



The Cybersecurity Visibility Readiness Checklist

From Collection to Incident Recovery



The Cybersecurity Visibility Readiness Checklist

Prevention gets the investment. Investigation gets the evidence you kept. This checklist helps security teams test whether the logging architecture behind their security operations would hold up on the day an incident has to be reconstructed, explained and recovered from.

It follows the life of security evidence in eight stages. Each stage has five checks. It is written to be vendor-neutral and to complement the SIEM, EDR and other tools you already run.

How to use it

- Work through each stage with the people who own it: SOC, identity, infrastructure, cloud, and governance.
- Score each check Yes (2), Partly (1) or No (0). Be honest. “Partly” is the right answer more often than people expect.
- Add up each stage out of 10, then the total out of 80 on the scorecard.
- Pick your three lowest-scoring stages and agree one action for each. Revisit in a quarter.

This is a self-assessment to start a conversation, not an audit or a compliance test.

Obligations and retention requirements vary by jurisdiction, industry and contract.



1.Collection

Are we capturing the evidence an investigation would need?

The investigator's question: Which account did this, from where, and what did it touch?

Check	Yes (2)	Partly (1)	No (0)
Core Windows Security events are collected from servers and domain controllers: logon and failed logon (4624/4625), special-privilege assignment (4672), account and group changes (4720, 4728, 4732), log clearing (1102) and process creation (4688). Event 4688 only records command lines if command-line auditing ("Include command line in process creation events") is enabled, so confirm it is on.	☐	☐	☐
Execution and persistence events are collected, with the relevant audit policy enabled: PowerShell script block logging (4104), service installs (7045), scheduled-task creation (4698) and Kerberos authentication events on domain controllers (4768, 4769, 4771).	☐	☐	☐
Identity provider sign-in and administrative audit logs (SSO, MFA, conditional access) are collected, along with cloud control-plane and SaaS audit logs for every platform that holds business-critical or personal data.	☐	☐	☐
Network and remote-access sources (firewall, VPN, DNS, proxy) are collected, and logs from admin platforms such as RMM, hypervisors and backup consoles are included.	☐	☐	☐
Logs from public-facing APIs and third-party integrations are collected, including request rates, keys used and record counts, not only status codes.	☐	☐	☐

Stage 1 score: _____ /10



2.Coverage

Do we know what is not being collected?

The investigator's question: Is there any system an attacker could use that we would never see?

Check	Yes (2)	Partly (1)	No (0)
A current asset inventory exists and every in-scope asset is mapped to the log sources that cover it.	☐	☐	☐
Critical systems and sensitive-data stores are identified, and each has defined logging requirements.	☐	☐	☐
Coverage has been reviewed against MITRE ATT&CK detection strategies and analytics to identify the techniques we could not currently detect or reconstruct.	☐	☐	☐
External-facing and shadow assets are discovered on a regular schedule and brought into logging scope.	☐	☐	☐
Onboarding a new system, application or supplier includes a logging requirement before go-live.	☐	☐	☐

Stage 2 score: _____ /10



3.Integrity

Can we trust the evidence if we have to rely on it?

The investigator's question: Could someone have changed or deleted this record, and would we know?

Check	Yes (2)	Partly (1)	No (0)
Logs are forwarded off the originating system in near real time, so a compromised host cannot rewrite its own history.	☐	☐	☐
Write, delete and administrative access to the log platform is restricted, and separated from day-to-day administrator accounts.	☐	☐	☐
Log clearing, audit-policy changes and logging-service stops generate alerts, and we detect when an expected log source goes silent, with a named owner for the response.	☐	☐	☐
Time is synchronised across systems so events from different sources can be ordered reliably.	☐	☐	☐
Logs are encrypted in transit (for example, TLS) between sources, collectors, the log platform and any downstream tools such as the SIEM, and certificates are managed and renewed. Unprotected log traffic can be read or altered before it is stored.	☐	☐	☐

Domain 3 score: _____ /10



4.Routing

Does the right evidence reach the right place?

The investigator's question: Can we use the evidence in more than one tool, and change tools without losing it?

Check	Yes (2)	Partly (1)	No (0)
High-value events are routed to our SIEM or analytics platform, while the full evidence set is retained in an independent store.	☐	☐	☐
Routing and filtering rules are documented, reviewed on a schedule, and approved.	☐	☐	☐
Data is normalised before it reaches downstream tools, so fields and timestamps are consistent, while the original raw logs are kept as evidence.	☐	☐	☐
Collection is separate from any single analytics platform, so changing or adding a SIEM does not mean re-collecting or losing history.	☐	☐	☐
Buffering or failover prevents data loss when a destination is unavailable.	☐	☐	☐

Stage 4 score: _____ /10



5.Retention

Is the evidence still there when the investigation starts?

The investigator’s question: Can we look back past the first alert?

Check	Yes (2)	Partly (1)	No (0)
Retention periods are defined per log type, based on risk, regulatory and contractual requirements, and approved by the security owner.	☐	☐	☐
Searchable retention is set with realistic dwell time in mind. Mandiant’s M-Trends 2026 reports a 14-day global median, and half of intrusions run longer.	☐	☐	☐
Identity, authentication and privileged-activity logs are searchable for at least 90 days and archived for at least 12 months (see the benchmark below).	☐	☐	☐
A legal-hold process exists and has been tested.	☐	☐	☐
We have verified, by sampling, that data older than the oldest alert we would ever investigate can actually be retrieved.	☐	☐	☐

A CONCRETE RETENTION BENCHMARK

Start with 90 days searchable and 12 months archived for identity, authentication and privileged-activity evidence. **Why:** Mandiant’s M-Trends 2026 puts the global median dwell time at 14 days, so 90 days covers more than six times the median, and it matches the 90-day lookback in everyday investigation questions such as “Has this account done this anywhere else in the last 90 days?” Twelve months archived covers the long tail and aligns with PCI DSS v4.0.1 Requirement 10.5.1, which requires 12 months of audit-log history with the most recent three months immediately available. This is a starting benchmark, not a universal standard: raise it for regulated data, long-dwell threats or contractual requirements.

Stage 5 score: _____ /10



6.Storage

Is the evidence stored securely, and can we afford to keep it?

The investigator’s question: Can we keep what we need for as long as we need it, and get it back?

Check	Yes (2)	Partly (1)	No (0)
Storage is tiered, so recent data is quickly searchable and older data is retained at lower cost.	☐	☐	☐
Stored logs are encrypted at rest, and access to them is controlled and logged.	☐	☐	☐
Storage capacity and ingest growth are monitored, with alerts before limits are reached.	☐	☐	☐
Archived data can be restored and queried, and a restore has been tested within the last twelve months.	☐	☐	☐
The storage location meets our data-residency and sovereignty obligations.	☐	☐	☐

Stage 6 score: _____ /10



7.Investigation

Can analysts get answers in the time an investigation has?

The investigator's question: Can we answer the first ten minutes of questions without hand-writing six query languages?

Check	Yes (2)	Partly (1)	No (0)
Analysts can search across identity, endpoint, server, cloud, SaaS and network evidence from one place.	☐	☐	☐
We can answer, in minutes, "Has this account done this anywhere else in the last 90 days?"	☐	☐	☐
We can answer, in minutes, "Did we see this indicator anywhere before the alert fired?"	☐	☐	☐
Saved searches or runbooks exist for the most common investigation questions, and are reviewed after each incident.	☐	☐	☐
Natural-language or guided querying is available on top of integrated, retained evidence, so analysts do not need to be specialists in every source.	☐	☐	☐

Stage 7 score: _____ /10



8.Incident Recovery

Does the evidence support recovering from an incident, and being accountable afterwards?

The investigator’s question: Can we show the board, regulators, insurers and counsel what happened, and prove it?

Check	Yes (2)	Partly (1)	No (0)
Identity infrastructure, virtualisation and backup systems are logged, because these are targeted to prevent the organisation recovering.	☐	☐	☐
We can reconstruct a scoped timeline (first activity, accounts, systems, data touched) from retained evidence alone.	☐	☐	☐
The incident response plan names the log sources and owners needed for each stage of an investigation.	☐	☐	☐
A decision log records what was known, when, and who decided what during an incident.	☐	☐	☐
Each incident ends with a review that feeds logging gaps back into Coverage, Routing and Retention.	☐	☐	☐

Stage 8 score: _____ /10



Your Score

Transfer each domain total below.

Stage	Score (out of 10)
01 Collection	
02 Coverage	
03 Integrity	
04 Routing	
05 Retention	
06 Storage	
07 Investigation	
08 Incident Recovery	
Total (out of 80)	

What your score suggests

Total	Where you are	Suggested focus
0–30	Foundations	Start with Collection, Integrity and Retention (Stages 01, 03 and 05). Evidence you do not collect or cannot trust cannot be recovered later.
31–55	Building	Close coverage and retention gaps, then work on Routing and Investigation so the evidence is usable.
56–70	Strong	Test it. Run a timeline-reconstruction exercise on a recent incident and time the answers.
71–80	Leading	Keep it that way: review after each incident, and as the environment and your tools change.



Your three priority actions

1. Stage: _____ Action: _____ Owner: _____

2. Stage: _____ Action: _____ Owner: _____

3. Stage: _____ Action: _____ Owner: _____

A TEN-MINUTE TEST

Pick a recent closed incident. Using only retained logs and no alert context, rebuild the timeline: when did it start, which account was involved, which systems were accessed, did privileges change. How far back could you go, and how long did it take? The result tells you more than the score.



Where Snare fits

Snare is built around this evidence lifecycle and sits alongside the tools you already use. Endpoints and servers are collected with the Snare Agent. Identity, cloud, SaaS, network and admin sources go directly to Snare Central.

The evidence is retained and can be routed to your SIEM or analytics platform, and AskSnare, our cybersecurity AI assistant, lets analysts ask questions of the retained evidence in plain language. It supports analyst judgement; it does not replace it.

Snare Platform Modules

A COMPLETE LOG SECURITY PLATFORM
FROM COLLECTION TO INVESTIGATION

VISIBILITY
INTEGRITY
INTELLIGENCE
A MORE SECURE
TOMORROW



AskSnare now supports
multiple languages.



Snare Agent

COLLECT EVERY
CRITICAL LOG

- Forensic-grade endpoint and OS log collection
- Windows, Linux, and macOS coverage
- Tamper-resistant collection and secure forwarding
- Flexible policy-based forwarding



Snare Central

CENTRALISED CONTROL
AND RETENTION

- Centralised log management and control
- Secure storage, search, and retention
- Supports on-prem environments and broader source ingestion
- Investigation-ready security evidence



Snare Reflector

ROUTE DATA.
YOUR WAY.

- Intelligent routing to SIEM and other destinations
- Filtering, aggregation, and deduplication
- Field remapping and event replay
- Vendor-neutral portability across platforms



AskSnare

INVESTIGATE SMARTER
WITH AI

- AI-assisted investigation and search
- Natural-language interrogation of logs with multi-language support
- Faster threat hunting and analyst workflows
- Intelligent compression and optimisation of retained security data



References

Mandiant / Google Threat Intelligence Group, "M-Trends 2026," 23 March 2026.
cloud.google.com/blog/topics/threat-intelligence/m-trends-2026 | NIST, SP 800-92, Guide to Computer Security Log Management. csrc.nist.gov | MITRE ATT&CK, Detection Strategies and Analytics (data sources deprecated in ATT&CK v18, October 2025).

attack.mitre.org/detectionstrategies/ | PCI SSC, PCI DSS v4.0.1, Requirement 10.5.1.
pcisecuritystandards.org | Microsoft, Windows security auditing event reference (events 1102, 4104, 4624, 4625, 4672, 4688, 4698, 4720, 4728, 4732, 4768, 4769, 4771, 7045).
learn.microsoft.com |



Toll Free US: 1(800) 834 1060
Asia/Pacific: +61 8 8213 1200
UK/Europe: +44 (800) 368 7423

AMERsales@prophecyinternational.com
APACsales@prophecyinternational.com
EMEA sales@prophecyinternational.com

