ISSN 2319-5991 www.ijerst.com
© 2026 IJERST. All Rights Reserved
Peer Reviewed, Referred & Indexed Journal

Research Paper

THREAT INTELLIGENCE SHARING PLATFORM IMPLEMENTATION USING MISP

[1]PULAGAM SIVANI, [2]Y SRINIVAS RAJU

[1]Students, Department of MCA, B V Raju College, Bhimavaram Ap

[2]Assistant Professor**,** Department of MCA, B V Raju College, Bhimavaram Ap

ABSTRACT

With the increasing number of cyber threats and malicious activities in organizational environments, effective threat detection and information sharing have become essential for maintaining cybersecurity. Traditional security systems often operate in isolation, limiting their ability to detect and respond to emerging threats in real time. This project proposes a Threat Intelligence Sharing Platform using the Malware Information Sharing Platform (MISP) to monitor, detect, and share threat information across users within an organization. The system continuously monitors user activities such as login attempts and web resource access to identify suspicious behavior, including unauthorized login attempts and access to malicious domains. When a threat is detected, the system restricts access and logs the activity. These threat logs are shared across the organization, enabling all users to stay informed about potential risks. The platform includes modules for admin and employee roles, where the admin can manage users, view threat logs, and visualize threat activities, while employees can access web resources and view shared threat intelligence. Visualization tools are used to represent threat and normal activities, improving understanding and decision-making. The integration of MISP enhances real-time threat detection and collaborative security. This system provides a proactive approach to cybersecurity by enabling early detection, prevention, and sharing of threats, thereby strengthening organizational security and awareness.

Keywords : Cybersecurity, MISP, Threat Intelligence, Malware Detection, Network Security, Threat Sharing, Intrusion Detection, Data Visualization, Access Control, Security Monitoring

I. INTRODUCTION

In today's digital era, organizations are increasingly dependent on online systems and networked environments, making them more vulnerable to cyber threats such as malware attacks, unauthorized access, and phishing attempts. Traditional security systems often rely on isolated detection mechanisms, which limit their ability to identify and respond to emerging threats effectively. As cyber-attacks

become more sophisticated, there is a growing need for advanced systems that can not only detect threats in real time but also share threat intelligence across users and systems to enhance overall security.

Threat intelligence sharing has emerged as a powerful approach in cybersecurity, allowing organizations to collaboratively identify and respond to potential threats. The Malware Information Sharing Platform (MISP) is one such framework that enables the collection, analysis, and sharing of threat intelligence. MISP helps organizations detect malicious activities such as unauthorized login attempts and access to harmful domains, and it allows sharing of this information across users to prevent further attacks. By leveraging such platforms, organizations can build a proactive defense mechanism rather than reacting to threats after they occur.

In this project, a threat intelligence sharing platform is proposed using MISP to monitor user activities and detect potential threats in an organizational environment. The system includes modules for admin and employee roles, where the admin can manage users, view logs, and analyze threat activities, while employees can access web resources and receive alerts for malicious domains. The platform also provides visualization of threat data to improve understanding and decision-making. This approach enhances cybersecurity by enabling real-time detection, prevention, and sharing of threats within the organization.

II SURVEY OF RESEARCH

1. Traditional Intrusion Detection Systems (IDS)

Traditional Intrusion Detection Systems are designed to monitor network traffic and detect suspicious activities based on predefined rules or signatures. These systems can identify known threats effectively but struggle to detect new or unknown attacks. Research shows that signature-based IDS lacks adaptability, while anomaly-based systems often generate false positives. Additionally, these systems operate independently and do not share threat information across networks. This limitation reduces their effectiveness in preventing widespread attacks. The need for collaborative and intelligent systems has led to the development of advanced threat intelligence platforms.

2. Threat Intelligence Sharing Platforms

Threat intelligence sharing platforms enable organizations to share information about cyber threats, improving collective security. Research indicates that sharing threat data such as malicious IP addresses, domains, and attack patterns helps organizations respond more quickly to emerging threats. Platforms like MISP provide a standardized framework for collecting, analyzing, and distributing threat intelligence. These systems enhance situational

awareness and reduce response time. This project utilizes MISP to enable real-time threat sharing and improve organizational security.

3. Malware Detection Techniques

Malware detection is a critical aspect of cybersecurity. Traditional techniques include signature-based detection and heuristic analysis. However, these methods are limited in detecting new and evolving malware. Research highlights the use of machine learning and behavioral analysis to improve malware detection accuracy. These techniques analyze patterns in user behavior and network traffic to identify anomalies. This project incorporates MISP's capabilities to detect malicious domains and suspicious activities effectively.

4. Role-Based Access Control (RBAC)

Role-Based Access Control is widely used to restrict system access based on user roles. Research shows that RBAC improves security by ensuring that users can only access resources relevant to their roles. In organizational environments, RBAC helps prevent unauthorized access and reduces the risk of insider threats. This project implements RBAC by defining roles such as admin and employee, ensuring controlled access to system functionalities.

5. Data Visualization in Cybersecurity

Data visualization plays a crucial role in analyzing and understanding cybersecurity data. Graphical representations such as charts and dashboards help administrators quickly identify patterns and trends in threat activities. Research indicates that visualization tools improve decision-making and reduce response time. This project includes visualization modules to display threat and normal activities, enabling better analysis of system behavior.

6. Challenges in Cybersecurity Systems

Despite advancements in cybersecurity technologies, challenges such as data privacy, scalability, and real-time processing remain significant. Research highlights that handling large volumes of data and ensuring accurate threat detection without false positives are major concerns. Additionally, integrating multiple security tools can be complex. This project addresses these challenges by integrating MISP with a user-friendly platform that provides efficient threat detection, sharing, and visualization, ensuring a practical and scalable solution for organizational security.

III. WORKING METHODOLOGY

The proposed Threat Intelligence Sharing Platform begins with user registration and authentication, where the admin creates employee accounts and assigns login credentials. The system implements role-based access control, allowing only authorized users to access specific functionalities. Once users log in, the platform starts monitoring all user activities, including login attempts and web resource access. These activities are

continuously tracked and sent to the MISP framework for analysis. The system collects logs such as accessed domains, user actions, and timestamps, which are stored in a centralized database and also shared across users for awareness.

In the next phase, the MISP framework analyzes the collected data to detect potential threats. When an employee attempts to access a domain, the system checks whether the domain is safe or malicious by comparing it with known threat intelligence data. If the domain is identified as harmful, access is immediately restricted, and an alert is generated. Similarly, suspicious login attempts, such as unauthorized access to admin accounts, are detected and logged. All detected threats are stored and shared among users, enabling collaborative awareness and prevention. This automated detection process enhances the system's ability to respond quickly to security risks.

Finally, the system provides visualization and reporting features for better analysis of threat activities. Admin users can view detailed logs of all user activities and visualize the number of threats and normal actions through graphical representations. Employees can also access shared threat logs to stay informed about potential risks. The system ensures transparency by maintaining a record of all activities and sharing threat intelligence across the organization. By integrating MISP with monitoring, detection, and visualization modules, the proposed methodology provides an efficient, secure, and proactive approach to managing cybersecurity threats.

IV RESULTS EXPLANATIONS

In propose work employing MISP (Malware Information Sharing Platform & Threat Sharing) framework to detect threats from organization environment. This tool will be listening on all activities which are perform online such as invalid login to admin account, reaching or accessing to IP or domain which contains malware contents and then block users from accessing such domains.

In organizations employees are allowed to access their own accounts but sometime some malicious employees may try to login to higher authority account and such activities can be detected using MISP.

Often employees allow to access online web resources and those resource domain may contain harmful malware which can corrupt server. MISP will monitor all browsing domain and then restrict user from accessing online such domains and then share all threat detected domains with other users

To implement this project we have designed following modules

1) Admin Login: admin can login to system using username and password as 'admin and admin'. After login admin will add employee details and issue

login details to employee for accessing accounts

2) View Threat Log: using this module admin can view all browsing logs which are access by employees. This log automatically share with all users whatever activity perform by one user. By using this log admin and other employees can know which domain is harmful or normal
3) Visualize Threat Activities: using this module admin can visualize how many threats and normal activities perform by employees

Employee Modules

1) Employee Login: employee can login to system using username and password given by admin
2) Access Web Resources: using this module employee can access desired domains and then MISP will monitor all those domains to alert employees
3) View Share Threats: can view all threats access perform by employees



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 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 can see all types of activities share from other employees.

V. CONCLUSION

The proposed Threat Intelligence Sharing Platform using MISP provides an effective and proactive solution for detecting, preventing, and sharing cybersecurity threats within an organization. By continuously monitoring user

activities such as login attempts and web resource access, the system is capable of identifying suspicious behavior and restricting access to malicious domains in real time. The integration of MISP enhances the system's ability to analyze and share threat intelligence across users, improving overall awareness and response to potential attacks. Role-based access control ensures secure and controlled system usage, while visualization tools help administrators understand threat patterns and make informed decisions. The system reduces the risk of cyber-attacks, prevents unauthorized access, and promotes collaborative security. Overall, this project demonstrates the importance of threat intelligence sharing and provides a scalable, efficient, and reliable approach to strengthening organizational cybersecurity.

REFERENCES

[1] S. Axelsson, "Intrusion detection systems: A survey and taxonomy," Technical Report, 2000.

[2] R. Sommer and V. Paxson, "Outside the closed world: On using machine learning for network intrusion detection," in *Proc. IEEE Symposium on Security and Privacy*, 2010, pp. 305–316.

[3] E. Alpaydin, *Introduction to Machine Learning*, 3rd ed., Cambridge, MA, USA: MIT Press, 2014.

[4] MISP Project, "Malware Information Sharing Platform & Threat Sharing," 2020.

[5] C. Tankard, "Advanced persistent threats and how to monitor and deter them," *Network Security*, vol. 2011, no. 8, pp. 16–19, 2011.

[6] W. Stallings, *Network Security Essentials: Applications and Standards*, 6th ed., Pearson, 2017.

[7] B. Schneier, *Applied Cryptography: Protocols, Algorithms, and Source Code in C*, Wiley, 1996.

[8] J. Behl and S. Behl, *Cybersecurity and Cyberwar: What Everyone Needs to Know*, Oxford University Press, 2017.

[9] National Institute of Standards and Technology (NIST), "Guide to Intrusion Detection and Prevention Systems (IDPS)," Special Publication 800-94, 2012.

[10] Kaspersky Lab, "Cyber threat intelligence reports," 2020.