Cyber Threat Intelligence Exchange- A Growing Requirement

N Veerasamy
Council for Scientific and Industrial Research, Pretoria, South Africa
nveerasamy@csir.co.za

Abstract: Managing the rise of cyber-attacks has become a growing challenge. Cyber space has become a battleground of threats ranging from malware to phishing, spam and password theft. Cybersecurity solutions mainly try to take a defensive stance and build a wall around pertinent technologies in an effort to protect them. However, perpetrators still manage to find a way to infiltrate networks and systems. This is where cyber intelligence can play a fundamental role. Cyber intelligence provides an alternative route for countering complex threats as it provides a collated manner in which to gain new insights and develop detective and reactive actions. Cyber intelligence supports the understanding of not only known threats and also looks to investigating the source, motivation and capabilities of the attacker. Cyber threat intelligence sharing encompasses various sources, uses, types of data, tools, skills and challenges. This paper proposes a framework that places these various aspects in perspective in order to provide background information for the initiation of a cyber threat intelligence sharing and exchange initiative.

Keywords: Cyber Threat, intelligence, exchange, cyber attack

1. Introduction

The threat landscape continues to evolve at a rapid rate. The number of cyber-attacks against global governments and commercial enterprises continues to grow in frequency and severity (Ponemon Institute 2015). Cyber-attacks are on the rise, especially the progression of complex attacks. The hackers of today are far more skilled, organised and well-funded than before and are getting better at finding weaknesses, penetrating security barriers and enacting more damaging attacks once inside a company (Taylor 2016). Unlike malware developed years ago, which was easy to notice, much of today's malware is specifically designed to quietly spread to other hosts and gather information over extended period of time which will eventually lead to the exfiltration of sensitive data and other negative impacts (Souppaya and Scarfone, 2013). Known as Advanced Persistent Threats (APTs) this type of malware has emerged as a critical concern.

Intrusion prevention and detection systems depend on signature and behavioural matches in order to detect anomalies. Signature and behaviour detection rely on patterns or detection of suspicious activity. Such techniques produce good results for blocking a large majority of incoming attacks but there is still a gap in terms of new threats-zero day attacks and other complex attacks targeting systems and networks. Signature and reputation feeds may help block mass attacks but they can miss targeted attacks for which no signatures exist (Isight Partners 2015). Today more than ever before, a passive approach to detecting and preventing economic crime is a recipe for disaster (PWC 2016). This is where cyber threat intelligence has an important role to play. It can provide useful knowledge of emerging or existing threats so that appropriate actions can be taken in response to the threat. Network security is no longer sufficient to detect and protect against the growing array of cyber threats.

An intelligence capability enables organisations to identify potential threats and vulnerabilities in order to minimize the "threat attack window" and limit the amount of time an adversary gains access to the network before they are discovered (KPMG 2013). Through threat intelligence, organisations can make better decisions in response to an impending danger based on the contextual information about the attack which may include the technique, tactics, pattern, indicator, actor and location.

Organisations could grow to depend on multiple data feeds that have been aggregated and analysed as such consolidated data could provide deep insights into attack trends. Cyber Threat Intelligence consists of functional visualisations displaying the data feeds as well as informational aggregated data. Cyber threat Intelligence tries to provide answers for the following questions (see Fig 1): "Who is attacking us?", "Why is there an attack?", "What are they attacking?" "How are they attacking?" "How can the attack be stopped?". Cyber Intelligence seeks to not only understand network operations and activities but also who is doing them, why and what happen next (Matern, Felker, Borum & Bamford, 2014).

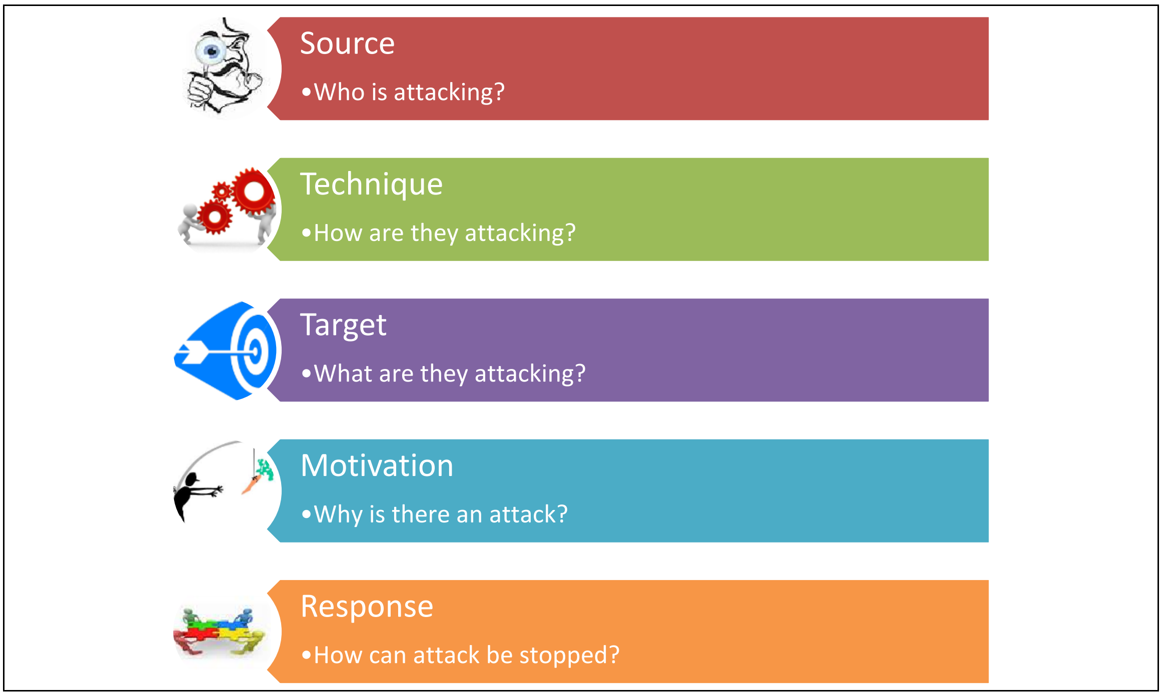


Figure 1: Cyber Threat Intelligence Objectives

Cyber Threat Intelligence goes beyond a list of malicious IP addresses or URLs. It places attacks into perspective by providing details covering attacks. When dealing with cyber intelligence key markings are the Indicators of Attack (IOA) and Indicators or Compromise (IoC). Cyber Threat intelligence provides the ability to detect attacks and thereafter develop better methods of protection and response. Cyber Intelligence is not just about data but needs the data to be contexualised. This will help provide insights about emerging threats and how to better protect the organisations infrastructure. Strategically it is important to determine who is carrying out attacks so that deterrence methods can be developed to prevent future attacks. Threat intelligence needs to be actionable sot that timely responses can be carried out.

Cyber Threat Intelligence aims to not only stop attacks but also to determine who is attacking, how is the attack being carried out, the target and motivation. In order to determine these issues, data can be collected in different means. Hugh (a) (2016) speaks of the three means of gathering cyber threat intelligence- Signal Intelligence, Open source Intelligence and Human Intelligence (see Fig 2).

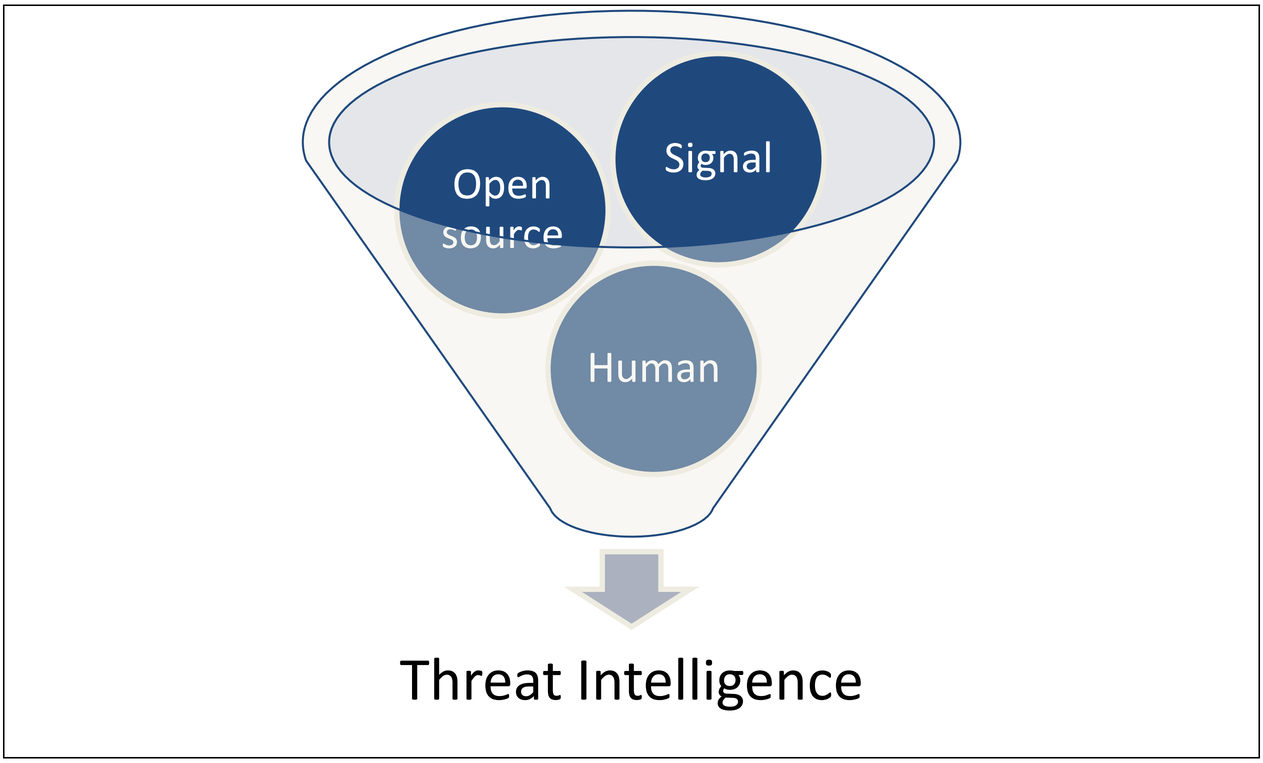


Figure 2: Means of Threat Intelligence

Signal intelligence (SIGNIT) results from the interception and analysis of signals, usually those used for communications and includes the monitoring of all signals coming into the networks.

Open source intelligence (OSINT) is derived from publically available information like books, publications, radio and television. In the context of the cyber threat intelligence, it can be sourced from the Internet from search engines and other "crawling" technology.

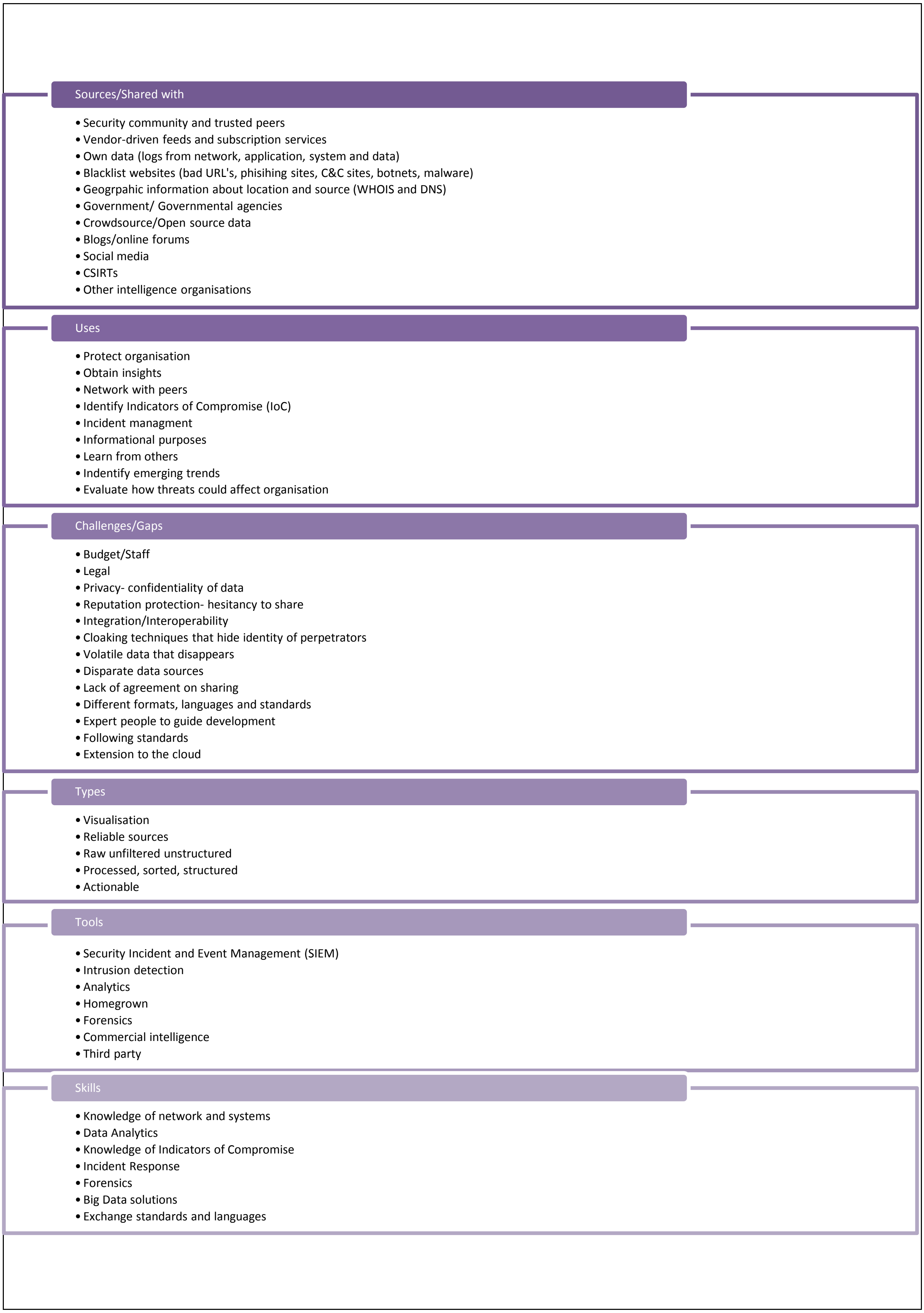
Human intelligence (HUMINT) differs somewhat in that SIGINT and OSINT can come from passive forms of intelligence collection like automated software but HUMINT is strongly active. It could consist of human sources studying threat actors.

Through SIGINT, anomalies in the network data can be identified. OSINT can produce large volumes of data that can produce good results and provide useful threat alerts. HUMINT can detect emerging trends and threat actors.

Overall cyber threat intelligence is a massive topic and has a broad range. In order to develop threat intelligence, this broad field can be narrowed down into different points from which to commence from. In the next section a framework is proposed that addresses the various issues relevant to the broad field of Cyber Threat Intelligence.

2. Framework for Cyber Threat Intelligence Sharing Paradigm

Various issues can affect the development and growth of Cyber Threat Intelligence sharing. This paper proposes a framework that places the paradigm of Cyber Threat Intelligence in context of all the issues facing this area of research. The framework is not exhaustive but rather documents the various sources, challenges, uses, types, tools and skills so that researchers engaging in this field of expertise have a baseline for initiating their Cyber Threat Intelligence Sharing efforts. The first grouping of issues influencing Cyber Intelligence is the source of information or the potential for involvement in information-sharing efforts.



Sources/Shared with

- Security community and trusted peers
- Vendor-driven feeds and subscription services
- Own data (logs from network, application, system and data)
- Blacklist websites (bad URL's, phisihing sites, C&C sites, botnets, malware)
- Geogrpahic information about location and source (WHOIS and DNS)
- Government/ Governmental agencies
- Crowdsource/Open source data
- Blogs/online forums
- Social media
- CSIRTs
- Other intelligence organisations

Uses

- Protect organisation
- Obtain insights
- Network with peers
- Identify Indicators of Compromise (IoC)
- Incident managment
- Informational purposes
- Learn from others
- Indentify emerging trends
- Evaluate how threats could affect organisation

Challenges/Gaps

- Budget/Staff
- Legal
- Privacy- confidentiality of data
- Reputation protection- hesitancy to share
- Integration/Interoperability
- Cloaking techniques that hide identity of perpetrators
- Volatile data that disappears
- Disparate data sources
- Lack of agreement on sharing
- Different formats, languages and standards
- Expert people to guide development
- Following standards
- Extension to the cloud

Types

- Visualisation
- Reliable sources
- Raw unfiltered unstructured
- Processed, sorted, structured
- Actionable

Tools

- Security Incident and Event Management (SIEM)
- Intrusion detection
- Analytics
- Homegrown
- Forensics
- Commercial intelligence
- Third party

Skills

- Knowledge of network and systems
- Data Analytics
- Knowledge of Indicators of Compromise
- Incident Response
- Forensics
- Big Data solutions
- Exchange standards and languages

Figure 3: Framework for Cyber Threat Intelligence

2.1 Sources/Shared with

Gathering relevant information is the first step toward generating actionable intelligence (KPMG 2013). Various role-players can serve as a source of cyber threat information. Information can also be shared with these sources to form a mutually beneficial sharing partnership. Alienvault (2016) identifies the following potential sources of cyber threat information:

- Own detection processes
- Trusted peers
- Paid subscription services
- Government/government agencies
- Crowdsources/open sources
- Blogs/online forums

In the proposed framework these sources have been adopted and also updated to show a more comprehensive list of potential sources. The security community has many websites and services to offer information. Information can also be received from feeds that may include subscription fees. Social media can also serve as a source of data. Relationships with Computer Incident Response Teams can provide threat information as well as other intelligence organisations. Overall, data can be collected and exchanged with a wide variety of sources. The next aspect of the framework is the uses of cyber threat intelligence.

2.2 Uses

The main uses of cyber threat intelligence sharing is to involve relevant parties in identifying incidents, patterns and trends that can be of benefit to relevant stakeholders. This can be used for attack prevention, detection and reaction as well as improving functionality. Isight (2015) explains that the advantages of cyber threat intelligence are greater visibility into threats and it gives insight into new indicators of compromise. The Computer Incident Response Centre in Luxemborg (2008) provides the following benefits of information sharing:

- Learning from others
- Acquire information about emerging threats or risks to other organisations
- Evaluate what threats could affect own organisation
- Make improvements to organisations threat and incident management
- Help protect organisations own infrastructure
- Support intelligence gathering efforts

Furthermore, Alienvault (2016) mentions that threat intelligence can be used to:

- Protect organisation's network from threats
- Obtain insights not capable of finding on own
- Use it to network with peers
- Manually ingest indicators of compromise
- Use it for incident response purpose
- Collect for informational purposes

In the framework, the uses of Cyber Threat Intelligence sharing have been summarised. The listed uses encompass the most pertinent applications of Cyber Threat Intelligence collection and sharing.

Development of cyber threat intelligence may bring with it various challenges and gaps may form. These issues mentioned in the framework are discussed next.

2.3 Challenges/Gaps

There are high expectations that Cyber Threat Intelligence will vastly improve security defence after it is integrated into current technologies and infrastructure. However, like every new development, there will be initial challenges and gaps as the technology grows and matures over time. When dealing with cyber intelligence, 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 (KPMG 2013). Some companies may be hesitant to share information due to the fear of reputation damage that may arise from disclosing attack information. With every new development, budget and skilled staff are required. Experts that are knowledgeable in the various standards and toolkits will be required. Cyber threat intelligence has various established standards and protocols. These include (Shackleford 2015):

- Open Threat Exchange (OTX)
- Structure Threat Information Expression (STIX)
- Collective Intelligence Framework (CIF)
- Open Indicators of Compromise (OpenIOC) framework
- Trusted Automated eXchange of Indicator Information (TAXII)
- Traffic Light Protocol (TLP)
- Cyber Observable eXpression (CyBox)

A major challenge will be the functioning and integration these various standards and formats to speak seamlessly to each other in a functioning system. Adherence and interoperability will thus become a growing challenge. Furthermore, as the data grows in size, extension to the cloud may become a viable option for data storage and protection. Cyber Intelligence encompasses various sources and formats of data. Information sharing agreements will have to be developed. Protection of Information and Communication Technologies (ICT) from cyber threats requires collaborative relationships for exchanging cyber defense data and the ability to establish trusted relationships (Vasquez, Brown, Spirito, 2012). Merging and working with volumes of data will bring many challenges both technically and procedurally. Cloaking techniques could be used to hide data or data could disappear from volatile operations and thus this could bring its own set of challenges. Cyber threat intelligence can be gathered from various types of data formats. The types of data that can be utilised is discussed in the next section.

2.4 Types

The data can be broadly classified as visualisation data, reliable sources (stemming from established trusted collaborative relationships), raw unfiltered, unstructured formats, processed, sorted, structured, and actionable data in which an acceptable response can be immediately executed. This grouping in the framework looks at the manner in which the data is presented and the influence on how it can be utilised. Unstructured data will require some processing. Actionable data will provide for immediate response action. Sorted and structured data can be utilised for intelligence functionality required. Visualisation data will help with the display and location of threats. Overall, data can fall into different classes depending on its level of usefulness. Data can be collected using various tools. The next section summaries useful tools that can be used in cyber threat intelligence efforts.

2.5 Tools

The SANS report on Who's Using Cyberthreat Intelligence and How? (Shackleford 2015) discusses the tools for aggregating and using Cyberthreat Intelligence. Some of the tools used include Security Incident and Event Management (SIEM), Intrusion Detection, Analytics, Homegrown, Forensic, Commercial and Third-party. A wide range of tools will be required to gather and analyse data. This list merely provides a basic description of typical tools that can be used for Cyber Threat Intelligence gathering and analysis as the tools required will be far more extensive. In order to utilise various tools, skills will also be required. In the next section, a listing of vital skills is provided.

2.6 Skills

The type of skills that will required to perform Cyber Threat Intelligence spans various domains like Networks and Systems, Intrusion Detection (Indicators of Compromise), Data Analytics, Incident Response, Forensics, Big Data and intelligence exchange standards and formats. One of the important skills is analysis. During this phase, large quantities of raw information will be processed into relevant, actual intelligence (Hugh (b) 2016). Developers will also need to have an understanding of networks and systems in order to analyse signature and event log data. Furthermore, once the data is analysed using forensics and possibly Big Data for processing the data, actionable steps may be taken. This will influence the Incident Response procedures in the organisation. Various skills can be utilised for cyber threat intelligence and can be further expanded. The listing provided in this section contains the most essential skills required which helps provide contextual details for cyber intelligence researchers to commence from.

3. Conclusion

Various issues can influence the development of cyber threat intelligence. This paper proposes a framework that encompasses the influential issues in the field of cyber threat intelligence sharing.

The framework allows for adaptation while still providing background details with regards to the most significant considerations for the development of cyber threat intelligence. The framework covers the issues of sources, uses, challenges, tools, techniques and skills. As emerging issues arise, it can be added to the framework. The usefulness of the framework is that it can be used for introducing and explaining the field to researchers embarking on a cyber threat intelligence investigation. Overall, the framework places the field of cyber threat intelligence sharing in context of the cyber threat landscape.

References

AlienVault, Threat Intelligence Déjà Vu, Blackhat 2016, Available https://www.alienvault.com/docs/analyst-reports/analyst-report-blackhat-2016.pdf, Accessed 20161020.

Computer Incident Response Centre Luxemborg (CIRCL), Information Sharing and Cyber Security- the Benefits of the Malware Information Sharing Platform (MISP), 2008, Available

https://www.circl.lu/assets/files/infosharing.pdf, Accessed 20161101

P Hugh (a), Improve your Threat Intelligence Strategy with these ideas, 2 February 2016, Recorded Future, https://www.recordedfuture.com/threat-intelligence-strategy/

P Hugh (b), What is Threat Intelligence?Definition and Examples, 22 September 2016, Recorded Future, Available https://www.recordedfuture.com/threat-intelligence-definition/.

Isight Partners, Executive Perspectives on Cyber Threat Intelligence, 2015, Available https://scadahacker.com/library/Documents/Threat_Intelligence/iSight%20Partners%20-%20Executive%20Perspectives%20on%20Cyber%20Threat%20Intelligence.pdf, Accessed 20161123.

KPMG, Cyber Threat Intelligence and the lessons from Law Enforcement, 2013, Available http://www.kpmg.com/BE/en/IssuesAndInsights/ArticlesPublications/Documents/Cyber-threat-intelligence.pdf, Accessed 20161123.

T Matern, J Felker, R Borum and G Bamford, Operational levels of Cyber Intelligence, International Journal of Intelligence and CounterIntelligence, 6 August 2014, Volume 27 http://www.tandfonline.com/doi/full/10.1080/08850607.2014.924811?scroll=top&needAccess=true

Ponemon Institute, 2015 Cost of Cyber Crime Study Global, October 2015, http://www8.hp.com/us/en/software-solutions/ponemon-cyber-security-report/, Accessed 20161028

Price Waterhouse Coopers, Global Economic Survey Adjusting the Lens on Economic Crime, Preparation bring opportunity back into focus, Available http://www.pwc.com/gx/en/economic-crime-survey/pdf/GlobalEconomicCrimeSurvey2016.pdf, Accessed 20161028

Shackleford D, Who's Using Cyberthreat Intelligence and How?, February 2015, SANS, Available https://www.sans.org/reading-room/whitepapers/analyst/cyberthreat-intelligence-how-35767

M Souppaya and K Scarfone, Guide to Malware Incident Prevention and Handling for Desktops and Laptops, NISt Special Publication 800-83 Revision 1, 2003, http://nvlpubs.nist.gov/nistpubs/SpecialPublications/NIST.SP.800-83r1.pdf, Accessed 20161028

H Taylor, An Inside Look at What's Driving the Hacking Economy, Feb 2016, CNBC, http://www.cnbc.com/2016/02/05/an-inside-look-at-whats-driving-the-hacking-economy.html, Accessed 20160828

DF Vasquez S Brown C Spirito, Conceptual Framework for Cyber Defence Information Sharing within Trust Relationships, 2012, IEEE, 4th International Conference on Cyber Conflict (Vasquez, Brown & Spirito 2012).