Practice within Fujitsu of Security Operations Center: Operation and Security Dashboard

● Takayoshi Sadamatsu ● Yoshihiko Yoneyama ● Kai Yajima

Recently, cyber crimes have been rapidly increasing in Japan and overseas and their methods are becoming more complicated and sophisticated. Targets of cyber attacks are shifting from individuals to enterprises, and cyber spy activities targeting confidential information of enterprises have become conspicuous. Under the circumstances, there is a global need to improve capabilities to promptly identify risks and quickly respond to incidents, in addition to improving security measures that can respond to the actual conditions for defending against cyber attacks. The Fujitsu Group has been implementing in-house activities to quickly detect signs of cyber attacks and other cyber threats for immediate incident response at the security operations center (SOC). With the existing operation model, however, there still remains demand for global-level standardization of the incident response process for faster responses. This paper describes an approach to meeting this challenge. It involves analyzing the actual business processes and standardizing their operations before introducing an automation tool, with which incident response time can be reduced and potential risks in the corporate network can be eliminated at an early stage. In addition, it presents a security dashboard that visualizes the operation status of the SOC by using key performance indicators (KPIs).

1. Introduction

Targeted cyber attacks are on the increase, stealing confidential information from enterprises. Attackers employ more and more complex tactics,[1] and damage from unauthorized access to corporate data is increasing every year, with the total damage in 2013 reported to be over 375 billion USD.[2] Information leaks are a global phenomenon today, and enterprises, in Japan and abroad alike, need to equip themselves with a system to protect sensitive information from targeted attacks and other threats, providing a means to counteract quickly if required.

Against these security threats including targeted attacks, Fujitsu operates an integrated log-management system in Japan that centrally manages security alerts. This system makes it easier to quickly detect security alerts at the Security Operations Center (SOC), and provide countermeasures on a round-the-clock basis to quickly respond to them.

Efficiently operating the SOC requires the automation of processes from information gathering and damage survey through to the provision of countermeasures. Thus, we developed definitions and a design for globally aligned SOC operations, and standardized the countermeasures, thereby realizing a scheme that allows the SOC to implement a swift response.

This paper presents the internal initiative at Fujitsu to introduce an automation tool to enhance the SOC efficiency for quick-response operation. It also describes the dashboard that is introduced to visualize the SOC operation status.

2. Approach to incident response

Fujitsu was providing its domestic and overseas group companies with an SOC service that was centrally controlled in Japan. The issues with the service were as follows.

1) While security alerts detected at any given location were centrally controlled by the SOC, there were communication issues due to time zone and language differences. It was also challenging to maintain skilled local staff.
2) In order to operate the SOC efficiently and

ensure that the control was effective in each region, it was necessary to standardize the security processes and decentralize the system (to allocate security staff in each region). While the standardization and decentralization were successfully implemented to facilitate quicker responses, procedures for performing the incident responses became more complicated in terms of information-gathering, countermeasure requests, verification of risk levels, and collation of the same phenomena. Thus, further improvements were necessary to enhance incident response speed and reduce the person-hours needed to handle them.

3) The decentralized system gave rise to the need for visualizing local operations and ensuring high-quality responses.

As a means to address these challenges, we introduced an automation tool to support local security staff with their tasks, aiming to expedite the incident responses and reduce person-hours globally. Furthermore, we developed a dashboard for visualizing incident response statuses by defining key performance indicators (KPIs) to evaluate the achievement level. The following steps were taken to make this happen.

1) Analyzing the current situation

Analyze how the SOC is operated in Japan and overseas to clarify the processes that may be automated through standardization.

2) Designing the operational system

Specify the input/output data for each process identified in the above step, and coordinate these processes to prepare workflows to be applied to automation. This allows the user to create a series of actions for immediate response as a result of automatic attachment of the information necessary for incident responses to the input data.

3) Applying to the SOC operation

Associate these prepared workflows with the automation function (FUJITSU Software Systemwalker Security Control)[3] for automatic generation of incident tickets[note] based on alert information.

4) Defining KPI

Define KPIs for each incident response phase, and integrate them with the ticket management system. The KPIs are then visualized as a dashboard.

In the following section, we will give detailed descriptions of the method employed when using this automation tool and visualization by the dashboard, together with the obtained effects.

3. Analyzing the current situation

3.1 Number of incidents handled

Through the SOC operation, we analyze over 600 million security alerts a day. There are about 100 incidents a month that require countermeasures. The term incident here refers to events that represent a threat to information management and system operation, including malware infection, unauthorized external communication, and suspicious internal communications that are prone to information leakage.

In particular, in recent years malware has increasingly been intruding into intra-networks in enterprises, accounting for an increasing portion of security incidents that result in information leakage or security breaches. Given this context, the SOC incident response is putting more emphasis on closely monitoring malware infection.

3.2 Tasks involved

There are mainly the following four tasks involved in the SOC initial response against incidents:

1) Assessing risk levels,
2) Prioritizing response cases,
3) Identifying administrators of infected terminals, and
4) Requesting terminal administrators to implement countermeasures.

As an initial step, check the security alert to identify signs of a threat in the log of the sensors installed on the network gateways.

1) Time of the incident detection
2) Name of the host device
3) Event name
4) IP address of the device
5) Destination IP address
6) Accessed URL

Based on these items, risk levels to understand the significance of the threat and response priorities

note) The alert information issued by security monitoring equipment is supplemented with other necessary information, and prepared for SOC operators to process. This constitutes a unit as a case for the SOC operators to handle.

are determined by referencing the alert response manual and alert assessment manual. Then, using the network database search system, information about the administrator who is responsible for the affected terminals is obtained; such as his/her name, affiliation, e-mail address, and telephone number. Once the information is in place, consult the administrator and ask about details such as the operating system or last security definition update using a template e-mail for contacting administrators. Then give him/her instructions on the necessary actions to take, such as a virus scan and/or OS re-installation.

Security risks increase in proportion to the amount of time that has elapsed after the onset of incidents. The longer the incidents are left unattended, the greater are the risks of an information leak through unauthorized external communication or further damage. For this reason, an accurate and prompt initial response is crucial.

To improve the efficiency in executing these actions, we investigated the time required for an initial response per incident. It turned out that the average time over a whole incident (from the time an incident occurred until the initial response was completed) was about 30 minutes, and most of it was accounted for by manual work throughout the initial response procedures, such as performing various assessments, searching on the Web system, and selecting templates to use. A particularly time-consuming step was consultation of manuals. This is because SOC operators need to proceed carefully, taking the time to search for information based on the incident information from the sensors, and interpret them.

4. Designing the operational system

From the results of the analysis of SOC operators' initial response execution, we found that the response time must be improved. Therefore, we aimed to automate some system-based tasks, and designed the operational system, including the standardization of the following procedures.

4.1 Clarification of procedures

We extracted the minimum necessary processes based on the actual tasks performed by the SOC, for standardization. To help people have a better understanding of the context in which the tasks are executed, we identified the input data required to implement each task and output data obtained at their completion. In this way, we clarified the procedures necessary for incident response, which are as follows:

1) Deciding the response procedures

Decide the actions necessary based on the event name (alert name),

2) Assessing risk level

Assess the risk level based on the preset definitions,

3) Deciding the priority level

Decide the priority level of the incident based on the risk level and the number of accesses made externally,

4) Selecting the e-mail template

Select the e-mail template for contacting the terminal administrator,

5) Identifying the High Value Target (HVT)

Identify enterprise systems, servers and devices that executives own since they will have a larger impact if they are targeted or infected, and

6) Identifying repeated access

Observe external accesses. The number of such attempts is added to the work ticket information. Notify the administrator of the data leak and/or signs of spreading infection.

The processes of identifying HVT and repeated accesses have been added to the existing response procedures. These additions are made based on the results of a recent malware threat assessment, which suggested that they needed to be included in the automated processes to ensure accurate decision and action execution.

4.2 Selecting a system to be introduced

To automate these procedures and incident management, we selected Systemwalker Security Control as the middleware to be deployed because its features were appropriate for these purposes. One of the advantages is that processes may be easily modified in the future if necessary, because they are developed as workflows through standardization of the processes. Regarding the incident ticket management system, we decided that it was possible to get a comprehensive understanding of the situation and optimize administrator allocation by consolidating incident information globally. Upon introducing the middleware,

we provided the development department with SOC operation know-how, which helped to quickly automate processes and the functions necessary for the incident management.

4.3 Reform to a system-centered arrangement

In tandem with transforming tasks into workflows, we redefined the responsibilities of incident handlers and SOC operators.

These are described below.

1) Local operator

An operator who identifies the origin of incidents and implements prompt measures. This operator is appointed at each operation base.

2) Incident manager

An administrator who assists with the incident response, and is responsible for overall management of incident handling

3) System operator

A system operation administrator who operates the security monitoring platform to promptly perform system failure recovery

By delineating the responsibilities of each party involved in the incident response as described above, we developed the automated workflows to be provided by the system we introduced, as well as the operational arrangement that was optimized for the ticket management system.

4.4 Automatic issuance of incident tickets

All the security alerts that the monitors installed in bases across the world detect are gathered into the integral log management system, which has been deployed in Japan.

This system performs a correlation analysis between the alerts and the threats, and extracts the alerts that require incident responses. The alerts thus singled out then undergo a series of work processes as described in "Clarification of procedures" above, automatically executed by the Systemwalker Security Control, and the resulting information is attached to the security alert.

The security alert with information added will be sent to the ticket management system of the Systemwalker Security Control, and registered as an incident ticket. This registered ticket contains information on infected terminals' IP addresses and the administrators responsible for them; the ticket is then sent to those local operators responsible for the bases that are found to be relevant to the IP addresses (**Figure 1**).

4.5 Workflow for each SOC operator

Upon receiving the incident ticket, a local operator logs on to the ticket management system, and reviews the infection information written on the ticket.

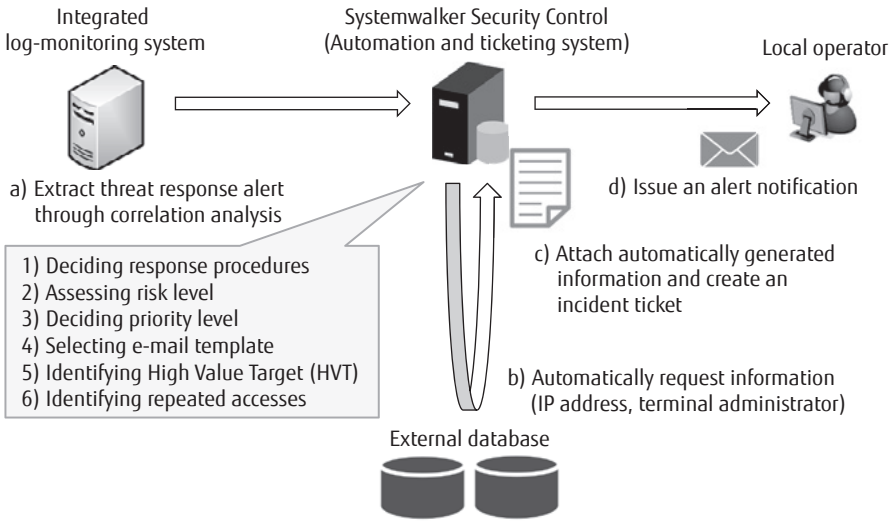

Figure 1
Automatic creation of incident tickets.

Subsequently, the operator updates the ticket management system with the commencement of response actions, and using the e-mail template attached to the ticket, the operator sends a request to the terminal administrator for verification and implementation of countermeasures.

An incident manager monitors and manages the progress of incident handling by the local operators with reference to the incident ticket concerning the area under his/her responsibility. If the local operators are found to be struggling with the procedures, causing a delay in the implementation of the countermeasures, the manager gives support with the response actions. After successful completion of the response actions, the manager logs on to the ticket management system to close the incident ticket after ensuring that there are no further problems.

The system operator observes the security monitors, the integrated log management system, and the ticket management system installed globally for stable operations, to ensure a reliable operation of the SOC (**Figure 2**).

5. Scaling the automation function

In addition to the workflows for local operators and incident managers described above, tasks for security analysts are also considered for automation. These analysts perform a correlation analysis of the security events and identify the attack scenarios and their logic. They have the following three major responsibilities:

1) Investigate and analyze security log,
2) Gather information on security threats and vulnerabilities, and
3) Instruct setting modifications for security monitors, and propose new measures to the business management.

Of these tasks, the investigation and analysis of a security log was automated. In order to identify attack scenarios, it is necessary to investigate and analyze the security alerts detected by various security monitors. If the correlation analysis successfully identifies the attack scenario, it is possible to verify if the intra-network is at a security risk by expanding the scope of security survey.

In this case, manual efforts to single out the attack scenario may delay the identification of urgent security alerts, allowing the risk factor to penetrate deeply within the intra-network for longer. Using the automation tool to convert attack scenarios into rules (workflows) would help to identify multiple security risks immediately as these rules can be applied to a large volume of log data to search and correlate with the events that match the rules instantly.

The security alerts thus detected automatically by the automation tool will subsequently prompt the SOC operators to implement incident countermeasures without delay.

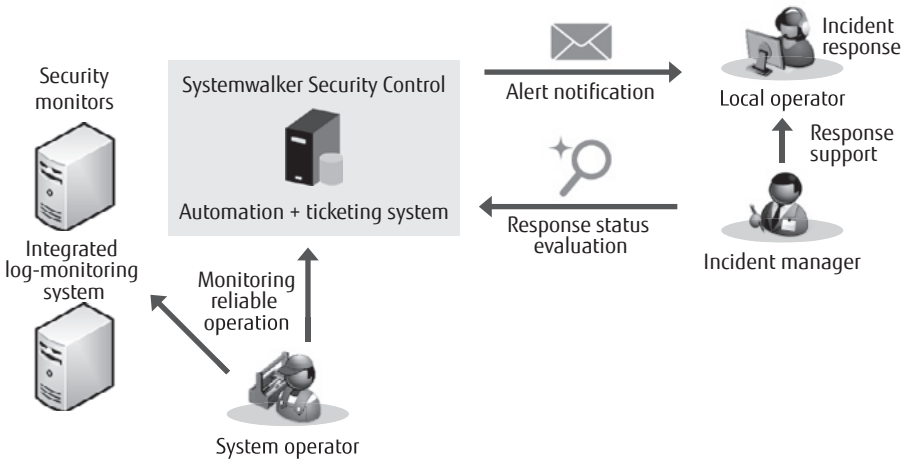

Figure 2
Constellation of SOC operators.

6. Visualization of SOC operational statuses

We aimed at visualizing the operational statuses of the SOC by defining the KPIs for evaluating the SOC performance in order to ensure high-quality incident responses. The following items are set as parameters:

1) Time to commence initial response

The time elapsed from the onset of an incident to the implementation of initial response,

2) Time to close the case

The time elapsed from the incident occurrence to the completion of countermeasures implemented,

3) Success rate

The rate of successful solution of incidents without necessitating an escalation to the incident manager, and

4) Error rate

The rate of incidence of human errors.

We introduced a security dashboard system that is designed to make it easier to automatically calculate the above KPI values and visualize them. The system automatically gathers information on the progress of each incident being handled, and calculates the KPI values, which then will be shown on the dashboard display. The incident response statuses and risk levels are also indicated on the display.

By visualizing SOC operators' conditions, the system allows the user to monitor in real time the critical factors such as slowed responses, compromised response quality, delays of responses due to an increase in incidents, and unattended high-risk incidents. This has made it possible to implement appropriate actions in response to various situations (**Figure 3**).

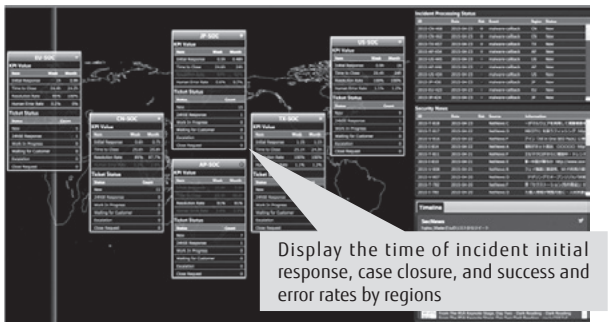

Figure 3
Security dashboard.

7. Effects achieved through the automation

As we automated the processes by standardizing various tasks of the SOC, such as incident handling and log analysis/investigation, we reduced the person-hours needed for the following procedures:

1) Local operator

The operator's initial response time has been reduced by 97% (to 1 minute from 30 minutes), and

2) Security analyst

Introduction of the automation tool has made it possible to consolidate the functions of security analysts, resulting in a 50% cost reduction.

In addition to the person-hour reduction, it has led to qualitative improvements as follows.

1) Enhancement of risk assessment accuracy through standardization

Standardizing the incident response procedures allowed for an automation of risk assessment processes, which led to an improvement in the risk assessment accuracy. As a result, prompt incident responses have become possible with consideration given to urgency.

2) Risk visualization

The previous procedures involved manual execution of tasks such as searching, investigating and identifying security alerts based on identified attack scenarios. By automating these tasks, more time can be dedicated to further research and analysis of attack scenarios of different kinds. Extended benefits include more opportunities to prepare more diverse attack-detection rules, contributing to the discovery of more unauthorized network accesses and new threats.

8. Conclusion

While automation of operations using software has become popular with many practical applications cited in a variety of contexts, there are still many business operators who are skeptical about leaving operations to a computer system. There are only few cases of enterprises applying automation to SOC operation, and this was a big challenge. We attribute the establishment of the SOC described in this paper to the accumulation of practical know-how gained through cross-sectional collaborations.

The threats of malware are progressive and growing. Security measures need to evolve constantly

to counter such threats. Fujitsu will continue making efforts to add more measures to counter ever-increasing threats, and help to maintain secure network environments based on the flexibility of systems and operations.

References

1) Ministry of Internal Affairs and Communications: Information and Communications in Japan 2013 (in Japanese).
http://www.soumu.go.jp/johotsusintokei/whitepaper/ja/h25/pdf/index.html
2) Center for Strategic and International Studies: Net Losses: Estimating the Global Cost of Cybercrime. June 2014.
http://www.mcafee.com/hk/resources/reports/rp-economic-impact-cybercrime2.pdf
3) Fujitsu: FUJITSU Software Systemwalker Security Control (in Japanese).
http://systemwalker.fujitsu.com/jp/securitycontrol/

Takayoshi Sadamatsu
Fujitsu Ltd.
Mr. Sadamatsu is currently engaged in planning and verification of Managed Security Service for businesses.

Yoshihiko Yoneyama
Fujitsu Ltd.
Mr. Yoneyama is currently engaged in security management of Fujitsu's internal network.

Kai Yajima
Fujitsu Ltd.
Mr. Yajima is currently engaged in security management of Fujitsu's internal network.