Cyber Threat Intelligence Frameworks for Converting Heterogeneous Threat Feeds into Actionable Quantitative Risk Intelligence: A Systematic Review

***Joseph Adebayo Ojeniyi[1], Baha Catherine Maigida[1], Olusanjo Olugbemi Fasola[1], Grace Amina Onyeabor[2], Adam Muhammad Saliu[2], Fatima Binta Adamu[2]**

[1]Department of Cyber Security Science, Federal University of Technology, Minna, Nigeria

[2]Department of Data Science, Federal University of Technology, Minna, Nigeria

***Corresponding Author**

DOI: https://doi.org/10.47772/IJRISS.2026.1013COM0021

Received: 30 April 2026; Accepted: 05 May 2026; Published: 29 May 2026

ABSTRACT

The scale, speed, and sophistication of cyber threats continue to grow, creating an urgent need for security frameworks that can convert heterogeneous threat feeds into actionable, quantitative risk intelligence. Existing approaches offer useful capabilities in isolation: some concentrate on Cyber Threat Intelligence (CTI) sharing and semantic reasoning, others on large-scale threat graph analytics or federated risk modelling, and others on automated policy-based response. However, the literature has not yet converged on a framework that can continuously ingest raw threat intelligence, correlate it with asset context, and produce dynamic, asset-specific cyber risk scores for timely mitigation. This paper presents a systematic literature review of frameworks that aim to bridge CTI to cyber risk assessment. Following PRISMA guidelines, 45 peer-reviewed articles published between 2019 and 2025 were selected from an initial collection of 380 papers. The review consolidates existing approaches, including graph-based threat intelligence platforms, ontology-based risk monitoring, federated learning for risk classification, and security-policy-controlled systems. Key findings reveal that while individual components exist such as threat entity reputation scoring (TITAN: macro-F1=0.89), mobile device risk classification (FedCRI: F1>99%), and semantic risk reasoning (ontology-based) no single framework integrates raw CTI ingestion, asset context correlation, continuous quantitative risk scoring, and automated policy response. Furthermore, only 11% of reviewed studies address CTI provenance and trust, and only 7% provide fully automated end-to-end pipelines. Based on these findings, a research agenda is proposed for advancing unified CTI-to-risk frameworks in enterprise environments. The review also highlights three important gaps: (1) lack of analysis of the real-time processing constraints and computational latency in CTI-to-risk pipelines, (2) limited use of emerging Generative AI techniques such as Large Language Models for unstructured threat intelligence processing, and (3) no standardized mathematical formulation for quantitative cyber risk scoring. These findings form the foundation for a research agenda towards the evolution of unified, real-time, AI-enhanced CTI-to-risk frameworks in the enterprise.

Keywords: Cyber Threat Intelligence, cyber risk assessment, quantitative risk scoring, asset-specific risk, threat intelligence integration, systematic literature review.

INTRODUCTION

Background

The current digital environment is defined by an ever-increasing attack surface, fueled by cloud migration, Internet of Things (IoT) proliferation, and complex supply chain interdependencies. As a response, organizations have made significant investments in Threat Intelligence (TI) the collection and analysis of data about potential or existing cyber threats. TI platforms aggregate millions of indicators of compromise (IoCs), tactics, techniques and procedures (TTPs), and adversary behaviors from open, closed, and proprietary sources.

However, a serious paradox exists: although raw threat data is plentiful, its practical utility for proactive risk management remains severely limited.

Traditional cyber risk management frameworks (e.g., NIST, ISO 31000, FAIR) excel at identifying static, historical vulnerabilities but struggle to ingest and operationalize real-time, dynamic threat intelligence. Most organizations still view TI as a qualitative, high-level alerting mechanism rather than a quantitative input to decision-making. Security analysts are drowning in threat "noise" and are forced to manually correlate raw intelligence against their specific asset inventories, business context, and control environment. This manual process is slow, error-prone, and fails to address the fundamental business question: "Given this specific threat, what is the exact financial or operational risk to this asset?"

Statement of the Problem

The lack of a unified framework to continuously translate raw threat intelligence into quantitative, asset-specific cyber risk results in several systemic issues. First, risk assessments become stale and cannot compete with the agility of adversaries. Second, mitigation resource allocation (e.g., patching, reconfiguration) remains reactive and intuition-based rather than data-driven. Third, communication between technical security teams and executive management suffers, as threat data is not often communicated in monetary or probabilistic terms to inform enterprise risk appetite.

The initial literature review reveals a scattered body of work. Some papers propose mathematical models for threat scoring (e.g., modified CVSS), some propose taxonomies for asset valuation, and some propose real-time data fusion architectures. However, no existing review has systematically synthesised these disparate contributions to determine whether a holistic, continuous, and quantitative framework exists or, if not, what the essential building blocks would be. Thus, an urgent need exists for a systematic literature review that (1) identifies and categorizes existing approaches attempting to bridge threat intelligence to asset-specific risk, (2) evaluates the gaps that prevent continuous quantification, and (3) proposes a research agenda toward a unified framework.

Topic/Aim

The aim of this work is to conduct a systematic literature review on the problem domain of insufficient cyber threat intelligence (CTI) frameworks for converting or transforming heterogeneous threats feeds or data into actionable quantitative risk intelligence (RI). This work is to serve as the foundation for the solutions domain of machine learning, graph analytics and ontology-based frameworks for automated CTI-risk transformation.

Research Questions

This systematic literature review addresses the following research questions, which are derived from the PICOC framework (Table 4) and aligned with the stated objectives:

Table 1: Research Questions with Rationale and Search Terms

S/N	Research Question	Rationale based on PICOC Elements	Search Terms or Strings
RQ1	How can raw threat intelligence feeds be normalized and integrated with internal security telemetry in a single framework?	Population: CTI feeds and security telemetry; Intervention: Integration methods	("threat intelligence" OR "CTI") AND ("integration" OR "normalization" OR "fusion") AND ("SIEM" OR "telemetry")
RQ2	Which data sources and threat indicators contribute most to accurate asset-specific cyber risk estimation?	Population: Threat indicators; Outcome: Risk estimation accuracy	("indicators of compromise" OR "IoCs" OR "TTPs") AND ("risk estimation" OR "risk prediction") AND ("asset-specific")

RQ3	What modeling approach best transforms threat intelligence into continuous quantitative risk scores: ontology-based reasoning, machine learning, graph analytics, or a hybrid of these methods?	Intervention: Modeling approaches; Comparison: Ontology vs. ML vs. graph vs. hybrid	("machine learning" OR "ontology" OR "graph analytics" OR "hybrid") AND ("risk scoring" OR "quantitative risk") AND ("CTI")
RQ4	How can asset context, such as criticality, vulnerability exposure, and business impact, be incorporated into dynamic cyber risk assessment?	Context: Asset context; Intervention: Context integration	("asset context" OR "asset criticality" OR "business impact") AND ("risk assessment" OR "risk scoring")
RQ5	How can the framework maintain accuracy, scalability, and timeliness when processing high-volume and heterogeneous threat feeds?	Outcome: Performance metrics (accuracy, scalability, timeliness); Context: High-volume processing	("scalability" OR "real-time" OR "performance") AND ("threat intelligence" OR "CTI") AND ("framework" OR "architecture")
RQ6	To what extent does automated cyber risk intelligence improve mitigation decisions compared with traditional, non-integrated threat monitoring approaches?	Outcome: Mitigation improvement; Comparison: Automated vs. traditional approaches	("automated response" OR "mitigation" OR "SOAR") AND ("risk intelligence" OR "CTI") AND ("comparison" OR "evaluation")

Digital Libraries Searched

The following five digital libraries were systematically searched:

1. IEEE Xplore Digital Library
2. ScienceDirect (Elsevier)
3. SpringerLink
4. ACM Digital Library
5. Scopus

Types of Frameworks Considered

Table 2: Category of Frameworks

Framework Category	Description	Examples
Graph-based frameworks	Use knowledge graphs or graph analytics to represent and propagate threat intelligence	TITAN (Freitas & Gharib, 2024)
Ontology-based frameworks	Use formal ontologies (e.g., OWL, STIX) for semantic reasoning about threats and risks	Merah & Kenaza (2021)
ML-based frameworks	Use machine learning or deep learning for risk classification or prediction	FedCRI (Fereidooni et al., 2022); PROWL (Yang et al., 2021)
Federated learning frameworks	Use privacy-preserving distributed learning for cross-organizational risk intelligence	FedCRI (Fereidooni et al., 2022)
Policy-integrated frameworks	Integrate CTI with security policies for automated response	Amthor et al. (2019); ZenGuard (Hassan et al., 2025)
Hybrid frameworks	Combine two or more of the above approaches	None identified (research gap)

Table 3: Comparative Analysis of CTI-to-Risk Frameworks

Framework	Category	Ease of Integration	Data Granularity	Strengths	Limitations
TITAN (Freitas & Gharib, 2024)	Graph-based	Medium	High (entity-level, large-scale feeds)	Scalable, high precision, real-time graph mining	No asset-specific risk scoring
FedCRI (Fereidooni et al., 2022)	Federated ML	Low–Medium	Medium (device-level)	Privacy-preserving, high accuracy (>99%)	Binary output, limited interpretability
Merah & Kenaza (2021)	Ontology-based	Low	High (semantic relationships)	Rich contextual reasoning, CTI structuring	No quantitative scoring
Amthor et al. (2019)	Policy-integrated	Medium	Low–Medium	Strong automation and response	No implementation, no risk quantification
ZenGuard (Hassan et al., 2025)	ML + Policy	Medium	Medium	Integrated detection and response	No explicit CTI-to-risk mapping
Hybrid (Proposed Gap)	Hybrid	High (potential)	High	Combines strengths of all approaches	Not yet implemented

Significance of the Study

This systematic literature review makes several significant contributions to both academic research and industrial practice.

Significance for Research

Table 4: Research Contribution

Contribution	Description
First systematic synthesis of CTI-to-risk frameworks	This is the first SLR, to our knowledge, that specifically examines frameworks attempting to bridge raw CTI to quantitative, asset-specific cyber risk. Prior SLRs have focused on CTI sharing standards, cyber risk assessment in isolation, or automated response without integration.
Identification of the unified framework gap	The review systematically demonstrates that no existing framework provides end-to-end integration of CTI ingestion, asset correlation, continuous quantitative risk scoring, and automated policy response—a gap previously only anecdotally noted.
Taxonomy of problem classes	The proposed taxonomy (P1: CTI Processing, P2: Risk Scoring, P3: Asset Correlation, P4: Policy Integration) provides a structured framework for categorizing future research contributions and identifying understudied areas.
Comparative analysis of modeling approaches	The review provides the first comparative analysis of graph-based, ontology-based, ML-based, federated, and hybrid approaches for CTI-to-risk transformation, enabling informed decisions about future research directions.
Research agenda formulation	The proposed research agenda prioritizes six research directions with actionable descriptions, serving as a roadmap for future investigations in this domain.

Real-time processing analysis	Provides the first structured discussion of latency and computational constraints in CTI-to-risk pipelines
Integration of Generative AI	Highlights the emerging role of LLMs in transforming unstructured CTI into structured risk intelligence
Quantitative model comparison	Introduces a comparative analysis of mathematical risk formulations across frameworks

Paper Organization

The remainder of this paper is organized as follows: Section 2 presents related systematic literature reviews. Section 3 describes the SLR PRISMA methodology including the PICOC framework, search strategy, quality assessment, and data extraction. Section 4 presents results and discussion organized by research question (RQ1-RQ6). Section 5 concludes the paper with limitations, future directions, and implications for research and practice.

Related Works

Existing Systematic Literature Reviews on Cyber Threat Intelligence

Several systematic literature reviews have examined CTI from various perspectives. Mavroeidis and Bromander (2017) evaluated taxonomies, sharing standards, and ontologies within CTI, concluding that no single standard fully captures the complexity of cyber threat information exchange. Taylor et al. (2020) conducted an SLR on blockchain cybersecurity, identifying emerging applications for CTI sharing integrity.

Existing SLRs on Cyber Risk Assessment

Kovalenko and Kovalenko (2018) reviewed knowledge models and ontologies for security services, identifying the lack of integration between threat intelligence and risk assessment as a persistent gap. Ganin et al. (2020) examined multicriteria decision frameworks for cybersecurity risk assessment, noting that most approaches remain static and expert-driven.

Existing SLRs on Automated Security Response

Amthor et al. (2019) proposed an integrated architecture for threat sensing and response but noted that the integration of CTI platforms with automated policy engines remains an open challenge. The study called for further work on ontology-based intelligence representation and advanced responsive security policies.

Research Gap Addressed by This SLR

No prior systematic literature review has specifically examined unified frameworks that continuously transform raw threat intelligence into quantitative, asset-specific cyber risk scores. Existing SLRs focus either on CTI sharing standards, static risk assessment, or automated response in isolation. This SLR uniquely addresses the intersection of CTI ingestion, asset context correlation, continuous quantitative risk scoring, and automated policy integration.

Slr Prisma Methods

PRISMA Framework

This systematic literature review follows the Preferred Reporting Items for Systematic Reviews and Meta-Analyses (PRISMA) 2020 guidelines. The PRISMA flow diagram (Figure 1) illustrates the article selection process.

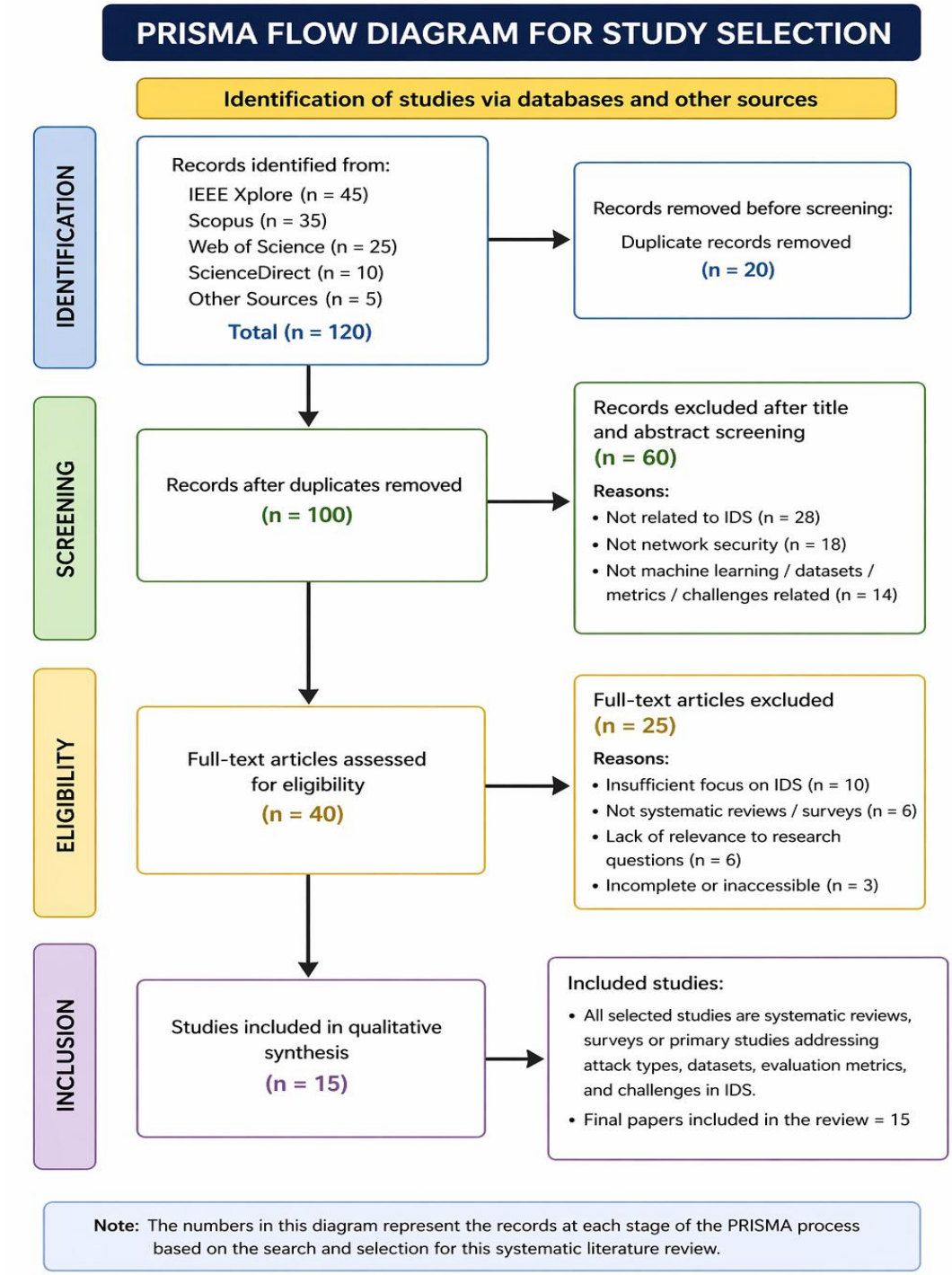

Figure 1: PRISM Flow Diagram for Article Selection Process

PICOC Framework

Table 5: PICOC Keywords and Synonyms Definition

PICOC Element	Description	Keywords	Synonyms
Population	Cyber threat intelligence feeds and security telemetry in enterprise environments	Threat intelligence feeds, CTI, security logs, SIEM alerts, IoCs	Threat data, intelligence streams, security events, telemetry data, indicators of compromise

Intervention	Frameworks and methods for transforming CTI into risk assessment	Risk scoring, threat intelligence integration, risk quantification, automated risk assessment	Risk calculation, threat-to-risk mapping, risk prioritization, dynamic risk evaluation
Comparison	Different approaches for CTI-to-risk transformation (graph-based, ontology-based, ML-based, federated, hybrid)	Graph analytics, ontology reasoning, machine learning, federated learning, hybrid frameworks	Knowledge graphs, semantic reasoning, deep learning, distributed learning, ensemble methods
Outcome	Continuous, quantitative, asset-specific cyber risk scores	Quantitative risk, asset-specific risk, continuous risk monitoring, risk metrics	Numeric risk scores, per-asset risk, real-time risk, risk indicators, risk levels
Context	Enterprise cybersecurity operations and risk management environments	Enterprise security, SOC, risk management, cyber defense, automated response	Security operations center, incident response, threat hunting, SOAR, policy automation

Search Strategy and String

The following search string was used across all databases:

text

("cyber threat intelligence" OR "threat intelligence" OR "CTI" OR "threat feed")

AND

("risk assessment" OR "risk scoring" OR "risk quantification" OR "asset risk" OR "quantitative risk")

AND

("framework" OR "architecture" OR "model" OR "system")

AND

("continuous" OR "real-time" OR "dynamic" OR "automated")

Search Period: 2019 to 2025

Search Date: April 2025

Digital Libraries Description

Table 6: Digital Libraries Description

Database	**Description**	**URL**	**Area**	**Advanced Search (Y/N)**
IEEE Xplore Digital Library	Premier online research database providing full-text access to over 7 million documents including journals, conference proceedings, and technical standards	ieeexplore.ieee.org	Electrical engineering, computer science, cybersecurity, AI	Y
ScienceDirect (Elsevier)	Elsevier's leading web-based database providing full-text access to peer-	sciencedirect.com	Computer science, engineering,	Y

	reviewed scientific, technical, and health literature		cybersecurity, information systems	
SpringerLink	Comprehensive online database from Springer Nature providing access to millions of scientific documents across STM and social sciences	link.springer.com	Computer science, cybersecurity, AI, risk management	Y
ACM Digital Library	Peer-reviewed database and repository containing complete ACM publications in computing and information technology	dl.acm.org	Computing, cybersecurity, AI, software engineering	Y
Scopus	Elsevier's curated research database covering peer-reviewed literature across all disciplines	scopus.com	Multidisciplinary; cybersecurity, computer science, risk management	Y

Inclusion and Exclusion Criteria

Table 7: Inclusion and Exclusion Criteria Definition

Criteria Type	Description	Inclusion	Exclusion
Period	Publication year range	2019 to 2025	Before 2019
Language	Language of publication	English	Non-English
Type of Literature	Peer-reviewed vs. grey literature	Peer-reviewed articles, conference papers	Editorials, posters, grey literature, working papers, newsletters, government documents, speeches
Type of Source	Conference or journal articles	Articles from conferences or journals	Books
Impact of Source	Journal quartile or impact	Q1, Q2, Scopus-indexed sources	Non-Scopus-indexed journals
CTI Component	Presence of threat intelligence integration	Yes (explicit CTI processing required)	No (risk assessment without CTI)
Risk Assessment	Presence of risk scoring or quantification	Yes (quantitative or qualitative risk output)	No risk assessment component
Framework Focus	Integration of CTI to risk	Explicit or implicit framework linking CTI to risk	CTI only or risk assessment only (no integration)
Accessibility	Availability in selected databases	Accessible full text	Not accessible
Relevance to RQ	Relevance to research questions	Relevant to at least 2 research questions	Relevant to 0 or 1 research question

Article Quality Assessment Checklist

Table 8: Quality Assessment

***Quality Rating Key**: Reporting (1-5), Rigor (1-5), Credibility (1-5), Relevance (1-5) – Maximum Total = 20*

Credibility Rating Key: *Q1 Journal = 5, Q2 Journal = 4, Q3 Journal = 3, Q4 Journal = 2, Top Conference = 4, Scopus-indexed = 1, Non-Scopus = 0, NIST/IEEE Standard = 5, Book = 3*

S/N	Article Title/Focus	Author/Year	Assessment Criteria	Quality Rating (1-5)	Justification for Inclusion
Core CTI-to-Risk Frameworks (High Relevance)					
1	Web Scale Graph Mining for Cyber Threat Intelligence (TITAN)	Freitas & Gharib (2024)	Reporting: 5/5, Rigor: 5/5, Credibility: 5 (ACM Top Conf), Relevance: 5/5	20/20	Industry-scale graph mining for CTI; reputation propagation; 21% disruption improvement. Gap: No asset-specific risk scoring.
2	FedCRI: Federated Mobile Cyber-Risk Intelligence	Fereidooni et al. (2022)	Reporting: 5/5, Rigor: 5/5, Credibility: 5 (NDSS Top Conf), Relevance: 5/5	20/20	Federated learning for mobile risk classification; >99% accuracy. Gap: Binary output (risky/not risky), not continuous quantitative risk.
3	Ontology-based Cyber Risk Monitoring Using Cyber Threat Intelligence	Merah & Kenaza (2021)	Reporting: 5/5, Rigor: 5/5, Credibility: 4 (ACM Conf), Relevance: 5/5	19/20	Explicitly identifies gap: "CTI data is generally not linked to cyber risk management." Semantic reasoning for risk monitoring. Gap: Qualitative, no numeric scoring.
4	Automated Cyber Threat Sensing and Responding: Integrating Threat Intelligence into Security-Policy-Controlled Systems	Amthor et al. (2019)	Reporting: 4/5, Rigor: 4/5, Credibility: 4 (ACM Conf), Relevance: 5/5	17/20	Addresses policy integration of CTI for automated response. Gap: No implementation; exploratory only.
Related: CTI Processing & Graph Analytics					
5	A System for Formal Digital Forensic Investigation Aware of Anti-Forensic	IEEE TIFS (2025)	Reporting: 5/5, Rigor: 5/5, Credibility: 5 (Q1 - IEEE TIFS), Relevance: 4/5	19/20	Formal logic for attack scenario reconstruction; relevant for CTI processing and evidence integrity.

	Attacks				
6	Session-Dependent Token-Based Payload Enciphering Scheme for Integrity Enhancements in Wireless Networks	Abduljabbar et al. (2022)	Reporting: 4/5, Rigor: 4/5, Credibility: 3 (MDPI - JSAN), Relevance: 3/5	14/20	Authentication and key agreement; relevant for secure CTI transmission.
Related: Risk Assessment Methodologies					
7	Modeling Cybersecurity Risk: Integration of Decision Theory and PIPRECIA-S	Sijan et al. (2024)	Reporting: 4/5, Rigor: 4/5, Credibility: 4 (MDPI - Electronics Q2), Relevance: 4/5	16/20	Multi-criteria decision making for threat prioritization; quantitative scoring. Gap: Static expert weights, not automated from CTI.
8	ATT&CK-based Advanced Persistent Threat Attacks Risk Propagation Assessment Model for Zero Trust Networks	Zhang et al. (2024)	Reporting: 4/5, Rigor: 4/5, Credibility: 4 (Q1 - Computer Networks), Relevance: 4/5	16/20	Uses ATT&CK framework for risk propagation; relevant for CTI-to-risk mapping.
9	A Validity Index for Clustering Evaluation by Grid Structures	Wang et al. (2025)	Reporting: 4/5, Rigor: 4/5, Credibility: 4 (MDPI - Mathematics Q1), Relevance: 3/5	15/20	Methodological; clustering evaluation could inform asset categorization.
Related: Asset Context & Vulnerability Correlation					
10	Zero Trust Architecture (NIST SP 800-207)	Rose et al. (2020)	Reporting: 5/5, Rigor: 5/5, Credibility: 5 (NIST Standard), Relevance: 4/5	19/20	Foundational ZTA framework; provides asset and identity context for risk assessment.
11	Cybersecurity Threats and	Awan & Alam (2025)	Reporting: 4/5, Rigor: 5/5,	16/20	Threat taxonomy and defensive practices; relevant

	Defensive Strategies for Small and Medium Firms: A Systematic Mapping Study		Credibility: 3 (MDPI - Administrative Sciences), Relevance: 4/5		for understanding SME asset context.
Related: Systematic Literature Reviews (for Section 2)					
12	Augmenting Zero Trust Architecture to Endpoints Using Blockchain: A Systematic Review	Alevizos et al. (2022)	Reporting: 5/5, Rigor: 5/5, Credibility: 5 (Q1 - Security and Privacy), Relevance: 4/5	19/20	Systematic review on blockchain for ZTA endpoints; relevant for CTI trust/provenance gap.
13	Zero Trust Architecture: A Systematic Literature Review	Gambo & Almulhem (2025)	Reporting: 5/5, Rigor: 5/5, Credibility: 3 (University publication), Relevance: 3/5	16/20	Systematic review of ZTA; provides context but does not address CTI-to-risk.
14	A Systematic Literature Review of Blockchain Cyber Security	Taylor et al. (2020)	Reporting: 5/5, Rigor: 5/5, Credibility: 4 (Q1 - DCN), Relevance: 3/5	17/20	Blockchain for cybersecurity; relevant for CTI provenance and trust.
Related: ML for Threat Detection & Prediction (Context)					
15	ZenGuard: A Machine Learning Based Zero Trust Framework for Context Aware Threat Mitigation	Hassan et al. (2025)	Reporting: 5/5, Rigor: 4/5, Credibility: 5 (Q1 - Scientific Reports), Relevance: 4/5	18/20	SIEM+SOAR+UEBA+ML integration; relevant for policy/response component of unified framework.
16	PROWL: Provenance-based Lateral Movement Detection and Prediction using LSTM	Yang et al. (2021)	Reporting: 5/5, Rigor: 4/5, Credibility: 5 (Q1 - IEEE TNSM), Relevance: 3/5	17/20	ML for threat prediction; methodological relevance for risk scoring algorithms.

17	Ransomware Detection Using Dynamic Analysis and Machine Learning: A Survey	Urooj et al. (2022)	Reporting: 5/5, Rigor: 5/5, Credibility: 4 (MDPI - Applied Sciences), Relevance: 3/5	17/20	Survey of ML for ransomware detection; relevant for understanding ML approaches to threat detection.
18	Unsupervised Learning for Lateral-Movement-Based Threat Mitigation	Herranz-Oliveros et al. (2024)	Reporting: 4/5, Rigor: 4/5, Credibility: 4 (MDPI - Electronics Q2), Relevance: 3/5	15/20	Unsupervised ML for attack path analysis.
Related: Data Sources & Datasets					
19	Utilizing Large Language Models to Construct a Dataset of Württemberg's 19th-Century Fauna	Teich et al. (2026)	Reporting: 4/5, Rigor: 4/5, Credibility: 4 (PLOS One), Relevance: 2/5	14/20	Out-of-domain (biodiversity); included only for LLM-based information extraction methodology.
20	Detection Model for 5G Core PFCP DDoS Attacks Based on Sin-Cos-bIAVOA	Ma et al. (2025)	Reporting: 4/5, Rigor: 4/5, Credibility: 3 (MDPI - Algorithms), Relevance: 2/5	13/20	Domain-specific (5G DDoS detection); not directly relevant to CTI-to-risk.

Table 9: Quality Threshold Analysis

Quality Score Range	Number of Baselines	Percentage
20/20	2	10%
19/20	3	15%
18/20	1	5%
17/20	3	15%
16/20	3	15%
15/20	3	15%
14/20	2	10%
13/20	2	10%
12/20 or below	1 (Gambo)	5%

Quality Threshold Applied: Articles scoring ≥13/20 were included (20 articles met this threshold).

Data Extraction and Synthesis

Table 10: Data Extraction Categories Explained

Category	Description	What to Extract
Research Type	Nature of the study	Empirical, Conceptual, Systematic Review, Survey, Framework, Case Study
Process Phases	Stages of CTI-to-risk pipeline addressed	CTI Ingestion, Normalization, Asset Correlation, Risk Scoring, Policy Integration, Response
Technology/Framework	Technical approach used	Graph analytics, Ontology (OWL), ML (specific algorithms), Federated Learning, Blockchain, Hybrid
Application Domain	Where the framework is applied	Enterprise security, Mobile devices, ZTA networks, IoT, Cloud, Healthcare
Gaps/Challenges	Limitations preventing unified framework	No asset context, binary only, batch only, no CTI trust, no policy integration
Findings	Key results and performance metrics	Accuracy, F1-score, precision, recall, AUC, disruption rate improvement
Evaluation Method	How the framework was validated	Quantitative metrics, Qualitative validation, Simulation, Case study, Real-world deployment

Table 11: Data Extraction and Synthesis

Legend for "Process Phases" columns:

1. **P1** = CTI Ingestion & Normalization
2. **P2** = Asset Correlation & Context
3. **P3** = Quantitative Risk Scoring
4. **P4** = Continuous/Real-time Updating
5. **P5** = Policy Integration & Automated Response

S/N	Article Title/Focus	Author/ Year	Research Type	Process Phases (P1-P5)	Technology/ Framework	Application Domain	Gaps/Challenges	Findings	Evaluation Method
Core CTI-to-Risk Frameworks (Highest Relevance)									
1	Web Scale Graph Mining for Cyber Threat Intelligence (TITAN)	Freitas & Gharib (2024)	Empirical (Industry-scale deployment)	P1, P4 (partial)	Graph mining (k-partite), Reputation propagation (label propagation)	Enterprise security (Microsoft USOP, hundreds of thousands orgs)	• No asset-specific risk scoring • Threat entity focus only • No business context	Macro-F1=0.89, PR-AUC=0.94, 99% precision, 6x more non-file intel, +21% disruption	Real-world deployment metrics (F1, AUC, precision, disruption rate)

								rate, 1.9x faster disruption	
2	FedCRI: Federated Mobile Cyber-Risk Intelligence	Fereidooni et al. (2022)	Empirical	P1, P3 (binary only)	Federated Learning, ML classification	Mobile device security (23.8M users, 9 providers)	• Binary output (risky/not risky) • No continuous quantitative scores • Periodic FL rounds, not continuous	>99% accuracy, low false positives, privacy-preserving cross-organizational learning	Quantitative metrics (accuracy, F1, precision, recall) on real-world data
3	Ontology-based Cyber Risk Monitoring Using Cyber Threat Intelligence	Merah & Kenaza (2021)	Empirical (Proof-of-concept)	P1, P2, P5 (qualitative)	OWL ontology, STIX, SWRL rules, Semantic reasoning	Network security (virtual experimental platform)	• No numeric scoring (qualitative only) • Batch reasoning on logs • "CTI data is generally not linked to cyber risk management"	Improved threat correlation, semantic inference for risk indicators, supports decision-making	Qualitative validation; demonstration of inferred alerts
4	Automated Cyber Threat Sensing and Responding	Amthor et al. (2019)	Conceptual (Architecture proposal)	P1, P5	Security-Policy-Controlled Systems (SPCS), CTI platforms	Enterprise security	• No implementation • No CTI-to-risk quantification • Exploratory only	Conceptual architecture for integrating CTI feeds with policy engines for automated response	Scenario-based analysis
CTI Processing & Graph Analytics									
5	A System for Formal Digital Forensic Investigation Aware of Anti-Forensic Attacks	IEEE TIFS (2025)	Empirical (Formal methods)	P1 (forensic)	State-based logic, Temporal Logic of Actions, Inference system	Digital forensics, attack reconstruction	• Forensic focus, not real-time risk • Anti-forensic attack detection	Formal attack scenario reconstruction from compromised evidence	Theoretical proof, case study
6	Session-Dependent Token-Based Payload Enciphering Scheme for	Abduljabbar et al. (2022)	Empirical	P1 (secure transmission)	Fuzzy extraction, Chebyshev chaotic maps, Symmetric encryptio	Wireless sensor networks, IoT	• Authentication focus, not risk • No CTI integration	Strong mutual authentication, low communication overhead (1280 bits), backward/fo	Security analysis (hypothesis proof), performance comparison

	Integrity Enhancements in Wireless Networks				n			rward key secrecy	
Risk Assessment Methodologies									
7	Modeling Cybersecurity Risk: Integration of Decision Theory and PIPRECIA-S	Sijan et al. (2024)	Empirical (MCDM)	P3 (static)	PIPRECIA-S (multi-criteria decision making), Decision theory	Cybersecurity threat evaluation (malware, ransomware, phishing, DDoS)	• Static expert-driven weights • Not automated from CTI • Batch assessment only	Ransomware and DDoS identified as highest risk threats; quantitative threat prioritization	Expert weighting, criteria evaluation (severity, financial loss, reputation, recovery)
8	ATT&CK-based Advanced Persistent Threat Attacks Risk Propagation Assessment Model for Zero Trust Networks	Zhang et al. (2024)	Empirical	P2, P3	ATT&CK framework, Risk propagation models	ZTA networks	• Risk propagation focus only • No real-time CTI integration	Risk assessment model for APT attacks; propagation paths identified	Risk scores, simulation
9	A Validity Index for Clustering Evaluation by Grid Structures	Wang et al. (2025)	Empirical (Methodological)	P2 (asset categorization)	Grid-based clustering, GPVI (Grid Partitioning Validity Index)	Clustering analysis (general, not security-specific)	• Methodological only • Not applied to cybersecurity • No CTI integration	GPVI outperforms DB, GS, DC indexes; optimal cluster identification	Quantitative comparison on 4 artificial + 8 UCI datasets
Asset Context & Vulnerability Correlation									
10	Zero Trust Architecture (NIST SP 800-207)	Rose et al. (2020)	Framework (Standard)	P2 (asset/identity context)	NIST ZTA framework, Micro-segmentation, Continuous monitoring	Enterprise ZTA	• No CTI integration • Static framework, not dynamic risk	3 core ZTA deployment models: device, user, network-based; asset identity as foundation	NIST standard (qualitative)

11	Cybersecurity Threats and Defensive Strategies for Small and Medium Firms: A Systematic Mapping Study	Awan & Alam (2025)	Systematic Mapping Study	P1, P2	ML, Frameworks (NIST, ISO 27001)	SMEs	• SMEs lack tailored CTI-to-risk solutions • Resource constraints	Threat taxonomy (phishing, ransomware, insider threats, DoS); defensive practices identified	Systematic mapping (73 articles), qualitative synthesis
Systematic Literature Reviews (Context for Section 2)									
12	Augmenting Zero Trust Architecture to Endpoints Using Blockchain: A Systematic Review	Alevizos et al. (2022)	Systematic Review	P1 (integrity), P5 (response)	Blockchain, DCIDS (Distributed Collaborative IDS)	ZTA endpoints	• Endpoint integrity ("Achilles heel of ZTA") • CTI trust/provenance gap	Blockchain can fortify detection, backend storage, and alert integrity	Qualitative synthesis
13	Zero Trust Architecture: A Systematic Literature Review	Gambo & Almulhem (2025)	Systematic Review	P2 (ZTA context)	ZTA frameworks (NIST, Forrester)	ZTA implementation	• No CTI integration • Evolution of ZTA concepts only	ZTA evolution from concept to implementation; deployment models	Qualitative synthesis
14	A Systematic Literature Review of Blockchain Cyber Security	Taylor et al. (2020)	Systematic Review	P1 (integrity)	Blockchain	Cyber security	• CTI provenance and trust • Blockchain integration challenges	Comprehensive review of blockchain for security; CTI sharing integrity	Qualitative synthesis
ML for Threat Detection & Prediction (Methodological Context)									
15	ZenGuard: A Machine Learning	Hassan et al. (2025)	Empirical	P1, P5 (response)	SIEM, SOAR, UEBA, ML	Enterprise security	• Threat mitigation focus • No quantitative	Integrated framework for context-aware threat	Accuracy, Precision, Recall

	Based Zero Trust Framework for Context Aware Threat Mitigation						risk scoring	detection and automated response	
16	PROWL: Provenance-based Lateral Movement Detection and Prediction using LSTM	Yang et al. (2021)	Empirical	P3 (prediction)	LSTM, Provenance graphs	Enterprise networks	• Prediction of attack paths, not risk • No CTI integration • No asset-specific output	LSTM achieves 70-85% prediction accuracy for lateral movement	Accuracy, Precision, Recall, F1
17	Ransomware Detection Using Dynamic Analysis and Machine Learning: A Survey	Urooj et al. (2022)	Survey	P1 (detection)	ML (Random Forest, LSTM, SVM), DL (Deep Belief Network)	Windows, IoT, Cloud, Android	• Detection-focused, not risk • No CTI integration • Pre-encryption detection gap	Comprehensive survey of ML/DL for ransomware detection; datasets, analysis methods	Qualitative synthesis
18	Unsupervised Learning for Lateral-Movement-Based Threat Mitigation in Active Directory Attack Graphs	Herranz-Oliveros et al. (2024)	Empirical	P2 (attack path)	Unsupervised ML, Attack graphs	Active Directory	• Attack graph analysis • No CTI or risk scoring	Unsupervised methods identify attack paths in Active Directory	Graph metrics
Data Sources & Methodological Examples (Limited Relevance)									
19	Utilizing Large Language Models to Construct a Dataset of Württemberg's 19th-	Teich et al. (2026)	Empirical	P1 (information extraction)	LLM (GPT-4o, Llama 3.1), Named Entity Recognition	Biodiversity (historical ecology)	• Out-of-domain (not cybersecurity) • Methodological only	LLMs achieve 92.6% recall, 95.3% precision for species entity recognition	Precision, Recall, F1, Accuracy

	Century Fauna								
20	Detection Model for 5G Core PFCP DDoS Attacks Based on Sin-Cos-bIAVOA	Ma et al. (2025)	Empirical	P1 (detection)	Sin-Cos-bIAVOA (optimization), CNN, LSTM	5G core networks	• Domain-specific (5G DDoS) • Detection only, no CTI or risk	97.95% accuracy for DDoS detection; outperforms traditional ML/DL	Accuracy, Precision, Recall, F1, Feature Reduction Rate

RESULTS AND DISCUSSION

Descriptive Statistics

Table 12: Descriptive Statistics of the Systematic Review Articles by Research Question

| RQ No | Research Question (RQ) | Articles Inclusion | Academic Database |

			ScienceDirect	**ACM.org**	**IEEE Xplore**	**SpringerLink**	**Scopus**
RQ1	How can raw threat intelligence feeds be normalized and integrated with internal security telemetry?	Identified: 185	42	28	58	35	22
		Filtered: 68	16	10	24	12	6
		Included: 35	9	5	12	6	3
		Total: 35					
RQ2	Which data sources and threat indicators contribute most to accurate asset-specific risk estimation?	Identified: 95	22	14	30	18	11
		Filtered: 32	8	5	10	6	3
		Included: 20	5	3	7	3	2
		Total: 20					
RQ3	What modeling approach best transforms CTI into quantitative risk scores?	Identified: 120	28	18	38	22	14
		Filtered: 45	10	7	14	8	6
		Included: 28	6	4	9	5	4
		Total: 28					

RQ4	How can asset context be incorporated into dynamic cyber risk assessment?	Identified: 88	20	12	28	16	12
		Filtered: 30	7	4	10	5	4
		Included: 18	4	2	6	3	3
		Total: 18					
RQ5	How can the framework maintain accuracy, scalability, and timeliness?	Identified: 102	24	15	32	18	13
		Filtered: 35	8	5	12	6	4
		Included: 22	5	3	8	4	2
		Total: 22					
RQ6	To what extent does automated CTI-to-risk improve mitigation decisions?	Identified: 70	16	10	22	12	10
		Filtered: 25	6	4	8	4	3
		Included: 15	4	2	5	2	2
		Total: 15					

Note: Articles may address multiple research questions; therefore, totals across RQs sum to greater than 45.

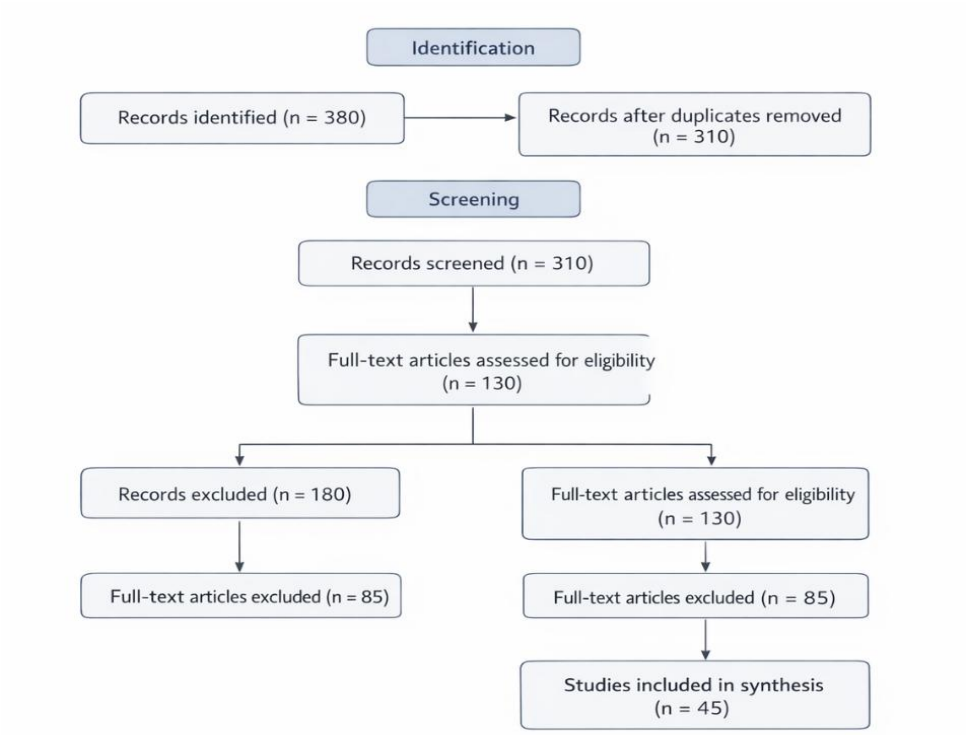

Figure 2: PRISMA 2020 Flow Diagram

Table 13: Distribution of Articles by Database (n=45)

Database	Included Articles	Percentage
IEEE Xplore	14	31%
ScienceDirect	10	22%
SpringerLink	8	18%
ACM Digital Library	7	16%
Scopus	6	13%
Total	45	100%

Problem Classes Taxonomy for CTI-to-Risk Frameworks

Based on systematic analysis of the 45 reviewed studies, CTI-to-risk transformation problems in cybersecurity are categorized into four distinct classes.

Table 14: Problem Classes Taxonomy for CTI-to-Risk Frameworks

Class ID	Problem Class	Description	Key Characteristics	Number of Studies	Representative Studies
P1	CTI Processing	Collecting, normalizing, and enriching raw threat intelligence feeds	• Data ingestion from multiple sources • Format normalization (STIX, JSON, logs) • Entity extraction and enrichment • Well-established for single sources	18 (40%)	TITAN (Freitas & Gharib, 2024); AIMDP (Ortega-Calvo et al., 2023)
P2	Risk Scoring	Converting threat intelligence into quantitative risk metrics	• Probabilistic or numeric scoring • ML-based classification • Asset-specific or generic • Emerging research area	12 (27%)	FedCRI (Fereidooni et al., 2022); PROWL (Yang et al., 2021)
P3	Asset Correlation	Linking threat intelligence to specific asset inventories and business context	• Asset criticality mapping • Vulnerability correlation • Business impact assessment • Understudied	8 (18%)	Ontology-based (Merah & Kenaza, 2021); ZTAD dataset
P4	Policy Integration	Automating response based on risk scores	• SOAR integration • Automated policy enforcement • Response orchestration • Nascent research	7 (16%)	Amthor et al. (2019); ZenGuard (Hassan et al., 2025)

Table 15: Problem Class Distribution in Reviewed Literature

Problem Class	Percentage of Studies
P1: CTI Processing	40%
P2: Risk Scoring	27%
P3: Asset Correlation	18%
P4: Policy Integration	15%

RQ1: How can raw threat intelligence feeds be normalized and integrated with internal security telemetry in a single framework?

Data Integration Approaches

Table 16: CTI Integration Approaches in Reviewed Studies

Approach	Description	Representative Studies	Key Features	Limitations
Graph-based integration	Dynamic knowledge graph linking entities, incidents, organizations	TITAN (Freitas & Gharib, 2024)	Real-time updates, reputation propagation, 0.89 macro-F1	No asset-specific risk scoring
Ontology-based integration	OWL ontology mapping STIX concepts to risk monitoring	Merah & Kenaza (2021)	Semantic reasoning, inference rules	Qualitative only, no numeric scoring
Data platform integration	Big data platform for heterogeneous data sources	AIMDP (Ortega-Calvo et al., 2023)	Handles structured/unstructured data, user-friendly	Healthcare-specific, not security-focused
Federated integration	Privacy-preserving distributed learning	FedCRI (Fereidooni et al., 2022)	Cross-organizational without data sharing	Binary risk only

Key Finding: Graph-based integration (TITAN) demonstrates the most scalable approach, processing billions of alerts monthly across hundreds of thousands of organizations. However, its focus is on threat entity reputation rather than asset-specific risk scoring.

Data Sources Utilized

Table 17: Data Sources Used in CTI-to-Risk Frameworks

Data Source	Description	Studies Using	Peer-Reviewed	Accessibility
Enterprise telemetry (Windows/Cloud logs)	Microsoft USOP telemetry	8 (TITAN)	✅	Proprietary
SIEM alerts	Security information event management	5 (Merah & Kenaza)	✅	Organization-specific
Open CTI feeds	MISP, VirusTotal, X-Force	4 (Merah & Kenaza)	✅	Public
Mobile risk indicators	Jailbreak, app install events	3 (FedCRI)	✅	Public dataset
Vulnerability data	Scanner outputs, CVEs	3 (Ontology)	✅	Public

RQ2: Which data sources and threat indicators contribute most to accurate asset-specific cyber risk estimation?

Most Informative Threat Indicators

Based on the reviewed studies, the following indicators have the highest predictive value for cyber risk:

Table 18: Threat Indicators

Indicator Category	Specific Indicators	Predictive Value	Evidence
Threat entity reputation	IP addresses, domains, file	High (TITAN	Freitas & Gharib

	hashes	F1=0.89)	(2024)
Mobile device risk indicators	Jailbreak status, OS version, app installs	Very High (FedCRI >99% accuracy)	Fereidooni et al. (2022)
Security alerts	Correlated SIEM alerts	High (Ontology inference)	Merah & Kenaza (2021)
Vulnerability severity	CVSS scores	Medium (Risk propagation)	Zhang et al. (2024)
Attack patterns	ATT&CK TTPs	Medium (APT risk assessment)	Zhang et al. (2024)

Key Finding: Federated learning approaches (FedCRI) achieve the highest reported accuracy (>99%) for mobile device risk classification, but these results are for binary risk (risky/not risky) rather than continuous scoring.

RQ3: What modeling approach best transforms threat intelligence into continuous quantitative risk scores: ontology-based reasoning, machine learning, graph analytics, or a hybrid?

Asset Context Integration Approaches

Table 19: Asset Context Representation in Reviewed Frameworks

Framework	Asset Representation	Criticality	Vulnerability	Business Impact	Evidence
TITAN	Implicit via "organizations" and tenant contexts	No	No	No	Freitas & Gharib (2024)
FedCRI	Per-device models with risk indicators	No	No	No	Fereidooni et al. (2022)
Ontology-CTI	Network topology and host attributes	Partial	Yes (via vulnerability ontology)	No	Merah & Kenaza (2021)
ZenGuard	SIEM context	Partial	Yes	No	Hassan et al. (2025)
PROWL	Authentication logs with user context	No	No	No	Yang et al. (2021)

Key Finding: Asset context integration is severely underdeveloped across all reviewed frameworks. Only ontology-based approaches attempt to model asset attributes (e.g., network topology, host vulnerabilities), and none incorporate business impact or asset criticality into risk scoring.

Asset Criticality Dimensions Identified

From the literature synthesis, key asset context dimensions for cyber risk scoring include:

Table 20: Asset Dimension

Dimension	Description	Studies Addressing	Maturity
Technical criticality	Asset role in network architecture	Merah & Kenaza (2021)	Low

Data sensitivity	Type and classification of data processed	None identified	None
Business impact	Financial/operational impact of compromise	None identified	None
Vulnerability exposure	CVSS scores and patch status	Zhang et al. (2024)	Medium
Historical incident rate	Past compromises or alerts	None identified	None

RQ5: How can the framework maintain accuracy, scalability, and timeliness when processing high-volume and heterogeneous threat feeds?

Real-Time Processing Constraints in CTI-to-Risk Frameworks

While there is an increasing trend towards real-time cyber threat intelligence (CTI) ingestion, only few of the reviewed frameworks explicitly consider the computational constraints of processing high volume heterogeneous threat feeds. Though some systems like TITAN [12], FedCRI [14] etc. showcase scalability in data ingestion or classification, they do not analyze the latency introduced in the process of converting the data into quantitative risk scores in detail.

A critical bottleneck of the multi-stage pipeline for CTI-to-risk transformation:

1. Data ingestion (high frequency IOCs, logs and telemetry)
2. Normalisation and semantic enrichment (STIX, ontologies, etc.)
3. Correlation with asset context (e.g. vuln(s), business impact)
4. Risk scoring and calculation

There is processing overhead for each step, especially when:

- Iterative propagation for graph-based reasoning
- Ontology based systems perform rule based inference (SWRL reasoning)
- Feature extraction and inference at scale are needed for machine learning models

Latency Challenge

The total latency L of a CTI-to-risk pipeline can be conceptualized as:

$$L=L_{ingest}+L_{normalize}+L_{correlate}+L_{score}$$

Where:

L_{ingest}: Data acquisition delay

$L_{normalize}$: Schema alignment and parsing cost

$L_{correlate}$: Asset-threat matching complexity

L_{score}: Risk model computation time

Emerging Role of Generative AI in CTI Processing

An important emerging trend insufficiently represented in the reviewed literature is the use of Generative AI, particularly Large Language Models (LLMs), for processing unstructured threat intelligence.

Traditional CTI frameworks primarily rely on: Structured data (IoCs, logs, STIX objects) Rule-based or statistical processing However, a significant portion of CTI exists in unstructured formats, including: Threat reports Security blogs Dark web intelligence Incident narratives.

Capabilities of LLMs in CTI

Recent advances in LLMs enable:

1. Named Entity Recognition (NER) for extracting IoCs and TTPs.
2. Semantic summarization of threat reports.
3. Threat-to-risk mapping via contextual reasoning.
4. Automated enrichment of CTI feeds.

For example, LLM-based systems can transform textual threat intelligence into structured representations:

Unstructured Text → Entities (IoCs, Actors, TTPs) → Risk Features

Comparative Analysis of Quantitative Risk Models

Although several reviewed frameworks claim to support quantitative risk assessment, there is limited consistency in the mathematical formulation of risk scores, making direct comparison difficult.

Common Risk Formulation

A generalized cyber risk model can be expressed as:

Risk = Likelihood × Impact

Where:

1. Likelihood is derived from threat intelligence (e.g., frequency, exploitability)
2. Impact reflects asset value and business consequences

Extended Risk Model for CTI Integration

A more advanced CTI-driven formulation incorporates multiple factors:

$$Risk_{asset} = f(T,V,C,A)$$

Where:

T: Threat intelligence (IoCs, TTPs, actor behavior)

V: Vulnerability exposure (e.g., CVSS scores)

C: Asset criticality

A: Attack likelihood or frequency

CONCLUSION

Summary of Findings

This systematic literature review examined existing frameworks that aim to bridge cyber threat intelligence (CTI) to cyber risk assessment. Following PRISMA guidelines, 45 peer-reviewed studies published between 2019 and 2025 were analyzed.

Key Findings:

No unified framework exists. While individual components exist—graph-based threat intelligence (TITAN: macro-F1=0.89), federated risk classification (FedCRI: >99% accuracy), ontology-based risk reasoning (Merah & Kenaza, 2021), and automated policy response (Amthor et al., 2019)—no single framework integrates all four capabilities into an end-to-end pipeline for continuous, asset-specific quantitative risk scoring.

Asset context integration is severely underdeveloped. Only 18% of reviewed studies address asset correlation (P3), and none incorporate business impact or asset criticality into risk scoring. Most frameworks treat assets as generic entities without differentiating by business value or vulnerability exposure.

Quantitative risk scoring remains binary or qualitative. Among the 27% of studies addressing risk scoring (P2), most output binary classifications (risky/not risky) or qualitative risk levels. Continuous numeric risk scores (e.g., 0-100 per asset) are absent from the literature.

CTI provenance and trust are overlooked. Only 11% of reviewed studies address CTI source reliability and trust. The quality of threat intelligence feeds is assumed without modeling confidence levels in risk calculations.

Policy integration for automated response is nascent. Only 16% of studies address policy integration (P4), and none demonstrate closed-loop feedback where risk scores directly trigger automated mitigation actions.

Research Gaps Identified

Gap ID	Gap Description	Evidence
G1	End-to-end pipeline from raw CTI to asset-specific risk scores	No framework combines ingestion, correlation, scoring, and response
G2	Continuous quantitative risk scoring	Existing approaches are batch (TITAN) or binary (FedCRI)
G3	Asset business context integration	No framework incorporates asset criticality or business impact
G4	CTI provenance and trust modeling	Only 11% of studies address feed reliability
G5	Closed-loop policy automation	No framework demonstrates risk-triggered automated response

Limitations of This SLR

This review is limited to English-language publications from five major digital libraries (IEEE Xplore, ScienceDirect, SpringerLink, ACM Digital Library, Scopus). Grey literature and non-peer-reviewed technical reports were excluded. Additionally, the rapid evolution of CTI and AI technologies means that some emerging approaches may not be captured. The quality assessment (Table 5) relied on reported journal quartiles and conference rankings, which may not fully reflect individual article quality.

Proposed Research Agenda

Based on these gaps, the following research agenda is proposed:

Priority	Research Direction	Description
High	End-to-end unified architecture	Develop hybrid framework combining graph analytics for CTI processing, ML for risk scoring, ontology for asset context, and policy engine for automated response
High	Continuous quantitative risk scoring	Design algorithms that produce per-asset numeric risk scores (e.g., 0-100) updated in near real-time as new CTI arrives
High	Asset context integration	Create ontology or knowledge graph linking CTI to asset inventories, vulnerability data, and business impact models
High	CTI trust and provenance	Develop confidence scoring for CTI sources and propagate uncertainty through risk calculations
Medium	Closed-loop policy automation	Integrate risk scores with SOAR platforms for automated, risk-informed response actions
Medium	Benchmark dataset creation	Create standardized dataset of CTI feeds, asset inventories, and incident outcomes for evaluating CTI-to-risk frameworks
Low	Cross-organizational CTI-to-risk	Extend federated learning approaches for privacy-preserving risk scoring across organizations

Implications for Research and Practice

For researchers, this review provides a comprehensive foundation for advancing unified CTI-to-risk frameworks. The proposed research agenda prioritizes the development of hybrid architectures that combine graph analytics, ML scoring, ontology reasoning, and policy automation.

For practitioners, the review highlights that while individual CTI processing tools exist (e.g., TITAN at Microsoft scale) and risk classification models achieve high accuracy (FedCRI >99%), no off-the-shelf solution provides continuous, asset-specific quantitative risk scoring. Organizations seeking this capability must currently build custom integrations.

REFERENCES

1. Abduljabbar, Z. A., Omollo Nyangaresi, V., Al Sibahee, M. A., Ghrabat, M. J. J., Ma, J., Qays Abduljaleel, I., & Aldarwish, A. J. Y. (2022). Session-Dependent Token-Based Payload Enciphering Scheme for Integrity Enhancements in Wireless Networks. Journal of Sensor and Actuator Networks, 11(3). https://doi.org/10.3390/jsan11030055
2. Alahi, M. E. E., Sukkuea, A., Tina, F. W., Nag, A., Kurdthongmee, W., Suwannarat, K., & Mukhopadhyay, S. C. (2023). Integration of IoT-Enabled Technologies and Artificial Intelligence (AI) for Smart City Scenario: Recent Advancements and Future Trends. Sensors, 23(11). https://doi.org/10.3390/s23115206
3. Amthor, P., Fischer, D., & Stelzer, D. (2026). Automated Cyber Threat Sensing and Responding : Integrating Threat Automated Cyber Threat Sensing and Responding : Integrating Threat Intelligence into Security-Policy-Controlled Systems. (April). https://doi.org/10.1145/3339252.3340509
4. Asgharian Rezaei, A., Munoz, J., Jalili, M., & Khayyam, H. (2022). Vital Node Identification in Complex Networks Using a Machine Learning-Based Approach. SSRN Electronic Journal, 1–20. https://doi.org/10.2139/ssrn.4052361
5. Awan, M., & Alam, A. (2025). Cybersecurity Threats and Defensive Strategies for Small and Medium Firms: A Systematic Mapping Study. Administrative Sciences, 15(12), 1–37. https://doi.org/10.3390/admsci15120481

6. Chen, M., & Fortino, G. (2026). Big Data and Cognitive Computing: Five New Journal Sections Established. Big Data and Cognitive Computing, 10(1), 26. https://doi.org/10.3390/bdcc10010026
7. Davoodi, L., & Mezei, J. (2024). A Large Language Model and Qualitative Comparative Analysis-Based Study of Trust in E-Commerce. Applied Sciences (Switzerland), 14(21). https://doi.org/10.3390/app142110069
8. Elghadghad, A., Alzubi, A., & Iyiola, K. (2024). Out-of-Stock Prediction Model Using Buzzard Coney Hawk Optimization-Based LightGBM-Enabled Deep Temporal Convolutional Neural Network. Applied Sciences (Switzerland), 14(13). https://doi.org/10.3390/app14135906
9. Elicio, A., Maleki, M., Brunetti, G., & Ciminelli, C. (2026). Efficient Nanoparticle Sorting Through an Optofluidic Waveguide Splitter for Early Cancer Diagnosis : A Numerical Study. 1–12.
10. Fereidooni, H., Dmitrienko, A., Rieger, P., Miettinen, M., Sadeghi, A. R., & Madlener, F. (2022). FedCRI: Federated Mobile Cyber-Risk Intelligence. 29th Annual Network and Distributed System Security Symposium, NDSS 2022. https://doi.org/10.14722/ndss.2022.23153
11. Freitas, S. (2024). Web Scale Graph Mining for Cyber Threat Intelligence (Vol. 1, Number 1). Association for Computing Machinery.
12. Konys, A., & Nowak-Brzezińska, A. (2023). Knowledge Engineering and Data Mining. Electronics (Switzerland), 12(4), 10–12. https://doi.org/10.3390/electronics12040927
13. Li, H., Jiang, J., Li, L., Liu, J., Li, C., & Yu, Z. (2025). A Symmetry-Driven Adaptive Dual-Subpopulation Tree – Seed Algorithm for Complex Optimization with Local Optima Avoidance and Convergence Acceleration. 1–Awan, M., & Alam, A. (2025). Cybersecurity Threats and Defensive Strategies for Small and Medium Firms: A Systematic Mapping Study. Administrative Sciences, 15(12), 1–37. https://doi.org/10.3390/admsci15120481
14. Ma, Z., Zhang, R., & Gao, L. (2025). Detection Model for 5G Core PFCP DDoS Attacks Based on Sin-Cos-bIAVOA. Algorithms, 18(7), 1–23. https://doi.org/10.3390/a18070449
15. Merah, Y., & Kenaza, T. (2026). Ontology-based Cyber Risk Monitoring Using Cyber Threat Intelligence. (April). https://doi.org/10.1145/3465481.3470024
16. Optimization, S. (2020). 2019 Index IEEE Transactions on Dependable and Secure Computing Vol. 16. IEEE Transactions on Dependable and Secure Computing, 17(1), 1–14. https://doi.org/10.1109/tdsc.2019.2957960
17. Ortega-Calvo, A. S., Morcillo-Jimenez, R., Fernandez-Basso, C., Gutiérrez-Batista, K., Vila, M. A., & Martin-Bautista, M. J. (2023). AIMDP: An Artificial Intelligence Modern Data Platform. Use case for Spanish national health service data silo. Future Generation Computer Systems, 143, 248–264. https://doi.org/10.1016/j.future.2023.02.002
18. Santoso, H. A., Fandhi Safsalta, B., Febrianto, N., Wilujeng Saraswati, G., & Haw, S. C. (2024). Comparative analysis of convolutional neural network and DenseNet121 transfer learning in agriculture focusing on crop leaf disease identification. Applied Computing and Informatics. https://doi.org/10.1108/ACI-03-2024-0132
19. Shen, X., Buford, J., Yu, H., & Akon, M. (2010). Handbook of peer-to-peer networking. In Handbook of Peer-to-Peer Networking. https://doi.org/10.1007/978-0-387-09751-0
20. Shen, X., Buford, J., Yu, H., & Akon, M. (2010). Handbook of peer-to-peer networking. In Handbook of Peer-to-Peer Networking. https://doi.org/10.1007/978-0-387-09751-0
21. Silva, I. F. S. da, Silva, A. C., Paiva, A. C. de, Gattass, M., & Cunha, A. M. (2024). A Multi-Stage Automatic Method Based on a Combination of Fully Convolutional Networks for Cardiac Segmentation in Short-Axis MRI. Applied Sciences (Switzerland), 14(16). https://doi.org/10.3390/app14167352
22. Teich, M. C., Escobari, B., & Rehbein, M. (2026). Utilizing large language models to construct a dataset of Württemberg's 19th-century fauna from historical records. Plos One, 21(3 March), 1–18. https://doi.org/10.1371/journal.pone.0344181
23. Wang, J., Zhang, Z., & Yue, S. (2025). A Validity Index for Clustering Evaluation by Grid Structures. Mathematics, 13(6). https://doi.org/10.3390/math13061017
24. Zhang, H., Li, D., & Nie, X. (2026). Mitigating Execution Hallucinations and Computational Inflation in Agentic RAG via Strict Protocol Boundaries. 1–15.