The Implementation of Strategic Threat Intelligence for Business Organization

[1]Leong Yee Ling and [2]Zolkipli, Mohamad Fadli
[1]Department of College Arts and Sciences, Faculty of School of Computing, Universiti Utara Malaysia, 06010 Sintok, Kedah Darul Aman, Malaysia.
[2]Department of College Arts and Sciences, Faculty of School of Computing, Universiti Utara Malaysia, 06010 Sintok, Kedah Darul Aman, Malaysia.
email: [1] leong_yee_ling1@soc.uum.edu.my, [2] m.fadli.zolkipli@uum.edu.my

Date received: 8 May 2021
Date accepted: 2 July 2021
Date published: 1 November 2021

Abstract - *Nowadays strategic threat intelligence is very important to all the organization. Strategic cyber threat intelligence can determine who and why to provide key insights to the organization. It purpose is to determine who is behind a particular threat or threat family and addressing to evolving trends. The strategic level of cyber threat intelligence also included and explains about why. Why makes a company or an organization a target? Strategic Threat Intelligence offer the overview of the threat status of the organization. Therefore, the C-Suite include chief executive officer (CEO), chief financial officer (CFO), chief operating officer (COO) and chief information officer (CIO) of the organization use cyber threat intelligence data to understand the high-level trends and threats to the company or the organization. The C-Suite of the organization also need to know how to implement the strategic threat intelligence to prevent unexpected things happen. This research paper aims to discuss about the importance of the strategic threat intelligence to the company or organization and how to implement it. After knowing and understanding the implementation of strategic threat intelligence to the company or organization, this research paper also will discuss about the when of using strategic threat intelligence. The issue and challenges is also discussed in the article.*

Keywords: Strategic, Data Intelligence, Threat, Business Organization, Threat Intelligence, Strategic Threat Intelligence.

1 Introduction

What is meant by strategic? The meaning of strategic is a plan that help to achieve. Few years ago, many people say that it is a hard work for having a succeed strategy management. Having a succeed strategy management need many resources, takes time and will disperse attention from operating daily business (Fadillah, 2019). Nowadays, this view is totally disagree. After reading many papers and found out that there are many benefits to developing and implementing a strategy in an organization. Therefore, the owner of the organization and CEOs that found out the value of having a succeed strategy. They start to invest their time and resources to manage and execute for having improvement on their performance continuously.

Strategy is a bridge that connecting producers and consumers (Fadillah, 2019). The strategic must be the most suitable and accurate steps and plans. Therefore, those strategies is able to build a more successful organization. For many reasons, all organizations have inherent weaknesses. All strategies have to do is try to make up for these weaknesses so that the organization does not trip up and suffer too much influence. The strategy also included many key principles that outline how an organization will achieve these goals.

What is data intelligence? Data intelligence is refer to an organization used all the tools and methods for analysis to understand more about the collected information and improve the quality of the services or investments. Data intelligence involves in analysing and interacting with data by a meaningful way in order to improve future decision-making (Landon-Murray, 2016). All data intelligence specialist will focus on the following main components. That are descriptive data, prescriptive data, diagnostic data, decisive data and predictive data. To

make a better decisions, data intelligence focus on understanding the data, discovering alternative explanations, solving problems, determine the future trends. Others than that, data intelligence can help organization to accelerated analysis by neatly arranging all data and frame a clearer models to store and clean up large data sets. Data intelligence is an important part of any organization's work to enhance the services that they employ and forward-looking the strategies that they use.

The remainder of this research paper is organized as follows. Section 2 will discuss about the literature review. The reasons of threat intelligence leakage will be discussed in Section 3. Section 4 will discuss about the importance of strategic threat intelligence. The issue and challenges in strategic threat intelligence will be discussed in Section 5. Section 6 will discuss the implementation of strategic threat intelligence. The when of using strategic threat intelligence will be discussed in Section 7. Last but not least, the final section will conclude this research paper.

2 Literature Review

To allow the readers more understand about the research paper title. Therefore, in this section it will be divided into several parts. That are the definition of threat, threat intelligence and strategic threat intelligence.

2.1 Threat

One of the famous worldwide strategy tools is SWOT Analysis. “S” represent as Strengths, “W” represent as Weaknesses, “O” represent as Opportunities and “T” represent as Threats. Therefore, it form the word of SWOT. It is one of the technique to show how much we understand about the business going on (Puyt et al., 2020). SWOT Analysis can be use so it brings advantages of an organization. It helps to reduce the chances of an organization towards failure by understanding what is the organization lacking of. Albert Humphrey is the creator of SWOT Analysis and it was created in the 1960 at Stanford Research Institute. This method was conducted because Albert Humphrey wanted to identify why corporate did not consistently to achieve their goal (GÜREL, 2017). Since then, SWOT Analysis was used quite often this days especially for business owner to start their own business organization.

“T” in SWOT represent as Threats. Threat include any external element that you cannot control and might negatively affect the organization from the outside. One of the factors that increase the difficulty or impossible the organization to achieve the goals is threat. These threat will stop the organization from maintaining the business or forfeit the competitive superiority and this will unfavorable for the organization. Threat can be the challenges that face by the organization on the path to success and it will cause irreparable loss (GÜREL, 2017). Such as the issues of supply chain, the changes in market demand or shortage of new employees. Before the organization become one of the threats’ victim or stagnant growing, it is important to anticipate the threat and take action to counter them. As a business owner or CEOs, you should always think over that what are the competitors doing now and whether the focal point of the organization should be changed to face the challenge.

2.2 Threat Intelligence

Threat Intelligence is any evidence-based knowledge about threats, which can provide a basis for decision-making (Tounsi & Rais, 2018; McMillan, 2013). Threat Intelligence is the process to gain knowledge that concerning cyber threat from multiple sources and it can protect the organization’s assets by detect malicious events (Moustafa et al., 2018). Considering the use of threat intelligence is a common step when the organization aims to improve the quality of the information security team and strengthen the defenses of the security. The goal of threat intelligence is to detect events or incidents as early as possible and possibly even prevent the events or incidents happen (Bromiley, 2016). Threat intelligence is often used by the information security teams that are mature enough to strengthen the environment and get ready to face those known or unknown threats. The business owner, stakeholders, CEOs or executives begin to be aware of cyber threats when they saw their competitors suffer from data breaches. Therefore, the organization need to have the understanding on Threat intelligence before integrate threat intelligence into the organization's defense.

Nowadays, threat intelligence services will keep developing is because of the targeted cyber-attacks are growing rapidly and growing exponentially. The most important reason of the emergent of the threat intelligence is because threat intelligence is to minimize the security vulnerabilities (Chandel et al., 2019). In order to maintain the attributes of the monitoring and analysis platform and properties of network traffic, threat intelligence expand the concept of intrusion detection by using signatures or anomaly-based technique or the mix of the two technique (Moustafa et al., 2018). When there are any rules triggered, the signature-based technique can tracks events of the host, network system, mobile device or computers and match with the predefined attack signature blacklist. The

signature-based method can effectively detect the existing network attacks, but it takes a lot of time to check and update the known of attack rules and it is inherently impossible to detect zero-day attacks without predefined rules. Threat intelligence has achieved a positive and great results in defending against the cyber-attacks throughout the world. Threat intelligence not only focusing on detection threat, but also focusing on prevention threats.

2.3 Strategic Threat Intelligence

There are four type of threat intelligence. That are Strategic Threat Intelligence, Tactical Threat Intelligence, Technical Threat Intelligence and Operational Threat Intelligence. Strategic Threat Intelligence offer the overview of the threat status of the organization (Dog et al., 2016; Tounsi & Rais, 2018). It is designed to provide information for high-level decisions made by managers and other decision makers in the organization. Therefore, its content is usually less or non-technical and presented through reports or briefings. Although the final product is less or non-technical product, generating effective strategic intelligence requires in-depth research through large amounts of data. Even for those rare analysts who have the appropriate language skills, technical background or industry skills, this can make it very difficult to manually collect and process data. Threat intelligence solutions that automated data collection and processing can help reduce the burden of the analysts and enable analysts that do not have much professional knowledge to work more efficiently.

3 Reasons of Threat Intelligence Leakage

Data leakage is one of the main cybersecurity issues and it will affect the digital economy (Confente et al., 2019; Ibrahim et al., 2020). Unfortunately, data leakages carry a variety of direct and indirect cost factors and these factors are critical to the survival and competitiveness of the organizations. The operational, financial, regulatory aspects and reputation of the organizations will be effected too.

3.1 Weak Password

Although it's seems easy, but weak passwords are usually the culprit for threat intelligence leakage of the organization. 48% of the threat intelligence leakage consist of stolen passwords and this statement is supported by a Verizon study (Verizon, 2020). Passwords that are too liable to guess or getting the password from keylogging malware or phishing attacks is the reason that threat intelligence leakage occur in the organization. Business owner or CEOs can bring out a Multi-Factor Authentication method for all the employees to protect the data or information of the organization. Multi-Factor Authentication is a secure authentication method that request to two or more authentication technique to get the right of use of a resources (Dasgupta et al., 2017). Therefore, the employees need to get and enter the code that send to the second device before login to the system. When somebody are trying to login and enter the system, Multi-Factor Authentication will give an alert notification.

3.2 Vulnerabilities

Hackers who set up an intrusion system usually utilize the SQL to inject the backdoors of the vulnerabilities. Vulnerabilities is still listed as one of the top reasons for threat intelligence leakage in the organization even though the abuse of buffer overflow vulnerabilities accounts for only 1% of hacking incidents. Therefore, employees that work in the security team should employ the applications that can do the scanning for the system. Then the organization can strict the protection of the database by identifying any vulnerabilities and solve the vulnerabilities.

3.3 Human Error

When programmers mistakenly or accidentally open the databases of the organization to the public or search engines then the threat intelligence leakage will occur. In this case, the confidential and private information will be leaked and anyone can get the access the database of the organization. This condition will continue until the database of the organization lock down. When this situation happened, those who interest in the data or information of the organization and wanted to hack into the organization's database or system will take the photo and print all of the confidential and private information of the organization out to keep for future use. When one of the employee in the organization is sending email that involve sensitive or important data to the wrong people or competitors and this is the common human error that will cause threat intelligence leakage. Most employee will use the function of "reply to all" when sending the emails to the customers or to the executives of the organization because it is more efficient for the worker and it will make employee get used to use the function. But can you imagine that if the email have the confidential and private information and what will happen?

3.4 Malicious Attacks

Mostly threat intelligence leakage will occur is because somebody or the competitors of the organization wanted to get the confidential data or information of the organization. The competitors can utilize any of the vulnerabilities or malicious attacks to find out the weak security and gain the threat intelligence. One of the operated method that hackers earn a huge amount of ransom are holding the organization data hostage. Thus, the hackers can easily to earn fast money by promising that will not publish the sensitive or confidential information of the organization to the public. The hacker will assume control or takes over the organization's database or encrypts the organization's files until the ransom is paid by the organization. This is Ransomware.

4 The Importance of Strategic Threat Intelligence

Regardless of scope, business or location, every organization will have certain core goals. These include increasing revenue, reducing expenditures, reducing risks, increasing employee satisfaction, increasing customer or consumer satisfaction and complying with compliance regulations (Bromiley, 2016). In general, it seems to have a negative impact on many of these goals if the organization focusing on information security. After all, security solutions will not be spent on other profitable tasks but will increase costs, and spent the time on training and stricter authentication. Of course, the areas where it can be adjusted, such as reducing business risk or compliance, but are not as attractive as increasing revenue. So why organization should care or concerned about information security?

4.1 Reduce Risk

Firstly, Strategic Threat Intelligence is important because it can reduce risk. Opponents, cybercriminals or anyone with the intent and ability to do harm are keeping on to discovery the new ways to penetrate the network of the organization. The visibility into these existing or new security hazards can offer by threat intelligence. By getting the knowledge and apply it to your organization, you can decrease the data loss of riskiness, improve regulatory compliance and prevent or minimize the interference of the business operations. By failing to prepare, you are preparing to fail. It is better to be prepared when nothing happen than things already happen but not be prepared. Which is true when discussing cyber security and threat intelligence.

4.2 Maximizing Staffing Efficiency

Others than that, maximizing staffing efficiency is also one of the importance of Strategic Threat Intelligence. Strategic threat intelligence cause the current security team more efficient and will not burn out due to alert fatigue. Manually verifying and correlating threat intelligence will spend a lot of time and occupy a lot of resources. Therefore, use a platform designed to produce this intelligence automatically and integrate it into the organization's infrastructure. It can shorten the security response time and enable your staff to focus on other important tasks and this also can save around millions of ringgits for your organization.

4.3 Invest In the Organizations' Infrastructure Wisely

Furthermore, Strategic Threat Intelligence is important because it can invest in the organizations' infrastructure wisely. While freeing up the workers of the organization to meet other needs, when you know the most urgent threats to the organization, the organization can address these critical issue by appropriately assign more investment in the organization's infrastructure. The important step towards the direction of resource priority is integrate the internal intelligence (vulnerability and patch management) with external intelligence. You can centralize the investment on a solution to solve the problem when you observe the increase in alerts at the organization's office in a specific location.

4.4 Reduce Organization Expenses

Lastly, Strategic Threat Intelligence is important because it can reduce organization expenses. Based on the points above, threat intelligence can ultimately reduce your costs and save the organization's capital. The improvement on defensive posture gained through threat intelligence helps to maximize the investment allocation of security, reduce the organization's risk and shorten the response time. By focusing resources on important matter or problem, the financial and human capital of the organization can achieve more savings.

5 Issue and Challenges in Strategic Threat Intelligence

It is essential to understand the current issues and challenges in the strategic threat intelligence field (Conti et al., 2018) when threat intelligence, data source of threat and threat intelligence sharing platform are inspected.

5.1 The Overload of Threat Data

The challenges that facing by the organization is the overload of threat data. Threat intelligence has been developed in a short period of time. Whether it is open sources, close sources or free use, there are around hundreds type of threat data sources available (Sahrom Abu et al., 2018). Organization must seasonably access that related and feasible strategic threat information and the ability to take action based on that intelligence in order to defend against the cyber-attacks (Johnson et al., 2016). However, many of the organization still face the dilemma of a large amount of threat data and lack of personnel expertise to make full use of their threat intelligence programs. To solve this problem, most of the organizations have successfully definite different kinds of resources and technologies to help to improve the utility of the threat intelligence.

5.2 The Quality of Threat Data

The second challenges that facing by the organization is the quality of the threat data. It is usual behaviour for security feed providers to market threat feeds as cyber threat intelligence. 70% of threat intelligence sources are briefly and unreliable in terms of quality and this statement is supported by a study (Sahrom Abu et al., 2018). In order to capture and abundant the data and help Decision Support Systems to improve the value of threat intelligence and make it feasible, the security sensors must be redesign by the security feed providers. The Cyber Threat Alliance launched a program to improve the quality of threat intelligence that will be shared among the community members. The threat intelligence from the members of the Cyber Threat Alliance will automatically rate the quality of the threat intelligence, and only when the members of the Cyber Threat Alliance provided the sufficient quality input, the members of the Cyber Threat Alliance only can extract the threat intelligence.

5.3 The Issue of Privacy and Legal

The third challenges that facing by the organization is the issue of privacy and legal. Organization need to think about the privacy and legal problem and related the problem to how to share the data and which laws manage the data sharing. Many organizations are cautious about sharing data or information that may have a negative impact on the organization's brands (KPMG, 2013). Because of the concerns on leaking attack information and it may damage the reputation of the organization. Therefore some organization may hesitate to share data or information. So far, Threat Intelligence Sharing Platform have provided functions that can build the trust between organizations. But Threat Intelligence Sharing Platform is just only for Group-Based Access Control and Ranking Mechanisms.

6 Implementation of Strategic Threat Intelligence

Before selecting the strategic of the threat intelligence, it is important to decide the organization's potential uses cases (Dog et al., 2016). Instead of select a strategic of the threat intelligence and try to accord and implement in the organization use cases to the strengths of the strategic. It is because the strategic of the threat intelligence can be used in many ways.

6.1 Abundant Other Security Technologies

In order to ameliorate in making decision for incident response and policy enforcement, the security processes that currently existing by the organization should integrate the strategic threat intelligence. (McMillan, 2013) stated that, recently most of the security technologies are starting widely applied the strategic threat intelligence. This included invaded detection and defense, application for web protection, management on vulnerability, firewall and threat management system, Secure Email Gateway (a software that used to monitor email that be sent and received), Secure Web Gateway (a solution that protect the organization by preventing or blocking the unsecured internet traffic to enter the internal network of the organization), Distributed Denial-of-Service (DDoS), Security Information and Event Management (SIEM) and others.

A good starting point is to see what the organizations are using currently and take a look that how strategic threat intelligence can help the organization or make the organization more effective, in case the organization has not included the strategic threat intelligence in the organization security procedures. Nowadays, mostly strategic threat intelligence provide advanced machine intelligence that can be seamlessly integrated with the security products

that the organization are using currently. Moreover, there are more and more solutions are implementing open source standards and enable the data sharing across platforms to be more easier than ever.

6.2 Evaluating Vulnerabilities

The uses of strategic threat intelligence is to collect data and carried out analysis, which will help the organization create a simple indicators for assessing the vulnerabilities. The indicator should measure the overlap between the issue that organization can solve and the solutions. These solutions will work the best role by given the available time and available resources to the organization. Prioritizing vulnerabilities is a traditional method, but the best security method is to "fix everything in anytime at anywhere". Therefore, the organizations will inevitably compromises and solve the biggest issues first by adopting this method. The biggest issues (based on the actual damage caused) are the old vulnerability that still the same and continues to be utilize. Kindly remember that, the issue is not about zero-day threats or clever new attack exploits.

Threat actors are also limited by time and resources. As long as the threat actors continue to offer the results, the simplest and least resource intensive exploits will be used by the threat actors. In the past ten years of the analysis of the vulnerabilities progress, the discovery rate of new vulnerabilities is basically stable, while the number of exploits in the same period has increased exponentially (McMillan, 2013). This shows that most of the new vulnerabilities are actually variants of the old ones. Therefore, the top priority for any organization should be patch up the known vulnerabilities and not to worry about new threats.

6.3 Brand Monitoring

Even though the discussion above mention that vulnerabilities mostly related to internet, but choosing a strategic threat intelligence to monitor open source will also have great value, especially social media channels. These threats are emerging in public and will receive a wider review. They may be more secret and usually depend on social engineering techniques rather than software vulnerabilities and requires a certain degree of professional knowledge to be recognized.

Strategic threat intelligence that include brand monitoring will determine which links have been posted to the social media profile that are malicious, find out the malicious or fake social media configuration file that the employees have approved, assess the loss and abuse of intellectual property or imitate employee's profile. Phishing, domain scam or false flag program are the attacks that able to determine through brand monitoring and social media. Compared with open source tools, fewer misstatement or misinformation will be produce and will have higher efficiency when implement professional strategic threat intelligence.

6.4 Open Web, Deep Web and Dark Web Monitoring

A good strategic threat intelligence should collect its data from open sources and closed sources on the Internet (McMillan, 2013). Everybody on the Internet are available to use open source. This includes all data indexed on the search engines or the surface web. Deep web and dark web are include in closed sources. The parts of the internet that are protected by encrypted logins or paywalls and preventing search engine crawlers from accessing them are refers as deep web. The dark web consists of websites that can only be accessed through browsers that provide encryption and anonymity, such as Tor. Although not the only case, many dark web websites act as black market marketplaces for illicit products and services.

Vulnerabilities and exploits are usually discussed and traded by parties and threat actors who want to protect their security in the deep and dark web spaces. Therefore, data must be collected from these sources to keep it more comprehensive and up-to-date understanding of existing threats. Due to accessing these spaces will requires more skills and is more risky especially those on the dark web, one of the main values of strategic threat intelligence is that the strategic threat intelligence will do it for the organization.

7 When to Implement the Strategic Threat Intelligence

7.1 Before an attack

Before an attack occurs (Berndt & Ophoff, 2020), organizations can identify new and established threats and automatically defend them by directly integrating strategic threat intelligence into the intrusion detection system (IDS). Cyber threat intelligence can be used both proactively and reactively for strategic level. Strategic threat intelligence can be used actively or passively. It's a chance to use contextual information about new and existing

threats to keep attackers one step ahead. A threat actor analysis can reveal that a specific company or organization at risk and allowing security teams to take action to protect their company or organization before it is too late.

7.2 During an attack

The term of "acceleration" is one of the most widely used in the business, and it's easy to see why. Strategic threat intelligence can speed up the classification process from the start. When an attack has begun (Piplai et al., 2020), strategic threat intelligence may be used in a technique called threat hunting. This means looking and searching for the signs of an incident, instead of waiting for an alert when an attack occurs. Strategic threat intelligence provides strategies for the security teams of the organization to look for subtle evidence, included file deletions, changes to operating processes, registry settings and other signs of existence. This strategic threat intelligence also allows the security team of the organization to gain a deeper understanding of the attacker's motives by narrowing the scope of the search.

8 Conclusions

This research paper review on Strategic Threat Intelligence. Strategic threat intelligence can help organizations to predict threats before they appear, and plan accordingly to avoid. It also can prevent incidents first, such as malware signatures that can be used to update signature-based detection mechanisms. The extent to which an organization can use strategic threat intelligence in multiple business functions will depend on the quality of the material that provided and the maturity of the consumer organization. Therefore, strategic threat intelligence is important for all organization. The organization should implement the strategic threat intelligence to build a more successful organization. The current issue and challenge of the strategic threat intelligence is already discuss in the research paper.

All in all, the more prepared the security team in an organization, the stronger the security situation in an organization. Strategic threat intelligence can help security teams to determine the priority of the activities to counter the most likely threats of occurring and to protect the asset that most likely will be targeted.

Acknowledgements

The authors would like to thank to all School of Computing members who involved in this study. This study was conducted for the purpose of System and Network Security Research Project. This work was supported by Ministry of Higher Education Malaysia and Universiti Utara Malaysia.

References

Berndt, A., & Ophoff, J. (2020). Exploring the value of a cyber threat intelligence function in an organization. Information Security Education. Information Security in Action, 96–109. https://doi.org/10.1007/978-3-030-59291-2_7

Bromiley, M. (2016). *Threat Intelligence: What It Is, and How to Use It Effectively*. A SANS Whitepaper.

Chandel, S., Yan, M., Chen, S., Jiang, H., & Ni, T.-Y. (2019). Threat Intelligence Sharing Community: A Countermeasure Against Advanced Persistent Threat. *2019 IEEE Conference on Multimedia Information Processing and Retrieval (MIPR)*. https://doi.org/10.1109/mipr.2019.00070

Confente, I., Siciliano, G. G., Gaudenzi, B., & Eickhoff, M. (2019). Effects of data breaches from user-generated content: A corporate reputation analysis. European Management Journal, 37(4), 492–504. https://doi.org/10.1016/j.emj.2019.01.007

Conti, M., Dargahi, T., & Dehghantanha, A. (2018). Cyber Threat Intelligence: Challenges and Opportunities. *Advances in Information Security*, 1–6. https://doi.org/10.1007/978-3-319-73951-9_1

Dasgupta, D., Roy, A., & Nag, A. (2017). Multi-Factor Authentication. *Infosys Science Foundation Series*, 185–233. https://doi.org/10.1007/978-3-319-58808-7_5

Dog, S. E., Tweed, A., Rouse, L. R., Chu, B., Qi, D., Hu, Y., … Al-Shaer, E. (2016). Strategic Cyber Threat Intelligence Sharing: A Case Study of IDS Logs. 2016 25th International Conference on Computer Communication and Networks (ICCCN). https://doi.org/10.1109/icccn.2016.7568578

Fadillah, M. (2019). REVIEW OF COFFEE MARKETING STRATEGIES IN BUSINESS COMPETITION. *SCIENTIFIC JOURNAL OF REFLECTION: Economic, Accounting, Management and Business*, *2*(2), 131-140. https://doi.org/10.37481/sjr.v2i2.59

GÜREL, E. (2017). SWOT ANALYSIS: A THEORETICAL REVIEW. *Journal of International Social Research*, *10*(51), 994–1006. https://doi.org/10.17719/jisr.2017.1832

Ibrahim, A., Thiruvady, D., Schneider, J.-G., & Abdelrazek, M. (2020). The Challenges of Leveraging Threat Intelligence to Stop Data Breaches. *Frontiers in Computer Science*, *2*. https://doi.org/10.3389/fcomp.2020.00036

Johnson, C. S., Badger, M. L., Waltermire, D. A., Snyder, J., & Skorupka, C. (2016). Guide to Cyber Threat Information Sharing. https://doi.org/10.6028/nist.sp.800-150

KPMG. (2013). *Cyber threat intelligence and the lessons from law enforcement*. KPMG Cybersecurity.

Landon-Murray, M. (2016). Big Data and Intelligence: Applications, Human Capital, and Education. Journal of Strategic Security, 9(2), 94–123. https://doi.org/10.5038/1944-0472.9.2.1514

McMillan, R. (2013). *Definition: Threat Intelligence*. Gartner.

Moustafa, N., Adi, E., Turnbull, B., & Hu, J. (2018). A New Threat Intelligence Scheme for Safeguarding Industry 4.0 Systems. *IEEE Access*, *6*, 32910–32924. https://doi.org/10.1109/access.2018.2844794

Piplai, A., Mittal, S., Abdelsalam, M., Gupta, M., Joshi, A., & Finin, T. (2020). Knowledge Enrichment by Fusing Representations for Malware Threat Intelligence and Behavior. 2020 IEEE International Conference on Intelligence and Security Informatics (ISI). https://doi.org/10.1109/isi49825.2020.9280512

Puyt, R., Lie, F. B., De Graaf, F. J., & Wilderom, C. P. M. (2020). Origins of SWOT Analysis. Academy of Management Proceedings, 2020(1), 17416. https://doi.org/10.5465/ambpp.2020.132

Sahrom Abu, M., Rahayu Selamat, S., Ariffin, A., & Yusof, R. (2018). Cyber Threat Intelligence – Issue and Challenges. *Indonesian Journal of Electrical Engineering and Computer Science*, *10*(1), 371. https://doi.org/10.11591/ijeecs.v10.i1.pp371-379

Tounsi, W., & Rais, H. (2018). A survey on technical threat intelligence in the age of sophisticated cyber attacks. *Computers & Security*, *72*, 212–233. https://doi.org/10.1016/j.cose.2017.09.001

Verizon, D. (2020). Data Breach Investigations Report 2020. *Computer Fraud & Security*, *2020*(6), 4. https://doi.org/10.1016/s1361-3723(20)30059-2