Development of a Semantic-Enabled Cybersecurity Threat Intelligence Sharing Model

Jabu Mtsweni[1, 2], Nobubele Angel Shozi[3], Kgwadi Matenche[1], Muyowa Mutemwa[1], Njabulo Mkhonto[1] and Joey Jansen van Vuuren[1]
[1] Council of Scientific and Industrial Research (CSIR), Defence, Peace, Safety and Security, Pretoria, South Africa
[2] University of South Africa (UNISA), Science Campus, Florida, South Africa
[3] Council of Scientific and Industrial Research (CSIR), Meraka Institute, Pretoria, South Africa
jmtsweni@csir.co.za
ashozi@csir.co.za
kmatenche@csir.co.za
mmutemwa@csir.co.za
nmkhonto@csir.co.za
jjvvuuren@csir.co.za

Abstract: Big Data is transforming the global technological landscape by elevating online information access required for addressing everyday challenges, such as detecting in real-time the spread of diseases within areas of interest. As the data in the cyberspace continues to grow in a gargantuan manner due to the popularity and successes of Web 2.0 technologies and social networks, amongst other reasons, organizations also continue to face the complex challenge of sifting through this data to timely detect and respond to security threats relevant to their operating domain. Traditional businesses and governmental organisations generally rely on inefficient and discrete solutions that rely on limited sources of information, signature-based and anomaly-based approaches to detect known cyber threats and attacks. On the contrary, threat agents continue to develop advanced techniques for their cyber espionage, reconnaissance missions, and ultimately devastating attacks. In addition, emerging cybersecurity intelligence solutions lack the semantic knowledge essential for automated sharing of timely and context-aware information within a specific operating domain. Moreover, existing cybersecurity information sharing solutions lack the visualization and intelligence necessary for handling the large volume of unstructured data generated by multiple sources across different sectors. In an attempt to address some of these challenges, this paper presents a preposition of a semantic-enabled sharing model for exchanging timely and relevant cybersecurity intelligence with trusted collaborators. Drawing from previous research and open source sharing platforms, such as CRITS, this model is underpinned by common information exchange standards, such as STIX and TAXII. The proposed cross-platform sharing model is evaluated by exploiting a large stream of cybersecurity-related tweets and semantic knowledge available from a variety of data sources. Preliminary results suggest that semantic knowledge is essential towards enabling collaborative and automated exchange of timely and actionable cybersecurity intelligence.

Keywords: cybersecurity, threat intelligence, crowdsourcing, big data, web security, vulnerabilities

1. Introduction

Governments, businesses, and individuals continue to rely on the Internet for effective information sharing and communication. At the same time, the Internet has become instrumental in enabling these key stakeholders to be prosumers; that is both producers and consumers of large information on the Internet. This has inadvertently led to what is commonly called Big Data -"*extremely massive and highly complex sets of information*" that is continuously increasing in volume, velocity, and variety (Khan et al., 2014; Zikopoulos, Eaton, & DeRoos, 2012). Although, Big Data presents various opportunities for organisations (Kaisler, Armour, Espinosa, & Money, 2013), it also introduces numerous challenges, such as difficulties in collecting and analysing all this data to timely act upon it or timely extract value (Katal, Wazid, & Goudar, 2013; Zikopoulos et al., 2012).

This is pertinent in the cybersecurity, where threats and attacks continue to increase in number and complexities. As such, cybersecurity threat intelligence is gaining prominence, mainly to collect such Big Data in order to recognize, understand and protect oneself against sophisticated cyber adversaries and vulnerabilities that are reported on daily basis. However, organizations are also finding it increasingly challenging to adequately tap into security-related Big Data and implement appropriate solutions for the exposed vulnerabilities or imminent threats. The main reason for this as highlighted in the abstract is that most organisations still operate

in silos when it comes to gathering cybersecurity intelligence. However, it is apparent that no one organisation can act on all the security-related Big Data alone.

Notably, in the developed world, large organisations are already collecting and sharing threat intelligence in order to protect themselves from emerging threats and attacks (Brown, Gommers, & Serrano, 2015). Powerful governments, such as in the United States and United Kingdom are already having legislations that attempt to encourage cybersecurity information sharing (Fransen, Smulders, & Kerkdijk, 2015; Ring, 2014) between the government and private organisations. At the same time, large organisations across the world already have security teams gathering large security datasets in order to understand the current threats and protect themselves from imminent cyber-attacks. Computer Incidents Response Teams (CSIRTs) are also common in many countries for receiving, reviewing, and responding to computer security incidents.

Nevertheless, cybersecurity threat intelligence is still emerging and possibly immature, thus many nations, particularly developing nations are lagging behind. In addition, relevant use cases and models that could encourage cybersecurity information sharing are limited. Existing solutions for sharing cybersecurity information are mostly commercial, and most lack the necessary semantics, intelligence, and visualizations necessary for sharing reliable, context-aware, and timely information. CSIRTs are mostly reactive and do not have foresight capabilities, and tend to focus on multitude of vulnerabilities and incidents, which are not necessarily relevant to every organization within a specific domain. Thus, in this paper we present a preliminary semantic-enabled threat intelligence sharing model that could be used by collaborating and trusted stakeholders to share cybersecurity information that might make it possible to timely limit and/or prevent cyber-attacks.

The rest of the paper is structured as follows: Section 2 briefly presents background information related to cyber threat intelligence, Big Data, and threat exchange platforms and standards. In Section 3, the research approach adopted for the research work conducted for this paper is presented. The proposed sharing model is discussed in Section 4 and Proof-of-Concept using Twitter as a case study is described in Section 5. The paper is concluded in Section 6 by re-affirming the key contributions from the research presented in this paper.

2. Background

In the fast moving domain of cybersecurity *"receiving the right information at the right time*" is vital towards reducing security risks, deterring attackers, and improving the security posture of an organisation (Goodwin et al., 2015). Hence, making effective use of cyber threat intelligence is an important component of any organisation's cybersecurity strategy. In the context of the government and military environments, intelligence is a well-understood concept and involves the collection, analysis, and interpretation of information for battlespace awareness (Waltz, 1998), and eventually for decision-making purposes (for example: defend or attack). This concept is also gaining ground within the cybersecurity space, chiefly because software vulnerabilities, threats and attacks are becoming more complex, severe, and dynamic. Threats are changing on daily basis and so are the solutions. Therefore, intelligence and continuous awareness of the software vulnerabilities, cyber threats, and attacks that faces individuals and organisations on daily basis are essential for mission accomplishment in the cyber space (Polancich, 2014; Ring, 2014).

Table 1: Information vs intelligence (Mishra, 2014)

Information	Intelligence
Structured, unstructured, raw (general), unfiltered information.	Structured, relevant, sorted and processed information
Aggregated from virtually every source.	Reliably aggregated and correlated for accuracy
May be true, false, misleading, incomplete relevant or irrelevant	Accurate, timely, complete (as possible), assessed for relevancy
Not actionable	Actionable

Before, we delve into the definition of threat intelligence, it is important to make a clear distinction between security information and cybersecurity intelligence. Table 1 highlights some of the differences. As may be noted in Table 1, ordinary security information, such as those that are found in common vulnerabilities databases might be unstructured and raw making it a challenge for organizations to timely act on it. In essence, Big Data can be classified as a large set of raw information. On the contrary, cybersecurity intelligence is information that is possibly structured, relevant, actionable and timely to achieve business goals (e.g. secure information assets).

Although cybersecurity intelligence is an emerging discipline, it is fairly defined (Brown et al., 2015; Ring, 2014). It is often referred to as threat intelligence, intelligence-driven information security, cyber intelligence or cyber threat intelligence (Eom, 2014; Farnham, 2014; Goodwin et al., 2015; Mishra, 2014; Ring, 2014). In this paper, these terminologies are used interchangeably to loosely refer to the collection and analysis of cybersecurity vulnerabilities, threats, incidents, indictors of compromise (IOCs) such as malicious IPs and URLS, and tactics, techniques and procedures (TTPs).

According to Eom (2014), "*cyber intelligence refers to the collection, processing, analysis, integration, evaluation, and interpretation of data concerning hostile cyber organization, cyber forces capabilities, network systems, hardware, software, threats and vulnerabilities*". In addition, McMillan (2013) defines threat intelligence as "evidence-based knowledge, including context mechanisms, indicators and actionable advice about an existing or emerging menace or hazard to assets that can be used to inform decisions regarding the subject's response to that menace or hazard". It is important to highlight that threat intelligence is about the discovery of vulnerabilities and threats before attacks are performed. Hence, Farnham (2014) cites that intelligence is actionable information. Threat intelligence could also be classified as strategic, operational or tactical (Eom, 2014). In this paper the focus is on tactical intelligence, which deals with information such as incidents, threats, vulnerabilities, TTPs, and IOCs (Goodwin et al., 2015).

According to Ring (2014), threat intelligence is an expensive exercise, which only few big organizations could afford to invest on their own and as such other small organizations are priced out of the threat intelligence market. Nevertheless, different types of threat intelligence collection mechanisms are emerging including Open Source Intelligence, Cyber Space Intelligence and Human Intelligence (Sood & Enbody, 2014).

At the same time, there are a variety of cybersecurity threat intelligence sources, mainly classified as internal or external and categorized as public or private. Presently, the manner in which threat intelligence is gathered and actioned is solely based on individual organisations and the challenge with this approach is well recognised, that is, lack of collaborations amongst organisations and governments (Ring, 2014). The insights shared in this paper contribute to this space of collaborative and coordinated tactical cybersecurity threat intelligence. Thus, in this paper we posit that securing oneself against complex cybersecurity threats and attacks calls for a shared and a coordinated approach that involves a number of stakeholders, such as the owners, developers, and users of the systems who are susceptible to cyber-attacks.

There are different approaches that could be adopted to exchange cybersecurity information, and as per (Goodwin et al., 2015), some of them could be: (1) voluntary exchange, (2) mandatory disclosure, (3) formalized exchange, (4) security-clearance-based exchange, (5) trusted-based exchange, and (6) ad-hoc exchange. For the purposes of this paper, trusted-based, ad-hoc, and voluntary exchange approaches are adopted. These approaches will be further elaborated in Section 4 and Section 5.

2.1 The rise of big data

The importance of Big Data in the cybersecurity space cannot be overly emphasized. In countries such as the United States it is even viewed as a national challenge and priority along with health care and national security. Big Data presents a number of interesting challenges for cyber intelligence. For example: quality of data, privacy and security (Katal et al., 2013; Khan et al., 2014). These challenges are compounded by the fact that Big Data are generated on daily basis through various media, and this further makes it impossible for one organization to store and timely process such data for decision-making purposes. IOCs (e.g. cyber threats, vulnerabilities, viruses, and malicious sites) contribute to the scale of Big Data. These IOCs are released on daily basis by individuals, private, and public organisations. However, organisations are unable to timely act on these IOCs because of a number of reasons, one of them being that organizations still rely heavily on traditional systems. Traditional systems suffer when it comes to dealing with Big Data, and as such new ways of dealing with Big Data, especially within the context of cybersecurity threat intelligence are needed.

2.2 Cybersecurity threat intelligence exchange platforms

As touched in Section 1, there are a couple of commercial and open source threat intelligence platforms that exist on the Web and in other closed environments. These platforms vary in terms of their features and target market. In the following subsections, we present a systematic literature review of these platforms, and motivate our chose for proof-of-concept purposes.

2.2.1 Malware Information Sharing Platform (MISP)

MISP is a platform for sharing, storing and correlating indicators of compromises of targeted attacks by allowing organisations to share information about malware and their indicators (MISP, 2015). MISP is a web based tool using a REST API to send and receive data. The MISP platform allows for storing of technical and non-technical information about malware and attacks, correlation between malwares, storing data in a structured format, exporting and importing in various formats, data sharing with other parties and trust groups using MISP and STIX support to export data in STIX format (Barnum, 2012). This platform is limited since it only focuses on malware information.

2.2.2 AbuseHelper

This is an open source project that is used to automatically process incident notifications. This tool is developed for CERTS and Internet Service Providers (ISPs) to help them in their daily jobs of following and treating a wide range of high volume information sources (AbuseHelper, 2011). The tool is not meant to be used for threat intelligence, thus not appropriate for the proposed sharing model.

2.2.3 IntelMQ

IntelMQ is a solution that was designed for CERTS to collect and process security feeds, pastebins and tweets using a message queue protocol. Its main goal is to give incident responders an easy way to collect and process threat intelligence to improve the incident handling processes of CERTS (InteMQ, 2015). The solution is generally limited to data collection and does not provide for custom sharing of threat intelligence.

2.2.4 Cyber Threat XChange (CTX)

CTX is a component of the HITRUST Cyber Threat Intelligence and Incident Coordination Centre (C3), which was created to detect and respond to cyber threats that are targeting the health care industry (HITRUST Alliance, 2015). CTX collects and analyses the cyber threats and distributes actionable indicators in electronically consumable formats that organizations can utilize to improve their cyber defences (HITRUST Alliance, 2015). The platform is limited to the health care industry.

2.2.5 Open Threat Exchange (OTX)

It is an open threat information sharing and analysis network that is created to put effective security measures within the reach of all organisations (Vault, 2014). OTX provides real time actionable information. The information shared is anonymized and shared with the AlienVault community. This solution although available online for used by the AlienVault community, it is not open source and thus not appropriate for proposed sharing model.

2.2.6 Soltra

It is a commercial cyber threat intelligence sharing platform. It integrates with various other systems, and is capable of pulling security data from disparate sources. It de-duplicates the data, routes intelligence to users, devices, or communities in real-time (Soltra, 2015). This platform was tested and found to be extensive; but because it is not open source at the time of the study, it was not used for the implementation of the proposed model.

2.2.7 Collaborative Research into Threats (CRITS)

CRITS is an open source malware and threat repository that uses other available open source software to enable users to create incidents and share them with others (MITRE, 2015). It can also be used by analysts and security experts to defend against malware and cyber threats. CRITS data is converted to CybOX objects, packaged within STIX documents. As such CRITS uses STIX as a common standard to convey the full range of cyber threat information. TAXII is the preferred method of exchanging information represented using the STIX language (Goffin, 2014). CRITS can also be locally, remotely or via custom APIs. In this paper, we are exploiting all the different access mechanisms as part of testing the feasibility of the sharing model within a distributed environment. Since it is open source and allows for integration with other systems using open source APIs, CRITS can also be extended, which is essential for adapting the sharing model to the needs of different stakeholders.

2.3 Exchange standards

There is a number of information sharing standards and languages. However, STIX developed by MITRE (Barnum, 2012) is one of the commonly used standards for exchanging cyber threat information. In this case, threat information can be exchange in a platform independent manner using languages such as XML and JSON.

2.3.1 Structured Threat Intelligence eXpression (STIX)

STIX is a structured language for representing structured cyber threat information in a fully expressive, extensible, automatable and human readable format (Barnum, 2013). STIX is made up of various packages and is capable of representing and sharing different types of cyber threat intelligence, including TTPs, incidents, vulnerabilities, trends, IOCs, and many others. It is also customisable, meaning that other relevant information can also be embedded within a STIX document, such as Traffic Light Protocol Information.

2.3.2 Trusted Automated Exchange of Indicator Information (TAXII)

TAXII is a MITRE's standard that can be used for automatically transporting cyber threat information across different STIX-enabled platforms. TAXII defines a set of services and message exchanges that when implemented enable the sharing of cyber threat information across organisations and service boundaries (Davidson & Schmidt, 2014). TAXII uses XML and HTTP for message content and support and allows for custom formats and protocols. In essence, it enables organisations to share structured cyber threat information in a secure and automated manner.

2.3.3 Incident Object Description Exchange Format (IODEF)

IODEF is a CML-based standard that can be used by CSIRTs to share incident information. It defines an information framework to represent computer and network security incidents (MILE, 2015).

2.3.4 Collective Intelligence Framework (CIF)

The CIF is a cyber threat intelligence system that allows its users to combine malicious threat information from various sources and use that information to identify, detect and mitigate any threats, which they find in their own systems (CIF, 2015). The CIF database mostly contains IP addresses, domains and URLS of the malicious activities that are observed.

2.3.5 Traffic Light Protocol (TLP)

TLP is a set of designations used to ensure that sensitive information is shared with the correct audience (US-CERT, 2015). It uses four colours to indicate different degrees of sensitivity and the corresponding sharing considerations to be applied by the recipient.

3. Research approach

The research presented in this paper followed an experimental approach as subscribed by the Design Science Research (Vaishnavi & Kuechler, 2004). This was preceded by a systematic literature review, where an extensive study was conducted on the existing threat intelligence exchange platforms, including *de facto* and *de jure* threat exchange standards. From the literature, it was determined that a number of threat intelligence sharing platforms exist, however most of these platforms are isolated and do not necessarily adopt any sharing model or use semantic knowledge to ensure that actionable information is shared.

In addressing the main research problem raised in Section 1, a conceptual modelling and practical approach was followed to realize a proof of concept (POC) for the proposed semantic-enabled sharing model. The POC was implemented by using a series of integrated components, including an existing platform (i.e. CRITS) as a foundation. In addition, Twitter, a popular social media platform, was selected as a data source. It was an obvious choice, mainly because it is capable of generating Big Data on daily basis. There are over 400 million tweets that are recorded per day (Tsukayama, 2013), and this makes Twitter a relevant case as it is highly improbable that one person or organisation can go through all these tweets or even share them with relevant stakeholders using traditional approaches.

4. Semantic-enabled threat intelligence sharing model

The proposed sharing model is presented in Figure 1. The model was derived based on the literature review and proof of concept experiments, which are elaborated in Section 5. The model comprises key components that are briefly outlined as follows:

- **Data Sources**: the complexities of cybersecurity demand that both external and internal information sources are considered for purposes of defending organisations' technological infrastructure and information assets. As such, cybersecurity threat intelligence can be obtained internally and from external sources, and must be collected, analysed, shared and leveraged. In the proposed model, considerations are made for two types of data sources. Raw data sources and "Stixified" data sources. By "Stixified" data sources, we refer to sources where data has already been prepared for an exchange platform that is STIX compatible (for example: hail-a-taxii data source). In our case, twitter is a raw data source, meaning data from Twitter would still need to be prepared using the streaming API.

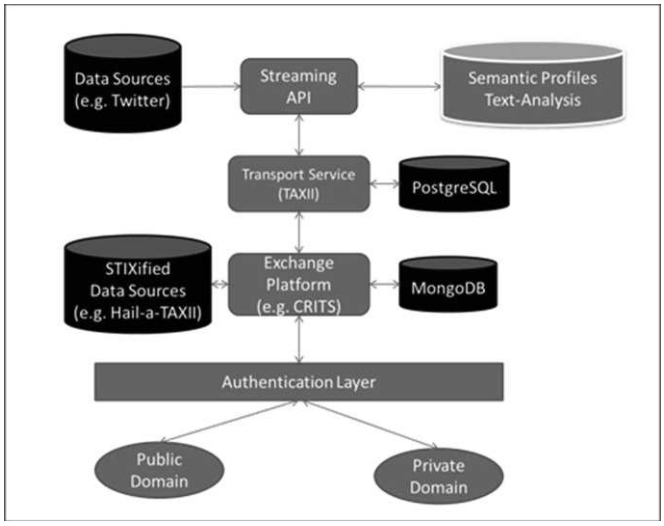

Figure 1: Proposed semantic-enabled sharing model

- **Streaming API**: it is responsible for searching, filtering, and cleaning tweets collected from Twitter based on specific keywords (e.g. malware). The streaming API is also responsible for embedding semantic knowledge in filtered tweets using text-analysis techniques and semantic profiles of organisations that are part of the sharing community. The filtered tweets, after being semantic-enabled, are converted into a STIX format (that is: STIXify). This is important for purposes of transporting them over the network to the TAXII server, which makes it possible for the data to be pulled by any STIX-enabled exchange platform. In our case, we adopted the CRITS platform for this exact purpose. Within the streaming API, a number of algorithms were implemented, such as algorithms for analysing the data to pick up malicious patterns, algorithms for detecting similarities between duplicate tweets, algorithm for crawling URLs found in tweets to ensure that they are not malicious, and others. However, these algorithms are beyond the scope of this paper.
- **Transport Service**: it is implemented using the TAXII server. This approach is preferred since it makes it possible to automatically exchange threat information with any platform that is STIX enabled. Any data source that could be represented in an XML format using STIX language could easily be shared with relevant stakeholders, and collaborators do not need to use the same platform for consuming threat intelligence information.
- **Exchange platform**: as discussed in literature, there are a number of threat exchange platforms that currently exist. Thus, the proposed sharing model is not tightly coupled to any specific threat platform. However, it is compatible with common exchange standards, that is STIX and TAXII (Barnum, 2013; Davidson & Schmidt, 2014). The techniques used exchanging information in the proposed model are trusted-based, ad-hoc, and voluntary (Goodwin et al., 2015). Trusted-based exchange deals with exchanging cybersecurity information with a closed community (e.g. banks). For our proof of concept, this is accommodated via the private domain and the Traffic Light Protocol (TLP) is used to classify all the information that is shared between different stakeholders. Regarding voluntary exchange, stakeholders share as they identify the need to do so, and could also share with any interested party they choose. This approach is regarded as the "richest and most valuable" (Goodwin et al., 2015). Lastly, ad-hoc exchange occurs in an episodic manner

where information is only shared in response to an incident or event. It is considered as relevant for addressing an emergent set of problems.

- **Authentication layer**: the exchange platforms enable stakeholders to share information using different modalities. For an example, in CRITS collaborators are able to create community groups operating within the same domain or environment to share information. Some of the information that is shared in specific groups must not be viewed by groups that are not part of the initial sharing groups. As such, the authentication layer plays the critical role of authenticating, managing and administering users that are part of the exchange platform. Furthermore, the authentication layer is essential for separating users who are supposed to view public domain content only and those that are privileged to view private domain cyber threat intelligence information.

In the following section, we elaborate on the proof-of-concept of the proposed model using Twitter as a case study.

5. Proof of concept: Twitter streaming and analysis

To combat the impact of cyber-crime and cyber-attacks organisations need to share the known threats with other relevant trusted organizations as soon as possible. Enormous amount of data exist from various sources, such as Twitter. In this section, we explore how the Big Data from a social network such as Twitter could be used to achieve the objective of sharing semantic-enabled threat intelligence information. Data can be pulled from Twitter, then be filtered and cleaned as it arrives on the system. It can then be semantically filtered using stakeholder profiles and text-analysis APIs, such as TextRazor (TextRazor, 2015).

For demonstration purposes, Python was used to implement the streaming API. The input to the API is a set of keywords that would assist in sourcing the relevant tweets. Figure 2 indicates an extract of the filtered tweets that the API was able to source in this specific experiment. It should be noted that the Twitter Search API puts restrictions on the number of tweets that can be streamed by external applications, however from our experiments conducted over few days, over 300 000 thousands tweets were acquired.

Figure 2: Sample of tweets extracted using the proposed sharing model

Once the data is filtered and cleaned, it is then tagged with the semantic data for the different stakeholders or keywords that a particular organisation is interested in.

Figure 3: Tweet converted to STIX

Once all tweets are cleaned and tagged, they are "Stixified" and pushed to the transport service in a STIX format as illustrated in Figure 3, where they could be pulled by any other exchange platform. This makes our approach platform-independent and loosely coupled.

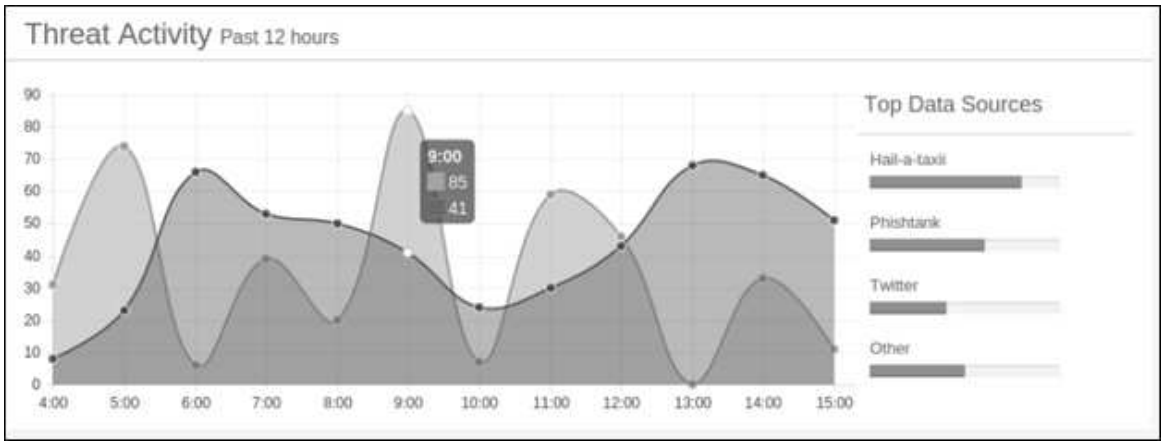

Figure 4: Private Dashboard – CRITS

Once the stream tweets or any other "Stixified" data sources have been pushed into the transport service, they can then be visualized. In our case, the visualization feature was incorporated into the modified CRITS platform using the crossfilter and D3.js plugins. As seen in Figure 4, only actionable threat intelligence is shared with the relevant stakeholders. Top data sources are also visualized, but additional data sources can be added as required. The significance of the proposed sharing model is that only the relevant threat intelligence is shared with the trusted parties. One other important feature of the model is that it accommodates both automatic and manual sharing of threat intelligence, and private and public sharing of threat intelligence is also possible. Due to space limitations, not all features of the model are discussed in this paper.

6. Conclusion and further research

The threats to cybersecurity are on the rise from different sources and for different reasons. This paper discusses the need for a collaborative tool which can be used to analyse Big Data related to cybersecurity using rights management to separate publicly and privately accessible intelligence. Herein intelligence is defined as analysed information, which enables actionable reactions by stakeholders to events in some cases even before these events occur. For the conceptual model, this paper discusses several options for the exchange platforms and exchange standards. By putting together the different exchange platforms and exchange standards a conceptual model was selected and implemented using the experimental and practical research approach. The data sources fed into the conceptual model was raw Twitter feeds, which were stixified and pulling into CRITS using a TAXII server as the Transport Service, the analysis of this data was display on the CRITS dashboard.

Further researcher could point to integrating more data sources into the model, and building common APIs that could accommodate different and unstructured data sources.

References

AbuseHelper. (2011). Abuse Helper. Retrieved from http://abusehelper.be/

Barnum, S. (2012). Standardizing cyber threat intelligence information with the Structured Threat Information eXpression (STIX™). *MITRE Corporation*. Retrieved from http://stix.mitre.org/about/documents/STIX_Whitepaper_v1.1.pdf

Barnum, S. (2013). Information with the Structured Threat Information eXpression (STIX™). Retrieved from http://stix.mitre.org/about/documents/STIX_Whitepaper_v1.0.pdf

Brown, S., Gommers, J., & Serrano, O. (2015). From Cyber Security Information Sharing to Threat Management. In *Proceedings of the 2nd ACM Workshop on Information Sharing and Collaborative Security - WISCS '15* (pp. 43–49). New York, New York, USA: ACM Press. doi:10.1145/2808128.2808133

CIF. (2015). Collective intelligence framework. Retrieved June 18, 2015, from https://code.google.com/p/collective-intelligence-framework/wiki/WhatisCIF

Davidson, M., & Schmidt, C. (2014). TAXII–Overview. Retrieved from https://taxii.mitre.org/specifications/version1.1/TAXII_Overview.pdf

Eom, J. ho. (2014). Roles and Responsibilities of Cyber Intelligence for Cyber Operations in Cyberspace. *International Journal of Software Engineering and Its Applications*, *9*(9), 137–146.

Farnham, G. (2014). Tools and and Standards for Cyber Threat Intelligence. Retrieved from http://www.sans.org/reading-room/whitepapers/warfare/tools-standards-cyber-threat-intelligence-projects-34375

Fransen, F., Smulders, A., & Kerkdijk, R. (2015). Cyber security information exchange to gain insight into the effects of cyber threats and incidents. *E & I Elektrotechnik Und Informationstechnik*, *18*. doi:10.1007/s00502-015-0289-2

Goffin, M. (2014). The Role of Structured Data Exchange in CRITS. Retrieved May 15, 2015, from https://github.com/crits/crits/wiki/Structured-Data-Exchange-Format-Implementations.

Goodwin, C., Nicholas, J. P., Bryant, J., Ciglic, K., Kleiner, A., Kutterer, C., … Sullivan, K. (2015). *A framework for cybersecurity information sharing and risk reduction*. Retrieved from http://download.microsoft.com/download/8/0/1/801358EC-2A0A-4675-A2E7-96C2E7B93E73/Framework_for_Cybersecurity_Info_Sharing.pdf

HITRUST Alliance. (2015). Cyber Threat XChange. Retrieved August 20, 2015, from https://hitrustalliance.net/cyber-threat-xchange/

InteMQ. (2015). CERT Tools - IntelMQ. Retrieved from https://github.com/certtools/intelmq

Kaisler, S., Armour, F., Espinosa, J. A., & Money, W. (2013). Big Data: Issues and Challenges Moving Forward. In *2013 46th Hawaii International Conference on System Sciences* (pp. 995–1004). IEEE. doi:10.1109/HICSS.2013.645

Katal, A., Wazid, M., & Goudar, R. H. (2013). Big data: Issues, challenges, tools and Good practices. In *Sixth International Conference on Contemporary Computing (IC3)* (pp. 404–409). IEEE.

Khan, N., Yaqoob, I., Hashem, I. A. T., Inayat, Z., Ali, W. K. M., Alam, M., … Gani, A. (2014). Big Data: Survey, Technologies, Opportunities, and Challenges. *The Scientific World Journal*, *2014*. doi:http://dx.doi.org/10.1155/2014/712826

MILE. (2015). Managed Incident Lightweight Exchange. Retrieved July 17, 2015, from https://datatracker.ietf.org/wg/mile/charter/

Mishra, P. (2014). Cyber Threat Intelligence. Retrieved from http://www.slideshare.net/prachimishra31/cyber-threat-intelligence

MISP. (2015). Malware Information sharing platform (MISP) – a threat sharing platform. Retrieved from https://www.circl.lu/services/misp-malware-information-sharing-platform/

MITRE. (2015). Collaborative Research Into Threats. Retrieved May 28, 2015, from https://crits.github.io/.

Polancich, J. (2014). Cyber Risk Intelligence: What You Don't Know is Most Definitely Hurting You. Retrieved from http://www.securityweek.com/cyber-risk-intelligence-what-you-don't-know-most-definitely-hurting-you

Ring, T. (2014). Threat intelligence: why people don't share. *Computer Fraud & Security*, *2014*(3), 5–9. doi:http://dx.doi.org/10.1016/S1361-3723(14)70469-5

Soltra. (2015). Soltra Edge Threat Intelligence Solution. Retrieved December 12, 2015, from https://soltra.com/

Sood, A. K., & Enbody, R. (2014). Chapter 2 - Intelligence Gathering. In A. K. Sood & R. Enbody (Eds.), *Targeted Cyber Attacks* (pp. 11–21). Boston: Syngress. doi:http://dx.doi.org/10.1016/B978-0-12-800604-7.00002-4

TextRazor. (2015). Extract Meaning from your Text. Retrieved December 9, 2015, from https://www.textrazor.com/

Tsukayama, H. (2013). Twitter turns 7: Users send over 400 million tweets per day. *Washington Post*. Retrieved from https://scholar.google.co.za/scholar?q=tweets+per+day&hl=en&as_sdt=0,5&scilu=3,2512304968481909214:375&scisig=AMstHGQAAAAAVmf40TyZSEwHjesHmMn8jmNtbevDMTaf#0

US-CERT. (2015). Traffic light protocol matrix. Retrieved October 5, 2015, from https://www.us-cert.gov/tlp

Vaishnavi, V., & Kuechler, W. (2004). Design Science Research in Information Systems. Retrieved from http://www.desrist.org/design-research-in-information-systems/

Vault, A. (2014). The Value of Crowd-Sourced Threat Intelligence. Retrieved from https://www.alienvault.com/docs/whitepapers/AlienVault_The-Value-of-Crowd-Sourced-Threat-Intelligence.pdf

Waltz, E. L. (1998). *Information Warfare Principles and Operations*. Artech House, Inc.

Zikopoulos, P., Eaton, C., & DeRoos, D. (2012). *Understanding big data*. *New York et al: McGraw …*. Retrieved from http://www.lavoisier.fr/livre/notice.asp?ouvrage=2609842