International Journal of Critical Infrastructure Protection 26 (2019) 100312

Contents lists available at ScienceDirect

International Journal of Critical Infrastructure Protection

journal homepage: www.elsevier.com/locate/ijcip

The enhanced security control model for critical infrastructures with the blocking prioritization process to cyber threats in power system

Choong-Hee Han[a], Soon-Tai Park[b], Sang-Joon Lee[c,*]

[a] Security Information Strategy Office of KPX-Korea Power Exchange, 625 Bitgaram-ro, Naju-si Jeollanam-do 58327,Republic of Korea
[b] Security Threat Response R&D Team of Korea Internet & Security Agency (KISA), 9 Jinheung-gil, Naju-si Jeollanam-do 58324, Republic of Korea
[c] Departement of Business Administration Graduate School of Chonnam National University, 77 Yongbong-ro Buk-gu, Gwangju 61186, Republic of Korea

ARTICLE INFO

Article history:
Received 17 April 2019
Accepted 25 July 2019
Available online 29 July 2019

Keywords:
Incident response
Security operation center
Cyber-attacks
Cyber threat intelligence
Critical infrastructure Protection

ABSTRACT

There have been a lot of efforts and studies to improve the safety of critical infrastructures. As one of efforts, there have been numerous constructions of security operation center (SOC) to protect against cyber-attacks. Unfortunately, it is too difficult to protect from cyber-attacks, because there are too many security events to analyse and respond. Reducing security events are very essential to improve the efficiency of incidents response. In this paper, we studied four years cyber threats against a Korean electric power organization by analysing IPS and FW raw data. As a result of this analysis, we found that 95% of all cyber-attacks were from foreign nations. If an IT system is not related with foreign business, we should think about blocking unnecessary foreign IP ranges. So, we propose the Enhanced Security Control (ESC) model with Blocking Prioritization (BP) process for critical infrastructures to improve daily incidents response activities. This ESC model has a BP process with six factors to consider when deciding which IT systems to be blocked from foreign IP ranges: foreign relation, real login, blocking complexity, stop tolerance, outer relation and stop impact. By considering these six factors, the ESC model can make it possible to prioritize Blocking Impact Degree (BID) of IT systems and help making decision to block from unnecessary foreign IP ranges. This ESC model will reduce security events and make a better condition for concentration on the remaining unblocked and crucial IT systems.

1. Introduction

Due to the breakneck proliferation of advanced cyber threats, cyber security operations today face challenges that are conflating at an exponential rate [1]. Cyber-attacks are occurring with ever increasing frequency these days due to the development of the Internet infrastructure and the spread of automated attack tools, and such attacks are becoming increasingly intelligent over time. In addition, cyber-attacks were made in the past against unspecified individuals for the purpose of showing off the attackers' skills and satisfying their curiosity, while secondary attacks were caused by securing zombie PCs. However, most cyber-attacks these days aim to cause social chaos, steal personal data, or obstruct or damage the business of a specific group or organization. For example, spear phishing, which is used to spread malicious codes or infiltrate a specific attack group, increased by 55% in 2015 from the previous year, whereas e-mail attack targets decreased by 39%. These figures indicate that while attacks are more frequent, the target is changing from unspecified individuals to specific groups [2]. In addition, the file-less attack [3], in which an attack is launched without a malicious code file and without installing malicious code files in the target system or PC, is increasing sharply (i.e. 3782 attacks in 2016, showing a fourfold increase over the previous year [4]). Such cyber-attacks can be made more frequently by reducing the time required to prepare an attack by using a similar attack technique or re-using the infrastructure. However, there are only a few experts who can analyze or respond to these attacks, making it difficult to respond immediately or take measures against cyber-attacks before damages are caused [5].

Cyber-attackers make transit & spread places multi-leveled to avoid detection. Cyber-attackers change transit & spread places continuously to minimize exposure and bypass incident response activities. The most critical problem of the web-based IT systems is that web-browsers are not in control of the web-server application: vulnerabilities like SQL-injection, Cross Site Script and Active-X [6,7]. So the web-browser is in danger of being easily changed, managed, and contaminated by cyber-attackers. From A1 to A10 in OWASP TOP 10, there are many vulnerabilities of the web based

* Corresponding author.
E-mail addresses: justicehan@kpx.or.kr (C.-H. Han), stpark12@kisa.or.kr (S.-T. Park), s-lee@chonnam.ac.kr (S.-J. Lee).

https://doi.org/10.1016/j.ijcip.2019.100312
1874-5482/

IT system. Cyber-attacks are continuously changing to attack IT systems [6].

The remainder of this paper is organized as follow: Section 2 details the security operation activities, cyber threat information sharing and the crisis of the electric power grid. Section 3 introduces the origins of cyber threats and the cyber-attack possibilities according to the types of authentication. Section 4 details the time assumptions of incident response and propose Enhanced Security Control (ESC) model and Blocking Prioritization (BP) process to decide which IT system should be blocked from unnecessary foreign IP ranges. Section 5 concludes this paper.

2. Related work

2.1. Security operation & activities

The security operation of the cyber security operations center (CSOC) is the most important task for the cyber threats defense system of critical infrastructures. The basic purpose of the security operation is to monitor and respond to security events from mainly IPS, IDS, and Anti-DDoS. This is especially critical since a cyber infringement accident could generate an enormous impact on a nation [8].

The task of incident response starts when suspicious events trigger alerts is triaged and the incident is deemed worthy of being investigated further. Following an incident triage, the details of the incident are provided for further investigation, such as: traffic originating entity (source IP address of event or group of events), entity name (hostname, fully qualified domain name), traffic type (RDP, SSH, FTP, HTTP, HTTPS, TLS, SSL etc.), protocol (TCP/UDP) payload information, suspected attack payload / attack vector (provided by the log source that raised the alert, e.g., known signature or heuristics), target asset (IP address of the target endpoint), and occasionally the geoIP locational information (this is geographic information associated with the origin of the source IP address used in the attack. E.g. IP address originating from a country/city) [8].

2.2. Cyber threat information sharing

Information sharing is becoming essential in cyber defense. Recently issued regulatory directives such as those from the European Commission (2016) and from the White House (2013), and technical recommendations (e.g., ENISA, 2013a and NIST, 2014), clearly demand the establishment of technologies and procedures for cyber security information sharing with the purpose of revealing modern cyber-attacks and timely mitigating their effects. Sharing relevant incident information intelligence among SOCs enables a greater knowledge of the current cyber security situation of federated organizations' infrastructures and facilitates the detection of covert large-scale cyber-attacks and new malware. Analysis of shared incident information is crucial in attempting to recognize the presence of a threat within an organization's infrastructure that has already been detected in other cooperating organizations. Analysis is also essential in order to achieve scalability and efficiency in incident handling. In fact, in the proposed hierarchical approach, incident analysis performed at national and international levels allow SOC operators to have a quick overview on the current cyber security situation of all the monitored CIs on the national territory and to properly derive suitable countermeasures in case of threat. The presented work is carried out within the framework of the EU-FP7 research project ECOSSIAN. As depicted in Fig. 1, we foresee three types of SOCs: Organization SOC (O-SOC), National SOC (N-SOC), and European SOC (E-SOC) [9].

In order to support interoperability, ECOSSIAN makes use of widely adopted standards and protocols for cyber incident information representation and exchange. The diagrams in Figs. 2 and 3 illustrate the intended use of three separate data sharing and collection mechanisms respectively for information exchange between O-SOC and N-SOC, and between N-SOC and E-SOC.

- **IODEF** is used to *COLLECT* structured event-level incident data from the O-SOCs (N-SOCs). **RID** is adopted as transport protocol.
- **STIX** over **TAXII** is used to *SHARE* structured threat data with O-SOCs (N-SOCs).
- **JSON** delivered over **REST** is used for *ADHOC COMMUNICATIONS* between O-SOCs, N-SOCs and E-SOC [9].

2.3. The crisis of the electric power grid

Global Energy Interconnection between now and 2050 will connect all continents and the largest areas where the renewable and other energy sources are concentrated. The formation of GEI, however, will be a staged process [10]. In the first stage until 2030, it is necessary to provide a coordinated development of national and international electric power systems and force the adoption of environmentally clean energy sources worldwide. The generated electricity can be supplied to consumers through existing and evolving international electric power interconnections. In this case, the system benefits from the optimal use of various energy sources can be implemented to the maximum, thus enhancing the efficiency of electric power system operations and expansion. The key objectives of the second stage (2030–2040) will be the development of the largest areas with concentrated renewable energy sources in arctic and equatorial regions as well as the design of continental power interconnections. In this stage, the construction of main transmission lines between continents will be started. Another crucial objective will be to devise the principles for coordinating joint efforts and incentivizing the cooperation among countries to build the Global Energy Interconnection and control its operation. The third stage (2040–2050) suggests the completion of the GEI concept implementation through the establishment of a system for technological and commercial control, which can be based on different principles and structures [11,12]. This will allow a substantial rise in the international and intercontinental power exchanges, a reduction in power cost, and higher reliability of power supply. Fig. 4 depicts the structure of interstate power interconnections in northeast Asia in the future.

Modern power grid control systems are not isolated islands – disturbances in one system can cause instabilities or even blackouts in adjacent systems. Cyber-attacks on power grids could result in significant economic losses. Indeed, cyber weapons have already targeted power systems in Europe [14]. The integration of the pan-European electricity transmission system, which began in 2009, has greatly influenced the reliability of operations, optimal management and sustainable development, the goal being to ensure the security of electricity supply and to meet the needs of the growing energy market [15].

The existing electric power grid has been upgraded into a smart grid through intelligent communication infrastructures, layers of information, as well as extensive computing and sensing technologies. These cyber and physical components of the grid together constitute a complex cyber-physical system (CPS), and this integration increases the risk of cyber-attacks and introduces new vulnerabilities to the power system [16].

Smart grids are modernized electrical grids and are generally referred as the next generation's power system. For the purpose of sensing, monitoring, protecting and controlling, information and communication technology systems are being deployed in modern power systems. With this integration, smart grids are expected to greatly enhance efficiency, reliability and economy of power production and consumption along with the integration of renewable energy resources, as well as demand response and distributed

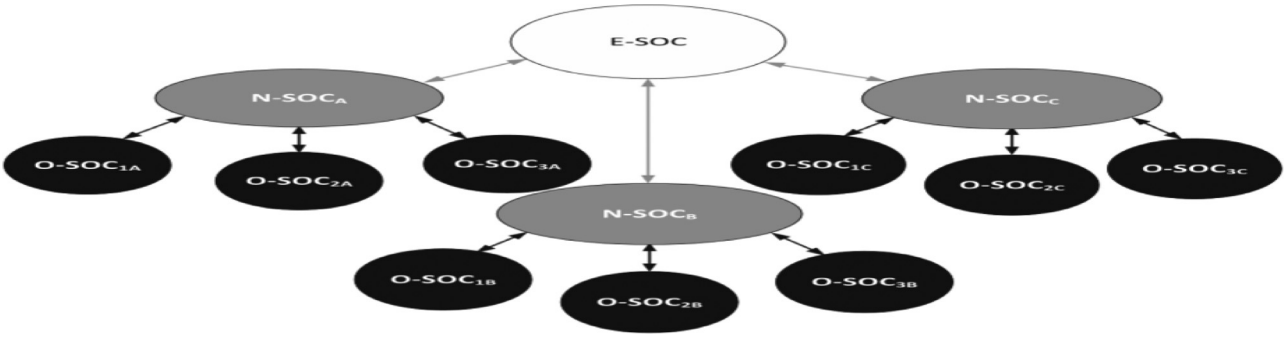

Fig. 1. Ecossian ecosystem for cyber threat intelligence of EU [9].

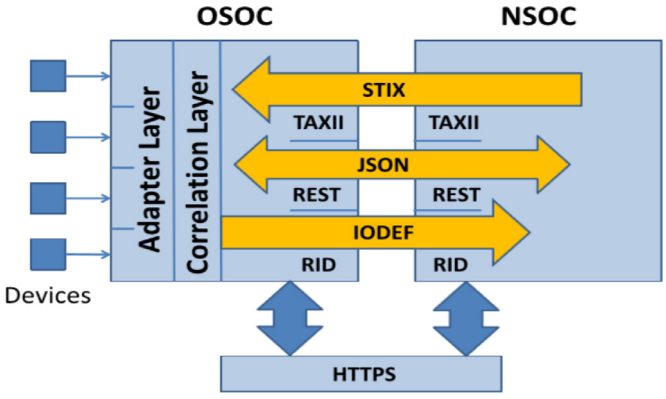

Fig. 2. O-SOC/N-SOC data exchange protocol stack [9].

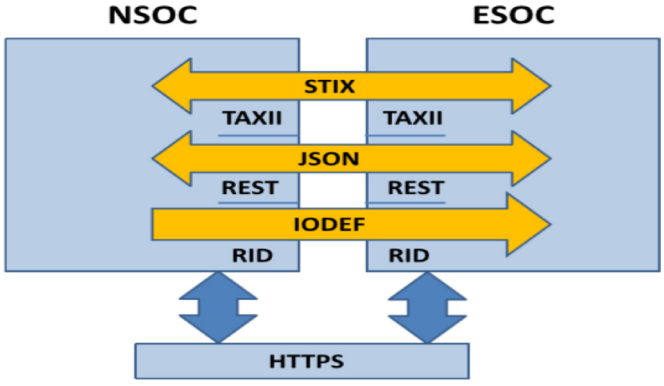

Fig. 3. N-SOC/E-SOC data exchange protocol stack [9].

intelligence [17]. Although the current smart grid initiatives are expanding the use of information technologies to modernize the existing grid, their adoptions in cyber physical systems (CPS) have introduced power system security issues [18,19]. Attacks on either cyber or the physical part of the smart grid will possibly impact the stability of the entire system. Recent research of cyber-attacks against smart grids have shown that these intentional attacks can have an impact on power system operation in terms of stability and economy. For example, authors in [20] commented that cyber-attacks in measurements of static var compensator (SVC) or static synchronous compensator (STATCOM) can degrade the system's stability margin. Cyber-attacks including false data injection attacks can mislead the state estimating process [21] or even can impact the economic operation of electric power market operations by manipulating the nodal price [22].Similarly, denial of service (DoS) attacks in the cyber layer of smart grids can affect the dynamic performance of physical power system [23]. It is also important to verify the device settings, algorithms and application before they are deployed in real power systems to avoid any unfortunate incident. For example, malfunctioning of relays can lead to false tripping of breakers /which can cause cascading failures. In this case, cyber-physical testbeds can serve as a tool for simulating the power system model accurately and also helps to understand the complex relation between cyber and physical domains. Although United States Department of Energy (DoE) is giving considerable attention to the security enhancements of cyber-physical power system, the research related to cyber-attack and impacts are constrained by the availability of realistic cyber physical system testbed. In many cases, cyber and/or physical attacks also result in the stability issues in smart grids and microgrids. There are several dynamic events happening in power system, e.g., a sudden change in load, fault in transmission lines or buses, and generator

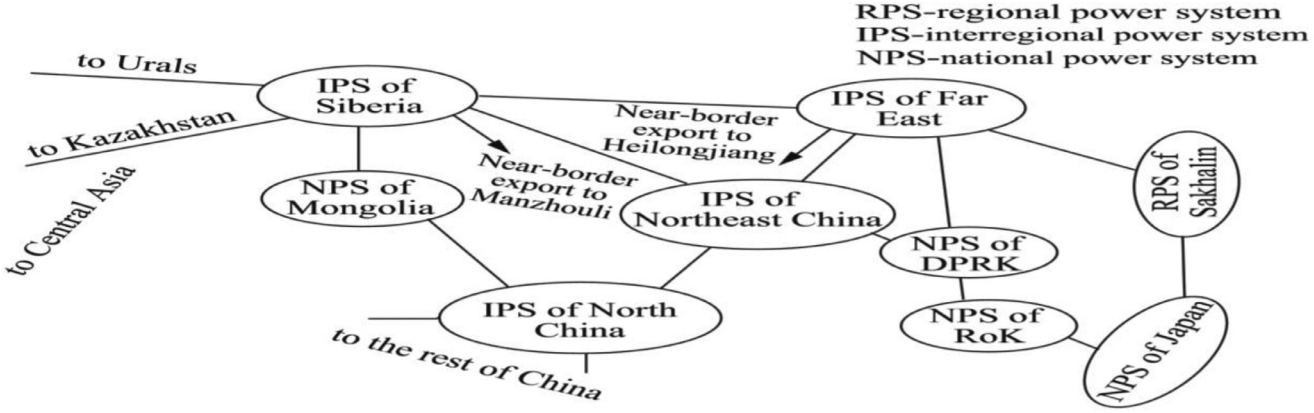

Fig. 4. Structure of interstate power interconnection in Northeast Asia in the future [13].

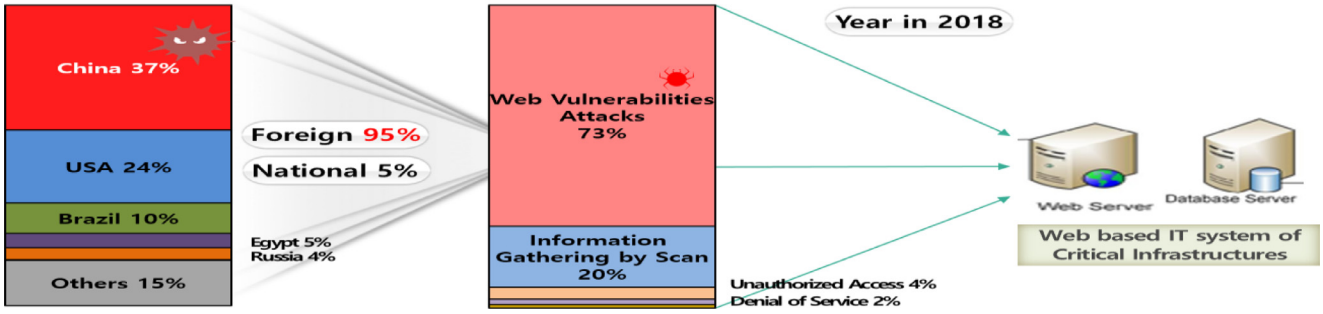

Fig. 5. Origins of cyber threats of a Korean electric power organization in 2018.

Table 1
Percentages of top 3, 10, 20 bad IP nations from 2015 to 2018 against a Korean electric power organization.

Category	2015	2016 (%)	2017 (%)	2018 (%)	Average (%)
Top 3 Nations	51.0	60.0	51.0	50.0	53.0
Top 10 Nations	75.8	79.7	72.7	69.9	74.5
Top 20 Nations	83.6	89.1	80.7	84.1	84.4

Table 3
Cyber-attack possibility per web authentication types.

Category	Non-authenticated members	Authenticated members
URL Authentication like 'url.com/admin'	O	O
ID/PWD Authentication	O	O

out of service. These events will impact the system's stability and can ultimately lead to loss of synchronism. Stability control is also an important piece in cyber-physical system [24]. Computational intelligence (CI) based supplementary adaptive control approaches for microgrid have been investigated in simulation platforms with the consideration of different faults [25–27].

3. Origins of cyber threats

We studied four years of bad IP data from the SOC in a Korean electric power organization which is designated as a Critical Infrastructure Protection (CIP) by a Korean Authority. We found that the types of cyber threats are continuously changing, which makes it difficult for us to develop automated security operation tools. However, there is one thing that did not change for four years. That was the origins of cyber threats. The origins of cyber threats were from foreign nations, especially China, the USA, Brazil, Egypt and Russia. About 95% of all cyber-attacks were from foreign nations; less than 5% were from internal attacks. Fig. 5 shows the origin analysis of cyber threats.

The top three nations' attacks accounted for more than 50% of all cyber-attacks each year, and the top twenty nations' attacks accounted for about 80% of all cyber-attacks. This can be explained by the Pareto principle (also known as the 80/20 rule. Roughly 80% of the effects come from 20% of the causes). Table 1 gives the percentages of bad IPs coming from foreign nations over four years.

Another analysis of cyber threats is about the bad IP total per retention IP total and the IP ranges total of each nation. Without considering the retention IPs and IP ranges of each nation, the top five bad IP nations were China, the USA, Brazil, Russia and Egypt. However, if we consider the retention IP and IP ranges of each nation, the top five bad IP nations shifted as shown in Table 2. We compared other nations with China because China led the world in cyber-attack statistics from 2015 to 2018. When we considered the IP ranges of each nation, the bad IP nation sequence was Egypt, China, Brazil, Russia and the USA. When we considered the retention IPs of each nation, the bad IP nation sequence became Egypt, China, Russia, Brazil and the USA.

In general, most critical infrastructures, like those within electric power organizations, have three types of IT systems. The first is the Industry Control System (ICT) for operating the critical infrastructures for each nation. The second is the semi-ICT which is connected to critical infrastructures for HTTP service to each nation, and the third is just general IT systems for ERP, mailing and reporting. From the point of security operations of an organization, the second and third types are vulnerable to cyber-attacks. Fig. 6 explains the general IT concept of most critical infrastructures.

There is one more important thing that we have to consider. The web authentication by ID/PWD & URL cannot defend against cyber-attacks from the world. Many people mistakenly believe that their IT systems are safe because they have been authenticated by ID/PWD or URL. SOC's daily reports about cyber-attacks tell us that authentication by ID/PWD or URL cannot prevent cyber-attacks. Table 3 explains the possible situation of cyber-attacks per authentication types.

The vulnerability that web authentication is not enough to prevent cyber-attackers from the semi-ICT can make the crisis of electric power grid. Since cyber-attackers can manipulate input data of semi-ICT, the power plants' operation can be malfunctioned with the manipulated input data. More global energy interconnection and smart grid, more crisis of electric power grid can be possible.

Table 2
Bad IP ratio per each nation's IPs total & IP ranges total against a Korean electric power organization in 2018.

category	USA	Brazil	Russia	China	Egypt
Total Retention IP Ranges (A)	53 632	9197	8890	8272	164
Total Retention IP (B)	1 604 256 984	8 763 386	45 496 570	30 349 322	22 823 096
Total Bad IPs in 2018 (C)	2584	1088	418	3948	401
Bad IP Ratio per retention IP ranges(C/A)	4.82%	11.83%	4.70%	47.73%	244.51%
Bad IP Ratio Magnification with China	0.10	0.25	0.10	1.00	5.12
Bad IP Ratio per retention IPs (C/B)	0.000161%	0.001284%	0.000919%	0.001160%	0.001757%
Bad IP Ratio Magnification with China	0.13	1.11	0.79	1.00	1.51

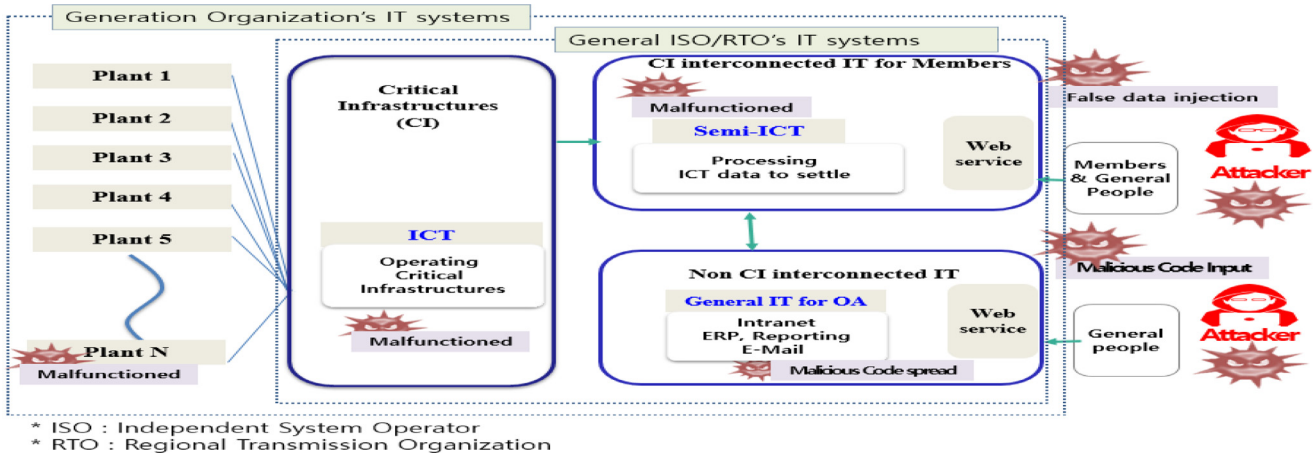

Fig. 6. General IT concept of critical infrastructures (ISO/RTOs, Generation Organizations).

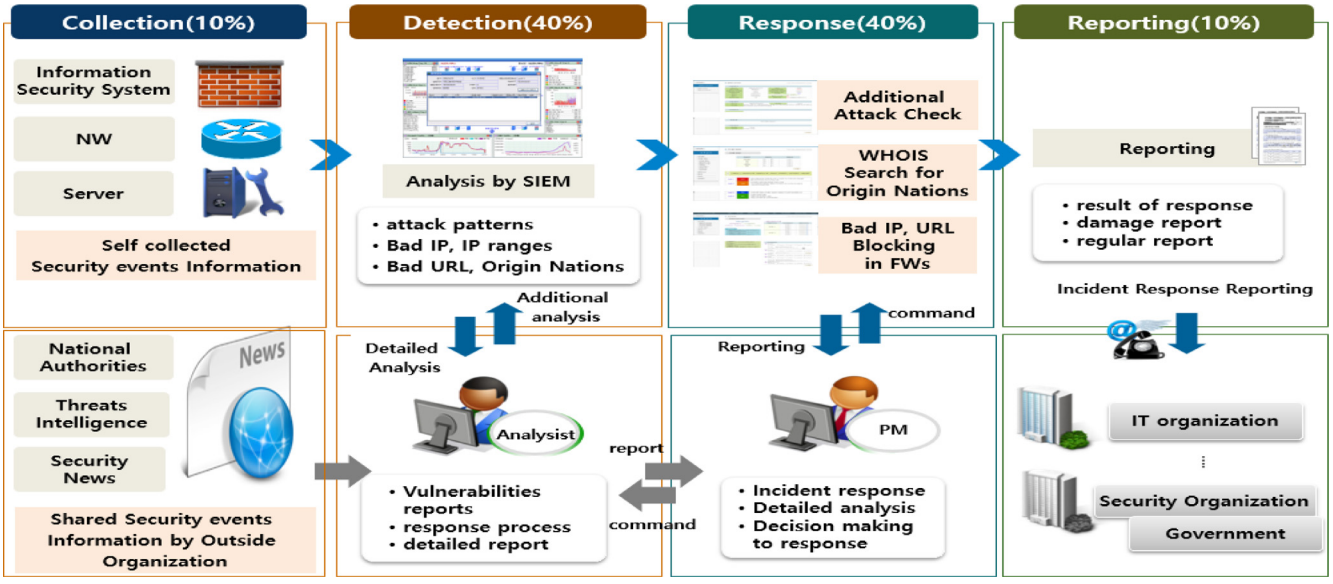

Fig. 7. Major four activities of the security operation center.

4. The ESC (Enhanced Security Control) model

4.1. Activities & time assumption of incident response

The activities of the CSOC can be split into four major categories – Collection, Detection, Response and Reporting. The major two activities are Detection and Response. Detection can be performed by operators who monitor the systems, networks, applications and services. ESM (Enterprise Security Management) based on SIEM helps operators to detect many incidents.

The percentages of the security operation activities of the CSOC are in Fig. 7 and have been obtained from the experience of security operation experts.

Unfortunately, it is too difficult for security analysts and operators to follow up on all security events. Some of the security events can be easily missed, and others can be overlooked. Furthermore, it takes too much time to respond to all suspicious security events. There are three activities in response to block bad IPs in a Korean electric power organization. The first step is to check whether there have been other additional cyber-attacks from the same bad IP. The second step is to find out the nations of origin and the IP ranges by searching WHOIS. The third step is to add the bad IP to the firewall and other security systems. We studied an SOC of a Korean electric power organization, and we surveyed 128 experts and 46 SOC operators from 19 different organizations to find out how much time they took to respond to each bad IP. The main activities and processing time of incident responses for each bad IP is shown in Table 4.

Responding to security events is a very time consuming job for people in the SOC. The total response time can be calculated by the summation of every detailed step per total bad IPs.

V1 = Additional attacks checking time, V2 = WHOIS IP Checking time, V3 = Bad IP enrollment time for each network gate firewall

RT = Responding time for M bad IPs = (V1 + V2+ V3) * M total counts of bad IPs

If there are N networks to connect with the Internet, additional time should be added in the calculation.

V1 = Additional attacks checking time, V2 = WHOIS IP Checking time, V3 = Bad IP enrollment time for network gate firewall

RT=Responding Time for M suspicious security event & N networks = (V1 + V2+ V3 * N) * M total counts of bad IPs

In a Korean electric power organization, the SOC blocked 132 bad IPs each day in 2018. In 132 bad IPs, 41 were self-detected by their own IPS, IDS, and Anti-DDoS. 91 were from the detected by

Table 4
Main activities and processing time of incident response for each bad IP in the SOC of a Korean electric power organization.

Category	Detailed steps	Minimum Time (s)	Average Time (s)	Maximum Time (s)
Self-analysis by security events collection from SOC's IPS, IDS	①Checking additional attack from same bad IP	60	152	300
	②WHOIS search to find out origin Nations and IP ranges	60	109	300
	③Deny bad IPs with FW & IPS	60	124	300
Outer-analysis by outer Cyber Threat Intelligence	① Deny bad IPs with FW & IPS	60	124	300

Table 5
Incident response time calculation for blocking bad IPs in the SOC of a Korean electric power organization.

Category	Minimum time	Average time	Maximum time
Responding time	5.77 h	12.06 h	28.83 h

cyber threat intelligence of other organizations. If there are two networks connected to the Internet, the total time for responding to 132 bad IPs can be calculated with Table 4 and the above formula. It is easily seen that incident response activities are very time consuming for SOCs. Table 5 illustrates the minimum time, average time and maximum time of blocking bad IPs.

If minimum time is considered, the responding time is

$$\begin{aligned} RT &= (60 + 60 + 60 * 2) * 41 + (0 + 0 + 60 * 2) * 91 \\ &= 9,840 + 10,920 = 20,760\text{sec} = 5.776\,\text{Hours} \end{aligned}$$

If average time is considered, the responding time is

$$\begin{aligned} RT &= (152 + 109 + 124 * 2) * 41 + (0 + 0 + 124 * 2) * 91 \\ &= 20,869 + 22,568 = 43,437\text{sec} = 12.06\,\text{Hours} \end{aligned}$$

If maximum time is considered, the responding time is

$$\begin{aligned} RT &= (300 + 300 + 300 * 2) * 41 + (0 + 0 + 300 * 2) * 91 \\ &= 49,200 + 54,600 = 103,800\text{sec} = 28.83\,\text{Hours} \end{aligned}$$

4.2. Enhanced Security Control

It is very important for security operations to reduce the time of responding to all suspicious security events since it can improve efficiency. There are many studies of automating response procedures to reduce security operation time, but it is too difficult for automated procedures to accomplish perfect cyber threat defense without human involvement like meetings, discussions, decisions, normalizing the cyber threat detection patterns and so on. Since there are 43 hundred million IPs in the world, cyber-attackers change bad IPs endlessly to make their cyber-attacks successful. The ESC model will help to make decisions about blocking foreign IP ranges for 95% of all cyber-attacks, therefore allowing organizations to concentrate on the 5% of national cyber-attacks.

We propose the ESC model and BP process with three steps and six factors to reduce response time to many security events. Many cyber-attacks come from foreign nations. In an electric power organization in Korea, the percentages of foreign cyber-attacks are more than 95%; less than 5% of cyber-attacks are internal. It is very important to think about the purpose of internet-connected IT web systems. If there is no need to permit foreign IP ranges, blocking them would be more effective for security purposes. There are three steps to enhance the efficiency of security operations. The first step is to identify which IT assets to protect from cyber-attacks. If IT assets have a public IP to service HTTP, they must be included in this asset identification. The second step is to decide Blocking Impact Degree (BID) to prioritize web IT assets to block from foreign IP ranges. The third step is to concentrate on non-blocked IT assets to make security operations more effective.

Since blocking foreign IP ranges is a very controversial process, the ESC model and BP process will guide to help in decision making with following six factors. The first factor is Foreign Relation (FR) of HTTP services. The level of foreign relations is the most important factor in deciding whether to block foreign IP ranges or not. The second factor is Real Login (RL) from foreign regular users. Even if the HTTP services are related to foreign business, if there is no real login for foreign regular users, blocking foreign IP ranges is needed to improve the cyber safety of those HTTP services. The third factor is Blocking Complexity (BC). If it would cause to much additional work, blocking foreign IP ranges is not recommendable for those HTTP services. The fourth factor is Stop Tolerance (ST). If stop tolerance time is short, it is necessary to block foreign IP ranges. The fifth factor is Outer Relation (OR). If HTTP services are connected to internal and external IT systems, it is also necessary to block foreign IP ranges. The sixth factor is Stop Impact (SI). If HTTP services' stop has national influence, it is recommendable to block foreign IP ranges. The operational definition of these six factors can be found in Table 6.

The detailed criteria to review the six factors is like below in Table 7. It is recommendable to block when FR, RL, BC and ST points are lower. However, it is recommendable to block when OR and SI is higher. It means four factors (FR, RL, BC and ST) have same direction and other two factors (OR and SI) have opposite direction. So, the ESC model put opposite score to OR and SI in criteria of the six factors. Opposite score to OR and SI make prioritization of Blocking Impact Degree (BID) possible.

The Blocking foreign IP ranges Impact Degree (BID) can be calculated by the summation of all six factors' evaluated points.

Table 6
Operational definition & criteria about six factors [28–31].

Factors	Definition	Criteria
Foreign Relation(FR)	Business relationship with foreign regular users	Purpose of HTTP service
Real Login(RL)	Frequency of real login	Real login counts for 6 month
Blocking Complexity(BC)	Additional consideration and efforts to unblock foreign IP ranges	Counts of exception handling
Stop Tolerance(SI)	Acceptable stop duration level of HTTP service	Acceptable stop time of HTTP service
Outer Relation(OR)	Outer connectivity level of HTTP service	Counts of outer IP systems connected with HTTP service
Stop Impact(SI)	Stop influence level of HTTP service	Size of stop influence

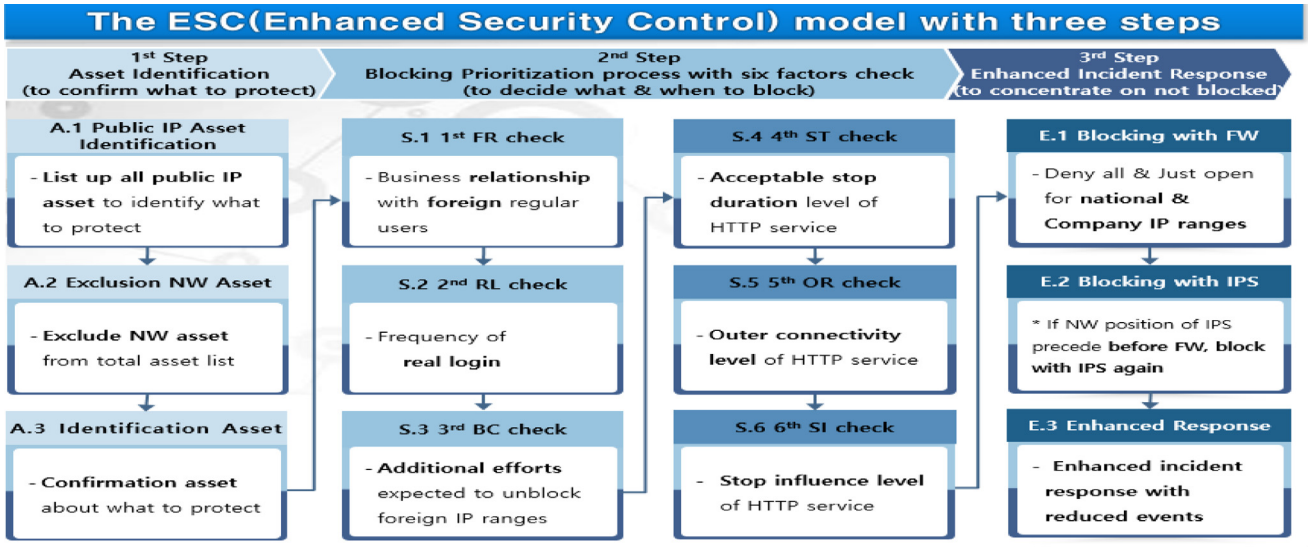

Fig. 8. The ESC model with BP process by considering six factors.

Table 7
Detailed criteria for the six factors.

Factors	Detailed criteria	Score
Foreign relation(FR)	Complete business purpose for foreign users	High(2)
	A certain degree business purpose for foreign users	Medium(1)
	No business purpose for foreign users	Low(0)
Real login(RL)	More than 5 times real login for 6 months	High(2)
	From 1 to 4 times real login for 6 months	Medium(1)
	No real login for 6 months	Low(0)
Blocking Complexity(BC)	A lot of additional efforts expected to unblock foreign IP ranges	High(2)
	Some additional efforts expected to unblock foreign IP ranges	Medium(1)
	Few additional efforts expected to unblock foreign IP ranges	Low(0)
Stop Tolerance(ST)	More than 1 day of acceptable stop time	High(2)
	From 4 h to 1 day of acceptable stop time	Medium(1)
	Less than 4 h of acceptable stop time	Low(0)
Outer Relation(OR)	Less than 1 outer connected IT systems	Low(2)
	From 2 to 4 outer connected 1 day IT systems	Medium(1)
	More than 5 outer connected IT systems	High(0)
Stop Impact(SI)	Small amount of stop influence level	Low(2)
	Medium amount of stop influence level	Medium(1)
	Large amount of stop influence level	High(0)

Lower BID systems are recommendable for blocking foreign IP ranges.

$$\begin{aligned}\text{BID (Blocking foreign IP ranges Impact Degree)} &= \text{FR (Foreign Relation)} + \text{RL (Real Login)} \\ &+ \text{BC (Blocking Complexity)} + \text{ST (Stop Tolerance)} \\ &+ \text{OR (Outer Relation)} + \text{SI (Stop Impact)}\end{aligned}$$

The BID ranges from 0 to 12. A lower BID means that it is recommendable to block foreign IP ranges. The Degree of Assurance (DOA) is dependent on the organization's management decisions. In this paper, we would like to propose 10 points as a DOA. From 0 to 9 BID, it is recommendable to block foreign IP ranges. From 10 to 12 BID, it would be better not to block these ranges because the benefit of blocking is less than the expected additional effort for blocking. The blocking prioritization of foreign IP ranges is depicted in Table 8.

To make security operations more efficient, the ESC model will guide to decide what to protect in the SOC and how to block with FW and IPS. The concept of the ESC model for security operation efficiency is shown in Fig. 8.

First of all, it is very important for the SOC to confirm what to protect in their daily operations. We defined this first step as Asset Identification. The criteria of asset identification is whether the IT system has a public IP address for HTTP service or not. If there is a public IP address, we should exclude NW assets in Asset Identification. The second step is to decide which IT systems to block foreign IP ranges if there is no foreign business needs for the IT system. We propose six factors to help in making decisions with the consideration about how much large blocking impact of

Table 8
Blocking prioritization for foreign IP ranges.

Category	Prioritization of blocking	Decision making about foreign IP ranges
0–3 point	1st Blocking	Recommendable to block foreign IP ranges
4–6 point	2nd Blocking	Recommendable to block foreign IP ranges
7–9 point	3rd Blocking	Recommendable to block foreign IP ranges
10–12 point	No Blocking(Enhanced Security Operation)	Not- recommendable to block foreign IP ranges (Benefit of blocking Foreign IP ranges is less than additional effort after blocking)

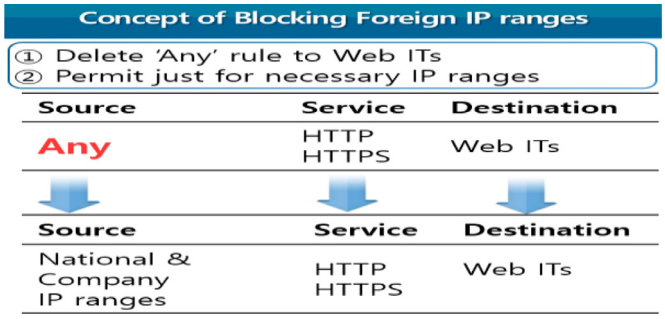

Fig. 9. Blocking concept.

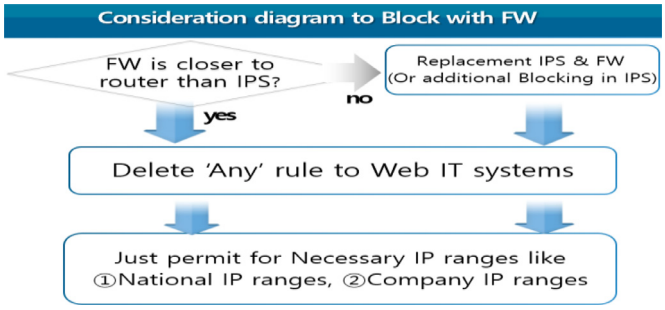

Fig. 10. Consideration diagram to block with FW.

Table 9
Example of asset identification of a critical infrastructure.

No	Asset	Public IP	No	Asset	Public IP
1	IT System 1	150.***.205	8	IT System 8	150.***.212
2	IT System 2	150.***.206	9	IT System 9	150.***.213
3	IT System 3	150.***.207	10	IT System 10	150.***.214
4	IT System 4	150.***.208	11	IT System 11	150.***.215
5	IT System 5	150.***.209	12	IT System 12	150.***.216
6	IT System 6	150.***.210	13	IT System 13	150.***.217
7	IT System 7	150.***.211	14	IT System 14	150.***.218

web IT systems. These six factors will help in reducing enormous amount of unnecessary security events in the SOC. The third step is the EIR (Enhanced Incident Response). We propose permitting only national IP ranges after denying all in FW. Also, if IPS is located before FW, IPS should be blocked together. But it is not easy work for us to apply this rule of denial to IPS like FW; we had better consider the replacement of IPS to behind FW, or new FW addition in front of IPS. Figs 9 and 10 explain the concept and process of blocking foreign IP ranges.

Table 11
Test results of the ESC model for a Korean electric power organization.

No	Category	Details
1	Start time of blocking	Dec 2018
2	Blocking equipment/Service	FW/HTTP, HTTS
3	Blocking target	Foreign IP ranges
4	Open target	①National IP ranges ②Company IP ranges
5	Blocking efficiency (Demonstrated)	①Reducing 2 bad IP blocking per day => It saved about 10~20 Mins ②Reducing 2000~5000 security events
6	Blocking efficiency (Expected blocking 60% IT systems)	①Reducing 30 bad IP blocking per day => It will save about 3~5 h ②Reducing 30,000~50,000 security events

Tables 9 and 10 explain the examples of asset identification and BID (Blocking abroad IP ranges) evaluation of IT systems in critical infrastructures.

People always ask us what they can do if cyber-attackers change their foreign IPs to a national IPs. The solution is very simple and clear. The ESC model will reduce the size of the gate to the web-based IT system and make our cyber threat defense system's effective range long enough to kill every cyber-attack from the outer world. In other words, the ESC model will make the web-based IT systems' gates much smaller, and because cyber-attackers will have to pass through these much smaller gates, the incident response teams will be able to concentrate the cyber threat defense systems to these smaller gates to respond to every security incident. The concept of this solution is depicted in Fig 11.

This ESC model should be considered to enhance incident response activities in SOCs. We propose that every critical infrastructure should apply the ESC model at least once a year to protect critical IT infrastructures and precious data. The reason we have to circulate the ESC model is to review the changes of IT systems, because IT systems are continuously changing and changing. A lot of developments for new IT systems are continuously changing IT systems situation. The circulation of the ESC model to enhance cyber safety of critical infrastructures depicted in Fig 12.

4.3. Efficiency of the ESC model

We applied this ESC model to security operations of a Korean electric power organization to reduce security events and to reduce incident responses. The final result of blocking foreign IP ranges is shown in Table 11.

If a SOC responds to 50 bad IPs a day and the ESC model decides that 60% of the IT system can be blocked from foreign IP

Table 10
Example of BID evaluation of identified assets.

Identified Assets	Public IP	1st FR Check	2nd RL Check	3rd BC Check	4th ST Check	5th OR Check	6th SI Check	BID	Decision
IT System 1	150.***.205	0	0	0	0	1	0	1	Blocking
IT System 2	150.***.206	0	0	0	0	1	1	2	Blocking
IT System 3	150.***.207	0	0	0	0	1	1	2	Blocking
IT System 4	150.***.208	1	1	1	1	1	1	6	Blocking
IT System 5	150.***.209	0	0	0	0	1	1	2	Blocking
IT System 6	150.***.210	2	1	1	2	1	1	8	Blocking
IT System 7	150.***.211	0	0	0	0	1	1	2	Blocking
IT System 8	150.***.212	0	0	0	1	1	1	3	Blocking
IT System 9	150.***.213	0	0	0	1	1	1	3	Blocking
IT System 10	150.***.214	0	0	0	1	1	1	3	Blocking
IT System 11	150.***.215	2	2	2	2	2	2	12	Enhanced
IT System 12	150.***.216	1	2	2	1	2	2	10	Enhanced
IT System 13	150.***.217	1	2	1	2	2	2	10	Enhanced
IT System 14	150.***.218	2	2	1	2	2	2	11	Enhanced

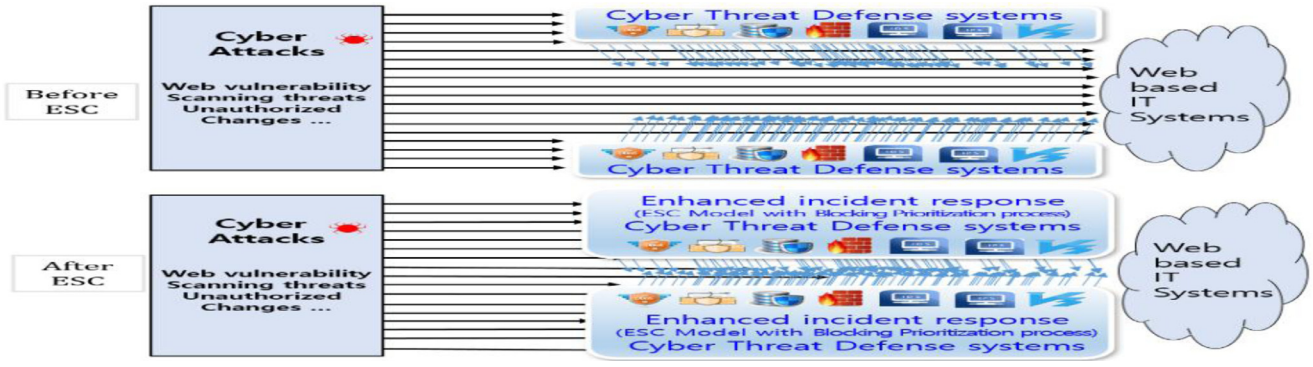

Fig. 11. How to enhance cyber safety with the ESC model.

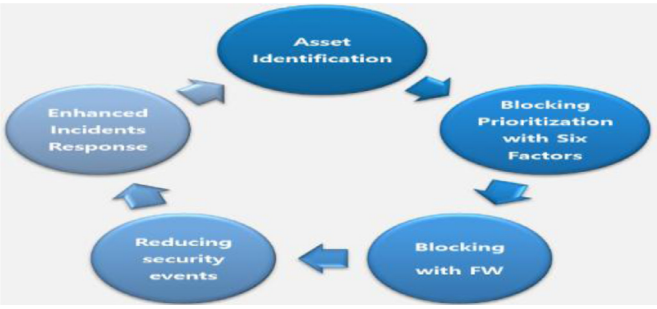

Fig. 12. Circulation of ESC model.

Table 12
Incident response time calculation for blocking 30 bad IPs.

Category	Minimum time	Average time	Maximum time
Responding time	2 h	4.24 h	10 h

ranges, 30 bad IPs could be reduced. If we consider the minimum time, average time and maximum time of Table 5, the amount of time saved could be from 2 to 10 h. Table 12 illustrates three cases.

V1 = Additional attacks checking time, V2 = WHOIS IP Checking time, V3 = Bad IP enrollment time for network gate firewall
RT = Responding Time for M suspicious security event & N networks = (V1 + V2 + V3 * N) * M total counts of Bad IPs

If minimum time is considered, responding time is

$$RT = (60 + 60 + 60 * 2) * 30 + (0 + 0 + 60 * 2) * 0 = 7200 + 0 = 7200\ \text{s} = 2\ \text{h}$$

If average time is considered, responding time is

$$RT = (152 + 109 + 124 * 2) * 30 + (0 + 0 + 124 * 2) * 0 = 15,270 + 0 = 15,270\ \text{s} = 4.24\ \text{h}$$

If maximum time is considered, responding time is

$$RT = (300 + 300 + 300 * 2) * 30 + (0 + 0 + 300 * 2) * 91 = 36,000 + 0 = 36,000\ \text{s} = 10\ \text{h}$$

5. Conclusion

In this thesis, we defined the ESC (Enhanced Security Control) model with BP (Blocking Prioritization) process to decide which IT systems should be blocked from unnecessary foreign IP ranges. This ESC model will improve the efficiency of incident response of critical infrastructures, because it will eliminate unnecessary security events of SOC. In the ESC model, there are BP process with six factors: FR (Foreign Relation), RL (Real Login), BC (Blocking Complexity), ST (Stop Tolerance), OR (Outer Relation) and SI (Stop Impact). By these six factors, we can decide BID (Blocking foreign IP ranges Impact Degree) to prioritize IT systems to block from foreign IP ranges. If BID is over the DOA (Degree of Assurance), we can decide not to block from foreign IP ranges. It means we can tell which IT systems should be concentrated with enhanced security operation. This ESC model is an effective approach to enhance cyber safety of critical infrastructures to help decision making in blocking prioritization. The ESC model can be used every SOC to improve security operation.

Declaration of Competing Interest

None.

References

[1] D.H. McCallam, P.D. Frazier, Architecting the next generation cyber security operation, Proceedings of the Seventh Annual IEEE International Conference on Ubiquitous Connectivity and Threats, 2017, pp. 1506–1509.
[2] Symantec, internet security threat report 2016, April 2016.
[3] B.S. Rivera, R.U. Inocencio, Doing more with less: A study of fileless infection attacks, VB 2015.
[4] Hauri, http://www.hauri.co.kr/support/hauriNews_view.html?intSeq=421&page=1, 2017.
[5] G. Parekh, D. DeLatte, G.L. Herman, Identifying core concepts of cybersecurity: Results of two Delphi processes, IEEE Transactions on Education 61 (1) (2018) 11–20.
[6] D. Stuttard, M. Pinto, The web application hacker's handbook: Finding and exploiting security flaws, 2014
[7] S. Lim, APT present condition and malignant code countermeasures, Journal of the Korea Institute of Information Security & Cryptology 24 (2) (2014) 63–70.
[8] C. Onwobiko, Cyber security operation centre: Security monitoring for protecting business and supporting cyber defense strategy, Intelligence & Security Assurance, E-Security Group, London, UK, 2018.
[9] G. Settanni, F. Skopik, Y. Shovgenya, R. Fiedler, M. Carolan, A collaborative cyber incident management system for European interconnected critical infrastructures, Journal of Information Security and Applications 34 (2017) 166–182.
[10] Z. Liu, Global Energy Interconnection, Elsevier Academic Press, 2015, p. 396.
[11] Haeger U., Rehtanz Ch, Voropai N. (eds) (2014) Monitoring, Control and Protection of Interconnected Power Systems. Springer, New York, 391 p
[12] M.L. Korolev, V.A. Makeechev, O.A. Sukhanov, et al., Modeling-based optimization of electric power system operation, Elektrichestvo (Electricity) (3) (2006) 22–31 (in Russian).
[13] N. Voropai, S. Podkovalnikov, K. Osintsev, From interconnections of local electric power systems to global energy interconnection, Global Energy Interconnection Development and Cooperation Organization 1 (1) (2018), doi:10.1417/j.2096-5117.gei.2018.01.001.
[14] J. Jarmakiewicz, K. Parobczak, K. Maslanka, Cybersecurity protection for power grid control infrastructures, International Journal of Critical Infrastructure Protection 8 (2017) 20–33.
[15] European Network of Transmission System Operators for Electricity, ENTSO-E work Programme, 2015 through December 2016, Brussels, Belgium (www.entsoe.eu/Documents/Publications/ENTSO-E%20general%20publications/151218_AWP2016_Final_post_ACER_opinion.pdf), 2016.
[16] S. Poudel, Z. Ni, N. Malla, Real-time cyber physical system testbed for power system security and control, International Journal of Electrical Power and Energy Systems 90 (2017) 124–133.

[17] W. Wang, Z. Lu, Cyber security in the smart grid: Survey and challenges, Computer Networks 57 (5) (2013) 1344–1371.
[18] S. Poudel, Z. Ni, T.M. Hansen, R. Tonkoski, Cascading failures and transient stability experiment analysis in power grid security, in: Proceedings of the 2016 IEEE Power Energy Society Innovative Smart Grid Technologies Conference (ISGT), 2016, pp. 1–5, doi:10.1109/ISGT.2016.7781166.
[19] S. Poudel, Z. Ni, X. Zhong, H. He, Comparative studies of power grid security with network connectivity and power flow information using unsupervised learning, in: Proceedings of the 2016 International Joint Conference on Neural Networks (IJCNN), IEEE, 2016, pp. 2730–2737.
[20] B. Chen, K.L. Butler-Purry, D. Kundur, Impact analysis of transient stability due to cyber attack on facts devices, in: Proceedings of the 2013 North American Power Symposium, 2013.
[21] Y. Liu, P. Ning, M.K. Reiter, False data injection attacks against state estimation in electric power grids, ACM Transactions on Intelligent Systems and Technology (TISSEC) 14 (1) (2011) 13.
[22] L. Xie, Y. Mo, B. Sinopoli, Integrity data attacks in power market, operations, Transactions on Smart Grid 2 (4) (2011) 659–666.
[23] S. Liu, X.P. Liu, A. El Saddik, Denial-of-service (DOS) attacks on load frequency control in smart grids, in: Proceedings of the 2013 IEEE PES Innovative Smart Grid Technologies (ISGT), IEEE, 2013, pp. 1–6.
[24] P. Kundur, M. Klein, G. Rogers, M.S. Zywno, Application of power system stabilizers for enhancement of overall system stability, IEEE Transactions Power Systems 4 (2) (1989) 614–626.
[25] Y. Tang, H. He, J. Wen, J. Liu, Power system stability control for a wind farm-based on adaptive dynamic programming, IEEE Transactions on Smart Grid 6 (1) (2015) 166–177.
[26] D. Molina, G.K. Venayaga moorthy, J. Liang, R.G. Harley, Intelligent local area signals based damping of power system oscillations using virtual generators and approximate dynamic programming, IEEE Transactions on Smart Grid 4 (1) (2013) 498–508.
[27] Fu X., Li S., Fairbank M., Wunsch D.C., Alonso E. Training recurrent neural networks with the Levenberg–Marquardt algorithm for optimal control of a grid-connected converter. IEEE Trans Neural Netw Learn Syst.
[28] S.-T. Park, W.S. Yi, B.-n. Noh, The detailed evaluation criteria for designation of critical information infrastructure in the field of broadcasting and communication, WSEAS Transactions on Information Science & Applications 7 (2) (2010) 252–262.
[29] S.-T. Park, B.-n. Noh, in: A Study on the Improvement of Method for Critical Information Infrastructure Designation, Chonnam National University of Korea, 2010.
[30] J.-S. Kim, S.-J. Lee, The improvement of the SLA evaluation indicator in public hardware maintenance, Journal of Information Technology and Architecture 13 (2) (2016) 341–353.
[31] R.A. Miller, There's infrastructure and … critical infrastructure, International Journal of Critical Infrastructure Protection 2 (1–2) (2009) 3–4.