

Relation of Data Visualization Techniques with the phases of Cybersecurity Incidents Response process

Ivo Ricardo Dias Rosa
 Invited Assistant Professor at ISTECS – ivo.rosa@my.istec.pt

Abstract: *Globally for nations and organizations (also due to the impositions and response needs imposed by security and privacy regulations) it is increasingly relevant to strengthen the ability of organizations to anticipate and detect possible security events in a timely manner; even when it is not possible to contain the threat it is necessary that incident response teams are able to tell and explain what happened.*

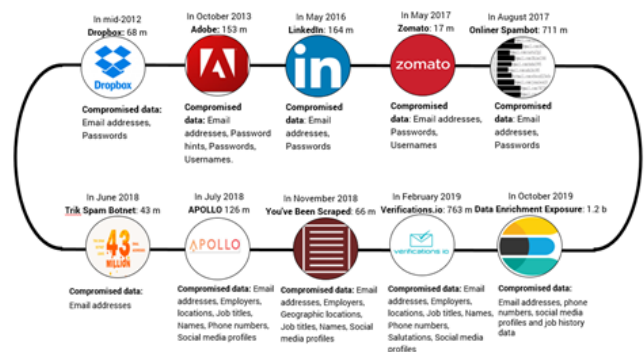
This article provides a review was made concerning Cybersecurity, in particular the importance and relevance of the security incident response process, which may have operational and reputational impacts, and the identification and mapping of the purposes of applying data visualization techniques to give meaning or explain the typical phases of the security incident response process.

Keywords: *Cybersecurity, cybersecurity incidents, incident response process, data visualization*

I. Introduction

Nowadays it is very common to say that data is the new gold or that it are the crown jewels that organizations want to defend and protect from the point of view of information security and consequently of data protection [1]. We live in the era of digital and knowledge societies, however we are facing a new problem, is that every day the number of data grows exponentially and sometimes without proper control, however this lack of control can be reflected in financial and reputational impacts for organizations. It is increasingly common to see

in the news the occurrence of data leaks or companies that have been the target of cyber incidents and that the personal data of their customers or employees were unduly exposed, and this situation impacts the image and reputation of organizations because it can affect the relationship of trust between customers and organizations that provide services and/or products. Figure 1 shows a compilation of some of the major data leaks that have occurred in the last 10 years involving large volumes and variety of data that has been compromised in many different digital products or services. This is an increasingly relevant theme for both nations and organizations, both for operational



and legal reasons, and is therefore part of the WEF - World Economic Forum agenda.

Picture 1 - Major leaks in volume and variety of data that have occurred in the last 10 years. Source: compilation created by the author.

II. Cybersecurity and Data Protection

In general, the data leaks resulted from lack of adequate cybersecurity measures to protect the data. Cybercrime and cyberthreats have been increasing year after year and there is

no evidence or trend for decrease in the near future, so it is essential for organizations to increase their ability to react to cybersecurity incidents. Security incidents, depending on their nature and origin, can affect the availability of information system resources and critical infrastructures, leakage of commercially sensitive or advantageous information, personal data and financial, image and reputational impacts.

Cybersecurity is a term that is applicable to all activities that may occur in a new and recent space of action called Cyberspace [2]. Diakun [3] proposes the following definition for Cybersecurity:

“Cybersecurity is the organization and collection of resources, processes, and structures used to protect cyberspace and cyberspace-enabled systems from occurrences that misalign de jure from de fact property rights.” [3]

Cybersecurity is part of the general concept of Information Security which, even in the international community through the ISO27001 [4] reference, is defined as being based on three main pillars that are Technologies, People and Processes and identifies a set of key controls in order to ensure information security. More recently, the international standard ISO27701 [5] was created to expand the information security controls of IS27001, identifying a set of controls for privacy, more specifically, what entities must do to ensure the correct collection, handling and processing of personal data in order to prevent their unauthorized use or disclosure.

Cybersecurity concerns have become an increasingly global concern, the remaining world countries are adopting laws similar to the GDPR (General Data Protection Regulation) so that privacy is guaranteed, recently the WEF - World Economic Forum [6][7] identified Cybersecurity threats, which includes technical issues related to privacy and data protection, as one of the 10 most likely risks.

III. Information Security Incident Response

Regarding security incident management and according to international standards [4]

identifies two major concepts, distinct but related: security event and security incident.

An information security event is understood as the identified occurrence in a system, service, network or resource that indicates a possible failure in the application of the information security policy, failure of/in security controls or a previously unknown situation that may be relevant to information security. On the other hand, an information security incident corresponds to a failure or breach of information security policies, procedures or rules, and/or an unexpected and unwanted event or series of information security events/vulnerabilities that compromise or may compromise an organization's business operations and information security.

The NIST - National Institute of Standards and Technology and the SANS - Institute are two reference entities with duly recognized credibility within the Cybersecurity industry, these identities and with respect to security incident response identify a minimum set of steps that must be ensured [8].

Incident Response Steps	
NIST	SANS
1) Preparation	1) Preparation
2) Detection and Analysis	2) Identification
3) Containment, Eradication, & Recovery	3) Containment
4) Post-Incident Activity	4) Eradication
	5) Recovery
	6) Lessons Learned

Picture 2 - Comparison of NIST and SANS incident response models and steps.

In the picture 2 shows the different stages identified by each of the institutions, but we can consider that the model and sequence is similar, but with a slightly different nomenclature. Using as reference the NIST reference, 4 stage model, we can conclude that there is equivalence with the 6 stage model identified by SANS [8].

In an attempt to standardize the language used to characterize security incidents the ENISA - European Union Agency for Cybersecurity defined a categorized and taxonomic classification of incidents [9].

IV. Data visualization and its relationship with security incident response processes

The applications of information visualization techniques can and are a very useful tool to help provide answers that would be difficult to analyze and detect. It is also important to mention that in the context of event and security incident management there is a great concern in anticipating the detection and consequently the response to a particular problem, due to the importance of these two variables make information visualization techniques more advantageous when compared to other approaches in this topic [10].

Data visualization solutions can help to more easily identify graphically detectable patterns facilitating the extraction of knowledge [10][11], because when compared with traditional event correlation solutions these involve and require more manual work, in particular with the goal of filtering the information to the really important and relevant events maintaining the coherence and integrity of a given sequence of events[10].

Tuffe [12] in his book with the title *The Visual Display of Quantitative Information* mentions that graphs on data can do much more than simply be substitutes for small statistical tables. At their best, graphs are tools for understanding quantitative information. Often the most effective way to describe, explore, and summarize a set of numbers-even a set with many numbers-is to see pictures of those numbers. Additionally, of all the ways to analyze and communicate statistical information, well-made graphs on data are usually both the simplest and the most powerful.

This definition about the concepts of information visualization is very applicable in the analysis of security events, because in many cases the simple graphical representation of figures with a certain logical arrangement can be much more enlightening or guiding about the origin of a certain problem than the manual or aggregated visualization of data in statistical measures.

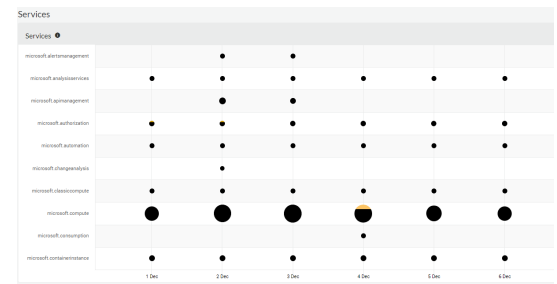
Visualization of technical-scientific data, such as data related to information security, can serve various purposes and goals such as [11]:

- **Exploratory analysis** - This objective is used when we have a significant set of data, but at first glance we can't extract hypotheses and scenarios about it, so visualization techniques can be useful in identifying patterns or in the rational

inverse deviations from common patterns.

As a practical example of this purpose, we have the Trend View and Map View approaches, which may not identify a specific scenario or threat, but by their characteristics help to identify patterns or baselines.

Trending View techniques are widely applied to analyze the most common services or protocols over time, with the size of the representations corresponding to the level of volume identified. With this approach it will be possible to identify services that in some cases were not even aware of their use.



Picture 3 - Example of a trend view application focused on identifying the most and least used



services

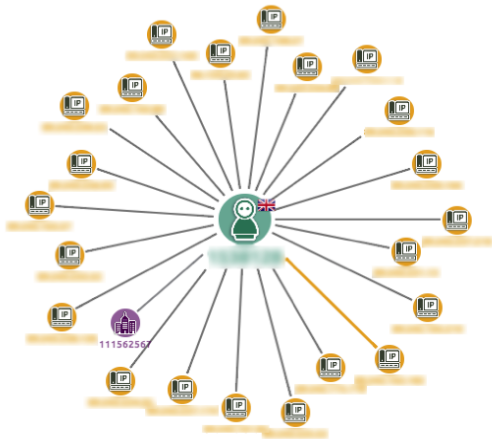
Map View techniques generally allow visualization of the origin, destination and volume of traffic communications of a computer network based on the geographical context.

Picture 4 - Example of a map view techniques.

These visualization techniques do not clearly identify a cybersecurity problem but guide experts to focus on certain more specific aspects.

- **Analysis to confirm events** - In these cases there is a defined and concrete scenario and object of study and visualization techniques are used to help validate or reject the occurrence of certain events.

Examples of this purpose may result from an in-depth analysis of cases that have aroused interest from a Trend or Map View analysis but that already correspond to several types of security incidents, as are the cases of port scanning, analysis of malicious or suspicious communications with command and control (C2C) addresses, possible dictionary attacks through brute force mechanisms or scenario of potential unauthorized access as in the example in picture 5 [13] to explain why a certain user logged on to the system in a short period of time from more than 20 locations.



Picture 5 - Graphical example of a potential unauthorized access [13].

Security event correlation systems already try to identify this type of scenario, however there are some techniques to try to hide or difficult its interpretation inside so many events that these platforms process and are only detectable through visualization techniques.

- **Presentation/dashboard** - This is a technique widely used for data demonstration and hypothesis scenarios that may correspond to suspicious behaviors based on a set of base indicators (usually aggregate and show several cybersecurity indicators). This presentation of data should be chosen and adjusted so that it can be easily/quickly read and interpreted.

These purposes of information visualization techniques and applying with different techniques, are also directly mappable with phases 2 - Detection and Analysis, 3 -Containment, Eradication, & Recovery, 4 - Post-Incident Activity when compared to the NIST 4-step model of Cybersecurity incident response (picture 2).

V. Future Work

An opportunity for future work will be to systematize and evaluate in depth the type and technique of data visualization that best applies or best describes and fits the various types of information security incidents, which are already properly typified through a taxonomic classification used internationally to standardize responses to cyber incidents.

V. Conclusion

As we have seen information visualization techniques are extremely useful for explaining, and in some cases unraveling, certain

security events, these techniques fit in with the typical steps of the incident response process. However, there are types of visualization techniques that are best suited for certain phases of the incident response process, and this may correspond in better levels of efficiency and effectiveness in detecting certain threats.

A future approach to this topic is to evaluate the types of data visualization techniques and depending on the type of security data variables under analysis which best fit them to use according to taxonomic and specific classification for security incidents.

VI. References

1. DADOS - A Nova Jóia da Coroa. September 04, 2017. Available online: <https://dataprivacy-on.com/comunicacao/2017/11/9/dados-a-nova-joia-da-coroa>. Accessed on 25-02-2022.
2. Bravo, R. (2020). Segurança da informação e Cibersegurança: aspetos práticos e legislação. Segurança Da Informação e Cibersegurança: Aspetos Práticos e Legislação.
3. Diakun-Thibault, Nadia. (2014). Defining Cybersecurity. Technology Innovation Management Review. 2014.
4. ISO/IEC 27001 - INFORMATION SECURITY MANAGEMEN. Available online: <https://www.iso.org/isoiec-27001-information-security.html>. Accessed on 25-02-2022
5. ISO/IEC 27701:2019 Security techniques — Extension to ISO/IEC 27001 and ISO/IEC 27002 for privacy information management — Requirements and guidelines. Available online: <https://www.iso.org/standard/71670.html>. Accessed on 25-02-2022
6. World Economic Forum. The Global Risks Report 2021 16th Edition - INSIGHT REPORT. In partnership with Marsh McLennan, SK Group and Zurich Insurance Group published by the World Economic Forum. 2021. Available online: http://www3.weforum.org/docs/WEF_The_Global_Risks_Report_2021.pdf. Accessed on 12-03-2022
7. World Economic Forum. The Global Risks Report 2022 17th Edition - INSIGHT REPORT. In partnership with Marsh McLennan, SK Group and Zurich Insurance Group published by the World Economic Forum. 2022. Available online: http://www3.weforum.org/docs/WEF_The_Global_Risks_Report_2022.pdf. Accessed on 12-03-2022
8. Incident Response Steps and Frameworks for SANS and NIST. 3 de Janeiro de 2020. Available online: <https://cybersecurity.att.com/blogs/security-essentials/incident-response-steps-comparison-guide>. Accessed on 10-03-2022
9. ENISA. 2018. “Reference Incident Classification Taxonomy Task Force Status and Way Forward.”
10. Marty, R. (2008). Applied Security Visualization. Addison Wesley Professional Indianapolis, Indiana, ISBN-10:0-321-51010-0.
11. Ricardo, André & Grégio, André & Pereira, Benício & Filho, Carvalho & Montes, Antonio & Santos, Rafael. (2009). Capítulo 5 Técnicas de Visualização de Dados aplicadas à Segurança da Informação. Available online: https://www.researchgate.net/publication/268397430_Capitulo_5_Tecnicas_de_Visualizacao_de_Dados_aplicadas_a_Seguranca_da_Informacao. Accessed on 10-03-2022
12. Tufte, Edward R.. The Visual Display of Quantitative Information. Graphic Press, 2nd edition, 2001.
13. Data visualization techniques for cyber security analysts — Guest Blog by Cambridge Intelligence. Department for International Trade The Netherlands. February 13, 2020. Available online: <https://medium.com/cfs2020/data-visualization-techniques-for-cyber-security-analysts-guest-blog-by-cambridge-intelligence-1b3d8ddbfc56>. Accessed on 12-03-2022.