A Survey of Automated Information Exchange Mechanisms Among CERTs

Muhammd Mudassar Yamin, Basel Katt

Norwegian University of Science and Technology, Teknologivegen 22, 2815 Gjøvik, Norway
{muhammad.m.yamin,basel.katt}@ntnu.no

Abstract. Nowadays innovative computer related exploits are released every single day, which makes researching about those exploits a significant task. A CERT (Computer Emergency Response Team) is an expert group that is responsible for handling cyber security incidents and for issuing feasible advisories and countermeasures for new vulnerabilities. There exist national CERTs and CERTs that belongs to large organizations; and the coordination among them to share knowledge of new threats and countermeasures is very essential for a timely emergency response. This can be done by a systematic information exchange process among different CERTs. The purpose of the present research paper is to give a review about automated information exchange mechanisms at CERTs. Furthermore, issues, challenges and various technologies used to automate information exchange are discussed.

Keywords: CERTs · Information Exchange · Autonomous

1 Introduction

In the field of cyber security latest vulnerability and malware signatures are detected by CERTs on daily basis. Exchanging the information about various signatures is essential for effective defense strategy. However, in the view of latest cyber crime events [1][2], the effectiveness of information sharing process among CERTs is questionable. Thus, the present research will analyze how automation will makes information sharing process more effective and reliable and how to maintain threat detection in organizations at the root level. The researcher would briefly present the available research related to information exchange processes between different CERTs. The present report seeks answers to the following research questions.

- What is the current state of the art of information exchange mechanism used by CERTs?
- What are the automated information sharing processes presently working in CERTs?
- What mechanisms are present to avoid crossing the boundaries of information sharing between CERTs?

- What are the control filtering mechanisms between CERTs?
- What are the limitations and problems present in automated information sharing between CERTs?

The rest of the paper is organized in the following sections. Firstly, the authors states a brief introduction of the automated information exchange processes used by CERTs. Secondly, the literature related to the automated information exchange mechanisms at CERTs is stated. Thirdly, the current status of information exchange mechanism at CERTs is stated. Then, the authors would reflect upon the automated information sharing process, infiltrating the boundaries of information sharing, control filtering process and the discussion about limitation and problems in the process of information sharing between CERTs would be analyzed. Finally, the researcher would then conclude the paper.

2 Related Work

Skopik et al. in 2016 [3] stated in *a survey on the dimensions of collective cyber defense through security information sharing* the brief description of information exchange mechanisms formulated by authentic bodies. The authentic bodies and the related enterprises consist of such product significance such as how to produce reliable security exchanging networks. Some of the examples are given as follow

- NIST guideline "Framework for Improving Critical Infrastructure Cybersecurity".
- ENISA documents "Cyber Security Information Sharing: An Overview of Regulatory and Non-regulatory Approaches" and "Cybersecurity cooperation: Defending the digital frontline".
- ISO/IEC standard 27010 "Information technology - Security techniques - Information security management for inter-sector and inter organizational communications".
- EU Network Information Security Directive.

Creating a reliable and secure cyber atmosphere is a priority for all member states of EU (European Union). This also include key internet enablers, critical infrastructure operators, such as e-commerce platforms, social networks, and operators in energy, transport, banking and health care services operating within EU. EU uses the ENISA (European Network and Information Security Agency) to help the member states and the commission by catering them with professional help and guidance. The structure of cyber security information for the purpose of information exchange between different networks can be formed by considering the following factors.

- Recognizing and finding out about cyber security information and bodies. Forming reliable and information exchange policy between exchanging CERTs.
- Pledging and reacting towards cyber security information; Ensuring the security of the cyber security information exchange.

– Suggesting the security and quality of shared reports about cyber security in information sharing data format, protocols and standards.

After discussing the above factors of information sharing, a research centre is formed as a reliable body consisting of security specialists, from enterprises belonging to various information technology industries, devoted to secure the information technology process by identifying the threats and risks in it, and propose countermeasures. Seeking recurrent structures from event log data sets and marginal reporting from various equipment across different locations ensure the consideration of information across hundreds of users, applications and protocols. It joins the given data, enabling the user to have an overview of network activity combining log management, asset management, information from security controls and detection systems. The EU motivates the enlargement and the related usage of synergies between civilian and military facilities for securing the important cyber assets by producing research and development programs and by fostering coordination between governments, private sector and academia in EU.

Franke et al. in 2014 [4] investigated *Cyber situational awareness*. A research on cyber situational awareness was presented in eleven groups. Accordingly, the cyber situational awareness is mostly about knowledge regarding cyber issues. Such cyber issues need to be studied along with relevant data to get the complete realization of a situation. Instead of talking about the complexity of situational knowledge, majority of the available data is focused on cyber issues such as how cyber sensors can play a part in the complete understanding of the situation, or by focusing on the relations among particular cyber sensors in threat information acquisition, handeling and processing. The similarity among cyber sensors and their role in the overall situational awareness are studied, however the antonymic similarity in which the routine sensors have got the potential to play part in the cyber event is not covered fully. The eleven theme-based groups are discussed as follow.

– General cyber situational awareness
– Tools, architectures, and algorithms
– Information fusion
– Cyber situational awareness for industrial control systems
– Cyber situational awareness for emergency management
– Visualization for cyber situational awareness
– Human-computer interaction
– Nation-wide, large scale cyber situational awareness
– Exercises relating to cyber situational awareness
– Information exchange for cyber situational awareness
– Military cyber situational awareness

According to researchers in [4] given the prominent role of high-level cyber situational awareness in national cyber strategies, it seems that more attention should be directed to the risk of deception. On the rather liberal interpretation of a non-trivial empirical contribution slightly below 45% of the articles reviewed

were classified into this category, but it is noteworthy that only 3 out of 102 articles were found where exercises were used as vehicles to gather empirical data on cyber situational awareness. Cyber security exercises of various kinds offer a particularly interesting source of data on cyber situational awareness

Tounsi et al. in 2017 [5] stated that there is a particular interest in the favor of threat detection, when organizations nowadays are investing to procure different types of threat detecting tools, largely concentrating on the Technical Threat Intelligence(TTI). The researchers have concluded that in comparison to what was identified earlier, the quick exchanging of TTI is not enough to get rid of persistent attacks. Security lies in effective exchange of threat information among organizations. A standardized way for exchanging TTI reduces the risk of losing the quality of threat data, thus enables applying automated analytics on large bulks of TTI and the selection of the threat intelligence tool depends upon the objectives of the organization, as in some organizations the information processing and automatic analytics is desired. Majority of organizations motivate the threat information exchange by enhancing support between threat defenders. The benefits of exchanging data also consist of a good knowledge of the situational awareness of the threat scenario. The format of threat intelligence libraries or platforms are fabricated in such a way as that their main purpose is to overcome the bulk of problems of TTI and to help in exchanging the threat information with other organizations in the threat intelligence arena.

Bartnes et al. in 2016 [6] investigated *The future of information security incident management training* and concluded that the practice for reacting to information security events is treated with less enthusiasm and also various bodies like business managers and technical professionals have diverse opinion about information security. The aim of the information security incident management training is to give resilience to the potentials of the company in response to the events that could be helpful for business operations continuity. The human resource element acts here as a factor for the domain of resilience engineering, and the relation between the incident management process and resilience engineering activity. When their is no major security events limiting the preparatory activities, then a mark of preparation and importance is limited to event management planning and preparation activities between cyber security officials are restricted, specifically in comparison to the suggestions by ISO/IEC 27035. The recommendations from the cyber security officials stated that no prodigious information security events had been noticed that had affected their business endeavors. Probing into information security incidents is never given much attention as compared to other items, although the information and training are giving more importance than the written material in the wake of an event. Getting experience from previous events and getting ready for the upcoming events would help to device more strategies against the threats. The experience for getting knowledge about different tasks consists of security specialists, acquiring new perceptions on how to solve the problems, how to make better methods, performing the threat analysis, finding out direct causes, discussing new security measures that are desirable, and up-gradation the risk assessments.

3 Methodology

In order to understand the literature review of the present research paper, a keyword-based research is employed. The researcher started with *CERT* and *Information Exchange* with *automated*. The researcher investigated the following keywords in academic databases like Google scholar, IEEE and ACM to acquire the better understanding of the given terms [7]. The researcher also made himself familiar with the related literature on the given topic. The researcher spotted a lot of related information but employed them in indexed research articles only. The researchers conducted a thorough research and collected good amount of relevant literature in an organized manner, but the repetition of literature gathering process may yield slightly different results [9]. Hence, the researchers are including only the inclusion and exclusion criteria in the paper to lessen the variation of results in other literature reviews.

3.1 Inclusion Criteria

The researchers have followed the following inclusion criteria for the survey:

- Articles which are published in English.
- Articles which are directly related to CERTs.
- Articles that discusses Information exchange mechanisms in CERTs.

3.2 Exclusion Criteria

In respect of the huge amount of related data, the researchers have followed the following exclusion criteria:

- Articles that mention CERTs to some extent but are not directly related to it are not taken into consideration.
- The researcher also excluded conference abstracts, book reviews, conference information, discussions, editorials, mini reviews, news, and short communications for the survey .

3.3 Quality of Articles

The researchers have carefully gathered the relevant research articles for the present survey. The main purpose of this exercise was to build a stance for the survey and to extend it in the light of a specific research framework. The researcher evaluated the related articles with the help of a pre-defined criteria containing five quality assurance factors. The points are allocated on the scale of one to five, in which five is considered the highest value and one the lowest. The articles whose score topped the chart were given priority in the survey. The researchers have employed the following criteria.

- Reputation of publication channel, the publication channels which are well known and recognized by academia scored higher in our criteria.

- Citation of article, the articles which consist of more citations were given higher score in our criteria.
- The relevance of article, content in relation to survey topic were also given high score.
- Publication date of articles, the articles which are published recently received higher score as compared to older articles.
- The articles in which there was more number of references used to build the argument scored higher .

4 Information Exchange Mechanisms Among CERTs

During the survey we identified multiple information exchange mechanisms among CERTs details of which is as follows:

- CybOX [8]
  The first mechanism is The Cyber Observable expression cybox language, produced by a wide range of industry, academia, and government organizations all around the world. It standardizes the encoding and communication of highly confidential information about cyber observable, whether they are dynamic events or stateful measures observable in the operational cyber domain. The cybox Language consists of three overarching principal objectives: Firstly, to develop a common solution for all relevant usage cases. Secondly, to support multiple cyber security use cases. Thirdly, to develop it in a form that is flexible enough to offer a common solution for all cyber security use cases requiring the ability to deal with cyber observable. The Cybox language is defined within a set of specification documents as follows: cybox Language Core Specification specifies the purpose, approach, conventions and usage of the cybox language as well as the detailed language data models for the language core and set of common types. Cybox Language defined objects Specification restates some language basics from the Cybox Language Core Specification as well as specifies the detailed language data models for the official set of Cybox defined objects.
- TAXII [12]
  The researchers stated that the present cyber threat information sharing is either a time-consuming, manually processed or automation effort have limited scope and are tied to a particular cyber threat information sharing community or technology. As the value of cyber threat information sharing has increased, the number and kinds of cyber threat information sharing communities has also grown.The goals of TAXII (The Trusted Automated exchange of Indicator Information) are to enable timely and secure sharing of threat information both within and between cyber defender of multiple organizations. Leveraging consensus standards to enable the sharing of actionable indicators and more across organization and product/service boundaries extend indicator sharing to enable robust, secure, high-volume exchanges of significantly more expressive sets of cyber threat information. It supports a broad range of use cases and practices common to cyber threat information

sharing communities. Leverage must be given to existing mature standards, where appropriate eventual adoption by one or more international standards organizations is required. In order to enable the automated sharing of a wide range of threat data beyond simple threat information, atomic indicators are also employed. Thus it requires fewer analyst-eyes needed to screen and enable cross organization analyst collaboration on the truly challenging issues. Standardized threat data formats and sharing implementations will achieve these goals. As noted in the *Roadmap to Intelligence-driven Information Security*, Automated data-exchange systems need to be established to remove the dependency on specific bodies. In addition, "harmonized standards for representing attack information in machine-readable format, delivering it securely, and consuming it in real time would help to enable automation." Additionally, as noted in *Breaking Down Barriers to Collaboration in the Fight Against Advanced Threats* [12]: "There is a Lack of inter-operable standards to describe advanced threats - The security industry has yet to align behind a set of uniform, machine-readable standards to capture, integrate and communicate threat information".

– STIX [10]
  STIX (Structured Threat Information Expression) provides a single architecture tying together a diverse set of cyber threat information including: cyber observables indicators, incidents adversary tactics, techniques, and procedures. It exploits targets courses of action cyber attack campaigns by cyber threat actors. To enable such an aggregate solution to be practical for any single use case STIX is both flexible and extensible. The core use cases targeted by STIX analyzing cyber threats a cyber threat analyst reviews structured and unstructured information regarding cyber threat activity from a variety of manual or automated input sources. By specifying indicator patterns for cyber threats, a cyber threat analyst specifies measurable patterns representing the observable characteristics of specific cyber threats along with their threat context and relevant metadata for interpreting, handling, and applying the pattern and its matching results. For managing cyber threat response activities, cyber decision makers and cyber operations personnel work together to prevent or detect cyber threat activity and to investigate and respond to any detected incidences of such activity. Cyber threat detection operations personnel apply mechanisms to monitor and assess cyber operations in order to detect the occurrence of specific cyber threats whether (1)in the past through examples, (2) currently ongoing through dynamic situational awareness, or (3) through predictive interpretation of leading indicators. A core requirement for maturing effective cyber threat intelligence and cyber threat information sharing is the availability of an open-standardized structured representation the cyber threat information.
– CYBEX [11]
  CYBEX (Cyber Security Information Exchange) researchers argued that previous research did not consider any specific type of information to share and the range of information sharing amount varies between 0 to 1.The re-

searchers have adopted a 2-stage Bayesian game considering the information as the number of bugs and by using backward induction from previously shared information of bugs they have derived the optimal investment quantity and a number of bugs to share with the other firms participating in information sharing. A dynamic cost of participation mechanism is necessary to let both CYBEX and information sharing firms coexist in a sharing market such that firms can take the advantage of information sharing and CYBEX can manage the participation as well as CTI(Cyber-Threat Intelligence) sharing. The researchers assumed that every participating firm in CYBEX shares a constant amount of CTI. However, realistically some rational firms may share less whereas some firms share more based on their best interest. CYBEX introduces two different incentive parameters for two different sharing levels that researchers called as high sharing strategy and low sharing strategy. Differentiated sharing gain when a firm is not participating in the sharing framework, then researchers can infer that the firm is not interested in sharing its CTIs with others and decides to tackle cyber security issues solely. Low sharing strategy is only favorable in two scenarios, (1) when the firms do not get the value of their truthfully shared cyber-threat information, and (2) when firms decide not to share all of their information and free-ride on others' CTIs, so that the cost of information sharing is reduced.

– MISP [13]
  In MISP (Malware Information Sharing Program), a user can describe an event with multiple attributes while providing as much information as possible, or one can only put a minimum of information for an event. The pull mechanism allows a MISP instance to discover available events on a connected instance and download any new or modified events. It automatically goes through each of the event IDs that are eligible, converting them to MISP's JSON format and POST them to the event creation API of the remote end. The event already exists and can be edited, while the remote side will match the event by UUID to a local event and return the URL that could to be used to update the event. It shows an index, description, events, attributes, correlations found, proposals, active users, organizations, discussion threads, discussion posts, number of instances to ease the usage of MISP. The CIRCL (Computer Incident Response Center Luxembourg) provides a feed of events that can be easily shared; such as OSINT events and attributes that are classified as unclassified information that can be distributed without any restrictions.

– Traffic Light Protocol [19]
  The TLP (Traffic Light Protocol) was created by UK (United Kingdom) in early 2000 to control the flow of information withing or outside the organization. The protocol mark the information with 4 colors red, amber, green and white. Information marked as red should not be shared by the recipient of the information. Information marked as amber can be shared by the recipient with the member of its own organization. Information marked as green

can be shared with affiliated organizations. Information marked as white can be publicly shared.

4.1 Automated Information Sharing

The multinational alliance for collaborative cyber situational awareness's for information sharing framework was formed to describe how sensitive information should be shared across organizations and governments. Content consumers can generate security reports after automatically assessing devices based on automated security content, and security information can be exchanged automatically. The TAXII [12] information exchanged is represented in the XML-based structured threat information expression language. The US DISA(Defense Information Systems Agency) fields XCCDF (xtensible Configuration Checklist Description Format) [14] with CPE (Common Platform Enumeration) and OVAL (Open Vulnerability Assessment Language) [17] to publish security technical I implementation guides, which are the configuration standards for the US Department of defense IA (Information Assurance Division) and IA-enabled devices and systems. INCH WG (Extended Incident Handling Working Group) goal is to define a data format, information model, and messaging format to exchange security incident information used by CSIRTs. ICSG (Industry Connections Security Group) work is to efficiently describe and share threat information, which is studied in ICSG's MMDEF (Malware Meta Data Exchange Program), Malware, and Stop eCrime WGs [16]. MMDEF WG. The MMDEF WG's goal is to standardize and enrich captured and shared malware information. The RESTful architecture style can be used for resource discovery and exchange of information represented by various data models. Even though it's flexible, the resource-oriented architecture is still a pull model in which threat information can't be distributed only to interested parties. For some countries with different privacy laws for personally identifiable information, information collection and sharing methods will need to be designed carefully.

4.2 Crossing the Boundaries

Classified information such as undersigned unclassified data and personally identifiable information may be faced when an expert is checking cyber threat data. The data from the intelligence are mostly written papers that discuss about the TTPs, actors, types of systems and data being targeted, and other threat related knowledge that are worthy of importance for a company. In order to describe the significance of data sharing activities, companies must narrate the extent of their data sharing activities by describing the kinds of data available for exchange, the environment under which exchange of this data is allowed, and the bodies with whom the data could be exchanged. A company may set regulations that could narrow down the sharing of highly classified data with infiltrated groups, which could permit the exchange of medium classified data with particular reliable users, and also that allow data of less classified information to be highlighted in the range of packed sharing group, and also that permit the unhindered sharing

of non-classified data in national data exchanging platforms. The secrecy effect level as described in NIST SP 800-122 [18] and 800-150 [19] is a productive tool for getting the classified data to be secured.

4.3 Control Filtering Mechanism between CERTs

When a company signs a pact for data exchanging policy, earlier it must get the approval from the administrative team, who should must have a specific system for checking the data sharing activities and for handling the tools essential for the company's data exchanging assist. NIST SP 800-150 [19] *GUIDE TO CYBER THREAT INFORMATION SHARING* discusses the control filtering process for the judicial team and the one with the authorization to come into contact with the privacy officers and other significant stakeholders who play their part in the collection, ingestion, storage, analysis, publication, or protection of threat data. Majority of companies can get threat data by the channels of email lists, text alerts, and web portals in the absence of autonomous mechanism related to data sharing. Though the material obtained by these production ways could also be handed manually. A creator of exchanged threat data could make his mind what device could be used in case any metadata is assisting exchanged data, what data patterns could be used, how the classified data could be handled, and in which way data exchanging regulations can be upgraded with the passage of time. A measured non-sensitive data is the one for which the laws, regulations and government policy need to have ways of protection or disintegrating controls, that are taking out the data which are sensitive.

4.4 Limitations and Problems

Innovative researches in the field of technology play a significant part for CERTs, and the method is also important by which specifically nation-wide CERTs have to work and the way they react with other bodies. International cyber security rules can be viewed as a method of lessening the threats of cyber security events, and the progress of event responses as well. The Internet is a huge system and it shows that CERTs must establish contacts to perform their task of incident reporting. The first ever CERT, CERT/CC was made to undergo coordinating role, afterwards CERTs have a way of establishing contact that is also strengthened by the RFC 2350 [20], which illustrates a mini design to show the activities of a CERT. Different helpers are present to discuss how to set up a CERT e.g. from ENISA or the NIST publication Security Incident Handling Guide, where the communication area is also discussed briefly. The complete new method is that the part of CERTs, especially national CERTs is limited in a narrow connecting manner. An eye catching dimension of CERTs is that not only the national CERTs might be taking into consideration but all CERTs are held responsible for important security incidents and digital service providers. CERTs need to maintain contact to fulfill their compulsory supporting process. Helping this communication should be according to the political arena. There are several hindering elements in this regard as well. The new part that CERTs assume in

national and international cyber security strategies puts forward tough questions in regard to the support of national security interests versus the interest of global cyber security. The handling of this situation cannot be completely overcome by technical support measures alone, it also needs a strategic approach to encounter it as well.

5 Conclusion

The conclusion drawn from the above survey is that there are various information exchange platforms already existing among different CERTs. But the exchange of data is dependent upon the significance of the data and the importance of the strategic data for the receivers. For a collective defense mechanism, political obstacles should be removed so that nationwide CERTs could cooperate with each other in a productive manner in the wake of political conflicts. The new processes reflect that categorizing the data independently will enhance the performance of present automatic information exchange process among CERTs. This would make the exchange of data easier which would lessen the risk of threat exploiting and vulnerability and would increase the defense power of information sharing CERTs collectively.

References

1. Ehrenfeld, J. M. (2017). Wannacry, cybersecurity and health information technology: A time to act. Journal of medical systems, 41(7), 104.
2. Caldwell, T. (2018). Plugging IT/OT vulnerabilities–part 1. Network Security, 2018(8), 9-14.
3. Skopik, F., Settanni, G., and Fiedler, R. (2016). A problem shared is a problem halved: A survey on the dimensions of collective cyber defense through security information sharing. Computers and Security, 60, 154-176.
4. Franke, U., and Brynielsson, J. (2014). Cyber situational awareness–a systematic review of the literature. Computers and Security, 46, 18-31.
5. Tounsi, W., and Rais, H. (2017). A survey on technical threat intelligence in the age of sophisticated cyber attacks. Computers and security.
6. Bartnes, M., Moe, N. B., and Heegaard, P. E. (2016). The future of information security incident management training: A case study of electrical power companies. Computers and Security, 61, 32-45.
7. Jesson, J., Matheson, L., and Lacey, F. M. (2011). Doing your literature review: Traditional and systematic techniques. Sage.
8. Barnum, S., Martin, R., Worrell, B., and Kirillov, I. (2012). The CybOX Language Specification. draft, The MITRE Corporation.
9. Kitchenham, B., Brereton, P., Li, Z., Budgen, D., and Burn, A. (2011, April). Repeatability of systematic literature reviews. In Evaluation and Assessment in Software Engineering (EASE 2011), 15th Annual Conference on (pp. 46-55). IET.
10. Iannacone, M., Bohn, S., Nakamura, G., Gerth, J., Huffer, K., Bridges, R., ... and Goodall, J. (2015, April). Developing an ontology for cyber security knowledge graphs. In Proceedings of the 10th Annual Cyber and Information Security Research Conference (p. 12). ACM.

11. Tosh, D., Sengupta, S., Kamhoua, C. A., and Kwiat, K. A. (2016). Establishing evolutionary game models for cyber security information exchange (cybex). Journal of Computer and System Sciences.
12. Connolly, Julie, Mark Davidson, and Charles Schmidt. "The trusted automated exchange of indicator information (taxii)." The MITRE Corporation (2014). http://www.standardscoordination.org/sites/default/files/docs/STIX_Whitepaper_v1.1.pdf
13. Wagner, C., Dulaunoy, A., Wagener, G., and Iklody, A. (2016, October). Misp: The design and implementation of a collaborative threat intelligence sharing platform. In Proceedings of the 2016 ACM on Workshop on Information Sharing and Collaborative Security (pp. 49-56). ACM.
14. Waltermire, D., Schmidt, C., Scarfone, K., and Ziring, N. (2011). Specification for the Extensible Configuration Checklist Description Format (XCCDF) Version 1.2. National Institute of Standards and Technology, Gaithersburg, MD, 20899-893.
15. Azodi, A., Jaeger, D., Cheng, F., and Meinel, C. (2013, December). Pushing the limits in event normalisation to improve attack detection in IDS/SIEM systems. In Advanced Cloud and Big Data (CBD), 2013 International Conference on (pp. 69-76). IEEE.
16. Kampanakis, P. (2014). Security automation and threat information-sharing options. IEEE Security and Privacy, 12(5), 42-51.
17. Wu, B., and Wang, A. J. A. (2011, March). EVMAT: an OVAL and NVD based enterprise vulnerability modeling and assessment tool. In Proceedings of the 49th Annual Southeast Regional Conference (pp. 115-120). ACM.
18. McCallister, E., Grance, T., and Scarfone, K. A. (2010). Guide to protecting the confidentiality of Personally Identifiable Information (PII)(No. NIST SP 800-122). Gaithersburg, MD: National Institute of Standards and Technology.
19. Johnson, C., Badger, L., Waltermire, D., Snyder, J., and Skorupka, C. (2016). Guide to cyber threat information sharing. NIST special publication, 800, 150.
20. Brownlee, N., and Guttman, E. RFC 2350: Expectations for Computer Security Incident Response, 1998. Online: http://www. ietf. org/rfc/rfc2350. txt.