The number of attacks on operational technology (OT) is increasing rapidly, and effective security solutions are needed to properly protect it. This report outlines a real-world success story in the Oil & Gas sector – one of Telefónica’s and Nozomi Networks’ key areas of expertise.
Introduction

Case study introduction

Phases in the implementation of a monitoring solution

- Phase 1: Project management
- Phase 2: Consultancy
- Phase 3: Architectural analysis
- Phase 4: Implementation - deployment of sensors and training
- Phase 5: Definition and implementation of use cases

Conclusions
Executive Summary

The convergence between IT and OT worlds is increasing, which brings many opportunities but also increases the attack surface, making it necessary to take appropriate security measures.

The Oil & Gas sector has some characteristics that make it different from other industries. The challenges it faces are also different. One of the important aspects to consider is that the infrastructure is dispersed and includes remote stations and legacy technology with different capabilities that are being integrated into the IT infrastructure, which increases the attack surface. Moreover, it should be mentioned that the number of attacks is increasing and even targeted malware is being designed. Another challenge in this sector is that the number of actors in the supply chain is high, ranging from state-owned oil companies, to smaller companies that focus on certain aspects or multiple suppliers, so end-to-end protection is another challenge facing this industry.

It is therefore essential to have visibility of what assets are connected in the network, identifying the number of connected elements and their typology. In addition, the vulnerabilities associated with these assets must be monitored, as well as the expected behaviour of both the assets and the industrial process.

This report tells the experience of a real success story in the Oil & Gas sector. In this case, the client needed greater visibility of what was happening in its OT network, as well as greater control over the infrastructure.

In order to meet these needs, a monitoring solution has been implemented which has been specially designed for the protection of industrial environments and which is capable of analysing the protocols used in these environments. Firstly, the solution consists of a consultancy phase, which is completed with the findings of the monitoring solution based on Nozomi Networks technology. This phase includes everything related to the study of the network, choice of deployment points for the sensors, installation and configuration, training, etc. In order to complete the solution, the operation of the service is offered, supported by the experience of Telefónica’s SOC, which has certified experts distributed in 11 locations worldwide.

Thanks to this project and the analysis of the client’s network, a better understanding of the layout of the network has been gained, as well as visibility of the assets connected to the client’s network, understanding what type of assets is connected to each site and what their associated vulnerabilities are. In addition, security alerts managed by the SOC and reported to the client in the event of security incidents have been obtained and resolved together with the client to ensure greater security of the client’s network and business.
Industry is experiencing an increase in the connectivity of its industrial control systems (ICS) as well as the integration of digital technologies. The use of digital technologies enables a world of possibilities— including the ability for companies to increase their flexibility, improve the services they provide and become more efficient. This need for greater connectivity occurs both externally, i.e. with clients and suppliers, and internally, achieving greater coordination and integration between different organisations and departments.

Many industries are undergoing this digital transformation, including the Oil & Gas sector. According to a Frost & Sullivan study entitled “Global Assessment of the Oil & Gas Infrastructure Security Market,” the total Oil & Gas infrastructure security market is expected to grow from $18 billion per year in 2011 to $31 billion by 2021.

It is important to note that this digitalisation also brings with it an increase in the attack surface. In the Oil & Gas sector, a 2017 Ponemon Institute study found that in a 12-month period, almost 70% of companies suffered a security compromise that resulted in the loss of confidential information or operational disruptions in their ICS/SCADA environments.

The number of attacks in the industry is increasing. According to Kaspersky, the number of ICS devices on which malicious actions were blocked increased by 15% in the Oil & Gas sector from the last half of 2019 to the first half of 2020. In mid-2020, the total percentage of devices stood at 37.8%. This trend is worsened by the global pandemic we find ourselves in. Changes in work practices brought about by COVID-19 have left systems more vulnerable to attacks. In addition, having fewer staff physically located in factories is impacting the ability to respond to and mitigate attacks.

When it comes to the critical systems society relies on every day, protecting them is of vital importance. Having effective security measures in place is also essential to protect businesses and company reputations.
Additionally, it should be noted that the Oil & Gas sector has characteristics that may introduce greater challenges than in other industries. For example, Oil & Gas infrastructure is geographically dispersed and includes remote stations and legacy operational technology that are being integrated into the IT infrastructure. This increases and widens the attack surface.

Another major challenge involves the end-to-end protection of supply chains comprised of a large number of actors who participate in different aspects of the business. This includes both independent and state-owned oil companies, smaller companies that focus only on certain aspects, and multiple service suppliers and other third parties. This environment must be adequately protected – any oversight in the chain can lead to security complications.

Hence, there are several needs that arise within this field.

- **Visibility into the assets that are connected to the network.** In many cases, the industry has evolved by maintaining its systems and networks, which may be several decades old. These systems coexist to a greater or lesser extent with flat networks and ad hoc extensions that have been added over the years. This results in a lack of knowledge of what is actually connected to the network. Therefore, the ability to see all assets on a network and identify the number of connected elements and their typology is essential. Visibility is the first step to protection, as you cannot protect what you cannot see.

- **Identification of vulnerabilities.** Since old and outdated software is often found in traditional industries, it is not only necessary to discover the assets, but to be aware of associated vulnerabilities.

- **Detection and monitoring of all assets.** A system should not only detect the different types of attacks, but also ensure that these assets behave in appropriate ways – carrying out the actions you want them to fulfill and avoiding unexpected behaviours.

Given the criticality of the aforementioned environments, solutions adapted to the specific needs of their environments are necessary. They must contain cyber-intelligence capable of detecting attacks specially designed to affect industrial systems, as well as an understanding of industrial protocols.

To meet these challenges and adequately protect clients’ business and infrastructure, Telefónica offers specific OT security services. Among them is our OT Security Monitoring service. This document outlines Telefónica’s experience implementing this solution in a real-life success case in the Oil & Gas sector.
This case study focuses on Telefónica’s experience with one of the largest and most well-known Oil & Gas organizations in Latin America. The company is active in exploration, transportation, production, refining and commercialisation of products.

It employs approximately 10,000 people and has revenues of more than $22 million USD. This project provides protection for 10 of the company’s industrial sites, with different functions in the company’s business, from well development to refining to crude oil transportation.

It is worth mentioning that prior to the start of this project, the client had lack of visibility into activity on its OT network. Furthermore, it had no real control over the infrastructure. Thanks to this project, in which an OT security monitoring solution was implemented, this problem was solved and, additionally, several situations that were endangering the security of the client’s business were detected and resolved.

The different phases followed in the development of the project, from planning to production, are explained below.
3 Phases in the implementation of a monitoring solution

3.1. Phase 1: Project management

Good project management is key to successfully undertake projects, coordinate the different teams, meet deadlines and ensure client satisfaction. Telefónica considered the most appropriate approach for managing this project, taking into account its size and the client’s needs. Due to the nature of the project, the needs of the client and the global pandemic situation, we adopted an agile methodology.

Division of the project into small deliverables and early value delivery. The project is divided into the following phases:
- Consultancy.
- Architectural analysis, where the deployment points of the sensors are identified, the alternatives for traffic capture are analysed and the general architecture of the solution is defined.
- Implementation, including the deployment of sensors and a training phase.
- Operation, where the use cases are defined and implemented.

Formation of a working team in which the manager of each industrial site is included as part of the project. A RACI Matrix was a great help for this purpose.

Continuous communication with the client. Weekly meetings were held with the client to report on the progress of each of the target sites.

Efficient response to change. Real changes and immediate changes were adapted thanks to the involvement of the implementation team.

This agile approach was based on the principles of the agile manifesto:

- **Division of the project into small deliverables and early value delivery.**
- **Formation of a working team in which the manager of each industrial site is included as part of the project.**
- **Continuous communication with the client.**
- **Efficient response to change.**

Thanks to this methodological approach based on delivering value to the client, the project was successfully developed. Below we give a more detailed overview of each of the phases undertaken for this project, and how Telefónica developed the work and solved the challenges that appeared in each one of them.
3.2. Phase 2: Consultancy

A security consultancy is one of the key steps to begin the project. This allows us to understand the client’s environment and network architecture, in order to analyse their current state and determine if they comply with security recommendations. As a result of the audit, a report is delivered to the client, indicating the conclusions found as well as security recommendations that the client must undertake to adequately protect their infrastructure and business.

The first step in any cybersecurity assessment is to define its scope, in other words, the networks and systems that will be studied, both at a technical level and at a management and administration level (policies and procedures). The IEC 62443 standard, widely used as a reference when implementing cybersecurity in industrial environments, refers to this scope as SuC (System under Consideration). In complex infrastructures typical of the Oil & Gas sector, such as a refinery, an interesting option for delimiting SuC is based on a Hazard and Operability Study (HAZOP) analysis. This Process Hazard Analysis (PHA) technique is based on the premise that risks, accidents or operability problems occur as a consequence of a deviation of the process variables with respect to the normal operating parameters. Delimiting the SuC based on HAZOP allows feeding the cybersecurity risk analysis with all hazards identified in the HAZOP engineering process.

The OT consultancy service can be provided at three levels depending on the client’s needs:

**BASIC ASSESSMENT:**
Obtain an overview of the cybersecurity posture of the target industrial plant.

This consists of conducting an OT cybersecurity maturity analysis of the target plant or SuC.

**INTERMEDIATE ASSESSMENT:**
Get a detailed view of the cybersecurity posture of the target industrial plant.

This includes conducting a maturity analysis, a high-level risk assessment and a review of the high-level cybersecurity documentation in place at the target site. This is done by conducting interviews with the heads of the respective cybersecurity areas, complemented by on-site inspections or passive walkdowns to verify the ‘physical’ presence of measures and equipment.

**ADVANCED ASSESSMENT:**
Obtain a comprehensive view of the cybersecurity posture of the target industrial plant.

At this level, the security policies and procedures in place are initially reviewed. With this knowledge base, the team proceeds to assess the plant’s maturity level and completes a high-level risk analysis, both based on interviews and working sessions with plant personnel. To verify the information gathered in the interviews, active walkdowns are carried out, which verify the ‘physical’ presence and check the configuration of the most relevant communications, security and control system equipment (servers and/or stations). Finally, and as a complement to all of the above, network traffic is captured and subsequently analysed in a laboratory environment with various tools, including Network-Based Anomaly Detection (NBAD) systems and Next-Generation Firewalls.
The activities included in the different levels of evaluation above are detailed below.

For all levels, the development of this service is divided into four stages:

**Preparation**
Telefónica requires the client to have access to the information relevant to the development of the work, such as the organisation chart and roles related to security, security policies and procedures, network information, control system technologies (DCS, PLCs, RTUs, industrial protocols, etc.), equipment configuration, etc. The amount and detail of information required depends on the level of the assessment to be carried out. The team of consultants, in permanent contact with the plant personnel, analyses this information and prepares the work to be performed in the next stage.

During this Preparation stage, the interlocutors are also selected and the interviews to be held during the Evaluation stage are determined.

**Evaluation**
This stage takes place at the client’s premises, i.e., onsite for intermediate and advanced level services, and remotely for initial assessments. Most of the assessment activities are carried out during this stage.

**Analysis**
The information gathered in the previous stages is analysed, ordered and added in a results report, which includes information such as the level of cybersecurity maturity, inventory of assets, list of findings, an action plan to cover the deficiencies found, a proposal for improvements, etc. An executive report is also elaborated with the most relevant aspects of the outputs.

**Results**
At the end of the consultancy service, the team travels to the site again to deliver the reports and, if required, to make an executive presentation of the results.

The description of the different activities is given below:

- **Documentation review** to understand the security status of the target plant, including review of policies, procedures, configuration files, network maps, etc.

- **Interviews** with plant personnel to gain first-hand knowledge of all relevant information regarding cybersecurity, including not only technological protection measures installed in the target plant, but also the processes and operations that affect the control systems.

- **OT cybersecurity maturity assessment**, applying our own industrial cybersecurity maturity model and assessment tool, based on three widely known references in the field of cybersecurity and industrial cybersecurity: NIST Cybersecurity Framework (NIST CSF), ISA/IEC 62443 and NIST 800-82r2. In addition to interviews with plant personnel, a tool is used to assess the protective measures, both administrative and technical, in all areas of security as set out in the NIST CSF:
  - risk strategy and organisation
  - protection capabilities
  - detection capabilities
  - response capabilities
  - recovery capabilities

- **High-level risk analysis.** identifying areas of the network and assets that require a higher level of protection and weighing the associated security measures.

- **Walkdowns**, which consist of physically viewing devices or applications that contribute to security (switches, firewalls, domain managers, etc.) or belong to the control systems (servers, engineering stations, operating stations, etc.). During these inspections or walkdowns, it will therefore be possible to check the presence of controls and/or take evidence of findings that will be integrated in the report of results. The walkdowns may be passive, simply verifying the existence of controls, or active, which also include the review of the configuration of those controls or other equipment such as stations, servers, communication equipment, etc.
Network traffic analysis. This analysis is performed in a secure laboratory environment. After taking captures of the plant’s network traffic, these are analysed with various Network Behaviour Anomaly Detection (NBAD) tools, designed for industrial environments, and other applications, such as next-generation firewalls (NGFW). The main purpose of NBAD tools is to monitor network security, alerting in case of an attack, an infection, or a deviation from ‘normal’ network traffic. One such technology is Nozomi Networks, which will be explained in more detail below. However, for the consultancy service, NBAD systems provide valuable and complementary information to the information obtained in the other activities, such as a detailed inventory of devices, vulnerabilities affecting equipment and protocols, problematic network links or misconfigurations. They do so without interfering with the operation of the industrial process by working with a copy of the network traffic. This is an essential factor in the cybersecurity analysis of industrial environments, whose assets, especially PLCs and controllers, are particularly unstable in the face of active cybersecurity breaches.

The following figure shows the relationship of the activities with the stages of the consultancy.

![Consultancy Stages Diagram]
3.3. Phase 3: Architectural analysis

3.3.1. Identification of the points where the sensors are to be deployed

When implementing a security monitoring solution that analyses network traffic, it is vital to have knowledge of the network architecture. In the consultancy section, the network is analysed to see the state and level of security. As a result of this consultancy, the implementation of a network security monitoring solution can be considered as a security recommendation. In this case, it is necessary to analyse the network architecture in order to identify the most suitable locations for the sensors. The location of the sensors determines the visibility of the network that can be achieved; therefore, it is essential to properly locate the traffic aggregation points and identify the key points where the sensors should be placed. The information obtained in the consultancy phase can be a useful starting point for this study.

The difficulty in identifying deployment points is influenced by several factors, including the size of the factory and the client’s knowledge of the network. In some cases with large and complex networks, the identification of the sensor deployment point can be simple when the client is clear about where to place the sensors. The decision can also be quick in instances with only one traffic aggregation point. However, in places with limited knowledge of the network, a network survey phase may be necessary to determine the optimal deployment point. This decision is also influenced by an accurate understanding of the client’s core business and which type of network is most important for them to protect.

For instance, it may be the well network in one location, the gas network in another, and so on. As it can be seen, the client’s cooperation is essential in this process to fully understand and meet their needs. Technological maturity factors are another aspect that may influence these decisions, such as the capabilities of some elements of the client’s network to obtain a copy of the traffic. This is discussed in more detail in the following section.

3.3.2. Analysis of alternatives for traffic capture

In industrial environments, and the Oil & Gas sector, it is important to have passive solutions that do not interfere with or inject traffic into the network. As mentioned above, availability is a factor that must be always provided when working in industrial environments. To guarantee this, monitoring solutions work by analysing a copy of the traffic, not the traffic itself. This ensures that the traffic is not affected, and that no delays are introduced. Even if the security solution went down, the original traffic would never be affected.

There are several technological alternatives available to create these traffic copies. The simplest and cheapest is to use a spam port of a switch. The drawback of this solution is that, if the switch is overloaded, some traffic packets may be dropped, and therefore would not be analysed by the monitoring solution. This is why in some cases it is considered more convenient to install network elements called terminal access points (TAPs), which allow a copy of the traffic without packet loss. There are several models in which even a loss of power would not affect the traffic flowing through the network. Although this is a costly solution, it can be worthwhile in many cases, and there is minimal downtime for the installation. Another situation where it may be advisable to install a TAP when the technology at the site is old or there are purely industrial switches without port mirroring capability.

This is another important point to discuss with clients, to analyse which solution is best suited to their particular case.
### 3.3.3. General architecture of the solution

Once the above points are clear, the general architecture of the solution can be designed. In this case, the security monitoring solution from Nozomi Networks, which specialises in the industrial sector, has been used.

This solution has several functionalities:

- Identification and profiling of each of the assets connected to the client’s network, including the specification of their generic or proprietary operating systems, firmware, software and applications.
- Identification and management of vulnerabilities detected in the client’s network assets.
- Detection of anomalies and threats in the control network thanks to the traffic analysis with deep packet inspection provided by the proposed solution.
- Alerts and alarm notifications classified by level of criticality.
- Report generation.
- Integration with network elements for the mitigation and remediation of security incidents that may arise.

These functionalities can be summarised in three key steps: visibility, threat detection and mitigation, as explained in the figure below.

<table>
<thead>
<tr>
<th>Visibility</th>
<th>Threat Detection</th>
<th>Mitigation</th>
</tr>
</thead>
<tbody>
<tr>
<td>Visibility and profiling of devices (extracting normal patterns of their behavior).</td>
<td>Detection of anomalies and attacks by means of ML and IoT specific cyberintelligence feeds.</td>
<td>Easy integration with main firewalls and SIEMs.</td>
</tr>
</tbody>
</table>

The Nozomi Networks solution is composed of several elements:

- **Sensors**. They are located in the client’s network infrastructure, at the previously located deployment points. They are passive and perform device discovery as well as any security incident or anomaly-related alerting. In this project, physical sensors have been chosen, although they could have also been virtualised as well as containers or cloud appliances. Depending on the number of nodes to be protected, the volume of traffic to be monitored, the number of ports required, whether it needs to be rugged and other parameters, there are multiple sensor models.

  It should be mentioned that the sensors rely on a combination of Machine Learning and cybersecurity techniques for threat detection. Machine Learning techniques allow the behaviour of assets to be profiled and the detection of anomalies that deviate from normal behaviour. In turn, the signatures allow the detection and identification of attacks affecting the client’s assets, taking into account that specific sources are used to detect attacks aimed at the OT sector.

  For this project, a sensor has been located at each industrial site and several sensor models have been used to adapt to the needs of each location.

- **Centralized Management**. This is used for centralized management and analysis in cases where a site has more than one sensor, or where there are sensors at multiple sites. Organizations can utilize the Vantage software-as-a-service platform, or can deploy physical, virtual, or cloud-based central management appliances if they prefer.

  In the case of this project, there is one physical Central Management Console (CMC) that has visibility of all sensors and is connected to the Security Information and Event Management (SIEM).

- **Threat Intelligence and Asset Intelligence**. These services provide regular updates to the threat and anomaly detection capabilities of the sensors, to ensure they are instrumented with the most current threat indicators and asset profiles.
The architecture of the project looks like this:

![Architecture Diagram]

### 3.4. Phase 4: Implementation - deployment of sensors and training

At this point, we are ready to carry out the implementation, which includes the configuration and installation of the sensors. Furthermore, given that the sensors use Machine Learning and Artificial Intelligence techniques to profile the devices and detect anomalies, it is necessary for the sensors to have an initial learning phase before moving on to the protection status.

Once the location of the sensors has been determined, a deployment plan is established.

The project has been executed during the COVID-19 pandemic, which has made travel difficult in some cases. The deployments were initially planned to be carried out in person, but given the circumstances, the plan had to be modified. Telefónica responded quickly to this situation and adapted by looking for solutions and people who were in situ and could carry out the physical installations themselves, guided remotely by the team of experts. To do this, a configuration was made so that the Telefónica teams could remotely access the sensors, as well as make sure that everything was prepared for the installation: power supply, wiring, racks, etc. Once everything was ready, the appropriately configured sensor was sent to be physically installed at the corresponding industrial site. After that, the sensor was put into operation, the necessary adjustments were made, and it was ready and running. It was then verified that the sensor had communication with the CMC and that the information detected by the sensor could be seen from the CMC.

Even while in learning mode, the sensor can begin alerting the client on detected security events, as some alerts do not depend on Machine Learning algorithms.

It should be noted that Telefónica works with a risk analysis methodology in relation to the deployment of the sensors. Although this type of deployment does not usually give rise to problems, Telefónica considered the risk situations that could arise, including occupational risk situations or others such as the assignment of a duplicate IP, and indicated the measures to be taken to resolve them in the event of their occurrence. This ensures that the installation is carried out correctly, anticipating problems so that they do not occur and minimising risks for the client.

Initially the sensors start in learning mode and remain in this mode as long as it takes for them to learn the normal behaviour of the network. This generally takes about one month, after which they can perform detection in the protection mode.
3.5. Phase 5: Definition and implementation of use cases

Once a sensor alert is received, it is crucial to manage those alerts appropriately. For clients, it is essential not only to be aware of the alerts but also to know what to do with them.

This is where Telefónica provides great value to the client through its security alert management service, which is carried out from Telefónica’s SOC, distributed in 11 locations around the world.

The phases following the configuration and learning of the sensors can be structured in the following way:

- **Pre-production socialisation and mitigation phase.** This includes the tasks of sensor recognition, alert notification to the site manager and mitigation.

- **Sensor integration and alert production phase.** In this phase, the integration with the SIEM, generation of use cases, definition of resolution groups and generation of alarms to the identified resolution groups are carried out.

Further details of the experience in developing these phases of the project are given below.

Once the alerts are received in the SIEM, the use cases are created. The Nozomi Networks solution has about 95 types of alerts categorised into 5 different groups. For the project in this case study, the CMC is linked to an SIEM which receives and correlates the alerts. In turn, the SIEM is connected to a Security Orchestration, Automation and Response (SOAR) which allows orchestration and automation of certain tasks through the development of playbooks.

In this case, a security monitoring service is also offered in both IT and OT environments. Telefónica has extensive experience in the management of this type of IT services, which is also used for the management of OT environments, with the appropriate adaptations.

The stages of the SOC operating model are summarised in the following figure:
In this sense, Telefónica is working closely with the client to reduce the volume of alerts and assign them to different resolution groups depending on the nature of the alert. To this end, several meetings are held in a pre-operational stage in which we work with the client and decide how we wish to deal with each type of alert. Initially, we start by analysing the most critical alerts, as these can have the greatest impact on the client’s security and business and also require the fastest response. Several criteria have been used to select the use cases: the volume of alerts of each type and the risk associated with each alert, so that the alerts with the highest volume and highest risk have been prioritised.

In these meetings, an action plan is established for the remediation of the alerts, as well as a follow-up to ensure that everything is running smoothly. This part is of great value to the client, since in order to have an optimal security service, it is not only important to have good technology but also to have a team specialised in managing and optimising it for the client’s needs.

Initially, when the sensors are in a learning period and have not been properly adjusted, the alert volume may be higher. This is why this alerting optimisation process is carried out to reduce the volume of alerts, since a high number of alerts makes it difficult not only to manage but also to react to.

Once the alerts have been profiled and the use cases defined, together with the resolution groups and the escalation patterns, this information enters the operation flow of Telefónica’s SOCs. At this stage, playbooks are developed to automate tasks and assign them to the corresponding resolution groups, which may be more focused on the IT or OT area depending on the nature of the alert. Telefónica’s SOC has a level 1 that operates 24/7 resolving incidents and discarding false positives. If necessary, the incident can be escalated to a level 2 for further analysis and investigation. It is worth mentioning that an integration with the client’s ticketing tool has also been implemented.

Telefónica’s SOC has a team of experts and extensive experience in the management of this type of service, with a multidisciplinary team and 24/7 support. Telefónica’s experts are certified in Nozomi Networks technology both globally and locally, in order to develop projects with maximum guarantees.

As a result of the implementation of the solution, several security incidents affecting the client’s assets were detected. For example, a serious vulnerability was detected in some of their equipment and connections to disreputable IPs were also detected. These incidents have been discussed with the client and appropriate security measures have been agreed upon to mitigate the risk and prevent further damage. Therefore, having this visibility and management of alerts has been of great benefit to the client and has resulted in a higher level of security for their business.
Companies in the OT sector are exposed to a wide range of threats. Therefore, visibility and mitigation of these threats through threat detection becomes essential for a properly secured environment.

This document explains a successful case of a real project in which Telefónica has participated by implementing and operating a security monitoring service through the analysis of network traffic, using technologies specialised in analysing industrial protocols, as well as the detection of threats directed at this environment.

In the particular case of this project, the implementation of the solution has made it possible to:

› Firstly, a better understanding of their network by the client.

› Secondly, gaining visibility over the assets connected to the client’s network, understanding what type of assets are connected at each site and what their associated vulnerabilities are.

› In addition, alerts have been obtained and managed by the SOC and reported to the client in the case of security incidents. In particular, in this case, equipment with vulnerabilities or connections to malicious sites were identified. Thanks to the adoption of the OT security monitoring service, these threats have been reported to the client and appropriate remediation measures have been taken, resolving the security issues and creating a much safer environment for the client’s operation centres.

Given this successful case, the recommendation for companies in the Oil & Gas sector is that, first of all, they should carry out a security audit that allows them to understand where they are and what recommendations are necessary to strengthen their security status.

Having a security monitoring service in place brings the advantage of gaining visibility into what elements are connected to the network, which is a fundamental and crucial step, since what cannot be seen cannot be protected. Knowing which vulnerabilities are present in assets, or which may be old in many cases, allows preventive measures to be taken to avoid these vulnerabilities being exploited. In addition, having the experience of Telefónica and having the peace of mind that its experts are monitoring system alerts 24/7 is a great benefit for the client, who can know when one of its assets is not performing correctly and can even detect anomalies in the variables of the industrial process.

If you would like to know more about this and other cyber security solutions, please do not hesitate to contact us, we will be delighted to help you.
About Telefónica Tech

Telefónica Tech is a key holding of the Telefónica Group. The company offers a wide range of integrated technology services, reaching more than 5.5 million customers in 175 countries every day. Telefonica TECH will host other digital businesses in the future, including in the B2C segment.