Inquisitive Employee

How can you prevent a malicious employee from accessing customer information to be used for fraudulent reasons?

What you want to avoid

As your employees need to access information for their daily activities, it is very difficult to find cases where they misuse regular access rights for fraudulent purposes.

An inquisitive employee could browse through your client base to spot potential targets for frauds: dormant accounts where fund transfer would remain undetected, behavioural patterns of a given customer in order to tailor an elaborate scam scheme, etc.

How our solution works

Our Smart Control Objective relies on a fully customisable, non-intrusive behavioural pattern engine that identifies unusual activities from your employees, in terms of volumes or targeted data.

Our solution correlates audit trails from multiple sources. Client browsing, search for dormant accounts, or queries on your customers' data are detected in a timely manner.

The relevant information is brought forward to spot the employee who acted maliciously.

Outcome

Alerting
Alerts are automatically sent by email or SMS in case of suspicious human behaviour.

Investigation and follow-up
You can drill down the audit trails thanks to our forensic capabilities to explore the incidents. Reports are generated, enabling activity review of your employees.

Tickets are automatically created in the Case Management solution for incident follow-up.

Interested? Contact us!

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