Ref. Ares(2023)3025723 - 28/04/2023

DELIVERABLE

D3.8 State of the art in information sharing mechanisms in the context of ICTs

Project Acronym:	LAZARUS	
Project title:	pLatform for Analysis of Resilient and secUre Software	
Grant Agreement No.	101070303	
Website:	https://lazarus-he.eu/	
Contact:	info@lazarus-he.eu	
Version:	1.0	
Date:	28/04/2023	
Responsible Partner:	DC	
Contributing Partners:	DC, ARC, UCM, UNIPD, DC, LIST, BNR, APWG, MAG	
Reviewers:	Constantinos Patsakis (ARC) Miltiadis Anastasiadis (MOT)	
Dissemination Level:	Public	X
	Confidential – only consortium members and European Commission Services	

This project has received financial support from the European Union Horizon 2020 Programme under grant agreement no. 101070303.

Revision History

Revision	Date	Author	Organisation	Description
0.1	17/02/2023	George Pantis, Nikolaos Lykousas	DC	Initial draft
0.2	22/02/2023	George Pantis, Nikolaos Lykousas	DC	First contributions
0.3	10/03/2023	Multiple authors	DC, ARC, UCM, UNIPD, DC, LIST, BNR, APWG, MAG	First partner contributions
0.4	21/03/2023	George Pantis, Nikolaos Lykousas	DC	Restructure sections and work on ontologies
0.5	31/03/2023	Multiple authors	DC, ARC, UCM, UNIPD, DC, LIST, BNR, APWG, MAG	Final partner contributions
0.6	14/04/2023	Multiple authors	DC, ARC, UCM, UNIPD, DC, LIST, BNR, APWG, MAG	Draft for review
0.7	21/04/2023	C.Patsakis, M. Anastasiadis	ARC, MOT	Review Comments
1.0	28/04/2023	Nikolaos Lykousas	DC	Final version

Every effort has been made to ensure that all statements and information contained herein are accurate, however the LAZARUS Project Partners accept no liability for any error or omission in the same.

Table of Contents

List of Tables

List of Figures

1 Executive Summary

This deliverable aims to explore the current state-of-the-art of best practices, standards, and mechanisms for effective data sharing among stakeholders within the cybersecurity landscape, specifically focusing on the requirements of the LAZARUS project. As cyber threats continue to evolve, the need for efficient collaboration and rapid mitigation strategies becomes increasingly crucial. This report aims to facilitate the enhancement of collaboration between Computer Emergency Response Teams (CERTs) and Computer Security Incident Response Teams (CSIRTs) to create a robust cybersecurity framework.

2 Introduction

The rapid growth of digital technology and the increasing interconnectedness of systems have led to an escalation in the complexity and frequency of cyber threats. To effectively address these challenges, organisations need to collaborate and share relevant information related to vulnerabilities, threats, and incident response. The importance of collaboration and information sharing is particularly evident in the context of Computer Emergency Response Teams (CERTs) and Computer Security Incident Response Teams (CSIRTs), whose primary role is to detect, analyse, and respond to security incidents. In the context of the LAZARUS project, which aims to address security issues throughout the software development lifecycle (SDLC) by leveraging advanced machine learning and artificial intelligence techniques, information sharing is a critical component for creating a more secure and resilient digital ecosystem.

This deliverable presents an overview of the current techniques, standards, and mechanisms for cybersecurity information sharing in the context of Information and Communication Technologies (ICTs). The goal is to provide a comprehensive understanding of existing models and systems for enhancing collaboration between stakeholders and enabling faster mitigation mechanisms in different setups and contexts.

The following sections cover various aspects of cyber information sharing, including central concepts and organisation (2.1), characteristics of cyber information sharing models (2.2), sharing technologies for cybersecurity information (2.4), shared situational awareness (2.5), and cyber threat intelligence (3). We also delve into the role of ontologies (4) in standardising and facilitating the exchange of cybersecurity information.

Concretely, this report is organised as follows:

- Core Concepts
    - This section provides an overview of the central concepts presented in this report. It introduces the key components and structures that facilitate the exchange of threat intelligence and incident response information among organisations, CERTs, and CSIRTs.
- Characteristics of Cyber Information Sharing Models
    - In this section, we analyse the fundamental aspects of cyber information sharing models, including what information to share, with whom to share, why to share, and the main challenges associated with threat information sharing. We also discuss various sharing architectures, methods, exchange methods, and mechanisms of sharing.
- Sharing Technologies for Cyber Security Information
    - This section examines the different technologies and methodologies used for sharing cybersecurity information, focusing on the interactions between CERTs/CSIRTs and law enforcement agencies. We provide an overview of the most commonly used tools and platforms that enable effective information exchange.
- Shared Situational Awareness
    - In this section, we discuss the concept of shared situational awareness and its importance in enhancing the collaboration between different stakeholders in the cybersecurity ecosystem. We explore how shared situational awareness enables organisations to better understand and respond to emerging threats and vulnerabilities.
- Cyber Threat Intelligence
    - This section delves into the domain of cyber threat intelligence, covering various aspects such as security vocabularies, cyber threat intelligence formats, sharing and analysis platforms, and actionable cyber threat intelligence. The aim is to provide a comprehensive understanding of how organisations can effectively utilise and share threat intelligence to enhance their security posture.
- Ontology

- Finally, we explore the role of ontologies in the context of cybersecurity information sharing. We present an overview of related work and discuss the Unified Cyber Ontology (UCO) and the Cyber-investigation Analysis Standard Expression (CASE) as examples of ontologies that facilitate standardised information exchange and collaboration in the cybersecurity domain.

2.1 Central concepts

• Alert and detection system: An alert and detection system generates information that can warn other parties about a detected threat and improve the detection process. Customers have the ability to specify the type of data that the system handles, and the data ownership remains within the company on its devices. By offering insights into the organisation's own and overall information security state, the system's situation awareness information enhances comprehension.

• Computer Security Incident Response Team (CSIRT) or Computer Emergency Response Team (CERT): The term "incident response services" refers to organisations that offer preventive measures, such as security management alerts or advisories, to victims of attacks. These organisations can be governmental, academic, or private bodies with the ability to respond to incidents [1]. In 2012, the EU Computer Emergency Response Team (CERT-EU) was established to respond promptly and effectively to information security incidents and cyber threats, specifically for EU institutions, agencies, and bodies.

• Critical Infrastructure Protection (CIP): Critical infrastructure (CI) refers to the essential physical facilities, electronic services, and functions required for society's basic operations. These include energy production, transmission, and distribution networks, ICT systems and services (such as mass communication), financial services, transportation and logistics, water supply, infrastructure construction and maintenance, and waste management in specific situations. A smart grid that enables two-way energy and communication flows is being developed to replace the country's outdated power system [2]. This intelligent network will combine information and communication technologies with power delivery infrastructure.

• Critical Information Infrastructure Protection (CIIP): The term "Critical Information Infrastructure" refers to any information system, whether physical or virtual, that manages, manipulates, transfers, receives, or stores electronic data, voice or video, which is essential for the operations of critical infrastructure. These interconnected networks and systems are crucial, and their disruption or destruction would severely impact the health, safety, security, economic well-being of citizens, as well as the effective operation of the government or economy [3].

• Cyber Threats in Critical Infrastructure: Cyber threats encompass various types of attacks, such as denial of service (DoS), unauthorised vulnerability probes, botnet command and control, data exfiltration, deliberate data corruption, or even physical destruction caused by the modification of critical software or data. These threats can be facilitated by malware, social engineering, or highly sophisticated advanced persistent threats (APTs), which can be targeted and prolonged. Channel jamming is considered one of the most effective methods for initiating physical-layer DoS attacks, especially for wireless communications [4].

• The European Union Agency for Network and Information Security (ENISA): ENISA serves as a hub for network and information security (NIS) expertise for the EU, its member states, the private sector, and European citizens. ENISA collaborates with these groups to develop advice and recommendations on best practices for information security. It aids EU member states in executing relevant EU legislation and strives to enhance the durability of Europe's critical information infrastructure and networks. ENISA proposes

suggestions on cybersecurity, provides support for policy development and implementation, and collaborates with other operational teams throughout Europe [5].

- National Regulatory Authority (NRA): NRA can assume various responsibilities in cybersecurity matters. In Finland, their responsibilities include managing and overseeing the activities of telecom operators, ensuring information security and preparedness, such as monitoring adherence to information security regulations, directing and overseeing robust electronic identification, and providing qualified certificates. They also monitor compliance and carry out yearly audits of certification authorities that issue qualified certificates [6].

- The European Cyber Security Organisation (ECSO): ECSO acts as the contractual partner of the European Commission in executing the Cyber Security contractual Public-Private Partnership. ECSO has a diverse membership that includes large corporations, small and medium-sized enterprises (SMEs), research centres, universities, end-users, operators, clusters, associations, and various European Member States' local, regional, and national administrations, as well as countries that are part of the European Economic Area and the European Free Trade Association and those associated with H2020 [7].

- Information Sharing and Analysis Centres (ISACs): ISAC is a collaborative community established to facilitate sector-specific national or international information sharing. These Information Sharing and Analysis Centres are reliable entities that encourage the exchange of information and best practices concerning physical and cyber threats and their mitigation. ISACs could assist with the implementation of new European legislation, such as the NIS Directive, or support economic interests [8].

- Information Sharing and Analysis Organisation (ISAO): An ISAO is an entity or collaboration established by public or private sector organisations to collect and analyse critical information related to cybersecurity. Its objective is to gain a better understanding of security issues and interdependencies among cyber systems to ensure their availability, integrity, and reliability. Unlike ISACs, ISAOs are not limited to specific sectors and can serve any community or industry. Membership in an ISAO does not require involvement in critical functions for society [9].

- Industrial Internet of Things (IIoT): IIoT involves the gathering of information from various connected devices, such as smart machines and tools, in factories or plants, and then utilising advanced software and networking technology to analyse this data. A complete IIoT setup requires a combination of hardware, software, and communication and networking technologies. The smart grid is a significant area in which IoT is involved in managing energy systems. Through IoT, the benefits of smart grid extend beyond the utilities' automation, distribution, and monitoring processes [10].

- Risk Assessment Framework (RAF): A RAF is a method used to rank and communicate information about security risks facing an IT organisation. NIST [11] defines risk assessments as a way to provide decision-makers with information and support risk responses by: a) identifying threats that are relevant to an organisation or threats that are directed through organisations to other organisations; b) identifying vulnerabilities, both internal and external, that an organisation faces; c) determining the potential impact on organisations that could occur if threats exploit vulnerabilities; and estimating the likelihood of harm. The outcome of these steps is a determination of risk.

- Risk Management Framework (RMF): RMF is a systematic and adaptable approach to handle security and privacy risks. It encompasses various stages such as categorising information security, choosing and

implementing controls, evaluating their effectiveness, granting system and common control authorizations, and conducting continuous monitoring [12].

- Standard ISO/IEC 27010:2015: ISO/IEC 27010:2015 is an important aspect of trusted information sharing, specifically for managing information security in inter-sector and interorganizational communications. It serves as a supporting entity, which refers to a trustworthy independent organisation designated by the information sharing community to facilitate their activities, such as offering a source anonymisation service [13].

- Tactics, Techniques, and Procedures (TTPs): The actions of an actor can be described by tactics, techniques, and procedures. Tactics provide an overall description of the behaviour, techniques offer more detailed explanations of the behaviour in the context of a tactic, and procedures provide highly specific and detailed descriptions of behaviour within the context of a technique [14].

- Threat Information: Threat information refers to any data that could assist an organisation in safeguarding itself against a threat or identifying the actions of an attacker. Indicators, TTPs, security alerts, threat intelligence reports, and tool configurations are some of the primary forms of threat information [14].

2.2 Characteristics of cyber information sharing models

The objective of sharing Cyber Threat Intelligence is to establish a system where practical cyber threat intelligence is automatically exchanged instantly to facilitate the real-time protection, detection, prevention, and reduction of cyber threats before or at the time they occur. The five problems that need to be addressed are:

1. What to share?
2. With whom to share?
3. Why to share?
4. What are the main challenges of threat information sharing?
5. How to share? (Sharing architectures; Sharing methods; Exchange methods; Mechanisms of sharing)

Below, these issues are addressed.

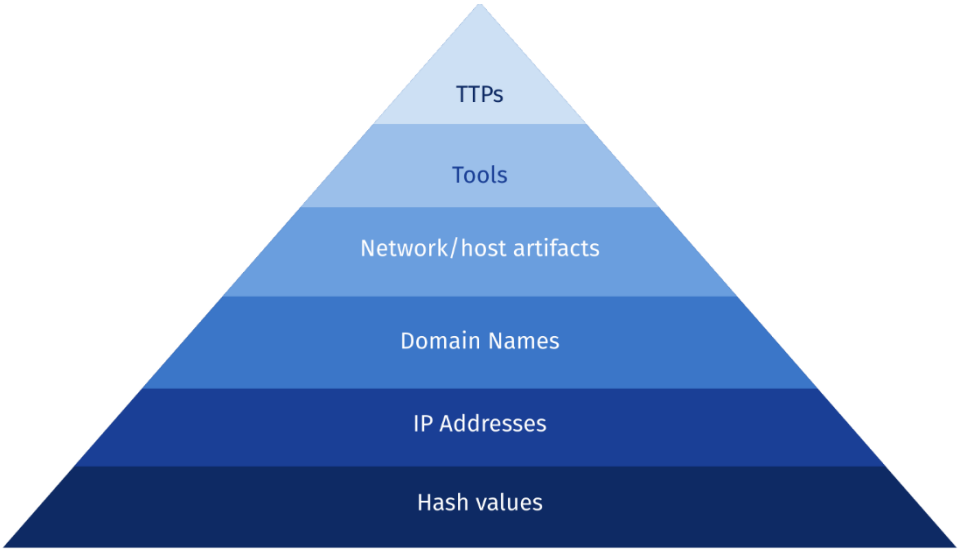
2.2.1 What to share?

Sharing cybersecurity-related information can enhance an organisation's cybersecurity defences and incident response. Munk [20] categorises this information into four groups: information regarding events, vulnerabilities, threats, and other information. Sedenberg and Dempsey [15] classify it as incidents (including attack methods), best practices, tactical indicators, vulnerabilities, and defensive measures. Specifically, organisations share tactical indicators, also known as "indicators of compromise" (IOCs), which are artefacts related to a specific security incident or attack, such as file names, IP addresses, hashes, hostnames, and other data. Cyber defenders may use IOCs to identify or prevent the compromise [15]. Overall, cyber threat information refers to any information concerning a threat (IOCs, TTPs, security alerts, etc.) that can aid an organisation in protecting itself from a threat or detecting potential or actual threat actors.

Indicators of Compromise (IoCs): IoCs refer to technical clues or events that suggest a potential attack or ongoing security breach. These may include unusual network activity, changes in system files or registry

settings, or anomalous user account behaviour. IoCs are typically specific and repeatable, and can be easily anonymized and standardised for efficient sharing among organisations. Common examples of IoCs include IP addresses, data strings, file hashes, and exploit payloads. Sharing IoCs can improve cybersecurity defences without risking the disclosure of sensitive data. Technical indicators make up the bulk of available threat information, and automated sharing can lead to significant benefits [16].

The figure below illustrates Bianco's "Pyramid of Pain"[1]. In essence, the pyramid illustrates the escalation of difficulty in collecting and denying IoCs. As a result, the pyramid represents a hierarchy of IOCs, with the most basic and easily changed indicators at the bottom and the most difficult to alter indicators at the top.



Security alerts: Security alerts are concise notifications that provide information about current security vulnerabilities, exploits, and other issues. They may be called bulletins, advisories, or vulnerability notes and are typically easy for humans to read and understand. These alerts can come from various sources, such as commercial security service providers, security researchers, CSIRTs, and SIRTs.

TTPs: TTPs, which stand for Tactics, Techniques, and Procedures, refer to the typical methods and strategies that an attacker employs, including their choice of malware, attack tools, or delivery mechanisms.

Tool configurations: Tool configurations refer to guidelines for configuring and utilising tools that facilitate the automated gathering, exchange, processing, analysis, and application of threat information. This information can provide instructions on the installation and use of utilities designed for detecting and removing rootkits or creating and adjusting intrusion detection signatures, firewall rules, router access control lists (ACLs), or web filter configuration files.

Threat intelligence reports: To enhance an organisation's situational awareness, threat intelligence reports are documents that typically detail TTPs used by actors, targeted systems and information types, and other relevant threat information. Threat intelligence refers to threat information that has undergone aggregation, transformation, analysis, interpretation, or enrichment to provide the necessary context for decision-making processes.

[1] https://detect-respond.blogspot.com/2013/03/the-pyramid-of-pain.html

2.2.2 With whom to share?

Organisations often share knowledge and experiences to enhance their defensive capabilities. The actors involved in this process include:

1. Governments and public safety organisations, who need to safeguard their classified and unclassified systems, combat cybercrime, and reduce cybersecurity risks.

2. Private critical infrastructure providers, who aim to protect critical infrastructure to ensure critical national interests like public health and defence.

3. Business enterprises, who have a vested interest in maintaining the security of sensitive information such as customer and supplier data, trade secrets, and contract information.

4. IT companies, who strive to safeguard the security and integrity of their products. They often share information on product or service vulnerabilities to enable security firms to create solutions to fix them, or they may release software updates that address vulnerabilities for their customers.

5. IT security firms, computer forensics experts, antivirus and antimalware vendors, and penetration testers, who collect and sell cybersecurity information.

6. Security researchers, who study cyber incidents and identify vulnerabilities in software, hardware, and services through academic work. They usually help mitigate threats and address weaknesses [17].

2.2.3 Why to share?

When an organisation experiences a cyber attack, it gains valuable information about cyber threats that can be beneficial to other organisations. By sharing this information, organisations can improve their own security measures as well as those of others. This exchange of information among private and public entities is an effective way to gain a comprehensive understanding of the constantly changing threat environment and learn about serious risks, vulnerabilities, and potential solutions.

There are several reasons why sharing this information is important:

1. Improved preventive functions: The development of a cyber-ecosystem requires a faster response against hybrid threats, such as those in the industrial sector. Sharing information in near real-time requires further development of sensor and signal techniques.

2. Enhanced threat understanding: Sharing threat information provides organisations with a better understanding of the threat environment and enables them to improve their cybersecurity and risk management practices. With shared information, organisations can identify affected systems or platforms, implement protective measures, enhance detection capabilities, and more effectively respond and recover from incidents based on observed changes in the current threat environment.

3. Knowledge improvement: Sharing and analysing seemingly unrelated observations from different organisations can enhance the value of information by developing knowledge of actor tactics, techniques, and procedures (TTPs) associated with a specific threat, incident, or campaign. Correlating indicators can provide valuable insights into the relationships between them, improving existing indicators and enriching the knowledge base.

4. Increased protection: organisations that act upon the threat information they receive can protect others who have not yet received or acted upon the information. By reducing the number of viable attack vectors, organisations can minimise vulnerability and increase protection.

5. Enhanced defensive agility: Threat actors constantly adapt their TTPs to avoid detection and exploit new vulnerabilities. organisations that share information are better informed about changing TTPs and can more rapidly detect and respond to threats, increasing their defensive agility.

6. Strengthen cyber defence: Since attackers often use similar methods to target different organisations, sharing information can help organisations improve their defence against cyber threats and make the most of their resources. This approach, in which one organisation's detection can prevent an attack on another organisation, is a modern and sophisticated concept that enhances the security of organisations in advance.

7. Increase awareness: Sharing information allows organisations to benefit from the collective knowledge, experiences, and analytical capabilities of their partners within a community of interest, thereby improving the defence capabilities of multiple organisations. Even a single contribution, such as a new indicator or observation about a threat actor, can increase the awareness and security of an entire community.

8. Foster trust: Repeated exchanges over time build trust and establish expectations that parties will consistently and reliably minimise harm and maximise protection.

2.2.4 What are the main challenges of threat information sharing?

1. Building trust: Trust is the foundation of information sharing, but it takes time and effort to establish and maintain. Regular communication, such as in-person meetings or phone calls, can help foster trusted relationships. Trust leads to confidence that shared information will be used appropriately and protected. Legislation can require incident reporting, but it doesn't increase trust or collaboration. A collaborative approach between private and public entities is necessary to address cybersecurity threats.

2. Ensuring interoperability: standardised data formats and transport protocols are crucial for interoperability, enabling secure and automated exchange of structured threat information between organisations, repositories, and tools. However, adopting specific formats and protocols can be time-consuming and costly, and the investment value may decrease if sharing partners require different formats or protocols.

3. Protecting sensitive but unclassified information: Sharing sensitive information such as trade secrets, intellectual property, or proprietary information can lead to financial loss, reputation damage, and violate sharing agreements. Unauthorised disclosure may disrupt ongoing investigations, future legal proceedings, or response actions. Organisations should implement policies, procedures, and technical controls to actively manage the risks of disclosing sensitive but unclassified information.

4. Protecting classified information: Government sources may mark information as classified, making it difficult for many organisations to use. organisations may also need to request and maintain clearances for ongoing access to classified information sources, which can be costly and time-consuming.

There are several reasons why some entities may hesitate to engage in sharing cyber threat information, such as concerns about potential legal liability that could arise from sharing such sensitive information with

other private organisations or the government. The legal complexities surrounding cyber information sharing are broad, including those related to sharing between private entities as well as within government agencies. Therefore, it is important to establish a legal framework for cyber information sharing that addresses questions about what information can be shared, with whom it can be shared, and for what purposes. Additionally, the broader scope and goals of cyber security legislation must also be carefully considered.

2.2.5 How to share?

2.2.5.1 Sharing architectures

Figure 1 shows the main groups of existing architectures and frameworks for cybersecurity information sharing within public organisations, which are currently limited in number. MITRE has classified information sharing models into three main categories, with a fourth model being a combination of the others [18].

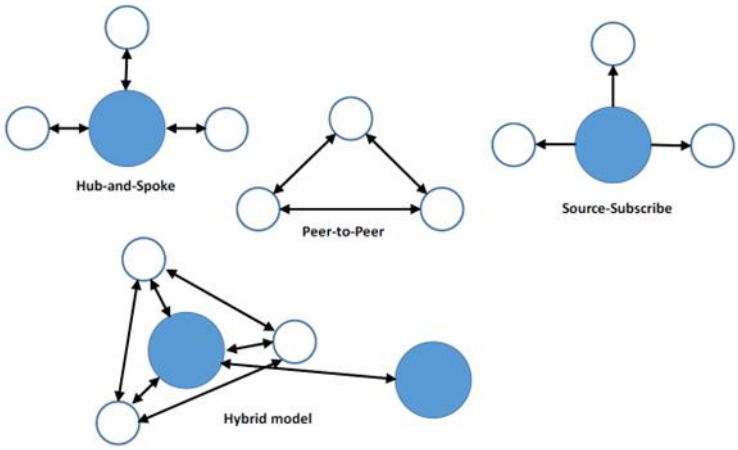


Figure 1 Traditional classification of information sharing models

- Hub-and-Spoke

The Hub-and-Spoke architecture is a model of information sharing in which a central hub collects data from member spokes and can distribute it to other members or add value through additional analysis or data. The hub serves as a clearinghouse, facilitating secure sharing of information while protecting member identities. Spokes can both contribute data to and access data from the hub [19].

Information Sharing and Analysis Centers (ISACs) are examples of private sector associations that utilize a hub-and-spoke model. These non-profit organisations serve as a central resource for collecting information on cyber threats, particularly for critical infrastructure, and allow for two-way sharing of information between the private and public sectors [19]. ISACs operate by having members from a specific industry or region share cyber threat data with centrally located analysts who then enrich and distribute intelligence back to the community [20].

The ISAC model enables businesses to share information about various security threats like malware attacks, phishing campaigns, system vulnerabilities, etc. to help each other prevent incidents from occurring. The information sharing is done anonymously to protect the reputation of the companies involved, and the communities typically have established rules in place to manage the dissemination of this information [21].

The Dutch National Detection Network (NDN) is an instance of a network that employs the hub-and-spoke model. It is an initiative aimed at achieving faster and more effective detection of digital threats and risks by sharing information about them. Through the sharing of threat intelligence, organisations can take timely and effective measures to limit or prevent damage caused by such threats. This helps them to better fulfil their responsibility to protect their own systems and assets [22].

The NDN focuses on two main groups: private companies in critical industries such as energy, water, and telecommunications, and various departments and agencies of the Dutch national government. To facilitate the exchange of technical threat information, NDN employs the MISP platform and a hub-spoke architecture. This centralised approach was chosen to prevent practical obstacles from hindering community uptake. Other organisations that use the hub and spoke model include national CERTs, DHS AIS, US-CERT, Electronic Crimes Taskforce (ECTF), FBI's e-guardian and ECS.

- Peer-to-peer

The model that allows any member of a community to share and interact with any other member, rather than going through a central hub, is called a decentralised model. According to the MITRE Corporation in [19], trust is crucial among members for the success of the model. Designing the information exchange to a specific mission creates an atmosphere of trust, as members share common threats and focus on the community's objectives. Trust is also strengthened through face-to-face meetings and individuals who have a long history of personal rapport. To maintain communication among existing members and facilitate the introduction of new members, the information-sharing model should develop vetting requirements and procedures. The security, speed, and convenience of these communication mechanisms will vary based on the organisation's mission and requirements [19].

Peer-to-peer networks can offer advantages for smaller groups or situations where members have limited interactions with the rest of the community. They may also be useful for groups with unequal trust relationships or where information sharing needs vary based on the content or current threats.

The ETIS CERT-SOC Telco Network is an example of a peer-to-peer sharing community. It was established by ETIS, a membership-based organisation that promotes collaboration among European telecom providers. The group is composed of security operations and incident response specialists from various member organisations, and it focuses on exchanging threat information and incident response experiences. The group uses the MISP platform to facilitate its automated threat exchange channels. Notably, large telecommunications companies such as Proximus, Kpn, Swisscom, and A1 Telekom Austria have joined the CERT-SOC Telco Network [23].

- Source-Subscriber

The model where a single entity shares information with a group of consumers is often used in commercial settings where a vendor provides information to subscribers who pay for access. This model is also used for free alerts provided by authoritative sources [18].

- Hybrid

One option for an information exchange is to use a peer-to-peer model to exchange intrusion indicators while sending incident-response data to a centralised hub for analysis. This approach enables the hub to analyse data from multiple organisations and produce analytic reports for everyone to use. Another option is for members of the information exchange to send the same data to each other and to a central hub [19].

A hybrid model can also refer to the use of multiple hubs at the EU level, which can strengthen national hubs. In this approach, a European hub would serve as the primary hub, but there would also be sub-hubs at the national level. Supranational organisations such as Interpol, which investigate crime, also require data for crime prevention. Thus, having only one centralised hub may become too difficult to manage.

2.2.5.2 Sharing methods

- Publish-subscribe

The method of sharing threat intelligence through publish-subscribe involves a producer who regularly or irregularly publishes information that can be subscribed to by one or more members of the community. This method can be used in both the peer-to-peer and hub-and-spoke sharing models. In a peer-to-peer network, a producer can automatically share cyber threat indicators into a repository that other members can access, or post alerts to a message board/forum that subscribers can receive. In a hub-and-spoke model, the publisher may be the hub and the members can submit their information to the hub for processing before it is published to the subscribers. This method allows for the aggregation and analysis of information in a central location, providing a more complete understanding of an incident or actor. This is particularly useful in a rapidly evolving environment where many participants are sharing different observations and analyses.

- Crowdsourcing

Crowdsourcing involves members collaborating to transform fragmented threat data into a more cohesive threat intelligence by contributing to a discussion thread, a cyber threat sharing repository, or another system. As members participate in crowdsourcing, the intelligence picture is shared among them. Crowdsourcing can occur in both peer-to-peer and hub-and-spoke networks, with the primary difference being the presence of a central party directing the crowdsourcing through the hub. In contrast, true organic collaboration among the community members characterises peer-to-peer networks. Both approaches can be highly effective. Crowdsourcing also fosters regular social interactions among members, building trust and strengthening the community.

2.2.5.3 Exchanges methods

There are various ways for organisations to share information, as mentioned by]Goodwin and Nicholas in [17]. These methods include formalised, security clearance-based, trust-based, and ad hoc. The method of exchange plays a crucial role in determining the participants and the scope of the program. It is therefore important to choose the appropriate method when designing an exchange to match the group's goals and membership.

- Formalised exchanges

A formalised exchange is an exchange based on an agreement, such as a legal contract, non-disclosure agreement, or a membership agreement. The agreement typically identifies the parties involved, outlines what information is to be exchanged, how it can be used, and how confidentiality will be protected. An example of a formalised exchange is the Microsoft Active Protections Program (MAPP), which brings together over 80 partners and provides security vulnerability information from the Microsoft Security Response Center (MSRC) to its members before monthly security updates. Another example is the Asia Pacific Computer Emergency Response Team, a membership-based organisation that fosters cooperation among over 30 CERTs in the Asia Pacific region. It is important to select the appropriate method of exchange when

designing an information exchange program as it will determine the actors that can be included and the scope of the program [17].

- Security clearance-based exchanges

According to the article [23], certain information exchange programs, particularly those that involve intelligence agencies, require exchanging classified or sensitive information through secure channels, often directly with a single entity. A security clearance-based exchange is a type of formalised exchange that is more restricted in scope and participation. The security clearance process can promote trust among participants over time. However, it can also limit the actors involved, such as restricting participation to those of a particular country, which can be challenging in a global market. Private sector participants can find it challenging and time-consuming to obtain security clearance, especially given the international workforce found in many large technology companies. Exchanges involving classified information are more likely to be successful when they involve defence contractors or other entities experienced in working with classified material [17].

- Trust-based exchanges

Groups based on trust are typically exclusive groups of cybersecurity professionals who share information on an as-needed basis when they detect security issues of mutual interest. These groups operate on the premise that trust is extended to unknown members through a series of trusted relationships with known members. Although they do not typically have formal contracts or agreements regarding information exchange, they may use systems like the Traffic Light Protocol (TLP), which employs a colour-coded system to indicate with whom information may be shared, reducing concerns about disclosure. Trust among members can be established and maintained in a variety of ways, ranging from simple nominations by current members to thorough vetting and verification processes. Trust is generally placed in individuals rather than in the organisations they represent, meaning that if an individual leaves an organisation, the organisation may not be able to nominate another representative to the group. Trust is developed among members based on their contributions, joint activities, and shared experiences [17].

- Ad hoc exchanges

Ad hoc or episodic information sharing is typically triggered by specific incidents or crises and is usually temporary in nature. It tends to be highly targeted and aims to address a particular set of issues. If it proves effective, it can serve as a basis for more structured and organised forms of information exchange [17].

2.2.5.4 Mechanisms of sharing

According to Goodwin and Nicholas [17], there are multiple mechanisms that can be leveraged for information exchange, depending on factors such as the type of information and the actors involved. It is important to consider the level of automation required and the format of the information when selecting the most appropriate mechanism. The two main information exchange mechanisms identified by Goodwin and Nicholas are person-to-person and machine-to-machine.

- Person-to-person exchanges

Person-to-person exchange mechanisms are common in information exchange, and usually involve unstructured information [17]. The exchange can occur through email, phone calls, encrypted email, or web

portals. Web portals, like those used by the Financial Services Information Sharing and Analysis Center (FS-ISAC) and the US CERT, allow participants to submit threat data. The UK self-help portal for small communities, "Warning, advice and reporting point" (WARP), is another example. This type of exchange can handle large amounts of data and allows anonymous submissions. However, the challenge with person-to-person exchanges is scaling them up, which requires significant personal relationships built on trust and a history of successful exchanges.

- Machine-to-machine exchanges

Security professionals are focusing on creating automated systems for exchanging information. These systems are believed to help identify important information more quickly and enable automated threat mitigations. In the US, examples of machine-to-machine information exchanges include Security Event System, Collective Intelligence Framework, PRISEM, and Enhanced Cybersecurity Services. Microsoft Interflow is a cybersecurity platform that uses industry standards like STIX and TAXII to create an automated, machine-readable feed of threat and security information that can be shared in real-time. This automation can reduce costs and speed up the defence process by automating tasks that are currently performed manually [17].

1.4 Cyber information sharing governance structures

Authors from [39] discuss the governance structures for sharing cyber information. Its Table 1 in the section highlights some articles about sharing cyber situational awareness information, while its Table 2 presents a classification of information sharing models developed by Sedenberg and Dempsey [15]. They identify several types of cyber information sharing models:

1. The Government-centric model is a centralised approach where a central organisation may share information with others or enrich data by performing processing. The Department of Homeland Security is an example of a hierarchical government-centric organisation that uses open, standard data formats and transport protocols [24, 25].

2. The Sector-based Information Sharing and Analysis Centers (ISACs) are a type of Government-Prompted, Industry-Centric Sharing Models. These non-profit, member-driven organisations were established by critical infrastructure owners and operators to exchange information between government and industry. ISACs work through the National Infrastructure Protection Plan (NIPP13). The National Cybersecurity and Communications Integration Center (NCCIC) coordinates with all ISACs through the National Council of ISACs. These centres function as collection and analysis points for private sector entities to share data on a peer-to-peer basis, provide information to the federal government, and facilitate the flow of federal information to the private sector. Information Sharing and Analysis organisations (ISAOs) are designed to gather, analyse, and distribute cyberthreat information, but unlike ISACs, they are not affiliated with any particular sector or community and do not have to be part of the 16 critical infrastructures [26].

3. Corporate-Initiated, Peer Based Groups are cybersecurity information sharing entities that are privately sponsored. These companies voluntarily coordinate information sharing among their members without any government intervention. They customise their information exchanges to meet the specific needs of their members [16].

4. Individual-Based Groups are small online communities of peers that share sensitive information with the aim of immediately combating attacks. Trust is essential in these groups [16].

5. Open Communities and Platforms are sharing platforms that are open-source. STIX indicators and open-source intelligence feeds are examples of this type of format. The Malware Information Sharing Platform (MISP)[2] is a free and open-source platform developed by researchers from the Computer Incident Response Center of Luxembourg, the Belgian military, and NATO.

6. The category of Proprietary Products and Commercialised Services includes antivirus software and firewalls that provide cybersecurity information via software updates. These companies can also take part in other information sharing programs [16].

2.4 Sharing technologies for cyber security information

Some of the commonly used technical standards for exchanging cybersecurity information in the context of cyber situational awareness, as listed in [39], are described below.

The U.S. Department of Homeland Security employs a system called Automated Indicator Sharing (AIS) to facilitate the sharing of cybersecurity threat indicator information. AIS enables bidirectional sharing of information between participants and the DHS-managed system located at the National Cybersecurity and Communications Integration Center (NCCIC). Each stakeholder has a server at their location that allows them to exchange indicators with the NCCIC, as shown in Figure 2. Participants can share indicators they've observed during their own network defence efforts, and they also receive DHS-developed indicators that the agency shares with all AIS participants [27].

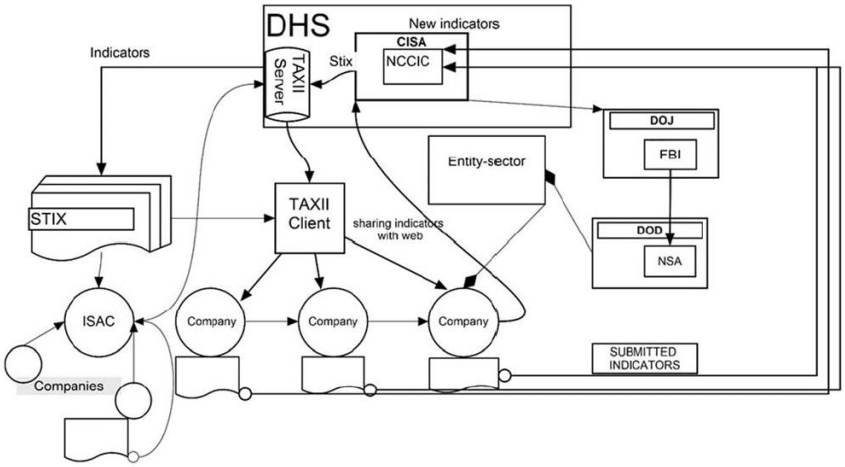


Figure 2 Cyber information sharing model in the U.S.

AIS system users can choose to remain anonymous and not have their identity disclosed as the source of shared indicators to other participants, unless they explicitly consent to it. DHS does not validate the indicators but instead prioritises sharing them quickly and in large volumes. It is up to the participants to verify the indicators they receive through AIS. The main aim of the US government is to obtain useful information about the indicators shared [27].

The Automated Indicator Sharing (AIS) system uses two specifications, Structured Threat Information Expression (STIX) and Trusted Automated eXchange of Indicator Information (TAXII)[3], for communication

[2] https://www.misp-project.org/
[3] https://oasis-open.github.io/cti-documentation/

between machines. STIX provides a language and format for consistent and machine-readable exchange of Cyber Threat Intelligence (CTI) between organisations. TAXII is an application layer protocol that allows the exchange of CTI over HTTPS. In [39] the architecture of STIX is analysed along with use cases where STIX is used for sharing cybersecurity information between organisations.

OASIS is a non-profit organisation that promotes the development and adoption of open standards for the global information society. It has defined twelve STIX Domain Objects, including Attack Pattern, which describes methods used by threat actors to attack targets, Campaign, which is a collection of malicious activities or attacks that occur over a period of time against a specific set of targets, Course of Action, which is an action taken to prevent or respond to an attack, Identify, which refers to individuals or organisations, Indicator, which is a pattern used to detect suspicious or malicious cyber activity, Intrusion Set, which is a group of adversarial behaviours and resources with common properties believed to be organised by a single threat actor, Malware, which is malicious code or software used to compromise a victim's data or system, Observed Data, which conveys information observed on a system or network, and Report, which is a collection of threat intelligence focused on one or more topics such as a description of a threat actor, malware, or attack technique, including contextual details.

TAXII is primarily used to transfer cyber threat information in STIX. According to Figure 3, communication based on collections refers to the scenario where a single TAXII client requests information from a TAXII server, which retrieves the information from a database. In the publish-subscribe model, TAXII channels in the TAXII server allow clients to exchange information with each other. Clients can push messages to channels or subscribe to channels to receive published messages. Multiple channels may be hosted by a TAXII server for each application programming interface root. It is possible for stakeholders to share indicators with DHS through an ISAC or ISAO without the use of a TAXII client [28].

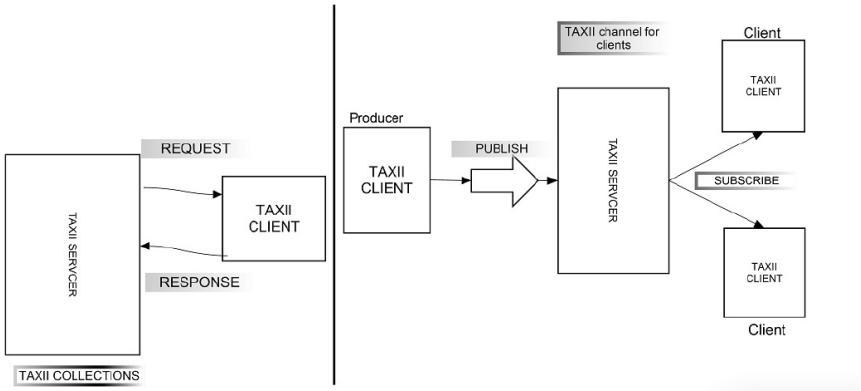


Figure 3 Flow of cyber threat information in TAXII (Modified from [29]).

Kokkonen and colleagues have developed a model for building information-sharing communities to improve cyber security situational awareness, as described in [30, 39]. They also propose using the Traffic Light Protocol (TLP), which involves four colour-coded categories for sharing information: red (restricted to participants only), amber (limited disclosure), green (limited disclosure with restrictions), and white (no restrictions on disclosure). TLP categories can be used to define information sharing rules and create a filtering system for data exchanged between organisations [31].

2.4.1 Information sharing methodologies between CERTS/ CSIRTS and Law Enforcement

The communities of National Information Security (NIS), including CERTS, are an essential part of the cyber-ecosystem, and it is not sufficient for small closed groups to share information without collaborating with public safety organisations. The primary objective of the Europol Information System (EIS) is to serve as a reference system for offences, individuals involved, and other related data to assist EU Member States, Europol, and its cooperation partners in combating organised cybercrime, terrorism, and other serious crimes. For instance, the European Cybercrime Centre (EC3), a part of Europol, employs an open-source Malware Information Sharing Platform (MISP). MISP is a tool that facilitates information sharing about malware samples and related malicious campaigns associated with particular malware variants. It provides architectural flexibility that allows it to be utilised as both a centralised platform (e.g., CIRCL and FIRST instances) and a decentralised (peer-to-peer) platform. The MISP project has developed the Permissible Actions Protocol (PAP) to specify how the received information can be utilised.

The Secure Information Exchange Network Application (SIENA) was created by Europol to provide a secure and user-friendly platform for the exchange of crime-related intelligence and information among EU Member States, public safety organisations, and law enforcement cooperation partners. SIENA functions as a VPN to facilitate this communication. In the United States, the National Information Exchange Model (NIEM) is an XML-based partnership mechanism established by the Departments of Justice and Homeland Security, which enables information-sharing among organisations as part of their business practices. InfraGard's Secure Web Portal, hosted by the FBI, also provides secure messaging and cyber-incident reporting tools for the private sector. InfraGard membership allows for peer-to-peer collaboration, information sharing, and relationship building with the FBI and law enforcement, as well as subject matter expert engagement and threat issue resolution across each of the 16 critical infrastructure sectors, DHS, and the National Infrastructure Protection Plan [26, 32].

The Digital Forensics XML toolset aims to represent several kinds of forensic data [23]. These include:

1. Metadata, which describes the source disk image, file, or other input information.

2. Detailed information about the forensic tool used during processing, such as the program name and where it was compiled or linked libraries.

3. Information about the state of the computer where the processing occurred, including the computer name, time of program execution, and dynamic libraries utilised.

4. The evidence or information that was extracted, including how and where it was found. The toolset also includes cryptographic hash values of specific byte sequences, as well as operating-system-specific information that is useful for forensic analysis.

CYBEX aims to automate cybersecurity information exchange and one of its operation domains is CYBEX Forensics which facilitates law enforcement operations by collecting evidence. The Evidence Database stores all the required information for this operation. CYBEX offers a framework to share information between a network mediation point and a law enforcement facility in real-time, providing a range of network forensics related to a specific incident or event.

The Cybersecurity Information Exchange Framework (CYBEX) is designed to improve the automation of information exchange for cybersecurity. CYBEX Forensics domain supports law enforcement by collecting evidence and storing it in the Evidence Database. The framework facilitates real-time network forensics

associated with a specific event, enabling the exchange of information between a network mediation point and law enforcement facilities. Privacy-Preserving Cybersecurity Information Exchange mechanism and CYBEX-P are adaptations of CYBEX and are built on a robust operational and administration structure. Privacy-Preserving Cybersecurity Information Exchange mechanism allows organisations to share their cybersecurity information without revealing their identities. CYBEX-P addresses the inefficiency of individual entities in dealing with cybersecurity issues by facilitating real-time exchange of threat data to enable organisations to analyse threats and prevent future cyber-attacks. CYBEX-P involves three parties: client organisations, CYBEX-P, and analysts/researchers. The processing server in CYBEX-P includes a TPM to verify the integrity of the software and hardware. Automating information sharing is necessary when quick exchange of essential information between stakeholders is required [34, 35].

2.5 Shared situational awareness

The Theory of Situational Awareness (SA) and Endsley's situational awareness model is discussed in [40]. It also outlines the general requirements for situation awareness. The concept of "shared situational awareness" is crucial for public safety actors, such as European law enforcement agencies, to achieve operational cooperation based on a reliable platform for cross-border tasks. Good team SA depends on team members' understanding of the shared information, which requires the exchange of pertinent data and a higher level of SA. Effective and efficient exchange of information between cybersecurity organisations is necessary for successful cooperation, and information interoperability is essential for achieving a common understanding of information. Since humans are not as proficient at processing large volumes of data quickly and consistently, flexible autonomy should provide a seamless transition of functions between the human and the system, according to Endsley's model [36, 37, 38].

Shared Situational Awareness is strongly linked to the exchange of cybersecurity information, as a shared understanding of the situation is incomplete without trusted information sharing [38]. There are four key factors involved in the development of shared Situational Awareness [38]:

1. The shared requirements of the team members to understand what information is necessary for the other team members;
2. The shared devices used for communication;
3. The shared mechanisms for establishing mental models; and
4. The shared processes to ensure effective team collaboration and the sharing of relevant information.

3 Cyber Threat Intelligence

Numerous organisations gather, generate and exchange information associated with probable or known cyber-attacks. As per the National Institute of Standards and Technology (NIST), information about cyber threats refers to any information that can assist organisations in protecting themselves against cyber-attacks or identifying the actions of adversaries. Cyber Threat Intelligence (CTI) is the knowledge derived after processing and analysing threat information, according to another definition given by Gartner. Many organisations, such as NIST and MITRE, have developed inventories of malware, vulnerabilities, and exploits. MITRE, in particular, manages three dictionaries, namely Common Vulnerabilities and Exposures (CVE), Common Platform Enumeration (CPE), and Common Weakness Enumeration (CWE).

3.1 Security vocabularies

In the late 1990s, the CVE was created to address the issue of a lack of standard identifiers for known vulnerabilities, which made it difficult for cybersecurity tools to share information. Another issue was the lack of a standardised basis for vulnerability evaluation since different tools used different metrics to declare the number of vulnerabilities they detected. While the CVE deals with specific instances within a system or product, the CWE defines a list of standard software and hardware weakness types. According to MITRE, CWE identifies errors in the implementation, code, or architecture of software or hardware. If such errors are not addressed, it can leave a system or network vulnerable to cyberattacks. On the other hand, the CPE is an XML-based dictionary that follows a structured naming scheme for IT systems, software, and packages. It provides a common representation of a specific software product, including its name, vendor, and version.

The dictionaries discussed earlier are significant sources of information, but they do not provide details on how attackers exploit vulnerabilities in systems or software. To address this gap, the MITRE Corporation released the Common Attack Pattern Enumeration and Classification (CAPEC) dictionary in 2007. The CAPEC dictionary consists of descriptions of common techniques and characteristics used by adversaries to exploit known weaknesses, referred to as Attack Patterns. Each Attack Pattern provides insight into the various stages and elements of an attack, as well as potential measures to mitigate its impact.

2.2 Cyber threat intelligence formats

In recent years, several approaches for sharing CTI have been defined. One such approach is OpenIOC, which is an extensible XML scheme used to describe technical characteristics that can identify known threats or the methodology used by the threat agent. However, OpenIOC has limited commercial adoption compared to other standards, and it lacks the ability to describe TTPs. Another approach is the Incident Object Description Exchange Format (IODEF), which is an open standard that defines an XML data representation for sharing information about computer security incidents. However, IODEF requires other formats for describing TTPs and campaigns, and it was primarily designed for sharing incident data rather than IoCs. The Collective Intelligence Framework (CIF) is an open-source platform used for storing and sharing CTI. CIF uses the IODEF data format and covers various data observations from any source to create a series of observations. However, CIF does not provide a description of TTPs or threat actor data.

The National Institute of Standards and Technology (NIST) states that organisations gather and exchange information related to potential and known cyberattacks, known as cyber threat information (CTI). Once processed and analysed, it becomes cyber threat intelligence (CTI1), which involves context, mechanisms, indicators, implications and actionable advice about an existing or emerging threat. To aid in this process,

organisations such as NIST and MITRE have created dictionaries of types of malware, vulnerabilities, and exploits, including the Common Vulnerabilities and Exposures (CVE4), Common Platform Enumeration (CPE5), and Common Weakness Enumeration (CWE6). MITRE also developed the Common Attack Pattern Enumeration and Classification (CAPEC7) dictionary, which describes the methods that adversaries use to exploit known weaknesses. Several methods for CTI sharing exist, including OpenIOC8, Incident Object Description Exchange Format (IODEF), and Collective Intelligence Framework (CIF9). The Structured Threat Information Expression (STIX10) language and Trusted Automated Exchange of Intelligence Information (TAXII11) provide a consistent and machine-readable format for exchanging CTI, with two major versions available online: STIX1.x and STIX2.x. STIX2.x is defined using JSON and features 18 top-level objects called STIX Domain Objects (SDOs) and STIX Relationship Objects (SROs) that define relations between SDOs.

Table 1 STIX Objects.

Object name	Description
Observed Data	Conveys information about cybersecurity related entities such as files, systems, and networks.
Attack Pattern	Belongs to TTPs that describe ways that adversaries attempt to compromise targets.
Campaign	A grouping of adversarial behaviours that describes a set of malicious activities or attacks.
Indicator	Contains a pattern for detecting a suspicious or malicious activity.
Malware	Belongs to TTPs and represents malicious code.
Malware Analysis	The metadata and results of a particular static or dynamic analysis performed on malware.
Tool	Legitimate software that can be used by adversaries to initiate and perform attacks.
Vulnerability	A mistake in software that can be used by an adversary to gain access to a system or network.
Course of Action	A recommendation from a producer of intelligence to a consumer for mitigating and/or preventing an attack.
Identity	Individuals, organisations, or groups as well as classes of individuals, organisations, systems or groups.
Threat Agent	Individuals, groups, or organisations believed to be operating with malicious intent.
Infrastructure	Belongs to TTPs and describes a system, software service and any associated physical or virtual resources used by adversaries.
Intrusion set	Describes a set of adversarial behaviours and resources with common properties used by a single organisation.
Opinion	Describes a textual assessment of the information correctness in a STIX Object produced by a different entity.
Location	Represents a geographic location.
Report	A collection of CTI focused on one or more topics.

Note	Contains informative text to provide further context or additional analysis not contained in the STIX Objects.
Grouping	Asserts that the referenced STIX Objects have a shared context.
Relationship	Link together two SDOs or SCOs to describe their relation.
Sighting	Denotes the belief that something in CTI was seen.

In addition to the STIX standard, which outlines the general concepts of CTI, MITRE introduced the Malware Attribute Enumeration and Characterization (MAEC) language in early 2011 to share and encode high-quality information about malware. The aim of MAEC is to enhance communication and reduce duplication of malware analysis by eliminating inaccuracies and uncertainties in malware descriptions. Like STIX, MAEC defines several top-level objects, including *Behaviours, Malware Actions, Malware Families, Malware Instances*, and *Collections*. The data model of MAEC is represented as a connected graph of nodes and edges, where top-level objects represent the nodes, and relationships between MAEC objects are the edges, which are described briefly in Table 2.2.

Table 2 MAEC Objects.

Object name	Description
Malware Actions	Represents an abstraction on a system-level API call called by the malware instance during its execution.
Malware Families	Defines a set of malware instances that are related by common authorship or lineage.
Malware Instances	A single member of a Malware Family packaged as a binary.
Collections	Captures a set of MAEC entities or STIX Cyber Observables that are related or associated.

The STIX2.x and MAEC languages define objects through properties that convey specific information. In 2013, MITRE began creating the ATT&CK framework to accumulate knowledge about known cyberattacks, particularly the tactics and techniques used by adversaries, and provide guidance for resolving security issues. The framework uses the STIX2.x standard for describing CTI, allowing it to be shared using compatible tools and standards. However, a recent study revealed that while STIX and TAXII have attracted interest in 18 countries, their adoption has faced some barriers, such as the initial setup and learning curve, organisational compatibility and maturity, understanding of cyber threat vocabulary, and lack of conformity in data notation [41]. Nevertheless, some benefits of adoption include enhanced sharing of structured relationship data, data restriction enabling, structured documentation mark-up, and improved interoperability.

Numerous standards and data formats have been proposed for a comprehensive description of CTI. However, the need to extend these approaches still exists and has been recognized [42]. Some works have been proposed to extend the STIX standard, such as an extension for describing complex patterns, which allows security specialists to tag object attributes and describe precise relations between different objects [43].

However, this extension only applies to the XML-based version of the STIX language, while the latest STIX version defines multiple relations between cyber-observable objects and other STIX domain objects. Another extension proposed a representation of the Data-Sharing Agreement, including actions to be enforced before sharing CTI reports, to satisfy GDPR constraints [44]. This extension was validated by enforcing the anonymisation mechanism on spam-emails. Finally, an extension was proposed to allow describing sticky policies as a package of multiple custom STIX objects, including conditions for restricting usage of CTI reports and requirements to be enforced before sharing those reports [45]. This extension was validated with a designed tool that allows writing sticky policies and enforcing specified anonymisation action in an automated manner.

3.3 Cyber threat intelligence sharing and analysis platforms

The CTI sharing platform is a platform that provides various capabilities such as CTI creation, collection, exchange, and analysis within one or multiple communities. These platforms may also offer automated dissemination or implementation of actionable CTI concepts, such as courses of action, to detect or prevent cyberattacks. Additionally, organisations can use multiple sharing platforms to exchange CTI within different levels, such as between communities and organisations. However, different platforms may use different terms to describe the same concept, such as CTI record, Event in MISP, Pulse in OTX, and Activity in IBM X-Force Exchange. Table 2.3 provides some examples of well-known CTI sharing platforms.

Table 3 Sharing platforms.

Product	Vendor	Description
Malware Information Sharing Platform	Open Source	Free and open-source community sourced CTI sharing platform
OpenCTI	Open Source	An open-source platform allowing organisations to manage their cyber threat intelligence knowledge and observables. It has been created to structure, store, organise, and visualize technical and non-technical information about cyber threats.
ThreatConnect	ThreatConnect	General CTI platform with community sharing capabilities
Cyber Threat Exchange	NC4	CTI sharing platform used by the FS-ISAC
Blueliv Threat Intelligence Platform	Blueliv	General CTI platform with community sharing capabilities

Since the CTI management field is still evolving, the capabilities and features of current CTI sharing platforms are subject to change. Each platform has its own philosophy, terminology, features, and focus on specific cyber threat data. Despite this, MISP has become the de facto standard for collecting and sharing CTI in recent

years. It is a community sharing platform that relies on content generated by communities, and it allows CTI sharing via a web interface or Python library. A hub-spoke sharing community can be set up, and MISP has a protocol for synchronising between different instances. The platform supports several synchronisation mechanisms, including pull, push, and cherry-picking. With pull, one MISP instance can discover events from another MISP instance based on predefined distribution rights. Push allows single or multiple records to be sent to a remote instance, while cherry-picking enables users to select records from another MISP instance to be pulled to their local instance. MISP also allows defining the distribution of CTI records among organisations, communities, connected communities, and all sharing levels. The platform supports export of records and attributes in various formats such as OpenIOC, CVS, STIX in XML, and JSON, making it possible to integrate with other tools. Moreover, signatures for IDS including Bro, Suricata, and Snort can be exported.

MISP is more than just a software tool; it also includes a range of data models developed by the MISP community. The MISP platform uses JSON as its core format for sharing information, and this format is described in an RFC draft. The MISP format is based on the concepts of objects, attributes, and taxonomies. Attributes contain the actual data and are organised into various categories and types, such as bank-account-nr for financial fraud. MISP objects are collections of attributes defined by a template. MISP also incorporates various taxonomies, including classifications used by CSIRTs/CERTs, national classifications, and threat models, for organising events and attributes.

3.4 Actionable cyber threat intelligence

A survey conducted in 2017 among 1,200 IT and IT security practitioners in the United States and EMEA revealed that there had been a considerable increase in the consumption and sharing of threat intelligence since 2015. However, the majority of respondents were dissatisfied with the exchange and utilisation of threat intelligence. The main complaint regarding threat intelligence was that it was not actionable, timely, or accurate enough, according to the survey [46].

Before CTI can be considered actionable, there are various processes involved in receiving and submitting information about vulnerabilities. ENISA has defined actionable CTI as meeting five criteria: relevance, timeliness, accuracy, completeness, and ingestibility [47].

The study outlined in [48] identified four groups of individuals who utilise CTI: high-level executives, threat managers, threat analysts, and incident response teams. Depending on the source or stakeholder, the quality of CTI may vary. Quality can be assessed by its accuracy, relevance, timeliness, usefulness, and uniqueness [49]. Additionally, a CTI community member who consistently provides valuable and timely information may be recognized as a quality stakeholder [50].

Additionally, the threat landscape is constantly evolving, necessitating prompt action on CTI. The significance of swift sharing is apparent since the value of CTI diminishes rapidly, often becoming obsolete within hours or days [51]. Previous studies have shown that 60% of malicious domains have a lifespan of one hour or less, underscoring the need for timeliness in CTI sharing [52]. Timeliness is not only determined by the age of the information, but also by the regularity of updates on threat activities, alterations, or advances in capabilities or infrastructure [53].

To protect clients' privacy, organisations need to ensure that CTI is only shared with trusted stakeholders or anonymized. Anonymization techniques such as k-Anonymity [54], l-Diversity [55], and t-Closeness [56] have been developed to protect shared information. However, stakeholders are often hesitant to share

information about breaches due to concerns about reputational damage [57]. Encryption is another important aspect of privacy protection when sharing CTI between stakeholders to prevent Man-in-the-Middle attacks. To address this, a protocol called PRACIS was introduced in [58] for privacy-preserving data forwarding and aggregation for semi-trusted message-oriented middleware. In addition, [59] proposed an architecture to compute privacy risk scores over CTI by analysing the privacy risks associated with extracting personal information from threat intelligence reports. Combining these two works can help to enhance privacy in a CTI program.

4 Ontology

The community standard known as DFAX was created to represent and share digital forensic information. It utilised the Cyber Observable eXpression (CybOX) to represent technical information like binary artefacts and search patterns [60]. However, CybOX had limitations in representing digital forensic and cyber-investigation information, and was replaced by STIX Cyber Observables in 2016 as an integrated component of the STIX standard, which focuses on cyber threat intelligence. STIX Cyber Observables is not suitable as a foundation for representing various cyber-investigation use cases. Based on the lessons learned from CybOX and DFAX, CASE and UCO were developed to provide an improved data model and ontology for cyber-investigations in any context, including criminal, corporate and intelligence. CASE is a specific profile of UCO that supports cyber-investigations.

CASE and relevant parts of UCO are based on the Hansken data model, which was created and put into practice by the Netherlands Forensic Institute (NFI). Hansken builds on the success of its predecessor XIRAF, and is used for numerous investigations every year. The Hansken data model forms a strong basis for developing CASE, as it already includes the most frequently encountered traces in cyber investigations and can easily accommodate new types of traces due to its flexibility.

CASE and UCO enable a broad range of analysis and correlation techniques by fully structuring data. Other ontology-based initiatives aimed at analysing digital evidence have been narrow in focus and can utilise CASE as their specification language. For example, the Ontology for the Representation of Digital Incidents and Investigations (ORD2i) referenced DFAX and UCO and demonstrated a proof-of-concept implementation for timeline reconstruction and analysis [61]. DESO proposed an ontology-based approach for representing known digital traces and supporting triage searches of a digital crime scene for matching characteristics. Additionally, the ParFor project proposed an ontology-based approach for representing activities on computer systems. These initiatives illustrate the recognition of the need for a standardised way to represent and share cyber-investigation information. Prior to UCO, there was little agreement across the diverse community regarding such an ontology. CASE and UCO fill this void by providing an ontology that can serve as the basis for community consensus and interoperability across organisations and tools.

The purpose of the CASE specification language is not to dictate how tools or systems should structure their data internally, but rather to serve as a shared language that applications can use to import and export data, thus facilitating interoperability and standardisation. Developers of systems and applications can translate CASE into their own internal implementations. The suggested JSON serialisation is just one possible serialisation format, and the shared format could also be represented in other formats such as XML, Turtle (RDF), protocol buffers, or other types of serialisations.

4.1 The role of ontologies

An ontology defines the basic terms and relations comprising the vocabulary of a topic area, as well as the rules for combining terms and relations to define extensions to the vocabulary [80]. As such, it is a formal, explicit specification of a shared conceptualization [81].

The UCO complements CASE by providing a structured framework that can be used to develop specifications for different cyber domains, following a consistent and compatible approach. UCO can be thought of as a set of building blocks and components, such as big and small blocks, tables, windows, and wheels. CASE is one

type of construction that uses some of these components, tailored for its specific needs. Other domains can also utilise many of the same building blocks and components, customised for their unique requirements.

Information representations can be created with varying degrees of formality, ranging from informal serialisation schemas to formal models/ontologies. Serialisations are crucial for implementing exchange in concrete systems. Using explicit ontology specifications as the foundation for these serialisations provides significant benefits, such as:

1. Reducing the risk of ambiguity and misinterpretation by defining both semantics and syntax;
2. Abstracting concepts and structures for consistency and reuse;
3. Enabling portability across serialisations and technologies, rather than being confined to a single approach;
4. Ensuring the integrity of representation is more resistant to evolution and change.

Representing information at a high level of abstraction and formality can lead to a clear understanding of information concepts and structures within a particular domain and how they relate to the broader context. In the case of CASE, the domain of interest is cyber-investigation, which is connected to various related domains such as digital forensic science, incident response, and criminal justice. To ensure consistency, flexibility, and interoperability across these domains, it is necessary to have consistent representations of information concepts and structures. This means that some concepts and structures required for CASE will also be necessary for other use cases within the broader ecosystem. For instance, representing information such as files, emails, or actions is essential not only for CASE but also for other domains.

Creating a formal ontology provides a clear and explicit foundation for matching the semantics of the modelled information with other domain ontologies. This allows for automated translation of instance content between ontologies, as well as the use of instance content as linked data. This enables seamless querying and aggregation of distributed content across different domains, regardless of the original ontology used.

4.2 Related work

In the past, proposed schemas were limited to specific subsets of digital traces and did not cover the entire range of cyber-investigation information [62, 63, 64, 65, 66, 67]. Digital Forensics XML (DFXML) is a schema used by several tools to represent file system information [68, 69]. However, DFXML only focuses on storage media information and does not encompass the diverse range of digital traces in cyber-investigations. Furthermore, DFXML's representation of provenance is limited to tool execution and does not cover the complete scope of provenance in cyber-investigations.

Some tools use the Advanced Forensic Format (AFF4) with the Resource Description Framework (RDF) to store digital forensic information [70, 71]. AFF4 is highly adaptable for storing raw data, including features like compression and encryption. However, AFF4 doesn't include the full range of cyber-investigation information that is covered by CASE and UCO. CASE and AFF4 can be used together when data have been saved in an AFF4 file. For example, an investigation modelled with CASE can connect to a forensic copy of storage media saved in an AFF4 file.

The U.S. government developed the XML Data Encoding Specification for Intelligence Document and Media Exploitation (DOMEX) to share specific types of information, including some mobile device details [72]. While the DOMEX standard includes elements to track the origin of information, its usefulness is limited due to the

lack of an accompanying ontology, low expressive power for describing cyber observables, and the inability to capture relationships.

CASE is a digital forensic schema that has been developed using lessons learned from previous schemas, and it builds on the Hansken data model created by the Netherlands Forensic Institute. The Hansken data model has improved upon an earlier version called XIRAF, and it consists of a unique ID, a name, and a set of types with properties [73]. The Hansken data model uses duck typing, which allows data to be defined by its inherent characteristics instead of enforcing strict data typing. The Hansken trace model's types can be compared to a predefined Property Bundle in CASE. CASE objects can be assigned any combination of Property Bundles, and the data types are evaluated using the duck test, which uses inference to the best explanation. This approach is preferred over using the OWL concept of inheritance to define an object with various properties, which becomes unwieldy when unexpected combinations of objects are encountered [74, 75].

Hansken uses types such as 'file', 'email', and 'contact', with a special type called 'data' (renamed 'ContentData' in CASE) to describe properties of trace data such as entropy and hash values. Another special type in Hansken is 'tool', which captures the 'how' aspect of provenance for the trace. Each type in Hansken has an origin, indicating where the trace type comes from, which can be 'extracted', 'mined', 'processed', or 'user-added'. Extracted types are deterministic results of applying forensic tools to data, while mined types such as 'entity' are the result of applying probabilistic algorithms and have a confidence property. Processed types describe the process and provide provenance details, such as the 'tool' type, while user-added types describe metadata added by a user during trace analysis. CASE supports the full range of information covered by Hansken.

CASE and the Unified Cyber Ontology (UCO) are developed simultaneously to ensure that the same constructs are represented consistently across various cyber-related domains, promoting interoperability among these domains.

ORD2I and UCO both reference a separate layer for representing specialised domain knowledge as objects, which can be mapped to a standard representation for sharing and correlating between organisations and tools [76]. Both UCO and ORD2I provide a generic way to represent activities involving objects and entities, as well as case information and provenance. The compatibility between UCO and ORD2I reflects growing community consensus that has strengthened the development of CASE. By using Provenance Records to further characterise Traces with information specific to the cyber-investigation domain, CASE encompasses all aspects of provenance in cyber-investigation domains, while ORD2I concentrates on provenance in the context of data processing using forensic tools. The use of a standardised Traces layer can help represent in-depth knowledge of specialised domains and can be shared and maintained across related domains such as digital forensic science, intrusion investigation, incident response, and cyber threat intelligence.

UCO and the PROV ontology share some similarities in representing the provenance of data. While developing UCO, it is useful to consider PROV as a reference. However, PROV is more focused on data production and does not cover some essential cyber-investigation use cases. Unlike an Activity in PROV, an Action in UCO/CASE can specify inputs, outputs, and instruments used. Additionally, the result of an Action in CASE can be another Action, which is not possible in PROV. Moreover, PROV lacks the flexibility of CASE to represent links and associations between objects using Relationship objects. Despite these limitations, PROV will continue to be a valuable resource for reference as UCO and CASE are developed.

Other ontologies and frameworks have been developed to enable advanced analysis and can adopt CASE to facilitate standardisation and interoperability. For example, the Digital Evidence Semantic Ontology (DESO) can utilise CASE to represent digital traces that are known and to assist in triage searches for matching characteristics at a digital crime scene [77]. The Digital Evidence Management Framework (DEMF) can use CASE to portray metadata and provenance information [78]. Similarly, the ParFor project can implement CASE to illustrate activities that occur on computer systems [79].

4.3 UCO overview

The information that needs to be represented can be divided into layers, with the bottom layer representing raw data, the middle layer representing provenance, and the top layer representing behaviour. UCO offers an ontology that provides a universal way of organising this information and can be applied in various domains such as digital forensics, incident response, and counterterrorism.

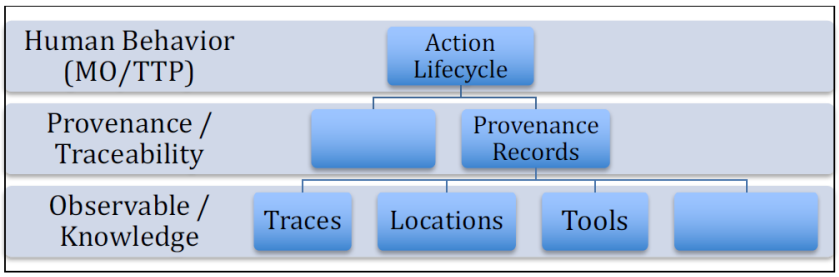


Figure 4 Layers of representing cyber-investigation information.

4.4 CASE overview

One of the core components of cyber-investigations involves identifying and examining traces, which can be defined as any detectable alteration or absence of expected data resulting from an event in a digital crime scene. Traces are used to answer a variety of questions that typically focus on the what, where, when, who, how, and why of a given event. It is also essential to document the state of each trace, such as whether it is allocated or deleted, and whether an anticipated trace exists or not.

The CASE specification language is designed to be adaptable enough to depict various types of traces, such as those defined in the UCO, as well as their corresponding properties, such as disks, devices, and file systems. This creates a reliable foundation for detailing information during cyber-investigations. Figure 5 showcases a File object that has several property bundles. The idea of using Property Bundles in CASE was influenced by the "duck" model integrated into the Hansken system (van Baar, van Beek, van Eijk, 2014). These properties can contain different information, such as date-time stamps, trace content, and hash values, including MD5 and SHA256.

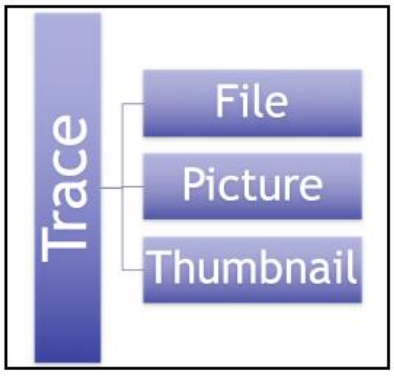


Figure 5 Duck model allows flexible representation of traces using various combinations of property bundles.

The DFAX system initially used XML as its default serialisation, but after gathering feedback from the community, CASE/UCO chose JSON-LD as their primary serialisation binding. Although JSON is powerful and flexible, it requires additional scaffolding to validate against an ontology. JSON-LD, on the other hand, offers the necessary structure to fully validate JSON content to its associated ontological specification, as depicted in Figure 6. Explicit validation provided by JSON-LD ensures the integrity between the ontology and serialisation, and brings about automation advantages, including built-in API support for various programming languages (Python, Ruby, PHP, Go, C#, Java, etc.) and lossless transformation between multiple serialisation formats (JSON-LD, RDF-XML, Turtle-RDF, etc.).

```
{
 "@context": {
  "@vocab": "https://github.com/casework",
   },
 "@graph": [
    {
    "@id": "digital_photograph1",
    "@type": "Trace",
    "propertyBundle": [
     {
       "@type": „File",
       "magicNumber": "/9j/4AAQSkZ",
       "mimeType": "image/jpg"
     },
     {
       "@type": "ContentData",
       "data": "/9j/4AAQSkZJRgABAQAAAQAB...",
       "size": 35000
     },
     {
       "@type": "RasterImage",
       "format": "jpg",
       "height": 12345,
       "width": 12345,
       "bitsPerPixel": 2
     },
     {
       "@type": "hash",
       "hashMethod": "MD5",
       "value": "3d137a188c1e82247b815209ce44af2c"
     },
     {
       "@type": "EXIF",
       "exifData": [
            "key": "Make",
            "value": "Canon"
           ...
  ]
 },
```

Figure 6 Example of CASE being used to represent a file.

The JSON in Figure 6 is JSON-LD, which uses strict, namespaced @type values to specify the type for all JSON objects, enabling their explicit traceability back to the specifications for these types in the UCO.

5 Conclusions

In conclusion, effective collaboration and information sharing between stakeholders, including CERTs, CSIRTs, and other organisations, are crucial for enhancing the security of modern software and systems. The LAZARUS project aims to address security issues throughout the software development lifecycle by leveraging advanced machine learning and artificial intelligence techniques. A key component of this endeavour is understanding and implementing state-of-the-art data sharing models that enable faster mitigation mechanisms and facilitate cooperation among different stakeholders.

This report has provided an overview of the current techniques, standards, and mechanisms for information sharing relevant for the LAZARUS project, focusing on characteristics of cyber information sharing models, sharing technologies for cybersecurity information, shared situational awareness, cyber threat intelligence, and the role of ontologies. The insights presented in this deliverable are expected to contribute to the ongoing efforts of the LAZARUS project to develop and integrate effective data sharing models that enhance collaboration and support a more secure and resilient digital ecosystem.

As cybersecurity threats continue to evolve and become more sophisticated, it is essential for organisations and researchers to stay abreast of the latest developments in information sharing models and technologies. Future work should focus on refining these models and developing new, innovative approaches to improve the efficiency, scalability, and security of information sharing systems. This will help ensure that the LAZARUS project, as well as the broader cybersecurity community, can continue to adapt and respond effectively to emerging challenges in the constantly changing digital landscape.

6 References

[1] ENISA, "Information sharing and common taxonomies between CSIRTs and Law Enforcement," 2015.

[2] The Department of Homeland Security (DHS), “Blueprint for a Secure Cyber Future - The

Cybersecurity Strategy for the Homeland Security Enterprise,” DHS, 2011.

[3] OECD Legal Instruments, "Recommendation of the Council on the Protection of Critical Information Infrastructures," 30 04 2008. [Online]. Available: https://legalinstruments.oecd.org/en/instruments/121. [Accessed 22 10 2019].

[4] National Institute of Standards and Technology (NIST), "Guidelines for smart grid cybersecurity In Smart grid cybersecurity strategy, architecture," U.S. Department of Commerce, USA, 2014.

[5] European Union Agency For Network And Information Security (ENISA), "Programming Document 2019-2021," ENISA, Heraklion, Greece, 2019.

[6] L. Ladid, J. Armin and H. Kivekäs, “The Finish electronic communications regulator TRAFICOM - A cybersecurity reference model for Europe.,” SAINT Consortium/ Traficom., Helsinki, 2019.

[7] ECSO European Cyber Security Organisation, “About ECSO,” 2019. [Online]. Available: https://ecs-org.eu/. [Accessed 2 9 2019].

[8] ENISA & ITE, “Information Sharing and Analysis Centres (ISACs) Cooperative models,” European Union Agency for Network and Information Security, Greece, 2017.

[9] G. White and R. Lipsey, “ISAO SO Product Outline,” ISAO Standards organisation, 2016.

[10] Electrical Technology, “Internet of Things (IOT) and Its Applications in Electrical Power Industry,” 2016. [Online]. Available: http://www.electricaltechnology.org/2016/07/internet-ofthings-iot-and-its-applications-in-electrical-power-industry.html. [Accessed 10 8 2019].

[11] National Institute of Standards and Technology (NIST), “Guide for Conducting Risk Assessments. 800-30,” U.S. Department of Commerce, Gaithersburg, 2013.

[12] National Institute of Standards and Technology (NIST), “Special Publication 800-37 R.2, Risk Management Framework for Information Systems and organisations,” U.S. Department of Commerce, Gaithersburg, 2018.

[13] The International organisation for Standardization (ISO), “International Standard ISO/IEC 27010:2015. Standard edn.,” Switzerland, 2015.

[14] National Institute of Standards and Technology (NIST), “Guide to Cyber Threat Information Sharing. NIST Special Publication 800-150,” U.S. Department of Commerce, Gaithersburg, 2016.

[15] E. M. Sedenberg and J. X. Dempsey, "Cybersecurity Information Sharing Governance Structures: An Ecosystem of Diversity, Trust, and Tradeoffs," 31 May 2018. [Online]. Available: https://arxiv.org/abs/1805.12266. [Accessed 30 March 2019].

[16] "Technical threat indicator," [Online]. Available: https://itlaw.wikia.org/wiki/Technical_threat_indicator.

[17] C. Goodwin and J. Nicholas, "A framework for cybersecurity information sharing and risk reduction," [Online]. Available: https://www.slideshare.net/RoyRamkrishna/framework forcybersecurityinfosharing-1.

[18] MITRE Corporation, "Trusted Automated eXchange of Indicator Information — TAXII™

Enabling Cyber Threat Information Exchange," [Online]. Available:.

https://makingsecuritymeasurable.mitre.org/docs/taxii-intro-handout.pdf

[19] MITRE Corporation, "Cyber Information-Sharing Models: An Overview," 2012. [Online].

Available: https://www.mitre.org/sites/default/files/pdf/cyber_info_sharing.pdf

[20] RSAC contributor, "RSA conference - Threats Are Omnipresent But You Have Options," 11

june 2019. [Online]. Available: https://www.rsaconference.com/industry-topics/blog/threatsare-

omnipresent-but-you-have-options.

[21] P. McGlone, “Threats Are Omnipresent But You Have Options,” 11 June 2019. [Online].

Available: https://securityboulevard.com/2019/06/threats-are-omnipresent-but-you-haveoptions/.

[22] L. J. Janczewski and W. Caelli, Cyber Conflicts and Small States. New York: Routledge, 2016.

[23] F. Skopik, Collaborative Cyber Threat Intelligence: Detecting and Responding to Advanced Cyber Attacks at the National Level, Boca Raton: CRC Press, 2017.

[24] Johnson, et al., Guide to cyber threat information sharing, NIST special publication, NIST, 2016.

[25] M. He, L. Devine and J. Zhuang, "Perspectives on Cybersecurity Information Sharing among Multiple Stakeholders Using a Decision-Theoretic Approach: Cybersecurity Information Sharing," Risk Analysis, 2017.

[26] Department of Homeland Security, , "NIPP 2013 - partnering for critical infrastructure security and resilience.," DHS, 2013.

[27] The Department of Homeland Security (DHS), “Automated indicator sharing AIS,” DHS, Washington, U.S, 2019.

[28] OASIS Cyber Threat Intelligence;DHS, “"TAXII™ version 2.0. committee specification 01," OASIS Open, Tech. Rep. taxii-v2.0-cs01,” OASIS, 2017.

[29] Cyber Threat Intelligence Technical Committee, “Introduction to TAXII,” 2019. [Online]. Available: https://oasis-open.github.io/cti-documentation/taxii/intro [Accessed 22 10 2019].

[30] T. Kokkonen, J. Hautamäki, J. Siltanen and T. Hämäläinen, "Model for Sharing the Information of Cyber Security Situation Awareness between organisations," 23rd International Conference on Telecommunications, 2016.

[31] T. Kokkonen, Anomaly-Based Online Intrusion Detection System as a Sensor for Cyber Security Situational Awareness System, Jyväskylä: University of Jyväskylä, 2016.

[32] The Criminal Intelligence Coordinating Council, "National criminal intelligence sharing plan. Building a national capability for effective criminal intelligence development and the nationwide sharing of intelligence and information," CICC, 2013.

[33] I. Vakilinia, D. K. Tosh and S. Sengupta, "Privacy-preserving cybersecurity information exchange mechanism," International Symposium on Performance Evaluation of Computer and Telecommunication Systems (SPECTS), pp. 1-7, 2017.

[34] Sadique, F. et al,, "A System Architecture of Cybersecurity Information Exchange with Privacy (CYBEX-P)," IEEE 9th Annual Computing and Communication Workshop and Conference (CCWC), pp. 493-498, 2019.

[35] M. Endsley, "Design and evaluation for situation awareness enhancement.," in Proceedings of the Human Factors Society 32nd Annual Meeting, 1988.

[36] M. Endsley and M. Robertson, "Situation awareness in aircraft maintenance teams," International Journal of Industrial Ergonomic, vol. 26, pp. 301-325, 2000.

[37] M. Endsley and M. Robertson, "Training for situation awareness in individuals and teams," in Situation Awareness Analysis and Measurement, Mahwah, LEA, 2000.

[38] C. Bolstad and M. Endsley, "The effect of task load and shared displays on team situation awareness," in The 14th Triennial Congress of the International Ergonomics Association and the 44th Annual Meeting of the Human Factors and Ergonomics Society, Santa Monica, CA, 2000.

[39] J. Rajamäki, I. Tikanmäki & J. Räsänen In vol. 43 of Information & Security: An International Journal, https://doi.org/10.11610/isij.v43 Reproduced with the Creative Commons BY-NC-SA 4.0 license.

[40] J. Pöyhönen, V. Nuojua, M. Lehto & J. Rajamäki In vol. 43 of Information & Security: An International Journal, https://doi.org/10.11610/isij.v43 Reproduced with the Creative Commons BY-NC-SA 4.0 license.

[41] Gong N., 2019. Barriers to Adopting Interoperability Standards for Cyber Threat Intelligence Sharing: An Exploratory Study. In: Arai K., Kapoor S., Bhatia R. (eds) Intelligent Computing. SAI 2018. Advances in Intelligent Systems and Computing, vol. 857. Springer, Cham.

[42] Fransen, Frank, Andre Smulders, and Richard Kerkdijk. "Cyber security information exchange to gain insight into the effects of cyber threats and incidents." e & i Elektrotechnik und Informationstechnik 132, no. 2 (2015): 106-112.

[43] Ussath, Martin, David Jaeger, Feng Cheng, and Christoph Meinel. "Pushing the limits of cyber threat intelligence: extending STIX to support complex patterns." In Information Technology: New Generations, pp. 213-225. Springer, Cham, 2016.

[44] Martinelli, Fabio, Oleksii Osliak, and Andrea Saracino. "Towards general scheme for data sharing agreements empowering privacy-preserving data analysis of structured CTI." In Computer Security, pp. 192-212. Springer, Cham, 2018.

[45] Osliak, Oleksii, Andrea Saracino, and Fabio Martinelli. "A scheme for the sticky policy representation supporting secure cyber-threat intelligence analysis and sharing." Information & Computer Security (2019).

[46] Institute, P., 2017. Third Annual Study on Exchanging Cyber Threat Intelligence: There Has to Be a Better Way. https://www.ponemon.org/local/upload/file/2017%20Inflobox%20Report%20V6.pdf

[47] Pawlinski, P., Jaroszewski, P., Kijewski, P., Siewierski, L., Jacewicz, P., Zielony, P., Zu- ber, R., 2014. Actionable information for security incident response. European Union Agency for Network and Information Security, Heraklion, Greece.

[48] Brown, S., Gommers, J., Serrano, O., 2015. From cyber security information sharing to threat management. In: Proceedings of the 2nd ACM Workshop on Information Sharing and Collaborative Security. ACM, pp. 43–49.

[49] Al-Ibrahim, O., Mohaisen, A., Kamhoua, C., Kwiat, K., Njilla, L., 2017. Beyond free riding: quality of indicators for assessing participation in information sharing for threat intelligence. arXiv: 1702.00552.

[50] Mohaisen, A., Al-Ibrahim, O., Kamhoua, C., Kwiat, K., Njilla, L., 2017. Rethinking information sharing for actionable threat intelligence. CoRR. arXiv: 1702.00548.

[51] Farnham, G., Leune, K., 2013. Tools and Standards for Cyber Threat Intelligence Projects.

[52] Alliance, H.I.T., 2015. Health Industry Cyber Threat Information Sharing and Analysis. Technical Report.

[53] ThreatConnect, 2015. Threat Intelligence Platforms - Everything You've Ever Wanted to Know But Didn't Know to Ask. Technical Report.

[54] Sweeney, L., 2002. k-anonymity: a model for protecting privacy. Int. J. Uncertain. Fuzziness Knowl. Based Syst. 10 (5), 557–570.

[55] Machanavajjhala, A., Kifer, D., Gehrke, J., Venkitasubramaniam, M., 2007. L -diversity: privacy beyond k -anonymity. TKDD 1 (1), 3.

[56] Li, N., Li, T., Venkatasubramanian, S., 2007. t-closeness: privacy beyond k-anonymity and l-diversity. In: Proceedings of the 23rd International Conference on Data Engineering, ICDE 2007, The Marmara Hotel, Istanbul, Turkey, April 15–20, 2007, pp. 106–115.

[57] Garrido-Pelaz, R., González-Manzano, L., Pastrana, S., 2016. Shall we collaborate? A model to analyse the benefits of information sharing. In: Proceedings of the 2016 ACM on Workshop on Information Sharing and Collaborative Security. ACM, pp. 15–24.

[58] de Fuentes, J.M., González-Manzano, L., Tapiador, J., Peris-Lopez, P.,2016. PRACIS: privacy-preserving and aggregatable cybersecurity information sharing. Comput. Secur.

[59] Best, D.M., Bhatia, J., Peterson, E.S., Breaux, T.D., 2017. Improved cyber threat indicator sharing by scoring privacy risk. In: Technologies for Homeland Security (HST), 2017 IEEE International Symposium on. IEEE, pp. 1–5.

[60] Casey E, Back G, Barnum S (2015) "Leveraging CybOX to standardize representation andexchange of digital forensic information" Proceedings of the 2nd annual DFRWS EUConference, Digital Investigation, Volume 12, Supplement 1, Elsevier

[61] Chabot Y, Bertaux A, Nicolle C, Kechadi T (2015) "An Ontology-Based Approach for theReconstruction and Analysis of Digital Incidents Timelines" Digital Investigation:Volume 15, December 2015, Pages 83-100, Elsevier: London (DOI: 10.1016/j.diin.2015.07.005)

[62] Turner, P., September 2005a. "Unification of digital evidence from disparate sources (digital evidence bags)" proceedings of DFRWS2005. Digit. Investig. 2 (3), 223e228. Elsevier.

[63] Turner, P., 2006. Selective and intelligent imaging using digital evidence bags proceedings of DFRWS2006. Digit. Investig. 3 (Suppl.), 59e64. Elsevier.

[64] Eaglin, R., Craiger, J.P., 2005. Data sharing and the digital evidence markup language. In: Presented at 1st Annual GJXDM Users Conference, Atlanta.

[65] Lee, S., Park, T., Shin, S., Un, S., Hong, D., 2008. A new forensic image format for high capacity disk storage. Information Security and Assurance, 2008. ISA 2008. In: International Conference on Information Security and Assurance. IEEE Computer Society, 24e26 April.

[66] Levine, B.N., Liberatore, M., September 2009. DEX: digital evidence provenance supporting reproducibility and comparison. Digit. Investig. 6 (Suppl.), S48eS56. Elsevier.

[67] Flaglien, A.O., Mallasvik, A., Mustorp, M., Arnes, A., November 2011. Storage and exchange formats for digital evidence. Digit. Investig. 8 (2), 122e128.

[68] Garfinkel, Simson, 2009. Automating Disk Forensic Processing with SleuthKit, XML and Python. Systematic Approaches to Digital Forensics Engineering (IEEE/ SADFE 2009). California, Oakland.

[69] Garfinkel, S., 2012. Digital forensics XML and the DFXML toolset. Digit. Investig. 8, 161e174. Elsevier.

[70] Schatz, B., 1995. Digital Evidence: Representation and Assurance. PhD Dissertation. Queensland University of Technology. http://eprints.qut.edu.au/16507/1/Bradley_Schatz_Thesis.pdf .

[71] Cohen, M., Schatz, B., Garfinkel, S., September 2009. "Extending the advanced forensic format to accommodate multiple data sources, logical evidence, arbitrary information and forensic workflow. Proceedings of DFRWS2009 Digit. Investig. 6 (Suppl.), S57eS68. Elsevier.

[72] Office of the Director of National Intelligence, 2016. XML Data Encoding Specification for Intelligence Document and Media Exploitation. https://www.dni.gov/index.php/about/organisation/chief-information-officer/informationsecuritymarking-access?id¼1204.

[73] van Beek, H.M.A., van Eijk, E.J., van Baar, R.B., Ugen, M., Bodde, J.N.C., Siemelink, A.J., 2015. Digital forensics as a service: game on. Digital Investigation Special Issue Big Data Intelligent Data Analysis 15, 20e38. Elsevier.

[74] Alink,W., Bhoedjang, R., Boncz, P., de Vries, A., 2006. Xirafexml-based indexing and querying for digital forensics. In: Suppl. 1, Proceedings of the 6th Annual DFRWS Conference, Digital Investigation, vol. 3. Elsevier.

[75] Bhoedjang, R.A.F., van Ballegooij, A.R., van Beek, H.M.A., van Schie, J.C., Dillema, F.W., van Baar, R.B., et al., 2012. Engineering an online computer forensic service. Digit. Investig. 9 (2). Elsevier.

[76] Chabot, Y., Bertaux, A., Nicolle, C., Kechadi, T., December 2015. An ontology-based approach for the reconstruction and analysis of digital incidents timelines. Digit. Investig. 15, 83e100. http://dx.doi.org/10.1016/j.diin.2015.07.005 . Elsevier: London.

[77] Brady, O., Overill, R., Keppens, J., 2015. DESO: addressing volume and variety in large-scale criminal cases. Digit. Investig. 15, 72e82. Elsevier.

[78] Cosic, J., Baca, M., 2015. Leveraging DEMF to ensure and represent 5ws&1h in digital forensic domain. Int. J. Comput. Sci. 13 (2).

[79] Turnbull, B., Randhawab, S., June 2015. Automated event and social network extraction from digital evidence sources with ontological mapping. Digit. Investig. 13, 94e106.

[80] Neches, R., Fikes, R., Finin, T., Gruber, T., Patil, R., Senator, T., Swartout, W.R., 1991. Enabling technology for knowledge sharing. AI Mag. Winter 36e56.

[81] Studer, Benjamins, Fensel, 1998. Knowledge engineering: principles and methods. Data Knowl. Eng. 25, 161e197.