Q&A

INTRODUCTION OF TENABLE.IO FOR VULNERABILITY MANAGEMENT, AN IMPORTANT MEASURE TO PROTECT THE INFORMATION ASSETS OF OUR CUSTOMERS

The MUFG Bank, Ltd., based in Tokyo with 519 domestic branches and 107 overseas branches, is one of the world's leading banks. Recently, MUFG Bank introduced "Tenable.io" to automate and centralize vulnerability management in its systems. Here, we interviewed Mr. Tsunemi and Mr. Uchida about the background and benefits of the introduction.

BUSINESS NEEDS

Company: MUFG Bank, Ltd.

Revenue: 1,719.9 billion yen (non-consolidated)

Number of employees: Over 30,000

Number of branch offices: Domestic 519, Overseas 107

Industry: Finance

Impact of Tenable deployment

- By automating vulnerability management, the client has been able to make a start on centralizing management.
- The client also plans to use it to automate compliance checks to evaluate compliance with major security standards in OS and middleware settings.

Official website: www.bk.mufg.jp

Solution:

Interviewees

Atsushi Tsunemi, Deputy General Manager (Special), Cyber Security Group, Cyber Security Promotion Department

Yu Uchida, Senior Investigator, Cyber Security Group, Cyber Security Promotion Department

MUFG Bank, Ltd. Q&A

Regarding the challenge to increase frequency of vulnerability management cycles

Could you please tell us about the security efforts being made by MUFG Bank, Ltd?

Mr. Uchida: Our mission is to protect our customers' valuable assets and ensure our financial services are provided safely and stably, and to achieve this, we are developing comprehensive cyber security measures.

Mr. Tsunemi: We've launched MUFG-CERT, which is an incident response team, and we're moving forward with cyber security measures such as global SOC and the formation of a dedicated line for threat analysis. We also participate in efforts to ensure that cyber-attack information is being shared among the financial institutions and that countermeasures are put in place.

Could you please tell us about the security measures you will be prioritizing in the upcoming year?

Mr. Uchida: We are continuing to focus on areas that lead to the strengthening of our internal defense capabilities, such as information system robustness, vulnerability management, and ID access management. For vulnerability management, in particular, we're aiming to automate and centralize the process as much as possible so that we can perform the cycle of detecting, assessing, and addressing with vulnerabilities with high frequency.

Could you tell us about the challenges that led to the introduction of Tenable.io?

Mr. Uchida: Until now, we were manually running vulnerability diagnosis tools to deal with the risk of security breaches in systems open to the Internet and the risk of residual vulnerabilities in OSs and servers.

And so, as I mentioned before, to allow us to increase the frequency of vulnerability management cycles and thereby increase the level of security, one of the major challenges was that we needed further efficiency gains.

With certain vulnerabilities, the time between the vulnerability information being released and an attack that exploits it can be much shorter than what you might imagine. So, we felt that if we continued with manual vulnerability diagnosis, we might not be able to respond quickly enough to critical vulnerabilities and leave the system open to exploitation by attackers.

Mr. Tsunemi: According to security vendor research reports, until a few years ago, many of the incidents reported were those of malwares originating from suspicious emails and websites, but in recent years, the most frequent reports are those of information leaks and ransomware attacks, as a result of exploitation of servers open to the internet and vulnerabilities in devices. This tells us that the threat landscape has changed. For double-extortion ransomware, which has been causing a lot of damage recently, it has been confirmed that vulnerable VPN devices and RDP misconfigurations were targeted as breach routes. And so, it is important that we implement a more frequent cycle of vulnerability management and misconfiguration checks.

Tenable recognized for compliance checks and extensive support

Please tell us how you came to select the solution and why you chose Tenable.io?

Mr. Uchida: We gathered information and examined products and solutions from many vendors, focusing on major vulnerability scanning tools. Ultimately, we chose Tenable.io for its wide range of detectable vulnerabilities, and because it has a compliance check function to evaluate compliance with major security standards in OS and middleware settings, and because Tenable provides us with generous support in Japan.

Mr. Tsunemi: The ability to centrally manage vulnerability information on the dashboard was another of the deciding factors for our choice, as centralization of vulnerability management is what we are aiming towards.

Could you tell us about how long it took to get Tenable.io. up and running, from your initial planning stage?

Mr. Uchida: Originally, we were considering Tenable.io for the purpose of strengthening our compliance checks. Subsequently, on recognizing that we also needed to strengthen vulnerability management, we accelerated the introduction of vulnerability management in combination with the compliance check solution, starting in 2019.

We conducted a proof of concept using Tenable.io around November 2019 and decided to introduce it around June of the following year, and it has been in use in our production environment since November 2020. Since this was the first attempt at automation of vulnerability scanning for our proprietary system, we took our time to analyze issues and define our requirements. The deployment is now complete, but we plan to gradually expand the extent of use in the future and so it feels like we have only just started.

Did the deployment itself proceed without any problems?

Mr. Uchida: There were two things we wanted to achieve. One was to create a mechanism to scan the global IP addresses from the cloud, and this was not a problem because Tenable.io has a cloud scanner, and we were able to use it as soon as the licensing agreement was signed. The other was to scan for devices connected to the internal network. To achieve this, it was necessary to install an on-premises scanner server. And, as we have multiple data centers and multiple systems, it took time to determine the most efficient server location and network configuration.

The deployment allowed us to get to the start line of automation and centralization of vulnerability management

Could you tell us about the changes and benefits brought about by the introduction of Tenable.io?

Mr. Uchida: I believe that our achievement to have established the start of automation and centralization has been the biggest change. This is because we believe it is necessary to enhance our vulnerability management and compliance checks, and by extension, to enhance our internal defense capabilities. Also, we have many mission-critical systems, for which we may go on standby in case they are affected during a vulnerability scan. In order to increase the frequency of such scans, it was important to create a state where vulnerability assessment could be performed safely and securely. One of Tenable.io's plus points in this respect is that you can make detailed settings for each assessment.

Mr. Tsunemi: Maintaining the quality of vulnerability diagnosis while increasing the frequency would have been a difficult task using our old methods. So one benefit of introducing Tenable.io has definitely been that it has allowed us see the potential of automation.

Could you please tell us about future initiatives being made by MUFG Bank, Ltd?

Mr. Uchida: In the area of vulnerability management and compliance checks, as I mentioned above, we are going move forward with further automation and centralization centered on Tenable.io. Vulnerability management is also important from the perspective of increasing resistance to cyber attacks and maintaining the provision of stable financial services, and so, ensuring this is achieved will enable us to maintain customers' trust in our organization. I hope very much that we can continue to work together with Tenable to find solutions.

Please give us your thoughts and opinions on Tenable.

Mr. Uchida: Tenable has a reputation for its dedication to vulnerability management solutions. I think it is wonderful. The vulnerability analysis reports, which could only be offered by such a specialist vendor, and the webinars about how to make use of them are also useful, and Tenable is always helpful when we consult them. So I hope we can continue to work together to strengthen vulnerability management.

About Tenable

Tenable, Inc. is the Cyber Exposure company. Over 40,000 organizations around the globe rely on Tenable to understand and reduce cyber risk. As the creator of Nessus, Tenable extended its expertise in vulnerabilities to deliver the world's first platform to see and secure any digital asset on any computing platform. Tenable customers include more than 50 percent of the Fortune 500, more than 40 percent of the Global 2000 and large government agencies. Learn more at www.tenable.com.