exabeam

CASE STUDY

BERKSHIRE BANK GAINS BETTER VISIBILITY INTO INSIDER ACTIONS WITH EXABEAM

Easier Correlation of Anomalous Events and Automated Timeline Creation Improves ROI

Established in 1846 and headquartered in Boston, Berkshire Bank is one of oldest and largest banking institutions in Western Massachusetts. It takes pride in providing excellent service and innovative performance, calling itself "America's Most Exciting Bank," based on people, attitude, and energy.

Like any financial institution, Berkshire Bank must protect customer information and assets. Additionally, since the bank deals in mortgage and insurance products, protecting customers' data is critical in an era of increasingly strict privacy regulations. Addressing these concerns requires technologies that help its security team meet the challenges involved in detecting and remediating both external and insider threats.

Consequently, Berkshire Bank looked at vendors that could help it gain more visibility across the organization to prevent data loss. For example, it wanted the ability to assess and quickly determine whether or not a given behavior was high risk. Leveraging such visibility as a way to protect data from insider threats was a main use case that prompted the bank's team to evaluate Exabeam and its next-generation SIEM system.

VENDOR SELECTION AND PROOF OF CONCEPT

Berkshire Bank's IT group divides projects into two phases: discovery and execution. In discovery, it looks at various vendors, then has the most promising demonstrate how their solution will best suit the bank. "Right away we were able to see value from what Exabeam provided as proof of concept," recalls Ryan Melle, SVP, CISO.

"With our previous data loss prevention (DLP) solution, alerts would come in such as 'Somebody tried to send something out, but it got blocked'. But with Exabeam, we're now able to detect if someone attempted to do that multiple times—or if they tried to send something out through email. And after being blocked, we can detect if they loaded something onto a USB drive or tried to print it."

"By bringing all the data from a specific use case into Exabeam, we were able to tie it all together, and then immediately generate a timeline showing what the user was doing," continues Melle. "Given that view we could determine right away whether this activity was malicious or—more likely—normal behavior for that type of user."

"Now we have all the information we need in one place, and have it all correlate in a user-friendly timeline, so we can immediately act on it," says Melle. "The value and benefits we're seeing—by being able to tie all this data together—provides tremendous efficiency. And it's an advantage for my security operations team to be proactive rather than reactive."

EASE OF USE MEANS SHORT RAMP-UP TIME

Berkshire Bank's IT leadership also wanted a system that any analyst could easily use, without having to be an expert in building out a SIEM or understanding how to configure systems.

SOC Analysts of All Skill Levels Can Quickly Assess Threats Using Exabeam

"With Exabeam, any analyst can sit down and—without extensive training—really understand our system use cases and be able to easily drill down to the core of what happened—where a threat came from, who to escalate to, and similar actions."

RYAN MELLE, SVP, CISO, BERKSHIRE BANK

During the execution phase, Exabeam further eliminated the problem faced by many IT departments—where they immediately have to add staff to manage a new system. Berkshire Bank's policy is that whichever system they introduce, they don't have to bring in experts, take time learning the system, or go through training—because that adds costs. Melle says, "There weren't hidden costs with the Exabeam solution. I can have junior level, or not-so-extremely technical people jump on the system and use it right away. Exabeam's automated timeline building also frees up my senior team to focus on more important matters, rather than training people."

ENABLES TEAMS TO FOCUS ON WHAT MATTERS

Another Exabeam benefit that the bank's security team likes is its ability to cut out the noise. With prior solutions, much of the information pulled from logs and data from multiple systems the team just didn't need. Instead, collecting it all in Exabeam makes it possible for the team to focus on what really matters. "It has saved a lot of analysts' time: My team isn't constantly digging and hunting for items that really aren't of any consequence," concludes Melle. "With the data being fed into Exabeam, they can comb through exactly what it is we need to see, exactly when we need to see it. All of the noise associated with that is filtered out."

Berkshire Bank's SOC experts also value the ease with which they can choose various use cases, run daily reports, and use dashboards to immediately deal with critical incidents—rather than having to laboriously pull data from multiple systems and correlate information. This provides them with a single pane of glass from which it's easier and faster to get visibility into what is happening across the organization and escalate high-risk user activity.

KEY BENEFITS

Berkshire Bank has seen specific benefits from its Exabeam deployment:

- Improved ROI by enabling broader use of personnel with varying skill levels to monitor for anomalous user behavior
- Single pane of glass makes it easier and faster to get visibility into what is happening across the organization and escalate high-risk user behavior
- Faster response to critical incidents