DECEPTION CHECK

NODE-RED / FLOW AND EVIDENCE REVIEW

Know what is still running.

Use with the application or controls owner. Preserve originals before changing a production workflow.

01 / Identify the instance

Review date, owner, host/product, running version, management URL, and approved clients.

02 / Review both authentication boundaries

Editor/Admin API: authentication and write permissions. Flow HTTP endpoints: authentication, callers, and downstream actions.

03 / Preserve and compare the flow

Restricted copy/version, capture time, evidence custodian, approved baseline, unfamiliar nodes, wiring, and command inputs. Do not write credentials here.

A LOGIN IS NOT A FLOW CLEANUP

Review automatic Inject nodes, Exec commands, and HTTP In paths that reach privileged actions. These can be legitimate. Ask who approved the workflow and compare it with the baseline.

DECEPTION CHECK

NODE-RED / FLOW AND EVIDENCE REVIEW

Separate the three records.

A request, a deployment, and an executed command answer different questions. Keep each conclusion tied to its source.

REQUEST / DEPLOYMENT

Access logs, flows.set audit, caller, time, management path, status, and change approval.

FLOW / HOST PROCESS

Preserved flow version and wiring, then supported EDR or process logs: parent, child, account, and time.

OUTBOUND REQUEST

Independently retained proxy, DNS, firewall, or network data: destination, port, and result.

04 / Decide the next action

Preservation location, containment/change window, recovery owner, exposed-secret review, next action, and due date.

REFERENCES AND RESOURCES

deceptioncheck.ai/research

Siemens SSA-834709 applies to its listed IoT2050 Advanced configuration. Use vendor-supported response and logging on embedded devices.