Naples, Italy
December 4 – December 6, 2023

MINDS

Surveying Cyber Threat Intelligence and Collaboration: A Concise Analysis of Current Landscape and Trends

Panagiotis Radoglou-Grammatikis, Elisavet Kioseoglou, Dimitrios Asimopoulos, Miltiadis Siavvas, Ioannis Nanos, Thomas Lagkas, Vasileios Argyriou, Konstantinos E. Psannis, Sotirios Goudos, Panagiotis Sarigiannidis

Presentation Structure

AI4CYBER – Artificial Intelligence for next generation CYBERsecurity

https://ai4cyber.eu

Funded By the European Union

Authors & Contributors

MINDS

Dimitrios-Christos Asimopoulos

UNIVERSITY OF WESTERN MACEDONIA

Panagiotis Radoglou Grammatikis
Elisavet Kioseoglou
Panagiotis Sarigiannidis

ARISTOTLE UNIVERSITY OF THESSALONIKI

Sotirios Goudos

INTERNATIONAL HELLENIC UNIVERSITY

Thomas Lagkas

Kingston University London

Vasileios Argyriou

UNIVERSITY OF MACEDONIA

Konstantinos E. Psannis

SIDROCO

Ioannis Nanos

This project has received funding from the European Union's Horizon 2020 research and innovation programme under grant agreement No 101070450 (AI4CYBER) .

Introduction

Main Part

Conclusions

1

2

3

Introduction

Objectives

CTI Presentation

Importance of Cyber Threat Intelligence (CTI)

Analysis of Current CTI Solutions

Sum up important key points

Future Work

Q/A

Introduction, Objectives, CTI Presentation

Introduction

Evolving Cybersecurity Landscape: In an era where cyber threats are increasingly sophisticated, understanding the evolving landscape of cybersecurity is crucial. This paper delves into how Artificial Intelligence (AI) is reshaping both cyberattacks and defense strategies.

Role of AI in Cybersecurity: AI's role is explored, highlighting its use in automating and enhancing cyberattacks, as well as its potential in developing robust cybersecurity measures, particularly through Machine Learning (ML) and Deep Learning (DL) techniques.

Focus on Cyber Threat Intelligence (CTI): The paper emphasizes the importance of Cyber Threat Intelligence (CTI) in this dynamic environment. CTI involves the collection, analysis, and dissemination of information about potential cyber threats, aiding organizations in proactive defense.

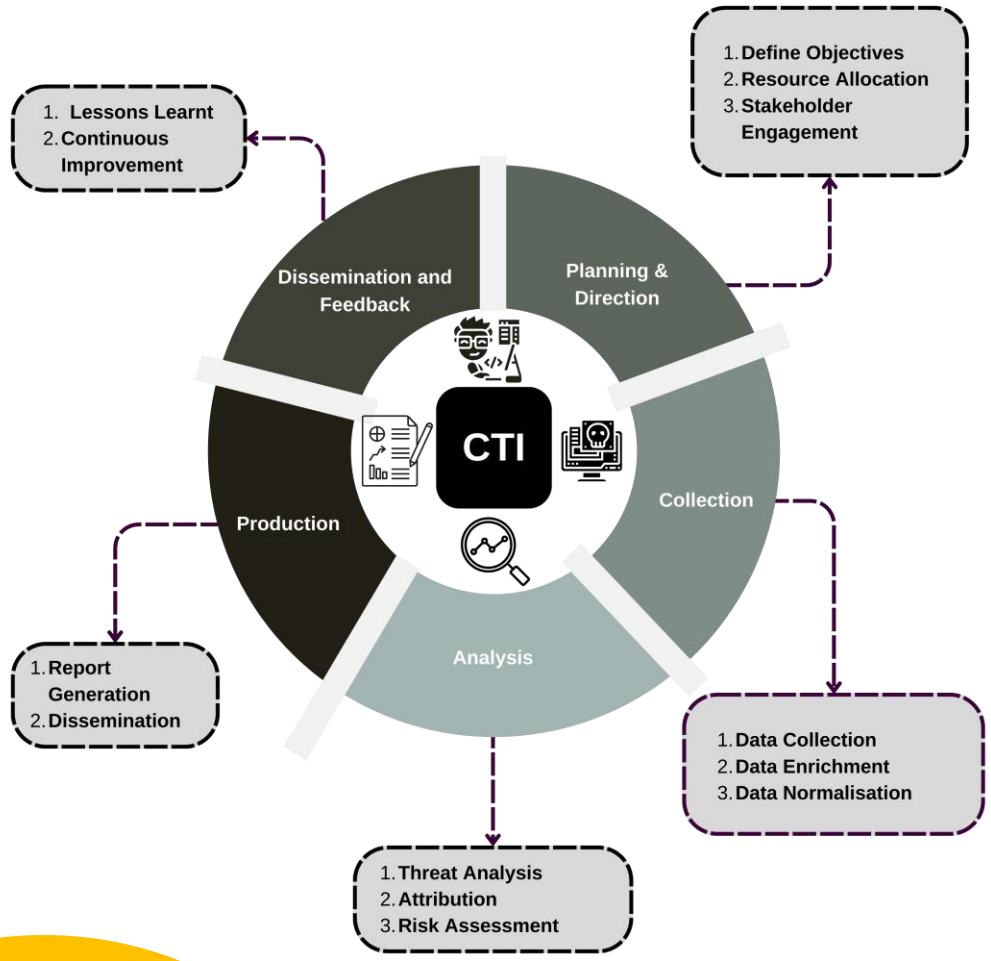
Objectives

Focus on Cyber Threat Intelligence (CTI) Mechanisms: The paper specifically centers on exploring and analyzing the mechanisms of Cyber Threat Intelligence.

Analysis of Existing Solutions: Provide an overview of current solutions in CTI, focusing on their strengths and limitations in addressing modern cyber threats.

Objective of the Paper: The objective of this paper is to provide a concise analysis of the current landscape and trends in CTI and collaboration, offering insights into existing solutions and future directions in cybersecurity."

CTI presentation



This figure illustrates the five main stages of the Cyber Threat Intelligence System (CTIS): (a) Planning and Direction, (b) Collection, (c) Analysis, (d) Production, and (e) Dissemination and Feedback.

- **Planning and Direction**: Establishing objectives and requirements for the intelligence-gathering process.
- **Collection**: Gathering relevant data and information from various sources.
- **Analysis**: Processing and examining the collected data to identify patterns and insights.
- **Production**: Compiling the analyzed information into actionable intelligence.
- **Dissemination and Feedback**: Sharing the intelligence with relevant stakeholders and receiving feedback to refine the process.

Importance of Cyber Threat Intelligence (CTI)

The Importance of Cyber Threat Intelligence (CTI)

Enhance Proactive Defense:
CTI enables organizations to stay ahead of potential threats, allowing them to detect and prevent attacks before they occur, thereby enhancing their overall security posture.

Incident Response:
CTI is crucial in providing detailed information about the nature and scope of threats, aiding organizations in responding more effectively and efficiently to security incidents.

Patch and Vulnerability Management:
By understanding emerging threats, CTI helps prioritize which vulnerabilities should be addressed first, ensuring that resources are focused on the most critical issues.

Risk Assessment:
CTI plays a key role in evaluating the potential impact of various threats on an organization's systems and data, aiding in comprehensive risk management.

Cybersecurity Strategy:
CTI supports the development of a strategic approach to cybersecurity, focusing resources on the most relevant and likely threats to ensure effective defense.

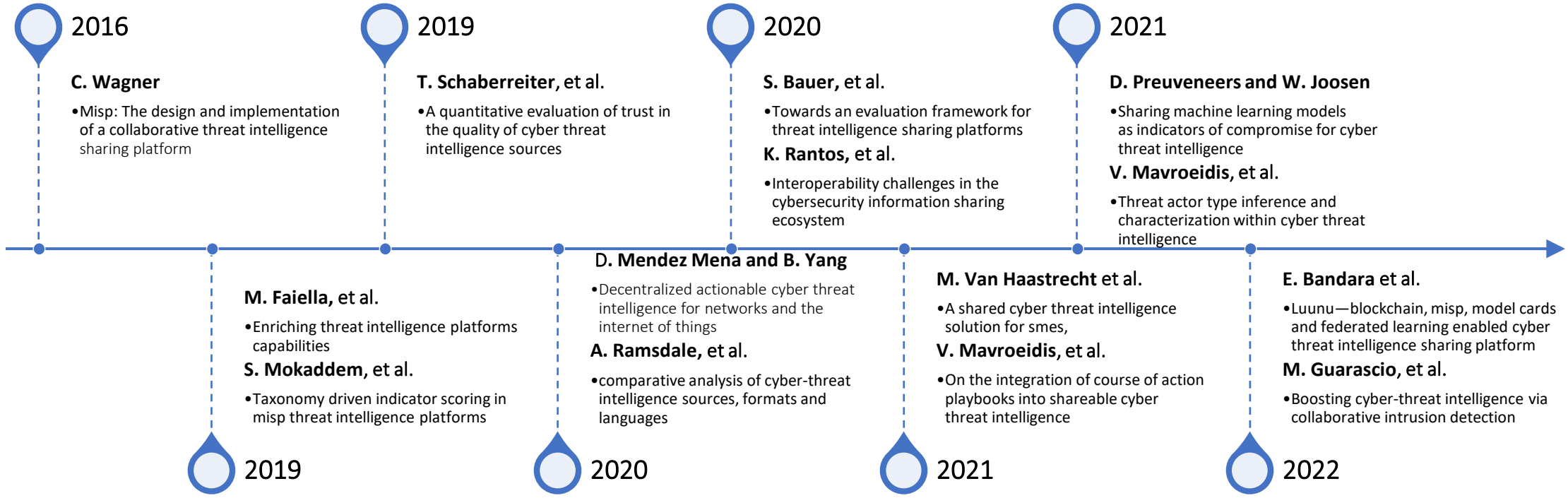
Sharing Insights:
Through CTI, organizations can share valuable insights within their industry or sector, fostering a collaborative approach to cybersecurity.

Decision Making:
CTI provides actionable insights that are essential for making informed decisions regarding security measures and investments.

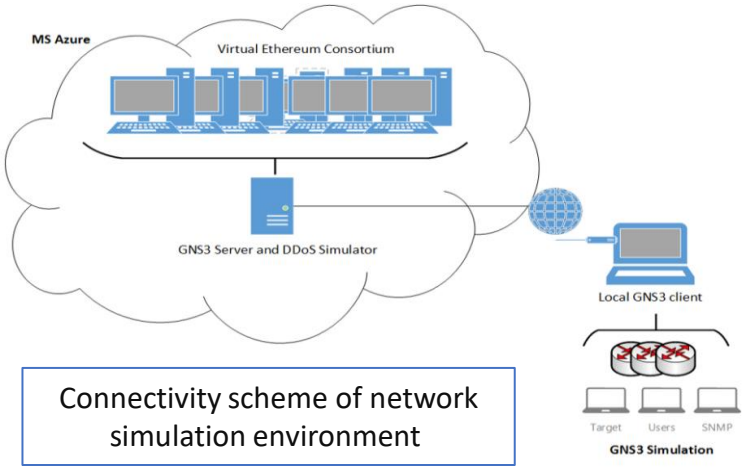
Understanding Attackers:
Studying CTI allows organizations to gain deeper insights into the motivations, techniques, and intentions of various threat actors, which is vital for developing targeted defense strategies.

Analysis of Current CTI Solutions

Existing Works Analysis



Blockchain Protocol in IoT Networks



Connectivity scheme of network simulation environment

Title: Decentralized Actionable Cyber Threat Intelligence for Networks and the Internet of Things

Study: M. Mena and B. Yang's implementation of blockchain protocol in a home network with IoT devices.

Objective: To provide a decentralized system for sharing CTI between service providers and consumers.

Methodology: A network simulation environment with an Ethereum blockchain network, a GNS3 server, and a gateway server.

Application: Simulating a DDoS attack using Bonesi to test the effectiveness of the blockchain-based CTI sharing system.

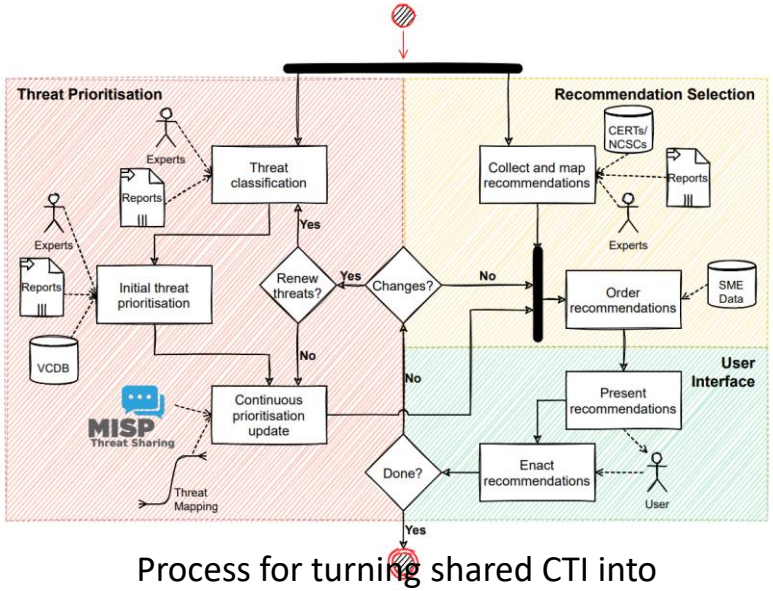
Evaluating network performance, Ethereum network performance, and network security capabilities under two scenarios

- one without attacks to establish a baseline
- another under DDoS attacks

They compared a control group without blockchain and an experimental group with blockchain during a YouTube streaming test.

The **results** showed that when a DDoS attack occurred, it triggered a blockchain transaction via Snort, which then broadcasted to the network and stopped the attack. The impact on home network response time was a minor 2% delay, and the control group had better connection speed. Additionally, a blockchain-based CTI report was generated and distributed to other nodes within 55 seconds of detecting the attack.

CTI for SMEs: A Systematic Review and Prototype Development



Process for turning shared CTI into actionalbe recommendations for SME users

Study Objective: Addressing the limited use of CTI in Small and Medium-sized Enterprises (SMEs) by reviewing current CTI sharing approaches and developing a prototype.

Methodology:

- **Literature Review**: Conducted using a combination of active learning and backward snowballing phases.
- **Focus on SMEs**: Emphasis on identifying CTI sources suitable for SMEs, particularly those less digitally mature.

Key Findings:

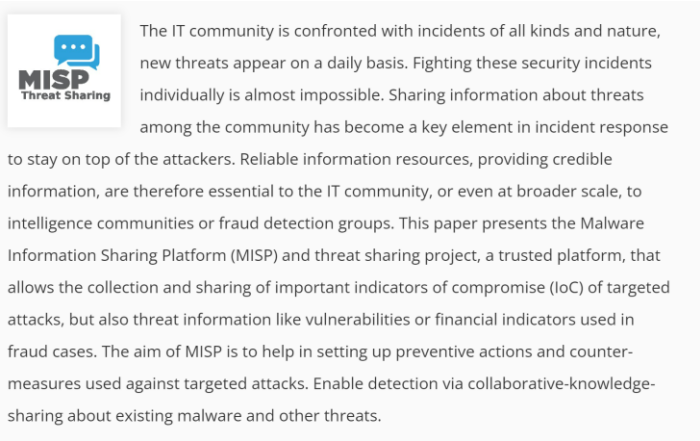
- **Suitable CTI Sources for SMEs**: Structured open-source intelligence sources, especially the VERIS Community Database (VCDB), are identified as most suitable for SMEs.
- **Need for Complementary Sources**: These sources should be complemented by the ENISA rankings for a more comprehensive approach.

Prototype Development:

- **Integration with MISP**: Utilizing the Malware Information Sharing Platform (MISP) in conjunction with the GEIGER application.
- **CERT-RO CTI Feed**: Processed MISP events are provided to GEIGER via its API.
- **Threat Prioritization Process**: Using VCDB data, threats are prioritized for different types of SMEs (digitally dependent, digitally-based, and digital enablers) using an exponential smoothing algorithm.
- **Automated Threat Prioritization**: This process classifies threats relevant to SME users and updates threat prioritization and countermeasures periodically, eliminating the need for a security expert.

These **results** highlight the effectiveness of the proposed prototype in addressing the specific CTI needs of SMEs, especially those with limited digital maturity or cybersecurity expertise. The study demonstrates a practical approach to making CTI accessible and manageable for SMEs, enhancing their ability to respond to cyber threats proactively.

Overview of MISP: Methodologies and Applications



Objective: To provide a comprehensive overview of the Malware Information Sharing Platform (MISP), focusing on its data format, sharing models, taxonomy structures, and synchronization protocols.

Methodology:

- **Data Format Analysis**: Examining the structure and format of event data in MISP.
- **Sharing Models**: Analyzing the various models for sharing information within MISP.
- **Taxonomy Analysis**: Investigating the triple tag structure used in MISP for categorizing information.
- **Synchronization Protocol Study**: Delving into the synchronization mechanisms within MISP, including the push and pull mechanism and the cherry-pick technique.

Application: The study's methodologies are applied to understand the operational aspects of MISP, a critical tool in cybersecurity for sharing malware information and intelligence.

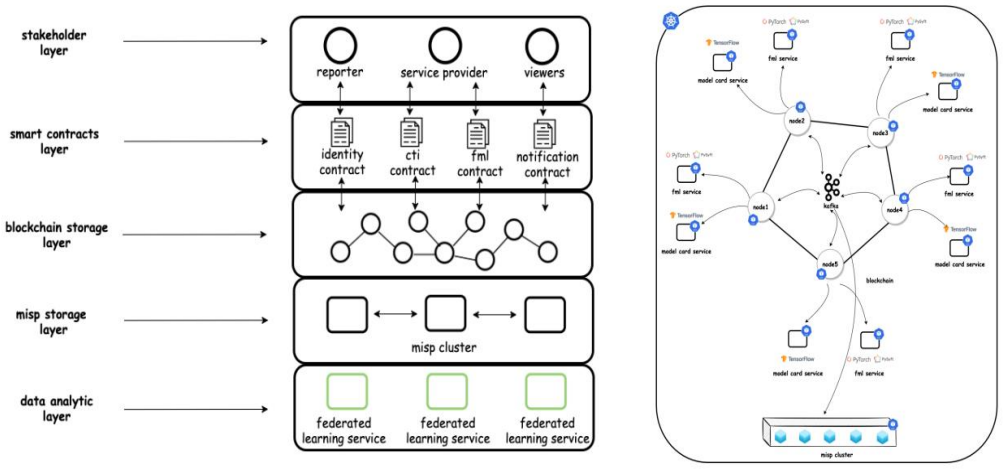
1. **Detailed Analysis**: In-depth insights into the data format, sharing models, taxonomies, and synchronization protocols of MISP.
2. **Usage Statistics**: Presentation of MISP usage data, showing a distribution of events per month from 2013 to 2016.
3. **Peak Usage**: A notable peak in published events was observed in 2015 and 2016, indicating increased utilization of MISP during these years.

LUUNU: Blockchain-Based CTI Sharing Platform

Objective: To present LUUNU, a novel CTI sharing platform that integrates blockchain technology, MISP, Model Cards, and Federated Learning (FL) to enhance transparency, credibility, and anonymity in CTI sharing.

Methodology:

1. **Platform Architecture**: Developing a five-layer architecture for LUUNU:**Stakeholder Layer**: Involving incident reporters/viewers and admins.
    - **Smart Contract Layer**: Storing digital identity proofs, CTI, FL, and notification contracts.
    - **Blockchain Storage Layer**: Containing nodes for each participating organization.
    - **MISP Layer**: Storing Model Card objects and facilitating interaction with blockchain smart contracts.
    - **Data Analytic Layer**: Providing FL services for cyberattack detection.
2. **Integration of Technologies**: Combining various technologies like Rahasak blockchain, Pytorch, Pysyft, TensorFlow Model C Toolkit, and Apache Kafka for different functionalities within LUUNU.



(a) Luunu platform layers. (b) Luunu platform blockchain ledger.

Figure 1: Luunu platform architecture.

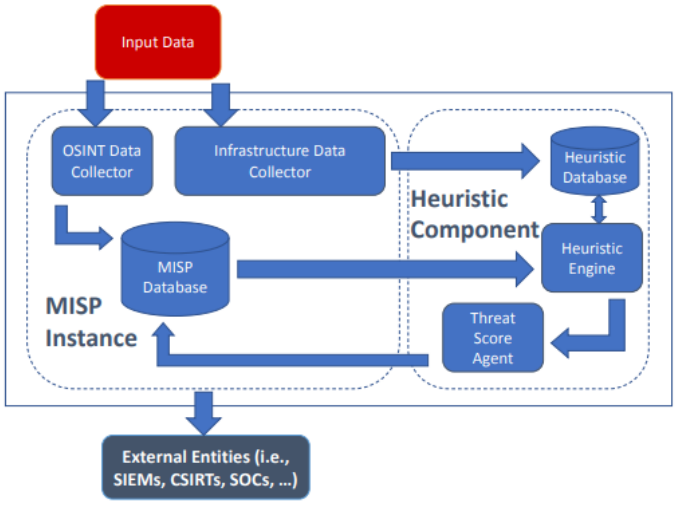
Application: LUUNU is used for registering organizations on the platform as blockchain nodes, enabling them to report incidents. These incidents are encoded into Model Card objects and saved in the MISP database. The platform utilizes Federated Learning (FL) models to detect cyberattacks and ensures the anonymity of reporting organizations through a self-sovereign identity-enabled mobile wallet.

Implementation Details: The platform is implemented on the Rahasak blockchain, with FL functions from Pytorch and Pysyft, Model Card service built with TensorFlow Model Card Toolkit, and blockchain operations managed by Apache Kafka.

Results

- **Enhanced CTI Sharing**: LUUNU provides a transparent and credible system for CTI sharing, leveraging blockchain technology and Model Cards.
- **Anonymity and Security**: The platform ensures the anonymity of organizations reporting CTI data, enhancing security and trust.
- **Effective Incident Reporting and Analysis**: The multi-layered architecture allows for efficient incident reporting and analysis using advanced technologies like FL and blockchain.

Enriched Threat Intelligence Platform (ETIP)



Objective: To introduce ETIP, a platform designed to collect, relate, and aggregate Open Source Intelligence (OSINT) data and data from monitored infrastructure, enhancing the functionality and efficiency of Intrusion Detection Systems (IDS) and Security Information and Event Management (SIEM) tools.

Methodology:

1. **Platform Architecture**: ETIP consists of two main modules:
   - **Composed IoC Module**: Collects and interrelates Indicators of Compromise (IoCs) to enrich them.
   - **Context-Aware Intelligence Sharing Module**: Contains a MISP instance and a heuristic component for further data analysis.
2. **Data Storage and Integration**:
   - OSINT data are stored in the MISP database.
   - Infrastructure data are stored in the Heuristic Component database.
   - MISP was selected for its integration capabilities with SIEM and IDS tools.

Application:

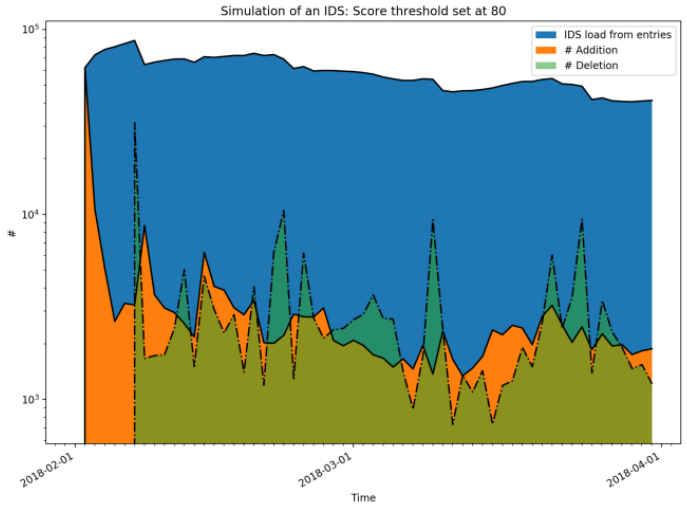
- ETIP's primary function is to feed enriched data to IDS or SIEM systems.
- The heuristic component processes data from MISP to produce a Threat Score (TS) for the received data, using a Weighted Mean (WM) function based on criteria like relevance, accuracy, variety, and timeliness.
- The TS helps in determining the risk score for potential threats in IDS and SIEM tools.

Integration with Existing Tools: ETIP's compatibility and integration with existing IDS and SIEM tools demonstrate its practical applicability in real-world cybersecurity environments.

Results

•**Enhanced Threat Intelligence**: ETIP successfully enriches IoCs by interrelating them and evaluating their threat score.
•**Effective Risk Assessment**: The platform aids analysts in determining the risk score of potential threats, enhancing the effectiveness of IDS and SIEM tools.
•**Weighted Threat Scoring**: The use of a weighted mean function for computing the Threat Score, considering various criteria, provides a nuanced and accurate assessment of potential threats.

Data Interaction and Scoring in MISP



Scoring Models: Two models for calculating the score were considered – one with exponential digression and another with a polynomial function. The polynomial function was found to be more advantageous.

Objective: The paper aims to describe the methods of data interaction used in MISP (Malware Information Sharing Platform) for evaluating exchanged information and proposes a novel scoring technique for decaying information.

Methodology:

- **Use of Taxonomies**: Employing taxonomies in MISP, a classification method with its own vocabulary, as part of the scoring model through tagging.
- **Data Interaction Method - Sightings**: Sightings in MISP provide information about the validity of an attribute, categorizing it into priority or decaying attributes.
- **Scoring Model Parameters**:
  - Base score calculation of an attribute using weighted applied tags and source confidence.
  - Consideration of the time difference between the current time and the attribute's last sighting.
  - Decay rate, indicating the speed at which the attribute's score decreases.

Application: The application of this methodology is to enhance the accuracy and relevance of threat intelligence in MISP by implementing a dynamic scoring system for attributes based on their decay over time.

Integrating Security Playbooks into MISP

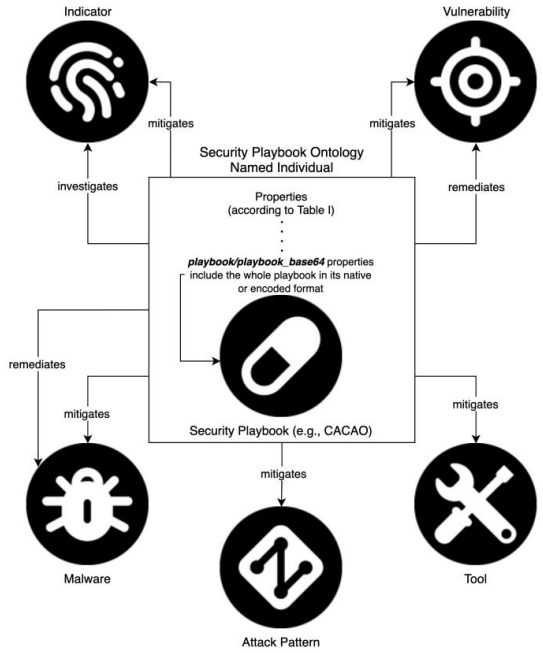


Fig. 4. Example illustration of TAC security playbook individual and its semantic relationships as specified on the STIX 2.1 standard.

Objective: The paper introduces a metadata template designed to integrate security playbooks, specifically the Collaborative Automated Course of Action Operations (CACAO) playbook, into the MISP threat intelligence platform, along with the development of a cyber threat intelligence ontology named Threat Actor Context (TAC).

Methodology:

- **Metadata Template Creation**: Developing a metadata template to map the metadata of CACAO playbooks, including elements like ID, description, impact, and severity.
- **Integration with MISP (Malware Information Sharing Platform):**
  1. Enhances the ability of organizations to collect, store, process, analyze, and share actionable information.
  2. MISP serves as a core format for representing threat information and ensuring interoperability.
  3. Features a structured format for objects that represent complex structures and link attributes.
  4. Utilizes a security playbook object template for creating shareable MISP security playbook objects .
- **Threat Actor Context (TAC) Ontology:**
  1. An open-source, modular knowledge representation framework developed by the OASIS Threat Actor Context Technical Committee.
  2. Captures the context around adversaries in a structured, machine-readable format.
  3. Integrates with the security playbook ontology to improve context around adversaries and relevant security playbooks.
  4. Can be used to create a searchable knowledge base of security playbooks .

Results

- **Effective Integration of Playbooks**: Successful integration of CACAO playbooks into MISP using the newly created metadata template.
- **Creation of MISP Security Playbook Object**: Establishment of a new object in MISP that describes the measures for responding to an attack, enhancing the platform's functionality.

Application:

- The application involves integrating CACAO playbooks, which consist of actions for cyberdefense functions like threat hunting or attack emulation, into shareable threat intelligence on MISP.
- The CACAO playbooks are represented in JSON format and can be digitally signed for authentication.

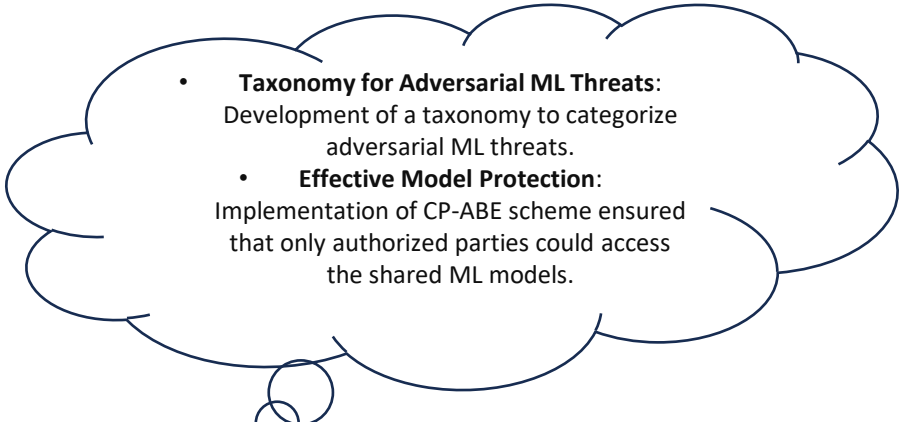
ML Models for Threat Detection and Cryptographic Protection

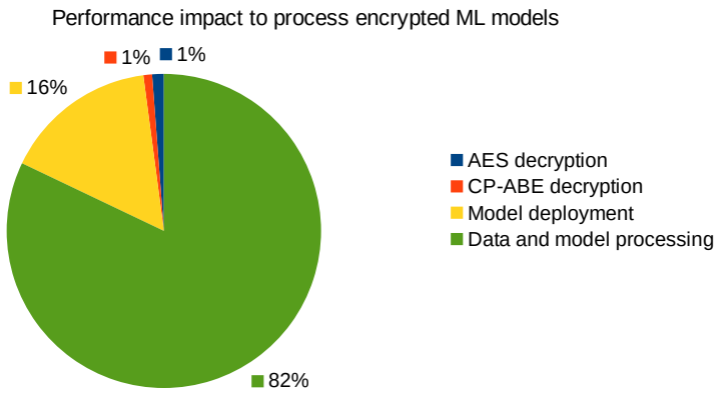
Objective: The paper proposes a solution for sharing ML models for threat detection within a community, ensuring their protection through a cryptographic scheme to restrict access to authorized parties.

Methodology:

- **Framework for Sharing ML Models:**
  1. A framework is developed for sharing ML models for threat detection, operating atop the mentioned CTI platforms.
  2. The framework includes a threat taxonomy to annotate ML models and artifacts, indicating the presence of adversarial ML threats .
- **Cryptographic Scheme Implementation**: Enforcing a Ciphertext-Policy Attribute-Based Encryption (CP-ABE) scheme for securing the data on the MISP database.
- **ML Model Sharing**: Utilizing a MISP object template for sharing ML models within the community.
- **Use of Python-Based Frameworks:** The implementation leverages Python-based frameworks like Scikit-Learn for traditional ML models and TensorFlow 2 and Keras for deep learning-based models .

Application: The application involves testing different ML models, including Decision Tree Classifier, Random Forest Classifier, OneClassSVM, Multi-Layer Perceptron (MLP), and autoencoders, to determine their effectiveness in identifying malicious traffic, particularly in scenarios involving modified HTTP payloads.





Results

Model Performance Analysis:

- Decision Tree Classifier showed almost perfect classification but failed with modified HTTP payloads.
- Random Forest Classifier improved performance but still misclassified modified HTTP payloads.
- OneClassSVM didn't perform as well as the first two but correctly identified modified HTTP payloads as malicious.
- MLP binary classifier exhibited excellent performance and correctly classified modified HTTP payloads.
- Autoencoders, trained unsupervised on benign traffic, successfully identified modified HTTP payloads as malicious.

Analysis of CTI Formats, Languages, and Sources

Objective: The paper aims to investigate the various formats, languages, and sources of threat feeds in CTI, assessing their suitability for different security-related use cases.

Methodology:

- **CTI Source Examination**: Analyzing CTI sources based on their origin (internally sourced like system logs, externally sourced observables, and open-source intelligence).
- **Focus on CTI Standards**: Investigating CTI standards used for representation, such as STIX, CybOX, CVRF, and MISP, as well as application/vendor-specific formats and legacy formats.
- **Analysis of CTI Source Feeds**:
  - Examining the originality of CTI sources (original vs. retransmitted).
  - Assessing the range of CTI types (e.g., IP, URL, domain) in the source feeds.
  - Defining rich CTI (with more than two types in the feed) and sparse CTI.

Application: The study's application involves evaluating the efficiency of various CTI formats and languages in different use cases like Email Blocklists, Spam filters, Network IDS (NIDS), or malware analysis.

electronics

MDPI

Article

A Comparative Analysis of Cyber-Threat Intelligence Sources, Formats and Languages

Andrew Ramsdale [1], Stavros Shiaeles [2,*] and Nicholas Kolokotronis [3]

[1] School of Computing, Electronics and Mathematics, Faculty of Science and Engineering, Plymouth University, Plymouth PL4 8AA, UK; andrew.ramsdale@postgrad.plymouth.ac.uk
[2] School of Computing, Faculty of Technology, University of Portsmouth, Portsmouth PO1 2UP, UK
[3] School of Economics and Technology, Faculty of Informatics and Telecommunications, University of Peloponnese, 22131 Tripolis, Greece; nkolok@uop.gr
* Correspondence: stavros.shiaeles@port.ac.uk

Received: 5 April 2020; Accepted: 13 May 2020; Published: 16 May 2020

check for updates

Abstract: The sharing of cyber-threat intelligence is an essential part of multi-layered tools used to protect systems and organisations from various threats. Structured standards, such as STIX, TAXII and CybOX, were introduced to provide a common means of sharing cyber-threat intelligence and have been subsequently much-heralded as the de facto industry standards. In this paper, we investigate the landscape of the available formats and languages, along with the publicly available sources of threat feeds, how these are implemented and their suitability for providing rich cyber-threat intelligence. We also analyse at a sample of cyber-threat intelligence feeds, the type of data they provide and the issues found in aggregating and sharing the data. Moreover, the type of data supported by various formats and languages is correlated with the data needs for several use cases related to typical security operations. The main conclusions drawn by our analysis suggest that many of the standards have a poor level of adoption and implementation, with providers opting for custom or traditional simple formats.

Keywords: cyber-threat intelligence; threat exchange; vulnerability alerts; incident reporting; indicators of compromise; cyber-observables

1. Introduction

With the advent of the *Internet of things* (IoT), there has been an unprecedented increase of cyber-attacks, which have evolved and become more sophisticated. Adversaries now use a vast set of tools and tactics to attack their victims with their motivations ranging from intelligence collection to data destruction or financial gain. Understanding the attacker has become more complicated and even more important as this knowledge, if transformed into actionable information, can be used to adapt networks' defences in an automated manner to better protect the network against possible threats. *Cyber-threat intelligence* (CTI) focuses on the capabilities, motivations and goals of an adversary and how these could be achieved. Intelligence is the information and knowledge gained about an adversary through observation and analysis; intelligence is not just data, but the outcome of an analysis and must be actionable to meet the needs of current defensive systems that have to deal with and respond to cyber-attacks. Amongst others, examples of CTI include indicators (system artefacts or observables associated with an attack), security alerts, incident reports and threat intelligence, along with any other relevant information on recommended (or vulnerable) security tool configurations [1,2].

The efficient sharing of CTI is at the core of cyber-threat detection and prevention, as it allows building multi-layer automated tools with sophisticated and effective defensive capabilities that continuously analyse the vast amounts of the heterogeneous CTI related to attackers' *tactics, techniques*

Results

- **CTI Source Feed Findings**: Only half of the examined feeds contained rich CTI.
- **Diversity in CTI Formats and Languages**: A wide range of CTI formats and languages were identified, each with varying degrees of efficiency for different use cases.
- **Use Case Suitability**: The study provides insights into which CTI formats and languages are most efficient for specific security use cases.

Identifying Polymorphic Threat Actors

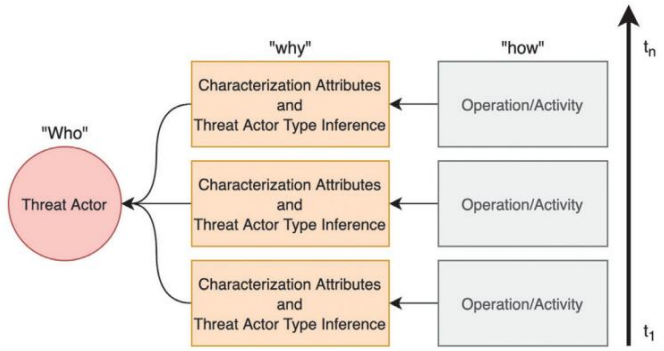
Objective: The paper aims to address the challenge of identifying changes in threat actors' behaviors and the polymorphism in their actions over time, particularly when obfuscation techniques hinder the association of events with specific threat groups.

Methodology:

- **Ontological Representation of TAL**: Utilizing a proof-of-concept ontological representation of the Threat Agent Library (TAL) to identify threat actor types from CTI objects.
- **Refinement of Threat Actor Knowledge Bases**: Presenting several threat actor knowledge bases and demonstrating the need for a more structured and automatic way to query them.
- **Domain Ontology Creation**: Developing a domain ontology for threat actor profiling to remove ambiguities and enhance clarity in identifying threat actors.

Application: The application involves using the domain ontology to categorize threat actor types, such as HostileThreatActorType or NonHostileThreatActorType, and to clarify motivations and objectives of threat actors.

FIGURE 1: SEMANTIC MODELING OF THREAT ACTOR POLYMORPHISM



Results

•**Enhanced Threat Actor Identification**: The ontological approach successfully refines the identification of threat actor types, reducing ambiguities.
•**Case Study - Lazarus Group**: The Lazarus Group case study illustrates how the ontology can automatically identify a polymorphic group exhibiting diverse behaviors (e.g., organized cybercrime, hacktivism, cyber vandalism).
•**Effective Characterization of Attacks**: By characterizing attacks like the DarkSeoul attack using the proposed domain ontology, the study revealed the Lazarus Group as the perpetrator, showcasing the ontology's effectiveness in identifying complex threat actors.

Criteria for Evaluating Threat Intelligence Platforms

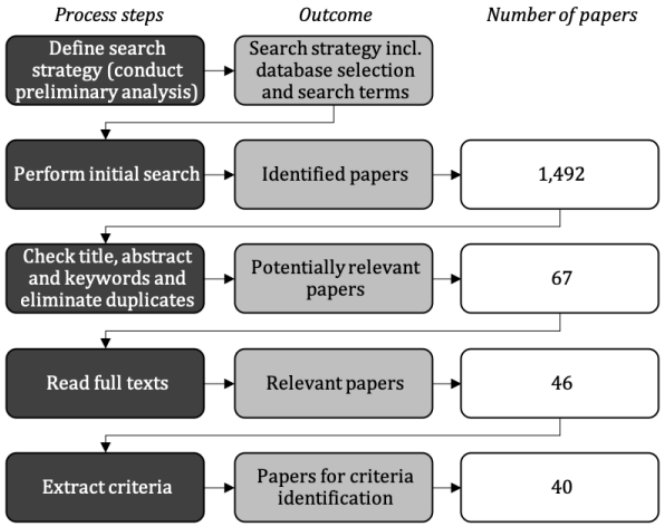


Figure 1. Systematic literature review process.

Objective: The paper's goal is to establish criteria for evaluating various Threat Intelligence Platforms (TIPs) by conducting a literature review and analyzing studies related to threat intelligence sharing (TIS) and TIPs.

Methodology:

- **Literature Review**: Gathering 40 relevant papers to extract criteria for TIP evaluation.
- **Criteria Extraction**: Identifying a set of 62 criteria, grouped into functional and non-functional categories.

Functional Criteria:

- **Phases of TIS**: Collection, Aggregation, Analysis, and Dissemination of Threat Intelligence (TI), each with subphases, available functions, and degrees of automation.
- **Cross-Phase Support**: Including Information Security, Data Privacy, Data Quality, Trust, Import and Export, Collaboration (Anonymity Levels), Reporting, and Additional Functions.

Non-Functional Criteria:

- **Architecture and Interfaces**: Type of Platform, Architecture, APIs, User Interface.
- **Content and Standardization**: Data Origin, Threat Intelligence and Standardization.
- **Provider and Users**: Usage Fees, License, Geographical Focus, Sectoral Focus.

Application: The application of this framework involved testing ten TISPs, with detailed analysis of three platforms: MISP, OTX, and ThreatQ.

Commonalities Across Platforms: All tested platforms provide collection, aggregation, and dissemination of TI and use standards like STIX, TAXII, and OpenIOC.

Differences in Data Quality and Reporting: Only OTX offers comprehensive reporting and individualization.

Focus Variations: MISP focuses on IoCs, while OTX and ThreatQ focus on TTPs (Tactics, Techniques, and Procedures).

Framework for Evaluating Trust in CTI Sources

Objective: The paper presents a framework designed to evaluate the trustworthiness and quality of CTI sources, based on a closed-world assumption.

Methodology:

- **Closed-World Assumption**: Operating under the assumption that the information provided by a specific set of CTI sources represents all existing information in the world of CTI.
- **Quantitative Evaluation Parameters**: Defining and computing parameters like Extensiveness, Maintenance, False Positives, Verifiability, Intelligence, Interoperability, Compliance, Timeliness, Completeness, and Similarity.
- **Trust-Based Quality Indicator**: Developing a trust indicator (TI) for each intelligence source, based on the weighted sum of the respective parameters and recalculated at specific intervals.

Application: The application involves using the framework to assess the quality of each CTI source within the worldview, with recalculations of the trust indicator at intervals dependent on the rate of parameter value changes and the specific needs of the use case.

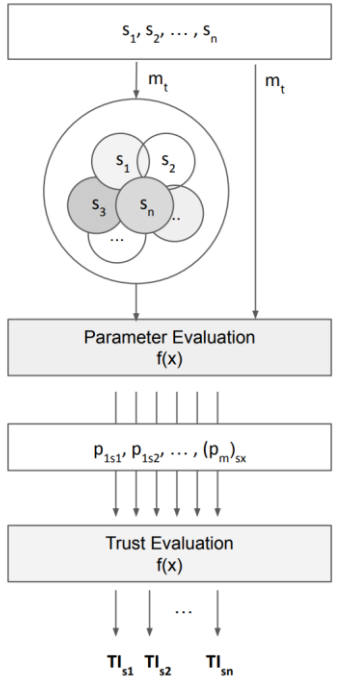


Figure 1: Methodology for CTI evaluation.

Trust Indicator Calculation: Illustration of the trust indicator calculation through an example involving the Extensiveness quality indicator, using three STIX messages from MISP as a data sample.

Dynamic Trust Evaluation: The framework allows for dynamic re-evaluation of trust parameters each time new CTI is shared, adapting to the evolving nature of CTI sources.

Practical Use Case Adaptability: The selection of the time interval for recalculating the trust indicator is flexible, catering to the specific needs and dynamics of different use cases.

ORISHA: Orchestrated Information Sharing and Awareness Platform

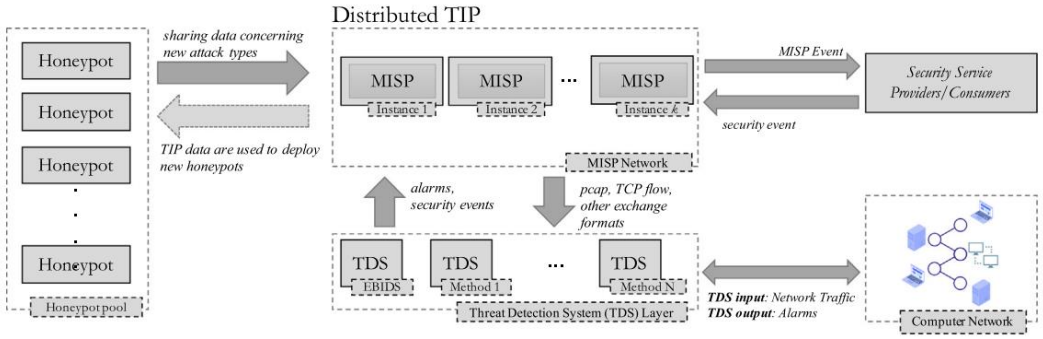


Fig. 1. ORISHA platform.

Objective: The paper introduces ORISHA, a platform designed to enhance detection accuracy for Threat Detection Systems (TDS) and facilitate reliable threat detection information sharing among organizations with different TDSs.

Methodology:

- **Distributed TIP**: Utilizing a network of several MISP instances for data storage and distribution.
- **TDS Layer**: Incorporating ensemble-based IDS (EBIDS), a machine learning-based intrusion detection method for classifying network flows.
- **Honeynet Layer**: A component of the platform aimed at further enhancing threat detection.
- **Query-By-Committee (QbC) Strategy**: Implementing a cooperative and active learning approach among TDSs to improve detection capabilities.

Application: The application involves using ORISHA for dynamic interaction between TDSs. For example, if TDS1 detects an anomaly, it triggers a MISP security event, which is then analyzed and potentially re-evaluated by TDS2, enhancing the overall accuracy of threat detection.

Enhanced Collaboration: The platform demonstrated the effectiveness of collaborative threat detection and information sharing among different TDSs.

Performance Metrics: The performance of classification models was measured using metrics like AUC, AUC-PR, and F-measure.

Improved Detection Accuracy: Experimental results showed a significant improvement in detection accuracy due to the implementation of ORISHA.

Layered Model for CTII Interoperability Challenges

Objective: The paper proposes a layered model aimed at addressing the various interoperability challenges organizations face when sharing CTII.

Methodology:

- **Four Interoperability Layers**: Identifying and addressing different aspects of interoperability in CTII sharing.
- **Legal Interoperability**: Covers legal restrictions and data privacy impacts during sharing.
- **Policy and Procedures**: Formal statements of organizational objectives and instructions for achieving them.
- **Semantic and Syntactic Interoperability**: Concerns different data types and standards in CTII, like STIX, MISP, CAPEC, MAEC, IODEFv2, and IDMEF.
- **Technical Interoperability**: Involves protocols for CTII transmission and information protection during sharing.

Application: Conducting an analysis of various CTII sources with respect to these interoperability layers, focusing on semantic and syntactic standards as well as policies.

Figure 2. The 5 Ws and 1 H of CIE policy.

Format Preferences: 50% of sources preferred the JSON format, while 59% and 31% chose plaintext and CSV, respectively.

Standard Usage: A small percentage opted for CTII-oriented standards like MISP, with most sources providing information in generic formats.

Policy Transparency: Only 15 out of 32 sources provided open and public information regarding their policies.

Evaluation Methodology for Threat Intelligence Standards and Platforms

Objective: The paper presents a methodology for evaluating threat intelligence standards and platforms, focusing on the most popular free and open-source options.

Methodology:

- **Selection Criteria**: Excluding standards and platforms that do not cover two or more stages of the threat intelligence production process flow.
- **Holistic Architecture Model**: Utilizing the 5W3H (what, who, why, when, where, how, how much, how long) method, with additional entities like Threat, Incident, Threat Actor, and Defense.
- **Standards and Platforms Analysis**: Evaluating based on popularity, applicability in different use cases, and processual criteria.

Standards Evaluated: STIX, TAXII, IODEF, RID, CybOX, and OpenIOC.

Platforms Evaluated: MISP, CIF, CRITs, OpenCTI, and Anomali STAXX.

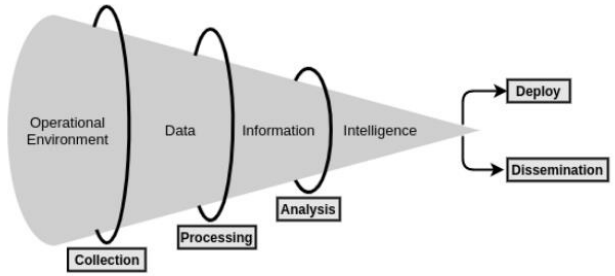


Figure 1. Threat Intelligence Production Process Flow.

Table 1. Description of the 5W3H method.

Question	Description
What	Directly describes the topic being addressed
Where	Specifies geographic references about the topic
When	Specifies relevant time frames to the topic like date and time
Who	Associates the topic with an entity capable of executing it
Why	Describes possible motivations for the occurrence of the topic
How	Describes the main characteristics and mechanisms of the topic
How much	Refers to the costs and impacts generated by the topic
How long	Description of the topic's effectiveness in terms of time

Best Standards: STIX, combined with TAXII, was identified as the best choice based on the holistic architecture and applicability.

Top Platforms: MISP and OpenCTI emerged as the most complete platforms, excelling in aspects like collection process, correlation and classification mechanisms, visualization, and integration with other security tools.

Conclusion & Future Work

Trends and Future Directions in Cyber Threat Intelligence

Key Trends

Automation and AI: Increasing use of automation and AI for faster and more accurate data processing, analysis, and threat detection.

Contextual Threat Intelligence: Enhancing CTI relevance and effectiveness by considering industry-specific risks, geopolitical events, and organizational infrastructure.

Dark Web Monitoring: Essential for understanding cybercriminal activities and staying ahead of emerging threats through intelligence sharing.

Threat Actor Attribution: Growing interest in accurately attributing cyberattacks to specific actors or groups to understand motives and tailor responses.

Emerging Research Directions

Regulatory Compliance: Using CTI for compliance with data protection regulations like GDPR and CCPA, ensuring data safety and legal adherence.

Machine-Readable Threat Intelligence (MRTI): Adoption of standardized formats for easier sharing, integration, and automation across security tools.

Edge and Remote Workforce Focus: Adapting CTI to address security challenges in edge services and remote work environments.

Conclusions

The continuous evolution of cyber threats necessitates adaptable and proactive countermeasures. This paper's focus on CTI mechanisms highlights the importance of evolving strategies and technologies in cybersecurity.

Thank you for your attention!

This project has received funding from the European Union's Horizon 2020 research and innovation programme under grant agreement No 101070450 (AI4CYBER) .