

Análisis avanzado de ficheros

¿Qué es Marta?

Marta es una plataforma avanzada de multi-sandboxing dedicada al análisis automatizado de múltiples tipos de ficheros que pudieran tener un comportamiento malicioso. A partir de la información que Marta recoge, un analista podrá determinar qué tipo de funcionalidad y qué implicaciones tiene para su organización.



¿Por qué usar Marta?

Permite **almacenar, clasificar y tener disponible** todas las muestras de código dañino en un entorno controlado.

La **información está disponible** para ser analizada en cualquier momento bajo las condiciones que se deseen.

Cuenta con **múltiples sistemas de sandboxing** para analizar y delimitar el comportamiento de cada muestra de código.

Reduce los tiempos del análisis y reporte que, en caso de incidente, pueden ser críticos.

Propiedades

Solicitud de análisis bajo demanda con configuraciones ad-hoc.

Análisis estático.

Análisis dinámico.

Informes automáticos personalizados con los resultados de los análisis.

Clasificación por etiquetas.

Motor de análisis y categorización basado en reglas IOC y YARA.

Editor de nuevas reglas de detección.

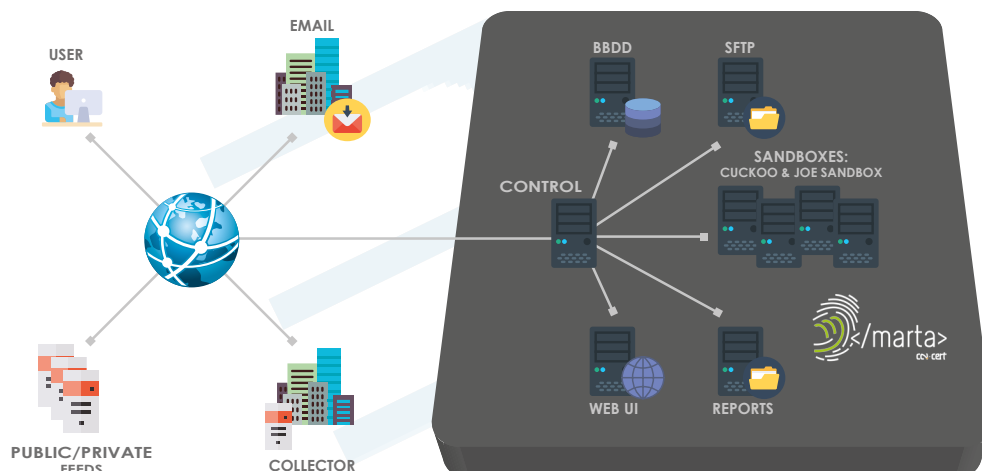
¿Cómo funciona?

Marta almacena las evidencias de cada uno de los análisis para su posterior procesamiento, revisión o presentación y permite retroalimentarse analizando objetos extraídos de otros análisis. Al subir un fichero, dichos análisis se realizan en tres fases:

Análisis estático: en primer lugar se pasa una serie de scripts estáticos sobre el fichero (el código dañino no se ejecuta mientras se analiza). Así se obtiene información específica como tipo de fichero (exe, dll, docx, pdf, Android, etc), hashes (MD5, SHA1, SSDEEP, etc), información de cabecera o tabla de directorios, entre otras.

Análisis dinámico: la funcionalidad más relevante de Marta consiste en arrancar una máquina virtual infectada con el código dañino, siendo un entorno controlado lo más parecido al sistema de una víctima. De este modo, se comprueba sus características, acciones y comportamientos.

Post-Análisis: una vez finalizado el análisis dinámico, se lanzan los procesos que analizan los patrones IOC y YARA que permiten clasificar los análisis por su comportamiento y actividad.



Integración con otras soluciones CCN-CERT



Intercambio de información de
ciberamenazas



Solución Multiantivirus



Detección y análisis avanzado
de ficheros



marta@ccn-cert.cni.es

www.ccn-cert.cni.es

