Cyber Threat Intelligence Sharing Platforms: A Comprehensive Analysis of Software Vendors and Research Perspectives

MASTER'S THESIS

Department of Information Systems, Production and Logistics Management |
Department of Computer Science
University of Innsbruck

for the Attainment of the Degree
Master of Science
in Information Systems

Advisor:
Clemens Sauerwein, PhD

Editor:
Tanja Staiger [11830428]

Innsbruck, [November 2021]

Table of contents

Abbreviations

API *Application Programming Interface*
CERT *Computer Emergency Response Team*
CIF *Collective Intelligence Framework*
CIRCL *Computer Incident Response Centre Luxembourg*
CRITs *Collaborative Research into Threats*
CSIRT *Computer Security Incident Response Team*
CTI *Cyber Threat Intelligence*
CTIS *Cyber Intelligence Information Sharing*
CVE *Common Vulnerabilities and Exposures*
CybOX *Cyber Observable eXpression*
ENISA *European Union Agency for Cybersecurity*
GUI *Graphical User Interface*
IDS *Intrusion Detection System*
IOC *Indicator of Compromise*
ISAC *Information Sharing and Analysis Center*
ISAO *Information Sharing and Analysis Organization*
ISIC *International Standard Industrial Classification*
LDAP *Lightweight Directory Access Protocol*
MISP *Malware Information Sharing Platform*
MLR *Multivocal Literature Review*
NIDS *Network Intrusion Detection System*
OpenCTI *Open Cyber Threat Intelligence Platform*
OpenIOC *Open Indicator of Compromise*
OSINT *Open Source Intelligence*
OTX *Open Threat Exchange*
REST-API *RESTful API*
SDK *Software Development Kit*
SIEM *Security Information and Event Management*
SLR *Systematic Literature Review*
SOAR *Security Orchestration, Automation and Response*
STIX *Structured Threat Information eXpression*
TAXII *Trusted Automated eXchange of Indicator Information*
TI *Threat Intelligence*
TIC *Threat Indicator Confidence*
TIP *Threat Intelligence Platform*
TIS *Threat Intelligence Sharing*
TISP *Threat Intelligence Sharing Platform*
TLP *Traffic Light Protocol*
TX *Facebook Threat Exchange*
UI *User Interface*
XFE *IBM X-Force Exchange*

List of figures

List of tables

Abstract

The use of threat intelligence to improve the cybersecurity of organizations is on the rise. Cyber-attacks are steadily increasing and becoming more sophisticated. Threat intelligence and threat intelligence sharing play a critical role in combating cyber-crime. Therefore, it is necessary to understand the concept and operation of threat intelligence sharing platforms.

This thesis aims to examine the current market for threat intelligence sharing platforms and compare the available solutions. Therefore, a multivocal literature review was conducted. Of the tools identified in the literature review, 13 threat intelligence sharing platforms were examined in detail using a framework of more than 50 criteria.

The analysis of the platforms revealed several commonalities and differences among the platforms. Most platforms support the entire process of sharing threat data. The platforms differ regarding their capabilities and automation options and their flexibility and compatibility with standards and systems. Aspects such as trust and data quality are not sufficiently addressed and should be part of future research.

1 Introduction

Cyberattacks and cybersecurity failure have been identified as high-likelihood and high-impact global risks of the next decade. Organizations of all types are concerned about rising threats in the form of cyberattacks, misinformation, targeted strikes, and resource grabs [1, 2]. The function, target, and scope of attacks and the motivation and tactics, techniques, and procedures (TTPs) of adversarial attacks are becoming increasingly sophisticated and unpredictable [3–5]. In addition, massive amounts of data and a shortage of analysts are currently shaping the cybersecurity landscape [6].

These developments raise awareness among organizations to address these threats and take proactive rather than reactive countermeasures [7–10]. Therefore, the concept of cyber threat intelligence (CTI) was established, including more complex analysis of existing cyber threat data. CTI provides input for tactical decisions to address cyber threats' increased number and complexity [3, 9, 10]. The concept of CTI is promising in that it counters targeted attacks with targeted defenses. Companies should be enabled to deal with business risks, transform unknown threats into known and mitigated threats, and thus improve the effectiveness of the defense [11]. A recent CTI survey[1] identified organizations to use CTI for threat detection (89%), threat prevention (77%), threat response (72%), and threat mitigation (59%) [12].

Due to the broad spectrum of cyber threats, the increasing number of attacks, and the data involved, it is nearly impossible for organizations to analyse and combat these threats independently. Instead, it requires collaborative relationships and the ability to build trusting relationships. Therefore, the concept of cyber threat intelligence sharing (CTIS) was developed to enable cross-organizational information sharing and to quickly implement remedial actions [7–10, 13, 14].

In the context of CTI, time is a critical component, and automation capabilities are needed to provide real-time information and increase the efficiency of CTIS. Starting with small ad hoc tasks performed and exchanged in an informal, manual manner (e.g., emails, web portals), CTI has evolved into robust programs that establish formal, (semi-)automated information exchange. However, implementing a CTI program that consumes and shares threat information on time is challenging for practitioners. According to [12], two-thirds of respondents still use manual sharing mechanisms in the form of email or documents (e.g., spreadsheets, PowerPoint) to disseminate CTI [10, 12, 15]. To address these issues and requirements, several taxonomies (e.g., CVE, CAPEC), sharing standards (e.g., STIX, MAEC, OpenIOC), and ontologies relevant to cyber threat intelligence have been developed [16]. Additionally, Dandurand et al. [17] introduced the concept of a knowledge management platform, which serves as the basis of today's threat intelligence sharing platforms (TISP).

TISPs aim to manage and process vast amounts of data and provide actionable intelligence to various stakeholders [3, 9]. Recently, an increasing need and interest in CTI sharing and TISPs has been observed in both research and practice. In the future, widespread adoption of TISPs is

[1] 2020 SANS Cyber Threat Intelligence (CTI) Survey: A CTI survey with n=1006 organizations, from various industries (e.g., Government, banking and finance, cybersecurity service provider, technology), different organizational sizes (small, medium, large), multiple roles (e.g. security operations/security analyst, incident responder, security managers or director).

expected, and the use of threat intelligence (TI) programs as part of proactive cybersecurity will become mandatory for organizations [10, 18, 19]. As the field grows rapidly, a heterogeneous market has emerged that includes various tools with different aims and capabilities. However, there is a lack of a unified definition and ontology that covers the full spectrum of the concept of cyber threat intelligence [16, 20].[2]

Several efforts have been conducted in this field within the past years, but research still seems to be in its infancy. From the practical perspective, the last years were shaped by growth regarding the implementation of threat intelligence platforms, the used indicators (e.g., hash values, TTPs), and the number of TI sources available. As the field settles into its new maturity, understanding and improving the effectiveness of CTI programs will become even more critical [12, 21].
Until now, several TISPs have been identified, analysed and a classification framework has been developed (e.g. [13, 19]). What is still lacking is a broad-based examination of existing TISPs using a comprehensive and broadly applicable framework.
This work aims to tie in with current research activities and to contribute to closing existing research gaps. For this purpose, a comprehensive overview and evaluation of different TISPs, including their characteristics and requirements, is provided. Following this, the results of this analysis and their implications for future research are discussed. The focus is on the following research questions: (a) What is the state-of-the-art of TISPs from a theoretical and practical perspective? (b) Which differences and similarities exist between TISPs? and (c) What are further research perspectives and challenges of TISPs?
In order to gain a broad knowledge base about TISPs and the TISP market, a comprehensive market survey in the form of a multivocal literature review (MLR) was conducted based on Kitchenham [22], Garousi et al. [23], and Islam et al. [24]. The findings obtained from the MLR were used to intensively analyse the platforms and finally classify them into the framework by [13]. The research led to 15 key findings discussed in terms of their implications for research and practice.

The remainder of this paper is structured as follows: Section 2 provides an overview of the topic, including relevant background information and related work. Section 3 describes the applied research methodology. Section 4 outlines the results of the literature review and the platform analysis. Section 5 discusses the key findings of the research, their implications, and limitations. The paper concludes with a summary and an outlook on future research.

[2] For this paper, the terms Threat Intelligence (TI) and Cyber Threat Intelligence (CTI), as well as Threat Intelligence Sharing (TIS) and Cyber Threat Intelligence Sharing (CTIS), are used synonymously. However, the topic of this thesis refers to the cyber domain.

2 Overview

The following chapter provides an overview of the theoretical foundations of this thesis. In addition to basic terms and background information on the underlying concepts, related work is also outlined.

2.1 Background information

A common understanding of the relevant concepts and terminologies is required when dealing with cyber threats and the associated data and information [16]. Therefore, the individual terms will be discussed in more detail.

2.1.1 Intelligence

When examining the concept of cyber threat intelligence, it is advisable first to consider the traditional notion of intelligence [3, 11]. So far, several approaches define the concept of intelligence (e.g., [3, 11, 25]).

Dealing with the concept of intelligence requires a deeper understanding of the underlying terms of data and information [3].
Data comprises captured and stored activities or situations in the form of symbols or signal readings. The utility of raw data itself is limited. Instead, data can be described as mere representation and storage of intrinsic meaning. The primary purpose of data is to record activities or situations, aiming to capture the true picture or real event [25, 26].
Processing the collected data into an understandable form creates more significant value in the form of *information*. Information contains relevant meaning, implications, or input for decisions and actions based on current and historical sources. Essentially, the purpose of information is to make decisions and solve problems or realize an opportunity [25, 26].
By linking information with other information and previous experiences in the environment, a new level of information is created, also known as *intelligence*. The base of the intelligence production process is that analysts relate or compare information to other information or databases and draw conclusions. Ultimately, intelligence has two critical properties that distinguish it from information. Intelligence enables anticipation or prediction of future situations and circumstances, and it informs decisions by illuminating differences in available courses of action. Regardless of the situation, intelligence assessments and estimates enable plans to be formulated and better decisions based on that knowledge. Thus, predictive, accurate, and relevant intelligence can mitigate cyber domain risks and increase success. In this context, intelligence encompasses the organizations, capabilities, and processes involved in collecting, processing, exploiting, analyzing, and disseminating information or actionable intelligence [25].

After reviewing several concepts and approaches, Abu et al. [3] summarize intelligence as a process by which collected data from the operational environment is processed and refined to produce information. Finally, this information is analysed and converted into an actionable format called intelligence.

A visual representation of the relationship between operational environment, data, information, and intelligence is additionally shown in Figure 1.

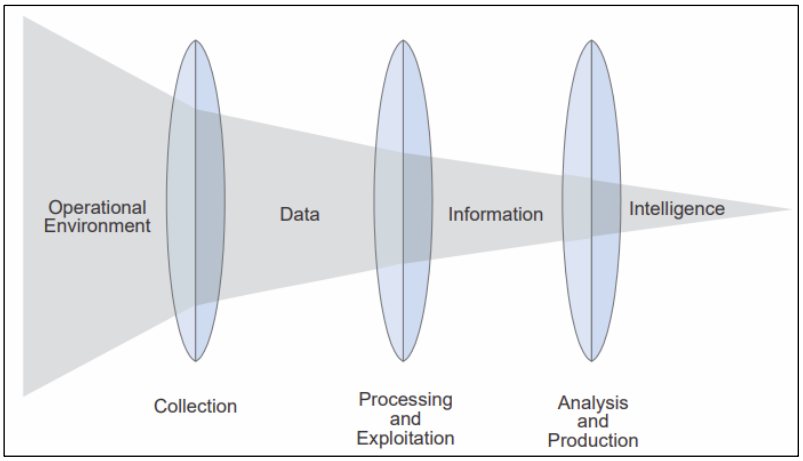


Figure 1: Relationship of Data, Information, and Intelligence [25].

2.1.2 (Cyber) Threat Intelligence

Regarding the cyber domain, a threat describes the possibility of someone accessing or disrupting an information network without being authorized to do so [6]. However, there is not yet a universally accepted, standard definition for the term cyber threat intelligence, in part due to the inconsistent use of the terms threat intelligence and cyber threat intelligence in research and practice. Moreover, researchers tend to define and adapt the term depending on the work environment and situation [3].

Several efforts have been made to define threat intelligence [3, 9, 11, 27–32]. The essence of all approaches implies that threat intelligence is simply traditional intelligence applied to cyber threats [11]. TI refers to more complex, evidence-based cyber threat information or data about existing or emerging threats gained through collecting, processing, and analyzing existing information about the capabilities, opportunities, and intent of advisories. These insights are used to illuminate the risk landscape or aid decisions to prevent or mitigate an attack on time [3, 9, 11, 12, 28]. According to Abu et al. [3], relevant, timely, and actionable intelligence must always be the end goal of the threat intelligence lifecycle to improve cybersecurity.

As depicted in Figure 2, another approach to describe threat intelligence is based on the concept of ‘knowns’ and ‘unknowns’. An ‘unknown unknown’ can be described as a threat with no awareness that the threat exists. With a ‘known unknown,’ there is an awareness that an attack will occur without details about the threat (e.g., who, why, when, how). 'Known knowns' describes threats whose existence and details are known. Intelligence refers to the process of moving from ‘unknown unknowns’ to ‘known unknowns’ by detecting the existence of threats and then shifting ‘known unknowns’ to ‘known knowns’ where the threat is well understood and mitigated [11].

Figure 2: Concept of 'knowns' and 'unknowns' [11].

Threat data comes from various internal and external sources, allowing an organization to create the most relevant and accurate threat profile possible. Internal sources comprise threat data from the organizations' network sensors (i.e., event logs, DNS logs, firewall logs). External sources include intelligence from open source (OSINT), private sources, or commercial sources (e.g., indicators, feeds, structured and unstructured reports). External sources can vary widely, especially in terms of their trustworthiness [4].

As shown in Figure 3, different types of TI can be distinguished, including strategical TI, operational TI, tactical TI, and technical TI Figure 3[11, 32]:

- *Technical TI* includes data and information in the form of Indicator of Compromises (IOCs) (e.g., IP addresses, MD5 hashes). IOCs contain various information about a particular threat in the form of logically grouped sets. In addition, IOCs can help detect historical attacks and are also used for analysis tools, visualizations, and dashboards. This type of TI often has a short lifespan and therefore needs to be consumed automatically. Technical TI is regularly consumed by technical means, i.e., by feeding it into an organization's defensive infrastructure (e.g., firewall, mail filtering devices) [11, 32, 33].
- *Tactical TI* is often referred to as TTPs and includes information on how threat actors conduct attacks (attackers' methods, tools, and tactics). This type of TI is used to prepare defenses, alerts, and investigations for current tactics. This TI is available through white papers, trade press, communication with colleagues in other organizations, or purchase from a provider of such intelligence. Tactical TI is regularly consumed by defenders and incident responders [11, 32].
- *Operational TI* includes information about specific imminent attacks against an organization. This type of TI is rare and difficult to obtain. In most cases, only governments have access to this type of TI, while private entities often cannot access attack groups and their infrastructure legally. However, in some cases (e.g., attacks by more public actors), operational TI can be accessed through open-source intelligence or vendors with access to closed chat forums. Operational TI is typically consumed by higher-level security staff, such as security managers or incident response leaders [11, 32].
- *Strategic TI* includes high-level information, mainly in the form of reports, briefings, conversations, and others. Strategic TI helps understand current risks, identify additional risks, and mitigate attacks. Typically, this form of TI is non-technical and focuses on issues that support high-level decisions (e.g., financial impact, attack trends) [11, 32].

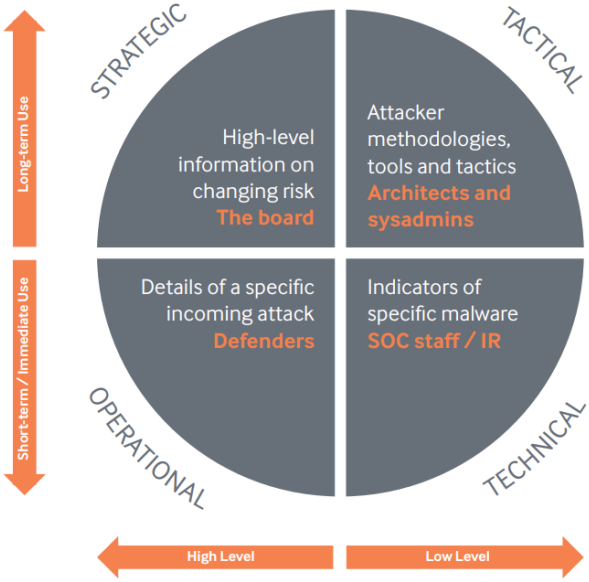


Figure 3: Subtypes of threat intelligence [11].

2.1.3 Threat Intelligence Sharing and Standards

The cyber threat landscape is constantly changing. To help organizations keep pace with these developments, the concept of threat intelligence sharing has evolved. TIS enables information sharing between different parties regarding evolving threats and vulnerabilities [7, 8, 10]. The exchange of threat information enables organizations to leverage collective knowledge and enrich existing information. By analysing and correlating different sources, better situational awareness and a deeper understanding of the threat landscape can be gained. Additionally, easier identification of sector-specific or cross-sector campaigns is enabled. This should improve the quality of threat information and more efficient detection and remediation strategies [34, 35].

Threat intelligence sharing can occur either formally or informally in an automated or manual manner (emails, meetings, phone calls, shares databases, web portals, data feeds). The first category distinguishes API-based automated sharing, private websites, or via a secure portal. Informal sharing is carried out by personal meetings, public websites, notifications, or teleconferences [10, 15, 36].
Successful, efficient, and timely exchange of TI requires structured, automated information exchange [10, 37]. This requires common representation, standard formats, and exchange protocols to solve interoperability issues between peers and facilitate the exchange of threat information in a standardized, automated manner [3, 16, 32].
Several ontologies and standards have been developed by organizations such as MITRE, MILE, Mandiant, and others (e.g., CAPEX, CybOX, IODEF, MAEC, OpenIOC, RIF, STIX, TAXII, VERIS). These standards can facilitate and accelerate the exchange of information between organizations [3, 32, 37, 38]. While some standards overlap, some were developed for specific purposes. An organization may use one or more standards depending on individual requirements [3].

The most common and popular standards are STIX, TAXII, CybOX, and OpenIOC [20].
The *Structured Threat Information eXpression (STIX)* standard is a structured, machine-readable language and serialization format developed by MITRE and now maintained by OASIS. The

standard was developed specifically for capturing and exchanging threat information and enables organizations to exchange TI in a consistent and machine-readable manner. The following 18 core constructs are provided for this purpose, which STIX can represent: Attack Pattern, Campaign, Course of Action, Grouping, Identity, Indicator, Infrastructure, Intrusion Set, Location, Malware, Malware Analysis, Note, Observed Data, Opinion, Report, Threat Actor, Tool, and Vulnerability. This is expected to improve automated threat sharing, collaborative threat analysis, and automated defence and response, among other capabilities. STIX is designed quite flexibly, allowing integrations to various tools and systems. The language of STIX is dependent on the version, either XML or JSON. The current version of the standard is STIX 2.1 (JSON) [36, 39–41].

The *Trusted Automated eXchange of Indicator Information (TAXII)* standard is an application layer protocol developed by MITRE and now maintained by OASIS. TAXII enables easy and scalable transport of threat information. Therefore, a set of services and message exchanges are defined in a RESTful API (REST-API). TAXII was explicitly developed for compatibility with STIX and the TI it represents, but both standards can be used independently. In addition, several transport mechanisms are compatible with STIX, and TAXII can also transport threat data in other formats. Therefore, TAXII supports three threat sharing models: Hub-and-Spoke, Peer-to-Peer, and Source-Subscriber. The current version of the standard is TAXII 2.1 [42, 43].
The *Cyber Observable eXpression (CybOX)* standard developed by MITRE is a structured language for representing cyber observables. Since its integration into STIX 2, CybOX no longer serves as a stand-alone language. Within STIX, CybOX is represented as a Cyber Observable Object to define a structured representation for observable objects in the cyber domain [20, 44].
The *Open Indicator of Compromise (OpenIOC)* standard developed by Mandiant serves as a framework in a standardized, structured, and machine-readable format (XML). OpenIOC allows various types of threat information to be recorded, defined, and exchanged. In addition, OpenIOC, described as an open and flexible standard, can be easily converted or parsed into other formats [33].

As mentioned earlier, several sharing models represent the architecture of how TI is shared between providers and customers [45]. As depicted in Figure 4, the following sharing models have been identified in research:

- The *peer-to-peer* architecture enables ad-hoc exchange and interaction between all entities in a community. There is no intermediary to regulate and coordinate the exchange. Organizations can share information directly with each other with a high degree of choice and freedom [36, 46].
- The *hub-and-spoke* model involves a central clearinghouse (hub) to coordinate information sharing. Members of the community (spokes) can produce and consume information shared and redistributed through the hub. This model enables the centralization, formalization, and influence of information sharing between organizations [36, 46].
- In the *source-subscriber* architecture, all information is pooled exclusively at one organization, passing the information on to the subscribers [46].

White et al. [36] also identified a *hybrid* approach of the peer-to-peer model and the hub-and-spoke model, where exchanges occur depending on the type of threat intelligence.

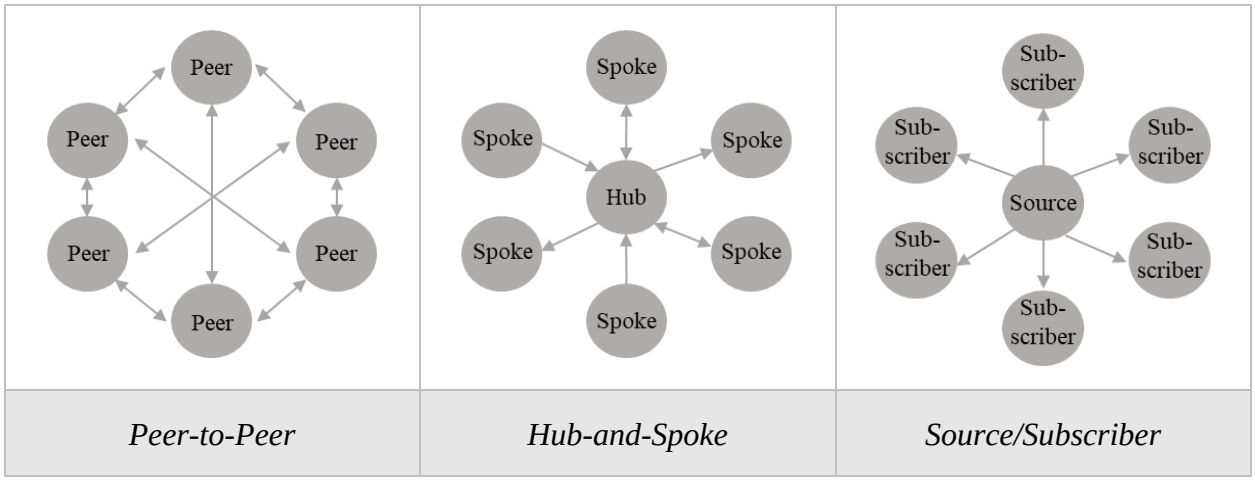


Figure 4: Sharing Models (Own representation based on [46]).

2.1.4 Threat Intelligence Sharing Platforms

Today's cyber threat landscape faces an overabundance of threat data and the challenge of shifting threats to known-knowns. To address these issues, various tools are offered under the buzzword ‘threat intelligence’. Some of the products and services offered vary widely in scope, usability, objectives, and content and range from deep dark web monitoring to IOC analysis and vulnerability management [11, 15]. However, most of these tools do not consider threat intelligence sharing and offer few integration options [6]. Therefore, threat intelligence sharing platforms have been developed to manage vast amounts of data and support automated threat intelligence sharing. Furthermore, these platforms process the provided data to provide various tools and stakeholders with actionable intelligence [3, 9, 37]. The previously outlined standardization efforts facilitate this exchange and serve as the basis for threat intelligence sharing platforms [3, 19].

The cornerstone of today's TISPs was first presented in 2013 by Dandurand and Serrano [17], who introduced the concept of a knowledge management platform specifically for cyber security threat intelligence (Cyber Security Data Exchange and Collaboration Infrastructure). The core idea and requirement of the proposed concept is to support organizations by providing means to facilitate information sharing and support data generation, refinement, and vetting by enabling automation and collaboration capabilities.

De Melo et al. [20] describe the main task of a threat intelligence platform (TIP) based on the intelligence production process. Considering the requirements for actionable intelligence to be timely, accurate, and relevant, the authors extended the general intelligence production process [31]. As shown in Figure 5, in addition to the three phases (1) Collect, (2) Process, and (3) Analyse, the two phases (4) Deploy and (5) Disseminate were added.

(1) Collection: comprises the gathering of threat data (e.g., indicators, facts)
(2) Processing: includes processing and combining data to transform data into information
(3) Analysis: evaluates data and information to gain actionable intelligence
(4) Deploy: use of the generated intelligence
(5) Dissemination: sharing the intelligence generated [20].

The overarching goal of a TISP is to provide a holistic decision-making foundation for organizations. Therefore, the TISP ideally provides support for all five phases of the threat intelligence production process. The number of platforms that can meet these criteria increases, contributing to faster and better threat detection [21, 28, 47]. These platforms are partly complementary and can be used together, e.g., to combine outputs and thus create the broadest possible information base [32].

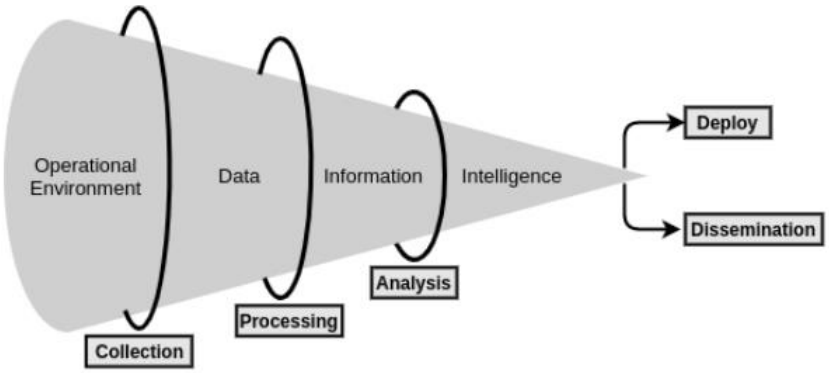


Figure 5: Threat Intelligence Production Process Flow [20].

There is inconsistent use of the terms Threat Intelligence Platform, Threat Intelligence Sharing Platform, Cyber Threat Intelligence Platform, and Cyber Threat Intelligence Sharing Platform in research. This is partly due to the lack of a general definition. In the remainder of this article, the terms will be used interchangeably, but the focus will be on platforms that meet the above requirements of Dandurand and Serrano.

2.2 Related work

Although the field of threat intelligence sharing and threat intelligence sharing platforms is relatively young, several efforts have been made over the past decade to make this field more accessible.

In 2008, Brown et al. [48] published a paper in which they examined the concept of information security and its various ontologies. The authors found a lack of reusability, communication, and knowledge sharing within the security community. Building on this, Dandurand and Serrano [17] recognized the need for improved knowledge management, information sharing, and information automation in cybersecurity. In 2013, they published a paper introducing the concept of Cyber Security Data Exchange and Collaboration Infrastructure and establishing eleven high-level requirements. Particular emphasis was placed on collaboration capabilities and quality assurance of shared data. This concept represents the cornerstone of today's TISPs.

Since then, several papers have been published that analyze different tools declared as threat intelligence according to different criteria. The various works differ in terms of their approach, focus, and perspective.

In 2014, Serrano et al. [49] published a paper about cyber security information sharing, where some essential information about four platforms is provided. However, no set of criteria has been applied. In 2017, Sauerwein et al. [19] conducted an exploratory study in the form of workshops and an MLR. As a result of their market study, 22 open- and closed-source platforms have been

analysed. The platforms have been analysed and compared according to 11 criteria: Licensing model, use cases, supported standards, supported threat intelligence constructs, shared information/threat intelligence, sharing functionalities, collaboration capabilities, integration capabilities, analysis, deployment, and provided user interfaces. In 2017 and 2018, Wagner et al. [50, 51] published two studies, analysing the same set of 30 open- and closed-source platforms. While one study analysed the platforms in terms of relevance filtering methods, the other focuses on anonymity. In 2018, Tounsi et al. [32] published a comprehensive paper on cyber threat intelligence that focused explicitly on technical threat intelligence. In the course of this work, six open- and closed-source platforms were examined based on seven criteria: Import format, integration with/export to standard security tools, support of collaboration, data exchange standards, analysis, graph generation, license. In their paper published in 2019, Keim et al. [52] propose an improved cyber threat intelligence framework. Therefore, the authors analysed four open-source platforms relating to information such as features, methods of countermeasures, language specification of the threat indicators, license type, owning organization. Furthermore, a set of nine requirements addressing import and export capabilities, data sharing capabilities, automation capabilities, and efficacy of CTI feeds is considered. Following [32], Faiella et al. [53] published a paper in 2019 in which they presented an enriched threat intelligence platform. For this purpose, four open-source solutions were analysed and compared based on the following eight criteria: Import/export format, integration capabilities, data exchange standards, support of collaboration, analysis capabilities, graph generation, license, hardware requirements. In 2020, de Melo et al. [20] published a paper proposing a methodology for evaluating standards and platforms for cyber threat intelligence. As part of the research, five open-source platforms were examined according to the following ten criteria: import formats, automatic gathering, export format, graphic visualization, correlation, classification, integration, sharing method, documentation, and license model. In 2020, Menges et al. [54] published a paper presenting a blockchain-based, decentralized platform for sharing cyber threat intelligence. For this, six platforms have been analysed according to the following seven criteria: Platform availability, data availability, integrity, non-repudiation, incentives, fairness, quality assurance. In 2020, Noor et al. [15] published their work in which they proposed a framework for ranking CTI service providers based on weighted evaluation criteria. The research is based on an MLR. The authors analysed 14 open- and closed-source platforms within their work according to the following nine criteria: Information sharing model, sharing mechanism, security services, information source, company size, security threats, information type, sharing frequency, and monthly cost. Additionally, the authors ranked the platforms according to customer requirements.

In 2020, Bauer et al. [13] published a classification framework that allows detailed descriptions and comparisons of TISPs. The development of the framework and its criteria is based on an SLR, which was used to identify the requirements and characteristics of TISPs.
From a higher-level perspective, the framework distinguishes between two categories of criteria: functional and non-functional criteria. These two categories are divided into six sub-categories, which in turn are divided into 25 criteria and 56 sub-criteria.
Functional criteria are differentiated into two sub-categories: Phases of TIS and Cross-phase support. These sub-categories are in turn divided into the following criteria and *sub-criteria*, listed in Table 1.

Table 1: Framework – Functional criteria.

	Functional criteria
Phases of TIS	The authors summarized the phases of the TI production process flow (Figure 5) into four phases: • Collection of TI ▪ *Available Functions (functions a platform provides to support a phase)* ▪ *Degree of Automation (fully-automated, semi-automated, manual)* • Aggregation of TI ▪ *Available Functions* ▪ *Degree of Automation* • Analysis of TI ▪ *Available Functions* ▪ *Degree of Automation* ▪ *Visualization (if results can be displayed visually)* ▪ *Rating/ Prioritization (options to rate or prioritize TI)* • Dissemination of TI ▪ *Available Functions* ▪ *Degree of Automation* ▪ *Dissemination Mechanism (push [originator of TI disseminates information], pull [platform user launches the dissemination])* ▪ *Real-Time Capacity (share TI in real time)*
Cross-phase support	Functions that comprise more than one phase: • Information security ▪ *Available Functions (measures to protect confidentiality, integrity and availability of information and services e.g., encryption mechanisms)* • Data privacy ▪ *Available Functions (to enforce data privacy rules)* ▪ *Supported Countries/ Federations (consideration of regulatory differences)* • Data quality ▪ *Available Functions (control mechanisms to ensure data quality)* • Trust ▪ *Available Functions (mechanisms to enhance trust e.g., reputation mechanisms)* • Import and export ▪ *Available Functions (to import and export platform content)* ▪ *Supported Import and Export Standards* • Collaboration ▪ *Available Functions (to support collaboration between platform user)* ▪ *Anonymity Levels (anonymously, pseudonymously, publicly)* ▪ *Exchange Channels (privately, publicly, in communities)* • Reporting ▪ *Available Functions (reporting mechanisms)* ▪ *Filtering (to customize reports)* ▪ *Form (visual, textual)* • Additional functions (further salient functions)

Non-functional criteria are differentiated into four sub-categories: Architecture & Interfaces, Content & Standardization, Provider & Users and Usage Fees, License & Distribution. These sub-categories are in turn divided into the following criteria and *sub-criteria*, listed in Table 2.

Table 2: Framework – Non-functional criteria.

Non-functional criteria	
Architecture & Interfaces	• Type of platform (operational, software to build) • Architecture (on which the platform is based e.g., client-server, peer-to-peer, hub and spoke) • APIs ▪ *Types of APIs (offered by the platform)* ▪ *Supported IT Systems (which can be integrated into the platform e.g., incident management system)* • User interface ▪ *Types (graphical user interface (GUI), command line)* ▪ *Languages (in which the user interface is available)*
Content & Standardization	• Data origin (internal [generated by platform provider or platform users], external [generated from third parties]) ▪ *Number of Internal and External Sources* ▪ *Type of External Data Sources (public, commercial)* • Threat intelligence ▪ *Content Type (objects described by the platform e.g., IOCs, TTPs)* ▪ *Content Form (structured, unstructured)* ▪ *Content Language (in which TI is expressed)* • Standardization ▪ *Description Standards (e.g., STIX)* ▪ *Exchange Protocols (e.g., TAXII)* ▪ *Standard Extensions (published by the platform)*
Provider & Users	• Provider ▪ *Sector (21 International Standard Industrial Classification (ISIC) categories)* ▪ *Location (where provider resides)* ▪ *Organization Size (small, medium, large)* ▪ *Role (if the provider uses the platform or acts as an intermediary)* • User ▪ *Sector* ▪ *Location* ▪ *Organization Size* ▪ *Number of Users* ▪ *Number of Active Users (who regularly uses the platform)*
Usages Fees, License & Distr.	• Usage fees ▪ *Non-Recurring* ▪ *Recurring* • License (open sources, closed source) • Geographical focus (regional, national, international, global) • Sectoral focus (specific industrial sector, multi-sector focus)

The applicability of the framework was successfully demonstrated by the authors on a subset of 10 TISPs. However, only three platforms are presented in detail within the associated publication.

To date, there has been a lack of systematic and broad-based analysis of platforms based on a comprehensive and well-founded framework. Apart from the presented work by Bauer et al., there is no comparable framework for categorizing TISPs to date.
The present work represents a continuation and extension of previous research. In terms of research objective and methodology, the present work is similar to Sauerwein et al. The added value of this work lies in its connection with the findings of Bauer et al. For this purpose, this work uses the proposed framework to classify a set of platforms. Furthermore, this work conducts an MLR that incorporates the practice perspective, whereas the work of Bauer et al. is based on a literature review including only academic sources.

3 Applied research methodology

The applied research methodology is based on an MLR, serving as foundation for the subsequent analysis and comparison of TISPs. An MLR is an extended form of a systematic literature review (SLR), a secondary study whose goal is to provide a scientific knowledge base relevant to a specific research question, topic, or phenomenon of interest [22, 55].

MLRs and SLRs differ in terms of the sources that are included in the research process. SLRs focus on academic, peer-reviewed papers to provide a broad overview of state of art on a particular topic [23, 55]. However, especially in software engineering, experts often publish essential information about their experiences and opinions in grey literature (e.g., white papers, websites, blogs) [23]. An MLR allows for a broader source base that incorporates the state of practice on a given topic by including grey literature. Within the cybersecurity marketplace, which is characterized by different tools and functionalities, the inclusion of this perspective is critical to bridging the gap between practice and academic research [23, 55]. Likewise, within the TISP market, characterized by various tools and functionalities, this perspective is crucial to close the gap between practice and academic research.

The MLR for this work was conducted between October and December 2020 and is based on Kitchenham [22], Garousi et al. [23], and Islam et al. [24]. The following procedure was applied and adapted to the characteristics and requirements of this work: Search strategy, paper, and platform selection, data extraction and platform analysis. The entire MLR process is shown graphically in Figure 6 and is explained in detail below.

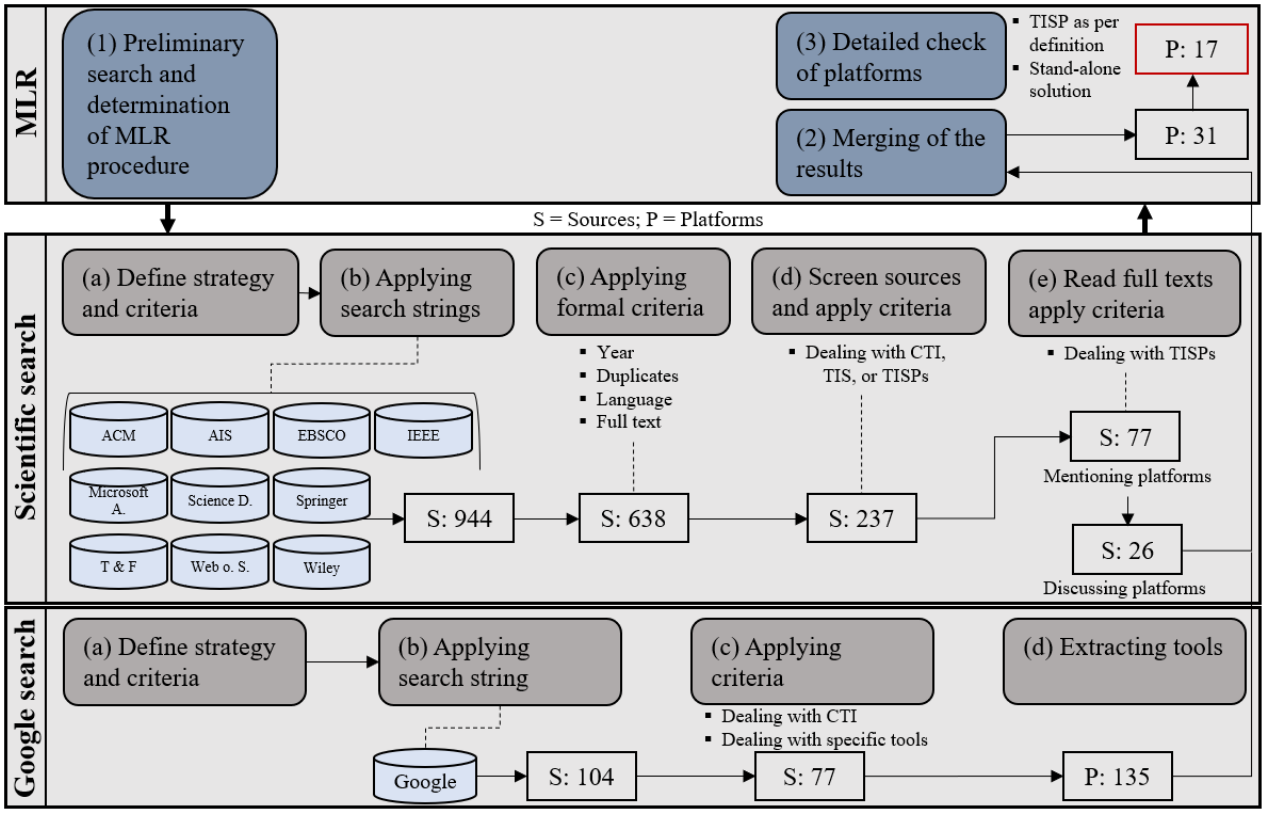


Figure 6: MLR process. Own representation based on [24].

3.1 Search strategy

Prior to the core research of this thesis, a preliminary search was conducted. To gain some basic knowledge of the topic and determine the research approach, a Google search was conducted using the keyword ‘Cyber Threat Intelligence Sharing Platform’. Based on these insights, the exact structure of the following research was defined.

The core research conducted is divided into two parts. The first part aims to identify scientific literature dealing with threat intelligence and threat intelligence sharing, focusing on sources that discuss specific platforms. The second part involves an ordinary Google search to identify all currently available and most widely used TISPs on the market.
Due to the lack of a general definition within the TI domain, the search string was defined quite generally and extensively. In addition, due to the peculiarities of some search engines, the search string had to be partially adapted for the academic search. Within the Google search, synonyms and extended strings (e.g., ‘cyber threat intelligence platform’, ‘threat intelligence sharing platform’, academic search string) were also considered, but the most promising hits were obtained by using a more general search term.

1. Academic search:
    a. ACM Digital Library, AIS Electronic Library, EBSCOhost, IEEE Xplorer Digital Library, Microsoft Academic Search, Taylor & Francis Online, Web of Science, Wiley Online Library:
    (threat OR cyber (threat OR security)) AND (intelligence OR information OR knowledge OR data) AND (sharing OR platform OR service OR tool OR system OR software)
    b. SpringerLink:
    "threat intelligence platform" OR "threat intelligence sharing" OR "threat intelligence tool" OR "threat intelligence software" OR "threat intelligence service" OR "threat intelligence system" OR "security intelligence sharing" OR "threat knowledge platform" OR "threat knowledge sharing"
    c. ELSEVIER ScienceDirect:
    (Cyber Security OR Threat OR cyber threat) AND (Intelligence OR Information OR Data OR knowledge) AND Sharing (Platform OR Tool)
2. Google search*: threat intelligence platform*

In order to create the most comprehensive base of sources possible, the following databases were used: ACM Digital Library, AIS Electronic Library, EBSCOhost, ELSEVIER ScienceDirect, IEEE Xplorer Digital Library, Microsoft Academic Search, SpringerLink, Taylor & Francis Online, Web of Science, Wiley Online Library, and Google.

3.2 Paper and platform selection

The following section describes in detail the procedure applied to select all relevant sources and tools from the scientific search and the Google search. Furthermore, the results of both searches are combined to obtain a final list of platforms for further analysis.

Scientific search:

For the scientific search, depending on the database, the search string was applied in abstract, keywords, title, and full text. This resulted in a total of 944 hits. To identify all relevant sources from this pool, the inclusion and exclusion criteria listed in Table 3 were applied.

Table 3: Exclusion and inclusion criteria for scientific search.

Exclusion criteria	Inclusion criteria
▪ older than 2010 ▪ duplicates ▪ no full text available ▪ not in English language ▪ not addressing organizational cyber security ▪ not dealing with CTI or TIS or TISP	▪ providing detailed information about a TISP ▪ in addition, sources of general information on CTI, TIS, and TISPs are included for background and related work

The elimination of all duplicates, sources not in English language, older than 2010, or not available as full text resulted in a pool of 639 sources. After reviewing the title, abstract, and full text of the remaining sources, 237 sources were identified that address CTI. Extracting all the tools mentioned in the 77 sources resulted in a list of 117 tools which can be found in Appendix A.1. Of the 77 sources, 26 sources provide detailed information about specific platforms. Extracting the tools discussed in detail, resulted in a list of 58 tools that can be found in Appendix A.2., including the frequency with which each tool is mentioned in the 26 sources.

Google search:

A similar procedure was used for Google search. The application of the search string resulted in tens of thousands of hits. Due to decreasing relevance of sources and quality issues with grey literature, the procedure was based on [56]. The principle of theoretical saturation was applied as a stopping criterion within this Google search. Therefore, the search was limited to the first ten pages because, after the tenth page, no more added value by additional sources was recognizable. This resulted in 104 sources. Due to two error messages, 102 sources remained. These sources were reviewed using the exclusion and inclusion criteria listed in Table 4:

Table 4: Exclusion and inclusion criteria for Google search.

Exclusion criteria	Inclusion criteria
▪ not dealing with CTI	▪ dealing with specific tools

This procedure resulted in the identification of 77 relevant sources, from which 135 tools were extracted, listed in Appendix A.3.

Concerning quality issues in grey literature, the use of traditional selection criteria is usually not sufficient. Several works provide insights and recommendations for assessing the quality of grey literature (e.g., [24, 56]). In the context of this work, the goal of the Google search is to obtain a list of all CTI tools currently available on the market. Therefore, the focus is on the mention of platforms and not primarily on the overall quality of the source. Apart from that, the identified sources of Google search are not used in detail.

Combination:

In order to obtain a final list of platforms to be included in the study, it was necessary to validate the quality or actual relevance of the identified tools for this work. Therefore, the starting point for merging the results are the 58 tools discussed in detail in the scientific search and the 135 tools identified in Google search. The next step was to identify all platforms that are mentioned in the Google search and discussed in the scientific search or tools discussed in more than one source in the scientific search. This resulted in a list of 31 platforms subjected to further examination according to the criteria listed in Table 5.

Table 5: Exclusion and inclusion criteria for tools.

Exclusion criteria	Inclusion criteria
▪ not addressing CTI	▪ TISP as defined by [17] ▪ stand-alone solution

The application of the listed criteria resulted in a list of 17 platforms, attached in Appendix A.4. However, after a thorough review, further restrictions and exclusions of platforms had to be made. This applies to Flashpoint, HP Threat Central, MANTIS, and SoltraEdge. These platforms can still be found in some publications, especially older ones. However, the platforms no longer exist in their original form and are therefore not included in the research.
The Flashpoint Intelligence Platform [57] does not provide the basic functionalities of a TISP. Flashpoint provides a collection engine, a data pipeline, and an analytics engine to process TI. However, these functionalities take place outside the platform. From the given information, it was concluded that the platform only serves as a distributor of the given information. In the case of HP Threat Central, further investigation revealed that there is no current information about the platform. No homepage could be identified, and the last product sheet provided by HP dates back to 2015 [58]. The MANTIS (Model-based Analysis of Threat Intelligence Sources) framework [59] is no longer in service. The functionalities of the platform are now provided by MISP [60]. SoltraEdge has been taken off the market in 2017 [61].

Furthermore, ambiguities have arisen regarding LookingGlass, which is referred to as LookingGlass and LookingGlass scoutPRIME in scientific search and identified as LookingGlass scoutPRIME and LookingGlass scoutTHREAT in Google search. For simplicity, LookingGlass is presented as one platform in the following, and a more precise distinction is made in 4.2.

Taking these circumstances into account, a final list of 13 platforms remains, which will be the subject of further investigation.

3.3 Data extraction and platform analysis

Threat intelligence sharing platforms provide insights into the practical perspective of cyber threat analysis and sharing. Based on the previously conducted MLR, 13 platforms were extracted. To obtain a comprehensive and comparable view of TISPs and answer the defined research questions, the following approach was used.

For each platform, a detailed analysis and classification of relevant works and additional sources was performed in order to subsequently extract all useful information. For this purpose, as shown in Figure 7, an Excel spreadsheet was developed using the 56 criteria of the previously presented framework [13] as columns to classify all relevant information of the identified sources. Furthermore, information that was not yet included in the framework but was deemed relevant was also extracted. In addition to the identified sources from the MLR, a targeted Google search was conducted for each platform to obtain additional information (e.g., vendor pages). A separate sheet was used for each platform, and the results were summarized in a summary table.[3]

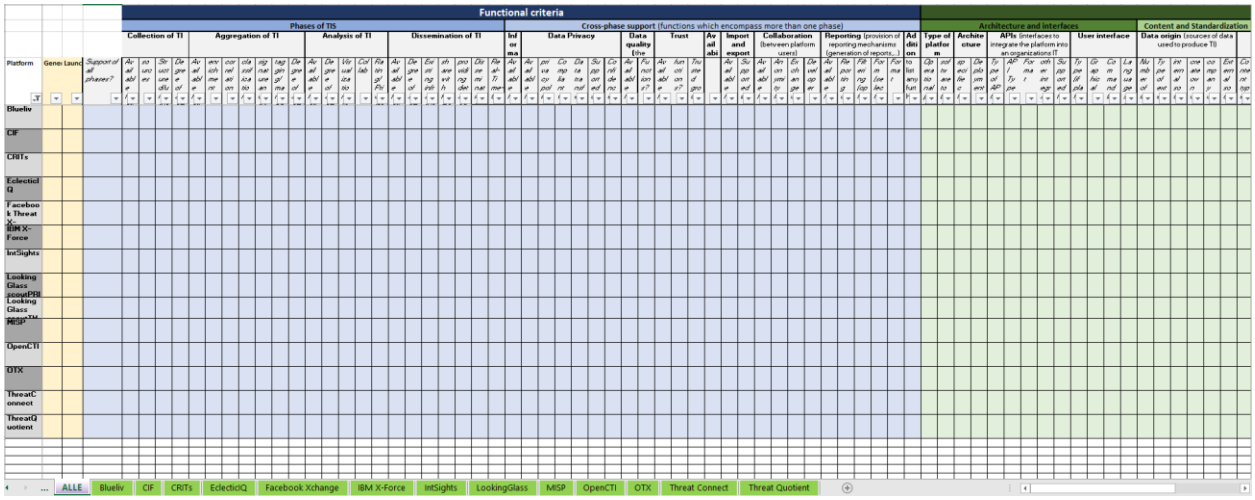


Figure 7: Excel spreadsheet for platform analysis.

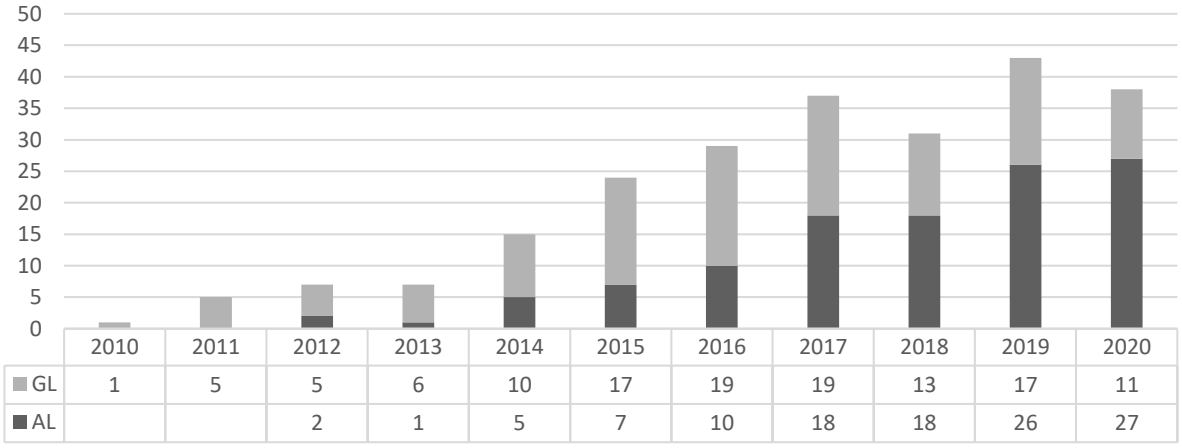
[3] The Excel spreadsheet with the summary table can be found here: https://ifi-nabu.uibk.ac.at/index.php/s/bCZ8QML6SsaRtxQ (Password: TISP2021!)

4 Results

This section presents the results of the research conducted. First, the main results of the literature review are outlined, including some statistics. Then, the results of the platform analysis are presented.

4.1 Literature review

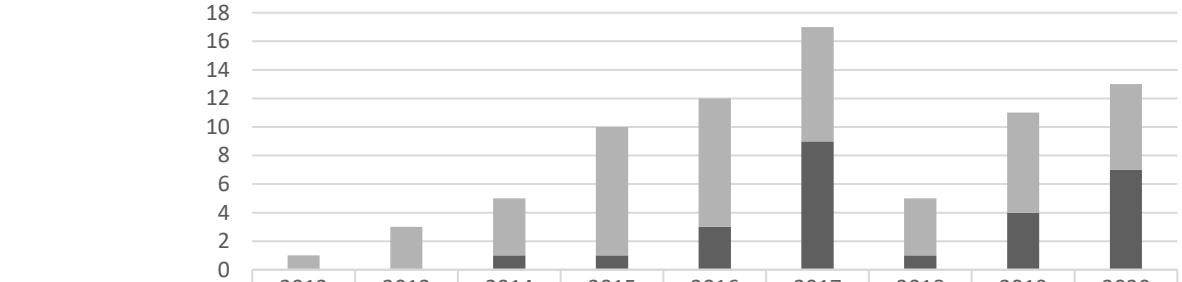
Within the scientific search, 237 sources were identified dealing with CTI. The number of sources per year is shown in Figure 8. In addition, the share of academic literature (articles from journals, conferences or workshops, books) and grey literature (patents, periodicals, dissertations, government documents, news, reports) is shown.



	2010	2011	2012	2013	2014	2015	2016	2017	2018	2019	2020
GL	1	5	5	6	10	17	19	19	13	17	11
AL			2	1	5	7	10	18	18	26	27

Figure 8: CTI literature per year and source type.

Figure 9 shows the distribution of the sources mentioning and discussing platforms by year.



	2012	2013	2014	2015	2016	2017	2018	2019	2020
Mentioning platforms	1	3	4	9	9	8	4	7	6
Discussing platforms			1	1	3	9	1	4	7

Figure 9: Sources mentioning and discussing platforms per year.

Furthermore, Figure 10 shows the distribution of AL and GL within the previously distinguished sources. Extracting the tools that are either mentioned or discussed, leads to a list of 117 resp. 58 tools (Figure 11).

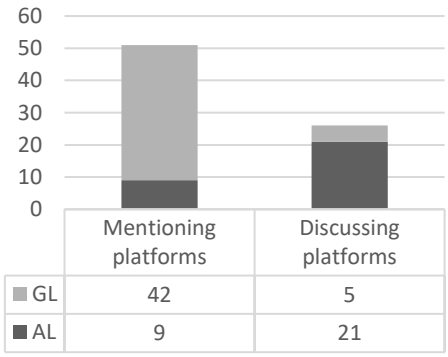


Figure 10: Type of sources mentioning and discussing platforms.

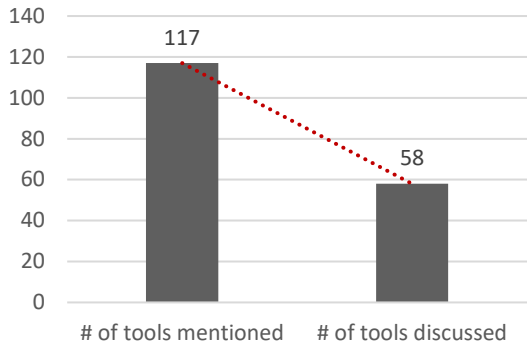


Figure 11: Number of identified tools (mentioned/discussed).

Within the Google search, most of the sources are grey literature (websites, vendor pages, advertising), shown in Figure 12. Of the identified 102 sources, 77 sources are dealing with specific TISPs (Figure 13).

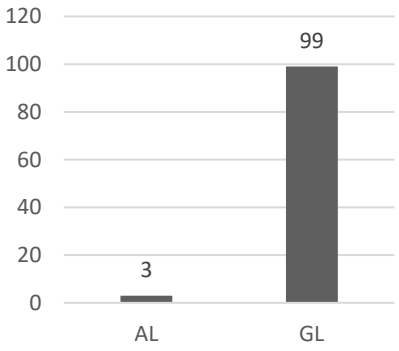


Figure 12: Type of Google source.

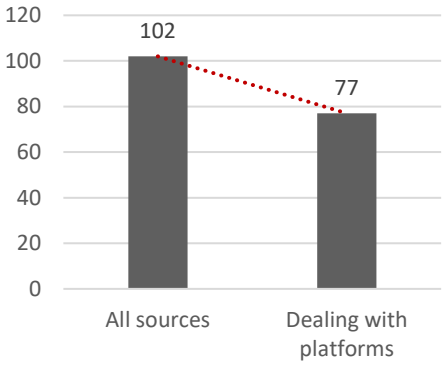


Figure 13: Sources dealing with platforms.

Merging the results of the scientific search and the Google search and applying further criteria as described in Section 3.2 resulted in a final list of 13 platforms.

Blueliv Threat Compass, Collective Intelligence Framework (CIF), Collaborative Research into Threats (CRITs), EclecticIQ, Facebook Threat Exchange, IBM X-Force Exchange, IntSights, LookingGlass, Malware Information Sharing Platform (MISP), Open Cyber Threat Intelligence Platform (OpenCTI), Open Threat Exchange (OTX), Threat Connect, ThreatQuotient.

The exact distribution and frequency of each platform is shown in Figure 14.

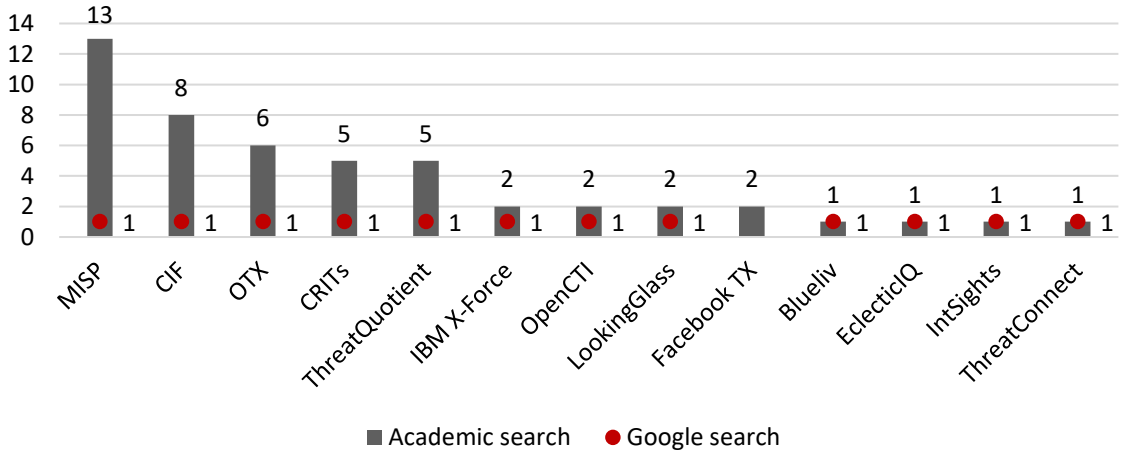


Figure 14: Platform synthesis of scientific search and Google search.

Table 6 provides an overview of the scientific literature used in the following platform analysis. The sources are listed in chronologically descending order.

Table 6: Mapping of analysed platforms to the used academic literature.

Source \ Platform	Blueliv	CIF	CRITs	EclecticIQ	Facebook TX	IBM X-Force	IntSights	LookingGlass	MISP	OpenCTI	OTX	ThreatConnect	ThreatQ
Bauer et al. (2020). Towards an Evaluation Framework for Threat Intelligence Sharing Platforms.									■		■		■
Chadwick et al. (2020). A cloud-edge based data security architecture for sharing and analysing cyber threat information.		■											
de Melo e Silva et al. (2020). A Methodology to Evaluate Standards and Platforms within Cyber Threat Intelligence.		■	■						■	■			
Menges et l. (2020). DEALER: decentralized incentives for threat intelligence reporting and exchange.					■	■			■	■			
Noor et al. (2020). Customer-Oriented Ranking of Cyber Threat Intelligence Service Providers.	■				■		■						
Riesco et al. (2020). Cybersecurity threat intelligence knowledge exchange based on blockchain.									■				
Faiella et al. (2019). Enriching Threat Intelligence Platforms Capabilities.		■	■						■				
Keim et al. (2019). Cyber threat intelligence framework using advanced malware forensics. International Journal of Information Technology.		■				■					■	■	
Mokaddem et al. (2019). Taxonomy driven indicator scoring in MISP threat intelligence platforms.									■				
Wagner et al. (2018). A Novel Trust Taxonomy for Shared Cyber Threat Intelligence.				■	■	■		■	■		■	■	■
Liu et al. (2017). A Research and Analysis Method of Open Source Threat Intelligence Data.		■											

Mutemwa et al. (2017). Developing a cyber threat intelligence sharing platform for South African organisations.													■
Tounsi & Rais (2017). A survey on technical threat intelligence in the age of sophisticated cyber attacks.		■	■						■				
Wagner et al. (2017). Relevance Filtering for Shared Cyber Threat Intelligence (Short Paper).				■				■	■				
Mtsweni et al. (2016). Development of a semantic-enabled cybersecurity threat intelligence sharing model.			■								■		

4.2 Platform analysis

In this section, the previously selected platforms are examined in detail based on the proposed framework. To ensure the most objective presentation possible, the platforms are presented in alphabetical order.

Blueliv Threat Compass [62]

Blueliv's Threat Compass platform aims to centralize operational, tactical, and strategic TI based on a modular architecture.

The platform supports all four phases of the TIS process. The collection of TI occurs through ingesting data from multiple sources, including open, closed, and private sources [15]. Therefore, the platform uses sinkholes, honeypots, crawlers, and sensors. The gathering of data takes place in an automated manner and allows multiple formats. The aggregation of TI is enabled by various functions to process, enrich, correlate, categorize, and validate data in an automated manner. Therefore, the platform states to provide honey client direct side validation, human intelligence, sandbox analysis, botnet identification, and threat classification and scoring. Furthermore, platform users can create their own YARA rules. In terms of TI analysis, Blueliv offers big data analytics capabilities. In addition, Blueliv claims to analyse TI automatically. The platform provides powerful visualization tools and a customizable dashboard, including graphical interrelationships. Furthermore, the platform enables to focus on specific TI. A push mechanism supports the dissemination of TI. TI can be integrated into existing security solutions (e.g., SIEM, SOAR) or shared with peers and trusted parties. Therefore, machine-readable data formats (STIX, TAXII), an API, and plugins are provided, enabling a formal sharing mechanism [15]. The platform states to deliver real-time TI.
Relating to information security, Blueliv states to use generally accepted industry standards. Furthermore, a privacy policy is provided, referring to the Spanish Data Protection Agency. Enabling the import and export of data, the platform uses STIX and TAXII. Collaboration is supported among internal groups or with trusted third parties. No information is provided relating to data quality, trust, and the platform's reporting capabilities.

Blueliv's threat compass has been identified as a cloud-based, operational platform. The architecture of the platform is modular and subscription-based, allowing the user to purchase each module individually. Therefore, the platform currently provides ten modules (threat context, credentials, dark web, credit cards, hacktivism, malware, mobile apps, social media, data leakage, and domain protection). Integration to existing security infrastructure (e.g., SIEM, SOAR) is enabled through the platform's API and flexible plugins. Blueliv has various technology alliances, e.g., AlienVault,

Elastic, Splunk, ThreatQuotient, DFLABS, Eleven paths. The user interface is provided in a web-based, graphical form in English language.

Blueliv ingests data from open, private, and closed sources, including global threat databases, hacktivism resources, social network-driven threats, sinkhole sensors, honeypots and crawlers, customers, community, partnerships, and alliances. Additionally, for further enrichment Blueliv's feed, 'Machine Readable Threat Intelligence feed', can be integrated into existing security infrastructure, containing data in the form of Crimeservers, Bot IPs, Attacking IPs, Malware hashes, Hacktivism ops, and TOR IPs. Regarding the TI provided on the platform, Blueliv states to centralize operational, tactical, and strategic TI. Therefore, IOCs, TTP, CVEs, and further information about threat actors, campaigns, malware indicators, attack patterns, tools, and signatures are available on the platform [15]. However, the provided TI depends on the subscribed module. TI is available in a structured and unstructured format. Following standard machine-processable information exchange format, STIX is listed as description standard, and TAXII is mentioned as exchange protocol [15].

Blueliv is a brand of Leap in Value SL, a medium-sized company for cyber security founded in 2009 (ISIC category 'J'). Blueliv is headquartered in Barcelona, Spain, and has an additional office in London, UK. There is no evidence that the company uses the platform and its information for its own purposes. Apart from the fact that wizlynx groups, BBVA, and Telefonica are among the platform users, nothing is known about the platform's users.

The Blueliv platform is closed-source and based on a pay-as-you-need modular architecture. A demo version and a free trial are available. The platform provider focuses on banking, insurance, telecommunications, utilities, and retail in Spain, the UK, and the US [63].

Collective Intelligence Framework (CIF) [64, 65]

CIF is a CTI intelligence management system, providing unified intelligence to support the identification, detection, and mitigation of threats. The platform was launched in 2012 and currently runs under version CIFv5.

The platform supports all four phases of the TIS process. CIF allows the ingestion and storage of data from various sources, ranging from private to open source intelligence data. The platform ingests basic indicators (e.g., IP addresses, domain names, URL) via YAML configuration file, allowing XML, JSON, and CSV. Therefore, CIF uses an application, called cif-smrt, to download, parse and ingest data into the platform. Data collection takes place 24/7 and is stored in ElasticSearch (JSON) [52, 66, 67]. The platform provides built-in functionalities to perform automatic gathering of data [20]. The aggregation of TI is supported by functions enabling to parse, normalize, aggregate, and enrich the collected data. According to de Melo et al. [20], CIF does not focus on correlation and classification mechanisms. The platform provides tagging mechanisms applied to describe the threat data. Furthermore, capabilities are provided to whitelist indicators and mark ingested data sets with a confidence level. Additionally, enrichment capabilities as GEO, DNS, and ASN tagging are supported. To support this phase, tools as ULResolver, Spamhaus, and BGPWhitelist are available. The processing of data is performed in an automated manner. The analysis phase is supported by cif-worker, the analytics pipeline within CIF. Cif-worker can process information and generate new intelligence out of it. Within this phase, users are allowed to create new data sets and define the relevance of specific IOCs [68]. CIF is a command-line tool

and provides no visualization capabilities but uses Kibana for graph generation [20, 32]. Furthermore, the analysis phase is supported by advanced collaboration capabilities [32]. The dissemination of TI is enabled by both a push and pull mechanism. TI can be pushed to other instances or integrated into existing security infrastructure. Furthermore, users can pull data by setting filters [32, 52]. To share TI selectively, CIF allows creating groups [20, 32]. No information is provided relating to the platform's real-time capacity.
The platform provider published a privacy statement in English to strengthen data privacy and information security, including a commitment to the US-EU and US-Swiss Safe Harbor Privacy Principles. When sharing data, the platform provides the capability to provide authentication and confidentiality, using Traffic Light Protocol (TLP) to shield sensitive information [52]. However, the platform does not provide any anonymization or encryption techniques [69]. To enhance data quality and trust, the platform enables tagging of threat data with a confidence level to describe the degree of certainty of a given observation and the creation of trusted groups [52]. The platform allows importing and exporting threat details to and from other systems in a standard format, providing automation capabilities [52]. CIF supports a wide range of import (e.g., XML, JSON, zip) and export (e.g., CSV, JSON, table) formats. However, STIX is provided only in a basic format by default [32]. Collaboration and sharing are supported via a private instance or by using a trusted and reliable partner or community among different instances, enabled through a centralized service [20, 32, 53]. Users can join the CIF users' group within Google groups or the CIF channel on Freenode to interact with the CIF community. No information is provided about the platform's reporting capabilities.

CIF is a modular and scalable platform, serving as an operational platform, with the option to build on it. Therefore, various software development kits (SDK) are available to enhance and adjust the functionalities and capabilities of the platform (e.g., Perl, Python, JavaScript) [68]. The platform is based on a client-server concept, allowing users to access the CIF server via a browser plugin, CIF client (Perl), or CIF-API [66]. Tounsi et al. [32] noted that a new ZeroMQ technology (ZYRE1) is in the works, allowing users to connect their CIF router via a peer-to-peer-like framework. The platform provides a REST-API, enabling management and query TI data within the platform [52, 66]. The platform's API provides various integration capabilities to standard security tools like IDS, SIEMs, or firewalls (e.g., Zeek (formerly Bro), Snort, Bind/RPZ, TippingPoint) [20, 32, 53]. CIF is based on a command-line interface [20, 66].
The platform is quite flexible, allowing various sources, internal and external, to flow into the platform. Per default, the platform provides integrations to currently 31 open source intelligence feeds (e.g., Abuse.ch, PhishTank, Spamhaus) [52]. Additionally, CIF allows to create own data feeds from its database. The TI is published in the form of IOCs (IP addresses, domains, URLs), available in structured (JSON) format. JSON is listed as a description standard. STIX is supported in a basic format but can be extended with extra modules [32]. CIF does not support TAXII as an exchange standard. Instead, the platform uses feeds to exchange TI between CIF instances [20, 32, 53].
CIF was developed by REN-ISAC and several other contributors in 2012 [32]. Today it is provided by CSIRT Gadgets, LLC, a small-sized non-profit organization (ISIC category 'U') located in New York, US. The platform is not vendor-supported and has no commercial support but provides a community [68]. In 2015, the CIF community counted 450 members. In 2017, 12 contributors

and 1000 commits had been identified [70]. The platform is widely used by the higher education community [68].
The use of CIF is free of charge, and the source code is publicly available under Mozilla's MPlv2 license. Neither a geographical nor a sectoral focus has been identified.

Collaborative Research Into Threats (CRITs) [71, 72]

CRITs is a malware and threat repository, combined with an analytic engine, that leverages other open-source software to create a unified tool. The platform was launched in 2014.

CRITs supports all four phases of the TI process. However, little to no information is provided by CRITs itself. The collection of TI occurs by the ingestions of indicators (domain, IP, malware sample, email) or raw data, allowing PDF files, whitepapers, forums, logs, emails, articles, or outputs from other tools. To store the ingested data, CRITs uses the non-relational database MongoDB. Automated gathering of information is possible via API integrations [20]. To support aggregation of TI, CRITs states to facilitate managing, enriching, and tagging the previously collected data. According to de Melo et al. [20], the platform does not provide classification and correlation mechanisms. The processing of data, either manually or automated, is supported by CRITs services, providing various integration capabilities (e.g., Yara, RAT decoder) [73]. Analysis of TI is supported by advanced analysis capabilities, allowing the platform users to collaborate [53]. CRITs enables the analysis of samples, PCAPs, and linkage to a Cuckoo sandbox [32]. Additional services as PYEW or Entropycalc can be integrated. Graphical visualization of TI is provided via a customizable drag-and-drop dashboard, allowing visualization of relationships via services [20, 53]. Therefore, Maltego transform supports graph generation. These functions allow to uncover patterns and identify critical information automatically [32]. Little information is available about the platform's capabilities for disseminating TI, other than the ability to create trusted groups of instances for sharing [20]. Faiella et al. [53] found that the platform has poor built-in sharing and integration capabilities.
MITRE, the owner of CRITs, provides a privacy policy in English language. No information is provided to certifications, standards, or data transfers with other countries [74]. To improve information security and data privacy, the platform provides an authentication layer to authenticate, manage, and administrate the platform user [75]. Furthermore, CRITs allows the marking of indicators with a confidence level and provides releasability capabilities, allowing for tracking information sharing. No information is provided relating to data quality and trust. The platform supports a considerable amount of import (e.g., STIX, CybOX, bulk-import via CSV file, blob, and spreadsheet) and export (STIX, CybOX, CSV) formats [32, 53]. Collaboration is enabled either via a private instance or by using a trusted group of instances [20, 32, 53]. As for the reporting features, the platform's content can be downloaded in a customizable way in zip or STIX format.

CRITs has been identified as an operational platform, providing a core installation. However, the functionalities and capabilities of CRITs can be extended and customized by deploying services from a service framework or writing own services. Faiella et al. [53] identified the platform to have advanced hardware requirements, accessible either locally, remotely, or via custom APIs [75]. CRITs plugs into a centralized intelligence data repository but can also be used as a private instance [32]. The platform is based on a REST-API, supporting import, export, and updates [32]. Services enable integrations to third-party services, and sources are possible (e.g., DataMiner,

OpenDNS, ThreatExchange, Yara) [53]. As per default, CRITs is not constructed to integrate with existing security infrastructure (e.g., SIEMs, IDS) [32, 53]. The platform provides a web-based GUI including several dashboards, using the Django framework. Furthermore, interacting with the API is also enabled via a command line.
There is little information available about the origin of the data, except that internal and external sources are fed into the platform [32]. CRITs provides information about technical and tactical TI in the form of TTPs and IOCs. TI is provided in a structured format. The platform lists STIX as a description standard and TAXII as an exchange protocol, with some integration required for the latter [20, 32, 53].
CRITs has been developed by the MITRE Corporation, a large-sized non-profit organization (ISIC category 'U'). The organization focuses on assisting the U.S. government by operating several unique organizations for research and development. The headquarters are in Massachusetts, US, and Virginia, US. Additionally, MITRE provides various locations worldwide (e.g., Germany, Japan, UK) [74]. CRITs was initially developed as an internal project of MITRE, beginning in 2010, to better protect the organization's own information technology network. 2011 the CRITs operational prototype was provided by MITRE. In 2014, the platform was publicly launched, open-source and free-to-use. Today, CRITs is being evaluated and used by multiple researchers and organizations. Since then, many specialists joined the project to use CRITs, commit, or contribute to the project. CRITs is a community-driven project with a strong community of users and developers, which requires the participation of its community in the project.
CRITs addresses organizations worldwide, is supported by a global developer network, and thus has no geographical focus. Furthermore, both, public and private sector is targeted by the platform.

EclecticIQ [76]

EclecticIQ is an analyst-centric threat intelligence platform, providing a central intelligence repository of cyber threat intelligence. The platform was launched in 2014.

The platform supports all four phases of the TIS process. The collection of TI occurs through data ingestion from multiple sources, internal and external, allowing multiple formats, structured and unstructured. The collection phase is supported by an ingestion engine based on quuz, providing real-time metrics to monitor incoming data. Furthermore, a CTI clipboard is used to capture data from websites and feed it directly into the platform. EclecticIQ offers various functions to consolidate, normalize, correlate, de-duplicate, and enrich the previously ingested data to aggregate TI. Incoming data automatically gets correlated with existing data. User-generated tags or pre-defined taxonomies can be used for tagging. The platform's API provides out-of-box integration to several enrichment services (e.g., DomainTools, Geo-IP, VirusTotal) to enrich information for an easier later review. Furthermore, the platform states to leverage the latest data management technologies, enabling to process huge amounts of information at high speed. EclecticIQ enables the elimination of manual and repetitive processing of multiple intelligence feeds. The platform provides functionalities to search, prioritize, visualize, and collaborate to support the analysis phase. Advanced search tools allow comprehensive exploration and pivoting of the data repository using tags and search terms [50]. Threats can be sorted and rated (e.g., per confidence, reliability, time, kill chain), with the ability to add queries, graphs, free text, and assign tasks. Qualifying threats based on their relevance enables the conduction of triage. Alerts can be set based on advanced search logic and

network graph correlation matrices. The platform provides graphing capabilities to support exploration, enabling to see connections. The analysis is supported by collaboration within dynamic workspaces, allowing the creation of briefings or advisories. Both manual and automatic processes support the analysis phase. The dissemination of TI is provided by a push mechanism, sharing TI with internal and external stakeholders. The TI is distributed in the form of digests and reports that can be sent via email or directly to existing security controls. The platform's API offers various integration options, allowing it to deliver TI into existing security infrastructure automatically (e.g., SIEM, IDS). Notifications can be delivered either from within the EclecticIQ platform or through e-mail. Distributing intelligence to human stakeholders takes place by using granular distribution policies to define approved and audited recipients. Furthermore, intelligence can be shared with ISACs, ISAOs, interest groups and other sharing communities using STIX, TAXII, and community-specific protocols. The platform provides real-time access to TI by enabling dissemination at machine speed.
To enhance information security, the platform states that it strives to improve its data security standards continuously. Secure Sockets Layer technology connections support the processing of sensitive data, and third-party API tokens are provided with high-level encryption. EclecticIQ provides a privacy policy, including a commitment to act in conformity with the GDPR. The data security guidelines also apply to international data transfers but can be extended in certain cases through contractual agreements to ensure conformity with European standards. To provide authentication and authorization, EclecticIQ uses internal protocols or LDAP. To enhance data quality, the platform performs automatic quality determination for IOCs, improving the effectiveness and relevance of IOC databases. Furthermore, Wagner et al. [77] identified an internal vetting process to be in place within the platform. No information is provided relating to trust. STIX supports the import and export of information. The platform describes itself as a single collaborative workspace enabling analysts to exchange information and knowledge. Secure workspaces are provided to collaborate with colleagues, including the support of task assigning and management. Furthermore, findings can be commented on and shared to contribute to a centralized intelligence knowledge base. EclecticIQ enables the creation of customizable reports in PDF format. Reports can contain information in the form of textual parts and graphical parts (e.g., multi-paragraph reports; reports on specific tools, techniques, and procedures; actor profiles, campaign profiles, incident reports, and indicator reports). Additionally, reports can be easy linked to other structured and unstructured intelligence and context in the EclecticIQ platform.

EclecticIQ has been identified as an operational platform, allowing various customization and extension options via SDK. Additionally, EclecticIQ provides the open-source projects, Cabby and OpenTaxii, supporting implementation and interaction with TAXII services. The platform provides various cloud (e.g., Microsoft Azure), on-premise (e.g., Red Hat), and hybrid deployment options. The platform's REST-API enables configuration and integration with existing security infrastructures (e.g., IBM QRadar SIEM), TI vendors (e.g., Bitdefender), central sources of technical data (e.g., CVE), and ISACs (e.g., FS-ISAC). In total, the platform currently provides 86 integration options. An interface in the form of a GUI in English language is provided.
EclecticIQ allows internal as well as external data to flow into the platform [77]. External data sources include DNS information, actor databases, virus databases, public databases, and internal databases from open sources, commercial suppliers, and industry partnerships. Currently, the

platform provides 59 out-of-box integrations with intelligence providers (e.g., DHS AIS, Flashpoint, Intel 471) and enrichment services. Additionally, EclecticIQ launched its own EclecticIQ Open sources feed and EclecticIQ Commercial sources feed. The TI provided on the platform ranges from technical to strategic TI, including observables, indicators, threat actors, malware, vulnerabilities, attack patterns or other TTPs, campaigns, incidents, courses of action, and high-level reports. Both, structured and unstructured (English) form is available. The platform provides support for STIX and TAXII. With Version 2.9, the platform released extended interoperability for STIX 2.1 and TAXII 2.1. Furthermore, the platform provides community-specific protocols for sharing intelligence. However, no detailed information is provided.
The platform is owned by EclecticIQ B.V. (formerly Intelworks), a medium-sized company for cybersecurity (ISIC category 'J') [78]. The company was founded in 2014 in Amsterdam, NL, and has additional offices in North America (Virginia), UK (London), and Eastern Europe (Moldova). EclecticIQ manages and maintains the platform. The platform's clients are some of the most targeted organizations globally.
The platform is closed source without providing further information regarding the pricing conditions. A free demo of the platform can be acquired. According to its offices, EclecticIQ operates globally with no geographical focus. The homepage itself states to address governments, large enterprises, and service providers with its solutions. Jansen [79] identified the platform to focus on governments and financial institutions.

Facebook Threat Exchange (TX) [80]

TX is an API platform that leverages the management and sharing of TI in the form of signals. The platform was launched in 2015.

TX is based on three core concepts: signals (threat indicators), descriptions of signals (threat descriptors), and visibility of signals. The platform supports the collection, aggregation, and dissemination of TI. However, it remains unclear whether the platform supports the analysis of TI. The collection of TI is supported by ingesting data from internal sources into the platform [77]. Via user interface (UI), either a single threat descriptor can be uploaded, or a bulk-upload of threat descriptors from CSV or JSON files can be conducted. Additionally, the use of templates allows the upload of huge amounts, independently of the format. Furthermore, data can be submitted via the platform's API. The platform provides a high data availability, as data can be uploaded and is available regardless of the user's status [54]. No information relating to automation capabilities is provided. The aggregation of TI is supported by capabilities to correlate, tag, mark, edit and duplicate the ingested data. Data processing can be done via API and UI, whereas the UI also allows bulk actions. Tagging can be done via subjective threat tags, used to label objects. Furthermore, the UI enables the cloning of threat descriptors. Furthermore, edges between signals can be created to express relationships. The platform also enables automatic soft-deletes for data and relationships that are no longer valid to counteract false-positive cases. Relating to the analysis of TI, little information is provided. The previously tagging of data enables simplified searching and querying for indicators. Text-based search results can be sorted by relevance. TX provides functions to react on data and express a structured opinion on it, via API or UI. Bulk-reaction via UI is enabled as well as retrieving reactions of other users. No visualization capabilities could be identified. To support the dissemination of TI, TX follows an automated, formal sharing mechanism pushing

data into existing clients and workflows [15, 54]. Furthermore, sharing of signals is enabled via UI and Python packages. The platform supports sharing of TI based on individually defined privacy rules among predefined groups of members in a secure, privacy-compliant, and automated way. Besides the sharing capabilities, TX uses Webhooks to provide real-time information and push notifications.

To enhance information security, the platform states to take appropriate measures. Furthermore, the TX terms prohibit the sharing of sensitive personal information. However, data integrity or availability is not conclusively assured [54]. The platform provider (Facebook Inc.) provides a privacy policy concerning all its products and services. An additional privacy policy is provided for Facebook open source projects. Furthermore, Facebook states to act in conformity with the Privacy Shield Frameworks and the GDPR. Global data transfers take place according to Facebook's privacy and standard contractual clauses provided by the European Commission. To further enhance information security and data privacy, privacy controls are provided, allowing to set sharing, re-sharing, and visibility levels, based on TLP. Additionally, threat data can be equipped with a confidence level. Relating to data quality, Wagner et al. [77] identified an internal vetting process to be in place. Whereas Menges et al. [54] identified quality assurance and relationship of trust between platform users is not particularly focused. In 2018, a TI blog certified TX poor quality data and untrustworthy data [81]. Information in the form of a status page is provided relating to the platform availability, showing several issues and downtimes in Q1 2021. For uploading and downloading data, TX supports CSV and JSON format. According to Wagner et al. [77], collaboration with other stakeholders is not allowed within TX. For sharing of TI between platform users, three approaches are provided: all members, private groups, and members of a whitelist. From the developer perspective, TX is based on an open source community and aims to enforce sharing, collaboration, and mutual learning. Community members are expected to engage in the community. For developers, a developer supports site as well as a ThreatExchange Facebook group is provided to exchange information and discuss about bugs, feedback, updates, release and more. No information is provided relating the reporting capabilities or further salient functions of the platform.

TX has been identified as an operational platform. According to Noor et al. [15], the platform follows the hub-and-spoke model. The platform can be used either via UI, API, or Python package to build integrations. The platform builds on Facebook's existing platform infrastructure and its Graph API ecosystem. TX thereby represents a subset of API endpoints that allows third-party developers to interact with TX. Currently, the platform provides five direct integrations to existing workflows (e.g., Carbon Blac, Demisto, Splunk add-on). The APIs default language is JSON but can be implemented in various languages using Python, Ruby, Java, PHP, or cURL wrapper. The platform provides a GUI in English (default). The language likely adapts to the user’s settings, i.e., country.

Facebook itself provides no information about the datasets used within TX. Wagner et al. found that no external sources flow into the platform [77]. The TI shared on the platform is available in the form of IOCs. Currently, over 80 types of indicators (e.g., hashes for malware, phishing site URLs, malicious domains, or IP addresses) can be shared on TX. Typically, details about specific attacks or campaigns, e.g., phishing attempts, malware, or bad domains/IPs, are shared within TX. Also, information on bad actors (e.g., email addresses) or signatures for detecting threats (e.g.,

Yara or Snort formatted signatures) can be shared. The TI is available in a structured format (CSV and JSON). According to Noor et al. [15], TX follows a standard machine-processable information exchange format. The exchange of TI takes place via HTTPS, using the RESTful API.
TX is owned by Facebook Inc., a large-sized company headquartered in California, US. The company offers various services in the field of information and communication (ISIC category 'J'). Besides offices in more than 80 cities worldwide, Facebook has 17 data centers globally. No information is provided regarding the provider's role. Companies from various industries are part of the TX community.
The source code is publicly available for free on GitHub. However, there are some requirements to use TX. A Facebook account is required to sign up and create a developer app, which will be used to connect to TX. For participation in the community, a Code of Conduct is provided by Facebook. The platform offers no free trial.

IBM X-Force Exchange (XFE) [82, 83]

IBM X-Force Exchange is a cloud-based threat intelligence sharing platform, serving as a repository for IBM Security Intelligence [84, 85]. The platform was launched in 2015.

XFE supports the collection, analysis, and dissemination of TI, whereas aggregation of TI is not particularly addressed. The collection phase is supported by internal and external sources to be ingested into the platform, including the company's own infrastructure and databases, open-source intelligence, commercial sources, deep web, and partnerships with third-party sources. No information regarding automation capabilities is provided. Besides the platform's capability to aggregate and organize data, no further information is provided relating to the aggregation of TI. The analysis of TI is supported by a collaborative interface, allowing users to manage, annotate and prioritize findings [86]. Therefore, the platform allows users to create their own collections of indicators, to add context to threats [85]. A collection is a repository of information where reports, comments, and other content can be stored. Via tags, collections and reports can be connected. Other collections can be accessed along with timelines, blogs, public collections, and search functions, and content relevance can be improved [77, 85]. XFE provides a dashboard, which among others, visualizes indicators and threat activity. Within the dashboard, threats can be reported distinguishing four threat levels: normal threats, increased vigilance, focused attacks, and catastrophic threats [52]. Furthermore, platform users can comment on indicators and configure watchlists, enabling continuous monitoring [85]. The analysis of TI is supported by integrated workflow support [87]. Dissemination of TI is supported by push and pull mechanisms, allowing to research, consume, and share threat intelligence data, including collections [54]. The platform's API allows automated querying of XFE data and integrations to existing security infrastructures [84]. As a result, near real-time monitoring and decision support are provided.
The platform provider states to have implemented 'reasonable physical, administrative and technical safeguards to protect the user's personal information and maintain its accuracy. Furthermore, Binding Corporate Rules are used to protect personal information. Data integrity is not considered [54]. Relating to data privacy, the platform is certified with the IBM Privacy Shield for IBM Cloud Services. Additionally, IBM provides a traditional privacy statement and an online privacy statement, focusing on the online context. The privacy statement is available in various languages. A Data Processing Addendum is provided for various countries. Regarding international transfers of

personal information, IBM implements Standard Contractual Clauses approved by the EU Commission, if necessary. X-Force Exchange is furthermore conforming with GDPR, NIS Directive, ISO/IEC 27001, ISO/IEC 27017, ISO/IEC 27018, California Consumer Privacy Act (CCPA), APEC Cross Border Privacy Rules (CBPR) system, and the EU-US Privacy Shield and Swiss-US Privacy Shield Framework. Furthermore, the provider publishes a transparency report. The assurance of the platform's data quality is not taken into account [54]. Wagner et al. [77] identified that no internal vetting process is in place. No functionalities to enhance trust have been identified. To ensure platform availability, XFE uses increased parallelization [54]. However, the status page of XFE shows some downtimes of the platform in the last 90 days. No details are provided regarding the import and export capabilities of the platform, besides mentioning STIX as an export standard (e.g., for collections). Collaboration between platform users is highly supported within XFE. The concept of collections enables users to share and collaborate on existing and emerging security threats. Therefore, peer collaboration via private groups and shared collections is enabled, not only limited to the same industry [77]. Additionally, public groups visible for all XFE users are available. Groups can be created or joined by users and queried for collections [85]. Additional support can be leveraged by the XFE community and an expert blog to gain tips, insights, new perspectives, and expert guidance. Reports can be generated and exported in STIX format, consisting of graphical and textual elements.

XFE has been classified as an operational platform, providing a Node SDK. XFE is cloud-based and can be run on Firefox, Chrome, Microsoft Edge, and Safari. The platform provides a REST-API in JSON format, providing programmatic access to the XFE platform via automated querying [84]. The API enables integration to existing security solutions. The API is available with different scopes and functionalities and partly requires authentication (Non-commercial API, commercial API, enterprise API, and Advanced Threat Protection Feed). The API output language can be changed. XFE provides a web user interface in the form of a GUI in various languages.
XFE has a huge universe of resources, providing an extensive database of machine-generated data and human-generated intelligence [85]. In order to produce TI, XFE uses data from internal and external sources accessed via API [77]. To provide internal data, the platform uses IBM’s repository from IBM-developed infrastructure and databases collected over 20 years from IBM X-Force [85, 87]. This includes the following feeds: IBM Advance Threat Protection Feed, IBM X-Force IRIS Premium Threat Intelligence Reports, IBM Early Warning Feed. External sources are used from open-source intelligence, commercial sources, deep web, and partnerships with third-party sources, including crawler robots, honeypots, darknets, and Spamtraps [86]. Therefore, the platform has implemented a threat feed manager that controls partnerships with third-party intelligence sources, simplifying getting data out of various sources into one view. Currently, seven third-party threat intelligence feeds are available in the threat feed manager (e.g., BotScout, VirusTotal). XFE is a tactical-based model, providing over 900 terabytes of threat intelligence through reports, advisories, and collections [52]. Threat intelligence is provided by a combination of observables and indicators, including vulnerabilities, malware, malware families, IP reputation, URL reputation, Web applications, pDNS, Whois information, malicious domains, and higher-order intelligence like actors, campaigns, incidents, and TTPs. TI is available in structured (STIX, JSON, CSV) and unstructured (plain text) form in English language. TAXII is mentioned as an exchange protocol.

XFE was launched in 2015 by IBM Security, a subsidiary of IBM Corporation. IBM Security is a large-sized company for cybersecurity, headquartered in Massachusetts, US (ISIC category ‘J’). The TI provided by XFE is used internally, serving as a repository for IBM Security Intelligence [85]. However, no detailed information is provided about the platform's users, except that some of the world’s top 10 retailers and top 10 banks use the platform [87].
The license type of the platform remains unclear. Menges et al. [54] identified the platform as closed-source, whereas Keim et al. [52] identified the platform as open source. The XFE platform itself and the basic API are free of charge. The no-cost API provides a limited free tier of access for non-commercial use, offering up to 5.000 records per month [87]. The Advanced Threat Protection Feed, X-Force Exchange Commercial API, and X-Force Exchange Enterprise API require a fee for additional data. A free trial of all editions is available. No geographical and sectoral focus of the platform has been identified. XFE addresses any size of organization [87].

IntSights [88]

The all-in-one TIP by IntSights is the core of the IntSights External Threat Protection Suite. The platform was launched in 2018.

IntSights supports all four phases of the TIS process. The collection of TI is supported by the platform's proprietary collection engine, capturing various sources of intelligence, internal and external. The platform ingests data in the form of IOCs, malicious IPs, CVEs, and other complex signals captured from across the clear, deep, and dark web in STIX format. No details regarding automation capabilities are given. To support the aggregation of TI, the platform provides functions to organize, aggregate, correlate and enrich the previously ingested data. Existing results and information can be correlated with additional indicators to enrich organization-specific IOCs and other threat indicators at a large scale. On-demand enrichment capabilities augment existing data sets with organization-specific IOCs and contextual intelligence. This is supported by various enrichment services (e.g., DNS records, Whois Data). As a result, IOCs' automatic and continuous connection, fewer duplicates, and false positives are enabled. The analysis of TI is supported by functions to investigate, pivot, prioritize, and visualize threat information, enabling automated threat intelligence analysis. The platform’s API, therefore, enables deep threat investigations. IntSights Query Language (IQL) enables optimized searchability and control. Additionally, pivoting, ranking, and prioritization of IOCs are provided. All IOCs can be automatically organized and visualized within one single easy-to-use dashboard, summarized by severity and confidence level (low, medium, high, critical) [89]. The visualized investigation dashboard allows continuous monitoring and mitigation of threats. Collaboration capabilities support the analysis phase. The dissemination of TI is enabled by a push mechanism, enabling customized outputs and automatic integration of threat data to existing security infrastructure. This allows updating critical blocklists, proactively monitoring, and automated threat blocking. The platform delivers real-time contextual visibility into organization-specific IOCs and other threat indicators. Based on that, automated incident response and mitigation and alerts in real-time and at scale are facilitated.
To protect the information security, the platforms provider takes ‘administrative, technical, and physical security measures to help protect your personal information’. Furthermore, the platform is SOC 2 and ISO/IEC 27001 certified. A privacy policy is provided on the website. No functions could be identified to assure data quality and enhance trust. Information about the platform

availability is provided via the status page of the operating systems (e.g., dashboard, API, ISPP). Until today, no unscheduled incident has occurred. STIX is named as standard to ingest and share threat intelligence data. The platform states to allow teams to collaborate. There is no further information on the collaboration and reporting features of the platform. As additional functions, IntSights provides built-in remediation and takedown capabilities to remove malicious content from the web.

IntSights has been classified as an operational platform. The platform's REST-API (Investigation API) allows various integrations to existing security infrastructures as well as cloud solutions (e.g., SIEMs, firewalls, Office 365 Exchange) [89]. A GUI is provided in English language.
The platform ingests a wide range of intelligence sources, including internal and external sources. IntSights provides its own feeds, including three premium feeds and three public feeds. Furthermore, customized and manually created intelligence feeds can be ingested into the platform [89]. The API provides a wide variety of data enrichment sources and other feeds from leading threat intelligence providers to enhance context further. The platform provides information relating to threat intelligence, phishing, and vulnerability information [15]. The TI on the platform is provided in the form of IOCs, malicious IPs, CVEs, and contextual intelligence. TI is provided in a structured format. IntSights follows a standard machine-processable information exchange format, using STIX as description standard and TAXII as exchange protocol [15].
The platform belongs to the eponymous company IntSights, a medium-sized company for cybersecurity founded in 2015 by former members of the Israel Defense Forces (ISIC category 'J') [90]. The company is headquartered in New York, US, and has additional offices in Israel, Japan, Massachusetts, Netherlands, Singapore, and Texas. Little information is provided relating to the platform users, only that IntSights is used by many of the world's largest companies.
The platform provides no information about its pricing policy but has been described as cost-prohibitive [89]. IntSights is a commercial TIP, providing a free demo version [89]. The platform addresses organizations of any type or size without focusing on a specific region or sector.

LookingGlass [91]

LookingGlass is a frequently named product in threat intelligence platform research. Most sources rely on scoutPRIME, a Cyber Situational Awareness Platform [50, 77, 92–95]. However, the company declares scoutTHREAT, a Digital Risk Assessment Platform, as a Threat Intelligence Platform [96, 97]. In [15], the authors do not precisely specify which product they are referring to. Concerning their functionalities, both platforms are considered separately in the following.

ScoutPRIME [92]:

ScoutPRIME is a Global Attack Surface Management platform launched in 2015.

The platform supports all four phases of the TIS process. The collection of TI occurs by automated ingestion and indexing of data from multiple sources, including external [50]. ScoutPRIME allows the collection of structured and unstructured data. The aggregation of TI takes place by normalizing and automatic correlation of the ingested data. Various investigation and enrichment tools support the processing of TI (e.g., Shodan, PassiveDNS, WhoIS, Reverse WhoIs, YARA rules, geolocation information) [93]. To support the analysis of TI, the platform states to provide deep data analytics. Therefore, various functions to organize, analyse, search, score, and prioritize the

data are provided. ScoutPRIME supports ranking and prioritization of threats by enriching data with Threat Indicator Confidence (TIC) scores. This enables prioritization and identification of high-priority alarms and threats [94]. Furthermore, the platform provides customizable footprinting capabilities to focus on assets or networks most relevant to an organization. Customizable workflows and dashboards enable a visual representation and continuously monitoring of incoming threats and relationships, supported by Graph Explorer [93, 94]. The dissemination of TI is enabled by a push mechanism, allowing to share TI with colleagues and third-party systems (e.g., SIEMs) [94]. Furthermore, notifications and alerts can be configured as well as scheduling of reports. The platform provides real-time capacity in the form of alerts about new threats.
To ensure the security of personal information, LookingGlass states to apply various practices and security measures. The company provides a privacy policy in English language. Relating to data quality, Wagner et al. [77] identified no internal vetting process to be in place. No information is provided relating to enhancing trust. The platform enables the export of TI via API and third-party system integrations. Export is supported in multiple formats (e.g., JSON, CSV) and supported by STIX and TAXII [93]. ScoutPRIME enables collaboration between colleagues, supported by customizable dashboards that can be configured to functional roles. Furthermore, dashboards and other tools such as checklists can be shared [94]. Regarding the platform's reporting capabilities, the creation of unlimited management reports, scorecards, and other reports is provided. The distribution and destination of these reports can be scheduled automatically or manually on-demand.

ScoutPRIME has been identified as a cloud-based operational platform, providing a python SDK to extend the platform's functionalities [93]. An extensible API is provided, allowing integrations to other third-party tools (e.g., SIEMs, big data solutions). The platform provides a GUI in English language.
In terms of data sources, the platform allows the ingestion of external sources from various providers, including commercial feeds [77]. Currently, the platform uses 88 out-of-the-box sources of technical and threat-related data, of which 18 are proprietary indicators and feeds. The platform acquires intelligence from botnet sinkholes, internet sensors, and LookingGlass' proprietary sensors. The company has investigatory tools for the dark web as well [93]. ScoutPRIME provides information about TTPs, IPs, URLs, CIDRs, websites, mail servers, domains, phishing activity, port/cert information, CVE data, malware, viruses, and more [94, 98]. STIX 2.0 is listed as a description standard, whereas TAXII 2.0 is mentioned as an exchange protocol.

ScoutTHREAT [96]:

ScoutTHREAT is a Digital Risk Assessment platform designed by Goldman Sachs and launched in 2017. The platform is described as a centralized repository and management for the request for information (RFI). However, little information is provided relating to the characteristics and functionalities of the platform.

Relating the collection of TI, scoutTHREAT allows structured and unstructured data that get parsed and indexed [97]. The aggregation of TI takes place by processing and operationalize the previously ingested data. Furthermore, the linking of data and correlations is enabled by advanced threat modeling. The analysis of TI is supported by threat frameworks such as cyber kill-chain and MITRE ATT&CK. Prioritization of specific threats is enabled by mapping threat data, assigning risk scores, and conducting gap analysis. Search capabilities allow the user to retrieve TI news

from its organization. Furthermore, an analysis desk is provided to process incoming data automatically. To disseminate TI, a push mechanism is provided that integrates information into existing security infrastructure. The distribution of TI aims to identify and counteract attacks automatically and in real-time.
To ensure the security of personal information and data privacy, LookingGlass states to apply various practices and security measures and provides a privacy policy in English language. Additionally, scoutTHREAT states of being a secure platform, satisfying privacy concerns. To further enhance information security and data privacy, the platform uses access controls and data marking via TLP. Import and export of data occur based on the STIX format. ScoutTHREAT provides workbenches and workflows to organize work and enhance collaboration [97]. No functions could be identified relating to data quality, trust, and reporting capabilities.

The platform has been classified as an operational platform. The REST-API allows the creation of custom rulesets and integrations.
Relating to the data origin, the platform's API allows the integration of other data feeds. ScoutTHREAT deals with TI in the form of IOCs and TTPs. The platform is based on a structured data model with STIX as a description standard [97].

LookingGlass Cyber Solutions, Inc., is a large-sized company for cybersecurity, founded in 2009 (ISIC category ‘J’). The company is headquartered in Virginia (US) and has additional offices in California (US), Maryland (US), Utah (US), and Prague (Czech Republic). The company states to have more than 300 customers globally, commercial and government [91]. ScoutPRIME is used from intermediate to expert level (i.e., security operations staff, threat analysts, third-party risk monitors) [94].
Both platforms are closed source and require a fee. A free trial can be requested. LookingGlass distributes its products worldwide with no specific focus [91].

MISP - Open Source Threat Intelligence Platform [99, 100]

MISP - Open Source Threat Intelligence Platform, formerly Malware Information Sharing Platform, has been identified as the most extensive, popular, flexible, and used TI platform [20, 101]. The platform was launched in 2012.

MISP supports all four phases of the TIS process. Data collection takes place by ingesting various feeds, including the MISP feed and any other TI or OSINT feed from third parties. MISP allows ingestion in structured and unstructured format (e.g., CSV, MISP standardized format (JSON), free text (PDF)). The platform's default feeds are automatically provided within the server, without the need to import them directly. The free text importer enables the integration of unstructured reports (PDF) and TI into the platform. The gathering of data is enabled in an automated manner [20]. The aggregation of TI is enabled by capabilities to correlate, classify, and tag previously ingested data. Correlation and classification mechanisms are well performed by MISP [20]. The platform enables automatic correlation for every data in the platform to identify relations between indicators and attributes [20, 32]. This is enabled by a correlation engine, enabling advanced correlations as Fuzzy hashing correlation or CIDR block matching. Various taxonomies enable tagging and classification of threat data. Either existing taxonomies or own classification schemes can be used. MISP provides 126 taxonomies and classification schemes per default (e.g., CERT-

XLM, Diamond Model, Kill Chain), supporting standard classification used by ENISA, Europol, DHS, CSIRTs, or many other organizations. The analysis of TI is supported by functions to pivot, filter, visualize, and collaborate. Users are enabled to pivot through events, define a threat level for an event (low, medium, high) and improve content relevance using tags [50]. Furthermore, advanced filtering functionalities are provided as well as the option to create warning lists. Users have multiple options to collaborate on events, attributes, or indicators, to achieve more efficient analysis. Furthermore, MISP provides feedback loops in the form of proposals to make suggestions for changes or updates on given information. For the presentation of the information, a generic and customizable dashboard is provided. Also, graphical visualization of relationships is supported [20, 32]. The platform provides various tools to support analysis (e.g., GFI Sandbox, Graphviz). The dissemination of TI is provided by push, pull, and cherry-picking (selectively pick and choose events) mechanisms, using the platform's API and UI. MISP enables the generation of several rules for NIDS (e.g., Snort, Suricata) and other export formats for automated import into existing security infrastructure. In addition, various distribution models can be used for sharing TI between MISP instances. ZeroMQ enables real-time integration of MISP activities. Furthermore, auto-alerts allow notifications about new activities within the platform [20].
The platform handles information security management, relying on the ISO/IEC 27000 series, focusing on ISO/IEC 27010:2015. To ensure data privacy, MISP provides a set of legal and policy compliance analyses. Furthermore, the platform states to deal with data protection based on the legal foundation of the GDPR. To further enhance information security and data privacy, the platform uses TLP for distributing information. Additionally, notifications can be encrypted and signed via PGP or S/MIME. Relating to data quality, no internal vetting process is in place [77]. MISP considers quality assurance for future work [54]. The platform's objective is to create a platform of trust. Therefore, taxonomies enable adding of reliability and credibility measures to attributes to be shared [102]. Furthermore, users can create trust relationships. The platform provides export capabilities into existing security infrastructure in an automated manner. Therefore, standards as STIX (STIX 1.0/ STIX 2.0) and OpenIOC are used. Furthermore, the platform supports various import (bulk-import, batch-import, free-text import, import from OpenIOC, GFI sandbox, ThreatConnect CSV, MISP format) and export (IDS, OpenIOC, plain text, CSV, RPZ, MISP XML or JSON, Graphviz, gexf) formats. Additional modules for importing and exporting can be added [53]. The platform provides advanced support and multiple options relating to collaboration [32, 53]. When sharing information, an organization can act pseudo-anonymously and disseminate TI publicly or on a trusted basis [13]. Therefore, five options are provided: organization only (default), community only, connected communities, all communities, sharing group. Furthermore, collaboration via proposals and discussion forums, and threats is enabled. Except that graph generation can be exported as graphviz and gexf files, the platform does not provide any information about reporting capabilities [32].

MISP has been classified as an operational platform, providing various autonomous modules to expand and customize the core functionalities of the platform [13]. The sharing architecture of the platform is based on a peer-to-peer concept [53, 102]. MISP provides a REST-API in JSON format. The API allows high integrations capabilities to existing security infrastructure as SIEMs or IDS (e.g., Snort, Zeek) and other TI platforms [13, 20, 32, 53]. Additionally, MISP provides various modules for expansion and other services, including expansion modules (e.g., CVE,

DomainTools, Joe Sandbox), export modules (e.g., GoAML export, VirusTotal Graph), and import modules (e.g., Cuckoo JSON, ThreatAnalyzer). Furthermore, the API integrates PyMISP into the platform, a flexible Python Library. MISP provides a graphical web interface in English language [13]. Additionally, command-line tools are provided to interact with the background workers.

To create TI, MISP allows internal and external sources to flow into the platform [77]. Internal sources are created by platform users, whereas external sources include open-source feeds and other third parties' threat intelligence [13]. MISP currently provides 63 OSINT feeds (e.g., PhishTank, Malware Bazaar) per default, described in JSON format. MISP provides technical and non-technical information about malware samples, incidents, attackers, and intelligence, especially in the form of IOCs and other indicators (e.g., financial indicators) (e.g., [20, 32, 102]). TI is provided in structured (STIX, OpenIOC) and unstructured (English only) form. Due to a flexible data model and various built-in capabilities to exchange TI, the platform is compatible with different formats and has adaptable core functionalities [13, 20, 53]. Amongst others, the platform supports STIX 1.0, STIX 2.0, OpenIOC, and TAXII 1. Future compatibility with TAXII 2 is planned.

A group of developers has developed MISP from Computer Incident Response Centre Luxembourg (CIRCL) and other contributors (e.g., NATO, CERT-EU). Today it is financed by CIRCL, a small-sized organization based in Luxembourg, with the additional support of the EU. The platforms contributors are primarily non-profit organizations (ISIC category ‘U’). CIRCL itself operates several MISP instances to deal with cyber-attacks in Luxembourg and outside. Currently, MISP is used by more than 6000 organizations worldwide, in various sectors.

The platform is free and open-source licensed under GNU Affero General Public License Version 3, available on GitHub. MISP has neither a geographical nor a sectoral focus. The platform addresses private organisations, organisations, private researchers, or CERTs.

Open Cyber Threat Intelligence (OpenCTI) [103]

OpenCTI is a platform that aims to provide a powerful knowledge management database [103]. The platform was launched in 2018 and is still undergoing intensive development [104].

OpenCTI supports all four phases of the CTI lifecycle. The collection of TI takes place by ingesting data from internal and external sources (e.g., AlientVault, CVE, MISP) in a structured format (STIX 2.0) [103–105]. Furthermore, own datasets can be implemented [106]. Data collection can be performed manually via the user interface or automatically via API, using connectors to third-party sources [20, 104]. Various functions support the aggregation of TI in order to structure, organize, correlate and enrich the ingested data [103–106]. Both correlation and classification mechanisms are well performed by OpenCTI [20]. To structure and classify the data, OpenCTI provides a connector to use the MITRE ATT&CK framework. Therefore, a knowledge schema based on the STIX 2.0 standards is used [104, 106]. The platform also provides connectors to enrichment services (e.g., AbuselPDB and Malbeacon) and stream consumers (e.g., Splunk, QRadar) [104]. Tools as MapReduce and Pregel computations support exploration and correlation of data. Automatic correlation of all data in the platform is enabled and will be further developed in the future [20, 103]. Furthermore, the platform relies on a knowledge hypergraph based on an entities-relations model, allowing the usage of entities and relationships to add knowledge to the platform

[103, 104]. Linking mechanisms allow inferences of relations to support the knowledge management of information. Therefore, OpenCTI uses the capabilities of the Grakn database [104, 106]. To support the analysis of TI, the platform states to explore, pivot, and visualize existing information. However, there is no detailed information about the functions and tools available to support the analysis phase. To support the analysis of TI, connectors to third-party tools like Cortex and Maltego are provided [104]. OpenCTI visualization capabilities, allowing entities and relationships to be visualized via customizable dashboards offering multiple views and dynamic widgets. Therefore, the platform relies on various tools, including visualization plugins [20, 103–106]. The platform does not mention rating or prioritization capabilities. The dissemination of the TI takes place by a push mechanism, enabling to export and share knowledge in various formats [105]. The platform provides real-time capacities by synchronizing multiple OpenCTI platforms and automated reasoning performed by the database engine [103, 107].
Relating to data privacy, the platform provider offers a short privacy policy on the homepage without indicating its validity for the OpenCTI platform [108]. OpenCTI uses TLP for information sharing. Furthermore, relationships between entities are connected to a specific source provided with a specific confidence level to evaluate information and the associated source [105]. According to Menges et al. [54], the platform does not address data integrity, data availability, quality assurance, or fairness. However, OpenCTI partially addresses non-repudiation, which is ensured by the platform administrator and requires an appropriate level of trust [54]. Importing data is possible in PDF and STIX format and export of data in CSV and STIX format. The import of data can be performed either automatically or manually [20, 104, 106]. OpenCTI follows a community-centered approach. Data access and collaboration between platform users can be performed using particular instances or groups, with permissions based on markings [20, 103]. From a developer perspective, OpenCTI wants users to share their knowledge to support the usage and improvement of the platform. However, the platform does not provide an incentive system to foster active participation within the community [54]. Several communication channels are provided, also concerning development issues (e.g., slack channel, troubleshooting page, Github issues module, Twitter, LinkedIn) [104, 106]. The platform allows the creation of reports in PDF format. Knowledge can be added to existing reports to source entities and relationships. This can be done either programmatically (via connectors or python client) or manually (via web interface) [104].

OpenCTI has been classified as an operational platform built on a modular approach that allows expansions and forks. From an architectural perspective, the API serves as the platform's core and allows clients to interact with the database and broker (messaging system) [104]. To use the platform, different deployment options such as virtual machine template, docker, or manual deployment are provided [104, 106]. OpenCTI provides a GraphQL API, allowing the integration with external tools and applications (e.g., MISP, TheHive, MITRE ATT&CK). Therefore, the platform provides so-called connectors for the following purposes: external data import (e.g., AlienVault, CVE), stream consumer (e.g., ElasticSearch, Q-Radar), enrichment (e.g., AbuselPDB, Malbeacon), internal files import (PDF, STIX), internal files export (CSV, STIX), and third parties modules and plugins (Cortex, Maltego). Connectors are python processes based on RabbitMQ, developed and contributed by both the platform's core development team and the community [104, 106]. As of today, the platform provides no integration capabilities to existing security infrastructure. However, this is planned for future developments [103]. OpenCTI is designed as a modern web

application and has a user-experience-oriented GUI in the form of a dashboard, available in English and French [103, 104, 106].
To produce TI, OpenCTI uses various external sources (e.g., AlienVault, CVE) and allows users to add their own datasets [104–106]. OpenCTI provides technical and non-technical TI, ranging from the strategic level (e.g., intrusion sets, campaigns, malware) to technical (indicators, TTPs, and observables). The platform provides TI in a structured form (STIX) [103–105]. OpenCTI is based on a holistic, unified, and consistent data model, relying on a knowledge hypergraph. STIX (STIX 2.1) is mentioned as a description standard, whereas some integration is required to use TAXII 2 as an exchange protocol [20, 103, 104, 106].
The OpenCTI project was initially launched in 2018 internally by the French national cybersecurity agency (ANSSI) in collaboration with the Computer Emergency Response Team of the European Union (CERT-EU). The primary goal of this project was to develop and facilitate ANSSI's cyber defense missions and interaction with its partners. For sharing the OpenCTI platform, including the knowledge to the global cyber threat intelligence community, the source code was released publicly in 2020. Today, public OpenCTI is developed and maintained by Luatix, a French non-profit organization belonging to the Citeum foundation [103–106]. According to the ISIC classification, all three mentioned organizations belong to the category 'U'. No information is provided relating to the platform's user.
The source code is free of charge and available under Apache 2 license. Furthermore, a free demo instance is available [20, 54, 103, 104, 106]. To support OpenCTI, different types of memberships and donation options are provided [104]. No sectoral and geographical focus has been identified. OpenCTI aims to be used by any public or private organization that needs to structure its cyber threat intelligence knowledge [109].

Open Threat Exchange (OTX) [110]

OTX is part of the AT&Ts Unified Security Management (USM) platform and is labelled the world's largest open threat intelligence community. The platform was launched in 2012.

OTX supports three phases of the TIS process [13]. The collection of TI occurs through the ingestion of various sources (e.g., blogs, threat reports, log files, emails, URLs, PCAPs, text files). Data can be ingested manually via the web interface or semi-automatically via the platform's API [13]. The ingested threat data are called pulses, presenting collections of IOCs (at least one IOC per pulse). Pulses provide details and a summary of the threat, the software targeted, and the related IOCs reported by the OTX community worldwide [52]. To support the aggregation of TI, OTX provides a pulse wizard, automatically extracting IoCs from the ingested sources. Furthermore, the platform states to enable validation, editing, and tagging of threat data. Users can edit pulses with suggestions such as new tags, targeted countries and industries, new references, and indicators of compromise. The analysis of TI has been outsourced to experts of AT&T Cybersecurity, testing, evaluating, and reprocessing the previously ingested threat data [13]. Therefore, the Alien Labs malware and threat analysis engine is used, providing static and dynamic analysis. All files and URLs ingested into the platform automatically run through the engine, including multiple layers of automated checks, analytics, and machine learning (ML). Afterward, a dynamic analysis using the platform's sandbox can be conducted. For this process, a dashboard is provided to see the status of a submission. The resulting indicator (IOC) of the analysis can be added to a new pulse or an

existing pulse. OTX provides a history of all submissions, including easy search and filter capabilities within the dashboard. Furthermore, OTX Endpoint Security provides a threat-scanning service to identify malware and other threats on endpoints by searching for IOCs. The dissemination of TI takes place by various options, including automated push and manual pull mechanisms [13]. The OTX DirectConnect API allows to integrate and synchronize TI with existing security infrastructure automatically. Additionally, browsing and search capabilities are provided to subscribe to relevant pulses submitted by the OTX community. The web interface can download TI in multiple formats and ingest threat data into existing security tools. Sharing can occur either public or private, providing real-time capacity [13, 75].
To ensure the security of personal data, the provider states to apply several technological and organizational security controls. The provider's privacy policy regulates data privacy. An additional Data Processing Addendum is provided, including GDPR-conform policies and processes. AT&T issues specific privacy notices to meet the data privacy requirements of other countries or regions (e.g., EU's General Data Protection Regulation (GDPR), Brazil's General Data Protection Law (LGPD), New Zealand's Privacy Act). To further enhance information security and data privacy, the platform uses TLP when sharing TI. A transparency report is published by AT&T Cybersecurity twice a year. According to Bauer et al. [13], OTX takes internal measures relating to data quality, whereas Wagner et al. [77] identified no internal vetting process to be in place. Relating to trust, OTX fosters reputation building by a mechanism to subscribe, follow and vote for pulses or OTX contributors [13]. However, critical in terms of increasing trust is that OTX allows threat feeds to be entered anonymously without requiring authentication of the feed owner [52]. Regarding the service availability of the platform, a monitoring page shows the operational status of OTX. The last unscheduled downtime of the system was in October 2019. OTX provides automation capabilities regarding the import and export of TI data [52]. Therefore, the platform supports STIX as import and export standards and additional OpenIOC and CSV as export standards [13]. Within the OTX community, everyone can actively discuss, research, validate, and share the latest threat data, trends, and techniques. Additionally, collaboration is enhanced by the previously mentioned option to subscribe and follow pulses and contributors. TI, in the form of pulses, can be shared either to the whole community, a specific group or kept private. Furthermore, OTX provides comment sections and forums [13]. OTX provides comprehensive reporting functions, allowing customized and visual reports [13]. In the analysis engine, a results overview is generated on the dashboard, providing details of the analysis in textual form.

The platform has been identified as an operational platform, providing various SDKs to extend and customize the platform's functionalities (e.g., Java SDK, Python SDK, and Golang SDK) [13]. Concerning the sharing concept, Wagner et al. [77] identified the platform as a hub-to-spoke model. The DirectConnect API allows integrations to existing security infrastructure using DirectConnect agents (e.g., AlienVault USM, TAXII, Suricata). Currently, OTX lists 29 out-of-box API integrations (e.g., MISP Importer, Signature Base, HostIntel, ThreatPinch). The platform provides a GUI in English language [13].
OTX ingests internal and external sources, including private entities, public entities, and other resources [77]. Additionally, honeypots operated by the provider are used by OTX [13]. OTX provides TI ranging from technical TI to strategic TI, including CVEs, IOCs, and high-level

reports. The TI is provided in structured and unstructured form (English) [13, 52]. STIX is listed as a description standard, whereas TAXII serves as an exchange protocol [13].
OTX is a product of AT&T Cybersecurity (formerly AlienVault), a subsidiary of AT&T Communications LLC (subsidiaries of AT&T Inc.). AT&T Cybersecurity is a medium-sized company for computer and network security founded in 2007 (ISIC category 'J') [111]. The company is headquartered in Texas (global), Ireland (EMEA), and Australia (APAC), with additional offices in Spain and Texas. Regarding the provider's role, AT&T Cybersecurity uses the platform for its own Unified Security Management [13]. OTX currently has more than 100 000 participants in 140 countries (e.g., Shake Shack, Soulcycle, Apple Bank, pwc).
The platform is open-source licensed and free of charge [13, 52]. OTX targets a global intelligence community and has no specific geographical focus. OTX follows a multi-sector focus, addressing, amongst others, private companies, government agencies, and independent security researchers.

Threat Connect [112]

ThreatConnect is an intelligence-based model supporting a broad range of use cases [52]. It combines cyber risk quantification, threat intelligence, orchestration and automation, analytics, and templated workflow. The platform was launched in 2013.

ThreatConnect supports all four phases of the TIS process. The platform uses Playbooks to orchestrate people, processes, and tools along the whole intelligence process. Playbooks provide a drag-and-drop interface, enable automation of cybersecurity tasks and continuous dynamic decision-making. The collection of TI occurs by ingesting data from internal and external sources in an automated manner. Both structured and unstructured formats are allowed [52, 113]. The aggregation of TI is supported by functions to correlate, enrich, tag, map, format, and associate data. Therefore, various enrichment services are provided, enabling automated data processing (e.g., DNS, Maltego, WHOIs, IP Geolocation). Furthermore, Playbooks provide automation capabilities of various processing and exploitation methods. To support the analysis of TI, functions are provided to browse, filter, prioritize and visualize data. The analysis phase is supported by intelligence frameworks such as the Diamond Model of Intrusion Analysis, Lockheed Martin's Cyber Kill Chain, or MITRE ATT&CK [52]. Via the platform's API, integrations to multiple analysis tools are provided (e.g., ANY.RUN, Joe Sandbox, Splunk). Furthermore, the platform provides an automated analysis of phishing emails. Visualization capabilities are provided in the form of customizable real-time dashboards [52]. Furthermore, GraphView enables the illustration of relational information between indicators. Scoring rules and indicator ratings can be performed, and advanced filtering methods using the platform's query language (TQL). To disseminate the produced TI, ThreatConnect uses a push mechanism. The platform's API enables integration of TI to existing security infrastructure (e.g., SIEMs, firewall, EDS). Furthermore, TI can be shared to other ThreatConnect instances, using comments, notifications, emails, and integrations to third-party reporting tools. ThreatConnect Playbooks support real-time access to TI.
ThreatConnect provides functions to enhance information security by implementing and maintaining appropriate technical and organizational measures. Furthermore, data privacy is guaranteed by the platform's privacy policy, which is compliant with GDPR 2016/679. International transfers of personal related information outside the EEA are protected by safeguards, including the use of EC-conform standard data protection clauses, binding corporate rules conforming with the Swiss-U.S.

and EU-U.S. Privacy Shield or other adequate safeguards. According to Keim et al. [52], ThreatConnect provides authentication and confidentiality when sharing data. The platform provides no details on how to enhance data quality. Wagner et al. [77] identified no internal vetting process to be in place. No information is provided by the platform on how trust gets enhanced. The platform states to provide automated email import and allows export of TI in the form of reports. STIX is used to support TI sharing. Additionally, Keim et al. [52] identified the platform allowing imports in various formats (e.g., CSV, custom XML/JSON, IODEF, OpenIOC, PDF, Office documents, email). Furthermore, the authors identified a restriction of import and export indicator details to limited open source communities [52]. Collaboration between platform users is enhanced by sharing information with other teams across organizations and industries. Thereby, a feedback and improvement loop is established. Integrations like Microsoft Teams or Slack support collaboration. Furthermore, TC Exchange, located within the platform, gives platform users a chance to collaborate, share information, and join or create communities. No information relating to anonymity levels is given. Relating to developer issues, via ThreatConnect's Github repository, users can share various tools, Playbooks, and Apps they have created for the platform. ThreatConnect enables the creation and sharing of threat reports on various types of data from the platform. The reports can be customized with filtering options such as specific threat actors or campaigns and downloaded in PDF format.

ThreatConnect has been classified as an operational platform, providing several SDKs for customizing and extending the platform's capabilities (Java, JavaScript, Python) [114]. Addressing different network designs, various deployment options are provided like dedicated cloud, on-premise, and cloud-based. The platform is based on a REST-API, enabling integrations to existing security infrastructure (e.g., SIEMs, firewalls, EDR solutions). Furthermore, integrations to various tools, including data enrichment, malware analysis, and vulnerability management, are provided. ThreatConnect currently offers 106 integrations (e.g., Joe Sandbox, Splunk, Qualys). The platform provides a GUI in English language.

ThreatConnect uses internal and external sources to produce TI [52, 77]. These include internal logs, OSINT feeds, blogs, RSS feeds, and other intelligence feeds provided by a third-party provider or an ISAC. Currently, ThreatConnect provides 30 external feeds. A unique feature is the provided ThreatConnect Intelligence Source feed; a premium intelligence source focused on criminal and nation-state threats. Furthermore, the platform provides so-called Collective Analytics Layer (CAL) feeds, including CAL Suspicious New Resolution IPs, CAL Suspicious Newly Registered Domains, CAL Suspicious Nameservers, and CAL Suspected Ranking Manipulator. The TI provided by the platform ranges from tactical TI, including IOCs, up to strategic TI in the form of executive-level reports about threats, available in structured and unstructured format [52]. ThreatConnect provides a flexible data model, using STIX as a description standard and TAXII as an exchange protocol.

The platform is owned by ThreatConnect, Inc., a medium-sized company for cyber and network security founded in 2011 (ISIC category 'J') [115]. The company is headquartered in Arlington, VA, US, and has an additional office in London, UK. Regarding the user group, the platform states that security professionals around the globe of every level and discipline are using ThreatConnect. No information was available regarding the number of users and their organization size.

The platform is closed source licensed and requires a recurring fee per subscription period to use the offered services [52]. Creating a user account is for free. Furthermore, the platform provides a demo version. Besides its comprehensive closed-source platform, ThreatConnect also offers TC Open, an open-source and free format to start with threat intelligence [52]. Compared to the full platform, the capabilities of TC Open are significantly limited. TC Open includes one user license; Access to 100+ open source intelligence feeds (OSINT); Access to threat, incident, and adversary data; Ability to collaborate or consume active and historic indicators, incidents, and threats; Validate your findings with peers in the ThreatConnect Common Community. ThreatConnect is not restricted to any geographical area. The platform explicitly targets the following key industries: financial services, government, healthcare, MSSP, retail, technology, and energy and utilities.

ThreatQuotient [116]

ThreatQ is a threat-centric platform, supporting various use cases, reactive and proactive [117]. The platform was launched in 2015.

The platform supports all four phases of the TIS process [13]. Across phases, the platform claims to have built-in operations to automate manual tasks. The collection of TI occurs by ingesting threat data from multiple sources, both internal and external [13, 118]. ThreatQ allows ingestion in either structured or unstructured format (e.g., STIX, XML, JSON, PDF, email). Furthermore, the processing of bulk data is enabled. The aggregation of TI is supported by functions to deduplicate, normalize, correlate and enrich threat data [13, 118]. The platform supports the aggregation phase by providing signature and rule management (YARA, OpenIOC, Bro/Zeek, Suricata, Snort). Automation capabilities are provided relating to aggregation and optimization of threat data. TI analysis is supported by capabilities to analyse, visualize, score, and prioritize the previously processed data. Therefore, ThreatQ provides functions like adversary handling, spear phish parsing, and alert triage [13]. Adversary handling aims to build a holistic picture of an adversary, campaign, TTP, and others. The automatic spear phish parser enables more efficient triage based on analyst familiarity of adversary TTPs. ThreatQ furthermore enables alert triage, supported by visualization of alerts and context. User-specific scoring and automatic prioritization of threat data are enabled, allowing a dynamic assessment of threats. Relating to visualization capabilities, customizable dashboards, including watchlists and event timelines, are provided [118]. During analysis, the collaboration between platform users is enabled [13]. The analysis phase offers customization options regarding the automation of processes, where users can decide to automate an entire process or just selected aspects. The dissemination of TI takes place by automated push mechanisms [13]. The created TI can be automatically shared internally to team members or externally to third parties. Reporting and export capabilities allow the integration of TI into existing security infrastructure (e.g., SIEMs, EDR). Sharing controls enable a customized sharing of threat data. Real-time capacity is not exclusively mentioned by the platform but can be assumed according to various automation mechanisms.
Concerning information security, the platform states to apply appropriate technical and physical safeguard measures [13]. Data privacy and the related information collection, information use, sharing, and disclosure is governed by the platforms privacy policy based on US law [13]. Furthermore, ThreatQ complies with the European Union’s General Data Protection Regulation (GDPR), the EU-U.S. Privacy Shield Framework and Swiss-U.S. Privacy Shield Framework. To

ensure the data privacy of cross-border data transfers to third parties outside the European Economic Area (EEA), the platform developed appropriate safeguards. To further enhance information security and data privacy, the platform defined sharing controls based on TLP and data ownership. Data ownership is dependent on the deployment option. Relating to data quality, Wagner et al. [77] identified an internal vetting process to be in place. According to Bauer et al. [13], the privacy policy is also used to build trust. ThreatQ states to provide various formats for importing and exporting data (e.g., STIX, XML, JSON, PDF, email, and other formats). Bauer et al. [13] identified STIX and OpenIOC as import standards and STIX as export standard. ThreatQ allows sharing and collaboration across industries and to other stakeholders [77]. ThreatQ designed a cybersecurity situation room (ThreatQ Investigations) for collaborative threat analysis, shared understanding, and coordinated response to facilitate collaboration and coordination among and across teams. Team tasking allows assigning tasks, collaborating, and coordinating responses and investigations between cross-functional teams [13]. All security teams can use and update threat intelligence as part of their existing workflow without changing processes. Furthermore, feedback is captured in a central database for instantaneous knowledge sharing. Regarding the reporting capabilities, the platform states to generate strategic, operational, and tactical reports. The reports can be customized and are available in PDF or JSON format.

ThreatQ has been classified as an operational platform, providing an SDK to extend and customize the platform [13]. Flexible deployment options are provided to fit the individual network design, including on-premise, cloud-based, virtual instance, dedicated appliance, and air-gapped. The platform is based on an open API, allowing various integrations to existing security infrastructure (e.g., SIEMs, log repositories, ticketing systems). Furthermore, multiple integrations to third-party services are provided, e.g., for enrichment or analysis. Currently, the platform provides 110 out-of-box integrations. The platform provides a GUI in English language [13].
The platform allows internal and external data sources to flow into the platform [13, 77, 118]. ThreatQ ingests various feeds, including commercial, open-source, government, industry, internal, and custom intelligence feeds. Currently, integrations to over 50 commercial data feeds and more than 100 public data sources are provided. The TI provided by ThreatQ includes tactical TI (TTP) and strategic TI (high-level reports) in a structured and unstructured format (English) [13]. Organizations can also define custom objects to collect information that is of particular importance to their organization. The platform has a flexible data model, supporting STIX and OpenIOC as description standards and TAXII as exchange protocol [13]. Furthermore, the platform supports STIX 1.1, STIX 1.2, and STIX 2.0.
The platform is owned by ThreatQuotient, Inc., a medium-sized company for cyber and network security, founded in 2013 (ISIC category ‘J’) [119]. The company is based in Northern Virginia, US, and has additional Europe, APAC, and MENA operations. The TI generated on the platform is used by the platform's internal IT security management [13]. Leading global companies, including Fortune 100 and Fortune 500 companies, major retail, hospitality, healthcare, technology, finance, and defense customers belong to the users of the platform (e.g., Airbus Cybersecurity, Sopra Steria) [120].
ThreatQ is a commercial product and requires payment. Furthermore, the platform provides a free demo version. With its operations worldwide, ThreatQ can be classified as a globally operating platform. The platform has no specific sectoral focus, as datasheets are available for various

industries (technology companies, critical infrastructure, government agencies, healthcare, financial services, retail, and hospitality) and different professional roles (CISOs, threat intelligence analysts, SPCs, and incident response teams).

Table 7 and Table 8 summarize the analysis of the platforms and give an overview of the classification of the platforms.[4] Both tables are based on 13 platforms, as LookingGlass scoutTHREAT is not included due to low information. The tables show the number of platforms that provide functionality for a given criterion. The statistics do not take into account the extent to which a platform supports a particular variable. A detailed evaluation and discussion of these results is the subject of Section 5 of this paper.

Table 7: Overview analysed platforms (Functional criteria).

Supported phases of TIS	#
Collection	13
Aggregation	13
Analysis	12
Dissemination	13

Cross-phase support	#
Information security	13
Data privacy	13
Data quality	5
Trust	5
Platform availability	4
Import and export	
Import	11
Export	13
Collaboration	13
Reporting	9
Additional functions	1

Table 8: Overview analysed platforms (Non-functional criteria).

Architecture and interfaces	#
Type of platform	
Operational	13
Software-to-build	10
APIs	
REST-API	9
Others	4
To existing security infrastructure	11
SIEM	9
Firewalls	5
IDS	4
Other (e.g., SOAR, Log management)	6
User interface	
Graphical	12
Command-line	3

Content and standardization	#
Data origin	
Internal	12
External	12
TI provided	
Technical	13
Tactical	11
Operational	6
Strategic	6
TI content form	
Structured	12
Unstructured	7
Standardization	
STIX	12
TAXII	11
OpenIOC	2
Other	3

[4] For the detailed results of the analysis, see also: https://ifi-nabu.uibk.ac.at/index.php/s/bCZ8QML6SsaRtxQ (Password: TISP2021!)

Provider and users		#
Provider		
	ISIC category	J (9), U (4)
	Size	s (2), m (6), l (4)
	Origin	US (9), other (4)
Users		
	Community-driven	5

Usage fees, license and distribution		#
License model		
	Open source	6
	Closed source	6
	Free-of-charge	6
Geographical focus		1
Sectoral focus		3

5 Discussion

In the following section, the key findings of this work and their implications for research and practice are outlined and discussed. In addition, the limitations of this work are discussed. A total of 13 platforms are included in the discussion. LookingGlass scoutTHREAT was not included in the comparison because very little information was available and the results should not be biased due to insufficient information.

5.1 Key findings

Key finding 1: Growing scientific interest as well as several practical implementations in the field of cyber threat intelligence have been observed over the past decade, with a lack of clear delineations

Over the past decade, there has been a significant increase in the number of sources dealing with cyber threat intelligence in general. The proportion of academic literature and grey literature is quite similar. However, especially in the last four years, the proportion of academic literature has increased significantly. Literature dealing with specific platforms has also increased in importance, although there is no discernible steady growing trend. However, only a small subset of sources provides detailed information on specific platforms, predominantly in the form of academic literature.

Looking at the practical side of CTI, almost all the platforms analysed were launched within the last decade, illustrated in Figure 15. CRITs and OpenCTI were initially developed for internal use and later introduced publicly. Blueliv is the only platform for which no launch date could be identified. However, the company itself was not founded until 2009.
A few of these platforms in particular are frequently the subject of in-depth investigations and studies (e.g., CIF, CRITs, MISP, OTX, ThreatQ).

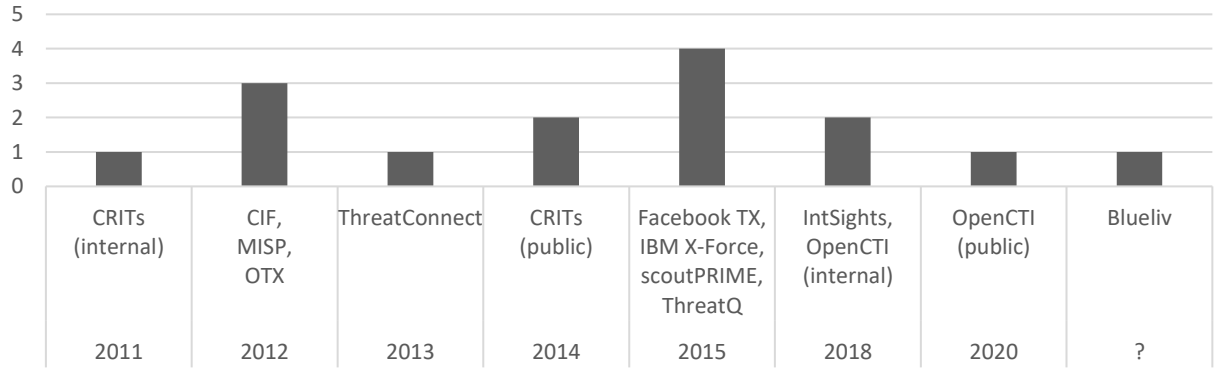


Figure 15: Launch of platforms.

Looking more closely at the theoretical side, different research directions can be identified. For basic research and introduction to the topic, several papers deal with fundamental terms and concepts of CTI. These include the meaning and relevance of TI, different types of threats, and levels of TI. Another direction includes works that addresses TI sharing and standardization. In addition to the benefits of and need for TI sharing, sharing architectures and standardization efforts have

also been examined. Further, some works focuses more on specific aspects and details relevant to TIS and TISPs, such as data quality, trust, and privacy. Finally, several contributions attempt to provide a holistic overview of the TISP landscape. To this end, the currently available solutions are examined according to various criteria.

A closer look at the practical side shows that a variety of solutions have been developed in recent years. There are many different tools on the market that are declared to be CTI-related. However, on closer inspection and following Dandurand et al. [17] these often cannot be classified as TISP. Rather, there are now a wide variety of CTI products and services to meet the individual needs and use cases of users (e.g., PhishTank, VirusTotal). Not all the tools identified in the course of the MLR were examined in this work as relatively narrow inclusion criteria were developed due to the scope of this work. However, based on the tools examined, it can be said that the various tools vary in focus, scope, use cases and popularity. This reflects that consistent definitions and terminologies are lacking and a clear delineation between CTI products is largely absent.
Regarding the features of the available TISPs, almost all platforms take into account the entire TIS process, but some are rather basic in terms of further functionalities. If one considers the details already identified in the literature, such as data quality, privacy or trust, these aspects are mostly not sufficiently taken into account.

In summary, practical development is still in its infancy and the literature is a step ahead, dealing with issues (e.g., sharing model, data quality) at a finer and more abstract level.

Key finding 2: Almost all platforms support all four phases to some degree and provide different automation capabilities

Almost all the platforms analysed support all four phases of the TIS process, even if to varying degrees. For illustration purposes and grouping detection, specific metrics were developed. Therefore, the number of functions provided as well as the given details has been focused, per platform and phase. To measure and compare the different characteristics, a rating schema from 0 up to 3 is underlying. Grey (0) implies that the respective phase is not supported. Orange (1) implies that the platform provides weak support for the respective phase. Yellow (2) implies that the platform provides average support for the respective phase, with some details provided. Green (3) implies comprehensive support for a phase with various functionalities. The results are presented in Table 9.

Table 9: Platforms and four phases.

Phase / Platform	Collection	Aggregation	Analysis	Dissemination
Blueliv				
CIF				
CRITs				
EclecticIQ				
Facebook TX				
IBM X-Force				
IntSights				
scoutPRIME				

MISP				
OpenCTI				
OTX				
ThreatConnect				
ThreatQuotient				

not supported | weak support | average support | comprehensive support

The metrics show that the platforms provide mostly average to comprehensive functionality for the four phases. However, five platforms are providing limited support for a particular phase. CRITs, for example, offers limited capabilities for disseminating TI. For TI analysis, Facebook TX provides only basic functionalities such as searching, querying, and responding to data. IBM X-Force claims to aggregate TI but does not provide further insight into its functions. OTX provides a comprehensive analysis of TI, but this functionality is outsourced within AT&T Cybersecurity. OpenCTI does not allow to disseminate TI into existing security infrastructure.

Overall, most platforms focus on the analysis and dissemination phase. The collection and aggregation phase are supported in average by most platforms.

As shown in Figure 16, the following groups can be identified when considering the phases that are comprehensively supported (marked green in Table 9) by a platform.

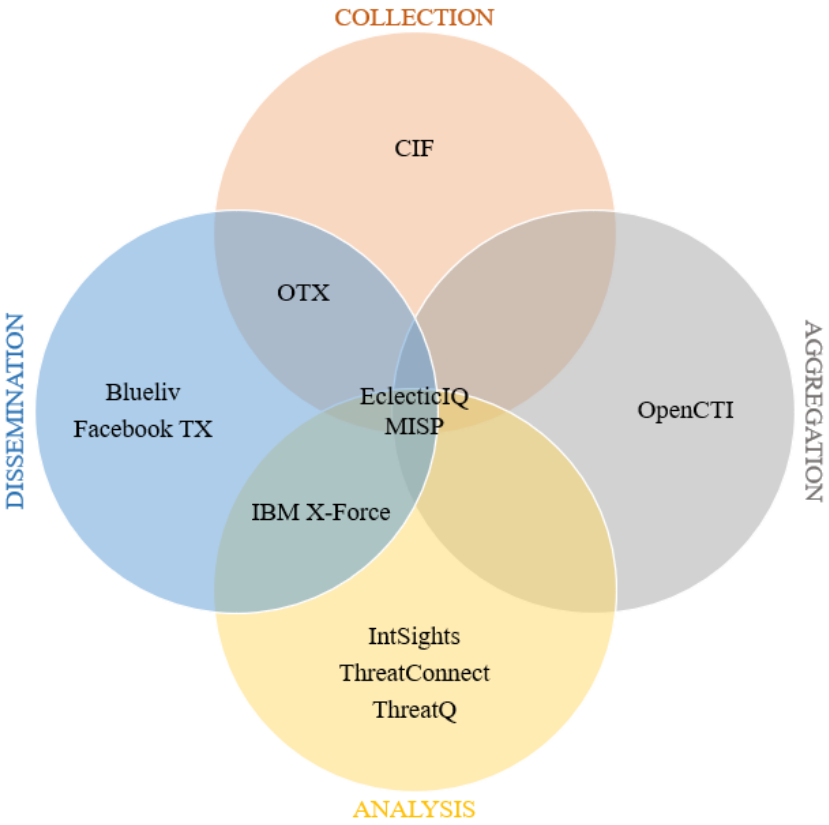


Figure 16: Platform grouping per phase.

EclecticIQ and MISP stand out as the most robust platforms and can be described as allrounders, as they provide comprehensive support for all four phases. CIF and OTX mostly focus on the collection of TI. OpenCTI focuses on the aggregation of TI. IBM X-Force, IntSights,

ThreatConnect, and ThreatQ focus on the analysis of TI. Blueliv, Facebook TX, IBM X-Force and OTX focus on the dissemination of TI.
CRITs and scoutPRIME have been identified as lowest performer as both provide no comprehensive support for any phase. Furthermore, OpenCTI and OTX show a rather narrow focus and support two phases each averagely to comprehensively, while the other two phases are either weakly supported or not supported at all.

With regards to automation capabilities, the platforms support the four phases of the TIS process to varying degrees. Two-thirds of the platforms offer functions for automating the collection process. For the aggregation phase, 12 of 13 platforms offer automation capabilities, at least in part. For the analysis phase, two-thirds provide at least partial automation support. Finally, two-thirds of all platforms offer automation capabilities concerning the dissemination of TI. For some platforms, such as CRITs and ThreatConnect, integrations are partially required.

The different platforms provide automation capabilities to varying degrees. For illustrative purposes and to detect cluster, metrics have been developed to rate the different platforms. Therefore, three categories are distinguished to describe the level of automation. Red implies that no automation capabilities are present or mentioned. Yellow means that automation capabilities are partially present, i.e., for individual processes. However, this partly requires integrations or customizations. Green means that comprehensive automation capabilities are provided by default. Table 10 shows an illustration of the automation capabilities of the platforms for each phase.

Table 10: Automation capabilities.

Phase / Platform	Collection	Aggregation	Analysis	Dissemination
Blueliv				
CIF				
CRITs				
EclecticIQ				
Facebook TX				
IBM X-Force				
IntSights				
scoutPRIME				
MISP				
OpenCTI				
OTX				
ThreatConnect				
ThreatQuotient				

no automation capabilities partial automation options comprehensive automation capabilities

Of the four phases, most automation options are available for the aggregation phase. Conversely, the fewest automation options provided by the different platforms are available for the analysis phase. Overall, rather good automation capabilities were identified for three platforms (Blueliv, EclecticIQ, OTX). Likewise, three platforms offer relatively weak automation capabilities (Facebook TX, IBM X-Force, scoutPRIME). The remaining seven platforms have average to slightly above-average automation capabilities.

In conclusion to the findings shown, it can be said that the differences between the platforms, some of which are considerable, reflect the lack of basic understanding of the entire topic.

Key finding 3: Almost all platforms allow the ingestion of structured data from multiple sources

Across all platforms, the collection of TI is well performed. To generate TI, platforms can use both internal sources generated by the platform or the user of the platform and external sources generated by third parties. Almost all platforms (11 out of 13) allow multiple sources to be included, including internal and external. CRITs does not provide any information at all about the sources used. Facebook TX is the only platform that does not ingest external sources. In summary, platforms draw external information from various sources, including open, private/commercial, and closed sources. These include blogs, partnerships, hacktivism resources, sinkhole sensors, honeypots, crawlers, spam traps, darknets, DNS information, global threat databases, and many other databases (e.g., actor databases). Seven platforms provide an overview of all sources used to create TI. ThreatQ offers the most comprehensive set of external data sources, with over 50 commercial and more than 100 public data sources.

In addition, some platforms offer special services. For example, five platforms offer one or more platform- or vendor-specific feeds. IBM X-Force has also implemented a threat feed manager that enables the aggregation of multiple sources. ThreatConnect provides a feed focused on criminal and nation-state threats. ScoutPRIME makes it possible to pull information from the dark web.

Regarding the data format, five platforms were identified to allow structured and unstructured data for ingestion (EclecticIQ, scoutPRIME, MISP, ThreatConnect, ThreatQ). Another three platforms claim to ingest different formats (Blueliv, CRITs, Facebook TX). In the case of CIF, IntSights, and OpenCTI, at least structured data can be ingested into the platform. IBM X-Force is the only platform that does not provide any information about the supported ingestion formats.

There is little to no information on how to handle unstructured data. In general, unstructured data, unlike structured data, requires additional steps and tools to store, process, and analyse the data. As outlined earlier, several platforms claim to enable the ingestion of unstructured data. To further process this data, platforms list features such as automatic collection, free text importers, and parsing. CIF, CRITs, and MISP enable parsing of unstructured data. In addition, CIF and CRITs state to use a non-relational database (ElasticSearch, MongoDB) where raw and unstructured data can be stored. MISP further mentions the use of a heuristic-based algorithm to further process the raw data.

Key finding 4: Platforms focus primarily on correlation and enrichment of data to support aggregation of TI

Almost all platforms support TI aggregation. Looking at the aggregation capabilities of all platforms, it is noticeable that there is a focus on correlation and enrichment functions. For this, the platforms use various third-party services such as DNS, Geo-IP, or WhoIs. In addition, functions for tagging and marking threat data are offered by half of all platforms. Classification functions and the application of signatures and rules are less focused. Classification functions are only offered by a quarter of all platforms examined. Frameworks such as MITRE ATT&CK, Diamond

Model, or Kill Chain are provided for this purpose. Four platforms use signatures or rules such as YARA rules.

MISP and OpenCTI provide the most extensive functionality to support the aggregation of TI. Blueliv also claims to provide many functionalities, but no details are provided. Poor functionalities are provided by CIF, Facebook TX, and OTX. Finally, in the case of IBM X-Force, the platform claims to aggregate and organize data but does not provide any further information.

Key finding 5: Collaboration during analysis is allowed, providing different functionalities

The analysis of TI is supported by almost all platforms. EclecticIQ, IBM X-Force, ThreatConnect, and ThreatQ provide the most comprehensive analytics capabilities and information. CIF and Facebook TX offer minor capabilities or details about them. OTX outsources analysis of TI.

Except for OTX and Facebook TX, all platforms offer visualization capabilities, some of which require third-party services such as Kibana and Maltego (e.g., CIF, CRITs). In addition, three-quarters of the platforms enable sorting, scoring, or prioritizing threat data.

Collaboration and threat intelligence sharing are enabled and supported by almost all platforms. Sharing threat intelligence and knowledge between users can help provide more profound and robust insights on threat intelligence. However, the ability within platforms to do this varies.
Eleven platforms offer specific exchange channels that allow users to collaborate privately, publicly, or in communities. These include private instances, internal groups, trusted third parties, communities, or secure workspaces. Additionally, MISP allows users to act pseudo-anonymously. IntSights and scoutPRIME do not specify support for different exchange channels.
In addition, some platforms offer features such as comments, forums, and voting to enhance collaboration (e.g., EclecticIQ, MISP, OTX). EclecticIQ and ThreatQ enable task assignment and management. ScoutPRIME enables sharing of customizable dashboards and other tools such as checklists. ThreatConnect and ThreatQ capture feedback generated during collaboration and use it for improvement and knowledge sharing. ThreatQ has developed its own cybersecurity situation space to support collaborative threat analysis. OpenCTI and ThreatConnect provide integrations (e.g., Microsoft Teams, Slack) to support collaboration. For CIF, Facebook TX, OpenCTI, and ThreatConnect, additional channels and resources support platform handling and development issues (e.g., GitHub).

Key finding 6: The dissemination of TI is largely enabled by push mechanisms as well as out-of-the-box integrations into the existing security infrastructure

The dissemination of TI is supported by almost all platforms, while CRITs offers only limited sharing capabilities. The remaining 12 platforms follow a formal sharing mechanism in the form of a push mechanism to disseminate TI. Four platforms additionally provide a pull mechanism (CIF, IBM X-Force, MISP, OTX). Finally, MISP also uses a third mechanism, cherry-picking.

All platforms except CRITs and OpenCTI enable the dissemination of TI into the existing security infrastructure. To do this, the platforms provide out-of-the-box integrations that allow TI to be fed directly into an organization's internal security tools to get the most value from the platform.

Unlike stand-alone platforms, these integrations accelerate the automation of TI sharing and save resources on manual TI dissemination and interface setup.

The following Table 11 provides an overview about the tools, each platform can interact with by default. Most platforms provide out-of-the-box integrations to IDS, firewalls, and SIEMs.

Table 11: Interaction with existing security infrastructure.

Tools / Platform	IDS	Firewalls	SIEM	SOAR	Log management	Endpoint protection	Others
Blueliv			x	x			
CIF	IDS, IPS	x	x				
CRITs	Not per default, only via extensions						
EclecticIQ	x		x			Endpoint Protection & Monitoring	Incident workflow, IDP, IAM
Facebook TX				x	Log-, monitoring- & reporting platform		
IBM X-Force	No further details						
IntSights		x	x				
scoutPRIME		x	x				Security gateways
MISP	x	x	x				
OpenCTI	Planned for future developments						
OTX	x		x				
ThreatConnect		x	x			EDR	
ThreatQ			x	x	Log repositories	EDR	Ticketing systems, incident response platforms

In addition, nearly all platforms enable sharing with colleagues, teams, or other instances. Only IntSights does not explicitly mention this capability. Furthermore, nine platforms mention the opportunity of customizable distribution policies.

Apart from CIF and CRITs, all platforms offer the possibility of accessing TI in real-time. In the case of ThreatQ, this capability is not explicitly mentioned, but is very likely due to various automation options.

Key finding 7: Measures are taken to improve information security and privacy without considering data integrity and availability

In order to assure and enhance information security and data protection, the majority of platforms provide a data protection policy and other measures. To this end, the platforms use company-

specific safeguards in the form of technical and organizational measures, rules, and practices. Furthermore, as shown in Table 12, general standards and directives are used (e.g., EU-US Privacy Shield, GDPR, ISO/IEC 27000 series). Additionally, five platforms consider data transfers in their privacy statements and offer extensions, primarily based on EU-compliant standards. CIF, CRITs, and OpenCTI do not mention specific information security measures, while no privacy policy was found for the latter either.

About two-thirds of the platforms offer additional functions to ensure information security and data protection. For example, nine platforms offer features to support confidentiality and authentication when exchanging information (e.g., TLP, confidence levels). In addition, EclecticIQ and MISP also provide encryption capabilities.

Any platform gives neither data integrity nor data availability special consideration. However, especially data availability is difficult to measure.

Table 12: Information security and data privacy directives.

Directive / Platform	GDPR	EU-US Privacy Shield	ISO/IEC 27000 series	Others
Blueliv				Spanish Data Protection Agency
CIF		x		
CRITs				
EclecticIQ	x			
Facebook TX	x	x		
IBM X-Force	x	x	27001, 27017, 27018	NIS Directive, California Consumer Privacy Act (CCPA), APEC Cross Border Privacy Rules (CBPR) system, Binding Corporate Rules
IntSights			27001	SOC 2
scoutPRIME				
MISP	x		esp. 27010:2015	
OpenCTI				
OTX	x			Brazil's General Data Protection Law (LGPD), New Zealand's Privacy Act
ThreatConnect	x	x		
ThreatQ	x	x		

Key finding 8: Data quality assessment and measures to increase trust are insufficiently addressed

There is a discrepancy between the state of the science and the state of the practice regarding data quality and trust. Science is further along in this regard and has identified challenges that are important to platforms and are often the subject of CTIS research (e.g., [3, 7, 18, 121]). High-quality CTI is the overarching goal to detect and defend against cyberattacks. However, the increasing

amount of available CTI and the distribution of CTI tools require a closer look at the quality of the information [3, 7].

Scientific research has identified data quality and trust as critical factors in threat intelligence sharing that require further research. Data quality has been identified as a crucial challenge in TI sharing, especially concerning OSINT [3]. In addition, data quality significantly influences trust in the data and thus between users, which is also an essential factor in a shared TI environment. Various attributes and dimensions were developed to measure data quality and trust, such as objectivity, relevancy, reputation, provenance, and believability [7, 18]. In terms of trust in TI sharing, Wu et al. [121] identified three different types: trust between users, trust in the platform, and trust in data quality. Trust in the platform refers to mechanisms supporting confidentiality, integrity, and privacy. However, the assessment and assurance of data quality and trust are not satisfactorily addressed by current approaches [7, 121].

Concerning the subset of platforms studied, neither data quality nor trust are sufficiently addressed. For data quality, Wagner et al. [77] found that EclecticIQ, Facebook TX, and ThreatQuotient have an internal vetting process in place. In addition, CIF allows tagging of threat data to describe the level of certainty of a given observation. EclecticIQ performs automatic quality determination for IOCs. OTX uses internal voting processes to improve data quality. In the case of MISP, quality assurance will be part of future work.

In terms of trust, some platforms offer features that can increase trust when interacting with the platform and sharing information. These include the way users can interact with each other, the reliability of the information available, but also the availability and stability of a platform.
MISP allows reliability and credibility measures to be added to attributes. OpenCTI deals with non-repudiation, which requires an appropriate level of trust. OTX uses internal follow and vote mechanisms to encourage reputation building. However, the owner of the feed can appear anonymous within OTX, which in turn minimizes trust. ThreatQ uses its privacy policies to increase trust. Another measure to increase trust can be to build trusting relationships. Ten platforms allow users to build trusted relationships through private groups, secure channels, or whitelists. Furthermore, four platforms provide information about the status of their operating systems. IntSights and OTX can be described as stable, without any unscheduled downtimes the last year. In contrast, Facebook TX and IBM X-Force had several issues and downtimes since the beginning of 2021.

According to the three types of trust presented earlier, trust in the platform and trust between users are considered quite well by some platforms. Regarding the last type, trust in data quality, only a few details are given. However, based on the information given, careful consideration of this aspect lacks due to the lack of systematic quality assessment.

Key finding 9: The design and capabilities of the reporting features are quite different

Reporting capabilities are provided by nine platforms, six of which are customizable. Few platforms provide more detailed information about the capabilities: EclecticIQ allows for a wide range of reports (e.g., multi-paragraph reports; reports on specific tools, techniques, and procedures; actor profiles, campaign profiles, incident reports, and indicator reports) and allows reports to be linked to other information within the platform. ThreatQ also allows the creation of various reports,

ranging from tactical to strategic. ScoutPRIME offers various reports and allows manual on-demand or scheduled automatic distribution of reports. OpenCTI also allows reports to be created either manually via a web interface or programmatically via API. In the case of OTX, the analysis engine automatically provides the results in the form of text reports.

There is little information about the available form of reports. EclecticIQ, IBM X-Force, and OTX state they allow visual and textual reports. MISP allows visual reports. The most common format for reports is PDF. Other formats mentioned are STIX, JSON, gexf, graphviz, and zip.

Key finding 10: Sharing architectures are in practice hard to identify

The proposed framework distinguishes three sharing architectures that a platform can rely on and which have evolved from the TAXII standard. These include client-server, peer-to-peer, and hub-and-spoke. As described at the beginning of this thesis (Section 2.1.3), the academic literature and the developed standards use these concepts to describe the sharing mechanism of a platform.

In practice, however, it is difficult to identify the underlying concept of a platform. The present work attempted to determine the architecture of the platforms based on the aforementioned sharing taxonomies. However, in most cases, there was not enough information available to do so. Instead, detailed knowledge related to software architecture documentation is required.

Nevertheless, there are some platforms for which information regarding sharing architectures is available or which have already been identified by previous research. Currently, CIF is based on a client-server approach, with the progress of a new technology to enable a peer-to-peer architecture in the future. Facebook TX and OTX have been identified to follow the hub-and-spoke model. OpenCTI provides descriptions of its architecture that indicate the platform is based on the hub-and-spoke model.

Based on the current state of information, this criterion might be excluded from future work as it does not add significant value.

Key finding 11: Most platforms provide a REST-API to enable integrations and customizations

All platforms provide an API that enables integrations with other applications and systems. Nine platforms provide a REST-API. The rest either uses a different type or does not provide further details (e.g., OpenCTI has a GraphQL API).
Facebook TX, IBM X-Force, and MISP provide their REST-API in JSON format. Moreover, Facebook TX's API can be implemented in different languages, namely Python, Ruby, Java, PHP, or cURL wrappers. In addition, IBM X-Force allows changing the output language of the API. A special feature of IBM X-Force is that the API of the platform is available with different scopes and functionalities.

All platforms except CRITs and OpenCTI provide the functionality to integrate with existing security infrastructure (e.g., SIEMs, IDS, firewalls). In addition, eleven platforms were identified to enable integrations to third-party tools and services, such as data sources, enrichment, and analysis. ThreatConnect and ThreatQ stand out with their more than 100 out-of-box integrations each. Facebook TX is the only platform that does not disclose integrations to third-party vendors.

All platforms are available as an operational platform. In addition, ten of them offer an SDK or additional modules and services to extend the platform's functionality and capabilities. In particular, CIF and OTX, and ThreatConnect all offer various SDKs (e.g., Java, JavaScript, Perl, Python, Golang). EclecticIQ offers two open-source projects (Cabby, Open-TAXII) that enable the use of TAXII services. OpenCTI allows its users to create a fork.
SDKs serve as a construction kit to configure the platform according to individual requirements. A platform can be both operational and software to build. This is important regarding individual use cases of organizations.

In addition, seven platforms provide information on deployment options. Six platforms are cloud-based or at least offer a cloud-based deployment option. Other deployment options mentioned are air-gapped, dedicated, docker, hybrid, on-premise, and virtual machine. ThreatQ offers the most flexible deployment options.

Most platforms provide a graphical user interface in English language. All platforms except for CIF provide a GUI in English language. Facebook TX and IBM X-Force provide their GUI in various languages. OpenCTI provides the GUI also in French. CIF is based on a command-line interface. MISP additionally provides command-line tools to interact with the background workers. CRITs provide a command line to interact with the API.

Key finding 12: All platforms provide TI in a structured format, half of which cover the entire range from technical to strategic TI

As introduced in Section 2.1.1, four levels of TI are distinguished that target different stakeholders: technical, tactical, operational, and strategic. The platforms studied differ significantly in terms of the TI they provide. All platforms provide technical TI, consumed by technical means or security operating centre staff. Almost all platforms, 11 in number, also provide tactical TI, consumed by defenders and incident response teams. Operational and strategic TI, consumed by higher-level security staff and at board level, is provided by only six platforms, which indicate that they cover the full range from technical to strategic TI.

Just under half of the platforms offer their TI in at least a structured format. Seven platforms offer their TI in both structured and unstructured formats. The most commonly used standard for structured TI is STIX. In cases where TI is provided in unstructured form, English is the default language.

Key finding 13: STIX and TAXII are the most supported standards to describe and share threat intelligence

STIX, followed by OpenIOC, is the most widely used standard for describing, importing, and exporting TI. All platforms except Facebook TX support STIX as a description standard. Further, all platforms except Facebook TX and scoutPRIME were identified to support STIX as an import and export standard. In the case of CIF, STIX is only supported in a basic format per default. Facebook TX does not explicitly mention supporting STIX. However, the platform was identified to follow a standard machine-processable information exchange format and exchanges TI over HTTPS. In the case of scoutPRIME, STIX could only be identified as an export standard. MISP and ThreatQ additionally support OpenIOC.

TAXII is supported as an exchange protocol by all platforms except CIF and Facebook TX. However, in the case of CRITs, some integration is required. Furthermore, some platforms provide additional functionality to exchange TI. For example, CIF uses feeds to exchange TI between CIF instances. EclecticIQ provides community-specific protocols for exchanging information. Standard extensions (e.g., STIX 2, TAXII 2) are supported by EclecticIQ, scoutPRIME, MISP, OpenCTI, and ThreatQ.

In general, the flexibility and compatibility of the platforms are quite different. In terms of the data model, MISP was identified as the most flexible platform. OpenCTI stands out in that the platform is based on a knowledge hypergraph.

Furthermore, the platforms differ in the design of their import and export functionalities by supporting different formats. The most flexible platforms in terms of data import are CRIT (e.g., STIX, CybOX, bulk import via CSV file, Blob, and Spreadsheet) and MISP (e.g., (bulk import, batch import, free-text import, import from OpenIOC, GFI sandbox, ThreatConnect CSV, MISP format). MISP (IDS, OpenIOC, free text, CSV, RPN, MISP XML or JSON, Graphviz, gexf) is also considered the most flexible platform for exports. Automation options in terms of import and export are mentioned for CIF, MISP (export only), OpenCTI (import only), OTX, and ThreatConnect (email import only).

Key finding 14: Half of the platforms are closed-source, and half are open-source, of which more than a third are community-driven

Six platforms are open-source and charge a usage fee, and six platforms are closed-source and free. In the case of Blueliv, the platform offers a modular architecture that is paid for as needed. ThreatConnect additionally offers an open-source and free option, effectively a light version of the full platform. CRITs and OpenCTI were initially launched as closed source and later made available to the open-source community. For IBM X-Force, different details on the license type can be found in the literature. The platform offers different versions of its API, with the basic version being free. More than two-thirds of the platforms offer a free trial or demo version.

Almost all open-source platforms, except OTX, are community-driven. In the case of CIF, CRITs, Facebook TX, MISP, and OpenCTI, diverse users and developers are welcome and encouraged to contribute. Four platforms (CIF, CRITs, MISP, OpenCTI) are provided by organizations belonging to the ISIC category ‘Activities of extraterritorial organizations and bodies’. The development of each of these platforms involved various institutions, all of which are non-profit organizations, international organizations, or government agencies (e.g., MITRE, REN-ISAC, CERT-EU, NATO). CIF, MISP, and OpenCTI are all maintained today by small, non-profit organizations. CRITs is still maintained by MITRE, a large non-profit organization. These organizations are located in the U.S. (CIF, CRITs), Luxembourg (MISP), and France (OpenCTI). Facebook TX and OTX have commercial providers.

More than two-thirds of the platforms, mostly closed-source, are provided and maintained by organizations that belong to the ISIC category of ‘Information and communications’. Most of them are cybersecurity companies. These companies range from mid-sized (e.g., IntSights) to very large (e.g., Facebook, Inc.). Most of the companies (7 out of 9) are based in the US. Blueliv is based in Spain, and EclecticIQ is based in the Netherlands. Most of the companies have other offices spread

around the world. Facebook Inc., in particular, has a vast number of offices and data centers around the world.

In terms of the role of vendors, IBM X-Force, OTX, and ThreatQ use the platform's produced TI for their own security management. CRITs and OpenCTI were developed primarily as internal projects. CIRCL runs multiple MISP instances to manage cyber-attacks.

Key finding 15: Most platforms are not focused on a specific geographic or sectoral area

In general, the platforms provide little information about their users. Eight platforms report having customers worldwide (EclecticIQ, IBM, IntSights, scoutPRIME, MISP, OTX, ThreatConnect, ThreatQ). In addition, four platforms say they have customers from different sectors and industries (TX, MISP, ThreatConnect, ThreatQ). IBM X-Force specifically cites banks and retailers as customers. ScoutPRIME claims to have commercial and government customers. CIF states to be used by a higher education community. Only a few platforms mention the number of their users. MISP with 6000 organizations and OTX with 100,000 participants stand out.

Except for Blueliv, no geographical focus could be identified for the platforms analysed. Blueliv claims to focus on Spain, the United Kingdom, and the United States.
Additionally, no sectoral focus is identifiable for most platforms. EclecticIQ was found to have a focus on governments and financial institutions. ThreatConnect and ThreatQ focus on key industries such as financial services, government, healthcare, MSSP, retail, technology, and energy and utilities. In Blueliv's case, the vendor focuses on banking, insurance, telecommunications, utilities, and retail. Facebook TX does not have an industry focus but primarily looks for users with technical backgrounds to contribute high-quality and trusted information.

5.2 Implications for future research

In the previous section, the key findings of the literature review and platform analysis were presented. By outlining the state of the art of TISPs as well as the differences and similarities, research questions (a) and (b) in particular were answered. Insufficient attention was paid to research question (c), which addresses further research perspectives and challenges of TISPs.

As key finding 1 showed, the market for TI tools is still quite heterogeneous. In addition, a significant gap was found between the state of research and the state of practice. It appears that the practical side is still in its infancy and platforms are partly being developed in a fairly simple format. This is underlined by key findings 7 and 8, which noted that aspects such as data quality, trust, data integrity, and availability are not sufficiently addressed in platforms. Future work should therefore develop assessments and guidelines for measuring these aspects. Furthermore, there is also a need to explore what factors are useful for building trust. Based on this, practical implementation of these aspects should be the subject of future steps to make TISPs more robust and sounder.

Key finding 2 showed that the features and functionalities of the analyzed platforms differ significantly, which in turn reflects that there is a lack of fundamental understanding of the whole topic around TIS. It also showed that most platforms do not support all four phases of the TIS process to the same extent and have a specific focus. Furthermore, in some cases, certain functionalities

and automation capabilities are insufficiently available. In addition, key finding 12 determined what level of TI is provided by each platform. The subject of future research could build on existing definitional approaches, to develop generally applicable criteria that allow cybersecurity tools to be classified as TISPs (e.g., providing crucial functionalities). With respect to stakeholders and end users, a more detailed examination of the information and scope provided by platforms could be useful. Based on that, a grouping of the platforms can be developed to allow users to make more precise choices based on individual needs or use cases.

Key finding 5 found that most platforms support collaboration, but the ability to do so varies. Because collaboration and sharing are critical factors in combating cyberattacks, further research should be conducted on the different ways and channels through which users can collaborate and share information, as well as how users appear when sharing (e.g., anonymously). Research should also be conducted on what is needed to increase users' willingness to share. From a more architectural perspective and following key finding 10, future research should also investigate the meaning and implementation of sharing architectures. So far, this aspect can only be found in the literature, but the platforms themselves provide little information about it. For this purpose, comprehensive documentation on architectures is necessary.

Key finding 6 noted that most platforms allow integration with existing security infrastructure. To provide long-term cybersecurity and threat intelligence solutions, linkages should be supported and isolated stand-alone solutions should be avoided. To further improve this, interfaces should fundamentally be improved, especially to enable further integrations with other platforms, tools, and other services. As a result, automation would also be driven forward. Future efforts should therefore focus on identifying key security tools and technical requirements for interfaces and integrations. As key finding 11 noted, most platforms rely on a REST API, which is therefore ideally suited for customizations due to its high flexibility and compatibility. In addition, key finding 13 has shown that so far almost all platforms support STIX and TAXII, which can be described as de-facto standards in TIS. Nevertheless, further efforts should be made to advance standardization.

5.3 Limitations

The significance of the results obtained, and the conclusions drawn based on them may present some threats to validity. These include (i) the definition of the search strategy (search terms, inclusion and exclusion criteria), (ii) the definition of TISP, (iii) the conduct of MLR, (iv) insufficient or missing information related to platforms, (v) information quality and trustworthiness, and (vi) generalization and sampling bias. These weaknesses and limitations of the present work are highlighted, as are the measures taken to address them.

A limitation related to the methodology underlying this work might be the definition and application of the MLR procedure. To address this, an extensive preliminary search of the existing literature was conducted to define the MLR procedure, including the search strategy, search terms, and inclusion and exclusion criteria. In addition, to increase validity, the key definitions were reviewed by a second person.
Related to the application of the procedure, there is still a risk due to selection bias. One person performed the MLR without the entire process being reviewed by a second person or the procedure being repeated. Only the final result was reviewed again by a second person. However, it could be

that the inclusion and exclusion criteria were not applied correctly or were influenced by subjective opinions. This, in turn, could lead to an incomplete or distorted literature list and consequently platform list. To minimize this risk, the platform list was compared with previous research and studies.

The MLR is used to identify all platforms currently available on the market and for which research has already been conducted. To identify the platforms relevant to this work, the initial quite extensive list of tools was re-examined against the definition of Dandurand et al. There are two potential risks to this approach.
First, some platforms had to be excluded from the study because the information base was insufficient. Furthermore, platforms may have been misclassified and misrepresented due to insufficient information, leading to bias. Consequently, it cannot be guaranteed that all important information and platforms are sufficiently and correctly represented in the study.
Second, there is no universally accepted definition for TISPs. Although the definition of Dandurand et al. is widely and frequently used, it is still possible that a different definition would have resulted in a different final list of TISPs.

Conducting an MLR implies the integration of non-academic sources in the form of grey literature. For this work, it was necessary to incorporate practical perspectives and opinions into the research and knowledge base. To this end, websites, vendor information, blogs, forums, and other sources were reviewed. Although these sources may be informative, some of them have weaknesses in their quality, trustworthiness, and objectivity. The latter is particularly problematic in the case of commercial platforms, as the providers want to place their product on the market in the most profitable way possible and present it accordingly in an attractive manner. To counteract this problem, as many sources as possible were included per platform to integrate as much different information and opinions as possible and thus reduce biased information.

In addition, a threat to objectivity could also occur in connection with the analysis and classification of the platforms. Only one author carried out the description and subsequent evaluation of the platforms. This must be considered, especially for criteria for which hardly any information was available (e.g., dissemination mechanism, sharing architecture).

Last but not least, another threat to validity could be the generalization of this work. Since only a subset of all TISPs was analysed and evaluated in this work, this sample's general validity and applicability might be limited. Furthermore, the classification system used is not a comprehensively closed framework; instead, it may require expansion to include relevant criteria and weightings. Furthermore, it is fundamentally rather challenging to generalize information about TI, TIS, and TISP. This is due to lacking or heterogeneous definitions and terminologies and thus sometimes strongly diverging results and conclusions. This weakness could not be addressed accordingly, but it could be a topic for future work to build a more comprehensive picture.

6 Conclusion and outlook

The objective of the present study was to investigate the state of the art of TISPs from both theoretical and practical perspectives. For this purpose, to obtain as broad an information base as possible, an MLR was performed, which resulted in an initial number of 1,048 sources. Based on a subset of 15 relevant papers, 13 platforms were identified and analysed, considering the defined research questions. The recently published framework by Bauer et al. [13] was used to classify the platforms. This approach provided a general overview of the TIS field and challenges and further research perspectives. In addition, 15 key findings were derived.

The results show the increasing importance of TI and TISPs. From a theoretical point of view, there has been an increasing interest in the subject in recent years, in various studies. Concerning the practical perspective, various tools have been developed, and various standards and taxonomies established. However, the literature search has shown that only a small subset of all tools is treated intensively in research.

The platforms analysed in this paper have some similarities but also differences. In general, the availability and granularity of information differ, as does the presentation and clarity of the information that the platforms reveal. Almost all platforms support all four phases of the TIS process while enabling collaboration and allowing TI to be shared. However, the individual capabilities behind these functions vary significantly, as each platform has different focuses and goals. Common to all platforms is a focus on correlation and push mechanisms for aggregation and dissemination of TI. Consistently missing is sufficient consideration of data integrity, availability, quality, and trust. For the most part, internal and external sources are used to create TI, but the number of sources available varies widely between platforms. The TI created from these sources ranges from simple TI to high-level TI, with the latter provided by less than half of the platforms. For data dissemination and integration, most platforms use a REST API and support STIX and TAXII. In general, the flexibility and compatibility of the platforms vary widely, especially in terms of import and export formats. However, almost all platforms can be extended and customized.

This work aimed to link to existing research in this field and to answer the defined research questions. Furthermore, it confirms that unified and universal terminologies and specifications for the field of TIS are still missing. Starting from a less granular level, the analysed platforms are quite similar in structure. However, on a more detailed level, the heterogeneity of the platforms reflects a lack of regulation of the TISP market. Furthermore, additional insights could be derived. State of the art in research and state of the art in practice differ, sometimes significantly. Research has identified significant issues concerning some aspects, but these have not yet been sufficiently implemented in practice.

The topic around cyber threat intelligence is still young and constantly evolving. This work has shown that there are still some challenges to overcome to achieve effective cyber threat information sharing. Future efforts and investigations should therefore build on existing research and pursue the following directions.

First, a large-scale study that examines and classifies the entire TISP market should be conducted to obtain a more comprehensive overview. Larger samples can provide more valid and representative results for the defined research questions.

Second, this work has identified several aspects that are important for TIS but have not yet been sufficiently researched and implemented. Of particular note are the criteria of trust, data quality, and integrity. However, there is also room for improvement in terms of automation capabilities as well as integrations and interfaces. In terms of collaboration capabilities, more attention should be paid to how users can collaborate and how anonymity can be handled. Further research is also needed on the importance and implementation of sharing architectures.

Third, as Bauer et al. have already suggested in their work, a weighting of the criteria is still pending. Future work could explore the nature of weighting, i.e., whether individual criteria should be weighted or whether grouping would be appropriate. In addition, research should be conducted into the extent to which weighting makes sense, especially concerning individual use cases and the goals of platform users.

To address these points, it may be helpful to include practical expertise in the form of expert interviews with users and developers.

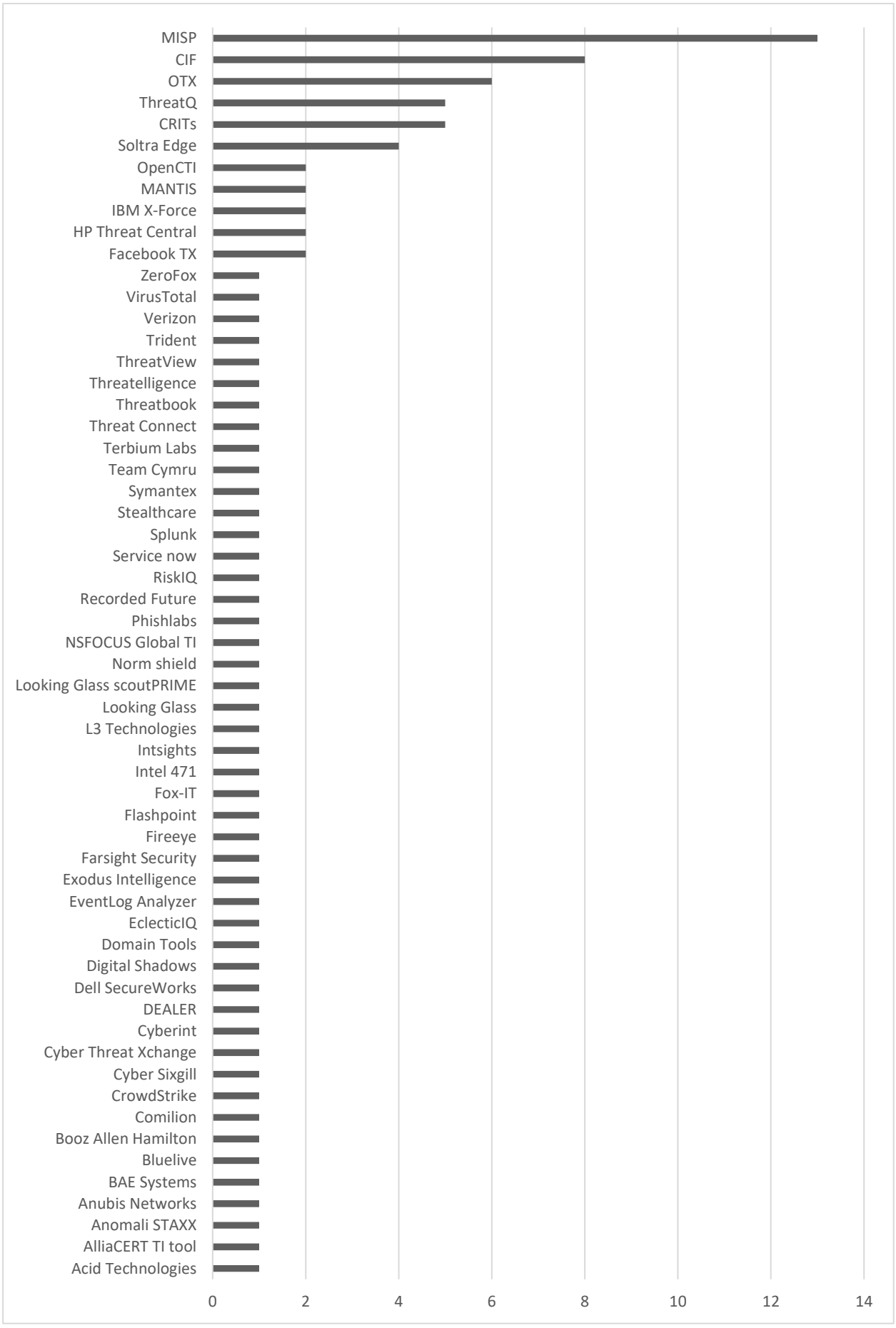
Appendix

A.1 Tools mentioned in the scientific search (N=117)

Accenture Cyber Intelligence Platform	Demisto Security Operations Platform
Acid Technologies	Department of Homeland Security (DHS) Automated Indicator Sharing (AIS)
Alien Vault Unified Security	Digital Shadows
AlliaCERT TI Tool	Domain Tools
Analyst1	**EclecticIQ**
Anomali	EventLog Analyzer
Anomali STAXX	Exodus Intelligence
Anomali ThreatStream	**Facebook Threat Exchange**
Anubis Networks	Falcon Intelligence
AutoFocus	Falcon Intelligence Crowdstrike
BAE Systems	Farsight DNSDB
Blueliv	Farsight Security
Booz Allen Hamilton	Fireeye
Brand Protect	FireEye iSIGHT Intelligence
BrightPoint Security Sentinel	Flashpoint
BT Cyber Security Platform	Fox-IT
BT Security Threat Monitoring	HP ThreatCentral
Cerebral	**IBM X-Force**
Checkpoint IntelliStore	Infoblox threat intelligence data exchange
CIF	Intel 471
Cisco Talos	Intelworks
Cisco Threat Grid - Curated STIX Feeds	**IntSights**
Comilion	Kaspersky Threat Intelligence Portal
CRITs	L3 Technologies
CrowdStrike	Looking Glass
CrowdStrike Falcon	**Looking Glass ScoutPrime**
Crowdstrike Intelligence exchange	LQMT
Cyber Sixgill	MANTIS
Cyber Threat XChange (CTX)	McAfee
CyberConnector	McAfee Enterprise Security Manager
Cyberint	McAfee Threat Intelligence Exchange
Cyber-security information sharing partnership (CISP)	Micro Smart Protection Platform
CyberX	Microsoft Interflow
Cymon	**MISP**
Cyware's Situational Awareness Platform (CSAP)	MTNGOV
DEALER	National Cyber Security Centre (NCSC)
Defense security information exchange	NECCOMAtter
Dell SecureWorks	Norm shield

NSFOCUS Global Threat Intelligence
NTT Global Managed Security Services Platform
OpenCTI
OTX
Palo Alto Networks Next-Generation Security Platform
Palo Alto Wildfire
Phishlabs
PhishMe Intelligence™
PlanetRisk's Global Risk Platform (GRX)
R-CISC
Recorded Future
Risk I/O
RiskIQ
RiskIQ PassiveTotal
RSA NetWitness® platform
SAP EnterpriseThreat Detection
ScoutIQ
SecureWorks Next-Generation Firewall Management Service
SentinelOne’s threat intelligence platform
ServiceNow Bright point
SoltraEdge
Splunk
Stealthcare
StreamForce
Symantex
Team Cymru
Terbium Labs
Threat Intelligence Platform, LLC
ThreatBook
ThreatCloud IntelliStore
ThreatConnect
Threatelligence
ThreatIQ
ThreatQuotient
ThreatStream
ThreatTrack
ThreatView
Verizon
VirusTotal
Vorstack
ZeroFox

A.2 Tools discussed in the scientific search (N=58)



A.3 Tools identified in the Google search (N=135)

A1000	Event Log Analyzer ManageEngine
AbuseIPDB	Exabeam Security Management Platform
Accenture Cyber Intelligence Platform	FireEye AX
ACT	FireEye Helix Security Platform
ActivTrak	FireEye iSight Threat Intelligence
AlienVault OTX	Flashpoint
AlienVault USM	Flowmon Platform
Anomali ThreatStream	Fortinet
Anubis Networks Cyberfeed	Global Threat Intelligence Platform (GTIP)
ANY.RUN	Group-IB Threat Intelligence
Application Insight Cloud Center (AICC)	IBM Qradar
Atera	IBM X-Force Exchange
Augurio	Imperva Attack Analytics
Aushield Defend	Infoblox Threat Intelligence Data Exchange
Authentic8 Silo	IntSights Threat Intelligence Platform (TIP)
AutoFocus	Kaspersky Private Security Network
AV-Atlas	Kaspersky Threat Intelligence Portal
Bitdefender Advanced Threat Intelligence	Kaspersky Threat Intelligence Services
BitLyft	KnowBe4
Blueliv	Lacework
BlueVoyant Threat Intelligence Services	Lastline Defender
BrightPoint Security Sentinel	LogPoint SIEM Threat Intelligence Application
buguroo	LogRhythm
Censys	LogRhythm NextGen SIEM
CenturyLink Analytics and Threat Management	LookingGlass Cyber Solutions scoutPRIME
Check Point ThreatCloud	LookingGlass Cyber Solutions scoutTHREAT
CIF	Malware Bazaar
Cisco SecureX (formerly Threat Response)	ManageEngine Log360 (FREE TRIAL)
Cisco Talos	Mandiant Threat Intelligence (FireEye)
Cisco Threat Grid	Marlabs' Cyber Threat Intelligence Platform Rapid 360°
Cofense Intelligence	McAfee (Enterprise Security Manager)
CRITs	McAfee MVISION Insights
CrowdStrike Falcon X	McAfee Threat Intelligence Exchange
DarkOwl	Mimecast Threat Intelligence
Datadog	MISP
Dataminr	MXToolbox
Digital Shadows SearchLight™	NovaSense
DomainTools	Ontic Technologies
DroneSec Notify Threat Intelligence	OpenCTI
EclecticIQ	OpenIOC

Palo Alto Wildfire	Threat Crowd
PhishTank	ThreatBook
Prevalent Third-Party Risk Management Platform	ThreatConnect
Prey	ThreatMark
Proofpoint Domain Discover for Email	ThreatMatch
Proofpoint ET Intelligence	ThreatMiner
Proofpoint Nexus	ThreatQuotient
Recorded Future Express	TruSTAR
Recorded Future Security Intelligence Platform	Trustwave
RedLegg's Threat Intelligence Service	URLhaus
Resecurity	Verint Web Intelligence
ReversingLabs Titanium Platform	VirusTotal
RiskIQ's security intelligence platform	Webroot BrightCloud Threat Intelligence Services
RSA NetWitness Platform	WhoisXML API Enterprise API and Data Feed Packages
Seceon	ZeroFOX Platform
SecLytics	
SecureX	
Securonix Security Operations and Analytics Platform	
Sentinel IPS	
SheldVision	
Shodan	
SIRP	
SIX Threat Intelligence Platform as a Service (TIP)	
Skurio	
SlashNext	
Snare	
SolarWinds MSP Threat Monitor	
SolarWinds Security Event Manager EDITOR's CHOICE	
SoltraEdge	
Sophos Central	
Sophos UTM	
Splunk Enterprise Security	
Spotlight Secure Threat Intelligence Platform	
STIX	
Sumo Logic	
Symante Cyber Security Services: DeepSight Intelligence	
Symantec WebPulse	
TAXII	
T-Eye	
TheHive	

A.4 Platform list combined from scientific search and Google search (N=17)

Blueliv Threat Compass
CIF
CRITs
EclecticIQ Platform
Facebook Threat Exchange
Flashpoint Intelligence Platform
IBM X-Force
IntSights Threat Intelligence Platform
LookingGlass scoutPRIME
LookingGlass scoutTHREAT
Malware Information Sharing Platform (MISP)
MANTIS
OpenCTI
OTX
SoltraEdge
ThreatConnect
ThreatQuotient

References

1. The Global Risks Report 2021. Insight Report
2. Bendovschi, A.: Cyber-Attacks – Trends, Patterns and Security Countermeasures. In: Procedia Economics and Finance 28, 24–31 (2015)
3. Abu, M.S., Selamat, S.R., Ariffin, A., Yusof, R.: Cyber Threat Intelligence – Issue and Challenges. Indonesian Journal of Electrical Engineering and Computer Science, 371–379 (2018)
4. Threat Intelligence Platforms:. Everything You've Ever Wanted to Know But Didn't Know to Ask. Arlingto, VA, USA (2019)
5. Leszczyna, R., Wróbel, M.R.: Threat intelligence platform for the energy sector. Software Practice and Experience 49, 1225–1254 (2019)
6. Anomali: What is a Threat Intelligence Platform (TIP)? Collect, manage, and share threat intelligence, https://www.anomali.com/resources/what-is-a-tip
7. Schlette, D., Böhm, F., Caselli, M., Pernul, G.: Measuring and visualizing cyber threat intelligence quality. In: International Journal of Information Security (2020)
8. Albakri, A., Boiten, E., Lemos, R. de: Risks of Sharing Cyber Incident Information. In: Proceedings of International Conference on Availability, Reliability and Security, 1–10 (2018)
9. Brown, S., Gommers, J., Serrano, O.: From Cyber Security Information Sharing to Threat Management. In: WISCS '15: Proceedings of the 2nd ACM Workshop on Information Sharing and Collaborative Security, 43–49 (2015)
10. Wagner, T.D., Mahbub, K., Palomar, E., Abdallah, A.E.: Cyber threat intelligence sharing: Survey and research directions. In: Computers & Security 87, 1–13 (2019)
11. Chismon, D., Ruks, M.: Threat Intelligence: Collecting, Analysing, Evaluating (2015)
12. Lee, R.M.: 2020 SANS Cyber Threat Intelligence (CTI) Survey. A SANS Survey (2020)
13. Bauer, S., Fischer, D., Sauerwein, C., Latzel, S., Breu, R.: Towards an Evaluation Framework for Threat Intelligence Sharing Platforms. In: Proceedings of the 533rd Hawaii International Conference on System Sciences, 1947–1956 (2020)
14. Vázquez, D.F., Acosta, O.P., Spirito, C., Brown, Sarah, Reid, Emily: Conceptual framework for cyber defense information sharing within trust relationships. 4th International Conference on Cyber Conflict (CYCON 2012), 1–17 (2012)
15. Noor, U., Anwar, Z., Altmann, J., Rashid, Z.: Customer-Oriented Ranking of Cyber Threat Intelligence Service Providers. Electronic Commerce Research and Applications (2020)
16. Mavroeidis, V., Bromander, S.: Cyber Threat Intelligence Model: An Evaluation of Taxonomies, Sharing Standards, and Ontologies within Cyber Threat Intelligence. 2017 European Intelligence and Security Informatics Conference (EISIC), 91–98 (2017)
17. Dandurand, L., Serrano, O.S.: Towards Improved Cyber Security Information Sharing. Requirements for a Cyber Security Data Exchange and Collaboration Infrastructure (CDXI). In: 5th International Conference on Cyber Conflict, 1–16 (2013)
18. Sillaber, C., Sauerwein, C., Mussmann, A., Breu, R.: Data Quality Challenges and Future Research Directions in Threat Intelligence Sharing Practice. In: Proceedings of the 2016 ACM on Workshop on Information Sharing and Collaboration Security, 65–70 (2016)

19. Sauerwein, C., Sillaber, C., Mussmann, A., Breu, R.: Threat Intelligence Sharing Platforms: An Exploratory Study of Software Vendors and Research Perspectives. In: 13th International Conference on Wirtschaftsinformatik, 837–851 (2017)
20. Melo e Silva, A. de, Gondim, J.J.C., Oliveira Albuquerque, R. de, Villalba, L.J.G.: A Methodology to Evaluate Standards and Platforms within Cyber Threat Intelligence. Future Internet, 1–23 (2020)
21. Rantos, K., Spyros, A., Papanikolaou, A., Kritsas, A., Ilioudis, C., Katos, V.: Interoperability Challenges in the Cybersecurity Information Sharing Ecosystem. Computers, 1–17 (2020)
22. Kitchenham, B.: Procedures for Performing Systematic Reviews. Keele, UK, Keele University 33, 1–26 (2004)
23. Garousi, V., Felderer, M., Mäntylä, M.: The need for multivocal literature reviews in software engineering: complementing systematic literature reviews with grey literature. In: Proceedings of the 20th International Conference on Evaluation and Assessment in Software Engineering, 1–6 (2016)
24. Islam, C., Babar, M.A., Nepal, S.: A Multi-Vocal Review of Security Orchestration. ACM Computing Surveys, 1–45 (2019)
25. US Joint Chiefs of Staff: Joint Publication 2-0 Joint Intelligence, https://www.jcs.mil/Portals/36/Documents/Doctrine/pubs/jp2_0.pdf
26. Liew, A.: Understanding Data, Information, Knowledge And Their Inter-Relationships. Journal of Knowledge Management Practice, (2007)
27. Gschwandtner, M., Demetz, L., Gander, M., Maier, R.: Integrating Threat Intelligence to Enhance an Organization's Information Security Management. ARES 2018: Proceedings of the 13th International Conference on Availability, Reliability and SecurityAugust 2018, 1–8 (2018)
28. Amthor, P., Fischer, D., Kühnhauser, W.E., Stelzer, D.: Automated Cyber Threat Sensing and Responding: Integrating Threat Intelligence into Security-Policy-Controlled Systems. ARES '19: Proceedings of the 14th International Conference on Availability, Reliability and Security, 1–10 (2019)
29. McGillan, R.: Definition: Threat Intelligence, https://www.gartner.com/en/documents/2487216
30. Planque, D.: Cyber Threat Intelligence From confusion to clarity; An investigation into Cyber Threat Intelligence (2017)
31. Friedman, J., Bouchard, M.: Definitive Guide to Cyber Threat Intelligence. Using Knowledge about Adversaries to Win the War against Targeted Attacks. Annapolis, MD, USA
32. Tounsi, W., Rais, H.: A survey on technical threat intelligence in the age of sophisticated cyber attacks. In: Computers & Security 72, 212–233 (2018)
33. Sophisticated Indicators for the Modern Threat Landscape: An Introduction to OpenIOC (2011)
34. Zheng, D.E., Lewis, J.A.: Cyber Threat Information Sharing. Recommendations for Congress and the Administration. Washington, DC (2015)
35. Johnson, C., Badger, L., Waltermire, D., Snyder, J., Skorupka, C.: Guide to Cyber Threat Information Sharing. NIST Special Publication 800-150 (2016)

36. White, G.B.: ISAO 300-1: Introduction to Information Sharing. v1.01 (2016)
37. Fransen, F., Smulders, Andre, Kerkdijk, Richard: Cyber security information exchange to gain insight into the effects of cyber threats and incidents. e & i Elektrotechnik und Informationstechnik, 106–112 (2015)
38. Burger, E.W., Goodman, M.D., Kampanakis, P., Zhu, K.A.: Taxonomy Model for Cyber Threat Intelligence Information Exchange Technologies. WISCS '14: Proceedings of the 2014 ACM Workshop on Information Sharing & Collaborative Security, 51–60 (2014)
39. Jordan, B., Piazza, R., Darley, T.: STIX™ Version 2.1 (2021)
40. Introduction to STIX (2021)
41. Luber, S. and Schmitz, P.: Was ist STIX?, https://www.security-insider.de/was-ist-stix-a-830518/
42. Introduction to TAXII (2021)
43. Jordan, B., Varner, D.: TAXII™ Version 2.1. (2020)
44. Cyber Observable eXpression (CybOX™) Archive Website (n.d.)
45. Rashid, Z., Noor, U., Altmann, J.: Network Externalities in Cybersecurity Information Sharing Ecosystems: 15th International Conference, GECON 2018. Economics of Grids, Clouds, Systems, and Services 2019, 116–125
46. The MITRE Corporation: About TAXII (Archive), https://taxiiproject.github.io/about/
47. Exploring the opportunities and limitations of current Threat Intelligence Platforms (2017)
48. Blanco, C., Lasheras, J., Valencia-García, R., Fernández-Medina, E., Toval, A., Piattini, M.: A Systematic Review and Comparison of Security Ontologies. In: The Third International Conference on Availability, Reliability and Security, 813–820 (2008)
49. Serrano, O., Dandurand, L., Brown, S.: On the Design of a Cyber Security Data Sharing System. WISCS '14: Proceedings of the 2014 ACM Workshop on Information Sharing & Collaborative Security, 61–69 (2014)
50. Wagner, T.D., Palomar, E., Mahbub, K., Abdallah, A.E.: Relevance Filtering for Shared Cyber Threat Intelligence (Short Paper). Information Security Practice and Experience: 13th International Conference, 576–586 (2017)
51. Wagner, T.D., Palomar, E., Mahbub, K., Abdallah, A.: Towards an Anonymity Supported Platform for Shared Cyber Threat Intelligence. Risks and Security of Internet and Systems, 175–183 (2018)
52. Keim, Y., Mohapatra, A.K.: Cyber threat intelligence framework using advanced malware forensics. International Journal of Information Technology, 1–10 (2019)
53. Faiella, M., Granadillo, G.G., Medeiros, I., Azevedo, R., Gonalez-Zarzosa, S.: Enriching Threat Intelligence Platforms Capabilities. 16th International Conference on Security and Cryptography (SECRYPT) (2019)
54. Menges, F., Putz, B., Pernul, G.: DEALER: decentralized incentives for threat intelligence reporting and exchange. International Journal of Information Security (2020)
55. Ampatzoglou, A., Ampatzoglou, A., Chatzigeorgiou, A., Avgeriou, P.: The financial aspect of managing technical debt: A systematic literature review. In: Information and Software Technology, 52–73 (2015)

56. Garousi, V., Felderer, M., Mäntylä, M.: Guidelines for including grey literature and conducting multivocal literature reviews in software engineering. In: Information and Software Technology 106, 101–121 (2019)
57. Flashpoint, https://www.flashpoint-intel.com/
58. Hewlett-Packard Development Company, L.P.: Data sheet: HP Threat Central, http://www.hp.com/hpinfo/newsroom/press_kits/2015/RSA2015/ThreatCentralDataSheet.pdf
59. Siemens: The MANTIS Cyber-Intelligence Management Framework, https://django-mantis.readthedocs.io/en/latest/index.html
60. GitHub, Inc.: django-mantis, https://github.com/bgro/django-mantis
61. Kitten, T.: Plug Pulled on Soltra Edge Threat Info Sharing Platform, https://www.bankinfosecurity.com/plug-pulled-on-soltra-edge-threat-info-sharing-platform-a-9547
62. Blueliv, https://www.blueliv.com/
63. Bloomberg L.P.: Leap in Value SL, https://www.bloomberg.com/profile/company/1057513D:SM
64. CSIRT GADGETS, L.L.C., https://csirtgadgets.com/
65. GitHub, Inc.: CSIRT Gadgets, https://github.com/csirtgadgets
66. Liu, R., Zhado, Z., Sun, C., Yang, X., Gong, X., Zhang, J.: A Research and Analysis Method of Open Source Threat Intelligence Data. Data Science. ICPCSEE 2017. Communications in Computer and Information Science, 352–363 (2017)
67. Poputa-Clean, P.: Automated Defense - Using Threat Intelligence to Augment (2015)
68. Cheek, K., Coons, M.: Threat Intel and IR Tools for Dummies: Real-Life Use Cases (2019)
69. Chadwick, D.W., Fan, W., Constantino, G., Lemos, R. de, Di Cerbo, F., Herwono, I., Manea, M., Mori, P., Sajjad, A., Wang, X.-S.: A cloud-edge based data security architecture for sharing and analysing cyber threat information. Future Generation Computer Systems, 710–722 (2020)
70. Nakagawa, I.: SecBI: Cyber Threat Intelligence (2017)
71. The MITRE Corporation: CRITs. Collaborative Research Into Threats, https://crits.github.io/
72. GitHub, Inc.: CRITs. Collaborative Research Into Threats, https://github.com/crits
73. St. John, M.: Samples and Analysis with CRITs, https://cyberdefenses.com/crits-samples-analysis/
74. The MITRE Corporation, https://www.mitre.org/
75. Mtsweni, J.S., Shozi, N.A., Matenche, K., Mutemwa, M., van Jansen Vuuren, J.: Development of a semantic-enabled cybersecurity threat intelligence sharing model. 11th International Conference on Cyber Warfare & Security (2016)
76. EclecticIQ B.V., https://www.eclecticiq.com/
77. Wagner, T.D., Palomar, E., Mahbub, Khaled, Abdallah, Ali E.: A Novel Trust Taxonomy for Shared Cyber Threat Intelligence. Security and Communication Networks, 1–11 (2018)
78. Owler, Inc.: EclecticIQ, https://www.owler.com/company/eclecticiq
79. Jansen, C.: EclecticIQ raises €5.5M to develop cyber-threat intelligence for enterprises, https://techseen.com/eclecticiq-raises-e5-5m-to-develop-cyber-threat-intelligence-for-enterprises/
80. Facebook, Inc.: ThreatExchange Documentation, https://developers.facebook.com/docs/threat-exchange

81. Jigsaw Security Enterprise Inc.: Facebook Issues? - Why we don't use Facebook ThreatExchange, https://www.jigsawsecurityenterprise.com/post/2018/03/21/facebook-issues-why-we-dont-use-facebook-threatexchange
82. IBM Security: IBM X-Force Exchange, https://exchange.xforce.ibmcloud.com/
83. IBM: IBM X-Force Exchange, https://www.ibm.com/products/xforce-exchange
84. Franklin, D.: A Gentle Introduction to the X-Force Exchange API, https://securityintelligence.com/a-gentle-introduction-to-the-x-force-exchange-api/
85. SC Media: IBM Security IBM X-Force Exchange, https://www.scmagazine.com/review/ibm-security-ibm-x-force-exchange/
86. Raguseo, D.: Introducing IBM X-Force Exchange. A new way for the world to leverage collaborative threat intelligence, http://www.energiamedia.it/wp-content/uploads/2015/09/XFE-Client-Presentation-v2.pdf
87. Robb, D.: IBM X-Force Exchange Threat Intelligence Platform, https://www.esecurityplanet.com/products/ibm-xforce/
88. IntSights, https://intsights.com/
89. Hreben, M. and Diehl, M.: IntSights Cyber Intelligence Threat Intelligence Platform, https://www.scmagazine.com/review/intsights-cyber-intelligence-threat-intelligence-platform/
90. Owler, Inc., https://www.owler.com/company/intsights
91. LookingGlass Cyber Solutions, Inc., https://www.lookingglasscyber.com/
92. LookingGlass Cyber Solutions, Inc.: scoutPRIME, https://www.lookingglasscyber.com/products/threat-platforms/scoutprime/
93. Kissel, C.: Cybersecurity Beyond the Network Reach (2018)
94. Threat Intelligence Platform. From Limitless Information to Actionable Cyber Threat Intelligence (2016)
95. SC Media: LookingGlass scoutPRIME 2019.2.J.46, https://www.scmagazine.com/review/lookingglass-scoutprime-2019-2-j-46/
96. LookingGlass Cyber Solutions, Inc.: scoutTHREAT, https://www.lookingglasscyber.com/products/threat-platforms/scoutthreat/
97. The Power of a Tailored Threat Model
98. Weil, T.: LookingGlass scoutPRIME 2019.2.J.46, https://www.scmagazine.com/review/lookingglass-scoutprime-2019-2-j-46/
99. MISP project, https://www.misp-project.org/
100. CIRCL Computer Incident Response Center Luxembourg: MISP - Open Source Threat Intelligence Platform, https://www.circl.lu/services/misp-malware-information-sharing-platform/
101. Riesco, R., Larriva-Novo, X., Villagra, V.: Cybersecurity threat intelligence knowledge exchange based on blockchain. Telecommunication Systems, 259–288 (2020)
102. Mokaddem, S., Wagener, G., Dulaunoy, A., Iklody, A.: Taxonomy driven indicator scoring in MISP threat intelligence platforms. ArXiv (2019)
103. Luatix: OpenCTI, https://www.opencti.io/en/
104. Notion Labs, Inc.: OpenCTI Public Knowledge Base, https://www.notion.so/OpenCTI-Public-Knowledge-Base-d411e5e477734c59887dad3649f20518

105. ANSSI, https://www.ssi.gouv.fr/en/
106. GitHub, Inc.: OpenCTI-Platform / opencti, https://github.com/OpenCTI-Platform/opencti
107. Hassine, S.: Your Cyber Threat Intelligence Knowledge in a Magic Box, https://medium.com/luatix/your-cyber-threat-intelligence-knowledge-in-a-magic-box-af2cbf7dd4be
108. Luatix, https://www.luatix.org/en/
109. Richard, J.: OpenCTI and SSO (Single Sign On), https://medium.com/luatix/opencti-and-sso-single-sign-on-1c9aaf1d4d87
110. AT&T Cybersecurity, https://cybersecurity.att.com/
111. Owler, Inc., https://www.owler.com/company/alienvault
112. ThreatConnect, Inc., https://threatconnect.com/
113. Wilson, M.: Threat Intelligence Platforms – Here the Best TIPS for Managing Security in Your Networks!, https://www.pcwdld.com/threat-intelligence-platforms-tips
114. ThreatConnect, Inc.: ThreatConnect Developer Documentation, https://docs.threatconnect.com/en/latest/index.html#
115. Craft.co: ThreatConnect, https://craft.co/threatconnect
116. ThreatQuotient, Inc., https://www.threatq.com/
117. Cybersecurity Excellence Awards: ThreatQ Threat Intelligence Platform, https://cybersecurity-excellence-awards.com/candidates/threatq-threat-intelligence-platform-3/
118. Mutemwa, M., Mtsweni, J.S., Mkhonto, N.: Developing a cyber threat intelligence sharing platform for South African organisations. 2017 Conference on Information Communication Technology and Society (ICTAS), 1–6 (2017)
119. Craft.co: ThreatQuotient, https://craft.co/threatquotient
120. OpenChannel: Leading Security Operations and Threat Intelligent Platform Provider, ThreatQuotient, Leverages OpenChannel for ThreatQ Marketplace, https://openchannel.io/blog/threatquotient-platform-marketplace/
121. Wu, Y., Qiao, Y., Ye, Y., Lee, B.: Towards Improved Trust in Threat Intelligence Sharing using Blockchain and Trusted Computing. 2019 Sixth International Conference on Internet of Things: Systems, Management and Security (IOTSMS), 474–481 (2019)

Plagiarism Disclaimer

I hereby declare that this diploma thesis is my own and autonomous work. All sources and aids used have been indicated as such. All texts either quoted directly or paraphrased have been indicated by in-text citations. Full bibliographic details are given in the list of works cited, which also contains internet sources including URL and access date. This work has not been submitted to any other examination authority.

01.11.2021,

Date, Signature