



Entelgy
GO FOR IT

IMA

El objeto del proyecto **IMA** es una novedosa solución multi-cliente de Ciber-Seguridad que permite la gestión inteligente, rápida y eficaz de incidentes de seguridad. Está integrada con distintos sistemas SIEM para la obtención de eventos y alarmas. Así mismo está integrada con distintos sistemas de ticketing para un seguimiento integral del ciclo de vida de los incidentes de seguridad reportados a los clientes..

Beneficios:

- *Detección de amenazas*
- *Colaboración centralizada*
- *Automatización de tareas*

Los objetivos de I+D son:

- ▶ Soporte Multiplataforma (SIEM y ticketing).
- ▶ Operador virtual.
- ▶ Gestor de creación e incidentes.
- ▶ Motor blacklist

Los objetivos del proyecto son:

- ▶ Permitir la integración con las principales herramientas SIEM del mercado (Qradart, SIEMonster (ELK Stack) y AlienVault).
- ▶ Incorporar un operador virtual que permita la asistencia al análisis de los eventos recibidos.
- ▶ Permitir la integración con los principales sistemas de ticketing (Remedy, RTIR...).
- ▶ Tener claro el nivel de riesgo que corre una organización en base a los eventos de seguridad registrados.
- ▶ Permitir la gestión de excepciones de forma paralela a las herramientas SIEM.
- ▶ Permitir el envío y gestión automatizada de las notificaciones.
- ▶ Integrarse con diferentes listas negras públicas y privadas unificando la inteligencia de forma centralizada y automatizada.

IMA (IDI – 2016-0017)



Centro para el Desarrollo
Tecnológico Industrial



GOBIERNO
DE ESPAÑA

MINISTERIO
DE ECONOMÍA
Y COMPETITIVIDAD



UNIÓN EUROPEA
FONDO
EUROPEO DE
DESARROLLO
REGIONAL

"Una manera de hacer Europa"



entelgy.com

©Entelgy | Todos los derechos reservados