snare
A PROPHECY SOLUTION

A SNARE SOLUTIONS RESOURCE • SECURITY OPERATIONS

Telemetry Service Scorecard

Prove that the pipeline feeding your SOC is healthy: a practical scorecard for SOC leaders, security architects and MSSPs.

- Six measures for every critical source-to-destination path
- Objectives by source tier, with clear Green, Amber and Red rules
- A printable worksheet, a worked example and a tamper-event checklist
- A monthly telemetry health report, with per-tenant reporting for MSSPs

WHY A SCORECARD

Most SOC dashboards describe threats. Few describe the pipeline that feeds them.

Visibility gaps aren't only sources that were never onboarded. Some open silently when an onboarded source stops delivering, and some are opened deliberately by an attacker.

Cyber leaders surveyed for the SANS 2026 SOC Survey rank lack of enterprise-wide visibility as the top barrier to SOC capability, ahead of staffing. Coverage programmes rightly focus on onboarding the sources that are missing. Far less attention goes to proving that the sources already onboarded are still arriving, complete and on time.

A destination can be reachable while delivery latency climbs, queues build, or individual sources go quiet. These are service reliability problems, and they need service reliability measures. This scorecard treats each critical source-to-destination path as a service, with an owner, an expected delivery pattern and an objective.

Three ways a source goes quiet

Operational failure

Agent stopped, certificate expired, disk full, network path changed, destination rejecting events. You see a drop in volume, transport errors and queue growth.

Configuration drift

Audit policy changed by a GPO update, a host re-imaged with defaults, a filter edited too broadly. Specific event types disappear while overall volume looks normal.

Adversary action

Logging disabled or cleared, indicators blocked at the host (MITRE ATT&CK T1562.002, T1562.006, T1070.001). You see tamper events at the source, then silence.

How to use this scorecard

1. **List your critical paths.** One row per source-to-destination path, such as domain controllers to SIEM, with a named owner and a source tier.
2. **Set objectives by tier** (page 3). The figures supplied are illustrative starting points, not benchmarks.
3. **Record six measures each period** on the worksheet (page 5): freshness, latency, delivery success, queue pressure, recovery testing and change control.
4. **Rate each measure Green, Amber or Red** using the rules on page 3. Any Red makes the path Red.
5. **Check your tamper events** (page 6) and **publish the monthly report** (page 7).

NIST CSF 2.0 · PR.PS-04 | ISO/IEC 27001:2022 · A.8.15–8.17 | MITRE ATT&CK · T1562, T1070

NIST SP 800-92 Rev. 1 (draft)

STEP 1 · SET YOUR OBJECTIVES

Objectives by source tier

Not every source needs the same objective. An identity provider stream used for immediate investigation needs a tighter freshness and latency target than a lower-priority operational stream. Adjust these to your environment; the rules below apply whatever values you choose.

Source tier	Examples	Freshness objective	Latency p95 target	Delivery success target	Queue amber / red	Recovery test due
Tier 1 Identity & privileged access	Domain controllers, identity provider, PAM, EDR	15 min	5 min	99.9%	50% / 80%	Every 90 days
Tier 2 Core infrastructure	Servers, firewalls, VPN, cloud control plane	60 min	15 min	99.5%	60% / 85%	Every 180 days
Tier 3 Operational & low-volume	Application logs, infrequent appliances	24 hours, or a learned weekly pattern	60 min	99.0%	70% / 90%	Every 365 days

Illustrative starting points, not benchmarks. Latency measurement depends on synchronised clocks (ISO/IEC 27001:2022 Annex A 8.17) and consistent measurement points.

The six measures and how to rate them

Measure	What to record	Green	Amber	Red
Source freshness	Minutes since the source last produced an expected event	Within objective	Up to 2× objective	Beyond 2× objective
End-to-end latency	p95 minutes from event creation to arrival at the destination	Within target	Up to 2× target	Beyond 2× target
Delivery success	Accepted events as a share of events sent, after rejections for authentication, parsing, size or rate limits	At or above target	Up to 1 percentage point below	More than 1 point below
Queue & buffer pressure	Share of buffer capacity in use at peak, and the retry trend	Below amber threshold	Between thresholds	At or above red threshold
Recovery performance	Date delivery was last tested resuming after an outage, with loss, duplication and reordering documented	Within due interval	Up to 50% overdue, or never tested	More than 50% overdue
Change control	Were routing, destination and filter changes this period version-controlled and approved?	Yes, or no changes	–	Unapproved change

OVERALL PATH STATUS

Any Red makes the path Red. Otherwise any Amber, or a path with no recovery test on record, makes it Amber. Only a path where all six measures are Green is Green.

WORKED EXAMPLE

Four paths, four stories

How the rules play out for four typical paths. Each row is rated against the objectives on page 3.

Path	Freshness	Latency	Delivery	Queue	Recovery	Change	Overall
Domain controllers → SIEM Tier 1	6 min Green	2 min Green	99.95% Green	22% Green	72 days ago Green	Approved Green	Green
Identity provider audit log → SIEM Tier 1	42 min Red	4 min Green	99.92% Green	35% Green	55 days ago Green	No changes Green	Red
Perimeter firewalls → evidence store Tier 2	35 min Green	9 min Green	99.20% Amber	68% Amber	261 days ago Amber	Approved Green	Amber
Line-of-business app logs → evidence store Tier 3	5 hours Green	25 min Green	99.60% Green	40% Green	Never Amber	Unapproved Red	Red

What the scorecard tells you

IDENTITY PROVIDER: A SOURCE HAS GONE QUIET

Every delivery measure is healthy, but no event has arrived for 42 minutes against a 15-minute objective. Volume dashboards would look normal. Check the collector, the provider's audit configuration and any tamper events before assuming the identity plane is simply quiet.

PERIMETER FIREWALLS: DRIFT, NOT FAILURE

Three measures are Amber at once: delivery just under target, the buffer above 60%, and recovery untested for 261 days against a 180-day interval. Nothing is broken yet, but the trend points to an outage that will be hard to recover from cleanly.

APPLICATION LOGS: A GOVERNANCE GAP

The data is flowing, but a routing change went in without approval and recovery has never been tested. Red here is about control rather than health: an unrecorded change is how events end up silently filtered or sent to the wrong destination.

STEP 2 · RECORD AND RATE

Telemetry service worksheet

Organisation / tenant _____ Reporting period _____ Completed by _____ Date _____

Telemetry path source → destination	**Tier** 1 / 2 / 3	**Owner**	**Freshness** min since last event	**Latency** p95, min	**Delivery** success %	**Queue** % used	**Recovery** last test date	**Change** approved?	**Overall** circle one	**Notes / action**
e.g. Domain controllers → SIEM	1	SOC platform	6	2	99.95%	22%	15 Sep	Yes	G A R	All within objective
									○ ○ ○	
									○ ○ ○	
									○ ○ ○	
									○ ○ ○	
									○ ○ ○	
									○ ○ ○	
									○ ○ ○	
									○ ○ ○	
									○ ○ ○	
									○ ○ ○	

Rules (p. 3): G within objective A up to 2× objective · ≤1 pt under delivery target · between queue thresholds · recovery ≤50% overdue or untested

R beyond those, or unapproved change

STEP 3 · WATCH FOR SILENCE THAT SOMEONE CAUSED

Tamper-event checklist

Windows records changes to its own logging. For each event, confirm it is collected, forwarded off-host and alerted on centrally, before the silence begins.

Event ID	Log	What it means for telemetry health	ATT&CK	Collected	Forwarded off-host	Alerting
1100*	Security	The event logging service has shut down.	T1562.002	☐	☐	☐
1102	Security	The audit log was cleared.	T1070.001	☐	☐	☐
104	System	A log (for example System) was cleared.	T1070.001	☐	☐	☐
1104*	Security	Log full. Rare on default overwrite settings; mainly seen in some STIG builds.	Operational	☐	☐	☐
4719	Security	System audit policy was changed.	T1562.002	☐	☐	☐
4616	Security	The system time was changed, which affects every timeline built from the host.	Operational	☐	☐	☐
6005 / 6006	System	The event log service was started / stopped. Correlate gaps with reboots.	Operational	☐	☐	☐
Sysmon 4	Sysmon	Sysmon service state changed.	T1562.001	☐	☐	☐
Sysmon 16	Sysmon	Sysmon configuration changed.	T1562.001	☐	☐	☐

Events fully covered: _____ of 9

Snare Agent default advanced auditing policies collect every event above (Sysmon events where Sysmon is installed) except those marked *, which can be added to the policy.

COLLECTING IS ONLY HALF THE CONTROL

Windows records the clearing itself: event 1102 (104 for the System log), plus another for every further attempt. What it can't bring back is the cleared history, so forward these events off-host as they occur and alert centrally. Snare forwards every 1102, repeats included, so the central copy keeps both.

Catching silence early

Source inventory

Reconcile sources that should report (CMDB, agent console, cloud accounts) with those that did.

Heartbeats

Have each collector emit a heartbeat, and alert when it stops.

Event-class checks

Track key event types, not just volume: a DC sending Kerberos but no 4688 has a policy problem.

Learned baselines

Compare with the same hour and weekday over four weeks; join alerts with change records.

STEP 4 · REPORT IT

Monthly telemetry health report

Pipeline reliability belongs in the SOC operating model, with thresholds, owners and runbooks. A short monthly report keeps it visible to SOC leadership, and for MSSPs it is the clearest way to show each client its coverage, not just its alert counts.

Report item	Owner	Due	Done
Sources expected versus sources reporting, by tier, with the gap list and an owner for each item			☐
Freshness and latency against objective for Tier 1 sources, including the worst five			☐
Delivery rejection rates by destination and cause			☐
Tamper-relevant events (1100, 1102, 104, 4719) and how each was resolved			☐
Routing and filter changes made during the month, with approver			☐

For MSSPs: telemetry health is a client commitment

A detection SLA is only as strong as the evidence that the sources it depends on were reporting. Complete a worksheet for each tenant, and report source freshness and delivery success per client alongside detection metrics.

Proves coverage

Clients see which of their sources were reporting, on time and complete, during the period the SLA covers.

Grows onboarding

Gaps in Tier 1 and Tier 2 make the case for connecting the sources a client hasn't onboarded yet.

Protects the provider

A recorded drop in freshness shows when a change on the client's side, not the provider's, opened a gap.

TECHNICAL TAKEAWAY

Treat collection and forwarding as managed production services, with objectives, owners and incident runbooks, not as one-off integration tasks documented once and forgotten.

WHERE SNARE FITS

Measure delivery health, rather than inferring it from silence

Snare works alongside the SIEM, XDR and analytics platforms you and your clients already use, and makes the collection layer something you can manage and measure.

Component	Role in telemetry health
Snare Agents	Collect configured security events at endpoints and servers across Windows, Linux, Unix and macOS, and forward them off-host.
Snare Central	Receives agent events plus identity, SaaS, cloud, network and admin-platform logs via syslog, API and cloud audit feeds. Provides remote agent management and centralised archiving, with retention configurable from 90 days to 7+ years. MSSPs can manage multiple customer environments from one console.
Snare Reflector	Caches, filters and forwards events in real time to one or more SIEM, XDR and storage destinations, and exposes per-destination delivery statistics. A full raw copy is retained.
AskSnare	A cybersecurity AI assistant, fed by the Snare evidence layer, that lets analysts ask plain-English questions of retained log data, with humans making the decisions.

TAKE THE NEXT STEP

See how Snare can make your telemetry pipeline measurable. Talk to the team about collection, retention and delivery health across your environment, or across every tenant you manage.

snaresolutions.com • Request a demo • Subscribe to the Snare Insider

Sources and references

SANS Institute, 2026 SOC Survey Insights (June 2026). NIST Cybersecurity Framework 2.0, PR.PS-04. NIST SP 800-92 Rev. 1 (Initial Public Draft), Cybersecurity Log Management Planning Guide. ISO/IEC 27001:2022, Annex A 8.15 Logging, 8.16 Monitoring activities, 8.17 Clock synchronisation. MITRE ATT&CK: T1562.001 Disable or Modify Tools, T1562.002 Disable Windows Event Logging, T1562.006 Indicator Blocking, T1070.001 Clear Windows Event Logs. Objectives in this scorecard are illustrative starting points, not industry benchmarks.

snare
A PROPHECY SOLUTION

© 2026 Prophecy International
snaresolutions.com