UNIVERSIDAD ABIERTA PARA ADULTOS

UAPA

DIRECCION ACADEMICA DE POSGRADO

MAESTRÍA EN CIBERSEGURIDAD

PROPUESTA DE IMPLEMENTACIÓN DE SISTEMAS DE MACHINE LEARNING E INTELIGENCIA ARTIFICIAL PARA PROTEGER EL PERÍMETRO DE LA RED LAN DE TELEVIADUCTO, S.R.L. EN EL PERIODO ENERO - MARZO 2022.

INFORME FINAL DE INVESTIGACIÓN PRESENTADO COMO REQUISITO PARA OPTAR POR EL TÍTULO DE MAGISTER EN CIBERSEGURIDAD

POR:

SAMUEL YNOA

EDGAR GUTIÉRREZ

ASESOR(A):

CARMEN LUISA AYBAR DE NICASIO

SANTIAGO DE LOS CABALLEROS

REPÚBLICA DOMINICANA

DICIEMBRE 2022

TABLA DE CONTENIDO

Capítulo III: Marco Metodológico

Capítulo IV: Descripción De La Propuesta

RESUMEN

Este proyecto tiene como objetivo principal implementar un sistema basado en inteligencia artificial utilizando Machine Learning para la protección de la red LAN de la empresa Televiaducto S.R.L., esto será llevado a cabo mediante un análisis de vulnerabilidades, entrenamiento del algoritmo, plan de implementación y validación de la solución. Para esta investigación se utilizará el método cualitativo, en el que se estarán aplicando cuestionarios al equipo de TI para hacer análisis de la infraestructura, se harán escaneos de tráfico para la recogida de datos de la red, se utilizarán algoritmos y librerías para el entrenamiento del programa y se presentarán las conclusiones del estudio.

La investigación se divide en 5 partes:

El problema de investigación: En esta parte de la investigación, se realiza el planteamiento del problema, se le da al lector una pincelada de lo que se estará trabajando, los objetivos que se tendrán para el proyecto, así como la justificación y limitaciones, este capítulo dará una idea acabada sobre lo que se estará tratando de resolver.

Marco Teórico: Este es el capítulo para los entusiastas tecnológicos, aquí se detallarán todos los conceptos que serán utilizados como parte del proyecto, dígase, tecnologías a utilizar, métodos, algoritmos, técnicas, entre otros conceptos, para así luego de conocer la problemática, también conocer a fondo las herramientas de solución.

Marco Metodológico: Como su nombre lo indica, este capítulo destila la parte metodológica de la investigación, es decir, tipo de investigación, instrumentos que se utilizarán para apoyar y la población a trabajar.

Descripción de la propuesta: Este capítulo muestra la contextualización del proyecto, o sea nos da lugar, hora, fecha de cómo y dónde se estará realizando la investigación, los objetivos del mismo y su alcance.

Validación de la propuesta: Para esta parte con la ayuda de un experto en el área se estará buscando validar si la solución propuesta es factible, lograble e implementable.

CONCLUSIONES

Las empresas necesitan protección ante las ciberamenzas, y no siempre cuentan con las herramientas necesarias para asegurar esta protección. Como se ha podido observar, además de las realidades antes planteadas, también existe un sinnúmero de herramientas que buscan salvaguardar la seguridad de las instituciones.

Para brindar la protección necesaria se debe manejar cualquier implementación como una investigación que utiliza el método científico en donde se observa lo que está implementado en la actualidad, se identifican las posibles amenazas o puntos a mejorar, se hace una hipótesis o propuesta, pruebas para probar el funcionamiento del sistema, para luego finalizar dando soporte a la herramienta, o más bien, traduciendo esto a tecnología se puede afrontar el proyecto analizando cada una de las capas del modelo OSI.

Repasando el procedimiento seguido podemos nombrar las etapas del proyecto en primer lugar como un análisis de la red donde se determinó cual es el tráfico habitual para una empresa como la es Televiaducto S.R.L, para luego de contar con esta data, se entrena un algoritmo machine learning para aprender que ese tráfico habitual es el que se debe permitir y con una base de datos de fallos existentes en redes de telecomunicaciones con característica escalable se le muestra cual es el tráfico que no debería permitir.

La posibilidad de contar con un sistema que maneje las amenazas de una forma mucho más eficiente de lo que lo hacen las soluciones actuales, representa una grandísima oportunidad para que las diferentes instituciones puedan alcanzar sus objetivos en torno a la seguridad de la red.

Finalmente es necesario mencionar que un sistema de IA que proteja una red LAN no pretende ni debe ser la única herramienta o modo de protección con el que cuente una institución. Sin embargo, es una herramienta que será de muchísima ayuda para el personal de TI o el personal encargado de la seguridad, pues les ofrecerá una visión más amplia del espectro que pretenden proteger, así como también como hacerlo mejor.

REFERENCIAS BIBLIOGRÁFICAS

Abdulghani, S. (2009). Design and Implementation of a Network Security Model for Cooperative Network. International Arab Journal of e-Technology, 1, 26–36.

Abeliuk, A., & Gutiérrez, C. (2021). Historia y evolución de la inteligencia artificial. Revista Bits de Ciencia, 21, 14-21 pp.

Adam, P. (2014). Implementación de un esquema robótico para la optimización de comportamientos en ambientes no estructurados utilizando algoritmos bioinspirados.

Alós, J. G. (1989). Modelos de evaluación de programas educativos. 43–78.

ALPAYDIN, E. (2021). Machine Learning (Revised and Updated Edition). MIT. https://books.google.es/books?hl=es&lr=&id=2nQJEAAAQBAJ&oi=fnd&pg=PR7&dq=machine+learning&ots=fH36R5SBkq&sig=IKYszuovqybCyl9Yv3auWDIaCBs#v=onepage&q=machine%20learning&f=false

Alpaydın, E. (2021). Machine Learning: Revised and Updated Edition.

Arribas, M. C. M. (s/f). Diseño y validación de cuestionarios. 5(2004).

Boden, M. A. (2017). Inteligencia Artificial. Turner.

Brendan Chartor. (2021, mayo 20). Ransomware Attacks Are Spiking. Is Your Company Prepared? https://hbr.org/2021/05/ransomware-attacks-are-spiking-is-your-company-prepared

Bustamante, G., Rivera, J., & Salinas, S. (2015). La ciberdefensa como parte de la agenda de integración sudamericana 1. Línea Sur, 100–116.

Cardenas, Juan Manuel. (s/f). EL MACHINE LEARNING A TRAVÉS DE LOS TIEMPOS, Y LOS APORTES A LA HUMANIDAD. https://repository.unilibre.edu.co/handle/10901/17289

Centeno, F. J. U. (s/f). CIBERATAQUES, la mayor amenaza actual. 09.

Cervantes, S. (2021). Propuesta de implementación de un sistema de gestión customer centric basado en inteligencia artificial.

Cervera, D. R. C. (s/f). MÉTODOS Y TÉCNICAS DE INVESTIGACIÓN EN RELACIONES INTERNACIONALES.

Clifford Stoll. (1989). The Cuckoo's Egg: Tracking a Spy Through the Maze of Computer Espionage. http://bayrampasamakina.com/tr/pdf_stoll_4_1.pdf

Dobrev, D. (2012). A Definition of Artificial Intelligence (arXiv:1210.1568). arXiv. http://arxiv.org/abs/1210.1568

Espinal, N. (2022). Sistema detector de intrusos usando Machine Learning y orientada en la IIoT.

Estepa, M. D. T. (s/f). Clasificación de Ataques a una Red de Telecomunicación con Deep Learning. 189.

Ethem Alpaydin. (s/f). Machine Learning, revised and updated edition. https://books.google.es/books?hl=es&lr=&id=2nQJEAAAQBAJ&oi=fnd&pg=PR7&dq=machine+learning&ots=fH34T2YFpn&sig=2p6Rkfe4y4z4N4WZcthd2PBD8yU#v=onepage&q=machine%20learning&f=false

Evaluación de la probabilidad-impacto—Praxis Framework. (s/f). Recuperado el 23 de diciembre de 2022, de https://www.praxisframework.org/es/library/probability-impact-assessment

Hernández Sampieri, R., Fernández Collado, C., & Baptista Lucio, P. (2010). Metodología de la investigación. Quinta Edición. ISBN 9786071502919.

IDS: Historia, concepto y terminología - OSTEC Blog. (2015, septiembre 1). OSTEC | Segurança digital de resultados. https://ostec.blog/es/seguridad-perimetral/ids-conceptos/

Introduction to Grafana | Grafana documentation. (s/f). Grafana Labs. Recuperado el 19 de diciembre de 2022, de https://grafana.com/docs/grafana/latest/introduction/

J Mena. (s/f). Data Mining your website. Digital Press.

José Díaz Ramirez. (2021, junio). Aprendizaje Automático y Aprendizaje Profundo. 29, 2.

Kazemitabar, H., Ahmed, S., Nisar, K., Said, A. B., & Hasbullah, H. B. (2010). A comprehensive review on VoIP over Wireless LAN networks. 2, 16.

Kok, J. N. (s/f). Artificial Intelligence: Definition, Trends, Techniques and Cases. ARTIFICIAL INTELLIGENCE, 5.

Liu, L., Wang, P., Lin, J., & Liu, L. (2021). Intrusion Detection of Imbalanced Network Traffic Based on Machine Learning and Deep Learning. IEEE Access, 9, 7550–7563. https://doi.org/10.1109/ACCESS.2020.3048198

Manrrique, E. (2020, Abril). Machine Learning: Análisis de lenguajes de programación y herramientas para desarrollo. 15.

McCarthy, J. (s/f). WHAT IS ARTIFICIAL INTELLIGENCE? 15.

MISP Community. (s/f). MISP Threat Sharing. https://www.circl.lu/doc/misp/book.pdf

Munera, L. E. (1991). Inteligencia artificial y sistemas expertos. Inteligencia artificial y sistemas expertos.

Neural Designer. (2022). https://www.neuraldesigner.com/

Ocampo, D. S. (2021, febrero 9). El estudio de caso. Investigalia. https://investigaliacr.com/investigacion/el-estudio-de-caso/

Pita Fernández, S., & Pértegas Díaz, S. (2002). Investigación cuantitativa y cualitativa. Cad aten primaria, 9(1), 76–78.

Quesada, D., & María, J. (s/f). Aprendizaje supervisado para la detección de amenazas web mediante clasificación basada en árboles de decisión: Aplicación de técnicas de machine learning a la ciberseguridad.

Renear, A. H., Sacchi, S., & Wickett, K. M. (2010). Definitions of dataset in the scientific and technical literature. Proceedings of the American Society for Information Science and Technology, 47(1), 1–4.

Ribas, A. M., Moreno, A., & Universitat Politècnica de Catalunya. (s/f). Aprendizaje automático. UPC, S.L., Edicions.

Roca, X. S. (s/f). Ciberseguridad, contrainteligencia y Operaciones encubiertas en el programa nuclear de Irán: De la neutralización selectiva de objetivos al “cuerpo Ciberiraní*. 42.

Rouhiainen, L. (2020). Inteligencia artificial: 101 cosas que debes saber hoy sobre nuestro futuro (3ª ed). Alienta.

Salcedo, M. (2018). IMPLEMENTAR CHATBOT BASADO EN INTELIGENCIA ARTIFICIAL PARA LA GESTIÓN DE REQUERIMIENTOS E INCIDENTES EN UNA EMPRESA DE SEGUROS.

Snider, K. L. G., Shandler, R., Zandani, S., & Canetti, D. (2021). Cyberattacks, cyber threats, and attitudes toward cybersecurity policies. Journal of Cybersecurity, 7(1), tyab019. https://doi.org/10.1093/cybsec/tyab019

Strelkova, O. (2017). Three types of artificial intelligence.

Taipe, J. S. V., & Huanga, D. F. V. (s/f). OPTIMIZACIO´ N DE UNA RED LAN DESPUE´ S DE UN ATAQUE DDOS DETECTADO CON TE´ CNICAS DE INTELIGENCIA ARTIFICIAL.

Thing, V. L. L. (2017). IEEE 802.11 Network Anomaly Detection and Attack Classification: A Deep Learning Approach. 2017 IEEE Wireless Communications and Networking Conference (WCNC), 1–6. https://doi.org/10.1109/WCNC.2017.7925567

TIPOS DE INVESTIGACION. (s/f).

Vargas Adrian & Victor Santiago. (2021). SISTEMA DE DETECCIÓN DE INTRUSOS BASADO EN MACHINE LEARNING. https://repositorio.uta.edu.ec/jspui/bitstream/123456789/34028/1/t1911mtel.pdf

Villamizar, G., & Donoso, R. (2013). Definiciones y teorías sobre inteligencia. Revisión histórica. Psicogente, 16(30), Art. 30. http://revistas.unisimon.edu.co/index.php/psicogente/article/view/1927

William Santana Mendez. (2010). Gestión de procesos de negocio. Enfoque conceptual orientado a los sistemas de información empresariales. https://www.redalyc.org/pdf/1814/181421569002.pdf

Yoo, S. J. (2018). Study on Improving Endpoint Security Technology. Convergence Security Journal, 18(3), 19–25.

Yuchong Li, Qinghui Liu,. (s/f). A comprehensive review study of cyber-attacks and cyber security; Emerging trends and recent developments. https://www.sciencedirect.com/science/article/pii/S2352484721007289#b7

(S/f-a). https://books.google.es/books?hl=es&lr=&id=2nQJEAAAQBAJ&oi=fnd&pg=PR7&dq=machine+learning&ots=fH34T2YFpn&sig=2p6Rkfe4y4z4N4WZcthd2PBD8yU#v=onepage&q=machine%20learning&f=false

(S/f-b). Recuperado el 23 de diciembre de 2022, de https://www.broadberry.com/markets/artificial-intelligence-ai-servers

INSTRUCCIONES PARA LA CONSULTA DEL TEXTO COMPLETO:

Para consultar a texto completo esta tesis solicite en este formulario (https://forms.gle/vx5iLzv1pAMyN3d59 como hipervínculo) o dirigirse a la Sala Digital del Departamento de Biblioteca de la Universidad Abierta para Adultos, UAPA.

Dirección

Biblioteca de la Sede – Santiago

Av. Hispanoamericana #100, Thomén, Santiago, República Dominicana

809-724-0266, ext. 276; biblioteca@uapa.edu.do

Biblioteca del Recinto Santo Domingo Oriental

Calle 5-W Esq. 2W, Urbanización Lucerna, Santo Domingo Este, República Dominicana.

Tel.: 809-483-0100, ext. 245. biblioteca@uapa.edu.do

Biblioteca del Recinto Cibao Oriental, Nagua

Calle 1ra, Urb Alfonso Alonso, Nagua, República Dominicana.

809-584-7021, ext. 230. biblioteca@uapa.edu.do