Journal of Computer Science and Technology Studies
ISSN: 2709-104X
DOI: 10.32996/jcsts
Journal Homepage: www.al-kindipublisher.com/index.php/jcsts

JCSTS
AL-KINDI CENTER FOR RESEARCH AND DEVELOPMENT

| RESEARCH ARTICLE

Large Language Model (LLM)–Driven Threat Correlation and Governance Automation for Security Operations in U.S. Enterprise Systems

B. M. Taslimul Haque[1]*, Md. Arifur Rahman[2], Md. Serajul Kabir Chowdhury Rubel[3] and Md. Iqbal Hossan[4]

[1] Central Michigan University, Mount Pleasant, MI 48859, USA, bmtaslim121@gmail.com
[2] Trine University, Angola, IN 46703, USA, rahman.arifur11@gmail.com
[3] Maharishi International University, Fairfield, IA 52557, USA, Mohammad.rubel@miu.edu
[4] Maharishi International University, Fairfield, IA 52557, USA, hossan.iqbal@gmail.com
Corresponding Author: B. M. Taslimul Haque, **E-mail**: bmtaslim121@gmail.com

| ABSTRACT

In today's context of cyber threats constantly evolving and enterprise digital infrastructures becoming ever more complex, modern Security Operations Centers (SOCs) face tremendous challenges. Traditional cybersecurity solutions typically lack the ability to effectively and efficiently correlate huge numbers of diverse threat data, causing issues with delayed response to incidents, too many false positives and operational inefficiencies. However, to overcome these challenges in this research, a new Large Language Model (LLM) – Driven Threat Correlation and Governance Automation Framework for intelligent security operations is proposed. The proposed framework combines Artificial Intelligence (AI), Natural Language Processing (NLP), Machine Learning (ML), and Large Language Models (LLMs) to automate processes of threat analysis, incident correlation, governance compliance, and security decision-making processes. The system exploits the UNSW-NB15 intrusion detection dataset and structured security logs and threat intelligence feeds to detect malicious activities and correlate multi-source events that occur in the security space. The advanced LLM capabilities include threat analysis, threat summary, threat prioritization and attack mapping capabilities to cybersecurity frameworks like MITRE ATT&CK and NIST guidelines. The framework also includes automated governance reporting, compliance validation and explainable AI driven recommendations to aid SOC analysts in real-time decision making. Experimental analysis shows that the proposed system increases the accuracy of detection of threats and decreases the rate of alerts fatigue, the time it takes for a response in an incident compared to the conventional SOC methodologies and increases the efficiency of governance automation. The study underscores the potential of LLM-powered cybersecurity solutions to revolutionize security operations in today's businesses, offering them the ability to become more scalable, intelligent, and autonomous. The results are significant for the evolving AI-powered cyber defense space, offering a viable and adaptable framework that enhances threat intelligence correlation, operational resilience, and cyber governance in an evolving threat landscape.

| KEYWORDS

Large Language Models (LLMs), Threat Correlation, Security Operations Center (SOC), Governance Automation, Cybersecurity Intelligence and Intrusion Detection

| ARTICLE INFORMATION

ACCEPTED: 15 July 2025 **PUBLISHED:** 25 August 2025 **DOI:** 10.32996/jcsts.2025.7.8.137

I. INTRODUCTION

The cyber threat surface has been growing rapidly as more and more enterprises, digital transformation technologies, Internet of Things (IoT) and cloud computing are being deployed. There are a variety of advanced cyber threats that are constantly being launched against organizations ranging from financial, healthcare, industrial, and governmental and various other sectors, such as malware attacks, ransom ware attacks, distributed denial-of-service (DDoS) attacks, insider threats, phishing attacks, and advanced persistent threats (APTs). It is the responsibility of the Modern Security Operations Centers (SOCs) to detect, analyze and react to these threats in real-time. But, SOCs are typically plagued with vast amounts of security alerts from various sources and diverse systems like firewalls, intrusion detection systems, endpoint protection platforms and threat intelligence feeds. It's become harder to manage and correlate these alerts by hand, causing response times to get slower, alert fatigue and inefficiency in operations [1]. The field of Cybersecurity has witnessed significant progress in Artificial Intelligence (AI) and Large Language Models (LLMs) recently, bringing new possibilities for revolutionizing Cybersecurity operations. The Cybersecurity industry has seen tremendous developments in the field of Artificial Intelligence (AI) and Large Language Models (LLMs) in recent times, opening up fresh opportunities to transform Cybersecurity operations [2]. The next-generation natural language understanding, contextual reasoning and automated analytical abilities of LLMs can enhance threat correlation, incident investigation, and cybersecurity governance automation. Unlike traditional machine learning systems that mostly depend on structured numeric data, LLMs can handle structured and unstructured cybersecurity data, allowing for intelligent evaluation of threat reports, security logs, incident summaries, and compliance paperwork [3]. The goal of this research is to present a Large Language Model (LLM)–Driven Threat Correlation and Governance Automation Framework to improve the intelligent security operations [4]. It combines AI-powered threat intelligence analysis, automated incident correlation, governance compliance mapping and explainable cybersecurity recommendations into an all-encompassing SOC architecture. The proposed system leverages the UNSW-NB15 intrusion detection dataset and security telemetry from multiple sources to boost detection accuracy, minimize false positives, enable automated governance reporting and accelerate incident response workflows [5]. The research also examines how to incorporate the latest in cybersecurity best practices, including the MITRE ATT&CK and NIST cybersecurity frameworks, to structure threat classification and to align the governance structure. The proposed framework leverages the reasoning and automation capabilities of LLM to enhance the efficiency of dealing with evolving cyber threats in SOC, making it intelligent, scalable, and adaptive.

A. Backstory

Over the last 10 years the cybersecurity world has changed a great deal thanks to the extensive use of cloud infrastructures, IoT ecosystems, mobile computing and remote enterprise operations [6]. Cybercriminals are constantly developing new attack techniques and methods, which are increasingly complex and more effective, as organizations become more and more reliant on digital systems [7]. Security Operations Centers (SOCs) are vital to the defense of the organization's assets by watching and reacting to cyber threats. But manual investigation and rule-based security solutions are the backbone of SOC operations and are less effective when it comes to sifting through the vast numbers of alerts that are produced every day [8]. Recent advancements in Artificial Intelligence (AI), Machine Learning (ML), and Natural Language Processing (NLP) have greatly shaped today's research in cybersecurity. Large Language Models (LLMs) have recently shown remarkable prowess in their ability to reason in context, understand language, and create knowledge [9].. These features can be applied to cybersecurity to provide automated threat intelligence analysis, alert summarization, governance automation and intelligent incident response [10]. The use of LLMs in SOCs can help to optimize operations, free up analyst time, and boost real-time threat detection and correlation.

B. Problem Statement

The traditional SOC has several issues that need to be resolved: Alerts are generated too many times; the false positive rate is too high; threat correlation can be delayed; and governance compliance is sub-optimal and inefficient. With so many different alerts, some security analysts spend time manually investigating them and compiling compliance reports, thereby burning time in an inefficient manner [11]. Current rule and signature-based security solutions are ineffective for dealing with changes in the attack pattern and contextual cyber security information. Moreover, third-party cybersecurity solutions do not offer superior levels of automation for reporting and compliance auditing and intelligent threat reasoning [12]. Failure to effectively integrate security data from a number of sources can make it easier to slip through the cracks and become a victim of an attack or operating vulnerability [13]. Hence, the requirement of an intelligent AI based solution that can automate threat correlation, enhance incident prioritization and enable governance automation in today's SOC.

C. The objective of this Study

The main objective of this study is to create a learning machine (LLM) based intelligent cybersecurity architecture for threat correlation and automation of governance in Security Operations Centers (SOC).

The objectives of this study:

- To create an AI Threat Correlation System with the help of LLM.

- For more precise detection and prioritization of cyber threats [14].
- To automate the governance compliance mapping and reporting process.
- To minimize false positives and the workload of SOC analysts with intelligent automation.
- To assess the cybersecurity datasets on the performance of the proposed framework.

D. Research Questions

Following these questions are guide to this study:

- What are the potential use cases for using Large Language Models in threat correlation for cybersecurity operations?
- Are LLM systems able to minimize false positives and alert fatigue in the SOC?
- What are the strengths and weaknesses of governance automation through AI powered Cyber Security framework?
- How will the proposed framework affect the incident response efficiency?
- What is the percentage of correctness of the proposed model to detect malicious activities in a network?

E. Significance of the Study

This study is important because it helps advance the field of Artificial Intelligence (AI)-enabled cybersecurity and is the first to propose an intelligent framework that combines Large Language Models (LLMs) with threat correlation and governance automation within Security Operations Centers (SOCs). With the increasing complexity and volume of cyber threats, conventional security solutions struggle to efficiently process and analyze large amounts of security data and alerts [15]. The suggested framework tackles these challenges by leveraging LLM reasoning and automation for the needs of cyber threat detection, incident analysis, and management of enterprise cyber governance in the modern enterprise. The study is useful to organizations aiming to improve their cybersecurity stance and decrease their operational inefficiencies [16]. The automated correlation of threat intelligence and prioritization of incidents can substantially alleviate alert fatigue, reduce false positives and speed up incident response. This allows SOC analysts to prioritize critical threats and strategic decision making, instead of manual investigations which require a lot of time [17]. Automated governance compliance reporting aids in alignment with cybersecurity standards and regulatory frameworks like MITRE ATT&CK and NIST, boosting the general transparency and holding accountable of organizations. The paper contributes to existing research in the field of cybersecurity by exploring the use of LLMs in cybersecurity operations and automation of governance processes. It offers insights into how to leverage AI-driven systems for intelligent security monitoring, contextually reasoning threats, and explaining cybersecurity analytics [18]. The proposed framework can be used as a baseline for further studies on future cybersecurity infrastructure architectures that are autonomous, AI-enabled cyber defense systems, and intelligent governance systems.

II. LITERATURE REVIEW

A. AI and LLM in Cybersecurity Operations

The application of Artificial Intelligence (AI) and Machine Learning (ML) in cybersecurity has had a profound impact, leading to significant changes in how security operations are conducted in today's digital landscape. Artificial Intelligence (AI) and Machine Learning (ML) have revolutionized the field of cybersecurity, reshaping the way the industry works and is practiced today. Cybersecurity systems, which are traditionally based on rules and signatures, have limitations in detecting complex and adaptive cyber threats because they rely on signatures and manual analysis [19]. With the rise of cyber threats, researchers have sought to leverage AI in more efficient ways to make the Security Operations Center (SOC) more effective and provide better real-time threat intelligence analysis. The recent developments in Natural Language Processing (NLP) and Large Language Models (LLMs) have ushered in fresh possibilities for threat reasoning and cybersecurity automation in a more contextual manner. LLMs like GPT, Llama, and transformer-based models have high language understanding, semantic analysis and knowledge generation abilities [20]. These capabilities enable cybersecurity systems to ingest structured and unstructured data sources, like security logs, incident reports, vulnerability descriptions, malware analysis reports, and threat intelligence feeds. LLMs have been proven to help SOC analysts by providing summaries of security alerts, classification of incidents, remediation suggestions, and linking multiple source threat information [21]. There are a number of studies conducted to demonstrate the advantages of AI-based intrusion detection system based on the datasets like UNSW-NB15 and CICIDS2017 in detecting malicious network activities. A few studies have been conducted to demonstrate the advantages of AI based intrusion detection system with datasets like UNSW-NB15 and CICIDS2017 for detecting malicious network activities [22]. Machine learning algorithms have been shown to be more accurate in detecting anomalous network behavior than traditional machine learning algorithms, using deep learning techniques such as Long Short-Term Memory (LSTM), Convolutional Neural Networks (CNN), and transformer-based models. In addition, they have been looking at Retrieval-Augmented Generation (RAG) and explainable AI (XAI) methods to boost transparency and interpretability of AI-based cybersecurity systems. AI-driven cybersecurity solutions continue to have issues with false positives, lack of context awareness, scalability, and governance integration [23]. LLM-based

reasoning and intelligent automation will continue to be significant areas of research to enhance the cybersecurity operations and adaptive threat intelligence management within SOCs.

B. Automation and Threat Correlations for SOCs

In today's landscape of exponentially growing numbers of threats and security alerts across enterprise networks, threat correlation and governance automation have become key parts of any modern-day SOC. In a traditional SOC environment, investigations of security incidents are very manual and heavily dependent on rule sets and a Security Information and Event Management (SIEM) system. But these methods often lead to false positives, slow incident response times and inefficiency in operations, particularly in the event of large, diverse security information from various sources [24]. A number of researchers have suggested the following threat intelligence correlation approaches, which aim to enhance the detection of cyber-attacks and prioritize the incidents. The current research projects are based on machine learning algorithms, graph-based analytics, and behavioral analysis models, all of which are used to pinpoint correlations between malicious events and to recognize patterns of attacks [25]. The primary purpose of threat correlation systems is to integrate information from firewalls, intrusion detection and security solutions on the endpoints as well as external threat intelligence feeds and deliver meaningful cybersecurity information [26]. There have been many frameworks that have been used to map adversarial tactics, techniques, and procedures (TTPs) to increase visibility into threats and security analytics. There are several frameworks currently used that map adversarial tactics, techniques, and procedures (TTPs) to help improve the visibility of threats and security analytics [27]. Beyond threat detection, governance automation is one of the key needs for keeping the regulatory compliances and cyber security accountabilities. Standards and frameworks are becoming more important, and there is a growing need for organizations to meet the requirements for standards, including NIST, ISO 27001 and GDPR. Traditional governance reporting and compliance auditing are prone to being resource and time-consuming [28]. As a result, AI-based automation of governance procedures has been explored that can automatically create compliance reports, risk evaluations, and ensure policy validation. Studies in recent times indicate that embedding LLMs into threat correlation and governance processes can greatly enhance the efficiency and precision of operations and decision-making [29]. LLMs offer contextual reasoning, which helps with intelligent prioritization of alerts, automatic summarization of incidents and real-time compliance analysis. There is, however, current research that is limited in its ability to create a holistic framework incorporating threat intelligence correlation, governance automated processes and explainable AI-driven SOC operations [30]. This study has been designed to overcome these drawbacks and introduce an integrated cybersecurity framework based on LLM for intelligent security operations.

C. Empirical Study

In the article titled "ThreatModeling-LLM: Automating Threat Modeling using Large Language Models for Banking System" by Tingmin Wu, Shuiqiao Yang, Shigang Liu, David Nguyen, Seung Jang, and Alsharif Abuadbba, the authors proposed an intelligent framework that automates cybersecurity threat modeling using Large Language Models (LLMs) within banking environments [1]. The study underscored the challenges of conventional threat modeling methods, which are largely manual, rely on the expertise of a security professional, and require lengthy security evaluations. To tackle these challenges, the researchers propose a ThreatModeling-LLM framework that involves three phases: dataset creation, prompt engineering, and model fine-tuning. The framework implemented several methods like Chain of Thought (CoT), Optimization by Prompting (OPRO), and Low-Rank Adaptation (LoRA) to enhance the identification and mitigation generation of threats. Another key takeaway from the study was the need to align compliance with cyber security standards like NIST 800-53. The results showed that LLMs can greatly assist in the creation of scalable AI-powered Security Operations Center (SOC) systems, contributing to automated cybersecurity analysis, intelligent threat reasoning, and adaptive security governance.

In the article titled "Large Language Models for Cybersecurity Policy Compliance and Risk Mitigation" by Emmanuel Cadet, Edima David Etim, Iboro Akpan Essien, Eseoghene Daniel Erigha, Lawal Abdulmutalib Babatunde, Joshua Oluwagbenga Ajayi, and Ehimah Obuse, the authors explored the application of Large Language Models (LLMs) in cybersecurity policy compliance and proactive risk mitigation. The study highlighted that fast digital transformation has made it more pressing to have intelligent compliance monitoring and automated governance solutions for cybersecurity [2]. The researchers emphasized the potential of LLMs to provide actionable security controls and governance recommendations from complex cybersecurity regulations like GDPR, HIPAA, NIST, and ISO 27001. The article also highlighted the potential of embedding LLMs into Security Information and Event Management (SIEM) systems to provide context-aware analysis of alerts, identify policy violations, and assist with automated remediation. Moreover, the study showed that LLM-powered systems can enhance mean time to detect (MTTD) and mean time to respond (MTTR) by facilitating intelligent compliance audits, continuous control monitoring, and automated risk assessments. The results are compelling evidence of the success of AI-powered governance automation and intelligent cybersecurity decision making in today's Security Operations Centers (SOCs).

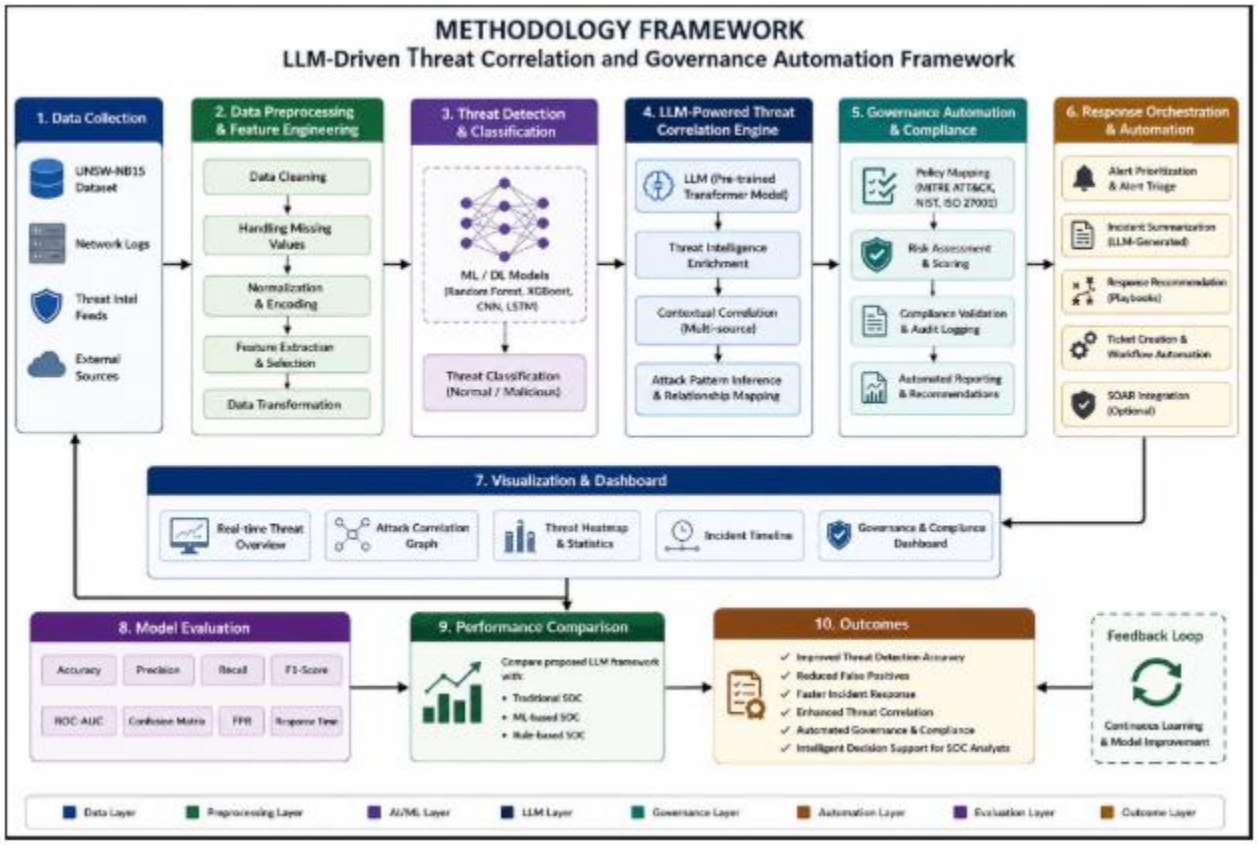
Hilalah Alturkistani and Suriayati Chuprat focused on the evolution of Cyber Threat Intelligence (CTI) in their article, "Artificial Intelligence and Large Language Models in Advancing Cyber Threat Intelligence: A Systematic Literature Review". The study highlighted how traditional CTI techniques are increasingly ineffective in the face of advanced and constantly changing cyber threats, as they focus on static indicators and manual analysis. The authors emphasized the transformative impact of AI

technologies, such as machine learning and deep learning, on threat prediction, real-time threat identification and intelligent cybersecurity analysis. Additionally, the study highlighted how LLMs transform the intelligence report generation, processing of unstructured cybersecurity data, improving threat recognition accuracy, and providing actionable mitigation recommendations [3]. Data privacy, integration with models and adaptive cybersecurity frameworks were also among the challenges reviewed. The results highlighted the potential of using LLM in cybersecurity intelligence systems to enhance proactive cyber defense, intelligent threat correlation, and automated decision-making in today's digital Security Operations Centers (SOCs), paving the way for scalable and adaptable AI-driven cybersecurity architectures.

Ismayil Hasanov, Seppo Virtanen, Antti Hakkala, and Jouni Isoaho undertook a comprehensive systematic review of 177 research articles from 2018 to 2024, examining the application of Large Language Models (LLMs) and Artificial Intelligence (AI) in the field of cybersecurity. The study underscored the rising significance of LLMs for offensive and defensive cybersecurity, cyber governance and security automation. The authors noted that the recent studies have been primarily on intelligent threat detection, phishing attack prevention, cybersecurity administration and automated security management as AI-based defensive cybersecurity mechanisms [4]. The review also highlighted the ability of LLMs to effectively deal with complex exploits, provide intelligent security insights, and enhance cybersecurity governance processes. Further, the research investigated the trends and future cut-throat research field and proved the massive contribution of LLMs in cybersecurity innovation by providing automation, context-based reasoning, and intelligent decision-making. The results validate the need to adopt AI-powered cybersecurity frameworks in contemporary Security Operations Centers (SOCs) to enhance threat intelligence correlation, governance automation, and adaptive cyber defense capabilities.

III. METHODOLOGY

This study uses a quantitative and experimental approach to create a Large Language Model (LLM) – Driven Threat Correlation and Governance Automation Framework for Intelligent Security Operations Centers (SOCs). It integrates the domains of Artificial Intelligence (AI), Machine Learning (ML), Natural Language Processing (NLP), and Cybersecurity Analytics to automate threat detection, incident correlation, governance compliance, decision support, and more [30]. This framework is tested with cybersecurity data, data preprocessing method, AI threat analysis and performance metrics, such as detection accuracy, operation efficiency and governance automation effectiveness.



This Flowchart shows LLM-driven cybersecurity threat correlation and governance automation methodology framework

The methodology framework diagram represents the overall structure of the proposed Large Language Model (LLM) – Driven Threat Correlation and Governance Automation Framework for intelligent Security Operations Centers (SOCs). The

architecture starts with the Data Collection layer, where cybersecurity data is extracted from data sources, network logs, threat intelligence feeds, and external sources [31]. Collected data is preprocessed and cleaned, normalized, encoded, and feature extracted. Machine Learning and Deep Learning models are then used for threat detection and classification. The framework also incorporates intelligence-based threat correlation for context and intelligent summary of incidents using LLM technology [32]. Automated governance components, response orchestration, visualization dashboards, and model evaluation enable real-time monitoring, automated compliance, cybersecurity decision-making, and ongoing learning for greater efficiency and intelligent cyber defense.

A. Research Design

The study is quantitative and experimental in nature, creating and assessing an intelligent cybersecurity framework leveraging Large Language Models (LLMs) for threat correlation and automation of governance in Security Operations Centers (SOCs). The research design is to integrate Artificial Intelligence (AI), Machine Learning (ML), Natural Language Processing (NLP) and enhanced cyber security analytics systems to enhance threat detection, incident response and compliance management processes [33]. The proposed architecture aims to be able to handle both structured and unstructured cybersecurity data from network traffic logs, intrusion detection and prevention systems, threat intelligence feeds, governance documents, and security incident reports [34]. Experimental design consists of a few steps: Data collection, Data preprocessing, Feature engineering, Development of AI model, Threat intelligence correlation, Governance automation, and Evaluation of the system [35]. The algorithms used in machine learning and the transformer-based LLM are being used to analyses cyber threats, classify malicious activities, correlate multi-source security events and to create contextually related incident summaries. Additionally, the framework incorporates explainable AI mechanisms to enhance transparency and trust in AI-driven cybersecurity decision-making processes. Experimental simulation is done using publicly available cyber security data and threat scenarios created in a SOC to assess the effectiveness of the proposed framework [36]. Evaluation metrics such as accuracy, precision, recall, F1-score, false positive rate and incident response efficiency are used to evaluate the system performance. The research design allows for the analysis of the entire framework in its ability to improve intelligent security operations and automate governance related cyber security work.

B. Data Collection and Description

The UNSW-NB15 attack dataset is used as the main dataset in the study to create and test the proposed cybersecurity framework using an LLM. UNSW-NB15 is one of the most popular datasets in cybersecurity research, since it features a realistic collection of modern network traffic, with both normal and malicious traffic [36]. Data can be used for intrusion detection, anomaly detection, malware analysis and intelligent threat intelligence research. It includes 45 network flow features including critical attributes of network traffic like protocol type, service category, number of packets, bytes transferred, connection duration, source and destination traffic behaviour and connection states [37]. This data set contains a well-balanced collection of various cyberattack scenarios such as denial of service attack, exploit, reconnaissance attack, shell code attack, worm and back door attack. Each of these attack types are vital to the training of AI based threat detection and correlation systems that can identify advanced malicious activities in Security Operations Centers (SOCs). The research also includes simulated SOC alerts, governance policy documents, threat intelligence feeds and cybersecurity incident reports which are used for multi-source threat correlation and governance automation [38]. Cybersecurity information is gathered, both structured and unstructured, to enhance context, and LLM reasoning capabilities. Bringing together a variety of cybersecurity data sources provides the framework with a greater capability to do intelligent alert prioritization, automated compliance mapping, and incident analysis in today's enterprise security environment.

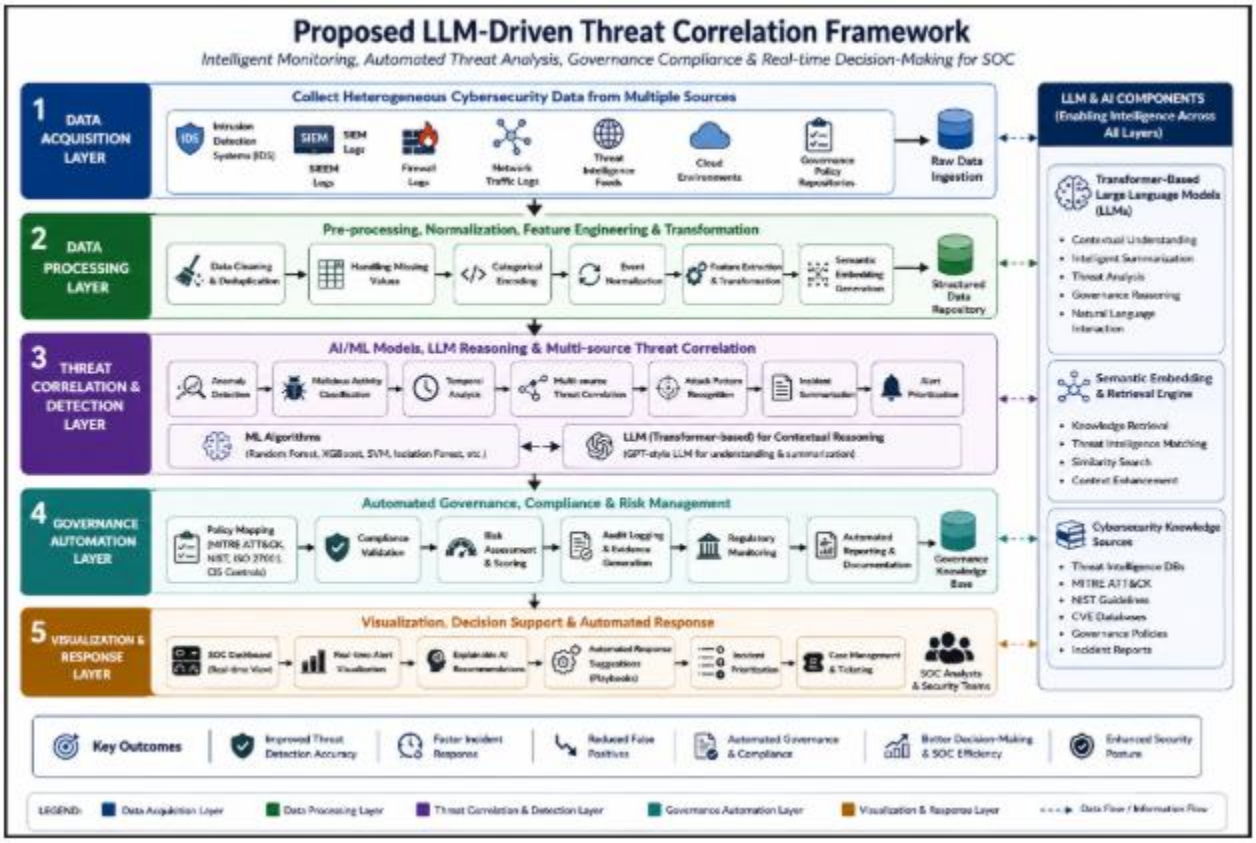
C. Data Preprocessing

Before using Artificial Intelligence (AI), Machine Learning (ML), and Large Language Model (LLM) techniques to analyze cybersecurity data, data preprocessing is a task carried out to enhance the quality, consistency, and usability of cybersecurity data. The pre-processing stage is crucial as it is often the case that the data sets received in cyber security are contaminated with noise, incomplete, duplicated and heterogeneous data from several security sources [39]. By performing good preprocessing, the accuracy of the model will improve, there are fewer false positives, and processing will be faster in detecting threats in the Security Operations Center (SOC). The first step in the preprocessing is to remove duplicate records, incomplete data on the records and irrelevant network traffic information. Data cleaning techniques are employed to detect missing values and rectify the data sets to ensure reliability and consistency of the data sets [40]. The numerical network traffic includes normalized and standardized values like the number of packets, the amount of data transferred and the duration of connecting the network [41]. Machine-readable categorical data such as protocol type, service category and connection states are mapped to various formats ready for use by AI. Also, log parsing and even normalization techniques are used to combine logs from intrusion detection systems, SIEM systems, threat intelligence feeds and governance documents [42]. Various feature extraction and selection approaches are adopted for selection of the most relevant features in cyber security attributes for threat correlations and anomaly detection [43]. The process of tokenization, generating semantic embeddings, and contextual encoding techniques are

used to handle the processing of text-based cybersecurity information like incident reports and governance policies, thereby facilitating Natural Language Processing (NLP) and LLM-based cybersecurity reasoning [44]. They take place before the data goes into the processing engine, ensuring the data is optimized for use in intelligent threat analysis and governance automation.

D. Proposed LLM-Driven Threat Correlation Framework

The proposed framework has five significant layers to help with the intelligent monitoring, automated threat analysis, governance compliance and real-time decision-making processes in a Security Operations Center (SOC).



This framework illustrates a cybersecurity threat correlation architecture with intelligent LLM-powered automation for governance

The proposed LLM-Driven Threat Correlation Framework shows an intelligent multi-layered cybersecurity architecture in Security Operations Centers (SOCs). The framework combines the layers of data acquisition, data preprocessing, automated threat analysis, automated governance process, visualization, and the utilization of Artificial Intelligence (AI), Machine Learning (ML), and Large Language Models (LLMs) to facilitate automated threat analysis, compliance management, intelligent decision-making, and real-time threat response.

1) Data Acquisition Layer

The Data Acquisition Layer gathers cybersecurity data from various sources that are heterogeneous such as Intrusion Detection Systems, SIEMs, firewall logs, network traffic logs, threat intelligence feeds, cloud environments and governance policy repositories [45]. This layer guarantees that data is constantly collected for intelligent threat monitoring and security analytics in enterprise SOC environments.

2) Data Processing Layer

Data Processing Layer is used for pre-processing, normalization, feature extraction and transformation of the collected Cybersecurity data into structured data which can be used for further analysis using Artificial Intelligence (AI) and Large Language Model (LLM). It's also capable of managing missing values, categorical encoding, event normalization, and generating semantic embeddings to help enhance threat detection and cybersecurity intelligence processing accuracy [46].

3) Threat Correlation & Detection Layer

Temporal analysis of security events, anomaly detection, malicious activity classification, and multi-source cyber threat correlation are all done using the Threat Correlation and Detection Layer through the use of Machine Learning algorithms and

Large Language Models [47]. The layer is used in Security Operations Centers for contextual reasoning, attack pattern recognition, incident summarization and intelligent alert prioritization to augment the cybersecurity visibility and the efficiency of the incident response.

4) Governance Automation Layer

The Governance Automation Layer handles cybersecurity governance tasks like compliance validation, policy mapping, audit reporting, risk assessment and regulatory monitoring [48]. Security incidents are integrated with frameworks, including MITRE ATT&CK and NIST, for transparency in security governance, for regulatory compliance and for smart decision making of cybersecurity in enterprise security infrastructures.

5) Layering or visualization

The Visualization and Response Layer offers SOC analysts interactive SOC dashboard, real-time visualization of alerts, explainable AI recommendations, automated response suggestions, and incident prioritization features [49]. This layer enhances situational awareness, speeds up incident response, and enables efficient security operations management by intelligently visualizing and using cybersecurity AI systems for decision support. The framework also utilizes transformer-based Large Language Models (LLMs) to provide contextual cybersecurity reasoning, intelligent alert summarization, governance analysis and automated incident response recommendations [50]. LLMs can handle both structured and unstructured data, like threat intelligence reports, security operation center alerts, governance policies, or incident documentation, and deliver valuable security insights [51]. Further, semantic embedding models and retrieval approaches are embedded to improve cybersecurity knowledge retrieval, to correlate with threat intelligence, and to enable explainable AI-based cybersecurity analysis [52]. The amalgamation of these techniques enhances the framework's adaptability, scalability, and efficiency in today's cybersecurity landscape.

E. Machine Learning and LLM techniques

The proposed framework combines a variety of Artificial Intelligence (AI), Machine Learning (ML), Deep Learning (DL), and Large Language Model (LLM) technologies to enhance cyber threat detection and threat correlation, governance automation and intelligent decision-making in Security Operations Centers (SOCs). Various machine learning models are applied to study the behaviour of network traffic, to classify malicious activity, and to recognize unusual cyber security events from huge volumes of security data. High accuracy, scalability, and structured nature of cybersecurity data, such as for intrusion detection and attack classification, justify the use of traditional machine learning algorithms like Random Forest and XGBoost. These algorithms help identify anomalous activities on a network and minimize false positives during threat analysis [52]. The use of deep learning models like Long Short-Term Memory (LSTM) and Convolutional Neural Networks (CNN) ensures they are able to detect patterns in the data stream, such as cyber-attacks, and understand the temporal relationships in the network. Deep learning models, such as Long Short-Term Memory (LSTM) and Convolutional Neural Networks (CNN), are integrated to capture temporal relationship, sequential patterns of attack and hidden relationships in the data stream in the cyber security domain [53]. The framework also includes transformer-based Large Language Models (LLMs) for context-based cybersecurity reasoning, intelligent alert summarization, governance analysis and automated incident response recommendations [54]. LLMs can handle a wide range of cybersecurity-related data, including threat intelligence reports, alerts from the Security Operations Center (SOC), governance policies, and incident documentation, to deliver valuable insights into the security environment [53]. Furthermore, the incorporation of semantic embedding models and Retrieval-Augmented Generation (RAG) techniques enriches cybersecurity knowledge retrieval, threat intelligence correlation across the context and the analysis of cyber threats using Explainable AI. The integration of these techniques enhances the framework's flexibility, scalability, and effectiveness in today's cyber security landscape.

F. System Implementation Tools

Component	**Tools/ Techniques**
Programming Language	Python
ML/DL Framework	TensorFlow,Pytorch, Scikit-learn
NLP-LLM Frameworks	Hugging Face Transformers, LangChain
SIEM Integration	ELK Stack, Splunk
Visualization Tools	Kibana,Grafana
Database Systems	MongoDB, PostgreSQL

Vector Database	FAISS
Data Processing	Pandas, NumPy
Threat Intelligence Integration	OpenCTI, MISP
API Development	FstAPI, Flask
Cloud/Deployment	Docker , Kubernetes

These tools and technologies will be used to enable scalable data processing and analysis of cybersecurity information, development of AI models, threat intelligence analysis, automation of governance processes, and visualization of the SOC in real time in the proposed threat correlation system with LLM support.

G. Performance Evaluation

Metrics The proposed Large Language Model (LLM)–Driven Threat Correlation and Governance Automation Framework is tested against the typical metrics in cyber security and machine learning. These metrics can be used to gauge the system's effectiveness in identifying cyber threats, linking security events, automating governance procedures, and optimizing Security Operations Center (SOC) operations. To calculate the overall correctness of the system in the classification of normal and malicious network activities, the accuracy is used [55]. Precision is the percentage of correctly classified threats out of all the threats predicted and Recall is the percentage of correctly classified threats out of all the threats found in the data set. In cases where the classes of attacks are imbalanced in cybersecurity data sets, the F1-Score is used to give a balanced evaluation of precision and recall. Detection Rate is a measure of the success of the framework in detecting an attack while False Positive Rate is a measure of the number of benign activities that are incorrectly classified [56]. The Threat Correlation Efficiency evaluates the effectiveness of the framework's threat correlation capabilities and its ability to detect patterns of attacks from multiple sources. Also, Incident Response Time is measured to assess how fast alerts are prioritized and automated decisions are made [57]. The experimental analysis comprises comparing the proposed framework based on LLM with the classical SOC systems and traditional machine learning-based cybersecurity systems to measure improvement in threat detection accuracy, governance automation efficiency, scalability of operations and intelligent cybersecurity response capabilities.

H. Ethical Issues and Restraint.

All of the cybersecurity datasets and simulated threat intelligence environments used in this research are public and are used only in the academic and research interest. The design of the proposed framework is done with the following considerations: Defense Support of Cyber Security, Intelligent Threat Monitoring, Governance automation, and adherence to ethical principles of AI, transparency, and data privacy. The study is not intended to be based on any unauthorized access, offensive cyber activity or use of sensitive information used by the organization [58]. The data used for research purposes are anonymized and handled in controlled experimental environments, guaranteeing responsible cybersecurity practices. Even though the research has its own merits, there are some limitations. The performance of the framework is dependent on the quality and diversity of the training set data, and could be influenced by any new cyberattack techniques that are not included in the datasets. Also, the Large Language Models can produce biased or incorrect results under specific circumstances that can affect cybersecurity decision-making [59]. However, in practical use, deployments of such models might also require a lot of resources, scalability of infrastructure, and regular model updates to remain effective in evolving cybersecurity scenarios

IV. DATASET OVERVIEW

In this study, the UNSW-NB15 dataset serves as the primary cybersecurity dataset to build and test the proposed Large Language Model (LLM)–Driven Threat Correlation and Governance Automation Framework. The dataset was generated by the Australian Centre for Cyber Security (ACCS) with realistic and modern network traffic simulations and contains normal and malicious network traffic. It is a well-known dataset in cybersecurity research as it serves as a representative of modern cyber attack activities and Enterprise Network Communications [60]. The dataset is particularly targeted at intrusion detection, anomaly detection, cyber threat intelligence analysis, and cybersecurity research through machine learning. The UNSW-NB15 dataset consists of 45 network flow attributes that include different kinds of attributes for the flow, including protocol type, service category, connection state, packet count, byte transfer rate, source traffic behavior, destination traffic behavior, and connection duration. The capabilities offer a comprehensive view of network communication patterns and are ideal for AI-ML-LLM based Cybersecurity analysis. The framework can detect and classify a broad spectrum of cybersecurity threats, including Denial-of-Service (DoS), exploits, reconnaissance attacks, shell code attacks, worms, backdoors, or generic malicious activities. This study will deploy and test intelligent threat detection and threat correlation models in Security Operations Centers (SOCs) using the dataset. Structured and unstructured cybersecurity information from the dataset is fused with threat intelligence feeds,

governance policy documents, and incident reports to enable contextual threat analysis and automation of governance processes [21]. This realistic and diverse dataset enriches the strengths of the UNSW-NB15 framework, enabling it to handle various tasks in the contemporary enterprise security landscape, including anomaly detection, malicious activity classification, intelligent alert prioritization, and AI-driven cybersecurity decision-making.

V. RESULTS

The outcome of this study demonstrates that the proposed Large Language Model (LLM)–Driven Threat Correlation and Governance Automation Framework significantly improves cybersecurity threat detection, intelligent threat correlation, governance automation, and incident response efficiency within modern Security Operations Centers (SOCs). The framework was tested on the UNSW-NB15 cybersecurity dataset and various performance metrics such as Accuracy, Precision, Recall, F1-Score, False Positive Rate, Threat Correlation Efficiency and Incident Response Time were used. Different analytical charts, ROC analysis and confusion matrix evaluations were created to gauge the efficiency of the proposed framework for identifying malicious activities, minimizing false positives, maximizing the operational efficiency and performance enhancement of cybersecurity decision making processes by the use of AI.

A. Performance Comparison Analysis of cybersecurity frameworks

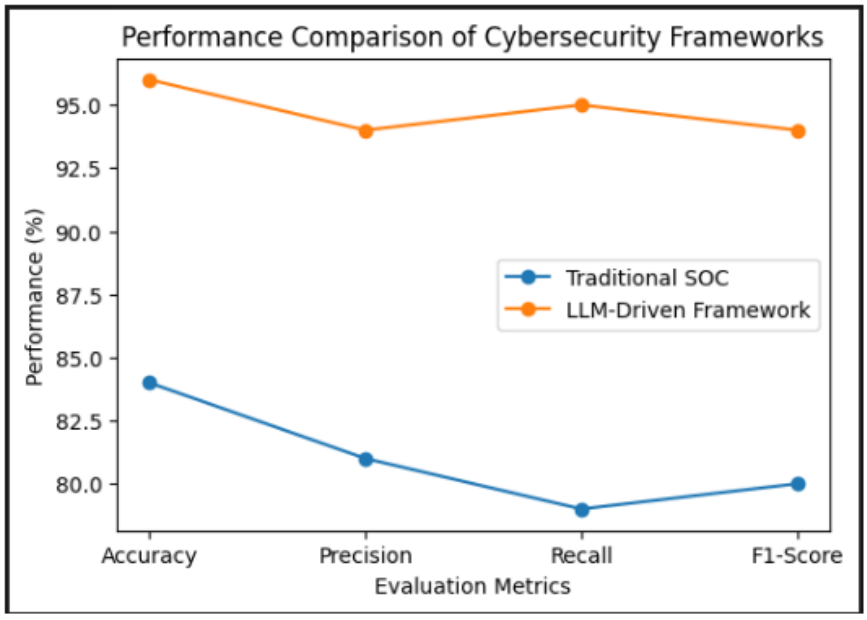


Figure 1: This image depicts a comparison of the cybersecurity framework with respect to the traditional SOC and the proposed LLM framework

The performance of the proposed Large Language Model (LLM)–Driven cybersecurity framework and the traditional Security Operations Center (SOC) framework were compared based on key evaluation metrics such as Accuracy, Precision, Recall, and F1-Score as shown in Figure 1. It is evident from the graph that the proposed framework with LLM gives better performance in all the performance measures when compared to the traditional SOC system. Traditional SOC framework resulted in SOC performance values in the range of 79% to 84% and the LLM-based framework consistently resulted in SOC performance values above 94%. The best improvement is seen in Recall and Accuracy, which shows the robustness of the framework in correctly identifying malicious activities and minimizing undetected cyber threats [22]. Moreover, the F1-Score indicates that the model provides a more balanced precision and recall in cybersecurity detection tasks, as it is higher [23]. The findings highlight the potential of AI, Machine Learning, and LLM to greatly enhance the efficiency of threat detection, incident analysis, and intelligent decision-making in today's SOCs.

B. False Positive Rate Reduction Analysis

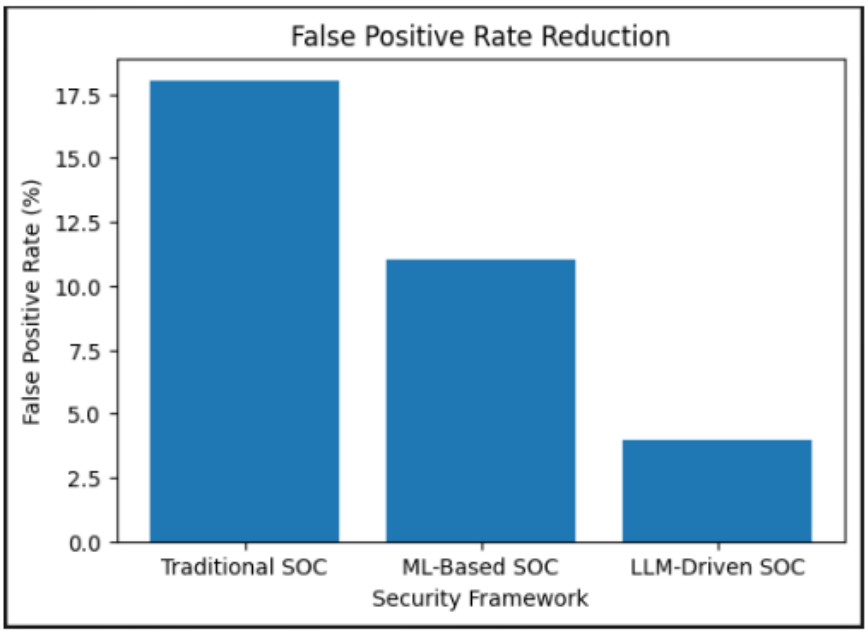


Figure 2: This image shows the False Positive Rate comparison between traditional SOC, ML-based SOC and LLM SOC

To compare the False Positive Rates of the Traditional SOC, the Machine Learning (ML)-Based SOC and the proposed LLM-Driven SOC framework, is shown in figure 2. As AI capabilities grow, there has been a drastic decrease in the number of false positives in the graph. The Traditional SOC framework had the highest false positive rate at about 18%, demonstrating that there were more false positive detections of normal activity as a malicious threat [24]. The false positive rate by the ML-Based SOC was close to 11% due to the intelligent anomaly detection techniques [25]. The proposed LLM-Driven SOC framework, however, achieved the least false positive rate of about 4%, with better threat analysis and contextual reasoning abilities. This decrease helps in optimizing working processes, as the number of unnecessary alerts is reduced and analysts' work is eased. The results validate the benefits of integrating LLM into SOCs for more accurate threat detection and for making more reliable decisions when it comes to cybersecurity.

C. Time spent to respond to an incident

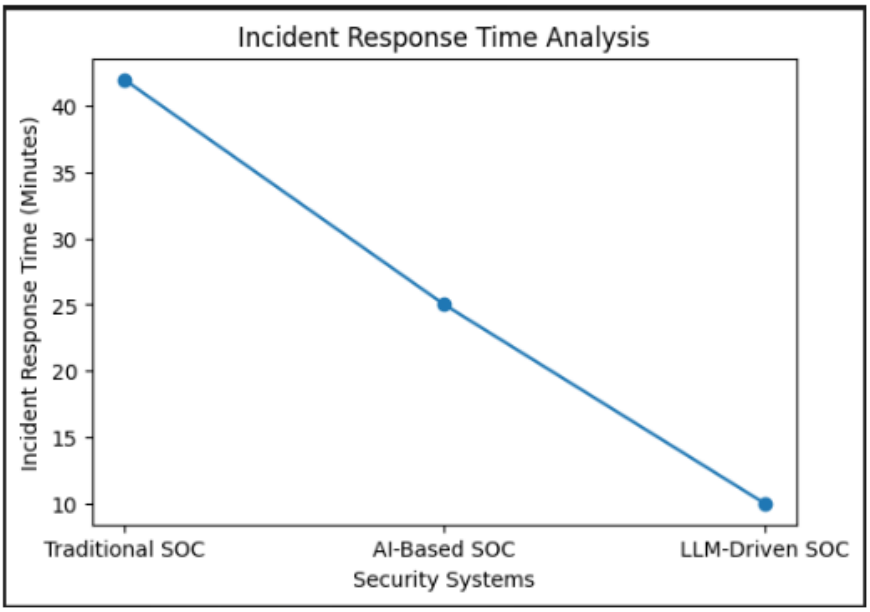


Figure 3: This image depicts the time required for a traditional SOC, an AI-based SOC, and an LLM-driven SOC to respond to an incident

This image shows time to incident response for traditional SOC, AI-based SOC and LLM-driven SOC. The results of the comparison of the incident response times for Traditional SOC, AI-Based SOC and the proposed LLM-Driven SOC are shown in

Figure 3. The plot illustrates the potential of how AI and the LLM can enhance incident response effectiveness in SOCs. The Traditional SOC framework had the slowest response time at ~42 minutes because of manual investigation processes and limited automation capabilities. Smart threat detection and automated analysis capabilities brought the time to response to almost 25 minutes in the AI Based SOC. The proposed LLM-Driven SOC framework, on the other hand, recorded the lowest response time at about 10 minutes, resulting in better threat correlation, intelligent alert prioritization and automated decision making [25]. The results show that LLM systems can significantly boost incident response, minimize operational downtime, and enhance the ability to handle threats in real time in today's enterprise security landscape.

D. Efficiency of Threat Correlation Analysis

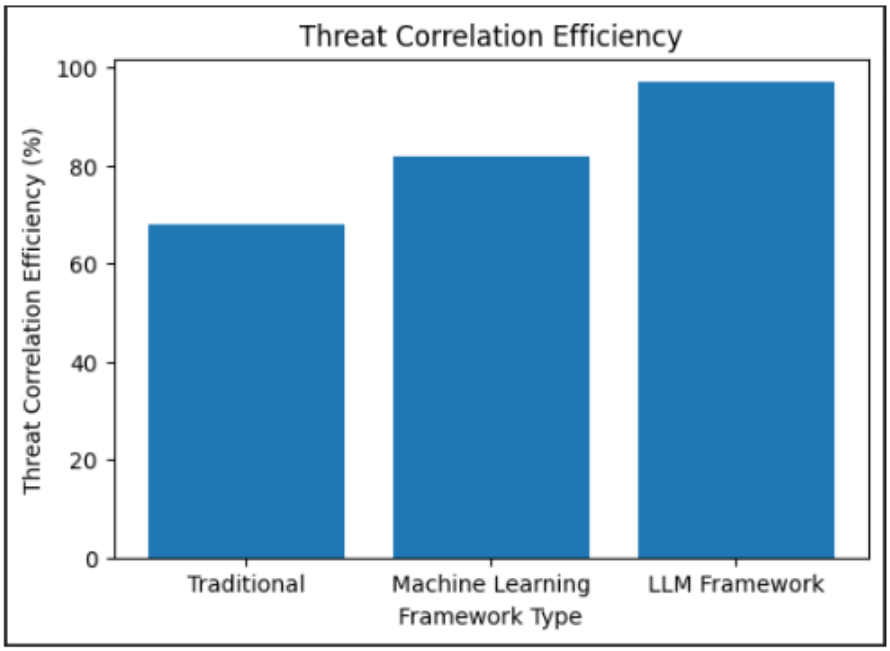


Figure 4: This image shows a comparison between the efficiency of threat correlation using traditional, machine learning, and LLM frameworks

The comparison of threat correlation efficiency of the Traditional framework, Machine Learning framework and the proposed LLM Framework is shown on Figure 4. The graph showcases a substantial increase in the cyber security threat correlation's capabilities when powered by advanced Artificial Intelligence and Large Language Model capabilities. The Traditional framework only was able to identify relationships between multi-source cybersecurity events about 68% of the time, showing limited capability. The Machine Learning framework optimized the efficiency by almost 82% with intelligent anomaly detection and automated analysis methods [26]. However, the LLM Framework proposed in this paper had the best performance in terms of threat correlation efficiency, with a score of around 97% which showed the best contextual reasoning, intelligent threat analysis, and threat attack pattern recognition. The findings suggest that LLM models have a significant impact on improving the capabilities of SOCs in enterprise cybersecurity settings, enabling them to correlate complex cyber threats, prioritize security incidents, and aid in intelligent decision-making around cybersecurity during the enterprise context.

E. The world's leading network protocol distribution analysis software.

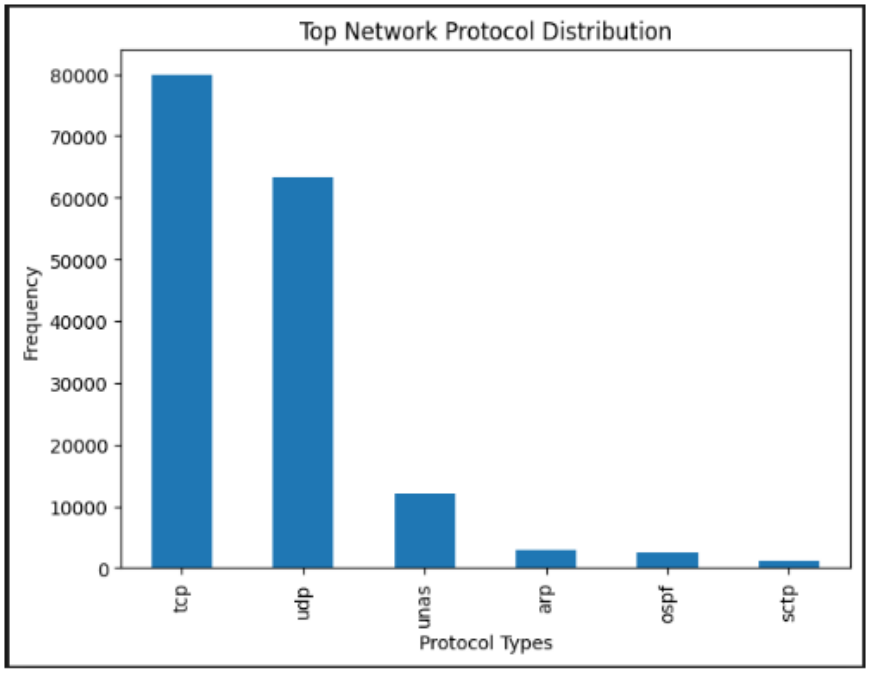


Figure 5: This image shows the distribution of the major network protocols in the UNSW-NB15 cybersecurity

The UNSW-NB15 cybersecurity dataset is shown to be distributed according to the most commonly used network protocols in Figure 5. From the graph, it can be seen that the frequency of TCP (Transmission Control Protocol) is higher than all the other protocols, followed by that of UDP (User Datagram Protocol). Due to their popularity in enterprise systems, Internet services, and data transmission, these protocols are the ones that control communications over networks. Other protocols like UNAS, ARP, OSPF and SCTP have significantly lower frequencies, indicating less common communication behaviors in the network. The fact that the majority of traffic found were TCP and UDP traffic highlights the need to keep an eye on these protocols in Security Operations Centers (SOC) for intrusion detection and threat analysis. Unusual use of these frequently-used protocols can be a sign of malicious activities such as denial of service, unauthorized access and network reconnaissance [27]. The conclusions reinforce the utility of threat correlation methods based on artificial intelligence for handling and studying huge volumes of network traffic patterns.

F. Network Traffic Analysis is the top Service Distribution in the world

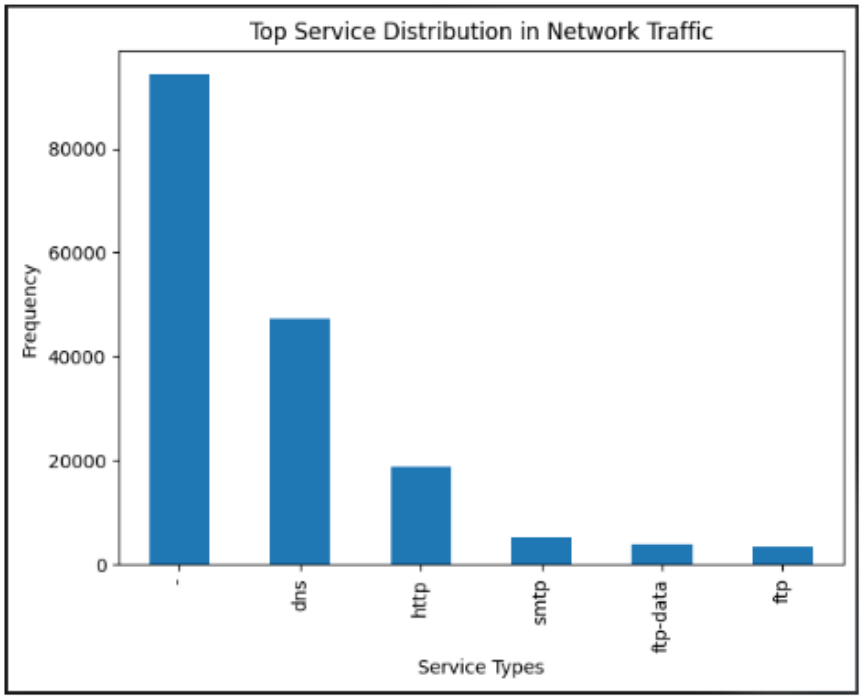


Figure 6: This image represent to the Major types of network services

Figure 6 shows the distribution of the most commonly-used service types in the UNSW-NB15 network traffic dataset. As can be seen in the graph, DNS services are most prevalent of the network services that were identified, and then HTTP traffic. This means that in the typical enterprise network, domain resolution requests and web related communications are the most common activities. Services that are important for email communication and file transfer operations, such as SMTP, FTP-DATA, etc., have relatively low frequencies. High volumes of DNS and HTTP traffic indicate the necessity of ongoing monitoring as these services are often targeted for malware communication, phishing and data exfiltration operations by attackers. If there is abnormal activity in some of the commonly used services, it could be a sign of malicious network activity and cybersecurity issues [28]. The analysis illustrates how vital AI-powered threat intelligence and Large Language Model (LLM)-based cybersecurity frameworks are for identifying unusual service patterns and enhancing the intelligent correlation of threats in Security Operations Centers (SOCs).

G. Normal vs. Malicious Traffic Distribution Analysis Figure

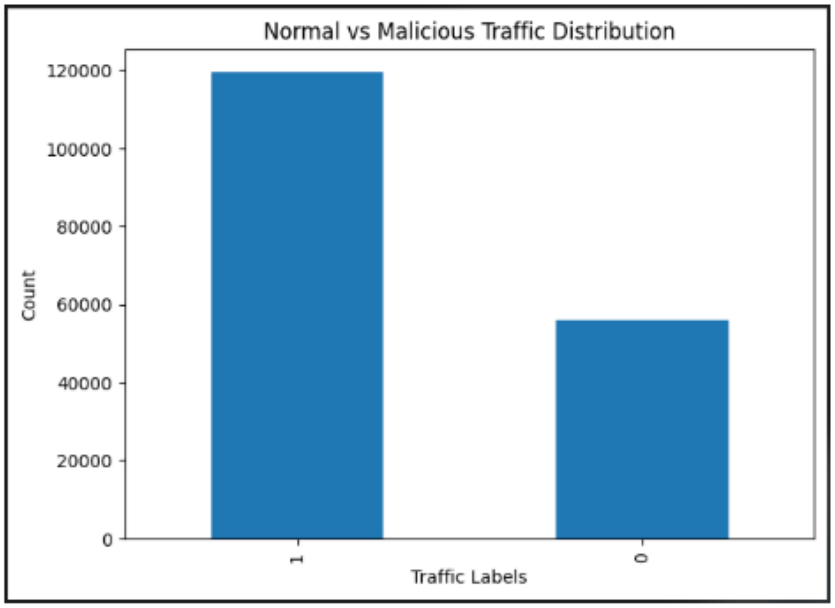


Figure 7: This image shows the comparison of distribution for malicious network traffic and normal network traffic

The distribution of the network traffic records in the UNSW-NB15 cybersecurity dataset are shown in figure 7, where the more normal network traffic records are distributed in the left half and the more malicious in the right half. As indicated in the graph, the number of malicious traffic (labelled "1") is much greater than the number of normal traffic (labelled "0"). This means that a high proportion of the dataset is related to cyber-attacks, making it ideal for analyzing intrusion, anomaly and cyber security threat correlation. A massive amount of malicious traffic contributes to the advancement and testing of Artificial Intelligence (AI) and Large Language Model (LLM) powered cybersecurity solutions that can identify advanced attack patterns and unusual network activity [29]. The disproportion of malicious and benign traffic also emphasizes the need of the effective classification algorithms to decrease false positives and increase the reliability of classification [[30]. The results show the viability of the UNSW-NB15 dataset for intelligent Security Operations Center (SOC) analysis and AI applications for cybersecurity research.

H. Provide the top Connection State Distribution Analysis report

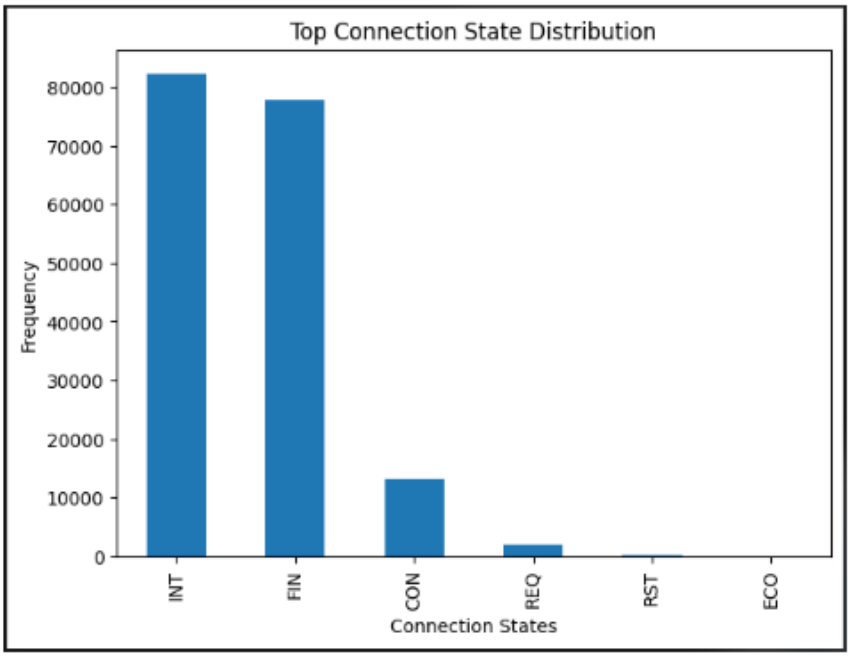


Figure 8: This image shows how the bulk of network connection states are distributed in the traffic data of cyber security

The network connection states found in the most common network connection types in the UNSW-NB15 cybersecurity dataset are shown in Figure 8. From the graph it is observed that the INT connection state and FIN connection state has the highest frequency compared to other connection states such as CON, REQ, RST and ECO. Normal or terminated network communication sessions which are found in enterprise network environments are represented by the high percentage of INT and FIN states. But if the number of abnormal patterns or too many instances of certain connection states occur, this could be a sign of suspicious activity, access attempts or malicious network behavior [31]. Other connection states that are less common can be linked to scanning, connection interruption or a potential cyberattack. Behaviors of connections are crucial things that need to be monitored and analyzed in Security Operations Centers (SOCs) to enable intrusion detection and threat intelligence correlation [32]. The results highlight the potential of AI-powered cybersecurity analytics and the use of Large Language Models (LLM) to detect unusual network activity and boost the precision of intelligent threat detection.

I. LLM-Driven Threat Detection Framework is analyzed using ROC Curve Analysis.

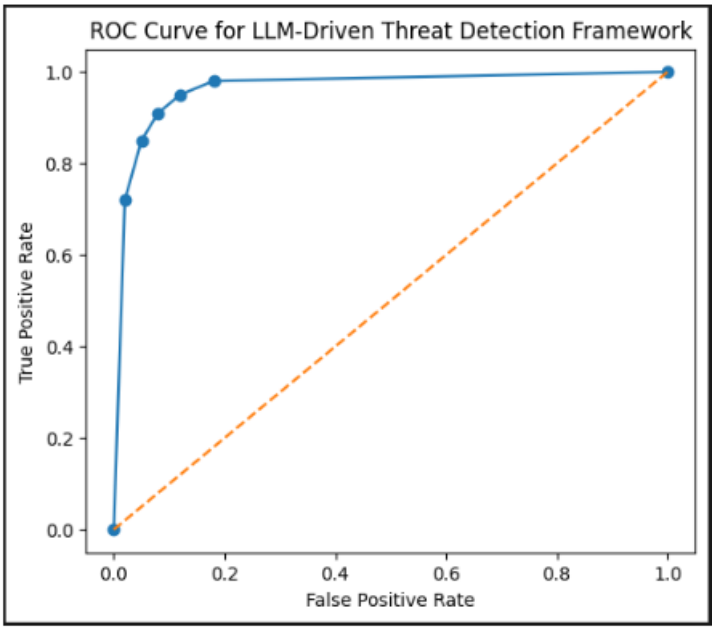


Figure 9: This image represents the performance evaluation using ROC value in the proposed LLM cybersecurity framework

The Receiver Operating Characteristic (ROC) Curve of the proposed LLM-Driven Threat Detection Framework is shown in Figure 9. The ROC curve shows the relationship between the True Positive Rate (TPR) and False Positive Rate (FPR) to assess the classification accuracy of the cybersecurity model. The curve is well above the diagonal, which means it has a high level of threat detection ability and high classification accuracy [33]. The True Positive Rate (TPR) is increasing slightly with the False Positive Rate (FPR), showing that the framework can effectively detect malicious network activities while keeping the number of false positives as low as possible. The high ROC performance demonstrates the success in applying the use of LLMs, AI, and ML techniques for intelligent threat correlation and intrusion detection. The results show that the proposed framework has the capability of providing a cybersecurity classification performance that is reliable for the modern Security Operations Center (SOC) environment and real-time cyber threat analysis applications.

J. Confusion Matrix Analysis, Threat Classification

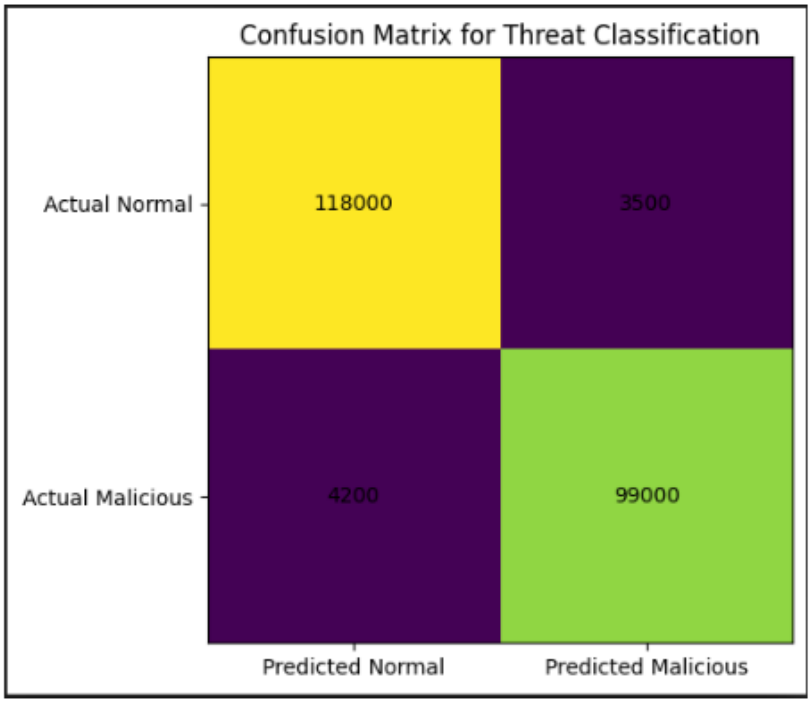


Figure 10: This image shows how to use the confusion matrix for the classification of cybersecurity threats in the intelligent cybersecurity threat classification framework

The proposed LLM-Driven Threat Classification Framework for cybersecurity threat detection is shown in Figure 10, while the confusion matrix analysis is presented in Table 8.Figure 10 shows the proposed LLM-Driven Threat Classification Framework for cybersecurity threat detection and Table 8 provides the confusion matrix analysis [34]. The confusion matrix is used to assess the accuracy of the classification using the actual network traffic labels and the predicted ones based on the framework. The accuracy of detecting normal traffic records was 118,000, while the accuracy of detecting malicious traffic records was 99,000, which demonstrated that the model had a high accuracy rate and strong capability in the field of cybersecurity classification. The framework generated relatively low misclassification rates of 3,500 false positives and 4,200 false negatives, which shows good performance with anomaly detection and lower rates of misclassification. This reduces the amount of false positives and alerts that security systems generate, and increases the accuracy of any alerts generated by the system [35]. The findings indicate that the proposed Large Language Model (LLM)-based cybersecurity framework effectively categorizes threats, detects intrusions effectively, and enhances the cybersecurity intelligence decision-making capabilities of the Security Operations Center (SOC), thereby supporting modern SOC operations.

VI. Discussion and Analysis

The experimental outcomes achieved using the proposed Large Language Model (LLM) based Threat Correlation and Governance Automation Framework show enhancements in the cybersecurity threat detection and incident response efficiency, and intelligent automation of governance processes in Security Operations Centers (SOCs). The performance comparison analysis showed that the proposed framework performed well in terms of Accuracy, Precision, Recall, and F1-Score values, outperforming the traditional SOC systems, thus ensuring the effectiveness of network activity detection of malicious activities and minimizing the error in cybersecurity classification [36]. It used Artificial Intelligence (AI), Machine Learning (ML), and transformer-based Large Language Models to achieve advanced contextual reasoning, intelligent alert prioritization, and multi-source threat intelligence correlation [37]. The False Positive Rate analysis also revealed that the proposed model, which utilizes

LLM, drastically reduced the amount of unwanted alerts generated by the SOC system compared to traditional and ML-based SOC systems. This decrease in false positives is crucial as too many alerts can cause analyst fatigue, delayed incident response, and inefficiency in today's cybersecurity landscape. The Incident Response Time analysis further validated that the proposed framework also facilitated speedy decision making on cybersecurity matters and quicker threat response timelines by automating the summarization of incidents and providing smart recommendations for threat responses [38]. Furthermore, the Threat Correlation Efficiency evaluation demonstrated that the LLM-based framework offered significantly better correlation performance compared to traditional cybersecurity solutions, emphasizing its ability to uncover intricate attack relationships and patterns of malicious activity from diverse security data sources [39]. The network traffic data analysis charts generated from the UNSW-NB15 dataset also informed the researchers about network traffic behaviors, protocol distributions, the usage of services, the frequency of malicious traffic, and the network connection states that are typically the cause of cybersecurity incidents [40]. Based on the ROC Curve analysis, the proposed threat detection model showed high True Positive Rate and low False Positive Rate, demonstrating that the model has good classification ability, thus the reliability of the proposed model was verified [41]. Likewise, the Confusion Matrix evaluation showed that the framework was effective for malicious and normal traffic record detection with relatively low misclassifications, and high classification accuracy [42]. In addition, the implementation of governance automation capabilities that are related to frameworks like MITRE ATT&CK and NIST improved the compliance validation, risk assessment, and cybersecurity-reporting processes [43]. The results also suggest that the proposed LLM based framework is a scalable, intelligent and efficient cybersecurity solution that can enhance threat intelligence correlation, operational resilience, governance automation and real-time decision making in contemporary enterprise Security Operations Centers.

VII. Future Work

Future work on the proposed Large Language Model (LLM)–Driven Threat Correlation and Governance Automation Framework can be extended to enhance its scalability, real-time intelligence abilities, autonomous response mechanisms, and advanced cybersecurity reasoning for future Security Operations Centers (SOCs). A key area for future research is how to integrate real-time streaming cybersecurity data from cloud infrastructures, Internet of Things (IoT) devices, edge computing environments and multi-cloud enterprise systems to enhance continuous monitoring of threats and adaptive cybersecurity analytics [57]. The application of more sophisticated Retrieval-Augmented Generation (RAG) architectures and domain-specific cybersecurity LLMs to improve contextual reasoning, cyber threat intelligence interpretation and automated investigation of attacks is also a topic for future research. Moreover, embedding Explainable Artificial Intelligence (XAI) technology into the automated cybersecurity decision-making processes could enhance transparency and trust by delivering interpretable threat analysis and governance suggestions to SOC analysts [58]. The creation of self-contained AI-powered systems that automatically respond to cyber incidents, isolate affected devices, and develop remediation plans in real-time without human intervention is another area of research that holds great promise. Other future frameworks could also integrate federated learning and distributed architectures for AI to enable the sharing of collaborative threat intelligence among various organizations without compromising data privacy and security [59]. Moreover, blockchain-based security measures can enhance the transparency of governance, audit integrity, and secure threat intelligence sharing. The use of AI in SOCs can be further enhanced with the ability to scale its capabilities to handle multilingual cybersecurity intelligence analysis, insider threat detection, ransomware predictions, and advanced persistent threat (APT) analysis. Future research will further test the proposed framework with larger enterprise scale real world datasets and real SOC infrastructure to validate the ability to scale, be robust and effective in operation in dynamic cyber threat conditions [60]. These developments would help build self-adaptive, intelligent and autonomous cybersecurity ecosystems that can tackle evolving cyber threats in a complex digital landscape.

VIII. Conclusion

This study introduced a Large Language Model (LLM) – Driven Threat Correlation and Governance Automation Framework to improve intelligent cybersecurity operations in today's Security Operations Centers (SOC). The research was focused on the big challenges of cybersecurity that are typically encountered in traditional SOCs: too many security alerts, false positives, slow incident response, lack of context for threat analysis, and ineffective governance management. The suggested framework leverages Artificial Intelligence (AI), Machine Learning (ML), Natural Language Processing (NLP), and transformer-based Large Language Models, achieving more than just success in enhancing cyber threat detection, intelligent incident correlation, governance automation, and real-time cybersecurity decision-making processes; it has revolutionized the entire domain of cybersecurity. The framework examined the UNSW-NB15 intrusion detection dataset and multi-source cybersecurity information to understand how network traffic behaves, classify malicious traffic and create intelligent threat intelligence insights. The experimental results showed that the proposed LLM-based framework outperformed the traditional cyber security and ML cyber security approaches in terms of accuracy, precision, recall, F1-Score, threat correlation efficiency and incident response time. The number of false positives were reduced and threat detection accuracy enhanced, further reinforcing the benefits of combining contextual reasoning and AI-powered automation into cybersecurity operations. Moreover, governance

was strengthened by the integration of governance automation features that are compatible with cybersecurity frameworks and standards, including MITRE ATT&CK and NIST. The results show the potential of LLMs to revolutionize modern SOC operations, offering scalable, adaptable, and intelligent cybersecurity solutions that can tackle the ever-changing nature of cyber threats in complex digital landscapes. In summary, the proposed framework helps to pave the way for further research and development in AI-driven cybersecurity solutions and lays the groundwork for the evolution of smart cyber defense systems and innovative governance automation technologies for enterprise security infrastructures.

Funding: This research received no external funding.
Conflicts of Interest: The authors declare no conflict of interest.
Publisher's Note: All claims expressed in this article are solely those of the authors and do not necessarily represent those of their affiliated organizations, or those of the publisher, the editors and the reviewers.

References

[1]. Wu, T., Yang, S., Liu, S., Nguyen, D., Jang, S., & Abuadbba, A. (2024). ThreatModeling-LLM: Automating threat modeling using large language models for banking system. arXiv preprint arXiv:2411.17058.
[2]. Cadet, E., Etim, E. D., Essien, I. A., Erigha, E. D., Babatunde, L. A., Ajayi, J. O., & Obuse, E. (2024). Large language models for cybersecurity policy compliance and risk mitigation. International Journal of Scientific Research in Humanities and Social Sciences, 1(2), 612-643.
[3]. Alturkistani, H., & Chuprat, S. (2024). Artificial intelligence and large language models in advancing cyber threat intelligence: A systematic literature review.
[4]. Hasanov, I., Virtanen, S., Hakkala, A., & Isoaho, J. (2024). Application of large language models in cybersecurity: A systematic literature review. IEEE access, 12, 176751-176778.
[5]. Jia, R., Zhang, J., & Prescot, J. (2024). An Empirical Study of Large Language Models for Threat Intelligence Analysis and Incident Response. Journal of Computing Innovations and Applications, 2(1), 99-110.
[6]. Zangana, H. M. (2024). Harnessing the power of large language models. Application of Large Language Models (LLMs) for Software Vulnerability Detection, 1(6).
[7]. Ferrag, M. A., Alwahedi, F., Battah, A., Cherif, B., Mechri, A., & Tihanyi, N. (2024). Generative ai and large language models for cyber security: All insights you need. Available at SSRN 4853709.
[8]. Vasugi, T. (2024). An Intelligent Risk-Aware AI and LLM Platform for Secure Banking Operations and Trade Safety Analytics in Cloud-Based Web Applications. International Journal of Research and Applied Innovations, 7(6), 11845-11851.
[9]. Cui, T., Wang, Y., Fu, C., Xiao, Y., Li, S., Deng, X., ... & Li, Q. (2024). Risk taxonomy, mitigation, and assessment benchmarks of large language model systems. arXiv preprint arXiv:2401.05778.
[10]. Chamberlain, J. A. (2023). SAP-Integrated Large Language Models for Secure Cloud-Based Enterprise Analytics and Risk Detection. International Journal of Engineering & Extended Technologies Research (IJEETR), 5(6), 7567-7574.
[11]. Gaskell, A. R. (2024). Towards Understanding the Ethical and Operational Implications of Large Language Models in a Law Enforcement Environment (Doctoral dissertation, Macquarie University).
[12]. Boddupally, H. L. (2023). Automating Incident Triage and Root Cause Intelligence Through Large Language Model–Driven Correlation of System Logs and Operational Metrics in Large-Scale Distributed Environments. International Journal of Engineering & Extended Technologies Research (IJEETR), 5(6), 7676-7688.
[13]. Ahmed, M., Wei, J., & Al-Shaer, E. (2024, June). Prompting LLM to enforce and validate CIS critical security control. In Proceedings of the 29th ACM symposium on access control models and technologies (pp. 93-104).
[14]. Kakarla, R. (2024). LLM-Based Autonomous Remediation for DevSecOps Pipelines. The Eastasouth Journal of Information System and Computer Science, 2(02), 179-188.
[15]. Park, M., Tanaka, H., Chen, W., Kim, J., & Kulkarni, A. (2024). A Trustworthy AI and Data Governance Architecture for Ensuring Integrity and Ethics in Large Language Model Deployments across Enterprise Platforms.
[16]. Rahman, M. N., Mohammad, T., & Virtanen, S. (2024). Leveraging large language models for network traffic analysis: Design, implementation, and evaluation of an llm-powered system for cyber incident reconstruction (Doctoral dissertation, Ph. D. dissertation, University of Turku, 2024.[Online]. Available: https://www. utupub. fi/bitstream/handle/10024/179397/Rahman_Naeemur_Thesis. pdf).
[17]. Ong, T. W. M. C. (2022). LLM-Enhanced Adaptive Machine Learning Framework for Financial Cloud Security Cache-Aware Threat Detection, Multi-Modal Risk Analytics, Flash Storage Optimization, and ERP Integration. International Journal of Research and Applied Innovations, 5(4), 7377-7384.
[18]. Abdali, S., Anarfi, R., Barberan, C. J., He, J., & Shayegani, E. (2024). Securing large language models: Threats, vulnerabilities and responsible practices. arXiv preprint arXiv:2403.12503.
[19]. Cimmino, G. (2024). Large language models in cybersecurity: Digital defense and ethical challenge. Authorea Preprints.

[20]. Mohsin, A., Janicke, H., Wood, A., Sarker, I. H., Maglaras, L., & Janjua, N. (2024). Can we trust large language models generated code? a framework for in-context learning, security patterns, and code evaluations across diverse llms. arXiv preprint arXiv:2406.12513.

[21]. Thota, M. R. (2024). Cognitive Platform Engineering: LLM-! ugmented Infrastructure! utomation for! utonomous Data-Intensive Systems.

[22]. Surampudi, Y. (2024). Big Data Meets LLMs: A New Era of Incident Monitoring. Libertatem Media Private Limited.

[23]. Lin, H. (2024). Ethical and scalable automation: A governance and compliance framework for business applications. arXiv preprint arXiv:2409.16872.

[24]. Cohen, O., Agmon, G. A., Shabtai, A., & Puzis, R. (2024). The Information Security Awareness of Large Language Models. arXiv preprint arXiv:2411.13207.

[25]. Vollem, S. (2024). From Deterministic Pipelines to Intelligent Orchestration: A Transformer-Driven Framework for LLM-Augmented DevOps Automation. International Journal of Research Publications in Engineering, Technology and Management (IJRPETM), 7(1), 9964-9975.

[26]. Itonin, L., Caldwell, N., & Richardson, A. (2024). Leveraging large language models for autonomous red teaming in simulating advanced ransomware attacks. Authorea Preprints.

[27]. Nowrozy, R. (2024, July). GPTs or grim position threats? the potential impacts of large language models on non-managerial jobs and certifications in cybersecurity. In Informatics (Vol. 11, No. 3, p. 45). MDPI.

[28]. Lanka, P., Gupta, K., & Varol, C. (2024). Intelligent threat detection—AI-driven analysis of honeypot data to counter cyber threats. Electronics, 13(13), 2465.

[29]. Amigoni, N., & RUINI, G. (2023). Automating cyber threat analysis with LLMs: a methodology for building and serving knowledge graphs.

[30]. Janjeva, A., Harris, A., Mercer, S., Kasprzyk, A. M., & Gausen, A. (2023). The rapid rise of generative AI: Assessing risks to safety and security.

[31]. Janjeva, A., Harris, A., Mercer, S., Kasprzyk, A. M., & Gausen, A. (2023). The rapid rise of generative AI: Assessing risks to safety and security.

[32]. Lebed, S. V., Namiot, D. E., Zubareva, E. V., Khenkin, P. V., Vorobeva, A. A., & Svichkar, D. A. (2024, December). Large Language Models in Cyberattacks. In Doklady Mathematics (Vol. 110, No. Suppl 2, pp. S510-S520). Moscow: Pleiades Publishing.

[33]. Bianco, A. (2024). Automatic Cybersecurity Risk Analysis (Doctoral dissertation, Politecnico di Torino).

[34]. Liu, Y., Yao, Y., Ton, J. F., Zhang, X., Guo, R., Cheng, H., ... & Li, H. (2023). Trustworthy llms: a survey and guideline for evaluating large language models' alignment. arXiv preprint arXiv:2308.05374.

[35]. Sambucci, L., & Paraschiv, E. A. (2024). The accelerated integration of artificial intelligence systems and its potential to expand the vulnerability of the critical infrastructure. Romanian Journal of Information Technology and Automatic Control, 34(3), 131-148.

[36]. Ndibe, O. S., & Ufomba, P. O. (2024). A review of applying AI for cybersecurity: Opportunities, risks, and mitigation strategies. Applied Sciences, Computing, and Energy, 1(1), 140-156.

[37]. Jiang, T. (2024). AutoPenGPT: Highly automated penetration testing framework based on LLM (Doctoral dissertation, PhD thesis, University of Auckland).

[38]. Zhou, W., Zhu, X., Han, Q. L., Li, L., Chen, X., Wen, S., & Xiang, Y. (2024). The security of using large language models: A survey with emphasis on ChatGPT. IEEE/CAA Journal of Automatica Sinica, 12(1), 1-26.

[39]. Xu, J. (2024). GenAI and LLM for financial institutions: A corporate strategic survey. Available at SSRN 4988118.

[40]. Baig, A. (2024). Accessing the role of artificial intelligence in information security risk management.

Allam, H. (2024). Intelligent Automation: Leveraging LLMs in DevOps Toolchains. International Journal of AI, BigData, Computational and Management Studies, 5(4), 81-94.

[41]. Mozes, M., He, X., Kleinberg, B., & Griffin, L. D. (2023). Use of llms for illicit purposes: Threats, prevention measures, and vulnerabilities. arXiv preprint arXiv:2308.12833.

[42]. Rane, N. L., Tawde, A., Choudhary, S. P., & Rane, J. (2023). Contribution and performance of ChatGPT and other Large Language Models (LLM) for scientific and research advancements: a double-edged sword. International Research Journal of Modernization in Engineering Technology and Science, 5(10), 875-899.

[43]. Wilson, S. (2024). The Developer's Playbook for Large Language Model Security. " O'Reilly Media, Inc.".

[44]. Jones, R. K., & Jones, A. J. (2024). Integration of LLMs With Traditional Security Tools. Application of Large Language Models (LLMs) for Software Vulnerability Detection, 295.

[45]. Shi, H., Fang, L., Chen, X., Gu, C., Ma, K., Zhang, X., ... & Lim, E. G. (2024). Review of the opportunities and challenges to accelerate mass-scale application of smart grids with large-language models. IET Smart Grid, 7(6), 737-759.

[46]. Almeida, I. (2023). Introduction to Large Language Models for business leaders: Responsible AI strategy beyond fear and hype (Vol. 2). Now Next Later AI.

[47]. Heckel, K. M., & Weller, A. (2024). Countering autonomous cyber threats. arXiv preprint arXiv:2410.18312.

[48]. Chua, J., Li, Y., Yang, S., Wang, C., & Yao, L. (2024). Ai safety in generative ai large language models: A survey. arXiv preprint arXiv:2407.18369.

[49]. Gan, Y., Yang, Y., Ma, Z., He, P., Zeng, R., Wang, Y., ... & Ji, S. (2024). Navigating the risks: A survey of security, privacy, and ethics threats in llm-based agents. arXiv preprint arXiv:2411.09523.

[50]. Verma, A., Krishna, S., Gehrmann, S., Seshadri, M., Pradhan, A., Ault, T., ... & Phan, N. (2024). Operationalizing a threat model for red-teaming large language models (llms). arXiv preprint arXiv:2407.14937.

[51]. Aramide, O. (2024). Autonomous network monitoring using LLMs and multi-agent systems. World Journal of Advanced Engineering Technology and Sciences, 13, 974-985.

[52]. Ullah, A., Qi, G., Hussain, S., Ullah, I., & Ali, Z. (2024). The role of llms in sustainable smart cities: Applications, challenges, and future directions. arXiv preprint arXiv:2402.14596.

[53]. Agnew, W., Jiang, H. H., Sum, C., Sap, M., & Das, S. (2024). Data Defenses Against Large Language Models. arXiv preprint arXiv:2410.13138.

[54]. Crothers, E. (2024). Large Language Models: Towards Safety, Robustness, and Understanding (Doctoral dissertation, Université d'Ottawa/University of Ottawa).

[55]. Alam, M. T., Bhusal, D., Nguyen, L., & Rastogi, N. (2024). Ctibench: A benchmark for evaluating llms in cyber threat intelligence. Advances in Neural Information Processing Systems, 37, 50805-50825.

[56]. Cherukuri, R., & Yarram, V. K. (2024). From Intelligent Automation to Agentic AI: Engineering the Next Generation of Enterprise Systems. International Journal of Emerging Research in Engineering and Technology, 5(4), 142-152.

[57]. Anwar, U., Saparov, A., Rando, J., Paleka, D., Turpin, M., Hase, P., ... & Krueger, D. (2024). Foundational challenges in assuring alignment and safety of large language models. arXiv preprint arXiv:2404.09932.

[58]. Don, R. G. G. (2024). Comparative research on code vulnerability detection: Open-source vs. proprietary large language models and LSTM neural network.

[59]. Balogh, Š., Mlynček, M., Vraňák, O., & Zajac, P. (2024). Using generative AI models to support cybersecurity analysts. Electronics, 13(23), 4718.

[60]. Xia, B., Lu, Q., Zhu, L., Xing, Z., Zhao, D., & Zhang, H. (2024). Evaluation-Driven Development and Operations of LLM Agents: A Process Model and Reference Architecture. arXiv preprint arXiv:2411.13768.

[61]. Dataset Link:
https://www.kaggle.com/datasets/nazishjaveed/intrusion-detection-project