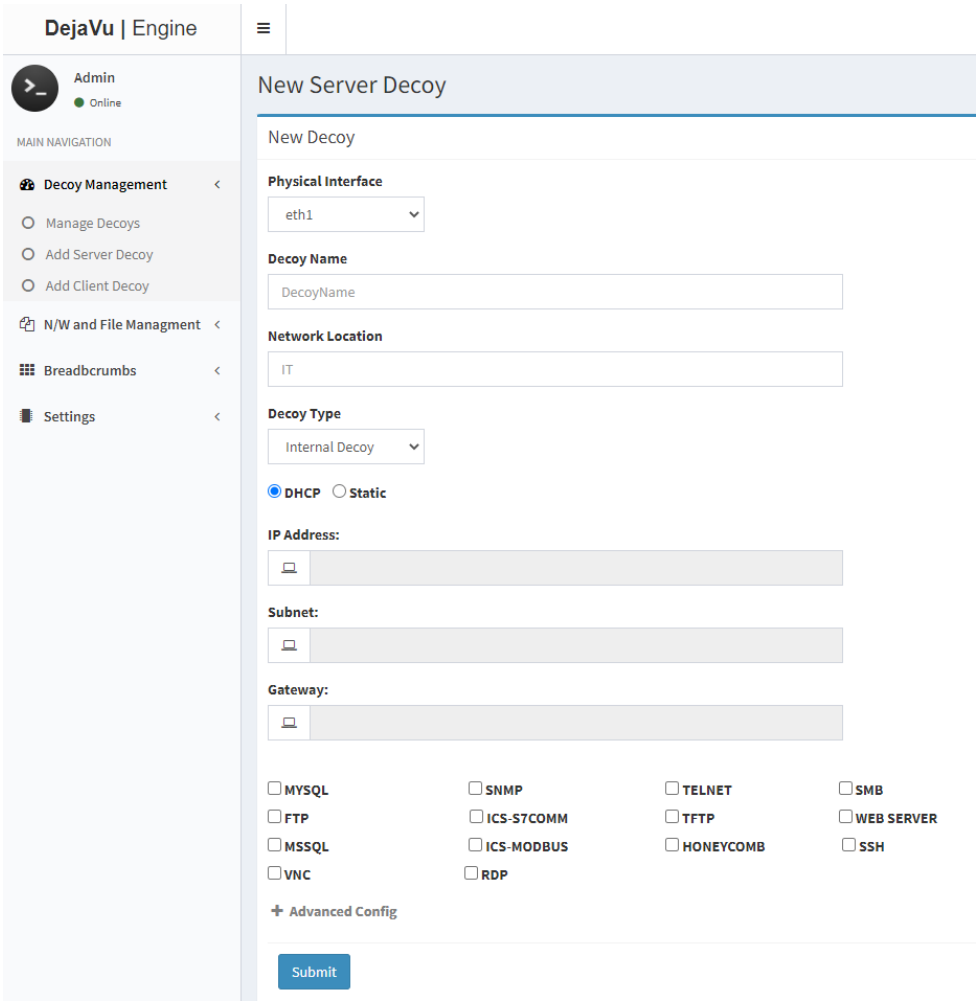

Ilustración 38: Creación de señuelos con DejaVu

[24] https://csrc.nist.gov/glossary/term/Tactics_Techniques_and_Procedures

Al tratarse de un entorno industrial emplearemos por un lado los dos señuelos propios de entornos ICS (Industrial Control Systems):

- S7 Comm
- Modbus

Adicionalmente, de forma que podamos probar algún escenario distinto también emplearemos un señuelo basado en protocolo VNC, ampliamente extendido en entornos industriales para la operación y gestión remota y local de dispositivos.

Todos estos señuelos se expondrán de manera dinámica según se vayan creando mediante la interfaz de red definida para ello, en este caso la eth1.

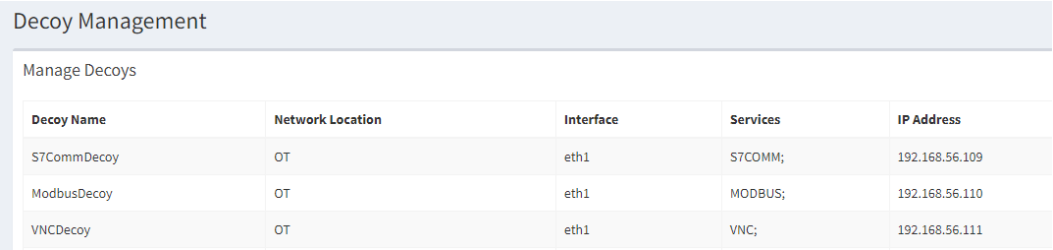

Ilustración 39: Señuelos creados para escenario 1

De este modo, de forma totalmente transparente para la operación del entorno industrial se han desplegado de manera ficticia unos señuelos en forma de servidores. Estos señuelos ahora conviven en paralelo con los dispositivos productivos, pero sin establecer ningún tipo de comunicación con los mismos de forma que no afectan a la disponibilidad del entorno. Además, se ha desplegado una línea de detección de seguridad en un entorno donde en un principio los dispositivos alojados en dichos niveles inferiores de la automatización no son capaces por lo general de implementar mecanismos de seguridad, como por ejemplo basados en agente.

Este último punto es de especial relevancia, ya que según el diseño que se otorgue a cada campaña de Deception los señuelos contarán con una "interactividad" mayor o menor de forma que el atacante se entretenga más o menos y en consecuencia debe estar alineado con no levantar sospechas ya que en dicho caso, la validez de las pruebas y la información recabada quedaría en entredicho.

En este punto adoptaremos la postura de un posible atacante, el cual ha conseguido acceso a este segmento de red y busca información que pueda exfiltrar para la competencia o inclusive para llevar a cabo un ataque dirigido tipo APT. Siguiendo esta lógica del atacante emplearemos como mencionamos anteriormente la suite Kali al contar con multitud de herramientas útiles ya preinstaladas.

Uno de los primeros pasos sería ejecutar un descubrimiento de activos de forma que podamos tener visibilidad de la red comprometida:

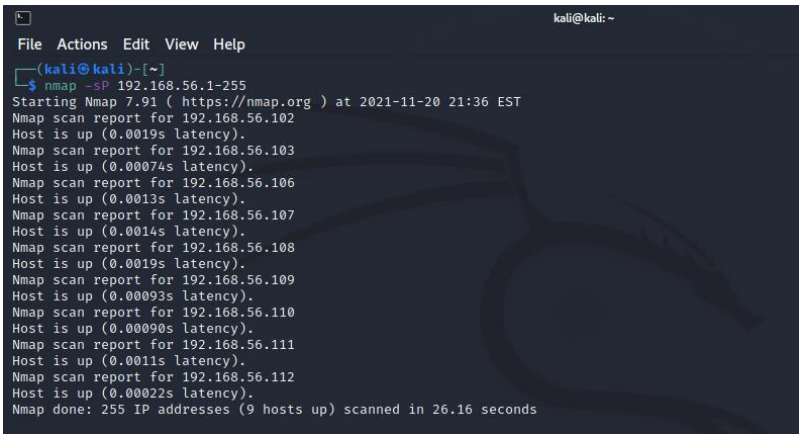

Ilustración 40: Descubrimiento de activos con Nmap

Vemos que existen por tanto unos cuantos dispositivos disponibles en la red, entre ellos dispositivos reales, pero también los relacionados con la campaña de Deception, pero no solo los señuelos que son evidentemente candidatos a ser descubiertos, sino también el propio motor y la consola de gestión. Este aspecto es de especial relevancia ya que en caso de que el atacante descubra la "fórmula" del engaño (en este caso basado en DejaVu) la campaña sería un fracaso ya que el atacante habría detectado que se encuentra en un escenario el cual potencialmente está siendo manipulado.

Como contramedida a este aspecto, lo ideal sería que tanto el motor como la consola no sean accesibles por parte del atacante, en este caso concreto al tratarse de una red plana es sencillo, pero la consola de gestión debería estar localizada en capas más superiores como una DMZ. Por su parte el motor por lo general estará cercano a puntos de conexión vía switch, sobre todo por su capacidad de crear y gestionar señuelos en distintas VLAN apoyándose en la función de trunk port ofrecida por multitud de dispositivos de electrónica de red, por lo que se deberá proteger mediante mecanismos de filtrado de tráfico. Idealmente se podría aplicar un filtrado de acceso al portal web, de forma que sólo se pueda acceder a los portales de gestión desde los dispositivos autorizados (este mecanismo puede ser vulnerado mediante técnicas de *spoofing* pero para ello el atacante deberá conocer las direcciones permitidas lo cual se antoja más complejo).

Volviendo al flujo de ejecución del atacante, a pesar de haber realizado solo un pequeño barrido de descubrimiento de máquinas ya se ha generado una serie de alertas en la consola de gestión, las cuales en caso de estar configuradas podrían haber generado el envío de notificaciones a los responsables.

Una de las funciones más útiles es la que emplea gráficos para esbozar la trazabilidad de las acciones del atacante:

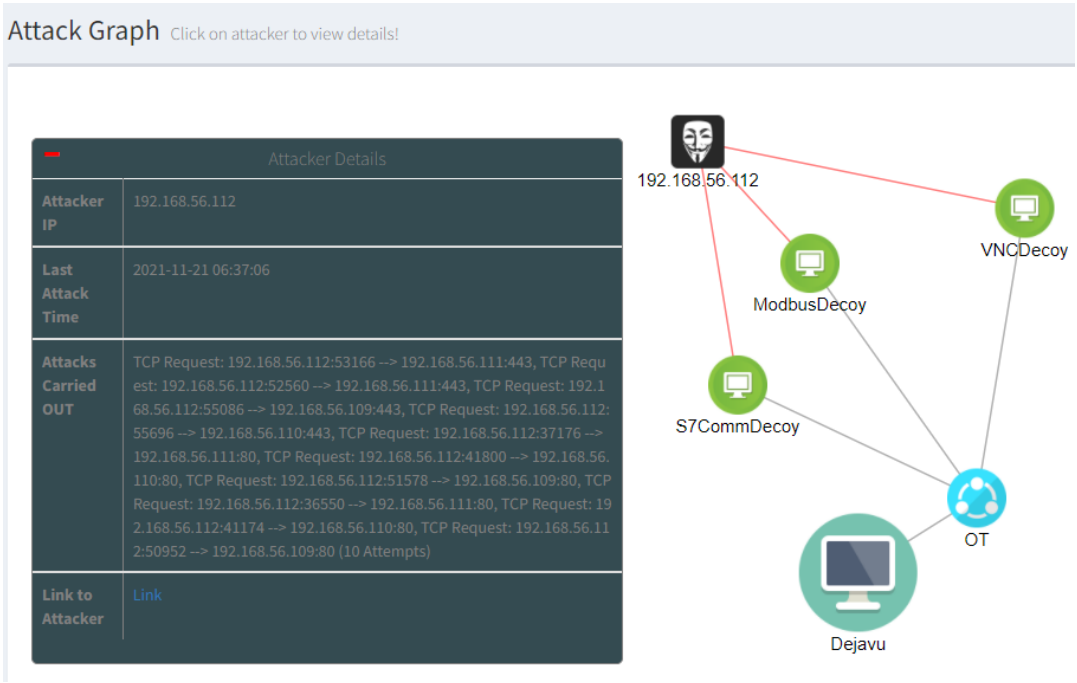

Ilustración 41: Gráfico de ataque DejaVu

De igual manera, la herramienta es capaz de capturar a nivel de logs la información que está también disponible en la interfaz web e inclusive es posible realizar una integración vía Syslog lo cual podría por tanto permitir una integración de herramienta tipo SIEM para correlación de eventos de seguridad:

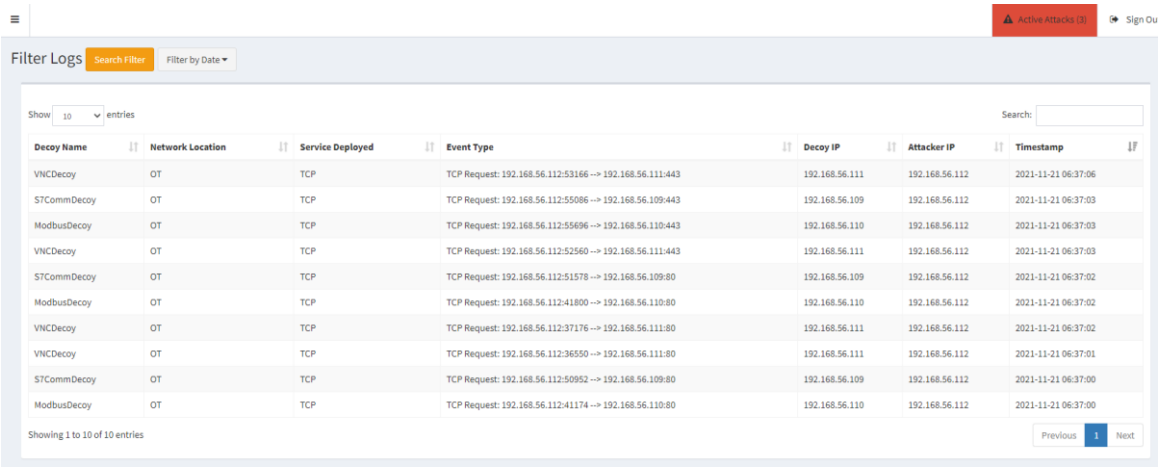

Ilustración 42: Logs de actividad DejaVu

Veamos ahora que ocurre si focalizamos los esfuerzos en el señuelo de tipo Modbus. El atacante ejecuta un escaneo de puertos un poco más dedicado de forma que sea capaz de identificar el activo y de este modo ve que el puerto 502 está abierto en el señuelo de Modbus. Por ello, mediante metasploit se pretende detectar dicho servicio Modbus:

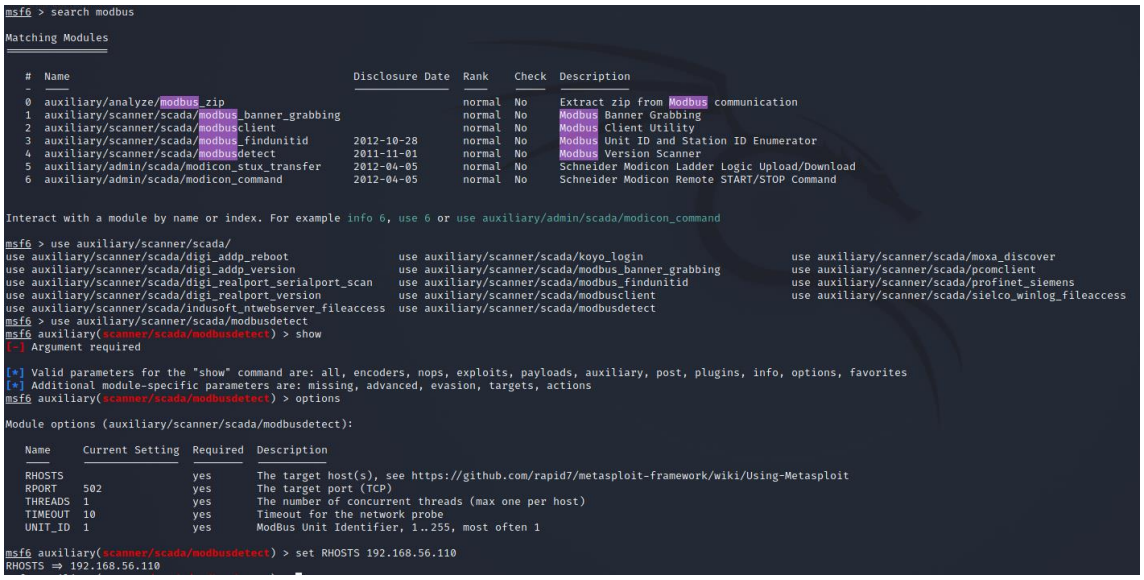

Ilustración 43: Utilización metasploit Modbus

Tras la ejecución del exploit, se ha generado una nueva alerta en la consola central que se enseña a continuación permitiendo incluso descargar un fichero de tipo pcap con las comunicaciones registradas:

Ilustración 44: Alerta de detección Modbus

Aplicando la misma lógica, el atacante es capaz de detectar también el puerto 102 abierto en otro dispositivo, lo cual lo perfila con el servicio iso-tsap característico de la familia de dispositivos S7 que emplean su protocolo de comunicaciones propio y para el cual existen multitud de vulnerabilidades conocidas que en caso de dispositivos sin actualizar podrían ser explotados.

Por último, realizamos un escaneo sobre el señuelo tipo VNC y obtenemos los siguientes resultados en cuanto a puertos abiertos:

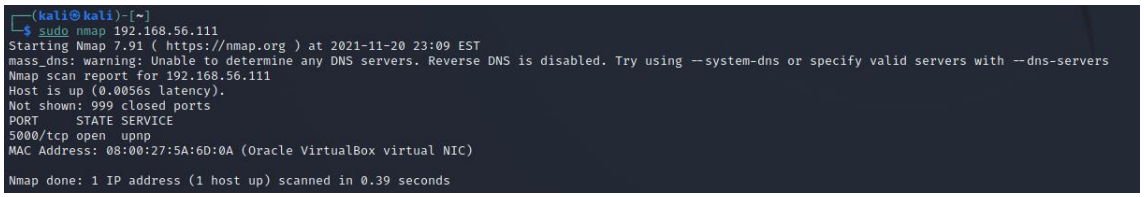

Ilustración 45: Escaneo de puertos VNC

En este caso concreto no es posible ejecutar ataques concretos más avanzados contra servicios Upnp, además de estar fuera del alcance del presente trabajo. Sin embargo, de forma que podamos explorar un poco más en profundidad las opciones disponibles a nivel de interacción con los señuelos procedemos a

desplegar un nuevo señuelo basado en un servidor SSH, que por ejemplo en este escenario actual podría ser el terminal de acceso local del proceso y mediante el cual se realizan tareas de administración a más bajo nivel.

Procedemos por tanto a realizar un escaneo mediante NMAP del nuevo señuelo detectado por el atacante, obteniendo la siguiente información:

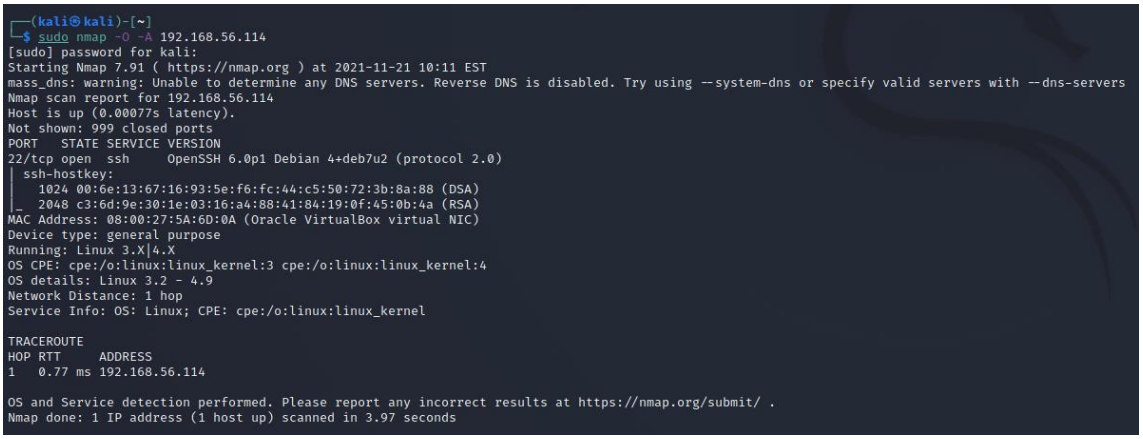

Ilustración 46: Escaneo de puertos de señuelo SSH

Vemos que cuenta con el puerto de administración remota por defecto (22) abierto para conexiones SSH. De modo que probamos con el usuario administrador por defecto como haría cualquier atacante real:

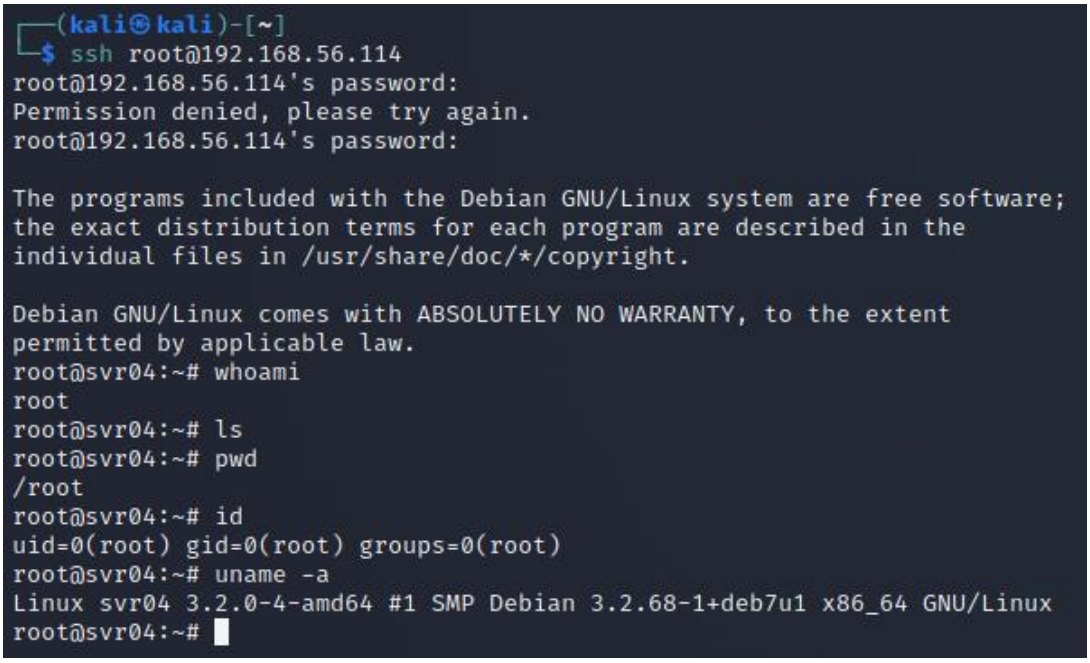

Ilustración 47: Login en señuelo SSH con privilegios

En este caso el señuelo utiliza las credenciales por defecto para el usuario administrador de Linux (*root:toor*) y además emplea cierta interacción con el

atacante. Procedemos a buscar información interesante del propio señuelo como pueden ser ficheros de usuarios y hashes:

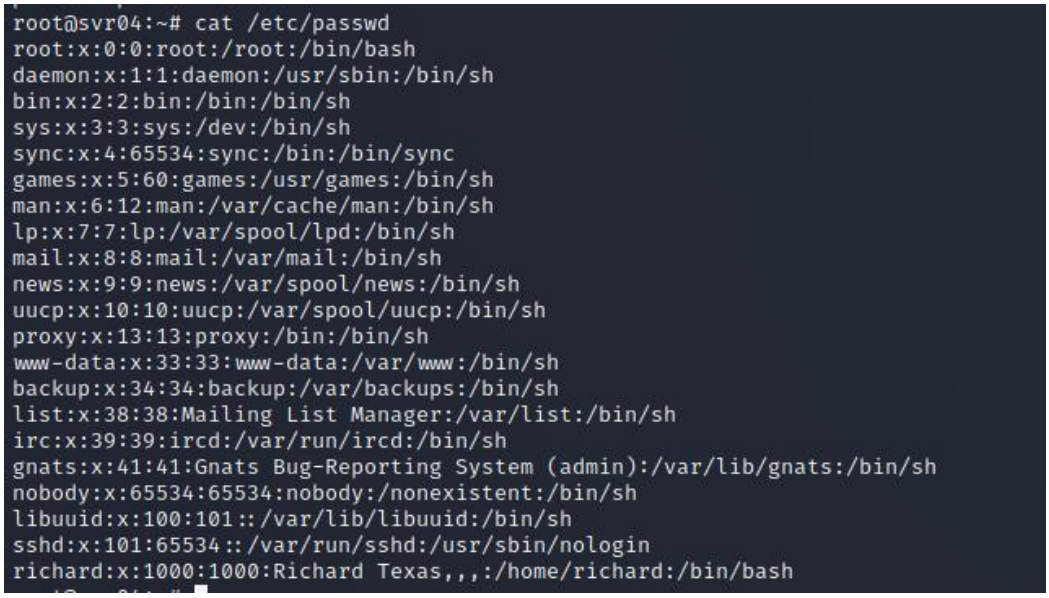

Ilustración 48: Consulta de información en señuelo SSH

Por su parte si acudimos a la consola de gestión de la solución vemos que se han registrado todas las acciones efectuadas por el atacante, de forma que es posible entender el flujo de ejecución del ataque y aprender incluso de esta manera más detalles de cómo podría ser una posible *kill-chain* de un actor concreto.

De forma que se realicen tareas de detección más avanzadas se pueden ejecutar una serie de tareas mediante orquestación del motor Deception como podría ser añadir los señuelos a un dominio o inclusive crear cuentas de usuarios de forma que el atacante ejecute un ataque tipo "*pass-the-hash"* con herramientas como Mimikatz[25] según vaya avanzando el flujo de ataque definido por la campaña.

Siguiendo esta idea se podrían seguir desplegando nuevos señuelos en los cuales a su vez expondremos ficheros con un nombre el cual puede llamar la atención del atacante, este tipo de artefactos se le conocen como migas de pan en la terminología de tecnologías Deception.

Tal y como hemos mencionado anteriormente, durante la ejecución de estas pruebas no ha habido ninguna alteración de los dispositivos "reales" del entorno industrial, por lo que podemos valorar de manera positiva este tipo de tecnología si se emplea de manera correcta y bajo unas reglas de campañas claramente definidas.

Es importante reseñar también, que en este caso concreto la herramienta DejaVu es bastante intuitiva y permite cierta configuración y parametrización de los artefactos y señuelos Deception. Sin embargo, en comparación con otras

[25] https://github.com/ParrotSec/mimikatz

soluciones de mercado comerciales se encuentra en una etapa más temprana de desarrollo, especialmente en lo que se refiere a la utilización de mecanismos de engaño para entornos industriales de capas más inferiores como los que se han empleado en este escenario. Es por este motivo también por el que llevaremos a cabo un segundo escenario para entornos OT, pero enfocado a capas más superiores del modelo de Purdue, como podría ser una DMZ industrial donde es más factible encontrarse con elementos más parecidos al mundo IT como servidores y clientes de ingeniería.

4.2 Escenario 2: niveles superiores y DMZ industrial

En este segundo escenario se pretende emular una DMZ industrial. Dicho segmento de red se caracteriza por ser la red desmilitarizada bajo la cual es posible efectuar intercambios de comunicación entre capas superiores e inferiores. Por este motivo se suele encontrar con ciertos servicios que puedan salir a internet ya sea de manera enrutada por la red corporativa (mejor escenario posible a nivel de seguridad) o en otros casos desde este punto. Los dispositivos que se suelen encontrar en este tipo de redes suelen ser servidores de actualizaciones (de parches, firmas de base de datos de virus, etc), máquinas de salto para accesos remotos y servidores de intercambio de archivos. Es por tanto evidente que este escenario es más similar al mundo tradicional de IT por lo que no se entrará tanto en detalle como el apartado anterior el cual era específico del mundo industrial.

De esta manera procedemos a desplegar de igual forma una serie de máquinas que actuarán de esta forma en el entorno de modo que el escenario desplegado sería el siguiente:

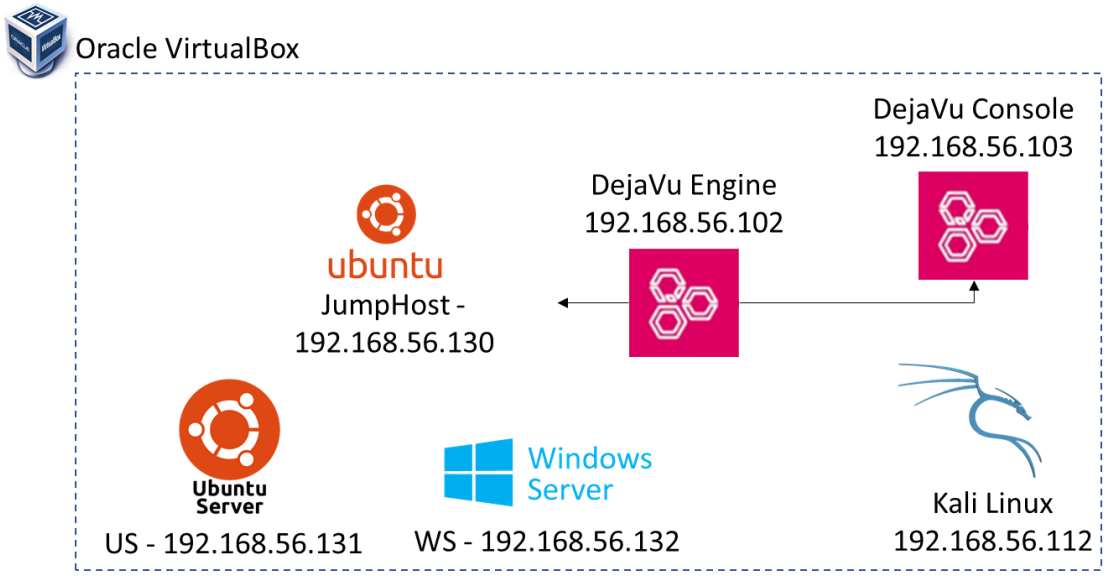

Ilustración 49: Escenario 2 DMZ industrial

Con esta arquitectura pasamos a utilizar nuevamente nuestro framework Deception DejaVu de forma que en este caso utilicemos señuelos que podría un atacante encontrarse en este tipo de redes y escenario. Es importante destacar que este tipo de redes DMZ estarán protegidas por un firewall perimetral el cual permitirá únicamente el tráfico entrante necesario como podría ser el que vaya dirigido al servidor de salto y aplicando restricciones como pueden ser control de autenticación basado en doble factor. Este firewall perimetral en este caso no se virtualiza ya que no es relevante para la consecución de los objetivos de este caso concreto y se partirá de la base de que se exponen ciertos señuelos alcanzables desde la red corporativa o en algunos casos desde redes externas de forma que se lleve a cabo una campaña avanzada para recabar información de posibles actores externos.

En primera instancia desplegamos un señuelo tipo WebServer en el cual se emulará el portal Web de la VPN del fabricante de seguridad F5, bastante extendido en el sector.

Pasamos como atacante a realizar un escaneo sobre IPs en expuestas en la DMZ y vemos que existe una IP la cual no tenemos constancia de su existencia. Procedemos por tanto a realizar un escaneo un poco más dedicado de forma que podamos extraer algo más de información:

Ilustración 50: Escaneo sobre señuelo web server

Vemos que se trata de una máquina con el puerto web expuesto, tanto el 80 como el 443 (podemos ver incluso ciertos datos del certificado como el país de emisión). Procedemos a abrir dicho portal web y nos encontramos con el control de autenticación del portal de F5 networks el cual podría corresponderse con el cliente utilizado para servicios de conexión remota tipo VPN:

Ilustración 51: Portal web de autenticación F5

Tras probar varios tipos de credenciales el atacante desiste ya que no ha conseguido entrar al sistema.

Desde la consola de gestión de señuelos toda esta actividad se ha registrado como se puede ver a continuación:

Decoy Name	Network Location	Service Deployed	Event Type	Decoy IP	Attacker IP
WebServerDecoy	DMZ	APACHE	Authentication attempt using username=admin and password=admin HTTP1.1" 200 6106 "https:192.168.56.116" "Mozilla5.0 Windows NT 10.0 Win64 x64 AppleWebKit537.36 KHTML like Gecko Chrome96.0.4664.45 Safari537.36"	192.168.56.116	192.168.56.1
WebServerDecoy	DMZ	APACHE	Authentication attempt using username=admin and password=admin" "Mozilla5.0 Windows NT 10.0 Win64 x64 AppleWebKit537.36 KHTML like Gecko Chrome96.0.4664.45 Safari537.36"	192.168.56.116	192.168.56.1
WebServerDecoy	DMZ	APACHE	HTTP Connection: -	192.168.56.116	192.168.56.1
WebServerDecoy	DMZ	APACHE	HTTP Connection: -	192.168.56.116	192.168.56.1
WebServerDecoy	DMZ	APACHE	HTTP Connection: GET	192.168.56.116	192.168.56.1
WebServerDecoy	DMZ	APACHE	HTTP Connection: GET	192.168.56.116	192.168.56.112

Ilustración 52: Actividad señuelo WebServer

Pasamos a desplegar un segundo señuelo, en este caso basado en el servicio RDP el cual permite realizar sesiones remotas a nivel escritorio con equipos Windows. Este tipo de escenarios es común para la ejecución de tareas de operación en entornos remotos y los servicios expuestos tipo RDP abundan en buscadores tipo *Shodan*[26].

De esta forma el atacante descubre un servicio RDP expuesto y por tanto ejecuta un intento de inicio de sesión por el puerto por defecto 3389:

[26] https://www.shodan.io/

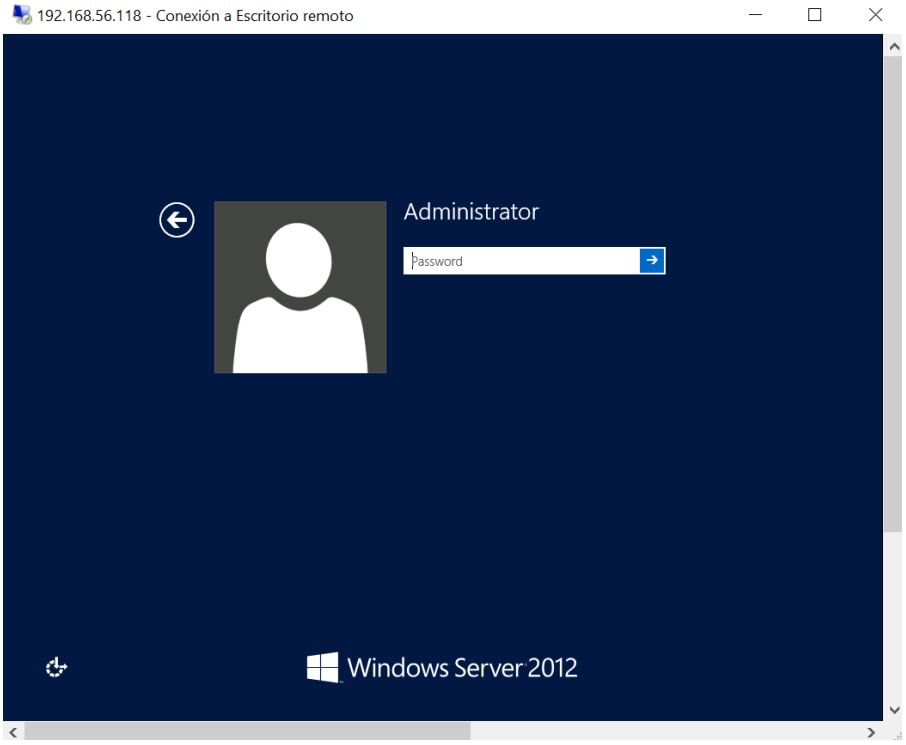

Ilustración 53: Señuelo basado en RDP para DMZ

En este caso, este tipo de señuelo no presenta mayor interacción y solo permite llevar un conteo de los intentos de conexión por el puerto RDP.

Por último, pasamos a desplegar un señuelo que nos permita simular un entorno de almacenamiento de archivos o información, que podría ser considerado como Historian del entorno industrial y el cual proporcionaría datos de relevancia de la producción para su explotación exterior (por ejemplo, para la optimización de procesos o de cara a almacenamiento histórico de volumetrías). Para ello se desplegará un servidor de tipo FTP para el alojamiento y compartición de archivos. En multitud de ocasiones se emplea este mecanismo para poder compartir información en entornos industriales, al ser sencillo de utilizar y permitir el intercambio de datos como pueden ser volúmenes de producción o incluso datos relacionados con inventario. Además, se desplegará también un servicio MySQL en el señuelo de forma que sea evidente el objetivo de esta máquina en el entorno. Es por ello por lo que una campaña Deception podría apoyarse en este tipo de señuelo, el cual pasamos a desplegar e interactuar con él mediante el motor DejaVu.

Una vez más, simulando ser un atacante que pretende obtener información sobre los activos alcanzables, procedemos a hacer un *Ping Sweep* de forma que detectemos posibles IPs. Tras ello detectamos una IP nueva la cual escaneamos con NMAP para poder enumerar sus servicios y puertos abiertos, de modo que vemos el puerto 21 para FTP y el 3306 para MySQL.

Ilustración 54: Señuelo FTP/MySQL desplegado en entorno DMZ

Vemos que expone por tanto ambos servicios y sus versiones específicas. En caso de emplear soluciones Deception de tipo más avanzado como las que se distribuyen a nivel profesional se podría elaborar una campaña más específica creando las denominadas migajas pan, con por ejemplo información tipo credenciales de sesiones *ssh* para de este modo orquestar la creación de otros señuelos en base al descubrimiento de estas pistas dejadas de forma intencionada. Por ejemplo, otro tipo de flujo de ataque sería la búsqueda de *exploits* asociados a las versiones que se ejecutan en ambos servicios.

Por tanto, hemos visto en este último apartado que este tipo de soluciones Deception es también compatible en entornos menos OT o capas superiores del entorno industrial, de forma que se pueda presentar como una solución completa hasta el punto de poder emplearse con distintos mecanismos y diversas campañas Deception que permitan mejorar las capacidades de detección y ciber inteligencia de la organización sin afectación a su operación diaria.

5. Conclusiones

En la presente sección pasamos a desglosar las conclusiones obtenidas tras la ejecución del presente trabajo, en base los objetivos y metodología definidos.

Como hemos visto, sobre todo en las últimas fechas, la ciberseguridad es una preocupación a nivel global, llegando incluso a igualarse con temas tan importantes como el cambio climático o las fluctuaciones económicas del mercado. Si ahondamos un poco más, en lo que se refiere a ciberseguridad en entornos industriales el panorama es incluso más alarmante al tratarse de una considerada como asignatura pendiente hasta hace no demasiados años. Los entornos OT son especialmente críticos al tratarse en muchas ocasiones de entornos para los cuales la vida humana tiene una gran dependencia como por ejemplo empresas de servicios críticos como pueden ser las de generación o distribución de energía o inclusive de tratamiento de aguas o distribución de alimentos.

Es por este motivo por el cual se planteó el objetivo de, basándonos en los estándares del sector como el IEC 62443, la idea de definir una arquitectura de referencia de seguridad la cual permita contar con un nivel mínimo de seguridad. Adicionalmente, se planteó la idea de utilizar una tecnología considerada bastante novedosa como es Deception, en los entornos industriales. Para ello se realizó un estudio teórico de este tipo de soluciones y su aplicabilidad, para posteriormente realizar un estudio práctico basado en herramientas de código abierto el cual permitió obtener una serie de conclusiones:

- La tecnología Deception se caracteriza por ser autocontenida, lo cual es muy interesante para entornos industriales al no tener interacción con demás elementos.
- Permite la creación de mecanismos automatizados, precisos y aplicando correlación de eventos en base a las campañas de detección de señuelos desplegada.
- Las herramientas gratuitas de código abierto son limitadas, sin embargo, las herramientas de mercado ofrecen multitud de posibilidades avanzadas.
- Permite entender cómo funcionan los potenciales ciber atacantes de forma que permite aplicar contramedidas de acuerdo con las tendencias.
- Debe ser interpretado como una capa adicional de protección en cuanto a ciber inteligencia, pero no como una solución única de seguridad que anule a otros mecanismos como bastionado, protección mediante agentes cuando es posible, etc.

Por tanto, se ha cumplido la planificación planteada del trabajo unida a la metodología definida, incluyendo el estudio teórico junto con las pruebas prácticas lo cual ha permitido obtener las conclusiones desglosadas anteriormente.

6. Glosario

- **OT:** Tecnología operacional
- **Deception:** Tecnología de engaño, definida como la evolución de los tradicionales Honeypots.
- **ICS:** Sistemas de control industrial.
- **SIEM:** Security Information and Event Management.
- **PLC:** Controlador lógico programable.
- **DCS:** Sistema de control distribuido.
- **SCADA:** Supervisión, control y adquisición de datos

7. Bibliografía

William Turton and Kartikay Mehrotra. (4 de junio de 2021). *Hackers Breached Colonial Pipeline Using Compromised Password*. Obtenido de Bloomberg Cybersecurity: https://www.bloomberg.com/news/articles/2021-06-04/hackers-breached-colonial-pipeline-using-compromised-password

ACATECH. (2013). *Recommendations for implementing the strategic initiative INDUSTRIE 4.0.* Germany. Obtenido de https://www.din.de/blob/76902/e8cac883f42bf28536e7e8165993f1fd/recommendations-for-implementing-industry-4-0-data.pdf

Attivo Networks. (s.f.). *Security Solutions for the Energy Sector*. Obtenido de https://www.attivonetworks.com/solutions/energy/

CounterCraft - Richard Barrel. (s.f.). *Boosting OT Security with Cyber Deception*. Obtenido de https://www.countercraftsec.com/blog/post/boosting-ot-security-with-cyber-deception/

David Kushner | IEEE Spectrum & Kasperksy Lab. (2013). *IEEE Spectrum*. Obtenido de THE REAL STORY OF STUXNET: https://spectrum.ieee.org/the-real-story-of-stuxnet

Deloitte. (s.f.). *Deloitte insights*. Obtenido de COLLECTION INDUSTRY 4.0: https://www2.deloitte.com/us/en/insights/focus/industry-4-0.html

Gartner. (18 de May de 2015). *What Is Industrie 4.0 and What Should CIOs Do About It?* Obtenido de Gartner Press Releases: https://www.gartner.com/en/newsroom/press-releases/2015-05-18-what-is-industrie-4-and-what-should-cios-do-about-it

History: A&E Television Networks. (s.f.). *History.com*. Obtenido de Industrial Revolution: https://www.history.com/topics/industrial-revolution/industrial-revolution

INCIBE. (25 de 08 de 2015). *IEC 62443: Evolución de la ISA 99*. Obtenido de Incibe CERT: https://www.incibe-cert.es/blog/iec62443-evolucion-isa99

ISA 95 / IEC. (s.f.). *IEC 62443.*

Kaspersky. (s.f.). *A Brief History of Computer Viruses & What the Future Holds*. Obtenido de https://www.kaspersky.com/: https://www.kaspersky.com/resource-center/threats/a-brief-history-of-computer-viruses-and-what-the-future-holds

Keith Stouffer (NIST), S. L. (May de 2015). *Guide to Industrial Control Systems (ICS) Security*. Obtenido de CSRC NIST: https://csrc.nist.gov/publications/detail/sp/800-82/rev-2/final

World Economic Forum. (2021). *The Global Risks Report 2021.* Davos: World Economic Forum. Obtenido de https://www3.weforum.org/docs/WEF_The_Global_Risks_Report_2021.pdf