Suspicious Transaction

How to detect if seemingly unrelated people, running seemingly unrelated activities, are teaming up to spot potential targets and behave maliciously?

What you want to avoid

The database administrators are your most powerful users. They have all the tools to search your client base and spot potential fraud targets.

They can identify target dormant accounts, or the ones with high volumes of transactions, where the fraud would probably remain undetected.

In the context of collusion with other individuals having knowledge in business and the right for transactions, imagine how easy it is for fraudsters to identify opportunities and create complex fraudulent schemes that would remain undetected.

How our solution works

By providing a fully customisable, non-intrusive behavioural pattern engine, our Smart Control Objective is able to analyse your database administrator inquiries.

It correlates activities from multi-channel, multi-layer sources, and highlights potential fraudulent users' behaviours.

If IT users target accounts by inquiries, then these transactions are automatically reported.

Furthermore, if you want to drill down unusual transactions, our forensic capabilities facilitate investigation on suspicious queries and highlights potential collusion evidences.

Outcome

Alerting
In case of suspect use of database queries or behaviours, alarms are raised and sent by email or SMS to security teams. Response to a potential threat can be then deployed in a timely manner.

Review and investigation
Reports are generated, showing the potential collusion cases between IT and business employees, and enabling further investigation thanks to our forensic capabilities. For follow-up and documentation purposes, tickets are automatically created in the Case Manager workflow solution.

Interested? Contact us!

NetGuardians Y-Parc, Rue Galilée 6, Yverdon-les-Bains, Switzerland, netguardians.ch, info@netguardians.ch