Success Factors for Cyber Security Operation Center (SOC) Establishment

M. Abd Majid[1], K. A. Zainol Ariffi[2]

{maziana@mampu.gov.my [1], k.akram@ukm.edu.my[2] }

Prime Minister Department, MAMPU,Malaysia[1],
Faculty of Information Science & Technology, Universiti Kebangsaan Malaysia, Malaysia[2]

Abstract . The boundless in the digital world is one of the terms used to describe the present state where everything depends mostly on the use of technology. The increased dependency on these technology services has indirectly increased the risk of threats and cyber-attacks. One of the popular solutions to defend against these threats is by implementing the Cyber Security Operation Center (SOC) to monitor, track and handle the cyber incidents. However, there are a number of factors that affect the success of the SOC. Therefore, this paper aims to highlight the importance of the human, process and technology factors towards the establishment of SOC. A comparison of the previous establishment of SOC from the literature is made. The inputs from the literature come from the journal, proceeding, report starting from the year 2011 until 2018. From the result of the comparison, it presents the requirement of human, process, and technology to make sure the SOC work efficiently to defend against the cyber-attack.

Keywords : *Cyber security, operation, SOC, Information security strategy, Prevention, Defence in depth*

1 Introduction

The world transformation towards the fourth industrial revolution can be seen from our daily routine which has depend mainly on the use of technology. The technology has given many benefits to us, and it can assist us in our way to manage our lives efficiently. However, with increased dependence on technology, it also has indirectly increased the risk of threats and cyber-attacks. The cyber-attacks are not new to our world; it has begun as early as the 1960s where the hacking activity happened on the frequency of telephone systems [1]. Since then, its concept has become increasingly popular and evolving as technology progresses.

Previously, in the 1970s to 1990s, the recorder cyber-attacks were aimed at honouring the technical skills, seek recognition, and to show courage. During these times, the attackers were called “Kiddies Scripts” or unprofessional cyber attackers. At this point, this malware is not destructive or damaging to the property of the victim. It's more to prove the skills that hackers have and to gain recognition. However, as the world moves forward the purpose of the cyber-attacks also evolved into different dimensions where the hackers create malicious software to steal sensitive information, interrupt operation and obtain unauthorized access to systems [2].

By the late 2000s, the emergence of various online trading activities changed the hacker's perspective by targeting a large-scale financial profit by implementing more organized

INCITEST 2019, July 18, Bandung, Indonesia

DOI 10.4108/eai.18-7-2019.2287841

cybercrime [3]. This statement is supported by [4] stating that the exploration of malicious activities is increasingly sophisticated, with specific targets and increasingly severe. It also noted that the main aim of the cyber-attacks are businesses, governments, and particular individuals are the existence and dissemination of malware [5]. For example, the malware that is known as ILOVEYOU have exploited weaknesses in the WINDOWS system at that time.

Multilevel It was spread through e-mails using the Love Letter subject and resulted in a loss of $ 9 billion within a month worldwide. Subsequently, in 2003, the Slammer spreads through memory processes and infects computers connected within the network. This malware disturbed the network traffic as it eventually caused the network packets to drop and cripple the computer systems in the infected organization. The estimation of losses by Slammer was about USB 1 Billion within five (5) days.

Due to the evolution, and increasingly widespread, the organizations must implement defence mechanisms to protect themselves. One of the relevant mechanisms is developing a Cyber Security Operation Center (SOC) to monitor and prevent any attacks from damaging the organization. This statement is supported by [6], [7], and [8] by highlighting that the cyber-attacks are a widespread problem and need to be contained through an organizational monitoring by the SOC.

The success of the SOC establishment relies heavily on the number of factors such as management, monetary support, strategy, human, process, technology, environment, physical space, and continuous improvement. This paper aims to identify the most crucial factors to ensure the success of SOC from the previous literature and highlight the critical element for each of them. It will present a comparison of the prior establishment of SOC from the previous research and suggest the requirement of the crucial factors to make sure the SOC work efficiently to defend against the cyber-attacks.

This paper is divided into six (6) sections. Section 2 will present the recently well-known cyber-attacks and identify the weakness that allowed these attacks to happen. In section 3, the cybersecurity implementations to defend against the attacks are explained. A comparison between two established SOCs will be highlighted in section 4. The discussion about the crucial elements in SOC will be presented in section 5. Finally, section 6 is the conclusion of the paper.

2 Purpose of Cyber Attacks

The time has proven that the malware is used in various cyber-attacks to gain the highest goal in creating damage and loss. It also contributes to the difficulty for the organizations to handle the cyber-attacks as the malware become more complex and complicated to analyze [9]. The study by [10] has found that millions of new types of malware have been implemented in the attacks and this number keeps increasing over the year. The comparison between three (3) mainly cyber-attacks which have received worldwide coverage will be discussed in Table 1; the attack on Ukrainian regional electricity distribution companies, the Bangladesh National Bank robbery and the WannaCry Ransomware (Table 1).

Table 1. Cyber Security Case Study.

Source	Description	Date impact	Attack Modus Operandi
Bock et al. [15]; FireEye [16]; Lee et al. [10]	Attack on Three (3) Regional Electric Distribution Companies of Ukraine	December 2015 Affecting electricity supply to nearly 225,000 users.	-Insider attacks -Specific phishing method -Spy on operation - Use BlackEnergy3 for malicious activity
Kaspersky Lab [17]; Yeoman & Findlay [18}	Bangladesh National Bank Robbery Case	February 2016 National Bank Bangladesh suffered a loss of $ 81 million.	-Run an unauthorized transaction -Delete log trail and activities system functions -Using the legal credentials owned by Bangladesh National Bank -Manipulate the time differences between New York and Bangladesh -Using malicious software from Lazarus hacker group.
Askarifar et al. [19]	WannaCry *Ransomware*	May 2017 Affecting organizations in more than 150 countries that resulted in losses of almost $1 billion within a week	-Demand ransom money from victims by encrypting the files, and disks on the computer. -Use hybrid cryptographic techniques -The malware is known as WannaCry

Based on the description of Table 1, there is a similarity in each of the cases where the hackers are targeting specifically to a particular organization. Further, these attacks have a malicious motive by taking advantage to interrupt the service which in return give a negative impact on the organization. Besides, it also shows clearly a weakness in human, processes and technology aspects within the organization being attacked. In term of the human aspect, the level of cybersecurity awareness among the employees is low may contribute to the attacks. With the possibility of no rotation and filtration on the scope of work can also be one of the reasons for insider attacks. In the aspect of the process, it can be stated that the organization is lack of internal process and procedures to handle the cyber-attacks. Nevertheless, the lacking in defence mechanism and infrastructure such as monitoring unit also provide an upper hand to the attackers to launch the attacks.

Throughout the description in Table 1, it has shown that attackers have implemented a proper and planned preparation before executing an attack. The attackers identify the weaknesses in the organization such as human error and exploit them to gain access and run malicious activities on the systems. The modus operandi has proven the consistency and efficiency of the attackers in designing and implementing high impact cyber-attacks which are in line with the technological development (i.e., include encryption, hybrid mechanisms and other). Therefore, the organizations should also be prepared to defend themselves from any attempted advanced cyber-attack.

The advancement of a cyber-attack has become global issues and need to be solved effectively. To date, the goals and motives of cyber-attacks are also changing and focusing on a variety of matters such as political, revenge, monetary and destruction towards specific targets [11], [12]. The study by [13] states that no matter what the purpose of the cyber-attack is, it will compromise the confidentiality, integrity, and availability of the victim's information. At the same time, the victims receive the possibility of loss information, interruption of business or service, revenue loss and damage to their operation.

3 Defence Mechanisms for Cyber Security

The defence mechanisms for cybersecurity are divided into two (2) groups, which are placed as external and within the organization [13]. A country is responsible for addressing the issues of cyber-attacks at the national level. For an example, the offense committed by the attackers will be placed under the specific law is such as a way to deal with and curb the widespread cyber-attacks such have been focused in (Mohamed 2013; Muniandy et al., 2012).

The study by [14] has presented a survey on ten (10) organizations that focus on implementing the protection of information security infrastructure. Accordingly, it highlights the need of the organization to take steps to prevent cyber-attacks through the technology and non-technology approaches. In the technology approach, the use of access controls, intrusion detection, and software controls will be implemented. Whereas in the non-technology approach, the Non-Disclosure Agreement will be applied to protect any lost on sensitive information. The study also reveals that some organization believes in cybersecurity detection as an effective operational-level strategy to identify the attacks. Once the attacks have been identified, the implementation of the response team and corrective actions need to take place to handle the incident. In addition to that, the organizations also agree that disciplinary action can influence the human to behave better and reduce the error that may give an advantage to the attackers.

According to, organizations need to strengthen the security infrastructure to ensure that the organization is well-established and robust to counter cyber-attacks. The organization can implement a continuous risk assessment as a countermeasure to the cyber-attacks; perform scheduled maintenance on a scheduled basis; create policies and procedures to protect information security. Together with the risk assessment, the organization must also apply mainly three (3) security stages namely Prevention, Detection and Correction Control to improve the cybersecurity.

4 Cyber Security Operation Center (SOC)

The Cyber Security Operation Center (SOC) is one of the popular solutions to monitor, track, handle cyber incidents. With the increase in cyber-attacks, the establishment of SOC as organizational monitoring to contain these widespread problems is relevant and a must. [20], [21], [22], [23].

SOC is defined as a centrally-developed facility that dedicates to assist the organization in identifying, managing, monitoring security events and restoring the cyber incidents (Jacobs et al., 2013). It is also aiming to protect the confidentiality, integrity, and availability of information throughout continuous monitoring [24]. The study by has further elaborated the definition of SOC by stating that it is a cyber-security monitoring center that covers all three aspects of human, process, and technology. Thus, by this definition, it means that the technical personals are responsible for monitoring the systems and infrastructure within the organization, according to proven processes and procedures with a set of advanced technology. The monitoring task is intended to prevent the computer abuse and policy violations; to prevent and detect cyber-attacks, misuse, and leakage of data; and to respond to the incidents. According to [23], the SOC must work with a skilled workforce, predefined working process and the use of integrated intelligence technology to assist and manage the incident. It must include the incident management, digital forensic and reporting elements to ensure the success of the SOC. Table 2 highlights the comparison between two proposed frameworks of SOCs by [21] and [23].

Based on the both proposed frameworks, there is a similar function of the SOC. Both studies state the scope of monitoring, analysis, and reactions to be implemented to address threats and cyber-attacks. Although both studies use different terms, the essence of the three scopes is to refer to the same activities. Thus, this implies that the range of monitoring, analysis, and response can be categorized as the necessary scope that must exist for a sustainable SOC. In term of threat intelligence, the study by [21] does not mention the threat intelligence in the analysis function.

In contrast, [23] clearly state the threat intelligence as one of the functions of the SOC. In addition to that, the framework in [23] makes essential cyber security functions such as vulnerability scans and penetration testing functions as part of the SOC. This function is not specified in the study by [21] because generally this function can be implemented by the organization's ITC or any qualified third party. The survey by [23] believes that every SOC has different implementation and design and depends on the method of administration of their respective organizations. This view is supported by [25] which claims that organizational goals to achieve a better cyber security vision depend on the financial, human, process and infrastructure provisions set by the organization and how the cyber security program is managed and optimized over the long term.

Table 2. Framework of Cyber Security Operation Center.

Description	**Schinagl et al. [23]**	**Onwubiko [21]**
Environment	Amsterdam,Netherland	London, United Kingdom
Approach and Research Methodology	-Conduct a collaboration with VU University in Amsterdam Use the Research Methods for Case Studies and Design by Robert K. Yin.	Using HMG Good Practice Guide (GPG13) – Protective Monitoring for HMG ICT Systems as the basis of the study.
Validation	Endorsed by the stakeholders in SOC that involved with the study and Netherlands Cyber Security Community	Endorsed by representative of SOC in London.
Component of SOC	-Governance -Infrastructure for Information Technology and Communication -Operation Center (ITC)	-Infrastructure for Information Technology and Communication (ITC -Operation Center
Function of SOC	-Monitor -Threat of Intelligence -Forensic -Basic Cyber Security -Penetration Test	-Collection -Analysis -Response and Forensic

Although both above-discussed frameworks of SOC can be used as an organizational reference, the function and roles of SOC must always keep up with the current development in cybersecurity to stay relevant. As the technology develops and sophisticated cyber-attacks today, so is the Cyber Security Operation Center. Based on a report by Gartner, the current era requires SOC intelligence (Rochford & MacDonald 2015). These statements and requirements are in line with the growing threats and cyber incidents that are increasingly sophisticated in terms of attack techniques used. The existing SOC needs to use threat technology and threat intelligence to meet the growing threat of "detection and response" paradigm. This statement is also supported by a study [26], [27] which agrees that existing SOC has the limitations in detecting today's increasingly sophisticated cyber threats and attacks. Thus, the SOC must include the element of monitoring with prediction and proactive approach to strengthening Defence-in-Depth's strategy in the organization.

The use of intelligence technology in the SOC is beyond event-based prevention and monitoring technology. A study by [28] agrees that the existing SOC is currently conducting monitoring is based on the set of rules. Monitoring dependency through preventive and tracking-through technology requires prior knowledge of attack is unable to protect the organization from anomalous attacks. It only works to detect the threats and cyber-attacks that have ever been encountered.

Generally, there are four (4) aspects of security architectural framework that is suggested by Gartner [28]. It includes the element predict, prevent, detect and respond as shown in Figure 1. The core of this framework is the ongoing analysis and monitoring that the organization needs to take. It can work well by integrating the human, process, and technology into a smart SOC.

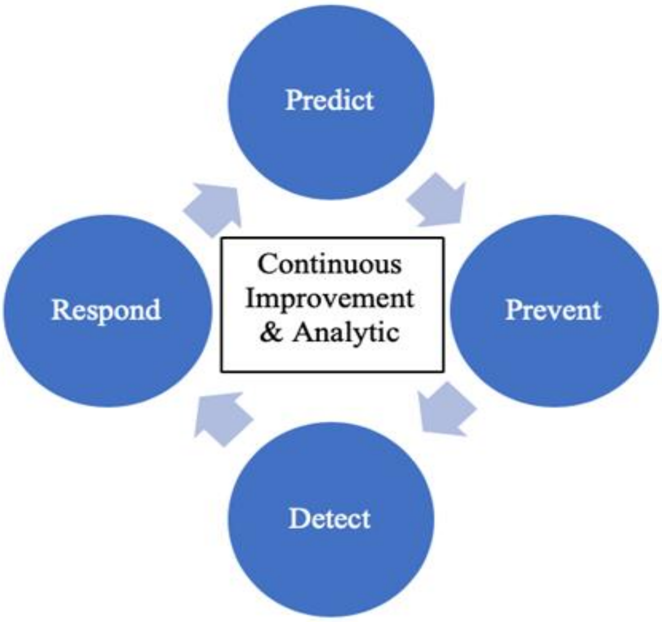

Fig 1. Security Architectural Framework by Gartner.

The detect and respond aspect is the main component in the basic functional of the existing SOC as outlined in Table 2. The additional aspect such as prevent is one of the security mechanisms for the organization to protect against any threats and cyber-attacks. The predict aspect is where the threat intelligence integrated with the SOC. Thus, with this finding, it shows that the smart SOC must adopt the threat intelligence technology to stay relevant and to maximize protection on organization. However, the success of threat intelligence technology depends on the knowledge and skills of the SOC personnel.

The requirements of the Threat Intelligence function are in line with the knowledge and skills required by Cyber Security Operation Center personnel [6], [7], [8], [20], [21], [22], [23]. The personnel must acquire with required skill and knowledge as it can help them to understand the scenario happens in the incident and react accordingly. Besides, the setup of the smart SOC also dependent on the financial capabilities as the most advanced technology will be at higher cost [7]. Therefore, the organizations must balance up between the security need with the cost that they need to incur. Due to this scenario, Gartner estimates that only 40% of the smart SOC can be established by year 2020 [28].

5 Success factor for SOC Establishment

Although the organization independently conduct the SOC in its way, the past studies can be acted as the guidance to ensure its implementation is in the right direction and effective. The success factor of the SOC to be described in this section is based on the ten (10) previous studies as listed in Table 3.

Table 3. Success Indicators of SOC Establishment.

Previous Study	Top Management Support	Monetary	Strategy	Human	Processes	Technology	Environment	Analysis/Reporting	Physical Space	Continuous Improvement
IBM Global Technology Services (2013)				√	√	√				
Ernst & Young (2014)	√	√	√	√	√	√	√	√	√	√
RSA Technical Brief (2014)				√	√	√				
Torress (2015)				√	√	√				
Schinagl et al. (2015)	√	√		√	√	√				
Onwubiko (2015)			√	√	√	√				√
Mansfield-Devine (2016)		√		√	√	√		√		
McAfee & Intel Security (2016)			√	√	√	√				√
Sundaramurthy et al. (2017)				√	√	√				√
MDEC (2017)	√	√	√	√	√	√	√	√	√	√

From table 3, it shows that all ten (10) previous research agree with the importance of human, process and technology indicators as the element in a success SOC. There are increasing in the success indicators from three (3) indicators in 2013 to ten (10) signs in 2014. It also emphasizes the importance of ten (10) indicators in 2017 as well. Despite changes to the success indicators, humans, processes, and technologies are still crucial for the successful implementation of the SOC. Based on previous studies, it is found that these three indicators are interconnected and require each other to enable the SOC to function effectively and productively. The coordination between people, processes, and technologies is essential to form harmony among human skills, systematic procedures, and technologies used to produce robust cyber defence to safeguard organizational assets. At the same time, five (5) out of ten (10) studies also agree that continuous improvement is an essential indicator of the success of a SOC. This indicator implies that the SOC needs to be continually changing as technology develops and the evolution of sophisticated cyber-attacks. This indicator is in line with the development of the SOC discussed in the preceding section. Here's a brief overview of every succession indicator of Cyber Security Operating Center:

A. *Top Management Support*

This indicator is needed to establish a clear direction and long-term strategy for SOC. Besides, it will also contribute to the drive of cybersecurity culture in organization.

B. *Monetary*

Financial allocation is significant in developing a SOC due to the use of the latest technology to ensure it is always relevant to current cyber challenges.

C. *Strategy*

The SOC must have clear vision, mission and objectives in the context of addressing existing risks, supporting core functions and meeting organizational compliance obligations.

D. *Human*

The SOC requires skilled and knowledgeable employee. Employees also need to have various capabilities and experience to ensure that each incident received can be effectively addressed. In addition the deep understanding of information technology (IT) environment and infrastructure is also crucial as to support the core functions of the organization.

E. *Processes*

SOC must clearly define processes to enable consistent operation and repeatable results. All documentation and communications must be recorded effectively.

F. *Technology*

Implementation of SOC should be equipped with technology appropriate to the organization's security posture. However, a technology plan is encouraged to consider the existing technology in the organization first as to reduce the cost effectively. Increased equipment and additional technology can be made in line with current requirements. For obtaining maximum returns from technology investments, organizations must to implement strategic initiatives to cater for the use of technology by establishing governance, systematic processes, training and promoting cyber security awareness in the organization.

G. *Environment*

Among the goals of the SOC is to protect the organization from any cyber-attacks. As such, SOC employee should be knowledgeable about organizational priorities to ensure that the reactions are the most appropriate and appropriate.

H. *Analysis and Reporting*

SOC must to be able to perform data analysis on various systems and tools to produce comprehensive reports.

I. *Physical Space*

SOC should be located in a safe and well-equipped area. Establishing a specific location can shorten the response time to an incident and also promote sharing of knowledge and teamwork. While physical space is said to be one of the success factors, the study by Mansfield-Devine (2016) says that the SOC can be implemented virtually.

J. *Continuous Improvement*

In line with current technological developments, the SOC should always be improved. It should provide ongoing training so that the employee's skills and knowledge can grow in tandem with the ever-changing cyber threats landscape. At the same time, the process should also be constantly updated and improved. It also requires for constantly evaluation of the technological capabilities to stay relevant and effective in protecting the organization from cyber-attacks from inside or outside.

6 Conclusion

The impact of cyber-attacks on organizations is far more pronounced, especially if it involves financial losses or affecting the reputation of the organization. Cyber-attacks cannot be eliminated as the advancement of emerging technologies is in tandem with the progress of cyber-attack techniques. Thus, the implementation of SOC is seen as a solution to protecting organizations from cyber-attacks. Even so, the general knows that cyber-attacks are a global issue and the way to handle them is through the cooperation of countries across the continent. As such, the implementation and establishment of the SOC to monitor and manage cyber-attacks, particularly by one national, is relevant. In this regard, the framework of a SOC can be implemented according to the mission, objectives, financial factors and other factors that affect the organization. While it can be developed based on organizational needs, the SOC should implement the necessary scope such as monitoring, analysis, and response. Nevertheless, the indicators such as human, processes, and technology are interconnecting to each other to enable the SOC to function effectively.

Acknowledgements

The authors would like to thank the Faculty of Information Science and Technology for supporting this work. We also would like to thank Universiti Kebangsaan Malaysia (UKM) for supporting this work under grant GGPM-2017-026.

References

[1] Halim, M. A, Abdullah, and A., Ariffin, K. A. Z.: Recurrent Neural Network for Malware Detection, Int. J. Advance Soft Compu. Appl. Vol. 11(1), pp 46-63 (2019)

[2] Ariffin, K. A. Z., Mokhtar, R. M., and Rahman, A. H. A.: Peerformance Analysis on LEACH Protocol in Wireless Sensor Network (WSN) under Black Hole Attack, Advanced Science Letters, Vol. 24(3), pp. 1791-1794 (2018)

[3] Baumard, P.: Cybersecurity in France, Springer, pp.17-31 (2017)

[4] Choo, K. K. R.: The cyber threat landscape: Challenges and future research directions, Cumputer & Security, Vol. 30(8), pp. 719-731 (2011)

[5] Milošević, N.: History of malware, Digital forensics magazine, Vol. 1(16), pp. 58-66, (2013)

[6] Arimatsu, T., Yano, Y. And Takahashi, Y.: Security operations center (SOC) and security monitoring services to fight complexity and spread of cyber threats, NEC Technical Journal, Vol. 12(2), pp. 34–37 (2018)

[7] Ernst & Young.: Security Operations Centers — helping you get ahead of cybercrime (2014) .

[8] IBM Global Technology Services.: Strategy considerations for building a security operations center. (2013) .

[9] Sihwail, R., Omar, K., and Ariffin, K. A. Z.: A Survey on Malware Analysis Techniques: Static, Dynamic, Hybrid and Memory Analysis, International Journal on Advanced Science Engineering Information Technology, Vol. 8, pp. 1662-1671 (2018)

[10] Lee, T., and Kwak, J.: Effective and Reliable Malware Group Classification for a Massive Malware Environment, International Journal of Distributed Sensor Networks, pp. 1-6 (2016)

[11] Gandhi, R., Sharma, A., Mahoney, W., Sousan, W., Zhu, Q. and Laplante, P.: Dimensions of Cyber-Attacks: Cultural, Social, Economic, and Political. IEEE Technology and Society Magazine 30(1), pp. 28–38 (2011)

[12] Uma, M., and Padmavathi, G.: A Survey on Various Cyber Attacks and Their Classification. International Journal of Network Security Vol. 15 (2013)

[13] Bendovschi, A.: Cyber-Attacks – Trends, Patterns and Security Countermeasures. Procedia Economics and Finance, Vol 28, pp. 24–31. (2015)

[14] Ahmad, A., Maynard, S. B., and Park, S.: Information security strategies: towards an organizational multi-strategy perspective, Journal of Intelligence Manufacturing, Vol. 25(2), pp. 357-370 (2014)

[15] Bock, P., Hauet, J.-P., Francoise, R. and Foley, R.: Ukrainian Power Grids CyberAttack, The International Society of Automation (2017)

[16] FireEye.: Cyber Attacks on the Ukrainian Grid: What You Should Know. (2016)

[17] Kaspersky Lab.: LAZARUS UNDER THE HOOD. (2017)

[18] Yeoman, A. & Findlay, B.: CYBER SECURITY AND RISKS IN THE FINANCIAL SECTOR (2017) .

[19] Askarifar, S., Abd Rahman, N.A. and Osman, H.: A review of latest wannacry ransomware: Actions and preventions. Journal of Engineering Science and Technology 13 (Special Issue on ICCSIT 2018), pp. 24–33 (2018)

[20] Kowtha, S., Nolan, L.A. and Daley, R.A.: Cyber security operations center characterization model and analysis. 2012 IEEE International Conference on Technologies for Homeland Security, HST 2012, pp. 470–475 (2012)

[21] Onwubiko, C.:Cyber security operations centre: Security monitoring for protecting business and supporting cyber defense strategy, 2015 International Conference on Cyber Situational Awareness, Data Analytics and Assessment (CyberSA) (2015)

[22] RSA Technical Brief.: Building an Intelligence-driven Security Operations Centre (2014)

[23] Schinagl, S., Schoon, K. and Paans, R: A framework for designing a security operations centre (SOC). Proceedings of the Annual Hawaii International Conference on System Sciences, pp. 2253–2262 (2015)

[24] Sundaramurthy, S.C., Case, J., Truong, T., Zomlot, L. and Hoffmann, M. 2014. A Tale of Three Security Operation Centers. Proceedings of the 2014 ACM Workshop on Security Information Workers - SIW ’14, pp. 43–50. (2014)

[25] Torress, A.S. 2015. Interested in learning SANS Institute InfoSec Reading Room (2015)

[26] MDEC.: INDUSTRY GUIDANCE FOR NEXT GENERATION MANAGED SECURITY OPERATING CENTRE (2017)

[27] Miloslavskaya, N.: Security Intelligence Centers for Big Data Processing. Proceedings - 2017 5th International Conference on Future Internet of Things and Cloud Workshops, W-FiCloud, pp. 7–13. IEEE (2017)

[28] Rochford, O. and MacDonald, N.: The Five Characteristics of an Intelligence-Driven Security Operations Center. (2015)

[29] Milošević, N. 2013. History of malware (February 2013)

[30] Somov, A.: Wildfire safety with wireless sensor networks. EAI Endorsed Transactions on Ambient Systems. pp. 1-11 (2011)

[31] Motaz, A.: Start programming using Object Pascal. Vol. 2, pp. 10-11. Legally Free Computer Books, US (2013)