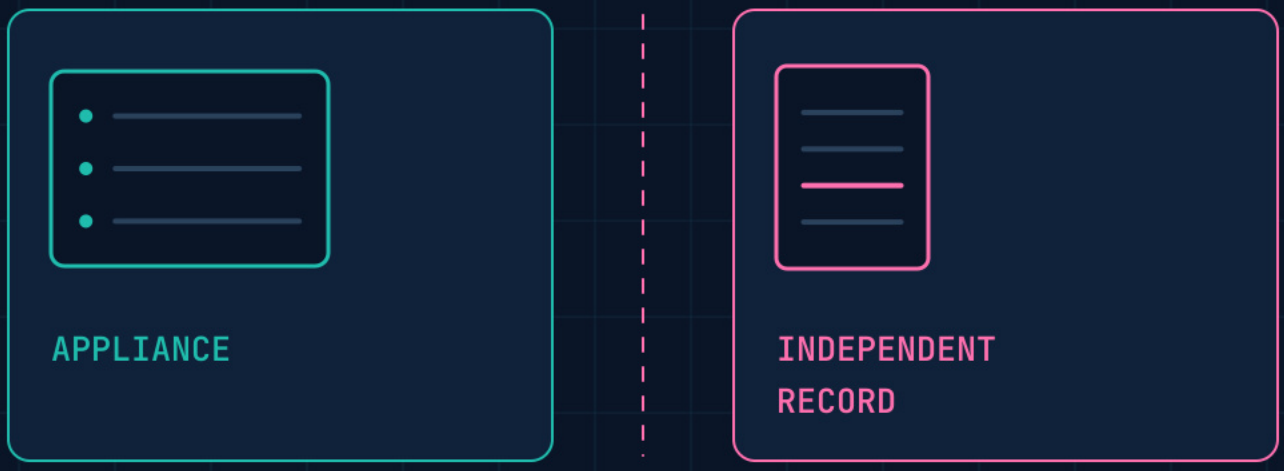
FORTISIEM / RESPONSE NOTES

Who watches the SIEM?

When the monitoring system is the target, its own clean-looking dashboard is not enough.



Keep an independent record.

CVE context: Fortinet / Response: Deception Check

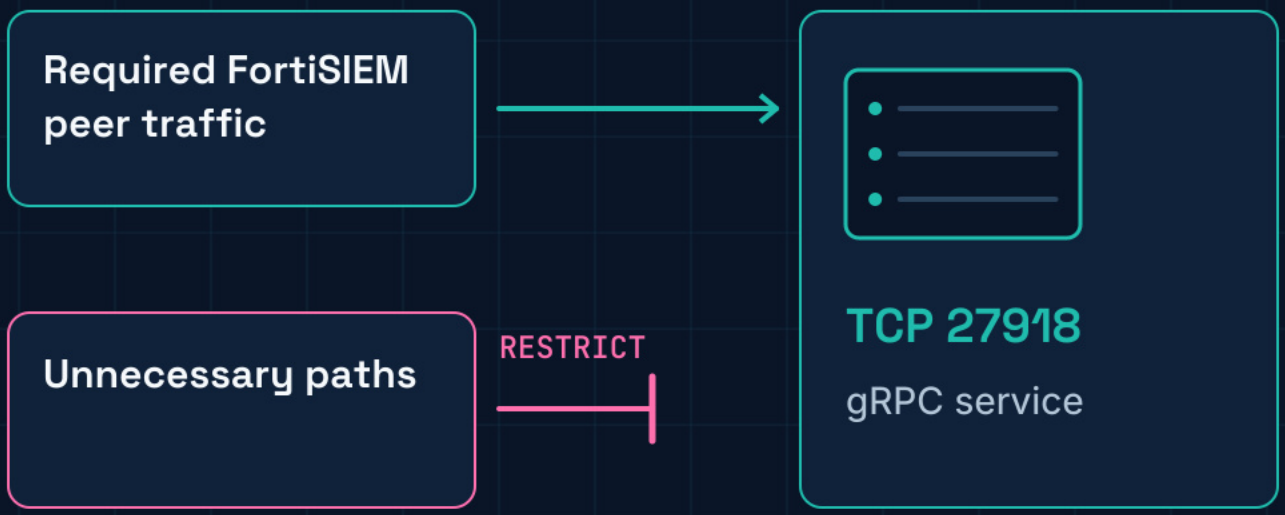
Response notes / 21 Oct 2026

Vendor advisory: https://fortiguard.fortinet.com/psirt/FG-IR-26-180

01 / CHECK YOUR EXPOSURE

Internal service. Actual reachability.

For CVE-2026-106173, check access to TCP 27918. Keep required FortiSIEM peer traffic; restrict unnecessary paths.



Check the route, not the label.

Service guidance: Fortinet FG-IR-26-180

Response notes / 21 Oct 2026

Vendor advisory: https://fortiguard.fortinet.com/psirt/FG-IR-26-180

02 / KEEP THE STEPS SEPARATE

A connection is not execution.

Connection seen. Request understood. File changed. Code executed. Each needs its own evidence.

01	CONNECTION	Connection seen.
02	REQUEST	Request understood.
03	FILE	File changed.
04	EXECUTION	Code executed.

State what your telemetry can actually show.

Response notes / 21 Oct 2026

Vendor advisory: https://fortiguard.fortinet.com/psirt/FG-IR-26-180

03 / INVESTIGATE CHANGES

Patch the flaw.
Explain the change.

Use a trusted same-build baseline. Correlate unexpected file changes with independent activity records.



Trusted same-build baseline

COMPARE



Unexpected file changes

EXPLAIN



Independent activity records

An unchanged timestamp is not an all-clear.

04 / TEST THE EVIDENCE PATH

Separate storage. Separate control.

Can the appliance's credentials alter the evidence copy? Can another analyst retrieve it if the appliance is unavailable?



A second copy needs its own access boundary.

Response notes / 21 Oct 2026
Vendor advisory: https://fortiguard.fortinet.com/psirt/FG-IR-26-180

05 / CLOSE TWO DIFFERENT QUESTIONS

Fixed?
Investigated?

Record the supported update and exposure controls separately from the investigation, evidence gaps, and next action.



FIXED

Supported update / Exposure controls

OWNER



INVESTIGATED

Investigation / Evidence gaps / Next action

OWNER

Give every open question an owner.