TRABAJO DE GRADO
Opción Seminario-Diplomado.

ALGORITMO COMPUTACIONAL PARA EL ANÁLISIS Y TOMA DE DECISIONES EN DATOS DE ATAQUES CIBERNETICOS Y CIBERSEGURIDADA A COMPAÑIAS PULL DE ABOGADOS EN COLOMBIA, UTILIZANDO ESTRATEGIAS DE MACHINE LEARNING

Corporación Universitaria Remington.
Facultada Ingeniería
Ingeniería de Sistemas

Estudiante:
JEYSON ESNEYDER MORA ALVARADO
Tutor: Juan Carlos Briñez de León

Opción de Trabajo de grado Seminario-Diplomado.
2024.

Dedicatoria

Dedicado Principalmente a Dios quien es el que nos permite estos logros personales y profesionales , a quienes me apoyaron durante todo este viaje que culmina con la presentación de este documento, a la institución educativa, a las compañías donde trabajaba mientras me brindaron la posibilidad de hacerlo mientras estudiaba, a mis familiares que fueron un pilar fundamental durante todo el camino, a mi esposa quien siempre fue una voz de aliento en todo momento sobre todo en momentos de dificultad.

Agradecimientos

Agradezco en primera medida a Dios quien siempre me ha guiado y me ha dado fuerzas para ir por un logro más, todos mis triunfos siempre son en nombre de él y para él.

Quiero agradecer sinceramente a mis padres. Gracias a su apoyo incondicional y constante, pude alimentar mi pasión por el conocimiento y alcanzar nuevas metas. Estoy eternamente agradecido por su amor y orientación, ya que son el motor que impulsa mi éxito gracias a su sacrificio y dedicación.

Quiero expresar mi agradecimiento especial a mi amada esposa. Tu comprensión, paciencia y ánimo han sido esenciales en cada paso de este camino. Gracias a tu apoyo inquebrantable, tengo la fuerza necesaria para seguir adelante con mis estudios y metas profesionales. Este logro no sería posible sin ti a mi lado.

Quiero agradecer también a la Universidad Uniremington, mi alma mater. Gracias a su excelencia académica y recursos, he obtenido una educación sobresaliente que me ha capacitado para enfrentar los retos del ámbito académico y profesional. Agradezco el apoyo continuo de mis profesores y compañeros, quienes me han inspirado y motivado.

En resumen, quiero expresar mi agradecimiento a todas las personas que han contribuido a mi crecimiento y logros en este seminario. Gracias a sus palabras de aliento, apoyo y guía

invaluables, he sido impulsado a alcanzar nuevas alturas. Agradezco sinceramente por esta experiencia y anhelo seguir creciendo y aprendiendo en los próximos tiempos.

Tabla de Contenidos

Contenido

Resumen

En un entorno donde la seguridad de la información se vuelve cada vez más importante, la realización de una investigación tipo tesis centrada en el análisis de brechas de ciberseguridad y vectores de ataques dirigidos específicamente a bufetes de abogados representa un área de estudio crucial. Los bufetes de abogados se convierten en objetivos potenciales para los ciberataques porque manejan datos confidenciales y sensibles de sus clientes, lo que resalta la importancia de comprender y mitigar las vulnerabilidades en sus sistemas de información.

La investigación se centrará en identificar y analizar las brechas de seguridad en los sistemas de TI utilizados por los bufetes de abogados. Esto requeriría un examen completo de la infraestructura de TI, que incluye redes, sistemas de almacenamiento de datos, aplicaciones y dispositivos utilizados en la comunicación con clientes y la gestión de casos legales. Se pueden encontrar puntos débiles potenciales que los actores malintencionados podrían explotar mediante el uso de técnicas de evaluación de vulnerabilidades y análisis forense digital.

La investigación también se enfocaría en comprender los vectores de ataques más comunes dirigidos a los bufetes de abogados, además del análisis de brechas de seguridad. Esto implica investigar cómo los ciberdelincuentes afectan la seguridad de la información en este sector. Estos vectores de ataque podrían incluir ataques de phishing destinados a obtener credenciales de acceso, ransomware destinado a cifrar datos confidenciales y exfiltración de información a través de fallas en aplicaciones o sistemas de almacenamiento.

Palabras clave

Ciberseguridad, Amenazas cibernéticas, Hackeo, Ataque cibernético, Intrusión, Exploit, Vulnerabilidad, Brecha de seguridad, Malware,Virus informático, Ransomware, Troyano, Gusano informático, Phishing, Ingeniería social, Ataque de denegación de servicio DDoS), Botnet, Spoofing, Pharming, Man-in-the-middle (MitM), Ataque de fuerza bruta, Ataque de diccionario, Ataque de inyección SQL, Cross-Site Scripting (XSS), Cross-Site Request Forgery (CSRF), Zero-day, Backdoor, Puerta trasera, Malvertising, Keylogger

Rootkit, Ataque de amplificación, Ataque de canal lateral, Ataque a la infraestructura crítica, Ciberespionaje, Ciberterrorismo, Hacking ético, Auditoría de seguridad, Incidente de seguridad, Gestión de incidentes de seguridad, Análisis de malware, Sandbox, Autenticación multifactor, Criptografía, Firewall, IDS (Intrusion Detection System),

IPS (Intrusion Prevention System), Seguridad perimetral, Seguridad de red

Seguridad de la información

Marco conceptual y contextual

En la actualidad, la tecnología está omnipresente en nuestras vidas diarias, lo que ha cambiado drásticamente la forma en que llevamos a cabo nuestras actividades profesionales. Como parte importante de la sociedad, la abogacía ha sido afectada por este rápido cambio. En Colombia, se han llevado a cabo reformas legales significativas que han transformado los procedimientos judiciales, cambiando de sistemas obsoletos basados en papel a entornos digitales que facilitan el acceso a la justicia y mejoran la eficiencia procesal. Sin embargo, este cambio presenta nuevos desafíos, especialmente en lo que respecta a la seguridad y protección de datos sensibles.

Debido al rápido desarrollo de la tecnología y a las crecientes vulnerabilidades de la información en circulación, la ciberseguridad se ha convertido en una preocupación de alcance global. Aunque la tecnología ha facilitado la comunicación global sin precedentes, también ha permitido que los ciberdelincuentes ingresen a sistemas gubernamentales y comerciales, exponiendo información confidencial. Ante esta situación, se han establecido marcos normativos tanto a nivel nacional como internacional para abordar estos problemas y garantizar la seguridad cibernética.

Colombia ha sido víctima de importantes ataques cibernéticos, como el cometido por el grupo Anonymous en 2011 durante una protesta contra la Ley "Lleras", lo que ha llevado a la implementación de políticas para reducir los peligros de estas amenazas. Como respuesta a esta necesidad, entidades como ColCERT han surgido para ofrecer servicios de prevención de

amenazas informáticas y respuesta a incidentes en colaboración con organizaciones públicas y privadas, algunas leyes colombianas que se han creado con base a este avance tecnologico son:

- Ley 527 de 1999, relacionada con el Comercio electrónico.
- Ley 1266 de 2008, o Ley del Habeas Data.
- Ley 1273 de 2009: Ciberdelitos.
- Conpes 3701
- Conpes 3854
- Circular 007 de 2018 (Entidades Financieras)

En sectores cruciales como el financiero, la ciberseguridad es crucial porque se enfrenta constantemente a ciberataques destinados a la extracción de información y el robo de activos. La Superintendencia Financiera de Colombia define la ciberseguridad como un conjunto de medidas y políticas que tienen como objetivo salvaguardar a los consumidores financieros y los activos de las entidades que operan en el mundo virtual. En respuesta a esta preocupación, se emitió la Circular 007 en 2018. Esta Circular establece requisitos mínimos para la gestión de riesgos de ciberseguridad en el sector financiero que se centran en la prevención, protección, detección, respuesta, comunicación, recuperación y aprendizaje de posibles amenazas cibernéticas.

Pregunta problema:

¿Cómo un algoritmo de machine Learning puede ayudar a crear una estrategia de ciberseguridad enfocado a empresas del sector legal o llamadas de otra forma bufetes de abogados en Colombia teniendo en cuenta que las organizaciones enfrentan en el actual contexto de transformación digital, y cómo estas amenazas pueden afectar la integridad, confidencialidad y disponibilidad de la información crítica de estas compañías

Acercamiento a los datos: Para llevar a cabo esta investigación usando vectores de Machine Learning se ha acudido a información del portal Kaggle (www.kaggle.com) y allí se ha identificado una base de datos de nombre Cybersecurity Risk Attacks, dicha base de datos contiene mas de 8500 registros de diferentes ataques Cibernéticos los cuales hacen match con mittre attack como fuente de referencia y clasificación de estos datos.

Descripción de variables.

A continuación, se muestra la elección de campos de la base de datos seleccionada:

	cve_id	vendor_project	product	vulnerability_name	date_added	required_action	pub_date	cvss	cwe	vector	complexity	severity
0	CVE-2021-27104	ACCELLION	FTA	Accellion FTA OS Command Injection Vulnerability	2021-11-03	Apply updates per vendor instructions.	2021-02-16	9.8	CWE-78	NETWORK	LOW	CRITICAL
1	CVE-2021-27102	ACCELLION	FTA	Accellion FTA OS Command Injection Vulnerability	2021-11-03	Apply updates per vendor instructions.	2021-02-16	7.8	CWE-78	LOCAL	LOW	HIGH
2	CVE-2021-27101	ACCELLION	FTA	Accellion FTA SQL Injection Vulnerability	2021-11-03	Apply updates per vendor instructions.	2021-02-16	9.8	CWE-89	NETWORK	LOW	CRITICAL
3	CVE-2021-27103	ACCELLION	FTA	Accellion FTA SSRF Vulnerability	2021-11-03	Apply updates per vendor instructions.	2021-02-16	9.8	CWE-918	NETWORK	LOW	CRITICAL
4	CVE-2021-21017	ADOBE	Acrobat and Reader	Adobe Acrobat and Reader Heap-based Buffer Ove...	2021-11-03	Apply updates per vendor instructions.	2021-02-11	8.8	CWE-787	NETWORK	LOW	HIGH
5	CVE-2021-28550	ADOBE	Acrobat and Reader	Adobe Acrobat and Reader Use-After-Free Vulner...	2021-11-03	Apply updates per vendor instructions.	2021-09-02	8.8	CWE-416	NETWORK	LOW	HIGH
6	CVE-2018-4939	ADOBE	ColdFusion	Adobe ColdFusion Deserialization of Untrusted ...	2021-11-03	Apply updates per vendor instructions.	2018-05-19	9.8	CWE-502	NETWORK	LOW	CRITICAL
7	CVE-2018-15961	ADOBE	ColdFusion	Adobe ColdFusion Remote Code Execution	2021-11-03	Apply updates per vendor instructions.	2018-09-25	9.8	CWE-434	NETWORK	LOW	CRITICAL
8	CVE-2018-4878	ADOBE	Flash Player	Adobe Flash Player Use-After-Free Vulnerability	2021-11-03	The impacted product is end-of-life and should...	2018-02-06	9.8	CWE-416	NETWORK	LOW	CRITICAL
9	CVE-2020-5735	AMCREST	Cameras and Network Video Recorder (NVR)	Amcrest Camera and NVR Buffer Overflow Vulnera...	2021-11-03	Apply updates per vendor instructions.	2020-04-08	8.8	CWE-787	NETWORK	LOW	HIGH

```
[27] #Información de la estructura de datos
     Conjunto_Datos.info()

     <class 'pandas.core.frame.DataFrame'>
     RangeIndex: 774 entries, 0 to 773
     Data columns (total 16 columns):
      #   Column              Non-Null Count  Dtype
     ---  ------              --------------  -----
      0   cve_id              774 non-null    object
      1   vendor_project      774 non-null    object
      2   product             773 non-null    object
      3   vulnerability_name  774 non-null    object
      4   date_added          774 non-null    object
      5   short_description   768 non-null    object
      6   required_action     774 non-null    object
      7   due_date            774 non-null    object
      8   notes               0 non-null      float64
      9   grp                 774 non-null    int64
      10  pub_date            765 non-null    object
      11  cvss                609 non-null    float64
      12  cwe                 760 non-null    object
      13  vector              609 non-null    object
      14  complexity          609 non-null    object
      15  severity            609 non-null    object
     dtypes: float64(2), int64(1), object(13)
     memory usage: 96.9+ KB
```

La elección de los campos CVE_ID, vendor_project, product, vulnerability_name, date_added, required_action, pub_date, CVSS, CWE, vector, complexity y severity en una evaluacion de ciberseguridad está fundamentada en la necesidad de proporcionar una visión integral y detallada de las vulnerabilidades de seguridad en los sistemas de información. Estos campos permiten una comprensión profunda de los riesgos de seguridad asociados con diferentes productos y tecnologías, así como la evaluación de su impacto y la identificación de acciones correctivas necesarias.

Posibles Aplicaciones

Se pueden utilizar vectores de machine learning para analizar información sobre ataques cibernéticos durante los años 2021, 2022 y 2023, lo cual tiene múltiples aplicaciones potenciales.

Detección de anomalías: Usar aprendizaje automático para detectar patrones anómalos en los datos de ataques cibernéticos ocurridos en los últimos años. Esto podría asistir a las

organizaciones en la detección de posibles amenazas y ataques desconocidos que no se correspondan con los patrones normales de comportamiento.

Predicción de tendencias: Analizar los datos históricos de ataques cibernéticos utilizando algoritmos de machine learning para predecir posibles tendencias futuras en términos de tipos de ataques, métodos utilizados y objetivos de los atacantes. Las organizaciones podrían anticiparse a las amenazas emergentes y prepararse de manera adecuada.

Identificación de vulnerabilidades: Usar machine learning para analizar datos de ataques cibernéticos y relacionarlos con información sobre vulnerabilidades conocidas en sistemas y aplicaciones. Ayudaría a identificar las vulnerabilidades más explotadas por los atacantes y a priorizar las acciones de mitigación y parcheo.

Perfilado de atacantes: Crear perfiles de los atacantes basados en características como el tipo de ataque, la frecuencia, los objetivos y los métodos utilizados utilizando técnicas de machine learning. Ayudar a las organizaciones a comprender mejor a sus oponentes y tomar medidas proactivas para protegerse.

Optimización de la respuesta a incidentes: Desarrollar modelos predictivos utilizando machine learning para analizar los datos de ataques cibernéticos y evaluar la gravedad y el impacto potencial de los incidentes de seguridad. Las organizaciones podrían priorizar y asignar recursos de respuesta de manera más efectiva.

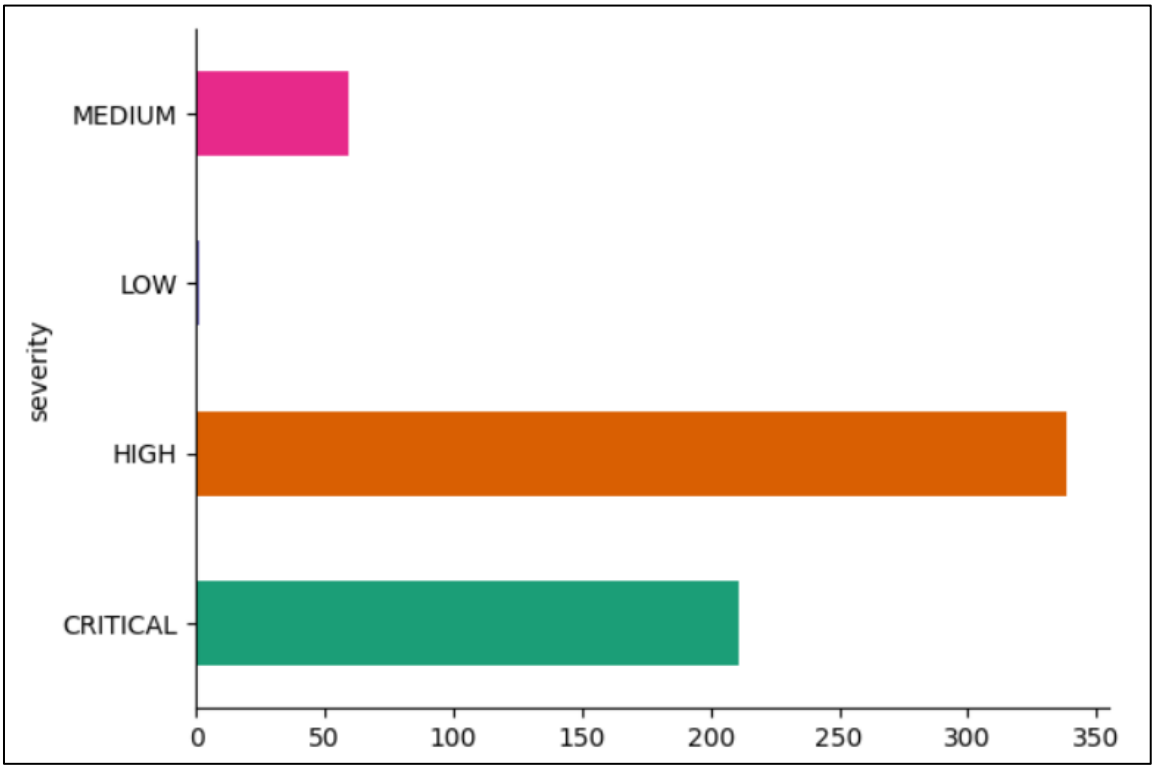
Mejora de la seguridad de la red: Usar el aprendizaje automático para examinar el tráfico de la red y identificar patrones sospechosos o comportamientos anómalos que puedan señalar

actividad maliciosa. Podría ayudar a fortalecer las defensas de seguridad de la red y prevenir intrusiones no autorizadas.

Aproximaciones con gráficos

Revisando las lecturas preliminares de los datos se inicia por el grado de severidad de los datos alimentados en el algoritmo de machine Learning, en esta primera grafica podemos observar la criticidad de las detecciones en un total de 775 registros debidamente categorizados por prioridades Critical, High, Medium respectivamente.

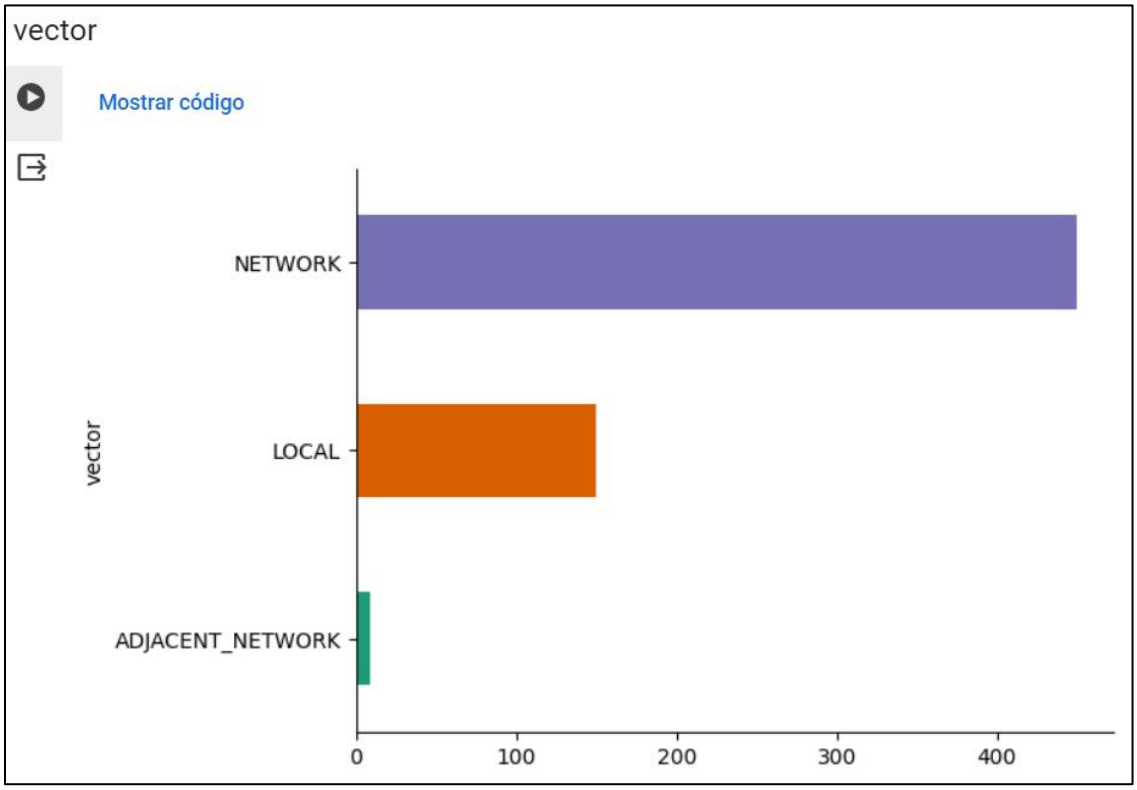
1. Lectura grafico Severidad



Como lo vemos en la imagen anterior, se inicia este assesment identificando el riesgo más importante en base a la cantidad total de detecciones, esto nos permite observar que de todos los

datos analizados tenemos mayor cantidad de vulnerabilidades en severidad ***High***, seguido de ***Critical***, ***Medium*** y finalmente ***Low***, tras este análisis requerimos identificar la cantidad y cuales son estas amenazas para diseñar la estrategia de protección mas adecuada y el orden de ejecución de esta.

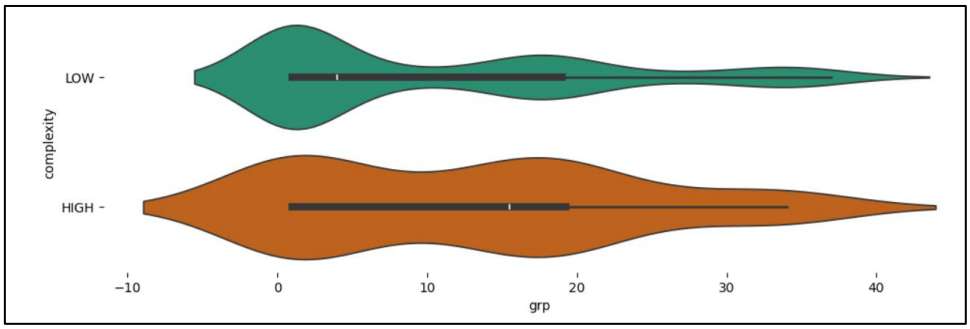
1.2. Lectura grafico Vector de Ataque



Otro grafico que cobra gran relevancia en este assesment es justamente el de vector de ataque dado que con esta información podremos identificar cuáles son las exposición mas explotadas y

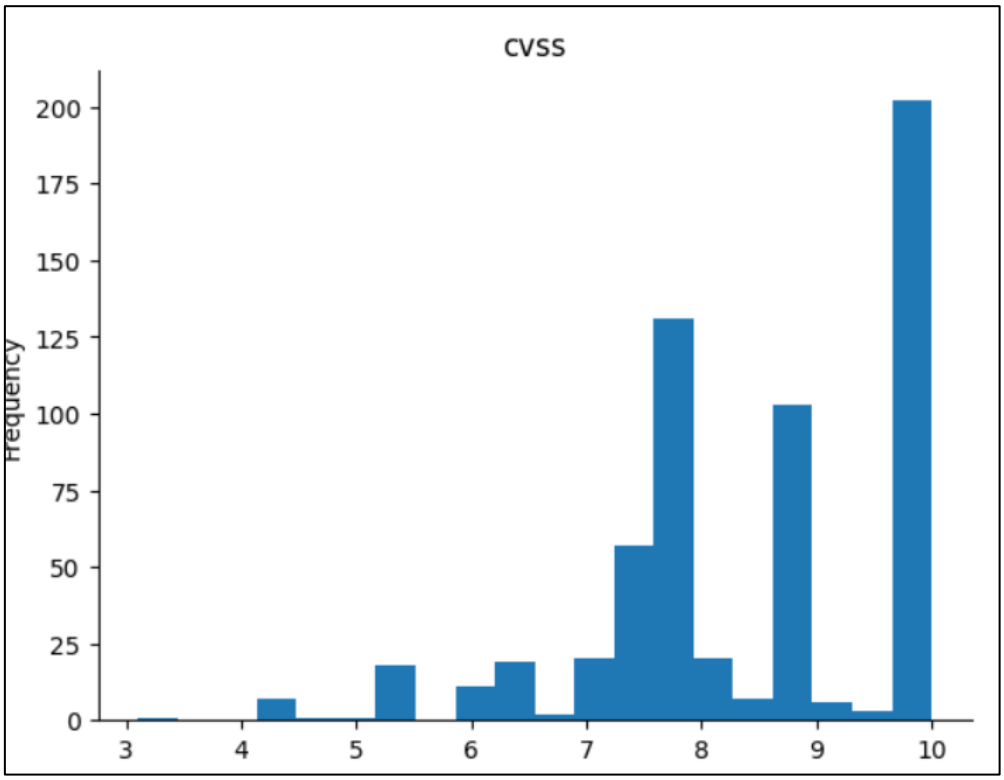
cerrar la brecha, la imagen anterior nos muestra que el vector mas explotado es ***NETWORK*** seguido de ***LOCAL (dentro de la categoría local se engloban vulnerabilidades en aplicaciones, controladores, actualizaciones y características del los sistemas operativos en las estaciones de trabajo)*** para finalizar con ***ADJACENT Network.***

1.3 Lectura grafico Complejidad



En el grafico anterior el algoritmo de machine Learning nos muestra el grado de complejidad totalizado de las detecciones que fueron tenidas en cuenta para en análisis, como se puede ver en la gráfica, el grado de complejidad de las vulnerabilidades identificadas se encuentran en su maría en nivel ***High*** seguido de ***Low*** y es aquí donde analizaremos justamente la prioridad de inicio del cierre de estas brechas de seguridad.

1.4 Lectura grafico CVSS (Common Vulnerability Scoring System).



Para finalizar la evaluación de la ingesta de la data a los algoritmos de machine Learning, encontramos el grafico ***CVSS*** (Common Vulnerability Scoring System) en cual nos aporta información muy importante sobre la puntuación de estas detecciones indexadas basándose en la matriz de Mitre Atta&ck, mitre realiza una puntuación de criticidad basándose en tácticas y técnicas de explotación, una vez calificadas todas las detecciones ingresadas en el algoritmo de machine Learning por mitre se procede a identificar a través de la imagen anterior la cantidad de detecciones versus la puntuación de 1 a 10 donde 1 es calificación baja con menos riesgo y 10 es la calificación más alta con más riesgo de ser victima de un ataque cibernético,

Objetivos:

Objetivo general.

Implementar un algoritmo computacional para el análisis y toma de decisiones a partir de datos de detecciones de amenazas cibernéticas de los años 2020, 2021, 2022 y 2023, utilizando estrategias de machine learning.

Objetivos especificos

- Caracterizar y procesar los datos de interés, con miras a la toma de decisiones informadas.
- Implementar un algoritmo de Machine learning para la toma de decisiones a partir de los datos de interés.
- Evaluar y analizar el desempeño de los algoritmos implementados para la toma de decisiones.
- Validar el funcionamiento de toma de decisiones a partir de datos nuevos.

Desarrollo e implementación del aprendizaje

Evaluacion preliminar

En esta evaluación preliminar se va a determinar algunos hallazgos correspondientes a la base de datos consultadas para esta investigación, inicialmente, se va a analizar con vectores de inteligencia artificial las técnicas y tácticas de ataques más comunes basados en la muestra que se va a usar en esta investigación la cual a su vez hace match con la matriz de mittre attack para traer a esta investigación información más certera y precisa sobre las tendencias de ataque actuales, posteriormente, se procederá a realizar una evaluación de los hallazgos iniciales para la toma de decisión de inversión en materia de ciberseguridad buscando justamente que a través de los algoritmos de machine learning podamos crear un assesment de ciberseguridad para esta compañía, impactando con argumentos sólidos la toma de decisión de inversión a corto, mediano y largo plazo, esta iniciativa busca también que a través del uso de estos algoritmos de inteligencia artificial podamos identificar las brechas más críticas y sensibles a las cuales se encuentran expuestas las compañías en general; en esta segunda etapa se pretende realizar un programa de protección de ciberseguridad teniendo en cuenta los resultados preliminares de la investigación y de los datos obtenidos inicialmente, finalmente, se va a justificar la inversión económica obtenida a través de una matriz de regresión con algoritmos de machine Learning donde se obtendrá el ROI (Retorno de Inversión) con una proyección a 5 años y de esta manera justificar la inversión en materia de ciberseguridad para el Buffete de abogados

Procesamiento de los datos

Carga de datos:

```
import pandas as pd
from google.colab import files
uploaded = files.upload()
for filename in uploaded.keys():
    Dataset = pd.read_excel(filename)

Dataset.head(12)
```

Elegir archivos Regrecion4.xlsx

- **Regrecion4.xlsx**(application/vnd.openxmlformats-officedocument.spreadsheetml.sheet) - 11558 bytes, last modified: 5/4/2024 - 100% done

Saving Regrecion4.xlsx to Regrecion4 (1).xlsx

	Filtro de seguridad	Merramienta de Control	Fabricante	Producto	Mes	Estrategia 1Y	Estrategia 2Y	Estrategia 3Y	Estrategia 4Y	Estrategia 5Y
0	Network	Swiches	Fortinet	FORTISWITCH 124E-FPOE	1	350000	210000	245000	168000	3150000
1	Network	Firewall	Fortinet	FORTIGATE 100F	2	600000	360000	420000	288000	5400000
2	Network	NDR	Fortinet	FORTIGATE 100F	3	150000	90000	105000	72000	1350000
3	Auth	MFA Entrust	Entrust	MFA Entrust	4	100000	60000	70000	48000	900000
4	Vulnerability	Vicarius Assest	Vicarius	Vicarius Assest	5	750000	450000	525000	360000	6750000
5	Endpoint	Endpoint + XDR	Crowdstrike	Falcon	6	685000	411000	479500	328800	6165000
6	capacitacion	Capacitacion	Gamma	Capacitacion	7	23000	13800	16100	11040	207000
7	Vulnerability	Assesment Vulnerability	IBM	Guardium	8	90000	54000	63000	43200	810000
8	Management	MTR	Crowdstrike	MTR Crowdstrike	9	780000	468000	546000	374400	7020000
9	Management	Auditorias	Gamma	Auditorias	10	10000	6000	7000	4800	90000
10	Monitoreo	CSOC	Momitoreo	CiberSOC	11	185000	239000	302000	345200	1155200
11	Administracion	Administracion	Administracion	Administracion	12	19010	487010	1033010	1407410	8427410

Creación y Roadmap de estrategia de Ciberseguridad

Para crear una estrategia de protección de ciberseguridad efectiva, centrada en mitigar los ataques dirigidos a la red y las más de 200 detecciones de MITRE con calificación 10 de severidad crítica y alta como lo muestran las grafias de detecciones de los algoritmos de machine learning, es fundamental implementar un enfoque integral que aborde tanto la prevención como la detección y respuesta ante posibles incidentes.

Segmentación de red: Dividir la red en segmentos más pequeños y asegurar el tráfico entre ellos. Esto puede reducir la superficie de ataque y limitar la propagación de amenazas en caso de compromiso.

Implementación de firewalls avanzados: Utilizar firewalls con funcionalidades avanzadas de inspección de paquetes, filtrado de contenido y detección de intrusiones para proteger los puntos de entrada y salida de la red.

Monitorización continua del tráfico de red: Implementar soluciones de detección de anomalías y comportamientos sospechosos en el tráfico de red. Esto puede ayudar a identificar actividades maliciosas, como escaneos de puertos, tráfico no autorizado o intentos de exfiltración de datos.

Adopción de autenticación multifactor (MFA): Implementar la autenticación multifactor en todos los sistemas y servicios de la red para agregar una capa adicional de seguridad y mitigar el riesgo de compromiso de credenciales.

Actualización regular de sistemas y parches de seguridad: Mantener actualizados todos los sistemas y aplicar parches de seguridad de manera regular para mitigar vulnerabilidades conocidas que podrían ser explotadas por atacantes.

Implementación de soluciones de detección y respuesta de endpoints (EDR): Utilizar soluciones de EDR para monitorear y responder a actividades sospechosas en los dispositivos finales dentro de la red, lo que puede ayudar a detectar y contener ataques antes de que causen un daño significativo.

Capacitación y concienciación del personal: Educar a los empleados sobre las prácticas de seguridad cibernética, incluyendo la identificación de correos electrónicos de phishing, la creación de contraseñas seguras y el uso adecuado de dispositivos y aplicaciones en la red corporativa.

Implementación de herramientas de gestión de vulnerabilidades: Utilizar herramientas de gestión de vulnerabilidades para identificar, priorizar y remediar las vulnerabilidades en la red de manera proactiva.

Desarrollo de un plan de respuesta a incidentes: Establecer un plan detallado de respuesta a incidentes que incluya roles y responsabilidades definidos, procedimientos de comunicación, y procesos de recuperación de datos y sistemas en caso de una brecha de seguridad.

Auditorías de seguridad regulares: Realizar auditorías de seguridad periódicas para evaluar la efectividad de los controles de seguridad implementados y garantizar el cumplimiento de las políticas y estándares de seguridad establecidos.

Implementación en contextos reales

El nuevo conjunto de datos sobre la matriz de inversión en cuanto a ciberseguridad incluye una visualización exhaustiva del cuadro de inversión por capas, enfatizando la implementación específica de un filtro mensual que requiere mantenimiento a lo largo de cinco años, junto con los costos asociados.

Esta matriz organiza las diversas capas de seguridad y identifica las áreas críticas que requieren inversión para garantizar la protección efectiva de los sistemas y datos frente a amenazas cibernéticas potenciales. Cada capa se examina en función de su relevancia y de la necesidad de implementar medidas de seguridad adicionales.

El filtro mensual, que se centra como una implementación clave en esta matriz, se refiere a una medida específica de seguridad que se aplicará regularmente para filtrar y monitorear el tráfico entrante y saliente, identificando posibles actividades maliciosas y protegiendo así la infraestructura de la red.

Para garantizar la eficacia continua de este filtro y su capacidad para adaptarse a las nuevas amenazas y desafíos en el entorno cibernético en constante evolución, se recomienda su mantenimiento mensual durante cinco años. Esto incluye actualizaciones de software, parches de seguridad, revisiones de políticas de filtrado y cualquier otra acción necesaria para mantener la efectividad y la integridad del filtro.

Realice un programa para el modelado de los datos en Python

```
[9] import pandas as pd
    from google.colab import files
    uploaded = files.upload()
    for filename in uploaded.keys():
        Dataset = pd.read_excel(filename)

    Dataset.head(12)
```

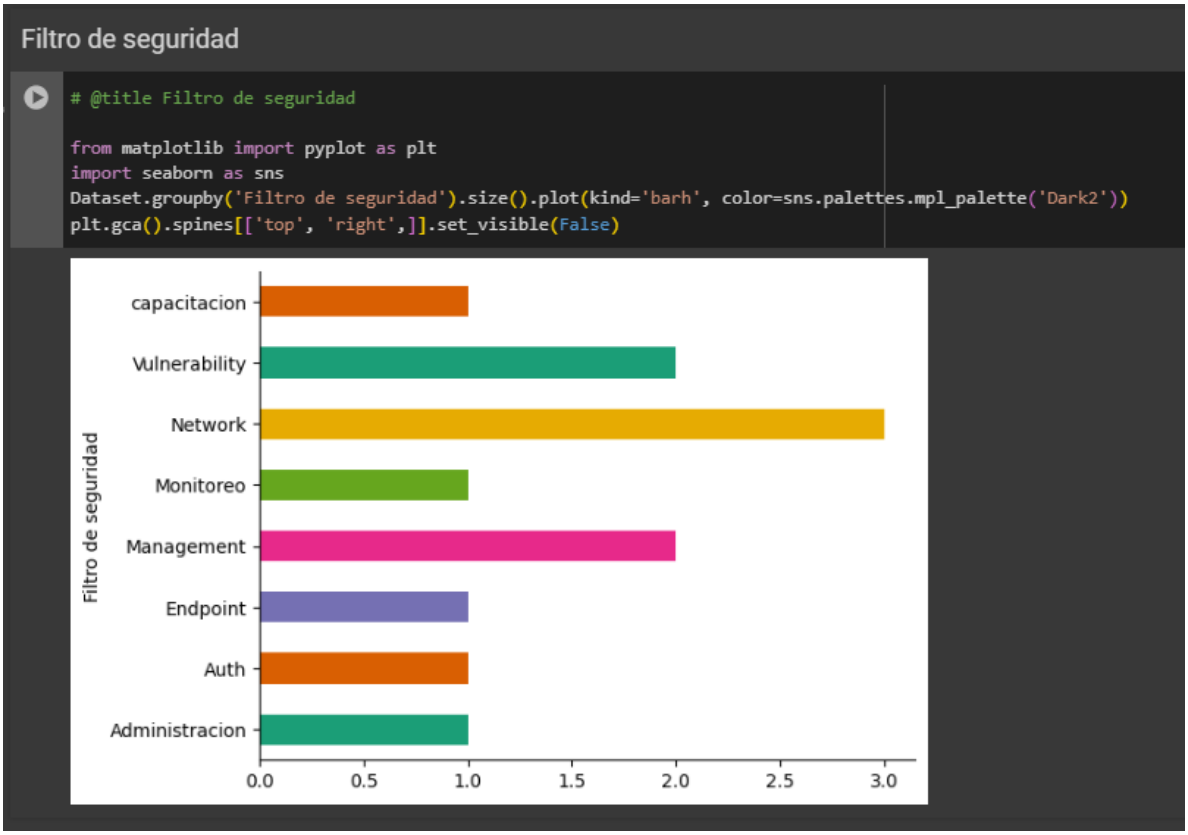
Elegir archivos Regrecion4.xlsx

- **Regrecion4.xlsx**(application/vnd.openxmlformats-officedocument.spreadsheetml.sheet) - 11558 bytes, last modified: 5/4/2024 - 100% done

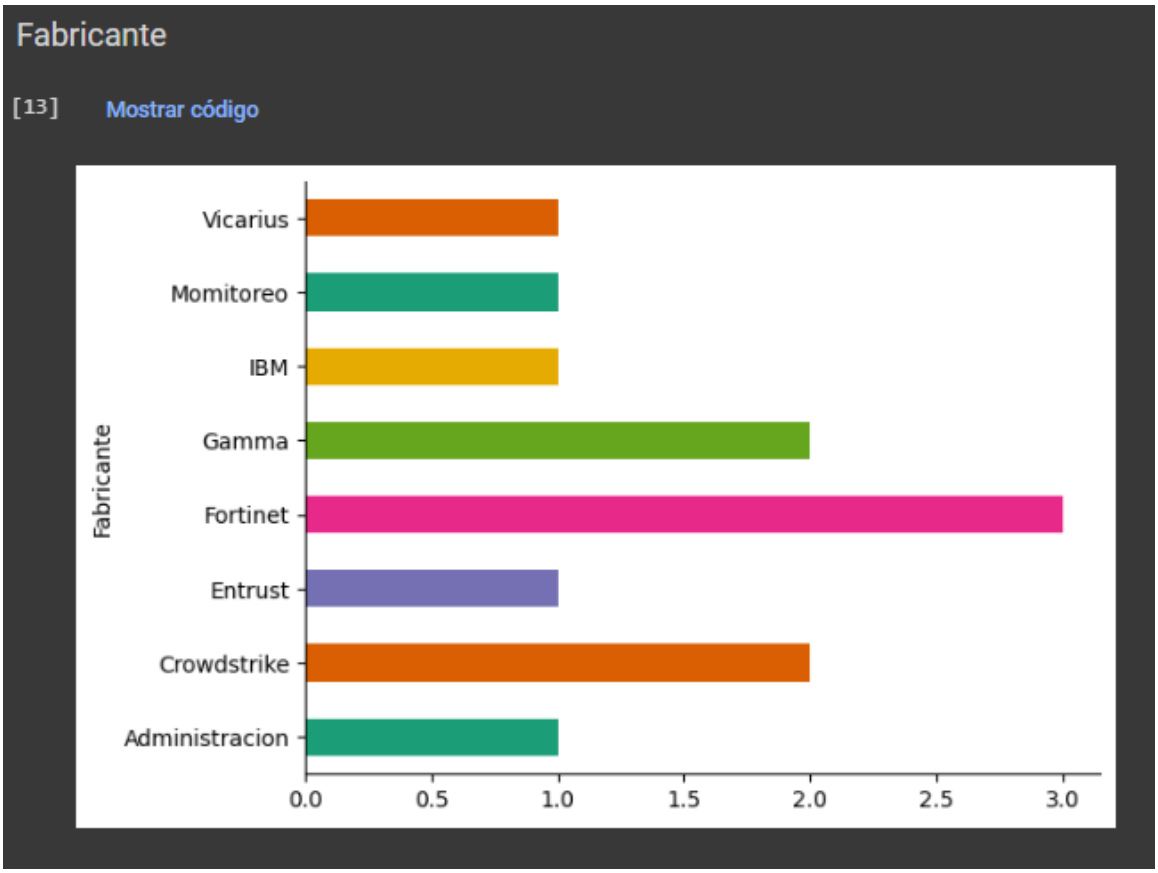
Saving Regrecion4.xlsx to Regrecion4 (1).xlsx

	Filtro de seguridad	Merramienta de Control	Fabricante	Producto	Mes	Estrategia 1Y	Estrategia 2Y	Estrategia 3Y	Estrategia 4Y	Estrategia 5Y
0	Network	Swiches	Fortinet	FORTISWITCH 124E-FPOE	1	350000	210000	245000	168000	3150000
1	Network	Firewall	Fortinet	FORTIGATE 100F	2	600000	360000	420000	288000	5400000
2	Network	NDR	Fortinet	FORTIGATE 100F	3	150000	90000	105000	72000	1350000
3	Auth	MFA Entrust	Entrust	MFA Entrust	4	100000	60000	70000	48000	900000
4	Vulnerability	Vicarius Assest	Vicarius	Vicarius Assest	5	750000	450000	525000	360000	6750000
5	Endpoint	Endpoint + XDR	Crowdstrike	Falcon	6	685000	411000	479500	328800	6165000
6	capacitacion	Capacitacion	Gamma	Capacitacion	7	23000	13800	16100	11040	207000
7	Vulnerability	Assesment Vulnerability	IBM	Guardium	8	90000	54000	63000	43200	810000
8	Management	MTR	Crowdstrike	MTR Crowdstrike	9	780000	468000	546000	374400	7020000
9	Management	Auditorias	Gamma	Auditorias	10	10000	6000	7000	4800	90000
10	Monitoreo	CSOC	Momitoreo	CiberSOC	11	185000	239000	302000	345200	1155200
11	Administracion	Administracion	Administracion	Administracion	12	19010	487010	1033010	1407410	8427410

En la siguiente imagen justificaremos la mayor inversión realizada justamente sobre la infraestructura dado que fue el vector que mas fue atacado y por ende es al que se enfoco de manera prioritaria para lograr una nivelación en cuanto a la protección de activos., seguido a esto, se procede a trabajar sobre la capa de vulnerabilidades con herramientas de propósito especifico seguido de una fuerte apuesta en materia de Managemente la cual va a permitir que fabricantes se apropien de la estrategia en lo que se logra una estabilidad, la cuarta capa y no menos importante es la protección de endpoint con XDR la cual va a permitir lograr una protección con Deep Learning en las estaciones de trabajo.



En materia de fabricantes, se realiza un análisis de la compra donde Fortinet con sus productos de protección en red tiene la ventaja seguido de servicios profesionales Gamma y Crowdstrike con su XDR se lleva el tercer puesto.



Conclusiones

Con el fin de completar el proyecto de seguridad cibernética para compañías legales, se han identificado una serie de elementos cruciales y sugerencias importantes para mejorar la perspectiva sobre la seguridad cibernética:

Conciencia y capacitación: la capacitación continua del personal en ciberseguridad es esencial para garantizar que todos los empleados estén al tanto de las mejores prácticas de seguridad y las amenazas más recientes. Esto comprende reconocer correos electrónicos de phishing, crear contraseñas seguras y comprender las políticas de seguridad de la empresa.

Implementación de políticas sólidas: Es fundamental establecer regulaciones claras y sólidas en materia de seguridad de la información que aborden temas como el uso de dispositivos personales, el acceso a las redes corporativas y la protección de datos confidenciales de los clientes.

Protección de datos confidenciales: Las firmas legales manejan una gran cantidad de datos confidenciales y delicados, por lo que es fundamental tomar medidas adecuadas para proteger los datos, como cifrado de datos, control de acceso y protección contra pérdida.

Actualizaciones de software y parches de seguridad: mantener todos los sistemas y software actualizados es fundamental para reducir las vulnerabilidades conocidas y protegerse contra

posibles ataques de seguridad. Para garantizar que los sistemas estén protegidos contra las últimas amenazas, se debe establecer un proceso regular de actualización y parcheo.

Respaldo de datos y planes de continuidad comercial: la implementación de planes de continuidad comercial y la realización de copias de seguridad regulares ayudarán a reducir los efectos de un ataque cibernético o una pérdida de datos. La identificación de sistemas críticos, la planificación de respuestas a incidentes y la realización de simulacros de seguridad son algunos de los pasos que se pueden tomar en este sentido.

La ciberseguridad es un proceso en constante evolución y evaluación. Se deben realizar evaluaciones regulares de la posición de seguridad cibernética de la empresa para encontrar áreas de mejora y cambiar las estrategias de seguridad según sea necesario.

Referencias

(Gato, s.f.)

(Cuestas, s.f.)