IT Change For Accomplice

Collusion between business employees and IT is often elaborate and tough to detect.

What you want to avoid

When you combine the powerful access rights of IT administrators with the business knowledge of other employees, under-the-radar operations can be sophisticated and remain undetected.

These complex schemes may include fake user account creation and granting of extensive access rights to unauthorized employees.

Thanks to their powerful privileges, a malicious administrator can also erase or alter any trace of such activities, rendering the offence nearly impossible to detect.

How our solution works

Our Smart Control Objective is able to analyse your user activities, providing multi-channel, multi-layer real-time auditing. Accountability of IT admin actions is enforced thanks to our Console Tracking System.

By correlating available data from multiple sources, seemingly unrelated human behaviours are tied together to identify cases of potential collusion.

For example, our solution detects if a user account is created by an admin, used by another employee for a fraudulent transaction, and then deleted.

Outcome

Real-time alerting
As soon as activities happen on critical access rights, or unusual human behaviours are detected, an alert is automatically created and sent by SMS or email.

Activity review
For investigation purposes, reports are generated, enabling detailed admin account activity review.

Incident follow-up
Automatically created tickets enable incident follow-up and detailed comprehensive documentation in the NG|Case Manager solution.

Interested? Contact us!

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