Study on Dual Data Structure in Enterprise Information Security Architecture

Mikio Suzuki
President of eVan TEC, Ltd.
Tokyo, Japan
e-mail: mikioszk@evan-tec.com

Fumihiro Kubota
eVan TEC, Ltd.
Tokyo, Japan
e-mail: fkubota@evan-tec.com

***Abstract*— Security Operation Center is known as a centralized team within the organization working against critical cyber threat by mainly analyzing logs. This paper points out the duality of information on Security Operation Center and proposes several issues according to its new security scheme and also raised awareness to protect confidential business information and employees' rights of privacy.**

Keywords—Security Operation Center; logs; Dual Data Structure; Information Security Policy.

I. INTRODUCTION

An increase in sophisticated cyber attacks seems to be all over the world. The essential cause of this fact is that the Internet is open and free. Although this aspect brings great advantages in our highly informed society, it causes the threat of cyber attacks. Security Operation Center (SOC) specializes in investigating cyber attacks by analyzing logs [1]. Security Information Event Management (SIEM) is a related technology for analyzing logs automatically [2]. In other words, analyzing the logs is essential to make counter strategies against cyber attacks. However, the results of analyzing of logs include not only cyber attack data, but also confidential business intelligence and private information. This paper points out the recognition of dual data structure in data flow of SOC and the necessity of developing an information security policy on SOC.

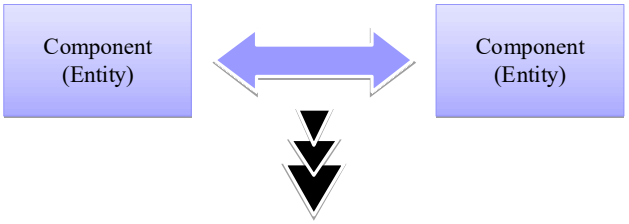
II. DATA STRUCTURE

A. Dual data structure on the information security

To study the data flow in an enterprise computer system, we consider the Enterprise Architecture (EA), which is a methodology or a guideline for entities in an enterprise to normalize information and optimize business strategies [3]. Then, we study the data flow among the entities which compose the EA. As depicted in Fig. 1, data flow between entities is an objective of our study. Business process causes data flows between entities. At the same time, the result of observing or monitoring the data by SOC includes business data flow as well as intelligence data or private data. In this study, we refer to this fact as "dual data structure".

Let us take an example to understand the duality of data mentioned above. One might easily recognize that most of the log data might be business relating data. However, very small combinations of log data, very difficult to find, might possibly be related to cyber attacks, although each log does not indicate the illegal action. This means the log data has another aspect of information relating to business intelligence as well as cyber attack information.

Data confidentiality should be classified into three ranks (High, Middle, and Low) in designing of an information security policy [4]. It seems that the low rank data takes a low risk; however, it might be reclassified into a high risk data after being analyzed by SOC. This implies low rank data cannot be assumed as low risk data without analyzing.



"Dual data structure in their information is shown by analyzing the information between Entities."

Figure 1. Dual Data Structurer generated by two entities

B. Several effects on the information security caused by Dual Data Structure

Dual Data Structure changes several aspects in information security architecture as follows.

1) Dual Data Structure in SOC changes Reference Monitor Model (RM)

In designing SOC and the related RM concept [5], technical qualification needs to be reconsidered as an essential security model. In Fig. 2, the log database is produced by each monitoring log data and, after analyzing the log database, new confidential information will emerge. It indicates that security requirements have to focus on the issue of dual data structure when building SOC scheme as well.

 ISBN: 978-1-61208-493-0

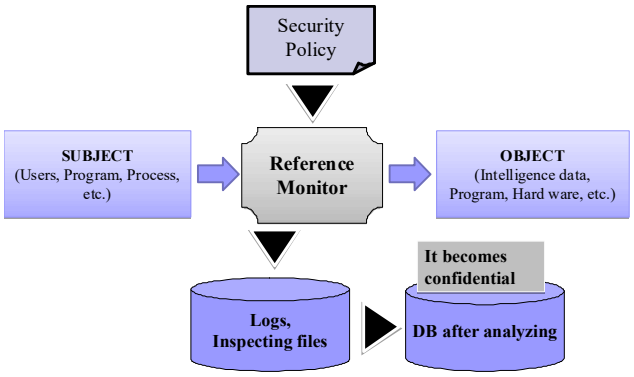


Figure 2. Information Reference Model [4].

2) Dual Data Structure in SOC relating privacy

The basic structure of log data contains the user information, such as, ID information, or name, time, subject, object and behavior as depicted in Fig. 3. This issue should be under the privacy impact assessment [5] and Tokenization or Anonymous is also under the consideration to be introduced into the log data structure.

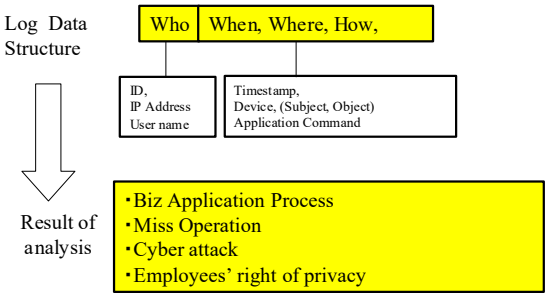


Figure 3. Dual Data Strucuture in SOC data.

C. *Understanding Dual Data Structure*

To understand the essential meaning of Dual Data Structure, we suppose the concept of "Unknown unknowns" [6]. Critical targets of SOC are "Unknowns". They are almost impossible to identify. In other words, under the condition of "unknown unknowns", SOC is working on daily missions to analyze unknowns of cyber attacks.

Professionals of Information Security in SOC should transfer the status "Unknown unknowns" to the status "Unknown known". This means that they present the actual attack evidence from the results of SIEM by their experience or the outside information, and transfer findings to managerial persons of the enterprise. In case of both outside or inside SOC analyzing log data which belongs to an enterprise, a professional has the responsibility to analyze the results.

D. *The issue of security policy relating to SOC*

We have studied several aspects of data relating to SOC in terms of RM, privacy rights. Further discussions about information security policy related to duality are as follows.

1) Data handling policy of DB based on log data

Those data should be kept in highly confidential status and integrity of the data should be kept safe.

2) Review of Privacy impact assessment

Privacy impact analysis should be studied in design stage of SOC as well as operational stage.

3) Outsourcing of SOC work

Review the risk of outsourcing of SOC taking into account the duality of SOC data. We would like to suggest that outsourcing of SOC work had better be avoided.

III. CONCLUSION

This paper points out a duality in EA data. From the comprehensive thoughts, it is concluded that recognition of dual data structure and necessity of developing information security policy regarding SOC must be argued.

This idea contribution raised the importance to consider the dual aspect in information security. The followings are expected for further study.

1) Information security policy of SOC

To the best knowledge of the authors, there is no security policy relating to SOC which is taking duality into account.

2) Advanced analyzing logs in duality

Maching learning is the new trend in analyzing logs. Duality in the result of analyzing logs must be governed by the above information security policy.

REFERENCES

[1] Barbara A Nadel, "Building security: handbook for architectural planning and design", McGraw-Hill, 2004, p.220.

[2] David R. Miller, Shon Harris, Alan Harper, Stephen VanDyke, and Chris Blask "Security information and event management implementation" McGraw-Hill Education; 2010

[3] Col Perks, and Tony Beberidge, "Guide to enterprise IT architecture" Springer-Verlag New Yourk, Inc., 2003.

[4] US Department of defense, "Trusted computer system evauation criteria (TCSEC)", DoD 5200.28-STD, December 26, 1985.

[5] CISSP® Common body of knowledge review, "Security architecture & design domain" Version 5.10, P.65.

[6] David Wright and Paul de Hert, "Privacy Impact Assessment (Law, Governance and Technology Series)", Springer; 2012 edition (July 22, 2012).

[7] Charles Saatchi, "Unknown unknowns", Booth-Clibborn; First Edition, 2015.

 ISBN: 978-1-61208-493-0