Analysis of correlation rules in Security information and event management systems

Sievierinov Oleksandr[1]

[1]Kharkiv National University of Radio Electronics, 14 Nauky
Ave, Kharkiv UA-61166, Ukraine,
oleksandr.sievierinov@nure.ua

Ovcharenko Margaret[2]

[2]Kharkiv National University of Radio Electronics, 14 Nauky
Ave, Kharkiv UA-61166, Ukraine,
marharyta.ovcharenko@nure.

Abstract*. This article discusses the main components of information security systems and information security incident management. The methods of non-signature, as well as signature analysis of rules and decision-making that are used in such systems are considered. The analysis of existing methods of correlation rules. The main types of each method have been identified.*

Keywords: *correlation, information security management, signature method, non-signature method, incident security, event security, SIEM.*

I. Introduction

With an ever increasing amounts of information being processed in various information and communication systems in the first place come the availability of the tool with which it was possible to analyze events in real time. Because of the vast amounts of data to be processed is difficult to focus on the important aspects of information security company [6]. One solution is to use a Security information and event management system (SIEM) [1]. Base SIEM system is that data security incidents collected from various sources and the result of their treatment is given in a single report, which facilitates handling the incident and the decision to reduce the residual risk and losses [8]. The system SIEM consists of two segments - Segment Information Security Management (SIM), which is responsible for analyzing data to improve system efficiency and segment management of security incidents (SEM), with total media chooses the one with which incidents can be detected immediately [2].

Today SIEM system is one of the most common tools of analysis of information security incidents, so essential to clearly and correctly determine the rules by which your system will determine which event is incident and which - the result of the normal operation of the system, process or user. This article will discuss and analyze the main types of correlation method in SIEM systems and identify the basic methods that may be optimal for use in the design phase of SIEM systems.

II. Correlation of events in SIEM systems

An information security event is an identified case of system or network status that indicates a potential breach of information security policy or security failure, or a previously unknown situation that may be material to the security policy.

An information security incident is a single event or a series of unwanted and unanticipated information security events that could result in business information being compromised and information security threats.

SIEM is a software solution that collects and analyzes data from many sources. The SIEM system collects data from network devices, servers, network event logs, antivirus software, firewalls, and other information security incident management systems, such as Data Leak Prevention (DLP) and Intrusion Detection System/ Intrusion Prevention System (IDS/IPS) [3]. SIEM stores, normalizes, applies to data that will be obtained from sources in previous stages, analytics that help identify events and information security incidents.

In practice, the circuit is implemented using the appropriate components[4]:

1. Agents (collecting data from various sources);
2. Collector servers (accumulation of information received from agents);
3. Database server (information storage);
4. Correlation Server (information analysis).

Correlation methods are used to more effectively process data and identify events in the information and telecommunication system as incidents of information security.

The correlation rules in SIEM systems are created using the following algorithm:

1. The target for which correlation will be performed is selected.
2. Information security events and conditions are selected.
3. The sequence of events is adjusted.
4. Specifies the time interval during which the event should occur.
5. A new rule is established.

There are two types of correlation methods in SIEM. The first type includes methods called signatures. These methods can be adjusted by the system user. The second type includes non-signatures, that is, those that independently detect security incidents and ensure their fixation and processing, which is used in most SIEMs.

There are many non-signature analysis methods. Usually the following methods are used in practice [6]:

1. Statistical - a method that essentially uses measurements of two or more variables and defines a statistical relationship between them.
2. A rule-based or template-based method is a method used to determine the cause-and-effect relationship of a rule that has been previously defined by administrators.
3. Graph-based method - correlation is performed by finding the dependence between the network components and plotting it as a graph. If component dependency was found, then the graph is used to find the events that caused this information security incident.
4. Neural Network Based Method - Correlation occurs by teaching neural networks to distinguish between information

security events and incidents and to perform certain actions that should minimize or even eliminate the risks to the system.

5. Codebook-based Method - Correlation occurs using vectors that fit from a predefined event matrix.

Despite the variety of non-signature methods, there is no way to overcome their major drawback. As non-signature correlation methods are developed and implemented by SIEM system vendors, the end-user is unable to make changes to their implementation, leading to a greater shift away from non-signature methods toward signature ones.

Signature methods are more flexible and effective for use in modern software implementations than non-signature methods [4]. The following notation is introduced to explain the operation of the signature methods:

1. P - problem, incident.
2. C - cause.
3. S - symptom.

An outline diagram of incident detection is shown in Fig. 1.

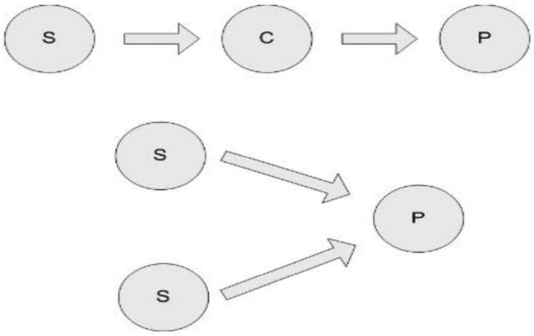

Figure 1. Diagram of information security incident detection

Signature methods are based on determining the criticality of an incident. There are two methods of determining it - quantitative and probabilistic. The quantitative method takes into account the number of symptom-cause-problem relationships. In the probabilistic method, each link is exposed to the likelihood of this symptom. Based on the sum of the corresponding probabilities, the criticality of the incident is exhibited [6].

The idea behind the signature method is to find matches with predefined correlation rules, each designed to identify and counteract a particular information security event, but several different rules can be triggered for each information security incident.

The rule includes a trigger that has a condition, a counter, and scenarios that describe the system's response to an information security incident.

The counter is used to calculate matches according to the same correlation rule. The trigger is waiting for one of the conditions to be enforced to enforce one of the predefined rules. And after a certain period of time (resetting the session), the trigger returns to zero until the next condition.

III. Conclusion

Thus, the analysis identified the main methods that can be used to correlate rules in SIEM systems, which in turn allow for a more accurate and effective analysis and counteraction to information security incidents that occur in information and telecommunication systems and can lead to significant system damage.

It has also been identified that the use of SIEM systems results in reduced response time to information security incidents and consequently lowers the economic costs that an individual business or government may incur. All that has been said, leads to the fact that the use of SIEM systems with signature methods of defining correlation rules and responding to them, increases the controllability of information security systems.

References

[1] H. Karlzen, «An Analysis of Security Information and Event Management Systems: The Use of SIEMs for Log Collection, Management, and Analysis.» January 2009

[2] Сєвєрінов О.В. Управління інформаційною безпекою згідно міжнародних стандартів / О.В. Сєвєрінов, В.І. Черниш, М.Є. Молчанова // Системи управління, навігації та зв'язку. – К: ДП «ЦНДІ НіУ». - 2011. – Вип. 4(20). – С. 250-253.

[3] Алексей Дрозд, Обзор SIEM-систем //SearchInform [Электронный ресурс] — Режим доступа. — URL: http://www.antimalware.ru/analytics/Technology_Analysis/Overview_SECURITY_systems_global_and_Russian_market

[4] Martovytskyi V.A. Модель мультиагентної системи збору та зберігання інформації / V.A. Martovytskyi, I.V. Ruban // Системи управління, навігації та зв'язку. Збірник наукових праць. – Полтава: ПНТУ, 2017. – Т. 6 (46). – С. 150-153.

[5] Олеся Шелестова. Корреляция SIEM. Сигнатурные методы //исследовательский центр Positive Research [Электронный ресурс] 2012. URL:http:// www.securitylab.ru/analytics/431459.php

[6] Борисов В. И., Шабуров А. С.О Применении сигнатурных методов анализа информации в SIEM-системах

[7] Ушатов В. Проблеми оперативного виявлення і реагування на інциденти інформаційної безпеки / В. Ушатов, О. Сєвєрінов // GLOBAL CYBER SECURITY FORUM. Матеріали першого міжнародного науково-практичного форуму – Х.: ХНУРЕ, 2019. – С. 104-105.

[8] Овчаренко М. Аналіз сучасних систем управління інформаційною безпекою та інцидентами безпеки / М. Овчаренко, О. Сєвєрінов // Проблеми інформатизації: Тези доповідей сьомої мужнародної науково-технічної конференції – Х.: НТУ «ХПІ», 2019 – С.102.