UNIVERSITAT POLITÈCNICA DE VALÈNCIA

DEPARTAMENTO DE COMUNICACIONES

Threat Hunting basado en técnicas de Inteligencia Artificial

Autor:
Mario Aragonés Lozano

Director:
Dr. Manuel Esteve Domingo
Dr. Israel Pérez Llopis

Resumen

Tanto la cantidad como la tipología de los ciberataques va en aumento día a día y la tendencia es que continúen creciendo de forma exponencial en los próximos años. Estos ciberataques afectan a todos los dispositivos, independientemente de si su propietario es un particular (o ciudadano), una empresa privada, un organismo público o una infraestructura crítica y los objetivos de estos ataques son muchos, desde la solicitud de una recompensa económica hasta el robo de información clasificada. Dado este hecho, los individuos, las organizaciones y las corporaciones deben tomar medidas para prevenirlos y, en caso de que en algún momento los reciban, analizarlos y reaccionar en caso de que fuese necesario.

Cabe destacar que aquellos ataques que buscan ser más eficientes, son capaces de ocultarse un largo tiempo, incluso después de sus acciones iniciales, por lo que la detección del ataque y el saneamiento del sistema puede llegar a dificultarse a niveles insospechados o, incluso, no tenerse la certeza de que se ha hecho correctamente.

Para prevenir, analizar y reaccionar ante los ataques más complejos, normalmente conocidos como ataques de día cero, las organizaciones deben tener ciberespecialistas conocidos como cazadores de amenazas. Éstos son los encargados de monitorizar los dispositivos de la empresa con el objetivo de detectar comportamientos extraños, analizarlos y concluir si se está produciendo un ataque o no con la finalidad de tomar decisiones al respecto.

Estos ciberespecialistas deben analizar grandes cantidades de datos (mayormente benignos, repetitivos y con patrones predecibles) en cortos periodos de tiempo para detectar ciberataques, con la sobrecarga cognitiva asociada. El uso de inteligencia artificial, específicamente aprendizaje automático y aprendizaje profundo, puede impactar de forma notable en el análisis en tiempo real de dichos datos. Además, si los ciberespecialistas son capaces de visualizar los datos de forma correcta, éstos pueden ser capaces de obtener una mayor consciencia situacional del problema al que se enfrentan.

Este trabajo busca definir una arquitectura que contemple desde la adquisición de datos hasta la visualización de los mismos, pasando por el procesamiento de éstos y la generación de hipótesis acerca de lo que está sucediendo en la infraestructura monitorizada. Además, en la definición de la misma se deberá tener en consideración aspectos tan importantes como la disponibilidad, integridad y confidencialidad de los datos, así como la alta disponibilidad de los distintos componentes que conformen ésta. Una vez definida la arquitectura, este trabajo busca validarla haciendo uso de un prototipo que la implemente en su totalidad. Durante esta fase de evaluación, es importante que quede demostrada la versatilidad de la arquitectura propuesta para trabajar en diferentes casos de uso, así como su capacidad para adaptarse a los cambios que se producen en las distintas técnicas de aprendizaje automático y aprendizaje profundo.