International Journal of Engineering Research and Science & Technology

V THREAT INTELLIGENCE SHARING PLATFORM USING MISP

Mrs.K.RANJITHAKALA[1],NEELAGIRI KARTHIK[2], CHILUMURI SRI HARI[3], PILLI PRAVALLIKA[4]

[1]Associate Professor Department of CSE, V.K.R,V.N.B&A.G.K College of Engineering,Gudivada.

[234]UG Students,Department of CSE, V.K.R,V.N.B&A.G.K College of Engineering,Gudivada.

ABSTRACT

In the modern digital era, cybersecurity threats are becoming more advanced, frequent, and globally distributed. Organizations require collaborative systems to detect, analyze, and respond to cyberattacks efficiently. A Threat Intelligence Sharing Platform using MISP (Malware Information Sharing Platform) provides a structured and automated approach to sharing cybersecurity threat information. MISP is an open-source platform designed to collect, store, correlate, and distribute Indicators of Compromise (IOCs) such as malicious IP addresses, domains, file hashes, URLs, and attack patterns. This system enables real-time sharing of threat intelligence between organizations, improving situational awareness and reducing incident response time. By integrating automation, standardized formats, and APIs, the platform ensures efficient communication of security data. The proposed system strengthens cybersecurity defense mechanisms by enabling proactive threat detection and collaborative response across multiple organizations

I INTRODUCTION

Cybersecurity has become a critical concern for governments, enterprises, and individuals due to the increasing number of cyberattacks such as phishing, ransomware, malware infections, and data breaches. Traditional security systems operate independently and lack effective mechanisms for sharing threat information. As a result, organizations often respond to threats after damage has already occurred. Threat Intelligence Sharing Platforms address this gap by enabling organizations to exchange security-related data in real time. MISP is widely used for this purpose, as it provides a standardized and automated environment for sharing threat intelligence. The proposed system leverages MISP to create a centralized platform that enhances collaboration, improves detection capabilities, and strengthens overall cybersecurity posture.To overcome these challenges, Threat Intelligence Sharing Platforms have been developed to enable collaboration among organizations by sharing information about cyber threats in real time. These platforms help security teams understand attack patterns, identify Indicators of Compromise (IOCs), and respond more effectively to emerging threats.MISP (Malware Information Sharing Platform) is an open-source threat intelligence platform designed to collect, store, analyze, and share structured cybersecurity information. It allows organizations to exchange threat data in a standardized format, improving interoperability and automation. By using MISP, security analysts can correlate threat data from multiple sources, enhance situational awareness, and take proactive measures against potential attacks.

II RELATED WORK

Threat intelligence sharing has gained significant attention in recent years due to the increasing complexity and frequency of cyberattacks. Several research studies and frameworks have been proposed to improve the way organizations collect, analyse , and share cybersecurity information .One of the widely used approaches in earlier systems is the use of Security Information and Event Management (SIEM) tools. SIEM systems collect logs from different sources and provide centralized monitoring and alerting. However, SIEM systems mainly focus on internal organizational data and have limited capability for external threat sharing.Another important development in this area is the STIX (Structured Threat Information eXpression) and TAXII (Trusted Automated eXchange of Intelligence Information) standards. These frameworks provide a structured format and protocol for exchanging cyber threat intelligence between systems. They have improved interoperability but still require integration with platforms for practical implementation.K

The Malware Information Sharing Platform (MISP) has emerged as one of the most effective open-source solutions for threat intelligence sharing. MISP supports the collection, storage, correlation, and distribution of Indicators of Compromise (IOCs) in a standardized and machine-readable format. It also allows organizations to share threat data in real time through APIs and automated feeds. Many cybersecurity organizations and government agencies have adopted MISP due to its

Recent research has also focused on integrating MISP with machine learning techniques to improve threat prediction and anomaly detection. Some studies explore the combination of MISP with SOAR (Security Orchestration, Automation, and Response) tools to automate incident response workflows.

Despite these advancements, challenges such as data privacy, trust between organizations, and scalability still exist in threat intelligence sharing systems. The proposed system builds upon these existing approaches by leveraging MISP to provide a more efficient, standardized, and collaborative platform for sharing cyber threat intelligence.

III LITERATURE REVIEW

The concept of threat intelligence sharing has been widely studied in cybersecurity research, focusing on improving collaboration between organizations to detect and mitigate cyber threats effectively. Various researchers have proposed frameworks, models, and tools to enhance the sharing of Indicators of Compromise (IOCs) and improve incident response capabilities.

Early research in cybersecurity primarily focused on intrusion detection systems (IDS) and firewalls, which were designed to protect individual systems rather than facilitate information sharing. These systems were effective in detecting known attacks but lacked the ability to share threat data across organizations, limiting their overall effectiveness in combating large-scale cyberattacks.

With the increasing complexity of cyber threats, researchers introduced standardized frameworks such as STIX (Structured Threat Information eXpression) and TAXII (Trusted Automated eXchange of Intelligence Information). These standards helped in structuring and exchanging threat intelligence data in a machine-readable format.

Studies show that STIX/TAXII significantly improved interoperability between different cybersecurity tools, but their adoption required complex integration efforts.

The Malware Information Sharing Platform (MISP) has been extensively studied and adopted as an open-source solution for collaborative threat intelligence sharing. According to multiple research papers, MISP provides a flexible and scalable platform for collecting, storing, and distributing cybersecurity information.

It supports automated sharing of threat events, correlation of indicators, and integration with external security tools. Researchers highlight that MISP reduces response time and improves situational awareness among security teams.

Recent studies have focused on enhancing MISP by integrating it with machine learning algorithms for predictive threat detection. These approaches aim to identify patterns in historical threat data to predict future attacks. Other research explores combining MISP with SOAR (Security Orchestration, Automation, and Response) systems to automate incident handling and response workflows.

Despite these advancements, literature also identifies several challenges such as data privacy concerns, trust issues between sharing organizations, and scalability limitations in large deployments. Some studies suggest implementing access control mechanisms and encryption techniques to address these issues.

Overall, existing literature supports the effectiveness of MISP as a robust platform for threat intelligence sharing, while also highlighting the need for further improvements in automation, scalability, and intelligent threat prediction. The proposed system builds on these findings to develop an efficient and secure threat intelligence sharing platform.

IV EXISTING SYSTEM

In the existing cybersecurity environment, organizations mainly rely on isolated security solutions to protect their systems from cyber threats. These include firewalls, antivirus software, intrusion detection systems (IDS), intrusion prevention systems (IPS), and Security Information and Event Management (SIEM) tools. These systems are designed to detect and prevent attacks within a single organization but do not effectively support cross-organization threat intelligence sharing.

In most cases, threat information is shared manually through emails, reports, or informal communication channels between security teams. Some organizations use basic threat feeds provided by third-party vendors, but these feeds are often generic and not customized to specific organizational needs. Although SIEM systems collect and analyze security logs from multiple sources, their focus remains internal, limiting their ability to contribute to broader threat intelligence ecosystems.

A few advanced systems support structured data sharing using standards such as STIX and TAXII. However, these systems require complex configuration and are not widely implemented in small and medium-scale organizations. As a result, real-time collaboration between different organizations is still limited.

DISADVANTAGES

The existing cybersecurity systems have several limitations that reduce their efficiency in handling modern and complex cyber threats. Most organizations rely on isolated security tools such as firewalls, intrusion detection systems, antivirus software, and SIEM

systems, which mainly focus on internal protection rather than external collaboration. Threat intelligence sharing is often done manually through emails, reports, or informal communication, making the process slow, error-prone, and inefficient. There is also a lack of standardized formats for exchanging threat data, which leads to inconsistencies and difficulties in analysis across different systems. Due to limited real-time collaboration between organizations, the response to cyber incidents is often delayed, allowing attackers to cause significant damage before countermeasures are implemented.

Additionally, existing systems lack proper automation and scalability, making it difficult to handle large volumes of threat data from multiple sources. Overall, these limitations result in poor threat visibility, weak coordination, and reduced effectiveness in preventing advanced cyberattacks.

V PROPOSED SYSTEM

The proposed system is a Threat Intelligence Sharing Platform using MISP (Malware Information Sharing Platform) that enables organizations to efficiently collect, analyze, and share cybersecurity threat information in a structured and automated manner. This system is designed to overcome the limitations of existing isolated security solutions by providing a centralized platform for real-time threat intelligence sharing. MISP allows the integration of multiple data sources such as security tools, external threat feeds, and partner organizations to gather Indicators of Compromise (IOCs) like malicious IP addresses, domains, file hashes, and URLs.

The proposed system standardizes all threat data into a unified format, ensuring consistency and easy interpretation across different organizations. It supports automated sharing through APIs, enabling real-time synchronization of threat information between connected systems. The platform also provides features such as event correlation, data enrichment, tagging, and classification of threats, which help security analysts understand attack patterns more effectively.

In addition, the system includes role-based access control to ensure secure sharing of sensitive intelligence only among authorized users. A centralized dashboard is provided for monitoring, visualization, and analysis of threat activities. By combining automation, standardization, and collaboration, the proposed system significantly improves the speed and accuracy of threat detection and response.

Overall, the proposed MISP-based platform enhances cybersecurity by enabling proactive threat intelligence sharing, reducing response time, and strengthening collaboration between organizations to effectively combat evolving cyber threats.

ADVANTAGES

The proposed Threat Intelligence Sharing Platform using MISP offers several advantages that significantly improve cybersecurity operations and collaboration between organizations. It enables real-time sharing of threat intelligence, allowing security teams to quickly respond to emerging cyber threats and reduce potential damage. By using a standardized format for Indicators of Compromise (IOCs), the system ensures consistency, accuracy, and easy interpretation of threat data across different platforms.

The platform improves collaboration between multiple organizations by allowing secure and automated exchange of threat information through APIs. This enhances collective defense mechanisms and helps identify global attack patterns more effectively. Automation of threat collection, analysis, and sharing reduces manual effort and minimizes the chances of human error.Another key advantage is faster incident response, as security teams can access updated and relevant threat intelligence instantly. The system also provides better visibility into cyber threats through centralized dashboards and correlation of events from multiple sources. Additionally, role-based access control ensures secure handling of sensitive data, maintaining trust and confidentiality among participating organizations.

VI METHODOLOGY

The methodology of the proposed Threat Intelligence Sharing Platform using MISP is designed to collect, process, analyze, and share cybersecurity threat data in a structured and automated manner. The system follows a step-by-step approach to ensure efficient handling of threat intelligence and real-time collaboration between organizations.

Initially, threat data is collected from multiple sources such as security tools (IDS/IPS, firewalls, antivirus systems), external threat feeds, and partner organizations. This data includes Indicators of Compromise (IOCs) like malicious IP addresses, domains, URLs, file hashes, and suspicious activity patterns.Once collected, the data is normalized and converted into a standardized format supported by MISP. This ensures consistency and allows seamless sharing across different systems. The processed data is then stored in the MISP database as structured events, where each event represents a specific threat scenario.After storage, the system performs correlation and enrichment of threat data by linking related indicators and identifying attack patterns. This helps in improving the understanding of cyber threats and identifying possible relationships between different incidents.

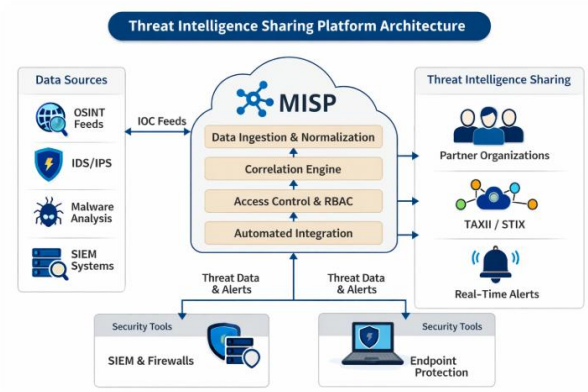
The platform then enables automated sharing of threat intelligence using APIs and secure communication channels. Authorized organizations can access, update, and share relevant threat information in real time based on predefined access controls.

Finally, a web-based dashboard is used to visualize threat data, monitor ongoing events, and analyze trends. This helps security analysts make informed decisions and respond quickly to cyber incidents.

Overall, the methodology ensures efficient data flow from collection to sharing, enabling proactive threat detection and improved cybersecurity collaboration.

VII SYSTEM MODEL

SYSTEM ARCHITECTURE



VIII RESULTS AND DISCUSSIONS

The implementation of the Threat Intelligence Sharing Platform using MISP demonstrates significant improvements in the way cybersecurity threat data is collected, analyzed, and shared across organizations. The system successfully integrates multiple threat intelligence sources and converts raw security data into structured Indicators of Compromise (IOCs), enabling efficient analysis and collaboration.

The results show that real-time sharing of threat information is achieved through automated APIs, reducing the dependency on manual reporting. Security events such as malicious IP addresses, suspicious domains, and file hashes are efficiently stored, correlated, and distributed among connected organizations. This leads to faster identification of cyber threats and improved incident response time.

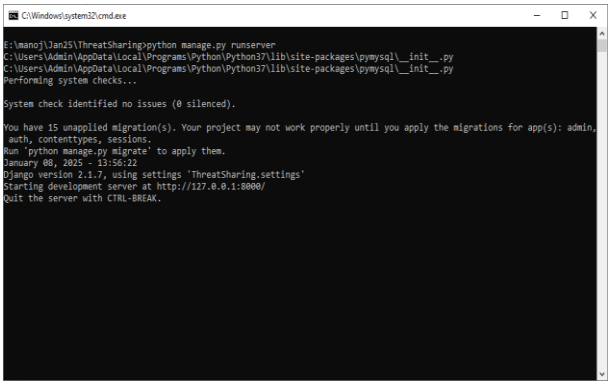
The centralized dashboard provides clear visualization of threat trends, helping security analysts understand attack patterns and take proactive measures. Event correlation features in MISP allow the system to identify relationships between different threats, which enhances situational awareness and supports better decision-making.

In terms of performance, the system reduces redundancy in threat data and ensures consistency through standardized formats. Organizations participating in the platform benefit from shared intelligence, which improves their overall cybersecurity posture. The system also demonstrates scalability, as it can handle increasing volumes of threat data from multiple sources without performance degradation.

From the discussion perspective, it is observed that collaborative threat intelligence sharing significantly strengthens defense mechanisms against evolving cyberattacks. However, challenges such as trust between organizations, data privacy concerns, and proper access control must be carefully managed. Despite these challenges, the MISP-based platform proves to be an effective solution for modern cybersecurity needs by enabling proactive, automated, and coordinated threat intelligence sharing.

SCREEN SHOTS

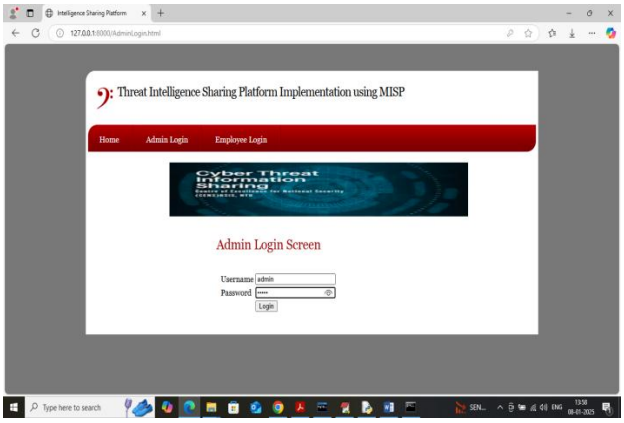
Now double click on 'run.bat' file to start python server and get below page



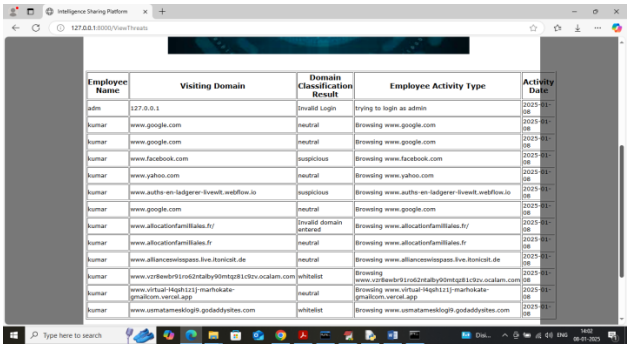
In above screen python web server started and now open browser and enter URL as http://127.0.0.1:8000/index.html and then press enter key to get below page

In above screen click on 'Admin Login' link to get below page

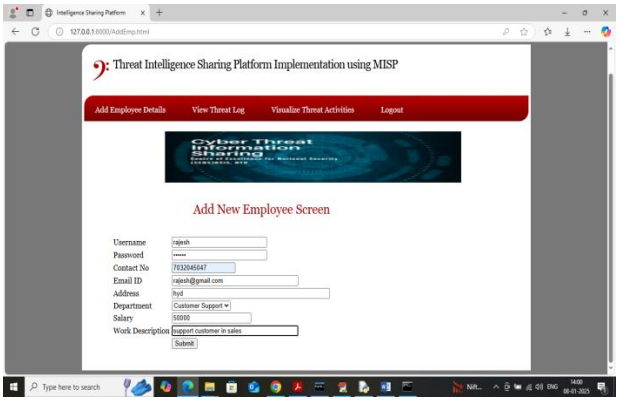
International Journal of Engineering Research and Science & Technology



In above screen admin is login and after login will get below page

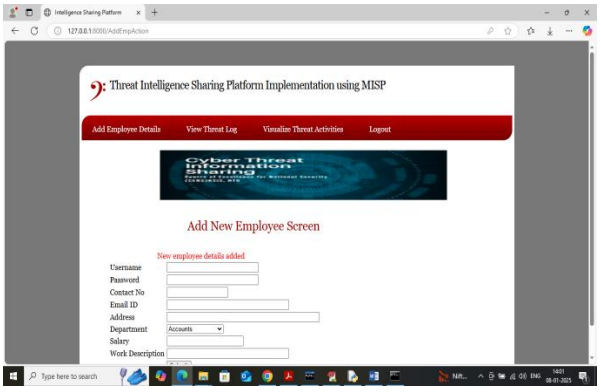


In above screen admin can view all threats access domain activities done by employees along with username. In above screen domain access classification is done by using MISP ML module. Now click on 'Visualize Threat Activities' link to get below page

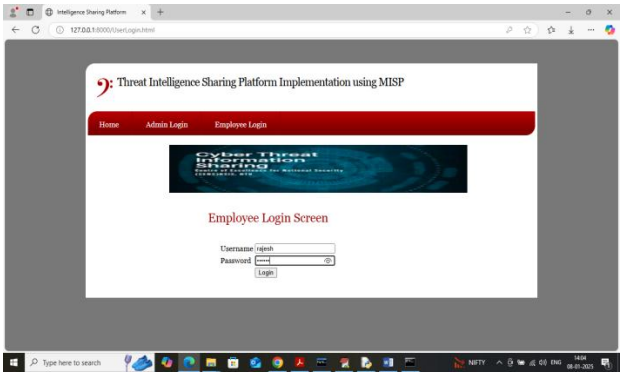


In above screen admin is adding employee details and then press button to get below page

In above screen admin can view activities graph where x-axis represents 'type of activity' detected by MISP and y-axis represents counts. Now logout and login as employee

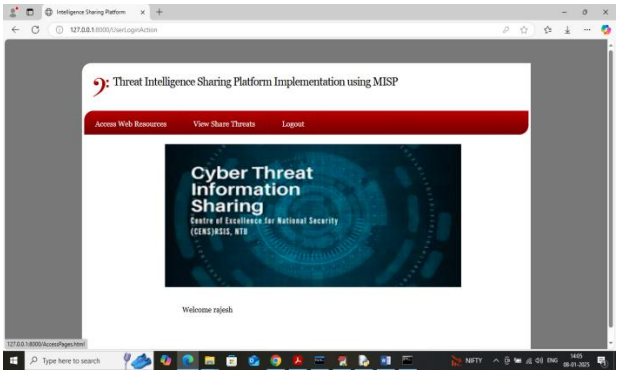


In above screen employee details added to database and now admin can click on 'View Threat Log' link to view all activities done by his employee

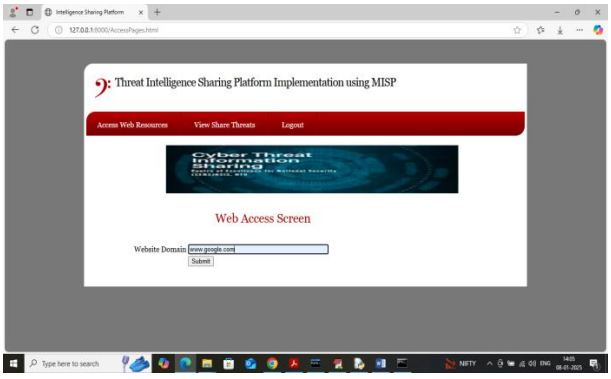


In above screen employee is login and if employee enter invalid login then that also detected and added to logs and after login will get below page

International Journal of Engineering Research and Science & Technology

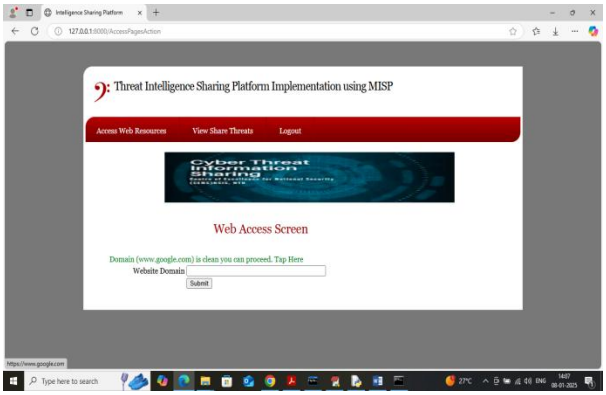


In above screen employee can click on 'Access web Resources' link to get below page

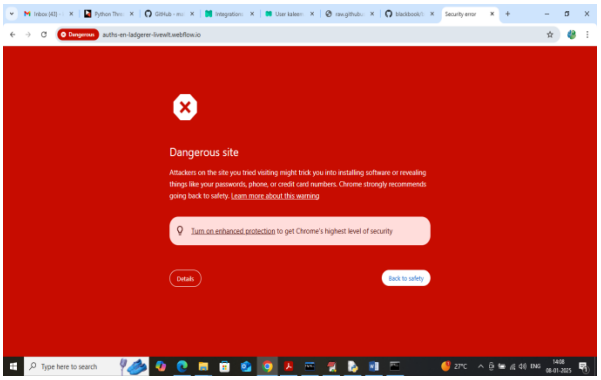


In above screen employee will enter names of domain which he wants to access and then MISP will monitor above domain and then alert employee with below response. (Note: in real time employees will not have free access to browser and they have to access using office provided browser software)

.

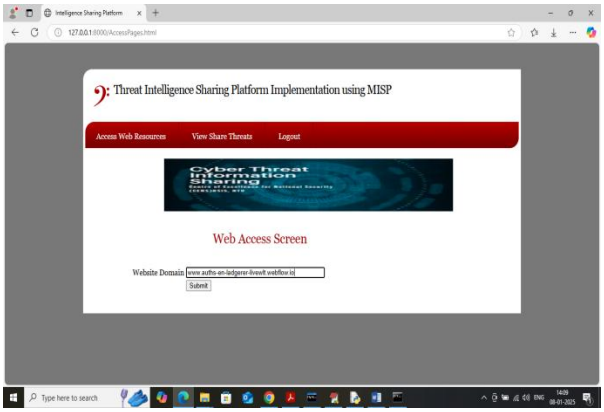


In above screen MISP generated response in green colour by saying 'domain is clean and employee' allowed to access so employee can click on that green text to access resource. Now try another URL

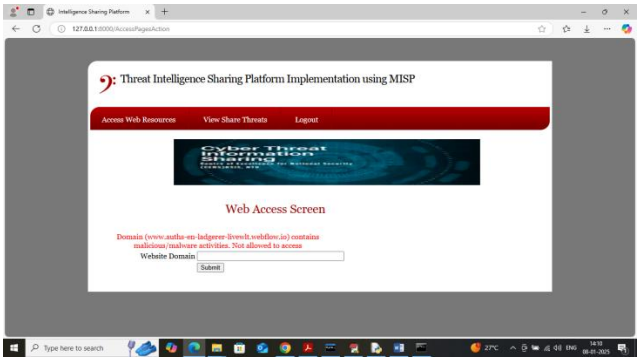


In browser you can see above URL is danger to access which is alert by chrome and now same URL will test with MISP in below pag

e



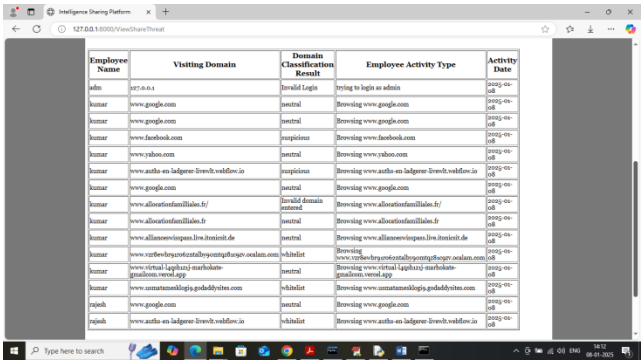
In above screen employee is trying to access harmful malware page and below is the MISP response



In above screen MISP responded with red colour text saying 'Not allowed to access'. (note: we kept some

malicious URL inside code folder which you can use for testing and this filename is 'malicious-url.txt').

Now click on 'View Share Threat' link to view all threats access share and perform by other employees.



In above screen employee can see all types of activities share from other employees.

Similarly by following above screens you can save server from accessing malware based domains.

IX CONCLUSION

The Threat Intelligence Sharing Platform using MISP provides an efficient and reliable solution for enhancing cybersecurity through collaborative threat information exchange. The system successfully addresses the limitations of traditional security approaches by enabling real-time, automated, and standardized sharing of cyber threat intelligence among multiple organizations. By collecting and analyzing Indicators of Compromise (IOCs) from diverse sources, the platform improves the ability to detect, analyze, and respond to cyberattacks more effectively.

The use of MISP ensures structured data representation, better correlation of threat events, and seamless integration with various security tools and external feeds. This significantly reduces response time and enhances situational awareness for security analysts. The centralized dashboard further supports monitoring and decision-making by providing clear visualization of threat activities and patterns.

Overall, the proposed system strengthens organizational cybersecurity by promoting proactive defense strategies instead of reactive responses. It enhances collaboration, improves efficiency, and provides a scalable framework for handling evolving cyber threats. Therefore, the MISP-based Threat Intelligence Sharing Platform is a robust and practical solution for modern cybersecurity challenges.

REFERENCES

- MISP Project Documentation – Malware Information Sharing Platform & Threat Sharing(2026). https://www.misp-project.org/
- MITRE ATTACK Framework(2025). https://attack.mitre.org/
- NIST Cybersecurity Framework(CSF) (2026) https://www.nist.gov/cyberframework
- STIX&TAXII Standards–OASIS Cyber Threat Intelligence(2026). https://oasis-open.github.io/cti-documentation/
- ENISA Threat Landscape Reports – European Union Agency for Cybersecurity(https://www.enisa.europa.eu/ (2026).
- IEEE Xplore Digital Library–Cyber Threat Intelligence and Information SharingResearch Papers(2026) https://ieeexplore.ieee.org/
- Open Source Security Information Sharing Platforms and MISP Integration Studies (Various Journals)(2026).