Rogue Administrator

Despite the use of generic accounts, how can you still detect the fraudsters?

What you want to avoid

Manipulation of your Bank's data would disrupt your operations, cause financial losses or hurt your reputation by causing not only a press scandal but also impacting your customers' trust.

The IT team has privileged access rights, making them the most powerful users in your organisation. Generally, such credentials are shared among the IT team by using generic accounts, and you have no way of pinpointing who is accountable in case of fraudulent activities.

How our solution works

Our Smart Control Objective is able to analyse your IT administrator activities thanks to our non-intrusive Console Tracking System technology. It provides real-time auditing of admin activities and generic user account mapping with the real user name.

As our Smart Control Objective correlates both the transactions and the user behaviour, it is able to determine, with a 100% reliability, who infringed the rule.

Outcome

Alerting
As soon as an admin uses a critical command, an alert is created. SMS and emails are immediately sent to designated investigators.

Reporting
For investigation purposes, reports are generated to show detailed admin account activity.

Workflow
In order to ensure incident follow-up, a ticket is automatically created in the Case Manager workflow solution. You can easily document the reasons of IT admin activities.

Interested? Contact us!

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