|  |  |  |  |  |  |  |
| --- | --- | --- | --- | --- | --- | --- |
| **Studies** | **Research Objectives** | **Output Formats** | **Identify Entity** | **Identify Relation** | **Context of Relation** | **Methods** |
| AttacKG [1] | Extract attack behavior graph & identify attack techniques | Attack Behavior Graphs | V | V |  | Entity Recognition,  Graph Alignment |
| TTPDrill [2] | Learn attack pattern (TTPs) | STIX Objects | V |  | V | Ontology TF-IDF, Dependency Parser |
| LADDER [3] | Extract attack patterns | Knowledge Graph Triplet | V | V | △ | BERT, TuckER |
| EXTRATOR [4] | Extract attack behaviors | Attack Behavior Graphs | V | V | △ | ER, Semantic Role Labeling |
| Our Research | Extract attack activities | *OPen* pair | V | V | V | Dependency Parser, BERT embedding |

表格二: Threat Report Processing

表格描述: Comparison of automatic threat report extraction and processing researches. The triangle symbol represents that only predefined context words or relationship type can be assigned.

\cite{li\_2022\_attackg, husari\_2017\_ttpdrill, alam\_2022\_looking, satvat\_2021\_extractor}

#可以用白色的 ref{} 來產生論文的引用編號，再把引用編號寫死在表格上。

|  |  |  |  |  |  |  |
| --- | --- | --- | --- | --- | --- | --- |
| **Studies** | **Research Objectives** | **Data Source** | | **Label**  **System**  **Objects** | **Graph Representation** | **Approach** |
| **Audit Logs** | **Syscall Traces** |
| TPG [5] | Technique Classification | V |  | V | V | Rules by Symantic EDR |
| HOLMES [6] | Technique Classification | V |  |  | V | Event Rules |
| Log2Vec [7] | Anomaly Detection | V |  |  | V | Graph Rules,  Cluster Detection |
| Tiresias [8] | Event Forecast | V |  |  |  | RNNs |
| SetConv [9] | Tactic Classification |  | V | V |  | OAML, CNNs |
| Our Research | Display & Query Malware Execution Steps |  | V | V | V | Execution Causal Relationship |

表格三: Log Processing and Provenance Graph Construction

表格描述: Comparison of log processing researches. Most of the studies convert and merge log data as a provenance graph-like data-structure. \cite{milajerdi\_2019\_holmes, hassan\_2020\_tactical, liu\_2019\_log2vec, shen\_2018\_tiresias, akbar\_2021\_identifying}

|  |  |  |  |  |
| --- | --- | --- | --- | --- |
| **Studies** | **Research Objectives** | **Target on Platform** | **Target on Document** | **Require Expert** |
| [23] | Construct contextual CTI Ontology | V |  | V |
| [24] | Propose Data Quality methodologies | V |  |  |
| [25] | Evaluate Quality of CTI services | V |  | V |
| [26] | Evaluate Quality of CTI feeds | V |  | △ |
| [48] | Evaluate Trustworthiness of CTI sources | V |  |  |
| Our Research | Evaluate Quality of CTI documents |  | V |  |

表格一: Cyber Threat Intelligence Evaluation

表格描述: Comparison of CTI evaluation researches. The triangle symbol represents that there is a requirement of establishing lists of unroutable and active IPs by experts.