



TANGO
TECHNOLOGIES

THE KEY TO UNLOCKING SECURE ROLE SOLUTIONS



SENSE

Smart Architecture

Detection

Financial Control

SENSE fundamentally redefines SAP threat detection and audit log analysis within the Cortex Suite. Operating through an executive command centre, **SENSE** delivers real-time operational clarity across all managed systems by surfacing live health metrics, open alerts, enabled rules, and total detection items. A built-in system lag early-warning indicator calculates the exact duration evaluation lags behind log collection to prevent silent security monitoring failures. In-app settings governance allows administrators to securely update thresholds directly within the launchpad, utilising strict delete-and-insert mechanisms to eliminate duplicate entries and database inconsistencies.

Streamlining audit log collection, the high-performance collection engine minimises processing overhead by capturing only what is strictly necessary. **SENSE** utilises targeted log sweeping to rapidly interrogate managed SAP systems, dynamically reading active rule matrices to exclusively extract logs required by active rules. An integrated automated housekeeping mechanism ages out and deletes historical data based on customer-defined retention windows, while collection simulation enables administrators to execute test sweeps and assess workload counts before committing to actual database reads.

Decoupling the threat detection engine from log collection provides security teams with maximum tuning flexibility. By operating detection as an independent job from log collection, security teams can actively retune rule thresholds and re-evaluate identical time periods without executing redundant, expensive database reads. A safe re-evaluation engine evaluates records securely based on composite keys of rule, system, object, and day, safely permitting historical periods to be re-analysed without ever duplicating existing alerts.

The Active Alert Console forces strict accountability by ensuring every security decision is backed by concrete proof. A unified evidence and decision view displays raw audit rows and historical logs directly alongside response actions, while mandatory disposition enforcement rejects silent closures by requiring formal classification as confirmed, false positive, or accepted risk. Accepted risks enforce strict time-bound validity end-dates to ensure exceptions automatically expire, with every event recorded permanently in an append-only, immutable alert ledger.

Forensic timeline reconstruction reads deep into core recording structures to display a continuous, chronological sequence of user actions executed before and after any flagged incident occurs. To defend against risk and mitigate threats immediately, **SENSE** executes automated response actions directly from the alert console. Security teams can dispatch native requests to lock compromised user accounts, revoke specific dangerous roles, or flag suspicious profiles for proactive watch and elevated tracking over defined timeframes.

Dynamic rule and threshold governance provides total control over detection sensitivity and system scope. An interactive rule workbench governs the fifteen shipped detection rules through an intuitive interface, allowing administrators to seamlessly activate rules, modify severities, and configure precise alerting thresholds. Deactivating a rule immediately narrows the scope of future log collection sweeps to optimise system performance, while centralised critical object master lists feed parameters directly into evaluation engines to enhance governance and deliver rapid, fully compliant audit results.

Bespoke SAP Security & Licencing Solutions. Talk to us Today!

[Tango Technologies Website](https://www.tangotech.co.uk) / info@tangotech.co.uk / [+44 121 838 5210](tel:+441218385210) / [LinkedIn](#)

Cortex Suite