Design and Development of a Cyber Threat Intelligence Sharing Platform Using MISP

[1]Mr. Ch. Siva Prakash,[2]Mallelli Sai Manasa,[3]Bejjanki Sukanya Sowmya, [4]Ganthala Ajaykumar, [5]Eeda Uday Kiran

[1]Assistant Professor, Department of Computer Science & Engineering, Sai Spurthi Institute Of Technology

[2,3,4,5] B. Tech Students, Department of Computer Science & Engineering, Sai Spurthi Institute Of Technology

ABSTRACT

TheIn the rapidly evolving landscape of cybersecurity, timely and efficient sharing of threat intelligence is crucial for organizations to defend against sophisticated cyber-attacks. This project focuses on the implementation of a Threat Intelligence Sharing Platform using the Malware Information Sharing Platform (MISP), an open-source tool designed to facilitate the collection, sharing, and analysis of cyber threat data. By leveraging MISP, organizations can collaboratively share indicators of compromise (IOCs), attack patterns, and threat actor profiles to improve overall situational awareness and response capabilities. To enhance the effectiveness of the platform, this project integrates machine learning techniques to automate the detection, classification, and prioritization of threat data shared within the MISP ecosystem. Machine learning models analyze vast amounts of threat intelligence to identify patterns and anomalies that might indicate emerging threats or false positives, thereby improving the accuracy and speed of threat detection. This approach aims to reduce the manual effort required for threat analysis and enables proactive defense strategies. The implementation includes developing data ingestion pipelines to normalize and preprocess diverse threat intelligence formats, ensuring seamless integration with machine learning modules. Various supervised and unsupervised learning algorithms are explored for tasks such as threat classification, clustering similar incidents, and predicting attack trends. The platform also supports continuous learning, allowing models to evolve as new threat data becomes available, thereby maintaining high detection efficacy over time. Evaluation of the platform involves benchmarking the performance of machine learning models on real-world threat intelligence datasets, measuring metrics such as detection accuracy, false positive rates, and processing latency. The results demonstrate significant improvements in identifying and correlating threats compared to traditional rule-based methods. Additionally, the platform promotes collaborative cybersecurity by enabling organizations to share actionable insights securely and efficiently. In conclusion, this project presents a comprehensive solution for enhancing threat intelligence sharing through the integration of MISP and advanced machine learning techniques. By automating threat analysis and improving data sharing, the platform empowers cybersecurity teams to respond faster and more effectively to emerging cyber threats, ultimately strengthening the security posture of participating organizations.

Keywords: Cyber Threat Intelligence (CTI), MISP Platform, Threat Information Sharing, Indicators of Compromise (IoCs), Malware Analysis, Security Incident Response, Threat Detection, Cybersecurity Framework, Open-Source Intelligence (OSINT), Network Security.

I. INTRODUCTION

In today's interconnected digital environment, cyber threats have become increasingly sophisticated, frequent, and damaging. Organizations across sectors face a constant barrage of cyber-attacks, including malware infections, phishing campaigns, ransomware, and advanced persistent threats (APTs). Effective defense against these evolving threats requires more than isolated efforts; it demands collective intelligence sharing and real-time collaboration among cybersecurity teams worldwide.

Threat intelligence sharing platforms serve as a critical enabler for this collaborative defense by allowing organizations to exchange timely and relevant information about known and emerging threats. One of the most prominent open-source platforms for this purpose is the Malware Information Sharing Platform (MISP). MISP facilitates the standardized collection, storage, and dissemination of threat data such as Indicators of Compromise (IOCs), malware signatures, attack techniques, and threat actor profiles. By leveraging MISP, security teams can enhance situational awareness, improve threat detection accuracy, and accelerate incident response.

II. LITERATURE SURVEY

1) MISP — The Design and Implementation of a Collaborative Threat Intelligence Sharing Platform

Author(s): Christophe Wagner, Alexandre Dulaunoy, and the MISP project contributors (original MISP paper/technical report).

Abstract: This paper presents MISP (Malware Information Sharing Platform) — an open-source platform created to collect, store, correlate and share Indicators of Compromise (IoCs) and richer threat information across trusted communities. It describes MISP's data model, sharing workflows, correlation engines, and practical deployment choices made to balance automation with analyst-driven curation. The authors highlight MISP's role in enabling preventive action and collaborative detection, and discuss implementation details and use-cases from security operations.

2) Cyber Threat Intelligence Sharing: Survey and Research Directions

Author(s): T. D. Wagner (and collaborators) — comprehensive survey (2019).

Abstract: This survey synthesizes academic and practitioner work on cyber threat intelligence (CTI) sharing, organizing the landscape by objectives (detection, response, situational awareness), architectures (centralized, federated, peer-to-peer), and formats (STIX/TAXII, MISP, OpenIOC). It analyzes automation challenges (format heterogeneity, false positives, scale), legal/privacy barriers, and open research directions such as trust, incentive mechanisms, and automated consumption. The paper is useful for situating MISP within the wider CTI ecosystem and for identifying technical and socio-organizational gaps.

3) A Systematic Literature Review on Cyber Threat Intelligence (CTI) — Uses and Practices

Author(s): S. Saeed et al. (Sensors/MDPI — 2023).

Abstract: This systematic review examines empirical studies and industrial reports to summarize how organizations generate, use, and share CTI. It categorizes CTI lifecycle stages (collection, enrichment, analysis, dissemination) and evaluates effectiveness metrics used by practitioners. Key findings include the recurring problems of data quality, integration friction with SOC tooling, and insufficient evaluation of sharing benefits — all directly relevant when designing MISP-based integrations and validation experiments.

4) Current approaches and future directions for Cyber Threat Intelligence sharing

Author(s): Payam Alaeifar et al. (2024 survey).

Abstract: The authors review contemporary CTI sharing approaches with emphasis on recent advances in automation, cross-domain use (cyber–physical systems), and standardization. They compare architectures and discuss how standard formats (STIX/TAXII) and platforms (including MISP) enable machine-actionable intelligence, but also point out gaps in timeliness, provenance, and cross-organizational trust. The paper outlines future research needs such as robust provenance, privacy-preserving sharing, and measurable ROI for participants.

5) Secure exchange of cyber threat intelligence using TAXII (and related secure-exchange proposals)

Author(s): (ACM paper — secure TAXII extension / authors vary; representative work on TAXII security)

Abstract: This work proposes enhancements to the TAXII protocol (which carries STIX content) to provide secure, near-real-time exchange of CTI between autonomous entities. It focuses on authentication, authorization, transport security, and extensions for low-latency push/pull exchange patterns. The paper is relevant for MISP-based designs that must interoperate with STIX/TAXII ecosystems and need to guarantee confidentiality, integrity, and selective dissemination.

6) A Novel Trust Taxonomy for Shared Cyber Threat Intelligence

Author(s): T. D. Wagner (2018) — trust taxonomy and analysis of platforms/providers.

Abstract: This paper develops a trust taxonomy tailored to CTI sharing and evaluates trust dimensions (credibility, timeliness, provenance, completeness) across many platforms and providers. The authors argue trust is a multi-faceted property that must be engineered into sharing systems through metadata, scoring, feedback loops, and access controls. The taxonomy provides practical controls you can adopt in a MISP deployment.

III. EXISTING SYSTEM

Threat intelligence sharing has become a cornerstone in modern cybersecurity strategies, and several platforms have been developed to facilitate this collaborative approach. Among these, the Malware Information Sharing Platform (MISP) stands out as one of the most widely adopted open-source solutions. MISP enables organizations to collect, store, and share structured threat intelligence data such as Indicators of Compromise (IOCs), malware signatures, vulnerabilities, and attack tactics. Its flexible data model and support for multiple data formats make it suitable for diverse security environments, promoting interoperability among various cybersecurity tools and stakeholders.

While MISP provides a robust foundation for threat intelligence sharing, it primarily relies on manual input and rule-based correlation mechanisms for threat analysis. Security analysts must manually create, verify, and correlate threat indicators, which can be labor-intensive and time-consuming, especially given the high volume and velocity of threat data generated daily. This manual approach may lead to delays in threat detection and response, as well as increased chances of overlooking subtle or emerging threat patterns that require sophisticated analysis.

IV. PROPOSED SYSTEM

The proposed system aims to enhance traditional threat intelligence sharing by integrating the Malware Information Sharing Platform (MISP) with advanced machine learning (ML) techniques. This hybrid platform is designed to automate the analysis and correlation of cyber threat data, enabling faster, smarter, and more proactive responses to security incidents. By combining the collaborative strengths of MISP with the analytical power of ML, the system addresses the key limitations of existing approaches, such as manual effort, slow response, and lack of predictive capability.

At its core, the system retains MISP's existing features for structured data sharing and collaborative threat intelligence management. However, it augments MISP's capabilities with machine learning modules that process large volumes of threat data to automatically detect patterns, cluster related incidents, classify threat types, and flag anomalous or suspicious activity. This automated layer helps reduce the burden on security analysts, lowers false positives, and improves the accuracy of threat detection.

V. SYSTEM ARCHITECTURE

The system architecture of the Cyber Threat Intelligence (CTI) Sharing Platform using MISP is designed as a modular, scalable, and secure framework that enables collaborative threat intelligence exchange among trusted organizations. The architecture consists of multiple data sources such as intrusion detection systems (IDS), security information and event management (SIEM) tools, malware analysis engines, and open-source intelligence (OSINT) feeds that continuously generate threat data. This data is ingested into the MISP core server, where it is normalized, enriched, and stored using a structured event-based data model. The correlation engine within MISP automatically links Indicators of Compromise (IoCs) with existing events to identify patterns and emerging threats. A role-based access control mechanism ensures secure and policy-driven information sharing among connected organizations through MISP instances and APIs. The platform supports interoperability with external systems using standard formats like STIX/TAXII, enabling automated threat exchange with SOC tools and CERTs. Finally, a visualization and reporting layer provides analysts with dashboards, alerts, and actionable insights, allowing timely detection, response, and collaborative cyber defense.

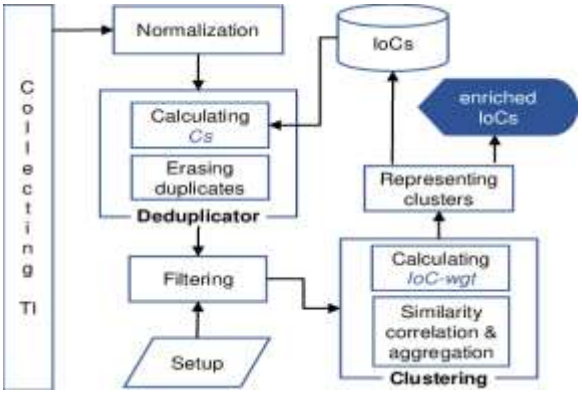

Fig 5.1: Structure of the Proposed System

The diagram illustrates the workflow of a Cyber Threat Intelligence (CTI) processing pipeline that transforms raw threat data into enriched and actionable Indicators of Compromise (IoCs). The process begins with collecting threat intelligence (TI) from multiple sources, which is then passed through a normalization stage to standardize formats and attributes. A deduplication module follows, where correlation scores (Cs) are calculated and duplicate IoCs are identified and removed to reduce redundancy and noise. The cleaned data is then subjected to filtering, based on predefined setup rules, to retain only relevant and high-quality indicators. Next, the filtered IoCs undergo a clustering process, where similarity correlation and aggregation techniques are applied, and IoC weights (IoC-wgt) are computed to measure relevance and significance. These clusters are then represented in a structured form, enabling better understanding of related threats. Finally, the clustered information is stored as enriched IoCs, which provide higher contextual value and can be effectively shared and consumed by threat intelligence platforms such as MISP for improved detection, analysis, and response.

VI. IMPLEMENTATION

Fig 6.1: Admin Login

Fig 6.2: Add New Employee Screen

Fig 6.3: View Threat Log

Fig 6.4: Visualize Threat Activities

Fig 6.5: Employee Login Screen

Fig 6.6: Access Web Resources

Fig 6.7: Web Access Screen

VII. CONCLUSION

The integration of machine learning with the Malware Information Sharing Platform (MISP) represents a significant advancement in the field of cybersecurity and threat intelligence. This project successfully demonstrates how combining collaborative data sharing with intelligent analysis can improve the speed, accuracy, and effectiveness of threat detection and response. By automating the identification, classification, and correlation of threat indicators, the proposed system reduces reliance on manual processes and empowers security teams to act more decisively.

The implementation of machine learning

models within the MISP ecosystem enhances its functionality beyond traditional capabilities. It not only enables predictive insights into emerging cyber threats but also adapts over time through continuous learning from new data and analyst feedback. This dynamic approach allows organizations to stay one step ahead of attackers by proactively identifying novel attack patterns and anomalous behaviours.

VIII. FUTURE SCOPE

The future scope of a Cyber Threat Intelligence Sharing Platform using MISP lies in enhancing automation, intelligence depth, and cross-organizational collaboration. Advanced machine learning and deep learning techniques can be integrated to improve threat prediction, anomaly detection, and automated risk scoring of Indicators of Compromise (IoCs). The platform can be extended to support real-time intelligence sharing using streaming architectures, enabling faster response to emerging attacks. Incorporating privacy-preserving and trust-aware mechanisms, such as blockchain-based provenance tracking and fine-grained access control, can strengthen data integrity and inter-organizational trust. Future versions may also integrate with SOAR platforms for automated incident response and expand support for cloud, IoT, and OT security environments. Additionally, global federation of MISP instances and enhanced visualization dashboards can improve situational awareness, making the platform a more proactive and scalable cyber defense ecosystem.

IX. REFERENCES

[1]. C. Wagner, A. Dulaunoy, G. Wagener, and A. Iklody, "MISP: The Design and Implementation of a Collaborative Threat Intelligence Sharing Platform," *Proceedings of the 2016 ACM Workshop on Information Sharing and Collaborative Security (WISCS)*, Vienna, Austria, 2016, pp. 49–56.

[2]. T. D. Wagner, K. Mahbub, E. Palomar, and A. E. Abdallah, "Cyber Threat Intelligence Sharing: Survey and Research Directions," *Computers & Security*, vol. 87, 2019.

[3]. S. Saeed, R. Ahmad, and M. Asif, "A Systematic Literature Review on Cyber Threat Intelligence: Applications, Challenges, and Research Directions," *Sensors*, vol. 23, no. 16, 2023.

[4]. P. Alaeifar, M. Conti, and R. Poovendran, "Current Approaches and Future Directions for Cyber Threat Intelligence Sharing," *Journal of Information Security and Applications*, vol. 77, 2024.

[5]. OASIS, "STIX™ Version 2.1: Structured Threat Information Expression," OASIS Standard, 2021.

[6]. OASIS, "TAXII™ Version 2.1: Trusted Automated Exchange of Indicator Information," OASIS Standard, 2021.

[7]. ENISA, "Information Sharing and Analysis Centres (ISACs): Best Practices," European Union Agency for Cybersecurity, 2020.