USE CASE: SECURING EXECUTIVE ACCOUNTS

A rogue IT admin at a financial services company was reading an executive's inbox and marking messages as unread.

It went unnoticed until the firm installed Varonis and got an alert on suspicious mailbox activity. The audit trail showed that the unscrupulous admin was hunting for emails related to a rumored acquisition.

How does Varonis detect compromised executive accounts and prevent unauthorized access to executive files and emails?

Varonis can automatically identify executive accounts without manual configuration – so executive accounts are always monitored and protected.

Varonis profiles the behavior of executives and alert on abnormal activity from an individual executive account or across all executive accounts. Unusual account lockouts, an increase in access denied events, or strange file and email activity which may indicate account compromise or impending resignation.

Varonis also gives you a clear picture of which non-executive users can and do access sensitive data and will alert you of suspicious file and email activity.

Relevant DatAlert threat models

- Abnormal executive behavior: unusual amounts of access to script, configuration and backup files across executive accounts
- Abnormal executive behavior: unusual amounts of access-denied events across executive accounts
- Suspicious mailbox activity: multiple messages marked as unread by user other than the mailbox owner