exabeam

Case Study

Equipping Swedbank With the Tools to Carry Out Faster, More Complex Investigations

Swedbank

Industry
Finance

Exabeam Products
Data Lake | Cloud Connectors | Advanced Analytics | Threat Hunter

Expanding visibility into increasingly dispersed systems and preparing for more mature adversaries.

One of the world's 100 largest banks, Swedbank is a Nordic-Baltic banking group with subsidiaries in Luxembourg, Estonia, Latvia and Lithuania and a presence throughout Scandinavia as well as the United States, South Africa and China. Swedbank offers retail banking, asset management, financial, and other services to more than 7.3 million private and 546 000 corporate customers globally.

> We were impressed by how we were able to leverage Exabeam to help identify the real user within an environment where that user might have multiple identities, and how easily the people who have to use the solution on a daily basis were able to do so.
>
> **Jan Willekens**
> APO Cyber Defense Center & Cyber Security Incident Manager
> Swedbank

Securing a Global Financial Network Safely, and Efficiently

Operating in an environment that relies heavily on trust, compliance and speed, the Swedbank team understood that, as adversaries and their tactics become more mature, so too should the technology used to defend against them.

“What prompted us to lifecycle our existing tool was the increased maturity of the adversaries out there, as well as their ability to hide within different technologies,” said Jan Willekens, APO Cyber Defense Center & Cyber Security Incident Manager, Swedbank.

Another reason Jan’s team knew they needed a more modern solution was the lag in performance of their existing tool and from a strategic perspective, the need to enact policies like data loss prevention, privilege access management and business-critical use cases like safely managing SWIFT.

Why Exabeam

When the time came to look at different vendors, a key consideration for the Swedbank team was finding an extensible system, particularly one where they could write custom rules and build custom models within the user behaviour analytics tool; something not all solutions facilitate.

“We needed to be able to let our own data scientists go in and, based on what our specific needs were, customize rules and create custom models,” said Jan.

PCI compliance and the ability to monitor the PCI environment was another important factor, one that adds additional performance requirements to an already high-performance team. To that end, whichever solution Swedbank chose would have to be able to handle masses of log data, empower their team with the ability to conduct quick searches and be built on a modern tech stack to match their own.

Exabeam ultimately won out based on the above requirements, as well as having a predictable pricing model that meant more consistent budgeting going forward.

“Catching More Bad Guys” with Exabeam

Straight off the bat, the Swedbank team noticed that, with Exabeam’s performance they were able to look at greater volumes of interesting degradation use cases, giving Jan’s team the ability to increase the number of threat intelligence searches they carry out. They were also able to look at more complex detection use cases, like scouting for rogue devices on the network.

“With Exabeam we’re able to see incidents that we weren’t able to before. That’s a big one, essentially we’re able to catch more bad guys,” said Jan, adding that they’ve cut down on triage and investigation time significantly.

The time Jan’s team is saving has contributed greatly to efficiency and, generally, a happier team, because they’re able to carry out more investigations… more quickly.

Separating Normal From Abnormal Behavior

When looking at cyber threats, a key aspect of detection is the ability to establish a baseline of what normal behavior is, in order to quickly pick up on the abnormal, another is how well your tools are able to present the data you've collected.

For the Swedbank team, a notable benefit is the ability to establish baseline behavior, organize large volumes of data AND easily navigate the tools they use, ultimately to support triage and investigation in a manner that boosts their own efficiency.

"We were impressed by how we were able to leverage Exabeam to help identify the real user within an environment where that user might have multiple identities, and how easily the people who have to use the solution on a daily basis were able to do so," said Jan.

Key benefits

- Greater visibility
- Reduced time to triage
- Faster threat intelligence searches
- More complex detections

About Exabeam

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 repeatedly delivers successful outcomes. Behavioral analytics allows security teams to detect compromised and malicious users that were previously difficult, or impossible, to find. Automation helps overcome staff shortages by minimizing false positives and dramatically reducing the time it takes to detect, triage, investigate and respond. For more information, visit www.exabeam.com.

exabeam

To learn more about how Exabeam can help you visit exabeam.com today.