Kokkonen T. (2016). Architecture for the Cyber Security Situational Awareness System. In O. Galinina, S. Balandin, Y. Koucheryavy (eds.) Internet of Things, Smart Spaces, and Next Generation Networks and Systems. NEW2AN 2016, ruSMART 2016. Lecture Notes in Computer Science, vol. 9870, 294-302.

DOI: https://doi.org/10.1007/978-3-319-46301-8_24

URL: https://link.springer.com/chapter/10.1007%2F978-3-319-46301-8_24

Architecture for the Cyber Security Situational Awareness System

Tero Kokkonen

Institute of Information Technology, JAMK University of Applied Sciences,
Jyväskylä, Finland
tero.kokkonen@jamk.fi

Abstract. Networked software systems have a remarkable and critical role in the modern society. There are critical software systems in every business area. At the same time, the amount of cyber-attacks against those critical networked software systems has increased in large measures. Because of that, the cyber security situational awareness of the own assets plays an important role in the business continuity. It should be known what is the current status of the cyber security infrastructure and own assets and what it will be in the near future. For achieving such cyber security situational awareness there is need for the Cyber Security Situational Awareness System. This study presents the novel architecture of the Cyber Security Situational Awareness System. The study also presents the use case of threat mitigation process for such Cyber Security Situational Awareness System.

Keywords: Cyber Security; Situational Awareness; Multi Sensor Data Fusion; Situational Awareness Information Sharing; Early Warning

1 Introduction

Situational awareness and early warning capability is extremely important for command and control of the own assets or making decisions related to the mission or business. Military aviation has a long history of using command and control systems with situational awareness generated by multi sensor information that could also be shared from the systems of other organisations. There are similar requirements for situational awareness in the cyber domain. Sensor feed from multiple different sensors should be fused automatically and visualised for the decision maker. Additionally, the information of known cyber threats should be shared with other organisations.

The terms situational awareness and situation awareness are mixed in the literature and used for describing the same phenomenon. In this paper the term situational awareness is used because situational awareness is considered to describe the phenomenon more accurately.

As stated in [1] real time cyber security situational awareness and data exchange are required in several strategic guidelines of different countries, for example in

Finland's Cyber Security Strategy [1], [2]. A systematic literature review [1] indicates that there are several studies related to situational awareness in cyber domain; however, it is still stated in [3] that there is no solution for Cyber Common Operating Picture (CCOP).

This paper proposes state of the art architecture for the Cyber Security Situational Awareness System including a multi sensor data fusion component and data exchange with trusted partner organisations. The paper also presents the use case process for the Cyber Security Situational Awareness System and threat mitigation. The paper consists of a comprehensive set of reference literature and research papers as the background of the study. First, the Cyber Security Situational Awareness is discussed and the Data Fusion process is described. Also, the interfaces are presented, and the requirements for Human Machine Interface and data visualisation are analysed, followed by the description of the proposed architecture and finally, the conclusion with proposed items for further work is presented.

2 Cyber Security Situational Awareness

Endsley specifies one of the most used definitions of situational awareness (or as stated in the original reference situation awareness) as in the volume of time and space gathering information and elaborating understanding of what is happening and prediction of what will happen in the near future [4], [1]. From the point of view of Cyber Security Situational Awareness System, it means that there is multi sensor information available indicating what is happening, there is the capability for analysing such information, and there is also capability for making predictions what will happen in the near future.

As stated in [5] there are three types of information needed for situational awareness in cyber security: information of computing and network components (own assets), threat information, and information of mission dependencies. According to [6] there are four components of situational awareness: Identity (organisation's goals, structure, decisions making processes and capabilities), Inventory (hardware and software components), Activity (past and present activity of own cyber assets), and Sharing (both inbound and outbound). Paper [7] proposes a framework that consists of real-time monitoring, anomaly detection, impact analysis, and mitigation strategies (RAIM). The U. S. Army Innovation Challenge for Cyber Situational Awareness covers analytics, data storage, and visualisation of networks, assets, open-source information, user activity, and threats [8].

It is important to notice that there is a large and increasing number of systems, devices and cyber security applications or sensors in the organisation network providing data to be analysed. Analysing that increasing amount of information requires high computational power [9]. Data fusion is a recognised technique in surveillance and the security systems used for merging the scattered surveillance and status information as integrated totality. For example, paper [10] introduces data fusion for intrusion detection information.

3 Multi Sensor Data Fusion

The data fusion is defined as *"the process of combining data to refine state estimates and predictions"* [11]. The dominant data fusion model is JDL model by the US Joint Directors of Laboratories Data Fusion Sub-Group. In the JDL model the fusion process is divided into different levels. Originally, there were levels 0-4. Nowadays, there are levels 0-6 which can be described for the cyber domain as follows [11], [12], [13], [14], [15], and [16]:

- Level 0 (Data Assessment). Cyber security sensor feed to the system.
- Level 1 (Object Assessment). Identification of cyber entities for example services, devices, physical network connections or information flows and the properties of those entities.
- Level 2 (Situation Assessment). State of the systems in cyber domain. Combining, for example information of software versions, vulnerabilities or patches installed.
- Level 3 (Impact Assessment). Information related to an ongoing attack or threat, indicating the damage and mitigation actions or incident response required or already done.
- Level 4 (Process Refinement/Resource Management). Management of cyber sensors. Selection of used sensors, configuration of sensor settings and definition of the reliability score of each sensor.
- Level 5 (User Refinement/Knowledge Management). Human Machine Interface (HMI) providing access to control each layer of fusion. An important part of that level is effective visualisation of information to the user.
- Level 6 (Mission Management). Determination of mission objectives and policy for supporting decision making.

Giacobe presents an application of the JDL data fusion process model for cyber security utilising JDL levels 0-5 [14], and paper [15] introduces adapted national level JDL data fusion model for levels 0-5.

Paper [16] divides multi sensor data fusion algorithms under four main categories: Fusion of imperfect data, Fusion of correlated data, Fusion of inconsistent data, and Fusion of disparate data. There are several mathematical algorithms under those four categories. For example, [17] utilises Support Vector Machines (SVMs) as the fusion algorithm for network security situational awareness, and paper [18] proposes a Hierarchical Network Security Situation Assessment Model (HNSSAM) with DS data fusion for cyber security. Spatiotemporal event correlation is used for anomaly detection and for network forensics in study [19].

4 Interfaces

The proposed architecture includes several types of input information for data fusion supporting all the levels of JDL Data Fusion process. Because of that, the data fusion engine should implement several different data fusion algorithms chosen to support data fusion of such data. Following interfaces are proposed for the architecture.

4.1 Sensor Information

Input interfaces for the information from the cyber security sensor feeds such as information from anomaly based or signature based Intrusion Detection Systems (IDS), Intrusion Prevention Systems (IPS), firewalls, antivirus systems, log file analyser, authentication alarms etc.

4.2 Own Assets Status Information

Input interfaces for the information of the systems in the cyber domain. All the entities and their properties should be identified as well as their status and configuration information. Includes also the information of the sensors with their status and configuration information. Some of the systems are able to automatically inform their status and configuration information. Otherwise, the user will update the status information using HMI. If the service is under attack, the impact assessment status information is most likely input to the system by user. Additionally, the spare parts of the physical devices should be input to the system.

4.3 Analysis Information

The analysed impact assessment information about an ongoing attack or threat; caused damage, information of attacker, what are the used attack methods, what are the countermeasures, present and past mitigation activities or incident response activities, and the result of those activities. The analysis information also consists of Indicators Of Compromise (IOC) information and open source intelligence information originated, for example from social media, news or CERT-bulletins concerning systems in the use or the business area represented. Such open source intelligence information might offer early warning information about incoming threats or information needed for incident response. Paper [20] states that pure technical data is just a part of bigger situational awareness fused with intelligence information.

Certain policies or objectives that should be noticed as part of the Situational Awareness and decision-making information are input as part of the analysis information. The analysis information is input to the system both automatically and using HMI.

4.4 Sharing the Information

Information sharing is one of the most critical elements in cyber security. If there is a trusted network of other organisations and there is the capability to share information with those organisations, there is much more information available for the data fusion. With shared information there are requirements for filtering the information before sharing it according to the company policy. All the information cannot be shared because of the confidentiality of the security information. Inbound data should also be analysed and the reliability score assigned.

In the case of simultaneously ongoing data fusion and data sharing processed the origin of the information should be indicated because of the data-loops. If the information is shared (outbound) to any organisation of the information sharing community and after while the same information is shared back (inbound) from any organisation of the information sharing community, there is a data-loop. Data-loops produce problems with the data fusion algorithms. If the origin of the information is indicated and data fusion algorithm notices that inbound information originates from itself, such information should be perceived in the fusion process.

There are standards called Structured Threat Information eXpression (STIX™) [21] and Trusted Automated eXchange of Indicator Information (TAXII™) [22] for exchanging cyber threat information. The information sharing community using such standards could be formed as described in paper [23].

5 HMI and Visualisation layer

HMI should propose access to modify and add information for all the layers of fused data as described earlier in 3 and 4. It should also visualise the information efficiently for the user to obtain the scattered information more understandable format.

The visualisation part of the Cyber Security Situational Awareness System offers the Cyber Common Operating Picture to the user. The required data is in the system, the question is how to visualise that data to the user, especially for the decision maker who might not have deep technical background and knowhow. Many tools in cyber security are only for special purpose and certain data, not for integration of several types of data and without interoperability with other tools [24]. The authors of paper [25] used attack graphs for visualisation and ArcSight was used for visualisation in [26]. The paper [27] focuses on visualisation of threat and impact assessment.

The cyber domain is complex and there is plenty of different information available. The main conclusion for the visualisation problem is that there should be different visualisation tools and techniques for different purposes and for different user roles. Visualisation tools for high level decision makers are totally different to the tools for the analyst. Using case studies, the authors of paper [28] emphasise the potential for several different visualisation tools.

A solution for visualisation problem would be the usage of common symbols. Paper [29] suggests usage of military symbols, for example defined in standard MIL-STD-2525 [30]. Such standards should be extended for cyber domain, for example a military symbol for pending identity could mean a new incident in cyber domain. The common symbols should be defined and adopted as global standard for cyber security.

6 Proposed Architecture

The proposed novel architecture for the Cyber Security Situational Awareness System includes data fusion engine according to 3, interfaces described in 4, as well as HMI and Visualisation layer described in 5. Because there is plenty of different information

from different sources the information needs to be normalised. The blog diagram of the proposed architecture is presented in **Fig. 1**.

The ultimate goal for such systems is that described functionalities are as automatic as possible; however, there is analyst operator required for controlling the data fusion, controlling the sensors, and adding analysis information to the system. For example, cyber security sensors might produce false alarms and the data fusion might help with the false alarms by fusing the information from multiple sources; however, the analyst operator is required to analyse the sensor feed and maybe configure the sensors or indicating to the system that false alarms are occurring. Also, if there is a real incident ongoing, the analyst operator is capable of inputting the case related additional information to the system. The possible process for situational awareness and threat mitigation using the proposed architecture is presented in **Fig. 2**.

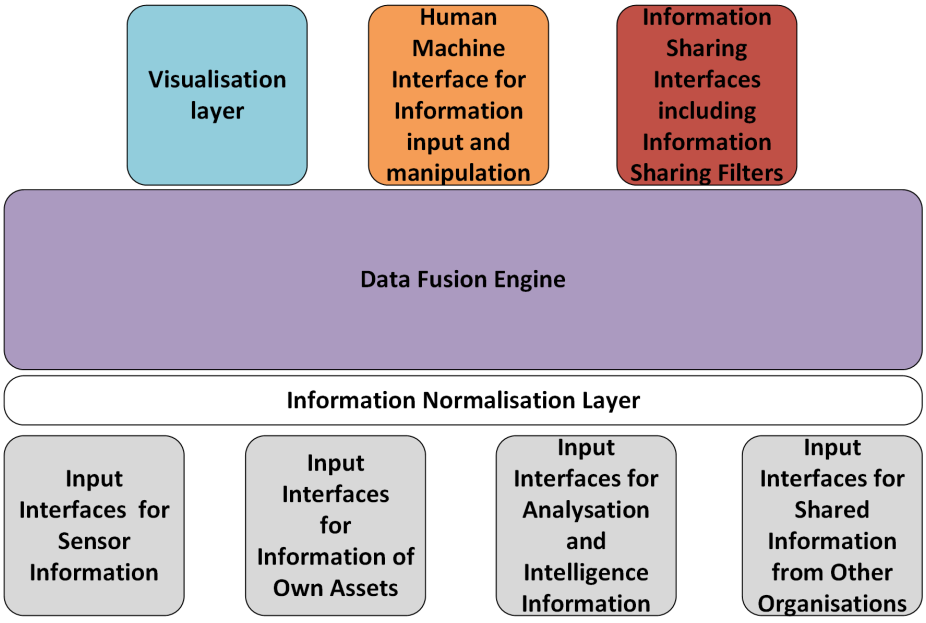

Fig. 1. Blog diagram of proposed architecture

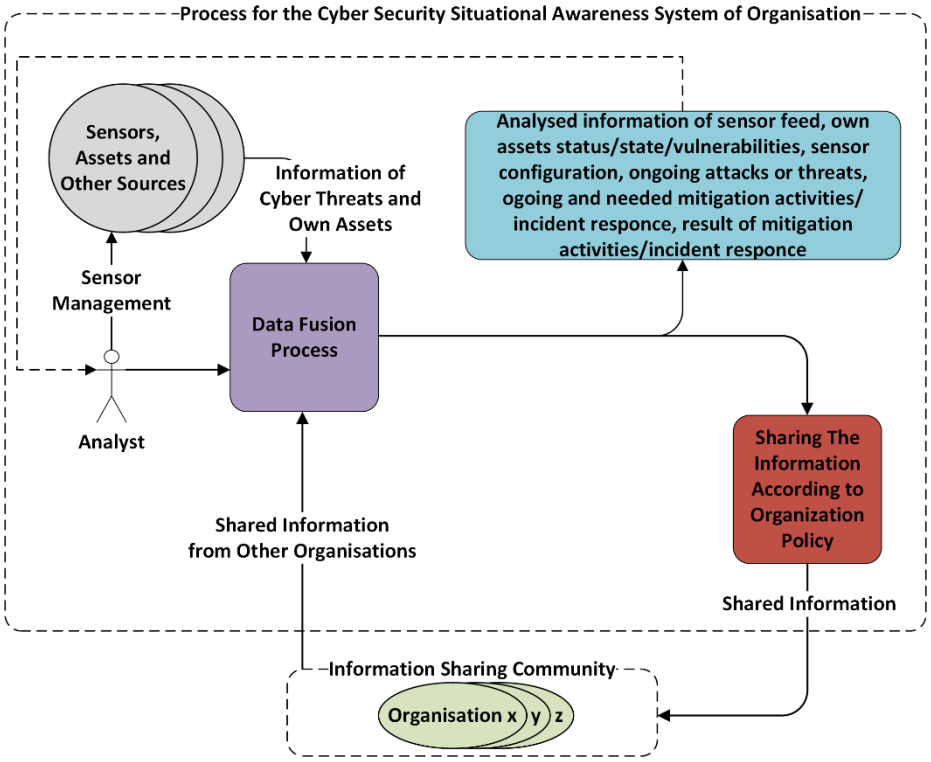

Fig. 2. Use case process for the Cyber Security Situational Awareness System

The proposed architecture represents the state of the art system in the domain of cyber security situational awareness systems utilising both data fusion engine and data exchange mechanisms at the same time. It also provides capability for implementation of all the levels of JDL data fusion process. Even the highest levels could be implemented and input to the system as a part of the Situational Awareness. The Visualisation could be deployed in layers for supporting the totally different requirements of different user roles, for example decision maker compared to analyst.

Detailed system requirements for the Cyber Security Situational Awareness System can be derived using proposed architecture. There are requirements for the data fusion engine according to 3, interfaces according to 4, HMI and Visualisation layer according to 5 and use case process presented in **Fig. 2**.

Developing such a system as product for the operational use requires detailed design and a great deal of software development. There are plenty of technical difficulties for developing such a system. Data models of the input information might be one of those. Some devices and sensors use standardised data models and protocols and some might use proprietary models. Some information is human made and some is automatically generated, the problem comes with the human made information, is it always without errors and structured correctly. Similar problems exist with many

other integrated systems and can be solved using standardisation and structured data formats. Initial versions should be implemented with certain sensors and data feeds and extended gradually.

Processing a large amount of data could require lot of computational power; however, during the exact design of the system it could be divided into different nodes. The visualisation should be tested deeply with different user roles. There is a global requirement for common standardisation of visualisation symbols in cyber domain. Visualisation should be implemented layer by layer for different users and use cases.

7 Conclusion

The study proposes novel architecture for the Cyber Security Situational Awareness System. It includes the process for using such a system for achieving the cyber resilience of the business or mission. The proposed architecture includes both multi sensor fusion process and information exchange process which both are required for achieving proper situational awareness of the cyber security infrastructure and own assets. The architecture utilises all the levels of JDL data fusion model. Pure technical situational awareness could be enriched, for example using open source intelligence information, impact analysis information, information of incident response actions and certain polices of the organisation. The proposed architecture could be used both in government and industry organisations for state of the art Cyber Security Situational Awareness System.

The next steps for the study are developing a proof of concept system using the proposed architecture, testing different multi sensor data fusion algorithms for the proposed architecture and visualising the situational awareness of a complex distributed network system. Developed proof of concept system could be used for functional evaluation of the theoretical architecture proposed in this study. Additionally, automatic threat mitigation based on situational awareness would be an interesting domain of research and development.

Acknowledgment

This work was funded by the Regional Council of Central Finland/Council of Tampere Region and European Regional Development Fund/Leverage from the EU 2014-2020 as part of the JYVSECTEC Center project of JAMK University of Applied Sciences Institute of Information Technology.

References

1. Franke, U., Brynielsson, J.: Cyber situational awareness - A systematic review of the literature. In: Computers & Security 46, pp. 18-31 (2014).

2. Secretariat of the Security Committee: Finland's Cyber Security Strategy. Government Resolution 24.1.2013.
3. Conti, G., Nelson, J., Raymond, D.: Towards a Cyber Common Operating Picture. In: Proc. of the 5th International Conference on Cyber Conflict (CyCon), NATO CCDCOE Publications, Tallinn (2013).
4. Endsley, M.: Toward a Theory of Situation Awareness in Dynamic Systems. In: Human Factors: The Journal of the Human Factors and Ergonomics Society, March 1995, vol. 37, no. 1, pp. 32-64 (1995).
5. The MITRE Corporation: Cybersecurity, Situation Awareness. In: https://www.mitre.org/capabilities/cybersecurity/situation-awareness/, accessed on 23.5.2016.
6. The Industrial Control System Information Sharing and Analysis Center (ICS-ISAC): Situational Awareness Reference Architecture (SARA). In: http://ics-isac.org/blog/sara/, accessed on 23.5.2016.
7. Ten, C. W., Manimaran, G., Liu, C. C.: Cybersecurity for Critical Infrastructures: Attack and Defense Modeling. In: IEEE Transactions on Systems, Man, and Cybernetics - Part A: Systems and Humans, vol. 40, no. 4, pp. 853-865, July 2010 (2010)
8. Keller, J.: Army Cyber Situational Awareness Innovation Challenge focuses on cyber threats at brigade level. In: Military & Aerospace Electronics, November 18 2015.
9. Yu, W., Xu, G., Chen, Z., Moulema, P.: A Cloud Computing Based Architecture for Cyber Security Situation Awareness. In: Proc. of the IEEE Conference on Communications and Network Security (CNS), National Harbor, MD, pp. 488-492 (2013).
10. Bass, T.: Intrusion Detection Systems and Multisensor Data Fusion. In: Communications of the ACM Magazine, Volume 43 Issue 4, April 2000, pp. 99-105 (2000).
11. Steinberg, A., Bowman, C., White, F.: Revisions to the JDL Data Fusion Model. In: SPIE Proceedings Vol. 3719, Sensor Fusion: Architectures, Algorithms, and Applications III, pp. 430-441 (1999).
12. Azimirad, E., Haddadnia, J.: The Comprehensive Review On JDL Model In Data Fusion Networks: Techniques and Methods. In: International Journal of Computer Science and Information Security (IJCSIS), Vol. 13, No. 1, January 2015.
13. Blasch, E., Steinberg, A., Das, S., Llinas, J., Chong, C., Kessler, O., Waltz, E., White, F.: Revisiting the JDL model for information exploitation. In: Proc. of the 16th International Conference on Information Fusion (FUSION), Istanbul, pp. 129-136 (2013).
14. Giacobe, N.: Application of the JDL Data Fusion Process Model for Cyber Security. In: SPIE Proceedings Vol. 7710, Multisensor, Multisource Information Fusion: Architectures, Algorithms, and Applications, 77100R (April 28, 2010)
15. Swart, I., Irwin, B., Grobler, M.: MultiSensor National Cyber Security Data Fusion. In: Proc. of the 10th International Conference on Cyber Warfare and Security (ICCWS), pp. 320-328 (2015).
16. Khaleghi, B., Khamis, A., Karray, F. O., Razavi, S. N.: Multisensor data fusion: A review of the state-of-the-art. In: Information Fusion, Volume 14 Issue 1, January 2013, pp. 28-44 (2013).
17. Liu, X., Wang, H., Liang, Y., Lai, J.: Heterogeneous Multi-Sensor Data Fusion with Multi-Class Support Vector Machines: Creating Network Security Situation Awareness. In: Proc. of the Sixth International Conference on Machine Learning and Cybernetics, Hong Kong, pp. 2689-2694 (2007).
18. Zhanga, Y., Huanga, S., Guob, S., Zhu, J.: Multi-sensor Data Fusion for Cyber Security Situation Awareness. In: Proc. of the 3rd International Conference on Environmental

Science and Information Application Technology (ESIAT 2011), Procedia Environmental Sciences 10, pp. 1029-1034 (2011).
19. Xie, Y.: A Spatiotemporal Event Correlation Approach to Computer Security. Doctoral Dissertation, Carnegie Mellon University, School of Computer Science, Pittsburgh, PA, USA (2005).
20. Kornmaier, A., Jaouën, F.: Beyond technical data - a more comprehensive Situational Awareness fed by available Intelligence Information. In: Proc. of the 6th International Conference on Cyber Conflict (CyCon), NATO CCDCOE Publications, Tallinn (2014).
21. Barnum, S.: Structured Threat Information eXpression (STIX™). Version 1.1, Revision 1, February 20 2014. In: http://stixproject.github.io/getting-started/whitepaper/, accessed on 24.5.2016.
22. Connolly, J., Davidson, M., Schmidt, C.: Trusted Automated eXchange of Indicator Information (TAXII™). May 2 2014. In: http://taxiiproject.github.io/getting-started/whitepaper/, accessed on 24.5.2016.
23. Kokkonen, T., Hautamäki, J., Siltanen, J., Hämäläinen, T.: Model for Sharing the Information of Cyber Security Situation Awareness between Organizations. In: Proc. of the 23rd International Conference on Telecommunications (ICT), Thessaloniki, Greece (2016).
24. Fink, G., North, C., Endert, A., Rose, S.: Visualizing Cyber Security: Usable Workspaces. In: Proc. of the 6th International Workshop on Visualization for Cyber Security (VizSec), Atlantic City, NJ, pp. 45-56 (2009).
25. Jajodia, S., Noel, S., Kalapa, P., Albanese, M., Williams, J.: Cauldron Mission-Centric Cyber Situational Awareness with Defense in Depth. In: Proc. of the Military Communications Conference (MILCOM), Baltimore, MD, 2011, pp. 1339-1344 (2011).
26. Briesemeister, L., Cheung, S., Lindqvist U., Valdes, A.: Detection, Correlation, and Visualization of Attacks Against Critical Infrastructure Systems. In: Proc. of the 8th Annual Conference on Privacy, Security and Trust, Ottawa, Canada (2010).
27. Nusinov, M.: Visualizing threat and impact assessment to improve situation awareness. Thesis. Rochester Institute of Technology (2009).
28. Hall, P., Heath, C., Coles-Kemp, L.: Critical visualization: a case for rethinking how we visualize risk and security. In: Journal of Cybersecurity, 1(1), pp. 93-108 (2015).
29. Grégoire, M., Beaudoin, L.: Visualisation for Network Situational Awareness in Computer Network Defence. In: Visualisation and the Common Operational Picture. RTO-MP-IST-043 (2005).
30. U.S Department of Defence Interface Standard, Joint Military Symbology: MIL-STD-2525D, 10 June 2014.