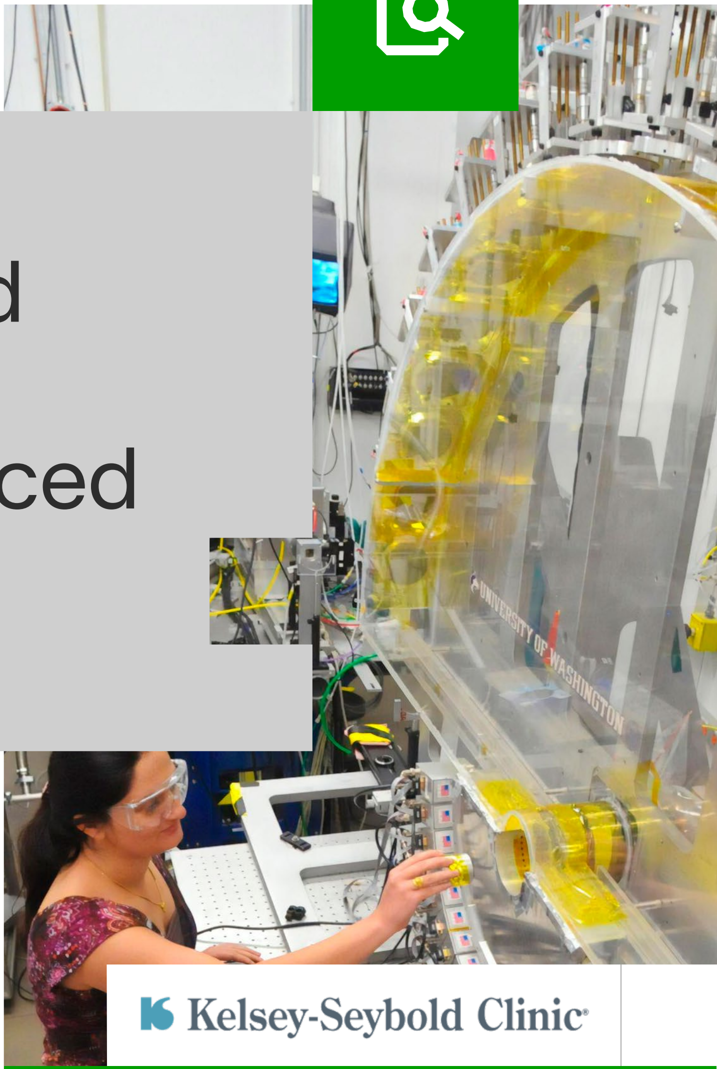
exabeam

Case Study

The Kelsey-Seybold Clinic Partners with Exabeam for Advanced Threat Hunting and Powerful Analytics

Industry	Exabeam Products
Healthcare	Data Lake | Advanced Analytics | Threat Hunter



Kelsey-Seybold Clinic

Bringing greater visibility, with a competitive price point and meaningful security insights.

The Kelsey-Seybold Clinic is a large multi-specialty clinic system operating 19 locations with more than 350 physicians throughout the Houston area. With its administrative headquarters in Pearland, Texas the clinic system is a major provider of healthcare for Greater Houston, its surroundings, and is a 5 star Medicare Advantage health plan.

> With Exabeam we're able to go back to the business and say with some intelligence that we are watching what the users are doing. We can see activity across the board, and we have something that's showing us, based off of what this person normally does, that they could be an outlier, and that we should investigate. We can document our investigations and move on with other operational tasks.
>
> **Joe Horvath**
> Manager, Enterprise Information Systems Security
> Kelsey-Seybold Clinic

More Than Just a Checkbox

The healthcare industry has long been a favorite target for cyber attacks, as medical groups host vast amounts of sensitive personal data as well as patients' financial information. The Kelsey-Seybold Clinic is no different, and the team there saw that the security landscape had evolved to where a SIEM now forms an integral part of any cybersecurity posture.

"In the past, SIEM might just have been a checkbox, but now it's become a tool for us," says Joe Horvath, Manager, Enterprise Information Systems Security at Kelsey-Seybold Clinic.

At the time, the Kelsey-Seybold team was using Logrhythm, but needed to find a more cost-effective and adaptable SIEM solution that could ingest and make sense of masses of data, but also a solution with more flexible hardware configurations and personalization.

"We were running Logrhythm for quite a long time, really as a checkbox rather than a security solution and my concern was that we were really not getting any meaningful security utility out of our SIEM. The landscape has evolved to a point where your SIEM needs to be an integral part of your security solution," says Martin Littmann, Chief Information Security Officer at Kelsey-Seybold Clinic.

With their old solution, the team had to decide which logs and events they would be able to act on while discarding other potentially critical events; as the system wasn't able to give them an overall snapshot of what was happening in their security environment.

"We have more tools, more cloud presence, more places that are sources of logs. And quite simply, we couldn't keep up with the demand, so we had to make decisions like picking and choosing and saying: hey, we can only bring this data source in or we can only bring this data source in," says Joe.

Vendor Selection and Proof of Concept

Having made the decision to scout for a new SIEM solution, Littmann's team considered other vendors like Splunk, but did so knowing that they needed a next-generation SIEM. Exabeam's powerful automation meant that the Kelsey-Seybold Information Security team, which had both incident response and operational responsibilities, could remain relatively small and agile while carrying out threat hunting and response at speeds more akin to much larger SOCs.

"In our team specifically, we have a handful of folks, and they have both operational and IR responsibilities. So there's not a lot of bandwidth to go just threat hunting without having any level of direction of where you need to go," says Horvath.

Leveraging UEBA to Make Sense of Masses of User Data

Healthcare organizations deal with a lot of patient data, and much if not all of it comes with strict regulations. Add to that the fact that the data changes often, they have to be able to correlate everything that's coming in from across the organization. Leveraging Exabeam's powerful UEBA capabilities, the Kelsey-Seybold team is able to refine security alerts coming in and distill them into meaningful actions without overwhelming the team.

This doesn't mean limiting the amount of data coming in, however, but rather being able to compartmentalize what's critical and acting on it in a timely manner. This has improved the team's efficiency as they're able to accurately look at the risk scores of employees and act accordingly.

"With Exabeam we're able to go back to the business and say with some intelligence that we are watching what the users are doing. We can see activity across the board, and we have something that's showing us, based off of what this person normally does, that they could be an outlier, and that we should investigate. We can document our investigations and move on with other operational tasks," says Joe.

Strengthening the Culture of Trust

A significant factor for Martin's team is trust. Kelsey-Seybold Clinic's entire security program centers around the trust they've built with executive management. To date, the security investments Martin and his team have made have worked towards safeguarding that trust and has meant that the Clinic benefits from a higher security profile than many other organizations.

In order to achieve that, cybersecurity purchases have to provide meaningful outcomes, just as the Kelsey-Seybold Clinic provides meaningful care to its patients.

"Our process provides a lot of meaning to the overall health of the security of the organization," says Littmann.

Key benefits

- Operational efficiency
- Greater visibility
- Business agility
- Cost savings
- Faster insider threat detection

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.