Diseño de sistema de prevención deintrusiones (IPS) mediante herramientas de Inteligencia Artificial

Problema a resolver

Actualmente,la seguridad en las redes es un tema crítico debido a los ataques recurrentes de los ciberdelincuentes. Según reporte del fabricante Crowdstrike, más del 50% de las intrusiones se ubica en la región del norte de América (incluyendo México). Ninguna organización se encuentra exenta de un ataque, sin importar su giro.Hoy en día, las organizaciones carecen de herramientas efectivas para detectar las vulnerabilidades y prevenir los intentos maliciosos de acceso a sus sistemas informáticos. Por otra parte, los ciberdelincuentes tienen disponibles herramientas más sofisticadas y de acceso inmediato, por lo que la función de los responsables de la seguridad se complica cada día más. La tarea de seguridad representa un reto en entidades públicas por el hecho de trabajar con datos personales y sensibles, ya que son sujetos a la normatividad aplicable. Por lo que surge la necesidad de contar con un esquema de seguridad que proporcione un grado de certidumbre a las partes interesadas.
Con el desarrollo de la inteligencia artificial, se abre una gama de oportunidades para desarrollar soluciones de seguridad que permiten el monitoreo y prevención de intrusiones en una red.
Si bien en el mercado existen alternativas de solución, estas son en algunos casos muy caras y no están al alcance de instituciones públicas. De igual forma, las herramientas comerciales no se adecuan de manera natural a la operación de la red existente, por lo que se requiere un periodo largo para adaptarlas al entorno local.

Por lo que este trabajo tiene por objetivo diseñar un sistema de detección de intrusionesmediante herramientas de inteligencia artificial que sea robusto, flexible, económico y capaz de satisfacer los requerimientos de protección de la red.

Productos académicos comprometidos:

1 artículo de conferencia internacional y 1 artículo en revista indizada

Detalles sobre 1 Estancia del estudiante:

Estancia corta en el Centro de Operaciones de Seguridad (SOC) del CUDI.

Detalles sobre 1 Conferencia del estudiante:

Congreso Internacional de Ciberseguridad, (CIBERTIC 2026)

Referencias

- *Crowdstrike (2024) Global Threat Report*
- UNESCO (2022)*, Recomendación sobre la ética de la inteligencia artificial.*
- Maasaoui, Z.; Merzouki, M.; Battou, A.; Lbath, A. A Scalable Framework for Real-Time Network Security Traffic Analysis and Attack Detection Using Machine and Deep Learning. *Platforms* **2025**, *3*, 7. https://doi.org/10.3390/platforms3020007.
- *M. Kamruzzaman, M. K. Bhuyan, R. Hasan, S. F. Farabi, S. I. Nilima and M. A. Hossain, "Exploring the Landscape: A Systematic Review of Artificial Intelligence Techniques in Cybersecurity," 2024 International Conference on Communications, Computing, Cybersecurity, and Informatics (CCCI), Beijing, China, 2024, pp. 01-06, doi: 10.1109/CCCI61916.2024.10736474.*

- *A. P. Olatunji, E. Alozie, H. Olagunju and F. Udensi, "A Systematic Review of the Role of Artificial Intelligence in Cybersecurity,"* 2024 IEEE 5th International Conference on Electro-Computing Technologies for Humanity (NIGERCON)*, Ado Ekiti, Nigeria, 2024, pp. 1-6, doi: 10.1109/NIGERCON62786.2024.10926941*.
- *2024. MACHINE LEARNING FOR CYBERSECURITY FOR DETECTING AND PREVENTING CYBER ATTACKS. Machine Intelligence Research. 18, 1 (Aug. 2024), 672–689.*
- Erskine, S.K. Real-Time Large-Scale Intrusion Detection and Prevention System (IDPS) CICIoT Dataset Traffic Assessment Based on Deep Learning. *Appl. Syst. Innov.* **2025**, *8*, 52. https://doi.org/10.3390/asi8020052