Global Managed Security Service to Protect Customers' ICT Environments

● Katsuhiro Kawahara ● Hisahiro Naito

With an increase in security attacks in recent years, methods of attack are becoming increasingly complex and sophisticated, and security monitoring is critical for detecting such attacks quickly. Fujitsu offers FUJITSU Security Solution Global Managed Security Service (GMSS), which provides a one-stop solution for the operation of customers' security management. One feature of this service is that specialized security analysts with advanced skills stay on top of the latest security trends and the characteristics of customers' ICT environments. Based on this information, the analysts provide support ranging from temporary to permanent measures by closely examining alerts and proposing methods for handling any problems encountered. In addition, Fujitsu's proprietary technologies and advanced technologies from security vendors from all over the world are combined to build a platform capable of high-level detection of threats. This paper describes the features and scope of application of GMSS as well as the latest technological trends in cybersecurity monitoring.

1. Introduction

Cybersecurity related damage has been increasing in recent years and has become a frequent news topic. The motives of attackers have also diversified to include crimes done for fun, financial purposes, and theft of confidential data.

According to a report of the Center for Strategic and International Studies (CSIS) published in 2018, the economic impact of cybercrime around the world amounts to about 600 billion dollars each year.[1)] Further, the average amount of damage per personal information leak incident in 2017 in Japan was 548.5 million yen (about 5 million dollars).[2)] Thus cybersecurity measures have become essential for enterprises. On the other hand, the shortage of cybersecurity personnel at enterprises is an issue.

In view of this situation, Fujitsu offers FUJITSU Security Solution Global Managed Security Service (GMSS), a solution that monitors cybersecurity in environments such as customers' endpoints and networks.

This paper describes the current situation of ICT use and security threat trends, the characteristics and application areas of GMSS, and the latest technology trends in security measures.

2. Changes in ICT usage in enterprises and security threat trends

In recent years, the way ICT is used has been changing due to the promotion of reform in working styles and the spread of the cloud environment.

In the past, it was common to install a firewall at the boundary between the in-house network and the Internet to protect the in-house network from cyber attacks. However, as more and more employees work remotely from their home and as use of cloud services is expanding, data stored on the cloud is increasing. While this depends on company policy, remote work and use of cloud services are done in many cases by accessing the cloud directly from home, not via the corporate network. A suitable environment for using such ICT and security measures designed for the increasing variety of services are required.

Moreover, with the globalization of companies, there are also cases where their in-house network is connected to overseas bases. Therefore, if a malicious attacker manages to penetrate a given overseas site, not only that site but the entire internal network is at risk. Under these circumstances, customers who want comprehensive and unified cybersecurity monitoring

that covers both overseas bases and domestic bases are increasing.

It is difficult to cope with all sorts of diversified and sophisticated cyber attacks with anti-virus products and firewalls alone. It has also been reported that it takes an average of 101 days from the occurrence of a security breach until its detection,[3] during which time the intruder may gain access to the internal network and steal information. To avoid such massive damage, cybersecurity monitoring services are also needed.

Furthermore, in Japan, the Ministry of Economy, Trade and Industry and the Information-technology Promotion Agency (IPA) revised Cybersecurity Management Guidelines 2.0[4] in November 2017. In these Guidelines, companies are required to have not only defenses against cyber attacks, but also a broad range of countermeasures from the detection of attacks to recovery from the same. Thus, enterprises need to make preparations on the assumption that they will suffer intrusions.

To respond to such situations, Fujitsu offers GMSS, which provides a one-stop solution for the operation of customers' security management.

3. GMSS features

Among the services offered by Fujitsu throughout the customer's security life cycle, GMSS provides a security monitoring service that corresponds to the operation part.

It is important to introduce security products for protection. However, new methods of attack constantly emerge, and the methods are becoming more sophisticated and complex. Taking these facts into consideration, it is necessary to detect and respond to security risks by continuous security monitoring. GMSS performs tuning according to the security situation on a daily basis for better detection accuracy.

The following are some of the features of GMSS.

1) Experts with advanced skills

Security experts who have acquired Fujitsu's Security Meister certification[5] understand the latest trends in cybersecurity and attack methods and carry out monitoring of the customer's ICT environment.

2) Platform for detecting threats with high accuracy

Cybersecurity monitoring requires components such as sensors that monitor the security status, an engine that analyzes log alerts to identify threats, and a dashboard that shows visually the current status. The GMSS platform uses Fujitsu's proprietary technologies. This includes high-speed forensic technology researched and developed in collaboration with Fujitsu Laboratories, enabling quick identification of the scope of damage,[6] and the Active Directory log analysis technology described later.

These technologies are combined with industry standard products from partner companies with advanced security related technologies. The result is a platform capable of high detection accuracy.

3) Cyber threat intelligence

Cyber threat intelligence (CTI) is information obtained by cyber attack analysis conducted by security analysts and aggregated to a format that computers can use. CTI combines 5W1H, which includes information about the attacker (who), time (when), objectives (why), attack targets (what), intrusion routes (where), and intrusion method (how).

Fujitsu has established the FUJITSU Advanced Artifact Analysis Laboratory (A3L), which aggregates and analyzes CTI, and is developing an environment for malware analysis and digital forensic analysis (**Figure 1**). A3L collects and analyzes the latest security information from the Internet. In addition to analyzing security incidents and malware with GMSS, threat information from vendors and other external sources is used to discover and analyze new attack methods. Indicators of compromise (IoC) are pieces of forensic data, such as data found in system log entries or files, that identify potentially malicious activity on a system or network. Some organizations provide IoCs for security administrators as IoC feeds. The following are some of the features of A3L.

- Wide-ranging information collection

Information is collected from over 30 unique sources of information and various communities. In particular, information on targeted attacks in Japan and Asia is collected.

- Advanced analytical capabilities

Malware analysis technology including reverse engineering and open-source intelligence (OSINT) analysis technology that can detect signs of attack are utilized. A proprietary analysis system researched and developed with BAE Systems, Inc.[7] is used.

- Provision of customer-specific information

Threat information about the attacks to which

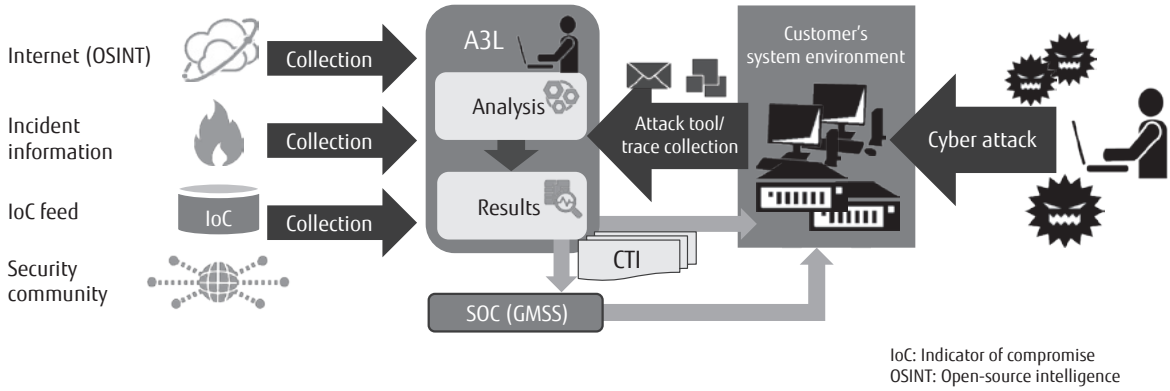

Figure 1
Roles of FUJITSU Advanced Artifact Analysis Laboratory (A3L).

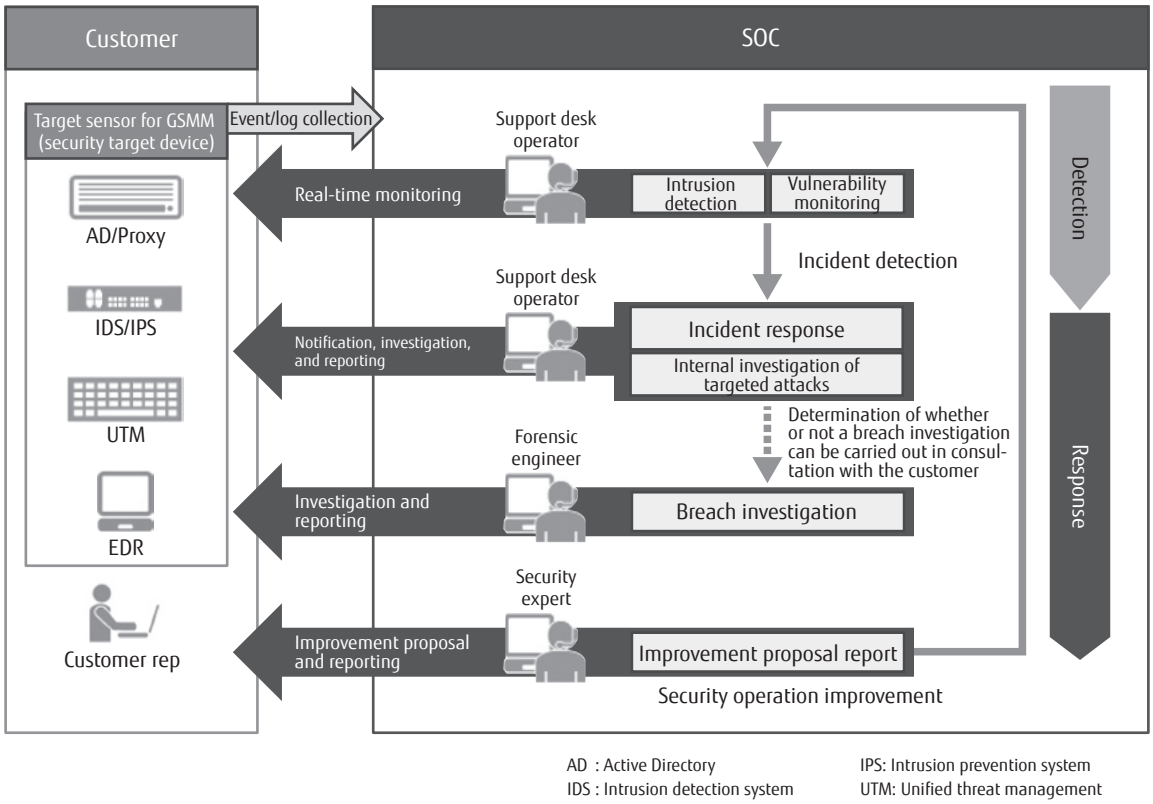

Figure 2
Overview of GMSS.

the customer is being subjected is provided. For example, the attack servers an attack group uses and the characteristics of each attack are determined from information such as which servers on the Internet the malware connects to. The new findings obtained therefrom are deployed to GMSS, where they are used to further improve the accuracy of intrusion detection, analysis and handling.

GMSS, which has the above three features, monitors the customer's environment from Fujitsu's Security Operations Center (SOC) as shown in **Figure 2**. GMSS can respond flexibly according to customer requests,

such as effective utilization of the existing security equipment of the customer's ICT environment. Fujitsu offers also a service called GMSS Express. This service systematizes highly necessary implementation content in line with the security operation pattern of the customer, thereby shortening the introduction phase, such as the definition of requirements, and providing faster start of service use.

4. Expansion of GMSS application areas

As the ways in which ICT is used change and security technology advances are made, GMSS is strengthening services along the horizontal axis and vertical axis shown in **Figure 3**. By expanding coverage of these two axes, the application areas of GMSS are expanding.

The security measures phase on the horizontal axis, which consists of "identification," "protection," "detection," "response," and "recovery," is derived from the framework proposed by the National Institute of Standards and Technology (NIST) in the U.S.[8] Until now, GMSS has dealt with security threats with emphasis on "protection" and "detection." However, it has become difficult to cope with all the diversifying and sophisticated cyber attacks that are taking place, and the service has been strengthened all the way to the "response" phase on the premise that customers will suffer intrusions.

Next, the monitoring target segments of GMSS, which correspond to the vertical axis, are described.

1) Internet boundary

The logs of firewalls and proxy servers at the boundary between the Internet and intranets are continually monitored to detect any abnormal communications. This makes it possible to detect attacks between the Internet and intranets and communications related to malware infections. In addition to the 24-hour monitoring service of major firewalls, Fujitsu offers also targeted attack detection services using sensors with Fujitsu's proprietary detection technology (Malicious Intrusion Process Scan).

2) Intranets

When an intranet endpoint is infected with malware, the attacker will attack other endpoints in the intranet or Active Directory, and finally acquire administrator privileges for Active Directory. There are cases when network monitoring is unable to detect intrusions. To detect security violations early, Fujitsu emphasizes monitoring within the intranet, and performs monitoring at the following points.

- Endpoints

Conventional antivirus software can detect known malicious files by pattern matching. However, these days, variants of malicious files can be easily created, resulting in a situation that pattern matching is unable to fully cover.

Therefore, there are now products that install software called Endpoint Detection and Response (EDR) at each endpoint to monitor activity at endpoints in greater detail and enable prompt response after infection. Such products detect abnormal behavior at endpoints, and if endpoints are infected by malware, they record post-infection behavior. Monitoring services that use EDR are called Managed Detection and

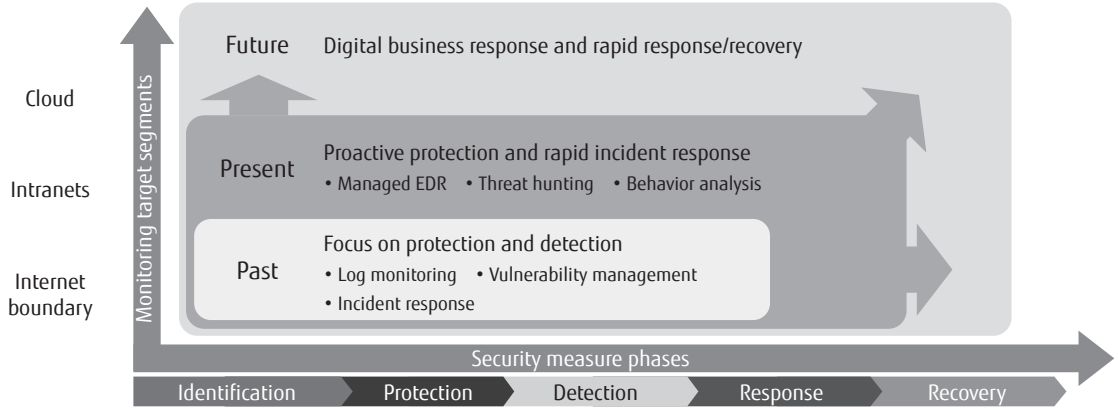

Figure 3
Direction of future GMSS enhancements.

Response (MDR). In addition to detailed analysis at the terminal level, they make it possible to quarantine infected terminals and quickly respond to infections through remote operation.

- Active Directory

If an endpoint in the intranet is infected with malware and can be remotely controlled, the malicious attacker will attempt to gain administrator privileges for Active Directory. Active Directory is the heart of the Windows system in the intranet, and usurpation of administrator privileges for Active Directory allows the attacker to gain access to all information on the Windows network. Therefore, detection and protection against attacks on Active Directory are critical.

Fujitsu provides an Active Directory monitoring service that uses proprietary technology. Normally, to take over administrator privileges for Active Directory, the attacker must go through a number of steps and in doing so leaves traces. By verifying these traces, which individually do not tell whether an attack is taking place, as a time series, attacks can be detected and steps taken to prevent damage. Further, by setting an operation policy, it is possible to easily detect deviation patterns.

3) Cloud

As enterprises increasingly use cloud services, they increasingly store their data not only in their intranets but also in the cloud. This means that the area to be protected is expanding not only to intranets but also to the cloud. To this end, detection of unusual behavior such as unauthorized login to a cloud system or downloading of a large amount of data over a short time by a single user is effective as a security measure.

Fujitsu offers a 24-hour security monitoring service that utilizes Microsoft security functions such as Office 365 Cloud App Security and Office 365 Advanced Threat Protection.

5. Latest trends in cybersecurity monitoring technology

In targeted attacks, after infecting a terminal with malware, in many cases the attacker tries to acquire administrator privileges for Active Directory on the network, as mentioned above. To protect the network against such attempts, it is necessary to detect and deal with the problem immediately when a terminal is infected with malware in order to prevent usurpation of the domain administrator's privileges.

In terms of technology trends, in order to realize this, security measures are being automated, and if a terminal is infected with malware, processing is carried out to automatically quarantine the infected terminal as soon as the infection is detected. The main components of such automation are CTI capable of highly accurate detection of infections, and automation and orchestration tools for the execution of automation.

Automation and orchestration tools define in advance workflows as to how each security device operates when an incident occurs. When an incident actually occurs, they automatically give each security device operating instructions when an incident actually occurs in order to deal with it.

For example, when the analysis engine for security logs detects the infection of a terminal by malware, it is possible to automatically quarantine the infected terminal from the internal network through collaboration among the automation and orchestration tools and the software installed on the network equipment or the infected terminal. Compared with manual response according to guidance, this has the advantage of shorter processing time and the prevention of human error. Moreover, threat hunting, which effectively uses CTI to actively detect threats that could not be detected in real time, will spread in the future.

6. Conclusion

This paper described the features and application areas of GMSS, Fujitsu's cybersecurity monitoring service, and the latest technology trends.

The world of cybersecurity is fast-paced and attack methods evolve every day. We will continue to expand the scope of application of GMSS and improve detection accuracy to help our customers maintain secure ICT environments.

References

1) CSIS: Economic Impact of Cybercrime. *https://www.csis.org/analysis/economic-impact-cybercrime*
2) Japan Network Security Association (JNSA): 2017 Information Security Incident Survey Report. (in Japanese). *https://www.jnsa.org/result/incident/data/2017incident_survey_sokuhou_ver1.1.pdf*

3) FireEye: M-Trends 2018.
https://content.fireeye.com/m-trends/rpt-m-trends-2018
4) Ministry of Economy, Trade and Industry–Information-technology Promotion Agency: Cybersecurity Management Guidelines Ver. 2.0. (in Japanese).
http://www.meti.go.jp/press/2017/11/20171116003/20171116003-1.pdf
5) K. Katayama et al.: Practice of Training Security Engineers Desired in Cyber Society. FUJITSU Sci. Tech. J., Vol. 52, No. 3, pp. 85–91 (2019).
https://www.fujitsu.com/global/documents/about/resources/publications/fstj/archives/vol52-3/paper13.pdf
6) Fujitsu: Fujitsu Enhances Intranet and Endpoint Security by Expanding its Global Managed Security Service.
https://www.fujitsu.com/global/about/resources/news/press-releases/2017/0512-01.html
7) Fujitsu: Fujitsu Develops Cyber Threat Intelligence Utilization System with BAE Systems, Inc.
https://www.fujitsu.com/global/about/resources/news/press-releases/2016/0516-02.html
8) NIST: CYBERSECURITY FRAMEWORK.
https://www.nist.gov/cyberframework

Katsuhiro Kawahara
Fujitsu Ltd.
Mr. Kawahara is currently engaged in cybersecurity related research and development.

Hisahiro Naito
PFU Ltd.
Mr. Naito is currently engaged in cybersecurity related work.