DECEPTION CHECK

PLACEMENT / NEXT LOG / NAMED OWNER

A canary fired.
Give the next step an owner.

Capture what happened, what remains unknown, and who will check next.

> Use case aliases and evidence references. Keep live token URLs, credentials, raw host details, and original records in your approved evidence store. Share this worksheet only through an approved channel.

Case alias

Analyst / case owner

Collection time (UTC)

Clock source / uncertainty

Record collection time in UTC. Note the source clock, any conversion, and uncertainty. Preserve original event times in the evidence store.

01 / Placement and purpose

Where was the canary placed, who should encounter it, and what question should it answer? Use a token alias, placement type, expected audience, and placement owner.

02 / Preserve the original observation

Record event time with its timezone and precision. Preserve original time, source address as logged, request details, and response in the evidence store; put references here. A URL request alone does not establish authentication or compromise.

03 / Check expected activity

Match approved tests to the owner, window, token, and action. For crawler candidates, record the claimed identity and how it was checked, using approved verification sources and a check time. A User-Agent string alone is not identity proof. Retain uncertainty.

DECEPTION CHECK

TURN THE OBSERVATION INTO A HANDOFF

The next log. The next owner.

Case alias

Next review time (UTC)

04 / Choose the next log from the placement

For a document, consider access and sharing history; for a repository, audit and access records; for a credential lure, authentication records. Name the actual available source, search window, expected evidence, and coverage gaps. Keep URL requests and authentication results separate.

05 / Decide urgency and preserve safely

State the current disposition and what supports it. Set urgency from the placement, exposure, observed activity, and corroborating records. Preserve original alert and relevant logs before retention expires. Do not browse or replay a live token to investigate it. Follow your incident process for containment.

06 / Name the owner and next review

Assign one person to the next evidence request and a due time in UTC. State what would change the decision. After this case, plan an approved end-to-end test of collection, alert delivery, retention, and responder handoff.

> A URL request, an authentication attempt, and a successful authentication are different observations. Record each only when the corresponding evidence supports it.