1. **Fuentes y Tipos de Ataques:**
   * ¿Cuáles son las fuentes más comunes de ciberataques?
   * ¿Qué tipos de ataques son más frecuentes (por ejemplo, phishing, ataques de fuerza bruta, malware)?
   * ¿Cómo han evolucionado los métodos de ataque con el tiempo?
2. **Ubicación Geográfica:**
   * ¿Cuáles son los países de origen más frecuentes de los ciberataques?
   * ¿Existen patrones geográficos en los países de destino de los ataques?
   * ¿Las organizaciones de sectores específicos son más propensas a ser atacadas desde ciertas regiones?
3. **Protocolos y Puertos:**
   * ¿Qué protocolos son más vulnerables o son objetivos comunes de ataques?
   * ¿Hay patrones en los puertos utilizados durante los ataques?
   * ¿Cómo ha evolucionado el uso de protocolos y puertos a lo largo del tiempo?
4. **Sectores Específicos:**
   * ¿Existen sectores profesionales que son más susceptibles a ciertos tipos de ataques?
   * ¿Cómo varía la frecuencia y naturaleza de los ataques entre sectores (financiero, salud, gobierno, etc.)?
5. **Duración y Detección:**
   * ¿Cuánto tiempo transcurre típicamente entre el inicio de un ataque y su detección?
   * ¿Hay patrones en la duración de los ataques según el tipo y la fuente?
   * ¿Qué medidas de seguridad son más efectivas para la detección temprana?
6. **Tipos de Malware:**
   * ¿Cuáles son los tipos de malware más comunes?
   * ¿Cómo se propaga el malware y cuál es su vector de entrada más común?
7. **Respuestas y Mitigación:**
   * ¿Cómo responden las organizaciones a los ataques (tiempo de respuesta, estrategias de mitigación)?
   * ¿Existen patrones en las estrategias de mitigación efectivas?
8. **Tendencias Temporales:**
   * ¿Existen tendencias temporales en la frecuencia o gravedad de los ciberataques?
   * ¿Cómo han evolucionado las tácticas y técnicas a lo largo de los años?
9. Distribución de Ataques:
10. ¿Cuál es la distribución de los diferentes tipos de ataques en el conjunto de datos?
11. ¿Cuántos incidentes de cada tipo de ataque se registran?
12. Conclusión: Obtener una comprensión general de la prevalencia de diferentes tipos de ataques.
13. Análisis Temporal:
14. ¿Cómo varían los ataques a lo largo del tiempo en el conjunto de datos?
15. ¿Hay patrones estacionales o tendencias a lo largo de los años?
16. Conclusión: Identificar posibles patrones temporales en los ataques.
17. Origen de los Ataques:
18. ¿Cuál es la distribución geográfica de los ataques (por país, región)?
19. ¿Existen patrones en los países de origen de los ataques?
20. Conclusión: Entender la geografía de los ataques y posiblemente identificar ubicaciones de mayor riesgo.
21. Consecuencias y Respuestas:
22. ¿Cuáles son las consecuencias de los ataques en términos de severidad?
23. ¿Cuál es la acción tomada en respuesta a los ataques?
24. Conclusión: Evaluar el impacto de los ataques y la eficacia de las respuestas.
25. Frecuencia de Protocolos:
26. ¿Cuáles son los protocolos más utilizados en los ataques?
27. ¿Existe un protocolo predominante en ciertos tipos de ataques?
28. Conclusión: Identificar los protocolos más susceptibles o comúnmente explotados.
29. Exploración de Características:
30. ¿Cómo se distribuyen las características específicas del conjunto de datos (por ejemplo, puertos, direcciones IP)?
31. ¿Existen patrones notables en las características utilizadas en los ataques?
32. Conclusión: Profundizar en las características específicas que podrían ser indicativas de vulnerabilidades o puntos de entrada comunes.
33. Correlaciones y Relaciones:
34. ¿Hay correlaciones entre diferentes variables en el conjunto de datos?
35. ¿Existen relaciones entre el tipo de ataque y otras características?
36. Conclusión: Identificar posibles factores que estén relacionados entre sí y podrían tener implicaciones en la ciberseguridad