IJARSCT

International Journal of Advanced Research in Science, Communication and Technology

International Open-Access, Double-Blind, Peer-Reviewed, Refereed, Multidisciplinary Online Journal

ISSN: 2581-9429

Volume 5, Issue 8, May 2025

Impact Factor: 7.67

Cyber Watch India

Samay Khandelwal[1], Pranav Pardeshi[2], Prof. Savitri Chougule[3]
Students, Department of Computer Science[1,2]
Faculty, *Department of* Computer Science[3]
MIT ADT University, Pune, India

Abstract: *The surge in digitization across India has amplified exposure to cyber threats, creating an urgent need for advanced cybersecurity frameworks. Despite the existence of several threat intelligence platforms, current solutions are hampered by issues such as fragmented infrastructures, insufficient real-time data exchange, and limited inter-agency collaboration. These challenges hinder effective detection, response, and mitigation of cyber incidents. This research paper examines the critical role of real-time threat intelligence sharing and proposes a collaborative framework that leverages modern technologies such as AI, machine learning, and automation to strengthen India's cybersecurity posture. The proposed system offers a centralized platform for data collection, visualization, and incident response, promoting timely information dissemination and cooperation between public and private stakeholders.*

Keywords: Cybersecurity, Threat Intelligence, Collaborative Platform, Incident Response, Real-time Monitoring, MISP

I. INTRODUCTION

The rapid digitization of services and the accelerated deployment of digital infrastructure across various sectors in India have contributed to an unprecedented rise in cybersecurity risks. As sectors such as finance, healthcare, energy, and government services shift to online platforms, the attack surface for cyber adversaries has broadened significantly. India has witnessed a steep increase in cyberattacks, including ransomware campaigns, data breaches, phishing attacks, and state-sponsored intrusions that target critical infrastructure and sensitive government data [1], [2]. Many of these attacks are increasingly sophisticated, leveraging advanced persistent threats (APTs) and zero-day vulnerabilities that exploit loopholes in outdated and uncoordinated cybersecurity architectures [2].

Global cybersecurity frameworks like the NIST Cybersecurity Framework and the Lockheed Martin Intrusion Kill Chain offer structured, intelligence-driven defense models that emphasize risk management, threat detection, and incident response [3], [7]. However, their success heavily relies on timely sharing of threat intelligence, automation of response mechanisms, and robust coordination among key stakeholders. In India, these enablers are often lacking due to fragmented regulatory oversight, a shortage of skilled cybersecurity professionals, and limited interoperability among existing defense systems [2], [5]. Government entities and private sector organizations still operate largely in silos, impeding the real-time exchange of actionable threat intelligence and collaborative defense efforts [5].

Recent advancements in cybersecurity, such as the integration of Threat Intelligence Platforms (TIPs), Security Information and Event Management (SIEM) systems, and real-time analytics, have shown promise in strengthening situational awareness and improving response agility [4], [8]. Despite these technological gains, core challenges persist—such as the lack of standardized protocols for data exchange, minimal public-private synergy, and insufficient investment in indigenous security research and development [2], [5].

This paper advocates for the establishment of a centralized, proactive cybersecurity ecosystem tailored specifically to India's digital landscape. By consolidating threat intelligence, streamlining inter-agency cooperation, and promoting automation and transparency, a national platform could enhance India's cyber resilience, reduce response time, and mitigate the impact of future attacks [9].

DOI: 10.48175/IJARSCT-26942

II. LITERATURE SURVEY

Barros and Kurek emphasize the significance of collaborative platforms for sharing malware information, demonstrating how efficient data sharing enhances threat detection and fosters a proactive cybersecurity environment [3]. However, their study also acknowledges the challenge of ensuring timely and accurate data exchange across diverse organizations.

Hutchins et al. introduce the intrusion kill chain model, which provides a strategic framework for understanding and disrupting adversary campaigns [4]. While effective in analyzing attack stages, the model's practical implementation requires robust intelligence feeds and cross-sector integration, which many systems still lack.

The CERT-In 2023 report highlights the escalating complexity and volume of cyberattacks in India, urging the need for collaborative mechanisms and real-time response systems [5]. Nevertheless, the absence of centralized infrastructure and inconsistent reporting standards remain significant limitations.

Smit and Dovey demonstrate that threat intelligence sharing improves situational awareness and accelerates response times [6]. Yet, organizational hesitancy in sharing sensitive data due to legal and privacy concerns often reduces the effectiveness of such systems.

A. Problems in Existing Approaches

Despite advancements in cybersecurity technologies and frameworks, several challenges persist in the effective detection, analysis, and mitigation of cyber threats. These challenges arise due to fragmented systems, slow response times, and limited collaboration among stakeholders. The following key issues highlight the limitations of current cybersecurity approaches:

1) Fragmented Cybersecurity Infrastructure

Cybersecurity efforts in many countries, including India, remain fragmented across different agencies, sectors, and regions. The absence of a centralized platform for monitoring, analyzing, and responding to cyber incidents leads to slow coordination, duplicated efforts, and inconsistent security measures. Sharma [12] highlights that government bodies, private sector organizations, and security agencies in India often operate in isolation, slowing the national response to large-scale cyber threats. The lack of seamless integration further complicates realtime data exchange, making it difficult to mitigate risks swiftly.

2) Slow Incident Detection and Response

Traditional cybersecurity frameworks often rely on manual processes and outdated technologies, leading to delayed detection and response to cyber incidents. Many organizations still operate legacy systems that generate high volumes of false positives, making it difficult for security teams to focus on real threats. According to Singh et al. [13], legacy systems lack automation in incident response, allowing critical breaches to remain undetected for extended periods, increasing potential damage.

3) Inefficient Data Visualization and Decision-Making

The complexity of cybersecurity data makes it difficult for decision-makers to interpret and act upon it in real time. Many cybersecurity platforms present raw data or overly technical reports that require specialized knowledge. Kim and Lee [14] note that ineffective data visualization hinders security professionals from quickly identifying attack patterns, trends, and vulnerabilities. This inefficiency makes it challenging to prioritize threats, particularly for non-technical stakeholders responsible for decisionmaking during a crisis.

4) Limited Collaboration Between Public and Private Sectors

Although collaboration between the public and private sectors is widely recognized as essential, significant barriers remain. Public organizations like CERT-In focus on national-level threats, whereas private entities prioritize their proprietary data and systems. This lack ofcollaboration creates gaps in cybersecurity defenses, as private organizations

DOI: 10.48175/IJARSCT-26942

hesitate to share threat data with public agencies. Misra et al. [15] highlight that India's cybersecurity landscape suffers from a lack of effective public-private partnerships, leading to uncoordinated and fragmented defense efforts.

5) Inadequate Proactive Measures

Current cybersecurity frameworks emphasize reactive rather than proactive threat mitigation. While intrusion detection and prevention systems focus on identifying and stopping attacks, they often lack predictive analytics to prevent threats before they occur. Platforms like Cyber Watch India attempt to bridge this gap with proactive threat monitoring, but most systems still rely on post-event analysis, delaying containment efforts.

6) Skill Shortage and Knowledge Gaps

A major challenge in the cybersecurity landscape is the shortage of skilled professionals. The Indian Cyber Crime Coordination Centre (I4C) reports a significant gap between the demand for cybersecurity talent and the availability of qualified professionals. This shortage contributes to slow detection, delayed response times, and difficulties in implementing advanced security solutions. Many organizations struggle to recruit personnel capable of managing sophisticated threat detection and response systems, increasing their vulnerability to cyber threats [16].

7) Legal and Privacy Concerns in Threat Intelligence Sharing

While threat intelligence sharing is critical for cybersecurity, privacy and legal concerns create significant barriers. Organizations hesitate to share data due to compliance concerns, regulatory restrictions, and fears of sensitive information misuse. In India, the cybersecurity regulatory framework is still evolving, and existing laws do not always address the complexities of cross-jurisdictional data sharing. As highlighted by Shoshitaishvili et al. [17], these legal complexities prevent organizations from fully participating in collaborative cybersecurity initiatives, leaving gaps in threat intelligence sharing.

III. PROPOSED SYSTEM

Building upon the limitations identified in India’s fragmented cybersecurity ecosystem, the proposed system introduces a unified, highly adaptive, and collaborative platform to enhance national cyber resilience. This system centralizes the collection, processing, and dissemination of threat intelligence, enabling a holistic approach to monitoring and responding to cybersecurity incidents. Unlike traditional systems that function in isolated silos, this platform encourages synchronized operations between various stakeholders including government agencies, private organizations, and academic institutions. Through this alignment, the system addresses the urgent need for real-time, interoperable cybersecurity solutions in a rapidly evolving digital landscape.

At the foundation of this architecture lies the integration of open-source threat intelligence technologies, particularly the Malware Information Sharing Platform (MISP). MISP enables the system to aggregate, structure, and disseminate threat intelligence from diverse sources such as national security agencies, cybersecurity vendors, telecom networks, and publicly available databases. Each piece of intelligence is automatically standardized to ensure uniformity and interoperability, minimizing the risk of misinterpretation across different tools and infrastructures. By unifying data formats and protocols, the system ensures seamless compatibility with external cybersecurity frameworks and platforms.

The platform incorporates a continuous data correlation mechanism that analyzes incoming threat indicators in real time.These indicators include malicious IP addresses, URLs, file hashes, exploit signatures, and behavioral patterns of emerging malware strains. The system uses automated correlation engines to link disparate indicators to known threat campaigns and assigns dynamic risk scores based on severity, impact, and frequency. These real-time analytics empower cybersecurity personnel to prioritize incidents that pose the highest risk, allowing for rapid containment and minimal damage.

An intuitive web-based interface provides stakeholders with a centralized view of the national threat landscape. Through this dashboard, users can monitor live feeds of incidents, access reports on sector-specific attack trends, and visualize patterns of threat evolution across geographies. The interface is designed with simplicity and adaptability in mind, making it accessible to both technical analysts and non-technical decision-makers. Interactive charts, heatmaps, and drill-down views facilitate swift interpretation of complex data, reducing cognitive overload during critical decision-making scenarios.

A key innovation of the proposed system is its secure collaborative environment that supports multi-stakeholder participation. It facilitates real-time sharing of Indicators of Compromise (IOCs), incident reports, mitigation strategies, and observed vulnerabilities, all within an encrypted, role-based framework. This ensures that sensitive data is shared only with authorized entities, preserving organizational privacy and integrity. By creating a trustworthy environment for cooperation, the platform helps bridge the long-standing gap between the public and private sectors in India's cybersecurity space.

Although the platform itself does not serve as a direct response tool, it is engineered to integrate with existing security infrastructures such as firewalls, SIEM systems, and endpoint detection tools. Through these integrations, predefined actions such as alerting stakeholders, isolating affected nodes, and updating blocklists can be executed automatically. The system supports realtime dissemination of warnings via secure APIs, messaging systems, and notification protocols, thereby ensuring swift action during the early stages of cyberattacks.

Designed with modularity and future scalability in mind, the platform allows seamless integration of third-party analytics engines, threat detection algorithms, and emerging AIbased tools. It can accommodate regional threat monitoring centers, support distributed deployments, and scale horizontally to meet increasing demand. Additionally, the system complies with relevant data protection laws and cybersecurity standards, offering features like anonymization, audit logging, and tamper-proof logging to ensure transparency, trust, and legal adherence.

Ultimately, this proposed system redefines how India's cybersecurity infrastructure can be restructured into a proactive, collaborative, and technology-driven defense mechanism. By converging intelligence, automation, and cooperation within a single ecosystem, it lays the groundwork for a smarter, faster, and more resilient national cybersecurity strategy.

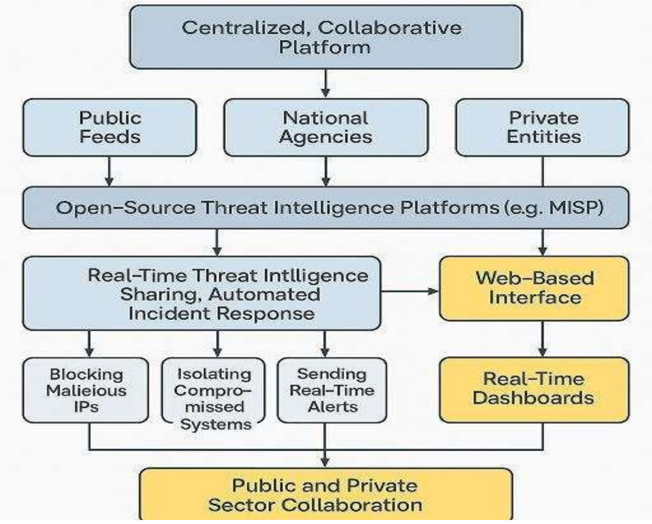

Centralized, Collaborative Platform
Public Feeds
National Agencies
Private Entities
Open–Source Threat Intelligence Platforms (e.g. MISP)
Real–Time Threat Intlligence Sharing, Automated Incident Response
Web–Based Interface
Blocking Malieious IPs
Isolating Compro– missed Systems
Sending Real–Time Alerts
Real–Time Dashboards
Public and Private Sector Collaboration

Fig. 1 Proposed System

I. The diagram represents a centralized, collaborative cybersecurity platform designed to bring together threat intelligence from multiple sources. This kind of system helps improve coordination and response to cyber threats across different sectors.

II. It collects data from public feeds, national government agencies, and private organizations. These sources provide a wide variety of threat information, making the platform more effective in identifying potential risks from different angles.

DOI: 10.48175/IJARSCT-26942

III. The collected data is processed using open-source threat intelligence tools like MISP (Malware Information Sharing Platform). These tools help standardize the data and allow for real-time sharing across systems. This makes it easier for organizations to quickly understand and act on threat information.
IV. Once processed, the system supports automated responses such as blocking dangerous IP addresses, isolating infected systems, and sending alerts. This reduces the time taken to respond to attacks and helps limit their impact.
V. A web-based interface and real-time dashboards allow users to visualize threats and monitor activity. By connecting both public and private sectors through this platform, the system encourages better collaboration and faster decision-making in the fight against cybercrime.

IV. RESULT

The integration of MISP (Malware Information Sharing Platform) with Wazuh was successfully implemented to establish a comprehensive, real-time threat detection and intelligence-sharing framework. This system was designed to bridge the gap between structured threat intelligence and endpoint/network-level security monitoring. MISP was configured to regularly ingest IOCs such as malicious domains, IP addresses, hashes, and URLs from open threat intelligence sources. These indicators were then automatically pushed into Wazuh using the MISP API, where they were stored and correlated with real-time events captured across monitored systems.

To verify the effectiveness of this setup, a test scenario was executed where a system under Wazuh surveillance attempted to ping a domain previously flagged as malicious and listed in MISP. As intended, the connection attempt was logged by Wazuh's network traffic monitoring engine (Suricata), which was configured to forward logs to the Wazuh manager through Filebeat and Logstash. Upon recognizing the domain as a known IOC imported from MISP, Wazuh generated a high-priority security alert and tagged it accordingly in the dashboard.

The event record contained detailed contextual information including the hostname of the source machine, the domain queried, timestamps, and the nature of the threat. Most importantly, it included a direct reference to the IOC from MISP, thus validating the correlation engine. The alert was immediately displayed on the Wazuh dashboard within the MITRE ATT&CK matrix and custom threat dashboard modules, confirming real-time detection, correlation, and visualization functionality.

This validation scenario proved the system's ability to synchronize threat intelligence feeds and apply them for proactive detection. The integration supports a scalable model where continuously updated threat data is directly usable by the detection engine. Additionally, since all components of the system are open-source, the implementation is both cost-effective and highly customizable for institutional or national-level deployment.

The collaborative operation between MISP and Wazuh demonstrated that centralized intelligence gathering combined with endpoint-level monitoring and alerting forms an efficient and intelligent cyber defense mechanism. This real-time pipeline enables organizations to act quickly against validated threats, minimizing the window of exposure and enhancing their incident response readiness.

Areas Covered

- MISP successfully ingested open-source IOCs and pushed them to Wazuh for threat correlation.
- Wazuh detected and alerted on real-time events that matched with MISP indicators.
- Integration validated through a controlled test involving a malicious domain access.
- Alerts displayed with full context, including source, threat type, and reference to IOC.
- Fully open-source and scalable architecture, suitable for national cybersecurity frameworks.

DOI: 10.48175/IJARSCT-26942

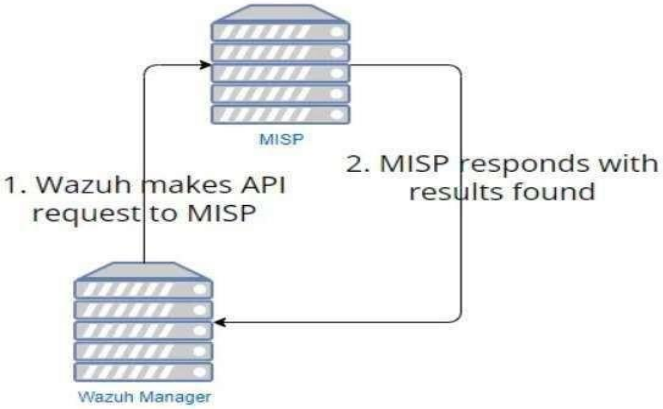
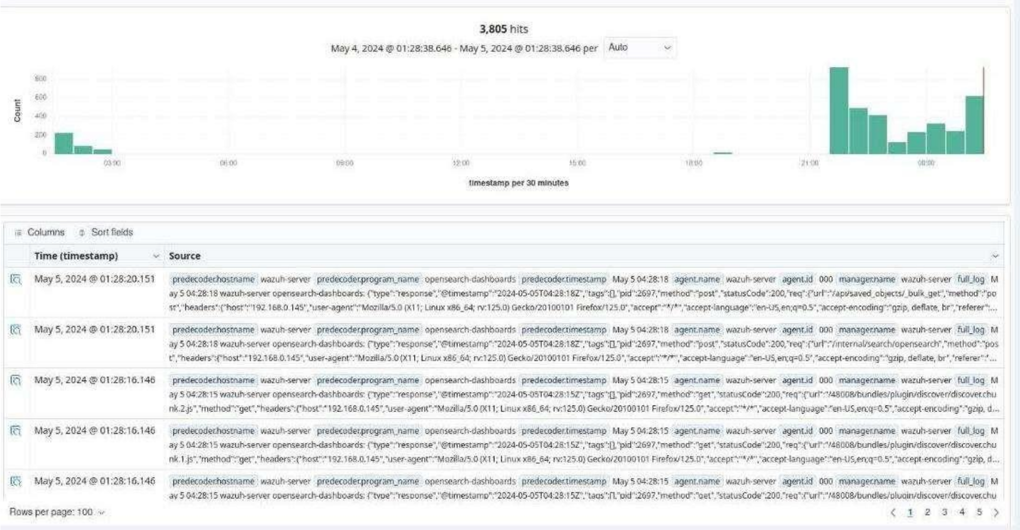
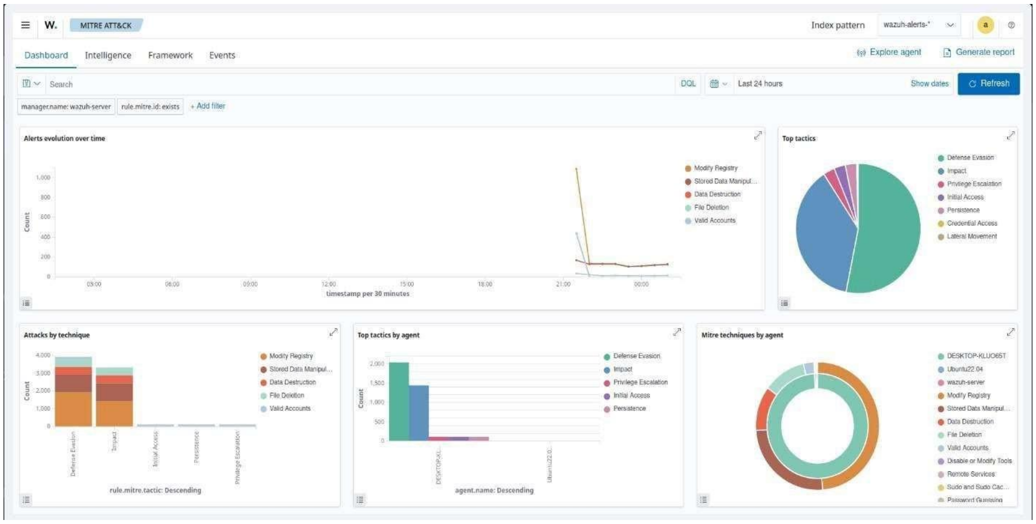

MISP
1. Wazuh makes API request to MISP
2. MISP responds with results found
Wazuh Manager

Fig. 2 Integration Workflow



Time (timestamp)	Source
May 5, 2024 @ 01:28:20.151	predecoder.hostname wazuh-server predecoder.program_name opensearch-dashboards predecoder.timestamp May 5 04:28:18 agent.name wazuh-server agent.id 000 manager.name wazuh-server full_log May 5 04:28:18 wazuh-server opensearch-dashboards: {"type":"response","@timestamp":"2024-05-05T04:28:18Z","tags":[],"pid":2697,"method":"post","statusCode":200,"req":{"url":"/api/saved_objects/_bulk_get","method":"post","headers":{"host":"192.168.0.145","user-agent":"Mozilla/5.0 (X11; Linux x86_64; rv:125.0) Gecko/20100101 Firefox/125.0","accept":"*/*","accept-language":"en-US,en;q=0.5","accept-encoding":"gzip, deflate, br","referer":...
May 5, 2024 @ 01:28:20.151	predecoder.hostname wazuh-server predecoder.program_name opensearch-dashboards predecoder.timestamp May 5 04:28:18 agent.name wazuh-server agent.id 000 manager.name wazuh-server full_log May 5 04:28:18 wazuh-server opensearch-dashboards: {"type":"response","@timestamp":"2024-05-05T04:28:18Z","tags":[],"pid":2697,"method":"post","statusCode":200,"req":{"url":"/internal/search/opensearch","method":"post","headers":{"host":"192.168.0.145","user-agent":"Mozilla/5.0 (X11; Linux x86_64; rv:125.0) Gecko/20100101 Firefox/125.0","accept":"*/*","accept-language":"en-US,en;q=0.5","accept-encoding":"gzip, deflate, br","referer":"...
May 5, 2024 @ 01:28:16.146	predecoder.hostname wazuh-server predecoder.program_name opensearch-dashboards predecoder.timestamp May 5 04:28:15 agent.name wazuh-server agent.id 000 manager.name wazuh-server full_log May 5 04:28:15 wazuh-server opensearch-dashboards: {"type":"response","@timestamp":"2024-05-05T04:28:15Z","tags":[],"pid":2697,"method":"get","statusCode":200,"req":{"url":"/48008/bundles/plugin/discover/discover.chunk.2.js","method":"get","headers":{"host":"192.168.0.145","user-agent":"Mozilla/5.0 (X11; Linux x86_64; rv:125.0) Gecko/20100101 Firefox/125.0","accept":"*/*","accept-language":"en-US,en;q=0.5","accept-encoding":"gzip, d...
May 5, 2024 @ 01:28:16.146	predecoder.hostname wazuh-server predecoder.program_name opensearch-dashboards predecoder.timestamp May 5 04:28:15 agent.name wazuh-server agent.id 000 manager.name wazuh-server full_log May 5 04:28:15 wazuh-server opensearch-dashboards: {"type":"response","@timestamp":"2024-05-05T04:28:15Z","tags":[],"pid":2697,"method":"get","statusCode":200,"req":{"url":"/48008/bundles/plugin/discover/discover.chunk.1.js","method":"get","headers":{"host":"192.168.0.145","user-agent":"Mozilla/5.0 (X11; Linux x86_64; rv:125.0) Gecko/20100101 Firefox/125.0","accept":"*/*","accept-language":"en-US,en;q=0.5","accept-encoding":"gzip, d...
May 5, 2024 @ 01:28:16.146	predecoder.hostname wazuh-server predecoder.program_name opensearch-dashboards predecoder.timestamp May 5 04:28:15 agent.name wazuh-server agent.id 000 manager.name wazuh-server full_log May 5 04:28:15 wazuh-server opensearch-dashboards: {"type":"response","@timestamp":"2024-05-05T04:28:15Z","tags":[],"pid":2697,"method":"get","statusCode":200,"req":{"url":"/48008/bundles/plugin/discover/discover.chu

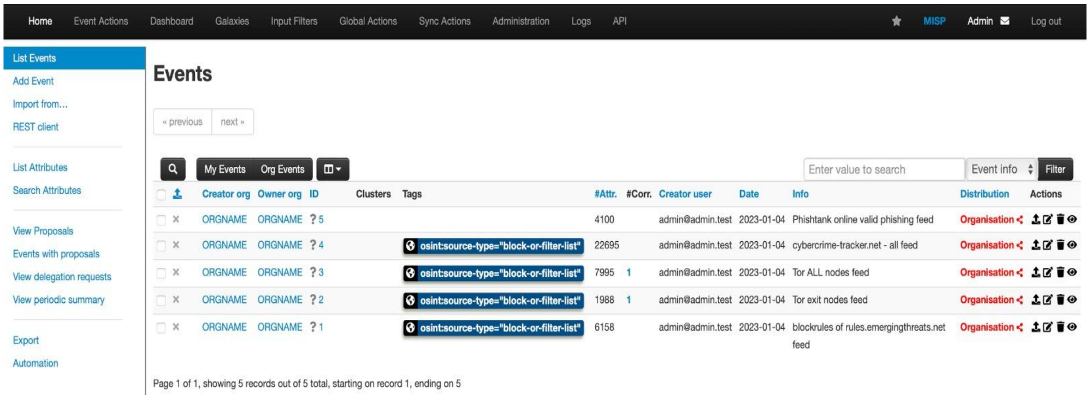
Fig. 3 Wazuh Events



manager.name: wazuh-server
rule.mitre.id: exists

Fig. 4 Wazuh Agent Alerts

DOI: 10.48175/IJARSCT-26942



Events

		Creator org	Owner org	ID	Clusters	Tags	#Attr.	#Corr.	Creator user	Date	Info	Distribution	Actions
□	×	ORGNAME	ORGNAME	? 5			4100		admin@admin.test	2023-01-04	Phishtank online valid phishing feed	Organisation	
□	×	ORGNAME	ORGNAME	? 4		osint:source-type="block-or-filter-list"	22695		admin@admin.test	2023-01-04	cybercrime-tracker.net - all feed	Organisation	
□	×	ORGNAME	ORGNAME	? 3		osint:source-type="block-or-filter-list"	7995	1	admin@admin.test	2023-01-04	Tor ALL nodes feed	Organisation	
□	×	ORGNAME	ORGNAME	? 2		osint:source-type="block-or-filter-list"	1988	1	admin@admin.test	2023-01-04	Tor exit nodes feed	Organisation	
□	×	ORGNAME	ORGNAME	? 1		osint:source-type="block-or-filter-list"	6158		admin@admin.test	2023-01-04	blockrules of rules.emergingthreats.net feed	Organisation	

Page 1 of 1, showing 5 records out of 5 total, starting on record 1, ending on 5

Fig. 5 MISP Events

Soghoian underscores the critical importance of real-time intelligence sharing and the formation of robust cross-sector partnerships to effectively counter advanced and evolving cyber threats [7]. He emphasizes that genuine collaboration between public and private entities can significantly improve threat visibility, reduce response times, and enable coordinated mitigation strategies. However, despite this recognition, many existing partnerships tend to be superficial, ad hoc, or limited to policy-level engagements, lacking the depth and operational integration necessary to tackle real-world threats. As a result, their impact on actual cyber threat mitigation remains minimal.

Wang and Yu, through their comprehensive survey of threat intelligence platforms, identify essential technologies and standards such as STIX (Structured Threat Information Expression) and TAXII (Trusted Automated Exchange of Indicator Information), which are designed to standardize and facilitate seamless sharing of threat data across organizations [8]. These standards support enhanced scalability, interoperability, and automation—critical components for modern cybersecurity ecosystems. Nevertheless, their study reveals that adoption of such standards and platforms is highly uneven. Technologically advanced organizations are more likely to implement these solutions effectively, while others, particularly those with limited resources, struggle with integration and operationalization.

Rashid and Smith further explore how threat intelligence platforms contribute to improving an organization's cyber resilience by enabling proactive detection, faster incident response, and better preparedness against evolving threats [9]. Their research validates the value of embedding such platforms within security infrastructures. However, they also identify key challenges that inhibit widespread adoption, including a shortage of skilled cybersecurity professionals and the substantial infrastructure costs associated with deploying and maintaining these systems. These limitations make it difficult for smaller organizations or developing regions to fully benefit from such platforms.

The NIST Cybersecurity Framework provides a structured, risk-based approach to securing critical infrastructure by promoting continuous improvement, threat awareness, and resilience [6]. It has been widely acknowledged as a foundational model for cybersecurity governance across various sectors. Despite its strengths, one notable drawback is its voluntary nature in many jurisdictions, which results in inconsistent enforcement and varied levels of implementation. This lack of uniform adoption undermines its potential effectiveness as a national or global standard.

Collectively, these studies highlight the significant promise of collaborative threat intelligence, standardized platforms, and structured cybersecurity frameworks in strengthening defenses against sophisticated cyber threats. At the same time, they reveal persistent challenges that must be addressed—such as delayed data sharing, fragmented infrastructures, regulatory and legal complexities, and a global shortage of skilled cybersecurity personnel. To unlock the full potential of these frameworks, it is essential to foster deeper collaboration, enforce standardized practices, and invest in education, training, and scalable technologies.

V. CONCLUSION

This research highlights the critical need for a unified and collaborative approach to cybersecurity in India. The proposed system addresses key shortcomings in existing frameworks by enabling real-time threat intelligence sharing, automated incident response, and effective data visualization. Through the integration of platforms like MISP and

DOI: 10.48175/IJARSCT-26942

adoption of open standards, the solution fosters interoperability and scalability. By promoting publicprivate cooperation and enhancing situational awareness, the system offers a robust foundation for strengthening India’s cyber defense capabilities. Future work will focus on real-world deployment, user training, and long-term performance evaluation.

VI. ACKNOWLEDGMENT

We would like to express our sincere gratitude to MIT Art, Design and Technology University, Pune, for offering us the platform and academic environment to carry out our research project titled “Cyber Watch India.” We are deeply thankful to our guide, Prof. Savitri Chougule, whose expert guidance, timely suggestions, and unwavering support played a crucial role in shaping our research.

We extend our heartfelt appreciation to the global open-source communities and development teams behind MISP (Malware Information Sharing Platform) and Wazuh, whose robust platforms enabled us to successfully implement a real-time cybersecurity framework. Their contributions were fundamental to integrating structured threat intelligence with endpoint-level monitoring, allowing us to validate threat correlations and enhance response mechanisms.

This project specifically focused on bridging the gap between centralized threat intelligence and real-time network-level monitoring, with the goal of strengthening India’s proactive cyber defense infrastructure.

REFERENCES

[1] MISP Malware Information Sharing Platform & Threat Sharing, “MISP Project Documentation,” 2023. [Online]. Available: https://misp.github.io/

[2] C. Stoll, The Cuckoo’s Egg: Tracking a Spy Through the Maze of Computer Espionage. New York: Doubleday, 1995.

[3] R. Barros and A. Kurek, “Malware information sharing in the context of cyber threat intelligence,” J. Cybersecurity, vol. 15, no. 2, pp. 35–47, 2019, doi: 10.1109/JCYB.2019.2905237.

[4] CERT-In, Cybersecurity Threats in India: Annual Report. Indian Computer Emergency Response Team (CERT-In), 2023. [Online].

[5] K. Smit and B. Dovey, “Cyber threat intelligence: The value of sharing threat data and threat intelligence platforms,” Int. J. Cybersecurity, vol. 6, no. 1, pp. 45–56, 2018, doi: 10.1002/csy2.101

[6] NIST, Framework for Improving Critical Infrastructure Cybersecurity (Version 1.1), National Institute of Standards and Technology, 2020.

[7] C. Soghoian, “Collaborative cybersecurity in a digital age: Leveraging threat intelligence and data sharing,” Cybersecurity J., vol. 11, no. 4, pp. 22–30, 2019, doi: 10.1109/SCJ.2019.2872901.

[8] J. Wang and J. Yu, “Threat intelligence sharing platforms: A survey of current trends and technologies,” Int. J. Comput. Appl., vol. 175, no. 9, pp. 34– 39, 2018, doi: 10.5120/ijca2018915987.

[9] A. Rashid and H. Smith, “Threat intelligence platforms: Their role in enhancing cybersecurity posture,” J. Inf. Secur., vol. 45, no. 3, pp. 56–62, 2020, doi: 10.1016/j.jinfosec.2020.03.004.

[10] E. M. Hutchins, M. J. Cloppert, and R. Amin, “Intelligence-driven computer network defense informed by analysis of adversary campaigns and intrusion kill chains,” in Proc. 6th Int. Conf. Inf. Warfare Secur., 2011, pp. 91–98.

DOI: 10.48175/IJARSCT-26942