MISSION CRITICAL SOC

OT & IT Segregation and OT Segmentation

HOW CAN TELEFÓNICA TECH HELP?

Telefónica Tech offers this service specially designed for industry that manage complex control networks.

These companies typically operate multiple manufacturing plants, each with critical automated systems, such as assembly lines, industrial robots, SCADA (Supervisory Control and Data Acquisition) systems, and other IoT and OT (Operational Technology) devices.
The purpose is to ensure that these industrial networks are protected against cyberattacks, minimizing the risk of production disruptions that could have a significant impact on operational efficiency and end-product quality.

Due to the pace of technological change and the need for specialized equipment, most organizations do not have the capacity to respond to today's sophisticated threats, leading to painful business processes, large ransomware payouts, legal expenses, reputational losses, etc.

In industrial environments, innovative applications and systems often coexist alongside equipment and operating systems that have been in the field for several years and will most likely need to remain in operation for several more years. These systems cannot always be updated, so it is necessary to establish protection mechanisms that make it impossible for cybercriminals to exploit vulnerabilities.
In this context, it is essential to design and implement a secure network architecture based on the segregation of IT and OT environments and the appropriate segregation of OT networks..

WHO IS THIS SERVICE FOR?

Our professional industrial security service is for those organizations with the need to address the following industry challenges:

Increased Connectivity and Attack Surface: The integration of IT and OT technologies and the increase in connected devices expand the opportunities for cyberattacks.

Critical and Sensitive Systems: Industrial environments often operate with systems that cannot afford downtime, making security and resilience critical.

Evolving Threats: Cyber threats are becoming more sophisticated, requiring advanced solutions that can adapt and respond effectively.

Visibility and Monitoring: Many organizations lack complete visibility into their OT systems, making it difficult to detect and respond to security incidents.

Regulations and Compliance: Industries are subject to strict regulations that require the implementation of robust security measures to protect critical data and infrastructure.

OUR VALUE PROPOSITION

Our service

Telefónica Tech ' s value proposition in IT/OT segregation and OT segmentation for industry lies in its ability to offer a **comprehensive and customized solution** that ensures the integrity, availability, and confidentiality of industrial systems.

- **Tailor-made design:** Adaptation of the network architecture to the specific needs of the plant, taking into account the particularities of each control system and the highly automated nature of the processes.
- **Advanced technology:** Implementation of next-generation firewalls, intrusion detection systems (IDS/IPS), and other technological solutions that ensure that OT networks are completely isolated from IT networks, thereby preventing a breach in the corporate network from affecting production systems.
- **Regulatory compliance:** Ensuring that the company complies with industrial cyber security regulations, such as IEC 62443, and other applicable standards, which not only protects against threats, but also facilitates audits and regulatory reviews.

What does it allow you to do?

- **Isolate critical OT networks:** Ensure that networks controlling production processes are completely separated from IT networks, thereby reducing the attack surface and protecting industrial control systems (ICS) from potential cyberattacks.
- **Control and monitor network traffic:** Enable detailed monitoring and control of traffic between different segments of the OT network, ensuring that only necessary and authorized communications take place, thus limiting the risk of lateral movement of threats within the network.
- **Optimize security and performance:** Maintain the balance between security and operational efficiency, allowing the plant to continue to operate smoothly while minimizing cyber security risks.

Benefits

1. Protection against advanced cyber-attacks: :

The risk of a cyberattack compromising critical production systems is significantly reduced by segmenting the OT network. This is vital in an environment where disruption of the production process can lead to significant economic losses.

2. Improved operational resiliency:

With a well-segmented network, an incident in one segment does not affect the entire plant, allowing for rapid containment and recovery, keeping most operations running without interruption.

3. Regulatory compliance:

Comply with automotive-specific cyber security regulations, facilitating audits and improving customer and business partner confidence.

4. Improved Visibility and Control:

Log collection and analysis, reporting and graphical representations provide a clear and detailed understanding of the status of systems, enabling organizations to make informed and strategic decisions.

Telefónica Tech's differential value

Experience and Expertise: Telefónica Tech has a team of industrial cyber security experts who understand the specific needs of each sector. This includes a deep understanding of industrial control systems and the unique challenges they present.

Leading technology: Integration of advanced technologies, such as next-generation firewalls and continuous monitoring solutions, which are designed to protect highly automated industrial environments and ensure data security and process integrity.

Comprehensive and managed approach: Provision of an end-to-end managed service, from planning and design of the network architecture to implementation and ongoing monitoring, ensuring that the plant is protected at all times.

Scalability and flexibility: Ability to adapt and scale the solution according to the specific needs of each plant or production line, ensuring that cyber security evolves along with the business.

Continuous and local support: Telefónica Tech offers specialized and local technical support, ensuring that cyber security solutions are kept up to date and adapted to the latest threats and needs of the sector.

EQUIPMENT, TEAMS, AND ACHIEVEMENTS

The team behind this industrial cyber security proposal is comprised of specialists in several key areas.

1. Cyber Security Operators and Analysts:

Monitoring and Response: Specialists in continuous monitoring of endpoints for detection and response to security incidents, using advanced malware detection and threat analysis tools.

Threat Intelligence: Ability to feed protection systems with real-time threat intelligence to identify and mitigate emerging attacks.

2. Security Engineers and Consultants:

Design and Implementation: Responsible for the design and implementation of endpoint security solutions, ensuring protection against malware and other threats on critical devices.

Assessments and Audits: Perform endpoint security assessments to identify vulnerabilities and propose improvements to the organization's security posture.

3. Specialists in Security Technologies:

Implementation of next-generation firewall (NGFW) solutions for perimeter protection and segmentation of production networks.

Centralized management of security policies and secure remote access through ZTNA (Zero Trust Network Access.

Telefónica Tech has successfully implemented and managed cyber security solutions in a variety of industry sectors.
Some of the most outstanding achievements include:

1. Energy Sector:

Power Generation and Distribution: implementation of an OT security monitoring solution that spans multiple locations, improving asset visibility and vulnerability detection..

2. Naval Sector:

Civilian and Military Shipbuilding: Design and integration of cyber security capabilities in new generation naval platforms, focusing on control and combat systems.

3. Healthcare Sector:

Leading Private Healthcare Sector: Complete visibility of electro-medical assets, risk management and customization of security solutions to integrate with tools that are already deployed.

4. International Projects:

Multinationals in Different Sectors: Provision of managed security monitoring services for companies in sectors such as water treatment, theme parks and logistics, achieving a significant improvement in threat detection and critical infrastructure protection.

BUSINESS MODEL

The business model of the proposal is based on a combination of managed services and customized projects, structured in several phases:

1. Initial Assessment:
Deployment of Technologies: Installation and configuration of next generation firewalls (NGFW), authentication and security monitoring systems to ensure continuous protection of industrial environments.

2. Planning and Design:
Secure Architecture Design: Development of a detailed secure network architecture plan, including network segregation and segmentation, as well as implementation of perimeter protection measures.

3. Implementation:
Technology Deployment: Installation and configuration of next generation firewalls (NGFW), authentication and security monitoring systems to ensure continuous protection of industrial environments.

4. Management and Continuous Monitoring:
Managed Services: Provision of continuous security monitoring and management services, including traffic analysis, threat detection and incident response through a dedicated Security Operations Center (SOC).

5. Training and Awareness:
Training: Training internal personnel in industrial cyber security practices, ensuring that employees are able to identify and respond appropriately to threats.

6. Optimization and Continuous Improvement:
Review and Update: Periodic evaluation of security posture and updating of implemented policies and technologies to adapt to new risks and challenges.

RELATED PARTNERS

FORTINET paloalto NETWORKS CHECK POINT CISCO

RELATED SERVICES

OT & IoT Security Monitoring

A comprehensive solution for asset visibility and threat detection through traffic analysis, offered as a managed service by Telefónica Tech as part of a SOC specialized in industrial and healthcare environments.

Aristeo

Telefónica Tech's OT network for predictive threat capture and analysis that generates intelligence with differential value.

OT EDR

Comprehensive and advanced protection for industrial OT environments, with an emphasis on operational continuity. The Zero Trust model protects all components and communications within the system, mitigating risks without interfering with continuous operations. They also offer implementation, support, maintenance, and technology management services. A 360° service.

Contact us to start the digital transformation of your organization.