MISSION CRITICAL SOC

Aristeo - DaaS

HOW CAN TELEFÓNICA TECH HELP?

Deception Technology systems substantially improve detection mechanisms through early detection of malicious activity and improved knowledge of cybercriminals. Although they can be applied in all types of environments and systems, they are particularly valuable in industrial environments, critical infrastructures and essential services, where the consequences can be serious, including the interruption of processes, damage to both physical elements and people, economic and reputational losses.

Telefónica TECH helps you through the implementation of a Deception as a Service (DaaS), a pioneering cyber security solution designed for industrial environments (OT) and Internet of Things (IoT). We therefore deploy a network of industrial decoys with the aim of capturing and analyzing cyber threats in a predictive and proactive manner. As a differential value, we add decoys in physical environments that replicate real processes of our customers to the virtual decoys. This allows us to:

. This allows us to:

- Early and reliable threat detection,
- Risk mitigation in obsolete systems,
- Reduction of false positives,
- Attacker detour and containment,
- Obtaining intelligence on attack methods,
- Rapid and effective response.

WHO IS THIS SERVICE FOR?

The DaaS service is aimed at companies that want to improve their proactive threat detection capabilities. It is ideal for industries whose business depends on critical systems that are essential for business availability, such as manufacturing, energy, automotive, connected medical equipment and any other industry with operations that rely on interconnected industrial devices.

Our deception as a service is adaptable and scalable, helping our customers, regardless of their cyber security maturity level, to meet growing challenges:

Increased Connectivity and Attack Surface:
The integration of IT, OT, and IoT technologies and the increase in connected devices expands the surface of exposure to cyberattacks.

Critical and Sensitive Systems:
Medical and industrial environments often operate 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/ IoT 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

Our DaaS service integrates two types of solutions: one is the Aristeo advanced cyberintelligence platform (patented and developed entirely from the Innovation area of Telefónica TECH) that uses real industrial hardware.

The second is third-party systems and appliances that are market leaders in the development of deception cases. The integration of the two technologies ensures the authenticity and accuracy of threat information. To offer a joint, innovative, and differential solution, designed to adapt to the specific needs of each customer, allowing the configuration of decoys to represent any industrial process or productive sector.

What does it allow you to do?

1. Capture and predictive threat analysis:

DaaS deploys a network of industrial decoys that act as “traps” for attackers. These decoys are designed to resemble real, virtualized industrial systems and processes. This attracts cybercriminals and allows them to interact with an environment they consider legitimate. Thanks to our approach, capturing these interactions is done in real time, enabling in-depth analysis of the tactics, techniques and procedures (TTPs) used by attackers. This not only helps to identify current and 0-day threats, but also allows to foresee future attack attempts, based on observed behavioral patterns.

2. Simulation of real industrial environments:

Unlike other market solutions, we add an extra layer of exposure and interaction with real decoys. This ensures that threat behavior is captured more accurately and that the countermeasures developed are highly effective.

3. Predictive and actionable intelligence:

Thanks to continuous data capture, DaaS identifies patterns that could indicate new and emerging threats. This predictive intelligence enables our customers to anticipate and prepare for attacks before they occur, providing a significant advantage in protecting their critical assets.

4. DaaS service integration with existing defense systems:

It can be integrated with other defense tools and systems that the company already has in place, such as security information and event management (SIEM) systems and threat intelligence platforms (TIP) managed by our SOCs or by our customers’ SOCs.

5. Operational continuity without interruption:

DaaS runs in parallel with our customers’ actual operational systems and does not require modifying existing infrastructure, companies can benefit from its protection **without any disruption to their operations.** Decoys can be deployed externally or on the customer’s infrastructure, depending on specific needs, which offers total flexibility in their implementation.

6. Detailed and customized report generation:

We have the ability to generate detailed reports that analyze the behavior of detected threats, exploited vulnerabilities and possible mitigations, thanks to the intelligence obtained. These reports can be customized to meet specific customer needs, providing in-depth and specific knowledge that translates into practical actions to improve security.

Benefits

1. Advanced threat detection:

Early identification of advanced threats, including APT (Advanced Persistent Threats) groups and unknown vulnerabilities (0-day).

2. Predictive intelligence:

Continuous analysis of threats to anticipate potential attacks and strengthen security.

3. Adaptability and flexibility:

Ability to adapt to the customer's specific infrastructure and processes, without the need to take up space in their infrastructure or facilities in the case of physical decoys, although the service is also available on premises.

4. Constant protection:

Our DaaS solution operates 24/7, providing continuous monitoring and real-time updates on new threats.

5. Compliance support:

DaaS further helps companies comply with industry-specific cyber security regulations and standards by providing a test environment in which to check whether the measures in place for such compliance are adequate and the infrastructure and processes are protected against current and emerging threats.

Telefónica Tech's differential value

Telefónica Tech offers a disruptive and innovative approach to industrial cyber security with its DaaS solution, differentiating itself from other services by being able to incorporate the use of real hardware. This adds to the intelligence gained by allowing attackers to also interact with a more realistic environment and providing high quality data on their tactics, techniques, and procedures.

EQUIPMENT, TEAMS, AND ACHIEVEMENTS

The DaaS proposal has been developed and is managed by cyber security experts at Telefónica Tech, seeking to protect the industry, critical and essential infrastructures. It unites the knowledge and development of own solutions, such as Aristeo, with solutions from third party market leaders, improving the ability to detect threats that have not been previously identified by other intelligence platforms.

1. Development, Innovation, and Product Team:

A DaaS value proposition is defined from the Product area with the clear objective of positioning Telefónica TECH as a benchmark in the field of industrial cyber security, working with the best partners in the market and preparing differential and high value offers for our customers. We are not simply resellers; we provide value through the integration of Telefónica TECH's own technology with Aristeo. Aristeo is a solution developed in the Industrial Cyber Security Center of Telefónica Tech C4IN in León, a specialized laboratory that focuses on creating innovative solutions to protect industry, critical and essential infrastructures.

2. Implementation and Support Team:

The implementation and support team is responsible for customization, deployment, and maintenance of the solution. This team works closely with customers to ensure that the solution is perfectly tailored to their specific needs.

- The implementation experts have a deep understanding of industrial infrastructures and are able to adapt the DaaS configuration to optimally integrate into the customer's operating environment. They also provide ongoing support, ensuring that the solution works efficiently and that any problems are quickly resolved.

- The team has successfully deployed Aristeo in several critical industrial facilities, maintaining uninterrupted operation and adapting the solution to various complex infrastructures, such as automotive factories, power plants and advanced manufacturing processes.

3. Threat Research and Analysis Team:

This team is responsible for analyzing threats captured by the DaaS solution and converting that data into actionable intelligence.

- The cyber security analysts in this team are specialized in identifying advanced threats, such as APTs (Advanced Persistent Threats) and 0-day vulnerabilities. They are also experts in applying artificial intelligence and machine learning techniques to improve the accuracy of threat detection and prediction.
- The team has also developed a series of intelligence reports that enable customers to understand the up-to-date state of the global cyber threat ecosystem, so they can anticipate targeted attacks and proactively improve their defenses.

4. Customer Management and Strategy Team:

This team manages customer relationships and ensures that DaaS aligns with the strategic objectives of each organization. They are also responsible for coordinating projects and customizing the service to fit the specific needs of each customer.

- Account managers and strategists have a deep understanding of the industry sector, and the security needs of their customers. They are experts in customizing services and creating long-term strategies that optimize cyber security investment.
- Thanks to their customized approach, this team has been able to establish trusted relationships with key clients in sectors such as automotive, energy, and manufacturing, contributing to Aristeo's expansion in the market.

Telefónica Tech has successfully implemented and managed cyber security solutions in a variety of industry sectors.

Some of the most outstanding achievements include:

1. Critical Infrastructure Protection:

DaaS has been implemented in factories and critical facilities, where it has detected and neutralized advanced threats that could have caused serious disruptions or damage. An outstanding example is the protection of the HORSE plant in Valladolid, where early vulnerabilities have been identified and potential threats have been anticipated.

2. Innovation in industrial cyber security:

Aristeo's team has developed a unique approach to industrial cyber security, which has been recognized in international technology and cyber security forums. Its ability to combine real hardware with advanced intelligence has set new standards in protecting OT environments.

3. Development of New Capabilities:

The team continues to enhance and expand DaaS capabilities with other market solutions, incorporating new predictive analytics functions and artificial intelligence capabilities, positioning us with adaptable, flexible and scalable solutions, and one of the most advanced on the market.

BUSINESS MODEL

The DaaS service is offered under a managed service model, which includes consulting, installation, maintenance, and ongoing support. It is tailored to customer needs with flexible integration options, allowing companies to access an advanced cyberintelligence solution without the need for large infrastructure investments, 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:** evelopment of a detailed secure network architecture plan, including network segregation and segmentation, if necessary, as well as implementation of perimeter protection measures.

- **Procurement Model:**
  - On-premise:
    - Acquisition of physical equipment with license included.
    - Deployment on customer's virtual machine, software licensing.
  - Cloud deployment:
    - Services deployed on Telefonica infrastructure.

3. Deployment:

- **Deployment of Technologies:** Installation and configuration of next generation firewalls (NGFW), authentication and security monitoring systems to ensure continuous protection of industrial environments.
- **Deployment of campaigns and** decoys.

4. Continuous management and 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 of 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.

Contact us to start the digital transformation of your organization.