Ficha de Resumen de Artículo Científico: Measuring the Quality Information of Sources of Cybersecurity by Multi-Criteria Decision Making Techniques

Ficha elaborada por: Ines Salamanca Estévez

Título del artículo: Measuring the Quality Information of Sources of Cybersecurity by Multi-Criteria Decision Making Techniques

Autor/es del artículo: Noemí DeCastro-García, Enrique Pinto

Año: 2022

Enlace: https://link.springer.com/chapter/10.1007/978-3-031-15471-3_7

Resumen

El artículo presenta un software de soporte a la decisión que evalúa la calidad de la información de las fuentes de datos de ciberseguridad utilizando técnicas de toma de decisiones multicriterio (MCDM). Se integran el Modelo de Suma Ponderada (WSM) para una clasificación general y el Proceso Analítico Jerárquico (AHP) para clasificaciones más flexibles. También se calcula el coeficiente de Goodman y Kruskal para medir la concordancia entre las clasificaciones. El estudio se realizó con un conjunto de datos real de 25 millones de registros de eventos de ciberseguridad de 27 fuentes y 55 tipos de eventos, permitiendo un diagnóstico para identificar áreas de mejora.

Ideas principales

- Se ha desarrollado un software de soporte a la decisión para evaluar la calidad de la información de las fuentes de datos de ciberseguridad, esencial para equipos de respuesta a incidentes (CSIRT/CERT) para garantizar decisiones y contramedidas adecuadas.
- El software integra dos técnicas de toma de decisiones multicriterio (MCDM): el Weighted Sum Model (WSM) para obtener una clasificación general de las fuentes de datos y el Analytic Hierarchy Process (AHP) para clasificaciones más flexibles y adaptables a la importancia de las dimensiones de calidad.
- Se incluye el cálculo del coeficiente de Goodman y Kruskal para medir la concordancia entre las clasificaciones obtenidas con WSM y AHP, sirviendo como alerta si la concordancia es baja y ayudando al experto a ajustar los pesos en WSM.
- El estudio se llevó a cabo sobre un conjunto de datos real proporcionado por INCIBE, que contenía 25.297.210 registros de eventos de ciberseguridad, de 27 fuentes (propias, públicas y privadas) y 55 tipos de eventos de ciberseguridad.
- Los resultados muestran que, en general, el nivel de calidad de la información en el sistema no es suficientemente alto (puntuación media de 0.4449 sobre un máximo de 1.5), destacando que las fuentes propias ofrecen la mejor calidad, mientras que las fuentes privadas tienen una puntuación baja (0.3242 de media), lo que sugiere la necesidad de analizar su valor o eliminarlas.

Material usado

Datos:

- Real dataset: 25.297.210 registros de eventos de ciberseguridad.
- 27 fuentes de datos de ciberseguridad (propias, públicas, privadas).
- 55 tipos de eventos de ciberseguridad.
- Muestra de datos anonimizada proporcionada por INCIBE.

Software:

- Python 3.7 (para el desarrollo del software y la anonimización de datos).
- Script de Python (para anonimizar la muestra de datos).
- Código fuente disponible en Github [25].

Hardware:

- Windows 10
- 1 CPU (Intel I5 CPU Model)
- 8 GB de RAM

Herr. matemáticas:

- Weighted Sum Model (WSM)
- Analytic Hierarchy Process (AHP)
- Coeficiente Goodman y Kruskal (para medir la concordancia)
- Escala de Saaty de 1 a 9 puntos (para comparaciones pareadas en AHP)
- Ratio de matriz de consistencia (CR) e índice de matriz de consistencia (CI)

Palabras clave

Data quality, Cybersecurity, Decision making systems, Diagnosis, Data sources

Referencias relevantes

8 ENISA. (m-d). NCSA/CSIRT: Incident response in practice [online]. https://www.enisa.europa.eu/publications/national-csirt-capabilities-and-csirt-maturity-v2/at_download/fullReport

26 DeCastro-García, N., Pinto, E.: Dataset for measuring the quality information of sources of cybersecurity. https://github.com/NoemiDecastro/Dataset-Quality-Information-Cybersecurity-Sources (2022)

27 Saaty, T.L.: The Analytic Hierarchy Process. McGraw-Hill, New York (1980)

30 Fishburn, P.C.: Weighted sum methods for multiattribute utility functions. Naval Res. Logist. Q. 29(4), 629–635 (1982)

10 Goodman, L.A., Kruskal, W.H.: Measures of association for cross classifications. J. Am. Stat. Assoc. 49(268), 732–764 (1954)

Observaciones / Comentarios

Estucio de la calidad de los datos del MICs.