PREDRAG ŠKUNDRIĆ
Ibis-instruments,
Belgrade, Serbia,
E-mail: predrag@skundric.com

VANJA KORAĆ
Mathematical Institute SASA,
Belgrade, Serbia,
E-mail: vanja@mi.sanu.ac.rs

ZORAN DAVIDOVAC
Mathematical Institute SASA,
Belgrade, Serbia,
E-mail: zorandavidovac@mi.sanu.ac.rs

Received: September 17th 2020
Accepted: December 10th 2020
Original research article
007:004.056.5
659.23:004.056.5
COBISS.SR-ID 29249545
https://doi.org/10.18485/arhe_apn.2020.16.13

SECURITY OPERATION CENTRE MODULES – TECHNOLOGICAL ASPECT

ABSTRACT

The Security Operation Centre of an organisation represents a platform whose purpose is to provide detection and response services in cases of security incidents. In this paper, the technological focus is on the modules of the Security Operation Centre within an organisation, whose goal is to perform security events operations. Within the analysis of individual modules, their advantages and limitations will be presented.

KEYWORDS: SOC, SECURITY OPERATION CENTRE, INFORMATION SECURITY.

Security Operation Centre (hereinafter: SOC) is a general term used to describe an entire platform or a part of it whose purpose is to provide detection and response services in the event of security incidents. On that basis, we can distinguish four essential operations that a SOC is required to perform [1]:

- generating security events,
- collecting security events,
- storing security events,
- analysis and response in the event of detected incidents.

At this point, it is essential to denote the difference between a SOC and a CERT. CERT is a considerably wider term and, aside from the already mentioned modules and activities, it encompasses a significantly more complex spectre of activities and individuals (starting from raising consciousness, all the way to the creation of strategies linked to information security and, in final instances, the creation of national CERT drafts for laws and bylaws).

In order to ensure easier understanding of the matter at hand, we will use the term "box", which was first introduced into the terminology in *Network Intrusion Detection – An Analyst's Handbook*, a book by Stephen Northcutt and Judy Novak, which, essentially, presents individual system modules, as follows [2]:

- **E-box** for security event generators,
- **D-box** for systems used for storing and keeping events, i.e. events database,
- **R-box** for systems used for generating activities in cases when certain events are detected,
- **A-box** for systems used for analysing events,
- **C-box** for systems used for collecting and formatting events,
- **K-box** for systems used as a knowledge da-

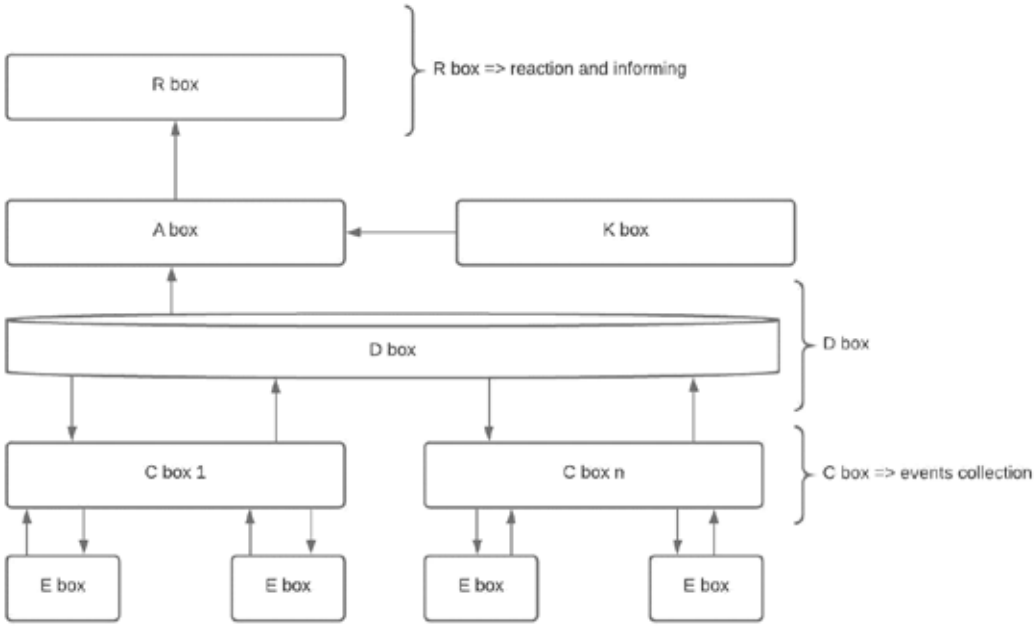

Fig. 1. General overview of the SOC modules

tabase. This system is used for managing knowledge databases for systems that are being monitored, as well as databases of detected vulnerabilities, i.e. systems for managing vulnerability tests of the computer infrastructure.

Each box describes a functional group of "modules" which perform certain operations. As an example, we can take E-boxes, which can, essentially, be any group of applications that generate system events through a standard *syslog* interface of the given operating system on which they are started. Aside from the above, network IDS or any other device or system within the infrastructure which is capable of creating system events can also be a security events generator.

As can be seen from the previous part of the paper, sometimes the term "security event" is used and sometimes simply "event", because some systems do not have a separate subcategory of security-related events, hence, the system itself has to have the option of recognising them and enabling them to be filtered so that they can be suitably categorised.

Generally speaking, all the listed modules should function on the basis of the diagram shown on Figure 1.

Aside from the obvious problem of data exchange between modules, each of the modules also has certain limitations, which will be explained in the text that follows.

E box

Boxes are in charge of generating and sending events. There are two basic types of boxes:

- event-based generators (sensors), which generate events on the basis of certain actions executed on operating systems, applications and computer network, and
- generators which generate events because of certain activities (poolers), which represent a response to an external event, such as ping, data integrity verification, or service status verification.

Sensors

The most widespread example of sensors are IDS systems, which can be organized as host based or network based. This category also includes every traffic filtering system (based on network, applications or work stations, i.e. server surroundings) which can ensure records creation, e.g. firewalls, routers with ACL-s, switches, RADIUS server etc. Finally, we can even include honeypots

and network sniffers within this category.

Every sensor is considered as a separate system, which has to meet some of the following criteria:

- continuous work,
- error resilience,
- external hazards resilience,
- minimal additional load on the system, and
- being adjustable to the system.

Poolers

Poolers represent a separate type of events generators. Their function is to generate a certain system record solely in cases when a certain state occurs, i.e. in the case of a predefined event which occurs on monitored systems. A typical example of such systems are network management systems. In this case, the pooler verifies the status of a system (e.g. via ping/SNMP tests et al.) and, if the system is unavailable (in the "down" regime), it generates a certain record which is sent to the records management system. In the context of information system security, poolers would be responsible for checking services (in order to detect DoS attacks), i.e. data integrity (most commonly in the case of web pages).

The basic limitation with poolers is their performance, because it's very difficult to configure a system so that it would verify the status of a large number of end devices, or systems, very often, without endangering the normal functioning of the system, which is a necessary condition. Aside from that, limitations occur in monitored systems as well because frequent verifications can cause processors, or network resources, to be very busy.

C and D boxes

Boxes for collecting events are used for collecting system records from different sensors and translating them into a standard format which can be comprehended by the system. Thus, a unique homogenous database of all records is made, which can be used by the system later, for further uses. As in the previous case, the main challenge is the availability and scalability of devices. Solving these challenges, however, is manageable through the use of clusters, creating high accessibility systems, similar to the implementation of the server infrastructure.

At this point, it is necessary to stress the fact that standard formatting of collected data is still in the phase of theoretical discussion and is the subject of different controversies within expert organisations linked to information security. Also, it is important to point out that the IETF (*Internet Engineering Task Force*) is working on standards linked to the standardisation of messages, or, more precisely, on the standardisation of formats of messages which are sent to the systems, or modules used for collecting events. For the time being, however, as we can see for ourselves, the situation is such that every solution manufacturer has separate record formats and manners of managing them.

D-boxes represent modules which are present in all implementations of SOC solutions and are most commonly formatted in the form of databases in which already processed system records are being stored.

Aside from classic challenges linked to database availability, integrity and confidentiality (the famous "CIA principle" = ***C****onfidentiality*, ***I****ntegrity*, ***A****vailability*), D-boxes face challenges linked to their performances because sensors can generate a large amount of messages over a short period of time (most often calculated in EPS => *Events per Second*). All these messages have to be saved, processed, and analysed in the shortest time possible in order to enable a timely response to attempts of endangering information systems, and with the goal of diminishing damage or completely removing potential risks. When it comes to the "CIA principle" (confidentiality, integrity and availability), the challenge in information security is precisely in finding a good balance between safety and functionality. If something is confidential, and the integrity of it is being protected, but it isn't available to the person who needs to have access to it, then it serves no purpose; similarly, if it is available without being secure, that is not a good situation either. Therefore, it is necessary that all three conditions are met in order to ensure security quality, but it is also necessary to find the optimal balance, without compromising the functioning of the organisation itself [3].

A and K boxes

These boxes (modules) are responsible for the analysis of events previously stored within D-boxes. On the basis of predefined algorithms,

which usually depend on the manufacturers and represent the most responsible factor in determining the quality of monitoring solutions, these two modules perform different operations on records in order to provide an adequate level of quality alarms and reports. It is precisely these mechanisms, or algorithms which are behind the alarm produced by the system, that define, and on the basis of collected system records, which particular design would be used in the SOC implementation. Since it is the SOC which deal with tracking and assessing the security of the information system that we are considering here, we favour the viewpoint which highlights the structural approach to attack analyses, as well as behaviour analyses, in accordance with predefined security policies.

It is evident that analytic processes require input data from the database containing predefined threats, polices, and also algorithms for analyses and intercorrelation of rules. This is, in fact, the essential application of K-boxes.

R boxes

Box is a generic term used to define a group of tools used in reports and incident response processes which are generated in the case of events which endanger, in a manner, the normal operation of monitored systems.

Experience tells us that the display of reports and predefined actions depends on the subjective feeling of the individuals who perform the task of tracking and responding to detected problems, and they include graphic displays utilised by users/administrators (GUI), strategies of application of security polices, legal limitations, as well as contractual obligations which the SOC providers have with their clients.

CONCLUSION

The reality we are facing is that security breaches occur every day and that is why today there is a need for operation monitoring systems. Experience shows us that a pragmatic approach should be applied in order to implement a professional Security Operation Centre in an organisation, which can provide reliable results. We can conclude that the only adequate approach to creating and managing reports is the one which applies all the measures defined by best business practice. Aside from all the aforementioned, it is also necessary to point out that the use of R-boxes infers certain risks and cannot be left to chance, because inadequate use can lead to a bad or late response, which, in turn, leads to using exclusively "post mortem" analyses, that is to say – digital forensic analyses.

BIBLIOGRAPHY

Škundrić, P. 2017
Koncepti i implementacija Centra za upravljanje bezbednošću kompanija, Beograd: Ibis instruments.

Novak, J. and Stephen Northcutt, S. 2000
Network Intrusion Detection: An Analyst's Handbook, 2nd Edition, *Que Publishing.*

Korać, V., Prlja, D. and Diligenski, A. 2016
Digitalna forenzika, Centar za nove tehnologije Viminacium, Arheološki Institut, Institut za uporedno pravo: Beograd.

REZIME
MODULI CENTRA ZA UPRAVLJANJE BEZBEDNOŠĆU ORGANIZACIJE – TEHNOLOŠKI ASPEKT

KLJUČNE REČI: SOC, IDENTIFIKACIJA, INFORMACIONA BEZBEDNOST.

Centar za upravljanje bezbednošću organizacije predstavlja platformu čija je svrha pružanja usluge i detekcije i reakcije u slučaju bezbednosnih incidenata. U radu je istaknut tehnološki fokus na module Centra za upravljanje bezbezdnošću organizacije čiji je cilj sprovodjenje operacija sigurnosnih događaja. U sklopu analize pojedinačnih modula prikazane su njihove prednosti i ograničenja.

* * *