Online at: https://researchtrendsjournal.com
Indexed Journal

ISSN No: 2584-282X
Peer Reviewed Journal

INTERNATIONAL JOURNAL OF TRENDS IN EMERGING RESEARCH AND DEVELOPMENT

Volume 3; Issue 6; 2025; Page No. 122-132

Received: 09-09-2025
Accepted: 17-10-2025
Published: 17-11-2025

COGCYBER: An Ai-Powered Cyber Threat Intelligence Architecture for Adaptive Defense and Real-Time Incident Response

[1]Latesh Kumar and [2]Dr. Prince Jain

[1]Research Scholar, Department of Computer Science & Application, Mahakaushal University, Jabalpur, Madhya Pradesh, India
[2]Associate Professor, Department of Computer Science & Application, Mahakaushal University, Jabalpur, Madhya Pradesh, India

DOI: https://doi.org/10.5281/zenodo.18266224

Corresponding Author: Latesh Kumar

Abstract

The architecture of the proposed threat intelligence system, covering data preprocessing, training mechanisms, and performance metrics. Empirical analysis illustrates the model's superiority over traditional methods in detecting zero-day attacks, phishing, and malware intrusions. The paper concludes that AI-powered threat intelligence systems are essential for contemporary cybersecurity frameworks, offering scalable, adaptive, and real-time defense mechanisms that empower organizations to pre-emptively neutralize sophisticated threats and ensure operational continuity.

Keywords: AI, Threat, System and Operational, COGCYBER, Threat Intelligence, IoT

Introduction

Identification Malware Classification and Analysis Hackers pose a significant threat to computer networks and systems via malware, sometimes known as dangerous software. Traditional malware detection approaches depend on methods that rely on signatures, which can't change with the dynamic nature of threats. Positive results have been achieved using AI and ML techniques for malware classification based on structural and behavioral characteristics. A typical strategy involves classifying software samples as safe or harmful using supervised learning techniques like as decision trees, random forests, or support vector machines (SVMs) with the use of a set of extracted properties.

These attributes may be static (like variable (such as network traffic, API calls, or the use of system resources), or static (such the size of a file, its header information, or its byte sequences). Deep learning methods, such as RNNs and CNNs, have also found utility in malware detection. These models can create hierarchical feature representations from unstructured data. One example is RNNs may be trained to simulate the sequential behavior of API request sequences or network traffic patterns. They may also compare and contrast different malware detection approaches that rely on machine learning (ML), pointing out the benefits and drawbacks of each. disadvantages.

Network intrusion detection systems (NIDS) aim to prevent unauthorized access to computer networks. Traditional NIDS, employing signature and rule-based methods, are effective against known threats but struggle with novel ones. Enhanced NIDS can leverage machine learning (ML) and artificial intelligence (AI) techniques, utilizing adaptive learning from network traffic data to identify unknown attack patterns. Supervised learning algorithms, such as neural networks and decision trees, require labeled datasets of both valid and malicious traffic for training. Unsupervised learning techniques, including anomaly detection and clustering, help uncover unusual network

activity without relying on labeled data.

Fraud Identification Fraudulent practices, such in cases of identity theft, fraud involving credit cards, and insurance, pose a serious threat to both individuals and companies, and result in substantial financial losses. By sifting through mountains of transaction data for trends and outliers, AI and ML systems could be useful in the fight against fraud. Supervised learning algorithms like logistic regression, decision trees, and neural networks can be taught using labelled datasets that contain both legitimate and fraudulent transactions. Because of this, they can now classify fresh cases according to their characteristics. Among these traits could be the device's fingerprints, transaction values, location information, or user activity patterns.

Unsupervised learning methods, such as clustering or anomaly detection, may be used to identify anomalies or unexpected patterns in transactional data in the absence of labeled examples. When new forms of fraud arise that don't conform to established patterns, these techniques shine. Combining graph theory with furthermore, by capitalizing on the relational aspect of networks, fraud detection using these approaches has shown some encouraging results transactional data. Finding suspicious subgraphs or odd connection patterns may be phrased as the challenge of identifying fraud via the representation of Transactions inside a network or graph, whereby nodes represent entities (such accounts or individuals) and edges denote connections or relationships.

Literature Review

Harris, Lorenzaj. (2025) [6]. Organizations rely on threat information, which present cybersecurity frameworks, in order to detect, assess, and react to potential security threats. Traditional threat detection mechanisms, reliant on rule-based models, often fail since attack patterns are always changing, calling for more sophisticated defenses. Anomaly detection powered by artificial intelligence (AI) and its incorporation into security operations centers (SOCs) is the focus of this article to enhance threat intelligence. AI-powered models Real-time anomaly detection is provided by these systems, especially those using methods of machine learning and deep learning. This contributes to enhancing the accuracy of threat identification while limiting false positives.

Wajid, Faheem *et al*. (2021) [7]. Conventional Security Operations Centers (SOCs) are struggling with real-time detection and mitigation of sophisticated threats. AI-driven threat hunting has emerged as a transformative solution, enhancing SOC capabilities through automated threat detection, improved cyber protection measures, and expedited event response. This technology leverages behavioral analytics and machine learning to identify hidden threats proactively. By monitoring vast volumes of security data in real-time, SOC teams can detect new threats quickly. AI algorithms help in recognizing anomalies in network activities and provide actionable insights, predictive analytics, and automated responses, thereby strengthening SOC operations.

Asad, Fatima *et al*. (2025) [8]. Artificial intelligence (AI) is transforming cybersecurity by enhancing threat prediction, detection, and prevention. With the increase in frequency and complexity of cyberattacks, traditional security measures are becoming inadequate. AI technologies, such as machine learning (ML) and natural language processing (NLP), enable security teams to analyze vast amounts of data for patterns, allowing for quick identification of threats. AI's predictive capabilities assess historical data to recognize emerging attack patterns, providing organizations with the ability to anticipate and prevent potential threats. By detecting anomalies in network activity, AI helps security professionals take preventive measures, ensuring that defenses remain effective as hackers evolve their tactics.

Sheriffdeen Olayinka Kayode (2022) [9]" "Innovating Cyber Defense: AI and ML for Next-Gen Threats" examines the transformative impact of artificial intelligence (AI) and machine learning (ML) on cybersecurity. The research highlights the necessity for a shift in cybersecurity policies due to the inadequateness of traditional defenses against sophisticated cyber threats. AI and ML are presented as pivotal tools for enhancing cyber defense through advanced algorithms and predictive analytics. Organizations can proactively identify and mitigate risks in real time, automate response mechanisms, detect anomalies, and uncover vulnerabilities with remarkable speed and precision.

Ebunoluwa, Adewunmi *et al*. (2025) [10]. Cybersecurity has advanced to require intricate defenses capable of detecting and managing dynamic attacks. Traditional products like endpoint protection and firewalls are now inadequate against sophisticated threats. Deception-based security, particularly honeypots, is increasingly utilized to attract and analyze attackers. However, static honeypots struggle with advanced persistent threats (APTs) and automated systems. In response, AI-powered honeypots have emerged, leveraging automated responses and machine learning to enhance their effectiveness in threat detection, analysis, and adaptation.

Research Methodology

COGCYBER - An AI-Powered Cyber Threat Intelligence System: Maximizing Big Data's Potential for Superior Cyber Defense

Cyberattacks are more common, complex, and damaging than ever before. The number of entry points for malicious actors is rising in tandem with the proliferation of internet-connected gadgets and systems. To safeguard enterprises from the ever-increasing danger of cyber-attacks, Effective cyber security solutions are now more important than ever. This necessity has led to CTI's emergence as a vital resource for businesses to identify, evaluate, and combat cyber dangers before they happen.

Collecting, evaluating, and sharing data about cyber hazards to an organization-whether real or perceived-is what's known as "cyber threat intelligence" (CTI). The tactics, procedures, and techniques used by cybercriminals are illuminated, along with the Indicators of Compromises (IoCs) that may be utilized to detect and avoid such assaults. Organizations struggle to efficiently gather, process, and interpret CTI because to the rapidity and amount of data produced by contemporary information systems and networks. Big data is useful in this context. "Big Data" is a way to characterize these complex and large databases. produced by today's computer networks and information systems. Traditional data processing approaches struggle to

decipher the information generated by these systems because to its volume, velocity, and diversity. Big data technologies, however, have enabled the real-time storage, processing, and analysis of enormous datasets.

Intelligence on Cyber Threats (CTI): A Preliminaries

Organizations conduct computing threat intelligence (CTI) to gather, assess, and disseminate information regarding cyber risks that could impact their IT assets and infrastructure. The global cyber security market, valued at over $173.5 billion in 2022, is expected to exceed $266.2 billion by 2027, driven by an 8.9% CAGR as businesses prioritize cyber security to mitigate potential attacks. Cyber-attacks have become increasingly sophisticated, with hackers employing various techniques, including coaxing users into executing harmful files and exploiting zero-day vulnerabilities. Moreover, adversaries are developing new attack methods that allow them to hide within legitimate systems.

Table 1: Methods for Cyber Threat Intelligence (CTI) and Details on Them

Protocols	Description
STIX	The XML-based language known as Structured Threat Information expression (STIX) is used to communicate threat intelligence. A standard for defining cyber threat intelligence, including malware, campaigns and incidents is provided by STIX (Zhou et al., 2022).
TAXII	A mechanism for exchanging cyber threat intelligence is called Trusted Automated exchange of Indicator Information (TAXII). Organisations can communicate cyber threat intelligence in a secure, automated fashion by using the services defined by TAXII.
OpenIOC	An XML-based standard called Open Indicators of Compromise (OpenIOC) is used to share threat intelligence. A common language for describing indicators of compromise, such as file hashes, IP addresses and domain names, is provided by OpenIOC (Sakellariou 2023).
CybOX	Cyber observables expression CybOX that can be seen in network traffic, system logs and other sources of security data. Cyber Observable expression (CybOX) is an XML-based language for defining these objects. It is a standardized approach to describe cyber observables, such as file objects, network connections and email messages.
MISP	A platform for exchanging threat intelligence is called the Malware Information Sharing Platform (MISP). MISP offers a suite of tools for gathering, archiving and disseminating cyber threat intelligence, such as malware samples, indicators of compromise and threat actor data.
IODEF	Information concerning security incidents can be sent using the Incident Object Description Exchange Format (IODEF), an XML-based format. IODEF offers a common terminology for describing security incidents, together with information on their time frame, impact and affected assets.
CIF	An open-source framework for gathering and disseminating information on cyber threats is called Collective Intelligence Framework (CIF) (Lin *et al.*, 2023). CIF compiles threat intelligence from various sources and offers a selection of tools for data analysis and visualization.
CRITs	An open-source platform called Collaborative Research into Threats (CRITs) is used to gather, evaluate and share information about cyber threats. CRITs offer a set of technologies for gathering, storing and correlating threat intelligence, such as malware samples, indicators of compromise and threat actor data.

COGCYBER: The Proposed Architecture: A Cyber Threat Information (CTI) system enhances the collection and dissemination of threat data by automatically sourcing information from various platforms, including OSINT feeds and system logs. It employs technologies such as data mining, Machine Learning (ML), Deep Learning (DL), and Natural Language Processing (NLP) to analyze the data, identifying trends and potential threats more efficiently.

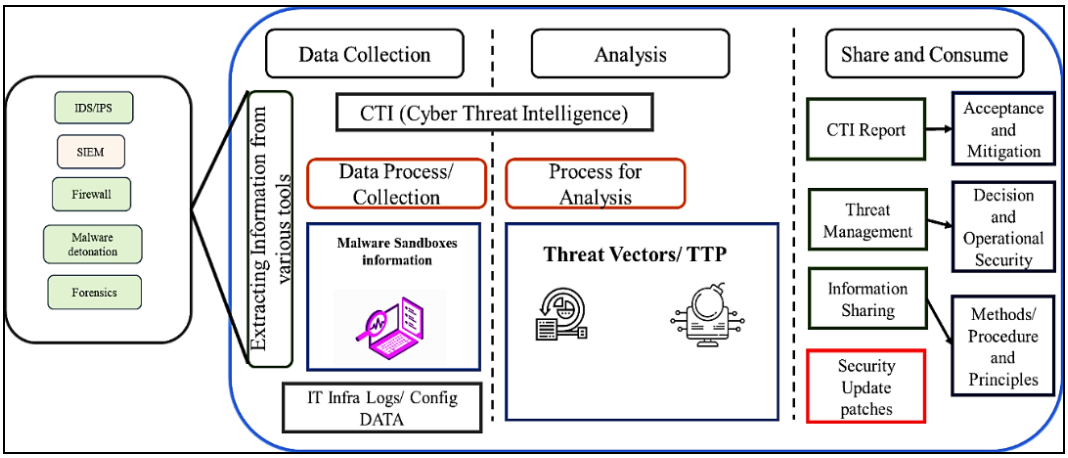


Fig1: Proposed Framework of CTI

Table 2: Some of the Tools, Techniques and Attack Detection of CTI

Tools	Techniques	Attack Examples
Malte go	Open-Source Intelligence (OSINT)	Phishing
Shodan	Dark web monitoring	Ransomware
Virus Total	Signature-based detection	Distributed Denial of Service (DDoS) attacks
Snort	Network-based intrusion detection	Man-In-The-Middle (MITM) attacks
Bro	Network security monitoring	Advanced Persistent Threats (APTs)
Yara	Rule-based detection	Malware infections
FireEye	Threat intelligence platform	Spear-phishing
IBM X-Force	Security research and insights	Zero-day exploits
CrowdStrike	Endpoint detection and response	Fileless attacks

An Integrated Cyber Threat Intelligence Architecture for Proactive Defense and Enhanced Incident Response

Organizations must take preventative measures to ensure cyber security in order in order keeping up with the ever-evolving sophistication of cyber-attacks. This necessitates regularly identifying, assessing, and reacting to any dangers prior to their occurrence. can do significant damage. An essential step in this direction involves creating Cyber Threat Intelligence (CTI), which may help companies with the data and insights they need to properly protect their digital assets. Information concerning possible cyber dangers is systematically gathered, analyzed, and used in a variety of ways; these processes make up CTI. The main goal is to provide enterprises with practical information that will help them strengthen their security, prioritize investments, and react quickly and effectively to cyber-attacks. To effectively manage the risks posed by the constantly shifting cyber threat environment, enterprises must remain one step ahead of their enemies.

The study's overarching goal is to provide a unified CTI architecture that can improve incident response capabilities and go above and beyond conventional methods by facilitating the gathering, analyzing, and use of data about cyber threats. By using this design, businesses may better comprehend the current state of cyber threats, strengthen their defenses, and lessen the blow of cyberattacks.

Data Analysis

COGCYBER - An Ai-Powered Cyber Threat Intelligence System: Maximizing Big Data's Potential for Superior Cyber Defense

The experimental setup aims to construct a Security Operations Center (SOC) that, by combining CTI with big data technology, can detect and respond to cyber-attacks as they happen. Some examples of open-source software are Apache Spark, Apache Hadoop, and Apache Kafka big data technologies that went into building the SOC. Others include MISP, OpenCTI, and The Hive, which are CTI tools. The SOAR part of the SOC is constructed with the use of free and open-source software like Kibana, Elasticsearch, and Cortex. Here are the parts that make up the experimental setup:

1. **Data Ingestion:** This part makes use of Apache Kafka so that the big data platform may get data from several sources. Some examples of such places include security logs, system logs, and logs of network traffic. Distributed File System (HDFS) by Apache Hadoop is where the data is kept for further processing. The data intake modules are shown and described in Table 1.
2. **Data Processing:** The data includes tasks such as cleaning, normalizing, and feature engineering. processing that Apache Spark does on the imported data. After processing, the data is saved in HDFS for future use in analytics.
3. **Threat Intelligence Integration:** Here, we use MISP and OpenCTI to correlate the integrated data set with data from other sources of threat information. Following this, the processed data is supplemented with background information on recognized vulnerabilities, threats, and Indicators of Compromise (IOCs) by means of the threat intelligence data.
4. **ML Models:** Here, supported This enhanced data is used for the purpose of training several models that are capable of detecting and categorizing cyber threats. These models include logistic regression, decision trees, random forests, support vector machines (SVMs), and likelihood ratio (KNNs) hazards.
5. **Cyber Threat Detection in Real-time:** In this case, the trained ML models are used in real-time to identify and categorize cyber threats. The ML is received by the SOAR component of the SOC. model outputs and uses them to trigger an automatic reaction.

6. **Automated Response:** Cortex, Elasticsearch, and Kibana were used to build the SOAR component of the SOC. When threats are discovered, this component automatically blocks IP addresses, quarantines computers, and informs security staff.

Table 3: Data Sources and Technologies

Data Sources	Description
Social media	Gather threat intelligence data from various social media platforms.
Open-Source Intelligence (OSINT) Feeds	Collect publicly available information and intelligence feeds.
Network Traffic Logs	Capture and analyze network traffic data to identify potential threats.
System Event Logs	Monitor system events and logs to detect security- related activities.
SIEM	Ingest security event data from Security Information and Event Management systems.
IDS	Collect intrusion detection system logs for analyzing detected threats.
IPS	Capture intrusion prevention system data to identify and prevent network intrusions.
Firewalls	Extract logs and data from firewalls to analyze network traffic and security events.
Malware Detection Units	Integrate antivirus and anti-malware systems to analyze malware detection data.
Forensics Tools	Utilize forensics tools to investigate security incidents and gather evidence.

Testing and Validating the Experimental Setup

We test the experimental setup with real-world datasets that include system logs, security logs, and network traffic logs. Precision is used to assess ML model performance, recall, accuracy, and metrics like F1-score. We test the SOAR security orchestration architecture component to see how well it can automate the detection and response process, decrease reaction time, and strengthen the safety net that the company has in place. how well SOC operates. The efficacy of the experimental apparatus was evaluated via a sequence of mock assaults. In order to implement automatic reactions in Splunk Phantom and The Hive, rules were built using Cortex and Information about potential threats was included into MISP and OpenCTI. Ansys, Elasticsearch, Hadoop, and Spark were used to gather and analyze the logs produced by the various technologies.

We developed a use case to identify and react to phishing emails in order to evaluate the CTI and SOAR configuration. The procedure is as follows:

- After Apache Kafka was used to feed the email logs into the big data platform., they were analyzed with Apache Spark to clean, normalize, and engineer features.
- Apache To store the processed data, Hadoop Distributed File System (HDFS) was used. for further analysis.

Utilizing MISP and OpenCTI, processed email logs were integrated with external threat intelligence data, incorporating Indicators of Compromise (IoCs), vulnerabilities, and threats. Machine learning models, including Random Forest and Naïve Bayes, were trained to identify and categorize phishing emails in real-time. The Security Orchestration, Automation, and Response (SOAR) component of the Security Operations Center (SOC) was employed to automate responses based on these models. This culminated in the establishment of an automated system using Splunk Phantom and The Hive via Cortex, which responds to identified phishing emails by banning addresses, quarantining emails, and notifying security personnel.

Metrics to measure the CTI

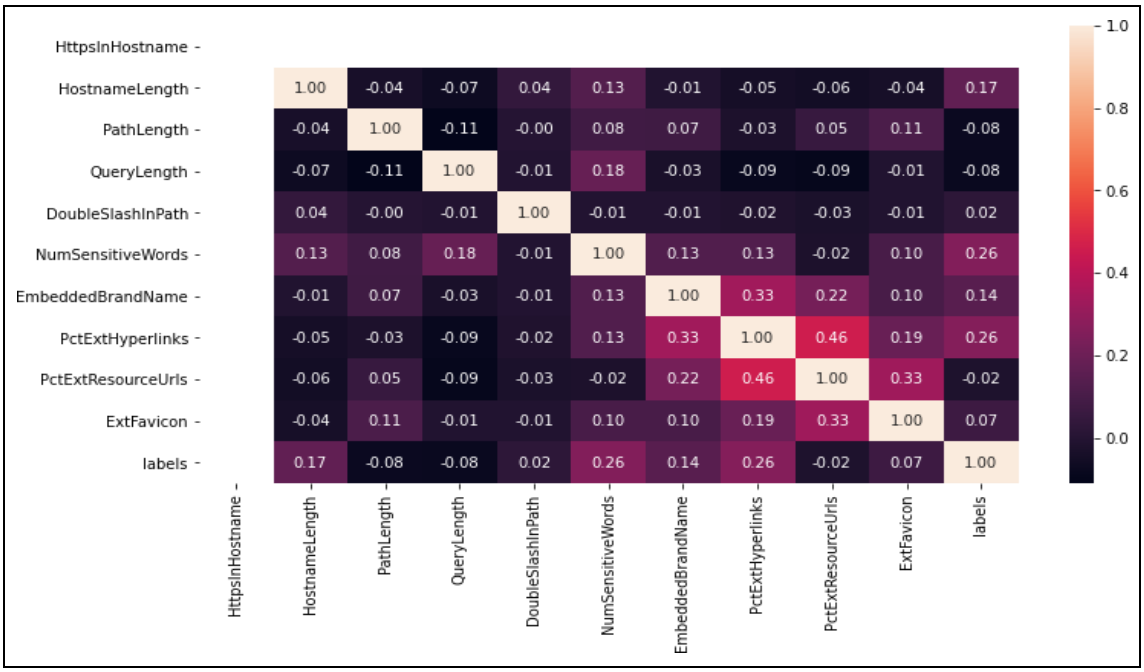
The efficacy assessment of cyber threat information is possible via the use of following metrics:

1. A program's efficacy may be gauged, in part, by how much time passes before an attack or threat is perceived. This statistic tracking how long it takes to discover a threat following it first appears.
2. The CTI program's an indicator of how well a system works is its false positive rate. A high rate of alerts that are later determined to be unfounded, squandering resources and increasing the burden of analysts, is indicated by a high false positive rate.
3. The third indication evaluates how well the CTI program deals with problems, measured in terms of the

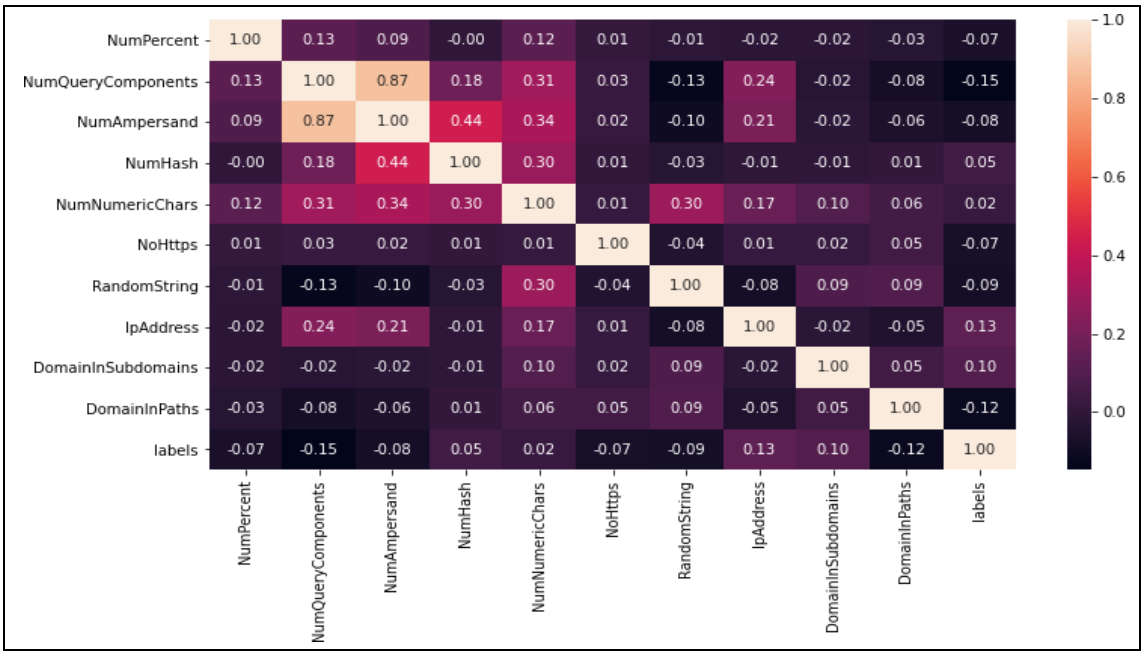
number of incidents that were effectively addressed. If more incidents are successfully addressed, the program is considered more effective.

4. The breadth of dangers addressed by the CTI program may provide insight on its performance. An effective program will take into account a wide range of potential threats rather than focusing on a small subset of them.
5. Actionable intelligence: One way in order to evaluate the CTI program's efficacy is by looking at the number of alerts that lead to actionable information. "Actionable intelligence" refers to data that may be used to avert or mitigate the consequences of an assault.

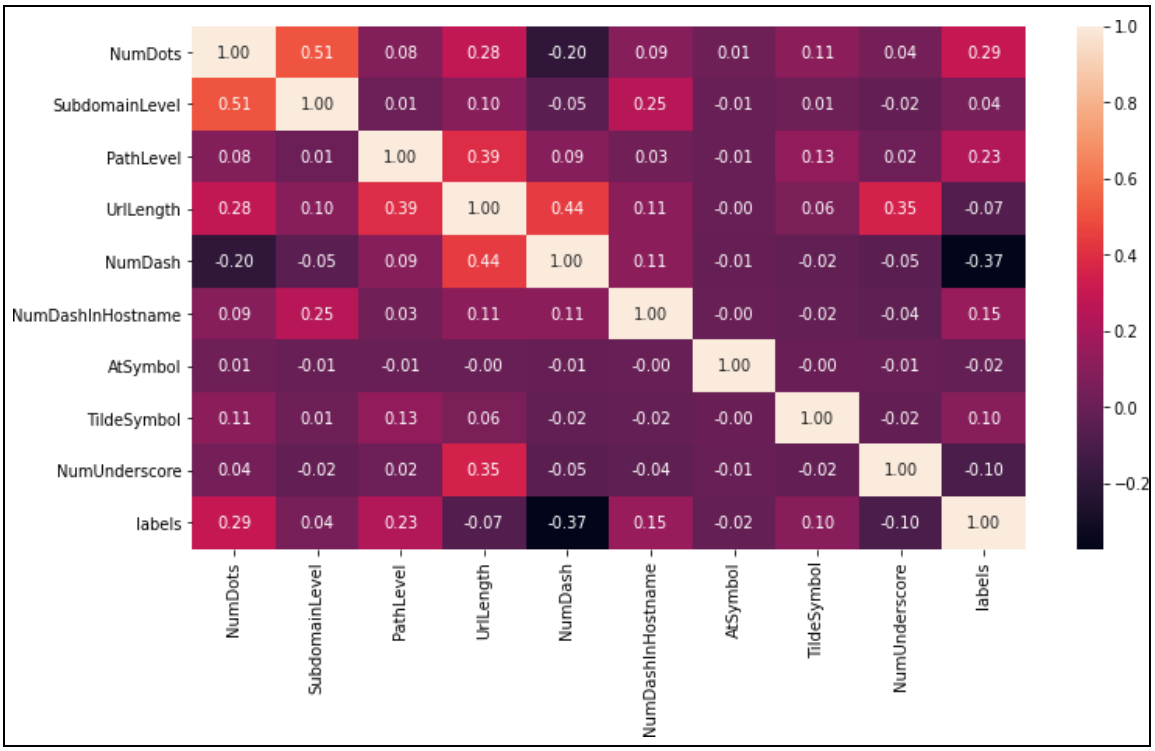
Using these indicators, one can determine the program's efficacy and pinpoint where CTI may need improvement.



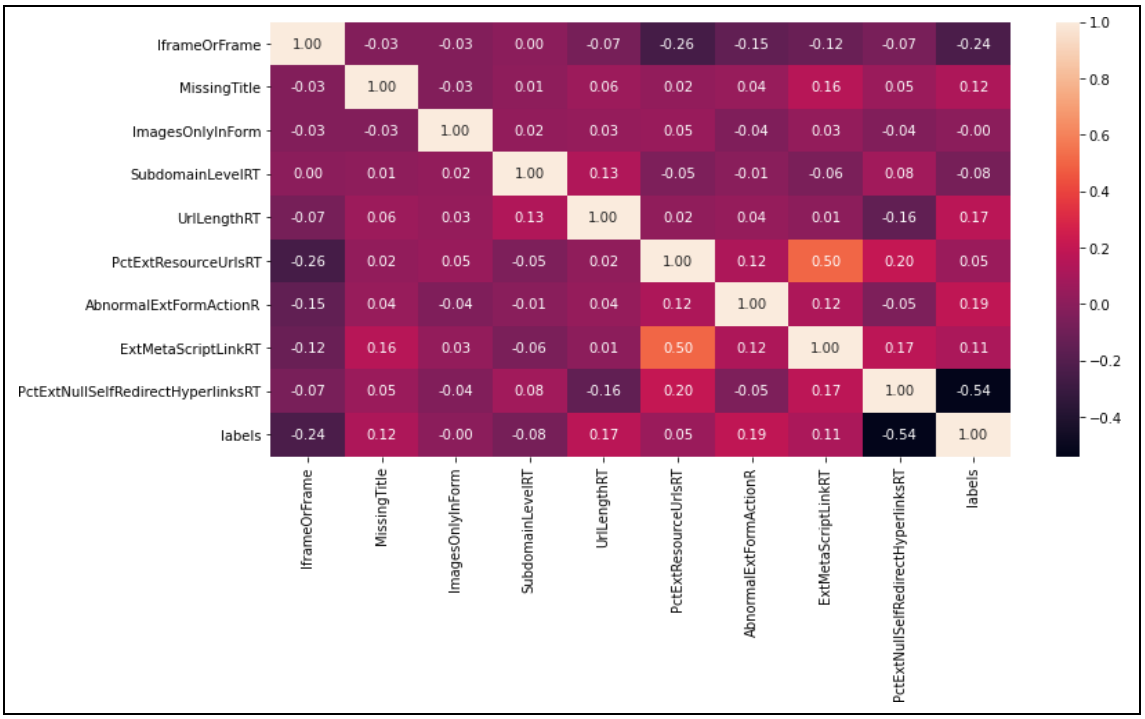
(a) Classified Host Features' Confusion Matrix



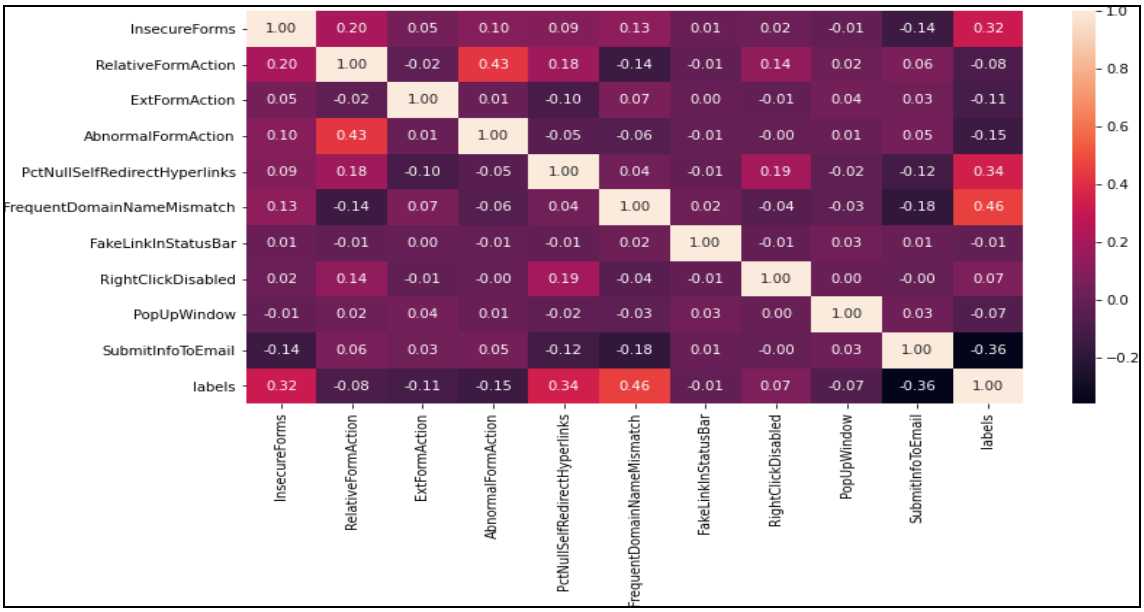
(b) URL Classification Data Confusing Matrix



(c) URL Data Classification, Subdomain Details Confusing Matrix)



(d) URL Features Confusion Matrix



(e) A URL Form Data Confusion Matrix Overall Data Confusion Matrix

Fig 2: URL Form Data Confusion

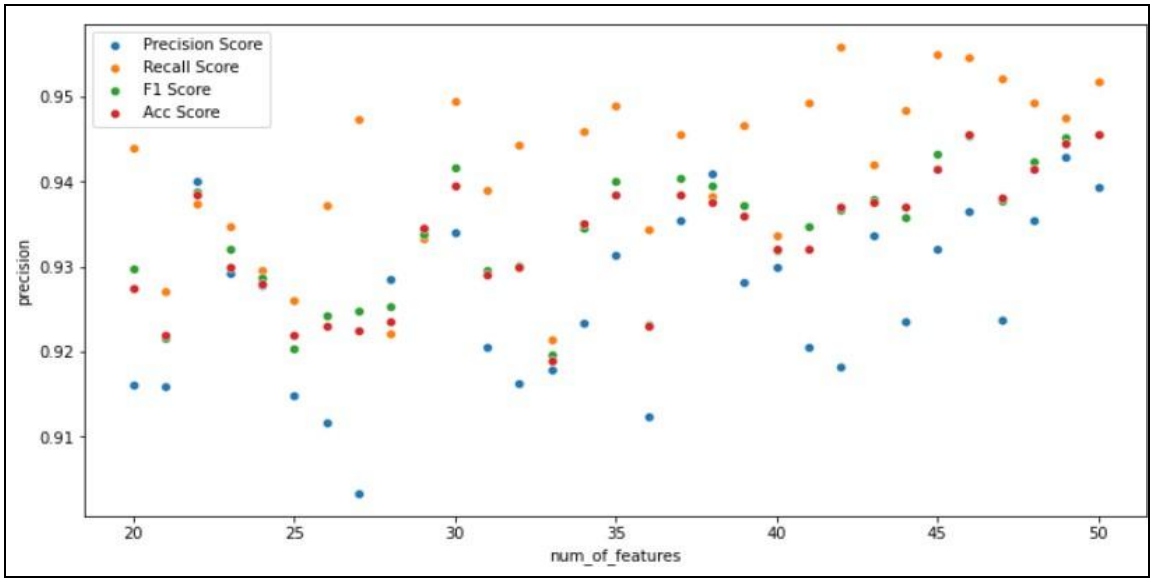


Fig 3: The NB ML Model's Performance Metric

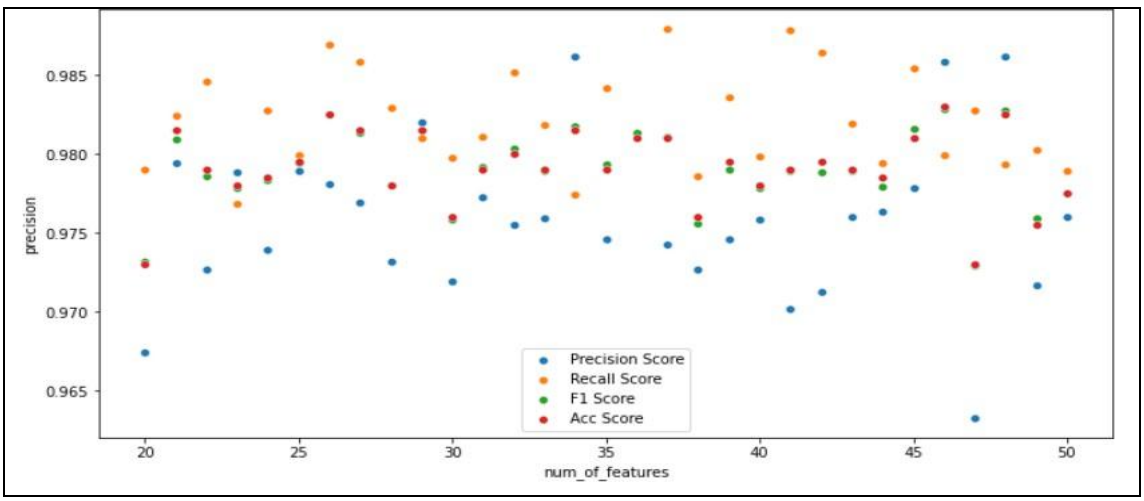


Fig 4: Ratio of RF ML Model Performance

The entire data Figure 2 displays the confusion matrix. To be considered useful, an ML model must first crucial to assess its performance measure in relation to the features it takes into account. This experimental setup aims to construct an Integrating CTI with big data technology allows the Security Operations Center (SOC) in order to identify and counteract cyberattacks instantly. The Naïve Bayes (NB) model's performance may be assessed with the use of several characteristics. When it comes to cyber security, the NB model is among the most utilized machine learning algorithms for categorization, which is based on Bayes' theorem. This theory effectively works with high-dimensional datasets and on the premise that the attributes do not interact with one another problems.

In the experimental setup, real-time data including security logs, in order to train the NB and RF models, system logs and network traffic records are used. The amount of feature engineering, the type of features (numerical, binary, categorical, etc.), and the number of features is among the numerous parameters considered while evaluating the model. was carried out. Figures 3 and 4. show some of NB and RF models were assessed using a variety of performance criteria, including as F1-score, recall, accuracy, and precision. With an eye toward determining how well the model classified and categorizing cyber risks, several metrics are crucial.

ICTI: A Cyber Threat Intelligence Architecture for Improved Incident Response and Preventative Measures

Through the use of the experimental setup, the efficacy of the integrated Cyber Threat Intelligence (iCTI) architecture was evaluated in a real-time setting. With the help of appropriate components for security, including computers, servers, firewalls, and IDS/IPS, a production environment was built to simulate the organization's architecture and network. In order to ensure smooth integration with current cyber security tools and systems, the iCTI architecture was integrated into the production environment with all the required components set. Using automation methods and APIs, real-time cyber threat information was continually gathered from many places like Twitter and other social media, as well as specialist intelligence streams (SIEM feed), as well as OSINT (Open-Source Intelligence).

Integrated Security System used for Experimentation

The iCTI architecture was smoothly integrated with pre-existing cyber security systems and technologies inside the production environment. Here are some of the tools and systems:

1. **Section One the SIEM System for Security Information and Event Management:** A security information and event management (SIEM) system may collect, correlate, and analyze log data and security events from many sources inside the network., such WAZUH, was used.
2. **Infiltration System for Intrusion Detection and Prevention (IPS):** Suricata to monitor network traffic and detect any potential intrusion attempts, and comparable systems were installed.
3. **Endpoint Protection Platforms (EPP):** To safeguard specific computers and servers, we used endpoint protection platforms like Open EDR.

Firewalls for Networks: Access control rules were enforced and incoming and outgoing network traffic was monitored using firewalls for networks and Sophos XG 210.

Attack Simulation

Figure 5 shows the experimental configuration that made use of the Splunk Attack Range v2 for attack simulation and other types of testing. To determine how well cyber security measures work and how well the integrated Cyber Threat Intelligence (iCTI) architecture responds to attacks, attack simulation is essential. To simulate an attack, one must first design controlled and realistic situations that reflect actual cyber assaults. Organizations may find security flaws and test their defenses by modeling several malware infections, data breaches, social engineering, and other forms of assaults network intrusions. Finding out how well the iCTI architecture can identify, stop, and react to these mock assaults is the main objective.

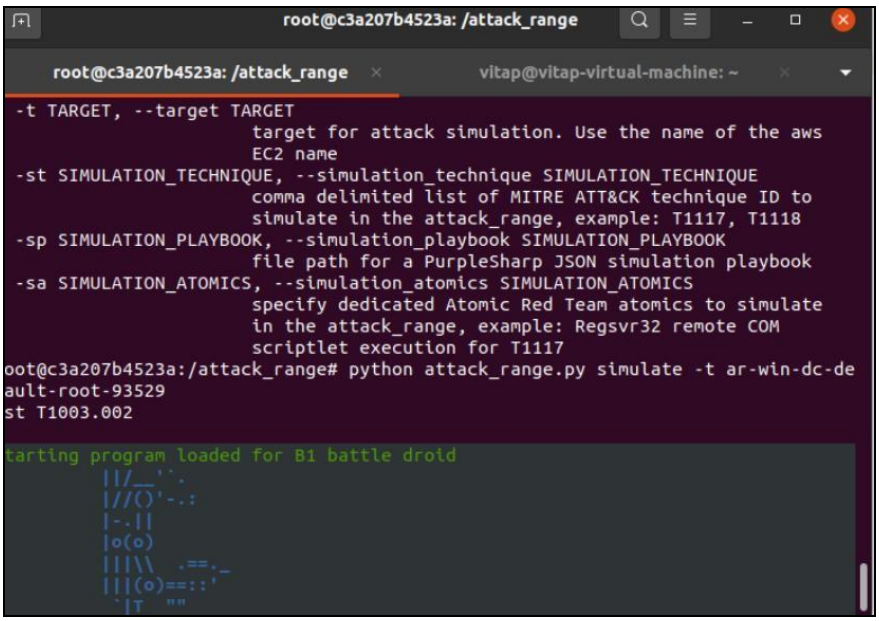


Fig 5: Attack Range Execution in the Production Environment

(a) Suricata Alert (Generic)

(b) Suricata Alert (DNS Query)

(c) Suricata Alert (Malware)

(d) Suricata Alert (External Recursive DNS Quering)

Fig 6: Suricata IDPS Alerts

Figure 6 (a) illustrates the process by which Suricata identified potentially malicious recursive DNS requests and raised alarms. Its ability to analyze the DNS protocol let it see suspicious DNS activity, such unusual query patterns or excessive recursion, which might be signs of DNS-based assaults or setup errors. The execution of the self-developed malware may be detected and alerted for by Suricata thanks to its robust signature-based detection and file extraction capabilities, as shown in Figure 6 (b). Suricata identified the harmful activity and prompted warnings to begin the proper incident response activities by evaluating the malware's behavior, payload characteristics, and network communication patterns.

The effectiveness of Suricata's DNS inspection and anomaly detection capabilities in identifying and alerting on malicious DNS requests is seen in Figure 6 (c). Suricata let enterprises react proactively to DNS-related risks by identifying and alerting on suspected malicious DNS activity by monitoring DNS traffic and comparing it against known dangerous indicators or suspicious patterns. The method by which Suricata's intrusion detection capabilities identified and notified about brute-force SSH login attempts is shown in Figure 6 (d). Suricata detected many unsuccessful login attempts from the same source IP address by analyzing network traffic and monitoring authentication events. This allowed enterprises to take fast action to neutralize the threat.

Figure 7 shows the outcomes of using Suricata's alert and splunk features to identify and notify on different cyber threats. Suricata was an integral part of the iCTI architecture's detection and response mechanism, thanks to its strong rule sets, protocol analysis, and anomaly detection capabilities. Insights into possible security problems were given by the notifications produced by Suricata, which allowed enterprises to react quickly and efficiently to lessen the impact of the assaults.

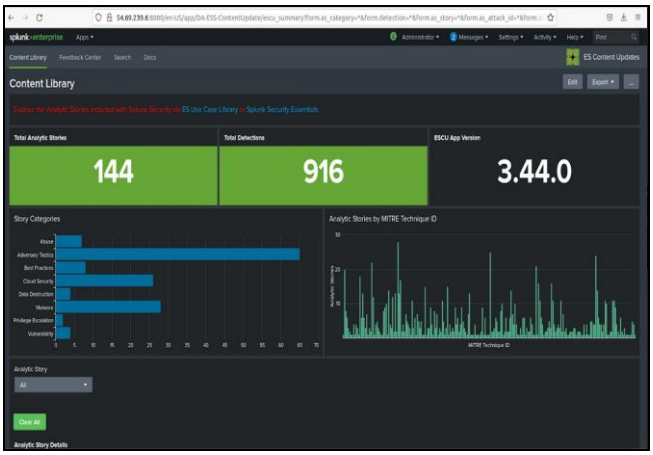


Fig 7: Screenshot of Results in SPLUNK Dashboard

The Splunk dashboard also shows details about the simulated attackers' usernames and hosts. The information gathered includes the usernames used in the mock assaults, the systems or hosts that were impacted, and any pertinent metadata linked to those entities. To ascertain the full scope of the assaults and locate any possibly compromised accounts or systems, this data is vital. Lastly, companies may get a comprehensive picture of the Splunk assault Range v2 assault simulations by using the Splunk dashboard. The contents of the simulation run, the strategies

and methods used by MITRE ATT&CK, and the accompanying login and host information are all shown in a consolidated manner. Because of this, businesses are able to conduct thorough analyses of the outcomes, find weak spots, and strengthen their defensive measures and incident response capacities.

Conclusion

One effective method for preventing cyberattacks is cyber threat intelligence (CTI) mining, which may provide previously unknown details about possible cyber threats and assaults. We need to do CTI mining generating robust and practical insights by using information gathered from many sources, both public and private.Algorithms for machine learning, data preprocessing, feature extraction, and data collecting are just a few of the ways that need to be fine-tuned for this to work. Nevertheless, issues might develop when mining CTI. The complexity and volume of data, the need for real-time analysis, and the challenge of differentiating between serious threats and false positives may all be significant hurdles.

References

1. Abbas F, Best T. Emerging threats in cybersecurity: how artificial intelligence is enhancing cyber defense. 2025. doi:10.13140/RG.2.2.15512.10245.
2. Kahan N, Reddy P. AI-powered cybersecurity: predicting and preventing future threats. 2023. (Unpublished report / white paper).
3. Vemulawada N. AI in cybersecurity for proactive threat detection and prevention. International Journal of Science and Engineering Applications. 2025;14:66–69. doi:10.7753/IJSEA1404.1010.
4. Koppireddy V, Arokiyasamy S. AI-driven cybersecurity integration: a comprehensive framework for enterprise security automation and threat management. International Journal of Advanced Research in Engineering and Technology. 2025;16:189–200.
5. John J, Mary R. AI-powered security: enhancing cyber defense in an age of emerging threats. 2022. (Unpublished manuscript / technical report).
6. Harris L. Enhancing threat intelligence with AI-driven anomaly detection in security operations centers (SOCs). 2025. (Unpublished manuscript / thesis, if applicable).
7. Wajid F, Shah W. AI-driven threat hunting: revolutionizing SOC capabilities for advanced cyber defense. 2021. doi:10.13140/RG.2.2.16198.59205.
8. Asad F, Steltzer H. Artificial intelligence in cyber defense: predicting and preventing cyber threats. 2025. doi:10.13140/RG.2.2.33128.17920.
9. Sheriffdeen OK. Innovating cyber defense: AI and machine learning for next-generation threats. 2022. (Unpublished report / white paper).
10. Ebunoluwa A, James A. AI-powered honeypots: enhancing deception technologies for cyber defense. 2025. (Unpublished manuscript / technical report).