exabeam®

CASE STUDY

LEVERAGING EXABEAM'S CLOUD-BASED SECURITY MANAGEMENT PLATFORM FOR IMPROVED INSIGHTS AND EFFICIENCY

"COMPLETELY DIFFERENT FROM THE SIEM OF A FEW YEARS AGO." Business Brain Showa-Ota Inc.(BBS) was established as an audit corporation consulting firm and system integration company, and is listed on the first section of the Tokyo Stock Exchange as a provider of a range of services from consulting to SI, business establishment, system maintenance and operation, and BPO. Speaking to Exabeam APJ Partner, Macnica Networks; Hitoshi Uehara, General Manager of Information Systems at Business Brain Showa-Ota Inc. outlines why they chose Exabeam above its competitors.

MOVING BEYOND A CONVENTIONAL SIEM SOLUTION

BBS regularly conducts information security assessments in line with the expansion of the Group's management base through M&A and new businesses. During information security assessments, issues are identified taking into

> "We considered a large number of SIEM products and integrated SOC services, but due to the high introduction cost and operational hurdles, we thought that it would be impossible to operate integrated log management with a small number of personnel, so we thought about introducing a product that facilitates log management for each device. At that time, I was introduced to Exabeam from GSX, and with this product, we could use existing logs without replacing equipment. I was fascinated by the fact that the part that humans need to analyze could be greatly reduced, and that it would be possible to grasp the situation simply by following what is displayed in Exabeam."
>
> HITOSHI UEHARA, GENERAL MANAGER OF INFORMATION SYSTEMS AT BUSINESS BRAIN SHOWA-OTA INC.TELECOMMUNICATIONS

INDUSTRY

Financial Services

EXABEAM PRODUCTS

- SaaS Cloud Essential SIEM
- SaaS Essential Cloud Connectors

consideration not only changes in the IT environment but also changes in social conditions. Improvements to promote security measures include the introduction of sandbox products on the network and next-generation endpoint products.

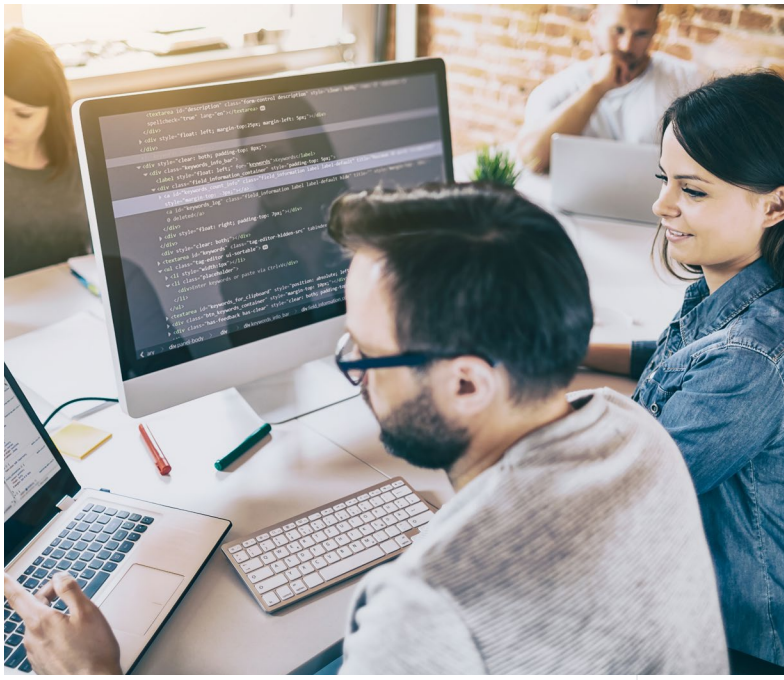
Within this backdrop, BBS, as an operator of security products, servers, and network products collects and stores logs, but only searches for the necessary data from a huge amount of logs in the event of an emergency. So, they started to wonder if they could come up with ways to make effective use of these saved logs.

As a result of the latest information security assessment, the construction of a platform for monitoring, analyzing, managing, and accumulating logs was identified as an important issue. In particular since April 2020, due to the influence of COVID-19 with increasing numbers of people working from home,the above-mentioned issues became even more urgent.

UTILIZING LOG SETS WITHOUT REPLACING EXISTING EQUIPMENT

"Up to that point, it was necessary to see alerts and logs from various devices, and a great deal of man-hours were spent investigating and responding to suspicions of minor incidents that occur on a daily basis. In addition, we also wanted to drastically improve the system of individuals with product knowledge needing to provide support," says Uehara.

"We considered a large number of SIEM products and integrated SOC services, but due to the high introduction cost and operational hurdles, we thought that it would be impossible to operate integrated log management with a small number of personnel, so we thought about introducing a product that facilitates log management for each device. At that time, I was introduced to Exabeam from GSX, and with this product, we could use existing logs without replacing equipment. I was fascinated by the fact that the part that humans need to analyze could be greatly reduced, and that it would be possible to grasp the situation simply by following what is displayed in Exabeam."



OVERCOMING IMPLEMENTATION HURDLES OF TRADITIONAL SIEM SOLUTIONS

"Conventional SIEM products have many implementation hurdles, and we couldn't see how they could be operated continuously in-house. In particular, since "detection conditions" needed to be set, specialized knowledge and support would be required, and we got the impression that it would be necessary to continuously train and newly hire people with such skills," says Uehara.

Exabeam UEBA supports flexible log sources, it can handle text-based logs. Even if the relevance is not easily grasped by the human eye from those logs, Exabeam automatically organizes and links the relevance to show it in an easy-to-understand manner.

MAKING SENSE OF A GROWING NUMBER OF LOGS AND MITIGATING INSIDER THREATS

"Even if you just look at the logs of one device, it is very difficult, and it is difficult to link the logs. Users and terminals are linked from various logs and shown on the timeline without permission, so even if you do not have advanced skills, you can quickly grasp the situation," says Uehara.

"It had previously been difficult to detect internal fraud at an early stage, but Exabeam scores all suspicious activities, so you can understand at a glance what is different and how it is different. Another advantage of Exabeam is that it does not require advanced skills."

ADJUSTING A COVID-FRIENDLY WORLD

"Due to COVID-19, teleworking has increased rapidly as part of the measures to counter the pandemic," says Uehara, adding that "the way employees work changed drastically, we must change to a more secure network configuration. We would like to import the logs of the services used into Exabeam more and more. We believe this is an advantage of Exabeam, which does not change the cost even if the amount of logs to be captured increases. Even in a teleworking environment, we feel that it is our mission to improve the IT environment so that people can utilize IT systems more safely and with greater peace of mind."

KEY BENEFITS

- Increased visibility
- Cost savings
- Increased efficiency

ABOUT EXABEAM

From the CISO to the analyst, Exabeam helps security teams outsmart the odds by adding intelligence to their existing security tools – including SIEMs, XDRs, cloud data lakes, and hundreds of other business and security products. Out-of-the-box use case coverage delivers repeatable outcomes. Behavioral analytics allows security teams to detect compromised and malicious users that were previously difficult, or impossible, to find. And alert enhancement and automated timeline creation help overcome staff shortages by minimizing false positives and reducing the time it takes analysts to detect, triage, investigate, and respond to incidents by 51 percent. For more information, visit https://www.exabeam.com.

TO LEARN MORE ABOUT HOW EXABEAM CAN HELP YOU, VISIT EXABEAM.COM TODAY.