Metodología de selección de modelos de analítica de datos para la detección de APT con enfoque en la confiabilidad y optimización

Methodology for selecting data analytics models for APT detection with a focus on reliability and optimization

Adrián Hernández Rivas[a]*, Julia Patricia Sánchez Solís[a]
[a]Doctorado en Ciencias de la Ingeniería Avanzada, Departamento de Ingeniería Eléctrica y Computación, Instituto de Ingeniería y Tecnología, Universidad Autónoma de Ciudad Juárez, México
*Autor de correspondencia. Correo electrónico: al240311@alumnos.uacj.mx

No. de resumen
6CP23-5

Evento
6.º Coloquio de Posgrados del IIT

Tema
Cómputo aplicado

Fecha de la presentación
Noviembre 23, 2023

Formato
Cartel

Presentador
Adrián Hernández Rivas

Estatus
Estudio en curso

Resumen

El desarrollo de una metodología de selección de modelos de analítica de datos para la detección de amenazas persistentes avanzadas (APT, por sus siglas en inglés), requiere la inclusión de técnicas orientadas a la selección de modelos efectivos que den respuesta a situaciones dentro de entornos dinámicos donde se presentan dichas APT. Además, es necesario explorar y seleccionar métodos para agregar interpretabilidad que permita mejorar la confiabilidad de las predicciones. Como parte de la confianza agregada a los modelos, se debe planificar la protección de estos de manera que permitan hacer frente a los ataques de *adversarial machine learning*. La investigación aborda preguntas cruciales sobre mejoras, avances metodológicos y contribuciones a la ciberseguridad. Además, la hipótesis propuesta sugiere que la implementación de este enfoque mejorará la eficiencia en la detección de amenazas. El incremento en la sofisticación de amenazas cibernéticas y la carencia de combinación de técnicas, como la optimización de modelos, la interpretabilidad y la protección de los modelos para una mayor confiabilidad, subrayan la necesidad de desarrollar enfoques que integren estas dimensiones. Este tipo de estrategias contribuirá al progreso de las técnicas de analítica de datos en la detección de APT, atendiendo a la evolución constante de los desafíos en ciberseguridad.

Palabras clave: APT; detección; metodología; confiabilidad; optimización.

Abstract

The development of a methodology for selecting data analytics models for advanced persistent threat (APT) detection requires the inclusion of techniques designed for the selection of effective models capable of handling situations within dynamic environments where these APTs manifest. Furthermore, it is crucial to explore and select methods to introduce interpretability that enhances the reliability of predictions. As an element of the confidence instilled in the models, careful planning for their protection is essential to counter adversarial machine learning attacks. The research delves into critical inquiries concerning improvements, methodological advancements, and contributions to cybersecurity. Furthermore, the proposed hypothesis posits that implementing this approach will enhance the efficiency of threat detection. The escalating sophistication of cyber threats, coupled with the lack of integration of techniques such as model optimization, interpretability, and model protection for heightened reliability, underscores the imperative to develop approaches that seamlessly integrate these dimensions. Such strategic endeavors will undoubtedly contribute

to the progression of data analytics techniques in APT detection, effectively addressing the ongoing evolution of challenges in the realm of cybersecurity.

Keywords: APT; methodology; reliability; optimization; detection.

Entidad legal responsable del estudio
Universidad Autónoma de Ciudad Juárez

Financiamiento
Consejo Nacional de Humanidades, Ciencias y Tecnologías (CONAHCYT).

Conflictos de interés
Los autores manifiestan que no tienen conflicto de interés.