Cyber Security Information Sharing During a Large Scale Real Life Cyber Security Exercise

Jari Hautamäki(✉), Tero Kokkonen, and Tuomo Sipola

Institute of Information Technology,
Jamk University of Applied Sciences,
Jyväskylä, Finland
{jari.hautamaki, tero.kokkonen, tuomo.sipola}@jamk.fi

Abstract. In the event of a cyber attack, the efficient production and utilisation of situational information is achieved by sharing information with other actors. In our research, we have discovered how information related to cyber security can be shared online as efficiently as possible between organisations. We used the constructive method to implement a cyber sercurity information sharing network using the Malware Information Sharing Project (MISP). The model was tested in a pilot exercise in fall 2021. The key findings in connection with the pilot showed that it is particularly important for the recipient of information security information how quickly and accurately the information security event is described. In order to help quick reaction, it would also be necessary to implement informal channels, through which security information can be shared easily without structured event descriptions.

Keywords: Cyber Security; Security Information Sharing; Situational Awareness; Threat Information Sharing, Indicator of Compromise

1 Introduction

The efficient production and utilisation of security information is intensified by sharing relevant information with other actors in the information distribution network quickly and reliably, without compromising the confidential information of actor's own organisation. It shall be recognized that, typically, organisations are cautious about sharing that information because it might include sensitive details of critical systems vulnerabilities. However, sharing and exchanging it is extremely valuable as it allows early warning of threats and new vulnerabilities for improved situational awareness initiating early mitigation processes. This action allows the recipient of the information to react in a timely manner to potential cyber security threats before they materialise in their own organisation. [12,19,11]

The problem with cyber security information sharing is that information about data breaches and vulnerabilities usually cannot be passed to everyone or it comes too late to enable the prevention or mitigation of damage caused by attack or intrusion. On the other hand, the information provided might be

The original article appeared as: Jari Hautamäki, Tero Kokkonen, and Tuomo Sipola. "Cyber Security Information Sharing During a Large Scale Real Life Cyber Security Exercise". In: *Good Practices and New Perspectives in Information Systems and Technologies. WorldCIST 2024.* Ed. by Álvaro Rocha, Hojjat Adeli, Gintautas Dzemyda, Fernando Moreira, and Aneta Poniszewska-Marańda. Vol. 3. Lecture Notes in Networks and Systems 987. Cham, Switzerland: Springer, 2024, pp. 45–55. https://doi.org/10.1007/978-3-031-60221-4_5

too general to be used in defence procedures. [10] The exercise, where the implementation was tested, was executed in September 2021 in project the Healthcare Cyber Range HCCR Project. [14]

The rest of the paper is constructed as follows. First the chosen research approach, the constructive and observational research methodology is introduced. It is followed by illustrations of the situational awareness and cyber security exercise concepts. After that, the technical implementation with the test case exercise scenarios are explained. Finally, the analysed results are presented and the whole study is concluded with found future research topics.

2 Research Approach

In this study, the constructive research methodology is used for finding the answer of the research question. By using the constructive research approach, state-of-the-art constructions are implemented as a resolution for domain-specific real world problems. Those implemented artefacts or constructions can for example be software components, tools, processes, or practices. When utilising the constructive research approach, both practical and theoretical aspects of the problem should be considered. Both quintessential research question and implemented practical solution should be bound to the theoretical basics of the phenomena. [8,21]

The data acquisition methods used in the study were feedback discussion session immediately after the training ended, and a formal survey. The survey was administered to all participants about a week after the exercise. Feedback was collected in the so-called with a semi-structured method, where the organisers of the exercise prepare a frame for the issues and events to be handled in the feedback situation. The collection of feedback took place in the so-called through a protocol analysis, where the participants in the exercises brought out observations, their own interpretations and conclusions about the content and implementation of the exercise. [22]

The research objective of this study is to research and develop a implementation of cyber security information sharing system and test that system during the national wide real life cyber security exercise. The research focuses answering for the following research question:

- How to develop a cyber security information sharing system that can be utilised for real life cyber security exercise of critical infrastructure actors? The main research question can be divided into the following sub-questions:
  - Can the implemented system be technically based on Malware Information Sharing Project (MISP)?
  - What is the proper information sharing architecture or hierarchy?
  - Is the implementation effective enough for real-life exercise usage?

3 Cyber security information sharing

The sharing of cyber security information can be seen from two different perspectives. From an information sharing perspective, an event is a cyber security incident in an organisation. An incident will be reported in a way that information can be shared with other actors in the information-sharing community without a risk of sharing confidentional information from an organisation.

For the receiving organisation, the information appears as cyber security threat information. This is not necessarily an actual event in the recipient's organisation, but it is a potential threat. How potential it is depends the receiving organisation's technology environment, information and other relevant assets. In order to target the threat information as well as possible to organisations, it is advisable to share the information among actors in the same industry. For example, a few years ago, ransomware attacks were particularly targeted at hospital environments, where the sharing of threat information among industry players would have helped organisations respond in a timely manner to potential threats [23].

4 Cyber Security Exercise

A cyber security exercise is an event in which an organisation trains its preparedness for various cyber disruptions in the most appropriate way. The cyber security exercise is used to simulate or model cyber disruptions. This creates imaginary conditions in which the effects of the disorder and recovery can be tested.

There are different types of exercises depending on what kind of competences an organisation want to develop. Traditionally, technical exercises are supported by experts and technical maintenance expertise, while management and business exercises are provided to management. The co-operation exercise, on the other hand, applies to everyone and develops the skills of all staff and stakeholders. An exercise may also be a combination of different types of exercise, such as a technical-functional exercise. [18,17,16]

In the cyber security exercise, participants are organised into different teams with their own roles. The teams are named by colours depending on what their role is. The Red Team (RT) represents the attackers and is responsible for planning and executing attacks according to training scenarios. Usually, the RT is made up of the technical experts of the training provider. The Blue Team (BT) is a defensive team made up of staff from the organisations participating in the exercise. The competence profile of the participants can vary a great deal depending on the focus of the exercise. In the wide-ranging exercises, the BT consists of a mix of technical experts, administrative staff, and other experts, such as communications experts. In large execrcise there can be several blue teams. The White Team (WT), also known as Exercise Control (EXCON), controls the entire exercise. It directs the cyber security exercise activity and monitors the progress of the exercise. Other color codes can also be used to describe the different actors in the exercise to clarify the tasks of the groups. The Purple Team (PT) can act as a combined offensive and defensive team. The Yellow Team (YT) is responsible for building the exercise environment. The Green Team (GT) is responsible for the technical support and maintenance of the training environment during the exercise. [9,24]

5 Technical Implementation

The cyber security information sharing model was developed first for the HCCR project's and tested in pilot exercise in September 2021.

5.1 Implemented Construction

In the developed model, the cyber security information sharing architecture was formulated on three actors level: International level, national Information Sharing and Analysis Center (ISAC) level and enteprise/organisation level. The cyber security center located at the international level representing national CERT-FI (Computer Emergency Response Team - Finland). CERT-FI is responsible for cyber security information sharing between other national CERTs [1]. All national ISAC groups located on the ISAC level. Particularly the social welfare and health care ISAC was represented in the pilot exercise. Each ISAC group share security information from their responsible area of industry sector [3,2]. The lowest level actors represent companies and public organisations that utilise the threat information they receive in their operations and share threat information about cyber security breaches and verified events with other actors. The sharing of information takes place both horizontally, e.g., in the same industry and also vertically to the ISAC level and the international level (CERT).

In this information sharing architecture, the CERT shares and receives threat data that is expected to have a broader national impact. There are also vendors and providers on the ISAC level that receive and share threat information for their specific area. The sharing of cyber security-related information is based on verified events that are shared with others as threat information. Within the actor's own organisation, shared information is treated as cyber security incident information. Currently, the most popular cyber security information sharing solution is the MISP [20]. MISP can also be used as a threat intelligence platform to store and correlate targeted attacks, threat information, and vulnerability information. The European Union funds MISP development work.

5.2 Modeled Cyber Security Exercise a Real Life Test Event

The operating environment of the exercise included two hospitals and national services. In one of the hospitals modeled an intensive care unit (ICU) that included a patient simulator, a patient monitor, and a ventilator, which are commercial medical devices. Both hospitals had a modeled patient information system, referrals, prescriptions, imaging, and a laboratory. In addition, the exercise modeled national health-related services, such as DigiFinland's Omaolo service, KELA's (Social Insurance Institution of Finland) OmaKanta service, prescription center and the patient information and imaging archive for hospital districts as well as THL's (Finnish Institute for Health and Welfare) health information services. The pharmacy function was also modeled, allowing prescriptions to be redeemed. The exercise was attended by three hospital districts and four authorities, as well as four companies providing digital services to healthcare providers, including the National Cyber Security Center. [14,15,13,5,4]

The aim of the exercise was to test the planned healthcare training environment by producing disruption situations in the environment and to observe how different organisations react to them. Disruptions addressed to the training forces affected a single organisation or, on a large scale, multiple organisations. The exercise was a technical-functional exercise that lasted for three days, the first of which was set aside to familiarise the participants with the operating environment of the exercise. Cyber security status information was shared between organisations through the MISP application. The threat information identified during the exercise was routed to different actors through distribution groups configured in MISP.

Participating organisations were the following: (i) the three hospital districts participating in the pilot represented healthcare specific sector, (ii)other IAC groups and other actors represented security authorities, (iii) companies and service providers, (iv) social wellfare and healthcare ISAC represented the Finnish health and wellbeing services, (v) and Finnish Transport and Communications Agency – National Cyber Security Center (NCSC-FI) represented CERT-FI. In addition, one service provider participated in the exercise from outside the project partners. All the organisations had a representative in the exercise situation management (White Team, WT, 1 team) and a training force (Blue Team, BT, 6 teams) as shown in Figure 1. Several organisations had sent an observer to follow up their own BT activities or to participate in the monitoring of the whole exercise. White team (WT) also represent European CERTs and International Service Providers. The total number of attendees to the exercise was 68 persons.

All these compositions had their own instance (MISP-server). In the MISP installation sharing of threat information was configured by "Sharing Group" method (Figure 2). Sharing groups were following. SG: SHPT group was for sharing information between hospital districts, SG: Nat-Providers was for sharing between other ISAC's and national providers, SG: SOTE-ISAC was for information sharing between district hospitals and ISAC-SOTE actors, and SG: ISAC-Communities used to sharing information between different ISAC organisations. SG: INT-Providers and SG: INT-ISPs were groups for information sharing between national ISACs and international providers and ISPs. White teams represented those international actors. SG: EU-CERTs sharing group simulated information sharing between other international CERTs (in the exercise White Team) and national CERT-FI. All national cyber security threat information from hospital district level and ISAC level also shared with national CERT. All organsations also shared with method "Your organisation only" internally. Cyber security information sharing was classified ENISA [6] and TLP (Traffic Light Protocol) taxonomy [7]. Information was also shared by non-formal text mode.

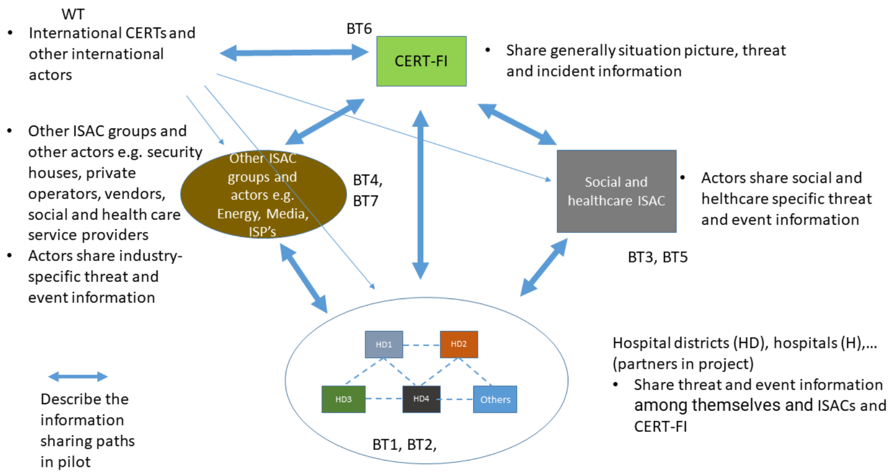

WT
International CERTs and other international actors
BT6
CERT-FI
Share generally situation picture, threat and incident information
Other ISAC groups and other actors e.g. security houses, private operators, vendors, social and health care service providers
Actors share industry-specific threat and event information
Other ISAC groups and actors e.g. Energy, Media, ISP's
BT4, BT7
Social and healthcare ISAC
Actors share social and helthcare specific threat and event information
BT3, BT5
HD1
HD2
HD3
HD4
Others
BT1, BT2,
Hospital districts (HD), hospitals (H),… (partners in project)
Share threat and event information among themselves and ISACs and CERT-FI
Describe the information sharing paths in pilot

Fig. 1. Cyber security information sharing architecture

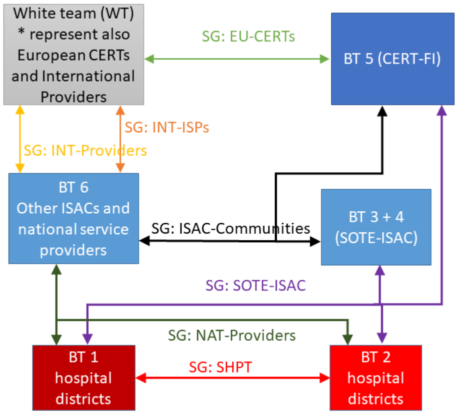


Fig. 2. Configuration of information sharing architecture in MISP platform

6 Results

The results from sharing cyber security information in the exercise were collected in two ways. In the end of the exercise instant feedback session was held, where all the attendees gave their firsthand feedback from the exercise. Feedback was also collected from the participants with a survey. A total of 67 people responded to the feedback (68 people participated in the exercise). The following are excerpts from the feedback and observations of the pilot exercise on the sharing of threat information.

6.1 Free-form feedback

A wider gathering of opinions and comments took place immediately after the exercise. This was carried out under the guidance of the leader of the exercise. A total of 31 answers and observations were written down. The results of these were classified into four categories; attitude towards the use of MISP, development proposals for the use of MISP, the usability of sharing information security information and development proposals for sharing information security information in general. Based on the results, a table (Table 1) was prepared according to the previously mentioned categories.

Table 1. Feedbacks at the end of exercise

Category	**Positive**	**Negative**	**Neutral**	**Suggestions**
Attitude for the using MISP	11	8	12	
Improvement suggestions for the use of MISP				13
Security information sharing tool is useful	11	6	14	
Improvement suggestions for the used sharing architecture				8

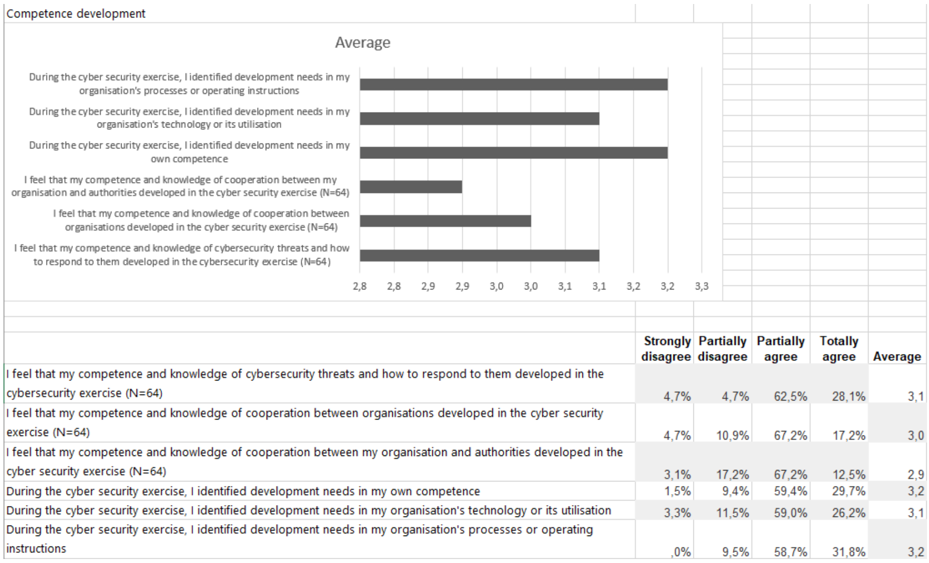
The results are fairly evenly distributed based on attitude to use MISP in exercise. About a third of respondents have a positive (11 responses) or neutral (12) attitude towards the use of MISP in sharing information security information. Accordingly, almost a third (8) did not find the use of MISP meaningful.”The use of the Data Sharing Application (MISP) would initially require a broader orientation before the exercise, e.g. where assembling MISP users to common training session”. ”I do not want to share unfinished data as is”. A total of 31 proposals were made to develop the sharing of security information. In the development proposals (13) to the use of MISP emphasize e.g. the following: ”There is a need for centralized maintenance and collection of situational awareness and communication to the management team.” ”It is important that the WT members leading the exercise are physically in the same space so that the information about the exercise spreads easily." , "In the future, it would be advisable to authorize a special person to share information and use the MISP tool." and "Clear instructions are needed on which distribution group to use for data sharing." Accordingly, there were a total of 8 development proposals related to the general sharing of information security. Among these rose out e.g. a suggestion for a lighter tool to share first-hand threat information: "A lighter tool is needed, eg IRC channels, which could be used to share early observations even with rather imprecise data." and "Representatives from each area should be brought together in case of deviations."

6.2 Feedback survey

The feedback survey was organised via electronic questionnaire. The main findings from the survey were: The majority (94%) of the respondents (N=66) agreed or totally agreed that the organised exercise developed the competence. Cooperation between organisations in knowledge and competence was reported to have developed (N=64) by the majority (84%). Cooperation between the knowledge and knowledge organisation and authorities was reported (N=64) by 80% (51) of the respondents. 89% (n=57) of respondents (N=64) report that they have identified development needs in their own competence. 85% (n=52) of the respondents (N=61) report that they have identified development needs in their own organisation's technologies or in its utilisation. In the organisation's code of conduct and processes, 91% (n=57) of respondents (N=63) identified areas for development. The majority (68%) of the respondents (N=59) either agreed or agreed with the following statement 'The environment used in the exercise (RGCE and the organisational environment) corresponded to the real world'. 80% of the respondents (N=58) either agreed or fully agreed with the statement "Data, systems and modelled processes in the training environment" from a national point of view. The majority, i.e. 90% of the respondents (N=64), felt that their knowledge of cyber security threats and their reintegration developed during the pilot exercise. Results has been described in Figure 3.

7 Conclusion

The data sharing architecture tested in the pilot exercise revealed a few bottlenecks in data sharing that can be summarised in the following observations. The transmission of sensitive information between operators must be confidential. The effectiveness of communication depends on how quickly and accurately a cyber security attack is described. Unnecessary information should be avoided in the sharing of information between actors in order to avoid a flood of information to detect relevant information. The pilot showed that researching and documenting cyber security attacks is time consuming and requires resources that may not be available at the same time. There is also a need for an informal channel such as chat channel for sharing threat information, where information can be shared in an informal form at a very early stage, when a possible attack


Competence development
Average
During the cyber security exercise, I identified development needs in my organisation's processes or operating instructions
During the cyber security exercise, I identified development needs in my organisation's technology or its utilisation
During the cyber security exercise, I identified development needs in my own competence
I feel that my competence and knowledge of cooperation between my organisation and authorities developed in the cyber security exercise (N=64)
I feel that my competence and knowledge of cooperation between organisations developed in the cyber security exercise (N=64)
I feel that my competence and knowledge of cybersecurity threats and how to respond to them developed in the cybersecurity exercise (N=64)
2,8
2,8
2,9
2,9
3,0
3,0
3,1
3,1
3,2
3,2
3,3

	Strongly disagree	Partially disagree	Partially agree	Totally agree	Average
I feel that my competence and knowledge of cybersecurity threats and how to respond to them developed in the cybersecurity exercise (N=64)	4,7%	4,7%	62,5%	28,1%	3,1
I feel that my competence and knowledge of cooperation between organisations developed in the cyber security exercise (N=64)	4,7%	10,9%	67,2%	17,2%	3,0
I feel that my competence and knowledge of cooperation between my organisation and authorities developed in the cyber security exercise (N=64)	3,1%	17,2%	67,2%	12,5%	2,9
During the cyber security exercise, I identified development needs in my own competence	1,5%	9,4%	59,4%	29,7%	3,2
During the cyber security exercise, I identified development needs in my organisation's technology or its utilisation	3,3%	11,5%	59,0%	26,2%	3,1
During the cyber security exercise, I identified development needs in my organisation's processes or operating instructions	,0%	9,5%	58,7%	31,8%	3,2

Fig. 3. Competence development in pilot exercise

is suspected. Such a communication channel allows the recipient of the information to tune in to a potential threat situation before transmitting more detailed threat information through a formal information sharing community.

The main research question was ”How to develop a cyber security information sharing system that can be utilised for real life cyber security exercise of critical infrastructure actors?”

During the development of the cyber security information sharing system, three different levels of division were identified within the architecture: international, national industry specific and organisational levels. On this basis, a data sharing architecture was developed in which the sharing took place both vertically and horizontally using the sharing groups of the MISP platform. The configuration of the distribution groups was carried out according to plan. The implementation is in line with the Cyber Security Centre's plans for a national data sharing architecture.

The main research question was divided into the following sub-questions: ”Can the implemented system be technically based on MISP?”, ”What is the proper information sharing architecture or hierarchy?” and ”Is the implementation effective enough for real-life exercise usage?”

The technical implementation based on MISP platform. MISP platform is mostly used platform in cyber security information sharing and ENISA has encourage organisation in Europe to use it as common European level security information sharing by publishing its own cyber security information taxonomy. The cyber security information sharing architecture developed in the exercises is in line with how ISACs and CERT-FI in Finland have been organised. As the results show, the implemented cyber security information sharing architecture and system is a workable solution to implement the exercise. However, the system requires an in-depth study of the incident before the results of the investigation can be shared with others. This undermines the efficiency of data sharing and thus delays actions against potential threats. There is also a need for a lower-level information-sharing method that does not similarly require a formal description of incidental security incidents. The most suitable solution for this purpose would be a chat application for sharing pre-information.

Acknowledgements

This research was partially funded by the Regional Council of Central Finland/Council of Tampere Region and European Regional Development Fund as part of the Health Care Cyber Range (HCCR) project of JAMK University of Applied Sciences Institute of Information Technology (grant number A74537) and by the Resilience of Modern Value Chains in a Sustainable Energy System project, co-funded by the European Union and the Regional Council of Central Finland (grant number J10052). The authors would like to thank Ms. Tuula Kotikoski for proofreading the manuscript and Mr. Henri Tervakoski for installing all the MISP instances and configurations which were used in exercise.

References

1. CERT. URL https://www.kyberturvallisuuskeskus.fi/en/our-activities/cert
2. HAVARO service | NCSC-FI. URL https://www.kyberturvallisuuskeskus.fi/en/havaro-service
3. ISAC information sharing groups | NCSC-FI. URL https://www.kyberturvallisuuskeskus.fi/en/our-services/situation-awareness-and-network-management/isac-information-sharing-groups
4. My Kanta pages - Citizens. URL https://www.kanta.fi/en/my-kanta-pages
5. Omaolo service. URL https://digifinland.fi/en/our-operations/omaolo-service/
6. Reference Incident Classification Taxonomy. URL https://www.enisa.europa.eu/publications/reference-incident-classification-taxonomy
7. CIRCL: Traffic Light Protocol (TLP) - Classification and Sharing of Sensitive Information. URL https://www.circl.lu/pub/traffic-light-protocol/
8. Crnkovic, G.D.: Constructive research and info-computational knowledge generation. In: L. Magnani, W. Carnielli, C. Pizzi (eds.) Model-Based Reasoning in Science and Technology: Abduction, Logic, and Computational Discovery, pp. 359–380. Springer Berlin Heidelberg (2010). DOI 10.1007/978-3-642-15223-8_20
9. Diogenes, Y.: Cybersecurity - attack and defense strategies: infrastructure security with red team and blue team tactics (2018)
10. Goodwin, Cristin and Nicholas, J Paul and Bryant, Jerry and Ciglic, Kaja and Kleiner, Aaron and Kutterer, Cornelia and Massagli, Alison and Mckay, Angela and Mckitrick, Paul and Neutze, Jan and others", title = "A framework for cybersecurity information sharing and risk reduction: (2015). https://www.microsoft.com/en-us/download/confirmation.aspx?id=45516

11. He, M.: Perspectives on Cybersecurity Information Sharing among Multiple Stakeholders Using a Decision-Theoretic Approach: Cybersecurity Information Sharing. Risk analysis **38**(2), 215–225 (2018). DOI 10.1111/risa.12878
12. Imanimehr, F., Gharaee, H., Enayati, A.: An architecture for national information sharing and alerting system. In: 2020 10th International Symposium onTelecommunications (IST), pp. 217–221 (2020). DOI 10.1109/IST50524.2020.9345861
13. JAMK University of Applied Sciences: Terveydenhuoltoalan kyberturvallisuus kehittyi yhdessä alan toimijoiden kanssa | Tech to the Future. URL https://blogit.jamk.fi/techtothefuture/2022/02/14/jamkissa-kehitettiin-terveydenhuoltoalan-kyberturvallisuutta-yhdessa-alan-toimijoiden-kanssa/
14. JAMK University of Applied Sciences: Real life medical equipment and simulated public health services in healthcare cyber security exercises (2021). https://jyvsectec.fi/2021/04/real-life-medical-equipment-and-simulated-public-health-services-in-healthcare-cyber-security-exercises/
15. JAMK University of Applied Sciences: Terveydenhuollon kyberharjoitusympäristön kehittäminen etenee (2021). https://blogit.jamk.fi/techtothefuture/2021/02/19/terveydenhuollon-kyberharjoitusympariston-kehittaminen-etenee/
16. JYVSECTEC: Kyberhäiriöiden hallinta - käsikirja terveydenhuollon toimijoille (2020). https://jyvsectec.fi/wp-content/uploads/2020/12/kyberhairioiden-hallinta-kasikirja-terveydenhuollon-toimijoille.pdf
17. Karjalainen, M., Kokkonen, T.: Review of Pedagogical Principles of Cyber Security Exercises. Advances in Science, Technology and Engineering Systems Journal **5**(5), 592–600 (2020). DOI 10.25046/aj050572
18. Karjalainen, M., Kokkonen, T., Puuska, S.: Pedagogical aspects of cyber security exercises. In: 2019 IEEE European Symposium on Security and Privacy Workshops (EuroS PW), pp. 103–108 (2019). DOI 10.1109/EuroSPW.2019.00018
19. Khajeddin, S.N., Madani, A., Gharaee, H., Abazari, F.: Towards a functional and trustful web-based information sharing center. In: 2019 5th International Conference on Web Research (ICWR), pp. 252–257 (2019). DOI 10.1109/ICWR.2019.8765297
20. project, M.: Misp - open source threat intelligence platform & open standards for threat information sharing. https://www.misp-project.org/. Accessed: 25 Jan 2022
21. Rautiainen, A., Sippola, K., Mättö, T.: Perspectives on relevance: The relevance test in the constructive research approach. Management Accounting Research **34**, 19–29 (2017). DOI https://doi.org/10.1016/j.mar.2016.07.001. URL https://www.sciencedirect.com/science/article/pii/S1044500516300233
22. Steven J., T., Robert, B., Marjorie, D.: Introduction to Qualitative Research Methods : A Guidebook and Resource., vol. 4th edition. Wiley (2016). URL http://search.ebscohost.com.ezproxy.jamk.fi:2048/login.aspx?direct=true&db=nlebk&AN=1061324&site=ehost-live
23. Thamer, N., Alubady, R.: A survey of ransomware attacks for healthcare systems: Risks, challenges, solutions and opportunity of research. In: 2021 1st Babylon International Conference on Information Technology and Science (BICITS), pp. 210–216 (2021). DOI 10.1109/BICITS51482.2021.9509877
24. Traficom: Kyberharjoitusohje - traficomin julkaisuja 26/2019 - käsikirja harjoituksen järjestäjälle (2022)