exabeam®

CASE STUDY

HELPING JUPITER TELECOMMUNICATIONS FIGHT INTERNAL FRAUD ACROSS A DISPERSED ENVIRONMENT

PARTNERING WITH JAPAN'S LARGEST CABLE TV PROVIDER FOR BETTER VISIBILITY AND ANALYTICS. Founded in 1995, Jupiter Telecommunications Co., Ltd. operates telecommunication businesses throughout Japan. The company provides cable television broadcasting, cable internet, cable telephone, and consulting services. Speaking to Seio Ohara of Exabeam APJ Partner, Macnica Networks; Hideki Tsutsui, Cybersecurity Manager at Jupiter Telecommunications outlines why they chose Exabeam above its competitors.

> "The biggest evaluation point is how much we can capture our logs. No matter how good the detection capability is and it can respond to unknown threats, it cannot be analyzed without the prerequisite data. A closer look at log capture revealed that the flexible Exabeam Advanced Analytics was overwhelmingly advantageous."
>
> HIDEKI TSUTSUI, CYBERSECURITY MANAGER AT JUPITER TELECOMMUNICATIONS

INCREASED COMPLEXITY AND SCALE THROUGH A SERIES OF BUSINESS ACQUISITIONS

First of all, what kind of security issues did J:COM have?

"We had expanded as we acquired various corporations such as cable TV stations, but the security level varied depending on the corporation.

INDUSTRY

Telecommunications

EXABEAM PRODUCTS

- Advanced Analytics
- Threat Hunter

Therefore, as a company, we set a security level baseline, and after external threat countermeasures, we decided to embark on internal fraud countermeasures. We hadn't had any particular incidents related to internal fraud, but we heard of incidents at other companies and as we have millions of personal information about our customers, we felt establishing strong internal fraud countermeasures were essential," says Tsutsui.

Why did you choose Exabeam's Security Management Platform as an internal fraud countermeasure?

"When I launched the project, I didn't know how to monitor internal fraud in the first place. As the first approach, we conducted threat modeling with field personnel from various departments such as in-house sales and customer centers to deal with cases targeted by the company, such as leakage of contractor information held by the sales department. As a result, I came to the conclusion that it would be better to use the logs that we already have in large quantities to detect abnormal behavior, and when I consulted with Macnica Networks, we decided to go with Exabeam, taking advantage of log analysis and machine learning to detect user's fraudulent behavior."

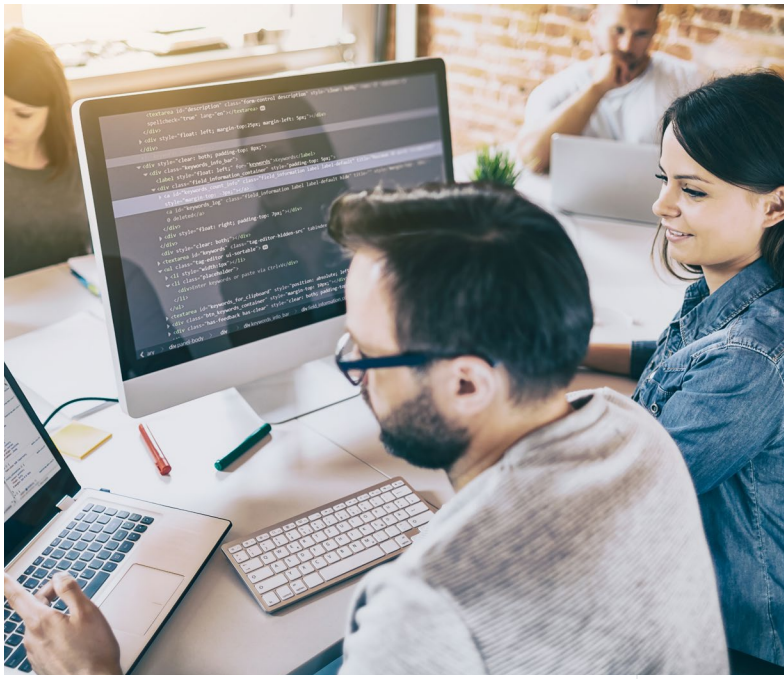
There are other companies that use UEBA, but what was your particular evaluation of "Exabeam Advanced Analytics"?

"First of all, Exabeam's products have been selected as a Gartner leader. Among them, one of the products that can be procured in Japan was "Exabeam Advanced Analytics", so I chose it. The biggest evaluation point is how much we can capture our logs. No matter how good the detection capability is and it can respond to unknown threats, it cannot be analyzed without the prerequisite data. A closer look at log capture revealed that the flexible Exabeam Advanced Analytics was overwhelmingly advantageous."

EFFICIENT ROLLOUT AND WORLD-CLASS SUPPORT

In order to capture logs using UEBA, you need a "parser" that understands and analyzes the logs of asset management tools. How did this development go?

"It was encouraging both in terms of functionality and support, as it implemented the parser developed by Exabeam instead of developing the parser at our company."



That is the difference from other companies' products. If you develop a parser in-house, you will have to recreate the model for learning and the rules for fraud detection, which tends to narrow the scope of support. In that respect, Exabeam does not have these drawbacks. Was there any other deciding factor for the introduction?

"I also highly appreciate the earnest efforts of Macnica Networks and Exabeam. Of course, we didn't know the specifications of the product, but we were able to trust it with the careful support. The project itself came up in the fall of 2018, and it was talked about entering the POC from the end of March, and from April we started importing using the real logs that we had accumulated. We asked Exabeam to develop a parser during the Golden Week period, and continued POC until August while making fine adjustments. As a result, we were able to properly acquire the log of the desired event such as PC operation history, so we decided to introduce it. After that, we placed an order in September and cutover in October, so I think it went smoothly."

FUTURE GOALS AND IMPACT

"A traditional SIEM generally adds log-based charges, but since this product is user-licensed, you can rest assured that the charges will not increase even if the types of logs you want to import in the future increase. It's only a short time since the operation started, but of course it's not the end of the introduction, and in the future we will still have to produce results through internal fraud countermeasures. Currently, it is not possible to completely prevent intrusion of threats from the outside, and how to detect them after after they're already inside our environment is an issue for security in general, but by accumulating know-how on internal fraud countermeasures, we expect that "Exabeam Advanced Analytics" can be used as a countermeasure for detection after intrusion."

KEY BENEFITS

- Internal fraud detection
- Flexibility
- Increased visibility
- Predictable cost model

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.