Government

Justice +
Law enforcement

Financial institutions

DATAENFORCE

DAEDALUS©

PLATAFORMA PARA EL ANÁLISIS AVANZADO DE SOFTWARE MALICIOSO

Capacidad de procesamiento multidimensional, multivector y de alta concurrencia

Análisis multidimensional y multivectorial

COMPUTADORES

Análisis de muestras nativas diseñadas para sistemas Microsoft Windows, Apple Mac OSX y plataformas Linux

INTERNET

Análisis de direcciones Web para la identificación de ataques por suplantación (*Phishing*) o páginas con programación maliciosa

DISPOSITIVOS

Análisis de ejecutables y de comportamiento en tiempo real sistemas Google Android y Apple iOS

CATÁLOGOS
Ficha técnica con los elementos mas sobresalientes de las muestras analizadas. Permite tener un inventario sumarial que puede ser compartido con interesados.

CLASIFICACIÓN
Generación de perfiles preliminares de autor(es) del código malicioso, ayudando a determinar el grado de habilidad y recursos técnicos empleados asi como posible región de origen.

CASOS
Creación de expedientes que permiten realizar un seguimiento ordenado a las investigaciones desde el inicio hasta su conclusión.

CORRELACIÓN
Búsqueda automática de relaciones entre muestras analizadas, apoyando al investigador en el hallazgo de posibles vinculaciones entre casos.

www.dataenforce.com

info@dataenforce.com

DAEDALUS©

DAEDALUS© es una plataforma capaz de realizar avanzados y múltiples tipos de análisis de software malicioso en modo estático, dinámico y en modo nativo sobre el equipo o dispositivo.

ANÁLISIS DISPONIBLES

Análisis estático.
Disección de la muestra sin realizar ningún tipo de ejecución de código. El análisis es inerte y busca la identificación y catalogación de la posible amenaza por firmas y patrones de código.

Análisis en tiempo real.
Dispositivos Android y iOS pueden conectarse a la plataforma para un examen en vivo y en tiempo real del comportamiento del equipo para la búsqueda de software malicioso.

Análisis dinámico.
Gracias a este proceso de ejecución controlada de la muestra en un ambiente simulado, es posible obtener información como características y capacidades, técnicas de evasión, propagación, transmisión y recepción de datos.

MULTIUSUARIO
Pueden ser creados múltiples operadores con zonas aisladas y políticas de uso para el análisis de muestras. El administrador tiene visibilidad completa en la plataforma.

COOPERACIÓN
Módulo para la recepción de muestras desde fuentes externas, sin comprometer el acceso directo al sistema.

REPORTES
Generación de reportes detallados de diferentes clases dependiendo de la necesidad: ejecutivo, técnico, judicial. Posibilidad del usuario de personalizar el formato del reporte.

ESTADÍSTICAS
Provee las tendencias de las muestras procesadas en el tiempo, ayudando a la predicción y a la toma de decisiones basadas en su interpretación.

DATAENFORCE

info@dataenforce.com