RESEARCH ARTICLE

Threat intelligence platform for the energy sector

Rafał Leszczyna[1] | Michał R. Wróbel[2]

[1] Faculty of Management and Economics, Gdańsk University of Technology, Gdańsk, Poland
[2] Faculty of Electronics, Telecommunications and Informatics, Gdańsk University of Technology, Gdańsk, Poland

Correspondence
Rafał Leszczyna, Gdańsk University of Technology, Narutowicza 11/12, 80-952 Gdańsk, Poland. Email: rle@zie.pg.gda.pl

Summary

In recent years, critical infrastructures and power systems in particular have been subjected to sophisticated cyberthreats, including targeted attacks and advanced persistent threats. A promising response to this challenging situation is building up enhanced threat intelligence that interlinks information sharing and fine-grained situation awareness. In this paper a framework which integrates all levels of threat intelligence i.e. strategic, tactical, operational and technical is presented. The platform implements the centralised model of information exchange with peer-to-peer interactions between partners as an option. Several supportive solutions were introduced, including anonymity mechanisms or data processing and correlation algorithms. A data model that enables communication of cyberincident information, both in natural language and machine-readable formats was defined. Similarly, security requirements for critical components were devised. A pilot implementation of the platform was developed and deployed in the operational environment, which enabled practical evaluation of the design. Also the security of the anonymity architecture was analysed.

KEYWORDS:
cybersecurity, threat intelligence, situation awareness, information sharing, ISAC, power systems, testing, critical infrastructures

1 | INTRODUCTION

In the last years, a significant extension of the cyberthreat landscape has been observed. Attacks have changed visibly with respect to their target, function, range, and form. Modern, advanced threats are multi-vectored and multi-staged as they utilise various attack vectors, including e-mail, portable media, or vulnerable web protocols and are conducted in several stages, often extending over a longer period of time (*advanced persistent threats – APTs*)[1,2,3]. Next to classical, general attacks that affect large numbers of arbitrary computer systems, highly targeted and specialised cyberthreats have been introduced (*targeted attacks*)[4]. They can encrypt critical organisational data to interrupt business processes (NotPetya), withdraw financial documents related to oil and gas field exploration and gather operational details of industrial production (Night Dragon), observe designated office personnel (Flame) or modify programmable logic controllers (Stuxnet)[5,6,7,8]. Such attacks are not any longer conducted by malevolent individuals. Large, organised groups of specialists that aim at gaining real financial profits or political benefits stay behind them instead[1]. Also, the extensive expertise necessary for conducting such sophisticated attacks campaigns within a reasonable time can be only acquired by teams.

These threats can have very severe consequences especially in case of critical infrastructures i.e. the facilities that are crucial in the provision of vital societal functions, such as healthcare, utilities, financial services or food supply and communications[9,10].

Among them, the electricity sector is assigned the highest priority[11], which is due to the high reliance on it of other infrastructures. Unfortunately, with increased dependence on Information and Communication Technologies and wide adoption of commodity ICT solutions, they have become a common attack target[2,12]. Typical cyberattacks against critical infrastructures include Denial of Service (DoS) or Distributed Denial of Service (DDoS), malicious software, eavesdropping, intrusions, identity spoofing, password theft and side-channel attacks[13]. Modern critical infrastructures are constantly exposed to DDoS, which represent various attack types that aim at impairing the availability of a system function,. Already in 2011, McAfee revealed that 80% of critical facilities faced DDOS attack that year, while around 25% had to deal with DDoS on a weekly basis[14].

Organisations suffer the consequences of such attacks, despite considerable cybersecurity investments. The problem is that novel, advanced cyberattacks effortlessly circumvent classical, individually deployed protection measures, such as firewals or anti-malware, which mostly rely on static threat signature or pattern matching mechanisms designed for the previous generation of attacks[1,2]. New paradigms and techniques are required to protect from the new types of threats.[1,15].

As many cyberattacks can only be detected by correlating evidence provided from different sites[16], collaborative security solutions constitute a promising direction[17,18,19]. In the concept, system monitoring data are gathered from multiple distributed locations and analysed collectively to support security-related decisions[17]. This approach enables faster reaction to new attacks, facilitates detecting distributed attacks (such as DDoS) and proves good performance in mobile environments[17]. If managed properly, it also enables fine-grained situational awareness that is indispensable to contemporary computer systems. For these reasons, collaborative security has been attracting much attention in the last decade[17,18,19]. It is worth to note that so far collaborative security has been focusing on incident detection. However, the same approach could be applied to incident response, where multiple security solutions would be deployed in distributed system locations to enable the collective reaction to an incident.

Effective security information sharing, which in fact could be perceived as a different dimension of collaborative security, constitutes another important remedy for contemporary sophisticated threats[2,20]. This is particularly relevant to the protection of critical infrastructures, where partnerships between public and private sectors are indispensable for adequately protecting the infrastructures from emerging threats[16]. In these settings, sector-specific views together with experiences and extended case descriptions need to be exchanged to derive complete benefits[2]. Cyberincident information sharing has the potential for improving vulnerabilities discovery with reduced costs[21]. It facilitates keeping up with the evolving threat landscape[20], enhances threat awareness and enables effective incident response[15]. The benefits of information sharing are summarised in Table 1. To make such information exchange more effective, sector-specific views along with rich information and experience reports are required to provide an added value to professional users[2].

Consequently, collaborative cybersecurity and cyberincident information sharing have been widely reflected in various initiatives[24,2,25,26]. For instance, in response to the growing demand for European collaboration in protecting energy sectors, the European Energy – Information Sharing & Analysis Centre (EE-ISAC) was established in 2015. The EE-ISAC is a a public-private partnership where members share knowledge and report cyberincidents in trust-circles during meetings or using an information sharing platform[27,25]. A similar initiative, the Electricity Information Sharing and Analysis Center (E-ISAC) has been operating for North American electricity sectors[27]. Also the Oil and Natural Gas Information Sharing and Analysis Center was set up for analogous purpose[28]. The Retail Cyber Intelligence Sharing Center (www.r-cisc.org) already at its beginning associated more than 50 retailers[29].

The recognition of information sharing and situational awareness as of effective measures for combating modern cyberthreats has been broadly reflected in national and corporate cybersecurity strategies[30]. With natural differences between strategies developed in diverse environments, the common priorities are the protection of critical infrastructures, enhancing situational awareness and promoting information exchange[30]. During the last years, it has been widely acknowledged that sharing cybersecurity information will play a pivotal role in deploying the effective cyberdefence[16].

However, organisations are reluctant to share information on experienced cyberincidents either with partners, governments or competitors[1,31,24]. Unease about admitting of being involved in a cyberincident, potentially negative consequences related to damaged reputation and a competitive disadvantage in the market, sensitivity and criticality of data or natural, instinctive reluctance to sharing delicate data[31,32,1] are just some examples of reasons for organisations not joining cyberincident information sharing initiatives. Table 2 provides an overview of the reasons for the reluctance.

This paper presents a threat intelligence (TI) platform for the energy sector that encompasses all TI layers (strategic, tactical, operational and technical) and consolidates cyber-physical situation awareness networks with cyberincident information exchange (mostly utilised by human operators). The framework responds to the recommendation on establishing specialised, sectoral solutions instead of general approaches[2] in order to better address sector-specific issues.

TABLE 1 Benefits from cyberincident information sharing or areas that it improves.

	Benefit or improved area
1.	Reducing cyberattack consequences [15]
2.	Increasing the effectiveness of cyberincident response [15,22]
3.	Improved understanding of security problems [15]
4.	Enhanced threat awareness [1]
5.	Facilitated threat monitoring [15]
6.	Timely disaster recovery [1]
7.	Effective preparation for large-scale incidents [2]
8.	In-depth understanding of large-scale cyberincidents [2]
9.	Discovering covert cyberattacks and new malware [2]
10.	Running coordinated and effective countermeasures [2]
11.	Identifying threat agents and targeted assets [1]
12.	Preventive support to potential future targets on [2]
13.	Learning from incidents [23]
14.	Sharing lessons learned inside and outside organisations [23]
15.	Issuing early warnings and security advice [2]
16.	Distributing threat intelligence data [2]
17.	Reducing the chances of attackers repeatedly exploiting the same vulnerabilities in different organisations [21]
18.	Diminishing the likelihood of attackers compromising organisations to collect data helpful in attacking other organisations [21]
19.	Avoiding the duplication of efforts [20]

TABLE 2 The reasons for reluctance to participate in cyberincident information sharing.

	Reason
1.	Sensitivity and criticality of data [1]
2.	Legal requirements [1,33,34,35,2]
3.	Privacy issues [1,33,34,35,2,26]
4.	The fear of consequences [32]
5.	The fear of negative publicity [36,37,35,38]
6.	Discomfort in claiming of being involved in a cyberincident [31]
7.	The lack of trust in the sharing infrastructure [24]
8.	Costs [1,32,2]
9.	Insuficcient quality of shared information [1,33,39,32,40]
10.	Limited sharing of implications of relevant information [41]
11.	Unrecognised need for developing trust [41]
12.	Natural reluctance to sharing [32,1]
13.	Changing nature of cyber attacks [32,1]
14.	Unawareness of being involved in an incident [37,1]
15.	The lack of belief in successful prosecution [37,1]
16.	Obscured information sharing models [15]
17.	Misapprehended costs and benefits [15]
18.	The lack of understanding of differences in the role and expression of emotions during information sharing [41]
19.	Unrecognised differences in implementations of shared symbols [41]

In the following sections, after the introduction of the terminology (see Section 2) and the discussion of the relevant work (see Section 3), the platform is described, starting from the higher level related to strategic and tactical TI and associated with the exchange of cyberincident information (see Section 5). Lower-level threat intelligence solutions that aim at providing technical and operational situation awareness, are explained in Section 6. Section 7 is devoted to the evaluation of the threat intelligence platform. It includes an overview of utilised testing metrics and description of testing environments, integrity and usability tests as well as security analysis. The paper closes with concluding remarks.

2 | COLLABORATIVE SECURITY, INFORMATION SHARING, SITUATION AWARENESS, THREAT INTELLIGENCE

The terms collaborative security, information sharing, situation awareness and threat intelligence are strongly interrelated. The concept of *collaborative security* was introduced a decade ago[42,17]. It refers to the collective management of multiple security solutions or agents deployed in distributed system locations to improve overall security posture and to obtain effects unachievable with individual security[17]. Collaborative security has been applied in multiple security domains, including intrusion detection, anti-spam, anti-malware, identification of insider attackers and detection of botnets[17]. Although the term regards both attack detection and response, the studies conducted and solutions developed have focused on the incident monitoring and analysis part[42,17,18,19]. Similarly, the majority of developed applications have concentrated on the technical dimension, while on the higher level, the security collaboration can be established between people and organisations.

Cybersecurity information sharing is often presented as a primary instance of collaborative security[24]. It relies on partners sharing with each other crucial incident-related knowledge including the descriptions of experienced disturbances, indicators of compromise, proposed remedies and other security expertise. The key aim of the information exchange is to enhance the organisations' situational awareness to enable preparation for large-scale incidents and future threats[24,2,16].

The two most commonly adopted information sharing models are *peer-to-peer* and *centralised*[15] (see Figure 1a and 1b). In the former, participants exchange data directly between each other, in the latter a central node is introduced which acts as an intermediary in transferring the data. The communication can be either *synchronous* (e.g. videoconferences, phone calls) or *asynchronous* (e.g. e-mails, forum posts)[43]. From these basic configurations further, *confederated* topologies can be derived with smaller communities grouped around multiple central nodes that are connected to each other[44] (see Figure 1c). The communication between the network members and the central node can be unidirectional or bidirectional. In the first case, the central node acts as a source of information which publishes it among the participants. In the second case, the central node constitutes a hub which facilitates the data transfer between the participants[45,46] (see Figure 2).

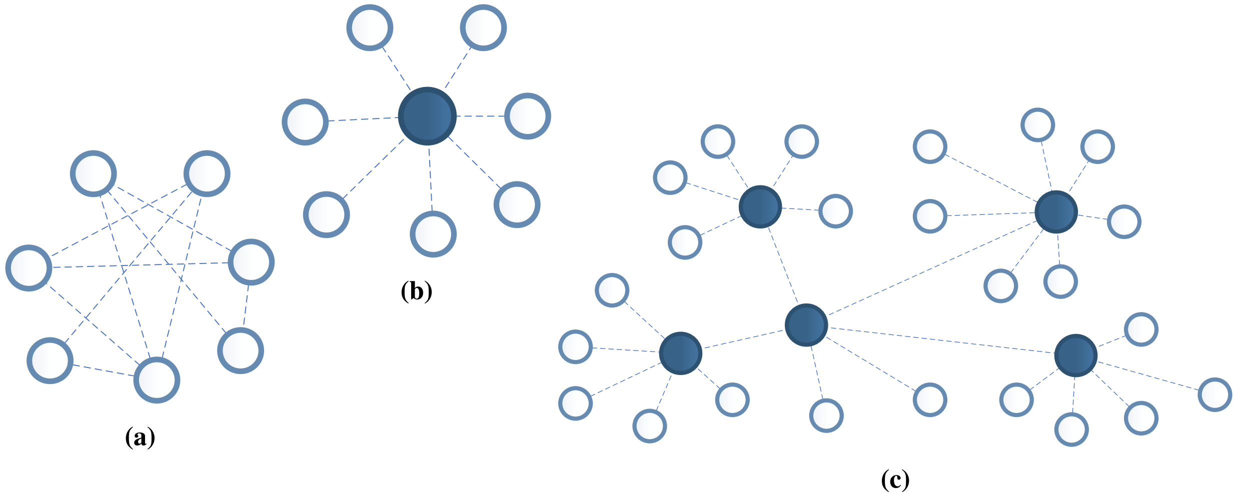

FIGURE 1 Information sharing topologies: (a) decentralised, peer-to-peer; (b) centralised; (c) confederated.

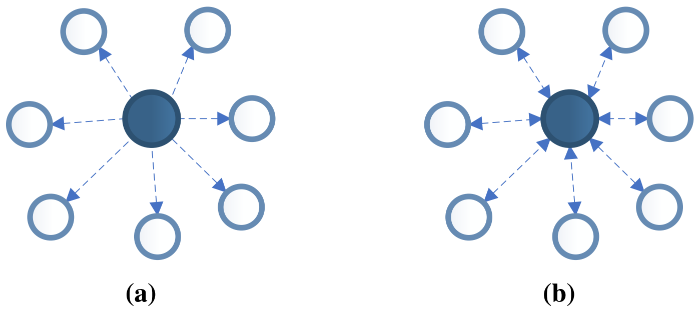

FIGURE 2 The modes of communication with the central node in centralised and confederated information sharing models: (a) unidirectional, the central node acts as a source of information; (b) bidirectional, the central node acts as a hub.

Contemporarily, Information Sharing and Analysis Centres (ISACs) are the institutions designated to lead sector-specific cyberincident information exchange[15]. With the aim of improving cybersecurity in independent industry areas, they often interlink the industry and the governmental organisations, forming public-private partnerships. In recent years multiple ISACs have been established, including the EE-ISAC[27,25], the E-ISAC[27], the ONG-ISAC[28] or DNG-ISAC[47]. He et al.[15] distinguishes 15 sample configurations of information exchange between different partners, including ISACs, IS participants, government organisations or vendors.

According to Skopik et al.[2] the principal scenarios that evidence the necessity of sharing cybersecurity information and demonstrate high economic potential are related to reporting recent or ongoing incidents, informing about service dependencies, sending the security status of services (e.g. in terms of their availability, confidentiality and integrity) and request assistance of other organisations. The authors also describe five dimensions of information exchange that should be taken into account when establishing an IS community, namely the efficient collaboration and coordination, laws and regulations, standardisation, existing implementations and the technology integration[2].

Situational awareness (SA), which is highly grounded in military intelligence[48], over the years has found its application in many critical domains where a solid recognition of the situation is required before making a decision. It regards a thorough explaration of the overall decision-making context and embraces the time-extended perception of an environment, the comprehension of observations and the projection of their status onto the proximate future[49,50,30]. Current methods for developing cybersecurity situation awareness include networks and systems monitoring, intrusion detection and alert correlation, security information and event management (SIEM), attack trend analysis, damage assessment and vulnerability analysis[51,52,46,53]. These methods deliver clusters of information that at a higher level still need to be analysed by humans[51]. *Situation awareness networks* (SANs) are technical architectures designed to provide SA by combining multiple sensors deployed in various system locations[54].

Threat intelligence (TI) is closely related to cybersecurity information sharing and situational awareness. It embraces all evidence-based knowledge about existing or emerging threats, that can be used to support cyberdefence decisions[1,55,56]. Threat intelligence has recently attracted great attention, including vendors of security solutions who offer diverse TI solutions[55,57,58,56].

Depending on the classification[1,59,60], threat intelligence can be formal and informal and provided at the strategic, tactical, operational or technical level. *Informal* TI regards unofficial modes of exchanging cybersecurity knowledge between organisations, while *formal* TI regards organisations sharing technical indicators of compromise[52,51]. *Strategic* TI concerns high-level cybersecurity knowledge, usually obtained from reports, seminars or conversations, to be used primarily by decision-makers when developing strategies, policies or regulations. *Tactical* TI represents detailed attack descriptions that are indispensable for appropriate preparation of countermeasures. *Operational* TI regards the information on cybersecurity events occurring in organisations during the daily performance which is provided and analysed by security personnel. *Technical* TI is the lowest-level data, gathered and processed by technical tools[1]. An important factor that should be considered in the TI domain is users' privacy as a considerable amount of data delivered to TI services originally contain identifiers of their source[58].

3 | RELATED WORK

The research on threat intelligence, information sharing and situational awareness centres around five main domains, namely the economic aspects of information sharing, determinants of IS and threat intelligence, data formats, tools supporting and conceptual frameworks. In the next sections, an overview of studies in these areas is provided and summarised.

3.1 | Economic aspects

Economic aspects of information sharing have been broadly studied both in and without relation to cybersecurity already for several decades[61]. Initial documents were published in the eighties[62,63]. In 1986 Shapiro[62] researched the benefits and motivations of sharing sensitive budgeting data between competitors. The study concluded that the exchange of cost information positively influences company profits and welfare, but diminishes expected consumer surplus. Kirby[63] evaluated the incentives for competing organisations to distribute information about an unknown demand. More recently, Soŝić[64] and Jain et al.[65] studied the role of information exchange in supply chains.

As far as the cybersecurity domain is concerned, Gordon et al.[66] investigated the impact of knowledge sharing on security investments and analysed the incentives for information exchange based on economic models. The authors admitted, however, that the data they used for the analyses were limited. The analogous topic was also addressed by Gal-Or and Ghose[67] who applied the game theory to it. In addition, they analysed how selected market characteristics, including company size and business model, influence the knowledge sharing behaviours between competitors as well as price competition between these firms. Game theory was also employed by Hausken[68] who evaluated company interdependencies and motivations of sharing cybersecurity information in the occurrence of an incident.

The relationships between knowledge sharing decisions and cybersecurity investments were analysed by Liu et al.[61]. As, according to the research, the levels of expenditures chosen in equilibrium tend to be lower than optimal, the authors proposed incentive schemes for helping organisations in coordinating investment choices in the context of knowledge sharing. Gordon et al.[69] applied the real options theory to illustrate how information exchange reduces the deterrence to cybersecurity acquisitions and stimulates more proactive investment behaviours. The work of Tosh et al.[70] is one of the most recent economic studies dedicated to the topic of cybersecurity information sharing. The authors model the problem area as an evolutionary game between organisations. They investigate the economic benefits of knowledge exchange and analyse the effects of not participating in the game.

3.2 | Determinants

Factors that determine information sharing and threat intelligence, encourage participation or cause reluctance, attributes that characterise them as well as other determinants have been studied for many years both outside and inside the cybersecurity domain.

As far as the broad information exchange context is concerned, Hilverda and Kuttschreuter[31] studied information sharing incentives taking the context of food decisions as a reference. The authors developed a structural equation model with four categories of determinants including individuals' beliefs about sharing, social factors, information characteristics, and risk-perception attributes. Kulikova et al.[71] distinguished four principal factors that influence organisational decisions on sharing cyberincident information, namely mitigation and prevention of harmful consequences, regulatory compliance, cost-efficiency and restoration of reputation. Cultural and social determinants of information exchange in the business environment were discussed by Boden et al.[72] who analysed two real-world cases with international enterprises operating in the IT sector. The impact of information exchange on teams performance was investigated by Rafaeli and Ravid[73].

In the disaster recovery area, Waring et al.[74] studied mechanisms that influence information exchange between emergency response teams. Their analyses revealed that clearly stated rationale, proper assignment of roles and well established procedures facilitate the information sharing, while limited situational awareness and incapacitated expression of information impede it. Complementarily to this research, Stemn et. al[75] examined the process of learning from safety incidents to determine potential points of its improvement.

In the cybsersecurity domain, Vakilinia and Sengupta[76] analysed incentives to share sensitive cyberincident data, with particular consideration to rewarding and participation-fee allocation mechanisms. Analogous, participation cost-related factors were investigated by Tosh et al.[77]. Ghose et al.[78] modelled relationships between attackers carrying out an attack against an enterprise to investigate the incentives for and the optimal level of sharing the information about the company's vulnerabilities. Nikoofal and Zhuang[79], Zhuang et al.[80], Zhuang and Bier[81], and Dighe et al.[82] applied game theory to determine the role of sharing cybersecurity information in cyberdefence strategies. Another approach was adopted by Sedenberg et al.[83] who analysed public healthcare as a model that enabled identifying guiding principles for cybersecurity information sharing. The principles encompassed governance, reporting, anonymisation, and use limitations.

3.3 | Data formats

To enable the effective exchange of cybersecurity information between heterogeneous actors, including individuals and organisations (e.g. computer emergency response teams – CERTs, ISACs), but also technical solutions (e.g. intrusion detection and prevention systems, SIEMs), appropriate data models and formats are required[24]. Over the last decade, multiple data specifications and standards have been developed. Among diverse initiatives in this area, stands out the community-driven work moderated by MITRE Corporation's System Engineering and Development Institute (SEDI) on behalf of the Department of Homeland Security, which resulted in the definition of the Trusted Automated Exchange of Indicator Information (TAXII), Cyber Observable Expression (CybOX) and Structured Threat Information Expression (STIX)[24,84,46,85].

TAXII specifies models and services for exchanging cyberthreat information. STIX is a structured language for representing the exchanged cybersecurity data that, while being highly human-readable, enables automated machine processing, facilitates describing a broad range of cybersecurity events and is flexible and extensible. CybOX is a standardised schema for the specification and communication of system events and properties[85].

Many new developments are derived from these solutions. An extension to STIX that supports sharing the information about the impact of cyberevents outside an organisation was proposed by Fransen et al.[46] who discuss it in the context of operation of the Dutch National Detection Network (NDN). Qamar et al.[86] integrated concepts of STIX and CybOX together with the Common Vulnerabilities and Exposures (CVE)[87] notation and a network model into a Web Ontology Language (OWL)-based ontology that enables threat-related specifications, semantic reasoning and contextual analyses. De Fuentes et al.[24] enhanced STIX with privacy-preserving mechanisms.

A detailed overview of existing solutions in this field of threat intelligence is provided in the report of ENISA[33].

3.4 | Supportive solutions

Over the years, multiple solutions have been proposed for supporting threat intelligence. For instance, Vakilinia[88] defined an anonymisation mechanism for information exchange that comprises four main components: registration, sharing, dispute and rewarding. Jajodia et al.[89] described Cauldron – a topological vulnerability analysis tool that aims at supporting mission-centric situational awareness. Cauldron enables modelling of attacks and vulnerabilities based on data from various sources. It also facilitates alert correlation and mission impact analysis. The importance of provisioning and utilising appropriate tools in collaborative security and in collective risk management in particular, was highlighted by Dehmer et al.[43], who discussed typical information sharing solutions, such as Content Management Systems (CMSes), video teleconferencing and electronic mails.

As a promising direction in detecting modern cyberattacks, collaborative intrusion detection (CIDS) has been studied intensively already for more than a decade[90]. Recent proposals include a privacy-preserving machine-learning based CIDS for vehicular ad hoc networks (VANETs)[91], a CIDS designed specifically to protect the smart grid[92], a trust-based clustering solution that supports deploying CIDS in wireless sensor networks (WSN)[93] or a CIDS for Advanced Metering Infrastructure (AMI)[94].

The critical notion of trust in the exchange of sensitive data has been addressed in the research. For instance, an interest-based trust model and an information sharing protocol for government agencies was proposed by Liu and Chetal[95]. Carter et al.[96] introduced a formalisation of trust for Mobile Agent System (MAS)-based information sharing. Several solutions that support situational awareness are described in the edited volume of Jajodia et al.[48].

3.5 | Conceptual frameworks

As far as operational threat intelligence architectures are concerned, broadly available platforms, such as AlienVault Open Threat Exchange (OTX)[97], Malware Information Sharing Project (MISP)[98,99] or ThreatView's Cyber Threat & Reputation Intelligence[100,101] have been developed either commercially or by community-driven projects. The scientific research has been focusing on conceptual models of TI architectures or methodologies of their development, deployment and governance[102,103,104,22].

A conceptual framework of situational awareness architecture for critical infrastructure protection was developed by the European Control System Security Incident Analysis Network (ECOSSIAN) project which concluded in 2017[105]. The authors promote the establishment of the National Security Operation Centre (N-SOC) which integrates diverse Operator Security Operation Centers (O-SOCs) deployed locally at the operators' premises[102].

Another conceptual model was introduced by Barth et al.[103] who describe an intra-organisational knowledge-management-based operational analysis platform. A prototype of the architecture was implemented using an open-source content management system. Alternatively, Klump and Kwiatkowski[106] proposed an architecture for sharing cyberincident information among smart grid stakeholders, while Brunner et al.[104] devised a concept of decentralised security information sharing that supports privacy of collaborating partners.

Alcaraz and Lopez[22] proposed a systematic approach for developing and establishing situational awareness architectures in the context of critical infrastructure protection. The methodology is built upon two fundamental stages and combines human-supervisory control that requires the presence of human operators with an automated option which is particularly suitable for isolated environments.

3.6 | Summary

The analysis of the scientific literature on threat intelligence, information sharing and situational awareness has revealed that the research offers many insights into these domains. In particular, determinants including incentives, barriers and economic factors, and supportive solutions in diverse functional areas that encompass, for instance, collaborative IDS indispensable for situational awareness, or privacy mechanisms that enable the exchange of sensitive information have been broadly investigated. Substantial work has also been done in the data models and formats area, crucial for effective communication and sharing of cyberincident data.

However, as far as holistic threat intelligence architectures are concerned, the prevalence of scientific proposals are still on a conceptual level, while commercial or community-driven solutions do not provide sufficient documentation regarding adopted, potentially innovative, mechanisms. In addition, both, scientific and commercial/open-source contributions tend to separately address high-level, strategic (e.g. sectoral) cyberincident information exchange and technical situational awareness. At the same time, the joint approach is highly recommended, especially in the context of critical infrastructure protection[22].

4 | THREAT INTELLIGENCE PLATFORM FOR THE ENERGY SECTOR

The threat intelligence platform for the energy sector proposed in this paper integrates all levels (strategic, tactical, operational and technical – see Section 2) of threat intelligence interlinking technical situational awareness mechanisms that enable machine-generated input with higher levels of information exchange where data are shared between organisations and individuals. Embedded anonymisation mechanisms aim at strengthening the motivation for sharing sensitive data even with competitive organisations in the sector.

At the technical level, Security Information and Event Management (SIEM) systems aggregate and process detailed technical data delivered by diverse sensors, such as IDS/IPS or network monitoring tools, deployed in multiple locations of an organisation's system. These processed data are then delivered to the dashboard located in the central node of the threat intelligence platform for high-level analysis. The SIEMs together with sensors constitute (technical) situation awareness networks (SANs) (see Section 6). Besides the technical level functions, the SANs aim at supporting the operational TI. Once a cyberincident is detected, they alert security officers and provide them with all relevant data, including network status and system logs, in the most concise form.

Based on this input, detailed attack descriptions are prepared which can be shared with the TI community. SAN dashboards facilitate visualisation of incident-related data and preparation of comprehensive documentation indispensable for the development of appropriate countermeasures. This constitutes the tactical level of TI. The strategic tier is mostly related to the activities of the information sharing and analysis centre (ISAC) and members of the TI community. Based on the input shared between stakeholders, sectoral cybersecurity strategies and policies are collaboratively (public-private partnership) developed.

The architecture of the threat intelligence platform is presented in Figure 3. The two main architectural components of the TI are the information sharing platform and situational awareness networks. These solutions together with supporting mechanisms for users' anonymity, data aggregation and sanitisation, models and rules are described in the following sections.

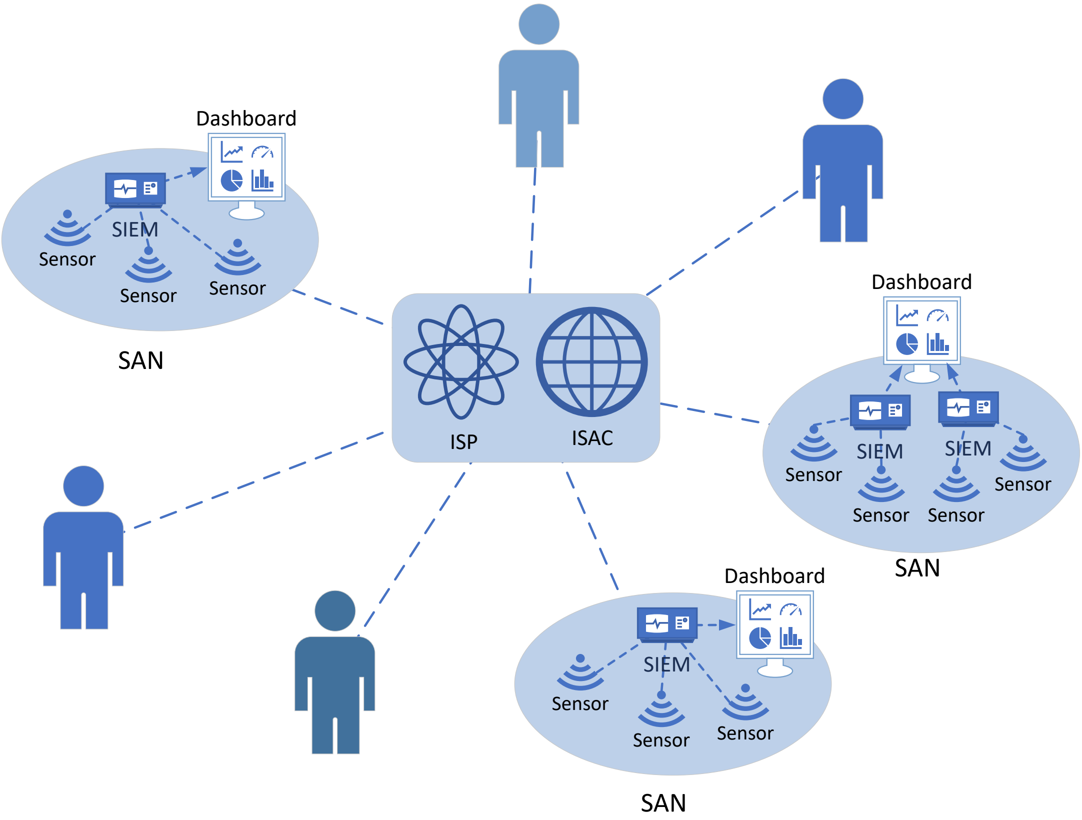

FIGURE 3 The architecture of the threat intelligence platform for the energy sector.

5 | INFORMATION SHARING PLATFORM

The information sharing platform constitutes the skeleton of the threat intelligence framework as it provides the infrastructure for the transmission of all cyberincident-related data, both in natural language and machine-readable formats. For the latter purpose, the appropriate data model was developed, which incorporates established specifications in this area (see Section 5.1).

The centralised model of information exchange (see Section 2) is implemented with information sharing and analysis centre as the central node. The ISAC-moderated information sharing is promoted in the platform to enable uniform distribution of the information in the whole community, however, also peer-to-peer interactions between partners are possible. Both, unidirectional and bidirectional communication with the central node is facilitated, primarily in the asynchronous form, where incident data are encapsulated into messages prepared in accordance with the proposed data model. Synchronous communication is predominant at the strategic level, where formal and informal threat intelligence is enabled.

To encourage sharing delicate information, an anonymity architecture has been established (see Section 5.5) and data sanitisation mechanisms (see Section 5.2) have been introduced. The architecture takes advantage of the mobile agents paradigm that is particularly suitable for the deployment in heterogeneous environments, such as the energy sector. Data sanitisation, on the other hand, enables maintaining a good equilibrium between security and usefulness of exchanged data. Cybersecurity requirements brought out specifically for the energy sector's information sharing platform are described in Section 5.4.

5.1 | Data model

The crucial element during the development of an information sharing platform is designing a data model. This step is essential to:

- determine the types of data exchanged in the platform,
- facilitate the communication between the developers of the ISP and its future users, in particular during the elicitation and analysis of software requirements,
- support the specification of other functionalities including data sanitisation or aggregation (see Sections 5.2 and 5.3).

The energy sector exposes specific characteristics that need to be embraced in the model. In particular, the *heterogeneity and geographical distribution of participants* and *automatically generated data* should be considered. The future users of the ISP represent diverse domains and sectors, implement various business models and have different (sometimes opposite) interests and forms of activity. In addition, they are situated in dispersed, often remote, geographical locations. As a result, establishing an effective communication with all participants is hindered, especially in regard to physical meetings-based. Such communication is indispensable for obtaining users' input and feedback regarding the types and format of exchanged. As far as the second characteristic is concerned, part of the information exchanged in the ISP would be delivered by SANs and security solutions such as IDS/IPS or anti-malware tools. The developed data model needs to encompass the machine-generated contents.

In order to incorporate these requirements, a tailored approach was proposed that merges the classical data modelling methodology with an adaptation of the iterative and incremental software development model. In the approach, four classical phases of data model design are passed, namely *business requirements analysis*, *conceptual data modelling*, *logical data modelling*, and *physical design*. During the process, the three main increments of the data model are developed, i.e.*very high-level data model (VHLDM)*, *high-level data model (HLDM)*, and *logical data model (LDM)*. These increments reflect the key products of standard data modelling. At least three iterations need to be performed for each increment. During the first iteration, the data model is created without direct users' involvement. It is based on the input received during an earlier increment and/or the analysis of available documentation, standards and other literature. In the second iteration, the data model is presented to users in an electronic form. The third iteration starts after obtaining the users' feedback. A document synthesising the received input is submitted for a discussion during a physical meeting. The process can be repeated until the model is accepted by all stakeholders[107].

To assure data model compatibility with machine-generated contents, standardised data representations for security information i.e. the Intrusion Detection Message Exchange Format (IDMEF)[108] and the Incident Object Description and Exchange Format (IODEF)[109], as well as the Dublin Core Metadata[110] for general purpose documents were integrated into the model. IDMEF specifies formats and procedures for the exchange of information between intrusion detection and response systems as well as management systems that need to interact with them[108]. IDMEF was developed by The Internet Engineering Task Force (IETF). Although the IETF work on the IDMEF was suspended and the specification has never been adopted as a standard, almost all popular IDS, including Snort, Suricata or OSSEC enable IDMEF-based communication. IODEF defines a common data format for describing and exchanging information about incidents between Computer Security Incident Response Teams (CSIRTs). It is fully compatible with IDMEF, yet extends it with objects enabling communication between people and teams[109]. Dublin Core, standardised as ISO 15836:2009[110], specifies a set of fifteen properties for describing resources. It enables detailed descriptions of documents[111]. The approach was applied to create the entire, 3-levelled data model for the cyberincidents information sharing platform for the energy sector[107,112]. A very high-level data model diagram is presented in Figure 4. Information assets were identified based on the analysis of data which can be created and shared by sectoral stakeholders.

5.2 | Data sanitisation

At the stage of detecting a cyberincident, its descriptive data should be as detailed as possible, to enable an effective response. For this purpose, the information about IP addresses, protocols, ports, event timing, sensor identity, and often packet headers or the payload are captured. However, when this data is to be shared on an ISP, the high level of detail in the information may contradict its security. The data are no longer delivered to a trusted and well-known system administrator who usually works for the company but need to be shared with all external participants of the information sharing platform. This creates various opportunities for an attacker to explore and misuse the shared data. In addition, sharing certain details may be undesirable, even in trusted circles.

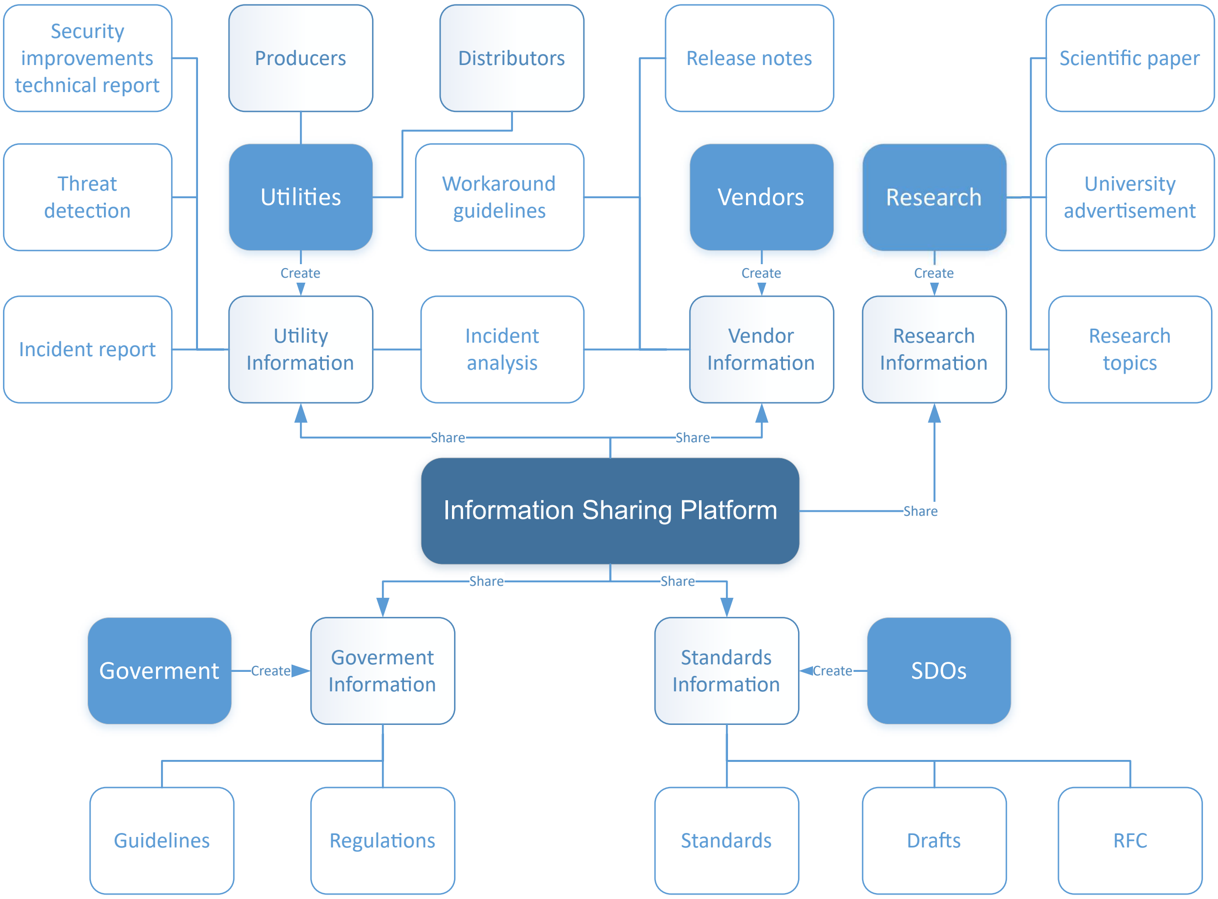

FIGURE 4 Very High-Level Data Model of Incident Information Exchange in Energy Sector.

A technique that enables preserving a balance between security and usefulness of shared data is *data sanitisation*. It aims at preventing information from being used for unintended purposes, which is achieved by removing or altering its sensitive parts. Multiple methods of data sanitisation exist, which are summarised in Table 3. The advantage of these techniques is that they do not utilise cryptography and consequently they do not require keys management. This renders them very suitable for the application in the energy sectors. There, the key management process is very demanding due to the scale and diversity of participating information systems.

Sanitisation rules were defined for each entity of the data model described in Section 5.1. Two sanitisation levels were distinguished. The low level of sanitisation refers to the situation where only the most sensitive data are sanitised. High-level sanitisation, on the other hand, aims at protecting also the data which could only potentially provide some indirect indications to an attacker, who based on additional knowledge, could infer the value of critical data. Sample sanitisation rules are presented in Table 4.

5.3 | Data aggregation

As written in Section 5.1, part of the data exchanged in the information sharing platform are generated automatically by SANs and security solutions such as SIEMs or IDS/IPS. In certain situations, these tools may expose the tendency of providing large amounts of redundant information that could be difficult to process and comprehend by human participants.

For instance, during a large-scale brute force attack against network entry points of sectoral stakeholders, individual notifications would be issued for each attacked system, resulting in dozens of new messages sent to the ISP. Similarly, an attack campaign with diversified attack vectors would lead to numerous messages posted to the ISP, even if it originated from a common source. In that case, each message would reflect a different attack vector treated as a distinct attack.

TABLE 3 Sanitisation methods summary[113,114,90,115,116].

Method	Description
Generalisation	Replacing a value with a range of possible values that the attribute may assume. Generalisation methods include *suppression* – omitting a sensitive datum, *deletion* removing a value, *aggregation* – categorising a datum with other data, *number variance* – modifying each number value by a random percentage of its original value, *substitution* – replacing with less specific values (for instance, replacing a birth date with the birth year or rounding an age to the nearest ten), *shuffling* – replacing with a value from the same set of the values being sanitised.
Perturbation	Retaining a single value, but transforming it in some way. Examples: masking data or adding a random value to a data (a noise).
Gibberish generation	Substituting parts of a text with random content.
K-anonymity	A widely-used sanitisation technique based on generalising information so that the generalisation is valid for at least *k* entities. It exists in several variants which address specific problems.
L-diversity	A variant of k-anonymity in which every group of quasi-identifiers i.e. the data which allows for identifying an entity uniquely, must have some number of distinct values for the sensitive attribute.
Bloom filters	One-way data structures on which only two operations are possible, namely the insertion and verification so that while no data can be extracted after being inserted into a Bloom filter, it can be verified if it was previously inserted into the filter if presented a second time to the filter. The technique is used for sanitising IP addresses.
Data cubes	Hashing the addresses of observables to a limited set of coordinates, and represent the intensity of observables as two-dimensional values, and time as a third dimension.

TABLE 4 Sanitisation rules for the *Operating system* data model entity.

Title	Operating system		
Description	The entity represents the operating system which was the target or the source of an Attack.		
Field	Description	Sanitisation	
		Low	High
Type	Operating system type	No	No
Name	Operating system name	No	No
Version	Operating system version	No	Yes

To avoid this situation, it is necessary to implement algorithms that enable correlation and aggregation of shared data. In the first example, other (not attacked) stakeholders would like to receive general information about the incident, depicting the scale of the attack, exploited vulnerabilities and affected services. The expected message to be published in the ISP, would contain a description of the attack and the information about the starting time of the attack, the number of affected computers, the numbers of attacked ports, service numbers or names. In addition, with the arrival of new data regarding the ongoing attack, the information should be updated on the ISP, rather than new posts created.

For the second case, a common part of all notifications received by the ISP is the information about the attacker. Therefore, the platform should group all the data describing the attacker and, based on the collected data, indicate suspicious IP addresses from which the attacks were carried out. This data could be enriched with a list of vulnerabilities and techniques used during the attack. As in the first example, the appearance of new information about the attack should lead to post update, instead of the creation of a new one.

Prior to the development of aggregation algorithms, grouping attributes need to be chosen i.e. the data entities for which identical or similar values (depending on the selected criteria) in distinct messages would result in aggregating the messages. Examples of grouping attributes include the attack source, the attacked service, the attack method, the attacked application or the attacked operating system. The next step is to map the selected attributes to the appropriate entities in the data model. For the sample grouping attributes, the following assignments

- Attack source: Incident → Attack → Source → Location (address, netmask)
- Attacked service: Incident → Attack → Target → Service (protocol, port)
- Attack method: Incident → Method (type, name)
- Attacked application: Incident → Attack → Target → Program (name, version)
- Attacked operating system: Incident → Attack → Target → OS (type, name, version)

The aggregation will be possible only if grouping attributes have not been previously sanitised (see Section 5.2). Thus, a verification step needs to be incorporated into an aggregation algorithm, to check whether data have not been sanitised. As a result, the general form of an aggregation algorithm presented in Figure 5 was proposed. When creating specific instances of the algorithm, the [attribute] field in the scheme, should be replaced with a particular grouping attribute. In the algorithms, the maximum time between incidents (MTBI) plays an important role as it is used to determine whether an incident can be treated as part of a previously detected attack. For instance, if set to 1 hour, the information about a DoS attack against the same group of hosts with an interval larger than 1 hour would be recognised on the ISP platform as two separate incidents. For each grouping attribute, a separate MTBI can be assigned.

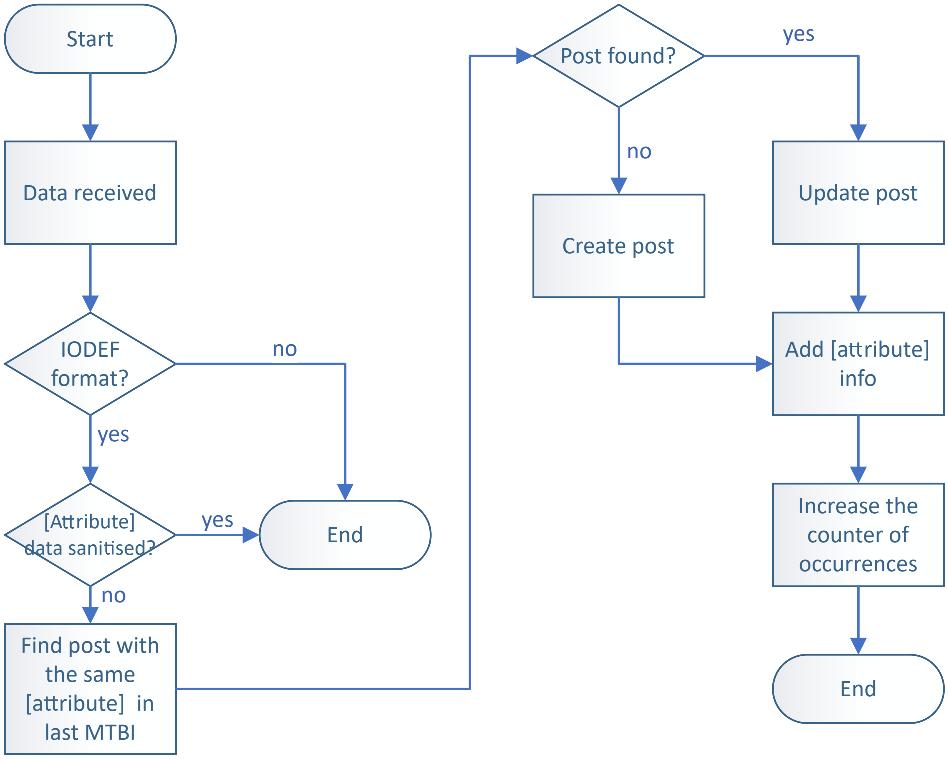
Start
Data received
IODEF format?
no
yes
[Attribute] data sanitised?
yes
End
no
Find post with the same [attribute] in last MTBI
Post found?
yes
no
Create post
Update post
Add [attribute] info
Increase the counter of occurrences
End

FIGURE 5 General form of the data aggregation algorithm. In its specific instances, the [attribute] field should be substituted with a particular grouping attribute such as attack source, attacked service, attack method or attacked application. MTBI depicts the maximum time between incidents.

5.4 | Cybersecurity requirements

Cybersecurity requirements for the information sharing platform were elicited based on the study that comprised the following stages:

- the identification of available security requirements for alternative security ISPs developed for other industries,
- the review of the literature on security requirements engineering,
- the analysis of the available sources of security requirements for Content Management Systems (CMSs), web applications and databases – as an ISP is a form of a specialised CMS.

As a result security requirements categorised into 15 areas have been identified which are presented in Table 5. Sample definitions of the requirements for the first three categories (risk assessment, authentication, authorisation and access control) are as follows:

- *The risk assessment must be performed against all the data assets of the ISP.*
- *Authentication policies, processes, and logging must be designed, developed and documented to assure that the application keeps unauthorised users from accessing the site.*
- *Access control must be implemented for the ISP components which are available only to the authorised parties.*

TABLE 5 Categories of security requirements for the information sharing platform.

Security requirements categories		
A. Risk Assessment	F. Database Protection	K. Administration
B. Authentication	G. Cryptography	L. Configuration
C. Authorisation and Access Control	H. Passwords	M. Penetration Testing, Server and Application Validation
D. Session Management	I. Error Handling	N. Protection from Malicious Code
E. Data and Input / Output Validation	J. Logging	O. Anonymity and data sanitisation

More details on the requirements and their elicitation process can be found in[117].

5.5 | Anonymisation mechanisms

In addition to data sanitisation (see Section 5.2) which principally prevents shared data from being used for unintended purposes by obscuring unnecessary details, the mechanisms that enable anonymity of the information senders have been introduced. This is to encourage the exchange of even highly sensitive information between platform participants with different trust levels.

Anonymity is a property that an entity is not identifiable among other entities[118]. Anonymity mechanisms in the information sharing platform for the energy sector aim at protecting the identity of information senders. This is achieved by concealing all personally identifiable information (PII) as well as by mitigating more sophisticated attacker techniques which aim at revealing the target's identity. These techniques refer to *traffic analysis* (TA), i.e. analysing network communication in order to *trace* the target (see Figure 6)[119].

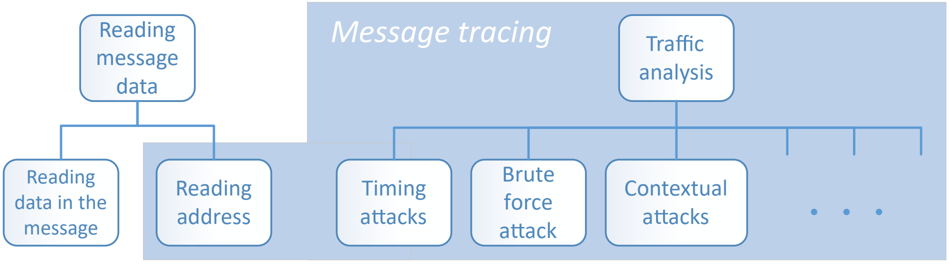

FIGURE 6 Techniques of attacks against anonymity in the network communication.

A mobile agent-based anonymity architecture described in[119,120,121] was adapted to the ISP. The architecture is composed of two modules, namely the *Module I: Untraceability Protocol Infrastructure* and the *Module II: Additional Untraceability Support* (optional). The first module constitutes the core of the architecture. It implements an untraceability protocol to assure that the address of a message sender to the ISP is obfuscated. The second part of the anonymity architecture aims at providing further anonymity protection i.e. the protection against traffic analysis and tracing through reading data held by agents. This module is based on optional components, which implementation and application should be preceded with a thorough requirements analysis and feasibility study as each of the components, while strengthening the security of the system, also introduces an (often significant) overhead[122].

To effectively protect the ISP, the anonymity architecture should be deployed in multiple, dispersed network nodes. In the energy sector, the heterogeneity and geographical distribution of its participants constitutes a strength, that should be taken advantage of at this stage. With the variety of participating stakeholders, organisations, technological solutions and system architectures, the energy sector is a complex environment, in which anonymisation nodes of the anonymity architecture can become practically completely secure from being altogether, or in a large subset, observed by an attacker. For instance, in the power grid, the anonymisation nodes can be deployed in offices, power plants, substations which is visualised in Figure 7.

Mobile agents facilitate deployment and communication in such complex and heterogeneous environments[123,124]. A mobile agent is a software which can roam networks making independent decisions regarding its destinations. To accomplish their objectives (*goals*), mobile agents move from one network node (called a *container*) to another, starting from a *base* (a *base station*). The sequence of containers to be passed during the itinerary is called a *route*[124].

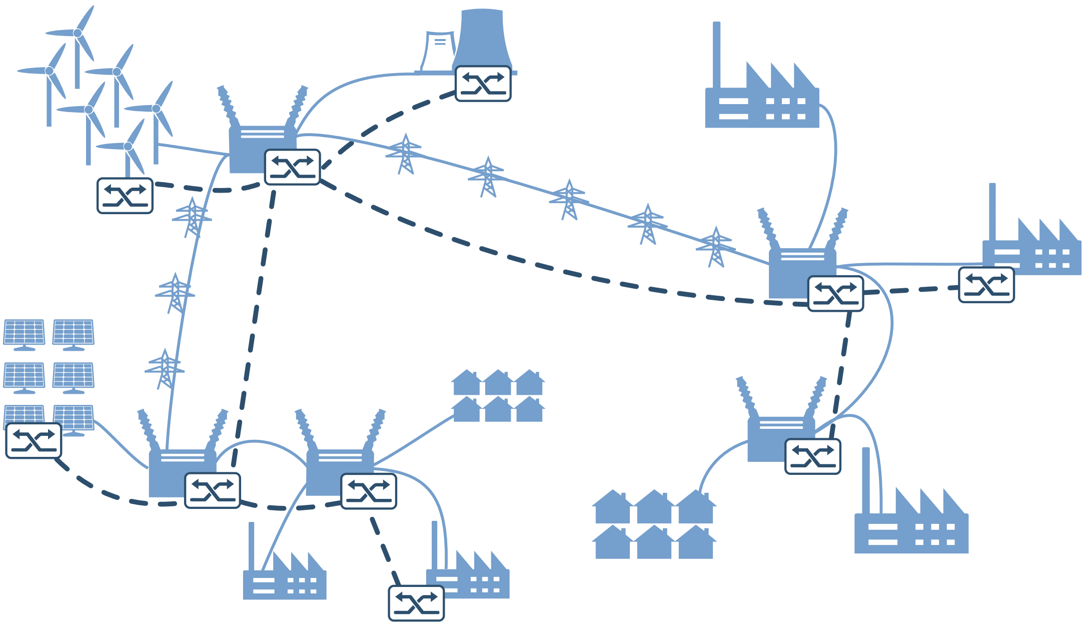

FIGURE 7 Anonymity architecture deployment in the power sector.

6 | SITUATION AWARENESS NETWORK

Situation awareness networks (SANs) are technical architectures designed to provide situation awareness (SA) by combining multiple sensors deployed in various system locations[54]. Conceptually, SANs are the direct instantiation of the collaborative security paradigm. In the proposed energy sector's threat intelligence framework, SANs are responsible for the provision of detailed, processed cyberincident information at the technical and operational level.

A specialised SAN architecture was designed, which takes advantage of Security Information and Event Management (SIEM) systems as well as diverse types of sensors, including communication protocols dedicated to energy systems'[125,54,53]. Data processing techniques, including data correlation (see Section 5.3), are implemented in order to reduce the number of false positives, increase detection efficiency and facilitate the comprehension of reported information by human operators. This, in turn, facilitates decision making and fosters faster reaction to threats and incidents. The architecture is described in Section 6.1.

6.1 | Architecture

The SAN for the energy sector represents a three-tiered architecture illustrated in Figure 8 [125,54,53].

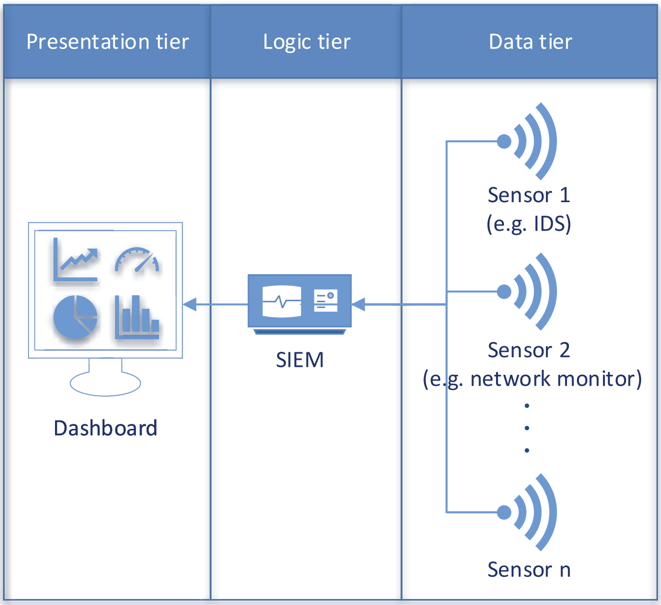

FIGURE 8 The logical architecture of the cybersecurity situation awareness network for the energy sector.

The lowest tier – the *data tier* – comprises diverse network and host-based sensors, including different IDS/IPS architectures, network monitoring software and traffic analysis tools, which facilitate system inspection and detection of suspicious events. For instance, a signature-based network intrusion detection system, such as Snort [126,127] and Suricata [128], can be applied to detect well-known attack payloads, and several behavioural-based engines to analyse both payloads and flows for anomalies. The need for joining together multiple, heterogeneous sensors stems from the observation that monitoring tools became specialised and currently they focus on specific threat vectors and analysis approaches. Thus to assure a broader overview of system situation, multiple alternative monitoring techniques need to be applied.

The middle tier of the architecture – the *logic tier* – is dedicated to the Security Information and Event Management (SIEM) system. The SIEM aggregates data from sensors, pre-processes them and transfers to the presentation layer. The sensor data are provided in the `syslog` format. An openly available implementation of a SIEM for industrial environments was a preferable option for application in the energy systems SAN. The Bro Network Security Monitor is a network analysis framework which satisfies this criterion. Not constrained to a particular type of detection, it enables implementing proprietary algorithms on the top of its protocol parsers [129,130].

The top tier – the *presentation tier* – corresponds to visualisation of the overall system cybersecurity status, which is crucial to attain situational awareness [30]. The data obtained from the logic tier are further processed and posted on a dedicated dashboard. The dashboard utilises multiple, flexibly configurable visualisation components that enable monitoring of diverse aspects of system security situation (see Figure 9). The additional tier that enhances the presentation capabilities of SIEM systems was introduced to support recognising the anomalies undetectable to automatic systems due to their mode of operation or particular configuration. The dashboard fosters analysing and filtering large amounts of data to concentrate on the most critical determinants of a cyberincident. It enables observing the evolution of the system situation after an event is reported, to thoroughly analyse its nature and to confirm or deny the existence of a threat.

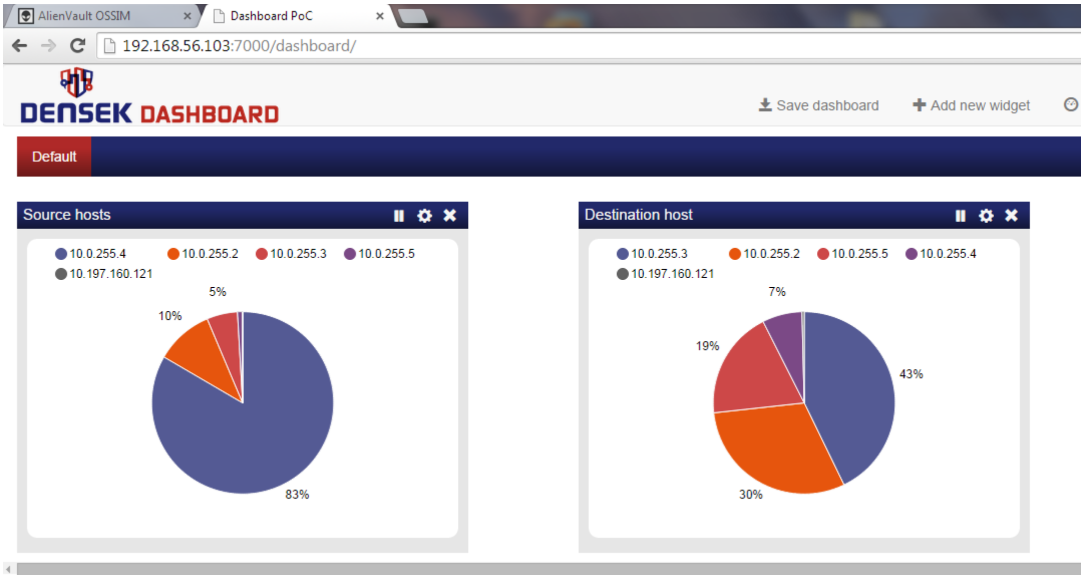

FIGURE 9 Situation awareness dashboard utilises multiple, flexibly configurable visualisation components that enable monitoring of diverse aspects of the system security situation.

6.2 | Security requirements for sensors

The security requirements for the SAN sensors were selected based on the National Information Assurance Partnership (NIAP) protection profiles for intrusion detection systems, sensors, scanners and analysers, published by the U. S. National Security Agency[131,132,133,134]. The Protection Profiles (PPs) are compliant with Common Criteria. The Common Criteria is an international standard that specifies the criteria for security evaluation of IT hardware and software products (hardware and software)[135]. Selected security objectives and functional requirements for sensors and their supporting environments are presented in Tables 6 and 7.

TABLE 6 Selected cybersecurity objectives for the sensors of the cybersecurity situation awareness network for the energy sector.

	Security objective
1.	auto-protection from unauthorised modifications and access to functions and data
2.	collection and storage of information about all events that may indicate an inappropriate activity
3.	effective management of functions and data
4.	granting authorised users the access only to appropriate functions and data
5.	identification and authentication of authorised users prior to granting access to functions and data
6.	appropriate handling of potential audit and sensor data storage overflows
7.	recording audit records for data accesses and use of the sensor functions
8.	assuring the integrity of all audit and sensor data
9.	ensuring the confidentiality of sensor data when available to other SAN components
10.	secure delivery, installation, management and operation of sensors
11.	protection of critical sensor elements from physicals attacks
12.	protection of access credentials
13.	careful selection and training of personnel working as authorised administrators

TABLE 7 Selected cybersecurity functional requirements for the sensors of the cybersecurity situation awareness network for the energy sector.

	Functional requirement
1.	sensor data collection
2.	restricted data review
3.	sensor data availability
4.	prevention of sensor data loss
5.	audit data generation
6.	audit review
7.	restricted audit review
8.	selectable audit review
9.	selective audit
10.	audit data availability
11.	prevention of audit data loss
12.	timing of authentication
13.	user attribute definition
14.	timing of identification
15.	management of security functions behaviour
16.	security roles
17.	reliable timestamps

6.3 | Event correlation rules

Event correlation rules are machine-readable definitions that allow the SAN finding relations between cybersecurity events, identifying associated events, recognising their common source or target etc., which altogether should facilitate detecting even the most subtle or complex cybersecurity threats.

Correlation rules that introduce prioritisation of SAN alerts were specified, to reduce the number of false positives received from the lowest SAN tier, i.e. the data tier. The incident detection rules implemented in the data tier mostly correspond to common industrial automation and control systems (IACS) attack vectors. The highest-priority alerts require an immediate response. Medium-priority alarms automatically start auto-protection actions, such as IP address blocking. The lowest-priority alerts are registered in the audit log and can be resolved in a convenient time.

As far as the correlation rules are concerned, the highest-priority alerts require the simultaneous occurrence of at least two alerts defined in the correlation table. In addition, a condition needs to be satisfied that the attack target is situated in the protected network. In this mode, alerts dispatched by random events are limited, while the overall detection capability remains unaffected. Medium-priority alerts are raised, when two alerts of any type are signalled in close time proximity from the data tier. Usually, this corresponds to the situation when an adversary attempts to conduct an automated attack without prior network cognisance. The remaining individual and separate alerts originated from the data tier are assigned the low priority.

7 | EVALUATION

The evaluation of the threat intelligence framework for the energy sector embraced both, its the technical and higher-level dimensions. The former were mostly related to situational awareness networks, while the latter – predominately associated with information sharing. To enable systematic measurements, testing metrics specific to the sectoral TI platform were derived. Integrity tests were conducted to examine interoperation of SAN components. To assess the quality of interfaces and human-computer interactions involved in information exchange activities usability tests were performed. Also, the security of the anonymity architecture was analysed.

7.1 Testing metrics

Testing metrics enable objective evaluation of products and their development processes. Various types of metrics, including performance, effectiveness or complexity metrics, have been devised for different ICT domains. The TI area, however, due to its novelty, required new consideration. When introducing metrics, specific criteria were taken into account, namely the metric should[54,53]:

- enable consistent measuring,
- be expressed as a cardinal number or percentage,
- be represented in units of measure,
- be contextually specific,
- be achievable at a reasonable cost,
- be straightforwardly implementable in the TI context at every stage of development.

Three categories of metrics have been proposed: *testing process metrics*, *cybersecurity metrics* and *usability metrics*[54,53]. *Testing process metrics* facilitate the control and management of a testing procedure. The selected metrics include source code coverage, test case defect density, failures detection rate and test improvement in product quality. *Cybersecurity metrics*, derived from the IDS/IPS and SIEM domains, are directly related to TI technical-level operation. They include accuracy, detection rate, false positive rate, mean time between failures and time to protect. *Usability metrics* refer to the usability of TI tools and are mainly associated with the quality of the TI interfaces and the human-machine interactions it enables. The selected metrics include task success, time-on-task, efficiency, errors and learnability. The metrics were applied during the tests described in the next sections. For instance, the results obtained for the *time-on-task* metric are presented in Table 8.

7.2 Testing environment

The tests of the threat intelligence platform were performed mostly in two testing environments. At the technical and operational level, in major part related to SA instrumentation, including SANs, SIEMs and sensors, the TI was tested in the cybersecurity laboratory of the Enel Engineering and Research located in the power plant area of Livorno. This laboratory is designed to replicate operational environments associated with power generation. The tests of higher-level TI, predominately linked to information sharing, where human interactions are strongly involved, were carried out in the laboratory at Gdańsk University of Technology.

The Enel laboratory was designed for testing and development of process control applications. It comprises all crucial components of industrial control systems, including PLCs and Distributed Control Systems (DCSs) from various vendors. Its computer network is layered in the same way as in a production plant. The physical part of this cyber-physical system reproduces the closed water cycle similar to the associated with electric power generation. It is equipped with field devices such as pressure meters, valves, pumps, inverters, etc. controlled by PLCs.

The primary logical areas of the testing environment are:

- *Field system* constitutes this part of the system which is most near to the physical process. It comprises all PLCs, RTUs and sensors of the power plant.
- *Process control and data acquisition system* is responsible for controlling the field system.
- *Control network* provides the infrastructure and services for controlling the experiments performed in the environment.
- *Data network* supports collecting and processing of data produced during experiments.
- *Business network* reflects this part of the power plant network, which is related to office work.
- *Demilitarised zone* hosts various power plant servers that are accessible from the outside of the local network.

The network diagram of the testing environment is presented in Figure 10.

The infrastructure of the laboratory at Gdańsk University of Technology utilised in tests consisted of several interconnected desktop computers with the following software installed:

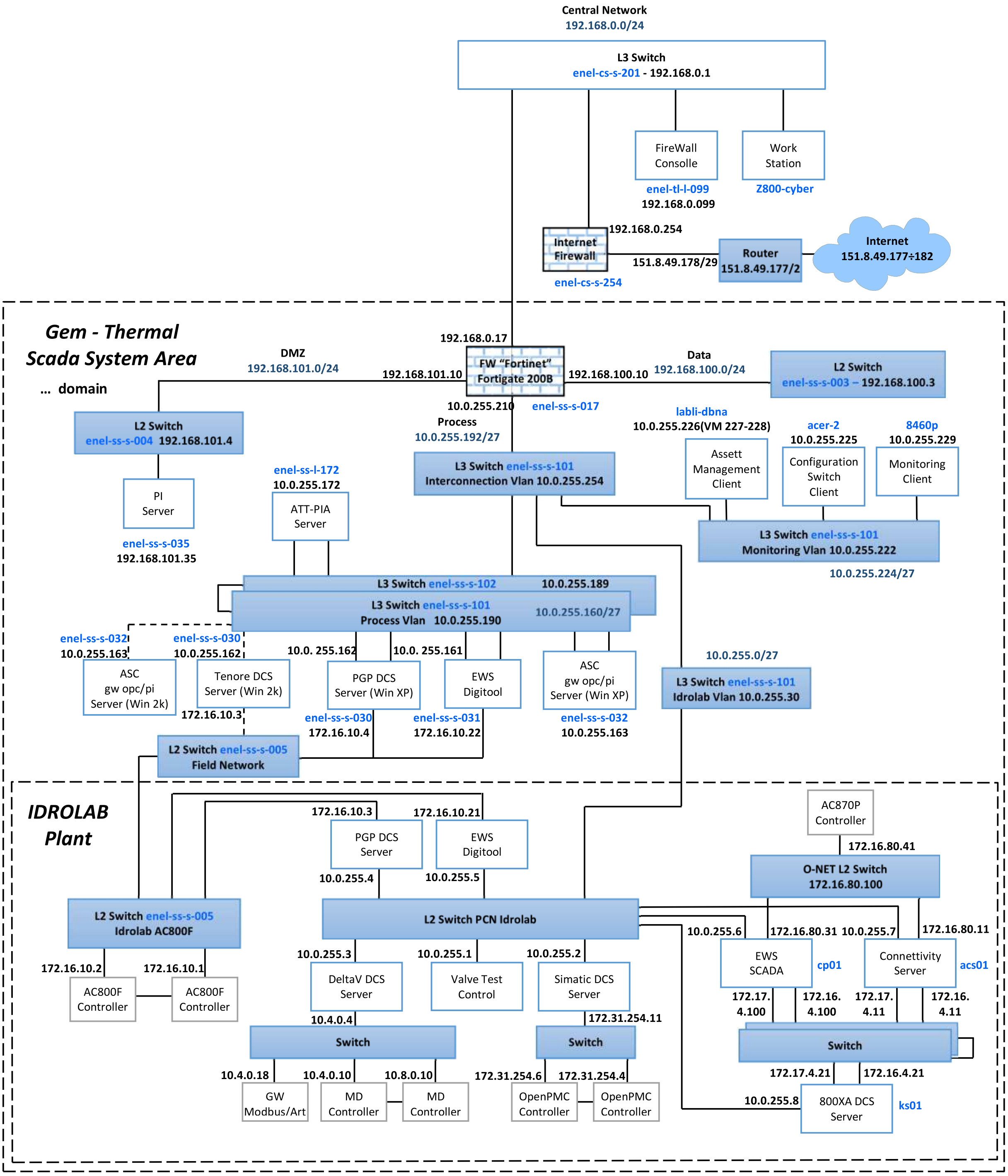

FIGURE 10 Network diagram of the Enel cybersecurity laboratory testing environment.

- *JADE (ver. 4.3.3)* – an agent platform i.e. the middleware that enables deployment and operation of agent systems,
- *VirtualBox (ver. 4.3.30)* – an emulation software that enables the creation of virtual machines – emulated computer systems that very faithfully reproduce original hardware architectures. Several virtual machines can be set up on one physical device, each well separated from the underlying computer system.
- *Vagrant (ver. 1.7.2)* – development environments management software that facilitates building and replication of testing system configurations.

- *Wordpress (ver. 4.2.5)* – the content management system (CMS) used in the experiments to reflect information sharing activities. JSON API and JSON API AUTH libraries are used for integration.
- *Eclipse (ver. Luna 4.4.1)* – a software development environment that facilitates integration with other elements of the development process, including Maven or Git.
- *Maven (ver. 3.2.5)* – a software project management framework. It facilitates project integration, unit testing and project structure definition.
- *Git (ver. 1.9.5)* – a version-control system. It significantly improves the software development process with the support for collaborative development and non-linear workflows as well as enhanced changes tracking.

7.3 | Integrity tests

Integrity tests aimed at verifying correct interoperation of SAN components. The evaluated SAN architecture consisted of the dashboard (see Section 6.1), a SIEM (the AlienVault's OSSIM[136]) and the Argus network analyser[137] together with the Snort Network Intrusion Detection and Prevention System[126] as SAN sensors. In addition, the TCPReplay, Oinkmaster and Barnyard2 open software tools were used to facilitate test performance.

The primary test cases aimed at checking the dashboard operation with the Argus analyser as the data source. During these tests, several problems were identified. All of them related to the processing and visualisation of a large amount of data specific to the power plant environment. Feedback from testing helped developers to identify and fix bugs.

During the second phase of testing, the integration between Snort IDS and Ossim SIEM was examined. While during the deployment and configuration of both systems no issues were encountered, the testing in a larger-scale environment revealed problems with communication between subnets. This was a relatively critical issue, as in real production environments sensors will be dispersed across regions and countries, and their stable and secure connection with the SIEM node is indispensable for providing situational awareness.

The last test cases were designed to evaluate the full integration of the SAN. Communication through all tiers of the SAN architecture was tested. The data collected by sensors were delivered to the SIEM system. There, after the application of data processing and analysis algorithms, alerts were raised and the dashboard was notified. The operator was informed about detected threats through the dashboard widgets. During the tests, several minor issues and bugs were identified, however the overall SAN design proved correct.

7.4 | Usability tests

Usability tests were performed to evaluate the quality of interfaces and human-computer interactions involved in information sharing activities. To enable relative assessments, anonymity architecture-supported (see Section 5.5) message sending was compared to the analogous task performed with Tor Browser[138]. Tor Browser is the most popular anonymisation tool available on the Internet. It adapts a modified version of Mozilla Firefox browser, connected to a proprietary, community-driven network of anonymisation (mix[139]) nodes deployed on the Internet.

There are different opinions regarding the optimal size of the test group for usability tests. Practical approaches suggest users teams of between 5 and 10 members, but certainly the most suitable number depends on the concrete system, laboratory size and equipment and users availability. The tests performed at Gdańsk University of Technology involved 11 participants. Their usability perceptions were measured using the Likert scale, after the comparative analysis of four software usability metrics, namely the System Usability Scale (SUS), Software Usability Measurement Inventory (SUMI), Computer System Usability Questionnaire (CSUQ) and Website Analysis and MeasureMent Inventory (WAMMI).

Each participant was provided with a description of two tasks, separately for the two interfaces i.e. the anonymity architecture and the ToR browser. The first task regarded the installation of the interface, the second – sending of an anonymous message. After the tasks' completion, users were filling in a questionnaire comprising 14 closed-ended and one open-ended question. The closed-ended questions aimed at determining the level of ease of use, impressions regarding the graphical aspects of the interface and other perceptions, using the Likert scale or yes/no answers. The open question was dedicated to suggestions on the improvement of the interfaces.

The tests showed faster completion of the message sending task using the anonymity architecture (see Table 8). At the same time, the majority of users preferred the ToR browser interface, indicating that it is more ’user-friendly’ and ’intuitive’. Consequently, the improvement of the anonymity architecture front-end constitutes a potential subject of further works on the solution.

TABLE 8 The values (in the format: minutes:seconds) of the *time-on-task*[54,53] metric obtained during the usability tests. Performed tasks included: T1.1 – installation of the ToR browser, T1.2 – sending an anonymous message with the ToR browser, T2.1 – installation of the anonymity architecture, T2.2 – sending an anonymous message with the anonymity architecture.

Participant	Task			
	T1.1	T1.2	T2.1	T2.2
1	00:30	02:00	02:00	00:45
2	00:41	02:11	02:30	00:57
3	00:34	01:49	01:52	00:58
4	00:28	01:22	01:00	00:48
5	00:31	02:49	02:43	00:39
6	00:39	02:38	02:07	01:27
7	00:21	02:17	01:18	01:00
8	00:31	03:17	01:48	01:34
9	00:27	02:20	01:36	02:51
10	00:28	02:43	02:14	02:22
11	00:19	02:01	01:15	00:51
Average	00:29	02:18	01:51	01:17

7.5 | Security assessment

The security of the anonymity architecture for the threat intelligence described in Section 5.5 was analysed by verifying the fulfilment of its security objectives, given the assumed network and adversary model[120].

7.5.1 | Security objective

The security objective of the anonymity architecture is as follows:

> *The architecture* ***should*** *allow agent owners to hide (make unreadable to unauthorised parties) the address of the agent’s base station. This obfuscation* ***should*** *not constrain the autonomy of the agent in planning and following its route. Despite the obfuscation, the agent* ***should*** *be able to come back to the base station.*

7.5.2 | Network model

The architecture is dedicated to an agent platform complying to the FIPA specifications[140]. It centres around the aspects of agent mobility (migration between containers) and aims at protecting agents against being followed. It is assumed that in normal conditions (when neither the entire platform nor any of its parts are compromised), the following conditions are satisfied:

A.1. Third parties (agents, users) are not informed about the presence of other agents without their authorisation. It is impossible to introduce agents aiming at observing or following other agents.

A.2. It is impossible to learn the container’s state from outside.

A.3. Each container participating in untraceable migration owns a securely stored individual symmetric key.

A.4. The individual keys are securely generated and stored, and they not available to third parties.

A.5. All cryptographic techniques are correctly implemented and applied providing information computational security, so a computationally bound adversary is unable to subvert these cryptographic techniques.

A.6. Each container is able to provide an agent with the identifier of the previous container visited by the agent. The identifier is destroyed after the agent leaves out.

A.7. This identifier is available to the agent.

7.5.3 | Model of the adversary

The following types of adversaries are considered in the security analysis:

- Internal/external – *external* adversaries compromised communication media that connect containers while *internal* adversaries compromised containers themselves[141].
- Omnipresent/k-listening – *omnipresent* adversaries succeeded in attacking all containers, *k-listening* – *k* of them[142], while *single adversaries* attacked only one container[143].
- Active/passive – *active* adversaries can arbitrarily modify computations and data whereas *passive* adversaries can only read the data[141].
- Static/adaptive – *static* adversaries can choose the resources to compromise only before starting an attack. *Adaptive* adversaries are able to change the resources they control during an attack[141,144].
- Hybrid – hybrids and alliances of adversaries, such as external-active or colluding internal and external[143].

7.5.4 | Analysis

In the analysis, the notation analogous to Syverson's et al.[143] is applied. ac_l denotes the l-th agent container on agent's route (the container passed by the agent as the l-th one). CAC refers to the set of Agent Containers (ACs) compromised by the adversary i.e. the set of Compromised Agent Containers (CAC). N indicates the number of ACs in the mobile agent system (MAS).

When describing the level of achieved confidentiality of the address data, the expressions introduced by Reiter et al.[145], namely *exposed*, *beyond suspicion*, and *hidden* are used. *Exposed* address data are completely readable by an adversary, and the adversary knows (has 100% surety) that the data indicate the base container. Address data *beyond suspicion* refer to an exposed address, which probability of being the base address is not higher than for any other address used in the MAS. *Hidden* address data are not readable by an adversary, under the assumption of their bounded computational power and information computational security of encryption techniques applied in MAS.

The first part of the analysis is dedicated to the core module of the anonymity architecture i.e. the Untraceability Protocol Infrastructure (see Section 5.5).

In reference to the internal adversary, the following three cases need to be examined: 1) The adversary compromised the base station; 2) The adversary compromised the second container; 3) The adversary compromised a further container.

Case 1: An internal adversary compromised the base station.

$$ac_1 \in CAC$$

An internal adversary compromised the agent's base station, can read all agent's information, including the base address. Thus the address is *exposed*.

Case 2: An internal adversary compromised the second container.

$$ac_2 \in CAC$$

An internal adversary located at the second container of an agent's route can read the base address because they can read the address of the previous container. However, since the agent's LIFO queue of encrypted container identifiers is filled with random values, the adversary does not know that they are located at the second container of the agent's route, and consequently that the address of the previous container is the address of the base container. Thus even though the address is *exposed*, it is *beyond suspicion*. It means that for the adversary the probability of the address being the base address is equal to $\frac{1}{N-1}$.

Case 3: An internal adversary compromised any further container.

$$ac_l \in CAC, \quad l \in \langle 3, N \rangle$$

An internal adversary located at any further container of the agent's route can't read the base address. The address (of the previous container) read by the adversary has $\frac{1}{N-1}$ chance to be the address of the base container. Thus address is *hidden*.

As far as an external adversary is concerned, they cannot read the base address. The address is *hidden*. The probability of obtaining the base address is equal to $\frac{1}{N}$.

For k-present adversaries, in the case of *reading* data which is in the scope of this study, k-presence doesn't introduce any additional power to the adversary (except the N-presence describing omnipresent adversaries). The adversary should be respected as a single adversary in relation to the three cases (as for internal adversary):

- The base container was compromised.
- The second on the route container was compromised.
- Any further container of the agent's route was compromised.

For this type of adversary, the same figures as for single adversary are in force.

In the context of the study, the case of the internal omnipresent adversary is homogeneous to the case of the internal adversary compromised base container. Consequently, the external k-present adversary, the same as the single external adversary can't read the base address. The address is *hidden*.

Similarly to k-present adversaries, static adversaries should be considered according to the three cases depicted for analysis of the protocol in reference to internal adversaries. Again, as for k-present adversaries, the figures for single adversary are valid. Adaptive adversaries are out of the scope of the study since their adaptiveness goes beyond the activity of *reading* of agent's data (and implies TA).

According to the security objective, the architecture is required to protect the base address from an adversary able to *read* agents' data. Thus active, adaptive as well as hybrid attackers are excluded from the analysis.

The analysis shows that Module I: Untraceability Protocol Infrastructure fulfils its security objective given the assumed network and the adversary model. It hides (makes unreadable to unauthorised parties) the address of the agent's base station. The results of the study are summarised in Table 9.

Adversary	Internal	External
(a) $ac_1 \in CAC$	$P(A) = 1$	$P(A) = \frac{1}{N}$
(b) $ac_2 \in CAC$	$P(A) = \frac{1}{N-1}$	$P(A) = \frac{1}{N}$
(c) $ac_l \in CAC, \quad l \in \langle 3, N \rangle$	$P(A) = \frac{1}{N-1}$	$P(A) = \frac{1}{N}$

TABLE 9 Module I evaluation: probability $P(A)$ of obtaining the base address in relation to the type of adversary and to the attack scenario: (a) base container was compromised; (b) the second on the route container was compromised; (c) any further container of the agent's route was compromised.

In regard to the second, optional, module of the architecture (the Additional Untraceability Support, see Section 5.5), an alternative security evaluation approach was utilised, based on the list of known attacks. This approach is more suitable for analysing more complex systems. However, with the drawback, that provided security statements are valid only in reference to the attacks in the list. Thus the comprehensiveness of the list of threats plays a crucial role in the study. With this aim in view, a broad study of the relevant literature was conducted. In particular, the anonymity bibliography available at www.freehaven.net/anonbib/ was reviewed. The identified attacks include time correlation, brute force attacks, contextual attacks or active attacks exploiting user reactions[146,147,145,148,142,141]). The study showed that a very powerful adversary, e.g. k-present, may succeed in tracing an agent to its sender. However, such attacks, besides requiring substantial resources, can be countered by enabling successive protection mechanisms of Module II. The details of the study are described in[120]. Another potential approach to the security evaluation could be applying threat model-based security testing. Marback et al.[149] proposed a method where test cases are generated systematically from threat trees. The technique proves very effective in discovering software vulnerabilities. Applying it to the TI framework is a considered direction of further developments.

8 | CONCLUSIONS

The proposed threat intelligence framework aims at providing a comprehensive response to the evolving threat landscape of contemporary energy systems. This is achieved by integrating all levels of TI. At the technical level, situation awareness networks (SANs) interlink Security Information and Event Management (SIEM) systems with heterogeneous sensors deployed in multiple system locations. The sensors, such as intrusion detection tools or network monitors, deliver to the SIEMs precise technical data, which are aggregated and processed to enable operational decisions and actions of security personnel. In addition, at the tactical level of TI, the most critical information is visualised in SAN dashboards and compiled into detailed attack reports which are shared with the TI community or used during the development of countermeasures. The strategic level encompasses the activities of the information sharing and analysis centre (ISAC) and the members of the TI community. There, sectoral cybersecurity strategies and policies are collectively developed, based on the knowledge distributed between stakeholders.

The framework introduces several innovative proposals, including:

- the 3-tier SAN architecture which enhances classical SANs with dashboards to facilitate recognising the anomalies undetectable to automatic systems,
- anonymisation mechanisms that take advantage of the heterogeneity and geographical distribution of TI participants,
- a dedicated data model adapted to the data shared in the energy sector, parts of which are machine-generated,
- data sanitisation rules, to protect shared data by hiding unnecessary details which can be exploited by adversaries,
- data aggregation rules, for processing large amounts of system monitoring data, to extract the essential information useful to human operators,
- energy sector-tailored cybersecurity requirements for the ISP and SAN sensors,
- event correlation rules that enable detecting relations between cybersecurity events or identifying their common source to facilitate recognition of sophisticated cybersecurity threats,
- adapted testing metrics for objective evaluation of the developed framework.

A prototype of the framework was developed and set up to enable its evaluation and experiments. The technical and operational level functions were examined in the Enel cybersecurity laboratory, designed to replicate operational environments associated with power generation. The assessment of higher-level TI was performed in the laboratory at Gdańsk University of Technology. The evaluation allowed for identifying the areas that required further improvements including SAN intra-network communication, data processing and visualisation algorithms or the interface of the anonymity architecture. The latter will be subject to further development activities.

The high-level part of the platform, associated with information exchange was adopted by the European Energy – Information Sharing & Analysis Centre (EE-ISAC). This step enabled preliminary validation of the platform by the stakeholders of the energy sector. Although the general reception was positive (the platform met the expectations of its users), comments gathered during the process will provide a basis for further improvements. Progressively, with the complete adoption of the entire TI framework, its subsequent components will be undergoing further validation by the stakeholders. In addition, the current, informal, user-based validation of the TI platform, could be enhanced with a more formalised approach. Recently, Brucker et al.[150] proposed a software modelling and validation framework that is particularly focused on system security properties. The framework takes advantage of ConSpec – a formal language for policy specification[151], as well as Business Process Model and Notation (BPMN), that provide grounds for structured, systematic system modelling and validation. Moreover, the framework offers security-centric ranking capabilities that enable comparing alternative software systems. This feature could be particularly beneficial with the advent of new, alternative TI platforms, for instance, dedicated to other economic sectors. However, since the main characteristics considered in the assessments enabled by the framework are security, availability and cost, to achieve a more comprehensive view, further software metrics[152,153,54] and selection approaches[154,155] would need to be investigated. For instance, the system selection situation can be represented as a multicriteria decision-making problem (MCDM), for which several solutions are available, including the analytic hierarchy process, the Technique for Order of Preference by Similarity to Ideal Solution (TOPSIS) or data envelopment analysis. This observation was utilised in the development of FOSSES – the Framework for Open-Source Software Evaluation and Selection[154].

9 | ACKNOWLEDGEMENTS

The study presented in this paper is based on work carried out in the DEnSeK (Distributed Energy Security Knowledge) project founded by the European Commission, Directorate-General for Home Affairs (Programme „Prevention, Preparedness and Consequence Management of Terrorism and other Security-related Risks" – CIPS, Project Reference: HOME/2012/CIPS/ AG/ 4000003772) and partially supported from the project funds. It is also supported by the DS Programs of Faculty of Management and Economics and Faculty of Electronics, Telecommunications and Informatics of Gdańsk University of Technology.

References

1. Tounsi W, Rais H. A survey on technical threat intelligence in the age of sophisticated cyber attacks. *Computers and Security*. 2018; 72: 212–233. doi: 10.1016/j.cose.2017.09.001

2. Skopik F, Settanni G, Fiedler R. A problem shared is a problem halved: A survey on the dimensions of collective cyber defense through security information sharing. *Computers and Security*. 2016; 60: 154–176. doi: 10.1016/j.cose.2016.04.003

3. Chen J, Su C, Yeh KH, Yung M. Special Issue on Advanced Persistent Threat. *Future Generation Computer Systems*. 2018; 79: 243–246. doi: 10.1016/J.FUTURE.2017.11.005

4. Sun CC, Hahn A, Liu CC. Cyber security of a power grid: State-of-the-art. *International Journal of Electrical Power & Energy Systems*. 2018; 99: 45–56. doi: 10.1016/J.IJEPES.2017.12.020

5. ENISA. ENISA threat landscape report 2017: 15 Top Cyber-Threats and Trends; 2018.

6. Kushner D. The real story of stuxnet. *IEEE Spectrum*. 2013; 50: 48–53. doi: 10.1109/MSPEC.2013.6471059

7. Falliere N, Murchu LO, Chien E. W32.Stuxnet Dossier. tech. rep., Symantec Security Response; 2011.

8. Das SK, Kant K, Zhang N, Cárdenas AA, Safavi-Naini R. Chapter 25 – Security and Privacy in the Smart Grid. In: Handbook on Securing Cyber-Physical Critical Infrastructure. 2012: 637–654.

9. European Commission. Communication from the commission to the council and the European parliament. Critical Infrastructure Protection in the fight against terrorism COM(2004) 702 final; 2004.

10. The White House. Presidential Policy Directive (PPD)-21 Critical Infrastructure Security and Resilience; 2013.

11. European Commission. Communication from the commission on a European Programme for Critical Infrastructure Protection COM(2006) 786; 2006.

12. Jang-Jaccard J, Nepal S. A survey of emerging threats in cybersecurity. *Journal of Computer and System Sciences*. 2014; 80(5): 973–993. doi: 10.1016/j.jcss.2014.02.005

13. Yang Y, Littler T, Sezer S, McLaughlin K, Wang HF. Impact of cyber-security issues on Smart Grid. In: 2011 2nd IEEE PES International Conference and Exhibition on Innovative Smart Grid Technologies. Manchester, United Kingdom: IEEE; 2011: 1–7.

14. Baker S, Filipak N, Timlin K. In the Dark: Crucial Industries Confront Cyberattacks. tech. rep., McAfee; Santa Clara, California: 2011.

15. He M, Devine L, Zhuang J. Perspectives on Cybersecurity Information Sharing among Multiple Stakeholders Using a Decision-Theoretic Approach. *Risk Analysis*. 2018; 38(2): 215–225. doi: 10.1111/risa.12878

16. Hernandez-Ardieta JL, Suarez-Tangil G, Tapiador JE. Information Sharing Models for Cooperative Cyber Defence. In: 2013 5th International Conference on Cyber Conflict. Tallinn, Estonia; 2013: 60– 87.

17. Meng G, Liu Y, Zhang J, Pokluda A, Boutaba R. Collaborative Security. *ACM Computing Surveys*. 2015; 48(1): 1–42. doi: 10.1145/2785733

18. Vasilomanolakis E, Karuppayah S, Mühlhäuser M, Fischer M. Taxonomy and Survey of Collaborative Intrusion Detection. *ACM Comput. Surv.* 2015; 47(4): 55:1—–55:33. doi: 10.1145/2716260

19. Patel A, Júnior JC, Pedersen JM. An intelligent collaborative Intrusion Detection and Prevention System for Smart Grid environments. *Computer Standards & Interfaces*. 2013.

20. Moriarty KM. Incident coordination. *IEEE Security and Privacy*. 2011; 9(6): 71–75. doi: 10.1109/MSP.2011.164

21. Kamhoua C, Martin A, Tosh DK, Kwiat KA, Heitzenrater C, Sengupta S. Cyber-Threats Information Sharing in Cloud Computing: A Game Theoretic Approach. *Proceedings – 2nd IEEE International Conference on Cyber Security and Cloud Computing, CSCloud 2015 – IEEE International Symposium of Smart Cloud, IEEE SSC 2015*. New York, USA: IEEE; 2016: 382–389. doi: 10.1109/CSCloud.2015.80

22. Alcaraz C, Lopez J. Wide-area situational awareness for critical infrastructure protection. *Computer*. 2013; 46(4): 30–37. doi: 10.1109/MC.2013.72

23. Bartnes Line M, Anne Tøndel I, Jaatun MG. Current practices and challenges in industrial control organizations regarding information security incident management – Does size matter? Information security incident management in large and small industrial control organizations. *International Journal of Critical Infrastructure Protection* 2016; 12: 12–26. doi: 10.1016/j.ijcip.2015.12.003

24. Fuentes dJM, González-Manzano L, Tapiador J, Peris-Lopez P. PRACIS: Privacy-preserving and aggregatable cybersecurity information sharing. *Computers and Security*. 2017; 69: 127–141. doi: 10.1016/j.cose.2016.12.011

25. ENISA. Report on Cyber Security Information Sharing in the Energy Sector. tech. rep., 2016.

26. Stevenson J, Prevost RJ. Securing the Grid: Information Sharing in the Fifth Dimension. *The Electricity Journal*. 2013; 26(9): 42–51. doi: 10.1016/j.tej.2013.10.003

27. Information Sharing & Analysis Centre (EE-ISAC). 2019. https://www.ee-isac.eu/

28. Oil and Natural Gas Information Sharing and Analysis Center (ONG-ISAC). 2019. https://ongisac.org/

29. Kshetri N. Recent US Cybersecurity Policy Initiatives: Challenges and Implications. *Computer*. 2015; 48(7): 64–69. doi: 10.1109/MC.2015.188

30. Franke U, Brynielsson J. Cyber situational awareness - A systematic review of the literature. *Computers and Security*. 2014; 46: 18–31. doi: 10.1016/j.cose.2014.06.008

31. Hilverda F, Kuttschreuter M. Online Information Sharing About Risks: The Case of Organic Food. *Risk Analysis*. 2018; 38(9): 1904–1920. doi: 10.1111/risa.12980

32. Ring T. Threat intelligence: Why people don't share. *Computer Fraud and Security*. 2014; 2014(3): 5–9. doi: 10.1016/S1361-3723(14)70469-5

33. Bourgue R, Budd J, Homola J, Wlasenko M, Kulawik D. Detect, SHARE, Protect Solutions for Improving Threat Data Exchange among CERTs. Tech. Rep. October, 2013.

34. Murdoch S, Leaver N. Anonymity vs. Trust in Cyber-Security Collaboration. In: Proceedings of the 2nd ACM Workshop on Information Sharing and Collaborative Security – WISCS '15. Denver, Colorado, USA: 2015.

35. Peretti K. Cyber Threat Intelligence: To Share or Not to Share – What Are the Real Concerns? *Privacy and Security Law Report*. 2014: 1–8.

36. Chismon D, Ruks M. Threat Intelligence: Collecting, Analysing, Evaluating. tech. rep., MWR InfoSecurity Ltd; 2015.

37. Choo KKR. The cyber threat landscape: Challenges and future research directions. *Computers and Security*. 2011; 30(8): 719–731. doi: 10.1016/j.cose.2011.08.004

38. Richards K. The Australian Business Assessment of Computer User Security: a National Survey. *Research and public policy series No. 102.*. 2009: 1–102.

39. Ponemon Institute. Second Annual Study on Exchanging Cyber Threat Intelligence: There Has to Be a Better Way. tech. rep., Ponemon Institute; 2015.

40. Sillaber C, Sauerwein C, Mussmann A, Breu R. Data Quality Challenges and Future Research Directions in Threat Intelligence Sharing Practice. In: Proceedings of the 2016 ACM on Workshop on Information Sharing and Collaborative Security - WISCS'16. Vienna, Austria: 2016.

41. Sonnenwald DH. Challenges in sharing information effectively: Examples from command and control. *Information Research*. 2006; 11(4).

42. Seigneur JM, Slagell A. *Collaborative Computer Security and Trust Management*. Advances in Information Security, Privacy, and Ethics. IGI Global; 2010.

43. Dehmer M, Meyer-Nieberg S, Mihelcic G, Pickl S, Zsifkovits M. Collaborative risk management for national security and strategic foresight. *EURO Journal on Decision Processes*. 2015; 3(3-4): 305–337. doi: 10.1007/s40070-015-0046-0

44. Ward D, Kourti N, Lazari A, Cofta P. Trust building and the European Reference Network for Critical Infrastructure Protection community. *International Journal of Critical Infrastructure Protection*. 2014; 7(3): 193–210. doi: 10.1016/j.ijcip.2014.07.003

45. Connolly J, Davidson M, Richard M, Skorupka C. The Trusted Automated eXchange of Indicator Information (TAXII^{TM}). Tech. rep., MITRE Corporation; 2012.

46. Fransen F, Smulders A, Kerkdijk R. Cyber security information exchange to gain insight into the effects of cyber threats and incidents. *e & i Elektrotechnik und Informationstechnik*. 2015; 132(2): 106–112. doi: 10.1007/s00502-015-0289-2

47. Downstream Natural Gas Information Sharing Analysis Center. 2019. https://www.dngisac.com/

48. Jajodia S, Liu P, Swarup V, Wang C. *Cyber situational awareness: advances in information security*. Springer, Berlin; 2010.

49. Tadda GP, Salerno JS. Overview of Cyber Situational Awareness. In: Jajodia S, Liu P, Swarup V, Wang C., eds. *Cyber Situational Awareness*. 46 of *Advances in Information Security*. Boston, MA: Springer US. 2010 (pp. 15–35).

50. Endsley MR, Garland DJ. *Situation Awareness Analysis and Measurement*. CRC Press, Inc.; 2000.

51. Barford P, Dacier M, Dietterich TG, et al. Cyber SA: Situational awareness for cyber defense. In: Jajodia S, Liu P, Swarup V, Wang C., eds. *Cyber Situational Awareness – Issues and Research*. Springer Science+Business Media, LLC.; 2010 (pp. 3–14).

52. Aguirre I, Alonso S. Improving the Automation of Security Information Management: A Collaborative Approach. *IEEE Security & Privacy Magazine*. 2012; 10(1): 55–59. doi: 10.1109/MSP.2011.153

53. Leszczyna R, Małkowski R, Wróbel MR. Testing Situation Awareness Network for the Electrical Power Infrastructure. *Acta Energetica*. 2016; 3(28): 81–87. doi: 10.12736/issn.2300-3022.2016308

54. Bolzoni D, Leszczyna R, Wróbel MR, Wrobel M. Situational Awareness Network for the electric power system: The architecture and testing metrics. In: Ganzha M, Maciaszek L, Paprzycki M., eds. *Proceedings of the 2016 Federated Conference on Computer Science and Information Systems, FedCSIS 2016*. Gdansk, Poland: IEEE; 2016: 743–749

55. Ward L. Building an effective threat intelligence platform that would make Einstein proud. *Computer Fraud and Security*. 2017; 2017(4): 11–12. doi: 10.1016/S1361-3723(17)30031-3

56. Elmellas J. Knowledge is power: the evolution of threat intelligence. *Computer Fraud and Security*. 2016; 2016(7): 5–9. doi: 10.1016/S1361-3723(16)30051-3

57. Anstee D. The great threat intelligence debate. *Computer Fraud and Security*. 2017; 2017(9): 14–16. doi: 10.1016/S1361-3723(17)30099-4

58. Dara S, Zargar ST, Muralidhara VN. Towards privacy preserving threat intelligence. *Journal of Information Security and Applications*. 2018; 38: 28–39. doi: 10.1016/j.jisa.2017.11.006

59. Ahrend JM, Jirotka M, Jones K. On the collaborative practices of cyber threat intelligence analysts to develop and utilize tacit Threat and Defence Knowledge. In: Proceedings of the 2016 International Conference On Cyber Situational Awareness, Data Analytics And Assessment (CyberSA). London, UK: IEEE; 2016: 1–10.

60. Korstanje ME. *Threat mitigation and detection of cyber warfare and terrorism activities*. IGI Global. 2016.

61. Liu D, Ji Y, Mookerjee V. Knowledge sharing and investment decisions in information security. *Decision Support Systems*. 2011; 52(1): 95–107. doi: 10.1016/j.dss.2011.05.007

62. Shapiro C. Exchange of Cost Information in Oligopoly. *The Review of Economic Studies*. 1986; 53(3): 433–446. doi: 10.2307/2297638

63. Kirby AJ. Trade Associations as Information Exchange Mechanisms. *The RAND Journal of Economics*. 1988. doi: 10.2307/2555403

64. Sošić G. Stability of information-sharing alliances in a three-level supply chain. *Naval Research Logistics (NRL)*; 57(3): 279–295. doi: 10.1002/nav.20403

65. Jain A, Seshadri S, Sohoni M. Differential pricing for information sharing under competition. *Production and Operations Management*. 2011; 20(2): 235–252. doi: 10.1111/j.1937-5956.2010.01161.x

66. Gordon LA, Loeb MP, Lucyshyn W. Sharing information on computer systems security: An economic analysis. *Journal of Accounting and Public Policy*. 2003; 22(6): 461–485. doi: 10.1016/j.jaccpubpol.2003.09.001

67. Gal-Or E, Chose A. The economic incentives for sharing security information. *Information Systems Research*. 2005; 16(2): 186–208. doi: 10.1287/isre.1050.0053

68. Hausken K. Information sharing among firms and cyber attacks. *Journal of Accounting and Public Policy*. 2007; 26(6): 639–688. doi: 10.1016/j.jaccpubpol.2007.10.001

69. Gordon LA, Loeb MP, Lucyshyn W, Zhou L. The impact of information sharing on cybersecurity underinvestment: A real options perspective. *Journal of Accounting and Public Policy*. 2015; 34(5): 509–519. doi: 10.1016/j.jaccpubpol.2015.05.001

70. Tosh D, Sengupta S, Kamhoua CA, Kwiat KA. Establishing evolutionary game models for CYBer security information EXchange (CYBEX). *Journal of Computer and System Sciences*. 2018; 98(July 2016): 27–52. doi: 10.1016/j.jcss.2016.08.005

71. Kulikova O, Heil R, Van Den Berg J, Pieters W. Cyber crisis management: A decision-support framework for disclosing security incident information. *Proceedings of the 2012 ASE International Conference on Cyber Security, CyberSecurity 2012*. Washington, DC, USA: IEEE; 2013: 103–112. doi: 10.1109/CyberSecurity.2012.20

72. Boden A, Avram G, Bannon L, Wulf V. Knowledge sharing practices and the impact of cultural factors: reflections on two case studies of offshoring in SME. *Journal of Software: Evolution and Process*. 2012(July 2010);24(2): 139–152. doi: 10.1002/smr.473

73. Rafaeli S, Ravid G. Information sharing as enabler for the virtual team: An experimental approach to assessing the role of electronic mail in disintermediation. *Information Systems Journal*. 2003; 13(2): 191–206. doi: 10.1046/j.1365-2575.2003.00149.x

74. Waring S, Alison L, Carter G, et al. Information sharing in interteam responses to disaster. *Journal of Occupational and Organizational Psychology*. 2018; 91(3): 591–619. doi: 10.1111/joop.12217

75. Stemn E, Bofinger C, Cliff D, Hassall ME. Failure to learn from safety incidents: Status, challenges and opportunities. *Safety Science*. 2018; 101(September 2017): 313–325. doi: 10.1016/j.ssci.2017.09.018

76. Vakilinia I, Sengupta S. A coalitional game theory approach for cybersecurity information sharing. *Proceedings – IEEE Military Communications Conference MILCOM*. Baltimore, MD, USA; IEEE: 2017: 237–242. doi: 10.1109/MILCOM.2017.8170845

77. Tosh D, Sengupta S, Kamhoua C, Kwiat K, Martin A. An evolutionary game-theoretic framework for cyber-threat information sharing. *IEEE International Conference on Communications*. London, UK; IEEE: 2015: 7341–7346. doi: 10.1109/ICC.2015.7249499

78. Ghose A, Hausken K. A Strategic Analysis of Information Sharing Among Cyber Attackers. *Journal of Information Systems and Technology Management*. 2015; 12(2): 245–270. doi: 10.2139/ssrn.928138

79. Nikoofal ME, Zhuang J. On the value of exposure and secrecy of defense system: First-mover advantage vs. robustness. *European Journal of Operational Research*. 2015; 246(1): 320–330. doi: https://doi.org/10.1016/j.ejor.2015.04.043

80. Zhuang J, Bier VM, Alagoz O. Modeling secrecy and deception in a multiple-period attacker-defender signaling game. *European Journal of Operational Research*. 2010. doi: 10.1016/j.ejor.2009.07.028

81. Zhuang J, Bier VM. Reasons for Secrecy and Deception in Homeland-Security Resource Allocation. *Risk Analysis*. 2010. doi: 10.1111/j.1539-6924.2010.01455.x

82. Dighe NS, Zhuang J, Bier VM. Secrecy in defensive allocations as a strategy for achieving more cost-effective attacker deterrence. *International Journal of Performability Engineering*. 2009; 5(1): 31–43.

83. Sedenberg EM, Mulligan DK. Public health as a model for cybersecurity information sharing. *Berkeley Technology Law Journal*. 2015. doi: 10.3945/ajcn.115.110825.Reply

84. Impe KV. How STIX, TAXII and CybOX Can Help With Standardizing Threat Information. 2015. https://securityintelligence.com/how-stix-taxii-and-cybox-can-help-with-standardizing-threat-information/

85. US-CERT. Information Sharing Specifications for Cybersecurity. 2013. https://www.us-cert.gov/Information-Sharing-Specifications-Cybersecurity

86. Qamar S, Anwar Z, Rahman MA, Al-Shaer E, Chu BT. Data-driven analytics for cyber-threat intelligence and information sharing. *Computers and Security*. 2017; 67: 35–58. doi: 10.1016/j.cose.2017.02.005

87. MITRE. CVE – Common Vulnerabilities and Exposures (CVE). 2019. https://cve.mitre.org/

88. Vakilinia I, Tosh DK, Sengupta S. Privacy-Preserving Cybersecurity Information Exchange Mechanism. In: 2017 International Symposium on Performance Evaluation of Computer and Telecommunication Systems (SPECTS). Seattle, WA, USA; IEEE: 2017: 1–7.

89. Jajodia S, Noel S, Kalapa P, Albanese M, Williams J. Cauldron: Mission-centric cyber situational awareness with defense in depth. *Proceedings - IEEE Military Communications Conference MILCOM*. Baltimore, MD, USA; IEEE: 2011: 1339–1344. doi: 10.1109/MILCOM.2011.6127490

90. Locasto ME, Parekh JJ, Keromytis AD, Stolfo SJ. Towards collaborative security and P2P intrusion detection. In: Proceedings from the 6th Annual IEEE System, Man and Cybernetics Information Assurance Workshop, SMC 2005. West Point, NY, USA; IEEE: 2005: 333–339.

91. Zhang T, Zhu Q. Distributed Privacy-Preserving Collaborative Intrusion Detection Systems for VANETs. *IEEE Transactions on Signal and Information Processing over Networks*. 2018; 4(1): 148–161. doi: 10.1109/TSIPN.2018.2801622

92. Patel A, Alhussian H, Pedersen JM, Bounabat B, Júnior JC, Katsikas S. A nifty collaborative intrusion detection and prevention architecture for Smart Grid ecosystems. *Computers and Security*. 2017; 64: 92–109. doi: 10.1016/j.cose.2016.07.002

93. Abdellatif T, Mosbah M. Efficient monitoring for intrusion detection in wireless sensor networks. *Concurrency and Computation: Practice and Experience*. 2017: e4907. doi: 10.1002/cpe.4907

94. Liu X, Zhu P, Zhang Y, Chen K. A Collaborative Intrusion Detection Mechanism Against False Data Injection Attack in Advanced Metering Infrastructure. *IEEE Transactions on Smart Grid*. 2015; 6(5): 2435–2443. doi: 10.1109/TSG.2015.2418280

95. Liu P, Chetal A. Trust-based secure information sharing between federal government agencies. *Journal of the American Society for Information Science and Technology*. 2005; 56(3): 283–298. doi: 10.1002/asi.20117

96. Carter J, Bitting E, Ghorbani A. Reputation Formalization for an Information–Sharing Multi–Agent System. *Computational Intelligence*. 2002; 18(4). doi: 10.1111/1467-8640.t01-1-00201

97. AlienVault. AlienVault Open Threat Exchange (OTX). 2019. https://www.alienvault.com/open-threat-exchange

98. MISP – Open Source Threat Intelligence Platform & Open Standards For Threat Information Sharing. 2019. http://www.misp-project.org/index.html

99. Wagner C, Dulaunoy A, Wagener G, Iklody A. MISP: The Design and Implementation of a Collaborative Threat Intelligence Sharing Platform. In: Proceedings of the 2016 ACM on Workshop on Information Sharing and Collaborative Security. Vienna, Austria; ACM: 2016: 49–56.

100. ThreatView. Cyber Threat & Reputation Intelligence. 2019. www.threatview.ca

101. Mutemwa M, Mtsweni J, Mkhonto N. Developing a cyber threat intelligence sharing platform for South African organisations. *2017 Conference on Information Communication Technology and Society, ICTAS 2017 - Proceedings*. Umhlanga, South Africa; IEEE: 2017. doi: 10.1109/ICTAS.2017.7920657

102. Kaufmann H, Hutter R, Skopik F, Mantere M. A structural design for a pan-European early warning system for critical infrastructures. *e & i Elektrotechnik und Informationstechnik*. 2015; 132(2): 117–121. doi: 10.1007/s00502-015-0286-5

103. Barth R, Meyer-Nieberg S, Pickl S, Schuler M, Wellbrink J. A toolbox for operational analysis. In: Society for Computer Simulation International; 2012; Orlando, Florida, USA: 106–113.

104. Brunner M, Hofinger H, Roblee C, Schoo P, Todt S. Anonymity and privacy in distributed early warning systems. In: Critical Information Infrastructures Security. 6712 LNCS. Springer, Berlin, Heidelberg; 2011: 81–92.

105. ECOSSIAN. European COntrol System Security Incident Analysis Network (ECOSSIAN) Project Website. 2019. http://ecossian.eu/

106. Klump R, Kwiatkowski M. Distributed IP watchlist generation for intrusion detection in the electrical smart grid. *IFIP Advances in Information and Communication Technology*. 2010; 342 AICT: 113–126. doi: 10.1007/978-3-642-16806-2_8

107. Leszczyna R, Wróbel MR. Data Model Development for Security Information Sharing in Smart Grids. *International Journal for Information Security Research*. 2014; 4: 479–489.

108. Debar H, Curry D, Feinstein B. RFC 4765 – The intrusion detection message exchange format (IDMEF). 2007. https://www.ietf.org/rfc/rfc4765.txt

109. Danyliw R, Meijer J, Demchenko Y. RFC 5070 - The Incident Object Description Exchange Format (IODEF). 2007. https://tools.ietf.org/html/rfc5070

110. ISO. ISO 15836:2009 – Information and documentation – The Dublin Core metadata element set. 2009.

111. DCMI. Dublin Core Metadata Initiative. 1995. http://dublincore.org/

112. Leszczyna R, Wrobel MR. Security information sharing for smart grids: Developing the right data model. In: The 9th International Conference for Internet Technology and Secured Transactions (ICITST-2014). London, UK; IEEE: 2014: 163–169.

113. Crawford R, Bishop M, Bhumiratana B, Clark L, Levitt K. Sanitization models and their limitations. In: Proceedings of the 2006 Workshop on New security Paradigms. Schloss Dagstuhl, Germany; ACM: 2007: 41–56.

114. Bishop M, Cummins J, Peisert S, et al. Relationships and data sanitization: a study in scarlet. In: NSPW '10 Proceedings of the 2010 New Security Paradigms Workshop. Concord, Massachusetts, USA; ACM: 2010: 151–164.

115. Valdes A, Fong M, Skinner K. Data cube indexing of large-scale Infosec repositories. SRI International: 2006. http://www.csl.sri.com/papers/AusCERT_2006/

116. Edgar D. Data Sanitization Techniques. Tech. rep., Net 2000; 2004. http://www.orafaq.com/papers/data_sanitization.pdf

117. Leszczyna R, Wrobel MRM, Malkowski R. Security requirements and controls for incident information sharing in the polish power system. In: Proceedings - 2016 10th International Conference on Compatibility, Power Electronics and Power Engineering, CPE-POWERENG 2016. Bydgoszcz, Poland; IEEE: 2016: 94–99.

118. Pfitzmann A, Hansen M. A terminology for talking about privacy by data minimization: Anonymity, Unlinkability, Undetectability, Unobservability, Pseudonymity, and Identity Management. 2010. http://dud.inf.tu-dresden.de/Anon_Terminology.shtml

119. Leszczyna R. Anonymity Architecture for Mobile Agent Systems. In: Mařík V, Vyatkin V, Colombo AW., eds. *Holonic and Multi-Agent Systems for Manufacturing*. 4659 of *Lecture Notes in Computer Science*. Heidelberg, Germany: Springer Berlin Heidelberg. 2007 (pp. 93–103).

120. Leszczyna R, Górski J. An Untraceability Protocol for Mobile Agents and Its Enhanced Security Study. In: 15th EICAR Annual Conference Proceedings. Hamburg, Germany; ESAT (Ecole SupÃľrieure et d'Application des Transmissions): 2006: 26–37.

121. Leszczyna RR, Górski J. Untraceability of mobile agents. In: Proceedings of the fourth international joint conference on Autonomous agents and multiagent systems – AAMAS '05. Utrecht, the Netherlands; ACM: 2005; 3: 1233. doi: 10.1145/1082473.1082709

122. Leszczyna R, Łosiński M, Małkowski R. Security Information Sharing for the Polish Power System. In: Proceedings of the Modern Electric Power Systems 2015 – MEPS 2015. Wroclaw, Poland; IEEE: 2015; : 163 – 169.

123. Gray RS, Kotz D, Cybenko G, Rus D. Mobile Agents: Motivations and State-of-the-Art Systems. Tech. Rep. TR2000-365, Dartmouth College; Hanover, NH: 2000.

124. Odell J. Introduction to Agents. Tech. rep.; 2000. http://www.objs.com/agent/agents_omg.pdf

125. Leszczyna R, Wrobel MR. Evaluation of open source SIEM for situation awareness platform in the smart grid environment. In: 2015 IEEE World Conference on Factory Communication Systems (WFCS). Palma de Mallorca, Spain; IEEE: 2015: 1–4.

126. CISCO. Snort – Network Intrusion Detection & Prevention System. https://www.snort.org/

127. Zhou Z. The study on network intrusion detection system of Snort. In: 2010 International Conference on Networking and Digital Society. Wenzhou, China; IEEE: 2010: 194–196.

128. OISF. Suricata – Open Source IDS / IPS / NSM engine. 2019. http://suricata-ids.org/

129. The Bro Network Security Monitor. 2016. https://www.bro.org/

130. Varadarajan GK. Web Application Attack Analysis Using Bro IDS. Tech. rep.; SANS Institute: 2012. https://www.sans.org/reading-room/whitepapers/detection/web-application-attack-analysis-bro-ids-34042

131. Science Applications International Corporation . Intrusion Detection System System Protection Profile Version 1.4. Tech. rep.; National Security Agency, USA: 2002.

132. Science Applications International Corporation . Intrusion Detection System Sensor Protection Profile Version 1.2. Tech. rep.; National Security Agency, USA: 2005.

133. Science Applications International Corporation . Intrusion Detection System Scanner Protection Profile Version 1.2. Tech. rep.; National Security Agency, USA: 2005.

134. Science Applications International Corporation . Intrusion Detection System Analyzer Protection Profile Version 1.2. Tech. rep.; National Security Agency, USA: 2005.

135. Leszczyna R. Standards on Cyber Security Assessment of Smart Grid. *International Journal of Critical Infrastructure Protection*. 2018; 22: 70–89. doi: 10.1016/j.ijcip.2018.05.006

136. AlienVault. OSSIM: Open Source SIEM. 2019. https://www.alienvault.com/products/ossim

137. Argus – The All Seeing – System and Network Monitoring Software. 2019. http://argus.tcp4me.com/

138. Tor Project. Tor Browser. 2019. https://www.torproject.org

139. Chaum D. Untraceable electronic mail, return addresses, and digital pseudonyms. *Communications of the ACM*. 1981; 4(2).

140. Foundation for Intelligent Physical Agents (FIPA) . FIPA Abstract Architecture Specification. 2002. http://www.fipa.org/specs/fipa00001/

141. Raymond JF. Traffic Analysis: Protocols, Attacks, Design Issues and Open Problems. In: Federrath H. , ed. *Designing Privacy Enhancing Technologies: Proceedings of International Workshop on Design Issues in Anonymity and Unobservability*. Berkeley, California, USA; Springer-Verlag: 2001: 10–29.

142. Dolev S, Ostrobsky R. Xor-trees for efficient anonymous multicast and reception. *ACM Transactions on Information Systems Secururity*. 2000; 3(2): 63–84.

143. Syverson P, Tsudik G, Reed M, Landwehr C. Towards an analysis of onion routing security. In: Federrath H. , ed. *Proceedings of Designing Privacy Enhancing Technologies: Workshop on Design Issues in Anonymity and Unobservability*. Berkeley, California, USA; Springer-Verlag: 2001: 96–114.

144. Lindell Y. Foundations of Cryptography 89-856. Tech. rep.; 2006. http://u.cs.biu.ac.il/ lindell/89-856/complete-89-856.pdf

145. Reiter M, Rubin A. Crowds: Anonymity for Web Transactions. *ACM Transactions on Information and System Security*. 1998; 1(1).

146. Kesdogan D, Egner J, Büschkes R. Stop-and-Go MIXes: Providing Probabilistic Anonymity in an Open System. In: Proceedings of Information Hiding Workshop (IH 1998). 1525 of *Lecture Notes in Computer Science*. Portland, Oregon, USA; Springer-Verlag: 1998.

147. Goldberg I, Wagner D. TAZ servers and the rewebber network: Enabling anonymous publishing on the world wide web. *First Monday*. 1998; 3(4).

148. Mazières D, Kaashoek MF. The Design, Implementation and Operation of an Email Pseudonym Server. In: Proceedings of the 5th ACM Conference on Computer and Communications Security (CCS 1998). San Francisco, California, USA; ACM Press: 1998.

149. Marback A, Do H, He K, Kondamarri S, Xu D. A threat model-based approach to security testing. *Software: Practice and Experience*. 2013; 43(2): 241–258. doi: 10.1002/spe.2111

150. Brucker AD, Zhou B, Malmignati F, Shi Q, Merabti M. Modelling, validating, and ranking of secure service compositions. *Software: Practice and Experience*. 2017; 47(12): 1923–1943. doi: 10.1002/spe.2513

151. Aktug I, Naliuka K. ConSpec – A formal language for policy specification. *Science of Computer Programming*. 2008; 74(1-2): 2–12. doi: 10.1016/j.scico.2008.09.004

152. Kumar V, Sharma A, Kumar R, Grover PS. Quality aspects for component-based systems: A metrics based approach. *Software: Practice and Experience*. 2012. doi: 10.1002/spe.1153

153. Cruz D, Wieland T, Ziegler A. Evaluation criteria for free/open source software products based on project analysis. *Software Process Improvement and Practice*. 2006; 11(2): 107–122. doi: 10.1002/spip.257

154. Adewumi A, Misra S, Omoregbe N, Sanz LF. FOSSES: Framework for open-source software evaluation and selection. *Software: Practice and Experience*. 2019(September 2018): 1–33. doi: 10.1002/spe.2682

155. Jadhav AS, Sonar RM. Framework for evaluation and selection of the software packages: A hybrid knowledge based system approach. *Journal of Systems and Software*. 2011; 84(8): 1394–1407. doi: 10.1016/j.jss.2011.03.034

How to cite this article: Leszczyna R., Wróbel M. R. (2019), Threat intelligence platform for the energy sector, *Softw Pract Exper. 2019;00:1–6*.