Cyber Threat Intelligence as an Knowledge Sharing Platform

Intan Maratus Sholihah, Hermawan Setiawan and
Olga Geby Nabila

December 6, 2021

Cyber Threat Intelligence as an Knowledge Sharing Platform

Intan Maratus Sholihah
Crypto Software Engineering
Politeknik Siber dan Sandi Negara
Bogor, Indonesia
intan.maratus@student.poltekssn.ac.id

Hermawan Setiawan
Crypto Software Engineering
Politeknik Siber dan Sandi Negara
Bogor, Indonesia
hermawan.setiawan@poltekssn.ac.id

Olga Geby Nabila
Crypto Software Engineering
Politeknik Siber dan Sandi Negara
Bogor, Indonesia
olga.geby@student.poltekssn.ac.id

***Abstract*— this research will develop a web-based Information Sharing and Analysis Center (ISAC) platform as a means to collect information and view a list of attacks and threats in the cyber world. The list of attacks and threats will be obtained through the Malware Information Sharing Platform (MISP) and processed using the OpenCTI platform.**

Keywords— knowledge sharing

I. Introduction

Information Sharing and Analysis Center (ISAC) is a non-profit organization that provides a central resource for gathering information on cyber threats on critical infrastructure that can share information between the public and private sectors [4]. ISAC has five benefits for the cyber world, the first is increasing awareness of the threats and risks of each stakeholder in the digital world and providing ideas to stakeholders to find prevention, protection and defense measures for their information [3]. Second, as a means to share cybersecurity information to increase the knowledge of stakeholders in terms of reporting, strategy or operational monitoring, and technical or legal monitoring [3]. Third, eradicating cyber crimes that require preventive measures so as to reduce the chances of these crimes occurring [3]. Fourth, produce a standard for cyber security as one of the real examples in information sharing [3]. Fifth, it is used to control cybersecurity vulnerabilities and incidents [3]. Based on these five benefits, several resources are needed to run ISAC, both in the areas of strategy, technology, and human resources.

Parties that can contribute to ISAC are the public and private sectors. There are three kinds of information sharing, namely between the public-public sector, private-private, and public-private [3]. There are five important parts to the ISAC, including the structure of strategy, technology, human resources, management, and economics [3]. In the field of technology, it is a platform that is used to share information [3]. There are two types of cybersecurity information that can be used to share information, namely technical-threat indicators and contextual threat intelligence [1]. Technical-threat indicators contain Cyber-threat Indicators such as incidents, vulnerabilities and threats [1]. Meanwhile, contextual-threat intelligence contains mitigation, situational awareness, best practices and strategy analysis [1]. From the existing information data, it can be used to collaborate effectively in tackling threat risks and detecting threats [1].

Cyber Threat Intelligence (CTI) is a platform used by every organization to identify, assess, control and respond to cyber threats [7]. OpenCTI is an open source platform that can be used by an organization to store, manage, visualize, and as a means of sharing knowledge about cyber security threats [8]. The main purpose of the OpenCTI platform is to provide a database of knowledge about cyber threats and cyber operations [8]. Users can use the OpenCTI framework to visualize data retrieved from the openCTI platform and can also be used to access all the knowledge contained in the framework. In addition, OpenCTI is also used to display technical information (such as TTP and observations) and non-technical information (such as attribution, victimology, etc.) [8]. OpenCTI data retrieval can be done by integrating with the Application Programming Interface (API). The information data can be modified automatically by the user to produce an attractive data visualization according to the user's needs [8]. The API integration process in OpenCTI can be done with the pycti library which is designed to integrate into the OpenCTI framework [8]. Threat and attack information data is obtained from the Malware Information Sharing Platform (MISP). MISP is a platform that lists threats and attacks that are open source..

II. Comparisson of research

II.1 Information sharing in cybersecurity

This research was conducted by Solange Ghernaouti, Léonore Cellier and Bastien Wanner by analyzing the needs and constraints on information sharing to produce cyber security and resilience [3]. This study recommends the development of a platform for Information Sharing and Analysis. The things needed in the development of the ISAC platform are to define the type of information to be shared, define the IT infrastructure requirements needed on the ISAC platform, and define how the information is collected, stored, processed, served, returned, and secured.

II.2. Developing a cyber threat intelligence sharing platform for South African organisations

This research was conducted by Muwoya Mutemwa, Njabulo Mkhonto and Jabu Mtsweni [18]. This study discusses the development of a Cyber Threat Intelligence platform for organizations in South Africa. The reason for the establishment of the CTI platform is as a place to collect, analyze, and classify various attacks and threats from various data sources including integration with other sources. The platform to be developed also uses the Traffic Light Protocol (TLP) to classify threat information data for public or private.

II.3 Web service and plug-in architecture for flexibility and openness of environmental data sharing platforms

This research was conducted by S. Knox, P. Meler and J. Harou [19]. This study discusses the model of the platform used for data sharing. The model used for data sharing utilizes a web service interface that functions to manage input data that is entered and managed for display. The web service interface is also connected to the database to store input data. The managed input data is displayed on the platform interface that connects with the user.

II.4 Information Sharing in Cybersecurity: A Review

This research was conducted by A. Pala, J. Zhuang [1]. This study discusses the reasons why ISAC is needed, who is involved in ISAC, types of information that can be shared, architecture, and benefits of ISAC. One of the reasons for the establishment of ISAC is the increase in cyber attacks which are directly proportional to technological developments. So, we need a way to prevent the increase in cyber attacks. As noted in this study, ISAC can be used to strengthen cyberattack prevention and response capabilities to cyberattacks. ISAC also provides a feature that can be used to gather knowledge and effective collaboration for threats and risks that can occur, improve attack detection and analyze investment strategies in the cyber world.

II.5 Interoperability Challenges in the Cybersecurity Information Sharing Ecosystem

This research was conducted by Konstantinos Rantos, et al. [7]. This study discusses Cyber Threat Intelligence (CTI). CTI is a platform that contains knowledge or services about cyber threats that can be used to carry out cyber defenses that are more effective and efficient. This study also discusses how to analyze CTI data obtained from various sources according to four layers at the data sharing stage, including legal, policies and procedures, semantics and syntactics, as well as technical interopability characteristics. Legal is a layer that contains data restrictions, privacy, and data obligations to share. Policies and procedures contain data recipients, business processes and objectives and instructions to the organization. Semantics and syntax contain data types and formats that can be used for information sharing. The technical layer contains how the process of transmitting and securing the shared data.

II.6 Assessment of the Information Sharing and Analysis Center Model

This study was conducted by McCarthy et al. [5]. This study discusses what must be in ISAC, including [5]:

a. To provide an effective forum for sharing information in certain sectors with other organizations or the government.

b. Provide analysis of relevant threats, vulnerabilities and incidents.

c. Provide features to share threat alerts, threat assessments and threat notifications with ISAC members.

d. Provide a quick response in an emergency situation effectively by communicating and coordinating among ISAC members.

Based on the four points above, ISAC can function as a platform to communicate cyber security in each sector, support information sharing activities between ISAC members and between the government and the National Critical Infrastructure (IKN) sector [5].

III. Testing

The Information Sharing and Analysis Center (ISAC) system is a web-based system developed to make it easier for users to access it from various electronic devices. In general, the ISAC system was created to make it easier for users to share and/or obtain information related to threats, attacks and news within the scope of cybersecurity. In the formation of this ISAC system prototype, the design method used includes an overview of the system created, analysis of functional and non-functional requirements, system design, and implementation of the ISAC system prototype.

After determining the general description of the system to be made, the next step is to analyze what needs are needed to build an ISAC system prototype. This analysis was carried out by studying literature and discussions with the locus. It was found that the system that must be built must have basic functions including an input form for the user to make a 'complaint' in order to be able to share information with each other. From these needs, certain tools and functions are needed that are considered to be able to meet these needs. The following are the requirements needed to build the ISAC platform.

IV.1. Functional Needs

Functional requirements are requirements related to a process in the system that must be met. Functional requirements are obtained from benchmarking results on ENISA's ISAC products which then obtain the minimum features available on the ISAC product. After that, a literature study was carried out on the existing aspects and a list of functional requirements was obtained

IV. Conclusion

The integration of the OpenCTI platform has not been successful because there was an error on the OpenCTI server when it was going to parse data from the Malware Information Sharing Platform. However, threat and attack data can already be displayed by integrating the website with the API from MISP. Server running on the Ubuntu 20.04 LTS Virtual Machine.

References

[1] A. Pala and J. Zhuang, “Information sharing in cybersecurity: A review,” Decis. Anal., vol. 16, no. 3, pp. 172–196, 2019, doi: 10.1287/deca.2018.0387.

[2] “Jumlah Serangan Siber Meningkat.” .

[3] S. Ghernaouti, L. Cellier, and B. Wanner, “Information sharing in cybersecurity : Enhancing security, trust and privacy by capacity building,” 2019 3rd Cyber Secur. Netw. Conf. CSNet 2019, pp. 58–62, 2019, doi: 10.1109/CSNet47905.2019.9108944.

[4] ENISA, Information Sharing and Analysis Centres (ISACs) Cooperative models. 2017.

[5] C. McCarthy, K. Harnett, A. Carter, and C. Hatipoglu, “Assessment of the Information Sharing and Analysis Center Model,” Nhtsa, no. October, 2014.