Proceedings of the 19th Conference on Computer Science and Intelligence Systems (FedCSIS) pp. 591–596
DOI: 10.15439/2024F8106
ISSN 2300-5963 ACSIS, Vol. 39

Dynamic Threat Intelligence for Improvement of Resilience of Critical Infrastructure During Pandemics

Pablo de Juan Fidalgo
0000-0003-1347-6000
Eviden Spain, Albarracin 25, 28037 Madrid, Spain, Email: pablo.dejuan@eviden.com

Aljosa Pasic
0000-0003-0150-5732
Eviden Spain, Albarracin 25, 28037 Madrid, Spain
Email: aljosa.pasic@eviden.com

Susana Gonzalez Zarzosa
0000-0002-3402-2385
Eviden Spain, Albarracin 25, 28037 Madrid, Spain, Email: susana.gzarzosa@eviden.com

***Abstract*— The COVID-19 pandemic is an example of a temporary situation when critical infrastructure (CI) operators had to operate with continuously changing conditions. The role of cyber infrastructure during pandemics, for example for the remote work or access to critical systems, has also changed. This resulted in frequent re-evaluation of risks and adaptations of security policies or mitigation measures. Use and sharing of cyber threat intelligence (CTI) proved to be valuable to stay up to date, but challenges related to trust and confidence emerged. We designed and developed dynamic CTI to be used by CI operators for risk reassessment and improvement of resilience. Several enhancements will be validated in the forthcoming pilots in SUNRISE project.**

***Index Terms*—Cybersecurity, cyber resilience, threat intelligence, critical infrastructure, pandemics.**

I. Introduction

RESILIENCE is a concept that originally comes from disaster and crisis management and is closely related to efforts to analyse and manage preparedness, but also resistance and recovery from adverse events. It refers to the ability of a system, community, or society to resist, absorb, accommodate to, and recover from the effects of a hazard or incident. It is also characterized by "changing conditions" and "deliberate attacks", especially if we move to cybersecurity resilience definitions [1, 2]. When it comes to general characteristics of resilience, described in [3], these include uncertainty and dynamism in different circumstances, as well as complexity and difficulty to measure. These are especially challenging for the resilience of complex and interconnected systems such as Critical Infrastructures (CIs). In this context, we can mention many EU efforts, starting from the European program for critical infrastructure protection (Directive 2008/114 [4]), which establishes a procedure for identifying and designating European CI, to a more recent Directive on the Resilience of Critical Entities (CER Directive, PE-CONS 51/22 [5]) that entered into force on 16 January 2023. There are several slightly different definitions of CIs or Critical Entities (CEs) but for the purpose of simplicity (and because Member States have until 17 October 2024 to adopt national legislation to transpose the CER Directive), we will keep term CIs. In contrast to the previous approach, with more focus on prevention and mitigation, CER directive also focuses on the response and the rapidity of recovery during and after the event.

During the COVID-19 pandemic, we have seen what the consequences are not only for the healthcare system, but equally as much for other interdependent CI entities. The functioning of CIs was highly unpredictable due to the multitude interdependencies, including interruptions in supply chain, effects on essential employees both physically and mentally, or changes of organizational priority and incident response strategy. To address these challenges, SUNRISE research and innovation project was co-funded by the European Commission and started in November 2022 with a duration of 36 months. Project activities are executed by a consortium of 42 partners from different countries and are considering research activities, as well as the integration and adaptation of relevant tools and practices related to CI resilience, based on the lessons learned from pandemics, such as interlinking of different types of risk inputs and indicators. The SUNRISE strategy consists of distinctive missions, one of them being awareness of the dynamic threat landscape related to and implied by pandemics. One of the key results of SUNRISE project to accomplish this mission is an integral cyber-physical resilience (CPR) tool composed of:

- AI-based anomaly detector (AD) that analyses log files from different CI systems and components.
- Enhanced cyber threat intelligence (CTI) platform and sharing service for (CI) operators.
- Semi-automated risk assessment engine, extended to include physical risk indicators, models that correspond to pandemic-specific strategies of CI operators, as well as temporary condition changes.
- Incident response and reporting management that takes inputs from other tools, including legacy tools, and considers incident reporting thresholds and

workflows that are compliant with EU and national legislation for CI.

There are several innovations in each part of CPR, which are also described in a previous paper about CPR architecture [6]. In this paper we will focus on concepts and design of enhancements of CTI platform, some of which are related to pandemics scenarios of adaptivity, collaboration and absenteeism, while others are applicable to CTI in any context and conditions. We start with the description of related work, before addressing conceptual design and implementation of enhancements. Since these are related to threat intelligence and model, we also explain links to the main risk and resilience concepts, such as calculation of probabilities. We briefly cover validation, which is still in progress and finish with conclusions.

II. RELATED WORK

ENISA launched already in 2010, a study on Measurement Frameworks and Metrics for Resilient Networks and Services. The methodology included both a survey, a desktop research and further consultation [7], as well as supportive taxonomy issued in 2011 [8]. In [9] authors deal with challenge of representing interconnections among system components across operational domains (physical, information, cognitive, or social) and present the cyber resilience matrix with four capacities (plan and prepare/absorb/recover/adapt) and four domains. None of these works addresses the use and sharing of threat intelligence and its impact on resilience.

In some of our previous works ([10],[11],[12]) several enhancements of threat intelligence platform, and enhancement of operational threat indicators have been described. The platform receives structured cyber threat information from multiple sources and performs the correlation with both static and dynamic data coming from the monitored infrastructure. This allows the evaluation of a threat score through heuristic-based analysis, used for enriching the information received from open-source intelligence (OSINT) and other sources. While these remain relevant and useful, in fast changing temporary conditions, such as during pandemics, there is a need for further adaptation to have dynamic adaptation of parameters used threat intelligence trust scoring or source confidence.

In addition, experience with COVID-19 showed that both closed community-based platforms, as well as social media platforms were used to share news, ideas, or opinions, which enabled data processing to serve more efficient and valuable pandemics surveillance. Data derived from related health trends can help to predict workforce availability or absenteeism, and in this way improve critical infrastructure (CI) risk assessment during pandemics. Collaboration between various public health stakeholders, for example, is exemplified in Epidemic Intelligence from Open Sources (EIOS) initiative [13], regional monitoring [14] or European Centre for disease prevention and control (ECDC) project that performs epidemic intelligence [15] for early detection, verification, assessment, and communication of health threats. The use of crowdsourced OSINT as an alternative to commercial or community-based threat intelligence, is also explored and described in many papers, for example its effectiveness in malware detection which is described in [16], or crowdsourced support for discovery and verification of OSINT sources [17]. Confidence in sources and threat score proved to be one of the biggest challenges, especially due to the context and dynamics of temporary situations.

In our work we use open-source Malware Information Sharing Platform (MISP) platform [18] as a basis for our CTI tool. There was already work on COVID-19 MISP instance focusing on three areas of sharing: medical information, cyber threats related to COVID-19 and disinformation about COVID-19. In addition, MISP taxonomies [19] and tools for mapping and a comprehensive checklist of activities related to MISP implementation in the context of COVID-19 that cut across critical domains [20], have also been developed and offered free of charge. This information sharing community has a low barrier of entry, and everyone can contribute or use the data, which is one of the reasons why in SUNRISE we conceptualized and developed CTI tool with fine grained data sharing policy, as well as dynamic threat scoring and source confidence detection.

III. CPR DESIGN AND CTI TOOL ENHANCEMENTS

In this chapter, our focus of enhancements is threat intelligence scoring module, that was extended with source confidence evaluation for better management of intelligence sources, mapping of Indicators of Compromise (IoCs) with MITRE ATT&CK matrix techniques and sharing of contextual events and temporary conditions that are related and relevant for pandemics (e.g. absenteeism, workforce availability prediction, etc). However, since CTI is used as a module within CPR, we will also describe some of CPR concepts.

A. Conceptual Design

During temporary unforeseen circumstances like pandemics, the availability of qualified staff may fluctuate, potentially impacting the credibility of certain sources within the CTI ecosystem. This fluctuation exemplifies the necessity for adaptivity, where systems must dynamically adjust their trust assessments based on evolving contextual factors. The dynamic adjustment of score confidence allows CTI systems to recalibrate their trust scores in real-time, accounting for changes in source reliability and relevance. We argue that for the fast-changing cybersecurity landscape, and contextualization of the available information in changing circumstances, approach based on Observe, Orient, Decide, Act (OODA) loop is more appropriate than predominant Plan, Do, Check, Act (PDCA) approach.

In the practical application of this approach, we start from what is available among observation sources: types of data or assessments that already exist in CI operators that act as SUNRISE project users. In parallel we develop an idea about what is desirable for CPR tool in general and CTI

enhancement in particular, especially for the orientation and decision phase of OODA loop. We proceed with a theoretic model that links different observed or inferred data/events (from log files, network, external threat sources, surveys, manual inputs etc.) with two level orientation and decision assessments (Figure 1):

- strategic/tactical level, dealing with priorities, asset values etc
- operational level, with rule-based assessments and incident response

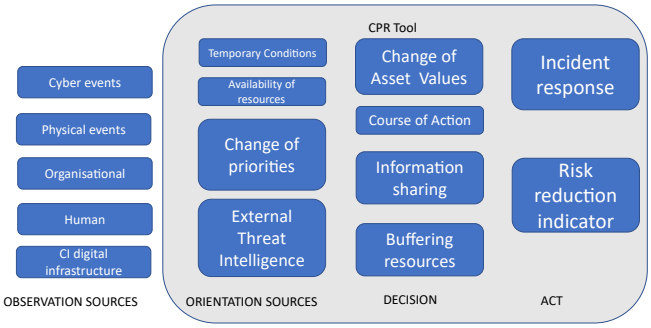

Fig 1. Mapping of CPR tool Conceptual Design to OODA loop

There are many possible enhancements in orientation phase, where external threat intelligence can be used. The effectiveness of security controls may decrease due to temporary changes in another CI (e.g. due to the disruption of supply chain or workforce availability). The threat environment or the technical environment (e.g., the introduction of new technologies in CI digital infrastructure such as pandemic-specific access control equipment) also change. In parallel, the relative priorities of cyber resiliency objectives may shift based on inputs from other stakeholders, current concerns, or available resources and funding.

B. Link of CTI to Risk Assessment and Threat Model

The risk assessment module takes into consideration several types of inputs, both static and real-time. These come from observation and orientation sources. For example, inputs related to the operational context model (business profile, sector specific inputs such as supply chain, human resources etc) are static and come from the relevant employees. Target asset model also uses static inputs about e.g. asset value, asset connectivity etc. Both types of inputs have separated user interfaces, but these can be changed through a new option in dashboard for “temporary conditions” which overwrites the default values. Application, which collects health-related data of citizens, will typically have higher asset value in temporary model, which overwrites its default value, and therefore increases impact and related risks. Similar holds for absenteeism prediction input that might increase vulnerabilities value in assets operated by absent employees, and therefore related risks would also increase.

Unlike static inputs, real data ingestion model does not depend on temporary conditions. This data is provided by the existing cybersecurity tools, such as intrusion detection system (IDS), security event and information management system (SIEM), physical access events and others.

Selection of threat models was done by using MITRE ATT&CK knowledge base of adversary tactics and techniques based on real-world observations. ATT&CK framework is also used to build detailed attack emulation scenarios and to verify that the events collected by agents and analytics can be used as risk indicators and mapped into risk models. In the case of a highly protected and controlled environment, such as in CI, tactic such as privilege escalation can be an objective with associated technique such as access token manipulation or theft. With escalated privileges, an adversary could, for example, program the mobile device to impersonate USB devices such as input devices (keyboard and mouse), storage devices, and/or networking devices. Other examples of physical events and human errors could include attempt to exfiltrate data or insert ransomware/malware over a USB connected to a physical device, or “shoulder surfing”, which in SUNRISE is detected by means of video processing and is fed into the risk assessment module. Combination with IoC received about phishing attacks in organisations that work as a supplier to CI operator, could, for example, reveal that attack on CI core system is in preparation.

Each threat is usually associated with several inputs, that could be further linked to specific questions for questionnaire or detection by some cybersecurity tools. For example, Phishing and Impersonation Attacks questions are: Are employees aware and trained against Phishing? Is multi-factor authentication (MFA) implemented for user login? Is the account locked or did you have too many login attempts? Is there an unusual user behaviour or pattern?

C. Threat Intelligence Engine Architecture

In [6] the CPR architecture, that includes CTI module, was described, based on the main outcomes of the initial project workshops, whose objective was to understand the circumstances in which the CI operators and authorities found themselves during the COVID- 19 pandemic. In this paper we give a more detailed architecture of CTI module that includes proposed enhancements for “orientation” phase. CTI module is based on open source from MISP Project.

Threat Intelligence Engine (TIE) is the IoC enhancement module that acquires events from the MISP instance and generates a threat score. This score can be divided into two parts: the initial segment is public, as it is founded on open-source data, and it gauges the threat based on diverse metrics like timeliness, trending, and completeness. The second segment, which is private, encompasses these metrics along with the relevance heuristic that factors in CI infrastructure data. To shield against potential information leaks, this segment is encrypted, particularly due to the criticality of its assessment of the infrastructure’s vulnerability against threats. Exposure of this information could have severe consequences, enabling attackers to exploit vulnerabilities

and target the entity. By partitioning the score, we adhere to the principle of sharing data through the public channels (see also Article 29, Cybersecurity information-sharing arrangements and Article 30, Voluntary notification of relevant information, of Network and Information Security – NIS 2 directive [21]), while simultaneously safeguarding the organization's confidential data by encrypting it. Concurrently, we augment the received event's contextual information, procedure referred to as CTI enrichment, described in Figure 2.

The central part of TIE is the Heuristic Engine. It processes API requests containing MISP Events and computes the score by considering information about the critical infrastructure and dynamic data such as events, alerts, vulnerability assessments, temporary conditions etc.

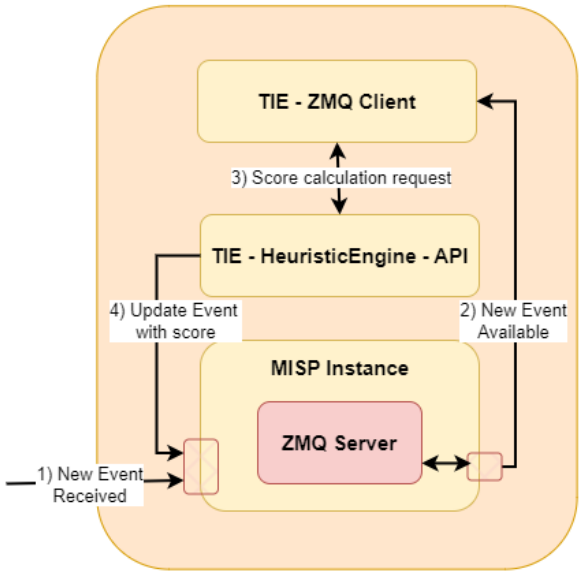

Fig 2. TIE architecture

Subsequently, this score is integrated as an event attribute, updating the MISP Event within the MISP Instance. The second element in TIE's architecture is the ZeroMQ client. A MISP Instance can be configured with a ZeroMQ Server, which has several advantages. The ZMQ Client is established as part of TIE and subscribes to the MISP Instance's ZMQ queue. When a fresh event arrives, the client sends a request to the Heuristic Engine component. This action triggers the execution of heuristic functions that enhances intelligence and ultimately leads to the threat score computation.

TIE currently does not encompass all MISP objects; instead, it concentrates on four specific objects (domain-ip, vulnerability, file, btc-address) considered highly valuable in the realm of threat intelligence and that comprise various attributes, including required and optional ones, which later contribute to the heuristics' calculations and allow the operator to operator to track the main sightings of an attack.

D. CTI enhancements implementation

CTI module, that facilitates secure CTI exchange and enhances cyber-physical risk calculation, has several layers that includes authentication, transport, and privacy/enrichment. The Orchestrator facilitates communication among modules and provides an API for user interaction. The WEB-GUI simplifies tool usage and integrates authentication mechanisms. The new functionality "Source Confidence Calculation" has been implemented and operates in three different modes. Furthermore, admiralty taxonomy is integrated into IoC decay calculation, adjusting IoC significance based on taxonomy classification. Another important feature that has been integrated is the ability to enrich IoC with techniques from the MITRE ATT&CK matrix. Prediction of workforce absenteeism for posterior integration of related intelligence in decisions, such as team assignment, prioritization or calculations of confidence in data sources, is also a new feature from the previous iteration of this component.. It leverages on open-source data, such as anomalies in the number of social network or search engine queries related to health topics, so that CI operators may be able to predict whether their workforce is likely to be unavailable to attend to their workplace due to illness.

E. Assumptions and Constraints

One of the key steps in CPR tool is to identify and map candidate risk mitigations, both to general tactics, techniques and procedures (TTP) from MITRE ATT&CK framework, as well as to security controls specifically applicable to a particular CI. The existing mitigation measure and cyber resiliency controls mappings to ATT&CK techniques are based on engineering analysis rather than on operational experience. In operation settings, risk reduction, and in consequence resilience improvement, will depend on how the controls are specified, how they are implemented, and how the implementation is used. In addition, only the direct effects that a given control are considered. Indirect effects are not considered, while other criteria for the selection of mitigation measures (cost of measure implementation, damage or side-effects) are not considered in this iteration of tool.

F. (Re) Calculation of probabilities, based on CTI

The system was adapted to dynamically update the source's confidence level. The Threat Scoring Model, that contains four heuristics (extensiveness, timeliness, completeness and whitelist overlap) was adjusted, and the output has been used in risk assessment, in order to finetune risk probability. Extensiveness measures how much context an intelligence feed provides to complement additional information. With extensiveness, we assign a higher source confidence to intelligence feeds that give more context per IoC. Timeliness defines how fast an intelligence feed shares its IoCs compared to other feeds. If certain intelligence feed shares the same IoCs later than others, the IoCs could be outdated. Considering the slowness in sharing its IoCs, we will assign less source confidence to it. Completeness defines how much an intelligence feed contributes to the total collection of IoCs. Please note that this score focuses more on the quantity than

on the quality of an intelligence feed, assuming that if it has many IoCs, it indicates the feed is more useful. Whitelist Overlap Score defines how much of the IoCs in an intelligence feed also exist in a trusted whitelist, avoiding the consumption of false positives by the system. These four heuristics are used in a weighted mean to calculate the source confidence of the gathered intelligence feeds. This is the value that will appear in the tag "Source-Score" of the MISP event associated with a feed and is a value exported to risk assessment engine in CPR tool.

An example for risk probability recalculation is threat score parameter "timeliness" that changes perspective of the economic impact. We used historic data about "time to publish" of threat intelligence regarding the new malicious phishing threats with message body that includes COVID-19 information, as well as generic information about average speed of spreading this threat intelligence indicator related to phishing, and a "speed of digestion" in user organization, which is then combined to make calculation about risk probability. In the case that information is shared more than 40 hours before phishing attack on CI entity occurs, which is likely situation, damage reduces significantly, almost to 85 % of what would have been size of damage without the use of threat intelligence.

Finally, we should also mention fine grained policy for CTI sharing. CI organisations are now increasingly aware of the consequences of sharing versus not sharing information, and with new functionalities they can create communities or clusters between entities and employees that work in the same sector or same country, and apply fine grained policy that allows anonymization, encryption, and other operations on threat intelligence data. This is further improving cyber-physical resilience by preparing CI operators against attackers, that use the same TTPs to attack different entities.

IV. VALIDATION

Validation and testing process is scheduled for the summer of 2024 until H2 2025 and will happen in three phases:

- A Proof of Concept will simulate incoming logs from selected applications to identify potential threats to the systems under analysis.
- The tools will be deployed within CI operator to integrate and aggregate logs with the existing SIEM system in the testing environment. Additionally, integrations with the current MISP instance in the user infrastructure may be explored to enhance CTI sharing between departments and organisations.
- The tools will be piloted in the operational environment of CI operator. The tools' output will be monitored using real data from the applications under analysis, as well as simulated data for vulnerability tests. The CI operator Blue Team might oversee these operations.

In summary, plan is to test and validate this tool on a specific part of its regional critical infrastructure, including VPN Servers and the healthcare application. The testing will progress through phases, beginning with a Proof of Concept, followed by integration with SIEM and MISP, and concluding with operational environment monitoring.

V.CONCLUSIONS

The COVID-19 pandemic is an example of a temporary situation when CI had to operate with continuously changing conditions. This was reflected in changes of cyber-physical risk assessment, and in consequence, also changes of resilience assessment for CI. Infrastructure parts, employees or assets which were not perceived as critical before the pandemic were revealed to be critical during the pandemic. Due to the temporary conditions, it was not possible to deliver many different supplies for the correct infrastructure operation. The move to remote working highlighted the lack of computers for remote workers, and vulnerabilities with up-to-date configuration or relaxing cybersecurity policies. Most previous approaches describing resilience for critical infrastructure did not mention the essential role of specialists, also termed as "essential workers". Absenteeism was rarely discussed, as well as the impact on the health or safety of essential workers at their workplace.

Though cyber infrastructures have already been one of the most discussed parts of critical infrastructures prior to the COVID-19 pandemic, its role during pandemics, for example for the remote work or access to critical systems, has also changed. This resulted in re-evaluation of security policies, for example for remote workstation configurations, or higher asset value for some online applications, such as e-health, that must be used by citizens.

Priority or asset value can change and can be very specific for each critical infrastructure. This represents a challenge to keep risk assessment dynamic and in consequence also to increase cyber-physical resilience.

We started from investigation of these challenges with mappings of different static and dynamic inputs from internal "observation" sources that are relevant for cyber-physical risk models, usually a combination of events that can be collected through existing cyber tools, and information that can be statically provided by the CI operator. In addition, external sources of information, such as threat intelligence, were considered and modelled to make an impact on risk assessment. These external sources and events were also enhanced with threat score, as well as enriched with strategic information about adversary TTPs through "orientation" phase, and different heuristics of calculated score were considered for the re-calculation and adjustment of risk assessment.

Our approach shows that some temporary changes need to be modelled in advance and that collaboration through tools such as threat intelligence sharing, as well as dynamic enhancements and adaptations to temporary conditions, is essential in adjustment to temporary conditions.

In summary, we show how sharing and enhancing threat intelligence can have several impacts on CI resilience, including:

- Increased awareness about dynamic changes and temporary conditions,

- Improved detection capabilities (e.g. decreased time to develop new rules for intrusion detection systems or multi-factor authentication),
- Enhanced risk assessment by adjusting the potential impact of attacks, as well as the likelihood of occurrence.
- Informed decision-making to allocate scarce resources more effectively, prioritize security controls and countermeasures, and invest in relevant security technologies and training programs.

There is still work to do in the SUNRISE project, including validation by the end users and increasing the complexity of system under observation, according to the definition of complex system [22]. Balance might need to be found between the system dynamics, organisational priorities, and behavioural aspects. We need re-assessment every time there is a change of risk inputs or indicators, change of dependencies between them, or if a gap between strategic/tactical level decisions and the operational cybersecurity management (monitoring, detection, and operational response) has been detected. This might lead to "assessment fatigue" or even congestion in decision making. Finetuning might be needed to reach these balances and work on trade-offs between dealing with dynamicity and tool practicality.

By combining sensing ("observation") of external environment (incidents from SIEM or IDS tools, threats from CTI platforms, vulnerability from scanners, abnormal behaviour events, etc.), with a cognitive process of "orientation" (including threat score calculation or mapping to TTPs), we move towards cyber-physical resilience which is having ability to anticipate unknown faults or incidents. In this direction, we think that new research is needed in the areas related to dynamic and adaptable threat intelligence sharing, probably as a part of a different research project.

ACKNOWLEDGMENT

This work has been supported by the European Commission through SUNRISE project (grant no. 101073821) under the Horizon Europe research programme.

REFERENCES

[1] Developing Cyber-Resilient Systems: A Systems Security Engineering Approach, NIST Special Publication 800-160, Volume 2, Revision 1, https://nvlpubs.nist.gov/nistpubs/SpecialPublications/NIST.SP.800-160v2r1.pdf

[2] National definitions of Cyber resilience, CIPedia: https://websites.fraunhofer.de/CIPedia/index.php/Cyber_Resilience

[3] Birkie, Seyoum Eshetu & Trucco, Paolo & Kaulio, Matti. (2014). Disentangling core functions of operational resilience: a critical review of extant literature. Int. J. of Supply Chain and Operations Resilience. 1. 76-103. 10.1504/IJSCOR.2014.065461.

[4] Council directive 2008/114/EC of 8 December 2008 on the identification and designation of European critical infrastructures and the assessment of the need to improve their protection, https://eur-lex.europa.eu/LexUriServ/LexUriServ.do?uri=OJ:L:2008:345:0075:0082:EN:PDF

[5] Directive (EU) 2022/2557 of the European Parliament and of the Council of 14 December 2022 on the resilience of critical entities and repealing Council Directive 2008/114/EC, https://eur-lex.europa.eu/eli/dir/2022/2557/oj

[6] P. de Juan Fidalgo, A. Pasic, J. M. Del Álamo, R. Tourís and A. Álvarez, "TERME: a cyber-physical resilience toolset for risk assessment," 2023 JNIC Cybersecurity Conference (JNIC), Vigo, Spain, 2023, pp. 1-6, doi: 10.23919/JNIC58574.2023.10205687.

[7] ENISA technical report, Measurement Frameworks and Metrics for Resilient Networks and Services: Technical report, February 2011

[8] ENISA report Ontologies and Taxonomies for Resilience , 2011 https://www.enisa.europa.eu/publications/ontology_taxonomies

[9] Eisenberg, Daniel, Plourde, Kenton, Seager, Thomas, Allen, Julia & Kott, Alexander. (2013). Resilience metrics for cyber systems. Environment Systems and Decisions. 33. 10.1007/s10669-013-9485-y.

[10] Gustavo González-Granadillo, Mario Faiella, Ibéria Medeiros, Rui Azevedo, Susana González-Zarzosa, ETIP: An Enriched Threat Intelligence Platform for improving OSINT correlation, analysis, visualization and sharing capabilities, Journal of Information Security and Applications, Volume 58,2021, 102715, ISSN 2214-2126, https://doi.org/10.1016/j.jisa.2020.102715.

[11] Faiella, M.; Gonzalez-Granadillo, G.; Medeiros, I.; Azevedo, R. and Gonzalez-Zarzosa, S. (2019). Enriching Threat Intelligence Platforms Capabilities. In Proceedings of the 16th International Joint Conference on e-Business and Telecommunications - SECRYPT; ISBN 978-989-758-378-0; ISSN 2184-3236, SciTePress, pages 37-48. DOI: 10.5220/0007830400370048

[12] G. Gonzalez-Granadillo, M. Faiella, I. Medeiros, R. Azevedo and S. Gonzalez-Zarzosa, "Enhancing Information Sharing and Visualization Capabilities in Security Data Analytic Platforms," 2019 49th Annual IEEE/IFIP International Conference on Dependable Systems and Networks Workshops (DSN-W), Portland, OR, USA, 2019, pp. 1-8, doi: 10.1109/DSN-W.2019.00009.

[13] World Health Organisation initiative: https://www.who.int/initiatives/eios

[14] Abbas H, Tahoun MM, Aboushady AT, Khalifa A, Corpuz A, Nabeth P. Usage of social media in epidemic intelligence activities in the WHO, Regional Office for the Eastern Mediterranean. BMJ Glob Health. 2022 Jun;7(Suppl 4):e008759. doi: 10.1136/bmjgh-2022-008759. PMID: 35764352; PMCID: PMC9240825.

[15] European Centre for Disease Prevention and Control web page: https://www.ecdc.europa.eu/en/information-social-media-monitoring-epidemic-intelligence-purposes

[16] A. K. Daou, F. Li and S. Shiaeles, "A Cost-Efficient Threat Intelligence Platform Powered by Crowdsourced OSINT," 2023 IEEE International Conference on Cyber Security and Resilience (CSR), Venice, Italy, 2023, pp. 48-53, doi: 10.1109/CSR57506.2023.10225008.

[17] Anirban Mukhopadhyay, Sukrit Venkatagiri, and Kurt Luther. 2024. OSINT Research Studios: A Flexible Crowdsourcing Framework to Scale Up Open Source Intelligence Investigations. Proc. ACM Hum.-Comput. Interact. 8, CSCW1, Article 105 (April 2024), 38 pages. https://doi.org/10.1145/3637382

[18] MISP platform to gain situational awareness in regards to the COVID-19 situation: https://www.misp-project.org/covid-19-misp/

[19] MISP taxonomy for COVID-19: https://github.com/MISP/misp-taxonomies/blob/main/pandemic/machinetag.json

[20] Toolkit for Mapping of the MISP for SRH and its Adaptation for Preparedness and Response to COVID-19 and Other Pandemics and Major Outbreaks, https://iawg.net/resources/toolkit-for-mapping-of-the-misp-for-srh-and-its-adaptation-for-preparedness-and-response-to-covid-19-and-other-pandemics-and-major-outbreaks

[21] Directive (EU) 2022/2555 on measures for a high common level of cybersecurity across the Union, also known as NIS2 Direcive, https://eur-lex.europa.eu/eli/dir/2022/2555

[22] Jan Žižka, Bruno Rossi, Tomáš Pitner, Towards a Definition of Complex Software System, Position Papers of the 18th Conference on Computer Science and Intelligence Systems, M. Ganzha, L. Maciaszek, M. Paprzycki, D. Ślęzak (eds). ACSIS, Vol. 36, pages 119–126 (2023), DOI: http://dx.doi.org/10.15439/2023F2898