DECEPTION CHECK

RESPONSE WORKSHEET / OCT 31, 2026

Record the fix. Trace the credentials.

One worksheet per response. An installed update and an investigated incident are separate receipts. Keep internal identities, addresses, and evidence locations in your private copy.

01 / Platform owner

Record the running fix

Appliance and response owner

Installed release line and full running build

Vendor advisory revision and time checked

Internet exposure period and evidence source

Maintenance completed and running build verified by

02 / IDENTITY OWNER

Map what the gateway could expose

List gateway service accounts, stored secrets, directory permissions, and reachable systems. Assign an owner to assess access and verify any replacement or revocation.

Identity owner / service account references

Secrets and downstream access in scope

DECEPTION CHECK

RESPONSE WORKSHEET / OCT 31, 2026

Make recovery an accountable decision.

Preserve evidence and coordinate containment with the service owner. A clean integrity result or a quiet endpoint console is not an all-clear for the gateway.

03 / RESPONSE + IDENTITY OWNERS

Keep the recovery receipt

Evidence retained: collection time, custodian, source records

Activity reviewed: identities, period, findings, and gaps

Containment / reset or rebuild decision and owner

Credential and secret actions: replacement, revocation, verification

Restore-service decision: approver, time, remaining actions

BEFORE YOU CLOSE

For suspected or confirmed compromise, follow the current vendor recovery procedure. Account for physical versus virtual/cloud appliances, current fixed firmware, affected accounts and secrets, and downstream investigation.

The October 29 companion table lists 25.1.1.3 for the affected 25.1.1 line and 22.8R2.6 for the affected 22.8 line. Other branches, migration paths, and hardware requirements need the complete advisory. Record the running build after maintenance.

Guide + current sources:

deceptioncheck.ai/blog/ivanti-new-fixes-credential-response