MISSION CRITICAL SOC

Aristeo - DaaS

¿CÓMO TE AYUDAMOS DESDE TELEFÓNICA TECH?

Los sistemas de engaño (*Deception Technology*) mejoran sustancialmente los mecanismos de detección mediante la detección temprana de actividad maliciosa y el mejor conocimiento de los cibercriminales. Aunque pueden aplicarse en todo tipo de entornos y sistemas, resultan particularmente valiosos en entornos industriales, infraestructuras críticas y servicios esenciales, donde las consecuencias pueden ser graves, incluyendo la interrupción de procesos, daños tanto a elementos físicos como a las personas, pérdidas económicas y de reputación.
Desde Telefónica TECH te ayudamos mediante la implementación de un servicio *Deception as a Service (DaaS)*, una solución pionera en ciberseguridad diseñada para entornos industriales (OT) y de Internet de las Cosas (IoT). Para ello desplegamos una red de señuelos industriales con el objetivo de capturar y analizar amenazas cibernéticas de manera predictiva y proactiva. Como valor diferencial, añadimos a los señuelos virtuales, señuelos en entornos físicos que replican procesos reales de nuestros clientes.

Esto permite:

- La detección temprana y fiable de amenazas,
- Mitigación del riesgo en sistemas obsoletos,
- Reducción falsos positivos,
- La desviación y contención de atacantes,

¿A QUIÉN VA DIRIGIDO ESTE SERVICIO?

El servicio *DaaS* está dirigido a empresas que quieran mejorar su capacidad de detección proactiva de amenazas. Es ideal para industrias cuyo negocio depende de sistemas críticos cuya disponibilidad sea esencial para el negocio, como manufactura, energía, automoción, equipamiento médico conectado y cualquier otra con operaciones que dependen de dispositivos industriales interconectados.

Nuestro servicio de *deception as a service* es adaptable y escalable, ayudando a nuestros clientes, independientemente del grado de madurez en ciberseguridad, a hacer frente a los retos crecientes:

Mayor Conectividad y Superficie de Ataque:
La integración de tecnologías IT, OT e IoT y el aumento de dispositivos conectados amplían la superficie de exposición a ataques cibernéticos

Sistemas Críticos y Sensibles:
Los entornos médicos e industriales a menudo operan con sistemas que no pueden permitirse tiempo de inactividad, lo que hace que la seguridad y la resiliencia sean fundamentales.

Amenazas Evolutivas: Las amenazas cibernéticas se están volviendo más sofisticadas, requiriendo soluciones avanzadas que puedan adaptarse y responder eficazmente.

Visibilidad y Monitoreo: Muchas organizaciones carecen de visibilidad completa sobre sus sistemas OT / IoT, lo que dificulta la detección y respuesta a incidentes de seguridad.

Regulaciones y Cumplimiento:
Las industrias están sujetas a regulaciones estrictas que requieren la implementación de medidas de seguridad robustas para proteger datos e infraestructura crítica.

NUESTRA PROPUESTA DE VALOR

Nuestro servicio

Nuestro servicio *DaaS* integra dos tipos de soluciones: una es la plataforma Aristeo de ciberinteligencia avanzada (patentada y desarrollada íntegramente desde el área de Innovación de Telefónica TECH) que emplea *hardware* industrial real, la segunda son sistemas y *appliances* de terceros líderes en el mercado en el desarrollo de casos de engaño. La integración de las dos tecnologías asegura la autenticidad y precisión de la información sobre amenazas. Ofrecer una solución conjunta, innovadora y diferencial, diseñada para adaptarse a las necesidades específicas de cada cliente, permitiendo la configuración de los señuelos para representar cualquier proceso industrial o sector productivo.

¿Qué te permite?

1. Captura y análisis predictivo de amenazas:

DaaS despliega una red de señuelos industriales que actúan como "trampas" para los atacantes. Estos señuelos están diseñados para parecerse a sistemas y procesos industriales reales y virtualizados, lo que atrae a los ciberdelincuentes y les permite interactuar con un entorno que consideran legítimo. Gracias a nuestra propuesta la captura estas interacciones se realiza en tiempo real, permitiendo un análisis profundo de las tácticas, técnicas y procedimientos (TTP) utilizados por los atacantes. Esto no solo ayuda a identificar amenazas actuales y *zero days*, sino que también permite prever futuros intentos de ataque, basados en patrones de comportamiento observados.

2. Simulación de entornos industriales reales:

A diferencia de las otras soluciones de mercado, añadimos una capa extra de exposición e interacción con señuelos reales. Así aseguramos que el comportamiento de las amenazas se capture con mayor precisión y que las contramedidas desarrolladas sean altamente efectivas.

3. Inteligencia predictiva y accionable:

Gracias a la captura continua de datos, *DaaS* identifica patrones que podrían indicar nuevas amenazas emergentes. Esta inteligencia predictiva permite a nuestros clientes anticiparse y prepararse a ataques antes de que ocurran, proporcionando una ventaja significativa en la protección de sus activos críticos.

4. Integración servicio *DaaS* con sistemas de defensa existentes:

Puede integrarse con otras herramientas y sistemas de defensa que la empresa ya tenga implementados, como sistemas de gestión de eventos e información de seguridad (SIEM) y plataformas de inteligencia de amenazas (TIP) gestionadas por nuestros SOCs o por los SOC de nuestros clientes.

5. Continuidad operativa y sin interrupciones:

DaaS funciona en paralelo con los sistemas operativos reales de nuestros clientes y no requiere modificar la infraestructura existente, las empresas pueden beneficiarse de su protección **sin ninguna interrupción en sus operaciones**. Los señuelos se pueden desplegar externamente o en la infraestructura del cliente, dependiendo de las necesidades específicas, lo que ofrece total flexibilidad en su implementación.

6. Generación de informes detallados y personalizados:

Gracias a la inteligencia obtenida, disponemos de la capacidad de generar informes detallados que analizan el comportamiento de las amenazas detectadas, las vulnerabilidades explotadas y las posibles mitigaciones. Estos informes pueden ser personalizados para cubrir las necesidades específicas del cliente, ofreciendo un conocimiento profundo y específico que se traduce en acciones prácticas para mejorar la seguridad.

Beneficios del servicio

1. Detección avanzada de amenazas:

Identificación temprana de amenazas avanzadas, incluyendo grupos APT (Advanced Persistent Threats) y vulnerabilidades desconocidas (0-day).

2. Inteligencia predictiva:

Análisis continuo de las amenazas para prever posibles ataques y reforzar la seguridad.

3. Adaptabilidad y flexibilidad:

Capacidad para adaptarse a las infraestructuras y procesos específicos del cliente, sin necesidad de ocupar espacio en su infraestructura ni en sus instalaciones en el caso de señuelos físicos, aunque el servicio también está disponible on premise.

4. Protección constante:

Nuestra solución *DaaS* opera 24x7, proporcionando vigilancia continua y actualizaciones en tiempo real sobre nuevas amenazas.

5. Compatibilidad con el cumplimiento normativo:

DaaS ayuda, además, a las empresas a cumplir con las normativas y estándares de ciberseguridad específicos del sector industrial, proporcionando un entorno de pruebas en el que comprobar si las medidas establecidas para dicho cumplimiento son adecuadas y la infraestructura y procesos están protegida contra las amenazas actuales y emergentes.

Valor diferencial de Telefónica Tech

Telefónica Tech ofrece un enfoque disruptivo e innovador en la ciberseguridad industrial con su solución *DaaS*, diferenciándose de otros servicios al poder incorporar el uso de hardware real. Esto suma a la inteligencia obtenida mayor grado de confianza a permitir a los atacantes interactuar también con un entorno más realista y proporcionando datos de alta calidad sobre sus tácticas, técnicas y procedimientos.

EQUIPO Y LOGROS

La propuesta de DaaS ha sido desarrollada y es gestionada por expertos en ciberseguridad de Telefónica Tech, buscando la protección de la industria, de las infraestructuras críticas y esenciales. Une el conocimiento y desarrollo de soluciones propias integrables, como Aristeo, con soluciones de terceros líderes de mercado, mejorando la capacidad de detección de amenazas que no han sido identificadas previamente por otras plataformas de inteligencia.

1. Equipo de Desarrollo e Innovación:

Desde el área de Producto se define una propuesta de valor de DaaS con el claro objetivo de posicionar a Telefónica TECH como referente en el ámbito de la ciberseguridad industrial, trabajando con los mejores partners del mercado y preparando ofertas diferenciales y de alto valor para nuestros clientes. Este es el caso de DaaS, no somos simplemente unos resellers, aportamos valor a través de la integración con tecnología propia de Telefónica TECH con Aristeo. Aristeo es una solución desarrollada en el Centro de Ciberseguridad Industrial de Telefónica Tech C4IN en León, un laboratorio especializado que se centra en la creación de soluciones innovadoras para proteger a la industria, infraestructuras críticas y esenciales.

2. Equipo de Implementación y Soporte:

El equipo de implementación y soporte se encarga de la personalización, despliegue y mantenimiento de la solución. Este equipo trabaja en estrecha colaboración con los clientes para garantizar que la solución se adapte perfectamente a sus necesidades específicas.

- Los expertos en implementación tienen una profunda comprensión de las infraestructuras industriales y son capaces de adaptar la configuración de DaaS para integrarse de manera óptima en el entorno operativo del cliente. Además, ofrecen soporte continuo, asegurando que la solución funcione de manera eficiente y que cualquier problema sea resuelto rápidamente.

- El equipo ha logrado implementar Aristeo en varias instalaciones industriales críticas, manteniendo la operación sin interrupciones y adaptando la solución a diversas infraestructuras complejas, como fábricas de automóviles, plantas de energía y procesos de manufactura avanzada.

3. Equipo de Investigación y Análisis de Amenazas:

Este equipo es responsable de analizar las amenazas capturadas por la solución *DaaS* y convertir esos datos en inteligencia accionable.

- Los analistas de ciberseguridad en este equipo están especializados en la identificación de amenazas avanzadas, como APTs (Advanced Persistent Threats) y vulnerabilidades de día cero. También son expertos en la aplicación de técnicas de inteligencia artificial y machine learning para mejorar la precisión de la detección y la predicción de amenazas.
- El equipo también ha desarrollado una serie de informes de inteligencia que permiten a los clientes entender el estado actualizado del ecosistema de ciberamenazas a nivel mundial, para poder anticiparse a ataques dirigidos y mejorar sus defensas de manera proactiva.

4. Equipo de Gestión de Clientes y Estrategia:

Este equipo gestiona las relaciones con los clientes y asegura que *DaaS* se alinee con los objetivos estratégicos de cada organización. Además, son responsables de la coordinación de proyectos y la personalización del servicio para que se adapte a las necesidades específicas de cada cliente.

- Los gestores de cuentas y estrategas tienen una profunda comprensión del sector industrial y de las necesidades de seguridad de sus clientes. Son expertos en la personalización de servicios y en la creación de estrategias a largo plazo que optimicen la inversión en ciberseguridad.
- Gracias a su enfoque personalizado, este equipo ha logrado establecer relaciones de confianza con clientes clave en sectores como la automoción, la energía y la manufactura, contribuyendo a la expansión de Aristeo en el mercado.

Telefónica Tech ha logrado implementar y gestionar con éxito soluciones de ciberseguridad en diversos sectores industriales.

Algunos de los logros más destacados incluyen:

1. Protección de Infraestructuras Críticas:

DaaS ha sido implementado en fábricas e instalaciones críticas, donde ha detectado y neutralizado amenazas avanzadas que podrían haber causado graves interrupciones o daños. Un ejemplo destacado es la protección de la planta de HORSE en Valladolid, donde se ha permitido identificar vulnerabilidades tempranas y anticipar potenciales amenazas.

2. Innovación en Ciberseguridad Industrial:

El equipo continúa mejorando y expandiendo las capacidades de Aristeo, incorporando nuevas funciones de análisis predictivo y capacidades de inteligencia artificial, lo que asegura que la solución siga siendo una de las más avanzadas en el mercado.

3. Desarrollo de Nuevas Capacidades:

El equipo continúa mejorando y expandiendo las capacidades de *DaaS* con otras soluciones de mercado, incorporando nuevas funciones de análisis predictivo y capacidades de inteligencia artificial, posicionándonos con soluciones adaptables, flexibles y escalables, y una de las más avanzadas en el mercado.

MODELO COMERCIAL

El servicio *DaaS* se ofrece bajo un modelo de servicio gestionado, que incluye consultoría, instalación, mantenimiento y soporte continuo. Se adapta a las necesidades del cliente con opciones de integración flexibles, permitiendo que las empresas accedan a una solución de ciberinteligencia avanzada sin la necesidad de realizar grandes inversiones en infraestructura, estructurados en varias fases:

1. Evaluación Inicial:

- **Diagnóstico y Evaluación de Riesgos:** Realización de auditorías y evaluaciones de ciberseguridad para identificar activos críticos, vulnerabilidades y riesgos asociados.

2. Planificación y Diseño:

- **Diseño de Arquitectura Segura:** Desarrollo de un plan detallado de arquitectura de red segura, incluyendo segregación y segmentación de redes, así como implementación de medidas de protección perimetral.

MODELO COMERCIAL

› **Modelo de adquisición:**

- On-premise:
  - Adquisición de equipo físico con la licencia incluida.
  - Despliegue en máquina virtual del cliente, licenciamiento de software
- Despliegue cloud:
  - Servicios desplegados en infraestructura Telefónica.

3. Implementación:

› **Despliegue de Tecnologías:** Instalación y configuración de firewalls de próxima generación (NGFW), sistemas de autenticación y monitorización de seguridad para garantizar la protección continua de los entornos industriales.

› **Despliegue de campañas** y señuelos (decoys).

4. Gestión y monitorización continuas:

› **Servicios Gestionados:** Provisión de servicios continuos de monitorización y gestión de seguridad, incluyendo análisis de tráfico, detección de amenazas y respuesta a incidentes mediante un Security Operations Center (SOC) especializado.

5. Formación y Concienciación:

› **Capacitación:** Formación de personal interno en prácticas de ciberseguridad industrial, asegurando que los empleados sean capaces de identificar y responder adecuadamente a las amenazas.

6. Optimización y Mejora Continua:

› **Revisión y Actualización:** Evaluación periódica de la postura de seguridad y actualización de las políticas y tecnologías implementadas para adaptarse a nuevos riesgos y desafíos.

Contáctanos para empezar la transformación digital de tu organización.