Proof-of-Concept for a Granular Incident Management Information Sharing Scheme

1st Outi-Marja Latvala
VTT Technical Research Centre of Finland
Oulu, Finland
outi-marja.latvala@vtt.fi

2nd Ivo Emanuilov
KU Leuven Centre for IT & IP Law
Leuven, Belgium
ivo.emanuilov@kuleuven.be

3rd Tatu Niskanen
VTT Technical Research Centre of Finland
Espoo, Finland
tatu.niskanen@vtt.fi

4th Pia Raitio
Finnish Transport Infrastructure Agency
Helsinki, Finland
pia.raitio@vayla.fi

5th Jarno Salonen
VTT Technical Research Centre of Finland
Tampere, Finland
jarno.salonen@vtt.fi

6th Diogo Santos
Sistrade – Software Consulting, S.A.
Porto, Portugal
diogo.santos@sistrade.com

7th Katerina Yordanova
KU Leuven Centre for IT & IP Law
Leuven, Belgium
katerina.yordanova@kuleuven.be

***Abstract*—Trust is a key ingredient in collaboration between security operations centers (SOCs). The collaboration can enhance defense and preparedness against cyberattacks, but it is also important to limit the attacker's ability to infer their potential for success from the communication between SOCs. This paper presents a proof-of-concept for a granular information sharing scheme. The information about a security incident is encrypted and the SOCs can decide with great precision which users or user groups can access it. The information is presented in a web-based dasboard visualization, and a user can communicate with other SOCs in order to access relevant incident information.**

***Index Terms*—Incident management, Information sharing, Fine-grained access control**

I. Introduction

Digitalisation in the modern world can be considered a double-edged sword. It allows us to access information around the world and communicate easily with people from different countries and cultures. However, it also makes us vulnerable to malicious third parties that may gain access to our computer, use our browsing information for malicious purposes or try to cheat us somehow. In other words, we are used to locking our doors, but still tend to leave our cyberdoors and -windows wide open. The same applies to the fourth industrial revolution and the factories of the future (FoF) where the physical facilities are often locked, secured and guarded, but the digital facilities and assets may be vulnerable to cyberattacks and data breaches.

The digital convergence of traditional manufacturing companies has changed the way they are connected to the network and how they use data, and the pace of this digital transformation may be too fast for them. According to Deloitte (2017), cyberattacks may have far more extensive effects than ever before and individual manufacturing companies and their supply networks are unprepared for the potential risks [1]. For companies in the critical infrastructure sector, these risks are often more complex and involve big responsibilities, for instance, in terms of energy distribution or providing connectivity. Critical infrastructure companies are often supported by national or in some cases even sector-specific computer emergency response teams (CERT), computer security incident response teams (CSIRT), and other supporting agencies such as national emergency supply agencies (NESA) and national cyber security centres (NCSC), the latter of which normally also host and coordinate the CERT activities.

A security operations center (SOC) combines the people, processes and technologies that are needed to respond to cybersecurity incidents into one unit inside an organization. The mission of the SOC is to prevent, detect, respond and analyze such incidents to keep the company's networks, devices, databases and any other assets safe. Information about the security status of these assets is gathered from various monitoring tools and combined at the SOC to provide the overarching view of security.

Several SOCs working together form a collaborative security operations center (CSOC) that can provide an even wider view on cybersecurity. For example, several companies along a supply chain could benefit from shared information if one of them detects cybercriminal activity. However, establishing and maintaining *trust* is key to a functioning CSOC.

This paper is structured as follows: Section 2 overviews previous work on information sharing, trust and collaboration frameworks. For practical realization of trust, we also sum-

978-1-6654-8453-4/22/$31.00 ©2022 IEEE

marize fine grained access control methods for collaborative environments. In Section 3 we describe the scenario behind and the implementation of our proof-of-concept. Discussion on the proof-of-concept and its place in building trust between SOCs is presented in Section 4, and conclusions in Section 5 close the paper.

II. Background

Within the European Union, cybersecurity information exchange is a form of strategic partnership among key public and private stakeholders, where the aim is to address malicious cyberattacks, natural disasters and physical attacks [2]. In 2015 ENISA [3] highlighted the strong need for the exchange of data to support the management of vulnerabilities, threats and incidents, as well as other cybersecurity activities. However, in the field of cybersecurity, trust is one of the most significant barriers to organizational information sharing. [4]

The two main actors identified in the cybersecurity information sharing research are the defenders and attackers. It is imperative for the defenders to share cyberthreat information like knowledge about threats, incidents, vulnerabilities, mitigation methods, leading practices and suitable tools. After all, when an attacker has the means and a motivation to threaten one organization, they may become a threat to the wider defending community.

The sharing of cybersecurity information improves (i) awareness of current cyberthreats affecting any relevant sectors, (ii) understanding of attackers' tactics, techniques, and procedures, (iii) acquisition of information that would otherwise be unavailable through public sources or security vendor reporting, (iv) decision-making regarding technology, controls, and resources allocation and escalation, (v) detection capabilities on networks, and (vi) mitigation and responses prior to an actual event [5].

Additionally, for the information sharing to be useful, the organizations must have good documentation and inventory management. There should also be coordination of best practices among the teams managing cybersecurity and risk to determine the most effective medium for information sharing (e.g., email, reporting etc.) and how the information is best shared. Finally, senior leadership's role in setting up information sharing mechanisms cannot be neglected. Mid-managers and practitioners should engage in collaboration and should be given the competences to engage, share and collaborate with external trusted counterparts on threats and incidents. [5]

A. Trust and Information Sharing

As SOCs grow in size and complexity, the level of abstraction increases as well. Larger and more complex SOCs are more likely to be physically separated from the monitoring infrastructure. Moreover, abstractions such as virtualization and security as a service can create technical and legal limitations concerning multi-tenancy, logical network segregation, integration etc. [6].

Similar concerns emerge around the use of threat intelligence platforms, which are often seen as part of a SOC. The main limitations of these platforms comes from the large quantity of information: it is difficult to find relevant information and generate value out of it [7]. Furthermore, the threat triage and relevancy determination is currently a manual process, hence it takes time and expertise. Also, data warehouses focus on data collection, but not so much on other phases of the intelligence life-cycle.

The participating organizations need to have certain levels of trust towards the platform operator as well as towards the other organizations. ENISA [7] identified the following categories of trust relationships that develop in this context: (i) Organization trusts platform, provided that handling shared information and access control does not expose confidential data to unauthorized recipients, (ii) organization trusts other participating organizations that handling of shared information is performed in accordance with a predetermined protocol, e.g. TLP, (iii) platform provider and other organizations trust the organization that information shared by it is reliable and credible.

There are also some practical limitations for taking part in threat intelligence sharing. There may be concerns about the quality of shared threat data and issues of confidence and information provenance. Limited advanced analytic capabilities and lack of automation of tasks, the diversity of data models and formats used, and wide variety of APIs and integration requirements could be additional limitations for many organizations to participate in threat intelligence platforms. [7]

B. Frameworks for Collaboration

Collaboration when responding to cyberincidents has been a topic of interest for some time. For example, system models for collaborative incident response involving multiple organizations and legal entities, organized around an independent central node like Palantir [8] and Cerebro [9] have been proposed. Both of these models define sets of roles and responsibilities as well as a process for the incident response, and present an implementation of their respective schemes. More recently, Settanni et al. [10] showcased a layered collaborative cyberincident management system for European interconnected critical infrastructures. The organizational SOCs at the lowest layer use sensors and tools to detect threats and report to national SOCs at the middle layer for incidents that might have cross-organizational relevance. National SOCs are responsible for gaining situational awareness on the network of national critical infrastructures. They perform information aggregation, correlation, classification and analysis, and provide advice on mitigation and early warnings back to relevant SOCs. At the top layer the European SOC performs analysis of strategic information shared by the different national SOCs and distributes advisories to targeted lower level SOCs and other European security entities.

Meng et al. [11] provided a comprehensive overview of the concept of *collaborative security* based on an investigation of 44 different systems. They divided the different collaborative security systems into collaborative intrusion detection

systems, anti-spam, anti-malware, identification of malicious nodes, malware detection in Mobile operating systems, and detection and resistance to botnets. The taxonomy they provide considers the target of analysis (host or network), timeliness of analysis (online or offline), architecture (centralized, decentralized, hierarchical, hybrid) , network infrastructure (wired, wireless), initiative (active, passive collaboration), shared information (raw, partially or fully processed), and interoperability (standard or custom communications). The authors pinpoint seven threats these systems face: privacy leakage, privilege escalation, authentication violation, denial of service, malicious code execution, abuse of functionality and resource depletion.

Irrespective of the tools and frameworks used, trust between the collaborators is an important issue. A recent approach aims to improve the trust, accountability and consensus between participants of a collaborative intrusion detection system (CIDS) by incorporating distributed ledger technologies (i.e., blockchain) into the system [12]. The authors provide a generic architecture for a distributed CIDS, where the participating nodes exchange messages in two layers, an alert exchange layer and a consensus layer. The first layer is used to propagate information and the second layer is used to make decisions about what should be included in the ledger.

An example of a collaboration framework focusing on the privacy of the participants is the PRACIS (PRivacy-preserving and Aggregatable Cybersecurity Information Sharing) scheme [13]. It provides privacy-preserving data forwarding and aggregation in a data sharing network. The system uses existing format preserving encryption techniques to the messages (structured threat information expression, or STIX data format) and uses homomorphic encryption to provide some simple statistics about the about reported information in a privacy-preserving way.

Before an incident has even happened, there are opportunities for collaboration. Malware information sharing platform (MISP) [14] can be used to collect and share important indicators of compromise of targeted attacks, as well as other threat information like vulnerabilities or financial indicators used in detecting fraud cases.

Finally, in order to exchange precise information between SOCs we need a common technical language. The incident object description exchange format (IODEF) [15] represents computer security information commonly exchanged between collaborative SOCs and other similar organizations. It provides an XML representation for conveying threat characterizations, security incident reports, response activities and metadata for exchanging all this information. The structured format of IODEF allows for machine-to-machine information exchange and automated processing of data.

C. Fine Grained Access Control

Access controls are needed to prevent unauthorized access to system resources. Different access control models, e.g., role-based access control (RBAC) [16], have been under active research for decades. There are comprehensive surveys on traditional tasks and groups -focused access control for collaborative systems [17] as well as on more dynamic, community-based collaborative systems based on users' established interpersonal relationships [18].

In collaborative environments there is often a need for more fine grained access control than traditional RBAC can offer. Albulayhi et al. [19] reviewed different fine grained access control models intended for cloud computing environments. They split the models into three categories: traditional, encryption based and modern. In their analysis, the encryption based models offer high granularity but have more processing overhead. Traditional models have better performance, but some of them are not comparatively fine grained and lack security features like backward and forward security.

Adding to that, there has also been a good amount of research on fine-grained access control (FGAC) systems for XML-documents, the de facto standard language for information exchange on the Internet. For example, Damiani et al. [20] present an access control model that exploits XML's internal cababilities to define and enforce access restrictions, directly in the XML document content and structure, and another model called QFilter rewrites user's query to a new one that will not return data violating access control rules, to achieve both security and efficiency in query processing. [21] A framework for different XML access control mechanisms has been proposed by Luo et al. [22].

III. FGAC for Information Sharing

In this section we first present the larger context of enhancing trust between SOCs. Then we describe the proof-of-concept implementation that combines an event generator and a dashboard visualization for exchanging incident information between two SOCs.

A. The underlying scenario

One of the major goals of our project wast to design and implement a collaborative security operations center. In order to help the organizations with preparing for and preventing cyberattacks, we need to support their threat, vulnerability and incident management by enhancing information sharing among them. However, one major obstacle for information sharing is a lack of trust. Within the project, we wanted a CSOC to collect relevant information, analyse it and respond to security incidents without unnecessary delay. There were several objectives for the CSOC: (i) enabling collaborative incident response in manufacturing environments, (ii) hastening decision making, and (iii) optimizing costs for responding to attacks.

We aimed to enhance the trust between organisations by using fine grained access control for incident information sharing: only relevant pieces of incident data would be shared to specific users or groups. For example, if an automotive factory faces a cyberattack, they could share only basic information about the incident to other factories in Europe, more specific information to other automotive factories, if the attack seems

to target their sector in particular, and finally give full access to their closest collaborating SOC operator.

The amount of information that needs to be shared should be carefully considered, as it is possible that the attacker is also observing the situation in order to gauge the success of their attack. In our work we wanted to balance the need to share enough information to the right people – but not too much that it becomes a threat in itself. We created a proof-of-concept system using fine grained access control, that allows an organization to share incident information while maintaining trust.

B. Our implementation

The proof-of-concept (PoC) consists of an event generator and an incident management dashboard, see Figures 1-3. The event generator was developed for simulation purposes. The PoC can gather information about the performance and responses of the monitored system. The event generator is the base engine of the simulation environment. It fires stochastic incident events, imitating what could happen in a real productive scenario. This simulated data can then be visualized at the dashboards of the collaborating actors and locations.

The event generator system uses object-oriented design; there is a clear segregation of responsibilities between its components. Firstly, IODEFGenerator is responsible for generating the documents and assigning them to different products. Secondly, an XML Processor component is responsible for building valid XML documents from the generated incidents and sharing them with the incident response team. Each of the fired incident events follows the IODEF standard [23]. There is at least one incident entity in each file, and each entity is comprised of the fields detailed in Table I. Finally, since the visualization dashboards of the collaborators are assumed to be web-based, the event generator uses the HTTPS protocol for data exchange with the different dashboards.

The IODEF documents are enhanced with fine-grained access control tags, that act as attributes to the fields holding the incident information, in order to visualize the incidents. We grant access to the encrypted information to the users based on these tags.

Now, we can control the users' ability to visualize these fields in a differential way because of the FGAC tags. In the demonstration, the event generator randomly selects a subset of tags within the IODEF document, and encrypts them with a randomly generated key and a certified and secure cryptographic algorithm. When the document is shared, the encrypted tags containing the sensitive information cannot be viewed without the key. These encrypted tags contain the FGAC keyword as an XML Attribute with those teams' identification numbers, that can access and decrypt them. In order to access this data, an external team needs to provide all required information, e.g., team and incident identifiers.

We save the users in a database and give them two tag-attributes: one specifies the clearance group the user belongs to and the other is a specific tag belonging to the user. These attributes can be used when the SOC of the original incident

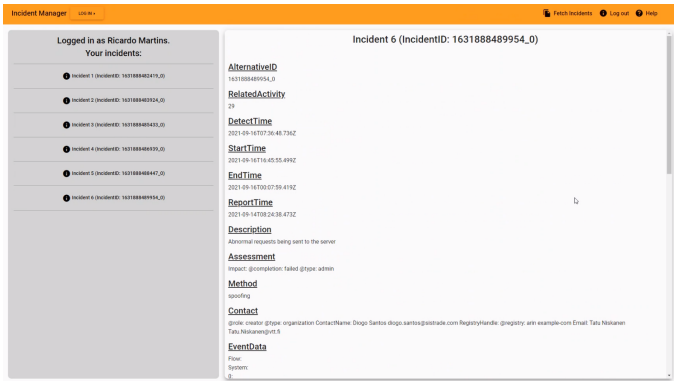

Fig. 1. The basic view of the dashboard for a user that has access to all incident data. This is the case for at least the SOC that first discovers the incident.

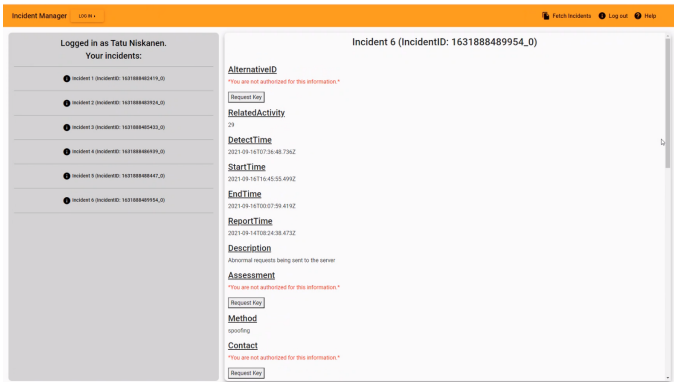

Fig. 2. In this dashboard the user does not have access to all incident information. The system presents a red "You are not authorized for this information" label to them instead. Now the user can click the button below the red notification to request access for this particular field for this particular incident.

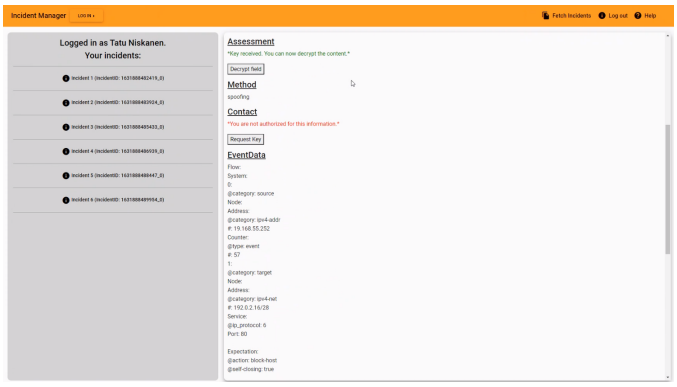

Fig. 3. Here the user has been granted access to one of the fields. The system displays a message in green: "Key received. You can now decrypt the content". Now the user can click the button to decrypt the information.

TABLE I
IODEF FILE FIELDS

Field	Multiplicity	Description
IncidentID	One	An incident identification number assigned to this incident by the CSIRT who creates the IODEF document.
AlternativeID	Zero or one	The incidents ID numbers used by other CSIRTs to refer to the incident described in the document.
RelatedActivity	Zero or one	The ID numbers of the incidents linked to the one described in this document.
DetectTime	Zero or one	Time at which the incident was detected for the first time.
StartTime	Zero or one	Time at which the incident started.
EndTime	Zero or one	Time at which the incident ended.
ReportTime	One	Time at which the incident was reported.
Description	Zero or more	Non-formatted textual description of the event.
Assessment	One or More	A characterization of the incident impact.
Method	Zero or More	Techniques used by the intruder during the incident.
Contact	One or More	Contact information for the groups involved in the incident.
EventData	Zero or More	Description of the events involving the incident.
History	Zero or More	A log, of the events or the notable actions which took place during the incident management.
AdditionalData	Zero or More	Mechanism which extends the data model.

decides who to disseminate information to; they can choose to distribute the IODEF information based on the clearance groups or by the specific user. The IODEF document simply needs to be populated with the corresponding tag-attributes within the information fields.

From the point of view of the information receiving parties, the web front-end compares the tags within the IODEF document to the ones held by the user that is currently logged in to the dashboard application. When the tags match, i.e the user or their group is allowed to access the encrypted information, the web front-end displays the content to the user. Otherwise the user sees a placeholder text "You are not authorized for this information".

In our PoC, we have users from two different organizations. For some of them some information is encrypted and therefore un-viewable. However, such a user can request a key for decrypting the information, and the original SOC can accept or decline the request.the demonstration we have users from two different organizations. In Figure 1 a user from the originating SOC has full view of the incident information. Now, in Figure 2 a user from another SOC can see partial information about the incident. There is, however an option of requesting the key for each of the encrypted fields. In the final Figure 3 the second user has been granted access to one of the fields and can move forward with decryption.

IV. DISCUSSION

This proof-of-concept demonstrated a fine-grained way of sharing information between SOCs. Because of the detailed control over who can access the data, the originating SOC can be reassured that only the minimal necessary amount of information about their processes is exposed to external collaborators. On the other hand, the granular nature of this method requires good communication and networking skills from the personnel of the SOCs; the hard technical controls are very limiting if there is no ongoing human-to-human contact between the people analyzing the incidents and making decisions on who would benefit from the information, and how much information should be shared. Similarly, when requesting access to encrypted data in the incident reports, it is also important to have a good rapport with the other SOCs.

The FGAC on the shared information is also beneficial in keeping as much information out of the hands of attackers as possible. However, if we assume that the access control and encryption are capable of thwarting traditional hacking attacks, we still need to consider social engineering attacks, that try to take advantage of any weaknesses in the collaboration between SOCs.

Creating and maintaining a strong trust relationship is very vital in this information sharing scheme. This means that both the encryption algorithm and key length should be designed precisely for this purpose. Even though the proof-of-concept wasn't focused on these kinds of technical aspects, but instead in demonstrating the visualisation and sharing functionalities of incident information, previous work defined an Attribute Based Encryption (ABE) scheme for another project use case that could perhaps be applied also to our scheme [24].

In this demonstration we implemented an access control tag that allowed for encrypting and decrypting individual fields of data in an incident report. For future work, these incident reports could be further enriched with insights from the cybersecurity analysts. The current version of the dashboard is plain and simple, and in a future project it might be useful to explore different kinds of visualizations for the incident data. The randomly generated events in the PoC allow for fine-tuning and testing different options while the possibilities and limits of this system are explored. However, in a future project it would be interesting to replace the generated events with real data.

V. CONCLUSIONS

In order to facilitate collaboration between SOCs, a sufficient level of trust needs to be established. In this paper we have presented a system for sharing security incident

information in a granular way. The access to the information can be granted to either user groups or individual users, and it is possible to request or grant access to individual data points within the incident documents. Thus, the SOCs have a great amount of control on what information to reveal to which collaborators. These technical safeguards enhance trust between SOCs and also limit the attacker's opportunities for gaining insight into how their attack has succeeded.

ACKNOWLEDGMENTS

This work has been conducted in the Secure Collaborative Intelligent Industrial Assets (SeCoIIA) project that aims at securing the digital transition of manufacturing industry towards more connected, collaborative, flexible and automated production techniques. The project has received funding from the European Union's Horizon 2020 research and innovation programme under grant agreement No 871967.

REFERENCES

[1] R. Waslo, T. Lewis, R. Hajj, and R. Carton, "Industry 4.0 and cybersecurity: Managing risk in an age of connected production," *Deloitte Insights.*, 2017.

[2] J. Simola, "Comparative research of cybersecurity information sharing models," *Information & Security*, vol. 43, no. 2, pp. 175–195, 2019.

[3] European Union Agency for Cybersecurity, "Cyber security information sharing: An overview of regulatory and non-regulatory approaches," 2015.

[4] A. Pala and J. Zhuang, "Information sharing in cybersecurity: A review," *Decision Analysis*, vol. 16, no. 3, pp. 172–196, 2019.

[5] "Cyber-threat intelligence information sharing guide," 2021, accessed 14-03-2022. [Online]. Available: https://www.gov.uk/government/publications/cyber-threat-intelligence-information-sharing

[6] S. G. Radu, "Comparative analysis of security operations centre architectures; proposals and architectural considerations for frameworks and operating models," in *Innovative Security Solutions for Information Technology and Communications*, I. Bica and R. Reyhanitabar, Eds. Cham: Springer International Publishing, 2016, pp. 248–260.

[7] European Union Agency for Cybersecurity, "Exploring the opportunities and limitations of current threat intelligence platforms," 2018.

[8] H. Khurana, J. Basney, M. Bakht, M. Freemon, V. Welch, and R. Butler, "Palantir: A framework for collaborative incident response and investigation," in *Proceedings of the 8th Symposium on Identity and Trust on the Internet*, ser. IDtrust '09. New York, NY, USA: Association for Computing Machinery, 2009, p. 38–51. [Online]. Available: https://doi.org/10.1145/1527017.1527023

[9] A. Connell, T. Palko, and H. Yasar, "Cerebro: A platform for collaborative incident response and investigation," in *2013 IEEE International Conference on Technologies for Homeland Security (HST)*, 2013, pp. 241–245.

[10] G. Settanni, F. Skopik, Y. Shovgenya, R. Fiedler, M. Carolan, D. Conroy, K. Boettinger, M. Gall, G. Brost, C. Ponchel, M. Haustein, H. Kaufmann, K. Theuerkauf, and P. Olli, "A collaborative cyber incident management system for european interconnected critical infrastructures," *Journal of Information Security and Applications*, vol. 34, pp. 166–182, 2017. [Online]. Available: https://www.sciencedirect.com/science/article/pii/S2214212616300576

[11] G. Meng, Y. Liu, J. Zhang, A. Pokluda, and R. Boutaba, "Collaborative security: A survey and taxonomy," *ACM Comput. Surv.*, vol. 48, no. 1, Jul. 2015. [Online]. Available: https://doi.org/10.1145/2785733

[12] N. Alexopoulos, E. Vasilomanolakis, N. R. Ivánkó, and M. Mühlhäuser, "Towards Blockchain-Based Collaborative Intrusion Detection Systems," in *Critical Information Infrastructures Security*, G. D'Agostino and A. Scala, Eds. Cham: Springer International Publishing, 2018, pp. 107–118.

[13] J. M. de Fuentes, L. González-Manzano, J. Tapiador, and P. Peris-Lopez, "Pracis: Privacy-preserving and aggregatable cybersecurity information sharing," *Computers & Security*, vol. 69, pp. 127–141, 2017, security Data Science and Cyber Threat Management. [Online]. Available: https://www.sciencedirect.com/science/article/pii/S0167404816301821

[14] C. Wagner, A. Dulaunoy, G. Wagener, and A. Iklody, "Misp: The design and implementation of a collaborative threat intelligence sharing platform," in *Proceedings of the 2016 ACM on Workshop on Information Sharing and Collaborative Security*, ser. WISCS '16. New York, NY, USA: Association for Computing Machinery, 2016, p. 49–56. [Online]. Available: https://doi.org/10.1145/2994539.2994542

[15] R. Danyliw, "The Incident Object Description Exchange Format Version 2," RFC 7970, Nov. 2016. [Online]. Available: https://rfc-editor.org/rfc/rfc7970.txt

[16] R. S. Sandhu, "Role-based access control," ser. Advances in Computers, M. V. Zelkowitz, Ed. Elsevier, 1998, vol. 46, pp. 237–286, portions of this chapter have been published earlier in Sandhu et al. (1996), Sandhu (1996), Sandhu and Bhamidipati (1997), Sandhu et al. (1997) and Sandhu and Feinstein (1994). [Online]. Available: https://www.sciencedirect.com/science/article/pii/S0065245808602065

[17] W. Tolone, G.-J. Ahn, T. Pai, and S.-P. Hong, "Access control in collaborative systems," *ACM Comput. Surv.*, vol. 37, no. 1, p. 29–41, Mar. 2005. [Online]. Available: https://doi.org/10.1145/1057977.1057979

[18] F. Paci, A. Squicciarini, and N. Zannone, "Survey on access control for community-centered collaborative systems," *ACM Comput. Surv.*, vol. 51, no. 1, Jan. 2018. [Online]. Available: https://doi.org/10.1145/3146025

[19] K. Albulayhi, A. Abuhussein, F. Alsubaei, and F. T. Sheldon, "Fine-grained access control in the era of cloud computing: An analytical review," in *2020 10th Annual Computing and Communication Workshop and Conference (CCWC)*, 2020, pp. 0748–0755.

[20] E. Damiani, S. De Capitani di Vimercati, S. Paraboschi, and P. Samarati, "A fine-grained access control system for xml documents," *ACM Trans. Inf. Syst. Secur.*, vol. 5, no. 2, p. 169–202, May 2002. [Online]. Available: https://doi.org/10.1145/505586.505590

[21] B. Luo, D. Lee, W.-C. Lee, and P. Liu, "Qfilter: rewriting insecure xml queries to secure ones using non-deterministic finite automata," *The VLDB Journal*, vol. 20, no. 3, pp. 397–415, 2011.

[22] ——, "A flexible framework for architecting xml access control enforcement mechanisms," in *Workshop on Secure Data Management*. Springer, 2004, pp. 133–147.

[23] J. Meijer, R. Danyliw, and Y. Demchenko, "The Incident Object Description Exchange Format," RFC 5070, Dec. 2007. [Online]. Available: https://www.rfc-editor.org/info/rfc5070

[24] A. Bkakria, R. Yaich, and W. Arabi, "Secure and robust cyber security threat information sharing," in *International Symposium on Foundations & Practice of Security*, 2021.