Q&A

"VULNERABILITY COUNTERMEASURES" REQUIRED FOR GLOBAL ALLIANCES

Installation of Tenable.io Enables Low-Load Vulnerability Management — KLab

KLab offers popular well-known digital video games with a mission to "be excited by the world and yourself." The company also handles video game apps from outside Japan and is often asked about the status of its information security measures and potential vulnerabilities. KLab knew that a vulnerability management solution would help them reduce risk and stay informed of their cybersecurity status. This led the company to adopt Tenable.io. We spoke with Mr. Kihira and Mr. Fude about the process and effectiveness of Tenable.io.

BUSINESS NEEDS

Company: KLab K.K.

Capital: 5,363.64 million yen (as of Sept 2022)

Number of employees: 553 (as of Sept 2022)

Official website: www.klab.com/en

Industry: Mobile online game business

Our effectiveness:

- Provides visibility of internal assets, including management ports such as iDRAC and iLO
- The "Cyber Exposure News Feed" ensures security teams have constantly updated information on recent security events and developments
- Provides immediate insight into security status, making it easy to share security measures and security status, to game publishers and business partners.
- Delivers cloud-based vulnerability management, decreasing cost and man hours spent managing and maintaining on-prem servers

Solution:

tenable.io vulnerability management

Interviewees

Hiroshi Kihira, Information Systems Group, Engineering Division, K Laboratory

Tomoaki Fude, Technology Public Relations Group, Infrastructure Group, Engineering Division

KLab Q&A

KLab has strong technological capabilities in games and infrastructure

Could you tell us your position and the nature of your work?

Kihira: I'm in charge of two departments: K Laboratory, which is mainly engaged in research and development, and the Information Systems Group of the Engineering Division, which coordinates the technical departments. At K Laboratory, we take on interesting technical challenges, and the Information Systems Group is responsible for the overall construction and design of the company's infrastructure, including the formulation of rules and regulations.

Fude: I'm in the Infrastructure Group of the Engineering Division, and I'm primarily responsible for the cloud portion of each project, which involves building and operating the environment based on the infrastructure of the AWS cloud. I'm also in charge of the Technology Public Relations Group, which manages activities such as Twitter and technical blogs. I was also in charge of tool selection for the current vulnerability scanner.

Kihira: Rather than being 100% business, the company culture is such that I could work as an engineer while also doing interesting R&D and PR activities.

Please tell us about KLab.

Kihira: KLab was originally launched as the research and development division of CYBIRD. K Laboratory became a joint stock company and the name was changed to KLab. As a result, KLab has a strong flavor as a research and development company. We've been developing applications for mobile phones since the flip phone era, and we have been entrusted with fairly high-load systems. Our strength in that kind of infrastructure technology has led us to focus mainly on the game business. One of the features of our business is that we offer many games based on famous works.

The company has headquarters and satellite offices in Roppongi, Tokyo, as well as offices in Osaka and Fukuoka. Each location has its own engineers and creators. We also have a gaming subsidiary called Global Gear Inc. in Fukuoka and an overseas subsidiary called KLab China Inc. in Shanghai.

Fude: KLab has a "doburoku" system which allows employees to spend time doing things they like, such as research they really want to do, without supervisor approval, as long as it is no more than 10% of their standard working hours. I myself applied this time to writing articles for technical book reviews. I think it's a very good system and a great company.

Kihira: I believe that we have an engineer-friendly culture. I have been with this company for over 10 years, and I feel very comfortable here.

Tenable.io was selected for a completely cloud-based management server

Please tell us what led you to adopt Tenable.io?

Kihira: KLab's strength is in its infrastructure. When we build Linux-based on-premise servers, we start from the boot script and rebuild the kernel ourselves. When we discover a high-impact vulnerability, we rebuild from source to address it. Of course, we also implement all the security measures commonly used around the world.

As for Tenable.io, the truth is that we introduced it because we wanted to prove that we have implemented vulnerability countermeasures, especially to our overseas business partners. We are often subject to surveys and interviews about KLab's security measures when we do business with companies with intellectual property rights. In order to gain trust, it is important that the vulnerability management process, including the vulnerability scanner, is well established and effective with the ability to discover all assets and their vulnerabilities, and report on vulnerability and remediation status.

What were the reasons for selecting Tenable.io?

Kihira: In one such interview, one of our business partners mentioned Tenable and one other company as an example. And so we considered these two major companies and one open-source product as candidates. It was important that the vulnerability management solution continuously captured newly published vulnerability information and was able to update that information on a daily basis. Therefore, we decided that a commercial product which is updated on a daily basis would be better than a formal vulnerability checker, and so we narrowed down our choices to the two major companies and proceeded with trials and technical evaluation.

Based on the results, we decided to adopt Tenable.io. The most important point was that the management server is completely cloud-based and did not need to be built on-premise. On-premise servers require man-hours for maintenance and management, and vulnerability countermeasures are also necessary when the management UI is a web service. It was very important for us to eliminate this cost and man-hours. In addition, other companies' products needed to have their parameters tuned. Otherwise, huge traffic from servers overwhelmed our 'conntrack' iptables which we use at site gateways, such that connections could not be tracked and would drop out.

Fude: We conducted a 30-day trial of each, compared them, and finally decided on Tenable.io. That was in December 2021.

Visualization of all "hidden vulnerabilities"

Please tell us about the effects of introducing Tenable.io.

Kihira: Tenable.io allows us to define subnets and resources and scan them, so all assets in the subnet are picked up and visualized. This has been very effective. I like to draw network diagrams and such, so I was documenting my own company's network, but servers these days have many management ports, such as iDRAC and iLO. The size of the firmware is also huge, and the product probably is running some kind of operating system. Further, the number of vulnerabilities detected against its Web UI is high, and we realized that we need to ensure that not only the server itself but also iDRAC and iLO are updated. Tenable.io has helped manage vulnerabilities and misconfigurations, ensuring that software updates are complete. This has decreased the number of vulnerable assets.

Fude: At the top of Tenable.io's dashboard, there is a "Cyber Exposure News Feed," and just by looking at this feed, I can catch up on recent security developments. I also follow the Twitter accounts of security researchers, and the Cyber Exposure News Feed covers information that has been leaked, which gives me peace of mind.

Kihira: Recently, we had a tough time dealing with the Log4j vulnerability. Instead of general applications, the management tools, middle-ware tools, or Web UI of backup products actually have Java or Tomcat running behind the scenes, and there were quite a few cases where Log4j was included in them. Because they are included in utilities, these tend to be left installed. Tenable.io provides visualization of this and issues alerts, which gives me peace of mind.

Fude: Another feature is Frictionless Assessment. This is used for projects that require the use of EC2 spot instances, where EC2 instances are frequently launched and deleted. With this, there is concern that assets will be wasted. But by using the Frictionless Assessment feature, it is possible to reuse the EC2 instance for other things the day after it is deleted. I thought that was a very nice feature in terms of cost effectiveness.

About Tenable

Tenable® is the Exposure Management company. Approximately 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 approximately 60 percent of the Fortune 500, approximately 40 percent of the Global 2000, and large government agencies.
Learn more at www.tenable.com.

No major complaints, great usability

Are there any points that you feel dissatisfied with while using it?

Kihira: I have no complaints at all. But now that you mention it, the documents were machine-translated from English to Japanese, making them difficult to read and understand. However, I feel that overall the interface is easy to understand, easy to read, and extremely good. Also, we have had no trouble with the introduction of the system, and the merits of visualization are overwhelmingly clear. The response to the actual scanning results is also progressing as planned, so we believe we can make good reports to our customers.

Fude: In any case, it has the best usability.

Please tell us what will happen next.

Kihira: We are in the process of discussing our security structure, policies, and product implementation with senior executives. Personally, I am looking into approaches to balance security and convenience in my work. KLab still uses legacy VPNs so we would like to promote total security that includes endpoints and networks, and catch up with the latest trends such as zero-trust.

Fude: As for the future, we currently rely on our own infrastructure team to check our AWS-based infrastructure environment, but I am personally considering having it reviewed by an outside expert even though it will be expensive.

Thank you very much.