	List of all related survey papers (or other non technical papers)						
#	**Author**	**Year**	**Title**	**Focus**	**Difference to our approach**	**Relevant to our work?**	**Link**
1	Rahman	2023	What Are the Attackers Doing Now? Automating Cyberthreat Intelligence Extraction from Text on Pace with the Changing Threat Landscape: A Survey	Main Goal: (i) Aid cybersecurity researchers understand the current techniques used for cyberthreat intelligence extraction from text through a survey of relevant studies in the literature (ii) Systematically collect "CTI extraction from text"-related studies from the literature and categorize the CTI extraction purposes (iii) Proposal of a CTI extraction pipeline (identify the data sources, techniques, and CTI sharing formats utilized)	Probably the closest "related work," but mainly focusing on the review of literature without any exploration of the data sources (no technical part, it's "just" a survey)	YES	https://dl.acm.org/doi/10.1145/3571726
2	Arazzi	2023	NLP-Based Techniques for Cyber Threat Intelligence	Review of NLP techniques applied for CTI extraction, very detailed on the NLP level	Paper does not focus on the data source	NO	https://arxiv.org/abs/2311.08807
3	Rahman	2020	A Literature Review on Mining Cyberthreat Intelligence from Unstructured Texts	Identify and analyze existing research on mining CTI	Prior version of the Rahman 2023 paper: What are attackers doing now? - Refer to the more recent and elaborated version.	NO	https://ieeexplore.ieee.org/document/9346318
4	Basheer	2021	Threats from the Dark: A Review over Dark Web Investigation Research for Cyber Threat Intelligence	comprehensive analysis of techniques, methods, tools, approaches, and results, and discussing possible limitations and future work in darkweb monitoring.	Primarily focus on darknet sources, and detailed investigation of prior work until 2021 - good reference for prior work, but no experimental analysis (it's a review paper)	YES	https://www.hindawi.com/journals/jcnc/2021/1302999/
5	Samtani	2020	Cybersecurity as an industry: A cyber threat intelligence perspective	Systematic analysis of CTI platforms (focus on industry) with the following focus: (1) shift from reactive to proactive OSINT-based CTI platforms (2) enhancement of natural language processing (NLP) and text mining capabilities (3) enhancement of data mining capabilities	Interesting paper for some additional insights, but not highly relevant	NO	https://www.researchgate.net/publication/335688262_Cybersecurity_as_an_Industry_A_Cyber_Threat_Intelligence_Perspective
6	Cascavilla	2021	Cybercrime threat intelligence: A systematic multi-vocal literature review	The paper reviews grey and white literature about cybercrime detection by using cyber threat intelligence. They review prior work and investigate multiple questions related to the main topics studied in the darknet/deepweb and surface net, as well as the depth and focus of these topics given these three data sources.	Paper is not really relevant to us. They apply topic modeling to study the topics of prior work (topic modeling is done on prior papers).	NO	https://www.sciencedirect.com/science/article/pii/S0167404821000821
7	Singh	2022	Cyber Threat Intelligence “Comparative Analysis of Its Sources and Parameters of Evaluation”	Review of a variety of cyber threat intelligence sources and prototypes that are used to extract data and detect cyber threats. Social media intelligence and open-source intelligence could be a method of collecting information from publicly available sources; specifically in global health security management in situations like infectious disease outbreaks	Rather high-level review with a focus on health-related incidents, such as the pandemic. Authors argue why social media is an important source of CTI.	NO	https://link.springer.com/content/pdf/10.1007/978-981-16-8987-1_25.pdf
8	Sun	2023	Cyber Threat Intelligence Mining for Proactive Cybersecurity Defense: A Survey and New Perspectives	Provide a taxonomy to summarize the studies on CTI mining based on the intended purposes (i.e., cybersecurity-related entities and events, cyber attack tactics, techniques and procedures, profiles of hackers, indicators of compromise, vulnerability exploits and malware implementation, and threat hunting), Also identify interesting research challenges and possible future research directions for CTI mining	Interesting insights on the type of data extracted from CTI sources and its application/further use	YES	https://ieeexplore.ieee.org/abstract/document/10117505