MISSION CRITICAL SOC

OT EDR

HOW CAN TELEFÓNICA TECH HELP?

Telefónica Tech offers an endpoint protection solution for OT and IoT environments backed by innovative technology from TXOne Networks.

These services are designed to safeguard digital assets against increasingly sophisticated cyber threats. They provide a comprehensive endpoint protection solution that includes **inspection, auditing, defense from the network, and centralized management** through unified consoles.

Due to the pace of technological change and the need for specialized teams, most organizations do not have the capacity to respond to today's sophisticated threats. This results in painful business processes, large ransomware payouts, legal expenses, reputational losses, etc. Effective detection and response requires **world-class** detection technology, managed by a dedicated team that enables proactive threat assessments and rapid containment of attacks.

WHO IS THIS SERVICE FOR?

Telefónica Tech's endpoint protection service is aimed at a wide range of industrial organizations operating in OT environments such as manufacturing, energy, agribusiness, chemical, mining, transportation, and a long etc.... This service is crucial for those companies facing specific challenges related to the convergence of IT (Information Technology), IoT (Internet of Things), and OT technologies.

Our professional industrial security service is aimed at 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 focuses on offering comprehensive and advanced protection for industrial OT environments, with a focus on Operational Continuity, implementing the Zero Trust model to secure each component and communication within the system, thus mitigating risks without interfering with continuous operation. We also provide a service of implementation, support, maintenance, and operation of the technology.

What does it allow you to do?

1. Specialized support:

- Upgrades and maintenance.
- Log collection and analysis.
- Policy and profile management.
- Network monitoring and management.

2. Implementation::

- Initial assessment and planning.
- Hardware and software acquisition.
- Device configuration and preparation.
- Implementation and deployment.

3. Much more ...

- Detection and removal of malware in endpoints.
- Security inspections and audits.
- Centralized security management through consoles.
- Continuous innovation using the latest technology.
- Availability of an expert team with more than 15 years of experience in managed security services.
- Resilience and Redundancy, ensuring high availability and secure network segmentation.
- Improved visibility of OT systems, enabling early detection and rapid response.

4. Technology exploitation:

- Monitoring and alert generation.
- Proactive updating and maintenance.
- Reporting and data analysis.
- Graphical representation and asset management.

5. Equipment maintenance:

- Initial evaluation and diagnosis.
- Equipment management.
- Monitoring and management of maintenance contracts..

Benefits

1. Performance and availability optimization:

Proactive hardware and software deployment, maintenance, and upgrades ensure that devices perform optimally, reducing downtime and improving operating efficiency.

2. Security and compliance:

Specialized support and proactive operation services ensure that systems are always protected against new threats, comply with security regulations and maintain information integrity.

3. Efficient management of incidents and updates:

Through reactive and proactive support and ongoing maintenance, rapid identification and resolution of technical issues is ensured, minimizing disruptions, and maximizing business continuity.

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

Technology expertise:
Our team is highly trained and specialized in the latest EDR technologies. Not only do we have in-depth knowledge of the most advanced tools on the market, but we are also constantly updated to apply best practices in protecting your systems from cyber threats.

Implementation and operation capabilities from our SOC:
Our Security Operations Centers (SOCs) are the heart of service management. This is where we efficiently deploy the EDR solution, ensuring its correct configuration and continuous monitoring to detect and respond to incidents in real time. Our ability to proactively monitor, analyze, and adjust the system ensures that your company is always protected.

Expertise in managing security services for a broad customer base:
We have years of experience in managing cyber security services for many customers. We understand the diversity of needs in different sectors. This allows us to offer a flexible and tailored service, designed to maximize security according to the particular characteristics of each business.

Specialized end-to-end approach to industrial cyber security:
Our approach to cyber security goes far beyond EDR for operational environments (OT). We offer a comprehensive solution that covers all layers of security in critical industrial environments, from the protection of control systems to the monitoring of industrial networks, ensuring a robust and specialized defense for any challenge.

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. Endpoint Protection Technology Specialists:

Use of security agents installed on devices for monitoring and blocking malicious activities.

Centralized management: Implementation of management control panels for centralized administration of endpoint protection agents.

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:
Diagnostics and Risk Assessment: Conducting cyber security audits and assessments to identify critical assets, vulnerabilities, and associated risks.

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

txOne networks

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.

OT & IT segregation and OT segmentation

A solution based on the design and implementation of a network architecture that allows segregating IT and OT environments as well as segmenting OT environment networks, complemented with additional technologies to advance the application of ZeroTrust models.

Industrial Cyber Security Assessment

The service evaluates cyber security in OT environments using the ISA/IEC 62443 standard as a reference. It combines the analysis of documentation provided by the organization with a technical assessment based on the analysis of captured network traffic. A compliance assessment with respect to applicable regulations, such as ISA/IEC 62443 or other industry-specific standards (e.g. NERC for energy, LPIC for critical infrastructure) can also be performed. Additionally, it includes ethical hacking activities to assess the security level of infrastructures.

Contact us to start the digital transformation of your organization.