snare
A PROPHECY SOLUTION

AI-Ready Logging Checklist

Is Your Logging Foundation Defensible in an AI-Driven Investigation?

AI-Ready Logging Checklist

Is Your Logging Foundation Defensible in an AI-Driven Investigation?

Artificial intelligence may accelerate detection and analysis.

It does not replace evidence.

Use this checklist to assess whether your logging environment is operationally sound, defensible, and investigation-ready.

Scoring Your Readiness

For each section:

0–1 checks = High Risk
2–3 checks = Moderate Risk
4+ checks = Strong Control

If you score High Risk in any category, prioritise remediation in your next security roadmap cycle.

AI-Ready Logging Checklist

1. Log Source Coverage

□ All critical endpoints are generating security event logs
□ Domain controllers and identity infrastructure are fully logged
□ Privileged account activity is captured consistently
□ Cloud workloads and SaaS audit logs are collected
□ Network security devices forward complete event telemetry

Risk if unchecked:

AI and analytics operate on partial visibility.

2.Log Integrity & Tamper Resistance

□ Logs are written in a way that prevents unauthorised modification
□ Administrative users cannot delete or alter collected logs
□ There is separation between collection and analytics platforms
□ Integrity validation checks are performed regularly

Risk if unchecked:

Evidence may not withstand regulatory or legal scrutiny.

3.Retention & Historical Context

□ Log retention aligns to regulatory and investigation requirements
□ Retention is not solely dependent on SIEM licensing limits
□ Historical logs can be accessed without rehydration delays
□ Storage architecture supports long-term forensic review

Risk if unchecked:

Investigations lose context beyond short retention windows.

4. Missing Log Detection

□ The team is alerted when a critical log source stops reporting
□ Baselines exist for expected log volume per source
□ There is monitoring for unusual drops in telemetry
□ Log pipeline health is monitored independently of analytics alerts

Risk if unchecked:

Silent failures create invisible security gaps.

5. Collection Optimisation & Cost Control

□ Log filtering occurs at the collection layer, not only at the SIEM
□ High-volume, low-value logs are rationalised before ingestion
□ Compliance retention is separated from high-cost analytics tiers
□ Ingestion cost growth is reviewed quarterly

Risk if unchecked:

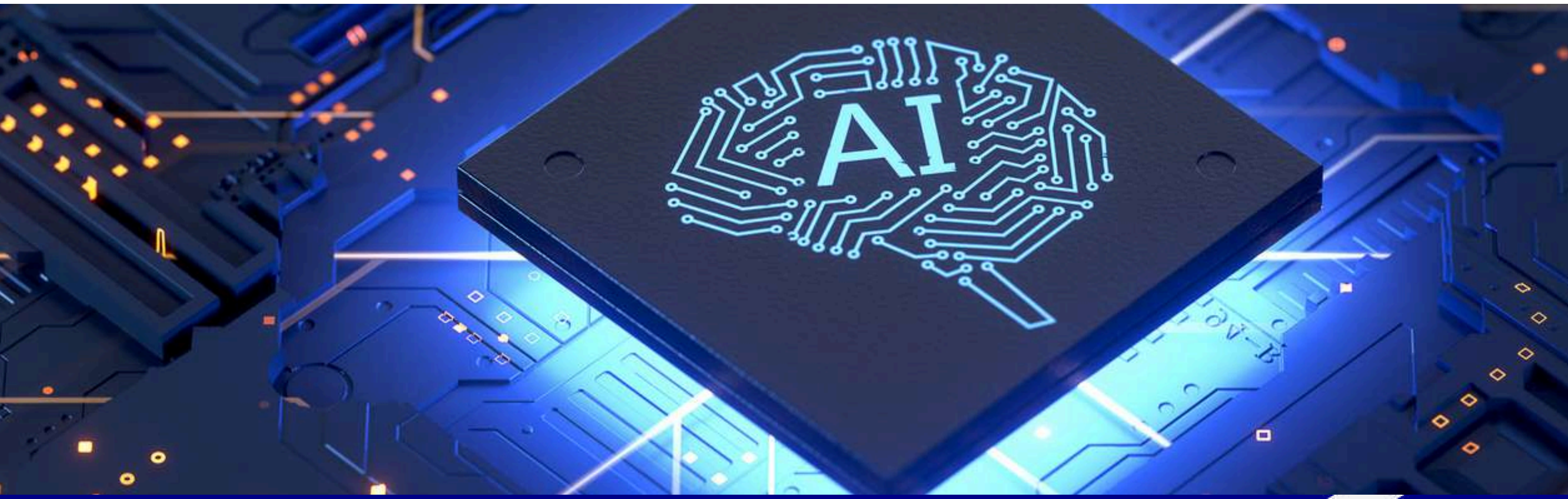
Budget pressure drives unsafe visibility reductions.

6. Replay & Investigation Capability

□ Logs can be replayed independently of the analytics platform
□ Raw event data is preserved for forensic reconstruction
□ Analysts can reconstruct timelines without vendor constraints
□ Chain-of-custody processes are documented

Risk if unchecked:

Investigations rely on incomplete summaries rather than evidence.



7. Governance & Accountability

□ Logging ownership is formally assigned
□ Logging standards are documented and enforced
□ Logging posture is reviewed at least annually
□ Logging maturity is benchmarked against frameworks such as:

- Australian Cyber Security Centre Essential Eight
- NIST Cybersecurity Framework
- ISO 27001

Risk if unchecked:

Logging becomes operational rather than strategic.

Executive Reflection Questions

- Would you confidently defend your logging posture in litigation?
- Could you prove log integrity to a regulator?
- Are logging decisions currently driven by cost rather than risk?
- If a critical log source went silent today, how long before you knew?

Final Positioning Statement

AI may assist investigations.

But only logs provide evidence.

Your logging foundation determines whether your organisation can explain, defend, and withstand scrutiny in 2026 and beyond.

Next Steps

Read : *The 5 Logs Most Often Missing During Breach Investigations*

Book : *A Log Strategy Session with a Snare Specialist*

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
EMEAsales@prophecyinternational.com

snare
A PROPHECY SOLUTION