DECEPTION CHECK

EVIDENCE DECISION WORKSHEET

OCTOBER 29, 2026

Map the evidence before closing the ticket.

Use asset aliases here. Keep raw logs, addresses, and sensitive evidence in your approved store. Digital fields are fillable; the same page works in print.

SCOPE	FIX	ACCESS	EVIDENCE
Dependency	Running build	Review	Second source

01 Name the system and the decision owner.

ASSET / SERVICE ALIAS

RESPONSE OWNER / ROLE

WHAT DEPENDS ON IT? WHAT WOULD CONTAINMENT AFFECT?

02 Connect the fix and access review to receipts.

SUPPORTED RUNNING BUILD / RECEIPT

ADMIN ACCESS / CHANGE REVIEW RECEIPT

VENDOR / MAINTENANCE REFERENCE

REVIEW TIME UTC / NEXT REVIEW

03 Map what each source can actually show.

SOURCE	WHERE RETAINED	WHAT IT CAN SHOW	OWNER
Host / application			
Identity			
Management plane			
Network / collector			

A second copy preserves a generated record. A different source can show another part of the activity. Neither reconstructs an event automatically.

Test it. Record the gap. Hand it over.

Use an approved harmless event, not exploit traffic. Record collection failure and monitor failure as separate cases.

04 Run one safe collection test.

APPROVED EVENT / SOURCE / UTC TIME

RECEIPT / DELAY / RETENTION REFERENCE

- [ ] Event arrived
- [ ] Record retained
- [ ] Responder reached

WHO GETS A COLLECTION-FAILURE ALERT?

WHO NOTICES IF THE MONITOR STOPS?

05 Capture the unresolved gap and the next action.

GAP / ALTERNATIVE EVIDENCE / SECURITY IMPACT

NEXT ACTION / OWNER / DUE DATE

- [ ] Running fix verified
- [ ] Access reviewed
- [ ] Evidence test recorded
- [ ] Follow-up required
- [ ] Containment review needed
- [ ] Ready for closeout

Record the decision and its owner; check the statuses that apply.

FILLED EXAMPLE / FICTIONAL DATA

Asset: Virtualization host A
Second source: Identity sign-ins retained in the central collector
Test receipt: Received and retained; responder reached
Gap: Management tasks are not mapped into the investigation view
Next action: Platform team maps task records, then repeats the test
Decision: Follow-up required; keep the gap open

Get the technical chain, Sigma rules, platform translations, and validation notes:
deceptioncheck.ai/blog/when-admin-actions-go-unlogged