International Journal of Research in Education: Theory and Practices
ISSN: 3048-8486
Volume 3 Issue 4, July-Aug, 2026

An Intelligent Cyber Threat Intelligence Framework for Network Indicator Analysis and Proactive Threat Detection Using MITRE ATT&CK

P.Premchand Goud[1], Valli Mounika[2]

[1]Assistant Professor, Department of MCA, Megha Institute of Engineering and Technology for Women, Edulabad (Village), Ghatkesar (Mandal), Medchal District, Telangana – 501301, India.

[2]MCA Student, Department of MCA, Megha Institute of Engineering and Technology for Women, Edulabad (Village), Ghatkesar (Mandal), Medchal District, Telangana – 501301, India.

Abstract. The increasing dependence on digital infrastructure has significantly expanded the cyber threat landscape, making organizations more vulnerable to sophisticated cyber-attacks. Traditional security mechanisms often rely on reactive defense strategies that struggle to identify emerging threats before they compromise critical assets. To address these challenges, this research proposes an intelligent Cyber Threat Intelligence (CTI) framework that utilizes technical threat indicators to strengthen proactive cyber defense. The proposed framework focuses on the collection, processing, correlation, and consumption of network-based indicators such as malicious IP addresses, suspicious domains, intrusion detection signatures, and vulnerability intelligence. Threat information is organized using standardized CTI formats and mapped to the MITRE ATT&CK framework to improve the understanding of attacker behavior and support effective defensive decision-making. The framework further integrates network intrusion detection systems, vulnerability repositories, Sigma rules, YARA signatures, and threat intelligence feeds to enable continuous monitoring and rapid detection of malicious activities. By combining structured intelligence with real-time security monitoring, the proposed solution enhances threat visibility, reduces response time, and supports proactive mitigation against advanced cyber threats. The framework also assists security analysts in prioritizing vulnerabilities, identifying attack patterns, and strengthening organizational cyber resilience through intelligence-driven security operations.

keywords: Cyber Threat Intelligence, Cybersecurity, MITRE ATT&CK, Indicators of Compromise, Threat Detection, Network Security, STIX, TAXII, Intrusion Detection System, Sigma Rules, Vulnerability Management, YARA, SIEM, Threat Hunting

I. Introduction

The rapid digital transformation of modern organizations has significantly increased their dependence on interconnected information systems, cloud computing platforms, mobile technologies, and Internet-based services. While these technological advancements have improved operational efficiency and enabled seamless communication, they have also expanded the cyber threat landscape, exposing organizations to increasingly sophisticated and persistent cyber-attacks. Cybercriminals continuously develop new attack techniques that exploit software vulnerabilities, misconfigurations, and human errors to compromise critical infrastructure, steal confidential information, disrupt business operations, and cause substantial financial losses. Consequently, cybersecurity has evolved from being a purely technical concern into a strategic organizational priority that requires continuous monitoring, proactive defense mechanisms, and intelligence-driven decision-making. Traditional security approaches that primarily rely on signature-based detection or reactive incident response are no longer sufficient to defend against modern cyber threats, emphasizing the need for more adaptive and intelligence-oriented security frameworks.

The frequency and complexity of cyber-attacks have increased considerably in recent years due to the widespread adoption of cloud services, remote working environments, Internet of Things (IoT) devices, and highly interconnected enterprise networks. Advanced Persistent Threats (APTs), ransomware campaigns, phishing attacks, botnets, supply chain compromises, and zero-day exploits have become increasingly common, targeting both public and private organizations worldwide. Unlike conventional attacks that primarily focus on exploiting individual vulnerabilities, modern adversaries employ carefully planned attack campaigns involving multiple stages, sophisticated evasion techniques, and coordinated attack infrastructures. These evolving attack strategies require organizations to move beyond conventional perimeter security and adopt proactive cybersecurity practices capable of identifying malicious activities before significant damage occurs. Effective cyber defense therefore depends not only on detecting attacks but also on understanding attacker behavior, motivations, infrastructure, and operational techniques.

Cyber Threat Intelligence (CTI) has emerged as one of the most effective approaches for strengthening organizational cybersecurity by transforming raw security data into meaningful intelligence that supports threat detection, risk assessment, and incident response. Rather than focusing exclusively on individual security events, CTI provides contextual information regarding attacker tactics, techniques, procedures (TTPs), infrastructure, malware behavior, and Indicators of Compromise (IoCs). This contextual understanding enables security analysts to identify emerging threats, predict potential attack patterns, prioritize defensive actions, and improve the overall effectiveness of security operations. By integrating intelligence collected from multiple internal and external sources, organizations can establish a proactive security posture capable of anticipating attacks instead of merely reacting after compromise has occurred. Conse-

quently, Cyber Threat Intelligence has become an essential component of modern Security Operations Centers (SOCs), threat hunting activities, and incident response programs.

Among the various components of Cyber Threat Intelligence, technical threat indicators play a particularly significant role because they provide measurable evidence of malicious activity occurring within organizational networks. These indicators include malicious IP addresses, suspicious domain names, file hashes, malware signatures, intrusion detection rules, command-and-control server addresses, vulnerability identifiers, and other observable artifacts associated with cyber-attacks. Security devices such as firewalls, Intrusion Detection Systems (IDS), Intrusion Prevention Systems (IPS), Security Information and Event Management (SIEM) platforms, Endpoint Detection and Response (EDR) solutions, and threat hunting platforms continuously utilize these indicators to detect, analyze, and block malicious activities. The effectiveness of these defensive technologies largely depends on the accuracy, relevance, and timeliness of the threat intelligence consumed by the organization.

To facilitate efficient sharing and utilization of cyber threat information, several standardized intelligence frameworks have been developed. One of the most widely adopted standards is Structured Threat Information Expression (STIX), which provides a structured representation for describing cyber threats, indicators, vulnerabilities, malware, attack patterns, and threat actors. STIX is commonly combined with the Trusted Automated Exchange of Intelligence Information (TAXII) protocol, enabling automated exchange of threat intelligence among organizations, government agencies, and cybersecurity vendors. Standardized intelligence formats significantly improve interoperability between different security platforms while reducing manual processing efforts and enabling real-time threat information sharing. These standards have become fundamental building blocks for collaborative cybersecurity defense initiatives across both public and private sectors.

Another important advancement in intelligence-driven cybersecurity is the adoption of the MITRE ATT&CK framework, which provides a comprehensive knowledge base describing adversary behavior throughout the cyber kill chain. Instead of focusing solely on Indicators of Compromise, MITRE ATT&CK organizes attacker activities according to tactics, techniques, and procedures observed during real-world cyber intrusions. This structured mapping enables security professionals to identify detection gaps, evaluate defensive coverage, develop threat hunting strategies, and prioritize mitigation activities based on actual attacker behavior. By correlating technical threat indicators with ATT&CK techniques, organizations gain deeper visibility into adversary operations and can design more effective detection and response mechanisms.

II. Literature Survey

The rapid evolution of cyber threats has significantly influenced the development of Cyber Threat Intelligence (CTI) frameworks for proactive cybersecurity. Traditional security solutions primarily relied on signature-based detection techniques that identified previously known malicious activities. Although these methods were effective against well-documented attacks, they demonstrated limited capability when confronting sophisticated threats such as Advanced Persistent Threats (APTs), ransomware campaigns, phishing attacks, and zero-day exploits. As cyber adversaries continuously modify their attack strategies, researchers have emphasized the importance of intelligence-driven security approaches that combine threat analysis, contextual information, and behavioral monitoring to improve threat detection and incident response. Cyber Threat Intelligence has consequently emerged as a critical component of modern cybersecurity operations by enabling organizations to understand attacker behaviors and strengthen their defensive capabilities.

Several researchers have investigated the role of structured threat intelligence in improving cybersecurity operations. Standardized intelligence-sharing frameworks such as Structured Threat Information Expression (STIX) and Trusted Automated Exchange of Indicator Information (TAXII) have become widely accepted for exchanging threat information among organizations. These standards enable security systems to share malicious IP addresses, domain names, malware signatures, vulnerabilities, attack patterns, and threat actor information in a structured format. Researchers have reported that standardized intelligence sharing significantly enhances interoperability between different security platforms while reducing the complexity associated with manual threat analysis. Furthermore, automated intelligence distribution enables security teams to receive updated threat indicators in real time, thereby improving organizational readiness against emerging cyber threats.

Network-based threat intelligence has received considerable attention because network traffic provides valuable evidence regarding malicious activities occurring within enterprise infrastructures. Various studies have demonstrated that malicious IP addresses represent one of the most frequently used technical indicators for identifying compromised systems, botnet communication, command-and-control servers, and malicious scanning activities. Researchers have proposed IP reputation systems that combine historical attack records, geolocation information, proxy detection, VPN identification, TOR exit node classification, and abuse reports to improve threat detection accuracy. Such reputation-based approaches allow organizations to prioritize defensive actions according to the severity and credibility of detected indicators while minimizing false-positive alerts.Domain-based threat intelligence has also become an important research area due to the increasing use of malicious domains in phishing campaigns, malware distribution, and command-and-control communication. Cybercriminals frequently utilize Domain Generation Algorithms (DGAs) to produce thousands of dynamically generated domain names, making traditional blacklist-based detection ineffective. Consequently, researchers have developed several machine learning and deep

learning techniques capable of identifying suspicious domains through lexical analysis, entropy measurements, statistical feature extraction, and neural network classification. Recent studies have shown that artificial intelligence significantly improves DGA detection accuracy while reducing the computational overhead associated with maintaining extremely large domain blocklists. Similarly, domain similarity analysis and typosquatting detection have proven effective in identifying fraudulent websites designed to imitate legitimate organizations for credential theft and phishing attacks.

Intrusion Detection Systems (IDS) and Intrusion Prevention Systems (IPS) remain essential components of network security infrastructures. Numerous researchers have investigated the integration of Cyber Threat Intelligence with IDS platforms such as Snort and Suricata to enhance real-time attack detection capabilities. Signature-based intrusion detection systems compare network traffic against predefined rules that represent known attack patterns. While these systems efficiently detect previously identified threats, they often struggle against new or modified attack techniques.

III. Research Methodology

The proposed research methodology presents a comprehensive Cyber Threat Intelligence (CTI) framework for improving proactive cyber defense through the effective utilization of technical threat intelligence indicators. The methodology integrates threat intelligence collection, data standardization, network traffic analysis, indicator correlation, vulnerability assessment, attack behavior mapping, and security monitoring within a unified cybersecurity architecture. The primary objective of the proposed framework is to assist security analysts in detecting, analyzing, and responding to cyber threats more efficiently by utilizing structured threat intelligence and standardized detection mechanisms. The methodology emphasizes the practical consumption of technical indicators such as malicious IP addresses, suspicious domain names, intrusion detection signatures, malware indicators, and vulnerability intelligence to strengthen organizational security against evolving cyber-attacks.

The first stage of the proposed methodology involves threat intelligence collection. Technical threat indicators are gathered from multiple trusted intelligence sources, including public threat intelligence repositories, cybersecurity research organizations, commercial threat feeds, vulnerability databases, malware repositories, and open-source intelligence platforms. These sources continuously provide updated information regarding malicious IP addresses, compromised domains, malware signatures, Indicators of Compromise (IoCs), Common Vulnerabilities and Exposures (CVEs), and attacker infrastructure. Collecting intelligence from multiple sources improves data diversity and increases the probability of identifying newly emerging cyber threats before they impact organizational networks.

After intelligence acquisition, the collected threat information undergoes data normalization and standardization using Structured Threat Information Expression (STIX). Standardization ensures that threat indicators originating from different intelligence

providers are represented in a common format, thereby improving interoperability between cybersecurity platforms. The standardized intelligence is stored within a centralized Cyber Threat Intelligence repository where it can be efficiently searched, updated, and correlated with organizational security events. The use of standardized CTI formats simplifies automated intelligence sharing while enabling seamless integration with various security monitoring solutions.

The next phase focuses on network indicator analysis, where different categories of technical threat indicators are processed independently according to their characteristics. Malicious IP addresses are evaluated using historical reputation information, geographical location, proxy detection, VPN identification, TOR exit node classification, and previous attack records. Suspicious domain names are analyzed through domain reputation databases, domain generation algorithm (DGA) detection, phishing identification, and typosquatting analysis. Network intrusion signatures obtained from trusted rule repositories are incorporated into intrusion detection systems for identifying malicious traffic patterns. Similarly, vulnerability intelligence is collected from vulnerability databases and exploit repositories to identify software weaknesses that may be targeted by attackers.

Once technical indicators are processed, the framework performs network traffic monitoring using Intrusion Detection Systems (IDS) and Intrusion Prevention Systems (IPS). Security devices continuously inspect inbound, outbound, and internal network traffic while comparing observed communication patterns against the threat intelligence repository. Signature-based detection rules are utilized to identify known attack behaviors, whereas anomaly-based monitoring assists in discovering suspicious activities that may not exactly match predefined signatures. This continuous inspection enables the organization to detect malicious communication involving compromised IP addresses, unauthorized domains, malware distribution channels, command-and-control servers, and lateral movement activities within enterprise networks.

To improve malware detection capabilities, the methodology incorporates YARA rule-based analysis. YARA signatures provide pattern-matching mechanisms capable of identifying malicious files through textual strings, binary signatures, hexadecimal patterns, and behavioral characteristics. Network traffic and extracted files are examined against continuously updated YARA repositories to detect malware families, ransomware variants, exploit frameworks, and advanced persistent threat artifacts. The implementation of Detection-as-Code principles further simplifies the maintenance and deployment of custom YARA rules, allowing security teams to rapidly respond to newly emerging malware campaigns.

Another important component of the methodology is vulnerability assessment and prioritization. Organizational software inventories are compared against vulnerability repositories such as the National Vulnerability Database (NVD) and MITRE Common Vulnerabilities and Exposures (CVE) database. The detected vulnerabilities are further evaluated using the Exploit Prediction Scoring System (EPSS), which estimates the

probability of real-world exploitation based on historical attack behavior and exploit availability. This prioritization mechanism enables security administrators to allocate remediation resources more efficiently by focusing on vulnerabilities that pose the highest operational risk. Integration with exploit repositories further assists analysts in identifying vulnerabilities that already possess publicly available exploit code.

To understand attacker behavior beyond simple Indicators of Compromise, the proposed framework integrates the MITRE ATT&CK framework. Technical indicators identified during monitoring are mapped to corresponding attacker tactics, techniques, and procedures (TTPs), enabling security analysts to understand the complete attack lifecycle rather than isolated security events. The ATT&CK mapping supports threat hunting activities by identifying detection gaps, improving defensive coverage, and assisting in the development of new security monitoring rules. Heatmaps generated from ATT&CK techniques further help prioritize defensive efforts by highlighting the most frequently exploited attack techniques relevant to organizational environments.

The methodology also incorporates Sigma rule-based detection engineering to improve Security Information and Event Management (SIEM) capabilities. Sigma rules provide vendor-independent detection logic that can be translated into multiple SIEM platforms without modifying the original detection strategy. Security events collected from firewalls, intrusion detection systems, endpoint security solutions, authentication logs, and application logs are correlated with Sigma detection rules to generate actionable security alerts. This standardized detection mechanism improves portability, simplifies rule management, and enables efficient sharing of detection knowledge across different organizations.

Following threat detection, the framework performs correlation and incident analysis by combining multiple technical indicators associated with the same security event. Instead of evaluating individual alerts independently, the system correlates malicious IP addresses, suspicious domains, malware signatures, vulnerabilities, ATT&CK techniques, and SIEM events to construct a comprehensive threat profile. This contextual analysis significantly reduces false-positive alerts while improving the confidence level of generated security incidents. Security analysts can therefore prioritize incident response activities based on the severity, credibility, and potential impact of detected threats.

Finally, the effectiveness of the proposed methodology is evaluated through continuous security monitoring and threat intelligence updates. Newly discovered indicators are periodically incorporated into the centralized intelligence repository, ensuring that detection capabilities remain synchronized with the rapidly evolving cyber threat landscape. Performance evaluation focuses on detection accuracy, indicator correlation efficiency, false-positive reduction, incident response improvement, and overall enhancement of organizational cybersecurity posture. Continuous feedback obtained from security operations supports ongoing refinement of detection rules, intelligence sources,

and analytical models, thereby establishing an adaptive Cyber Threat Intelligence framework capable of responding to modern cyber threats.

IV. Existing System

Existing cybersecurity infrastructures primarily rely on conventional security technologies such as firewalls, antivirus software, Intrusion Detection Systems (IDS), Intrusion Prevention Systems (IPS), Security Information and Event Management (SIEM) platforms, and signature-based detection mechanisms to defend organizational networks against cyber threats. These solutions generally identify malicious activities by comparing network traffic, files, and system events against predefined signatures, rule sets, or static blacklists of known Indicators of Compromise (IoCs). Although these approaches provide an essential layer of protection against previously identified attacks, they are predominantly reactive in nature and often fail to detect sophisticated cyber threats that continuously evolve through new attack techniques, obfuscation methods, and zero-day vulnerabilities. Consequently, organizations relying solely on traditional security mechanisms experience increasing difficulty in defending against modern cyber-attacks that rapidly adapt to bypass conventional detection systems.

Most existing cybersecurity environments utilize threat intelligence feeds containing malicious IP addresses, suspicious domain names, malware signatures, and vulnerability information to strengthen network monitoring capabilities. These indicators are commonly integrated into perimeter firewalls, IDS/IPS devices, and endpoint security platforms to block or detect known malicious activities. However, many existing implementations treat threat indicators as isolated data elements without sufficient contextual analysis regarding attacker behavior, attack progression, or adversary objectives. Static blocklists frequently become outdated because cybercriminals continuously modify their infrastructure by changing IP addresses, generating new domains, or deploying previously unknown malware variants. As a result, organizations often struggle to maintain current intelligence repositories capable of providing reliable protection against rapidly emerging threats.

Another significant limitation of existing systems is their heavy dependence on signature-based detection techniques. Security solutions such as Snort and Suricata compare network packets against predefined rule databases to identify malicious traffic patterns. While these systems perform effectively when detecting known attacks, they exhibit limited capability when confronted with novel attack strategies, polymorphic malware, encrypted communications, or advanced persistent threats. Maintaining large signature databases also increases computational overhead and requires frequent updates to ensure detection accuracy. Furthermore, manually creating and maintaining custom detection rules demands experienced cybersecurity professionals, making continuous rule management both time-consuming and resource-intensive.

Domain-based threat detection within existing systems also presents several operational challenges. Traditional blacklist approaches simply block previously identified

malicious domains without considering newly generated or dynamically created domain names. Modern malware families frequently employ Domain Generation Algorithms (DGAs) that automatically produce thousands of unique domains, making conventional blacklist techniques ineffective. Similarly, phishing attacks increasingly utilize domain impersonation and typosquatting methods that closely resemble legitimate organizational websites. Many existing detection systems lack advanced analytical mechanisms capable of identifying these sophisticated domain manipulation techniques, resulting in delayed detection and increased exposure to phishing campaigns and malware distribution.

Vulnerability management represents another area where conventional approaches demonstrate important shortcomings. Existing systems typically identify software vulnerabilities using vulnerability scanners and compare detected weaknesses against publicly available vulnerability databases. However, remediation prioritization often depends solely on severity scores without adequately considering exploit availability, attacker activity, or the actual probability of exploitation. Consequently, organizations frequently allocate security resources inefficiently by attempting to remediate all identified vulnerabilities equally, regardless of their practical risk. This approach increases operational complexity while delaying remediation of vulnerabilities that pose the greatest threat to organizational security.

V. Proposed System

The proposed system introduces an intelligent Cyber Threat Intelligence (CTI) framework that enhances organizational cybersecurity through the effective collection, analysis, correlation, and utilization of technical threat intelligence indicators. Unlike conventional security mechanisms that primarily depend on static signatures and reactive detection strategies, the proposed framework adopts a proactive intelligence-driven approach capable of identifying potential cyber threats before they significantly impact critical information systems. The framework integrates multiple sources of threat intelligence, including malicious IP addresses, suspicious domain names, intrusion detection signatures, malware indicators, vulnerability repositories, and attacker behavioral information into a centralized security architecture. By combining these diverse intelligence sources, the proposed system provides comprehensive visibility into emerging cyber threats while enabling rapid detection, efficient analysis, and timely incident response.

Initially, the framework continuously collects threat intelligence from trusted cybersecurity repositories, open-source intelligence platforms, commercial threat feeds, vulnerability databases, malware repositories, and security research organizations. The collected information includes Indicators of Compromise (IoCs) such as malicious IP addresses, compromised domains, malware signatures, Common Vulnerabilities and Exposures (CVEs), exploit intelligence, and attacker infrastructure. To ensure interoperability among various security platforms, the collected intelligence is standardized using Structured Threat Information Expression (STIX) and securely maintained within

a centralized Cyber Threat Intelligence repository. This structured storage mechanism enables efficient threat searching, automated intelligence updates, and seamless information sharing across different security components.

The proposed framework performs continuous monitoring of enterprise network traffic through Intrusion Detection Systems (IDS) and Intrusion Prevention Systems (IPS). Network packets, DNS requests, email communications, and internal traffic are continuously inspected and compared against the threat intelligence repository to identify malicious activities. Suspicious IP addresses are analyzed using reputation information, geolocation, proxy identification, VPN detection, TOR exit node verification, and historical attack records. Similarly, suspicious domain names are evaluated using domain reputation analysis, Domain Generation Algorithm (DGA) detection, phishing identification, and typosquatting detection techniques. This comprehensive inspection process enables the framework to recognize malicious communication channels before attackers successfully compromise organizational resources.

To improve malware detection capabilities, the proposed system incorporates YARA rule-based analysis, allowing security devices to identify malicious files through advanced pattern matching techniques. Network traffic and extracted files are scanned using continuously updated YARA rule repositories capable of recognizing malware families, ransomware variants, command-and-control tools, exploit frameworks, and advanced persistent threat artifacts. The implementation of Detection-as-Code principles further enables cybersecurity teams to develop and deploy customized detection rules rapidly in response to newly emerging attack techniques. This flexible detection strategy significantly improves malware identification while reducing dependency on traditional antivirus signatures.

An important feature of the proposed framework is its intelligent vulnerability management mechanism. Organizational software inventories are automatically compared with information obtained from the National Vulnerability Database (NVD), Common Vulnerabilities and Exposures (CVE) repository, and other trusted vulnerability intelligence sources. Each identified vulnerability is further analyzed using the Exploit Prediction Scoring System (EPSS) to estimate the probability of real-world exploitation. This risk-based prioritization enables security administrators to focus remediation efforts on vulnerabilities most likely to be exploited by attackers, thereby improving patch management efficiency and reducing organizational exposure to cyber threats.

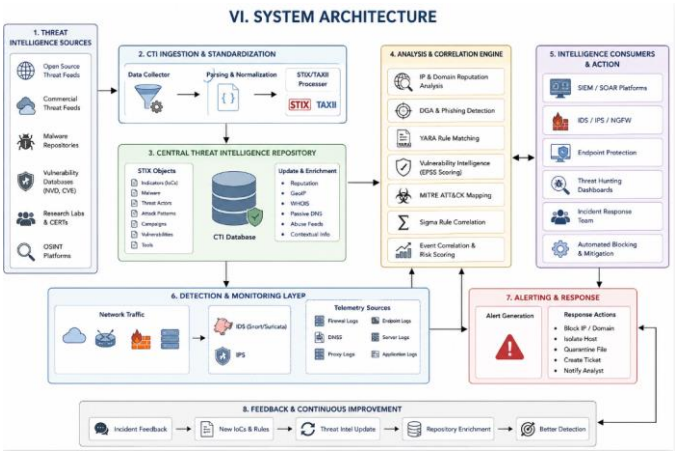
The proposed system also integrates the MITRE ATT&CK framework to provide behavioral analysis of attacker activities. Instead of evaluating Indicators of Compromise independently, detected events are mapped to corresponding attacker tactics, techniques, and procedures (TTPs). This behavioral correlation enables security analysts to understand the complete attack lifecycle, identify defensive gaps, improve threat hunting activities, and develop more effective mitigation strategies. Furthermore,

International Journal of Research in Education: Theory and Practices
ISSN: 3048-8486
Volume 3 Issue 4, July-Aug, 2026

ATT&CK-based heatmaps assist organizations in visualizing the most frequently exploited attack techniques, allowing security teams to prioritize defensive measures according to realistic threat landscapes.

To strengthen security monitoring, the framework utilizes Sigma rules for vendor-independent event detection across multiple Security Information and Event Management (SIEM) platforms. Security logs generated by firewalls, endpoint protection systems, authentication servers, application servers, and network monitoring devices are continuously correlated with Sigma detection rules to generate accurate security alerts. The vendor-neutral design of Sigma enables organizations to share detection rules across heterogeneous environments while simplifying rule management and reducing dependency on proprietary SIEM technologies.

VI. System Architecture



The proposed Cyber Threat Intelligence (CTI) system architecture is designed to provide a comprehensive, intelligence-driven framework for detecting, analyzing, and responding to modern cyber threats. The architecture integrates threat intelligence collection, data standardization, centralized intelligence management, network monitoring, behavioral analysis, and automated incident response into a unified cybersecurity platform. The overall objective of the framework is to continuously collect technical threat intelligence indicators, correlate them with organizational security events, and generate actionable intelligence that enables proactive protection against emerging cyber-attacks. By combining multiple cybersecurity technologies within a single architecture, the proposed system improves threat visibility, accelerates incident response, and enhances the overall resilience of enterprise networks.

The architecture begins with the Threat Intelligence Sources, where cybersecurity information is gathered from multiple trusted repositories, including open-source threat

intelligence feeds, commercial intelligence providers, malware repositories, vulnerability databases such as the National Vulnerability Database (NVD) and Common Vulnerabilities and Exposures (CVE), security research laboratories, Computer Emergency Response Teams (CERTs), and Open-Source Intelligence (OSINT) platforms. These sources continuously provide updated information regarding malicious IP addresses, suspicious domain names, malware signatures, Indicators of Compromise (IoCs), attacker infrastructure, vulnerabilities, and exploit intelligence. Collecting information from diverse intelligence providers ensures that the framework maintains a comprehensive and up-to-date understanding of the evolving cyber threat landscape.

Once the threat intelligence is collected, it enters the CTI Ingestion and Standardization module. In this stage, the raw intelligence data is parsed, normalized, and transformed into a structured format using Structured Threat Information Expression (STIX) and Trusted Automated Exchange of Intelligence Information (TAXII) standards. Standardization eliminates inconsistencies among different intelligence feeds and enables seamless interoperability between various cybersecurity tools. This process also simplifies automated intelligence sharing, allowing security systems to exchange structured threat information efficiently without requiring manual data conversion or interpretation.

The standardized intelligence is then stored within the Central Threat Intelligence Repository, which functions as the core knowledge base of the proposed architecture. The repository maintains structured information related to Indicators of Compromise, malware families, threat actors, attack patterns, vulnerabilities, campaigns, and security tools. In addition to storing threat indicators, the repository continuously enriches the collected information by incorporating reputation scores, geographical location data, WHOIS records, passive DNS information, abuse intelligence, and contextual metadata. This enrichment process improves the quality and reliability of threat intelligence, enabling more accurate threat assessment and informed security decision-making.

The enriched intelligence repository supports the Analysis and Correlation Engine, which serves as the intelligence processing component of the architecture. This module performs IP reputation analysis, domain reputation verification, Domain Generation Algorithm (DGA) detection, phishing detection, YARA rule matching, vulnerability assessment using the Exploit Prediction Scoring System (EPSS), MITRE ATT&CK mapping, Sigma rule correlation, and security event risk scoring. Instead of analyzing individual threat indicators independently, the correlation engine combines multiple technical indicators associated with the same security event to construct comprehensive threat profiles. This contextual analysis significantly improves detection accuracy while reducing false-positive alerts commonly generated by conventional security systems.

The proposed architecture further incorporates a dedicated Detection and Monitoring Layer responsible for continuously observing network activities throughout the enterprise infrastructure. This layer monitors inbound, outbound, and internal network traffic using Intrusion Detection Systems (IDS), Intrusion Prevention Systems (IPS), firewalls, DNS monitoring systems, proxy servers, endpoint security solutions, and application logs. Network packets and security events are continuously compared against the centralized threat intelligence repository and predefined detection rules to identify malicious communication, unauthorized access attempts, malware propagation, command-and-control activities, and suspicious network behavior. Continuous monitoring enables the framework to detect attacks during their early stages, thereby minimizing organizational risk.

VII. Conclusion

The proposed Cyber Threat Intelligence (CTI) framework presents an effective and proactive approach for strengthening modern cybersecurity by integrating technical threat intelligence indicators with advanced threat detection and analysis mechanisms. Unlike traditional security solutions that primarily depend on static signatures and reactive defense strategies, the proposed framework combines structured threat intelligence, network traffic monitoring, vulnerability assessment, behavioral analysis, and automated event correlation to provide comprehensive protection against evolving cyber threats. By utilizing standardized intelligence formats such as STIX and TAXII, the framework enables efficient collection, sharing, and management of cyber threat information across multiple security platforms, thereby improving interoperability and accelerating defensive decision-making. Furthermore, the incorporation of malicious IP analysis, domain reputation verification, intrusion detection signatures, YARA-based malware detection, vulnerability intelligence, and MITRE ATT&CK mapping provides security analysts with valuable contextual information regarding attacker tactics, techniques, and procedures. The integration of Sigma rules and centralized threat intelligence repositories further enhances security monitoring by improving event correlation, reducing false-positive alerts, and supporting rapid incident response. Continuous threat intelligence updates and automated security actions enable the framework to adapt effectively to the constantly changing cyber threat landscape while improving organizational resilience against sophisticated attacks. Overall, the proposed system offers a scalable, intelligence-driven, and practical cybersecurity solution that enhances threat visibility, accelerates detection and response capabilities, supports proactive threat hunting, and significantly strengthens enterprise security operations through the effective utilization of Cyber Threat Intelligence.

References

1. D. J. Bianco, "The Pyramid of Pain," Enterprise Detection and Response, 2014. [Online]. Available: https://detect-respond.blogspot.com/2013/03/the-pyramid-of-pain.html

2. MITRE Corporation, "MITRE ATT&CK Framework," MITRE ATT&CK Knowledge Base, 2024. [Online]. Available: https://attack.mitre.org/
3. OASIS Cyber Threat Intelligence Technical Committee, "STIX Version 2.1 Specification," OASIS Open Standards, 2021. [Online]. Available: https://docs.oasis-open.org/cti/stix/v2.1/
4. OASIS Cyber Threat Intelligence Technical Committee, "TAXII Version 2.1 Specification," OASIS Open Standards, 2021. [Online]. Available: https://docs.oasis-open.org/cti/taxii/
5. G. Gyebnár and S. Magyar, "Consumption of Technical Threat Intel Indicators," in Proc. IEEE 23rd World Symposium on Applied Machine Intelligence and Informatics (SAMI), Stará Lesná, Slovakia, 2025, pp. 177–182.
6. B. Al-Sada, A. Sadighian, and G. Oligeri, "Analysis and Characterization of Cyber Threats Leveraging the MITRE ATT&CK Database," Journal of ICT Research and Applications, vol. 17, no. 3, pp. 245–262, 2023.
7. A. Manoharan and M. Sarker, "Revolutionizing Cybersecurity: Unleashing the Power of Artificial Intelligence and Machine Learning for Next-Generation Threat Detection," International Research Journal of Modernization in Engineering, Technology and Science, vol. 4, no. 12, pp. 2151–2162, 2022.
8. M. Kont and M. Pihelgas, "IDS for Logs: Towards Implementing a Streaming Sigma Rule Engine," NATO Cooperative Cyber Defence Centre of Excellence (CCDCOE), Tallinn, Estonia, 2020.
9. N. Khamphakdee, N. Benjamas, and S. Saiyod, "Improving Intrusion Detection System Based on Snort Rules for Network Probe Attack Detection Using Association Rule Mining," Journal of ICT Research and Applications, vol. 9, no. 3, pp. 234–251, 2015.
10. Zeek Project, "Zeek Network Security Monitor Documentation," Zeek Project, 2024. [Online]. Available: https://docs.zeek.org/
11. AbuseIPDB, "AbuseIPDB: IP Address Reputation Database," 2024. [Online]. Available: https://www.abuseipdb.com/
12. National Institute of Standards and Technology (NIST), "National Vulnerability Database (NVD)," 2024. [Online]. Available: https://nvd.nist.gov/
13. C. Sabottke, O. Suciu, and T. Dumitras, "Vulnerability Disclosure in the Age of Social Media: Exploit Prediction Scoring System (EPSS)," ACM Digital Library, vol. 5, no. 2, pp. 1–15, 2021.
14. Florian Roth, "Sigma: Generic Signature Format for SIEM Systems," SigmaHQ Project Documentation, 2024. [Online]. Available: https://github.com/SigmaHQ/sigma
15. Florian Roth, "YARA Rules Repository for Malware Detection," Nextron Systems, 2024. [Online]. Available: https://github.com/Neo23x0/signature-base
16. M. M. H. Khan, A. Shahriar, and M. Rahman, "Cyber Threat Intelligence for Proactive Cyber Defense: A Systematic Review," IEEE Access, vol. 11, pp. 47856–47878, 2023.
17. S. Noel and S. Jajodia, "Cyber Threat Intelligence Sharing for Enterprise Security Enhancement," Computers & Security, vol. 121, Art. no. 102839, 2022.

18. A. Shalaginov, K. Franke, and S. N. Al-Nemrat, "Threat Intelligence Platforms: Architecture, Challenges, and Future Directions," Future Internet, vol. 14, no. 5, pp. 1–22, 2022.
19. R. Sommer and V. Paxson, "Outside the Closed World: On Using Machine Learning for Network Intrusion Detection," IEEE Symposium on Security and Privacy, pp. 305–316, 2010.
20. E. M. Hutchins, M. J. Cloppert, and R. M. Amin, "Intelligence-Driven Computer Network Defense Informed by Analysis of Adversary Campaigns and Intrusion Kill Chains," Leading Issues in Information Warfare & Security Research, vol. 1, pp. 80–106, 2011.