Journal of Global Research in Electronics and Communication (JGREC)
Volume 2 | Issue 11 | November 2026 | Pages 01–07
DOI: https://doi.org/xxxxxxxxxxxxx
e-ISSN: 2321-3175
REVIEW ARTICLE OPEN ACCESS Available online: https://jgrec.info/index.php/jgrec/index

An Analysis of Large Language Models for Cyber Threat Intelligence and Incident Response

Mr. Mohit Sahu
Assistant Professor
Mandsaur University, Mandsaur
Department of Computer Sciences and Applications
mohit.sahu@meu.edu.in

Corresponding Author: * Mohit Sahu (mohit.sahu@meu.edu.in)

Received: 2 November 2026 | **Revised:** 5 November 2026 | **Accepted:** 12 November 2026

***Abstract*—Cyber Threat Intelligence (CTI) and Incident Response (IR) are indispensable for the identification, analysis, and mitigation of evolving cyber threats. Malware, DOS assaults, vulnerabilities, and complex hostile activities are on the rise, necessitating automated and intelligent cybersecurity solutions. One intriguing technology that has recently surfaced is the Large Language Model (LLM). LLMs can handle large amounts of unstructured security data, identify vulnerabilities, analyses network traffic, and help incident response efforts. Extraction of threat intelligence, cyber threat analysis, vulnerability identification, intrusion detection, and security operations are the primary areas of focus in this examination of LLMs' function in CTI and IR. A unified taxonomy is considered across three dimensions: AIGC-driven cyber threats, LLM-enabled defensive capabilities, and security evaluation, red-teaming, and governance. The study also examines the incident response lifecycle, including preparation, detection and analysis, containment, eradication, recovery, and post-incident activities, and discusses how LLMs can support these stages. Furthermore, challenges related to hallucination, data quality, explainability, privacy, adversarial manipulation, reliability, and governance are highlighted. The review demonstrates that LLMs can strengthen CTI and IR by improving automation, analysis, decision support, and response efficiency while requiring robust validation and responsible deployment.**

***Keywords*—Cyber Threat Intelligence, Large Language Models, Incident Response, Threat Detection, Vulnerability Detection, Cybersecurity.**

I. INTRODUCTION

The rising frequency and sophistication of cyberattacks has raised the demand for effective cybersecurity measures, making proactive threat intelligence and advanced analytical approaches indispensable for defending digital systems and key assets. Cybersecurity generally refers to the techniques used to protect the cyber environment, including users, devices, networks, applications, and software, from cyberattacks [1][2]. Cyber Threat Intelligence (CTI) has become a cornerstone of modern cybersecurity, enabling organizations to anticipate threats and act proactively. With the increasing complexity of digital systems and the continuous evolution of attack techniques, traditional reactive approaches have become insufficient for protecting critical assets [3]. CTI combines the collection, analysis, and sharing of threat information, enabling organizations to respond quickly and accurately to emerging risks [4]. The use of machine learning algorithms to automate the examination of massive amounts of data has greatly enhanced danger detection. Traditional signature-based approaches are outperformed by algorithms like Convolutional Neural Networks (CNNs) and Support Vector Machines (SVMs) when it comes to detecting patterns and anomalies that suggest suspicious behavior [5]. Their adaptability also supports the detection of advanced threats, such as Advanced Persistent Threats (APTs), which often employ sophisticated techniques to evade conventional detection.

Incident Response (IR) typically follows a structured lifecycle consisting of detection, analysis, containment, eradication, recovery, and post-incident analysis. Traditional approaches rely heavily on signature-based detection, manual analysis, and human decision-making. Although signature-based solutions work well against known threats, they can't catch zero-day vulnerabilities or new types of assaults [6]. Moreover, the growing volume of security alerts can cause alert fatigue, making it difficult for analysts to prioritize and respond effectively [7]. Automated threat analysis, alarm prioritization, and assistance for proper reaction measures are hence necessary capabilities of intelligent systems.

Large Language Models (LLMs) are deep neural networks trained on large volumes of text to predict the next word or token. Their capabilities include language understanding, code generation, factual recall, and adaptation to different writing styles [8]. New capabilities, not seen in smaller models, have emerged in LLMs as their size and amount of training data have grown. These capabilities have made LLMs powerful tools for processing, generating, and understanding information across various domains [9]. In cybersecurity, their ability to analyze unstructured text, summarize information, identify relevant patterns, and generate contextual responses creates opportunities to enhance CTI analysis and support incident response. It is crucial to grasp the potential of LLMs

Copyright © 2026 The Author(s).
This is an open access article distributed under the terms of the Creative Commons Attribution 4.0 International (CC BY 4.0) License (https://creativecommons.org/licenses/by/4.0/), which permits unrestricted use, distribution, adaptation, and reproduction in any medium, provided the original author(s) and the source are properly credited.

J. Glob. Res. Elec. Comm., 2 (11):01-07
DOI: https://doi.org/xxxxxxxxxxxx

to enhance current cybersecurity operations by analyzing their capabilities and efficacy in CTI and IR.

A. *Structure of the Paper*

The paper is organized as follows: Section II presents Cyber Threat Intelligence, Section III discusses Applications of LLMs in Cyber Threat Intelligence, Section IV explains LLMs for Cyber Threat Intelligence and Incident Response, Section V presents the Literature Review, Section VI provides Conclusion and Future Work.

II. Cyber Threat Intelligence

In the realm of cybersecurity, Cyber Threat Intelligence (CTI) is the process of collecting, organizing, analyzing, and disseminating intelligence about threats to the security of organizations, governments, and industries. This information is useful in mitigating cyberattacks, as it provides stakeholders with valuable intelligence about potential threats and helps them proactively identify these threats and associated threat groups [10]. CTI is gathered by monitoring various open-source intelligence sources, forums, and the dark web, and contains information about Advanced Persistent Threat (APT) groups.

A. *Malware Attacks*

Malware is an umbrella word for a wide variety of harmful programs that are placed on end-user devices and servers. It is a prevalent cyber threat. There are several varieties of malware, but one of the most common is Android malware, which targets devices that use the Android operating system (AOS) [11][12]. Without the user's knowledge or permission, it can sneak into, harm, or exploit systems. Below, you'll find descriptions of the many sorts of malware, including but not limited to: spyware, adware, ransomware, scareware, backdoors, rootkits, trojan horses, viruses, and worms (Figure 1):

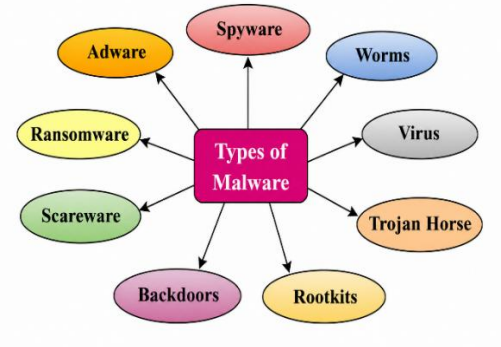

Fig. 1. Different Types of Malware

- **Spyware:** The purpose of this program is to keep tabs on people's internet behavior and record private data, such as their financial information. In addition to recording keystrokes, it has the ability to change device security settings and execute its tasks.
- **Adware:** This software is often bundled with other programs and automatically displays advertisements, mainly through web browsers. It is usually noticeable through frequent pop-up advertisements and may sometimes be associated with spyware.
- **Ransomware:** Software that encrypts data or limits system access and demands payment to restore it is known as malevolent software. It may threaten data deletion or leakage and often spreads by phishing emails, harmful downloads, or exploited vulnerabilities.
- **Scareware:** This malware uses deceptive warnings to frighten users into performing specific actions. It often displays false system alerts claiming that the device is compromised and requires a particular program for recovery, which may install malware when executed [13].
- **Backdoor:** Unauthorized access can be obtained through this malware by bypassing standard authentication mechanisms. It enables attackers to remotely access resources and execute system commands while remaining difficult to detect.
- **Rootkit:** Operating-system modifications are used by this malware to create hidden backdoors and enable unauthorized remote access. It may exploit vulnerabilities, modify system files, escalate privileges, and interfere with forensic or monitoring tools, making detection difficult.
- **Trojan Horse:** Harmful activities are performed by this malware while appearing legitimate to users. It commonly uses user permissions and may be disguised as images, audio files, or games. Unlike viruses, Trojans do not self-replicate but facilitate malware infiltration [14].
- **Virus:** This software often needs human input to activate, and it replicates by injecting its code into executable files or documents. Spreading via email, network shares, optical discs, or USB devices, it has the ability to alter or erase data.
- **Worms:** Independent replication allows this malware to spread rapidly from one system to another without continuous user interaction [15]. It commonly exploits system vulnerabilities, contains malicious code, and propagates across networks, sometimes alongside legitimate software or Trojan horses.

B. *Denial-of-Service (Dos) Attack*

A denial-of-service (DoS) assault is a type of network attack that is relatively easy to execute, even by a novice attacker. When a denial-of-service attack occurs, it stops users, devices, or apps from accessing network services [16]. Figure 2 shows that, in contrast to Distributed Denial of Service (DDoS) attacks, which aim to overwhelm a network, service, or website with a flood of traffic from multiple sources, botnets send out an overwhelming number of connection requests to the target system, making it inoperable:

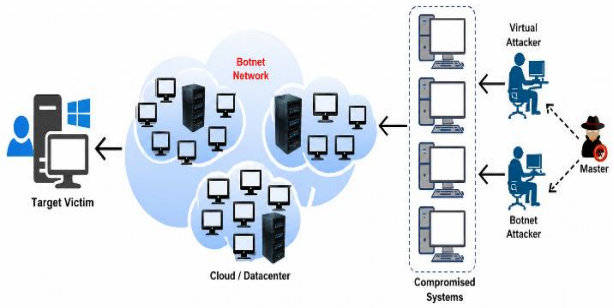

Fig. 2. Schematic Representation of Ddos Attack

- **Volumetric Attacks:** The goal of these assaults is to overwhelm the target's bandwidth by sending a deluge of traffic at it. Common instances include ICMP

DOI: https://doi.org/xxxxxxxxxxxx

floods, UDP floods, DNS amplification, NTP amplification, and others.

- **Protocol Attacks:** These attacks disrupt services by taking advantage of vulnerabilities in network protocols. These issues primarily revolve on the exhaustion of server or network resources. The ping of death and the SYN flood are two examples.
- **Application Layer Attacks:** These types of attacks are designed to target certain apps and drain server resources by mimicking real traffic patterns. Two such instances are HTTP flood and Slow Loris.

C. Cyber Threat Detection and Classification

Cybersecurity relies on threat detection and classification to discover and categories harmful behaviors that might jeopardize system availability, confidentiality, or integrity [17].

- **Threat Detection:** The goal of threat detection is to find instances of harmful or unauthorized behavior in a system by analyzing patterns of behavior, anomalies, or known signatures. It allows for quick responses by spotting questionable behaviors before they might cause significant harm.
- **Threat Classification:** Threat categorization, on the other hand, involves categorizing recognized threats based on their characteristics, attack routes, or likely outcomes. The first step is to classify the identified threat into one of several families, such as malware, spyware, trojans, ransomware, worms, etc. Precise categorization allows for the execution of focused defensive measures to successfully combat certain kinds of threats.

III. Applications of LLMs in Cyber Threat Intelligence

LLM models are a combination of AI algorithms and NLP techniques. They are powerful tools used across various industries to enhance language-related applications. They generate human-like text based on the context [18]. user inputs. They have improved chatbots, content generation platforms, virtual assistants and customer service automation.

A. Rationale for the Proposed Taxonomy

The motivation for the proposed taxonomy is threefold. First, existing surveys frequently examine offensive misuse, defensive applications, or ethical considerations of LLMs in isolation, resulting in fragmented insights that obscure the co-evolution of threats and countermeasures [19]. By explicitly integrating threat, defense, and evaluation dimensions, the proposed taxonomy captures their interdependencies and reflects the concurrent evolution of attacker innovation, defensive adaptation, and governance constraints.

B. AIGC-Driven Cyber Threats

The first dimension of the taxonomy captures how generative AI and LLMs expand the cyber threat surface by automating deception, lowering technical skill barriers, and enabling adaptive attacks at scale. Across the reviewed literature, AIGC-driven threats consistently emerge as a dominant research focus, reflecting widespread concern regarding the misuse potential of generative model [20]. Unlike conventional cyber threats, these attacks exploit linguistic fluency, contextual awareness, and automation, enabling adversaries with limited expertise to execute sophisticated campaigns [21].

C. LLM-Enabled Defensive Capabilities

The unified taxonomy, the second dimension captures how LLMs are operationalized as defensive instruments to support cybersecurity monitoring, analysis, and response. In contrast to threat-centric research, this body of work primarily conceptualizes LLMs as augmentative components embedded within existing security workflows rather than as fully autonomous decision-makers [22]. Across the 167 reviewed studies, defensive applications consistently cluster into three capability classes: (i) threat intelligence extraction and security operations support, (ii) secure coding, vulnerability assessment, and risk prediction, and (iii) anomaly detection, behavioral modelling, and policy reasoning.

D. Security Evaluation, Red-Teaming, and Governance

The third dimension of the unified taxonomy encompasses research focused on evaluating the trustworthiness, robustness, and governance readiness of LLM-enabled cybersecurity systems. Unlike threat- or defense-centric studies, which emphasize capability expansion, this dimension interrogates whether such systems can be safely, reliably, and legally deployed in security-sensitive environments [23]. Across the 167 analyzed studies, evaluation and governance emerge as indispensable complements to both offensive and defensive research, reflecting a growing consensus that unregulated or inadequately assessed LLM integration may introduce systemic risks that outweigh operational benefits.

E. Threat Intelligence

It is very difficult to extract information from a large number of threat intelligence documents. Some researchers turn to LLMs to organize and analyze these massive and cluttered data [24].

F. Vulnerability Detection

The main studies on vulnerability detection using LLMs (blur the concepts of “vulnerability” and “software defect” in this part). Through these studies, aim to shed light on the progress, challenges, and future directions of leveraging LLMs to enhance cybersecurity. Whether LLMs have the ability to detect vulnerabilities [25].

IV. LLMs for Cyber Threat Intelligence and Incident Response

CTI and IR are essential components of modern cybersecurity that help organizations identify, analyze, and respond to evolving cyber threats. While IR concentrates on identifying, examining, containing, and recovering from security incidents to reduce organizational harm and operational interruption, CTI offers useful information about threats, vulnerabilities, and attack patterns.

A. Incident Response Lifecycle

The Incident Response Lifecycle refers to an organization's structured response process for cybersecurity incidents. This lifecycle is essential for minimizing a cyber-attack's impact and restoring normal operations as quickly as possible in organizations. By following a systematic approach, organizations can address immediate threats and enhance their ability to prevent future incidents and cyber-

DOI: https://doi.org/xxxxxxxxxxxxx

attacks. The NIST breaks the cyber incident response lifecycle into four main stages: Preparation, Detection & analysis, Containment, eradication, & recovery, and Post-incident activity [26]. Figure 3 below shows the lifecycle of an incident response:

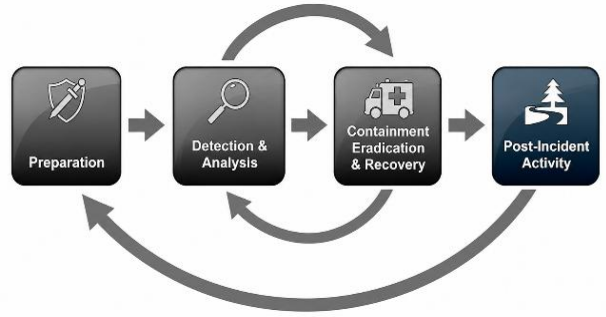

Fig. 3. Incident Response Life Cycle

1) Preparation

In the preparation phase, the possible incidents are evaluated and assessed to determine the potential impact and the steps that can be taken to reduce damage. With proper preparation, an organization could avoid severe financial losses, compliance issues, and long-term damage to its reputation [27]. The incident response team's primary goal during this initial phase is incident prevention. They work to protect the organization by executing asset inventory and ranking, risk assessments, security monitoring, vulnerability assessments, monitoring, planning, and training, among other tasks. This phase results in a clear incident response plan to identify, prioritize, and address security incidents.

2) Detection & Analysis

This stage involves identifying, investigating, and assessing suspicious activities or security incidents within an organization's network or systems. It ensures that potential security breaches are promptly addressed to minimize their impact. At this stage, a cyber-attack or threat is identified, and appropriate response procedures are initiated. Log monitoring, anomaly detection, and alerting systems are implemented with the principal goal of discovering security events or harmful actions, such as malware, data exfiltration, and unauthorized access. These methods facilitate the early identification of cyber-attacks before they escalate.

3) Containment, Eradication & Recovery

Once an incident has been identified and appropriate action is deemed necessary, measures are taken to limit its impact and prevent further damage. This involves gathering information about the incident, identifying affected assets, and isolating compromised systems until normal operations are restored. Prompt implementation of these measures helps minimize damage and prevents the incident from spreading further [28]. Thompson highlights that eradication involves removing all remnants of a cyberattack, with particular focus on eliminating malicious artifacts.

4) Post-Incident Activity

The goal of this phase, also known as a post-mortem, is to understand precisely what occurred, why it happened, and how to prevent it from happening again. This review goes beyond technical aspects, it may also involve changes to policies or infrastructure [29]. The purpose of this phase is not to assign blame (though this can sometimes occur) but rather to reduce the likelihood or impact of future incidents. Additionally, heightened system logging and network monitoring are often implemented during this stage. It's common for attackers to target the same system again or use similar methods to compromise other resources within the organization.

B. Incident response

This crucial stage seeks to contain the event, eliminate the danger, and return operations to normalcy [30]. Steps to take include isolating compromised systems through containment measures, tracking down the attack's origin, and finally, eradicating the danger and restoring compromised systems.

1) Eradication

This step's primary objective is to eradicate the incident's origin and eradicate the threat from the system altogether to forestall its return. It requires in-depth investigation to ascertain the cause of the security breach or incident. Gathering and analyzing firmware for malware, linking exploited vulnerabilities to attack type, or employing any appropriate methodology that reveals attacker attack techniques are all possible options.

2) Lesson Learnt

The strength and safety of the agricultural technology ecosystem are greatly enhanced during this stage. In this stage, we aim to strengthen the system and enhance future reactions by drawing useful insights from accidents. The current incident response (IR) plan has to have its merits and shortcomings identified through an exhaustive evaluation.

3) Feedback

To finish the paperwork that wasn't finished during the incident and any other paperwork that might come in handy for future incidents, hold a meeting as soon as the situation is under control to learn from IR, go over the plan to update the system, and get feedback using a standard form or template.

C. LLMs in Network Security

LLMs in the subject of network security. Some of the things that need doing are online fuzzing, cyber threat analysis, penetration testing, and intrusion and anomaly detection:

- **Web fuzzing:** One mutation-based fuzzier is web fuzzing, which accepts coverage feedback from instrumented online applications and builds test cases gradually. Safety is of the utmost importance when it comes to web applications [31].
- **Traffic and intrusion detection:** Network security and management relies heavily on intrusion and traffic detection [32]. From conventional web apps to IoT and in-vehicle network situations, LLMs have found extensive use in network intrusion detection activities.
- **Cyber threat analysis:** CTI reporting is crucial in modern risk management techniques, according to recent studies. The demand for automated technologies to help with report production is increasing as the amount of CTI reports continues to climb [33]. Network threat analysis using LLMs falls into two main categories: CTI generation and CTI analysis for decision-making.
- **Web vulnerability detection:** Web application vulnerabilities may also be found using LLMs, although there are obstacles to overcome when it comes to language-specific traits and data availability

DOI: https://doi.org/xxxxxxxxxxxx

[34]. Improving LLM's performance in finding PHP vulnerabilities is the goal of frameworks like RealVul.

V. Literature of Review

This section reviews recent studies on LLM-based cybersecurity, focusing on cyber threat intelligence, incident response, threat modeling, automated analysis, RAG, knowledge graphs, and intelligent security systems, highlighting their contributions and limitations.

M. Niveditha, et al. (2026) Used an AI-powered cyber threat intelligence process that combines automated OSINT collection pipelines with an LLM to overcome these constraints. The EXA Intelligence API gathers real-time threat indicators, malware campaigns, and CVEs, which are processed using a multi-agent reasoning framework. Threat aggregation, vulnerability correlation, severity evaluation, and mitigation strategy creation are automated. Experimental results show that the proposed architecture enhances early threat detection, improves visibility, and reduces the workload associated with human analysis [35].

R. Özbay, et al. (2026) A PRISMA-guided bibliometric and thematic review of 149 studies published between 2015 and 2025, including 117 peer-reviewed journal and conference articles, examining publication trends and dominant research themes in LLM-enabled cybersecurity. The review is organized around five research questions: (i) secure incorporation of LLMs into cyber threat intelligence workflows; (ii) hybrid architectures for privacy-preserving and real-time threat detection; (iii) LLM-enabled secure code remediation; (iv) adversarial misuse and dual-use risks; and (v) multi-layer defense strategies addressing prompt injection, model inversion, and data poisoning [36].

A. Tellache, et al.(2025) A novel Retrieval-Augmented Generation (RAG)-based framework that leverages LLMs to automate and enhance IR by integrating dynamically retrieved CTI. The approach combines NLP-based similarity searches within a CTI vector database with standardized queries to external CTI platforms, enabling context-aware security alert enrichment. An LLM-powered response-generation module formulates precise, actionable incident-mitigation strategies. A dual evaluation paradigm is proposed, where automated assessment using an auxiliary LLM is cross-validated by cybersecurity experts [37].

A. George, et al. (2025) an automated incident response system that improves cyber threat intelligence by integrating real-world indicators of compromise from open-source threat intelligence feeds into an enriched knowledge graph containing static and dynamically gathered data. OpenAI language models analyze indicators, match them with known attack techniques and defense strategies, and automatically generate intelligence reports with investigation summaries, mapped techniques, defense recommendations, and tailored mitigation steps, providing security analysts with actionable insights [38].

M. S. Salek et al.,(2025) The Transportation Cybersecurity and Resiliency Threat Modeling Framework (TraCR-TMF), an LLM-based threat modeling framework for transportation CPS requiring limited cybersecurity expert intervention. TraCR-TMF identifies threats, potential attack techniques, and relevant countermeasures. Three LLM-based approaches support these identifications: (i) a retrieval-augmented generation approach requiring no cybersecurity expert intervention, (ii) an in-context learning approach with low intervention from cybersecurity experts, and (iii) a supervised fine-tuning approach with moderate cybersecurity expert intervention [39].

D. R. Arikkat et al. (2024) Intell Bot, a cybersecurity chatbot built using advanced LLMs, Lang Chain, and a Retrieval-Augmented Generation model. Intell Bot aggregates data from diverse sources to create a comprehensive knowledge base on vulnerabilities, cyber threats, and emerging trends. It provides intelligent responses to support threat intelligence, incident response, and security awareness. Evaluation achieved a BERT score above 0.8, cosine similarity of 0.8–1, and RAGAS scores above 0.77, confirming its effectiveness [40].

Z. C. Khan, et al. (2023) used CTI is an essential component of a Cybersecurity program but is often overlooked. It can assist in identifying future and potential cyber threats. Organizations process large volumes of data containing CTI, but this is often not collected, processed, or considered as CTI. South African organizations continue to feel the repercussions of cyber-attacks if actions are not taken. To bring clarity and allow South African organizations to leverage on CTI, this work aims to categorize CTI for organizations. Several characteristics of CTI are discussed, and thereafter a model is presented. The applicability of this model is demonstrated by a short use-case [41].

Despite significant progress in applying LLMs to CTI, several research gaps remain. Existing approaches address threat extraction, indicator analysis, vulnerability correlation, and intelligence generation, while real-time processing, data quality, hallucination, context understanding, and reliable classification remain insufficiently addressed. Limited research integrates diverse CTI sources while ensuring privacy and accuracy. In IR, RAG, knowledge graphs, automated investigation, and response recommendations have been explored, but prompt injection, adversarial manipulation, response reliability, and human oversight remain challenging. LLM integration with CTI platforms, SIEM, SOAR, and automated response systems is also underexplored. Dependable, explicable, privacy-preserving, domain-specific, real-time LLM frameworks should be the focus of future study. Table I summarizes existing approaches, technologies, contributions, and limitations.

TABLE I. Summary of Key Studies on Large Language Models for Cyber Threat Intelligence and Incident Response

Author & Year	Research Focus	Method/Technology	Dataset/Environment	Key Contribution	Limitation
M. Niveditha et al. (2026)	AI-powered Cyber Threat Intelligence	OSINT, EXA Intelligence API, LLM, Multi-Agent Reasoning	Real-time threat indicators, malware campaigns, CVEs	Automated threat aggregation, vulnerability correlation, severity evaluation, and mitigation generation	Requires reliable real-time threat data and further validation
R. Özbay et al. (2026)	LLM-enabled Cybersecurity	PRISMA, Bibliometric and Thematic Analysis	149 studies published during 2015–2025	Identified major research themes including CTI, privacy, secure code remediation, and adversarial risks	Limited empirical validation of identified approaches

DOI: https://doi.org/xxxxxxxxxxxxx

A. Tellache et al. (2025)	LLM-based Incident Response	RAG, NLP, CTI Vector Database, External CTI Platforms	Cyber Threat Intelligence and security alerts	Enabled context-aware alert enrichment and actionable incident mitigation	Retrieval quality and LLM reliability remain challenges
A. George et al. (2025)	Automated Incident Response	OpenAI LLMs, IoCs, Knowledge Graph, CTI Feeds	Real-world open-source threat intelligence	Generated investigation summaries, attack-technique mapping, defense recommendations, and mitigation steps	Requires validation across diverse real-world attack scenarios
M. S. Salek et al. (2025)	LLM-based Threat Modeling	RAG, In-Context Learning, Supervised Fine-Tuning	Transportation Cyber-Physical Systems	Identified threats, attack techniques, and countermeasures with reduced expert intervention	Primarily focused on transportation CPS environments
D. R. Arikkat et al. (2024)	Cybersecurity Chatbot	LLM, LangChain, RAG	Vulnerabilities, cyber threats, and emerging trends	IntellBot improved threat intelligence, incident response, and security awareness	Performance depends on knowledge-base and retrieval quality
Z. C. Khan et al. (2023)	Cyber Threat Intelligence Classification	CTI Characteristics, Classification Model	South African organizational context	Developed a CTI categorization model to improve organizational threat-intelligence utilization	Does not extensively address LLM-based CTI automation or incident response

VI. Conclusion and Future Work

Large Language Models (LLMs) are becoming useful tools for enhancing Incident Response (IR) and Cyber Threat Intelligence (CTI). Modern cybersecurity operations may be made more efficient with their help in processing enormous amounts of unstructured data, finding important threat indicators, summarizing intelligence, detecting vulnerabilities, analyzing network activity, and supporting security decision-making. LLMs can also assist different stages of the incident response lifecycle, including detection, analysis, containment, eradication, recovery, and post-incident assessment. However, their practical adoption remains challenging because of hallucinations, inaccurate outputs, limited explainability, data privacy concerns, adversarial manipulation, and dependence on high-quality security datasets. Therefore, LLMs should be integrated with existing cybersecurity tools and human expertise rather than being used as completely autonomous systems. Overall, the reviewed research indicates that LLM-based CTI and IR solutions have significant potential to enhance threat detection, intelligence analysis, and response capabilities. Responsible deployment, continuous validation, and appropriate security controls are essential for achieving reliable cybersecurity outcomes.

Future research should develop reliable and explainable LLM frameworks for CTI and IR using real-world datasets, Retrieval-Augmented Generation, federated learning, and human-in-the-loop approaches. Further work should address hallucination, adversarial attacks, privacy, scalability, and real-time threat detection while establishing standardized evaluation benchmarks and governance mechanisms for secure enterprise deployment

- **Funding:** This research received no external funding.
- **Institutional Review Board Statement:** Not applicable.
- **Informed Consent Statement:** Not applicable.
- **Data Availability Statement:** The data supporting the findings of this study are available from the corresponding author upon reasonable request.
- **Conflicts of Interest:** The author declares no conflict of interest.

How to cite this article:
M. Sahu, "An Analysis of Large Language Models for Cyber Threat Intelligence and Incident Response," *Journal of Global Research in Electronics and Communication*, vol. 2, no. 11, pp. 01–07, Nov. 2026, Doi: XXXX

References

[1] A. Ahmed Jamal, A.-A. Mustafa Majid, A. Konev, T. Kosachenko, and A. Shelupanov, "A review on security analysis of cyber physical systems using Machine learning," *Mater. Today Proc.*, vol. 80, pp. 2302–2306, 2023, doi: 10.1016/j.matpr.2021.06.320.

[2] V. Chaturvedi, R. Narra, and S. K. Chintagunta, *Applied AI Engineering for Developers: Building Intelligent Applications at Scale*. WISSIRA RESEARCH LAB, 2026.

[3] K. Rajashekar and N. Swapna, "Extenuating Insider Data Robbery Attacks in the Cloud: Fog Computing," *Int. J. Res. Mod. Eng. Emerg. Technol.*, vol. 1, no. 7, pp. 9–15, August, 2013.

[4] A. L. Buczak and E. Guven, "A Survey of Data Mining and Machine Learning Methods for Cyber Security Intrusion Detection," *IEEE Commun. Surv. Tutorials*, vol. 18, no. 2, pp. 1153–1176, 2016, doi: 10.1109/COMST.2015.2494502.

[5] P. Santos, R. Abreu, M. J. C. S. Reis, C. Serôdio, and F. Branco, "A Systematic Review of Cyber Threat Intelligence: The Effectiveness of Technologies, Strategies, and Collaborations in Combating Modern Threats," *Sensors*, vol. 25, no. 14, p. 4272, Jul. 2025, doi: 10.3390/s25144272.

[6] S. K. Malaraju, "Process of OS Security Hardening - Red Hat Enterprise Linux," *Int. J. Lead. Res. Publ.*, vol. 1, no. 2, pp. 1–11, October, 2020, doi: 10.70528/IJLRP.v1.i2.1474.

[7] S. Varga, J. Brynielsson, and U. Franke, "Cyber-threat perception and risk management in the Swedish financial sector," *Comput. Secur.*, vol. 105, p. 102239, Jun. 2021, doi: 10.1016/j.cose.2021.102239.

[8] D. C. Krakauer, M. Mitchell, and J. W. Krakauer, "Large language models and emergence: a complex systems perspective," *Philos. Trans. R. Soc. A Math. Phys. Eng. Sci.*, vol. 384, no. 2320, p. 20250014, 2026, doi: 10.1098/rsta.2025.0014.

[9] V. Kouliaridis, G. Karopoulos, and G. Kambourakis, "Assessing the Effectiveness of LLMs in Android Application Vulnerability Analysis," in *Attacks and Defenses for the Internet-of-Things*, W. Meng, M. Yung, and J. Shao, Eds., Cham: Springer Nature Switzerland, 2025, pp. 139–154.

[10] A. Ali, R.-H. Hwang, and Y.-D. Lin, "Evaluating Cyber Threat Intelligence: Accuracy, Completeness, Relevance, and Freshness," *IEEE Access*, vol. 13, no. July, pp. 157863–157876, 2025, doi: 10.1109/ACCESS.2025.3606477.

[11] N. G. Ambekar, N. N. Devi, S. Thokchom, and Yogita, "TabLSTMNet: enhancing android malware classification through integrated attention and explainable AI," *Microsyst. Technol.*, vol. 31, no. 3, pp. 695–713, Mar. 2025, doi: 10.1007/s00542-024-05615-0.

[12] S. Chatterjee, "Advanced Malware Detection in Operational Technology: Signature-Based Vs. Behaviour-Based Approaches," *ESP J. Eng. Technol. Adv.*, vol. 1, no. 1, pp. 272–279, 2021, doi: 10.56472/25832646/JETA-V1I2P128.

[13] S. Sreevathsa, "Strategies for Reducing Alert Fatigue and Improving Signal Quality in Enterprise Monitoring Architectures," *Int. J. Adv. Eng. Manag. Sci.*, vol. 12, no. 3, pp. 444–451, May-Jun, 2026, doi: 10.22161/ijaems.123.42.

[14] S. C. Pallaprolu, J. M. Namayanja, V. P. Janeja, and C. T. S. Adithya, "Label propagation in big data to detect remote access Trojans," in *2016 IEEE International Conference on Big Data (Big Data)*, Washington, DC, USA: IEEE, Dec. 2016, pp. 3539–3547.

doi: 10.1109/BigData.2016.7841017.

[15] M. Alazab, "Profiling and classifying the behavior of malicious codes," *J. Syst. Softw.*, vol. 100, pp. 91–102, Feb. 2015, doi: 10.1016/j.jss.2014.10.031.

[16] J. Mirkovic and P. Reiher, "A taxonomy of DDoS attack and DDoS defense mechanisms," *SIGCOMM Comput. Commun. Rev.*, vol. 34, no. 2, pp. 39–53, Apr. 2004, doi: 10.1145/997150.997156.

[17] H. Mohamed and H. Ali, "Chapter 1 Introduction," in *Blockchain, Fintech, and Islamic Finance*, De Gruyter, 2022, pp. 1–10. doi: 10.1515/9783110745016-001.

[18] M. Raza, Z. Jahangir, M. B. Riaz, M. J. Saeed, and M. A. Sattar, "Industrial applications of large language models," *Sci. Rep.*, vol. 15, no. 1, p. 13755, Apr. 2025, doi: 10.1038/s41598-025-98483-1.

[19] M. Alawida, S. Mejri, A. Mehmood, B. Chikhaoui, and O. Isaac Abiodun, "A Comprehensive Study of ChatGPT: Advancements, Limitations, and Ethical Considerations in Natural Language Processing and Cybersecurity," *Information*, vol. 14, no. 8, p. 462, Aug. 2023, doi: 10.3390/info14080462.

[20] H. Alqahtani and G. Kumar, "A comprehensive review of generative AI techniques and their impact on cybersecurity," *Soft Comput.*, vol. 29, no. 13–14, pp. 4945–4982, Jul. 2025, doi: 10.1007/s00500-025-10702-z.

[21] H. Jin *et al.*, "LLM Maybe LongLM: SelfExtend LLM Context Window Without Tuning," *Proc. Mach. Learn. Res.*, vol. 235, pp. 22099–22114, 2024.

[22] Z. Liu, "A Review of Advancements and Applications of Pre-Trained Language Models in Cybersecurity," in *2024 12th International Symposium on Digital Forensics and Security (ISDFS)*, IEEE, Apr. 2024, pp. 1–10. doi: 10.1109/ISDFS60797.2024.10527236.

[23] M. M. Chowdhury, N. Rifat, M. Ahsan, S. Latif, R. Gomes, and M. S. Rahman, "ChatGPT: A Threat Against the CIA Triad of Cyber Security," in *2023 IEEE International Conference on Electro Information Technology (eIT)*, IEEE, May 2023, pp. 1–6. doi: 10.1109/eIT57321.2023.10187355.

[24] S. Bhattamishra, A. Patel, P. Blunsom, and V. Kanade, "Understanding in-Context Learning in Transformers and Llms By Learning To Learn Discrete Functions," *12th Int. Conf. Learn. Represent. ICLR 2024*, pp. 1–27, 2024, doi: 10.48550/arXiv.2310.03016.

[25] K. Tamberg and H. Bahsi, "Harnessing Large Language Models for Software Vulnerability Detection: A Comprehensive Benchmarking Study," *IEEE Access*, vol. 13, pp. 29698–29717, 2025, doi: 10.1109/ACCESS.2025.3541146.

[26] P. Cichonski, "Computer Security Incident Handling Guide : Recommendations of the National Institute of Standards and Technology," *NIST Spec. Publ.*, vol. 800–61, p. 79, 2012.

[27] H. Karlzen and T. Sommestad, "Automatic incident response solutions: a review of proposed solutions' input and output," in *Proceedings of the 18th International Conference on Availability, Reliability and Security*, in ARES '23. New York, NY, USA, NY, USA: ACM, Aug. 2023, pp. 1–9. doi: 10.1145/3600160.3605066.

[28] E. C. Thompson, "Eradication, Recovery, and Post-incident Review," in *Cybersecurity Incident Response*, Berkeley, CA, CA: Apress, 2018, pp. 117–123. doi: 10.1007/978-1-4842-3870-7_9.

[29] C. Ojo, E. A. Osoko, J. N. Okolo, and M. Jaji, "Incident response: A structured model from detection to containment and recovery," *World J. Adv. Res. Rev.*, vol. 24, no. 1, pp. 1401–1407, Oct. 2024, doi: 10.30574/wjarr.2024.24.1.3148.

[30] S. Rudrakar, P. Rughani, and L. Sadineni, "Digital forensics and incident response management model for IoT based agriculture," *Sci. Rep.*, vol. 15, no. 1, p. 17797, May 2025, doi: 10.1038/s41598-025-02635-2.

[31] I. P. A. Dharmaadi, V.-T. Pham, F. Mohsen, and F. Turkmen, "SQLiFuzz: Uncovering SQL Injection in Any Web Applications," *Proc. ACM Softw. Eng.*, vol. 3, no. FSE, pp. 3208–3229, Jun. 2026, doi: 10.1145/3808149.

[32] Y. Mirsky, T. Doitshman, Y. Elovici, and A. Shabtai, "Kitsune: An Ensemble of Autoencoders for Online Network Intrusion Detection," in *Proceedings 2018 Network and Distributed System Security Symposium*, Reston, VA: Internet Society, 2018, pp. 18–21. doi: 10.14722/ndss.2018.23204.

[33] H. Xu *et al.*, "Large Language Models for Cyber Security: A Systematic Literature Review," *ACM Trans. Softw. Eng. Methodol.*, vol. 35, no. 11, pp. 1–61, Nov. 2026, doi: 10.1145/3769676.

[34] D. Cao, Y. Liao, and X. Shang, "RealVul: Can We Detect Vulnerabilities in Web Applications with LLM?," in *Proceedings of the 2024 Conference on Empirical Methods in Natural Language Processing*, Y. Al-Onaizan, M. Bansal, and Y.-N. Chen, Eds., Stroudsburg, PA, USA, Florida, USA: Association for Computational Linguistics, Nov. 2024, pp. 8268–8282. doi: 10.18653/v1/2024.emnlp-main.472.

[35] M. Niveditha, M. Swetha, M. S. R. Krishna, S. Rashmi, B. Pallavi, and M. L. Neelima, "Smart Cyber Threat Intelligence System for Autonomous Threat Aggregation and Reporting," in *2026 International Conference on AI-Driven Innovations & Applications (IC-AIDA)*, IEEE, Apr. 2026, pp. 1–6. doi: 10.1109/IC-AIDA68291.2026.11564311.

[36] R. Özbay, M. Çelebı, and U. Yavanoğlu, "The AI-Cybersecurity Nexus: How Large Language Models are Reshaping Threat Intelligence and Digital Defense," *IEEE Access*, vol. 14, pp. 15558–15587, 2026, doi: 10.1109/ACCESS.2026.3658308.

[37] A. Tellache, A. A. Korba, A. Mokhtari, H. Moldovan, and Y. Ghamri-Doudane, "Advancing Autonomous Incident Response: Leveraging LLMs and Cyber Threat Intelligence," in *GLOBECOM 2025 - 2025 IEEE Global Communications Conference*, IEEE, Dec. 2025, pp. 25–30. doi: 10.1109/GLOBECOM59602.2025.11432623.

[38] A. George, S. G. Sayed, Y. Mostafa, and M. Zamzam, "LLM and Knowledge Graphs for Automated Cyber Threat Intelligence and Incident Response," in *2025 IEEE 7th International Conference on Cybernetics, Cognition and Machine Learning Applications (ICCCMLA)*, IEEE, Nov. 2025, pp. 1–6. doi: 10.1109/ICCCMLA66092.2025.11580423.

[39] M. S. Salek *et al.*, "A Large Language Model-Supported Threat Modeling Framework for Transportation Cyber-Physical Systems," *IEEE Access*, vol. 13, pp. 163046–163070, 2025, doi: 10.1109/ACCESS.2025.3603580.

[40] D. R. Arikkat *et al.*, "IntellBot: Retrieval Augmented LLM Chatbot for Cyber Threat Knowledge Delivery," in *2024 IEEE 16th International Conference on Computational Intelligence and Communication Networks (CICN)*, IEEE, Dec. 2024, pp. 644–651. doi: 10.1109/CICN63059.2024.10847404.

[41] Z. C. Khan, T. Mkhwanazi, and M. Masango, "A Model for Cyber Threat Intelligence for Organisations," in *2023 International Conference on Artificial Intelligence, Big Data, Computing and Data Communication Systems (icABCD)*, IEEE, Aug. 2023, pp. 1–7. doi: 10.1109/icABCD59051.2023.10220503.