Fortune 500 Financial Institution Builds Insider Fraud Solution to Protect Customer Data and Meet Regulatory Compliance

The Challenges

- **No oversight into how employees were working with sensitive data**
- **Inability to track sensitive data usage in custom apps**
- **Incident data lacked event context**

The Solutions

In-App Field Parsing
Track individual field-level activities across apps and websites, including custom-built

User and Entity Behavior Analytics
Detect behavior anomalies that fall outside of a defined threshold or behavioral baseline

Scriptable Rule Logic
Create custom metrics to track any activity and build custom responses that automatically respond to unauthorized behavior

Enterprise SLA & Professional Services
Dedicated, exclusive support and service

Summary

A Fortune Global 500 multinational bank needed a way to more accurately identify possible instances of insider fraud at their organization. To do so, the bank turned toward Teramind's behavior analytics. Knowing Teramind generated the type of detailed metrics and actionable insights they needed, the bank leaned into Teramind's customization capabilities to create an insider fraud detection program that revealed data misuse by employees, enriched their threat intelligence research and threat mitigation efforts and achieved regulatory compliance.

The Outcomes

- Gained visibility into field-level employee activity
- Enriched threat intelligence with irrefutable forensic evidence
- Streamlined incident triage with contextual activity data
- Built custom responses to thwart vulnerable employee behaviors
- Created an insider fraud mitigation program that accounted for user behaviors

The Power of Data Analytics

Insider fraud sometimes goes on for years undetected. The bank knew this all too well, after discovering some of their clients had been victims of insider fraud at the hands of corrupt bankers whose actions were nearly undetectable after having copied customer account information with a burner cell.

The bank needed to ensure the sensitive customer data that their employees worked with daily was safeguarded against fraud. To add to the battle, the data they needed to track and protect most was housed in individual form fields within the custom desktop app their employees used to access customer accounts.

Company Stats

Industry
Finance

Employees
220,000+

Customers
40 million

Other strategies they tried resulted in inaccurate activity data and produced too many false positives for the threat intelligence team. “There was no analysis. We weren’t able to figure out how much time was being spent looking at sensitive customer data. Basically, we didn’t know what was happening,” said the bank’s Senior Vice President of Fraud Prevention.

The lack of accurate data was leaving the bank vulnerable to threat. The longer they went without insights into how employees were interacting with sensitive data, the higher the chances were of another corrupt employee defrauding customers.

> *"Teramind is compatible with all systems, automatic, non-invasive and most of all, its parsing technology was completely accurate"*
>
> -Senior Vice President of Fraud Prevention

They came to Teramind looking for a custom solution that could provide the detailed, field level data they were after. Through Teramind's in-app field parsing, the bank was able to create rules that monitored the individual fields containing sensitive content in custom apps; relying on user and entity behavior analytics (UEBA,) behavioral baselines were established that alerted the security team when employees spent too long accessing those fields; while custom responses created contextual forensic evidence the security team could use to enrich threat intelligence and triage incidents.

Working with a dedicated engineer and CS manager from Teramind, the new insider fraud detection program was built and launched.

The bank was able to accurately assess how long employees needed to access sensitive data fields and identify which employees, if any, were exceeding the typical access parameters. Using the reports and session recording that come standard with Teramind, the fraud prevention team were able to put excessive access activity into context and elevate incidents appropriately. “We can say “Capture this” and it captures exactly what’s required and that helped us attain regulatory commitments. It’s a huge thing to be able to do.”