Overview of Prioritization Model for National Critical Sectors Protection

Ariani[1] and Muhammad Salman[2]
[1,2]Electrical Engineering, Universitas Indonesia, Depok, Indonesia
[1]**arianitkj2@gmail.com**, [2]**muhammad.salman@ui.ac.id**

ARTICLE INFO

Article History
Received 21 Oct 2020
Received in revised form 11 Jan 2021
Accepted 08 Mar 2021

Keywords:
critical sectors, protection, prioritizing response, service level agreement, security monitoring;

ABSTRACT

The national critical sectors are an important sector that should be paramount in maintaining the state security when cybersecurity incident occurs. The national critical sectors aim to secure facilities, networks, information and physical assets. Protection against national criticality involves protection of both physical and cyber components, where cyber protection plan must be included in the national defense strategy. This article aims to propose a design of prioritizing model as early detection of cyber incidents as part of managing the incident and protecting the national critical sector.

I. INTRODUCTION

Cyber-attacks or other undesirable cybersecurity incidents can cause disruption to our daily life. The impact of cybersecurity is one of the challenges in public life and even a challenge for the national defense of a state or country, thus it is required to have a cybersecurity strategy to be part of a protection plan program [1] to protect the national assets.

Since World War II, safeguarding national resources and assets have become part of national defense planning. Along with cyberspace development, the national defense's perception has begun to pay attention to securing information and physical-based facilities, networks, and assets [2]. Regner et al. stated that a country must define priorities, objectives, goals, and scope which cover cyberspace, cyber governance, cyber defense, cybersecurity, and cybercrime when designing a national strategy [3].

Important components related to this domain are cyber policy and cyber governance- thatuseful as national instruments to regulate and protect cyberspace. One of the regulations, which is noteworthy as national defense, defines critical sectors that become the most priority.

The definition of critical sectors are a sector group that must be protected as a top priority when an

ISSN 2636-9680
eISSN 2682-9266

incident occurs because its impact can lead to the collapse of a country. Critical sectors are sectors that have not only strategic infrastructure but also strategic information.

Therefore, it is important to focus on proactive steps to build the resilience of individuals, organizations, and countries against security threats such as cybersecurity capacity. One focus area is incident management and response, scoping on responding to the security incident and protecting infrastructure [4]. Enisa [5] stated that the national cybersecurity agencies, who have led the role of protection cybersecurity needed to the critical sectors (they have called it critical infrastructure), aim to provide the support for automated-prioritized handling of incidents affecting. So, the incidents that involve critical network assets are notified automatically, and the handling is prioritized.

Related to the protection infrastructure, NIST develops a framework to identify prioritized, flexible, repeatable, performance-based, and cost-effective approaches, including information security measures and controls. It can be adopted by other organizations [6]. One of the core frameworks is "detect", which makes it possible to indicate events that threaten cybersecurity. Examples of implementation within this function include Anomalies and Events; Security Monitoring; and Detection Processes.

Among the incredible number of events detected by detection tools like security monitoring, the handle response is considered the Service Level Agreement (SLA) management and security management. From a business perspective, the SLA aims to offer agreement between the users and the Service Provider, and it is to establish what is effectively granted in terms of quality [6]. From a defense perspective, SLA means the severity level on response prioritizing incidents that occurred.

The relationship between the national defense strategy in protecting critical sectors with response prioritizing incidents is how to design plans and programs specially made to protect the national critical sector security. A comprehensive design is needed to secure the critical sectors from a cyber perspective.

II. RELATED WORK

In [7], the authors have proposed SLA Mapping to be one part of the design SLA based on workflow management on intrusion tolerance with case cloud computing service. Jusas et al. [8] have proposed a logical filter to attack detection. They have said that the general classification of cyber-attacks includes the stage of the cyber kill chain, type attack, and target attack (object groups, state institutions, economic branches, social, etc.). So, the prioritizing an incident must pay attention to them, and the variable related to national cyber defense is the targeted attack.

Spring et al. [9] have proposed prioritizing vulnerability response specific to vulnerability categorization that occurs to stakeholders. The national sector's diversity must accommodate the primary function of handling rather than being included in optional features that are difficult to use.

In [10] [11], they have proposed a method to define an alert intrusion detection system's response as severity level selected, which focuses on target anomaly. It gives specific results for each event category when describing suspicious activities one type of suspicious event.

Bernieri et al. [12] have researched decision making method on intrusion detection as protection tools of critical infrastructure. The method used is based on Analytic Hierarchy Process (AHP). Their experiment identified the highlight of the methodology that have designed for the decision support.

Wang et al. [13] have proposed risk decision-making theory to prioritize incidents by minimizing the sum of business losses and risks. Imamverdiyev [14], Al-Subhi [15], and Berinjan [16] used Fuzzy decision making to prioritizing the incident, but without specific indicators. Another research was conducted by Dileep Kumar Singh [17]. He has implemented multicultural decision making using the ELECTRE method. Research on the priority of incidents was also had carried out by Renners et al. since 2017 [18].

They determine priority incidents by prioritizing rules with a tree model. In 2019, Renners et al. [19] modelled priority incidents by determining policies that have set rules and derived attributes; this policy is based on adaptive learning. Adaptive learning is used to enable an analyst to formulate feedback on incident responses. In [20] [21], Anuar et al have proposed incident prioritization using the Analytic Hierarchy Process (AHP) method and Risk Index Model. Furthermore, they have made detailed indicators that must be considered in determining priority incidents.

III. PROPOSED APPROACH

Our approach's baseline is first to find a prioritization mechanism for the security monitoring setup that has been researched by the researcher. It will give insights into the expected efficiency of proposed strategies to setup security monitoring. We could propose a design for automatically computing the prioritized result out of SLA mapping from these insights. The proposed prioritization model is illustrated in Fig. 1.

The first focus study defines severity by calculating features for indicator needed, which it could be customized on the feature of security monitoring. The next stage, mapping the sectors, which is defined as the national critical sectors. Then, the decision-making method needs research in-depth applicable to the real environment.

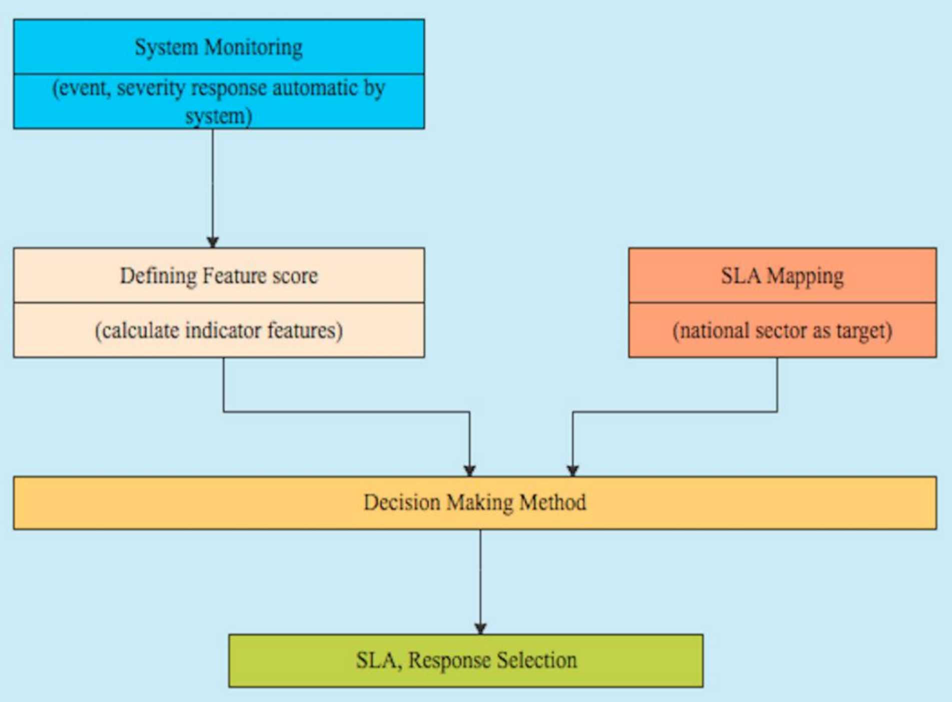
System Monitoring
(event, severity response automatic by system)
Defining Feature score
(calculate indicator features)
SLA Mapping
(national sector as target)
Decision Making Method
SLA, Response Selection

Fig. 1. Prioritization Model

A. Security Monitoring

The security monitoring system is a system used to secure infrastructure, usually using an intrusion detection system. The security monitoring system provides information in the form of logs and activities that occur on the network. Several security monitoring systems offer the anomaly category that an anomaly occurs, and the SLA system is automatically generated.

B. Defining Features Score

The next phase is defining the severity score by calculating features. This method was adopted from a previous research [10], which used this stage to get the score of each variable generated by the monitoring system's features by calculating the features into a formula to determine the response based on the average feature score. Every feature has a type of indicator which is defined by review of some research. In addition, these indicators are classified into 2 types- urgent and critical- which are displayed in TABLE 1 and it is illustrated in Fig. 2. Each indicator will be calculated by the appropriate formula.

TABLE 1. Indicator Classification

No.	Critical	Urgent
1	Criticality	Severity
2	Maintainability	Exploitability
3	Replace-ability	Similarity
4	Dependability	Sensitivity
5	Control	Frequency
6	Impact(CIA)	Vulnerability

No.	Critical	Urgent
7	Risk	Activity
8	Cost	Reliability

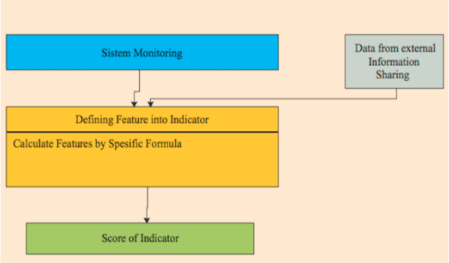
Sistem Monitoring
Data from external Information Sharing
Defining Feature into Indicator
Calculate Features by Spesific Formula
Score of Indicator

Fig. 2. Defining features Process

The critical type refers to a comparative state in which one incident is very important because of impacts are the three main attributes that are common in security, such as confidentiality, integrity, and availability (CIA). The Urgent type refers to circumstances where one incident requires a quick response compared to other incidents based on the possibility of threats and vulnerabilities.

Research and experiment have been done for this phase. It shows that the priority setting phase produces more detailed information in defining if the same event is a priority or not due to different feature scores. Priority responses given can differ depending on the most impact on the network so that it is quite sufficient to be applied with the response model.

C. SLA Mapping

The SLA Mapping is a service level agreement that is defining as important and prioritizing the critical sectors. The intension of protecting among the national defense by secure the government's critical sectors is defined. Those sectors list could be customized depending on the country regulation.

D. Decision-Making Method

The next process is the decision-making method as an algorithm or science method to give a decisive response. The method uses a decision-making algorithm because it does not need a learning process by training data. And lastly, after all the processes above, the result is a response selected as a service level handling incident. So, the incident handler can choose which the incident must be responded.

E. Discussion and Limitation

Each phase of prioritizing design to determine the service level agreement's response is important to determine effectiveness in analyzing a suspicious anomaly found in the monitoring system. Effective incident management provides benefits that allow an incident to be handled quickly under the appropriate time frame and handling process before the incident has a more significant impact. In this way, we can minimize the target's impact, especially national critical sectors, with good management visibility.

The proposed approach's focus is the design to determine the priority response of service level agreement, where the priority response is one of the incident management processes, triage incident. Although during our study, it did not evaluate all stages of the proposed design. However, theoretically and technically, it can be applied to the real environment.

Based on our experiment with sample IDS data attack, it shows that the SLA Mapping is able to prioritize incidents with regard to the impact of the most dangerous intrusion by considering the critical sectors even though the same intrusion occurred in some targets.

IV. CONCLUSION AND FUTURE WORK

Prioritizing response service level agreement on the national critical sectors is very important as a national defense firm. The proposed system design is a design based on an analysis of several related works' protection needs and national security. Even though the design experiment has not been entirely carried out, it is hoped that the proposed design could be an alternative in determining security monitoring priorities effectively and on target.

Further research is still required as an in-depth analysis of the specific method used, in term of the appropriate decision-making method to be implemented in the real security monitoring system.

V. REFERENCES

[1] D. Snyder, J. D. Powers, E. Bodine-Baron, B. Fox, L. Kendrick and M. H. Powell, "Findings and Recommendations," in *Improving the Cybersecurity of U.S. Air Force Military Systems Throughout Their Life Cycles*, RAND Corporation, p. 42, 2015.

[2] E. NICKOLOV, "Critical Information Infrastructure Protection: Analysis, Evaluation And Expectations," *Information & Security, An International Journal*, vol. 17, pp. 105-119, 2005.

[3] R. Sabillon, V. Cavaller and J. Cano, "National Cyber Security Strategies: Global Trends in Cyberspace," *International Journal of Computer Science and Software Engineering (IJCSSE)*, vol. 5, no. 5, pp. 67-81, May 2016.

[4] W. H. Dutton, S. Creese, R. Shillair and M. Bada, "Cybersecurity Capacity: Does It Matter?," *Journal of Information Policy*, vol. 9, pp. 280-306, 2019.

[5] Enisa, "Methodologies for the identification of Critical Information Infrastructure assets and services," 2015. [Online]. Available: https://www.enisa.europa.eu/publications/. [Accessed 2020].

[6] NIST, "Framework for Improving Critical Infrastructure Cybersecurity," 16 April 2018. [Online]. Available: https://nvlpubs.nist.gov. [Accessed 20 8 2020].

[7] M. Ficco and M. Rak, "Intrusion Tolerance as a Service: A SLA-Based Solution," in *Int. Conf. on Cloud Computing and Services Science*, 2012.

[8] V. Jusas, S. Japertas, T. Baksys and S. Bhandari, "Logical Filter Approach for Early Stage Cyber-Attack Detection," *Computer Science and Information Systems*, vol. 16, no. 2, p. 491–514, 2019.

[9] J. Spring, E. Hatleback, A. Householder, A. Manion and D. Shick, "Prioritizing Vulnerability Response: A Stakeholder-Specific Vulnerability Categorization," Software Engineering Institute Carnegie Mellon University, White Paper, 5 December 2019. [Online]. Available: https://resources.sei.cmu.edu/.

[10] Ariani and M. Salman, "Intrusion Response System based on Time Management Concept with the Critical IP Address as a

Parameter," *International Journal of Advanced Science and Technology (IJAST)*, vol. 29, no. 7s, pp. 3280-3288, May 2020.

[11] Ariani and M. Salman, "priority responses given can differ depending on the most impact to the network," in *The 6th International Conference on Science and Technology*, 2020.

[12] G. Bernieri, S. Damiani, F. D. Moro, L. Faramondi, F. Pascucci and F. Tambone, "A Multiple-Criteria Decision Making Method as Support for Critical Infrastructure Protection and Intrusion Detection System," in *42nd Annual Conference of the IEEE Industrial Electronics Society*, 2016.

[13] D. Wang, Z. Zhiqiang and a. S. Hao, "An Incident Prioritization Algorithm Based on BDIM," in *Computer Modeling and Simulation, International Conference* , 2010.

[14] Y. Imamverdiyev, "An Information Security Incident Prioritization Method," 2013.

[15] K. Alsubhi, E. Al-Shaer and a. R. Boutaba, "Alert prioritization in Intrusion Detection Systems," 2008.

[16] S. Berenjian, M. Shajari, N. Farshid and a. M. Hatamian, "Intelligent Automated Intrusion Response System based on Fuzzy Decision Making and Risk Assessment," in *2016 IEEE 8th International Conference on Intelligent Systems*, 2016.

[17] D. Singh and P. Kaushik, "Intrusion response prioritization based on fuzzy ELECTRE multiple criteria decision-making technique," in *Journal of Information Security and Applications*, 2019.

[18] L. Renners, F. Heine and a. G. Rodosek, "Modeling and learning incident prioritization," in *IDAACS*, 2017.

[19] L. Renners, F. Heine, C. Kleiner and a. G. Rodosek, "Adaptive and intelligible prioritization for network security incidents," in *Advances in Intelligent Systems and Computing*, 2019.

[20] N. B. Anuar, M. Papadaki, S. Furnell and a. N. Clarke, "A response selection model for intrusion response systems: Response Strategy Model (RSM)," *Security and Communication Networks*, pp. 1831-1848, 2013.

[21] N. B. Anuar, S. Furnell, M. Papadaki and N. Clarke, "A risk index model for security incident prioritisation," in *Australian Information Security Management Conference*, Perth Western, 2011.