Reveal security

CASE STUDY

LifeLabs Mitigates Security Risk in Applications with Reveal Security

Company Profile

With a legacy of serving Canadians for over 50 years, LifeLabs has evolved into the largest medical diagnostic services provider in Canada. Operating from over 400 locations across the nation, LifeLabs manages an immense volume of sensitive patient information daily. This significant responsibility has propelled the company to adopt a robust security stack comprising top-tier tools to ensure that data and systems are exclusively accessed by authorized personnel. In pursuit of this, LifeLabs turned to Reveal Security, a decision that has provided them with invaluable insights into how users and other identities are interacting with their applications and actionable guidance that has enhanced their data protection.
Mike Melo is LifeLabs' CISO. He recently sat down with us to tell the story of what life was like before the adoption of Reveal Security and what he has achieved since deployment.

Challenge

LifeLabs manages vast amounts of sensitive data in multiple applications that are accessed by many users across the company. With a growing business in a highly regulated industry, they knew they did not have good enough visibility into user activity in their applications that hold sensitive data. This lack of visibility also put the organization at risk of insider threats. With patients' medical records at risk, it was imperative that LifeLabs do everything possible to better understand user activity and application usage to ensure that security policies and laws were upheld. This problem is not unique to LifeLabs or the healthcare industry. It's a global issue illustrated constantly by the number of data breaches that involve identity compromise and occur without the organization involved even knowing there has been an incident for over months or even years. This delay between the initial breach and detection exposes the organization to increased risk of heavy fines, reputational damage, and substantial costs to remediate.

The lack of visibility into user behavior in and across applications drove LifeLabs to try to instrument their environment with mostly ineffective home-grown solutions. These solutions didn't deliver the needed results and proved complex and costly to maintain in the normal operation of a fluid organization.

Results

- Accurate detection of insider threats and identity-based attacks in and across applications
- Detection of both known and unknown threats
- Reduced MTTD and MTTR

> "Using Reveal Security, we've been able to reduce MTTD and MTTR by over 50%"
>
> — Mike Melo, CISO, LifeLabs

Solution

With the addition of the Reveal Security platform to their security stack, LifeLabs can now accurately detect abnormal user behavior in applications without adding stress to their SOC team. According to Melo, "with Reveal Security, we get an extremely accurate representation of how our users and identities are interacting with our data and application systems."

> "With Reveal Security, we get an extremely accurate representation of how our users and identities are interacting with our data and application systems."
>
> — Mike Melo, CISO, LifeLabs

The solution uses unsupervised machine learning to detect anomalous user behavior in and across applications. A highly accurate detection solution, each anomaly identified by the platform warrants further investigation. This reduces noise and alert fatigue, and provides actionable insight that allows LifeLabs to dramatically improve its security response.

Results

With Reveal Security in place, Melo sleeps more soundly, knowing that LifeLabs is now more able to meet the stringent regulatory and contractual requirements for data protection that previously proved so challenging. They have been able to reduce mean time to detect and mean time to respond by over 50%. Melo notes, "having a solution that we can rely on during any sort of threat detection whether it's known or unknown is huge for us."

Melo's security analysts are more engaged, responsive, and effective. For the first time, they are able to easily detect, investigate and respond to insider threats and identity-based attacks in their critical applications. Melo added, "my team doesn't have to be sold on it. They just love using it."

About Reveal Security

Reveal Security quickly and accurately detects insider threats and identity-based attacks in and across SaaS, cloud and on-premises applications. The Reveal Security platform is the only solution in the market based on patented Identity Journey Analytics™ technology that uses unsupervised machine learning to learn the usage patterns or typical "journeys" of human and machine identities in applications and uses it to detect anomalies. This approach delivers a superior level of accuracy and context, reduces alert volumes by orders of magnitude, and enables the business to respond quickly before a material breach can occur.

For more information, visit www.reveal.security