CYBERSANE

D6.1

Intelligence and Information Sharing Models Specifications

Project number:	833683
Project acronym:	CyberSANE
Project title:	Cyber Security Incident Handling, Warning and Response System for the European Critical Infrastructures
Start date of the project:	1st September, 2019
Duration:	36 months
Programme:	H2020-SU-ICT-2018

Deliverable type:	Report
Deliverable reference number:	DS-01-833683 / D<6.1>/ | N.1
Work package contributing to the deliverable:	WP 6
Due date:	02 2021 – M18
Actual submission date:	05/April/2021

Responsible organisation:	CNR
Editor:	Oleksii Osliak
Dissemination level:	PU
Revision:	| N.1

Abstract:	Report on the Intelligence and Information Sharing models in terms of stakeholders, models, collaborative workflows and interactions. This deliverable will be a report reflecting the outcomes of T6.1 and T6.2.
Keywords:	Cyber Threat Intelligence, Information Sharing, Trust Management
	The project CyberSANE has received funding from the European Union’s Horizon 2020 research and innovation programme under grant agreement No 833683.

Editor

Oleksii Osliak (CNR)

Contributors (ordered according to beneficiary numbers)

Luis Landeiro Ribeiro, Luis Miguel Campos (PDMFC)

Ruiz Jose Francisco (ATOS)

Fabio Martinelli, Oleksii Osliak(CNR)

Mitton Nathalie, Staddon Edward (INRIA)

Tzagkarakis Christos, Barmpaki Anthi (FORTH)

Kontakis Konstantinos, Spanoudakis Georgios (STS)

Karypidis Paris-Alexandros (SID)

Mouratidis Haris, Ismail Umar (UoB)

Reviewers

Kontakis Konstantinos (STS)

Papadogiannaki Eva, Athanatos Manos (FORTH)

Karypidis Paris-Alexandros (SID)

Disclaimer

The information in this document is provided “as is”, and no guarantee or warranty is given that the information is fit for any particular purpose. The content of this document reflects only the author`s view – the European Commission is not responsible for any use that may be made of the information it contains. The users use the information at their sole risk and liability.

Executive Summary

Due to the sensitivity of information produced, collected, and shared within Critical Infrastructures (CIs) and Critical Information Infrastructures (CIIs), enabling secure information sharing considering multiple aspects is a crucial task. In particular, data owners should be able to define the distribution level for sharing their information since it may discover sensitive data both of CIs and CIIs. This document provides results obtained after an in-depth assessment of the existing threat intelligence and trust management approaches and technologies highlighting current gaps and barriers. After series of discussions, the research areas were selected to incorporate approaches we have in the technical WP6 to formulate the proposed CyberSANE Intelligence and Information Sharing models. The document defines a set of Information Sharing models, functions and structures to facilitate the collaboration and dissemination of useful cyber incident information. The proposed models will provide reliability, robustness, and efficiency for automated and secure information sharing. The capabilities of tools owned by the consortium may be enhanced through the development of additional features discussed in this document.

Contents

List of Figures

List of Tables

Chapter 1 Introduction

This deliverable presents the findings and outcomes performed in Task 6.1 and Task 6.2. We have described the state-of-the-art of those threat intelligence and trust management approaches that could be possibly utilized for the development of the sharing and trust techniques used within CyberSANE's ShareNet component. There are plenty of technical areas covered in order to choose the most appropriate techniques fitting into today's Critical Infrastructures (CIs) and Critical Information Infrastructures (CIIs), and wherever it is deemed necessary, to proceed with the appropriate development or modification of consortium's tools. The rest of this document is structured as follows:

- Chapter 2 documents the cyber threat intelligence domain, its generic specifications, as well as the issues and challenges that should be addressed.
- Chapter 3 describes the prominent standards, languages, and platforms regarding vulnerability databases, scoring systems, and threat sharing solutions.
- Chapter 4 includes the most widely known and latest works on trust management approaches across various technological backgrounds including ontological frameworks, access control models, and reputation-based techniques.
- Chapter 5 describes initial results towards innovative secure CTI sharing.
- Chapter 6 features the concluding remarks of this deliverable.
- Chapter 7 includes a glossary of the most commonly used abbreviations.
- Chapter 8 concludes with all the bibliography of this deliverable.

Chapter 2 Cyber Threat Intelligence

Cyber Threat Intelligence (CTI) is a fast-developing field of the cyber-security domain which analyses previously identified and potentially emerged security vulnerabilities in a systematic way. Typical types of threat information examined include but are not limited to indicators, Tactics, Techniques, and Procedures (TTPs), security advisories, threat intelligence reports, and internal or external trusted data sources. Over the last few years, several organizations adopted a CTI initiative or developed their own CTI models to efficiently collect, assess, and share threat intelligence information (Dalziel, 2014). By doing so, their IT teams were able to set-up a barrier of proactive and preventing measures for the security enhancement of their organizations' assets. The research community has given birth to various generic-usage CTI approaches that deploy well-known frameworks like the NIST's Cybersecurity and OASIS's STIX (Arenas, 2017; Settanni, et al., 2017), while an additional set of promising threat intelligence schemes for safeguarding industry 4.0 systems (Moustafa, et al., 2018) and CIs (Lee & Shon, 2017) have been already presented in the near past. Within the context of the CyberSANE project, CTI aims at providing an evidence-based knowledge of a threat that is going to be leveraged for sharing and decision-making purposes regarding that threat.

2.1 Threat Intelligence Levels

CTI is typically composed of three distinct levels that each one aims at collecting and representing a different type of information. Ultimately, the correlation of the knowledge and the facts contained in all three level make feasible the faster detection and more accurate response against the involved threat data. These levels represent a generic split of intelligence produced by (UK Ministry of Defense, 2011) which was classified into the Strategic, Operational, and Tactical levels. Each of these levels is being described below in the context of CTI, followed also by Table 1 that illustrates the main differences between them, as well as the typical IT roles and tasks corresponding to each level according to (Friedman & Bouchard, 2015).

Strategic Level: It presents an overview of the current threat landscape and provides insights regarding the business issues that could possibly occur. Since the audience of the Strategic Threat Intelligence are high-level strategists and senior business leaders, the reports rarely include technical terms related to the cyber-security domain. Such reports instead focus on the underlying business terminology to address identified or potential financial, regulatory, and operational risks. Moreover, the dissemination of these reports usually takes place on a monthly or quarterly basis depending on the organization type and its employed decision-makers, in order to give them enough time to formulate an efficient long-term IT security strategy.

Operational Level: It acts as the medium of delivering critical information about an anticipated, impending attack which requires immediate attention. Consequently, the responsible personnel for handling Operational Threat Intelligence feeds are mostly found to be the Incident Response Teams and Threat Analysts. The CTI data are formatted either as human-readable, or machine-readable information, depending on the cyber-security tool and the data source(s) used. It is evident that the more sources, the better the results. However, regardless of the tools, sources, and the methodologies deployed, the main purpose of every peer involved is to provide, extract and correlate as much threat knowledge as possible. By doing so, he/she will be able to identify the potential motivations of a threat-actor, his/her technical skills, as well as the planned attack campaigns.

Tactical Level: It consists of information related to the threat-actors and the tactics, techniques, and procedures (TTPs) that they use to compromise the security of a system. This type of threat data usually originates from open source communities, whitepapers, technical papers, and collaboration with external organizations which share the same application area or geographical location. The Tactical Threat Intelligence is extremely useful for IT infrastructure operations' personnel, since they are the ones who have to investigate for security holes, and update or apply the necessary changes to specific software and hardware components. They are based on a supplied set of Indicators of Compromise (IOCs) to defend against previously identified attacks and to deploy additional proactive measures. Last but not least, it is worth mentioning that this kind of threat data feeds are sometimes taken into account from the Operational Level as well, since their content is highly actionable, and it is offered in a human-readable format.

	Strategic Level	Operational Level	Tactical Level
IT Roles	Chief Information Security Officer (CISO) Chief Information Officer (CIO) Risk Officer	Incident Response (IR) Team Threat Analysts Security Forensics Fraud Detection	Infrastructure Operations (Architects, DevOps, Sysadmins) Network Operations Centre (NOC) Security Operations Centre (SOC)
Assigned Tasks	Allocation of financial, human, and physical resources Communication with executive management	Examine an attack's details and designate actions Proceed to remediation if deemed necessary Conduct threat hunting	Feed security tools with indicators Patch security vulnerabilities Monitor for potential security alerts and escalate them
Known Problems	Unable to efficiently address investment priorities Executives are unaware of technical terminology	Reconstruction of attacks based on indicators is tedious Difficult to determine the damage and any additional security breaches	Unverified indicators generate false positives Patching management and prioritization is difficult Not feasible the timely investigation of such many alerts
CTI Value	Formulation of priorities based on business risks and the likelihood of an attack Application of business terms to identify threat-actors and cyber-threats	Provision of information which allows the faster reconstruction of an attack Provision of information which addresses the expected damage and breaches	Validation and prioritization of security indicators Prioritization of security patches Prioritization of security alerts

Table 1: IT roles, tasks and problems addressed across CTI levels

Besides the aforementioned three levels of CTI, the Centre for the Protection of National Infrastructure (CPNI) presented the four-tiered model of threat intelligence shown in Figure 1. According to their proposal (Chismon & Ruks, 2015), the fourth subtype is coined as Technical, and includes low-level and short-term operations conducted by an organization's Security Operations Centre (SOC) or Incident Response (IR) teams. The corresponding personnel takes advantage of technical means to detect and prevent any potentially malicious actions in a timely manner, by deploying a set of indicators optimized for specific types of cyber-threats like the malwares. However, their model does not greatly differentiates compared to the typical three-tiered model of CTI found on most studies and literature. The IT roles, tasks, problems and CTI value referenced in the Technical level of CPNI's model, are instead integrated into the Tactical level of the three-tiered model, where a couple of actions are also undertaken from the Operational level of the same model.

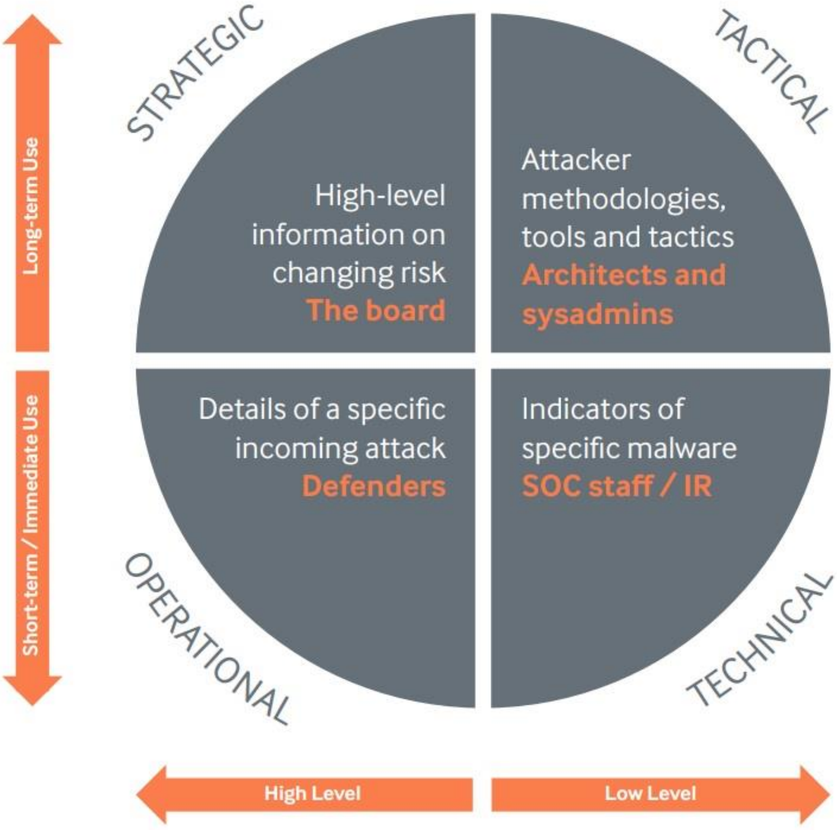

STRATEGIC
TACTICAL
OPERATIONAL
TECHNICAL
High-level information on changing risk
The board
Attacker methodologies, tools and tactics
Architects and sysadmins
Details of a specific incoming attack
Defenders
Indicators of specific malware
SOC staff / IR
Long-term Use
Short-term / Immediate Use
High Level
Low Level

Figure 1: CPNI's subtypes of threat intelligence[1]

2.2 Issues & Challenges

The sufficient and efficient deployment of a CTI sharing platform firstly involves the identification of the issues and the challenges met in its domain. So, this subsection aims to address those obstacles that have to be overcome, as well as the requirements that have to be satisfied, independent of the underlying organization and the infrastructure used. Our study keeps up and reinforces the results derived from (Abu, et al., 2018; Win & Thaw, 2019), since the same four cases described below also apply in the context of CyberSANE.

Threat Data Overload: CTI's ability to enable an alternative automated threat intelligence mechanism to defend against cyber-attacks led to its unprecedented adoption from both the research and the commercial communities. However, the question that quickly raised is whether this overwhelming amount of information is actually actionable from an interested third-party individual (Shouse, 2015). The threat data overload issue is further amplified due to the lack of

[1] http://www.icsdefender.ir/files/scadadefender-ir/paygahdanesh/gheyreboomi/BehtarinRaveshha/CPNI%20-%20Threat%20Intelligence%20-%20Collecting%20Analysing%20Evaluating.pdf

security experts in most organizations, unfortunately including several CIs and CIIs. (Ponemon Institute, 2015) have previously reported that the combination of data size and data complexity usually requires a qualified threat analyst to efficiently analyze and provide feedback in a timely manner. All the aforementioned issues and challenges are quite hard to be resolved, since more and more open and closed source data feeds are becoming available. However, a potential solution could be the introduction of more human-friendly data feeds, like the model proposed in (Afzaliseresht, et al., 2020) which applies novel storytelling techniques based on the security logs of a system. Similar methodologies could also be adopted or developed from scratch to deal with the threat data overload and complexity issues.

Threat Data Quality: One of the most important aspects of any CTI initiative is definitely the threat data quality being interchanged. Even though this type of challenge was initially found to bear no fundamentally new data quality issues (Sillaber, et al., 2016), the quick adoption of CTI domain gave birth to a series of security tools that should efficiently face scalability and data source integration issues. Such solutions have to be designed taken into consideration the software and hardware security components met in many industries, in order to enable the collection of network data and use them in decision-making as well. According to a threat intelligence study which evaluated the threat feeds' value of several cyber-security tools (Ponemon Institute, 2019), almost 70% of the CTI feeds were found to be inadequate and inefficient in terms of quality. A similar study tried to evaluate various open-source CTI feeds over an extended period of months, focusing into the timely provision of relevant and complete data (Griffioen, et al., 2020). The results of this study showed that most of indicators are active for many days before their listing takes place, while several threat data feeds are biased towards specific countries and IP addresses. Since such actions could lead to an excessive amount of collateral damage, an initiative lead by the Cyber Threat Alliance (CTA) proposed an automated data quality scoring algorithm and the extraction of information only if the necessary quality criteria are satisfied[2].

Interoperability Challenges: The cyber-defence collaboration and the establishment of a trusted CTI environment where organizations are able to share threat data come with a set of interoperability challenges which must be tackled. At first, (Vázquez, et al., 2012) explored four different aspects of CTI in order to propose a conceptual framework for the development of interoperable sharing models, which had its vocabulary and taxonomy based on NATO's CIS Security Capability Breakdown (Hallingstad & Dandurand, 2011). Their study focused into the incentives and barriers that could be used for threat data sharing, the collaborative risk management and information value perception, the available procedural models which could enhance information sharing, and finally, the potential automation of sharing mechanisms in cyber-security domain. The latter introduction of standardized languages and protocols like the Cyber Observable eXpression (CybOX)[3], Structured Threat Information eXpression (STIX)[4], and Trusted Automated eXchange of Indicator Information (TAXII)[5], gave the capability to individuals and organizations to solve the interoperability issues. However, according to (Gong, 2019) even today there are still barriers that prevent the adoption of such interoperability standards due to specific constraints. In these cases, data transformation solutions offered by community-driven specification languages (Casey, et al., 2017) could promote an alternative methodology to deal with the interoperability challenges in CTI.

Privacy and Legal Issues: Last but not least, there are also a set of rules that should be followed before, during, and after the exchange of threat intelligence information. Such rules make sure that no sensitive or confidential information is disclosed according to the privacy and legal laws

[2] https://www.cyberthreatalliance.org/how-our-sharing-works/
[3] https://cyboxproject.github.io
[4] https://oasis-open.github.io/cti-documentation/stix/intro.html
[5] https://taxiiproject.github.io

that govern the underlying industry or organization. (Fisk, et al., 2015) investigated the risks regarding the exposure of private data and defined a set of privacy principles as a sharing guide between the collaborated organizations. The privacy implications stemming from the Business-to-Business (B2B) sharing of CTI information also concerned (Sullivan & Burger, 2017), where the authors of this paper examined the sharing of IP addresses under the recent General Data Protection Regulation (GDPR) which applies across all European Union's countries. An extensive recent review of the legal issues that occur in the context of CIs has been presented in (Nweke & Wolthusen, 2020), providing additional guidance and incentives for the participation of private entities in CTI sharing.

Chapter 3 CTI Databases, Scoring & Sharing

Over the last decade, the emerge and rapid spread of new cyber-threats denoted the necessity of developing CTI solutions which could efficiently deal with such threats in a timely manner. This increasingly subject of interest aims at providing a set of languages, tools, and platforms to gather, score, and share any kind of information related with cyber-security threats or incidents. Today, several taxonomies and standards have been developed for the needs of CTI domain, where each one of them comes with its own advantages and drawbacks (Mavroeidis & Bromander, 2017). Therefore, in this chapter we describe the most widely used publicly available vulnerability databases, the scoring systems deployed for their sake, as well as the sharing standards adopted by several organizations, industries, and communities.

3.1 Vulnerability Databases

A vulnerability database can be seen as a platform which aggregates, maintains and disseminates publicly identified vulnerabilities. On such databases each vulnerability is comprehensively documented following a standardized format, which includes all the necessary information regarding the nature of the threat, its potential impact on the underlying system, as well as any known security patches or fixes. Typical security vulnerabilities listed on such databases include but are not limited to initial deployment failures, SQL injection attacks, and misconfigurations on software or hardware components. All vulnerability databases provide access to individuals and organizations through a multitude of Web Services, sharing in this way their security insights and allowing any interested party to rectify security holes and prevent a potential compromise of their system. It is worth noticing that variations of the vulnerability databases presented in the following subsections of this chapter can be also found on the commercial sector. Risk Based Security's VulnDB[6], Symantec DeepSight Intelligence[7], Snyk's Intel Vulnerability Database Access[8], Flexera's Software Vulnerability Management[9], and iDefense Vulnerability Intelligent Service[10] are some of the most prominent products regarding the intelligent management of security vulnerabilities, which however are paid solutions and their source code is of course kept private.

3.1.1 National Vulnerability Database

The National Vulnerability Database (NVD) is a product of the National Institute of Standards and Technology (NIST) that aims at providing a continuously updated repository of the existing and the latest emerged vulnerabilities (Booth, et al., 2013). All vulnerabilities are represented under a multipurpose protocol known as SCAP (Security Content Automation Protocol), which grants automated means for the vulnerability management, security measurement, and compliance. NVD incorporates various types of vulnerabilities ranging from software-related security flaws, to a potential and unintentional product misconfiguration that could lead to the compromise of a system. Each detected vulnerability is also attributed with a set of impact metrics to denote the importance and severity of the underlying threat. The required data interoperability is achieved

[6] https://vulndb.cyberriskanalytics.com/
[7] https://docs.broadcom.com/doc/cyber-security-services-deepsight-intelligence-en
[8] https://snyk.io/product/vulnerability-database/
[9] https://www.flexera.com/products/operations/software-vulnerability-management.html
[10] https://www.accenture.com/_acnmedia/PDF-57/Accenture-IDefense-Vulnerability-Intelligence.pdf

using the Security Content Automation Protocol (SCAP) protocol (Waltermire, et al., 2016), which is responsible for the collection and assessment of a device's state by conducting all the necessary security checks and verification procedures. Both NVD and SCAP specifications are also taken into consideration from a specific set of complementary models issued or backed by NIST, in to provide scoring and enumeration capabilities to the identified vulnerabilities.

3.1.2 Common Vulnerabilities and Exposures

Common Vulnerabilities and Exposures (CVE) is a list of publicly known vulnerabilities, where each one is identified by a unique identification number, followed by a standardized description and one or more URL references (The MITRE Corporation, 2020). The list currently counts hundreds of thousands of vulnerabilities and its accessibility is open to anyone desiring to search, use, and develop a custom-made tool based on the reference methodologies of the platform. Each identified vulnerability is registered as a distinct CVE entry correlated to a specific type of attack, with Figure 2 depicting the total number of those vulnerabilities by attack-type since 1999, without including however the current year (2020).

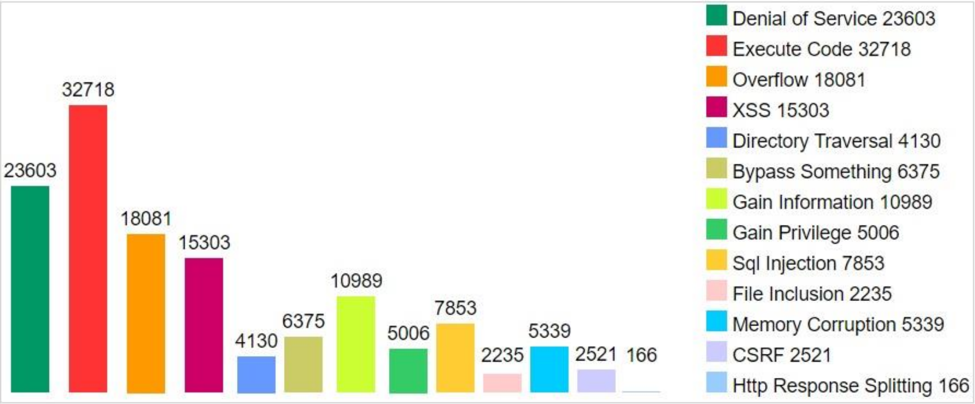


Figure 2: Number of identified CVEs by attack-type since 1999[11]

CVE identifiers act as the medium to make trivial the sharing of data across different types of security networks and infrastructures, enabling thus the immediate and accurate patch of a potential vulnerability in their codebase. (Cardoso & Freire, 2005) addressed the security vulnerabilities and exposures in systems and services interacting over the Internet before, so the introduction of CVE's dictionary was able to successfully fill this gap. Nowadays, it has found actual practicability in several industries for both sharing and assessment purposes, allowing them to enhance their native cyber-security mechanisms. However, it is worth noticing that latest studies showed that security enumerations like the CVE do not suffice towards specific application areas (Schlette, et al., 2020) and alternative models have been proposed to surpass the conciseness and usability deficiencies met in them (e.g. cyber-physical systems).

[11] https://www.cvedetails.com/vulnerabilities-by-types.php

3.1.3 VulDB

VulDB is a community-driven vulnerability database which documents security vulnerabilities, cyber-threats, as well as software and hardware exploits over the last 40 years (VulDB, 1997). Beyond the provision of technical details regarding the aforementioned vulnerabilities, VulDB also offers additional CTI information such as risk assignments, exploitability levels, remediation measures, etc. Moreover, VulDB claims that makes use of advanced artificial intelligence techniques to gather and analyze potential malicious activities across globe in real-time. All existing and newly identified vulnerabilities are attributed with their VulDB's CTI interest, activity, and geopolitical analysis scores. Since 2017, there is a free community edition which however allows a limited only number of Application Programming Interface (API) calls and comes with several restrictions in entries' searching and retrieval capabilities, compared to its commercial and enterprise paid solutions.

3.1.4 WhiteSource Vulnerability Database

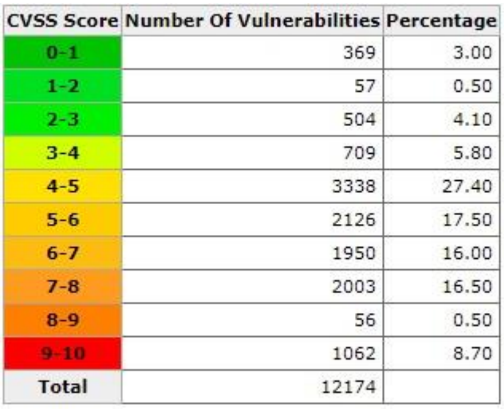
WhiteSource Vulnerability Database claims to be the largest open-source vulnerability database, due to the fact that it aggregates security vulnerabilities from hundreds of sources including those of NVD, security advisories, and open source issue trackers (WhiteSource Software, 2019). Each documented vulnerability is searchable through their API, while at the same time, they also provide an extensive monthly-based listing of all identified CVEs since 2002. Even though that WhiteSource's features are quite similar to the rest of vulnerability databases, they manage to differentiate by providing a vulnerability scanner for GitHub's private and public repositories which supports over 200 programming languages, as well as an Azure DevOps extension for the identification and scanning of a project's open-source components.

3.2 Scoring Systems

Over the last decade, CTI scoring initiatives have significantly evolved, giving birth to several systems with advanced methodologies for scoring vulnerabilities based on a specified set of criteria and procedures. In the past, each organization or IT security team had to define its own criteria based on the industry standards and the corresponding involved application. However, it quickly became evident that this type of scoring was a time-consuming, human resourceful, and sometimes inefficient task which also had to be updated on a regular basis. Such obstacles were topped with the introduction of the publicly available scoring systems presented in the following subsections of this chapter.

3.2.1 Common Vulnerability Scoring System

The Common Vulnerability Scoring System (CVSS) is an open-source framework of metrics proposed by NIST which are deployed for communicating the characteristics, severity, and impacts of cyber-security-related vulnerabilities (Mell, et al., 2006). The three primary group of metrics supported by CVSS include the Base metrics which are used to determine the severity factor, the Temporal metrics which are used for mitigation purposes, and the Environmental metrics which are used to characterize the expansion and correlation of the vulnerability in regards to the underlying system (Radack, 2007). The severity of an identified vulnerability in CVSS is reflected by a numerical score, which is based on a baseline analysis of the data provided by third-party researchers and organizations. This numerical representation is afterwards taken into consideration from security experts to properly access a cyber-threat, plan their actions against it, and if possible, mitigate its impact as well. The second version of CVSS (CVSS v2.0) has been proved to be the prevailing technique for the quantification of a vulnerability's severity in various application areas compared to the rest of the publicly available scoring systems. The latest version of CVSS (CVSS v3.1) was released about a year ago (FIRST, 2019), introducing major changes in the Base group of metrics along with a new scoring scale methodology, where the latter has been also reported to be the root cause of an increased average base score since v3.0 (Santos, 2016). In Figure 3 below can be seen the distribution of all identified vulnerabilities by CVSS scores, setting as searching period the start of January 2019 until end of May 2020.



CVSS Score	Number Of Vulnerabilities	Percentage
0-1	369	3.00
1-2	57	0.50
2-3	504	4.10
3-4	709	5.80
4-5	3338	27.40
5-6	2126	17.50
6-7	1950	16.00
7-8	2003	16.50
8-9	56	0.50
9-10	1062	8.70
Total	12174	

Figure 3: Vulnerabilities Distribution by CVSS scores between January 2019 and May 2020[12]

3.2.2 Common Weakness Scoring System

The Common Weakness Scoring System (CWSS) is a collaborative community-based scoring system maintained by MITRE (Martin & Christey, 2014), which aims at defining a standardized mechanism for the prioritization of software weaknesses depending on the underlying organization, institution, or individual being involved. CWSS can act as a complementary tool to the CVSS by offering a distinct framework for the identification, assessment, and prioritization of the discovered software weaknesses, which is backed by a set of qualitative measurements for the unfixed software weaknesses, and the capability of customized prioritization according to industry needs. CWSS is composed of three different metric groups where each one includes additional metrics termed factors for the efficient scoring computation of an identified weakness. The organization of these metric groups and their containment factors is illustrated in Figure 4.

[12] https://www.cvedetails.com/cvss-score-charts.php?fromform=1&vendor_id=&product_id=&startdate=2019-01-01&enddate=2020-05-29

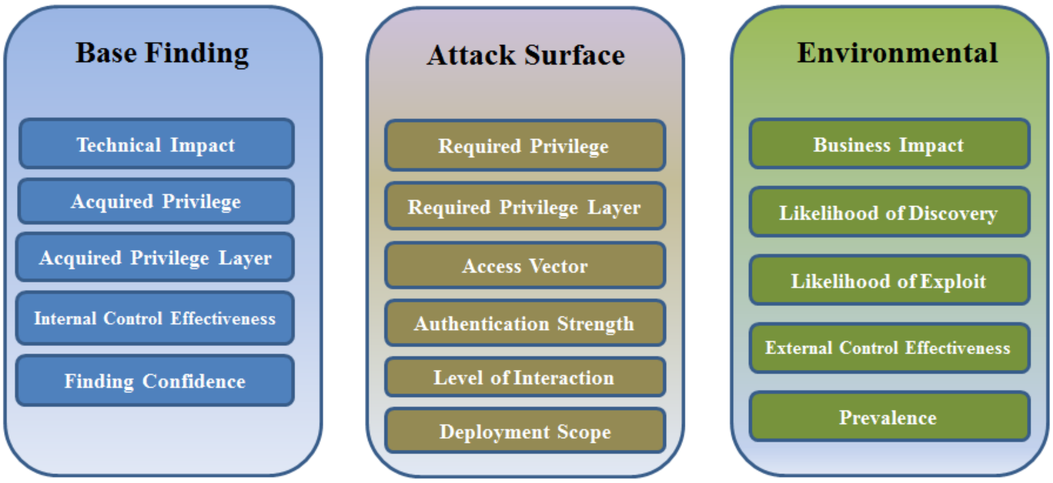


Figure 4: CWSS Metrics[13]

The first one is known as Base and aims at capturing the risk of the weakness, the second is named Attack Surface and tries to discover the security obstacles that have to be overcome by the malicious threat-actor, while the third metric group is the Environmental which intends to correlate a software weakness with a set of characteristics based on specific application or operational areas. Moreover, the variety of the depicted CWSS factors along with the automated calculation of score formulas, enable the generation of flexible CWSS vectors for business-critical applications met in today's CIs.

3.3 Sharing Standards & Platforms

The sharing of CTI information between organizations enhances their knowledge, experience, and prevention capabilities against previously identified cyber-threats. The security posture of any organization which participates in such a collaboration scheme moves to the next level, since their Computer Security Incident Response Teams (CSIRTs) are able to plan and develop the necessary countermeasures for the timely detection of the latest kind of attacks. Besides the advanced security posture discussed above, the shared situational awareness within a community of interest, the knowledge maturation coming from the correlation of initially unrelated data, and the improved defensive agility, are some of the most remarkable benefits that could attributed to an information sharing process (Johnson, et al., 2016). Taking into consideration that finding the appropriate CTI sharing platform has already concerned the research community before (Chantzios, et al., 2019), in this subchapter we aim to describe those initiatives and industry standards which have been developed for the sufficient and efficient sharing of threat-related information.

3.3.1 STIX & TAXII

STIX (Structured Threat Information eXpression) is a standardized language developed by MITRE[14] and OASIS[15] for modelling and representing CTI information in a consistent manner to

[13] https://cwe.mitre.org/cwss/images/CWSS-groups-10.png
[14] https://www.mitre.org/
[15] https://www.oasis-open.org/

facilitate the automation and analysis tasks (Barnum, 2014). Its architecture makes use of Extensible Markup Language (XML) definitions of standardized languages to describe a diverse set of CTI components which range from cyber observables, indicators and incidents, to TTPs (including attack-patterns, malware, kill chains, etc.), cyber-attack campaigns and cyber-threats actors. Doing so, STIX enables the sharing of more than 90 types of objects, instances of security events, and patterns of events represented by the CybOX language. At the same time, individuals or organizations who take advantage of STIX are given with the capability to choose which information they wish to share, and which information they wish to keep confidential. Last but not least, even though that STIX has been developed to be shared through the TAXII protocol, it still supports other kinds of sharing formats which however lack in the interoperability and standardization features met in TAXII.

Trusted Automated eXchange of Intelligence Information (TAXII) is a protocol which standardizes the sharing of CTI information related with software and hardware components, by supplying a set of HTTP services and message exchanges that match the needs of today's industries (Connolly, et al., 2014). TAXII has been designed to principally serve as the transportation mean of STIX language, providing thus several flexible sharing models which are in principal scheme variants of sharing information between a single source and a number of subscribers, between a single repository known as hub and a number of different but closely related entities known as spokes, or between peers of a same group. Each sharing model is also backed by four distinct but optional services, where each one of them can be combined based on a user's needs to ultimately form a different type of sharing model where:

i. "Discovery" aims at discovering the supported services for future interaction
ii. "Collection Management" aims at discovering and subscribing to a data collection
iii. "Inbox" aims at receiving information similar to a push message
iv. "Pol" aims at requesting information similar to a pull message

Besides its aforementioned sharing flexibility, TAXII also incorporates a secure communication mechanism and poses a minimal set of requirements that should be met, making its adoption independent of the underlying network protocol and message format used from an individual or within an organization. For all these reasons, STIX and TAXII nowadays have been acknowledged as the industry standards in exchanging CTI across several areas including commercial and non-profit organizations, while improvements to their sharing schemes have been already proposed for specific environments (Wang, et al., 2019). A typical architecture scheme that takes advantage of both STIX language and TAXII protocol can be seen in Figure 5.

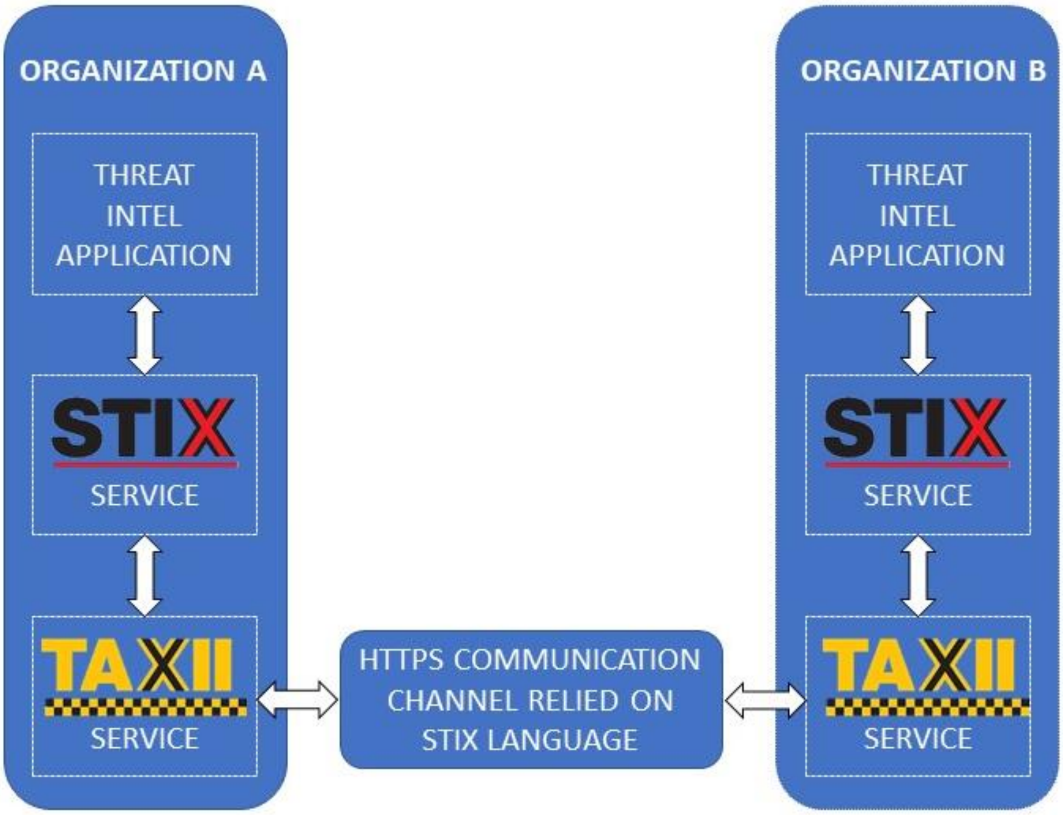


Figure 5: A high-level representation of a STIX/TAXII deployment

In our example, two different organizations decide to interchange their CTI information by developing locally their own JSON or XML-based services, depending on the needs of a custom security-oriented application and the underlying infrastructure used. In order to do so, these organizations also have to set-up and co-manage a trusted channel for the transmission of data according to the STIX language. This is of course a high-level representation of the potential deployment of a STIX/TAXII sharing platform, since additional security variables have to be taken into consideration, such as the provision of a commonly used authorization mechanism and a tampering-proof methodology.

3.3.2 CybOX

Cyber Observable eXpression (CybOX)[16] is a standardized language which allows the systematic encoding and sharing of information related with cyber observables. Cyber observable can be defined as any event or property that comes from a cyber entity or incident. Typical examples of cyber observables range from dynamic events to stateful measures, enabling thus the support of tasks related to threat assessments, event logging, incident response, cyber forensics, shared situational awareness, etc. The language also consists of several CybOX objects, where each one of them corresponds to a predefined schema of properties. The combination of these objects and properties is used to uniquely characterize a given object in the cyber security domain. Thanks to the modular architecture of the language, the selection and integration of specific only subsets of those schemas is also feasible, satisfying thus the needs of various individuals and organizations. CybOX has also laid the foundations for the development of higher level languages, schemas and conventions (Casey, et al., 2015), including the Malware Attribute

[16] https://cyboxproject.github.io/

Enumeration and Characterization (MAEC)[17] language, and the Common Attack Pattern Enumeration and Classification (CAPEC) list. The former is a standardized language for characterizing and exchanging malware-related system and network events, while the latter is a classification taxonomy of the most commonly used attack patterns. However, the most noticeable contribution of CybOX is definitely its adoption from STIX, since the second version of the standard (STIX 2.0) has fully integrated the CybOX language in order to characterize events and behaviours through observable patterns.

3.3.3 IBM X-Force

IBM X-Force (IBM Security, 2014) is a threat intelligence platform which enables users to stay ahead of emerging threats by allowing them to quickly search and timely share information regarding the latest security trends and vulnerabilities. The platform itself operates as a cloud-based infrastructure which incorporates both human-made and machine-generated intelligence, combined in a scalable environment where the security of the system and the privacy of the underlying data remain intact. However, it is worth noticing that the free version of the platform only offers access to an extensive collection of malicious IPs, URLs, botnets and security vulnerabilities. The support of advanced security features (e.g. early warning of newly identified threats, CTI reports, indicators of compromise) as well as the ability to consume X-Force's APIs using either the STIX/TAXII standard or any RESTful JSON-compatible format, are available exclusively to the paid versions of this platform.

3.3.4 Mandiant Threat Intelligence

FireEye's Mandiant Threat Intelligence[18] is a multi-layered next generation CTI product which provides deep context and conventional cyber-security operations, imitating the roles of a SOC or IR team. It incorporates core functions to leverage CTI information for the identification and mitigation of potential cyber-threats based on an infrastructure's components. Its integration is seamless and supports all three levels of threat intelligence, allowing the trusted manipulation and transformation of CTI information. Thanks to the aforementioned features and its satisfactory performance from the perspective of Threat Intelligence (Forrester Research, 2018), FireEye Mandiant is today deemed as one of the ideal solutions to deal with any mission-critical and business-critical applications operating in a wide range of sectors, including but not limited to financial, healthcare, energy, and government.

3.3.5 MISP Threat Sharing

MISP (Malware Information Sharing Platform) Threat Sharing is an open-source threat intelligence sharing platform which enables the collection and exchange of threat-related information including cyber-security indicators (Wagner, et al., 2016). The collaborative nature of the platform is able to enhance the security situational awareness of its users, allowing them to develop mechanisms for the efficient detection of existing vulnerabilities or adopt a series of preventive measures against specific kind of attacks. Such solutions are feasible by implementing a new software product which is compatible with MISP's core format, or by integrating MISP's data models as additional components to an existing product. The data models introduced in MISP involve the standard description format that should be used to create simple and complex

[17] https://maecproject.github.io/

[18] https://www.fireeye.com/mandiant/threat-intelligence.html

events, where each event object is correlated with one or more characteristics called “attributes”. Even though that such attributes may contain any information relevant to the identified threat (e.g. date of compromise, threat level, organization name, etc.), the most prominent fields are the “category” and “type”. The former aims at describing what the current attribute represents (e.g. network activity, financial fraud, etc.), while the latter aims at describing how the attribute represents the chosen category (e.g. IP address, email headers, etc.). This data model is further backed by the capability of a user to define the desired depth of data share, the definition and reusing of human-readable tags based on a taxonomy system (Cope, 2007), and a synchronization protocol with pull and push mechanisms which employ JSON (JavaScript Object Notation), UUIDs (Universally Unique Identifiers), and cherry picking technologies. Thanks to these features and its continuous community-driven development, MISP instances can be found today across several organizations, institutions, or even community-based projects.

3.3.6 C3ISP Collaborative Framework

C3ISP is a collaborative and confidential information sharing and analysis framework which was funded under H2020-EU.3.7. (European Commission CORDIS, 2016). The framework can be deployed as a service to enhance the cyber-security protection of various types of organizations,

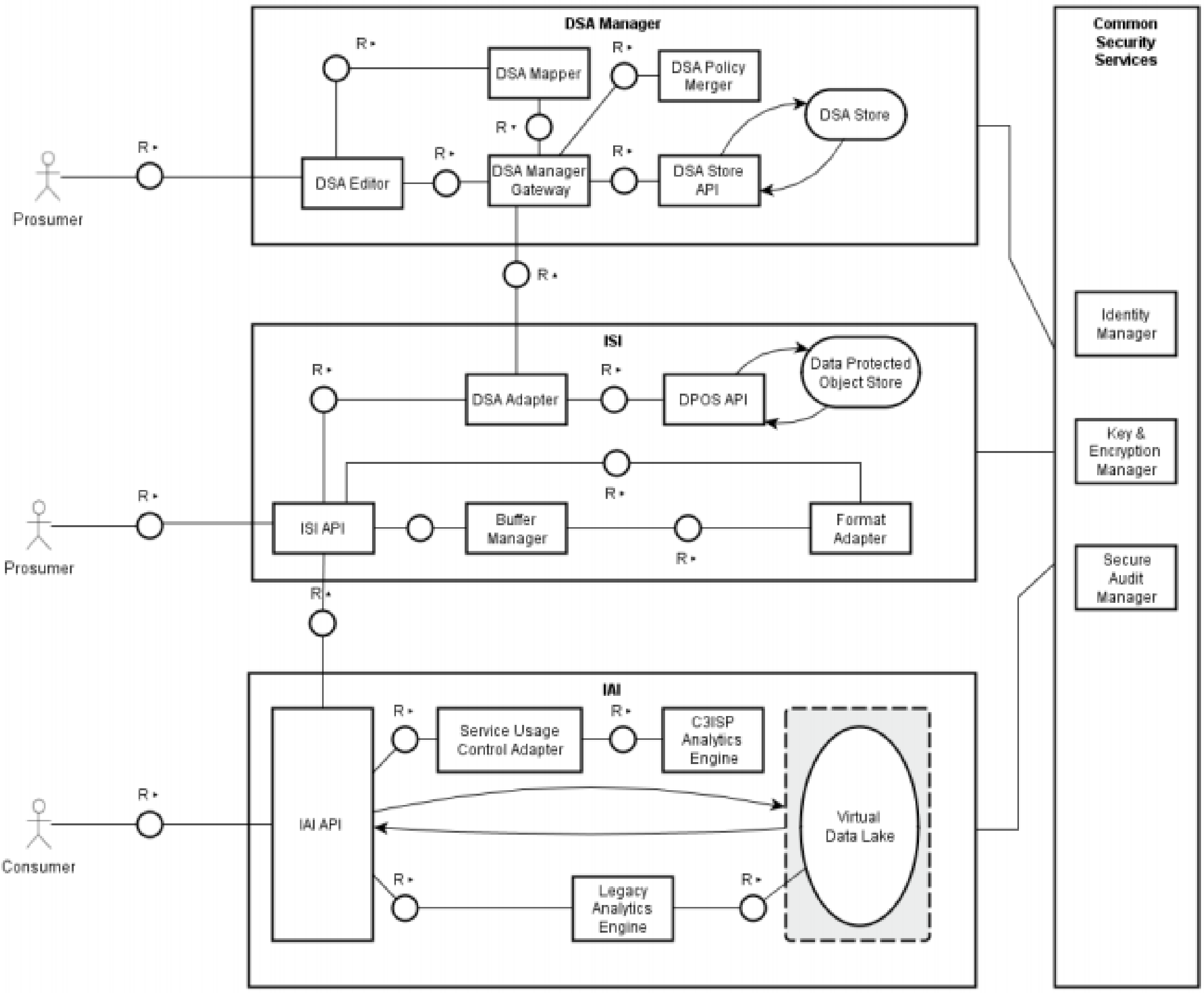


Figure 6: C3ISP high level architecture

by acting as a service to enhance the cyber-security protection of various types of organizations, also by acting as a flexible and controllable medium for the sharing of data between them. Its carefully designed and versatile architecture also enables the preservation of privacy and the confidentiality of the exchanged information, covering several areas including but not limited to Internet Service Providers (ISPs), Computer Emergency Response Teams (CERTs), and any application domain of a small or medium-sized enterprise. (Fan, et al., 2019) took advantage of the capabilities provided by the C3ISP framework and presented an API gateway which allows the sharing of multiple common components between different organizations, reducing thus the deployment time, cost, and maintenance. The main advantage of the C3ISP framework is the secure sharing, storing and analysis of information, which is achieved through the continuous enforcement of security policies. Data owners can define security constraints through security policies written in the human-readable Data Sharing Agreements (DSAs). Figure 6 depicts the high-level architecture of the C3ISP framework.

There are two types of entities that interact with the C3ISP platform, i.e., data producers and data consumers. These entities also expanded with their specific roles. An entity that provides data to the C3ISP platform is a data producer. The data producer is an entity that provides data to the C3ISP platform and thus shares it with other entities known as data consumers. C3ISP regulates information sharing according to policies, where each policy defines a set of rules for data access and usage. The data prosumer is a generalization of the data producer and data consumer roles. Hence, any entity may act as both the data producer and data consumer. Thus, in a collaborative approach, that entity may provide data to the C3ISP platform to improve the knowledge base shared between other entities and also retrieve data supplied by others or run analytics services on the whole dataset.

The C3ISP platform includes 4 main subsystems, namely Data Sharing Agreement (DSA) Manager, Information Sharing Infrastructure (ISI), Information Analytics Infrastructure (IAI), and a bunch of integrated Common Security Services (CSS).

3.3.6.1 DSA Manager

The Data Sharing Agreement Manager (DSA Manager) component is in charge of handling security policies. Each policy is a DSA object that encapsulates the policy requirements (i.e. the set of rules) under which a protected data object (CTI record) can be used and shared by other entities. The DSA Manager subsystem handles the DSA lifecycle, from the editing phase to its usage till its termination. The data prosumers collaboratively define the sharing and analytics rules used by the C3ISP platform to handle information provided by data prosumers, thus considering all the set of jointly agreed requirements.

3.3.6.2 Information Sharing Infrastructure

The Information Sharing Infrastructure (ISI) is a subsystem that allows data prosumers uploading their information to the C3ISP users (i.e. the other data prosumers) under the governance of an appropriate DSA. The implementation of the ISI subsystem enables its deployment both locally and remotely depending on multiple factors, including, computational capabilities, trust and other security requirements, etc. However, in both implementation scenarios, the DSA Adapter provides a core feature. This component is able to enforce the DSA rules. Particularly, it enforces DSA related to data access and data usage control. The DSA Adapter may also enforce one or multiple Data Manipulation Operations (DMOs) to preserve privacy. A data producer can submit her data to the C3ISP platform, and the data consumer could use the ISI to retrieve shared data under the constraints defined in the DSA policies. Furthermore, the C3ISP platform stores information under the DSA policies in a Data Protected Object Storage. Hence, the C3ISP platform allows storing datasets as Data Protected Objects (DPOs), thus only authorized entities can access them. However, depending on access privileges assigned to entities, different anonymization operations must be enforced on various pieces of data.

3.3.6.3 Information Analytics Infrastructure

The Information Analytics Infrastructure (IAI) is a subsystem that offers a set of analytics services. Depending on the DSA associated with information that has been shared and stored using ISI subsystem, entities may request an execution of different analytics. Furthermore, same DSA rules may be also applied for handling results of the analytics services. Hence, the IAI submits results to the ISI in order to share them with the C3ISP users and possibly used as an input for a new analytics service. In addition, the subsystem provides a Virtual Data Lake (VDL), prepared to be used by certain analytics services. The VDL contains data that is prepared according to the DSA rules and usage constraints (e.g. part of the data could be anonymized, etc.).

3.3.6.4 Common Security Services

As set of Common Security Services (CSS) are used to support the functions of the C3ISP Framework. Therefore, access and usage control need identities and profile information from the Identity Manager to evaluate access requests. The C3ISP platform uses the Secure Audit Manager to trace the performed operations. Finally, the C3ISP platform uses a Key and Encryption Manager to enable the confidential computations and the secrecy for the shared CTI. To enable data usage control and continuous enforcement of security policies, the C3ISP platform relies on the Usage Control Systems (UCS) that implements the UCON paradigm. The following section describes the UCS in more detail.

Chapter 4 Trust Management Approaches

The collection and sharing of CTI goes hand in hand with the adoption of a trust management approach that should be responsible for the appropriate qualification of services, the enhancement of user privacy, and the boost of the exchanged information security. Even though that the modelling and implementation of a trust management system between different information systems has concerned the research community before (Ruohomaa & Kutvonen, 2005), the type of information security has been reported to be entirely different with the traditional one (Von Solms & Van Niekerk, 2013). This lies to the fact that cyber-security domain has to deal with the efficient protection of an additional set of resources like the assets, persons, etc. In this chapter we address the most prominent solutions in various technological backgrounds with respect to those trust management solutions which could be of potential use in CyberSANE project. All of the below mentioned frameworks, techniques, and algorithms, shall be taken into consideration for the upcoming implementation of the information sharing and trust management scheme, which is going to be used in the ShareNet component of CyberSANE (Papastergiou, et al., 2019).

4.1 Ontological Frameworks

Today, different types of ontological frameworks have found application across a wide range of domains, boosted by the growth of Semantic Web and the language-dependent conceptualization capabilities met in any ontology (Guarino, 1998). Several computational ontologies have been proposed in the context of cyber-security domain as well, including some novel trust management approaches. One of the first ontology-based approaches which made use of a trust management system was proposed in (Squicciarini, et al., 2006). The authors of this paper formulated a mechanism to overcome the privacy concerns of trust negotiation systems by deriving disclosure policies and attributing semantic relationships. A few years later, (Blasch, 2014) presented the first satisfactory definition of a trust ontology associated with the underlying areas of any system. The outcomes of this study pointed the necessity to differentiate and fuse information between machine, hardware, software, user, application, and network areas. CRATELO (Oltramari, et al., 2014) is another sample of a three-level modular ontology focused on the cornerstone aspects of cyber-security, where among others includes a series of trust management approaches. Its trust-related component focuses into the characteristics, relationships, and situational awareness of individuals, assisting in this way on the prediction and quantitative analysis of risk assessments. This Human Factors Trust Ontology (HUFO) was later enhanced with additional semantics to enable the insightful and actionable reasoning of information under a scalable and portable platform (Oltramari, et al., 2015).

According to a study conducted by (Huang & Fox, 2006), any trust ontology has to focus on formally modelling trust structures as information sources and information dependencies. Taking into account the outcomes of this study, as well as the Quality-of-Service and Quality-of-information criteria which are also deemed of high importance in CIIs, (Oltramari & Cho, 2015) presented a composite trust-based ontology framework consisting of four ontologies for information fusion and human-decision purposes. Their work took also advantage of the DOLCE (Descriptive Ontology for Linguistic and Cognitive Engineering) foundational ontology (Masolo, et al., 2002) to represent trust attributes in the context of cyber-security domain, according to the modelling examples previously proposed in (Oltramari, et al., 2014). Therefore, each integrated component of their system was developed to deal with one of the trust types depicted in Table 2, covering in this way all the necessary attributes related with reliability, availability, confidentiality, integrity, and certainty.

Trust Type	Communication Trust	Information Trust	Social Trust	Cognitive Trust
Trustee	Medium & Machine source	Information	Relationships	Human Cognition
Evaluating Factor / **Attribute**	Quality of Service	Quality of information	Social Capital	Judgement Competence
Reliability	Packet Delivery	Source Credibility	Expertise	Logical Thinking
Availability	Service Availability	Information Availability	Willingness	Willingness
Confidentiality	Authentication	Accessibility	Privacy	Morality
Integrity	No Network Attack	Correctness	Honesty	Truth Seeking
Certainty	Consistent Data Processing	Consistency	Stability	Responsibility

Table 2: Correlation of trust types with trustees, attributes & evaluating factors

Furthermore, the massive adoption of Internet-of-Things (IoT) technologies in Smart Cities, Industry 4.0 and eHealth initiatives which has been observed over the last few years, gave birth to a set of recommendations (Simon, 2017), specially addressed to overcome the security risks identified in today's CIs. For that reason, (Gonzalez-Gil, et al., 2019) proposed an ontology for the context-based IoT security evaluation which among others employed trust management capabilities based on an observer's concerns, interests, assets, and information sharing preferences. Last but not least, a promising proposal for a Reference Ontology of Trust that could potentially find application as a medium of trust management within a CI was presented in (Amaral, et al., 2019). The foundations of their trust-based ontological scheme is based on the Unified Foundational Ontology (UFO) proposed back in 2008 by (Guizzardi, et al., 2008), but the authors of the paper clearly state that their approach has to be validated against real-world scenarios and an expansion of trust assessment factors between the trustor and the trustee is a pending issue.

4.2 Access & Usage Control Models

The collaboration and sharing of CTI information between different CIs and CIIs emerged among others the necessity of adopting a trust management solution that could efficiently satisfy a common set of criteria defined by all participants. Such solutions tend to enforce various access control policies defined by specific collaborative models that aim to achieve business continuity. However, the classical access control models were not able to sufficiently deal with the agile and quickly evolving permission landscape (Kalam, et al., 2003), giving birth thus to several organization-based access control models over the last years. (Nasser, et al., 2005; Cuppens, et al., 2006) investigated the access control policies between different virtual organizations and proposed a set of OrBAC (Organization Based Access Control) approaches to efficiently manage the underlying security policy interoperability. In contrast to the aforementioned OrBAC models, (Baina, et al., 2008; Abou El Kalam, et al., 2009) took into account the highly interdependent nature of CIs/CIIs and presented instead a collaborative access control framework known as PolyOrBAC. Any organization which adopts a PolyOrBAC approach is capable of collaborating with another organization by exposing a set of Web Services, keeping however its resources and internal security policy intact.

(Aali, et al., 2015) took a step forward and implemented a Trust-PolyOrBAC architecture for the establishment of trust between different CIs during their collaboration process. Their approach took advantage of evaluated certification and authentication methodologies (Kent, 1998), and they were able to define and identify those trust parameters that could be of use in a CTI sharing initiative of Electrical Grid infrastructures. On the other hand, CIs which had their information migrated and shared on the cloud, needed another near real-time, scalable, and efficient set of rules and security policies. (Saidi, et al., 2012) proposed a trust organization-based access control model for cloud computing systems coined as TOrBAC, which was afterwards replaced by an advanced access control protocol (Saidi & Marzouk, 2013). The latter study gave birth to a Multi-TrustOrBAC cloud computing environment based on the notion of a trusted third party[19] who was responsible to piece together each organization's security policies and enforce all organizations to address all of these policies. Finally, trust access control mechanisms have been also presented in the context of fog computing (Daoud, et al., 2019), where several CIIs are already operating on a large scale for telecommunications, IoT, and information sharing purposes. The proposed model in this occasion lies to the integration of a distributed access control and monitoring scheme, which comes with native proactive capabilities based on the trustworthiness of the data being exchanged between its peers.

Notwithstanding the aforementioned models consider trust as the principal aspect, which influences the final decision, two main drawbacks bind together traditional access control and trust-based models. Hence, the first drawback is flexibility, which allows expressing various conditions affecting the decision-making process. While the second drawback mainly correlates to the lack of continuity of data usage control over time. In fact, an efficient access control model, known as ABAC (L. Wang, 2004), which characterizes subjects, objects, and the operational environment through the set of corresponding attributes, provides a flexible approach for expressing various security constraints. Moreover, the model received high attention and many implementations were proposed. Thus, in (E. Yalcinkaya, 2017) proposed an implementation of ABAC model for CI with a focus on Industrial Control System (ICS). The approach aims at providing the access control to a PLC controlled robotic arm considering the multiple conditions expressed through attributes. However, although ABAC allows describing a subject also considering an assigned trust or reputation level as an additional attribute, the main limitation of this model is a lack of control over attribute value changes within time. Meanwhile, to cover the limitations of traditional and trust-based access control models, in (J. Park, 2004) R. Sandhu and J. Park proposed a revolutionary usage control model referred to as UCON. Hence, differently from traditional access control models, the UCON allows not only describing entities but also provides control over the mutability of attribute values. Thus, whenever attribute values change and do not satisfy security policies anymore, the system accompanied by the UCON model will immediately revoke the usage of a resource, excluding the information abuse. Considering the advantages of the UCON among traditional access control models, several works proposed implementation of UCON for different scenarios. The work presented in (G. Baldi, 2020) proposes the BigUCON framework that exploits UCON for providing an enhanced, expressive and flexible authorization support for data protection within the Apache Hadoop ecosystem. The proposed framework allows considering the trustworthiness of a network to which the device is connected as an essential attribute required for the decision-making process. Although the UCON model

[19] https://en.wikipedia.org/wiki/Trusted_third_party

does not consider trust as a separate aspect that influences the access decision, describing trust, rating, and reputation of an organization through attributes is a common approach nowadays.

4.3 Reputation-Based Techniques

Reputation-based techniques is one more research domain which aims at dealing with the trust management issues coming from the rapid growth of information sharing. The establishment of trust in these occasions usually takes place by calculating and assigning a trust score to each participant of a peer-to-peer (P2P) network. One of the first and most prominent works on this area was presented by (Aberer & Despotovic, 2001). The authors of this paper introduced and combined several scalable data structures and algorithms, in order to efficiently deal with trust management both on data and semantic levels. A couple of years later, (Buchegger & Le Boudec, 2003) presented a modified Bayesian approach as a trust score reputation mechanism which was also resistant against false disseminated information, while the study of (Kamvar, et al., 2003) provided a distributed and secure methodology to compute global trust values over a sharing network of legitimate and malicious files. Last but not least, it is worth also noticing the reputation-based trust management solution proposed in (Xiong & Liu, 2004), where the trustworthiness of peers is accessed based on a decentralized transaction-based feedback system.

On the other hand, (Zhou & Hwang, 2007) presented an adaptable reputation system for large-scale grid applications, where the reputation accuracy and aggregation speed were improved over time, thanks to the deployment of a distributed ranking mechanism of their peers. This mechanism was based on the power-law nodes methodology presented in (Faloutsos, et al., 1999), while a historical reputation ranking of peers between CIs has been also proposed by (Dionysiou, et al., 2008) as the recommended trust management approach. A few years later, (Zhao & Li, 2013) adopted the notion of trust overlay networks and presented a trust-vector aggregation algorithm for any type of P2P network, upon which the reputation of each peer is based on his distributed historical malicious -or not- behaviour and activities. Last but not least, it is worth noticing a relatively recent survey which addresses the issue of reputation-based trust management systems in those application domains that come with a large number of physical entities (Chen, et al., 2019). The authors of this paper presented a novel trust architecture by combining a soft-defined networking control layer with a cross-layer authorization protocol, backed by both behaviour-based and organization-based reputation evaluation schemes.

Additionally, other works proposed taxonomy-based approaches to evaluate the trust of resources of CTI and/or organizations, which request to use CTI records. Hence, the work proposed in (T. Schaberreiter, 2019) defines a methodology for evaluating CTI sources according to quantitative parameters. The presented methodology aims to contribute to the trust establishment of CTI sources, based on a weighted evaluation method. The method allows a single entity to adapt the proposed methodology to predefined priorities and security constraints. The approach was adapted and evaluated together with the STIX standard. Another approach proposed in (T. D. Wagner, 2018) presents a trust taxonomy for establishing a trusted CTI sharing environment. The proposed trust taxonomy relies on multiple attributes, including sharing activity, rating provided by other peers, which evaluated shared CTI, etc. and those attributes are used to create a trust profile of the entity. In (Arachchilage, 2013) the authors presented a taxonomy for trust domains to enable entities to collaborate securely across functions, geographies, and corporate boundaries. The proposed taxonomy can be adapted while designing information-sharing environments in order to prevent information leaks, still enabling entities to define constraints on how their resources can be shared. Also, the study reported in (L. Qiang, 2018)presents the quantization and evaluation method used as a reference while measuring the quality of CTI content from the perspective of a user.

4.4 Trust in Cyber-Physical Systems

The majority of CIs are nowadays composed of numerous physical objects which are responsible for computation, networking, and communication tasks. Embedded systems, supervisory control and data acquisition (SCADA) systems, power grids, and transportation infrastructures, are a few only CIs where Cyber-Physical Systems (CPS) undertake such roles between the peers of their internal or external networks and have to be sufficiently secured (Das, et al., 2012). The efficient defending of these CIs against cyber-threats, as well as the enhancement of their trust and sharing capabilities, requires either the adoption or the development of an appropriate CPS design methodology followed by a virtual simulation and validation of its outcomes in terms of security and trust (Shukla, 2016). The trustworthiness of data is also attributed as one of the core concepts of aspects is the CPS-related framework proposed by NIST (Griffor, et al., 2017), since the security gaps regarding the exchange of trusted information in these environments have concerned the research community before. One of the first extensive studies with respect to managing trust in CIIs took place in (Sabo, 2004), where several operational, policy, and privacy issues are discussed in the context of information sharing. (Tang, et al., 2010) presented a trustworthy alarm detection framework where security events construct an object-alarm graph, which is in turn used to carry out the desired trustworthiness inference at network level. On the other hand, (Li, et al., 2011) proposed a trust management solution applicable on wireless networks by employing a context-aware trust evaluation scheme with a set of policy rules.

Following the same pattern, a holistic approach to address the policy and trust issues met in any kind of CPS components of a CI was also presented by another study of (Li, et al., 2011). The proposed framework was able to manage trust relationships between different network entities, and derive the trustworthiness of the reported security events based on three different types of trust, the device trust, the report trust, and the event trust. A few years later, (Saqib, et al., 2015) presented a two-tiered trust-based approach where the boundary of trust is created internally and externally between all the interconnected CPS components, while (Taylor & Sharif, 2017) reviewed the challenges of providing the necessary information assurance in the context of integrity and confidentiality. The authors of the former study managed to identify the lack of trust in CPS domain and noted the necessity to extend or implement additional trust management approaches, whereas the latter study examined and proposed a series of novel approaches to boost the trust management of the system and reduce the security complexity overhead. Both works conclude that the trust management lifecycle has to remain context-dependent of the underlying industry (Blaze, et al., 1996), as well as flexible and scalable in order to cover future system modifications and misuse patterns. Last but not least, the need of the reliable and secure exchange of trusted information in a CPS embedded system was also recently addressed in (Lamba, 2020). The proposed solution was once more a two-tiered trust-based framework which resembled the functionality and architecture previously presented by (Saqib, et al., 2015).

4.5 Trust and Reputation for Cyber Threat Intelligence

Trust and reputation are fundamental aspects of an organization that shares information. Furthermore, if information aims at describing cyber-incidents and potential countermeasure strategies, trust in this information is an essential feature for decision making. Thus, it may be used to define whether the specified countermeasures can lead to a potential negative impact on the system's security. According to (Abimbola, 2007), establishing trust in CTI sharing is one of the most crucial attributes used to build relationships between stakeholders. Furthermore, according to a survey[20] conducted by Ponemon Institute, timeliness and trust in the source are among the most important attributes for the evaluation of actionable CTI. In fact, the lack of stakeholders' trust may pursue the organization not to share its CTI since it may reveal that the security of this organization were breached (Ruks, 2015).

Most available and used Threat Intelligence Platforms (TIPs) establish trust through the vetting process. Usually, producers or vendors of CTI conduct this process. On the other hand, several platforms use recommendation systems. These systems enable organizations to recommend other stakeholders. Hence, it is possible to compute trust based on those recommendations. Existing TIPs provide a limited approach for establishing trust manually or automatically. The main focus of existing TIPs is the incident indicators sharing and their visualization in a graphical interface. Additionally, most approaches provide the internal verification process, which shifts the responsibility to the provider. Therefore, the provider and its vetting processes have to be trusted and understood by others. Nevertheless, this fact limits the establishment of trust circles with decentralized peers. Thus, CTI may be very limited since it is only shared in small circles. On the contrary, a wide range of connected stakeholders enables participants to use threat sensors globally. Therefore, each stakeholder enables threat monitoring techniques and detection systems to produce the results, which will be automatically consumed by all community members. As mentioned in (Thomas D. Wagner, 2018), various platforms enable specific vetting processes to establish a trusted environment. However, external connections are out of the scope, and it is not possible to share CTI with other sources leading to the limitation of CTI sources. The majority of currently existing TIPs provide CTI directly to their stakeholders. On the other hand, only four platforms enabled the manual connections between stakeholders or to external threat intelligence feeds alongside their vetted CTI. However, approaches used to establish trust are mostly vetting processes. These processes are not transparent for users to see. Hence, this fact requires stakeholders to trust the TIPs.

4.5.1 Trust Taxonomy for Shared Cyber Threat Intelligence

Trusted relationships between organizations stimulate confidence that the result of provided CTI application will as expected. Stakeholders expect that CTI will not harm the system and will not affect on organization's assets negatively. Hence, identifying the membership criteria for any CTI sharing effort will result in building transparent and trustful relationships from the beginning. As one of the approaches for establishing transparent relationships between stakeholders, different trust taxonomies, including (Garcia-Molina, 2006), (Almeroth, 2012), and (Nalin Asanka Gamagedara Arachchilage, 2013) have been widely accommodated. Furthermore, different schemes, including 5x5x5 which evaluate intelligence according to the source, data validity, and sensitivity with grades from 1 to 5, are widely used nowadays. Additionally, the Admiralty Code is adapted to evaluate the reliability of the source and the confidence in the information. These approaches recently appeared in various TIPs to evaluate CTI.

The approach proposed in (Thomas D. Wagner, 2018), proposed a trust taxonomy targeted to establish a trusted threat sharing environment. In particular, the taxonomy consists of four different attributes. The fist attribute belongs to the trust level in the source, which requires transparency related to the generation of CTI. In some cases it may lead to the intelligence life cycle, including malicious activity identification, vulnerability disclosure, defining of countermeasure strategies, etc. The proposed taxonomy considers five levels of trust, namely 1 = Very High, 2 = High, 3 = Medium, 4 = Low, and 5 = Very Low.

[20] https://www.brighttalk.com/webcast/5385/288467/exchanging-cyber-threat-intelligence-there-has-to-be-a-better-way

The second attribute considered in the proposed taxonomy is the rating of a stakeholder, which may be obtained from other stakeholders' reviews that received CTI. The attributes used to evaluate the rating of the stakeholder may span from quality or timeliness up to communication. Similarly to levels of trust, the rating consists of five possible levels, including 1 = Poor, 2 = Bad, 3 = Moderate, 4 = Good, and 5 = Excellent.

The third attribute is the activity with which a stakeholder shares CTI. Although the number of CTI contributions may not be a direct indicator for trust, sharing activity may signal the stakeholder that someone is not attempting to share their CTI. In this case, some particular circumstances, including the low level of trust in the sharing community, insufficient resources to produce CTI, or it has potentially low quality. The proposed approach considers three different values for characterizing activity. These values are: Very Active, meaning that CTI has been shared in the past seven days, Active - CTI has been shared in the past thirty days and Inactive - CTI has been shared more than thirty days.

Finally, the fourth attribute describes the sector or domain of the sharing stakeholder. In particular, the proposed taxonomy considers the following domains: Finance, Retail, Academia, Automotive, and Electricity. The affiliation of a stakeholder to a particular industrial group can contribute to the trust level by being part of a respected group.

The parameters for the proposed taxonomy attributes are set to have sharing activity as 9%, stakeholder’s rating as 36%, same source 18%, and same industry as 37% weight. Hence, the maximum value for the sharing activity is 9% only if the stakeholder shares CTI very actively and it could be 4.5% if the stakeholder shares CTI only in 30 days. Otherwise, the sharing value equals 0% since the stakeholder either do not share CTI or share it once in more than 30 days. The max value for the stakeholder’s rating equals 36% only if other peers evaluated this stakeholder as excellent. This parameter has the second highest contribution to the overall trust since other peers may evaluate the trustworthiness according to the quality of CTI and the conduct after receiving the information. Another aspect of the taxonomy described through the attribute is related to the source of CTI. Information regarding whether the sharing stakeholder actually produced CTI or forwarded it from another unknown source is a valuable parameter. Finally, the affiliation of the stakeholder to a specific industry or domain has the highest value of all four attributes.

4.5.2 Peer-to-Peer Trust Taxonomies

In the Peer-to-Peer (P2P) networks, trust model can effectively reduce the influence of malicious nodes. Eigen Trust is one of the most authoritative trust model, which is mainly applied to the P2P data sharing system. Furthermore, this approach is the theoretical basis of many trust model. Many works have improved the Eigen Trust in different aspects for enhancing the performance of the model. The model use service trust value to indicate node's recommendation trust, which failed to prevent a node that has high service trust value and provides malicious recommendation. Therefore, the work proposed in (Gray, 2003) provides a trust model based on the recommendation trust. The proposed trust model can prevent a node with higher service trust value to defame a normal node by distinguish between the service trust value and recommendation trust value. On the other hand, the access control mechanism has been added into the considered system to limit the node’s access permission that do not sharing file actively.

During the past decade, online trust and reputation systems have provided convincing answers to emerging challenges in the global computing infrastructures relating to computer and network security, electronic commerce, virtual enterprises, social networks and cloud computing. The goal of these systems in such global computing infrastructures is to allow entities to reason about the trustworthiness of other entities and to make autonomous decisions on the basis of trust. This requires the development of computational trust models that enable entities to reason about trust and to verify the properties of a particular interaction. The robustness of these mechanisms is one of the critical factors required for the success of this technology.

4.5.3 Trust Evaluation in Threat Intelligence Sources Quality

The quality of CTI records is a crucial characteristic that must be considered while applying shared information, since it may harm systems to which those CTI records are applied. Nowadays, different approaches for evaluating CTI sources exist. Those approaches are divided into two groups according to the purpose of the collected information and the source type. Multiple approaches, including (Botega, 2017), (Li Cai, 2015) and (Hongwei Zhu, 2009), consider the source analysis based on the quality of the provided information. However, considering the era of big data and big data analysis, this analysis becomes more challenging.

Hence, in the aforementioned article (Li Cai, 2015), the authors introduced a big data quality assessment framework that relies on five dimensions, including availability, usability, reliability, relevance, and presentation quality of a source. Furthermore, each item of the proposed dimensions consists of multiple elements. On the other hand, in (Hongwei Zhu, 2009) the authors introduce a set of metrics to determine the quality of the source. Additionally, the work presents an approach to perform the validation of the source. Differently from the introduced approaches, the authors in (Botega, 2017) identified metrics and indicators specific to the domain in which the information will be used. In particular, the proposed work presents a structured methodology consisting of five assessment criteria, including syntax accuracy, timeliness, completeness, situation certainty, and consistency and relevance. The approach aims to improve critical information received by emergency response teams by evaluating the sources according to the above criteria.

In the CTI area, proposed methods for CTI evaluation, including (Meier, 2018) and (Qiang, 2018), are mostly theoretical and not yet publicly available. Although the criteria selected by the authors in (Qiang, 2018) are useful for a general assessment of CTI sources, the need for manual evaluation performed by experts via a questionnaire still exists. Then the obtained results of the questionnaire are adjusted using a multi-objective algorithm. This approach evaluates commercial CTI providers, while the work on the micro-level of CTI is still required.

The authors in (Liao, 2016) have created an automated solution scanning thousands of blog entries and creating relevant cyber threat entities after matching information collected. This tool relies on Natural Language Processing (NLP) while identifying threat information in the unstructured text. Although the proposed approach focuses more on cyber threats on a micro-level. However, it does not offer any analysis of collected information. Finally, in (Meier, 2018), the authors presented an approach that uses the automated analysis of each single cyber threat message to derive an overall rating for its source. The approach is based on Google's PageRank (Page, 1999). In this way, the algorithm performs a ranking of feeds according to the originality of feed content and its reuse.

Apart from mentioned methods for evaluating trust of the CTI sources, another approach exists. It focuses on how much the CTI source can be trusted. This method has been applied to P2P information sharing platforms, including (Mokaddem, 2019), and (Wagner, 2018). Furthermore, commercial anti-virus providers like (Al-Ibrahim, 2017), use the same approach. Considering that each peer in the P2P community can access and share information, it is essential to trust peers. However, existing P2P networks use personal validation of their peers and base trust on personal experience.

The authors in (Schaberreiter, 2019) proposed an approach for performing quantitative evaluation of trust according to the quality of the shared CTI. The goal of the proposed methodology is to facilitate trust establishment to sources of CTI using the weighted evaluation method. The considered approach enables entities to adapt it based on their own needs and requirements. By using the presented methodology, stakeholders can derive a trust value for each CTI source based on the quantitative evaluation of parameters for each message provided by a CTI source. To validate information provided by a source, the proposed methodology validates CTI provided by one source against the information provided by the other sources. In this way, concrete conclusions about specific parameters (Table 3), including time when the information has been shared, its originality and added intelligence are used to compare each CTI record with other shared by different sources.

Parameter	Description
Extensiveness	Evaluates the number of optional parameters filled in the record
Maintenance	Determines the frequency of updating the messages
False Positives	Determines how often messages of a source are invalidated
Verifiability	Expresses how often a CTI source verifies the information they provide by linking their source
Intelligence	Indicates the added value of a source by linking it to other objects
Interoperability	Indicated the data format of a provided CTI
Compliance	Determines the compliant of a source
Similarity	Indicated similarity of specific entries between two sources
Timeliness	Specifies which source provides information first
Completeness	Indicates the number of occurrences of the same source

Table 3: Parameters for CTI source evaluation

The fact that the proposed methodology has been used to evaluate the quality of the source that shares CTI represented in the STIX 2.0 format makes it possible to integrate it into a ShareNet component of a CyberSANE framework. Hence, considering that the trust in the CTI source is dynamic, the continuous authorization engine of the ShareNet system will use the trust value associated with the CTI source (a stakeholder) to evaluate the access and usage requests. In this way, the CyberSANE framework will ensure the quality of the CTI provided by different entities. Furthermore, the quality of the CTI content, its freshness, and low similarity with other information will directly affect the reputation of a CTI source, which is also will be used for evaluating access and usage requests against security policies.

Chapter 5 Innovative CTI Sharing

This chapter provides an overview of the high-level architecture of the ShareNet system for the advanced CTI sharing and dissemination. The ShareNet system exploits advantages both of the C3ISP and MISP platforms. This chapter also describes architecture of specific ShareNet system modules used to achieve privacy and security requirements through the evaluation of usage control policies also considering trust and reputation associated with stakeholders.

5.1 Usage Control for information sharing

As described in ((C3ISP), 2019) the C3ISP platform implements the Usage Control (UCON) model introduced by Jaehong Park and Ravi Sandhu (Sandhu, 2002). Figure 7 depicts the eXtensible Access Control Markup Language (XACML) (Rissanen, n.d.) reference model called UCS (Enrico Carniani 2016), (Aliaksandr Lazouski 2012) that includes three main blocks.

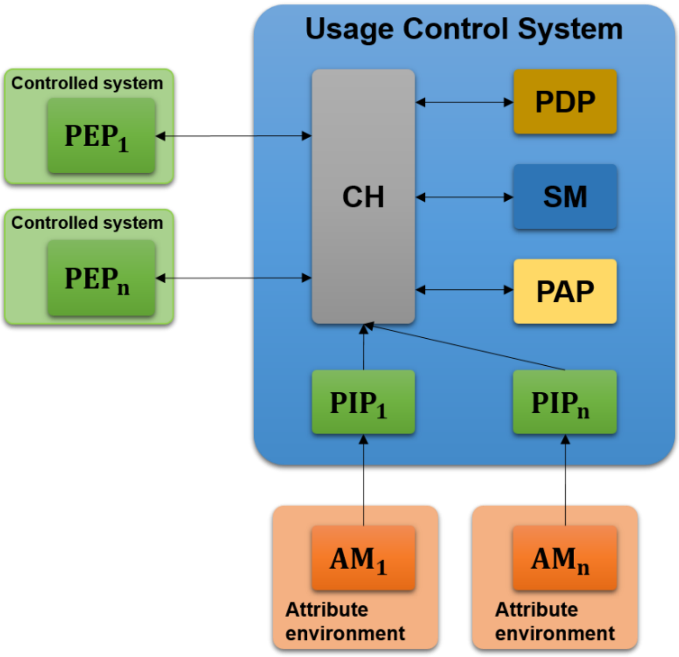


Figure 7: Usage Control Framework

The controlled system block is a component on which the UCS enforces UCON policies through the Policy Enforcement Point (PEP) component following described. The second block is Attribute Manager (AM) that provides attributes required to evaluate a request against policies. Finally, the third block it the UCS that includes seven different components. The main component of the UCS is a Context Handler (CH) that acts as a frontend. This component is invoked by the security operations (e.g., subject's request) intercepted by the PEP. This component is implemented into the controlled system. The UCS can have multiple Policy Information Points (PIPs) that are invoked by the CH component to retrieve attributes. All attributes are managed by the corresponding component called AM. This component provides an interface used for retrieving attributes and updating their values. Attributes can be required by the Policy Decision Point (PDP) in order to evaluate the request according to policies. Usage control policies can be retrieved either from the PEP or from Policy Administration Point. The last component is a Session Manager

(SM) that stores active sessions together with information for policy re-evaluation. Finally, since values of attributes can change during the session, the PIP component is responsible for detecting such changes. There are three different phases of decision process in usage control. Typically, these phases are regulated by the interactions between UCS and PEP components.

- *tryAccess*: belongs to the pre-decision phase. It starts with the TryAccess message from the PEP component to the UCS. PEP creates and send this message when subject requests to execute an access. The tryAccess phase ends when UCS sends the response message to the PEP component. The response could be either "*permit*" or "*deny*";
- *startAccess*: belongs to the first part of the ongoing-phase. The startAccess phase begins with the relative message sent to the UCS by the PEP component. The phase finishes after the policy evaluation and when the response has been sent back to the PEP;
- *revokeAccess*: defines the second part of the ongoing-decision phase that is executed whenever an attribute changes its value. The revokeAccess phrase finishes when the policy is evaluated and if a policy violation occurs. Then the UCS sends the RevokeAccess message to the PEP component.

The evaluation of the subject’s request begins when the subject tries to execute an action. The PEP component suspends the execution, retrieves attributes related to this request and sends the TryAccess message to UCS. As the next step, the UCS evaluates the request and returns the result to the PEP component. If the execution of the action is permitted, the PEP will send the StartAccess message to the UCS right after the moment when the execution of the action started. During the execution of the permitted action, the UCS will evaluate the policy whenever an attribute changes its values. If the attribute value changed and the new value does not satisfy the policy anymore, the UCS will send the RevokeMessage message to the PEP component in order to stop the access session.

In the scope of the CyberSANE project, the information and intelligence sharing infrastructure will enable advanced data distribution control according to constraints expressed through the set of security policies by using the extended and integrated UCS. Furthermore, the ShareNet system must enables prosumers to security policies in the form of human-readable DSA, which will be transformed to the XACML language described in the following section.

5.1.1 XACML Policy Specification Language

The XACML (Rissanen n.d.) standard is the most widely-used access control policy language. It allows expressing arbitrary types of attributes, and thus making the XACML standard application-independent and extensible to accommodate requirements of specific application domains. Although the XACML standard facilitates to express traditional access control models, which provides an access decision only when a request arrives, it lacks in the expressiveness of advanced features considered in the UCON model, including continuity of an access decision evaluation and attributes value mutability. Therefore, to satisfy these needs, Colombo et al. in their work (Maurizio Colombo, 2010) proposed an extension to the XACML standard called U-XACML. The extended version of the XACML standard defines three top-level policy elements namely <PolicySet>, <Policy> and <Rule>>. Although the <PolicySet> is an optional element, it may contain different <Policy> elements. The <Policy> element may contain one or multiple <Rule> element, thus its decision result is implied by a combination of <Rule> elements it contains. U-XACML specification defines several different *rule-combining algorithms*, which in the end affect the final decision. Additionally, the set of <obligation> elements accompanies the final decision result produced by the <Policy> element.

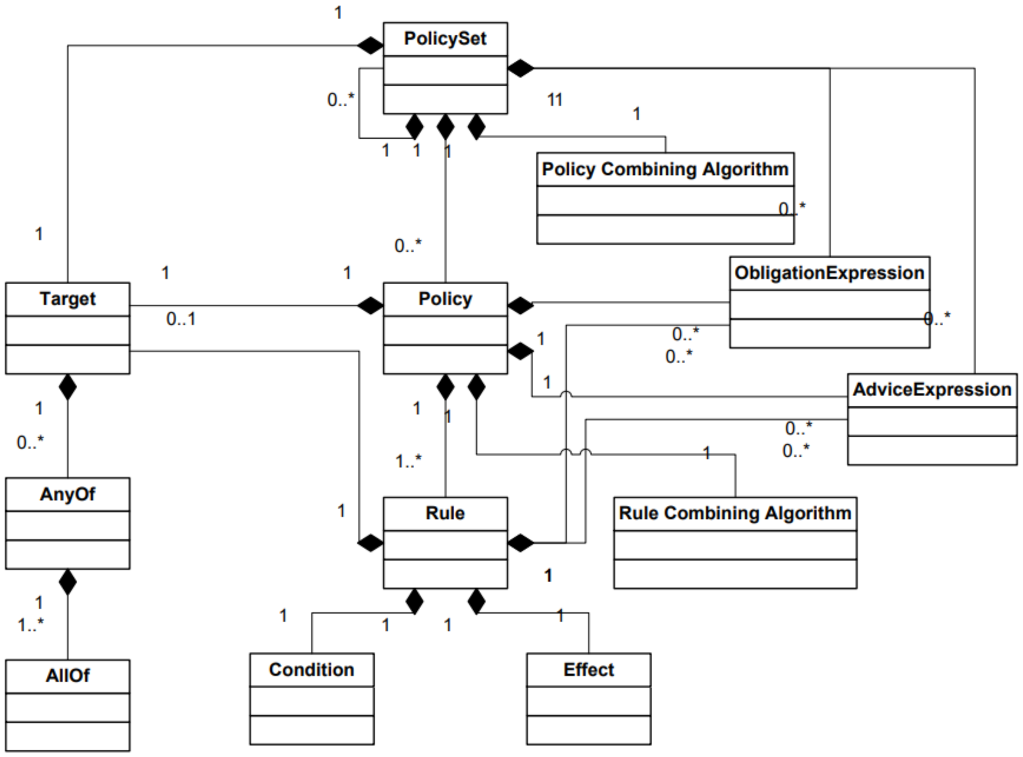


Figure 8: U-XACML Policy Meta-model

The U-XACML introduces also new elements, including <AttrUpdates>, <AttrUpdate>, <UpdateTime> and <UpdateExpression>. The <AttrUpdates> element also contains a collection of <AttrUpdate> elements, and each of them refers to a specific attribute and specifying a single update action. The <UpdateTime> statement specifies when an update action must be performed, i.e., *pre*-, *on*- and *post-updates*. The <UpdateExpression> element is a specific update function used to compute a new value of the attribute.

5.2 High-level Architecture of the ShareNet system

To enable all components of the CyberSANE framework to securely exchange information with external platforms and systems, the ShareNet component must provide an infrastructure for sharing CTI in the automated and secure manner. Furthermore, it must allow data-owners to define security constraints that must be satisfied before providing access, during access rights execution, and after usage of CTI records.

Figure 9 depict the high-level architecture of the ShareNet system that includes two main components, i.e., DSA Manager and the Information Sharing Infrastructure. The DSA Manager component of the C3ISP platform has been adapted to satisfy specific needs of the ShareNet infrastructure. This component enables data-owners to define security policies in the form of the human-readable DSA that are further represented in the U-XACML format. The DSA Manager includes five different elements described as following:

- **DSA Editor** provides an infrastructure for creating, editing and mapping security policies.
- **DSA Mapper** is in charge of modifying XML document returned by the DSA Editor and transform it to the XACML policy that can be further enforced by a specific engine.
- **DSA Store** is a repository used to store DSA.

- **DSA Store API** is an interface of the DSA Store that provides multiple functionalities for managing DSA.
- **DSA Manager Gateway** is an interface of the DSA Manager that provides a set of functionalities invoked by the DSA Adapter of the ISI component of the ShareNet system.

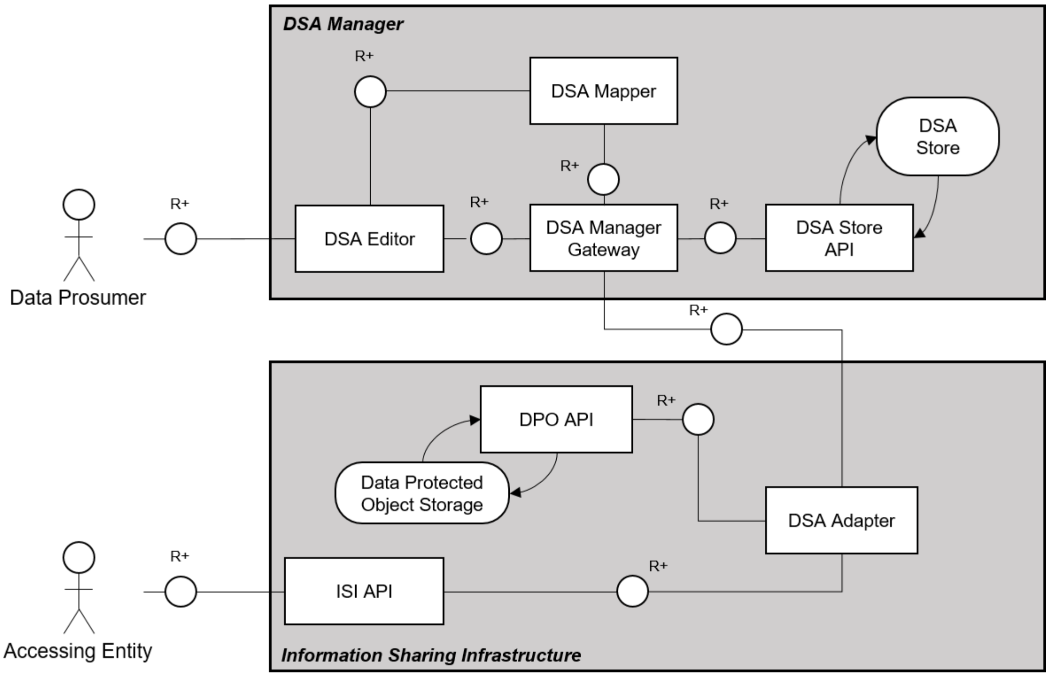


Figure 9: ShareNet high-level architecture

The second component of the ShareNet is ISI that provides multiple features for achieving secure CTI sharing. It includes four elements described as following:

- **ISI API** is an interface of the ISI component that is in charge of authenticating requests and communicating with DSA Adapter. It allows stakeholder to perform multiple operations on data they want to upload.
- **DSA Adapter** is an element used to evaluate security policies and enforce them whenever the execution of an operation (read, write, delete) is requested. Section 5.2.1 describes this element in a more detail.
- **Data Protected Object Storage (DPOS)** stores CTI uploaded by data-owners in a form of compressed bundle that includes CTI record, corresponding DSA ID, and relevant metadata (e.g., event type).
- **DPOS API** is the interface of the DPOS invoked by the DSA Adapter in order to store CTI records shared by stakeholders.

5.2.1 DSA Adapter

The DSA Adapter of the ShareNet system enables multiple security features used to protect sensitive information described in CTI records from potential misuse or its disclosure to third parties. As mentioned, the DSA Adapter interacts both with ISI API and the DPOS. However, the DSA Adapter is also in charge of communication with the DSA Manager, the Identity and Access Manager, and multiple sources that provide context information through attributes. Figure 10 depicts the DSA Adapter architecture that includes multiple components.

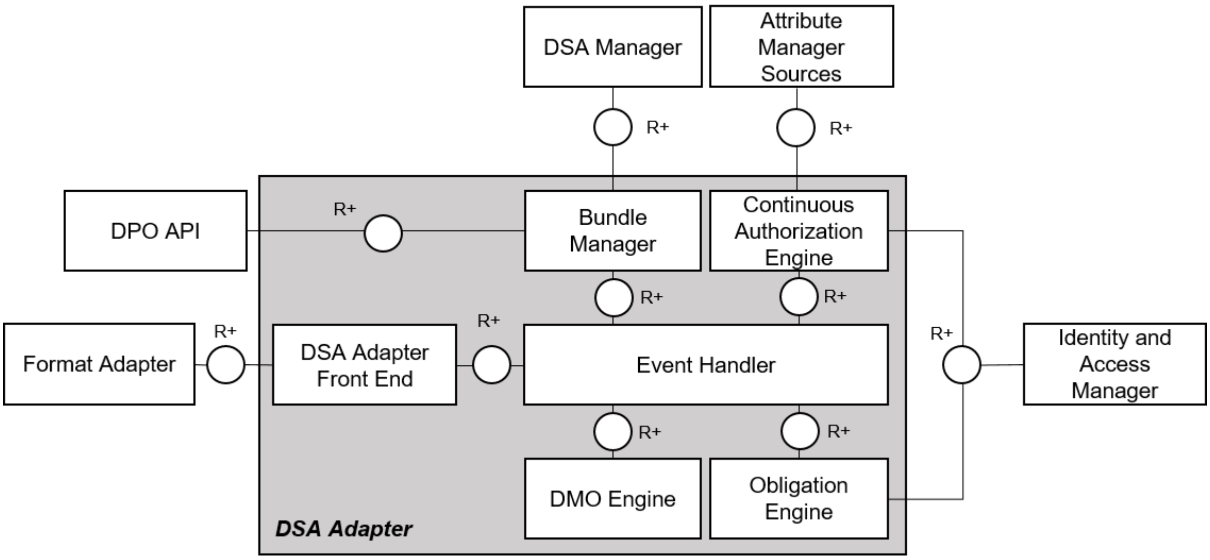


Figure 10: DSA Adapter of the Sharing Infrastructure

The DSA Adapter receives CTI records from the Format Adapter by using the DSA Adapter Front End. Data owners may request the Format Adapter to change the data format before storing that data on the platform. The main element of the DSA Adapter is the Event Handler

5.2.1.1 Continuous Enforcement of Security Policies for Information Sharing

The ShareNet platform enforces and evaluates security policies using the DSA Adapter component of the ISI subsystem. The DSA Adapter is in charge of evaluating the DSA policy paired with the CTI data and enforcing it when the execution of some operation on the data is requested (e.g. create, read, move, analytics execution, etc.). The UCS described in Section 5.1 was adapted to satisfy the security and privacy needs defined for the ShareNet and address challenges related to access and data usage control while sharing CTI. This adaptation result in the Continuous Authorization Engine (CAE) (see Figure 11).

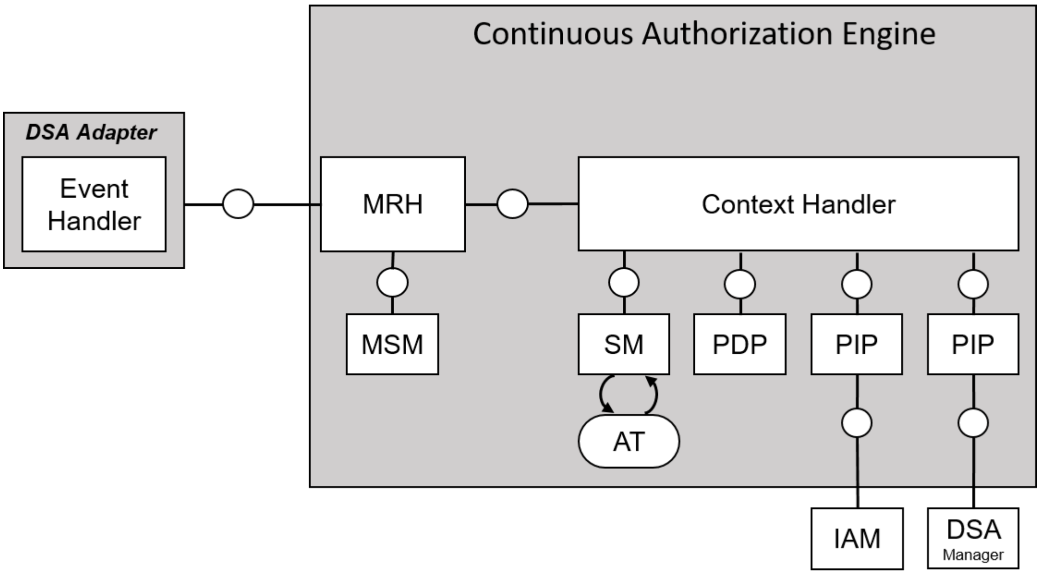


Figure 11: Continuous Authorization Engine

It supports traditional access control (i.e., the authorization process performed at request time) and continuous access control (an enhanced feature introduced by the UCON paradigm). The traditional access control phase, which is called preAuthorization in UCON, enforces the security policy when the system receives the access request in order to check whether the subject who requesting the access holds the right to perform the action on the object. The continuous authorization phase, which is called onAuthorization in UCON, checks that the right to perform the action continuously holds during the execution of the action itself in order to take a countermeasure as soon as this right expires. The countermeasure may vary from interrupting or suspending the execution of the action.

The CAE component of the ISI includes seven types of elements as following:

- **Context Handler (CH)** is the entry point of the Continuous Authorization Engine and it manages the protocol for communicating with the Event Handler. This protocol, which regulates the interactions between the Event Handler and the CH, is defined by a subset of the usage control actions: tryaccess, permitaccess, denyaccess, revokeaccess, and endaccess.
- **Session Manager (SM)** is the components responsible for keeping track of the ongoing usage sessions, i.e., of the access that are currently in progress, and it exploits an Access Table (AT) to store the meta-data regarding these sessions. It is the key component of the continuous authorization phase, and it represents an extension with respect to the XACML reference architecture.
- **Policy Decision Point (PDP)** is the component that evaluates security policies and produces the access decision. The PDP evaluates standard XACML policies because the usage control specific features are managed by the CH and by the SM.
- **Attribute Managers (AMs)** are modules, which manage attributes, allowing to retrieve and to update their current values for running the policy evaluation process. AMs could be local, i.e., they run on the same machine as the Continuous Authorization component or remote, i.e., they could run on external servers that could be even located in other domains run by third-parties.
- **Policy Information Points (PIPs)** are interfaces for interacting with Attribute Managers in order to perform the following 3 main operations on attributes: retrieve, subscribe/unsubscribe and update. In general, distinct Attribute Managers that provide different functionalities manage attributes required for the evaluation of a usage control policy and require different protocols for interacting with them.
- **Multi-Resources Handler (MRH)** enable the CAE to deal with access requests involving multiple resources. It accepts multiple resources access requests, invoked by the Event Handler of the DSA Adapter to perform the usage decision process. The protocol is defined by a subset of the usage control actions: tryaccess, permitaccess, denyaccess, revokeaccess, and endaccess, as for the CH component.
- **Multi Session Manager (MSM)** is a component that keeps track of a set of data to connect the usage session of each single CTI dataset with the multi resource access request it belongs to.

Since the UCS enables enforcement of the obligations, the ShareNet also supports execution of these operations. To enforce obligations, the ShareNet uses the Obligation Engine that is a module used for the execution of specific operations when certain conditions are met. Obligations are prescribed by the DSA associated to a specific dataset. Therefore, an obligation results in the execution of a particular action, when a specific event occurs. However, any action execution occurs only if a condition is verified.

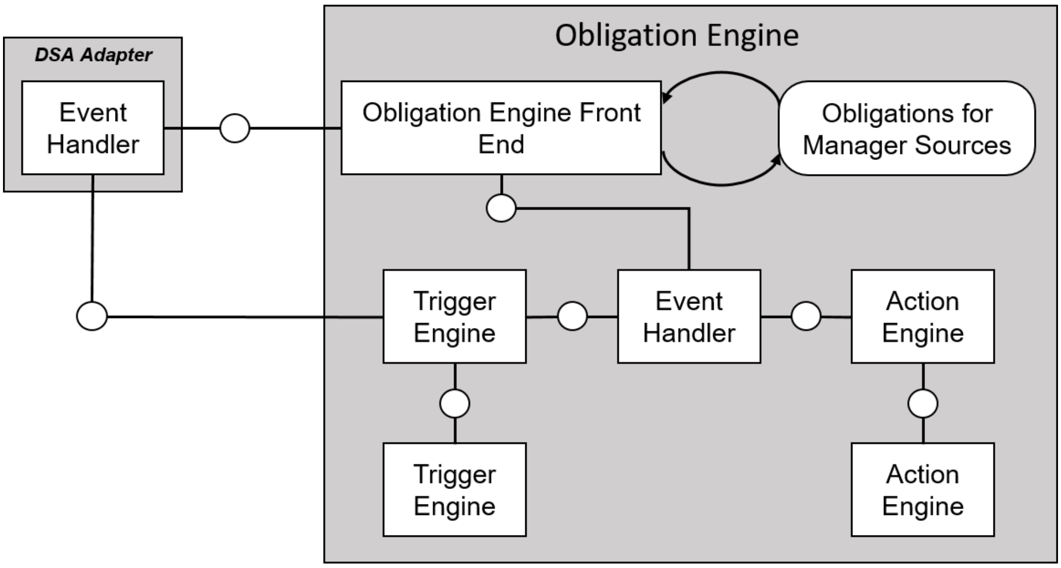


Figure 12: Obligation Engine Diagram

Figure 12 depicts the diagram of the Obligation Engine that consists of a number of modules being described:

- The **Trigger Engine**, which supports multiple types of triggers by implementing their specific business logic;
- The **Action Engine**, that, similarly to the trigger engine, is responsible for materialising the actions in obligations;
- The **Obligation Engine Front End** that interacts with the Event Handler of the DSA Adapter to filter and process the events relevant to its **Event Handler**.
- The **Obligation Engine Event Handler** which is in charge of processing the obligation definitions coming from the policies;
- The **Trigger** and **Action Engines** regulate the set of triggers and actions respectively. Both engines have methods to register new managed elements and to invoke them if requested by the Obligation Engine Front End.

The Obligation Engine may return a trigger that in turn may invoke a DMO Engine in order to execute specific operations on data to anonymize personal or confidential information (see Section 5.3).

5.2.1.2 Data format

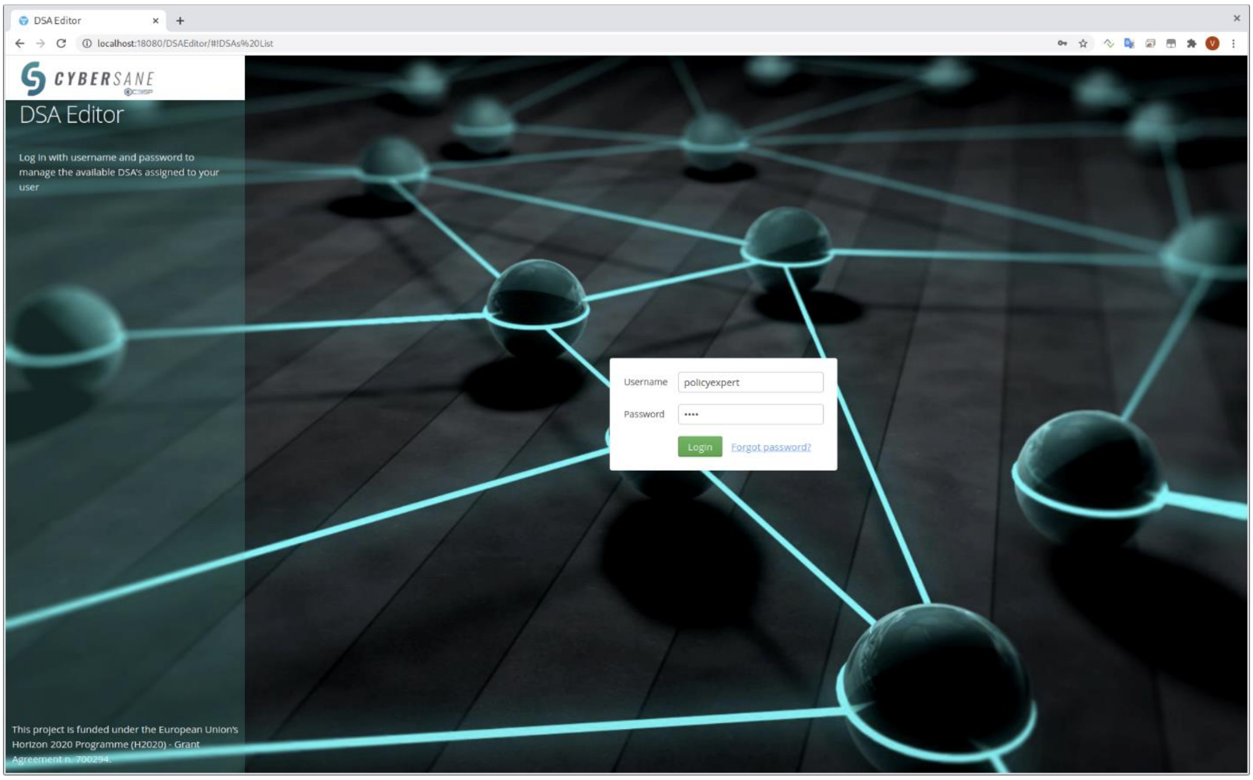
The C3ISP platform allows sharing information regardless specific data format. However, the platform was designed to collect, analyse and share CTI reported in a STIX format. Meanwhile, considering the wide adaptation of the MISP sharing platform that also defines its unique JSON-based data format, and due to the C3ISP framework flexibility, which allows operating with information reported in different formats, the further version of the C3ISP platform is expected to share and analyse information reported in the MISP data format following MISP taxonomies and galaxies.

Moreover, the C3ISP platform stores all information shared by data owners as Data-Protected Object (DPO), where each DPO contains uploaded data, related metadata, and security policy as the encrypted and compressed bundle. Thus, an access to a particular dataset is granted only to authorized entities, whose characteristics (e.g., role, affiliation, network type, etc.) represented through the corresponding attributes, satisfy security policies. Furthermore, the final decision also depends on context information (e.g., time, date). Hence, even if attributes of an entity requesting the access satisfy security policies, the C3ISP platform may deny access due to current values of attributes, which characterize context information. In this way, C3ISP ensures correct data access and data usage allowing access only to authorized entities also considering context information.

5.2.1.3 Data Sharing Agreements for CyberSANE

Nowadays, many organizations share their CTI using the MISP platform. The authors in (Wiem Tounsi, 2018) described advantages of MISP platform comparing to other initiatives. However, the main drawback is limited control over data access and its sharing. For example, once the data owner uploads the dataset to the MISP platform with the Amber Traffic Light Protocol (TLP)[21], the organization to which this information is shared can access it. However, the TLP does not allow security specialists to define advanced security limitations, i.e., specific role within the organization, location, network connection type, etc. Therefore, to overcome these limitations, the ShareNet system enables the enforcement of fine-grained security policies. This fact allows restricting access to a particular dataset or its usage if certain conditions are not satisfied. As mentioned, for this purpose, the ShareNet system uses the CAE that is a version of the UCS adapted and extended for a specific purpose.

Furthermore, the ShareNet system offers the DSA Manager that supports security specialists with policy management capabilities. With the available user-friendly interface, data-owners can define access and usage restrictions through the human-readable DSA that will be transformed to enforceable U-XACML policies.



Log in with username and password to manage the available DSA's assigned to your user

Username policyexpert

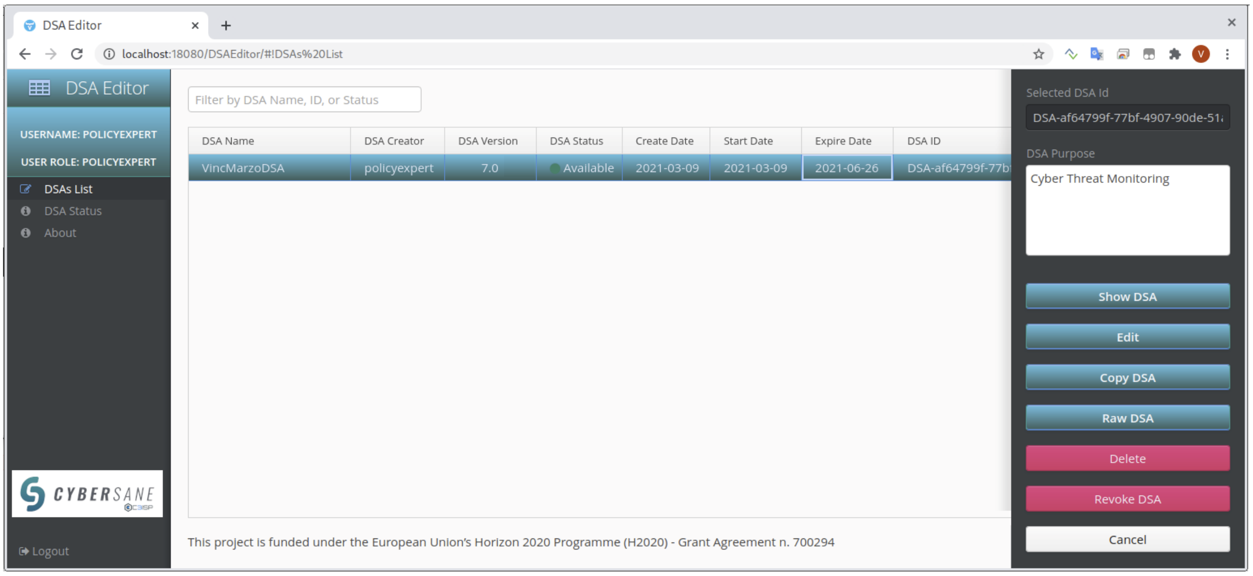
Password ••••

This project is funded under the European Union's Horizon 2020 Programme (H2020) - Grant Agreement n. 700294.

Figure 13: Login page of the DSA Editor

[21] https://www.circl.lu/pub/traffic-light-protocol/

Figure 13 depicts the first page of the DSA editor. An entity that want to create a policy must login into a system before its functionalities will be available.



USERNAME: POLICYEXPERT

USER ROLE: POLICYEXPERT

Filter by DSA Name, ID, or Status

DSA Name	DSA Creator	DSA Version	DSA Status	Create Date	Start Date	Expire Date	DSA ID
VincMarzoDSA	policyexpert	7.0	Available	2021-03-09	2021-03-09	2021-06-26	DSA-af64799f-77b

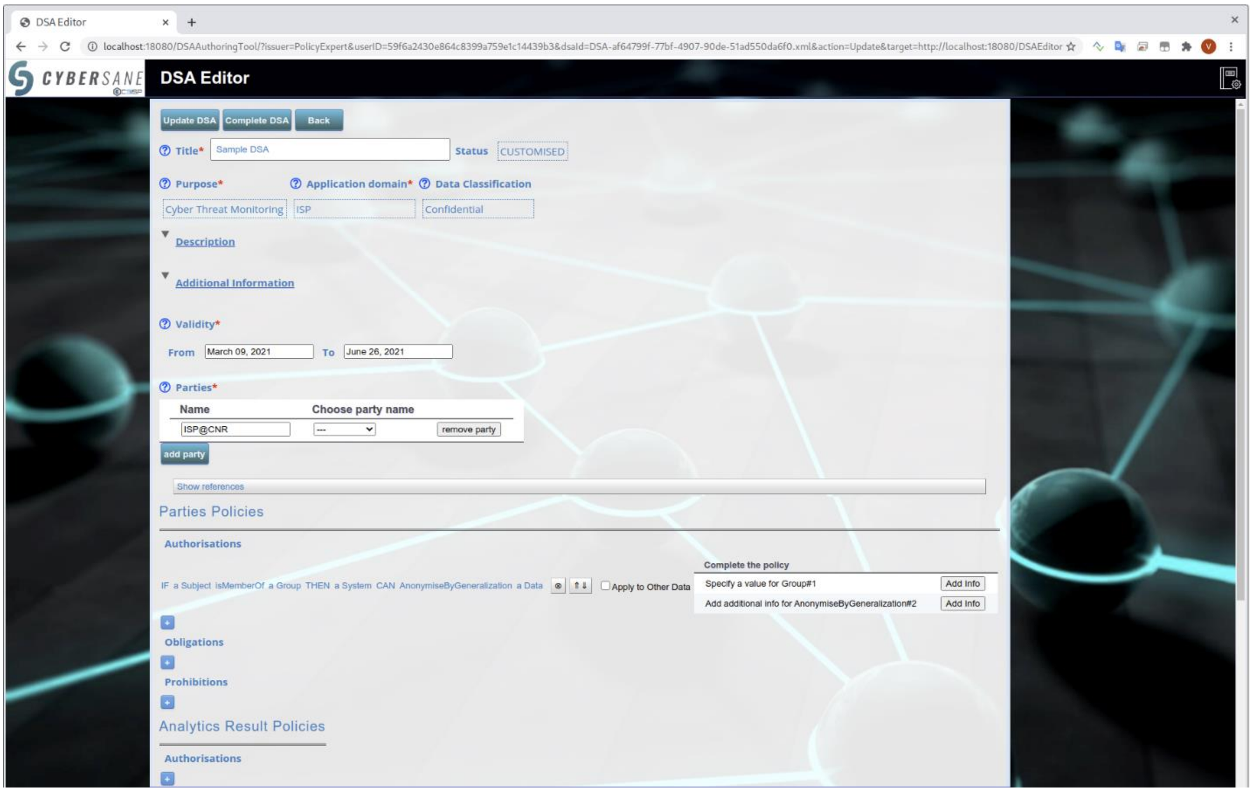
Selected DSA Id: DSA-af64799f-77bf-4907-90de-51a

DSA Purpose: Cyber Threat Monitoring

This project is funded under the European Union's Horizon 2020 Programme (H2020) - Grant Agreement n. 700294

Figure 14: First Page of the DSA Editor

Figure 14 provides a general view of the page with a list of available policies. An entity may review available policies, where each DSA has its own characteristics, including DSA name, ID, version, status that indicated whether the DSA is available to be mapped/attached to a dataset or not, date when the DSA was created, and validity period characterized by two dates. By using functional menu on the right side of the DSA Editor, entities may review, delete, revoke and edit each DSA.


DSA Editor
localhost:18080/DSAAuthoringTool/?issuer=PolicyExpert&userID=59f6a2430e864c8399a759e1c14439b3&dsaId=DSA-af64799f-77bf-4907-90de-51ad550da6f0.xml&action=Update&target=http://localhost:18080/DSAEditor
CYBERSANE
DSA Editor
Update DSA
Complete DSA
Back
Description
Additional Information
add party
remove party
Show references
Add Info
Add Info

Title*: Sample DSA   Status: CUSTOMISED

Purpose*: Cyber Threat Monitoring   Application domain*: ISP   Data Classification: Confidential

Validity*: From March 09, 2021 To June 26, 2021

Parties*

Name	Choose party name
ISP@CNR	---

Parties Policies

Authorisations

IF a Subject isMemberOf a Group THEN a System CAN AnonymiseByGeneralization a Data   □ Apply to Other Data

Complete the policy
- Specify a value for Group#1
- Add additional info for AnonymiseByGeneralization#2

Obligations

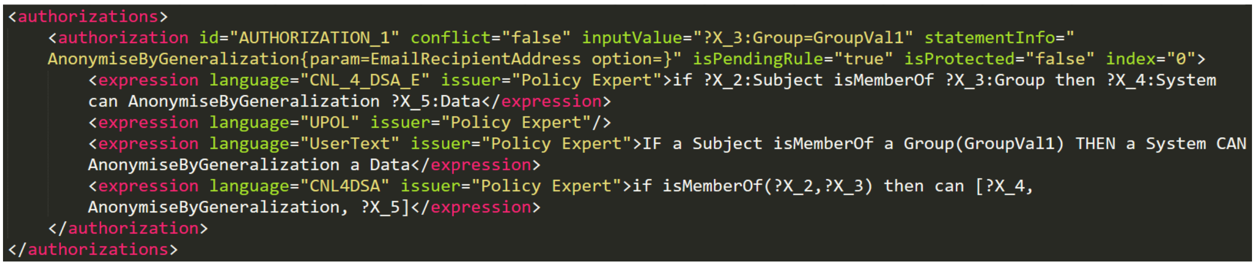
Prohibitions

Analytics Result Policies

Authorisations

Figure 15: DSA Editor - DSA Specification page

Figure 15 depicts a user-friendly GUI that enables stakeholders managing DSA. The DSA Editor allows entities to specify name and purpose of the DSA, specify additional information and provide description. Two dates specify the validity period. The date that indicates the beginning of the validity period may be different from the date when the DSA has been created. Additionally, stakeholders may specify one or multiple organizations to which the particular DSA is applied. This information further can be used to specify authorizations, obligations, and conditions of the policy. For example, the authorization presented on Figure 15 enables system to anonymize specific data by using the generalization method if a subject that requests access belongs to a particular group. Then, this DSA is transformed to the U-XACML policy format as depicted in Figure 16.



```
<authorizations>
    <authorization id="AUTHORIZATION_1" conflict="false" inputValue="?X_3:Group=GroupVal1" statementInfo="
    AnonymiseByGeneralization{param=EmailRecipientAddress option=}" isPendingRule="true" isProtected="false" index="0">
        <expression language="CNL_4_DSA_E" issuer="Policy Expert">if ?X_2:Subject isMemberOf ?X_3:Group then ?X_4:System
        can AnonymiseByGeneralization ?X_5:Data</expression>
        <expression language="UPOL" issuer="Policy Expert"/>
        <expression language="UserText" issuer="Policy Expert">IF a Subject isMemberOf a Group(GroupVal1) THEN a System CAN
        AnonymiseByGeneralization a Data</expression>
        <expression language="CNL4DSA" issuer="Policy Expert">if isMemberOf(?X_2,?X_3) then can [?X_4,
        AnonymiseByGeneralization, ?X_5]</expression>
    </authorization>
</authorizations>
```

Figure 16: U-XACML Authorization

Furthermore, additionally to the authorizations and obligations, data owners may specify prohibitions, which are specific elements of the U-XACML policies that describe different restrictions. For example, prohibitions may state that access is forbidden for an entity if this entity has particular characteristics, e.g., IP address, affiliation to a specific organization, role, etc.

5.2.1.4 Interaction between MISP and ShareNet

During several discussions, multiple approaches regarding the integration of a UCON paradigm into MISP platform have been investigated. One of them is to use external authentication tools that organizations can use together with platform to secure their MISP instances. Furthermore, organizations can use custom external modules for authorization to enhance security capabilities of the MISP instances.

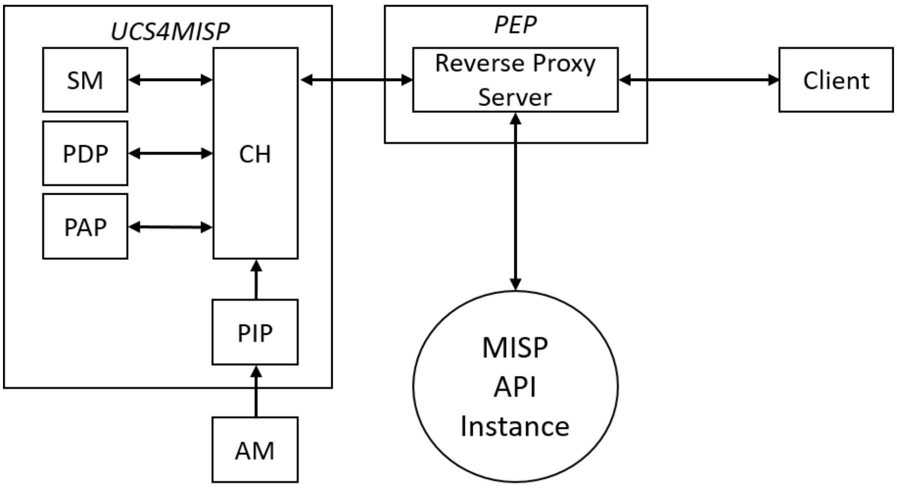


Figure 17: Usage Control with Reverse Proxy for MISP instance

To enable the continuous access control and to improve the security capabilities of the MISP instance, the UCON paradigm in a form of the UCS can be potentially integrated. This implementation will allow ongoing data usage control according to the XACML policies.

Figure 17 represents an architecture of possible implementation of the UCS within the MISP instance. The architecture includes standard UCS components as well as Client and MISP API instance elements. The *Reverse Proxy* server acts as the PEP that forwards the request from a client to the CH element of UCS. The UCS evaluates the request according to security policies stored in PAP. Once the client's request is evaluated positively, the SM element of UCS registers the session. However, if any additional attributes are required for the evaluation of the request, then the CH component retrieves those attributes from using one or multiple PIPs. In fact, the PIP element can also provide security policies, if the AM is implemented within the external Policy Data Base. For example, the Security Policies of the ShareNet system defined with the DSA Manager, can be retrieved from the DSA store. Hence, the PAP element can be omitted from this architecture. It is worth noting, that the system with this architecture is not capable to enforce security policies in other MISP instances.

Although the ShareNet system provides secure and privacy-aware information sharing, the need to share information with external MISP instance exists in order to enable advanced CTI sharing among different stakeholders. For this reason, the ShareNet component exploits MISP API platform to satisfy security and privacy needs for CTI sharing defined for the CyberSANE framework. In this case, the ShareNet platform stores sensitive information, ensuring that only authorized entities can access the requested dataset. Furthermore, depending on the request and other context information, ShareNet can invoke the PrivacyNet system to anonymize sensitive data. On the other hand, the MISP instance is used to share non-sensitive data with external MISP instances.

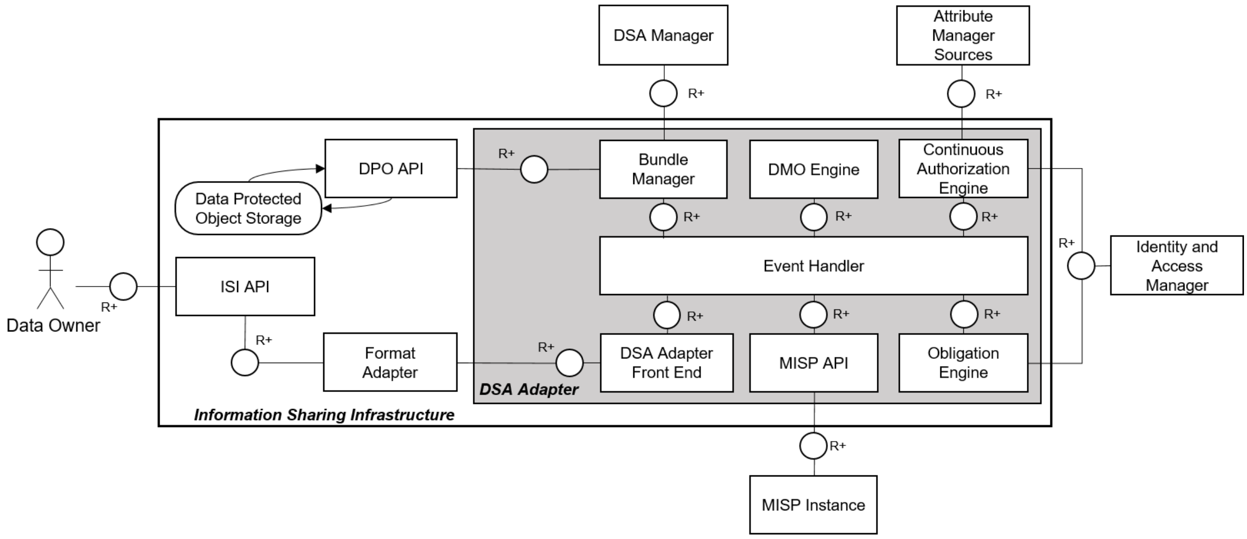


Figure 18: ISI Component (Extended)

Figure 18 depicts the ISI component of the ShareNet system extended to satisfy sharing requirements. Data owners may define security policies that will require system to execute privacy-preserving operations on the corresponding dataset before publishing it on the local MISP Instance. For this purpose, the DSA Adapter element of the ISI component, uses the CAE, described previously, and invokes the MISP API to export data to external MISP Instance. Hence, if a security policy associated with the particular dataset requires the platform to anonymize sensitive data, the DSA Adapter will invoke the PrivacyNet system by using the DMO Engine.

5.3 Trust and Reputation for controlling access and usage of CTI

The authors in (Albakri, 2018) have provided a comprehensive analysis of CTI reporting through the STIX standard and identified the threats of disclosing sensitive and identifying information. Since CTI may describe sensitive information of CI and CII, access to CTI records must be allowed not only to authorized entities, but also to whom a data owner trusts. For this purpose, an authorization mechanism alongside other characteristics must use trust and reputation values associated with a particular stakeholder to verify whether this entity is authorized to access and use CTI.

Trust in stakeholders that share CTI and trust in the CTI itself is crucial for deciding whether apply recommendations specified in CTI or not. Considering that in some cases, CTI may be used as a part of a malicious campaign against a specific organization, trust in the resource is crucial. Some of the existing approaches use stakeholders' reputation to define the trust in the resource, while other methods consider the quality of the CTI shared by the particular organization.

The flexibility of security policies used by the ShareNet system allows specifying different characteristics of entities through attributes. Apart from using attributes for defining the specific role of an entity, organizational domain, or nationality, attributes may be used to define the trust associated with the organization or the CTI produced by that organization. In this case, attributes that describe the trust or reputation level of a specific organization will be used to evaluate the access control policies. Different taxonomies can be potentially adapted to perform an automatic evaluation of the quality of shared CTI. The system may assign computed value to the profile of a particular stakeholder, reflecting its reputation level. In some cases, it can also stimulate organizations to produce highly-qualified CTI and share it timely as possible, thus acting most transparently. Furthermore, organizations that share CTI may define the lowest level of a stakeholder’s reputation and use this parameter in security policies. For example, stakeholders with low reputation levels will not be able to access information to which the aforementioned security policies are attached. Hence, the assigned trust value may affect the final decision-making, thus protecting CTI from unwilling usage.

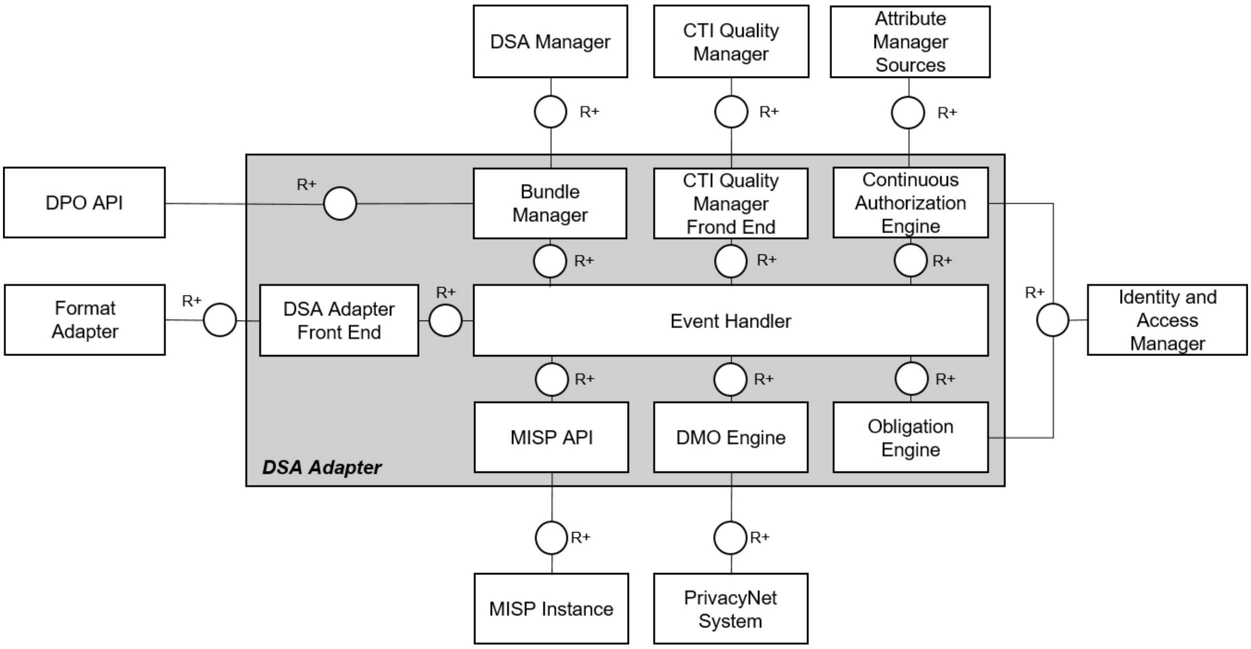


Figure 19: DSA Adapter with external modules

The approach proposed in (Schaberreiter, 2019) enables to assess the trust based on the multiple parameters of shared STIX content. Hence, the need for a specific component exists to evaluate the quality of the STIX records shared by entities. For this purpose, to enable evaluation of CTI records quality, the ISI component of the ShareNet system has been extended to handle this operation. Figure 19 depicts the DSA Adapter extended with the CTI Quality Manager, which is in charge of evaluating multiple parameters of the CTI records.

Additionally to the CTI Quality Manager, Figure 19 depicts connections both to the MISP Instance and PrivacyNet System exploiting their APIs. Hence, once the data owner uploaded her data to the ShareNET system, the CTI Quality Manager will evaluate the quality of the provided dataset according to multiple parameters and update the trust value associated with the data owner. In this manner, the updated trust level may affect the access decision for other datasets uploaded by different stakeholders.

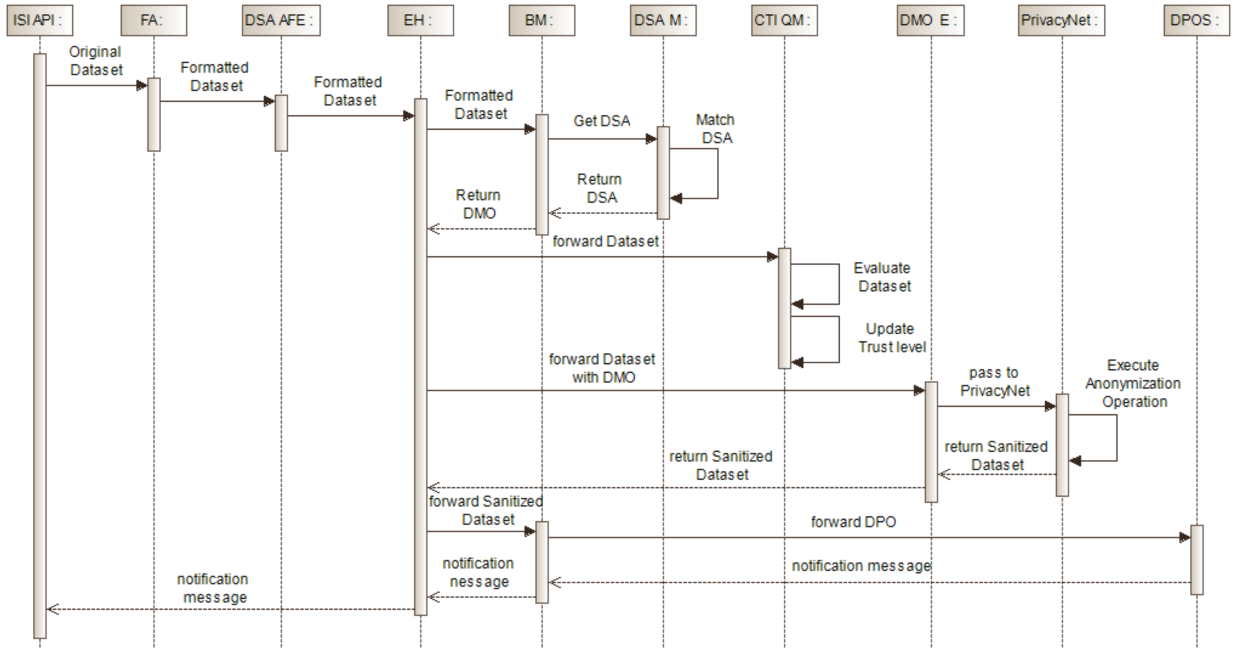


Figure 20: Data Flow Sequence Diagram

Figure 20 depicts the workflow diagram. Data Prosumers can upload their data by using ISI API. Additionally, if data owners have specified the need to format their data to a STIX data model, the designed format-adapter toolbox will initiate the operation. Once the toolbox formats the input dataset to the STIX standard it forwards the formatted dataset to the DSA adapter invoking DSA Adapter Frontend (DSA AFE) in order to create a Data Protected Object (DPO). Each DPO is the encrypted and compressed bundle that contains uploaded data, related metadata, and the ID of the corresponding security policy defined by the data-owner.

The core element of the DSA Adapter is an Event Handler (EH) that interacts with other components. The EH element invokes the Bundle Manager (BM) to create the DPO. This element has been designed for both packing and unpacking operations. During the packing phase, the BM is used for creating a bundle by retrieving a DSA from the DSA Manager and pairing the DSA with the uploaded dataset. On the contrary, in the unpacking phase, the DSA Adapter uses BM to extract the DSA from the bundle and send extracted DSA to the EH for the policy evaluation. Additionally, the BM is used to retrieve the CTI, if the DSA Policies evaluation results in the permit.

To evaluate the quality of the uploaded dataset, we have designed the CTI Quality Manager, referred to as CTI QM. Hence, once the dataset is uploaded to the system, the EH will invoke the CTI QM by forwarding the corresponding dataset. As the next step, the CTI QM assesses the uploaded dataset according to multiple parameters defined in Table 3. Then, after the evaluation of the CTI quality, the CTI QM will update the trust level associated with the data owner. Thus, this value will be used for the evaluation process of other policies.

We consider that the security constraints defined with the DSA require a platform to execute one of the DMO operations once data has been uploaded to the system. Therefore, the EH element of the DSA Adapter will invoke the DMO Engine, depicted as DMO E, by forwarding the encoded dataset together with the required operation. In turn, the DMO Engine (depicted in Figure 20 as DMO E) invokes the PrivacyNet component of the CyberSANE platform exploiting available PrivacyNet API. The PrivacyNet component executes the requested operation on the encoded dataset and returns its sanitized version to the DMO Engine of the DSA Adapter. Once the Event Handler receives the sanitized version of the dataset it invokes the BM for packing data and store it in the Data Protected Object Storage (DPOS). Finally, the notification message is produced informing the data owner about successful operations. Thus, the platform will provide access only to the sanitized version of the dataset if security policies have been satisfied. Otherwise, the final decision for providing access will result in denial.

5.3.1 Trust and reputation for access control decision

Since trust is an essential characteristic that may be used to define whether the entity can access information or not, it is necessary to consider this aspect during policy evaluation. To achieve this, we have provided the extended version of the CAE element of the DSA Adapter. Figure 21 depicts an extended version of the CAE of ISI as a part of the ShareNet system. The extended version of the CAE interacts with two additional components. The first component is a Trust Manager (TM) that is in charge of evaluating trust of a stakeholder based on different aspects (e.g., information quality) described in previous sections. On the other hand, the second element is Reputation Manager (RM) that supports CAE with an attribute that characterize a stakeholder with its reputation value. The TM engine retrieves information directly from the CTI QM that assesses CTI records uploaded by stakeholders. On the other hand, the RM engine may also use information provided by the CTI QM after assessing uploaded CTI.

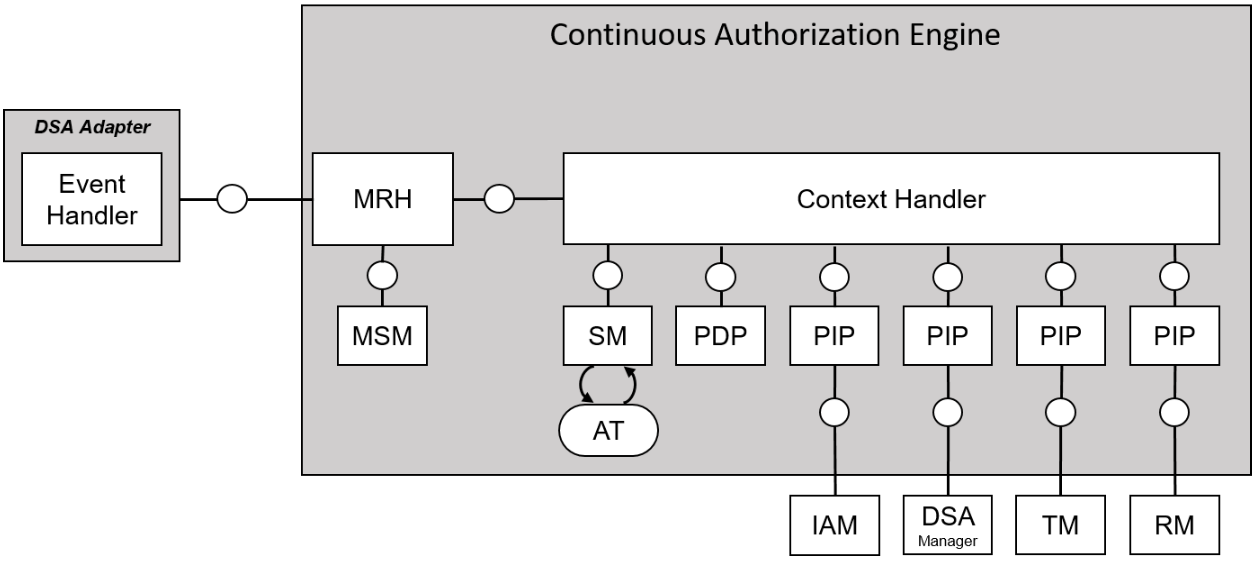


Figure 21 : Continuous Authorization Engine (extended)

However, it also provides information regarding the reputation of a particular entity. Stakeholders may evaluate the reputation of each other according to multiple parameters.

5.3.1.1 CTI Quality Manager – Trust Manager

The CTI Quality Manager (CTI QM) is a module that is in charge of evaluating the quality of CTI records shared by stakeholders. As mentioned, the assessment is done according to multiple parameters describe in Table 3. Once the data owner uploaded dataset to the ShareNet component, the EH element of the DSA Adapter will invoke the CTI QM to assess this dataset. The CTI QM module provides a computation result of the CTI record quality. In this case, the obtained value can be used for further operations related to the evaluation of security policies. Figure 22 depict the architecture of the CTI QM module.

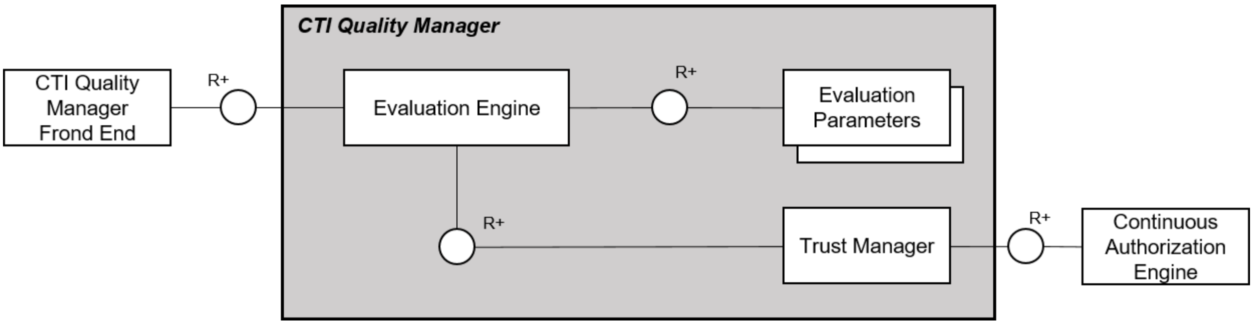


Figure 22 : CTI Quality Manager Architecture

The CTI QM constitutes of three main components as Evaluation Engine that assesses each CTI record according to Evaluation Parameters, and Trust Manager (TM), which is in charge of storing a trust value associated with a particular stakeholder in a form of key-value pairs, where key specifies an ID of the stakeholder. The TM acts as the Attribute Manager for the CAE that retrieves the trust level associated with the stakeholder in order to evaluate the request against policies.

5.3.1.2 Specifying trust in Usage Control Policies

As mentioned, the CAE evaluates access control policies reported in the U-XACML language.

A Rule object of the XACML policy

```
<Rule RuleId= "urn:oasis:names:tc:xacml:3.0:example:Permit-If-Trust" Effect="Permit">
  <Description>
    Any subject with trust rank equal or higher than 0.7 can access data
  </Description>
  <Condition DecisionTime="ongoing">
    <Apply FunctionId="urn:oasis:names:tc:xacml:1.0:function:integer-less-than" >
      <Apply FunctionId="urn:oasis:names:tc:xacml:1.0:function:integer-one-and-only" >
        <AttributeDesignator
          AttributeId="SubjectTrustRank"
          Category="urn:oasis:names:tc:xacml:1.0:subject-category:access-subject"
          DataType="http://www.w3.org/2001/XMLSchema#integer"
          MustBePresent="true" >
        </AttributeDesignator>
      </Apply>
      <AttributeValue DataType="http://www.w3.org/2001/XMLSchema#integer">0.7</AttributeValue>
    </Apply>
  </Condition>
</Rule>
```

Table 4 : XACML Rule object with the condition element

The flexibility of the XACML standard allows to define specific attributes of subjects, objects and environment and create fine-grained policies. Table 4 provides one of the rules used in the XACML policies, which are deployed within the CAE for evaluation of requests from stakeholders.

By using the DSA Editor described in Section 5.2.1.3, stakeholders may specify security constraints applied to their data and which must be satisfied in order to access information. For example, the security policy rule object (see Table 4) allows access to a dataset only to subjects with the trust level equal or higher than 0.7. Otherwise, the CAE will deny access even if other attributes satisfy the corresponding security policy. In this way, the quality of CTI provided by a stakeholder will directly affect the decision regarding the access to threat-related information reported by other entities. Hence, this fact will stimulate each entity to provide qualitative CTI as timely as possible.

Chapter 6 Conclusions

This deliverable has roundly described both the conventional and latest advances in the CTI domain that could be of potential use in CyberSANE. The main goal of this document was to identify and provide the most prominent strategies and techniques which could be adopted for enhancing consortium’s existing tools. Therefore, we focused into outlining the essential CTI sharing platforms, the most widely used standardizations and agile platforms, as well as the newest research works regarding trust management approaches. All of the aforementioned standards, platforms, works, and methodologies, shall be taken into account in the upcoming tasks of WP6 in order to develop a secure and trusted communication mechanism for CyberSANE’s CIIs. Furthermore, this document describes a high-level architecture of the ShareNet system and how it communicates with other systems of the CyberSANE platform.

Chapter 7 List of Abbreviations

Abbreviation	Translation
ABAC	Attribute-Based Access Control
AM	Attribute Manager
B2B	Business-to-Business
CAPEC	Common Attack Pattern Enumeration and Classification
CERT(s)	Computer Emergency Response Team(s)
CH	Context Handler
CI(s)	Critical Infrastructure(s)
CII(s)	Critical Information Infrastructure(s)
CIO	Chief Information Officer
CISO	Chief Information Security Officer
CPNI	Centre for the Protection of National Infrastructure
CSIRT(s)	Computer Security Incident Response Team(s)
CTA	Cyber Threat Alliance
CTI	Cyber Threat Intelligence
CVE	Common Vulnerabilities and Exposures

CVSS	Common Vulnerability Scoring System
CWSS	Common Weakness Scoring System
CybOX	Cyber Observable eXpression
CPS	Cyber-Physical Systems
DOLCE	Descriptive Ontology for Linguistic and Cognitive Engineering
DPO	Data Protected Object
GDPR	General Data Protection Regulation
HUFO	Human Factors Trust Ontology
IOCs	Indicators of Compromise
IoT	Internet-of-Things
IR	Incident Response
ISP(s)	Internet Service Provider(s)
JSON	JavaScript Object Notation
MAEC	Malware Attribute Enumeration and Characterization
MISP	Malware Information Sharing Platform
NIST	National Institute of Standards and Technology
NOC	Network Operations Centre
NVD	National Vulnerability Database

OrBAC	Organization Based Access Control
P2P	Peer-to-Peer
PAP	Policy Administration Point
PDP	Policy Decision Point
PEP	Policy Enforcement Point
PIP	Policy Information Point
SCADA	Supervisory Control And Data Acquisition
SCAP	Security Content Automation Protocol
SM	Session Manager
SOC	Security Operation Centre
STIX	Structured Threat Information eXpression
TAL	Threat Agent Library
TAXII	Trusted Automated eXchange of Intelligence Information
TTPs	Tactics, Techniques, and Procedures
UCON	Usage Control
UCS	Usage Control System
UFO	Unified Foundational Ontology
UUID(s)	Universally Unique IDentifier(s)

XACML	Extensible Access Control Markup Language

Chapter 8 Bibliography

(C3ISP), C. a. C. I. S. a. A. f. C. P., 2019. *C3ISP Final Reference Architecture,* s.l.: s.n.

Aali, N., Baina, A. & Echabbi, L., 2015. *Trust integration in collaborative access control model for Critical Infrastructures.* Rabat, IEEE, pp. 1-6.

Aberer, K. & Despotovic, Z., 2001. *Managing Trust in a Peer-2-Peer Information System.* Atlanta, Association for Computing Machinery, p. 310–317.

Abimbola, A., 2007. Information security incident response. *Network Security, Elsevier*, pp. 10-13.

Abou El Kalam, A., Deswarte, Y., Baïna, A. & Kaâniche, M., 2009. PolyOrBAC: A security framework for Critical Infrastructures. *International Journal of Critical Infrastructure Protection,* 2(4), pp. 154-169.

Abu, M., Selamat, S., Ariffin, A. & Yusof, R., 2018. Cyber Threat Intelligence - Issue and Challenges. *Indonesian Journal of Electrical Engineering and Computer Science,* 10(1), pp. 371-379.

Afzaliseresht, N. et al., 2020. From logs to Stories: Human-Centred Data Mining for Cyber Threat Intelligence. *IEEE Access,* Volume 8, pp. 19089-19099.

Albakri, A. a. B. E. a. D. L. R., 2018. Risks of sharing cyber incident information. *Proceedings of the 13th International Conference on Availability, Reliability and Security*, pp. 1-10.

Aliaksandr Lazouski, G. M. F. M. a. P. M., 2012. Usage control in cloud systems. *In 2012 International Conference for Internet Technology and Secured Transactions, IEEE*, pp. 202-207.

Al-Ibrahim, O. a. M. A. a. K. C. a. K. K. a. N. L., 2017. Beyond free riding: quality of indicators for assessing participation in information sharing for threat intelligence.

Almeroth, M. T. a. K. C., 2012. A taxonomy to express open challenges in trust and reputation systems. *Journal of Communications,* pp. 538-551.

Amaral, G., Sales, T., Guizzardi, G. & Porello, D., 2019. Towards a Reference Ontology of Trust. In: H. Panetto, et al. eds. *On the Move to Meaningful Internet Systems: OTM 2019 Conferences. OTM 2019. Lecture Notes in Computer Science, vol 11877.* Rhodes: Springer, pp. 3-21.

Arachchilage, N. A. G. a. N. C. a. M. A., 2013. A taxonomy for securely sharing information among others in a trust domain. *8th International Conference for Internet Technology and Secured Transactions (ICITST-2013)*, pp. 296-304.

Arenas, E., 2017. *Cyber Threat Intelligence Information Sharing,* Queensland, Australia: School of Engineering and Technology, CQUniversity.

Baina, A., Kalam, A., Deswarte, Y. & Kaaniche, M., 2008. Collaborative Access Control For Critical Infrastructures. In: M. Papa & S. Shenoi, eds. *Critical Infrastructure Protection II. ICCIP 2008. The International Federation for Information Processing, vol 290.* Arlington: Springer, pp. 189-201.

Barnum, S., 2014. *Standardizing Cyber Threat Intelligence Information with the Structured Threat Information eXpression (STIX™),* s.l.: The MITRE Corporation.

Blasch, E., 2014. Trust metrics in information fusion. *International Society for Optics and Photonics,* Volume 9119, p. 91190L.

Blaze, M., Feigenbaum, J. & Lacy, J., 1996. *Decentralized trust management.* Oakland, IEEE, pp. 164-173.

Booth, H., Rike, D. & Witte, G., 2013. *The National Vulnerability Database (NVD): Overview,* s.l.: National Institute of Standards and Technology (NIST).

Botega, L. C. J. O. d. S. F. R. J. C. S. C. M. R. d. C. V. P. d. A. N. a. R. B. d. A., 2017. Methodology for data and information quality assessment in the context of emergency situational awareness. *Universal Access in the Information Society, Springer*, pp. 889-902.

Buchegger, S. & Le Boudec, J., 2003. *A robust reputation system for mobile ad-hoc networks.* Boston, Second Workshop on Economics of P2P Systems.

Cardoso, R. & Freire, M., 2005. Security Vulnerabilities and Exposures in Internet Systems and Services. In: *Encyclopedia of Multimedia Technology and Networking.* s.l.:IGI Global, pp. 910-916.

Casey, E., Back, G. & Barnum, S., 2015. Leveraging CybOX™ to standardize representation and exchange of digital forensic information. *Digital Investigation,* 12(1), pp. S102-S110.

Casey, E. et al., 2017. Advancing coordinated cyber-investigations and tool interoperability using a community developed specification language. *Digital Investigation,* Volume 22, pp. 14-45.

Chantzios, T. et al., 2019. The Quest for the Appropriate Cyber-threat Intelligence Sharing Platform. *DATA,* pp. 369-376.

Chen, J. et al., 2019. Trust architecture and reputation evaluation for internet of things. *Journal of Ambient Intelligence and Humanized Computing,* 10(8), pp. 3099-3107.

Chismon, D. & Ruks, M., 2015. *Threat Intelligence: Collecting, Analysing, Evaluating,* s.l.: MWR InfoSecurity Ltd.

Connolly, J., Davidson, M. & Schmidt, C., 2014. *The Trusted Automated eXchange of Indicator Information (TAXII™),* s.l.: The MITRE Corporation.

Cope, A., 2007. *Machine tags - Flickr API.* [Online] Available at: https://www.flickr.com/groups/api/discuss/72157594497877875/ [Accessed 13 5 2020].

Cuppens, F., Cuppens-Boulahia, N. & Coma, C., 2006. Virtual Private Organizations to Manage Security Policy Interoperability. In: A. Bagchi & V. Atluri, eds. *Information Systems Security. ICISS 2006. Lecture Notes in Computer Science, vol 4332.* Kolkata: Springer, pp. 101-115.

Dalziel, H., 2014. *How to Define and Build an Effective Cyber Threat Intelligence Capability.* Waltham: Syngress.

Daoud, W. et al., 2019. TACRM: trust access control and resource management mechanism in fog computing. *Human-centric Computing and Information Sciences,* 9(1), p. 28.

Das, S., Kant, K. & Zhang, N., 2012. *Handbook on Securing Cyber-Physical Critical Infrastructure.* s.l.:Elsevier.

Dionysiou, I., Frincke, D., Bakken, D. & Hauser, C., 2008. An Approach to Trust Management Challenges for Critical Infrastructures. In: J. Lopez & B. Hämmerli, eds. *Critical Information Infrastructures Security. CRITIS 2007. Lecture Notes in Computer Science, vol 5141.* Rome: Springer, pp. 173-184.

E. Yalcinkaya, A. M. a. M. O., 2017. Application of Attribute Based Access Control Model for Industrial Control Systems. *International Journal of Computer Network and Information Security,* 9(2).

Enrico Carniani, D. D. A. L. F. M. a. P. M., 2016. Usage control on cloud systems. *Future Generation Computer Systems 63*, pp. 37-55.

European Commission CORDIS, 2016. *Collaborative and Confidential Information Sharing and Analysis for Cyber Protection.* [Online] Available at: https://cordis.europa.eu/project/id/700294 [Accessed 6 6 2020].

Faloutsos, M., Faloutsos, P. & Faloutsos, C., 1999. On Power-Law Relationships of the Internet Topology. *Proceedings of the Conference on Applications, Technologies, Architectures, and Protocols for Computer Communication,* 29(4), pp. 251-262.

Fan, W. et al., 2019. *Enabling Privacy-Preserving Sharing of Cyber Threat Information in the Cloud.* Paris, IEEE, pp. 74-80.

FIRST, 2019. *Common Vulnerability Scoring System version 3.1 - Specification Document - Revision 1.* [Online] Available at: https://www.first.org/cvss/v3-1/cvss-v31-specification_r1.pdf [Accessed 22 5 2020].

Fisk, G. et al., 2015. *Privacy Principles for Sharing Cyber Security Data.* San Jose, IEEE.

Forrester Research, 2018. *The Forrester New Wave™: External Threat Intelligence Services, Q3 2018,* s.l.: Forrester Research.

Friedman, J. & Bouchard, M., 2015. *Definitive Guide to Cyber Threat Intelligence: Using Knowledge about Adversaries to Win the War against Targeted Attacks,* s.l.: CyberEdge Press.

G. Baldi, Y. D.-T. T. D. F. M. C. M. P. M. O. O. a. A. S., 2020. Session-dependent Usage Control for Big Data. *Journal of Internet Services and Information Security,* 10(3), pp. 76--92.

Garcia-Molina, S. M. a. H., 2006. Taxonomy of trust: Categorizing P2P reputation systems. *Computer Networks, Elsevier*, pp. 472-484.

Gong, N., 2019. Barriers to Adopting Interoperability Standards for Cyber Threat Intelligence Sharing: An Exploratory Study. *Intelligent Computing. SAI 2018. Advances in Intelligent Systems and Computing,* Volume 857, pp. 666-684.

Gonzalez-Gil, P., Skarmeta, A. & Martinez, J., 2019. *Towards an Ontology for IoT Context-Based Security Evaluation.* Aarhus, IEEE, pp. 1-6.

Gray, E. a. C. Y. a. J. C., 2003. Initial investigation into cross-context trust and risk assessment. *IASTED International Conference on Communication, Network, and Information Security*, pp. 56-61.

Griffioen, H., Booij, T. & Doerr, C., 2020. Quality Evaluation of Cyber Threat Intelligence Feeds. *Applied Cryptography and Network Security. ACNS 2020. Lecture Notes in Computer Science,* Volume 12147, pp. 277-296.

Griffor, E., Greer, C., Wollman, . D. & Burns, M., 2017. *Framework for Cyber-Physical Systems: Volume 1, Overview - Special Publication (NIST SP) - 1500-201,* s.l.: National Institute of Standards and Technology (NIST).

Guarino, N., 1998. *Formal ontology in information systems.* Trento, IOS press.

Guizzardi, G., de Almeida Falbo, R. & Guizzardi, R., 2008. *Grounding Software Domain Ontologies in the Unified Foundational Ontology (UFO): The case of the ODE Software Process Ontology.* Pernambuco, Curran Associates, Inc., pp. 127-140.

Hallingstad, G. & Dandurand, L., 2011. *CIS Security (including Cyber Defence) Capability Breakdown.* NC3A, The Hague, Netherlands, NATO Consultation, Command and Control Agency Reference Document RD-3060.

Hongwei Zhu, R. Y. W., 2009. Information quality framework for verifiable intelligence products. *Data Engineering*, pp. 315-333.

Huang, J. & Fox, M., 2006. *An Ontology of Trust: Formal Semantics and Transitivity.* Fredericton, Association for Computing Machinery, pp. 259-270.

IBM Security, 2014. *IBM X-Force Exchange.* [Online] Available at: https://exchange.xforce.ibmcloud.com/ [Accessed 27 5 2020].

J. Park, a. R. S., 2004. The UCONABC usage control model. *ACM Transactions on Information and System Security,* 7(1), pp. 128-174..

Johnson, C. et al., 2016. *Guide to Cyber Threat (No. NIST Special Publication 800-150),* s.l.: National Institute of Standards and Technology (NIST).

Kalam, A. et al., 2003. *Organization based access control.* Lake Como, IEEE.

Kamvar, S., Schlosser, M. & Garcia-Molina, H., 2003. *The Eigentrust Algorithm for Reputation Management in P2P Networks.* Budapest, Association for Computing Machinery, pp. 640-651.

Kent, S., 1998. Evaluating certification authority security. In: *1998 IEEE Aerospace Conference Proceedings (Cat. No.98TH8339).* Snowmass at Aspen: IEEE, pp. 319-327.

L. Qiang, J. Z. Y. Z. L. B. W. X. Z. Y., 2018. A quality evaluation method of cyber threat intelligence in user perspective. *2018 17th IEEE International Conference On Trust, Security And Privacy In Computing And Communications/12th IEEE International Conference On Big Data Science And Engineering (TrustCom/BigDataSE)*, pp. 269-276.

L. Wang, D. W. a. S. J., 2004. *A logic-based framework for attribute based access control.* s.l., ACM workshop on Formal methods in security engineering.

Lamba, A., 2020. *A Through Analysis on Protecting Cyber Threats and Attacks on CPS Embedded Subsystems.* [Online] Available at: https://ssrn.com/abstract=3517474 [Accessed 28 5 2020].

Lee, S. & Shon, T., 2017. *Open source intelligence base cyber threat inspection framework for critical infrastructures.* San Francisco, IEEE.

Li Cai, Y. Z., 2015. The challenges of data quality and data quality assessment in the big data era. *Data science journal, Ubiquity Press,* Volume 14.

Liao, X. a. Y. K. a. W. X. a. L. Z. a. X. L. a. B. R., 2016. Acing the ioc game: Toward automatic discovery and analysis of open-source cyber threat intelligence. *Proceedings of the 2016 ACM SIGSAC Conference on Computer and Communications Security*, pp. 755-766.

Li, W. et al., 2011. *CARE-CPS: Context-Aware Trust Evaluation for Wireless Networks in Cyber-Physical System Using Policies.* Pisa, IEEE, pp. 171-172.

Li, W. et al., 2011. Managing and Securing Critical Infrastructure - A Semantic Policy and Trust Driven Approach. In: S. Das, K. Kant & N. Zhang, eds. *Handbook on Securing Cyber-Physical Critical Infrastructure: Foundations and Challenges.* Baltimore: Morgan Kaufmann, pp. 551-572.

Martin, B. & Christey, S., 2014. *Common Weakness Scoring System (CWSS™).* [Online] Available at: https://cwe.mitre.org/cwss/cwss_v1.0.1.html [Accessed 28 5 2020].

Masolo, C. et al., 2002. *The WonderWeb Library of Foundational Ontologies. WonderWeb Deliverable D17.* [Online] Available at: http://wonderweb.semanticweb.org

Maurizio Colombo, A. L. F. M. a. P. M., 2010. A proposal on enhancing XACML with continuous usage control features. *In Grids, P2P and Services Computing, Springer, Boston, MA*, pp. 133-146.

Mavroeidis, V. & Bromander, S., 2017. *Cyber Threat Intelligence Model: An Evaluation of Taxonomies, Sharing Standards, and Ontologies within Cyber Threat Intelligence.* Athens, IEEE, pp. 91-98.

Meier, R. a. S. C. a. G. D. a. L. V. a. V. L., 2018. FeedRank: A tamper-resistant method for the ranking of cyber threat intelligence feeds. *2018 10th International Conference on Cyber Conflict (CyCon), IEEE*, pp. 321-344.

Mell, P., Scarfone, K. & Romanosky, S., 2006. Common Vulnerability Scoring System. *IEEE Security & Privacy,* 4(6), pp. 85-89.

Mokaddem, S. a. W. G. a. D. A. a. I. A., 2019. Taxonomy driven indicator scoring in MISP threat intelligence platforms.

Moustafa, N., Adi, E., Turnbull, B. & Hu, J., 2018. A New Threat Intelligence Scheme for Safeguarding Industry 4.0 Systems. *IEEE Access,* Volume 6, pp. 32910-32924.

Nalin Asanka Gamagedara Arachchilage, C. N. a. A. M., 2013. A taxonomy for securely sharing information among others in a trust domain. *8th International Conference for Internet Technology and Secured Transactions (ICITST-2013)*, pp. 296-304.

Nasser, B. et al., 2005. Access Control Model for Inter-organizational Grid Virtual Organizations. In: R. Meersman, Z. Tari & P. Herrero, eds. *On the Move to Meaningful Internet Systems 2005: OTM 2005 Workshops. OTM 2005. Lecture Notes in Computer Science, vol 3762.* Agia Napa: Springer, pp. 537-551.

Nweke, L. & Wolthusen, S., 2020. *Legal Issues Related to Cyber Threat Information Sharing Among Private Entities for Critical Infrastructure Protection.* Estonia, IEEE, pp. 63-78.

Oltramari, A. & Cho, J., 2015. *ComTrustO: Composite trust-based ontology framework for information and decision fusion.* Washington, IEEE, pp. 542-549.

Oltramari, A., Cranor, L., Walls, R. & McDaniel, P., 2014. *Building an Ontology of Cyber Security.* Fairfax, s.n., pp. 54-61.

Oltramari, A., Henshel, D., Cains, M. & Hoffman, B., 2015. *Towards a Human Factors Ontology for Cyber Security.* Fairfax, s.n., p. 26–33.

Page, L. a. B. S. a. M. R. a. W. T., 1999. *The PageRank citation ranking: Bringing order to the web.,* s.l.: Stanford InfoLab.

Papastergiou, S., Mouratidis, H. & Kalogeraki, E., 2019. Cyber Security Incident Handling, Warning and Response System for the European Critical Information Infrastructures (CyberSANE). In: J. Macintyre, L. Iliadis, I. Maglogiannis & C. Jayne, eds. *Engineering Applications of Neural Networks. EANN 2019. Communications in Computer and Information Science, vol 1000.* Xersonisos(Crete): Springer, pp. 476-487.

Ponemon Institute, 2015. *The Cost of Malware Containment,* s.l.: Ponemon Institute.

Ponemon Institute, 2019. *The Value of Threat Intelligence: Annual Study of North American & United Kingdom Companies,* s.l.: Ponemon Institute.

Qiang, L. a. Z. J. a. Z. Y. a. B. L. a. X. W. a. Y. Z., 2018. A quality evaluation method of cyber threat intelligence in user perspective. *2018 17th IEEE International Conference On Trust, Security And Privacy In Computing And Communications/12th IEEE International Conference On Big Data Science And Engineering (TrustCom/BigDataSE) IEEE*, pp. 269-276.

Radack, S., 2007. *The Common Vulnerability Scoring System (CVSS),* Gaithersburg: National Institute of Standards and Technology (NIST).

Rissanen, E., n.d. *Oasis extensible access control markup language (xacml) version 3.0,* s.l.: OASIS committee specification 1.

Ruks, D. C. a. M., 2015. Threat intelligence: Collecting, analysing, evaluating. *MWR InfoSecurity Ltd.*

Ruohomaa, S. & Kutvonen, L., 2005. Trust Management Survey. In: P. Herrmann, V. Issarny & S. Shiu, eds. *Trust Management. iTrust 2005. Lecture Notes in Computer Science, vol 3477.* Paris: Springer, pp. 77-92.

Sabo, J., 2004. Managing Trust in Critical Infrastructure Protection Information Sharing Systems. *ISSE 2004 — Securing Electronic Business Processes,* pp. 271-280.

Saidi, M., Elkalam, A. & Marzouk, A., 2012. TOrBAC: A Trust Organization Based Access Control Model for Cloud Computing Systems. *International Journal of Soft Computing and Engineering (IJSCE),* 2(4), pp. 122-130.

Saidi, M. & Marzouk, A., 2013. Multi-Trust_OrBAC: Access Control Model for Multi-Organizational Critical Systems Migrated To the Cloud. *International Journal of Soft Computing and Engineering (IJSCE),* 3(2), pp. 51-55.

Sandhu, J. P. a. R., 2002. *Towards usage control models: beyond traditional access control.* s.l., Proceedings of the seventh ACM symposium on Access control models and technologies.

Santos, O., 2016. *The Evolution of Scoring Security Vulnerabilities: The Sequel - Cisco Blogs.* [Online]
Available at: https://blogs.cisco.com/security/cvssv3-study
[Accessed 2 6 2020].

Saqib, A., Anwar, R. & Hussain, O., 2015. Cyber security for cyber physcial systems: A trust-based approach. *Journal of Theoretical and Applied Information Technology,* 71(2), pp. 144-152.

Schaberreiter, T. a. K. V. a. R. K. a. S. A. a. P. A. a. I. C. a. Q. G., 2019. A quantitative evaluation of trust in the quality of cyber threat intelligence sources. *Proceedings of the 14th International Conference on Availability, Reliability and Security*, pp. 1-10.

Schlette, D., Menges, F., Baumer, T. & Pernul, G., 2020. Security Enumerations for Cyber-Physical Systems. *Data and Applications Security and Privacy XXXIV. DBSec 2020. Lecture Notes in Computer Science,* Volume 12122, pp. 64-76.

Settanni, G. et al., 2017. *Acquiring Cyber Threat Intelligence through Security Information Correlation.* Exeter, IEEE, pp. 1-7.

Shouse, K., 2015. *Actionability of cyber threat intelligence - Doctoral dissertation,* s.l.: Utica College.

Shukla, S., 2016. *Cyber Security of Cyber Physical Systems: Cyber Threats and Defense of Critical Infrastructures.* Kolkata, IEEE, pp. 30-31.

Sillaber, C., Sauerwein, C., Mussmann, A. & Breu, R., 2016. *Data Quality Challenges and Future Research Directions in Threat Intelligence Sharing Practice.* Vienna, Association for Computing Machinery, pp. 65-70.

Simon, T., 2017. Chapter Seven: Critical Infrastructure and the Internet of Things. In: *Research Volume Five: Cyber Security in a Volatile World.* Ottawa: Centre for International Governance Innovation and the Royal Institute of International Affairs (CIGI), p. 142.

Squicciarini, A., Bertino, E., Ferrari, E. & Ray, I., 2006. Achieving privacy in trust negotiations with an ontology-based approach. *IEEE Transactions on Dependable and Secure Computing,* 3(1), pp. 13-30.

Standard, O., 2011. *extensible access control markup language (xacml) version 3.0.* [Online] Available at: http://docs. oasis-open. org/xacml/2.0/access_control-xacml-2.0-core-spec-os. pdf [Accessed 10 11 2020].

Sullivan, C. & Burger, E., 2017. “In the public interest”: The privacy implications of international business-to-business sharing of cyber-threat intelligence. *Computer Law & Security Review,* 33(1), pp. 14-29.

T. D. Wagner, E. P. K. M. A. E. A., 2018. A novel trust taxonomy for shared cyber threat intelligence. *Security and Communication Networks*.

T. Schaberreiter, V. K. K. R. A. S. A. P. C. I. G. Q., 2019. A quantitative evaluation of trust in the quality of cyber threat intelligence sources. *Proceedings of the 14th International Conference on Availability, Reliability and Security*, pp. 1-10.

Tang, L. et al., 2010. *Tru-Alarm: Trustworthiness Analysis of Sensor Networks in Cyber-Physical Systems.* Sydney, IEEE, pp. 1079-1084.

Taylor, J. & Sharif, H., 2017. *Security challenges and methods for protecting critical infrastructure cyber-physical systems.* Avignon, IEEE, pp. 1-6.

The MITRE Corporation, 2020. *CVE - Common Vulnerabilities and Exposures (CVE).* [Online] Available at: https://cve.mitre.org/ [Accessed 15 6 2020].

Thomas D. Wagner, E. P. K. M. a. A. E. A., 2018. A novel trust taxonomy for shared cyber threat intelligence. *Security and Communication Networks, Hindawi*.

UK Ministry of Defense, 2011. *Joint Doctrine Publication (JDP) 2–0: Understanding and Intelligence Support to Joint Operations,* s.l.: UK Ministry of Defense.

Vázquez, D. et al., 2012. *Conceptual framework for cyber defense information sharing within trust relationships.* Tallinn, IEEE, pp. 1-17.

Von Solms, R. & Van Niekerk, J., 2013. From information security to cyber security. *Computers & Security,* Volume 38, pp. 97-102.

VulDB, 1997. *VulDB - The Community-Driven Vulnerability Database.* [Online] Available at: https://vuldb.com/ [Accessed 5 5 2020].

Wagner, C., Dulaunoy, A., Wagener, G. & Iklody, A., 2016. *MISP: The Design and Implementation of a Collaborative Threat Intelligence Sharing Platform.* Vienna, Association for Computing Machinery.

Wagner, T. D. a. P. E. a. M. K. a. A. A. E., 2018. A novel trust taxonomy for shared cyber threat intelligence. *Security and Communication Networks, Hindawi*.

Waltermire, D. et al., 2016. *The Technical Specification for the Security Content Automation Protocol (SCAP): SCAP Version 1.3,* s.l.: National Institute of Standards and Technology (NIST).

Wang, G., Huo, Y. & Ma, Z., 2019. Research on University's Cyber Threat Intelligence Sharing Platform Based on New Types of STIX and TAXII Standards. *Journal of Information Security,* 10(4), pp. 263-277.

WhiteSource Software, 2019. *WhiteSource Vulnerability Database.* [Online] Available at: https://www.whitesourcesoftware.com/vulnerability-database [Accessed 28 5 2020].

Wiem Tounsi, H. R., 2018. A survey on technical threat intelligence in the age of sophisticated cyber attacks. *Computers & security, Elsevier,* Volume 72, pp. 212-233.

Win, K. & Thaw, Y., 2019. Information Sharing of Cyber Threat Intelligence with their Issue and Challenges. *International Journal of Trend in Scientific Research and Development (IJTSRD),* 3(5), pp. 878-880.

Xiong, L. & Liu, L., 2004. PeerTrust: supporting reputation-based trust for peer-to-peer electronic communities. *IEEE Transactions on Knowledge and Data Engineering,* 16(7), pp. 843-857.

Zhao, H. & Li, X., 2013. VectorTrust: trust vector aggregation scheme for trust management in peer-to-peer networks. *The Journal of Supercomputing,* 64(3), pp. 805-829.

Zhou, R. & Hwang, K., 2007. PowerTrust: A Robust and Scalable Reputation System for Trusted Peer-to-Peer Computing. *IEEE Transactions on Parallel and Distributed Systems,* 18(4), pp. 460-473.