personam™

INSIDER THREAT DETECTION

FRAUD | THEFT | SABOTAGE

CASE STUDY: Four employees conspire to steal client data

A Global IP Law Firm

Six worldwide offices supported by a central data center

A corporate policy encouraging file & resource sharing among staff

Routine uploads of large file collections to external url's (e.g. PTO)

A Personam ITD Deployment

Distributed sensors monitor all incoming & outgoing traffic to the data center and the Internet

Behavior profiles are established for all individuals and devices

Cohort Groups are identified across the organization

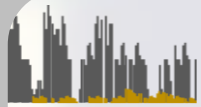
A Major Theft is Planned

A senior partner and three associates in a foreign office begin making electronic copies of client files

The collection activity is cautious and hidden within normal work activity

Behavioral Cues Are Picked Up

ALERT!



The subtle but widespread collection of files to desktop computers is detected by Personam ITD; their behavior is inconsistent with their respective cohort groups

Alerts are quickly generated; Personam staff receive notification from the system

Forensic Information

Personam staff generate a report of the activity; the firm's security administrator is notified within minutes

The report contains the names of the employees, a summary of outlier behavior, and lists of network resources and files accessed

Rapid Response

The employees are confronted with the forensic information

The incident is resolved without the loss of any client data, and the personnel actions are swift