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
005.922.1
COBISS.SR-ID 29189385
https://doi.org/10.18485/arhe_apn.2020.16.14

PROCESS MANAGEMENT WITHIN THE SECURITY OPERATION CENTRE OF AN ORGANIZATION

ABSTRACT

This paper comprehends the most important processes performed by the Security Operation Centre of an organization. The main processes, described separately in the paper, provide information for identifying, tracking, prioritizing, analysing, remediating, assessing and revising, in order to solve all incidents and/or illegal activities concerning the security of the organization itself, i.e. its information assets.

KEYWORDS: SOC, SECURITY OPERATION CENTRE, INFORMATION SECURITY.

The Security Operation Centre of an organization (hereinafter: SOC) represents one or more locations where all the data linked to information security of one or more companies are gathered, sorted, stored**,** analysed, and on the basis of which reactions are taken in accordance with the safety policies of the company in question or on the basis of legislative regulations.

One of the most valuable tools that the person in charge of managing critical systems has is a verification list. The goal of this list is to establish an adequate process for the verification and implementation of all steps, that is to say, to list every step, even the smallest, which has to be taken in order to maintain the required security level, avoid risks, and protect data and important information. The person in charge of creating processes and procedures is the SOC manager, and all others are required to follow his lead. There is a large list of activities that the SOC team has to perform in the exact predefined manner in order to protect the computer infrastructure in a suitable manner, that is to say, so that all the threats are foreseen, and, if they occur, the team can react in the correct manner and in time. In this part of the paper, we will describe the main processes that a SOC team has to perform with the goal of:

- detecting threats,
- establishing the scope of a threat and its influence on regular business activities, and
- securing an efficient and quick response.

Main processes within the SOC are:

- events classification and triage,
- prioritisation and analysis,

Alarm type	Description	Critical level	Activities of the first level analyst
Research and sounding	Behaviour which indicates activities whose goal is to discover information on the organization	Low	All the listed activities should be compared against the Threat Intelligence database
Attack attempt	Behaviour which indicates a potential attack by activating the detected vulnerability	Low/Medium	All the listed activities should be compared against the Threat Intelligence database
Successful usage of the detected vulnerability and installation of a malicious code	Behaviour which indicates successful usage of the vulnerability or backdoor/RAT which was installed into the computer system of the company	Medium/High	Verification and research – escalation to a higher level necessary (level 2)
Compromised system	Behaviour which indicates that the system has been compromised	High	Verification and research – escalation to a higher level necessary (level 2)

Table 1 Alarms and activities within a SOC

- remediation and restoring a previous version,
- assessment and revision.

The quality of implementation of these processes represents the basis for measuring the quality of services that can be provided by a SOC.

EVENTS CLASSIFICATION AND TRIAGE

The real value of gathering, collecting and analysing data, or system records, is in finding within the forest of data actual data that can have a certain value for the organization itself. The key indicators of the system being compromised can be found in records regarding users' activities, in active monitoring of system log records (IDS, Nagios, Icinga and the like), and accepted/rejected connections to firewall devices, etc. Additionally, a specific combination of the said events, in accordance with determined patterns, can be an indicator that certain activities require additional attention and processing. A typical example of these activities is an attempt to access administrative services from locations where there are certainly no administrators (e.g. attempt to access resources from certain countries via VPN et al.). Here, the key to success lies in the possibility of classifying such or similar events so that they can be prioritized and escalated as critical and requiring special attention.

A first level analyst is required to go over all the events with a high critical level, i.e. severity. Once it is established that the mentioned event deserves attention and further investigation, escalation to the second level of processing is performed, i.e. it is transferred to the second level analyst. It should be stressed that in cases of smaller teams, the role of the first level and second level analyst can be performed by just one person. It is essentially important here that every one of the mentioned events be recorded and documented.

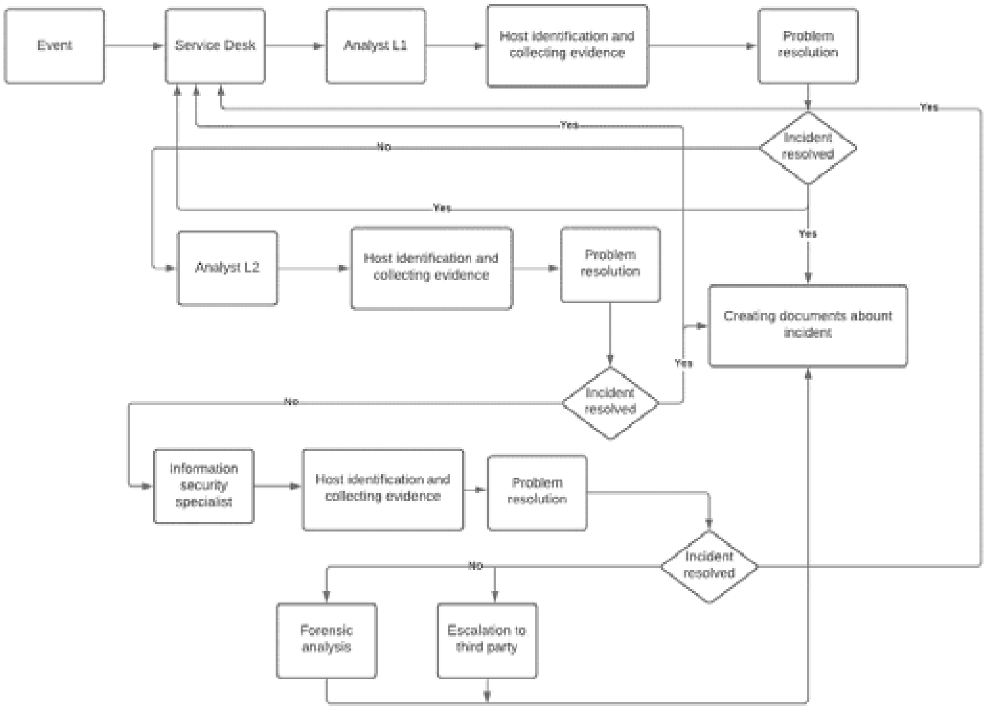
Event
Service Desk
Analyst L1
Host identification and collecting evidence
Problem resolution
Yes
Yes
No
Incident resolved
Yes
Yes
Analyst L2
Host identification and collecting evidence
Problem resolution
Creating documents abount incident
Yes
No
Incident resolved
Information security specialist
Host identification and collecting evidence
Problem resolution
Incident resolved
No
Forensic analysis
Escalation to third party

Fig. 1 Incident management process within the SOC

In most cases, the evaluation of events is done automatically, by verifying system records that have been previously correlated to predefined behaviour pattern, which can be found in certain forms of Threat Intelligence systems, which vary depending on the manufacturer but have the same principles.

Almost all alarms can be divided into four categories, on which further activities depend. The alarms and activities are given in the Table 1.

If the first level and second level analysts are not able to handle the incident successfully, it is escalated to an expert in the field of information security, and, if necessary, a CERT (Computer Emergency Response Team) is created – a team which will solve the mentioned problem [3]. In order to solve every detected incident successfully, the SOC has to have defined procedures which are described as follows:

- use of information system resources with the goal of solving incidents,
- overview of all open tickets linked to incidents,
- management of changes in incident status,
- activities taken if there is no response from the client (the client is considered to be integral part of the SOC and, in a certain number of cases, the end user can also be the system administrator),
- adding records in accordance with incident solving,
- additional escalations,
- manner of closing the incidents,
- management of high priority and high impact incidents, and
- activities in cases when a solution cannot be found.

A detailed representation of activities undertaken with the goal of solving an incident is given in Fig. 1.

As can be seen from Fig. 1, aside from the client and SOC, third parties can also sometimes be involved in the incident solving process, in order to perform additional forensic analyses, or to create necessary "patches" on systems or installations if the SOC or the end user do not have adequate resources for those activities.

Aside from a third party in the final instance, we can see that, at the beginning of the process, there is a central point for communication with clients (either internal, within a company, if there is a SOC, or external, if the SOC services are entrusted to others), which is performed through a service desk, or service centre, depending on the terminology used.

The role of the SOC manager in the incident solving process was removed from the diagram for the simple reason that situations where the SOC manager is involved are very rare in communication with end users, which is performed solely on management levels.

PRIORITISATION AND ANALYSIS

Prioritisation is the key to success in any venture, and it is even more critical in information security. The stakes are high, attack rates increase suddenly and show no signs of stopping. In the meantime, the means we have for protecting property from this type of attacks are very limited. It is necessary to focus on those events which could affect the business the most and which demand knowledge about the most critical means. At the end of the day, maintaining business continuity is the most important responsibility entrusted to the SOC team.

In order to prioritise the effects of potential attacks in the best manner possible, it is necessary to previously perform a complete inventory of the equipment which is being monitored. This inventory is not merely a list of equipment, but also a complete analysis of the software which exists in the monitored system, as well as detection and classification of data which are on the equipment itself, that is to say, assessing how critical they are to the company.

Within this process, the SOC has the task of overseeing and adequately responding to any activity which indicates that a malicious user has infiltrated the infrastructure of the company. Infiltration is possible by means of installing malicious software or even the presence of a malicious user. The end result of such infiltrations is communication being intercepted or data destroyed [2]. As in the previous process, prioritisation and analyses are performed on the basis of data correlated to the existing patterns or patterns defined by the user within the technological systems that the SOC has available.

In order to achieve the best possible results of analyses, in accordance with the existing technology and development level of the SOC, there is an increasing use of artificial intelligence and machine learning, whose task is to recognize the increasingly more diverse manners of spreading malicious codes and malicious activities.

REMEDIATION AND RESTORING A PREVIOUS VERSION

The sooner an incident is detected and responded to, the higher the possibility that damage will be completely avoided or reduced to the minimum. There are, however, certain cases when consistency cannot be confirmed with great reliability for all data, that is to say, when the system is compromised to the point that it becomes necessary to restore it to one of the valid previous copies, in accordance with the regulations or the business continuity plans of the company. Usually, the company handles the process of restoring a previous version and not the SOC team. The SOC team generally has an advisory/consulting role in such cases and that of the system verifier, by doing some of the following activities:

- reconfiguration of the system in accordance with the needs of the company,
- reconfiguration of the network and network parameters in accordance with the needs of the company,
- revision of the system security level in regard to the hardware-software protection,

- revision of the capability of the infrastructure to monitor events, and
- upgrading system software and applications in accordance with the recommendations of the manufacturer.

ASSESSMENT AND REVISION

Assessment and revision, essentially represent preventive testing of the information-communication system to vulnerabilities. System vulnerability analysis is very significant from the protection standpoint, so that organizations could know which oversights are present on systems, how difficult it is for an attacker to use them, and which consequences could be caused by them. It is always the optimal solution to deal with potential threats before an attacker actually discovers them. This is most commonly done precisely through system vulnerability testing, followed by a detailed analysis of the results, on the basis of which a report is created, with recommendations on how to enhance the overall security of the information system. These activities, essentially, represent the most widely spread manner of revision of the information-communication system. The revision process itself can be performed by the SOC, an external or an internal revision unit.

It is necessary, here, to point out that certain standards, such as PCI DSS standards, require regular scanning and prescribed levels of system protection so that the company will show required competencies. Aside from what we have already mentioned, it is important to stress that the system should be tested in such a manner so as not to disturb regular work flow. Testing is performed according to the plan made by the IT services for a closer monitoring of the systems which are being tested.

CONCLUSION

A Security Operation Centre within an organization represents one or more locations where all the information linked to the information security of one or more organizations are gathered, sorted, stored, kept, or analysed and on the basis of which measures are taken in accordance with the safety policies of the company in question or on the basis of legislative regulations. Both in the recent and more distant past, we were witnesses of minor or larger security breaches, the result of which was some kind of bad impact on the organization, in terms of either finances or reputation, and which disrupted, in some manner, the regular delivery of contracted services to third parties. The SOC represents a group/team/organizational unit which has the basic goal of protecting information resources, either through prevention, by raising the consciousness on risks, or reactively, in cases of successful or unsuccessful attacks on the computer infrastructure. The SOC consists of a large number of processes, and the most important ones have been examined in detail. Essentially, this consists of people and technology which have to work in a coordinated manner so as to avoid potential problems in detecting and removing the consequences of an attack.

BIBLIOGRAPHY

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

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

ENISA (European Union Agency for Network and Information Security) 2014
Triage and Basic Incident Handling.

Internet sources:
https://cybersecurity.att.com, pristupljeno 10.09.2020.
European Union Agency for Network and Information Security www.enisa.europa.eu Triage and Basic Incident Handling.

REZIME
UPRAVLJANJE PROCESIMA U OKVIRU CENTRA ZA UPRAVLJANJE BEZBEDNOŠĆU ORGANIZACIJE

KLJUČNE REČI: SOC, CENTAR ZA UPRAVLJANJE BEZBEDNOŠĆU, INFORMACIONA BEZBEDNOST.

Ovim radom su obuhvaćeni najvažniji procesi u okviru Centra za upravljanje bezbednošću organizacije. Glavni procesi koji su posebno opisani u radu pružaju informacije za identifikovanje, praćenje, prioritizaciju, analizu, remedijaciju, procenu i reviziju za razrešavanje onih incidenata i/ili protivpravnih aktivnosti koji se odnose na bezbednost same organizacije, odnosno njene informacione aktive.

* * *