Cyber Range CYBERIUM for Training Security Meisters to Deal with Cyber Attacks

● Kazuhiro Hara

Customer systems today are constantly exposed to the threat of cyber attacks. To protect customer businesses in this age, the capability to respond to cyber attacks on customer systems and minimize damage is key. Fujitsu addresses this issue by training Security Meisters, who are human resources capable of responding to cyber attacks. To improve response capabilities against cyber attacks, it is useful to train in a cyber range, a virtual environment that allows trainees to experience simulated cyber attacks. With existing cyber ranges, however, it was difficult to reproduce a wide range of systems and difficult for system engineers in different locations of the country to use them on demand. In response, Fujitsu developed CYBERIUM, a cyber range in which various systems can be reproduced in a virtual environment where trainees can learn online without time or location constraints. This paper describes the usefulness of CYBERIUM.

1. Introduction

In recent years, companies have become increasingly concerned about cyber attacks and have been implementing various security measures. Even so, more and more companies are falling victim to attack.[1)] When a company is under cyber attack, employees need to have the skill to correctly select a response that minimizes the damage; in other words, the capability to respond to cyber attacks is required. However, it is difficult to learn how to respond to cyber attacks. Cyber attacks have become highly sophisticated, adapted to the system OS, middleware type, system configuration, or operational status. This makes it essential to correctly identify the problem that occurred in the system in order to take effective measures. However, it may not be possible to minimize damage by responding just with predetermined procedures. Therefore, knowledge about the workings of security measures and cyber attacks is required, as well as the skill to respond flexibly in a limited time period or environment.

Fujitsu trains and certifies human resources as Security Meisters who have the capability required to respond to cyber attacks.[2)] When training Security Meisters, system engineers who work in different locations across the country need an opportunity to experience cyber attacks that may occur in customer environments. In response to this need, Fujitsu developed CYBERIUM, a cyber range that allows the flexible reproduction of customer environments and enables online learning from remote locations.

This paper summarizes the characteristics of existing cyber ranges, and then describes the key points in the development of CYBERIUM.

2. Requirements for cyber ranges

The most effective way of learning about something is through practice based on actual experience. When learning how to respond to incidents that are difficult to actually experience, an effective method is to use a simulator to simulate the experience. Simulators are used in a wide variety of fields, such as drive simulators, flight simulators, and simulators used in lunar activity or military communication simulation systems.

A cyber range is a kind of simulator in the cybersecurity field. Cyber ranges were first developed for military applications in order to train cybersecurity specialists who could be used in cyber warfare between countries. They were developed by Israel and the U.S., which place great focus on cybersecurity as a part of national defense. Fujitsu also tried to utilize existing cyber

ranges, but it realized they were not suitable for training Security Meisters due to the following two issues.

1) Difficulty in reproducing customer systems

In existing cyber ranges, training is performed in virtual environments that reproduce the internal network of an average company. Here, cyber attacks based on advanced and carefully designed exercise scenarios are performed, and the response to the resulting incidents can be learned. This experience is extremely realistic, but it takes a considerable amount of money and time to develop a single exercise scenario. Consequently, the available types of scenarios are limited, and customization is difficult.

Fujitsu builds and operates systems for customers in many different industries. The range of target systems is wide, from business and service applications to internal use. To train Security Meisters, exercise scenarios must be customized to match this wide variety of customer systems. But this is difficult with existing cyber ranges.

2) Difficulty in providing training environments

In existing cyber ranges, training is performed by receiving instructions from teachers who have advanced and expert security knowledge. In this training, virtual machines are used that are dangerous if operated incorrectly, such as machines infected with actual viruses or on which malicious tools are installed. To prevent any attacks on external networks, group training must be performed that uses a virtual environment that is isolated from other networks.

Fujitsu tried to develop a group training system for Security Meisters at a scale that could train all system engineers who work at 89 locations across Japan. However, in most locations it was difficult to obtain the required teachers, training environment, and site, as well as the necessary number of trainees. This led to training only being held at three locations, in Tokyo, Nagoya, and Osaka.

Due to the reasons above, Fujitsu determined that existing cyber ranges were not suitable for Security Meister training.

3. Issues resolved by CYBERIUM

Fujitsu developed CYBERIUM, its own cyber range for training Security Meisters in the skills required for responding to cyber attacks. The following requirements were defined before starting development.

- Learning should be possible through virtual environments and exercise scenarios that reproduce a wide range of customer systems.
- Learning should be possible even when no teachers are present.
- Safe, online learning should be possible.

This section describes the characteristic features of CYBERIUM.

3.1 Replaceable chapters

In existing cyber ranges, virtual environments must be built that match complex and large-scale exercise scenarios. For this reason, significant amounts of money and time are required to reproduce a wide range of customer systems. In CYBERIUM, the exercise scenarios are divided into many small scenarios called "chapters," and each chapter can be replaced by another (**Figure 1**).

This division into chapters enables complex exercise scenarios to be built by combining multiple chapters, which are the smallest building blocks. As a result, a wide variety of cyber attacks that may occur on customer systems can be reproduced.

Additionally, an interface between chapters and timelines (table of contents of exercise scenarios) has been integrated. This makes it easy to reuse exercise scenario chapters by replacing them with chapters from other exercise scenarios. This also reduces the time needed for building exercise scenarios.

For example, imagine two customers: one has built both an email server and web server on Linux, and the other has built an email server on Linux, but a web server on Windows. An exercise scenario is provided for a Security Meister responsible for the first system by combining a chapter using an email server built on Linux with a chapter using a web server built on Linux. For the second system, an exercise scenario is provided for the Security Meister by leaving the email server chapter unchanged, and replacing only the web server chapter with a chapter built on Windows.

3.2 Intuitive user interface

CYBERIUM is managed by linking to virtual environments and online teaching materials from within each chapter. This enables the user to display the required teaching materials at the required time in the training virtual environment. As a result, the user can

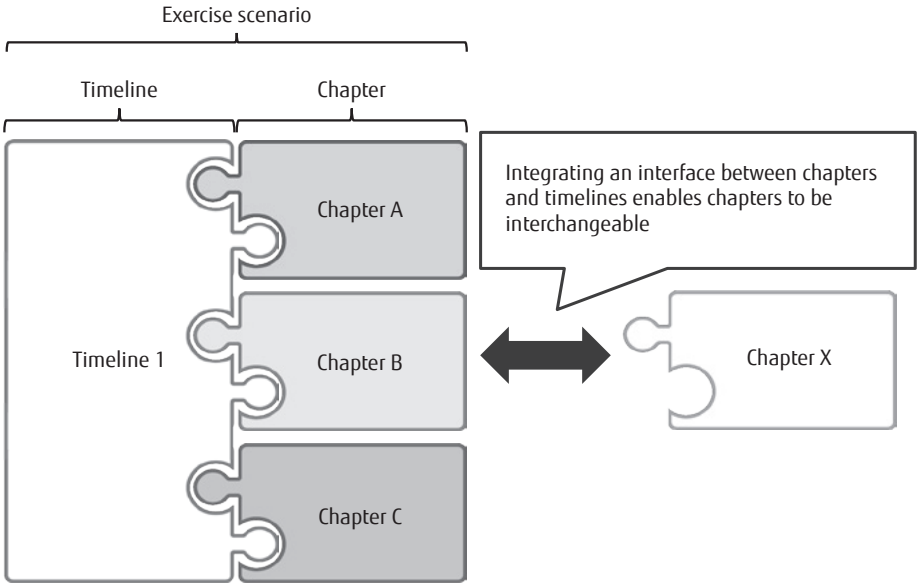

Figure 1
Configuration of exercise scenario in CYBERIUM.

be guided in detail on the next step to take and where to focus attention in the operation results.

The user can also overlay online teaching materials in the virtual environment according to the progress of training, hide the online teaching materials when they are no longer necessary, and change the size of these elements. Further, as the user requests access to the virtual environment as the exercise progresses, a dedicated console screen for the virtual environment is provided for each user account issued by CYBERIUM. This enables multiple virtual machines to be selected from a menu within the virtual environment, and makes it easy for the user to understand at a glance which virtual machine is currently being operated (**Figure 2**).

The CYBERIUM interface was developed in cooperation with Fujitsu Design Limited, and a user experience was adopted that is driven by user behavior and experience. The result is a stress-free interface that keeps users highly motivated as they learn how to respond to cyber attacks.

3.3 Safe access to isolated networks

Remote learning requires both the online operation of a virtual environment and the isolation of the environment from other networks. This is because the accidental outflow of viruses or attacks used in training exercises may damage external systems. Also, if a user accesses the virtual environment using a virtual private network (VPN), there is a risk of the user's computer becoming infected by a virus or exposed to attack.

Virtual Desktop Infrastructure (VDI) based on screen transfer is used as a technology to prevent these risks. In VDI, the client receives the screen information, and operates the virtual machine by sending keyboard and other operation information.

Usually in VDI, the user of VDI and that of the virtual machine use the same user account. In other words, the same user account used for VDI login authentication is also used for virtual machine login. This method is effective for applications that only access one virtual machine. However, it is not suitable when multiple accounts are handled on one virtual machine, or when multiple virtual machines are handled.

In response to this issue, CYBERIUM provides access from a single screen to a console connection for all virtual machines connected to the network (**Figure 3**). This enables users to safely operate an isolated virtual environment while accessing the network.

4. Benefits of CYBERIUM

Fujitsu continues to enhance the chapter components of exercise scenarios in order to increase the number of systems that can be reproduced on CYBERIUM.

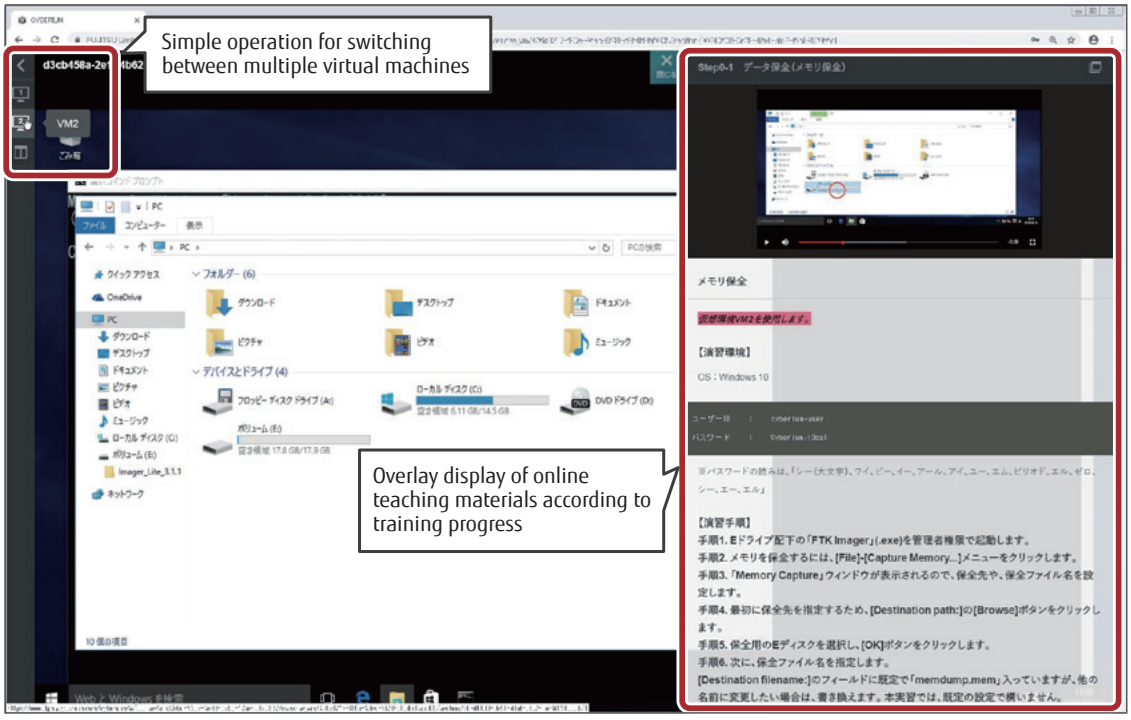

Figure 2
CYBERIUM interface.

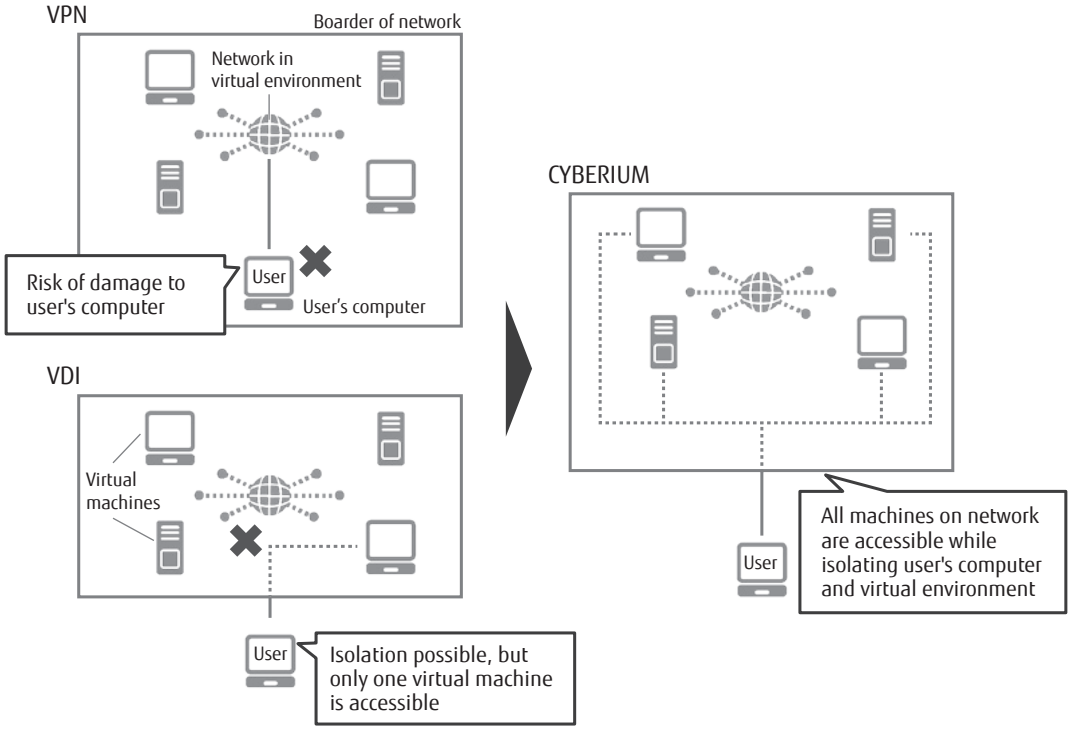

Figure 3
Access method for virtual environment.

In the six months since June 2018, 350 people have used CYBERIUM to learn how to respond to cyber attacks, resulting in their certification as Security Meisters with the capability to respond to cyber attacks. Of these, 100 people received their training from a remote location, enabling the certification of Security Meisters in regions where such training was previously difficult.

Activities other than training exercises include quizzes that test security skills, which have been configured as chapters, and security contests that have been held to measure capabilities of responding to cyber attacks. Holding events other than training led to the secondary effect of discovering new human resources.

Five hundred thirty people across the entire Fujitsu Group participated in a security contest[3] that was held over two weeks in October 2018. Of these, 120 people were new human resources who were not Security Meisters.

5. Conclusion

This paper described the features of CYBERIUM, which Fujitsu developed as its own cyber range for training Security Meisters in the skills required for responding to cyber attacks.

Fujitsu plans to expand the Security Meister to 11,000 engineers by FY2021.[4] The utilization of CYBERIUM has enabled steady progress to be made on this plan, establishing an organization where Security Meisters can protect a wide range of customer systems. In the future, Fujitsu will further enhance CYBERIUM to help us become a partner that can make customers feel safe and secure.

References

1) Ministry of Internal Affairs and Communications: Information and Communications in Japan; White Paper 2018. *http://www.soumu.go.jp/johotsusintokei/whitepaper/eng/WP2018/2018-index.html*
2) Fujitsu: Security Meister. (in Japanese). *http://www.fujitsu.com/jp/solutions/business-technology/security/secure/concept/security-meister/*
3) Fujitsu Cloud Technologies: Report from Fujitsu Cyber Security Workshop 2018 (FCSW2018). (in Japanese). *https://tech.fjct.fujitsu.com/entry/2018/12/18/095449*
4) Fujitsu: Management Direction—FY2018 Progress Review. *https://www.fujitsu.com/global/documents/about/ir/library/presentations/20181026-01.pdf*

Kazuhiro Hara
Fujitsu Ltd.
Mr. Hara is currently engaged in promoting the development of cybersecurity engineer human resources, focusing on CYBERIUM.