Security Operations Center (SOC) and Security Monitoring Services to Fight Complexity and Spread of Cyber Threats

ARIMATSU Tatsuhiko, YANO Yukiko, TAKAHASHI Yutaka

Abstract

In answer to the spread and sophistication of cyberattacks, newly developed countermeasure products are achieving positive results and a certain level of success. However, many of them rely on the judgment abilities of the operators and due to the difficulties of their operations the current situation does not succeed in reducing damage satisfactorily. The security operations center (SOC) described below provides services with which professionals perform the required operations by substituting end users and is one that is currently attracting special attention in the field of cybersecurity. This paper describes the core issues that are currently being experienced and the innovative approach related to the SOCs and security monitoring services. It also gives a perspective on the desirable shape for the SOCs of the future.

Keywords

security operations center, SOC, security monitoring service, AI, machine learning

1. The Environment Surrounding Cyberspace

1.1 Advancement and Sophistication of Cyberattacks

Information leak damage via cyberattacks by sending e-mails for targeted attacks or hitting a website vulnerability have been increasing in recent years. Cyberattacks aiming at illicitly acquiring money by means of banking malware and ransomware are also increasing. Particularly, attacks attributable to professional cybercrime organizations are noticeably increasingly innovative and sophisticated, making successful countermeasure extremely difficult to achieve.

For example, the pattern-matching type countermeasure products such as antivirus software, IDS and IPS often fail in detecting new attack techniques and malware, so they cannot be effective against the attacks until the product vendor distributes the signature after the damage is detected in the attacked organization. Recently the dissemination of sandbox type products and AI-based products has achieved a certain level of success. However, in reality, new attack techniques capable of passing through their countermeasures are already emerging. Some examples of techniques avoiding detection are the technique of creating a compressed file in which malware is encrypted or that of increasing the file size by adding a large amount of irrelevant codes to the malware codes.

As has been pointed out generally, countermeasures relying on a single type of security products have limitations of defense capability and it is necessary to enhance defense robustness by combining several countermeasures.

1.2 Outsourcing of Security Operations to Security Operations Centers (SOCs)

There are many organizations that are promoting preparedness against cyberattacks by introducing multiple security measures. On the other hand, following the increase of data exchanged via the Internet, the logs and alerts generated by security devices are also increasing, causing many organizations to be adversely affected by these issues. It is essential to determine if each log or alert signifies an erroneous detection (hereafter "false positive"), an event of minor importance or an incident to be noted quickly and optimally. Therefore, a wide

range of knowledge and expertise is required including: network skills, security knowledge on cyberattack techniques and vulnerability information and an understanding of system and network environments, as well as a substantial knowledge of security devices.

Under such circumstances, the trend of outsourcing the security monitoring and operations to a SOC run by an external specialist security company is accelerating over many organizations. Following the trend, there have been certain needs for the SOCs that simply sent reports on the alerts issued by security devices to customers so far. However, it is now expected that the increasing sophistication and advancement of cyberattacks will demand that security monitoring service must be provided by SOCs that have enough skills to judge security events properly.

2. Present Status of SOC Operations

2.1 Issues of Log Analysis

NEC and Infosec Corporation which is one of the security specialized affiliates of the NEC group run the "NEC Cyber Security Factory" which has SOC as one function. At the Cyber Security Factory, analysts perform original analysis of the large amounts of logs and alerts generated by security devices to determine the importance and seriousness of each event. In fact, the alert levels issued by security devices often differ from those concluded by their analysts, so the analysts determine whether or not an event generated from logs is a false positive and, if not, select the level of security event from Levels 1-4 (**Fig. 1**). Their analysis work makes it possible to notify the users optimally of only the necessary events.

However, in the traditional security service market in Japan, it is standard business practice to conclude a service agreement per security device. On the other hand, the logs and alerts sent from a single security device are often insufficient for determining the level of the event. In such a case, a judgment requires past experience and knowledge of the analyst (including that on the system environment and on the communication tendencies of customers) as well as secondary data enabling a final decision (**Fig. 2**). Such situations bring the difficulty of the analysis operations.

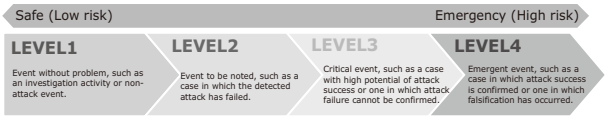


Fig. 1 Levels of security events.

As the false positive and attack failures form a fairly high percentage in the whole events, the analysts operations currently need much time for making judgments on such issues (**Fig. 3**).

As the growth trend of security events compared to previous years, Fig. 3, the burden of analysis operations on analysts are increasing continually, making it an urgent matter to improve the operational situations.

2.2 Resource-related Issues for SOC Analysts

The increased need of services might be dealt with by increasing the number of analysts, but such a solution involves a serious issue.

According to a survey by the Japanese Ministry of Economy, Trade and Industry, there is an insufficiency of about 130,000 human resources engaged in information security, and this number is expected to exceed 190,000 persons in 2020. The situation of scarcity is similar in

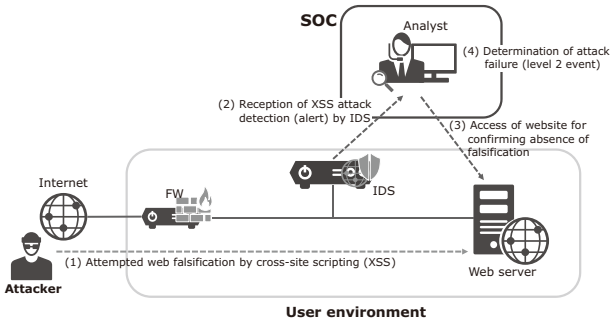
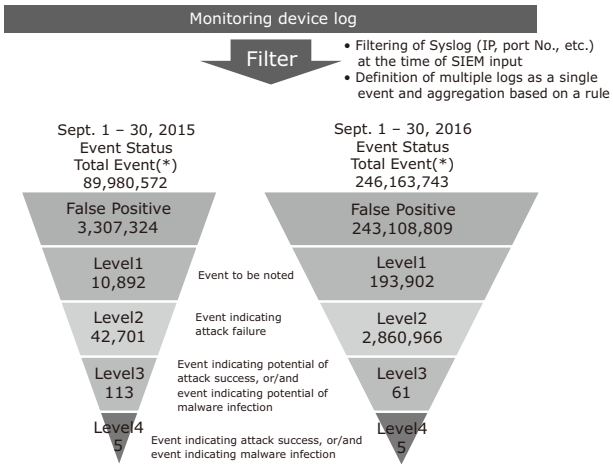


Fig. 2 Example of additional investigation for attack success/failure judgment.



(*) The "Total Event" refers to the total number of events entering SIEM after filtering of raw logs.

Fig. 3 Number and growth of events per category at Cyber Security Factory.

the job category of SOC analysts. The issue is more serious for the SOC analysts because the technical knowledge required for SOC analysts is especially high. The need for a longer time taken in training than for other security engineers poses a more serious issue.

For example, monitoring of gateway type security devices requires an accurate knowledge of networks. Since some events necessitate packet checking work, it is also necessary to acquire competent knowledge on the packet structures according to protocols. In particular, SOC requires speedy analysis and judgments, so technological understanding and capability at the level of immediate knowledge recall is an essential skill. Moreover, malware analysis becomes necessary in some incident cases, skill in reading program codes is also required.

In addition to the skills based on a general knowledge of IT and networks, it is also necessary to have a positive attitude and natural curiosity in order to catch up continually on attack methods, including on knowledge of typical or trendy cyberattack techniques.

Considering the technical level required by analysts, acquiring knowledge at the desktop is not enough in itself, the training process with OJT in the field (SOC) is indispensable. However, the OJT necessitates skilled analysts that already have important roles in field operations, the number of potentially trainable people is limited. Although efforts and the actual process of the human resource training of analysts is continuing constantly, the policy of training a large number of analysts in a short period is rather unrealistic.

3. New Approach Based on AI

As discussed in the above, the expansion of monitoring services via SOC encounters the important issues of increases in the amount of log analysis work and the shortage of analyst resources. Consequently, NEC and Infosec have started to develop the "threat analysis server" using AI (Artificial Intelligence) aiming at saving workload in log analyses. With the threat analysis server, the feature vectors of communication packets related to each event and the judgment results of analysts are used as the learning data to build a learned AI. This is then verified with real-time actual data in order to improve the judgment accuracy. However, when the setting (threshold value) is changed to significantly improve the accuracy to judge false positive detection as "false positive", false negative (overlooking, judgment of actual attack as a false positive) occasionally occurs as a trade-off. Since it is indispensable to maintain false negatives as close as null considering the properties of this service, the setting (threshold) is tuned very cautiously in order to avoid false negatives.

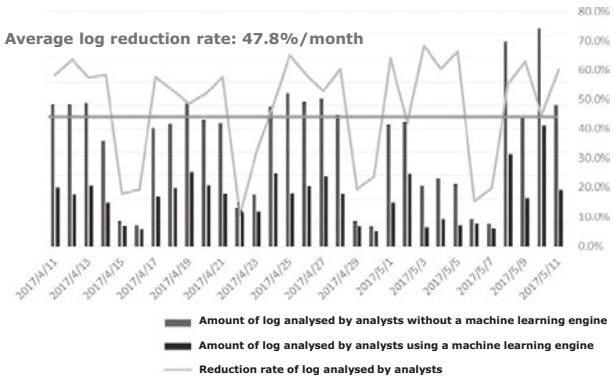


Fig. 4 Log analysis efficiency improvement using AI (machine learning) at Cybersecurity Factory.

More recently, these efforts have been started to expand the scope of applications of AI so that the AI is able to judge Level 1 and 2 events as well as false positive judgement. Even at the current stage, about 50% of the analysis logs compared to former status before using AI have been reduced successfully, thereby leading to improvements in the operational efficiency of the analysts (**Fig. 4**).

By using AI for auto analysis and judgments of minor events that occupy a large part of the operations of analysts, they can focus on more important activities such as the examination of methods for responding to the advancing attacks and improving their detection accuracy.

The authors believe that a positive use of AI can promote standardization of the quality of monitoring services and encourage innovative efforts of the analysts. It will also contribute to the implementation of a high-quality service, equipped with a high detection capability of even advanced attacks.

4. Towards the Advancement of Monitoring Services

As already noted, the logs and alerts of a single security device are often inadequate for an analyst to judge the level of an event, necessitating further time for analysis. There would also be same cases which an alert succeeds in detecting a real attack but is unable to determine whether it has succeeded or not (when the events are judged to be of Level 3, etc.). Such cases means an issue from the viewpoint of analysis accuracy.

To counter possible threats of increasing complexity in the future, it will be necessary to define the threats that an organization should defend against and combine the logs of multiple security devices as well as servers and clients and conduct analysis per each threat (**Fig. 5**).

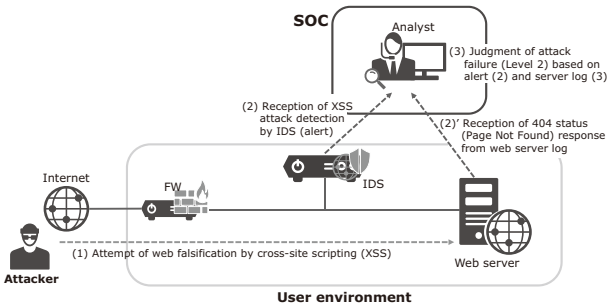


Fig. 5 Example of efficient judgment made by combination of multiple logs.

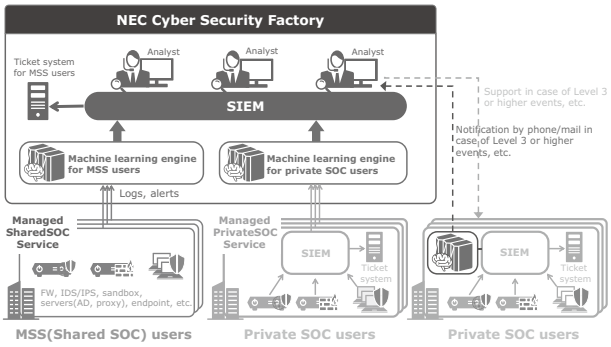


Fig. 6 Future image of SOCs in Cyber Security Factory.

For this purpose, the authors also believe that it is necessary to form a monitoring service market that is based on threat categories and also does not rely on single security devices, like as what the current monitoring services do.

When the logs and alerts from multiple devices (inputs) and the judgment results made by analysts (outputs) are accumulated as data, it is expected that sophisticated learning data that can indicate the high correlations between inputs and outputs can be built. It is also estimated that the analysis accuracy of AI can also be improved and the scope of use of AI in the SOC expanded further.

5. Future Perspectives of SOC

In the future the SOC will be able to implement a service that can monitor multiple devices logs, including servers and clients, and then the SOC must receive more logs and alerts than today. To make this possible, it is required to make active use of the AI to improve the function of filtering events of low importance and to prepare a process that allows the analysts to analyse and make judgments only on important events, as discussed in the above.

Some large-scale organizations have already introduced SOCs independently (private SOCs) for integrated management of logs and alerts in-house. On the other hand, considering the difficulty of employing analysts in-house, it is anticipated that cases of outsourcing the operations of private SOCs will increase in the future.

In fact, since operations of the SOCs differ depending on their organization it will be difficult for the vendors to undertake outsourcing of customers' original operation as it is and also because of the anticipated problems with the resources of the vendors. Therefore, the authors believe that it is necessary to implement a function for filtering general events exclusively for private SOCs, so that only the important events will be analysed by the service providers' analysts (**Fig. 6**).

In addition, NEC also aims at allowing the SOCs to provide prompt, seamless services covering advanced incident responses. This will include investigations of servers and clients in addition to the existing simple incident responses, such as closure of a firewall port when an event with a high potential of an incident is detected.

From the viewpoint of security operations, NEC and Infosec wish to resolve customer anxieties concerning cybersecurity by continuing to provide better services to ensure that critical incidents are prevented. We also aim to allow them to focus clearly on their primary business functions.

Authors' Profiles

ARIMATSU Tatsuhiko
General Manager
Cyber Intelligence Center
Infosec Corporation

YANO Yukiko
Senior Manager
National Security Solutions Division

TAKAHASHI Yutaka
Manager
Security Business Promotion Office

Information about the NEC Technical Journal

Thank you for reading the paper.
If you are interested in the NEC Technical Journal, you can also read other papers on our website.

Link to NEC Technical Journal website

Japanese

English

Vol.12 No.2 Cybersecurity

- Building Futureproof Security to Support Business Safety and Reliability -

Vol.12 No.2
January 2018

Special Issue TOP