Innovación, Ingeniería & Desarrollo

Artículo recibido: 16 de abril de 2016
Artículo aceptado: 25 de noviembre de 2016

Análisis del aporte del aprendizaje de máquinas a la seguridad de la información

Analysis of the contribution of machine learning to information security

Análise da contribuição do aprendizado de máquina para a segurança da informação

Juan Fernando Correa Wachter[1], Cesar Felipe Henao Villas[2], Federico Henao Villa[3], David Alberto García Arango.[4]

Resumen

Todo dispositivo informático tiene sus propios registros de seguridad. Al juntar miles de dispositivos que intervienen en las comunicaciones de computadores personales, bases de datos, servidores web, dispositivos de red, firewalls, etc., se genera un gran volumen de registros con información interesante desde el punto de vista de seguridad, aunque imposible de revisar por un ser humano. Ahí es donde hace sentido contar con herramientas automatizadas con cierta inteligencia capaces de realizar análisis y detectar patrones maliciosos que puedan afectar la confidencialidad, integridad y disponibilidad de la información.

Entre estas herramientas surge la Inteligencia Artificial y el Machine Learning las cuales están siendo incluidas por fabricantes en los productos de seguridad de última generación. El objetivo de este artículo es explicar en qué consiste el Machine Learning, su historia, componentes y su contribución como apoyo a la seguridad de la información.

Palabras clave: Ciencia de datos, Machine Learning, Inteligencia Artificial, Deep Learning, Tecnología, Seguridad.

Abstract

Every computer device has its own security records. By gathering thousands of devices that intervene in the communications of personal computers, databases, web servers, network devices, firewalls, etc., a large volume of records is generated with interesting information from the point of view of security, although it is impossible to review by a human being. Because of this, it makes sense to have automated tools with a certain intelligence capable of analyzing and detecting malicious patterns that may affect the confidentiality, integrity and availability of information.

Among these tools arises Artificial Intelligence and Machine Learning which are being included by manufacturers in the latest generation security products. The objective of this article is to explain what Machine Learning consists of, its history, components and its contribution as support for information security.

Keywords: Artificial Intelligence, Data Science, Deep Learning, Machine Learning, Technology, Security.

Negocios Internacionales. Corporación Universitaria Americana, jcorrea@coruniamericana.edu.co
Ingeniero de Sistemas. Corporación Universitaria Americana, dagarcia@coruniamericana.edu.co
Ingeniero de Sistemas. Corporación Universitaria Americana, , fhenao@americana.edu.co
Licenciado en Matemáticas y Física. Corporación Universitaria Americana, dagarcia@coruniamericana.edu.co

Resumo

Cada dispositivo de computação tem seus próprios registros de segurança. Ao reunir milhares de dispositivos que intervêm nas comunicações de computadores pessoais, bases de dados, servidores web, dispositivos de rede, firewalls, etc., é gerado um grande volume de registos com informações interessantes do ponto de vista da segurança, embora impossíveis de rever. por um ser humano. É aí que faz sentido ter ferramentas automatizadas com alguma inteligência capazes de realizar análises e detectar padrões maliciosos que podem afetar a confidencialidade, integridade e disponibilidade das informações.

Entre essas ferramentas estão a Inteligência Artificial e o Aprendizado de Máquina, que estão sendo incluídos pelos fabricantes na última geração de produtos de segurança. O objetivo deste artigo é explicar em que consiste o Aprendizado de Máquina, sua história, componentes e sua contribuição para apoiar a segurança da informação.

Palavras-chave: Ciência de Dados, Aprendizado de Máquina, Inteligência Artificial, Aprendizado Profundo, Tecnologia, Segurança.

INTRODUCCIÓN

El volumen de datos digitales por el uso de las tecnologías en las organizaciones ha aumentado considerablemente y con ello el riesgo de ser más vulnerables a ataques por parte de delincuentes informáticos. Las organizaciones consideran cada vez más la información como un activo valioso que se debe proteger utilizando a su vez la mejor tecnología a menor costo. Los delincuentes informáticos aumentan así mismo su nivel de sofisticación, por lo tanto, la industria está avanzando para contrarrestar la amenaza digital.

Dentro de las herramientas de última generación que permiten contrarrestar las diferentes amenazas por parte de los delincuentes informáticos, está la Inteligencia Artificial y Machine Learning. El sistema de aprendizaje automático o Machine Learning, posee la habilidad de analizar la información mediante algoritmos matemáticos para predecir el comportamiento de sus datos y arrojar resultados sorprendentes similares a los del humano. La experiencia ha mostrado como día a día, surgen nuevas modalidades de ataques hacia los sistemas informáticos, buscando alterar el normal desarrollo de las actividades informáticas, y afectar la continuidad del negocio.

Gracias a las herramientas de análisis y de detección de intrusos y de eventos de seguridad, mediante la intervención humana y por medio de la analítica de datos, se puede dar tratamiento de manera proactiva a muchos de los casos evidenciados en las organizaciones que cuentan con herramientas de última generación para estos análisis.

MATERIALES Y MÉTODOS

A partir de la información obtenida en esta investigación, este artículo busca explicar cómo Machine-Learning, una de las ramas de la Inteligencia Artificial (IA), apoya a la seguridad de la información en las organizaciones por medio de tecnologías y/o herramientas usadas en el análisis de las alertas y eventos de seguridad y tomar acciones en contrarrestar ataques hacia la red de información por los intrusos o atacantes informáticos.

La IA se basa en clasificar un grupo de patrones o comportamientos conocido como conjunto de pruebas en dos o más clases de categorías. Esto es posible al calcular las categorías del conjunto en prueba comparándolo con un conjunto de entrenamiento previo.

Importante es entonces, aclarar algunos conceptos básicos del tema para comprender su desarrollo, anotando algunas breves definiciones tales como inteligencia Artificial (IA), Machine Learning (ML), su historia y su clasificación. A medida que se desarrolla el tema se ampliaran los conceptos que motivan a la realización de este artículo de investigación.

Resultados

Casi todas las organizaciones públicas o privadas, al igual que las personas, dependen de alguna manera de la tecnología de la información como una herramienta esencial para lograr sus objetivos de negocio o para poder desarrollar actividades en su vida cotidiana; al mismo tiempo, todos tienen que enfrentarse con una amplia gama de amenazas y vulnerabilidades asociadas a los entornos informáticos de hoy [1.]

Los riesgos de la información están presentes desde que existan las amenazas y las vulnerabilidades, en este caso, las amenazas pueden ser de origen interno o externo en las organizaciones y son la probabilidad de ocurrencia de cualquier tipo de evento o acción que puede producir un daño en la información, por otra parte las vulnerabilidades son debilidades en la tecnología o en los procesos relacionados con la información, y como tal, se consideran características propias de los sistemas de información o de la infraestructura que la contiene [1]

Tipos de amenazas:

- Las organizaciones están expuestas a amenazas de diferentes orígenes, las cuales se pueden agrupar en las siguientes categorías.
- Factores Humanos (accidentales, errores)
- Fallas en los sistemas de procesamiento de información
- Desastres naturales y Actos maliciosos o malintencionados
- Las amenazas informáticas que afectan a la organización

Son muchas las amenazas a las que están expuestas las organizaciones a nivel informática, las más comunes son:

- Virus informáticos o código malicioso
- Uso no autorizado de Sistemas Informáticos
- Robo de Información
- Fraudes basados en el uso de computadores
- Suplantación de identidad
- Denegación de Servicios (DoS)
- Ataques de Fuerza Bruta
- Alteración de la Información
- Divulgación de Información
- Desastres Naturales
- Sabotaje, vandalismo
- Spyware (Programas espías): Código malicioso cuyo principal objetivo es recoger información sobre las actividades de un usuario en un computador.
- Troyanos, virus y gusanos: Son programas de código malicioso, que de diferentes maneras se alojan en los computadores con el propósito de permitir el acceso no autorizado a un atacante, o permitir el control de forma remota de los sistemas.
- El virus, adicionalmente, tiene como objetivo principal ser destructivo, dañando la información de la máquina, o generando el consumo de recursos de manera incontrolada para bloquear o negar servicios.
- Phishing: Es un ataque del tipo ingeniería social, cuyo objetivo principal es obtener de manera fraudulenta datos confidenciales de un usuario, especialmente financieros, aprovechando la confianza que éste tiene en los servicios tecnológicos, el desconocimiento de la forma en que operan y la oferta de servicios en algunos casos con pobres medidas de seguridad.
- Spam: Recibo de mensajes no solicitados, principalmente por correo electrónico, cuyo propósito es difundir grandes cantidades de mensajes comerciales o propagandísticos.
- Botnets (Redes de robots): Son máquinas infectadas y controladas remotamente, que se comportan como "zombis", quedando incorporadas a redes distribuidas de computadores llamados robot, los cuales envían de forma masiva mensajes de correo "spam" o código malicioso, con el objetivo de atacar otros sistemas.
- Trashing: Un método cuyo nombre hace referencia al manejo de la basura. No es una técnica relacionada directamente con los sistemas de información, pues los atacantes se valen de otra forma de ingeniería social y para ello, el mecanismo utilizado, es la búsqueda en las canecas de la basura o en los sitios donde se desechan papeles y documentos de extractos bancarios, facturas, recibos, borradores de documentos.

Ransomware: Un Ransomware es un tipo de programa dañino que restringe el acceso a determinadas partes o archivos del sistema infectado, y pide un rescate a cambio de quitar esta restricción [1]

Dado que la organización está expuesta a tantas amenazas y vulnerabilidades, se puede afirmar que la fórmula para prevenir ser víctima de un ataque informático hay que combinar elementos como educación, proactividad, políticas adecuadas y tecnología que permita realizar análisis proactivo.

A partir de las amenazas y vulnerabilidades descritas anteriormente en las organizaciones se está recurriendo al Machine-Learning, una de las ramas de la Inteligencia Artificial (IA), como apoyo para el análisis y toma de decisiones de eventos de seguridad . En este capítulo se da una descripción y clasificación de un abanico de algoritmos de Machine-Learnig organizados según su propósito.

Hay muchos algoritmos disponibles y se presentan dos formas de categorizar los algoritmos. El primero es una agrupación de algoritmos por el estilo de aprendizaje. El segundo es una agrupación de algoritmos por similitud en la forma o función [2]. Ambos enfoques son útiles, pero se centrará en la agrupación de algoritmos por similitud y se hará un recorrido por una variedad de diferentes tipos de algoritmos.

Hay diferentes maneras en que un algoritmo puede modelar un problema en función de su interacción con la experiencia o el entorno. Es popular en los libros de texto de aprendizaje automático e inteligencia artificial para considerar primero los estilos de aprendizaje que puede adoptar un algoritmo.

Solo hay unos pocos estilos de aprendizaje o modelos de aprendizaje principales que un algoritmo puede tener y se analizaran algunos ejemplos y tipos de problemas que se adaptan a ellos [3]. Esta taxonomía o forma de organizar algoritmos de aprendizaje automático es útil porque lo obliga a pensar en los roles de los datos de entrada y el proceso de preparación del modelo y seleccionar uno que sea el más adecuado para su problema para obtener el mejor resultado [4].

Tres estilos de aprendizaje diferentes en algoritmos de aprendizaje automático son:

1. Aprendizaje supervisado

En los algoritmos ML de aprendizaje supervisados los datos de ingreso se denominan datos de entrenamiento y tienen una etiqueta o resultado conocido, como spam/no-spam o un precio de acciones a la vez.

Un modelo se prepara a través de un proceso de capacitación en el que se requiere hacer predicciones y se corrige cuando esas predicciones son erróneas. El proceso de capacitación continua hasta que el modelo alcanza el nivel deseado de precisión en los datos de capacitación

Ejemplos de problemas son la clasificación y la regresión. Ejemplos de algoritmos de aprendizaje supervisado incluyen Regresión logística y la Red neuronal de propagación hacia atrás.

2. Aprendizaje no supervisado

En Algoritmos de aprendizaje no supervisados los datos de entrada no están etiquetados y no tienen un resultado conocido.
Se prepara un modelo deduciendo las estructuras presentes en los datos de entrada. Esto puede ser para extraer reglas generales. Puede ser a través de un proceso matemático para reducir sistemáticamente la redundancia, o puede ser la organización de datos por similitud .
Ejemplos de problemas son el agrupamiento, la reducción de la dimensionalidad y el aprendizaje de reglas de asociación. Los algoritmos de ejemplo incluyen: el algoritmo de Apriori y k-Means.

3. Aprendizaje semi-supervisado

En los algoritmos de aprendizaje semi-supervisados los datos de ingreso son una mezcla de ejemplos etiquetados y no etiquetados. Hay un problema de predicción deseado, pero el modelo debe aprender las estructuras para organizar los datos y hacer predicciones [5].

Ejemplos de problemas son la clasificación y la regresión. Los algoritmos de ejemplo son extensiones de otros métodos flexibles que hacen suposiciones acerca de cómo modelar los datos sin etiqueta.

Al procesar datos para modelar decisiones de negocios, lo más habitual es que utilice métodos de aprendizaje supervisados y no supervisados [4].

Un tema que está muy en auge son los métodos de aprendizaje semi-supervisados en áreas como la clasificación de imágenes donde hay grandes conjuntos de datos con muy pocos ejemplos etiquetados.

Algoritmos agrupados por similitud

Los algoritmos a menudo se agrupan por similitud en términos de su función. Por ejemplo, los métodos basados en árboles y los métodos inspirados en redes neuronales. [5]

Este es un método de agrupación puede presentar problemas debido a que hay algoritmos que podrían encajar fácilmente en múltiples categorías, como el Learning Vector Quantization, que es tanto un método inspirado en redes neuronales como un método basado en instancias. También hay categorías que tienen el mismo nombre que describen el problema y la clase de algoritmo, como Regresión y Agrupación en clúster. Se manejará este problema seleccionando el grupo que se ajuste más [5].

En esta sección, se enumera muchos de los algoritmos populares de aprendizaje automático más representativos. Se debe tener en cuenta que existe una fuerte tendencia hacia los algoritmos utilizados para la clasificación y la regresión, los dos problemas de aprendizaje automático supervisado más frecuentes que se encuentran [4].

Algoritmos de regresión: La regresión se ocupa de modelar la relación entre variables que se refina iterativamente utilizando una medida de error en las predicciones hechas por el modelo.

Los métodos de regresión son un caballo de batalla de las estadísticas y se han incorporado al aprendizaje estadístico de máquinas. Esto puede ser confuso porque se puede usar la regresión para referirse a la clase de problema y la clase de algoritmo. Realmente, la regresión es un proceso.

Los algoritmos de regresión más populares son:

- Regresión de mínimos cuadrados ordinarios (OLSR)
- Regresión lineal
- Regresión logística
- Regresión escalonada
- Splines de regresión adaptativa multivariante (MARS)

Suavizado de gráfico de dispersión estimado localmente (LOESS). Algoritmos basados en instancias: El modelo de aprendizaje basado en instancias es un problema de decisión con instancias o ejemplos de datos de entrenamiento que se consideran importantes o necesarios para el modelo.

Estos métodos generalmente construyen una base de datos de datos de ejemplo y comparan datos nuevos con la base de datos utilizando una medida de similitud para encontrar la mejor coincidencia y hacer una predicción. Por esta razón, los métodos basados en instancias también se denominan métodos ganadores para todos y aprendizaje basado en la memoria. Se enfoca en la representación de las instancias almacenadas y las medidas de similitud utilizadas entre las instancias [4].

Los algoritmos basados en instancias más populares son:

- k-vecino más cercano (kNN)
- Aprendizaje de cuantificación vectorial (LVQ)
- Mapa de autoorganización (SOM)
- Aprendizaje ponderado localmente (LWL)

Algoritmos de regularización: Son una extensión hecha a otro método (generalmente, métodos de regresión) que penaliza los modelos en función de su complejidad, favoreciendo modelos más simples que también son mejores para generalizar. Se ha enumerado los algoritmos de regularización por separado porque son modificaciones populares, potentes y generalmente simples hechas a otros métodos .

Los algoritmos de regularización más populares son:

- Regresión Ridge
- Operador de selección y contracción mínima absoluta (LASSO)
- Red elástica
- Regresión de ángulo menor (LARS)

Algoritmos del árbol de decisión: Los métodos del árbol de decisión construyen un modelo de decisiones basadas en los valores reales de los atributos en los datos.

Las decisiones se bifurcan en estructuras de árboles hasta que se toma una decisión de predicción para un registro determinado. Los árboles de decisión están entrenados en datos para problemas de clasificación y regresión. Los árboles de decisión son a menudo rápidos y precisos, y un gran favorito en el aprendizaje automático .

Los algoritmos de árbol de decisión más populares son:

- Árbol de Clasificación y Regresión (CART)
- Dichotomiser Iterativo 3 (ID3)
- C4.5 y C5.0 (diferentes versiones de un enfoque poderoso)
- Detección automática de interacción Chi-cuadrado (CHAID)
- Tocón de decisión
- M5
- Árboles de decisión condicional

Algoritmos Bayesianos: Los métodos Bayesianos son aquellos que aplican explícitamente el Teorema de Bayes para problemas como la clasificación y la regresión [2].

Los algoritmos bayesianos más populares son:

- Ingenuo bayes
- Gaussian Naive Bayes
- Multinomial Naive Bayes
- Estimadores de una dependencia media (AODE)
- Red de Creencia Bayesiana (BBN)
- Red Bayesiana (BN)

Algoritmos de agrupamiento: también conocidos como Algoritmos de Clustering, al igual que la regresión, describe la clase de problema y la clase de métodos.

Los métodos de agrupación en clúster suelen organizarse según los enfoques de modelado, como los basados en centroides y jerárquicos. Todos los métodos están relacionados con el uso de las estructuras inherentes en los datos para organizar mejor los datos en grupos de máxima similitud [6].

Los algoritmos de agrupamiento más populares son:

- k-medios
- k-medianos
- Maximización de la expectativa (EM)
- Agrupación jerárquica

Algoritmos de aprendizaje de reglas de asociación: Los métodos de aprendizaje de reglas de asociación extraen las reglas que mejor explican las relaciones observadas entre las variables en los datos [5]

Estas reglas pueden descubrir asociaciones importantes y comercialmente útiles en grandes conjuntos de datos multidimensionales que pueden ser explotados por una organización [5].

Los algoritmos de aprendizaje de reglas de asociación más populares son:

- Algoritmo de A-Priori
- Algoritmo Eclat

Algoritmos de redes neuronales artificiales: Las redes neuronales artificiales son modelos inspirados en la estructura y/o función de las redes neuronales biológicas.

Son una clase de coincidencia de patrones que se usan comúnmente para problemas de regresión y clasificación, pero en realidad son un subcampo enorme que consta de cientos de algoritmos y variaciones para todo tipo de problemas. Se debe tener en cuenta se ha separado Deep Learning de las redes neuronales debido al enorme crecimiento y la popularidad en este campo. Aquí se presentan los métodos clásicos .

Los algoritmos de redes neuronales artificiales más populares son:

- Perceptron
- Propagación hacia atrás
- Red Hopfield
- Red de función de base radial (RBFN)

Algoritmos de aprendizaje profundo: estos algoritmos son una actualización moderna de las redes neuronales artificiales que explotan la computación barata y abundante [5].

Se preocupan por construir redes neuronales mucho más grandes y complejas y, como se comentó anteriormente, muchos métodos se ocupan de problemas de aprendizaje semi-supervisados donde los conjuntos de datos grandes contienen muy poca información etiquetada [3]

Los algoritmos de aprendizaje profundo más populares son:

- Máquina de boltzmann profundo (DBM)
- Redes de creencias profundas (DBN)
- Red neuronal convolucional (CNN)
- Auto-codificadores apilados

Algoritmos de reducción de dimensionalidad: Como los métodos de agrupamiento, la reducción de dimensionalidad busca y explota la estructura inherente en los datos, pero en este caso de una manera no supervisada u ordenada para resumir o describir datos usando menos información.

Esto puede ser útil para visualizar datos dimensionales o para simplificar datos que luego pueden usarse en un método de aprendizaje supervisado. Muchos de estos métodos pueden adaptarse para su uso en clasificación y regresión [4]

- Análisis de componentes principales (PCA)
- Regresión del componente principal (PCR)
- Regresión de mínimos cuadrados parciales (PLSR)
- Mapeo de Sammon
- Escalamiento Multidimensional (MDS)
- Búsqueda de proyección
- Análisis Lineal Discriminante (LDA)
- Análisis Discriminante de Mezcla (MDA)
- Análisis cuadrático discriminante (QDA)
- Análisis Discriminante Flexible (FDA)

Algoritmos de conjunto: Los métodos de ensamblaje son modelos compuestos de múltiples modelos más débiles que se entrenan de manera independiente y cuyas predicciones se combinan de alguna manera para hacer la predicción general [5].

Se dedica mucho esfuerzo en qué tipos de aprendizajes débiles se combinan y las formas en que se pueden combinar. Esta es una clase muy poderosa de técnicas y como tal es muy popular .

- Impulso
- Agregación Bootstrap (Bagging)
- AdaBoost
- Generalización apilada (mezcla)
- Máquinas de mejora de gradiente (GBM)
- Árboles de regresión potenciados por degradado (GBRT)
- Bosque aleatorio

Otros algoritmos: Muchos algoritmos no fueron cubiertos. Por ejemplo, los algoritmos de tareas especializadas en el proceso de aprendizaje automático, como: Algoritmos de selección de características, Evaluación de la precisión del algoritmo, Medidas de desempeño, Inteligencia computacional (algoritmos evolutivos, etc.), Visión por Computadora (CV), Procesamiento del lenguaje natural (PNL), Sistemas de recomendación, Aprendizaje reforzado, Modelos gráficos, entre otros.

Discusión

Con la evolución en el desarrollo del software y de los modelos matemáticos y estadísticos predictivos de la actualidad, Machine Learning, dio un gran salto desde sus orígenes cuando en los años 50s, Arthur Samuel, pionero en el campo de los juegos informáticos, escribió el primer programa de aprendizaje informático.

En los años 60s, con la creación del algoritmo conocido como "nearest neighbor" las computadoras comenzaron a utilizar un reconocimiento de patrones muy básico, éste logró trazar un mapa de una ruta para vendedores ambulantes.

En la década de los 90s, el Machine Learning ganó popularidad gracias a la intersección de la informática y la estadística que dio lugar a enfoques probabilísticos en la IA. En este periodo se comenzó a utilizar esta tecnología en áreas comerciales para la minería de datos, software adaptable y aplicaciones web, aprendizaje de texto y aprendizaje de idiomas.

En el año 2000, Geoffrey Hinton acuña el término "Deep Learning", con el que se explican nuevas arquitecturas de Redes Neuronales profundas que permiten a las computadoras "ver" y distinguir objetos y texto en imágenes y videos.

Por su parte IBM. En su tecnología Watson de Inteligencia Artificial es capaz de responder a preguntas formuladas en lenguaje natural y logra vencer a un humano en el juego de Jeopardy.

Google. El científico informático Jeff Dean, empleado de Google, y Andrew Ng, de la Universidad de Stanford, lideran el proyecto GoogleBrain, que desarrolla una red neuronal profunda que puede aprender a descubrir y categorizar objetos de forma similar a como lo hace un gato.

Facebook. Desarrollan DeepFace, un algoritmo de software que puede reconocer o verificar individuos en fotos al mismo nivel que los humanos.

Amazon. Esta empresa crea su propia plataforma de machine Learning.

Microsoft. Logran que Kinect pueda rastrear 20 funciones humanas a una velocidad de 30 veces por segundo, lo que permite a las personas interactuar con la computadora a través de movimientos y gestos.

Y después de 3000 Investigaciones sobre Inteligencia artificial, respaldados por Stephen Hawking, Elon Musk y Steven Wosniak, se plantea el peligro en que se podría convertir el desarrollo de la inteligencia artificial en las practicas militares sin intervención del humano.

En el 2016 el algoritmo de inteligencia artificial de Google vence a un jugador profesional en el juego de mesa chino Go.

Con el aumento de Ciberataques y la evolución de malware forzó al empleo del aprendizaje automático en la prevención y detección de malware y las acciones para mitigarlo.

Para el análisis y aprendizaje automático en Machine Learning, es necesario lo siguiente:

- Base grande de Datos y de calidad (mientras más datos, mayor precisión)
- Tiempo para aprender y entrenarse, investigación, desarrollo de algoritmos e interpretación de los datos, que ayudan a las empresas a analizar mejor las amenazas y ser más efectivas a la hora de detener los incidentes de seguridad.

Cuando se habla de la seguridad de la información, debe entenderse de la seguridad defensiva y seguridad ofensiva, y en esta línea Machine Learning está presente en el campo de la seguridad para solucionar los problemas que se presentan en este sentido.

ML permite el análisis de lo que es normal y no es normal, para predecir el comportamiento de los datos mediante el entrenamiento continuo respecto a las acciones de un atacante.

En cuando a la seguridad defensiva, habitualmente ML se utiliza en control de acceso, autenticación, autorización, identificación y perfilado, en la gestión de la configuración, disponibilidad y verificación técnica y en el análisis de tráfico (IDS/IPS), fuga, detección de fraude y prevención de Malware.

En cuando a la seguridad ofensiva, se identifican los ataques clásicos utilizando ML, con Deep Learning, es decir el analizasen profundidad por capas.

CONCLUSIONES

Las Organizaciones buscan lograr sus objetivos maximizando su productividad y minimizando costos, por lo tanto, no es práctico ni deseable controlar cada posibilidad de ataque ni evitar los ataques centrándonos exclusivamente en el valor de los activos que se busca proteger. En su lugar, debe considerarse el contexto en el que se accede a estos activos y se utilizan. Por ejemplo, en un ataque a un sitio web, lo importante es el contexto de las conexiones, no el hecho de que el atacante esté apuntando a un activo de un sitio web en particular o tipo de funcionalidad.

El acceso a la información genera enormes cantidades de datos que indican qué actividades de usuario están permitidas y cuáles no. En conjunto, esta gran cantidad de datos puede proporcionar las claves necesarias para identificar las amenazas, pero solo si se tienen las herramientas capaces de desentrañar dichas amenazas. Este es precisamente el tipo de procesamiento en el que se destaca ML.

Al adquirir un amplio conocimiento de la actividad que rodea a los activos bajo su control, los sistemas de ML hacen posible que los analistas puedan discernir cómo los eventos se dispersan ampliamente en el tiempo y entre computadores, servidores, usuarios y redes diferentes. Aplicado correctamente, el ML puede proporcionar el contexto para reducir los riesgos de una infracción aumentando significativamente el “costo del ataque”.

A medida que ML prolifera en el panorama de seguridad, obliga a elevar el nivel de los atacantes. Hoy en día, cada vez es más difícil penetrar en los sistemas que hace algunos años. En respuesta, es probable que los atacantes adopten técnicas de ML para lograr sus objetivos. A su vez, los profesionales de la seguridad tendrán que utilizar ML de manera defensiva para proteger la red y los activos de información.

En muchos sentidos, las posturas de seguridad del ataque y la defensa son similares a ataque y rechazo. Con ML, emergerán amenazas completamente nuevas e inesperadas. En aproximadamente una década, puede verse un paisaje en el que los “robots de combate” atacan y defienden las redes casi en tiempo real. ML será necesario en el lado de la defensa simplemente para mantener la paridad.

Por supuesto, cualquier tecnología puede ser superada en ocasiones con suficiente esfuerzo y recursos. Sin embargo, se ha encontrado que las defensas basadas en ML complementan los sistemas tradicionales porque se dirigen a una región mucho más amplia del espacio de amenazas que cualquier otra cosa que se haya visto antes y porque poseen capacidades similares a las de los humanos para aprender de sus errores.

REFERENCIAS

[1]C. H. Tarazona, «Amenazas informáticas y Seguridad de la información,» *DerecPenalyCriminXXIX,* 2007.

[2]R. Duda, P. Hart y D. Stork, Pattern classification, New York: Wiley & Sons, 2001.

[3]P. Domingos, The Master Algorithm: How the Quest for the Ultimate Learning Machine Will Remake Our World (Ed. rev.), New York: Basic Books, 2015.

[4]J. Brownlee, A tour of Machine Learning Algorithms, Melbourne: Jason Brownlee, 2013.

[5]I. Witten, E. Frank y M. Hall, Data mining, Bunlington: Morgan Kaufmann Publishers, 2011.

[6]M. Mohri, A. Rostamizadeh y A. Talwalkar, Foundations of machine learning, Cambridge: MIT Press, 2012.