International Journal of Innovative Computer Science and IT Research

Volume 01, Issue 05 – Sep-Oct 2025 • E-ISSN: 3067-1108 | P-ISSN: 3067-1094

Threat Intelligence Analytics for Proactive Cybersecurity Management

David Stupples

Professor, Royal Holloway, University of London, United Kingdom

Abstract

The rapid evolution of cyber threats has increased the need for cybersecurity strategies that can anticipate malicious activities rather than responding only after security incidents occur. Threat intelligence provides organizations with information about adversaries, attack techniques, malicious infrastructure, vulnerabilities, indicators of compromise, and emerging threat patterns. However, the growing volume and heterogeneity of threat intelligence sources create significant challenges related to data quality, relevance, correlation, prioritization, and timely decision-making. This research examines threat intelligence analytics as a proactive cybersecurity management approach capable of transforming heterogeneous security information into actionable organizational intelligence. The proposed framework integrates threat data collection, normalization, enrichment, indicator analysis, behavioral correlation, risk assessment, prioritization, and security-response support.

The methodology combines structured and unstructured intelligence sources with computational analytics to identify relationships among indicators, assets, vulnerabilities, and adversarial behaviors. Machine learning, anomaly detection, natural language processing, graph-based analysis, and statistical techniques are considered for extracting meaningful patterns from large-scale threat information. Two analytical tables are used to examine major intelligence sources, analytical techniques, operational benefits, and limitations. The analysis demonstrates that threat intelligence analytics can improve proactive cybersecurity management by supporting early threat identification, vulnerability prioritization, attack-surface awareness, and informed defensive planning. However, challenges involving intelligence overload, unreliable sources, stale indicators, adversarial deception, data interoperability, privacy, attribution uncertainty, and analytical bias can reduce operational effectiveness. The study argues that threat intelligence should not be treated simply as a collection of indicators but as an analytical capability that connects external threat information with internal organizational context. Effective proactive cybersecurity management requires continuous intelligence collection, contextual enrichment, risk-based prioritization, automated correlation, and expert validation. The proposed framework provides a structured foundation for integrating threat intelligence analytics into cybersecurity operations and supports a transition from reactive incident handling toward continuous, evidence-based, and anticipatory security management.

Keywords: Threat Intelligence, Cybersecurity Management, Cyber Threat Analytics, Proactive Security, Machine Learning, Threat Detection, Risk Assessment, Security Intelligence, Cyber Threat Analysis, Vulnerability Management.

International Journal of Innovative Computer Science and IT Research

Volume 01, Issue 05 – Sep-Oct 2025 • E-ISSN: 3067-1108 | P-ISSN: 3067-1094

1. Introduction

The cybersecurity landscape has become increasingly dynamic as organizations expand their dependence on cloud computing, digital platforms, interconnected devices, remote services, and distributed information systems. Attackers continuously modify their techniques, infrastructure, and operational strategies to exploit emerging vulnerabilities and bypass established defensive controls. Organizations that rely primarily on reactive security mechanisms may discover threats only after compromise has occurred. Proactive cybersecurity management therefore requires mechanisms capable of identifying relevant threat information before it develops into a significant security incident.

Threat intelligence provides structured and contextual information about cyber adversaries, malicious infrastructure, vulnerabilities, attack techniques, and indicators associated with harmful activities. Intelligence may be collected from security feeds, incident reports, vulnerability databases, malware analysis, network monitoring, open-source information, and organizational security events. However, simply collecting large quantities of intelligence does not guarantee improved security. Organizations must determine which information is relevant to their assets, infrastructure, threat exposure, and operational priorities.

Threat intelligence analytics addresses this problem by applying computational methods to collected security information. Analytics can identify relationships between indicators, cluster similar threats, detect emerging patterns, prioritize vulnerabilities, and connect external intelligence with internal security events. Machine learning can assist with classification and anomaly detection, while natural language processing can extract relevant entities and relationships from unstructured threat reports. Graph-based approaches can additionally represent connections between threat actors, malware, infrastructure, vulnerabilities, and targeted assets.

The effectiveness of threat intelligence depends strongly on context. An indicator that represents a significant threat to one organization may have little relevance to another. Similarly, an old malicious domain may no longer represent an active threat. Therefore, intelligence should be evaluated according to factors such as freshness, confidence, relevance, affected assets, attack techniques, and potential business impact. Contextual analysis enables security teams to prioritize intelligence rather than responding indiscriminately to every reported threat.

This research develops a conceptual framework for threat intelligence analytics and proactive cybersecurity management. The framework integrates intelligence acquisition, preprocessing, enrichment, analytical modeling, correlation, risk prioritization, and response planning. It examines how organizations can use intelligent analytics to transform fragmented threat information into actionable security knowledge and strengthen their ability to anticipate, prevent, and mitigate cyber threats.

2. Objectives

The primary objective of this research is to develop a structured threat intelligence analytics framework that supports proactive cybersecurity management through continuous intelligence collection, contextual enrichment, intelligent correlation, threat prioritization, and risk-based decision-making. The framework seeks to help organizations identify relevant threats earlier and align defensive actions with actual organizational exposure.

Volume 01, Issue 05 – Sep-Oct 2025 • E-ISSN: 3067-1108 | P-ISSN: 3067-1094

2.1 Intelligence Collection and Contextualization

The first objective is to establish an approach for collecting threat intelligence from diverse internal and external sources and transforming it into structured, usable information. Intelligence should be evaluated according to source reliability, freshness, confidence, relevance, and organizational context. Contextual enrichment can connect indicators with affected assets, vulnerabilities, attack techniques, and historical incidents, allowing security teams to distinguish actionable intelligence from irrelevant information.

2.2 Intelligent Threat Pattern Identification

The second objective is to investigate computational techniques for identifying relationships and patterns within large-scale threat intelligence datasets. Machine learning, natural language processing, graph analytics, and anomaly detection can support automated identification of malicious infrastructure, attack patterns, related indicators, and emerging threats. Intelligent analysis can reduce manual processing requirements and provide analysts with a more comprehensive understanding of adversarial behavior.

2.3 Proactive Risk Prioritization

The third objective is to connect threat intelligence with organizational risk management. Intelligence should be prioritized according to the likelihood of exploitation, asset importance, vulnerability exposure, threat confidence, and potential business impact. Risk-based prioritization enables security teams to focus limited resources on threats most likely to affect critical systems rather than treating all intelligence with equal urgency.

3. Review of Literature

3.1 Foundations of Cyber Threat Intelligence

Cyber threat intelligence has developed as an approach for collecting and analyzing information about threats, adversaries, vulnerabilities, and malicious activities. Intelligence can exist at different levels, including strategic intelligence for organizational decision-making, operational intelligence for understanding campaigns, tactical intelligence for identifying attacker techniques, and technical intelligence for identifying indicators such as malicious addresses or file characteristics.

The value of intelligence depends on its ability to support decisions. Large collections of indicators without contextual interpretation can overwhelm security teams. Effective intelligence therefore requires collection, processing, analysis, dissemination, and feedback. Integrating intelligence with security operations allows organizations to connect external threat knowledge with internally observed activities.

3.2 Analytics and Machine Learning for Threat Intelligence

The growing volume of threat information has encouraged the use of machine learning and advanced analytics. Classification models can categorize indicators and malicious artifacts, while clustering can group related threat activities. Natural language processing can extract entities, vulnerabilities, attack techniques, and organizations from unstructured reports. Graph analytics can reveal relationships among threat actors, infrastructure, malware families, and targeted systems. Despite these advantages, machine learning models may encounter incomplete, biased, or outdated intelligence. Threat environments

change rapidly, and attackers may intentionally generate misleading information. Consequently, automated analytics should be continuously evaluated and combined with expert interpretation.

3.3 Proactive Cybersecurity and Risk Management

Proactive cybersecurity emphasizes anticipation and preparation rather than relying exclusively on incident response after compromise. Threat intelligence contributes to this objective by identifying vulnerabilities, adversarial techniques, emerging campaigns, and indicators associated with potential attacks. Security teams can use intelligence to adjust controls, prioritize patches, strengthen monitoring, and improve incident preparedness.

Risk-based intelligence is particularly valuable because organizational resources are limited. Security teams cannot investigate every threat equally. By combining threat likelihood, confidence, asset criticality, and vulnerability exposure, intelligence analytics can support more informed security investment and operational prioritization.

4. Methodology

4.1 Research Design and Threat Intelligence Framework

This study adopts a conceptual and analytical research design to develop an integrated framework for threat intelligence analytics and proactive cybersecurity management. The framework consists of sequential stages including intelligence collection, normalization, validation, enrichment, analytical processing, correlation, risk scoring, prioritization, and security-response support. It is designed to integrate external threat information with internal organizational telemetry and asset context.

The framework treats threat intelligence as a continuously evolving analytical resource rather than a static database of indicators. Intelligence records are associated with metadata describing source, timestamp, confidence, relevance, and observed relationships. Analytical mechanisms then compare external intelligence with organizational assets, vulnerabilities, network observations, and previous incidents. High-relevance findings are prioritized for security action, while low-confidence or outdated information is subjected to additional validation before operational use.

4.2 Intelligence Collection and Preprocessing

Threat intelligence can originate from multiple sources, including vulnerability databases, security advisories, incident reports, malware analysis, security feeds, open-source intelligence, internal incident records, and network observations. Collection mechanisms should establish source reliability and record contextual metadata. Information from different sources may use inconsistent formats, terminology, identifiers, and levels of detail, making normalization necessary before integrated analysis.

Preprocessing involves removing duplicate indicators, standardizing formats, resolving inconsistent identifiers, validating timestamps, and identifying outdated information. Indicators may include network addresses, domains, file hashes, vulnerabilities, behavioral descriptions, and attack techniques. Intelligence records should retain source attribution and confidence information so that analysts can distinguish verified intelligence from uncertain observations. The preprocessing stage therefore improves consistency while preserving information necessary for subsequent analytical evaluation.

Volume 01, Issue 05 – Sep-Oct 2025 • E-ISSN: 3067-1108 | P-ISSN: 3067-1094

4.3 Threat Analytics and Contextual Enrichment

Analytical processing applies computational techniques to identify meaningful relationships and patterns within threat intelligence. Machine learning can classify indicators and detect similarities among threat artifacts. Natural language processing can extract entities, vulnerabilities, techniques, and threat relationships from reports. Graph-based analytics can represent connections among threat actors, infrastructure, malware, vulnerabilities, and targeted assets.

Key analytical functions include:

- Indicator classification.
- Threat clustering.
- Vulnerability correlation.
- Malware relationship analysis.
- Natural language extraction.
- Threat-actor profiling.
- Infrastructure relationship discovery.
- Behavioral pattern recognition.
- Anomaly detection.
- Threat confidence scoring.
- Intelligence freshness evaluation.
- Asset exposure mapping.

Contextual enrichment connects external intelligence with internal organizational information. An indicator becomes more actionable when the organization can determine whether it relates to a vulnerable or critical asset. This process enables intelligence to be transformed from general threat information into organization-specific risk information.

4.4 Risk Assessment, Prioritization, and Validation

Risk assessment combines threat intelligence with organizational exposure. Factors such as asset criticality, vulnerability severity, threat confidence, observed activity, exploit likelihood, and potential business impact can contribute to a risk score. High-priority intelligence can be forwarded to security operations teams for investigation, monitoring, patching, blocking, or other appropriate defensive actions.

Validation is required before significant automated actions are performed. Threat intelligence can contain false positives, outdated indicators, conflicting reports, or incorrect attribution. Analysts should therefore verify high-impact findings against internal telemetry and trusted intelligence sources. Feedback from investigations should also be incorporated into intelligence-management processes. This creates a continuous cycle in which security events improve intelligence quality and improved intelligence strengthens future detection and prevention.

5. Analysis

5.1 Threat Intelligence Sources and Analytical Value

Threat intelligence originates from diverse sources that provide different levels of context and reliability. Technical feeds can provide indicators of compromise, while vulnerability databases identify

weaknesses and security reports can provide information about adversarial campaigns. Internal security telemetry is especially important because it provides direct organizational context.

Table 1: Threat Intelligence Sources and Their Proactive Security Applications

Intelligence Source	Information Provided	Proactive Application	Key Limitation
Threat Intelligence Feeds	Indicators of compromise	Early indicator monitoring	Possible indicator overload
Vulnerability Databases	Vulnerability information	Patch prioritization	May lack organization-specific context
Security Advisories	Emerging threats and mitigations	Defensive planning	Variable publication timing
Incident Reports	Historical attack information	Threat-pattern analysis	Potential reporting bias
Malware Analysis	Malicious behavior and artifacts	Detection engineering	Resource intensive
Open-Source Intelligence	Public threat information	Emerging threat awareness	Reliability variation
Internal Security Logs	Organization-specific activity	Threat validation	Requires integrated infrastructure
Security Research	Technical attack knowledge	Control improvement	May require expert interpretation

Interpretation: Demonstrates that different intelligence sources serve complementary purposes. External feeds can provide early indicators, while vulnerability databases and security advisories support preventive action. Internal telemetry is particularly important because it establishes whether external intelligence is relevant to the organization's actual environment. The limitations of individual sources reinforce the need for multi-source correlation. A proactive cybersecurity program should therefore evaluate intelligence based on source reliability, freshness, contextual relevance, and potential operational impact rather than simply maximizing the quantity of collected information.

5.2 Threat Intelligence Analytics Techniques

Advanced analytics can transform large intelligence collections into structured relationships and prioritized security information. Machine learning supports classification and pattern discovery, while natural language processing extracts information from unstructured reports. Graph analytics can reveal relationships among threat actors, infrastructure, malware, vulnerabilities, and organizational assets.

International Journal of Innovative Computer Science and IT Research

Volume 01, Issue 05 – Sep-Oct 2025 • E-ISSN: 3067-1108 | P-ISSN: 3067-1094

Table 2: Analytical Techniques for Proactive Cybersecurity Management

Analytical Technique	Primary Function	Proactive Security Benefit	Limitation
Machine Learning	Indicator classification and prediction	Automated threat prioritization	Data dependency
Anomaly Detection	Identification of unusual patterns	Emerging-threat discovery	False positives
Natural Language Processing	Intelligence extraction	Rapid report analysis	Language/context limitations
Graph Analytics	Relationship discovery	Threat infrastructure mapping	Computational complexity
Clustering	Threat grouping	Campaign and malware discovery	Cluster interpretation
Statistical Analysis	Trend identification	Early risk indication	Limited complex reasoning
Risk Scoring	Threat prioritization	Resource allocation	Model calibration requirements

Interpretation: Indicates that proactive cybersecurity management benefits from combining multiple analytical techniques. Machine learning and clustering can process large intelligence collections, while NLP can convert unstructured reports into structured security information. Graph analytics can reveal relationships that are difficult to identify from individual indicators. Risk scoring then translates analytical findings into operational priorities. The combination of these techniques can reduce manual processing and improve decision quality, although continuous validation remains necessary because intelligence data and threat behaviors change over time.

5.3 Intelligence-Based Risk Prioritization

The operational value of threat intelligence depends strongly on prioritization. Security teams may receive thousands of indicators from multiple sources, but only a subset may be relevant to their environment. Prioritization should consider asset criticality, threat confidence, indicator freshness, vulnerability exposure, observed activity, and potential impact. A contextual risk score can combine these factors to identify threats requiring immediate attention.

For example, an indicator associated with an actively exploited vulnerability on a critical internet-facing system should receive higher priority than an outdated indicator with no matching organizational exposure. This approach enables organizations to allocate defensive resources according to actual risk.

International Journal of Innovative Computer Science and IT Research

Volume 01, Issue 05 – Sep-Oct 2025 • E-ISSN: 3067-1108 | P-ISSN: 3067-1094

6. Discussion

6.1 Threat Intelligence as a Proactive Security Capability

Threat intelligence can shift cybersecurity management from reactive incident handling toward anticipatory risk reduction. Intelligence about emerging vulnerabilities, adversarial techniques, malicious infrastructure, and attack campaigns can inform preventive security actions before direct compromise occurs. Security teams can use this information to improve detection rules, strengthen controls, patch exposed systems, and conduct focused investigations.

The effectiveness of this approach depends on contextual relevance. Organizations should avoid treating every external intelligence item as equally important. Instead, intelligence should be connected with internal assets, vulnerabilities, security observations, and business priorities. Contextual intelligence transforms generic threat information into actionable organizational risk information.

6.2 Role of AI and Advanced Analytics

Artificial intelligence can increase the scalability of threat intelligence operations by processing large quantities of structured and unstructured information. Machine learning can identify patterns among indicators, while NLP can extract security-relevant entities from lengthy reports. Graph analytics can further reveal relationships among adversarial infrastructure and attack activities.

However, automation should support rather than eliminate expert analysis. Incorrect model predictions can result in unnecessary blocking or missed threats. Analysts should therefore have the ability to inspect the evidence supporting automated recommendations. Transparent scoring and evidence-linked intelligence can improve operational trust.

6.3 Integration with Security Operations

Threat intelligence becomes more valuable when integrated with security operations platforms. Correlating intelligence with network traffic, endpoint events, authentication logs, vulnerability information, and incident records can provide a more complete representation of potential threats. Such integration allows organizations to determine whether an external indicator corresponds to activity occurring within their environment.Feedback from security operations can also improve intelligence quality. Confirmed incidents can validate indicators, while false positives can reduce the priority of unreliable information. A continuous feedback loop therefore supports the progressive improvement of both intelligence sources and analytical models.

7. Challenges

One major challenge is intelligence overload. Organizations can receive information from numerous threat feeds, reports, vulnerability sources, and security platforms. Processing every indicator equally can overwhelm security teams and reduce attention to high-value threats. Effective intelligence programs therefore require deduplication, confidence scoring, contextual enrichment, and risk-based prioritization. Without these capabilities, large quantities of intelligence may increase operational complexity rather than improve cybersecurity.

Another challenge is the reliability and freshness of intelligence. Threat indicators can become obsolete, infrastructure can change ownership, and malicious resources can be reused or abandoned. Inaccurate attribution can additionally lead to incorrect assumptions about threat actors. Intelligence

systems must therefore evaluate source reliability, timestamps, corroborating evidence, and confidence levels before intelligence is used for significant security decisions.

A third challenge involves adversarial manipulation and interoperability. Attackers may intentionally distribute false information, alter infrastructure, or manipulate observable indicators to confuse defenders. At the same time, different intelligence providers may use inconsistent formats and terminology. Standardization, secure information exchange, analytical validation, and continuous monitoring are therefore essential for maintaining the quality and reliability of threat intelligence operations.

8. Future Research

Future research should investigate adaptive threat intelligence platforms capable of continuously learning from new indicators, incidents, vulnerabilities, and adversarial behaviors. Continual learning could help models adapt to rapidly changing threat environments without requiring complete retraining after every update. Research should also examine methods for identifying when intelligence has become obsolete and automatically adjusting its operational priority.

Another important direction is graph-based threat intelligence reasoning. Knowledge graphs can represent relationships among threat actors, malware, infrastructure, vulnerabilities, attack techniques, and targeted assets. Advanced graph analytics may enable organizations to identify indirect relationships and emerging campaigns that cannot be discovered by examining isolated indicators. Research should investigate scalable graph architectures capable of handling large and continuously changing intelligence datasets.

Future studies should also focus on explainable threat intelligence analytics. Security analysts need to understand why an intelligence item received a particular risk score or why an automated system associated two threat indicators. Explainable models can provide supporting evidence, confidence information, and relationship paths. Human-in-the-loop evaluation should determine whether such explanations improve analyst decision-making, reduce investigation time, and increase trust in automated cybersecurity management systems.

9. Conclusion

Threat intelligence analytics provides an important foundation for proactive cybersecurity management by enabling organizations to transform fragmented information about vulnerabilities, adversaries, malicious infrastructure, attack techniques, and security events into actionable knowledge. Traditional reactive approaches frequently focus on identifying and containing incidents after suspicious activity has already occurred.

Threat intelligence introduces the possibility of anticipating potential threats and preparing defensive actions before they become significant security events. The framework presented in this study integrates intelligence collection, normalization, contextual enrichment, analytical processing, correlation, risk assessment, prioritization, and validation. This integrated approach emphasizes that the value of threat intelligence is determined not by the quantity of collected indicators but by their relevance, reliability, freshness, context, and ability to support meaningful security decisions.

Advanced analytics can significantly improve the scalability and effectiveness of threat intelligence operations. Machine learning can classify indicators and discover patterns, natural language

Volume 01, Issue 05 – Sep-Oct 2025 • E-ISSN: 3067-1108 | P-ISSN: 3067-1094

processing can extract security information from unstructured reports, anomaly detection can identify unusual trends, and graph analytics can reveal relationships among threat actors, malware, infrastructure, vulnerabilities, and organizational assets.

Risk scoring provides an additional mechanism for translating analytical findings into operational priorities. Nevertheless, automated intelligence analysis faces challenges involving incomplete datasets, intelligence overload, false positives, outdated indicators, attribution uncertainty, adversarial deception, and model drift. For this reason, automated analytical outputs should be treated as decision-support information rather than unquestionable conclusions. Security analysts should retain the ability to validate important findings and examine the evidence supporting automated recommendations. Future threat intelligence systems should emphasize adaptive analytics, explainability, interoperability, privacy, and continuous contextual enrichment.

Continual learning can help systems respond to evolving adversarial behavior, while knowledge-graph approaches can improve understanding of relationships among seemingly unrelated indicators. Integration with security operations, vulnerability management, endpoint monitoring, network analytics, and incident-response systems can further increase the operational value of intelligence. Organizations should also establish feedback mechanisms through which confirmed incidents, false positives, and analyst assessments continuously improve intelligence quality.

A mature threat intelligence capability should therefore operate as a continuous organizational process connecting external threat knowledge with internal exposure and business priorities. By combining high-quality intelligence, advanced analytics, risk-based prioritization, and expert validation, organizations can move toward more anticipatory cybersecurity management and improve their ability to identify, prepare for, and mitigate emerging cyber threats.

References

1. Sun, N., Ding, M., Jiang, J., Xu, W., Mo, X., Tai, Y., & Zhang, J. (2023). Cyber threat intelligence mining for proactive cybersecurity defense: A survey and new perspectives. *IEEE Communications Surveys & Tutorials, 25*(3), 1748–1774. https://doi.org/10.1109/COMST.2023.3273282.
2. Ainslie, S., Thompson, D., Maynard, S., & Ahmad, A. (2023). Cyber-threat intelligence for security decision-making: A review and research agenda for practice. *Computers & Security, 132*, 103352. https://doi.org/10.1016/j.cose.2023.103352.
3. Conde, D. J. S., Kämpf, N. L., Rößler-von Saß, D., Schurig, T., & Kliewer, N. (2024). Privacy-preserving data sharing: A systematic review and future research directions. *European Conference on Information Systems*.
4. SANS Institute. (2024). *SANS 2024 CTI Survey: Managing the Evolving Threat Landscape*. SANS Institute.
5. Recorded Future. (2024). *2024 State of Threat Intelligence*. Recorded Future.
6. Zhao, J., Yan, Q., Li, J., Shao, M., et al. (2020). TIMiner: Automatically extracting and analyzing categorized cyber threat intelligence from social data. *Computers & Security, 95*, 101867. https://doi.org/10.1016/j.cose.2020.101867.
7. Shin, B., & Lowry, P. B. (2020). A review and theoretical explanation of the cyberthreat-intelligence capability that needs to be fostered in information security practitioners and how this

can be accomplished. *Computers & Security, 92*, 101761. https://doi.org/10.1016/j.cose.2020.101761.

8. Wagner, T. D., Mahbub, K., Palomar, E., & Abdallah, A. E. (2019). Cyber threat intelligence sharing: Survey and research directions. *Computers & Security, 87*, 101589. https://doi.org/10.1016/j.cose.2019.101589.
9. Tounsi, W., & Rais, H. (2018). A survey on technical threat intelligence in the age of sophisticated cyber attacks. *Computers & Security, 72*, 212–233. https://doi.org/10.1016/j.cose.2017.09.001.
10. Samtani, S., Chinn, R., Chen, H., & Nunamaker, J. F. Jr. (2017). Exploring emerging hacker assets and key hackers for proactive cyber threat intelligence. *Journal of Management Information Systems, 34*(4), 1023–1053. https://doi.org/10.1080/07421222.2017.1394049.
11. Husari, G., Al-Shaer, E., Ahmed, M., Chu, B., Niu, X., et al. (2017). TTPDrill: Automatic and accurate extraction of threat actions from unstructured text of CTI sources. *Proceedings of the ACM Workshop on Automated Information Extraction*.
12. Barnum, S. (2014). *Standardizing Cyber Threat Intelligence Information with the Structured Threat Information eXpression (STIX)*. MITRE Corporation.
13. OASIS Cyber Threat Intelligence Technical Committee. (2016). *TAXII Version 1.1.1: Trusted Automated eXchange of Indicator Information*. OASIS.
14. Sarhan, I., & Spruit, M. (2021). Open-CyKG: An open cyber threat intelligence knowledge graph. *Knowledge-Based Systems, 233*, 107524. https://doi.org/10.1016/j.knosys.2021.107524.
15. Li, X., et al. (2022). A novel threat intelligence information extraction system combining multiple models. *Security and Communication Networks, 2022*, 8477260.
16. Suryotrisongko, H., Musashi, Y., Tsuneda, A., & Sugitani, K. (2022). Robust botnet DGA detection: Blending XAI and OSINT for cyber threat intelligence sharing. *IEEE Access, 10*, 34613–34624. https://doi.org/10.1109/ACCESS.2022.3162588.
17. Li, Y., et al. (2023). K-CTIAA: Automatic analysis of cyber threat intelligence based on a knowledge graph. *Symmetry, 15*(2), 337. https://doi.org/10.3390/sym15020337.
18. Ezra, L. A. (2023). Big data analytics in cyber threat intelligence: A comprehensive literature survey on methodologies, challenges, and future directions. *International Journal of Computer Engineering in Research Trends*.
19. Brown, R., & Lee, R. M. (2019). *The Evolution of Cyber Threat Intelligence (CTI): 2019 SANS CTI Survey*. SANS Institute.
20. CISA & MITRE. (2021). *Guidance for Using MITRE ATT&CK for Cyber Threat Intelligence*. Cybersecurity and Infrastructure Security Agency / MITRE.