

Cyber Security Threat Hunting Through Log Analysis Using LLM

Student : OMAR SALEM ALMUTAIRI

Student ID: 251002148

MIDOCEAN UNIVERSITY

FOR MASTER OF AI PROGRAM

GRADUATION PROJECT 1

Introduction

The escalating sophistication of cyber threats demands innovative strategies for detecting and responding to malicious activities. **Threat hunting**, a proactive approach focused on identifying potential threats before they fully emerge, has become a cornerstone of modern cybersecurity frameworks. **Large Language Models (LLMs)** are increasingly proving to be powerful tools in this domain, particularly for **log analysis**, thanks to their capacity to process and interpret vast quantities of unstructured data. This literature review explores the current research landscape concerning the application of LLMs in threat hunting via log analysis, highlighting key findings, methodologies, and future prospects.

The Role of LLMs in Cybersecurity and Log Analysis

LLMs have transformed various aspects of cybersecurity, including **threat detection**, **vulnerability assessment**, and **incident response**. Their ability to process natural language and generate human-like text makes them especially well-suited for analyzing log data, which is often chaotic and complex. Traditional log analysis methods, relying heavily on predefined rules and manual scrutiny, are time-consuming and prone to errors. In contrast, LLMs can automate and improve log analysis by discerning patterns, identifying anomalies, and offering actionable insights [1, 2, 3].

A significant advantage of LLMs in log analysis is their proficiency in managing the diverse and intricate nature of log data. Logs can vary considerably in format, content, and structure, posing challenges for conventional processing methods. With their advanced natural language processing capabilities, LLMs can parse and interpret log data from a multitude of sources, including system, network, and application logs. This capability is particularly vital in threat hunting, where the ability to analyze disparate data sources is crucial for uncovering potential threats [4, 5].

Methodologies and Frameworks for LLM-Based Log Analysis

Various methodologies and frameworks have been proposed to harness LLMs for log analysis within threat hunting operations. These approaches can generally be classified into three main categories: **anomaly detection**, **log parsing and embedding**, and **multi-agent collaboration**.

Anomaly Detection

Anomaly detection is a critical element of threat hunting, as it involves pinpointing unusual patterns or behaviors that might signal a potential threat. LLMs have been successfully employed in anomaly detection for log analysis through diverse techniques. For instance, **LogLLM**, a log-based anomaly detection framework, leverages BERT to extract semantic vectors from log messages and uses Llama for classifying log sequences. This framework has demonstrated superior performance over traditional deep learning methods in capturing the semantic information embedded in log data [13].

Another strategy, **LogRAG**, utilizes a semi-supervised framework based on retrieval-augmented generation (RAG). This framework performs phased detection using both log tokens and log templates to mitigate the impact of log parsing errors. It also employs a single-class classifier to model normal system behavior, thereby reducing false

positives. Experimental results indicate that LogRAG achieves a 15% improvement in F1 Score on the BGL dataset and a 60% improvement on the Spirit dataset compared to previous leading semi-supervised learning algorithms [14, 15].

Log Parsing and Embedding

Log parsing and embedding are fundamental steps in preparing log data for analysis. Conventional log parsing methods often rely on manual rules or parsers, which can be error-prone and time-consuming. LLMs have been used to enhance log parsing and embedding through various techniques. For example, **LLMeLog**, a novel anomaly detection approach, leverages LLMs to enrich log events using in-context learning techniques. This approach fine-tunes a pre-trained BERT model with enriched log events and trains a transformer-based anomaly detection model. Evaluation results on three public log datasets show that LLMeLog achieves F1-scores exceeding 99%, even when using only 10% of labeled data as training data [16].

Another approach, described in Paper 17, employs LLMs for parsing and embedding by generating regular expressions (REGEX) for log parsing and utilizing a pre-trained LLM for event embedding. This framework also incorporates an autoencoder with an attention mechanism for unsupervised learning of log patterns. Experimental results highlight the model's effectiveness in anomaly detection, achieving 96% accuracy on a public dataset [17].

Multi-Agent Collaboration

Multi-agent collaboration is an emerging strategy in threat hunting that involves the coordination of multiple agents to execute complex tasks. **Audit-LLM**, a multi-agent framework designed for log-based insider threat detection, consists of three collaborating agents: the Decomposer, the Tool Builder, and the Executor. The Decomposer breaks down the intricate task of insider threat detection into manageable sub-tasks using Chain-of-Thought (COT) reasoning. The Tool Builder creates reusable tools for these sub-tasks, while the Executor generates the final detection conclusion by invoking constructed tools. The framework also employs a pair-wise Evidence-based Multi-agent Debate (EMAD) mechanism to refine conclusions through iterative reasoning exchange. Extensive experiments on three publicly available datasets demonstrate the superiority of this method over existing baselines, with significant improvements in the faithfulness of explanations generated by LLMs [18].

Challenges and Limitations

Despite the promising advancements in applying LLMs to log analysis for threat hunting, several obstacles and limitations persist. A primary challenge is the **scalability of LLMs** when dealing with vast volumes of log data. As the quantity of log data expands, the computational resources required for processing and analyzing it also increase, which can be a limiting factor for organizations with restricted resources [3, 4].

Another challenge is the issue of **false positives**. While LLMs have demonstrated impressive performance in anomaly detection, they can occasionally generate erroneous alerts due to their reliance on patterns and context. This can lead to

unnecessary distractions for security teams, thereby diminishing the overall effectiveness of threat hunting efforts [3, 5].

Furthermore, integrating LLMs into existing cybersecurity frameworks can be complex. Many organizations have established workflows and tools for log analysis, and incorporating LLMs into these environments demands substantial effort and resources. Additionally, the **interpretability and explainability** of LLM-based models can be a concern, as the decisions made by these models are often opaque, making it difficult for security analysts to comprehend and trust the results [4, 9].

Future Directions

The application of LLMs in threat hunting through log analysis is a rapidly evolving field, with several promising avenues for future research. One key area of focus is the development of more **interpretable and explainable models**. As LLMs become more integrated into cybersecurity frameworks, it is crucial to develop techniques that can provide clear and understandable explanations for the decisions made by these models. This will not only foster greater trust in LLM-based systems but also enable security analysts to refine and improve the models over time [4, 9].

Another important direction is the **enhancement of LLMs for domain-specific tasks**. While general-purpose LLMs have shown impressive capabilities in log analysis, domain-specific models tailored for cybersecurity tasks can further boost performance. Fine-tuning LLMs on cybersecurity-specific datasets and adapting them to the unique requirements of log analysis can lead to more accurate and relevant results [4, 5].

Finally, the development of more **robust and scalable frameworks** for LLM-based log analysis is essential. As the volume and complexity of log data continue to grow, it is crucial to design frameworks that can efficiently process and analyze large datasets while maintaining high performance. This includes exploring techniques such as distributed processing, parallel computing, and optimized pre-training strategies to enhance the scalability and efficiency of LLM-based systems [4, 9].

Conclusion

The incorporation of LLMs into threat hunting via log analysis represents a significant stride forward in cybersecurity. By harnessing the powerful natural language processing capabilities of LLMs, organizations can automate and enhance log analysis, leading to more effective and efficient threat detection. While challenges such as scalability, false positives, and model interpretability persist, ongoing research and development are anticipated to address these limitations and further improve the efficacy of LLM-based systems. As this field continues to advance, the application of LLMs in threat hunting is poised to play an increasingly vital role in safeguarding digital assets and bolstering cybersecurity resilience.

Table: Comparison of LLM-Based Log Analysis Frameworks

Framework	Key Features	Performance Metrics	Citation
LogLLM	Leverages BERT for semantic vector extraction and Llama for classification	Outperforms state-of-the-art methods in semantic understanding and anomaly detection	[13][14]
LogRAG	Semi-supervised framework with RAG and single-class classifier	15% improvement in F1 Score on BGL dataset, 60% improvement on Spirit dataset	[14][15]
LLMeLog	Enriches log events with in-context learning and fine-tunes BERT	Achieves F1-scores exceeding 99% on public datasets	[16]
Audit-LLM	Multi-agent collaboration with Decomposer, Tool Builder, and Executor agents	Demonstrates superiority over existing baselines with improved explanation faithfulness	[18]
Hybrid Approach	Combines LLM-based parsing with autoencoder and attention mechanism	Achieves 96% accuracy on public dataset	[17]

References :

Journal Article•10.22399/ijcesen.469 1. A Comprehensive Review of Large Language Models in Cyber Security. Mesut Güven 30 Sep 2024-International journal of computational and experimental science and engineering Request PDFPodcastChat	The paper highlights Large Language Models' efficacy in anomaly detection through log analysis, emphasizing their role in enhancing cyber threat intelligence and detection capabilities. It synthesizes recent literature, showcasing LLM applications in threat hunting and their transformative impact on
---	---

	cyber security frameworks.
10.1109/isdfs60797.2024.10527236 2. A Review of Advancements and Applications of Pre-Trained Language Models in Cybersecurity Zefang Liu 29 Apr 2024 Request PDFPodcastChat	The paper discusses the application of large language models (LLMs) in cybersecurity, particularly emphasizing their role in log analysis for threat hunting, showcasing advancements in utilizing PLMs to enhance detection and response capabilities in cybersecurity environments.
Journal Article•10.30574/wjaets.2024.13.1.0395 3. Large Language Models (LLMs) for Cybersecurity: A Systematic Review Yazi Gholami 30 Sep 2024-World Journal of Advanced Engineering Technology and Sciences Request PDFPodcastChat	The paper does not specifically address threat hunting using LLMs for log analysis. It focuses on LLM applications in vulnerability detection, malware analysis, and phishing detection, highlighting their advantages and challenges in cybersecurity without detailing log analysis techniques.

Preprint•10.48550/arxiv.2405.04760 4. Large Language Models for Cyber Security: A Systematic Literature Review Huilin Xu, S. Wang, N. Li +6 more 7 May 2024 PDFSummaryPodcastChat	The paper does not specifically address threat hunting using LLMs for log analysis. It focuses on various cybersecurity tasks facilitated by LLMs, including vulnerability detection and malware analysis, but lacks detailed insights on log analysis in threat hunting contexts.
Preprint•10.48550/arxiv.2405.03644 5. When LLMs Meet Cybersecurity: A Systematic Literature Review Jie Zhang, H. Bu, Hong Wen +3 more 6 May 2024 PDFSummaryPodcastChat	The paper discusses LLM applications in threat intelligence, including log analysis. Methods like LogPrompt and LEMUR enhance log parsing and semantic comprehension, improving efficiency and performance in identifying threats through structured report generation and semantic understanding of logs.
Preprint•10.21203/rs.3.rs-4387414/v1 6. Using Large Language Models to Better Detect and Handle Software Vulnerabilities and Cyber Security Threats Seyed Farid Taghavi, Farid Feyzi 21 May 2024 Request PDFPodcastChat	The paper does not specifically address threat hunting using LLMs for log analysis. It focuses on LLMs' applications in vulnerability detection, threat prediction, and automated code repair, highlighting their effectiveness in various cybersecurity domains but not in log analysis.

Journal Article•10.1109/access.2024.3505983 <u>7. Application of Large Language Models in Cybersecurity: a Systematic Literature Review</u> Ismayil Hasanov, Seppo Virtanen, Antti Hakkala +1 more 1 Jan 2024-IEEE Access Request PDFPodcastChat	The paper does not specifically address threat hunting using LLMs for log analysis. It focuses on the broader application of LLMs in cybersecurity, particularly in defensive measures, phishing simulations, and cybersecurity governance, without detailing log analysis.
Journal Article•10.21203/rs.3.rs-5423193/v1 <u>8. Artificial Intelligence and Large Language Models in Advancing Cyber Threat Intelligence: A Systematic Literature Review</u> Hilalah Alturkistani, Suriayati Chuprat 27 Nov 2024 Request PDFPodcastChat	The paper does not specifically address threat hunting using LLM for log analysis. It focuses on the broader application of AI and LLMs in Cyber Threat Intelligence, including automated report generation and threat detection, but lacks detailed literature on log analysis.
10.1186/s42400-025-00361-w <u>9. When LLMs Meet Cybersecurity: A Systematic Literature Review</u> Jie Zhang, Haoyu Bu, Hui Wen +3 more Request PDFPodcastChat	The paper does not specifically address threat hunting using LLMs for log analysis. However, it provides a systematic review of LLM applications in cybersecurity, highlighting various tasks and challenges, which may include aspects relevant to log analysis.

•Journal Article•10.1109/access.2022.3152549 10. Landscape of Automated Log Analysis: A Systematic Literature Review and Mapping Study 1 Jan 2022-IEEE Access Request PDFPodcastChat	The paper does not specifically address threat hunting using LLM for log analysis. It focuses on automated log analysis, its applications, and challenges, providing a systematic review of literature primarily from 2000 to June 2021 without mentioning LLMs.
Preprint•10.48550/arxiv.2402.19366 11. Exploring the Potential of Large Language Models for Improving Digital Forensic Investigation Efficiency Akila Wickramasekara, Frank Breitingner, Mark Scanlon 29 Feb 2024 PDFSummaryPodcastChat	The paper does not specifically address threat hunting using LLM for log analysis. It focuses on integrating LLMs into digital forensic investigations, exploring their architecture, usability, and potential applications, but lacks detailed literature on threat hunting in this context.
Journal Article•10.48550/arxiv.2412.01377 12. Adapting Large Language Models to Log Analysis with Interpretable Domain Knowledge Yuhe Ji, Yilun Liu, Feiyu Yao +9 more 2 Dec 2024 PDFSummaryPodcastChat	The paper does not specifically address threat hunting using LLMs for log analysis. It focuses on integrating interpretable domain knowledge into LLMs for log analysis tasks, enhancing performance and interpretability, but does not cover threat hunting literature.

Journal Article•10.48550/arxiv.2411.08561 13. LogLLM: Log-based Anomaly Detection Using Large Language Models Wei Guan, Jian Cao, Shiyu Qian +1 more 13 Nov 2024-arXiv.org Request PDFPodcastChat	The paper does not provide a literature review on threat hunting using large language models (LLMs) for log analysis. It focuses specifically on LogLLM, a framework for log-based anomaly detection leveraging LLMs, particularly BERT and Llama.
Journal Article•10.1109/issre62328.2024.00026 14. Leveraging RAG-Enhanced Large Language Model for Semi-Supervised Log Anomaly Detection Wanhao Zhang, Qianli Zhang, Enyu Yu +4 more 28 Oct 2024 Request PDFPodcastChat	The paper does not provide a literature review on threat hunting using large language models (LLM) for log analysis. It focuses on a semi-supervised log anomaly detection framework, LogRAG, leveraging RAG for improved accuracy in log anomaly detection.
Journal Article•10.1109/icws62655.2024.00129 15. LogRAG: Semi-Supervised Log-based Anomaly Detection with Retrieval-Augmented Generation Wanhao Zhang, Qianli Zhang, Enyu Yu +4 more 7 Jul 2024 Request PDFPodcastChat	The paper does not specifically address threat hunting using large language models (LLM) for log analysis. It focuses on a semi-supervised log anomaly detection framework utilizing retrieval-augmented generation (RAG) to improve log parsing and anomaly detection processes.

Journal Article•10.1109/issre62328.2024.00023 16. LLMeLog: An Approach for Anomaly Detection based on LLM-enriched Log Events Minghua He, Tong Jia, Chiming Duan +3 more 28 Oct 2024 Request PDFPodcastChat	The paper does not provide a literature review on threat hunting using LLM for log analysis. It focuses on LLMeLog, an anomaly detection approach that enhances log event representations using large language models for improved software reliability.
Journal Article•10.1109/ccece59415.2024.10667308 17. Log Anomaly Detection by Leveraging LLM-Based Parsing and Embedding with Attention Mechanism Asma Fariha, Vida Gharavian, Masoud Makrehchi +3 more 6 Aug 2024 Request PDFPodcastChat	The paper does not provide a literature review on threat hunting using LLM for log analysis. It focuses on a hybrid framework for log anomaly detection leveraging LLM for parsing and embedding, achieving 96% accuracy in anomaly detection.
Journal Article•10.48550/arxiv.2408.08902 18. Audit-LLM: Multi-Agent Collaboration for Log-based Insider Threat Detection Chengyu Song, Linru Ma, Jianming Zheng +3 more 12 Aug 2024 Request PDFPodcastChat	The paper does not provide a literature review on threat hunting using LLM for log analysis. It focuses on introducing Audit-LLM, a multi-agent framework for log-based insider threat detection, addressing challenges in discerning malicious activities from log entries.

Journal Article•10.1364/jocn.527874 19. Large Language Model-Based Optical Network Log Analysis Using LLaMA2 with Instruction Tuning Yue Pang, Min Zhang, Yanli Liu +6 more 2 Oct 2024-IEEE/OSA Journal of Optical Communications and Networking Request PDFPodcastChat	The paper does not specifically address threat hunting using LLM for log analysis. It focuses on log parsing, anomaly detection, and classification using LLaMA2, highlighting improvements in log analysis tasks rather than a comprehensive literature review on threat hunting.
Journal Article•10.3390/math12172758 20. Leveraging Large Language Models and BERT for Log Parsing and Anomaly Detection Yihan Zhou, Yan Chen, X. L. Rao +3 more 5 Sep 2024-Mathematics Request PDFPodcastChat	The paper does not provide a literature review on threat hunting using large language models (LLMs) for log analysis. It focuses on utilizing ChatGPT for log parsing and BERT for log anomaly detection, comparing performance with classical models.
Journal Article•10.48550/arxiv.2407.01896 21. LogEval: A Comprehensive Benchmark Suite for Large Language Models In Log Analysis Tianyu Cui, Shiyu Ma, Ziang Chen +10 more 1 Jul 2024 PDFSummaryPodcastChat	The paper does not specifically address threat hunting using LLMs for log analysis. It focuses on evaluating LLM capabilities in log parsing, anomaly detection, fault diagnosis, and summarization, providing insights into their performance in log analysis tasks.

Preprint•10.48550/arxiv.2406.07467 22. Anomaly Detection on Unstable Logs with GPT Models Fatemeh Hadadi, Qing Xu, Domenico Bianculli +1 more 11 Jun 2024 PDFSummaryPodcastChat	The paper primarily focuses on anomaly detection in unstable logs using LLMs, rather than threat hunting. It highlights challenges and opportunities for LLMs in log analysis, but does not specifically address threat hunting methodologies or literature.
Journal Article•10.48550/arxiv.2411.00914 23. AAD-LLM: Adaptive Anomaly Detection Using Large Language Models Alicia Russell-Gilbert, Alexander Sommers, Andrew Thompson +7 more 1 Nov 2024 PDFSummaryPodcastChat	The paper's title matches your query, but it doesn't address your specific question.
Journal Article•10.20944/preprints202412.2516.v2 24. Advancing Cyber Incident Timeline Analysis Through Retrieval-Augmented Generation and Large Language Models Fatma Yasmine Loumachi, Mohamed Chahine Ghanem, Mohamed Amine Ferrag 15 Jan 2025 Request PDFPodcastChat	The paper does not provide a literature review on threat hunting using LLM for log analysis. It focuses on a framework, GenDFIR, utilizing LLMs for cyber incident timeline analysis, emphasizing data preprocessing and context retrieval for incident reconstruction.

Journal Article•10.48550/arxiv.2409.02572 <u>25. Advancing Cyber Incident Timeline Analysis Through Rule Based AI and Large Language Models</u> Fatma Yasmine Loumachi, Mohamed Chahine Ghanem 4 Sep 2024-arXiv.org Request PDFPodcastChat	The paper does not provide a literature review on threat hunting using LLM for log analysis. It focuses on a novel framework, GenDFIR, combining Rule-Based AI and LLMs for timeline analysis in digital forensics and incident response.
Journal Article•10.48550/arxiv.2409.01909 <u>26. LUK: Empowering Log Understanding with Expert Knowledge from Large Language Models</u> Lipeng Ma, Weidong Yang, Sihang Jiang +5 more 3 Sep 2024 PDFPodcastChat	The paper does not specifically address a literature review on threat hunting using LLMs for log analysis. It focuses on enhancing log understanding through a framework called LUK, which utilizes expert knowledge from LLMs for smaller PLMs.
Journal Article•10.48550/arxiv.2409.05045 <u>27. Using Large Language Models for Template Detection from Security Event Logs</u> Risto Vaarandi, Hayret din Bahşi 8 Sep 2024 PDFSummaryPodcastChat	The paper primarily focuses on unsupervised template detection from security event logs using LLMs, addressing gaps in traditional algorithms. It does not specifically review threat hunting but highlights the potential of LLMs for log analysis in cybersecurity contexts.

Journal Article•10.1109/icws62655.2024.00106 28. LLM-powered Zero-shot Online Log Parsing Chen Zhi, Liye Cheng, Meilin Liu +3 more 7 Jul 2024 Request PDFPodcastChat	The paper does not specifically address threat hunting using LLM for log analysis. It focuses on YALP, a zero-shot log parsing solution utilizing ChatGPT, improving log parsing efficiency and effectiveness without user labeling across various log datasets.
Journal Article•10.1145/3643733 29. LILAC: Log Parsing using LLMs with Adaptive Parsing Cache Zhihan Jiang, Jinyang Liu, Zhuangbin Chen +6 more 12 Jul 2024 PDFSummaryPodcastChat	The paper does not provide a literature review on threat hunting using LLM for log analysis. It focuses on LILAC, a log parsing framework utilizing LLMs with an adaptive parsing cache to enhance log parsing accuracy and efficiency.
Journal Article•10.48550/arxiv.2407.17545 30. Large Language Models for Anomaly Detection in Computational Workflows: from Supervised Fine-Tuning to In-Context Learning Hong ei Jin, George Papadimitriou, Krishnan G. Raghavan +5 more 24 Jul 2024-arXiv.org Request PDFPodcastChat	The paper does not specifically address threat hunting using large language models (LLMs) for log analysis. It focuses on anomaly detection in computational workflows through supervised fine-tuning and in-context learning, highlighting their effectiveness in identifying anomalies.

Preprint•10.48550/arxiv.2406.06156 31. Stronger, Faster, and Cheaper Log Parsing with LLMs Xiaojian Yi, Van-Hoang Le, Hongyu Zhang 10 Jun 2024 PDFSummaryPodcastChat	The paper does not address threat hunting using LLM for log analysis. It focuses on log parsing techniques, particularly the LogBatcher framework, which improves efficiency and reduces costs in log parsing without requiring training or labeled demonstrations.
Journal Article•10.4018/979-8-3693-9311-6.ch003 32. Techniques and Approaches for Leveraging LLMs in Security Analysis Rebet Jones 18 Oct 2024-Advances in information security, privacy, and ethics book series Request PDFPodcastChat	The paper discusses leveraging LLMs for threat detection and anomaly analysis in security frameworks, highlighting their potential in log analysis. However, it does not specifically provide a literature review on threat hunting using LLMs for this purpose.
Journal Article•10.30574/wjarr.2024.24.2.3329 33. Automated threat detection and response using LLM agents Ramasankar Molleti, Vinod Goje, Puneet Luthra +1 more 3 Nov 2024-World Journal Of Advanced Research and Reviews Request PDFPodcastChat	The paper discusses LLM agents' application in threat detection, emphasizing their ability to analyze logs through natural language processing, contextual anomaly detection, and pattern identification, enhancing threat hunting capabilities and enabling proactive cybersecurity measures in existing systems like SIEM.

Preprint•10.48550/arxiv.2405.14487 34. A Comprehensive Overview of Large Language Models (LLMs) for Cyber Defences: Opportunities and Directions Mohammed Hassanin, Nour Moustafa 23 May 2024 PDFSummaryPodcastChat	The paper does not specifically address threat hunting using LLMs for log analysis. It focuses on LLM applications in cyber defense, including threat intelligence and vulnerability assessment, but lacks a literature review on log analysis in this context.
Journal Article•10.48550/arxiv.2311.14519 35. Benchmarking Large Language Models for Log Analysis, Security, and Interpretation Egil Karlsen, Xiao Luo, Nur Zincir-Heywood +1 more 24 Nov 2023-arXiv.org Request PDFPodcastChat	The paper does not specifically address a literature review on threat hunting using LLM for log analysis. It focuses on benchmarking various LLM architectures for log analysis in cybersecurity, emphasizing fine-tuning for effective domain adaptation and performance.
Journal Article•10.48550/arxiv.2310.01796 36. LLMParser: A LLM-based Log Parsing Framework Zhihan Jiang, Jinyang Liu, Zhuangbin Chen +6 more 3 Oct 2023-arXiv.org PDFSummaryPodcastChat	The paper does not specifically address threat hunting using LLM for log analysis. It focuses on log parsing challenges and introduces LLMParser, which leverages LLMs for accurate log parsing but does not cover threat hunting methodologies.

Journal Article•10.48550/arxiv.2311.05261 37. RAGLog: Log Anomaly Detection using Retrieval Augmented Generation Jonathan Pan, Swee Liang Wong, Yidi Yuan 9 Nov 2023-arXiv.org Request PDFPodcastChat	The paper does not provide a literature review on threat hunting using large language models (LLMs) for log analysis. It focuses on a novel approach, RAGLog, utilizing a Retrieval Augmented Large Language Model for log anomaly detection.
Journal Article•10.48550/arxiv.2311.05160 38. RAPID: Training-free Retrieval-based Log Anomaly Detection with PLM considering Token-level information Gunho No, Yukyung Lee, Hyeon Gyu Kang +1 more 9 Nov 2023-arXiv.org Request PDFPodcastChat	The paper does not address literature on threat hunting using LLM for log analysis. It focuses on RAPID, a training-free retrieval-based model for log anomaly detection, emphasizing real-time capabilities and token-level information without specific references to threat hunting.
Journal Article•10.48550/arxiv.2309.01189 39. LogGPT: Exploring ChatGPT for Log-Based Anomaly Detection Jiaxing Qi, Shaohan Huang, Zhongzhi Luan +2 more 3 Sep 2023-arXiv.org PDFSummaryPodcastChat	The paper does not specifically address threat hunting using LLMs for log analysis. It focuses on log-based anomaly detection using ChatGPT, reviewing existing methods and highlighting the potential of LLMs in this domain without direct mention of threat hunting.

40. LogGPT: Exploring ChatGPT for Log-Based Anomaly Detection

[CIBIN KI](#)

3 Sep 2023

[PDF](#) [Summary](#) [Podcast](#) [Chat](#)

The paper does not specifically address threat hunting using LLMs for log analysis. It focuses on log-based anomaly detection using ChatGPT, reviewing existing methods and highlighting the potential of LLMs in this domain without direct reference to threat hunting.