

Aristeo

Red OT de captura y análisis predictivo de amenazas de Telefónica Tech, generador de inteligencia con valor diferencial.

OT & IoT

Threat Intelligence

IA

Deception



SOBRE LA SOLUCIÓN

Gracias al despliegue de sus señuelos con hardware industrial real, Aristeo es capaz de capturar amenazas que otros sistemas no identifican. En este caso, un empleado de un cliente se conectó a un sitio web que fue bloqueado por los sistemas de seguridad de la empresa. El cliente nos solicitó más información. Aristeo había detectado que esa máquina llevaba un mes atacando a sus señuelos.

Ninguno de los motores de Threat Intelligence más importantes del mundo había identificado esta amenaza.

LO QUE OPINAN SOBRE ARISTEO

“Cualquier amenaza puede detener tu negocio. Es importante tener soluciones que refuercen los sistemas de seguridad con información de calidad. Aristeo encuentra amenazas rápido y nos ayuda a protegernos.”

OBJETIVOS DEL PROYECTO

Desde el DOC de Telefónica Tech requeríamos una **fuentes fiable y de calidad para reforzar los sistemas de seguridad perimetral** de sus clientes con **información de amenazas de entornos industriales**. Se aprovechó la capacidad de Aristeo como fuente de información para cargar los indicadores de ataque y de compromiso en estos sistemas perimetrales, identificando una amenaza nueva que aparentaba ser un servicio legítimo.

RESULTADOS

- Aristeo captura amenazas sobre sistemas reales y no sobre sistemas virtualizados. Esto hace que el análisis sobre estas genere inteligencia de calidad sobre amenazas industriales. **El atacante es incapaz de distinguir que no está en un entorno real, por lo que despliega sus mejores trucos, mientras Aristeo lo aprende todo de ellos.** Este valor es absolutamente diferencial para un equipo de seguridad encargado de tantos clientes, como el DOC de Telefónica Tech.
- Además, Aristeo consigue, de media, **identificar amenazas** (el 16% de todas las detectadas) **entre 8 y 12 días antes** que los principales motores de inteligencia del mercado.