Industrial Engineering Journal
ISSN: 0970-2555
Volume : 54, Issue 3, March : 2025

Proactive Cybersecurity: Integrating Incident Management and Real-Time Threat Intelligence

Yash Bhidekar[1], Dr. Ruchita Kale[2], Ganesh Thombare [3], Pratik Tayade[4], Sarthak Kadu[5]

[1,3,4,5] B.E. Final Year Student's, Dept. of CSE, Prof Ram Meghe Institute of Technology & Research, Badnera Amravati, Maharashtra, India, yashbhidhekar@gmail.com, kadusarthak70@gmail.com, ganeshthombare949@gmail.com, tayadepratik86@gmail.com

[2] Assistant Professor, Dept. of CSE, Prof Ram Meghe Institute of Technology & Research, Badnera, Amravati, Maharashtra, India, rakale@mitra.ac.in

ABSTRACT- *Today's cyber attacks have become more severe and frequent, necessitating a new level of security defenses. The dynamic nature of modern threats, characterized by their evasiveness, resilience, and complexity, challenges traditional security systems that rely on heuristics and signatures. Organizations are increasingly focused on gathering and sharing real-time cyber threat information, transforming it into actionable threat intelligence to prevent attacks or, at the very least, respond swiftly in a proactive manner. This paper focuses on enhancing organizational cybersecurity through an integrated approach combining incident management and real-time threat intelligence. By leveraging tools such as Cortex and TheHive for incident management and MISP for threat intelligence, the system collects, analyzes, and responds to security incidents and threats proactively. APIs form the integration layer, facilitating seamless data flow between these components. A visualization dashboard powered by Kibana provides real-time monitoring and analysis, enabling security analysts to swiftly detect, assess, and mitigate cyber threats. This holistic framework aims to minimize the impact of security incidents by fostering a proactive and responsive cybersecurity posture.*

Keywords- Cybersecurity Framework, Workflow Automation, Cyber Threat Analysis.

I. INTRODUCTION

In today's digital age, the frequency and sophistication of cyber threats are escalating at an unprecedented rate, posing significant challenges to organizations worldwide. As businesses increasingly rely on digital infrastructure, the need for robust cybersecurity measures has never been more critical. Proactive cybersecurity is essential for protecting sensitive information, maintaining operational integrity, and ensuring business continuity. By preemptively identifying, managing, and resolving security incidents, organizations can significantly reduce their vulnerability to cyber-attacks and mitigate potential damages.

This paper aims to develop a comprehensive cybersecurity framework that integrates incident management and real-time threat intelligence. The core of this system involves utilizing Cortex integrated with TheHive for efficient incident management and MISP for gathering and analyzing threat intelligence. The integration of these components through APIs enables a streamlined flow of information, ensuring that relevant threat data is promptly shared and acted upon. A visualization dashboard built with Kibana offers an intuitive interface for security analysts to

monitor and respond to threats in real-time, enhancing their ability to safeguard the organization against evolving cyber risks. By leveraging real-time threat intelligence, organizations can stay ahead of potential threats, enhancing their ability to detect and mitigate attacks before they cause significant harm. This proactive approach is crucial in the ever-evolving landscape of cybersecurity, ensuring robust protection and swift response to emerging threats.

II. LITERATURE REVIEW

N. Sun et al., In this paper, in order to make the most of CTI so as to significantly strengthen security postures, the author presents a comprehensive review of recent research efforts on CTI mining from multiple data sources in this article. Specifically, they provide and devise a taxonomy to summarize the studies on CTI mining based on the intended purposes (i.e., cybersecurity-related entities and events, cyberattack tactics, techniques and procedures, profiles of hackers, indicators of compromise, vulnerability exploits and malware implementation, and threat hunting), along with a comprehensive review of the current state-of-the-art. [1]

Ayesha Naseer, Humza Naseer, et al., In this paper, they argue that (1) organizations must develop 'agility' in their IR process to respond swiftly and efficiently to sophisticated and potent cyber threats, and (2) Real-time analytics (RTA) gives organizations a unique opportunity to drive their IR process in an agile manner by detecting cybersecurity incidents quickly and responding to them proactively. To better understand how organizations can use RTA to enable IR agility, they analyzed in-depth data from twenty expert interviews using a contingent resource-based view. [2]

Rehman, Fazalur, et al., This paper proposes a novel Hypervisor-based Virtual Machine Introspection (HVMI) for real-time detection and runtime forensic analysis of cyberattacks targeting cloud platforms. The framework proposed comprises several essential components, including a forensic application empowered by Virtual Machine Introspection (VMI) for real-time memory analysis, a centralized Cloud Forensic Tool (CFT) portal for streamlined incident management, and a data transmission and integration web service. Notably, this framework is founded upon a commitment to continuous optimization and enhancement. [3]

Naseer, Humza, Kevin Desouza, et al., In this paper, they explore how organisations enable agility in their cybersecurity incident response (IR) process by developing dynamic capabilities using real-time analytics (RTA). Drawing on RTA practices in the IR process at three large financial organisations, they develop a framework to explain how IR teams respond to the rapidly evolving cyber threat environment by developing RTA-based microfoundations that underpin the building of sensing, seizing, and transforming dynamic IR capabilities. [4]

Kure, Halima, et al., This paper aims to fill this gap by integrating CTI for improving cybersecurity risks management practice specifically focusing on the critical infrastructure. In particular, they have integrated concepts relating to CTI and CRM so that the threat actor's profile, attack details can support calculating the risk. They consider smart grid systems as a Critical Infrastructure to demonstrate the applicability of the work. [5]

Nova et al. highlight the role of Cyber Threat Intelligence (TI) in sustainable smart cities through three objectives. First, they explore TI's practical applications, including security integration, proactive measures, incident response, and threat assessment. Second, they classify TI into tactical (identifying IOCs), operational (understanding TTPs), and strategic (profiling threat actors and

mitigating APTs). Lastly, they outline the phases of the TI lifecycle, emphasizing its importance in enhancing cybersecurity across various levels [6]

Tahmasebi, et al., This research delves deep into the strategies required to respond to threats and anticipate and mitigate them proactively. Beginning with understanding the critical need for a layered defense and the intricacies of the attacker's journey, the research offers insights into specialized defense techniques, emphasizing the importance of timely and strategic responses during incidents. [7]

Gong, Seonghyeon, et al., This paper proposes a cyber threat intelligence framework to improve the energy cloud environment's security. Cyber Threat Intelligence (CTI) is a technology to actively respond to advanced cyber threats by collecting and analyzing various threat indicators and generating contextual knowledge about the cyber threats. The framework proposed in this paper analyzes threat indicators that can be collected in the advanced metering infrastructure and proposes a cyber threat intelligence generation technique targeting the energy cloud. [8]

Kayode-Ajala, et al., This research delves into the role of Cyber Threat Intelligence (CTI) in bolstering the security framework of financial entities and identifies key challenges that could hinder its effective implementation. CTI brings a host of advantages to the financial sector, including real-time threat awareness, which enables institutions to proactively counteract cyber-attacks. It significantly aids in the efficiency of incident response teams by providing contextual data about attacks. Moreover, CTI is instrumental in strategic planning by providing insights into emerging threats and can assist institutions in maintaining compliance with regulatory frameworks such as GDPR and CCPA. Additional applications include enhancing fraud detection capabilities through data correlation, assessing and managing vendor risks, and allocating resources to confront the most pressing cyber threats. [9]

Kotsias, James, et al., In this paper, they posit that the primary reason is the increasing asymmetry between the cyber-offensive capability of attackers and the cyber-defensive capability of commercial organisations. A key avenue to resolve this asymmetry is for organisations to leverage cyber-threat intelligence (CTI) to direct their cyber-defence. The research contributes practical know-how on the organisational adoption and integration of CTI, enacted through the transformation of cybersecurity practice, and enterprise-wide implementation of a novel solution to package CTI for commercial contexts. The study illustrates the inputs, processes, and outputs in clinical research as a genre of action research. [10]

III. METHODOLOGY

The proposed proactive cybersecurity system operates through a series of coordinated steps to enhance threat detection and response capabilities. Initially, data is collected from internal logs and external threat intelligence feeds. This data is ingested by MISP, which identifies and analyzes potential threats. TheHive serves as the incident management platform where these threats are logged and tracked. Cortex, integrated with TheHive, automates repetitive tasks and streamlines workflows by generating incidents from new threat data. APIs ensure seamless data flow between TheHive and MISP, enabling real-time data exchange and comprehensive analysis. An automated workflow is established to facilitate the timely sharing of threat information and triggering of alerts. Kibana provides a visualization dashboard where security analysts can monitor and analyze threats in real-time. Automated responses are triggered to mitigate identified threats, and the system continuously learns from each incident to improve future threat detection and response strategies.

Industrial Engineering Journal
ISSN: 0970-2555
Volume : 54, Issue 3, March : 2025

This comprehensive approach ensures that the organization can anticipate, detect, and respond to cyber threats effectively, thereby enhancing its overall security posture.

Fig1 shows the flowchart of proposed proactive cybersecurity system outlines the key steps in integrating real-time threat intelligence with incident management. It ensures that organizations can detect, analyze, and respond to cyber threats effectively. The flowchart consists of the following sequential processes:

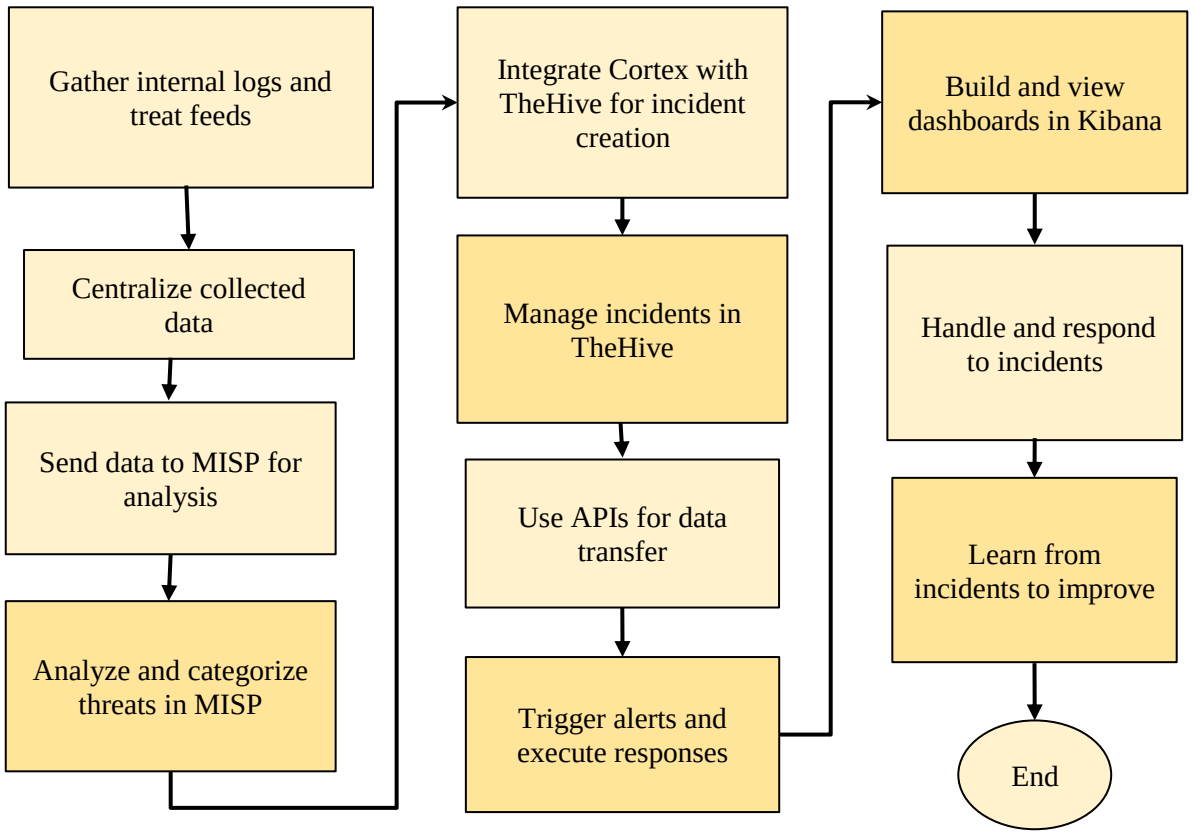


Fig 1 Proposed System Flowchart

➢ WORKING

- Data Collection
  The system gathers security data from two primary sources:
  a) Internal logs from network devices, endpoints, and security appliances.
  b) External threat intelligence feeds from open-source and commercial providers.
- Threat Intelligence Processing (MISP Integration)
  - The collected data is ingested into MISP
  - MISP identifies and classifies potential threats by correlating internal security data with external threat intelligence indicators.
  - Relevant indicators of compromise (IoCs) are extracted for further analysis.
- Incident Logging and Management (TheHive Integration)
  - TheHive serves as the central incident management platform where threats identified by MISP are logged and categorized.

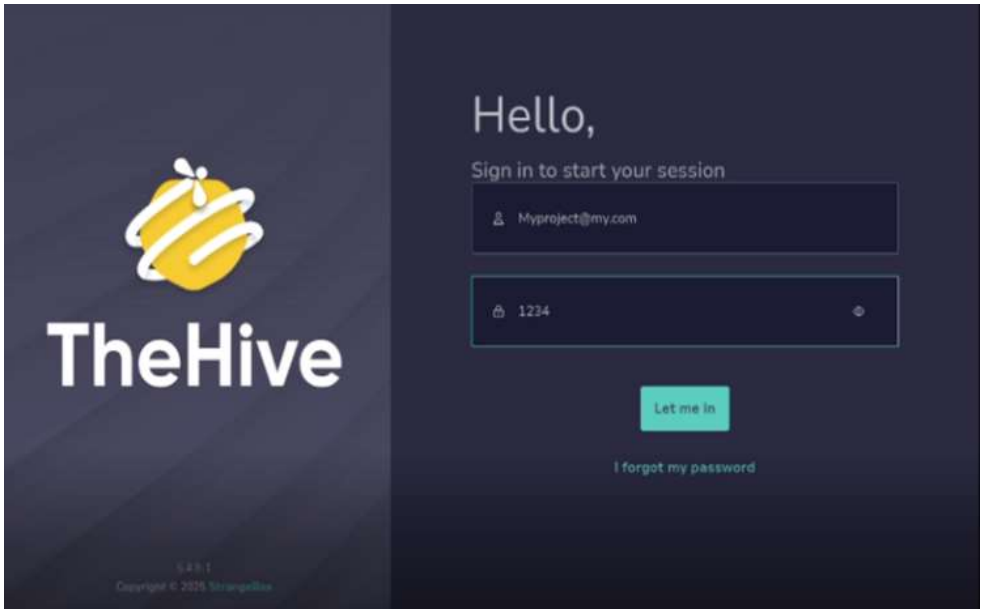
- Security analysts can manually verify and enrich threat data.

- Automated Threat Analysis (Cortex Integration)
  Cortex is integrated with TheHive to automate repetitive security tasks.
  - Cortex runs a series of analyzers on the incoming threat intelligence data, such as IP reputation checks, malware analysis, and forensic investigations.
  - If a verified threat is detected, Cortex automatically generates an incident report in TheHive.
- Seamless Data Exchange via APIs
  - APIs facilitate real-time data sharing between MISP, TheHive, and Cortex.
  - Threat intelligence, indicators, and incident reports are continuously updated across platforms.
  - This ensures that analysts have access to the most up-to-date information.
- Automated Workflow and Alerting
  - The system establishes predefined workflows to handle different threat scenarios.
  - If a high-severity threat is detected, automated alerts are triggered via email, SMS, or integrated Security Information and Event Management (SIEM) systems.
  - The system can initiate predefined response actions, such as blocking an IP address or isolating a compromised endpoint.
- Real-Time Threat Visualization (Kibana Dashboard)
  - All incidents and threat intelligence data are visualized in Kibana, allowing security analysts to monitor and analyze threats in real time.
  - The dashboard provides graphical insights into attack trends, threat sources, and response effectiveness.
- Automated Incident Response
  - Once a validated threat is detected, the system triggers automated mitigation actions, such as:
    - Blocking malicious IPs/domains on firewalls.
    - Quarantining infected endpoints.
    - Notifying security teams for immediate intervention.
- Continuous Learning and Improvement
  The system learns from past incidents by storing threat intelligence data and response patterns.
  - Machine learning models or rule-based updates enhance future threat detection capabilities.
  - Analysts can fine-tune detection rules based on new attack techniques.
- Enhanced Security Posture
- By automating threat intelligence, detection, and response, the system proactively defends against cyber threats.
- It significantly reduces incident response time, minimizes human intervention, and strengthens overall cybersecurity resilience.

IV. IMPLEMENTATION & RESULT

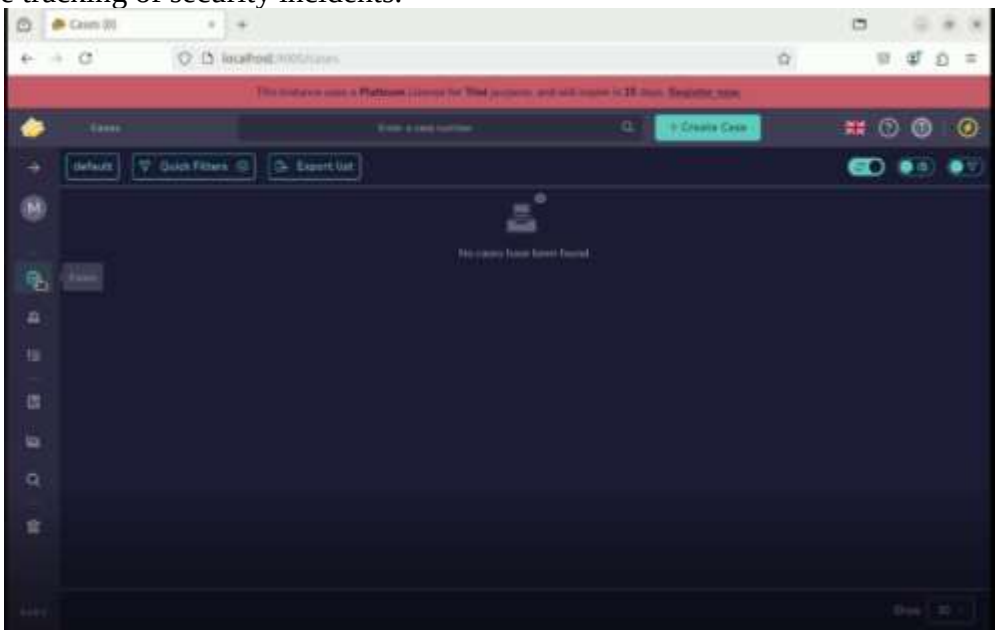
Screenshot 1 describes the dashboard overview provides an intuitive interface where security analysts can monitor incidents and threats in real time. It offers key metrics such as active threats, resolved incidents, and system alerts, enabling analysts to make informed decisions efficiently.

Industrial Engineering Journal
ISSN: 0970-2555
Volume : 54, Issue 3, March : 2025



Screenshot 1: Proposed System Dashboard

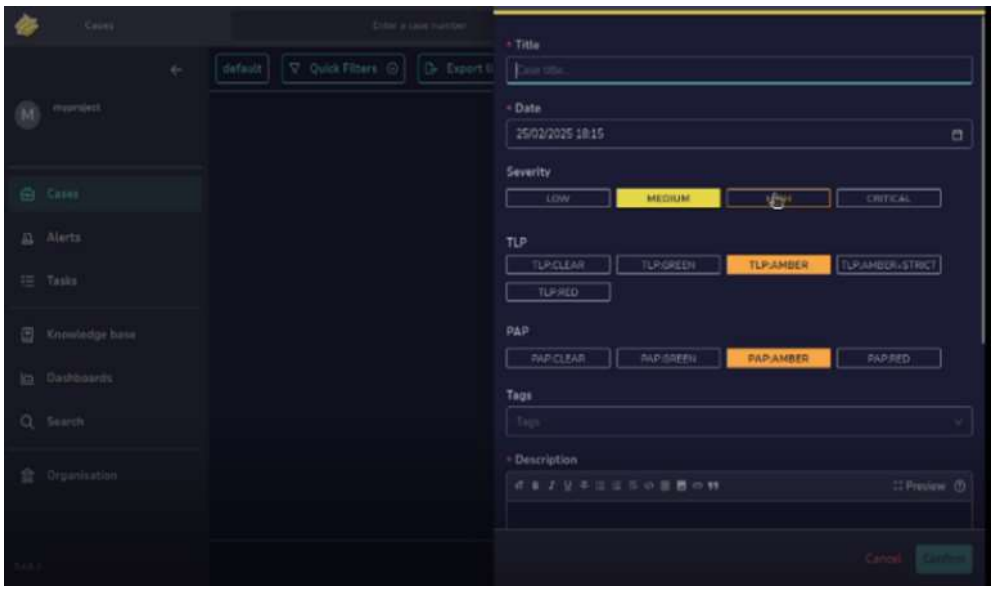
Screenshot 2 shows the create case page facilitates the manual or automated generation of new security cases, capturing critical threat details, severity levels, and affected systems, ensuring accurate tracking of security incidents.



Screenshot 2: Create Case Page

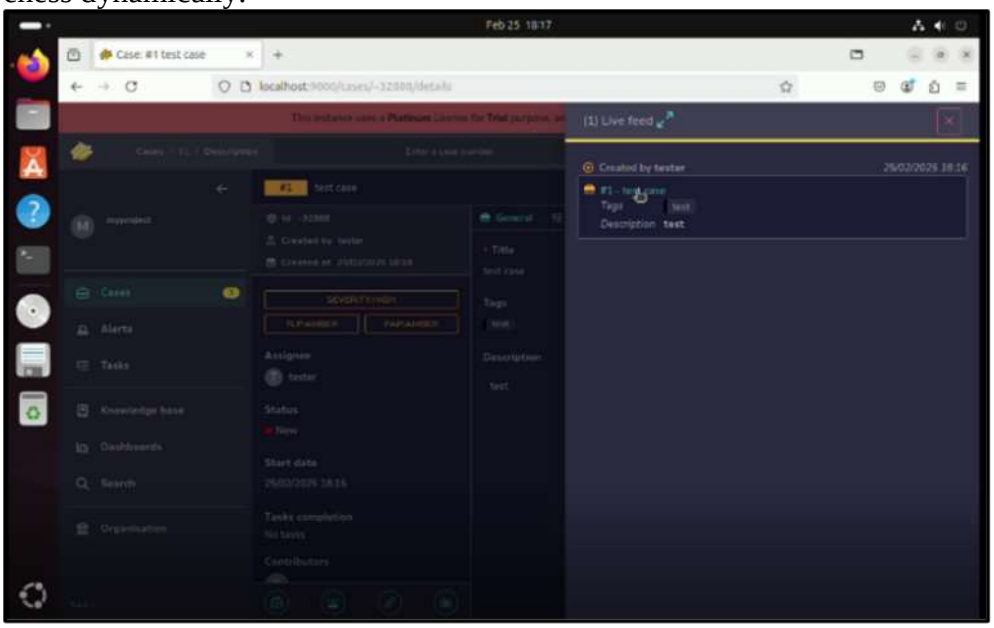
Screenshot 3 shows the case creation process demonstrates the step-by-step approach to generating and managing security cases. This process includes automated data enrichment using Cortex analyzers, which help in identifying the nature of the threats more precisely.

Industrial Engineering Journal
ISSN: 0970-2555
Volume : 54, Issue 3, March : 2025



Screenshot 3: Cases Creating

Lastly, screenshot 4 displays the live feed of cases displays real-time updates on active and resolved security incidents, helping security teams track ongoing investigations and response effectiveness dynamically.



Screenshot 4: Live Feed of Cases

The proposed proactive cybersecurity system successfully enhances threat detection and response by integrating MISP, TheHive, Cortex, and Kibana into a seamless workflow. Through automated data ingestion, real-time threat analysis, and incident tracking, the system effectively identifies and mitigates cyber threats. The use of APIs ensures smooth data exchange, while automated workflows and response mechanisms streamline security operations. Kibana's visualization dashboard enables real-time monitoring, allowing analysts to make informed decisions. Continuous learning from incidents further strengthens threat detection capabilities. Overall, the system significantly improves the organization's security posture by enabling proactive, automated, and intelligent cybersecurity measures.

V. CONCLUSION

The integration of incident management with real-time threat intelligence through the proposed proactive cybersecurity system significantly enhances an organization's ability to detect, respond to, and mitigate cyber threats. By leveraging tools such as Cortex, TheHive, and MISP, and integrating them through robust APIs, the system ensures seamless data flow and real-time analysis. The automation of repetitive tasks and workflows not only streamlines incident response but also ensures that critical alerts are promptly addressed, reducing response times and improving efficiency. The visualization capabilities of Kibana empower security analysts with real-time insights and comprehensive monitoring, facilitating informed decision-making. Moreover, the system's ability to learn from each incident and adapt its threat detection and response strategies continually fortifies the organization's defense mechanisms. This comprehensive approach not only strengthens the organization's security posture but also enhances its resilience against evolving cyber threats, ensuring sustained protection of critical assets and data in an increasingly complex threat landscape.

VI. REFERENCES

1. N. Sun et al., "Cyber Threat Intelligence Mining for Proactive Cybersecurity Defense: A Survey and New Perspectives", in IEEE Communications Surveys & Tutorials, vol. 25, no. 3, pp. 1748-1774, third quarter 2023.

2. Ayesha Naseer, Humza Naseer, Atif Ahmad, Sean B. Maynard, Adil Masood Siddiqui, “Real-time analytics, incident response process agility and enterprise cybersecurity performance: A contingent resource-based analysis”. International Journal of Information Management, 2021.

3. Rehman, Fazalur, and Safwan Hashmi. "Enhancing Cloud Security: A Comprehensive Framework for Real-Time Detection Analysis and Cyber Threat Intelligence Sharing." Advances in Science, Technology and Engineering Systems Journal 8, no. 6 (2023): 107-119.

4. Naseer, Humza, Kevin Desouza, Sean B. Maynard, and Atif Ahmad. "Enabling cybersecurity incident response agility through dynamic capabilities: the role of real-time analytics." European Journal of Information Systems 33, no. 2 (2024): 200-220.

5. Kure, Halima, and Shareeful Islam. "Cyber threat intelligence for improving cybersecurity and risk management in critical infrastructure." Journal of Universal Computer Science 25, no. 11 (2019): 1478-1502.

6. Nova, Kannan. "Security and resilience in sustainable smart cities through cyber threat intelligence." International Journal of Information and Cybersecurity 6, no. 1 (2022): 21-42.

7. Tahmasebi, Meysam. "Beyond defense: Proactive approaches to disaster recovery and threat intelligence in modern enterprises." Journal of Information Security 15, no. 2 (2024): 106-133.

8. Gong, Seonghyeon, and Changhoon Lee. "Cyber threat intelligence framework for incident response in an energy cloud platform." Electronics 10, no. 3 (2021): 239.

9. Kayode-Ajala, Olaolu. "Applications of Cyber Threat Intelligence (CTI) in financial institutions and challenges in its adoption." Applied Research in Artificial Intelligence and Cloud Computing 6, no. 8 (2023): 1-21.

10. Kotsias, James, Atif Ahmad, and Rens Scheepers. "Adopting and integrating cyber-threat intelligence in a commercial organisation." European Journal of Information Systems 32, no. 1 (2023): 35-51.