Proyecto de Ciencia de Datos

Análisis de Ataques de Ciberseguridad

Elaborado por José Luis Díaz Torres

Objetivo

Objetivo General:

Desarrollar un modelo predictivo que pueda determinar el tipo de ataque cibernético basado en las características del tráfico de red e indicadores de seguridad, utilizando técnicas de clasificación, buscamos identificar patrones y relaciones entre las variables del conjunto de datos que permitan prever el tipo de ataque con alta precisión

Objetivos Específicos:

- Analizar un dataset relacionado con ataques de ciberseguridad.
- Identificar y predecir tipos de ataques cibernéticos.
- Proporcionar información valiosa para mejorar las estrategias de defensa y mitigación de ataques.

Fuente del Dataset

Fuente del Dataset: Kaggle - Cyber Security Attacks

Descripción: El dataset proporciona una representación realista del historial de actividad en línea para evaluar mapas de calor, firmas de ataque, tipos y más.

URL: https://www.kaggle.com/datasets/teamincribo/cyber-security-attacks

Descripción de los Campos del Dataset

	Tipo de dato	Valores_nulos	Valores_únicos
Timestamp	object	0	39997
Source IP Address	object	0	40000
Destination IP Address	object	0	40000
Source Port	int64	0	29761
Destination Port	int64	0	29895
Protocol	object	0	3
Packet Length	int64	0	1437
Packet Type	object	0	2
Traffic Type	object	0	3
Payload Data	object	0	40000
Malware Indicators	object	20000	1
Anomaly Scores	float64	0	9826
Alerts/Warnings	object	20067	1
Attack Type	object	0	3
Attack Signature	object	0	2
Action Taken	object	0	3
Severity Level	object	0	3
User Information	object	0	32389
Device Information	object	0	32104
Network Segment	object	0	3
Geo-location Data	object	0	8723
Proxy Information	object	19851	20148
Firewall Logs	object	19961	1
IDS/IPS Alerts	object	20050	1
Log Source	object	0	2

Hipótesis

1. **Relación entre la Información de Red y Tipos de Ataques:**

Se espera que la información de red (Timestamp, Source IP Address, Destination IP Address, Source Port, Destination Port, Protocol, Packet Length, Packet Type y Traffic Type) tengan una correlación significativa con tipos específicos de ataques cibernéticos.

2. **Impacto de los Datos de Seguridad y Detección:**

La presencia de Datos de Seguridad y Detección (Malware Indicators, Anomaly Scores, Alerts/Warnings, Attack Signature, Severity Level y Action Taken) se correlacionará fuertemente con ciertos tipos de ataques, como malware y ransomware.

3. **Influencia del Usuario y su Dispositivo:**

La información de usuario y su dispostivo (User Information y Device Information) puede tener relación directa con el tipo de ataque.

4. **Correlación entre la Información de Red y Localización, y los tipos de Ataques:**

Se espera que la información de la red y la localización (Network Segment y Geo-location Data) más con unos tipos de ataque que con otros.

5. **Variación según los indicadores y los tipos de ataque:**

Hay algunos indicadores que van a estar presentes en unos tipos de ataque que en otros.

Campo Eliminados 

- **Payload Data**: Presenta una unicidad total, pues todos sus valores son distintos y no aportan información directa ni indirectamente, es decir, no se puede obtener datos que aporten al desarrollo del modelo.

- **User Information:** Presenta una alta unicidad (> 80%) y hace referencia a un datos personal (Nombre), dato que no contribuye al desarrollo del modelo.

- **Attack Signature:** Dado que indica la firma del ataque, hace parte de la variable objetivo.

- **Severity Level:** Indica la severidad del ataque, por lo tanto hace parte de la variable objetivo.

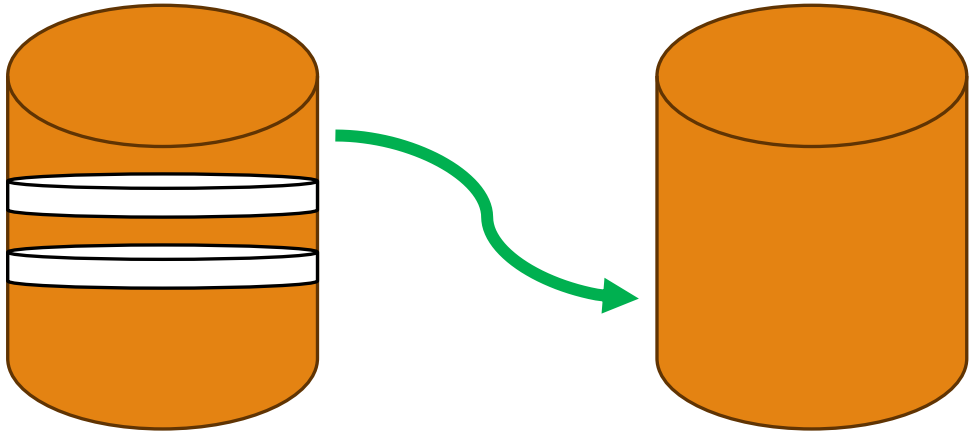
- **Action Taken:** Es una consecuencia del ataque detectado, no una característica predictiva.

Procesamiento de Campos

Campos a los que se les llenó los datos vacíos. Esto se hizo porque los datos vacíos de los campos, indicaban que dicho campo no lo tenía. El valor usado para llenar el vacío, es No.

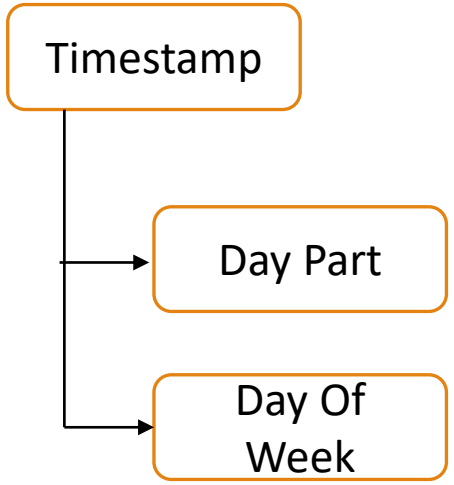
Campos con vaciós diligenciados:

- Malware Indicators
- Alerts/Warnings
- Firewall Logs
- IDS/IPS Alerts



Procesamiento de Campos

Con el campo Timestamp, se generaron dos campos nuevos:



- Day Part:
  - Early Morning (Madrugada).
  - Morning (Mañana).
  - Afternoon (Tarde).
  - Night (Noche).
- Day Of Week
  - 0 (Lunes)
  - 1 (Martes)
  - 2 (Miercoles)
  - 3 (Jueves)
  - 4 (Viernes)
  - 5 (Sábado)
  - 6 (Domingo)

El campo Timestamp fue eliminado.

Procesamiento de Campos

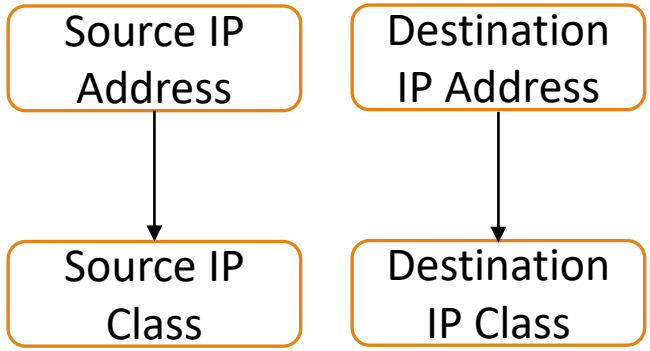
Con los campos que incluyen IP's (Source IP Address y Destination IP Address), se generaron dos campos nuevos:

- Source IP Class.
- Destination IP Class.

Criterio para generar los campos nuevos:

- Clase A: 1.0.0.0 a 126.255.255.255
- Clase B: 128.0.0.0 a 191.255.255.255
- Clase C: 192.0.0.0 a 223.255.255.255

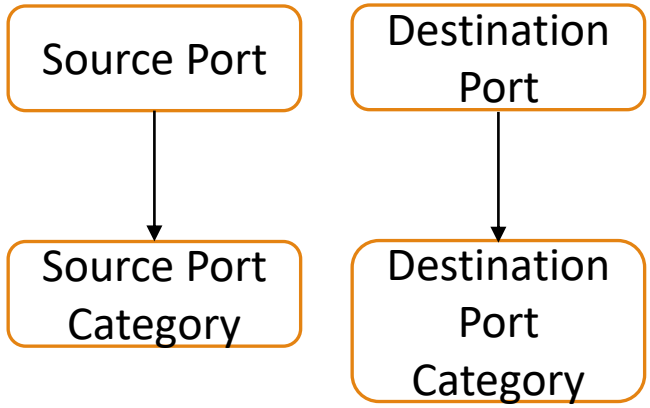
Los campos iniciales fueron eliminados.



Procesamiento de Campos

Con los campos que incluyen Puertos (Source Port y Destination Port), se generaron dos campos nuevos:

- Source Port Category.
- Destination Port Category.



Criterio para generar los campos nuevos:

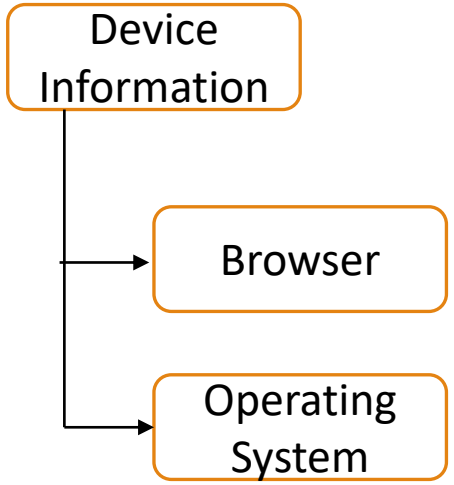
- Well-known Port: 1 - 1023
- Registered Port: 1024 - 49151
- Dynamic Port: 49152 - 65335

Los campos iniciales fueron eliminados.

Procesamiento de Campos

Con el campo Device Information, se generaron dos campos nuevos:

- Browser:
  - Mozilla.
  - Opera.
- Operating System
  - Android
  - iOS
  - Linux
  - Mac OS
  - Windows

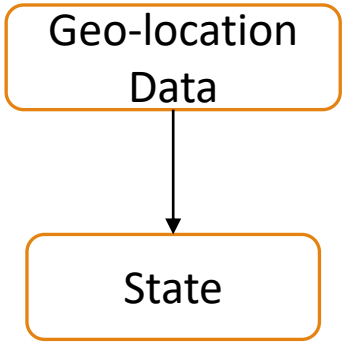


El campo Device Information fue eliminado.

Procesamiento de Campos

Con el campo Geo-location, se generó un nuevo campo:

- State (Estados de India).



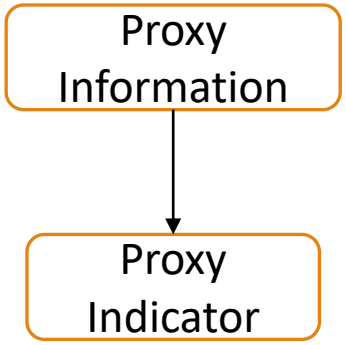
El campo inicial fue eliminado.

Procesamiento de Campos

Con el campo Proxy Information se generó un nuevo campo:

- Proxy Indicator.

  Indica sí la conexión usó un Proxy.



El campo inicial fue eliminado.

Dataframe Final

	Tipo de dato	Valores_nulos	Valores_únicos
Protocol	object	0	3
Packet Length	int64	0	1437
Packet Type	object	0	2
Traffic Type	object	0	3
Malware Indicators	object	0	2
Anomaly Scores	float64	0	9826
Alerts/Warnings	object	0	2
Attack Type	category	0	3
Network Segment	object	0	3
Firewall Logs	object	0	2
IDS/IPS Alerts	object	0	2
Log Source	object	0	2
Day Part	category	0	4
Day Of Week	int32	0	7
Source IP Class	object	0	3
Destination IP Class	object	0	3
Source Port Category	object	0	2
Destination Port Category	object	0	2
Browser	object	0	2
Operating System	object	0	5
State	object	0	28
Proxy Indicator	int64	0	2

EDA

Se realize un análisis exploratorio por cada Hipótesis del proyecto., en el cual se incluyó:

- Análisis Univariado.
- Análisis Bivariado.
- Análisis Multivariado.

EDA

Se realize un análisis exploratorio por cada Hipótesis del proyecto., en el cual se incluyó las siguientes visualizaciones y técnicas:

- Mapa de Calor de Correlación.
- Countplot (Cuenta los valores únicos [Frecuencia], útiles para las variables categoricas).
- Histograma.
- Boxplot.
- Mapa de Calor de la Tabla Contingencia, útil, para medir la correlación de dos variables categoricas.
- Violinplot (Gráfica dos variables categoricas en relación a una variable numerica).
- Scatterplot (Dispersión de 2 variables numericas).
- Pairplot (Gráfica todas las variables numericas contra todas las variables numericas).

Conclusiones

1. Relación entre la Información de Red y Tipos de Ataques:
   a. Los campos asociados a esta hipótesis tienen una distribución de frecuencia que se asemeja a una distribución rectangular, a diferencia de de las categorías creadas para las IP's y puertos, lo cual se debe a la dieferencia desproporcional de de los rangos.
   b. No se evidencia una relación directa entre las features (Variables de Entrada) y lel Label (Variable de Salida), salvo entre la variable Paquete Type y Attack Type, deonde se P Value es menor de 0.05.
2. Impacto de los Datos de Seguridad y Detección:
   a. Los campos asociados a esta hipótesis tienen una distribución de frecuencia que se asemeja a una distribución rectangular
3. Influencia del Usuario y su Dispositivo:
   a. Los campos asociados a esta hipótesis (Browser y Sistema Operativo) presentan un desbalanceo evidente, donde los sistemas más usados son los de Escritorio y en menor medida, los S.O. de smartphones.
   b. No se evidencia una relación directa entre las features (Variables de Entrada) y el Label (Variable de Salida).

Conclusiones

4. Correlación entre la Información de Red y Localización, y los tipos de Ataques:
   a. Los campos asociados a esta hipótesis presentan un balanceo de datos casi en su totalidad, es decir, la frecuencia de sus categorías son muy similares.
   b. No se evidencia una relación directa entre las features (Variables de Entrada) y el Label (Variable de Salida).

5. Variación según los indicadores y los tipos de ataque:
   a. Los campos asociados a esta hipótesis presentan un balanceo de datos casi en su totalidad, es decir, la frecuencia de sus categorías son muy similares.
   b. No se evidencia una relación directa entre las features (Variables de Entrada) y el Label (Variable de Salida).

6. Otras Conclusiones:
   a. La variable de Salida (Attack Type) tiene 3 categorías, las cuales tienen una frecuencia similar, por lo tanto, se encuentran balanceadeas.
   b. Dado que la gran mayoría de variables de entrada son categóricas, no se realizó un gráfico de histogrma, sino que se realizó un gráfico de recuento.