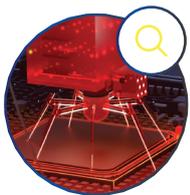


¿Qué es ADA?

ADA es una plataforma de **análisis avanzado de malware** capaz de conseguir un análisis **en profundidad**, similar al resultante de un proceso de investigación en detalle. Con ella, el CCN-CERT pone a disposición de la comunidad una interfaz simple, sencilla y con resultados interpretables dentro de un proceso complejo de investigación.



Propiedades

ADA utiliza varios entornos de **sandbox** que se combinan con múltiples soluciones de antivirus para realizar **análisis estáticos** y **dinámicos** de muestras. La solución soporta cualquier formato: binarios x86 y x64, documentos de ofimática, scripts en diferentes lenguajes, paquetes de captura de tráfico (pcap) o incluso mensajes de correo electrónico. Asimismo, permite gestionar y acceder a los resultados de todas las tecnologías que integra desde un único interfaz.



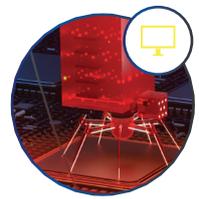
Análisis dinámico multi-tecnología:

envío de la muestra a diversas tecnologías de análisis dinámico gracias a la integración con la solución MARTA, soportando multitud de formatos de archivo.



Análisis estático en profundidad:

integración con la solución MARÍA para realizar un análisis utilizando diferentes motores de antivirus sobre todas las muestras enviadas.



Funcionalidades

ADA es la evolución natural de las capacidades de análisis dinámico (MARTA) y las capacidades de análisis estático (MARÍA). La solución incluye numerosas funcionalidades, siendo las más destacadas las siguientes:



Histórico de análisis: permite poder consultar todos los resultados generados, además de la evolución y seguimiento de las amenazas.

Diseñada desde el frontal, pensando en la mejor experiencia de usuario en busca de una usabilidad sencilla que permita a cualquier usuario realizar **investigaciones con una formación básica.**

Interfaz unificado desde el que se podrá controlar, gestionar y acceder a los resultados de todas las tecnologías de análisis que integra.

Entorno de análisis aislado de forma que su información no pueda ser consultada por el resto de usuarios y organismos.

Generación de informes automáticos personalizables, de tipo ejecutivo y técnico.

Interacción completa con el proceso de análisis, permitiendo interactuar de forma sencilla con la máquina virtual de análisis sin abandonar la plataforma.

