Reveal security

CASE STUDY

Reveal Security: No Fraud at this Bank

Large bank uses the Reveal Security platform to protect against internal and external fraud

Company Profile

A large financial-services institution has been in business for more than a century. From humble beginnings and through steady organic growth boosted by numerous acquisitions and consolidations, it now serves over 2 million customers via 200 branches. Employing 7,000 professionals, the bank offers a broad range of investment, commercial, and retail banking services including commercial, mortgage, auto and personal loans, credit cards, insurance, checking and savings accounts, and wealth management services.

Challenge

To meticulously protect its operations and customer transactions, the bank employs a well-equipped Security Operations Center (SOC) managed by a team of security analysts.

Prior to deploying Reveal Security, the security team spent a significant amount of time building detection rules for their SIEM, in order to detect internal and external fraud attempts.This approach is tedious and time-consuming for the analysts and resulted in their SIEM generating a lot of alerts, including many false positives. Furthermore, rules-based detection approaches such as this can detect only known threats and miss unknown or novel techniques.

The team was compelled to look for a solution that could improve their ability to quickly and accurately detect suspicious and malicious activity in their business critical applications, without generating so much noise in the SOC.

Results

- SecOps team has a streamlined and effective approach to keep the bank in compliance and protected from fraud
- The Reveal Security platform reduced alerts by 99%
- Typical MTTD and MTTR were cut by half

> “Reveal Security has transformed how we protect the bank against internal and external fraud. What took weeks for our security analysts, now takes hours.”
>
> — CISO, Large Bank

Solution

The Reveal Security platform accurately detects insider threats and identity-based attacks in and across applications and cloud services.

For financial institutions, the Reveal Security platform delivers a breakthrough approach to internal and external fraud detection. It's the only solution based on patented Identity Journey Analytics™ that uses unsupervised machine learning to learn the typical behaviors of human and machine identities in applications and detects anomalies that are highly correlated to malicious activities. This approach to detection delivers a superior level of accuracy and context, nearly eliminating false positives and enabling prompt response before business is impacted.

> Creating an easy-to-follow timeline of activities from multiple sources, **Reveal Security helps analysts understand what a deviation looks like and why it is risky.**

Analyzing user and identity activity collected via the audit logs of the bank's e-banking application, the Reveal Security platform automatically learns the typical behavior of individuals and similar groups of users in the application, and detects deviations. The SOC only receives alerts of anomalous activity that is always worthy of investigation.

Results

With Reveal Security, the security team has an effective and more automated approach to keep the bank in compliance and protected from fraud.

The team no longer has to spend time creating detection rules or investigating meaningless alerts. This frees up time to work on more strategic projects.

The Reveal Security platform significantly reduced the volume of alerts sent to the SOC to a very manageable number of true positives - 2-5 per week. Complex application log data in the alerts is automatically translated into easy-to-understand language that streamlines investigation and response. Analysts understand the threat and can take action without requiring guidance from engineering or application owners. As a result, typical MTTD and MTTR were cut by half.

About Reveal Security

Reveal Security quickly and accurately detects identity threats post-authentication in and across SaaS applications and cloud services. The Reveal Security ITDR platform is the only solution in the market based on patented Identity Journey Analytics™ technology that uses unsupervised machine learning to continuously analyze the activity of human and machine identities in applications and 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**