exabeam

CASE STUDY

NTT DATA SPINS UP A GLOBAL SECURITY VIEW WITH EXABEAM SIEM

NTT DATA is one of the world's leading providers of technology and services. Founded in 1988, the company has a global team of more than 129,000 employees in over 50 countries and regions. NTT DATA is transforming its previous role as a systems creator into a global business partner leading the way to international business success. The Japan business unit alone has 34,500 employees and is a dominant player in public administration and financial services. It also serves an array of customers in construction, real estate, manufacturing, logistics, retail, broadcasting, media, advertising, communications, transportation, and energy. Consolidated annual net sales were ¥2.1 trillion (US$18.9 billion) as of 31 March 2019. Shares of the company are publicly traded as NTT DATA (TSE:9613).

> "Having Exabeam's unlimited data lake and attractive pricing model made the difference for our large organization."
>
> **HIROSHI HONJO, HEAD OF CYBER SECURITY AND GOVERNANCE, NTT DATA CORPORATION**

BUSINESS CHALLENGE

The rapid pace of NTT DATA's transformation and growth strategy has included many company acquisitions and the inheritance of legacy technology platforms. The confluence of these disparate systems raised concern by executives for cybersecurity and compliance. "Our customers have very high expectations of us, especially in Japan, which means any security issue can cause serious damage with global effect," says Hiroshi Honjo, head of Cyber Security and Governance at NTT DATA.

The business challenge for NTT DATA security was managing multiple legacy security and information event management (SIEM) platforms left over from its business acquisitions. Legacy capabilities were unable to analyze all the operational and security data, which had increased by orders of magnitude over the past five years and was growing rapidly. In addition, legacy SIEM pricing models based on log volume were cost prohibitive for the company's massive global operations.

"We needed a solution that would look at the complete picture with better means of risk detection and tracing," says Honjo. Also required was a way to demonstrate compliance with international regulations such as the EU General Data Protection Regulation. "It was time to make the right IT infrastructure investments," he says.

VENDOR SELECTION AND PROOF OF CONCEPT

As security experts, Honjo's team was aware of severe limitations in legacy SIEMs caused by reliance on correlation rules. The company's mandate was to get deeper visibility on modern threats that evade rule-based detection. It also sought functionality that would streamline the labor that goes into detection and analysis using conventional methods, according to Honjo.

NTT DATA chose Exabeam over several competitive options. Criteria included cost model, multi-tenant compatibility, user and entity behavior analytics (UEBA) functionality to leverage machine learning and big data, available support locations, and multilingual support. "Having Exabeam's unlimited data lake and attractive pricing model made the difference for our large organization," says Honjo.

For the Tokyo office, the proof of concept and migration occurred from August through November 2018. While the project was a significant upgrade, initial rollout moved quickly due to skilled experience with legacy SIEMs held by the security team and collaboration with Exabeam engineers. Priorities were decided rapidly and teams focused on establishing data ingestion to support behavioral analytics of selected use cases.

QUICK DEPLOYMENT OF 50 USE CASES

Deployment in the early part of 2019 at Japan headquarters is gradually extending to North America, Europe, and Asia-Pacific. With the migration, NTT DATA is decommissioning all legacy SIEMs. To drive the change, implementation teams helped speed the use of more than 50 use cases. Use cases are unique security scenarios to which the Exabeam SIEM is applied for detection, tracking and remediation. Fifty use cases are an aggressive start for many SIEM deployments, but Exabeam eases the process by providing support models for more than 400 use cases.

Among the top use cases selected by NTT DATA was Compromised User Credentials, which is the primary vector for data breaches according to the Verizon 2018 Data Breach Investigation Report. UEBA capability detects unauthorized access across the combination of a user's account credentials, devices or IP addresses. Privileged-user Compromised was another chosen use case because when a hacker obtains a privileged user's credentials, the attack appears to be "normal" activity to legacy SIEMs. Exabeam's UEBA technology is able to distinguish malicious behavior with privileged credentials. The Insider Access Abuse use case implemented by NTT DATA takes detection a step further by determining when a privileged insider is performing risky activities that are outside of their normal baseline.

NTT DATA's aggressive rollout of use cases had two goals: to bolster its own detection and response capabilities, and to gain experience that would benefit its commercial and government customers.

exabeam

BRINGING EXABEAM TO NTT DATA CUSTOMERS

"Exabeam is a valued partner to NTT DATA," says Honjo. "We use its solution to protect our international business. Now we are offering the same solution to our own valued customers." According to Honjo, NTT DATA's top clients spend large budgets to protect their enterprises. Their legacy SIEMs share the same limitations of threat detection and tracking and they have the same need for a behavioral analytics-based approach. All have the same budget sensitivities to legacy pricing models that don't fit big data. "Our hope is to help our customers understand how Exabeam SIEM is the right approach for securing the global enterprise," says Honjo.

KEY BENEFITS

NTT DATA has seen specific benefits from its Exabeam deployment:

- Stronger global enterprise security and compliance with behavioral analytics of unlimited amounts of security data
- Deeper visibility on enterprise risks and a proactive method of addressing security issues
- An international solution that supports unlimited data with a flat pricing model

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

ABOUT EXABEAM

Exabeam is the Smarter SIEM™ company. We empower enterprises to detect, investigate, and respond to cyberattacks more efficiently so their security operations and insider threat teams can work smarter. Security organizations no longer have to live with excessive logging fees, missed distributed attacks and unknown threats, or manual investigations and remediation. With the Exabeam Security Management Platform, analysts can collect unlimited log data, use behavioral analytics to detect attacks, and automate incident response, both on-premises or in the cloud. Exabeam Smart Timelines™, sequences of user and device behavior created using machine learning, further reduce the time and specialization required to detect attacker tactics, techniques, and procedures. https://www.exabeam.com.