Cyber-Threat Information-Sharing Standards: A Review of Evaluation Literature

Nenekazi N. P. Mkuzangwe
Researcher, Defence and Security, Council for Scientific and Industrial Research (CSIR), Pretoria
https://orcid.org/0000-0002-2073-4082

Zubeida C. Khan
Senior Researcher, Defence and Security, Council for Scientific and Industrial Research (CSIR), Pretoria
https://orcid.org/0000-0002-1081-9322

Abstract

Cyber-threat information-sharing tools, through which cybersecurity teams share threat information, are essential to combatting today's increasingly frequent and sophisticated cyber-attacks. Several cyber-threat information-sharing standards exist, but there is at present no single standard or set of standards widely adopted by organisations and by computer security incident response teams (CSIRTs) operating at organisational, sectoral, national, and international levels. This introduces an interoperability problem in respect of communication across the various organisations and CSIRTs. Harmonised adoption of threat information-sharing standards would be of great benefit to cybersecurity efforts. In an effort to support harmonised use of cyber-threat information-sharing standards, this article provides findings from a review of the extant literature on such standards.

Keywords
cybersecurity, cyber-threats, information-sharing, standards, protocols, harmonisation, computer security incident response teams (CSIRTs), ontologies, use cases, semantic elements, syntactic elements, privacy, information security

DOI: https://doi.org/10.23962/10539/29191

Recommended citation
Mkuzangwe, N. N. P., & Khan, Z. C. (2020). Cyber-threat information-sharing standards: A review of evaluation literature. *The African Journal of Information and Communication (AJIC), 25*, 1-12. https://doi.org/10.23962/10539/29191

1. Introduction

Cyber-attacks are increasing in both frequency and sophistication, and no organisation is immune from attack. It thus becomes imperative for organisations to have mechanisms that will help improve their security and ability to defend against cybercrime—and, in turn, decrease their risks of suffering financial and/or reputational damage. Information-sharing about the various cyber-threats, vulnerabilities, and other malicious cyber-artefacts is one of the mechanisms used to help fight against the ever-growing and increasingly sophisticated cyber-attacks.

Key information-sharing entities at organisational, sector, national, and international levels are computer security incident response teams (CSIRTs), which are staffed by professionals performing both reactive and proactive services. These services include information-sharing, threat-sharing, incident-handling, and proactive threat intelligence. An example of an international CSIRT is the European Union Agency for Cybersecurity (known by the acronym ENISA, based on the agency's original name). CSIRTs typically have cyber-threat information-sharing standards and protocols in place, such as structured threat information expression (STIX), trusted automated exchange of intelligence information (TAXII), and cyber observable expression (CybOX). However, there are numerous available standards and protocols, and CSIRTs and organisations use varying standards, depending on their particular preferences. There is, thus, currently no widely adopted international set of standards for security teams' sharing of cyber-threat information. This lack of adoption of common standards can serve to undermine effective communication regarding cyber threats between organisations, and between organisations and sector, national and international CSIRTs.

According to Johnson et al. (2016), standardised data formats and transport protocols are important building blocks for interoperability, as they enable automation and allow information-sharing amongst organisations to occur at machine speed. Rantos et al. (2020) state that interoperability issues need to be addressed before any sharing of cyber-threat information and intelligence may occur, and they delineate the issues into the following categories: legal; policy and procedural; technical; and semantic and syntactic. Legal interoperability ensures the alignment of legal frameworks under which organisations operate and provide services, and it also caters to matters of data privacy. The policies and procedures for interoperability consist of formal statements that reflect organisations' objectives and detailed instructions to achieve these objectives. Technical interoperability relates to the implementation of tools that support the automated exchange of information (including delivery and consumption) and the underlying communication protocols used for the transport of the information. Semantic and syntactic interoperability involves conveying the necessary meaning via syntactically correct messages.

Several data formats (standards) are currently used for the exchange of cyber-threat information between entities, which is a situation that poses interoperability problems. Harmonised adoption of threat information-sharing standards is necessary for optimal cybersecurity. In an effort to support dialogue on harmonisation, this article provides findings from our review of literature evaluating existing cyber-threat information-sharing standards. The literature review was primarily conducted by means of keyword searches, using the following search string: "cyber threat information sharing standard", "cyber threat intelligence", and "cyber threat intelligence ontology". Initially Google Scholar was searched. Thereafter, academic databases such as Science Direct and IEEE Xplore Digital Library were searched. Citations and websites were gleaned from the collected literature and visited in order to augment the collection. It was found that the literature evaluating standards could be divided into four categories:

- ontologies;
- use cases;
- semantic and syntactic elements; and
- privacy and information security implications.

2. Ontologies

A proposed taxonomy for threat-sharing technologies and ontologies

Burger et al. (2014) propose a five-layer taxonomy for classifying threat-sharing technologies and for classifying ontologies of such technologies. The five layers proposed are: *transport*, *session*, *indicators*, *intelligence,* and *5Ws* (who, what, when, where, and why). The transport and session layers often ride over the hypertext transport protocol/transport layer security (HTTP/TLS). On the transport layer, the TLS is responsible for the encryption of the byte stream, which can be synchronous or asynchronous in order to ensure the confidentiality and integrity of the raw data (payload) that is being transported. The session layer is responsible for authentication and authorisation of users by defining the way in which users are authenticated to the system and what threat data they can access. The indicators layer represents cyber-intelligence payload and indicators. The intelligence layer specifies action and includes queries that are formulated from information gathered from the indicator layer about a target or targets. The 5Ws layer is used to gather information using "who", "what", "when", "where" and "why" questions, e.g., who is interested in the user or organisation?

Burger et al. (2014) use their model to evaluate two transport protocols—TAXII, and real-time internet-work defence (RID)—and two data representation formats: STIX, and versions of incident object description exchange format (IODEF). TAXII and RID are transport protocols for STIX and IODEF, respectively. Burger et al. (2014) found, via their evaluation, that:

- With respect to the transport protocol standards, TAXII and RID are in the *transport* and *session* layers since they provide secure transportation of cyber-threat intelligence. RID ensures that the client and the server are authenticated to each other, that the payload (the actual cyber-threat intelligence being transported) is encrypted (RID is primarily used over HTTP/TLS network protocol), and that privacy between partners is enforced. TAXII also encrypts the cyber-threat intelligence that is being transported, and authenticates users through network protocols like HTTP/S.
- With respect to the two data representation standards, STIX falls in the *indicators*, *intelligence* and *5Ws* layers, due to its wide range of objects. STIX's objects give it the ability to represent indicators, specific actions to be carried out, and the 5Ws. IODEF falls in the *indicators* layer since it consists of a data model that provides an XML representation of threat information shared amongst CSIRTs in relation to computer security incidents and events. IODEF for structured cybersecurity information (IODEF-SCI) falls in the *indicators* and *intelligence* layers since it extends IODEF to carry intelligence information. When deployed in conjunction with RID, IODEF can fall in the *intelligence* layer since it can be used as a query language.

Ontologies for semantic reasoning services

Asgarli and Burger (2016) analyse STIX and IODEF in order to map them to RDF/XML and to propose ontologies for semantic reasoning services. Semantic reasoning is the process of inferring new knowledge from an existing knowledge base using logical rules. The benefit in having an ontology is that, in addition to using it for threat intelligence, it can go a step further towards a more strategic approach that enables the system to make inferences about potential cyber-attacks in an effort towards automated response. Ontologies are created by entities (classes, object properties, and data properties) that are used to represent a domain. The Asgarli and Burger (2016) mapping process for STIX and IODEF results in an ontology for STIX containing 153 classes, 237 object properties, and 49 data properties. The resulting IODEF ontology contains 39 classes, 45 object properties, and 54 data properties. The STIX ontology is considerably larger because STIX contains definitions from CybOX, from common attack pattern enumeration and classification (CAPEC), and from malware attribute enumeration and characterisation (MAEC) standards.

Towards a comprehensive threat intelligence ontology

Mavroeidis and Bromander (2017) present a cyber-threat intelligence (CTI) model to characterise threat intelligence in terms of various dimensions. This model can be used for potential attack attribution. The model is characterised by *detective capabilities* and *preventive capabilities*. The authors use the CTI model to compare a set of 27 cyber-threat standards, taxonomies, and ontologies. They find that only two standards and two ontologies contain comprehensive threat information, according to their CTI model's characteristics, namely: the STIX1 and STIX2 standards, and the two unified cybersecurity ontology (UCO) standards. The authors find that other existing ontologies are not sufficiently comprehensive for use in representing information about cyber-threat intelligence, i.e., they lack formal constraints, which are used in ontologies to provide more specialised information about concepts such as cardinality (e.g., specifying that a certain threat has exactly one actor). Mavroeidis and Bromander (2017) also find that the ontologies target specific sub-domains of threat intelligence, and thus cannot be used for a wide range of cyber-threats.

In respect of the taxonomies they examine, Mavroeidis and Bromander (2017) find that relationships are not sufficiently established, in the taxonomies, between the motivations, goals, and strategies of the attackers— meaning the taxonomies are not sufficient for use in sharing information about cyber-threats. Mavroeidis and Bromander (2017) propose that the way forward is to develop a heavyweight ontology (one enriched with logical axioms describing concepts in details) for cyber-threats, so that information is represented in a uniform and logical format with the high degree of expressivity necessary for complex cyber-threat information.

3. Use cases

Overview of 22 standards' use cases

Kampanakis (2014) examines 22 standards in terms of the following: *each standard's purposes*, *other similar standards*, *where the standard is used*, and *its adoption level.*

Table: Standards examined in Kampanakis (2014)

Language standards	Transport standards	Scoring systems standards	Enumeration standards	Other
STIX	TAXII	common vulnerability scoring system (CVSS)	common platform enumeration (CPE)	software identification (SWID)
CybOX	RID	common configuration scoring system (CCSS)	common vulnerability enumeration (CVE)	
MAEC		common weakness scoring system (CWSS)	common configuration enumeration (CCE)	

open vulnerability and assessment language (OVAL)			common weakness enumeration (CWE)	
extensible configuration checklist description format (XCCDF)				
open checklist interactive language (OCIL)				
IODEF				
malware metadata exchange format (MMDEF)				
common vulnerability report format (CVRF)				
open indicators of compromise (OpenIOC)				
vocabulary for event recording and incident scoring (VERIS)				

Kampanakis (2014) finds that many of the standards overlap, and the choice of which standard to use depends on the context and use case. Accordingly, Kampanakis (2014) recommends that the first step should be to identify the use case of the security information to be represented and exchanged, followed by selection of the standard that covers that specific use case.

Incident reporting formats' strengths, weaknesses, use cases

Menges and Pernul (2018) propose a three-pronged model for evaluating incident reporting formats, based on the *structural*, *general*, and *additional* evaluation criteria. The *structural* evaluation criteria are based on a model that the authors call a universal pattern for structured incident exchange (UPSIDE). These criteria evaluate the incident reporting formats in terms of indicator, attacker, attack, defender, and contentual coverage. The *general* evaluation criteria, based on those proposed by Steinberger et al. (2015), evaluate the formats according to machine-readability, human-readability, unambiguousness of semantics, interoperability, extensibility, aggregability, practical application, and external dependencies. The *additional* evaluation criteria are licensing terms, maintenance effort, and documentation. Menges and Pernul (2018) apply this framework to four incident reporting formats:

- STIX versions 1 and 2;
- IODEF and IODEF version 2;
- VERIS; and
- extended abuse reporting format (X-ARF).

They find that, in terms of the structural/UPSIDE evaluation criteria, STIX and STIX 2 are able to represent the indicator, attacker, attack, defender, and contentual coverage specified in UPSIDE, while IODEF does not provide indicator, attacker, or defender coverage. IODEF also does not provide sufficient contentual coverage. IODEF 2 extends the first version of IODEF in being able to represent the attacker and defender entities of UPSIDE, and in having increased contentual coverage. VERIS represents the attacker, defender and attack entities of UPSIDE, with less contextual coverage than the two STIX and two IODEF versions. X-ARF provides attacker and attack coverage but no indicator or defender coverage, and the lowest contentual coverage among the reporting formats considered.

In terms of the general evaluation criteria, Menges and Pernul (2018) find that both versions of STIX meet most of the general evaluation criteria, except for (in the case of STIX 1) human readability and extensibility, and (in the case of STIX 2) human readability and practical application. IODEF is found to have high interoperability, extensibility, human readability, aggregability and practical application, but low machine readability, ambiguity problems, and no external dependencies. IODEF 2 is found to have improved (over the first version of IODEF) via better machine readability, changes to prevent ambiguity, and use of external references, but with poor human readability. The interoperability and extensibility of IODEF 2 are similar to that of the original IODEF. VERIS has adequate machine readability and human readability, and good interoperability and extensibility, but no aggregability, external dependencies, or wide practical application. Meanwhile, X-ARF is found to score well in human readability, poorly in machine readability and ambiguity, and to lack aggregability or external dependencies.

In terms of the additional evaluation criteria, Menges and Pernul (2018) find that all the examined standards are licensed, maintained, and documented. However, for STIX 1 and IODEF, maintenance effort has fallen away with the introduction of the new versions.

4. Semantic and syntactic elements

Fenz et al. (2008) provide a framework for evaluating the semantic elements of security advisory standards in terms of their *semantic usability*, *information complexity*, and *distribution*. In respect of semantic usability, Fenz et al. (2008) analyse the degree to which a standard uses a common language to ensure machine readability, and the degree to which it provides clear and unambiguous semantics to ensure machine recognition. In terms of information complexity, the authors analyse the extent to which the standard provides necessary elements for describing information technology (IT) security incidents. In respect of distribution, they analyse the degree to which the standard is used by major CSIRTs, whether it is still supported, and the last time the standard has been updated.

Fenz et al. (2008) use their framework to evaluate the following six standards:

- advisory and notification markup language (ANML);
- European information security promotion programme (EISPP);
- common announcement interchange format (CAIF);
- IODEF;
- common alerting protocol (CAP); and
- OVAL.

Fenz et al. (2008) find that, in terms of *semantic usability*, OVAL is the only standard of the six that met the elements of this criterion fully; in terms of *information complexity*, four of the six standards—ANML, EISPP, CAIF and OVAL—satisfy the criterion; and in terms of *distribution*, four of the six standards—EISPP, IODEF, CAP, and OVAL—are satisfactory. Fenz et al. (2008) thus deduce that OVAL is the most suitable of the six standards for automatic or semi-automatic interpretation of security threats, though they do at the same time find that OVAL falls short on some requirements, e.g., patch information such as download locations or required reboots.

Steinberger et al. (2015) evaluate standards in terms of their *interoperability*; *extensibility; scalability*; *aggregability*; *protocol independency*; *human readability*; *machine readability*; *confidentiality, integrity and authenticity*; and *practical application* and *reliable message transport* for exchange protocols. They apply their evaluation framework to the following exchange formats:

- IODEF;
- CAIF;
- ARF;
- X-ARF versions 1 and 2;
- common event expression (CEE); and
- Syslog RFC 5424.

Steinberger et al. (2015) also evaluate two exchange (transport) protocols—RID and common intrusion detection framework (CIDF)—and the following extensible messaging and presence protocols:

- XMPP extension protocol;
- incident handling protocol XEP-0268;
- intrusion detection exchange protocol (IDXP);
- simple mail transfer protocol (SMTP);
- common event expression (CEE) log transport (CLT); and
- Syslog RFC 3164 and RFC 5425.

For the exchange formats they have considered, the authors find that *extensibility* is high for all the exchange formats, while the *confidentiality, integrity and authenticity* and *practical application* criteria are not well-satisfied by any of the exchange formats.

ARF, CEE and both versions of X_ARF are found to be high on *interoperability*. All the exchange formats they have considered were low on *scalability*, while *aggregability* is found to be high in CAIF and X_ARF v0.2. *Protocol independency* is found to be high in CAIF, ARF and both versions of X_ARF. ARF, CEE and both versions of X_ARF are found to be high in *human readability*, while *computer readability* is high in all the exchange formats considered. The authors did not report the evaluation of Syslog RFC 5424 exchange format.

For the exchange protocols and the extensible messaging and presence protocols they have considered, Steinberger et al. (2015) found that *reliable message transport* and *scalability* are high for all the protocols, except for Syslog RFC 3164 and RID. *Confidentiality, integrity and authenticity* are high for all the considered protocols, except for SMTP and RFC 3164. *Interoperability* is high for all the considered protocols, except for CIDF, XEP-0268 and CLT. The rest of the protocols are low (CIDF, XEP-0268 and CLT) or medium (RID and IDXP) gradings in terms of *practical application*.

5. Privacy and information security implications

Information-sharing may result in leaking of the private information of entities, or revealing sensitive information about the context (since attributing attacks and performing various security analyses require contextual information) (Kampanakis, 2014). Disclosure of sensitive information, and personally identifiable information (PII) can result in, inter alia, financial loss and loss of reputation (Johnson et al., 2016). Therefore, it is important to evaluate the sharing standards in terms of how much private information they leak about the sharing entities.

Kampanakis (2014), based on the review of 22 standards discussed in section 3 above, advises that cyber-threat information collection and sharing be done in a systematic manner in order to mitigate privacy risks, and points to NIST's Preliminary Cybersecurity Framework Appendix B as a methodology for the protection of privacy and civil liberties within a cybersecurity programme (NIST, 2013).

Mohaisen et al. (2017), in their exploration of the privacy risks associated with threat intelligence information-sharing, include an analysis of the private information-leaking risks posed by 14 widely-used information-sharing standards in three categories:

- enumeration standards: CCE, CWE, CVE, CPE and common attack pattern enumeration and classification (CAPEC);
- scoring systems standards: CVSS and CWSS; and
- language standards: CybOX, MAEC, OVAL, IODEF, XCCDF, STIX and CEE.

For the 14 standards, Mohaisen et al. (2017) apply the following information-leakage scoring system:

- 0 for non-leaked or public data;
- 1 for leaked inferential data;
- 2 for leaked sensitive data; and
- 4 for leaked PII data.

Mohaisen et al. (2017) find that the language standards have the highest overall scores, with CybOX having the highest score of 65 and STIX the second-highest score of 36. The language standards also leak the most PII data. Thus, adoption of CybOX and STIX require the deployment of supplementary privacy controls.

Albakri et al. (2018) provide an analysis of the information that is shared by STIX, determining which information is contained in the incident reports and the risks associated with leaking such information. For every STIX data field, the threat associated with the disclosure of the information that corresponds to the data field is identified and its severity evaluated. The authors also evaluate the extent to which the disclosure of the information that corresponds with the data field identifies an individual or an organisation. The study provides detailed understanding of which information in the cyber-incident reports needs to be protected against specific attacks, and of the potential severity of such attacks. The authors aim to derive a set of guidelines on how to use STIX in a disciplined way that reduces the information-security risks. Their analysis indicates that certain STIX data fields can leak PII, organisational information, financial information, or cybersecurity information—largely because STIX consists of many free text fields with unconstrained properties.

To avoid information leakage via these fields, the authors advise the use of templates and that organisations use customised versions of STIX that meet their specific risk profiles.

6. Conclusions

This study reviewed cyber-threat information standards to assist with addressing interoperability issues in cyber-threat information-sharing. From the reviewed literature, eight reporting formats—namely, STIX 1, STIX 2, IODEF, IODEF 2, VERIS, ARF, CEE and X_ARF—and one exchange protocol, RID, were identified as being able to facilitate interoperability. However, from the studies that examined the privacy implications of the standards, the language standards CybOX, MAEC, OVAL, IODEF, XCCDF, STIX and CEE were found to leak the most private information, followed by the enumeration standards CCE, CWE, CVE, CPE and CAPEC, while the scoring standards CVSS and CWSS were found to leak no private information.

As pointed out in the literature, the leaking of private information violates legal interoperability and needs to be addressed before any information-sharing can occur. The works reviewed also suggest that, before adopting a standard, the use cases applicable to the incidents to be reported must be determined, and the standard that is capable of handling such use cases can then be selected.

References

Albakri, A., Boiten, E., & De Lemos, R. (2018). Risks of sharing cyber incident information. In *Proceedings of the 13th International Conference on Availability, Reliability and Security* (pp. 1–10). Association for Computing Machinery (ACM). https://doi.org/10.1145/3230833.3233284

Asgarli, E., & Burger, E. (2016). Semantic ontologies for cyber threat sharing standards. In *2016 IEEE Symposium on Technologies for Homeland Security (HST)* (pp. 1–6). Institute of Electrical and Electronics Engineers (IEEE). https://doi.org/10.1109/ths.2016.7568896

Burger, E. W., Goodman, M. D., Kampanakis, P., & Zhu, K. A. (2014). Taxonomy model for cyber threat intelligence information exchange technologies. In *Proceedings of the 2014 ACM Workshop on Information Sharing & Collaborative Security* (pp. 51–60). Association for Computing Machinery (ACM). https://doi.org/10.1145/2663876.2663883

Fenz, S., Ekelhart, A., & Weippl, E. (2008). Semantic potential of existing security advisory standards. In *Proceedings of the FIRST 2008 Conference-Forum of Incident Response and Security Teams*. https://doi.org/10.1109/aina.2008.69

Johnson, C., Badger, L., Waltermire, D., Snyder, J., & Skorupka, C. (2016). *Guide to cyber threat information sharing*. NIST Special Publication 800-150. https://doi.org/10.6028/nist.sp.800-150

Kampanakis, P. (2014). Security automation and threat information-sharing options. *IEEE Security & Privacy, 12*(5), 42–51. https://doi.org/10.1109/msp.2014.99

Mavroeidis, V., & Bromander, S. (2017). Cyber threat intelligence model: An evaluation of taxonomies, sharing standards, and ontologies within cyber threat intelligence. In *Intelligence and Security Informatics Conference (EISIC), 2017 European* (pp. 91–98). Institute of Electrical and Electronics Engineers (IEEE). https://doi.org/10.1109/eisic.2017.20

Menges, F., & Pernul, G. (2018). A comparative analysis of incident reporting formats. *Computers & Security*, *73*(March), 87–101. https://doi.org/10.1016/j.cose.2017.10.009

Mohaisen, A., Al-Ibrahim, O., Kamhoua, C., Kwiat, K., & Njilla, L. (2017, October). Rethinking information sharing for threat intelligence. In *Proceedings of the Fifth ACM/IEEE Workshop on Hot Topics in Web Systems and Technologies* (pp. 1–7). Association for Computing Machinery (ACM). https://doi.org/10.1145/3132465.3132468

NIST. (2013). Improving Critical Infrastructure Cybersecurity Executive Order 13636: Preliminary Cybersecurity Framework. https://doi.org/10.1002/9781119369141.app3

Rantos, K., Spyros, A., Papanikolaou, A., Kritsas, A., Ilioudis, C., & Katos, V. (2020). Interoperability challenges in the cybersecurity information sharing ecosystem. *Computers*, *9*(1), 18. https://doi.org/10.3390/computers9010018

Steinberger, J., Sperotto, A., Golling, M., & Baier, H. (2015). How to exchange security events? Overview and evaluation of formats and protocols. In *Integrated Network Management (IM), 2015 IFIP/IEEE International Symposium on Integrated Network Management* (pp. 261–269). Institute of Electrical and Electronics Engineers (IEEE). https://doi.org/10.1109/inm.2015.7140300