Telefónica Tech

NOZOMI NETWORKS

Ciberseguridad en entornos OT

Caso de estudio en el sector Oil & Gas

El número de ataques en el sector OT cada vez es mayor y por tanto hacen falta soluciones de seguridad para protegerlo adecuadamente. En este informe se cuenta la experiencia de un caso de éxito real del sector Oil & Gas en el que Telefónica ha trabajado.

1

Introducción

2

Introducción al caso de estudio

3

Fases de la implantación de una solución de monitorización

- Fase 1: Gestión del proyecto
- Fase 2: Consultoría
- Fase 3: Análisis de la arquitectura
- Fase 4: Implantación - despliegue de las sondas y entrenamiento
- Fase 5: Definición e implementación de los casos de uso

4

Conclusiones

Telefónica Tech

Resumen ejecutivo

La convergencia entre los mundos IT y OT es cada vez mayor, lo cual trae muchas posibilidades pero también aumenta la superficie de ataque, por lo que es necesario adoptar las medidas de seguridad adecuadas. En este informe se cuenta la experiencia de un caso de éxito real encuadrado en el sector Oil & Gas.

El proyecto consiste en una fase de consultoría acompañada de la implantación y operación de una solución de monitorización de seguridad. Como tecnología de monitorización se ha empleado la tecnología de Nozomi Networks. En el documento se describen con detalle las fases del proyecto y cómo se ha llevado a cabo cada una de ellas.

Como resultado de la implantación de esta solución se ha conseguido la detección de varias situaciones que suponían un riesgo para la seguridad de los emplazamientos industriales del cliente, las cuales se han mitigado y se ha reducido el riesgo al que estaba expuesto el cliente desde la perspectiva de la ciberseguridad.

1 Introducción

La industria está experimentando un incremento de conectividad de sus sistemas de control industrial además de la integración de tecnologías digitales. Las tecnologías digitales traen consigo un mundo de posibilidades que aporta muchas ventajas a las empresas para aumentar su flexibilidad, mejorar los servicios que prestan y ser más eficientes. Esta necesidad de mayor conectividad se produce tanto con el exterior, es decir, con sus clientes y proveedores, como internamente, consiguiendo una mayor coordinación e integración entre las diferentes organizaciones y departamentos.

Son muchos los sectores que están acometiendo esta transformación digital, entre los cuáles se encuentra el sector de Oil & Gas. Según un estudio de Frost & Sullivan titulado "Evaluación global del mercado de seguridad de infraestructura de petróleo y gas", se prevé que el mercado total de seguridad de infraestructura de petróleo y gas aumente de 18 mil millones de dólares al año en 2011 a 31 mil millones de dólares para 2021.

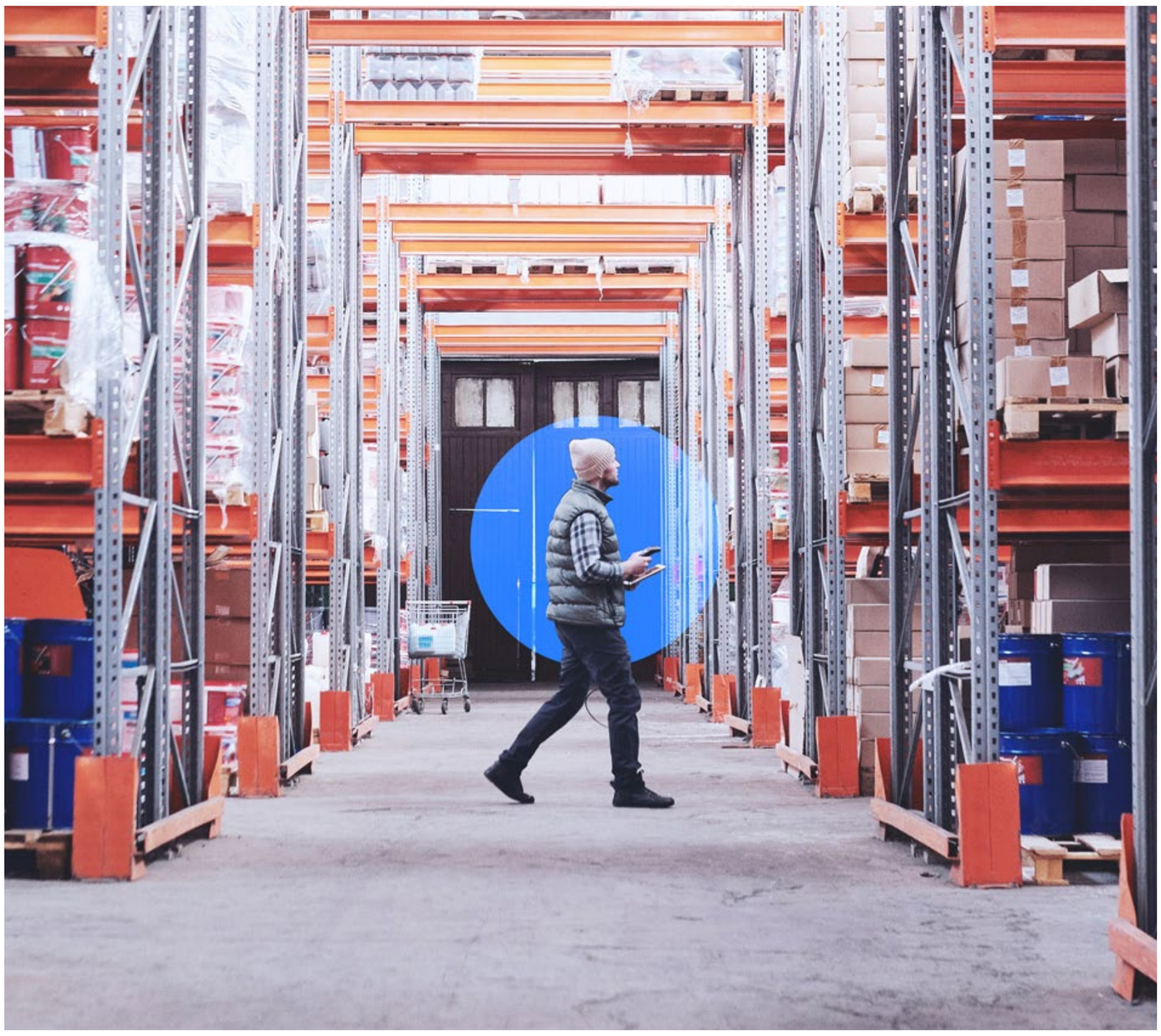
Es importante tener en cuenta que esta digitalización también trae consigo un incremento de la superficie de ataque.

Haciendo foco en el sector de Oil & Gas, se puede citar un estudio de Ponemon Institute de 2017, que afirma que casi el 70% de las empresas de este sector sufrieron un compromiso de seguridad que tuvo como consecuencia la pérdida de información confidencial o interrupciones operativas en sus entornos ICS/SCADA en un periodo de 12 meses.

La tendencia en el número de ataques en la industria va a más. Según Kaspersky, de la última mitad del año 2019 a la primera mitad del año 2020, la cantidad de equipos ICS (*Industial Control Systems*) en los que se bloquearon acciones maliciosas incrementó en 1.5% en el sector de Oil & Gas, situándose en 37.8% a mitad de 2020. Esta tendencia se ve agravada por la situación de pandemia mundial en la que nos encontramos. Los cambios en las prácticas laborales provocados por COVID-19 han dejado los sistemas más expuestos a los ataques. Además, el hecho de tener menos personal físicamente en las fábricas está impactando en la capacidad para responder y mitigar ataques.

Por todo lo mencionado, resulta evidente que es imprescindible contar con las medidas de seguridad adecuadas que permitan proteger el negocio al mismo tiempo que la reputación de la empresa. Cuando además se trata de sistemas críticos, la importancia de protegerlos correctamente toma una importancia capital.

Adicionalmente, se debe tener en cuenta que el sector de Oil & Gas tiene algunas características que pueden introducir desafíos mayores que en otras industrias. La infraestructura de petróleo y gas está geográficamente dispersa e incluye estaciones remotas y tecnología operativa heredada con diferentes capacidades que se está integrando en la infraestructura de TI, lo cual incrementa y hace más dispersa la superficie de ataque.



Otro de los grandes retos es la protección del extremo a extremo, donde hay que tener en cuenta que en la cadena de suministro intervienen un gran número de actores que participan en diferentes aspectos del negocio. Este entorno incluye compañías petroleras independientes, compañías petroleras estatales, compañías más pequeñas que se enfocan solo en ciertos aspectos así como múltiples proveedores de servicios y otros terceros. Este entorno debe protegerse adecuadamente puesto que cualquier descuido en la cadena puede suponer complicaciones desde el punto de vista de la seguridad.

Por ello, son varias las necesidades que surgen dentro de este ámbito:

- En primer lugar, hay que tener en cuenta que en muchos de los casos la industria ha evolucionado manteniendo sus sistemas y redes, los cuales pueden llegar a tener varias décadas de antigüedad. Esos sistemas conviven en mayor o menor medida con redes planas y ampliaciones *ad hoc* que se han ido añadiendo con los años. Todo esto resulta en un desconocimiento de qué hay realmente conectado a la red. Por ello, **tener visibilidad de qué activos hay conectados en la red** es fundamental, identificando el número de elementos conectados y su tipología. La visibilidad es el primer paso para la protección, ya que no se puede proteger lo que no se ve.

- Dado que en industrias tradicionales se puede encontrar *software* antiguo y desactualizado, además de descubrir los activos es necesario **identificar sus vulnerabilidades asociadas.**

- Como complemento a la necesidad de contar con un sistema que pueda **detectar este tipo de ataques, es necesario tener la certeza de que estos activos de comportan del modo adecuado** y hacen únicamente las acciones que se desea que hagan, evitando comportamientos fuera de lo esperado.

Dada la criticidad de los entornos mencionados, es necesario contar con soluciones específicas y adaptadas a estos entornos, que contengan la ciberinteligencia necesaria para detectar ataques especialmente diseñados para afectar a sistemas industriales y sean capaces de entender los protocolos industriales.

Para hacer frente a estos retos y proteger adecuadamente el negocio y la infraestructura de los clientes, Telefónica ofrece servicios específicos de seguridad OT. Entre ellos se encuentra el servicio de Monitorización de Seguridad OT.
En este documento se explica la experiencia de Telefónica en un caso de éxito real del sector de Oil & Gas donde se ha desplegado y operado este tipo de solución.

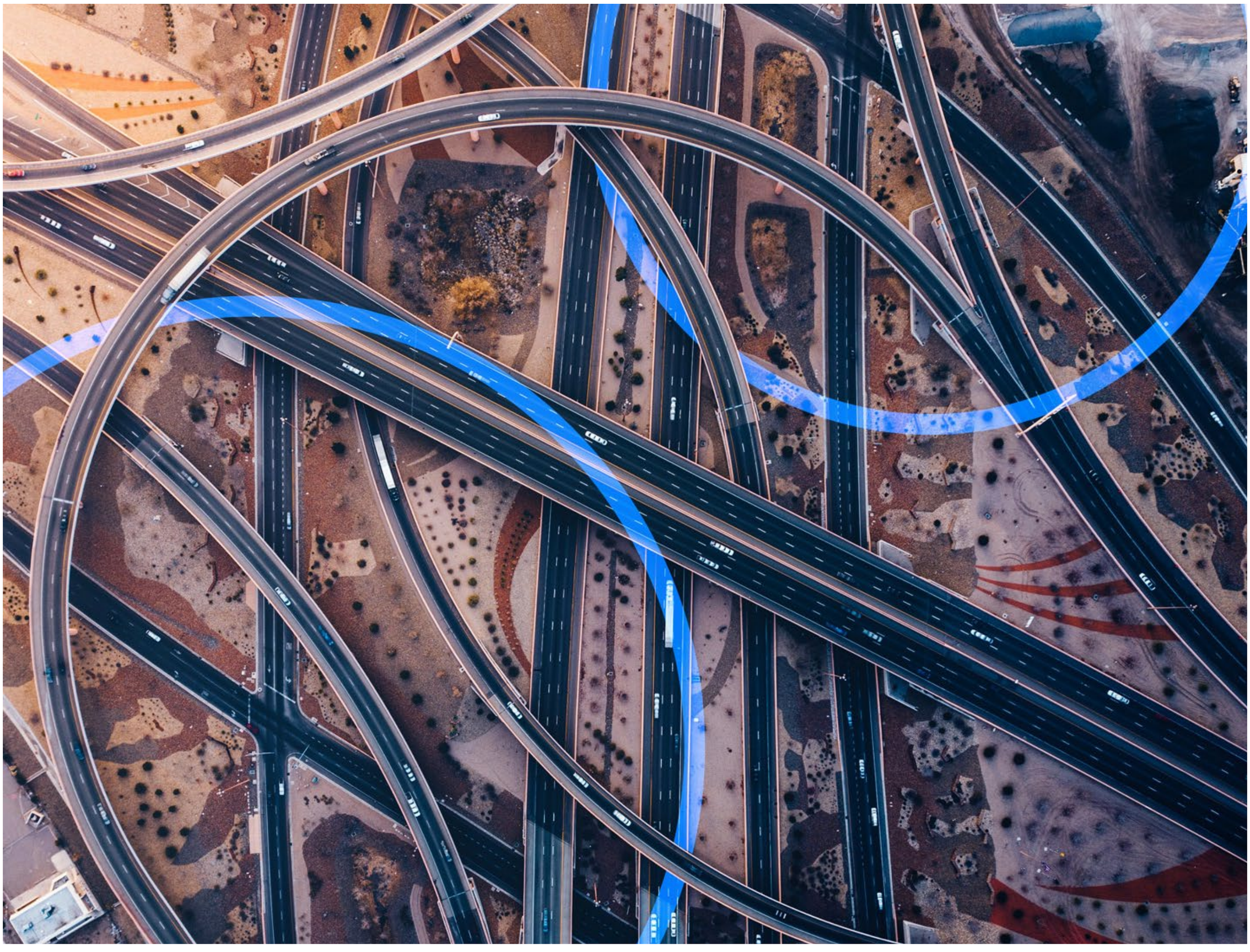
2 Introducción al caso de estudio

El caso de estudio se centra en la experiencia de Telefónica en un proyecto con un cliente del sector Oil & Gas. Se trata de una importante compañía en este sector y una de las más grandes en Latinoamérica. La empresa tiene actividad en las diferentes labores relacionadas con el sector Oil & Gas, incluyendo la exploración, transporte, producción, refinamiento y comercialización de los productos.

La compañía cuenta con aproximadamente 10.000 empleados y sus ingresos superan los 22 millones de dólares. En este proyecto se brinda protección a 10 emplazamientos industriales de la compañía, con funciones diferentes en el negocio de la compañía, desde la explotación de pozos hasta el refinamiento, pasando por el transporte del crudo.

Cabe mencionar que antes del inicio de este proyecto el cliente no tenía visibilidad alguna sobre lo que ocurría en su red OT. Además, no tenía un control real sobre la infraestructura. Gracias a este proyecto, en el que se ha implantado y operado una solución de monitorización de seguridad OT, esto fue solucionado y adicionalmente se detectaron y remediaron varias situaciones que estaban poniendo en peligro la seguridad del negocio del cliente.

A continuación, se explican las diferentes fases que se han seguido en el desarrollo del proyecto, que inicia con la planificación hasta su puesta en producción.

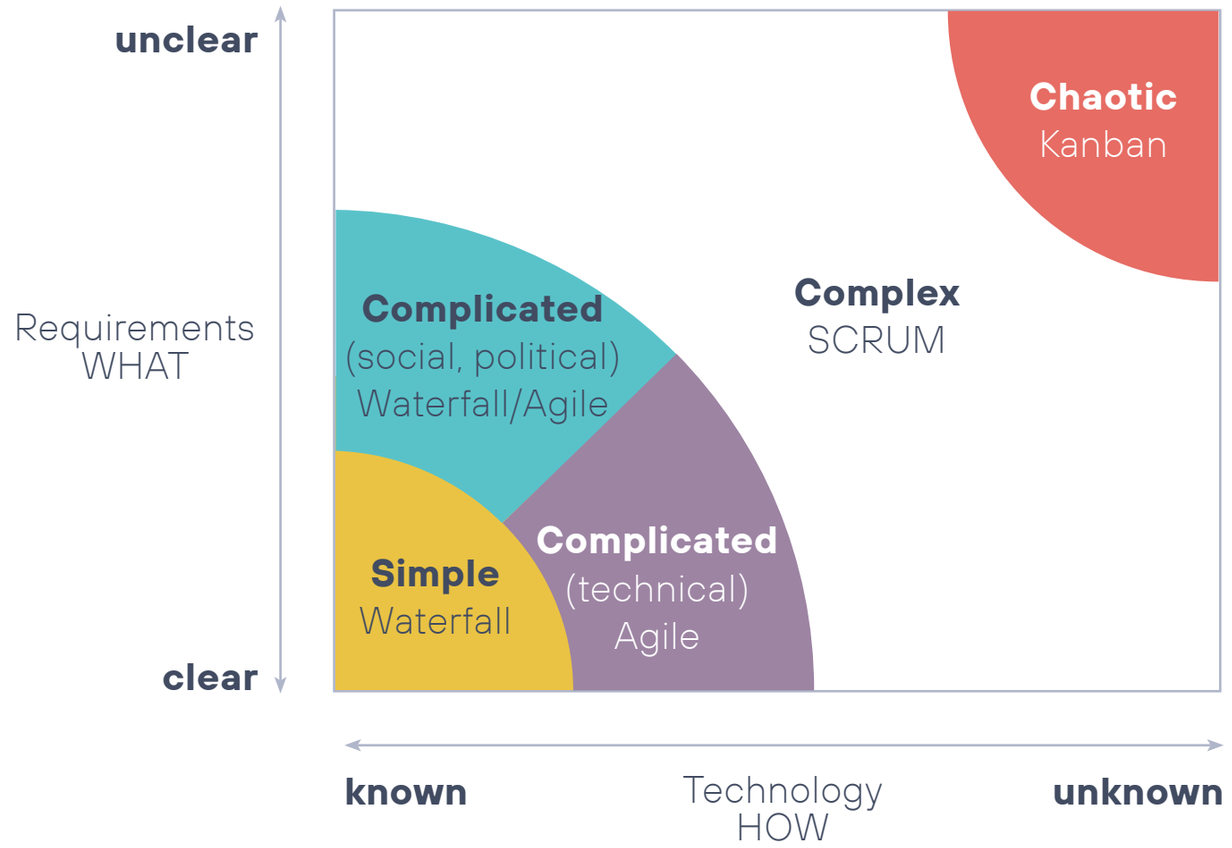


3 Fases de la implantación de una solución de monitorización

3.1. Fase 1: gestión de proyecto

Una buena gestión de proyectos es clave para acometerlos con éxito, coordinar a los diferentes equipos, cumplir plazos y asegurar la satisfacción del cliente.

Telefónica estudió cuál era el enfoque más adecuado para gestión de este proyecto, teniendo en cuenta su envergadura y las necesidades del cliente. Debido a la naturaleza del proyecto, las necesidades del cliente y la situación de pandemia global, se decidió usar una metodología *agile*.



Este enfoque ágil se basó en los principios del manifiesto ágil, esto es:

- **División del proyecto en pequeños entregables y entrega de valor temprana.** El proyecto se divide en las siguientes fases:
  - Consultoría.
  - Análisis de la arquitectura, donde se identifican los puntos de despliegue de las sondas, se analizan las alternativas para la captura de tráfico y se define la arquitectura general de la solución.
  - Implementación, contemplando el despliegue de sondas y fase de entrenamiento.
  - Operación, donde se definen e implementan los casos de uso.
- **Formar un equipo de trabajo en el que se incluye al director de cada emplazamiento industrial como parte del proyecto.** Una Matriz RACI fue de gran ayuda a tal efecto.
- **Comunicación continua con el cliente.** Se realizaron reuniones semanales con el cliente en las que se reportaba los avances de cada uno de los emplazamientos objeto.
- **Respuesta ante el cambio eficiente.** Cambios reales y cambios inmediatos adaptados gracias a la implicación del equipo de implementación.

Gracias a este enfoque metodológico basado en entregar valor al cliente, el proyecto se desarrolló exitosamente. A continuación se explican con más detalle cada una de las fases mencionadas para acometer el proyecto y cómo Telefónica desarrolló el trabajo y resolvió los retos que aparecían en cada una de ellas.

3.2. Fase 2: Consultoría

Uno de los puntos clave para comenzar los proyectos es la realización de una consultoría de seguridad, la cual permite entender el entorno del cliente y la arquitectura de red para analizar el estado en el que se encuentran y si cumplen con las recomendaciones de seguridad. Como resultado de la auditoría se entrega al cliente un informe que indica los hallazgos encontrados así como recomendaciones de seguridad que el cliente debe acometer para proteger adecuadamente su infraestructura y su negocio.

El primer paso a la hora de realizar cualquier consultoría de ciberseguridad es definir su alcance, es decir, las redes y sistemas que serán objeto de estudio, tanto a nivel técnico como a nivel de tareas de gestión y administración (políticas y procedimientos). El estándar IEC 62443, ampliamente utilizado como referencia a la hora de implementar ciberseguridad en entornos industriales, se refiere a este alcance como SuC (*System under Consideration*). En infraestructuras complejas propias del sector de Oil & Gas, como una Refinería, una opción interesante para delimitar el SuC es acotarlo en base a análisis HAZOP (*Hazard and Operability Study*). Esta técnica de Análisis de Riesgo de Proceso (PHA) se basa en la premisa de que los riesgos, los accidentes o los problemas de operabilidad, se producen como consecuencia de una desviación de las variables de proceso con respecto a los parámetros normales de operación. Delimitar el SuC en base al HAZOP permite alimentar el análisis de riesgos de ciberseguridad con todos los peligros identificados en el proceso de ingeniería del HAZOP.

El servicio de consultoría OT se puede dar en tres niveles dependiendo de las necesidades del cliente:

EVALUACIÓN BÁSICA:
Obtener una **visión genera**l de la postura de ciberseguridad de la planta industrial objetivo.

Consistente en la realización de un análisis de la madurez en ciberseguridad OT de la planta objetivo o SuC.

EVALUACIÓN INTERMEDIA:
Obtener una **visión detallada** de la postura de ciberseguridad de la planta industrial objetivo.

Incluye la realización de un análisis de la madurez, una evaluación de riesgos de alto nivel y la revisión de la documentación de ciberseguridad de alto nivel vigente en la planta objetivo. Para ello se celebran entrevistas con los responsables de las áreas relevantes para la ciberseguridad, complementadas con inspecciones en terreo o *walkdowns* pasivos para verificar la presencia 'física' de medidas y equipos.

EVALUACIÓN AVANZADA:
Obtener una **visión integral** de la postura de ciberseguridad de la planta industrial objetivo.

En este nivel se revisan inicialmente las políticas y procedimientos de seguridad vigentes. Con esta base de conocimiento, el equipo de trabajo procede a evaluar el nivel de madurez de la planta y un análisis de riesgos de alto nivel, ambas en base a entrevistas y sesiones de trabajo con el personal de la planta. Para verificar la información recopilada en las entrevistas, se realizan *walkdowns* activos, que verifican la presencia 'física' y chequean la configuración de los equipos más relevantes de comunicaciones, seguridad y sistemas de control (servidores y/o estaciones). Por último y como complemento a todo lo anterior, se realizan capturas de tráfico de red para, posteriormente, analizarlas en entorno de laboratorio con diversas herramientas, que incluyen Sistemas de detección de anomalías de red (*Network-Based Anomaly Detection* - NBAD) y cortafuegos de nueva generación (*Next-Generation Firewalls*).

Más adelante, se detallan las actividades incluidas en los distintos niveles de evaluación anteriores.

Para cualquiera de los niveles, el desarrollo de este servicio se divide en cuatro etapas:

Preparación

Telefónica requiere al cliente acceso a información relevante para el desarrollo del trabajo, como el organigrama y roles relacionados con la seguridad, políticas y procedimientos de seguridad, información de la red, tecnologías de sistemas de control (DCS, PLCs, RTUs, protolos industriales...), configuración de equipos, etc. La cantidad y detalle de la información requerida depende del nivel de la evaluación que se vaya a realizar. El equipo de consultores, en contacto permanente con el personal de la planta, analiza esa información y prepara el trabajo a realizar en la siguiente etapa.

Durante la preparación se determinan, además, los interlocutores y se fijan las entrevistas a celebrar durante la etapa de levantamiento.

Levantamiento

Esta etapa tiene lugar en las instalaciones del cliente, es decir, en campo, para servicios de niveles intermedio y avanzado, y en remoto para evaluaciones iniciales. Durante ella se realiza el grueso de las actividades de la evaluación.

Análisis

La información recogida en las etapas anteriores se analiza, ordena y agrega en un informe de resultados, que incluye aspectos tales como el nivel de madurez de ciberseguridad, inventario de activos, listado de hallazgos, plan de acción para cubrir las deficiencias encontradas, propuesta de mejoras, etc. Asimismo, se elabora un informe ejecutivo con los aspectos más relevantes de los entregables.

Resultados

Para finalizar el servicio de consultoría, el equipo se desplaza a planta de nuevo a hacer entrega de los informes y, en caso de requerirse, realizar una presentación ejecutiva de resultados.

A continuación, se incluye la descripción de las diferentes actividades:

- **Revisión de documentación** para a conocer el estado de seguridad de la planta objetivo, lo que incluye revisión de políticas, procedimientos, ficheros de configuración, mapas de red, etc.

- **Entrevistas con el personal de planta** para conocer de primera mano toda la información relevante en lo que respecta a la ciberseguridad, incluyendo no solo medidas de protección tecnológicas instaladas en la planta objetivo, sino de los procesos y la operativa que afecta a los sistemas de control.

- **Evaluación de la madurez en ciberseguridad OT**, aplicando nuestro propio modelo de madurez en ciberseguridad industrial y una herramienta para evaluarla, basados en tres referencias ampliamente conocidas en el campo de la ciberseguridad y la ciberseguridad industrial: *NIST Cyber Security Framework* (NIST CSF), ISA/IEC 62443 y NIST 800-82r2. Además de entrevistas con el personal de planta, se utiliza una herramienta evalúa las medidas de protección, tanto administrativas como técnicas, de todas las áreas de la seguridad que establece el NIST CSF:
  - Estrategia riesgos y organización.
  - Capacidades de protección.
  - Capacidades de detección.
  - Capacidades de respuesta.
  - Capacidades de recuperación.

- **Análisis de riesgos de alto nivel,** lo que permite identificar áreas de la red y activos que requieren un mayor nivel de protección y ponderar las medidas de seguridad asociadas.

- **Revisión en terreno de equipos en planta (*walkdowns*)**, que consiste en ver físicamente dispositivos o aplicaciones que contribuyen a la seguridad (*switches, firewalls*, administradores de dominio, etc.) o pertenecen a los sistemas de control (servidores, estaciones de ingeniería, estaciones de operación, etc.). Durante estas revisiones o *walkdowns* se podrá, por tanto, chequear la presencia de controles y/o tomar evidencias de hallazgos que serán integrados en el informe de resultados.
  Los *walkdowns* podrán ser pasivos, simplemente constatando la existencia de controles, o activos, que además incluyen la revisión de la configuración de esos controles u otros equipos como estaciones, servidores, equipos de comunicación, etc.

- **Análisis de tráfico de red.** Este análisis se realiza en un entorno seguro de laboratorio. Después de tomar capturas del tráfico de red de la planta, éstas se analizan con diversas herramientas de detección anomalías de red (en inglés, *Network Behaviour Anomaly Detection*, NBAD), concebidas para entornos industriales, y otros aplicativos, como *firewalls* de nueva generación (NGFW). La finalidad principal de las herramientas NBAD es el monitoreo de la seguridad de red, alertando en caso de que haya un ataque, una infección, o una desviación del tráfico de red 'normal'. Una de estas tecnologías es la de Nozomi, la cual se explicará con más detalle más adelante.
  Sin embargo, para el servicio de consultoría, los sistemas NBAD aportan información valiosa y como complementaria a la información obtenida en el resto de actividades, como el inventario detallado de dispositivos, vulnerabilidades que afectan a equipos y protocolos, enlaces de red problemáticos o malas configuraciones, y lo hace sin interferir en la operativa del proceso industrial al trabajar con una copia del tráfico de red. Este es un factor esencial en el análisis de ciberseguridad de entornos industriales, cuyos activos, especialmente PLCs y controladores, son especialmente inestables ante levantamientos de ciberseguridad activos.

En la siguiente figura se muestra la relación de las actividades con las etapas de la consultoría:

3.3. Fase 3: Análisis de la arquitectura

3.3.1. Identificación de puntos donde desplegar las sondas

Cuando se va a implantar una solución de monitorización de seguridad que analiza el tráfico de red es vital tener conocimiento sobre la arquitectura de red. En el apartado de consultoría se analiza la red para ver el estado y su nivel de seguridad. Como resultado de esta consultoría se puede ver como recomendación de seguridad la implantación de una solución de monitorización de seguridad de la red. En ese caso, es necesario analizar la arquitectura de red con el objetivo de identificar cuáles son los puntos más adecuados para situar las sondas. La ubicación de las sondas determina la visibilidad de la red que se puede alcanzar, por tanto es clave el localizar adecuadamente los puntos de agregación del tráfico y la identificación de los puntos clave en los que situar las sondas.

La información obtenida en la fase de consultoría puede ser útil para arrancar con este estudio.

En cuanto a la dificultad para identificar estos puntos de despliegue, nuestra experiencia en este proyecto nos hace concluir que hay varios factores que influyen en esta decisión. En primer lugar, el tamaño de la fábrica de la que se trate es determinante, pero también el nivel de conocimiento de esa red por parte del cliente. En nuestro caso nos hemos encontrado con casos de redes con gran tamaño y complejas en las que el cliente tenía muy claro dónde quería situar las sondas, por lo que en esos casos la identificación del punto de despliegue de la sonda fue muy sencillo. También se pueden dar casos en los que solo haya un punto de agregación de tráfico, por lo que en ese caso la decisión también es rápida. Sin embargo, en lugares donde no haya mucho conocimiento de la red puede ser necesaria una etapa de estudio de la misma para determinar el punto óptimo de despliegue.
En esta decisión también influye el entender con precisión el core del negocio del cliente y qué tipo de red toma más importancia para él proteger, por ejemplo, en un determinado lugar puede tratarse de la red de pozos, en otro caso la red de gas, etc. Como puede observarse, en este proceso es fundamental contar con la colaboración del cliente para entender y cubrir de forma óptima sus necesidades. Otros aspectos que pueden influir en estas decisiones son factores de madurez tecnológica, por ejemplo las capacidades de algunos elementos de la red del cliente para obtener la copia del tráfico.

Este punto se trata con más detalle en el siguiente apartado.

3.3.2. Análisis de alternativas para la captura del tráfico

En el ámbito industrial y también en el sector de Oil & Gas es importante contar con soluciones pasivas que no interfieran ni inyecten tráfico en la red. Como se ha comentado, la disponibilidad es un factor que se debe proporcionar en todo momento cuando se trabaja en ámbitos industriales. Para garantizar esto, las soluciones de monitorización trabajan analizando una copia del tráfico, no el tráfico en sí mismo, lo que garantiza que se afecta a dicho tráfico, no se introducen retardos e incluso en el caso de que llegase a caerse la solución de seguridad, no afectaría en ningún momento al tráfico original.

Para crear estas copias de tráfico hay varias alternativas tecnológicas disponibles. La más sencilla y económica es utilizar un puerto de spam de un *switch*. El inconveniente que puede encontrar esta solución es que, si el *switch* está sobrecargado, se puede eliminar algún paquete de tráfico, y por tanto éste no sería analizado por la solución de monitorización. Por eso en algunos casos se considera más conveniente instalar elementos de red llamados *Terminal Access Point* en inglés (TAP), que permiten hacer una copia del tráfico sin pérdida de paquetes. Hay varios modelos en los que incluso si este elemento perdiera alimentación, no afectaría al tráfico que circula por la red. Aunque es una solución que incrementa los costes, en muchos casos puede compensar, y el tiempo de corte para la instalación es mínimo. Otra situación en la que puede ser recomendable instalar un TAP es en aquellos casos en los que la tecnología en el emplazamiento es antigua o se cuenta con *switch* puramente industriales sin la capacidad de *port mirroring*.

Esta es otra de las discusiones importantes a tener con los clientes, para analizar cuál es la solución que mejor se adecúa a su caso particular.

3.3.3. Arquitectura general de la solución

Una vez que los puntos anteriores están claros, se está en disposición de diseñar la arquitectura general de la solución. En este caso se ha utilizado la solución de monitorización de seguridad de Nozomi, especializada en el ámbito industrial.

Esta solución cuenta con varias funcionalidades:

- Identificación y perfilado de cada uno de los activos conectados a la red del cliente, incluyendo la especificación de sus sistemas operativos genéricos o propietarios, firmware, programas y aplicaciones.
- Identificación y gestión de vulnerabilidades detectadas en los activos de la red del cliente.
- Detección de anomalías y amenazas en la red de control gracias al análisis de tráfico con la inspección profunda de paquetes que proporciona la solución propuesta.
- Notificación de alertas y alarmas clasificadas por nivel de criticidad.
- Generación de informes.
- Integración con elementos de red para la mitigación y remediación de los incidentes de seguridad que se produzcan.

Estas funcionalidades se pueden resumir en tres etapas fundamentales: visibilidad, detección de amenazas y mitigación, tal y como se explica en la siguiente figura:

Visibilidad	**Detección de amenazas**	**Mitigación**
Visibilidad y perfilado de los dispositivos (extrayendo los patrones normales de su comportamiento).	Detección de anomalías y ataques por medio de técnicas de *Machine Learning* y *feeds* de ciberinteligencia específicos de IoT/OT.	Fácil integración con los principales *firewalls* y SIEMs

La solución está compuesta por varios elementos:

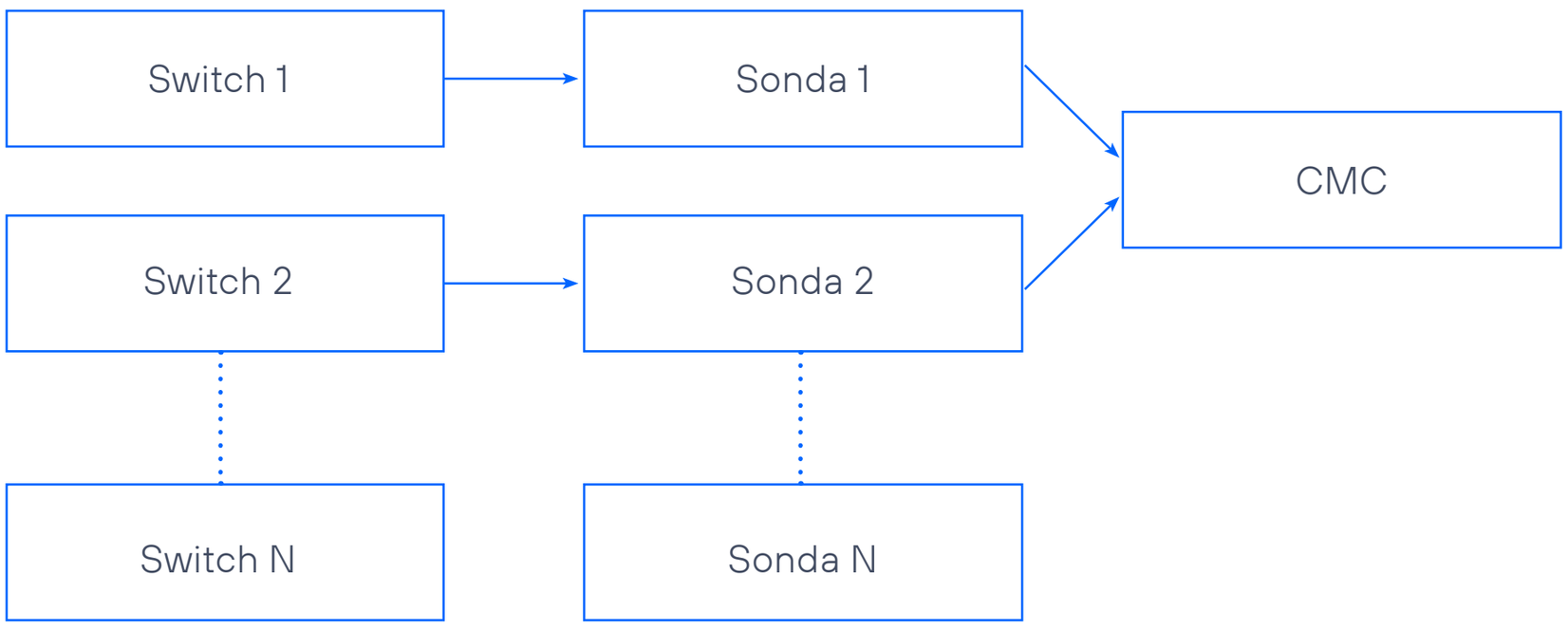
- **Sondas**. Se sitúan en la infraestructura de red del cliente, en los puntos de despliegue localizados anteriormente. Son pasivas y realizan el descubrimiento de los dispositivos así como el alertamiento relacionado con cualquier incidente o anomalía de seguridad. En este proyecto se ha optado por sondas físicas, aunque también podrían ser virtualizadas. En función del número de nodos a proteger, volumen de tráfico a monitorizar, número de puertos necesarios, si es necesario que esté rugerizado y algunos otros parámetros, es más conveniente aplicar un modelo de sonda u otro.

Ha de mencionarse que las sondas cuentan con una combinación de técnicas de *Machine Learning* y Ciberseguridad para la detección de las amenazas. Las técnicas de *Machine Learning* permiten hacer un perfilado del comportamiento de los activos y detectar cualquier anomalía que se desvié del comportamiento normal. A su vez, las firmas permiten detectar e identificar ataques que afecten a los activos del cliente, teniendo en cuenta que se utilizan fuentes específicas que permiten detectar ataques dirigidos al sector OT.
En el caso de este proyecto se ha ubicado una sonda en cada emplazamiento industrial y se ha trabajado con varios modelos de sonda para adaptarse a las necesidades de cada ubicación.

- **Consola de gestión central (*Central Console Management* en inglés, CMC)**. Habitualmente se utiliza en caso de que un emplazamiento tenga más de una sonda. A su vez, si hubiera varias CMCs, podría haber una CMC a un nivel superior para aglutinar la información de todas ellas y tener un punto de control central a un nivel superior.

En el caso de este proyecto se cuenta con una CMC que tiene visibilidad de todas las sondas y que está conectada con el SIEM.
La CMC se puede desplegar en un entorno virtualizado, existiendo también las opciones de despliegue físico y *Vantage*.

La arquitectura del proyecto tiene un aspecto como este:



3.4. Fase 4: Implantación – despliegue de las sondas y entrenamiento

En este punto ya se está en disposición de llevar a cabo la implantación, la cual incluye la configuración e instalación de las sondas. Así mismo, dado que las sondas utilizan técnicas de *Machine Learning* e Inteligencia Artificial para el perfilado de los dispositivos y detección de anomalías sobre los mismos, es necesario que las sondas tengan un periodo inicial de aprendizaje antes de pasar al estado de protección.

Una vez se ha determinado la ubicación de las sondas, se procede con un plan de despliegue.

El proyecto se ha llevado a cabo durante la pandemia por COVID 19, lo cual ha dificultado los traslados en algunos de los casos. Los despliegues estaban planificados inicialmente para realizarse de forma presencial con desplazamiento de los equipos, pero dadas las circunstancias hubo que adecuar el plan. Telefónica respondió rápidamente a ante esta situación y se adaptó buscando soluciones y personas que estuvieran in situ y que pudieran realizar ellos mismos las instalaciones físicas, guiadas remotamente por el equipo de expertos. Para ello, se realizó una configuración para que los equipos de Telefónica pudieran acceder remotamente a las sondas, además de asegurarse de que todo lo necesario para la instalación estaba listo: suministro eléctrico, cableado, racks, etc. Una vez está todo preparado, se envía la sonda adecuadamente configurada para que sea instalada físicamente en el emplazamiento industrial correspondiente. Tras ello, la sonda se pone en marcha, se hacen los ajustes necesarios y se deja lista y funcionando. Se comprueba que la sonda tenga comunicación con la CMC y que desde ella se pueda ver la información detectada por la sonda.

Es de destacar que Telefónica trabaja con una metodología de análisis de riesgos en relación con el despliegue de las sondas. Aunque en general este tipo de despliegues no suele dar problemas, Telefónica tiene contempladas cuáles son las situaciones de riesgo que se podrían dar, incluyendo situaciones de riesgo laboral u otras como por ejemplo, asignación de una IP duplicada, indicando además cuáles son las medidas a tomar para solucionarlo en caso de que se produjeran. De esta forma, se asegura que la instalación se realiza correctamente, adelantándose a los problemas para que no se produzcan y reduciendo al mínimo los riesgos para el cliente.

Inicialmente las sondas comienzan en modo aprendizaje y se mantienen en este modo el tiempo necesario para que aprendan el comportamiento normal de la red (un mes aproximadamente) y más tarde puedan realizar la detección en el modo de protección.

El hecho de que la sonda esté en modo aprendizaje no quiere decir que la sonda no pueda empezar a lanzar alertas de eventos de seguridad detectados, puesto que algunas alertas no dependen de los algoritmos de *Machine Learning*, y por tanto el cliente también puede recibir alertamiento durante ese periodo.

3.5. Fase 5: Definición e implementación de casos de uso

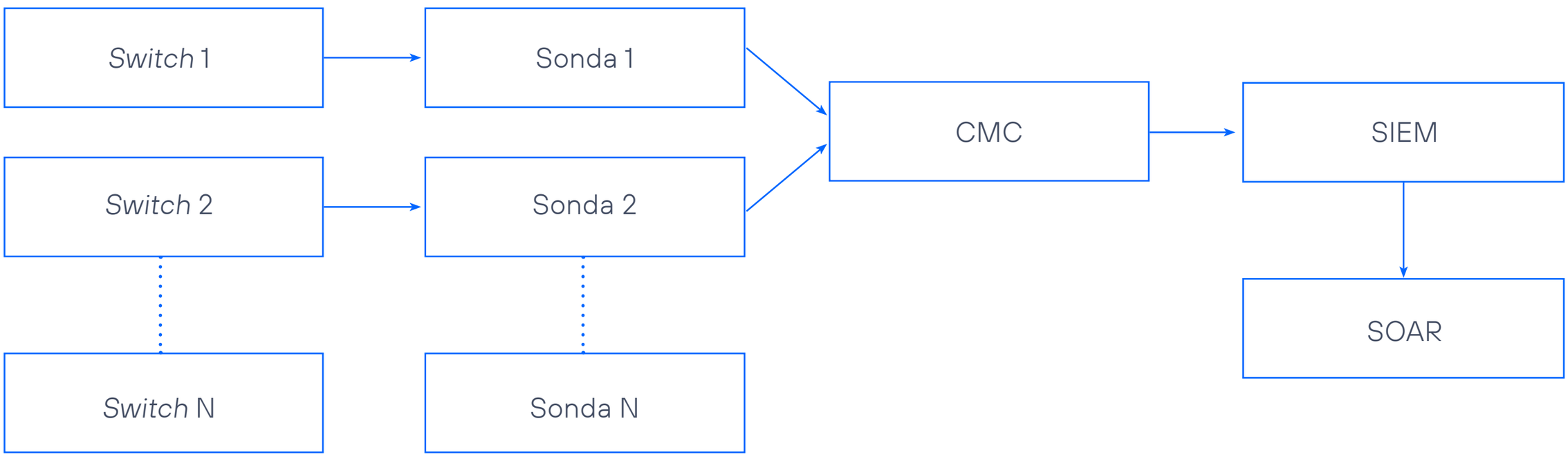
Una vez se recibe el alertamiento de la sonda es fundamental el gestionar esas alertas de la forma adecuada. Para los clientes es fundamental no solamente conocer las alertas sino saber qué hacer con ellas. Aquí Telefónica aporta un gran valor al cliente mediante su servicio de gestión de alertas de seguridad que se lleva a cabo desde el SOC de Telefónica distribuido en 11 localizaciones a lo largo del planeta.

Las fases siguientes a la configuración y aprendizaje de las sondas se pueden estructurar de la siguiente manera:

- **Fase de Socialización y mitigación en preproductivo**. Incluye las tareas de reconocimiento de la sonda, notificación de alertas al responsable del emplazamiento y mitigación.
- **Fase de integración sondas y puesta en productivo de alertamiento.** En esta fase se realiza la integración con el SIEM, generación de casos de uso, definición de grupos resolutores y generación de alarmas a los grupos resolutores identificados.

A continuación se dan más detalles de la experiencia en el desarrollo de estas fases del proyecto.

Una vez se reciben las alertas en el SIEM se procede a crear los casos de uso. Nozomi tiene reflejadas unos 95 tipos de alertas categorizadas en 5 grupos diferentes. En el caso de este caso de estudio, la CMC está vinculada a un *Security Information and Event Management* (SIEM) el cual recibe y correla las alertas. A su vez, el SIEM está conectado a un *Security Orchestration, Automation and Response* (SOAR) el cual permite orquestar y automatizar ciertas tareas mediante el desarrollo de *playbooks*.



tiene una gran experiencia en la gestión de este tipo de servicios IT, lo cual se aprovecha también para la gestión de entornos OT, con las adaptaciones pertinentes.

Las etapas del modelo operativo del SOC se resumen en la siguiente figura:

En este sentido, Telefónica está trabajando muy de cerca con el cliente para reducir el volumen de alertas y asignarlas a los diferentes grupos resolutores en función de la naturaleza de la alerta. Para ello se han llevado a cabo varias reuniones en una etapa preoperativa en las que se trabaja con el cliente y se decide cómo se desea tratar cada tipo de alerta. Inicialmente se comienza analizando las alertas más críticas, puesto que son las que pueden tener un mayor impacto en la seguridad y negocio del cliente y son las que necesitan una respuesta más rápida. En particular, para la selección de los casos de uso se han utilizado varios criterios, por un lado la volumetría de alertas de cada tipo y por otro el riesgo asociado a cada alerta, de modo que se han priorizado las alertas con mayor volumetría y riesgo alto.

En estas reuniones se fija un plan de acción para la remediación de las alertas así como un seguimiento al mismo para asegurarse de que todo marcha correctamente. Esta parte es de gran valor para el cliente, ya que para tener un servicio de seguridad óptimo no solo es importante contar con una buena tecnología sino también contar con el equipo humano especializado en gestionarlo y optimizarlo para las necesidades del cliente. Inicialmente, cuando las sondas están en periodo de aprendizaje y no han sido ajustadas adecuadamente, el volumen de alertamiento puede ser mayor. Por eso se realiza este proceso de optimización del alertado para reducir el volumen de alertas, puesto que un número elevado de alertas dificulta no solo su gestión sino también la capacidad de reacción antes las mismas.

Una vez perfiladas las alertas y definidos los casos de uso junto con los grupos resolutores y las matrices de escalamiento, esta información entra en el flujo de la operación de los SOCs de Telefónica. En esta etapa se lleva a cabo el desarrollo de *playbooks* para la automatización de tareas y asignación a los grupos resolutores correspondientes, que pueden estar más centrados en el ámbito IT u OT en función de la naturaleza de la alerta. El SOC de Telefónica cuenta con un nivel 1 que opera 24*7 resolviendo los incidentes y descartando falsos positivos. En caso necesario, la incidencia puede escalar a un nivel 2 para un análisis y una investigación más detallados. Cabe mencionar que además se ha realizado una integración con la herramienta de *ticketing* del cliente.

El SOC de Telefónica que cuenta con expertos y una gran experiencia en la gestión de este tipo de servicios, contando con un equipo multidisciplinar y un soporte 24*7. Telefónica cuenta con expertos certificados en la tecnología de Nozomi tanto a nivel global como local, para desarrollar los proyectos con las máximas garantías.

Como resultado de la implantación de la solución se han detectado varios incidentes de seguridad que estaban afectando a los activos del cliente. Por ejemplo, se detectó una vulnerabilidad grave presente en algunos de sus equipos y también se detectaron conexiones a IP con dudosa reputación. Estos incidentes se han comentado con el cliente y se han acordado las medidas de seguridad adecuadas para mitigar el riesgo y prever daños mayores.

Por tanto, el tener esta visibilidad y gestión de las alertas ha resultado de gran utilidad para el cliente y ha resultado en un mayor nivel de seguridad para su empresa.

4 Conclusiones

Las empresas en el sector OT están expuestas a una gran cantidad de amenazas. Por ello, la visibilidad y mitigación de estas amenazas por medio de la detección de amenazas se vuelve fundamental para contar con un entorno adecuadamente securizado.

En este documento se ha explicado un caso de éxito de un proyecto real en el que ha participado Telefónica implantando y operando un servicio de monitorización de seguridad mediante el análisis de tráfico de red, utilizando tecnologías especializadas en analizar los protocolos del ámbito industrial, así como la detección de las amenazas dirigidas a este ámbito.

En el caso concreto de este proyecto, la implantación de la solución ha permitido la detección de varias situaciones que suponían un riesgo para la seguridad de los emplazamientos industriales del cliente, identificando equipos con vulnerabilidades o conexiones a sitios maliciosos. Gracias a la adopción del servicio de monitorización de seguridad OT se han reportado estas amenazas al cliente y se han tomado las medidas de remediación adecuadas, solucionando los problemas de seguridad y creando un entorno mucho más seguro para los centros de operación del cliente.

Sobre Telefónica Tech

Telefónica Tech es un *holding* de empresas propiedad del grupo Telefónica. La compañía cuenta con una amplia oferta de soluciones tecnológicas llegando a más de 5,5 millones de clientes en 175 países.
Telefonica TECH podrá albergar otros negocios digitales a futuro, incluso del segmento B2C.

Telefónica Tech