ITI INVESTIGATE TO INNOVATE

OPOSSUM

SECURIZACIÓN DE APLICACIONES BASADA EN TÉCNICAS BIG DATA E INTELIGENCIA ARTIFICIAL

EL PROYECTO

OPOSSUM se centra en el análisis, diseño y desarrollo de herramientas de ciberseguridad para la securización de aplicaciones utilizando técnicas de Big Data e Inteligencia Artificial.

El número de incidencias de ciberseguridad no ha hecho más que crecer durante los últimos años, afectando a millones de usuarios en el mundo. Este espectacular aumento de las incidencias de ciberseguridad se sustenta a través de una industria del cibercrimen que se ha dado cuenta de los enormes beneficios que reporta su actividad.

La sociedad digital no puede sostenerse si ésta no es segura. Las soluciones serán seguras, o no serán, ya que las empresas dejarán de utilizar aquel software que no cumpla con unos criterios de seguridad elevados.

Es por ello que el proyecto **OPOSSUM**, tiene como objetivo principal la **investigación y desarrollo de herramientas software que aumenten los estándares de seguridad de las aplicaciones,** utilizando para ello técnicas basadas en **Big Data e Inteligencia Artificial,** así como el estudio, despliegue y extensión de un sistema que sirva como unidad de recogida, transformación y enriquecimiento de métricas y datos para el posterior entrenamiento de modelos de **Inteligencia Artificial,** así como punto de entrada para los ingenieros de seguridad, en el cual se pueda consultar información útil en tiempo real que les permita reducir sus tiempos de respuesta ante incidentes.

OBJETIVOS

- **Análisis y selección de telemetrías y orígenes de datos, tanto internos a los sistemas TIC, como externos a través de técnicas OSINT,** para aplicar posteriormente **un EDA que nos permita seleccionar las técnicas de Inteligencia Artificial más adecuadas** para mejorar la detección de amenazas.
- Creación de un **prototipo de Web Application Firewall** (WAF) y **API Gateway.**
- Creación de **modelos de Inteligencia Artificial** para la detección de amenazas de ciberseguridad.

Estos nuevos desarrollos serán compatibles con las técnicas de desarrollo software actuales y permitirán a las **empresas del sector TIC de la Comunidad Valenciana,** por un lado, desplegar aplicaciones con **altos estándares de seguridad** y, por otro lado, **reducir sus tiempos de respuesta** frente a incidencias, permitiendo al mismo tiempo **actuaciones de seguridad autónomas y automáticas.** De esta manera, se **aumentará el valor añadido de los servicios y productos software ofertados** por las empresas que hagan uso de estas tecnologías, lo que les permitirá **aumentar su competitividad con respecto a su competencia, reduciendo al mismo tiempo la inversión, tanto económica como de conocimientos,** necesaria para securizar sus productos.

A partir de estas herramientas, el conjunto de las empresas en general (no sólo las TIC) podrán desplegar sus productos de una forma más segura, utilizando **tecnologías punteras en Inteligencia Artificial,** donde el Instituto Tecnológico de Informática ha desarrollado una gran experiencia en los últimos años, sin necesidad de conocer los complicados detalles técnicos que requieren el uso de estas técnicas. El acceso a este tipo de herramientas y servicios es fundamental para las empresas de la Comunidad Valenciana, ya que **el ambiente digital se está haciendo cada vez más hostil, y las brechas de seguridad, así como sus consecuencias legales, suponen un riesgo para la continuidad de negocio.**

Es importante destacar que **las inversiones necesarias actualmente para disponer de estas herramientas son muy elevadas,** algo que dificulta su adopción y uso por las empresas en general, especialmente las PYMEs. Por una parte, es necesario aprovisionar un **clúster de computación** con un elevado número de CPUs, memoria RAM y almacenamiento. A este coste, ya de por sí elevado, hay que añadir los trabajos de instalación y configuración de herramientas Big Data. Estos trabajos son **muy complejos,** requieren de **personal especializado, y su coste no puede ser asumido por la mayoría de las empresas de la Comunidad Valenciana.** Además, hay que añadir el coste de los profesionales técnicos, como arquitectos de software, científicos de datos, expertos en ciberseguridad, etc. necesarios para procesar esa información, sintetizarla y empaquetarla en un modelo de Inteligencia Artificial de detección de amenazas. Es por eso por lo que **las empresas que utilicen estas herramientas se verán beneficiadas del conocimiento, habilidades e infraestructuras utilizadas en este proyecto, mejorando su competitividad.**

Este proyecto ha sido financiado por **IVACE / FEDER**
Nº de expediente: IMDEEA/2020/64
Financiación: 214.759,34€

GENERALITAT VALENCIANA · IVACE INSTITUTO VALENCIANO DE COMPETITIVIDAD EMPRESARIAL · Unión Europea · Fondo Europeo de Desarrollo Regional "Una manera de hacer Europa"