Ciberseguridad con Inteligencia Artificial

Dr. Vitali Herrera Semenets – CENATAV, La Habana, Cuba (vherrera@cenatav.co.cu)
MSc. Felipe Antonio Trujillo Fernández – IBERO, Ciudad de México, México (felipe.trujillo@ibero.mx)
MSc. Joshua Ismael Haase Hernández – IBERO, Ciudad de México, México (joshua.haase@ibero.mx)
Dr. Lázaro Bustio Martínez – IBERO, Ciudad de México, México (lazaro.bustio@ibero.mx)
Coordinación de Ciencia de Datos - Departamento de Estudios en Ingeniería para la Innovación – Ibero
Primavera 2024

1. Descripción del Taller

En un contexto de creciente interconexión digital, la Ciberseguridad se erige como un imperativo ineludible para salvaguardar la integridad de sistemas y datos ante amenazas cada vez más sofisticadas. En este escenario, el Aprendizaje Automatizado emerge como un recurso fundamental para fortalecer las defensas y mitigar riesgos. El taller "Ciberseguridad con Inteligencia Artificial" ofrecerá una aproximación práctica y accesible a este campo, explorando los fundamentos y aplicaciones de Inteligencia Artificial en la detección, prevención y respuesta ante ataques informáticos. A través de una combinación de instrucción teórica y ejercicios prácticos, los participantes adquirirán competencias para enfrentar desafíos en seguridad cibernética con eficacia y destreza técnica. Este taller está enfocado a participantes que dominen los fundamentos de programación en Python, aunque no es requisito obligatorio.

2. Objetivo general

El taller "Ciberseguridad con Inteligencia Artificial" tiene como objetivo proporcionar a los participantes una comprensión práctica inicial de la aplicación de técnicas de Inteligencia Artificial en la resolución de desafíos de ciberseguridad. A lo largo del taller, los participantes explorarán cómo utilizar algoritmos específicos para detectar amenazas, prevenir ataques y fortalecer la seguridad de sistemas y redes informáticas. A través de ejemplos prácticos y ejercicios guiados, se espera que los participantes adquieran habilidades para implementar soluciones innovadoras que protejan la integridad y confidencialidad de la información en entornos digitales. El éxito del taller se medirá por la capacidad de los participantes para aplicar los conceptos y técnicas aprendidas en situaciones reales de Ciberseguridad.

Al finalizar el taller, los participantes serán capaces de:

- Comprender los conceptos fundamentales del.
- Identificar y analizar posibles amenazas y vulnerabilidades en sistemas y redes informáticas utilizando técnicas de Inteligencia Artificial.
- Aplicar algoritmos de Aprendizaje Automatizado para detectar y prevenir ataques.
- Adquirir habilidades básicas para abordar desafíos específicos de seguridad cibernética utilizando herramientas y metodologías de Aprendizaje Automatizado.

3. Requisitos

El taller "Ciberseguridad con Inteligencia Artificial" ha sido diseñado para que pueda ser cursado por personas que no cuenten con una formación especial en el área, aunque se recomienda que los participantes tengan nociones de:

- Programación
- Lenguaje Python
- Ciencia de Datos
- Ciberseguridad

4. Temario

El taller consta de 5 temas, los cuales se detallan a continuación:

1) Introducción al Aprendizaje Automatizado en Ciberseguridad.
   a) Importancia y beneficios del uso de técnicas de Aprendizaje Automatizado en la protección de sistemas informáticos.
   b) Conceptos básicos de Aprendizaje Automatizado y sus aplicaciones en Ciberseguridad.
      i) Obtención, limpieza y preparación de datos.
      ii) Exploración de datos y estadísticas.
      iii) Aprendizaje supervisado y no supervisado.
         (1) Agrupamiento de datos.
         (2) Clasificación de datos.
         (3) Evaluación de clasificadores.
   c) Actividad práctica: Evaluación de contraseñas. A partir de una base de datos de contraseñas que han sido filtradas:
      i) Obtener los agrupamientos de contraseñas.
      ii) Entender la naturaleza de los grupos.
      iii) Entrenar un modelo de clasificación que permita etiquetar la fortaleza de una contraseña.
2) Detección de ataques de phishing con Aprendizaje Automatizado.

a) Procesamiento de Lenguaje Natural.
b) Phishing. Tipos de ataques de phishing.
c) Actividad práctica: Detección de ataques de phishing mediante Procesamiento de Lenguaje Natural.

3) Detección de anomalías y comportamientos maliciosos.
   a) Identificación de anomalías y comportamientos maliciosos.
   b) Técnicas de detección de anomalías.
   c) Actividad práctica: Ejemplo de detección de anomalías.
4) Detección de malware en APKs.
   a) Representación de APKs.
   b) Tendencias actuales en la detección de malware en APKs.
   c) Actividad práctica: Detección de malware en APKs.
5) Conclusiones
   a) Recapitulación de los temas tratados y discusión sobre su relevancia en el panorama actual de ciberseguridad.
   b) Recursos adicionales y recomendaciones para seguir profundizando en los temas después del taller.

5. Organización del Taller

El taller está concebido para que tenga un alto contenido práctico, y será impartido en 4 sesiones de 3 horas cada una, donde la primera hora de cada sesión será de revisión de la teoría y las siguientes dos horas serán de trabajo práctico guiado. Se recomienda que las actividades se realicen en equipos de hasta tres miembros. Esto lleva a que el número máximo de participantes idóneo para este curso sea de 30 estudiantes y el número mínimo sea de 15, para la creación de 10 y 5 equipos de trabajo respectivamente.

6. Cronograma de actividades

Los temas propuestos se abordarán de acuerdo con el siguiente cronograma:

No	Fecha	Actividad	Comentarios
1	09/04	Introducción al Aprendizaje Automatizado en Ciberseguridad.	
2	11/04	Detección de ataques de phishing con Aprendizaje Automatizado.	
3	16/04	Detección de anomalías y comportamientos maliciosos.	
4	18/04	Detección de fraudes Conclusiones	

Al finalizar el taller se entregará una constancia de completado a los participantes que hayan asistido al 75% de las sesiones.

7. Cuestiones técnicas

El taller ha sido diseñado para participantes que (aunque es recomendable que cuenten con los requisitos básicos solicitados) no necesariamente sean expertos en el área. Por tal motivo, las herramientas que se usarán serán gratis y de código abierto, implicando el menor esfuerzo por parte de los participantes para poder usarlas. En esta dirección, se usarán las siguientes herramientas:

- Python 3.8+
- Google Colab
- Visual Studio Code
- PyCharm

El taller cuenta con un sitio web, el cual puede ser visitado y que contiene todo el material que se usará. La dirección es: https://sites.google.com/view/cswia/inicio.

Aunque el taller se llevará a cabo en un salón equipado con computadoras, se recomienda que los participantes traigan sus propios equipos. Antes del evento, se proporcionará información sobre el software que los participantes deben tener instalado en sus equipos personales, así como la posibilidad de instalar software adicional durante el taller. La página web del taller servirá como el medio principal para publicar información oficial y relevante, por lo que se recomienda a los participantes que estén atentos a dicha página para recibir actualizaciones importantes.

8. Bibliografía

- Halder, S., & Ozdemir, S. (2018). Hands-On Machine Learning for Cybersecurity. Packt Publishing. ISBN: 9781788992282.
- PacktPublishing. (2024, 21 de febrero). Hands-on Machine Learning for Cyber Security. Recuperado el 21 de febrero de 2024, de https://github.com/PacktPublishing/Hands-on-Machine-Learning-for-Cyber-Security
- Gupta, B. B., & Sheng, Q. Z. (2019). Machine Learning for Computer and Cyber Security: Principle, Algorithms, and Practices. CRC Press.
- Chio, C., & Freeman, D. (2018). Machine Learning and Security. O'Reilly Media, Inc. ISBN: 9781491979907.
- Bertino, E., Bhardwaj, S., Cicala, F., Gong, S., Karim, I., Katsis, C., ... Mahgoub, A. Y. (Series Eds.). (2020). Machine Learning Techniques for Cybersecurity. Synthesis Lectures on Information Security, Privacy, and Trust. Springer Cham. https://doi.org/10.1007/978-3-031-28259-1

- Malik, P., Nautiyal, L., & Ram, M. (Eds.). (Year). Machine Learning for Cyber Security (Volume 15). De Gruyter Series on the Applications of Mathematics in Engineering and Information Sciences. https://doi.org/10.1515/9783110766745.
- Dua, S., & Du, X. (2011). Data Mining and Machine Learning in Cybersecurity. Auerbach Publications.
- Tsukerman, E. (2019). Machine Learning for Cybersecurity Cookbook. Packt Publishing.
- SANS Institute. (2024, 21 de febrero). Applied Data Science and Machine Learning. Recuperado de https://www.sans.org/cyber-security-courses/applied-data-science-machine-learning/