Journal of Data Acquisition and Processing
ISSN: 1004-9037
https://sjcjycl.cn/
DOI: 10.5281/zenodo.777808

ICTI: AN INTEGRATED CYBER THREAT INTELLIGENCE ARCHITECTURE FOR PROACTIVE DEFENSE AND ENHANCED INCIDENT RESPONSE

A. Kanthimathinathan
Research Scholar, Dept. of Computer Science and Engineering, Annamalai University
Annamalainagar – 608002, Chidambaram, Tamil Nadu, Email:kanthi_88@yahoo.co.in

Dr. S. Saravanan
Assistant Professor, Dept. of Computer Science and Engineering, Annamalai University
Annamalainagar – 608002, Chidambaram, Tamil Nadu, Email: ssaravau@gmail.com

Dr. G. Ramachandran
Associate Professor, Dept. of Computer Science and Engineering, Annamalai University
Annamalainagar – 608002, Tamilnadu, India, Email: gmrama1975@gmail.com

ABSTRACT

Cyber Threat Intelligence (CTI) is the process of collecting, analyzing, and utilizing information about potential cyber threats to an organization. The goal of CTI is to provide organizations with the knowledge and understanding the need to prevent, detect, and respond to cyber-attacks. CTI involves collecting and analyzing data from a variety of sources, including Open-Source Intelligence (OSINT), social media, and specialized intelligence feeds. The data is then used to create a comprehensive view of the current threat landscape, including information on the Tactics, Techniques, and Procedures (TTPs) used by attackers, as well as the types of attacks and vulnerabilities that are most commonly exploited. Organizations can use this information to improve their overall security posture, prioritize security investments, and respond more effectively to threats. Hence, this work proposes an integrated CTI (iCTI) architecture, which can also be used to develop proactive defense strategies and enhance incident response capabilities, helping organizations to better manage the risks posed by cyber threats.

The proposed integrated Cyber Threat Intelligence (iCTI) architecture combines the systematic collection, analysis, and the utilization of CTI with proactive defense strategies and enhanced incident response capabilities. By leveraging diverse data sources, including OSINT, social media, and specialized feeds, the architecture provides organizations with a comprehensive understanding of the current threat landscape, enabling the identification of emerging trends, prevalent attack vectors, and attacker tactics. The architecture emphasizes the development of proactive defense strategies based on the analysis of attacker TTPs, allowing organizations to prevent, detect, and mitigate potential cyber attacks. Additionally, the CTI architecture strengthens incident response capabilities by providing timely and actionable intelligence, enabling organizations to respond swiftly and effectively to minimize the impact of cyber attacks. Through the integration of CTI, organizations can proactively defend against

threats, optimize their security posture, and safeguard critical assets and information in the dynamic cyber security landscape.

Keywords: Cyber Threat Intelligence (CTI), integrated architecture, proactive defense, enhanced incident response, Open-Source Intelligence (OSINT), attacker Tactics, Techniques and Procedures (TTPs), incident response capabilities.

1. INTRODUCTION

In todays rapidly evolving digital landscape, the proliferation of cyber threats poses significant challenges to organizations across various sectors [1]. The ever increasing complexity and sophistication of cyber attacks necessitate a proactive approach to cyber security, where organizations must anticipate, detect, and respond to threats before they can cause substantial harm. Cyber Threat Intelligence (CTI) has emerged as a vital process in this endeavor, providing organizations with the knowledge and understanding required to safeguard their digital assets effectively [2][3].

CTI encompasses a range of activities that involve the systematic collection, analysis, and utilization of information about potential cyber threats. Its primary objective is to empower organizations with actionable insights, enabling them to bolster their security posture, prioritize investments, to respond swiftly and effectively to cyber attacks. By staying ahead of adversaries, organizations can better manage the risks associated with the dynamic and ever-evolving cyber threat landscape [4].

The purpose of this research is to propose an integrated CTI architecture, not only facilitates the core objectives of collecting, analyzing, and utilizing cyber threat information but also goes beyond traditional approaches by enabling the development of proactive defense strategies and enhancing incident response capabilities. By adopting this architecture, organizations can gain a comprehensive understanding of the threat landscape, enhance their defensive measures, and minimize the impact of cyber attacks.

The proposed CTI architecture takes a holistic approach to information gathering, leveraging various sources such as OSINT, social media, and specialized intelligence feeds. OSINT provides valuable insights by analyzing publicly available information, while social media platforms offer real-time indicators of emerging threats and potential attack vectors. Specialized intelligence feeds, often provided by trusted third-party vendors or industry-specific organizations, offer targeted and contextualized threat information. By aggregating data from these diverse sources, organizations can obtain a comprehensive view of the current threat landscape, enabling them to identify emerging trends, prevalent attack vectors, the tools and techniques employed by cyber adversaries.

1.1 Problem Statement and Motivation for the Work

Organizations face an increasing number of sophisticated cyber threats that pose significant risks to their critical assets and operations [5][6]. Traditional approaches to cyber security, such as reactive defense measures and incident response plans, are often inadequate in addressing the evolving threat landscape. There is a need for an integrated Cyber Threat

Intelligence (iCTI) architecture that combines comprehensive threat analysis, proactive defense strategies, and enhanced incident response capabilities to effectively manage and mitigate cyber threats.

Existing cyber security frameworks often lack the integration of diverse data sources and fail to provide a holistic view of the threat landscape [7][8]. Organizations struggle to collect, analyze, and utilize cyber threat intelligence from multiple sources, including open-source intelligence, social media, and specialized intelligence feeds. Without a comprehensive understanding of emerging threats, prevalent attack vectors, and attacker tactics, organizations are ill-equipped to develop proactive defense strategies and prioritize security investments effectively.

Moreover, incident response capabilities often suffer from delays and inefficiencies due to the lack of timely and actionable intelligence. Organizations struggle to respond swiftly and effectively to cyber-attacks, resulting in prolonged downtime, data breaches, and financial losses. The absence of a well-defined incident response framework tailored to the organization's specific threat landscape hinders their ability to minimize the impact of attacks and recover quickly.

In light of these challenges, there is a pressing need for an iCTI architecture that addresses the limitations of existing approaches. This architecture should enable organizations to collect and analyze diverse threat intelligence, understand attacker TTPs, develop proactive defense strategies, and enhance incident response capabilities. By doing so, organizations can effectively manage the risks posed by cyber threats, optimize their security posture, respond swiftly and effectively to cyber-attacks.

A key focus of the proposed architecture is the identification and understanding of the TTPs utilized by attackers. By studying the TTPs employed in cyber attacks, organizations can recognize patterns and signatures that aid in the detection and prevention of future attacks. This knowledge empowers organizations to develop proactive defense strategies, fortify their security infrastructure, and mitigate vulnerabilities before they can be exploited by malicious actors.

Moreover, the iCTI architecture strengthens an organization's incident response capabilities by providing timely and actionable intelligence. The collected data, analyzed within the context of an organization's unique infrastructure and systems, enables the development of tailored incident response plans. These plans outline pre-defined actions, procedures, and escalation protocols to be executed in the event of a cyber attack. By having a well - structured incident response framework in places and organizations, this can minimize the impact of attacks, reduce downtime, and accelerate recovery efforts.

By embracing the proposed CTI architecture, organizations can not only improve their ability to prevent, detect, and respond to cyber threats but also enhance their overall cyber security posture. The insights gained from the comprehensive analysis of threat data enable organizations to make informed decisions regarding security investments, prioritize remediation efforts, and align their cyber security strategies with emerging threats. This

proactive approach empowers organizations to stay ahead of cyber adversaries, reducing their susceptibility to attacks and safeguarding their critical assets and sensitive information.

1.2 Novelty of the Proposed iCTI

- Holistic integration of diverse data sources (open-source intelligence, social media, and specialized feeds) in a unified framework.
- Emphasis on proactive defense strategies based on attacker TTPs.
- Incorporation of specialized intelligence feeds for targeted and context-specific threat information.
- Enhancement of incident response capabilities through timely and actionable intelligence.
- Optimization of security investments by aligning resources with identified vulnerabilities and emerging threats.
- Facilitation of real-time threat intelligence sharing and collaboration with trusted external entities.
- Scalable and adaptable architecture to accommodate evolving cyber threats and technologies.

1.3 Contributions in this Paper

- The proposed research introduces an integrated Cyber Threat Intelligence (iCTI) architecture that combines multiple data sources, including OSINT, social media, and specialized intelligence feeds. This integration provides a comprehensive view of the threat landscape, enabling organizations to gather diverse and valuable insights.
- The research emphasizes the development of proactive defense strategies based on the analysis of attacker TTPs. By understanding TTPs, organizations can anticipate and mitigate potential cyber attacks before they occur, enhancing their overall security posture.
- The proposed iCTI architecture enhances incident response capabilities by providing timely and actionable intelligence. By leveraging collected threat data, organizations can develop tailored incident response plans and execute predefined actions, procedures, and escalation protocols, allowing for a swift and effective response to minimize the impact of cyber attacks.
- The research focuses on providing organizations with a comprehensive understanding of the threat landscape. By analyzing diverse data sources and identifying emerging trends and prevalent attack vectors, organizations can make informed decisions regarding security investments and prioritize remediation efforts.
- The architecture incorporates specialized intelligence feeds that offer targeted and contextualized threat information. This enables organizations to receive relevant and timely intelligence specific to their industry or infrastructure, enhancing the accuracy and relevance of their threat analysis.
- By leveraging the proposed iCTI architecture, organizations can optimize their security investments by aligning resources with identified vulnerabilities and emerging threats. This ensures that critical systems and assets receive the highest level of protection, minimizing the risk of potential attacks.

- The architecture facilitates real-time threat intelligence sharing and collaboration with trusted external entities. By participating in information sharing initiatives, organizations can benefit from collective intelligence, enabling faster detection and response to emerging threats.

1.4 Organization of this Paper

In Section I, Introduction provides an overview of the importance of Cyber Threat Intelligence (CTI) in proactive defense and enhanced incident response. Section II Literature Survey conducts a comprehensive review of existing research and literature related to CTI. It examines the current state of the field, identifies key challenges, and explores the various approaches and methodologies used in CTI. Section III Proposed iCTI Architecture explains the role of CTI in proactive defense and discusses the Cyber Threat Intelligence Architecture for Enhanced Incident Response. This section presents the proposed architecture, highlighting its components, functionalities, and how it integrates with existing security systems. Section IV, the Experimental Setup and Results focuses on the real-time environment created through the implementation of the experimental setup. It also discusses the Integrated Security system used for experimentation. This section provides a detailed analysis of the results, including the attack simulations conducted and how the iCTI architecture effectively defends against these attacks. The tools used to implement the iCTI system are also discussed. Section V Conclusion concludes the paper, summarizing the key findings and contributions of the research. It also highlights the practical implications and future scope of the proposed iCTI architecture in strengthening proactive defense and enhancing incident response capabilities.

2. LITERATURE SURVEY

This section discusses the related works based on the SOAR and CTI with Big data. Big data technologies are suggested by the author [6] as a framework for integrating Security Orchestration, Automation, and Response (SOAR) with Cyber Threat Intelligence (CTI). By utilising the real-time analytics and processing capabilities of big data technologies, the proposed framework seeks to increase the effectiveness and efficiency of security incident response. The author outlines the framework's architecture, which covers SOAR and CTI workflow implementation as well as the ingestion, processing, and analysis of security data from diverse sources.

The authors of this paper [7] begin by defining CTI and discussing its significance in the modern world. They next give an overview of big data analytics and machine learning approaches. The use of these approaches in CTI has recently been the subject of extensive research, with this survey paper providing a thorough overview of that work. It covers subjects including data collection and pre-processing, feature selection and extraction, classification and clustering, as well as visualisation and reporting. CTI-CORE [8], employs big data analytics to examine the vast quantities of security data for the purpose of identifying and combating cyber threats. Data pre-processing, analysis, and data gathering make up the framework's three core parts. To gather pertinent security data, the data collecting component makes use of a variety of data sources, including logs, network traffic, and threat intelligence feeds. The data is cleaned and transformed for analysis by the data pre-processing component. Data mining methods and machine learning techniques are used in the analysis component to identify security risks and extract insights.

The creation of a platform for CTI makes effective use of big data technology for the study and visualisation of security-related data. The authors proposed a system design that combines several data sources, such as internal security logs and external threat intelligence feeds, and processes them using a big data processing engine to produce useful information for security analysts. The software also has capabilities like a dashboard for tracking security occurrences in real-time and a collaboration module for exchanging information between security teams [9].A thorough analysis of the state-of-the-art in big data analytics for cyber threat intelligence is provided by the author [10]. It discusses a variety of topics, including data sources, big data technology, machine learning strategies, and CTI applications. The writers present insights into new research prospects while discussing the difficulties and directions this subject is headed in the future. The authors [11] brings out a methodology for processing massive amounts of data and producing insightful data using big data technologies like Hadoop, Spark, and Elasticsearch. The suggested framework is used in a case study to analyse cyber threat information pertaining to a particular kind of malware. Regarding accuracy, recall, and precision, the authors assess the framework's efficacy. The findings demonstrate that the suggested methodology is capable of successfully extracting useful insight from a significant amount of cyber threat data. The difficulties and possibilities of applying big data analytics for CTI, as well as the significance of CTI in the present threat environment, are discussed [12]. They also discuss the difficulties and restrictions of using big data analytics for CTI, including issues with data processing, data quality, and privacy. Table 1 shows the related works on CTI, SOAR with big data environment and its limitations.

Threat intelligence feeds, Security Information and Event Management (SIEM) systems, and incident response automation tools are all included in the framework of actionable cyber threat intelligence for automated incident response [19][20][21][22]. Through the incorporation of real-time threat intelligence and automation approaches, this effort seeks to improve the capabilities of conventional incident response systems. The constructions of automated incident response playbooks, interaction with SIEM systems, collecting and processing of threat intelligence data are only a few of the framework's essential elements covered by the author. They stress the significance of intelligence that can be used, or actionable intelligence, which offers precise and pertinent information to support efficient incident response operations [17].

Table 1 Related Works on CTI, SOAR with Big Data Environment and its Limitations

Techniques Used	Parameters Measured	Limitations
Apache Hadoop, Apache Spark, Apache Flink, Apache NiFi, and Elasticsearch	Efficiency, accuracy, and scalability of the framework	Lack of testing with real-world data, limited evaluation of the framework in comparison to existing solutions
Hadoop, Spark, and Elasticsearch	Precision, recall, and accuracy	Data Scalability, Data Quality and Variability, Data Privacy and Security, Resource Requirements

Hadoop, Apache Storm, Apache Cassandra, Elasticsearch, and Kibana	Detection accuracy, processing time, and scalability	Data Volume and Variety, Data Quality and Reliability, Scalability and Performance, Privacy and Security
Hadoop, Apache Spark, and Apache Cassandra	Accuracy, scalability, and performance of the platform	Scalability, Data Integration
Apache Spark, Apache Kafka, Elasticsearch, Kibana, and Apache Cassandra	Detection accuracy, processing time, and scalability	Data Volume and Velocity, Data Quality and Accuracy
Hadoop and Spark	Efficiency, accuracy, and scalability of the framework	Limited evaluation with real-world data, lack of comparison with existing solutions

Utilise automation and orchestration to improve the honeypots' detection and response capabilities [23]. Honeypots are decoy devices used to lure and capture attackers and gain useful information about their strategies [24]. In particular, behavioural honeypots actively observe and examine the behaviour of attackers by simulating real-world systems and applications. To automate the deployment and administration of these honeypots, the authors suggest a framework that integrates behavioural honeypots with a SOAR engine. The methodology intends to increase the speed and efficacy of identifying and addressing online threats [18].

3. PROPOSED iCTI ARCHITECTURE

Figure 1 illustrates the iCTI architecture, which integrates Zeek, Kafka, Metron, and iCTI components for Cyber Threat Intelligence (CTI) analysis. The architecture has different phases namely Data collection, Data Ingestion, Data processing, CTI integration, Threat Analysis and Visualization.

- **Data Collection**: The Zeek Network Security Monitoring (NSM) tool plays a crucial role in data collection. Zeek passively monitors network traffic by capturing packets and generating log files. These log files contain detailed information about network activities, including IP addresses, protocols, ports, connection details, and extracted files. Here Zeek collects network traffic by passively monitoring network packets. Zeek generates log files containing detailed information about network activities, such as IP addresses, protocols, ports, connection details, and extracted files.

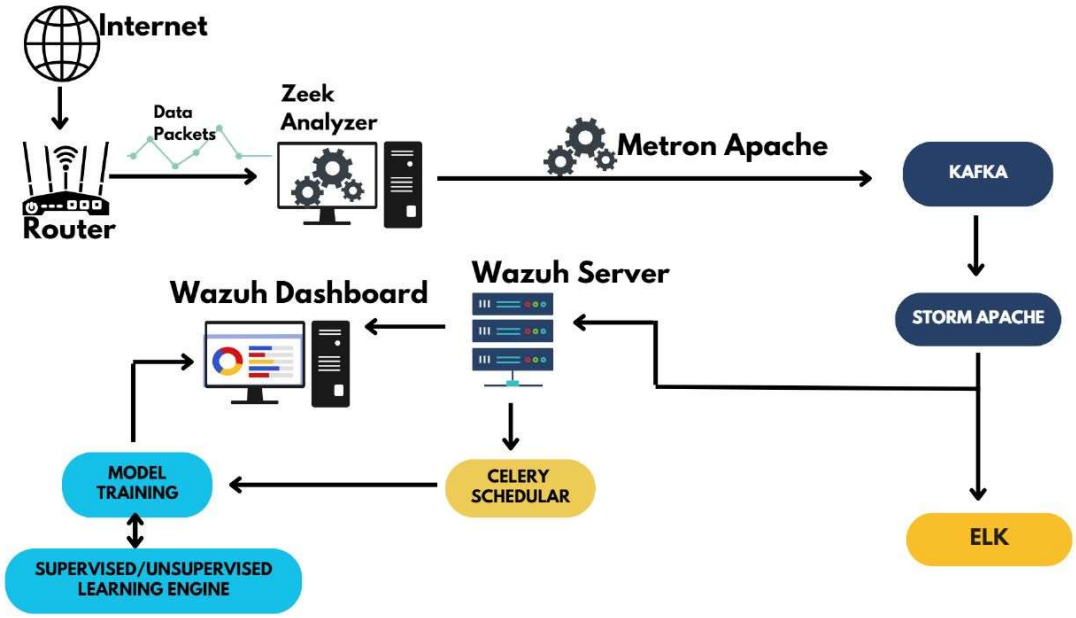


Figure 1 Proposed iCTI Architecture

- **Data Ingestion**: The collected Zeek log files are ingested into the Apache Kafka distributed streaming platform. Kafka acts as a scalable, fault-tolerant, and high-throughput data pipeline. It provides reliable ingestion of large volumes of data streams, ensuring data durability and allowing for real-time processing. The Zeek log files are ingested into the Apache Kafka distributed streaming platform. Kafka acts as a scalable and fault-tolerant data pipeline, ensuring reliable ingestion of the Zeek data. Zeek log files are partitioned and distributed across Kafka topics for efficient processing.
- **Data Processing**: The ingested Zeek data is processed and analyzed using the Apache Metron platform. Metron is an open-source solution for real-time data processing, threat detection, and security analytics. It combines various Apache projects to provide a comprehensive security analytics framework. Apache Metron performs real-time data processing and analysis on the ingested Zeek data.
    a. **Real-time Stream Processing:** Metron leverages Apache Storm, a distributed real-time stream processing system, to perform continuous analysis of the Zeek data streams. Storm allows for parallel processing of the data in a fault-tolerant and scalable manner. Apache Storm, a distributed real-time stream processing system, consumes the Zeek data from Kafka topics. Storm topologies are employed to process the data streams in parallel. Stream processing involves various tasks, such as data normalization, parsing, enrichment, and feature extraction.
    b. **Batch Processing:** Metron also utilizes Apache Hadoop for batch processing capabilities. Batch processing can be employed for historical analysis or processing large volumes of data that might not require real-time analysis. For historical analysis or processing large volumes of data, Apache Hadoop is utilized for batch processing capabilities. Batch jobs are executed to analyze the data stored in Hadoop Distributed

File System (HDFS). This allows for deeper analysis, correlation, and detection of patterns or trends across a larger dataset.

- **CTI Integration:** The architecture incorporates CTI feeds and intelligence sources into the Metron platform. These CTI feeds provide valuable information about known threat indicators, such as malicious IP addresses, domains, URLs, or file hashes. The integration of CTI enhances the threat detection capabilities of the system by enriching the Zeek data with up-to-date intelligence.CTI feeds and intelligence sources are integrated into the Metron platform.CTI data, containing known threat indicators and intelligence, is acquired and updated regularly. The CTI data is combined with the processed Zeek data to enrich it with up-to-date threat intelligence. This enrichment enhances the detection capabilities by identifying potential threats based on known indicators, such as malicious IP addresses, domains, URLs, or file hashes.
- **Threat Analysis and Visualization:** The processed data, enriched with CTI information, undergoes threat analysis to identify potential threats and anomalies. Various analysis techniques, such as statistical analysis, machine learning algorithms, and anomaly detection, can be applied to identify malicious patterns or behaviours. The results of the analysis are visualized through a user friendly interface or dashboard, enabling security analysts to gain actionable insights and make informed decisions. The enriched data undergoes comprehensive threat analysis to identify potential threats and anomalies. Detected threats are flagged and prioritized based on their severity and potential impact. The analyzed results are visualized through a user friendly interface or dashboard, providing security analysts with actionable insights and a holistic view of the threat landscape. Visualization includes detailed reports, charts, graphs, and alerts, enabling analysts to make informed decisions and initiate appropriate incident response actions.

The proposed iCTI architecture brings together the strengths of Zeek, Kafka, Metron, and CTI integration to provide a comprehensive solution for CTI analysis. It enables organizations to effectively analyze network traffic, detect potential threats in real-time, and respond proactively to emerging cyber threats. By leveraging the power of stream processing, batch processing, and CTI integration, the architecture enhances the organization's ability to detect and mitigate cyber threats, ultimately strengthening their overall security posture.

Also, the workflow ensures a seamless flow of data across the proposed iCTI architecture, from data collection with Zeek, ingestion into Kafka, real-time and batch processing with Metron, integration of CTI feeds, and finally, comprehensive threat analysis and visualization. This end-to-end data flow allows organizations to effectively analyze network traffic, detect potential threats, and respond promptly to emerging cyber threats.

3.1 Cyber Threat Intelligence Architecture for Proactive Defense

The Cyber Threat Intelligence (CTI) architecture for proactive defense is a comprehensive framework that enables organizations to anticipate, detect, and mitigate cyber threats before they can cause significant damage. This architecture combines the systematic collection and analysis of cyber threat data with proactive measures to enhance an organization's overall security posture.

The CTI architecture starts with the collection of data from various sources, including Open-Source Intelligence (OSINT), social media platforms, and specialized intelligence feeds. OSINT provides publicly available information that can be analyzed to identify potential threats and vulnerabilities. Social media platforms offer real-time insights into emerging threats and indicators of compromise. Specialized intelligence feeds, sourced from trusted third-party vendors or industry-specific organizations, deliver targeted and contextualized threat information. By aggregating data from these diverse sources, the CTI architecture provides a comprehensive view of the threat landscape, enabling organizations to identify emerging trends, prevalent attack vectors, and the tactics used by cyber adversaries.

An essential aspect of the CTI architecture is the analysis and understanding of attacker TTPs. By studying and documenting the TTPs employed in past cyber-attacks, organizations can identify common patterns, behaviours, and indicators that can aid in the detection and prevention of future attacks. This analysis allows organizations to develop proactive defense strategies tailored to their specific environment. For example, understanding the TTPs utilized in phishing attacks can help organizations implement more robust email filtering and employee training programs to prevent successful phishing attempts.

With the insights gained from data collection and TTP analysis, organizations can strengthen their defense mechanisms and mitigate vulnerabilities. This proactive approach involves implementing security controls, such as network segmentation, intrusion detection and prevention systems, and robust access controls. The CTI architecture also enables organizations to prioritize security investments by focusing on the area's most susceptible to threats based on the analyzed data. By aligning resources with identified vulnerabilities and emerging threats, organizations can maximize the effectiveness of their security measures and mitigate risks more efficiently.

Furthermore, the CTI architecture enhances incident response capabilities. By leveraging the collected and analyzed threat data, organizations can develop pre-defined incident response plans tailored to specific attack scenarios. These plans outline the steps to be taken, roles and responsibilities of personnel, communication protocols, and escalation procedures in the event of a cyber attack. With a well-structured incident response framework in place, organizations can respond swiftly and effectively, minimizing the impact of attacks, containing the breach, and restoring normal operations in a timely manner.

The CTI architecture emphasizes a proactive approach to defense, enabling organizations to stay ahead of cyber adversaries. By continuously monitoring and analyzing the threat landscape, organizations can anticipate potential attacks, identify emerging vulnerabilities, and adapt their security measures accordingly. This architecture facilitates the development of a mature security posture that goes beyond reactive measures and empowers organizations to address threats before they materialize into significant security incidents.

3.2 Cyber Threat Intelligence Architecture for Enhanced Incident Response

Cyber Threat Intelligence (CTI) architecture for enhanced incident response is a framework designed to leverage CTI to improve the effectiveness and efficiency of incident response activities within an organization. This architecture combines the systematic collection

and analysis of threat data with the development of tailored incident response plans, enabling organizations to respond swiftly and effectively to cyber attacks.

The CTI architecture begins with the collection of relevant data from various sources, including Open-Source Intelligence (OSINT), social media platforms, internal network logs, and specialized intelligence feeds. This data provides valuable insights into the current threat landscape, including indicators of compromise, attack patterns, and emerging trends. By gathering this information, organizations can better understand the TTPs employed by attackers, as well as identify potential vulnerabilities within their own systems.

Once the data is collected, it is analyzed within the context of the organization's unique infrastructure and systems. This analysis helps to identify potential threats and vulnerabilities specific to the organization, enabling the development of tailored incident response plans. These plans outline the predefined actions, procedures, and escalation protocols to be executed in the event of a cyber attack. By having well-defined incident response plans in place, organizations can ensure a swift and coordinated response, minimizing the impact of attacks and reducing downtime.

The integration of CTI into incident response planning allows organizations to take a proactive approach. By leveraging the analyzed threat data, organizations can anticipate potential attack scenarios and develop proactive defense measures to prevent or mitigate the impact of those attacks. For example, if the analysis reveals a specific malware variant being used in recent attacks, the incident response plan can include measures such as updating antivirus signatures or implementing network controls to block known command-and-control servers associated with that malware.

The CTI architecture also facilitates real-time threat intelligence sharing and collaboration. Organizations can establish partnerships with trusted external entities, such as other organizations in the same industry or cyber security information sharing platforms, to exchange threat information and gain additional insights. By participating in information sharing initiatives, organizations can benefit from collective intelligence, enabling faster detection and response to emerging threats.

Furthermore, the CTI architecture enhances incident response capabilities by enabling organizations to prioritize and allocate resources effectively. By understanding the severity and potential impact of different types of threats, organizations can allocate resources based on the level of risk. This ensures that critical systems and assets receive the highest level of protection and incident response preparedness. The analysis of threat data also helps organizations identify recurring attack vectors or vulnerabilities that require remediation, leading to more targeted investments in security controls and measures.

By incorporating CTI into incident response processes, organizations can improve their overall incident response maturity. The architecture enables organizations to move beyond reactive approaches and adopt a proactive stance. By leveraging timely and actionable intelligence, organizations can detect and respond to incidents more swiftly, minimize the dwell

time of attackers, and reduce the overall impact of security incidents on their operations and reputation.

4. EXPERIMENTAL SETUP

The effectiveness of the integrated Cyber Threat Intelligence (iCTI) architecture was assessed in a real-time environment through the implementation of the experimental setup. A representative production environment was created, closely mimicking the organizational infrastructure and network, incorporating servers, workstations, firewalls, intrusion detection systems, and relevant security components. The iCTI architecture was integrated within the production environment, with the necessary components configured for seamless integration with existing cyber security tools and systems. Real-time CTI was continuously collected from diverse sources, including OSINT, social media platforms (Twitter), and specialized intelligence feeds (SIEM feed), utilizing automation techniques and APIs. Advanced threat detection techniques and algorithms, incorporating machine learning and artificial intelligence approaches, were applied to analyze the collected data for real-time identification of patterns, anomalies, and potential cyber threats. Real-world cyber attacks and incidents were simulated within the production environment to test the incident response capabilities. This involves generating various attack scenarios using tools such as Metasploit, Nmap, and Burp Suite, and assessing the effectiveness of the iCTI architecture in detecting, mitigating, and responding to these attacks. The experimental setup allowed for the evaluation of the iCTI architecture's performance, detection accuracy, response time, and overall efficacy in a real-time operational environment.

4.1 Integrated Security System used for Experimentation

The iCTI architecture was integrated within the production environment, seamlessly integrating with existing cyber security tools and systems. These tools and systems include:

- **Security Information and Event Management (SIEM) System:** A SIEM system, such as WAZUH was utilized to collect, correlate, and analyze security events and log data from various sources within the network. The SIEM system helps to centralize and provide a unified view of security events, enabling efficient detection and response to potential threats.
- **Intrusion Detection System (IDS) / Intrusion Prevention System (IPS):** An IDS/IPS system, such as Suricata, was deployed to monitor network traffic and detect potential intrusion attempts. The IDS/IPS system uses signature-based and behavioral-based detection methods to identify known attack patterns and anomalies, providing an additional layer of defense against cyber threats.
- **Endpoint Protection Platforms (EPP):** Endpoint protection platforms, such as OpenEDR, were employed to secure individual workstations and servers. These platforms offered features such as antivirus, anti-malware, and host-based intrusion detection, enhancing the protection of endpoints against various cyber threats.
- **Network Firewalls:** Network firewalls, Sophos XG 210, were utilized to enforce access control policies and monitor incoming and outgoing network traffic. The firewall acts as a barrier between the internal network and external sources, helping to prevent unauthorized access and malicious activities.

- **Vulnerability Assessment Tools:** Tools like Nessus were used to perform regular vulnerability scans on the network infrastructure and systems. This tool identifies potential security weaknesses, such as outdated software versions or misconfigurations, allowing proactive mitigation of vulnerabilities before they could be exploited by attackers.
- **Threat Intelligence Platforms:** Splunk is deployed to act as threat intelligence platform to aggregate and analyze threat intelligence feeds from various sources. These platforms provides insights into emerging threats, attacker TTPs, and indicators of compromise, enhancing the ability to proactively detect and respond to cyber threats.

4.2 Attack Simulation

In the experimental setup, the Splunk Attack Range v2 was utilized for attack simulation and other experimentation as shown in Figure 2. Attack simulation plays a crucial role in assessing the effectiveness of cyber security measures and evaluating the response capabilities of the integrated Cyber Threat Intelligence (iCTI) architecture. Attack simulation involves creating controlled and realistic scenarios that mimic real-world cyber attacks. By simulating various attack techniques, such as network intrusions, malware infections, social engineering, and data breaches, organizations can identify vulnerabilities in their systems and evaluate their defensive measures. The goal is to understand how well the iCTI architecture can detect, mitigate, and respond to these simulated attacks.

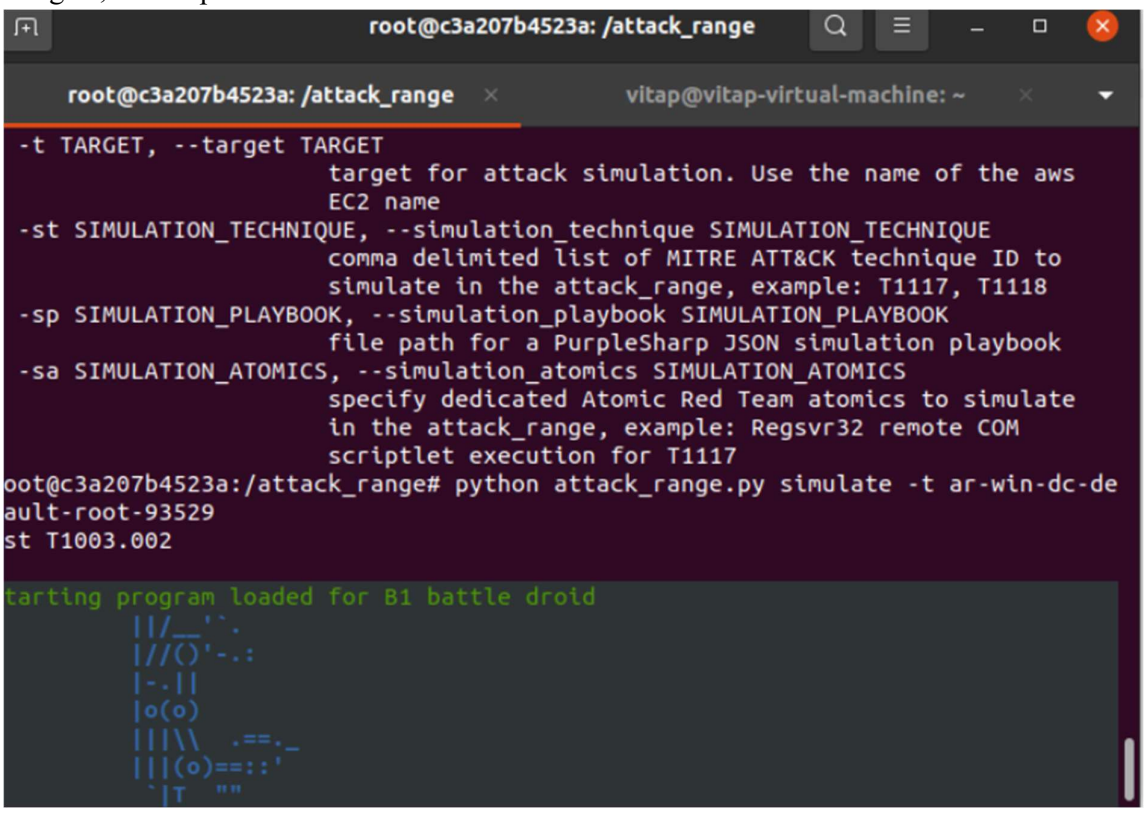


Figure 2 Attack Range Executions in the Production Environment

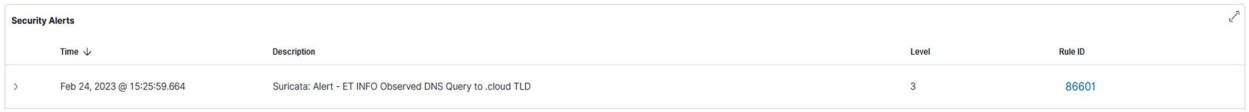
Splunk Attack Range v2 is a powerful tool specifically designed for creating a realistic attack environment. It provides pre-configured virtual machines with vulnerable applications, network configurations, and attack scenarios. These virtual machines are isolated from the

production environment, ensuring a safe and controlled testing environment. Using Splunk Attack Range v2, various attack scenarios can be generated to simulate real-world threats. This includes launching phishing campaigns, exploiting software vulnerabilities, conducting brute-force attacks, and executing malware. The tool also captures and logs the activities and events generated during the attack simulations, providing valuable data for analysis and evaluation. By incorporating Splunk Attack Range v2 into the experimental setup, the iCTI architecture's response to simulated attacks was assessed. The architecture's ability to detect and analyze the attack vectors, identify indicators of compromise, and trigger incident response actions was evaluated. The collected data from the attack simulations helped to measure the accuracy, timeliness, and effectiveness of the iCTI architecture's threat detection and response capabilities. The attack simulations provided insights into the strengths and weaknesses of the iCTI architecture, highlighting areas for improvement and fine-tuning. It allows organizations to identify gaps in their security posture, understand potential attack vectors, and optimize their incident response strategies. Additionally, the use of Splunk Attack Range v2 enhanced the realism of the experiments, providing a valuable testing ground for the iCTI architecture's performance in a controlled and safe environment. Overall, the integration of Splunk Attack Range v2 for attack simulation contributed to a comprehensive assessment of the iCTI architecture's capabilities. It allowed for a realistic evaluation of the architecture's ability to detect, respond, and mitigate cyber attacks, enabling organizations to refine their cyber security measures and enhance their overall defense against emerging threats.

(a) Suricata Alert (generic)

(b) Suricata Alert (DNS Query)

(c) Suricata Alert (Malware)



(d) Suricata Alert (External recursive DNS quering)

Figure 3 Suricata IDPS alerts

Figure 3(a) shows how Suricata successfully detected and generated alerts for suspicious recursive DNS queries. Its DNS protocol analysis capabilities allowed it to identify abnormal DNS behaviour, such as excessive recursion or anomalous query patterns, indicating potential DNS-based attacks or misconfigurations. Figure 3(b) shows how Suricata's powerful signature-based detection and file extraction capabilities enable it to identify and generate alerts

for the execution of the self-developed malware. By analyzing the malware's behaviour, payload characteristics, and network communication patterns, Suricata detected the malicious activity and triggered alerts to initiate the appropriate incident response actions. Figure 3(c) shows how Suricata's DNS inspection and anomaly detection capabilities were effective in detecting and alerting on malicious DNS queries. By analyzing DNS traffic and comparing it against known malicious indicators or suspicious patterns, Suricata identified and alerted on potential malicious DNS activities, helping organizations proactively respond to DNS-related threats. Figure 3(d) shows how Suricata's intrusion detection capabilities successfully detected and alerted on brute-force SSH login attempts. By analyzing network traffic and monitoring authentication events, Suricata identified repeated failed login attempts from the same source IP address, triggering alerts and allowing organizations to take immediate action to mitigate the attack.

The results obtained from Figure 4 shows Suricata's alert and splunk capabilities that demonstrated its effectiveness in detecting and alerting on various cyber threats. By leveraging its robust rule sets, protocol analysis, and anomaly detection features, Suricata played a vital role in the overall detection and response framework of the integrated Cyber Threat Intelligence (iCTI) architecture. The alerts generated by Suricata provided valuable insights into potential security incidents, enabling organizations to respond promptly and effectively to mitigate the impact of the attacks.

It is worth noting that while Suricata effectively detected the mentioned attacks, its performance can be further optimized by fine-tuning the rule sets, adjusting thresholds, and updating the threat intelligence feeds. Continual refinement of Suricata's configuration and rule sets can enhance its detection capabilities and reduce false positives, enabling organizations to stay resilient against evolving cyber threats.

5. RESULTS AND DISCUSSION

Figure 5 shows the Splunk dashboard which provides a comprehensive view of the simulation run, MITRE attack tactics and techniques (TTP), as well as username and host information. The Splunk dashboard showcases the details of the simulation run, including the specific attack scenarios that were executed, the duration of the simulation, and any relevant metadata associated with the run. This information helps in tracking and organizing the results of the attack simulations. In addition, the Splunk dashboard highlights the MITRE ATT&CK framework's tactics and techniques used during the attack simulations. It provides a breakdown of the different tactics employed by the simulated attacks, such as initial access, persistence, privilege escalation, and exfiltration. By mapping the attack techniques to the MITRE ATT&CK framework, organizations can gain a deeper understanding of the attack vectors and assess their security posture accordingly.

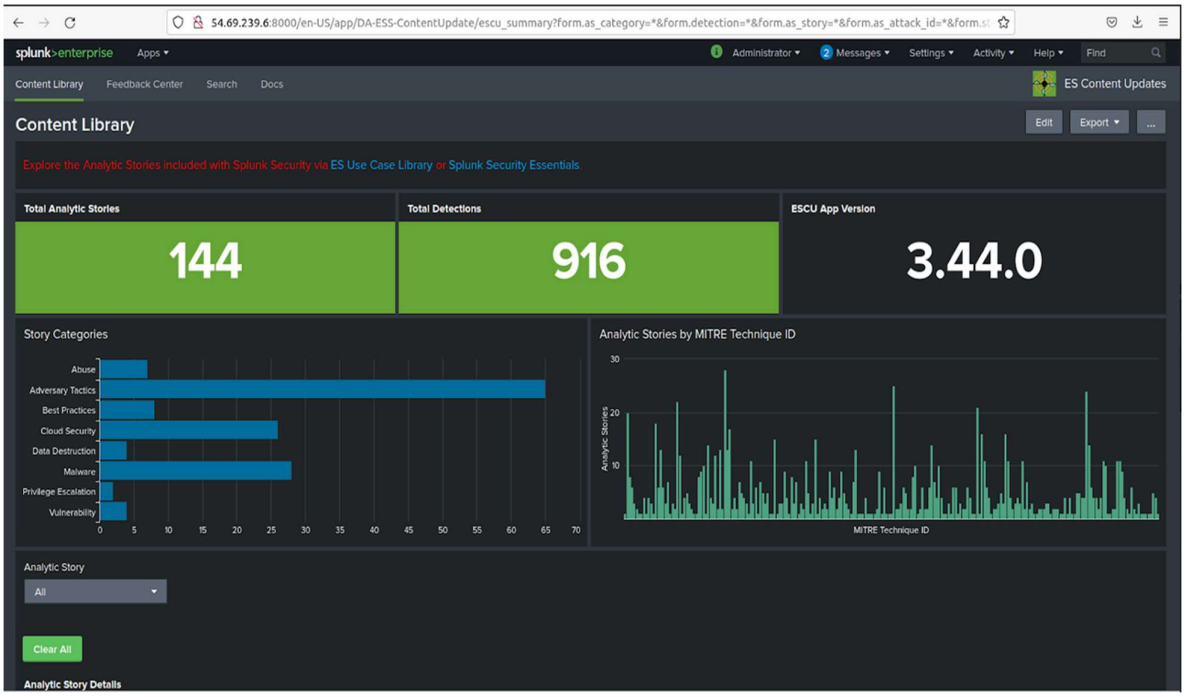


Figure 4 Screenshot of results in SPLUNK Dashboard

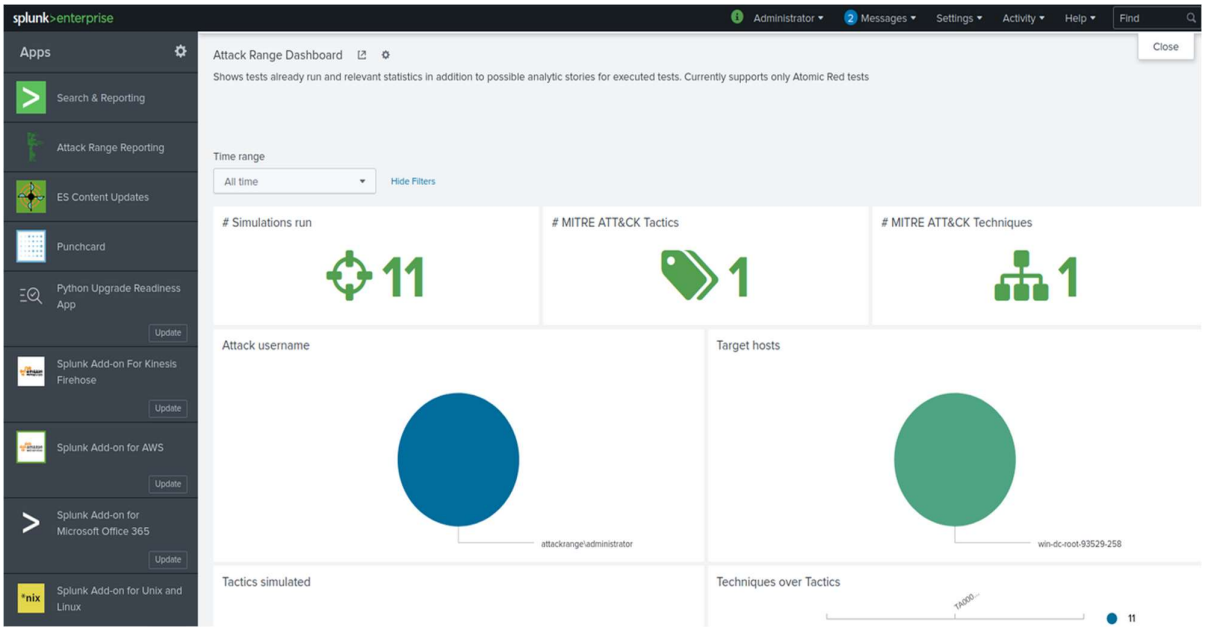


Figure 5 Screenshot of Attack Range V2 results in SPLUNK Dashboard

Also, the Splunk dashboard presents information related to the usernames and hosts involved in the attack simulations. It captures details such as the usernames used in the simulated attacks, the affected hosts or systems, and any relevant metadata associated with the user or host. This information is crucial for identifying the impact of the attacks and tracing any potential compromised accounts or systems. Finally, by leveraging the Splunk dashboard, organizations can gain a holistic view of the attack simulations conducted using Splunk Attack Range v2. It provides a consolidated display of the simulation run details, the MITRE ATT&CK

tactics and techniques employed, and the associated username and host information. This allows organizations to analyze the results effectively, identify potential vulnerabilities, and improve their defensive strategies and incident response capabilities.

6. CONCLUSION

Finally, the integrated Cyber Threat Intelligence (iCTI) architecture presented in this research offers a holistic and proactive approach to cyber security. By combining diverse data sources, including open-source intelligence, social media, and specialized intelligence feeds, the iCTI architecture provides organizations with a comprehensive view of the threat landscape. The integration of threat analysis, proactive defense strategies, and enhanced incident response capabilities enables organizations to better manage and mitigate cyber threats. Through the experimental setup, the effectiveness of the iCTI architecture was evaluated in a real-time environment. The architecture seamlessly integrated with existing cyber security tools and systems, including SIEM systems, IDS/IPS, EPPs, network firewalls, vulnerability assessment tools, and threat intelligence platforms. This integration allowed for a comprehensive assessment of the architecture's performance, detection accuracy, response time, and overall efficacy. The results of the experiments demonstrated the benefits of the iCTI architecture. Its proactive defense strategies, based on the analysis of attacker TTPs, proved effective in identifying and mitigating potential threats before they could cause significant damage. The real-time collection and analysis of diverse threat intelligence enables organizations to have a comprehensive understanding of emerging threats, prevalent attack vectors, and attacker tactics. Furthermore, the iCTI architecture enhances incident response capabilities by providing timely and actionable intelligence. This facilitates swift and effective response to cyber attacks, minimizing the impact and reducing downtime. The optimization of security investments, based on analyzed threat intelligence, allows organizations to allocate resources more effectively and enhance their overall security posture.

In summary, the iCTI architecture presented a novel and advanced solution to address the challenges faced by organizations in managing cyber threats. Its integration of diverse data sources, proactive defense strategies, and enhanced incident response capabilities showcased its effectiveness in real-time environments. By leveraging the iCTI architecture, organizations can better protect their critical assets, prioritize security investments, and respond effectively to the ever-evolving threat landscape.

The iCTI architecture presented in this research paves the way for several promising future directions. Integrating proactive threat hunting techniques can further empower organizations to actively search for and neutralize threats. Collaboration with external entities and standardized information sharing protocols can strengthen collective defense efforts. Improved threat intelligence visualization and presentation can enhance decision-making, while considerations of privacy and ethics must be addressed.

REFERENCES

1. Devi Priya V S, SC Sethuraman, Containerized cloud-based honeypot deception for tracking attackers, Scientific Reports, Nature, 2023.

2. Bucur, D., &Sgârciu, V. (2021). Big Data Analytics and Machine Learning for Cyber Threat Intelligence: A Survey. Sensors, 21(15), 5256.
3. SS Chakkaravarthy, Pranav Kompally, Saraju P Mohanty and Uma Chopalli, MyWear: A Novel Smart Garment for Automatic Continuous Vital Monitoring, IEEE Transactions on Consumer Electronics, IEEE, Vol. 67, No. 3, pp. 214-222, 2021.
4. Zhang, L., Yao, X., Liu, S., Liu, S., & Li, H. (2020). A SOAR and CTI framework with big data technologies. IEEE Access, 8, 151379-151388.
5. Gopinath M, SC Sethuraman, A comprehensive survey on deep learning based malware detection techniques, Computer Science Review, Vol. 47, February 2023, Elsevier.
6. Bucur, D., & Sgârciu, V. (2021). Big Data Analytics and Machine Learning for Cyber Threat Intelligence: A Survey. Sensors, 21(15), 5256.
7. Alkinj, I., Dehghantanha, A., Parizi, R. M., & Choo, K. K. R. (2021). CTI-CORE: A Cyber Threat Intelligence Framework for Big Data Analysis. IEEE Access, 9, 98404-98415.
8. D. Arivudainambi, K.A. Varun Kumar, S. Sibi Chakkaravarthy, P. Visu, Malware traffic classification using principal component analysis and artificial neural network for extreme surveillance, Computer Communications, Vol.147, November, 2019, pp.50-57.
9. Choi, S., & Lee, K. (2021). Development of a big data-based cyber threat intelligence platform. Information, 24(8), 4797-4802.
10. SC Sethuraman, Aditya Mitra, Kuan-Ching Li, Anisha Ghosh, M Gopinath, Nitin Sukhija, "Loki: A Physical Security Key Compatible IoT Based Lock for Protecting Physical Assets", Vol. 10, Pages. 112721-112730, IEEE Access, 2023.
11. Liu, S., Li, H., Li, J., & Sun, L. (2021). Big Data Analytics for Cyber Threat Intelligence: A Survey. IEEE Access, 9, 123018-123034.
12. Chen, W., Wu, Q., Zhao, C., Wu, Q., & Liu, Y. (2020). A Big Data Approach to Cyber Threat Intelligence Analytics. IEEE Access, 8, 162023-162038.
13. Zhang, Y., Qian, Y., Zhang, J., & Sun, L. (2020). Big Data Analytics for Cyber Threat Intelligence: Challenges and Opportunities. IEEE Access, 8, 118883-118896.
14. Dedipyaman Das, SS Chakkaravarthy, Suresh Chandra Satapathy, A Decentralized Open Web Cryptographic Standard, Computers and Electrical Engineering, Elsevier, Vol. 99, 107751, April, 2022.
15. Narayanan, S., Chandrasekaran, K., & Ganapathy, V. (2018). A big data framework for cyber threat intelligence analytics. International Journal of Computer Applications, 181(26), 9-15.
16. SS Chakkaravarthy, V. Vaidehi and Steven Walczak, Cyber Attacks on Healthcare Devices Using Unmanned Aerial Vehicles, Journal of Medical Systems, Vol.44, Article 29, Springer, 2020.
17. S. Sibi Chakkaravarthy, D. Sangeetha and V. Vaidehi, Intrusion Detection System to detect Wireless attacks in IEEE 802.11 networks, IET networks, July 2019, Volume 8, Issue 4, pp. 219- 232.
18. Nasr, K., Al-Yaseen, W., Alsmirat, M., & Jararweh, Y. (2018). Design and Implementation of a Cyber Threat Intelligence Platform for Big Data Analytics. In

Proceedings of the 2018 IEEE/ACM International Conference on Advances in Social Networks Analysis and Mining (pp. 678-685).

19. Shetty, S., Bagade, P., Mohite, S., & Kulkarni, V. (2018). A Framework for Cyber Threat Intelligence Analytics using Big Data Technologies. Procedia Computer Science, 132, 1339-1348. DOI: 10.1016/j.procs.2018.05.138.
20. Hosein, A., Tari, Z., & Yearwood, J. (2016). Big Data Analytics for Cyber Threat Intelligence. Procedia Computer Science, 82, 129-134.
21. Leite, C., den Hartog, J., Ricardo dos Santos, D., & Costante, E. (2023, January). Actionable Cyber Threat Intelligence for Automated Incident Response. In Secure IT Systems: 27th Nordic Conference, NordSec 2022, Reykjavic, Iceland, November 30–December 2, 2022, Proceedings (pp. 368-385). Cham: Springer International Publishing.
22. Bartwal, U., Mukhopadhyay, S., Negi, R., & Shukla, S. (2022, June). Security orchestration, automation, and response engine for deployment of behavioural honeypots. In 2022 IEEE Conference on Dependable and Secure Computing (DSC) (pp. 1-8). IEEE.
23. D. Sangeetha, S S Chakkaravarthy, Suresh Chandra Satapathy, Vaidehi V, Meenaloshini Vimal Cruz, Multi Keyword Searchable Attribute Based Encryption for efficient retrieval of Health Records in Cloud, Multimedia Tools and Applications, Springer, 2021.
24. SS Chakkaravarthy, D. Sangeetha, Meenalosini Vimal Cruz, V. Vaidehi and Vaidehi V, Design of Intrusion Detection Honeypot using Social Leopard Algorithm to detect IoT ransomware attacks, IEEE Access, IEEE, vol. 8, pp. 169944-169956, 2020.