Cyber Threat Intelligence – Issue and Challenges

Md Sahrom Abu[1], Siti Rahayu Selamat[2], Aswami Ariffin[3], Robiah Yusof[4]
[1,3]Malaysian Computer Emergency Response Team, Cybersecurity Malaysia
[2,4]Faculty of Information Technology and Communication,
Universiti Teknikal Malaysia Melaka, Malaysia

Article Info

Article history:

Received Jan 9, 2018
Revised Mar 2, 2018
Accepted Mar 18, 2018

Keywords:

Cyber Threat Intelligence
Data
Information
Intelligence

ABSTRACT

Today threat landscape evolving at the rapid rate with much organization continuously face complex and malicious cyber threats. Cybercriminal equipped by better skill, organized and well-funded than before. Cyber Threat Intelligence (CTI) has become a hot topic and being under consideration for many organization to counter the rise of cyber-attacks. The aim of this paper is to review the existing research related to CTI. Through the literature review process, the most basic question of what CTI is examines by comparing existing definitions to find common ground or disagreements. It is found that both organization and vendors lack a complete understanding of what information is considered to be CTI, hence more research is needed in order to define CTI. This paper also identified current CTI product and services that include threat intelligence data feeds, threat intelligence standards and tools that being used in CTI. There is an effort by specific industry to shared only relevance threat intelligence data feeds such as Financial Services Information Sharing and Analysis Center (FS-ISAC) that collaborate on critical security threats facing by global financial services sector only. While research and development center such as MITRE working in developing a standards format (e.g.; STIX, TAXII, CybOX) for threat intelligence sharing to solve interoperability issue between threat sharing peers. Based on the review for CTI definition, standards and tools, this paper identifies four research challenges in cyber threat intelligence and analyses contemporary work carried out in each. With an organization flooded with voluminous of threat data, the requirement for qualified threat data analyst to fully utilize CTI and turn the data into actionable intelligence become more important than ever. The data quality is not a new issue but with the growing adoption of CTI, further research in this area is needed

Corresponding Author:

Md Sahrom Abu,
Malaysian Computer Emergency Response Team,
Cybersecurity Malaysia,
43300 Seri Kembangan, Selangor D.E, Malaysia.
Email: sahrom@cybersecurity.my

1. INTRODUCTION

The latest threat landscape, shows that it is very difficult to prevent an attack and security breach due to attacker's capabilities to target vulnerabilities in people and process as well technology [1]. Cyber criminals have improved their tactics, techniques and procedures (TTPs) to the point where they have become difficult to detect and challenging to investigate and remediate [2]. Their TTPs become less predictable, more persistent, more resourceful, better funded, much more organized and motivated by money. Many organization being affected by organised criminal that deploy ransomware and demand payment to unlock critical data and systems. For example, the latest WannaCry ransomware attack that started on Friday, 12 May 2017, within a day spread over 150 countries and infect more than 230,000 computers [3].

In recent years, Cyber Threat Intelligence has received a considerable coverage by media and has been identified as a solution to counter the increased number and the complexity of security incidents. Many organization has opted to subscribe various threat intelligence collection whether from open-source or commercial sources. The problem is while too much data consumes and at the same time there is not enough data. This will lead to information overload issue. As a result, Threat Intelligence Sharing Platform (TISP) that can manage cyber threat intelligence data and convert this data into actionable intelligence, delivered to the different tools and assist in incident response has been introduced. Information security vendors and community are currently offering TISP solutions to provide threat intelligence feed and system that can assist cyber threat response. The solution can be divided into two categories which is content aggregation that can provide various threat data feeds and Threat Intelligence Management System for deriving business value from the collected information. Providers such as FS-ISAC, OASIS, IBM X-Force Exchange, Facebook Xchange, HP ThreatCentral, Checkpoint IntelliStore, Alienvault OTX, and Crowdstrike intelligence exchange more focus on content aggregation [4]. While Intelworks, Soltra, Threatstream, ThreatConnect, Vorstack, ThreatQuotient and CRITs to name a few, and more focus to Threat Intelligence Management System.

Apart from that most of information security vendors has come out with their own definition on Cyber Threat Intelligence to suit their business strategy and marketing. This confusion happens due to lack of academic literature discussing CTI between the community about the clear definition of CTI, the standard and protocol using in threat information sharing. This paper will serve as a guidance to better understand CTI by identifying the definition, current issue and challenge in CTI.

Section 2 of this paper describes the methodology that being implement for this literature review. Section 3 presents and describes various definition of CTI covered by the research community and how it complements the existing intelligence cycle. Section 4 presents the available standard and framework that being used in CTI. Section 5 identifies research challenge in CTI, providing analysis of the views in each area. As a conclusion, we provide a discussion and recommendation for future research in CTI.

2. RESEARCH METHOD

2.1. Search Strategy and Selection Criteria

The collection of targeted literature review for analysis in this paper based on keyword search. We performed information gathering on the definition, issue and challenge to cyber threat intelligence. Figure 1, shows the outlines our research approach. We started to review the literature from academic databases [5] such as IEEExplore and the ACM Digital Library. We followed-up citations and references in this literature to extend the number of relevant sources. We also identified literature by searching databases such as Google scholar. Using the search terms such as "Cyber Threat Intelligence" and "Actionable Intelligence". We searched for articles in peer-reviewed journals, books and grey literature (documents issued by government agencies e: g; federal, state, or local, private consultancies, non-governmental agencies, and private organizations).

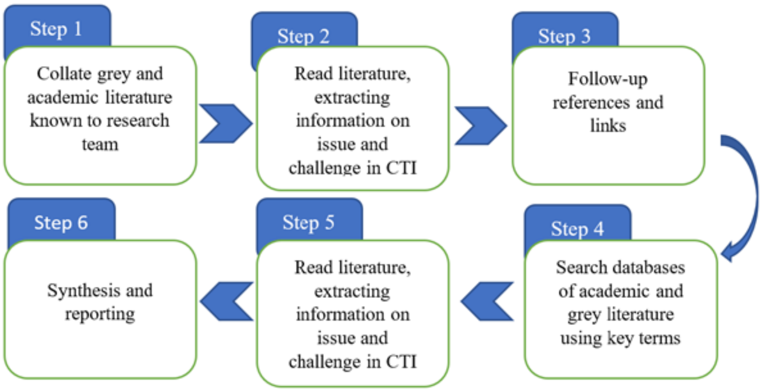
Step 1
Collate grey and academic literature known to research team
Step 2
Read literature, extracting information on issue and challenge in CTI
Step 3
Follow-up references and links
Step 4
Search databases of academic and grey literature using key terms
Step 5
Read literature, extracting information on issue and challenge in CTI
Step 6
Synthesis and reporting

Figure 1. Research Approach Overview

2.2. Data Analysis

Due to Cyber Threat Intelligence is a new topic, whitepapers from CERTS, software vulnerabilities and public information sharing platforms were also search for relevance information. The systematic review conducted using narrative synthesis by summarizing, comparing and contrasting the data for literature written in English since 2010.

2.3. Inclusion and Exclusion Criteria

The keyword search process produced a significant number of results. To ensure that only relevant sources were included for review, articles discovered by the search process were measured against several criteria. Each source had to meet one or more of the requirements identified. First, the source is directly addresses at least one specific aspect of cyber threat intelligence, such as relevance, timeliness or actionable. Second, the source is not directly related to cyber threat intelligence, but provides a definition of one or all.

These requirements are used in order to achieve the paper's aim of providing a concise introduction to the immediate challenges and issues facing in cyber threat intelligence.

3. CYBER THREAT INTELLIGENCE

As threat landscape evolve and grow more sophisticated, there is still no general agreement to define cyber threat intelligence with information security community often incorrectly using the terms intelligence, cyber intelligence and cyber threat intelligence [6]. It is important for information security community to understand the basic concept to define cyber threat intelligence and how it is derived. As a starting point, this paper will begin analyzing existing definition and term that always being used extensively and interchangeably by security community in threat intelligence. We decide to cover four relevant terms in this field: cyber-attack, cyber-threat, intelligence and cyber threat intelligence.

3.1. Cyber-Threats and Cyber-Attacks

Nowadays, there is no agreement between security community on how to clearly define cyber-attack and cyber-threat while this term being used interchangeably [7]. We start analyzing CTI definition for this paper by consider cyber-attack and cyber-threat because it is a basic building block in all hostile cyber situation [8].

There are many definitions to clarify cyber-attack and cyber-threat as both term being the most discussed issue in mainstream media. In 2013, the US Government defined cyber-threat as a broad definition that cover wide range of security measures:

It is stated that cyber-threats cover a wide range of malicious activities that can occur through cyberspace [9]. Such threats include web site defacement, espionage, theft of intellectual property, denial of service attacks, and destructive malware.

In contrast to US Government, the Oxford English Dictionary [10] defines cyber-threat, “as the possibility of malicious attempts to damage or disrupt a computer network or system”. While cyber-attack is “an attempt by hackers to damage or destroy a computer network or system”.

This definition gave us an insight that cyber-threats are the condition when there is a possibility of malicious activity happens and cyber-attacks are when the incident become reality.

3.2. Data Information and Intelligence

The main question to ask when we want to understand the concept of cyber threat intelligence is “What is intelligence?” The most common work as reference to answer this question is a keystone document by U.S. Department of Defense [11]. Figure 2 shows the relationship between data, information and intelligence that can lead to actionable intelligence. An actionable intelligence must always be the end goal in threat intelligence lifecycle to improve cyber security. Organizations need to invest more on human analyst to conduct analysis and produce actionable threat intelligence. Actionable threat intelligence can provide sufficient information to make an informed decision that can be acted upon.

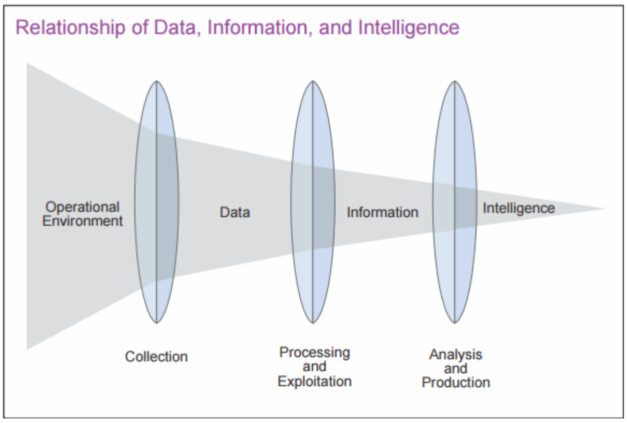

Figure 2. Relationship of Data, Information and Intelligence [11].

There's a huge difference between noise, threat data, information, and intelligence, and understanding the difference is essential to getting the most out of threat intelligence platform.

Data is comprised of the basic, unrefined and generally unfiltered information that are usually in the form of symbols and signals readings [12]. Symbols include words (text and/or verbal), numbers, diagrams, and images (still &/or video), which are the building blocks of communication. Meanwhile signals include sensor and/or sensory readings of light, sound, smell, taste, and touch.

Information is prepared data that has been processed, aggregated and organized into a more human-friendly format that provides more contexts and being useful for some form of analysis[12].

Dalziel [13] describes intelligence from professional perspective as data that has been refined, analysed and processed and the output must be relevant, actionable and valuable. Those three requirements can be achieved through logical and analytical process conduct by human that can provide contextual data and produce useable output.

While in the context of information security, Brown et al [4] describe intelligence as actionable information or the product of the intelligence lifecycle model, which includes several activities like planning, data collection, analysis and dissemination [14][15]. However, most of organization today primarily focuses on data collection and given less attention to other activities of intelligence lifecycle [16].

Comparing to the definition provided by Dalziel [13], the main purpose of intelligence is to support decision making or operational action such as detection, prevention and response.

Schoeman [17], expressed that tools and data feeds cannot by themselves provide threat intelligence without human intervention to derived intelligence from information and data. Agreeing with Schoeman, Lee stated that intelligence of any type requires analysis. Analysis is performed by humans. Automation, analytics and various tools can drastically increase the effectiveness of analysts but there must always be analysts involved in the process.

To summarize the data relationship, it can be said that data that collected from operational environment is processed and refined to produce information. Then the information is analysed and transformed to actionable format that constitute intelligence

3.3. Existing Cyber Threat Intelligence Definition

In recent years, Cyber Threat Intelligence (CTI) has become a hot topic in Information Security (IS) but the lack of literature review on clarifying the concept and companies tend to use their own definition to distinguish their product may lead to some ambiguity [18]. There are many different definitions to explain this term. As ambiguous as it can be, *Cyber Threat Intelligence* (CTI) can be define comprehensively as evidence-based knowledge, including context, mechanisms, indicators, implications and actionable advice, about an existing or emerging threat that can be used to inform decisions regarding the subject's response to that menace or hazard [19] . This definition stated that the organization can decide their action at the strategic, operational and tactical levels by using the collection of information that contain the details of current and emerging threat.

While Cloppert [18] offer several definitions to Cyber Threat Intelligence that based on operations, analysis and domain. Hence, he defined the Cyber Threat Intelligence Operations as actions taken in cyberspace to compromise and defend protected information and capabilities available in that domain. Meanwhile, Cyber Threat Intelligence Analysis as the analysis of those actions and the actors, tools, and techniques behind them to support Operations, and Cyber Threat Intelligence domain as the union of Cyber Threat Intelligence Operations and Analysis.

Based on Cloppert, threat intelligence is not only focus on nation state that bound by some technique to influencing national policy, but it is more on technical aspect such as tools and technique.

In contrast, Lee [18] proposed the definition for Cyber Threat Intelligence~~:~~ as “the process and product resulting from the interpretation of raw data into information that meets a requirement as it relates to the adversaries that have the intent, opportunity and capability to do harm”. From his study, Lee mentioned that threat intelligence involved the process of data transformation to information that relate to adversary.

Based on the definition reviewed, it shows that the definition given by Cloppert not only considers CTI being used to gain an advantage over the adversary, but that the adversary also uses it to gain an advantage over the defender. The definition given is also refers to more technical aspects such as tools and techniques. Compared to Lee, the definition given is refers to the intent, opportunity and capability to do harm.

3.4. Summary of CTI Definition

An analysis to the literature has shown that there is no widely accepted definition of cyber threat intelligence. Researchers tend to define the term based on their working environment and business nature. However, there is several key points that we can get from the existing definition namely context and element of CTI. Context is the pillar of CTI. Without context, CTI can easily become unmanageable stream of alert. Context allows security analyst to understand the type of threat or threat actor they are dealing with, so they can formulate an appropriate response plan. There are three main elements of CTI which are relevant, timeliness and actionable. The complete CTI definition need to cover these three elements to make sure only relevant threat data collected, analyze and processed in timely manner and the result can produce actionable intelligence to assist decision making.

‘

4. SOURCE OF THREAT INTELLIGENCE

The AlienVault [20] survey at Black Hat 2016 outlined that most of the correspondent rely on their own detection processes as a source for their threat intelligence strategy. Sixty-six percent of the respondents stated that data source come from their internal detection process, forty-eight percent from trusted peers, forty-four percent from paid subscription services, thirty-eight percent from government agencies, thirty-seven percent from crowdsourced/open source communities and twenty-eight percent from blogs or online forums.

An organisation can use their internal detection process as main source to gather data as it can provide higher visibility into their environment and will lead to a better use of information and tools in efficient way. While considering a government feed, or by pulling data from a crowdsourced platform as an option to give a comprehensive view of the overall threat landscape. A clear picture about their threat landscape can ease up organisation effort to develop, maintain and refine intelligence requirements that support business operation in planning and direction phase of Intelligence Lifecycle [11]. Hence, we can conclude that there are three categories of CTI source which are internal, external and community.

Internal sources for threat data collected from within the organization specifically internal network and SIEM that being implemented in organization. Threat data from internal network can be in the form of email log, alerts, incident response report, event logs, DNS logs, firewall log, etc.

External sources have a wide coverage of data and it requires verification by someone that have knowledge about organization threat landscape to determine its relevancy. Data feed from external can be from “Open source” intelligence (i.e., security researcher, vendor blogs, and publicly available reputation and block lists) that provide indicators for detection and context without any cost. However, the downside for open source intelligence is the data quality issue [21]. While private or commercial sources of threat intelligence are typically only available on a paid basis. It can include threat intelligence feeds, structured data reports (such as STIX), and unstructured reports (such as PDF and Word documents). Compared to open source, these feeds have a service level agreement on data quality through cyber threat intelligence update mechanism from vendor.

The threat data source from community category covered any CTI shared through trusted channel between members with the same interest. An example of formal community groups such as Information Sharing and Analysis Centers (ISACs) organized under the National Council of ISACs (NCI) specifically covered higher education or financial services. While Research and Education Networking (REN-ISAC) is a trusted community for research and higher education.

5. STANDARDS AND TOOLS IN THREAT INTELLIGENCE

To ease and speed up the intelligence sharing among organization, the need for structured automated exchange of information is required. Due to that, there is an increase of development to standard for threat intelligence sharing (e.g. CybOX, STIX and TAXII) and the development of threat intelligence sharing platform to support automated information sharing (e.g. MISP, OTX) [22]. As of today, STIX is considered as the de-facto standard for describing threat intelligence data and widely used by threat intelligence sharing platform [23].

5.1. Standards

There are many standards available for an organization to adapt depend on their specific needs. MITRE has developed three standards (CybOX, STIX, TAXII) as a package that were designed to work together for different needs in CTI management system. **CybOX** is refers to Cyber Observable eXpression XML schema. CYBOX characterize chronology and time range between events. CybOX XML schema is used to represent STIX observable that describe cyber artifact or event such as IPv4 address, with a few related objects [24]. **STIX** is Structured Threat Information Expression that leverage CybOX vocabulary for describing cyber threat information, so it can be shared, stored, and analyzed in a consistent manner. The architecture that represent STIX consist of nine construct such as observables, indicators, incidents, tactics, technique and procedure (TTP), exploit target, courses of action, campaigns, threat actors and reports. Indicators like IP addreses for command and control servers and malware hashes are the most frequently use among the community [25]. **TAXII** or Trusted Automated eXchange of Indicator Information is an open-source protocol and service specification to enable sharing of actionable cyber threat information across organization. TAXII addresses the sensitivity of threat data by providing common, open specifications for transporting cyber threat information messages, with capabilities such as encryption, authentication, addressing, alerting, and querying between systems in a secure and automated manner [26].

MILE also developed three standards as package that consist of Incident Object Description and Exchange Format (IODEF), Structured Cyber Security Information (IODEF-SCI) and Real Time Inter-Network Defense (RID). IODEF defined by RFC 5070 to normalize data from various sources for human analysis and incident response. While IODEF-SCI act as an extension to the IODEF standard that adds support for additional data and RID can be use as communication standard in CTI.

Mandiant also introduced Open Indicators of Compromise (OpenIOC) framework that can characterize static information.

While Vocabulary for Event Recording and Incident Sharing (VERIS) developed by Verizon allow the organization to share incident data and be part of the broad data set analysis.

5.2. Tools in Cyber Threat Intelligence

There is a growing interest from organization and security professional on collecting threat intelligence data and determining how to process this data. However, without the assistance from threat intelligence tools this threat data can become unmanageable stream of data. Due to that, many parties have developed tools that can help organization and security professional to manage the threat information sharing.

There are two tools that can be used for nomenclature and dictionary, Common Platform Enumeration (CPE) for hardware and Common Configuration Enumeration (CCE) for security software configurations.

REN-ISAC introduced Collective Intelligence Framework (CIF) as a client/server system for sharing enterprise threat intelligence data. CIF includes a server component that collects and stores threat intelligence data. Data can be IP addresses, ASN numbers, email addresses, domain names and uniform resource locators (URLs) and other attributes.

Alien Vault has taken an initiative to release Open Threat Exchange (OTX) for public to share research and investigate new threats. OTX can cleanses, aggregates, validates and enable the security community to share the latest threat data, trends, and techniques.

McAfee Threat Intelligence Exchange introduced ‘pull’ service for subscribers, virus definition, or DAT files contain up-to-date virus signatures and other information that McAfee anti-virus products use to protect a Linux, Windows or Mac computer against harmful software in circulation. New threats appear each day and McAfee constantly release new DAT files.

Finally, there is a project by The Computer Incident Response Center Luxembourg (CIRCL) developed Malware Information Sharing Platform (MISP) [27]. The main purpose for this trusted platform is to allows the collection and sharing of important indicators of compromise (IoC) of targeted attacks, but also threat information like vulnerabilities or financial indicators used in fraud cases.

5.3. Summary for Cti Standards and Tools

There is many tools and standards proposed and under development in CTI. While some of the standards overlaps with each other, many of them was use for specific objective. Standards also can ease and speed up the intelligence sharing among organization and form the basis for today's threat intelligence sharing platforms.

An organization can combine more than one tools and standards in their CTI program to make it fit with their specific requirement. Burger et al. [28] proposed an agnostic framework that can help to evaluate and assess the standard.

6. ISSUE AND CHALLENGES IN CTI

With cyber threat intelligence, type of threat data source and threat intelligence sharing platform (TISP) examined, it is crucial to look at the current issue and challenges in cyber threat intelligence area. This section identifies four current issues and challenges facing by consumer and producer of threat intelligence.

6.1. Challenge 1: Threat Data Overload

Threat intelligence has evolved in very short period and there is hundreds of threat data feed available whether from open source, closed source or free to use. To defend against cyber-attack, it is very important for customer to have timely access to relevant, actionable threat intelligence and the ability to act on that intelligence [29]. However, many of them still struggle with an overwhelming amount of threat data and a lack of staff expertise to make the most of their threat intelligence programs. According to a survey conducted by Ponemon [30] on 1000 IT practitioners in 2016, 70% of the respondent said threat intelligence is too voluminous and/or complex to provide actionable intelligence.

To address this issue many organizations have successfully identified a variety of resources and techniques to help maximize the effectiveness of their threat intelligence. This is support by the result of survey conducted by Ponemon [31] that show 80% of respondent agree that deploying threat intelligence platform can help the organization to automate threat intelligence. While 54% urge to have a qualified threat analyst staff to fully utilize threat intelligence potential.

6.2. Challenge 2: Threat Data Quality

It is common practice for security feed provider to market threat feeds as CTI. This statement support by a study conducted by Ponemon that indicate 70% of threat intelligence feeds are sketchy and not dependable in terms of quality. Security feed provider need to redesign their security sensors to capture and enrich the data to help decision-support systems increase the value of threat intelligence and make it actionable.

There is an initiative by Cyber Threat Alliance (CTA) to improve threat intelligence quality that being shared among community members. Threat intelligence coming from CTA members will be automatically scored for its quality, and members will be able to draw out threat intelligence only if they have provided sufficient quality input.

6.3. Challenge 3: Privacy and Legal Issue

When dealing with CTI, there are privacy and legal issues to consider that relates to how the data can be shared and which laws govern the sharing of data. Many organisations are wary of sharing information that could reflect negatively on their brand [32]. Some companies may be hesitant to share information due to the fear of reputation damage that may arise from disclosing attack information. As for now TISP already provide preliminary functionalities to establish trust between the organisations. However, it is limited to group-based access control and ranking mechanisms.

6.4. Challenge 4: Interoperability Issue in TISP

Vazquez et al. [33] raised an interoperability issue that face by existing threat sharing platform. The various standard and format use by threat sharing platform hindered the producer and receiver speak seamlessly to each other due to data extension is not supported by the used application.

As an initiative, MITRE group has developed three specifications/standards namely CYBOX (Cyber Observable Expression), STIX (Structured Threat Information Expression) and TAXII (Trusted Automated Exchange of Indicator Information) [24–26].

By adopting to the standard introduced by MITRE, interoperability issue between threat sharing peers can be solved. However, if there is no data standard can be established between peers due some constraint, data transformation can come in handy.

7. CONCLUSION

CTI adoption is still in early state and the needs for research and development is required to fully utilize its potential. This paper examines available literature that discuss the existing definition of CTI and the current state of development for common language and tools available in CTI.

We also identify several issues and challenges for data quality and CTI sharing platform. It is not a new issue for data quality but with the growing adoption of CTI, it is important to look at this as future research.

An organization can implement threat sharing platform to manage a large volume of threat feeds and hire a qualified threat data analyst to analyze, process and turn threat data to actionable intelligence. While at the community level, there is an initiative between community member to validate the threat data and make sure threat data shared among member have sufficient quality. There is also an effort by research and development center such as MITRE in developing standards format (e.g.; STIX, TAXII, CybOX) for threat intelligence sharing to tackle interoperability issue between threat sharing peers.

ACKNOWLEDGEMENTS

This work was kindly supported by The Ministry of Science, Technology and Innovation (MOSTI), Cybersecurity Malaysia and Universiti Teknikal Malaysia Melaka (UTeM).

REFERENCES

[1] Ernst & Young Global Limited. Cyber Threat Intelligence - How To Get Ahead Of Cybercrime. *Insights on Goverance, Risk and Compliance.* 2014.

[2] Watkins K-F. M-Trends 2017: A view from the front lines. Vol. 4, Premier Outlook. 2017.

[3] Kaur Sahi Asst S. A Study of WannaCry Ransomware Attack. *Int J Eng Res Comput Sci Eng*. 2017;4(9):7–9.

[4] Brown S, Gommers J, Serrano O. *From Cyber Security Information Sharing to Threat Management*. Proc 2nd ACM Work Inf Shar Collab Secur. 2015;43–9.

[5] Fiona M Lacey, Jill Jesson LM. Doing Your Literature Review: Traditional and Systematic Techniques. 1st ed. SAGE Publications Ltd; 2011.

[6] White TLP. An introduction to threat intelligence.

[7] Scarfone K, Piper S. Threat Intelligence for Dummies. *Norse Special Edition;* 2015.

[8] Robinson M, Jones K, Janicke H. Cyber warfare: Issues and challenges. *Comput Secur*. 2015;49:70–94.

[9] Niculae Iancu; Andrei Fortuna; Cristian Barna; Teodor Mihaela. Countering hybrid threats : lessons learned from Ukraine. Amsterdam : IOS Press; 2016.

[10] Press OU. Oxford English dictionary. 2013.

[11] US Joint Chiefs of Staff. Joint Publication 2-0 Joint Intelligence. Jt Publ. 2013;(October):144.

[12] Liew A. Understanding Data , Information , Knowledge And Their Inter- Relationships. *J Knowl Manag Pract*. 2007;8(2):1–7.

[13] Dalziel H. How to Define and Build an Effective Cyber Threat Intelligence Capability. *Elsevier Science & Technology Books,* 2014; 2014.

[14] Peter Gill MP. Intelligence in an Insecure World. 2012.

[15] Heuer RJ. Psychology of intelligence analysis. Technical Report. 1999.

[16] Sauerwein C, Sillaber C, Mussmann A, Breu R, Sauerwein C, Sillaber C, et al. Threat Intelligence Sharing Platforms : An Exploratory Study of Software Vendors and Research Perspectives. 2017;837–51.

[17] Schoeman A. Demystifying Threat Intelligence. 2014.

[18] Sergei Boeke J van de BDP. Cyber Threat Intelligence - From confusion to clarity; An investigation into Cyber Threat Intelligence. 2017.

[19] Li Qiang, Yang Zeming, Liu Baoxu, Jiang Zhengwei YJ. Framework of Cyber Attack Attribution Based on Threat Intelligence. *ICST Inst Comput Sci Soc Informatics Telecommun Eng* 2017. 2017;190:92–103.

[20] AlienVault. Threat Intelligence Déjà Vu. 2016.

[21] Amoroso E. Cyber attacks: protecting national infrastructure. 1st ed. Butterworth-Heinemann; 2011.

[22] Fransen F, Smulders A, Kerkdijk R. Cyber security information exchange to gain insight into the effects of cyber threats and incidents. *Elektrotechnik & Informationstechnik*. 2015;18:106–12.

[23] Sillaber C, Sauerwein C, Mussmann A, Breu R. *Data Quality Challenges and Future Research Directions in Threat Intelligence Sharing Practice*. Proc 2016 ACM Work Inf Shar Collab Secur. 2016;65–70.

[24] Casey E, Back G, Barnum S. Leveraging CybOX^{TM} to standardize representation and exchange of digital forensic information. *Digit Investig*. 2015;12(S1):S102–10.

[25] Barnum S. Standardizing cyber threat intelligence information with the Structured Threat Information eXpression (STIX^{TM}). *MITRE Corp* July. 2014;1–20.

[26] Connolly J, Davidson M, Schmidt C. The Trusted Automated eXchange of Indicator Information (TAXII ^{TM}). 2014;1–10.

[27] Wagner C, Dulaunoy A, Wagener G, Iklody A. MISP: *The Design and Implementation of a Collaborative Threat Intelligence Sharing Platform*. Proc 2016 ACM Work Inf Shar Collab Secur. 2016;49–56.

[28] Burger EW, Goodman MD, Kampanakis P, Zhu KA. *Taxonomy model for cyber threat intelligence information exchange technologies*. Proc ACM Conf Comput Commun Secur. 2014;2014–Novem(November):51–60.

[29] NIST. Guide to Cyber Threat Information Sharing. Vol. 150. 2016.

[30] Ponemon Institute LLC. The Value of Threat Intelligence : A Study of North American & United Kingdom Companies Sponsored by Anomali. 2016.

[31] Ponemon Institute LLC. The Cost of Malware Containment. 2015.

[32] KPMG. Cyber threat intelligence and the lessons from law enforcement. 2013.

[33] Vázquez DF, Acosta OP, Spirito C, Brown S, Reid E. *Conceptual framework for cyber defense information sharing within trust relationships*. Cyber Confl (CYCON), 2012 4th Int Conf. 2012;1–17.

BIOGRAPHIES OF AUTHORS

Md Sahrom Abu is a Senior Analyst at MyCERT, Cybersecurity Malaysia. His main task is focusing on cyber threats and research. He graduated from University of Teknologi, Malaysia for his Bachelor degree. Currently, he is pursuing a postgraduate degree.

Siti Rahayu Selamat is currently a senior lecturer at the Universiti Teknikal Malaysia Melaka, Malaysia. She received her Doctor of Philosophy in Computer Science (Digital Forensics). Her research interests include network forensic, cyber terrorism, cyber violence extremism, intrusion detection, network security and penetration testing. She is also a member of Information Security, Forensics and Networking (INSFORNET) research group and actively doing research in malware, criminal behavior and cyber violence extremism profiling.

Aswami Ariffin is a digital forensics scientist with vast experience in security assurance, threat intelligence, incident response and digital forensic investigation with various law enforcement agencies/regulatory bodies and provided expert testimonies in court. He received his Doctor of Philosophy in Computer Science (Digital Forensics). Currently, Aswami Ariffin is Senior Vice President of Cyber Security Responsive Services at CyberSecurity Malaysia. He is regularly consulted by the government, industries, universities and media on cyber security issues, strategies, research and development; also invitation as keynote speaker in conferences and providing expertise in community work.

Robiah Yusof received the BSc (Hons) of Computer Studies and Master of Information Technology from Liverpool John Moore's University, UK and Universiti Kebangsaan Malaysia respectively. She obtained the Doctor of Philosophy, Network Security from Universiti Teknikal Malaysia Melaka (UTeM) and currently a senior lecturer at the UTeM. She is also a member of Information Security, Forensics and Networking (INSFORNET) research group. Her research interests include network security, computer system security, network administration, network management and network design