DECEPTION CHECK

SSH KEY INVESTIGATION / PRESERVE THE CHANGE

One host. One trust change.

A password reset does not remove an unauthorized SSH key. Check the effective source, the change, and later authentication.

Use case aliases and evidence references. Keep original key lines, raw logs, and sensitive host/account details in your approved evidence store.

Case alias / analyst / review time UTC

Record the observation window and source-clock uncertainty.

01 / Effective key source

Host and account aliases; effective AuthorizedKeysFile or AuthorizedKeysCommand; account, key, and connection restrictions.

02 / Key identity

SHA-256 fingerprint and key type. Reference the preserved full line, restrictions, and comment. A comment is not key identity.

03 / Change and session

UTC time and precision; before/after content reference; file or provider audit record; writer/process ancestry and initiating session.

DECEPTION CHECK

What would change the decision?

04 / Approval

Expected administrator; approved change window; approval reference; what remains unexplained.

05 / Later authentication

Accepting host, account, UTC time, and key fingerprint if logged. Record observed use or the precise collection/retention gap.

06 / Response and next owner

Evidence preservation; authorized removal/revocation and account recovery; operational dependencies; named owner and next review UTC.

Closeout check

Can you explain what changed, whether it was approved, what access it could grant, and whether that access was used? A missing log field is a collection gap, not proof of no use.

Field note and references: deceptioncheck.ai/research