Establish what ran and what loaded

One record per host or linked execution. Use UTC times; retain original evidence.

Case / host reference

Analyst / response owner

Observed time / time range / source timezone

01 Establish origin and process context

Executable path / hash / version / signer / signature result

Origin: approved deployment, download, installer, or unknown / evidence reference

User / parent process / process ID or stable process key / launch time

02 Join the process to its loaded DLLs

An adjacent file is not proof it loaded. Link module evidence to the process and time.

DLL path / identity reference	Load time / process key	Hash / signer / evidence ref.

Module telemetry source / retention / collection enabled at the relevant time?

Missing module records are a visibility gap, not an all-clear.

Do not launch a suspicious copy to update it. Preserve evidence and follow incident response.

Primary source: Siemens ProductCERT, SSA-580366 v1.2; 19 Oct 2026 notice.
https://productcert.siemens.com/productcert/html/ssa-580366.html

Reviewed 20 Oct 2026 | Working record, not proof that a host is clean.

Separate patch status from incident closure

Keep uncertainty explicit. Assign each remaining action to an owner.

Case / host reference / investigation window

03 Follow-on activity and search coverage

Review area	Result / time / evidence reference
Startup / scheduled tasks	
Child processes / network	
Hosts / sources searched	
Retention / gaps / exclusions	

04 Response and operational safety

If isolation could affect operations, agree on safe containment with the operational owner.

Access / consequence / containment decision / decision maker / time

Evidence preserved / necessary response taken / outstanding response actions

05 Two closure records

PATCH: approved source / version 4.0.9.8 or later verified / change record / owner

INCIDENT: scope / execution explained / response evidence / unresolved gaps

Next action / named owner / due time / incident status

Primary source: Siemens ProductCERT, SSA-580366 v1.2; 19 Oct 2026 notice.
https://productcert.siemens.com/productcert/html/ssa-580366.html

Reviewed 20 Oct 2026 | Working record, not proof that a host is clean.