Counterfactual cut analysis: one page template

Incident: _____ Evidence cutoff: _____ Analyst: _____ Version: ___

1. Question. Start state: _____ Compromised workload: _____ Targets: t1 _____ t2 _____ t3 _____

2. Sources. Label each one as a vendor account, an observed log, a reconstruction or this analysis's interpretation.

Source	Label	Used for	Checked on

3. Transitions. One row per atomic step. Write AND when a step needs several states at once.

ID	From (AND)	To	Narrated, inferred or unresolved	Source and time

4. Open points. Every unresolved question becomes an assumption, and every plausible other route becomes an alternative.

ID	Assumption or alternative	Default or basis

5. Controls. Only prevent changes reachability.

ID	Prevent, constrain, detect or assure	Transitions	Pass test

6. Cuts. One row per scenario. Give a surviving route for every target that is not cut.

Scenario	t1 cut by	t2 cut by	t3 cut by	Surviving route

7. Independence. Name the holder of each authority. Credit a control only if no holder is reachable from the compromised workload.

Control	Configuration	Identity	Deployment	Bypass	Recovery	Evidence	Path from the workload?	Credited?

8. Residual paths.

Path	Control bypassed	Basis	Test that settles it

9. Decision. Controls to build: _____ Tests to run first: _____ Owner: _____ Date: _____