Q&A

SOMPO HOLDINGS DEPLOYS TENABLE'S VULNERABILITY MANAGEMENT AND ACTIVE DIRECTORY (AD) HARDENING SOLUTION FOR GROUP-WIDE INTEGRATION OF SECURITY PROGRAMS

BUSINESS NEEDS

Company: SOMPO Holdings, Inc.

Revenue: 100 billion yen

Industry: Insurance

Impact of Tenable deployment

- Automatic identification of assets
- Full visualization of asset risks – any user can take action from the information provided
- Vulnerability management in the cloud and on-premise, as well as Active Directory hardening and risk-reduction

Solution

tenable.ad tenable.io tenable lumin

Interviewess

Mr. Kenichiro Shimada, Product Owner, IT Strategy Planning Unit

Mr. Toshihiro Sueyoshi, Project Manager, IT Strategy Planning Unit

Mr. Toshinori Konaka, Security Evangelist, IT Strategy Planning Unit

SOMPO Holdings Customer Q&A

SOMPO Holdings is working toward establishing an SSC to centralize key operational functions

Can you give me an overview of SOMPO Holdings?

KS: SOMPO Group has been a long-standing provider of general insurance products for loss or damage of assets, since its inception as SOMPO Japan Insurance. In recent years, its business expanded beyond its original remit to include life insurance, nursing care and service for the elderly. In 2020, we started to develop our data business space, and in July 2021 founded our digital business subsidiary, SOMPO Light Vortex. We aim to expand our activities on the foundation of our insurance business, to provide the best quality service to contribute toward our customers' sense of security, safety and wellbeing, so that we may create a society where every person is able to enjoy a quality of life, each in his or her own way, with the benefit of health and affluence.

What is an SSC?

KS: An SSC is a "Shared Service Center' is a concept developed to centralize corporate functions that are common to, but which are currently performed separately by each subsidiary, such as general administration, HR, and accounts. We are working to realize this concept for the IT operations in these functions. We call this our SSC Transformation. We are transforming IT tasks so that they are provided via SSC.

SSC is also known as CoE (Center of Excellence). Instead of each subsidiary creating its own IT platform separately, we can create a unified platform for the entire group and optimize resources and costs. In terms of security, risk is more easily contained and mitigated. In addition to these two major perspectives, we are also bringing in new values that promote new working styles (where all services may be available without restrictions of location). So, we at SOMPO Holdings are also actively engaged in incorporating the latest technology in order to plan and build our SSC transformation of IT operations.

If we had adopted the approach that is still commonly practiced elsewhere, we would have built a system on the foundation or our core organization, SOMPO Japan Insurance, for the rest of the group companies to use. But we are not doing that. By not depending on that foundation, we are making ourselves free of the limitations of an insurance business organization. We believe that this departure is the major feature and strength of our project. In addition, SOMPO Holdings has other considerable strengths in terms of security. We have a research center in Israel, for example. So with all of this, we are aiming to achieve the SSC transformation of IT operations, which will incorporate much of the latest security technology, built by what we might call the "SOMPO Brand," the SOMPO way of building a security structure.

What is your day job?

KS: I belong to SOMPO Holdings IT Strategy Planning Unit, and I am mainly in charge of Group IT Governance. When a subsidiary creates a new plan for a system, it needs to be aligned with the general corporate policy as well as the business strategies of other subsidiaries, in order for it to be governed under one roof. This is where I come in, with a corporate perspective on IT governance, so that the system plans are not divergent from business plans, and in terms of cost and security, too, I check to ensure that they are in alignment with the management principles of SOMPO Group IT system.

TS: I also belong to the IT Strategy Planning Unit, where I work on alignment and uniformity of systems across SOMPO Holdings, and enforce our centralized purchasing policy. With regard to the SSC project, we are looking to implement a shared service for the group infrastructure, where we can basically share not only security management but also terminals, file servers and ID management. My role is to check the progress of the SSC transformation project from a technical perspective.

TK: I provide specific advice on security and selection of products for SOMPO Holding's group-wide projects. I also chair the Vulnerability Working Group for the Financial ISAC, which is an external organization. We meet regularly to share and exchange information. We may hear about the latest developments or projects other companies are pursuing, which helps us, too.

SOMPO Holdings' Challenges

What were the challenges that led you to deploy Tenable?

TK: We had three major challenges - to detect vulnerabilities in IT assets and reduce them by acting on them by a risk-based approach, to harden Active Directory (AD) and monitor in real time, and to increase the adoption of containers.

There are two categories of vulnerabilities in IT assets — known and unknown. Both categories need to be understood and managed properly, otherwise we will run into surprise security incidents.

We used to have various tools to do the job, but eventually it came down to manual management. Then the workload was so enormous that we were fast approaching the limit of what could be done. As for the assets, once they are detected, they need to be checked for vulnerability, and that they are correctly configured. Some have been migrated to the cloud, which means that checking the settings in the cloud is also important.

Our challenge was to understand all these correctly, so that we could reduce the points where a potential cyber attack could target. In other words, to reduce the attack surface and our exposure to the risk of attacks.

With regard to AD hardening, total removal of risk is not possible, even if we manage IT assets properly and ensure that they are correctly configured. For example, today, many threats are introduced by email. We have approximately 50,000 employees throughout our entire group in SOMPO Holdings, so you can be sure that one or two of them would, quite unintentionally, open a compromised email, which will compromise the terminal, and by lateral movement the AD controller, which will then be followed by an escalation of privileges, and access to important data. But by hardening the Active Directory, we can prevent its fraudulent access even in the event of a compromise. These were the two main challenges.

Reason and story behind choosing Tenable

How did you come to select Tenable?

TK: We already had Tenable scanners in place, and we were planning to replace them with view to rolling them out to the entire company. So we evaluated several products, and the results showed that even on the vulnerability management feature alone, Tenable was outstanding. Furthermore, as Tenable enabled configuration checks for the cloud, containers and API, as well as AD hardening and monitoring, and coupled with its cost implications, we felt that we would benefit greatly from its deployment.

The detection capability of Tenable was particularly stable and high. They are a well-established firm after all, dating back to the days of Nessus, which we felt was the source of their rich insight and excellent knowhow. So we decided to go for Tenable, and at the same time, we also added Tenable® Lumin. Now, Tenable® Lumin detects and visualizes not only vulnerabilities, but also misconfigurations in the entire environment. It also shows criticality in scores, which is effective for triage. It helps anyone to reach the same decision, which was also a key point for us.

Regarding AD hardening, Tenable first checks whether AD is hardened or not. On top of this, user activities are monitored, which help us understand what is normal and catch deviant behavior. For example, it can detect malware in lateral movement, or an attacker with fraudulent access rights taking control of a server and behaving as a legitimate user. These are also a part of the great benefits of having Tenable.

KS: Tenable was the product that could solve both of the two challenges we were facing. With SSC, we are also working to complete all the tasks in the cloud, so Tenable was an excellent fit to help us on our way to achieving zero trust in a full-cloud set up. We started our comparative evaluation in the summer of 2021 and concluded our contract with Tenable at the end of November. We now have instances set up and configuration is underway.

We hope next to work on security protection for our subsidiaries as they develop their own cloud applications. It is a kind of general strengthening of our Product Security Incident Response Team (P-SIRT) posture.

TS: SOMPO Holdings group comprises a large number of companies of varying sizes, operating in various industries. Their existing security programs are also diverse. It was a great headache for us to design a unified infrastructure for all of it. However, as each company works under the SOMPO brand, security issues have a direct impact on the value of the brand. Our Tenable deployment is also testament to our solid and robust preparation for brand protection and value creation, and we believe that it will have a positive impact on SSC transformation.

Expectations and Concerns

What do you expect to gain from your Tenable deployment?

TK: We believe we can integrate the various security schemes in place in our subsidiaries into a unified structure. Tenable Lumin will also help us visualize and take actions to mitigate risk, ensuring clarity for everyone to know which step to take. Asset management workload will be greatly reduced thanks to automation, so we expect to see a marked improvement in the security posture for the entire group.

Tenable enables us to do various things from a single product. We rate them very highly, including what they may provide in the future. Integration with Lumin is something we have high hopes for. I believe they have this on their roadmap. They also provide web application scanning features, something we would like to build our expertise on. Usability, for example, when we simulate a mock attack, can be complex and difficult. I hope that they will modify the user experience so that it will be easy to use for anyone, like their system risk view.

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.